RISC-V Day Tokyo2023 Summer

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

Thai-Ha Tran, Cong-Kha Pham, and Trong-Thuc Hoang
University of Electro-Communications (UEC), Tokyo, Japan
Corresponding author: thaiha@vlsilab.ee.uec.ac.jp

I. INTRODUCTION

Since UC Berkeley first announced the RISC-V project in 2010, we have seen RICS-V System on Chips (SoCs) develop rapidly in the field of information security, particularly in the development of cryptographic embedded systems. From an attacking perspective, however, SoC designs still have weaknesses and are vulnerable to side-channel attacks, such as power consumption, electromagnetic radiation, thermal, etc. This poster is a part of our recent work, which has been accepted and is under publication in IEEE Transactions on Computers [1]. We present an efficient strategy for attacking the cryptographic RISC-V SoC using the well-known Correlation Power Analysis (CPA) technique. In CPA attacks, the attackers use a power model to predict the power consumption of the device under test. In each model, the effectiveness of an attack depends on the transition factor *φ*, which is a ratio related to different characteristics of the device's power consumption. This proposal introduces a solution to estimate the quantity of leakage information by determining the relationship between the *SNR* and *φ*. The experimental results show that applying the Switching Distance model brings the highest performance. In the best-case scenario, the number of traces required to reveal the secret key can be reduced by 13.35% using our suggested range of transition factors.

II. ESTIMATE THE QUANTITY OF LEAKAGE INFORMATION

Algorithm 1 The probability of the transition α_{ij}

```
Input: Matrix plaintext and ciphertext $P_{D\times128}$, $C_{D\times128}$
Output: $\alpha_{01}$, $\alpha_{10}$
subset_0 = ∅; $N^{(0)}_{0\to1} = 0$; $N^{(0)}_{1\to0} = 0$          ▷ Initial values for subset_0
subset_1 = ∅; $N^{(1)}_{0\to1} = 0$; $N^{(1)}_{1\to0} = 0$          ▷ 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 ∪ {$m$}
        $N^{(0)}_{i\to j} = N^{(0)}_{i\to j} + n_{ij}$
    else                                                            ▷ Update values for subset_1
        subset_1 = subset_1 ∪ {$m$}
        $N^{(1)}_{i\to j} = N^{(0)}_{i\to j} + n_{ij}$
$\alpha^{(0)}_{ij} = \frac{1}{128\times|subset\_0|} N^{(0)}_{i\to j}$; $\alpha^{(1)}_{ij} = \frac{1}{128\times|subset\_1|} N^{(1)}_{i\to j}$
```

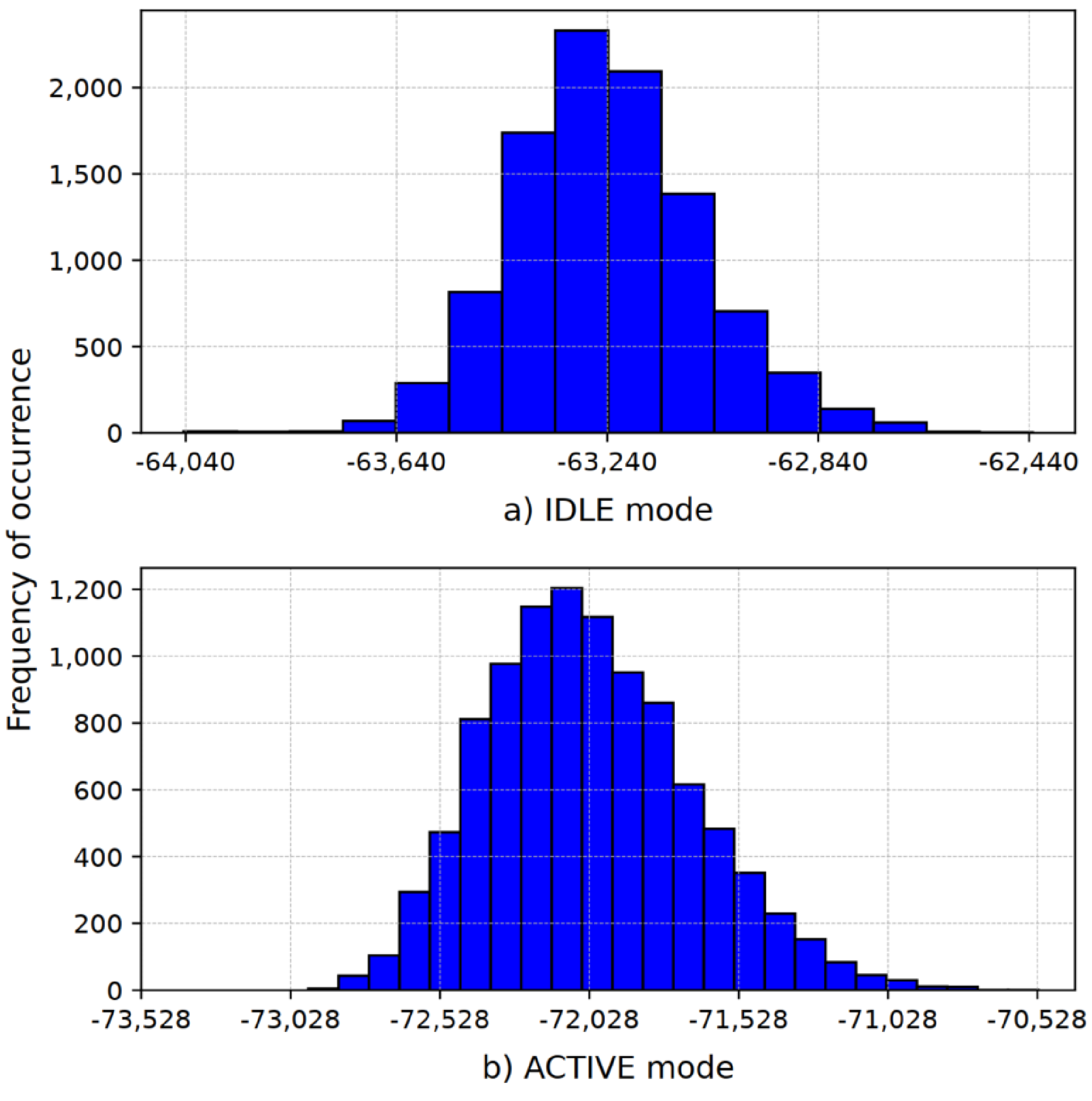

Fig. 1: Histogram of power consumption.

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

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

$$\Downarrow$$

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

$$\Downarrow$$

$$\varphi$$

III. TARGETED RISC-V COMPUTER ARCHITECTURE

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

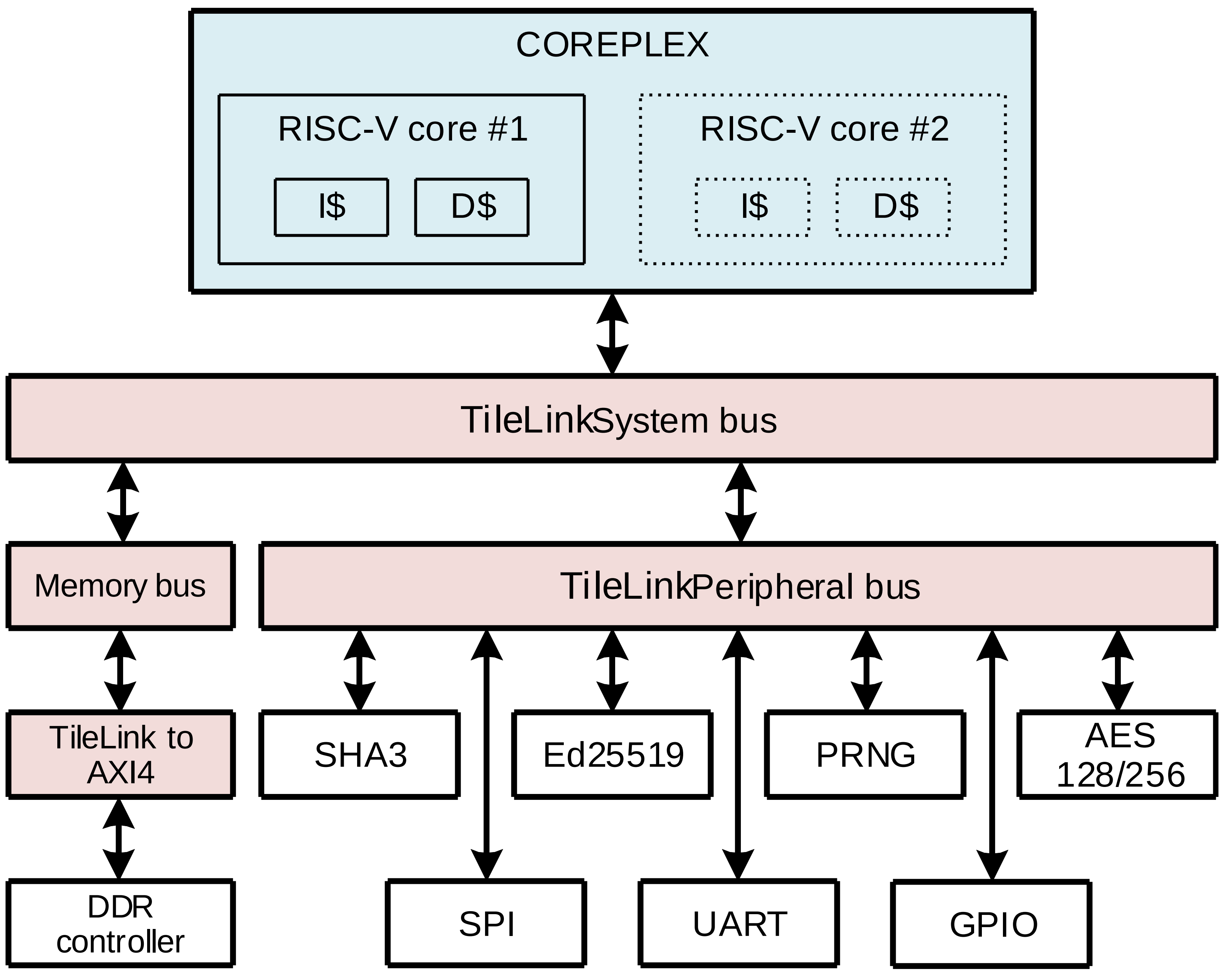

Fig. 2: The targeted RISC-V SoC architecture.

IV. EXPERIMENTAL RESULTS

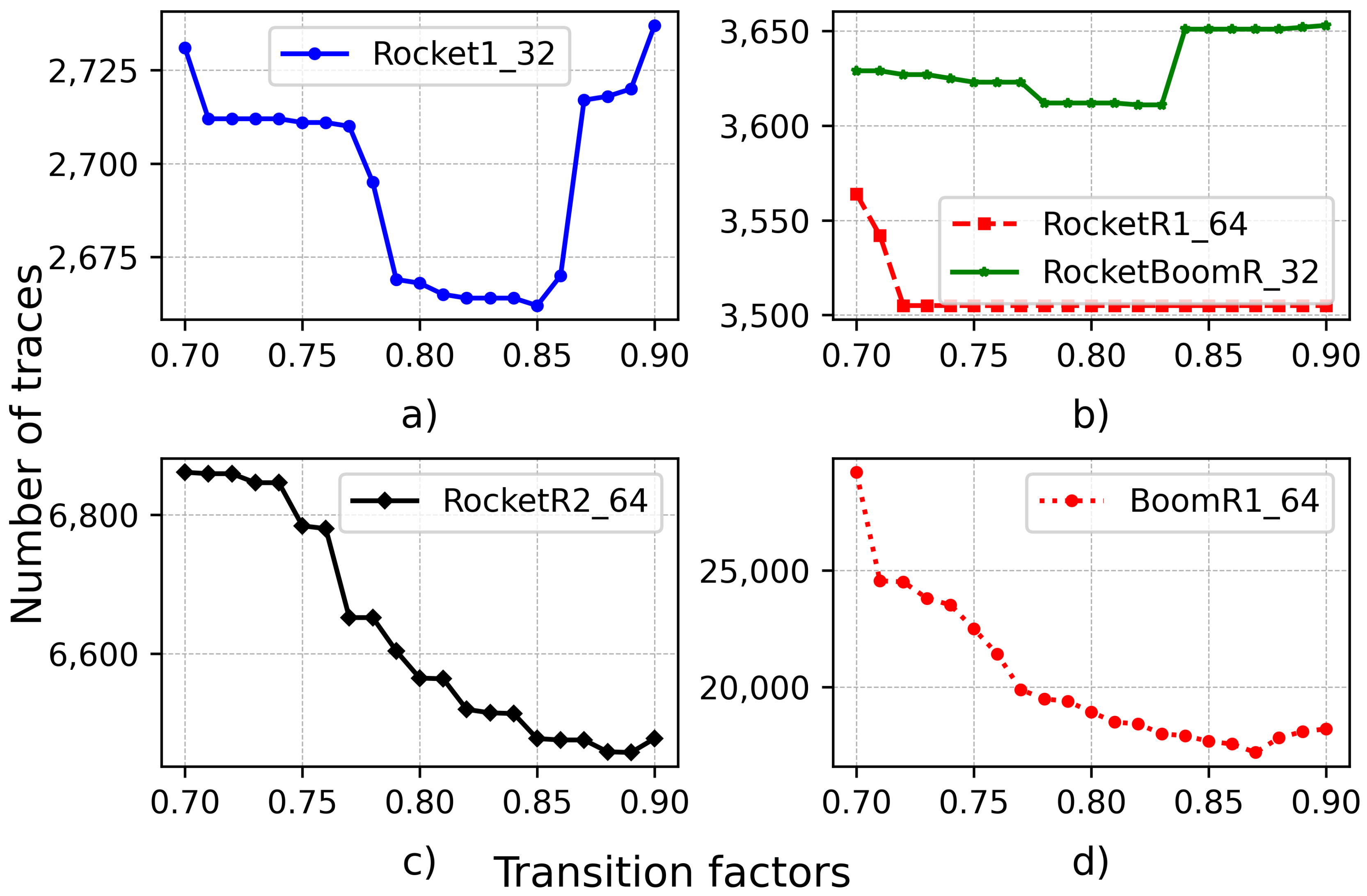

Fig. 3: Optimal range of transition factors.

- ❖ Recommended range: 0.85 ÷ 0.87
- ❖ Highest effectiveness: G_φ = 13.35 % at φ = 0.85

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. 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.

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