Universität Konstanz

Student Assistant in Cryptography

Context

Traditionally, authenticated encryption schemes are required to ensure confidentiality and authenticity. More recently, committing security—which prevents adversaries from finding ciphertexts that decrypt under multiple keys—turned out to be another relevant security goal. The absence of committing security can lead to attacks when using authenticated encryption schemes in larger protocols. This can for instance be seen in the attack against the Facebook message franking attack [DGRW18].
From 2018-2023, the National Institute of Standards and Technology (NIST) executed a standardization process on lightweight cryptography (LWC) [NIST]. Out of 57 initial submissions, 10 authenticated encryption schemes were selected as finalists, before Ascon was chosen to be standardized in 2023. Several finalists were shown to be vulnerable to various committing attacks [KSW23].

The Task

The overall goal of this position is to implement committing attacks against the finalists of the NIST LWC standardization process via the following steps:

1. acquire basic cryptographic background on authenticated encryption and committing attacks,
2. get familiar with the existing implementations of the NIST LWC finalists, and
3. implement the different committing attacks.

Requirements

- Solid programming skills
- Interest in cryptography
- Fluent in English

Application

If you are interested, please send an email to Patrick Struck (patrick.struck@uni.kn).

References

[DGRW18] – Dodis, Grubbs, Ristenpart, Woodage. Fast message franking: From invisible salamanders to encryptment. CRYPTO 2018. (https://ia.cr/2019/016)
[KSW23] – Krämer, Struck, Weishäupl. Committing AE from sponges: Security analysis of the NIST LWC finalists. Preprint 2023. (ia.cr/2023/1525)
[NIST] - https://csrc.nist.gov/Projects/lightweight-cryptography/