Report from Dagstuhl Seminar 17401

Quantum Cryptanalysis

Edited by

Michele Mosca[1], Nicolas Sendrier[2], Rainer Steinwandt[3], and Krysta Svore[4]

1 **University of Waterloo, CA,** michele.mosca@uwaterloo.ca
2 **INRIA – Paris, FR,** nicolas.sendrier@inria.fr
3 **Florida Atlantic University – Boca Raton, US,** rsteinwa@fau.edu
4 **Microsoft Corporation – Redmond, US,** ksvore@microsoft.com

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 17401 "Quantum Cryptanalysis." We start out by outlining the motivation and organizational aspects of the seminar. Thereafter, abstracts of presentations given by seminar participants are provided.

Seminar October 1–6, 2017 – http://www.dagstuhl.de/17401
1998 ACM Subject Classification E.3 Code Breaking, F.2 Analysis of Algorithms and Problem Complexity, G.2 Discrete Mathematics
Keywords and phrases computational algebra, post-quantum cryptography, quantum circuit complexity, quantum computing, quantum hardware and resource estimation
Digital Object Identifier 10.4230/DagRep.7.10.1
Edited in cooperation with John M. Schanck

1 Executive Summary

Michele Mosca
Nicolas Sendrier
Rainer Steinwandt
Krysta Svore

Motivation and scope

Like its predecessors, this fourth installment of a Dagstuhl seminar on *Quantum Cryptanalysis* was devoted to studying cryptographic solutions that might be suitable for standardization in the post-quantum setting and to studying quantum attacks against currently deployed cryptographic solutions. Two main thrusts were of particular interest:

Algorithmic innovation. Quantum resources can be used in various way for attacking cryptographic solutions, and the seminar included multiple presentations on exploiting quantum resources for cryptanalytic purposes. Both attacks on symmetric and asymmetric primitives were considered, and there were lively discussions on the feasibility of mounting particular types of attacks. Complementing the presentations on quantum attacks, the program included presentations on advanced classical algorithms, raising the question of identifying possibilities to speed up such classical attack venues through quantum "subroutines."

Quantum resource estimation. It goes without saying that asymptotic improvements are of great interest when trying to tackle computational problems underpinning the security of cryptographic constructions. However, when looking at an actually deployed scheme, quantifying the exact resources (such as the number of qubits) needed by an attacker is relevant to judge the practical impact of a proposed attack strategy. The seminar included presentations on the estimation of resources for attacking some prominent cryptographic schemes.

As expected from a seminar with this title, many talks were indeed devoted to cryptanalysis, but the program also included presentations on establishing provable security guarantees in a post-quantum scenario. With the field becoming more mature, we did not schedule much time for survey talks. However, we did include a presentation on the *status of the development of quantum computers* in the program, thereby helping to get a better idea of potential obstacles when trying to implement quantum cryptanalytic attacks.

Organization

This was the fourth Dagstuhl seminar devoted entirely to quantum cryptanalysis, and as in the prior editions the set of participants included both experts in quantum algorithms and experts in classical cryptography. Some of the participants had already participated in earlier editions of this seminar series, but a number of colleagues attended such a seminar — or any Dagstuhl event — for the first time. In total, we had 42 participants from academia, government, and industry. This time we also included an open problem session in the program, which will hopefully help to stimulate further work in this vibrant research area. In the schedule we tried to leave sufficient time for discussions and for collaborative work in smaller groups. In line with the Dagstuhl tradition, no presentations were scheduled for Wednesday afternoon, and the seminar participants could devote the afternoon to a hike, an excursion, or to their research.

Results and next steps

Over the course of the years, communication and collaboration between the classical cryptographic and the quantum algorithmic research communities has intensified, and many colleagues cross traditional discipline boundaries. As evidenced in the seminar, available quantum cryptanalytic results can go well beyond asymptotic statements and include rather fine-grained resource counts. The seminar covered the analysis of both symmetric and asymmetric primitives, and ongoing efforts toward standardizing quantum-safe cryptographic solutions are likely to stimulate more progress, in particular on the quantum cryptanalysis of asymmetric cryptographic primitives.

2 Table of Contents

3 Overview of Talks

3.1 Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts

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

Joint work of Gorjan Alagic, Alexander Russell
Main reference Gorjan Alagic, Alexander Russell: "Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts", CoRR, Vol. abs/1610.01187, 2016.
URL http://arxiv.org/abs/1610.01187

Recent results of Kaplan et al., building on previous work by Kuwakado and Morii, have shown that a wide variety of classically-secure symmetric-key cryptosystems can be completely broken by quantum chosen-plaintext attacks (qCPA). In such an attack, the quantum adversary has the ability to query the cryptographic functionality in superposition. The vulnerable cryptosystems include the Even-Mansour block cipher, the three-round Feistel network, the Encrypted-CBC-MAC, and many others. In this work, we study simple algebraic adaptations of such schemes that replace $(\mathbb{Z}/2)^n$ addition with operations over alternate finite groups–such as $\mathbb{Z}/(2^n)$–and provide evidence that these adaptations are qCPA-secure. These adaptations furthermore retain the classical security properties (and basic structural features) enjoyed by the original schemes. We establish security by treating the (quantum) hardness of the well-studied Hidden Shift problem as a basic cryptographic assumption. We observe that this problem has a number of attractive features in this cryptographic context, including random self-reducibility, hardness amplification, and–in many cases of interest–a reduction from the "search version" to the "decisional version." We then establish, under this assumption, the qCPA-security of several such Hidden Shift adaptations of symmetric-key constructions. We show that a Hidden Shift version of the Even-Mansour block cipher yields a quantum-secure pseudorandom function, and that a Hidden Shift version of the Encrypted CBC-MAC yields a collision-resistant hash function. Finally, we observe that such adaptations frustrate the direct Simon's algorithm-based attacks in more general circumstances, e.g., Feistel networks and slide attacks.

3.2 Improved Combinatorial Algorithms for the Inhomogeneous Short Integer Solution Problem

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

Joint work of Shi Bai, Steven D. Galbraith, Liangze Li, Daniel Sheffield
Main reference Shi Bai, Steven D. Galbraith, Liangze Li, Daniel Sheffield: "Improved Combinatorial Algorithms for the Inhomogeneous Short Integer Solution Problem", IACR Cryptology ePrint Archive, Report 2014/593, 2014.
URL https://eprint.iacr.org/2014/593.pdf

We discuss algorithms for the inhomogeneous short integer solution problem: Given (A, s) to find a short vector x such that $Ax \equiv s \pmod{q}$. We consider algorithms for this problem due to Camion and Patarin; Wagner; Schroeppel and Shamir; Minder and Sinclair; Howgrave-Graham and Joux (HGJ); Becker, Coron and Joux (BCJ). Our main results include: Applying the Hermite normal form (HNF) to get faster algorithms; A heuristic analysis of the HGJ

and BCJ algorithms in the case of density greater than one; An improved cryptanalysis of the SWIFFT hash function; A new method that exploits symmetries to speed up algorithms for Ring-ISIS.

3.3 Low-communication parallel quantum multi-target preimage search

Gustavo Banegas (TU Eindhoven, NL)

Joint work of Gustavo Banegas, Daniel J. Bernstein
Main reference Gustavo Banegas, Daniel J. Bernstein: "Low-communication parallel quantum multi-target preimage search", IACR Cryptology ePrint Archive, Report 2017/789, 2017.
URL https://eprint.iacr.org/2017/789

The most important pre-quantum threat to AES-128 is the 1994 van Oorschot–Wiener "parallel rho method", a low-communication parallel pre-quantum multi-target preimage-search algorithm. This algorithm uses a mesh of p small processors, each running for approximately $2^{128}/pt$ fast steps, to find one of t independent AES keys $k_1, \ldots, k_t$, given the ciphertexts $\mathrm{AES}_{k_1}(0), \ldots, \mathrm{AES}_{k_t}(0)$ for a shared plaintext 0. NIST has claimed a high post-quantum security level for AES-128, starting from the following rationale: "Grover's algorithm requires a longrunning serial computation, which is difficult to implement in practice. In a realistic attack, one has to run many smaller instances of the algorithm in parallel, which makes the quantum speedup less dramatic." NIST has also stated that resistance to multi-key attacks is desirable; but, in a realistic parallel setting, a straightforward multi-key application of Grover's algorithm costs more than targeting one key at a time. This paper introduces a different quantum algorithm for multi-target preimage search. This algorithm shows, in the same realistic parallel setting, that quantum preimage search benefits asymptotically from having multiple targets. The new algorithm requires a revision of NIST's AES- 128, AES-192, and AES-256 security claims

3.4 Classical Proofs for the Quantum Security of Classical Hash Functions

Serge Fehr (CWI - Amsterdam, NL)

Hash functions are of fundamental importance in cryptography, and with the threat of quantum computers possibly emerging in the future, it is an urgent objective to understand the security of cryptographic hash functions in the light of potential future quantum attacks. To this end, we reconsider the notion of the so-called collapsing property of hash functions, as introduced by Unruh, which replaces the notion of collision resistance when considering quantum attacks. Our contribution is the introduction of a framework that offers significantly simpler proofs for the collapsing property of hash functions. With our framework, we can prove the collapsing property for hash domain extension constructions entirely by means of decomposing the iteration function into suitable elementary composition operations. In particular, given our framework, one can argue purely classically about the quantum-security

of hash functions; this is in contrast to previous proofs which are in terms of sophisticated quantum-information-theoretic and quantum-algorithmic reasoning. This is work in progress.

3.5 Towards cryptographic applications of quantum walks

Peter Høyer (University of Calgary, CA)

Joint work of Cătălin Dohotaru, Peter Høyer, Mojtaba Komeili
Main reference Peter Høyer, Mojtaba Komeili: "Efficient Quantum Walk on the Grid with Multiple Marked Elements", in Proc. of the 34th Symposium on Theoretical Aspects of Computer Science, STACS 2017, March 8-11, 2017, Hannover, Germany, LIPIcs, Vol. 66, pp. 42:1–42:14, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.
URL http://dx.doi.org/10.4230/LIPIcs.STACS.2017.42

We give an introduction to quantum walks, including Szegedy's correspondence between random walks and quantum walks. We survey the main known general quantum walk algorithms. We discuss properties of three of the most commonly used classes of graphs in quantum algorithms and protocols: the complete graphs, the Johnson graphs, and the tori graphs. We show how a quantum walk on a Johnson graph is used in an algorithm for the computational problem of element distinctness. We show how a quantum walk on a torus is used in protocols for the 2-party communication problem of disjointness. We discuss and speculate on future potential uses of quantum walks in cryptographic protocols. We end with pointers to literature and surveys.

3.6 Post-quantum security of the sponge construction

Andreas Hülsing (TU Eindhoven, NL)

Joint work of Jan Czajkowski, Leon Groot Bruinderink, Andreas Hülsing, Christian Schaffner, Dominique Unruh
Main reference Jan Czajkowski, Leon Groot Bruinderink, Andreas Hülsing, Christian Schaffner, Dominique Unruh: "Post-quantum security of the sponge construction", IACR Cryptology ePrint Archive, Report 2017/771, 2017.
URL https://eprint.iacr.org/2017/771

We investigate the post-quantum security of hash functions based on the sponge construction. A crucial property for hash functions in the post-quantum setting is the collapsing property (a strengthening of collision-resistance). We show that the sponge construction is collapsing (and in consequence quantum collision-resistant) under suitable assumptions about the underlying block function. In particular, if the block function is a random function or a (non-invertible) random permutation, the sponge construction is collapsing.

3.7 Random self-reducibility for SIDH

David Jao (University of Waterloo, CA)

We discuss preliminary results concerning the self-reducibility of Supersingular Isogeny Diffie-Hellman (SIDH) problem instances over the same base field.

3.8 Connections between Learning with Errors and the Dihedral Coset Problem

Elena Kirshanova (ENS - Lyon, FR)

Joint work of Zvika Brakerski, Elena Kirshanova, Damien Stehlé, Weiqiang Wen
Main reference Zvika Brakerski, Elena Kirshanova, Damien Stehlé, Weiqiang Wen: "Learning With Errors and Extrapolated Dihedral Cosets", CoRR, Vol. abs/1710.08223, 2017.
URL http://arxiv.org/abs/1710.08223

In this talk I explained the result that shows that under quantum polynomial time reductions, LWE is equivalent to a relaxed version of the dihedral coset problem (DCP), which is called extrapolated DCP (eDCP). The extent of extrapolation varies with the LWE noise rate. By considering different extents of extrapolation, the result generalizes Regev's famous proof that if DCP is in BQP (quantum poly-time) then so is LWE (FOCS 02). I also discussed a connection between eDCP and Childs and Van Dam's algorithm for generalized hidden shift problems (SODA 07).The result implies that a BQP solution for LWE might not require the full power of solving DCP, but rather only a solution for its relaxed version, eDCP, which could be easier.

3.9 Quantum Cryptanalysis of Block Ciphers: A Case Study

Yi-Kai Liu (NIST - Gaithersburg, US)

Quantum computers can achieve a quadratic speedup over classical computers, when performing an exhaustive key search against a block cipher. This quantum attack uses Grover's algorithm, and it requires the implementation of the target cipher using reversible logic, so that it can be run on a superposition of different inputs.

We report quantum circuits and resource bounds for several well-known block ciphers: MARS, SERPENT, Simon, and Speck. We find that quantum cryptanalysis of Simon and Speck is feasible on relatively small quantum computers, with a few hundred logical qubits, and 10^5 to 10^6 quantum gates per Grover iteration. This is a consequence of the design of those ciphers, using large numbers of simple "ARX" operations (e.g., addition mod 2^n, bit-rotation, and bitwise XOR). SERPENT, which uses small S-boxes, has somewhat different

resource requirements. At the other extreme, MARS requires much larger quantum circuits, due to its complex internal structure and its large pseudorandom S-boxes.

3.10 Grover Meets Simon - Quantumly Attacking the FX-construction

Alexander May (Ruhr-Universität Bochum, DE)

Joint work of Gregor Leander, Alexander May
Main reference Gregor Leander, Alexander May: "Grover Meets Simon - Quantumly Attacking the FX-construction", in Proc. of the Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II, Lecture Notes in Computer Science, Vol. 10625, pp. 161–178, Springer, 2017.
URL http://dx.doi.org/10.1007/978-3-319-70697-9_6

Using whitening keys is a well understood mean of increasing the key-length of any given cipher. Especially as it is known ever since Grover's seminal work that the effective key-length is reduced by a factor of two when considering quantum adversaries, it seems tempting to use this simple and elegant way of extending the key-length of a given cipher to increase the resistance against quantum adversaries. However, as we show in this work, using whitening keys does not increase the security in the quantum-CPA setting significantly. For this we present a quantum algorithm that breaks the construction with whitening keys in essentially the same time complexity as Grover's original algorithm breaks the underlying block cipher. Technically this result is based on the combination of the quantum algorithms of Grover and Simon for the first time in the cryptographic setting.

3.11 New Results on Symmetric Quantum Cryptanalysis

Maria Naya-Plasencia (INRIA - Paris, FR)

Joint work of André Chailloux, María Naya-Plasencia, André Schrottenloher
Main reference André Chailloux, María Naya-Plasencia, André Schrottenloher: "An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography", in Proc. of the Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II, Lecture Notes in Computer Science, Vol. 10625, pp. 211–240, Springer, 2017.
URL http://dx.doi.org/10.1007/978-3-319-70697-9_8

In this talk I will present some recent results on symmetric quantum cryptanalysis: a new efficient quantum collision search algorithm (joint work with A. Chailloux and A. Schrottenloher) and an extensive analysis of the use of modular additions on symmetric primitives (joint work with X. Bonnetain).

3.12 Thermodynamic Analysis of Classical and Quantum Algorithms for Preimage and Collision Search Problems

Ray Perlner (NIST - Gaithersburg, US)

We analyze the performance of classical and quantum search algorithms from a thermodynamic perspective, focusing on resources such as time, energy, and memory size. We consider two examples that are relevant to post-quantum cryptography: Grover's search algorithm, and the quantum algorithm for collision-finding. Using Bennett's "Brownia" model of low-power reversible computation, we show classical algorithms that have the same asymptotic energy consumption as these quantum algorithms. Thus, the quantum advantage in query complexity does not imply a reduction in these thermodynamic resource costs. In addition, we present realistic estimates of the resource costs of quantum and classical search, for near-future computing technologies. We find that, if memory is cheap, classical exhaustive search can be surprisingly competitive with Grover's algorithm.

3.13 Quantum resource estimates for computing elliptic curve discrete logarithms

Martin Roetteler (Microsoft Corporation - Redmond, US)

Joint work of Martin Roetteler, Michael Naehrig, Krysta M. Svore, Kristin Lauter
Main reference Martin Roetteler, Michael Naehrig, Krysta M. Svore, Kristin E. Lauter: "Quantum resource estimates for computing elliptic curve discrete logarithms", CoRR, Vol. abs/1706.06752, 2017.
URL http://arxiv.org/abs/1706.06752

We give precise quantum resource estimates for Shor's algorithm to compute discrete logarithms on elliptic curves over prime fields. The estimates are derived from a simulation of a Toffoli gate network for controlled elliptic curve point addition, implemented within the framework of the quantum computing software tool suite Liquid. We determine circuit implementations for reversible modular arithmetic, including modular addition, multiplication and inversion, as well as reversible elliptic curve point addition. We conclude that elliptic curve discrete logarithms on an elliptic curve defined over an n-bit prime field can be computed on a quantum computer with at most $9n + 2\lceil \log_2(n) \rceil + 10$ qubits using a quantum circuit of at most $448n^3 \log_2(n) + 4090n^3$ Toffoli gates. We are able to classically simulate the Toffoli networks corresponding to the controlled elliptic curve point addition as the core piece of Shor's algorithm for the NIST standard curves P-192, P-224, P-256, P-384 and P-521. Our approach allows gate-level comparisons to recent resource estimates for Shor's factoring algorithm. The results also support estimates given earlier by Proos and Zalka and indicate that, for current parameters at comparable classical security levels, the number of qubits required to tackle elliptic curves is less than for attacking RSA, suggesting that indeed ECC is an easier target than RSA.

3.14 Factoring integers by algorithms for lattice reduction

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

URL http://www.math.uni-frankfurt.de/ dmst/research/papers/SVP9.pdf

We factor an integer N by enumeration algorithms that find vectors of the prime number lattice $\mathcal{L}(\mathbf{B}_{n,c})$ close to a specific target vector $\mathbf{N}_c$ representing N. The algorithm NewEnum performs the stages of exhaustive enumeration of close, respectively short lattice vectors in order of decreasing success rate, stages with high success rate are done first. These algorithms generate for the n-th prime p_n triples of p_n-smooth integers $u, v, |u - vN|$ that factorize the integer N. An integer N can be factored by about $n + 1$ p_n-smooth triples $u, v, |u - vN|$. Our CVP-algorithm generates for $n = 90$, $n + 1$ such relations and factors $N \approx 1014$ in 6.2 seconds. We consider extensions to large N.

3.15 Code based cryptography and quantum attacks

Jean-Pierre Tillich (INRIA - Paris, FR)

This talk is a survey of how quantum algorithms can be used to speed up the fundamental problem on which code-based cryptography relies, namely the decoding problem. I will first cover Bernstein's algorithm which uses Grover to get a quantum speed-up over the simplest information set decoding algorithm, namely the Prange algorithm. Then I will cover my work with Kachigar on how using quantum walk techniques with Grover to get a further quantum speed-up. I will also talk about a result of Grilo and Kerenidis using quantum Fourier techniques for solving the LPN/LWE problem in polynomial time if we have access to a quantum superposition of all LPN samples.

3.16 Security of Fiat-Shamir

Dominique Unruh (University of Tartu, EE)

Main reference Dominique Unruh: "Post-quantum Security of Fiat-Shamir", in Proc. of the Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I, Lecture Notes in Computer Science, Vol. 10624, pp. 65–95, Springer, 2017.
URL http://dx.doi.org/10.1007/978-3-319-70694-8_3

We describe how classical security proofs for Fiat-Shamir go wrong in the quantum setting, and what can be done about it.

3.17 Status of the development of quantum computers

Frank K. Wilhelm (Universität des Saarlandes - Saarbrücken, DE)

I am reviewing three major current routes to quantum correction. For cryptanalysis, fault-tolerant quantum computing with the surface code is currently the only viable way. I am proposing a five-tier evaluation system for the status of quantum computing implementations and describe candidates for the lowest three. I try to speculate on how to scale up to 1 MQubits.

4 Open problems

The discussion started with presentations of various challenge problem web pages.

Multivariate-quadratic challenges. Tsuyoshi Takagi (University of Tokyo, JP) started with an overview of the Fukuoka MQ challenge page, for solving multivariate quadratic polynomial challenges: www.mqchallenge.org. There are three sub-families of challenges, including three encryption schemes and three signature schemes (over finite fields of over 2, 2^8 and 31), and a Hall of Fame for each of the six families of schemes.
The coefficients of the challenges are generated from the digits of Π, however for the encryption schemes the MQ challenge team provide one random answer to guarantee a solution and thus the team does not participate in the three encryption challenges (but can participate in the signature challenges).

Lattice challenges. Johannes Buchmann (TU Darmstadt, DE) presented the lattice challenge web pages at latticechallenge.org. The main page outlines the challenge consisting of lattice bases for which the solution of SVP implies a solution of SVP in all lattices of a certain smaller dimension. There are two ways to enter the Hall of Fame:
- Find a short vector in a new challenge dimension
- Find an even shorter vector in one of the dimensions already listed in the hall of fame.

Wild McEliece challenges. Tanja Lange (TU Eindhoven, NL) presented the wild McEliece challenges at pqcrypto.org. The web page also lists other post-quantum challenge pages.

Other challenges. The NTRU challenges (www.onboardsecurity.com/products/ntru-crypto/ntru-challenge) and R-LWE challenges (web.eecs.umich.edu/~cpeikert/rlwe-challenges/) were also mentioned.

The discussion continued with presentations of other open problems.
- Yi-Kai Liu (NIST – Gaithersburg, US) highlighted a paper by Kimmel, Lin and Lin on "Oracles with costs" as a possible tool for quantum cryptanalysis. arXiv:1502.02174
- Phong Nguyen (University of Tokyo, JP) presented some open questions related to sampling vectors in a lattice.
- John Schanck (University of Waterloo, CA) presented a variant of the subset sum problem where the collection of numbers is a subset chosen from a much larger set of randomly sampled numbers.

Participants

- Gorjan Alagic
University of Maryland – College Park, US
- Shi Bai
Florida Atlantic University – Boca Raton, US
- Gustavo Banegas
TU Eindhoven, NL
- Daniel J. Bernstein
University of Illinois – Chicago, US
- Jean-François Biasse
University of South Florida – Tampa, US
- Alexei Bocharov
Microsoft Corporation – Redmond, US
- Johannes A. Buchmann
TU Darmstadt, DE
- Yfke Dulek
CWI – Amsterdam, NL
- Serge Fehr
CWI – Amsterdam, NL
- Tommaso Gagliardoni
IBM Research Zurich, CH
- Vlad Gheorghiu
University of Waterloo, CA
- Maria Isabel González Vasco
King Juan Carlos University – Madrid, ES
- Sean Hallgren
Pennsylvania State University – University Park, US
- Peter Hoyer
University of Calgary, CA
- Andreas Hülsing
TU Eindhoven, NL
- David Jao
University of Waterloo, CA
- Stacey Jeffery
CWI – Amsterdam, NL
- Elena Kirshanova
ENS – Lyon, FR
- Stavros Kousidis
BSI – Bonn, DE
- Thijs Laarhoven
IBM Research Zurich, CH
- Bradley Lackey
University of Maryland – College Park, US
- Tanja Lange
TU Eindhoven, NL
- Yi-Kai Liu
NIST – Gaithersburg, US
- Alexander May
Ruhr-Universität Bochum, DE
- Michele Mosca
University of Waterloo, CA
- Michael Naehrig
Microsoft Research – Redmond, US
- Anderson Nascimento
University of Washington – Tacoma, US
- Maria Naya-Plasencia
INRIA – Paris, FR
- Phong Q. Nguyen
University of Tokyo, JP
- Ray Perlner
NIST – Gaithersburg, US
- Martin Roetteler
Microsoft Corporation – Redmond, US
- Alexander Russell
University of Connecticut – Storrs, US
- John M. Schanck
University of Waterloo, CA
- Claus Peter Schnorr
Goethe-Universität – Frankfurt am Main, DE
- Nicolas Sendrier
INRIA – Paris, FR
- Daniel Smith-Tone
NIST – Gaithersburg, US
- Rainer Steinwandt
Florida Atlantic University – Boca Raton, US
- Adriana Suárez Corona
University of León, ES
- Tsuyoshi Takagi
University of Tokyo, JP
- Jean-Pierre Tillich
INRIA – Paris, FR
- Dominique Unruh
University of Tartu, EE
- Frank K. Wilhelm
Universität des Saarlandes – Saarbrücken, DE