SEC RISC-V Workshop 2020

UEC TOKYO

AIST
NATIONAL INSTITUTE OF
ADVANCED INDUSTRIAL SCIENCE
AND TECHNOLOGY (AIST)

Dynamic Frequency Scaling as a countermeasure against simple power analysis attack in RISC-V processors

Authors: Ba-Anh Dao, Anh-Tien Le, Trong-Thuc Hoang, Akira Tsukamoto, Kuniyasu Suzaki, Cong-Kha Pham

First International Workshop on Secure RISC-V Architecture Design Exploration (SECRISC-V'20)

Outline

- Motivation
- RISC-V Processors with Dynamic Frequency Scaling
- Simple Power Analysis Experiment
- Conclusion

Outline

- Motivation
- RISC-V Processors with Dynamic Frequency Scaling
- Simple Power Analysis Experiment
- Conclusion

Side-channel attacks (SCA)

- Side-channel information strongly depend on data and operation
- Passively record the leakage (power consumption, electromagnetic radiation) from device.
- Types of Power Analysis attack:
  - Simple Power Analysis (SPA) attack [2]
  - Differential Power Analysis (DPA) attack [3]
  - Correlation Power Analysis (CPA) attack [4]
  - …

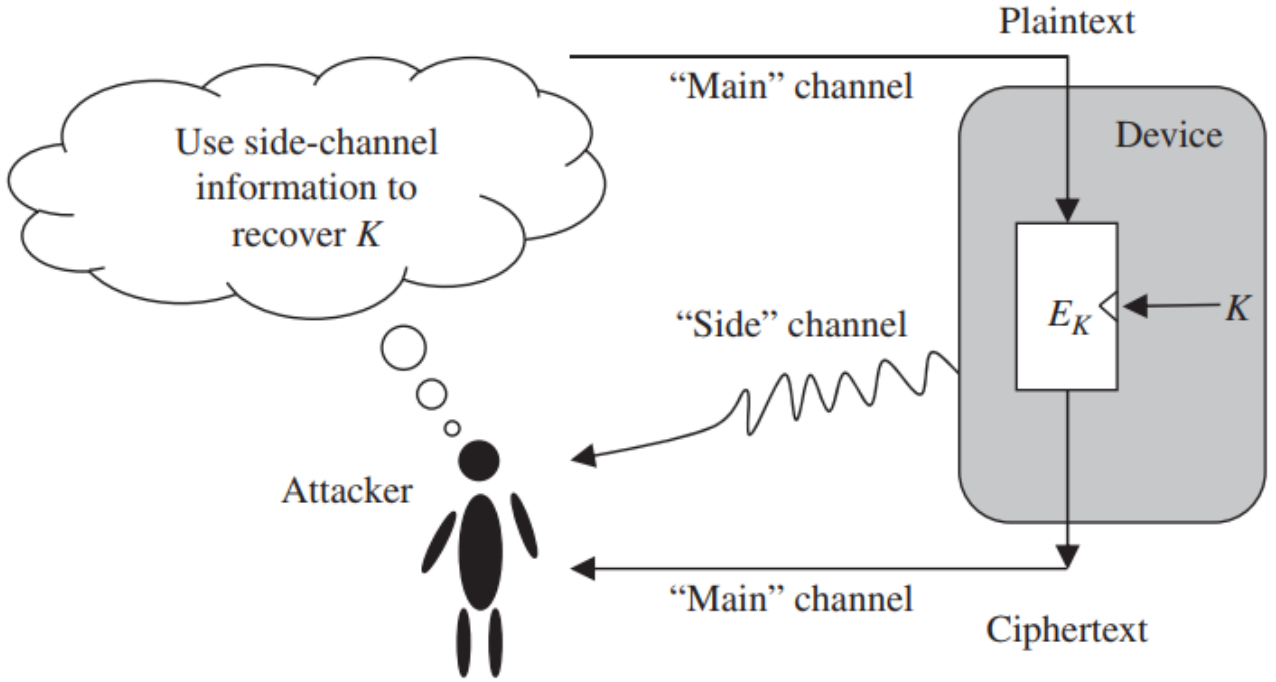


Fig.1. Main channel and side channel [1]

SCA's countermeasures

Software-based:

- "Leakage come from algorithm"
- Randomize the intermediate value or the operation
- Used in high abstraction level

Hardware-based:

- "Leakage come from implementation"
- Randomize the power consumption
- Used in physical, logic level

Outline

- Motivation
- RISC-V Processors with Dynamic Frequency Scaling
- Simple Power Analysis Experiment
- Conclusion

U500-Freedom platform

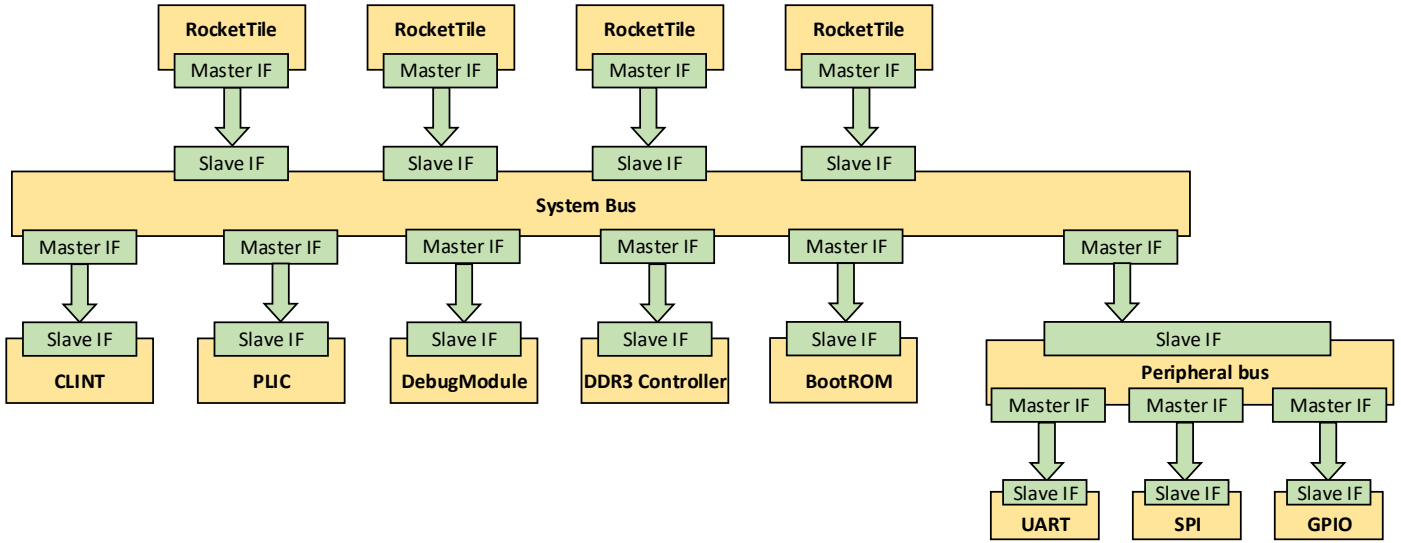


Fig.2. Block diagram of U500-Freedom platform

- U500-Freedom [5]:
  - Open-source RISC-V Processors
  - Multicore
  - Physically addressed, share-memory system
  - Booting Linux
  - TileLink interconnect standard

U500-Freedom platform

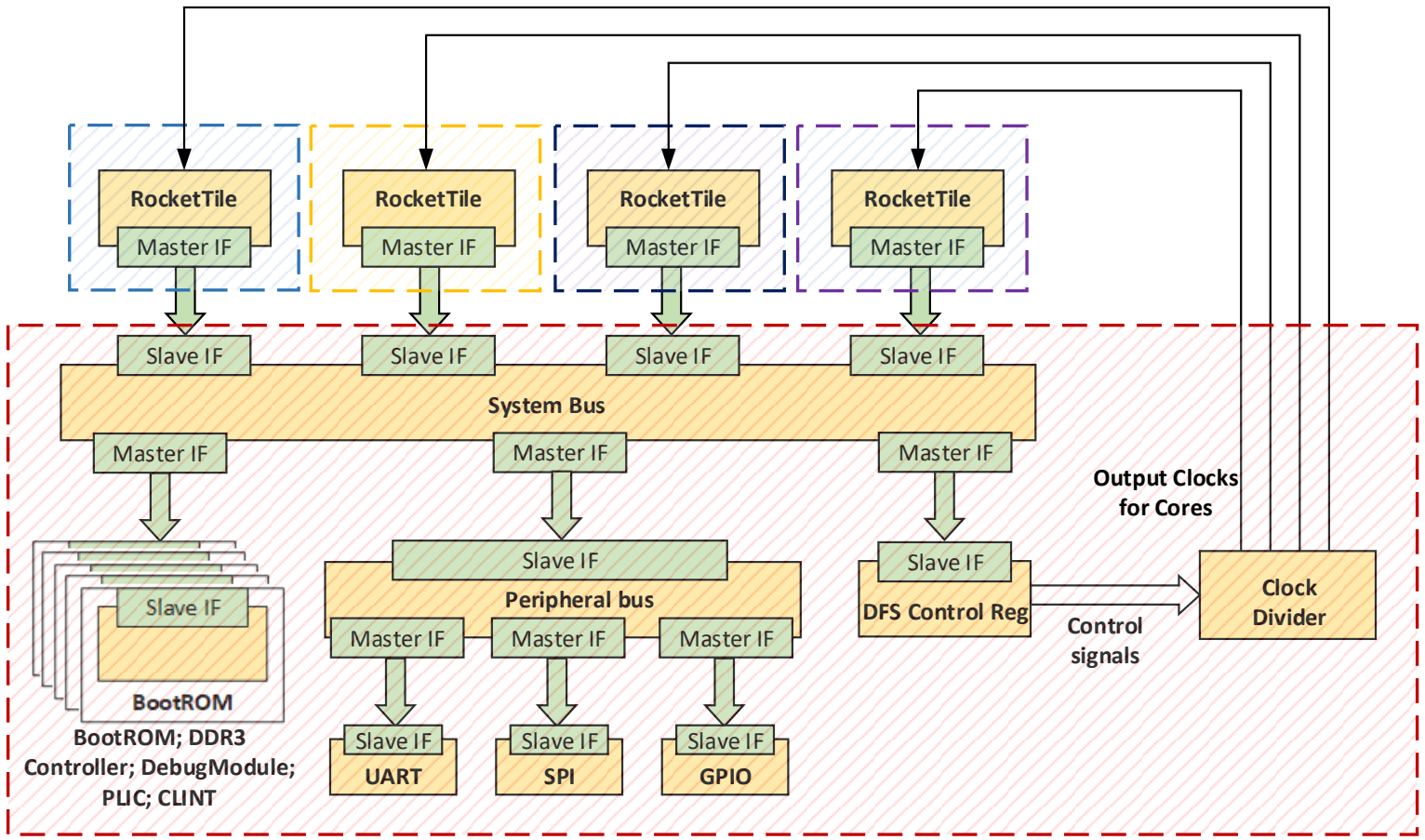


Fig.3. Block diagram of U500-Freedom platform with Dynamic Frequency Scaling

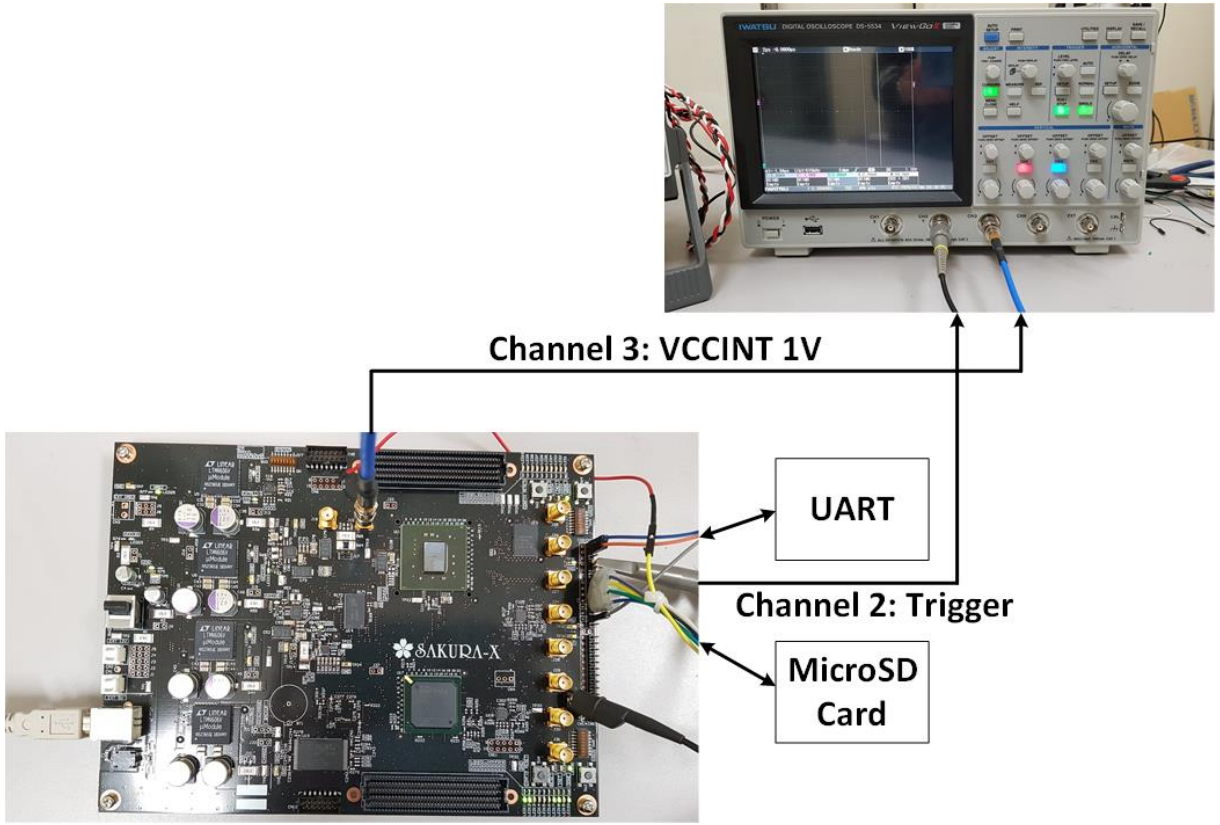
Modified, added modules:

- DFS Control registers
- Clock Divider:
  - Manual mode
  - Autonomous mode
- RocketTile – SystemBus TileLink interconnects

Outline

- Motivation
- RISC-V Processors with Dynamic Frequency Scaling
- Simple Power Analysis Experiment
- Conclusion

Simple Power Analysis Experiment



- Sakura-X: FPGA board for side-channel attack experiment
  - FPGA: Kintex-7 XC7K160T
  - Probe points at VCCINT1V (supply for internal logic cells)
- U500-freedom implemented on Kintex-7 XC7K160T
- AES-128 [6]: compiled, run on M-mode

U500-freedom on Sakura-X

- Number of Rocket cores: 2
- PLL generated clock: 100MHz

TABLE I: Post-implementation utilization.

Resource	Available	Proposed U500-Freedom platform		RocketTile module		Clock Divider module	
		Utilization	*Utilization%*	*Utilization*	*Utilization%*	*Utilization*	*Utilization%*
LUT	101,400	68,124	67.18	25,557	25.20	27	0.03
LUTRAM	35,000	3,037	8.68	112	0.32	0	0
FF	202,800	42,585	21.00	14,403	7.10	22	0.01
BRAM	325	50	15.38	24	7.38	0	0
DSP	600	30	5.00	15	2.50	0	0
MMCM	8	2	25.00	0	0	0	0
PLL	8	1	12.50	0	0	0	0

Measured results

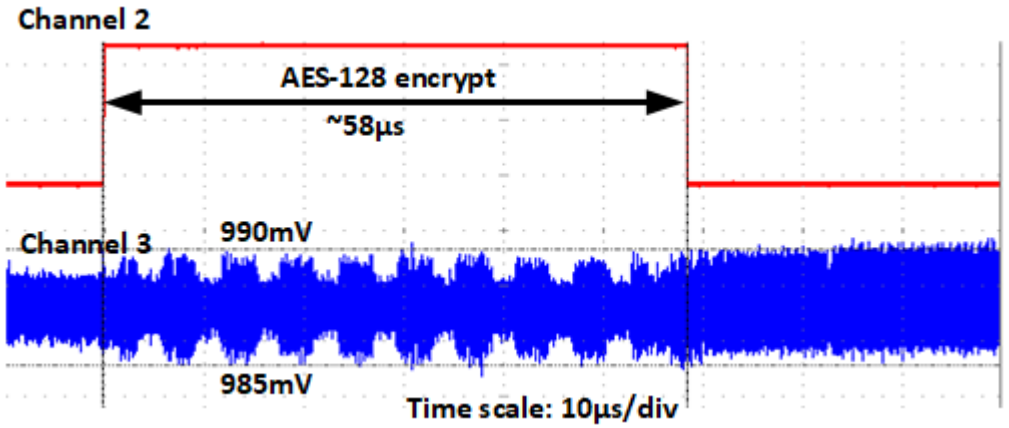


Fig.4. Power trace when core clocks is 100MHz

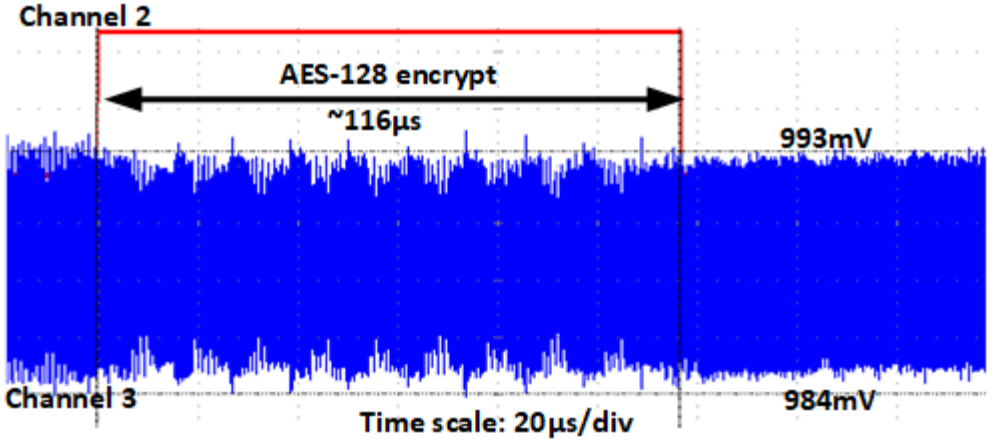


Fig.5. Power trace when core clocks is 50MHz

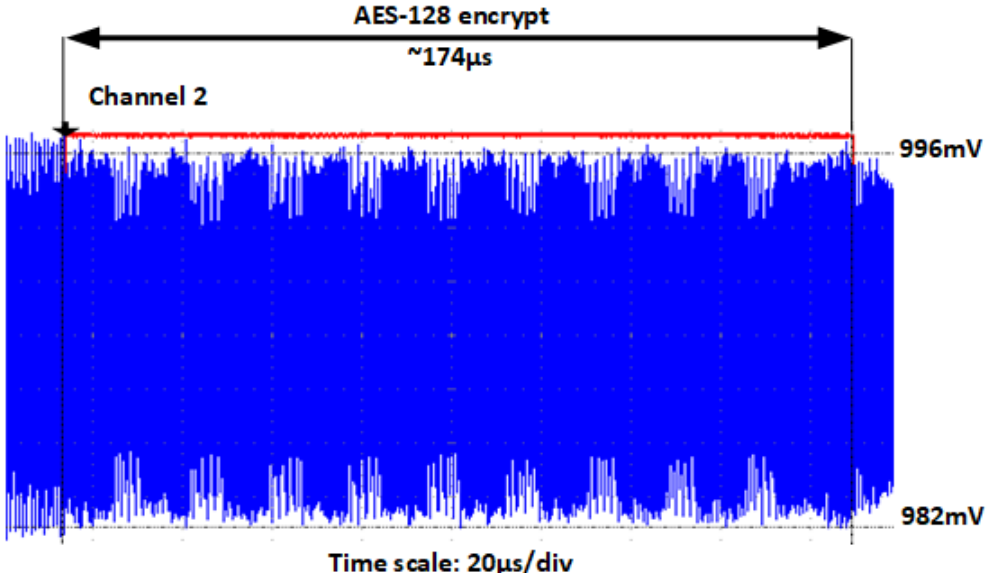


Fig.6. Power trace when core clocks is 33.33MHz

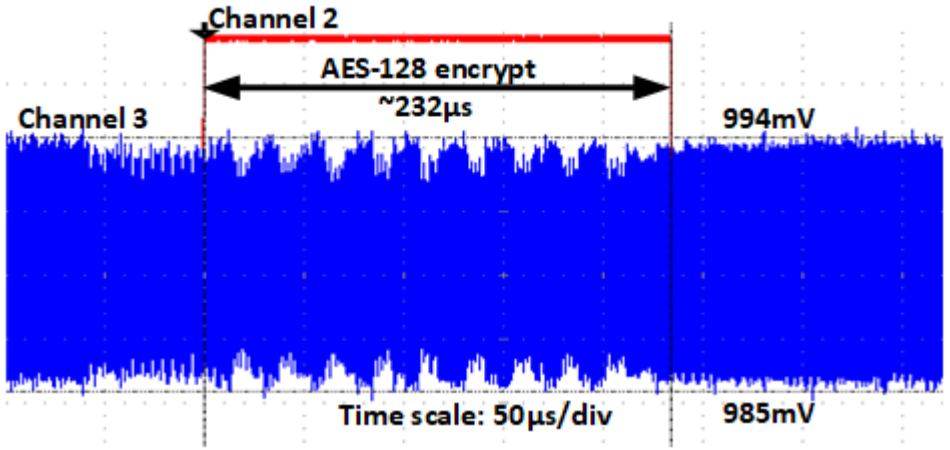
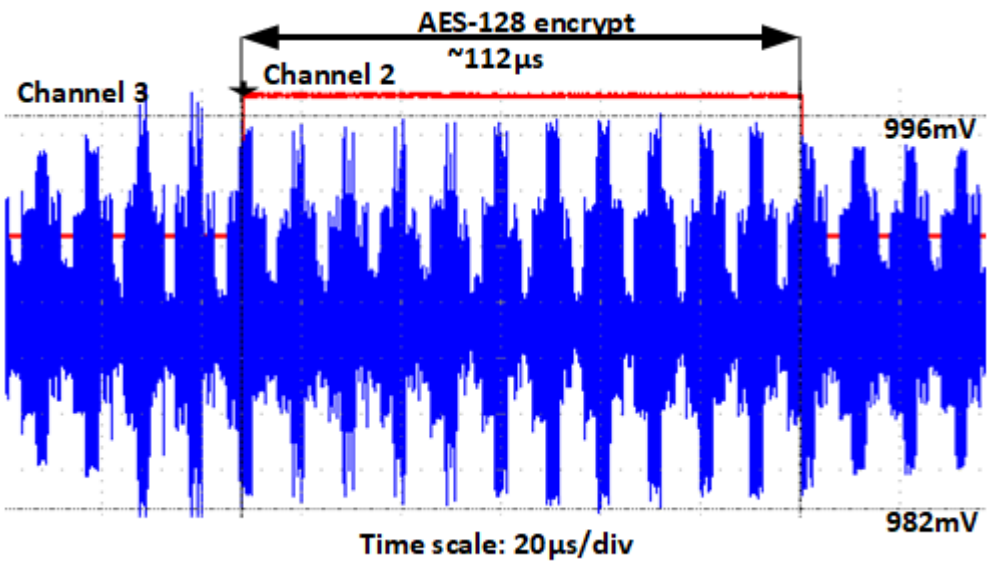
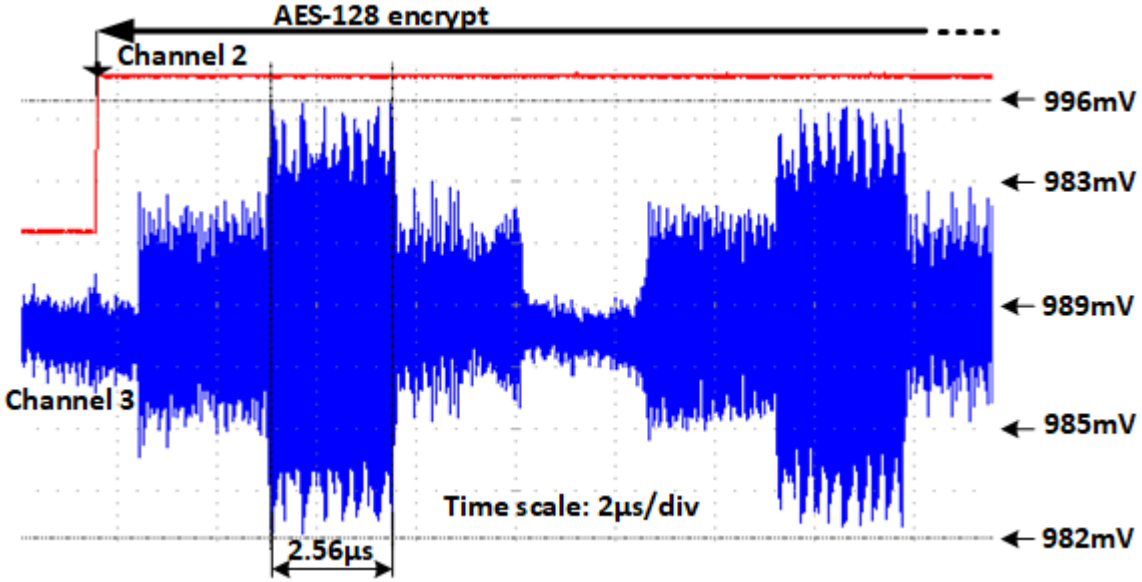


Fig.7. Power trace when core clocks is 25MHz

Measured results





- Rocket core clock changed every 2.56µs (100MHz, 50MHz, 33.33MHz, 25MHz)
- 10-rounds peak pattern of AES-128 cannot be seen.

Outline

- Motivation
- RISC-V Processors with Dynamic Frequency Scaling
- Simple Power Analysis Experiment
- Conclusion

Conclusion

- Propose & demonstrate using Dynamic Frequency Scaling with RISC-V processor as countermeasure for Simple Power Analysis attack.
- Can cover sensitive operation from visual observation.
- Hardware resources requirement is virtually unchanged.

Q&A

References

[1] K. Sakiyama, Y. Sasaki and Y. Li, “Security of Block Ciphers From Algorithm Design to Hardware Implementation”. Wiley, pp 153, 2015

[2] P. Kocher, J. Jaffe and B. Jun, “Differential power analysis,” in Proc. of19th annual international cryptology conference, pp. 388-397, 1999.

[3] P. Kocher, J. Jaffle, B. Jun et al., “Introduction to differential poweranalysis,” J. Cryptographic Engineering, vol. 1, pp. 5-27, Apr. 2011.

[4] J. S. Coron, P. Kocher and D. Naccache, “Statistics and secret leakage,”, in Proc. of International Conference on Financial Cryptography, pp.157-173, 2001.

[5] https://github.com/sifive/freedom.

[6] https://github.com/kokke/tiny-AES-c.