Report from Dagstuhl Seminar 13371

Quantum Cryptanalysis

Edited by

Serge Fehr[1], Michele Mosca[2], Martin Rötteler[3], and Rainer Steinwandt[4]

1 **CWI – Amsterdam, NL,** `serge.fehr@cwi.nl`
2 **University of Waterloo, CA and Perimeter Institute for Theoretical Physics, Waterloo, CA,** `mmosca@iqc.ca`
3 **Microsoft Research – Redmond, US,** `martinro@microsoft.com`
4 **Florida Atlantic University – Boca Raton, US,** `rsteinwa@fau.edu`

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 13371 "Quantum Cryptanalysis". In the first part, the motivation and organizational aspects of this meeting are outlined. Thereafter, abstracts for the presentations are provided (sorted alphabetically by last name of the presenter).

Seminar 08.–13. September, 2013 – www.dagstuhl.de/13371
1998 ACM Subject Classification E.3 Code Breaking, F.2 Analysis of Algorithms and Problem Complexity, G.2 Discrete Mathematics, G.3 Probability and Statistics
Keywords and phrases security of cryptographic schemes, quantum algorithms, computational hardness assumptions
Digital Object Identifier 10.4230/DagRep.3.9.59
Edited in cooperation with John M. Schanck

1 Executive Summary

Serge Fehr
Michele Mosca
Martin Rötteler
Rainer Steinwandt

Motivation and Background

This (second) quantum cryptanalysis seminar aimed at improving our understanding of quantum attacks against modern cryptographic schemes, a task that is closely related to the question of plausible quantum computational hardness assumptions. By bringing together researchers who work in the field of quantum computing with those who work in the field of classical cryptography, the seminar aimed at identifying practical approaches to achieve cryptographic security in the presence of quantum computers. A lesson learned from an earlier edition of this seminar (Dagstuhl Seminar 11381) was that statements about the security of cryptographic schemes in the presence of a quantum attacker require the study and characterization of quantum security parameters. Those parameters measure the amount of resources that have to be spent in order to "break" a system. In this spirit, the following three topics turned out to be particularly relevant for the seminar:

- *Quantum attacks on currently deployed schemes*: Derive quantitative estimates for the resources (like no. of qubits and quantum gates) that are needed to carry out quantum attacks with cryptographically relevant parameter choices.
- *New quantum algorithms to attack potential new hardness assumptions*: For instance, can quantum algorithms be used to improve on classical solutions for computational problems in lattices or for the decoding of error-correcting codes?
- *Quantum computational assumptions*: Which problems are currently considered as intractable, even for a quantum computer, and possibly might have the potential to be of cryptographic interest? Examples are certain hidden shift and hidden subgroup problems.

One indicator for the importance of these topics for the seminar was that most talks addressed (at least) one of them. The invited group of researchers as well as the organizing team was chosen to offer a balance of expertise from the different relevant disciplines, but also to have a substantial common ground for making progress towards the seminar goal.

Seminar Organization

The seminar involved 37 participants from around the globe, ranging from young researchers to colleagues with many years of interdisciplinary research experience. For young researchers the interdisciplinary set-up of the seminar offered an excellent opportunity to make new connections beyond the familiar research communities. Based on the experience from the predecessor (Dagstuhl Seminar 11381), we decided for a schedule which has enough flexibility to add presentations that grow out of discussions during the week, and indeed these additional slots could be brought to good use. We made an effort to keep the number of presentations limited to have ample time for open discussions between presentations. Having two research communities present at the meeting, it also seemed realistic to assume that not all participants are familiar with the latest developments in the complementing discipline. Placing survey presentations on critical topics early in the schedule was well received by the participants.

To ensure an adequate connection with the technological state-of-the-art of implementing quantum computers, one of the survey presentations was specifically devoted to this subject, and the seminar included discussions on implementation aspects of quantum computing. Keeping with the Dagstuhl tradition and the tradition of the predecessor, for Wednesday afternoon we did not schedule any presentations, allowing seminar participants to enjoy a hike in the woods, a visit to Trier, or to use the time for longer technical discussions.

Achievements and Next Steps

As in the first edition of this seminar, there were many fruitful discussions across discipline boundaries. At the time of writing this report, two seminar participants had already published a preprint with a generalization of a previously known quantum attack to a more general class of algebraic structures. We expect further publications to come forward in the coming months. While we are still far from a thorough understanding of the cryptanalytic potential of quantum computing, synergetic collaborations of seminar participants have helped greatly to advance the state-of-the-art in quantum cryptanalysis.

The seminar also successfully facilitated the exchange among colleagues from academia, government, and industry. We believe that in regard to a standardization of post-quantum cryptographic solutions, this type of exchange across community boundaries is valuable and deserves to be intensified further in future meetings.

2 Table of Contents

Executive Summary

Overview of Talks

3 Overview of Talks

3.1 Quantum algorithms for the subset-sum problem

Daniel J. Bernstein (University of Illinois – Chicago, US)

Joint work of Bernstein, Daniel J.; Jeffery, Stacey; Lange, Tanja; Meurer, Alexander

At Eurocrypt 2010, Howgrave-Graham and Joux introduced a subset-sum algorithm with heuristic asymptotic cost exponent 0.337. The idea, suitably adapted, can be combined with quantum walks, achieving exponent 0.241; this is joint work with Stacey Jeffery, Tanja Lange, and Alexander Meurer. I'll also include some experimental material on simulating quantum algorithms.

3.2 Hash-based signatures

Johannes A. Buchmann (TU Darmstadt, DE)

Joint work of Buchmann, Johannes A.; Coronado, Corlaos: Dahmen, Eric; Hülsing, Andreas

Digital signatures a very important tools for the protection of IT systems and, in particular, the Internet. They protect the authenticity of software updates. This is crucial since operating systems and application software are never error-free and must be fixed on a regular basis.

The digital signature schemes that are currently being used in practice are RSA or methods whose security is based on the hardness of computing discrete logarithms over finite fields or in the group of points of elliptic curves over finite fields. As Peter Shor showed in the late 90s, all these schemes can be broken by quantum computers. It is therefore essential to come up with alternative that resists quantum computer attacks.

In my talk I report on the extended Merkle signature scheme (XMSS) that is based on the Merkle signature scheme invented in the late 70s. I show that this scheme is very promising both from the theoretical and practical side. On the theoretical side, I prove that XMSS has minimal security requirements. In fact, it can be shown, that a secure instance of XMSS can be constructed as long as there is a one-way function. As one-way functions are known to be the minimal security requirement for digital signatures, this shows that XMSS has in fact minimal security requirements. I also report on the algorithmic improvements that have been found in my research group in the last years. Implementations and experiments show that the latest version of XMSS can compete with established signature schemes.

3.3 A new definition for the quantum conditional Rényi entropy

Frederic Dupont-Dupuis (Aarhus University, DK)

Joint work of Müller-Lennert, Martin; Dupuis, Frédéric; Szehr, Oleg; Fehr, Serge; Tomamichel, Marco
Main reference M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, M. Tomamichel, "On quantum Renyi entropies: a new generalization and some properties," arXiv:1306.3142v3 [quant-ph], 2013.
URL http://arxiv.org/abs/1306.3142v3

Very recently, a new definition for the quantum conditional Rényi entropy has been proposed. Unlike previous definitions, it satisfies most of the basic properties one would expect from a conditional entropy, and it coincides with other widely used entropies (min-, max- and collision entropy) for appropriate choices of parameters. It has also found an application to prove a strong converse for coding over entanglement breaking channels. I will present these recent developments and try to show why this might be the "right" definition.

The results presented can be found in the following papers:

References

1 Martin Müller-Lennert, Frédéric Dupuis, Oleg Szehr, Serge Fehr, Marco Tomamichel. *On quantum Rényi entropies: a new definition and some properties.* arXiv:1306.3142.
2 Mark M. Wilde, Andreas Winter, Dong Yang. *Strong converse for the classical capacity of entanglement-breaking channels.* arXiv:1306.1586.
3 Rupert L. Frank, Elliott H. Lieb. *Monotonicity of a relative Rényi entropy.* arXiv:1306.5358.
4 Salman Beigi. *Quantum Rényi divergence satisfies data processing inequality.* arXiv:1306.5920.

3.4 On quantum versions of the McEliece cryptosystem

Markus Grassl (National University of Singapore, SG)

Joint work of Grassl, Markus; Ezerman, Fred

Recently, quantum versions of the McEliece cryptosystem have been proposed. We will take a closer look at them and discuss consequences of particular choices made in the design, in particular the use of so-called CSS codes, a subclass of stabilizer quantum codes. This yields to some interesting questions which are open to us.

3.5 Lattice-based cryptography

Nadia Heninger (University of Pennsylvania, US)

We give a short survey of hard lattice problems and lattice-based cryptography. We discuss the shortest vector problem and closest vector problem, show how they are related to the short integer solution and learning with errors problem, and show how to construct collision-resistant hash functions and public-key encryption systems based off of the average case hardness of these problems. We finish with a discussion of ring learning with errors and hard problems on ideal lattices.

3.6 Hidden subgroup problems in quantum-resistant cryptography?

Gabor Ivanyos (Hungarian Academy of Sciences, HU)

This talk addressed the potential hardness of some simple Hidden-Subgroup-like problems for quantum computers. One of these is the discrete logarithm problem over a black box group with non- unique encoding. Another is the shift problem over cyclic groups (equivalently, the dihedral HSP). Regev's reduction to a version of the dihedral HSP suggests that it might be hard. Some easy and potentially difficult natural non-oracle instances of these problems were discussed: shift problems over cyclic permutations groups (e.g., shifts of graphs and hypergraphs), or shift problems over cyclic linear groups (e.g., shifts of linear subspaces).

3.7 Quantum walks for cryptanalysis

Stacey Jeffery (University of Waterloo, CA)

The aim of this talk will be to present the quantum walk search algorithm framework, and several recent extensions, so that a crypto audience will be able to apply the framework to construct quantum attacks on cryptosystems. I will present several examples of quantum walk algorithms that can solve very general types of problems, and explain how these may be adapted to other settings.

3.8 Quantum lattice cryptanalysis – Part 1

Thijs Laarhoven (TU Eindhoven, NL)

Main reference T. Laarhoven, M. Mosca, J. van de Pol , "Solving the Shortest Vector Problem in Lattices Faster Using Quantum Search," in Proc. of the 5th Int'l Conf. on Post-Quantum Cryptography (PQCrypto'13), LNCS, Vol. 7932, pp. 83–101, Springer, 2013.
URL http://dx.doi.org/10.1007/978-3-642-38616-9_6

Recently lattices have found many applications in cryptography, both in constructive "post-quantum" cryptography (FHE) and in cryptanalysis. Estimating the (quantum) complexity of lattice algorithms is crucial in understanding the security of lattice-based cryptography, and for choosing parameters in these cryptosystems. In Part 1, I will discuss how quantum algorithms can be used to significantly speed up two algorithms for finding shortest vectors in lattices, namely sieving and saturation. Other lattice algorithms, for which we did not yet obtain quantum speed-ups, are discussed in Part 2.

3.9 Comments on computing using a D-Wave chip

Bradley Lackey (National Security Agency – Fort Meade, US)

It is not uncommon in the literature to find the "D-Wave problem" referring to the problem of finding a ground state of a (typically random) Ising model on a particular graph. What a D-Wave chip does is produce a large number of samples from the lowest energy configurations of the programmed Ising model Hamiltonian. In this open discussion session, I commented that there are computational problems (e.g. decoding an LDPC code or, in more generality, Bayesian re-estimation) that can be formulated as finding the Helmholtz distribution of an Ising model Hamiltonian at some positive temperature. Since this is similar to what a D-Wave chip does empirically, it may be possible to solve such problems on a D-Wave machine better than known techniques. As an example I indicated that small cycles in the Tanner graph of an LDPC code's parity check matrix are known to cause belief propagation difficulties, however such structures seem irrelevant if one were to sample from the Helmholtz distribution directly.

3.10 Recent advances in decoding random binary linear codes

Alexander May (Ruhr-Universität Bochum, DE)

URL http://www.cits.ruhr-uni-bochum.de/personen/may.html

We review some recent algorithmic progress that led to faster algorithms for decoding random linear codes over $\mathbb{F}_2^n$. The worst case complexity for decoding these codes dropped from roughly $2^{n/8}$ to $2^{n/10}$. We also discuss some open problems whose (quantum) solution would provide further progress.

References

1 Anja Becker, Antoine Joux, Alexander May, Alexander Meurer *Decoding Random Binary Linear Codes in $2^{n/20}$: How $1+1=0$ Improves Information Set Decoding* , In Advances in Cryptology (Eurocrypt 2012), Lecture Notes in Computer Science, Springer-Verlag, 2012

2 Alexander May, Alexander Meurer, Enrico Thomae *Decoding Random Linear Codes in $O(2^{0.054n})$* , In Advances in Cryptology (Asiacrypt 2011), Lecture Notes in Computer Science, Springer-Verlag, 2011

3.11 Code-based verifiable encryption

Kirill Morozov (Kyushu University, JP)

Joint work of Hu, Rong; Morozov, Kirill; Takagi, Tsuyoshi
Main reference R. Hu, K. Morozov, T. Takagi, "Proof of plaintext knowledge for code-based public-key encryption revisited," in Proc. of the 8th ACM SIGSAC Symp. on Information, Computer and Communications Security (ASIA CCS'13), pp. 535–540, ACM, 2013.
URL http://dx.doi.org/10.1145/2484313.2484385

In this talk, we present a verifiable encryption with equality relation for the IND-CPA McEliece public key encryption. More specifically, this is a zero-knowledge (ZK) proof that a given (IND-CPA McEliece) ciphertext contains a given plaintext without revealing any information about the randomness used for encryption. Instrumental in our construction is code-based ZK identification scheme by Stern. Potential applications include designated confirmer signatures and escrow schemes.

3.12 Easy and hard functions for the Boolean hidden shift problem

Maris Ozols (IBM TJ Watson Research Center – Yorktown Heights, US)

Joint work of Childs, Andrew M.; Kothari, Robin; Ozols, Maris; Roetteler, Martin
Main reference A. M. Childs, R. Kothari, M. Ozols, M. Roetteler, "Easy and hard functions for the Boolean hidden shift problem," arXiv:1304.4642v1 [quant-ph], 2013.
URL http://arxiv.org/abs/1304.4642v1

We study the quantum query complexity of the Boolean hidden shift problem. Given oracle access to $f(x+s)$ for a known Boolean function f, the task is to determine the n-bit string s. The quantum query complexity of this problem depends strongly on f. We demonstrate that the easiest instances of this problem correspond to bent functions, in the sense that an exact one-query algorithm exists if and only if the function is bent. We partially characterize the hardest instances, which include delta functions. Moreover, we show that the problem is easy for random functions, since two queries suffice. Our algorithm for random functions is based on performing the pretty good measurement on several copies of a certain state; its analysis relies on the Fourier transform. We also use this approach to improve the quantum rejection sampling approach to the Boolean hidden shift problem.

3.13 On group isomorphism problem when Cayley tables are given

Youming Qiao (National University of Singapore, SG)

Joint work of Grochow, Joshua A.; Qiao, Youming
Main reference J. A. Grochow, Y. Qiao, "Algorithms for group isomorphism via group extensions and cohomology," arXiv:1309.1776v1 [cs.DS], 2013; and ECCC TR13–123.
URL http://arxiv.org/abs/1309.1776v1
URL http://eccc.hpi-web.de/report/2013/123/

Given the Cayley tables of two finite groups of order n, it is easy to test their isomorphism in time $n^{\log n+O(1)}$. The main question is to bring to polynomial time. Recently polynomial-time algorithms for several group classes have been devised, e.g. [1], [2], and [3]. In this work, we show that there is a common underlying scheme supporting these previous works: naively speaking, the key is to transform testing isomorphism of abstract groups, to testing whether certain functions arising from these abstract groups are in the same orbit under some concrete group action. These functions are derived from the extension theory of groups. Based on this underlying scheme, we devise a polynomial-time algorithm to test isomorphism of groups as central extensions of elementary abelian groups by a direct product of nonabelian simple groups. We then briefly describe the ingredients and ideas used to settle a minimal case in the work [2], as well as the above mentioned group class.

References

1. László Babai, Paolo Codenotti, and Youming Qiao. Polynomial-time isomorphism test for groups with no abelian normal subgroups – (extended abstract). In *ICALP*, pages 51–62, 2012.
2. László Babai and Youming Qiao. Polynomial-time isomorphism test for groups with Abelian Sylow towers. In *29th STACS*, LIPIcs, Vol. 14, pp. 453–464, Schloss Dagstuhl, doi: 10.4230/LIPIcs.STACS.2012.453.
3. Mark L. Lewis and James B. Wilson. Isomorphism in expanding families of indistinguishable groups. *Groups – Complexity - Cryptology*, 4(1):73–110, 2012.

3.14 Complete insecurity of quantum protocols for classical two-party computation

Christian Schaffner (University of Amsterdam, NL)

Main reference H. Buhrman, M. Christandl, C. Schaffner, “Complete Insecurity of Quantum Protocols for Classical Two-Party Computation,” Physical Review Letters, Volume 109, Issue 16, 160501 (5pp.), 2012.
URL http://dx.doi.org/10.1103/PhysRevLett.109.160501

A fundamental task in modern cryptography is the joint computation of a function which has two inputs, one from Alice and one from Bob, such that neither of the two can learn more about the other’s input than what is implied by the value of the function. In this work, we show that any quantum protocol for the computation of a classical deterministic function that outputs the result to both parties (two-sided computation) and that is secure against a cheating Bob can be completely broken by a cheating Alice. Whereas it is known that quantum protocols for this task cannot be completely secure, our result implies that security for one party implies complete insecurity for the other. Our findings stand in stark contrast to recent protocols for weak coin tossing and highlight the limits of cryptography within quantum mechanics. We remark that our conclusions remain valid, even if security is only required to be approximate and if the function that is computed for Bob is different from that of Alice.

3.15 Practical signatures from the partial Fourier recovery problem

John M. Schanck (University of Waterloo, CA)

Joint work of Hoffstein, Jeff; Pipher, Jill; Schanck, John M.; Silverman, Joseph H.; Whyte, William
Main reference J. Hoffstein, J. Pipher, J. Schanck, J. H. Silverman, W. Whyte, "Practical Signatures from the Partial Fourier Recovery Problem," Cryptology ePrint Archive: Report 2013/757, 2013.
URL http://eprint.iacr.org/2013/757

PASS, an authentication and signature scheme based on the problem of finding bounded norm preimages of a partial discrete Fourier transform, was first presented by Hoffstein, Lieman, and Silverman in 1999. The system had several attractive features, but suffered from transcript analysis attacks which rendered it completely insecure. Perhaps as a consequence, this interesting trapdoor function has received little attention since its introduction. In my presentation I demonstrated how recent techniques developed for lattice cryptography can be used to prevent the transcript attacks while salvaging most of the efficiency of the scheme, and discussed several open questions related to the scheme's security. Concrete parameter sets and benchmarks were also be presented.

A paper describing the system is in preparation, and software implementing it is available at https://github.com/NTRUOpenSourceProject/ntru-crypto.

3.16 Generic decoding of linear codes

Nicolas Sendrier (INRIA – Siège, FR)

The security of code-based cryptosystems relies heavily on the hardness of decoding in an arbitrary linear code. The problem only has exponential solutions in the classical computing model, and it seems that it remains the case with quantum computing, placing code-based crypto among the so-called post-quantum cryptographic techniques.

Even though quantum computer are not likely to allow generic decoding techniques with non-exponential complexity, it still allows some significant improvements. A few works have already explore this path.

The purpose of this survey is not to propose new decoding techniques taking advantage a quantum computing. Instead we intend to give a comprehensive description of the main decoding techniques. The best techniques are recent (2011 and 2012) and are in fact finely tuned trade-offs between several very basic techniques. We will come back to those basics, which are the birthday decoding (based on the birthday paradox), and the Prange or Lee & Brickell algorithms (which are essentially enumerations).

We feel that understanding each of those techniques in a quantum setting will simplify the search of an optimal quantum algorithm, and, hopefully, provide a simpler approach than directly "quantumize" the best known decoding techniques.

3.17 Quantum-resistant multivariate public key cryptography

Daniel Smith (NIST – Gaithersburg, US)

We discussed some of the developments which have arisen in post- quantum multivariate schemes. In particular, we focused on some of the fundamental complexity theoretic problems on which the security of a variety of multivariate schemes depend. We reviewed the classical complexity of the Morphism of Polynomials (MP) Problem as well as the closely related problems Isomorphism of Polynomials (IP) and IP with one secret (IP1S).

Some interesting complexity theoretic results are known in the classical model; however, IP1S lies in a particularly interesting location in the complexity hierarchy. The IP1S problem is graph isomorphism-complete, which places it in a small class of problems which are believed to lie strictly between P and NP. Since the factoring problem thus far seems to exist in this nether region in the classical model, there is some justification in addressing the complexity of IP1S in the quantum model.

For completeness, the discussion reviewed several relevant computational techniques of use in the cryptanalysis of modern multivariate schemes, and presented some recent theoretical results establishing some benchmarks for security, including classification techniques and theorems proving immunity from structural attacks as well as the calculation of degree of regularity indicating the complexity of algebraic analysis. There seems to be a dichotomy in multivariate cryptanalysis, with many schemes falling into potential wells into a realm of structural weakness, or of susceptibility to algebraic attacks. It is precisely the collection of schemes which avoid the known types of structural weakness and which also have a high enough degree of regularity which have survived. While classification techniques are algebraic arguments independent of the model of computing, it is possible that there may be polynomial speed-ups for generic algebraic polynomial system solvers in the quantum model.

The discussion concluded with reference to some of the recent developments in these areas, including some recent advances in the complexity theory of the above mentioned fundamental problems, as well as some new security calculations for specific schemes in terms of structural classification theorems and degree of regularity calculations.

3.18 Exponential improvement in precision for Hamiltonian-evolution simulation

Rolando Somma (Los Alamos National Lab., US)

Joint work of Somma, Rolando; Berry, Dominic; Cleve, Richard
Main reference Dominic W. Berry, Richard Cleve, Rolando D. Somma, "Exponential improvement in precision for Hamiltonian-evolution simulation," arXiv:1308.5424v3 [quant-ph], 2013.
URL http://arxiv.org/abs/1308.5424v3

I will present a quantum method for simulating Hamiltonian evolution with complexity polynomial in the logarithm of the inverse error. This is an exponential improvement over existing methods for Hamiltonian simulation. In addition, its scaling with respect to time is close to linear, and its scaling with respect to the time derivative of the Hamiltonian is logarithmic. These scalings improve upon most existing methods. Our method is to use a compressed Lie-Trotter formula, based on recent ideas for efficient discrete-time simulations of continuous-time quantum query algorithms.

3.19 Single-qubit quantum circuit decomposition

Krysta Svore (Microsoft Research – Redmond, US)

Joint work of Bocharov, Alex; Gurevvich, Yuri; Svore, Krysta
Main reference A. Bocharov, Y. Gurevich, K. M. Svore, "Efficient Decomposition of Single-Qubit Gates into V Basis Circuits," Physical Review A, Vol. 88, Issue 1, No. 012313 (13pp.); and available as pre-print arXiv:1303.1411v1 [quant-ph] , 2013.
URL http://dx.doi.org/10.1103/PhysRevA.88.012313
URL http://arxiv.org/abs/1303.1411v1

In this talk, I will present recent developments in single-qubit quantum circuit decomposition, a necessary component to implementation of quantum algorithms. In the past year, constructive algorithms for decomposing single- qubit rotations efficiently into $O(\log(1/\epsilon))$-depth circuits have been developed for several universal bases. I will present two algorithms for compiling single-qubit unitary gates into circuits over the universal V basis. The V basis is an alternative universal basis to the more commonly studied $\{H, T\}$ basis. The first algorithm has expected polynomial time (in precision $\log(1/\epsilon)$) and offers a depth/precision guarantee that improves upon state-of-the-art methods for compiling into the $\{H, T\}$ basis by factors ranging from 1.86 to $\log_2(5)$. The second algorithm is analogous to direct search and yields circuits a factor of 3 to 4 times shorter than our first algorithm, and requires time exponential in $\log(1/\epsilon)$; however, in practice the runtime is reasonable for an important range of target precisions.

3.20 Quantum lattice cryptanalysis – Part 2

Joop van de Pol (University of Bristol, GB)

Joint work of Laarhoven, Thijs; Mosca, Michele; van de Pol, Joop
Main reference T. Laarhoven, M. Mosca, J. van de Pol, "Solving the Shortest Vector Problem in Lattices Faster Using Quantum Search," in Proc. of the 5th Int'l Conf. on Post-Quantum Cryptography (PQCrypto'13), LNCS, Vol. 7932, pp. 83–101, Springer, 2013.
URL http://dx.doi.org/10.1007/978-3-642-38616-9_6

In Part 1 we have seen that we can use quantum algorithms to speed up lattice cryptanalytic algorithms such as the sieving/saturation algorithms. But what about the other lattice algorithms that are used in cryptanalysis? I will briefly describe our attempts in applying similar methods to these algorithms (basis reduction, enumeration and Voronoi cell) and the obstacles we encountered.

3.21 Simulating quantum circuits with sparse output distributions

Maarten van den Nest (MPI für Quantenoptik, DE)

Joint work of Schwarz, Martin;

We show that several quantum circuit families can be simulated efficiently classically if it is promised that their output distribution is approximately sparse i.e. the distribution is close to one where only a polynomially small – though a priori unknown – subset of the measurement probabilities are nonzero. Classical simulations are thereby obtained for quantum circuits which, without the sparsity promise, are considered hard to simulate. Our results apply in particular to a family of Fourier sampling circuits which contain Shor's factoring algorithm as a special instance, but also to other circuit families, such as IQP circuits. To achieve an efficient classical simulation, we employ and extend the Goldreich-Levin algorithm in combination with probabilistic simulation methods for quantum circuits.

3.22 Implementations of quantum computers

Frank Wilhelm-Mauch (Universität des Saarlandes, DE)

Implementing a scalable and useful quantum computer is a daunting task. I turns out that this goal has come a lot closer due to two reasons: i) the discovery of surface codes for error correction, which promise high error thresholds based on nearest-neighbour interaction only and ii) the progress in quantum computer implementations. I have mostly presented point ii) by giving an introduction to superconducting qubits and by reviewing milestones such as the great improvement of control and coherence over the last decade.

This presentation was mostly giving context to the main theme of the workshop.

Participants

- Aleksandrs Belovs
University of Latvia, LV
- Daniel J. Bernstein
Univ. of Illinois – Chicago, US
- Johannes A. Buchmann
TU Darmstadt, DE
- Andrew Childs
University of Waterloo, CA
- Frédéric Dupont-Dupuis
Aarhus University, DK
- Serge Fehr
CWI – Amsterdam, NL
- Katalin Friedl
Budapest University of Technology & Economics, HU
- Markus Grassl
National Univ. of Singapore, SG
- Nadia Heninger
University of Pennsylvania, US
- Peter Høyer
University of Calgary, CA
- Gabor Ivanyos
Hungarian Acad. of Sciences, HU
- Stacey Jeffery
University of Waterloo, CA
- Stephen P. Jordan
NIST – Gaithersburg, US
- Thijs Laarhoven
TU Eindhoven, NL
- Bradley Lackey
National Security Agency – Fort Meade, US
- Tanja Lange
TU Eindhoven, NL
- Yi-Kai Liu
NIST – Gaithersburg, US
- Alexander May
Ruhr-Universität Bochum, DE
- Kirill Morozov
Kyushu University, JP
- Michele Mosca
University of Waterloo and Perimeter Institute for Theoretical Physics – Waterloo, CA
- Maris Ozols
IBM TJ Watson Res. Center – Yorktown Heights, US
- Youming Qiao
National Univ. of Singapore, SG
- Martin Rötteler
Microsoft Res. – Redmond, US
- Louis Salvail
University of Montreal, CA
- Miklos Santha
University Paris-Diderot, FR
- Christian Schaffner
University of Amsterdam, NL
- John M. Schanck
University of Waterloo, CA
- Nicolas Sendrier
INRIA – Siège, FR
- Daniel Smith
NIST – Gaithersburg, US
- Rolando Somma
Los Alamos National Lab., US
- Fang Song
Penn State University, US
- Rainer Steinwandt
Florida Atlantic University – Boca Raton, US
- Krysta Svore
Microsoft Res. – Redmond, US
- Wim van Dam
University of California – Santa Barbara, US
- Joop van de Pol
University of Bristol, GB
- Maarten van den Nest
MPI für Quantenoptik, DE
- Frank Wilhelm-Mauch
Universität des Saarlandes, DE