Report from Dagstuhl Seminar 21421

Quantum Cryptanalysis

Edited by

Stacey Jeffery[1], Michele Mosca[2], Maria Naya-Plasencia[3], and Rainer Steinwandt[4]

1 **CWI – Amsterdam, NL,** smjeffery@gmail.com
2 **University of Waterloo, CA,** michele.mosca@uwaterloo.ca
3 **INRIA – Paris, FR,** maria.naya_plasencia@inria.fr
4 **University of Alabama in Huntsville, US,** rs0141@uah.edu

Abstract

This seminar report documents the program and the outcomes of Dagstuhl Seminar 21421 *Quantum Cryptanalysis*. The seminar took place in a hybrid format in Fall 2021. The report starts out with the motivation and comments on the organization of this instance of the Dagstuhl Seminar series on Quantum Cryptanalysis, followed by abstracts of presentations. The presentation abstracts were provided by seminar participants.

Seminar October 17–22, 2021 – http://www.dagstuhl.de/21421
2012 ACM Subject Classification Hardware → Quantum technologies; Security and privacy → Cryptanalysis and other attacks; Theory of computation → Computational complexity and cryptography
Keywords and phrases computational algebra, post-quantum cryptography, quantum computing, quantum resource estimation
Digital Object Identifier 10.4230/DagRep.11.9.64
Edited in cooperation with André Schrottenloher

1 Executive Summary

Stacey Jeffery (CWI – Amsterdam, NL)
Michele Mosca (University of Waterloo, CA)
Maria Naya-Plasencia (INRIA – Paris, FR)
Rainer Steinwandt (University of Alabama in Huntsville, US)

Motivation and scope

Owing to the ongoing pandemic, this (sixth) installment of the Dagstuhl Seminar series on *Quantum Cryptanalysis* was held in a hybrid format. The focus of this seminar was on deployed schemes and more mature post-quantum cryptographic schemes, such as Round 3 candidates in NIST's standardization effort. For the technical program of the seminar, we encouraged research on

Quantum algorithmic innovations to attack cryptographic building blocks, leveraging state-of-the-art quantum computing. How can we leverage quantum algorithms to improve cryptanalytic capabilities, and how can we optimize the best available cryptanalytic results in meaningful quantum attack models?

Techniques and software tools to optimize and quantify resources for such attacks. Can we establish reasonably precise quantum resource counts for cryptanalytic attacks, especially for problem instances and parameter choices that are actually deployed or considered for standardization for future deployment?

Quantum attacks against today's RSA or elliptic-curve based cryptography and against modern block ciphers, which help us understand the urgency for transitioning to post-quantum solutions, fall in the seminar scope. As in the past, the seminar brought together researchers who work in the field of quantum computing with experts in classical cryptography, taking into account the latest advances in both fields. With 26 participants on site and 29 remote participants, Schloss Dagstuhl hosted a broad group of leading experts from across the globe.

Organization

The ongoing pandemic impacted the organization of the seminar, which for the first time was offered in a hybrid format. Thanks to the available technology at Schloss Dagstuhl and the efficient support of two volunteers (Shaun Kepley and Galina Pass), integrating remote presentations into the schedule worked smoothly.

The scheduling accounted for time zone differences and, as in the past, we left ample time for discussions and collaboration – for a typical day, we scheduled no more than four presentations. Following the Dagstuhl tradition and in line with prior seminars in the Quantum Cryptanalysis series, there was no technical program during Wednesday afternoon, leaving participants time for exploring the surroundings, spending time on research, or taking care of testing requirements for upcoming international travel.

Results and next steps

The collaboration between cryptographers and experts in quantum computing has come a long way, and it seems fair to say that this Dagstuhl Seminar series has contributed to this positive development. The quantum cryptanalytic progress in symmetric cryptography is very noticeable. This was evidenced by the number and quality of presentations on this subject offered by seminar participants. On the asymmetric side, the presentations demonstrated fascinating research progress on understanding computational problems related to lattices and codes. At the same time, a need remains to better quantify the potential of quantum algorithms for tackling hardness assumptions as used in state-of-the-art post-quantum proposals.

2 Table of Contents

3 Overview of Talks

3.1 Enumeration-based Lattice Reduction

Shi Bai (Florida Atlantic University – Boca Raton, US)

Joint work of Martin R. Albrecht, Shi Bai, Pierre-Alain Fouque, Paul Kirchner, Damien Stehlé, Weiqiang Wen
Main reference Martin R. Albrecht, Shi Bai, Pierre-Alain Fouque, Paul Kirchner, Damien Stehlé, Weiqiang Wen: "Faster Enumeration-Based Lattice Reduction: Root Hermite Factor $k^{1/(2k)}$ Time $k^{k/8+o(k)}$", in Proc. of the Advances in Cryptology – CRYPTO 2020 – 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part II, Lecture Notes in Computer Science, Vol. 12171, pp. 186–212, Springer, 2020.
URL https://doi.org/10.1007/978-3-030-56880-1_7

Lattice reduction algorithms have received much attention in recent years due to their relevance to lattice-based cryptography. In this talk, we will discuss some of the recent developments on enumeration-based lattice reduction algorithms.

First, we will discuss a lattice reduction algorithm that achieves root Hermite factor $k^{(1/(2k))}$ in time $k^{(k/8+o(k))}$ and polynomial memory. This improves the previously best known enumeration-based lattice-reduction algorithms which achieve the same quality, but in time $k^{(k/(2e)+o(k))}$. The main idea is to conduct the preprocessing in a larger dimension than the enumerate dimension. Second, we discuss the usage of approximate enumeration oracles in BKZ, together with extended preprocessing ideas. In the end, we will illustrate some simulated results to demonstrate their practical behavior.

References

1 Martin R. Albrecht, Shi Bai, Pierre-Alain Fouque, Paul Kirchner, Damien Stehlé, Weiqiang Wen, Faster Enumeration-Based Lattice Reduction: Root Hermite Factor $k^{(1/(2k))}$ Time $k^{(k/8+o(k))}$. CRYPTO (2) 2020: 186-212

2 Martin R. Albrecht, Shi Bai, Jianwei Li, Joe Rowell, Lattice Reduction with Approximate Enumeration Oracles – Practical Algorithms and Concrete Performance. CRYPTO (2) 2021: 732-759

3.2 Quantum hardness of the code equivalence problem

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

Joint work of Alessandro Barenghi, Jean-François Biasse, Edoardo Persichetti, Paolo Santini
Main reference Alessandro Barenghi, Jean-François Biasse, Edoardo Persichetti, Paolo Santini: "LESS-FM: Fine-Tuning Signatures from the Code Equivalence Problem", in Proc. of the Post-Quantum Cryptography – 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20-22, 2021, Proceedings, Lecture Notes in Computer Science, Vol. 12841, pp. 23–43, Springer, 2021.
URL https://doi.org/10.1007/978-3-030-81293-5_2

In this talk we introduce quantum algorithms for solving the Code Equivalence problem. Code Equivalence can serve as the hardness assumption of certain code-based signature schemes. This problem has been studied for a long time, but not in the context of (post-quantum) cryptography. In this presentation, we showed how to use quantum computers to speed up the classical algorithm due to Leon (and its subsequent improvements, in particular a recent work from Beulens), and the Support Splitting Algorithm (SSA) due to Sendrier.

References

1 Jean-François Biasse, Giacomo Micheli, Edoardo Persichetti, Paolo Santini, LESS is More: Code-Based Signatures Without Syndromes. AFRICACRYPT 2020: 45-65

2 Alessandro Barenghi, Jean-François Biasse, Edoardo Persichetti, Paolo Santini, LESS-FM: Fine-Tuning Signatures from the Code Equivalence Problem. PQCrypto 2021: 23-43

3.3 Quantum Linearization Attacks

Xavier Bonnetain (University of Waterloo, CA)

Joint work of Xavier Bonnetain, Gaëtan Leurent, María Naya-Plasencia, André Schrottenloher
Main reference Xavier Bonnetain, Gaëtan Leurent, María Naya-Plasencia, André Schrottenloher: "Quantum Linearization Attacks", in Proc. of the Advances in Cryptology – ASIACRYPT 2021 – 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part I, Lecture Notes in Computer Science, Vol. 13090, pp. 422–452, Springer, 2021.
URL https://doi.org/10.1007/978-3-030-92062-3_15

Recent works have shown that quantum period-finding can be used to break many popular constructions (some block ciphers such as Even-Mansour, multiple MACs and AEs...) in the superposition query model. So far, all the constructions broken exhibited a strong algebraic structure, which enables to craft a periodic function of a single input block. Recovering the secret period allows to recover a key, distinguish, break the confidentiality or authenticity of these modes.

In this paper, we introduce the *quantum linearization attack*, a new way of using Simon's algorithm to target MACs in the superposition query model. Specifically, we use inputs of multiple blocks as an interface to a function hiding a linear structure. Recovering this structure allows to perform forgeries.

We also present some variants of this attack that use other quantum algorithms, which are much less common in quantum symmetric cryptanalysis: Deutsch's, Bernstein-Vazirani's, and Shor's. To the best of our knowledge, this is the first time these algorithms have been used in quantum forgery or key-recovery attacks.

Our attack breaks many parallelizable MACs such as LightMac, PMAC, and numerous variants with (classical) beyond-birthday-bound security (LightMAC+, PMAC) or using tweakable block ciphers (ZMAC). More generally, it shows that constructing parallelizable quantum-secure PRFs might be a challenging task.

3.4 Quantum Period Finding against Symmetric Primitives in Practice

Xavier Bonnetain (University of Waterloo, CA)

Joint work of Xavier Bonnetain, Samuel Jaques
Main reference Xavier Bonnetain, Samuel Jaques: "Quantum Period Finding against Symmetric Primitives in Practice", IACR Trans. Cryptogr. Hardw. Embed. Syst., Vol. 2022(1), pp. 1–27, 2022.
URL https://doi.org/10.46586/tches.v2022.i1.1-27

We present the first complete description of a quantum circuit for the offline Simon's algorithm, and estimate its cost to attack the MAC Chaskey, the block cipher PRINCE and the NIST lightweight candidate AEAD scheme Elephant. These attacks require a reasonable amount

of qubits, comparable to the number of qubits required to break RSA-2048. They are faster than other collision algorithms, and the attacks against PRINCE and Chaskey are the most efficient known to date. As Elephant has a key smaller than its state size, the algorithm is less efficient and ends up more expensive than exhaustive search.

We also propose an optimized quantum circuit for boolean linear algebra as well as complete reversible implementations of PRINCE, Chaskey, spongent and Keccak which are of independent interest for quantum cryptanalysis. We stress that our attacks could be applied in the future against today's communications, and recommend caution when choosing symmetric constructions for cases where long-term security is expected.

3.5 Lattice sieving via quantum random walks

André Chailloux (INRIA – Paris, FR)

Joint work of André Chailloux, Johanna Loyer
Main reference André Chailloux, Johanna Loyer: "Lattice Sieving via Quantum Random Walks", in Proc. of the Advances in Cryptology – ASIACRYPT 2021 – 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part IV, Lecture Notes in Computer Science, Vol. 13093, pp. 63–91, Springer, 2021.
URL https://doi.org/10.1007/978-3-030-92068-5_3

Lattice-based cryptography is one of the leading proposals for post-quantum cryptography. The Shortest Vector Problem (SVP) is arguably the most important problem for the cryptanalysis of lattice-based cryptography, and many lattice-based schemes have security claims based on its hardness. The best quantum algorithm for the SVP is due to Laarhoven [1] and runs in (heuristic) time $2^{0.2653d+o(d)}$ where d is the dimension of the lattice. In this article, we present an improvement over Laarhoven's result and present an algorithm that has a (heuristic) running time of $2^{0.2570d+o(d)}$ We also present time-memory trade-offs where we quantify the amount of quantum memory and quantum random access memory of our algorithm. The core idea is to replace Grover's algorithm used in [1] in a key part of the sieving algorithm by a quantum random walk in which we add a layer of local sensitive filtering.

References

1 Thijs Laarhoven. *Search problems in cryptography, From fingerprinting to lattice sieving*. PhD thesis, Eindhoven University of Technology, 2016

3.6 Quantum Reduction of Finding Short Code Vectors to the Decoding Problem

Thomas Debris-Alazard (Ecole Polytechnique – Palaiseau, FR)

Joint work of Thomas Debris-Alazard, Maxime Remaud, Jean-Pierre Tillich
Main reference Thomas Debris-Alazard, Maxime Remaud, Jean-Pierre Tillich: "Quantum Reduction of Finding Short Code Vectors to the Decoding Problem", CoRR, Vol. abs/2106.02747, 2021.
URL https://arxiv.org/abs/2106.02747

We give a quantum reduction from finding short codewords in a random linear code to decoding for the Hamming metric. This is the first time such a reduction (classical or quantum) has been obtained. Our reduction adapts to linear codes Stehlé-Steinfield-Tanaka-Xagawa' re-interpretation of Regev's quantum reduction from finding short lattice vectors to

solving the Closest Vector Problem. The Hamming metric is a much coarser metric than the Euclidean metric and this adaptation has needed several new ingredients to make it work. For instance, in order to have a meaningful reduction it is necessary in the Hamming metric to choose a very large decoding radius and this needs in many cases to go beyond the radius where decoding is unique. Another crucial step for the analysis of the reduction is the choice of the errors that are being fed to the decoding algorithm. For lattices, errors are usually sampled according to a Gaussian distribution. However, it turns out that the Bernoulli distribution (the analogue for codes of the Gaussian) is too much spread out and can not be used for the reduction with codes. Instead we choose here the uniform distribution over errors of a fixed weight and bring in orthogonal polynomials tools to perform the analysis and an additional amplitude amplification step to obtain the aforementioned result.

3.7 Cryptanalysis of HFEv-

Jintai Ding (Tsinghua University – Beijing, CN)

Joint work of Chengdong Tao, Albrecht Petzoldt, Jintai Ding
Main reference Chengdong Tao, Albrecht Petzoldt, Jintai Ding: "Efficient Key Recovery for All HFE Signature Variants", in Proc. of the Advances in Cryptology – CRYPTO 2021 – 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I, Lecture Notes in Computer Science, Vol. 12825, pp. 70–93, Springer, 2021.
URL https://doi.org/10.1007/978-3-030-84242-0_4

The HFE cryptosystem is one of the best known multivariate schemes. Especially in the area of digital signatures, the HFEv- variant offers short signatures and high performance. Recently, an instance of the HFEv- signature scheme called GeMSS was elected as one of the alternative candidates for signature schemes in the third round of the NIST Post Quantum Crypto (PQC) Standardization Project. In this paper, we propose a new key recovery attack on the HFEv- signature scheme. Our attack shows that both the Minus and the Vinegar modification do not enhance the security of the basic HFE scheme significantly. This shows that it is very difficult to build a secure and efficient signature scheme on the basis of HFE. In particular, we use our attack to show that the proposed parameters of the GeMSS scheme are not as secure as claimed.

3.8 On completely factoring any integer efficiently in a single run of an order-finding algorithm

Martin Ekerå (KTH Royal Institute of Technology – Stockholm, & Swedish NCSA, SE)

Main reference Martin Ekerå: "On completely factoring any integer efficiently in a single run of an order-finding algorithm", Quantum Inf. Process., Vol. 20(6), p. 205, 2021.
URL https://doi.org/10.1007/s11128-021-03069-1

In this talk, we present the recent paper [1]: Specifically, we show, for any integer N, that given the order of a single element selected uniformly at random from $\mathbb{Z}_N^*$, we can completely factor N efficiently classically with very high probability. The implication of this result, in the context of Shor's factoring algorithm, is that a single run of the quantum order-finding part is usually sufficient. All factors may then be recovered in a classical post-processing step.

The classical algorithm needed for this step is essentially a slightly modified randomized version of an algorithm due to Miller. For further details, interested readers are referred to the abstract and full text of [1].

References

1 Martin Ekerå, On completely factoring any integer efficiently in a single run of an order-finding algorithm. Quantum Inf. Process. 20(6): 205 (2021)

3.9 Limitations of the Macaulay matrix approach for using the HHL algorithm to solve multivariate polynomial systems

András Gilyén (Alfréd Rényi Institute of Mathematics – Budapest, HU)

Joint work of Jintai Ding, Vlad Gheorghiu, Sean Hallgren, Jianqiang Li
Main reference Jintai Ding, Vlad Gheorghiu, András Gilyén, Sean Hallgren, Jianqiang Li: "Limitations of the Macaulay matrix approach for using the HHL algorithm to solve multivariate polynomial systems", CoRR, Vol. abs/2111.00405, 2021.
URL https://arxiv.org/abs/2111.00405

Recently Chen and Gao (2017) proposed a new quantum algorithm for Boolean polynomial system solving, motivated by the cryptanalysis of some post-quantum cryptosystems. The key idea of their approach is to apply a Quantum Linear System (QLS) algorithm to a Macaulay linear system over $\mathbb{C}$, which is derived from the Boolean polynomial system. The efficiency of their algorithm depends on the condition number of the Macaulay matrix. In this paper, we give a strong lower bound on the condition number as a function of the Hamming weight of the Boolean solution, and show that in many (if not all) cases a Grover-based exhaustive search algorithm outperforms their algorithm. Then, we improve upon Chen and Gao's algorithm by introducing the Boolean Macaulay linear system over $\mathbb{C}$ by reducing the original Macaulay linear system. This improved algorithm could potentially significantly outperform the brute-force algorithm, when the Hamming weight of the solution is logarithmic in the number of Boolean variables. Furthermore, we provide a simple and more elementary proof of correctness for our improved algorithm using a reduction employing the Valiant-Vazirani affine hashing method, and also extend the result to polynomial systems over $\mathbb{F}_q$ improving on subsequent work by Chen, Gao and Yuan (2018). We also suggest a new approach for extracting the solution of the Boolean polynomial system via a generalization of the quantum coupon collector problem of Arunachalam, Belovs, Childs, Kothari, Rosmanis, and de Wolf (2020).

3.10 Quantum Collision Attacks on Reduced SHA-256 and SHA-512

Akinori Hosoyamada (NTT – Tokyo, JP)

Joint work of Akinori Hosoyamada, Yu Sasaki
Main reference Akinori Hosoyamada, Yu Sasaki: "Quantum Collision Attacks on Reduced SHA-256 and SHA-512", in Proc. of the Advances in Cryptology – CRYPTO 2021 – 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I, Lecture Notes in Computer Science, Vol. 12825, pp. 616–646, Springer, 2021.
URL https://doi.org/10.1007/978-3-030-84242-0_22

In this talk, we present dedicated quantum collision attacks on SHA-256 and SHA-512. The attacks reach 38 and 39 steps, respectively, which significantly improve the classical attacks for 31 and 27 steps. Both attacks adopt the framework of the previous work that converts many semi-free-start collisions into a 2-block collision, and are faster than the generic attack in the cost metric of time-space tradeoff. We observe that the number of required semi-free-start collisions can be reduced in the quantum setting, which allows us to convert the previous classical 38 and 39 step semi-free-start collisions into a collision. The idea behind our attacks is simple and will also be applicable to other cryptographic hash functions. This talk is based on our paper of the same title presented at CRYPTO 2021.

3.11 Automatizing applications of Simon's algorithm to symmetric crypto

Nils Gregor Leander (Ruhr-Universität Bochum, DE)

Joint work of Federico Canale, Nils Gregor Leander, Lukas Stennes

We simplify the search for new applications of Simon's algorithm and thereby overcome the increasing complexity of the attacks in the literature.

More precisely, we present a generic algorithm that aims at finding, given a symmetric cryptographic scheme E, non-trivial periodic functions f, that can then be efficiently computed by a quantum computer.

Our approach here is to represent those functions f dependent on E by a class of circuits. Those circuits can make use of oracle gates for E and potentially further oracle gates for internal parts of the scheme E. We then automatically examine all circuits up to a certain number of gates and test each of them for periodicity, by instantiating the respective function on small dimensions. Of course, this means that many useless circuits, as well as many useless periods, are generated. The main technical contribution and work is aimed at addressing this problem, and keeping the process efficient.

Using our approach, we automatically find the first efficient key-recovery attacks against constructions like 5-round MISTY L-FK or 5-round Feistel-FK (with internal permutation) using Simon's algorithm.

3.12 Test of Quantumness with Small-Depth Quantum Circuits

François Le Gall (Nagoya University, JP)

Joint work of Shuichi Hirahara, François Le Gall
Main reference Shuichi Hirahara, François Le Gall: "Test of Quantumness with Small-Depth Quantum Circuits", in Proc. of the 46th International Symposium on Mathematical Foundations of Computer Science, MFCS 2021, August 23-27, 2021, Tallinn, Estonia, LIPIcs, Vol. 202, pp. 59:1–59:15, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.
URL https://doi.org/10.4230/LIPIcs.MFCS.2021.59

Recently Brakerski, Christiano, Mahadev, Vazirani and Vidick (FOCS 2018) have shown how to construct a test of quantumness based on the learning with errors (LWE) assumption: a test that can be solved efficiently by a quantum computer but cannot be solved by a classical polynomial-time computer under the LWE assumption. This test has lead to several cryptographic applications. In particular, it has been applied to producing certifiable randomness from a single untrusted quantum device, self-testing a single quantum device and device-independent quantum key distribution.

In this paper, we show that this test of quantumness, and essentially all the above applications, can actually be implemented by a very weak class of quantum circuits: constant-depth quantum circuits combined with logarithmic-depth classical computation. This reveals novel complexity-theoretic properties of this fundamental test of quantumness and gives new concrete evidence of the superiority of small-depth quantum circuits over classical computation.

3.13 Quantum Time-Space Tradeoff for Finding Multiple Collision Pairs

Frédéric Magniez (CNRS – Paris, FR)

Joint work of Yassine Hamoudi, Frédéric Magniez
Main reference Yassine Hamoudi, Frédéric Magniez: "Quantum Time-Space Tradeoff for Finding Multiple Collision Pairs", in Proc. of the 16th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2021, July 5-8, 2021, Virtual Conference, LIPIcs, Vol. 197, pp. 1:1–1:21, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.
URL https://doi.org/10.4230/LIPIcs.TQC.2021.1

We study the problem of finding K collision pairs in a random function $f : [N] \to [N]$ by using a quantum computer. We prove that the number of queries to the function in the quantum random oracle model must increase significantly when the size of the available memory is limited.

Classically, the same question has only been settled recently by Dinur [Eurocrypt'20], who showed that the Parallel Collision Search algorithm of van Oorschot and Wiener achieves the optimal time-space tradeoff.

Our result limits the extent to which quantum computing may decrease this tradeoff. Our method is based on a novel application of Zhandry's recording query technique [Crypto'19] for proving lower bounds in the exponentially small success probability regime.

As a second application, we give a simpler proof of the time-space tradeoff for sorting N numbers on a quantum computer, which was first obtained by Klauck, Špalek and de Wolf.

3.14 Boosting the hybrid attack on NTRU

Phong Q. Nguyen (INRIA & ENS Paris, FR)

Main reference Nguyen, Phong Q.: "Boosting the Hybrid Attack on NTRU: Torus LSH, Permuted HNF and Boxed Sphere." Third PQC standardization conference, 2021.
URL https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/nguyen-boosting-hybridboost-pqc2021.pdf

We revisit collision attacks on NTRU, namely Odlyzko's meet-in-the-middle attack and Howgrave-Graham's hybrid attack. We show how to simplify and improve these attacks with respect to effi- ciency, analysis and ease of implementation. Our main ingredients are randomization and geometry: we randomize the attacks by introducing torus variants of locality sensitive hashing (LSH) and new HNF-like bases of the NTRU lattice; and we establish a connection between the success probability of the hybrid attack and the intersection of an n-dimensional sphere with a random box. We provide mathematical and algorithmic bounds for such intersections, which is of independent interest. Our new analyses remain partially heuristic, but are arguably much more sound than previous analyses, and are backed by experiments. Our results show that the security estimates of the NTRU finalist in NIST's post-quantum standardization need to be revised.

3.15 Scalable Methods and Tools for (Very Large) Quantum Circuits

Alexandru Paler (Aalto University, FI)

Quantum circuits compilation and optimisation are an important building block of the quantum computing software stacks. Quantum hardware is a very scarce resource, and the successful execution of the first practical quantum computations, error-corrected or not, depends on squeezing logical circuits on the available quantum hardware. Moreover, in the context of fault-tolerant quantum computations, the execution of the circuits requires online, real-time compilation and optimisation methods. Consequently, scalability is more than a desirable characteristic of the methods and tools forming the software stacks. This talk follows a top-down description of the steps involved in the preparation of fault-tolerant quantum circuit executions. We present state-of-the-art tools and analyse their scalability with respect to very large instances of practical quantum circuits. We also discuss methods for verifying the correctness of resulting optimised circuits, as well as preliminary results on applying machine learning techniques for circuit optimisation.

3.16 Fast factoring integers by SVP algorithms

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

Main reference Claus-Peter Schnorr:"Fast Factoring Integers by SVP Algorithms, corrected. IACR Cryptol. ePrint Arch. 2021: 933 (2021)
URL https://eprint.iacr.org/2021/933

To factor an integer N we construct n triples of p_n-smooth integers $u, v, |u - vN|$ for the n-th prime p_n. Denote such triple a fac-relation. We get fac-relations from a nearly shortest vector of the lattice $\mathcal{L}(\mathbf{R}_{n,f})$ with basis matrix $\mathbf{R}_{n,f} \in \mathbb{R}^{(n+1)\times(n+1)}$ where $f\colon [1,n] \to [1,n]$ is a permutation of $[1,2,\ldots,n]$ and $(f(1),\ldots,f(n),N' \ln N)$ is the diagonal and $(N' \ln p_1,\ldots,N' \ln p_n, N' \ln N)$ for $N' = N^{\frac{1}{n+1}}$ is the last line of $\mathbf{R}_{n,f}$. An independent permutation f' yields an independent fac-relation. We find sufficiently short lattice vectors by strong primal-dual reduction of $\mathbf{R}_{n,f}$. We factor $N \approx 2^{400}$ by $n = 47$ and $N \approx 2^{800}$ by $n = 95$. Our accelerated strong primal-dual reduction of [1] factors integers $N \approx 2^{400}$ and $N \approx 2^{800}$ by $4.2 \cdot 10^9$ and $8.4 \cdot 10^{10}$ arithmetic operations, much faster then the quadratic sieve and the number field sieve and using much smaller primes p_n. This destroys the RSA cryptosystem.

References

1 N. Gama and P.Q. Nguyen, Finding Short Lattice Vectors within Mordell's Inequality. Proc. of the 2008 ACM Symposiumon on Theory of Computing, pp. 208-216, 2008

3.17 Beyond quadratic speedups in quantum attacks on symmetric schemes

André Schrottenloher (CWI – Amsterdam, NL)

Joint work of Xavier Bonnetain, André Schrottenloher, Ferdinand Sibleyras
Main reference Xavier Bonnetain, André Schrottenloher, Ferdinand Sibleyras: "Beyond quadratic speedups in quantum attacks on symmetric schemes", CoRR, Vol. abs/2110.02836, 2021.
URL https://arxiv.org/abs/2110.02836

In symmetric cryptography, doubling the sizes of keys is often assumed to be a sufficient protection against quantum adversaries. This is because Grover's quantum search algorithm, which can be used for generically recovering the key, is limited to a quadratic speedup.

In this talk, we will study this key-recovery problem for block cipher constructions in the ideal model, such as the Even-Mansour or FX ciphers. In the superposition setting (a strong model of quantum attackers), some of these constructions are completely broken, even though they have classical security proofs. But attacks using only classical queries, which are deemed more realistic, have remained much more limited to date. As they were reaching quadratic speedups at most, they confirmed so far the intuition that security levels should just be doubled in general.

We will show that this is not always the case, by presenting a symmetric block cipher design with: 1. a security bound of $2^{2.5n}$ against classical adversaries, and: 2. a quantum attack in time roughly 2^n, that uses classical queries only. This gives, for the first time, a proven 2.5 speedup on a quantum attack in the classical query model.

3.18 Provable quantum algorithms for SVP

Yixin Shen (Royal Holloway University of London, GB)

Joint work of Divesh Aggarwal, Yanlin Chen, Rajendra Kumar, Yixin Shen
Main reference Divesh Aggarwal, Yanlin Chen, Rajendra Kumar, Yixin Shen: "Improved (Provable) Algorithms for the Shortest Vector Problem via Bounded Distance Decoding", CoRR, Vol. abs/2002.07955, 2020.
URL https://arxiv.org/abs/2002.07955

The most important computational problem on lattices is the Shortest Vector Problem (SVP). We present new algorithms that improve the state-of-the-art for provable quantum algorithms for SVP, ie, we present a quantum algorithm that runs in time $2^{0.953n+o(n)}$ and requires $2^{0.5n+o(n)}$ classical memory and poly(n) qubits. In the Quantum Random Access Memory (QRAM) model our algorithm takes only $2^{0.873n+o(n)}$ time and requires a QRAM of size $2^{0.1604n+o(n)}$, poly(n) qubits and $2^{0.5n}$ classical space. This improves over the previously fastest classical (which is also the fastest quantum) algorithm due to [1] that has a time and space complexity $2^{n+o(n)}$. The time complexity of our quantum algorithms are obtained using a known upper bound on a quantity related to the lattice kissing number which is $2^{0.402n}$. We conjecture that for most lattices this quantity is a $2^{o(n)}$. Assuming that this is the case, our quantum algorithm runs in time $2^{0.750n+o(n)}$ and our quantum algorithm in the QRAM model runs in time $2^{0.667n+o(n)}$.

References

1 Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the shortest vector problem in 2^n time using discrete gaussian sampling: Extended abstract. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*, pages 733–742, 2015.

3.19 NIST status update on the 3rd round

Daniel C. Smith-Tone (NIST – Gaithersburg, US)

NIST provided historical information, current status updates and future timeline information on the 3rd Round PQC standardization process.

Participants

- Marco Baldi
Polytechnic University of Marche, IT
- Jean-François Biasse
University of South Florida – Tampa, US
- Xavier Bonnetain
University of Waterloo, CA
- André Chailloux
INRIA – Paris, FR
- Thomas Debris-Alazard
Ecole Polytechnique – Palaiseau, FR
- Yfke Dulek
CWI – Amsterdam, NL
- Martin Ekerå
KTH Royal Institute of Technology – Stockholm, & Swedish NCSA, SE
- Stacey Jeffery
CWI – Amsterdam, NL
- Antoine Joux
CISPA – Saarbrücken, DE
- Stavros Kousidis
BSI – Bonn, DE
- Nils Gregor Leander
Ruhr-Universität Bochum, DE
- Frédéric Magniez
CNRS – Paris, FR
- Maria Naya-Plasencia
INRIA – Paris, FR
- Phong Q. Nguyen
INRIA & ENS Paris, FR
- Alexandru Paler
Aalto University, FI
- Galina Pass
CWI – Amsterdam, NL
- Edoardo Persichetti
Florida Atlantic University – Boca Raton, US
- Stephanie Reinhardt
BSI – Bonn, DE
- Paolo Santini
Polytechnic University of Marche, IT
- Claus Peter Schnorr
Goethe-Universität – Frankfurt am Main, DE
- André Schrottenloher
CWI – Amsterdam, NL
- Nicolas Sendrier
INRIA – Paris, FR
- Yixin Shen
Royal Holloway University of London, GB
- Jana Sotáková
University of Amsterdam, NL
- Rainer Steinwandt
University of Alabama in Huntsville, US
- Jean-Pierre Tillich
INRIA – Paris, FR

Remote Participants

- Andris Ambainis
University of Latvia – Riga, LV
- Shi Bai
Florida Atlantic University – Boca Raton, US
- Aleksandrs Belovs
University of Latvia – Riga, LV
- Daniel J. Bernstein
University of Illinois – Chicago, US
- Jintai Ding
Tsinghua University – Beijing, CN
- Philippe Gaborit
University of Limoges, FR
- András Gilyén
Alfréd Rényi Institute of Mathematics – Budapest, HU
- Maria Isabel González Vasco
King Juan Carlos University – Madrid, ES
- Akinori Hosoyamada
NTT – Tokyo, JP
- Tetsu Iwata
Nagoya University, JP
- Samuel E. Jaques
University of Oxford, GB
- Floyd Johnson
Florida Atlantic University – Boca Raton, US
- Elena Kirshanova
Immanuel Kant Baltic Federal Univ.- Kaliningrad, RU
- Péter Kutas
University of Birmingham, GB
- Tanja Lange
TU Eindhoven, NL
- François Le Gall
Nagoya University, JP
- Dustin Moody
NIST – Gaithersburg, US
- Michele Mosca
University of Waterloo, CA
- Ludovic Perret
Sorbonne University – Paris, FR
- Rachel Player
Royal Holloway University of London, GB
- Thomas Pöppelmann
Infineon Technologies AG – Neubiberg, DE
- Angela Robinson
NIST – Gaithersburg, US
- Yu Sasaki
NTT – Tokyo, JP
- John M. Schanck
Portland, US
- Daniel C. Smith-Tone
NIST – Gaithersburg, US
- Fang Song
Portland State University, US
- Adriana Suárez Corona
University of León, ES
- Dániel Szabó
University Paris Diderot, FR
- Bo-Yin Yang
Academia Sinica – Taipei, TW