Towards Mechanized Proofs of Composable Security Properties

BOSTON UNIVERSITY

Challenge:

- Society depends on complex cryptographic protocols for digital safety
- Proofs of such protocols are complex and error prone

Solution:

- *Modularity* using Universally Composable (UC) security
- DSL for *expressing* UC
- *Mechanization* using EasyCrypt proof assistant

EASYCRYPT

DSL for UC

Scientific Impact:

- EasyCrypt architecture and DSL for UC security
- Insights into UC theory
- Zero knowledge case study
- UC model of Signal messaging system

Broader Impact:

- Enabling application to complex protocols such as zero knowledge based on commitments and Signal messaging
- Fostering connections between formal methods and crypto communities, including training students to bridge this gap

NSF Grant 1801564, Boston University. Contact: stough@bu.edu.