Karlsruhe Institute of Technology

KASTEL - Institute of Information Security and Dependability
Cryptography and Security Group
https://crypto.kastel.kit.edu

Fairness in Multi-Party Computation using Trusted Computing

Master's Thesis

Multi-party computation (MPC) allows mutually distrusting parties to jointly compute a function over inputs. Most MPC protocols are correct, meaning the output complies with the result of the function given the inputs, and are private, meaning the protocol leaks no information about the inputs of the parties. A different, but equally important property is fairness. Fairness achieves, colloquially speaking, that if the adversary receives the output, the honest receive the output as well. However, fairness as stated above for arbitrary functions with two parties is generally impossible to achieve [Cle86]. Therefore, different fairness notions have been proposed, weakening the adversary, weakening the fairness requirement or introduce other means to achieve fairness such as time or trusted computing. One fairness notion is Δ-Fairness [PST16], that states that (for a function Δ) if the adversary receives the output at time t, the honest parties receive the output at time $\Delta(t)$. In [Bay+24] a variant for this fairness notion is proposed called hidden Δ-fairness, requiring additionally that the parameters such as Δ is unknown to the adversary to prevent timing attacks. To achieve both versions of Δ-fairness, a trusted computing device is required, which is abstracted by using a formalization of trusted computing [PST16].

This thesis aims to continue this thought by reevaluating fairness in MPC using different enclaves models.

Scope of the work

- Revisiting hidden Δ-fairness
- Evaluate different enclave models
- Exploring fairness in MPC using different enclave models

Requirements

- Background knowledge in cryptography is recommended, but also be acquired while working on thesis.
- Interest in the topic is strongly recommended.
- This thesis can be written in english or german.

Contact

In case of interest or for further information, please contact Saskia Bayreuther, saskia.bayreuther@kit.edu (Room 248/251, Building 50.34)

References

[Bay+24] Saskia Bayreuther, Robin Berger, Felix Dörre, Jeremias Mechler, and Jörn Müller-Quade. *Hidden Δ-fairness: A Novel Notion for Fair Secure Two-Party Computation.* Cryptology ePrint Archive, Paper 2024/587. 2024. URL: https://eprint.iacr.org/2024/587.

[Cle86] Richard Cleve. "Limits on the security of coin flips when half the processors are faulty". In: *Proceedings of the eighteenth annual ACM symposium on Theory of computing.* 1986, pp. 364–369.

[PST16] Rafael Pass, Elaine Shi, and Florian Tramer. *Formal Abstractions for Attested Execution Secure Processors.* Cryptology ePrint Archive, Paper 2016/1027. 2016. URL: https://eprint.iacr.org/2016/1027.