# Towards Stronger and Verified Security for Real-World Cryptography

## Challenge:

- Many real-world cryptographic schemes only have weak or no security guarantees.
- This either indicates a limitation of analysis, or suggests an actual vulnerability.

## Solution:

- Attack bad constructions:
  - Break NIST standards FF1/FF3 for encrypting credit-card numbers.
- Develop better analysis:
  - Give a tighter security bound for GCM encryption in TLS.
  - Analyze NIST standard CTR-DRBG of generating randomness.


NSF CRII 1755539
Viet Tung Hoang, Florida State University
tvhoang@cs.fsu.edu


**Attacks on NIST encryption standards**

FF1

FF3

**Better bounds on encryption in TLS**

Bank of America

GCM

**First analysis of NIST CTR-DRBG**

CTR-DRBG $\$\$\$\rightarrow$

## Scientific Impact:

- The FF1/FF3 standards have been revised due to the attacks in the project.
- The analysis of GCM and CTR-DRBG schemes will give theoretical assurance to their widespread usage.

## Broader Impact:

- Several companies have been patching their products due to the attacks in the project.
- The crypto course at FSU has been revised to have both theoretical rigor and practical skills to attack heuristic designs.