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

Speaker: Ghada Almashaqbeh https://eprint.iacr.org/2022/658
Date: Wednesday, October 19, 2022
Time:12 - 1:30pm
Location: ITE 401
Remote Access:https://uconn-cmr.webex.com/uconn-cmr/j.php?MTID=me8902798524818d27e24769f56e76289
Meeting number: 2620 576 7863
Password: e9YP38WfMwU

Unclonable Polymers and Their Cryptographic Applications

We propose a mechanism for generating and manipulating protein polymers to obtain a new type of consumable storage that exhibits intriguing cryptographic "self-destruct" properties, assuming the hardness of certain polymer-sequencing problems.
To demonstrate the cryptographic potential of this technology, we first develop a formalism that captures (in a minimalistic way) the functionality and security properties provided by the technology. Next, using this technology, we construct and prove security of two cryptographic applications that are currently obtainable only via trusted hardware that implements logical circuitry (either classical or quantum). The first application is a password-controlled secure vault where the stored data is irrecoverably erased once a threshold of unsuccessful access attempts is reached. The second is (a somewhat relaxed version of) one-time programs, namely a device that allows evaluating a secret function only a limited number of times before self-destructing, where each evaluation is made on a fresh user-chosen input.
Finally, while our constructions, modeling, and analysis are designed to capture the proposed polymer-based technology, they are sufficiently general to be of potential independent interest.

UCONN

CACC