

SECURE EMBEDDED SYSTEMS

May 19, 2008

Mahadevan Gomathisankaran

Security

2

English Definition (from m-w.com):

- the quality or state of being secure as
 - ▣ a: freedom from danger (safety)
 - ▣ b: freedom from fear or anxiety

Computer Security

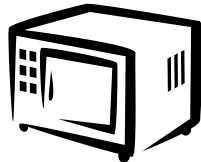
3

- NIST Handbook
 - ▣ The protection afforded to an **automated** information system in order to attain the applicable objectives of preserving the **integrity**, **availability** and **confidentiality** of information system resources

Embedded Systems

4

- A combination of computer hardware and software, and perhaps additional mechanical or other parts, designed to perform a dedicated function



Embedded Systems Evolution

5

- Intel 8051 (1980-)
 - μ C, 8-bit data, 16-bit address, 100 MHz
- Infineon Tricore (2002-)
 - μ P + DSP + ASIC, 32-bit, ~300 MHz,

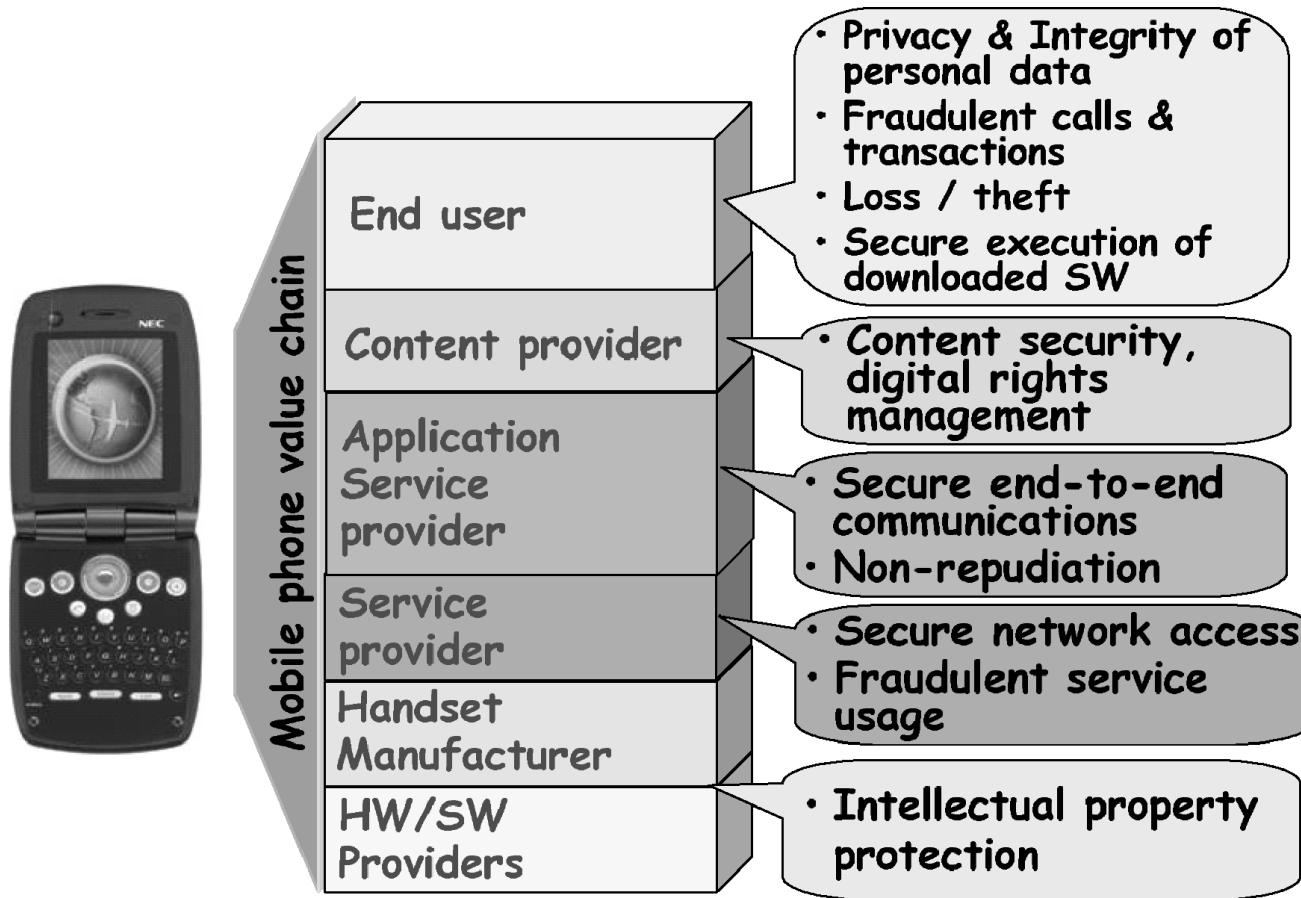
Inflection Point

6

- Pervasiveness of Embedded devices
- Criticality of Embedded systems
- Software complexity
- Attack capabilities
 - ▣ Cheap computing power
 - ▣ Physical access
 - ▣ Software vulnerabilities
- Constraints of Embedded Systems
 - ▣ Battery/Power
 - ▣ Computational Capabilities

Providing Security

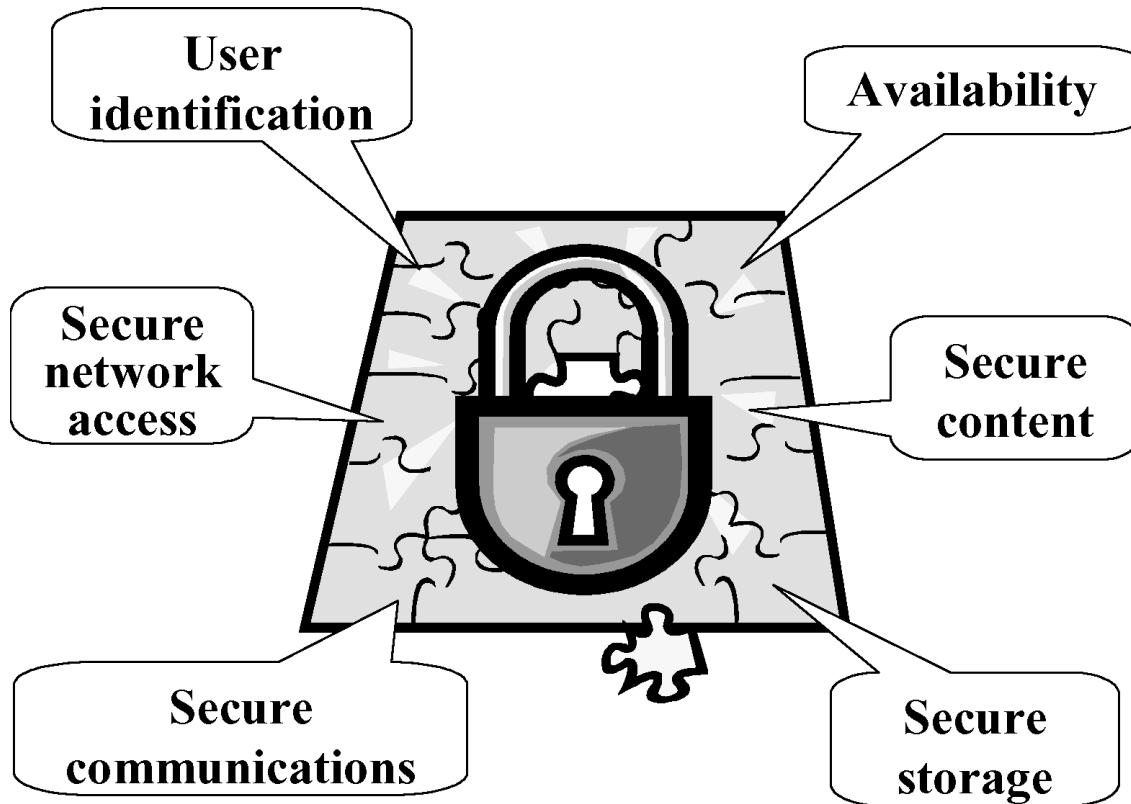
7



Source: S. Ravi et al. *Security in Embedded Systems: Design Challenges*, in ACM Trans. On Embedded Computing Systems, August 2004.

Requirements

8



Source: S. Ravi et al. *Security in Embedded Systems: Design Challenges*, in ACM Trans. On Embedded Computing Systems, August 2004.

Design Challenges

9

- Processing Gap
 - ▣ Security processing overhead
- Battery Gap
 - ▣ Energy consumption overhead
- Flexibility
 - ▣ Support multiple algorithms
- Tamper Resistance
 - ▣ Resist physical and side-channel attacks
- Assurance Gap
 - ▣ Graceful Failures
- Cost



Building Blocks

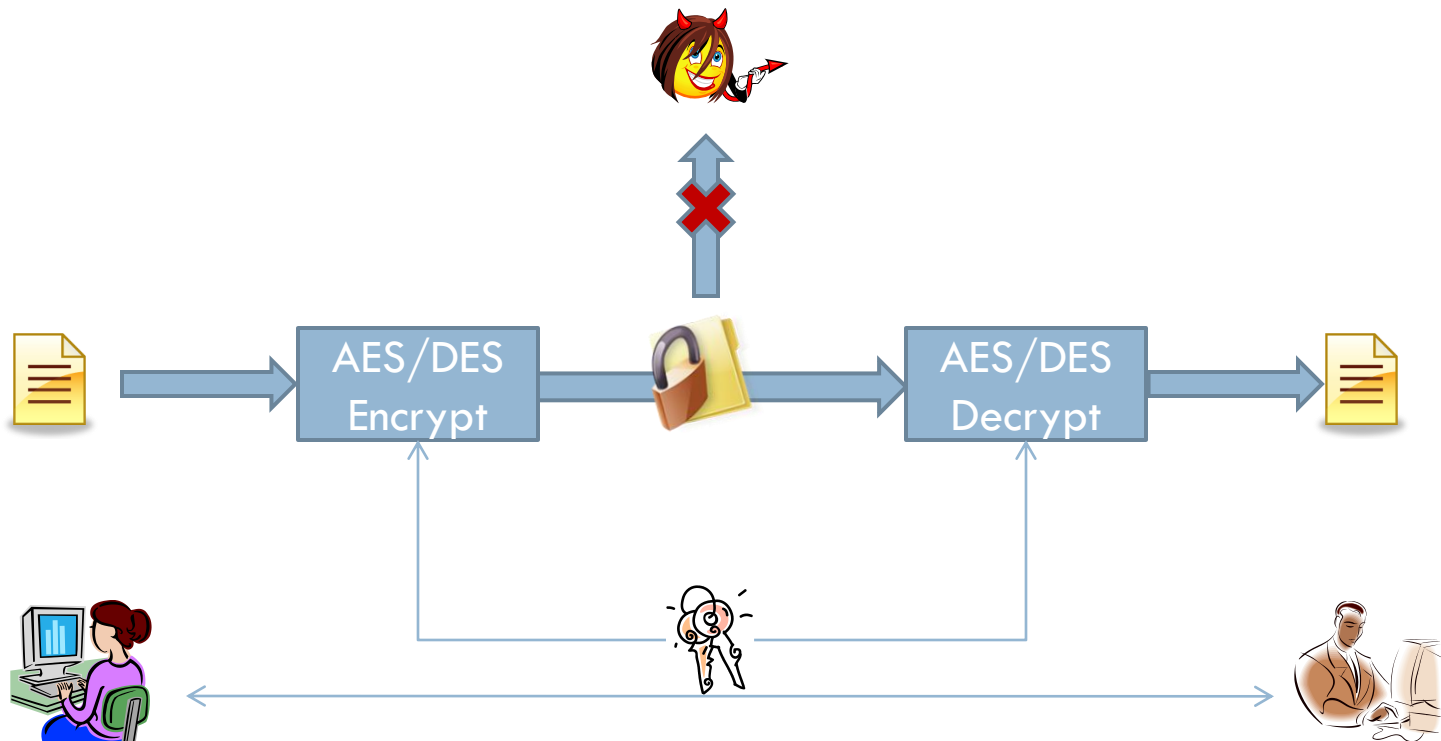
10

- Symmetric Ciphers
 - AES, DES
- Asymmetric Ciphers
 - RSA, Diffie-Hellman
- Hashing Algorithms
 - MD5, SHA



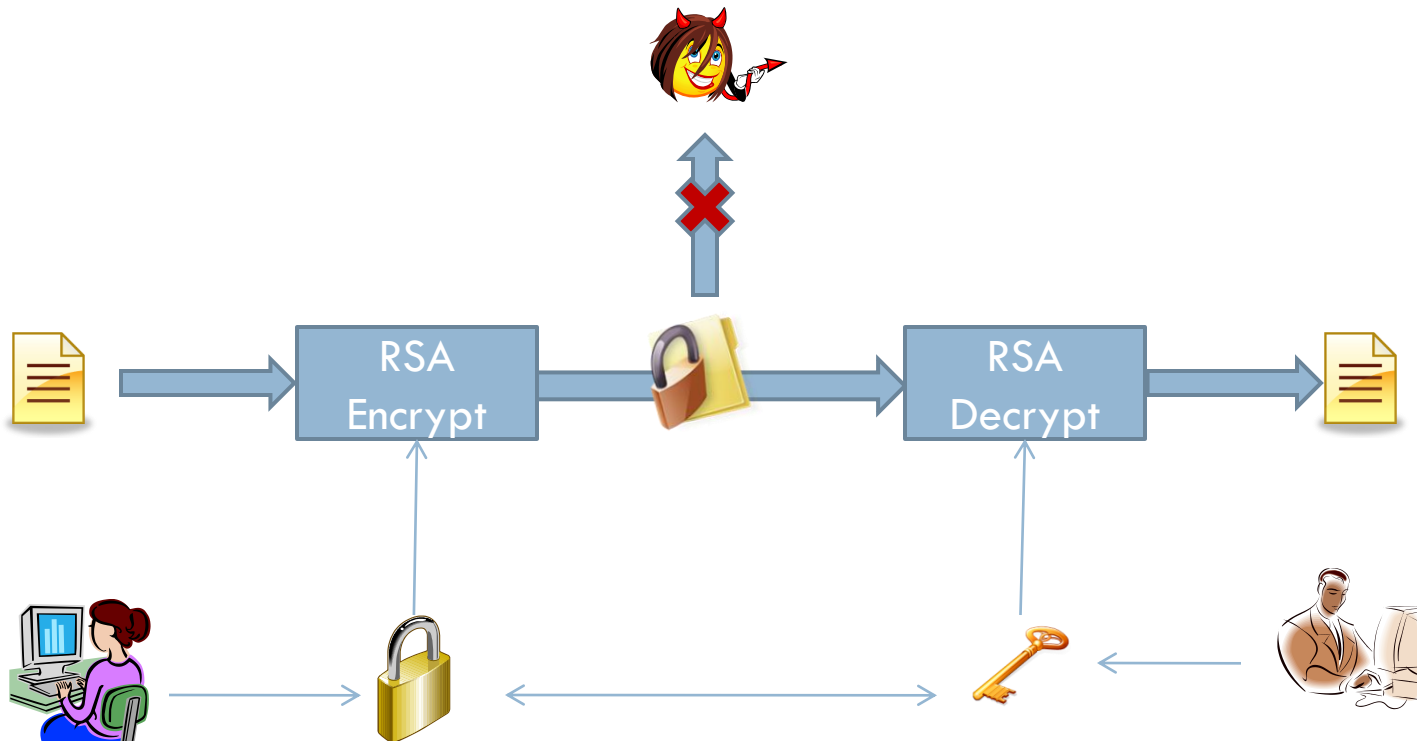
Symmetric Encryption

11



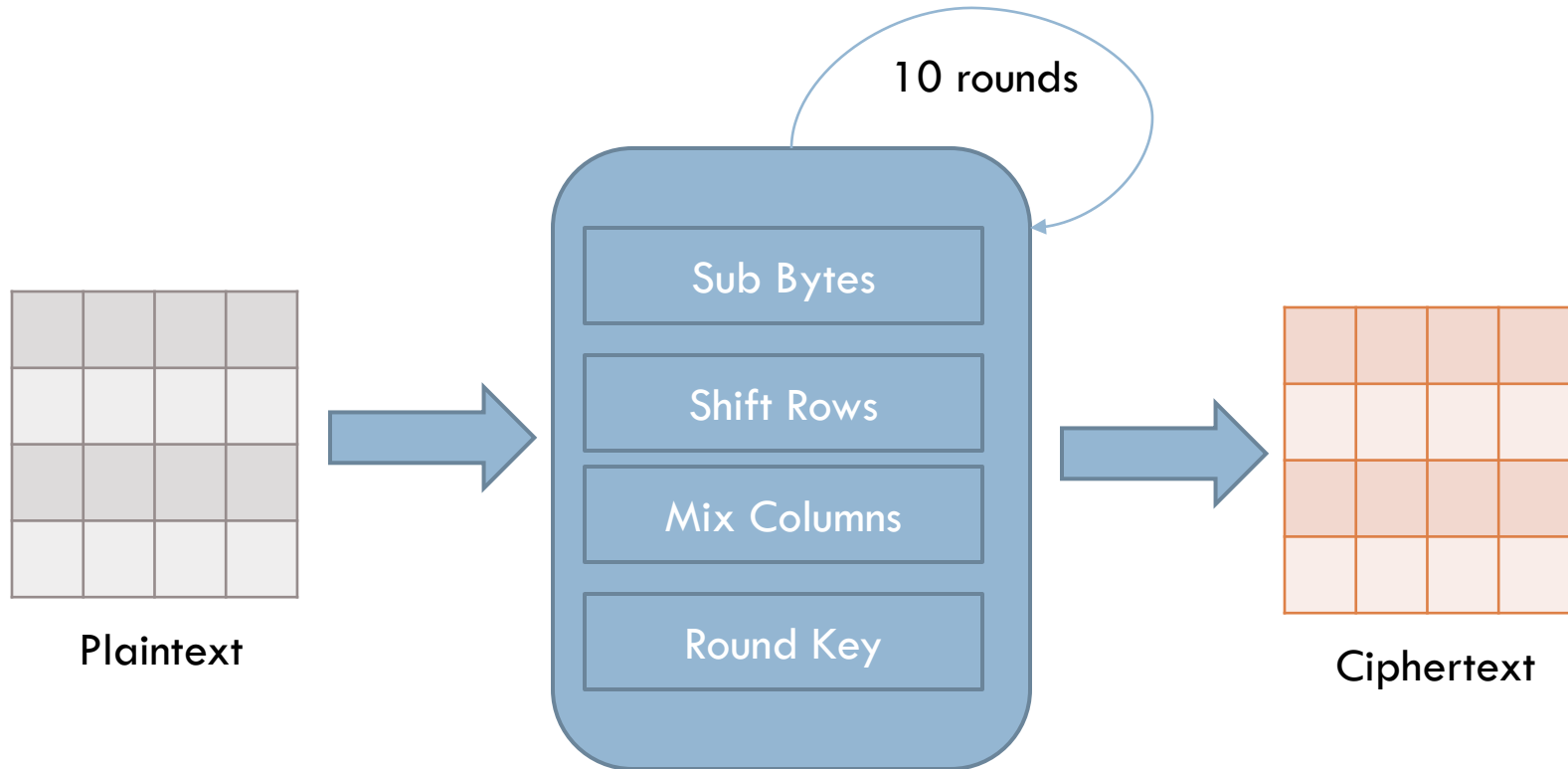
Asymmetric Encryption

12



AES

13



AES - Low Power Design

14

- Smaller Data-path (8-bits)
- Fixed Design size (128 bits)
- RAM vs FF ?
- Energy vs Power Consumption ?
 - Battery based devices
 - Passively powered devices

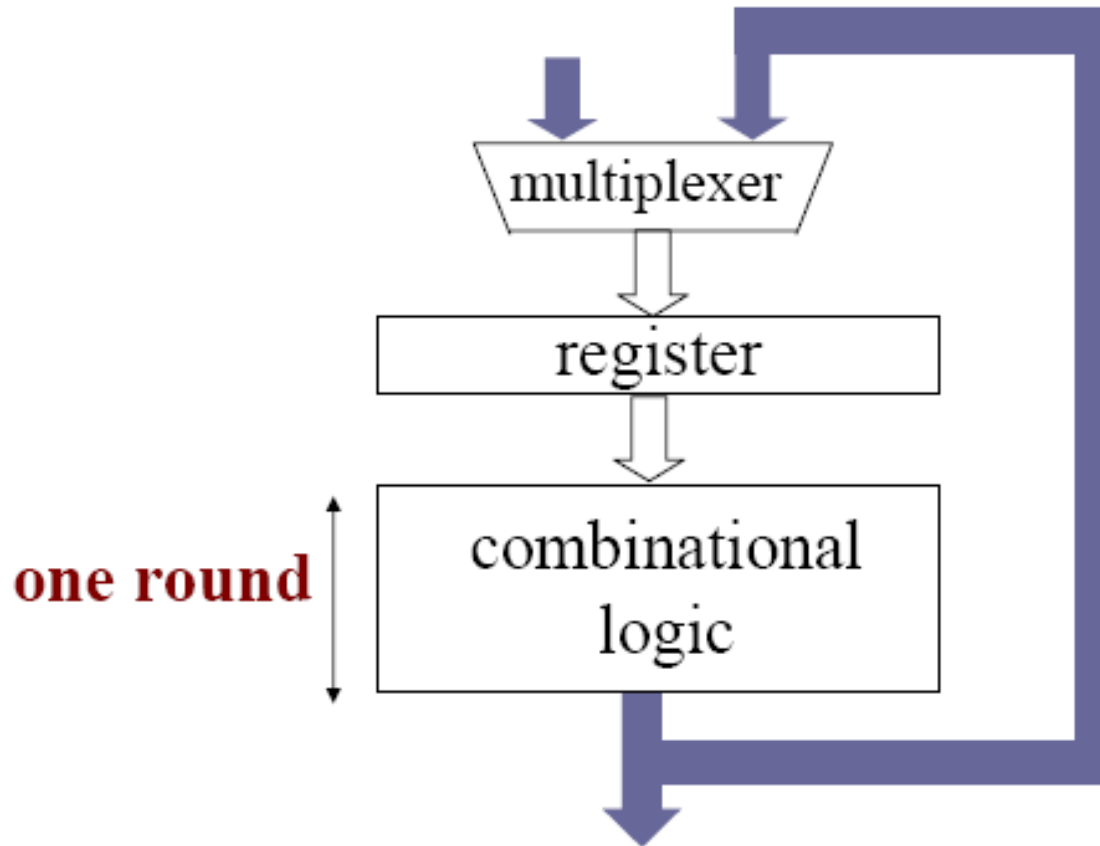
AES – High Speed Design

15

- Pipelining
 - Intra-round
 - Inter-round
- Data width
 - Shift columns -> Free (128 bits)
 - Sub bytes parallel -> 16 S-Boxes

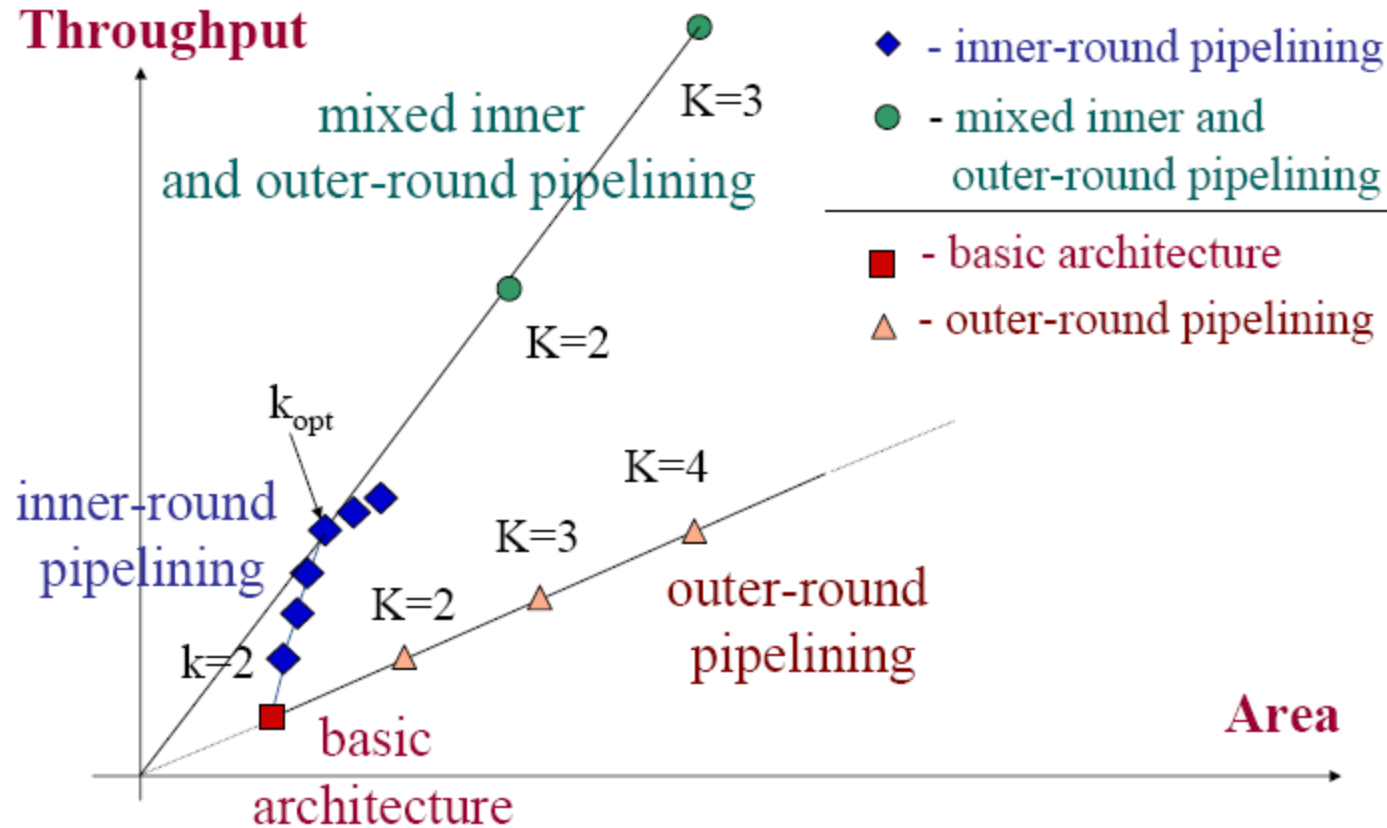
AES Design

16



AES Design Trade-off

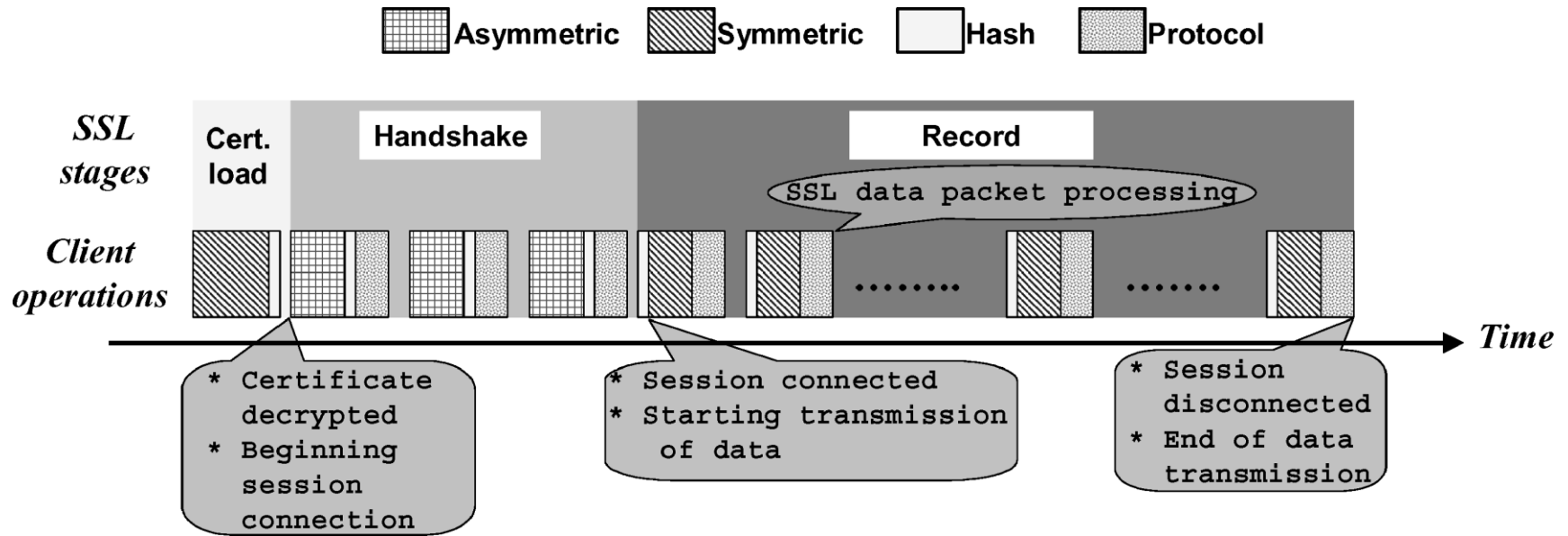
17



Source: P. Chodowiec et al. Fast Implementations of Secret-Key block ciphers using Mixed Inner and Outer round pipelining. ACM/SIGDA , April 2000.

Example: SSL

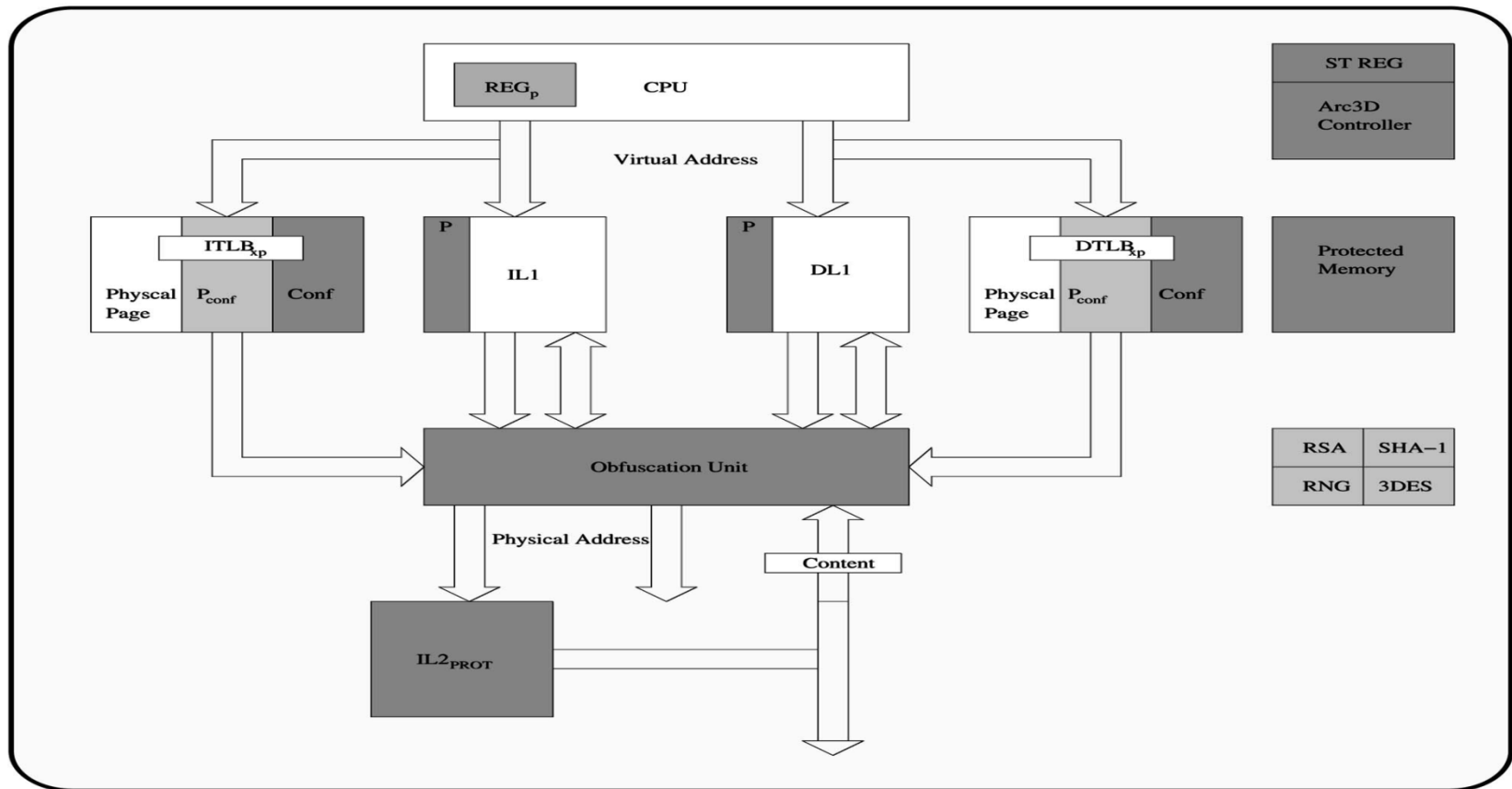
18



Source: S. Ravi et al. *Security in Embedded Systems: Design Challenges*, in ACM Trans. On Embedded Computing Systems, August 2004.

Architectural Solutions – Arc3D

19

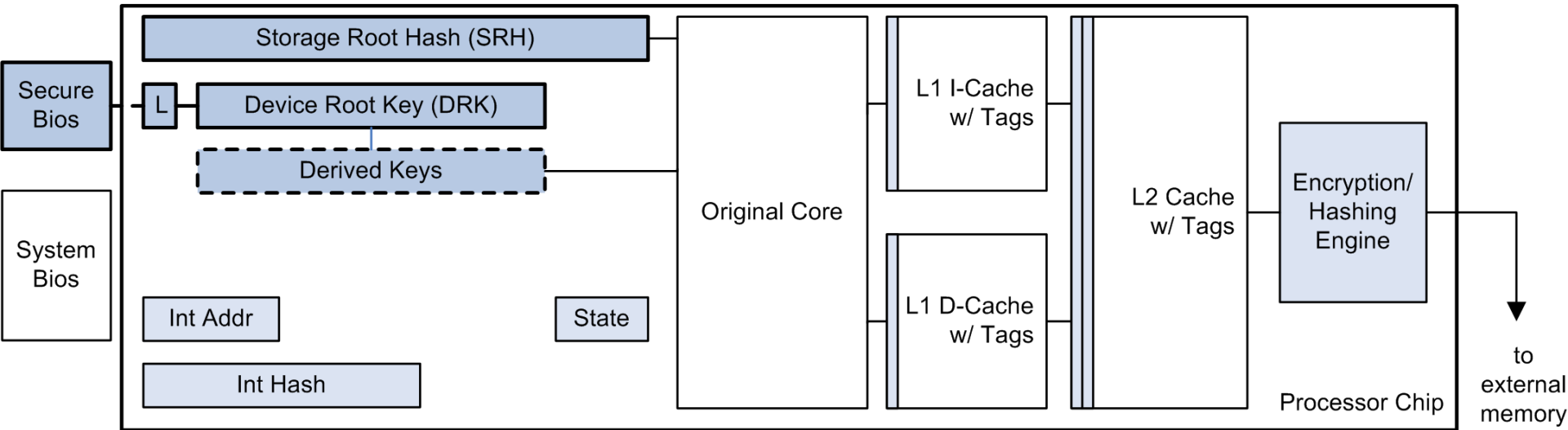


Source: M. Gomathisankaran et al. Architecture support for 3D Obfuscation. IEEE TC, 2006.

SP Architecture

20

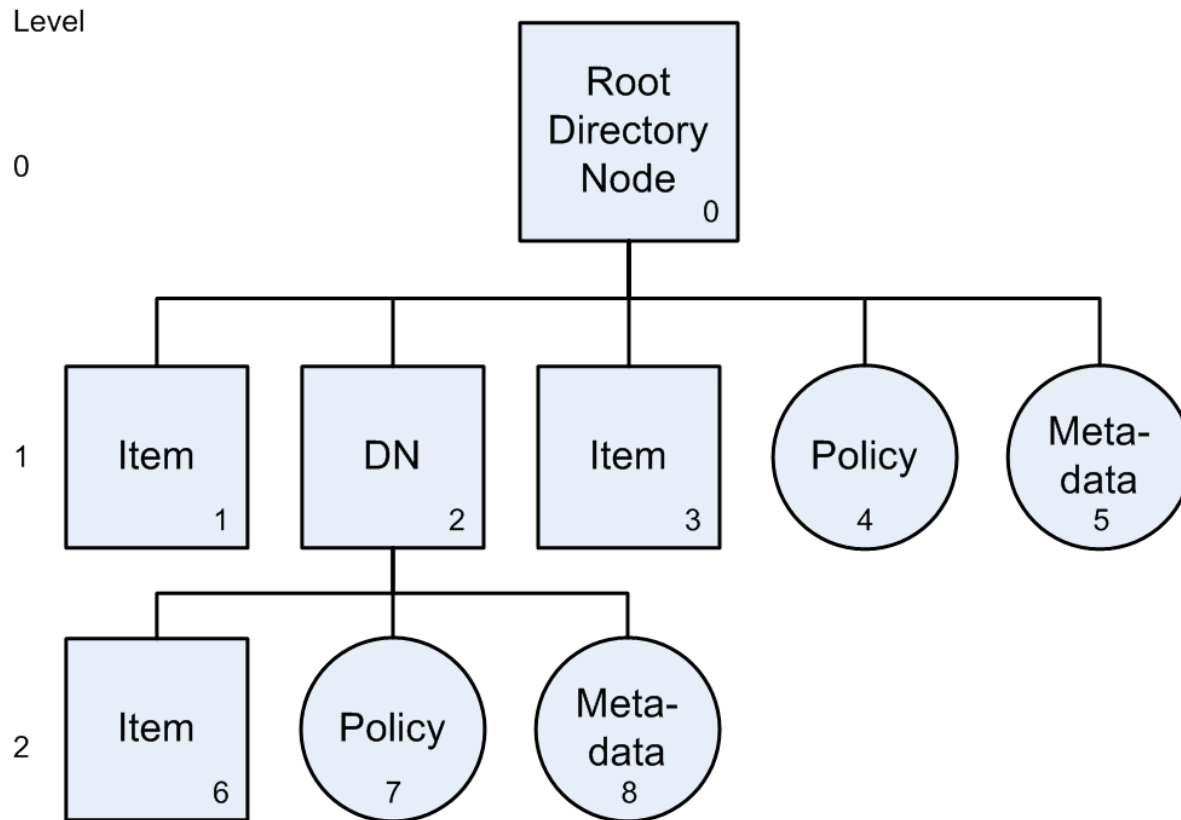
Secret Protecting Architecture – PALMS, Princeton University



Source: J. Dvoskin et al. Hardware rooted Trust from Secure Key Management and Transient Trust. ACM/CCS , 2007.

SP Architecture

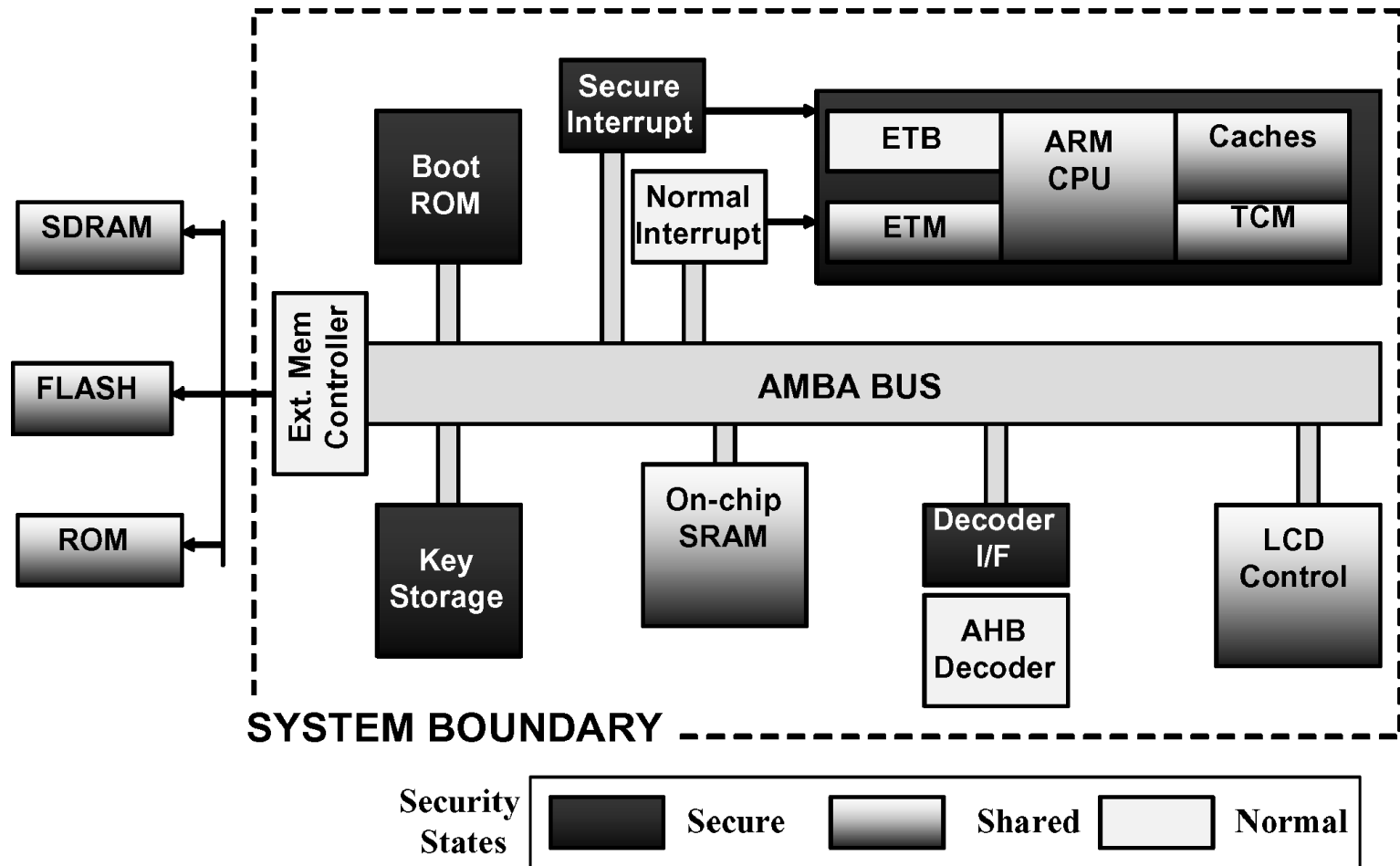
21



Source: J. Dwoskin et al. Hardware rooted Trust from Secure Key Management and Transient Trust. ACM/CCS , 2007.

ARM TrustZone

22



Identification

23

- Using PKI
 - ▣ Eg. Trusted Platform Module
- Using Physical Attributes
 - ▣ Physically Unclonable Functions

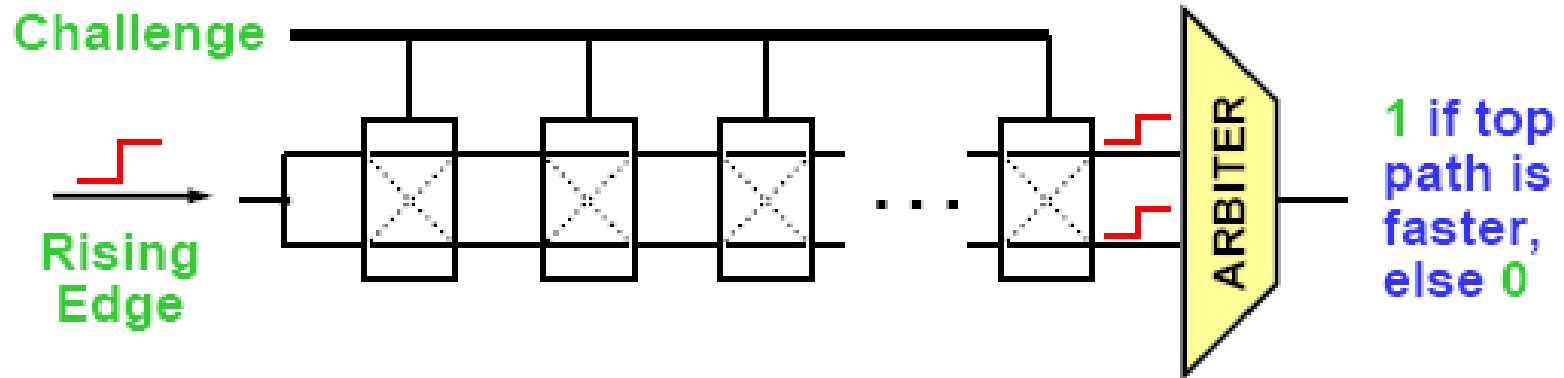
Silicon PUF

24

- Concept proposed by Srinivasa Devadas of MIT
- Process Variations
 - ▣ No two IC's are identical
- Circuit which amplify layout variations can be built
 - ▣ Observed delays can be used as identity

PUF

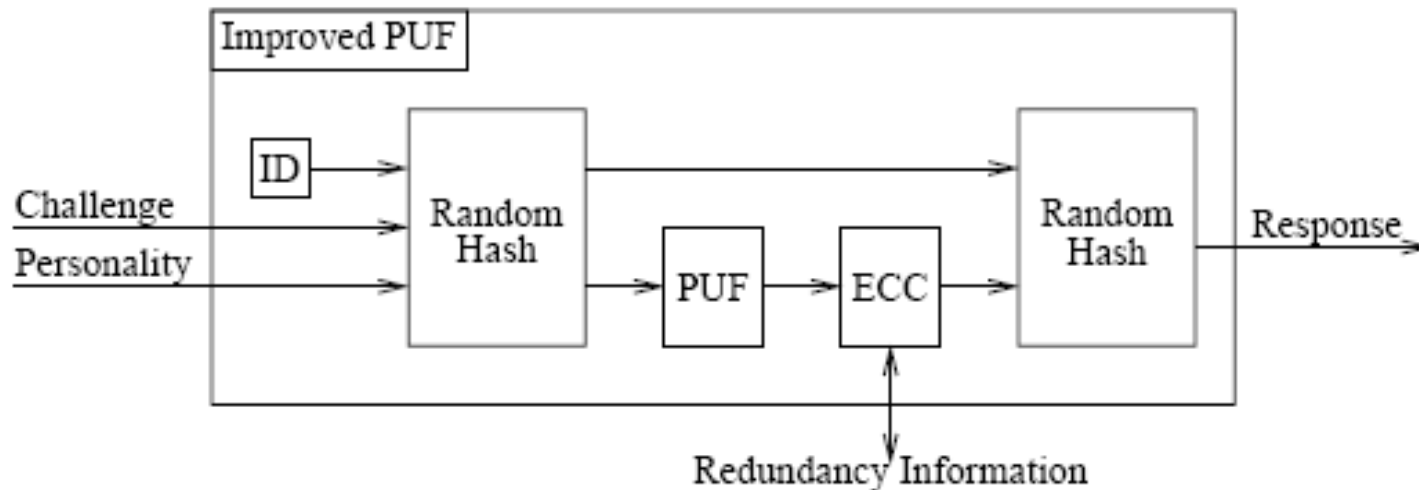
25



Source: B. Gassend et al. Silicon Physical Random Functions, MIT CSAIL Memo 456.

Improving PUF

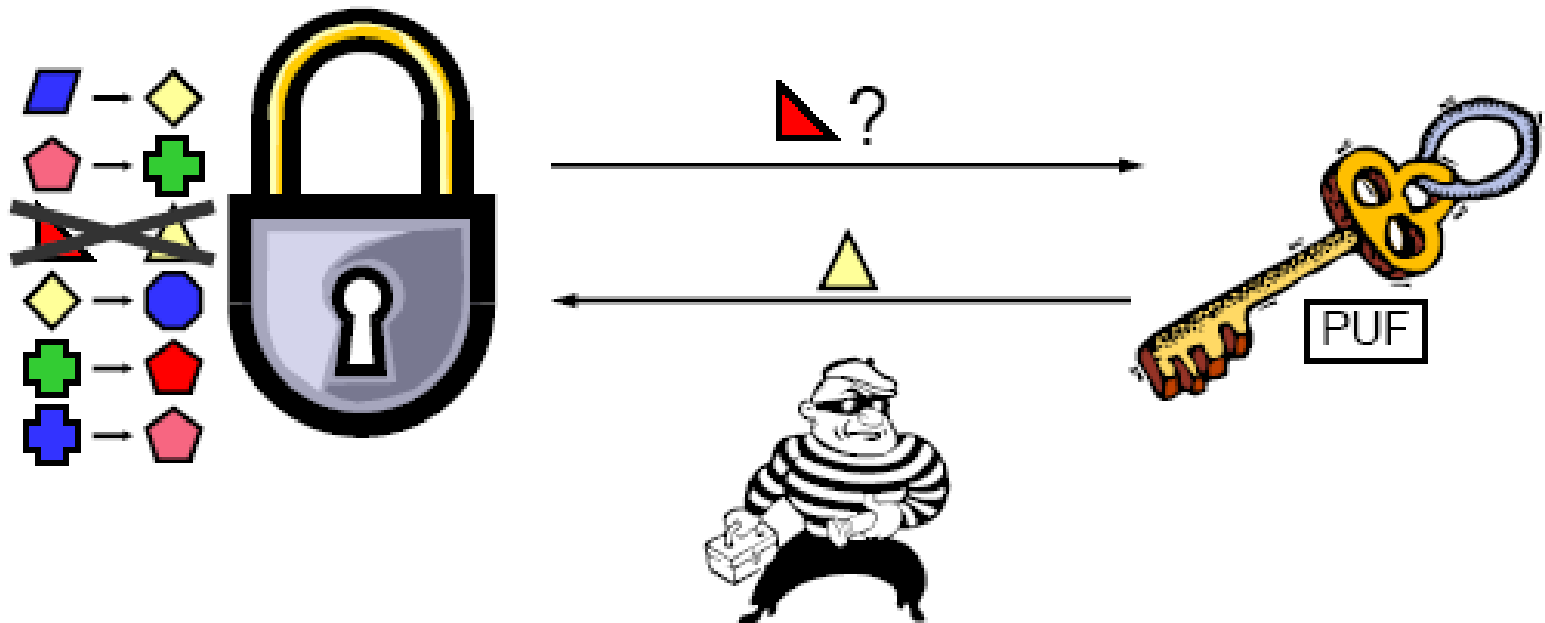
26



Source: B. Gassend et al. Silicon Physical Random Functions, MIT CSAIL Memo 456.

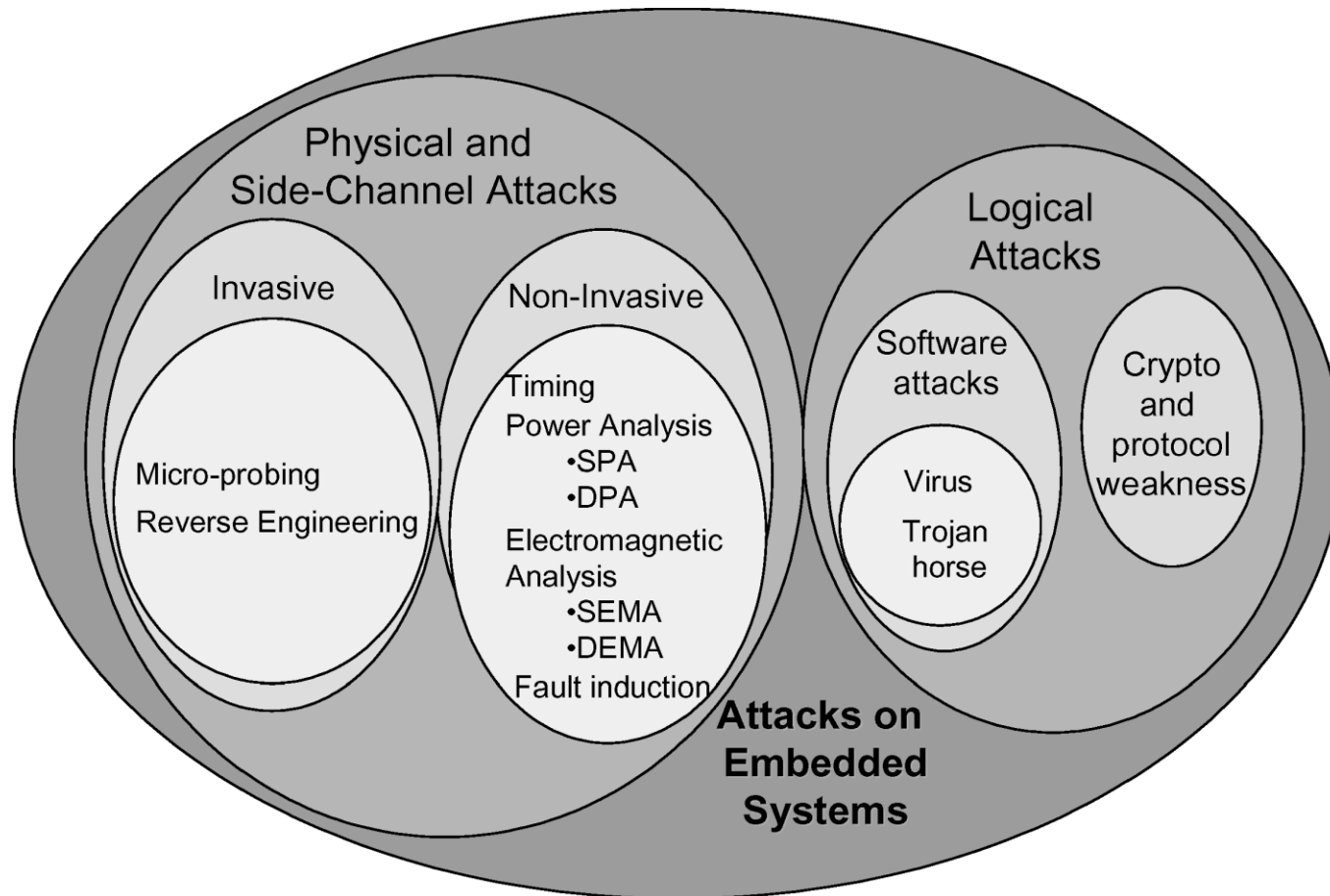
PUF Usage

27



Attacks

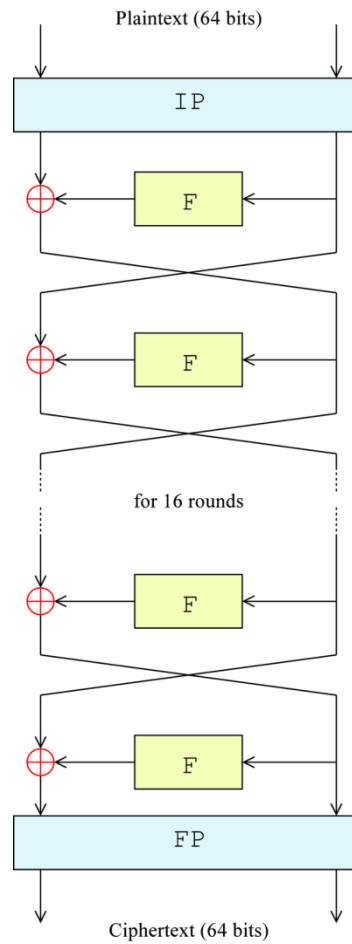
28



Source: S. Ravi et al. *Security in Embedded Systems: Design Challenges*, in ACM Trans. On Embedded Computing Systems, August 2004.

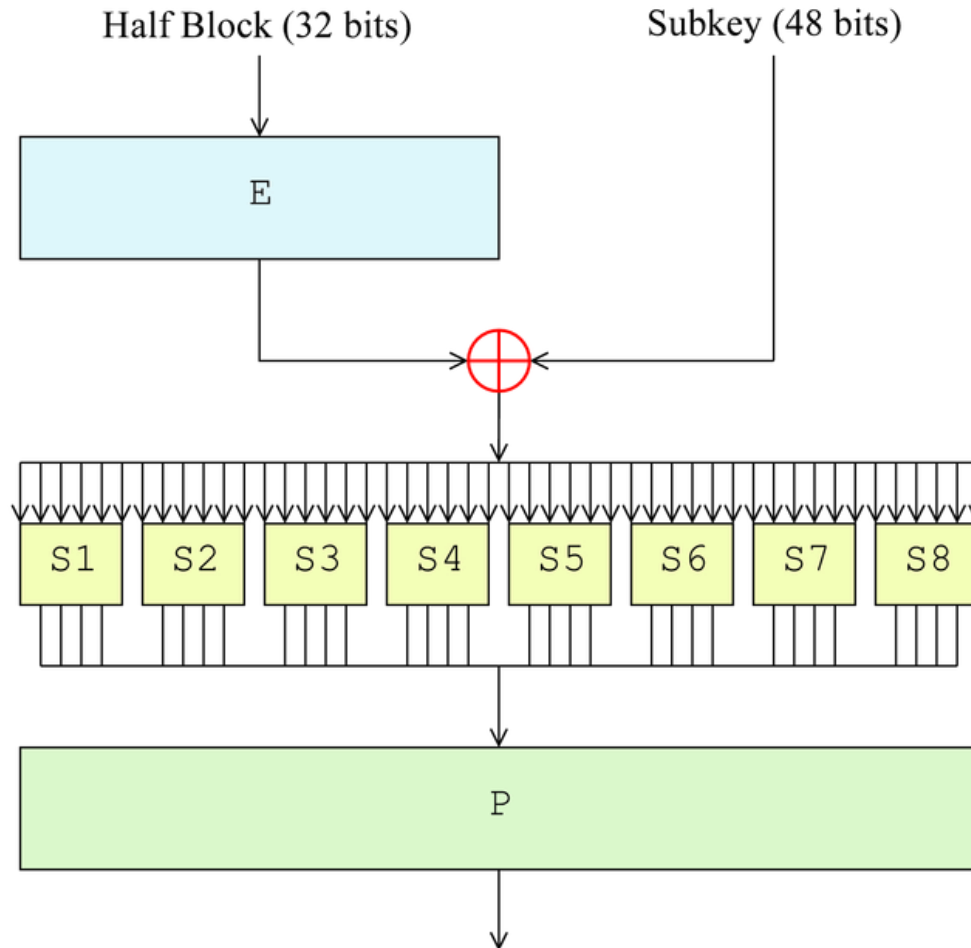
DES

29



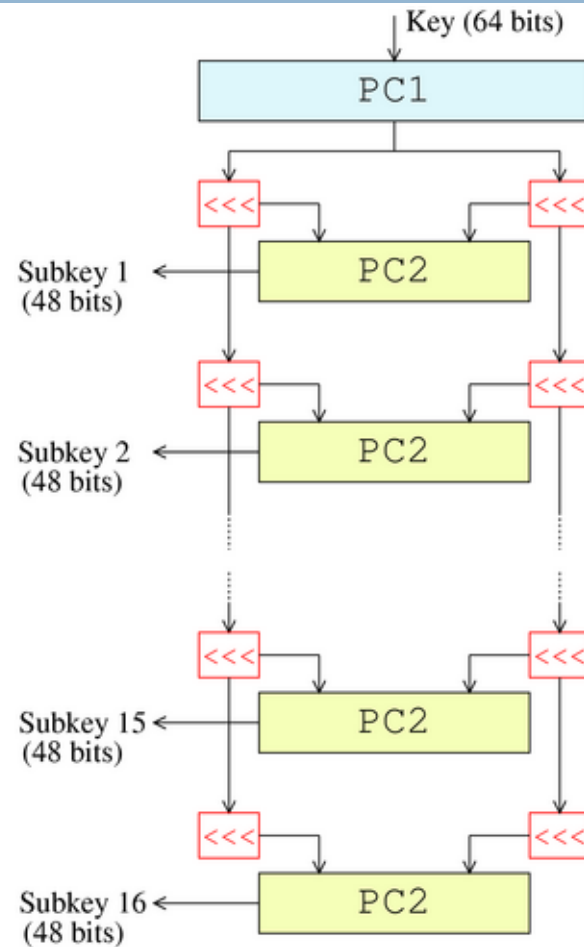
DES Fiestel Function

30



DES Key Schedule

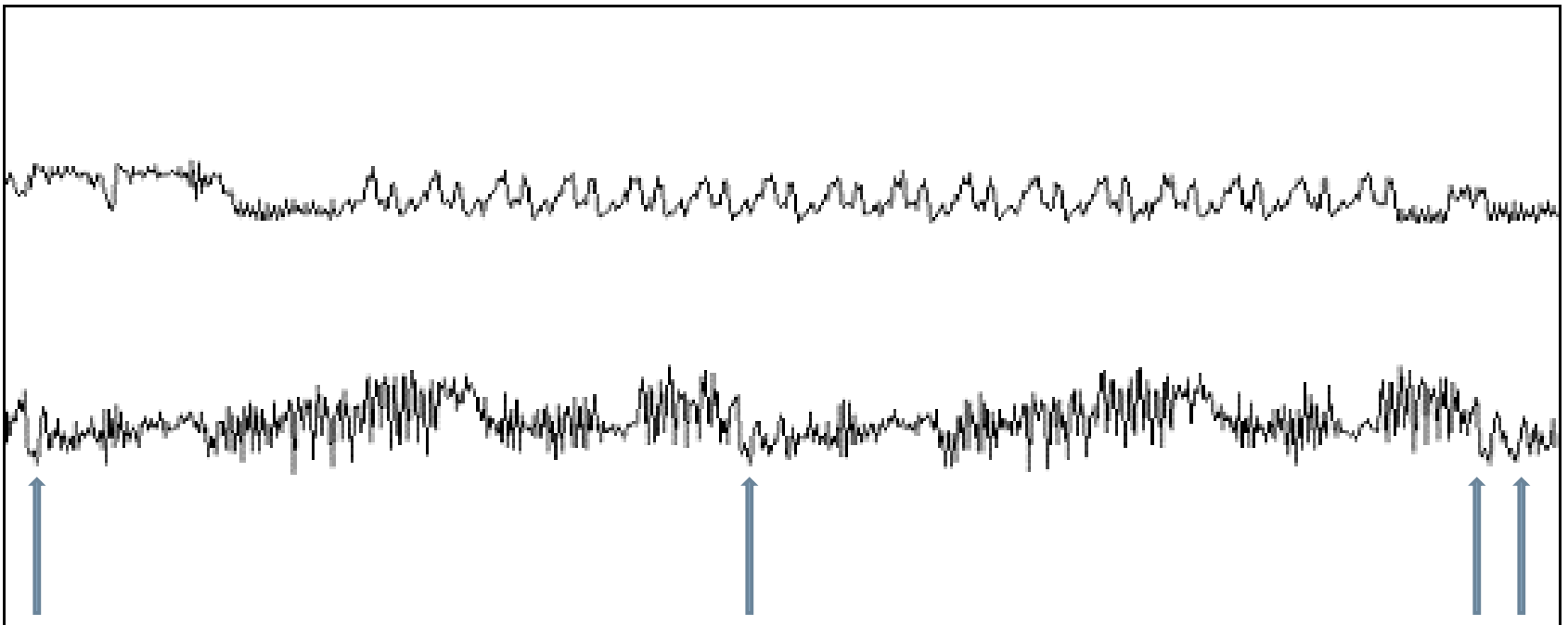
31



Simple Power Analysis

32

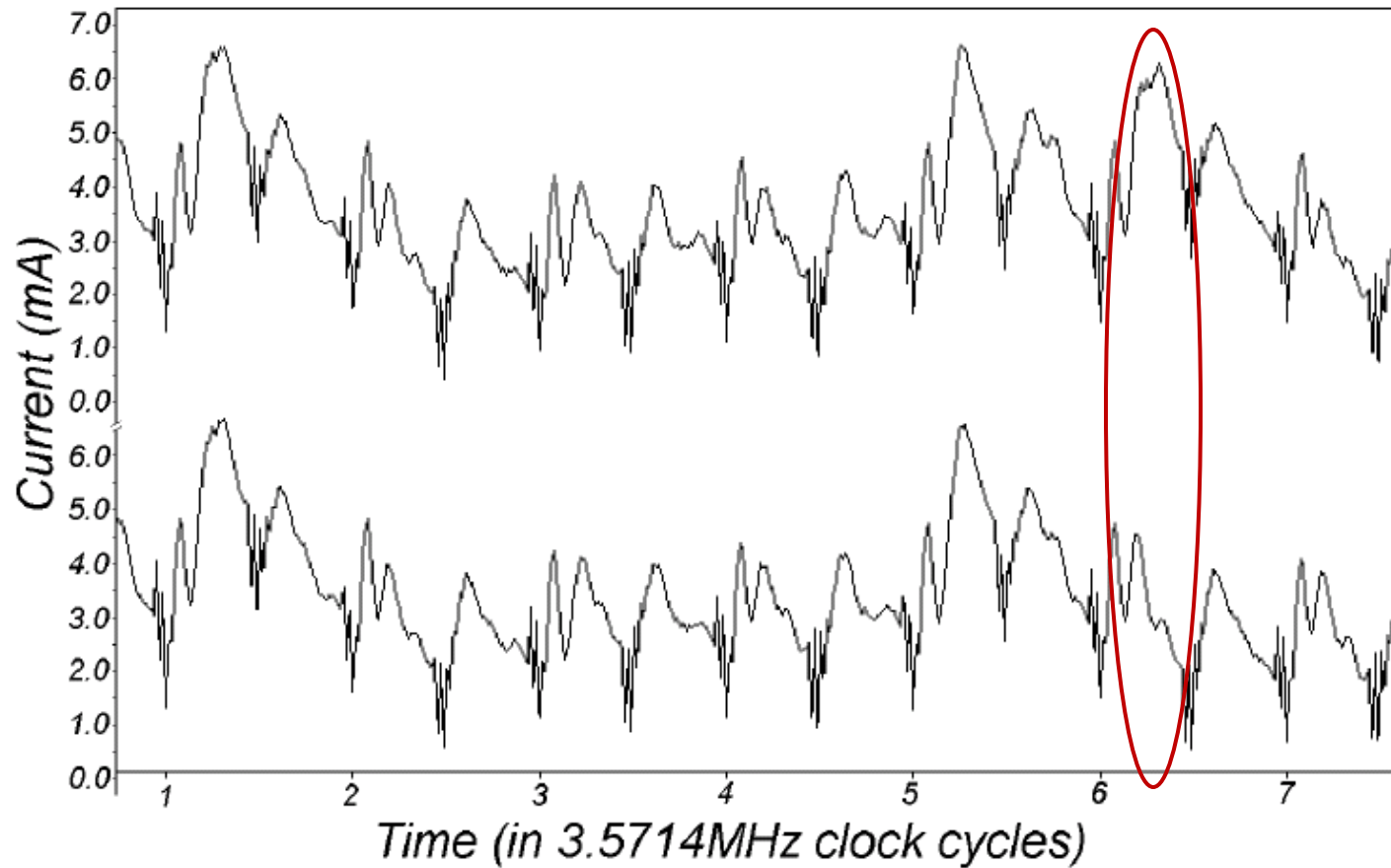
DES Power Profile



Source: P. Kocher et al. Differential Power Analysis, Crypto 99.

SPA

33



Source: P. Kocher et al. Differential Power Analysis, Crypto 99.

Differential Power Analysis

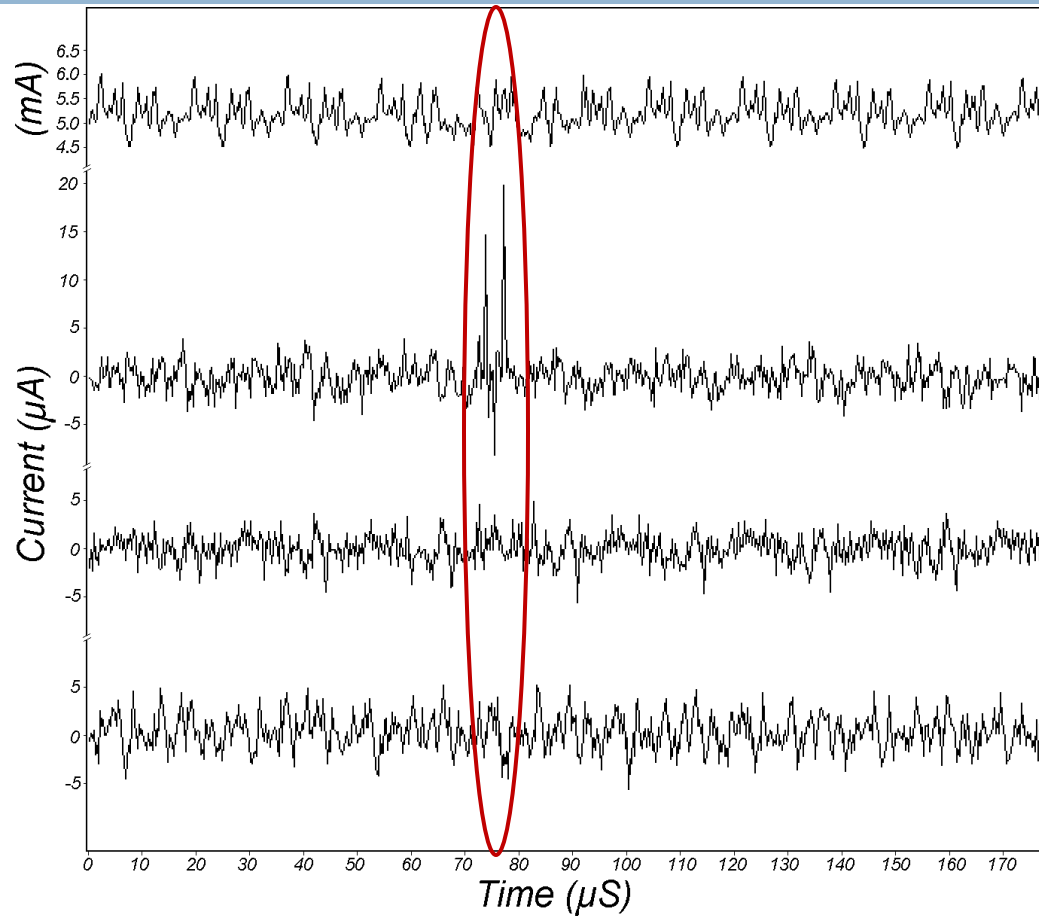
34

$$\begin{aligned}\Delta_D[j] &= \frac{\sum_{i=1}^m D(C_i, b, K_s) \mathbf{T}_i[j]}{\sum_{i=1}^m D(C_i, b, K_s)} - \frac{\sum_{i=1}^m (1 - D(C_i, b, K_s)) \mathbf{T}_i[j]}{\sum_{i=1}^m (1 - D(C_i, b, K_s))} \\ &\approx 2 \left(\frac{\sum_{i=1}^m D(C_i, b, K_s) \mathbf{T}_i[j]}{\sum_{i=1}^m D(C_i, b, K_s)} - \frac{\sum_{i=1}^m \mathbf{T}_i[j]}{m} \right).\end{aligned}$$

Source: P. Kocher et al. Differential Power Analysis, Crypto 99.

Differential Power Analysis

35



Source: P. Kocher et al. Differential Power Analysis, Crypto 99.

Timing Attacks

36

- Instruction Execution Variation
- Performance Optimizations

Fault Injection

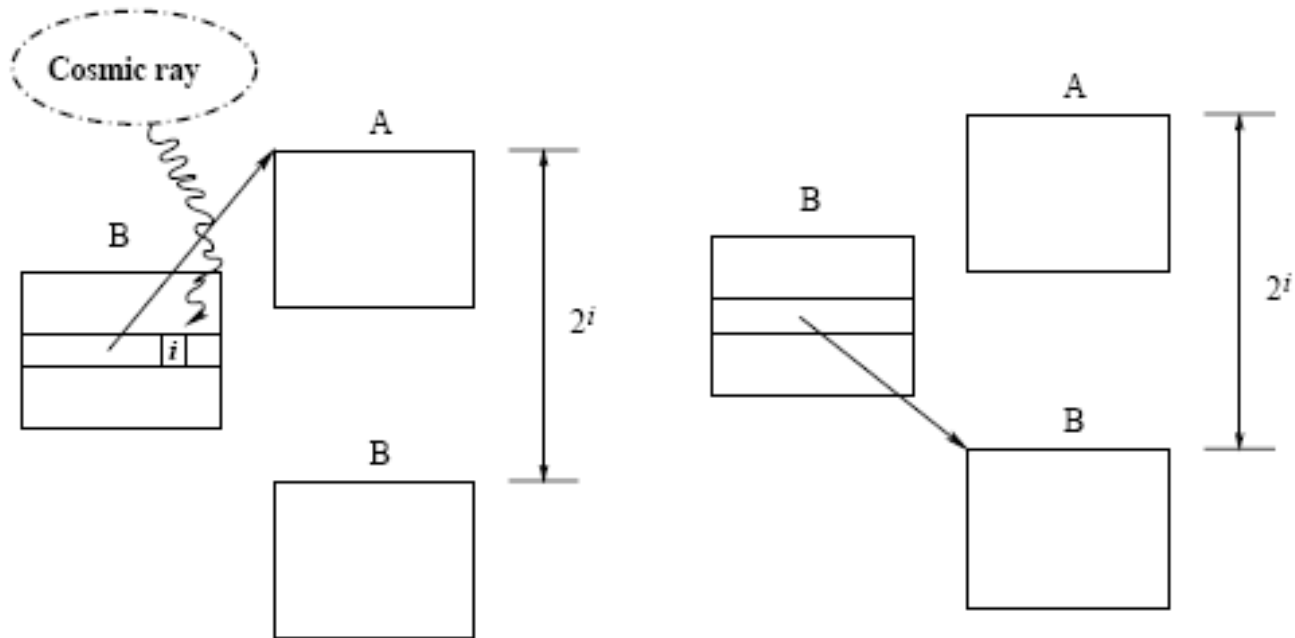
37

- $S = x^d \bmod N$
- Using CRT
 - $S1 = x^d \bmod p$ and $S2 = x^d \bmod q$ ($N = pq$)
 - $S = aS1 + bS2 \bmod N$
- Fault injected
 - $S1'$ not eq $S \bmod p$
 - $S2' = S \bmod q$
 - $\text{GCD}(S - S', N) = q$

Source: On the Importance of Eliminating Errors in Cryptographic Computations, Journal of Cryptology 2001.

Fault Injection

38



Source: Sudhakar et al. Using memory errors to attack a Virtual Machine, IEEE S&P 2003.

Logical Attacks

39

- Software Vulnerabilities
 - ▣ Buffer Overflow
- Protocol Vulnerabilities
 - ▣ Man-in-the-Middle

Take Aways

40

- Secure Embedded Systems is Imminent
- Every stage of design should consider security
- Should be built ground-up