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

SoK: Deniability in Multi-Party Protocols

Bachelor's Thesis

An interesting feature of multi-party protocols is *deniability*. A protocol that achieves deniability allows participants to plausibly lie about their behavior when pressed. For example, a political activist may be able to claim to be the author of a benign message rather than a critical one and avoid persecution. There are many different notions of deniability in the literature. The example above can be classified as *plausible deniability*, which is a common notion in communication [Kuh+21]. In multi-party computation, there is the notion of *incoercibility*, which, when achieved, which allows threatened parties to claim obedient behavior, but act otherwise [Alw+15].

The scope of this thesis is to explore multiparty protocols that offer deniability. Different notions of deniability are to be categorized, compared, and related to each other.

Scope of the work

- Literature research on deniability in cryptographic protocols.
- Categorization of deniability notions: What are they used for? How are they defined?
- How do different deniability notions relate to each other? Are there implications?

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

[Alw+15] Joël Alwen, Rafail Ostrovsky, Hong-Sheng Zhou, and Vassilis Zikas. "Incoercible multi-party computation and universally composable receipt-free voting". In: *Advances in Cryptology–CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II 35*. Springer. 2015, pp. 763–780.

[Kuh+21] Christiane Kuhn, Maximilian Noppel, Christian Wressnegger, and Thorsten Strufe. "Plausible deniability for anonymous communication". In: *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*. 2021, pp. 17–32.