Aalto University
School of Science

Quantum and post-quantum cryptography

Nikita Machine (nikita.machine@aalto.fi)
Department of Computer Science, Aalto University

1 Introduction

Cryptography is a subfield of mathematics and computer science concerned with achieving the following in digital communications:

- **Confidendiality**: ensuring that only the intended party can read your messages.
- **Integrity**: ensuring that third parties cannot modify messages that have been sent to you without being discovered.
- **Authenticity**: ensuring that a party sending you messages is who they claim to be.

Typically, cryptographic protocols are based on the assumed hardness of some mathematical problem. A popular choice is the discrete logarithm problem, where given $q \in \mathbb{Z}$ and $g, h \in \mathbb{Z}/q\mathbb{Z}$, you must find a such that:

$$g^a = h \pmod{q}$$

Some problems which are plausibly hard for classical computers are however efficiently solvable by quantum computers, including the discrete logarithm problem [Sho94]. While we do not yet have practical quantum computers, there is some concern that we are not adequately prepared for a future in which we do. As such, there is interest both in:

- **Post-quantum cryptography**: classical cryptography that is resilient against quantum attackers.
- **Quantum cryptography**: cryptography using quantum computers to achieve things not possible in classical cryptography.

2 Lattice-based cryptography

Lattice-based cryptography is an area of cryptography based on assumed hard problems over lattices. An important problem is SVP, which asks to find the shortest non-zero vector in a lattice given a basis for it. SVP is known to be NP-hard [Ajt96] and is therefore likely hard also for quantum computers.

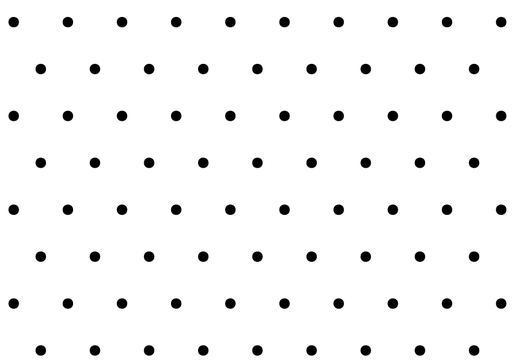

Figure 1: an example of a trivial lattice.

SVP gives rise to other lattice-based problems such as SIS and LWE, which have been used to construct cryptographic primitives such as hash functions [GGH00], encryption [Reg09], and signatures [GPV08], among others.

In addition to developing new protocols, my research will cover cryptanalysis of cryptographic protocols based on less well-accepted assumptions (such as NTRU) as well as considering reductions between and attacks against assumed quantum-hard problems.

3 Quantum money

Quantum money is an example of a quantum primitive that does not have a classical equivalent. A quantum money protocol consists of two procedures:

- `Gen`: which takes a security parameter 1^λ produces a quantum banknote $|\psi\rangle$ with classical serial number σ.
- `Ver`: which, given a quantum banknote $|\psi\rangle$ and classical serial number σ, outputs a bit depending on whether $|\psi\rangle$ corresponds to σ.

With the security requirement being that no BQP adversary can, given $(|\psi\rangle, \sigma \leftarrow \texttt{Gen}(1^\lambda))$, produce a second state $|\phi\rangle$ such that $\texttt{Ver}(|\phi\rangle, \sigma) = \texttt{Ver}(|\psi\rangle, \sigma) = 1$ [Wie83].

Such a notion cannot be achieved classically because all classical data can freely be copied. Thus, given some value x you can create as many copies of x as you like. This is not the case in the quantum world due to the *no-cloning* theorem, which states that there are no $U \in \mathrm{U}(\mathcal{H}^{\otimes 2}), |\phi\rangle \in \mathcal{H}$ such that:

$$U(|\psi\rangle|\phi\rangle) = |\psi\rangle|\psi\rangle$$

for arbitrary states $|\psi\rangle$. Essentially, this theorem states that there is no possible way to copy unknown quantum states, which is what makes quantum money unforgeability possible.
Quantum money is so-called because it can be used for a digital currency scheme that is very similar to physical currency, wherein:

- There is a central mint responsible for producing new banknotes.
- Mere possession implies ownership of a banknote.
- Transactions only involve physically exchaning banknotes.

Quantum money and related primitives also have applications beyond their use as currency. For instance: a strenghtening of quantum money called *quantum lightning* can be used to generate random numbers along with proofs that they are indeed random [Zha19].

4 Pseudorandom states and unitaries

Quantum computers are capable of generating truly random classical strings. However, there is also interest in producing quantum states and unitaries that are indistinguishable from random [JLS18]:

- **Pseudorandom states (PRSs):** efficiently-generable quantum states such that polynomially many copies of a random of a PRS are indistinguishable from as many copies of a Haar random state.
- **Pseudorandom unitaries (PRUs):** efficiently-generable quantum unitaries such that given access to polynomially many queries to either a PRU or a Haar random unitary, the two are indistinguishable.

Interestingly, neither PRSs nor PRUs imply the existence of classical one-way functions [Kre21]. Even more interestingly, they have been shown to be sufficient for constructing Minicrypt cryptographic primitives such as commitments and symmetric encryption [Ana+22].

References

[Ajt96] M. Ajtai. "Generating hard instances of lattice problems (extended abstract)". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, pp. 99–108. ISBN: 0897917855. DOI: 10.1145/237814.237838. URL: https://doi.org/10.1145/237814.237838.

[Ana+22] Prabhanjan Ananth et al. "Pseudorandom (Function-Like) Quantum State Generators: New Definitions and Applications". In: *Theory of Cryptography*. Ed. by Eike Kiltz and Vinod Vaikuntanathan. Cham: Springer Nature Switzerland, 2022, pp. 237–265. ISBN: 978-3-031-22318-1.

[GGH00] Oded Goldreich, Shafi Goldwasser, and Shai Halevi. "Collision-Free Hashing from Lattice Problems". In: *Lecture Notes in Computer Science* (Feb. 2000). DOI: 10.1007/978-3-642-22670-0_5.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. "Trapdoors for hard lattices and new cryptographic constructions". In: vol. 14. May 2008, pp. 197–206. DOI: 10.1145/1374376.1374407.

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. "Pseudorandom Quantum States". In: *Advances in Cryptology – CRYPTO 2018*. Ed. by Hovav Shacham and Alexandra Boldyreva. Cham: Springer International Publishing, 2018, pp. 126–152. ISBN: 978-3-319-96878-0.

[Kre21] William Kretschmer. "Quantum Pseudorandomness and Classical Complexity". In: *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*. Ed. by Min-Hsiu Hsieh. Vol. 197. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021, 2:1–2:20. ISBN: 978-3-95977-198-6. DOI: 10.4230/LIPIcs.TQC.2021.2. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.TQC.2021.2.

[Reg09] Oded Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *J. ACM* 56.6 (Sept. 2009). ISSN: 0004-5411. DOI: 10.1145/1568318.1568324. URL: https://doi.org/10.1145/1568318.1568324.

[Sho94] Peter W. Shor. "Algorithms for quantum computation: Discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[Wie83] Stephen Wiesner. "Conjugate coding". In: *SIGACT News* 15.1 (Jan. 1983), pp. 78–88. ISSN: 0163-5700. DOI: 10.1145/1008908.1008920. URL: https://doi.org/10.1145/1008908.1008920.

[Zha19] Mark Zhandry. "Quantum Lightning Never Strikes the Same State Twice". In: Apr. 2019, pp. 408–438. ISBN: 978-3-030-17652-5. DOI: 10.1007/978-3-030-17659-4_14.