Challenges in Post-Quantum Security Reductions

Patrick Struck
Technische Universität Darmstadt, Germany

29th Crypto Day, 6/7 September 2018

1 Preliminaries

Post-Quantum Cryptography. Due to the quantum algorithm for factoring integers by Shor [2], the field of post quantum cryptography arose. The name is be a bit misleading as it is actually classical, i.e. non-quantum, cryptography. However, it is based on hardness assumptions assumed to be secure once large quantum computers exist, e.g the learning with errors (LWE) problem.

Quantum Computation. In classical computation, we use bits to store information. A bit can either be 0 or 1. In quantum computation, information is stored in quantum bits (short: qubits). These are typically written in Dirac notation $|0\rangle$ and $|1\rangle$, the quantum analog to 0 and 1.

What makes quantum computation more powerful, is that a qubit is not limited to be either $|0\rangle$ or $|1\rangle$. Instead, it can be in a *superposition* of these. For instance the qubit $|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ is $|0\rangle$ and $|1\rangle$ at the same time. Another important aspect of quantum computation is the *no-cloning* theorem which states that an arbitrary superposition can not be copied.

Security Reductions. Security reductions are a common technique to prove the security of cryptographic schemes. In more detail, one tries to prove that a scheme is secure under the assumption that a certain problem P is hard to solve. This is proven by contradiction. We assume an hypothetical black-box adversary $\mathcal{A}$ against the scheme. Then we construct an algorithm $\mathcal{R}$ which solves problem P by using the adversary $\mathcal{A}$ as a subroutine which contradicts our assumption that P is hard to solve.

The (Quantum) Random Oracle Model. Many cryptographic schemes are proven secure in the so-called *random oracle model* (ROM). In this model, everyone, including the adversary, has access to a random oracle. Each time the random oracle is queried on a message, it checks whether it has already been queried on this message. If not, it returns a value sampled at random, otherwise, it returns the same value as done during the last query. As pointed out by Boneh et al. [1], for a quantum algorithm we need to use the *quantum random oracle model* (QROM), in which the random oracle can be queried on a superposition of inputs.

crypto day matters 29 (2018)
Beiträge vom 29. Krypto-Tag, 06.-07.09.2018, Bosch, Renningen.
doi:10.18420/cdm-2018-29-03

2 Challenges

In the following, we briefly describe some challenges that arise in security proofs in the QROM.

Oracle Simulation. In the ROM, the random oracle is typically generated on-the-fly, i.e. for each query, a new random value is sampled. This works, as for each new query, one random value has to be sampled. In the QROM, however, the adversary can query the random oracle on a superposition of all possible input in one query. This would require to sample exponentially many random values at once, which is not possible for the reduction. This issue can be solved using quantum secure pseudorandom functions [1] or q-wise independent functions [4].

Challenge Injection. Another common technique for the reduction is the injection of its own challenge to the random oracle. This is done by choosing a query by the adversary randomly and returning its own challenge, instead of a randomly sampled value. There is a significant chance that the adversary will use this injected challenge when breaking the scheme. In the QROM this simple idea does not work. Consider an adversary who queries the random oracle always on a superposition of all inputs. Then the output should be always the same, hence the adversary might notice that a challenge is injected. In the QROM, a challenge can be injected using so-called *semi constant distributions* [4], where the challenge is injected into a small but significant subset of all inputs.

Rewinding. Rewinding is a technique in which the adversary, after generating an output, is set to a previous (intermediate) state and executed again to obtain a different output. The important part is that the state of the adversary in both executions is equal up to the rewinding point. Rewinding in the QROM requires to copy the (quantum) state of the adversary. However, this is impossible due to the no-cloning theorem. Unfortunately, there is no simple workaround for this yet.

Oracle Reprogramming. The idea behind oracle reprogramming is to run the adversary up to a certain point, then reprogram the random oracle on a certain input, and continue running the adversary. The only chance for the adversary to detect a reprogramming on input x, is when he queried x before the reprogramming took place. In the ROM, the reduction sees all queries by the adversary, hence, it can reprogram the oracle on a not yet queried input. In the QROM, it is not known which values the adversary queried in superposition. Again, this follows from the no-cloning theorem, as this knowledge of the query would allow to copy the query. There are workarounds for this, e.g. by Unruh [3], which allow for some reprogramming of the random oracle. However, there is no general approach how to do this.

References

[1] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, pages 41–69, 2011.

[2] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, pages 124–134, 1994.

[3] Dominique Unruh. Revocable quantum timed-release encryption. *J. ACM*, 62(6):49:1–49:76, 2015.

[4] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, pages 758–775, 2012.