浙江大学 信息与电子工程学院

College of Information Science & Electronic Engineering, Zhejiang University

Improved low-entropy masking scheme for LED with mitigation against correlation-enhanced collision attacks

Fan Zhang, Liang Geng, Jizhong Shen,
Shivam Bhasin, Xinjie Zhao, Shize Guo

Zhejiang University

October 20, 2017
Beijing, China

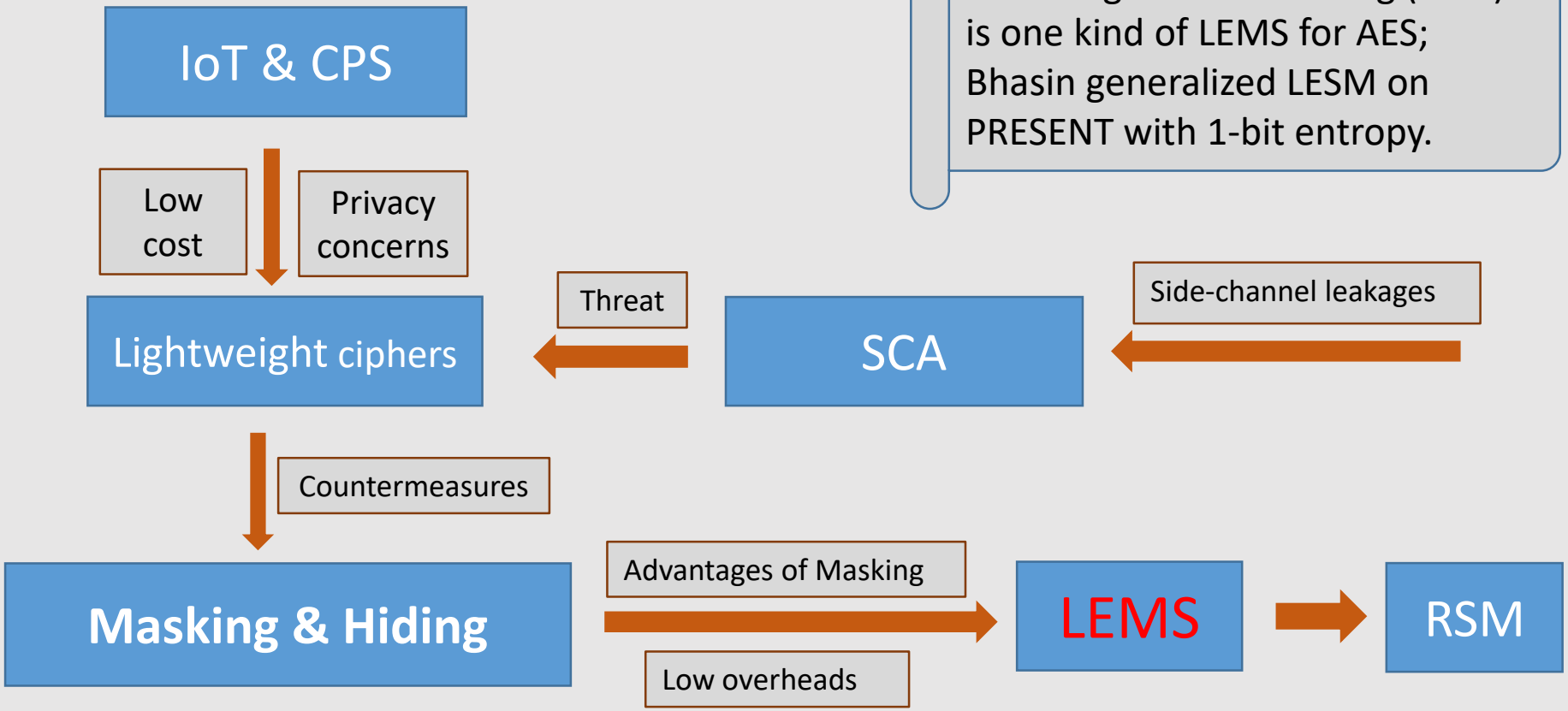
AsianHOST-2017

OUTLINE

1. Introduction

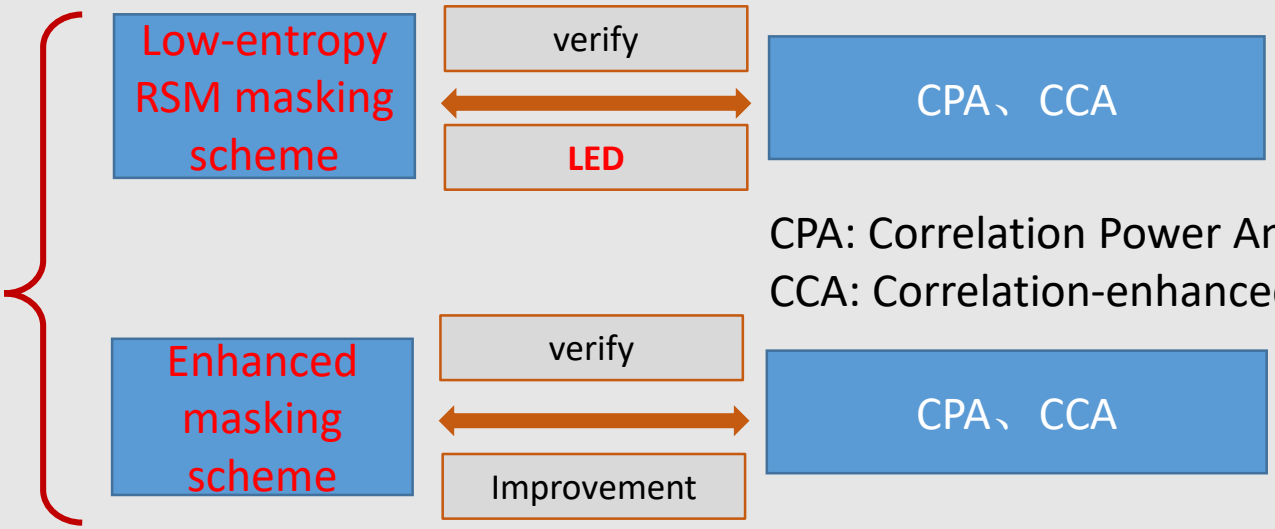
1.1 Low-Entropy Masking Scheme (LEMS)

"Rotating Sboxes Masking (RSM)" is one kind of LEMS for AES; Bhasin generalized LESM on PRESENT with 1-bit entropy.



浙江大学 信息与电子工程学院
College of Information Science & Electronic Engineering , Zhejiang University

1.2 Proposal



CPA: Correlation Power Analysis
CCA: Correlation-enhanced Collision Analysis

Why LED?

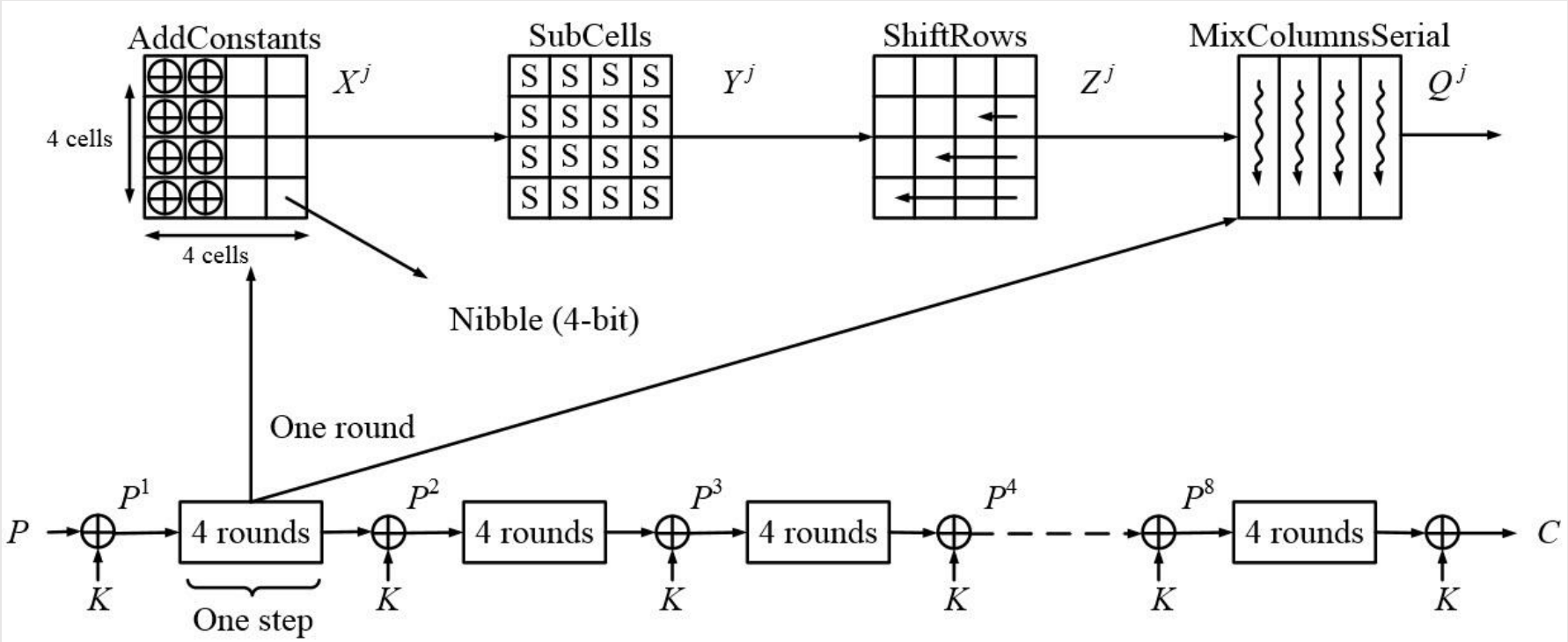
LED: newer than PRESENT and designed with a more compact structure.

OUTLINE

浙江大学 信息与电子工程学院
College of Information Science & Electronic Engineering , Zhejiang University

2.1 The LED Block Cipher

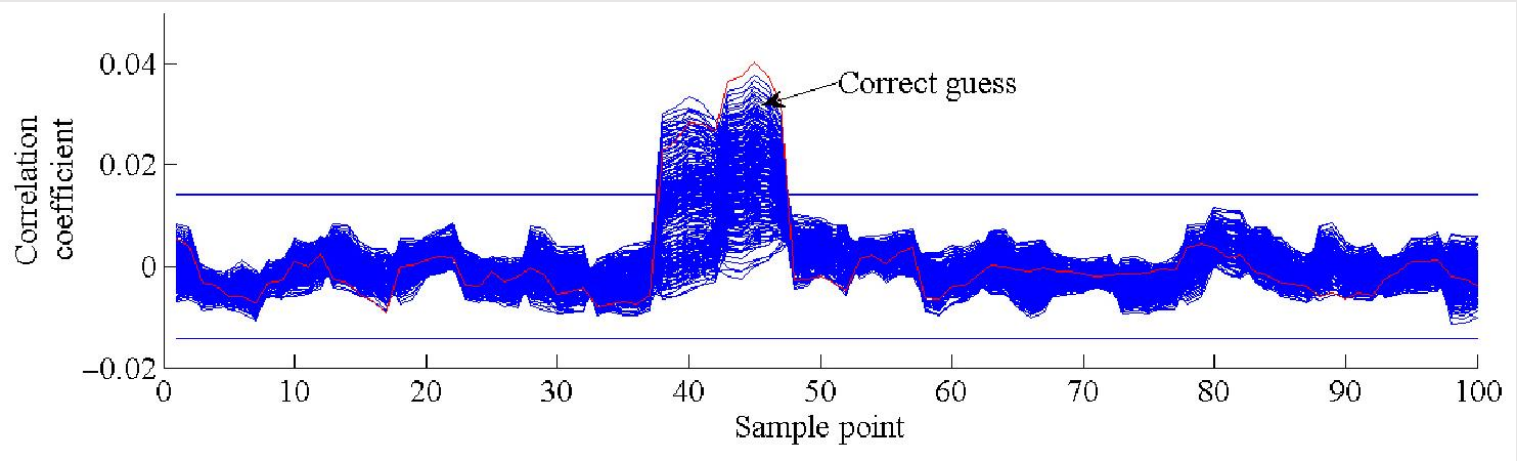
- The encryption procedure：
  - ✓ Addkey (*state, k)and* Step(*state*);



2.2 CPA、TVLA

- CPA (Correlation Power Analysis)：
  - ✓ Hamming weight model;
  - ✓ Pearson Correlation Coefficient;

$$\rho_{TH} = \frac{cov(TH)}{\sigma_T \sigma_H} = \frac{N\sum T_i H_{i,j} - \sum T_i \sum H_{i,j}}{\sqrt{N\sum T_i^2 - (\sum T_i)^2}\sqrt{N\sum H_{i,j}^2 - (\sum H_{i,j})^2}}$$



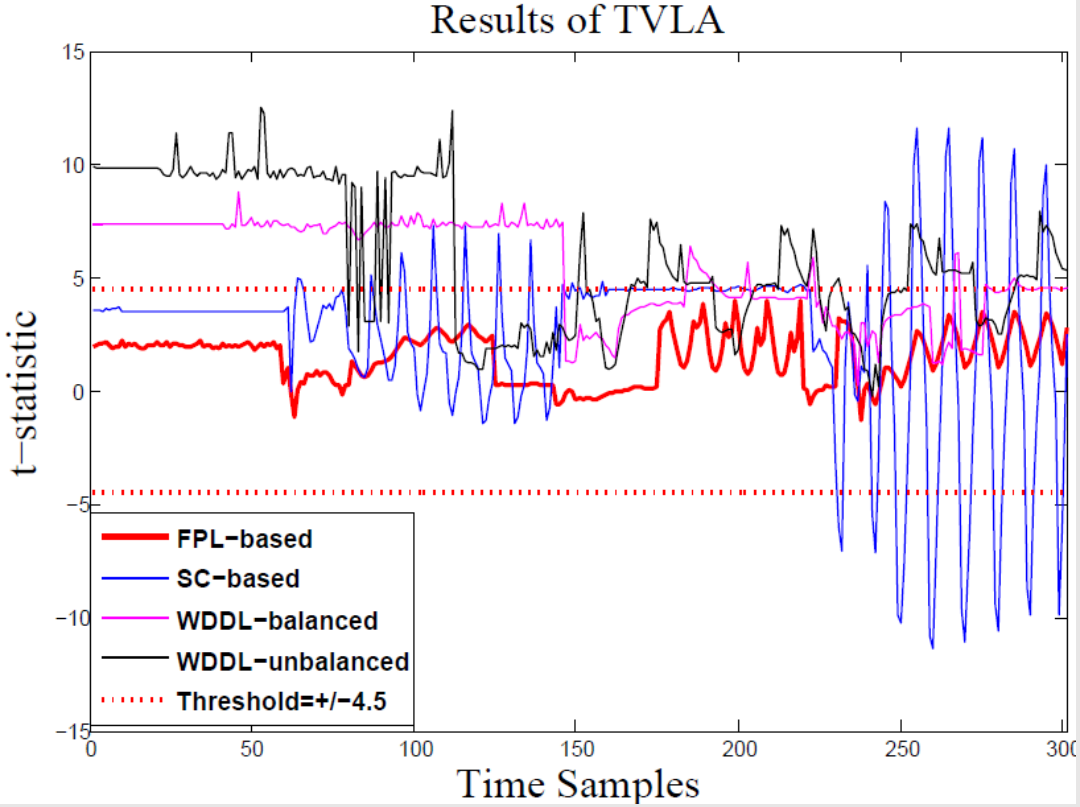
浙江大学 信息与电子工程学院
College of Information Science & Electronic Engineering , Zhejiang University

2.2 CPA、TVLA

- TVLA (Test Vector Leakage Assessment)：
  - ✓ Assess the potential SCAs;
  - ✓ Two groups:

    Fixed vs Random (FVR);

$$T = \frac{X_A - X_B}{\sqrt{S_A^2/N_A + S_B^2/N_B}}$$



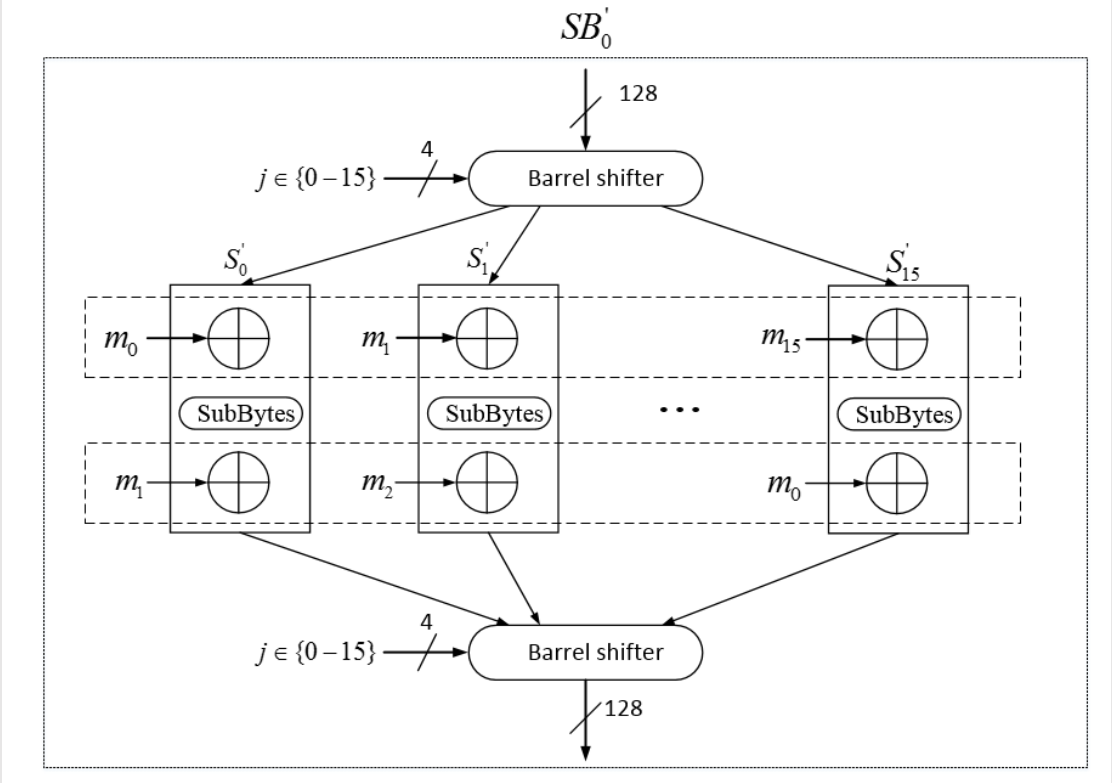
浙江大学 信息与电子工程学院
College of Information Science & Electronic Engineering , Zhejiang University

2.3 RSM

- RSM Countermeasures

  (M. Nassar, 2012):

  - ✓ Low cost and robust against first-order and zero-offset second-order DPA;
  - ✓ Keep same level performances and complexity;
  - ✓ Formula:



Masked-Subbytes: $SB'_j = SB(X' \oplus M_j) \oplus M_{(j+1) \bmod 16}$, $j \in \{0\text{-}15\}$

Mask-Compensation: $CSM_j = (M_j) \oplus SR(MC(M_j))$, $j \in \{0\text{-}15\}$

OUTLINE

浙江大学 信息与电子工程学院
College of Information Science & Electronic Engineering , Zhejiang University

3.1 Implementation of one-bit RSM for LED

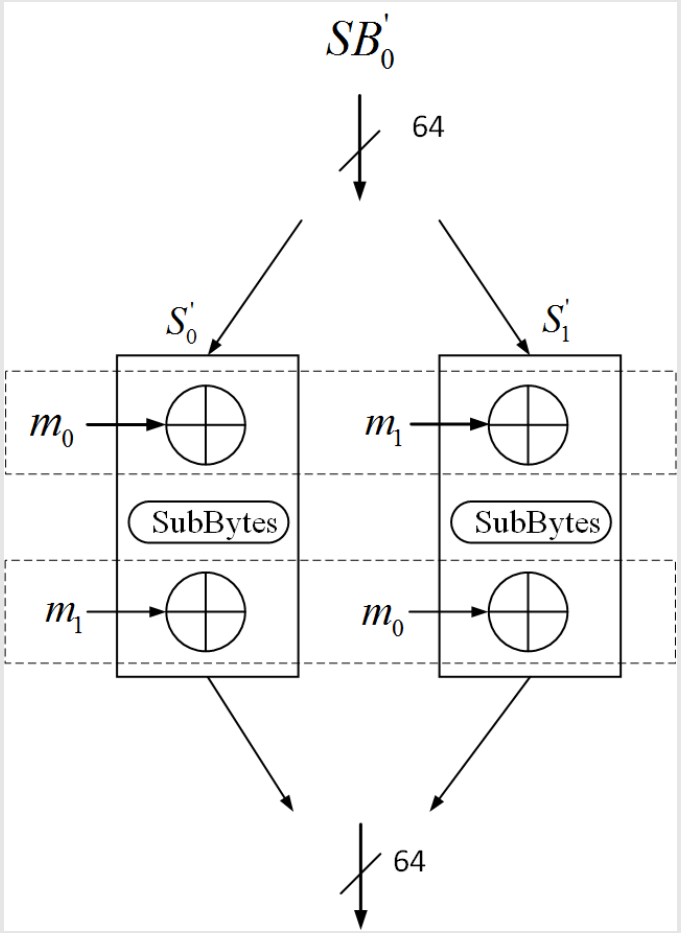
- Implement modified Sboxes;

$$S'_{m_i}(x') = S(x' \oplus m_i) \oplus m_{i+1 \bmod 2}$$

- Choose corresponding Sbox by random offset j;

- Masking the SR、MC and AK functions;

$$CSM_i = (M_i) \oplus SR(MC(M_i)), \forall i \in \{0,1\}$$



3. Implementation and Evaluation of M-LED

浙江大学 信息与电子工程学院
College of Information Science & Electronic Engineering , Zhejiang University

3.1 Implementation of one-bit RSM for LED

Algorithm 1: M-LED

Input: $m_0 : Mask \in [3, 5, 6, 9, a, c]$; n_trace : number of encryption; P : Array of plaintext
Output: C : Array of ciphertext

Define: $m_1 \in \mathbb{F}_2^4$, and $m_1 = \neg m_0$; $offset = j$;
$M_0 = \{m_0, m_1, \ldots, m_1\}$;
$M_1 = \{m_1, m_0, \ldots, m_0\}$

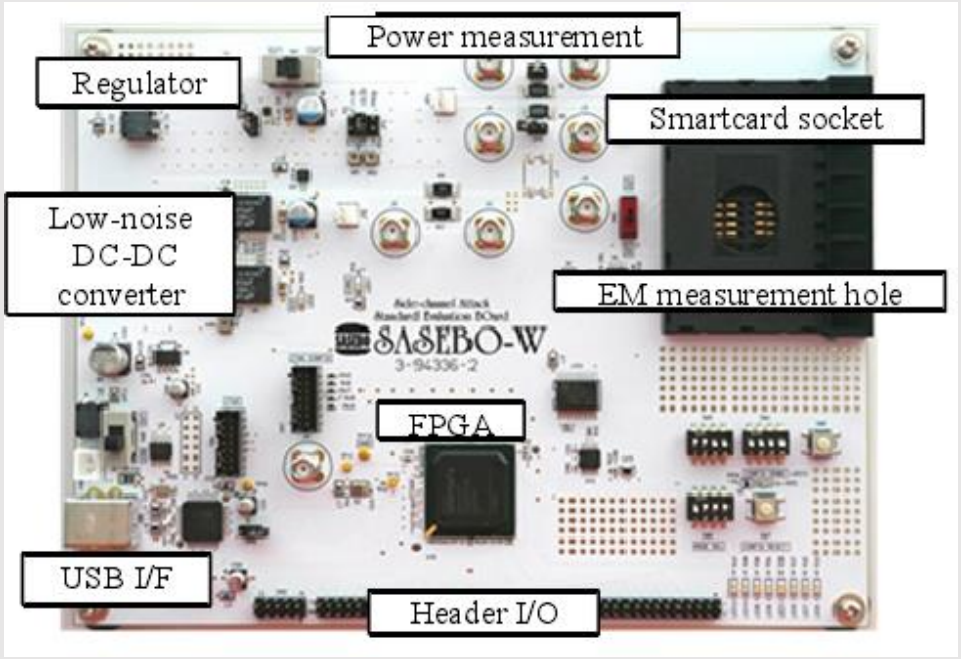
Compute: Mask SBoxes S'_{m0} and S'_{m1};
// $S'_{mi}(x') = S(x' \oplus m_i) \oplus m_{i+1 \bmod 2}$
Mask Compensation $CSM_i, \forall i \in \{0 - 1\}$

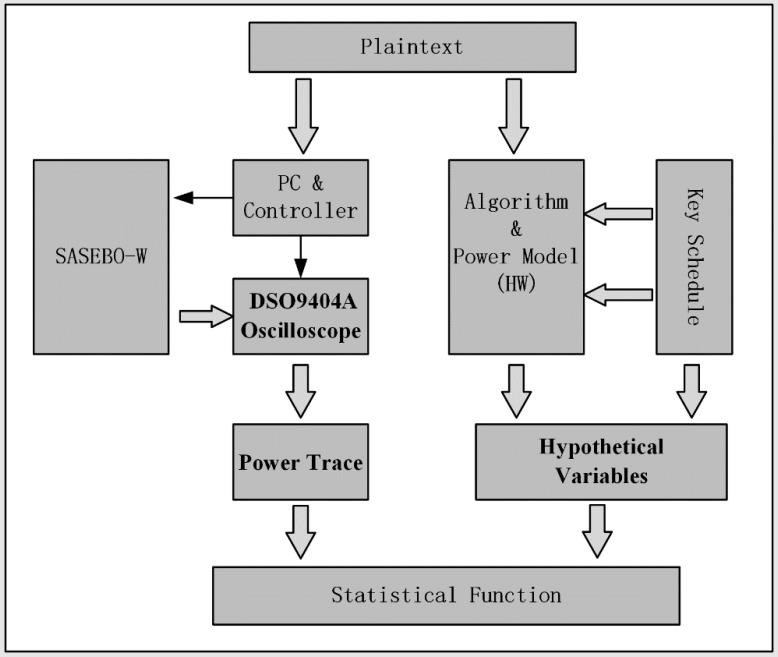
for $i = 1$ **to** n_trace **do**
  $j = rand()\%2$;
  $state \leftarrow P[i]$;$key \leftarrow K[i]$;
  LEDRound_mask $(j, state, keys)$
  if $j = 1$ **then**
    $offset_{index} = 0xAAAA, state \leftarrow M_1$
  else
    $offset_{index} = 0x5555, state \leftarrow M_0$
  AddKeys$(state, keys)$;
  for $round = 1$ **to** 32 **do**
    AddConstants$(state)$;
    SubCell$(state)$;
    ShiftRow$(state)$;
    MixColumn$(state)$;
    Maskcompensation$(j, state)$;
    $j = (j + 1)\%2$;
    if $j = 1$ **then**
      $offset_{index} = 0xAAAA; state \leftarrow M_1$
    else
      $offset_{index} = 0x5555, state \leftarrow M_0$
    AddKeys$(state, keys)$;
  return $state$

浙江大学 信息与电子工程学院
College of Information Science & Electronic Engineering, Zhejiang University

3.2 Experiment Platform

- Target Platform Notations:
  - ✓ SASEBO-W and SCA flow;



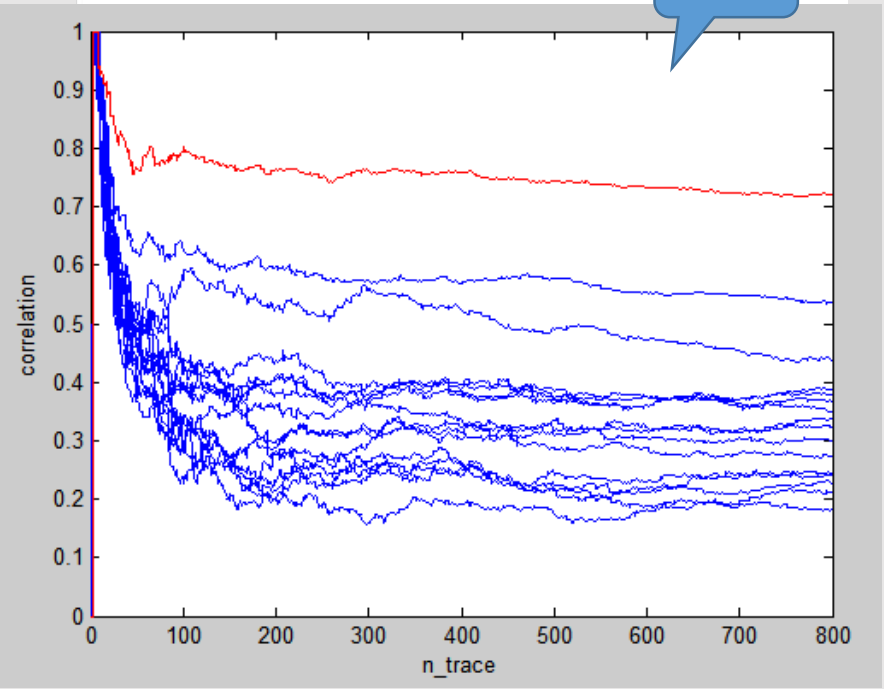


浙江大学 信息与电子工程学院
College of Information Science & Electronic Engineering , Zhejiang University

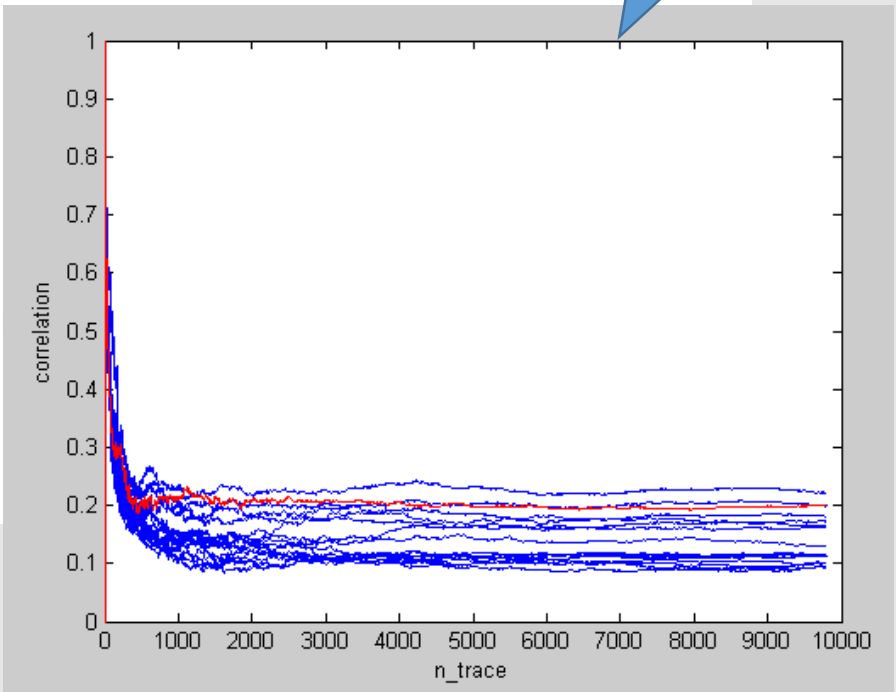
3.3 Evaluation against CPA

- Evaluation Results:
  - ✓ LED and M-LED;
  - ✓ For one nibble;

LED



M-LED



浙江大学 信息与电子工程学院
College of Information Science & Electronic Engineering, Zhejiang University

3.4 Evaluation against CCA

- Correlation-enhanced Collision Analysis (CCA):

$$m_i \oplus m_{i+1} = 0xF$$

$$k_{i-guess} = k_i \oplus k_{i+1}, i \in \{0-15\}$$

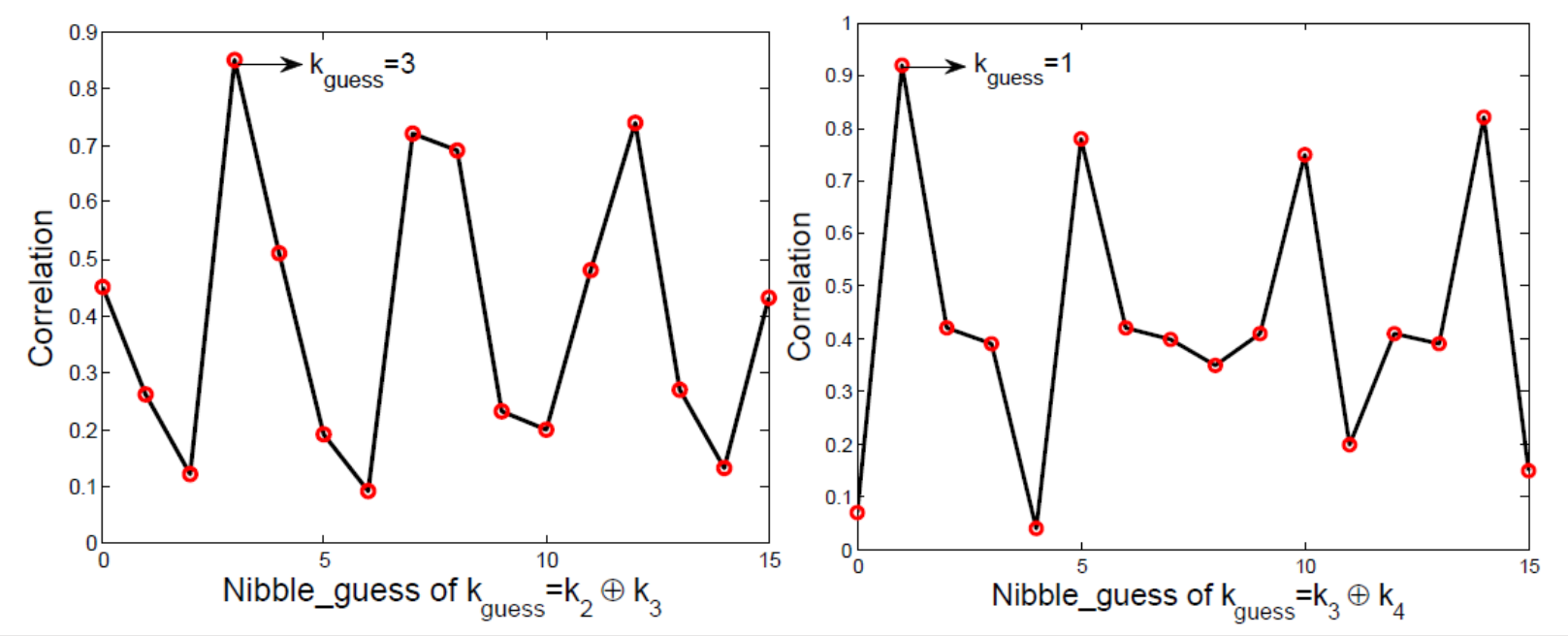
$$S'(x'_i \oplus k_i) = S'(x'_{i+1} \oplus k_{i+1}) \oplus 0xF, \forall i \in \{0-15\}$$

- CCA Attack Procedure:
  - ✓ Split power traces according to x_i, get $\overline{\sum t_{i,n}}$;
  - ✓ Split power traces according to $(x_{i+1} \oplus k_{i-guess} \oplus 0xF)$, get $\overline{\sum t_{i,m}}$;
  - ✓ Calculate the correlation between above two measurements;

浙江大学 信息与电子工程学院
College of Information Science & Electronic Engineering , Zhejiang University

3.5 Evaluation of M-LED against CCA

- Evaluation Results:
  - ✓ Need up to $2.5*10^4$ traces to reveal every nibble XOR,;



OUTLINE

浙江大学 信息与电子工程学院
College of Information Science & Electronic Engineering, Zhejiang University

4.1 Our Improvement: iM-LED

- Boost the security with reasonable overheads:
  - ✓ Randomize masks;
  - ✓ Disrupt the SC order;

Algorithm 2: Randomize masks

Input: $m_0 : Mask \in [3, 5, 6, 9, a, c]$;
$flag\_1$; // random mask index

1 **Define:** $m_1 \in \mathbb{F}_5^4$, and $m_1 = \neg m_0$;

Algorithm 3: Disrupt the SC order

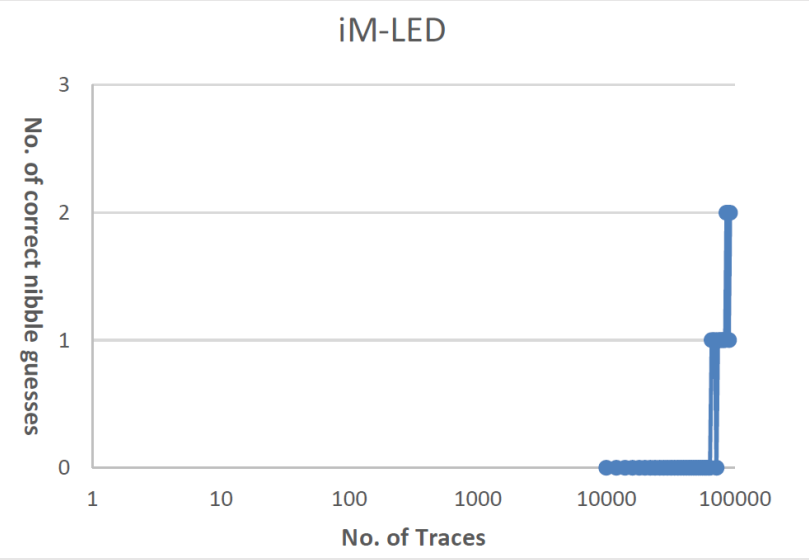
1 **Input:** count=0;
$flag\_2$; // random SBox index

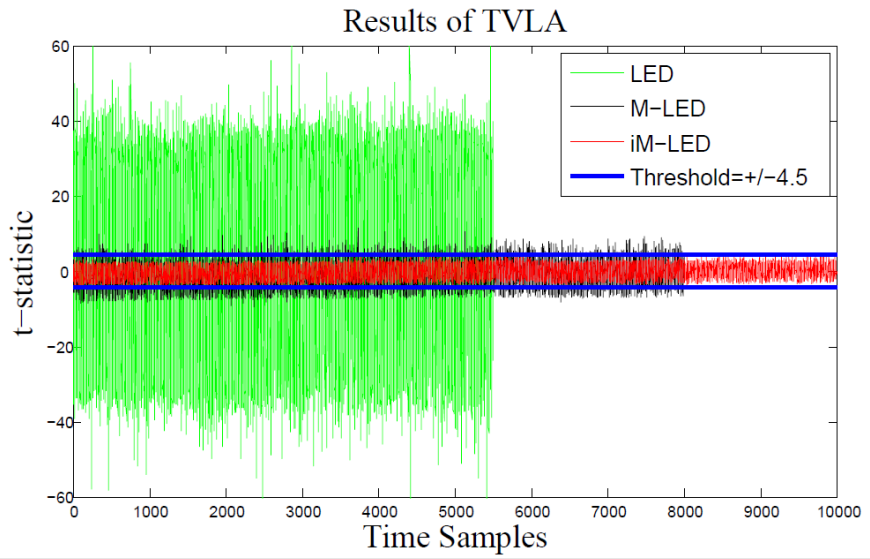
2 **for** $i = 1$ **to** n_trace **do**
// Shuffling
3 **for** $round = 1$ **to** 32 **do**
4 $flag\_2 = rand()\%16$;
5 **for** $count = 1$ **to** 16 **do**
6 SubCell($flag\_2$) ; // Firstly operate the flag_2 SBox;
7 ($flag\_2$++)%16;

浙江大学 信息与电子工程学院
College of Information Science & Electronic Engineering, Zhejiang University

4.2 Evaluation of iM-LED

- To evaluate the improved security:
  - ✓ CPA: MTD(Min. traces to disclose part of key)=10^5; [previously 10^4]
  - ✓ CCA: with $6*10^4$ traces, unable to reveal the key; [previously $2.5*10^4$ for all]
  - ✓ TVLA: The iM-LED(red curve) presents the least leakages.





浙江大学 信息与电子工程学院
College of Information Science & Electronic Engineering, Zhejiang University

4.3 Overhead comparison of various LED implementations

- Contents:
  - ✓ text: size of code segment which stores the instructions;
  - ✓ data: size of initialized variables in RAM and FLASH;
  - ✓ bss: the length of the bss section.

Algorithms	LED	M-LED	iM-LED
text	4076	6254	6906
data	188	232	456
bss	84	114	178
dec	4348	6600	7540

OUTLINE

5. Conclusion and Future Work

5.1 Conclusion

- Investigate LED against CPA and CCA;
- Verify CCA on M-LED which applies LEMS (one-bit entropy RSM);
- Make some Evaluation to M-LED, leading to iM-LED;
- Evaluate the security of iM-LED with CPA、CCA and TVLA.

浙江大学 信息与电子工程学院
College of Information Science & Electronic Engineering, Zhejiang University

5.2 Future Work

- Investigate other lightweight schemes on LED;
- Verify lightweight-RSM on other lightweight algorithms,

  e.g., PRESENT;
- Make full comparisons among various lightweight schemes;

Thank You !