SCIENCE CHINA
Information Sciences

• Supplementary File •

Transistor level SCA-resistant scheme based on fluctuating power logic

Liang Geng[1], Fan Zhang[1,2*], Jizhong Shen[1], Wei He[3], Shivam Bhasin[3], Xinjie Zhao[4] & Shize Guo[4]

[1]*College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou,* 310027*, China;*
[2]*Science and Technology on Communication Security Laboratory, Chengdu,* 610041*, China;*
[3]*Temasek Laboratories, Nanyang Technological University,* 637371*, Singapore;*
[4]*The Institute of North Electronic Equipment, Beijing,* 100191*, China*

Appendix A Experiment Results

In order to establish topological design rules and to recognize possible obstructions for securing an encryption block module against DPA at the cell level, we take fundamental components (SBox module) of Advanced Encryption Standard (AES) algorithm [1] as an example to further verify the proposed FPL logic in real scenarios. After acquiring the power traces for random input data, we then launch the power analysis to validate the enhanced security of the proposed logic-based circuits. In this part, we focus on correlation power analysis (CPA).

The experiment applied in this section is depicted in Fig. A1, which consists of two 8-bit input registers (Data, Key), one 8-bit XOR gate, the SBox module (i.e. a 256-bytes table look-up) from the AES algorithm and one 8-bit output register. The above circuit has been implemented in standard cell-based and FPL-based logics for comparisons.

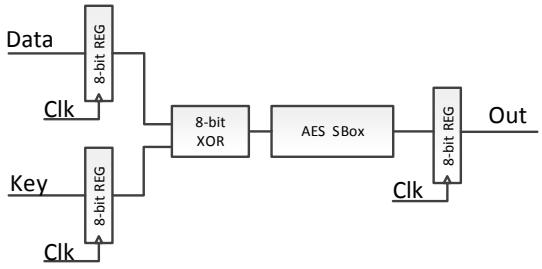
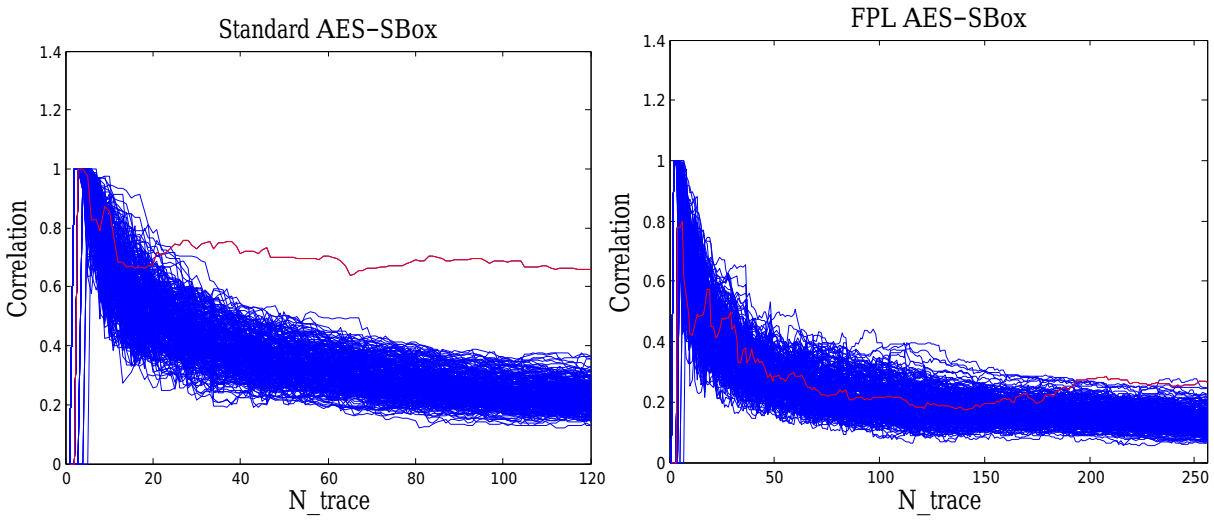


Figure A1 Simulation testbench for AES-SBox modules.

We evaluate the security of standard cell- (SC) ang FPL-based implementations of the AES-SBox module against CPA analysis. The attack results are shown in Fig. A2(a), where the red curve stands for the right key hypothesis. As shown in the figures, it's easy to reveal the right key of SC implementation of the AES-SBox module with only 22 traces, while the FPL logic greatly boosts the security of the AES-SBox module, which needs up to 250 power traces to reveal the secret key, shown in Fig. A2(b). Note that the FPL-based cells are built in a simplified way based on SC-based cells. So we believe that the expecting level of security of FPL implementation has been achieved and can be further enhanced with significantly increased complexity when combined with other cell-level countermeasures.

As a consequence, our proposed FPL logic is suited for SC-based modules, which is promising to be used in hardware implementations of Internet of Things (IoT) and Cyber-Physical Systems (CPS), especially on the embedded endpoints which are security-critical but resource-constrained.

* Corresponding author (email: fanzhang@zju.edu.cn)



(a) Correlation *vs.* number of traces (b) Correlation *vs.* number of traces

Figure A2 CPA attack results of standard AES-SBox modules.

References

1 Rijmen V, Daemen J. Advanced encryption standard. Proceedings of Federal Information Processing Standards Publications. National Institute of Standards and Technology, 2001, 19-22.

2 McEvoy R, Murphy C, et al. Isolated WDDL: a hiding countermeasure for differential power analysis on FPGAs. ACM Transactions on Reconfigurable Technology and Systems (TRETS), 2009, 2(1): 1-23.