Non-Black-Box Cryptography:
Defending Against and Benefiting from Access to Code

Challenge:

- Design and analyze cryptosystems secure against non-black-box attacks.
- Improve understanding of the effectiveness of non-black-box techniques in the construction of cryptosystems.

Solution:

- Develop and improve tools such as non-malleable codes for leakage/tamper resilience.
- Draw upon various areas of theoretical computer science to develop techniques for proving impossibility of non-black-box reductions.
- New notions and constructions of non-malleable codes.
- A new separation between public key encryption and one-way function in a non-black-box setting.

NSF CAREER award #CNS-1453045
University of Maryland
PI: Dana Dachman-Soled

Non-Black-Box Attacks

Real world side-channel attacks

↓

New mathematical models

↓

New provably-secure cryptosystems

↓

New practical implementations

Non-Black-Box Solutions

Minimal known assumptions for cryptographic tasks

Improve assumptions by considering non-black-box techniques

Prove assumptions cannot be improved, even with non-black-box techniques

Improve understanding of minimal assumptions. Inform community on which cryptosystems remain secure if assumptions proven false.

Scientific Impact:

- Introduce new mathematical models.
- Introduce new cryptographic techniques.
- Discover new connections between cryptography and other areas of theoretical computer science.
- Improve understanding of the strength of non-black-box techniques in cryptography.

Broader Impact:

- Advance the development of practical solutions against side-channel attacks.
- Curriculum development for undergraduate and graduate cryptography courses.
- Outreach to industry, and under-represented groups.
- Mentoring of graduate students, undergraduate students and high-school students.