RISC-V Day Tokyo2023 Summer

“An Effective Way to Perform Correlation Power Analysis Attack on Cryptographic RISC-V SoC”

Authors : Thai-Ha Tran, Cong-Kha Pham, and Trong-Thuc Hoang

Affiliation : Department of Computer and Network Engineering

The University of Electro-Communications, Tokyo, Japan

Position : Ph.D. student

OUTLINE

“An Effective Way to Perform Correlation Power Analysis Attack on Cryptographic RISC-V SoC”

- 1. INTRODUCTION
- 2. ESTIMATE THE QUANTITY OF LEAKAGE INFORMATION
- 3. TARGETED RISC-V COMPUTER ARCHITECTURE
- 4. EXPERIMENTAL RESULTS
- 5. CONCLUSION

1. INTRODUCTION

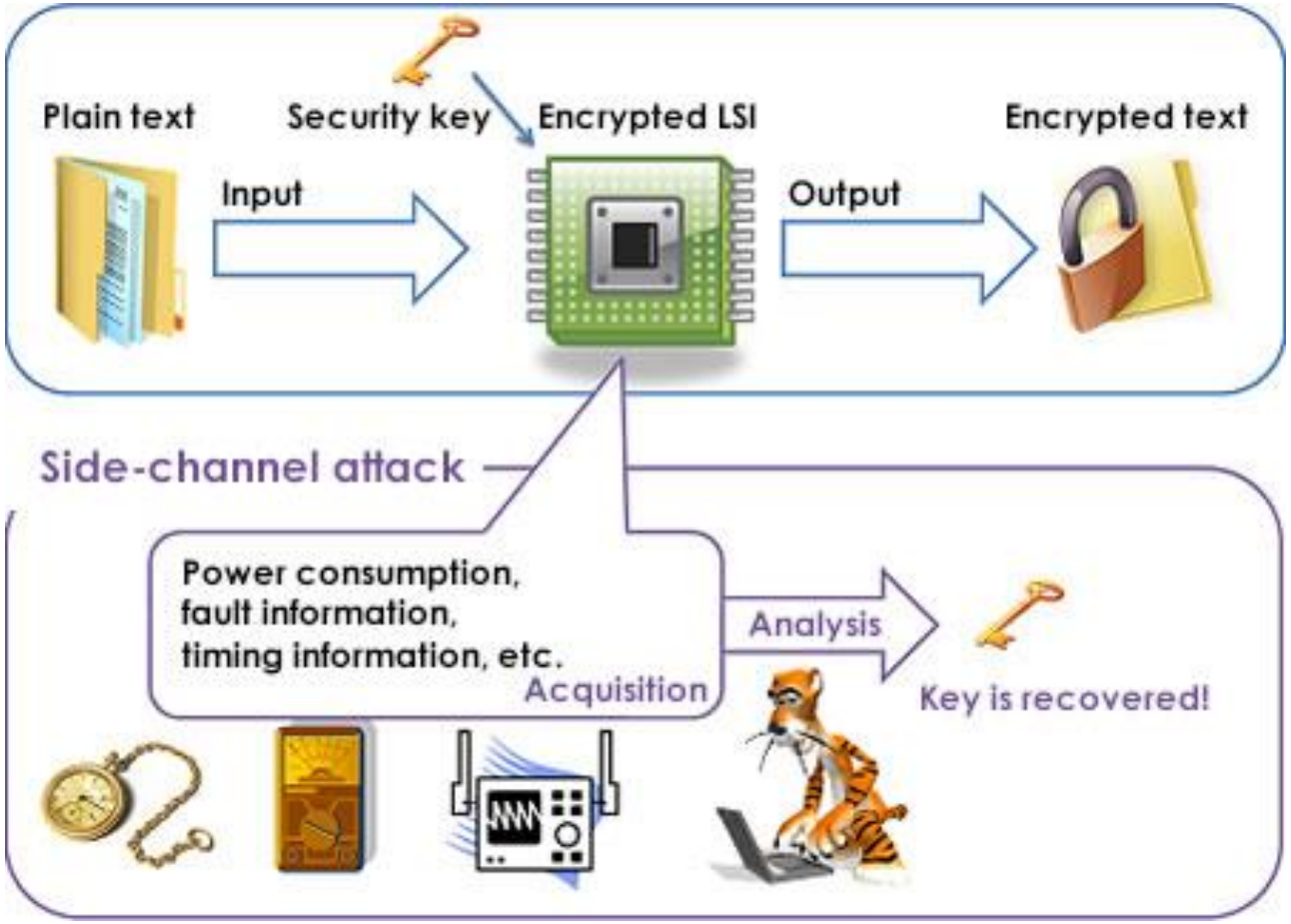


Fig. 1: Cryptographic design's vulnerability

- Profiled Power Analysis Attacks
- Non-profiled Power Analysis Attacks
  - Simple Power Analysis (SPA)
  - Differential Power Analysis (DPA)
  - **Correlation Power Analysis (CPA)**
  - Non-profiled Deep Learning-based SCA

- This poster is a part of our recent work, which is under publication in IEEE Trans. on Computers [1].

❖ Used power model in Correlation Power Analysis Attack

- ❑ *Hamming Weight model (HW)*: only 1 involves a significant amount of power consumption.
- ❑ *Hamming Distance model (HD)*: 0 → 1 and 1 → 0 transitions have the same contribution.
- ❑ Switching Distance model (SD): transition 0 → 1 is assigned 1, the transition 1 → 0 is assigned factor φ

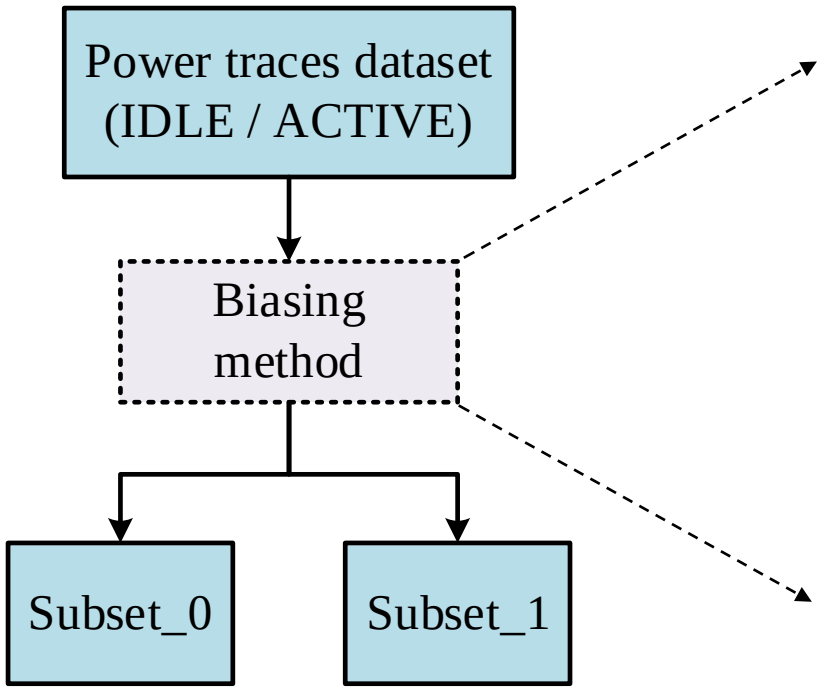
Table 1: Power consumption models [2].

Transition factors	HW	HD	SD
φ_{00}	0	0	0
φ_{01}	1	1	1
φ_{10}	0	1	φ
φ_{11}	1	0	0

OUTLINE

“An Effective Way to Perform Correlation Power Analysis Attack on Cryptographic RISC-V SoC”

2. ESTIMATE THE QUANTITY OF LEAKAGE INFORMATION



Algorithm 1 The probability of the transition α_{ij}

Input: Matrix plaintext and ciphertext $P_{D\times 128}$, $C_{D\times 128}$

Output: α_{01}, α_{10}

$subset\_0 = \emptyset$; $N^{(0)}_{0\to 1} = 0$; $N^{(0)}_{1\to 0} = 0$ ▷ Initial values for $subset\_0$

$subset\_1 = \emptyset$; $N^{(1)}_{0\to 1} = 0$; $N^{(1)}_{1\to 0} = 0$ ▷ Initial values for $subset\_1$

for m from 0 to $D-1$ **do**

  $n_{01} = 0$; $n_{10} = 0$ ▷ Set two counters

  for l from 0 to 127 **do**

    $p = P_{ml}$; $c = C_{ml}$ ▷ Extract current values

    if $p = 0$ **and** $c = 1$ **then**

      $n_{01} = n_{01} + 1$

    if $p = 1$ **and** $c = 0$ **then**

      $n_{10} = n_{10} + 1$

  if $n_{01} \geq n_{10}$ **then** ▷ Update values for $subset\_0$

    $subset\_0 = subset\_0 \cup \{m\}$

    $N^{(0)}_{i\to j} = N^{(0)}_{i\to j} + n_{ij}$

  else ▷ Update values for $subset\_1$

    $subset\_1 = subset\_1 \cup \{m\}$

    $N^{(1)}_{i\to j} = N^{(0)}_{i\to j} + n_{ij}$

$\alpha^{(0)}_{ij} = \frac{1}{128\times|subset\_0|} N^{(0)}_{i\to j}$; $\alpha^{(1)}_{ij} = \frac{1}{128\times|subset\_1|} N^{(1)}_{i\to j}$

2. ESTIMATE THE QUANTITY OF LEAKAGE INFORMATION

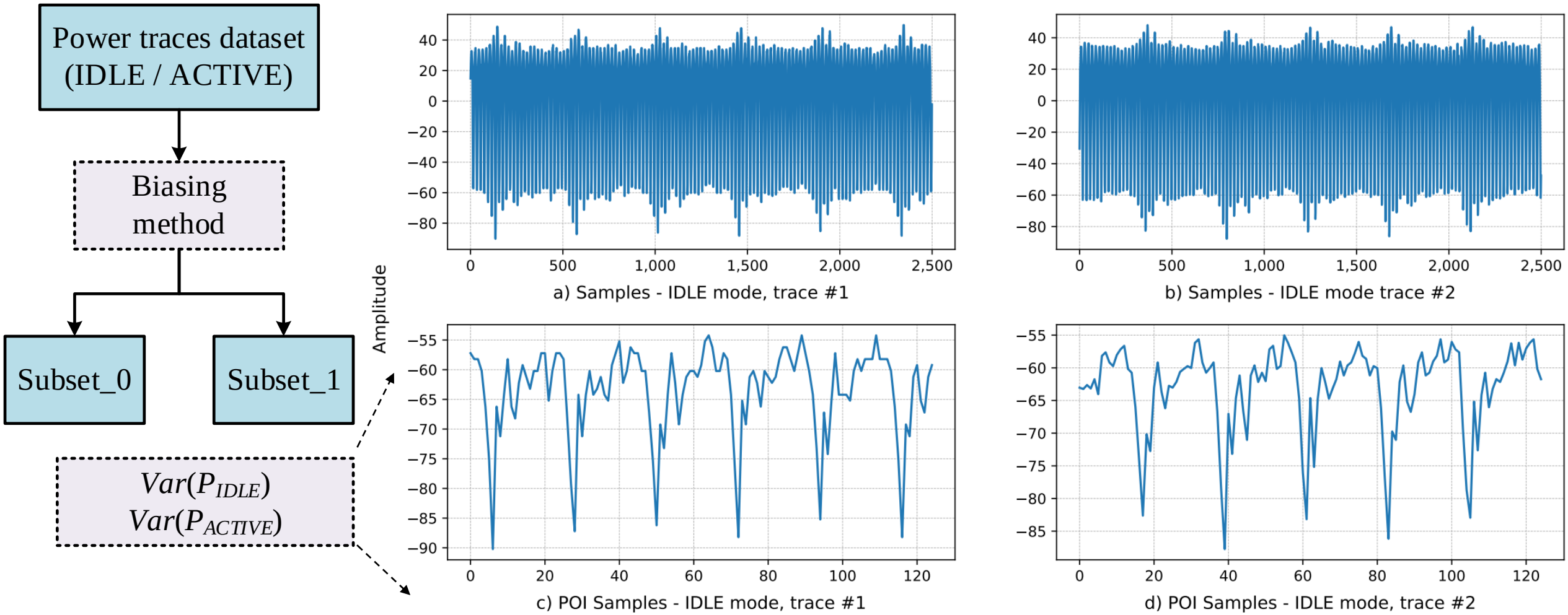
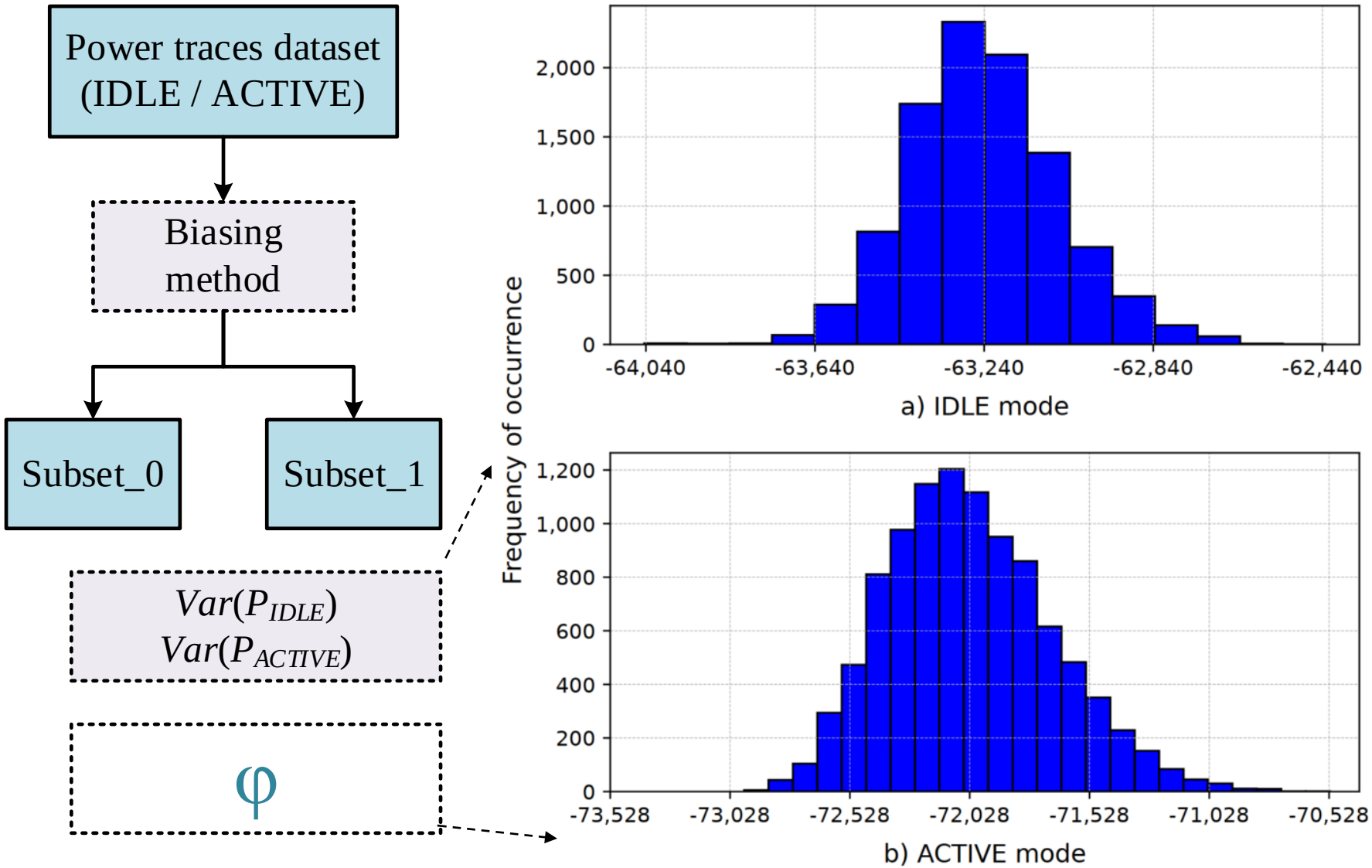


Fig. 2: Power traces in the IDLE mode

2. ESTIMATE THE QUANTITY OF LEAKAGE INFORMATION



$$SNR \approx \frac{Var\left(P_{active}\right) - Var\left(P_{idle}\right)}{Var\left(P_{idle}\right)}$$

$$\Downarrow$$

$$\begin{cases} SNR_0 \sim \left(\alpha_{01}^{(0)} + \varphi \cdot \alpha_{10}^{(0)}\right) \\ SNR_1 \sim \left(\alpha_{01}^{(1)} + \varphi \cdot \alpha_{10}^{(1)}\right) \end{cases}$$

$$\Downarrow$$

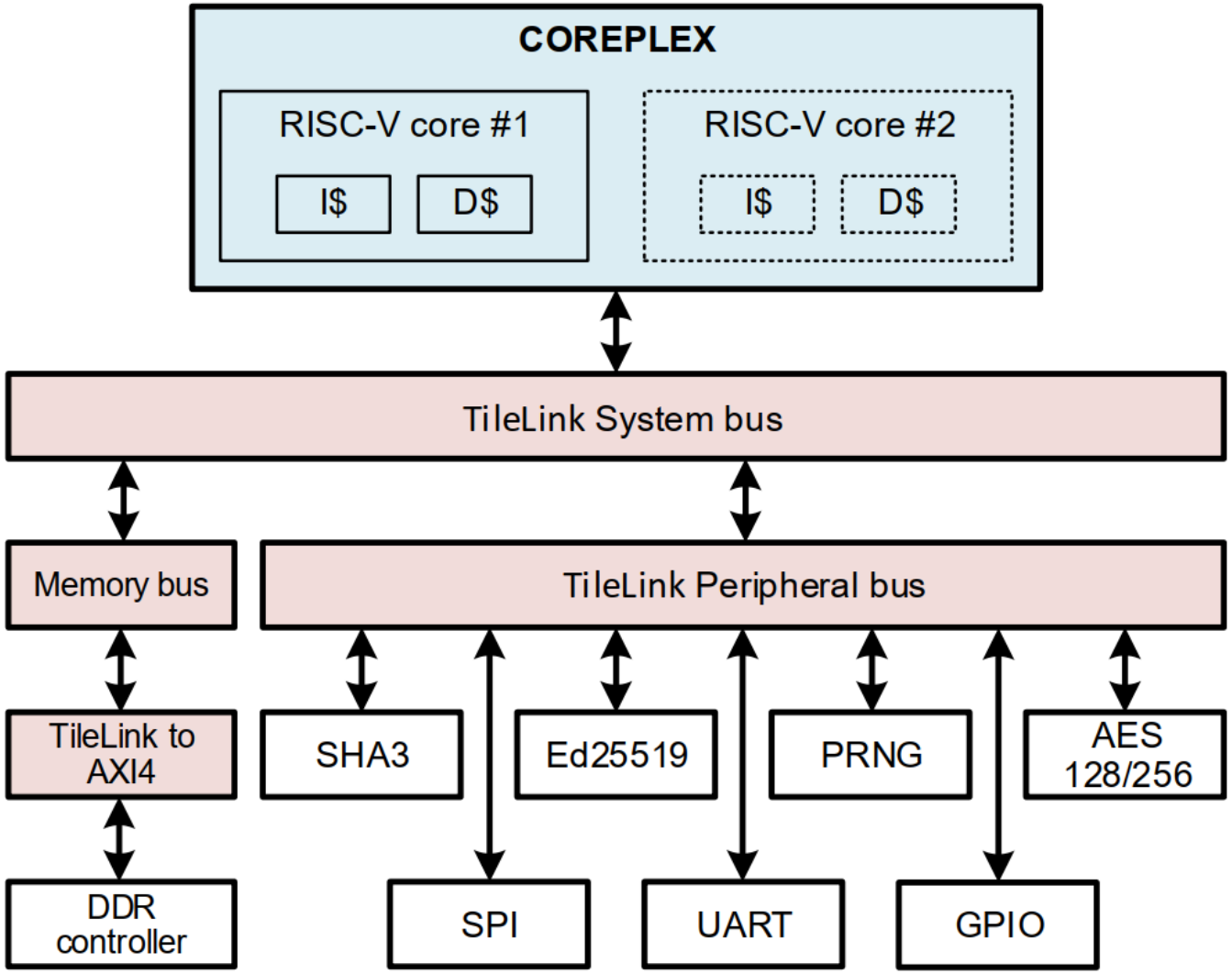
$$\varphi$$

Fig. 3: Histogram of power consumption

OUTLINE

“An Effective Way to Perform Correlation Power Analysis Attack on Cryptographic RISC-V SoC”

3. TARGETED RISC-V COMPUTER ARCHITECTURE



- Framework: Chipyard
- RISC-V cores: Rocket and Boom [3]
- Targeted algorithm: AES
  - Run directly inside a RISC-V core
  - Independent accelerator
- Instruction set: RV32IMAC; RV64IMAFDC [4]

Integer **M**ultiplication

Atomic **F**loating-point,

Double floating-point

Compress

Fig. 4: The targeted RISC-V SoC architecture

❖ Test platform: Kintex-7 XC7K160T of the Sakura-X side-channel analysis board.

Table 2: Post-implementation utilization of different config.

Name of configurations	Core #1	Core #2	AES Accelerator	
			LUTs (%)	FFs (%)
Rocket1_32	Rocket_32	-	6.89	9.59
RocketR1_64	RocketR_64	-	5.22	8.28
RocketBoomR_32	Rocket_32	BoomR_32	3.56	4.82
RocketR2_64	RocketR_64	RocketR_64	3.38	5.51
BoomR1_64	BoomR_64	-	3.09	4.87

OUTLINE

RISC-V Day Tokyo2023 Summer

“An Effective Way to Perform Correlation Power Analysis Attack on Cryptographic RISC-V SoC”


1. INTRODUCTION


2. ESTIMATE THE QUANTITY OF LEAKAGE INFORMATION


3. TARGETED RISC-V COMPUTER ARCHITECTURE


4. EXPERIMENTAL RESULTS


5. CONCLUSION

4. EXPERIMENTAL RESULTS

Table 3: The probability of the two transitions of biasing subsets.

m	Plaintext	Ciphertext	subset #0		subset #1	
			$N_{0\to1}$	$N_{1\to0}$	$N_{0\to1}$	$N_{1\to0}$
0	47d5 7467 aecf f97d 497e 1a15 ab96 c883	bcbd e5d9 6eca f855 3243 9185 c8c2 9c0d			25	32
1	17bc cd0a a6ee 0e35 7357 248c b42b 5556	0c5a 14b1 3f7e c21a fe83 f632 15cd bde4	36	33		
...	...	...	..	...	...	...
$D-1$	5c45 00a3 1cd9 b3c7 8740 3f05 3df0 d3dd	fb89 f26e 4641 f6f3 ebeb 20d0 697c bff7	39	25		
Total of the transitions			183,104	151,772	136,204	168,235
The probability of the transition α_{ij}			27.29%	22.63%	22.25%	27.61%
Number of elements			5,240		4,760	

❖ Evaluation metric: Relative gain

$$G_{\varphi} = \frac{N_{HD} - N_{\varphi}}{N_{HD}}$$

Name of config.	φ	G_{φ}
Rocket1_32	0.85	13.50
RocketR1_64	0.72 ÷ 0.90	1.07
RocketBoomR_32	0.82	5.74
RocketR2_64	0.89	6.55
BoomR1_64	0.87	12.15

4. EXPERIMENTAL RESULTS

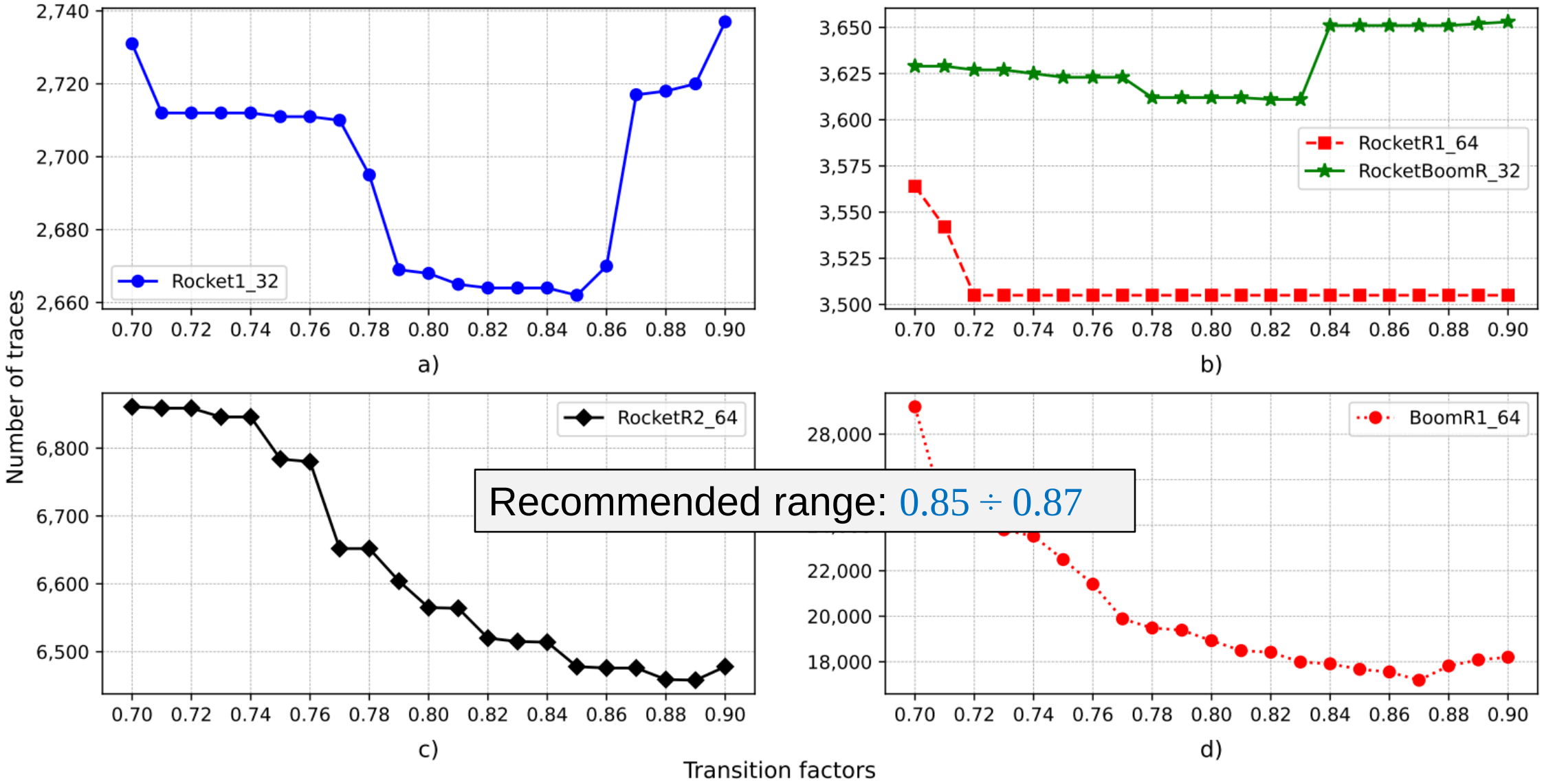


Fig. 5: Optimal range of transition factors.

OUTLINE

“An Effective Way to Perform Correlation Power Analysis Attack on Cryptographic RISC-V SoC”

5. CONCLUSION

- Overview the most suitable model for attacking the AES by applying three power consumption models: HW, HD, and SD.
- Suggest an initial step for estimating the relationship between the quantity of leakage information of the designs and the transition factors.
- The larger the relative gain is, the higher the attacking effectiveness is.
  - Recommended range: $0.85 \div 0.87$
  - Highest effectiveness: $G_{\varphi} = 13.35\ \%$ at $\varphi = 0.85$
- Future work:
  - Further experiment with other protected AES structures
  - Combines power consumption models with preprocessing techniques to enhance the performance of the CPA evaluation.

REFERENCES

[1] T. -H. Tran et al., "Transition Factors of Power Consumption Models for CPA Attacks on Cryptographic RISC-V SoC," in IEEE Transactions on Computers. doi: 10.1109/TC.2023.3262926.

[2] E. Peeters et al., “Power and electromagnetic analysis: Improved model, consequences and comparisons,” *Integration*, vol. 40, no. 1, pp. 52–60, 2007.

[3] A. Dorflinger et al., “A Comparative Survey of Open-Source Application-Class RISC-V Processor Implementations”. USA: Association for Computing Machinery, 2021.

[4] A. Waterman et al., “The RISC-V Instruction Set Manual, Volume I: User-Level ISA, Version 2.0,” Tech. Rep. UCB/EECS-2014- 54, May 2014.

“An Effective Way to Perform Correlation Power Analysis Attack on Cryptographic RISC-V SoC”

THANK YOU
FOR YOUR ATTENTION!