Composable Oblivious Pseudo-Random Functions via Garbled Circuits

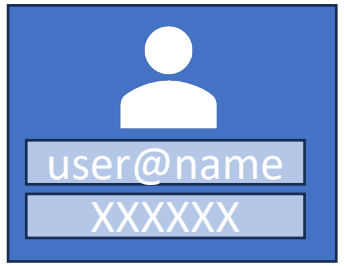
Sebastian Faller[1,2], Astrid Ottenhues[3,4], and Johannes Ottenhues[5]

[1]IBM Research Zurich, [2]ETH Zurich, [3]KASTEL Security Research Labs, [4]Karlsruhe Institute of Technology, [5]University of St. Gallen

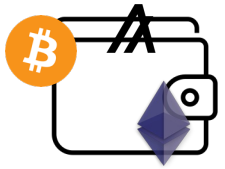
Password breaches are ubiquitous

Cryptography has good solutions for this!

- OPAUQA: Password-Authenticated Key Exchange



- Password-Protected Secret Sharing



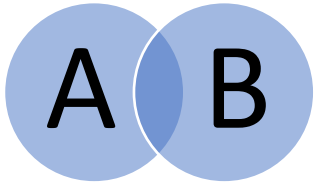
- Password-Protected Chat Backups

They all use oblivious pseudo-random functions!

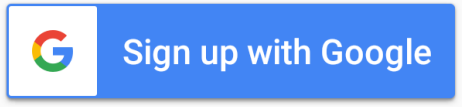
Oblivious pseudo-random functions have even more applications

- Privacy Pass

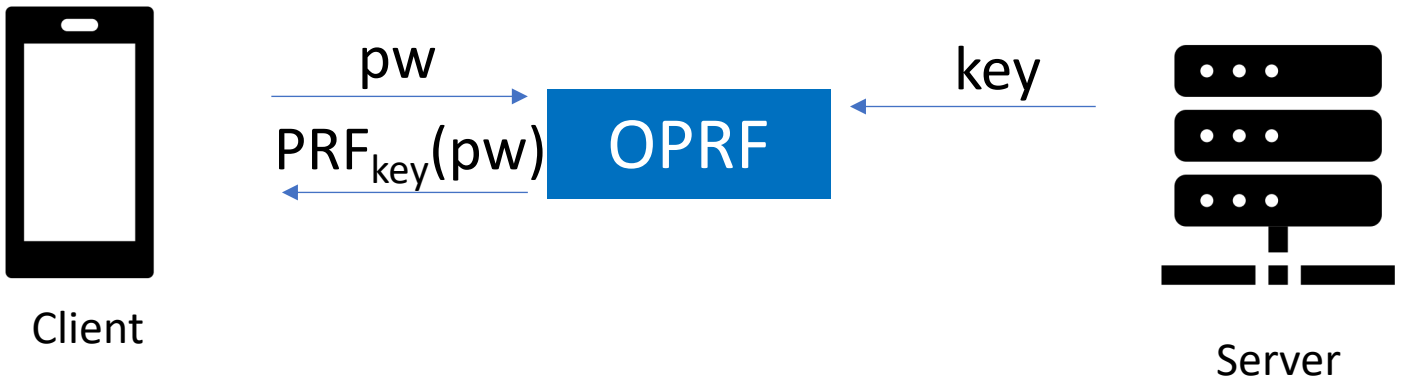
- Private Set Intersection



- Single Sign-On

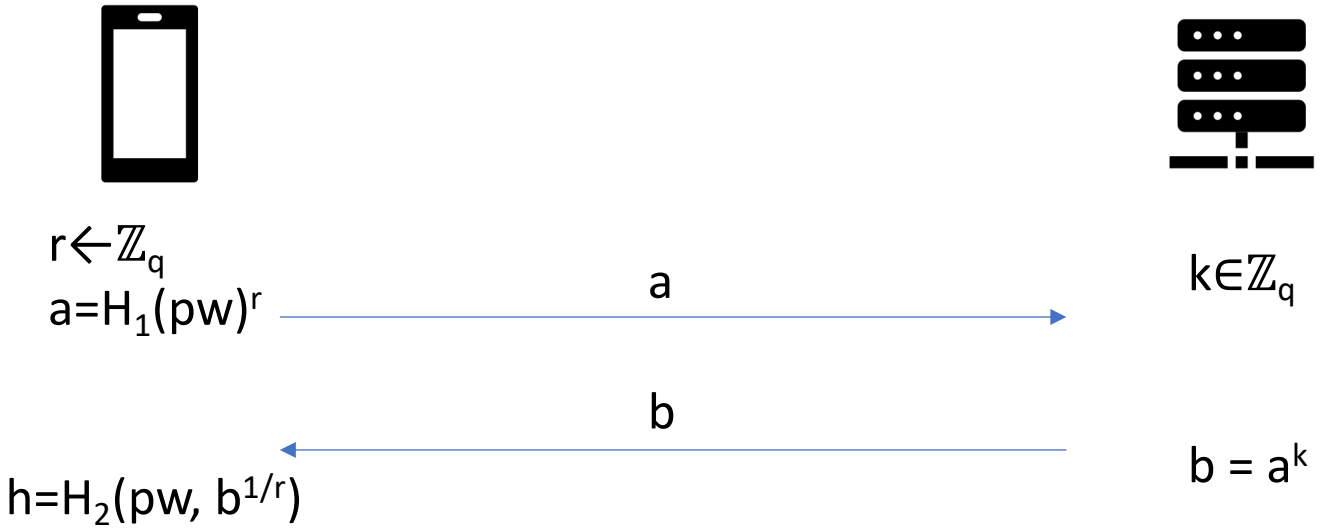


Oblivious Pseudo-Random Functions (OPRFs)



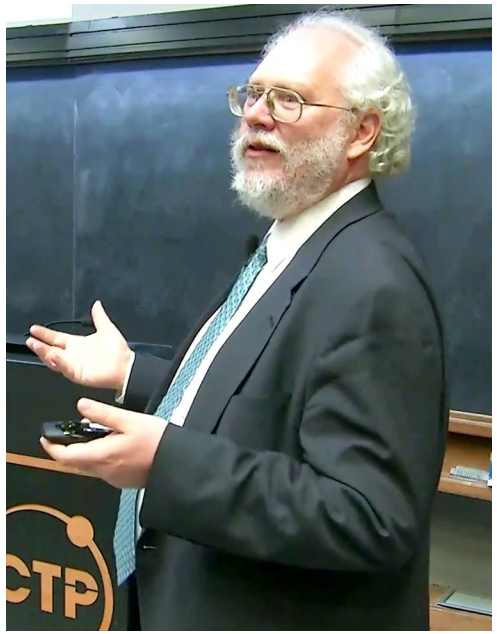
- Output is pseudo-random
- Server doesn't learn pw
- Client doesn't learn pw

2HashDH [JKKX16]



The spoilsports

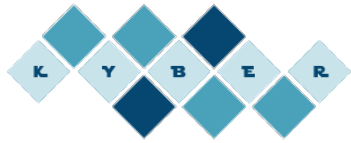
Quantum computers



Shor’s algorithms

Post-Quantum OPRFS

SPHINCS+

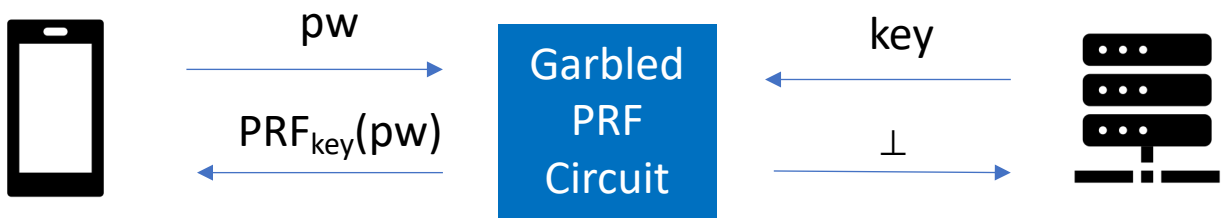


- For many crypto tasks, we have good PQ algorithms

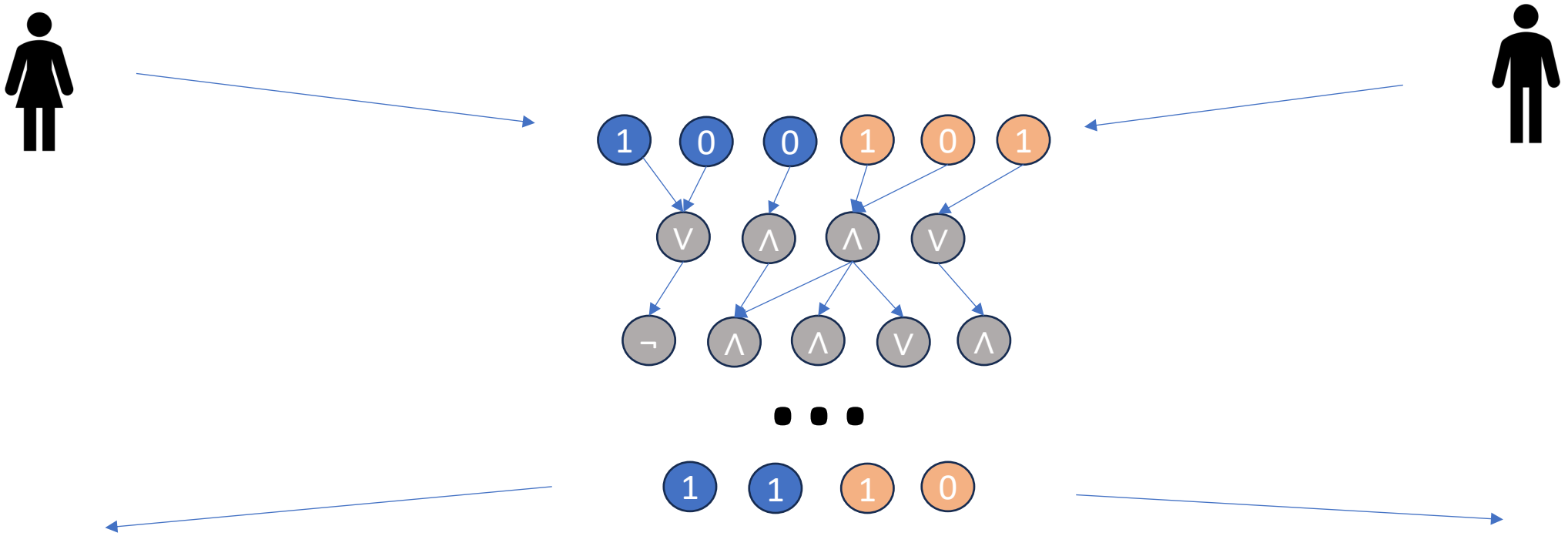
- For OPRFs: Several constructions proposed
  - Lattice-based: Not yet practically efficient [ADDS19, ADDG23]
  - Isogeny-based: One broken construction. Three others are proposed [BKW20,HMR23,Basso23]
  - Promising candidates from new ‘Dark-Matter’ weak PRF [BIPSW18, DGHIKS21]

The Garbled Circuits approach

- Proposed by Pinkas et al. [PSSW09]
- Garbled Circuits only need PQ oblivious transfer

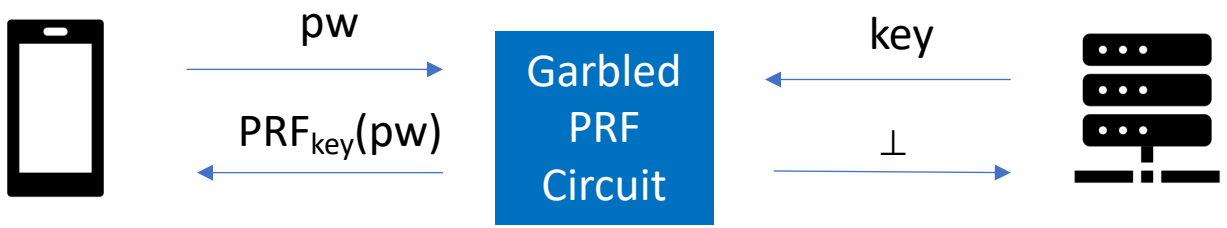


Garbled Circuits [Yao86]



The Garbled Circuits approach

- Proposed by Pinkas et al. [PSSW09]
- Garbled Circuits only need PQ oblivious transfer

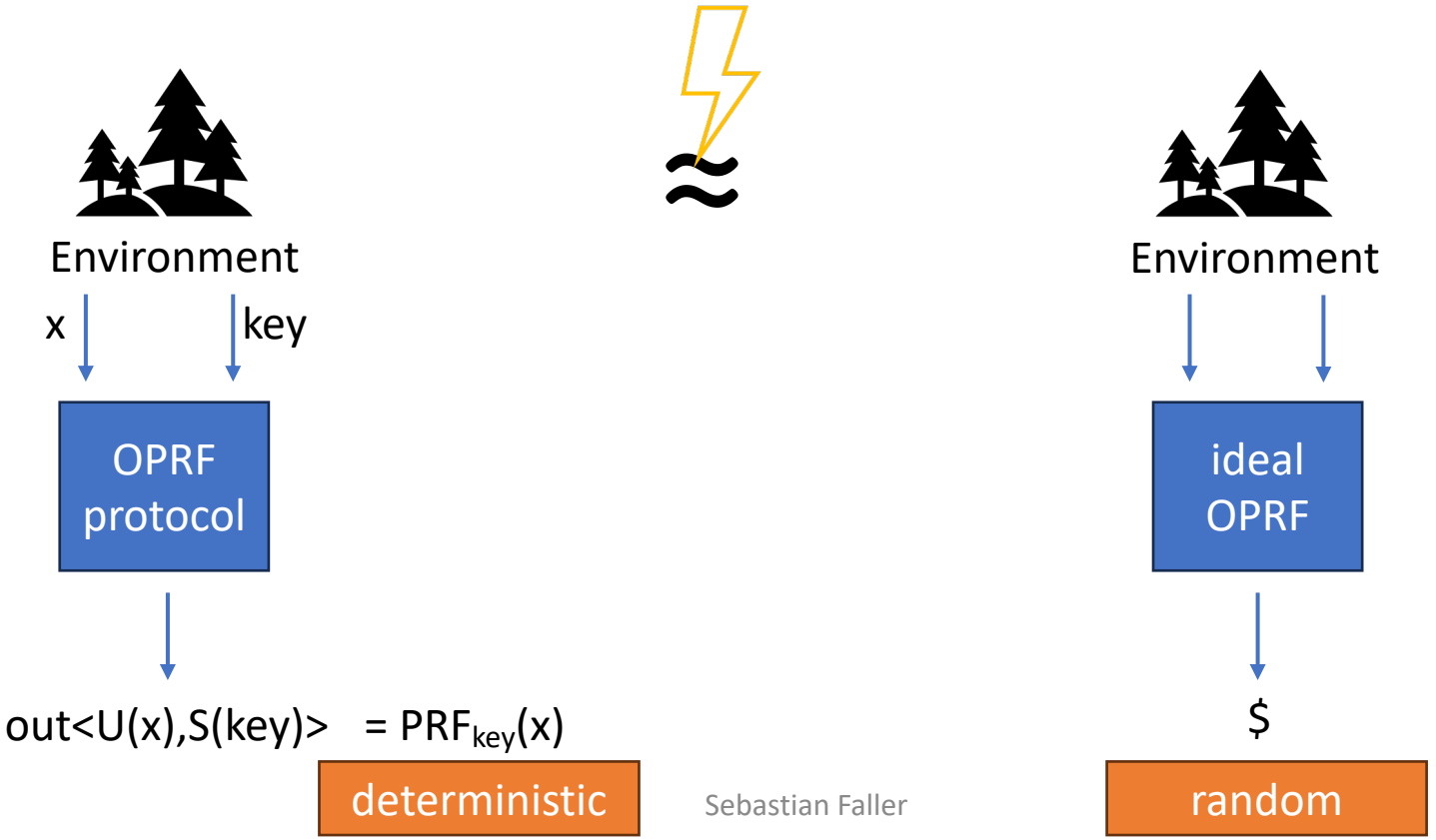


Questions:

- Security sufficient for applications?
  => Universal Composability (UC)?
- How efficient?

Limitations of ‘plain’ Garbled Circuits

- OPAQUE proof requires for corrupted servers:

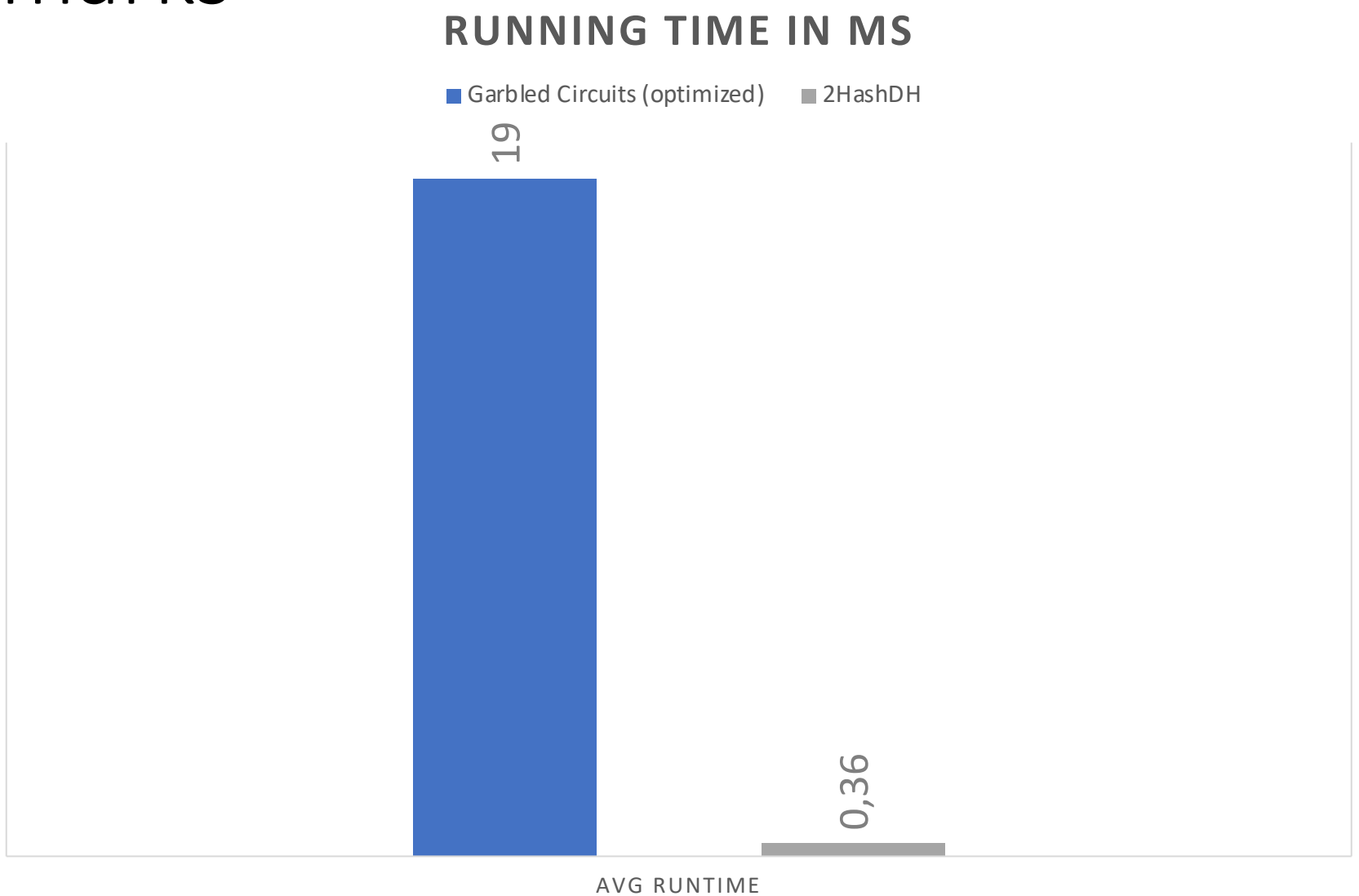


We showed:

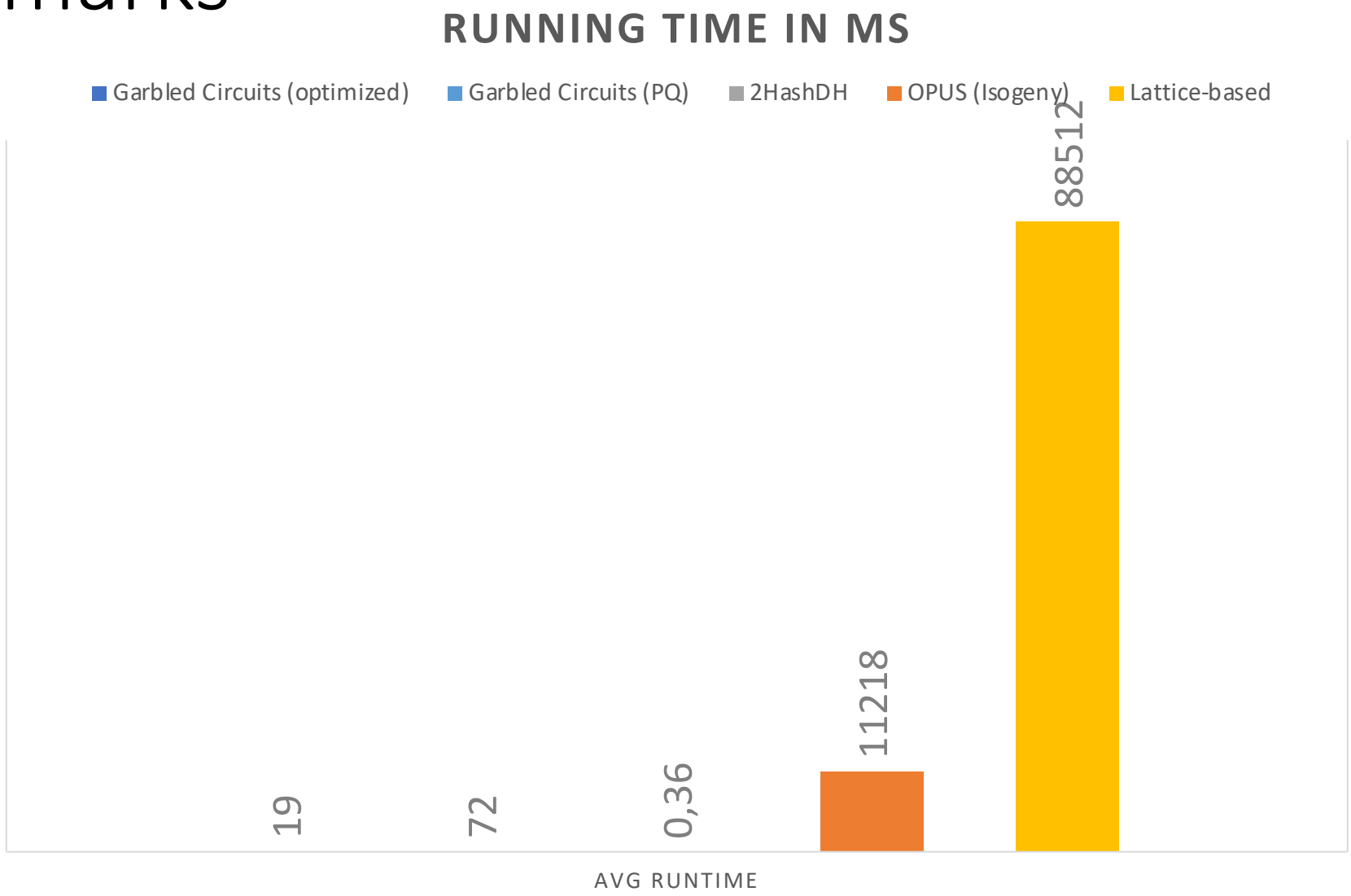
- Garbled Circuit OPRF can be made composable (using programmable random oracles)
- It is impossible to achieve UC secure* OPRFs using non-programmable random oracles
- The OPRF definition of [JKKX18] is strictly stronger than another proposed OPRF definition [CL17]

*using the OPRF definition of [JKKX18]

Benchmarks


RUNNING TIME IN MS
Garbled Circuits (optimized)
2HashDH
19
0,36
AVG RUNTIME

Benchmarks


RUNNING TIME IN MS
Garbled Circuits (optimized)
Garbled Circuits (PQ)
2HashDH
OPUS (Isogeny)
Lattice-based
19
72
0,36
11218
88512
AVG RUNTIME

Benchmarks

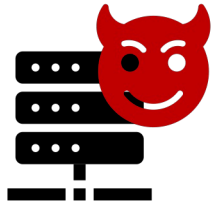
Protocol	Avg. Runtime (Local) [ms]	Avg. Runtime (WAN) [ms]	Network Traffic [kB]	UC	PQ
Our work (AES-128, EMP-Tool)	19.92 ± 0.77	268.19 ± 19.42	232.71	×	×
Our work (AES-256, EMP-Tool)	26.53 ± 0.99	282.48 ± 26.04	299.78	×	×
Our work (AES-128, PQ-MPC)	47.12 ± 3.22	1696.91 ± 53.62	4746.13	×	✓
Our work (AES-256, PQ-MPC)	72.63 ± 4.51	2074.42 ± 22.98	6787.48	×	✓
2HashDH [35]	0.36 ± 0.13	201.88 ± 0.21	0.07	✓	×
Lattice VOPRF [2]	88512.92 ± 2079.35	95418.25 ± 989.30	513.25 ± 0.17	×	✓
OPUS [31]	11218.45 ± 61.98	35285.26 ± 36.50	24.70	×	✓

Benchmarks

Protocol	Avg. Runtime (Local) [ms]	Avg. Runtime (WAN) [ms]	Network Traffic [kB]	UC	PQ
Our work (AES-128, EMP-Tool)	19.92 ± 0.77	268.19 ± 19.42	232.71	×	×
Our work (AES-256, EMP-Tool)	26.53 ± 0.99	282.48 ± 26.04	299.78	×	×
Our work (AES-128, PQ-MPC)	47.12 ± 3.22	1696.91 ± 53.62	4746.13	×	✓
Our work (AES-256, PQ-MPC)	72.63 ± 4.51	2074.42 ± 22.98	6787.48	×	✓
2HashDH [35]	0.36 ± 0.13	201.88 ± 0.21	0.07	✓	×
Lattice VOPRF [2]	88512.92 ± 2079.35	95418.25 ± 989.30	513.25 ± 0.17	×	✓
OPUS [31]	11218.45 ± 61.98	35285.26 ± 36.50	24.70	×	✓

Open Problems

- Malicious Server?
  - Actively secure GC not sufficient
  - Extraction problems
  - Maybe use weaker OPRF definition?



- Implementation of UC secure **and** PQ secure OT

Conclusion

Contributions

- Garbled Circuit-based OPRF can be adapted to be composable (assuming semi-honest servers)
- Assessed concrete performance in comparison to other OPRFs
- Gave impossibility result and related two commonly used OPRF definitions

Limitations

- Malicious server security seems hard to get
- Benchmarks should be taken with a grain of salt

Literature

- [ADDG23] M. R. Albrecht, A. Davidson, A. Deo, and D. Gardham, “Crypto Dark Matter on the Torus”.
- [ADDS19] M. R. Albrecht, A. Davidson, A. Deo, and N. P. Smart, “Round-optimal Verifiable Oblivious Pseudorandom Functions From Ideal Lattices,” 1271, 2019. Accessed: Jul. 20, 2021. [Online]. Available: https://eprint.iacr.org/2019/1271
- [Basso23] A. Basso, “A Post-Quantum Round-Optimal Oblivious PRF from Isogenies.” 2023. Accessed: Sep. 28, 2023. [Online]. Available: https://eprint.iacr.org/2023/225
- [BIPSW18] D. Boneh, Y. Ishai, A. Passelègue, A. Sahai, and D. J. Wu, “Exploring Crypto Dark Matter:: New Simple PRF Candidates and Their Applications,” in *Theory of Cryptography*, vol. 11240, A. Beimel and S. Dziembowski, Eds., in Lecture Notes in Computer Science, vol. 11240. , Cham: Springer International Publishing, 2018, pp. 699–729. doi: 10.1007/978-3-030-03810-6_25.
- [BKW20] D. Boneh, D. Kogan, and K. Woo, “Oblivious Pseudorandom Functions from Isogenies,” 1532, 2020. Accessed: Jul. 20, 2021. [Online]. Available: https://eprint.iacr.org/2020/1532
- [DGHIKS21] I. Dinur *et al.*, “MPC-Friendly Symmetric Cryptography from Alternating Moduli: Candidates, Protocols, and Applications.” 2021. Accessed: Jun. 06, 2023. [Online]. Available: https://eprint.iacr.org/2021/885
- [HMR23] L. Heimberger, F. Meisingseth, and C. Rechberger, “OPRFs from Isogenies: Designs and Analysis.” 2023. Accessed: Jun. 05, 2023. [Online]. Available: https://eprint.iacr.org/2023/639
- [JKX18] S. Jarecki, H. Krawczyk, and J. Xu, “OPAQUE: An Asymmetric PAKE Protocol Secure Against Pre-Computation Attacks,” 163, 2018. Accessed: May 02, 2022. [Online]. Available: https://eprint.iacr.org/2018/163
- [JKKX16] S. Jarecki, A. Kiayias, H. Krawczyk, and J. Xu, “Highly-Efficient and Composable Password-Protected Secret Sharing (Or: How to Protect Your Bitcoin Wallet Online),” 144, 2016. Accessed: Aug. 10, 2021. [Online]. Available: https://eprint.iacr.org/2016/144