Quantum Random Oracles

(References)

Dominique Unruh

Insufficiency of classical RO. The fact that the classical RO is not a good model in the quantum case was already observed in [BDF$^+$11], using the fact that the quadratic speedup in inverting a hash function is only captured by the QRO. In [YZ20], an example protocol is given that is secure in the RO and completely insecure in the QRO (not just a quadratic gap in attack complexity).

One-wayness. Hardness of preimage-finding / one-wayness of the QRO can be shown elementarily (slight adaptation of the optimality of Grover in [NC10], for example), is shown in different variations in a number of papers, and can also be shown easily using the O2H theorem. The specific bound given in the talk follows from [HRS16, Theorem 1 in the eprint].

Collision resistance. Collision resistance of the QRO is shown in [Zha15], together with other useful properties such as the indistinguishability of a random function and a random permutation.

Replacing the oracle. The "history-free reductions" from [BDF$^+$11] essentially do what I called "replacing the oracle". [BDF$^+$11] proves several special cases of full-domain hash using this method. Oracle-indistinguishability shows that two oracles are indistinguishishable if the distributions of the individual outputs are indistinguishishable [Zha12a, Section 7 of the eprint].

One-way to hiding. The original one-way to hiding theorem was presented in [Unr15]. More advanced O2H theorem, e.g., in [AHU19].

Compressed oracles. Compressed oracles were introduced in [Zha19]. The presentation in my talk is based on the introduction from [Unr21, Section 3.1].

Further techniques. A few useful techniques that I didn't cover: Small-range distributions [Zha12a], allowing us to see the QRO as a function with small range. 2q-wise independent functions [Zha12b, Thm. 6.1 of the eprint], allowing us simulate the QRO efficiently without using computational assumptions. The "polynomial-method" and the "adversary method" are useful tools for query complexity related questions (I am not very familiar with them, one example of the polynomial method is in [Zha15]).

References

[AHU19] Andris Ambainis, Mike Hamburg, and Dominique Unruh. Quantum security proofs using semi-classical oracles. In *CRYPTO 2019*, pages 269–295. Springer, 2019. eprint `https://eprint.iacr.org/2018/904.pdf`.

[BDF$^+$11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In *Asiacrypt 2011*, pages 41–69, Berlin, Heidelberg, 2011. Springer. eprint `https://eprint.iacr.org/2010/428.pdf`.

[HRS16] Andreas Hülsing, Joost Rijneveld, and Fang Song. Mitigating multi-target attacks in hash-based signatures. In *PKC 2016, Proceedings, Part I*, volume 9614 of *LNCS*, pages 387–416. Springer, 2016. eprint is `https://eprint.iacr.org/2015/1256.pdf`.

[NC10] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 10th anniversary edition, 2010.

[Unr15] Dominique Unruh. Revocable quantum timed-release encryption. *Journal of the ACM*, 62(6):49:1–49:76, 2015. eprint `https://eprint.iacr.org/2013/606.pdf`.

[Unr21] Dominique Unruh. Compressed permutation oracles (and the collision-resistance of sponge/sha3). `https://eprint.iacr.org/2021/062.pdf`, 2021.

[YZ20] Takashi Yamakawa and Mark Zhandry. A note on separating classical and quantum random oracles. `https://eprint.iacr.org/2020/787.pdf`, 2020.

[Zha12a] Mark Zhandry. How to construct quantum random functions. In *FOCS 2013*, pages 679–687, Los Alamitos, CA, USA, 2012. IEEE Computer Society. eprint is IACR ePrint 2012/182.

[Zha12b] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In *Crypto 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, 2012. eprint is `https://eprint.iacr.org/2012/076.pdf`.

[Zha15] Mark Zhandry. A note on the quantum collision and set equality problems. *Quantum Information & Computation*, 15(7&8):557–567, 2015. eprint arXiv:1312.1027v3 [cs.CC].

[Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In *Crypto 2019*, pages 239–268. Springer, 2019. Eprint is IACR ePrint 2018/276.