International Journal of Networking and Computing – www.ijnc.org, ISSN 2185-2847
Volume 14, Number 2, pages 108–122, July 2024

# A Light-weight Random Number Generation for Tamper-resistant AES Circuit

Tomoaki Ukezono
Fukuoka University, Dept. of EECS, 8-19-1, Nanakuma, Jhonan-ku
Fukuoka City, Fukuoka, 814-0180, Japan

Yui Koyanagi
Fukuoka University, Graduate School Engineering, 8-19-1, Nanakuma, Jhonan-ku
Fukuoka City, Fukuoka, 814-0180, Japan

Received: February 15, 2024
Revised: May 3, 2024
Accepted: June 1, 2024
Communicated by Takashi Yokota

**Abstract**

Various countermeasures have been proposed to reduce the characteristics that leak cryptographic keys from side-channel information such as power consumption and electromagnetic radiation. However, in the case of cryptographic processing with dedicated circuits, introducing high-quality random number generators lead to an increase in area cost of circuit implementation. Focusing on the parallel S-box implementation of AES, this paper proposes a novel circuit design that achieves improved tamper resistance while mitigating the increase in circuit area by reusing the existent S-boxes temporally and spatially.

*Keywords:* AES, S-box, Power Analysis Attack, Tamper-resistance, Random Value

## 1 Introduction

In recent years, IoT edge devices have been spreading, and there are expectations for the collection of big data for AI and the creation of novel services through the devices. IoT edge devices are small computers equipped with sensors and actuators that are connected to the internet, enabling information collecting and collaborative actions through the internet. IoT edge devices are produced in large quantities and operated through decentralization. As a result, it is essential for them to be producible at the lowest possible cost while encompassing necessary and sufficient functionalities.

In general, IoT edge devices are equipped with SoC chips to fulfill the specific functionalities required individually. Since wireless communication capability over the Internet is essential for IoT edge devices, the computation of AES, which is the standard encryption technology on the Internet, is required. AES processing, which directly affects communication speed, is commonly handled by dedicated circuit designs that leverage the high parallelism of the AES algorithm to increase energy efficiency with low-frequency-clocking, rather than processing with high-frequency-clocking CPUs that lead to higher chip-manufacturing cost. With the increase in implementation area associated with parallelized AES implementations, it may occupy on the chip area of SoCs larger.

However, in recent SoC implementations, the proportion of hierarchical cache memory in the occupied area of dies is dominantly large. Even if AES, which is crucial for IoT communication, is

parallelized, it remains relatively small in terms of die area compared to the benefits of achieving fast Internet communication at low clock frequency. These benefits outweigh the drawbacks of increased area occupancy due to parallelization. As evidence of our assertion, open-source SoCs[12][16][15][25] available today include external modules and their interfaces designed for parallel implementation, which are necessary for communication speed.

On the other hand, security threats related to the IoT edge devices are concerned. Due to the nature of numerous IoT edge devices making physical central management difficult, there is an increased likelihood that attackers can make contact with the devices physically without even involving the internet. If an attacker is able to contact physically to an IoT edge device, the device becomes vulnerable to side-channel attacks, as observable side-channels such as power consumption and electromagnetic emissions can allow the inference of internal information of processors. The most serious incidents in this threat involve the risk of cryptographic keys used in the communication of IoT edge devices being leaked through side-channel vulnerabilities. Once cryptographic keys are compromised, the information flowing over the internet in IoT services becomes susceptible to leaks and tampering, significantly undermining the reliability of IoT services. A well-known practical method of side-channel attack against AES, the lightweight and fast common-key encryption algorithm widely used on the internet, is the Correlation Power Analysis (CPA)[1]. CPA involves measuring the power consumption of the processor during AES encryption, performing statistical calculations using the power consumption waveforms as input that is called as traces, and identifying characteristics to leak the secret key used in AES encryption. Such side-channel attacks utilizing power consumption waveforms, known as power analysis attacks, can lead to the compromise of unprotected AES secret keys if an attacker is able to collect the power consumption of IoT edge devices directly. In the absence of countermeasures, an attack can be completed using information from just a few thousand traces of power consumption for AES encryption, resulting in key leakage in a matter of few ten minutes. While this side-channel vulnerability has been identified for over 20 years, a perfect solution has not yet been found. While comprehensive solutions are being pursued through mathematical and cryptographic research, there is also a need for practical approaches to mitigate the side-channel vulnerabilities, even if only to a limited extent.

There are conventional countermeasures against power analysis attacks when implementing cryptographic processes on dedicated circuits. WDDL[22][21], MDPL[17], MAO[23], and TI[11] correspond to these. These countermeasures focus on combinational circuits that process confidential information inside cryptographic circuits. They defend against power analysis attacks by smoothing or masking the dynamic power consumption of transistors that switch as the inputs to the combinational circuits change. For instance, the most representative countermeasure, WDDL, duplicates the logic of a combinational circuit, driving one instance as the straightforward circuit for processing, and the other as a circuit redesigned to consume complementary power to the straightforward circuit. This smoothens the power consumption waveforms (traces), which is a side-channel, and serves as a side-channel defense by eliminating distinguishing features from the traces. While these countermeasures, including WDDL, are highly effective in obfuscating trace characteristics, they lead to complex and extensive design of the targeted combinational circuits. As a result, they entail overhead in terms of increased implementation area. Even in the case of the smallest increase in area, WDDL, the area overhead for the targeted combinational circuit can be more than doubled.

Conventional countermeasures are not suitable for low-cost IoT edge devices due to their area overhead. Therefore, low-overhead countermeasures to power analysis attacks have been proposed, such as W-FF[24], FPU[8], and FPD[8]. Since these countermeasures are closely related to this paper, they will be explained in detail in the following section. These lightweight countermeasures to power analysis attacks have an innovative aspect in that they focus not on the combinational circuit itself but on its inputs. Transistors switch and generate dynamic power consumption due to changes in inputs. From this view point, these countermeasures aim to disrupt the bit transitions in inputs of the circuit by changing the original inputs to the combinational circuit, thereby preventing the transmission of internal information such as secret key through power consumption.

While W-FF, FPU, and FPD achieve low area overhead, they struggle to provide sufficient resistance against powerful power analysis attacks. This is due to the intentional simplicity and small scale of the proposed circuits, leading to a disruption of bit transitions that follows a certain

regularity. This paper focuses on addressing this weakness. To eliminate the problematic regularity, we employ random numbers. However, conventional pseudo random number generators (PRNG) lead to be large in implementation area, which contradicts the motivation of prior research aimed at minimizing area overhead. Consequently, this paper leverages the characteristics of parallel implementations of the existing AES[3] S-Box to propose a cost-aware approach for generating randomness tailored for power analysis attacks.

The remainder of this paper is organized as follows. Section 2 provides details of W-FF, FPU, and FPD. In section 3, we discuss the differences in the use of random numbers for encryption processing and for improving side-channel resistance, and introduce related work on generating random numbers using S-boxes. Section 4 demonstrates the proposed random number generator and its application to tamper-resistant design. Section 5 presents attack evaluation and area overhead assessment. Section 6 concludes this paper.

## 2 Related Work

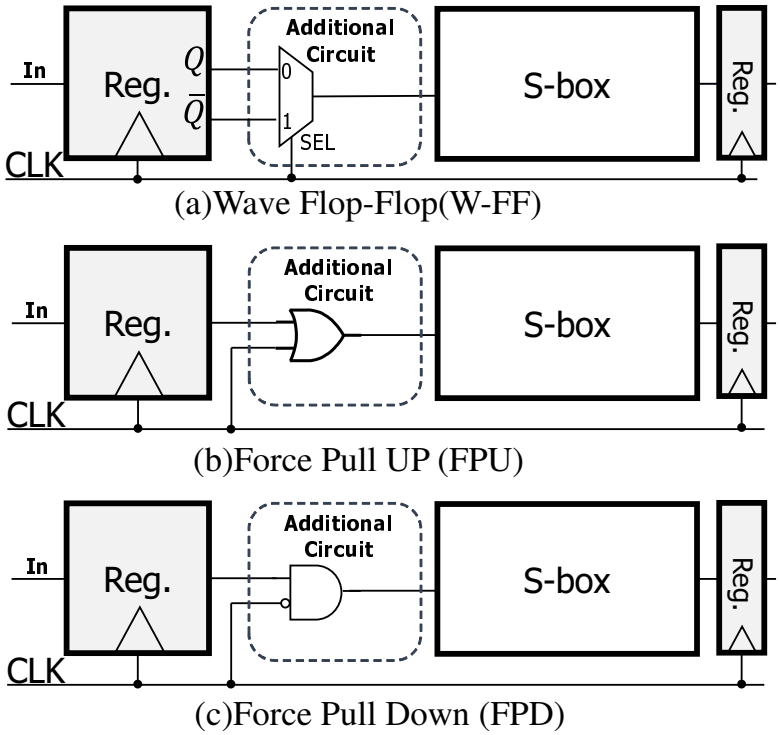


Figure 1: Lightweight Conventional Countermeasures against Power Analysis Attacks.

Figure 1 illustrates the block diagram of W-FF, FPU and FPD, lightweight tamper-resistant designs. Figure 1 (a), (b), and (c) correspond to W-FF, FPU, and FPD, respectively. FPU and FPD are even more lightweight tamper-resistant designs that further simplify W-FF. For each design, a small circuit is placed immediately before the input of the AES S-box. In the case of W-FF, a multiplexer is placed, while in FPU and FPD, several logic gates are placed. A notable aspect of these designs is that they repurpose the clock signal as an input to the S-box. W-FF provides the most understandable examples of utilizing the clock signal. In the case of W-FF, the clock signal is used as the selection signal for a multiplexer. When all flip-flops are driven at the rising edge of the clock signal, if the clock signal is at 0 just before the rising edge, W-FF inputs the value of the register directly to the S-box. Conversely, when the clock signal is at 1, W-FF inputs the inversion

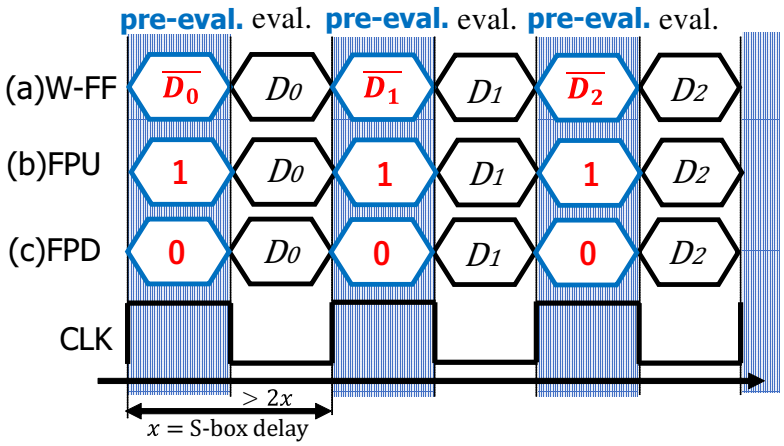


Figure 2: Timing Chart of Lightweight Conventional Countermeasures.

of the register value to the S-box. The same applies to FPU and FPD designs, where during the first half of the clock signal being 1, FPU forcibly inputs 1 to the S-box, and FPD forcibly inputs 0 to the S-box.

Figure 2 shows the timing charts for W-FF, FPU, and FPD. The values of the signals shown in the timing chart are the input values to the S-box. In the case of the no countermeasure circuit, values are input to the S-box in the order of $D_0$-$D_1$-$D_2$. It can be observed that these countermeasure circuits have different values for $D_0$, $D_1$, and $D_2$ during the first half of the clock cycle (*pre-eval.*). However, the S-box output using these different values is discarded at the end of first half of the clock cycle. In other words, whatever values are input to the S-box during the first half of the clock cycle, it does not affect the correct operation of the entire circuit. The correct computation of the S-box is completed during the second half of the clock cycle (*eval.*) using $D_0$, $D_1$ and $D_2$. An important point to note for the proper operation of W-FF, FPU, and FPD is the setting of the clock cycle time. Determining the clock cycle time based on the critical path delay is unlikely to ensure proper operation. This is because the most complex and slowest operation in AES is the S-box, and there is a high likelihood that the delay of the S-box becomes the critical path delay. Therefore, in order to ensure proper operation, W-FF, FPU, and FPD must set the clock cycle time to be more than twice the delay of the S-box, even if it significantly exceeds the overall critical path delay of the whole circuit. This performance degradation is a disadvantage for these lightweight power analysis countermeasures. However, for example, approaches like WDDL require precharge cycles, necessitating a doubling of the number of cycles required for computations. In comparison to conventional countermeasure such as WDDL and MDPL, this does not pose a significant disadvantage.

From a side-channel security perspective, in the no countermeasures, there exists a vulnerability where $D_0$, $D_1$, and $D_2$ can be inferred from the dynamic power consumption resulting from the transistor switches within the S-box due to bit transitions of input. In Figure 2, W-FF, FPU, and FPD insert different values between $D_0$ and $D_1$, as well as between $D_1$ and $D_2$, disrupting direct bit transitions. This effectively disturbs the side-channel of power consumption due to transistor switch thus achieving countermeasures against power analysis attacks. However, in their pursuit of low area overhead for IoT edge devices, W-FF, FPU, and FPD still retain vulnerability to bit transition disruption. This is because the inserted values exhibit regularity or patterns. When the inserted values are constants or easily computable values from the values before and after bit transitions, information that allows the inference of $D_0$, $D_1$, and $D_2$ remains in the side-channel, even if there are no direct bit transitions. Moreover, if the countermeasures are well-known, it is also possible to reverse-engineer from the side-channel.

Power consumption is determined by the Hamming distance of multiple-bit inputs observed over time. This is due to the dynamic power consumption of CMOS transistors when their inputs transi-

tion from 0 to 1 or from 1 to 0. Exploiting this, an attack analysis program can retroactively deduce the input bits by Hamming distance of input bit transitions observing power consumption. By inputting plaintext into the encryption processing system and collecting related traces through chosen plaintext attacks, the range of possible internal information states can be narrowed down to some extent based on the Hamming distance. Correlation Power Analysis (CPA)[1] performs Differential Power Analysis (DPA)[21] based on this concept to reduce the number of trace inputed to the attack program, calculating the correlation coefficient between the power consumption model of potential cryptographic key candidates within the system and the actual power consumption (traces). Therefore, CPA outputs the cryptographic key candidate with the highest positive correlation coefficient as the attack results (the guessed key).

The intention behind injecting random numbers ($R_0$, $R_1$, $R_2$) into bit transitions, as shown in Figure 4, is to conceal the original power consumption associated with bit transitions. By interfering with bit transitions through random number injection, the internal Hamming distance is altered. Consequently, it becomes possible to disrupt the predictions of CPA, which classify and prune branches of traces based on the Hamming distance, leading to an expectation of improved tamper resistance. From this consideration, conventional noise injection such as W-FF, FPU, and FPD, which predict constant or inverted original input values, is susceptible to predictable noise, resulting in limited enhancement of tamper resistance due to the regularity in the change of Hamming distance.

This paper designs a circuit configuration for AES that aims to eliminate the vulnerabilities in W-FF, FPU, and FPD by using random values for insertion into the bit transitions, which have no relation to the values before and after. However, high-precision pseudo-random number generators (PRNGs) typically come with a significant implementation area cost, making them less suitable for designs with the original aim of low area overhead, such as those targeting IoT edge devices as in related work. MW-FF[26], Our previous work used PRNGs to tamper-resistant design, however, The results confirmed that ignoring PRNGs that generate 128-bit random numbers at once would result in significant area overhead while a definite improvement in tamper resistance is achieved. Therefore, this paper proposes a technique that, without adding a new PRNG, ensures a sufficient level of randomness by reusing the output of existing parallel implementations of the S-box in AES. This approach is presented as a means to achieve tamper-resistant design. The details of this pseudo-random number generation will be elaborated in the following section.

## 3 Random Number Generation using S-boxes

The S-box in AES[3] serves as a unit for non-linear operation, designed under the premise that its processing, despite being a reversible non-linear operation, ensures sufficient complexity through multiple iterations of the S-box processing. This iterative process is defined as rounds in AES, where in the case of 128-bit AES, 6 rounds of processing are executed to ensure the complexity. There are multiple solutions for reversible non-linear computations achievable with the S-box. In AES, a composite S-box called Subbyte, which combines Galois field multiplications achievable only with XOR and AND operations, is adopted. Research to ensure the complexity of S-boxes, which is critical for the security of encryption, has advanced, and studies are still being conducted on selectively using S-boxes instead of fixed ones [20].

Many ideas have been studied in the past on fast random number generators suitable for encryption[7][19]. These random number generators pass sufficient randomness tests[18]; however, they incur significant implementation costs with noticeable overhead. In this paper, rather than using random numbers as part of encryption computations, they are used to enhance side-channel resistance. Thus, even if the randomness is low, it does not affect the security guarantees of the encryption itself. Random numbers used for jamming side channels only require sufficient complexity to prevent analyzing. Therefore, we propose in this study that this can be substituted by the round processing of S-box in AES.

In this study, although sufficient randomness is not required for the random numbers, the randomness provided by the S-Box in AES has been proposed as SBoNG(S-Box Number Generator)[9] by F. Neugebauer et.al., and reported that randomness reaches sufficent level for stochastic com-

puting is guaranteed. Therefore, we propose a low-cost implementation for tamper-resistant AES design by utilizing the originally embedded S-box in AES for random number generation.

# 4 Proposed Randam Generation for Tamper-resistant Design

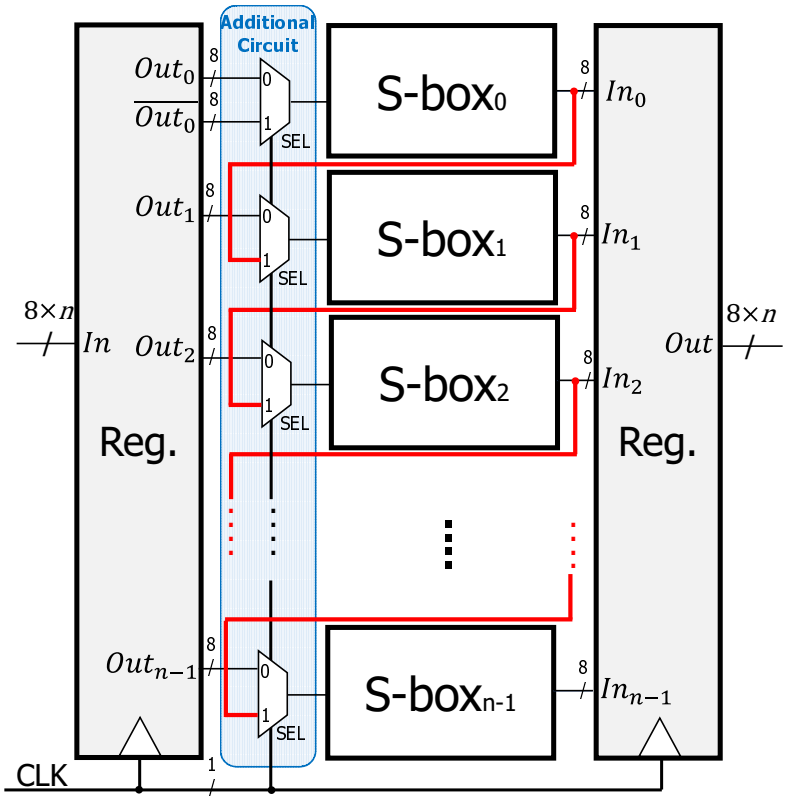


Figure 3: The Proposed Tamper-resistant AES Design.

The S-box is a non-linear operation in AES and is responsible for substitution processing. Substitution is a process where there is complicatedly mathematical relationship between the values before and after processing that is called as Galois field inverse element computation, and it is a reversible operation. The S-box is required for non-linear mixing operation in cryptographic processing, and due to its characteristic of producing non-linear outputs for consecutive input values, it can also be used incidentally as a source of randomness. Hence, we propose the shared use of the S-box for both the primary cryptographic processing and tamper-resistant design to obtain randomness without increasing the implementation area.

Figure 3 illustrates the block diagram of tamper-resistant design in an n-parallel S-box implementation. AES is defined with a block length of 128-bits and treats an element called the state as a processing unit in the form of a 4x4 two-dimensional array of 1-byte elements. The processing of the S-box is performed separately for each element of this array. Since there is no dependency between the processing of individual elements, all 16 elements within one state are allowed to be processed simultaneously by the S-box. Taking advantage of this characteristics, in the dedicated circuit implementation of AES, the S-boxes can be placed in parallel for each element of the S-state and executed simultaneously, thereby optimizing the processing efficiency. Hence, in Figure 3, n becomes 16 in the context of AES.

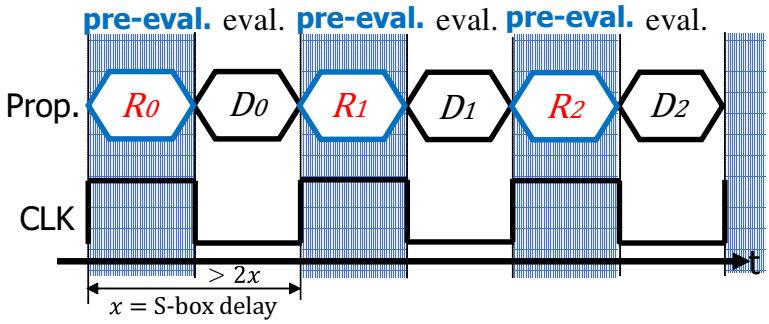


Figure 4: The Timing Chart of Proposed AES Design.

The proposed method is based on W-FF with small modifications. We have indicated the modifications compared to W-FF with red lines. In other words, the changes from W-FF are in the wiring only. $S-box_0$ functions as a regular W-FF, while S-box1 takes the output of the one directly above $S-box_0$ as input instead of the inverted input of W-FF, which serves as the random value input. Our proposed design is constructed by connecting such wiring in a daisy-chain fashion towards $S-box_{15}$. By implementing such wiring, it becomes possible to input random values ($R_0$ to $R_2$) derived from S-box outputs in the pre-eval. of all S-boxes except $S-box_0$, as shown in Figure 4. The bit fibers depicted in Figure 4 are also realized by a previous study called MW-FF, as described in Section 2. However, MW-FF uses a PRNG for random number generation, and this work aims to achieve the objectives of that prior work through a area-saved implementation.

At first glance, it may appear that only $S-box_0$ retains the original W-FF implementation without using random values, seemingly diminishing its resistance value. However, attacks on AES result in the leakage of the secret key only when all inputs to the S-boxes can be inferred from power consumption. Therefore, the vulnerability of a single S-box has a relatively small impact. $S-box_0$ serves a special role, as it generates random values using the S-box output in pre-eval. of W-FF as a random seed.

An important aspect of our proposed design, like W-FF, FPU, and FPD, is the setting of the clock cycle time. In the typical design flow of synchronous circuits, there exists a path of 16 sequential connections in the daisy-chain of S-boxes, making the path containing the red wires in Figure 3, which supplies random values to each S-box, inevitably become the critical path. Moreover, this delay becomes quite significant. However, there is no need to set the clock cycle time to accommodate this very long critical path delay because, as mentioned in Section II, this critical path is only used in the pre-eval. phase and does not relate to the accurate operation of the entire AES. Even if it does not guarantee that the signal reaches $S-box_{15}$, the characteristic that all intermediate stages in the daisy chain are random values makes it suitable for tamper-resistant design. In fact, the dynamic variation in the destination S-box for specific random values due to placement, wiring results, and temperature-induced delay fluctuations can be advantageous from a tamper resistance perspective. For the aforementioned reasons, it can be concluded that there is no need to make any changes to the clock cycle time settings similar to those of W-FF due to wiring modifications.

## 5 Evaluation

To evaluate the proposed AES design illustrated in Figure 3, we conducted a Correlation Power Analysis (CPA) [1] attack evaluation. Additionally, to evaluate the area overhead for tamper-resistant designs, we performed logic synthesis on ASICs and FPGAs.

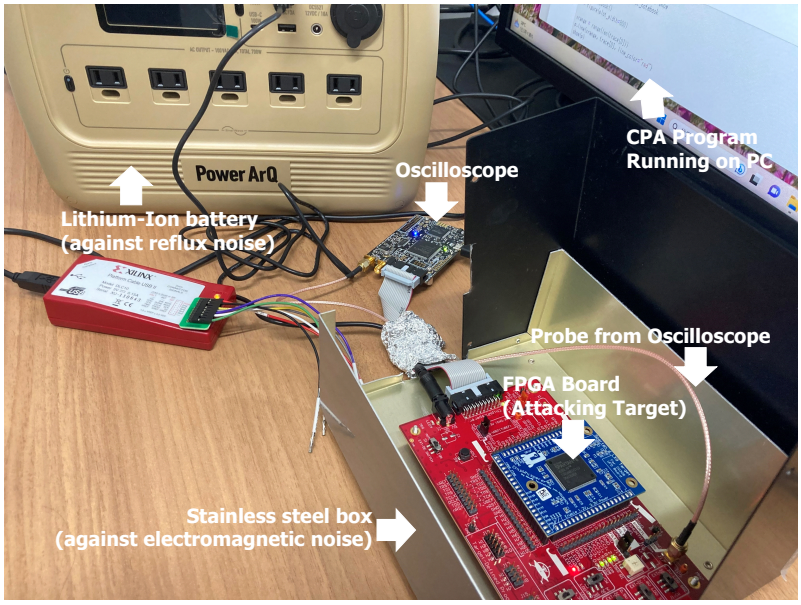


Figure 5: Experimental Environment.

## 5.1 Experimental Setup

Figure 5 shows the attack environment for the evaluation. The red and blue boards housed in the stainless steel case in the lower right corner of the photo are the target boards for the attack. During the attack, the stainless steel case is closed, and any gaps are sealed with aluminum tape to block external noise.

The red board serves as the power board and has probe points in the upper right corner to measure the voltage across shunt resistors, which allows for the acquisition of power consumption variations as a trace by measuring it with an oscilloscope. The red board is powered by a ocher lithium-ion battery, and supplying power from the battery helps to isolate the circuit from power supply noise returning from the electric outlets. The blue board is an FPGA board, equipped with the Xilinx Spartan6 XC6SLX9. A 128-bit AES is implemented on this FPGA. Plaintext is sent from a PC to this AES, and traces of the encryption process are captured using an oscilloscope. After the trace collection is completed, a CPA attack program[14] is performed by inputting the 50,000 traces to infer the secret key. The 128-bit AES implemented on the FPGA was based on Google Project Vault's RTL design[13]. In the evaluation of this paper, W-FF[24], MW-FF[26], and WDDL[22][21] were chosen as comparative design and applied to the S-box. The WDDL design was downloaded from the Yokohama National University's website[6].

Due to the difficulty of manufacturing chips to evaluate the circuit of proposed design, this paper utilizes FPGA for evaluation purposes. However, the proposed design in this paper is not specific to FPGA. Generally, there are minimal characteristic differences between FPGA and ASIC implementations in attack evaluations. It is often considered that FPGA implementations are more prone to leaking sensitive information in terms of power consumption compared to ASIC implementations, making attack evaluations using FPGAs a more stringent assessment in recent side-channel security research[2][4][10].

The proposed design performs original cryptgraphic processing on a half-clock cycle. Consequently, if the clock cycle period is set to the delay of the conventional (before applying the proposed design) critical path, the proposed design will not work properly. Therefore, the circuit must be supplied with a clock signal of at least double the critical path delay period or more. Hence, in our evaluation, we provided a sufficiently long period clock signal with a margin of more than 30 times the critical path delay obtained in the design before applying the proposed design. In addition, since

the information leakage from side channels remains unchanged regardless of whether the clock period is short or long, there is no issue with supplying a low-frequency clock signal as the measurement environment for experiments. Furthermore, if a very high-frequency clock signal were supplied, it would necessitate extremely expensive oscilloscopes, which are capable to sample in high rates to accurately capture side-channel information. In our evaluation, to collect traces using inexpensive oscilloscopes, the clock frequency of the target chip needs to be sufficiently low. For these reasons, we have set the clock frequency low as far as possible under conditions that allow us to complete the experiments within a realistic trace collection time..

Again, it is worth noting that when setting the clock cycle period, the delay of the daisy-chain in the proposed design need not be considered. This is because the signals in the daisy-chained path are used as generating random numbers and do not affect the output of the computation. Therefore, there is no need for the signals to stabilize. In other words, even if the first half of the clock cycle period is shorter than the delay of the daisy-chained path, it does not cause any malfunction in the computation. If the clock cycle period is significantly shorter, the daisy-chained path will be wave-pipelined for computation, however this does not pose a problem for the purpose of random number generation. Whether computation of this path is stable or not, unstable signals can still be used as generating random numbers. Hence, in our evaluation, we disregard the delay of the daisy-chained path and set the clock cycle period based on the critical path delay before applying the proposed design.

For an accurate evaluation of the area overhead, we performed logic synthesis of the entire AES using Synopsis Design Compiler and estimated the implementation area. The logic synthesis utilized a 45nm open-cell library[5]. The implementation area was extracted from the synthesis report output by the design compiler. Even prior to placement and routing processes, the design compiler can achieve highly accurate implementation area estimates by specifying the cell library. The open-cell library used in the evaluation of this paper was created based on the predictive technology model of Arizona State University. Although intentionally rendered non-manufacturable, it is only used for research and development purposes, resembling the 45nm manufacturing process as of 2011. Today, many research studies have been published using this library. Hence, the occupied area report from the design compiler does not significantly differ from the actual implementation area in the actual 45nm process. Additionally, considering that the evaluation aimed at relative assessment within the same environment, we believe the validity of the area evaluation method is high.

In addition to area evaluation in ASIC, this paper also evaluates the resource utilization of the proposed method in FPGAs. This is because the attack evaluation in this paper targets FPGAs, and we focus the evaluation of area-efficient implementation of the proposed method in FPGAs. It should be noted here that the proposal in this paper is not specific to FPGA but can be realized in digital circuits. Since it is difficult to evaluate by manufacturing chips, we evaluate our proposal only on FPGAs.In the area evaluation on FPGA, we extracted the number of registers, the number of lookup tables (LUTs), and the number of slice cells from the report generated by synthesizing logic using Xilinx's ISE 14.4 for Spartan6 XC6SLX9, and compared them for each.

At the end of this evaluation, we show waveforms (traces) collected with oscilloscopes for the attack to confirm changes in the shape of the trace. These traces include those from related work such as FPU, FPD, W-FF, as well as our proposed method and the comparison target for attack evaluation, WDDL. Additionally, traces with no countermeasures are presented to consider how the proposed method provides resistance to attacks by observing how the trace shapes change compared to other methods.

## 5.2 Attack Evaluations

The attack results are shown in Figure 6. The vertical axis in the figure represents the number of partially guessed round keys by CPA. When all 16 partial round keys are correctly inferred, the attacker can obtain the secret key of AES through the reverse calculation of the key generation algorithm. The horizontal axis in the figure represents the number of traces input into CPA. With a larger number of traces used for statistical analysis, CPA can provide more accurate inference.

From the figure, it can be observed that the AES design proposed in this paper, red line, exhibits

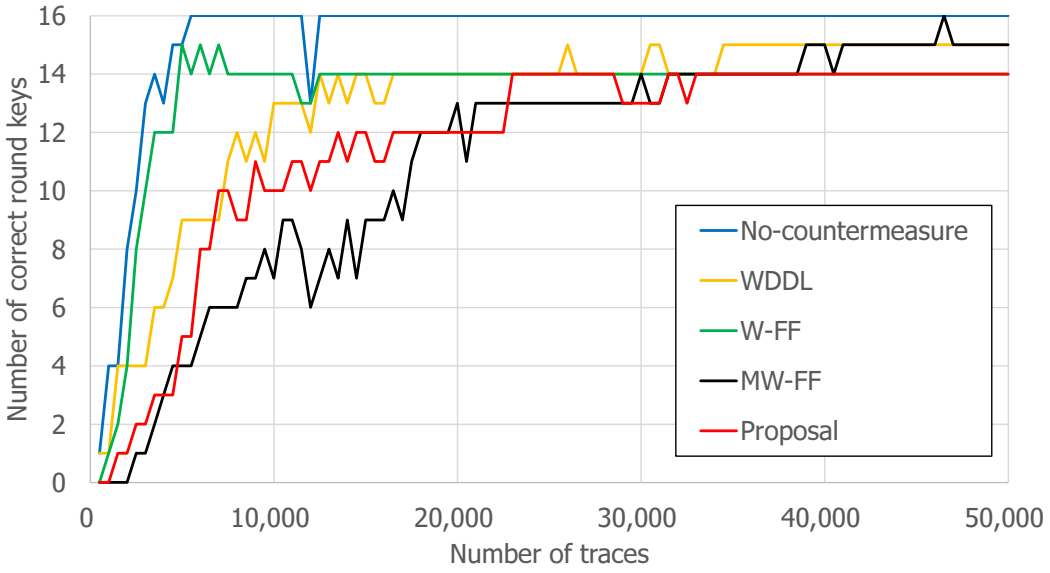


Figure 6: Attack Results.

the highest level of tamper resistance. The proposed design did not leak more than 14 partial round keys in our evaluation, regardless of the number of traces input. On the other hand, MW-FF, which uses random numbers like the proposed design, initially demonstrates better tamper-resistance than the proposed design in the analysis attack. However, in the later section of the analysis attack, it falls behind in terms of tamper-resistance compared to the proposed design, finally converging to the leakage of 15 partial round keys, and at one point during the analysis, allowing leakage of all 16 partial round keys. WDDL, yellow line, and W-FF, green line, exhibit similar tamper resistance towards the end of the analysis. However, since W-FF leaked 15 partial round keys in the early stages, while WDDL did not, it indicates that WDDL has higher tamper resistance than W-FF. The no countermeasure S-box (No-countermeasure), blue line, leaks all partial round keys with approximately 5,000 traces of input, indicating convergence.

## 5.3 Area Evaluations

Figure 7 shows the area evaluation. As evident from the figure, the implementation area of the proposed method and the base W-FF implementation remains almost the same. It is clear that the wiring of the daisy chain, which is a notable difference between the two, does not affect the area. Furthermore, with regard to MW-FF, albeit slight, an increase in implementation area compared to W-FF and the proposed design can be observed. This increase is attributed to the implementation area due to the PRNG. While it is expected that the proposed method can mitigate this aspect, the apparent small increment is because MW-FF utilizes a simple PRNG, XorShift. It can be easily anticipated that this difference would become significant by employing a more precise PRNGs. From this, it can be concluded that the tamper-resistant AES design proposed in this paper achieves an improvement in tamper resistance without compromising the primary goal of low area overhead as aimed in related work.

Figures 8 and 9 illustrate the area evaluation on FPGAs. Figure 8 shows the number of registers, Figure 9 shows the number of lookup tables (LUTs). Comparing these three figures with Figure 7, it can be observed a similar trend. One notable point is the significant increase in the number of registers in MW-FF. This is attributed to the addition of flip-flops used for the 128-bit PRNG, which notably occupy circuitry. In the case of FPGA implementation, this represents a significant occupation of registers within slices by the PRNG. Thus, it has been confirmed that similar effects

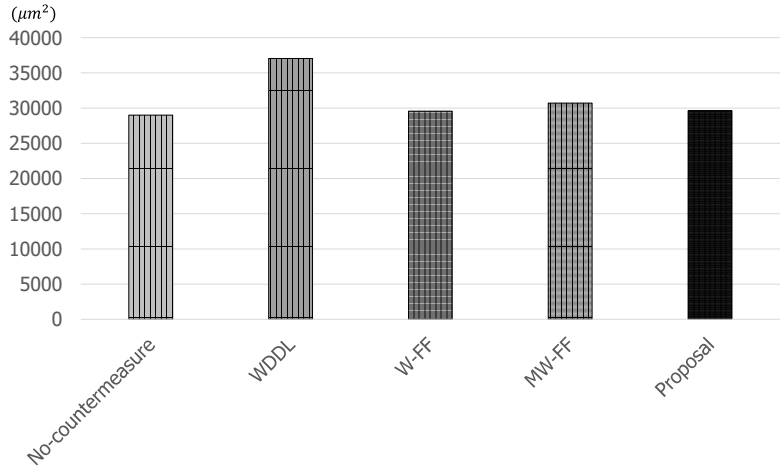


Figure 7: Implementation Area of Overall AES Design in ASICs.

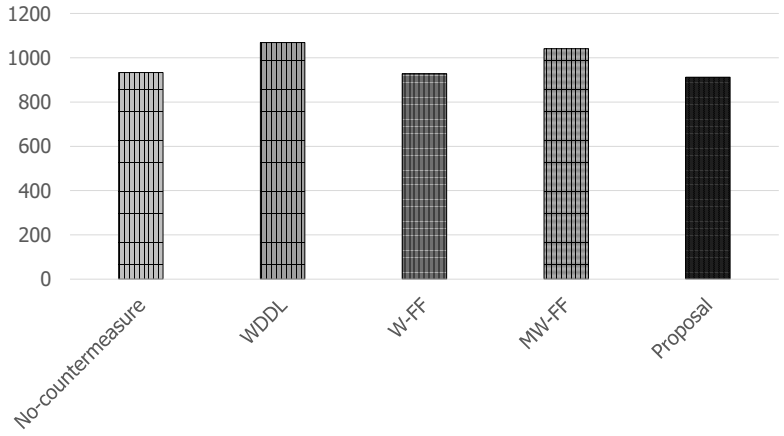


Figure 8: Number of Registers for FPGA Design.

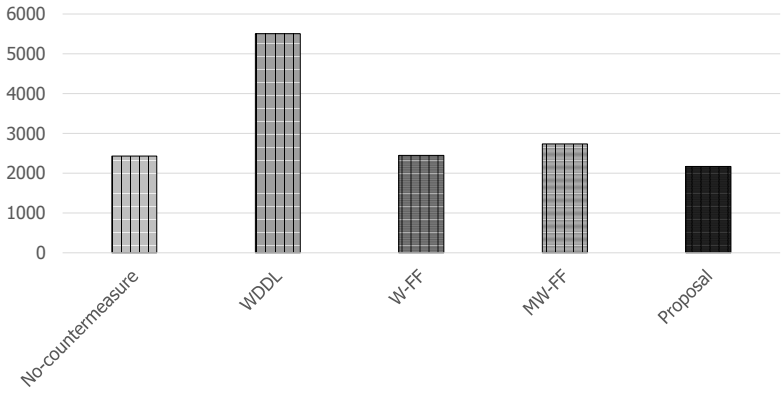


Figure 9: Number of LUTs for FPGA Design.

in terms of implementation area efficiency are obtained in both ASIC and FPGA implementations.

## 5.4 Comparison of Waveforms

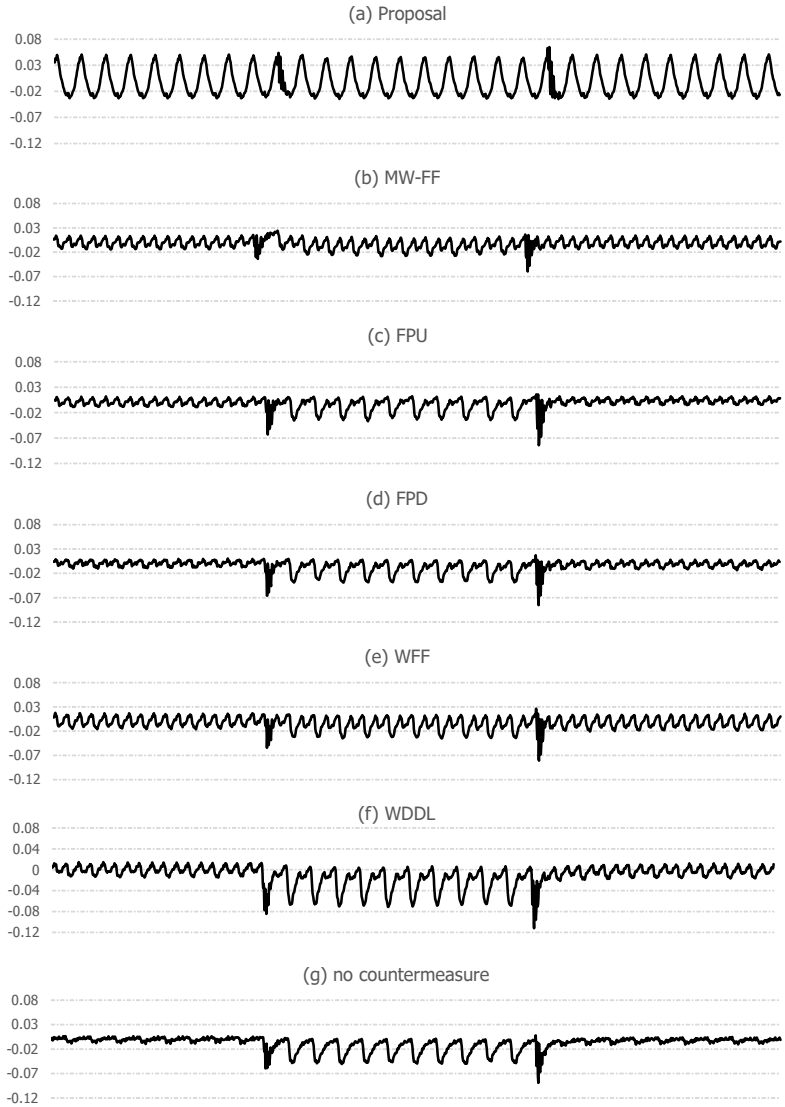


Figure 10: Comparison of Traces.

Figure 10 illustrates the waveforms of each countermeasure. The vertical axis of the graph represents the voltage of the shunt register, indicating the current consumption (energy consumption). The horizontal axis represents the passage of time, with these waveforms being power consumption waveforms (traces). These waveforms are used for the attack evaluation in CPA. It is evident that our proposed countermeasure (a) exhibits significant changes compared to other related research methods. The amplitude of the waveform increases, and it fluctuates at regular intervals. While the waveform near the center represents the operation of AES, significant variations are observed before and after. This implies that the number of transistor switches has significantly increased by connecting the S-boxes in series (daisy-chained), and regardless of the processing, it always occurs during the first half of the clock.

This significant change in shape, compared to countermeasures from other related work, effectively conceals or eliminates the characteristics of the no countermeasure shown in (g) within the large variations of steady-state power consumption. It can be concluded that this change has clearly enhanced the tamper resistance of the proposed countermeasure, resulting in evaluation outcomes that demonstrate the effectiveness of the proposed approach at a glance.

However, the tamper resistance of the proposed design is difficult to deem as extremely robust, as indicated by the fact that 14 out of 16 partial round keys are leaked, as evident from the figure 6. This is attributable to the conditions of the attack evaluation environment. For instance, previously existing and reliable tamper-resistant methods like WDDL, as shown in the figure 6, do not demonstrate such high tamper-resistance in this attack evaluation. There are two consideration for this result. One is the use of FPGAs in the attack evaluation environment, which consume more power compared to ASICs. FPGAs amplify the characteristics of waveforms indicating internal confidential information (partial round keys) on side channels, making them more vulnerable to power analysis attacks due to a higher S/N ratio when considering environmental noise. Other consideration lies in the optimization of FPGA-specific LUTs. FPGAs store truth tables in memory, known as LUTs, and drive them by reading from this memory. In this case, reading the memory introduces power consumption as a side-channel. Optimizations aim to integrate truth tables and reduce the amount of used memory. However, due to optimizations, the logic of combinatorial circuits redesigned to mask power consumption in FPGAs may not function as intended.

Taking the above into consideration, even if there are significant changes in shape of the waveforms visibly, it is only a change in the shape of the waveforms with a long period. The information of the short-period waveforms superimposed on this long-period waveforms is not completely eliminated, especially due to the second consideration mentioned above. This likely contributed to leaking many partial round keys in power analysis attacks. In other words, it can be said that our proposed method effectively masked information related to confidentiality that falls within the low-frequency bandwidth.

# 6 Conclusion

This paper aims to improve the tamper-resistant design with low area overhead in related work, namely W-FF, MW-FF, FPU, and FPD. It focuses on the parallel execution of S-box processing in dedicated circuit implementations for AES and proposes a design that generates random numbers by sharing the S-box for enhanced tamper resistance.

In the evaluation of this paper, the proposed design achieved further improvement in tamper resistance without compromising the low area overhead characteristics of W-FF.

# Acknowledgment

This work is supported by JSPS KAKENHI Grant Number 20K11823, 20H00590, and 24K14958. It is also supported by VLSI Design and Education Center (VDEC), the University of Tokyo in collaboration with Synopsys, Inc..

# References

[1] E. Brier, C. Clavier, and F. Olivier. Correlation power analysis with a leakage model. In *Proc. of International Workshop on Cryptographic Hardware and Embedded Systems*, volume 3156, pages 16–29, 2004.

[2] K.-S. Chong, J.-S. Ng, J. Chen, N. K. Z. Lwin, N. A. Kyaw, and W.-G. Ho. Dual-hiding side-channel-attack resistant fpga-based asynchronous-logic aes: Design, countermeasures and evaluation. In *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, volume 11, pages 343–356, 2021.

[3] J. Daemen and V. Rijmen. The block cipher rijndael. In *Proc. of International Conference on Smart Card Research and Advanced Applications (CARDIS 1998)*, volume 1820, pages 277–284, 1998.

[4] A. Dubey, R. Cammarota, and A. Aysu. Maskednet: The first hardware inference engine aiming power side-channel protection. In *Proc. of 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2020.

[5] Silvaco Inc. Pdk 45nm open cell library. In *https://si2.org/open-cell-library/*, 2023.

[6] Information and Physical Security Research Group (Yokohama National University). Cryptographic circuits with logic level countermeasures against dpa. In *https://ipsr.ynu.ac.jp/circuit/index.html*, 2023.

[7] B. Jun and P. Kocher. The intel random number generator. In *White Paper Prepared for Intel Corporation*, pages 1–8, 1999.

[8] Y. Koyanagi and T. Ukezono. An extremely light-weight countermeasure to power analysis attack in dedicated circuit for aes. In *Proc. of 19th International SoC Design Conference (ISOCC 2022)*, pages 85–86, 2022.

[9] F. Neugebauer, I. Polian, and J. P. Hayes. S-box-based random number generation for stochastic computing. In *Microprocessors and Microsystems*, volume 61, pages 316–326, 2018.

[10] J.-S. Ng, J. Chen, S. Wu, N. A. Kyaw, K.-S. Chong, Z. Lin, and B.-H. Gwee. Maskednet: The first hardware inference engine aiming power side-channel protection. In *Proc.of 2023 IEEE International Symposium on Circuits and Systems (ISCAS 2023)*, 2023.

[11] S. Nikova, C. Rechberger, and V. Rijmen. Threshold implementations against side-channel attacks and glitches. In *Proc. of International Conference on Information and Communications Security 2006 (ICICS 2006)*, volume 4307, pages 529–545, 2006.

[12] University of California at Berkeley. Chipyard: An agile risc-v soc design framework with in-order cores, out-of-order cores, accelerators, and more. In *https://github.com/ucb-bar/chipyard*, 2020.

[13] C. O'Flynn. Side-channel power analysis of aes core in project vault. In *https://colinoflynn.com/2015/05/side-channel-power-analysis-of-aes-core-in-project-vault/*, 2023.

[14] C. O'Flynn and Z. D. Chen. Chipwhisperer: An open-source platform for hardware embedded security research. In *Proc. of Constructive Side-Channel Analysis and Secure Design (COSADE2014)*, volume 8622, pages 243–260, 2014.

[15] et al. P. Mantovani. Hero: Heterogeneous embedded research platform for exploring risc-v manycore accelerators on fpga. In *arXiv:1712.06497*, 2017.

[16] et al. P. Mantovani. Agile soc development with open esp. In *Proc. of 2020 International Conference on Computer Aided Design (ICCAD 2020)*, 2020.

[17] T. Popp and S. Mangard. Masked dual-rail pre-charge logic: Dpa-resistance without routing constraints. In *Proc. of The annual Conference on Cryptographic Hardware and Embedded Systems 2005 (CHES 2005)*, volume 3659, pages 172–186, 2005.

[18] W. Schindler and W. Killmann. Evaluation criteria for true (physical) random number generators used in cryptographic applications. In *Proc. of The annual Conference on Cryptographic Hardware and Embedded Systems 2002 (CHES 2002)*, volume 2523, pages 431–449, 2002.

[19] B. Sunar, W. J. Martin, and D. R. Stinson. A provably secure true random number generator with built-in tolerance to active attacks. In *IEEE Transactions on Computers*, volume 59, pages 109–119, 2007.

[20] T. Tiessen, L. R. Knudsen, S. Kolbl, and M. M. Lauridsen. Security of the aes with a secret s-box. In *Proc. of International Workshop on Fast Software Encryption (FSE 2015)*, volume 9054, pages 175–189, 2015.

[21] K. Tiri, D. Hwang, A. Hodjat, B.-C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede. Prototype ic with wddl and differential routing - dpa resistance assessment. In *Proc. of The annual Conference on Cryptographic Hardware and Embedded Systems 2020 (CHES 2020)*, pages 354–363, 2020.

[22] K. Tiri and I. Verbauwhede. A logic level design methodology for a secure dpa resistant asic or fpga implementation. In *Proc. of Design, Automation and Test in Europe Conference and Exhibition (DATE2004)*, pages 246–251, 2004.

[23] E. Trichina. Combinational logic design for aes subbyte transformation on masked data. In *Cryptology ePrint Archive*, volume 236, 2003.

[24] T. Ukezono. Resistance for side-channel attack by virtual dual-rail effect. In *Proc. of 3rd International Conference on Electrical, Communication and Computer Engineering (ICECCE 2021)*, pages paper–89, 2021.

[25] B. Towles W. J. Dally. Route packets, not wires: on-chip inteconnection networks. In *Proc. of the 38th annual Design Automation Conference (DAC 2001)*, 2001.

[26] Y.Koyanagi and T. Ukezono. A cost-sensitive and simple masking design for side-channels. In *Proc. of 2023 IEEE Region 10 Technical Conference (TENCON 2023)*, pages 731–736,, 2023.