International Journal on Advances in Systems and Measurements

2012 vol. 5 nr. 1&2

The *International Journal on Advances in Systems and Measurements* is published by IARIA.
ISSN: 1942-261x
journals site: http://www.iariajournals.org
contact: petre@iaria.org

Sponsored by IARIA
www.iaria.org

International Journal on Advances in Systems and Measurements
Volume 5, Number 1 & 2, 2012

Daniela Dragomirescu, LAAS-CNRS / University of Toulouse, France
Matthew Dunlop, Virginia Tech, USA
Mohamed Eltoweissy, Pacific Northwest National Laboratory / Virginia Tech, USA
Paulo Felisberto, LARSyS, University of Algarve, Portugal
Miguel Franklin de Castro, Federal University of Ceará, Brazil
Mounir Gaidi, Centre de Recherches et des Technologies de l'Energie (CRTEn), Tunisie
Eva Gescheidtova, Brno University of Technology, Czech Republic
Tejas R. Gandhi, Virtua Health-Marlton, USA
Teodor Ghetiu, University of York, UK
Gonçalo Gomes, Nokia Siemens Networks, Portugal
João V. Gomes, University of Beira Interior, Portugal
Luis Gomes, Universidade Nova Lisboa, Portugal
Antonio Luis Gomes Valente, University of Trás-os-Montes and Alto Douro, Portugal
Diego Gonzalez Aguilera, University of Salamanca - Avila, Spain
Genady Grabarnik,CUNY - New York, USA
Craig Grimes, Nanjing University of Technology, PR China
Stefanos Gritzalis, University of the Aegean, Greece
Richard Gunstone, Bournemouth University, UK
Jianlin Guo, Mitsubishi Electric Research Laboratories, USA
Mohammad Hammoudeh, Manchester Metropolitan University, UK
Petr Hanáček, Brno University of Technology, Czech Republic
Go Hasegawa, Osaka University, Japan
Henning Heuer, Fraunhofer Institut Zerstörungsfreie Prüfverfahren (FhG-IZFP-D), Germany
Paloma R. Horche, Universidad Politécnica de Madrid, Spain
Vincent Huang, Ericsson Research, Sweden
Friedrich Hülsmann, Gottfried Wilhelm Leibniz Bibliothek - Hannover, Germany
Travis Humble, Oak Ridge National Laboratory, USA
Florentin Ipate, University of Pitesti, Romania
Imad Jawhar, United Arab Emirates University, UAE
Terje Jensen, Telenor Group Industrial Development, Norway
Liudi Jiang, University of Southampton, UK
Teemu Kanstrén, VTT Technical Research Centre of Finland, Finland
Kenneth B. Kent, University of New Brunswick, Canada
Fotis Kerasiotis, University of Patras, Greece
Andrei Khrennikov, Linnaeus University, Sweden
Alexander Klaus, Fraunhofer Institute for Experimental Software Engineering (IESE), Germany
Andrew Kusiak, The University of Iowa, USA
Vladimir Laukhin, Institució Catalana de Recerca i Estudis Avançats (ICREA) / Institut de Ciencia de Materials de Barcelona (ICMAB-CSIC), Spain
Kevin Lee, Murdoch University, Australia
Andreas Löf, University of Waikato, New Zealand
Jerzy P. Lukaszewicz, Nicholas Copernicus University - Torun, Poland
Zoubir Mammeri, IRIT - Paul Sabatier University - Toulouse, France
Sathiamoorthy Manoharan, University of Auckland, New Zealand
Stefano Mariani, Politecnico di Milano, Italy
Paulo Martins Pedro, Chaminade University, USA / Unicamp, Brazil

Daisuke Mashima, Georgia Institute of Technology, USA
Don McNickle, University of Canterbury, New Zealand
Mahmoud Meribout, The Petroleum Institute - Abu Dhabi, UAE
Luca Mesin, Politecnico di Torino, Italy
Marco Mevius, HTWG Konstanz, Germany
Marek Miskowicz, AGH University of Science and Technology, Poland
Jean-Henry Morin, University of Geneva, Switzerland
Fabrice Mourlin, Paris 12th University, France
Adrian Muscat, University of Malta, Malta
Mahmuda Naznin, Bangladesh University of Engineering and Technology, Bangladesh
George Oikonomou, University of Bristol, UK
Arnaldo S. R. Oliveira, Universidade de Aveiro-DETI / Instituto de Telecomunicações, Portugal
Aida Omerovic, SINTEF ICT, Norway
Victor Ovchinnikov, Aalto University, Finland
Telhat Özdoğan, Recep Tayyip Erdogan University, Turkey
Gurkan Ozhan, Middle East Technical University, Turkey
Constantin Paleologu, University Politehnica of Bucharest, Romania
Matteo G A Paris, Universita` degli Studi di Milano,Italy
Vittorio M.N. Passaro, Politecnico di Bari, Italy
Giuseppe Patanè, CNR-IMATI, Italy
Marek Penhaker, VSB- Technical University of Ostrava, Czech Republic
Juho Perälä, VTT Technical Research Centre of Finland, Finland
Florian Pinel, T.J.Watson Research Center, IBM, USA
Ana-Catalina Plesa, German Aerospace Center, Germany
Miodrag Potkonjak, University of California - Los Angeles, USA
Alessandro Pozzebon, University of Siena, Italy
Vladimir Privman, Clarkson University, USA
Konandur Rajanna, Indian Institute of Science, India
Stefan Rass, Universität Klagenfurt, Austria
Candid Reig, University of Valencia, Spain
Teresa Restivo, University of Porto, Portugal
Leon Reznik, Rochester Institute of Technology, USA
Gerasimos Rigatos, Harper-Adams University College, UK
Luis Roa Oppliger, Universidad de Concepción, Chile
Ivan Rodero, Rutgers University - Piscataway, USA
Lorenzo Rubio Arjona, Universitat Politècnica de València, Spain
Claus-Peter Rückemann, Leibniz Universität Hannover / Westfälische Wilhelms-Universität Münster / North-German Supercomputing Alliance, Germany
Subhash Saini, NASA, USA
Mikko Sallinen, University of Oulu, Finland
Christian Schanes, Vienna University of Technology, Austria
Rainer Schönbein, Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB), Germany
Guodong Shao, National Institute of Standards and Technology (NIST), USA
Dongwan Shin, New Mexico Tech, USA
Larisa Shwartz, T.J. Watson Research Center, IBM, USA
Simone Silvestri, University of Rome "La Sapienza", Italy

International Journal on Advances in Systems and Measurements
Volume 5, Numbers 1 & 2, 2012

CONTENTS

pages 70 - 88

Dependable Estimation of Downtime for Virtual Machine Live Migration

Felix Salfner, SAP Innovation Center Potsdam, Germany
Peter Tröger, Hasso-Plattner-Institute at University of Potsdam, Germany
Matthias Richly, Hasso-Plattner-Institute at University of Potsdam, Germany

Visualizing the Effects of Measurements and Logic Gates On Multi-Qubit Systems Using Fractal Representation

Mate Galambos
Department of Telecommunications
Budapest University of Technology and Economics
Budapest, Hungary
e-mail: mate.galambos@mcl.hu

Sandor Imre
Department of Telecommunications
Budapest University of Technology and Economics
Budapest, Hungary
e-mail: imre@hit.bme.hu

***Abstract*—Visual representation is essential to share ideas, interpret previous achievements or formulate new algorithms quickly and intuitively. Fractal representations of multi-qubit systems can visualize individual qubits even in case of entanglement. The proposed representation can be used to easily determine measurement probabilities. Connections with density matrices for pure and mixed states are also discussed. Finally, we visualize the effects of several single-qubit gates and controlled gates.**

Keywords - Quantum information; representation; visualization; fractals; binary trees

I. INTRODUCTION

Quantum computing and communications already promises applications that outperform classical solutions, e.g. Shor's prime factorization [2], the unconditional security of quantum cryptography [3], or practical realization of quantum communication [4]. It is also likely that this discipline will become even more important during the up-coming years. However, quantum mechanics is well-known for its counterintuitive nature that is hard to visualize thus making it problematic to quickly share ideas, interpret previous achievements, or formulate new algorithms quickly and intuitively.

In order to be able to solve these issues, a visual representation could be useful. The Bloch-sphere sufficiently represents one qubit [5] [6], or more qubits that are separable, but entanglement—one of the most important phenomena in quantum informatics—eludes this type of visualization.

Another possible approach is to use objects that have enough degree of freedom to represent the whole system. However, this method usually conceals the inner structure, and does not give us an idea of what happens if we measure the state of few qubits instead of the whole system—a method used in many algorithms and protocols. This approach does not handle well those cases where the addition of more qubits is decided or when dividing the system into smaller parts.

There are existing methods to generalize the Bloch-sphere e.g. through a mathematical structure called Hopf-Fibrations [7], but the arising geometrical structures are vastly complex and hard to read, thus making the method useless as a visualization technique.

An ideal visualization scheme would preserve the mathematical structure of a multi-qubit system in a way that is easy to interpret by the naked eye using compact and two dimensional images. The ideal solution should also give at least some insight to the states of single qubits, would work for any finite number of qubits, as well as it should show entanglement. Our work aims to examine the properties of such a scheme based on fractals with emphasis on the effect of measurement and logic gates [1].

This paper is organized as follows: Section II, III present the new proposed approach using fractals in single and multi-qubit states while and IV generalizes to non-binary multipartite quantum systems. Section V discusses the measurement, while Section VI explores the question of changing the order of qubits. Section VII and VIII focus on the connection with density matrices and possible representation of mixed states. Section IX and X discuss the effect of single-qubit and controlled gates in terms of the fractal representation. Finally we conclude the paper in Section XI.

II. REPRESENTATION OF A SINGLE QUBIT

For the sake of clarity, we begin with the single-qubit representation and the case of multiple qubits will be derived from these results.

The general form of a single qubit can be formulated by means of complex-valued probability amplitudes in exponential form and orthogonal basis vectors as:

$$|\varphi\rangle = A \cdot \exp(i \cdot \alpha) \cdot |0\rangle + B \cdot \exp(i \cdot \beta) \cdot |1\rangle, \quad (1)$$

$$A^2 + B^2 = 1. \quad (2)$$

Where A B α and β are real numbers. Let us draw a horizontal bar shown in Fig 1. Using a vertical gray line let us divide it into a black and a white side with respective lengths of A^2 and B^2 where the total length of the stripe is considered 1. This should give the probabilities of a measurement on the qubit producing the value 0 or 1. To avoid ambiguity, the black part of the bar corresponding to the measurement yielding 0 should always be placed first, and the white part corresponding to the measurement value 1

should placed second, thus representing them in ascending order.

A gray frame is added to the bar so that the white part can be easily seen in front of a white background. If the phase angle is zero or equivalent to zero due to 2π periodicity the horizontal line representing the phase information is considered to be behind the grey frame and is not visible.

A is proportional to the z coordinate of the Bloch vector and the difference $\beta-\alpha$ is proportional to the azimuth angle of the Bloch vector. As these values are close to each other for close quantum states in the Bloch representation, the closeness of widths of the bars and heights of the lines representing the phase indicate fidelity.

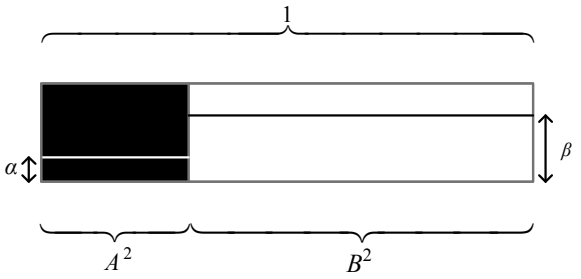


Figure 1. Representation of a single qubit. The respective lengths A^2 and B^2 of the black and white sides of the bar correspond to the probability of a measurement on the qubit yielding the bit value 0 or 1.

III. Representation of Tensor Products and Multi-Qubit Systems

Distributivity allows more than one way to mathematically formulate certain multi-qubit states, as it is illustrated in Equation 3.

$$\left(a|0\rangle + b|1\rangle\right)\otimes c|0\rangle \equiv ac|00\rangle + bc|10\rangle \qquad (3)$$

The left hand side of the equation will be referred as separated, the right hand side as expanded form of the tensor product. Each formulation can be visually represented in a different way. In the following section, an introduction is given to both representation, and the connection between them will be clarified.

A. Representing Expanded Tensor Products

In case the state of the multi-qubit system is given in the form of an expanded tensor product, the probability amplitudes can be written in exponential form. The system can be represented as series of columns, each column consisting of black or white bars stuck upon each other as shown in Fig. 2. The colors of the bars represent the qubit values from top to bottom, the width of the column the probability of the state corresponding to those values, and a horizontal line dividing the lowermost bar of the column the phase. This means we associate only one phase to every bit value combination. As in the single qubit case if the phase angle is 0°, the horizontal line is not visible.

The quantum system as a whole can be represented by placing these columns next to each other in ascending bit value order and merge those neighboring bars that has the same bit value and phase. This merging step produces one bar with black and white parts for the first qubit, two bars for the second etc. because of the ascending order of qubits. Since the lowermost bars are the most likely to have differently colored neighbors they are the most logical place for the lines indicating the phase.

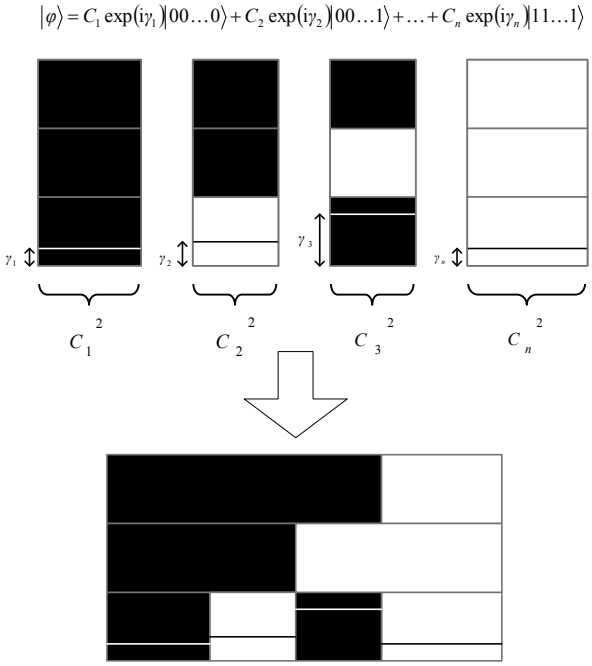


Figure 2. Representation of a multi-qubit system. Columns of black and white bars corresponding to the expanded tensor product describing the system. Probability amplitudes are written in Eulerian form, the width of each column is given by the square of the Eulerian amplitude and horizontal lines added to the lowermost bars to indicate the phase. The color of the bars in the columns will be determined by the bit values, from top to bottom black corresponding to 0 and white corresponding to 1.

B. Representing Separated Tensor Products

In order to represent separated tensor product of single qubits, the scaled down version of the bar representing the qubits should be copied under each black and white halves of the previous qubits as shown in Figure 3 [1]. This can be useful when the tensor product of known single qubit states have to be calculated.

If the system can be described as a separated tensor product of groups of inseparable qubits, then instead of single bars the representation of expanded tensor products should be copied under each other.

C. Connection Between the Representation of Expanded and Separated Tendor Products

The representations of separated tensor products are very similar to the expanded tensor products the only difference being the position of the lines indicating the phase. This follows from the definition of the two representations and the

properties of the tensor product. Thus the representation of the separated tensor product can be transformed to the representation of expanded tensor product by copying the horizontal lines to the lowermost bars and adding their heights taking 2π periodicity into consideration practically adding the phase angles of the qubits.

If the lowermost bars inherit the phase information, properties of the system as a whole can be read from the representation, while the non inheriting form makes it easy to make conclusions regarding the phase of the subsystems.

The representation of expanded tensor products can be transformed to the non inheriting representation of separated tensor products by reversing the process. This should be done by ensuring that the bars or groups of bars having the same phase are exact copies of each other as described in Section III B. If this step cannot be done that is an indication of the qubits being inseparable. Finally, in both cases the resulting structures are statistically self similar with the bars serving as unit fractal objects.

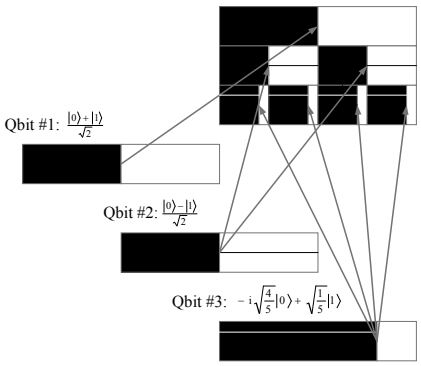


Figure 3. Fractal representation of a multi-qubit system and the separable qubits that serve as its building blocks. Note that after copying the phase information to the lowermost bars and adding their heights the same picture arises as from the representation of the expanded tensor product described in Section III A.

IV. Generalization for Multipartite System

In case of a multipartite quantum system whose parts are not qubits, but quantum systems with a small number of states, the representation can be generalized to describe this non-binary system. For example: three particles each with four excitation state and a ground state.

To represent the extra states, more bars with different colors should be added to the representation. These bars are packed above each other to create columns whose width represents the probability of a measurement finding the system in a certain state, while horizontal lines in the lowermost bars with complementary color [8] to the color of the bar represent the phase of the state.

In the example of the three particles with the five states each, the color black should be assigned to the ground state, white to the first excitation state, red green and blue to the second third and fourth excitation state. In this case a column whose colors from top to bottom are green, black and blue, with one half width and an orange horizontal line in the middle of the blue bar, means 50% probability of a measurement on the whole system finding the first particle in second excitation state, the second particle in ground state and the third particle in fourth excitation state while the phase of the total system is -1.

Since the color grey is it is own complementary color it should not be used for bars, only for the frame around the bars.

V. Conditional Probablilities

Probabilities of a measurement performed on the system as a whole yielding certain bit values can be read from the width of bars. However if measurements are performed on individual qubits, conditional probabilities can be read from the representation and changes introduced by the measurement can be anticipated. For this the qubits should be ordered from top to bottom in the order of the measurement.

Using the column vector formalism an *n*-qubit state has writes as:

$$|\varphi\rangle = \begin{bmatrix} C_1 \exp(i\gamma_1) \\ C_2 \exp(i\gamma_2) \\ \vdots \\ C_n \exp(i\gamma_n) \end{bmatrix} \tag{4}$$

and the state of the system after the measurement is shown in (5).

$$|\varphi'\rangle = \frac{M|\varphi\rangle}{\sqrt{\langle\varphi|M|\varphi\rangle}} \tag{5}$$

If the first qubit is measured and the measurement corresponds to one of the states used as the basis than the matrix of the measurement on the whole system can be written in the form of Equation 6 and 7.

$$M = \begin{bmatrix} m_0 & 0 \\ 0 & m_1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \cdots \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{6}$$

$$M = \begin{bmatrix} m_0 & & & & & \\ & \ddots & & & 0 & \\ & & m_0 & & & \\ & & & m_1 & & \\ & 0 & & & \ddots & \\ & & & & & m_1 \end{bmatrix} \tag{7}$$

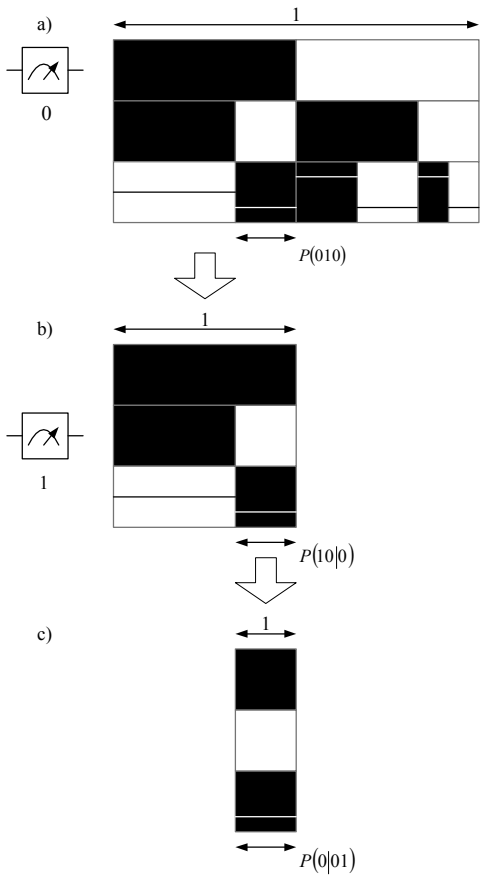


Figure 4. The effect of the measurements on single qubits. If we measure the first qubit in the system described by the fractal representation in part (a) of the figure and the measurement yields a zero then after the measurement the half under the black part of the first row shown in part (b) will describe the system. If the second qubit is measured and the measurement yields a one, then after the second measurement the system will be described by the half under the black part of the second row shown in part (c) of the figure. Thus the same width compared to the width of the different fractals in (a) (b) and (c) that are all considered unit length will give us the conditional probabilities of measurements on the rest of the system after the first few qubit was measured and found in certain states. The white arrows connect individual steps.

where either m_0 is 1 and m_1 is 0 or m_0 is 0 and m_1 is 1 depending on which basis vector was detected. Since the vector elements from top to bottom correspond to the columns of the representation from left to right, and

$$M|\varphi\rangle = \begin{bmatrix} m_0 C_1 \exp(i\gamma_1) \\ m_0 C_2 \exp(i\gamma_2) \\ \vdots \\ m_1 C_n \exp(i\gamma_n) \end{bmatrix} \quad (8)$$

this means if the measurement on the first qubit yields a zero, the half under the black part of the uppermost bar have to be examined. If the measurement yields a one, then the half under the white part will be significant as shown in Fig. 4. Taking the self similarity of the representation into consideration these halves also describe single or multi-qubit systems that will correspond to the rest of the system after the measurement is performed on the first qubit. To give the correct probabilities for these subsystems, their widths should be considered unit length according to the denominator in Equation 5. The width of individual columns will represent the conditional probability of the measurement on the rest of the system yielding the values represented by the colors of the bars.

After the measurement, the first qubit, which is now in a classical state, can be separated from the system and this logic can be recursively applied to the following qubits to get the conditional probabilities for the rest of the system after the first *n* qubit was measured.

VI. Changing the Order of Qubits and Recognizing Interchangeable Qubits

In some cases the question 'whether two qubits are in the same state or not' can be interesting. If the system is represented in a way corresponding to the separated tensor product, then two qubits can be determined to be in the same state if the bars representing them are the scaled versions of the same single qubit as shown in Fig. 5.

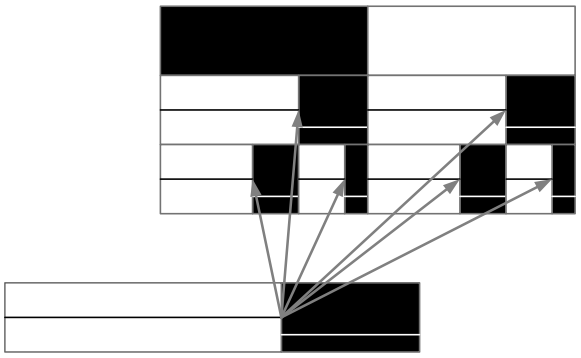


Figure 5. Since the second and third rows corresponding to the second and third qubits are consisting of scaled copies of the same single qubit representation, they are interchangeable.

If the representation is as described in Section III A, two qubits can be determined to be interchangeable if after changing the bit order the same fractal representation arises as shown in Figure 6.

The bit order can be changed by the following steps. First, changing the two lines of bars representing the two qubits, then determining the columns that make up the fractal representation by cutting the representation up at every point where two bars meet, copying the phase information to the lowermost bars, and finally reordering the columns so that the bit values represented by them are in ascending order and merging them in a way described in Section III A to form a new fractal representation.

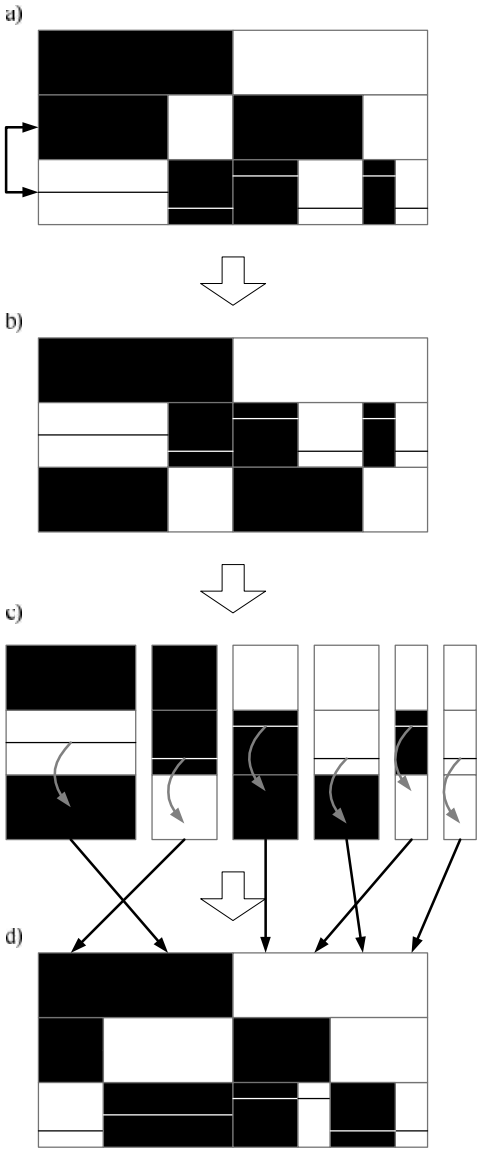


Figure 6. To change the order of two qubits, first the order of the corresponding rows have to be changed as shown in part (a) and (b) of the picture. After that the columns making up the representation have to be identified, and the phase information copied in the lowermost bars as shown by the gray arrwes in part (c). Finally, the columns have to be rearranged to ascending order as shown by the black arrows and the neighboring bars with the same color and phase remerged. Since the vector representations in this example before and after the reordering look differently, the two qubit was not interchangeable.

VII. Connection With the Vector Representation of Complex Numbers and the Density Matrix

In this section, the connections with other representations will be explained. Although using the absolute value square of the probability amplitude for the widths has its advantages, often the complex values of the probability amplitudes have to be represented in a vector form. The phase angle and thus the angle in polar coordinates can be read from the representation however for the length of the vector the square root of the columns have to be calculated. In a purely geometrical approach, this can be constructed using a parabola shown in Fig 7., whose equation is

$$y = x^2 \quad (9)$$

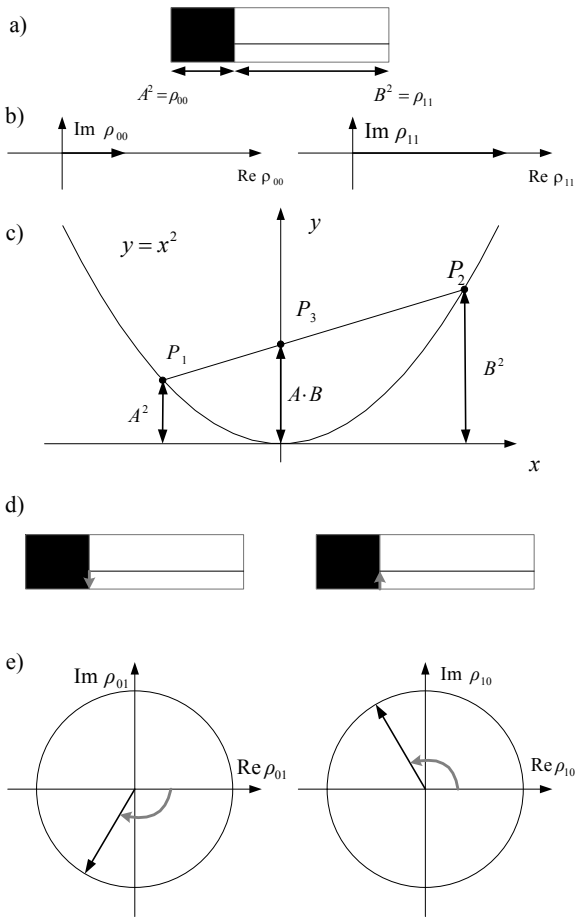


Figure 7. Geometric steps to determine the vector representation of the elements in the density matrix. The widths of the bars in part (a) are used represent the diagonal elements shown in part (b). A parabola shown in part (c) can be used to draft the squares square roots and products of certain lengths. The phase difference shown in part (d) will provide the angle of the vectors in part (e) corresponding to offdiagonal elements of the density matrix. The length of the vectors are given by the distance between the origin and P_3 in part (c).

This parabola can also be helpful if product of lengths or the square root of their product has to be calculated. It is easy to show that the points P_1 P_2 and P_3 are collinear, whose Cartesian coordinates are:

$$P_1 = \left(-A; A^2\right) \quad (10)$$

$$P_2 = \left(B; B^2\right) \quad (11)$$

$$P_3 = (0; AB) \quad (12)$$

This method can be useful when information regarding the density matrix is needed. The width of the columns will correspond to the elements in the main diagonal of the density matrix, and off-diagonal elements can be calculated from the difference in the heights of the horizontal lines representing the phase angles, and the square root of the product of the columns widths. As mentioned previously, this can be geometrically achieved by the following steps: 1, measuring them on the *y* axis, 2, projecting these heights onto the parabola, 3, connecting the resulting points with a line as shown in Figure 7.

From the density matrix of pure states, the fractal representation can be created using the elements in the main diagonal as widths of the columns and the negative phase angles of the first row in the density matrix as heights of the horizontal lines.

Since the vector representation of the quantum system cannot always be constructed from the density matrix, the fractal representation has a one-to-one correspondence only to the vector representation but not to the density matrix.

VIII. Representation of Mixed States

The fractal representation of these pure states can be used to represent the mixed state, if the mixed state is described by an ensemble of a small number of differing pure states.

$$|\varphi_{21}\rangle = |00\rangle \qquad |\varphi_{22}\rangle = |11\rangle$$

$$\rho_2 = P_1 |\varphi_{21}\rangle\langle\varphi_{21}| + P_2 |\varphi_{22}\rangle\langle\varphi_{22}|$$

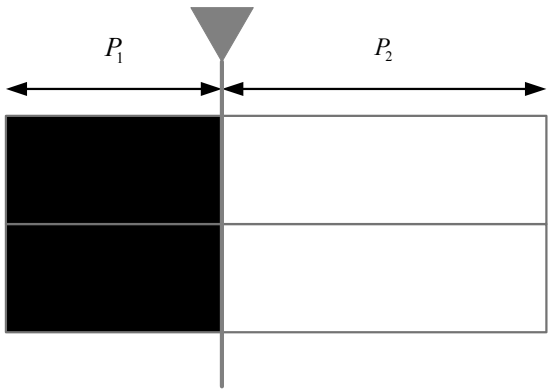


Figure 8. Representation of a mixed state that can be described as an ensemble of quantum systems in two possible pure states. The widths of the representations of pure states are scaled down by the factor of their weight in the ensemble.

The representation can be created by scaling the width of the fractal representation of each pure state by the factor of their probability in the ensemble and drawing them next to each other as shown in Fig. 8. The pure states are separated by grey lines extending above and below the fractal representation. For the sake of visibility, a gray triangle is added above the points where the representations of pure states meet.

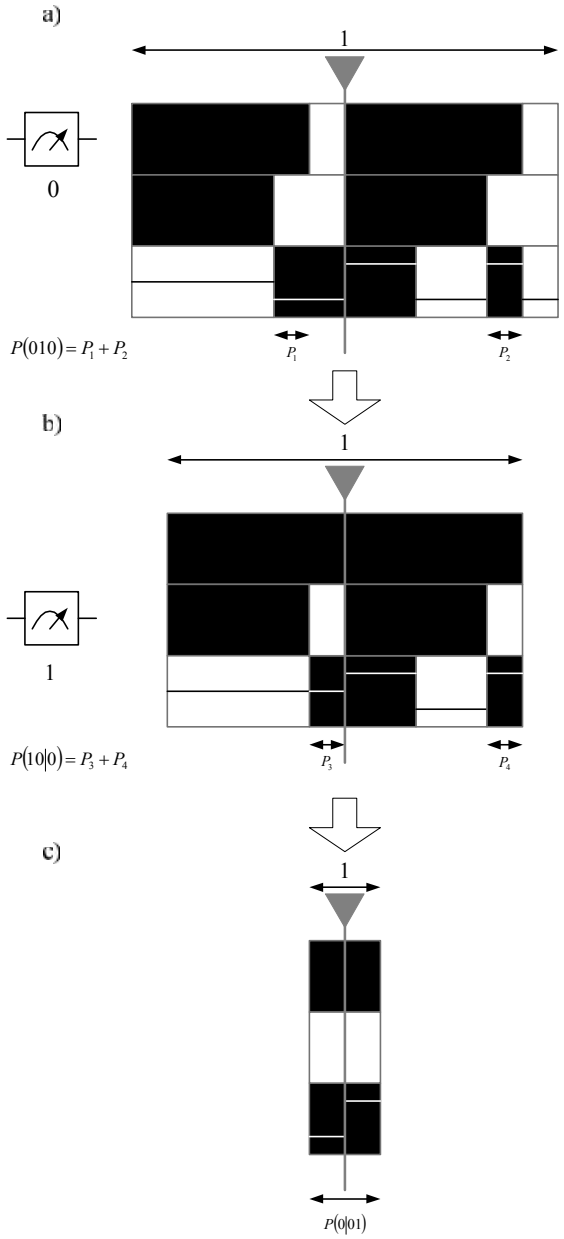


Figure 9. If a measurement is performed on the mixed state as a whole, the probability of the measurement collapses it into a certain state equals the sum of all the widths of the columns whose colors correspond to the state. If measurements are performed on single qubits, the logic described in Section V has to be applied to all of the representations of pure states separately, and the conditional probabilities will be given by the combined widths of all the columns with the corresponding colors. Note the similarities and differences between Figure 4 and Figure 9.

If a measurement is performed on all the qubits in the ensemble, the probability of a measurement yielding a string of zeroes or ones equals the combined widths of all the

columns whose color corresponds to the bit values in the string.

If the qubits of the ensemble are measured one by one, then the logic described in Section V has to be applied to all the fractal representations of pure states, and the conditional probability on the ensemble will be given by the combined widths of all the columns corresponding to the strings of bit values (see in Fig. 9.).

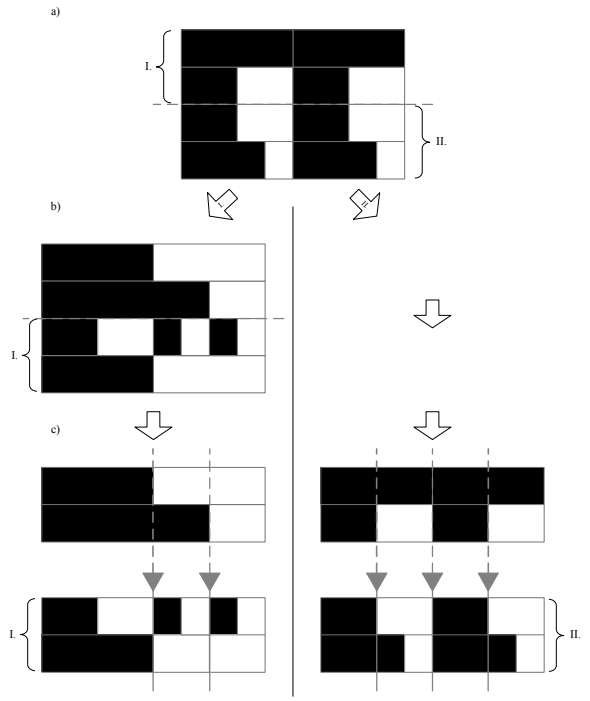


Figure 10. It seems that if a multi-qubit system is divided into two subsystems the parts that have to be handled as they are part of the same pure state are determined by color of the other qubits above them. For this the reordering of the qubits shown in part (b) is necessary for subsystem I since its qubits are not on the bottom of the representation. The same is not true to subsystem II.

The density matrix can be easily constructed from the fractal representation of mixed states. The steps are the following: 1, creating the density matrices of individual pure systems as described in Section VII., 2adding up the same matrix elements weighted by their probability in the ensemble.

Although we do not have a general proof yet, it seems that the subsystem of an entangled pure multi-qubit system can only be represented by copying the bits of the subsystem in the fractal representation below the rest of the qubits and handling them as if they would represent different pure states if the bars above them have the same colors.

It seems that if the pure multi-qubit system has to be divided into two or more subsystems that are all need to be examined, then as many copies with reordered rows of the original version of the fractal representation are needed as the number of subsystems (see in Fig. 10.).

This means that the usage of these extended grey lines could indicate more qubits not shown above the fractal representation whose bars meet where the extended lines indicate.

Because the density matrix is easily constructed from the fractal representation, the density matrix of subsystems seems to be created with this method without actually calculating the partial traces.

IX. SINGLE QUBIT GATES

In this section, the effects of the most common quantum gates are discussed in terms of the fractal representation.

A. Pauli X Gate

The Pauli X gate swaps the bit values thus effectively changing the color of the bars to the opposite. This means the bars should be rearranged with the purpose of satisfying the convention of ascending bit value order.

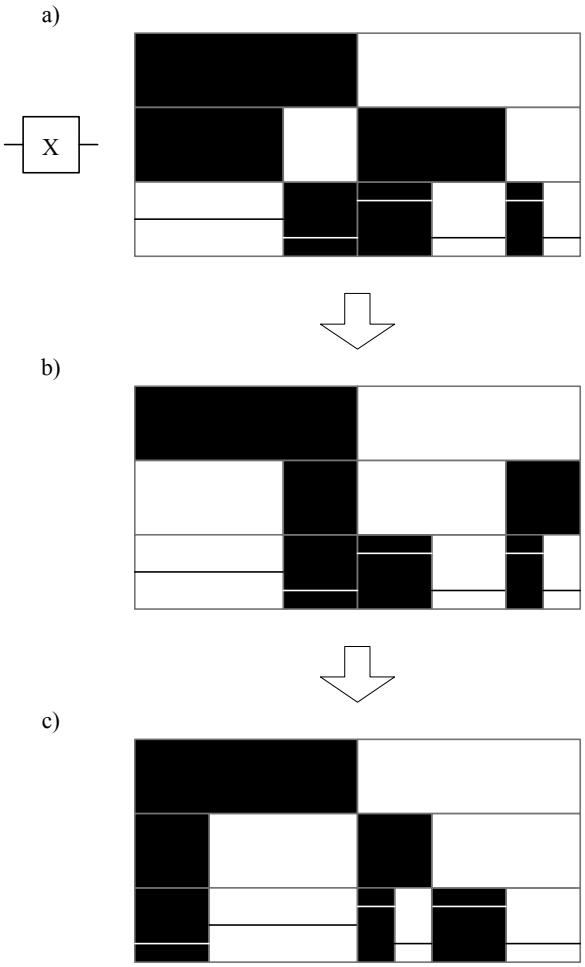


Figure 11. Effect of the Pauli X gate. All the colors of the bars in the row corresponding to the effected qubit are changed to the opposite. After the change an additional step of rearranging the columns in ascending order is required.

If the Pauli X gate affects one qubit in a multi-qubit system, the color of each bar in the row corresponding to the

affected qubit has to be changed, followed by the step of reordering the columns and remerging the neighboring bars with the same color and phase (Fig. 11.).

B. Pauli Y Gate

The Pauli Y gate acting on a single qubit changes the color of the bars to the opposite, and shifts upward the horizontal line indicating the phase in the bar changing from black to white with three fourths of the bars height while the in the bar changing from white to black the shift is only one fourth. During the shifting, the 2π periodicity of the phase has to be taken into consideration. Since the color is changed, an additional step of reordering is necessary (see Fig. 12.).

In case of a multi-qubit system, this color change affects every bar in the row corresponding to the qubit, while the phase change affects the lines I the lowermost bars. A step of reordering and remerging the columns is also necessary.

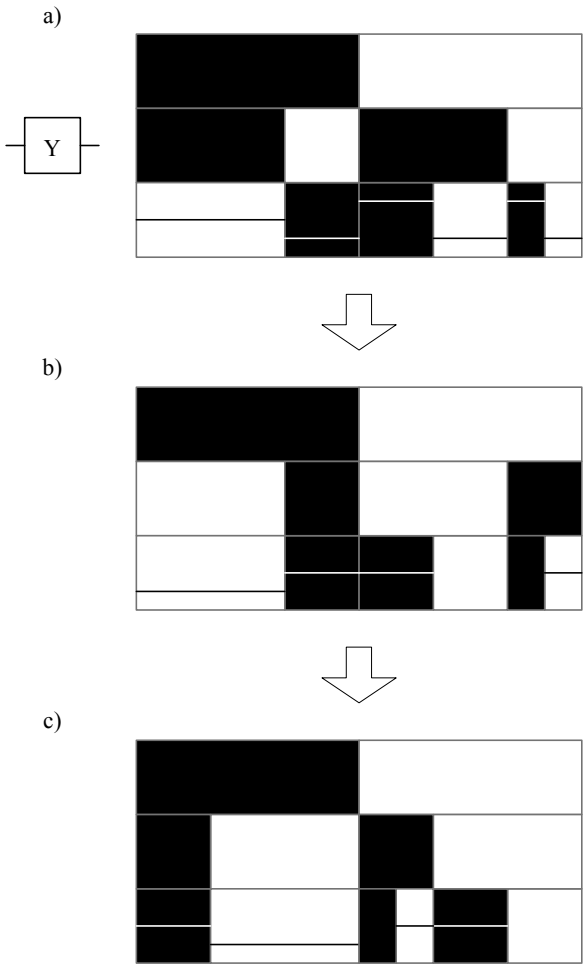


Figure 12. Effect of the Pauli Y gate. The colors in the row corresponding to the affected qubit change color and changes in the phase are introduced depending on the original color of the bars. Under black bars changing white the horizontal lines indicating the phase shift upward with three fourth of the bars height while under bars changing form while to black the shift is only one fourth. If the lines would shift above the bar the 2π periodicity has to be taken into consideration.

C. Pauli Z Gate

The Pauli Z gate does not change the color but shifts the line indicating the phase in the white colored bar upward with half the height of the bar. The 2π periodicity has to be taken into consideration, but reordering is not necessary.

In case of a multi-qubit system, the change will affect all the lines in the lowermost bars under the white bars in the row corresponding to the qubit as shown in Fig. 13.

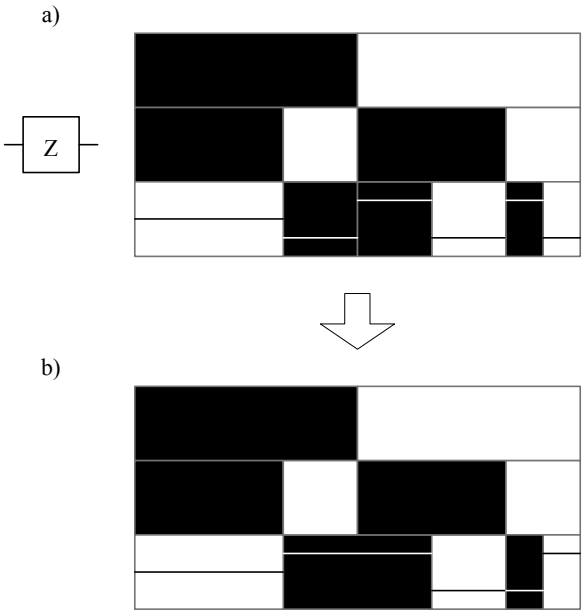


Figure 13. Effect of the Pauli Y gate. The color in the affected row remains unchanged while the lines representing the phase shif upwards with half the height of the bars below the white bars in row corresponding to the affected qubit. Since the colors are unchanged the additional step of reordering is not necessary but merging or cutting of bars can be necessary because of the phase changes introduced by the operation.

D. Hadamard Gate

The effect of the Hadamard gate on a single qubit can be easily calculated using the sum and difference of the probability amplitudes represented in vector form. This can be constructed using the method introduced in Section VII.

If a Hadamard operation is performed on one qubit of a multi-qubit system (shown in Fig. 14.), first the order of the qubits in the representation has to be changed so that the qubit affected by the operation becomes the lowermost. To perform the Hadamard operation, the lowermost bars should be grouped in way that those under the same colors are in the same group. Than the operation can be performed on each group in a way like they are all single qubits. Next the order of the qubits can be changed again, meaning the line representing the affected qubit does not have to be the lowermost.

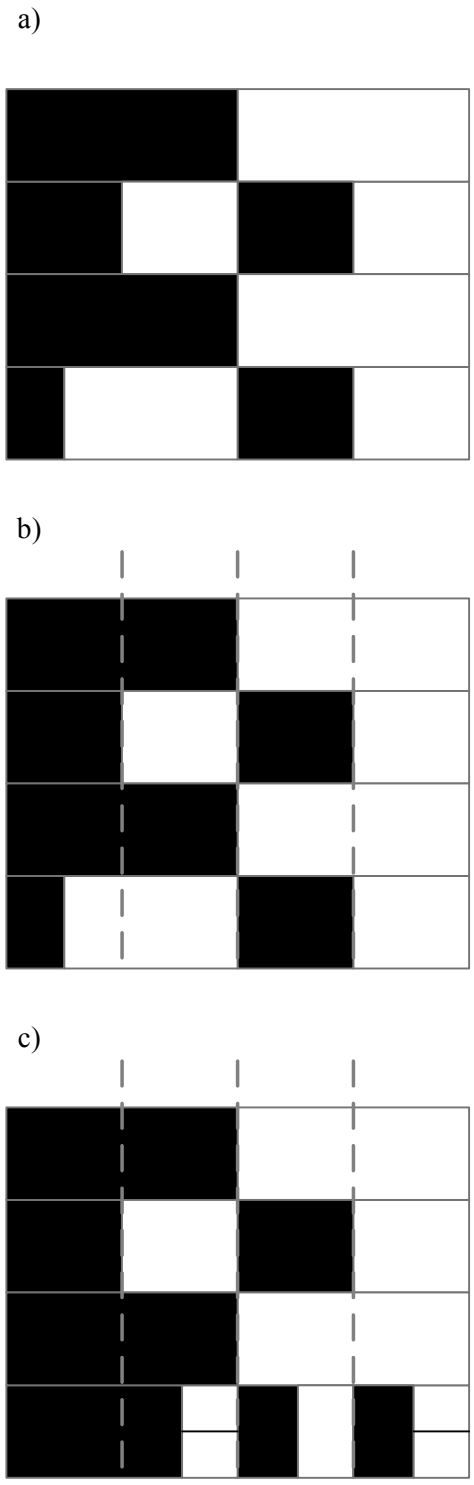


Figure 14. The effect of the Hadamard gate on the qubit corresponding to the lowermost row. The parts of bars in the lowermost row should be grouped together that are under the columns of bars with the same colors as shown in part (b). The Hadamard gate affects the bars of the lowermost row in the same group as if they are single qubits states as shown in part (c).

E. General Single Qubit Gate

If a generalized single qubit gate is given with the matrix of

$$U = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \tag{13}$$

then the effect of the gate on the last qubit can be described by the matrix

$$V = I \otimes \cdots \otimes I \otimes U = \begin{bmatrix} u_{11} & u_{12} & & & & & & 0 \\ u_{21} & u_{22} & & & & & & \\ & & u_{11} & u_{12} & & & & \\ & & u_{21} & u_{22} & & & & \\ & & & & \ddots & & & \\ & & & & & & u_{11} & u_{12} \\ 0 & & & & & & u_{21} & u_{22} \end{bmatrix}. \tag{14}$$

Thus the effect on the state vector can be described as the original U gate affecting numerous single qubits with probability amplitudes like the neighboring ones in the state vector. Since only those neighbors are grouped together whose corresponding bit value only differs in the last digit, this means that in the fractal representation the gate affecting the last qubit acts as if it is acting on several single qubits, who constitute of the lowermost bars of columns whose color differs in only the color of the lowermost bar. In other words, the place where any two bars meet except for the lowermost bars marks the border of a group and the gate acts as if it is acting on the state described by the lowermost bars in the same group.

In case of those gates that have nonzero off-diagonal elements an additional step of reordering and remerging the columns is necessary. If the gate is acting on any other qubit than the last one then the operation can be executed by first changing the bit order and thus the order of the rows followed by the reordering and remerging of the columns, so that the qubit in question becomes the last one.

X. CONTROLLED GATES

In this section the effect of controlled quantum gates are discussed in terms of fractal representation.

A. CNOT Gate

The effect of the Controlled NOT gate is very similar to the effect on the Pauli X gate but only the color of those parts of the bars are changed in the row corresponding to the target bit that are above or below white colored bars of the row corresponding to the control bit (see in Fig.15.).

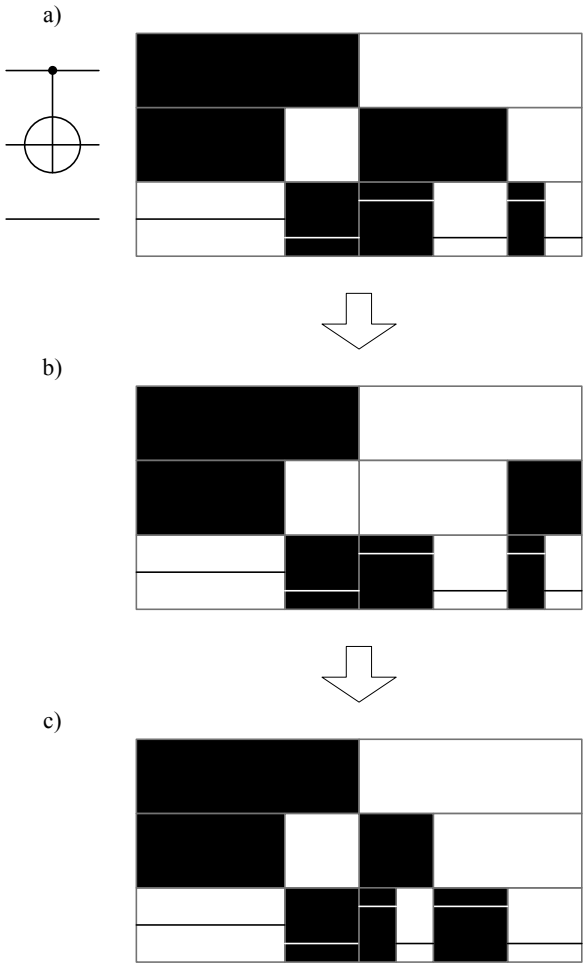


Figure 15. Representation of CNOT operation. The first qubit is the control bit and the second is the target. The effect is very similar to the effect of the Pauli X gate shown in Figure 11, but the color of the bars in the row of the target bit only changes in the columns where the color of the bars corresponding to the control bit is white. This property makes it easy to visualize how entanglement arises from a CNOT operation. Since the color of the bars are changing, an additional step of reordering shown in part (c) is required.

B. General Controlled Gate

A general controlled gate that affects the last qubit if and only if the value of the control bit is 1. In the fractal representation the effect will be similar to the uncontrolled version of the single qubit gate acting on the lowermost row, but only those parts of the bars will be affected that are under the white colored bars in the row corresponding to the control bit.

XI. CONCLUSION

Fractal representations can describe multi-qubits systems while providing insight to the state of individual qubits. In this paper, a possible generalization to non-binary multipartite quantum systems with finite number of discrete states has been presented.

By examining the effect of measurements on the whole system and on individual qubits, we concluded that conditional probabilities regarding measurements on one part of the system yielding certain qubit values after the rest of the qubits have been measured can be read by comparing the widths of the corresponding columns to the appropriate parts of the representation. The state of the system after the measurement yielding the given values is described by these parts.

We explained that the representations of the pure states can be used to represent the mixed state and measurements and operations act on the representation as if they are acting on separate pure states.

The effects of reordering the qubits and the connection with vector representation of complex numbers were discussed and used in examining the effects of certain logic gates. It has been concluded that single qubit operations on the qubit corresponding to the lowermost row act on the representation as if they are acting on single qubits described by a special grouping of the bars in the lowermost row. Controlled gates affect the qubit corresponding to the lowermost bar similarly but only those groups will change that are under white bars in the row corresponding to the control bit.

ACKNOWLEDGMENT

Special thanks to Laszlo Bacsardi and members of the BME Department of Telecommunications for their helpful comments.

REFERENCES

[1] M. Galambos, S. Imre, "New Method for Representation of Multi-qbit Systems Using Fractals", ICQNM 2011, The Fifth International Conference on Quantum, Nano and Micro Technologies, Issue 1, pages 52-56

[2] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM J. Comput. 26 (5): 1484–1509 (1997)

[3] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing”, Proc. IEEE International Conference on Comput., Systems and Signal Process. 1984, pp. 175–179

[4] L. Bacsardi “Satellite Communication Over Quantum Channel”, Acta Astronautica 2007: 61(1–6):151–159

[5] M. Nielsen and I. Chuang, “Quantum Computation and Quantum Information” Cambridge, England: Cambridge University Press, 2000

[6] S. Imre and B. Ferenc, “Quantum Computing and Communications: An Engineering Approach”, Wiley, 2005

[7] D. Chruscinski, “Geometric Aspects of Quantum Mechanics and Quantum Entanglement”, Journal of Physics: Conference Series 30 (2006) 9–16

[8] H. Levkowitz, “Color Theory and Modeling for Computer Graphics, Visualization, and Multimedia Applications”, Springer, 1997

Low-Cost Technology for the Integration of Micro- and Nanochips into Fluidic Systems on Printed Circuit Board: Fabrication Challenges

Nuria Berenice Palacios-Aguilera, Jeroen Bastemeijer, Jeff R. Mollinger, Andre Bossche
Electronic Instrumentation Laboratory
Delft University of Technology
Mekelweg 4,
2628CD Delft, the Netherlands
n.b.palaciosaguilera@tudelft.nl, j.bastemeijer@tudelft.nl,
j.r.mollinger@tudelft.nl, a.bossche@tudelft.nl

Venkata R. S. S. Mokkapati
Nanosystems, Health and Environment Department
Austrian Institute of Technology
Donau city strasse 1
1220 Vienna, Austria
v.r.s.s.mokkapati.fl@ait.ac.at

Hendrikus Antonius Visser, Remko Akkerman
Production Technology Group
University of Twente
7500AE Enschede, the Netherlands
h.a.visser@ctw.utwente.nl, r.akkerman@ctw.utwente.nl

***Abstract*—Nowadays, micro- and nanochips are usually fabricated with Silicon and/or glass. A simple, low-cost and reliable integration packaging method that provides flexibility to the incorporation of electronic and fluidic devices into a system has not been fully developed yet. The use of Printed Circuit Board material as substrate to create dry film resist microfluidic channels is the core technology to provide such an integration method. The feasibility and potential of the proposed packaging method is demonstrated in this work.**

Keywords - dry film resist, printed circuit board, inkjet printing, integration, low-cost.

I. INTRODUCTION

This paper is an extension of the work presented in [1] where the use of the TMMF dry film resist (DFR) from Tokyo Ohka Kogyo Co., Ltd. to create microfluidic channels on top of printed circuit board (PCB) to facilitate the access to nanofluidic channels is treated.

Microfluidic devices fabricated with dry film resist and Silicon (Si) and/or glass substrate have previously been reported [2] [3] [4]. Moreover, nanofluidic devices are usually fabricated with Silicon and/or glass [3] [5] [6] [7] [8]; even if nano-imprint technologies are used to fabricate them, a rigid substrate (usually glass) is required [9] [10]. What concerns the microelectronic chips; those are usually fabricated with Silicon.

The use of Silicon and/or glass to build fluidic systems elevates their cost [11] and the reliable fluidic connection of nanofluidic devices to the outside world still needs to be optimized in order to reduce costs and simplify the fabrication process.

Furthermore, a reliable method that combines great flexibility at integrating microelectronic devices in fluidic systems and low-costs are necessary to enable a broad use of microfluidic devices in quotidian life instead of expensive and voluminous equipment.

A low-cost fabrication method for microfluidic channels on top of a substrate composed by a micro- or nanochip inlaid in PCB material is presented. Inkjet printed interconnections are proposed to provide electrical connection between the chip(s) and the PCB electronics.

Following this approach, the chip(s) can be kept small in size and simple (standard) in technology thus decreasing costs. Furthermore, even if the silver ink and Rogers substrate have a relatively high cost, the overall cost is still lower than fabricating the devices with only Silicon and glass; even if some of the materials present relatively long curing times due to the low curing temperatures, still a device can be fabricated, with this technology, in less than seven days.

In addition, the low-cost PCB facilitates the fluidic and electrical connections to the outside world allowing the integration of micro- and nanodevices in a simple, robust and fast way.

In this work, the principle of the packaging integration technology is explained. In Section III, the physical properties of the materials used are presented. In Section IV, the fabrication process is detailed. Then, the challenges associated with the fabrication process are treated; first the challenges associated with the inlaying of the chip(s) in the PCB to form the substrate are described, followed by the fabrication of DFR fluidic channels on the substrate, and finally the challenges associated with the inkjet printing of electrical interconnections are discussed. The common factor to each challenge is the use of different materials as a substrate. Finally, the TMMF microfluidic interconnection is tested against leakage and the compatibility of the materials is studied by means of a thermal shock test in order to determine delamination. In addition, the suitability of the use

of inkjet printing technology for the creation of the electrical interconnections is studied by determining its performance under drastic temperature changes. To finalize this work, conclusions and future work are presented.

II. PRINCIPLE

The key material enabling the integration of micro- and nanochips into fluidic systems based on the lamination of DFR on PCB is a non-conductive adhesive (NCA).

The already fabricated chips are inlaid on the PCB material by means of a NCA. The chip(s) together with the PCB material compose the substrate for the fabrication of the microchannels that run over the chip. The microchannels are realized in dry film resist.

Concerning the electric access to the chip(s), inkjet printed interconnection lines are created between the electrical contacts of the chip(s) and the pads on the PCB.

Figure 1a shows a schematic of the concept when integrating a nanofluidic chip using the proposed technology; in this case the DFR microfluidic channels interconnect the nanofluidic channels in the chip to the macroworld. The microelectrodes in the nanofluidic device can be accessed via inkjet printed electrical interconnections.

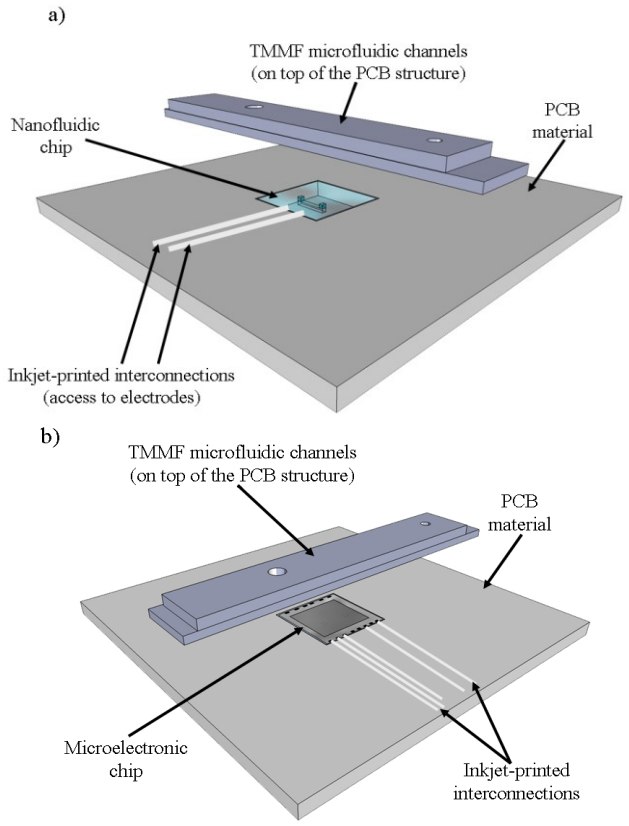


Figure 1. Schematic of different applications of the proposed technology, (a) integration of a nanofluidic chip, (b) integration of a microelectronic chip.

Figure 1b illustrates the concept when integrating a microelectronic chip using the proposed technology, for example an image sensor. In this case the dry film resist enables the construction of a microfluidic channel on top of the microchip and the inkjet printed conductive ink enables the possibility of accessing the functionality of the image sensor by the creation of electrical interconnection lines between the connection pads on the microchip and the pads on the PCB.

The challenges associated with the three aspects (NCA, DFR, inkjet printed ink) mentioned in this section are treated within the scope of this work. Quantitative as well as qualitative results are presented to evaluate the feasibility and robustness of the proposed integration method.

III. MATERIALS

TMMF dry film resist poses a unique stability when in contact with alkaline solutions and acids [3] [4] and provides high resolution and high aspect ratios [2] [4] making it the resist of choice for the fabrication of microfluidic channels.

The DFR used to fabricate the microfluidic channels is TMMF S2030, a permanent photoresist with a thickness of 30 µm for MEMS (microelectromechanical systems), manufactured by Tokyo Ohka Kogyo Co., Ltd. This negative photoresist is composed 5 % of antimony compound and 95 % of epoxy resin [2] [3].

Furthermore, the PCB material used as mechanical support for the whole system is Rogers RO4003C, a glass reinforced hydrocarbon laminate with low roughness characteristics.

Table I shows the physical characteristics of TMMF S2030 and Rogers RO4003C.

TABLE I. PHYSICAL PROPERTIES OF TMMF S2030 AND ROGERS RO4003C [2] [12]

Physical Properties of TMMF S2030 and Rogers RO4003C		
Physical Property	*TMMF S2030*	*Rogers RO4003C*
Coefficient of thermal expansion (ppm/°C)	65	X 11 Y 14 Z 46
Transition glass temperature (°C)	230	>280
Moisture absorption (%)	1.8	0.06
Dielectric constant	3.8	3.38±0.005
Transparency (nm)	400-600	-
Breaking strength (MPa)	60.3	-
Young modulus (MPa)	2100	26.889

The NCA used to glue the chips to the PCB material is a colorless two-parts epoxy-based adhesive with a glass transition temperature (Tg) of 45 °C and a coefficient of thermal expansion (CTE) of 56 ppm/°C when below the glass transition temperature, and 211 ppm/°C when above the glass transition temperature.

The ink used for the inkjet printed electric interconnections is a heat-curable silver nano-particle ink with a metal content of 20 % and a curing temperature of

125 °C. The thickness of one printed layer with such inks is in the range of 1-4 µm.

The names and brands of the NCA and the silver ink have been consciously left out.

IV. FABRICATION PROCESS

The fabrication process is divided in three steps:

- Inlaying of the chip in the PCB by using a NCA. The chip and the PCB together with the NCA form the substrate for the following steps.
- Fabrication of the microfluidic channels on the substrate.
- Fabrication of the inkjet printed interconnections between the chip and the PCB connection pads.

A. *Inlaying of the Chip(s) in the PCB*

The very first step to proceed to the fabrication of the TMMF microfluidic channels on top of PCB material is to form the substrate composed by the PCB and the chip(s). Figure 2 illustrates this process.

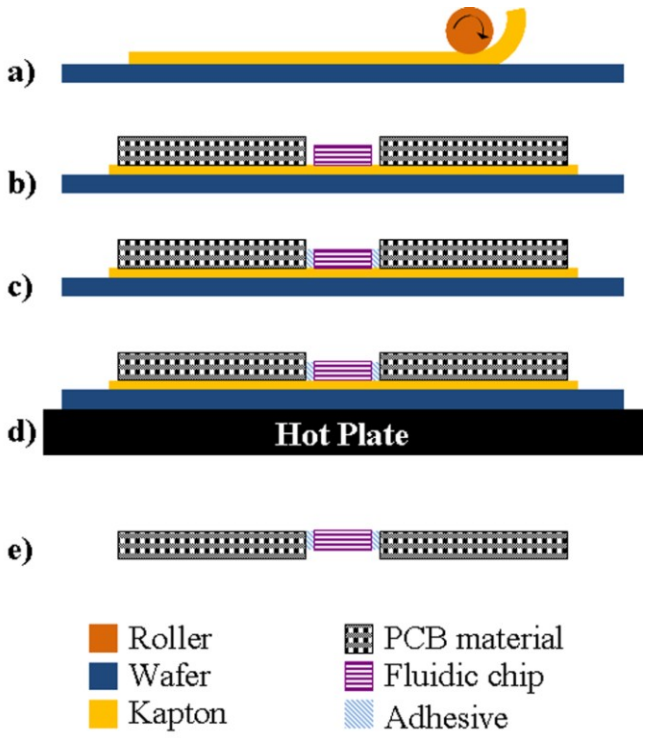


Figure 2. PCB material and nanofluidic chip leveling process flow chart.

According to Figure 2, to align the PCB material and the chip, a double sided Kapton tape is rolled on a Silicon or glass wafer or any other extremely flat and rigid surface (a). The PCB and the chip are adhered on the Kapton tape (b). The specimens are placed under vacuum to improve the adhesion between the Kapton tape and the components to be aligned. An Oxygen (O_2) plasma treatment at 50 W during 10 sec is performed using the Europlasma NV equipment. The epoxy-based adhesive is dispensed in the space between the PCB material and the chip (c). The materials are placed in a vacuum chamber to remove trapped air in the glue. The materials are placed in an oven or on a hot plate at 80 °C for 3 hours to cure the adhesive (d). When the adhesive is totally cured, the materials are cooled down to room temperature. The new substrate consisting of the chip inlaid in the PCB material is removed from the Kapton tape and turned 180 degrees (e).

To prepare the NCA, both parts from the adhesive are placed in a container and mixed with a Cat RM5 roller. The mix is placed in a vacuum chamber to remove possible trapped air.

B. *Fabrication of TMMF Microfluidic Channels*

The second stage of the fabrication process consists of laminating the TMMF microfluidic channels on top of the formed substrate. Figure 3 shows the flowchart for this process.

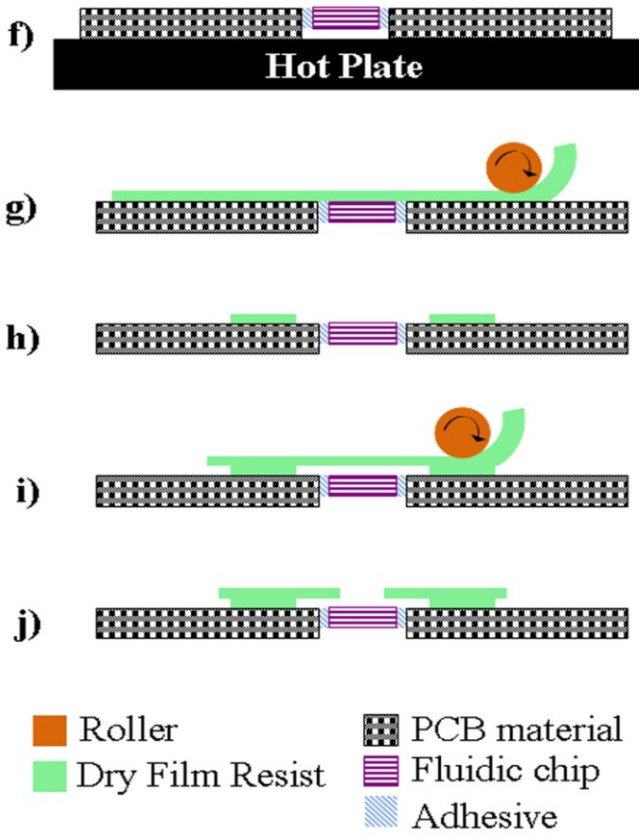


Figure 3. TMMF microfluidic channel lamination on top of the formed substrate.

The formed substrate is cleaned with ethanol and dried on a hotplate for 2 hours at 120 °C (f) to remove any adsorbed moisture; this will avoid that the humidity absorbed by the PCB material affects the DFR lamination process. An Oxygen plasma treatment is performed to the substrate in order to improve the adhesion between the TMMF resist and the formed substrate. The TMMF is protected on both sides with polyethylene terephthalate (PET).

The substrate is kept at 45 °C. One of the PET protective layers is removed from the DFR and the TMMF resist is

laminated on the substrate (g). The other PET layer is removed after the sample has cooled down. A soft baking step is performed at 90 °C during 5 minutes. The exposure is performed once the sample reaches room temperature. A post exposure baking step is performed with the same temperature and time than the soft baking step. The TMMF is developed using PGMEA (propylene glycol monomethyl ether acetate) after the sample has cooled down to room temperature (i).

Before closing the channels, the inkjet printed interconnections are printed.

A second layer of TMMF is laminated at 45 °C to close the microfluidic channels. The second layer is flood exposed after lamination without removing the remaining PET layer. The sample is cured at room temperature during one day. The PET layer is removed and access holes to the channel are punched with the help of a needle (j).

An alternative to create more stable and robust access holes instead of punching them in the TMMF is to use a through via in the PCB; in this case the access holes are accessed from the back side.

The alignment of the channels and the chip is performed manually, with the required equipment, and thus the accuracy is less than that of automated units.

C. *Fabrication of the Inkjet Printed Interconnections*

Finally, the inkjet printed interconnection lines are created.

The lines are printed with the drop-on-demand inkjet printer Jetlab 4 from Microfab Technologies, Inc., USA. The nozzle used is a piezo-actuated nozzle of 80 µm of diameter.

The substrate holder is heated at 65 °C during the printing process to avoid spreading of the ink.

The printed ink is cured in an oven during 16 hours at 125 °C.

With the 80 µm diameter nozzle, the smallest width line possible is 90 µm and the smallest space between lines possible is 70 µm.

V. CHALLENGES ASSOCIATED WITH THE FABRICATION PROCESS

Since the fabrication process is divided in three crucial tasks, the challenges associated with the fabrication process are grouped in three sections directly associated with each of the three crucial tasks.

A. *Challenges Associated with the Inlaying of the Chip(s) in the PCB*

The NCA used to keep together the chip(s) and the PCB material is an epoxy-based material.

Epoxy-based adhesives are known to present shrinkage due to the evaporation of the curing agent during the curing process [13] [14]. It is important to understand the behavior of this phenomenon given the fact that for a successful inkjet printing process, a flat surface is desired.

According to [15] a profile like the one in Figure 4 is expected after the NCA curing process.

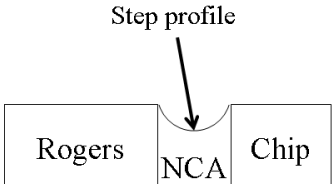


Figure 4. Profile expected in the NCA due to the curing process.

The effects of the glue shrinkage are studied into detail in Section VI Experiments.

B. *Challenges Associated with the Fabrication of TMMF Microfluidic Channels*

The challenges associated with the fabrication of TMMF microfluidic channels on the substrate are associated with the lamination of TMMF on PCB material and with the lamination of TMMF on the chip(s).

a) Lamination of TMMF on Rogers material: The challenges associated with the processing of TMMF resist on Rogers materials are pinholes in the photoresist, trapped bubbles between the resist and the PCB material, cracks in the photoresist, and closed channels.

Pinholes: TMMF might present pinholes after the soft baking step.

Experiments were conducted, and up to some extent, the pinholes can be decreased by using a plasma treatment, nevertheless, the crucial factor determining their presence is the moisture absorbed by the PCB material.

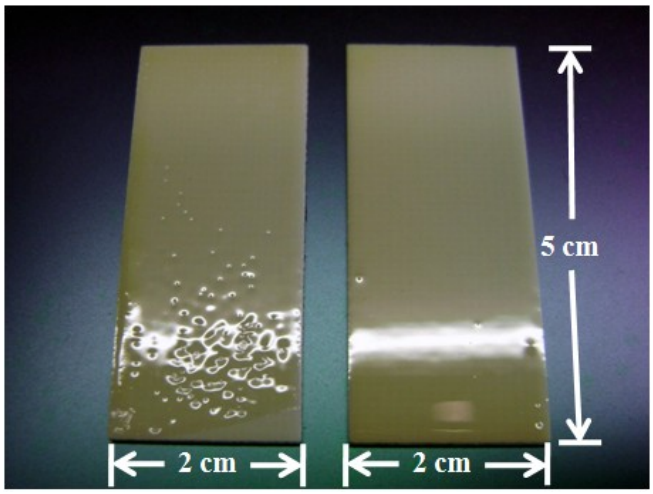


Figure 5. PCB material immersed under water prior to TMMF lamination (left) and PCB material dried at 120 °C prior to TMMF lamination (right). The presence of pinholes on the TMMF resist after soft baking is influenced by the moisture absorbed by the PCB.

Figure 5 shows two PCBs where TMMF was laminated and soft baked. In the specimen on the left side, the PCB material was immersed in water during 2 hours and its surface was dried with nitrogen prior to TMMF lamination. In the specimen on the right, the PCB material was placed on

a hotplate during 2 hours at 120 °C in order to evaporate the absorbed moisture prior to TMMF lamination.

Trapped bubbles and cracks: Experiments show that if the baking times are either higher or lower than the optimal time by at least one minute and the PCB material contains moisture absorbed from the atmosphere, trapped bubbles and cracks will form in the photoresist structures. The formation of trapped bubbles is directly related to the moisture absorbed by the PCB material and the use of inadequate baking times. The formation of cracks is related to the thermal stresses that result from a forced cooling down of the specimens after the baking steps and improper baking times. Furthermore, the moisture absorbed by the PCB material promotes the formation of cracks.

Figure 6 shows trapped bubbles between the TMMF and the PCB material as well as cracks in the dry film resist structures. The PCB material used for this experiment was not dried prior to TMMF lamination. Moreover, the baking times used in the processing were not optimal.

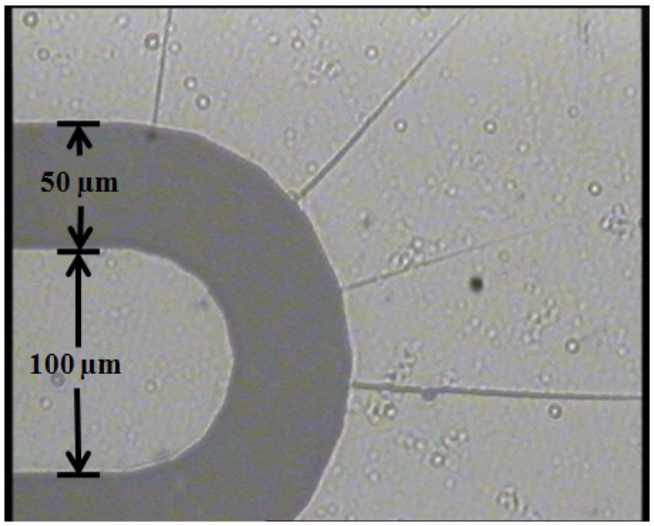


Figure 6. Trapped bubbles and cracks due to the humidity absorbed by the PCB material and the improper baking times used for processing of the TMMF.

Figure 7 shows a crack in the photoresist structure, but no trapped bubbles. The PCB material used for this experiment was dried prior to TMMF lamination, nevertheless, the baking times were not optimal.

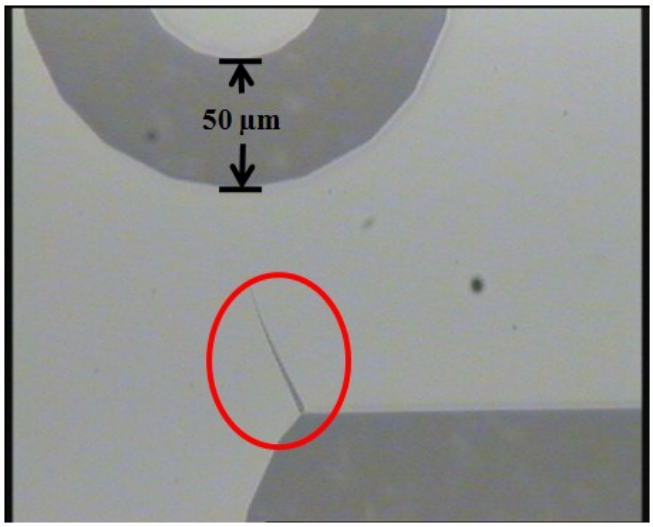


Figure 7. Cracks in the TMMF structures with angles close to 90 °. The circle in the image points the crack.The cracks are caused by the use of non-optimal baking times.

Closed channels: The exposure time should be controlled accurately when working with Rogers' materials. Scattering and diffraction of ultraviolet (UV) light during exposure is unavoidable when using a non-transparent material. Furthermore, the white color of the Rogers PCB material makes reflection of the waves a bigger problem.

The effects of an underexposed resist, as Figure 8 shows, are well known. On the other hand, overexposure can result in partially or totally closed fluidic channels.

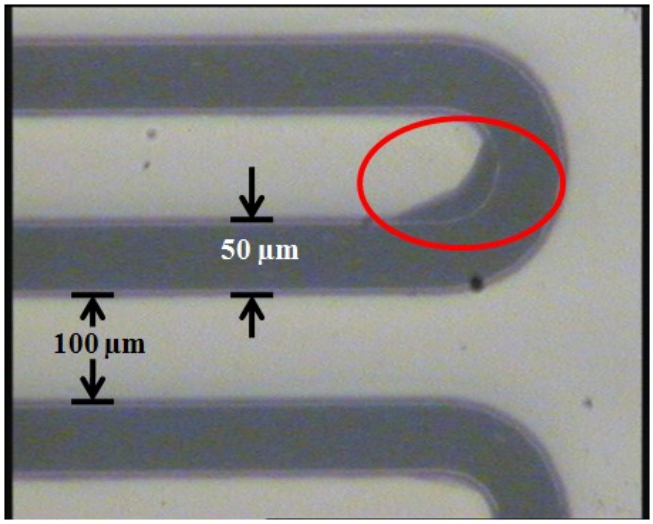


Figure 8. Effects of insufficient exposure time. The circle points an effect on the TMMF structure.

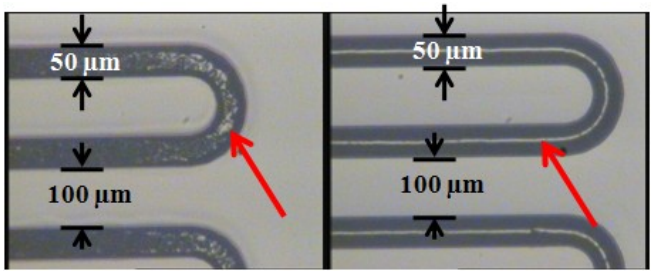


Figure 9. Closed channels on PCB material due to overexposure of the TMMF resist. The arrow in the left image points the effects of an overexposure of 2 seconds. The arrow in the right image points the effects of an overexposure of 6 seconds.

The more a sample is overexposed, the more closed the channels will be. Figure 9 shows a sample overexposed by 2 seconds (left) and a sample overexposed by 6 seconds (right).

b) Lamination of TMMF on the chip(s): Micro- and nanofluidic chips are usually made of glass and/or Silicon (Si), microelectronic chips are usually made of Silicon. PCB material and Si poses different thermal characteristics.

The thermal conductivity of the PCB material is approximately 0.71 W/m/°K [12] and the thermal conductivity of Si is around 140 W/m/°K [16]. Due to the thermal characteristics of the materials, heat transport at the baking steps is not a problem for the PCB material but it is for the Si chip(s).

The most common problem associated with the lamination of TMMF on Silicon is cracks due to heat transport at the baking steps and the difference in CTE [3]. Figure 10 illustrates this problem.

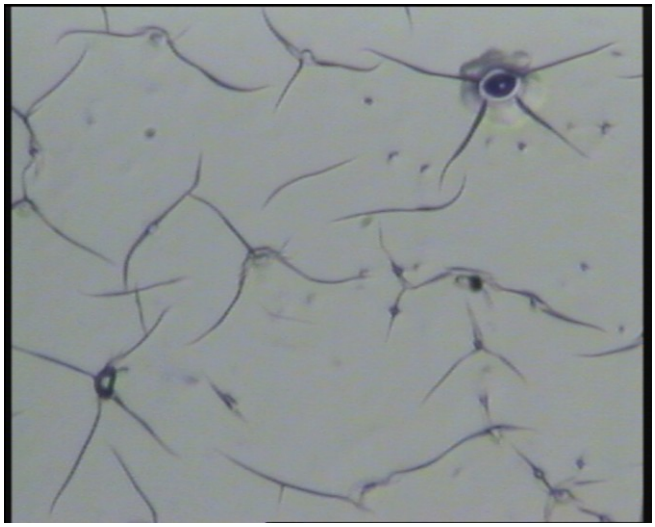


Figure 10. Cracks in the TMMF resist due to the CTEs difference between Silicon and the TMMF resist.

When the PCB material and the chip(s) are have the same thickness, as Figure 11a shows, the microfluidic chip will conduct heat around 25 times faster than the PCB material. Therefore, placing the substrate directly at 90 °C during the baking steps will originate cracks on the TMMF laminated over the chip. To solve this, the temperature needs to be ramped (2 °C/min) starting at 55 °C during the baking steps, when the temperature reaches 90 °C the samples are baked 5 minutes. Afterwards the hot plate's temperature is set to 25 °C, the sample is removed once the hot plate indicates 25 °C.

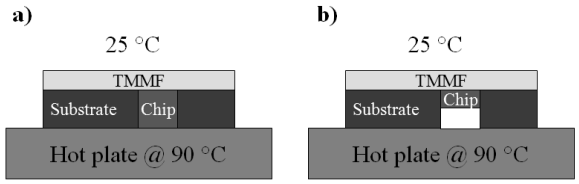


Figure 11. Cross-section of the substrate with TMMF on the hotplate when (a) the chip is the same thickness as the PCB material and (b) the chip is thinner than the PCB material..

Furthermore, if the chip is considerably thinner than the PCB material, as Figure 11b shows, the substrate can be placed directly at 90 °C. In this case, the thermal conductivity of the air between the chip and the hot plate will limit the heat flux to the chip, avoiding the presence of cracks on the TMMF.

This last method allows for less control thus the slow ramping of the temperatures is highly recommended.

C. Challenges Associated with the Fabrication of the Inkjet Printed Interconnections

The suitability of inkjet printed inks for their use in the proposed technology is studied. The main challenge and concern is the continuity of the interconnection lines, which can be affected by the step or curvature in the NCA due to its own shrinkage, especially if the step has a depth bigger than the thickness of the silver ink.

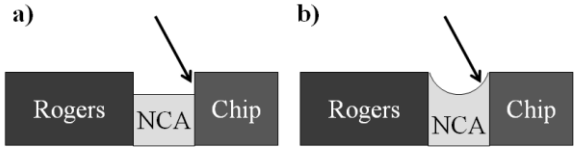


Figure 12. Possible step profiles, (a) steep step, (b) smooth step.

If the height difference between the chip and the NCA or the PCB and the NCA is steep as the arrow in Figure 12a indicates, it is expected that the continuity of the ink interconnection is interrupted. If the step is smooth as the arrow in Figure 12b points, the ink is expected to be continuous.

The adhesion of the ink is not expected to be a problem, since a plasma treatment is already performed prior to laminating the TMMF channels; however it is studied for confirmation.

VI. EXPERIMENTS

Each crucial aspect of the fabrication process is studied to test the feasibility of the proposed integration technology.

A. Inlaying of the Chip(s) in the PCB

In the case of the NCA shrinkage phenomenon, samples with different distance between the chip and the PCB material were prepared. The specimens were prepared following the procedure in Section IV.A.

The distance between the chip and the PCB is hardly controlled with precision. To control such gap, the chip(s) to be inlaid is measured and the desired distance between the chip and the PCB is added to the measurement; the hole in the PCB is created with these dimensions. The chip is placed carefully in the middle of the hole; this is the most difficult step since it is performed manually.

The step profile is measured with Dektak profiler and the angle of the step profile is obtained using Matlab code.

Figure 13 illustrates the measured step and the measured angle to avoid any misunderstanding. The step is measured from the deepest point in the NCA profile to the level of the PCB and/or chip. The angle of the NCA step with respect to a horizontal line is measured to determine the steepness of the step.

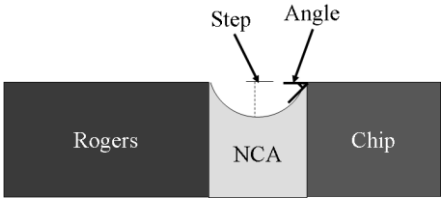


Figure 13. Sketch of where to locate the angle and step measured in each specimen.

Furthermore, few specimens cured at room temperature are prepared to determine the effects of the heat during the curing process in the substrate. Keep in mind that the materials in the substrate have very different CTEs thus the curing process temperature could affect the alignment of the chip and the PCB.

Since simulations of the curing process of an epoxy resin are complex and topic for a complete paper, it is not treated in this work and so the effect of the shrinkage in the substrate surface profile is determined in an experimental manner.

B. Fabrication of TMMF Microfluidic Channels

The TMMF microfluidic channels on the substrate are tested for leakage and exposed to sudden temperature changes.

The leakage test consists of injecting a rodhamine + ethanol + di water solution in the TMMF channels in one of the inlets. A visual inspection follows to detect any leakage. Special attention is given to the interconnection area between the different materials. Figure 14 shows the mentioned interconnection area before closing the TMMF channels.

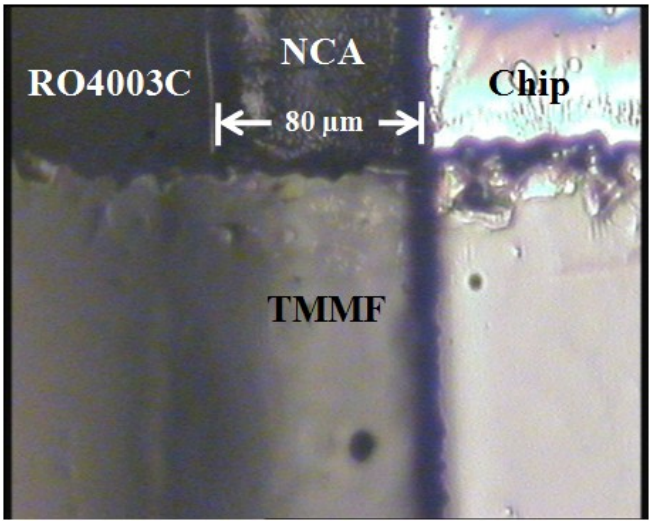


Figure 14. Close up of the interface between the different materials that form the fluidic interconnections to the nanofluidic chips.

The reliability test consists of a thermal shock test based on the military standard 883C. The purpose of this test is to accelerate the appearance of delamination and cracks.

The test consists of 15 cycles where each cycle is composed by a high temperature step at 100 °C and a low temperature step at 0 °C. The liquid used is water. After completing the test, a visual inspection is performed at a magnification no greater than 3x [17]. For further details about the test please refer to [17] and [18].

C. Fabrication of the Inkjet Printed Interconnections

The performance of the ink under sudden changes of temperature is studied to test the reliability of the inkjet printed interconnections. To do so, the resistivity of the ink is measured according to the Greek-cross method described in [18]. The resistivity is measured before and after the thermal shock test described in the previous subsection, with the exception that 20 cycles are performed during the test. The number of cycles has not considerably impact on the results; according to the standard, the cycles are increased during the test to compensate when there is less control on the temperatures and it is difficult to guarantee the variation limits specified by Option A [17]. Moreover, the adhesion of the ink is also studied before and after the reliability test using the Scotch-tape procedure described in [18]. The specimens used to perform the tests described in this paragraph are inkjet printed on Rogers.

The thickness of the ink is measured with a Dektak profiler. The thickness is necessary to calculate the resistivity values. The thickness measured is around 1 µm thus the ink thickness used for the calculations is 1 µm.

A resistivity change of maximal 20 % in the aged samples with respect to the fresh sample is considered a pass [19].

Furthermore, tests are performed printing on the whole substrate, that is to say, on the chip, NCA and the Rogers material, to test the continuity of the interconnection in the interface between the chip, the NCA and the PCB material.

Visual examination under a microscope is performed and the conductivity of the lines is tested with a multimeter.

VII. RESULTS AND SOLUTIONS

In this section the results are presented in three subsections.

First the results concerning the step originated by the shrinkage of the NCA.

Second, the results concerning the lamination of TMMF on PCB material and the chip(s) are presented. The leakage test results are exposed and the results concerning the compatibility of the TMMF and the different materials involved in the substrate.

Third, the results concerning the performance of the ink under sudden temperature changes and its continuity when printing on the materials' interface area are presented.

A. Inlaying of the Chip(s) in the PCB

Table II and Table III show the results of the step depth and angle measured for different spaces between the chip and the PCB material.

Section VI Experiments explains how the distance between the chip and the PCB material is controlled.

TABLE II. STEP DEPTH AND ANGLE

Distance between PCB and chip (µm)	Step depth (µm)	Angle side 1 (°)	Angle side 2 (°)
160	5.76	25.29	4.97
200	6.16	17.69	20.31
300	8.47	29.01	12.45

TABLE III. STEP DEPTH AND ANGLE

Distance between PCB and chip (µm)	Step depth (µm)	Angle side 1 (°)	Angle side 2 (°)
500	19.79	27.30	16.54
750	24.92	29.16	2.90
1000	32.00	3.40	30.13

The results in Table II are measured in a different specimen than those for Table III. According to Table II and Table III, the smaller the space between chip and PCB, the smaller the depth of the step is.

Furthermore, Figure 15 shows the profile of a specimen from Table II and Figure 16 shows the profile of a specimen from Table III.

According to the experiments, a NCA profile with the shape of Figure 16 can be obtained when the space between the chip and the PCB is at least 500 µm, if the space is less; a profile with peaks and irregular shape like in Figure 15 is obtained.

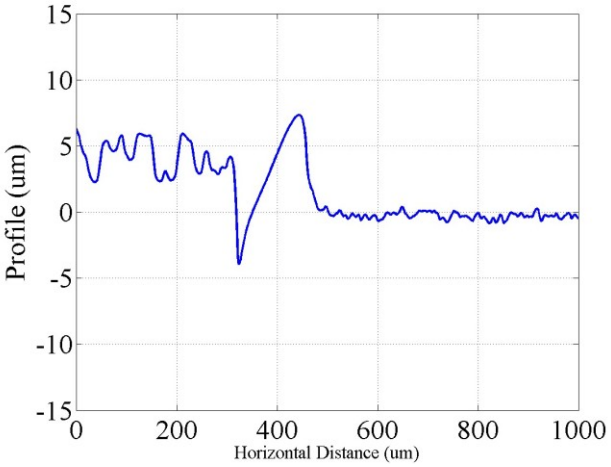


Figure 15. Profile of a specimen from Table II.

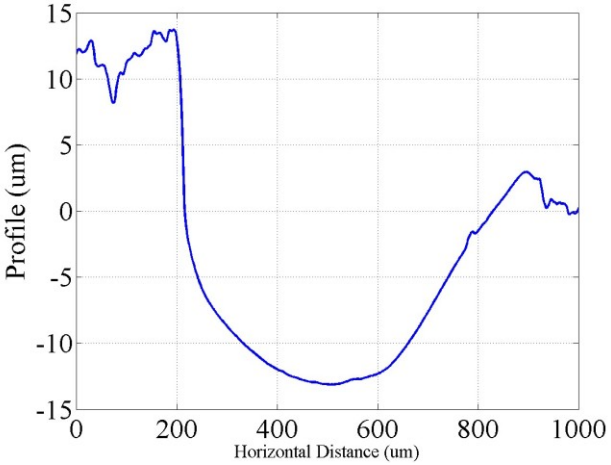


Figure 16. Profile of a specimen from Table III.

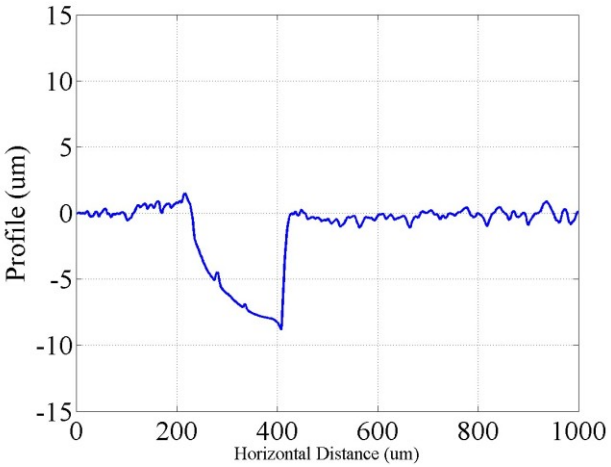


Figure 17. Profile of a specimen cured at room temperature.

Figure 17 shows the profile of a specimen cured at room temperature. During the experiments, it was observed that the specimens cured at room temperature present high

probabilities of keeping the PCB and the chip at the same level in the Z-axis, that is to say, horizontally aligned. Figure 16 shows the profile of a specimen that is cured at 80 °C; in this case the chip and the PCB are misaligned in the Z-axis by 10 µm, which is a typical value at this curing temperature.

B. Fabrication of TMMF Microfluidic Channels

The results in this section are presented in three subsections. First, the results relevant to the TMMF resist channels on the substrate; second, the results of the leakage test and third, the results of the reliability test to detect delamination problems.

a) *TMMF resist channels on the substrate.* Some factors should be kept in mind to obtain good results fabricating microfluidic channels on PCB materials. The baking times provided by the companies are optimal, nevertheless, different materials conduct the heat in a different rate, and therefore, the material temperatures might deviate from the prescribed temperature, especially when using a hot plate. Furthermore, PCB materials are more reflective than Silicon or glass; because of this, the exposure time should be tuned accurately; if channels of less than 50 µm are desired, this parameter is critical.

Figure 18 shows a TMMF structure on PCB material fabricated with optimal exposure and baking times.

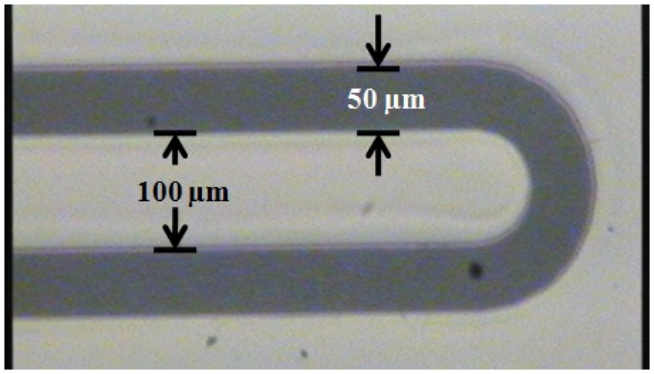


Figure 18. Microfluidic channels on PCB material. The image shows the results of optimal processing parameters (exposure and baking times).

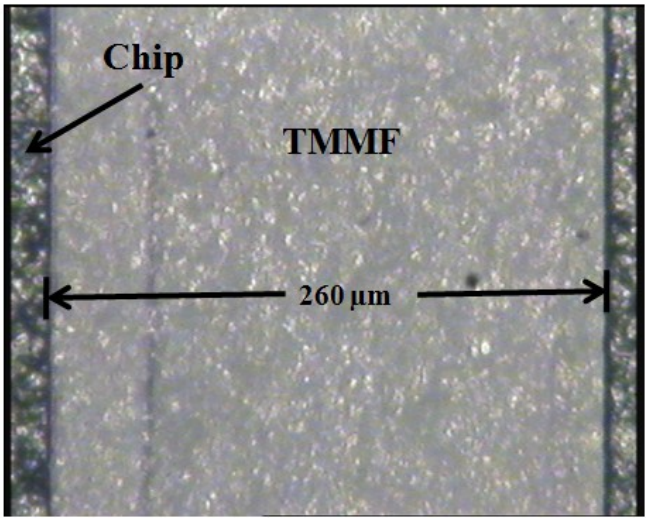


Figure 19. TMMF microfluidic channel walls on the Si chip, fabricated avoiding sudden temperature changes in the process.

Figure 19 shows the TMMF microfluidic channel walls on the Silicon chip fabricated in a way that sudden temperature changes are avoided; the temperature is slowly ramped during the baking steps. It is possible to observe that there are no cracks present in the TMMF structure.

b) Leakage test. Concerning the leakage test, Figure 20 shows a device fabricated with the packaging technology presented in this work.

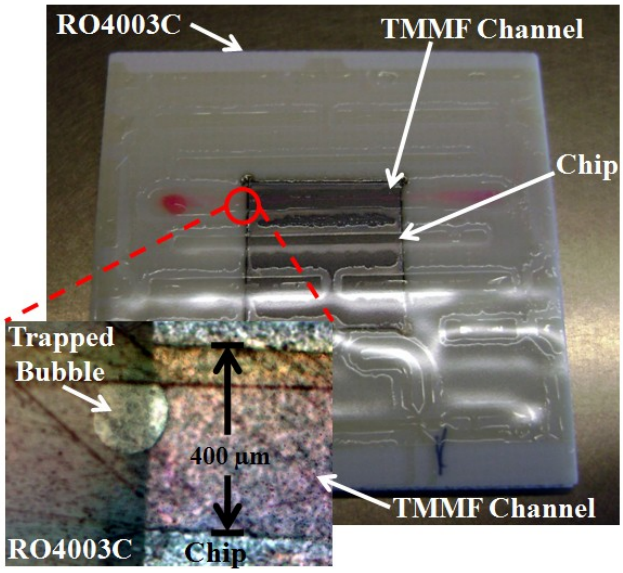


Figure 20. TMMF microfludic channels on PCB material as fluidic interconnections for nanofluidic chips. The small image in the lower left corner zooms in at the interface of the different materials that form the device; it shows no leakage of the rodhamine solution.

The pink liquid flowing through the TMMF channel is a solution of rodhamine + ethanol + di water. It is observed that no leakage occurs. The small image at the lower corner in the left was obtained with a 1X71 Olympus inverted microscope equipped with a low noise self cooling CCD

camera (color view II, Olympus); it shows, with 10x magnification, the area where the different materials interconnect. It is possible to observe the liquid solution flowing through the TMMF channel without leakage.

c) Reliability test. Figure 21 shows a device without closed channels after the thermal shock test.

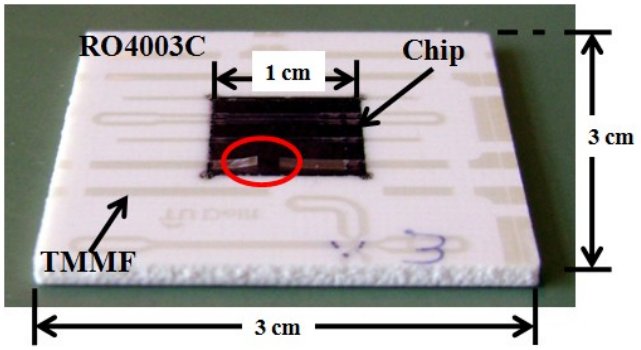


Figure 21. TMMF delamination on top of the Si chip after the thermal shock test. The circle points at the place where the delamination occurs.

The circle makes emphasis on a failure result from the test. Delamination of TMMF occurs on top of the fluidic chip. From the 3 tested specimens, the failure was observed only in the specimen from Figure 21.

C. Fabrication of the Inkjet Printed Interconnections

Table IV shows the measured resistivity values in μΩ·cm before and after the ageing test.

TABLE IV. RESISTIVITY OF THE INKJET PRINTED STRUCTURES BEFORE AND AFTER THE THERMAL SHOCK RELIABILITY TEST

Specimen number	Fresh specimen resistivity (μΩ·cm)	Aged specimen resistivity (μΩ·cm)	Increase (%)
1	38.75	38.43	-0.82
2	42.51	40.56	-4.58
3	26.79	26.47	-1.18

Even though the resistivity values can be considered high with respect to the values obtained in [18] and to the resistivity of bulk silver (1.59 μΩ·cm), the performance of the ink under sudden changes of temperature is good, in all the cases the resistivity decreased by a percentage of less than 5 %.

The adhesion characteristics before and after the ageing test are also good.

Scotch tape is used to test qualitatively the adhesion. The tape is rolled with pressure over the printed ink test structure, and then peeled off. The ink traces lifted with the tape when peeling it off are considered failures. There are no ink traces on the tape after peeling it off, which means that the ink was not peeled off from the Rogers material during the test.

The silver ink presented thus no adhesion failures before and after the reliability test.

Furthermore, Figure 22 shows the silver ink interconnection line printed on top of the components that form the substrate.

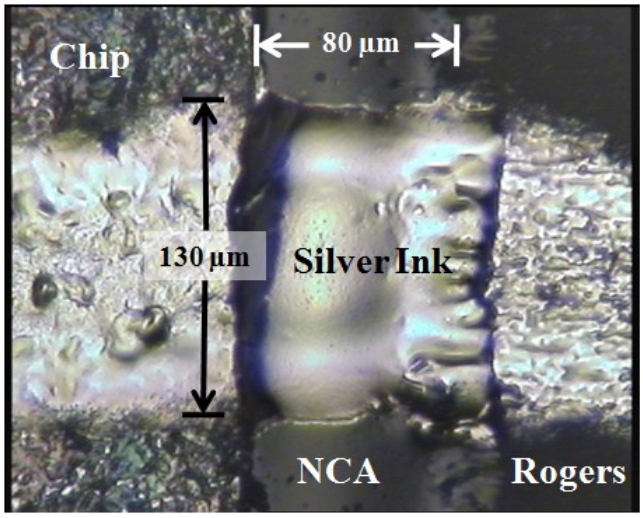


Figure 22. Interconnection silver ink line printed on the chip, the NCA and the Rogers material.

The printed silver ink line follows the profile of the surface with step depths measured in the range of 3-20 μm presenting electrical conductivity between both extremes of the line.

VIII. CONCLUSION AND FURTHER WORK

The experiments show that the step caused by the NCA cannot be completely eliminated.

To reduce the depth of the step it is recommended to have the minimum space possible between the chip and the PCB material.

Moreover, curing the NCA at room temperature is recommended in order to reduce the misalignment between the PCB and the chip in the Z-axis.

The thermal shock reliability test showed that the use of high temperature conditions could cause delamination problems mainly at the interface TMMF-NCA-Si chip. This means that the strength of the TMMF microfluidic interconnections decreases thus the probability of leakage increases.

Moreover, the experiments confirm the feasibility of the use of inkjet printed interconnection lines to create the electrical interconnection between the connection pads on the chip(s) and the connection pads on the PCB.

The silver ink shows perfect adhesion properties under room temperature conditions as well as under sudden temperature changes.

The electrical performance of the ink is not considerably affected by the rapid changes in temperatures.

Finally, the inkjet printing process and the characteristics of the NCA step allow the ink interconnection line to follow perfectly the substrate's profile, thus keeping the continuity in its conductivity and structure at all moments.

Further work includes the use of an image sensor available in the market to prove the feasibility of the proposed technology in a real life application. The PCB in turn can carry the necessary electronics for control and read-out. This enables the PCB as the core for the integration of micro- and nanochips together with electronics into a complex system.

Moreover, this work can be extended as assembly solutions for wider application areas as MEMS sensors and actuators.

ACKNOWLEDGMENT

The authors thank the Delft Institute of Microsystems and Nanoelectronics (Dimes) staff for their valuable help. Furthermore, the authors thank Rogers Corporation for providing low-roughness Rogers' material free of cost and Tokyo Ohka Kogyo Co., Ltd. for providing TMMF S2030 resist to develop this research. The authors also thank CMC Klebetechnik GmbH for providing double side Kapton tape. This work is supported by the Dutch Technology Foundation STW.

REFERENCES

[1] N.B. Palacios-Aguilera et al., "Dry film resist microfluidic channels on printed circuit board and its application as fluidic interconnection for nanofluidic chips: fabrication challenges", International Conference on Quantum Nano and Micro Technologies (ICQNM), 2011, Saint Laurent du Var, France, pp. 71-76.

[2] L. Zhang, Thesis: "Bioparticle separation in microfluidic devices for in-line application", Delft University of Technology, Delft, the Netherlands, 2009, pp.112-113.

[3] V. R. S. S. Mokkapati, "Micro and nanofluidic devices for single cell and DNA analysis", Delft University of Technology, Delft, the Netherlands, 2011.

[4] U. Stöhr, P. Vulto, P. Hoppe, G. Urban, and H. Reinecke, "High-resolution permanent photoresist laminate for microsystem applications", J. Micro/Nanolith. MEMS MOEMS, vol. 7(3), Jul.-Sep. 2008, doi: 10.1117/1.2964217.

[5] N. T. Nguten and S. T. Wereley., "Fundamentals and applications of microfluidics", Artech House Publishers, 2002, pp. 67-129.

[6] K. Wang et al., "Nanofluidic channels fabrication and manipulation of DNA molecules", IEE Proceedings Nanobiotechnology, Vol. 153, No. 1, Feb. 2006, doi:10.1049/ip-nbt:20050044.

[7] C. Song and P. Wang, "Fabrication of sub-10 nm planar nanofluidic channels through native oxide etch and anodic wafer bonding", IEEE Transactions on Nanotechnology, Vol 9, No. 2, Mar. 2010, doi:10.1109/TNANO.2009.2038377.

[8] C. Wu et al., "Design and fabrication of a nanofluidic channel by selective thermal oxidation and etching back of silicon dioxide made on a silicon substrate", Journal of Micromechanics and Microengineering, Vol 17, 2007, doi:10.1088/0960-1317/17/12/001.

[9] L. J. Guo, X. Cheng, and C. Chou, " Fabrication of size-controllable nanofluidic channels by nanoimprinting and its application for DNA stretching", Nanoletters, Vol. 4, No. 1, 2004.

[10] R. Yang et al., "Fabrication of micro/nano fluidic channels by nanoimprint lithography and bonding using SU-8", Microelectronic Engineering, 2009, doi:10.1016/j.mee.2009.02.002, Article in Press.

[11] K. Kalkandjiev et al., "Microfluidics in silicon/polymer technology as a cost-efficient alternative to silicon/glass", Journal of micromechanics and microengineering, Vol. 21, 2011, doi:10.1088/0960-1317/21/2/025008.

[12] Rogers Corporation Avanced Circuit Materiaals, "RO4000® laminates – data sheet", retrieved June 20, 2012 from http://rogerscorp.com/acm/products/16/RO4000-Series-High-Frequency-Circuit-Materials-Woven-glass-reinforced-ceramic-filled-thermoset.aspx.

[13] K.F. Schoch et al., "Real-time measurement of resin shrinkage during cure", Termochimica Acta 417, 2004, pp. 115-118.

[14] H. Yu et al., "Cure shrinkage measurement of nonconductive adhesives by means of a thermomechanical analyzer", Journal of Electronic Materials, Vol. 34, No. 8, 2005, pp. 1177-1182.

[15] B. Patham, "COMSOL implementation of a viscoelastic model with cure-temperature-time superposition for predicting cure stresses and springback in a thermoset resin", Excerpt from the proceedings of the COMSOL conference, 2009, Bangalore, India.

[16] H. R. Shanks et al., "Thermal conductivity of silicon from 300 to 1400 °K", Phys. Rev. (USA), Vol. 130, No. 5, pp. 1743–1748, 1963.

[17] Military standard: test methods and procedures for microelectronics MIL-STD-883C notice 6, August 1987.

[18] N.B. Palacios-Aguilera et al., "Shapeable Li-ion batteries as substrate: printed electronics reliability", International Conference on Electronics Packaging proceedings, 2011, Nara, Japan, pp. 844-848.

[19] Parlex Corporation, "Polymer thick film-material performance and reliability", retrieved June 20, 2012 from http://www.parlex.com/tech_library/PTFWhitePaper.pdf.

Turning Quantum Cryptography against itself: How to avoid indirect eavesdropping in quantum networks by passive and active adversaries

Stefan Rass
Alpen-Adria Universität Klagenfurt, Department of Applied Informatics
Universitätsstrasse 65-67
9020 Klagenfurt, Austria
stefan.rass@uni-klu.ac.at

Sandra König
Alpen-Adria Universität Klagenfurt
Universitätsstrasse 65-67
9020 Klagenfurt, Austria
sakoenig@edu.uni-klu.ac.at

***Abstract*—Quantum networks are communication networks in which adjacent nodes enjoy perfectly secure channels thanks to quantum key distribution (QKD). While QKD is renowned for perfect point-to-point security and its eavesdropping detection capabilities, end-to-end security is nontrivial to achieve. More importantly, the eavesdropping detection can indeed be turned against the system itself. It is known that perfect end-to-end security can be created from point-to-point security by means of multipath transmission (in fact, there is no other way to do this, assuming no pre-shared secrets and avoiding public-key cryptography). However, multipath transmission requires node-disjoint paths, which in turn are to be assured by the underlying routing protocol. At this point, an active or passive adversary may intentionally eavesdrop on the QKD protocol to temporarily cut a channel and to cause key-buffers running empty and enforcing local rerouting of packets towards nodes under his control. Consequently, the multipath transmission channels might no longer be non-intersecting, thus defeating the overall security by exploiting QKD's eavesdropping detection facilities. Alternatively, an active adversary may as well insert bogus traffic to cause local congestion, thus even sparing the effort of eavesdropping on a QKD link. In this work, we use Markov chains to model a multipath transmission, and we discuss the extent to which secure multipath transmission is resilient against local congestions caused by an adversary. We argue that a protection against an active adversary who uses bogus traffic to fiddle with the routing, calls for additional security measures, perhaps even beyond the capabilities of QKD or multipath transmission. It turns out that robustness against passive and active adversaries can be retained as long as no bogus traffic is observed.**

***Keywords*-Quantum Cryptography, Markov-Chain, Secure Routing, Information-Theoretic Security**

I. Introduction

Quantum key distribution (QKD) is known to provide perfect point-to-point security by virtue of its capability to detect passive eavesdropping. Despite considerable progress and ingenious concepts and results, QKD remains yet mostly limited to secure point-to-point connections. Although the theory of quantum repeaters is available in rich detail [2], these devices have not yet evolved beyond laboratory demonstrator status. On the classical road, perfect end-to-end security is achievable by means of multipath transmission. Remarkably, multiple paths have been proven to be both, a necessary and sufficient condition for perfect secrecy along a multihop connection (w.r.t. *not* assuming quantum repeater based transmission). The idea and security of such protocols (e.g., the one proposed by [3]) hinges on the chosen transmission paths to be pairwise non-intersecting. However, re-routing due to local congestions or intentionally caused blockages by the adversary can cause the network to temporarily allow intersections of paths and thus give an adversary an advantage when eavesdropping on relay nodes. More specifically, if the transmission uses t paths that are supposed to be disjoint (except for their respective end-points) then security against an adversary having up to k nodes under his control is not endangered as long as $t > k$ and the paths remain disjoint. More specifically, multipath transmission pursues the following general construction: to transmit a message m, the sender first puts it through a threshold secret sharing scheme, e.g., Shamir's (t, n)-scheme or plain (n, n)-sharing via the XOR of a sequence of random values, i.e., $m = s_1 \oplus s_2 \oplus \cdots \oplus s_n$, where $\oplus$ is the bitwise exclusive or. Each share s_i then travels over his own distinct path to the receiver, who reconstructs the message according to the chosen sharing scheme. In Shamir's case, this requires at least $t+1$ shares and in case of an XOR-sharing, all n shares are needed to recover m. In either case, the adversary needs to catch at least $t+1$ shares, respectively n shares, in order to learn anything. The simplest way to enforce a maximal number of corrupted nodes for that matter is having the paths pairwise non-intersecting, i.e., node-disjoint. If congestions cause local redirections such that multiple paths intersect in the same node, then the security of the transmission is doomed to fail, since the adversary may learn the required number of shares while perhaps having a much smaller number of nodes under his control. We introduce an attack in which the adversary exploits the eavesdropping detection facility of QKD without attempting to learn any of the secret key material. Instead, his only goal is to make the link run dry of key-material, so as to enforce the local neighborhood nodes to search for alternative paths over nodes that he controls. We call this an *indirect eavesdropping attack*.

The goal of this work is to investigate the resilience – in terms of end-to-end security – of quantum networks to such kind of incidents. We consider both, a passive and active adversary, being computationally unbounded and only constrained to have no more than k nodes in the network under his control. Moreover, we assume the routing to be under partial control of the sender, so that he can initiate a multipath transmission, but his chosen paths are potentially subject to temporary rerouting due to congestions. These congestions can be actively caused by the adversary, or coincidentally happen due to other reasons. In the latter case, we obtain simple sufficient criteria for perfectly secure communication remaining possible even if the routing is imperfect. The case of an active adversary causing traffic redirections is discussed based on these preliminary results.

Organization of the paper: We consider networks employing QKD for point-to-point- and multipath routing for end-to-end security, referred to as *quantum networks*. We briefly review the use of QKD with multipath transmission in Section IV. In Section V, we introduce a Markov-chain model for the path that a data packet takes from the sender to the receiver, with a particular focus to multipath transmission. Conditions under which an unreliable routing regime can yield perfect secrecy are derived in Section VI. Section VII is devoted to a discussion of active adversaries by extending the results from Section VI accordingly. Under suitable assumptions on his capabilities, we can retain security even against an active adversary. Dropping these assumptions, we demonstrate how an active adversary can indirectly influence the routing so as to direct the information flow towards his nodes without direct access to the routing. This form of indirect eavesdropping attack works even without using the eavesdropping facility of the underlying QKD protocol. An example supporting the practicability of our results is found in Section VIII. Final remarks are given in Section IX.

II. Related work

This work extends previous research described in [1]. Although eavesdropping detection in quantum key distribution [4] is quite well researched, only few authors deal with routing issues and even less consider problems arising from unreliable routing. Most closely related to ours is the work of [5], who provide a stochastic routing algorithm along with probabilistic measures of secrecy in a randomly compromised network. We improve on this by avoiding the assumption of some fixed routing algorithm. Instead, we formulate conditions under which a given routing protocol can provide perfect secrecy under random compromission. Consequently, the framework devised here is generic and requires simulations and empirical evaluation of the routing scheme at hand in order to be applied. Fortunately, simulation tools like OmNet++ [6] can rapidly provide such information. Practical QKD implementations are often subject to physical distance limitations (cf. [7], [8], [9] to name a few). Although unlimited distance QKD transmission is theoretically possible (see [10]), multipath transmission over disjoint channels remains up to now a practical necessity for perfect end-to-end security [11]. In particular, [3], [12], [13], [14] and references therein form the basis for our work, where our goal is to investigate a hidden assumption within these results: what happens if the routing is not fully reliable? Implementations of multipath transmission within the transmission control protocol (TCP) are currently under standardization, and many other protocols like stream control transmission protocol (SCTP [15]) as well facilitate concurrent transmission. Similarly as for a recently proposed extension of the secure socket layer (SSL) by QKD [16], [17], one could imagine QKD being integrated in such protocols. Load-balancing, local congestions and most importantly (adversarial) eavesdropping can all cause re-routing of packets and therefore make otherwise disjoint routes intersecting. Our work is an explicit account for security under such random distortions. To the best of our knowledge, such indirect eavesdropping attacks have not yet been considered elsewhere in the literature.

III. Preliminaries and Notation

Let $M \in \{0,1\}^*$ denote a binary string of arbitrary length. Let $|M|$ be its length (in bits), and let $H(M)$ denote the Shannon-entropy of a random message source M. A quantum network is an undirected graph $G = (V, E)$ in which each pair of adjacent nodes shares a channel that is secured by means of quantum key distribution. The sets of nodes and edges in G are denoted by $V(G)$ and $E(G)$, respectively. An $s-r$-*path* in a graph is an ordered sequence of adjacent nodes starting with $s \in V$ and ending in $r \in V$. We will denote a (general) path by ρ, and its set of nodes will be written as $V(\rho)$. Two $s-r$-paths ρ_1, ρ_2 are said to be *node-disjoint*, if $V(\rho_1) \cap V(\rho_2) = \{s, r\}$, i.e., the paths do not intersect elsewhere than in their start- and end-nodes. For any node $v \in V(G)$, we denote the collection of its immediate neighbors as $\mathrm{nb}(v) := \{u \in V | (v, u) \in E\}$.

Markov chains: As our routing model will be based on Markov chains, we briefly review the respective basics for convenience of the reader. We will straightforwardly focus on graph models for our introduction: once Alice has handed over her encrypted payload to the network for delivery to Bob, the actual journey of the packet can be considered as a random walk through the network until it reaches its final destination. Though the routing itself is essentially deterministic, randomness comes into play due to local congestions and subsequent re-routing. Consequently, we can consider the packet as describing a trajectory of a *stochastic process*, or more specifically a *Markov chain*, whose state space is the set $V(G)$, i.e., the set of all relay nodes that the packet can possibly visit. For any two nodes

$u, v \in V(G)$, assume that the packet travels from u to v with probability $p_{uv} = \Pr[u \to v]$. Since $V(G)$ is finite, we can fix any enumeration $V(G) = \{1, 2, \ldots, n\}$ and write p_{ij} for the chance of the packet traveling from i to j within one hop. To model this hop-by-hop forwarding, let us introduce the random variable $X(\tau) \in V(G)$ for $\tau = 1, 2, 3, \ldots$ telling us the node that hosts the data packet at time-step $\tau \in \mathbb{N}$. A *trajectory* is the sequence $(X(0), X(1), X(2), \ldots)$ describing the packet's trace, starting off at the sender $X(0)$ until it reaches its final destination (the receiver) at some later point in time. In terms of conditional probability, we have $p_{ij} = \Pr[X(\tau + 1) = j | X(\tau) = i]$ describing the one-step transition probability. The (one-step) *transition matrix* is defined as the $(n \times n)$-matrix $P = (p_{ij})_{i,j=1}^{n}$.

As we are dealing with multipath transmission in the following, consider t independent copies of a trajectory, named $1, 2, \ldots, t$. The particular state of the i-th trajectory at time τ is written as $X_i(\tau)$. Let the function $\pi_i(\tau, v) : \mathbb{N} \times V \to [0, 1]$ describe the chance that the i-th trajectory ($i = 1, 2, \ldots, t$) is within node v at time $\tau \in \mathbb{N}$, i.e., $\pi_i(\tau, v) = \Pr[X_i(\tau) = v]$. The whole distribution (supported on the set of nodes $V(G)$) is denoted as $\pi_i(\tau)$, and the whole ensemble of t trajectories is denoted as $\pi(\tau) = (\pi_1(\tau), \ldots, \pi_t(\tau))$.

Adversary Model: Our attacker will be a computationally unbounded active threshold adversary named Eve. That is, given a network $G = (V, E)$, with a sender s and receiver r (both in V), the adversary can compromise up to $k \leq |V \setminus \{s, r\}|$ *nodes* in G (thanks to QKD, an activity on any of the links would be detected anyway). Moreover, Eve knows all relevant protocol specification and the network topology, and is not bound to follow the protocol. A weaker notion is assuming her to stick passively to the protocol in order to extract secret information. We call this behavior *passive*, as opposed to an *active* adversary, as described previously and refined later in Section VII. Throughout the remainder of this work, the adversary's threshold will be denoted as k.

Security Model: Our notion of security is based on the concepts used in [11]. We need some notation: a general *protocol* Π is an interactive process between a sender and a receiver. In the course of Π, Alice exchanges a set $C = \{C_1, \ldots, C_n\}$ of messages with Bob in order to secretly transmit a message $M \in \{0, 1\}^*$ of entropy $H(M)$. The full set C is called the protocol's *transcript*. A subset $\mathrm{adv}(M) \subseteq \{C_1, \ldots, C_n\}$ of the transcript obtained by eavesdropping of the adversary is called his *view* in the protocol Π (a closely related equivalent notion is found used in [13]).

Definition III.1. *Let $\varepsilon > 0$, and let Π be a message transmission protocol. We call a protocol* ε-secure*, if the following two conditions are satisfied:*

1) *$H(M|adv(M)) \in \{0, H(M)\}$ and*
2) *$Pr[H(M|adv(M)) = 0] \leq \varepsilon$,*

i.e., the adversary can disclose M with a chance of at most ε. We call the protocol Π efficient*, if the size of the transcript, i.e., $\sum_{i=1}^{n} |C_i|$, is polynomial in the size of the message M, the size of underlying network (in terms of nodes), and $\log \frac{1}{\varepsilon}$. A protocol that is ε-secure for any $\varepsilon > 0$ is said to enjoy* perfect secrecy.

It is easy to see that if a protocol is ε-secure with $\varepsilon < 2^{-|M|}$, then simply guessing the message is more likely than breaking the protocol itself.

IV. QKD-Based Multipath Transmission

Multipath transmission pursues a simple idea: having t paths from s to r that are node-disjoint, the sender can transmit a message m by first putting it through a (t', t)-secret sharing (Shamir's for instance), giving the shares $s_1, \ldots, s_t$ and sending each share over its own (distinct) path to r. The adversary is successful if and only if he catches at least t' shares. Obviously, the scheme is unconditionally secure if $t' > k$ (where k is the adversary's threshold), but in addition, we require full knowledge of the topology, and assured delivery over the chosen disjoint paths. The general interplay between network connectivity and unconditional security has been studied extensively (cf. [14], [13], [3]). However, common to all these results is the implicit assumption of secure and reliable routing. That is, most existing multipath transmission regimes prescribe a fixed set of chosen node-disjoint paths. These paths are assumed stable and unchanged over the duration of a transmission; the adversary might intercept the paths but cannot redirect them. Hence, our goal in the next section is to find out whether or not unconditional security can be retained if the paths are not reliably under the sender's control. In other words, what happens if the adversary indirectly fiddles with the routing?

V. A Markov-Chain Routing Model

To simplify technicalities, let us assume a *synchronous* forwarding regime, i.e., the nodes simultaneously forward their packets at fixed times. This permits us to use a discrete time variable $\tau \in \mathbb{N}$. This assumption is not too restrictive, since even an asynchronous forwarding regime can be reasonably approximated by choosing a small unit of time and letting some nodes remain occasionally inactive in some steps.

Consider an arbitrary but fixed trajectory i among an ensemble of t independent trajectories in the following. It is well known from the theory of Markov chains that the state of the i-th chain at time $\tau \in \mathbb{N}$ is governed by $\pi_i(\tau) = P^{\tau} \cdot p_i(0)$, where P is the transition matrix. Our chain has only a *single absorbing state*, which is the receiver's state r (the receiver will surely not pass on his message any further). Furthermore, it can be assumed irreducible, because if it were not, then there would be at least two nodes u, v in the network whose chance of getting a packet from u to v is zero, so they could never communicate.

We write H_{jA} for the time (measured in *hops*) that it takes a trajectory to get from node j to any of the target nodes in the set $A \subseteq V$,

$$H_{jA} = \min\{\tau \geq 0 : X(\tau) \in A | X(0) = j\}.$$

The probability h_{jA} of the chain ever reaching A from j is therefore $h_{jA} = \Pr[H_{jA} < \infty]$, and the family $(h_{jA}; j \in V)$ is the smallest non-negative solution of the equation system

$$h_{jA} = \sum_{i \in V} p_{ji} h_{iA}, \tag{1}$$

where $h_{jA} = 1$ for all $j \in A$ and p_{ji} is the probability of passing from node j onwards to node i (see [18, p.123] for details). Writing down this system for, say 5 equations with $A = \{1, 3\}$, we get (after some minor algebra),

$$\begin{array}{rcccc} -p_{21} - p_{23} & = & (p_{22} - 1)h_{2A} & + & p_{24}h_{4A} \\ -p_{41} - p_{43} & = & p_{42}h_{2A} & + & (p_{44} - 1)h_{4A}, \end{array}$$

where we additionally substituted $h_{rA} = 0$, as r is the only absorbing state of our chains. Let us write (in a slight abuse of notation) $P_{-R,-C}$ to denote the matrix P with all rows in R and all columns in C *deleted*. Similarly, we use the notation $P_{R,C}$ to denote the matrix P only with the rows in R and columns in C retained. To ease notation, let us put $Q := P_{-r,-r}$, i.e., Q is P without the r-th row and column. If I is the identity matrix, and $\mathbf{1}$ is the vector of all 1's, then the above equation system takes the compact form

$$-Q_{-A,A} \cdot \mathbf{1} = (Q_{-A,-A} - I)h_A, \tag{2}$$

where h_A is the family $(h_{1A}, h_{2A}, \ldots, h_{rA})$, excluding $h_{rA} = 0$ and $h_{jA} = 1$ for all $j \in A$. In order to have the values h_j for $j \neq r$ and $j \notin A$ well-defined, we ought to show that $(Q_{-A,-A} - I)$ is invertible. This is our first

Lemma V.1. *Let P be a stochastic matrix of an irreducible Markov-chain with the state space V and exactly one absorbing state $r \in V$. Select any set of states $A \subset V$ with $r \in A$, and let $Q = P_{-A,-A}$ be the submatrix of P that describes transitions between states outside of A. Then $Q - I$ is invertible.*

Proof: Partition the state set V into $V_1 = A$ and $V_2 = V \setminus A$, then $r \in V_1$ and Q describes transitions *within* V_2. For each $v \in V_2$, write $\pi_{V_2}(\tau, v)$ for the chance of the chain being in state v after τ steps. From the theory of Markov-chains, we know that the vector $\pi_{V_2}(\tau) = (\pi_{V_2}(\tau, v))_{v \in V_2}$ is given by $\pi_{V_2}(\tau) = Q^\tau \pi_{V_2}(0)$. As the chain is irreducible, we will eventually reach r from *any* state in V_2, and since r is absorbing, this means that $Q^\tau \to 0$ as $\tau \to \infty$. Now, put $(Q - I)x = 0$. Then $Qx = x$ and on iterating $Q^\tau x = x$. As $\tau \to \infty$, $Q^\tau x = x \to 0$, so $Q - I$ is invertible. ∎

Lemma V.1 helps constructing a formula giving us the chance that exactly l trajectories pass through a given area $A \subseteq V$ that is under the adversary's control. We can solve the system (2) for any given set A and see whether it is passed with certainty. Similarly as for the binomial distribution, we can ask for the probability of a subset of l trajectories hitting A within finite time, with the remaining ones never reaching A. The probability we are after is the sum over all subsets of size l. Formally, we have

Proposition V.2. *Let a graph $G = (V, E)$ be given, and assume a random walk of t trajectories starting at nodes $1, 2, \ldots, t$. For a given $A \subseteq V$, the chance of l trajectories passing through A is given by*

$$p(A, l) = \sum_{\substack{M \subseteq [1:t] \\ |M| = l}} \left[\prod_{i \in M} h_{iA} \prod_{i \in ([1:t] \setminus M)} (1 - h_{iA}) \right],$$

where the vector $(h_{iA})_{i \in V}$ is calculated by putting $h_{rA} = 0, h_{jA} = 1$ for all $j \in A$, and calculating the remaining probabilities by solving (2)*. Here, $[1:t]$ is a shorthand notation for the set $\{1, 2, \ldots, t\}$.*

VI. Secrecy Against Passive Adversaries

According to Proposition V.2, the adversary will not learn anything unless he conquers some set A that is passed by sufficiently many, say l, trajectories. Consequently, his best strategy is attacking the set with maximum likelihood of seeing sufficiently many trajectories. It follows that the most vulnerable subset of nodes in the network is

$$A^* = \operatorname*{argmax}_{A \subseteq V} \Pr[l \text{ trajectories traverse } A] = \operatorname*{argmax}_{A \subseteq V} p(A, l). \tag{3}$$

The following result is an immediate consequence of the above discussion:

Theorem VI.1. *A network with a routing regime described by a transition matrix P can provide perfect secrecy without pre-shared end-to-end secrets, if and only if for some integer $l \geq 1$, we have $p(A, l) < 1$ for all $A \subseteq V$ that the adversary can compromise.*

Proof: Assume that $p(A, l) < 1$ for any set A and choose $\varepsilon > 0$ arbitrarily small. Put the message through a (n, n) secret sharing scheme, giving the shares $s_1, s_2, \ldots, s_n$. Send each s_i over l paths to the receiver. The adversary is successful if and only if he catches all shares, but the chance for this to happen decays exponentially fast as $p(A, l)^n \to 0$ as $n \to \infty$. It remains to choose n sufficiently large so as to have $p(A, l)^n < \varepsilon$.

Conversely, if $p(A, l) = 1$ for some set A, then there is no way to avoid the adversary when transmitting something over the network. Hence, secret communication is impossible. ∎

Despite this maximum likelihood optimization problem being sound, it is yet infeasible to evaluate as the number of subsets to test is exponential (in the adversary's threshold). We shall therefore set out to find sufficient criteria that are easier to test.

For a 1-passive adversary, we have the following test:

Theorem VI.2. *Let $t = |nb(s)| \geq 1$ count the sender s's neighbors. If, for each $v \in V$, we have $\sum_{i=1}^{t} h_{iv} < t$, then the network provides perfect secrecy against a 1-passive adversary.*

Proof: Put the secret message through a (t,t)-secret sharing and let each share take its own individual path through the network (i.e., do a random walk according to the transition matrix P). With the random indicator variable

$$\mathbb{I}_{i,j} := \begin{cases} 1, & \text{if } h_{ij} > 0 \\ 0, & \text{otherwise,} \end{cases}$$

the number of trajectories passing through a node $v \in V$ is given by $N_v := \sum_{i=1}^{t} \mathbb{I}_{i,v}$, and its expected value is $\mathsf{E}(N_v) = \mathsf{E}(\sum_{i=1}^{t} \mathbb{I}_{i,v}) = \sum_{i=1}^{t} h_{iv}$. The assertion now directly follows from Markov's inequality, since

$$\Pr[N_v \geq t] \leq \frac{\mathsf{E}(N_v)}{t} < \frac{t}{t} = 1,$$

which holds for all $v \in V$. The network thus provides perfect secrecy by Theorem VI.1. ■

Theorem VI.3. *Let $G = (V, E)$ be a graph, and let the sender and receiver be $s, r \in V$. Let the adversary be k-passive, i.e., up to k nodes in G can be compromised. For perfect secrecy, it is necessary that $|nb(s)| > k$. In that case, with $V^* := V \setminus \{s, r\}$, if*

$$\forall i \in nb(s) : h_{ij} \leq \frac{1}{ek} \;\; \forall j \in V^* \setminus \{i\}\,, \tag{4}$$

then the network provides perfect secrecy.

Proof: Without loss of generality, assume s's neighbors to be the nodes $\{1, 2, \ldots, t\}$, and put the secret message m through a (t,t)-secret-sharing scheme, transmitting the i-th share over the i-th neighbor of s (the remaining path of each is individual and determined by the network's transition matrix P). Observe that the adversary will not learn anything unless he gathers all t shares.

If $t \leq k$, then the adversary can "cut off" s from the rest of the network, thus reading all information conveyed by s, and perfect secrecy is impossible by Theorem VI.1.

Assume $t > k$ henceforth, so there exists at least one honest neighbor of s in every attack scenario. Let $A \subseteq V$ with $A = \{j_1, \ldots, j_k\}$ be a set of compromised nodes. The (mutually dependent) events $T_l^{j_i}$ for $i = 1, 2, \ldots, k$ occur when the trajectory starting off the node l reaches node j_i. For each (starting node) $l = 1, 2, \ldots, t$, we have

$$\Pr\left[T_l^{j_i}\right] = h_{lj_i} \leq \max\{h_{lv} | v \in V \setminus \{l, s, r\}\} \leq \frac{1}{ek}, \tag{5}$$

where the last inequality follows from our hypothesis. Since $\Pr\left[T_l^{j_i}\right] \leq \frac{1}{ek}$, then Lovász local lemma (symmetric version) implies

$$\Pr\left[\bigcap_{\nu=1}^{k} \overline{T_i^{j_\nu}}\right] > 0. \tag{6}$$

Protocol skeleton for secret and eff cient delivery of a message over an untrusted network.
Input: Message m, round number n and number t of shares per round.
Protocol steps for the sender:

1) Put m through a (n,n)-secret sharing, giving the shares $s_1, \ldots, s_n$.
2) For $i = 1, 2, \ldots, n$ do the following: put the i-th share s_i through a (t,t)-secret sharing, where $t = |\mathrm{nb}(s)|$, and transmit the j-th share of s_i over the j-th neighbor of s (cf. Theorem VI.3).

Figure 1. Multi-round multi-path transmission

In other words, the l-th trajectory has a positive chance of *evading* the set $\{j_1, \ldots, j_k\}$. Since inequality (5) holds independently of the particular j_i's, (6) is true for all these sets. If condition (5) holds for all $l = 1, 2, \ldots, t$, then in every attack scenario there is at least one trajectory with a positive chance of *not* passing through the compromised area in the graph. So, for every $A \subset V$ with $|A| \leq k$, it holds that $p(A, t) < 1$ and the network can provide perfect security by Theorem VI.1. ■

Eff ciency

Regarding the bandwidth demand, we require the overall network traff c (bit complexity) and round complexity to be polynomial in $\log \frac{1}{\varepsilon}$ for any chosen $\varepsilon > 0$. Assume the network satisf es the condition for perfect secrecy in Theorem VI.1.

Fix some $\varepsilon > 0$. We will prove the following transmission regime to enjoy eff cient bit- and round-complexity, i.e., polynomial efforts in $\log \frac{1}{\varepsilon}$. Let the secret message m be transmitted from s to r by virtue of the framework protocol shown in Figure 1. For a passive adversary with a threshold k, the number of shares t must be larger than k. The number n of rounds will be determined now.

Obviously, the attacker will not learn anything unless he gets all the information f owing over the network (due to the (n,n)- and (t,t)-sharings). Our task is proving n to be polynomial in $\log \frac{1}{\varepsilon}$ and the size of the network. For the proof, def ne an indicator variable for each round $i = 1, 2, \ldots, n$ via

$$\mathbb{I}_i = \begin{cases} 1, & \text{if the share } s_i \text{ was disclosed;} \\ 0, & \text{otherwise,} \end{cases}$$

so that $\mathbb{I}_i$ measures the adversary's success (in a binary scale) in the i-th round. By our hypothesis, Theorem VI.1 implies $\Pr[\mathbb{I}_i = 1] < 1$ for all rounds i and all sets of nodes that the adversary could have conquered (recall that the adversary is k-passive). Put $\rho := \max_{i=1,2,\ldots,n} \Pr[\mathbb{I}_i = 1]$, then $\rho < 1$. Since $0 \leq \mathbb{I}_i \leq 1$ for all i, the f rst moment $\mathsf{E}(\mathbb{I}_i)$ exists

and $\mathbb{I}_i$'s deviation from its mean is bounded by $-1 \leq \mathbb{I}_i - \mathsf{E}(\mathbb{I}_i) \leq 1$ for all i. Define $S := \sum_{i=1}^{n} \mathbb{I}_i$, then since $\mathsf{E}(\mathbb{I}_i) \leq \rho$, we get $\mathsf{E}(S) = \sum_{i=1}^{n} \mathsf{E}(\mathbb{I}_i) \leq n\rho$. Moreover, $S - \mathsf{E}(S) \geq S - n\rho \geq \tau$ for some τ to be fixed later. Application of a variant of Hoeffding's inequality (with relaxed independence constraints; see [19]) gives

$$\Pr[S - n\rho \geq \tau] \leq \Pr[S - \mathsf{E}(S) \geq \tau] \leq \exp\left(-\frac{\tau^2}{2n}\right)$$

Since $\frac{1}{n}S \geq \min_i \mathbb{I}_i$, we can choose τ to satisfy $\frac{\tau}{n} \leq \min_i \mathbb{I}_i - \rho \leq \frac{1}{n}S - \rho$. So we can continue the chain of inequalities on the left-side as

$$\Pr\left[\min_i \mathbb{I}_i - \rho \geq \frac{\tau}{n}\right] \leq \Pr[S - n\rho \geq \tau] \leq \exp\left(-\frac{\tau^2}{2n}\right),$$

and by taking $\delta := \frac{\tau}{n}$ we conclude that

$$p := \Pr\left[\min_i \mathbb{I}_i \geq \rho + \delta\right] \leq \exp\left(-\frac{n\delta^2}{2}\right)$$

for all $\delta \geq 0$. By construction, the adversary is successful if and only if $\mathbb{I}_i = 1$ for all rounds $i = 1, 2, \ldots, n$, or equivalently, $\min_i \mathbb{I}_i = 1$. Choosing $\delta := 1 - \rho > 0$, the number n of rounds until $\Pr[\min_i \mathbb{I}_i \geq \rho + \delta = 1] < \varepsilon$ is achieved comes to $n \in \mathcal{O}\left(\log \frac{1}{\varepsilon}\right)$. The bit-complexity is $n \cdot t \cdot |m|$, where $|m|$ is the length of the message, and as such in $\mathcal{O}\left(|m| \cdot |\mathrm{nb}(s)| \cdot \log \frac{1}{\varepsilon}\right)$, i.e., polynomial in the network size and $\log \frac{1}{\varepsilon}$. Summarizing the discussion, we have proved

Theorem VI.4. *If a given network provides perfect secrecy according to Theorems VI.1, VI.2 or VI.3, then there is an efficient protocol achieving this.*

VII. Secrecy Against Active Adversaries

It is easy to see that the results of Section VI no longer hold when the adversary becomes active. Picking up our line of arguments that led to Theorem VI.4, the adversary can destroy the message simply by fiddling with one of its shares. Equally obvious is a quick-fix by attaching a checksum to the message, which lets the receiver *detect* (not necessarily correct) this kind of manipulation upon combining the incoming shares. For later reference, we state this as remark:

Remark VII.1. *One can prove (see [20]) that if error detection is required reliably with a probability of at least $1 - \varepsilon$ for $\varepsilon > 0$, then the size of the share grows by at least $\log \frac{1}{\varepsilon}$ additional bits. So, attaching an appropriate checksum to the secret before sharing it is close to optimal in terms of additional overhead.*

To ease technicalities in the following, let us distinguish two different forms of activity for the adversary:

1) he participates only in the protocol, but is allowed to actively deviate from it as he wishes,
2) he participates in the protocol and additionally runs parallel sessions over the network.

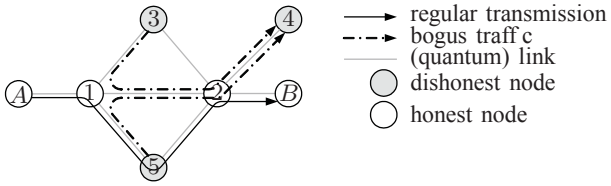


Figure 2. Path alteration via bogus traffic

The first kind of active adversary is easer to deal with, since his activity is basically focused on active modifications to the messages that he gets to pass his nodes. Modifying the routing information in order to redirect these messages differently than intended by Alice will not help him learn anything (simply because the packet is in his possession already). On the other hand, he cannot redirect packets that he does not get to see in order to acquire them. Theorem VII.2 is concerned with security against such an attacker.

This is the major difference to the second kind of adversary, who can attempt to redirect packets by intentionally congesting links that he does not directly control. To illustrate the problem, consider the simple topology displayed in Figure 2. In this scenario, Alice wishes to transmit a message to Bob, which would be possible over the path over the nodes 1 and 2. However, even though the adversary does not control this path, he can nevertheless congest the link from 1 to 2 with bogus traffic so as to enforce re-routing over node 5 (or node 3), which is under his control.

Testing whether this kind of attack is possible is highly nontrivial, because we now face an adversary who can manipulate the graph topology, while only being constrained by the link capacities. For instance, the adversary could look for a path cover of the graph G that respects the existing bandwidth limits. Indeed, even without the bandwidth restriction, the problem of finding a minimal path cover of this kind on a general graph is NP-complete, but becomes solvable in linear time for certain classes of graphs (see e.g., [21]). On the contrary, the adversary could as well compute a maximal multi-source multi-sink flow between his nodes in order to maximally congest the network. Abusing the Ford-Fulkerson approach, he could choose the flow-augmenting paths in a way so as to use as many links between honest nodes as possible. However, up to now, this is a mere heuristic and not yet a provably optimal attack strategy. Even worse, from the perspective of the honest parties, one would have to compute such a flow for all scenarios of attacking, which again boosts the computational efforts for analysis far out into infeasibility. The most trivial way of fixing this is to abandon all kinds of rerouting due to congestions and designing the relay nodes as mere queues, where messages are temporarily stored.

It appears that guarding against such kind of attack is

more a matter of congestion control. Consequently, going into more detail is thus beyond the scope of this work, as we did not presume any particular congestion control or routing scheme here.

However, if an active adversary of the first kind is assumed (i.e., bound to only manipulating, inserting or blocking of messages), we can reformulate our previous results accordingly to remain valid. The basic trick is to use the following property of secret-sharing and Reed-Solomon codes. It is well-known that Shamir's (t, n) secret sharing corresponds to a Reed-Solomon code of length n with t information words (cf. [22]). Consequently, we can recover from up to $\lfloor (n-t)/2 \rfloor$ modified shares by virtue of the Welch-Berlekamp algorithm [23] (in fact, this technique is standard in multipath transmission; cf. [3] for instance). From the error correction capacity of the code and the condition that the adversary should have less than t shares in his possession, we easily deduce the (also well known) fact that secret-sharing is robust against an active adversary with a threshold less than $n/3$. Hence, up to a third of the shares (i.e., paths) can be compromised and packets along them can be modified and the message remains concealed and intact upon reconstruction. This is the basic fact that yields to straightforward generalizations of the results in Section VI stated in the following.

Formally, a $(t, n)-$secret-sharing scheme is secure against a k-active adversary as long as its threshold k satisfies $k < \frac{n}{3} < t$ In analogy to Theorem VI.2 we get the following criterion for a 1-active adversary:

Theorem VII.1. *Let $t = |nb(s)|$ count the sender s's neighbors. If, for each $v \in V$, we have $\sum_{i=1}^{t} h_{iv} < \frac{t}{3}$, then the network provides perfect secrecy against a* 1*-active adversary.*

Proof: Put the secret message through a (t, t)-secret sharing and let each share take its own individual path through the network. With the random indicator variable

$$\mathbb{I}_{i,j} := \begin{cases} 1, & \text{if } h_{ij} > 0 \\ 0, & \text{otherwise,} \end{cases}$$

the number of trajectories passing through a node $v \in V$ is given by $N_v := \sum_{i=1}^{t} \mathbb{I}_{i,v}$, and its expected value is $\mathsf{E}(N_v) = \sum_{i=1}^{t} h_{iv}$. An active modification is possible if at least $t/3$ shares get compromised, so we can use Markov's inequality to conclude

$$\Pr[N_v \geq t/3] \leq \frac{\mathsf{E}(N_v)}{t/3} < \frac{t/3}{t/3} = 1,$$

which holds for all $v \in V$. The network thus provides perfect secrecy since the adversary can not intercept enough shares. ■

Unfortunately, Theorem VI.3 no longer holds for active adversaries. Still, we can use it to guard a transmission against an active adversary as well, yet we need some additional requirements on the network.

In fact, multipath transmission protocols usually hinge on the sender's ability to choose the paths in a way that he likes. This assumption is rarely stated explicitly (as for instance, it is used in [3] or [13]), but nevertheless of crucial importance. By specification [24, p.19], the internet protocol (IP) provides the following feature: the sender of a message can prescribe the list and order of intermediate nodes over which the packet must be forwarded until it reaches the receiver. The *Session Initiation Protocol* (SIP), specified in [25], defines a functional strict source routing mechanism, meaning that the sender can choose his relay nodes and no other nodes must be visited during a transmission. For our purposes, a weaker notion is sufficient, namely the symmetric answer property, which is introduced here:

Definition VII.1 (Symmetric Answer Property (SAP))**.** *Let a message transmission be over the relay nodes $v_1, v_2, \ldots, v_n$. If each relay node keeps the so-defined channel open for a subsequent response (e.g., an acknowledge message), i.e., the receiver can respond over the path $v_n, v_{n-1}, \ldots, v_2, v_1$, then the network is said to satisfy the* symmetric answer property.

In fact, it is this particular feature that is implicitly used in recent work on multipath transmission such as [3] or [13], although it is not explicitly stated there (usually, it is implicitly assumed in a sloppy form as saying that "the sender responds over the same channel over which he received the information"). Here, we will explicitly use this to construct a communication protocol that enjoys robustness against an active adversary. In the light of the previous discussion, this appears to be a mild and reasonable assumption, as it is included and supported by the common technological standards for data transmission, as referenced above.

Theorem VII.2. *Let $G = (V, E)$ be a graph, and let the sender and receiver be $s, r \in V$. Let the adversary be k-active, i.e., up to k nodes in G can be compromised. For perfect secrecy, it is necessary that $t = |nb(s)| > 3k$. If the network satisfies condition* (4) *and the symmetric answer property (SAP), then it permits perfect secrecy and resilience against an active adversary of the first kind.*

Notice that only the necessary condition has changed, but the sufficient condition was only augmented by assuming the SAP, since the line of arguments in the proof of Theorem VI.3 can no longer be used to prove that the adversary gets to see at most a third of the trajectories (as would be required). Nevertheless, we can use Theorem VI.3 to construct a protocol that guards us against active adversaries too.

The proof of Theorem VII.2 will partially rely on the robustness of secret sharing against modification of shares. The required result along these lines is summarized as

follows:

Lemma VII.3. *Let a general (u, v)-secret-sharing be given, and assume that the adversary has modified up to k shares. Then,*

- *if $0 \leq k < v/3 < u$ then there is no harm; all errors can be corrected.*
- *if $v/3 \leq k < u$, then the message cannot be disclosed by the attacker, but he can still thwart a correct reconstruction.*
- *if $u \leq k$, then the attacker can disclose the message without notice.*

This fact is quite well-known (cf. [26]), yet proofs can be found in [27].

Proof of Theorem VII.2: Without loss of generality, assume s's neighbors to be the nodes $\{1, 2, \ldots, t\}$, and put the message m through a (t, t)-secret-sharing scheme, transmitting the i-th share over the i-th neighbor of s.

If $t \leq 3k$, then the adversary can gain enough information to know and perhaps modify (replace) the message already after one transmission, hence $t > 3k$ is necessary for perfect security.

In the following, suppose that the sender transmits a message m along with a checksum $H(m)$ over node-disjoint channels to the receiver. The checksum (e.g., a cryptographic CRC; cf. [28]) will provide an additional mean of detecting manipulations once the error correction (and detection) capabilities of the encoding failed (cf. Remark VII.1).

Once the transmission has started, the proof of Theorem VI.3 ultimately concludes that at least one trajectory will bypass the adversary on its way from the sender to the receiver. The active adversary can either modify or not modify the shares that he intercepts. Not modifying anything literally means a passive adversary, which has been covered in the course of Theorem VI.3, hence we consider an active attacker in the following.

The protocol described now establishes a shared end-to-end secret between a sender and receiver. First, we transmit a (random) message m along with a cryptographic checksum $H(m)$ via a (t, t)-secret-sharing and (hopefully) disjoint paths over the network, and act as if the adversary were passive. This transmission process is repeated for several rounds, each of which yields a partial key K_i (for the i-th round) that we can use (e.g., concatenate and hash) to distill the final key for communication (e.g., to be used as a one-time pad over a classical, perhaps insecure, channel).

We have *two* mechanisms of error detection: the inherent error correction that comes with the secret-sharing (via the Welch-Berlekamp-Algorithm in case of Shamir's polynomial secret sharing), and the cryptographic checksum after the reconstruction. Let us abbreviate the error-correction as EC and the checksum verification as CV hereafter. Each of these can (independently) yield a positive or negative outcome, giving us four cases to distinguish in the i-th round:

1) EC points out no errors and the CV confirms the checksum: in that case, the adversary (with high probability) has either learnt nothing or everything, since the only case in which no error is determined by the error correction algorithm occurs when the adversary managed to replace *all* shares. If that happens, it is easy to replace the hidden secret by something else along with a matching checksum (hence the CV can be expected to return positive).
   Anyway, since there is a positive chance that the adversary has indeed discovered the secret, the receiver will discard any results in this case.
2) EC points out no errors but the CV fails: in that case, the adversary managed to replace all the shares, but has used a secret that is inconsistent with the reconstructed checksum. This would technically point out a manipulation while the adversary would have been capable of avoiding this detection. So, there is no point in acting like this, and this case is to be treated equally as case 1.
3) EC points out errors, but the CV confirms the checksum: in this case, the adversary must have managed to replace sufficiently many shares (cf. Lemma VII.3) to trick the error correction into wrongly indicating correct shares as malicious. Yet at least one original share has not been intercepted, because the error correction pointed out at least one error. Since we do not know which share is the correct one, but know that there must be at least one, we take the protocols output as the bitwise exclusive-or of all shares $s_1, \ldots, s_t$, that is we create
   $$K_i := s_1 \oplus s_2 \oplus \cdots \oplus s_t,$$
   knowing that the partial key K_i is entirely unknown to the adversary since at least one share in it acts like a one-time pad encryption key.
4) EC points out errors and the CV fails: in this case and by Lemma VII.3, at least $t/3$ but less than t shares must have been manipulated, since the adversary was unable to replace the secret consistently. In that case, as before, we use the bitwise XOR of all shares to distill the partial key K_i as the output of round i.

This protocol is repeated for several rounds until a sufficient amount of key-material (partial keys $K_1, K_2, \ldots$) has been produced. Notice that the actual information m transmitted through the secret-sharing is of no real value, and merely serves to create a redundancy scheme that we can use to detect a manipulation.

More importantly, observe that if case 1 occurs, then the adversary can easily make the protocol output to look like any of the other cases occurred. If this happens, then he has gained the correct information c that the receiver will use. However, the proof of Theorem VI.3 implies that with

a positive probability, cases 2, 3 or 4 must occur, hence he cannot entirely intercept the communication.

It is crucial for the sender to get notif ed in which rounds the protocol output has been discarded by the receiver. He does this by telling the sender which of the four cases above occurred, and sends this information identically back over all paths over which he received the shares originally. If the adversary missed one of the shares, then this channel will safely deliver the notif cation to the sender, thanks to the symmetric answer property. Hence, upon any two mismatching notif cations, the sender will automatically be notif ed of the attack attempt. Even in case 1, if the adversary managed to intercept all channels, he can either replace the notif cations or remain passive. In the former case, he would indicate an attack while he could have convinced the sender that there was no attack at all, so there is no point in acting like this. However, if an attack like in case 1 was successful, then the receiver would discard key-material that the sender would use, making the two end up using different (and hence useless) keys.

This kind of person-in-the-middle situation can be detected by letting the sender and receiver sacrif ce some key-bits for public comparison on a possibly insecure channel. Suitable protocols for this are well-known from quantum cryptography and we will therefore not go into further details here. If the two keys turn out different, then both discard their key-material and rerun the protocol from scratch. ■

As far as eff ciency of the transmission in the presence of an active adversary is concerned, the transmission's eff ciency is basically determined by the chance of at least one trajectory avoiding the adversaries premises. While there is a positive chance that this will happen eventually (thanks to Theorem VI.3), the number of repetitions until this occurs suff ciently often, is diff cult to determine without knowledge of the precise likelihoods. These can be obtained from simulations, but in any case, the protocol is to be repeated until the f nal verif cation indicates a correct and useable key. Nevertheless, in the next section, we use an example to show how the number of repetitions can be computed at least partially.

VIII. Application to Quantum Networks

It is important to emphasize that Theorems VI.1, VI.2 and VI.3 *should not* directly be applied to the communication network at hand. Instead, we are interested in estimating the harm that any deviation from a prescribed routing strategy causes. Going back to multipath transmission, our goal is using the results from the previous section to classify a given network as (in)secure under the assumption of random detours that a packet takes upon local congestions or empty local quantum-key-buffers.

We illustrate the application of Theorem VI.3 by using a simple example, which shall demonstrate the general line of reasoning. Take the network shown in Figure 3, with

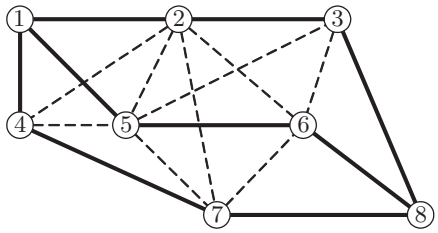


Figure 3. Example multipath transmission from 1 to 8

each link secured by means of QKD. Alice (node 1) performs a multipath communication over three disjoint channels $\rho_1 = (1 \to 2 \to 3 \to 8), \rho_2 = (1 \to 5 \to 6 \to 8), \rho_3 = (1 \to 4 \to 7 \to 8)$ (shown bold) to Bob's node 8. Assume that each node does the packet forwarding reliably, up to some chance of α for the packet to def ect from the prescribed route. Thus, assuming stochastic independence for the sake of simplicity, with probability $1 - \alpha^{\text{length}(\rho_i)-2}$, the packet will travel over ρ_i as desired. Notice that any path is accessible from any other, and that an adversary will surely not waste resources by attacking anywhere else than on the chosen paths. Hence, we can create an abstract model for such a multipath transmission by restricting the focus on whether the packets travel as desired (likelihood determined by the reliability of routing, i.e., the probability of the packet not deviating from its prescribed route), or whether they take detours (should happen with a small chance only) that could yield to intersecting paths and disclosure of the secret message.

For the analysis of a general network $G = (V, E)$ under a multipath transmission scenario, we therefore consider the auxiliary graph $G' = (V', E')$: let $\rho_1, \ldots, \rho_t$ be paths in G, then each of these becomes a node in G', which is connected to the sender and receiver, so put $V' := \{\rho_1, \ldots, \rho_t\} \cup \{s, r\}$. Attacking elsewhere than on the paths $\rho_1, \ldots, \rho_t$ is less paying for the adversary than compromising the paths themselves, so we may safely disregard any nodes in the network that are not on a chosen path. Also, assume that a packet can jump from any path to any other, so the nodes $\rho_1, \ldots, \rho_t$ form a clique. Finally, each path ρ_i is connected to the receiver r in a one-way manner, as the receiver is absorbing and will not pass anything further. Similarly, the sender is (one-way-)connected to all his chosen paths, though these transitions are of no further interest, since an accidental jump from a path back to the sender can trivially be corrected by the sender putting the packet back on its correct path. The set of edges therefore comes to $E' = \{\rho_1, \ldots, \rho_t\}^2 \cup \{(\rho_i, r), (s, \rho_i) | i = 1, 2, \ldots, t\}$. The resulting transition graph for the example is depicted in Figure 4, with arrows indicating possible state transitions.

The topology of the auxiliary graph G', excluding the transitions from s to each ρ_i (for obvious reasons) def nes the Markov-chain on which we can invoke the results from

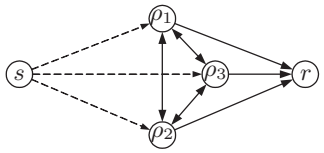


Figure 4. Auxiliary graph G' describing state transitions

Section VI. For the analysis, it remains to specify the following likelihoods:

- $\Pr[\rho_i \to r]$: with the parameter α as above, this is $\Pr[\rho_i \to r] = 1-\alpha^{\text{length}(\rho_i)-2}$. Notice that several events of node failure are not necessarily independent, and correlations among these must be considered in a more accurate (perhaps more realistic) model.
- $\Pr[\rho_i \to \rho_j]$: this quantity depends on the particular chances of jumping from a node on ρ_i to any node on ρ_j, and must be worked out individually for the network at hand. For the sake of simplicity and illustration, we assume an equal likelihood of jumping on any other path once ρ_i is left. For the example, we take $\Pr[\rho_i \to \rho_j] = \frac{1}{t-1}(1 - \Pr[\rho_i \to r])$.

Since the jumps from the sender to each of his chosen paths are uninteresting, we do not need to model the corresponding transition probabilities, nor must these appear in the transition matrix of the Markov-chain. These links are merely included to have G' consistent with our criteria, and are therefore shown dashed.

With $\alpha = 0.01$, we end up finding the transition matrix:

$$P = \begin{array}{c} \\ \rho_1 \\ \rho_2 \\ \rho_3 \\ r \end{array} \begin{array}{c} \begin{array}{cccc} \rho_1 & \rho_2 & \rho_3 & r \end{array} \\ \begin{pmatrix} 0 & 0.01 & 0.01 & 0.98 \\ 0.01 & 0 & 0.01 & 0.98 \\ 0.01 & 0.01 & 0 & 0.98 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Now, we can use Theorem VI.3 on this matrix to see that the network is indeed secure against a 2-passive adversary: with $V^* = \{1, 2, 3\}$ and by solving (2) for $A = \{1\}, \{2\}, \{3\}$, we find $h_{ij} = \frac{1}{99} < \frac{1}{2e} \approx 0.184$, for each $i, j \in V^*, j \neq j$. It follows that the network remains secure even under much less reliable routing. Indeed, we can tolerate up to $\alpha \approx 0.155$, i.e., a more than 15% chance of the packets becoming re-routed via indirect eavesdropping or congestion control. Finally, Theorem VI.4 tells that resilience against such incidents can be retained efficiently.

In order to illustrate Theorem VII.2, let us consider a network whose auxiliary graph has a similar topology as shown in Figure 4, but has 7 paths connecting Alice and Bob. The adversary is 2-active ($k = 2$), so that the necessary condition of more than $3k = 6$ neighbors is satisfied. Moreover, let the reliability of the network transmission be $\alpha = 80\%$, i.e., there is a chance of roughly 4% for the packet jumping from one path to another. Then, condition (4) is satisfied and the network provides perfect secrecy against a 2-active adversary by Theorem VII.2. With the concrete figures in hand, we can even compute the required number of protocol repetitions: it is the precise lower bound to the strictly positive probability (6) for a trajectory to bypass the adversary's servants. The sought bound is provided by the asymmetric version of the Lovasz local lemma from which the symmetric version of the Lovasz local lemma can be concluded. We spare the details for brevity, and draw the bound

$$\Pr\left[\bigcap_{\nu=1}^{k} \overline{T_i^{j_\nu}}\right] \geq \left(1 - \frac{1}{k+1}\right)^k$$

from the asymmetric (general) version of the lemma, where $T_i^{j_\nu}$ is the event of the l-th trajectory visiting the adversarial node ν starting from the sender's neighboring node i. In our case with $k = 2$, this bound evaluates to 0.44, so that there is quite a good chance for the adversary to miss at least one trajectory. This means that there is a $1 - 0.44 \approx 55.55\%$ chance for cases 2, 3 or 4 in the proof of Theorem VII.2 to occur. Since case 2 will never be observed for a reasonably acting adversary, we have a chance of $p = 0.55$ to distill key material in each round thanks to the remaining cases 3 and 4. So, the expected amount of key-material comes to $\approx 0.55n$ Bit for n rounds, and the required number of repetitions can be computed from the required amount of key-material. Still, this does not mean that case 1 is impossible and the adversary could have tricked the sender and receiver into thinking that cases 3 or 4 apply in some rounds. So, the final decision whether or not to use the key is up to the public comparison. The number of repetitions upon failure of this last step is geometrically distributed, yet the distribution parameter, namely the required success probability of a single Bernoulli trial (which is nothing else than a protocol execution), unfortunately cannot be computed from the given information.

IX. Conclusion

We have obtained simple criteria for protection against passive and active adversaries, if the activity is constrained to modifications and no bogus traffic. In case of coincidental redirection of packets along alternative routes, we have shown sufficient criteria for the transmission remaining secure in such cases. Based on these results, we have sketched how an active adversary can successfully be repelled by techniques of secret sharing, multipath transmission and error correction. Roughly speaking, our proposed protocols extend the purpose of QKD to create point-to-point secrets, to an application using QKD to establish end-to-end secrets.

Let us briefly review the results in chronological and condensed form. Our first main result is Theorem VI.1, which states that perfect secrecy is achievable if and only if the sender has a strictly positive chance to circumvent the adversary's corrupted nodes somehow. Theorem VI.2 and

Theorem VI.3 give sufficient conditions for this to happen, assuming a passive adversary listening. These conditions are derived from a Markov-chain model of the transmission. Basically, the analysis works by solving a linear equation system (1) for the vector of hitting probabilities h_{jA} (remember that h_{jA} is the chance for a packet starting off node j eventually reaching any node in the set A), where the hitting probabilities go directly into the criteria for secure communication. For solving (1), all we need are the likelihoods p_{ij} for a packet to travel to node j from node i. This is the description of the routing scheme as a Markov chain model. The model can of course be put to question, however, judging from the vast variety of routing strategies, routing table update procedures and possible flow control mechanisms, the Markov model appears to be sufficiently flexible to cover a large number of cases. If any of these sufficient criteria for perfect secrecy turns out satisfied, then Theorem VI.4 assures that the transmission is not only secure but also efficiently doable.

Regarding active adversaries, things are much more involved, and Figure 2 sketched a simple rerouting enforcement by inserting bogus traffic and exploiting load balancing and flow control. In alignment to our previous results, Theorem VII.1 transfers the known condition for 1-passive adversaries to its analogous form for 1-active adversaries. The transition from a 1-active to a k-active adversary calls for the additional hypothesis of symmetric answers, that is, the receiver must be able to reliably respond over the same channel over which he received a share in the first place. We call this the symmetric answer property, and Theorem VII.2 states that security against a k-active adversary can be achieved under roughly the same conditions as for a k-passive adversary, except for the additional assumption on symmetric answer channels. Unfortunately, all of these results refer to adversaries that do not run parallel sessions and particularly are not congesting links by bogus traffic. Defending the system against this kind of attack is beyond the capabilities of the given criteria and up to security systems linked to the flow and congestion control system within the quantum network.

Our results are only indirectly dependent on the quantum nature of the network, as the attack targets the multipath transmission regime only by *exploiting* general QKD properties. These are, moreover, independent of the particular QKD-implementation, and equally well apply to discrete or continuous quantum information encodings. In general, any successful denial-of-service attack, regardless of whether on a conventional or quantum line, can be used for indirect eavesdropping in the described form, as soon as secure multipath transmission is used.

This work is an explicit account for an adversary who turns the QKD eavesdropping detection against the network. If end-to-end security is set up by means of multipath transmission, then ”disconnecting” (by eavesdropping) otherwise adjacent nodes may enforce local re-routing of packets and in turn direct the information flow right into the adversary’s hands. We presented various sufficient criteria for a network to retain its security under indirect eavesdropping attacks by passive and certain active adversaries. Our results provide sufficient criteria to conclude that a network retains perfect secrecy under randomly compromised nodes and routes. Necessary criteria have not been given here, and are subject of future research.

Another interesting open problem is how to act against attacks involving bogus traffic in the quantum network. As has been demonstrated by a simple example scenario, an adversary can redirect traffic ”remotely” by cleverly overloading certain links and nodes (passive eavesdropping might as well yield such effects). Guarding a multipath transmission against this kind of attack is yet an open problem, and an interesting challenge of future research.

References

[1] S. Rass and S. König, “Indirect eavesdropping in quantum networks,” in *Proc. of the 5th Int. Conf. on Quantum-, Nano and Micro-technologies (ICQNM)*. Xpert Publishing Services, PO Box 7382. Wilmington, DE 19803, USA: Expert Publishing Services (XPS), 2011, pp. 83–88.

[2] Z.-S. Yuan, Y.-A. Chen, B. Zhao, S. Chen, J. Schmiedmayer, and J.-W. Pan, “Experimental demonstration of a BDCZ quantum repeater node,” *Nature*, vol. 454, pp. 1098–1101, 2008.

[3] M. Fitzi, M. K. Franklin, J. Garay, and S. H. Vardhan, “Towards optimal and efficient perfectly secure message transmission,” in *Proc. of 4th Theory of Cryptography Conf. (TCC)*, ser. LNCS 4392. Springer, 2007, pp. 311–322.

[4] C. Bennett and G. Brassard, “Public key distribution and coin tossing,” in *IEEE Int. Conf. on Computers, Systems, and Signal Processing*. IEEE Press, 1984, pp. 175–179.

[5] H. Wen, Z. Han, Y. Zhao, G. Guo, and P. Hong, “Multiple stochastic paths scheme on partially-trusted relay quantum key distribution network,” *Science in China Series F: Information Sciences*, vol. 52, no. 1, pp. 18–22, 2009.

[6] A. Varga and R. Hornig, “An overview of the OMNeT++ simulation environment,” in *Simutools ’08: Proc. of the 1st Int. Conf. on Simulation tools and techniques for communications, networks and systems & workshops*. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008, pp. 1–10. [Online]. Available: http://portal.acm.org/citation.cfm?id=1416222.1416290, last access: 06/19/2012.

[7] T. Schmitt-Manderbach, “Long distance free-space quantum key distribution,” Ph.D. dissertation, Ludwig–Maximilians–University Munich, Faculty of Physics, 2007.

[8] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, “Field trial of differential-phase-shift quantum key distribution using polarization independent frequency up-conversion detectors,” *Optics Express*, vol. 15, pp. 15 920–15 927, 2007.

[9] H. Xu, L. Ma, A. Mink, B. Hershman, and X. Tang, "1310-nm quantum key distribution system with up-conversion pump wavelength at 1550 nm," *Optics Express*, vol. 15, pp. 7247–7260, Jun. 2007.

[10] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, pp. 2050–2056, 1999.

[11] M. Franklin and R. Wright, "Secure communication in minimal connectivity models," *J. of Cryptology*, vol. 13, no. 1, pp. 9–30, 2000.

[12] M. Franklin and M. Yung, "Secure hypergraphs: privacy from partial broadcast," in *Proc. of the 27th annual ACM Symp. on Theory of computing*, ser. STOC '95. New York, NY, USA: ACM, 1995, pp. 36–44.

[13] Y. Wang and Y. Desmedt, "Perfectly secure message transmission revisited," *IEEE Trans. on Information Theory*, vol. 54, no. 6, pp. 2582–2595, 2008.

[14] M. Ashwin Kumar, P. R. Goundan, K. Srinathan, and C. Pandu Rangan, "On perfectly secure communication over arbitrary networks," in *PODC '02: Proc. of the 21st annual Symp. on Principles of distributed computing*. New York, NY, USA: ACM, 2002, pp. 193–202.

[15] R. Stewart, "RFC4960: Stream Control Transmission Protocol," http://tools.ietf.org/html/rfc4960, September 2007, last access: 05/17/2011.

[16] M. Pivk, C. Kollmitzer, and S. Rass, "SSL/TLS with quantum cryptography," in *Proc. of the 3rd Int. Conf. on Quantum, Nano and Micro Technologies*. IEEE Computer Society, February 2009, pp. 96–101.

[17] A. Mink, S. Frankel, and R. Perlner, "Quantum key distribution (qkd) and commodity security protocols: Introduction and integration," *Int. J. of Network Security & its Applications (IJNSA)*, vol. 1, no. 2, pp. 101–112, July 2009.

[18] D. Stirzaker, *Stochastic Processes & Models*. Oxford University Press, 2005.

[19] W. D. Smith, "Tail bound for sums of bounded random variables," URL: http://www.math.temple.edu/∼wds/homepage/works.html, April 2005, last access: 05/17/2011.

[20] M. Carpentieri, A. De Santis, and U. Vaccaro, "Size of shares and probability of cheating in threshold schemes," in *EUROCRYPT '93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 1994, pp. 118–125.

[21] R. Srikant, R. Sundaram, K. S. Singh, and C. P. Rangan, "Optimal path cover problem on block graphs and bipartite permutation graphs," *Theoretical Computer Science*, vol. 115, no. 2, pp. 351–357, July 19 1993.

[22] R. McElice and D. Sarwate, "On sharing secrets and Reed-Solomon codes," *Communications of the ACM*, vol. 24, no. 9, pp. 583–584, 1981.

[23] E. Berlekamp and L. Welch, "Error correction of algebraic block codes, US Patent Nr. 4,633,470,", 1986.

[24] J. Postel (ed.), "RFC 791 Internet Protocol - DARPA Internet Programm, Protocol Specif cation", Internet Engineering Task Force, September 1981, http://www.ietf.org/rfc/rfc791.txt, last access: 06/19/2012.

[25] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, "SIP: Session Initiation Protocol," RFC 2543 (Proposed Standard), Internet Engineering Task Force, March 1999, obsoleted by RFCs 3261, 3262, 3263, 3264, 3265. [Online]. Available: http://www.ietf.org/rfc/rfc2543.txt, last access: 06/19/2012.

[26] T. Rabin and M. Ben-Or, "Verif able secret sharing and multiparty protocols with honest majority," in *STOC '89: Proc. of the twenty-f rst annual ACM Symp. on Theory of computing*. New York, NY, USA: ACM, 1989, pp. 73–85.

[27] S. Rass, "On information-theoretic security: Contemporary problems and solutions," Ph.D. dissertation, Klagenfurt University, Institute of Applied Informatics, June 2009.

[28] H. Krawczyk, "LFSR-based hashing and authentication," in *CRYPTO '94: Proc. of the 14th Annual Int. Cryptology Conf. on Advances in Cryptology*. London, UK: Springer, 1994, pp. 129–139.

Reflectionless and Equiscattering Quantum Graphs and Their Applications

Taksu Cheon
Laboratory of Physics
Kochi University of Technology
Tosa Yamada, Kochi 782-8502, Japan
Email: taksu.cheon@kochi-tech.ac.jp

***Abstract*—The inverse scattering problem of a quantum star graph is shown to be solvable as a diagonalization problem of Hermitian unitary matrix when the connection condition is given by scale invariant Fulop-Tsutsui form. This enables the construction of quantum graphs with desired properties. The quantum vertices with uniform and reflectionless scatterings are examined, and their finite graph approximations are constructed. It is shown that a controllable spectral filter can be constructed from a certain reflectionless graph with the application of external potential on a line.**

***Keywords*-quantum graph; singular vertex; quantum wire; inverse scattering; quantum filter**

I. Introduction

The inverse scattering is one of the most intriguing problems in quantum mechanics. The inverse scattering problem of quantum graph [1], [2], [3], [4], in particular, has two aspects. Because the quantum graph is a nontrivial solvable system [5], it presents a challenge for extending the range of solvable inverse scattering problems. It is also increasingly becoming important as the design principle of single electron devices based on nanoscale quantum wires.

In this article, we consider the inverse scattering problem on a star graph with Fulop-Tsutsui vertices [6], the scale invariant subset of most general vertex couplings [7]. A star graph is the elementary building block of generic graph having many half-lines connected together at a single point, the singular vertex. The scattering matrix of star graph with Fulop-Tsutsui condition is energy independent. We exploit this simplicity to give the full answer to its inverse scattering problem in the form of *diagonalization problem of Hermitian unitary matrix*. Two special examples of inverse scattering problems, that of reflectionless transmission, and of equal-scattering including the reflection, are examined in detail. Very interesting designs involving Diophantine numbers emerge for the realization of quantum device with such properties. Since any singular vertex is effectively reduced to Fulop-Tsutsui vertex in both high and low energy limits [8], our study hopefully opens up a door for the full study of inverse scattering problems for general singular vertex.

The quantum graph has to be controllable by external field of macroscopic scale, if it is to be useful as a quantum device. We formulate scattering problems on a quantum graph with constant potentials with differing strengths applied to graph lines. The formalism is applied to analyze several models of quantum graphs with external potential on a line. The existence of threshold resonance phenomenon is pointed out, and it is shown to be useful in designing controllable spectral filtering devices. Specifically, a controllable band filter with flat spectral response is constructed from a $n = 4$ reflectionless quantum graph.

This article is organized as follows: In the second section, we formulate the inverse scattering problem of scale invariant graph vertices in terms of matrix diagonalization. In the third section, a scheme to approximate the vertex with small structures made up of δ-vertices is developed. In the fourth section, the scheme is applied to obtain reflectionless and equitransmitting quantum graphs. The accuracy of the approximating procedure is also examined in the same section. In the fifth section, with the application of the quantum graphs as controllable quantum devices in mind, the scattering formalism is extended to handle the added external potentials on the lines. In the sixth section, we take a look at the threshold resonance phenomenon which is found in the quantum graph with a line subjected to the added potential. In the seventh section, we examine a $n = 4$ reflectionless graph with a positive external potential on a line, and point out its utility as band spectral filter. The paper ends with the concluding eighth section.

II. Inverse scattering as diagonalization

The quantum graph is a system made up of interconnected one-dimensional lines on which a quantum particle moves around. The simplest nontrivial quantum graph is a star-shaped graph with a single node. This "elementary particle of quantum graph" is also referred to as singular quantum vertex. We start by considering a singular quantum vertex of degree n, having n half-lines comming out of a point-like node (Fig. 1). The quantum particle moving on i-th line is described by the wave function $\psi_i(x_i)$ which satisfies the Schrödinger equation, which, after proper rescaling of the units, read

$$-\frac{d^2}{dx_i^2}\psi_i(x_i) = k^2\psi_i(x_i) \quad (i = 1, ..., n). \tag{1}$$

The coordinates x_i on the i-th line are labeled outwardly from the singular vertex, which is assigned the value $x_i = 0$ for all i. The specification of the connection condition at the node

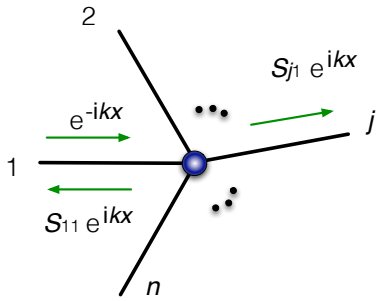


Fig. 1. Schematic representation of scattering of a quantum particle on a star graph of degree n.

$x_i = 0$ characterizes the system. Let us define the boundary vectors Ψ and Ψ' by

$$\Psi = \begin{pmatrix} \psi_1(0) \\ \vdots \\ \psi_n(0) \end{pmatrix}, \quad \Psi' = \begin{pmatrix} \psi_1'(0) \\ \vdots \\ \psi_n'(0) \end{pmatrix}, \tag{2}$$

in which $\psi_i'(x_i)$ is the spatial derivative of the wave function on i-th line. The current conservation at the node can be expressed as

$$\Psi^\dagger \Psi' - \Psi'^\dagger \Psi = 0. \tag{3}$$

It is hown in [7] that this condition can be rephrased as

$$A\Psi + B\Psi = 0. \tag{4}$$

with two $n \times n$ matrices A and B, which satisfy

$$A^\dagger B = B^\dagger A, \quad \mathrm{rank}(A, B) = n. \tag{5}$$

It is shown in [9] that this most general connection condition is characterized by a complex matrix T of size $(n-m) \times m$ where m can take the integer value $m = 1, 2, ..., n-1$, and is given by

$$\begin{pmatrix} I^{(m)} & T \\ 0 & 0 \end{pmatrix} \Psi' = \begin{pmatrix} S & 0 \\ -T^\dagger & I^{(n-m)} \end{pmatrix} \Psi, \tag{6}$$

where S is a Hermitian matrix of size $m \times m$. The scale invariant subfamily of most general connection condition is characterized by a complex matrix T of size $(n-m) \times m$ where m can take the integer value $m = 1, 2, ..., n-1$, and is given by

$$\begin{pmatrix} I^{(m)} & T \\ 0 & 0 \end{pmatrix} \Psi' = \begin{pmatrix} 0 & 0 \\ -T^\dagger & I^{(n-m)} \end{pmatrix} \Psi, \tag{7}$$

where $I^{(l)}$ signifies the identity matrix of size $l \times l$. To achieve the from (7), we may have to suitably renumber lines, in general.

The particle coming in from the j-th line and scattered off the singular vertex is described by the scattering wave function on the i-th line, $\psi_i^{(j)}(x)$ which is given in the form

$$\begin{aligned} \psi_i^{(j)}(x) &= \mathrm{e}^{-\mathrm{i}kx} + \mathcal{S}_{jj} e^{\mathrm{i}kx} \qquad (i = j) \\ &= \mathcal{S}_{ij} e^{\mathrm{i}kx} \qquad (i \neq j). \end{aligned} \tag{8}$$

Consider matrices $M = \{\psi_{ij}(0)\}$ and $M' = \{\psi_{ij}'(0)\}$. They are given, in terms of $\mathcal{S}$ by

$$M = I^{(n)} + \mathcal{S}, \quad M' = \mathrm{i}k(-I^{(n)} + \mathcal{S}), \tag{9}$$

Since each column of M and M' satisfies the equation (7), we have

$$\begin{pmatrix} I^{(m)} & T \\ 0 & 0 \end{pmatrix} M' = \begin{pmatrix} 0 & 0 \\ -T^\dagger & I^{(n-m)} \end{pmatrix} M. \tag{10}$$

From (9) and (10), we easily obtain the explicit solution of the scattering matrix $\mathcal{S} = \{\mathcal{S}_{i,j}\}$ in the form

$$\mathcal{S} = -I^{(n)} + 2 \begin{pmatrix} I^{(m)} \\ T^\dagger \end{pmatrix} \left(I^{(m)} + TT^\dagger \right)^{-1} \begin{pmatrix} I^{(m)} & T \end{pmatrix}. \tag{11}$$

Squared moduli of the elements of $\mathcal{S}$ have the following interpretation: $|S_{ij}|^2$ for $j \neq i$ represents the probability of transmission from the i-th to the j-th line, $|S_{jj}|^2$ is the probability of reflection on the j-th line. A notable feature of this $\mathcal{S}$ obtained from Fulop-Tutsui vertex its Hermiticity;

$$\mathcal{S}^\dagger = \mathcal{S}. \tag{12}$$

Since the scattering matrix is unitary for any system, in general, *i. e.*

$$\mathcal{S}^\dagger \mathcal{S} = I^{(n)}, \tag{13}$$

$\mathcal{S}$ belongs to a special class of square matrix that is at the same time *Hermitian and unitary* [10].

A natural question to be asked is what subset of Hermitian and unitary matrix, the scattering matrix of entire Fulop-Tsutsui vertex forms. To answer this question, we look for an alternative expression of (11). By multiplying $\begin{pmatrix} I^{(m)} & T \end{pmatrix}$ from the left, we obtain

$$\begin{pmatrix} I^{(m)} & T \end{pmatrix} S = \begin{pmatrix} I^{(m)} & T \end{pmatrix} \tag{14}$$

Similarly, by multiplying $\begin{pmatrix} T^\dagger & I^{(n-m)} \end{pmatrix}$ from the left, we obtain

$$\begin{pmatrix} T^\dagger & I^{(n-m)} \end{pmatrix} S = -\begin{pmatrix} T^\dagger & I^{(n-m)} \end{pmatrix}. \tag{15}$$

Combing these two expression, we have $X_m \mathcal{S} = Z_m X_m$ with the definitions

$$\begin{aligned} X_m &= \begin{pmatrix} I^{(m)} & T \\ T^\dagger & -I^{(n-m)} \end{pmatrix}, \\ Z_m &= \begin{pmatrix} I^{(m)} & 0 \\ 0 & -I^{(n-m)} \end{pmatrix}. \end{aligned} \tag{16}$$

Thus we can express $\mathcal{S}$ in the form of a products of three Hermitian matrices as [10]

$$\mathcal{S} = X_m^{-1} Z_m X_m. \tag{17}$$

Interestingly, (17) can also be viewed as the diagonalization of Hermitian unitary matrix $\mathcal{S}$ by a non-unitary Hermitian matrix X_m. We can show, in fact, that this form leads to the path to the inverse scattering problem for quantum graph vertex of Fulop-Tsutsui type: Let us suppose that the full set of scattering data is given in terms of an arbitrary Hermitian

unitary matrix $\mathcal{S}$. Let us signify the rank of the matrix $\mathcal{S}+I^{(n)}$ by m. After proper renumbering of lines, we can write this matrix in the form

$$\mathcal{S}+I^{(n)}=\begin{pmatrix} I^{(m)} \\ T^\dagger \end{pmatrix} M \begin{pmatrix} I^{(m)} & T \end{pmatrix}, \tag{18}$$

where M is a Hermitian $m\times m$ matrix, and T, a complex $(n-m)\times m$ matrix. From the unitarity of $\mathcal{S}$, we find the relation $(\mathcal{S}+I^{(n)})^2=2(\mathcal{S}+I^{(n)})$, from which we obtain

$$M=2(I^{(m)}+TT^\dagger)^{-1}, \tag{19}$$

and we therefore arrive at (11). We conclude, therefore, that *any Hermitian unitary matrix can be viewed as a scattering matrix $\mathcal{S}$ of a Fulop-Tsutsui vertex.*

In order for a quantum star graph to break scale invariance and obtain k-dependence, its scattering matrix needs to become non-Hermite. The existence and the uniqueness of the inverse scattering solution of quantum star graph extend to this more general non-Hermite case also. These observations can be reached easily and directly from the original "U-form" of connection condition using a unitary matrix [2], [7], but our procedure holds definite advantage of giving us T directly, which is known [9] to allow us the physical construction of a finite quantum graph whose small size limit reproduces the prescribed $\mathcal{S}$.

The procedure of diagonalization, in practice, is quite cumbersome for large n. A simpler alternative to obtain T from $\mathcal{S}$ is the following: Let us divide $\mathcal{S}$ into four submatrices $\mathcal{S}_{11}$, $\mathcal{S}_{12}$, $\mathcal{S}_{21}$ and $\mathcal{S}_{22}$ of size $m\times m$, $m\times(n-m)$, $(n-m)\times m$ and $(n-m)\times(n-m)$, respectively as

$$\mathcal{S}=\begin{pmatrix} \mathcal{S}_{11} & \mathcal{S}_{12} \\ \mathcal{S}_{21} & \mathcal{S}_{22} \end{pmatrix}. \tag{20}$$

These submatrices have the properties

$$\mathcal{S}_{11}^\dagger=\mathcal{S}_{11},\quad \mathcal{S}_{22}^\dagger=\mathcal{S}_{22},\quad \mathcal{S}_{21}^\dagger=\mathcal{S}_{12}, \tag{21}$$

and also

$$\begin{aligned} &\mathcal{S}_{11}^2+\mathcal{S}_{12}^2=I^{(m)},\\ &\mathcal{S}_{22}^2+\mathcal{S}_{21}^2=I^{(n-m)},\\ &\mathcal{S}_{11}\mathcal{S}_{12}+\mathcal{S}_{12}\mathcal{S}_{22}=0. \end{aligned} \tag{22}$$

From these equations, we have the explicit expressions of T in terms of $\mathcal{S}_{ij}$;

$$\begin{aligned} T &= \left(I^{(m)}+\mathcal{S}_{11}\right)^{-1}\mathcal{S}_{12}\\ &= \mathcal{S}_{21}^\dagger\left(I^{(n-m)}-\mathcal{S}_{22}\right)^{-1}. \end{aligned} \tag{23}$$

It is easy to check that the forms (11) and (17) can be kept under the index renumbering $\alpha\leftrightarrow\beta$ both for $\alpha,\beta\le m$ and for $\alpha,\beta>m$ with the proper transformation for the elements of T; It is given by $t_{\alpha j}\leftrightarrow t_{\beta j}$ for the former and $t_{i\alpha}\leftrightarrow t_{i\beta}$ for the latter. For the case of $\alpha\le m$ and $\beta>m$, it is given by $t_{ij}\to t'_{ij}$ with

$$\begin{aligned} t'_{ij} &= \frac{t_{ij}t_{\alpha\beta}-t_{\alpha j}t_{i\beta}}{t_{\alpha\beta}}\bar{\delta}_{i\alpha}\bar{\delta}_{j\beta}\\ &\quad -\frac{t_{\alpha j}\delta_{i\alpha}-\delta_{\alpha j}t_{i\alpha}+\delta_{i\alpha}\delta_{j\beta}}{t_{\alpha\beta}}, \end{aligned} \tag{24}$$

where we define $\bar{\delta}_{ij}=1-\delta_{ij}$. This implies that it is not possible to exchnage the indices α and β whose $t_{\alpha\beta}$ is zero. This corresponds to the index ordering for which both $(I^{(m)}+\mathcal{S}_{11})$ and $(I^{(n-m)}-\mathcal{S}_{22})$ are singular and the T is undefined, thus the boundary condition at the singular vertex does not take the form (7).

III. Finite approximation

Finite tubes connected at a node generically tend, in their small diameter limit, to a vertex with delta-like connections, given by $m=1$, and $T=\begin{pmatrix}1 & \cdots & 1\end{pmatrix}$, namely

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}\Psi'=\begin{pmatrix} v & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}\Psi, \tag{25}$$

and very often to its strength zero limit, $v=0$, a free vertex [11]. We might also consider applying localized magnetic field to achieve phase change. It is natural, therefore, to devise a design principle to construct arbitrary connection condition out of this elementary vertex. Once all elements of $T=\{t_{ij}\}$, $i=1,...,m$ and $j=m+1,..,n$, are obtained, a finite graph with internal lines and the δ-coupling vertices can be constructed systematically, whose small-size limit reproduces the boundary condition of Fulop-Tsutsui vertex, (7). The scheme developed in [12] works as follows.

(i) Assemble the edges of n half lines which we assign the numbers $j=1,2,...,n$, and connect them in pairs (i,j) by internal lines of length d/r_{ij} except when $r_{ij}=0$, for which case, the pairs are left unconnected. Apply vector potential A_{ij} on the line (i,j) to produce extra phase shift χ_{ij} between the edges when its value is nonzero. Place δ potential of strength v_i at each edge i.

(ii) The length ratio r_{ij} and the phase shift χ_{ij} are determined from the non-diagonal elements of the matrix Q defined by

$$Q=\begin{pmatrix} T \\ I^{(n-m)} \end{pmatrix}\begin{pmatrix} -T^\dagger & I^{(m)} \end{pmatrix}=\begin{pmatrix} -TT^\dagger & T \\ -T^\dagger & I^{(m)} \end{pmatrix}, \tag{26}$$

by the realation $r_{ij}e^{\mathrm{i}\chi_{ij}}=Q_{ij}$ $(i\ne j)$. This means that we have

$$\begin{aligned} r_{ij}e^{\mathrm{i}\chi_{ij}} &= -\sum_{l>m}t_{il}t_{jl}^* && (i,j\le m),\\ &= t_{ij} && (i\le m, j>m),\\ &= 0 && (i,j>m). \end{aligned} \tag{27}$$

(iii) The strength v_i is given by the diagonal elements of the matrix V defined by

$$V = \frac{1}{d}(2I^{(n)} - J^{(n)})R, \tag{28}$$

where R is the matrix whose elements are made from absolute values of matrix elements of Q, *i.e.*

$$R = \{r_{ij}\} = \{|Q_{ij}|\}. \tag{29}$$

The matrix $J^{(n)}$ is of size $n \times n$ with all elements given by 1. This means that we have

$$\begin{aligned} v_i &= \frac{1}{d}(1 - \sum_{l \le m} r_{li}) \qquad (i > m), \\ &= \frac{1}{d}(\sum_{l>m}[r_{il}^2 - r_{il}] - \sum_{l(\neq i)\le m} r_{il}) \qquad (i \le m). \end{aligned} \tag{30}$$

These fine tunings of length and strength are necessary to counter the generic opaqueness brought in with every addition of vertices and lines into a graph.

The wave function $\phi(x)$= $\phi_{i,j}(x)$ on any internal line (i, j), we have the relation

$$\begin{pmatrix} \phi'(0) \\ e^{i\chi}\phi'(\frac{d}{r}) \end{pmatrix} = -\frac{r}{d} \begin{pmatrix} F(\frac{d}{r}) & -G(\frac{d}{r}) \\ G(\frac{d}{r}) & -F(\frac{d}{r}) \end{pmatrix} \begin{pmatrix} \phi(0) \\ e^{i\chi}\phi(\frac{d}{r}) \end{pmatrix}, \tag{31}$$

with $F(x) = x\cot x$ and $G(x) = x\,\mathrm{cosec}\, x$. Combining (31) with the condition at the i-th endpoint,

$$\psi_i'(0) + \sum_{j\neq i} \phi_{ij}'(0) = v_i\psi_i(0) \tag{32}$$

where we have the δ-potential of strength v_i, we obtain the relations between the boundary values $\psi_i = \psi_i(0)$ and $\psi_i' = \psi_i'(0)$ in the form

$$d\psi_i' = \left(v_i d + \sum_{l\neq i} r_{il}F_{il}\right)\psi_i - \sum_{l\neq i} e^{\mathrm{i}\chi_{ij}} r_{il}G_{il}\psi_l, \tag{33}$$

where the obvious notations $F_{ij} = \frac{d}{r_{il}}\cot\frac{d}{r_{il}}$ and $G_{ij} = \frac{d}{r_{il}}\,\mathrm{cosec}\,\frac{d}{r_{il}}$ are adopted. Note that the equation (33) is exact and does not involve any approximation. In the short range limit $d \to 0$, we have $F_{ij} = 1 + O(d^2)$ and $G_{ij} = 1 + O(d^2)$. We can then show, with a straightforward calculation in the manner of [9], that the limit $d \to 0$ gives the desired connection condition for Fulop-Tsutsui vertex (7).

IV. Reflectionless and equiscattering graphs

With the solution of the inverse scattering fully formulated, it is now possible to find a Fulop-Tsutsui vertex from a given scattering matrix with specific requirement. Our previous results detailed in [12] showing the reconstruction of "Free-like" scattering is one such example, and could have been achieved easier with current method. We now ask whether there is fully reflectionless graph whose scattering matrix has only zeros for its diagonal elements, $\mathcal{S}_{ii} = 0$. Vertices yielding such scattering matrix is known to be useful in developing semiclasical theory of quantum spectra [13]. If we

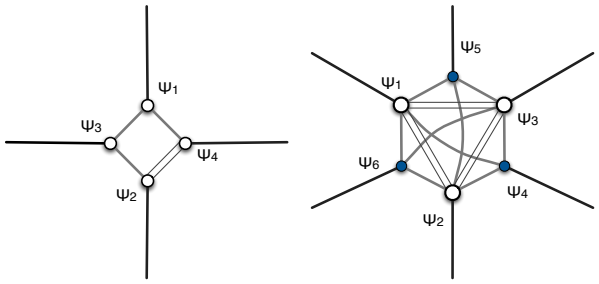


Fig. 2. Finite approximation to the reflectionless Fulop-Tsutsui vertices corresponding to (35) (left) and (41) (right) constructed according to (26)-(28). The relative length of internal lines r_{ij} and strength of the δ-potentials v_j for former are given by (40), while those for the latter are given by (43). Double lines indicate the existence of non-zero phase shift χ_{ij}.

limit ourselves to real $\mathcal{S}$, it becomes symmetric matrix with $\mathcal{S}_{ij} = \mathcal{S}_{ji}$.

We note a useful relation concerning the trace of the scattering matrix. Taking the trace of (17) and utilizing $\mathrm{tr}(AB) = \mathrm{tr}(BA)$, we have

$$\mathrm{tr}\,\mathcal{S} = \mathrm{tr}\, Z_m = 2m - n. \tag{34}$$

Since $\mathcal{S}$ for reflectionless scattering is traceless, we can have such scattering only for $n = 2m$.

Our first example is with $n = 4$ whose $\mathcal{S}$ is given by

$$\mathcal{S} = \begin{pmatrix} 0 & 0 & a & \sqrt{1-a^2} \\ 0 & 0 & \sqrt{1-a^2} & -a \\ a & \sqrt{1-a^2} & 0 & 0 \\ \sqrt{1-a^2} & -a & 0 & 0 \end{pmatrix}, \tag{35}$$

and the and corresponding T, by

$$T = \begin{pmatrix} a & \sqrt{1-a^2} \\ \sqrt{1-a^2} & -a \end{pmatrix}. \tag{36}$$

The finite approximation is characterized by

$$r_{12} = r_{34} = 0,\ r_{13} = r_{24} = a,\ r_{23} = r_{14} = \sqrt{1-a^2},$$

$$\begin{aligned} e^{\mathrm{i}\chi_{24}} = -1,\ e^{\mathrm{i}\chi_{ij}} = 1 \text{ all others}, \\ v_1 = v_2 = v_3 = v_4 = \frac{1 - a - \sqrt{1-a^2}}{d}, \end{aligned} \tag{37}$$

The finite graph approximation is schematically illustrated in the left side of Figure 1.

We next turn to reflectionless scattering with uniform transmission to all other lines. The smallest non-trivial example of such matrix exists for $n = 4$, and given by

$$\mathcal{S} = \frac{1}{\sqrt{5}} \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & -\mathrm{i} & \mathrm{i} \\ 1 & \mathrm{i} & 0 & -\mathrm{i} \\ 1 & -\mathrm{i} & \mathrm{i} & 0 \end{pmatrix}. \tag{38}$$

The corresponding T is given by

$$T = \begin{pmatrix} \omega & \omega^{-1} \\ \omega^{-4} & \omega^4 \end{pmatrix}. \tag{39}$$

with $\omega = e^{\mathrm{i}\frac{\pi}{6}}$. Our finite approximation is specified by following numbers.

$$r_{13} = r_{14} = r_{23} = r = _{24} = 1,\ r_{12} = r_{34} = 0,$$
$$e^{\mathrm{i}\chi_{13}} = e^{\mathrm{i}\frac{\pi}{6}}, e^{\mathrm{i}\chi_{14}} = e^{-\mathrm{i}\frac{\pi}{6}}, e^{\mathrm{i}\chi_{23}} = e^{-4\mathrm{i}\frac{\pi}{6}}, e^{\mathrm{i}\chi_{24}} = e^{4\mathrm{i}\frac{\pi}{6}},$$
$$v_1 = v_2 = v_3 = v_4 = -\frac{1}{d}, \tag{40}$$

The finite graph approximation is schematically illustrated in the right side of Figure 1.

If we limit ourselves to real scattering matrix, such matrix, called *symmetric conference matrix*, is known to exist for $n = 6, 10, 14, 18, 26, 30, 38, ...$ We look at the example of $n = 6$ whose $\mathcal{S}$ is given by

$$\mathcal{S} = \frac{1}{\sqrt{5}} \begin{pmatrix} 0 & -1 & -1 & -1 & 1 & 1 \\ -1 & 0 & -1 & 1 & -1 & 1 \\ -1 & -1 & 0 & 1 & 1 & -1 \\ -1 & 1 & 1 & 0 & 1 & 1 \\ 1 & -1 & 1 & 1 & 0 & 1 \\ 1 & 1 & -1 & 1 & 1 & 0 \end{pmatrix}. \tag{41}$$

The corresponding T is given by

$$T = \begin{pmatrix} 1 & 1+\gamma & 1+\gamma \\ 1+\gamma & 1 & 1+\gamma \\ 1+\gamma & 1+\gamma & 1 \end{pmatrix}. \tag{42}$$

where $\gamma = (\sqrt{5}-1)/2$ is the golden mean. Our finite approximation is specified by following numbers.

$$r_{12} = r_{23} = r_{13} = 4 + 3\gamma,\ r_{14} = r_{25} = r_{36} = 1,$$
$$r_{15} = r_{16} = r_{26} = r_{24} = r_{31} = r_{32} = 1 + \gamma,$$
$$r_{45} = r_{46} = r_{56} = 0,$$
$$e^{\mathrm{i}\chi_{12}} = e^{\mathrm{i}\chi_{23}} = e^{\mathrm{i}\chi_{13}} = -1,\ e^{\mathrm{i}\chi_{ij}} = 1 \text{ all others},$$
$$v_1 = v_2 = v_3 = -6\frac{\gamma+1}{d},\ v_4 = v_5 = v_6 = -2\frac{\gamma+1}{d}. \tag{43}$$

The finite graph approximation is schematically illustrated in the right side of Figure 1.

Our next example is the reflectionless equitransmitting graph with $n = 10$, that corresponds to the $\mathcal{S}$ matrix given by $n = 10$ conference matrix

$$\mathcal{S} = \frac{1}{3} \begin{pmatrix} 0 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & 0 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 0 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 0 & -1 & 1 & 1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & 0 & 1 & 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 & 1 & 0 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & 1 & 1 & 1 & 0 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & 1 & -1 & 1 & 0 & 1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & 0 \end{pmatrix} \tag{44}$$

The trace of $\mathcal{S}$ is zero again, and we have $m = \frac{n}{2} = 5$. The matrix T specifying the vertex is given by

$$T = \begin{pmatrix} -1 & 0 & 1 & 1 & 0 \\ 0 & -1 & 0 & 1 & 1 \\ 1 & 0 & -1 & 0 & 1 \\ 1 & 1 & 0 & -1 & 0 \\ 0 & 1 & 1 & 0 & -1 \end{pmatrix}, \tag{45}$$

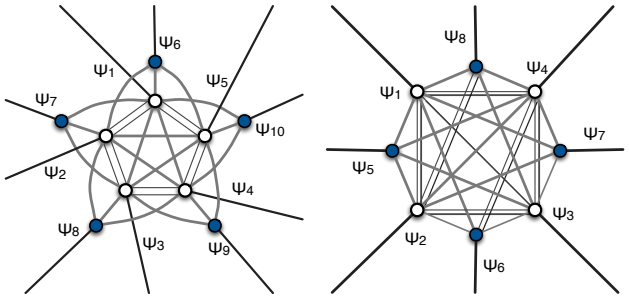


Fig. 3. Finite approximation to the equal-scattering Fulop-Tsutsui vertex corresponding to $n = 10$ conference matrix, (44) (left) and $n = 8$ Hadamard matrix, (47) (right) constructed according to to (26)-(28). The relative length of internal lines r_{ij} and strength of the δ-potentials v_j for former are given by (46), while those for the latter are given by (49). Double lines indicate the existence of non-zero phase shift χ_{ij}.

where $\sigma = \sqrt{2}-1$ is the silver mean. Our finite approximation is specified by following numbers for verteces;

$$r_{12} = r_{23} = r_{34} = r_{45} = r_{15} = 1,$$
$$r_{16} = r_{27} = r_{38} = r_{49} = r_{5a} = 1,$$
$$r_{18} = r_{29} = r_{3a} = r_{46} = r_{57} = 1,$$
$$r_{19} = r_{2a} = r_{36} = r_{47} = r_{58} = 1,$$
$$r_{13} = r_{14} = r_{24} = r_{25} = r_{35} = 2,$$
$$r_{17} = r_{28} = r_{39} = r_{4a} = r_{56} = 0,$$
$$r_{1a} = r_{26} = r_{37} = r_{48} = r_{59} = 0,$$
$$r_{67} = r_{78} = r_{89} = r_{9a} = r_{6a} = 0,$$
$$r_{68} = r_{79} = r_{8a} = r_{69} = r_{7a} = 0,$$
$$e^{\mathrm{i}\chi_{12}} = e^{\mathrm{i}\chi_{23}} = e^{\mathrm{i}\chi_{34}} = e^{\mathrm{i}\chi_{45}} = e^{\mathrm{i}\chi_{15}} = -1$$
$$e^{\mathrm{i}\chi_{16}} = e^{\mathrm{i}\chi_{27}} = e^{\mathrm{i}\chi_{38}} = e^{\mathrm{i}\chi_{49}} = e^{\mathrm{i}\chi_{5a}} = -1$$
$$e^{\mathrm{i}\chi_{ij}} = 1 \text{ all others},$$
$$v_1 = v_2 = v_3 = v_4 = v_5 = -\frac{6}{d},$$
$$v_6 = v_7 = v_8 = v_9 = v_a = -\frac{2}{d}. \tag{46}$$

Here, a in subscript stands for the index for 10th edge. The finite graph approximation for this case is schematically illustrated in the left side of Figure 2.

The last example is the equal-scattering graph, in which in the scattering is uniform in all lines including the line of incoming particle. Such matrix, called *symmetric Hadamard matrix*, is known to exist for $n = 2^k$, $k = 0, 1, ...$ An example of such $\mathcal{S}$ for $n = 8$ is given by

$$\mathcal{S} = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \\ -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 \end{pmatrix}. \tag{47}$$

The trace of $\mathcal{S}$ is again zero, and we have $m = \frac{n}{2} = 4$. The

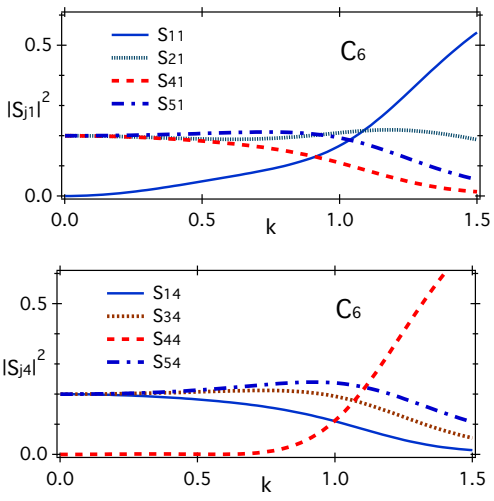


Fig. 4. Scattering probabilities as functions of incoming momentum k (in the unit of $1/d$) of finite quantum graph approximating the equal-transmitting reflectionless vertex with $n = 6$ edges represented in Figure 1, right.

matrix T specifying the Fulop-Tsutsui the vertex is given by

$$T = \frac{1}{\sigma+1}\begin{pmatrix} \sigma & 1 & 1 & 1 \\ 1 & \sigma & 1 & 1 \\ 1 & 1 & \sigma & 1 \\ 1 & 1 & 1 & \sigma \end{pmatrix}. \tag{48}$$

where $\sigma = \sqrt{2}-1$ is the silver mean. Our finite approximation is specified by following numbers for verteces;

$$\begin{aligned} r_{12} = r_{13} = r_{14} = r_{23} = r_{24} = r_{34} = 1+\sigma, \\ r_{15} = r_{26} = r_{37} = r_{48} = \frac{\sigma}{1+\sigma}, \\ r_{16} = r_{17} = r_{18} = r_{27} = r_{28} = r_{38} = \frac{1}{1+\sigma}, \\ r_{25} = r_{35} = r_{36} = r_{45} = r_{46} = r_{47} = \frac{1}{1+\sigma}, \\ r_{56} = r_{57} = r_{58} = r_{67} = r_{68} = r_{78} = 0, \\ e^{\mathrm{i}\chi_{12}} = e^{\mathrm{i}\chi_{13}} = e^{\mathrm{i}\chi_{14}} = e^{\mathrm{i}\chi_{23}} \\ = e^{\mathrm{i}\phi_{24}} = e^{\mathrm{i}\chi_{34}} = -1,\ e^{\mathrm{i}\chi_{ij}} = 1 \text{ all others}, \\ v_1 = v_2 = v_3 = v_4 = -\frac{5\sigma-3}{d}, \\ v_5 = v_6 = v_7 = v_8 = -\frac{\sigma+1}{d}. \end{aligned} \tag{49}$$

The finite graph approximation is schematically illustrated in the right side of Figure 2.

We now take a look at the convergence of the finite size graph approximation by numerical calculations. In Figure 3, we display the scattering matrix of the finite graph that is constructed to approximate equal-scattering reflectionless matrix, (41). These are calculated directly from (33). The value of the wave length k is in the unit of $1/d$. The convergence can be seen as quite good below $kd \lesssim 0.2$. Numerical analysis of other examples of different graphs give essentially the same conclusion that the construction does represent physical realization of singular Fulop-Tsutsui vertex.

V. Scattering Matrix for Graph with Potentials

We are interested in controlling the scattering properties of a quantum star graph with n lines through the addition of potentials on the lines. Suppose that constant potential U_i is applied to the i-th line. The Schrödinger equation now reads

$$-\frac{d^2}{dx_i^2}\psi_i(x_i) = (k^2 - U_i)\psi_i(x_i) \quad (i = 1, ..., n). \tag{50}$$

Suppose a quantum particle with mechanical energy E comes in the vertex from the j-th line, and scattered into all the lines through the vertex. The i-th component of the wave function is given by

$$\begin{aligned} \psi_i^{(j)}(x) &= \mathrm{e}^{-\mathrm{i}k_i x} + \mathcal{S}_{jj}e^{\mathrm{i}k_i x} \qquad (i = j) \\ &= \sqrt{\frac{k_j}{k_i}}\mathcal{S}_{ij}e^{\mathrm{i}k_i x} \qquad (i \neq j), \end{aligned} \tag{51}$$

where k_ℓ is the local momentum on the ℓ-th line, defined by

$$k_\ell = \sqrt{E - U_\ell}, \tag{52}$$

where U_ℓ is the potential on the ℓ-th line. The coefficients $\sqrt{k_j/k_i}$ is there to impose proper normalization to guarantee that the flux conservation is given by $\Psi^\dagger\Psi' - \Psi'^\dagger\Psi = 0$ as before. The scattering matrix $\mathcal{S} = \{\mathcal{S}_{ij}\}$ now depends, besides the internal properties of the vertex, on E and $U_1, U_2, \ldots, U_n$.

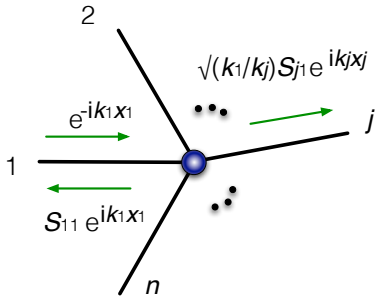


Fig. 5. Schematic representation of scattering of a quantum particle on a star graph of degree n with potentials U_i on the line i.

As before, we define matrices $M = \{\psi_{ij}(0)\}$ and $M' = \{\psi'_{ij}(0)\}$. This time, from (51), we have

$$\begin{aligned} M &= I^{(n)} + K^{-1}\mathcal{S}K, \\ M' &= \mathrm{i}K^2(-I^{(n)} + K^{-1}\mathcal{S}K), \end{aligned} \tag{53}$$

where the matrix K is defined by its elements

$$K_{ij} = \sqrt{k_i}\delta_{ij}. \tag{54}$$

The boundary condition $AM + BM' = 0$, together with (53) leads to [14]

$$\mathcal{S} = -(AK^{-1} + \mathrm{i}BK)^{-1}(AK^{-1} - \mathrm{i}BK), \tag{55}$$

which is the desired equation.

VI. Threshold resonance in star graph with external potential

Let us consider an $n = 3$ star graph with a Fulop-Tsutsui coupling with

$$T = \begin{pmatrix} a & b \end{pmatrix}, \tag{56}$$

which gives the explicit equation for the boundary condition $B\Psi' = -A\Psi$ in the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \Psi' = \begin{pmatrix} 0 & 0 & 0 \\ -a & 1 & 0 \\ -b & 0 & 1 \end{pmatrix} \Psi. \tag{57}$$

The scattering matrix in the absence of potentials $U_i = 0$ is given by

$$\mathcal{S} = \frac{1}{1+a^2+b^2} \begin{pmatrix} 1-a^2-b^2 & 2a & 2b \\ 2a & -1+a^2-b^2 & 2ab \\ 2b & 2ab & -1-a^2+b^2 \end{pmatrix}. \tag{58}$$

In order to make the system controllable with external field of macroscopic scale, we add a constant potential to one of the lines [14]. We choose the third line for this purpose, while leaving the other two lines free. The graph is schematically illustrated in Fig. 6. The system is conceived as a model of the quantum device that is controlled through the variation of the potential strength. The roles of individual lines are identified as follows:

- Line 1 is the *input*. Particles of various energies are coming in the vertex along this line.
- Line 2 is the *output*. Particles passed through the vertex are gathered on this line.
- Line 3 is the *controling line*. We assume that this line is subjected to an adjustable constant external potential U.

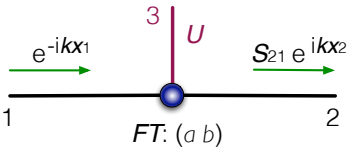


Fig. 6. Schematic depiction of the $n = 3$ star graph with an external potential U on the line 3.

A quantum particle with energy $E = k^2$ coming in the vertex from the input line 1 is scattered at the vertex into all the lines. The scattering amplitudes can be calculated by substituting the matrices A, B from the boundary condition (57) into equation (55), together with the local momenta

$$k_1 = k_2 = k, \quad k_3 = \sqrt{k^2 - U}. \tag{59}$$

For the incoming particles from the line 1, we obtain:

$$\mathcal{S}_{21}(k;U) = \frac{2a}{1+a^2+b^2\sqrt{1-\frac{U}{k^2}}}, \tag{60}$$

$$\mathcal{S}_{11}(k;U) = \frac{1-a^2-b^2\sqrt{1-\frac{U}{k^2}}}{1+a^2+b^2\sqrt{1-\frac{U}{k^2}}}, \tag{61}$$

$$\mathcal{S}_{31}(k;U) = \frac{2b\left(1-\frac{U}{k^2}\right)^{\frac{1}{4}}\Theta(k-\sqrt{U})}{1+a^2+b^2\sqrt{1-\frac{U}{k^2}}}. \tag{62}$$

The Heaviside step function $\Theta(k-\sqrt{U})$ in (62) is there to make the expression valid for all energies k^2, including $k^2 < U$. It represents the absence of the transmission to the line 3 below the threshold momentum

$$k_{\rm th} = \sqrt{U}. \tag{63}$$

We look at the probability of transmission from the input line 1 into the output line 2, which we denote by $\mathcal{P}(k;U)$, which is given by

$$\mathcal{P}(k;U) = |\mathcal{S}_{21}(k;U)|^2. \tag{64}$$

We are nterested in its k-dependence, in particular. We have, from (60),

$$\begin{aligned} \mathcal{P}(k;U) &= \frac{4a^2}{\left(1+a^2+b^2\sqrt{1-\frac{U}{k^2}}\right)^2} \quad (k \geq \sqrt{U}), \\ &= \frac{4a^2}{(1+a^2)^2+b^4(\frac{U}{k^2}-1)} \quad (k \leq \sqrt{U}). \end{aligned} \tag{65}$$

We observe that for a given constant potential on the line 3, $\mathcal{P}(k;U)$ as a function of k grows in the interval $(0,\sqrt{U})$, attains its maximum at $k = k_{\rm th}$, and decreases in the interval $(k_{\rm th},\infty)$. In particular, we have

$$\begin{aligned} \mathcal{P}(0;U) &= 0\,, \\ \mathcal{P}(k_{\rm th};U) &= \left(\frac{2a}{1+a^2}\right)^2, \\ \mathcal{P}(\infty;U) &= \left(\frac{2a}{1+a^2+b^2}\right)^2. \end{aligned} \tag{66}$$

If the parameters a, b satisfy

$$b \gg a \geq 1, \tag{67}$$

the function $\mathcal{P}(k;U)$ displays a sharp peak at the threshold momentum $k_{\rm th}$. Equation (66) implies that the peak attains the highest possible value 1 for $a = 1$. We conclude that, with the choice $b \gg a = 1$, the system has high input to output transmission probability for particles having momenta $k \approx k_{\rm th}$, and that the transmission is perfect for $k = k_{\rm th}$, while the transmission probability for other values of k is strongly suppressed. The situation is numerically illustrated in Fig. 7. The quantum graph schematically depicted in Fig. 6 can be therefore used as an adjustable spectral filter, controllable by the potential put on the controlling line 3. We remark that the resonance at the threshold momentum $k_{\rm th}$ is related to the pole of the scattering matrix which is located on the positive real axis at

$$k_{\rm pol} = \frac{b^2}{\sqrt{b^4-(1+a^2)^2}}\sqrt{U} \tag{68}$$

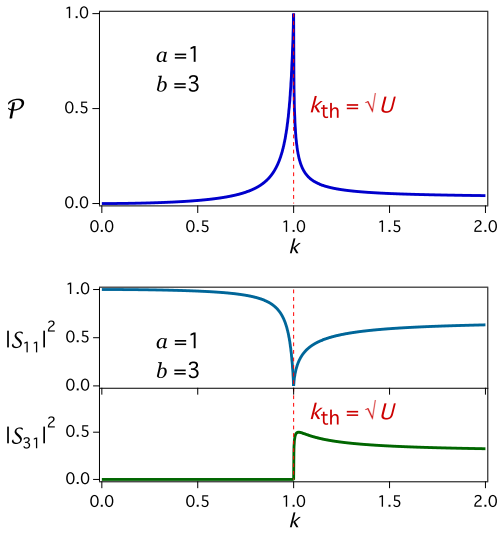


Fig. 7. Scattering characteristics of the graph from Fig. 6 with parameters $a = 1$, $b = 3$. The transmission probability $\mathcal{P}(k;U)$ as a function of k with the value of the potential set to $U = 1$ is plotted in the top figure. The lower figure shows reflection probability $|\mathcal{S}_{11}(k;U)|^2$ and the probability of transmission to the controlling line $|\mathcal{S}_{31}(k;U)|^2$.

on the unphysical Riemann surface, which is connected to the physical Riemann surface at the cut that runs between $k = \pm k_{\rm th}$.

VII. Flux control and quantum sluice-gate

Let us consider an $n = 4$ star graph, in search of another model of the quantum device, which is schematically illustrated in Fig. 8. The roles of individual lines are identified as follows:

- Line 1 is the *input*. Particles of various energies are coming in the vertex along this line.
- Line 2 is the *output*. Particles passed through the vertex are gathered on this line.
- Line 3 is the *controling line*. We assume that this line is subjected to an adjustable constant external potential U.
- Line 4 is the *drain* Our analysis has shown that this seemingly redundant line is needed for the device we wish to construct.

The vertex coupling is again assumed to be of a Fulop-Tsutsui type, specified by the coupling matrix

$$T = \begin{pmatrix} a & a \\ a & -a \end{pmatrix}, \tag{69}$$

which gives the explicit equation for the boundary condition in the form

$$\begin{pmatrix} 1 & 0 & a & a \\ 0 & 1 & a & -a \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \Psi' = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -a & -a & 1 & 0 \\ -a & a & 0 & 1 \end{pmatrix} \Psi \tag{70}$$

with $a \in \mathrm{R}$. The scattering matrix in the absence of potentials $U = 0$ is given by

$$\mathcal{S} = \frac{1}{1+2a^2} \begin{pmatrix} 1-2a^2 & 0 & 2a & 2a \\ 0 & 1-2a^2 & 2a & -2a \\ 2a & 2a & -1+2a^2 & 0 \\ 2a & -2a & 0 & -1+2a^2 \end{pmatrix}. \tag{71}$$

For a particle with energy $E = k^2$ coming in the vertex from

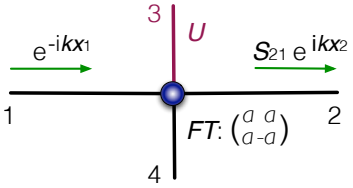


Fig. 8. Schematic depiction of the $n = 4$ star graph with an external potential U on the line No. 3.

the input line 1, we have

$$k_1 = k_2 = k, \quad k_3 = \sqrt{k^2 - U}, \quad k_4 = k. \tag{72}$$

The scattering amplitudes for particles entering from the line 1 can be calculated as

$$S_{21}(k;U) = \frac{2a^2\left(1 - \sqrt{1-\frac{U}{k^2}}\right)}{(1+2a^2)\left(1+2a^2\sqrt{1-\frac{U}{k^2}}\right)}, \tag{73}$$

and

$$S_{11}(k;U) = \frac{1 - 4a^4\sqrt{1-\frac{U}{k^2}}}{(1+2a^2)\left(1+2a^2\sqrt{1-\frac{U}{k^2}}\right)}, \tag{74}$$

$$S_{31}(k;U) = \frac{2a\left(1-\frac{U}{k^2}\right)^{\frac{1}{4}}\Theta(k-\sqrt{U})}{1+2a^2\sqrt{1-\frac{U}{k^2}}}, \tag{75}$$

$$S_{41}(k;U) = \frac{2a}{1+2a^2}. \tag{76}$$

We again denote the transmission probability from input to output lines by $\mathcal{P}(k;U) = |\mathcal{S}_{21}(k;U)|^2$. We obtain, for the transmission below the threshold,

$$\mathcal{P}(k;U) = \frac{4a^4U/k^2}{(1+2a^2)^2\left(1-4a^4+4a^4\frac{U}{k^2}\right)} \quad (k \le \sqrt{U}), \tag{77}$$

and above the threshold,

$$\mathcal{P}(k;U) = \frac{4a^4\left(1-\sqrt{1-\frac{U}{k^2}}\right)^2}{(1+2a^2)^2\left(1+2a^2\sqrt{1-\frac{U}{k^2}}\right)^2} \quad (k \ge \sqrt{U}). \tag{78}$$

Hence we have

$$\mathcal{P}(0;U) = \frac{1}{(1+2a^2)^2},$$
$$\mathcal{P}(\sqrt{U};U) = \frac{4a^4}{(1+2a^2)^2},$$
$$\mathcal{P}(\infty;U) = 0. \tag{79}$$

When U is fixed, $\mathcal{P}(k;U)$ as a function of k quickly falls off to zero at $k > \sqrt{U}$. A typical behaviour is illustrated in a numerical example in Fig. 9. The peak at the threshold

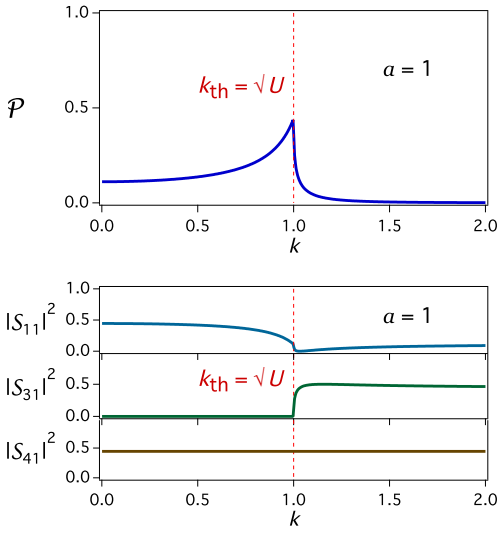


Fig. 9. Scattering characteristics of the graph from Fig. 8 with parameter $a = 1$. The transmission probability $\mathcal{P}(k;U)$ as a function of k with the value of the potential set to $U = 1$ is plotted in the top figure. The lower figure shows the reflection probability $|S_{11}(k;U)|^2$ and the probabilities of transmission to the controlling line $|S_{31}(k;U)|^2$ and to the drain line $|S_{41}(k;U)|^2$.

momentum $k_{\rm th} = \sqrt{U}$, appearing for $a > 1/\sqrt{2}$, is again related to the pole in the unphysical Riemann plane at

$$k_{\rm pol} = \frac{2a^2}{\sqrt{(4a^4-1)}}\sqrt{U}. \qquad (80)$$

There is a value of the parameter a that deserves a particular attention, namely $a = 1/\sqrt{2}$. For this choice of a, the peak disappears and the function $\mathcal{P}(k;U)$ becomes constant in the whole interval $(0, \sqrt{U})$;

$$\begin{aligned}\mathcal{P}(k;U) &= \frac{1}{4} \qquad (k \le \sqrt{U}) \\ &= \frac{1}{4}\left(\frac{1-\sqrt{1-\frac{U}{k^2}}}{1+\sqrt{1-\frac{U}{k^2}}}\right)^2 \qquad (k > \sqrt{U}). \end{aligned} \qquad (81)$$

The situation is evident in Fig. 10. This can be also regarded as the $a = 1/\sqrt{2}$ case of (35) considered in the section IV. Our device behaves as a spectral filter with a flat passband that transmits one fourth of quantum particles with momenta $k \in [0, \sqrt{U}]$ to the output, whereas particles with higher momenta are diverted to other lines, mainly to 3 and 4. The process is directly controlled by the external potential U. Note that, at this parameter value $a = 1/\sqrt{2}$, the scattering matrix without the external potential has the form

$$\mathcal{S} = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \end{pmatrix}. \qquad (82)$$

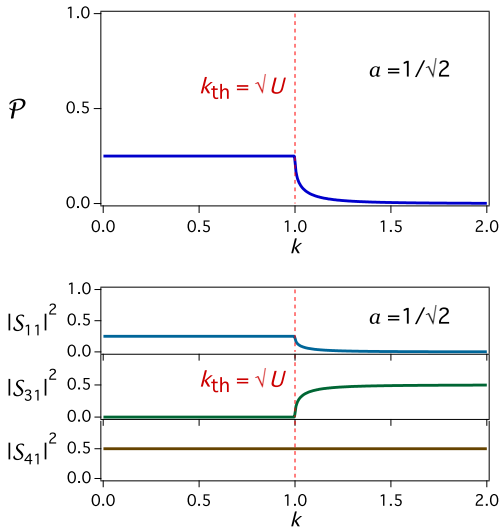


Fig. 10. Characteristics of the flat spectral filter obtained from the graph on Fig. 8 for $a = 1/\sqrt{2}$. The transmission probability $\mathcal{P}(k;U)$ as a function of k with the value of the potential set to $U = 1$ is plotted in the top figure. The lower figure shows the reflection probability $|S_{11}(k;U)|^2$ and the probabilities of transmission to the controlling line $|S_{31}(k;U)|^2$ and to the drain line $|S_{41}(k;U)|^2$.

Since increasing U opens the channel 1→2 for more particles, the device can be regarded as a *quantum sluice-gate*, applicable as a quantum flux controller (Fig. 11). When there are many particles described by the momentum distribution $\rho(k)$ on the line 1, the flux J to the line 2 is given by

$$J(U) = \int dk \rho(k) k \mathcal{P}(k;U)\,. \qquad (83)$$

Assuming the Fermi distribution with Fermi momentum k_F larger than our range of operation of $\sqrt{U}$, we can set $\rho(k) = \rho = \text{const}$. With the approximation $\mathcal{P}(k;U) \approx \frac{1}{4}\Theta(\sqrt{U}-k)$, we obtain

$$J(U) = \frac{1}{8}\rho U, \qquad (84)$$

which indicates the linear flux control.

The sluice-gate built from an $n = 4$ star graph has another possible mode of operation. We can apply another external field V which we assume to be in the range $0 < V < U$ to the line No. 4. The local momenta on lines 1 to 4 are given by

$$k_1 = k_2 = k, \quad k_3 = \sqrt{k^2 - U}, \quad k_4 = \sqrt{k^2 - V}. \qquad (85)$$

The system now has two threshold momenta given by

$$k_{\rm th1} = \sqrt{U}, \quad k_{\rm th2} = \sqrt{V}. \qquad (86)$$

For the incoming particles from the line 1, we obtain the scattering matrix in the form

$$\mathcal{S}_{21}(k;U) = \frac{-2a^2\left(\sqrt{1-\frac{U}{k^2}} - \sqrt{1-\frac{V}{k^2}}\right)}{\left(1+2a^2\sqrt{1-\frac{U}{k^2}}\right)\left(1+2a^2\sqrt{1-\frac{V}{k^2}}\right)}, \qquad (87)$$

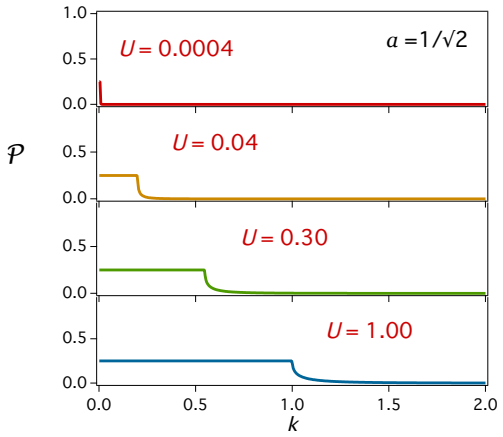


Fig. 11. The graph showing the sluice-gate operation of the quantum graph depicted in Fig. 8. The transmission spectra $\mathcal{P}(k)$ is plotted with various values of the control potential U.

$$\mathcal{S}_{11}(k;U) = \frac{1 - 4a^4\sqrt{1-\frac{U}{k^2}}\sqrt{1-\frac{V}{k^2}}}{\left(1+2a^2\sqrt{1-\frac{U}{k^2}}\right)\left(1+2a^2\sqrt{1-\frac{V}{k^2}}\right)}\,, \quad (88)$$

$$\mathcal{S}_{31}(k;U) = \frac{2a\left(1-\frac{U}{k^2}\right)^{\frac{1}{4}}\Theta(k-\sqrt{U})}{1+2a^2\sqrt{1-\frac{U}{k^2}}}\,, \quad (89)$$

$$\mathcal{S}_{41}(k;U) = \frac{2a\left(1-\frac{V}{k^2}\right)^{\frac{1}{4}}\Theta(k-\sqrt{V})}{1+2a^2\sqrt{1-\frac{V}{k^2}}}\,. \quad (90)$$

The channel 1→2 opens for particles with $k \in [k_{\rm th2}, k_{\rm th1}]$ and mostly closes for particles with k outside this interval (Fig. 12). The gate then works as a fully tunable band spectral filter. However, in contrast to the standard $V = 0$ operation mode, the filter with $V > 0$ does not have a flat passband.

We emphasize that the controllable filter using the threshold resonance is possible only with "exotic" Fulop-Tsutsui-type couplings in the vertices. Standard vertex couplings, namely the free and the δ-coupling, fail to work in this manner. It is essential, for the proposed designs to be experimentally realizable, that the required Fulop-Tsutsui vertices can be created using standard couplings, which themselves have a simple physical interpretation [15]. This problem has been addressed in [9] and [12], where it was proved that any Fulop-Tsutsui coupling given by b. c. with real matrices A, B can be approximately constructed by assembling a few δ-couplings. The solution for our case is shown in Fig. 13: For the $n = 3$ case (top), the δ-coupling strengths are given by $v_1 = [a(a-1) + b(b-1)]/d$, $v_2 = (1-a)/d$ and $v_3 = (1-b)/d$. For the $n = 4$ case (bottom), the strengths are $v_1 = v_2 = 2a(a-1)/d$, $v_3 = v_4 = (1-2a)/d$. The double line represents a line with a "magnetic" vector potential, which can be alternatively replaced by a line carrying the δ-coupling of strength $v_5 = -8a/d$ in its center, together with changing v_2 and v_4 to $v_2 = 2a(a-2)/d$, $v_4 = (1-4a)/d$.

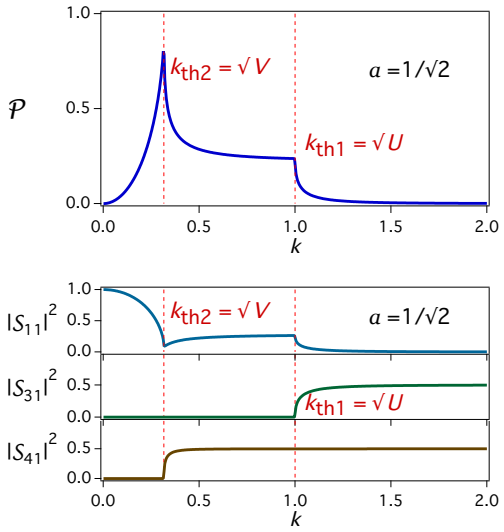


Fig. 12. Characteristics of the flat spectral filter obtained from the graph on Fig. 8 for $a = 1/\sqrt{2}$ and added second potential V on the 4th line. The transmission probability $\mathcal{P}(k;U)$ as a function of k with the value of the potentials set to $U = 1$ and $V = 0.1$ is plotted in the top figure. The lower figure shows the reflection probability $|S_{11}(k;U)|^2$ and the probabilities of transmission to the two controlling lines $|S_{31}(k;U)|^2$ and $|S_{41}(k;U)|^2$.

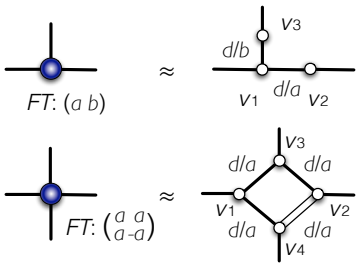


Fig. 13. Finite constructions of the Fülöp-Tsutsui couplings used. The design, based on [12], utilizes the δ-couplings connected by short lines. The small size limit $d \to 0$ with the δ-coupling strengths scaled with d effectively produces the required F-T vertex coupling.

VIII. Conclusion and Prospects

It has been shown, in this article, that the task of finding desired property of Flulop-Tsutsui graph can be turned into mathematical problem of identifying proper Hermitian unitary matrix. Naturally, the search of system with $\mathcal{S}$ having other interesting specifications should follow. Several questions arise along the line. One is the question whether we always have $\mathrm{tr}S = 0$ for systems with "exchange symmetric" $|S_{ij}|$. The generalization to complex $\mathcal{S}$ is also an interesting problem [16]. Other open questions include the generalization to non-Fulop-Tsutsui connection which yields general unitary $\mathcal{S}$ not limited to Hermitian ones. The study of the bound state spectra is one thing we have completely neglected in this work. Application to non-quantum waves, including electro-magnetic wave and water wave should be another interesting subject.

Through the finite construction of star graph with no internal lines, what we have shown, in fact, amounts to the study of the low energy properties of graphs with internal lines, all of

whose edges are connected to external lines. The examination of more complicated graphs, having purely internal lines, is the natural future direction.

The full solution to the inverse scattering problem and its use as a basis for filtering device, which we have shown in this article, amount to the partial fulfillment of the hope, that quantum graph could be a solvable model and useful design tool at the same time. The application of the quantum graphs we have considered here obviously is just a starting attempt, to which many follow-ups in the future should be expected.

ACKNOWLEDGMENT

This research was supported by the MEXT, Japan under the Grant numbers 21540402 and 24540412.

REFERENCES

[1] T. Cheon, *Reflectionless and equiscattering quantum graphs*, Proc. ICQNM 2011, Nice, France, 18–22 (2011).

[2] M. Harmer, *Inverse scattering on metrices with boundary conditions*, J. Phys. A: Math. Theor. **38**, 4875–4885 (2005).

[3] J. Boman and P. Kurasov, *Symmetries of quantum graphs and the inverse scattering problem*, Adv. Appl. Math. **35**, 58–70 (2005).

[4] B. Gutkin and U. Smilansky, *Can one hear the shape of a graph?* J. Phys. A: Math. Gen. **34** 6061-6068 (2005).

[5] P. Exner, J.P. Keating, P. Kuchment, T. Sunada, and A. Teplyaev, eds., *Analysis on Graphs and Applications*, AMS "Proceedings of Symposia in Pure Mathematics" Series, vol. 77, Providence, R.I., 2008, *and references therein*.

[6] T. Fülöp and I. Tsutsui, *A free particle on a circle with point interaction*, Phys. Lett. **A264**, 366–374 (2000).

[7] V. Kostrykin and R. Schrader, *Kirchhoff's rule for quantum wires*, J. Phys. A: Math. Gen. **32**, 595–630 (1999).

[8] T. Cheon, P. Exner, and O. Turek, *Tripartite connection condition for quantum graph vertex*, Phys. Lett. A **375**, 113–118 (2010).

[9] T. Cheon, P. Exner, and O. Turek, *Approximation of a general singular vertex coupling in quantum graphs*, Ann. Phys. (NY) **325**, 548–578 (2010).

[10] T. Cheon, P. Exner, and O. Turek, *Inverse scattering problem for quantum graph vertices*, Phys. Rev. A **83**, 062715 (4pp) (2010).

[11] P. Exner and O. Post, *Approximation of quantum graph vertex couplings by scaled Schrödinger operators on thin branched manifolds*, J. Phys. A: Math. Theor. **42**, 415305 (22pp) (2009).

[12] T. Cheon and O. Turek, *Fulop-Tsutsui interactions on quantum graphs*, Phys. Lett. **A 374**, 4212–4221 (2010).

[13] J.M. Harrison, U. Smilansky, and B. Winn, *Quantum graphs where back-scattering is prohibited*, J. Phys. A: Math. Theor. **40**, 14181-14193 (2007).

[14] O. Turek and T. Cheon, *Threshold resonance and controlled filtering in quantum star graphs*, arXiv.org: 1111.4775 (quant-ph) (4pp) (2011).

[15] P. Exner, *Weakly coupled states on branching graphs*, Lett. Math. Phys. **38**, 313–320 (1996).

[16] O. Turek and T. Cheon, *Quantum graph vertices with permutation-symmetric scattering probabilities*, Phys. Lett. A **375**, 3775-3780 (2011).

PCB Integration of Dye-sensitised Solar Cells for Internet of Things Applications

Jens Eliasson*, Jerker Delsing*, Simon J. Thompson†, Yi-Bing Cheng†, and Peter Chen‡
*Dept. of Computer science, space and electrical engineering
Luleå University of Technology, SE-971 87 Luleå, Sweden
Email: jens.eliasson@ltu.se
†Dept. of Materials Engineering, Monash University, Melbourne, Australia
Email: yibing.cheng@monash.edu
†Dept. of Photonics, National Cheng Kung University, Tainan, Taiwan
Email: petercyc@mail.ncku.edu.tw

***Abstract*—Internet of Things is envisioned to drastically chance the way sensor data from physical phenomena can be utilized by users on the Internet. However, one concern in deploying and maintaining a large number of sensor nodes is that replacing spent batteries will not be feasible. One solution to this issue may involve utilising energy harvesting technologies, e.g. solar, heat, or vibration, with solar being the most promising for general applications. However, using solar panels is currently a relatively expensive approach as they require a time-consuming and therefore costly assembly process. As an alternative, this paper suggests a new approach to powering networked sensors: the direct integration of a solar cell onto a sensor nodes printed circuit board. This approach eliminates the need for manual assembly and the use of expensive connectors.**

***Keywords*-Dye sensitised solar cells, energy harvesting, Internet of Things, wireless sensor networks**

I. INTRODUCTION

This paper, based on previous work from Eliasson et al. [1], presents new results and outlines application areas for the proposed approach. A wireless sensor and actuator network (WSAN) is composed of a large number of heterogeneous sensor nodes, or *sources*, that both sense phenomena in the physical world but also provide some control of the physical world [2]. A wireless sensor and actuator network also includes one or several gateways, or *sinks*, which forward sensor data from nodes in the internal network to an external network [3]. Research on WSAN technology originally focused on military applications, such as battlefield surveillance, land mine detection, and soldier monitoring [4]. Current wireless sensor network research is additionally motivated by an increasing number of civil usage scenarios, such as environmental and habitat monitoring, seismic and volcanic monitoring, structural monitoring, and industrial applications [5], [6].

Wireless sensors are expected to have a drastic impact on how measurements of the physical world will be presented to users on the Internet [7]. A vision, in which Internet-connected wireless sensors are deployed in the vicinity of users, named *the Internet of Things* [8] is also projected to enhance both safety and quality of life for future generations. For this vision to be realized, a number of issues must be resolved. Two of these issues, addressed by this paper, are:

- Enabling wireless power
- Lowering the cost of the sensor nodes

Reducing power consumption can be achieved using a number of methods, such as using more efficient components, integrating more intelligent routing protocols [9], or developing energy-aware computing. Wireless power requires power harvesting, power storage, and an appropriate power usage architecture at the sensor node; see for example [10], [11], [12]. A node's cost will be reduced with the use of more integrated components, and the price of printed circuit boards (PCB), integrated circuits (ICs), and other components will drastically decrease with increased production volumes. However, the costs of certain node components, such

as batteries and power supplies, do not scale as effectively as circuit board production volumes. The cost of packaging a complete node with a circuit board, batteries, solar panels, and enclosure will not be reduced by the same order of magnitude as that of the electronics. This is a major obstacle for realizing the vision of massive wireless sensor networks.

This paper presents a novel approach aimed at further reducing manufacturing and integration cost for solar cells for powering wireless sensor nodes. The approach is to manufacture a solar panel directly onto a sensor node's circuit board, thus reducing the cost of manufacturing the cell separately and eliminating the assembly cost. This has several benefits, as the resulting device consists of an integrated solution that effectively eliminates cables and connectors, and an additional integration step. The proposed approach also increases the system's robustness because there are no connectors or cables that can disconnect due to mechanical phenomena, e.g., vibrations or impacts. The ultimate aim of this research is to develop a holistic method for producing complete low-power systems, where assembly of the PCB, components, and an energy-harvesting device can be completed as a single process. The first steps have been taken - we have integrated a solar cell module with a PCB - and the authors envision that, in the future, a solar cell can be directly printed on a PCB using sequential build-up (SBU) techniques. For example, Blackshear et al. reported in 2005 [13] the advantages of using SBU for chip assembly onto circuit boards.

The paper is outlined as follows: this section has presented related work and a background of wireless sensor networks and solar cell technologies. The next two sections give an overview of some related work, application areas, and DSCs. Section V presents the new method of integrating a DSC directly onto a circuit board, and Sections VI and VII show the experimental setup, and results from real-world tests, respectively. Finally, conclusions and suggestions for future work are presented in Section VIII.

II. Related work

One consideration for energy harvesting relates to the energy density from different sources. It is clear that solar cells are superior to other energy harvesting approaches such as vibrations and thermoelectric power, as reported by Yang et. al [10]. When comparing different solar cell technologies, both power efficiency and cost must be considered. Two main candidate technologies: silicon based solar cells and dye sensitised solar cells (DSC), sometimes called Grätzel cells [14], have been selected for further investigation. A comparison between silicon based solar cells and DSC can be found in [15]. Regarding energy capability a traditional silicon-based solar cell offers about $43mA/cm^2$ at 0.7V, whereas current DSCs offer about $22mA/cm^2$ at about 0.6V [16]. Regarding cost, DSCs have potential to be lower cost due both cheaper feedin materials and inexpensive manufacturing techniques.

In [17], Usman showed by simulation that the use of DSC technology in close integration with modern electronics, i.e. PCB integration, is an interesting technology and emerging trend. In [1], Eliasson et al. showed the world's first working prototype of a device where a PCB and a DSC cell was successfully integrated. This paper further elaborates on application areas where this is feasible, and extends the conclusions by supplying new measurements and results.

III. Areas of application of proposed approach

The use of energy scavenging in real-world applications is becoming more and more common. By harvesting energy in the form of solar, wind, vibration, heat, etc, the need to replace or charge drained batteries can be avoided. In some cases, for example industrial applications, changing batteries might not be feasible due to a hazardous environment. Below are three different sensor networking applications identified, with their characteristics:

A. ITS

Intelligent transport systems (ITS) are believed to be an important tool for tomorrow's road infrastructures. ITS can help reducing the traffic's carbon dioxide foot print, improve safety and increase the traffic flow. ITS systems are usually composed of three main components: sensors for vehicle detection, actuators for informing drivers, and a back-end system. Sensors for vehicle detection are used to feed the back-end system with information about the traffic, with number of vehicles, thier speed, etc.

Vehicle detection has traditionally been performed using magnetic sensors, cameras, lasers and other expensive and power consuming devices. A road surface network (RSN) is a new type of ITS solution, where low-cost sensors are deployed directly onto a road's surface. This enables vehicle detection and classification, not only in cities, but also in rural areas. Since the sensors are solar-powered, there is no need for installing power cables, which further reduces the installation cost. The use of a wireless sensor and actuator network (WSAN), as suggested by Hostettler et al. [18] enables new possibilities of how modern, solar-powered electronics can be embedded in the physical world. The iRoad project [19] conducted at Luleå University of Technology aims at developing these types of systems. In these types of devices, it is important that both component and assembly costs are minimized.

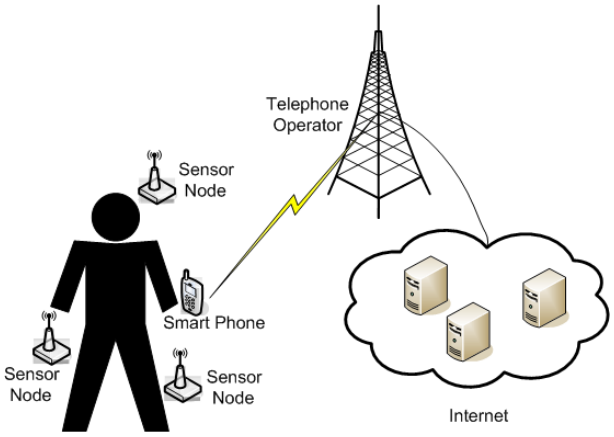


Fig. 1. Body area network

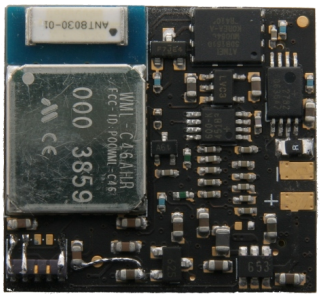


Fig. 2. Mulle v3.1 Embedded Internet System (EIS)

B. Healthcare

Most western countries have an aging population. This will drastically increase costs for each country's healthcare and elderly care systems. Using for example e-Health, where electronics and ITS systems [20] are used as tools for reducing healthcare costs, travel costs and increase the quality of life. With e-Health, people which can be treated in the comfort of their own homes can have the option to do so, thus minimizing hospital time. However, this requires that some sort of monitoring be used. With the use of (wireless) sensors, patients can have their medical status monitored remotely while maintaining mobility, and if some anomaly is detected by an e-Health device, an alarm or alert can be transmitted to the hospital. Figure 2 shows an example of an Internet-connected sensor platform, i.e. the Mulle. The Mulle is a low-power sensor node, measuring only 24x26x4 mm. This small size combined with the Mulle's support for Internet communication, enables the Mulle to be well suited for use on patients or elderly. The Mulle can be equipped with GPS, heart rate monitor, fall sensors, motion sensors and other types of sensors that can be used to monitor patients. Figure 1 shows a Body area network (BAN) architecture capable of monitoring various medical properties such as body temperature, posture, pulse, location, physical activity, etc. A number of sensor nodes would be deployed on a human user, and use the patients mobile phone to transmit sensor information to backend-systems for data analysis and alarm generation.

In e-Health applications, users expect not to change drained batteries more than a few times per year. If an e-Health device must be recharged daily or weekly, people will simply not use it, or forget to charge it resulting a health hazard. Therefore, e-Health devices must be very low power, and optionally use energy scavenging in order to prolong system lifetime. The Mulle's sleep current consumption is only 4 μA, which enables it to be used in combination with (solar) energy scavenging, as shown in [12].

One aspect of e-Health applications is that the users will spend a substantial time indoors. It is therefore beneficial if the solar panel used to power the sensor and actuator devices can provide some power output even in low light conditions i.e. from lamps and ambient sun light.

C. Home automation

Home automation using wireless sensor and actuator networks have the possibility to reduce energy

usage [21] and thus CO_2 emissions [22], increase safety and security while enhancing the users quality of life. By enabling different systems to exchange information and thus allow fine control of heating, ventilation, lighting etc, substantial savings can be accomplished. As an example, the building's security system can inform other systems that no one is present. Heating and ventilation can then be reduced, lighting switched off etc. Temperature sensors outdoors and indoors can help ensure that a comfortable temperature is provided in each individual room. Smart appliances, such as washing machines, can start during night when the electricity is cheap.

IV. Dye sensitised solar cells

The dye sensitised solar cell (DSC) is currently being investigated as a low cost method of harvesting the abundant energy of sunlight into electricity [14]. It offers the possible advantages of low cost and better light harvesting in low and/or diffuse lighting, which are more realistic conditions than those which are optimal for other photovoltaic devices, such as silicon-based cells.

The DSC operates by light exciting an electron in a dye molecule adsorbed onto a mesoporous semiconductor to an energy level above the conduction band of the semiconductor. The electron is quickly transferred to the conduction band of the semiconductor and transported through the network of interconnected nanoparticles to the electrode. The electron passes through the external circuit and then reduces an electrolyte at the counter electrode which in turn reduces the dye, returning it to its ground state. This type of solar cell has exhibited an efficiency of over 11 %, as shown by Han et. al [23]. The operation of the DSC allows for cheap, abundant materials to be used for device components, combined with less energy-intensive processes used during manufacture. This offers the potential for significantly lower production costs compared to more traditional silicon solar cells, in turn reducing the energy and cost payback times significantly. These factors make the DSC an attractive renewable energy source for the future.

The drawbacks for DSCs are, lower performance compared to silicon devices and a corrosive volatile electrolyte that limits material selection options and shortens device lifetimes. The most problematic of these is device lifetime, as it is difficult to construct devices with long lifetimes when encapsulation of a volatile, corrosive electrolyte is required. To this end alternative electrolytes have been investigated - generally highly viscous, non-volatile ionic liquids. Solid state hole conductors have also been considered and are a more elegant solution, as they also remove corrosive iodine from the system, expanding materials selection options within the cell as well as eliminating any solvent leakage issues, due to being a solid. The leading organic hole conductor is 2,2,7,7-tetrakis(N,N-di-p-methoxypheny-amine)-9,9-spirobifluorene (spiro-MeOTAD) [24], with reported device efficiencies up to 7.2% [25]. A solid state device is typically constructed onto fluorine doped tin oxide (FTO) glass with a titania (TiO_2) layer coated on top, which is dyed and then infiltrated with the hole conductor. The counter electrode is a gold layer evaporated onto the coated titania layer and connected to an electrically isolated section of the FTO glass. This architecture is ideal for integration with circuit boards, which has been realised by the authors and is shown in Figure 3. The circuit board was physically contacted to the gold contacts on the back of the DSC module, as shown in Figure 5. The connections was made such that each cell is independently measurable and thus can be bipassed if necessary, e.g. due to damage or during cell characterization.

V. PCB with integrated dye sensitised solar cell

DSC modules were created here using the screen printing technique, on pre-etched 100 mm $\times$ 100 mm 13 Ω/square FTO coated conducting glass (Nippon) masterplates. The etching to separate the contacts for the individual cells was performed using a laser engraving system, a Versa laser VL3.50 unit, which produced fine lines ($\sim$150μm) with high spacial precision. Following this procedure the glass was cleaned and a dense blocking layer of TiO_2 was deposited by spray pyrolysis, with the areas for electrical contacts by solder or the gold layer being masked by flattened aluminum rods.

The screen printing paste for the active layer contained 18 nm particles of anatase titania (obtained from JGC Catalysts and Chemicals Ltd) and was diluted by terpineol at a ratio of 2:1 paste (Fluka). The thickness of the titania layer was determined

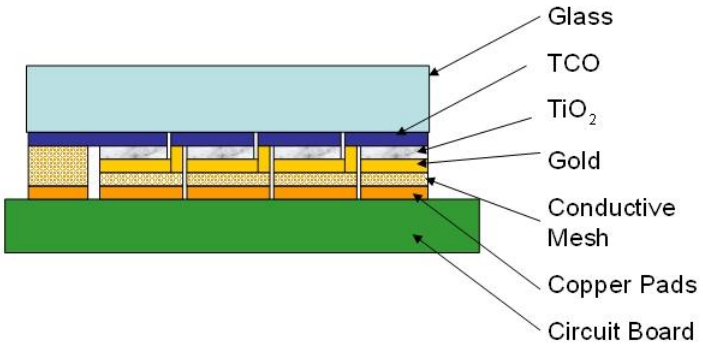


Fig. 3. Layout of the PCB with integrated dye-sensitised solar cell

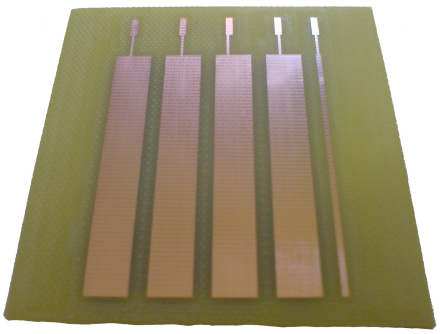


Fig. 4. Prototype board layout

by a Veeco Detak 150 stylus profilometer, to be $\sim$2 μm. The titania layer was incrementally heated to 450°C for 30 min and then to 500°C for 15 min. The master plates were cut into 50 mm $\times$ 50 mm modules and reheated to 500°C for 30 mins before being placed into the dye solution of 30 mM Z907 (Dyesol) in an acetonitrile/tert-butanol 1:1 mixture. for approximately 24 hours. The electrolyte was a solid state hole conductor, namely Spiro-MeOTAD, which was deposited by spin-coating using a solution that consisted of 180mg/mL of Spiro-MeOTAD (Merck) in chlorobenzene (Sigma) with additives of 4-tertbutylpyridine (TBP) (Sigma) (17.6ul/mL) and Li-TFSI (Sigma) (19.5mM). Chlorobenzene was used on a cotton bud to remove excess Spiro-MeOTAD from the glass were series interconnects were to be formed. The gold charge collecting layer was deposited onto the module via thermal evaporation, and the areas not to be coated with gold were masked with Kapton tape^{TM} (3M).

An attempt was made to integrate these devices onto a PCB using conductive epoxy however, this had a detrimental effect on the DSC leading to dye desorption. Therefore, this approach was abandoned in favour of using a soft compressible conductor. The material used was a polymer mesh substrate with copper deposited onto it. The copper mesh was cut into pieces of the same width as the pads, but slightly longer such that they could be laid over the pads and adhered using Kapton tape. The module was placed on top of the PCB such that the gold contacted the copper mesh and no shorting occurred between cells. The PCB and DSC module where then clipped into place using bulldog clips. During these alignment and clipping processes care was taken not to damage the fragile gold layer. Wires

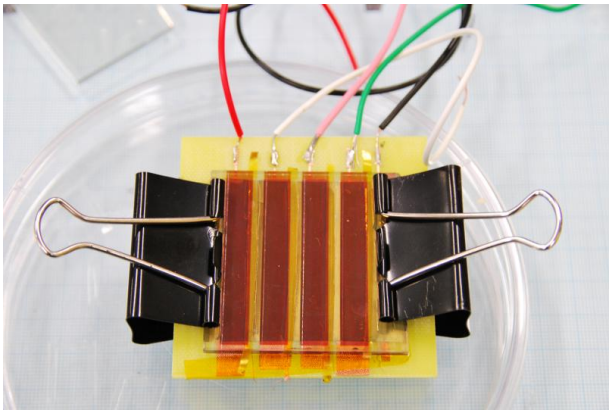


Fig. 5. PCB DSC solar panel prototype board, ready for integration with sensor node, the DSC module is 50 mm $\times$ 50 mm

were soldered onto the board such that the entire module could be used or individual cells could be measured and/or bypassed if faulty. Figure 4 shows the PCB that serves as the base for the new solar cell. The board, which is composed of four copper stripes each 49 mm wide and 6 mm long, was manufactured using a milling machine from an Eagle CAD design. In the next version of this prototype board, a modern maximum power point tracker (MPPT) will be integrated in the system. By using a MPPT, the cell's power output can be increased up to 15-20% [26].

Figure 5 shows a board produced with a DSC on a PCB. The module created was tested before and after integration with the PCB, using alligator clips to make the electrical connections for tests prior to the connection to the PCB was made, with wires soldered to the PCB used after connection. The module was also tested 5 months after construction. During storage the cell was placed in a drawer in ambient atmosphere and generally in the dark.

VI. Experimental setup

Several experiments were performed to investigate the performance of the PCB-based cell. To evaluate the performance of the module under standard conditions a solar simulator was used. The modules were tested under 1 Sun illumination, 100 mWcm^{-2} AM1.5G, using a 1000 W solar simulator xenon lamp (Oriel) fitted with an appropriate filter to achieve spectral match and a Keithley 2400 source meter. Illumination intensity was varied by the use of fine wire mesh and calibrated using a silicon diode. The active area was 10.5 cm^2, while the size of the glass was 25 cm^2, this shows a poor active area to device area ratio. In future work will attempt to increased this to over 90% coverage, as a challenging, yet achievable, target for an interconnected module of this size. No masking was used; efficiencies may therefore be over estimated due to light piping within the glass.

To investigate the real world performance and feasibility for practical use, tests were performed both indoors and outdoors using different light sources.

A. Measurement system

A measurement system was created to capture characterization measurements for the PCB solar cell. The measurement system, shown in Figure 6, consists of a 24-bit analog-to-digital converter (ADC) that measures the voltage drop over a 5Ω resistor, which is used to measure current. To obtain an I-V curve, a digitally programmable potentiometer was also used so that different loads could be presented to the cell. A Mulle v3.1 networked sensor node equipped with a Bluetooth 2.0 transceiver was connected to the measurement system. Using this approach, the PCB cell can be tested outdoors by having a wireless connection to a laptop or PC, which can be placed indoors. The measurement system will be used also to measure the temperature dependency of the cell during winter tests. In addition, the measurement system also serves as a building block in the power supply unit (PSU) that may be used together with the PCB-cell. The PSU includes a boost converter that generates a 5.0V output used to charge a super capacitor. A switch is used to select whether the Mulle should be powered by the super capacitor or by a battery. The Mulle v3.1 also features a battery monitor chip, capable

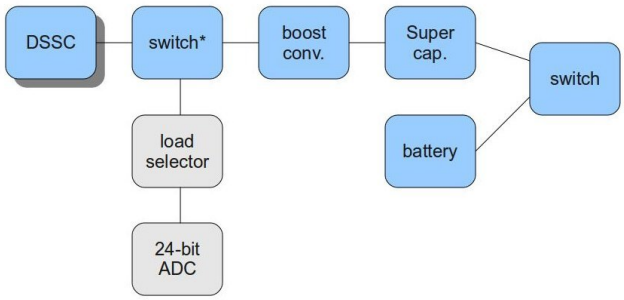


Fig. 6. Measurement system overview

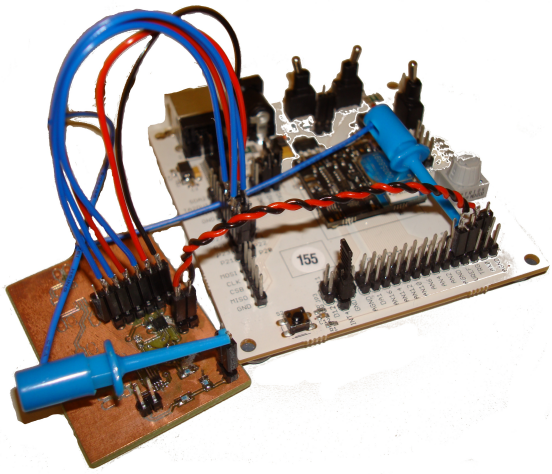


Fig. 7. Measurement system implementation

of measuring battery voltage, power consumption, available energy, and estimated lifetime. Combined with the Mulle's on-board features, the PSU can enable true energy- and power-aware operation.

Figure 6 shows the measurement system. The system can measure voltages up to 6.5V, and current with a resolution around 20μA. The load can be programmed to any value between 100Ω and 100kΩ in 256 steps. Its realisation is shown in Figure 7.

The measurement system is completely wireless, which allows remote monitoring of the PCB cell. A dedicated software written in C was used to retrieve data from the Mulle and store the results to file on a computer.

B. Performed measurements

The following experiments were performed in order to test the cell's performance under in a real-world setting. The different tests that the cell was tested in are typical application locations where a networked embedded system can be deployed.

TABLE I
MULLE V3.1 CURRENT CONSUMPTION

Mode	Delay	Current
All systems sleep	-	0.004 mA
MCU 10.0 MHz, BT off	-	7.6 ma
MCU 5.0 MHz, BT off	-	5.1 mA
MCU 2.5 MHz, BT off	-	3.1 mA
MCU 1.25 MHz, BT off	-	2.2 mA
MCU sleep, BT listen	2-12 s.	1.0 mA
MCU sleep, BT active	-	40.3 mA
MCU sleep, BT sniff (210 slots)	131 ms.	8.4 mA
MCU sleep, BT sniff (2010 slots)	1256 ms.	2.8 mA
MCU sleep, BT parked (18 slots)	13 ms.	7.5 mA
MCU sleep, BT parked (200 slots)	130 ms.	2.7 mA
MCU sleep, BT parked (4094 slots)	2560 ms.	1.8 mA

1) Measurement of the PCB DSC module's performance initially and after 5 months
2) Measurement of the PCB DSC's current response at various light incident angles
3) Measurement of the effect of varying light intensity on the current output of the PCB DSC module.
4) Tests of power generation at indoor and outdoor locations and different lighting conditions

The cell was tested for long term degradation effects and different light sources at different angles. However, no temperature tests were performed during the work.

C. Real-world energy usage

The feasibility of using the prototype solar cell, with the power characteristics presented in the previous section, for a real-world networked sensor is presented here. The Mulle node [27] has been used in a number of WSAN and BSN applications [28], which will be used as an example for calculating operational lifetimes when combined with the PCB cell. Table I shows examples of the current consumption of a Mulle v3.1 in different operating modes.

VII. RESULTS

The initial performance of the PCB DSC module was 1.4% prior to integration with the PCB, and was improved to 1.5% after integration. The performance degraded to approximately 1% after 5 months, as shown in Figure 8. It can be seen that integration with the PCB has improved device performance by increasing the short circuit current, although this could be partially explained by a change in the testing methodology, brought about by how the module is placed under the light beam due to the bulky PCB causing the device to be placed in a slightly different position in the light beam. The improvement in the electrical connection of the module to the testing apparatus by connection to the PCB would also account for some of the improvement, with sections not previously in electrical connection due to breaks or scratches in the gold layer being connected via the PCB. It is also possible that the increase in current is due to reflection from the metal surfaces associated with integration with the PCB. The overall device performance is not high, but as a prototype solid-state module it has sufficient performance to be a starting point for considering future applications. Over the course of 5 months it can be seen that the performance of the DSC module decreased by about 30%, which is quite good for a DSC with no encapsulation and stored under open circuit conditions in ambient atmosphere. The short circuit current reduction over the time was most likely due to the degradation of the dye molecules through interaction with atmospheric water, which may also explain the reduced fill factor as the water will have also degraded the Spiro-MeOTAD thus increasing series resistance.

Varying illumination angle was performed by the use of a rotating stage with a 360° protractor attached to its center to determine the angle. The modules were attached to the center of the freely rotating protractor and a mark on the board was used to determine the incident angle, where 0° corresponds to the light beam from the solar simulator being perpendicular to the surface of the module. A spirit level was used to determine when the modules were perpendicular to the light beam and all other angles were calculated from this calibration. From the data in Figure 9 the DSC module appears to have a reasonably low angular dependence, following the cosine law [29], where the cosine of the angle of illumination predicts the fraction of current being produced compared to perpendicular for collimated light sources such as the sun, due to its distance, or nominally the solar simulator. Comparing the experimental results with the cosine law shows that the currents produced are higher than expected for the DSC module. Possible reasons for this are, as the modules were rotated half approaches the light source, if the light beam is not properly collimated

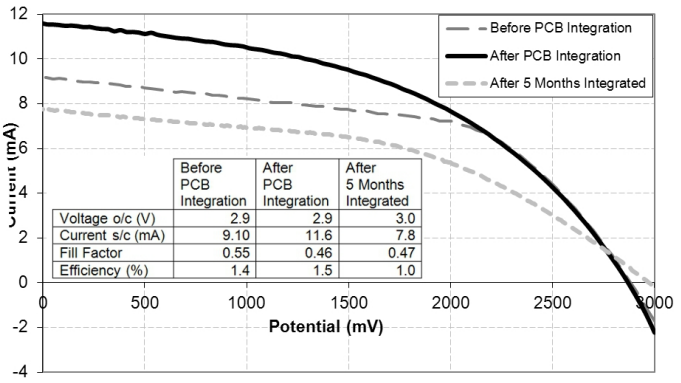
then the light will have higher intensity for the closer portion and thus the current will increase, alternatively it could be due to light piping effects through the glass from the edge of the device (4 mm) playing a role in capturing more light into the device. The important point to take from this experiment is that at 45° the DSC still produced about 80% output current, which shows for most of a given day the DSC will be performing with relatively good output regardless of the angle of incidence of solar illumination. The silicon module follows the theoretical curve more closely until around 60°, where it begin to perform below the curve. The comparison of these devices shows that the DSC has a lower angular dependence than the silicon module tested here, thus demonstrating a possible advantage for this technology for use in sensor nodes.

Figure 10 shows the variation of the output current with varied input light intensity, which remains linear for lower light intensities, but slightly decreases upon approaching full illumination, showing the cell is approaching it's photocurrent limit. This limiting would not be an issue for real world applications where the input light intensity would generally be lower than the standard 1 sun considered here, and in the context of Mulle sensor nodes then times of peak light intensity will typically be uninteresting as the device should have had the opportunity to fully charge by the time this level of irradiation is present. Meaning that the device will likely be charged during the morning before the peak light of the day in an outdoor application. This data may also be used to estimate the illumination intensity from the photocurrent produced by the module although this will exhibit a significant spectral mismatch for artificial light sources.

To evaluate the module's output in real world scenarios the short circuit current was measured at a number of locations that reflect typical applications for the sensor node which can be placed either outdoors or indoors.

The resulting data is in Table III. For a number of practical usage scenarios assuming no real-time radio communication, a small dye solar cell should be sufficient to provide the necessary power for making low-cost wireless power a reality.

When comparing the current output from the PCB DSC cell with Table I, it is clear that the generated current is sufficient for powering a Mulle sensor node as long as low-power modes are utilized. Since the peak power of a Mulle is higher than the maximum power output of the PCB DSC cell, some energy storage will always be required. A super capacitor, a rechargeable battery, or a combination of both can be used for energy storage. Performed



	Before PCB Integration	After PCB Integration	After 5 Months Integrated
Voltage o/c (V)	2.9	2.9	3.0
Current s/c (mA)	9.10	11.6	7.8
Fill Factor	0.55	0.46	0.47
Efficiency (%)	1.4	1.5	1.0

Fig. 8. PCB DSC current-voltage performance, initially and after 5 months

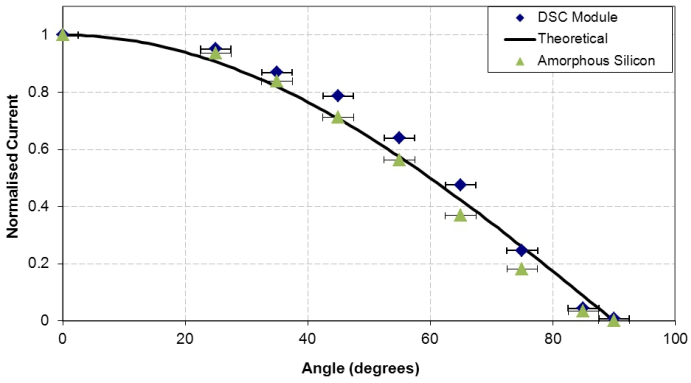


Fig. 9. PCB DSC short circuit current response for different light incident angles

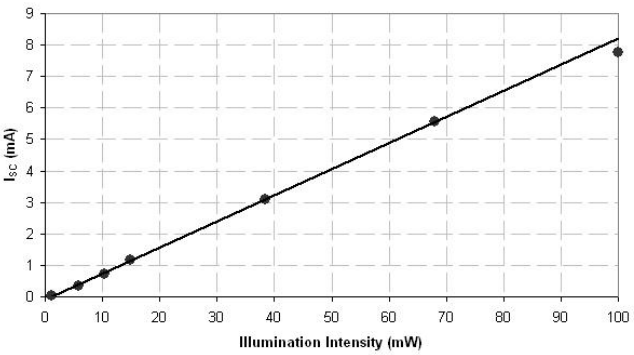


Fig. 10. Short circuit current response for the PCB DSC with light intensity varying between 1 and 100%

TABLE II
TEST LOCATIONS

ID	Description
1	Office with ceiling fluorescence lightning and ambient light from shaded windows; cell horizontal
2	Corridor with ceiling fluorescence lightning and no ambient light from windows, cell horizontal
3	Workshop well lit with with ceiling fluorescence lightning and some ambient light from shaded windows; cell horizontal
4	Office desk with 23W desk fluorescent lamp; cell horizontal
5	Near a closed window with no direct sunlight; cell horizontal
6	Near an open window with no direct sunlight; cell horizontal
7	Near a closed window with some direct sunlight; cell horizontal
8	Near a closed window with direct sunlight; cell horizontal
9	Near a closed window with no direct sunlight; cell tilted for maximum illumination
10	Outside in full sun light; cell horizontal
11	Outside in full sun light; cell tilted for maximum illumination

TABLE III
CURRENTS FROM PCB DYE SOLAR CELL IN TYPICAL USAGE SCENARIO LOCATIONS.

Test location	distance to source [m]	Current [μA]
1	2	6
1	0.3	60
1	0.1	220
2	1	6
2	0.1	90
3	2	50
4	0.2	240
4	0.01	3000
5	-	220
6	-	330
7	-	800
8	-	2650
9	-	3700
10	-	6800
11	-	8000

tests indicates that the presented approach is feasible for powering low-power electronics such as sensor nodes.

VIII. CONCLUSION AND FUTURE WORK

This paper has presented a novel approach for powering low-power electronic devices, such as networked embedded systems and sensor nodes. The approach integrates a dye sensitised solar cell directly onto a device's circuit board thereby reducing the material and assembly costs. A prototype device has been manufactured to demonstrate the feasibility of this approach and to enable the cells' real-world performance to be evaluated. Test results, both initial and after five months of degradation, have been presented to support the claims. Note that the performed tests only show the feasibility of the system, more tests are needed in order to fully characterize the cell's true performance.

By integrating the power supply directly onto a circuit board, the authors envision that networked sensors may be manufactured at a greatly reduced cost in the future. When combined with new technologies for energy storage and transparent encapsulation, the presented approach can be an enabling technology for future low-cost, large-scale wireless sensor networks, in support of the vision of *the Internet of Things*.

The first steps towards an integrated manufacturing process for solar-powered embedded systems have been successfully completed. The authors are now working on techniques to print a dye sensitised solar cell directly onto a printed circuit board using mass production techniques. The ultimate aim is to develop a method for assembling and manufacturing a complete system that includes a PCB, components, and a solar cell, using a single process.

Another issue that needs further investigation is how the system should be encapsulated in a transparent package. One method is to the embedd the entire system in optically transparent glue, as shown in [30]. How low temperatures are affecting the cell's performance must also be investigated. Finally, the use of a more low powered device, such as the Mulle v5.2 with an IEEE 802.15.4 radio, combined with a maximum power point tracker (MPPT) should be used to test the true performance in a wireless sensor and actuator network used in for example ITS applications, e-Heath or smart homes.

ACKNOWLEDGMENTS

Parts of this work have been conducted within the iRoad project that is hosted at Luleå University of Technology. Funding provided by Geveko ITS A/S, the Gunnar och Märtha Bergendahl foundation and VINNOVA are hereby gratefully acknowledged. The authors would like to thank Mikael Larsmark for help with the manufacturing of the circuit boards.

REFERENCES

[1] J. Eliasson, J. Delsing, S. Thompson, and Y.-B. Cheng, "PCB Integration of Dye-sensitised Solar Cells for Low-cost Networked Embedded Systems," in *SENSORCOMM*, Nice, France, July 2011.

[2] D. Culler, D. Estrin, and M. Srivastava, "Overview of sensor networks," *Computer*, vol. 37, no. 8, pp. 41–49, Aug 2004.

[3] Özgür B. Akan and I. F. Akyildiz, "Event-to-sink reliable transport in wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 13, no. 5, pp. 1003–1016, 2005.

[4] T. Bokareva, W. Hu, S. Kanhere, B. Ristic, N. Gordon, T. Bessell, M. Rutten, and S. Jha, "Wireless sensor networks for battlefield surveillance," 2006. [Online]. Available: http://www.cse.unsw.edu.au/~tbokareva/papers/lwc.html

[5] N. Xu, S. Rangwala, K. K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, and D. Estrin, "A wireless sensor network for structural monitoring," in *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*. New York, NY, USA: ACM, 2004, pp. 13–24.

[6] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring," in *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*. ACM Press, 2002, pp. 88–97.

[7] "IPSO Alliance," http://www.ipso-alliance.org/, 2010, [Online; accessed 11-June-2012].

[8] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.05.010

[9] K. Zeng, K. Ren, W. Lou, and P. J. Moran, "Energy aware efficient geographic routing in lossy wireless sensor networks with environmental energy supply," *Wireless Networks*, vol. 15, pp. 39–51, Jan 2009.

[10] R. Moghe, Y. Yang, F. Lambert, and D. Divan, "A scoping study of electric and magnetic field energy harvesting for wireless sensor networks in power system applications," in *Energy Conversion Congress and Exposition, 2009. ECCE 2009. IEEE*, sept. 2009, pp. 3550 –3557.

[11] V. Raghunathan, A. Kansal, J. Hsu, J. Friedman, and M. Srivastava, "Design considerations for solar energy harvesting wireless embedded systems," *IPSN '05: Proceedings of the 4th international symposium on Information processing in sensor networks*, vol. 64, p. 64, 2005, cited By (since 1996): 9. [Online]. Available: www.scopus.com

[12] J. Eliasson, P. Lindgren, J. Delsing, S. Thompson, and Y.-B. Cheng, "A power management architecture for sensor nodes," in *Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE*, march 2007, pp. 3008 –3013.

[13] E. Blackshear, M. Cases, E. Klink, and S. Engle, "The evolution of build-up package technology and its design challenges," *IBM journal of research and development*, vol. 49, pp. 641–661, 2005.

[14] B. O'Regan and M. Grätzel, "A low-cost, high-efficiency solar cell based on dye-sensitized colloidal tio2 films," *Nature*, vol. 353, no. 6346, pp. 737–740, 1991.

[15] B. A. Gregg and M. C. Hanna, "Comparing organic to inorganic photovoltaic cells: Theory, experiment, and simulation," *Journal of Applied Physics*, vol. 93, no. 6, pp. 3605–3614, 2003. [Online]. Available: http://link.aip.org/link/?JAP/93/3605/1

[16] M. A. Green, K. Emery, Y. Hishikawa, and W. Warta, "Short Communication Solar cell efficiency tables," *Progress in Photovoltaics: Research and Applications*, vol. 17, 2009.

[17] M. A. U. Usman, "Integrating dye-sensitized solar cell technology for implementation in modern day electronics," in *SOLAR 2010 Conference Proceedings*, Piscataway, NJ 08855-1331, United States, 2010.

[18] R. Hostettler, W. Birk, and M. Nordenvaad, "Feasibility of road vibrations-based vehicle property sensing," *Intelligent Transport Systems, IET*, vol. 4, no. 4, pp. 356 –364, December 2010.

[19] "The iRoad project," http://www.iroad.se, April 2011, [Online; accessed 19-May-2012].

[20] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The internet of things for ambient assisted living," in *Information Technology: New Generations (ITNG), 2010 Seventh International Conference on*, april 2010, pp. 804 –809.

[21] O. Asad, M. Erol-Kantarci, and H. Mouftah, "Sensor network web services for demand-side energy management applications in the smart grid," in *Consumer Communications and Networking Conference (CCNC), 2011 IEEE*, jan. 2011, pp. 1176 –1180.

[22] N.-H. Nguyen, Q.-T. Tran, J.-M. Leger, and T.-P. Vuong, "A real-time control using wireless sensor network for intelligent energy management system in buildings," in *Environmental Energy and Structural Monitoring Systems (EESMS), 2010 IEEE Workshop on*, sept. 2010, pp. 87 –92.

[23] L. Han, A. Fukui, N. Fuke, N. Koide, and R. Yamanaka, "High efficiency of dye-sensitized solar cell and module," in *IEEE 4th World Conference on Photovoltaic Energy Conversion*. IEEE, 2006, pp. 179–182.

[24] U. Bach, D. Lupo, P. Comte, J. E. Moser, F. Weissortel, J. Salbeck, H. Spreitzer, and M. Grätzel, "Solid-state dye-sensitized mesoporous tio2 solar cells with high photon-to-electron conversion efficiencies," *Nature*, vol. 395, pp. 583–558, 2009.

[25] J. Burschka, A. Dualeh, F. Kessler, E. Baranoff, N.-L. Cevey-Ha, C. Yi, M. K. Nazeeruddin, and M. Grtzel, "Tris(2-(1h-pyrazol-1-yl)pyridine)cobalt(iii) as p-type dopant for organic semiconductors and its application in highly efficient solid-state dye-sensitized solar cells," *Journal of the American Chemical Society*, vol. 133, no. 45, pp. 18 042–18 045, 2011. [Online]. Available: http://pubs.acs.org/doi/abs/10.1021/ja207367t

[26] F. Simjee and P. Chou, "Efficient charging of supercapacitors for extended lifetime of wireless sensor nodes," *Power Electronics, IEEE Transactions on*, vol. 23, no. 3, pp. 1526 –1536, may 2008.

[27] "Eistec AB," http://www.eistec.se, 2010, [Online; accessed 11-June-2012].

[28] J. Eliasson, P. Lindgren, and J. Delsing, "A Bluetooth-based Sensor Node for Low-Power Ad Hoc Networks," *Journal of Computers (JCP)*, pp. 1–10, May 2008.

[29] J. Balenzategui and F. Chenlo, "Measurement and analysis of angular response of bare and encapsulated silicon solar cells," *Solar Energy Materials and Solar Cells*, vol. 86, no. 1, pp. 53 – 83, 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S092702480400265X

[30] J. Eliasson and W. Birk, "Towards road surface monitoring: Experiments and technical challenges," in *Control Applications, (CCA) Intelligent Control, (ISIC), 2009 IEEE*, july 2009, pp. 655 –659.

Electro-Magnetic Modeling and Design of Through Silicon Vias Based Passive Interposers for High Performance Applications up to the V-Band

Olivier Tesson[1,2]
[1]NXP Semiconductors,
PCC RF Small Signal ICRF
Campus Effiscience, Colombelles
14906 Caen Cedex 09, France
[2]LAMIPS,
Laboratoire commun NXP-CRISMAT
UMR 6508 CNRS ENSICAEN UCBN
Olivier.tesson@nxp.com

Magali Duplessis
NXP Semiconductors, TCE-Caen
Campus Effiscience, Colombelles
14906 Caen Cedex 09, France
Magali.duplessis@nxp.com

Stéphane Charlot
FIME Ouest
8 av. Commodore J.H. Hallet
14000 Caen, France
Stephane.charlot@fime.com

***Abstract*— The present paper reports the design and Electro-Magnetic (EM) modeling of Through Silicon Via (TSV) based band-pass filters embedded in passive interposers for C and V-band applications. For each filter, EM simulations have been performed with the help of a FEM (Finite Element Method) 3D EM solver. Prior to filter implementation, a comparison between simulated and measured data is proposed on dedicated structures (3D solenoids, and transmission lines) to calibrate the simulator and validate the simulation methodology. The obtained simulation results are successfully correlated to measurement data up to 110 GHz. In addition, an original package characterization up to 30 GHz is also proposed to support filter design and implementation. The proposed filter architectures permit a clear reduction of the filter footprint (up to 90 % vs. conventional implementation on ceramic substrate) with good electrical performances. Depending on the application IL of 2,6 and 2,0 dB have been simulated respectively at 4 and 42 GHz. Discussion on advantages of using either high/low aspect ratio TSV together with different Back-End Of Line (BEOL) option is proposed based on these two typical examples. Perspectives are then given in terms of 3D-IC integration.**

Keywords - Finite Element Method; Through Silicon Via; Filtering; EM simulations; passive interposer; Millimeter-wave

I. INTRODUCTION

The concept of 3D Silicon integration using TSV stacking is one of the most promising technologies. It can extend Moore's law by stacking and shortening the connection path between memory and logic [2]. Due to the increase in functional integration requirements, more and more assembly house and wafer foundries are looking into 3D TSV technology, which allows stacking of Large Scale Circuits (LSI's) thereby enabling products to be made smaller with more functionality. 3D technology realizes miniaturization up to 300-400% compared to the conventional packaging [3]. Furthermore TSV are also relevant to develop "more than Moore" applications [4], where passive functions originally lying on the PCB (Printed Circuit Board) can be designed with the help of TSV up to the C-band using original component architectures such as embedded solenoids (see Figure 1). In that sense, distributed L, C filters based on TSV can be optimized and implemented within interconnect dies.

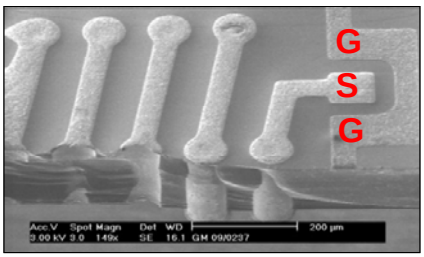
On the other hand, solenoids have limited performances at higher frequencies (in the millimeter-Wave domain). Indeed these solenoids made with low aspect ratio vias (300/75) exhibit non negligible parasitic capacitance with substrate that degrades their Self-Resonant Frequency (SRF) and thus their efficiency at higher frequencies [1]. Furthermore, passive interposer die with high aspect ratio vias cannot allow designing such solenoid but worth being considered to make filtering at higher frequencies (Ka and V bands) using a different architecture. Indeed, both Ka and V-bands – currently reserved for professional applications (aerospace, defense, satellite communications) - appear promising for developing applications such as automotive car-radar and wireless infrastructures [5][6] in order to face societal challenges: Energy harvesting, health, mobility and safety, security).

The paper will be organized as follow: a perceived state of art regarding passive component implementation is proposed in the following section of this document. Then, integrated solenoid as well as MOM capacitance will be introduced in the second section; their performances will be presented from an electrical point of view together with their relative precision taking into account the process spread. Solenoid performances obtained from wide-band frequency 2-ports S-parameter measurements will be presented. EM modeling done with the help of a 3D Finite Element Method (FEM) solver will be also described and compared to measurements. As the effect of packaging plays a significant role on the device performances, the third section of this study will be devoted to the characterization of a conventional QFN package using a very single test-case. Measurement data will be then used to calibrate the EM simulator. In the fourth section of this paper, we report the design methodology and the simulation results for a 4 GHz band-pass Chebyshev filter done using TSV. In the

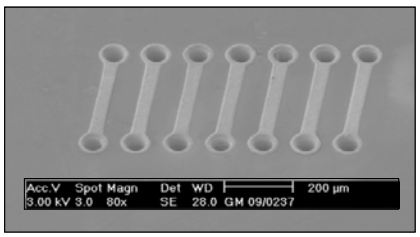
fifth section, we will introduce the micro-strip TSV based band-pass filter for Ka/V band applications. Its architecture will be presented together with characterization results obtained on transmission lines. These measured data will be used to calibrate the FEM solver and then propose an EM model of the proposed filters. The interest of using both high aspect and low aspect ratio of TSV in view of targeted applications is also documented in the paper. Simulation results based on different scenarios for BEOL and substrate options will be presented at the end of the document as well.

II. PERCEIVED STATE OF ART

Many efforts have been done to develop high performances active and passive devices especially in BiCMOS process [7][8][9] to support high performance applications. However, this is not enough; these high frequency applications will also require elite passive devices. Modification of BEOL and/or substrate properties (going to HRS for example) is already a good alternative but requires process update that is sometimes very expensive and can impact front-end components. In addition, the emergence of 3D interconnects such as TSV allows designing passive interposers to support these high performance applications. They render possible for example integrating passive filters necessary in every module.



(a)



(b)

Figure 1. SEM picturesTop view (a) and bottom view (b) of the 3D solenoids within GSG (Ground Signal Ground) pads – source IPDiA

Filters are either integrated on chip (using planar coils and Metal-Oxide-Metal (MOM) capacitors) or integrated in a hybrid application such as MCM (Multi-Chip Module) lying on a ceramic or organic substrate using a micro-strip architecture. Some well known structures have been already successfully implemented and extensively reported [10][11][12][13][14]. For the former ones, they can suffer from their low quality factors (mainly due to the resistive losses within the planar coils) while the latter ones exhibit high performances but can deviate a lot from nominal behavior compared to silicon because of process spread.

Another alternative also consists in implementing the filters on top of the carrier substrate (Printed Circuit Board for example) with the help of Surface Mounted Devices (SMD). The main advantage of such approach is the high quality factor value that can be reached. But generally they have limited performances at higher frequencies, the total footprint is bigger and the lack of accurate and scalable electrical models limits their applications and implementations in view of a high selectivity of the signals. In case of fully integrated filters within silicon IC processes, some passive integration dedicated processes have been already developed to tackle the low quality factor of the unit components. Devices are generally deposited on HRS (High Resistive Substrate) that clearly limits the effects of eddy currents [4] [15]. Thick top metals are also implemented and copper is often used to reduce the resistive losses. Thickness up to 8 µm can be considered in certain cases. Recent achievements have highlighted really good performances for band-pass filter for TV on Mobile applications [16]. For this application, coils exhibit regular planar shape, which provides a good compromise for designers between ease of layout, manufacturing and electrical performances. Besides that, Ka-band filters with really good performances have been also recently achieved using micro machined process either within silicon or glass substrate [17]. These technologies are really good candidates to develop applications in the millimeter-Wave domain. Notwithstanding, they require at least a substrate transfer technology (case of glass) that is not often compliant with classic wafers handler for which foundry need to adapt deeply their production environment [18]. On the other side, together with the emergence of new type of interconnects such as TSV, embedded solenoid implementation within silicon or glass substrate [19] is now considered to easily build a coil-type of structure. Several proposals have been done in that sense leading to very promising results [20][21]. In fact, integrated solenoids can be used to produce larger quality factor than in RF BiCMOS/CMOS planar technologies within a given footprint [22]. This increase in quality factor can be attributed to both metal thickness and the specific solenoid property of storing energy according to:

$$Q = \omega \cdot \frac{energy\ stored}{average\ power\ dissipated} \quad (1)$$

Where ω designates the pulsation (i.e.,2.π.freq)

Thus, the following part of this document will describe the solenoid architecture that we have adopted and summarize the main electrical performances measured on-wafer on this kind of devices.

III. 3D INTEGRATED SOLENOIDS

In this part, 3D integrated solenoid will be described in terms of geometry. Then, high frequency measurements will put in obviousness the real interest of such a device in the C-band.

A. Solenoid geometry description

We have already reported the fact that 3D TSV based solenoid can be implemented within a silicon die [22]. This process has been developed by IPDiA (formally NXP semiconductors). Contrary to the approach proposed in [23] where solenoid lies on top of the substrate, our 3D solenoid uses the thickness of the silicon as the third dimension. Indeed each turn of our solenoid is fabricated with the TSV as the vertical sides. A front side and back side metallization of the bulk wafer lead to connect the top and the bottom tracks, thanks to the TSV, allowing creating loops embedded within the silicon. Thereby we obtain a square section 3D solenoid architecture. On the top side of the silicon, a second level of metal is also used to realize MOM capacitors with a density of 100 pF/mm^2.

Copper is deposited onto front and back sides of a 300 µm depth high resistivity silicon substrate (HRS) according to a pattern defined in Figure 2. The vias are partially filled with the same metal on the external sides as highlighted by the SEM (Scanning Electron Microscopy) picture in Figure 1(b). Consequently N-turns 3D solenoids consist of N elementary spirals placed side by side and connected in the direction of the pitch between two consecutive vias (see Figure 2). Due to the TSV technology process, parameters such as via diameter and via height are fixed and so cannot be modified. In our case, the aspect ratio AR (height/diameter) is equal to 4. To avoid mechanical stress, the pitch between two consecutive vias is set to a minimum value equal to 125 µm. Nonetheless, the dimension of the metal tracks in front and back sides can be modified in order to improve the intrinsic component electrical characteristics as suggested by [24]. Hence the solenoid is defined according to its number of turns N, its width Dy and the metal track width W (that can be different between top and bottom traces). A change in the metal tracks width will also impact the spacing SP between two consecutive metal tracks.

B. Solenoid measurements

To support our theoretical investigations, solenoids with 1 to 6 turns were designed and grown on silicon. Then the designed test-case inductors have been placed within conventional GSG pads (Figures 3 and 4) and measured using a network analyzer PNA8364B from Agilent Technologies, with high frequency micro-probes. Full two ports S-parameter were performed for each device up to 20 GHz.

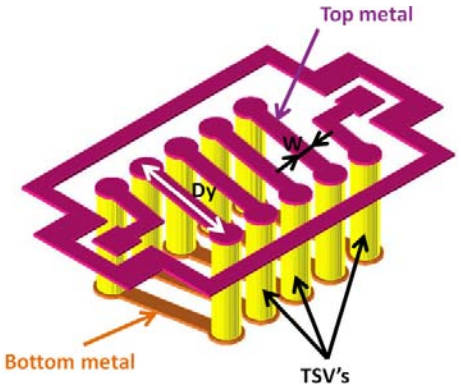


Figure 2. Synoptic representation of a 5 turns 3D solenoid within its RF test structure (bulk silicon is not represented on the picture)

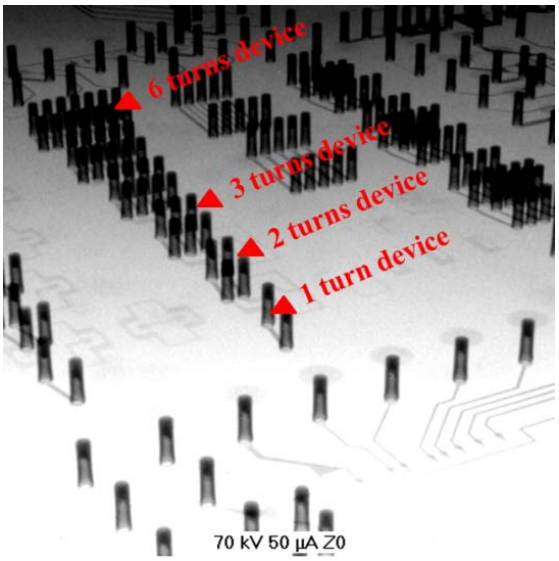


Figure 3. X-ray diffraction picture of the solenoid dedicated module (source IPDiA) – The bottom white face of the picture is the top side of the wafer

During the RF characterization, the wafer was stacked to a grounded chuck to ensure a global reference ground to the wafer, the network analyzer and the micro-probes. If no precautions are taken, a short circuit appears between the grounded chuck and the bottom metal tracks of the wafer. As a consequence, a sheet of glass fiber (~100 µm thick, ε_r =4.5) has been placed between them. The complete set of solenoids is shown on the previous X-ray diffraction picture. TSV can clearly be identified as a small vertical dark bar. For each measured device, self-inductance value and quality factor have been extracted on five crystals. In [22], we have already shown that the self-inductance variation versus the number of turns N was really close to a linear law, suggesting a very low inductive coupling between the loops. This is due to the minimum pitch defined by the process that is relatively large (= 125 µm). As a consequence, the capacitive coupling is also reduced, which allows using the inductors at several GHz. Furthermore, due to the typical

geometry of the solenoid, the quality factor is improved up to several GHz compared to classical planar IC coils either in CMOS or BiCMOS processes. A physical lumped elements electrical model was proposed also to simulate the device behavior versus frequency (see Section C.1). This model is indeed really helpful to generate contour plots in order to pick-up the right solenoid parameters (N, W, Dy, SP) and thus decrease the design iterations. Nonetheless, as any other compact model, it is not correlated to the global environment of the device (parasitic coupling, ground rails …). So in view of designing passive filters, we have also developed an EM (Electro-Magnetic) based model.

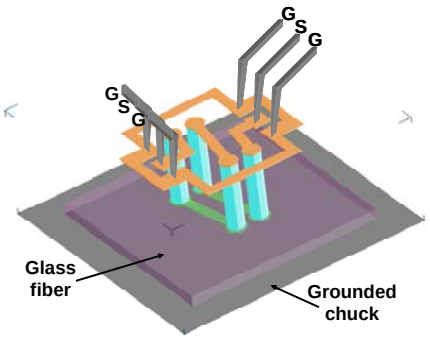


Figure 4. Illustration of the measurement test-bench used to guarantee a good ground reference together with an isolation between bottom metal traces and chuck (case of a 2-turns solenoid)

C. 3D solenoid modeling

Solenoid modeling is addressed first with a classical approach (i.e., compact modeling) and then with a 3D EM solver to provide modeling within a real environment.

1) Physical compact modeling

A first compact and physical model of the TSV based solenoid has been already issued. The schematic circuit of the model is presented in figure 5. This model has been built in order to figure-out the solenoid behavior within its RF test structure. Traditional model [25] –also called the "9 elements model" used for planar coils cannot be used in that case due to the 3D specificity of this kind of device with the parasitic 3D effects introduced by the vias. Our choice has been to follow the physical configuration of a 1-turn solenoid to deduce an RLC equivalent circuit model in the frequency range 100 MHz-10 GHz.

Knowing that each of both vias is modeled by two equivalent half-vias, the self-inductances of the top and bottom metal tracks as well as the vias are characterized respectively by L_{bot}, L_{top} and L_{via}. The metal tracks and the vias are sensitive to the skin effect. The skin depth in the copper, with a conductivity of 5.8 10^7 S/m, at 100 MHz and 1 GHz equals 6 µm and 2 µm respectively. Hence an RL ladder scheme [26] has been used to predict the increasing resistance against frequency for each of the metal tracks (R_{top} and R_{bot}) and the vias (R_{via}).

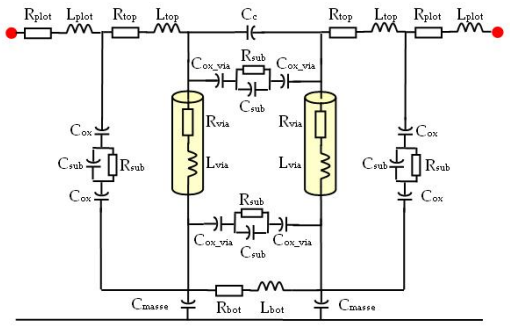


Figure 5. Schematic view of the equivalent circuit consider to derive the compact electrical model of 3D TSV based solenoid

Regarding the coupling between two adjacent vias, we can distinguish several contributions. The first one is the capacitance C_{ox_via} introduced by the oxide barrier (to avoid copper diffusion within the substrate) between the via and the substrate. The second one corresponds to the capacitance C_{sub} and the resistance R_{sub} of the substrate. As mentioned in the measurement results section, the backside of the wafer has been protected from the grounded chuck with a sheet of glass fiber. Notwithstanding, a capacitance C_{masse} exists between them and needs to be evaluated. The capacitance between the two consecutive top metal tracks (i.e. function of the spacing SP) is characterized by C_c. In the case of 1-turn 3D solenoid, C_{lines} is very weak due to the small area of the top metal tracks facing each other.

In order to address multi-turns solenoid modeling, each of the previously defined section is added for each loop of the solenoid. Coupling capacitances as well as coupling inductances are also implemented. Based on available test-structures, a good correlation has been obtained between both simulated and measured data [27].

The primary mean of this compact model is to correctly predict the main electrical characteristics of the device such as:

- its self-inductance value
- its quality factor (in link with resistive and substrate losses)
- its Self-Resonant Frequency (SRF)

Typically, designing an inductor can be very time consuming and needs most of time a real experience with this kind of device. In fact, the trade-off between series resistance and substrate losses represents a conventional scenario that RF designers need to address in an efficient and quick way when using on-chip inductors in their circuits. So, a design tool capable of optimizing the inductor layout by considering all these constraints (input parameters and overall performance) can significantly accelerate the design flow and have an impact on the time to market. Thus, a compact model that can predict the performances of a coil based on the parameters listed above – related to the input geometrical parameters (W, N, Dy), is really helpful and can be used to generate contour-plots in order to pick-up the right geometry and decrease the implementation time. The

following figures, propose some typical contour plots that can be generated with the proposed compact model:

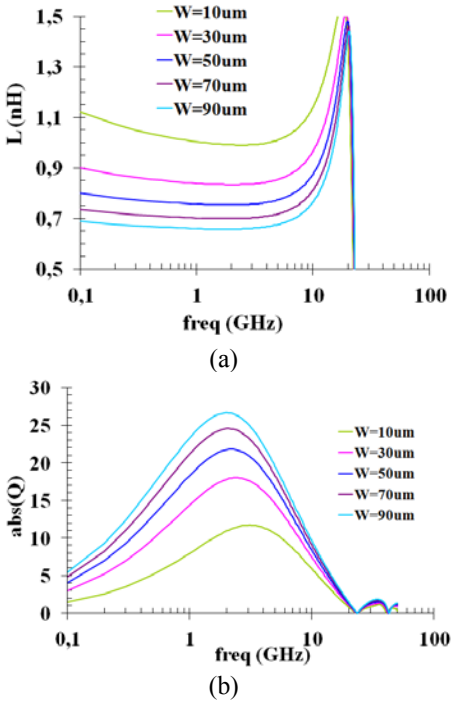


Figure 6. Simulated variations of (a) the self-inductance value and (b) quality factor vs. frequency for 1-turn solenoid (Dy was set to a fixed value during the simulations). These plots have been deduced from 2-ports S-parameter anlysis with a classical CAD simulator (i.e., SPICE). Compact model described in the previous paragraph has been used to extract the devices performances

Thanks to these plots, designers are able to find the compliant coil layout for achieving a specific inductance with the highest Q possible for a given technology of interest (only process parameters are required in the equations of the model). For example, considering a 700 pH inductor at 1 GHz, one can decide to have copper tracks that are 70 µm width with a 1-turn configuration. In that case, the expected quality-factor is equal to 22.

Nevertheless, this approach could not anticipate on the device behavior when placed in its environment. In micro wave a special care needs to be taken during the layout topology translation to tackle the unwanted current loops and identify both parasitic magnetic and electric couplings. Parasitic extractor provided by Electronic Design Automation (EDA) vendors are of particular relevance (when coupled with full-wave analysis) in that case especially for planar applications [28]. Unfortunately, they are not optimized to solve 3D problems like the one occurring in bulk silicon substrate.

2) Electro-Magnetic (EM) modeling

Dedicated test-cases presented in the previous paragraph have been simulated using the 3D FEM solver EMPro from Agilent. First, TSV have been defined within the substrate stack taking into account the partial fill of the vias with copper, the barrier between the copper and the silicon bulk (to avoid copper diffusion in the silicon). Geometry of the vias is also simplified: the circular shape of the TSV is converted to an octagonal one, in order to speed-up the mesh and thus the simulation time without losing any accuracy on the results. Bulk silicon has been described with the help of its relative dielectric permittivity (ε_r=11.9) and its resistivity - equal to 1000 Ω.cm. First a comparison between simulated and measured S-parameter has been performed (see Figure 7). Then, both self-inductance value and quality factor against frequency have been computed for comparison purpose (Figure 8). Self-inductance and quality factor values have been extracted according to the following relations:

$$L = \frac{imag\left(\frac{1}{Y_{11}}\right)}{2\pi \times freq} \quad (2)$$

$$Q = -\frac{imag(Y_{11})}{real(Y_{11})} \quad (3)$$

where ***freq*** is the working frequency and Y_{11} is the input admittance.

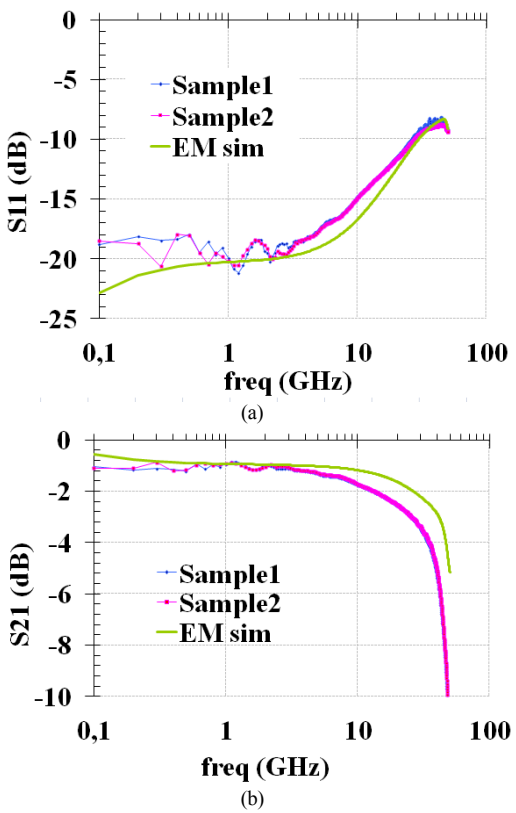


Figure 7. Comparison between Measured and simulated data on both (a) Reflection and (b) transmission S-parameter (1-turn solenoid)

From the available test-cases, a pretty good agreement is found for the self-inductance as well as the quality factor variations versus frequency.

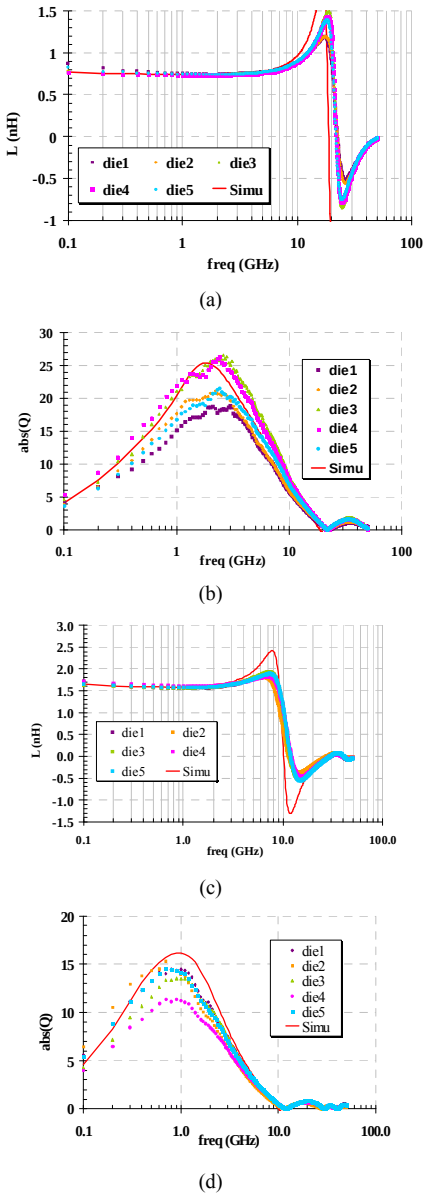


Figure 8. Comparison between measured and simulated data for 1-turn solenoid (a): self inductance value (b) quality factor and 2-turns solenoid (c): self-inductance value (d) quality factor

The SRF (Self-Resonant-Frequency) is also well predicted suggesting that the parallel capacitances are also well evaluated with the proposed approach. Typically, a difference of 3 % is observed on the self-inductance value and 10 % on the overall variations of the quality factor. This validates our approach that will be used to design a 3D solenoid based passive filter. Nonetheless, these measurements and simulations have been performed on-wafer without any coating on top of the substrate. In the following part of this paper, we propose to study a single test-case combining a chip, a package and a line on a board to validate our EM tool for packaging applications as well.

IV. PACKAGE MEASUREMENT AND MODELING

The following section will describe an original approach that has been considered to perform S-parameter measurements on a commercial package (QFN type).

A. Test-case description and measurement

Indeed, the emerging applications of wireless communications require effective low-cost approaches to microwave and RF packaging in order to meet the demand of the commercial marketplace. In that sense, surface mountable packages and especially plastic packages are a cost effective solution for low-cost assembly and packaging. However, plastic packages, whatever their types (standard QFN or flip chip based solutions such as BGA) contain unavoidable parasitic elements. As a consequence, development of characterization techniques for surface mounted packages is motivated by the need to predict the parasitic behavior of packages at microwave frequencies. In fact, the capability of accurately and easily characterizing packages provides a means to study and correctly model their high frequency behavior. Work in the literature relies mainly on EM simulations [29] [30]. In this paper, we will present an "on wafer" method of measuring the microwave performances of a chain containing a chip, a package and a 50 Ω line on Rogers substrate. Final goal of this part is to calibrate the EM simulator (in our case EMPro from Agilent) based on this single test-case.

B. Package modeling

One of the main problems of package characterization is that the terminals of the lead-frame are not accessible without significant modification to the investigated structure. To overcome the need for this modification, we have divided the test-case into three main parts. A photograph of the test case is provided on Figure 9.

So the first part of the test-case is a BiCMOS (NXP in house process) silicon die containing a coplanar line. The line is designed in such a way that it allows GSG probing with conventional micro-probes from Cascade Micro-Tech. This line is then connected with the help of 4 bond wires (2 for the signal and 2 for each ground path) to the pins of the package. Classical 20 µm diameter gold bond-wires have been considered for this study. Then, to be able to measure the electrical characteristics of the package, it is mounted onto a RO4003C substrate from Rogers Corporation (thickness = 406 µm, ε_r = 3.38, tan(δ) = 2.7e^{-3}). A specific coplanar access is also designed on the substrate allowing also GSG probing (bottom side of the photograph in Figure 9).

In order to perform 2-ports S-parameter measurements, the package is then opened to access the GSG pads on the chip. Prior to measurements, a Short-Open-Load-Thru (SOLT) calibration is performed. Four test-cases have been

measured up to 50 GHz to ensure a good reproducibility of the measurements. Results are presented in Figure 10.

The first results clearly show a good reproducibility between the measurements. Insertion and Return loss of the total chain are respectively equal to -1.3 and -10 dB at 4 GHz, which makes such a package suitable for multi-GHz applications. Of course, many improvements can be considered to enhance these performances (ground connection, wire loop profile, down bonds implementation). But, these techniques will not be addressed in this paper.

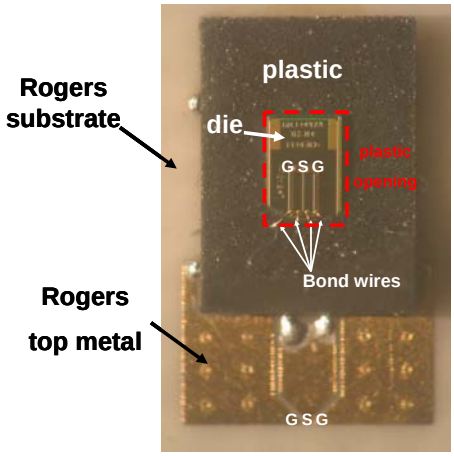
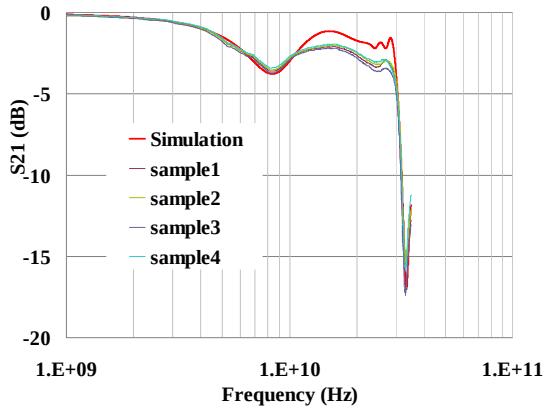


Figure 9. Photograph of the designed test-case suitable for microwave package characterization and modeling. Configuration allows 2 ports micro-probing: one on the inner die and the second one on the Rogers top metal (bottom of the picture)

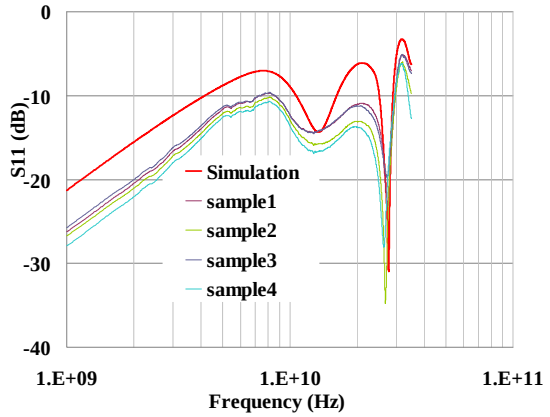
Aim of this section is to calibrate the 3D FEM solver EMPro from Agilent to correctly handle the S-parameter variations of the previously measured test-case. The 3D EM model should estimate the electrical performances of the package as accurately as possible, but on the other hand, should not be too complex for the EM simulations of more complex blocks. The following methodology has been applied:

- Bond wires cross-section have been first described with a square shape. Generally speaking, all round shapes should be avoided as much as possible as they are really time consuming for the simulations and the 3D mesh generation.
- Bond wire profiles were estimated based on a circle shape assumption as proposed by Alimenti et al. [31].
- Package terminals are defined into two equal steps (each is 100 µm thick) to have accurate modeling of the thick metal. One should try also to approximate their geometries with few corner points as possible but the modifications should not affect the electrical response of the simulator.
- Coplanar ports have been used on both the chip and substrate lines.
- All dielectrics are defined with finite bricks taking into account their relative permittivity and the loss tangent or the conductivity. Plastic brick is open with an "Air" brick in order to stick as much as possible to the measurement configuration.
- The common ground reference was set to the bottom metal of the Rogers substrate.

Both reflection and transmission S-parameter obtained from EM simulations are plotted in Figure 10 together with measured data. The simulated results corroborate the measured data with a good accuracy up to several tenths of gigahertz.



(a)



(b)

Figure 10. Comparison between measurements and simulated data vs. frequency on the package test-case – (a) transmission parameter, (b) reflection parameter

To conclude this part, the EM simulation tool enables relatively accurate and complex package analysis. So based on these two previously studied test-cases (solenoid and package) the FEM solver is calibrated and ready for embedded filter design with solenoid based TSV.

V. 4 GHz Band-pass Filter Modeling and Design

Based on the previous building blocks that have been studied in previous sections (i.e., package and solenoid measurements together with EM modeling), this part will focus on the design feasibility of a 4 GHz band-pass filter.

The objective is to design a band pass filter with a maximum of 4dB insertion loss.

A. Schematic design

First, a third order Chebyshev architecture has been considered to design a filter prototype. Nonetheless, taking into account coefficient in [32] and applying the well known transform from low-pass to band-pass filter, lead to an inductor value in the serial electrical path that is equal to 9.13 nH. Such an inductor will have a high serial electrical resistance that will seriously affect the insertion loss of the overall filter and will also have a Self-Resonant Frequency too close to operating frequency clearly limiting its usage. So, a choice has been made to split the filter into two different parts as shown on Figure 11 and already proposed in [16]. The first part is a 5th order low-pass filter while the second one is a 3rd order band-stop filter. Both are Chebyshev filters. By doing this, only MOM capacitors and small inductances values (i.e., 451 pH for L6 and L10) will be present in the serial path of the filters. This approach allows reaching the specified level of insertion loss.

All inductors will be designed using TSV with the same architecture as the ones presented in the first part of this document. The quality factors of inductors L6/L10 have been simulated prior to implementation and are equal to 10, which is sufficient for the targeted application. For inductors placed on the parallel paths (i.e., L1, L3, L5 and L9) their impact is really low regarding the insertion loss.

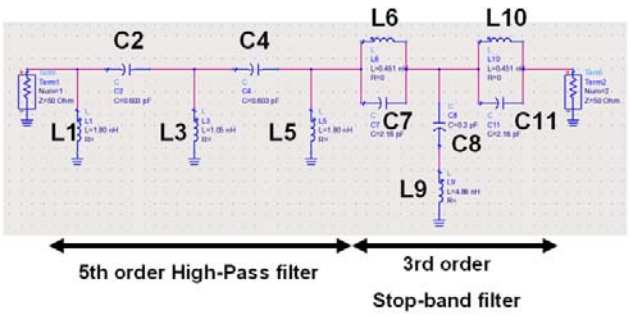


Figure 11. Schematic view of the 4 GHz band-pass filter considered for this study

For the capacitors, a choice has been made to use the "free" MOM capacitor offered by the process. In fact two metallization are present and can be patterned as well on the top-side of the wafer. They are separated by a classical oxide with a density of 0.1 nF/mm^2. A very low serial resistance value induced by the capacitor is expected to result from the use of two thick copper layers as device electrodes. Furthermore, very precise values of capacitance can be obtained since its relative precision is driven by the oxide thickness, which is really low (+/- 5%).

All these components will of course interact one with another leading to a change in the frequency response of the filter. That's why, a top level EM simulation is required to adjust and optimize the topology of the overall filter taking into account the interconnections as well as the ground return path.

B. Layout Implementation

Special care has been taken to optimize the electrical resistance on the serial path. Wherever possible, the RF path was designed by stacking both levels of metallization connected together using vias. Orientation and aspect ratio of capacitors have been chosen in such a way to minimize the resistive losses. A view of the simulated filter is shown on Figure 12.

First order dimensions of the solenoids (Dy, N) have been deduced from the analytical model provided in [22]. The value of the ground path inductance (metal tracks + bumps) is then taken into account as they participate to the self-inductance value from the RF path to the ground (inductors L1, L3, L5 and L9). The metal track inductances have been calculated in reference to partial inductance concept proposed by Ruehli and Zhong [33][34]. Electrical parameters of the bumps have been evaluated by calculation and single EM simulations as proposed in [35].

LC tanks (L6, C7 and L10, C11) in the stop-band filter have been realized with one-turn solenoids. Then prior to top simulations, each solenoid of the filter is placed with care in order to avoid as much as possible coupling between them. Typically the maximum space is considered, and an orientation of 90° between each inductor is applied to minimize magnetic coupling. Dimensions of the whole filter are 3.6x2.4 mm^2 and clearly outperform conventional microwave structures such as hairpin filter for similar application [30]. The full structure is then simulated within the package with the bump connection to the Rogers substrate. Results are presented on Figure 13.

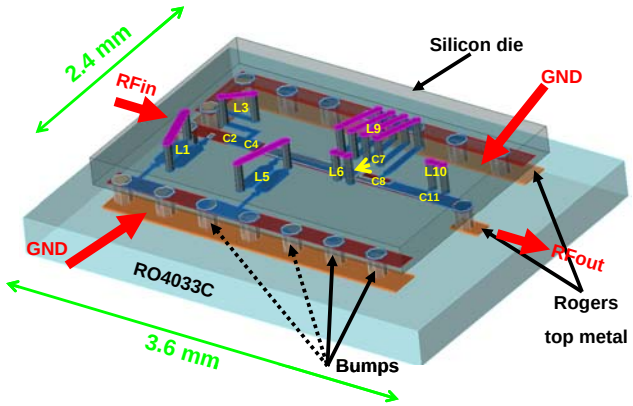


Figure 12. Top view of the simulated 4 GHz band-pass filter. Plastic of the package is not represented on the picture for clarity reason.

From the available results, the filter exhibits insertion and return loss of 2.6 and 16 dB respectively. Insertion losses are clearly within the specifications even if they are higher than classical micro-strip filters. The main contributors to the insertion losses are both inductors L6 and

L10 for whom electrical resistance increases very fast with the frequency.

C. Discussion

The approach described here gives indeed good results in case of moderate, loaded quality-factors (i.e., few units). Furthermore, it corroborates with the performances level already simulated by Georgia Tech on High Resistive Silicon (HRS) substrate [19]. On the other hand, it seems that this solenoid architecture is not appropriate in case of narrow fractional bandwidth where higher loaded quality factors are required.

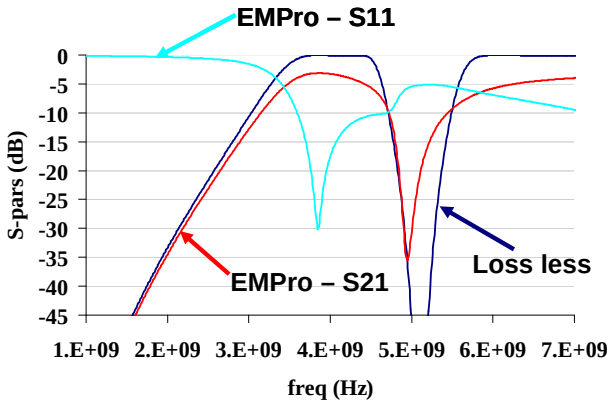


Figure 13. Simulation results of the proposed filter. Dark blue line corresponds to loss-less schematic filter simulated with ADS® schematic.

For these very specific applications, classical micro-strip filters deposited on low-loss substrates such as ceramic should be considered. TSV based solenoids can be used to build compact filtering applications up to several GHz. In fact, as shown by the solenoid characteristics on Figure 8(b) and Figure 8(d), the solenoid suffers from resistive losses at high frequencies on one side and from moderate SRF on the other side. The former effect is impacted by the classical phenomenon occurring at high frequencies within metallic conductors - the skin effect - while the latter one is due to the coupling capacitance between via metallization and the silicon substrate. One way to reduce it consists in using very high aspect-ratio TSV in combination with thinner silicon substrate. In the following part of this contribution, we propose to design a 42 GHz band-pass filter based on high aspect-ratio vias (50/7). In that case, solenoid type of component should be avoided and different filter architecture must be proposed.

VI. V-BAND BAND-PASS FILTER MODELING AND DESIGN

TSV building brick has been identified as a key enabler in view of promoting either C2C (chip to chip), C2W (chip to wafer), W2W (wafer to wafer) 3D IC integration in order to support high performances chips [37]. In a recent work [1], and in the previous study depicted in this document, we have shown some results obtained on 3D based solenoids band-pass filter at 4 GHz. Idea was to use low aspect ratio TSV to make embedded solenoids. Q-factor of the obtained devices was really promising (vs. planar solutions) especially below 5 GHz [22]. However, the devices suffer from the low self-resonant frequency due to the parasitic capacitance between the metal from the via and the silicon substrate, clearly limiting the range of applications of this kind of devices to the L and S bands. In fact, the capacitance between the via and the substrate is given by the following relation:

$$C_{val} = \frac{2\pi . \varepsilon_o \varepsilon_r h}{ln\left(\frac{R_2}{R_1}\right)} \quad (4)$$

In this relation, R_1 is the inner radius of the via while R_2 is the outer one. R_2-R_1 is no more than the thickness of the diffusion barrier between metal and the substrate. Typically, for low aspect ratio via considered in this study, this capacitance is in the order of 11 pF; so its impact is not negligible on the solenoid SRF.

So, one can clearly see the interest of using high aspect ratio vias with reduced substrate thickness down to 50 um. Furthermore, this will have an impact on solenoid density. So, for the filter proposed in the following part of this document, the architecture will be updated to avoid using solenoid that are clearly not suitable for high frequency operations (V-band targeted here). The second interest of TSV at high frequencies is the availability of such interconnect to make a clean and short connection to the ground reference (bipolar emitter, …). Indeed, this is a crucial point for millimeter-Wave applications and TSV will certainly help improving it like it is done in most of AsGa based processes [38][39]. In the following section of this paper, we propose to use intrinsic properties of TSV to make a short inductance value together combined with a clean ground connection in order to make a 3rd order 42 GHz band-pass filter. First, details about the filter architecture are given. Then another paragraph is devoted to the practical layout implementation of each of the sub-blocks of the filter. Prior to filter simulation, EM simulation results of the transmission lines used in the filters are given and compared to measurement data. Finally an analysis related to different process options is given at the end.

A. 42 GHz filter architecture

Our first idea was to reproduce a classical 3rd order Chebyshev filter. Applying the well-known transform from low-pass to band-pass filter and using the ad-hoc coefficient found in [32], it comes out that a 0.76 nH inductor appears to take place in the serial path of the filter (i.e., the serial LC resonator). In addition, the self-inductance values of the parallel resonator are in the order of 50 pH, which is weak and can be achieved with the help of one TSV. A 0.76 nH solenoid is easily achievable but will not support 40 GHz applications. The self-resonant frequency (SRF) is by far below this value. That's why, it has been decided to remove

the serial LC resonator and replace it by one parallel resonator placed between two λ/4 micro-strip lines. Doing that way, only 50 pH to 65 pH inductors are necessary to design the filter. Such inductance will be then TSV based. So the filter will use the well-known property of the quarter-wave lines to invert impedances. The schematic of the filter is provided on the figure below:

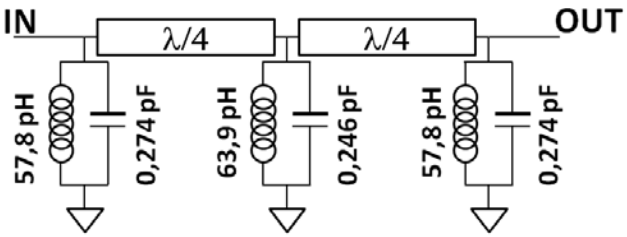


Figure 14. Schematic view of the 3rd order 42 GHz band-pass filter considered

So, basically, the filter will require the implementation of transmission lines, metal-oxide-metal (MOM) capacitors and short connections. The following part of this document will focus on the implementation of each of these sub-blocks.

B. Physical layout implementation

All devices that are used in this study are compliant with classical IC design rules (for this example, we have applied rules from NXP in house BiCMOS process).

1) Transmission Lines EM modeling

A synoptic representation of a transmission line pattern is proposed on the following figure:

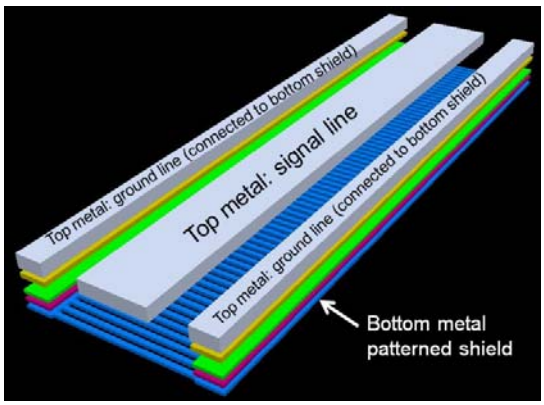


Figure 15. Layout pattern of the considered transmission lines used to calibrate the 3D EM simulator

Transmission lines considered here are mandatory to calibrate the 3D EM solver (i.e., EMPRo) and are based on the slow-wave concept and uses the latest metal level of the BEOL (Back-End Of Line) to propagate the signal. Typically, in this study, it is a 3 µm thick copper layer. All of them have been measured up to 110 GHz with a network analyzer from Agilent Technologies. Prior to parameter extraction, de-embedding was performed using a classical two-steps Open-Short method. A typical view of a transmission line between GSG pads is proposed on Figure 16. The bottom metal layer of the process is used for two main purposes:

- To shield the line and thus reduce and prevent the losses within the substrate. In fact, the metal shield is implemented in order to block the electric field penetration inside the lossy substrate. On the other side, a patterned design is adopted to be compliant with design rules and also to break current loops in it. In fact, these loops can have a significant impact on line attenuation.
- To connect the bottom face of the chip using TSV. TSV are used to connect the ground plane for the micro-strip line to the back side of the chip, which is indeed the real ground reference.

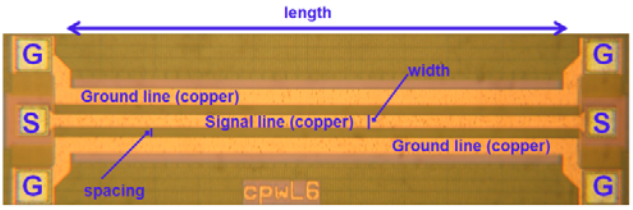


Figure 16. Photograph of a transmission line within GSG pads for two-ports S-parameter measurements, used to calibrate the 3D EM simulator

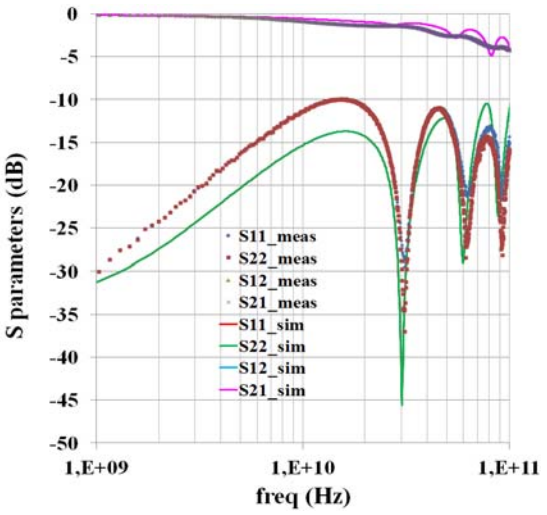


Figure 17. Comparison between simulated (EM) and measured S-parameter obtained on a transmission line (length = 2000 µm, width = 15 µm , spacing = 8.3 µm)

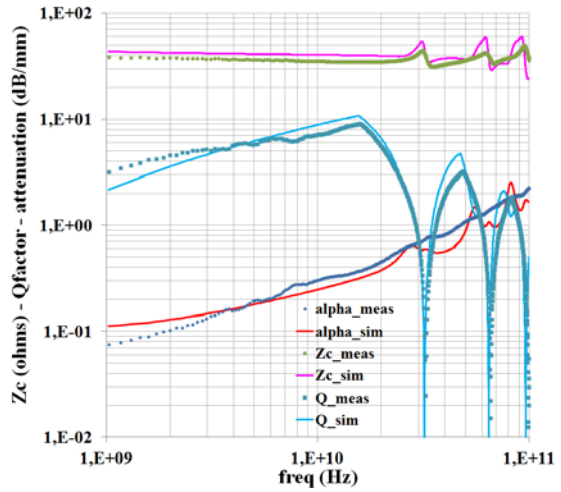


Figure 18. Comparison between measured and simulated data vs. frequency for transmission line characteristic impedance Zc, attenuation alpha and quality factor Q (length = 2000 µm, width = 15 µm, spacing = 8.3 µm)

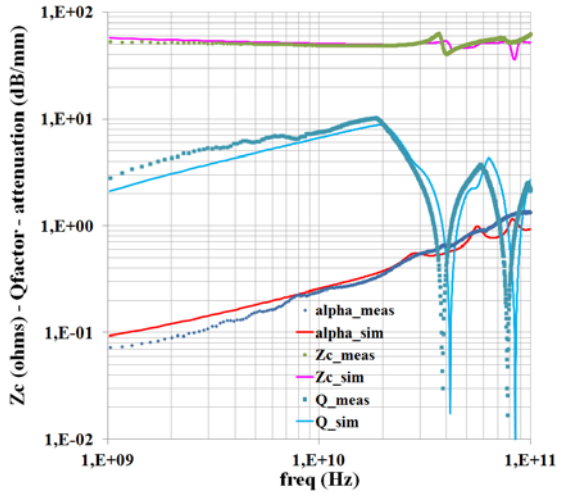


Figure 19. Comparison between measured and simulated data vs. frequency for transmission line characteristic impedance Zc, attenuation alpha and quality factor Q (length = 2000 µm, width = 15 µm, spacing = 8.3 µm, 4 bends)

A physical wide-band electrical modeling has been already proposed to deal with the electric behavior of such devices [44]. The accuracy is really excellent but like for solenoid this model can of course not take into account the global environment of the line. That's why, again an EM model is mandatory to correctly simulate the filter response.

EM simulator has been calibrated based on measurements performed up to 110 GHz on various geometric variants of the previously described transmission lines. Calibration has been performed based on S-parameter variations and extracted parameters. These electrical parameters are:

- The characteristic impedance Zc (ohms)
- The attenuation α (dB/mm)
- The quality factor Q

Based on the available data and results, the correlation between measurements and EM simulations is really satisfying up to 110 GHz. From a performance point of view, the attenuation constant is equal to 0.66 dB/mm, which is in good agreement with results already published in the literature [40]. The patterned shield plays a significant role in reducing the attenuation of the lines (i.e., in the order of 1.3 dB/mm without shield [41]). This is the last building brick necessary to achieve the design of the 42 GHz band-pass filter.

2) Filter implementation

The proposed transmission lines have a width of 15 µm and the ratio width/height (W/H) is equal to 1.75 to ensure a 50 ohms configuration. The simulated attenuation is equal to 0.53 dB/mm and the total length of each line is equal to 1.134 mm leading to an overall attenuation of the lines equal to 1.21 dB. Based on simulations, characteristic impedance of the transmission lines, Z_c, has been found equal to 50.5 ohms at 42 GHz. Taking into account this value, the new parallel inductance and capacitance values (see Figure 14) are calculated using the initial values deduced from the ad-hoc coefficients of the Chebyshev filter synthesis:

$$C_{new} = \frac{Y_c^2}{C\omega_0^2} \quad (5)$$

$$L_{new} = \frac{Z_c^2}{L\omega_0^2} \quad (6)$$

where Z_c is the characteristic impedance of the line (i.e., 50.5 ohms), $Y_c=1/Z_c$ and $\omega_0=2\pi f_0$ (f_0=42 GHz).

MOM (Metal Oxide Metal) capacitors are designed using two levels of metallization. Bottom level uses the lowest level offered by the process (same as the ground plane for transmission line) while top metal is used for the top electrode. Doing like that, an average density of 4.5 pF/mm^2 is achieved allowing designing capacitors with values up to 0.5 pF. Like for transmission lines, the lowest metal is connected to the ground reference with the help of TSV. It should be noted here that high aspect ratio vias allow decreasing the ground short inductance, which is mandatory at very high frequencies.

A special care has been taken during the implementation of the capacitor in order to reduce as much as possible the parasitic inductance value. In that sense, the form factor of the device must be chosen accordingly with a high ratio width/length.

Regarding the parallel inductances and short connections, the basic idea here consists in using the TSV to make the parallel inductance in the LC resonator and thus the connection to the ground reference. The self-inductance of a single via can, of course, not be changed and exhibits a fixed value of 22 pH (deduced from EM simulations). In order to adjust the parallel self-inductance value, the length/width of the metal track that connects the λ/4 lines to

the vias can vary. At the same time, as explained in the previous part of this paper, each TSV will also present a parasitic capacitance to the substrate due to the presence of the diffusion barrier. In our case, this capacitance is equal to 12.8 fF/via. It is then necessary to adjust the final value of the MOM capacitances taking into account the capacitance inherited from the TSV.

Finally, the layout topology of the filter is proposed in Figure 20.

C. Simulation results

EM simulations have been performed up to 80 GHz on the previous structure taking into account nominal process parameters. Prior to simulations, the bottom metal patterned shield has been simplified to decrease the mesh complexity as well as the simulation time. On the other side, these simplifications must lead to the same level of accuracy. So, the patterned metal shield is made of metal fingers of 5 µm width and 1 µm spacing. The filter has been simulated in its global environment including the bumps to connect it to the active die, and with and underfill material between the stacked dies (not represented on the figures above). Simulation results are proposed in the figure below:

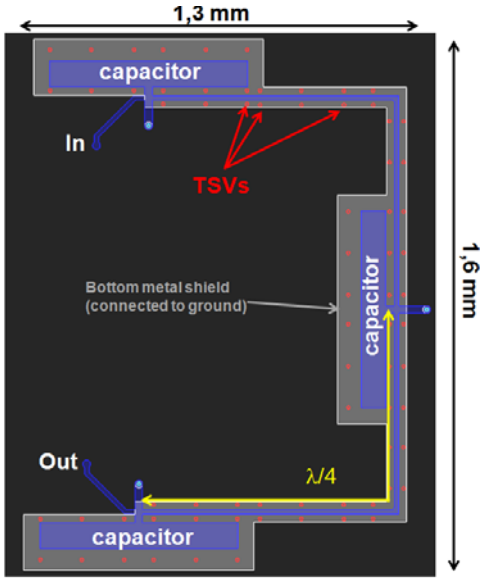


Figure 20. Top view (a) and 3D view – the gray bottom plate is the ground reference of the device (b) of the simulated band-pass filter

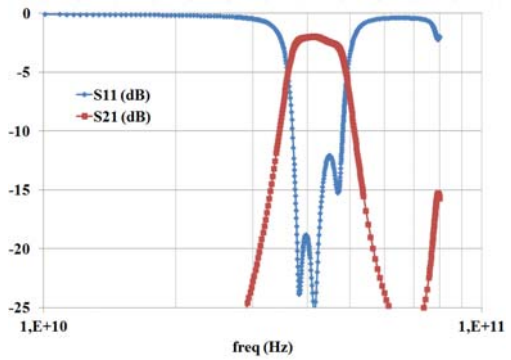


Figure 21. Simulated variations of transmission and reflection S-parameter of the proposed filter (nominal process parameters with copper back-end)

IL (Insertion Loss) and RL (Return Loss) are found to be equal to -2.0 dB and -18.5 dB respectively at 42 GHz. It appears that the losses are mainly dominated by the transmission lines losses. One way to reduce these losses consists in using thicker metal but requires process updates that are not always compliant with cost efficiency. The bandwidth of the filter at -3 dB is equal to 12.3 GHz, which was predicted by the theory. The filter exhibits a reduced footprint of about 2 mm^2 compared to classical interposer done with LTCC substrate [42] [43]. A summary of simulated filters intrinsic properties is proposed in the table below:

TABLE I. OVERVIEW OF FILTERS CHARACTERISTICS

	C-band filter	**V-band filter**
	Low-density TSV	***High density TSV***
f_0	4 GHz	42 GHz
IL[a] at f_0	-2,6 dB	-2,0 dB
RL[b] at f_0	-16,0 dB	-18,5 dB
Frac. Bandwidth[c]	16 %	29 %
footprint	8,6 mm^2	2 mm^2

a. Insertion loss
b. Return loss
c. Bandwidth is calculated at -3dB

However, the level of performance might be improved by looking into the best process options. Simulations have been performed in that sense and are presented in the last part of this work.

D. Process options

Several process options have been considered for investigation purpose:

- Thick copper: 8 µm instead of 3 µm
- Substrate resistivity: 20 ohms.cm instead of 200 ohms.cm
- BEOL: Al back-end instead of Cu back-end

Simulation results are on the following graph:

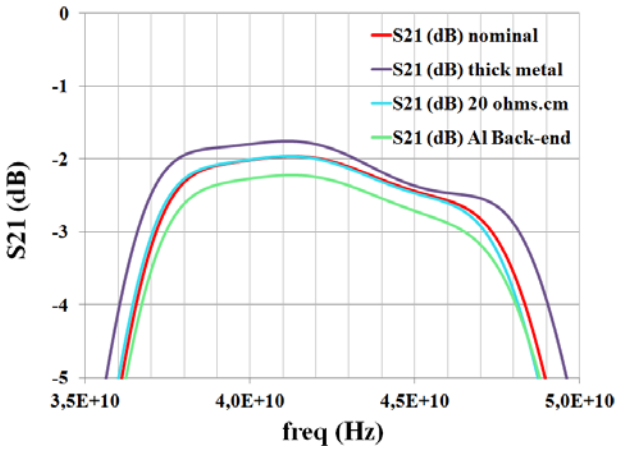


Figure 22. Variations of the Insertion Loss vs. frequency for different process options

Based on available results, one can clearly see that if a shield metal is used to block the penetration of electrical filed, the silicon conductivity has a minor impact on the insertion loss of the filter (provided that the substrate resistivity is between 10 and 1000 ohms.cm). Indeed, as already mentioned earlier, the losses are dominated by resistive losses within the transmission lines.

On the other side, one can remark that moving from Cu BEOL to Al BEOL only degrades the IL by 0.3 dB. Then this is a trade-off between process cost – compatibility between Al metal and Cu vias – process reliability. In the same way increasing the Cu thickness from 3 to 8 µm, only improves the IL by 0.2 dB. This point can be clearly understood if we take into account the skin depth of these materials at 42 GHz (i.e., 0.3 µm for Cu and 0.43 µm for Al). In fact it is relatively small compared to metal thickness. Conclusions would have been of course completely different for applications at lower frequencies (<5 GHz). But in that case such as design with λ/4 on silicon lines does not make sense.

- Changing the substrate resistivity also have a minor impact on the results for two reasons essentially: the presence of a bottom metal shield is the key point to reduce the transmission line losses within the substrate as suggested by [44]
- The use of high aspect-ratio within a "thin" substrate reduces drastically the losses induced by the TSV together with parasitic capacitive coupling with the substrate.

VII. CONCLUSION AND PERSPECTIVES

In this paper, two band pass filters for 3D-IC integration are proposed. The former one centered at 4 GHz is based on low aspect-ratio TSV and uses 3D integrated solenoid to design inductive elements. The latter is made of high aspect-ratio TSV combined with thin substrate. It uses λ/4 transmission lines to make impedance inverters and thus inductive elements are designed using single vias. Capacitive elements are classically made with MOM devices for both types of filter. The electrical characteristics of each single element on silicon (transmission lines, integrated solenoid, single via) have been measured up to 110 GHz and results have been cross-checked with 3D FEM data in order to make the 3D EM solver calibration. Modeling of the passive interposer's environment (i.e., the package and the under fill material) is also proposed and correlated to EM simulations. An original package characterization technique is also reported. It allows package modeling up to 50 GHz with high accuracy together with conventional measurements setup.

For both filters, good performances have been achieved. A bandwidth of 16% and 29% are reached with insertion loss of -2.6 dB and -2.0 dB combined with return loss of -16 dB and -18.5 dB respectively at the center frequencies for the S-band and V-band filters. It appears from these results that TSV based filtering applications are suitable for moderate loaded quality factor devices – typically few units. Classical micro-strip filters on LTCC should be preferred for very high loaded quality factors [45][46]. Investigation based on different process options is also proposed on the V-band filter. From available results on filter performances, they clearly highlight the interest of an efficient shielding technique rather than process updates. The presented technologies here show significant potential for millimeter-wave applications and are expected to allow 3D IC integration of high performances circuits. In fact, in order to reduce the footprint and enhance the performances of the products, a displacement from wire-bonding technology to flip-chip technology with TSV based passive interposers will take place. This new approach will help reducing the products size, weight and cost.

ACKNOWLEDGMENT

This project has been realized with the support of the French Ministry of Industry and Finance through the European joint project Catrene 3DIM3. Author would like to thank Jean-René Tenailleau from IPDiA for providing us with the samples of 3D integrated solenoids. We also thank Fabrice Goulet from NXP for his implication in the RF characterization of the devices and the package. The authors also wish to acknowledge Philippe Torregrossa and Vincent Poisson from Agilent for fruitful discussions and valuable support on EM simulations. We further wish to thank Dr. Ing. Sidina Wane from NXP for his valuable assistance in reviewing the paper and providing us with relevant suggestions.

REFERENCES

[1] O. Tesson, S. Charlot, and M. Duplessis, "Step-by-step design and EM modeling of a 3D solenoid-based 4 GHz band-pass filter (BPF) using through silicon vias, Proc. of 4th International Conference on Advances in Circuits, Electronics and Micro-Electronics 2011 (CENICS 11), pp. 23-28.

[2] P. Benkart, " 3D chip stack technology using through-chip interconnects ", IEEE J. Design and Test of Computers, vol. 22, n°6, Dec. 2005, pp. 512-518.

[3] S.W. Yoon, D.W. Yang, J.H. Koo, M. Padmanathan, and F. Carson, "3D TSV processes and its assembly/packaging",

Proc. of IEEE International Conf. on 3D System Integration 2009, 3DIC 09, pp. 1-5.

[4] F. Murray, F. Le Cornec, S. Bardy, C. Bunel, Jan F.C. Verhoeven, F.C.M. van der Heuvel, J.H. Klootwijk, and F. Roozeboom, "Silicon based SiP: a new technology patform supported by very high quality passives and system level design tools, Proc. of 7th Silicon Monolithic Integrated Circuits in RF 2007 (SiRF 07), pp. 149-153.

[5] Floyd, B. Pfeiffer, U. Reynolds, S. Valdes-Garcia, A. Haymes, C. Katayama, Y. Nakano, D. Beukema, T. Gaudier, and M. Soyuer, "Silicon millimeter-wave radio circuits at 60-100GHz", Proc. of 7th Silicon Monolithic Integrated Circuits in RF 2007 (SiRF 07), pp. 213-218.

[6] K.C. Eun, D.Y. Jung, J.J. Lee, S.J. Cho, H.Y. Kim, I.S. Song, Y.C. Lee, W.I. Chang, I.Y. Oh, J.H. Bang, C.S. Park, "LTCC SoP integration of 60 GHz transmitter and receiver radios, in Proc. of Asia-Pacific Microwave Conference 2008 (APMC 08), pp. 1-4.

[7] S.P. Voinigescu, T. Chalvatzis, K.H.K. Yau, A. Hazneci, A. Garg, S. Shahramian, T. Yao, M. Gordon, T.O. Dickson, E. Laskin, S.T. Nicolson, A.C. Carusone, L. Tchoketch-Kebir, 0. Yuryevich, G. Ng, B. Lai, and P. Liu "SiGe BiCMOS for analog, high-speed digital and millimetre-wave applications beyond 50 GHz", in Proc. of BiCMOS Circuits and Technology Meeting 2006 (BCTM 06), pp. 1-8.

[8] G. Avenier, M. Diop, P. Chevalier, G. Troillard, N. Loubet, J. Bouvier, L. Depoyan, N. Derrier, M. Buczko, C. Leyris, S. Boret, S. Montusclat, A. Margain, S. Pruvost, S.T. Nicolson, K.H.K. Yau, N. Revil, D. Gloria, D. Dutartre, S.P. Voinigescu, and A. Chantre, "0.13 µm SiGe BiCMOS technology fully dedicated to mm-wave applications", IEEE J. of Solid-State Circuits, vol 44, n°9, 2009, pp. 2312-2321.

[9] W.D. Van Noort, A. Rodriguez, Hong Jiang Sun, F. Zaato, N. Zhang, T. Nesheiwat, F. Neuilly, J. Melai, and E. Hijzen, "BiCMOS technology improvements for microwave application", in Proc. of BiCMOS Circuits and Technology Meeting 2008 (BCTM 08), pp. 93-96.

[10] Thomas H. Lee, "Planar Microwave engineering", Cambridge University Press, ISBN 0-521-83526-7, 2004.

[11] Zequan Guo, Jiamming Zhou, Ming Wei, and Boyu Li, "Ku-band filters using open-loop and quarter-wavelength resonators based on LTCC technology", in Proc. of 2nd International Conference on consumer electronics, Communications and Networks 2012 (CECNet 12), pp. 1104-1107.

[12] Yuta Takagi, Kei Satoh, and Shoichi Narahashi, "New Approach for Configuring a parallel-planar dual-band bandpass filter by employing multilayered LTCC technologies", in Proc. of IEEE Radio and Wireless Symposium 2012 (RWS 12), pp. 147-150.

[13] T.Y. Huang, T.M. Shen, and R.B. Wu, "LTCC embedded laminated waveguide filters and couplers for microwave SiP applications", in Proc. of IEEE Electrical Design of Advanced Packaging and Systems Symposium 2011 (EDAPS 11), pp. 1-4.

[14] S.M. Wu, M.H. Huang, C.H. Li, C.T. Kuo, and P. H. Yu, "A novel miniaturized coupled bandpass filter realized in laminate substrate", in Proc. of the Asia-Pacific Microwave Conference 2011 (APMC 11), pp. 1929-1932.

[15] F. Murray, "Silicon based system-in-package : a passive integration technology combined with advanced packaging and system based design tools to allow a breakthrough in miniaturization", in Proc. of BiCMOS Circuits and Technology Meeting 2005 (BCTM 05), pp. 169-173.

[16] C. Boucey, "Design and realisations of integrated filters on silicon for TV on mobile", in Proc. of National Micro-Wave Days 2007 (JNM 07), pp. 1-4.

[17] L. Martoglio, E. Richalot, G. Lissorgues-Bazin, and O. Picon, "Low-cost inverted line in silicon/glass technology for filter in the Ka-band", IEEE Trans. on Microwave Theory. and Techniques., vol. 54, n°7, 2006, pp. 3084-3089.

[18] R. Dekker, P.G.M. Baltus and H.G.R. Maas, "Substrate transfer for RF technologies", IEEE Trans. on Electron Devices, vol. 50, n°3, March 2003, pp. 747-757.

[19] V. Sridharan, "Design and fabrication of bandpass filters in glass interposer with through-package-vias (TPV)", in Proc. of IEEE Electronic Components and Technology Conference 2010 (ECTC 10), pp. 530-535.

[20] Z. El Abidine and M. Okoniewski, "High-quality factor micromachined toroid and solenoid inductors", in Proc. of European Microwave Integrated Circuit Conference 2007 (EuMIC 07), pp. 354 357.

[21] F. Hettstedt, H. Greve, U. Schurmann, A. Gerber, V. Zaporojtchenko, R. Knockel, F. Paupel, and E. Quandt, "Toroid microinductors with magnetic nano composite cores", in Proc. of European Microwave Conference 2007 (EMC 07), pp. 270-273.

[22] M. Duplessis, O. Tesson, J.R. Tenailleau, F. Neuilly, and P. Descamps, "Physical implementation of 3D integrated solenoids within silicon substrate for hybrid IC applications" , in Proc. of European Microwave Conference 2009 (EMC 09), pp. 1006-1009.

[23] J.B. Yoon, B.K. Kim, C.H. Han, E. Yoon, and C.K. Kim, "Surface micromachined solenoid on-Si and on-glass inductors for RF applications", IEEE Electron Device Letter, vol. 20, n°9, September 1999, pp. 487-489.

[24] O. Tesson, "High density inductor, having high quality factor", Patent WO 2009/128047, 2009.

[25] S.S. Mohan, M. del Mar Hershenson, S.P. Boyd, and T.H. Lee, "Simple accurate expressions for planar spiral inductances", IEEE J. of Solid-State Circuits, vol. 34, n°10, 1999, pp. 1419-1424.

[26] S. Kim and D.P. Neikirk, "Compact equivalent circuit model for the skin effect", in Proc. of IEEE International Microwave Symposium 1996 (MTT-S 96), vol. 3, pp. 1815-1818.

[27] M. Duplessis, "Contribution to RF characterization and modeling of 3D interconnection – through silicon vias – dedicated to a system in package", PhD Thesis, University of Caen Basse-Normandie France, November 2010.

[28] Cadence Design Systems, "Cadence QRC Extraction Datasheet", http://www.cadence.com/products/rf/qrc extraction/pages/default.aspx, 2011.

[29] I. Kelander, A.N. Arslan, L. Hyvonen, and S. Kangasmaa, "Modeling of 3D packages using EM simulators", in Proc. of 8th IEEE Workshop on Signal Propagation on Interconnects 2004, (SPI 04), pp. 186-189.

[30] R. Jackson, "A circuit topology for microwave modeling of plastic surface mount packages", IEEE Trans. Microwave Theory and Techniques, vol 44, n°7, July 1996, pp. 1140-1146.

[31] F. Alimenti, P. Mezzanotte, L. Roselli, and R. Sorrentino, " Modeling and characterization of the bonding-wire interconnection ", IEEE Trans. Microwave Theory and Techniques, vol 49, n°1, January 2001, pp. 142-150.

[32] A.I. Zverev, "Handbook of filter synthesis", ISBN 10: 0471986801, Wiley Inter-Science, 1967.

[33] A.E. Ruehli, "Inductance calculations in a complex Integrated circuit environment", IBM J. Res. Develop., September 1972, pp 470-481.

[34] G. Zhong and C. Koh-Koh, "Exact closed form formula for partial mutual inductances for on-chip interconnects", in Proc. of IEEE International Conference on Computer Design 2002 (ICCD 02), pp. 1349-1353.

[35] O. Tesson, S. Jacqueline, M. Duplessis, and P. Collander, "Hybrid integration of a decoupling system up to 6 GHz – 3D silicon based IPD combined with local interconnect modeling", in Proc. of International Microelectronics and Packaging Society 2009 (IMAPS Nordic 09), pp. 45-50.

[36] D. Brady, "The design, fabrication and measurement of microstrip filter and coupler circuits", High Frequency Electronics, pp. 22-30, July 2002.

[37] J.H. Lau, " Evolution, challenge, and outlook of TSV, 3D IC integration and 3D silicon integration", in Proc. of International Symposium on Advanced Packaging Materials 2011, (APM 11), pp. 462-488.

[38] J.S. Kofol, B.J.F. Lin, M. Mierzwinski, A. Kim, A. Armstrong, and R. Van Tuyl, "A backside via process for thermal resistance improvement demonstrated using GaAs HBTs", in Proc. of 14th Annual IEEE Gallium Arsenide Integrated Circuit Symposium (GaAs IC 92), 1992, pp. 267-270.

[39] R.J. Shul, M.L. Lovejoy, J.C. Word, A.J. Howard, D. Rieger, and S.H. Kravitz, "High rate reactive ion etch and electron cyclotron resonance etching of GaAs via holes using thick polyimide and photoresist masks", Journal of Vacuum Science & Technology B: Microelectronics and Nanometer Structures, vol 15, n°3, 1997, pp. 657-664.

[40] T. Quémerais, L. Moquillon, J.M. Fournier, and P. Benech, "65-, 45-, and 32-nm aluminium and copper transmission-line model at millimeter-wave frequencies", IEEE Transactions on Microwave Theory and Techniques, vol. 58, n°9, 2010, pp. 2426-2433.

[41] O. Tesson, "Electrical characterisation of on-silicon CPW lines for mm wave applications", Internal NXP report, June 2008, unpublished.

[42] Y. Yuanwei, Z. Yong, and Z. Jian, "Monolithic silicon micromachined Ka-band filters", International conference on Microwave and Millimeter Wave Technology 2008 (ICMMT 08), vol 3, pp. 1397-1400.

[43] Y.H. Cho, D.Y. Jung, Y.C. Lee, J.W. Lee, M.S. Song, E.S. Nam, S. Kang, and C.S. Park, "A fully embedded LTCC multilayer BPF for 3-D integration of 40-GHz radio", IEEE Transactions on Advanced Packaging, vol. 30, n°3, 2007, pp. 521-525.

[44] L.F. Tiemeijer, R.M.T. Pijper, R.J. Havens, and O. Hubert, "Low-loss patterned ground shield interconnect transmission lines in advanced IC processes", IEEE Transactions on Microwave Theory and Techniques, vol. 55, n°9, 2010, pp. 561-570.

[45] K. Nishikawa, S. Tomohiro, T. Ichihiko, and K. Shuji, "Compact 60-GHz LTCC stripline parallel-coupled bandpass filter with parasitic elements for millimeter-wave system-on-package", in IEEE MTT-S Int. Dig., June 2007, pp. 1649-1652.

[46] J.-H. Lee, S. Pinel, J. Laskar, and M. M. Tentzeris, "Design and development of advanced cavity-based dual-mode filters using low-temperature co-fired ceramic technology for V-band gigabit wireless systems", IEEE Trans. Microw. Theory Tech., vol. 55, n°9, Sept. 2009, pp. 1869-1879.

Dependable Estimation of Downtime for Virtual Machine Live Migration

Felix Salfner
SAP Innovation Center Potsdam
Potsdam, Germany
felix.salfner@sap.com

Peter Tröger and Matthias Richly
Hasso-Plattner-Institute at University of Potsdam
Potsdam, Germany
peter.troeger@hpi.uni-potsdam.de
matthias.richly@student.hpi.uni-potsdam.de

***Abstract*—Modern virtualization environments allow the live migration of running systems for load balancing and failover purposes in case of failing hosts. The overall duration of such migration and the short downtime during this process are essential properties when implementing service availability agreements. However, both metrics are currently only determinable through direct experimentation. For this reason, we present a new model for estimating the worst-case values of migration time and downtime in live migration. The prediction is based on a small set of input parameters characterizing the application load and the behavior of the host. We performed a large set of experimental evaluations for the model with three different virtualization products. The results show that total migration time as well as downtime are mainly influenced by the memory utilization pattern inside the virtualized system. The experiments also confirm that the proposed model can predict worst-case live migration performance with high accuracy, rendering the model a useful tool for implementing proactive virtual machine migration.**

***Keywords*-virtual machine; live migration; downtime analysis;**

I. Introduction

The concept of virtualization is known in computer science and IT industry since the late 60's [1]. Today, virtualization can be considered a standard technique in data centers. It is the foundation of modern computing and storage infrastructures such as used in cloud computing. Virtualization provides the following main advantages:

- *Hardware consolidation*. When running a software service on a server, the provider must offer enough capacity to handle peak load. This leads to under-utilization of the resources for most of the time. Virtualization enables the execution of multiple logical servers on the same physical host, which helps to reduce the total number of servers in the data center.
- *Load balancing*. Virtualization allows to control the assignment of physical server resources, such as memory and CPUs, to virtual machines. This assignment can even be changed during runtime. Additionally, services can be moved from one physical host to another by *virtual machine migration*. These techniques are used to manage and balance the load of services.
- *Maintenance*. In the case that maintenance needs to be performed at some physical host, virtual machine migration can be used to move virtual machines away so that the service can be provided while the physical machine is under maintenance.

First approaches to implement migration of a virtual machine relied on suspending the virtual machine before the transmission. In order to reduce the resulting downtime of the virtualized system, researchers and later on vendors turned to so-called *live migration* which reduces virtual machine downtime significantly. Today, the majority of virtualization products support live migration for moving a running virtual machine (VM) to a new physical host with minimal service interruption. This renders live migration an attractive tool also for dependable computing. However, each migration procedure still consumes time and still involves some short service unavailability. In the context of dependable computing the length of both time intervals are of great interest for two reasons: Service availability and proactive fault management.

Hosting a service in a data center is usually accompanied by a service level agreement (SLA) that promises some level of *service availability*. SLAs include not only such requirements, but also penalties if the agreed-on level of service is not met. In case that the service interruption introduced by live migration exceeds the client's expectation on responsiveness, a service unavailability is perceived that decreases overall service availability. Therefore, it is important for data center providers to estimate the worst case downtime for virtual machine migration as precise as possible. This becomes particularly important if the service should be migrated repeatedly following a predefined schedule.

The key notion of *proactive fault management* is to act upon a potential failure even before the failure has actually occurred. The goal is to either perform some action that is able to prevent an imminent failure so that it does not occur or to prepare recovery mechanisms for the likely occurrence of a failure. Both types of actions improve availability, by increasing mean-time-to-failure (MTTF) and decreasing mean-time-to-repair (MTTR). Virtual machine migration has been proven to be an effective tool for proactive fault management (see, e.g., [2]).

One of the key components of any proactive fault management is an online failure predictor that is able to accurately

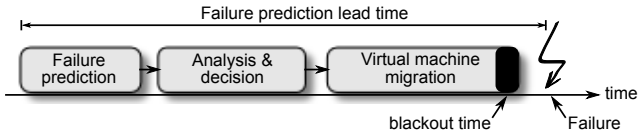


Figure 1. Time intervals involved in proactive fault management. The total duration of virtual machine migration needs to be known in order to determine the necessary failure prediction lead time.

identify imminent failures ahead of time. This must be performed during runtime based on monitoring data (see, e.g., [3] for an overview). Accuracy in this context means that it identifies as many true failures as possible with as few false alarms as possible. Accuracy is inversely related to the length of the time interval how far prediction reaches into the future, which is called the *failure prediction lead time* (see Figure 1): Prediction of failures that happen in the very near future (short lead time) is easier, i.e., more accurate, than a prediction that reaches further into the future (longer lead time). However, short lead times also require faster preventive counter-measure to be conducted. Most failure prediction algorithms allow to adjust their lead time. It should be as short as possible for maximum accuracy, but it has to be sufficiently long such that there is enough time to analyze the current situation, to decide upon which action to take and finally to execute and finish the action before the failure strikes (see Figure 1). In the case of applying virtual machine migration as proactive action, it is hence imperative to have a robust estimate of the maximum duration of the migration procedure.

A. Problem statement and contribution

The majority of existing work assumes some fixed, in many cases arbitrary, duration of the live migration procedure and the virtual machine downtime involved by it. This article systematically investigates the factors determining the duration and downtime of VM live migration (Section II). Building on this analysis, we propose a theoretical model by which the worst-case migration time and downtime can be estimated based on only a few well-defined parameters (Section IV). We demonstrate that our worst-case estimator is making accurate predictions by experiments using a worst-case synthetic load generator (Section VI) and by two benchmark applications for typical data center workload (Section VII).

This article is an extension to our previous work [4]. Whereas previous work focused solely on measuring the effects of various parameters such as the rate at which memory pages become dirty, this work introduces an analytic model that enables to estimate and predict the duration and downtime of virtual machine live migration. We test the estimator using the same load generator that was used in [4] and additionally performed experiments with two benchmark applications.

II. Related Work and Foundations

System virtualization has been a traditional approach for hardware consolidation and resource partitioning in the history of IT systems. The first operating system offering complete virtualization support was CP-40 by IBM in the 1960s. This first design was invented for time sharing operation of virtualized S/360 instances, and still acts as conceptional foundation for all later IBM virtualization technology in the mainframe area.

Meanwhile, virtualization also gained larger attention as research and development topic for other processor platforms. Popek and Goldberg formulated in 1974 [5] a set of essential characteristics for virtualizing *host* system resources for a *guest* operating system:

- *Equivalence*: The execution of software in a virtualized environment should be identical to the execution on pure hardware, despite timing effects.
- *Efficiency*: The majority of code running in the virtualized environment should run at native speed.
- *Resource Control*: The virtualization environment must have exclusive control over the physical hardware resources.

The same publication introduced the notion of a *virtual machine monitor (VMM)* that acts as execution platform fulfilling the given conditions.

Traditionally, the VMM is executing virtual machine instances in a less-privileged processor mode, in order to control relevant system state changes performed by the virtualized system. Popek and Goldberg classified the guest processor instructions accordingly: *Privileged instructions* lead to a hardware trap when they are executed in an unprivileged system mode, and *sensitive instructions* show a behavior that depends on the current system state (e.g. memory, registers). The most relevant aspect for any VMM solution is the handling of instructions that are sensitive, but not privileged.

Adams and Agesen [6] describe three major building blocks for a VMM implementation to deal with the obstacles of a given instruction set architecture. *De-privileging* makes use of the nature of privileged instructions by executing the guest operating system in a lower privilege level of the CPU. The handling of hardware traps occurring from the execution of privileged instructions in this mode is implemented by the VMM, based on a distinct virtual machine state. This relies on *shadow structures* of the hardware state (memory, processor registers) relevant for execution of the guest operating system. When unprivileged instructions can modify relevant system state too, the VMM must also implement *tracing* of such changes by built-in hardware protection mechanisms. One example is the modification of page table entry information to trap on unprivileged memory access operations in the guest operating system.

With the revival of virtualization in recent years, different

optimization strategies were introduced for performance reasons. One is the tighter integration of guest operating system and VMM by implementing a dedicated communication path. This concept, commonly known as *paravirtualization*, relaxes the original equivalence condition by Popek and Goldberg in favor of efficiency improvements.

If the guest software system must remain unchanged, there are two major approaches to deal with critical instructions. A *software-only VMM* implementation utilizes binary translation techniques for critical instructions. Typical solutions apply dynamic late translation during run-time to keep the performance penalty at a minimum. In contrary, a *hardware-assisted VMM* implementation can utilize virtualization support from the physical hardware devices. Modern processor architectures support the management of shadow structures and the de-privileging of guests as explicit features in the instruction set, which reduces again the overhead in comparison to software approaches. Examples are Intel VT, Intel EPT or AMD-V. Most of these techniques rely on the configuration of privileged instructions as part of the *virtual machine control structure* [6] in the processor hardware.

A. Investigated hypervisors

With the given variety of modern VMM approaches, we focused our investigations on three representative system virtualization products. The *Kernel-based Virtual Machine (KVM)* is a hardware-assisted open source VMM for Linux as host operating system [7]. Starting from the Linux kernel version 2.6.20, it is part of the main line and therefore available on all hosts. The virtualized devices for guest systems are provided by a modified version of the QEMU system emulator.

Xen is an open source VMM solution that acts as bare-metal hypervisor. It uses a modified Linux or Solaris operating system as privileged guest in the so-called 'dom0' domain. This domain has exclusive hardware access and management privileges. Guest systems for Xen run in additional domains and access the hardware through paravirtualization interfaces provided by the 'dom0' domain. Xen Linux guests are executed in paravirtualized mode, which requires a modified kernel using the paravirtualization interfaces. For other operating systems, such as Windows, hardware-assisted virtualization is also available in Xen. Different performance studies have shown that the usage of hardware virtualization demands some consideration in the guest operating system configuration [8].

VMware vSphere is a commercial product line for virtualization that relies on *bare-metal* virtualization, meaning that there is no explicitly installed host operating system. KVM and vSphere do not demand changes to the guest operating system due to the utilization of virtualization hardware support. vSphere can also apply binary translation techniques to the guest system, in case the X86 processor hardware is not suited for virtualization support.

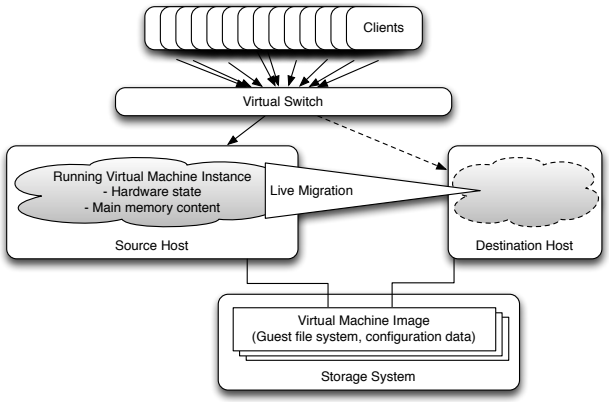


Figure 2. Principle of virtual machine live migration

B. Live migration of virtual machines

The migration of virtual machines is a stable feature of all modern hypervisor implementations, including the presented ones. Starting from early research prototypes ([9], [10]), companies such as VMware made this capability a part of their products since 2005.

Live migration describes the basic principle of moving a virtualized system from one host system to another while the guest is still running (see Figure 2). This activity must consider all hardware state, memory data, storage and network connections of the running virtual machine. Today's products realize this by a two-phase approach:

In the initial *warm-up phase*, the constantly changing main memory of the running guest is incrementally transferred to the destination host. When a product-specific threshold for main memory transfers is reached (time- or amount-based), the implementation switches to the *stop-and-copy* phase. The virtual machine is suspended for a short time period, the remaining resources are copied and the virtual machine is resumed on the destination host.

There are two relevant performance indicators for live migration arising from this concept:

- *Migration time* is the time from start of the live migration process until the virtualization framework declares the physical source host to be no longer relevant for the execution of the migrated virtual machine. The maximum tolerable migration time is determined by internal dependability assumptions at the provider side, e.g., maintenance intervals. It also plays a crucial role in proactive migration scenarios as motivated in Section I.
- *Downtime* or *blackout time* is the phase during live migration when there is a temporary (potentially user-perceptible) service unavailability, caused by the virtual machine suspending execution for the finalization of the movement. From a dependability perspective, blackout time is a crucial quantity when a virtualized service (e.g. server application) needs to fulfill reliability guar-

antees. Blackout time limits are therefore driven by dependability contracts between service provider and customer. Downtime and blackout time are used synonymously in this paper.

The most relevant part of live migration operation is the transfer of main memory state. Since live migration hosts share a common storage system within the migration cluster (see Figure 2), all information kept in the guest file system does not have to be considered. This relates especially to memory regions being swapped out by the memory management of the guest operating system. Some hypervisors also perform their own swapping of memory regions to secondary storage. Several virtualization frameworks use this property for reducing the length of the warm-up phase. A specialized *ballooning driver* allocates large amounts of memory inside the guest operating system, in order to enforce swapping of relevant memory information to secondary storage before migration.

Read-only memory regions (such as code pages) need to be copied to the destination host only once. This makes them a perfect candidate for bulk transfers in the warm-up phase. All remaining main memory information (data, stack, heap, ...) is potentially modified after the live migration process was started, and therefore needs a dedicated copying approach.

Clark et al. discuss the phases of copying memory information in more detail (see Figure 3) [11]:

In the initial *push phase*, the set of pages used actively is copied in rounds to the destination host. Memory regions being modified after transfer are re-sent, or marked for later bulk move when their modification happens too often. We define these modified but not yet transferred pages as *dirty pages*.

In the subsequent *stop-and-copy phase*, the virtual machine is suspended on the source host and resumed again on the destination host. The length of this phase determines the blackout time. Depending on the type of live migration, only portions or all of the remaining dirty pages are copied in this phase. In the former case, a sub-sequent *pull phase* takes care of moving remaining dirty pages from to source to the destination host on demand after VM execution has been resumed at the destination host. The end of the pull phase marks the end of the migration time. Most live migration products combine the first two phases as *pre-copy* approach, and omit the pull phase.

The time of transition from one phase to the next is controlled by product-specific adaptive algorithms. A quick move from push phase to stop-and-copy phase can have a positive influence on migration time, especially when the memory modification happens at high frequency. In contrast, a reduction of blackout time can be achieved by stretching the push phase so that nearly all memory is already transmitted before suspending the machine.

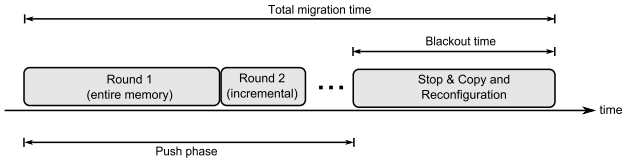


Figure 3. Phases of virtual machine live migration.

C. Analysis of Live Migration

In the area of dependable computing, virtual machine live migration has primarily been used as coarse-grained failover mechanism. Two examples are *proactive fault tolerance* [2] and the approach to resource allocation proposed by Fu [12].

A second group of related work deals with various aspects of implementing VM live migration. Several publications discuss the optimization of live migration and according usage scenarios, mostly with a focus on Xen technology.

Hines and Gopalan [13] discuss the modification of Xen for *post-copy* live migration. In this approach only the execution context of the VM is moved during the push-phase and memory pages are transferred on demand in the subsequent pull-phase after the VM has resumed execution on the destination host. The authors evaluate their solution with a stress test similar to the dirty page generator presented in this paper, the main difference being the distinction between read and write attempts in the memory load, as post-copy requires network interaction also on read attempts. This aspect is less relevant for the commercial products with pre-copy semantics, where read attempts can be served locally. However, for post-copy frameworks, our load model would need an extension with the access type as additional control parameter.

Sapuntzakis et al. [14] introduced several optimization approaches for VM live migration, among which *ballooning* is best-known, which forces the VM to swap out as much memory as possible. The performance investigation was conducted on a simulated work load with GUI end user applications, whereas our work targets server environments with periodic request-response interactions.

Du et al. [15] propose an extension of the Xen live migration mechanisms for improving overall migration performance. They identify the memory page re-writing rate as relevant factor for the migration time and downtime, which is in adherence to our results. The approach relies on a modification of the Xen hypervisor, whereas our work is intentionally restricted to un-modified standard virtualization products.

Nagarajan et al. [16] describe how to achieve pro-active fault tolerance through live migration in a high-performance computing environment. Experiments were conducted with several MPI benchmark applications, where the benchmark type defines the kind of load applied to the Xen live migration facility. Under the consideration of hardware

performance differences, the absolute migration time results from this study are similar to the ones obtained in our measurements. There were no investigations of downtime issues.

To the best of our knowledge this is the first work to introduce a prediction model for virtual machine live migration times and the involved blackout time. A work with close relation to this work is from Clark et al. [11], which – in addition to introducing the phases of live migration – investigates the effect of the size of the *writable working set*, which is the small set of memory pages that are updated too frequently to be coherently maintained on the destination machine. Based on different SPEC benchmarks as application-alike load generators, the authors developed a rate-adaptive algorithm to align the utilized bandwidth for memory pages transmissions. They also propose to stun processes that make live migration difficult. This corresponds to experiences with our Xen environment, where virtual machines with a running dirty page generator were marked as 'uncooperative'. The results are not directly comparable, since they focus on much smaller virtual machine sizes and application requirements.

Several publications discuss the application of live migration over Internet connections [17], [18]. The effects of network latency and bandwidth are more relevant in these cases, but from the perspective of migration load the load model remains the same.

III. Definitions and Assumptions

Having described the fundamentals of virtual machine live migration, a set of major influence factors can be identified that directly affect the performance of virtual machine live migration:

- System load on the source / destination host
- Capacity of the migration network link
- Static configuration of the migrated virtual machine
- System load of the migrated virtual machine

Specific higher-level activity (e.g., application workload) should also be reflected in these basic variables (see also Section VII).

For our further investigation in this article, we assume a typical (and recommended) setup with server applications only running in virtual machine installations. No additionally running processes with significant load are allowed on the physical hosts, except the hypervisor and its support code. This removes the physical host CPU load and memory utilization as control variables to be considered.

Concurrent system load could result from multiple large virtual machines being executed on the same host, so that they have to compete for host resources. This is typically denoted as *over-commitment*. One example is a scenario in which virtual machines with their configured RAM size sum up to an amount larger than the physical RAM available at the host. The hypervisor can make this possible through dedicated swapping to the attached storage system. In such cases, physical RAM for the virtualized operating system might have different performance characteristics, depending on the current over-commitment situation.

Since over-commitment would make hypervisor resource management strategies another variable to be controlled, we favored a performance-oriented system setup, where one virtual machine is running per host at a time. Similar behavior could be achieved by strict partitioning of hardware resources per virtual machine, which is common in mainframe virtualization. With standard processors, a pinning of virtual machines to physical CPUs and the avoidance of host memory exhaustion can lead to comparable results. If such a strong resource partitioning scheme is given, our results, which are based on a single host assumption, can also be applied for multiple virtual machines per physical host.

As final precondition, we assume that the network link between source and destination host has an appropriate available data rate, so that the live migration performance is not influenced by network saturation effects. Practical tests showed that current virtualization products handle the network capacity on the migration link carefully enough, so that this assumption appears valid.

With the given restrictions to static configuration and dynamic load of the migrated virtual machine, the following key factors can be identified:

1) CPU load inside the migrated virtual machine, based on a continuously running application.
2) Memory usage pattern of application and operating system inside the migrated virtual machine.
3) Main memory size configured for the virtual machine.

The memory usage pattern of the running virtual machine must be further separated into relevant factors for live migration performance. Since the memory transfer activities happen in parallel to the operation of the virtual machine, their characteristics can have a relevant impact on the migration performance.

We express the memory utilization pattern using four parameters (see also Figure 4):

The **virtual machine size (VMSIZE)** is the configured main memory size for the virtual machine. This is a constant value during run-time. In typical non-overload situations, the actually used amount of memory is much smaller.

The **working set (WSET)** is the region of the main memory on the source host that must be transferred to the destination host to finish the migration. This value can be roughly equal to the amount of main memory used by the guest operating system and all its processes, or can also be roughly equal to the configured amount of main memory for the virtual machine. This depends on the particular migration strategy of the hypervisor.

The **hot working set (HWSET)** is a subset of the WSET memory set. In our workload model, these memory regions are frequently changed while the migration is taking place.

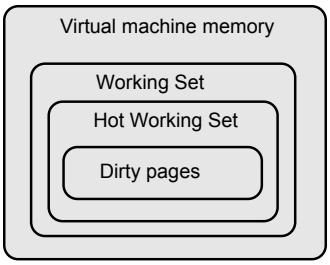


Figure 4. A classification of memory pages

The **modification rate (RATE)** expresses the average amount of memory modified per time unit while the migration takes place. The modifications described by this parameter are assumed to take place only in the memory region described by the HWSET parameter.

We distinguish the HWSET and the WSET to model the fact that there are different kinds of data stored in memory: some data are primarily read and have to be copied only once while others are subject to frequent updates and may have to be copied several times during the push phase, which affects overall live migration performance.

It should be noted that virtual machine live migration – and therefore all parameters listed above – rely on the concept of pages from operating system memory management. Amounts of memory and modification rates are hence expressed in pages but can easily be translated into bytes.

IV. A Predictor for Live Migration Downtimes

Based on the identification of core influence factors for live migration, we propose a predictor that allows to estimate both downtime and total live migration time for a specific application running at a specific (measurable) load. As indicated earlier, there are various use cases for such a predictor: For example, it can be used to plan SLA-bound data center operations, or it can be used to assess arbitrary load conditions which can be useful in system performance and reliability analysis.

The prediction model is based on a set of abstract parameters that express the memory load generated by a particular virtual machine instance, which has been introduced in Section III. Measurement of all parameters will be discussed in Section V.

A. Approach

In all existing virtualization frameworks, memory is managed at the level of memory pages and our model hence also works on this level of granularity. More specifically, the model estimates the number of pages that remain to be copied from the source to the destination host. As discussed in Sect. II, live migration copies the entire memory in a first iteration and then only copies pages that have become dirty. We presume that the number of remaining pages to copy is the key determining factor for the switch from pre-copy to the stop-and-copy phase, and therefore for the amount of time required for both migration and blackout time.

In order to determine the remaining number of pages we estimate the rate at which the number of dirty pages changes during the first iteration as well as during the subsequent copy rounds. The estimate is based on the workload parameters introduced in the last section, as well as on static execution environment characteristics.

The duration of the live migration procedure is determined by the sum of lengths of the various phases. More precisely, migration time is determined by the length of memory pre-copying in rounds, plus the time spent in the stop-and-copy and reconfiguration phase (see Figure 3). The decision to switch from pre-copy to stop-and-copy phase is always influenced by the number of pages that remain to be copied. There are two abstract conditions that can serve as trigger for changing from the first to the second phase:

1) *Condition 1:* The remaining number of memory pages to be copied is sufficiently small.
2) *Condition 2:* The pre-copy phase has already consumed a maximum amount of time.

When the live migration procedure hits one of the two boundaries it enters the stop-and-copy phase. An example for such a scenario is shown in Figure 5. It should be noted that Condition 2 is not present in all virtualization frameworks. In such cases the timeout can simply be set to infinity.

Figure 5 depicts the number of memory pages that remain to be copied over time. As can be seen from the Figure, our model distinguishes between the first round, in which the entire memory is copied, and the subsequent rounds, in which only pages that have become dirty are copied. The two stopping conditions are depicted by dash-dotted lines. The times of moving from one phase to the next are indicated as well. Time t_0 denotes the start of the live migration procedure, t_1 marks the end of the first round of memory page copying, t_2 the end of the pre-copy phase, and t_3 the end of the migration procedure.

B. Computing the Number of Remaining Pages

In order to determine migration times more precisely, we distinguish between different types of memory pages according to the classification shown in Figure 4. We estimate the progression of the number of pages that remain to be copied separately for each category:

- Unused memory pages (those that do not belong to the working set) do not contain data and can be copied in a compressed format and at a higher speed. The remaining number of such *empty* pages is estimated by $e(t)$. The rate at which such pages can be copied is denoted by $r_e \left[\frac{\text{pages}}{\text{s}}\right]$. Some hypervisor implementations might not copy empty pages at all, in which r_e equals infinity.
- Pages that belong to the working set but not to the hot working set need to be transferred only once. The

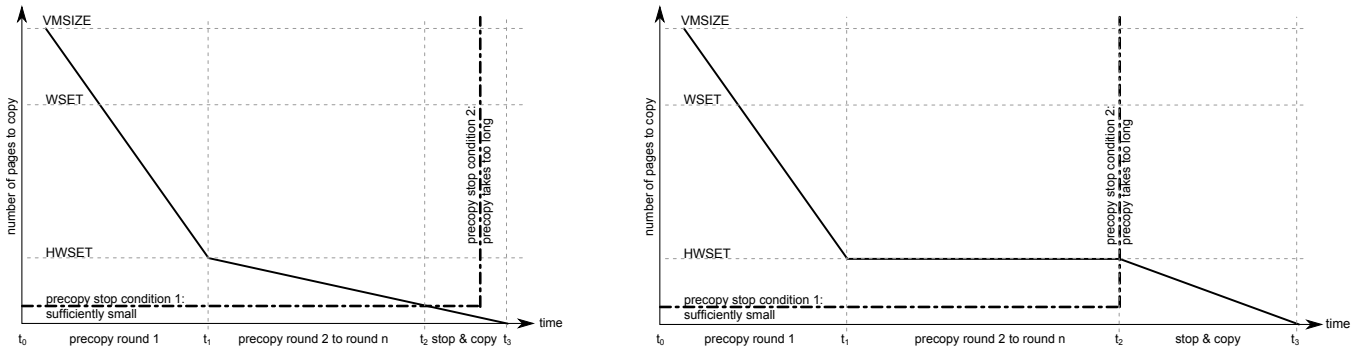


Figure 5. Prediction of live migration times. The predictor is based on the remaining number of dirty pages. The plot on the left shows the case where RATE is significantly smaller than the migration speed r_u. The plot on the right sketches the case when RATE is larger than the migration speed r_u.

remaining number of such *passive* pages is estimated by $p(t)$. The rate at which *used* memory pages can be copied is denoted by $r_u \left[\frac{\text{pages}}{\text{s}}\right]$.

- Pages that belong to the hot working set might become dirty between two successive rounds of copying. The remaining number of such pages is estimated by $h(t)$. These pages are also copied at a rate of r_u.

The number of remaining pages to be copied for a given point in time t is then determined by

$$f(t) = e(t) + p(t) + h(t) \tag{1}$$

The first round of copying in the pre-copy phase is significantly different from the subsequent rounds. Let t_1 denote the time of the end of the first round. We hence divide the definition of $f(t)$ in two phases ($t \leq t_1$ and $t > t_1$).

The remaining number of empty pages $e(t)$ is determined as follows:

$$e(t) = \begin{cases} \text{ESET} - r_e\, t & \text{for } 0 \leq t \leq t_1 \\ 0 & \text{for } t > t_1 \end{cases} \tag{2}$$

where

$$\text{ESET} = \text{VMSIZE} - \text{WSET} \tag{3}$$

is the set of unused, i.e., empty pages. Hence $e(t)$ describes the copying of unused pages at a higher rate. Since the pages in ESET are not used by the virtual machine, there is no contribution of $e(t)$ after the first round.

The remaining number of non-HWSET pages $p(t)$ is defined as follows:

$$p(t) = \begin{cases} \text{PSET} - \frac{\text{PSET}}{\text{WSET}}\, r_u\, t & \text{for } 0 \leq t \leq t_1 \\ 0 & \text{for } t > t_1 \end{cases} \tag{4}$$

where

$$\text{PSET} = \text{WSET} - \text{HWSET} \tag{5}$$

represents the passive (non-hot) working set. Hence $p(t)$ describes the copying of used, i.e., non-empty, pages that the virtual machine does not write to during the live migration process. Such pages have to be copied only once, which is the explanation why $p(t)$ equals zero in subsequent rounds of the pre-copy phase ($t > t_1$).

We assume that the system can copy non-empty memory pages at a fixed rate r_u. However, one fraction of non-empty pages are passive (they belong to PSET) while others are actively written to. We assume that the copy rate r_u is split proportionally among pages from within PSET and active non-empty pages (belonging to HWSET). Hence the copy rate equals $\frac{\text{PSET}}{\text{WSET}}\, r_u$.

The hot working set $h(t)$ is determined by

$$h(t) = \begin{cases} \min\left(\text{HWSET}, \max\left(0, h_1(t)\right)\right); & 0 \leq t \leq t_1 \\ \min\left(\text{HWSET}, \max\left(0, h_2(t)\right)\right); & t_1 < t \leq t_2 \\ h_3(t) & ;\ t_1 < t \leq t_3 \\ 0 & ;\ t > t_3 \end{cases} \tag{6}$$

The formula expresses that $h(t)$ stays within the interval $[0, \text{HWSET}]$. Not surprisingly, the number of remaining pages cannot be negative. The upper limit stems from the fact that applications and the operating system in a virtual machine write to only a subset of the working set – the hot working set HWSET. If RATE (the rate at which memory pages are written) becomes very large, the same pages within HWSET are written several times. The functions $h_1(t)$, $h_2(t)$, and $h_3(t)$ have been introduced for typesetting reasons, only. They express the evolution of the number of memory pages from within HWSET over time.

$$h_1(t) = \text{HWSET} + \left(\text{RATE} - \frac{\text{HWSET}}{\text{WSET}}\, r_u\right)\, t \tag{7}$$

$$h_2(t) = f(t_1) + (\text{RATE} - r_u)\, t \tag{8}$$

$$h_3(t) = f(t_2) - r_u\, t \tag{9}$$

As can be seen from (6), $h_1(t)$ determines the behavior for the first round in the pre-copy phase. As already mentioned, during this phase the copying of used, i.e., non-empty memory pages takes place at a rate of r_u, but the rate is split among passive and active pages (see explanations for Equation 4). The difference between pages of the hot working set (HWSET) and the pages of the passive working

set (PSET) is that hot working pages are written to with a rate determined by RATE. The progression of $h_1(t)$ is hence determined by the difference of the writing rate RATE and the fraction of the copy rate assigned to the copying of pages from the hot working set.

After the first round of copying has finished, copying progresses determined by the function $h_2(t)$. Now the full rate of non-empty page copying r_u can be assigned to the copying of pages from the hot working set, i.e., the copy rate is determined by the difference between RATE and r_u. Due to the use of the minimum operator in (6), it cannot be known a-priori what the value of $f(t)$ is at the end of the first round. We hence refer to this value by $f(t_1)$.

As discussed before, t_2 determines the end of the pre-copy phase, either caused by stop condition 1 or 2. At this point, the virtual machine is stopped and pages do not become dirty anymore. Hence the remaining dirty pages can be copied at the full rate r_u until no dirty pages are left. The latter time is denoted by t_3. Expression $h_3(t)$ describes the final copying. Again, since t_2 is determined by several factors, $f(t_2)$ cannot be known a-priori and we refer to the value $f(t_2)$ in (9).

C. Computing total migration and blackout time

So far we introduced $f(t)$, which estimates the number of memory pages that remain to be copied. However, the ultimate goal is to estimate both total migration time and blackout time of virtual machine live migration. As might have become clear already, both time intervals can be computed from t_2 and t_3:

$$\text{migration time} = t_3 - t_0 \tag{10}$$

$$\text{blackout time} = t_3 - t_2 \tag{11}$$

During the first phase all memory pages are copied once. Hence t_1 can be computed from the sizes of the empty and used memory pages, and the corresponding transmission rates. However, since the definitions of t_3 and t_2 are based on $f(t)$, we need to compute $f(t)$. Specifically, in order to compute t_2, the time of the intersection between $f(t)$ and break condition 1 needs to be determined.[1] The following equations provide the formulas to compute t_1 to t_3:

$$t_1 = \frac{\text{ESET}}{r_e} + \frac{\text{WSET}}{r_u} \tag{12}$$

$$t_2 = \min\left(t_{c1}, t_{c2}\right)) \tag{13}$$

$$t_3 = t_2 + \frac{f(t_2)}{r_u} \tag{14}$$

In (13), t_{c1} denotes the time when $f(t)$ equals the value of the pre-copy stop condition 1 and t_{c2} is the time predetermined by pre-copy stop condition 2. Finally, t_3 determines the end of the copying process and the time can be simply computed by how long it takes to transfer the remaining number of pages when entering the stop-and-copy phase, which is $f(t_2)$.

After the stop-and-copy phase some reconfiguration takes place. Assuming that such reconfiguration is constant and short and that copying memory pages is the determining factor, we neglect this aspect in our model. Results in subsequent sections will show that this already provides sufficiently accurate predictions of migration time and blackout time. We also assumed that the two rates r_e and r_u are independent, which is a valid assumption since the overhead for copying empty pages is very low or even zero, in case the framework does not copy them.

Table I lists the parameters that need to be determined in order to compute (10) and (11). The table lists four types of parameters:

- *Virtual machine-specific.* There is only one such parameter in Table I, which is VMSIZE. This parameter is statically configured when the virtual machine is set up.
- *Situation-specific.* These parameters require online measurements in the running virtual machine. If used for what-if-analyses, these are also the parameters that define the investigated scenario. The following Section V provides details about how situation-specific parameters can be measured.
- *System-specific.* Such parameters have to be determined once for any given setup of networking and physical host equipment. Section V provides an example of how such system-specific parameters can be obtained.
- *Hypervisor-specific.* There are two parameters that depend on the implementation and/or configuration of the hypervisor and which define the criteria to stop the pre-copy phase.

V. Experiment setup

To prove the feasibility of the presented prediction model, we conducted a large set of experiments with both artificial and real application load inside migrated virtual machines.

The test environment consisted of two Fujitsu Primergy RX300 S5 machines acting as migration source and destination. Both machines were equipped with an Intel E5540 QuadCore processor, 12GB of RAM and two Gigabit NICs each. One of the network cards per host was used for the dedicated migration network link. The other network card was used to connect the machine to a shared storage system via iSCSI. The storage system contained all virtual machine image data. If required a third machine was attached to the storage network as controller node.

In all experiments, the migrated virtual machine was either running a Linux 2.6.26-2 (64 bit) or a Windows Server 2008 R2 installation. All virtual machines were configured to have one virtual CPU and a varying amount of (virtualized) physical memory. In all cases, the virtualization guest tools / drivers were installed. Native operating system swapping

[1] t_{c1} has to be set to ∞ in the case that there is no intersection.

Table I
SUMMARY OF PARAMETERS OF THE PREDICTION MODEL

Parameter	Description	Type	Comment
VMSIZE	Configured memory size of the virtual machine	VM-specific	Setup of the the virtual machine
WSET	Working set (allocated memory)	Situation-specific	Measured during runtime
HWSET	Hot working set (actively used memory)	Situation-specific	Measured during runtime
RATE	Dirty page rate (rate at which pages are written)	Situation-specific	Measured during runtime
r_e	Transmission rate of empty pages	System-specific	Measured once for the system
r_u	Transmission rate of non-empty pages	System-specific	Measured once for the system
$c1$	Threshold value for pre-copy stop condition 1	Hypervisor-specific	Predetermined by the hypervisor
t_{c2}	Threshold value for pre copy stop condition 2	Hypervisor-specific	Predetermined by the hypervisor

was activated, but not aggressively in use due to the explicit limitation of the allocated amount of memory.

Experiments for VMware were performed using ESX 4.0.0 (build 208167), using the vCenter server software for migration coordination. High availability features had been deactivated. Experiments for Xen were performed using Citrix XenServer 5.6 (Xen 3.4.2). Both Xen hosts had been configured to form a pool, the test scripts were executed in the 'dom0' partition of the pool master. Experiments for KVM had been conducted with ProxmoxVE 1.7, which relies on QEMU 0.13.0 and a 2.6.32 Linux kernel.

One specific issue was memory management in the Xen environment, namely the *Dynamic Memory Control (DMC)* feature [19]. It allows the Xen hypervisor to change the amount of physical memory made available to the virtual machine at runtime, without reboot of the guest operating system. DMC is an advanced feature necessary to permit memory over commitment in Xen, since Xen never swaps out guest pages, as VMware or KVM do in case.

With activated DMC feature, it was observable that Xen tried to reduce the memory utilization by *ballooning* [14] inside the virtual machine instance before actually starting the migration process. This lead to problems with Linux as guest operating system, since its *out-of-memory (OOM) killer* wrongly assumed an out-of-memory condition from the many locked pages created by the load generator. In several constellations, the combination of DMC, our memory-locking load application and Xen led to random process termination by the OOM killer. We hence deactivated DMC explicitly to achieve repeatable measurements.

Total migration time was measured by capturing the runtime of the products command-line tool that triggers a migration. Downtime was measured by a high-speed ping (50 ms) from another host, since the virtualization products do not expose this performance metric by themselves. The downtime is expressed as the number of lost Ping messages multiplied by the ping interval. We assume here that all ping messages get lost in one continuous time interval during VM downtime.

A. Measuring memory utilization

In contrast to other performance metrics, the RATE parameter is not provided by the OS or any of the hypervisor products directly, probably because of the performance implied by monitoring memory activities. The usual operating system information about dirty pages is not usable here, since this information relates only to the pages not being swapped out by the memory management.

One possible solution could be to obtain direct information from the MMU hardware. Modern processors have special support to monitor low-level activities by performance monitoring units (PMUs). The utilization of such units is supported in Linux through the *libpfm* toolkit or the *perf_events* kernel interface.

We conducted a set of experiments to determine a set of hardware performance events that grow with the RATE parameter of an artificial load. It turned out that for the Intel Nehalem processor under investigation, 21 PMU events showed a strong correlation to the applied dirty page load. Even though this renders PMU a promising mechanism for memory activity monitoring, the application of this approach inside the virtual machine under test is still infeasible. The virtualization hardware and software simply does not support the necessary access to hardware registers.

Reading PMUs on the hypervisor level to infer memory activities of the virtual machine turned out to be infeasible, as we have confirmed in several experiments.

The second possibility for accurate measurements of the memory load is the hypervisor itself. By default, the virtualization products do not expose these metrics to the outside. Nevertheless, the hypervisor and its live migration facility use a tracking mechanism to identify pages that have become dirty. Therefore, we modified the source code of KVM slightly to facilitate measuring of the RATE parameter as will be documented in the next section.

B. KVM hypervisor extension for memory tracking

KVM consists of two parts, the KVM subsystem in the kernel and the qemu-kvm user space application. The user space application creates the virtual machine inside its own address space and communicates to the

KVM subsystem using I/O controls. The KVM kernel subsystem interfaces *KVM_SET_MEMORY_REGION* and *KVM_GET_DIRTY_LOG* allow the caller to keep track of dirty page state changes for the given virtual machine. KVM_SET_MEMORY_REGION can enable/disable dirty pages tracking, and KVM_GET_DIRTY_LOG returns a bitmap with all dirty pages since the last call. This allowed us to enable dirty page tracing on demand for measurements, even without having an actual live migration taking place.

C. Classifying hypervisor and system

The two system-specific parameters of our model, namely the transmission rates for empty and non-empty memory pages have been estimated using a virtual machine with a defined non-paged memory footprint as migrant.

In KVM, the hypervisor-specific parameters are determined by two parameters that can be passed to the hypervisor when initiating the live migration procedure. The number of pages that is considered to be sufficiently small is computed by the product of the KVM configuration parameters `migrate_speed` and `migrate_downtime`. The first parameter determines the maximum speed (in bytes per second) for the pre-copy phase of migrations while the second specifies the maximum tolerated downtime. If there are less remaining pages than `migrate_speed` × `migrate_downtime`, the stop-and-copy phase can be performed faster than the maximum tolerated time `migrate_downtime`.

For the pre-copy stop condition 2, the behavior of ProxmoxVE KVM can be expressed by the following equation:

$$t_{c2} = \frac{2\,\mathrm{VMSIZE}}{\texttt{migrate\_speed}} \tag{15}$$

This means that whenever the time has passed that would be sufficient to copy two times the entire virtual machine memory, the pre-copy mechanism is stopped and the remaining pages are copied at a modified rate in the stop-and-copy phase.

D. Determining situation-specific parameters

To determine the RATE parameter for dirty pages, we enabled the described dirty pages logging on all memory regions. Our modified KVM implementation measures the number of pages that have become dirty once every second. The RATE parameter is the average of the measured numbers.

The determination of the HWSET is more complex. We defined the HWSET to consist of all pages that are *frequently* changed. We estimated HWSET by determining the set of pages that have become dirty in a series of measurements. After computing the union of all pages that have become dirty in these measurements we counted only pages that have been marked dirty in a minimum number of measurements. The time interval between the individual measurements should be at least as long as we expect one migration pre-copy round to take, which is $WSET/migrate\_speed$ in the worst case. In our experiments with KVM, we used ten consecutive measurements within one minute and we considered only those pages as hot pages that were marked dirty in all ten measurements.

VI. Experiments with artificial load

Based on the theoretical investigation of relevant workload parameters and the described setup, we conducted a set of experiments for proving the feasibility of the model. In the first step, we conducted experiments with artificial work load generators. The intention was to stress the virtual machine migration in a controlled and reproducible way, before analyzing the impact of real-world application workload.

Since our set of relevant dynamic factors is restricted to the behavior of the guest operating system, we were able to perform all experiments with load generators inside the virtual machine. For the worst case analysis, we utilized load generators for CPU, locked pages and dirty pages.

The *CPU load generator* was used to produce artificial CPU load inside the virtual machine, in order to prove the independence of migration performance from the virtual machine computational load. We used the commonly known *burnP6* and *cpulimit* tools for generating a controllable CPU utilization. Our experiments proved that CPU load has negligible impact on virtual machine migration (see also [4]).

The *locked pages generator* was used to analyze the effects of static memory allocation. With this tool, locked pages are pinned in memory through operating system calls so that they cannot be swapped out. This ultimately increases the WSET value alone, without influence on both RATE and HWSET. The implementation first allocates a given amount of locked pages memory. In the next step, random data is written once to this memory region, in order to trigger delayed page table modification schemes in the operating system [20]. After that, the according regions are pinned by a system call.

The *dirty pages generator* was developed to artificially influence HWSET and RATE parameters in an experimental environment. This load application simulates a cyclic memory modification pattern by continuously writing pre-computed random data to pinned memory in round-robin fashion. This execution model is motivated by server applications that modify memory regions based on incoming requests. Those modifications have comparable characteristics for the majority of requests. Such servers are always reading some data, storing logging information in main memory, and return the computational result. The request inter-arrival time is assumed to show a constant average rate, so the modification attempts in memory can be modeled just by using parameters expressing the frequency and intensity of using a block of memory.

In order to remove systematic errors, a proper design of experiments usually demands randomization of the runs. In our scenario, an experiment is the migration of a virtual machine for a specific configuration of parameters. Randomizing this would identify potential unconsidered influences on the dependent variables. However, due to the closed experimental environment (no other users had access to the machines), and full automation of the measurements, we expect no major additional influence on the dependent variables. Selective tests confirmed this assumption. We therefore relied only on measurement series with predefined continuous data ranges.

The migrated virtual machine was running a load generator in a fresh operating system installation only. Before migration start, several minutes of warm-up time have been reserved for the virtualized operating system.

A. Influence of CPU load

For the investigation of the influence of the CPU load factor, we performed at least 10 migrations per CPU utilization degree, ranging from 0% to 100% artificial load in steps of ten. The results show that migration times of all virtualization products are not influenced by the CPU load. More precisely, migration times varied around mean values of up to 26 seconds within a 95% confidence interval of not more than +/- 1s (see [21] for details). As additional feasibility test, we investigated Xen both with and without activated DMC feature, which had serious impact on the absolute migration time, but the impact of CPU remained negligible.

The results suggest that virtualization frameworks reserve enough CPU time for their own management (migration) purposes. Live migration scenarios seems to be dependent only on non-CPU utilization factors.

The result convinced us that we could safely drop CPU load as an influencing factor in subsequent experiments.

B. Influence of WSET and filling degree

Using the locked pages generator, we varied the WSET parameter from zero to 90% of the main memory configured for the virtual machine (VMSIZE).

Our results showed that the VMware hypervisor has a linear dependency of migration time on memory utilization, while the downtime is not influenced significantly. With Xen, both the downtime and the migration time remained nearly constant in all memory utilization scenarios. The Xen virtual machine migration time depends mainly on the absolute amount of configured main memory.

In order to rely on the trap and page table mechanisms of the operating system, all virtual machine migration approaches copy memory content in the granularity of pages. Hence, an entire page has to be migrated even when writing only to a fraction of a page. We tested this assumption by "filling" memory blocks inside the locked region to a varying degree. We used a block size equal to the system page size (4kB) and conducted experiments with varying filling degrees of such blocks. As expected, all three virtualization toolkits showed no effect on downtime or migration time.

Changing only a single bit in a memory page makes it dirty from the viewpoint of the hypervisor, and therefore also a relevant candidate for live migration. We see a relevant issue here for 64 bit systems with potentially larger page sizes. In such systems the overhead of migrating only marginally modified pages could become significant. For our purposes, the conclusion is that the filling degree does not have to be considered in subsequent experiments.

C. Influence of HWSET + RATE + VMSIZE

We conducted a large set of multi-parameter experiments with the dirty page load generator, in order to determine the basic patterns of influence in virtual machine migration. The goal here was to determine the different worst-case settings for the combination of HWSET, RATE and VMSIZE. For this reason, we performed experiments according to a full factorial design, meaning that all possible combinations of parameter levels have been measured in the experiment. In each experiment we measured migration time and downtime as response variables. For Xen, we investigated a total number of 528 combinations (treatments), each with 20 measurements resulting in an overall number of 10560 migrations. In case of the VMware hypervisor, we performed experiments for 352 combinations resulting in 7040 migrations. For KVM, we tested 1652 combinations resulting in 33040 migrations.

As we have three factors (plus a response variable) we cannot present the entire results in one plot. Since VMSIZE has significantly less levels, we decided to plot the mean response, i.e. mean migration time or downtime, over HWSET and RATE for a fixed value of VMSIZE. The experiments have been performed using the DPG load generator, which simulates worst-case behavior in terms of memory usage.

One example for the results is the behavior of the Xen hypervisor. Downtime in general increases with increasing HWSET and increasing RATE (see Figure 6). This is not surprising as an increased usage of memory (more pages written at an increasing rate) requires more memory to be transferred in the stop-and-copy phase. We can also conclude from the figure that HWSET seems to have a linear effect on downtime, if the RATE is above some threshold value and regardless of the VMSIZE. This threshold value is around 30,000 pages/s or 117 MB/s with 4KB pages, which corresponds well to the expected migration speed over a 1 Gigabit Ethernet link.

One peculiarity in Figure 6 is the abrupt change at a RATE level around $30{,}000\frac{1}{s}$. In order to analyze this further, we conducted additional "zoom-in" experiments that investigated a sub-range of values for RATE at greater level of detail (see Figure 8-a). As it can be seen from the plot,

the change is not as abrupt as might have been concluded from Figure 6.

Turning to total migration time (Figure 7), we observe a sudden change at the same level of RATE as we have observed for downtime. Again, the "zoom-in" analysis shows that the change is smooth although rather steep. However, in general the mean migration time is more irregular. It came as a little surprise to us that for RATE levels "above the jump" total migration time decreases with increasing RATE. In order to check that this behavior really occurs we have carried out separate experiments specifically targeted to this question with the same consistent result. Although we cannot give a precise explanation, we presume that it is caused by the rate-adaptive algorithm employed by the hypervisor. This supports our assumption that a load model is essential in order to assess duration of live VM migration.

The effect of VMSIZE can be observed by comparing the two sub-figures 7 (a) and (b). It can be seen that VMSIZE has a non-trivial effect on migration time: since the shapes look very different at different levels of VMSIZE, the effect does not appear to be linear, except for the case where RATE equals zero.

There is no effect of any HWSET value if RATE is zero, which is consistent with the single variable experiments described in Section VI-B.

The plots in Figures 6 to 8 show migration times averaged over all measurements. In order to assess the variability in the data, we describe the ratio of maximum to minimum values as well as standard deviation for the data in Table II. Two ratios and two standard deviations are reported: the ratio of the maximum treatment mean to the minimum treatment mean and the ratio of the maximum to the minimum values across all measurements. Regarding standard deviations, the table describes the largest standard deviation computed within each treatment (parameter combination) as well as the standard deviation for the overall data set. In addition, the table reports the mean time averaged across all measurements. The data quantifies what has also been observable from the plots: Both migration time as well as downtime vary tremendously depending on VMSIZE and RATE.

For XenServer, one can observe that downtime is only 8.6% of the overall migration time. The fact that the overall standard deviation is far greater than the within-cell standard deviation supports the observation that there is a strong systematic variability in the live migration algorithm.

For KVM, Figure 9 and Figure 10 show the behavior under different conditions for HWSET and RATE. While the downtime behavior is comparable to Xen, the migration time development shows a completely different behavior. Here, above a certain RATE the migration times line up at a constant level, which is independent of the HWSET. A comparison of the two subfigures shows that this level is dependent on the VMSIZE. What we see here is the effect of the second stop condition explained above, which strikes if the RATE is larger than the effective migrate speed.

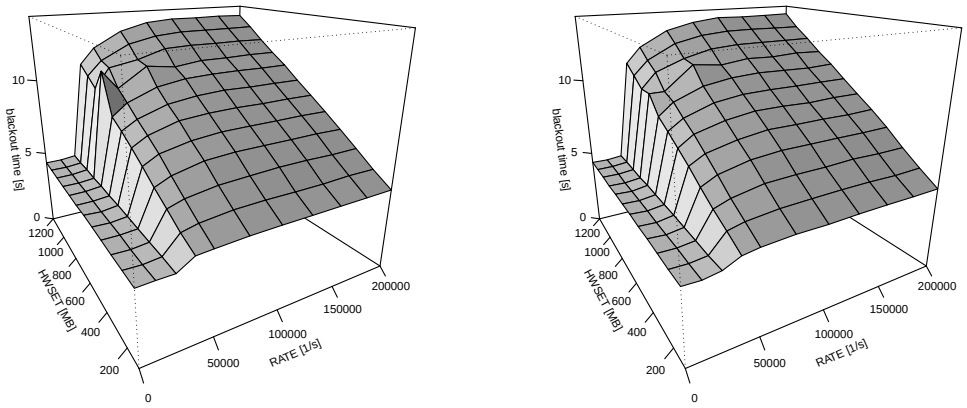
Since the VMware end user license agreement does not allow the publication of performance numbers, we omit the presentation of the gathered data here. We can report that the observed behavior of vSphere differs significantly from the one of Xen, which emphasizes that the choice of the hypervisor product can have significant impact on availability. The main reason for the different behavior seems to be the different rate-adaptive algorithms employed in the virtualization products. Rather than arguing which behavior is better we want to emphasize that it is mandatory to take the specific virtualization product into consideration when making assumptions on migration duration.

Regarding the max:min ratio of downtime computed from treatment means with VMware, we have observed a ratio of 16.27. This shows that due to different memory load, the maximum mean downtime can be 16.27 times as large as the minimum mean downtime. If we do not consider mean downtimes but the maximum and minimum value observed across all experiments, the factor even goes up to 23.83. The conclusion from this observation is that if service downtime is critical for meeting reliability goals, a realistic assessment of reliability can only be achieved if the maximum downtime for the application-specific memory load is figured out, which is the goal of our prediction model.

D. Comparing the predictor with experimental results

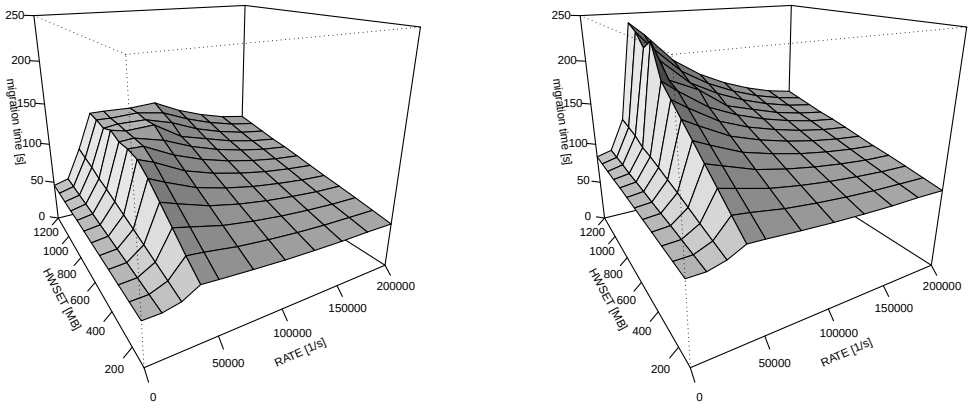
In order to test the feasibility of our predictor model, we compared the experimental results for KVM with the theoretical worst case assumptions from our model. We relied on the KVM results here, since the hypervisor modifications described in Section V-B allowed a fine-grained monitoring of the relevant metrics. Figure 11 shows the comparison for blackout time and migration time. In the absolute majority of cases, the model was able to provide a worst case prediction close to the real-world experiment results:

- For a total of 33040 measurement points, the model predicted migration times that were larger or equal to the corresponding measured migration times in 95.6% of the measurements. For blackout time, the predictor was right in 97.08% of the cases.
- The average absolute error, meaning the distance between the computed worst case value and the measured value, for the migration time prediction was 25,75s. For blackout time prediction, the average absolute error was 2,45s.
- The average under-prediction, meaning average error in the cases where the predicted value was below the actual measured value, was 2,95s for the migration time. For blackout time, the average was 0.13s.



(a) VMSIZE=4096 (b) VMSIZE=8192

Figure 6. Mean downtime for Xen



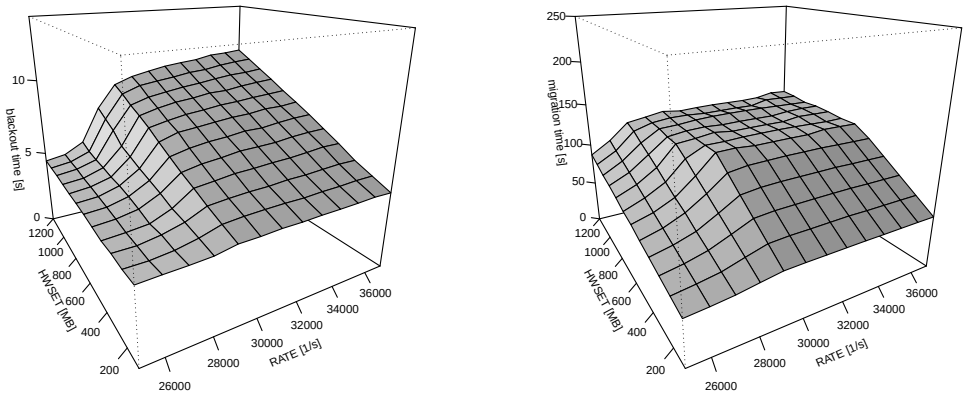
(a) VMSIZE=4096 (b) VMSIZE=8192

Figure 7. Mean migration time for Xen

E. Discussion

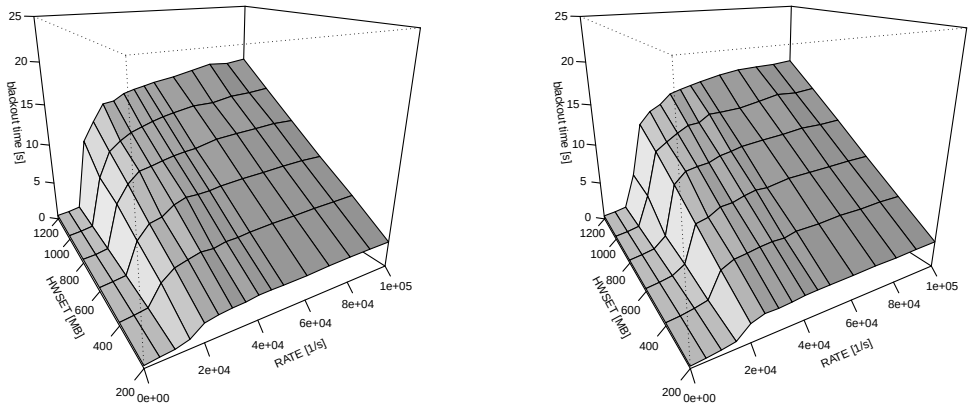
The statistical evaluation proves that our prediction model worked in more than 95% of the worst case load tests, which is especially important for dependability-related use cases. If a proactive failure predictor is able to implement a lead time larger than the worst case value from the migration time prediction model, than virtual machine migration can be used as preventive recovery strategy.

In order to understand the experiment results in more detail, we performed a source code analysis of Xen and had personal communication with VMware representatives. Live migration in fact is mainly related to the rate-adaptive migration control algorithm realized in the product. The relevant aspect here is the dirty page diff set – the fraction of pages that is scheduled to be copied in each next round of the pre-copy phase. The virtualization products identify ”hot pages” in this set and shift such pages more aggressively to the stop-and-copy phase, since the transfer in the stop-and-copy phase is potentially more effective, depending on “hotness” of the page, network link speed and other factors. This also appears to be an explanation for the increasingly large gap between predicted and measured migration and blackout times for large memory allocation sizes. Future extensions to our prediction model could take such effects



(a) Mean Downtime (b) Mean Migration Time

Figure 8. Xen behavior in the zoom-in area (VMSIZE=4096)



(a) VMSIZE=4096 (b) VMSIZE=8192

Figure 9. Mean downtime for KVM

into account to improve prediction accuracy.

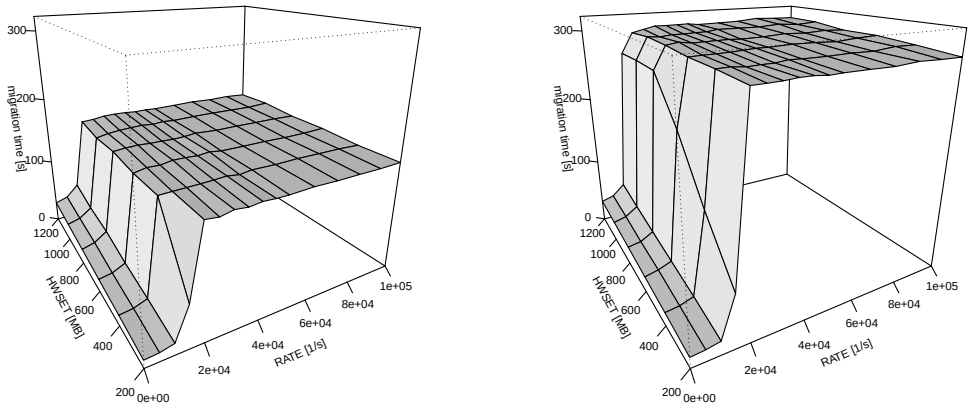
Akoush et al. [22] made similar investigations in their live migration performance analysis. Surprisingly, the downtime seems not to be influenced by the chosen strategy, which can be explained by the broad transmission capacity of the network link. Comparative measurements of the network saturation supported this assumption.

VII. Experiments with Real Load

For a further proof of the proposed migration and blackout time prediction model, we conducted another large set of experiments with real application load. We decided for two typical server application representatives – the SPEC jAppServer benchmark, and the Postal SMTP server benchmark in conjunction with the Postfix mail server.

A. SPEC Benchmark Results

The first set of tests relied on the SPEC jAppServer 2004 1.08 benchmark application. This program is intended to measure the performance of Java 2 Enterprise Edition (JavaEE) application servers. The benchmark simulates manufacturing, supply chain management, and order/inventory business processes. It consists of a database part and several JavaEE applications to be deployed. A driver component



(a) VMSIZE=4096

(b) VMSIZE=8192

Figure 10. Mean migration time for KVM

Table II
DATA VARIABILITY

Hypervisor / Guest	time	Mean time [s]	Max:Min Ratio		Standard Deviation	
			Mean	Overall	Treatment Max [s]	Overall [s]
XenServer / CentOS	migration	89.73	9.01	9.10	6.32	39.08
	downtime	7.69	3.17	3.46	0.62	2.94

simulates parallel client requests, where the request rate is controlled by a parameter called *txRate*.

We performed measurements for a total of ten configurations, each corresponding to a specific setting of the benchmark's *txRate* parameter (see Table III). For each setting we conducted more than 2300 migration experiments to collect statistically significant data. In each experimental run we measured total migration time and blackout time of the migration. We also determined for each configuration the values for WSET, HWSET and RATE using our modified KVM hypervisor.

Figure 12 shows the experimental results. The graphs plot measured blackout times (Fig. 12-a) and measured migration times (Fig. 12-b) together with the times predicted by our model. For measured blackout and migration times we also plotted 95% confidence intervals shown by vertical bars. We decided to plot absolute times rather than relative prediction accuracy since in real world dependable application scenarios absolute numbers are much more relevant.

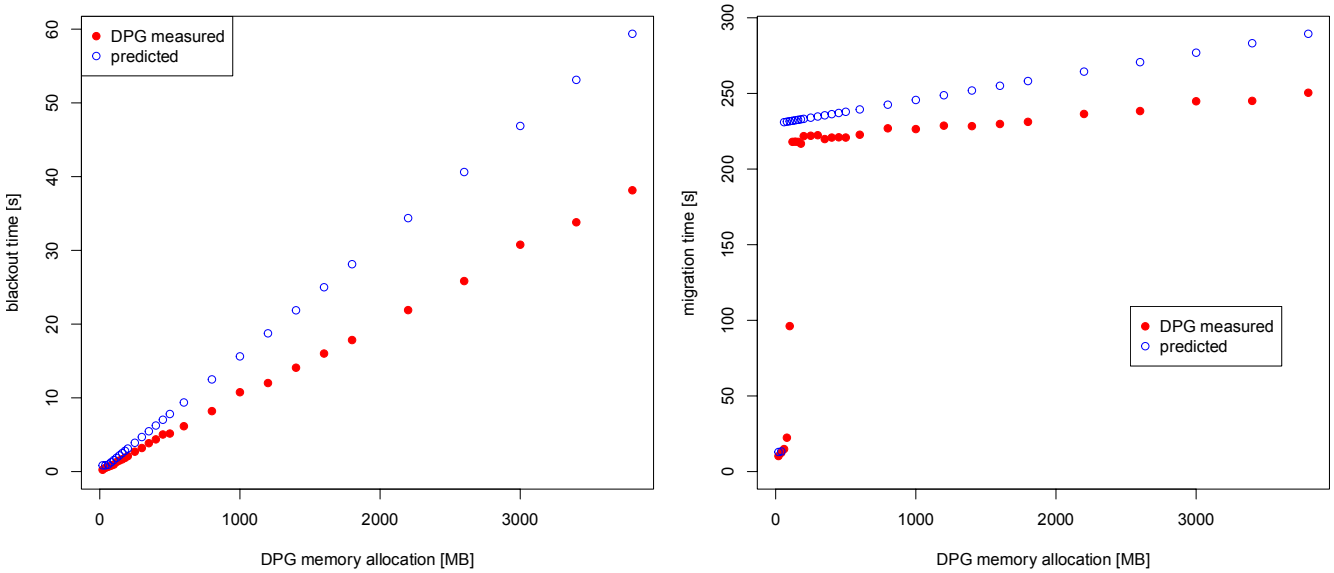
The graphs show that the proposed prediction model works well also for real applications. It can be seen that overall the predictor follows the non-linear shape of the curve, although there is significant over-prediction for parameter settings three and four for blackout time, and for settings two and three for total migration time.

In 98.03% of the cases, the worst case predictor returned a blackout time greater or equal to the corresponding measured time. The absolute error for blackout time prediction was 1.26s on average (4.01s maximum). Due to the fact that an under-estimation of downtime is critical, we separately investigated the cases in which our model predicted shorter migration times than the measured ones. The average deviation in these cases was 0.40s (3.20s maximum). For total migration time, the corresponding numbers are 97.56% accuracy, with an average absolute error of 38.12s (267.5s maximum) and an average under-estimation of 1.15s (9.50s maximum).

B. Postal SMTP Benchmark Results

As a second application benchmark we used the Postal SMTP benchmark 0.7 in conjunction with a Posfix 2.5.5. mail server. To get as close as possible to a realistic workload, we added a Spamassassin 3.2.5. installation to the configuration of the mail server. Postal sends SMTP requests of different kinds to the mail server running in the virtual machine. The varied parameter in our experiments is the number of SMTP messages per minute sent by the Postal application.

Similar to the SPEC benchmark we measured blackout and migration times for ten settings and determined the corresponding values for WSET, HWSET and RATE (see Table IV). Due to increased volatility of the Postal SMTP



(a) Blackout time (b) Migration time

Figure 11. Dirty page load generator (DPG) vs. worst case predictor

Table III
SPEC PARAMETER SETS

Setting	SPEC Driver txRate	Average WSET (pages/s)	Average HWSET (pages/s)	Average RATE (pages/s)
1	5	371228	41962	7802
2	10	388346	58787	13111
3	15	488656	71594	17993
4	20	569836	82140	22911
5	25	695151	86636	27744
6	30	688627	90284	33707
7	35	705575	93165	37911
8	40	732491	100686	43989
9	45	761932	104089	58090
10	50	756850	114790	59533

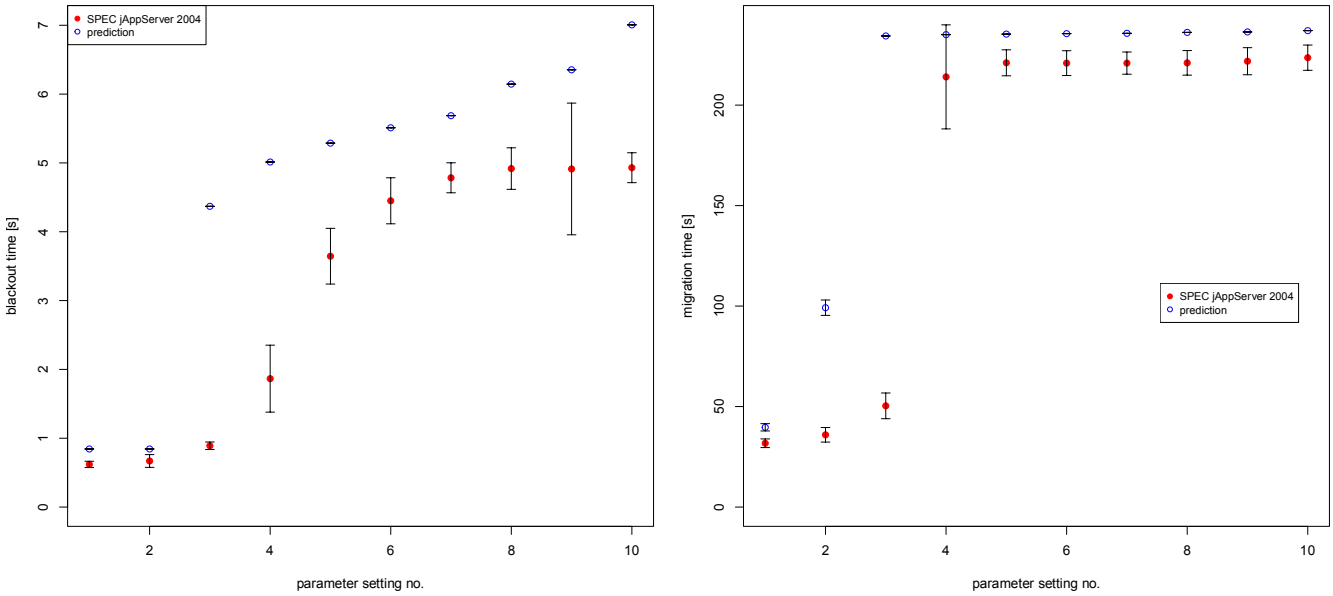
benchmark scenario we performed more than 3500 runs per setting in order to obtain statistically significant numbers.

Figure 13 shows the experimental results. Again, our prediction model resulted in relatively accurate predictions. The plots also show the necessity to leave some headroom for predictions. As can be seen from Figure 13-b, due to the increased volatility the 95% confidence intervals get close to the predicted values. More specifically, our predictor delivered a migration time that was above or equal to the measured performance in 90.18% of the measurements. The average absolute error in the migration time prediction was 62.38s (287.58s maximum), and the averge under-prediction was 36.27s (69.23s maximum). For blackout time, the worst case predictor was safe in 83.6% of all measurements. The average absolute error for blackout time prediction was 0.57s (1.47s maximum), and the average under-prediction error was 0.45s (1.05s maximum).

The results for the SMTP benchmark showed sub-optimal prediction quality for virtual machines with small VMSIZE. If only experiments with a VMSIZE value larger or equal to 4GB are considered, the migration time prediction success rate improve significantly. More specifically, the numbers are for migration time 98.85% accuracy with an average under-estimation of 2.01s (5.42s maximum), and for blackout time prediction accuracy goes up to 96.98% with an average under-estimation of 0.09s (0.27s maximum).

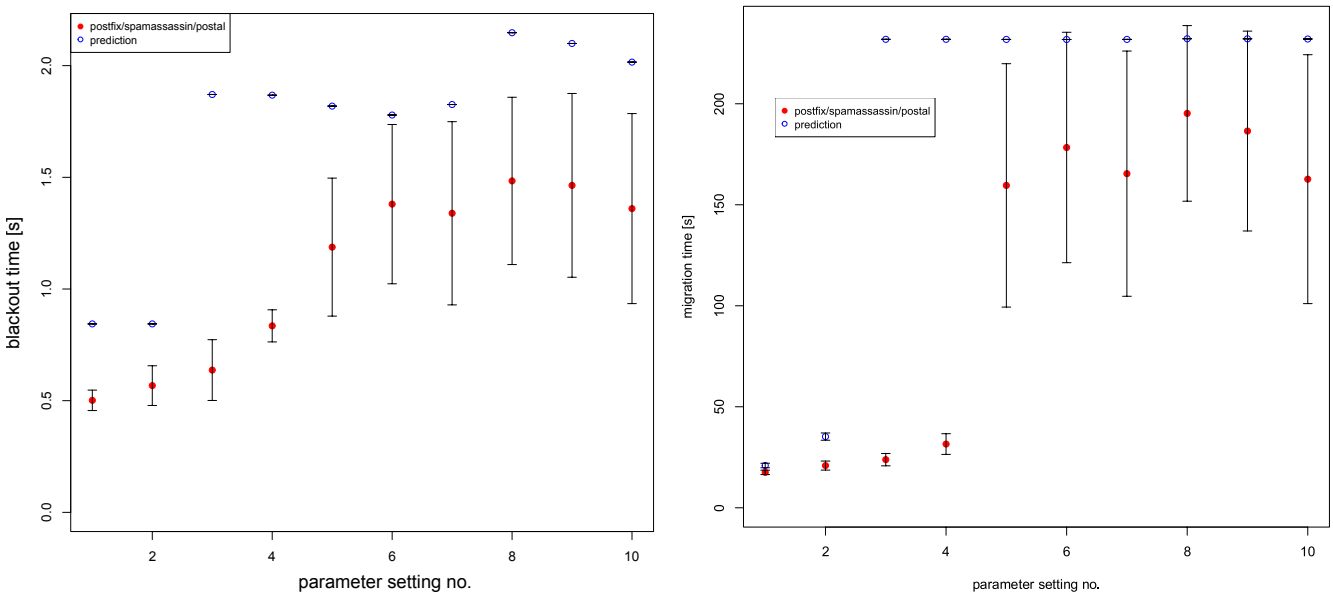
C. Discussion

The experiments have shown that our prediction model is able to forecast both total migration times as well as blackout times of real world applications. As it is the case for all worst-case predictors, predicted values have to be larger than the measured numbers but should nevertheless be as close as possible. This trade-off between accuracy and safety is well-known from other areas such as determination of the worst-case execution time (WCET). In our case the prediction is on the safe side in more than 96.98% of all cases.



(a) Blackout time (b) Migration time

Figure 12. SPEC jAppServer 2004 load vs. worst case predictor



(a) Blackout time (b) Migration time

Figure 13. Postal 0.7 + Postfix 2.5.5 application load vs. worst case predictor

Table IV
POSTAL / POSTFIX PARAMETER SETS

Setting	SMTP messages / minute	Average WSET (pages/s)	Average HWSET (pages/s)	Average RATE (pages/s)
1	100	154035	18348	8002
2	200	185759	32494	12377
3	300	210190	30654	16217
4	400	244276	30604	21003
5	500	443361	29802	23968
6	600	516652	29148	26023
7	700	559266	29917	27488
8	800	712506	35185	28080
9	900	765597	34396	27631
10	1000	728675	33028	27903

VIII. CONCLUSION

With growing capacity of commodity server hardware and increased consolidation efforts, virtualization has become a standard approach for cloud data center operation. Live migration of virtual server workloads can be employed to implement workload-driven system management as well as a mechanism to free server hardware that is due for maintenance and repair. However, in order to give guarantees on application availability or responsiveness as well as for proactive fault management, solid estimations either about the total duration of live migration or the length of service downtime are badly needed.

In this paper, we have presented a model that predicts total migration time as well as service blackout times based on a small number of characteristic parameters: virtual machine-specific parameters, i.e., the overall size of the virtual machine's memory, situation-specific parameters such as the size of working set, the size of the hot subset of the working set, i.e., the number of memory that are actively written, and the memory page modification rate, system-specific parameters such as memory page transmission rates over the network as well as hypervisor-specific parameters modeling the hypervisor's live migration strategy.

By carrying out a large number of experiments, we have shown that the prediction model is able to reliably forecast migration times in more than 95% of all cases. This holds for a worst-case load generator as well as for real-world server applications.

Our results are promising in the sense that they show applicability of live migration for scenarios where workloads have to be moved off potentially breaking servers. The experiment results show a remarkable performance of virtual machine migration even under unfair conditions. The performance numbers typically do not exceed the lead-time of state-of-the-art failure prediction algorithms, which makes the idea of proactive virtual machine migration a promising topic for future research.

REFERENCES

[1] R. Goldberg, "Survey of Virtual Machine Research," *IEEE Computer*, vol. 7, no. 6, pp. 34–45, Jun. 1974.

[2] C. Engelmann, G. Vallée, T. Naughton, and S. Scott, "Proactive Fault Tolerance Using Preemptive Migration," in *17th Euromicro International Conference on Parallel, Distributed and Network-based Processing*. Washington, DC, USA: IEEE Computer Society, 2009, pp. 252–257.

[3] F. Salfner, M. Lenk, and M. Malek, "A Survey of Online Failure Prediction Methods," *ACM Computing Surveys*, vol. 42, no. 3, pp. 10:1–10:42, Mar. 2010.

[4] F. Salfner, P. Tröger, and A. Polze, "Downtime Analysis of Virtual Machine Live Migration," in *The Fourth International Conference on Dependability (DEPEND 2011)*. IARIA, 2011, pp. 100–105.

[5] G. Popek and R. Goldberg, "Formal requirements for virtualizable third generation architectures," *Commun. ACM*, vol. 17, no. 7, pp. 412–421, Jul. 1974.

[6] K. Adams and O. Agesen, "A comparison of software and hardware techniques for x86 virtualization," *SIGARCH Comput. Archit. News*, vol. 34, no. 5, pp. 2–13, Oct. 2006.

[7] A. Kivity, Y. Kamay, D. Laor, U. Lublin, and A. Liguori, "KVM: The Linux virtual machine monitor," in *Ottawa Linux Symposium*, Jul. 2007, pp. 225–230.

[8] N. Bhatia, "Performance Evaluation of Intel EPT Hardware Assist," http://www.vmware.com/pdf/Perf_ESX_Intel-EPT-eval.pdf, Mar. 2009.

[9] M. Nelson, B.-H. Lim, and G. Hutchins, "Fast transparent migration for virtual machines," in *annual conference on USENIX Annual Technical Conference*. Berkeley, CA, USA: USENIX Association, 2005, pp. 25–25.

[10] K. Onoue and Y. Oyama, "A Virtual Machine Migration System Based on a CPU Emulator," in *2nd International Workshop on Virtualization Technology in Distributed Computing*. Washington, DC, USA: IEEE Computer Society, 2006, p. 3.

[11] C. Clark, K. Fraser, S. Hand, J. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield, "Live Migration of Virtual Machines," in *Proceedings of the 2nd conference on Symposium on Networked Systems Design and Implementation*. Berkeley, CA, USA: USENIX Association, 2005, pp. 273–286.

[12] S. Fu, "Failure-aware resource management for high-availability computing clusters with distributed virtual machines," *Journal of Parallel and Distributed Computing*, vol. 70, no. 4, pp. 384–393, 2010.

[13] M. Hines and K. Gopalan, "Post-copy based live virtual machine migration using adaptive pre-paging and dynamic self-ballooning," in *2009 ACM SIGPLAN/SIGOPS international conference on Virtual execution environments*. New York, NY, USA: ACM, 2009, pp. 51–60.

[14] C. Sapuntzakis, R. Chandra, B. Pfaff, J. Chow, M. Lam, and M. Rosenblum, "Optimizing the migration of virtual computers," *SIGOPS Oper. Syst. Rev.*, vol. 36, no. SI, pp. 377–390, 2002.

[15] Y. Du, H. Yu, G. Shi, J. Chen, and W. Zheng, "Microwiper: Efficient Memory Propagation in Live Migration of Virtual Machines," in *39th International Conference on Parallel Processing*, 2010.

[16] A. Nagarajan, F. Mueller, C. Engelmann, and S. Scott, "Proactive fault tolerance for HPC with Xen virtualization," in *ICS '07: Proceedings of the 21st annual international conference on Supercomputing*. New York, NY, USA: ACM, 2007, pp. 23–32.

[17] F. Travostino, P. Daspit, L. Gommans, C. Jog, C. Laat, J. Mambretti, I. Monga, B. Oudenaarde, S. Raghunath, and P. Wang, "Seamless live migration of virtual machines over the MAN/WAN," *Future Gener. Comput. Syst.*, vol. 22, no. 8, pp. 901–907, Oct. 2006.

[18] R. Bradford, E. Kotsovinos, A. Feldmann, and H. Schiöberg, "Live wide-area migration of virtual machines including local persistent state," in *3rd international conference on Virtual execution environments*. New York, NY, USA: ACM, 2007, pp. 169–179.

[19] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, "Xen and the art of virtualization," in *SOSP '03: Proceedings of the nineteenth ACM symposium on Operating systems principles*. New York, NY, USA: ACM, 2003, pp. 164–177.

[20] M. Russinovich, D. Solomon, I. Books24x7, and S. B. Online, *Microsoft Windows Internals: Microsoft Windows Server 2003, Windows XP, and Windows 2000*. Microsoft Press, 2005.

[21] P. Tröger, A. Polze, and F. Salfner, "On the Applicability of Virtual Machine Migration for Proactive Failover," in *SDPS International Conference, Special Track on Virtualization*, 2011.

[22] S. Akoush, R. Sohan, A. Rice, A. Moore, and A. Hopper, "Predicting the Performance of Virtual Machine Migration," in *18th Annual IEEE/ACM International Symposium on Modeling, Analysis, and Simulation of Computer Systems*. Los Alamitos, CA, USA: IEEE Computer Society, 2010, pp. 37–46.

www.iariajournals.org

International Journal On Advances in Intelligent Systems

ICAS, ACHI, ICCGI, UBICOMM, ADVCOMP, CENTRIC, GEOProcessing, SEMAPRO, BIOSYSCOM, BIOINFO, BIOTECHNO, FUTURE COMPUTING, SERVICE COMPUTATION, COGNITIVE, ADAPTIVE, CONTENT, PATTERNS, CLOUD COMPUTING, COMPUTATION TOOLS, ENERGY, COLLA, IMMM, INTELLI, SMART, DATA ANALYTICS

issn: 1942-2679

International Journal On Advances in Internet Technology

ICDS, ICIW, CTRQ, UBICOMM, ICSNC, AFIN, INTERNET, AP2PS, EMERGING, MOBILITY, WEB

issn: 1942-2652

International Journal On Advances in Life Sciences

eTELEMED, eKNOW, eL&mL, BIODIV, BIOENVIRONMENT, BIOGREEN, BIOSYSCOM, BIOINFO, BIOTECHNO, SOTICS, GLOBAL HEALTH

issn: 1942-2660

International Journal On Advances in Networks and Services

ICN, ICNS, ICIW, ICWMC, SENSORCOMM, MESH, CENTRIC, MMEDIA, SERVICE COMPUTATION, VEHICULAR, INNOV

issn: 1942-2644

International Journal On Advances in Security

ICQNM, SECURWARE, MESH, DEPEND, INTERNET, CYBERLAWS

issn: 1942-2636

International Journal On Advances in Software

ICSEA, ICCGI, ADVCOMP, GEOProcessing, DBKDA, INTENSIVE, VALID, SIMUL, FUTURE COMPUTING, SERVICE COMPUTATION, COGNITIVE, ADAPTIVE, CONTENT, PATTERNS, CLOUD COMPUTING, COMPUTATION TOOLS, IMMM, MOBILITY, VEHICULAR, DATA ANALYTICS

issn: 1942-2628

International Journal On Advances in Systems and Measurements

ICQNM, ICONS, ICIMP, SENSORCOMM, CENICS, VALID, SIMUL, INFOCOMP

issn: 1942-261x

International Journal On Advances in Telecommunications

AICT, ICDT, ICWMC, ICSNC, CTRQ, SPACOMM, MMEDIA, COCORA, PESARO, INNOV

issn: 1942-2601