A Reconfigurable Permutation Based Address Encryption Architecture for Memory Security

Yuchen Mei\(^1\), Li Du\(^1\), Xuewen He\(^1\), Yuan Du\(^1\), Xiaoliang Chen\(^2\), Zhongfeng Wang\(^1\)

ycmei@smail.nju.edu.cn, ldu@nju.edu.cn, mp1823002@smail.nju.edu.cn, yuandu@nju.edu.cn, xiaoliac@uci.edu, zfwang@nju.edu.cn

\(^1\)ICAIS Lab, Nanjing University, China
\(^2\)University of California, Irvine, USA
Outlines

➢ Introduction
➢ Permutation Based Address Encryption
➢ Reconfigurable Features
➢ Performance Analysis
➢ Further Enhancement
➢ Conclusion
Outlines

➢ Introduction
➢ Permutation Based Address Encryption
➢ Reconfigurable Features
➢ Performance Analysis
➢ Further Enhancement
➢ Conclusion
Introduction

➢ Traditional Memory Encryption Methods

• Elaborately designed with high security

• Software based and system-level
  ✓ Complex to implement on hardware
  ✓ Unfriendly to resource-constrained devices

• E.g.
  ✓ Lie, 2000, Execute-Only Memory
  ✓ Suh, 2007, One-Time-Pad
  ✓ Rogers, 2007, Address Independent Seed Encryption
Existing Address Encryption Architectures

- Logic functions with low complexity
  - XOR
  - Adder
  - Galois Field Multiplication (GF Multiplication)
- Not secure and lack quantitative evaluations
- E.g.
  - Gammel, 2019, GF Multiplication Encryption
  - Wong, 1999, Address Scrambling
  - Feuser, 2009, Address Encryption for Flash Memories
Introduction

➢ What led to our work?
   • Address encryption for memory which has:
     ✔ low hardware complexity
     ✔ high security level
     ✔ hardware-friendly features, e.g., reconfigurability
Outlines

➢ Introduction

➢ Permutation Based Address Encryption

➢ Reconfigurable Features

➢ Performance Analysis

➢ Further Enhancement

➢ Conclusion
Permutation Based Address Encryption

Top-level Architecture

- Three stages
  1. Adders with Key0
  2. Permutation block with Key1
  3. XOR with Key2
- Both linear and nonlinear bit mixing
- Keys are:
  - Pre-generated
  - Changed every time system is powered on
  - Unchanged within a single group of R/W cycles
Permutation Based Address Encryption

➢ Top-level Architecture

- Three stages
  ① Adders with Key0
  ② Permutation block with Key1
  ③ XOR with Key2

- Both linear and nonlinear bit mixing

- Keys are:
  ✓ Pre-generated
  ✓ Changed every time system is powered on
  ✓ Unchanged within a single group of R/W cycles
Permutation Based Address Encryption

➢ Top-level Architecture

• Three stages
  1. Adders with Key0
  2. Permutation block with Key1
  3. XOR with Key2

• Both linear and nonlinear bit mixing

• Keys are:
  ✓ Pre-generated
  ✓ Changed every time system is powered on
  ✓ Unchanged within a single group of R/W cycles
Permutation Based Address Encryption

- Utilize permutation network
- Why permutation network?
  - Nonlinear bit mixing
  - A few MUXes with low overhead
  - Long effective key length
- Recursive design with $4 \times 4$ subnetwork
- Numbers of MUXes and key length are:
  \[
  N = 2n(\log_2 n - 1) + 2, \\
  K = n(\log_2 n - 1) + 1
  \]
  - $N$: number of 2-input MUXes
  - $K$: effective key length
Outlines

➢ Introduction
➢ Permutation Based Address Encryption
➢ Reconfigurable Features
➢ Performance Analysis
➢ Further Enhancement
➢ Conclusion
Reconfigurable Features

- Handle various address widths
  - Enable $2^l \times 2^l$ PAE to encrypt $2^s$-bit addresses ($l > s$ and $l, s \in \mathbb{N}$)

- Utilize hardware resources efficiently
  - Encrypt sub-addresses concurrently

- One-hot configure signal $S$ to control working modes, e.g., $16 \times 16$ PAE:
  - $3'b100$: 16-bit mode
  - $3'b010$: 8-bit parallel mode
  - $3'b001$: 4-bit parallel mode
Reconfigurable Features

➢ Reconfigurable Ripple-carry Adders
  • Formed by cascaded 4-bit ripple-carry adders
  • Change the connection of carry bits to reconfigure
  • Eliminate interference among sub-addresses
Reconfigurable Features

- **Reconfigurable Permutation Network**
  - Change connection pattern to reconfigure
    - ✓ 16-bit mode
    - ✓ 8-bit parallel mode
    - ✓ 4-bit parallel mode
  - Avoid interference among sub-networks
  - Some bits of Key1 turn ineffective in parallel mode
Reconfigurable Features

➢ Reconfigurable Permutation Network

• Change connection pattern to reconfigure
  ✓ 16-bit mode
  ✓ 8-bit parallel mode
  ✓ 4-bit parallel mode

• Avoid interference among sub-networks

• Some bits of Key1 turn ineffective in parallel mode
Reconfigurable Features

➢ Reconfigurable Permutation Network
  • Change connection pattern to reconfigure
    ✓ 16-bit mode
    ✓ 8-bit parallel mode
    ✓ 4-bit parallel mode
  • Avoid interference among sub-networks
  • Some bits of Key1 turn ineffective in parallel mode
Reconfigurable Features

Arbitrary Bit Size Address Encryption

- Truncation method to handle address
- What is truncation method?
  ✓ Decompose address into power-of-2 bit sub-addresses
  ✓ Exclude excess bits
- Why truncation method?
  ✓ To handle non-power-of-2 address
  ✓ Permutation network requires power-of-2 input
  ✓ Number of truncated bits ≤ 3 with the algorithm
Outlines

➢ Introduction
➢ Permutation Based Address Encryption
➢ Reconfigurable Features
➢ Performance Analysis
➢ Further Enhancement
➢ Conclusion
Performance Analysis

➢ Evaluation Settings

- PAE, DES, AES and GF Multiplication based Encryption (GFEnc)
- Synthesized in SMIC 40nm CMOS technology
- Target frequency of 200 MHz
- Throughput is defined as:

\[
\text{Throughput} = \frac{L_{\text{input}} \times F}{T_{\text{clk}\_\text{cycle}}}
\]

\(L_{\text{input}}\): input block size
\(T_{\text{clk}\_\text{cycle}}\): clock cycles per encryption block
\(F\): target frequency

- Security level defined by brute force attack time:

\[
T_{\text{brute}\_\text{force}} = \frac{2^K \times T_{\text{clk}\_\text{cycle}}}{2}
\]

\(K\): effective key length
Performance Analysis

- PAE vs DES
  - ✓ 16× speed compared with DES
  - ✓ 1.4× effective key length of DES
Performance Analysis

• PAE+DES vs AES with Best Performance
  ✓ Combination of PAE and DES
  ✓ 1.5\times area efficiency of AES
  ✓ 1.76\times power efficiency of AES
  ✓ 18\times brute force attack time of AES
Performance Analysis

• PAE vs GFEnc

• PAE
  ✓ 85.71% power consumption of GFEnc
  ✓ 96.09% gate count of GFEnc
  ✓ 1.531 × longer key length than GFEnc

• Permutation Block in PAE
  ✓ 78.57% power consumption of GF Multiplication
  ✓ 70.87% gate count of GF Multiplication
  ✓ 2.06 × longer key length than GF Multiplication

(a) Performance parameters comparison

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Effective Key Length</th>
<th>Brute Force Attack Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAE</td>
<td>81 bit</td>
<td>$1.209 \times 10^{24}$ cycles</td>
</tr>
<tr>
<td>GFEnc</td>
<td>32 bit</td>
<td>$2.147 \times 10^{10}$ cycles</td>
</tr>
</tbody>
</table>

(b) Security parameters comparison
Outlines

➢ Introduction
➢ Permutation Based Address Encryption
➢ Reconfigurable Features
➢ Performance Analysis
➢ Further Enhancement
➢ Conclusion
Further Enhancement

- Complete demo on IoT devices
- More attack approaches for security evaluation
- Encryption processor containing PAE and customized crypto engine
Outlines

➢ Introduction
➢ Permutation Based Address Encryption
➢ Reconfigurable Features
➢ Performance Analysis
➢ Further Enhancement
➢ Conclusion
Conclusion

➢ Designed the Permutation Based Address Encryption for Memory Security:
  
  • Faster encryption speed and higher security level compared with DES:
    ✓ 16× encryption speed
    ✓ 1.4× effective key length
  
  • Better area and power efficiency and higher security level compared with AES:
    ✓ 1.5× area efficiency
    ✓ 1.76× power efficiency
    ✓ 18× brute force attack time to hack
  
  • Higher security level with less power and gate count overhead compared with GFEnc:
    ✓ 85.71% power consumption
    ✓ 96.09% gate count
    ✓ 2.53× effective key length
Thank You!

Yuchen Mei (ycmei@smail.nju.edu.cn)
Li Du (ldu@nju.edu.cn)
Xuewen He (mp1823002@smail.nju.edu.cn)
Yuan Du (yuandu@nju.edu.cn)
Xiaoliang Chen (xiaoliac@uci.edu)
Zhongfeng Wang (zfwang@nju.edu.cn)
Q&A