DPA countermeasures for reconfigurable crypto processor using non-deterministic execution

Hai Huang, Bin Yu, Zhiwei Liu, Rui Weng, Junfeng Gao, and Mingyuan Ren
School of Software and Microelectronics, Harbin University of Science and Technology, 52# Xuefu Road, Nangang District, Harbin, China
a) yubin@hrbust.edu.cn, Corresponding Author

Abstract: This brief proposes a differential power analysis (DPA) countermeasure for reconfigurable crypto processors. This method is verified on Field Programmable Gate Array (FPGA). The FPGA runs at clock frequency of 10 MHz, and AES algorithm is mapped on the array. Our countermeasure is based on random delay insertion (RDI), meanwhile keep pipeline processing of data. Effective DPA resistance is achieved by generating delays which subject to approximate uniform distribution and rearranging the processing order of data. This method can improve the difficulty of DPA and keep high throughput. This method also adapt to any other hardware pipeline style cipher processor.

Keywords: differential power analysis, reconfigurable crypto processor, non-deterministic execution, advanced encryption standard

Classification: Integrated circuits

References
[1] P. Kocher, et al.: “Differential power analysis,” Advances in Cryptology - Crypto (1999) 388.
[2] T. Güneysu and A. Moradi: “Generic side-channel countermeasures for reconfigurable devices,” presented at the Cryptographic Hardware and Embedded Systems (CHES) (2011) 33 (DOI: 10.1007/978-3-642-23951-9_3).
[3] M. Stöttinger, et al.: “Survey of methods to improve side-channel resistance on partial reconfigurable platforms,” Lecture Notes in Electrical Engineering 78 (2010) 63 (DOI: 10.1007/978-3-642-16767-6_4).
[4] G. Agosta, et al.: “The MEET approach: Securing cryptographic embedded software against side channel attacks,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst. 34 (2015) 1320 (DOI: 10.1109/TCAD.2015.2430320).
[5] D. May, et al.: “Non-deterministic processors,” Australasian Conference on Information Security and Privacy (2001) (DOI: 10.1007/3-540-47719-5_11).
[6] W. Shan, et al.: “A side-channel analysis resistant reconfigurable cryptographic coprocessor supporting multiple block cipher algorithms,” presented at the Design Automation Conference (DAC) (2014) (DOI: 10.1145/2593069.2593077).
[7] L. Liu, et al.: “SimRPU: A simulation environment for reconfigurable
architecture exploration,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 22 (2014) 2635 (DOI: 10.1109/TVLSI.2013.2295622).

[8] N. Mentens, et al.: “Power and fault analysis resistance in hardware through dynamic reconfiguration,” presented at the Cryptographic Hardware and Embedded Systems (CHES) (2008) (DOI: 10.1007/978-3-540-85053-3.22).

[9] H. Huang, et al.: “A low area-overhead higher-order low-entropy masking scheme (LEMS) against correlation power analysis attack,” IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. (2018) (DOI: 10.1109/TCAD.2018.2802867).

[10] R. Beat, et al.: “On reconfigurable fabrics and generic side-channel countermeasures,” presented at the International Conference on Field Programmable Logic and Applications (FPL) (2012) 663 (DOI: 10.1109/FPL.2012.6339147).

[11] Y. Lu, et al.: “Evaluation of random delay insertion against DPA on FPGAs,” ACM Trans. Reconfigurable Technol. Syst. 4 (2010) 11 (DOI: 10.1145/1857927.1857938).

1 Introduction

Differential Power Analysis (DPA) introduced in [1] has been proven one kind of the most powerful side-channel attack (SCA). DPA based on statistical hypothesis reveal the secret keys by collecting the different power traces, for each time instant, from the same operation at the same point. Hence, an effective countermeasure is to further randomize or shuffle the points in time when such attackable operations are processed [2]. Application Specific Integrated Circuits (ASIC) and Field Programmable Gate Array (FPGA) are two distinct alternatives for implementing cryptographic algorithms in hardware [3]. However, regardless of the technique used, the implementation of countermeasures does not come for free. Most hardware implementation introduce considerable power, area, and performance overheads. The real challenge is to provide efficient countermeasures that strike the balance among security, power consumption, area cost and performance.

DPA attacks are sensitive to measurement misalignments in the power samples that reduce the dependency between the power and the data [4]. Non-deterministic processors [5], schedule and execute instructions out-of-order, hence increases this misalignment by non-deterministic execution (NDE). However, the non-deterministic processors based NDE implement a hiding style countermeasure by randomizing execution of instructions. The instruction level parallelism is limited to particular applications, restricting the level of security in non-deterministic executions. Such an approach requires hardware modification to protect the crypto primitive, effectively resulting in a reduced applicability. Furthermore, they need to specific design for each crypto algorithm.

Reconfigurable crypto processor with the metrics of dynamic configuration, high performance is suitable for implementing multiple cipher algorithms by reconfigurable computing technology [6, 7]. It allows not only randomly insert dummy operation to change the execution time, but also to randomize the usage of the available hardware resources. Countering DPA without area and performance penalty thanks to the instinct characteristics of the reconfigurable computing [8]. In this brief, the combination of the metrics of the reconfigurable computing and non-
deterministic processor are used to promote the ability of countering DPA. A multiple stage architecture for block cipher algorithm AES is implemented on a FPGA and a countermeasure method, which keeps the approximately uniform distribution of delay, is provided to use time-varied delays for each datum. DPA experiments show that inserting random delay in pipeline can make a good balance between performance and security. For AES, it successfully resists DPA for more than one million traces.

2 Architecture and control circuit design

We presented a reconfigurable crypto processor suitable for multiple block cipher algorithms that provided dynamic reconfiguration capabilities to avoid attacks based on statistical analysis, e.g. DPA. The architecture of the reconfigurable crypto processor is shown in Fig. 1(a). The reconfigurable Crypto processor consists of a configuration controller and a processing core. The processing core consists of an RCA controller, permutation network, substitution boxes and reconfigurable cell array (RCA). The RCA is a coarse-grain reconfigurable array composed of reconfigurable arithmetic units and a series of registers and MUXs. Configuration controller is used for function configurations of multiple algorithms as well as countermeasure configurations. The round key flow and data flow control circuit is shown in Fig. 1(b). Pseudo Random Number Generators (PRNGs) are used to generate a uniform random number in the range of 0 to $N - 1$. The selection of a data path is done by alternating the configuration of the switch matrix, and the data path randomly switching between $N - 1$ different rounds of the AES. The initial key is expanded into an array of key schedule words, and then set to the specific AddK round operation according to the random number generated from PRNG. And the expanded round keys are broadcasted to the round key registers. Random Delay Insertion (RDI) like execution can be obtained by selecting the data path, the input data transfer to different data path needs different numbers of the period.

3 Proposed DPA countermeasures using non-deterministic execution on AES

The efficiency of an attack against a loop implementation is notably due to the fact
that most registers are predictable, because only one round is implemented. In case of unrolled and pipelined implementations, the situation strongly differs, as only the outer rounds are partially predictable. As a consequence, the inner rounds may be viewed as noise generators and therefore act as a well-known DPA countermeasure. Moreover, if the noise is added in the form of unrolled pipeline stages, it does not reduce the efficiency of an implementation. On the other hand, misalignment of data index will further decrease SNR. Since the success of DPA depends on the SNR, Non-deterministic execution will make DPA more difficult. Take the AES as example, we illustrate how the combination of pipelining and unrolling techniques may counteract power analysis attacks as a random noise generator.

3.1 AES data flow with deterministic execution

The AES data flow with deterministic execution is shown in Fig. 2(a). The purple line illustrates the data flow, and the direction of the data flow is indicated by arrowheads. In this mode, the blocks of the plaintext will be processed sequentially along the pipelined data path. The deterministic execution timing diagram is shown in Fig. 2(b). In Fig. 2(b), ten round keys been added to the blocks and ten operations executed at the same time. Thus, the power profile is the sum of the ten different operations.

3.2 AES data flow with non-deterministic execution

In this brief, we presented two modes execution control scheme, named as Mode 1 and Mode 2. For Mode 1, the first random number is generated randomly, and the other random numbers are generated by decrease progressively. While for Mode 2, all random numbers are generated randomly. The AES data flow with non-deterministic execution is shown in Fig. 3(a). For simplicity, only two data flow are given. The blue line illustrates the data flow when the random number \(N = 2\), while the red line illustrates the data flow when \(N = 9\). In this mode, the blocks of the plaintext will be processed parallely along the pipelined data path. The non-deterministic execution timing diagram in mode 2 with the random number \(N = 9\) is shown in Fig. 3(b). There are several (i.e. random number \(N\)) round keys been added to the blocks and several operations executed at the same time. Hence, although this solution is not perfect, it has the advantage to protect most critical parts of the data path while achieving an attractive trade-off between performance and security. Otherwise, summary of different AES modes are shown in Table I.
4 Experimental results

Fig. 4 shows the experiment environment of side channel attack. The AES design and the RDI countermeasure explained above are implemented on the Xilinx Spartan 6 FPGA (XC6SLX75-2CSG484C) of a SAKURA-G circuit board which is particularly designed for side-channel attack evaluations [9]. The instantaneous power traces are collected by means of using a Tektronix 500 MHz oscilloscope working at a sampling rate of 1 GS/s to capture the voltage drop across a 1Ω resistor placed in the VCCINT (1.2 V) path of the target FPGA. The SignalExpress is employed to record 10,000 signal samples per second.

In order to evaluate the leakage of the implementation and find a suitable power model for the correlation power analysis (CPA) attacks, we started the practical experiments when the maximum delay is set as a series values for comparisons. Since the S-box operations should have noticeable impact on the power consumption, we have used the Hamming weight of the 8-bit S-box input as the hypothetical power model in a CPA attack. We apply Correlation Power Analysis and use the

Table 1. Summary of different AES modes

| Throughput   | Mode   | DE | NDE mode 1 | NDE mode 2 |
|--------------|--------|----|------------|------------|
| ECB/CTR      | 1      | 0.67x | 0.5x       |
| CBC/CFB/OFB | 1      | 1 | 1          |

| Power/Area   | CBC/CTR | 1 | Proportional to N- | - |
|              | ECB/CTR | 1 | Easy              | Hard |
|              | CBC/CFB/OFB | Easy | Hard | Very hard |

4 Side Channel Attack

Fig. 4 shows the experiment environment of side channel attack. The AES design and the RDI countermeasure explained above are implemented on the Xilinx Spartan 6 FPGA (XC6SLX75-2CSG484C) of a SAKURA-G circuit board which is particularly designed for side-channel attack evaluations [9]. The instantaneous power traces are collected by means of using a Tektronix 500 MHz oscilloscope working at a sampling rate of 1 GS/s to capture the voltage drop across a 1Ω resistor placed in the VCCINT (1.2 V) path of the target FPGA. The SignalExpress is employed to record 10,000 signal samples per second.

In order to evaluate the leakage of the implementation and find a suitable power model for the correlation power analysis (CPA) attacks, we started the practical experiments when the maximum delay is set as a series values for comparisons. Since the S-box operations should have noticeable impact on the power consumption, we have used the Hamming weight of the 8-bit S-box input as the hypothetical power model in a CPA attack. We apply Correlation Power Analysis and use the

Fig. 4. The experiment environment of side channel attack
Pearson correlation coefficient $\rho(h, P(i))$ as statistical test. For AES, CPA attack results are shown in Fig. 5 focusing on the encryption region, with Hamming distance model to get the assumption intermediate value. It indicates that the maximum absolute value (0.027) at attack point of weaker protected AES with $N = 4$ discloses the right subkey after analyzing 100,000 traces, whereas the stronger protected AES with $N = 9$ uses 1,000,000 traces.

The measured performance is summarized in Table II and compared with prior art. As shown in Table II, the area and power overhead of the proposed method are only proportional to max random number. The proposed method (with max random number $N = 9$) is 0.88 times throughput of the design with no delay, meanwhile it keeps pipeline operation and its MTD is broadly comparable to that of other existing countermeasures. The performance summary RDI on various platform are shown in Table II.

### 5 Conclusion

The proposed countermeasure randomizes the order of data in data path, since operation moment will leak secret key information in power for DPA. The AES algorithm is used for evaluation of the countermeasure. DPA attacks with up to one million traces unsuccessful for maximum random 10. Scalable security without loss of throughput make this method and its implementation an excellent choice for coarse-grained reconfigurable array-based cipher processors. Other countermeasures can be added to our proposition in order to strengthen it against SCA.

### Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant No. 61604050) and the University Nursing Program for Young Scholars with Creative Talents in Heilongjiang Province (Grant No. UNPYSCT-2017081).