Post-quantum Resettably-Sound Zero Knowledge

Nir Bitansky Michael Kellner Omri Shmueli

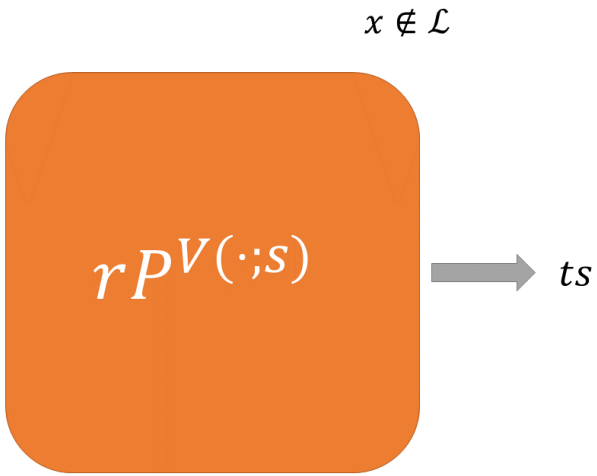
Tel-Aviv University

August 2021

Quantum Resettable Soundness

We initiate the study of Quantum Resettable Soundness

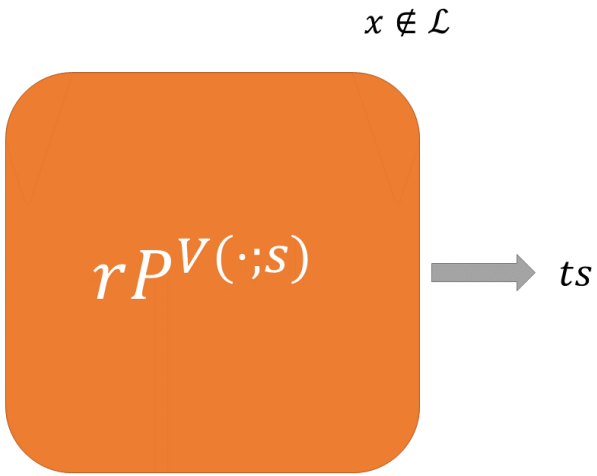
- Attackers perform *quantum* resetting attacks.



Quantum Resettable Soundness

We initiate the study of Quantum Resettable Soundness

- Attackers perform *quantum* resetting attacks.



- Motivations:
  - Achieving such a security guarantee.
  - Better understand post-quantum black-box zero knowledge.

Lower-Bounds on Post-quantum Black-Box Zero Knowledge

- Post-quantum zero knowledge protocols that are **three message or constant-round public-coin** cannot be black-box zero knowledge, except for languages in **BQP**.
  - Classical lower-bound don't extend to the quantum case - simulator has more power.

Lower-Bounds on Post-quantum Black-Box Zero Knowledge

- Post-quantum zero knowledge protocols that are **three message or constant-round public-coin** cannot be black-box zero knowledge, except for languages in **BQP**.
  - Classical lower-bound don't extend to the quantum case - simulator has more power.

Observation

If a language $\mathcal{L}$ has a post-quantum black-box zero-knowledge, resettably sound protocol, then $\mathcal{L} \in \mathbf{BQP}$.

Lower-Bounds on Post-quantum Black-Box Zero Knowledge

- Post-quantum zero knowledge protocols that are **three message or constant-round public-coin** cannot be black-box zero knowledge, except for languages in **BQP**.
  - Classical lower-bound don't extend to the quantum case - simulator has more power.

Observation

If a language $\mathcal{L}$ has a post-quantum black-box zero-knowledge, resettably sound protocol, then $\mathcal{L} \in \mathbf{BQP}$.

- Methodology - Transform protocol into resettably sound one.
  - Using measure-and-reprogram techniques (Don-Fehr-Majenz(20)[5]).

Constructing a Quantum Resettably Sound Zero Knowledge Protocol

We present a construction of a *post-quantum* resettably sound zero knowledge protocol for **NP**.

- Assumes QLWE and quantum FHE.
- The construction is constant round.
- Zero knowledge holds with regards to *quantum* verifiers.
- Starting point - The protocol of Bitansky-Shmueli(20)[4].
  - As is, protocol is not resettably sound, even classically.

From Resettable Soundness to Quantum Unobfuscatable Functions

A connection between resettable soundness and quantum VBB obfuscation.

- We show that if there exists a post-quantum resettably-sound zero-knowledge argument for **NP** and post-quantum one-way functions, then quantum VBB obfuscation is impossible.
- An analog of the classical result of Bitansky-Paneth(15)[3].

From Resettable Soundness to Quantum Unobfuscatable Functions

A connection between resettable soundness and quantum VBB obfuscation.

- We show that if there exists a post-quantum resettably-sound zero-knowledge argument for **NP** and post-quantum one-way functions, then quantum VBB obfuscation is impossible.
- An analog of the classical result of Bitansky-Paneth(15)[3].
- An alternative proof to results from Alagic-Brakerski-Dulek-Schaffner(20)[1], Ananth-La Placa(20)[2].
- Better resettably sound protocols imply better construction of unobfuscatability.

[1] G. Alagic, Z. Brakerski, Y. Dulek, and C. Schaffner. Impossibility of quantum virtual black-box obfuscation of classical circuits. *CoRR*, abs/2005.06432, 2020.

[2] P. Ananth and R. L. L. Placa. Secure software leasing. *CoRR*, abs/2005.05289, 2020.

[3] N. Bitansky and O. Paneth. On non-black-box simulation and the impossibility of approximate obfuscation. *SIAM J. Comput.*, 44(5):1325–1383, 2015.

[4] N. Bitansky and O. Shmueli. Post-quantum zero knowledge in constant rounds. In K. Makarychev, Y. Makarychev, M. Tulsiani, G. Kamath, and J. Chuzhoy, editors, *Proccedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2020, Chicago, IL, USA, June 22-26, 2020*, pages 269–279. ACM, 2020.

[5] J. Don, S. Fehr, and C. Majenz. The measure-and-reprogram technique 2.0: Multi-round fiat-shamir and more. In D. Micciancio and T. Ristenpart, editors, *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III*, volume

12172 of *Lecture Notes in Computer Science*, pages 602–631. Springer, 2020.