

Quantum Cryptanalysis

Gorjan Alagic^{*1}, Maria Naya-Plasencia^{*2}, Rainer Steinwandt^{*3}, and Manasi Shingane^{†4}

¹ University of Maryland – College Park, US. galagic@gmail.com

² INRIA – Paris, FR. maria.naya_plasencia@inria.fr

³ University of Alabama in Huntsville, US. rs0141@uah.edu

⁴ University of Maryland – College Park, US. mshingan@umd.edu

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 23421 “Quantum Cryptanalysis”. The seminar took place as an in-person event in October 2023 and was the seventh installment of the Dagstuhl Seminar series on Quantum Cryptanalysis. This report describes the motivation and technical scope of the seminar as well as the (updated) organizational structure of this week-long event. We also include abstracts of the seminar presentations given by participants and a description of the activities of the working groups.

Seminar October 15–20, 2023 – <https://www.dagstuhl.de/23421>

2012 ACM Subject Classification Security and privacy → Cryptanalysis and other attacks

Keywords and phrases computational algebra, cryptanalysis, post-quantum cryptography, quantum algorithms, quantum resource estimation

Digital Object Identifier 10.4230/DagRep.13.10.65

1 Executive Summary

Gorjan Alagic (University of Maryland – College Park, US)

Stacey Jeffery (CWI – Amsterdam, NL)

Maria Naya-Plasencia (INRIA – Paris, FR)

Rainer Steinwandt (University of Alabama in Huntsville, US)

License  Creative Commons BY 4.0 International license

© Gorjan Alagic, Stacey Jeffery, Maria Naya-Plasencia, and Rainer Steinwandt

Motivation and technical scope

Due to the coronavirus pandemic, the previous Dagstuhl Seminar in the Quantum Cryptanalysis series (in 2021) took place in a hybrid format. With this latest installment in 2023, we returned to the standard fully in-person format at Schloss Dagstuhl and incorporated more group work. Since the 2021 meeting, the scientific community progressed significantly in developing and standardizing post-quantum cryptography for general use. In particular, the U.S. National Institute of Standards and Technology (NIST) announced that it will standardize several public-key cryptographic schemes. The study of candidates in this process has been a focus of past installments of the Quantum Cryptanalysis seminar series and this year’s Dagstuhl Seminar. The 2023 seminar was also interested in the analysis of two more scheme categories. The first category consists of additional public-key schemes that either have different performance profiles, or different security properties (e.g., are based on the hardness of other mathematical problems) than the NIST-selected schemes. The second

* Editor / Organizer

† Editorial Assistant / Collector



Except where otherwise noted, content of this report is licensed under a Creative Commons BY 4.0 International license

Quantum Cryptanalysis, *Dagstuhl Reports*, Vol. 13, Issue 10, pp. 65–75

Editors: Gorjan Alagic, Maria Naya-Plasencia, and Rainer Steinwandt



Dagstuhl Reports

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

category consists of symmetric-key schemes; while post-quantum standardization has not as yet focused on symmetric-key cryptography, there are many open questions about their security in the presence of quantum adversaries.

As one would expect from the title of the seminar, studying the best-known algorithmic attacks on cryptographic schemes was a focus of the conversations. Understanding the best-known attacks enables cryptographers to select the strongest schemes and set their parameters in a manner that appropriately balances security with performance. Technical talks included work on quantum-computational algorithms for attacking three categories of public-key schemes: lattice-based, code-based, and isogeny-based. We also had two presentations on new ideas for attacking symmetric-key cryptography using quantum computers. In addition, the technical program included an update from NIST on the progress of their various standardization processes related to the seminar scope.

As in the past, the seminar brought together researchers in several relevant fields, including quantum-computational algorithms, classical public-key and symmetric-key cryptography, and the mathematics of lattices and codes. This enabled the participants to get an overview of the latest advances in all of these fields.

Organization

To leverage some of the unique opportunities Schloss Dagstuhl offers, as in the past, we left ample time for discussions and collaboration; the typical day called for between two and three presentations total. The remaining time was more structured than in past instances of the seminar. Before the seminar began, the organizers contacted the participants to solicit topics and started to organize working groups. The first day of the seminar was then mainly focused on establishing the working groups and the technical topics they would focus on. The working groups met throughout the week to discuss their technical subjects and regularly reported their progress to the entire seminar. The participant-selected working group topics were:

- quantum algorithms for the lattice isomorphism problem (a new problem with potential for post-quantum applications),
- Regev’s quantum factoring algorithm (a new algorithm that may affect how soon current cryptography will become obsolete),
- cryptanalysis of LR5 (a fundamental building block in symmetric-key cryptography), and
- code-based cryptosystems (these are next on the slate of possible standardized schemes).

Following the Dagstuhl tradition and in line with prior seminars in the Quantum Cryptanalysis series, there was no technical program during Wednesday afternoon. This enabled participants to explore the surroundings or spend more time on collaborative research.

With 34 participants, Schloss Dagstuhl hosted a diverse group of leading experts from across the globe. A significant number of the participants were graduate students. These young researchers were able to interact with leading experts in working on the latest science and gain valuable insights to help them developing their career.

Results and next steps

The working groups were a welcome addition this year, with several participants praising this style of seminar structure. The working groups were able to make technical progress during the week and several groups continued collaborating after the seminar.

The various technical presentations showed that significant progress is being made in the field more generally. This indicates that the intersection of quantum computing and classical cryptography is a vibrant and active field. The Dagstuhl Seminar series on Quantum Cryptanalysis plays an important role in this area of science. We expect this will continue, as the community carries on with the process of standardizing and deploying post-quantum cryptography in the real world. This process is already generating challenging scientific questions that the seminar could help address. For instance, the only general-purpose schemes currently slated for standardization are based on lattice problems; how can the community select high-performing replacement schemes that can serve as a backup in case lattices fail?

2 Table of Contents

Executive Summary

Gorjan Alagic, Stacey Jeffery, Maria Naya-Plasencia, and Rainer Steinwandt . . . 65

Overview of Talks

NIST PQC process update

Gorjan Alagic and Daniel C. Smith-Tone 69

Single-query Quantum Hidden Shift Attacks

Xavier Bonnetain 69

Quantum algorithms for isogeny-based cryptography

Péter Kutas 70

Quantum Linear Key-recovery Attacks Using the QFT

André Schrottenloher 70

Quantum algorithms for lattice problems

Yixin Shen 70

Quantum decoding problem

Jean-Pierre Tillich 71

Working groups

Quantum algorithms for Lattice Isomorphism Problem

Jean-François Biasse 71

Regev’s quantum factoring algorithm

Martin Ekerå 72

Cryptanalysis of LR5

Christian Majenz 73

Code-based group

Jean-Pierre Tillich 73

Participants 75

3 Overview of Talks

3.1 NIST PQC process update

Gorjan Alagic (University of Maryland – College Park, US) and Daniel C. Smith-Tone (NIST – Gaithersburg, US)

License  Creative Commons BY 4.0 International license
© Gorjan Alagic and Daniel C. Smith-Tone

Since 2016, the U.S. National Institute of Standards and Technology has been running a standardization process for post-quantum public-key cryptography. So far, this process has produced one standard for a key encapsulation mechanism (Kyber / ML-KEM) and three standards for digital signature schemes (Dilithium / ML-DSA, Falcon / FN-DSA, and SPHINCS+ / SLH-DSA). Three of these standards are currently drafts open for public comment. At the same time, NIST is continuing to look at post-quantum KEMs, and has begun an additional process for standardizing more signature schemes. This talk will give an overview of this process and what the future might hold.

3.2 Single-query Quantum Hidden Shift Attacks

Xavier Bonnetain (LORIA & INRIA Nancy, FR)

License  Creative Commons BY 4.0 International license
© Xavier Bonnetain

Quantum attacks using superposition queries are known to break many classically secure modes of operation. While these attacks do not necessarily threaten the security of the modes themselves, since they rely on a strong adversary model, they help us to draw limits on the provable security of these modes.

Typically these attacks use the structure of the mode (stream cipher, MAC or authenticated encryption scheme) to embed a period-finding problem, which can be solved with a dedicated quantum algorithm. The hidden period can be recovered with a few superposition queries (e.g., $O(n)$ for Simon's algorithm), leading to state or key-recovery attacks. However, this strategy breaks down if the period changes at each query, e.g., if it depends on a nonce.

In this talk, we focus on this case and give dedicated state-recovery attacks on the authenticated encryption schemes Rocca, Rocca-S, Tiaoxin-346 and AEGIS-128L. These attacks rely on a procedure to find a Boolean hidden shift with a single superposition query, which overcomes the change of nonce at each query. As they crucially depend on such queries, we stress that they do not break any security claim of the authors, and do not threaten the schemes if the adversary only makes classical queries.

3.3 Quantum algorithms for isogeny-based cryptography

Péter Kutas (University of Birmingham, GB)

License  Creative Commons BY 4.0 International license
© Péter Kutas

In the talk we surveyed quantum algorithms relevant to isogeny-based cryptography. One aspect of isogenies is that one can instantiate cryptographic group actions with them that still retain certain properties of discrete logarithms but are not susceptible to attacks via Shor’s algorithm. We discussed certain reductions between hard problems related to group actions most importantly the quantum equivalence of inverting the group action and the computational Diffie-Hellman problem (and that such an equivalence is highly unlikely in the classical setting as it would mean that the discrete logarithm and factoring assumptions do not hold). We also discussed recent quantum attacks on pSIDH utilizing a non-abelian hidden subgroup problem and improved quantum algorithms for finding fixed degree isogenies.

3.4 Quantum Linear Key-recovery Attacks Using the QFT

André Schrottenloher (INRIA – Rennes, FR)

License  Creative Commons BY 4.0 International license
© André Schrottenloher
Main reference André Schrottenloher: “Quantum Linear Key-recovery Attacks Using the QFT”, 2023.
URL <https://eprint.iacr.org/2023/184>

The Quantum Fourier Transform is a fundamental tool in quantum cryptanalysis. In symmetric cryptanalysis, hidden shift algorithms such as Simon’s (FOCS 1994), which rely on the QFT, have been used to obtain structural attacks on some very specific block ciphers. The Fourier Transform is also used in classical cryptanalysis, for example in FFT-based linear key-recovery attacks introduced by Collard et al. (ICISC 2007). Whether such techniques can be adapted to the quantum setting has remained so far an open question.

In this paper, we introduce a new framework for quantum linear key-recovery attacks using the QFT. These attacks loosely follow the classical method of Collard et al., in that they rely on the fast computation of a “correlation state” in which experimental correlations, rather than being directly accessible, are encoded in the amplitudes of a quantum state. The experimental correlation is a statistic that is expected to be higher for the good key, and on some conditions, the increased amplitude creates a speedup with respect to an exhaustive search of the key. The same method also yields a new family of structural attacks, and new examples of quantum speedups beyond quadratic using classical known-plaintext queries.

3.5 Quantum algorithms for lattice problems

Yixin Shen (King’s College London, GB)

License  Creative Commons BY 4.0 International license
© Yixin Shen

In this talk, I survey some algorithmic problems that arise from the cryptanalysis of lattice-based cryptographic schemes such as the Shortest Vector problem and the Learning with Errors problem. Then I particularly focus on how quantum algorithms can help us obtain speed-ups on different approaches to solve those problems.

3.6 Quantum decoding problem

Jean-Pierre Tillich (INRIA – Paris, FR)

License © Creative Commons BY 4.0 International license
© Jean-Pierre Tillich

One of the founding results of lattice based cryptography is a quantum reduction from the Short Integer Solution problem to the Learning with Errors problem introduced by Regev. It has recently been pointed out by Chen, Liu and Zhandry that this reduction can be made more powerful by replacing the learning with errors problem with a quantum equivalent, where the errors are given in quantum superposition. In the context of codes, this can be adapted to a reduction from finding short codewords to a quantum decoding problem for random linear codes.

We therefore consider in this paper the quantum decoding problem, where we are given a superposition of noisy versions of a codeword and we want to recover the corresponding codeword. When we measure the superposition, we get back the usual classical decoding problem for which the best known algorithms are in the constant rate and error-rate regime exponential in the codelength. However, we will show here that when the noise rate is small enough, then the quantum decoding problem can be solved in quantum polynomial time. Moreover, we also show that the problem can in principle be solved quantumly (albeit not efficiently) for noise rates for which the associated classical decoding problem cannot be solved at all for information theoretic reasons.

We then revisit Regev’s reduction in the context of codes. We show that using our algorithms for the quantum decoding problem in Regev’s reduction matches best known quantum algorithms for the short codeword problem. This shows in some sense the tightness of Regev’s reduction when considering the quantum decoding problem and also paves the way for new quantum algorithms for the short codeword problem.

4 Working groups

4.1 Quantum algorithms for Lattice Isomorphism Problem

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

License © Creative Commons BY 4.0 International license
© Jean-François Biasse

The lattice isomorphism problem (LIP) consists in finding a secret isometry between two input Euclidean lattices. LIP is a fundamental problem that has been studied for decades. Recently, Ducas and van Woerden proposed cryptosystems whose security rely on the presumed hardness of LIP. The known algorithms for the resolution of LIP rely on the calculation of short vectors in the input lattices. The shortest vector problem is a notoriously hard problem, even for quantum computers. This suggests that cryptosystems based on LIP might feature quantum resistance.

No quantum algorithms for the resolution of LIP have ever been described in the literature. The best classical algorithms for computing an isomorphism between two given lattices run in time n^n (or $2^{n/2}$ if one of the input lattices is $\mathbb{Z}^n$). Finding a quantum algorithm with a better complexity than the existing classical algorithms for the resolution of LIP is an open problem.

Our group investigated quantum algorithms for the resolution of LIP. Several avenues were considered:

- We rephrased LIP as a hidden shift problem, which is a task that can (in certain cases) be solved efficiently by quantum computers.
- We reviewed the generation of instances of the LIP that are used for the creation of cryptographic keys. We studied conditions on the parameters that can make the LIP-based cryptosystems insecure.
- We studied quantum analogues of the existing classical algorithms for the resolution of LIP.
- We researched quantum algorithms to compute short vectors in lattices that are rotations of $\mathbb{Z}^n$, which is a task for which there exist ad-hoc classical solutions that outperform generic methods.

4.2 Regev’s quantum factoring algorithm

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

License  Creative Commons BY 4.0 International license
© Martin Ekerå

The work in our breakout group focused on Regev’s recent d-dimensional variation [1] of Shor’s quantum factoring algorithm ([2], [3]), and on better understanding its advantages and disadvantages in practical implementations.

Of particular interest to our group was the very recent Fibonacci-based arithmetic [4] that seemingly resolves reversibility issues previously identified by Ekerå and Gidney in Regev’s binary tree-based arithmetic.

There were presentations of ongoing work, including work [5] on extending Regev’s algorithm to computing discrete logarithms, and work ([6], [7]) on simulating the quantum parts of the algorithms for integers of known factorization and for groups where computing discrete logarithms is classically easy.

The aforementioned simulators enable the heuristic assumptions in Regev’s analysis to be verified. Furthermore, they enable the robustness of the classical post-processing to erroneous runs to be analyzed – where an erroneous run is a run in which the error correction fails to properly correct all errors, leading to a bad vector being output. There was discussion in the group regarding options for filtering out good vectors from bad vectors.

For the extension to discrete logarithms to be efficient, it is required that the group has a notion of small elements, that when composed yield elements that are also small, and where the composition of small elements is considerably less expensive than the composition of arbitrary group elements. A notion of small elements exists for $\mathbb{Z}_p^*$. There was discussion in the group regarding whether a similar notion exists for elliptic curve groups.

References

- 1 Regev, O. An efficient quantum factoring algorithm. *ArXiv Preprint ArXiv:2308.06572*. (2023)
- 2 Shor, P. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium On Foundations Of Computer Science*. pp. 124-134 (1994)
- 3 Shor, P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*. **41**, 303-332 (1999)

- 4 Ragavan, S. & Vaikuntanathan, V. Optimizing Space in Regev’s Factoring Algorithm. *ArXiv Preprint ArXiv:2310.00899*. (2023)
- 5 Ekerå, M. & Gärtner, J. Extending Regev’s factoring algorithm to compute discrete logarithms. *ArXiv Preprint ArXiv:2311.05545*. (2023)
- 6 M. Ekerå and J. Gärtner: “Simulating Regev’s quantum factoring algorithm”. GitHub repository ekerå/regevnum. (2023) URL: <https://github.com/ekera/regevnum>
- 7 M. Ekerå and J. Gärtner: “Simulating our extension of Regev’s quantum factoring algorithm to compute discrete logarithms”. Unpublished GitHub repository. (2023)

4.3 Cryptanalysis of LR5

Christian Majenz (Technical University of Denmark – Lyngby, DK)

License © Creative Commons BY 4.0 International license
© Christian Majenz

The Feistel network is a versatile blueprint for constructing pseudorandom permutations (PRPs) and block ciphers. The simplest application is a family of constructions of a PRP from a pseudorandom function, indexed by the number of rounds. There is an extensive body of quantum attacks on the construction in the Q2 model, where an attacker has quantum query access to the PRP. For the five round variant, also known as LR5 (“Luby-Rackoff 5”), there is no quantum attack known separating its chosen-plaintext (CPA) security from its chosen-ciphertext (CCA) security (or its PRP security from its strong PRP security). In this working group, we explored a number of approaches of leveraging an existing polynomial-time on the four-round variant based on Simon’s algorithm to devise a CCA attack on five rounds that improves over the existing CPA attack.

4.4 Code-based group

Jean-Pierre Tillich (INRIA – Paris, FR)

License © Creative Commons BY 4.0 International license
© Jean-Pierre Tillich

In this working group we

1. first provided an introduction to the decoding problem suitable for a broad audience;
2. then we looked in detail at a recent (classical) algorithm for performing this task consisting in applying sieving techniques which are common in lattice based cryptography but not in code based cryptography. See [1]. A nice feature of this algorithm is that it uses relatively low memory and its running time is rather competitive when compared to the best decoding algorithms. This makes it a very good candidate for quantization.
3. In the last part of the working group, we went through one of the best quantum algorithm for performing lattice sieving based on random walks and suitable product codes for the unit sphere, see [2].

We concluded that these techniques should carry over for performing quantumly the sieving task relevant for decoding and discussed some technical points which can be found in Kevin Carrier’s thesis [3].

All in all this should lead to a new quantum algorithm for decoding a linear code which could be a record breaker in terms of complexity.

References

- 1 Ducas, L., Esser, A., Etinski, S. & Kirshanova, E. Asymptotics and Improvements of Sieving for Codes. *Cryptology EPrint Archive*. (2023)
- 2 Chailloux, A. & Loyer, J. Lattice sieving via quantum random walks. *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 27*. pp. 63-91 (2021)
- 3 Carrier, K. Recherche de presque-collisions pour le décodage et la reconnaissance de codes correcteurs. (Sorbonne université,2020)

Participants

- Gorjan Alagic
University of Maryland –
College Park, US
- Kaveh Bashiri
BSI – Bonn, DE
- Jean-François Biasse
University of South Florida –
Tampa, US
- Xavier Bonnetain
LORIA & INRIA Nancy, FR
- Yanlin Chen
CWI – Amsterdam, NL
- Arjan Cornelissen
IRIF – Paris, FR
- Martin Ekerå
KTH Royal Institute of
Technology – Stockholm, SE
- Lynn Engelberts
CWI – Amsterdam, NL &
QuSoft – Amsterdam, NL
- Simona Etinski
CWI – Amsterdam, NL
- Paul Frixons
INRIA Nancy – Grand Est, FR
- Vlad Gheorghiu
University of Waterloo, CA &
softwareQ Inc. – Waterloo, CA
- Sean Hallgren
Pennsylvania State University –
University Park, US
- Jacek Horecki
BEIT – Kraków, PL
- Akinori Hosoyamada
NTT – Tokyo, JP
- Péter Kutas
University of Birmingham, GB
- Johanna Loyer
INRIA – Paris, FR
- Frédéric Magniez
CNRS – Paris, FR
- Christian Majenz
Technical University of Denmark
– Lyngby, DK
- Alexander May
Ruhr-Universität Bochum, DE
- Garazi Muguruza
QuSoft & University of
Amsterdam, NL
- Maria Naya-Plasencia
INRIA – Paris, FR
- Lorenz Panny
TU München – Garching, DE
- Galina Pass
QuSoft – Amsterdam, NL
- Yu Sasaki
NTT – Tokyo, JP
- André Schrottenloher
INRIA – Rennes, FR
- Yixin Shen
King's College London, GB
- Manasi Shingane
University of Maryland –
College Park, US
- Daniel C. Smith-Tone
NIST – Gaithersburg, US
- Jana Sotáková
University of Amsterdam, NL
- Rainer Steinwandt
University of Alabama in
Huntsville, US
- Jean-Pierre Tillich
INRIA – Paris, FR
- Maya-Iggy van Hoof
Ruhr-Universität Bochum, DE
- Michael Walter
Ruhr-Universität Bochum, DE
- Sara Zafar Jafarzadeh
University of Waterloo, CA &
Synopsis Inc. – Ottawa, CA