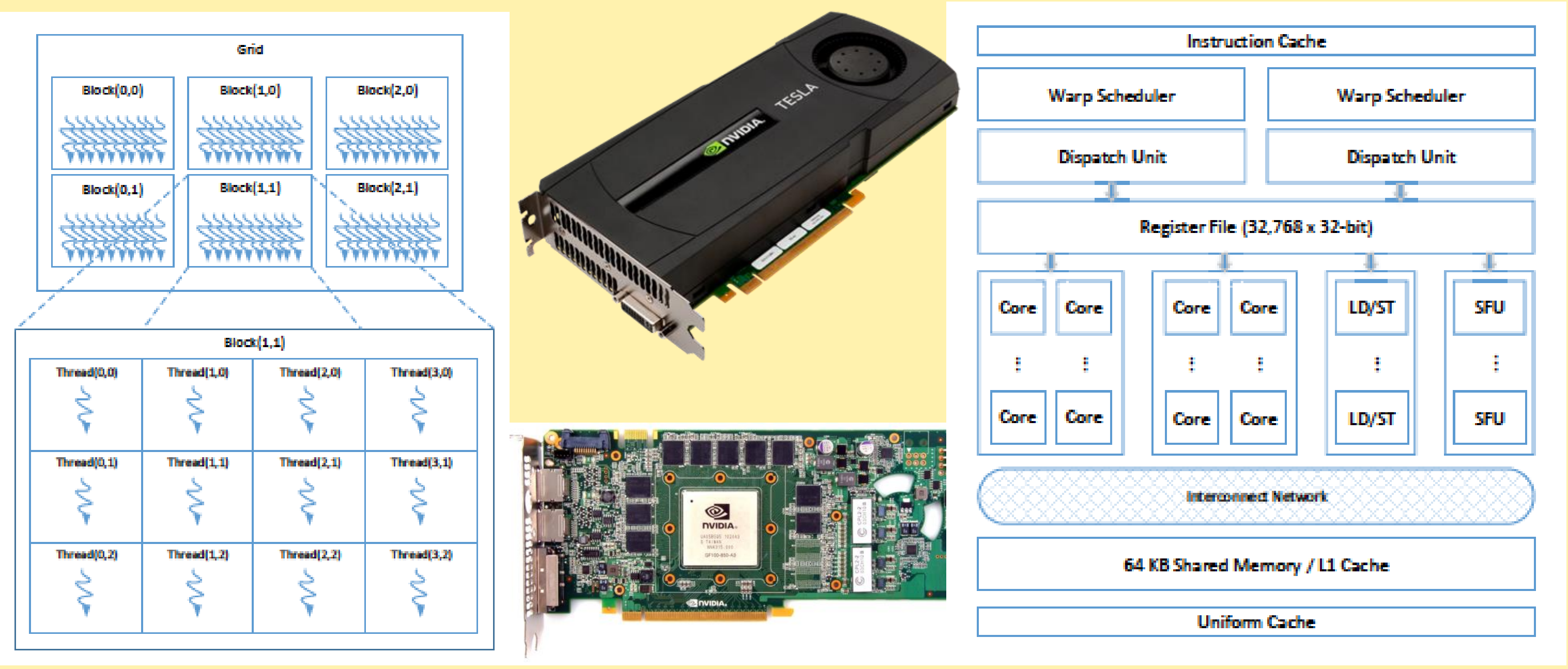
STARSS: Small: Side-Channel Analysis and Resiliency Targeting Accelerators

PIs: Prof. David Kaeli and Yunsi Fei
Electrical and Computer Engineering, Northeastern University, Boston, MA
http://tescase.coe.neu.edu/, kaeli/yfei@ece.neu.edu

Introduction

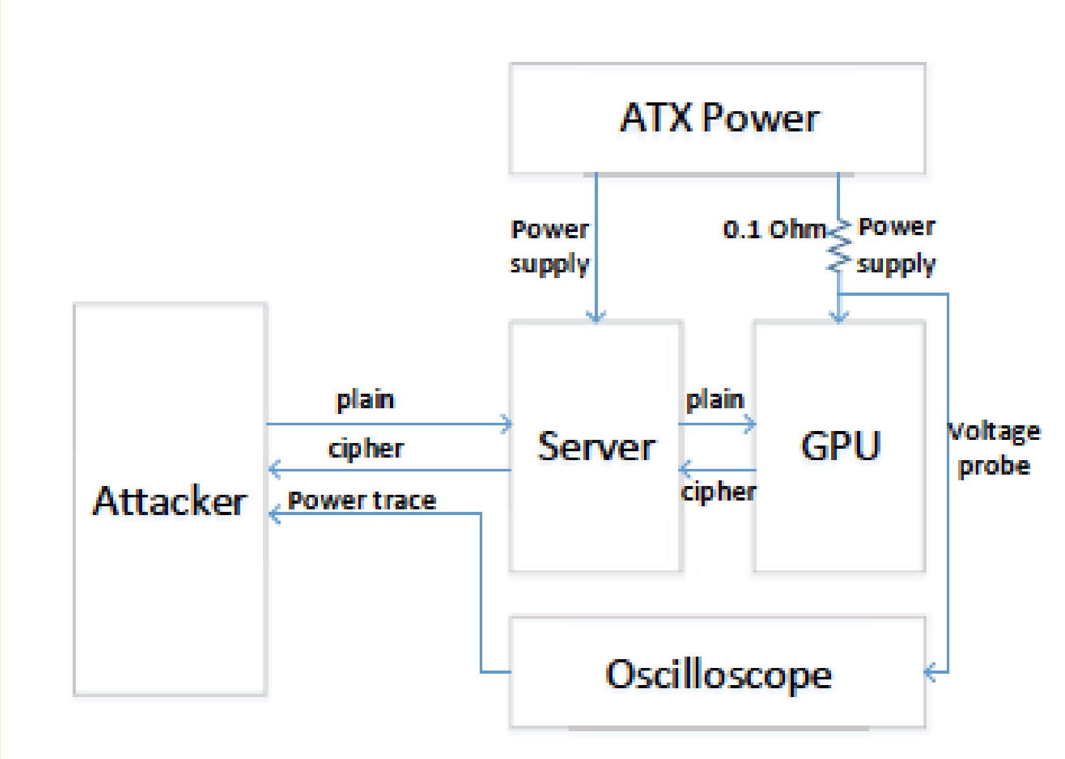
- GPUs have been used to accelerate general-purpose applications to deliver high throughput
- The rate GPU deployments used for accelerating cryptographic processing is only increasing
- The question "is a GPU a secure architecture for cryptographic processing" remains open.

Accelerators as Platform for Encryption



Power Analysis Attack Implementation

- 0.1Ω resistor in series with ATX 12V power supply
- Voltage drop across the resistor measured by Keysight MSOX4104A oscilloscope
- Execute AES encryption on the GPU
- Oscilloscope records power consumption, which can be analyzed to infer the encryption key



ATX Power

Power supply

0.1 Ohm

Power supply

Attacker

plain

cipher

Power trace

Server

plain

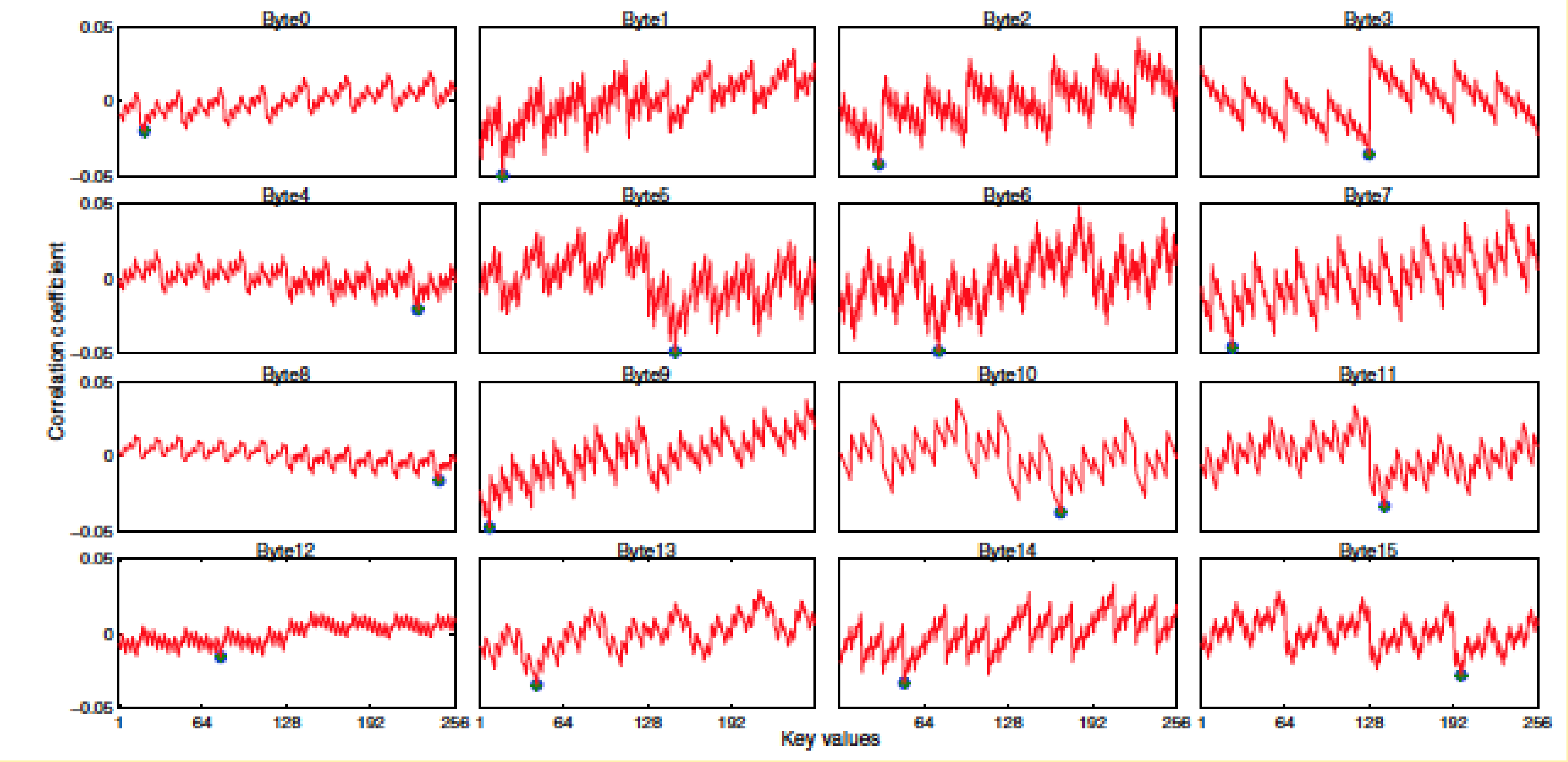
cipher

GPU

Voltage probe

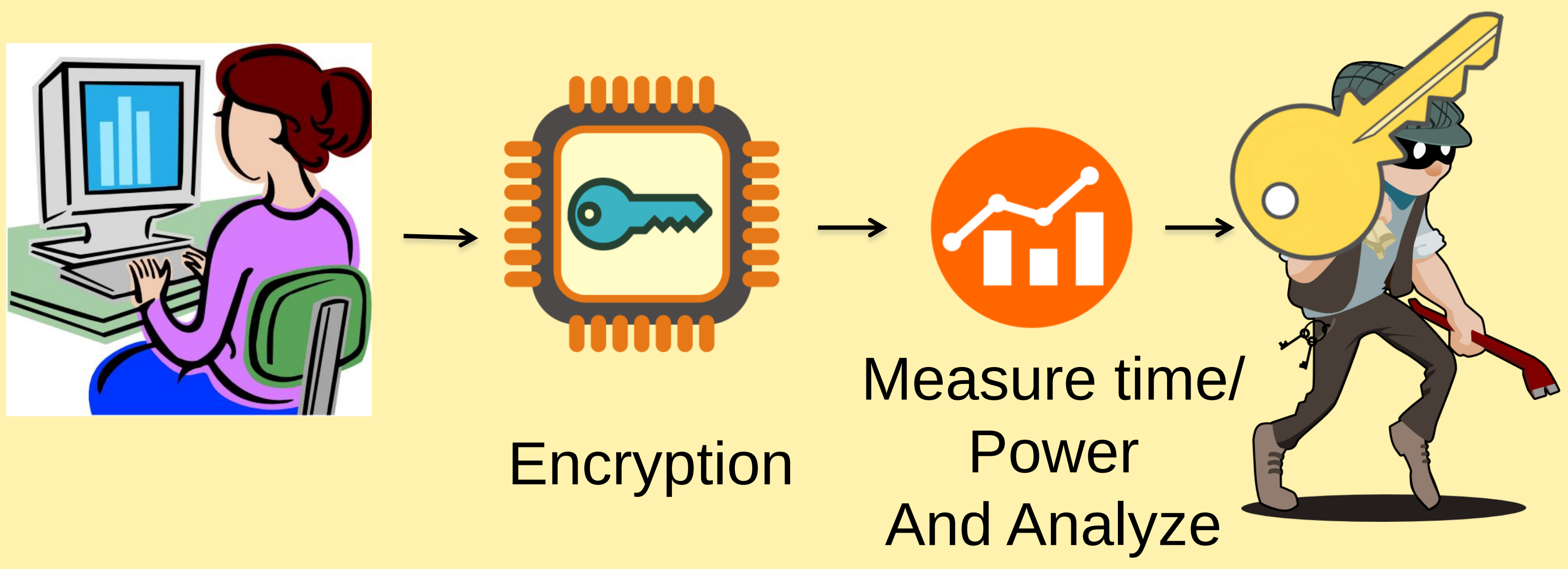
Oscilloscope

Key Recovery through Power Analysis



- Extraction of 16 key bytes, byte by byte
- Values with the highest negative correlation identify keys

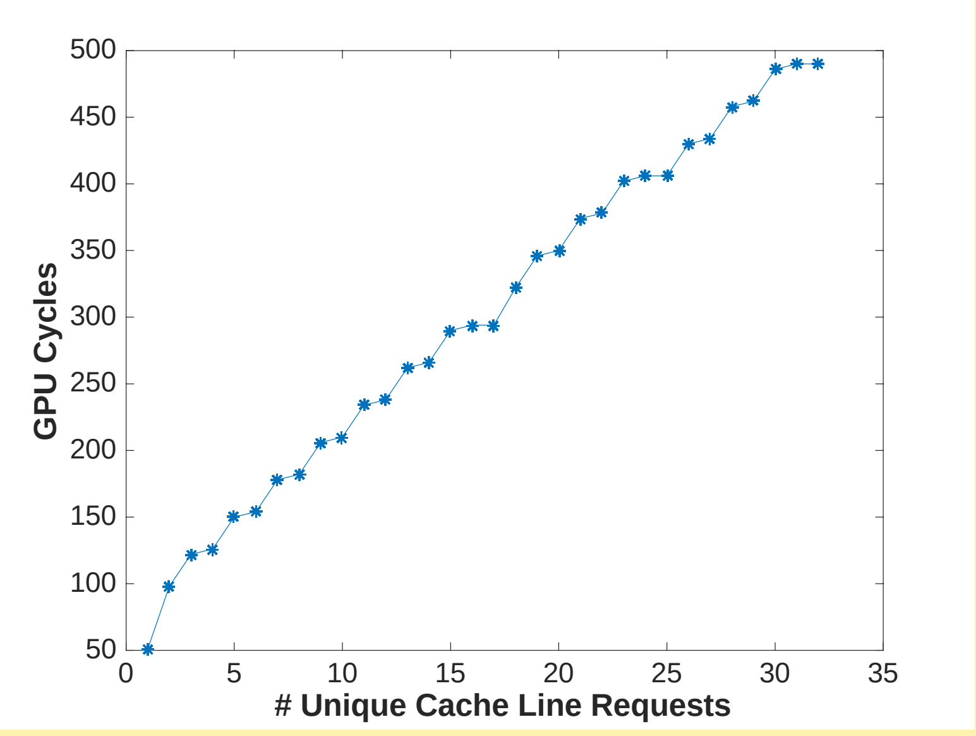
Side Channel Attack



→ Encryption → Measure time/ Power And Analyze →

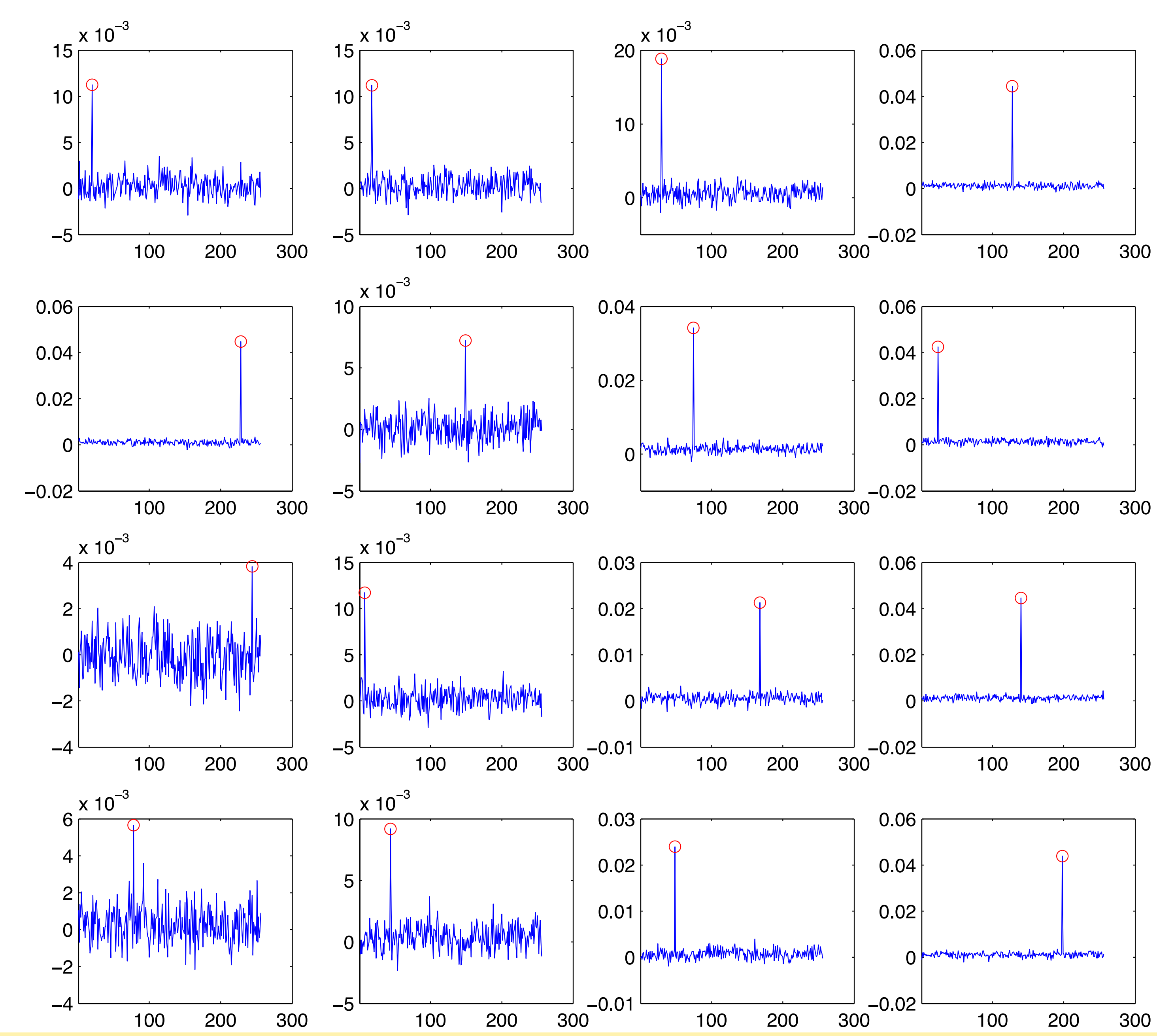
Timing Correlation Attack

- Identified a new GPU-specific timing channel - the coalescing unit
- Identified a linear relationship between SIMT load instruction execution time and the # of unique cache lines accessed



- Used one cipher text byte and one key byte guess to compute the number of unique cache line requests that would be generated during table lookup
- A strong correlation exists between the number of cache line requests and the total GPU encryption cycles
- Launched a successful differential timing attack on a GPU

Key Recovery through Timing Attack



Future Work

- Evaluating side-channel attack vulnerability on discrete GPUs, APUs and other accelerator devices such as Intel Phi
- In addition to timing and power analysis attacks, pursue electromagnetic emanation as an attack surface
- Explore additional encryption schemes (e.g., RSA)
- Develop resiliency against these attacks:
  - Explore software obfuscation approaches and address randomization on an accelerator
  - Hide timing leakage introduced by the address coalescing unit
  - Develop compiler-assisted modifications to address power and EM leakage
  - Design microarchitecture solutions that can obscure timing leakage

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

Northeastern