Security Vulnerabilities, Challenges and Opportunities in Hardware Design for IoT Devices

物联网设备硬件设计的安全隐患、挑战和机遇

Gang Qu

University of Maryland, College Park

2015 中国互联网安全大会

September 30, 2015

Hardware in Security and Trust

Evolving role of HW

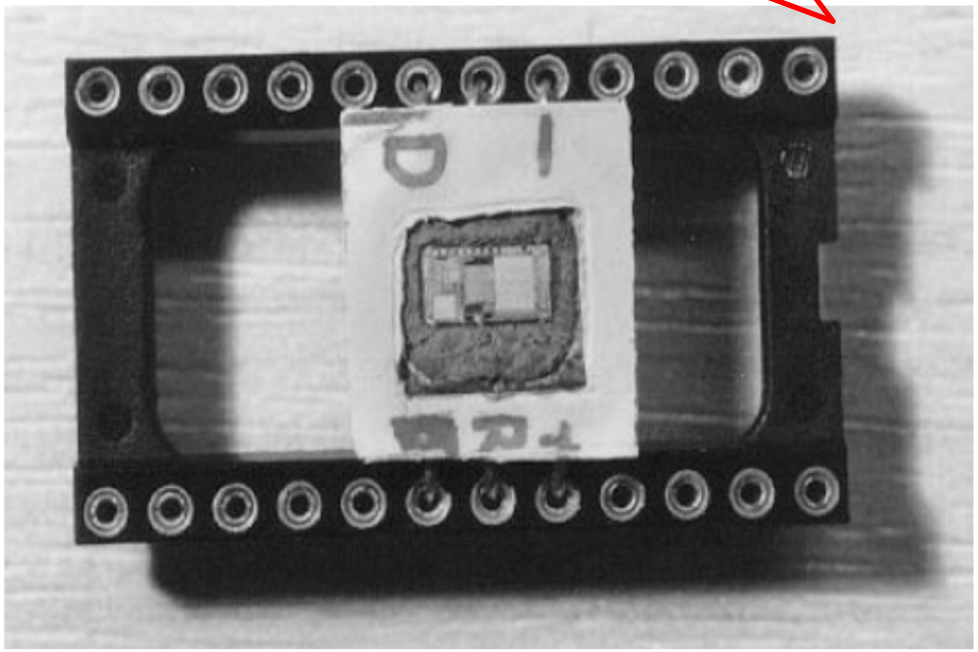
- Enabler
- Enhancer
- Enforcer

Be careful where you store the key

Physical Attacks

- Reverse engineering
- Side channel attacks
- Microprobing
- Fault generation
- Software attacks
- …

Be careful where you store the key



[Ross Anderson, Security Engineering 2001]

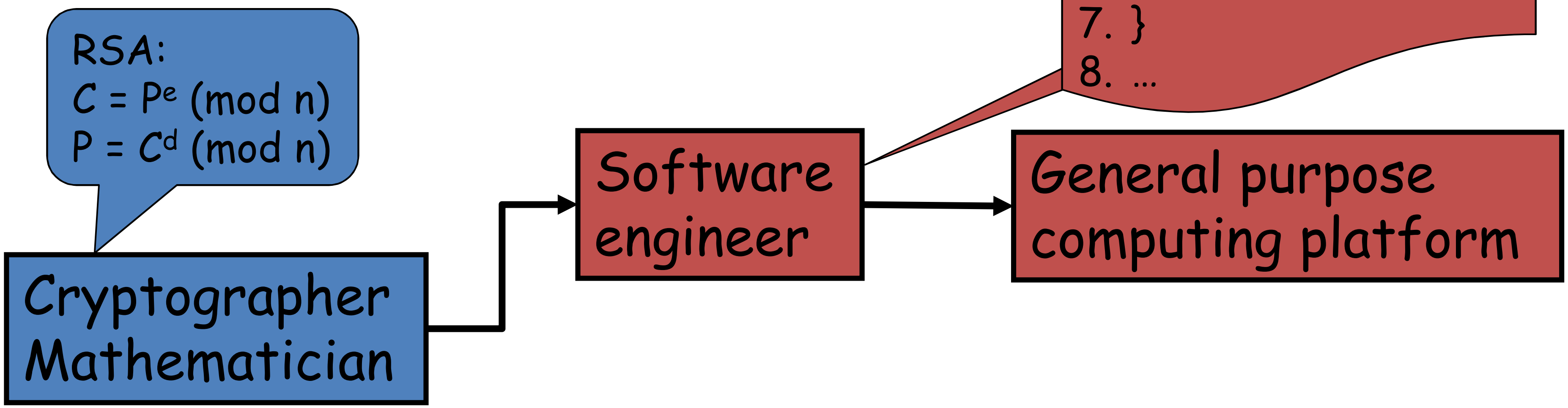
SCA: Attackers with Good Ears …

- Side channel analysis attacks:
  - Monitor/measure chip's physical characteristics during its normal operation
  - Perform data analysis to learn information
- Side channels:
  - cache memory, power/current, timing, scan chain, EM radiation, output signal …

Development of a Cipher

- Design and implementation of a cipher
  - Algorithm/protocol design
  - Software implementation

1. binary: $k_s k_{s-1} \ldots k_1 k_0$
2. b = 1;
3. for (i=s; i>=o; i--)
4. { b = b*b (mod n);
5.   if (k_i == 1)
6.   b = b * a (mod n)
7. }
8. …



Modular Exponentiation: a^e (mod n)

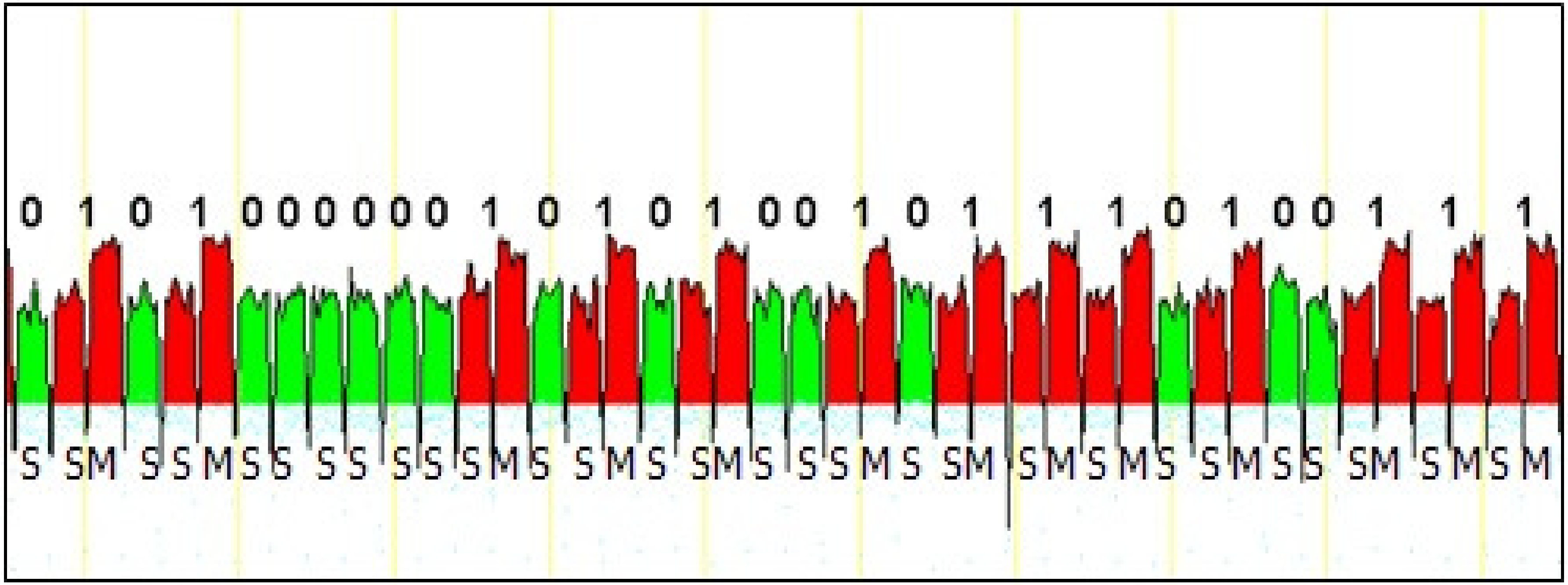
- Goal: Compute a^e (mod n)
  1. convert e to binary: $k_s k_{s-1} \ldots k_1 k_0$
  2. b = 1;
  3. for (i=s; i>=o; i--)
  4. { b = b*b (mod n);
  5. if (k_i == 1)
  6. b = b * a (mod n)
  7. }
  8. return b;

Side channel attacks!

Observable side channel info during hardware execution: current, power, timing, …

The value of bit k_i determines whether this non-trivial operation will be required.

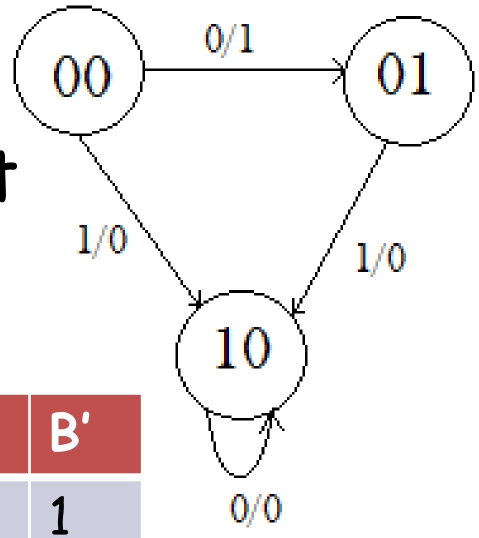
Power Analysis Attacks



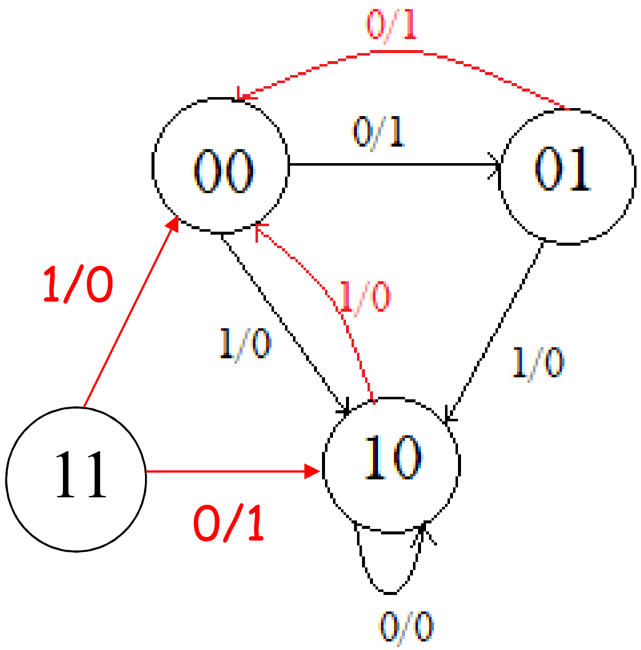
http://www.eetimes.com/document.asp?doc_id=1278081

Security comes by design, not by default!

Trust in Hardware Design



What I want

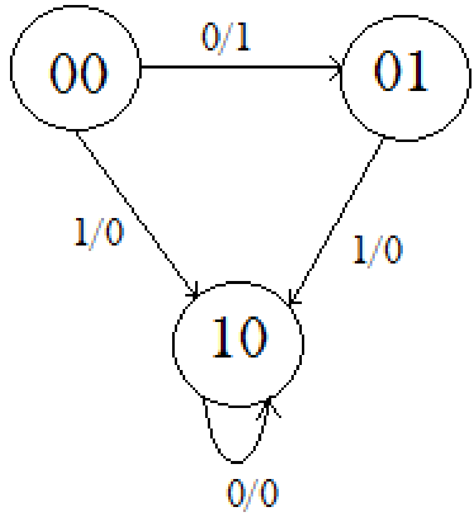


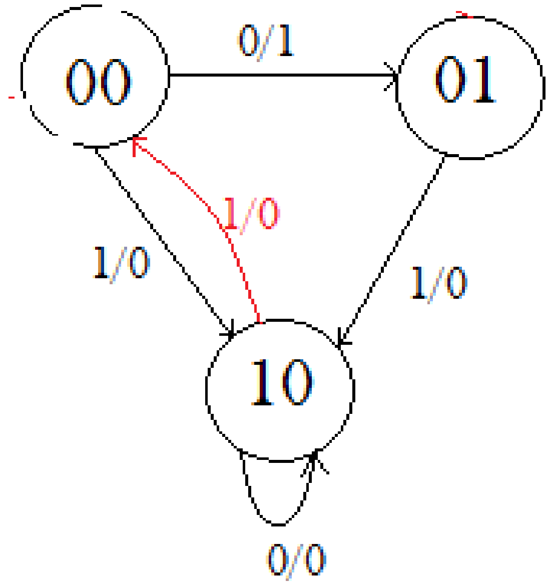
A	B	x	A'	B'
0	0	0	0	1
0	0	1	1	0
0	1	0	0	0
0	1	1	1	0
1	0	0	1	0
1	0	1	0	0
1	1	0	1	0
1	1	1	0	0

What I get works,
but is untrusted.
There are backdoors!

Malicious Design

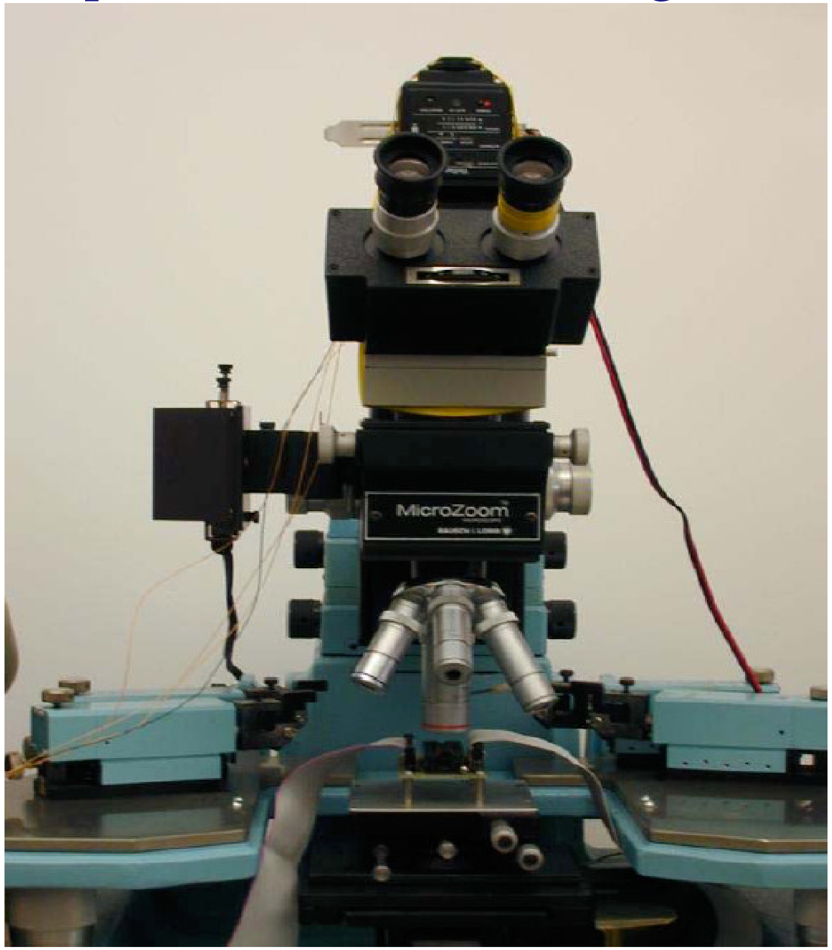
- Hardware Trojan horse: adding hidden access to state 00

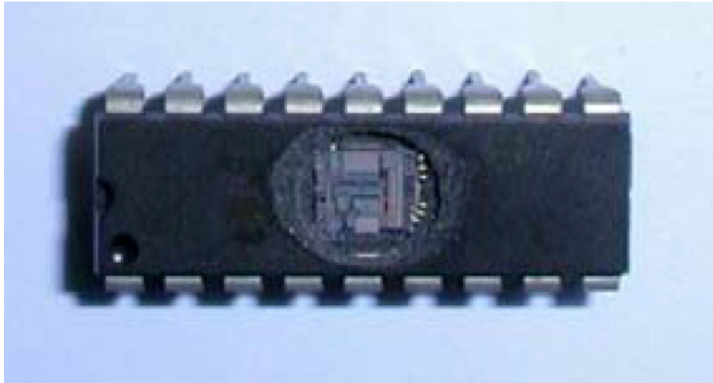


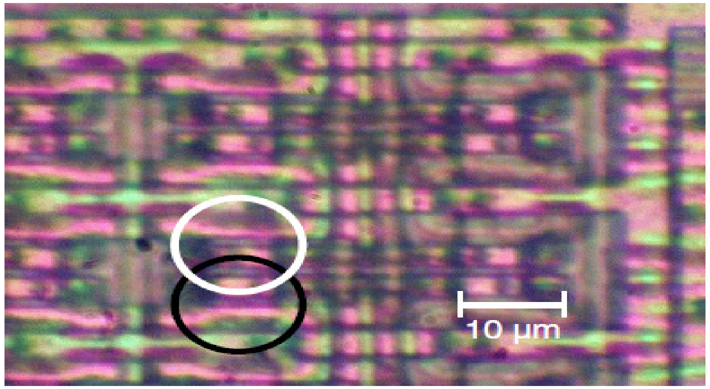


[Dunbar and Qu, TECS'14]
[Dunbar and Qu, IWLS'13]

Optical Fault Injection Attacks







[Sergei and Anderson et al, CHES 2002]

Hardware in Security and Trust

Evolving role of HW in security:

- Enabler
- Enhancer
- Enforcer

Weakest Link ?

Secure Systems based on Trusted Hardware

Great Promises!

- TPM
- PUF
- HW-SW co-design

Trust Platform Module (TPM)

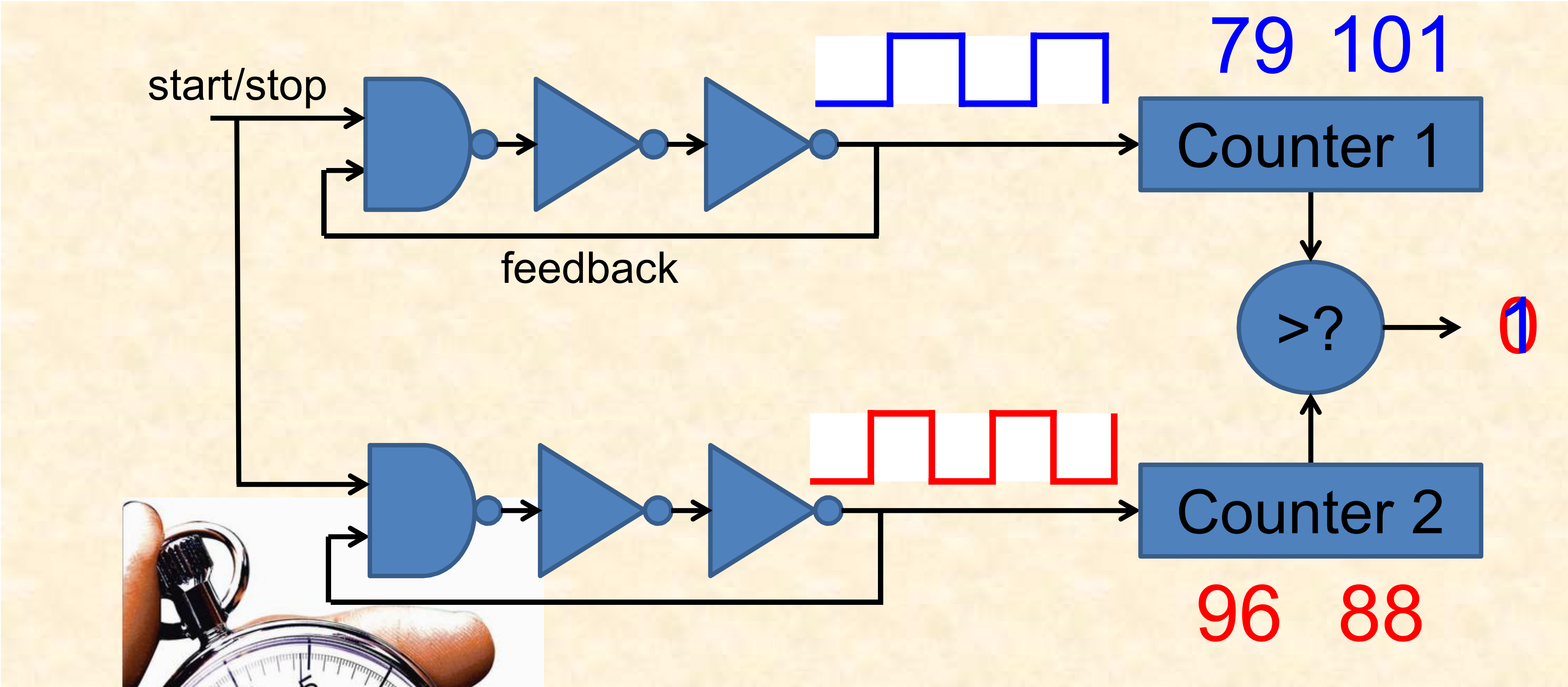
- TPM refers to
  - the set of specifications for a secure crypto-processor, and
  - chip implementation of these specifications.
- TPM chips
  - can be installed on the motherboard and is used in almost all PCs, laptops, and tablets; most smart phones.
  - Best to be used together with: firewall, antivirus software, smart card, biometric verification
  - Vendors: Atmel, Broadcom, Infineon, Sinosun, STMicroelectronics, Winbond, Toshiba, Intel, etc.

Main Functions of TPM

- hardware authentication
- cryptographic key generation
- protection of cryptographic keys
- hardware pseudo-random number generation
- sealed storage (passwords, encryption keys and digital certificates)
- remote attestation

Does TPM solves all the problems?

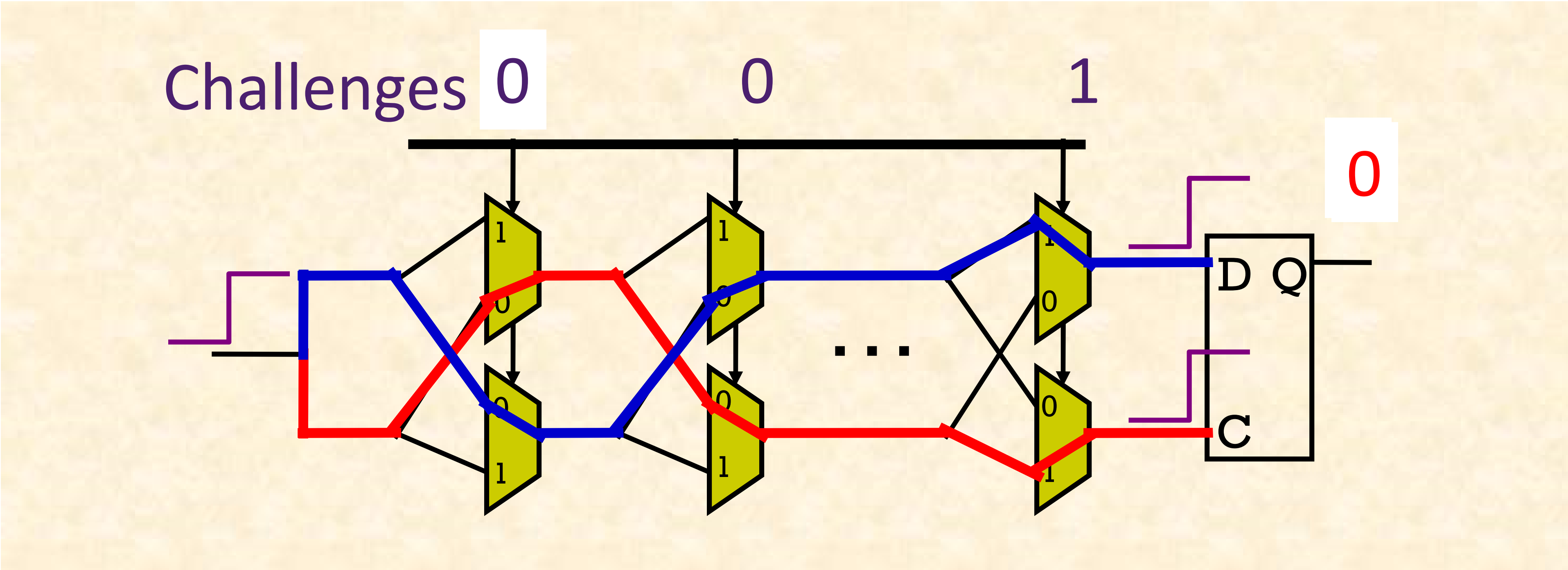
Physical Unclonable Function



Ring Oscillator PUFs

Physical Unclonable Function

Each challenge creates two paths through the circuit that are excited simultaneously. The digital response is based on a (timing) comparison of the path delays.

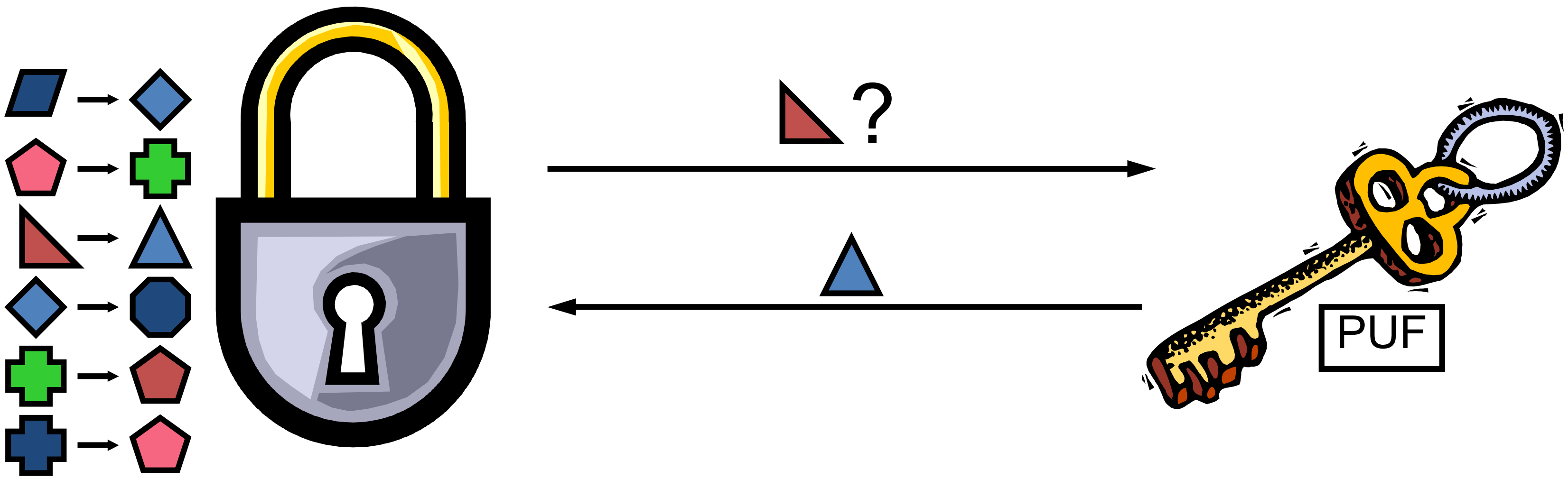


PUF: Unclonable Key

A Silicon PUF can be used as an unclonable key.

The lock has a database of challenge-response pairs.

To open the lock, the key has to show that it knows the response to one or more challenges.

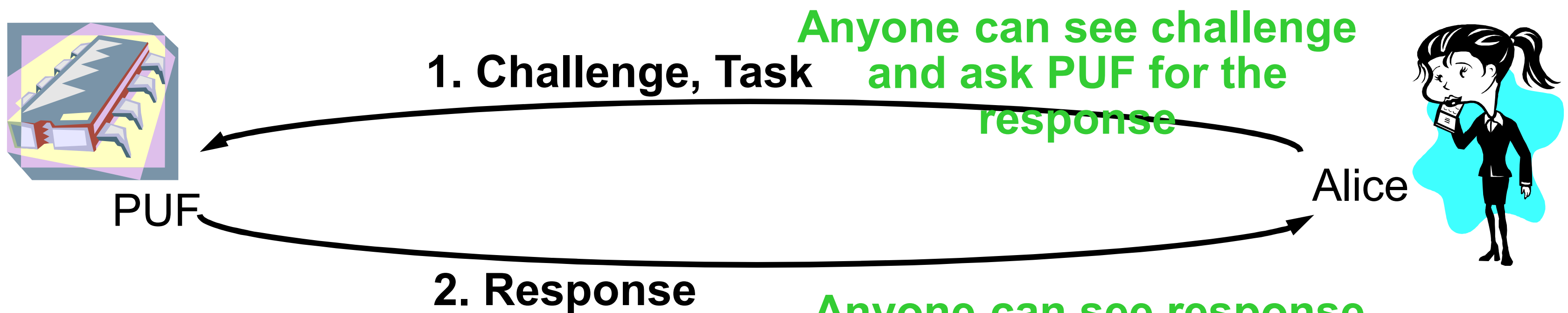


PUF: Secret Share

- If a remote chip stores a private key, Alice can *share a secret* with the chip if she knows the public key corresponding to the stored private key
  - Alice encrypts the *Secret* using chip's public key, only the right chip can decrypt the *Secret* using the stored private key.
  - The chip encrypts the *Secret* using chip's private key, it can only be decrypted when the correct public key is used.

PUF: Device Authentication

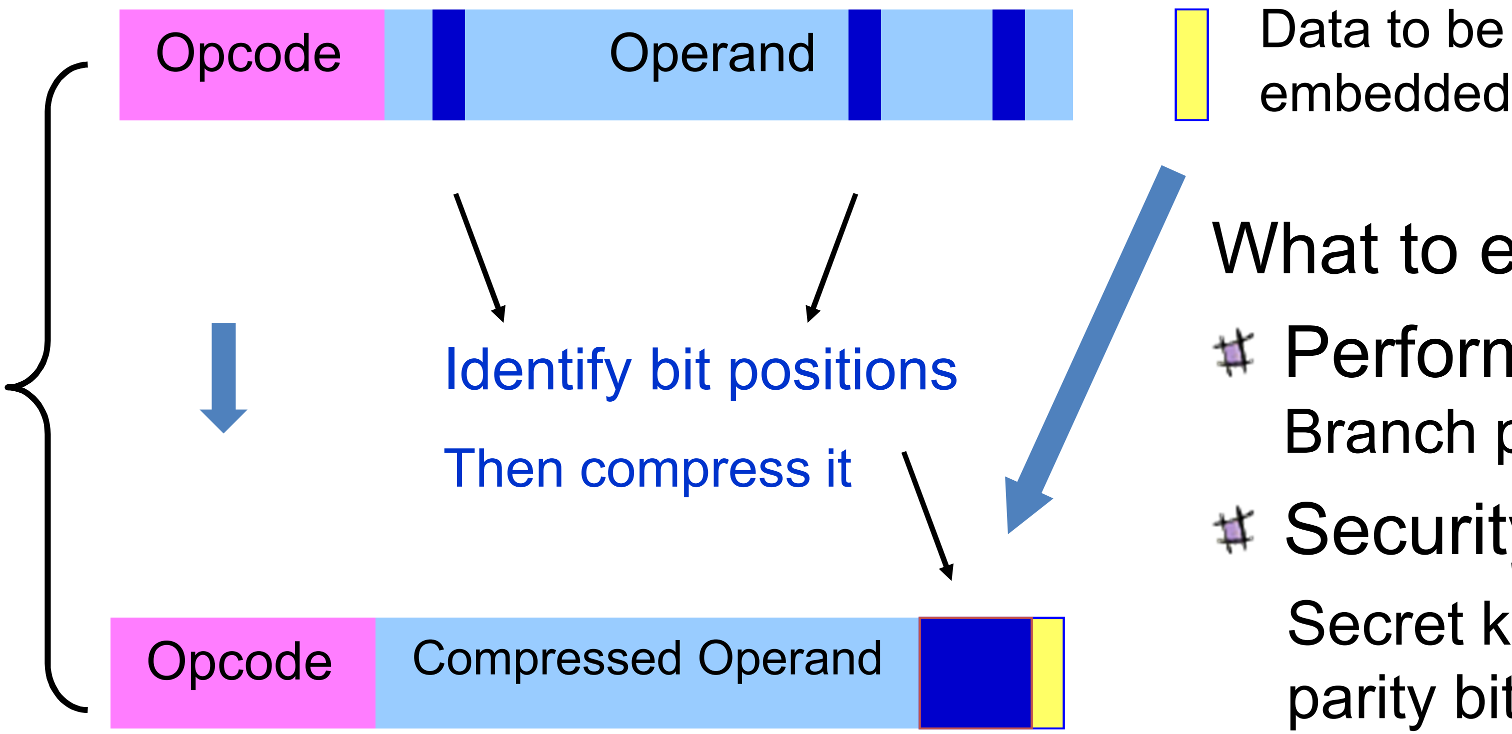
- Alice wishes to authenticate a chip
- She has a challenge response pair that no one else knows, which can authenticate the silicon PUF on the chip
- She asks for the response to the challenge
- Chip authenticated if response is correct



But only the genuine chip can generate the right response

数据驱动安全

Data Embedding in Binary Code

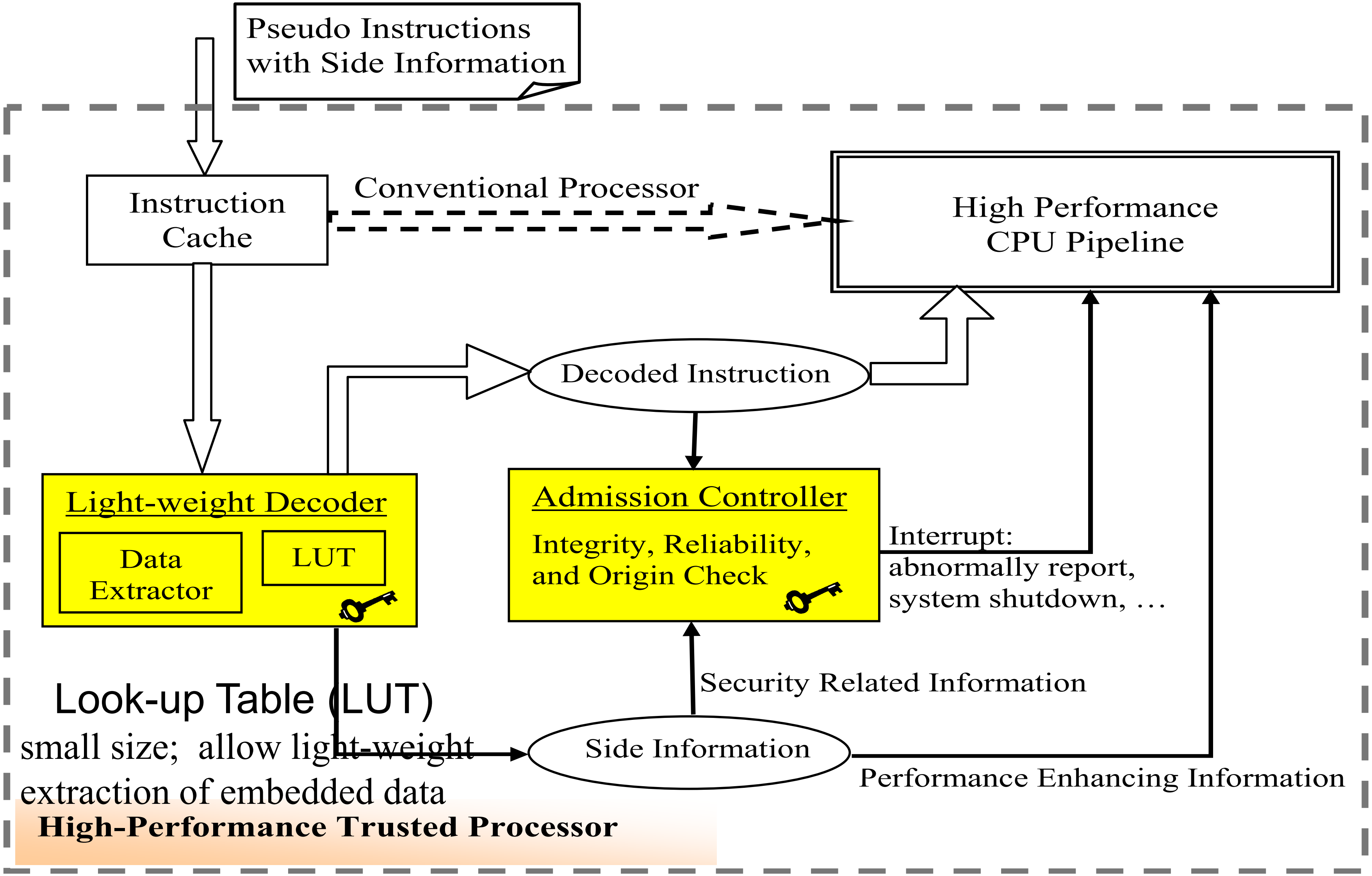


What to embed?

- Performance:
  Branch predictor
- Security:
  Secret key, ECC, parity bit, integrity checker,

- How much data can be embedded?
- How to ensure the code is still executable?

Trusted Execution Environment



Look-up Table (LUT)

small size; allow light-weight extraction of embedded data

[Taylor, Yin, Wu, and Qu, HOST 2008]

EDA Meets Designing the Things

Needs:	EDA tools	
• Function	√	X
• Miniature/size	√	X
• Performance	√	X
• Cost	√	?
• Low power	√	
• Reliability	√	
• Safety	√	

More Needs:

- Security
- Privacy
- Trust
- Lower power

Hardware has advantages in meeting these needs!

Nobody is An Island

- Security, privacy, trust issues remain as long as currency exists
- Attacking surface grows faster than countermeasures
- No system is an island,
  - a holistic approach to build secure system
  - Cryptography, software, hardware, communication, device, …
- Hardware is the root of security, trust, privacy

Enabler, Enhancer, Enforcer

Conclusions