Quantum algorithms for analysis of public-key crypto

organized by
Daniel J. Bernstein, Dan Boneh, Tanja Lange, and Michele Mosca

Workshop Summary

Summary of goals. The aim of this workshop was to establish a more intensive collaboration between mathematicians working on designing and analyzing public-key cryptosystems and computer scientists working on quantum algorithms. Bringing together this expertise is essential to ensure that current proposals in post-quantum cryptography, an area working on alternatives to cryptography based on factorization and discrete logarithms with the aim to find algorithms that withstand attacks by quantum computers, actually get analyzed with the full power of both fields.

Organization overview. The workshop was attended by 29 researchers from academia and industry, from the US, Canada, and some European countries. The participants were chosen to include researchers with expertise in post-quantum cryptography and researchers with expertise in quantum algorithms.

Each day started with plenary presentations. The afternoons were reserved for discussions, collection of problems, and collaborative work. For full details on the talks incl. slides from the talks and supplemental material see the https://pqcrypto.org/2019-aim.htmlworkshop page.

Schedule of plenary talks.

Monday 4 February:
Tanja Lange on post-quantum cryptography
Michele Mosca on quantum algorithms
Tuesday 5 February:
Elena Kirshanova on lattices
Daniel J. Bernstein on quantum walks
John Schanck on exact quantum cryptanalysis
Wednesday 6 February:
Kirsten Eisentraeger on quantum algorithms to find unit groups
Greg Kuperberg on hidden-shift algorithms
Thursday 7 February:
Lorenz Panny on isogenies
Gretchen Matthews on algebraic-geometry codes
Friday 8 February:
Matthew Amy on optimizing quantum circuits
Shi Bai on attacks

Working groups. Some open problems were collected before the beginning of the workshop. Monday afternoon provided a major push in collecting and organizing them. The problems can be categorized into

(1) Codes
(2) Competing with Grover's algorithm
(3) Concrete Costs
(4) Hidden Shift
(5) Isogeny-based cryptosystems
(6) Miscellaneous

Details are available at http://aimpl.org/quantumalg/AIM's problem page. For ease of reference they are included at the end of this report.

The organizers selected some topics and followed the AIM voting procedure to form working groups. During the week the following topics were covered. Participants were free to move between working groups, so the work reported here is the result of many people; some scientific papers are on the way. The summaries below are based on the group reports and the personal participation of the workshop organizers in the different working groups.

Attacks against lattice-based systems. This working group tried to tackle the holy grail problem of finding subexponential (quantum) attacks against lattice-based systems. To make this goal more realistic, some special lattice-based proposals (NTRU, Ring-LWE, ...) were considered, where the mathematical structure offers some more attack surface.

A different approach considered was to complete the picture of relations between the well-studied lattice problems; problems considered include DCP, LWE, EDCP, ...

Information-set decoding in rank metric. A relatively recent class of code-based systems are based on codes in the rank metric. This working group started with the target of transferring some of the improvements to information-set decoding in the Hamming metric to equivalent algorithms in the rank metric. Most of this area is not well studied and no specific quantum algorithms are known, hence, both classical and quantum algorithms were discussed.

This working group also looked at the general security of some of the NIST submissions in this area and noticed several omissions in the documentation.

Analysis of Kuperberg's algorithm and simulator. Kuperberg published two papers showing how to solve the hidden-shift problem in subexponential time using a quantum computer. During the week major progress was made in establishing the exact constants in the exponent of the complexity and in analyzing how the algorithms and the complexity analysis change depending on the group structure. At the end of the week some participants had implemented Kuperberg's second algorithm in a simulator. There still remain many open problems in the analysis, e.g., the analysis of lower-order terms in the complexity and figuring out how the algorithm behaves if some of the inputs are incorrect.

Attacks using image points in SIDH. SIDH stands for supersingular isogeny Diffie-Hellman, which is a system using isogenies between elliptic curves over finite fields to build a key exchange system. The system is broken if an attacker can find an efficient isogeny between two given curves. However, the attacker has more information than just curves E_0 and E_1 which he knows to be isogenous. Namely, the attacker knows that the secret isogeny ϕ has degree 2^n for some known n and he knows the image of two given points P, Q of order

3^m under ϕ. These image points have raised concern for the security of the system and the working group investigated several avenues of using them in attacks, including quantum attacks.

Open problems

Coding

[Edoardo Persichetti] Parameters: $n \geq 1$, $r \geq 1$, $\mathbf{F}_{q^m}$, $t \geq 1$. How quickly can we find $v \in \mathbf{F}_{q^m}^n$ with $Hv = s$ and $\mathrm{wt}(v) = t$, given $H \in \mathbf{F}_{q^m}^{r \times n}$ and $s \in \mathbf{F}_{q^m}^r$?
Here, $\mathrm{wt}(v)$ is defined to be the rank of the v, viewed as a matrix with n columns.

[Tanja Lange] Given a parity-check matrix H, find the hidden Goppa code in H. How quickly can we decode H, assuming Goppa decoder for H exists?

What witnesses are there of Goppa decodability or non-decodability?

Competing with Grover's algorithm

[Mike Hamburg] Given a function $f : \{0,1\}^n \to \{0,1,2\}$, find $x \in \{0,1\}^n$ to maximize $f(x)$. Measure average resulting $f(x)$ if, e.g., f has one 1, one 2, and all other values 0. Or consider the function $f : \{0,1\}^n \to \{0,1,2,\ldots,1000\}$. Or consider f which is i.i.d.

Is it possible to do better than Grover search for x such that $f(x) \geq T$ for threshold T?

[Mike Hamburg] Find x, y distinct with $f(x) = f(y) = 1$. Consider the case where there are many solutions at low density. How quickly can this be done? Faster than Grover?

More generally, find distinct $x_1, \ldots, x_m$ such that $f(x_1) = \cdots = f(x_m) = 1$. Can you do better than m preimage searches?

Concrete Costs

[Greg Kuperberg] Given: $x_0, \ldots, x_{2^n-1} \in \{0,1\}$. What is the real-world cost of

$$|i_1, \ldots, i_{n-1}, a\rangle \mapsto |i_1, \ldots, i_{n-1}, a \oplus x_i\rangle$$

where $i = i_0 + 2i_1 + \cdots + 2^{n-1}i_{n-1}$.

Can error correction be done efficiently for this problem?

[Shi Bai] What are the concrete costs of quantum sieving and quantum enumeration within BKZ? Go beyond asymptotics.

Hidden Shift

How fast are approximate SVP attacks via hidden shift algorithms?

How much noise is tolerated in hidden shift algorithms? Consider too many solutions vs. too few.

[Greg Kuperberg] Is there a fast hidden shift algorithm for Heisenberg group over $\mathbb{F}_p$?

Remark. HSP is known. [Tanja Lange] What is the cost of hidden shift on $\mathbf{Z}$ where the shift $s \in [a, b]$, under binary cost of oracle?

[Greg Kuperberg] Hidden shift on $\mathbf{Z}^d$ where f_0 and f_1 are periodic under unary oracle cost.

[Elena Kirshanova] How does Kuperberg's algorithm behave under multiple hidden shifts (with known relations between shifts, e.g. arithmetic progression) with Gaussians, using the work of Ivanyos, Prakash, and Santha?

Isogeny-based cryptosystems

[Kirsten Eisentraeger] Can quantum algorithms be used to attack SIDH by using the extra points? Are there SIDH attacks better than claw-finding?

[Lorenz Panny] Are there CSIDH attacks better than hidden shift? What is the cost of the hidden shift attack?

[Dan Boneh] Solve Decisional Diffie-Hellman (DDH) in the context of CSIDH: Let E_0 be a supersingular elliptic curve defined over $\mathbf{F}_p$ with endomorphism ring $\mathbf{Z}[\pi]$. Distinguish between triples $(\mathfrak{a} * E_0, \mathfrak{b} * E_0, \mathfrak{c} * E_0)$ and triples $(\mathfrak{a} * E_0, \mathfrak{b} * E_0, \mathfrak{ab} * E_0)$ where $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ are ideals in $\mathbf{Z}[\pi]$ of odd norm.

Miscellaneous

[John Schanck] $n \geq 2$ and $\alpha > 0$. Given independent uniformly random $x_1, x_2, \cdots \in S^{n-1} = \{v \in \mathbf{R}^n : \|v\|_2 = 1\}$, how quickly can we find a subsequence that covers S^{n-1}? (Here, "covers" means that every point of S^{n-1} is within angle α of a point in the subsequence.) For example, consider the case when $n = 1000$ and $\alpha = 75°$.

[Michele Mosca] Does HHL break crypto? (See recent papers https://arxiv.org/abs/1802.038561802.03856 and https://arxiv.org/abs/1712.062391712.06239.)
Understand condition number over $\mathbf{C}$ of matrix of coefficients of $f_1, f_2, \ldots$ (original equations), $xf_1, xyf_2, \ldots$ (only monomial terms).

[Greg Kuperberg] Is there a crypto problem that is solved by Simon's algorithm without superposition attackers? Which hidden subgroup problems have crypto applications? Or non-crypto instances?

Remark. "Instance": e.g. algorithm for $x \mapsto 2^x \bmod n$ in Shor's algorithm.

[Dan Bernstein] Compute short units in the ring of integers of $\mathbf{Q}[x]/(x^{312} - x^{156} - 1)$. How short can they be, and how fast can you find them?