Quantum Oracles for Recording Inverse Queries

Ritam Bhaumik (INRIA Paris)

Proposed talk for Journées C2, April 2022

Classical counting proofs generally rely on the *game transcript*, a list of all the queries along with the oracle responses. This is generally difficult to obtain in the quantum setting, since—among other things—measuring the shared state alters it in a way detectable by the adversary. Zhandry [Zha19] showed a new technique for recording quantum queries in a database, that can then be used in counting arguments. Hosoyamada and Iwata [HI19] adapted this technique to prove the qPRP security of 4-round Luby-Rackoff; they went on to use the same technique on HMAC/NMAC [HI21a] and a tweakable blockcipher construction [HI21b].

In this talk we explore some techniques for extending the Hosoyamada-Iwata Recording Oracle with Errors to an oracle capable of handling inverse queries in some meaningful way. We propose two oracles, both of which maintain two (possibly entangled) databases: one for forward queries and one for inverse queries. Both record the inverse of a query in either direction as follows: on the forward query of a basis state i, an oracle that returns j and records it in the first database then proceeds to XOR i to the j-th cell of the second database (initialised to 0 just like in the Hosoyamada-Iwata oracle).

The difference between the two oracles is that in the first, the recording is done in a way such that repeating the same query twice erases the recorded value in the inverse database, while in the second, an explicit state is assigned to the query number, so that erasing of the database only happens when the query number is forced to repeat.

We believe that both these oracles can be useful in certain contexts, especially in counting-based proofs involving invertible functions like blockciphers.

References

[HI19] Akinori Hosoyamada and Tetsu Iwata. 4-round luby-rackoff construction is a qprp. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part I*, volume 11921 of *Lecture Notes in Computer Science*, pages 145–174. Springer, 2019.

[HI21a] Akinori Hosoyamada and Tetsu Iwata. On tight quantum security of HMAC and NMAC in the quantum random oracle model. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I*, volume 12825 of *Lecture Notes in Computer Science*, pages 585–615. Springer, 2021.

[HI21b] Akinori Hosoyamada and Tetsu Iwata. Provably quantum-secure tweakable block ciphers. *IACR Trans. Symmetric Cryptol.*, 2021(1):337–377, 2021.

[Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 239–268. Springer, 2019.