Report from Dagstuhl Seminar 15371

Quantum Cryptanalysis

Edited by

Michele Mosca[1], Martin Roetteler[2], Nicolas Sendrier[3], and Rainer Steinwandt[4]

1 **University of Waterloo, CA,** mmosca@iqc.ca
2 **Microsoft Corporation – Redmond, US,** martinro@microsoft.com
3 **INRIA – Le Chesnay, FR,** nicolas.sendrier@inria.fr
4 **Florida Atlantic University – Boca Raton, US,** rsteinwa@fau.edu

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 15371 "Quantum Cryptanalysis". In this seminar, participants explored the impact that quantum algorithms will have on cryptology once a large-scale quantum computer becomes available. Research highlights in this seminar included both computational resource requirement and availability estimates for meaningful quantum cryptanalytic attacks against conventional cryptography, as well as the security of proposed quantum-safe cryptosystems against emerging quantum cryptanalytic attacks.

Seminar September 6–11, 2015 – http://www.dagstuhl.de/15371

1998 ACM Subject Classification E.3 Data Encryption, F.2 Analysis of Algorithms and Problem Complexity, G.2 Discrete Mathematics, G.3 Probability and Statistics

Keywords and phrases Cryptography, Quantum computing, Post-quantum cryptography, Quantum algorithms, Cryptanalysis, Computational algebra, Quantum circuit complexity, Quantum hardware and resource estimation

Digital Object Identifier 10.4230/DagRep.5.9.1

Edited in cooperation with Jennifer Katherine Fernick

1 Executive Summary

Jennifer Katherine Fernick

It is known that quantum algorithms exist that jeopardize the security of most of our widely-deployed cryptosystems, including RSA and Elliptic Curve Cryptography. It is also known that advances in quantum hardware implementations are making it increasingly likely that large-scale quantum computers will be built in the near future that can implement these algorithms and devastate most of the world's cryptographic infrastructure. What is not known is an estimate of the resources that will be required to carry out these attacks – or even whether other quantum attacks exist that have not yet been accounted for in our security estimates. In this seminar, we examined both computational resource estimates for meaningful quantum cryptanalytic attacks against classical (i.e.: conventional) cryptography, as well as the security of proposed quantum-safe cryptosystems against emerging quantum cryptanalytic attacks.

This seminar had a number of research highlights spanning the areas of implementations of quantum hardware and software, quantum algorithms, and post-quantum cryptography.

Quantum Cryptanalysis, *Dagstuhl Reports*, Vol. 5, Issue 9, pp. 1–17
Editors: Michele Mosca, Martin Roetteler, Nicolas Sendrier, and Rainer Steinwandt
DAGSTUHL REPORTS Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Implementations of quantum information processing were outlined to help contextualize the current state of quantum computation. Recent advances in the synthesis of efficient quantum circuits were presented, as well as an update on implementations – particularly in the domain of superconducting integrated circuits. Seminar participants were warned that traditional approaches to the modeling of quantum processors may be reaching an end, while the LIQUi|> software architecture for control of quantum hardware and simulation of quantum algorithms was unveiled. Challenges involving practical costs for error correction in systems with specific types of quantum memory (particularly quantum bucket brigade RAM architectures) were articulated.

In the domain of algorithmic advances, seminar participants demonstrated quantum improvements on the gapped group testing problem, as well as improvements on lattice sieving using nearest neighbour search algorithms. A discussion of how quantum computers can sometimes provide quadratic speedup for the differential cryptanalysis of symmetric-key cryptosystems was also presented. A quantum version of the unique-SVP algorithm was discussed, but it was found to have slightly worse performance than its' classical counterpart. For the purposes of improving our understanding quantum algorithms before large-scale quantum computers become available, a technique involving trapdoor simulation of quantum algorithms was proposed.

Seminar participants also gave a number of recent results in the domain of quantum-safe cryptography. These included a provably-secure form of Authenticated Key Exchange based on the Ring-Learning with Errors problem, a proposal for a quantum-safe method to prevent key leakage during key agreement failure stemming from invalid public keys, and updates on hash-based digital signatures. The EU PQCRYPTO project also presented some preliminary recommendations for post-quantum cryptography.

In the domain of code-based cryptography, it was demonstrated that assuming hardness of Niederreiter problem, CFS signatures are strongly existentially unforgeable in the random oracle model. A number of results related to lattice reduction were also presented, including an improvement on the BKZ lattice reduction algorithm, some lattice enumeration work involving factoring integers by CVP algorithms for the prime number lattice, and a reduction of gapped uSVP to the Hidden Subgroup Problem in dihedral groups. A LIQUi|> implementation of a quantum algorithm to extract hidden shift was also presented, as well as demonstration of instances of HSPs over dihedral group which can be efficiently solved on a quantum computer. Seminar participants also proposed alternative ways of thinking about the dihedral coset problem, including some hardness reductions. A very new result on finding a generator of a principal ideal was also debuted at this seminar and provoked lively and ongoing discussion among participants.

Other talks were presented on diverse and compelling topics including quantum-mechanical means for program obfuscation, and a means for quantum indistinguishability of some types of ciphertext messages. A presentation was also made about how standardization bodies and industry deal with information security and risk, and many discussions – both formal and informal – among participants began to deal with the applied challenges of developing and deploying quantum-safe information security standards and tools.

Overall, the success of this seminar can be observed not only through the quantity of new results, but also in their diversity and interdisciplinarity. While there exist venues for cryptography and cryptanalysis, for quantum algorithms, and for implementations of quantum information processing, it remains critical that these communities continue to come together to ensure rigorous and broad cryptanalysis of proposed quantum-safe cryptographic algorithms, and to share a well-defined mutual understanding of the quantum-computational resource requirements – and their present availability – for attacking both public and symmetric key cryptography. The security of the world's information depends on it.

The organizers (Michele Mosca, Martin Roetteler, Nicolas Sendrier, and Rainer Steinwandt) are grateful to the participants of this seminar and the team of Schloss Dagstuhl for an inspiring and productive third edition of this seminar series.

2 Table of Contents

Executive Summary

Overview of Talks

3 Overview of Talks

3.1 Obfuscation and Quantum Encryption

Gorjan Alagic (University of Copenhagen, DK)

Joint work of Broadbent, Anne; Fefferman, Bill; Gagliardoni, Tommaso; Schaffner, Christian; St. Jules, Michael

Encryption of data is fundamental to secure communication. Beyond encryption of data lies obfuscation, i.e., encryption of functionality. It has been known for some time that the most powerful form of classical obfuscation (black-box obfuscation) is impossible. In this talk, we discuss the potential of obfuscating programs via quantum-mechanical means. As a starting point, we will mention some quantum analogues of several foundational results in obfuscation, including the aforementioned impossibility result (joint work with B. Fefferman). Our proof involves a novel technical idea: chosen-ciphertext-secure encryption for quantum states. We will thus also discuss what it means to encrypt quantum states with computational assumptions (joint work with A. Broadbent, B. Fefferman, T. Gagliardoni, C. Schaffner and M. St. Jules.)

3.2 A Trapdoor Simulation of Quantum Algorithms

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

State-of-the-art algorithms to attack hard cryptanalytic problems never have complete proofs of their correctness and performance conjectures.The only reason for confidence in these conjectures is experiments showing that the algorithms work for many inputs. Trapdoor simulation builds the same confidence as experiment and is often much faster. Tung Chou and I have successfully simulated, e.g., the latest online Childs–Eisenberg distinctness algorithm and shown that it does notwork. This is a quantum algorithm using many qubits, with no other verification strategy.

3.3 Gapped Group Testing with Applications

Aleksandrs Belovs (University of Latvia, LV)

Joint work of Ambainis, Andris; Belovs, Aleksandrs; Regev, Oded; de Wolf, Ronald
Main reference A. Ambainis, A. Belovs, O. Regev, R. de Wolf, "Efficient Quantum Algorithms for (Gapped) Group Testing and Junta Testing," arXiv:1507.03126v1 [cs.CC], 2015.
URL http://arxiv.org/abs/1507.03126v1

In the group testing problem, given an oracle access to a function f on n variables that is promised to be the disjunction of some set S of at most k variables, the task is to identify S. We study the gapped version of this problem, where the task is to distinguish whether the set S is of size at most k or at least $k + d$ for some parameters k and d. We show the following. The randomized complexity of this problem is $\min\{k, (1+k/d)^2\}$ up to logarithmic factors. The quantum complexity of this problem is $\Theta(\sqrt{1+k/d})$. Note that this constitutes a quartic improvement for $d \geq \sqrt{k}$. We demonstrate an application of this subroutine in a quantum algorithm for testing k-juntas.

3.4 Finding a Generator of a Principal Ideal

Jean-François Biasse (University of South Florida – Tampa, US)

Some recent cryptosystems, including the multilinear maps of Garg, Gentryand Halevi and the fully homomorphic encryption scheme of Smart and Vercauteren, are based on the hardness of finding a short generator of an principal ideal (short-PIP) in a number field (typically in cyclotomic fields). However, the assumption that short-PIP is hard has been challenged recently by Campbel et al. They proposed an approach for solving short-PIP that proceeds in two steps: first they sketched a quantum algorithm for finding an arbitrary generator (not necessarily short) of the input principal ideal. Then they suggested that it is feasible to compute a short generator efficiently from the generator in Step 1. Campbel et al. conjectured that this attack could run in polynomial time, which drew a lot attention. Since then, the conjectured run-time for Step 1 has been retracted while Cramer et al. validated Step2 of the approach by giving a detailed analysis. Whether the first step could be salvaged remains an open question.

In this paper we investigate the first step of the attack of Campbel et al. formally. We first observe that their quantum algorithm for finding a generator essentially falls into a framework of quantum algorithms for the hidden subgroup problem described by Hallgren. Hence, it suffers from similar limits, and we can show that, according to the same line of analysis of Hallgren, the algorithm has running time exponential in the degree of the number field. It has been an open question whether one can improve the analysis of Hallgren. Therefore it indicates that it is at least difficult to prove that the quantum algorithm of Campbel et al. is efficient.

On the positive side, we show that if we adapt one component of the algorithm of Campbel et al. and combine it with techniques in a recent work by Eisentrager et al., then we can essentially use the quantum algorithm for computing the unit group described in Eisentrager at al. to compute the a generator of a principal ideal, thus efficiently solving the problem of Step 1.

3.5 Synthesis of Efficient Quantum Circuits

Alexei Bocharov (Microsoft Corporation – Redmond, US)

The talk offers a high-level overview of recent advances in number theoretic methods for synthesis of efficient quantum circuit. The disruptive move from circuits of nearly quartic complexity (obtained by generic Solovay-Kitaev algorithm) to circuits of linear complexity (known to exist over any specific universal quantum basis of interest) is summarized and analyzed. Examples for popular universal binary quantum bases are provided and a newer universal ternary basis is discussed in more detail. Many of the binary cases are now explained in the general framework developed in arXiv:1504.04350 and arXiv:1510.03888. Distinction between asymptotic optimality and practical optimality of efficient circuits is also explained in the talk.

3.6 A Simple and Provably Secure (Authenticated) Key Exchange based on the Learning Eith Errors Problems

Jintai Ding (University of Cincinnati, US)

Joint work of Ding, Jintai; Xie, Xiang; Lin, Xiaodong; Zhang, Jiang; Zhang, Zhenfeng; Snook, Michael; Dagdelen, Özgür
Main reference J. Ding, "A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem," IACR Cryptology ePrint Archive, Report 2012/688, 2012.
URL http://eprint.iacr.org/2012/688

Public key cryptosystems (PKC) are critical part of the foundation of modern communication systems, in particular, Internet. However Shor's algorithm shows that the existing PKC like Diffie-Hellmann key exhange, RSA and ECC can be broken by a quantum computer. To prepare for the coming age of quantum computing, we need to build new public key cryptosystems that could resist quantum computer attacks. In this lecture, we present a practical and provably secure (authenticated) key exchange protocol based on the learing with errors problems, which is conceptually simple and has strong provable security properties. Several concrete choices of parameters are provided, and a proof-of-concept implementation shows that our protocols are indeed practical.

3.7 Semantic Security and Indistinguishability in the Quantum World

Tommaso Gagliardoni (TU Darmstadt, DE)

Joint work of Gagliardoni, Tommaso; Hülsing, Andreas; Schaffner, Christian
Main reference T. Gagliaordoni, A. Hülsing, C. Schaffner, "Semantic Security and Indistinguishability in the Quantum World," arXiv:1504.05255v2 [cs.CR], 2015.
URL http://arxiv.org/abs/1504.05255v2

At CRYPTO 2013, Boneh and Zhandry initiated the study of quantum-secure encryption. They proposed first indistinguishability definitions for the quantum world where the actual indistinguishability only holds for classical messages, and they provide arguments why it might be hard to achieve a stronger notion. In this work, we show that stronger notions are achievable, where the indistinguishability holds for quantum superpositions of messages. We investigate exhaustively the possibilities and subtle differences in defining such a quantum indistinguishability notion for symmetric-key encryption schemes. We justify our stronger definition by showing its equivalence to novel quantum semantic-security notions that we introduce. Furthermore, we show that our new security definitions cannot be achieved by a large class of ciphers – those which are quasi-preserving the message length. On the other hand, we provide asecure construction based on quantum-resistant pseudo random permutations; this construction can be used as a generic transformation for turning a large class of encryption schemes into quantum indistinguishable and hence quantum semantically secure ones.

3.8 How Hard is Deciding Trivial versus Nontrivial in the Dihedral Coset Problem?

Sean Hallgren (Pennsylvania State University – University Park, US)

We revisit the dihedral coset problem and relax the problem to a decision problem where we only ask if the subgroup is order two, or trivial. The relaxed problem turns out to be as hard computationally. The decision problem asks if a given vector is in the span of all coset states. We approach this by first computing an explicit basis for the coset space and the perpendicular space. We then show that if this subspace membership problem can be efficiently solved by some restricted unitaries using the basis, then the random subset sum problem with density a constant greater than 1 can also be solved by using the same unitaries.

3.9 An Update on Hash-based Signatures.

Andreas Hülsing (TU Eindhoven, NL)

This talk will discuss recent developments in the field of hash-based signatures. On the one hand, it will give an overview of recent standardization efforts in IETF. The most recent draft describes a variant of XMSS which will be discussed, including design decisions and security reasoning. On the other hand, it will cover SPHINCS, the first practical stateless scheme solely based on hash functions and recent follow-up work.

3.10 Combining Lattice Sieving Algorithms with (Quantum) Nearest Neighbor Searching

Thijs Laarhoven (TU Eindhoven, NL)

Main reference T. Laarhoven, "Sieving for shortest vectors in lattices using angular locality-sensitive hashing," in Proc. of the 35th Annual Cryptology Conf. (CRYPTO'15), LNCS, Vol. 9215, pp. 3–22, Springer, 2015.
URL http://dx.doi.org/10.1007/978-3-662-47989-6_1

To deploy lattice-based cryptographic primitives in practice and to choose parameters for these schemes, it is critical to understand the (quantum) hardness of hard lattice problems such as the shortest vector problem (SVP): given a basis of a lattice, how long would it take a classical or quantum computer to find a shortest non-zero vector in this lattice? Various algorithms for solving SVP have been proposed over the years, and while enumeration has long stood as the main candidate for solving SVP in high dimensions, lattice sieving algorithms are closing in. In particular, the recent connection between lattice sieving and nearest neighbor searching has significantly reduced both the theoretical and practical complexities of sieving, making it competitive with enumeration.

In this talk we take a look at the main ideas behind these recent improvements to sieving using nearest neighbor search algorithms, and how quantum searching can lead to further reduced complexities when combined with classical nearest neighbor search methods for sieving. We conclude with an interesting direction for future research: Can quantum nearest neighbor methods be designed which can find nearby vectors even faster than by simply combining the best classical nearest neighbor algorithm with quantum searching?

3.11 Danger of Failure in Post-quantum Key Agreements

Bradley Lackey (University of Maryland – College Park, US)

Key agreement failure stemming from invalid public keys can lead to key leakage. We propose a method to block this, indirect public key validation, which is suitable for post-quantum key agreements.

3.12 Initial Recommendations of Long-term Secure Post-quantum Systems

Tanja Lange (TU Eindhoven, NL)

Joint work of Augot, Daniel; Batina, Lejla; Bernstein, Daniel J.; Bos, Joppe; Buchmann, Johannes; Castryck, Wouter; Dunkelman, Orr; Gueneysu, Tim; Gueron, Shay; Huelsing, Andreas; Lange, Tanja; Saied Emam Mohamed, Mohamed; Rechberger, Christian; Schwabe, Peter; Sendrier, Nicolas; Vercauteren, Frederik; Yang, Bo-Yin
URL http://pqcrypto.eu.org/

I will present the PQCRYPTO project's initial recommendations forpost-quantum cryptographic algorithms for symmetric encryption,symmetric authentication, public-key encryption, and public-keysignatures. These recommendations are chosen for confidence in theirlong-term security, rather than for efficiency (speed, bandwidth,etc.). Most of the talk slot is reserved for feedback and discussion on the proposal.

3.13 Quantum Differential Cryptanalysis

Anthony Leverrier (INRIA Rocquencourt, FR)

Joint work of Kaplan, Marc; Leurent, Gaëtan; Leverrier, Anthony; Naya-Plasencia, Maria

Quantum computers pose a serious threat to many cryptosystems. It is generally acknowledged that symmetric cryptography would be less impacted by quantum computing than public-key cryptography: indeed, in many cases, it seems that the best attack relies on Grover's search algorithm and therefore doubling the keysize essentially suffices to make a cryptosystem quantum resistant. Over the years, the symmetric cryptography community has come up with many cryptanalysis tools to test the security of symmetric cryptosystems, including for instance differential cryptanalysis. In this talk, we study the impact of quantum computing on this technique. In particular, while a quadratic speedup can be achieved sometimes, it turns out that the speedup is only sub quadratic in several cases of interest.

3.14 On the Possibility of a Quantum uSVP Algorithm

Alexander May (Ruhr-Universität Bochum, DE)

Joint work of Kirshanova, Elena; May, Alexander

We show how to turn Regev's reduction from uSVP to DCP into an algorithm. The basic idea is to use block reduction in order to compute a good basis, and to make Kuperberg's algorithm somewhat error-tolerant.Given a classical 2^{sn}-SVP algorithm, this leads to a quantum algorithm for $(n^{\frac{1}{2}+c})$-uSVP with time $2^{\sqrt{\frac{s}{c}}n}$ having constant success probability.

Unfortunately, it is not hard to show that for n^c-uSVP there is a classical algorithm with time $2^{\frac{s}{c}n}$ (having success probability 1). This also includes the special case where $c = \frac{n}{\log n}$, in which one solves $\exp(n)$-uSVP in polynomial time (by just using LLL).

So the quantum reduction achieves $\sqrt{\frac{s}{c}}$ as opposed to $\frac{s}{c}$.Unfortunately, this does not improve, since $\frac{s}{c} < 1$. Notice that $s \leq 1$ (even provably) and $c \geq 1$ (at least for the quantum algorithm, since we do not know how to completely avoid errors in Regev's reduction).

So the resulting quantum algorithm is (just) slightly worse than the classical one. Maybe with some additional tricks, this approach might eventually lead to a real improvement.

3.15 On Security of the Courtois-Finiasz-Sendrier Signature

Kirill Morozov (Kyushu University – Fukuoka, JP)

We show that the code-based Courtois-Finiasz-Sendrier (CFS) signature is strongly existentially unforgeable (SEUF-CMA) in the random oracle model, assuming hardness of the Niederreiter problem.

3.16 On the Robustness of Bucket Brigade Quantum RAM

Michele Mosca (University of Waterloo, CA)

Joint work of Arunachalam, Srinivasan; Gheorghiu, Vlad; Jochym-O'Connor, Tomas; Mosca, Michele; Srinivasan, Priyaa Varshinee
Main reference S. Arunachalam, V. Gheorghiu, T. Jochym-O'Connor, M. Mosca, P. V. Srinivasan, "On the robustness of bucket brigade quantum RAM," to appear in New Journal of Physics; pre-print available as arXiv:1502.03450v4 [quant-ph], 2015.
URL http://arxiv.org/abs/1502.03450v4

The practical cost of quantumly accessible classical memory will play a central role in the practical efficiency of some important quantum algorithms, including some algorithms relevant to quantum cryptanalysis. Will the cost be comparable to a similar amount of regular classical memory, or closer to the cost of a similar amount of general purpose fault-tolerant computational qubits?

I discussed the robustness of the bucket brigade quantum random access memory model introduced by Giovannetti, Lloyd, and Maccone. Their error analysis applies to algorithms that make few queries to the qRAM, however it does not extend to algorithms that require superpolynomially many queries. A result of Regev and Schiff [ICALP '08] implies that for a class of error models a non-trivial error rate per gate in the bucket brigade quantum memory nullifies the speed-up of the quantum searching algorithm. This motivates the need for quantum error correction within the quantum RAM, and we argue that quantum error correction for the circuit causes the quantum bucket brigade architecture to lose its primary advantages.

The practical cost of quantumly accessible classical memory remains an important open question.

References

1 Srinivasan Arunachalam, Vlad Gheorghiu, Tomas Jochym-O'Connor, Michele Mosca, Priyaa Varshinee Srinivasan. *On the robustness of bucket brigade quantum RAM*, in Proceedings of the 10th Conf. on the Theory of Quantum Computation, Communication and Cryptography (TQC'15), Leibniz International Proceedings in Informatics (LIPIcs), Vol. 44, pp. 226–244, Schloss Dagstuhl, 2015, http://dx.doi.org/10.4230/LIPIcs.TQC.2015.226.

2 Srinivasan Arunachalam, Vlad Gheorghiu, Tomas Jochym-O'Connor, Michele Mosca, Priyaa Varshinee Srinivasan. *On the robustness of bucket brigade quantum RAM*, to appear in *New Journal of Physics*.

3.17 Continuous Permutations and Entropy Power Inequalities

Maris Ozols (University of Cambridge, GB)

Joint work of Audenaert, Koenraad; Datta, Nilanjana

I described a unitary version of Cayley's theorem which allows to embed any finite group in a continuous subgroup of the unitary group. When applied to the symmetric group, this construction can be used to permute quantum systems in a continuous fashion. For the case of two systems, the resulting continuous swap operation obeys a discrete version of the entropy power inequality. My talk is based on [ADO] and [Oz].

References

1 Koenraad Audenaert, Nilanjana Datta, Maris Ozols.*Entropy power inequalities for qudits.* arXiv:1503.04213, 2015

2 Maris Ozols.*How to combine three quantum states.* arXiv:1508.00860, 2015

3.18 Dihedral HSP and Hidden Shifts: On Efficiently Solvable Instances and Small Scale LIQUi|> Simulations

Martin Roetteler (Microsoft Corporation – Redmond, US)

It has been known for some time [2] that gapped instances of the unique-shortest vector problem can be reduced to a hidden subgroup problem (HSP) in the dihedral groups D_N.

The standard approach to solving this problem is by considering coset states, however, this ignores some of the information that might be available from the hiding function $f : D_N \to S$, in particular, it ignores that values of the function. The talk is on work in progress that attempts to use the target values. I consider the equivalent formulation to this HS this HSP as a hidden shift problem over the cyclic (or more generally, abelian) group.

Starting from an already known case, namely the hidden shift problem over the hypercube where a class of efficiently solvable instances is known to correspond to so-called bent functions, I then present a simple quantum algorithm to extract the shift. The algorithm was implemented in the quantum programming LIQUi|> that is developed by the Microsoft group at Redmond [WS:2014] and a short demo of the implementation was given.

Finally, I showed that there are instances of HSPs over the dihedral group that can be solved fully efficiently—in terms of queries, time, and space complexity, as well as classical post-processing—on a quantum computer. These instances are constructed from so-called difference sets and are well-known in combinatorics. We show that the quantum algorithms for hidden shifts of the Legrende symbol [1] and of bent functions [3] can be recovered as special cases of shifted difference sets. Regarding difference sets in the cyclic group, which correspond to dihedral HSP instance, we show that a trace zero hyperplane in a finite geometry PG$(n, GF(q))$ gives rise to instances of hidden shifts in the group generated by a Singer cycle, hence, providing a new class of dihedral HSP instances that can be efficiently solved.

References

1 Wim van Dam, Sean Hallgren, and Lawrence Ip. Quantum algorithms for some hidden shift problems. *SIAM Journal on Computing*, 36(3):763–778, 2006.

2 Oded Regev. Quantum computation and lattice problems. *SIAM Journal on Computing*, 33(3):738–760, 2004.

3 Martin Roetteler. Quantum algorithms for highly non-linear Boolean functions. In *Proceedings of the 21st Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'10)*, pages 448–457, 2010.

4 Dave Wecker and Krysta M. Svore. LIQUi|>: A software design architecture and domain-specific language for quantum computing. arXiv.org preprint arXiv:1402.4467, February 2014.

3.19 Factoring Integers by CVP Algorithms for the Prime Number Lattice

Claus-Peter Schnorr (Goethe-Universität Frankfurt am Main, DE)

Main reference C-P. Schnorr, “Factoring Integers by CVP Algorithms,” in M. Fischlin, S. Katzenbach (eds.). “Number Theory and Cryptography – Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday,” LNCS, Vol. 8260, pp. 73–93, Springer, 2013.
URL http://dx.doi.org/10.1007/978-3-642-42001-6_6

1. Under reasonable heuristic assumptions it is shown that SVP and CVP of any lattice L of dimension n is solvable in polynomial time if the relative density $rd(L)$ of L is polynomially smaller than 1, essentially it is sufficient that $rd(L) = o(e\pi/2n)^{(1/4)}$. By definition $rd(L)$ is $\lambda_1(L)/max\lambda_1(L')$ for all lattices L' that have the same dimension and

the same determinant as L.Here $\lambda_1(L)$ denote the minimal length of non zero vectors of L.

2. The prime number lattice that is used for factoring large integers has a sufficiently small relative density.
3. There is a very practical speed up for the enumeration of short – resp. close – lattice vectors. The stages of the enumeration are performed according to their success probability to lead to a shorter – resp. closer – lattice vector. Stages with high success probability are done first.
4. For factoring the integer N we generate lattice vectors of the prime number lattice that are very close to the target vector $\mathbf{N}$ that represents N. For a sufficiently large prime base $p_1, ..., p_n$ such close vectors most likely yield a relation $\prod_{i=1}^{n} p_i^{e_i} = \pm \prod_{i=1}^{n} p_i^{e'_i} \mod N$ with small $e_i, e'_i \in \mathbb{N}$. We can easily factor N when given about n such independent $\mod N$ relations. Now an algorithm implemented by C. Morgan, A. Schickedanz, N. Hahn generates for $N = \Theta(10^{14})$ one $\mod N$ relation every 2 seconds on the average. This factors $N = \Theta(10^{14})$ in about 3 minutes. The method generates particular relations given by p_n-smooth integers u, v such that $|u - vN|$ is p_n-smooth too. (By definition u is p_n-smooth if it has no prime-factor larger than p_n. Here are some recent improvements).
5. We perform the stages in enumerating lattice vectors close to $\mathbf{N}$ according to their success rate to provide a $\mod N$ relation. Stages with high success rates are done first and stages with low success rate are put back to be performed later or they are even cut of if the success rate is extremely small. The success rate depends on the consumed distance to the target vector at the current stage and on the probability that the consumed distance can be extended to a new minimal distance of a lattice vectors to the target vector. This probability is based on the Gaussian volume heuristics for lattices.
6. In each round we randomly scale the basis vectors of a BKZ-reduced basis of the prime number lattice. The scaling fines each prime p_i randomly with probability 1/2. The scaling produces independent $\mod N$ relations each round.
7. We extremely prune the enumeration of lattice vectors close to $\mathbf{N}$ so that a very small fraction of these vectors can be efficiently generated still providing at least $n \mod N$ relations.

3.20 LIQUi|>: A Software Design Architecture and Domain-Specific Language for Quantum Computing

Krysta Svore (Microsoft Corporation – Redmond, US)

Joint work of Svore, Krysta; Wecker, Dave
Main reference D. Wecker, K. M. Svore, "LIQUi|>: A Software Design Architecture and Domain-Specific Language for Quantum Computing," arXiv:1402.4467v1 [quant-ph], 2014.
URL http://arxiv.org/abs/1402.4467v1

Languages, compilers, and computer-aided design tools will be essential for sscalable quantum computing, which promises an exponential leap in our ability to execute complex tasks. LIQUi|> is a modular software architecture designed tto control quantum hardware. It enables easy programming, compilation, and simulation of quantum algorithms and circuits, and is independent of a specific quantum architecture. LIQUi|> contains an embedded, domain specific language designed for programming quantum algorithms, with $F\#$ as the host language. It also allows the extraction of a circuit data structure that can be used for optimization, rendering, or translation. The circuit can also be exported to external hardware and software environments. Two different simulation environments are available to the user which allow a trade-off between number of qubits and class of operations. LIQUi|> has been implemented on a wide range of runtimes as back-ends with a single user front-end. We describe the significant components of the design architecture and how to express any given quantum algorithm.

3.21 Improvement on BKZ Lattice Reduction Algorithm

Tsuyoshi Takagi (Kyushu University – Fukuoka, JP)

Joint work of Wang, Yuntao; Aono, Yoshinori; Hayashi, Takuya

The security of lattice-based cryptography is based on the hardness of finding a short vector in the underlying lattice. Currently the most efficient algorithms for solving this problem in random lattices of large dimensions are perhaps the BKZ algorithm and its modifications. In this talk, we investigate a variant of BKZ algorithm, called progressive BKZ, which performs the BKZ reduction starting from the small block size and switches to larger ones so that the total cost used for the local enumeration algorithm is minimized. We discuss how to accelerate the speed of the progressive BKZ algorithm for optimizing the parameters: the block size, the search radius and probability of the local enumeration algorithm, and the successive sizes of Gram-Schmidt orthogonal basis known as geometric series assumption. Using our improved progressive BKZ we have solved the ideal lattice challenge from Darmstadt in $2^{20.7}$ and $2^{24.0}$ seconds on a standard PC for 600 and 650 dimensions, respectively.

3.22 How to Address Post-quantum in Economy

Enrico Thomae (Operational Services GmbH – Zwickau, DE)

This talk gives a brief overview on how information security is addressed in economy by national and international standards (e.g. ISO27001) and big companies (e.g. Volkswagen). Using the case study of broken RFID technology, we show the limitations of this process. The main part of the talk should be a discussion on how we could overcome those limitations for Post-Quantum Cryptography. We will encourage to participate in generating an open access risk analysis.

3.23 Progress Towards Quantum Processors and Quantum Interfaces: Why Experimentalists Start Listening to Computer Science

Frank K. Wilhelm (Universität des Saarlandes, DE)

As a peripheral guest to the event, I reported on the status of the implementation of quantum computers with a heavy focus on superconducting integrated circuits. There is a clear sign for optimism and the threshold at which a quantum processor outperforms a classical computer at least in simulating itself is imminent. While this is not a useful milestone, it shows that traditional approaches to modeling quantum processor experiments are reaching an end and experimentalists should work with computer scientists on topics like validation.

Participants

- Gorjan Alagic
University of Copenhagen, DK
- Aleksandrs Belovs
University of Latvia, LV
- Daniel J. Bernstein
Univ. of Illinois – Chicago, US
- Jean-François Biasse
University of South Florida – Tampa, US
- Alexei Bocharov
Microsoft Corporation – Redmond, US
- Harry Buhrman
CWI – Amsterdam, NL
- André Chailloux
INRIA Rocquencourt, FR
- Jintai Ding
University of Cincinnati, US
- Hang Dinh
Indiana Univ. South Bend, US
- Jürgen Eschner
Universität des Saarlandes, DE
- Jennifer Katherine Fernick
University of Waterloo, CA
- Tommaso Gagliardoni
TU Darmstadt, DE
- Markus Grassl
Univ. Erlangen-Nürnberg, DE
- Sean Hallgren
Pennsylvania State University – University Park, US
- Peter Hoyer
University of Calgary, CA
- Andreas Hülsing
TU Eindhoven, NL
- Stacey Jeffery
CalTech – Pasadena, US
- Stavros Kousidis
BSI – Bonn, DE
- Thijs Laarhoven
TU Eindhoven, NL
- Bradley Lackey
University of Maryland – College Park, US
- Tanja Lange
TU Eindhoven, NL
- Anthony Leverrier
INRIA Rocquencourt, FR
- Yi-Kai Liu
NIST – Gaithersburg, US
- Alexander May
Ruhr-Universität Bochum, DE
- Kirill Morozov
Kyushu Univ. – Fukuoka, JP
- Michele Mosca
University of Waterloo, CA
- Michael Naehrig
Microsoft Res. – Redmond, US
- Maris Ozols
University of Cambridge, GB
- Ray Perlner
NIST – Gaithersburg, US
- Martin Roetteler
Microsoft Corporation – Redmond, US
- Christian Schaffner
University of Amsterdam, NL
- John M. Schanck
University of Waterloo, CA
- Claus-Peter Schnorr
Goethe-Universität Frankfurt am Main, DE
- Nicolas Sendrier
INRIA – Le Chesnay, FR
- Dan J. Shepherd
CESG – Cheltenham, GB
- Daniel Smith-Tone
University of Louisville, US
- Fang Song
University of Waterloo, CA
- Rainer Steinwandt
Florida Atlantic University – Boca Raton, US
- Krysta Svore
Microsoft Corporation – Redmond, US
- Tsuyoshi Takagi
Kyushu Univ. – Fukuoka, JP
- Enrico Thomae
operational services GmbH – Zwickau, DE
- Jean-Pierre Tillich
INRIA – Le Chesnay, FR
- Joop van de Pol
University of Bristol, GB
- Frank K. Wilhelm
Universität des Saarlandes, DE
- Bo-Yin Yang
Academica Sinica – Taipei, TW