Secure Smartcard Design against Laser Fault Injection

FDTC 2007, September 10th

Odile DEROUET

Agenda

- Fault Attacks on Smartcard
- Laser Fault Injection
- Our experiment
- Background on secure hardware design
- Samsung Laser fault detectors design and validation
- Conclusion

Fault attacks on smartcard (principle)

Smartcard are specially designed:

- to protect sensitive content such as user secret data or cryptographic keys
  - Secure data storage
- Process those information securely
  - Secure execution (encryption, signature..)

Fault attack on smartcards

- Modify the device normal operating condition in order to generate processing errors (VCC glitch, light, laser…)
  - Retrieve secret information, secret keys
  - Bypass secure execution (pin code, call to crypto algorithm)

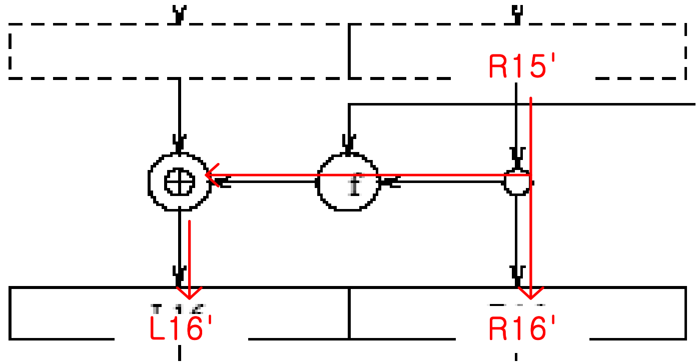
Fault Attacks on Smartcard (Example)

Bellcore attack on RSA CRT (1996)

$Sp = M^d \bmod P$
$Sq' = M^q \bmod Q$
$S' = CRT(Sp, Sq')$

$GCD(S - S', N) = p$

DFA on DES



Fault attack on Operating System

```
        ld      A8, #(SFRBASE+DESKEY1)
        ld      A10, #_DES_key
// fill K1
set_key1ns
        ldb     R0, @[A10+R6]
        ldb     @[A8+R6], R0
        bnzd    R6, set_key1ns
        nop
```

Corrupt register

Skip instruction

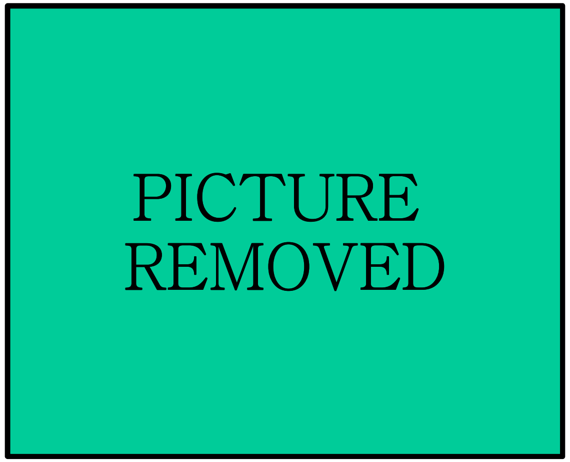
```
EXT     R4
LD      A12,#_DES_key
LD      A13,#_DES_data
JSR     $__DES_process
LDB     R4,@[A13]         ;_i
LD      R2,R4
```

SAMSUNG DIGITall everyone's invited

Laser Fault Injection

- **Laser fault injection consists in exposing the device to an intense light for a brief period**
- **Why this attack is so powerful :**
  - **Geometric accuracy:**
    - possibility to focus the laser on a very specific part of the device
      - ➲ up to 1~2um (in general ~40um square)
  - **Time accuracy:**
    - Possibility to select precisely the moment where the pulse should be sent
      - ➲ ~nanoseconds precision
  - **Generate temporary faults:**
    - the device remains functional after the fault is sent, attack is reproducible

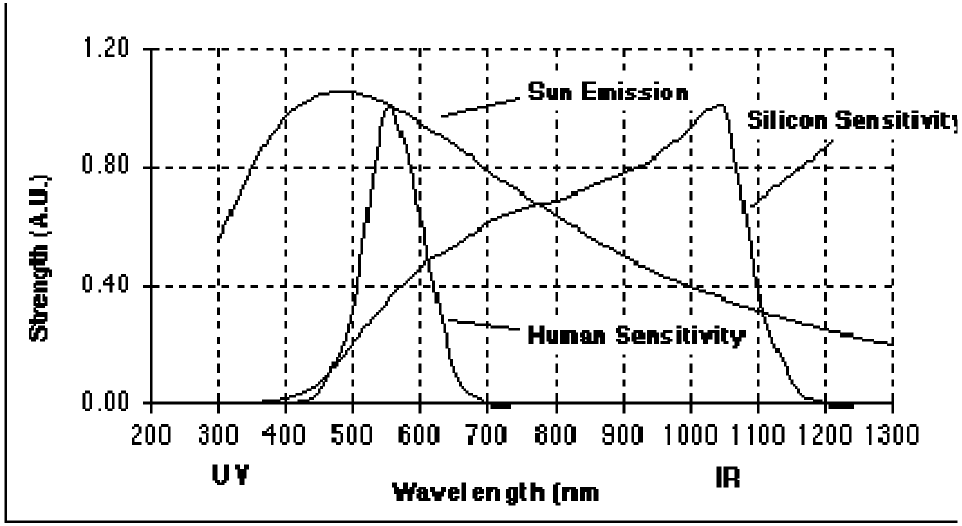
Laser Fault Injection



Common Setting

- Typical laser source : pulsed nanosecond laser with selectable wavelength
- Focused with optical microscope or` single lens
- The target device is mounted on an automated table
- The whole surface of the device can be scanned while pulses are sent on top of the devices
- Pulse moment is controlled by triggering the device IO
- Pulse duration should fit into the device cycle period (~several nanosecond)

Laser Fault Injection



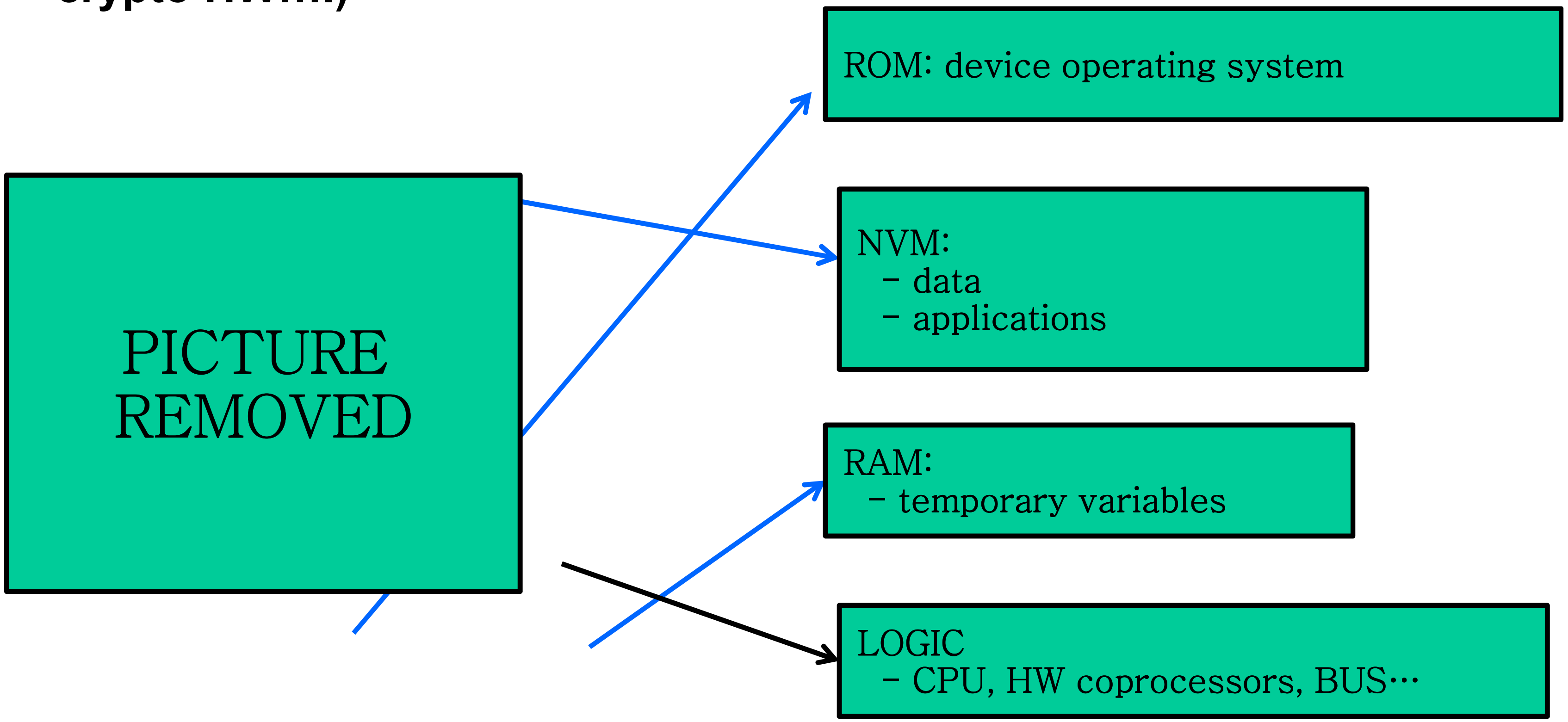
PICTURE REMOVED

- **Choice of the wavelength**
  - A smartcard microcontroller is generally made of several layers
    - Depending on the laser wavelength both front and back side of the device can be perturbed
  - From 400nm to 1200nm silicon might be perturb by the laser pulses
  - The penetration depth increase exponentially with the laser wavelength
    - Green light (~500nm) efficient on front side
    - IR (~1000nm) efficient on backside
- **Effect of laser**
  - When the charge accumulated by photons injected by laser exceed threshold value, the value of the transistor is switched

SAMSUNG DIGITall everyone's invited

Our experiment On a Dummy smartcard

- **Typical Smartcard : ROM, NVM, RAM, Logic (CPU, crypto HW….)**



- **Potentially, any part of the silicon can be attacked provided the pulse location matches with processed operation**

Our Experiment

- **Variety of error depending on pulse location**

	Logic	ROM	RAM	NVM
Wrong cryptographic calculation	X			
Data read or write error	X	X	X	X
Wrong address read or write	X			
Instruction skipped/corrupted	X	X		X
Wrong CPU calculation	X			
Register corruption	X			

- Several command involving different devices operations (CPU, crypto…) are performed
- Laser pulses are sent in "single" , "burst" or "continuous" mode while the whole surface of the device is scanned.
- When a a fault occurs the device send "error" code and the pulse location is recorded
- Among all areas, the logic part leads to a variety of different errors.

Our Experiment

- **For all error cases we cross checked the errors points with detailed layout of the device**

Spot:
holder

PICTURE REMOVED

- **We observed that most of error points matched with FLIP-FLOP and BUS holders (latch)**
  - We used this assumption to design our laser fault detectors

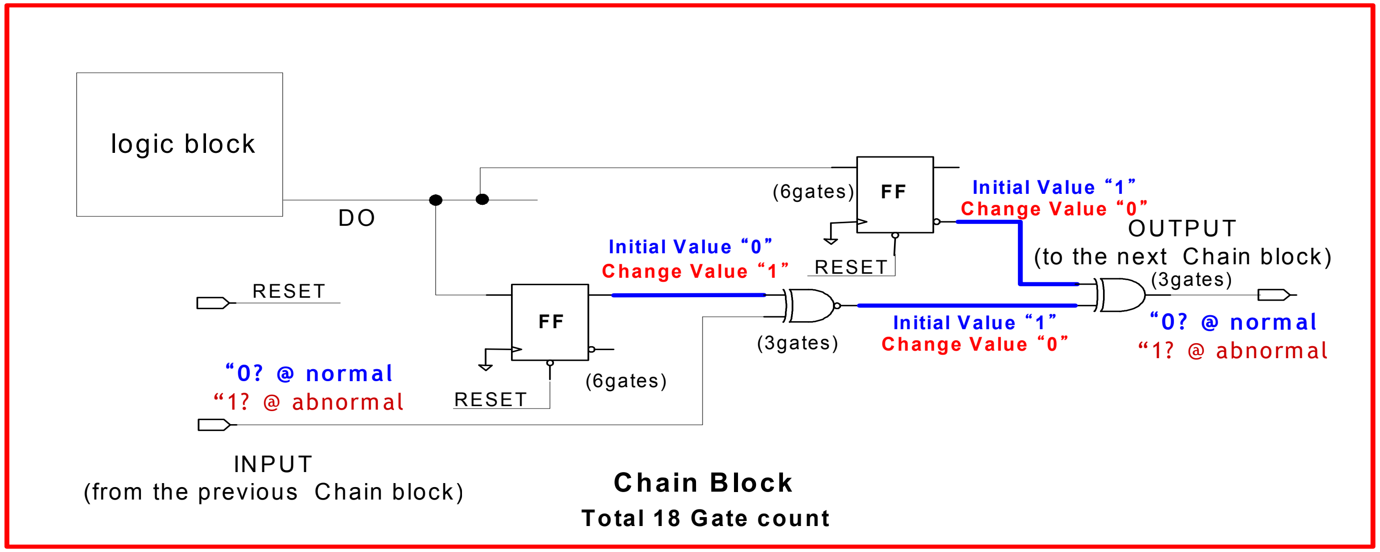
Background on secure hardware design

- **Standard Light detectors:**
  - Large photodiodes (Analogue Hard macro)
    - **big size, easy to localize by an attacker**
    - **difficult to integrate into the logic**
    - **Low security level**
- **Hardened design**
  - Dual rail logic with 1 state for fault detection
  - Redundant hardware
  - Hardened coprocessor, CPU
  - **Good security level but high cost**
    - **Dedicated to each IP = long design time**
- **Necessity to design low cost detector, easy to integrate into the logic and independent of the IP to be protected**

PICTURE REMOVED

Laser fault detectors design

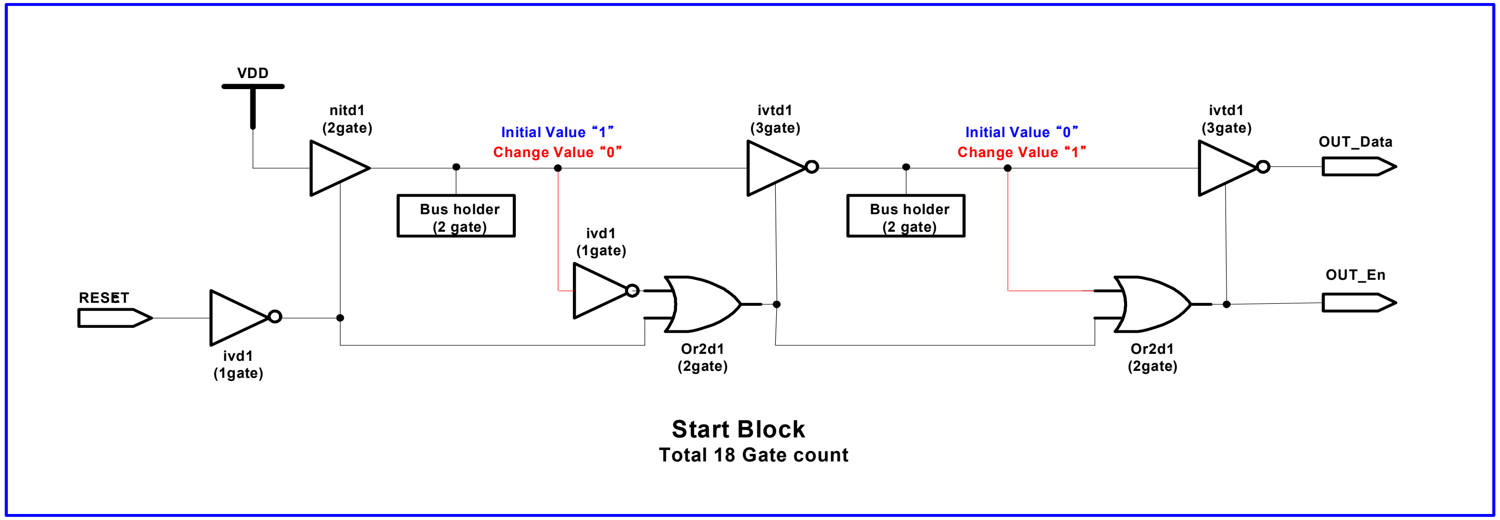
■ Virtual Cell detector



- Based on our assumption that flip-flip flop are sensitive to laser pulse
- A set of virtual cells made of flip-flop are connected one after the other
- After each reset each the cells are set to initial value "0" or "1"
- In case initial value is modified, the error is propagated and a detection signal is sent

Laser fault detectors design

- **Tri-State BUS holder detector**



- **Based on our assumption that BUS holders are sensitive to laser pulse**

- **Same principle that previous scheme, the holder are set to initial value 0 after reset, in case this value is modified, the error is propagated and a detection signal is sent**

Laser fault detectors design

- **Detectors spreading**
  - The cells of each detector are spread among the whole logic area
  - In our first trial the distance between two cells of same type was set to 150um
- **Detection mechanism: Interrupt generation**
  - When the laser pulse is detected an interrupt is generated
  - The interrupt allow user to take a security action such as card “killing mechanism” to prevent an attacker to reproduce attack on same device as soon as the laser is detected !

Laser fault detectors design

Main benefit of those detectors

Relative low cost	➢For 150um distance between two cells of same type the cost represent less than 0.3% of the total logic area protected
Easy to integrate into the logic	➢Use standard CMOS cells similar to the logic area cells ➢easy to places and route without change of the logic structure
Good spreading among the logic	➢All logic area is protected
Avoid reproducibility of the attacks	➢ Interrupt generation allow user to take security action and prevent the attacker to scan the whole device

Main drawback

- Difficult to integrate onto the memory blocks!

Laser Fault Detectors Validation

- **Targeted device was tested with same set of command that our first experiment (both front and back side)**
  - DES, RSA, CPU operation, Memory write read
- **With 150um square laser spot size the Virtual cell systematically detected the pulse**
  - One pulse is sufficient
  - No error possible on the logic
- **With smaller spot (up to 40um square) partial detection with both Virtual cell and Holder cells was possible**
  - The detector operates when the pulse matches with cell location (no or low spread of the pulse energy outside the spot)
    - Distance between cells and cells location should be chosen carefully
  - Virtual cell detection is faster than tri-state holder

Conclusion

- **Two laser detector types were presented**
  - Virtual cell detector
  - Tri-state BUS holder detectors
- **Both detectors are operating fine and can detect both front side and back side laser pulse**
- **Those detectors have low cost and integrate easily into the logic without high cost hardware change**
- **Those detectors are independent of the logic part it protects**
- **The distance and location of detector should be chosen carefully to fit with the most sensitive area of the logic**
- **Specific detection mechanism should be implemented on the Memory areas**