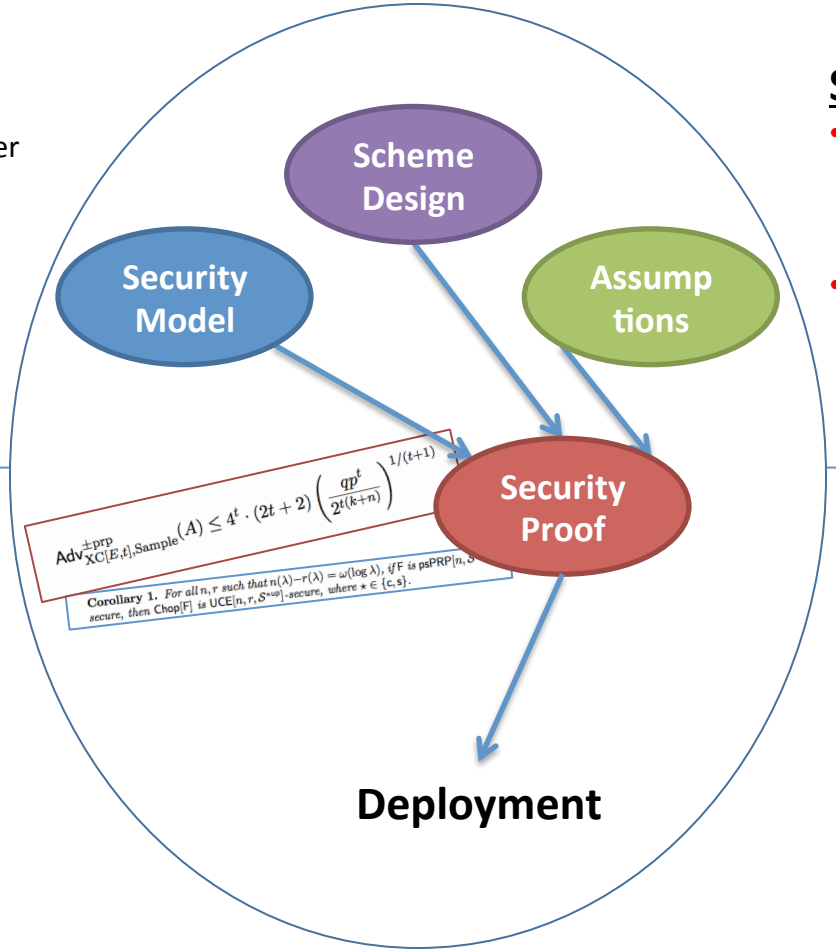
The Theoretical Foundations of Symmetric Cryptography (CAREER)

Challenge:

- Symmetric cryptography often favors attack-driven design over provable security.
- We want to **substantially increase the number of symmetric algorithms with security proofs.**
- Several technical barriers hinder meaningful security proofs.



Solution:

- Better **assumptions**.
- **Weakening of idealized models.**
- Study of **efficiency / security trade-offs.**
- **New theory**.

Grant CNS-1553758 (PI: Stefano Tessaro, University of California, Santa Barbara, tessaro@cs.ucsb.edu)

Scientific Impact:

- **New foundations** to support the development of provably-secure symmetric cryptography.
- **New connections** with information theory, combinatorics, and complexity theory.

Broader Impact:

- **Security validation** for widely deployed cryptographic algorithm.
- Annual **cryptography academy** for economically-disadvantaged high-school students.