Masking Regularity of Noise for Tamper-resistant Design on FPGAs

Yui Koyanagi
Graduate School Engineering
Fukuoka University
Fukuoka City, Japan
td232006@cis.fukuoka-u.ac.jp

Tomoaki Ukezono
Dept. of EECS
Fukuoka University
Fukuoka City, Japan
tukezo@fukuoka-u.ac.jp

Abstract - In recent years, there have been numerous instances of FPGA integration into products. However, FPGA implementations are inherently more vulnerable to side-channel attacks compared to ASIC implementations. Since FPGAs integrated into products need to be cheap, applying tamper-resistant circuit design that sacrifice the area overhead, as researched in the past, is not practical. This paper improves upon conventional study that leveraged FPGA hard macros to achieve low overhead while enhancing tamper-resistance. The proposed circuit configuration method achieves low overhead while further enhancing tamper resistance.

I. Introduction

FPGAs are reconfigurable devices, and their operation is not defined during chip manufacturing. Instead, their operation is defined by downloading circuit configuration (bitstream) before use. Originally, FPGAs are used for debugging logic design during ASIC development and for achieving high-performance computing by fine-grained parallelization of algorithms. However, a usage method has been established where small-scale FPGAs are used for low-volume product production without developing and manufacturing dedicated ASIC chips. This is because the unit cost of the small-scale FPGAs is in the range of tens of dollars, whereas ASIC design incurs initial costs of at least tens of thousands of dollars. For these reasons, especially in the case of chips that do not require extremely high performance, such as image processing, FPGAs are often integrated into early batches of products and are being used by consumers.

On the other hand, among researchers in side-channel security, it is known that FPGAs are highly vulnerable to side-channel attacks. This is because small-scale FPGAs that are integrated into products often use older generation manufacturing processes, requiring a significant amount of power consumption. Furthermore, due to the characteristics of FPGAs that route the input and output of existing circuit components, improving tamper resistance through layout design scheme is not expected.

Our work that focuses on FPGA side-channel security has been presented [1]. In the work, we achieved low area overhead and enhanced tamper resistance against side-channel attacks, specifically power analysis attacks, leaking encryption keys from an AES dedicated circuit implemented on an FPGAs, by leveraging a clock multiplication circuit called DCM that is inherently equipped as a hard macro inside the FPGAs. The tamper-resistant design of FPGA using DCM involves inputting the high-frequency clock signal generated from DCM as noise into the circuit, disrupting the bit transitions of the original inputs of the circuit, and thereby obfuscating the characteristics of inputs from dynamic power consumption. This makes it more difficult to infer confidential information inside the circuit for attackers.

However, our method achieves improved tamper resistance while keeping implementation area overhead low, however finally allows the leakage of the AES encryption key.

This study considers the cause to be the periodic nature of the clock signal. Noise with regularity is easy to eliminate for attacks based on statistical methods like CPA [2], and it is considered that this did not lead to significant improvement in tamper resistance. Therefore, this study focuses on the weaknesses of the related work and proposes a method to remove the regularity in the noise introduced by the related work and evaluates it.

The contributions of this paper are as follows:

- Enhancing the tamper resistance of FPGAs, which are vulnerable to side-channel attacks when integrated into products.
- Maintaining a small-scale circuit design by utilizing unused hard macros to avoid increasing the product cost.
- Focusing on our high-frequency noise injection technique [1], eliminating noise regularity, and achieving further improvements in tamper resistance.

This paper is constructed into the following sections. This section introduced the background and the most important related work, explaining the objectives of this study. The next section will detail specific methods of power analysis attacks, along with the improvements made by this study in the form of tamper-resistant design using high-frequency noise injection techniques tailored for FPGAs. Section III will present the proposed method, and Section IV will cover its evaluation. Finally, in Section V, we will conclude the contributions of this study.

II. Related Work

At present, the generally used AES, a common key cryptography algorithm on the Internet is known to be vulnerable to power analysis attacks. These power analysis attacks involve measuring the voltage variations in the shunt resistance of the power supply in systems where AES runs, collecting a large number of waveforms, and using them as input to attack programs, finally allowing an attacker to estimate the secret key. Among these attacks, correlation power analysis (CPA) [2] is the most well-known, and with no countermeasure AES on an FPGA, the analysis of the secret key can be completed in a relatively short amount of time.

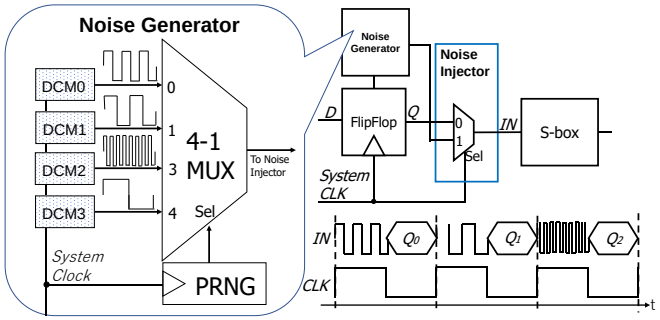

Fig. 1 Clock signal noise injection by CNS

These methods involve inferring the input values of the S-box of AES which is the target of the attack, from the dynamic power consumption resulting from input bit transitions to the S-box. Due to the round structure of AES, if the input values of an S-box for a specific round are determined through side-channel attacks, the attacker can obtain the round keys associated with that input. Since the round keys are generated by a reversible algorithm, attackers can easily obtain the secret key of the communication.

To solve the vulnerability, many tamper-resistant circuit design methods such as WDDL [3][4], MDPL [5], MAO [6], and TI [7] have been proposed. These methods significantly improve tamper resistance by modification of the circuit configuration for S-boxes but come with the drawback of requiring more than twice the implementation area of the original S-box [8]. This area overhead makes FPGAs integrated into products expensive, which is unacceptable.

Therefore, we proposed a method for acceptable tamper resistance improvement in FPGA implementations without modifying the S-box but by controlling the input to the S-box. In this paper, we will refer to this our related work as the Clock Noise Selector (CNS) for convenience. Figure 1 illustrates an overview of the CNS. The CNS involves configuring different frequency multiplication settings in the DCMs equipped in the FPGAs and generating noise by selecting it with a pseudo-random signal using a multiplexer. This noise is injected into the S-box during the first half of a clock cycle with a sufficiently long period, disrupting the bit transitions and attempting to obscure the characteristics of bit transitions Q_0-Q_1-Q_2 from dynamic power consumption. As mentioned above, if the bit transitions of Q_0-Q_1-Q_2 are leaked to the attackers, the secret key of AES also be leaked. The contribution of this study is achieving tamper resistance with a significantly smaller area overhead, using only three circuit components for each S-box: a 4-1 multiplexer, a 2-1 multiplexer, and a random number generator. This allows FPGAs to obtain tamper-resistance with a much smaller area overhead compared to conventional countermeasures such as WDDL that were difficult to implement on small scale FPGAs. However, in that evaluation, it was observed that a greater number of power consumption waveforms (traces) are required before the round keys are leaked compared to the case of no countermeasure, but finally, the round keys still leak. Therefore, this study focuses on this problem and aims to achieve further tamper-resistance while maintaining a concept of small size implementation for countermeasure.

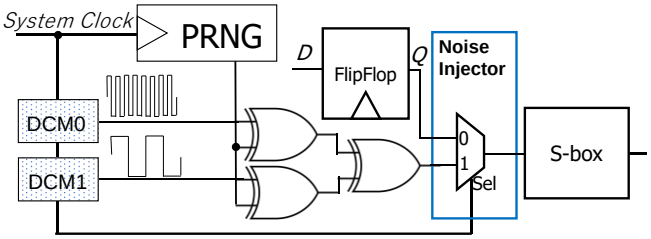

Fig. 2 Proposed noise generation & injection

III. Proposed Method

Our proposed method is illustrated in Figure 2. Our proposed method is exceedingly simple, as it merely replaces the noise generator from Figure 1 with an XOR tree. In Figure 2, there are only two DCMs, which is shown in accordance with the evaluation of this paper. The FPGA used for the evaluation has 4 DCMs, but not all of them can be used due to wiring constraints. Therefore, in the AES implementation for the evaluation in this paper, it was possible to synthesize using two DCMs. As a matter of course, even when using more DCMs, it can be accommodated by enlarging the XOR tree. The first stage of the XOR tree involves taking the XOR of each random value and the output of each DCM. It's important to note that a different random value must be input to each of the two XOR gates in the first stage. This enables that the noise clock inverts when the random value is 0. The second stage of the XOR tree mixes different noise clocks with distinct frequencies by XORing them together. This allows the synthesis of clocks with different frequencies.

This noise generator is capable of generating more complex noise compared to Figure 1, and it eliminates the regularity of noise through the use of random numbers. Furthermore, in the FPGA used for the evaluation in this paper, only two DCMs were available due to wiring constraints. However, as the number of available DCMs increases, it becomes possible to generate more complex waveforms of noise.

Considering the differences from Figure 1, we examine the area overhead of the proposed method. for both designs, the noise injector and PRNG are required, the only difference is the replacement of the noise generator in Figure 1 with the XOR tree. In general, a multiplexer is implemented by XNOR-ing the decoded selection signals and OR-ing them together. It is believed that there are no significant changes in circuit size in the proposed method since it also involves XOR-ing after XOR for consolidation.

IV. Evaluation

A. *Experimental Setup*

For our evaluation, we used the CW308 UFO Target Board and CW308T-S6LX9 from NewAE Technology Inc.. The CW308 UFO Target Board is a general-purpose power supply

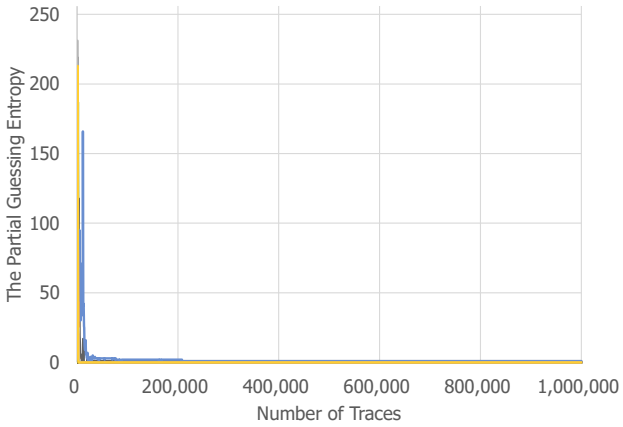

Fig. 3 The Partial Guessing Entropy of CNS

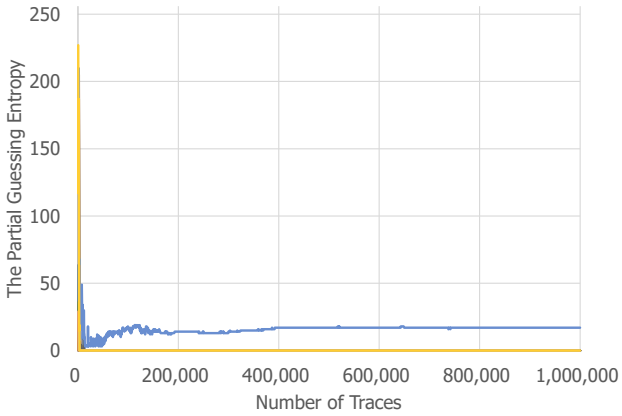

Fig. 4 The Partial Guessing Entropy of proposed method

board with probe points for measuring shunt resistor voltages. The CW308T-S6LX9 is a board equipped with Xilinx Inc. XC6SLX9-2TQG144C FPGA, and it is connected to the CW308 UFO Target Board for power supply. We design implementations of the circuits in Figure 1 and Figure 2 as 128-bit AES on this CW308T-S6LX9 respectively. The frequencies of each DCM are set to 2, 3, 4, 5 multiplication factors in CNS, while the proposed method uses 2, 3 multiplication factors. This setting is based on the knowledge from the paper of CNS, which indicated that higher multiplication settings did not result in better tamper-resistance. The implemented 128-bit AES was modified from the open-source code provided by Project Vault [9].

We utilized an open-source computer program as CPA attack created by O'Flynn et.al [10] and collected a total of 1,000,000 traces for input to the program. The program predicts 128-bit round keys in 8-bit partial round key increments, and it leaks the AES secret key when all 16 partial round key predictions are successful.

Implementation area was evaluated using the placement and routing results from Xilinx ISE 14.7 reports. Unlike ASICs, design on FPGAs occupy existing resources in the form of provided registers and lookup tables (LUTs) to reconfigure the circuit. Therefore, in the evaluation of this paper, the estimation of circuit size is based on how many registers and LUTs were used in the synthesis and placement and routing results for the entire implemented AES. Additionally, in the evaluation of this paper, the possibility of varying critical path delays with changes in implementation area was considered, so the operating frequency is also presented alongside the area evaluation. Furthermore, the logic synthesis and placement and routing in ISE 14.7 were performed without setting delay constraints, using default conditions.

B. *Tamper-resistance*

Figures 3 and 4 show the attack results for CNS and the proposed method, respectively. The vertical axis in the figures represents Partial Guessing Entropy (PGE). CPA infers partial round keys in 8-bit increments using correlation coefficients. There are 256 possible values for an 8-bit key, with one correct partial round key among them. CPA calculates correlation coefficients for all 256 partial round key candidates and ranks them by positive correlation values, considering the partial round key candidate with the highest positive correlation as the correct guess. PGE is an indicator of how the correct partial round key is ranked in the analysis, with the lower end of the vertical axis being the most vulnerable and higher values indicating stronger resistance for side-channel attacks.

Both Figures 3 and 4 have 16 legends overlapping, making it difficult to distinguish between them, but it is evident that the proposed method in Figure 4 offers better tamper-resistance than CNS in Figure 3. CNS shows that, with 200,000 traces input, the PGE for almost all correct partial round keys converges to around 0, indicating that CPA can predict nearly all partial round keys correctly. On the other hand, the proposed method has some partial round keys where PGE does not converge to 0 but remains around 20. These results are in line with our claim that by eliminating the regularity of the injected noise, the traces are modified, and CPA cannot calculate the correct correlation coefficients.

Additionally, it should be noted that while CNS uses four DCMs, the proposed method only uses two DCMs due to FPGA wiring constraints. This is an unfair comparison, and it's important to consider that the proposed method has a disadvantageous evaluation in terms of the number of sources for high-frequency noise. Even with this disadvantageous evaluation, the superiority of proposed method over CNS in terms of tamper-resistance further strengthens its advantage. Furthermore, as discussed in Section III, the modification of the noise generator in the proposed method is novel, and it has been considered that there are no significant changes in circuit size. The area evaluation, as described in the next subsection, concludes that the proposed method, which achieves tamper-resistance without significant changes in required resources, can be easily substituted for CNS.

C. *Area and delay overhead*

Table I shows area and delay estimation results. In the area evaluation, the proposed method was implemented with a significantly smaller implementation area compared to CNS.

TABLE I
Area and Delay Estimation Results

	# of Slice Registers	# of Slice LUT	Frequency (MHz)
CNS	957	3097	82.257
Proposed	919(-3.9%)	3029(-2.1%)	81.466(-0.9%)

An observed reduction of 3.9% in the number of registers and 2.1% in the number of LUTs is noted. This reduction is attributed to the fact that the proposed method's XOR tree requires fewer circuit resources compared to the 4-1 multiplexer used in CNS. While it was expected that both would result in similar circuit sizes in our discussion, the reason they didn't can be attributed to the fact that the CNS evaluated in this paper used 4 DCMs and had 4 sources of high-frequency noise, whereas the proposed method was restricted to using only 2 DCMs by wiring constrain, leading to a different circuit size. Taking this into consideration, the proposed method, which achieves higher tamper resistance while requiring a smaller circuit size, can be concluded to be a superior and cost-effective solution for FPGA-based side-channel attack mitigation compared to CNS.

On the other hand, while the change in critical path delay is small, the proposed method has a longer critical path delay and a lower operating frequency compared to CNS. The exact reason for this is not certain, but it is likely due to optimization errors in logic synthesis and placement and routing, as it is unlikely that it is caused by a high number of serial connections in the logic.

V. Conclusions

In this paper, we have improved the tamper-resistant design with reduced area overhead utilizing the high-frequency noises derived from DCMs equipped by FPGAs, as proposed by us. Additionally, by introducing an XOR tree, we have achieved further enhancement in tamper-resistance. Furthermore, we have conducted an evaluation of area overhead in FPGAs and confirmed that compared to related work, we can attain excellent tamper-resistance without an increase in area overhead.

ACKNOWLEDGMENT

This work is supported by JSPS KAKENHI Grant Number 20K11823 and 20H00590.

References

[1] T. Ukezono, and Y. Koyanagi , ”Effect of High Frequency Noise Using DCMs in FPGA on Power Analysis Attack,” Proc. of 2023 International Symposium on Communications and Information Technologies (ISCIT2023), pp.430--435, Oct. 2023.

[2] E. Brier, C. Clavier, and F. Olivier, “Correlation Power Analysis with A Leakage Model,” Proc. of International Workshop on Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science, Vol. 3156, Springer, pp. 16--29, 2004.

[3] K. Tiri and I. Verbauwhede, “A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation,” Proc. of Design, Automation and Test in Europe Conference and Exhibition (DATE2004), pp. 246--251, Feb. 2004.

[4] K. Tiri et. al., “Prototype IC with WDDL and Differential Routing – DPA Resistance Assessment,” Proc. of The annual Conference on Cryptographic Hardware and Embedded Systems 2020 (CHES 2020), pp. 354-365, 2005.

[5] T. Popp and S. Mangard, “Masked Dual-Rail Pre-charge Logic: DPA-Resistance Without Routing Constraints,” CHES 2005, LNCS 3659, pp.172--186, Springer, 2005.

[6] E. Trichina, “Combinational Logic Design for AES SubByte Transformation on Masked Data,” Cryptology ePrint Archive, 2003/236, 2003.

[7] S. Nikova, C. Rechberger and V. Rijmen “Threshold Implementations Against Side-Channel Attacks and Glitches,” ICICS 2006, LNCS 4307, pp.529--545, Springer, 2006.

[8] Y. Koyanagi and T. Ukezono, "A Cost-sensitive and Simple Masking Design for Side-channels," Proc. of 2023 IEEE Region 10 Technical Conference (TENCON 2023), pp.731--736, Oct. 2023.

[9] C. O’Flynn, “Side-Channel Power Analysis of AES Core in Project Vault,” https://colinoflynn.com/2015/05/side-channel-power-analysis-of-aes-core-in-project-vault/ [Accessed on Nov. 7, 2023].

[10] C. O’Flynn, Z. D. Chen, “ChipWhisperer: An Open-Source Platform for Hardware Embedded Security Research,” Proc. of Constructive Side-Channel Analysis and Secure Design (COSADE2014), Lecture Notes in Computer Science, vol. 8622, Springer, pp.243--260, 2014.