CT Advanced Computing Center (CACC) Security Seminar Series 2022-2023

Speaker: Peter Hall, Asiacrypt 22: https://eprint.iacr.org/2022/1108
Date: Wednesday, October 12, 2022
Time:12 - 1:30pm
Location: ITE 401
Remote Access: https://uconn-cmr.webex.com/uconn-cmr/j.php?MTID=m6e24b00880ea4a488adf302903cb9b63
Meeting number: 2621 780 2095
Password: EWt39phUyc4

Nonmalleable Digital Lockers and Robust Fuzzy Extractors in the Plain Model

In this work, we give the first constructions in the plain model of 1) nonmalleable digital lockers (Canetti and Varia, TCC 2009) and 2) robust fuzzy extractors (Boyen et al., Eurocrypt 2005) that secure sources with entropy below 1/2 of their length. Constructions were previously only known for both primitives assuming random oracles or a common reference string (CRS).

Along the way, we define a new primitive called a nonmalleable point function obfuscation with associated data. The associated data is public but protected from all tampering. We use the same paradigm to then extend this to digital lockers. Our constructions achieve nonmalleability over the output point by placing a CRS into the associated data and using an appropriate non-interactive zero-knowledge proof. Tampering is protected against the input point over low-degree polynomials and over any tampering to the output point and associated data. Our constructions achieve virtual black box security.

These constructions are then used to create robust fuzzy extractors that can support low-entropy sources in the plain model. By using the geometric structure of a syndrome secure sketch (Dodis et al., SIAM Journal on Computing 2008), the adversary's tampering function can always be expressed as a low-degree polynomial; thus, the protection provided by the constructed nonmalleable objects suffices.

UCONN

CACC