Evaluation of Power Analysis Attack Resistance of Masked Adders on FPGA

Yilin Zhao[1], Qidi Zhang[1], Hiroki Nishikawa[2], Xiangbo Kong[1] and Hiroyuki Tomiyama[1]

[1] *Graduate School of Science and Engineering, Ritsumeikan University, Shiga, Japan*
[2] *Graduate School of Information Science and Technology, Osaka University, Osaka, Japan*

Abstract

Many IoT circuits are under the threat of side-channel attacks such as power analysis attacks. Among the side-channel attacks, power analysis attacks are serious threat to security. Therefore, security measures are necessary to ensure the safe use of IoT devices. However, there are a wide variety of IoT devices, and the allowable cost, power, and required security strength vary depending on the system application. Therefore, in this study, we conduct an empirical study on masking for adders on FPGAs, and explore the trade-off between cost and safety by changing the bit length of the mask. The experimental results show that masking improves power analysis attack resistance, and series-connected masked adder is particularly effective in resisting power analysis attacks.

Keywords

Side channel attacks, T-test, Adders, FPGA, Masking, Carry save adder, Power analysis attacks, Xilinx

1. Introduction

Internet of things (IoT) devices which have become increasingly popular in recent years are vulnerable to side-channel attacks due to their exposure to the physical environment. Typical side-channel attacks include power analysis attacks, timing attacks [1], electromagnetic analysis attacks [2], and so on [3]. In particular, the power analysis attack, which infers security key from power consumption, is the most popular for side-channel attacks since an instrument is not expensive to analyze the power. According to the work [4], the power analysis attack is a serious threat to the security on not only application specific integrated circuits but also field programmable gate arrays (FPGAs). Therefore, security measures are essential for the safe use of IoT devices. Thus, one of the countermeasures against attacks is a technique called masking. Masking use random masks to split sensitive cryptographic intermediate variables into multiple shares. The side-channel information from the individual shares does not reveal the sensitive variable since the random masks should be unbreakable. Even if an attacker earns the side-channel leakage, the sensitive intermediate variable is mystified enough to keep secret. In the past, there have appeared a variety of masking methods such as multiplicative masking [5] and masked AND operation [6]. Such work aims to improve side-channel attack resistance. However, little work has investigated how masking mystifies the sensitive cryptographic variable [7]. Also, there is a wide variety of IoT devices, and the acceptable cost, power, and required security strength vary depending on the system's application. Therefore, a trade-off between implementation cost and safety can be expected by devising a method of masking.

This paper presents empirical studies on masking for adders on FPGA, focusing on adders as one of the most basic components of circuits. The contributions of this paper are two-fold. First, we compare two types of masked adders, i.e., a series-connected masked adder and a compression-based masked

The 4th International Symposium on Advanced Technologies and Applications in the Internet of Things (ATAIT 2022), August 24-26, 2022, Ibaraki, Japan
EMAIL: irin.cho@tomiyama-lab.org (Y. Zhao); qidi.zhang@tomiyama-lab.org (Q. Zhang); nishikawa.hiroki@ist.osaka-u.ac.jp (H. Nishikawa); kong@fc.ritsumei.ac.jp (X. Kong); ht@fc.ritsumei.ac.jp (H. Tomiyama)

adder. We also evaluate the impacts of the mask bit-length on the power analysis attack resistance. Specifically, we explore the trade-off between cost and security by changing the bit-length of masking.

The rest of this paper is organized as follows. In Section 2, we describe the two circuits used in our study and introduce the masking methods in these circuits. In Section 3, we present the experimental scenario and the results of the side-channel attack resistance. Section 4 gives a summary of this paper.

2. Masked arithmetic adders

In this section, we compare the power analysis attack resistance of two types of masked adders. In this paper, we make the following assumptions. An attacker inputs augend A to the adder and tries to identify the addend B through observing a side-channel leakage of the power consumption. Note that we assume the attacker cannot observe B and the sum C.

2.1. Series-Connected Masked Adder

Figure 1 shows the structure of a simple masked adder. It consists of two carry-propagate adders and one carry-propagate subtractor connected in series. First, the random number R generated by the pseudo-random number generator (PRNG) is added to A. Then, B is added to the output of A+R. Finally, R is subtracted to derive the final output of C (=A+B). In this example, we assume that A is masked with adding R, and its intermediate variable mystifies the side-channel leakage of the power consumption by the subsequent calculation. In this experiment, the pseudo-random number generator is excluded from the attack resistance evaluation, and only the arithmetic unit part is evaluated.

2.2. Compression-based Masked Adder

Figure 2 shows the compression-based masked adder. The series-connected masked adder previously presented has a long delay in adding the augend A, addend B, and random number R, since it is connected to two carry-propagate adders in series. Therefore, to reduce the delay, the three inputs are first compressed into two terms by carry save adder. According to the work [8], the carry save adder achieves the shortest latency among adders.

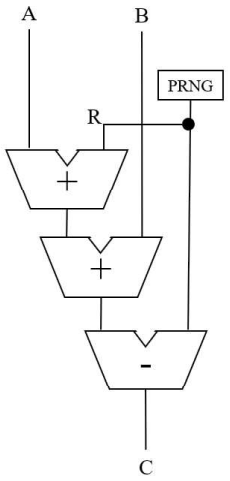

Figure 1: Series-connected masked adder

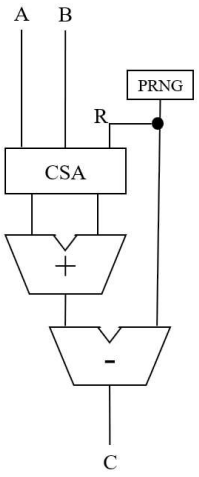

Figure 2: Compression-based masked adder

2.3. Experiments

We compare two types of masked adders. The number of bits is 128-bits. We synthesize with AMD Xilinx Vivado 2019.2. The target device is assumed to be Airtix-7 FPGA. Our synthesis has been performed with enabling a couple of optimization options to the performance. In addition, we use the tool introduced in the work [9] for power analysis. This tool can observe dynamic temporal changes in power. Table 1 shows the synthesis results. However, this table does not include the area and delay of the pseudo-random number generator.

Next, we evaluate the power consumption. Figure 3 shows the power consumptions on the compare circuits. The X-axis represents a hundred of testbenches of which each contains 2000 test vectors, and the Y-axis represents the power consumption. In the results, we focus on only the logic and signal power consumption. Table 1 also shows the average power consumption for each circuit. The results show the non-masked circuit consumes the least power since due to none of additional computation for masking. The power consumption on series-connected masked adder looks almost the same as that on compression-based masked adder.

Finally, for the evaluation of the resistance towards the side-channel leakage, we employ T-test to the results of the power analysis. It is a statistic methodology to evaluate the difference between the means of two sets of data [10-11]. T-test is expressed in the following equation:

$$t = \frac{\overline{X_1} - \overline{X_2}}{\sqrt{S_1^2/N_1 + S_2^2/N_2}} \quad (1)$$

Here, $\overline{X_1}$ and $\overline{X_2}$ represent the mean power consumption for random and fixed inputs, S_1 and S_2 are the standard deviation, and N_1 and N_2 represent the number of samples. The T-value t is desire to be less than 4.5 to meet security criteria. The results of the T-test for the two types of adders are shown in Figure 4 and Table 2. Figure 4 shows the T-value for each testbench, and the red lines represent the security criteria. Figure 4 indicates that T-values are frequently exceeded over 4.5 without masking. The T-values of series-connected masked adder are obviously ranged within the security criteria. The T-values of compression-based masked adder are seemingly larger than that of series-connected masked adder. The results show that the series-connected masked adder shows a high tolerance. Also, Table 2 shows the series-connected masked adder seems safe against power analysis attacks since T-value stays between -4.5 and 4.5 in any case, while the compression-based masked adder still exceeds the security criteria in eight testbenches.

Table 1

The number of LUTs, delay and power consumption for the synthesized adder circuits

Masks	Adders	LUTs	Delay(ns)	Power consumption(μW)
0-bit (Non-masked)	Carry propagate adder	128	8.470	699
128-bit (Full-masked)	Series-connected masked adder	384	11.048	9675
	Compression-based masked adder	511	10.268	9708

Table 2

The number of T-values violating a security criterion (>|±4.5|)

Masks	Adders	No. of T-values over |±4.5|	Maximum T-value
0-bit (Non-masked)	Carry propagate adder	23	12.10
128-bit (Full-masked)	Series-connected masked adder	0	3.07
	Compression-based masked adder	8	6.35

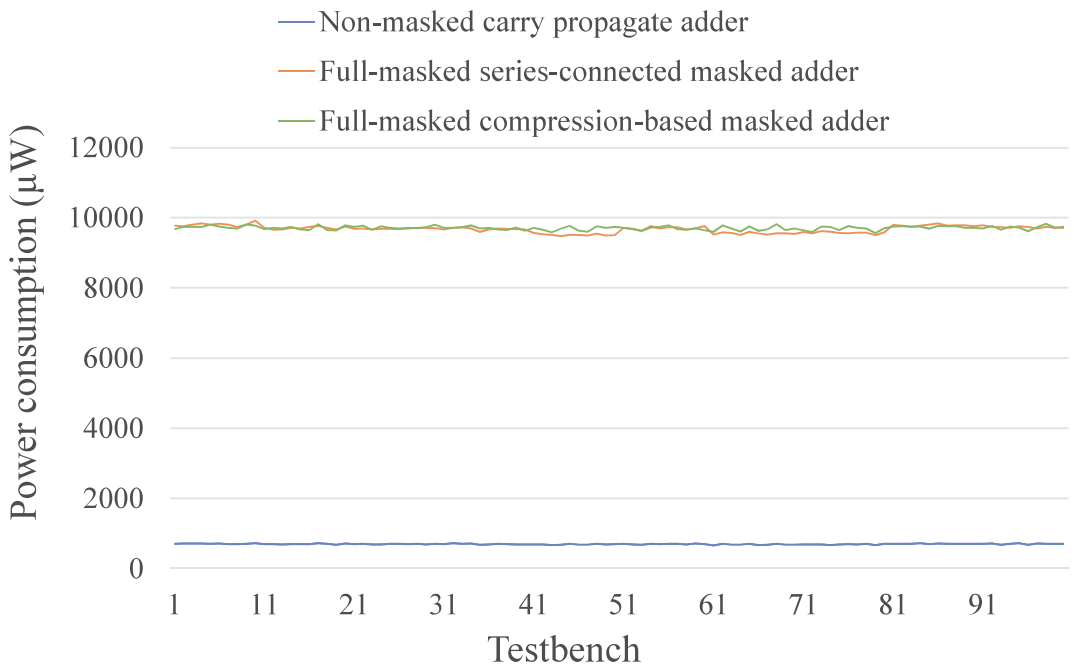

Figure 3: Analysis results of power consumption

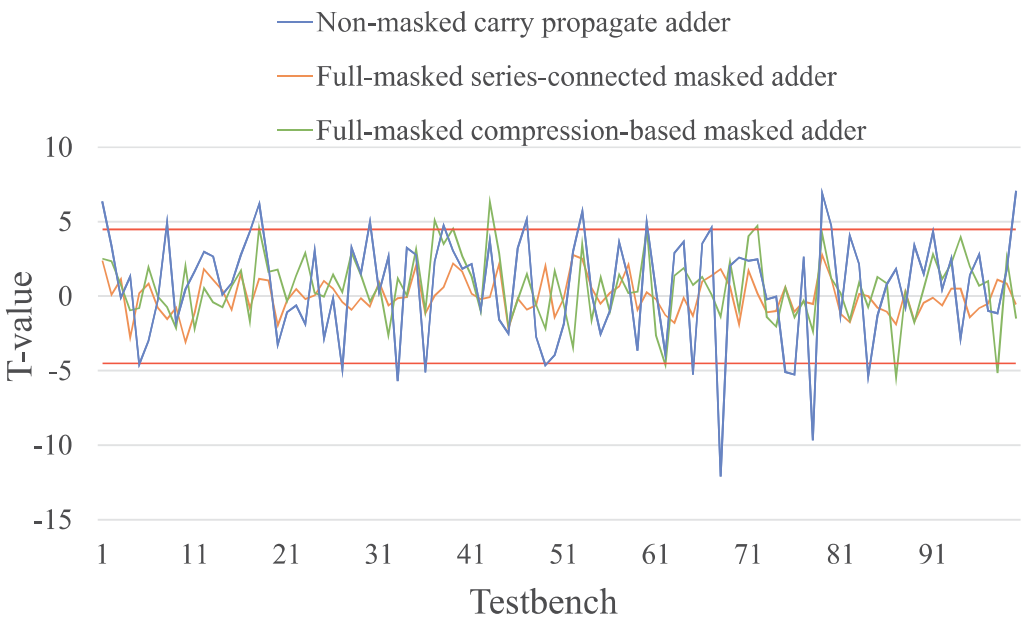

Figure 4: The results of T-test

3. Trade-off between cost and security

In the previous section, we have compared the circuits with non-masked and full-masked. In this section, unlike the previous section, we utilize the masks whose bit-widths are different. The experiments aim to explore the trade-off between the cost, power consumption, and side-channel attack resistance.

3.1. Experimental setup

In the experiments, we evaluate the power attack resistance of masked 128-bit series-connected masked adder and compression-based masked adder.

We prepare the following six different masks:

- ***Lower 32-bit mask***: Upper 96 bits in 128-bit are set to 0. The rest of lower 32 bits are assigned to a 0-1 random value R.
- ***Distributed 32-bit mask***: A 0-1 random value *R* is set every four bits and there is the mask for 32-bit in total as shown in Figure 5 (a).
- ***Lower 64-bit mask****:* Upper 64 bits in 128-bit are set to 0. The rest of lower 64 bits are assigned to a 0-1 random value *R*.
- ***Distributed 64-bit mask***: A 0-1 random value *R* is set every two bits and there is the mask for 64-bit in total as shown in Figure 5 (b).
- ***Lower 96-bit mask****:* Upper 32 bits in 128-bit are set to 0. The rest of lower 96 bits are assigned to a 0-1 random value *R*
- ***Distributed 96-bit mask***: 0 is set every four bits and the others are set to 0-1 random values *R*. The total number of bits for the mask is 96-bit as shown in Figure 5 (c).

We synthesize the adders described in the previous chapter with AMD Xilinx Vivado 2019.2. The target device and synthesis options are the same as the experiments in the previous chapter. After that, we analyze the power consumption of each circuit based on post-synthesis simulation. The power analysis tool presented in [9] is used with the Vivado toolkit.

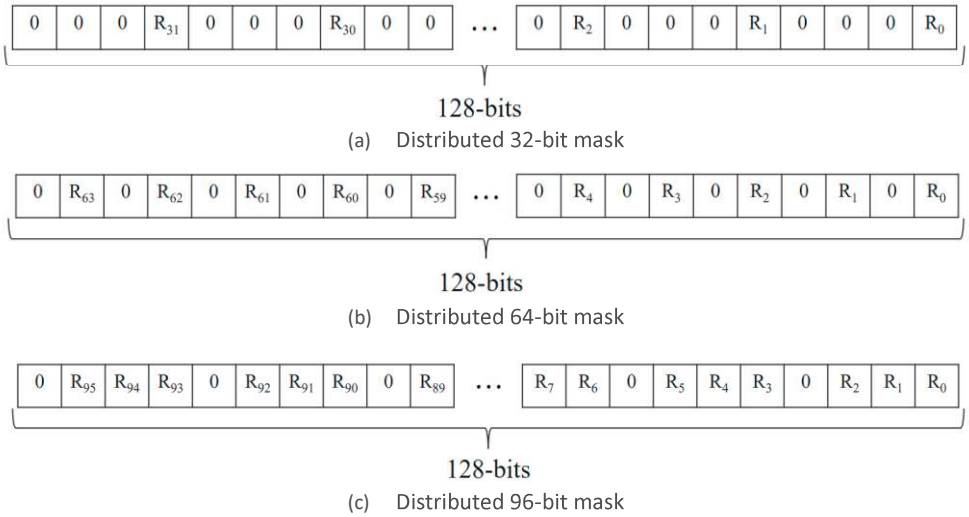

Figure 5: Distributed random masks

Table 3
Synthesis results with regard to the number of LUTs, delay and power consumption

Masks	Adders	LUTs	Delay(ns)	Power consumption (µW)
Lower 32-bit	Series-connected masked adder	288	11.048	4283
	Compression-based masked adder	511	10.268	6722
Dist. 32-bit	Series-connected masked adder	512	11.494	4772
	Compression-based masked adder	639	10.738	6923
Lower 64-bit	Series-connected masked adder	320	11.048	6128
	Compression-based masked adder	511	10.268	7714
Dist. 64-bit	Series-connected masked adder	512	11.494	6814
	Compression-based masked adder	639	10.738	8337
Lower 96-bit	Series-connected masked adder	352	11.048	7934
	Compression-based masked adder	511	10.268	8738
Dist. 96-bit	Series-connected masked adder	512	11.511	7994
	Compression-based masked adder	639	10.738	9673

Table 4
The number of T-values violating a security criterion (>|±4.5|)

Masks	Adders	No. of T-values over |±4.5|	Maximum T-value
Lower 32-bit	Series-connected masked adder	32	12.26
	Compression-based masked adder	44	19.04
Dist. 32-bit	Series-connected masked adder	28	10.98
	Compression-based masked adder	32	11.83
Lower 64-bit	Series-connected masked adder	12	8.23
	Compression-based masked adder	26	12.12
Dist. 64-bit	Series-connected masked adder	16	8.52
	Compression-based masked adder	27	10.92
Lower 96-bit	Series-connected masked adder	2	5.22
	Compression-based masked adder	18	8.11
Dist. 96-bit	Series-connected masked adder	1	4.62
	Compression-based masked adder	24	10.59

3.2. Synthesis results

The results of the number of look-up-tables (LUTs) and delay for each circuit are shown in Table 3. If the number of LUTs for the masked circuits are larger than that for the non-masked circuit shown Table 1 since the masked circuits require to mystify the intermediate variable by masking. In addition, the number of LUTs is increased as increasing the number of bits to mask. We highlight the circuits

with the smallest number of LUTs and the shortest delay. In the case of 32-bit masks, the series-connected masked adder by the lower 32-bit mask uses 288 LUTs. In terms of the delay, the compression-based masked adder by the lower 32-bit mask takes 10.268 ns. As shown in the table, it is found that the trend has been observed in any case. Overall, the series-connected masked adder uses the smallest number of LUTs, and the compression-based masked adder take the shortest delay.

3.3. Power analysis

The results of the power consumption are shown in Tables 3. Due to the larger circuit area, the compression-based masked adder is larger power consumption than the series-connected masked adder. Compared to the masks, the lower-bit masking shows the smaller power consumption than the distributed-bit masking. Thus, masking for the upper bits results in enlarging the dynamic power consumption, and the power consumption also tends to increase if the number of bits for masking is large.

3.4. Power side channel leakage analysis

Using the results of the power analysis, the T-test has been conducted with the power traces, and the results are shown in Table 4. Table 4 shows that the total number of times the T-values exceed ± 4.5 and the maximum T-value for each circuit. If a T-value exceeds ± 4.5, the case indicates that the circuit is vulnerable to power analysis side-channel attacks.

According to Table 4, the circuits masked for the lower 32-bit may spoil the security since the T-values of the lower and distributed 32-bits exceed the security criteria 32 and 28 times for the series-connected masked adder. However, the vulnerability decreases as the number of bits for masking increases. The results show that the masked circuits for series-connected masked adder are safer towards power side-channel attacks than the masked compression-based masked adder.

4. Conclusion

In this paper, we have investigated the resistance of masked adders against power side-channel attacks. The results show that the larger number of bits for masking presents the advantage in the masked adders. In addition, the masked series-connected masked adder achieves safer than the compression-based masked adder and they are superior in terms of the circuit area, while the compression-based masked adder is superior in terms of delay time.

In future, we plan to conduct a more detailed analysis of the relationship between the internal structure of masked circuits and their resistance to power analysis attacks.

5. Acknowledgments

This work is supported partly by KAKENHI 20H00590, and 21K19776.

6. References

[1] J. F. Dhem, F. Koeune, P. A. Leroux, P, Mestré, J. J. Quisquater, and J. L. Willems, “A practical implementation of the timing attack,” *International Conference on Smart Card Research and Advanced Applications*, pp. 167-182, 1998.

[2] K. Gandolfi, C. Mourtel, and F. Olivier, “Electromagnetic analysis: Concrete results,” *Cryptographic Hardware and Embedded Systems - CHES2001, LNCS*, vol. 2162, pp. 251-261, 2001.

[3] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” *Annual International Conference Cryptology*, pp. 388-397, 1999.

[4] F. X. Standaert, L. V. Oldeneel tot Oldenzeel, D. Samyde, and J. J. Quisquater, “Power analysis of FPGAs: How practical is the attack?,” *International Conference on Field Programmable Logic and Applications*, pp. 701-710, 2003.
[5] J. D. Golić, and C. Tymen, “Multiplicative masking and power analysis of AES,” *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 198-212, 2002.
[6] E. Trichina, “Combinational logic design for AES subbyte transformation on masked data,” *Cryptology EPrint Archive*, 2003.
[7] Y. Zhao, Q. Zhang, H. Nishikawa, X. Kong, and H. Tomiyama, “Power side-channel analysis for different adders on FPGA,” *International SoC Design Conference (ISOCC)*, pp. 367-368, 2021.
[8] M. SaiKumar, and P. Samundiswary, “Design and performance analysis of various adders using verilog,” *International Journal of Computer Science and Mobile Computing*, vol. 2, no. 9, pp. 128-138, 2013.
[9] Q. Zhang, X. Kong, and H. Tomiyama, “A toolkit for power behavior analysis of HLS-designed FPGA circuits,” *Low-Power and High-Speed Chips and Systems*, 2021.
[10] G. Goodwill, B. Jun, J. Jaffe, and P. Rohatgi, “A testing methodology for side-channel resistance validation,” *NIST Non-invasive Attack Testing Workshop*, vol. 7, pp. 115-136, 2011.
[11] T. Schnneider, and A. Moradi, “Leakage assessment methodology - A clear roadmap for side-channel evaluations,” *Cryptographic Hardware Embedded Syst*, pp. 495-513, 2015.