

Report from Dagstuhl Seminar 11381

Quantum Cryptanalysis

Edited by

Serge Fehr¹, Michele Mosca², Martin Rötteler³, and
Rainer Steinwandt⁴

1 CWI – Amsterdam, NL, Serge.Fehr@cwi.nl

2 IQC, University of Waterloo, and Perimeter Institute, CA, mmosca@iqc.ca

3 NEC Laboratories America, Inc. – Princeton, US, mroetteler@nec-labs.com

4 Florida Atlantic University – Boca Raton, US, rsteinwa@fau.edu

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 11381 “Quantum Cryptanalysis”. The first section gives an overview of the meeting, including organizational aspects. Subsequently abstracts of presentations at the meeting are provided (in alphabetical order).

Seminar 18.–23. September, 2011 – www.dagstuhl.de/11381

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

Keywords and phrases Security of cryptographic schemes, quantum algorithms, computational hardness assumptions

Digital Object Identifier 10.4230/DagRep.1.9.58

Edited in cooperation with Florian Speelman

1 Executive Summary

Serge Fehr

Michele Mosca

Martin Rötteler

Rainer Steinwandt

License  Creative Commons BY-NC-ND 3.0 Unported license
© Serge Fehr, Michele Mosca, Martin Rötteler, and Rainer Steinwandt

Motivation and Goals

Cryptography aims at providing tools for securing information and preventing critical information-processing operations from adversarially provoked malfunction. These are very crucial objectives in today’s society where the importance of information is steadily increasing. As such, great effort is put into studying and implementing cryptographic schemes that offer privacy-protecting solutions for various tasks, and, wittingly or unwittingly, many people rely on cryptography in daily life. However, most of the cryptographic schemes that are currently in use rely on computational hardness assumptions that fail to hold in the presence of a quantum computer (like the hardness of factoring large integers or of computing discrete logarithms in certain cyclic groups). Thus, if brought to fruition, a large scale quantum computer will have a poignant impact on the security of cryptographic schemes. The following extreme opinions are commonly encountered:



Except where otherwise noted, content of this report is licensed under a Creative Commons BY-NC-ND 3.0 Unported license
Quantum Cryptanalysis, *Dagstuhl Reports*, Vol. 1, Issue 9, pp. 58–75

Editors: Serge Fehr, Michele Mosca, Martin Rötteler, and Rainer Steinwandt



DAGSTUHL REPORTS
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

- *We'll deal with it later.* Subscribers to this point of view argue that because quantum computers currently are still in their infancy they do not pose a threat to existing schemes. Further, as it is unclear whether they will ever scale beyond the size of a handful qubits, it is not necessary to change security parameters of currently deployed practical systems, not to mention the need to switch to other systems with different (new) hardness assumptions.
- *Fight quantum with quantum.* Proponents of this view point out that the laws of quantum mechanics offer the possibility of information-theoretic security from first principles. Quantum key establishment is a prominent example of this line of research and (for shorter distances) has reached remarkable maturity. However, one should note that classical cryptographic components are often involved here, too— e.g. for ensuring authenticity, or even for encryption in order to reduce the amount of key material.

Both opinions have their merit, but offer no satisfying options for today's design of mid- and long-term secure cryptographic solutions, where a typical user does not have access to quantum links with other users, etc, as needed in quantum protocols. Completely ignoring the threat of a quantum computer looming on the horizon, means taking a systemic risk for real life applications. At the same time, there is no need for a panic type of reaction “just” because of an asymptotic threat for existing cryptographic infrastructures. Unfortunately, various cryptographic proposals made for “post quantum” cryptography build on hardness assumptions which have never been seriously cross-checked with experts in the design of quantum algorithms. This situation is rather unsatisfying and the goal of this Dagstuhl seminar was to pave the road towards a sound exploration of hardness assumptions and cryptographic protocol design where an adversary may use quantum algorithms. Loosely speaking, the idea was to “find and characterize quantum-resilience”: bringing together cryptographic experts with an interest in quantum computing and experts on quantum computing with an interest in cryptography, we want to study complexity and hardness assumptions of classical cryptographic schemes from a quantum perspective. We aim at the design of practical cryptographic schemes with tangible evidence for their “post quantum” security that goes beyond the mere non-existence of quantum attacks according to the current state of the art.

The seminar aimed at understanding the exact potential of quantum attacks on today's cryptographic schemes. This question is closely related to the question of plausible quantum computational assumptions. Motivating examples of such assumptions can be found in a cryptographic scheme of Regev from 2009 and a candidate one-way function suggested by Moore, Russell and Vazirani in 2007: the former is a classical public key scheme based on the hardness of the unique shortest vector problem for lattices. It can be argued to be resilient against quantum attacks by relating security guarantees to a hidden subgroup problem in dihedral groups for which, despite much effort by experts on quantum algorithms, no polynomial quantum algorithm has been found. Moore et al.'s proposal rests on an argument from lower bounds on the size of a quantum memory that would be required for the standard quantum approach to graph isomorphism by reducing again to a hidden subgroup problem.

Seminar Organization

A total of 41 scientists from across the world, including both young and senior researchers, visited Dagstuhl for this seminar. To ensure fruitful discussions between experts in quantum computing and in cryptography, the invited participants were chosen such that there is enough common ground/research experience to communicate with colleagues in the other

“camp”. We scheduled the talks with sufficient buffer to have time left for interaction during the talks and for discussions in smaller groups between the talks. Details of the schedule kept changing during the seminar, reflecting the dynamic nature of this meeting. For Wednesday afternoon no talks were scheduled and some participants took advantage of this free afternoon for a hiking trip, some for an excursion to Trier, and others for more discussions.

Topics and Achievements

As anticipated, one of the central topics of the seminar was the hardness of cryptographically relevant computational problems in the presence of quantum attacks: a number of talks addressed classical computational problems and the availability or non-availability of efficient quantum algorithms for these. Moreover, specific cryptographic proposals were discussed which were designed to offer resistance against adversaries with access to quantum computers. Security guarantees of such schemes may rely on some suitable computational hardness assumption, but also on other technological restrictions imposed on the attacker, or solely on the correctness of quantum mechanics. Talks on additional topics, specifically on efficient implementations, foundations of quantum computing and quantum information theory completed the program of the seminar. More details on the individual talks can be found in the abstracts following this introduction.

Looking at the extensive, fruitful, and passionate discussions in the seminar, it is fair to say that this meeting successfully fostered the exchange of two research communities. The presented talks and ensuing discussions added to our understanding of particular cryptographic constructions in the presence of quantum computers. Directions for future work on “quantum-resistant” cryptographic schemes have been indicated, and we hope that follow-up meetings will offer the opportunity to deepen the collaboration between quantum computing and cryptography and therewith help to advance the state-of-the-art in “post quantum” cryptography.

2 Table of Contents

Executive Summary

Serge Fehr, Michele Mosca, Martin Rötteler, and Rainer Steinwandt 58

Overview of Talks





Post-quantum cryptanalysis <i>Daniel J. Bernstein</i>	63
Quantum computing on encrypted data <i>Anne Broadbent</i>	63
Constructing elliptic curve isogenies in quantum subexponential time <i>Andrew Childs</i>	64
A quasipolynomial-time algorithm for the quantum separability problem <i>Matthias Christandl</i>	64
Free randomness amplification <i>Roger Colbeck</i>	65
Security against quantum side information in randomness amplification <i>Serge Fehr</i>	65
Quantum money with classical verification <i>Dmitry Gavinsky</i>	65
Computing the unit group, class group and compact representations in algebraic function fields <i>Sean Hallgren</i>	66
Random quantum circuits are approximate poly-designs <i>Aram W. Harrow</i>	66
Quantum money <i>Avinatan Hassidim</i>	66
Schemes for establishing keys with quantum eavesdroppers <i>Peter Hoyer</i>	67
Quantum fingerprints that keep secrets <i>Tsuyoshi Ito</i>	67
Complexity implications of quantum field theory <i>Stephen P. Jordan</i>	68
Simplified instantaneous non-local quantum computation with applications to position-based cryptography <i>Robert Koenig</i>	68
State-of-the-art branchless techniques for elliptic curve scalar multiplication <i>Tanja Lange</i>	69
Techniques for quantum circuit optimization <i>Dmitri Maslov</i>	69
Decoding random linear codes in $\tilde{O}(2^{0.054n})$ <i>Alexander May</i>	69

The McEliece cryptosystem resists quantum Fourier sampling attacks <i>Cris Moore</i>	70
Proof of plaintext knowledge for code-based cryptosystems <i>Kirill Morozov</i>	70
What can you hide in qutrit chains? <i>Daniel Nagaj</i>	71
Quantum algorithms for the hidden shift problem of Boolean functions <i>Maris Ozols</i>	71
Self-testing for sequential CHSH games <i>Ben Reichardt</i>	71
Quantum adversary lower bounds by polynomials <i>Jeremie Roland</i>	72
Improvements on circuit lattices <i>Igor A. Semaev</i>	72
On the hidden shifted power problem <i>Igor Shparlinski</i>	73
The garden-hose game and application to position-based cryptography <i>Florian Speelman</i>	73
Certifable quantum dice <i>Thomas Vidick</i>	73
Participants	75

3 Overview of Talks

3.1 Post-quantum cryptanalysis





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

License     Creative Commons BY-NC-ND 3.0 Unported license
© Daniel J. Bernstein
URL <http://cr.yptalks/2011.09.22/slides.pdf>

This talk surveyed the pre-quantum and post-quantum cryptographic landscape, and highlighted some examples of cryptanalytic challenges, including challenges where the best available attack algorithms should be accelerated by quantum computers.

3.2 Quantum computing on encrypted data

Anne Broadbent (University of Waterloo, CA)

License     Creative Commons BY-NC-ND 3.0 Unported license
© Anne Broadbent

We show that any two-party quantum computation, specified by a unitary which acts simultaneously on the registers of both parties, can be securely implemented against any specious (quantum semi-honest) adversary, with the only additional assumption that the parties have access to an ideal quantum SWAP gate. This establishes that unitaries alone are universal for private two-party evaluation of unitaries, thus answering an open question of Dupuis, Nielsen and Salvail.


We first give a simple protocol for computing the $\pi/8$ gate in a client-server scenario, where the client holds the encryption key for an encrypted qubit held by the server. The client need only prepare a single random auxiliary qubit (chosen among four possibilities), and exchange classical communication. This construction improves on previous work, which requires either multiple auxiliary qubits or two-way quantum communication. We show security against any adversarial server. We then show how to promote this protocol to be secure against both parties, without introducing any extra assumptions. Combined with [1], this shows our main result.

References

- 1 F. Dupuis and J.B. Nielsen and L. Salvail. Secure Two-Party Quantum Evaluation of Unitaries against Specious Adversaries. In *Proceedings of Crypto 2010*, pp. 685–706, LNCS, Vol. 6332, 2010.

3.3 Constructing elliptic curve isogenies in quantum subexponential time

Andrew Childs (University of Waterloo, CA)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Andrew Childs

Joint work of Childs, Andrew; Jao, David; Soukharev, Vladimir


Main reference A. M. Childs, D. Jao, V. Soukharev, “Constructing elliptic curve isogenies in quantum subexponential time,” arXiv:1012.4019

URL <http://arxiv.org/abs/arXiv:1012.4019>

Given two elliptic curves over a finite field having the same cardinality and endomorphism ring, it is known that the curves admit an isogeny between them, but finding such an isogeny is believed to be computationally difficult. The fastest known classical algorithm takes exponential time, and prior to our work no faster quantum algorithm was known. Recently, public-key cryptosystems based on the presumed hardness of this problem have been proposed as candidates for post-quantum cryptography. In this work, we give a new subexponential-time quantum algorithm for constructing isogenies between two such elliptic curves, assuming the Generalized Riemann Hypothesis (but with no other assumptions). Our algorithm is based on a reduction to a hidden shift problem, and represents the first nontrivial application of Kuperberg’s quantum algorithm for the hidden shift problem. This result suggests that isogeny-based cryptosystems may be uncompetitive with more mainstream quantum-resistant cryptosystems such as lattice-based cryptosystems.

3.4 A quasipolynomial-time algorithm for the quantum separability problem

Matthias Christandl (ETH Zürich, CH)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Matthias Christandl

Joint work of Brandao, Fernando; Christandl, Matthias; Yard, Jon


Main reference F. Brandao, M. Christandl, J. Yard, “A quasipolynomial-time algorithm for the quantum separability problem,” Proc. 43rd annual ACM Symposium on Theory of Computing (STOC’11), pp. 343–352.

URL <http://dx.doi.org/10.1145/1993636.1993683>

We present a quasipolynomial-time algorithm for solving the weak membership problem for the convex set of separable, i.e. non-entangled, bipartite density matrices. The algorithm decides whether a density matrix is separable or whether it is ϵ -away from the set of the separable states in time $\exp(O(\epsilon^{-2} \log |A| \log |B|))$, where $|A|$ and $|B|$ are the local dimensions, and the distance is measured with either the Euclidean norm, or with the so-called LOCC norm. The latter is an operationally motivated norm giving the optimal probability of distinguishing two bipartite quantum states, each shared by two parties, using any protocol formed by quantum local operations and classical communication (LOCC) between the parties.

3.5 Free randomness amplification

Roger Colbeck (Perimeter Institute – Waterloo, CA)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Roger Colbeck

Joint work of Colbeck, Roger; Renner, Renato


Main reference R. Colbeck, R. Renner, “Free randomness can be amplified,” arXiv:1105.3195v2 [quant-ph]

URL <http://arxiv.org/abs/1105.3195v2>

In many cryptographic tasks, it is assumed that parties have a source of local random bits. I will consider a scenario in which this assumption is weakened, imagining that instead a malicious adversary can influence the source to some extent. In such a scenario, it is known that no classical protocol can use such a source to generate even a single uniform bit. However, I will show that with a quantum protocol this can be done. Furthermore, this protocol remains secure even if quantum theory is one day superseded, provided that the new theory is non-signalling.

3.6 Security against quantum side information in randomness amplification

Serge Fehr (CWI – Amsterdam, NL)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Serge Fehr

Joint work of Fehr, Serge; Gelles, Ran; Schaffner, Christian

Main reference S. Fehr, R. Gelles, C. Schaffner, “Security and Composability of Randomness Expansion from Bell Inequalities,” arXiv:1111.6052v2 [quant-ph]


URL <http://arxiv.org/abs/1111.6052v2>

We consider the problem of randomness amplification from Bell inequalities, as initially proposed by Colbeck and worked out by Pironio et al. We show that in this setting, security against quantum side information comes for free.

Specifically, we show that a lower bound on the (worst case) min-entropy that is obtained under the assumption that the adversary holds no (quantum nor classical) side information, also holds in case the adversary holds quantum side information. This in particular implies that the bounds obtained by Pironio et al. extend to the setting with quantum side information.

3.7 Quantum money with classical verification

Dmitry Gavinsky (NEC Laboratories America, Inc. – Princeton, US)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Dmitry Gavinsky


Main reference D. Gavinsky, “Quantum Money with Classical Verification,” arXiv:1109.0372v1 [quant-ph]

URL <http://arxiv.org/abs/1109.0372>

We construct a quantum money scheme that allows verification through classical communication with bank. This is the first demonstration that a secure quantum money scheme exists that does not require quantum communication for coin verification.

3.8 Computing the unit group, class group and compact representations in algebraic function fields

Sean Hallgren (Penn State University, US)


License  Creative Commons BY-NC-ND 3.0 Unported license
© Sean Hallgren

Joint work of Eisentraeger, Kirsten; Hallgren, Sean

Number fields and global function fields have many similar properties. Both have many applications to cryptography and coding theory, and the main computational problems for number fields, such as computing the ring of integers and computing the class group and the unit group, have analogues over function fields. The complexity of the number field problems has been studied extensively and these problems have been the source of some exponential speedups by quantum computation. In this paper we study the analogous problems in function fields. We show that there are efficient quantum algorithms for computing the unit group, the class group and for solving the principal ideal problem in function fields of arbitrary degree. We show that compact representations exist, which allows us to show that the principal ideal problem is in NP. Unlike the number field case, we are also able to show that these compact representatives can be computed efficiently.

3.9 Random quantum circuits are approximate poly-designs

Aram W. Harrow (University of Washington, US)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Aram W. Harrow


Joint work of Brandao, Fernando G.S.L.; Harrow, Aram W.; Horodecki, Michal

An ϵ -approximate t -design is a distribution over unitaries such that t copies of a unitary from the distribution cannot be distinguished from t copies of a Haar-uniform unitary with bias greater than ϵ . In other words, designs look like they are uniformly random if we look at low-degree polynomials of their entries.

We prove that random circuits on n qubits of length $O(n^2 t^5 \log(1/\epsilon))$ are approximate t -designs. Previously random circuits were only known to be 3-designs, and efficient constructions of t -designs were only known for $t \leq n/\log(n)$. Our proof uses tools from many-body theory and from representation theory.

3.10 Quantum money

Avinatan Hassidim (MIT – Cambridge, US)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Avinatan Hassidim

Joint work of Aaronson, Scott; Farhi, Eddie; Gosset, David; Kelner, Jon; Lutomirski, Andy; Shor, Peter
URL <http://www2.lns.mit.edu/avinatan/publications.html>

One of the problems in classical security is that information can be copied: passwords can be stolen, songs can be pirated, and when you email an attachment, you still have the original. One implication is that E-commerce requires communicating with a server (e.g. the credit card company or PayPal) whenever one makes a transaction. One could hope that the no-cloning theorem would help circumvent this and enable a physical quantum state to

function like money. Such money could be used in transactions both in person and on a future “Quantum Internet,” not requiring contact with a central authority.

In the talk I will survey some recent progress on quantum money. I will present an impossibility result for a certain family of schemes, and a scheme which is based on ideas from knot theory.

3.11 Schemes for establishing keys with quantum eavesdroppers

Peter Hoyer (University of Calgary, CA)

License © © ⊖ Creative Commons BY-NC-ND 3.0 Unported license

© Peter Hoyer

Joint work of Brassard, Gilles; Høyer, Peter; Kalach, Kassem; Kaplan, Marc; Laplante, Sophie; Salvail, Louis

Main reference G. Brassard, P. Høyer, K. Kalach, M. Kaplan, S. Laplante, L. Salvail, “Merkle Puzzles in a Quantum World,” Proc. 31st Annual International Conference on Cryptology (CRYPTO 2011), pp. 391–410, LNCS Vol. 6841, 2011.

URL http://dx.doi.org/10.1007/978-3-642-22792-9_22

In 1974, Ralph Merkle proposed the first unclassified scheme for secure communications over insecure channels. When legitimate communicating parties are willing to spend an amount of computational effort proportional to some parameter N , an eavesdropper cannot break into their communication without spending a time proportional to N^2 , which is quadratically more than the legitimate effort. We showed in an earlier paper that Merkle’s schemes are completely insecure against a quantum adversary, but that their security can be partially restored if the legitimate parties are also allowed to use quantum computation: the eavesdropper needed to spend a time proportional to $N^{3/2}$ to break our earlier quantum scheme. Furthermore, all previous *classical* schemes could be broken completely by the onslaught of a quantum eavesdropper and we conjectured that this is unavoidable.

We give two novel key establishment schemes in the spirit of Merkle’s. The first one can be broken by a quantum adversary that makes an effort proportional to $N^{5/3}$ to implement a quantum random walk in a Johnson graph reminiscent of Andris Ambainis’ quantum algorithm for the element distinctness problem. This attack is optimal up to logarithmic factors. Our second scheme is purely classical, yet it cannot be broken by a quantum eavesdropper who is only willing to expend effort proportional to that of the legitimate parties.

3.12 Quantum fingerprints that keep secrets

Tsuyoshi Ito (University of Waterloo, CA)

License © © ⊖ Creative Commons BY-NC-ND 3.0 Unported license

© Tsuyoshi Ito

Joint work of Gavinsky, Dmitry; Ito, Tsuyoshi

Main reference D. Gavinsky, T. Ito, “Quantum Fingerprints that Keep Secrets,” arXiv:1010.5342v1 [quant-ph]

URL <http://arXiv.org/abs/1010.5342>


We consider the task of quantum fingerprinting (Buhrman, Cleve, Watrous, and de Wolf 2001) with an additional cryptographic requirement; namely, we require that if a fingerprint state is received by a malicious party, Eve, she cannot use the state to extract much classical information about the message. We show that there exists a fingerprinting scheme which encodes an n -bit classical message into an $O(\log n)$ -qubit fingerprint state such that

1. (Correctness) From two fingerprint states, one can decide whether they are made from the same message or not with error ε constant < 1 .
2. (Hiding property) The accessible information in the fingerprint state about the message is at most a constant independent of n or ε .
3. (Efficient construction) Construction is probabilistic, using $\text{poly}(n)$ bits of randomness, but these random bits are not required to be kept secret.

We also show a variation of this construction for equality testing in one-way communication model, where both the error probability and the accessible information tend to 0 as n tends to infinity.

3.13 Complexity implications of quantum field theory

Stephen P. Jordan (NIST – Gaithersburg, US)


License  Creative Commons BY-NC-ND 3.0 Unported license
© Stephen P. Jordan

Joint work of Jordan, Stephen P.; Lee, Keith S. M.; Preskill, John

The field of post-quantum cryptography is based on the assumption that the set of efficiently decidable problems is BQP. However, BQP is derived from the quantum circuit model, which is based on physics as we understood it in the 1930s. Today, our best physical model is the Standard Model of particle physics, which is a relativistic quantum field theory. Relativistic quantum field theories are defined using a formalism different from that used to define the quantum circuit model, and they exhibit new phenomena, such as particle creation, as well as new problems, such as renormalizability and continuum limits. Thus, it is necessary to carefully examine whether quantum field theories give rise to computational power beyond the standard quantum circuit model. We provide some evidence in the negative, showing that a certain quantum field theory (massive phi-fourth theory) can be efficiently simulated by standard quantum computers.

3.14 Simplified instantaneous non-local quantum computation with applications to position-based cryptography

Robert Koenig (IBM TJ Watson Research Center, US)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Robert Koenig

Joint work of Beigi, Salman; Koenig, Robert

Main reference S. Beigi, R. Koenig, “Simplified instantaneous non-local quantum computation with applications to position-based cryptography,” *New Journal of Physics* 13 (2011), 093036, arXiv:1101.1065v3 [quant-ph]

URL <http://arxiv.org/abs/1101.1065v3>





Instantaneous measurements of non-local observables between space-like separated regions can be performed without violating causality. This feat relies on the use of entanglement. Here we propose novel protocols for this task and the related problem of multipartite quantum computation with local operations and a single round of classical communication. Compared to previously known techniques, our protocols reduce the entanglement consumption by an exponential amount. We also prove a linear lower bound on the amount of entanglement required for the implementation of a certain non-local measurement. These results relate

to position-based cryptography: an amount of entanglement scaling exponentially in the number of communicated qubits is sufficient to render any such scheme insecure.

Furthermore, we show that certain schemes are secure under the assumption that the adversary has less entanglement than a given linear bound and is restricted to classical communication.

3.15 State-of-the-art branchless techniques for elliptic curve scalar multiplication

Tanja Lange (Technische Universiteit Eindhoven, NL)





License     Creative Commons BY-NC-ND 3.0 Unported license
© Tanja Lange

URL <http://hyperelliptic.org/tanja/vortraege/11/blackboard/images.html>

Researchers on elliptic-curve cryptography have investigated uniform branchless computations to avoid side-channel attacks and to make better use of SIMD instructions on modern CPUs. This talk surveys some of these techniques including our high-speed high-security elliptic curve signatures scheme Ed25519. The motivation to give this talk for this audience is that the same ideas should help to speed up breaking the ECDLP on a quantum computer

3.16 Techniques for quantum circuit optimization

Dmitri Maslov (NSF – Arlington, US)

License     Creative Commons BY-NC-ND 3.0 Unported license
© Dmitri Maslov

Joint work of Golubitsky, Oleg; Maslov, Dmitri





Main reference O. Golubitsky, D. Maslov, “A Study of Optimal 4-bit Reversible Toffoli Circuits and Their Synthesis,” IEEE Transactions on Computers, in print. arXiv:1103.2686

URL <http://arxiv.org/abs/1103.2686>

I will briefly discuss some known circuit optimization techniques and then concentrate on the in-depth analysis of the peep-hole optimization technique. In particular, I will discuss the efficient ways of synthesizing and accessing minimized/optimal implementations of small functions, illustrated with the optimal synthesis of any given and all 4-bit reversible functions. This presentation is based on the results reported in arXiv:1103.2686.

3.17 Decoding random linear codes in $\tilde{O}(2^{0.054n})$

Alexander May (Ruhr-Universität Bochum, DE)

License     Creative Commons BY-NC-ND 3.0 Unported license
© Alexander May

Joint work of May, Alexander; Meurer, Alexander; Thomae, Enrico

Main reference Alexander May, Alexander Meurer, Enrico Thomae, “Decoding Random Linear Codes in $\tilde{O}(2^{0.054n})$,” In Advances in Cryptology (Asiacrypt 2011), Lecture Notes in Computer Science, Springer-Verlag, 2011.

URL http://dx.doi.org/10.1007/978-3-642-25385-0_6

Decoding random linear codes is a fundamental problem in complexity theory and lies at the heart of almost all code-based cryptography. The best attacks on the most prominent


code-based cryptosystems such as McEliece directly use decoding algorithms for linear codes. The asymptotically best decoding algorithm for random linear codes of length n was for a long time Stern's variant of information-set decoding running in time $\tilde{O}(2^{0.05563n})$.

Recently, Bernstein, Lange and Peters proposed a new technique called *Ball-collision decoding* which offers a speed-up over Stern's algorithm by improving the running time to $\tilde{O}(2^{0.05558n})$.

In this work, we present a new algorithm for decoding linear codes that is inspired by a representation technique due to Howgrave-Graham and Joux in the context of subset sum algorithms. Our decoding algorithm offers a rigorous complexity analysis for random linear codes and brings the time complexity down to $\tilde{O}(2^{0.05363n})$.

3.18 The McEliece cryptosystem resists quantum Fourier sampling attacks

Cris Moore (University of New Mexico – Albuquerque, US)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Cris Moore


Joint work of Dinh, Hang; Russell, Alex

Since Shor's algorithm breaks RSA cryptography, it makes sense to look for post-quantum cryptosystems: cryptosystems that can be carried out with classical computers today, but which will remain secure even if and when quantum computers are built.

In this talk I will give an introduction to the McEliece and Niederreiter public-key cryptosystems, which are based on error-correcting codes, and argue that they are possible candidates for post-quantum cryptography. Specifically, I will show that they are immune to quantum algorithms based on the natural reduction to the Hidden Subgroup Problem, where we construct a coset state and perform strong Fourier sampling on it. This does not rule out other quantum (or classical) attacks on these systems, but it suggests that additional algorithmic ideas would be needed to break them.

3.19 Proof of plaintext knowledge for code-based cryptosystems


Kirill Morozov (Kyushu University, JP)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Kirill Morozov

We present a zero-knowledge (ZK) proof of plaintext knowledge for the code-based McEliece and Niederreiter public-key encryption schemes. It applies to both their original and randomized (IND-CPA) versions. Our proof uses Stern's ZK identification scheme.

3.20 What can you hide in qutrit chains?

Daniel Nagaj (Slovak Academy of Sciences – Bratislava, SK)


License  Creative Commons BY-NC-ND 3.0 Unported license
© Daniel Nagaj

Joint work of Caha, Libor; Bravyi, Sergey; Nagaj, Daniel

Instead of looking at QMA-completeness of problems involving chains of high dimensional qudits, we ask whether we could encode interesting problems in a chain of low-dimensional particles. We simplify the question, focusing on translationally invariant systems of qutrits in 1D with nearest neighbor interactions (projector terms), asking whether they are unfrustrated, i.e. whether there exists a state satisfying all of the local conditions (annihilated by all of the local terms). We present an interesting system with a unique ground state which is rather entangled, but still has a polynomial gap in the energy spectrum. It differs significantly from the usual history-state construction used in QMA-completeness results, and is related to a language of properly bracketed expressions.

3.21 Quantum algorithms for the hidden shift problem of Boolean functions

Maris Ozols (University of Waterloo, CA)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Maris Ozols

Joint work of Ozols, Maris; Roetteler, Martin; Roland, Jeremie


Main reference M. Ozols, M. Roetteler, J. Roland, “Quantum rejection sampling,” arXiv:1103.2774v3 [quant-ph]

URL <http://arxiv.org/abs/1103.2774v3>

We discuss several quantum algorithms for attacking the following problem: given oracle access to $f(x + s)$ where $f(x)$ is a known Boolean function, determine the hidden shift s . One of our approaches is a new quantum state generation technique—quantum rejection sampling. We use semidefinite programming to express the query complexity of our algorithm in terms of “water-filling” properties of the Fourier spectrum of f .

3.22 Self-testing for sequential CHSH games

Ben Reichardt (University of Waterloo, CA)


License  Creative Commons BY-NC-ND 3.0 Unported license
© Ben Reichardt

Joint work of Reichardt, Ben; Unger, Falk; Vazirani, Umesh

By collecting statistics on sequential CHSH games, we can gain confidence that the provers are playing according to an ideal strategy.

3.23 Quantum adversary lower bounds by polynomials

Jeremie Roland (Université Libre de Bruxelles, BE)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Jeremie Roland


Joint work of Magnin, Loïck; Roland, Jeremie

The polynomial method and the adversary method are the two main techniques to prove lower bounds on quantum query complexity, and they have so far been considered as unrelated. Here, we show an explicit reduction from the polynomial method to the multiplicative adversary method. The proof goes by introducing a new type of adversary method, which generalizes the polynomial method. We then show that this adversary bound can be obtained from the multiplicative adversary bound by taking the limit $c \rightarrow \infty$, where $c > 1$ is the maximum factor by which the adversary progress function can increase after each query.

Interestingly, it is also known that the additive adversary method can be obtained from the multiplicative method by taking the limit $c \rightarrow 1$, and this new result therefore provides a clear picture of the relation between the different lower bound methods. It also gives new hope to prove lower bounds on variations of problems such as *collision* and *ED*, for which the only known lower bounds are proved by the less flexible polynomial method.

3.24 Improvements on circuit lattices

Igor A. Semaev (University of Bergen, NO)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Igor A. Semaev





Circuit Lattice (CL) is a hardware tool for solving sparse Boolean equations. That is where the number of variables in each particular equation is bounded, though the overall number of variables is large. One introduces a guess on some variables and the device signals out whether it is wrong. CL may be constructed as a combination of wires and switches(transistors) on a semiconductor crystal and used for key search by bruit force in cryptanalysis. In contrast to a conventional computer, the transistors are not necessarily synchronized.

By gluing some of the cipher initial equations one may produce, at the expense of enlarging the number of local solutions to particular equations, a system with a reduced key search space. Now it is unlikely to implement CL for that on one semiconductor crystal. So whether the parallelism of quantum computing may replace electric potential expansion in CL is an interesting question.

In this talk I plan to explain some recent improvements to Circuit Lattices as reducing the number of required transistors and its new architecture more suitable for implementing by modern computer industry.

3.25 On the hidden shifted power problem

Igor Shparlinski (Macquarie University – Sydney, AU)

License     Creative Commons BY-NC-ND 3.0 Unported license
© Igor Shparlinski

Joint work of Bourgain, Jean; Konyagin, Sergei; Shparlinski, Igor





We consider the problem of recovering a hidden element s of a finite field \mathbb{F}_q of q elements from queries to an oracle that for a given $x \in \mathbb{F}_q$ returns $(x + s)^e$ for a given divisor $e \mid q - 1$. This question is motivated by some applications to pairing based cryptography.

Using Largange interpolation one can recover s in time $ep^{o(1)}$ on a classical computer. In the case of $e = (q - 1)/2$ an efficient quantum algorithm has been given by W. van Dam, S. Hallgren and L. Ip.

We describe some techniques from additive combinatorics and analytic number theory that lead to more efficient classical algorithms than the naive interpolation algorithm, for example, they use substantially fewer queries to the oracle. We formulate some questions and discuss whether quantum algorithms can give further improvement.

3.26 The garden-hose game and application to position-based cryptography

Florian Speelman (CWI – Amsterdam, NL)

License     Creative Commons BY-NC-ND 3.0 Unported license
© Florian Speelman

Joint work of Buhrman, Harry; Fehr, Serge; Schaffner, Christian; Speelman, Florian

Main reference H. Buhrman, S. Fehr, C. Schaffner, F. Speelman, “The Garden-Hose Game: A New Model of Computation, and Application to Position-Based Quantum Cryptography,” arXiv:1109.2563v2 [quant-ph]





URL <http://arxiv.org/abs/1109.2563v2>

We study position-based cryptography in the quantum setting. We examine a class of protocols that only require the communication of a single qubit and $2n$ bits of classical information. To this end, we define a new model of communication complexity, the garden-hose model, which enables us to prove upper bounds on the number of EPR pairs needed to attack such schemes.

This model furthermore opens up a way to link the security of quantum position-based cryptography to traditional complexity theory.

3.27 Certifiable quantum dice

Thomas Vidick (University of California – Berkeley, US)

License     Creative Commons BY-NC-ND 3.0 Unported license
© Thomas Vidick

Joint work of Vazirani, Umesh; Vidick, Thomas

We introduce a protocol through which a pair of quantum mechanical devices may be used to generate n bits of true randomness from a seed of $O(\log n)$ uniform bits. The bits generated are certifiably random based only on a simple statistical test that can be performed by the user, and on the assumption that the devices obey the no-signaling principle. No other assumptions are placed on the devices’ inner workings. A modified protocol uses a seed of

$O(\log^3 n)$ uniformly random bits to generate n bits of true randomness even conditioned on the state of a quantum adversary who may have had prior access to the devices, and may be entangled with them.

Participants

- Daniel J. Bernstein
University of Chicago, US
- Anne Broadbent
University of Waterloo, CA
- Harry Buhman
CWI – Amsterdam, NL
- Andrew Childs
University of Waterloo, CA
- Matthias Christandl
ETH Zürich, CH
- Roger Colbeck
Perimeter Inst. – Waterloo, CA
- Serge Fehr
CWI – Amsterdam, NL
- Dmitry Gavinsky
NEC Laboratories America, Inc.
– Princeton, US
- Sean Hallgren
Penn State University, US
- Aram W. Harrow
University of Washington, US
- Avinathan Hassidim
MIT – Cambridge, US
- Peter Hoyer
University of Calgary, CA
- Tsuyoshi Ito
University of Waterloo, CA
- Stacey Jeffery
University of Waterloo, CA
- Stephen P. Jordan
NIST – Gaithersburg, US
- Robert Koenig
IBM TJ Watson Res. Center, US
- Tanja Lange
TU Eindhoven, NL
- Frédéric Magniez
University Paris-Diderot, FR
- Loïck Magnin
University Paris-Diderot, FR
- Dmitri Maslov
NSF – Arlington, US
- Alexander May
Ruhr-Universität Bochum, DE
- Cris Moore
University of New Mexico –
Albuquerque, US
- Kirill Morozov
Kyushu University, JP
- Michele Mosca
University of Waterloo, CA
- Daniel Nagaj
Slovak Academy of Sciences –
Bratislava, SK
- Maris Ozols
University of Waterloo, CA
- Anupam Prakash
University of California –
Berkeley, US
- Ben Reichardt
University of Waterloo, CA
- Martin Rötteler
NEC Laboratories America, Inc.
– Princeton, US
- Jérémie Roland
Université Libre de Bruxelles, BE
- Alexander Russell
University of Connecticut –
Storrs, US
- Leonard J. Schulman
CalTech – Pasadena, US
- Igor A. Semaev
University of Bergen, NO
- Igor Shparlinski
Macquarie Univ.- Sydney, AU
- Rolando Somma
Los Alamos National Lab., US
- Florian Speelman
CWI – Amsterdam, NL
- Rainer Steinwandt
Florida Atlantic University –
Boca Raton, US
- Barbara Terhal
RWTH Aachen, DE
- Wim van Dam
University of California – Santa
Barbara, US
- Thomas Vidick
University of California –
Berkeley, US
- Arne Winterhof
RICAM – Linz, AT

