A Cost-sensitive and Simple Masking Design for Side-channels

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— **Conventional countermeasures against Power Analysis Attacks ignore area overhead for implementation since it only pursuit perfect tamper-resistance. While the countermeasures achieve high tamper-resistance, unacceptable area overhead is required. Thus, the design of the countermeasures cannot be applied for IoT edge devices, which are provided as cheaper products. In this paper, first, we show the unacceptable area overhead by the conventional countermeasures, then propose a lightweight and fundamental VLSI design method against Power Analysis Attack. Masked Wave Flip-Flop (MW-FF), proposed design method achieves higher tamper-resistance than Wave Dynamic Differential Logic (WDDL) that is one of the conventional countermeasures with small and acceptable area overhead. Our evaluations show that MW-FF requires only 12.51% and 5.89% of are overhead in FPGA and ASIC respectively, which is 114.03% and 21.82% saved comparing with WDDL.**

Keywords— Side-Channel Attack, Power Analysis Attack, Random Value

I. INTRODUCTION

The number of IoT edge devices has increased in recent years, posing a risk of information leakages via Side-Channel Attacks. Side-Channel Attack guesses internal information by observing and analyzing physical changes (e.g., processing times, power consumption, and electromagnetic waves). The threat of a Side-Channel Attack for IoT edge devices is the leakage of encryption keys used for communication. If the encryption keys are compromised, the information communicated by IoT edge devices is vulnerable to interception and tampering. This causes a decrease in reliance on services created by IoT.

Power Analysis Attack (PAA) is a kind of Side-Channel Attack and obtains confidential information in a chip by observing and analyzing the change in power consumption as side-channel while processing. There are two representative categories of PAAs. One is Simple Power Analysis (SPA) [1]. Using human eyes, SPA guesses the confidential information by investigating the characteristics from shapes of waveforms of power consumption which are obtained from oscilloscopes. In this paper, the waveforms are referred to as traces. SPA needs to capture the power consumption in individual processing steps of the algorithm implemented in a chip and is required that the noise of traces is relatively low. It is difficult to attack block ciphers such as AES [2] that are lightweight and highspeed because of difficulty of analyzing by human eyes. With the recent establishment of machine learning methods for classifying the appearance of waveforms, it can be assumed that SPA attacks will become an increasing threat [3].

The other category is statistical attack methods. Kocher et al. proposed a method, Differential Power Analysis (DPA) [1] of extracting only the change in power consumption due to secret information by calculating the difference between all traces and their average value, while minimizing the effects of measurement errors and noise by calculating the average value of large number of traces. Correlation Power Analysis (CPA) [4] has the same approach as DPA, but with the sophisticated idea of reducing the number of traces for analysis than DPA. DPA focuses on a bit of transition on input to a combinational circuit. When a specific 1-bit transition of input occurs, DPA analyzes the difference in power consumption. DPA can be used for AES attacks since it does not require knowledge of detailed cryptographic algorithms and its implementations, however it requires many traces. CPA focuses on multi-bit transitions and analyzes the correlation between predicted confidential information using traces reduced by the same Hamming distance, requiring fewer traces, and analyzing time than DPA. In this paper, we attack on AES by CPA as an evaluation of our proposal.

Many countermeasure circuits have been proposed to prevent PAAs. For example, Wave Dynamic Differential Logic (WDDL) [5][6], Masked Dual-Rail Pre-charge (MDPL) [7], Masked AND Operation (MAO) [8] and Threshold Implementation (TI) [9] are the representative countermeasure designs against PAA. We describe the details of these related work in the next section. While these countermeasure designs improve tamper resistance, they ignore the trade-offs involved in pursuing only perfect protection. For cost-sensitive devices such as IoT edge devices, the increase in implementation area on ASICs, which is the main cause of yield loss, is a major problem. However, conventional countermeasures are so large that the implementation area is unacceptably large for IoT edge devices. Preliminary evaluations for conventional countermeasures and discussion are presented in Section III. Tamper resistance is not a binary argument of perfect or not perfect. For example, in the PAAs, the greater number of traces required for leakage, the progressively more tamper-resistant it becomes. In this paper we focus on reducing the overhead of implementation area instead of aiming for perfect protection.

Our objective is to reduce the area of tamper-resistant designs. MW-FF, our proposed design improves tamper-resistance same as conventional countermeasures by adding a small circuit handling random values to original combinational circuit with no modification. In this paper, we evaluate MW-FF in the tamper-resistance and in the implementation area for ASICs and FPGAs. In addition, in the evaluation of this paper, AES is used as an example, however MW-FF can be applied to other ciphers since its design is not related to any specific application or algorithm, and it can be

979-8-3503-0219-6/23/$31.00 ©2023 IEEE

used in conjunction with conventional countermeasures which modifies the combinational circuit itself.

In summary, the main contributions of our work are:

- Our proposal focuses not only on achieving higher tamper-resistance work but also on area saving instead of aiming for perfect protection.
- Although AES was evaluated as an example in this paper, the proposed circuit can be widely used and can coexist with existing countermeasures if further improvement of tamper resistance is needed.

In this section, we described the background of our study. In Section II, we explain related work such as WDDL, MDPL, MAO and TI described above, and in Section III, we show the preliminary evaluation of related work in terms of implementation area. The proposed design is shown in Section IV, and the evaluation of our proposal is shown in Section V. Finally, the paper is concluded in the last section.

II. Related Work

Many countermeasure circuits against PAA exist. Wave Dynamic Differential Logic (WDDL) [5][6], Masked Dual-Rail Pre-charge (MDPL) [7], Masked AND Operation (MAO) [8] and Threshold Implementation (TI) [9] are the representative work.

The PAA infers the input value from the energy consumption by the combinational circuit and its output value. This is since there is a certain law in the energy consumption when the transistors inside the combinational circuit switch. Standard CMOS consumes energy for switching when the output value changes. In a logic circuit, the output value changes when the input value changes, and if the bits of the previous input value and the current input value are inverted, the output might change, and energy might be consumed. PAA can infer the input bit sequence to the combinational circuit by back calculating the input bits from the power consumption model and actual observations of power consumption. In well-known attacks to the AES [2], the input value to combinational circuits can be guessed to leak the information of the round key that is required to back-calculate the common key, which is internally handled in a secret. In the case of AES, the target combinational circuit of the PAA is the S-box, which is the conversion process of nonlinear calculation.

If the combinational circuit consumes power in the same consumption whether the bit sequences success the same input value or not, then the input bit sequences cannot be inferred from the power consumption. WDDL is a countermeasure that modifies the target combinational circuit to achieve the power consumption described above. WDDL duplicates the original logic circuit and drives the two logic circuits simultaneously as separate circuits. For this reason, WDDL is also called dual-rail logic. One of the duplicated circuits is redesigned to be complementary to the original circuit in terms of power consumption. In addition, to achieve this complementarity for power consumption, WDDL must modify the state and data-path control to insert pre-charge cycles to between original cycles. This pre-charge cycle is inserted to reset all inputs to the combinational circuit to zeros, and the duplicated circuits are designed with the calculation that both will have the same power consumption at the bit transition from the preceding zero. Naturally, WDDL requires twice the number of logic gates due to the dual-rail design, making the area overhead significant.

MDPL is one of the variants of dual-rail logic, a sophisticated design developed from the fact that WDDL cannot perfectly prevent data leakage from power consumption. In addition to the complementarity of power consumption of dual-rail logic, the effect of the masking by pseudo-random numbers is added to the side channel, power consumption, to make the countermeasure more secure. MDPL has the same area overhead of the dual-rail design as WDDL, the additional area overhead of the sophisticated side channel masked design due to random number generator and masking.

MAO is a design that focuses on all AND gates in the target combinational circuit and does not allow the AND gates to consume power using the original input to the AND gate. For this purpose, MAO must add a circuit for encryption using XOR with random numbers before the input of all AND gates and a decryption circuit after the output in series connection. It is mathematically guaranteed that the result of AND operation on the encrypted value after decryption and the result of original AND operation on the original value will have the same value. It can be said that MAO is a PAA countermeasure design that applies concept of secure computation [10]. Depending on the number of AND gates in the target combinational circuit, it is easy to imagine that the area overhead of adding encryption and decryption circuits to every AND gate is not small.

TI is a countermeasure that exploits secret sharing [11] techniques, hides the true data being processed in a chip, by using random numbers to covertly distribute the input values. This prevents processing on the true data in the combinational circuit making it difficult to infer the input value from its power consumption. The concept of hiding the true data in processing is like that of MAO. Secret sharing is a process with a very large computational overhead, and the area overhead of the computational logic to apply it to data during the processing inside VLSIs is too large to be ignored.

In the next section, we evaluate the area overhead of these PAA countermeasures, discuss the magnitude of the impact, and claim the advantage of our proposed method, which is cost-sensitive.

III. Preliminary Evaluation

In this section, we show the evaluation results of implementation area for related work, WDDL, MAO, MDPL and TI, and discuss the overheads. The RTLs of related work that is released from web site [12] of Information and Physical Security Research Group of Yokohama National University were used for our evaluation. In these designs that are developed by the research of [13] for the conversion process with nonlinear calculation, 16 S-boxes are implemented in parallel. Since the S-boxes occupy the largest area in entire AES implementation, the area of the S-boxes is only synthesized in our preliminary evaluation. The implementation area of related work is evaluated for FPGAs and ASICs. Synthesis tools, Synopsys Design Complier and Xilinx ISE 14.7 were used to our evaluation for ASICs and FPGAs respectively. In FPGA evaluation, we specified the target device as Xilinx Spartan6 XC6SLX9, and synthesized the RTLs with default constraints. The synthesis reports of ISE 14.7 are used to confirm the number of Slice LUTs, which was used as implementation area. Whereas in ASIC evaluation, Synopsys Design Compiler was used for logic

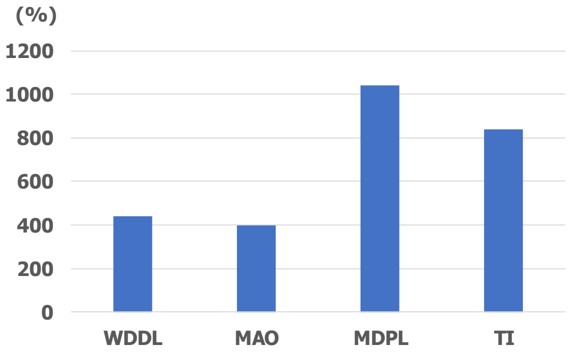

Figure 1 Comparison of utilization overheads of required LUTs in FPGA implementation among related work normalized by no-countermeasure

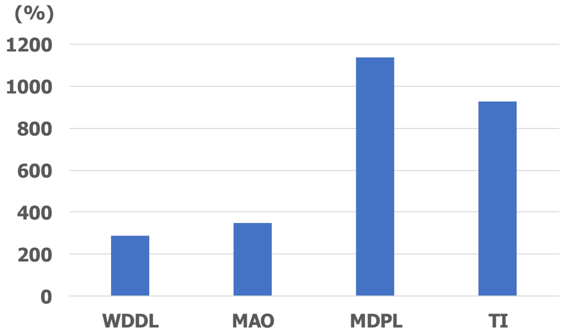

Figure 2 Comparison of area overheads of related work in ASIC implementation normalized by no-countermeasure

synthesis with Silvaco's 45 nm open-cell library [14]. The synthesis options were set to defaults, and the implementation area and critical path delay were obtained from a synthesis report of Design Compiler.

Figures 1 and 2 show the increase in implementation area of FPGAs and ASICs. The vertical axis indicates the rate of increase normalized by no-countermeasure circuit. In both figures, MDPL has the largest overhead which requires about 1000% and 1100% of implementation area in FPGAs and ASICs evaluation respectively. Comparing, WDDL and MAO require only third to half implementation area of MDPL design, which are the smallest area overheads in the related work. On the other hand, the delay of ASIC shown in Figure 3 indicates that MAO engages more than 1 ns of time than WDDL. Thus, WDDL showed the best evaluation result in FPGAs or ASICs implementation area and delay of ASIC. It should be remembered here that, as discussed in Section I, these conventional countermeasures are designed for achieving perfect tamper resistance. In a realistic VLSI design, there is no way to tolerate such a severe overhead that the area trade-off for tamper resistance exceeds 1000%, and it is unlikely that these countermeasures would be adopted unless the system is a special system that handles highly confidential information.

Regarding on implementation area, WDDL and MAO required at least 300% of overhead, though they showed the smallest implementation area. Thus, even related work with relatively small overhead requires a huge amount of implementation area for the trade-off of tamper-resistance. Since the chip cost is determined by the yield, related work requires a large amount of cost to implement. Although the related work represents relatively high tamper-resistance, the reduction of implementation area is more significant for realistic cost-sensitive devices like IoT devices rather than higher tamper-resistance. Therefore, we propose an area-saving countermeasure design. In this paper, WDDL is used as a criterion of our evaluation, since it showed the lowest area overhead and delay in the preliminary evaluation.

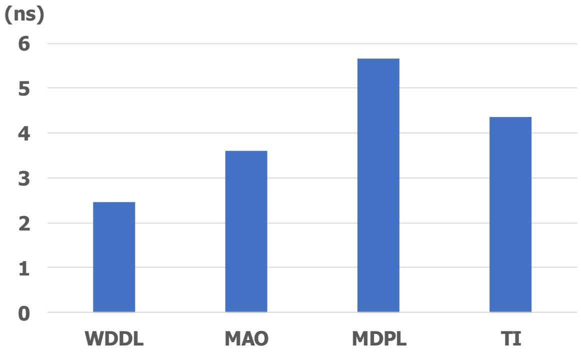

Figure 3 Comparison of delay of related work in ASIC implementation

IV. MASKED WAVE FLIP-FLOP

We considered leakage from the power consumption in VLSI from various perspectives of related work to achieve a tamper-resistant design with extremely lightweight. One of the viewpoints is the hiding method represented by dual-rail designs such as WDDL. The essence of the dual-rail design is to mask the power generated by the processing of attack target with the power generated by another. The dual-rail design has the potential to generate the masking power consumption at the same time exactly by adding circuitry, and to eliminate leakage completely within the power consumption, however it requires additional circuit area. In practice, even if complete masking is logically possible, perfect tamper resistance has not been achieved since it is difficult to achieve completely symmetrical power consumption at the physical design, especially in the layout level design. Particularly in the case of FPGAs, the layout design is a combination of prepared resources, and we have no control over the symmetry-aware design at all. We abandon the simultaneity to save area and focus on bit transitions instead. As described in Section II, standard CMOS has the property of consuming power when bit transitions occur on inputs to combinational circuits. We propose an additional circuit that does not mask the information in the power consumption, but rather disturbs this bit transition and transforms the information in the power consumption.

The other viewpoint is randomness that are equipped by MDPL, MAO and TI. The essence of these related work is to exploit the mathematical properties of information theory to transform the information to be processed in combinational circuits with the functions intact. Once this law of transformation of information is known to an attacker from the outside, these countermeasures will be useless. For this reason, these measures use random numbers to hide the law. Since the circuitry for the transformation of information is too large to be cost-effective, we decided to take advantage of only the random number property, which is difficult to guess from the outside. Our proposed design shown below combines the above two characteristics described above,

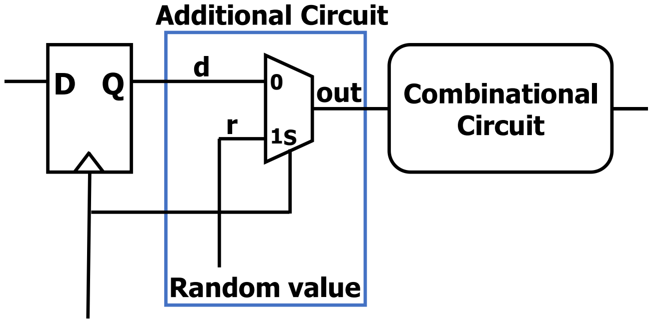

Figure 4 Structure of proposed Masked Wave Flip-Flop (MW-FF)

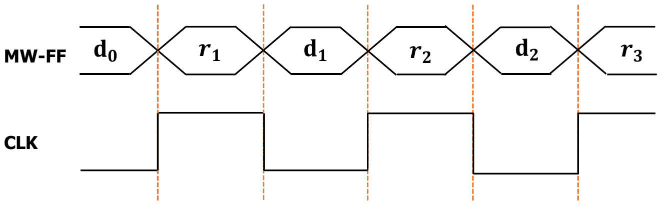

Figure 5 Disturbing bit transition by proposed Masked Wave Flip-Flop (MW-FF) using randomness

disturbing bit transition and randomness, to achieve tamper resistance by the lowest possible cost.

Our proposed design is called Masked Wave Flip-Flop (MW-FF). We show our proposed design in Figure 4. CLK signal selects the inputs to the multiplexor, which are the outputs of D-FF *d* and random value *r*. Comparing with related work such as WDDL, our proposal is placed to output of the D-FFs before input of S-boxes, while the related work has to redesign the S-boxes. Therefore, our proposed circuit and related work can be applied simultaneously, and our proposal does not attempt to compare tamper-resistance with the related work. Figure 5 shows the timing chart of our proposed design. Determining the law of bit transition disrupted by countermeasure is difficult since a random value is inputted while the clock signal rises.

Since MW-FF requires pseudo-random number generator, the increase of implementation area should be considered. The primary goal of our proposal is both achieving higher tamper resistance and area saving. Therefore, the pseudo-random number generator should also be as small as possible. We exploit an LFSR-compliant fast random number generator [15] to provide the signals that are represented as *r* in Figure 4. An LFSR (Linear Feedback Shift Register) is a shift register in which inputs are provided by the XOR from the output signal of own register. The most commonly linear bit function is XOR. In an LFSR, the input bits are frequently updated by the XOR of some shifts register bits. As a simple cyclic shift register, the LFSR can be configured with only D-FFs with initialization and a few XOR gates, resulting in a reduced implementation area and low delay due to dedicated circuitry at the expense of pseudo-random number accuracy. Therefore, to reduce the disadvantage of area increase as much as possible, MW-FF exploits the LFSR. In our evaluation, we implemented a 128-bit LFSR to fit the input bit width of the 16 parallel S-boxes.

V. EVALUATION

A. Experimetal Setup

The evaluation in this paper shows a result of PAA by CPA to evaluate tamper resistance for MW-FF and result of the implementation area in FPGAs and ASICs. WDDL and no-countermeasure are also evaluated as a criterion for performance of MW-FF. As described in Section IV, MW-FF does not require redesign for the combinational circuit and can be combined with conventional countermeasures such as WDDL. Therefore, since MW-FF is proposed for tamper resistance that can be achieved by very low cost, we exploit the WDDL which had the lowest overhead in the preliminary evaluation of Section II as a criterion to evaluate the degree to which MW-FF can achieve tamper resistance on its own, rather than in competition with WDDL.

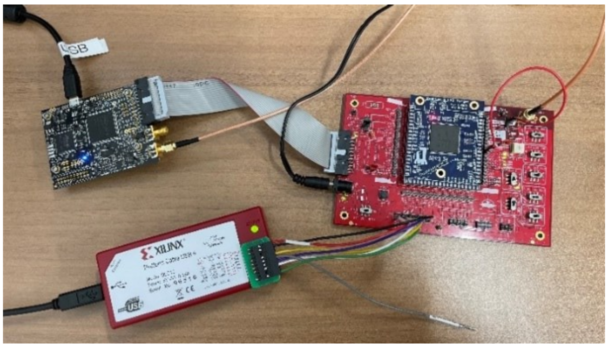

Figure 6 Experimental environment for collecting traces that are used to power analysis attack

We had chosen 128-bit AES [2] as the target of PAA, which is designed with a dedicated circuit. RTLs of AES Google Project Vault [16] were downloaded and synthesized as the target AES implementation. The countermeasures to be evaluated were applied to the S-boxes in the RTLs. In the evaluation of WDDL, RTL of S-box prepared by AES Google Project Vault is replaced to S-box designed by WDDL obtained from web site [12] of Information and Physical Security Research Group of Yokohama National University. In the evaluation of no-countermeasure, we designed the composite S-box as a combinational circuit without any countermeasures and replaced it to the preexisting S-box. In the evaluation of MW-FF, our proposal was applied by replacing the D-FF before S-box in AES Google Project Vault to MW-FF. We attack the countermeasure designs, MW-FF, WDDL and no-countermeasure by CPA that is provided in ChipWhisperer tool set [17].

Regarding the implementation area and delay, we evaluate the modified RTLs of AES Google Project Vault in the same condition presented in Section III for FPGAs and ASICs respectively.

Figure 6 shows our experimental environment. The red board is the power supply board for the daughter board located in the center of red board, and it has probe points at the right upper corner for measuring the voltage across the power supply circuit and equip a shunt resistor to obtain traces. The daughter board, blue board, equips an FPGA on which the AES circuit is configured. The blackboard is the USB-controlled oscilloscope. Furthermore, the blackboard has an UART interface through the 20-pins flat cable that sends plain text to the FPGA, allowing traces to be collected synchronizing with the busy signal of AES core. The blackboard can be controlled by PCs via USB connection and can be programmed in Python language to capture waveforms at preferred timing and transmit plain text. We collected

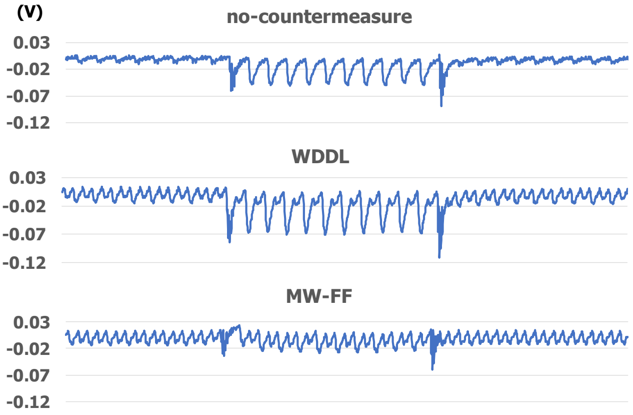

Figure 7 Comparison of the shapes of power consumption waveforms (traces)

traces of the final round (16th round) of AES since the structure of AES simplifies the process and makes the keys easy to infer. In our evaluations, we captured 50,000 traces.

After collecting all the traces, we used CPA [4] provided by the ChipWhisperer tool set to attack them. If the attack is successful, the 16 bytes (128-bit) round key of the final round in which the trace was captured can be deduced. Since the round key can be used to find the secret key by back-calculation of key generation algorithm, finally, the secret key of AES is leaked.

B. Shapes of traces

Figure 7 shows one of the traces obtained by an oscilloscope that is added to our experimental environment for each countermeasure. The vertical axis of the figure is the shunt resistor voltage, and the horizontal axis is the time lapse. The shape of the waveforms has changed in both WDDL and MW-FF compared to no-countermeasures. While the no-countermeasure curve is clean and periodic, the WDDL waveform is distorted and has a larger amplitude. The MW-FF flattened the overall waveform, and the overall voltage can be seen to shift upward. The results show that MW-FF eliminates the characteristics of the no-countermeasure waveform with a difference that is visible to the human eyes.

C. Tamper-resistance

Figure 8 shows tamper-resistance against CPA. The number of correct partial round keys is indicated on the vertical axis, and the number of traces is indicated on the horizontal axis. The length of each correct partial round key is 8-bit, and the entire round key is 128-bit. If all 16 correct partial round keys are leaked, the attack on AES is successful, and then the AES is defenseless against wiretapping and tampering. And if these 16 correct round keys leak in lower numbers of traces, the design shows lower tamper-resistance against CPA. Therefore, the farther design locates in the bottom right, the higher tamper-resistance it shows. It is known that WDDL which has relatively high tamper-resistance also leaks each of 16 partial round keys [18]. Therefore, in this paper, we focus on the beginning of 50,000 traces of the analysis.

In Figure 8, it is shown that the no-countermeasure circuit leaked all 16 correct partial round keys in approximately 4,000 traces, whereas WDDL leaked 15 correct partial round keys in approximately 50,000 traces. On the other hand, the MW-FF, our proposed design clearly shows better tamper resistance than WDDL. The red curve is gradual up to 40,000 traces, indicating that the number of correct partial round keys is significantly lower than in the WDDL, yellow line, as the analysis traces increase. This clearly shows that MW-FF has higher tamper resistance than WDDL up to 40,000 traces. After the 40,000 traces, MW-FF reaches 15 correct partial round keys, same as WDDL. MW-FF differs from WDDL in that it touches 16 only momentarily at the end of the analysis. However, this does not imply convergence to 16. After 40,000 traces, we can conclude that MW-FF has almost the same tamper resistance as WDDL. Again, since MW-FF is a method that can coexist with WDDL, a comparison between the two is not very meaningful. However, from these results, we can conclude that MW-FF has enough tamper resistance that exceeds that of WDDL on its own, and that its application to IoT edge devices is also meaningful if it can be implemented in a sufficiently small area. The next subsection evaluates the implementation area.

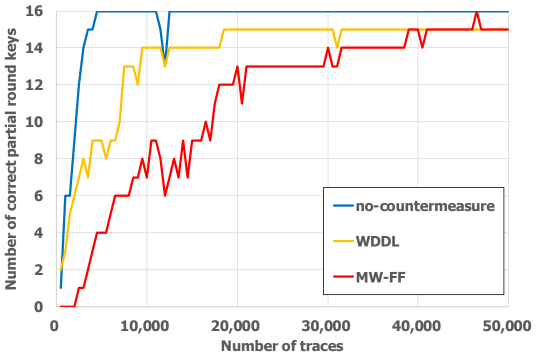

Figure 8 Tamper-resistance against Correlation Power Analysis (CPA)

D. Area result

The main objective of our proposal is to save the implementation area for reasonable tamper resistance. In this paper, the resource utilization of FPGAs in the environment shown in Figure 6, and the area evaluation if the same RTL is implemented in ASICs is shown for detailed area evaluation.

The WDDL requires twice the implementation area of a no-countermeasure circuit, whereas the MW-FF results in a 112.5% ratio of LUTs. This indicates that MW-FF requires only a 12.5% increase in the implementation area to show better tamper resistance than W-FF. In terms of the number of registers required, MW-FF has increased the number of resources for the random number generator, but this only represents an area overhead of 11.58% of the total, a reasonable increase in storage elements when the area overhead for the number of additional registers for WDDL control is 14.58%.

In terms of clock cycles in FPGA implementation, a 14.82% reduction in speed was observed. This is thought to be due to the effect of the pseudo-random number addition generator on the critical path delay. However, this is a very minor slowdown when compared with the 92.22% observed for WDDL.

The implementation area result for ASICs is shown in Table 2. MW-FF could be realized with an area overhead of 5.89% in ASIC implementation. This is sufficiently small compared with the 27.71% overhead of WDDL. On the other

TABLE I. UTILIZATION OVERHEADS AND CLOCK PERIODS IN FPGA IMPLEMENTATION

	#of registers	*#of LUTs*	*Clock period (ns)*
no-countermeasure	933	2430	12.284
WDDL	1069 (+14.58%)	5505 (+126.54%)	23.613
MW-FF	1041 (+11.58%)	2734 (+12.51%)	14.105

TABLE II. AREA OVERHEADS AND CRITICAL PATH DELAY IN ASIC IMPLEMENTATION

	Total cell area (um^2)	*Critical path delay (ns)*
no-countermeasure	29009.16	4.06
WDDL	37048.74 (+27.71%)	3.95
MW-FF	30718.21 (+5.89%)	3.81

hand, the critical path delay was within the error range due to synthesis optimization for all implementations (e.g., WDDL and MW-FF). These findings confirm that none of the countermeasure circuits have a significant impact on the ASIC's delay performance.

The results of the preceding analysis show that the MW-FF proposed in this paper can be realized with a reasonable and acceptable area overhead for both FPGA and ASIC implementations. Furthermore, in terms of tamper resistance, MW-FF is effective over WDDL, indicating that MW-FF is an effective countermeasure for cost-sensitive devices, including IoT edge devices. In addition, we evaluated MW-FF by applying to AES dedicated circuit in this paper. Since our proposed circuit can be widely used, MW-FF also can be applied to other cryptographic dedicated circuit. Furthermore, it can be combined with the other countermeasure design.

VI. CONCLUSIONS

Inexpensive tamper-resistant VLSI designs are required for IoT edge devices. Conventional countermeasures were shown to have unacceptable overhead more than 1000% in our preliminary evaluations. Therefore, our proposal does not aim to achieve a perfect tamper-resistance but a lightweight countermeasure. Our proposed design method, MW-FF improves tamper-resistance without any modification for combinational circuits. The additional circuit of MW-FF is small enough, since it replaces only the existing D-FFs. Our evaluations show that MW-FF requires only 12.51% and 5.89% of area overhead in FPGA and ASIC respectively, while 126.54% and 27.71% of increase is needed for WDDL that is a criterion of this paper. More importantly, our evaluation of Power Analysis Attack for AES shows that MW-FF has higher tamper-resistance than WDDL with lower area overhead.

In addition, Since MW-FF can be applied simply by replacing, the design cost is low enough. Therefore, MW-FF can be easily and immediately introduced to the existing VLSI designs without fear of a large increase in overhead. MW-FF is a versatile VLSI design method that is not dependent on specific applications such as AES and can be applied to various of VLSI designs and combined with conventional countermeasures.

ACKNOWLEDGMENT

This work is supported by JSPS KAKENHI Grant Number 20K11823 and 20H00590. It is also supported by VLSI Design and Education Center (VDEC), the University of Tokyo in collaboration with Synopsys, Inc.

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Proc. of International Cryptology Conference (CRYPO1999), Lecture Notes in Computer Science, Vol. 1666, Springer, pp. 388–397, Aug. 1999.

[2] T. Jamil, "The Rijndael algorithm," IEEE Potentials,Vol. 23, Issue 2, pp.36-38, 2004.

[3] G. Zaid, L. Bossuet, A. Habrard, A. Venelli, "Methodology for Efficient CNN Architectures in Profiling Attack," IACR Trans. Cryptogr. Hardw. Embed. Syst., 2020(1):1–36, 2020.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

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

[10] A. C. Yao, "How to generate and exchange secrets," FOCS'86, pp.162-167 , 1986.

[11] A.Shamir, "How to share a secret," Communications of the ACM, vol.22, no.11, pp.612–613, 1979.

[12] Information and Physical Security Research Group, "Cryptographic Circuits with Logic Level Countermeasures against DPA," Yokohama National University, https://ipsr.ynu.ac.jp/circuit/index.html [Accessed on March 16, 2023].

[13] M. Saeki, et al., "A Design Methodology for a DPA Resistant Cryptographic LSI with RSL Techniques," CHES 2009, LNCS 5747, pp. 189-204, Sep. 2009.

[14] Silvaco Inc., "PDK 45nm Open Cell Library,", https://si2.org/open-cell-library/ [Accessed on March 16, 2023]

[15] B. Mohammed, "Hardware Implementation of Pseudo Random NumberGenerator Based on Chaotic Iteration", Ph.D. Dissertation, University Bourgogne Franche-Comte, Jan. 2018.

[16] 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 March 4, 2023].

[17] 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.

[18] Y. Li, K. Ohta, K. Sakiyama, "Revisit fault sensitivity analysis on WDDL-AES," Proc. of 2011 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST 2011), pp.148-153, 2011