EO-Shield: A Multi-function Protection Scheme against Side Channel and Focused Ion Beam Attacks

Ya Gao, Qizhi Zhang, Haocheng Ma, Jiaji He, Yiqiang Zhao

School of Microelectronics, Tianjin University

Bio

- Ya Gao, School of Microelectronics, Tianjin University
- PhD student in Microelectronics and Solid State Electronics
- Research interest: hardware security and machine learning

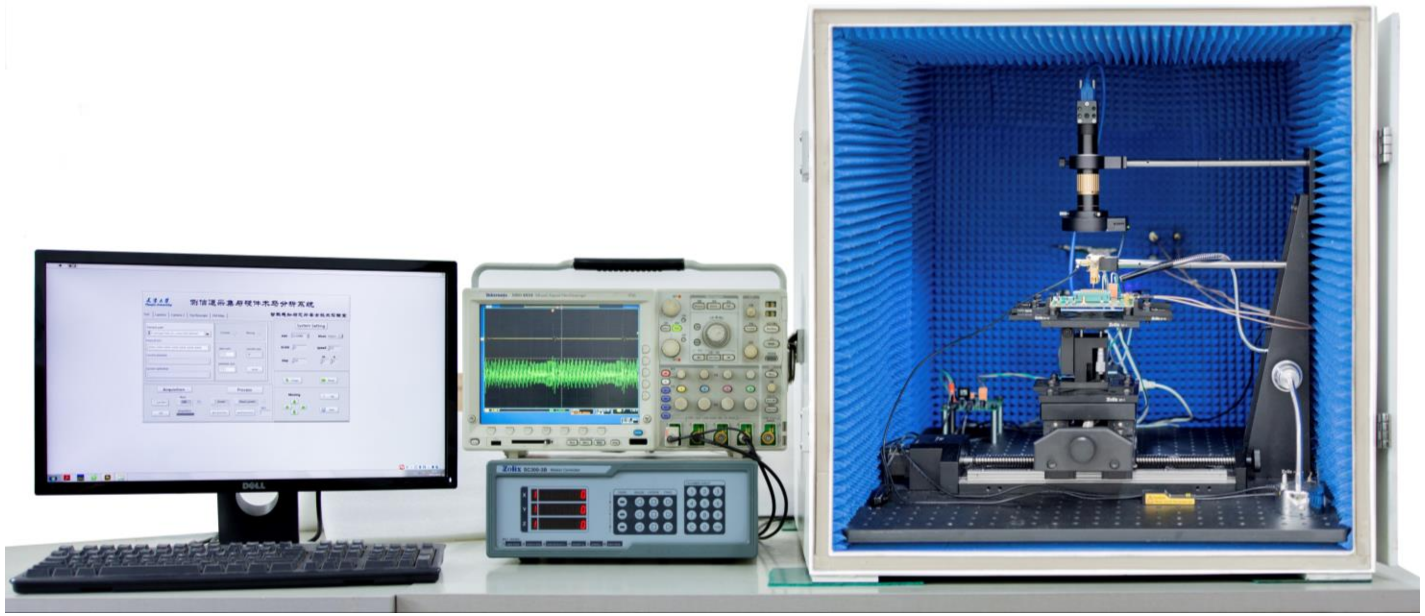
Outline

- Motivation
- EO-shield Protection System Design
- The Effect of EO-shield
- Conclusion

Motivation

Side channel analysis (SCA) attack

- SCA attacks try to extract sensitive information from the chip by collecting and analyzing the physical parameters (EM/power/timing) of the chip
- EM SCA requires no direct connections to the chips and can obtain local EM information with high signal-to-noise-ratio (SNR)

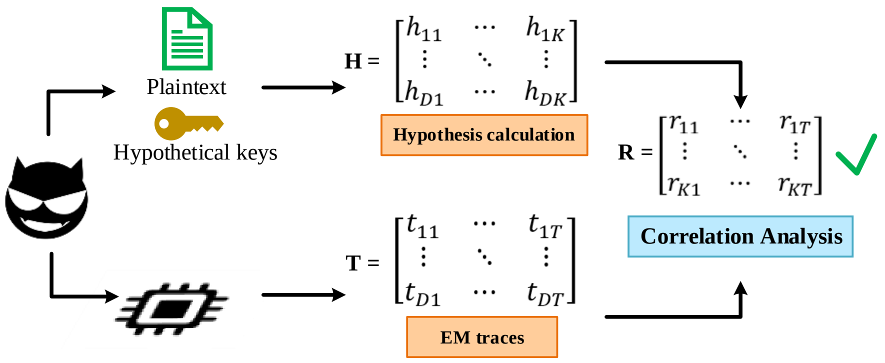


Motivation

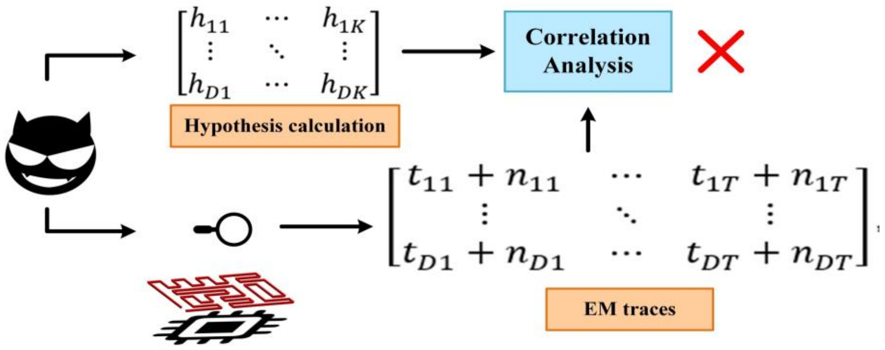
Correlation Electromagnetic Attack (CEMA)

- CEMA is a common side-channel attack method that uses Pearson's correlation as a statistical method to recover sensitive information
  - Select the middle value
  - Collect the EM traces
  - Calculate the hypothetical EM information leakage matrix
  - Correlation analysis

$$r_{i,j} = \frac{\sum_{d=1}^{D}(h_{d,i} - \bar{h}_i) \cdot (t_{d,j} - \bar{t}_j)}{\sqrt{\sum_{d=1}^{D}(h_{d,i} - \bar{h}_i)^2 \cdot (t_{d,j} - \bar{t}_j)^2}}$$



correlation electromagnetic attack

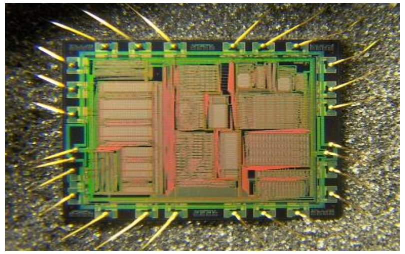


correlation electromagnetic attack with protection scheme

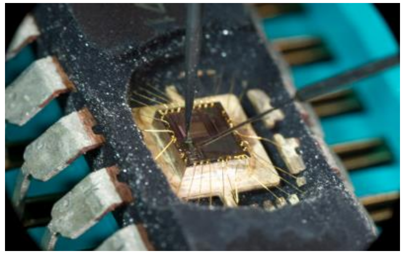
Motivation

Focused ion beam (FIB) attack

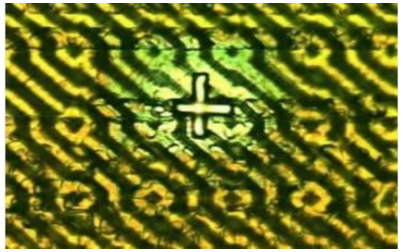
- Invasive attacks are the most effective and thorough means of physical attacks available
- Focused ion beam (FIB) attack is the most investigated invasive attack
- Active shield based solutions are so far the most common countermeasures



reverse engineering



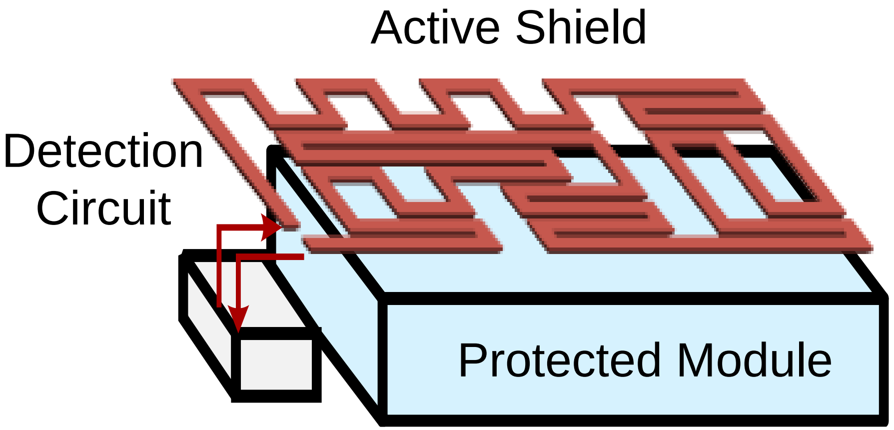
locate the target wire



create probe pad

extract target information

Typical FIB attack process



Active shield-based protection solutions

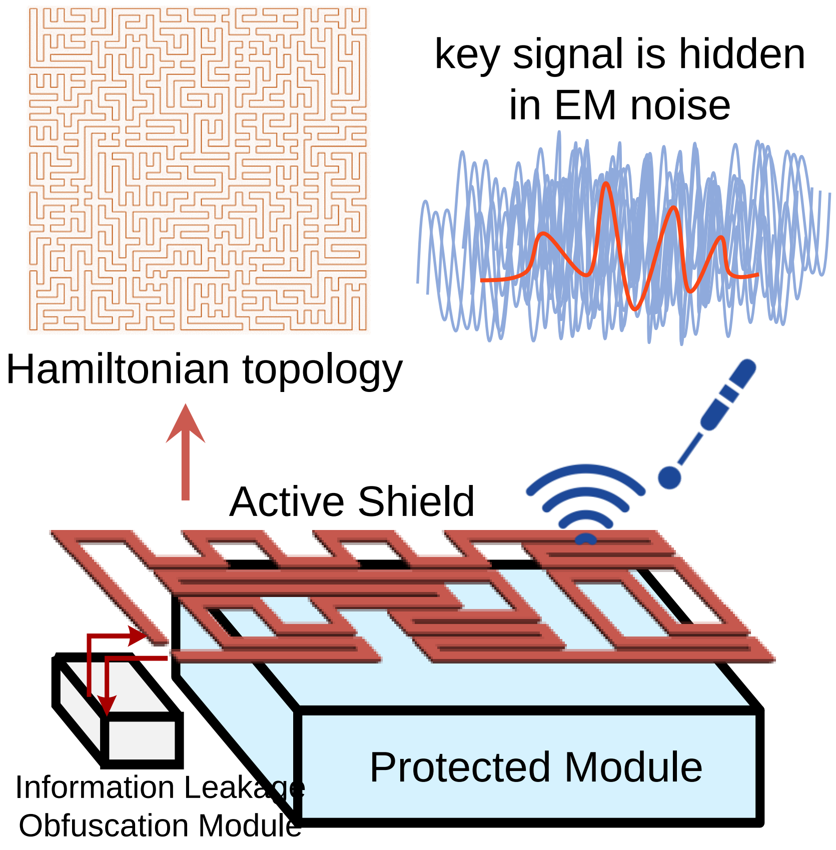
https://www.chinapcbcopy.com/ic-unlock-service/
https://www.ce.cit.tum.de/en/eisec/research/invasive-attacks/
Design principles for tamper-resistant smartcard processors
How microprobing can attack encrypted memory

This Work

- A multi-function protection scheme, namely **EO-shield**, to against both invasive and non-invasive attacks
  - EM side channel attack:

    An information leakage obfuscation module to implement EM noise injection (NI)
  - FIB attack:

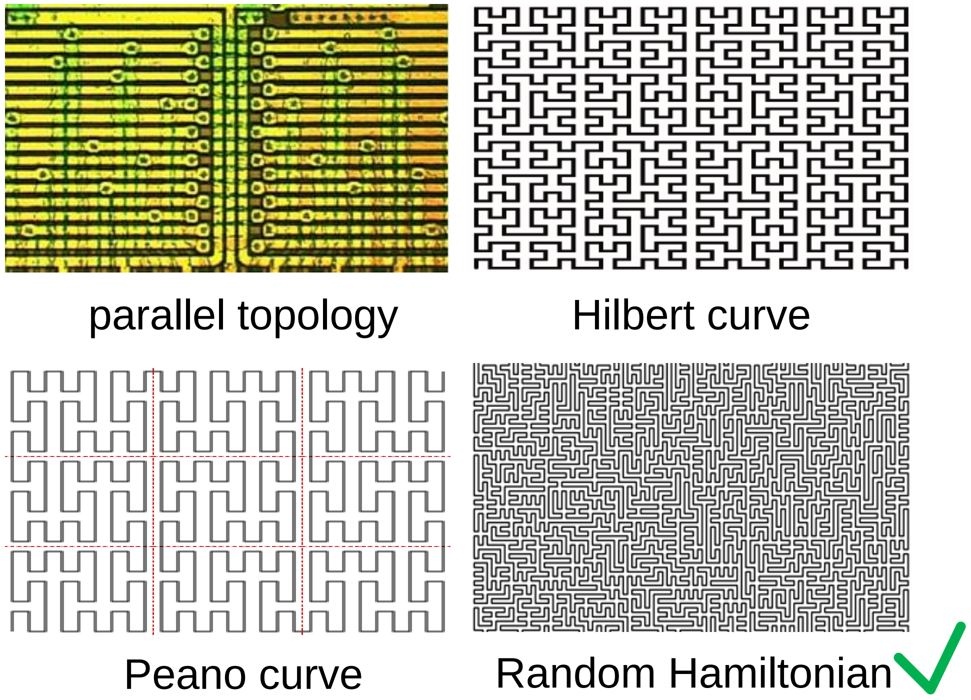
    An active shield with random Hamiltonian topology to protect key modules of the circuit
- The effectiveness of **EO-shield** is successfully validated through simulation



EO-shield Protection System Design

Random Active Shield Design and Implementation

- Active shield features:
  - utilize the top metal layer of the chip
  - require a high level of complexity
- Among typical topologies, the random Hamiltonian topology has the most random structure and is the most difficult to hack
- Based on our shield generation software, we produce active shields with random Hamiltonian topology based on the Artificial Fish-Swarm Random Hamiltonian algorithm (AFSRHA)



Typical topologies of active shields

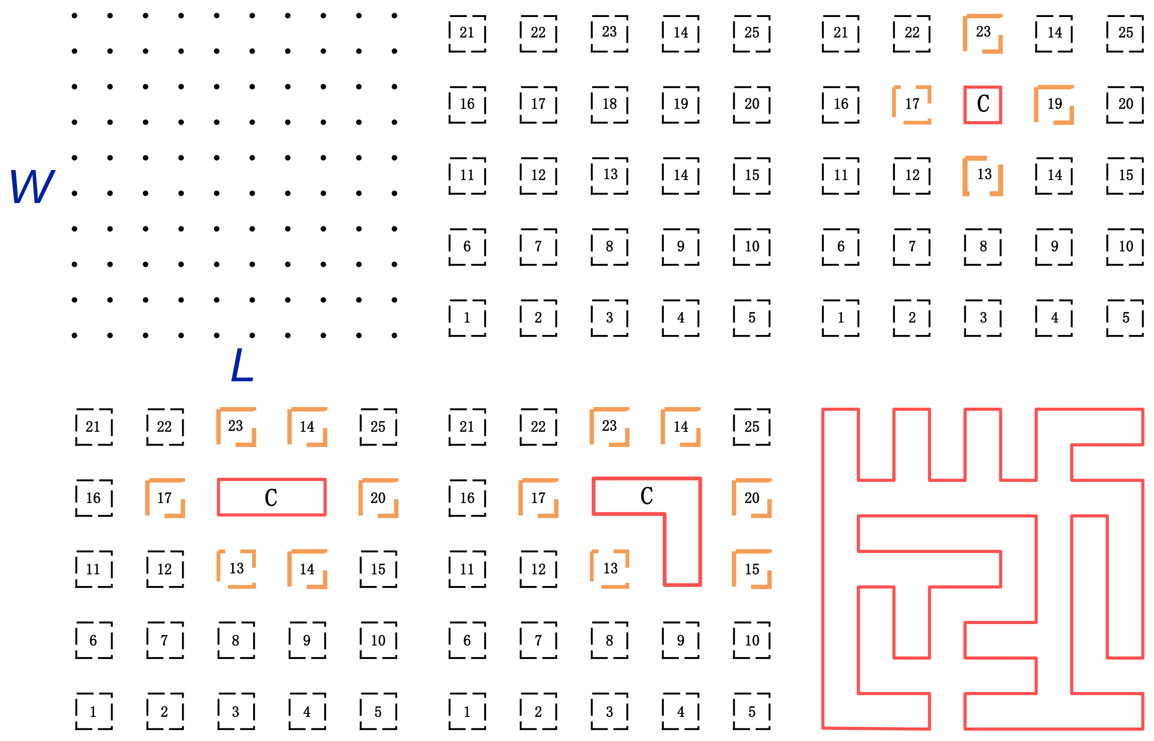
EO-shield Protection System Design

Random Active Shield Design and Implementation

- *L* and *W* are normalized into grid points by *wire_width* and *wire_space*

$$L, W \geq 8 \times (\text{wire\_width}+\text{wire\_space})$$

- A square formed by four adjacent grid points is defined as a *fish*
- A fish is randomly selected and merged with an adjacent fish to generate a *loop C*
- Iterate this process until all the fish are contained in loop C



The execution process of AFSRHA algorithm

EO-shield Protection System Design

Random Active Shield Design and Implementation

- For a narrow, elongated shield area:

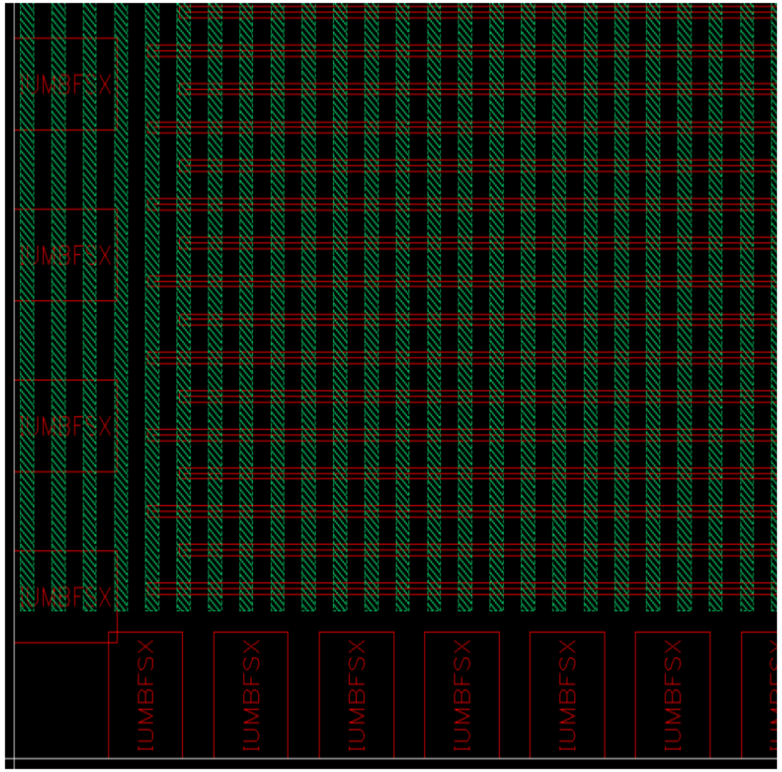
  The shield area is the gap between the dense power strips on the top layer

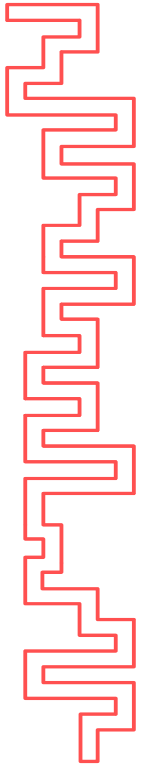
- *L* and *W* do not satisfy the equation:

$$L, W \geq 8 \times (\text{wire\_width}+\text{wire\_space})$$

- Random parallel shield topology:

  Randomly select the offset in the x-direction and y-direction during the generation process





Random Parallel Shield

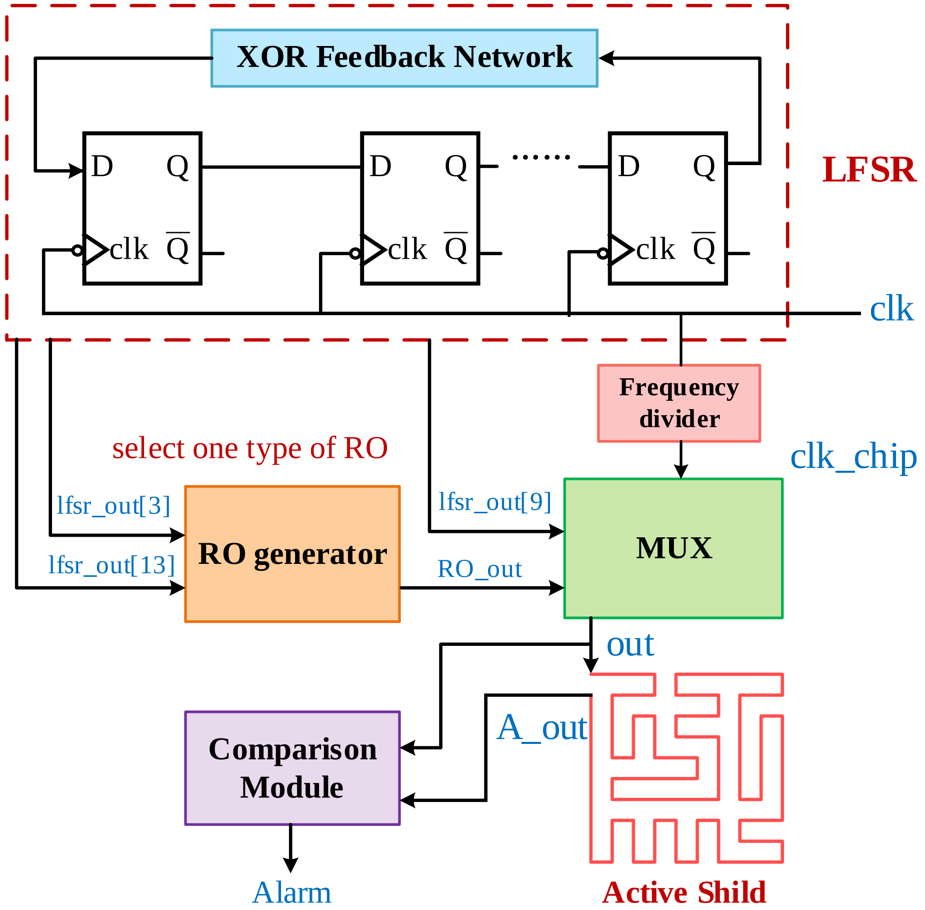
EO-shield Protection System Design

Information Leakage Obfuscation Module Design and Noise Signal Generation

- The linear feedback shift register (LFSR) :
  - Based on a Primitive Polynomial

$$X^{15} + x + 1$$

  - Generate a random signal (*lfsr_out[9]*) sent to the active shield
  - Generate two random signals (*lfsr_out[3]* and (*lfsr_out[13]*) to select one type of ROs

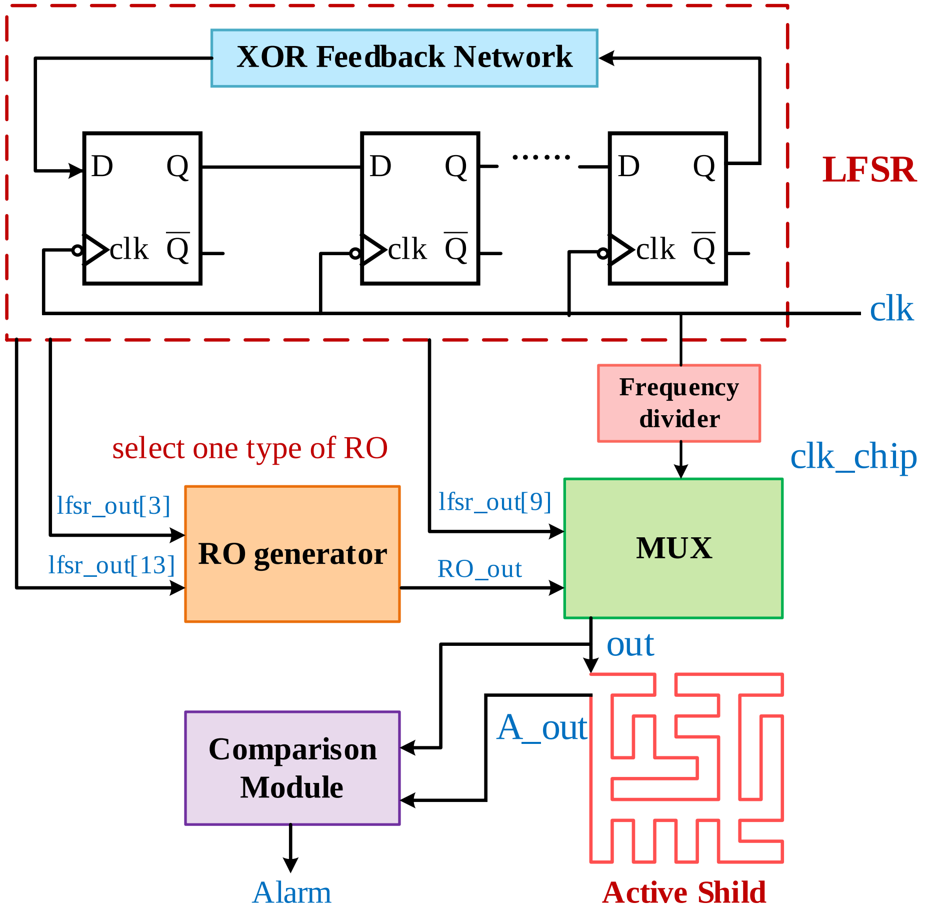


Information obfuscation circuit

EO-shield Protection System Design

Information Leakage Obfuscation Module Design and Noise Signal Generation

- RO generator circuit:
  - Include four RO oscillation circuits with 3, 5, 7 and 9 inverters respectively
  - Generate oscillation signals with four types of time delays
- MUX module:
  - According to the clock edge of the signal *clk_chip* to select whether to output *lfsr_out[9]* or *RO_out*
- Signal comparison module:
  - Compare *lfsr_out[9]* with *A_out* to achieve real-time monitoring of invasive attacks

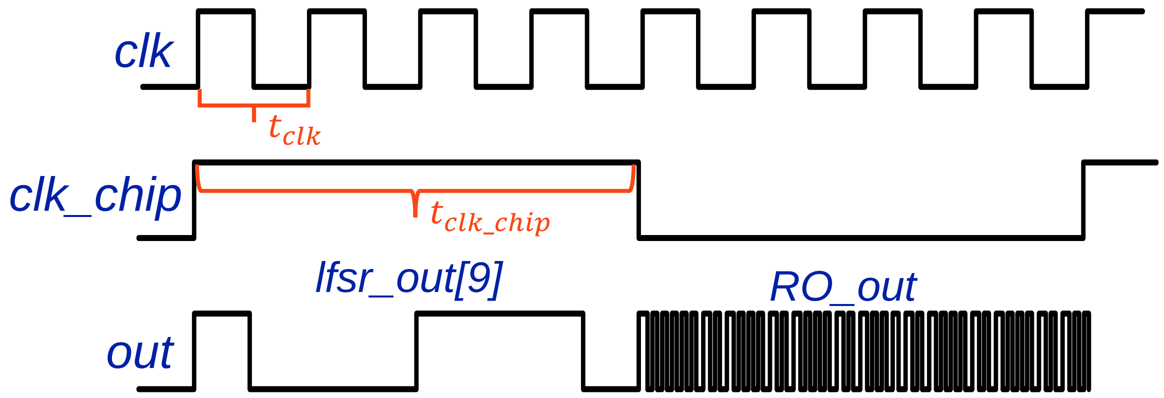


Information obfuscation circuit

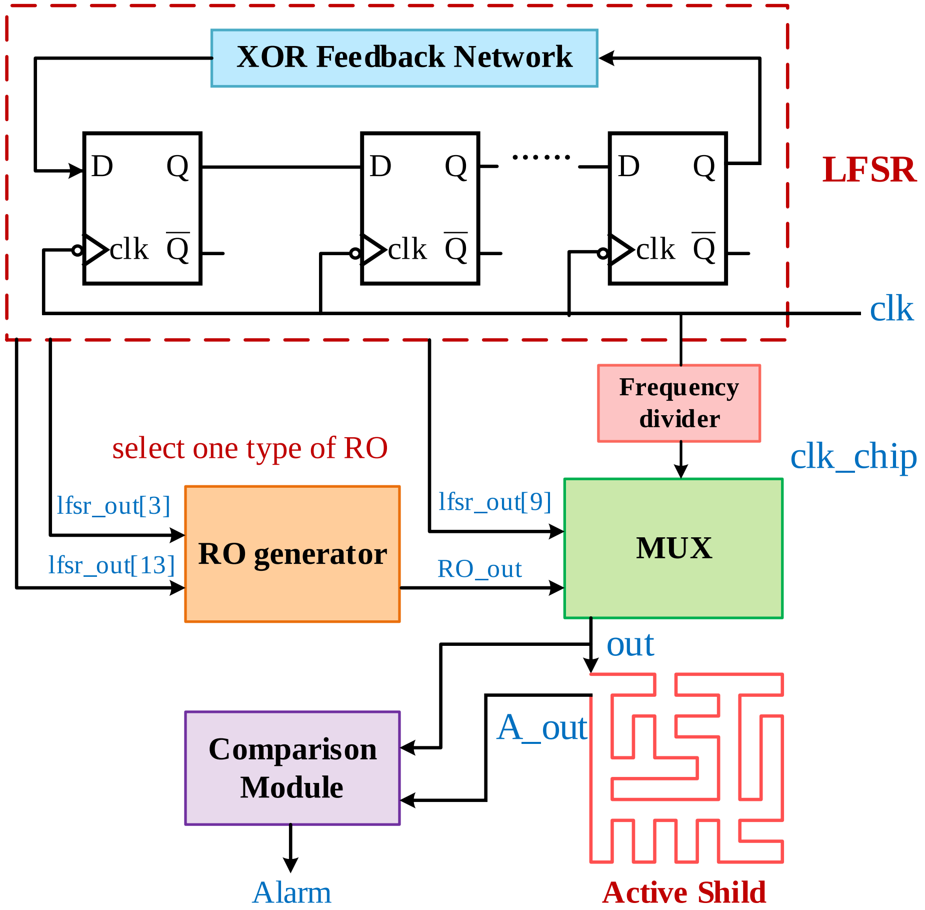
EO-shield Protection System Design

Information Leakage Obfuscation Module Design and Noise Signal Generation

- Frequency divider:
  - Divide the high frequency *clk* to *clk_chip*



  - Suppose t_{clk_chip} contains n t_{clk} , the generated pseudo-random number signal remains constant during the t_{clk_chip} is $1/2^n$

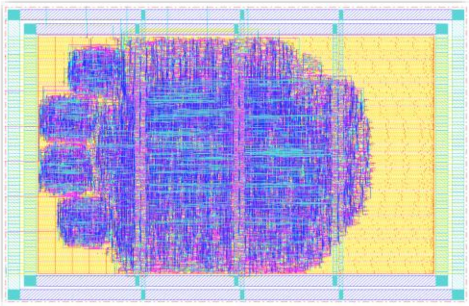


Information obfuscation circuit

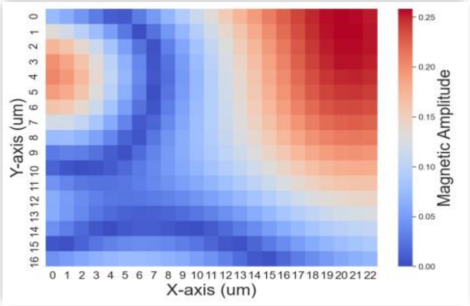
The Effect of EO-shield

EM Simulation

- AES_NIST:
  - AES is designed in the light of NIST standard, which includes128-bit plaintext and key
  - Use *180 nm* CMOS technology
  - Die size of the total chip occupies *1140μm×840μm*
  - The clock frequency is *25 MHz*
  - *1000* random plaintext inputs
- EMSim:
  - Our Electromagnetic emanation simulation tool at layout-level

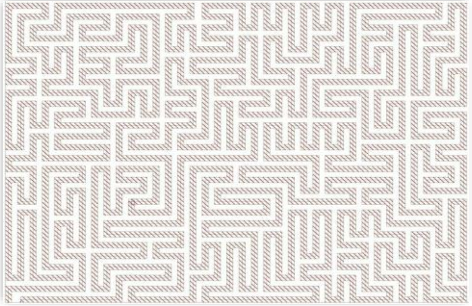


(a) Chip layout

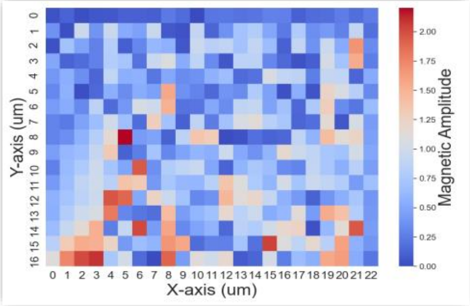


(b) EM map of the chip surface

Unprotected AES



(a) The active shield



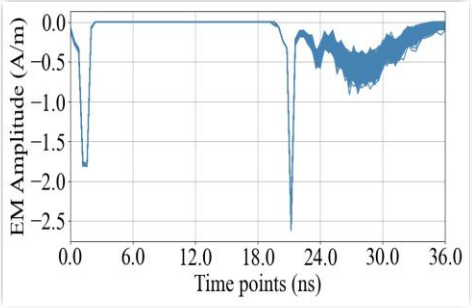
(b) EM map of the chip surface

Protected AES

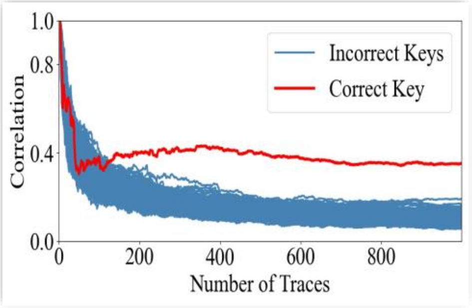
The Effect of EO-shield

CEMA attack

- Target the SubByte operation in the first S-Box

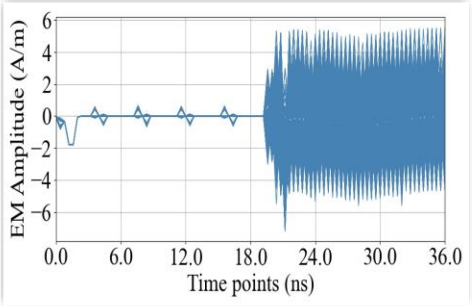


EM traces of the S-Box

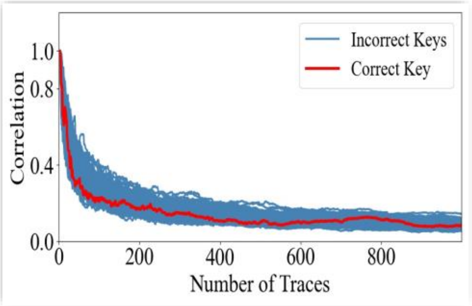


MtD results

Unprotected AES

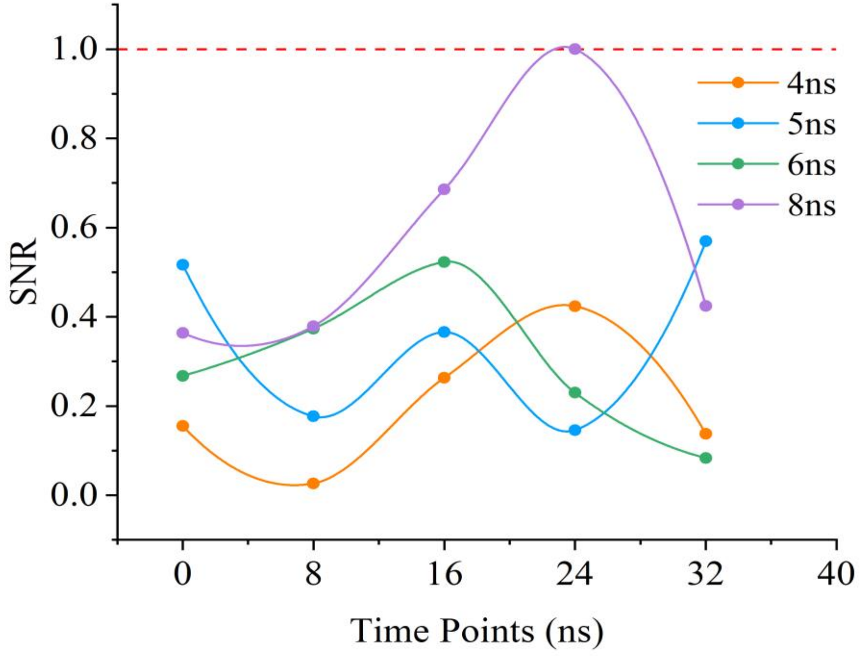


EM traces of the S-Box



MtD results

Protected AES



Conclusion

- Overhead Evaluation:

Circuits / Metrics	Unprotected AES (25Mhz)	Protected AES (250Mhz/200Mhz/166Mhz)	Increase Percentage
Area (μm^2)	288195	293227	1.75%
Power (w)	$1.51e-2$	$1.62e-2/1.618e-2/1.6e-2$	9.74%/7.15%/5.96%

- Signal Perturbation:

The time perturbation of the protected circuit due to effects such as parasitic resistance and parasitic capacitance caused by the information leakage obfuscation module can be neglected

- Process Antenna Effect (PAE):

The Process Antenna Effect (PAE) caused by long wire mesh can be eliminated by using jumpers, adding normally closed transmission gates (NC) or diode cells

Conclusion

- A multi-function protection scheme called ***EO-shield*** is proposed for the first time to combat both invasive and non-invasive attacks

- The core idea is to combine an active shield with an ***information leakage obfuscation module*** to mitigate non-invasive attacks by sending current stimuli to the ***active shield*** in a noise injection method

- Through simulation experiments, the correlation between EM emanations and processing data is also reduced to achieve ***a SNR lower than 1***. The security of the proposed EO-shield scheme is finally proved

THANK YOU!

gaoyaya@tju.edu.cn