UCLA

Challenges for the Logic Design of Secure Embedded Systems

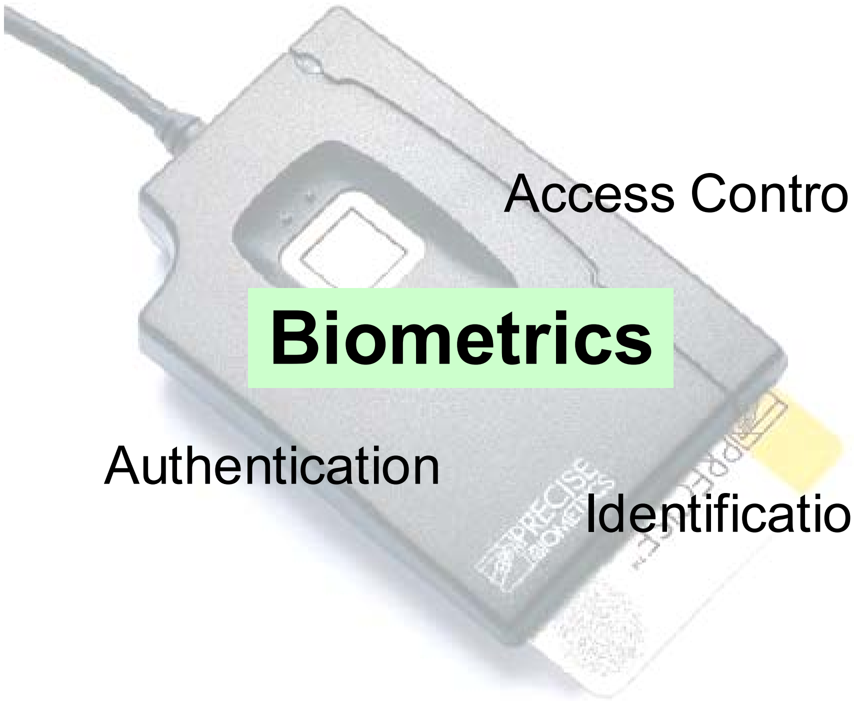
Patrick Schaumont, UCLA

Embedded Security Group (EMSEC) @ UCLA

Acknowledgements

- **ThumbPod2 Design Team:**
  - Kris Tiri, David Hwang, Alireza Hodjat, Bo-Cheng Lai, Shenglin Yang, Patrick Schaumont, Ingrid Verbauwhede
- **Research Support:**
  - NSF CCR 0310527, CCR 0098361
  - UC Micro
  - SRC 2003-HJ-1116
  - SUN
  - Panasonic
  - Atmel

Secure Embedded Systems

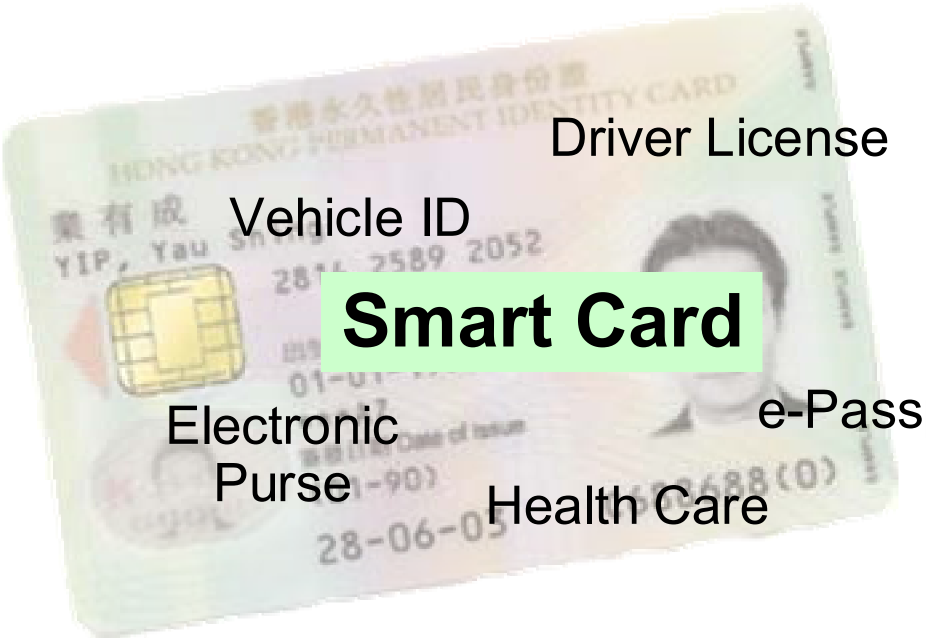


Access Control

Biometrics

Authentication

Identification



Driver License

Vehicle ID

Smart Card

Electronic Purse

e-Passport

Health Care

Electronic Ticketing

Keys

Inventory

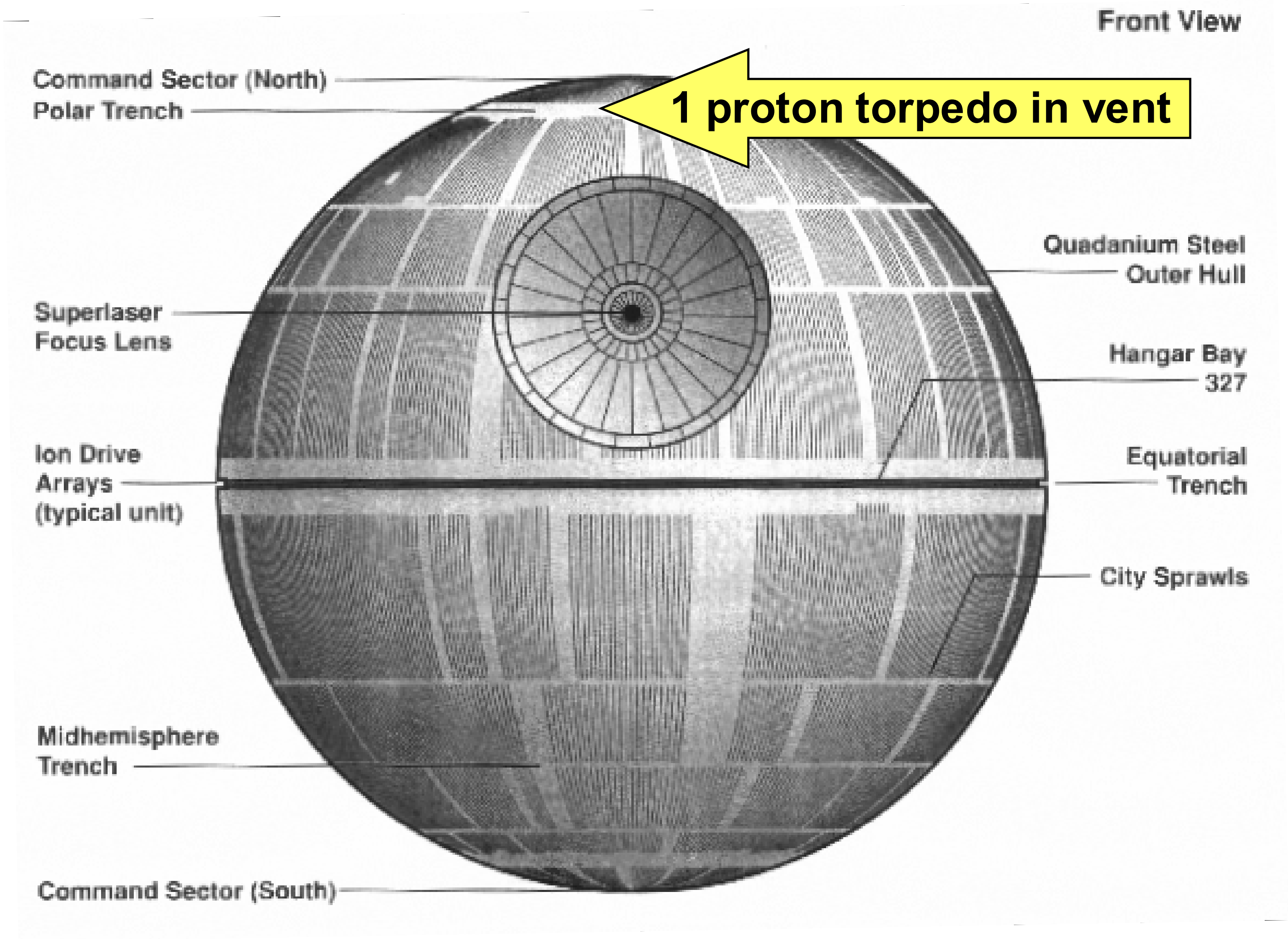
RFID

Tagging

Secure *embedded* systems face specific risks. They are

1. more accessible
2. more resource-constrained

Protecting the weakest link

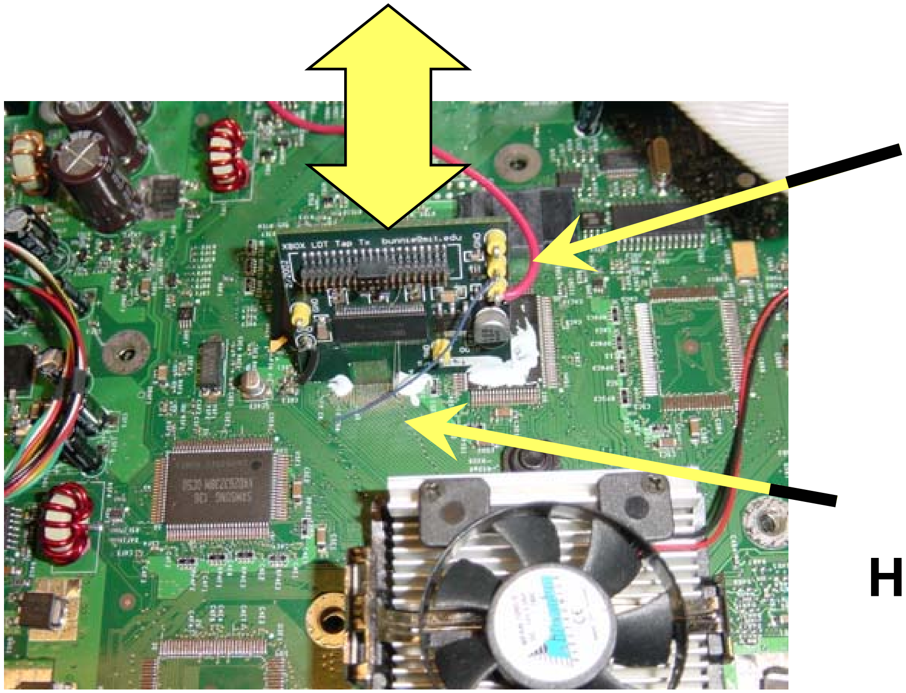


1 proton torpedo in vent

[http://www.obh.snafu.de/~madley/starwars/]

On a smaller scale: The X-Box case

To FPGA Board



Sniffer board

Northbridge
(with CPU)

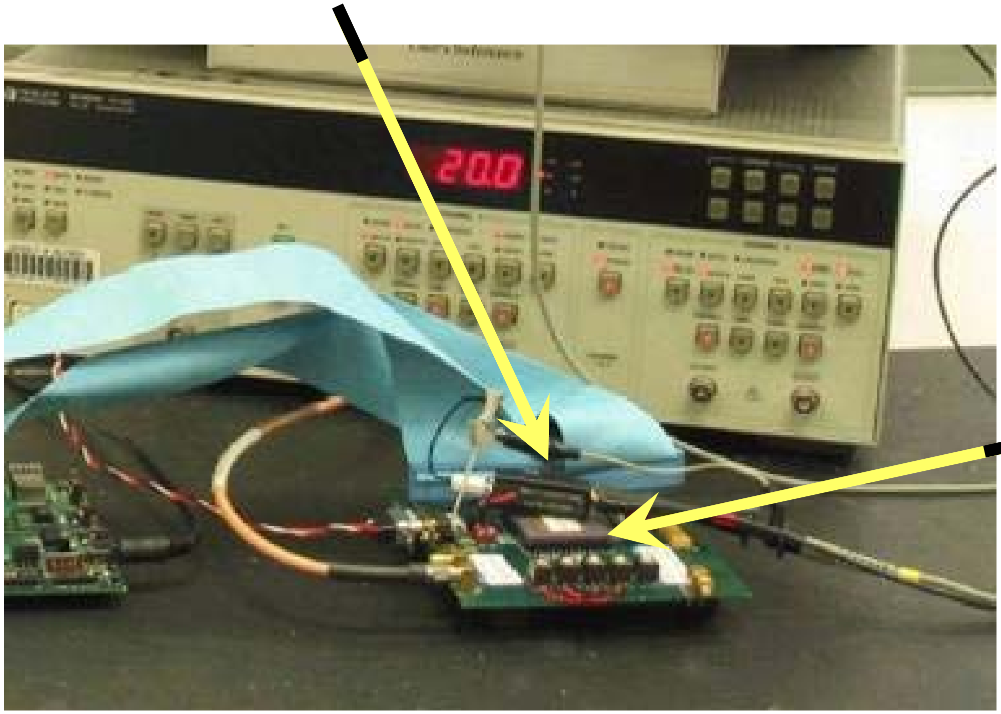
Differential
HyperTransport Bus

Southbridge
(with secret boot rom)

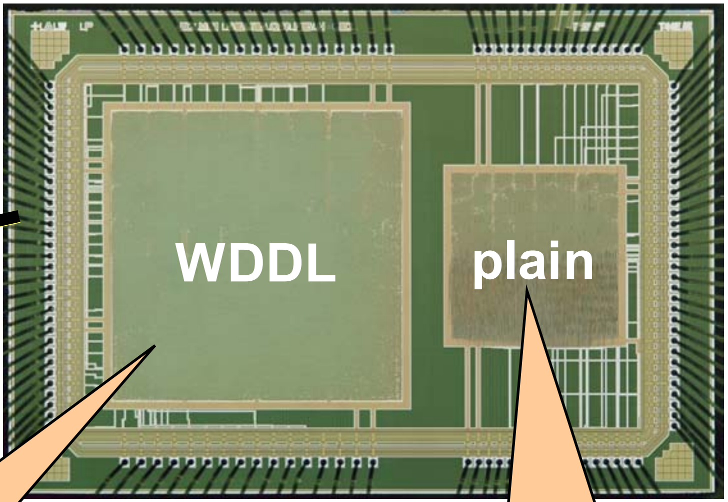
[by A. Huang, http://hackingthexbox.com/]

DPA Attack on ThumbPod

Current Probe



ThumbPod Chip (with 128-bit AES encryption unit)



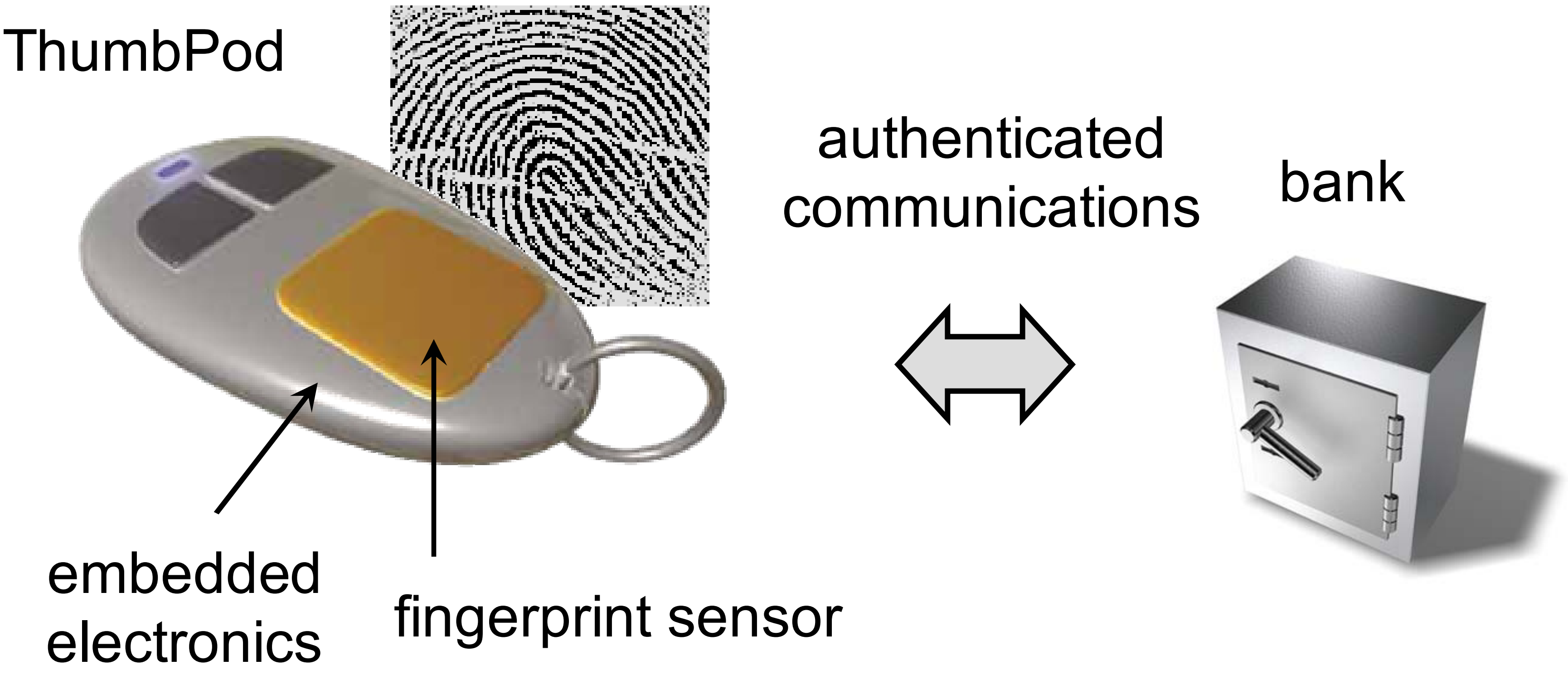
No full key disclosure under similar attack

Under DPA attack, key disclosure in 3 minutes

Overview

- The ThumbPod
  - Embedded Biometrics Authentication
- Side-channel attacks on embedded systems
- Systematic Design Methods for Security
  - System Design Methods
  - Logic Design Methods
- Design Challenges for Secure Embedded Systems

The ThumbPod Project



ThumbPod

authenticated
communications

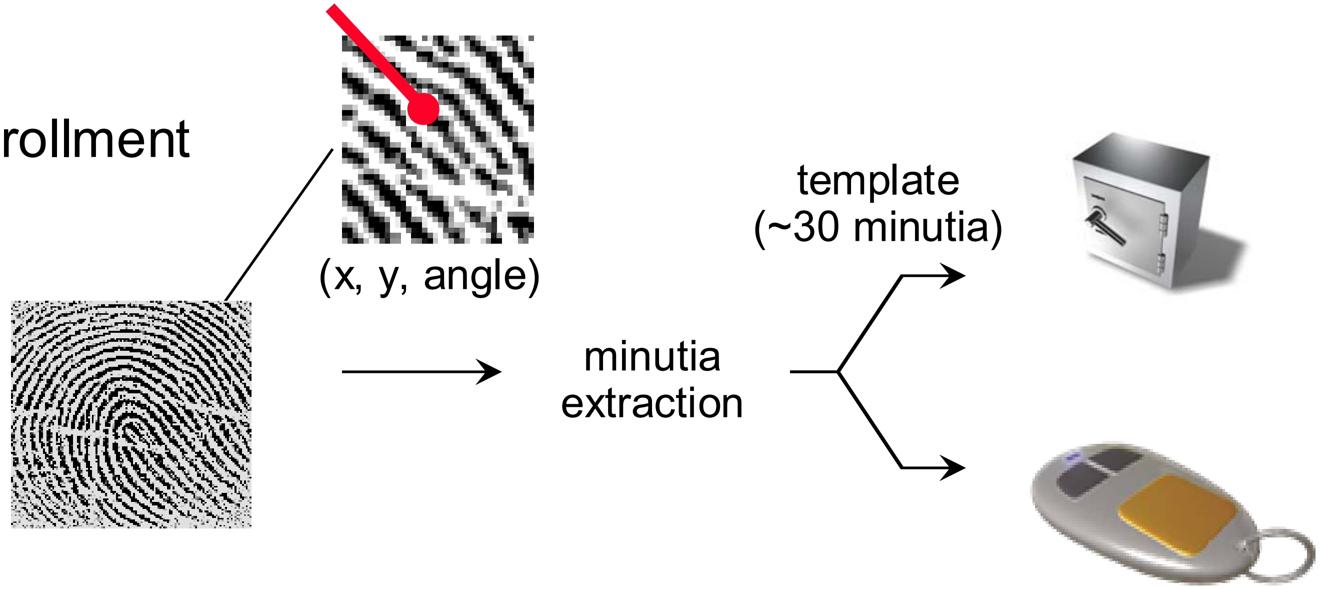
bank

embedded
electronics

fingerprint sensor

ThumbPod Operation

1. Enrollment

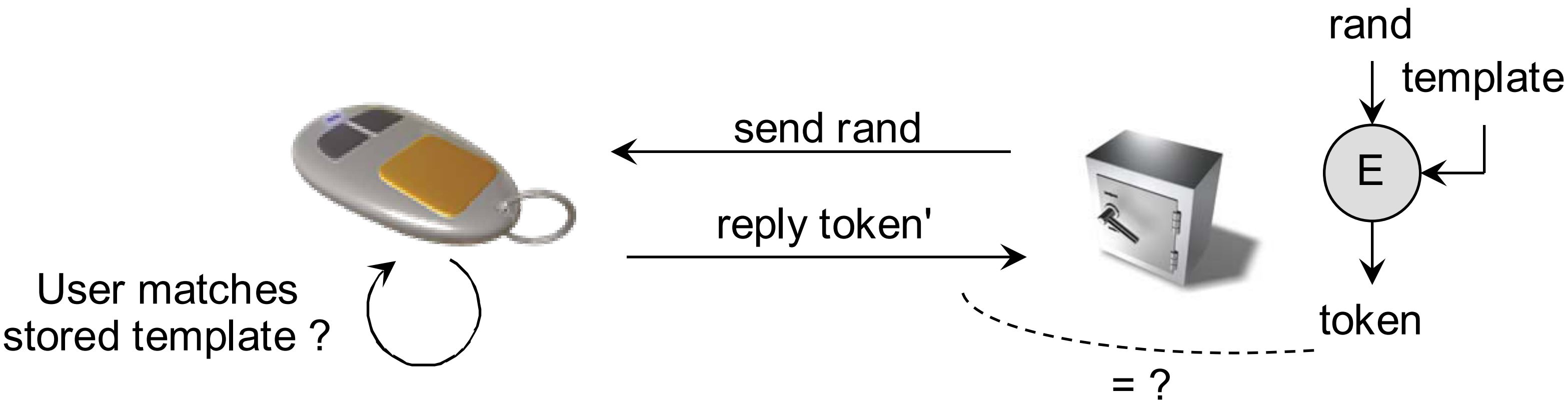


(x, y, angle)

minutia extraction

template (~30 minutia)

2. Normal Use



rand

template

E

token

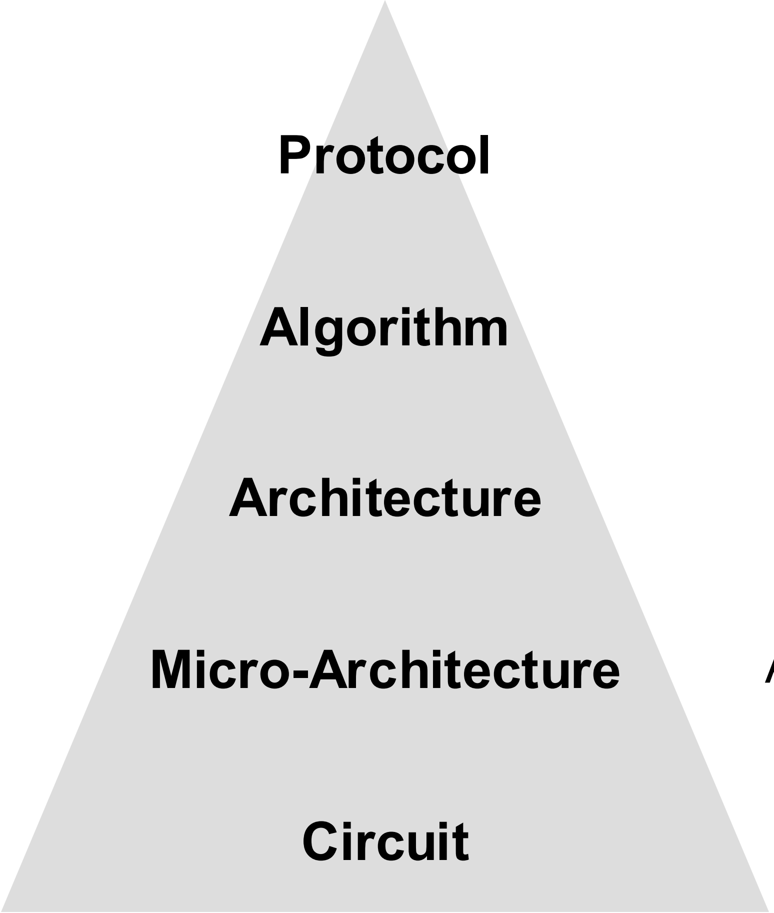
send rand

reply token'

= ?

User matches stored template ?

Securing Thumbpod

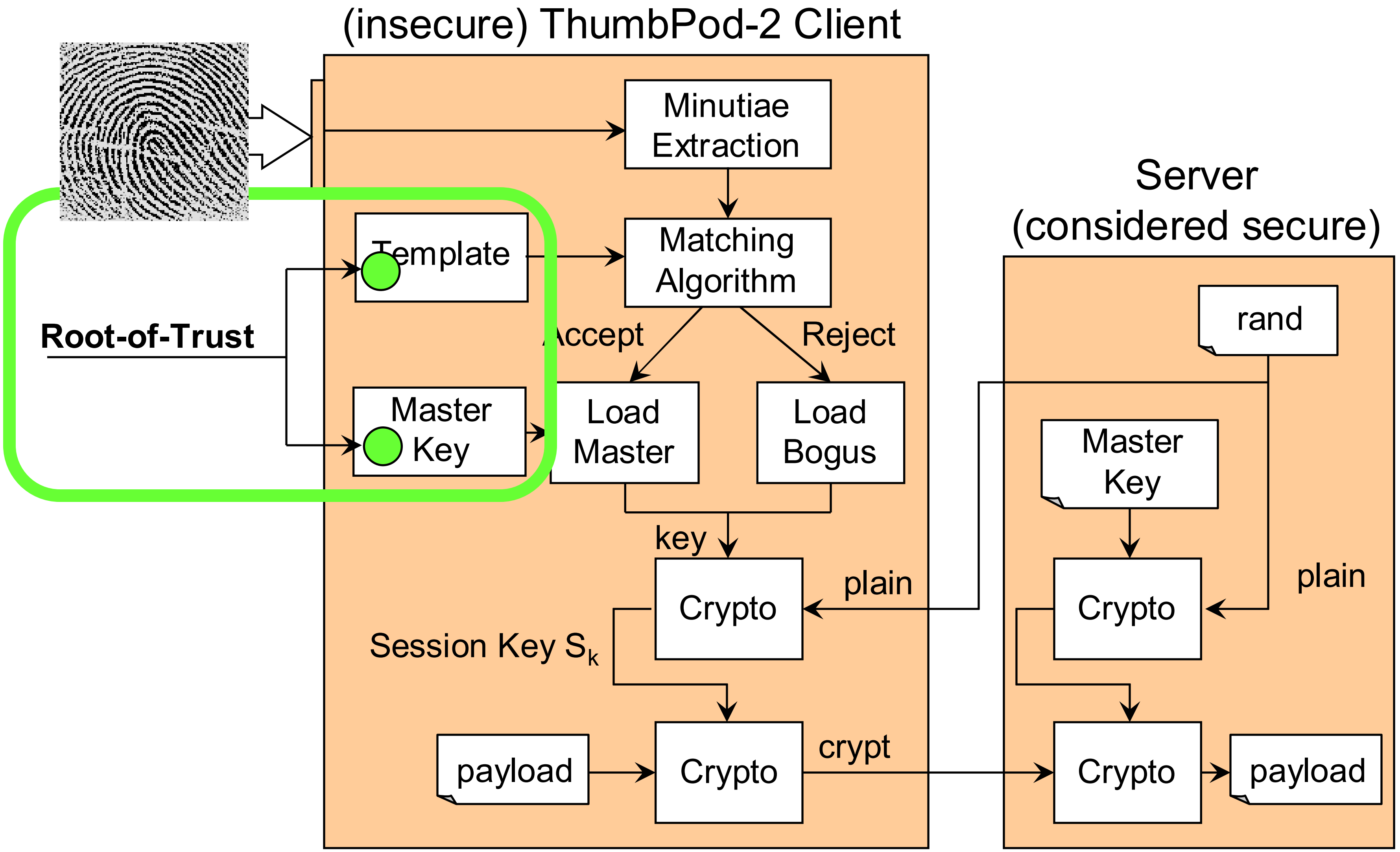


Security Abstraction Level	Security Objective	Side-channel attack
Protocol	Authenticated communications	Man-in-the-middle, Traffic analysis
Algorithm	Encryption/hashing	Known-plaintext, Known-cryptext
Architecture	Functional integration (SW)	Stack smashing
Micro-Architecture	Architecture integration (HW)	Bus probing
Circuit	Implementation	Differential Power Analysis

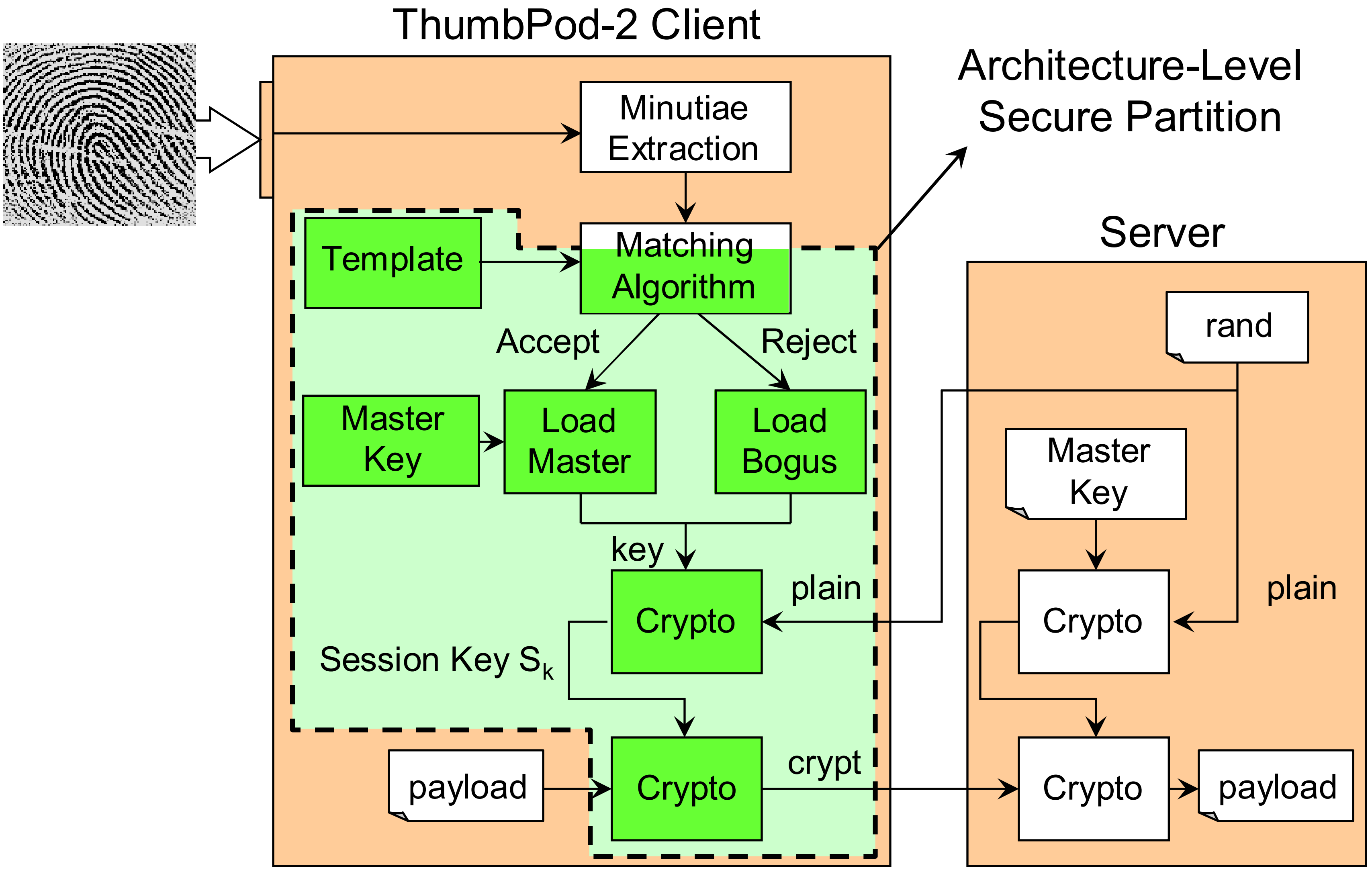
Systematic Design Methods

- **System Level**
  - Partition for security: protect Root of Trust
    - Root of Trust = A component that must behave as expected, because misbehavior cannot be detected (Trusted Computing Group)
    - Root of Trust = The part of the design that can hurt you ! (D. Gollmann)
  - Example to discuss - Secure biometrics in TP2
- **Logic Level**
  - How to create protection at the lowest abstraction level ?
  - Example to discuss - Protection of digital logic against Differential-Power Analysis

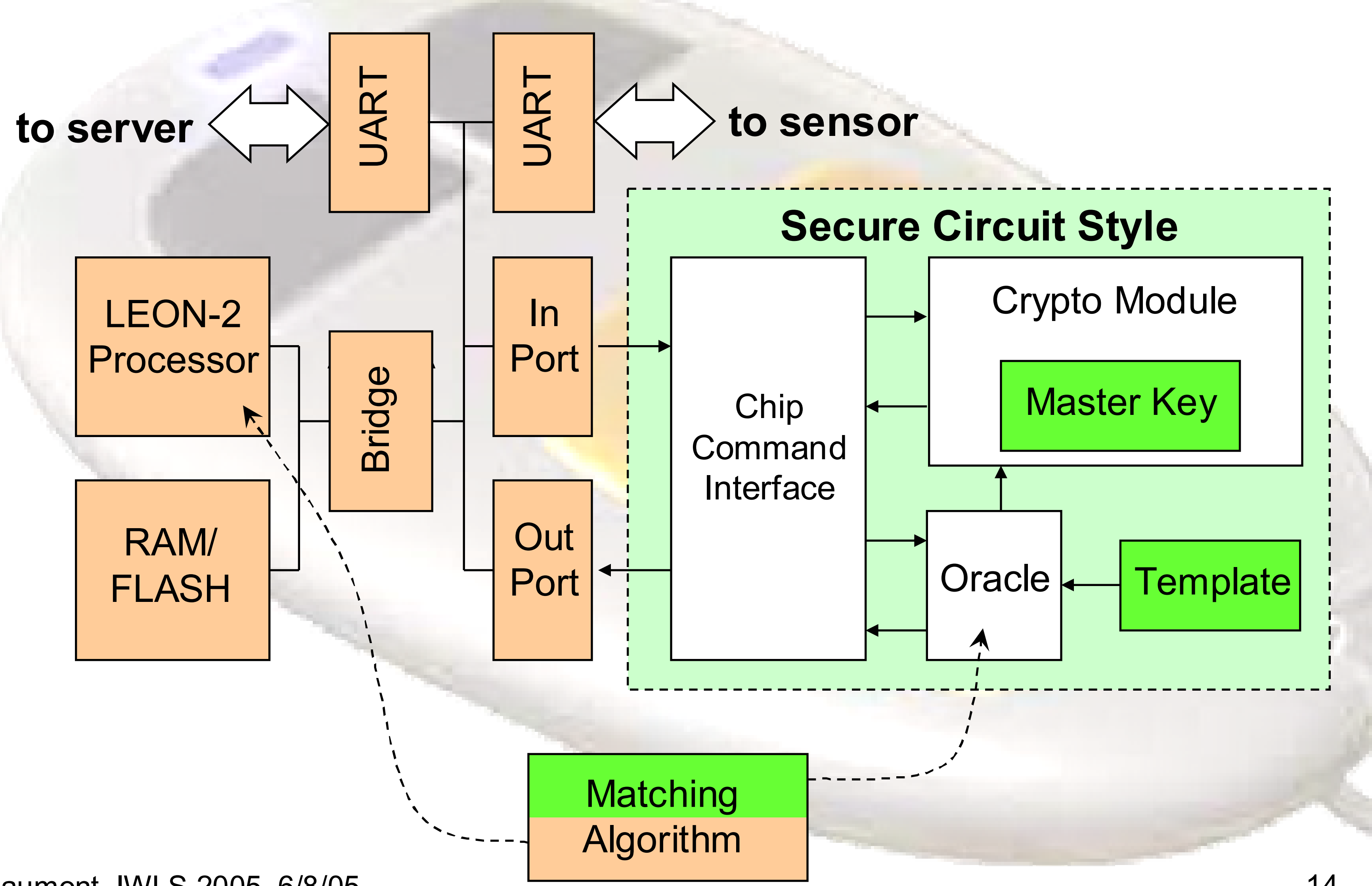
Partitioning the ThumbPod



Partitioning the ThumbPod



ThumbPod-2 Client Microarchitecture



Secure matching of Minutiae

Input

Template (secure)

Untrusted Software

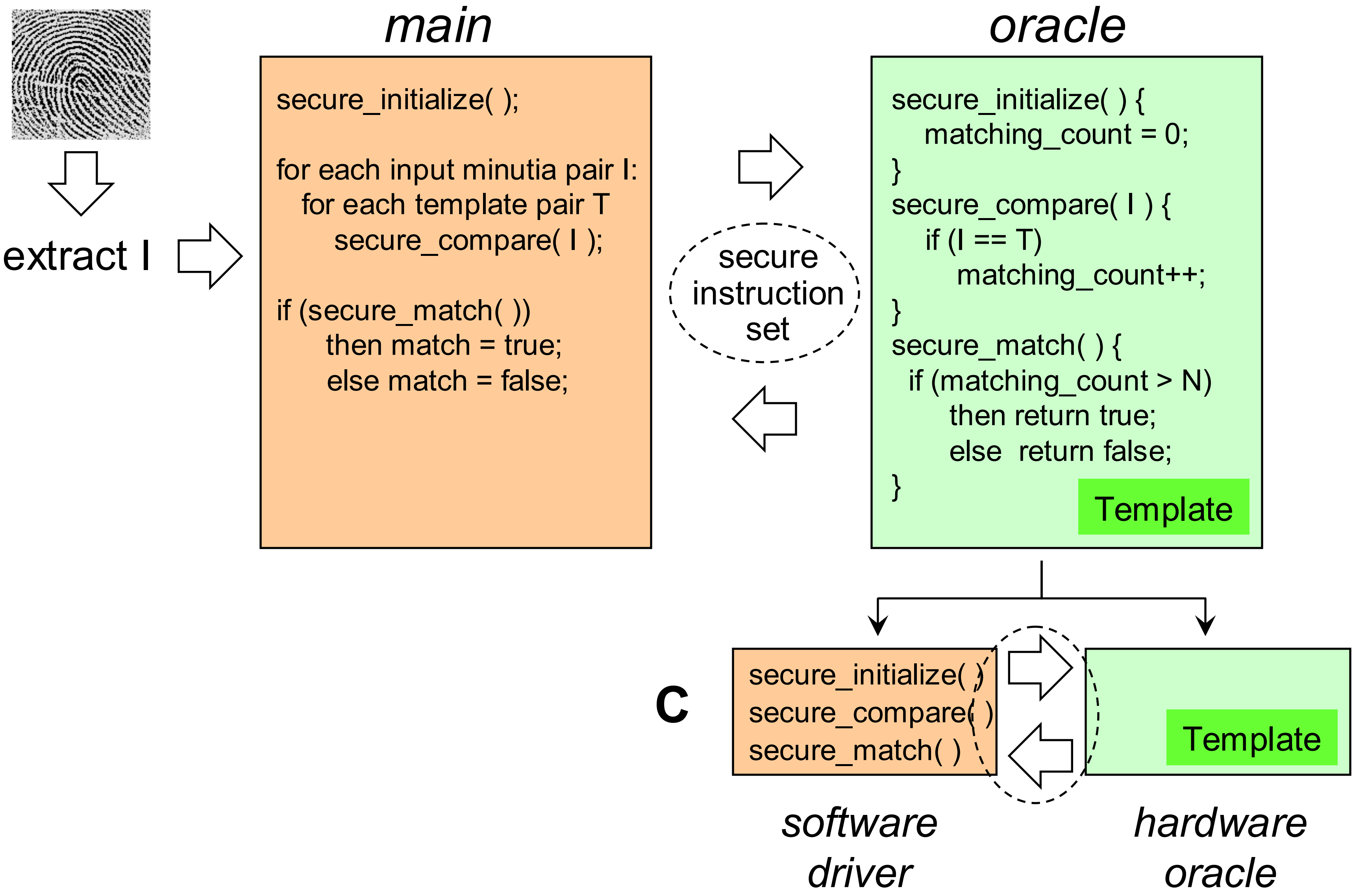
```
for each input minutia pair I:
  for each template minutia pair T:
```

Secure Circuit Style

```
    if (I ~ T)
      matching_count++;

if (matching_count > N) then match = true;
                         else  match = false;
```

HW/SW Partitions for secure matching



extract I

main

```
secure_initialize( );

for each input minutia pair I:
   for each template pair T
       secure_compare( I );

if (secure_match( ))
      then match = true;
      else match = false;
```

secure instruction set

oracle

```
secure_initialize( ) {
    matching_count = 0;
}
secure_compare( I ) {
    if (I == T)
        matching_count++;
}
secure_match( ) {
  if (matching_count > N)
       then return true;
       else  return false;
}
```

Template

C

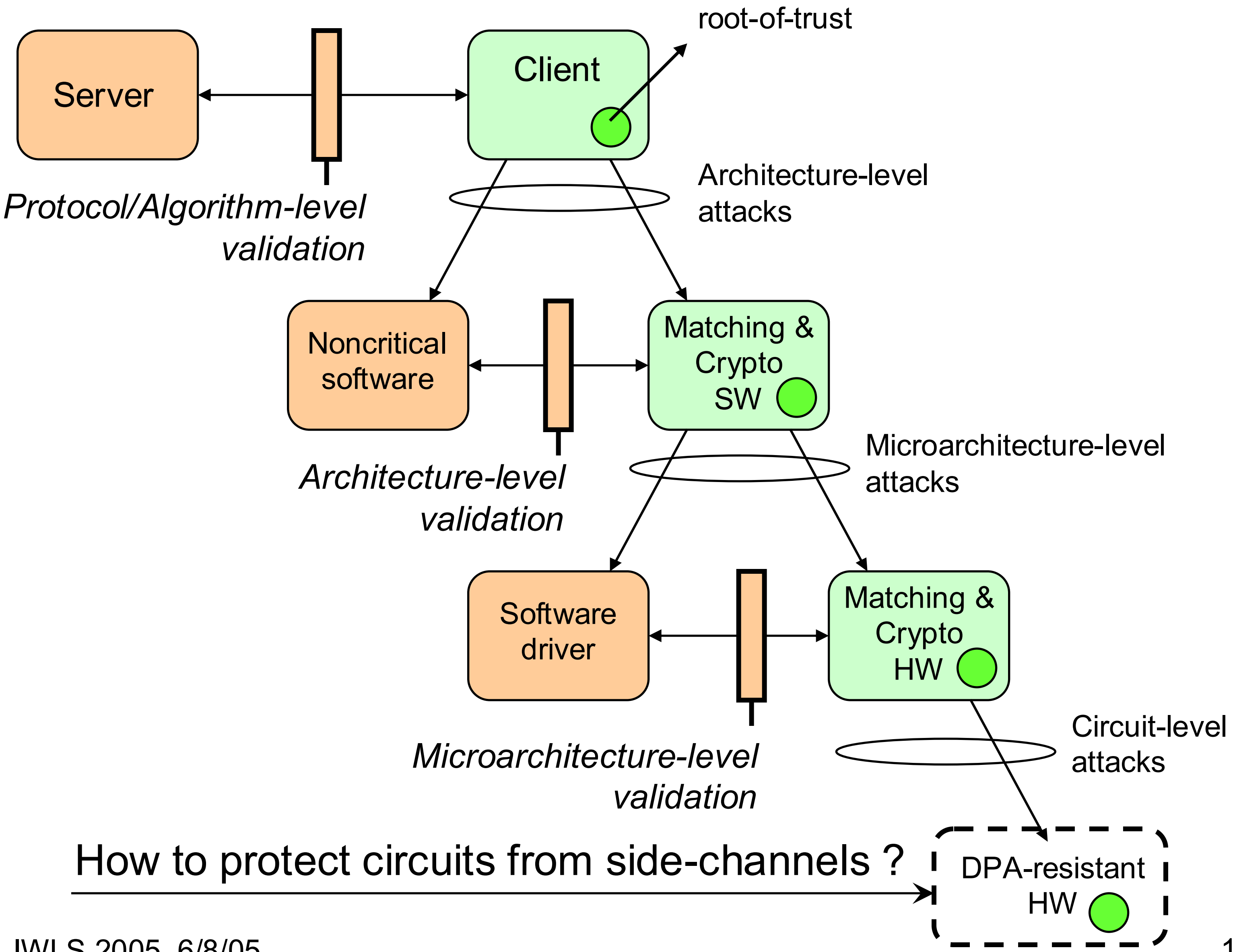
```
secure_initialize( )
secure_compare( )
secure_match( )
```

Template

software driver

hardware oracle

System-level Security Partitioning



Server

Client

root-of-trust

Protocol/Algorithm-level validation

Architecture-level attacks

Noncritical software

Matching & Crypto SW

Architecture-level validation

Microarchitecture-level attacks

Software driver

Matching & Crypto HW

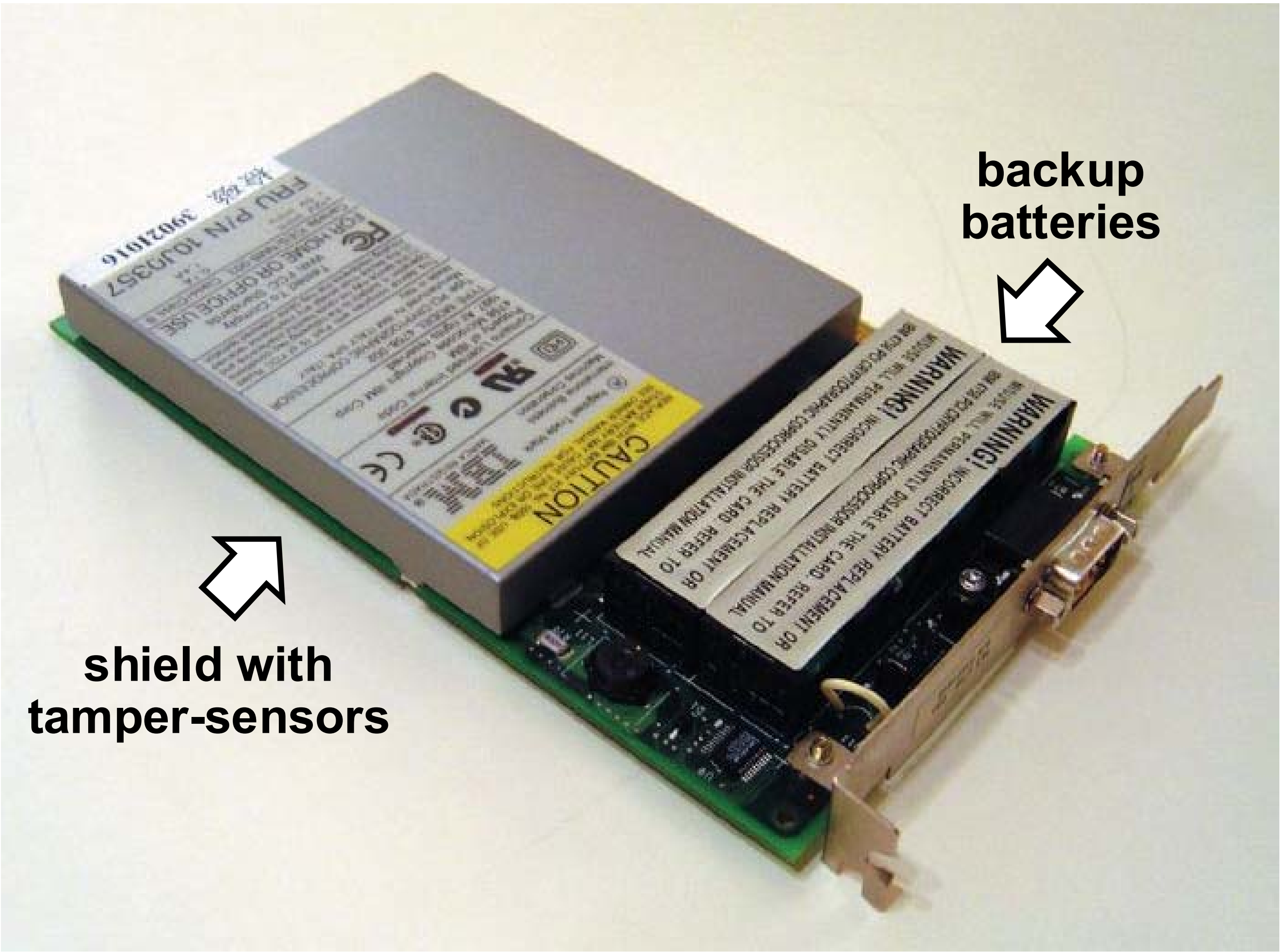
Microarchitecture-level validation

Circuit-level attacks

How to protect circuits from side-channels ?

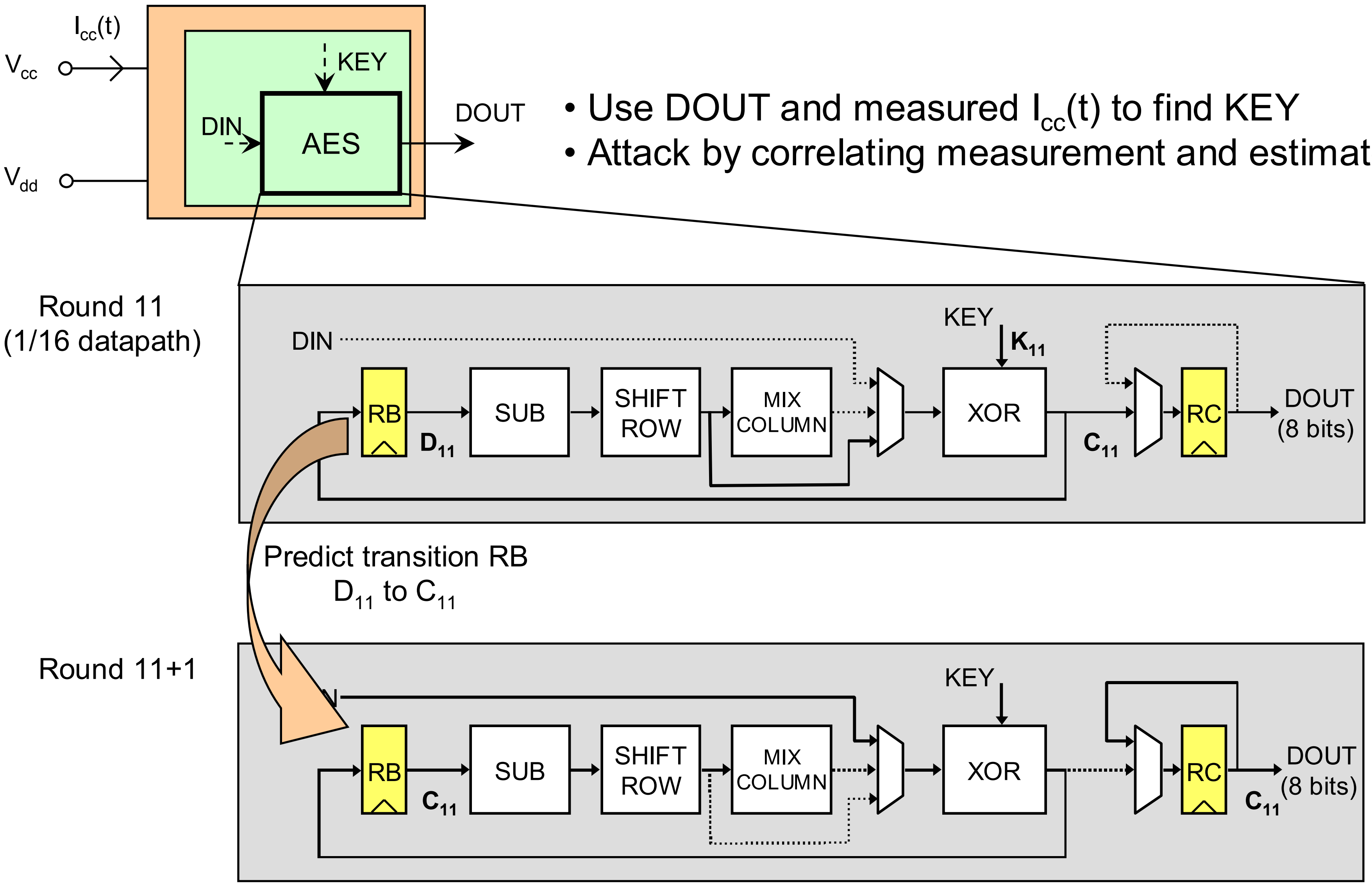
DPA-resistant HW

IBM 4758 Secure Coprocessor



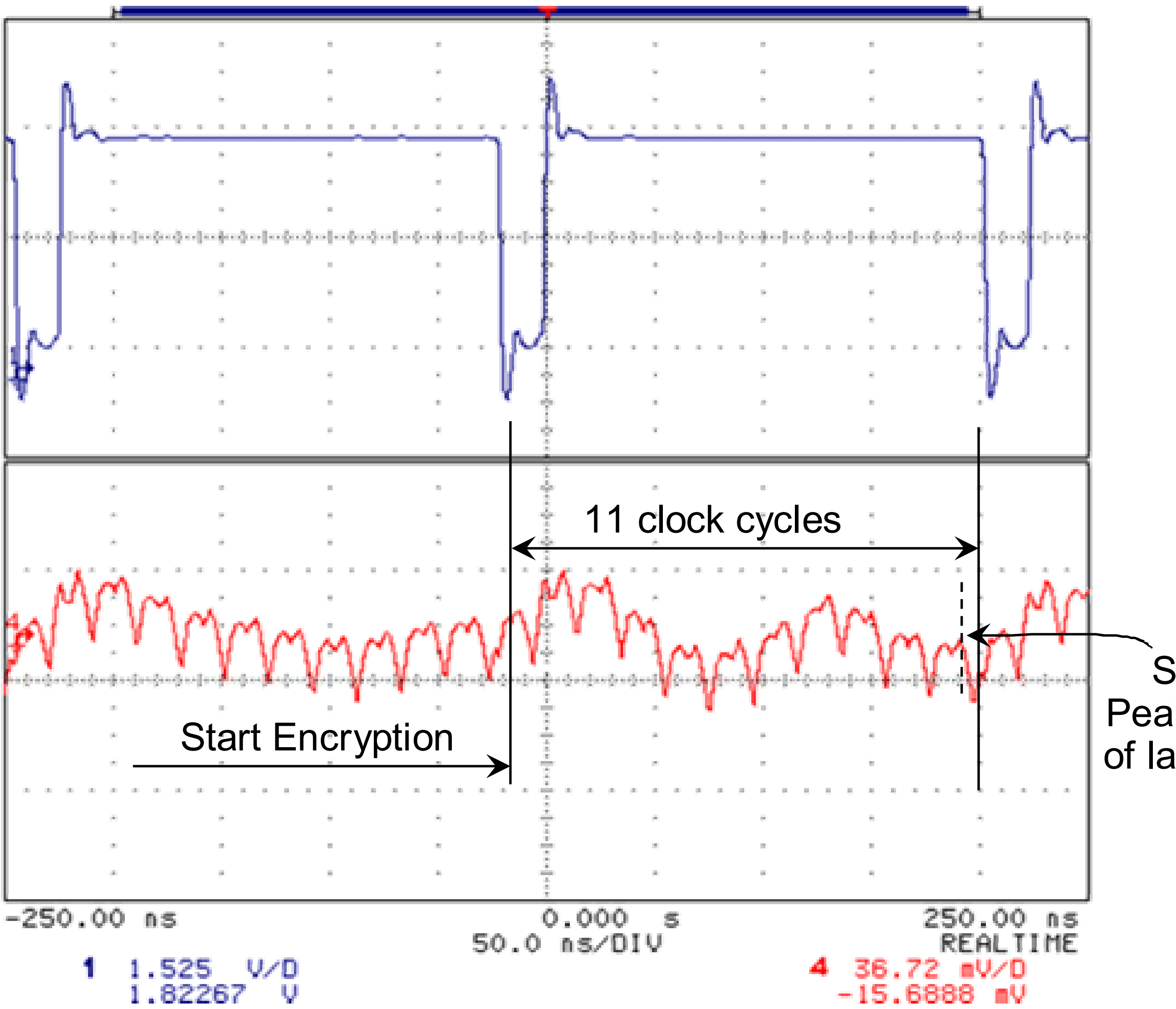
Differential Power Analysis Attacks

- Use DOUT and measured $I_{cc}(t)$ to find KEY
- Attack by correlating measurement and estimate



Example Power Measurement

Start Signal



Current Probe Output

11 clock cycles

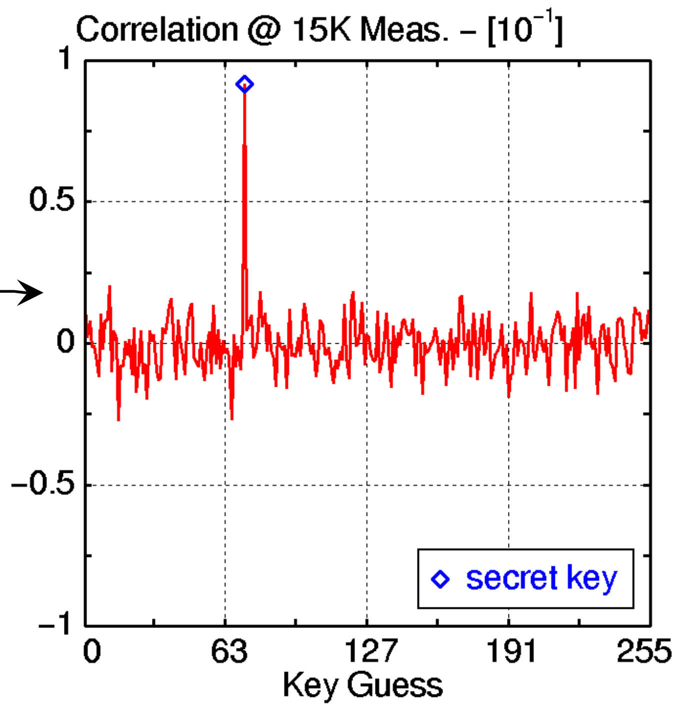
Start Encryption

Store Peak Value of last cycle

Differential Analysis Phase

Measurement	Actual P	Est. P $\vert_{KEY=K_i}$
1	P_1	E_1
2	P_2	E_2
3	P_3	E_3
4	P_4	E_4
5	P_5	E_5
N	...	...

$$C\Big|_{K_i} = \sum_{N} P_i\, E_i$$

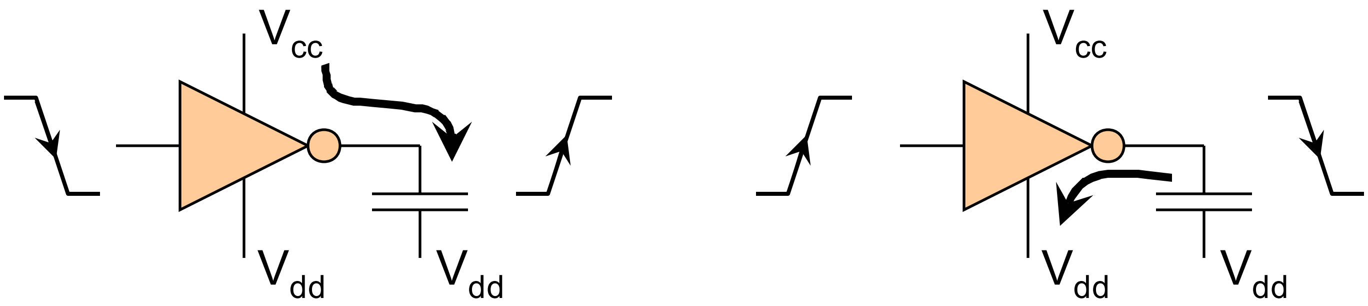


- Standard-cell AES is attacked in 3 minutes
  - 2^{128} problem converted into 16 * 2^8 problem
- Attack strength increases with number of measurements
- Measurement timing requires a priori knowledge on
  - crypto algorithm: cipher operation mode
  - crypto architecture: operation mapping & scheduling

Fighting DPA with constant-power circuits

The problem:

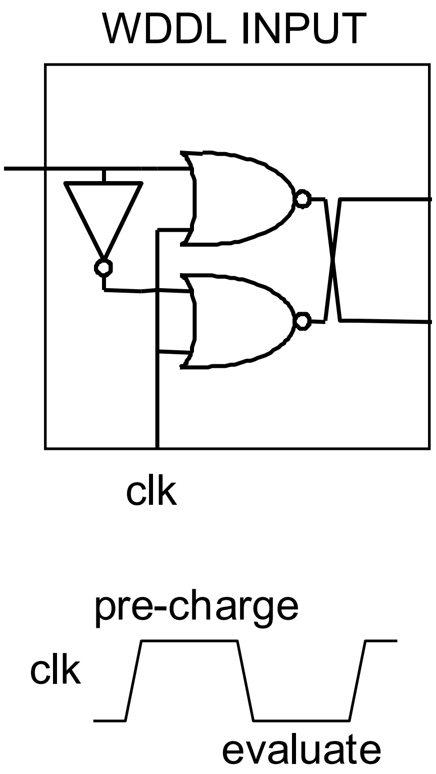
Dynamic power consumption is asymmetrical and dependent on data

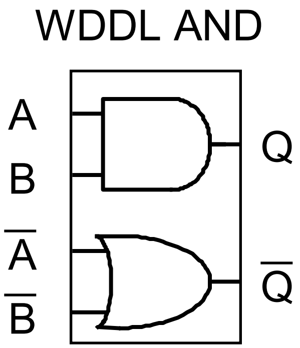


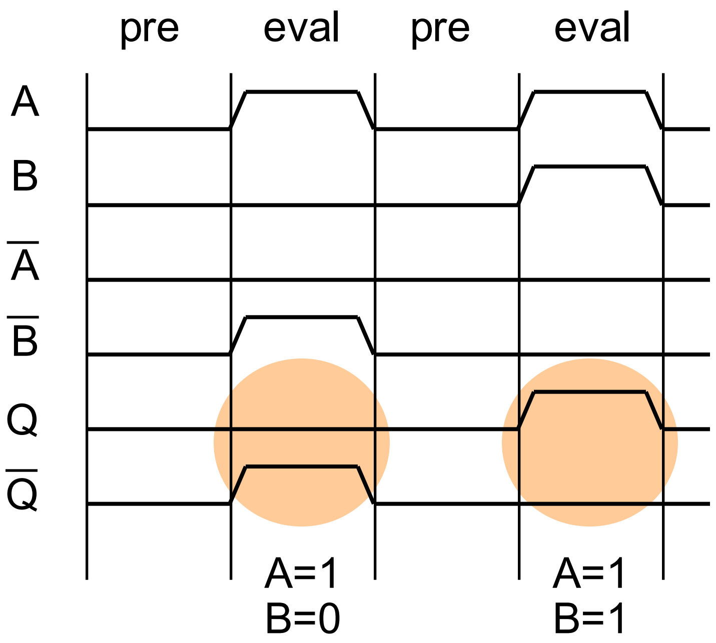
The solution:

- Consume the same current for all input patterns
- Differential Logic:
  - Use dual rail logic implementation
  - Makes '0' the same as '1' (hamming-weight independent)
- Dynamic Logic:
  - Use pre-charge phase and evaluate phase
  - Makes '0->0' the same as '0->1', '1->1', '1->0' (hamming-distance independent)

Wave Dynamic Differential Logic



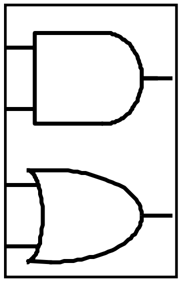




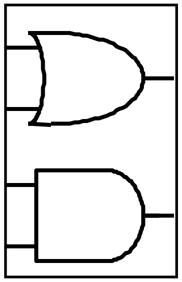
Always a single output transition

WDDL Library of 128 cells

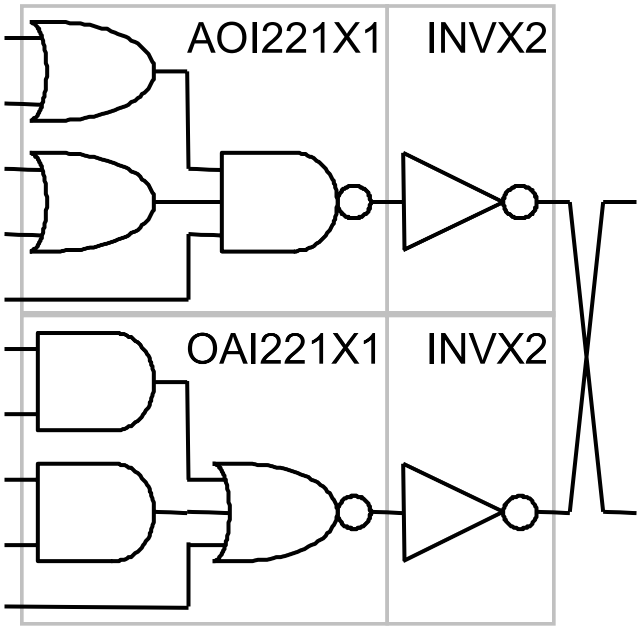
WDDL AND



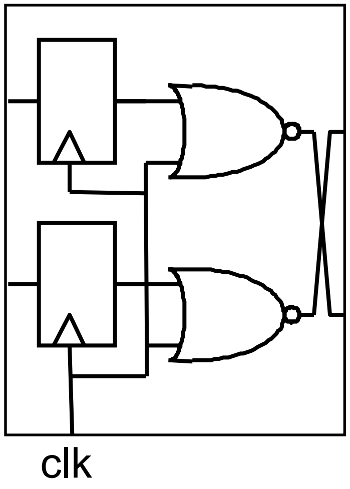
WDDL OR



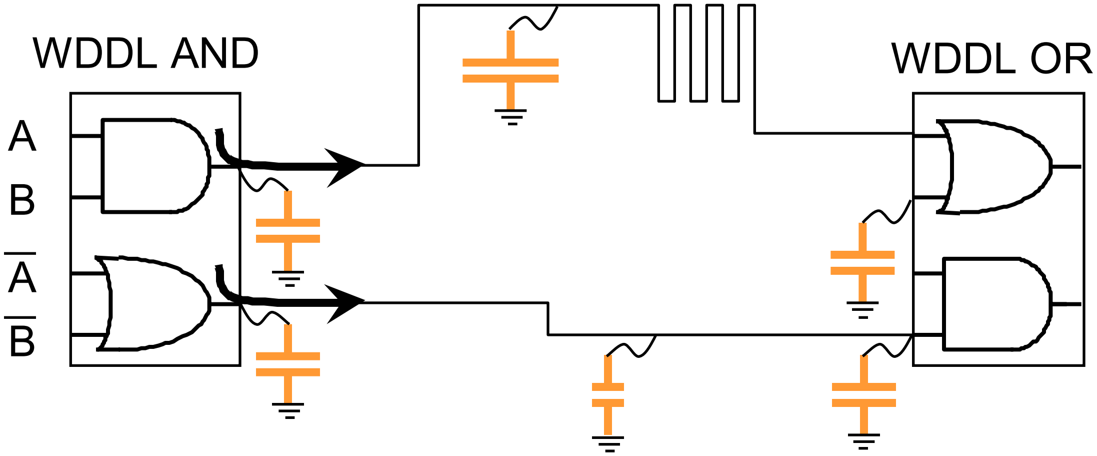
WDDL AOI221X2



WDDL register



Matching interconnect capacitance



Total capacitance = Output capacitance + Wiring capacitance + Input capacitance

(Cell design)

(Cell design)

Routing

Parallel tracks for constants mutual C

Equal via's, segment lengths, .. for constant R

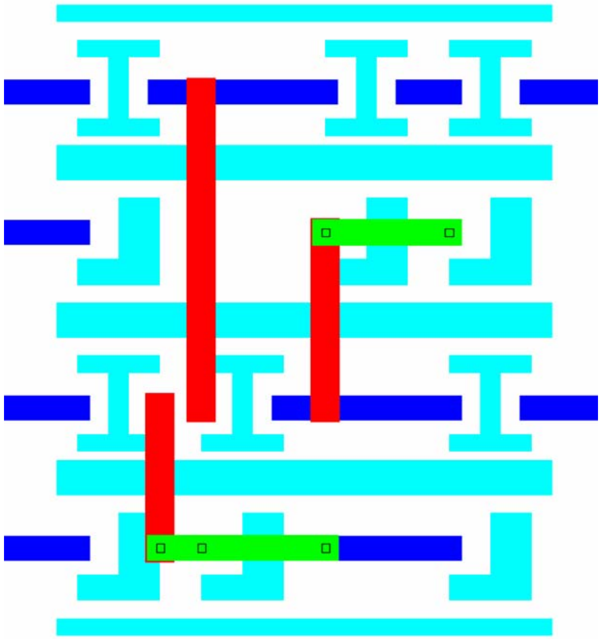
Identical crosstalk cap

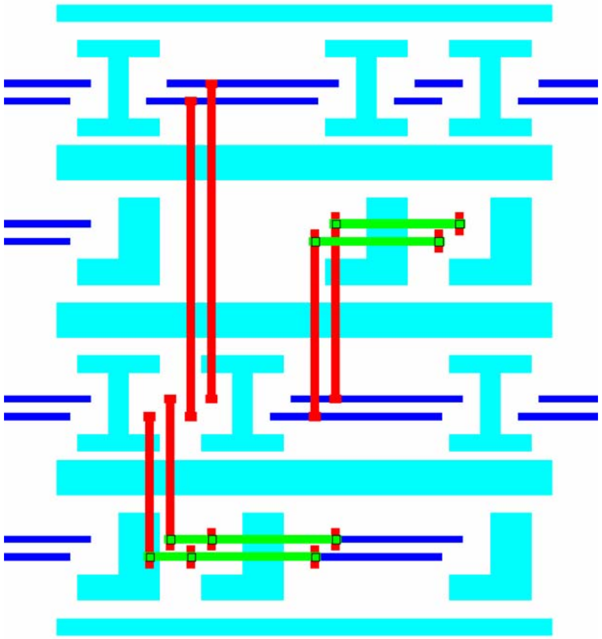
⇩

Mismatch causes 2nd order effects !

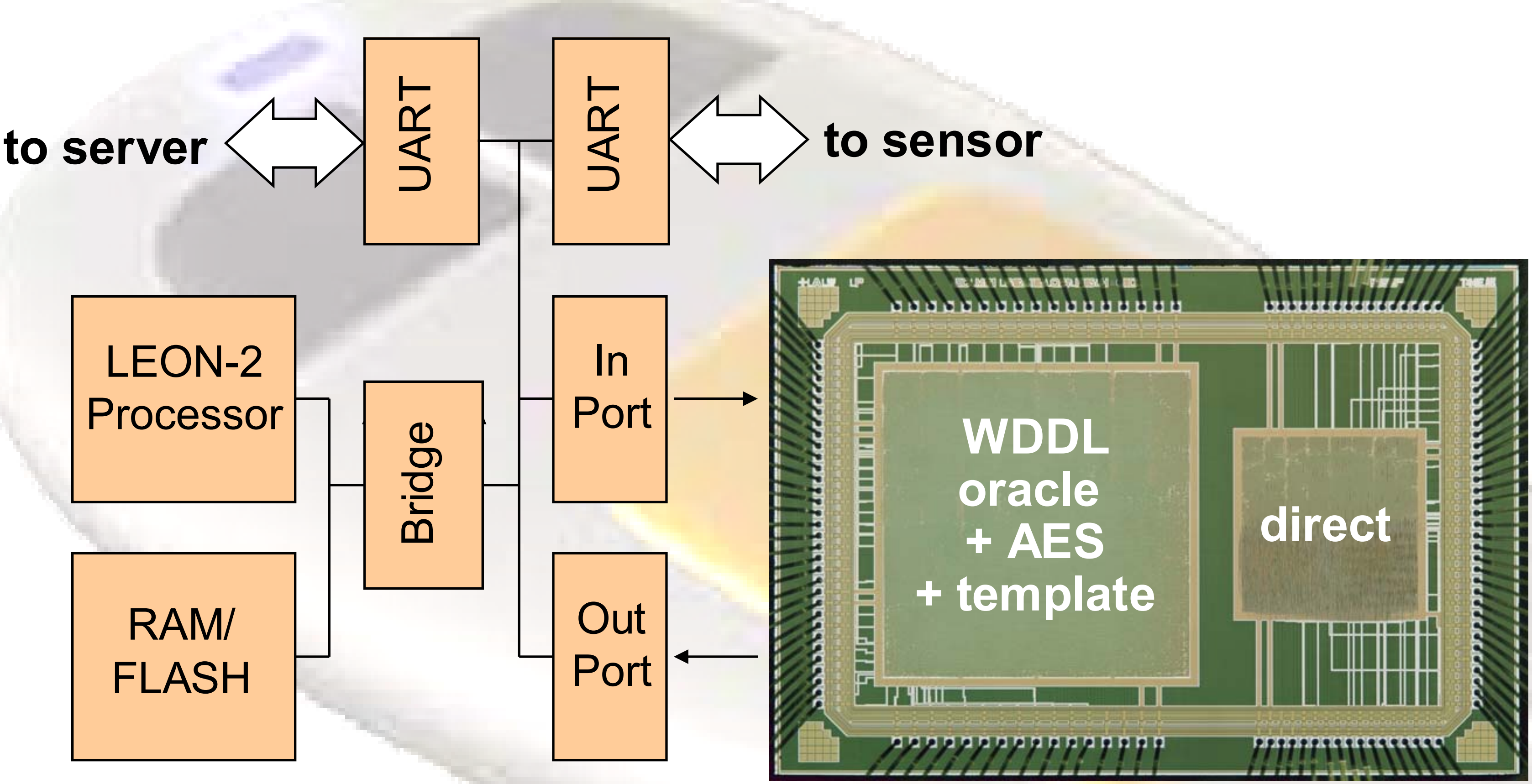
Differential Routing Technique

- Gridless routers do no scale well to complex netlists
- Gridded routers avoid parallel routing
- Enhanced gridded router with 'fat-wire' transformation technique produces accurate matching

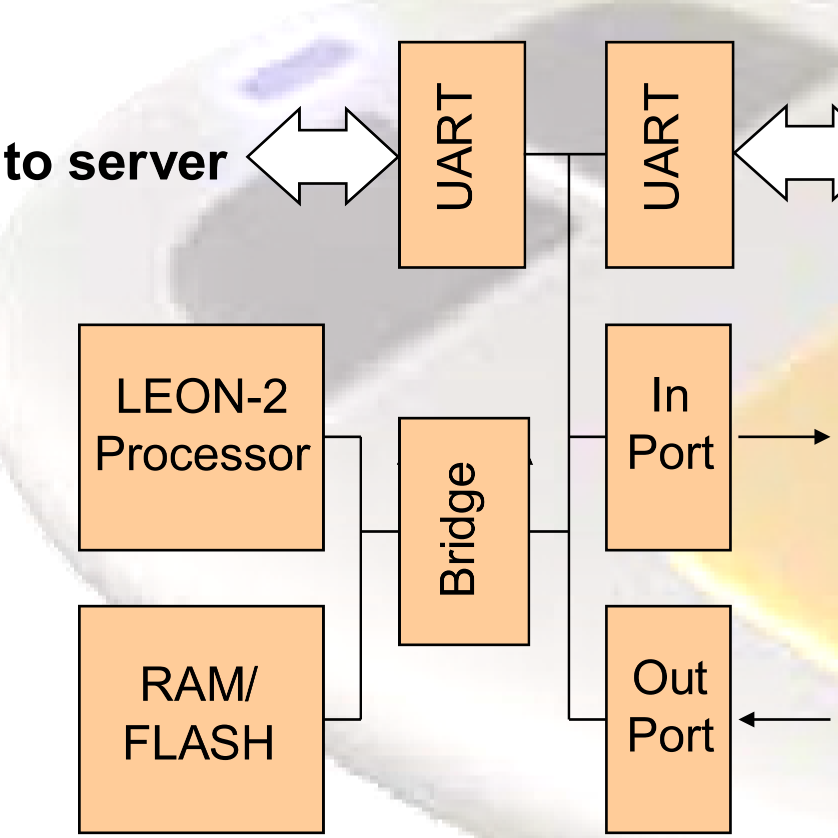


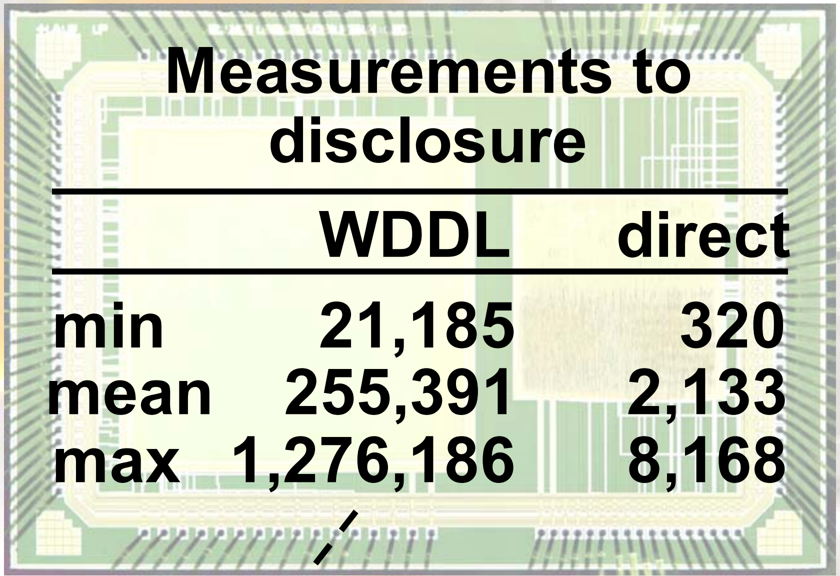


ThumbPod-2 Secure Coprocessor



DPA on ThumbPod 2



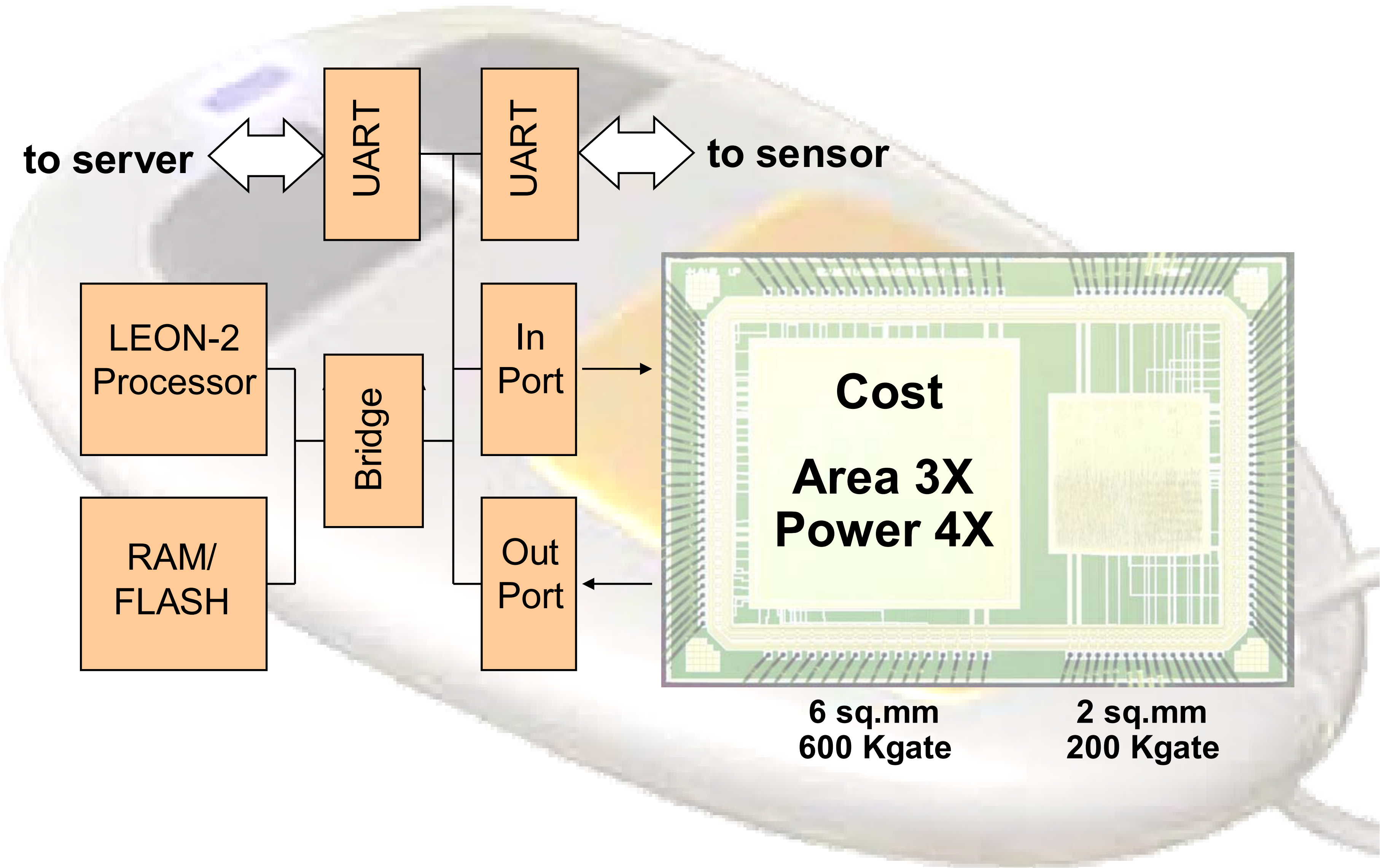


Measurements to disclosure

	WDDL	direct
min	21,185	320
mean	255,391	2,133
max	1,276,186	8,168

(11 key bytes from 16 are disclosed)

DPA on ThumbPod 2



to server

UART

UART

to sensor

LEON-2 Processor

Bridge

In Port

RAM/ FLASH

Out Port

Cost

Area 3X
Power 4X

6 sq.mm
600 Kgate

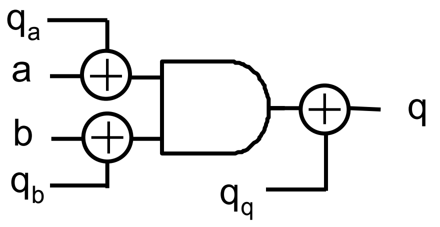
2 sq.mm
200 Kgate

Challenges for secure system design

- System level:
  - Trusted computing aims to support protected capabilities, integrity measurement, integrity reporting. http://www.trustedcomputinggroup.org
  - 'Trusted computing' covers only the general case, application-specific solutions are still needed
  - **Tool support** (for Thumbpod-type of designs)
    - Make security and trust 'measurable' as a quality of individual bits & operations on these bits (modeling issue)
    - Partition algorithms in secure/non-secure parts: measure information spread in the algorithm
    - Transform secure part to minimize complexity
    - Validate & verify security protocol and protocol faults

Challenges for secure system design

- Logic level:
  - Two approaches to make DPA hard:
    - Make measurements harder (random power variations etc): risky .. better to *remove* a side channel instead of obfuscating it
    - Make estimates harder: has algorithmic impact
  - Key issue in WDDL is to maintain symmetry.
    - Other technologies (e.g. FPGA) ? Other concepts (RAM) ?
  - Masking requires glitch-free implementation and is expensive: how to solve this ? (Mangard et al, RSA 2004)
  - Tools:
    - Accurate estimation (Power, Cap) WDDL is 'perfect' according to tools, but imperfect in real life ...



Corollary: Measurement is the best estimation

Challenges for secure system design

- Circuit level:
  - Reduce area/power overhead of secure implementation
  - Differential routing techniques for DPA resistance
  - Uniqueness (cfr Physically Unclonable Functions, PUF) for key-pair generation, tagging applications
- Additional notes
  - Embedded Security is a big opportunity for hardware and logic
  - Hardware offers qualities that software has lost (viruses etc)
    - Besides performance, offers *assured* and *constant-time* behavior
    - Recent attack on hyper-threaded processors clarifies the issue for software
  - But for Big Time Secure Hardware
    - need modeling & design support for the complete security pyramid (protocol, algorithm, ..., circuit)
    - need to recognize the weakest link principle:
      look at the *complete* system and at *multiple* abstraction levels

References

- ThumbPod Project
  - http://www.emsec.ee.ucla.edu/thumbpod
- Security Partitioning
  - D. Hwang, I. Verbauwhede, "*Design of Portable Biometric Authenticators—Energy, Performance, and Security Tradeoffs*", IEEE Trans. Consumer Electronics, November 2004.
- Embedded Security & Codesign
  - P. Schaumont, I. Verbauwhede, "*Domain specific codesign for embedded security*," IEEE Computer, April 2003.
- WDDL
  - K. Tiri and I. Verbauwhede, "*A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation*," DATE 2004.
- Measurement is the best estimation
  - K. Tiri and I. Verbauwhede, "*Simulation Models for Side-Channel Information Leaks*", DAC 2005 (Session 14.2)