Report from Dagstuhl Seminar 19421

Quantum Cryptanalysis

Edited by

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

1 **University of Waterloo, CA,** michele.mosca@uwaterloo.ca
2 **INRIA – Paris, FR,** maria.naya_plasencia@inria.fr
3 **Florida Atlantic University – Boca Raton, US,** rsteinwa@fau.edu

Abstract

This seminar report documents the program and the outcomes of Dagstuhl Seminar 19421 *Quantum Cryptanalysis*, which took place in October 2019. After outlining the motivation and organizational aspects of this particular seminar, abstracts of presentations that were given by participants are provided.

Seminar October 13–18, 2019 – http://www.dagstuhl.de/19421
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 circuit complexity, quantum computing, standardization
Digital Object Identifier 10.4230/DagRep.9.10.47
Edited in cooperation with Shaun Miller

1 Executive Summary

Michele Mosca
María Naya-Plasencia
Rainer Steinwandt

Motivation and scope

This fifth installment of a Dagstuhl seminar on *Quantum Cryptanalysis* was heavily informed by NIST's ongoing standardization effort in post-quantum cryptography. Several NIST employees attended the seminar and lead a discussion session on the topic. As one would hope hoped for, many talks had an algorithmic focus. Two areas were of particular interest for this seminar:

Quantum cryptanalytic progress. Identifying new cryptanalytic improvements that make use of quantum algorithms and expanding the applicability of the best known cryptanalytic attacks by means of quantum technology. Different quantum attack models can be considered here, and attack models that are close to being realizable with today's technology are particularly relevant. We want to fully leverage quantum computing, including expected mid-term advancements.

Quantum resource estimation. Establishing reasonably precise quantum resource counts for cryptanalytic attacks against symmetric and asymmetric schemes, especially for problem instances and parameter choices that are actually deployed or considered for

standardization for future deployment. In addition to logical resources, understanding the overhead caused by handling imperfections of quantum hardware is of interest.

In addition to original quantum cryptanalytic research, the program included presentations with a strong survey component, explaining key concepts of particular areas within post-quantum cryptography. Deviating from prior editions, this time we did not include a presentation to document the status of the development of quantum hardware. Such a talk could have been a welcome addition, but the seminar program was already packed with a substantial number of relevant cryptanalytic results, and it was important to leave sufficient time for discussions.

Organization

Following the organization of the prior quantum cryptanalysis seminars in Dagstuhl, for this fifth edition, again experts from academia, government, and industry came together. We re-invited a number of leading experts in the field from the prior quantum cryptanalysis seminar edition, and at the same time invited several new participants. This included in particular young scientists, who entered this exciting research area more recently. In total, we had with 46 participants a slightly larger number of participants than in the preceding meeting. In line with the Dagstuhl tradition and with prior quantum cryptanalysis seminars, for Wednesday afternoon we left the schedule open. Seminar participants could devote the afternoon to an excursion, to discussions, or to work on their research.

Results and next steps

At this point, communication and collaboration between the classical cryptographic and the quantum algorithmic research communities has become very fruitful, and it seems fair to say that this seminar is also of significant value in supporting ongoing standardization efforts in post-quantum cryptography. In addition to quantum cryptanalytic results on asymmetric cryptography, more results on symmetric cryptography are emerging. There is still substantial research potential – and research need – in quantifying security margins in the presence of quantum computing, and the field keeps moving fast. Improved software tools become available to analyze quantum resources and describe quantum algorithms, bringing research in quantum cryptanalysis closer together with areas in traditional computer science.

2 Table of Contents

3 Overview of Talks

3.1 Challenges in evaluating costs of known lattice attacks

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

This talk is a survey of open questions regarding the performance of algorithms in the literature to attack lattice-based cryptosystems.

3.2 On quantum algorithms for isogenies

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

In this presentation, we introduce two general frameworks to compute isogenies between elliptic curves using a quantum computer. First, in the more general case, we rely on the quantum search algorithm of Grover. We present recent results showing how to optimize this strategy by classically precomputing short isogeny paths and incorporating this information in the quantum circuit performing the Grover search. Second, we use a subexponential quantum algorithm which is applicable when the endomorphism ring of the elliptic curves involved in the instance of the problem is isomorphic to an imaginary quadratic order. This algorithm relies on the Sieve of Kuperberg which solves the Dihedral Coset Problem. We insist on a recent result showing that we can trade off quantum effort for classical one. This work in progress suggests that there might be hybrid classical/quantum attacks whose circuit size fit under both classical and quantum circuit size limits described by NIST in their standardization process.

3.3 Modeling the Runtime of Cryptanalytic Algorithms

Christian Bischof (TU Darmstadt, DE)

Joint work of Christian Bischof, Michael Burger, Giam Nam Ngyuen

To assess the hardness of lattice-based cryptography, we need to assess the time requitred to solve the shortest vector problem (SVP). Sieving algorithms exhibit exponential complexity in time and space, so actual computational experiments are inherently bounded as to what lattice dimensions can be solved. To extrapolate to larger lattices, we extended the extra-P modeling framework in joint work with Felix' Wolf Group at TU Darmstadt for exponential modeling. In addition to good predictions, it also enables us to investigate tradeoffs with respect to algorithmic parameter selection in sieving algorithms.

3.4 The offline Simon's algorithm

Xavier Bonnetain (INRIA – Paris, FR)

Joint work of Xavier Bonnetain, Akinori Hosoyamada, María Naya-Plasencia, Yu Sasaki, André Schrottenloher

In symmetric cryptanalysis, the model of superposition queries has lead to surprising results, with many constructions being broken in polynomial time thanks to Simon's period-finding algorithm. But the practical implications of these attacks remain blurry. In contrast, the results obtained so far for a quantum adversary making classical queries only are less impressive.

In this paper, we introduce a new quantum algorithm which uses Simon's subroutines in a novel way. We manage to leverage the algebraic structure of cryptosystems in the context of a quantum attacker limited to classical queries and offline quantum computations. We obtain improved quantum-time/classical-data tradeoffs with respect to the current literature, while using only as much hardware requirements (quantum and classical) as a standard exhaustive search using Grover's algorithm. In particular, we are able to break the Even-Mansour construction in quantum time $O(2^{n/3})$, with $O(2^{n/3})$ classical queries and $O(n^2)$ qubits only. In addition, we propose an algorithm that allows to improve some previous superposition attacks by reducing the data complexity from exponential to polynomial, with the same time complexity.

Our approach can be seen in two complementary ways: reusing superposition queries during the iteration of a search using Grover's algorithm, or alternatively, removing the memory requirement in some quantum attacks based on a collision search, thanks to their algebraic structure.

We provide a list of cryptographic applications, including the Even-Mansour construction, the FX construction, some Sponge authenticated modes of encryption, and many more.

3.5 On quantum versions of the Strong Exponential Time Hypothesis

Harry Buhrman (CWI – Amsterdam, NL)

Joint work of Harry Buhrman, Subhasree Patro, and Florian Speelman
Main reference Harry Buhrman, Subhasree Patro, Florian Speelman: "The Quantum Strong Exponential-Time Hypothesis", CoRR, Vol. abs/1911.05686, 2019.
URL https://arxiv.org/abs/1911.05686

The strong exponential-time hypothesis (SETH) is a commonly used conjecture in the field of complexity theory. It states that CNF formulas cannot be analyzed for satisfiability with a speedup over exhaustive search. This hypothesis and its variants gave rise to a fruitful field of research, fine-grained complexity, obtaining (mostly tight) lower bounds for many problems in P whose unconditional lower bounds are hard to find. In this work, we introduce a framework of Quantum Strong Exponential-Time Hypotheses, as quantum analogues to SETH.

Using the QSETH framework, we are able to translate quantum query lower bounds on black-box problems to conditional quantum time lower bounds for many problems in BQP. As an example, we illustrate the use of the QSETH by providing a conditional quantum time lower bound of $\Omega(n^{1.5})$ for the Edit Distance problem. We also show that the n^2 SETH-based lower bound for a recent scheme for Proofs of Useful Work, based on the Orthogonal Vectors problem, also holds for quantum computation assuming QSETH.

3.6 On factoring RSA integers and computing discrete logarithms on quantum computers

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

In this talk, we give an overview of the state of factoring integers and computing discrete logarithms on quantum computers, focusing on algorithms that have been demonstrated to be polynomial time. More specifically, we treat Shor's algorithms for the IFP, OFP and DLP, Seifert's algorithm for the IFP and OFP with tradeoffs, and our algorithms for the short DLP, DLP and RSA IFP, with or without tradeoffs.

We quantify the costs reductions we obtain, both in the logical circuit model, and in a full stack implementation modelled upon existing superconducting quantum computing architectures. The full stack cost estimates are a joint work with Craig Gidney.

We provide tight analyses of the success probabilities in the aforementioned algorithms, classical simulators for the algorithms, and efficient lattice-based post-processing. We show that our algorithms outperform Shor's and Seifert's algorithms for the short DLP and the RSA IFP.

3.7 Recent results onrank-based cryptography

Philippe Gaborit (University of Limoges, FR)

Rank-based cryptography was introduced by Gabidulin et al. in 1991, since then many systems have been proposed. Rank-based cryptography has the inherent good property that the complexity of best known attacks increases faster than for Hamming metric for a given size of key.In this talk we will review recent results on rank-based cryptography, in particular recent submissions to NIST, based on problems with no masking. We will consider the Ouroboros approach and some advanced encryption schemes.

3.8 Some new distributional property testing results

András Gilyén (Caltech – Pasadena, US)

A fundamental problem in statistics and learning theory is to test properties of distributions. We show that quantum computers offer speed-ups for such problems. We describe a natural query input model, that serves as the quantum analog of classical sampling. Then we describe a generic approach that leads to speed-ups for estimating the entropy of distributions, testing equality of two unknown distributions and other problems. Our approach is based on the results of Bravyi, Harrow, and Hassidim (2009), combined with the recent technique of Quantum Singular Value Transformation. The utilized general techniques also allow us to derive similar speed-ups for testing quantum distributions (i.e., density operators). We also

show that the quantum speed-ups are at most cubic for classical distributions, as implied by a recent result of Chailloux (2018). Finally, we mention a new result of van Apeldoorn and Montanaro for quadratically speeding-up the estimation of an entire distribution using the quantum Fourier transform.

3.9 Finding Hash Collisions with Quantum Computers by Using Differential Trials with Smaller Probability than Birthday Bound

Akinori Hosoyamada (NTT – Tokyo, JP)

Joint work of Akinori Hosoyamada, Yu Sasaki

We give dedicated quantum attacks on concrete hash functions that exploit their internal structures, which has not received much attention so far. We show collision attacks on 7-round AES-MMO and 6-round Whirlpool, which are not broken (from the view point of collision-resistance) in the classical setting.

3.10 Using isogenies for post-quantum cryptography

David Jao (University of Waterloo, CA)

We give a survey of isogeny-based cryptography and related quantum cryptanalytic techniques.

3.11 Improved quantum circuits for modular arithmetic and elliptic curve discrete log

Samuel E. Jaques (University of Oxford, GB)

Joint work of Samuel E. Jaques, Thomas Naehrig, Michael Häner, Martin Roetteler, Mathias Soeken

Shor's algorithm will break elliptic curve cryptography, but it will require a large quantum computer. How large, exactly? Previous work attempting to quantify the cost has mostly tried to minimize the number of logical qubits; however, error correction overhead could mean that a circuit with fewer gates but more logical qubits would require fewer physical qubits. Thus, we revisit the previous circuits, improve on them, and explore costs besides the minimum qubit count. Our main improvements come from measurement-based "AND" gates, alternative addition circuits, and more efficient pebbling. Our most dramatic result is a circuit depth nearly 10,000 times shorter with only 22% more qubits.

3.12 The Fermat-FHE system

Antoine Joux (Sorbonne University – Paris, FR)

In this talk, we recast state-of-the-art constructions for fully homomorphic encryption in the simple language of arithmetic modulo large Fermat numbers. The techniques used to construct our scheme are quite standard in the realm of (R)LWE based cryptosystems. However, the use of arithmetic in such a simple ring allows to present scheme from elementary mathematical concepts and to implement it easily based on a large number library.

In terms of performance, our test implementation of the proposed scheme is slower than the current speed records but remains within a comparable range. We hope that the detailed study of our Fermat-based scheme by the community can make it even more competitive and provide new insights into FHE constructions at large.

3.13 Quantum speed-ups for sieving algorithms

Elena Kirshanova (Immanuel Kant Baltic Federal University – Kaliningrad, RU)

Joint work of Elena Kirshanova, Erik Mårtensson, Eamonn W. Postlethwaite, Subhayan Roy Moulik
Main reference Elena Kirshanova, Erik Mårtensson, Eamonn W. Postlethwaite, Subhayan Roy Moulik: "Quantum Algorithms for the Approximate k-List Problem and their Application to Lattice Sieving", IACR Cryptology ePrint Archive, Vol. 2019, p. 1016, 2019.
URL https://eprint.iacr.org/2019/1016

The Shortest Vector Problem (SVP) is one of the mathematical foundations of lattice based cryptography. Lattice sieve algorithms are amongst the foremost methods of solving SVP. The asymptotically fastest known classical and quantum sieves solve SVP in a d-dimensional lattice in $2^{cd+o(d)}$ time steps with $2^{c'd+o(d)}$ memory for constants c, c'. In this work, we give various quantum sieving algorithms that trade computational steps for memory.

We first give a quantum analogue of the classical k-Sieve algorithm [Herold–Kirshanova–Laarhoven, PKC'18] in the Quantum Random Access Memory (QRAM) model, achieving an algorithm that heuristically solves SVP in $2^{0.2989d+o(d)}$ time steps using $2^{0.1395d+o(d)}$ memory. This should be compared to the state-of-the-art algorithm [Laarhoven, Ph.D Thesis, 2015] which, in the same model, solves SVP in $2^{0.2653d+o(d)}$ time steps and memory. In the QRAM model these algorithms can be implemented using $poly(d)$ width quantum circuits.

Secondly, we frame the k-Sieve as the problem of k-clique listing in a graph and apply quantum k-clique finding techniques to the k-Sieve.

Finally, we explore the large quantum memory regime by adapting parallel quantum search [Beals et al., Proc. Roy. Soc. A'13] to the 2-Sieve and giving an analysis in the quantum circuit model. We show how to heuristically solve SVP in 20.1037d+o(d) time steps using 20.2075d+o(d) quantum memory.

Category / Keywords: foundations / approximate k-list problem, cryptanalysis, distributed computation, grover's algorithm, lattice sieving, nearest neighbour algorithms, quantum cryptography, shortest vector problem, SVP

3.14 Quantum circuits for the CSIDH: optimizing quantum evaluation of isogenies

Tanja Lange (TU Eindhoven, NL)

URL https://quantum.isogeny.org/

Choosing safe post-quantum parameters for the new CSIDH isogeny-based key-exchange system requires concrete analysis of the cost of quantum attacks. The two main contributions to attack cost are the number of queries in hidden-shift algorithms and the cost of each query. This paper analyzes algorithms for each query, introducing several new speedups while showing that some previous claims were too optimistic for the attacker. This paper includes a full computer-verified simulation of its main algorithm down to the bit-operation level.

3.15 Quantum Period Finding with a Single Output Qubit-Factoring n-bit RSA with $n/2$ Qubits?

Alexander May (Ruhr-Universität Bochum, DE)

Joint work of Alexander May, Lars Schlieper
Main reference Alexander May, Lars Schlieper: "Quantum Period Finding with a Single Output Qubit – Factoring n-bit RSA with n/2 Qubits", CoRR, Vol. abs/1905.10074, 2019.
URL https://arxiv.org/abs/1905.10074

We study quantum period finding algorithms such as Simon and Shor (and its variants Ekerå-Håstad and Mosca-Ekert). For a periodic function f these algorithms produce – via some quantum embedding of f – a quantum superposition $\sum_x |x\rangle|f(x)\rangle$, which requires a certain amount of output qubits that represent $|f(x)\rangle$. We show that one can lower this amount to a single output qubit by hashing f down to a single bit in an oracle setting. Namely, we replace the embedding of f in quantum period finding circuits by oracle access to several embeddings of hashed versions of f. We show that on expectation this modification only doubles the required amount of quantum measurements, while significantly reducing the total number of qubits. For example, for Simon's period finding algorithm in some n-bit function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ our hashing technique reduces the required output qubits from n down to 1, and therefore the total amount of qubits from $2n$ to $n + 1$. We also show that Simon's algorithm admits real world applications with only $n + 1$ qubits by giving a concrete realization of a hashed version of the cryptographic Even-Mansour construction. Our oracle-based hashed version of the Ekerå-Håstad algorithm for factoring n-bit RSA reduces the required qubits from $(32 + o(1))n$ down to $(12 + o(1))n$. In principle our hashing approach also works for the Mosca-Ekert algorithm, but requires strong properties of the hash function family. A hashed version of Mosca-Ekert with as few as $O(\log n)$ qubits would imply classical polynomial time factoring. Therefore, the search for suitable hash functions might open a new path to factoring in $\mathcal{P}$.

3.16 Faster provable sieving algoriths for SVP and CVP in ℓ_p norm

Priyanka Mukhopadhyay (University of Waterloo, CA)

We give an overview some old and new provable sieving algorithms for SVP and CVP in l_p norm.

3.17 An attack on LEDAcrypt

Ray Perlner (NIST – Gaithersburg, US) and Daniel C. Apon (NIST – Gaithersburg, US)

We present an attack on LEDAcrypt that modifies standard information set decoding to take advantage of the product structure of the private key. By carefully choosing the information set decoding we can explore a much larger fraction of the key space with each iteration. As a result, for all parameters sets there are large classes of weak keys that can be broken faster than expected based on previous analysis and claimed security (e.g. for category 5, $n_0 = 2$, where the attack is most powerful, 1 in 2 to the 45 keys can be broken by an attack costing the equivalent of 2 to the 52 AES operations, and for category 1, $n_0 = 4$, where the attack is least powerful, 1 in about 2 to the 40 keys can be broken by an attack costing the equivalent of 2 to the 50 AES operations.) For some parameter sets (category 5, $n_0 = 2$) the attack most likely also reduces security for the entire key space, although more rigorous analysis is needed to quantify this effect.

3.18 On the condition number of Macaulay matrices

Rachel Player (Royal Holloway University of London, GB),

Joint work of Rachel Player, Jean-Charles Faugère, and Ludovic Perret
Main reference J. C. Faugère, L. Perret, R. Player. On the condition number of Macaulay matrices. In preparation, 2019.

We present a work-in-progress and preliminary results with a view to promote discussion and push forward the work. This work is motivated by the potential impact for cryptanalysis of Chen and Gao's recent quantum algorithm [CG18] for solving Boolean systems of multivariate equations. The complexity of this algorithm depends on the condition number of a certain Macaulay matrix arising from the input Boolean system. The goal of this work is to provide experimental data to determine the size of the condition number in situations of cryptanalytic interest. We also provide a theoretical upper bound on the condition number of a Macaulay matrix that applies in certain cases.

3.19 Quantum speedups for lattice sieves are tenuous at best

John M. Schanck (University of Waterloo, CA)

Joint work of Martin R. Albrecht , Vlad Gheorghiu , Eamonn W. Postlethwaite , John M. Schanck
URL https://materials.dagstuhl.de/files/19/19421/19421.JohnM.Schanck.Preprint.pdf

Quantum variants of lattice sieve algorithms are often used to assess the security of lattice based cryptographic constructions. In this work we provide a heuristic, non-asymptotic, analysis of the cost of several algorithms for near neighbour search on high dimensional spheres. These algorithms are used in lattice sieves. We design quantum circuits for near neighbour algorithms and provide software that numerically optimises algorithm parameters according to various cost metrics. Using this software we estimate the cost of classical and quantum near neighbour search on spheres. We find that quantum search may provide a small speedup in dimensions of cryptanalytic interest, but only under exceedingly optimistic physical and algorithmic assumptions.

3.20 Quantum Merging Algorithms

André Schrottenloher (INRIA – Paris, FR)

Joint work of Maria Naya-Plasencia, Andre Schrottenloher
Main reference María Naya-Plasencia, André Schrottenloher: "Optimal Merging in Quantum k-xor and k-sum Algorithms", IACR Cryptology ePrint Archive, Vol. 2019, p. 501, 2019.
URL https://eprint.iacr.org/2019/501

The k-xor or Generalized Birthday Problem aims at finding, given k lists of bit-strings, a k-tuple among them XORing to 0. If the lists are unbounded, the best classical (exponential) time complexity has withstood since Wagner's CRYPTO 2002 paper. If the lists are bounded (of the same size) and such that there is a single solution, the dissection algorithms of Dinur et al. (CRYPTO 2012) improve the memory usage over a simple meet-in-the-middle. In this paper, we study quantum algorithms for the k-xor problem. With unbounded lists and quantum access, we improve previous work by Grassi et al. (ASIACRYPT 2018) for almost all k. Next, we extend our study to lists of any size and with classical access only. We define a set of "merging trees" which represent the best known strategies for quantum and classical merging in k-xor algorithms, and prove that our method is optimal among these. Our complexities are confirmed by a Mixed Integer Linear Program that computes the best strategy for a given k-xor problem. All our algorithms apply also when considering modular additions instead of bitwise xors. This framework enables us to give new improved quantum k-xor algorithms for all k and list sizes. Applications include the subset-sum problem, LPN with limited memory and the multiple-encryption problem.

3.21 Implementing Grover oracles for quantum key search on AES and LowMC

Fernando Virdia (Royal Holloway University of London, GB)

Joint work of Samuel Jaques, Michael Naehrig, Martin Roetteler, Fernando Virdia
Main reference Samuel Jaques, Michael Naehrig, Martin Roetteler, Fernando Virdia: "Implementing Grover oracles for quantum key search on AES and LowMC", IACR Cryptology ePrint Archive, Vol. 2019, p. 1146, 2019.
URL https://eprint.iacr.org/2019/1146

Grover's search algorithm gives a quantum attack against block ciphers by searching for a key that matches a small number of plaintext-ciphertext pairs. This attack uses O(sqrt(N)) calls to the cipher to search a key space of size N. Previous work in the specific case of AES derived the full gate cost by analyzing quantum circuits for the cipher, but focused on minimizing the number of qubits.

In contrast, we study the cost of quantum key search attacks under a depth restriction and introduce techniques that reduce the oracle depth, even if it requires more qubits. As cases in point, we design quantum circuits for the block ciphers AES and LowMC. Our circuits give a lower overall attack cost in both the gate count and depth-times-width cost models. In NIST's post-quantum cryptography standardization process, security categories are defined based on the concrete cost of quantum key search against AES. We present new, lower cost estimates for each category, so our work has immediate implications for the security assessment of post-quantum cryptography.

As part of this work, we release Q# implementations of the full Grover oracle for AES-128, -192, -256 and for the three LowMC instantiations used in Picnic, including unit tests and code to reproduce our quantum resource estimates. To the best of our knowledge, these are the first two such full implementations and automatic resource estimations.

Participants

- Gorjan Alagic
University of Maryland – College Park, US
- Daniel C. Apon
NIST – Gaithersburg, US
- Daniel J. Bernstein
University of Illinois – Chicago, US
- Jean-François Biasse
University of South Florida – Tampa, US
- Christian Bischof
TU Darmstadt, DE
- Xavier Bonnetain
INRIA – Paris, FR
- Harry Buhrman
CWI – Amsterdam, NL
- Jintai Ding
University of Cincinnati, US
- Martin Ekera
KTH Royal Institute of Technology – Stockholm, SE
- Philippe Gaborit
University of Limoges, FR
- András Gilyén
Caltech – Pasadena, US
- Maria Isabel González Vasco
King Juan Carlos University – Madrid, ES
- Sean Hallgren
Pennsylvania State University – University Park, US
- Akinori Hosoyamada
NTT – Tokyo, JP
- David Jao
University of Waterloo, CA
- Samuel E. Jaques
University of Oxford, GB
- Stacey Jeffery
CWI – Amsterdam, NL
- Antoine Joux
Sorbonne University – Paris, FR
- Elena Kirshanova
Immanuel Kant Baltic Federal University – Kaliningrad, RU
- Thijs Laarhoven
TU Eindhoven, NL
- Bradley Lackey
Microsoft Corporation – Redmond, US
- Tanja Lange
TU Eindhoven, NL
- Alexander May
Ruhr-Universität Bochum, DE
- Shaun Miller
Florida Atlantic University – Boca Raton, US
- Dustin Moody
NIST – Gaithersburg, US
- Michele Mosca
University of Waterloo, CA
- Priyanka Mukhopadhyay
University of Waterloo, CA
- Maria Naya-Plasencia
INRIA – Paris, FR
- Phong Q. Nguyen
ENS – Paris, FR
- Ray Perlner
NIST – Gaithersburg, US
- Edoardo Persichetti
Florida Atlantic University – Boca Raton, US
- Rachel Player
Royal Holloway University of London, GB
- Thomas Pöppelmann
Infineon Technologies AG – Neubiberg, DE
- Yu Sasaki
NTT – Tokyo, JP
- John M. Schanck
University of Waterloo, CA
- André Schrottenloher
INRIA – Paris, FR
- Nicolas Sendrier
INRIA – Paris, FR
- Yixin Shen
Paris Diderot University, FR
- Daniel C. Smith-Tone
NIST – Gaithersburg, US
- Rainer Steinwandt
Florida Atlantic University – Boca Raton, US
- Adriana Suárez Corona
University of León, ES
- Jean-Pierre Tillich
INRIA – Paris, FR
- Iggy van Hoof
TU Eindhoven, NL
- Fernando Virdia
Royal Holloway University of London, GB
- Thomas Wunderer
BSI – Bonn, DE
- Bo-Yin Yang
Academia Sinica – Taipei, TW