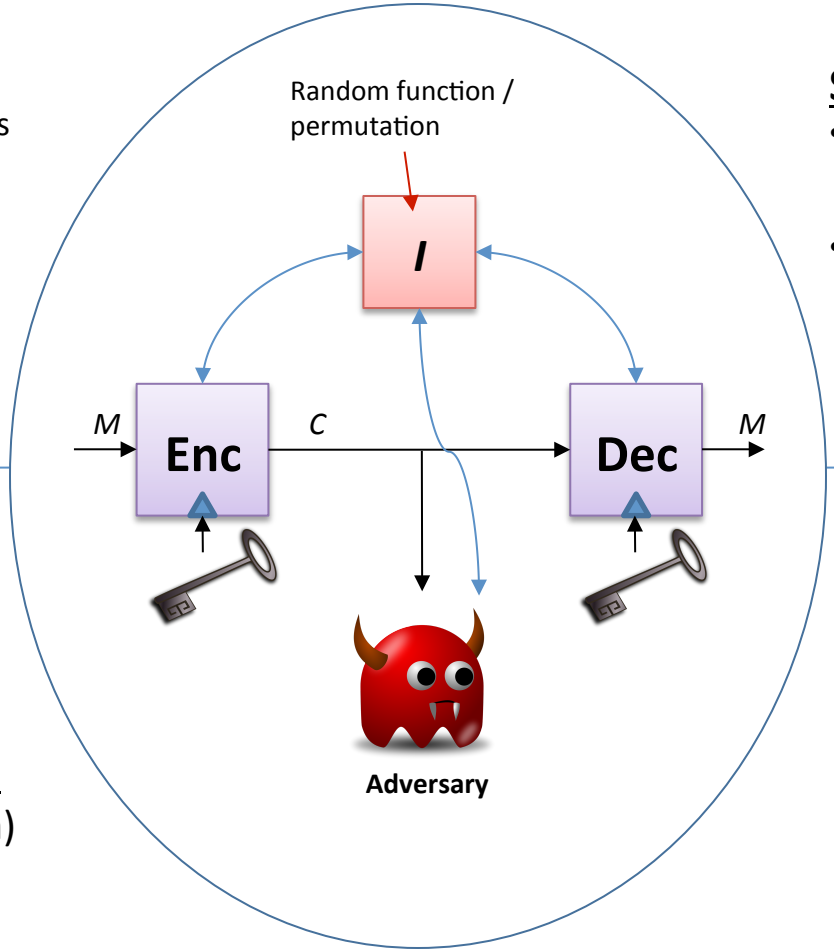
Better Security for Efficient Secret-Key Cryptography

Challenge:

- Design secret-key algorithms (e.g., block ciphers and MACs) which are both efficient and provably-secure.
- Target new security metrics of practical relevance (e.g., multi-user security)
- Traditional proof methods often insufficient.

Solution:

- Security proofs in models where a designated algorithm component is idealized (i.e., chosen at random)



Scientific Impact:

- New theory to prove ideal-model security of cryptographic algorithms.
- New theory for security proofs with respect to new metrics, in particular multi-user security.

Broader Impact:

- Security validation for widely deployed cryptographic algorithm.
- Support for the development of next-generation algorithms and standards.

Grant CNS-1423566 (PI: Stefano Tessaro, University of California, Santa Barbara, tessaro@cs.ucsb.edu)