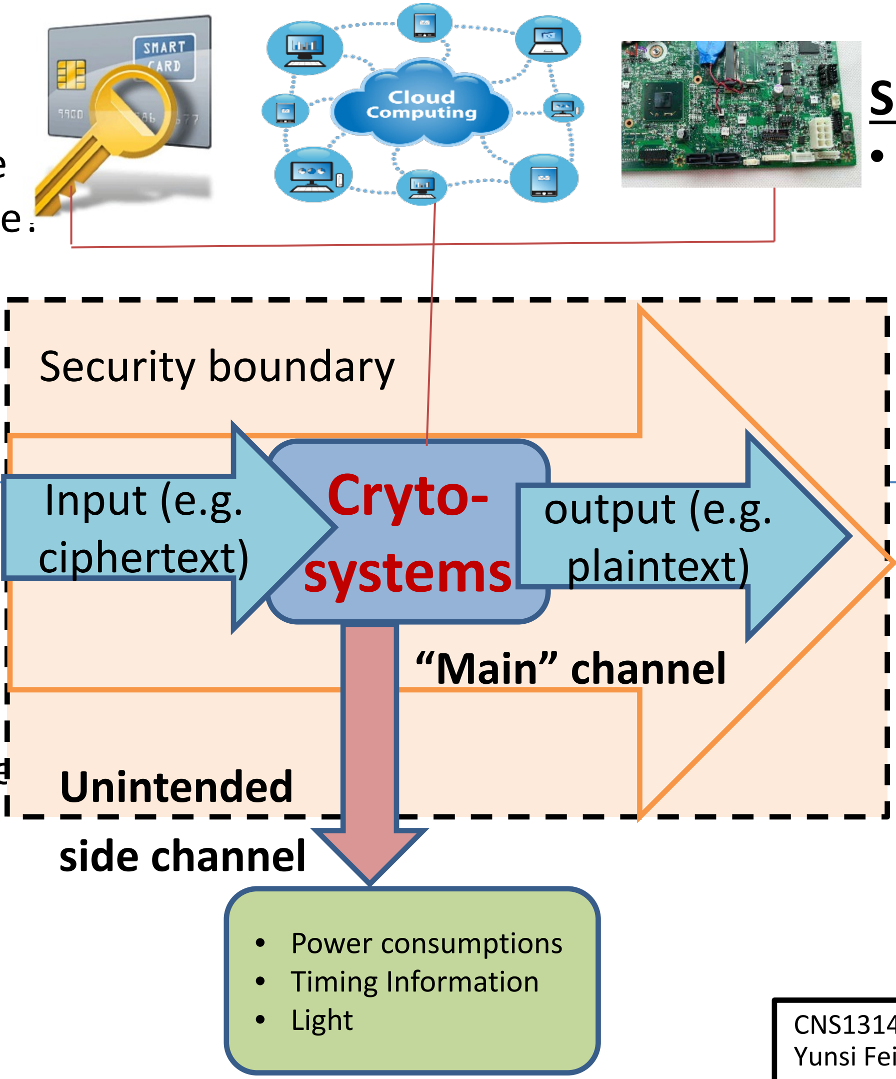
# Medium: A Unified Statistics-based Framework for Analysis and Evaluation of Side-channel Attacks in Cryptosystems

## Challenge:

- How to quantify the side-channel leakage?
- Fast and reliable evaluation of side-channel resilience.

## Solution:

- Through *confusion analysis* to establish accurate quantitative formula for the strongest side-channel analysis.
- Provides insight on how various components contribute to side-channel leakage.



Security boundary

Input (e.g. ciphertext)

Cryto-systems

output (e.g. plaintext)

“Main” channel

Unintended side channel

- Power consumptions
- Timing Information
- Light

## Scientific Impact:

- Easier accurate evaluation of physical system resilience against side-channel attacks on various crypto algorithms: DES, AES, Keccak, etc.

## Broader Impact:

- Synergies between statistics and side-channel security
- New graduate level computer hardware security course with industry students from industry

CNS1314655, Northeastern University,
Yunsi Fei and Aidong Adam Ding
{y.fei, a.ding}@northeastern.edu