Towards Mechanized Proofs of Composable Security Properties

BOSTON UNIVERSITY

Challenge:

- Society depends on complex cryptographic protocols
- Such proofs are complex and error prone

Modularity through UC Security

Solution:

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

EASYCRYPT

Mechanization

Scientific Impact:

- Novel EasyCrypt architecture and tool development for UC security
- New insights into theory of UC security

Broader Impact:

- Enabling application to protocols of practical interest
- Fostering connections between formal methods and crypto communities, including training students to bridge this gap

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