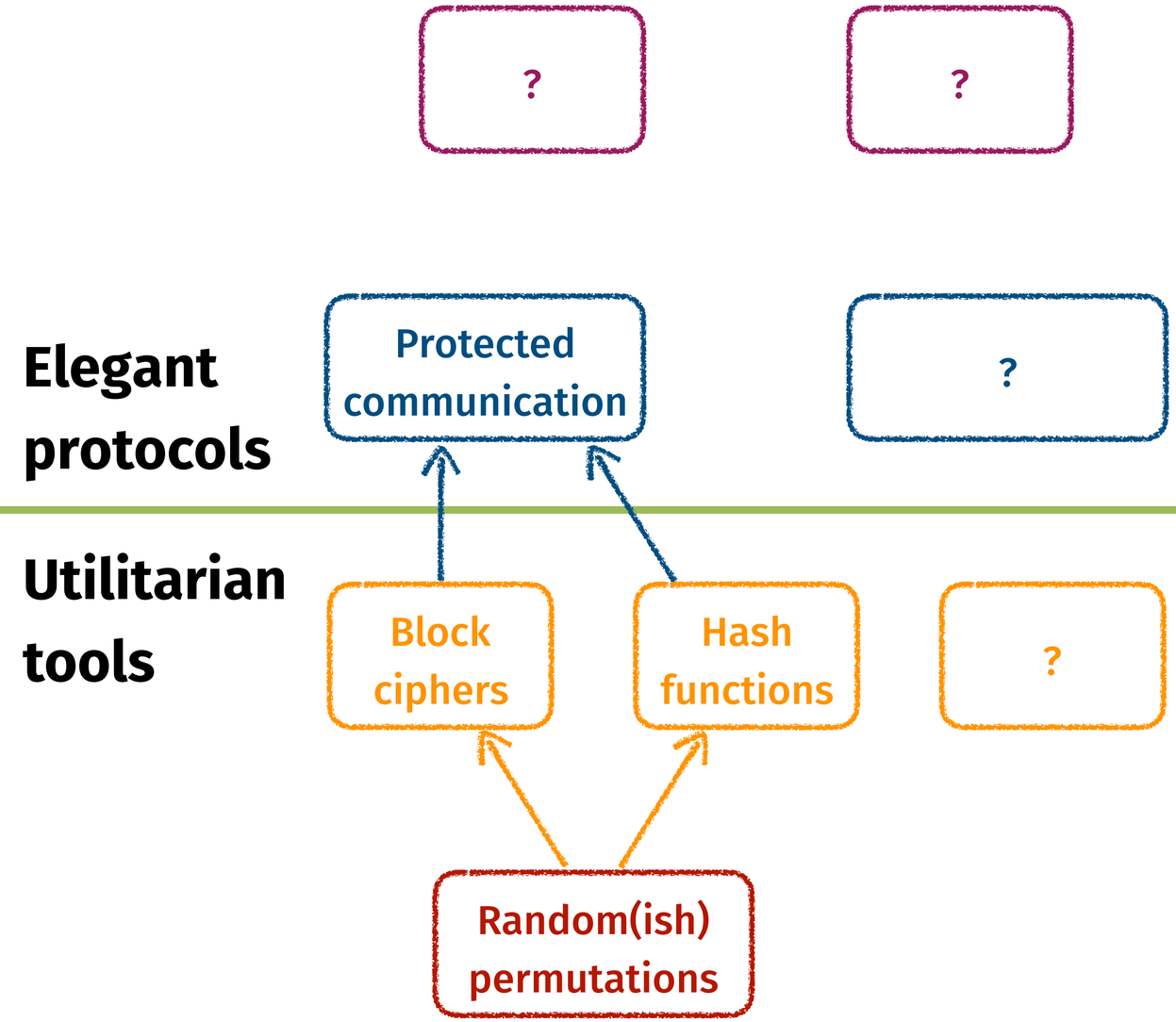
Lecture 9: Power analysis

- Midterm has been graded
  - Available on gradescope.com
  - Median grade = 88
- Lab 5 follows an unorthodox schedule
  - Posted this Thursday 2/28
  - Due next Friday 3/8 (just before spring break)
- (Moved my office hours this week to Tuesday afternoon)

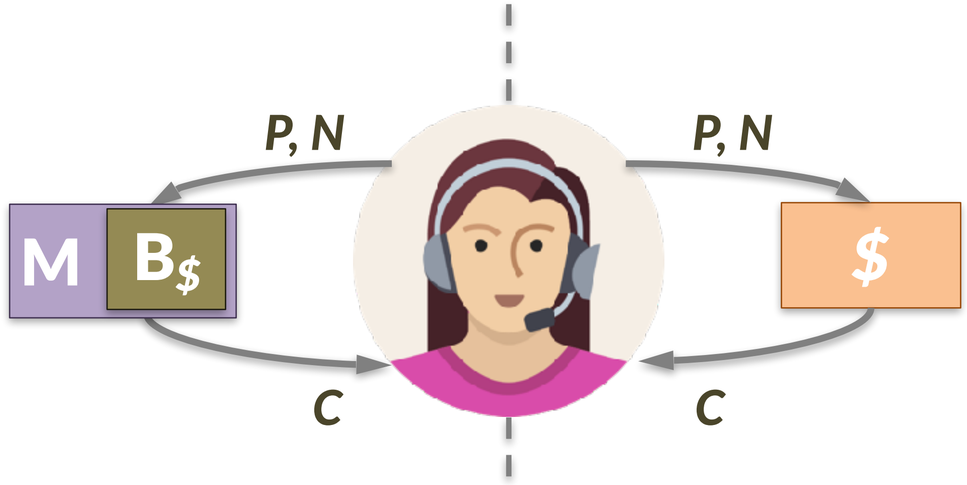
Course roadmap



Part 1: Privacy *XOR* authenticity

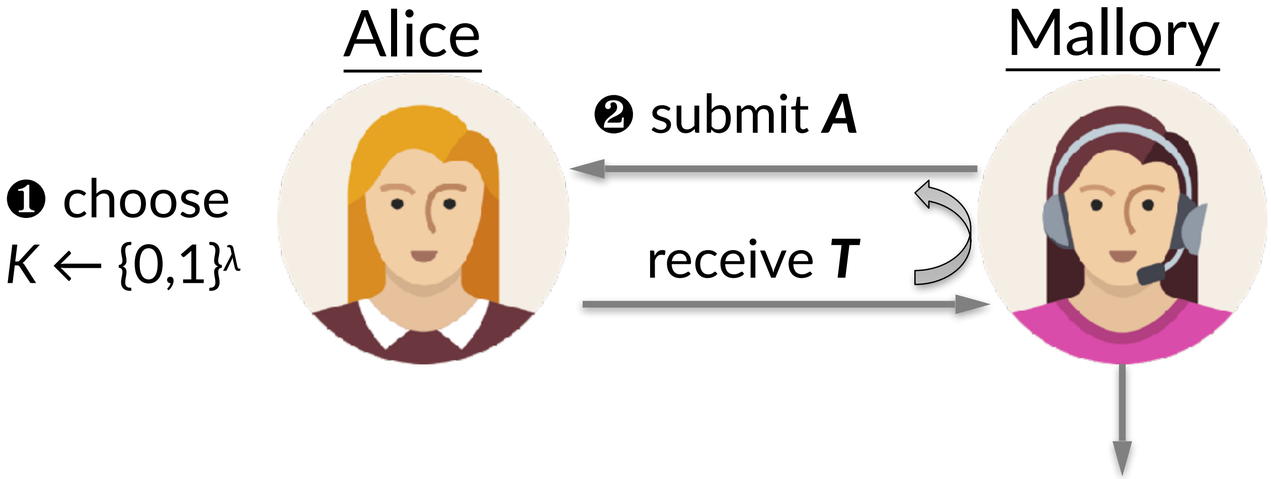
Privacy

IND$-CPA against
nonce-respecting Eve



Authenticity

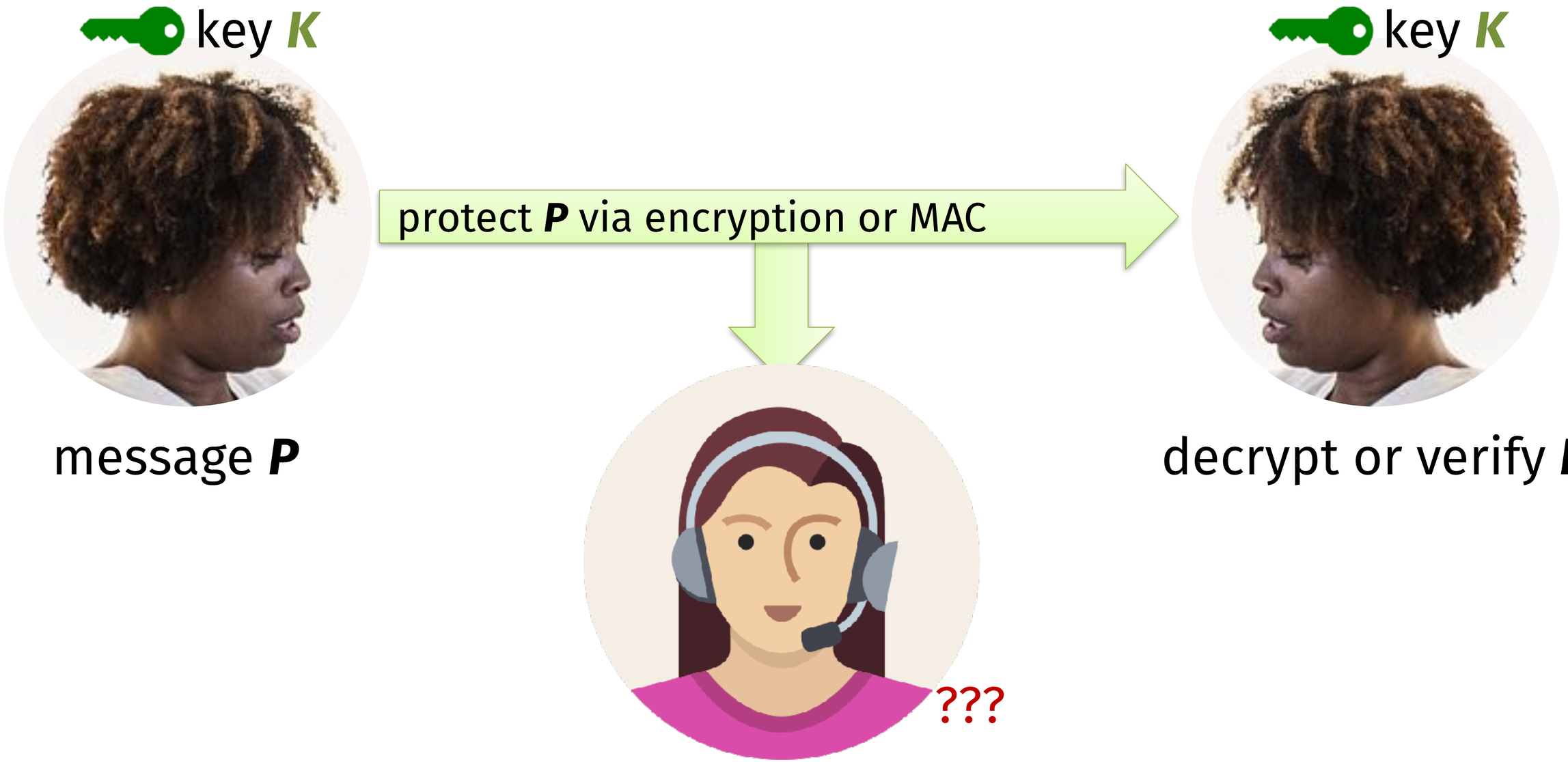
Even after viewing many (***A***, ***T***) pairs,
Mallory cannot forge a new one



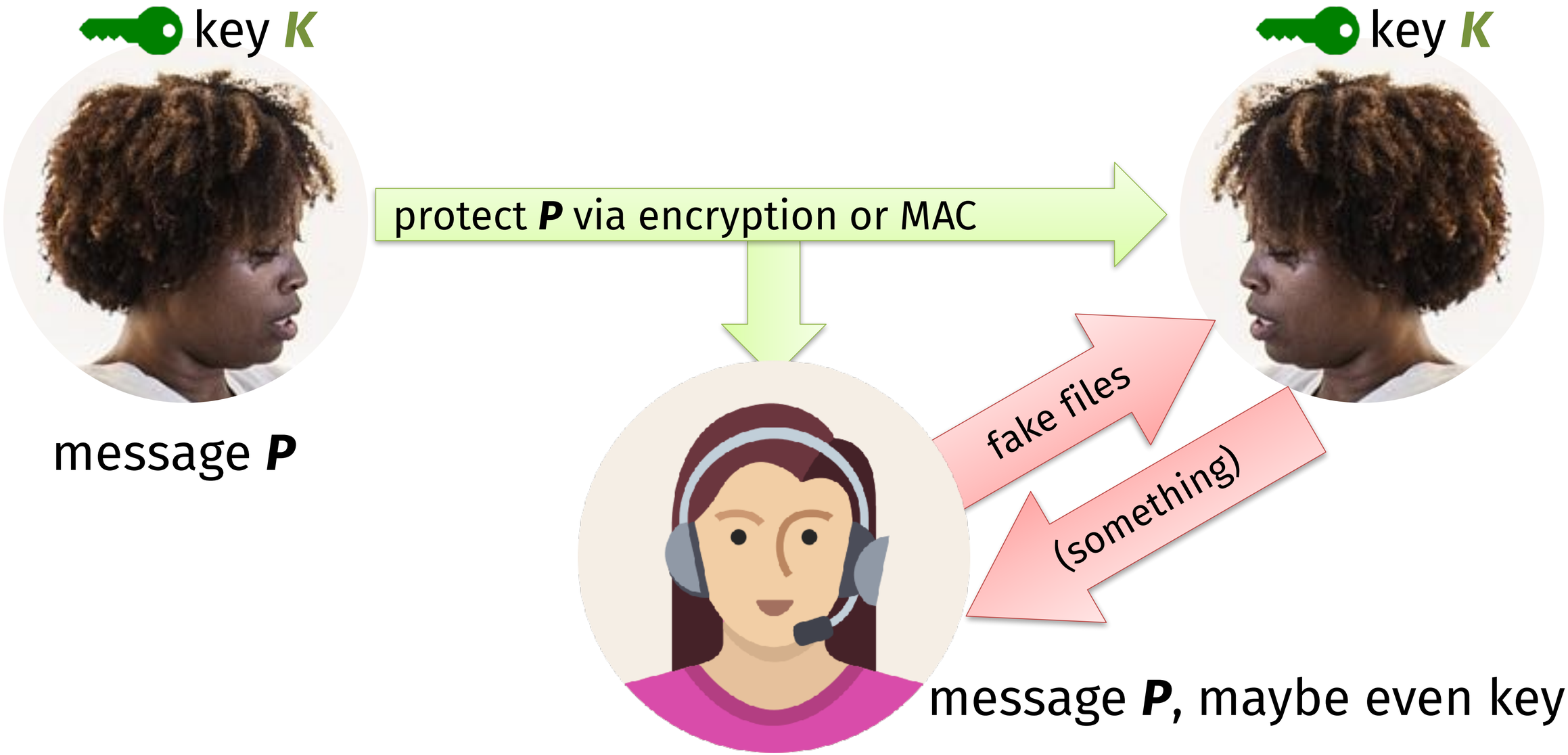
Mallory wins if:

1. It's a valid forgery
2. It's new

Part 1: Protecting data at rest



Part 2: *Breaking* data at rest



Crypto = Scientific field at intersection of many disciplines

Algorithms

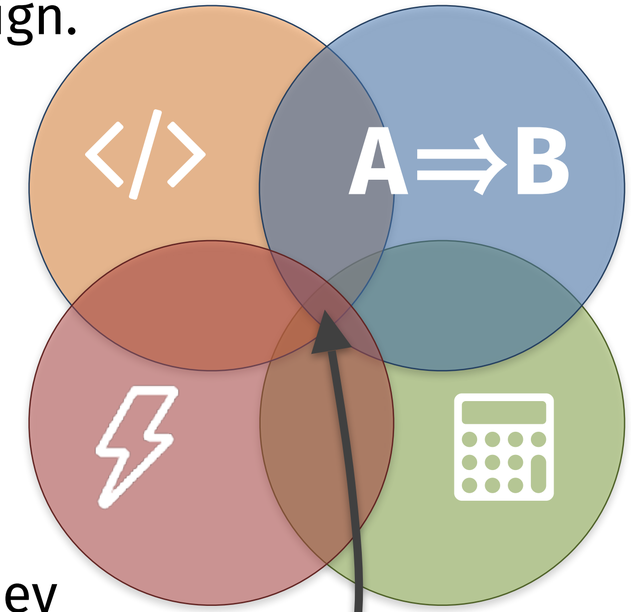
Known for cipher design.

Primarily found in European academia.

Complexity theory

Known for reductions.

Primarily found in American academia.



Engineering

Known for software dev and side channel attacks.

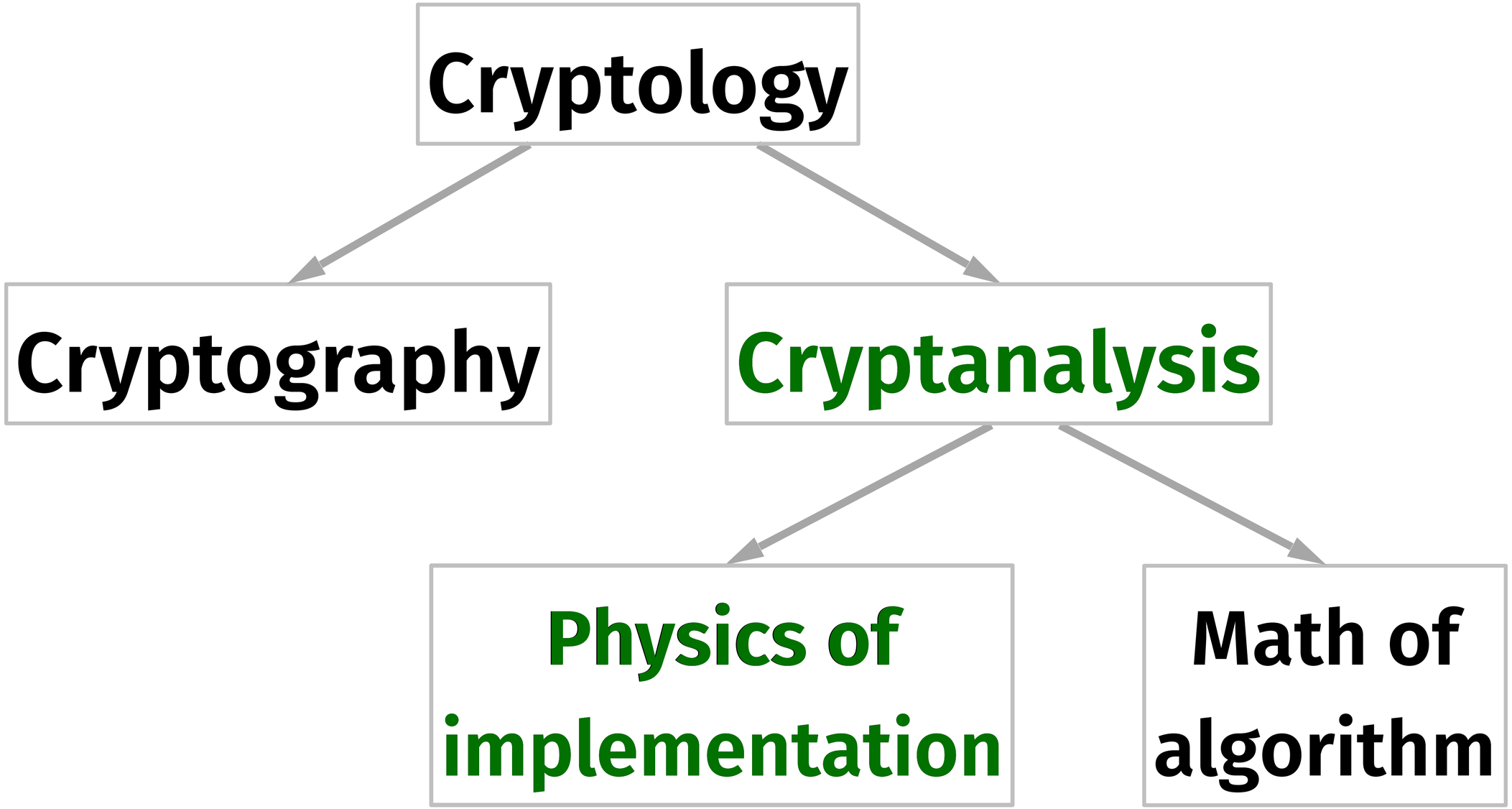
Primarily found in industry.

Mathematics

Known for cryptanalysis.

Primarily found in government.

This class

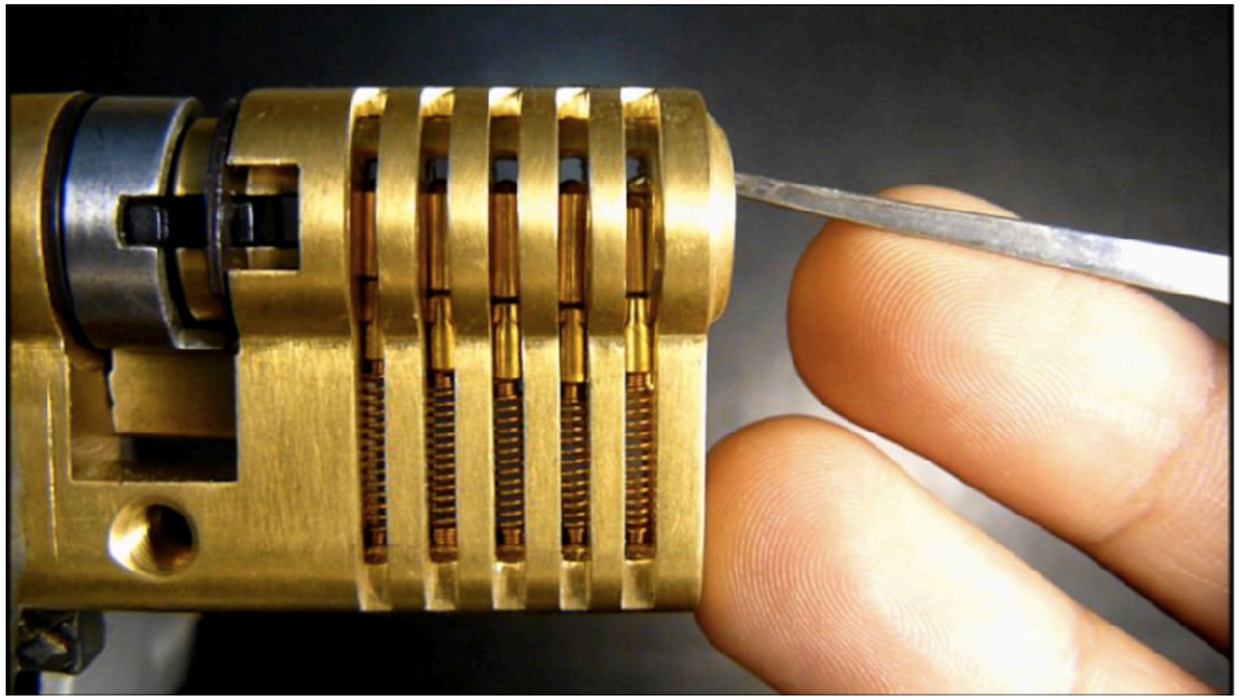

Cryptology
Cryptography
Cryptanalysis
Physics of implementation
Math of algorithm

Side channel attacks on crypto implementations

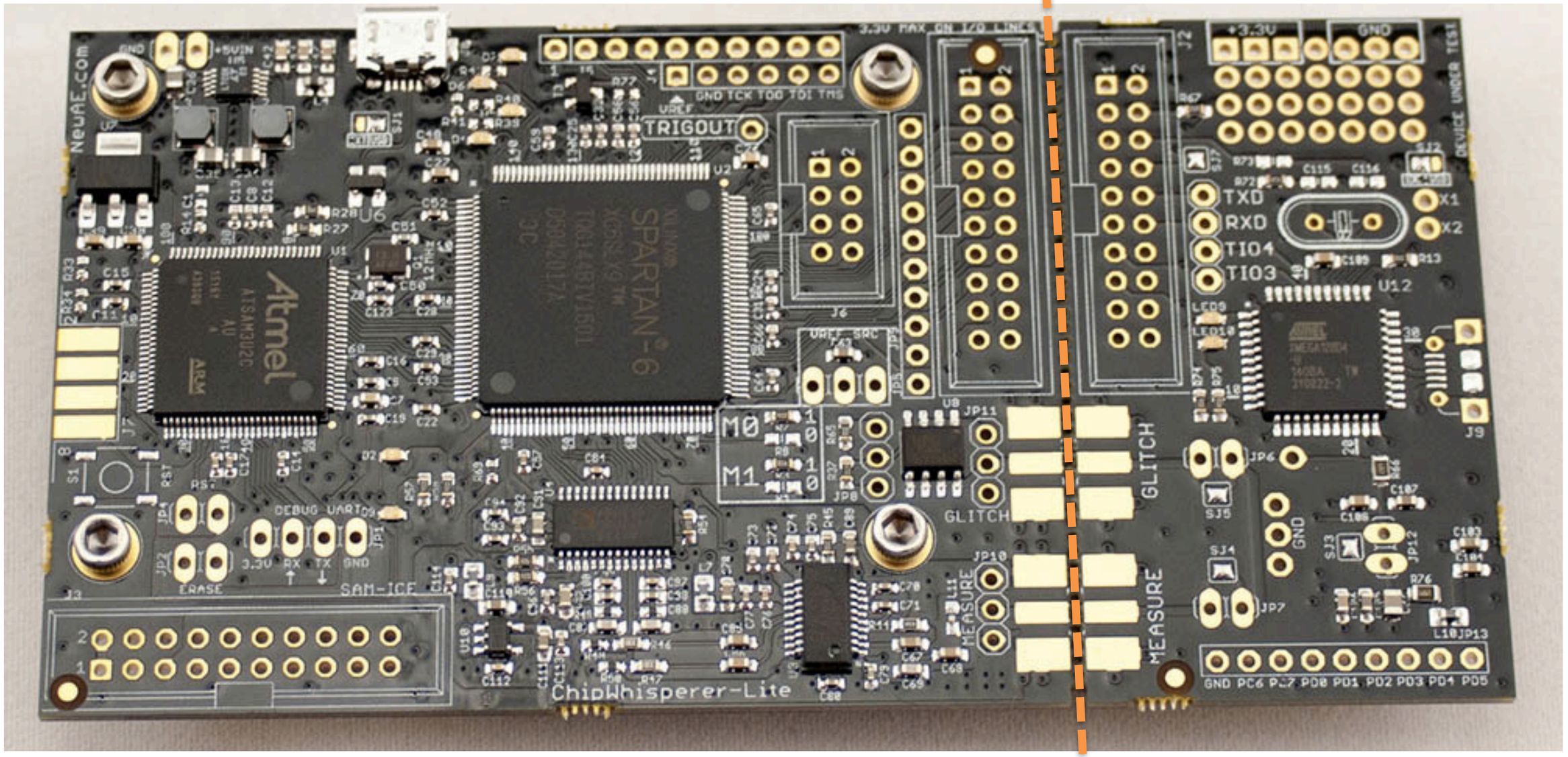
- So far, we have analyzed the security of cryptographic algorithms
- Security definitions ensure that a cryptosystem's output is "harmless"
  - EU-CMA: cannot forge tag, even if you see tags for prior messages of your choice
  - IND$-CPA: ciphertexts look effectively random, even if you choose the messages
- But, implementations of crypto can reveal more than its desired outputs
- Collectively we refer to these issues as *side channels*: they're potential channels of information that are outside of our definitions

Side channel attacks on crypto

- *Issue:* Physical inspection of a device can reveal more than its outputs
- *Sources of extra information:* power, sound, optics, time, cache, errors, network, …
- *Environments to attack:* PC software or hardware devices (less noisy)
- *Method of attack:* divide and conquer



Let’s see this in action ourselves

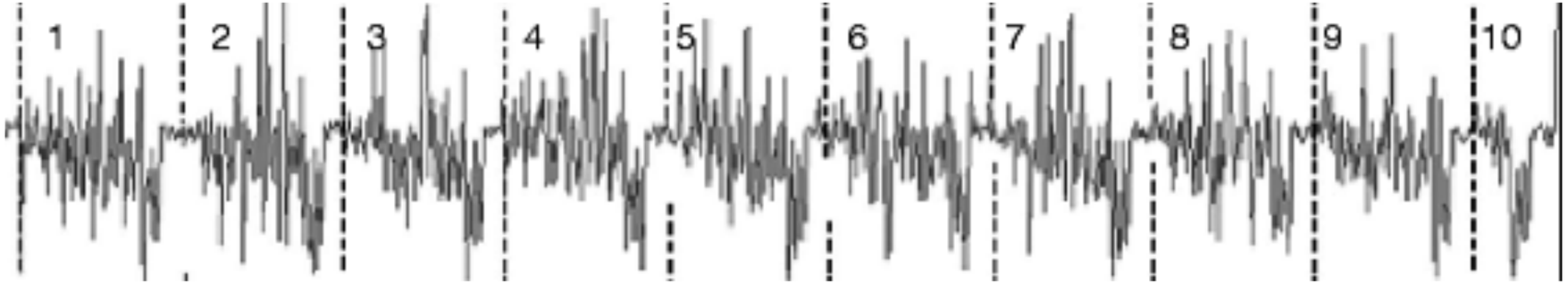


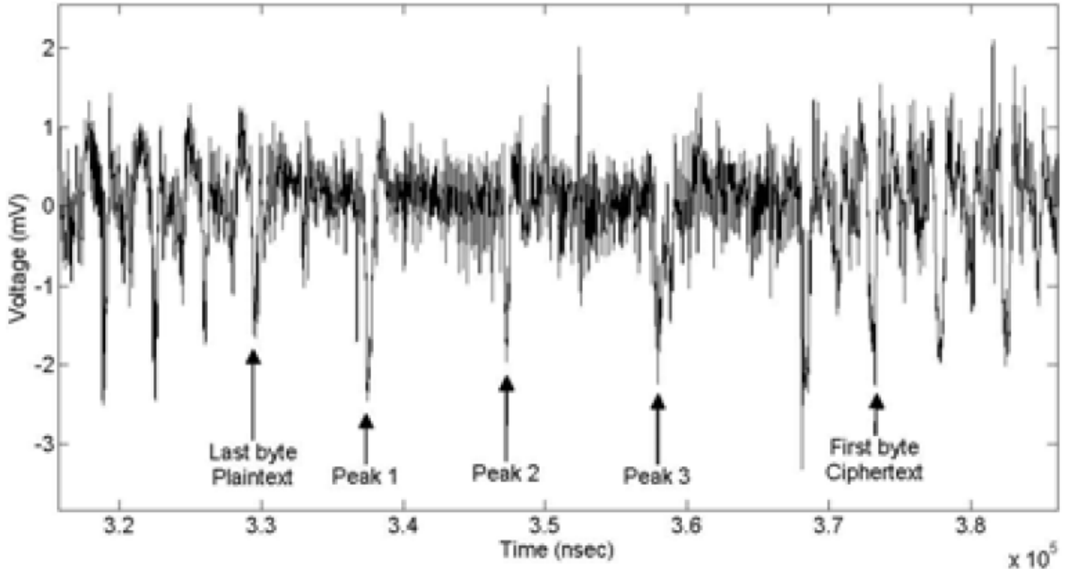
Attacker: oscilloscope to measure power

Target victim: FPGA that runs AES

Simple power analysis (SPA)

A single power trace can potentially reveal cryptographic information



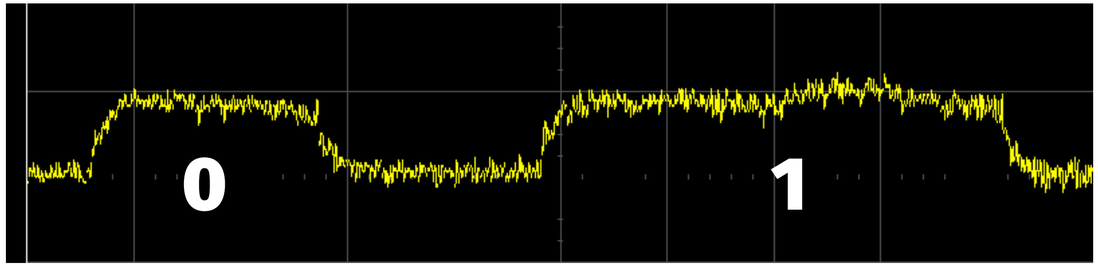


Simple power analysis (SPA)

Power consumption can depend on state, even secret state!

RSA square and multiply

```
x = C
for i = 1 to n
    x = mod(x^2, N)
    if k_i == 1 then
        x = mod(x · C, N)
return x
```

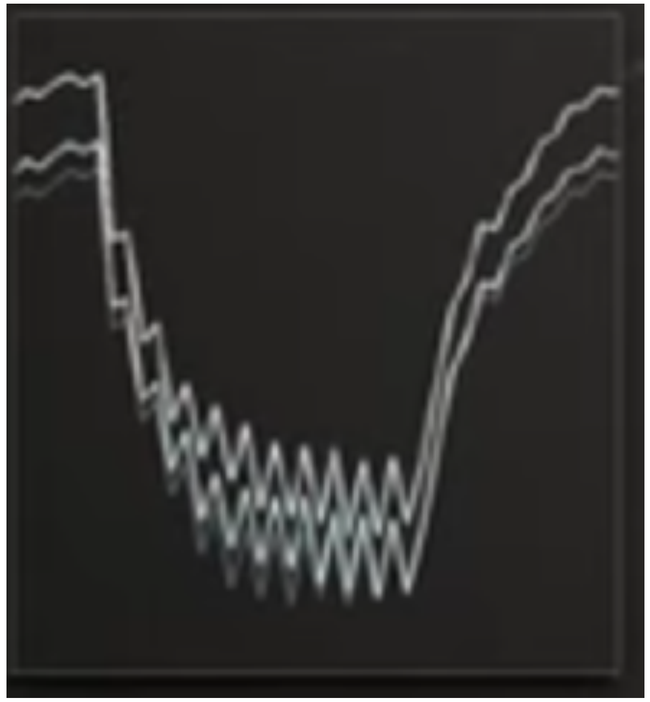


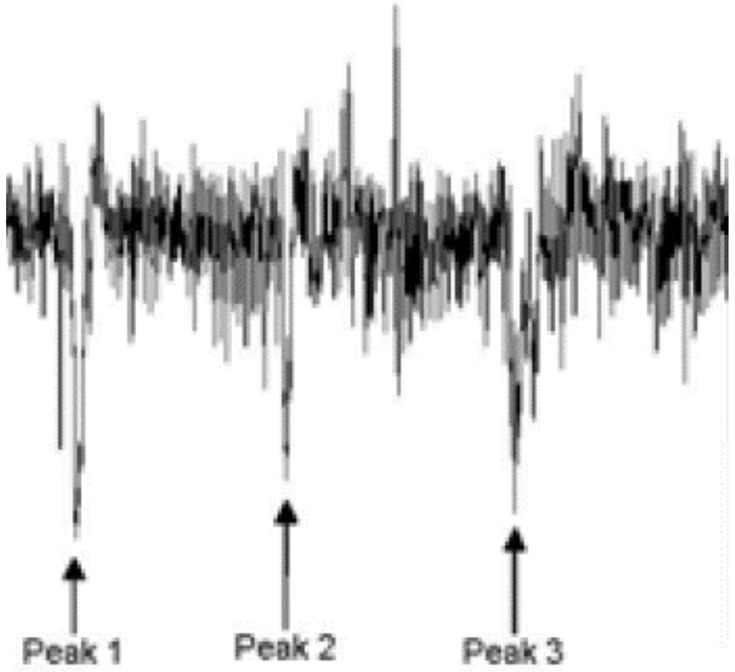
← Does work conditioned on 1 bit of secret key *K*

Lesson: never write crypto code that conditions on secret data!

Differential power analysis (DPA)

Subtle data-dependent differences in power consumed on different messages

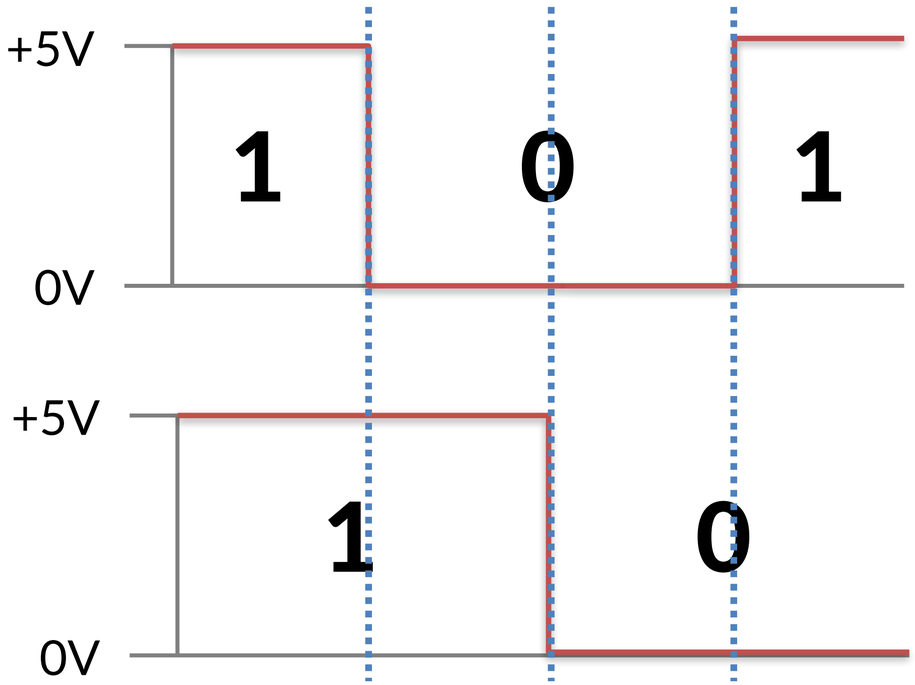




What consumes power, anyway?

Power consumed in transmission

- For each wire on a data bus, store a logical 0/1 as the voltage of the wire
- Power consumed ~ Hamming weight

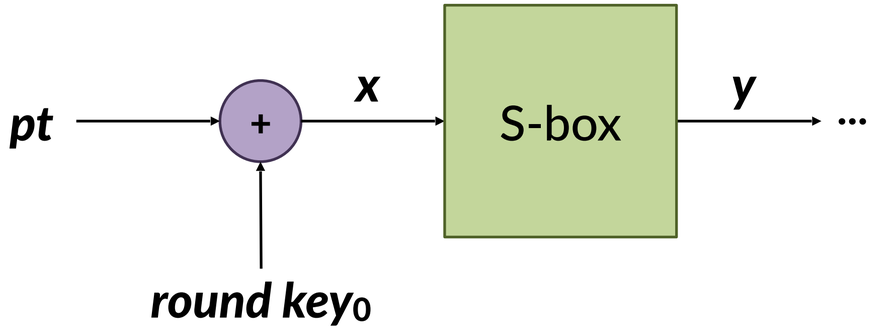


Power consumed in storage

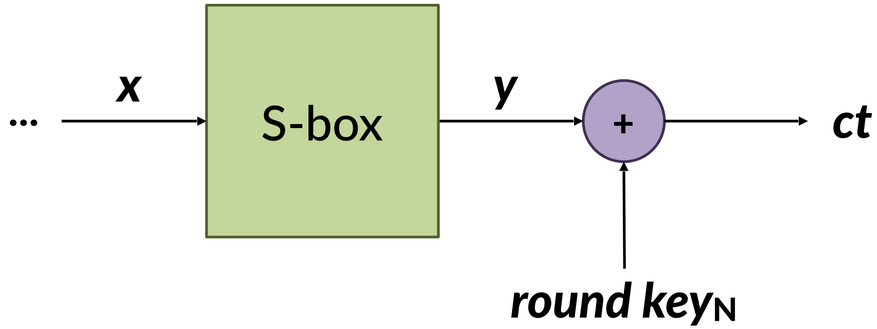
- Designed only to consume power during transitions 0 → 1 or 1 → 0
- Power ~ Hamming distance

Power analysis on AES

First round of AES:



Last round of AES:



Mallory can compute key from:

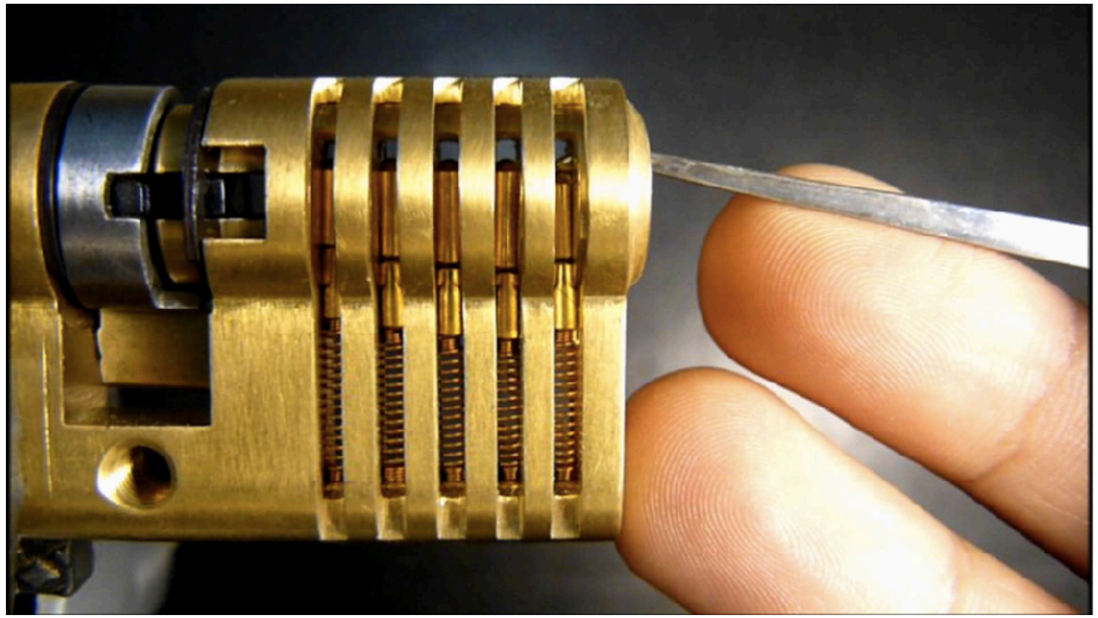
- Known *pt* (don't need to choose)
- Either *x* or *y* (they're equivalent)

Changes to attack the last round:

- Known *ct* rather than *pt*
- Learn last round key rather than 1st round key (they're equivalent)

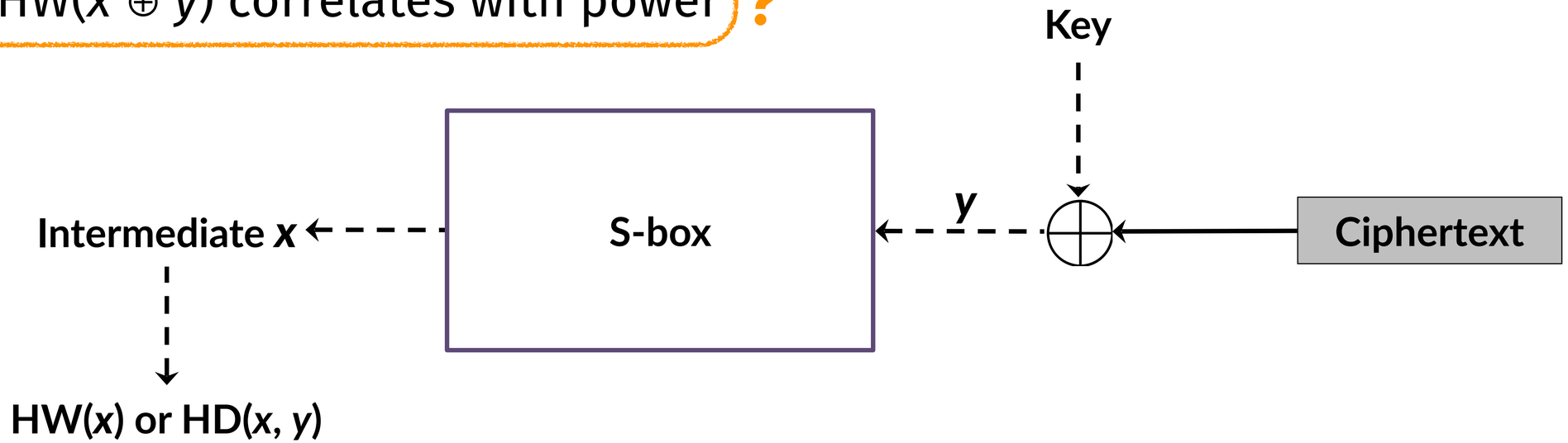
Divide and conquer

- Break 1 byte of the message or key at a time
- For each byte: guess all 256 values and check which works
- (Think: how you see crypto broken in any Hollywood movie)



Attack methodology on (simplified) final round of AES

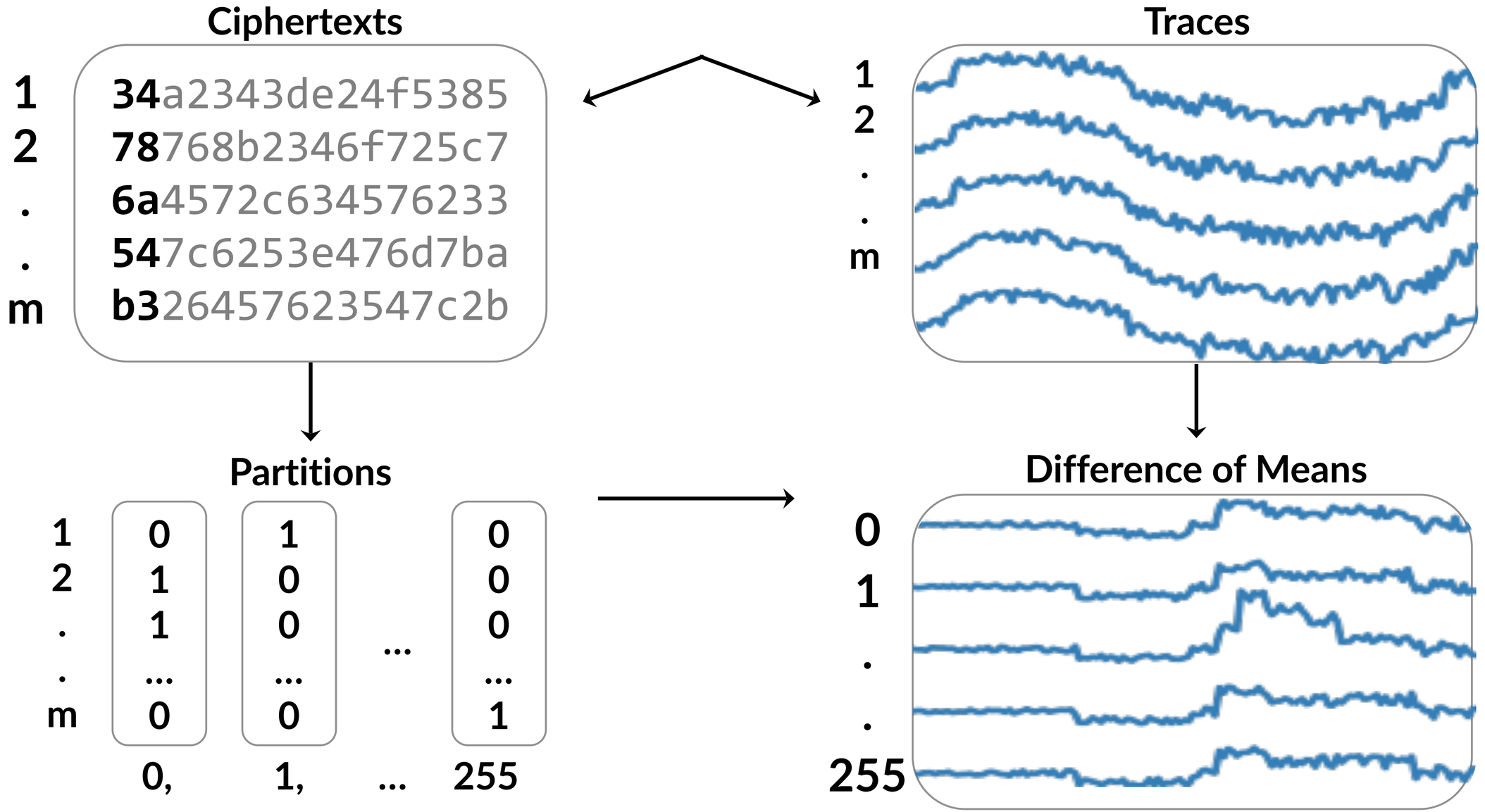
1. Guess *one byte* of the key
2. Compute the resulting byte of intermediate value x
3. Hope HW(x) or HW($x \oplus y$) correlates with power ?



Notes

- Can attack first round similarly, with known plaintext
- With power side channels, easy to isolate the signal for each round

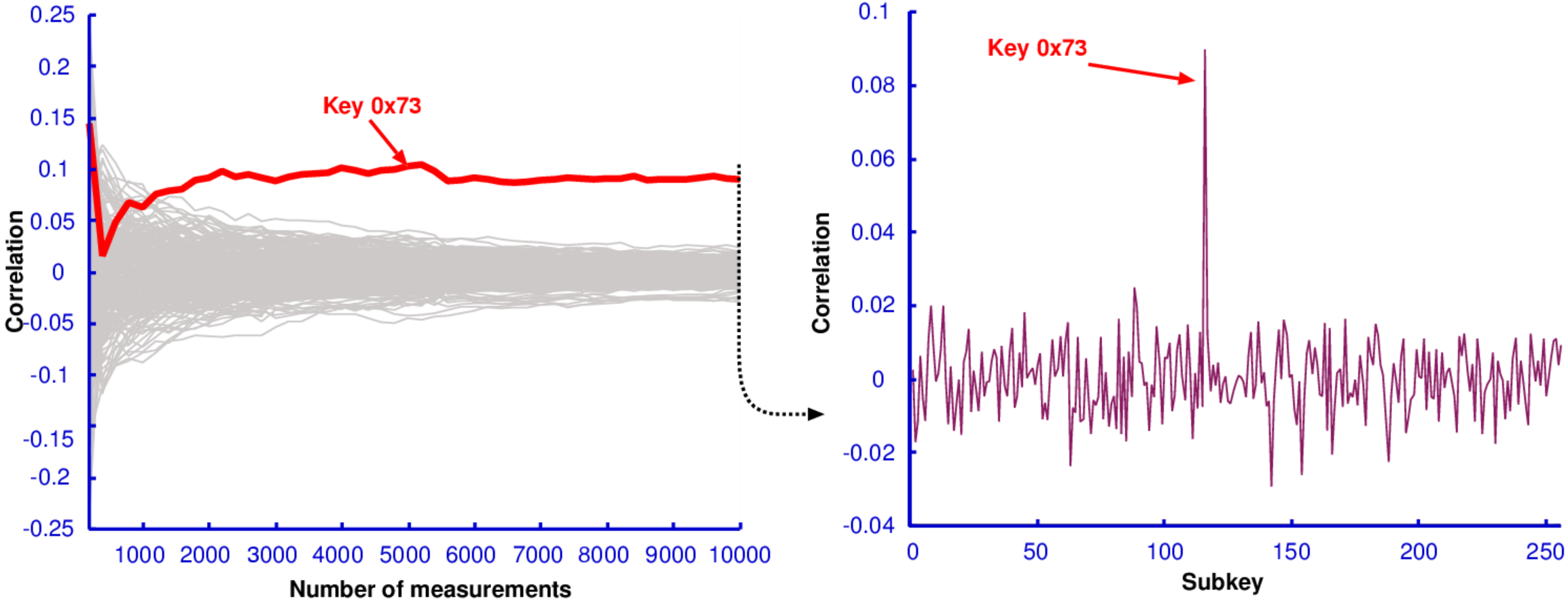
Differential Power Analysis (DPA)



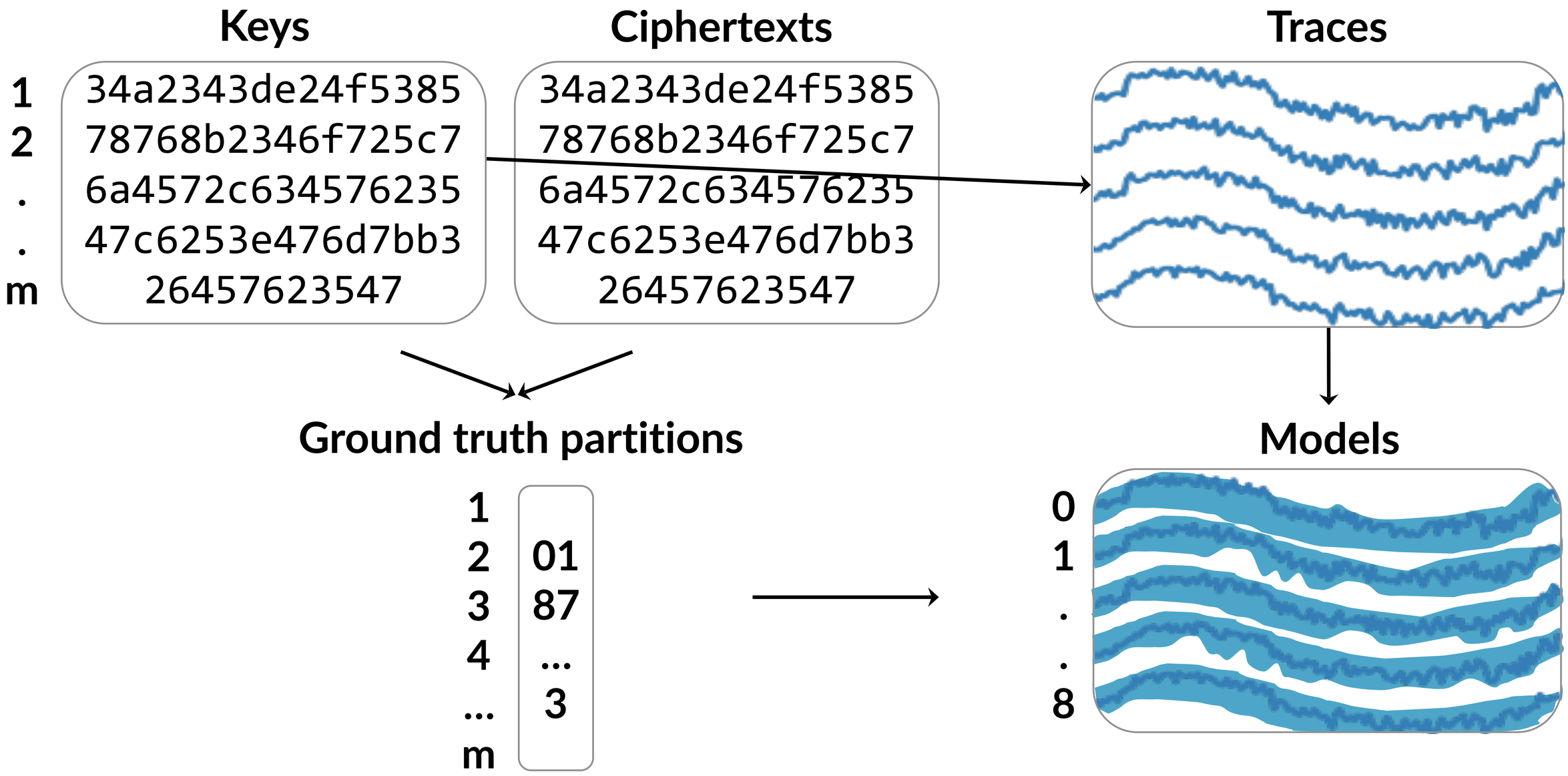
Kocher, Jaffe, and Jun, “Differential power analysis,” CRYPTO 1999.

DPA Example

Note: correlation of incorrect keys fades quickly with additional samples

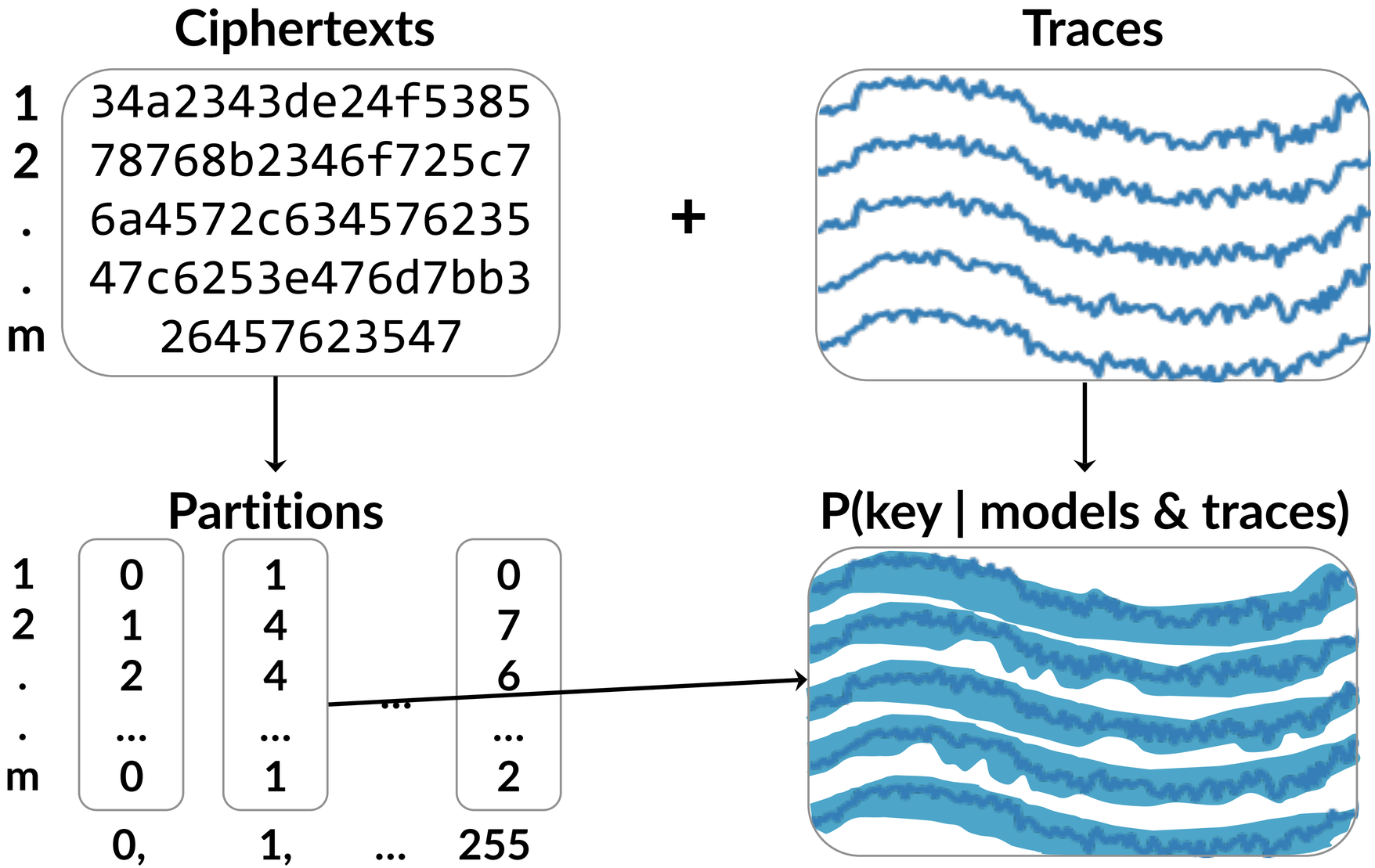


Template Attack: Profiling Phase



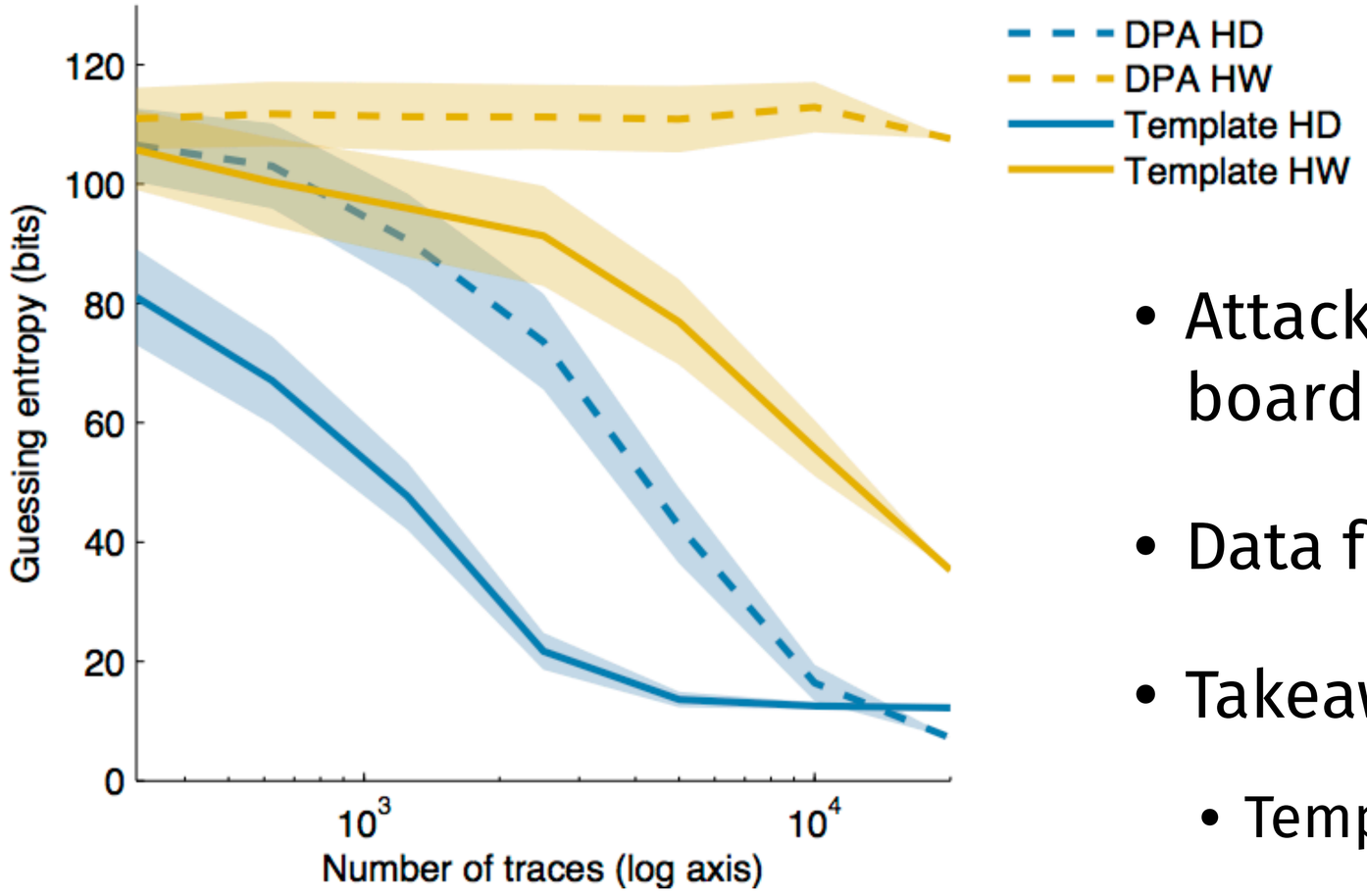
Chari, Rao, and Rohatgi. “Template attacks,” CHES 2002.

Template Attack: Attack Phase



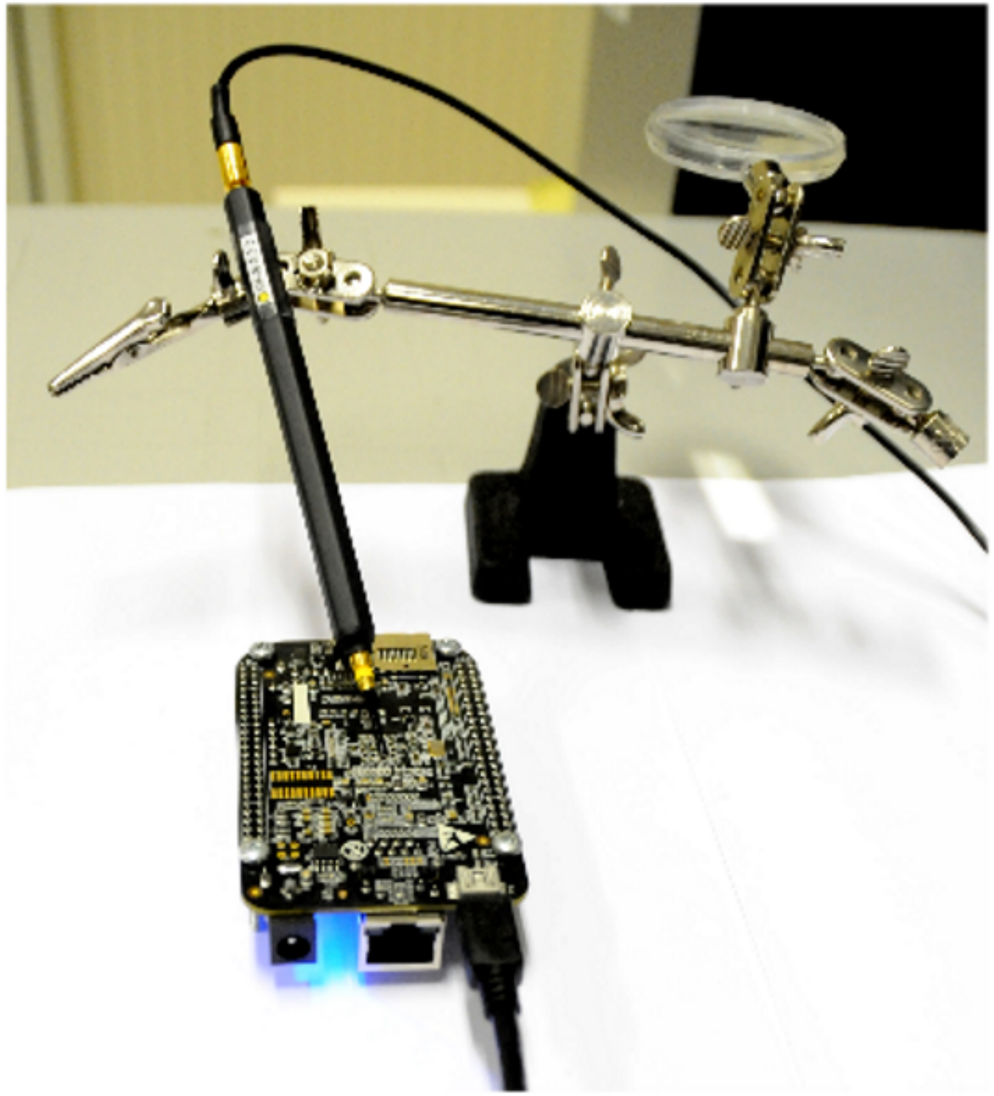
Chari, Rao, and Rohatgi. “Template attacks,” CHES 2002.

How well do power attacks work?



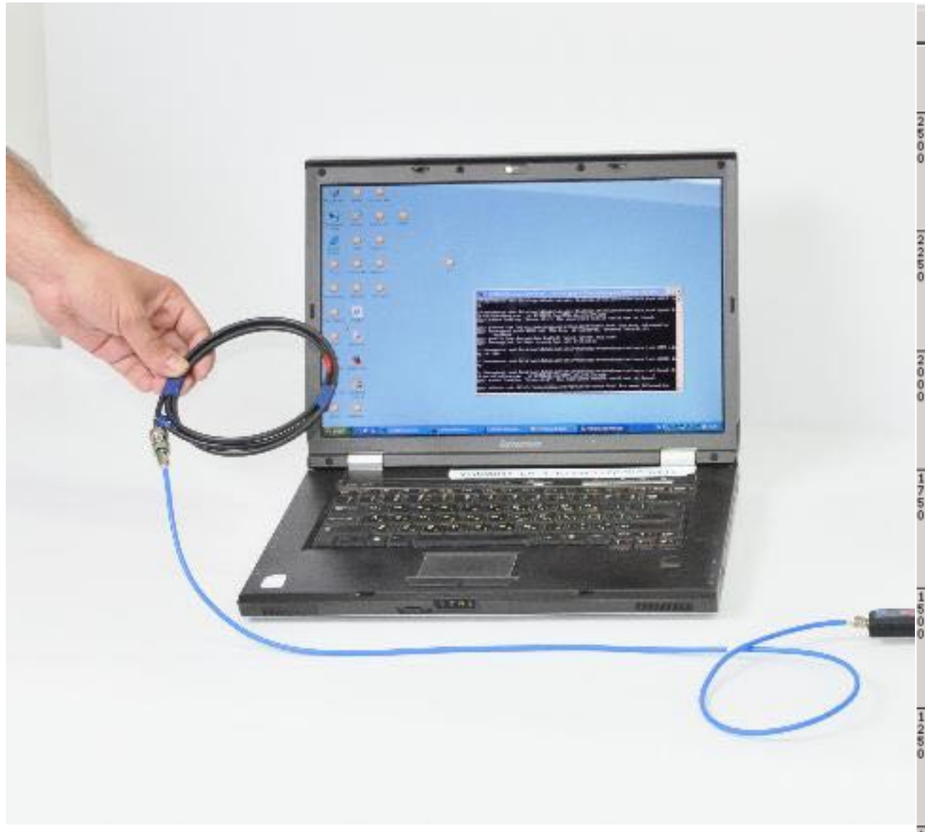
- Attack profiled on a SASEBO-GII board with a Virtex-5 FPGA
- Data from dpacontest.org/v2
- Takeaways
  - Template > DPA
  - Hamming distance > weight

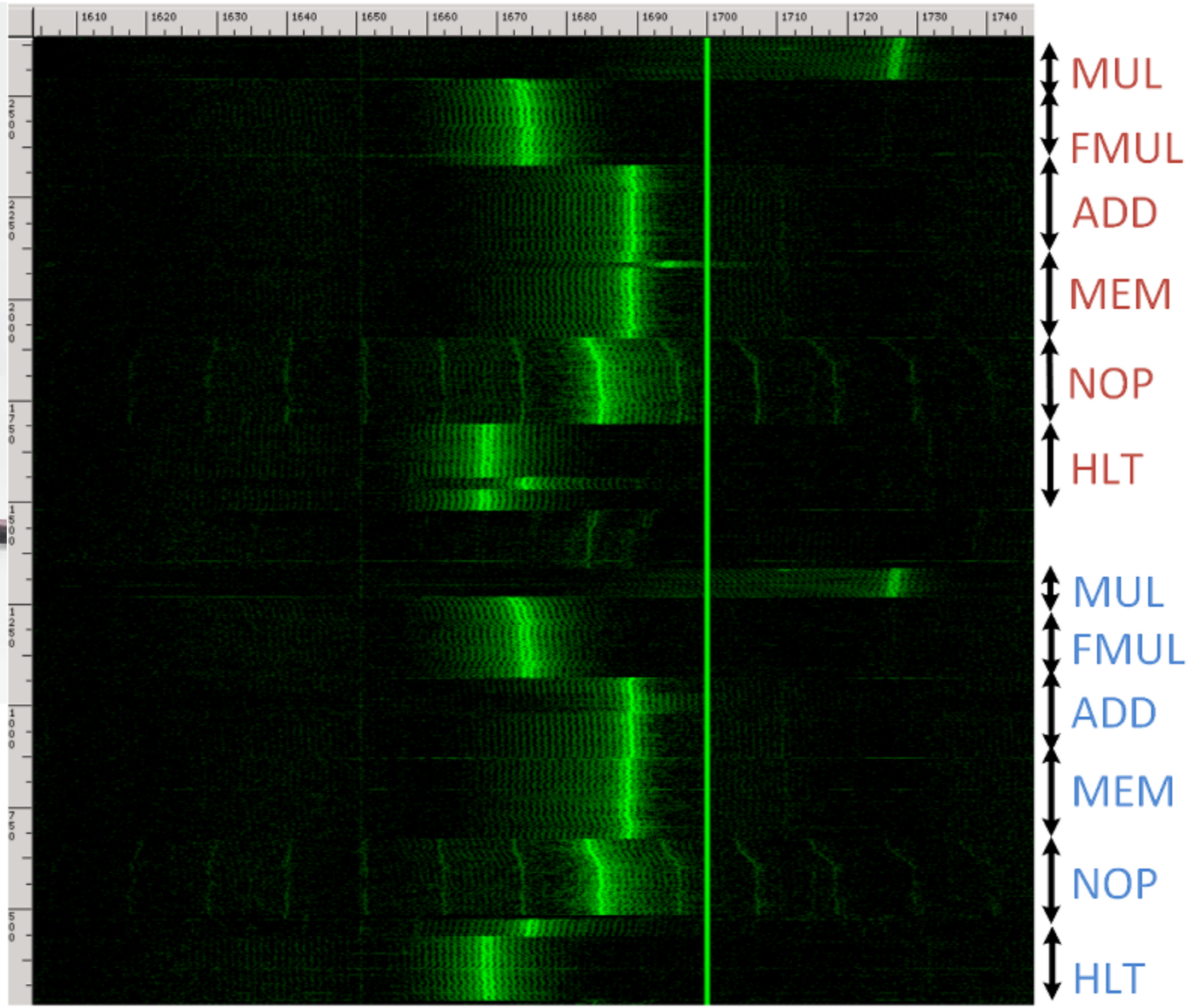
Alternatives: Electromagnetic probes



- Obtain data “similar” to power traces
- Can localize measurement to the unit performing crypto within a circuit board

Alternatives: Electromagnetic probes





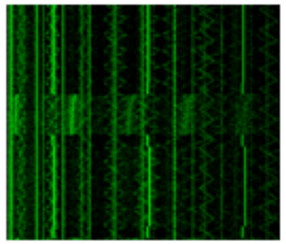
In the public key setting, even a low-frequency probe will do.

Can “see” differences in CPU instructions.

Alternatives: Electromagnetic probes

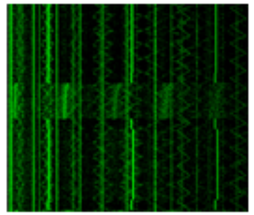
Can target a victim from a distance!

Alternatives: Chassis potential



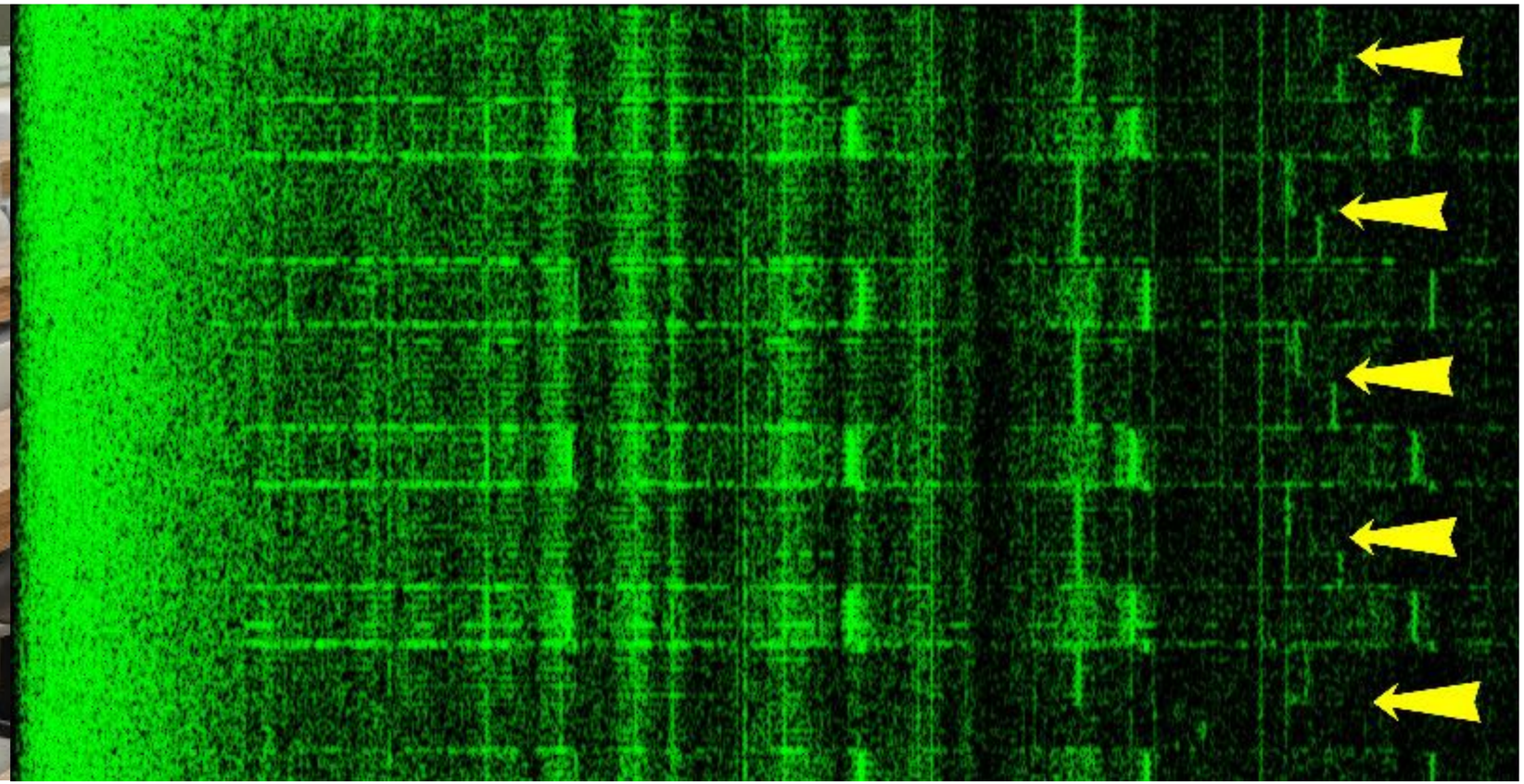
Key = 1110111011…

Alternatives: Chassis potential

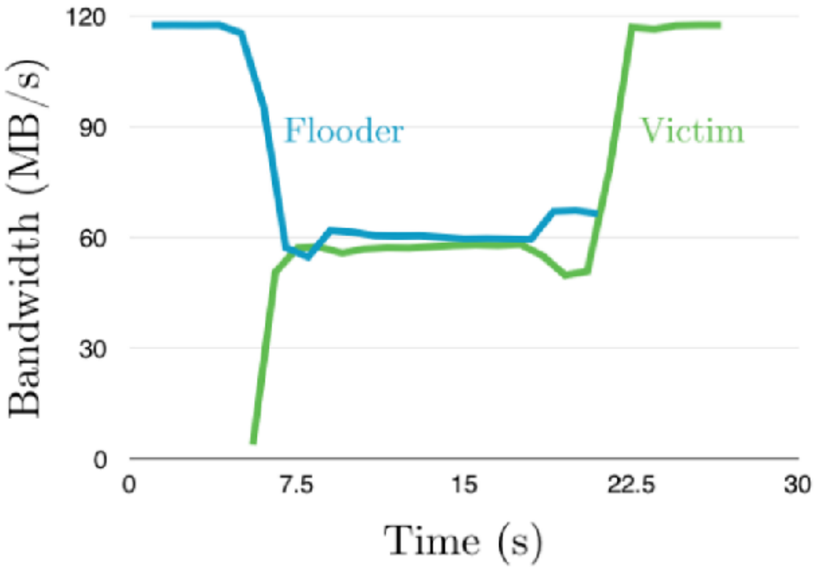


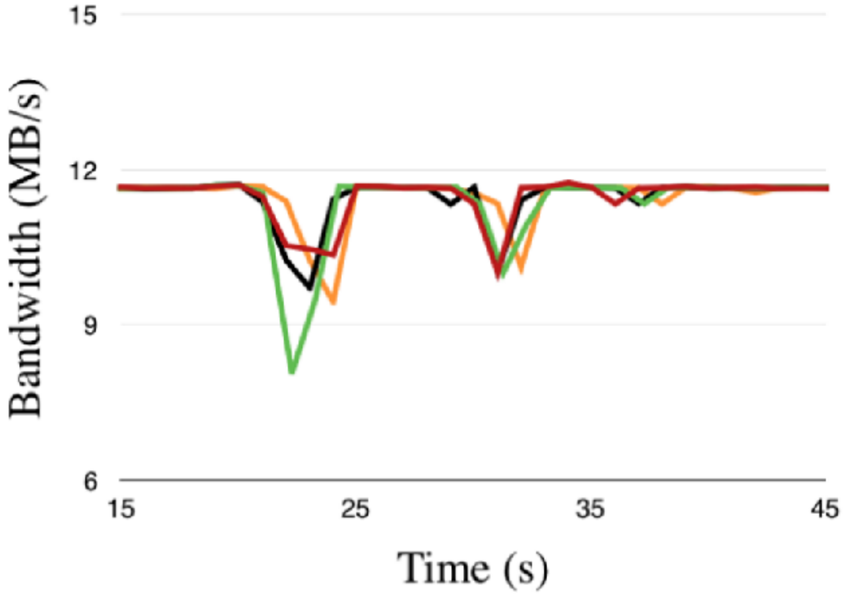
Key = 1110111011…

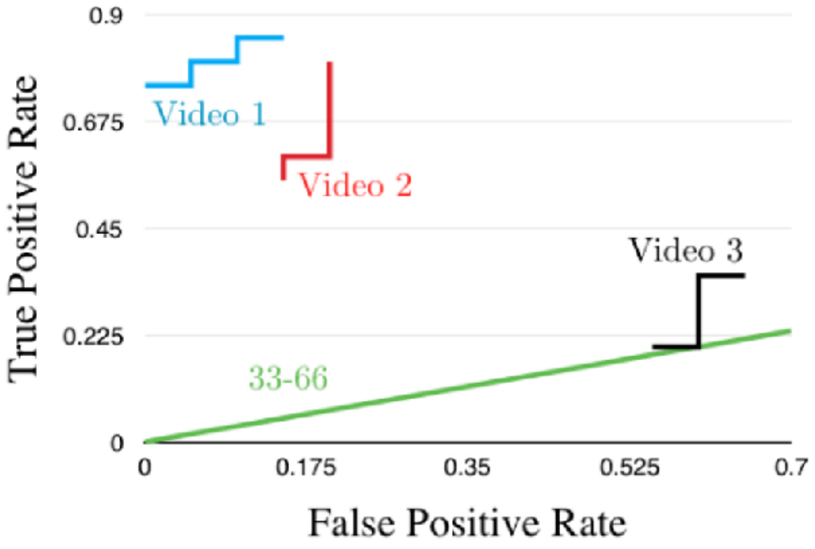
Alternatives: Sound



Alternatives: Network







Countermeasures to avoid power analysis?

- Eliminate Mallory's ability to see the power signal
  - *Shielding:* Physically enclose system so emanations cannot be captured
  - *WDDL:* For every 0 → 1 transformation, perform a mirror op 1 → 0
  - *ECC:* Perform ops directly over a const-weight error correcting code of data
- Eliminate Mallory's ability to make sense of the power signal
  - *Masking:* Split circuitry into pieces that can be recombined to construct output
  - *Variety:* Don't have just one S-box, but rather several so that x is unknown (chosen from a public set of S-boxes as per Kerckhoffs' principle)
  - …

Next time (pun intended)

Breaking AES in software if Mallory can observe its runtime