CAREER: New Analytic Frontiers for Symmetric Cryptography

Challenge:

- It’s hard to rigorously justify real-world cryptographic schemes.
- In many cases, the barrier indicates a lack of proper analytic methods.

Solution:

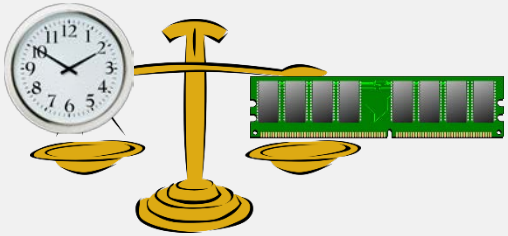
- Develop new analytic frameworks.
- Showcase their powers for real-world situations, such as analyzing randomness generators, or building a better scheme to encrypt credit card numbers.

NSF CNS 2046540 (CAREER)

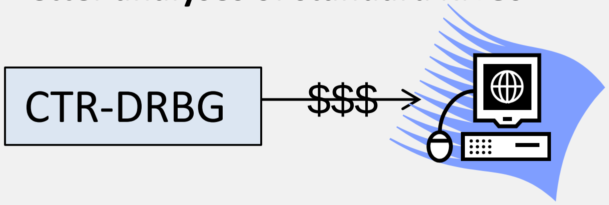
Viet Tung Hoang, Florida State University
tvhoang@cs.fsu.edu

Better way to encrypt credit card numbers

Time-space tradeoffs on crypto attacks



Better analyses of standard RNGs



Scientific Impact:

- Improve security guarantees for many widely used schemes.
- Develop a better way to encrypt credit card numbers

Broader Impact:

- Credit-card encryption scheme may be adopted by industry or NIST.
- Develop an original problem solving course to teach students the discovery process.