Karlsruhe Institute of Technology

KASTEL

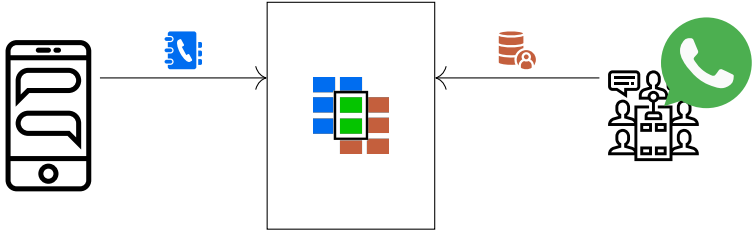
Practically Efficient Private Set Intersection From Trusted Hardware with Side Channels

Felix Dörre, Jeremias Mechler, and Jörn Müller-Quade | 6. December 2023

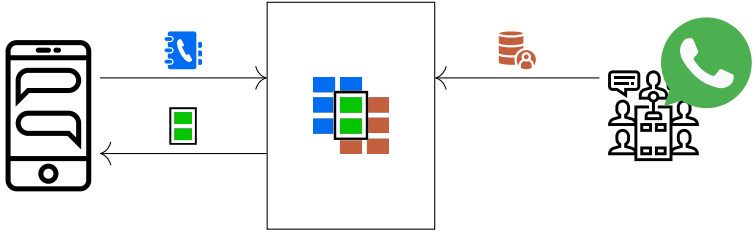
Private Set Intersection

All Icons by Pixel perfect, Eucalyp, Smashicons, monkik, Freepik, itim2101 from flaticon.com

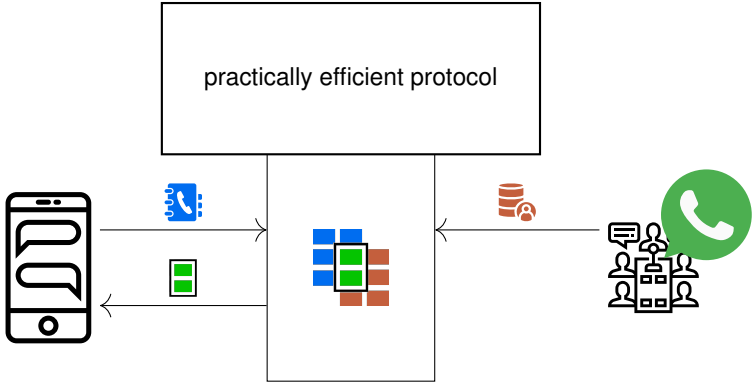
Private Set Intersection



Private Set Intersection

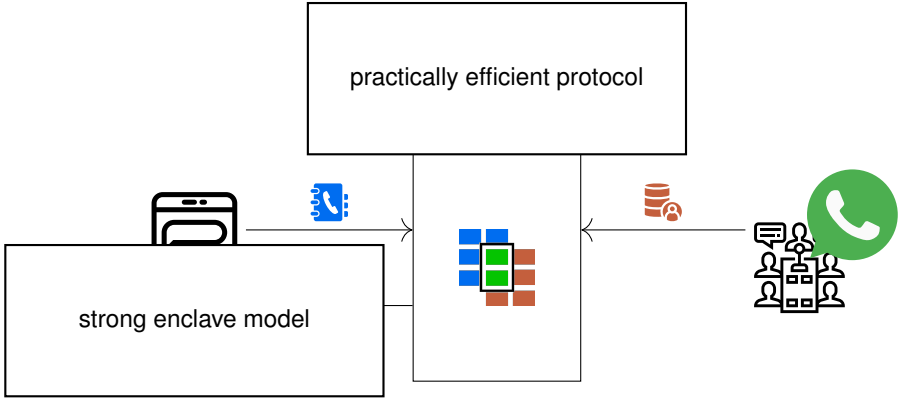


Private Set Intersection



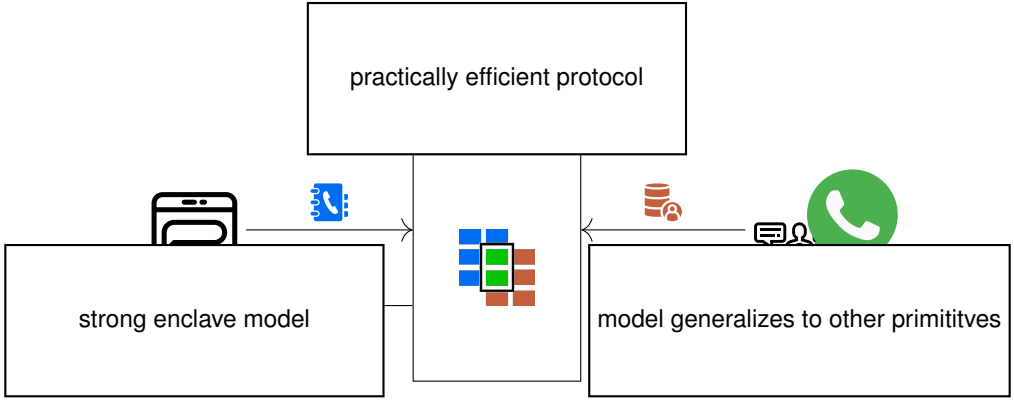
All Icons by Pixel perfect, Eucalyp, Smashicons, monkik, Freepik, itim2101 from flaticon.com

Private Set Intersection



All Icons by Pixel perfect, Eucalyp, Smashicons, monkik, Freepik, itim2101 from flaticon.com

Private Set Intersection



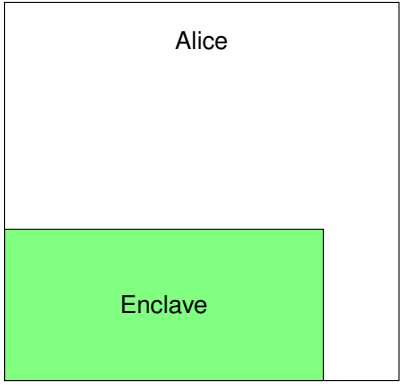
All Icons by Pixel perfect, Eucalyp, Smashicons, monkik, Freepik, itim2101 from flaticon.com

Many efficient PSI protocols use Random Oracles

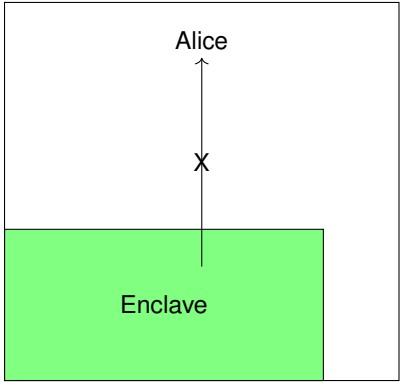
Recent PSI protocols: [RR17; Pin+20; Gar+21; RR22].

- Random Oracles are a very strong assumption.
- Provably cannot be instantiated by a cryptographic hash function. [CGH98; CGH04]
- Advanced protocols use special properties that may not hold for cryptographic hash functions.

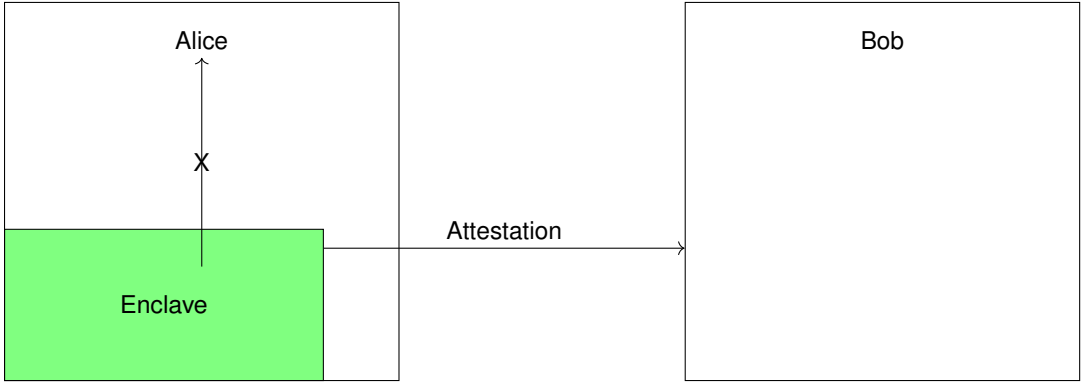
Secure Enclaves: Model



Secure Enclaves: Model



Secure Enclaves: Model



Assumption: Secure Enclaves (a closer look)

- Enclaves promise confidential and correct execution at near-native speed.
- However various side-channel attacks that routinely need to be mitigated [NBB20].
- Some side-channels like memory-access patterns are accepted.
- Formal Models: regular [PST17], transparent [Tra+17]

Assumption: Secure Enclaves (a closer look)

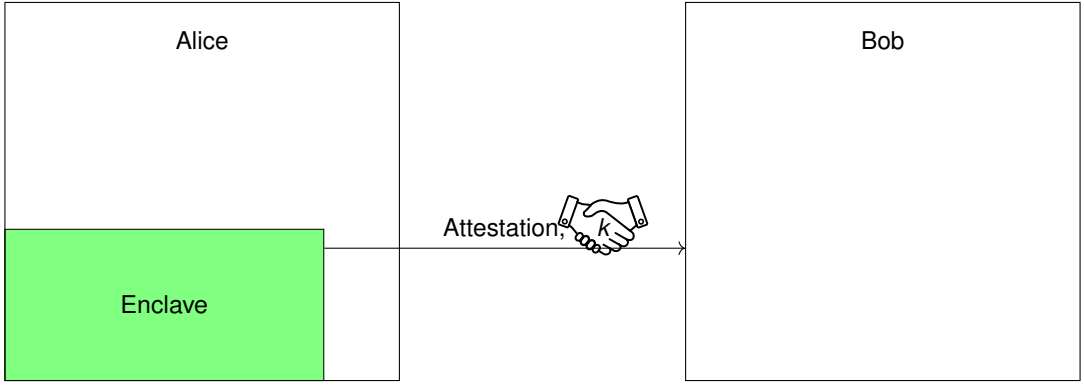
- Enclaves promise confidential and correct execution at near-native speed.
- However various side-channel attacks that routinely need to be mitigated [NBB20].
- Some side-channels like memory-access patterns are accepted.
- Formal Models: regular [PST17], transparent [Tra+17]

Definition: Almost-transparent Enclave (informal)

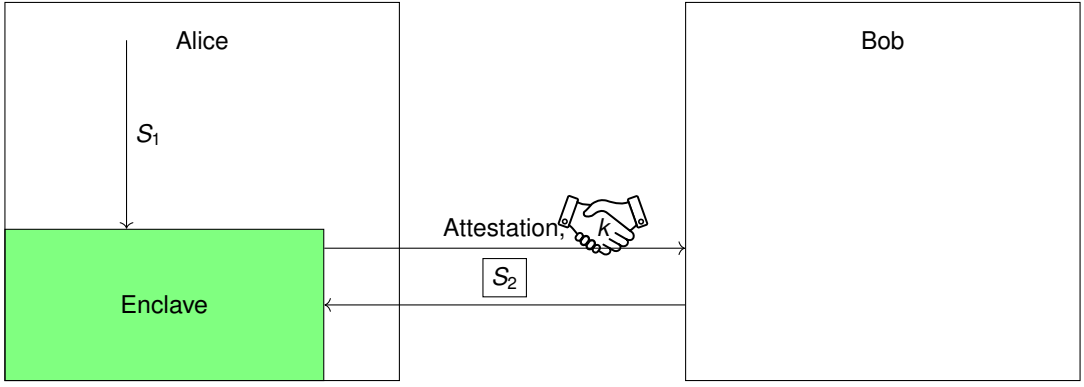
An enclave that leaks:

- all random bits generated internally
- the enclave memory before execution
- the output of all secure operations

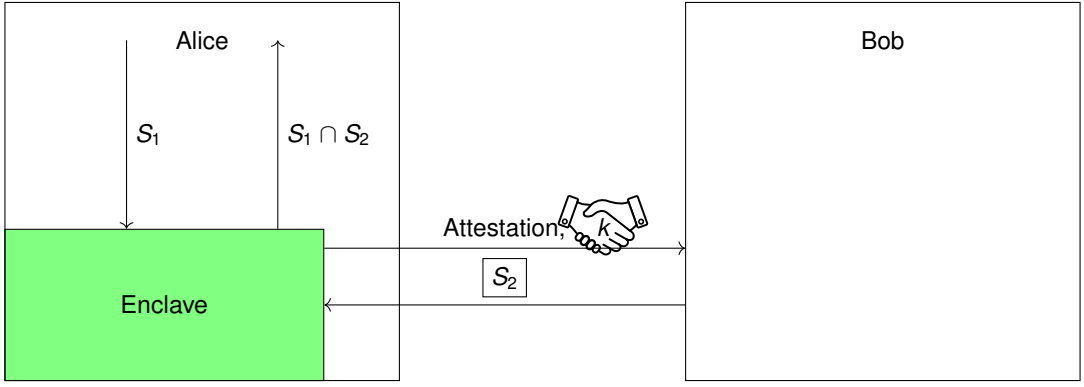
Naïve Approach



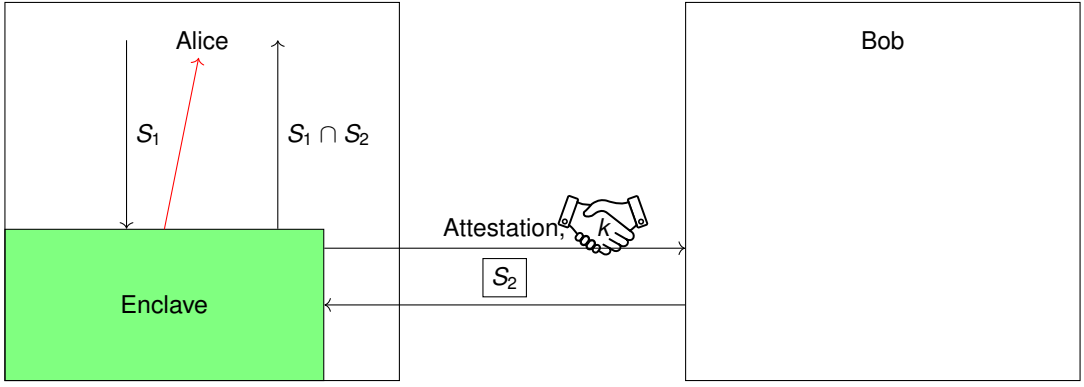
Naïve Approach



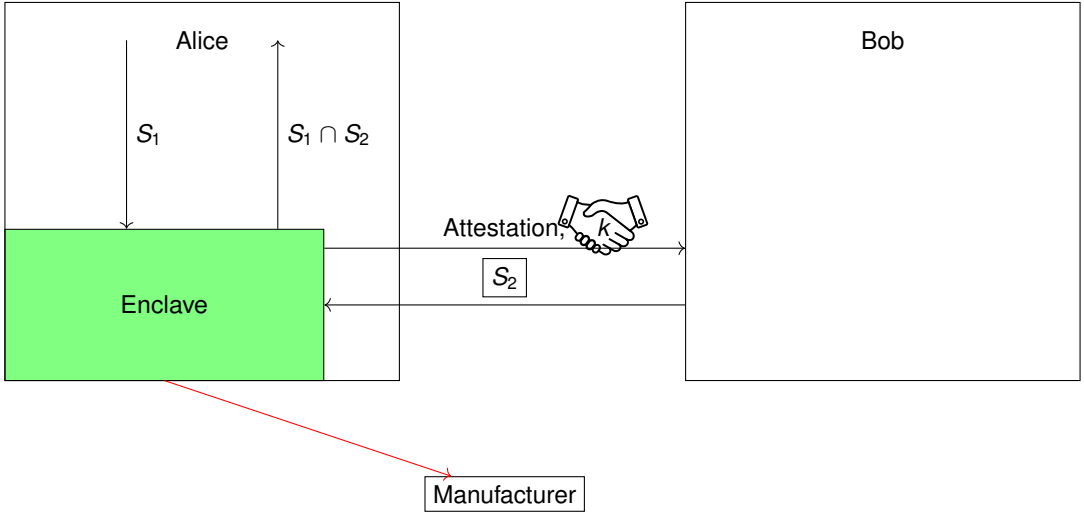
Naïve Approach



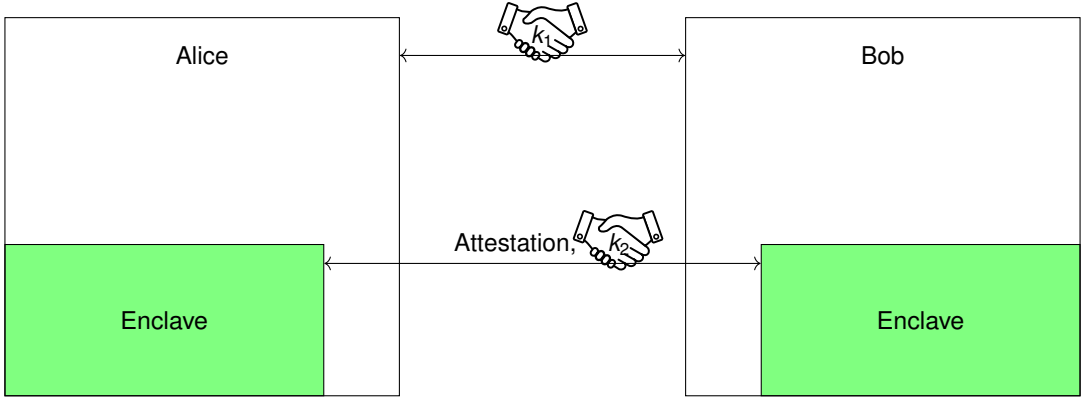
Naïve Approach



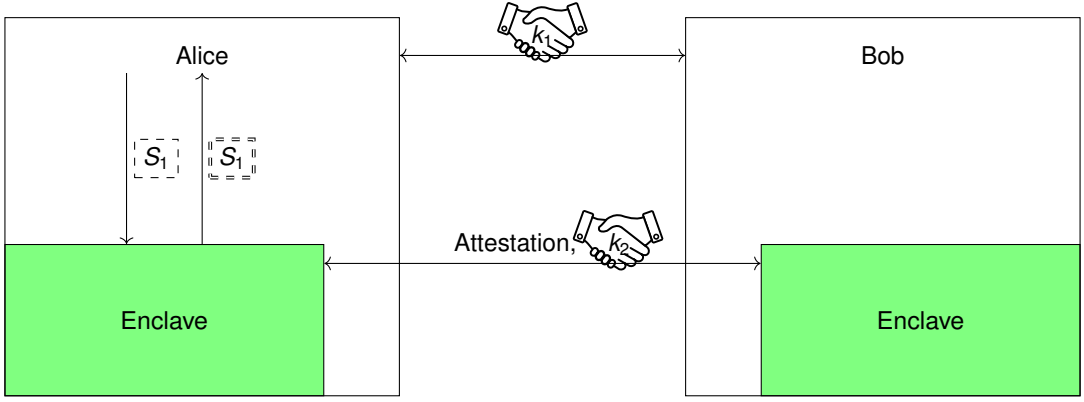
Naïve Approach



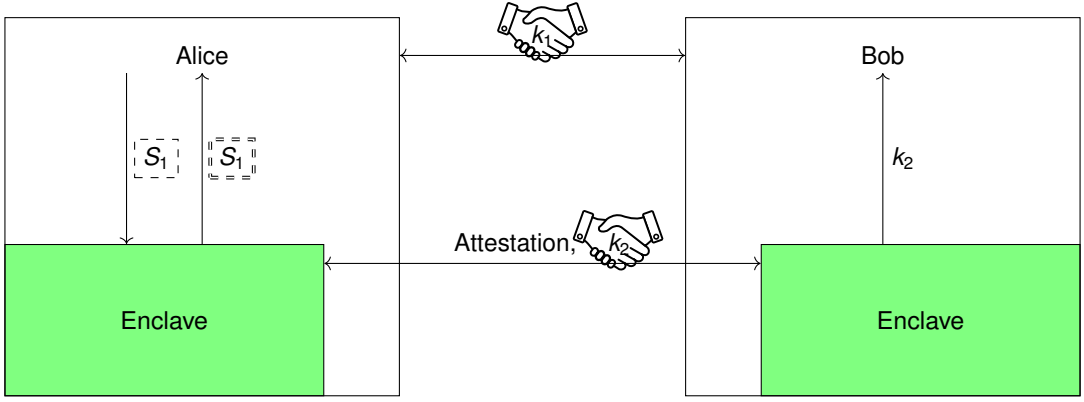
Slightly Better Approach



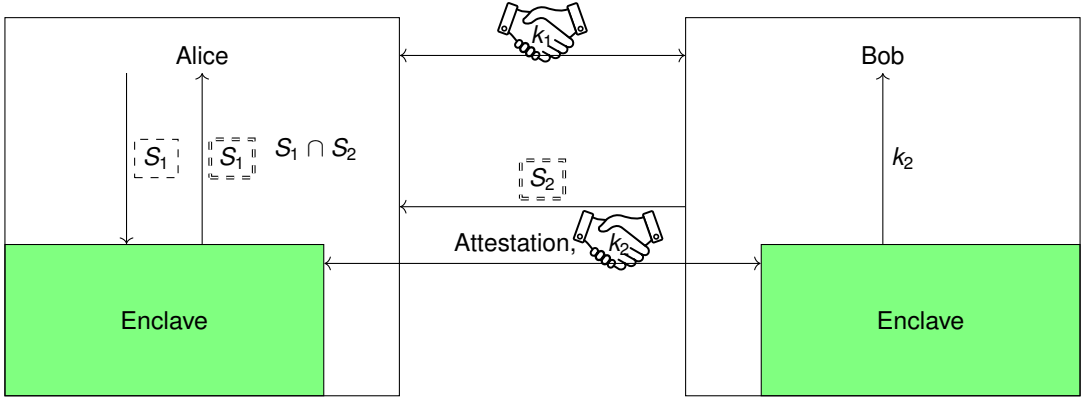
Slightly Better Approach



Slightly Better Approach



Slightly Better Approach



Implementation

- implemented on Intel SGX
- sets need to be sorted every time they pass between parties
- encrypt elements iteratively to reduce enclave memory

Implementation

- implemented on Intel SGX
- sets need to be sorted every time they pass between parties
- encrypt elements iteratively to reduce enclave memory

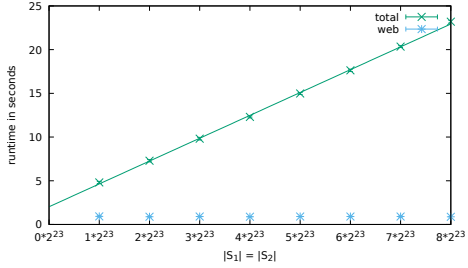


Figure: Runtime of the PSI protocol, depending on the number of elements in the input sets for elements of 128 bit size.

Summary

- fastest, practically efficient PSI protocol
- strong security model for enclaves: secure operations + full leakage to external party
- constructed variants, like limiting input sizes, realizing a trusted initializer or calculating hamming distance.

References I

[CGH04] Ran Canetti, Oded Goldreich, and Shai Halevi. “On the Random-Oracle Methodology as Applied to Length-Restricted Signature Schemes”. In: *TCC 2004: 1st Theory of Cryptography Conference*. Ed. by Moni Naor. Vol. 2951. Lecture Notes in Computer Science. Cambridge, MA, USA: Springer, Heidelberg, Germany, Feb. 2004, pp. 40–57. DOI: 10.1007/978-3-540-24638-1_3.

[CGH98] Ran Canetti, Oded Goldreich, and Shai Halevi. “The Random Oracle Methodology, Revisited (Preliminary Version)”. In: *30th Annual ACM Symposium on Theory of Computing*. Dallas, TX, USA: ACM Press, May 1998, pp. 209–218. DOI: 10.1145/276698.276741.

[Gar+21] Gayathri Garimella et al. “Oblivious Key-Value Stores and Amplification for Private Set Intersection”. In: *Advances in Cryptology – CRYPTO 2021, Part II*. Ed. by Tal Malkin and Chris Peikert. Vol. 12826. Lecture Notes in Computer Science. Virtual Event: Springer, Heidelberg, Germany, Aug. 2021, pp. 395–425. DOI: 10.1007/978-3-030-84245-1_14.

References

References II

[NBB20] Alexander Nilsson, Pegah Nikbakht Bideh, and Joakim Brorsson. “A Survey of Published Attacks on Intel SGX”. In: *CoRR* abs/2006.13598 (2020). arXiv: 2006.13598. URL: https://arxiv.org/abs/2006.13598.

[Pin+20] Benny Pinkas et al. “PSI from PaXoS: Fast, Malicious Private Set Intersection”. In: *Advances in Cryptology – EUROCRYPT 2020, Part II*. Ed. by Anne Canteaut and Yuval Ishai. Vol. 12106. Lecture Notes in Computer Science. Zagreb, Croatia: Springer, Heidelberg, Germany, May 2020, pp. 739–767. DOI: 10.1007/978-3-030-45724-2_25.

[PST17] Rafael Pass, Elaine Shi, and Florian Tramèr. “Formal Abstractions for Attested Execution Secure Processors”. In: *Advances in Cryptology – EUROCRYPT 2017, Part I*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Vol. 10210. Lecture Notes in Computer Science. Paris, France: Springer, Heidelberg, Germany, Apr. 2017, pp. 260–289. DOI: 10.1007/978-3-319-56620-7_10.

References

References III

[RR17] Peter Rindal and Mike Rosulek. “Improved Private Set Intersection Against Malicious Adversaries”. In: *Advances in Cryptology – EUROCRYPT 2017, Part I*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Vol. 10210. Lecture Notes in Computer Science. Paris, France: Springer, Heidelberg, Germany, Apr. 2017, pp. 235–259. DOI: 10.1007/978-3-319-56620-7_9.

[RR22] Peter Rindal and Srinivasan Raghuraman. “Blazing Fast PSI from Improved OKVS and Subfield VOLE”. In: *IACR Cryptol. ePrint Arch.* (2022), p. 320. URL: https://eprint.iacr.org/2022/320.

[Tra+17] Florian Tramèr et al. “Sealed-Glass Proofs: Using Transparent Enclaves to Prove and Sell Knowledge”. In: *2017 IEEE European Symposium on Security and Privacy, EuroS&P 2017, Paris, France, April 26-28, 2017*. IEEE, 2017, pp. 19–34. DOI: 10.1109/EuroSP.2017.28. URL: https://doi.org/10.1109/EuroSP.2017.28.

References