International Journal of Reconfigurable and Embedded Systems (IJRES)
Vol. 12, No. 3, November 2023, pp. 305~319
ISSN: 2089-4864, DOI: 10.11591/ijres.v12.i3.pp305-319

Empirical analysis of power side-channel leakage of high-level synthesis designed AES circuits

Takumi Mizuno[1], Hiroki Nishikawa[2], Xiangbo Kong[1], Hiroyuki Tomiyama[1]
[1]Graduate School of Science and Engineering, Ritsumeikan University, Shiga, Japan
[2]Graduate School of Information Science and Technology, Osaka University, Osaka, Japan

Article Info

Article history:

Received Feb 10, 2023
Revised Mar 22, 2023
Accepted Apr 28, 2023

Keywords:

Advanced encryption standard
High-level synthesis
Masking
Side-channel attack
T-test

ABSTRACT

Many internet of things (IoT) devices and integrated circuit (IC) cards have been compromised by side-channel attacks. Power-analysis attacks, which identify the secret key of a cryptographic circuit by analyzing the power traces, are among the most dangerous side-channel attacks. Gen-erally, there is a trade-off between execution time and circuit area. However, the correlation between security and performance has yet to be determined. In this study, we investigate the cor-relation between side-channel attack resistance and performance (execution time and circuit area) of advanced encryption standard (AES) circuits. Eleven AES circuits with different performances are designed by high-level synthesis and logic synthesis. Of the eleven AES circuits, six are circuits with no side-channel attack countermeasures and five are circuits with masking countermeasures. We employ four metrics based on a T-test to evaluate the side-channel attack resistance. The results based on the correlation coefficient show the correlation between side-channel attack resistance and performance. The correlation varies according to four metrics or masking countermeasure. We argue that designers should change their attitudes towards circuit design when considering security.

Corresponding Author:

Takumi Mizuno
Graduate School of Science and Engineering, Ritsumeikan University
1-1-1 Nojihigashi, Kusatsu, Shiga, 525-8577, Japan
Email: takumi.mizuno@tomiyama-lab.org

1. INTRODUCTION

Internet of things (IoT) devices and integrated circuit (IC) cards have become widespread in recent years, providing significant enrichment in our daily lives. While these devices are convenient, they are exposed to physical fields and attacked by others. Cryptographic circuits such as advanced encryption standard (AES) play an active role in protecting these devices. There are many methods used to attack cryptographic circuits, which are called side-channel attacks. Side-channel attacks expose information protected by cryptographic circuits by observing information (power traces and electromagnetic waves) emitted by devices [1], [2]. Power analysis attacks are among the most dangerous side-channel attacks because of the amount of information leaked from power traces [3]. Among power analysis attacks, simple power analysis (SPA) attacks [4], differential power analysis (DPA) attacks [5], [6] and correlation power analysis (CPA) attacks [7] are well known. Additionally, studies have focused on power analysis attacks [8], [9]. As countermeasures to side-channel attack, masking countermeasures come into play. Masking countermeasures inset random number during encryption. This approach makes it difficult for attackers to observe classified information.

On the other hand, high-level synthesis (HLS) techniques have been developed [10], [11]. HLS is a technique that automatically generates resister transfer level (RTL) circuits from high-level programming languages such as C/C++. In general, high-level programming languages are easier to understand and RTL programming languages are more difficult for beginners. Thus, high-level synthesis has an advantage when designing RTL circuits. Additionally, HLS optimization effects the performance of generated circuits [12]. Zhang *et al.* [13] optimizes the S-box of an AES circuit and evaluates side-channel attack resistance. Mizono in [14] optimizes AES performance during high-level synthesis and shows that a higher performance AES circuit has lower side-channel attack resistance. Balihar and Novotny [15] changes the synthesis parameters when synthesizing AES circuits and evaluates the side-channel attack resistance. The works in [16], [17] evaluate the side-channel attack resistance of AES circuits with masking countermeasures and show the advantages of masking countermeasures. Thus, how to design cryptographic circuits with higher side-channel attack resistance has been considered. However, the impact of circuits' performance on side-channel attack resistance requires further discussion. Depending on the impact, this paper proposes a change in mind to designers that focus only on the performance of cryptographic circuits.

This paper investigates the correlation between the performance (number of clock cycles and number of resources) and side-channel attack resistance of AES circuits. Six AES circuits without masking countermeasures and five AES circuits with masking countermeasures are designed and evaluated. Each AES circuit is a Pareto-optimal circuit. In terms of clock cycles and resources, the AES circuits without masking countermeasures have the trade-off relationship, but the AES circuits with masking countermeasures do not. Side-channel attack resistance is evaluated by the T-test that is calculated from power traces. We employ four metrics to compare the side-channel attack resistance. For AES circuits without masking countermeasures, there is a correlation between performance and side-channel attack resistance. The result varies according to the four metrics. We argue that the evaluation of side-channel attack resistance can change depending on the definition of security. Even in AES circuits with masking measures, there is some correlation between performance (number of clock cycles and number of resources) and side-channel attack resistance. However, quite unlike AES circuits without masking, the more ideal the circuit is, the more secure it is.

The contributions of this paper are as follows.

- We design eleven AES circuits with high-level synthesis and compare the correlation between the performance (number of clock cycles and resources) and side-channel attack resistance. Of the eleven circuits, six AES circuits have no masking countermeas-ures and five AES circuits have masking countermeasures.
- We evaluate side-channel attack resistance in four metrics to investigate the resistance in detail. The metrics are based on T-test.
- We show the correlation between the performance (number of clock cycles and number of resources) and side-channel attack resistance. Additionally, the correlation varies depending on whether there are masking countermeasures or not.

The paper is organized as follows. In section 2, we describe the prerequisites for this study. In section 3, we design AES circuits. In section 4, we evaluate side-channel attack resistance for both types of AES circuits. In section 5, we conclude the paper and describe future work.

2. PRELIMINARLIES

2.1. AES

AES is a type of cryptographic circuit, which stands for AES [18], [19]. AES is often used to encrypt communication data. It employs a common key cryptography, in which the sender and receiver use the same key to perform encryption and decryption. AES requires 128-bit plaintext input, and the key size can be selected from 128, 192, and 256 bits.

The main feature of AES is to use four types of transformations, which can be performed in a simple process. Additionally, these processes perform multiple times to increase the encryption strength. The four types of transformations performed by AES are SubBytes, ShiftRows, MixColumn, and AddRoundKey, respectively. SubBytes uses an S-box to perform substitutions in 8-bit units. ShiftRows performs to reorder data in 8-bit units. MixColumn performs matrix operations in 32-bit units. AddRoundKey performs to convert with a key generated from the encryption keys. The four conversions are simple calculations, and the decryption process performs the reverse conversions.

2.2. Power side-channel attacks

Side-channel attacks are an attack method used to obtain secret information by physically observing devices such as IoT devices and IC cards. These devices are equipped with cryptographic circuits and the circuits protect from other attacks. However, it is possible to infer the encryption key by observing the power traces. Attacks based on this technique are called power analysis attacks. The power analysis attack is one of the most dangerous side-channel attacks [3]. There are different types of power analysis attack, including SPA [4], DPA [5], [6] and CPA [7] attacks. Especially in the IoT field, CPA can be a threat.

A CPA attack is an attack method to identify a secret key by observing multiple power traces of a cryptographic circuit. The attackers use a computer that can send random but predetermined 128-bit plaintext to the target device. Next, they gather power traces of the data bus. After some amount of time, a dataset of known input and power traces are obtained. Then, they guess at a key for each input data, XOR those 8 bits (in total 128, 192, or 256), and run them into S-box to obtain a hypothetical output value. The output value is evaluated at its Hamming weight. For each hypothetical key, the attackers generate the value of Hamming weight that is seen on the collected power traces at some point in time (when the key value goes over S-box). It seems that at specific time, the guessed key value that is the closest match to the measured power traces must be the correct key value. To judge the match, the Pearson correlation coefficient is used. The pearson correlation coefficients are between -1 and 1, and the closer to -1 or 1, the stronger the match. The key with the highest pearson correlation coefficient is guessed as the correct key. These processes are repeated a certain number of times (16, 24 or 32), with 8 bits as a unit.

2.3. Masking countermeasure

Masking countermeasures are one of the methods against the power analysis attacks described above. This section describes masking countermeasures. There are two types of masking countermeasures. One is Boolean masking using logical operations and the other is arithmetic masking using arithmetic operations. Since Boolean masking is used in this study, this section describes this method [20].

Let pi be the i-th byte of the plaintext, ki be the i-th byte of the key, and SubBytes substitution be $Sbox($); the first process of AES is expressed as in (1) and (2).

$$a = p_i \oplus k_i \tag{1}$$

$$b = Sbox(a) \tag{2}$$

This b value is vulnerable to attack and must be protected. Therefore, if $m1$ and $m2$ are random masks, the first process of AES with masking countermeasures is expressed as in (3), (4), and (5).

$$a' = (p_i \oplus m_i) \oplus k_i \tag{3}$$

$$Sbox'(x) = Sbox(x \oplus m_i) \oplus m_2 \tag{4}$$

$$b' = Sbox'(a') \tag{5}$$

This b' value is independent of the key due to the random mask. Therefore, side-channel attack on this b'cannot identify the key. At the end of the final round, the ciphertext is output by removing the mask according to (6).

$$c = b' \oplus m_2 \tag{6}$$

2.4. T-test

T-test is one of the methods used to evaluate side-channel attack resistance [21]. It examines whether the mean and variance of two datasets are identical. One dataset is power traces with random plaintext input and the other dataset is power traces with fixed plaintext input. T-test indicates the variation of power traces at the same time. It calculates the T-value according to the following equation. The larger the T-value, the lower the side-channel attack resistance and the less secure the circuit. The T-value threshold is 4.5.

$$\mathrm{T} = \frac{|X_A - X_B|}{\sqrt{\frac{S_A^2}{N_A} + \frac{S_B^2}{N_B}}}$$

In this case, N_A and N_B are the number of samples, X_A and X_B are the sample means, and S_A and S_B are standard deviation. A and B are two sets of datasets. In this paper, T-values are evaluated in absolute values, as shown above.

3. AES CIRCUIT DESIGNS

3.1. High-level synthesis

We design circuits via high-level synthesis and logic synthesis. Figure 1 shows the experimental flow. The left block shows the circuit design, and the right block shows the power analysis and T-test. In this section, we introduce the circuit design method.

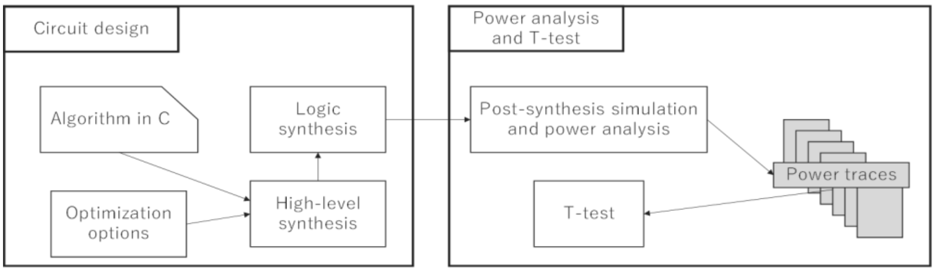


Figure 1. Experimental flow thai is circuit design, power analysis and T-test

High-level synthesis is a technique that automatically generates RTL circuits from high-level languages such as C/C++. We use Vivado HLS as a high-level synthesis tool. Vivado HLS has an optimization feature that allows designers to change the performance of circuits. Using optimization, we design twelve AES circuits from AES programs without a masking countermeasure and fifteen AES circuits from AES programs with a masking countermeasure. We then employ six AES circuits without a masking countermeasure and five AES circuits with a masking countermeasure, according to Pareto-optimal. The AES program without a masking countermeasure is quoted in the CHStone benchmark [22]. The AES program with a masking countermeasure is quoted in [23]. The simulation period for each AES circuit is 10 ns. Blömer *et al*. [24] showed that there may be a weakly masking countermeasure. However, the masked program [23] quoted in this paper was guaranteed to be secure in [25]. The algorithm of AES without masking countermeasure is shown in Figure 2. This algorithm is a basic AES algorithm where SubBytes, ShiftRows, MixColumn and AddRoundKey are processed in sequence. These processes are repeated ten times and all keys are generated by KeySchedule function prior to the encryption process. The algorithm of AES with a masking countermeasure is shown in Figure 3. Figure 3(a) shows the top function. Top function is almost the same as the program [22]. The only difference is the masking process with the reconfigure function. Figure 3(b) illustrates how to conduct the masking countermeasure using sBox_Masked in SubBytes. Figure 3(c) shows the reconfigure function. This function outputs sBox_Masked to mask the Sbox. This program conducts the masking countermeasure to Sbox; thus, Sbox is considered a more challenging target for a side-channel attack.

```
chstone_encrypt ( int  statemt[32], int  key[32], int  type ){
        KeySchedule( type, key ) ;
        AddRoundKey( statemt, type, 0 ) ;
        for ( int i = 0; i <= round_val + 9; ++1 ){
                ByteSub_ShiftRow( statemt, nb ) ;
                MixColumn_AddRoundKey( statemt, nb, i ) ;
        }
        ByteSub_ShiftRow( statemt, nb ) ;
        AddRoundKey( statemt, type, i ) ;
        return 0;
```

Figure 2. AES algorithm without masking countermeasure

The optimization for the AES program without masking measures is summarized in Table 1. The pipeline initiation interval indicates the strength of the pipeline shown in Figure 4. Pipelining is a technique that optimizes programs to schedule instruction efficiently. In Figure 4, RD means “data read”. CMP means “computation”. WR means “data write”. Figure 4(a) shows the process without pipelining. Figure 4(b) shows the pipelining process with initiation interval = 1. Figure 4(c) shows the pipelining with initiation interval=2. As shown in Figure 4, if the initiation interval is 1, the next process is set to start one clock later. Additionally, if the initiation interval is 2, the next process is set to start two clocks later. To compare Figures 4(a) and 4(b), Figure 4(a) that has no pipelining needs 9 clock cycles to conduct this instruction, however Figure 4(b) that has pipelining needs only 5 clock cycles. This is an advantage of pipelining. Thus, one can imagine that the larger the value of the initiation interval, the longer the execution time. For AES circuits without masking countermeasures, the initiation interval scheduled by the Vivado HLS are II=2, 3, and 4. At II=1, the scheduling is not possible, and at II = 5 and above, the performance does not change. The optimization of the AES program with masking countermeasures is summarized in Table 2. For AES programs with masking countermeasures, scheduling is possible even at an initiation interval of 1.

```
encrypt ( block_t  PlainText, key_t  Key,  block_t  MaskIn, block_t  MaskOut ) {
        reconfigure( MaskIn, MaskOut)
        block_t  Statemt = PlainText ;
        key_t  RoundKey = Key ;
        Statemt = addRoundKey( Statemt, RroundKey ) ;
        for( int round = 1; round < 10; round++) {
                roundKey = updateKey( RoundKey, round ) ;
                Statemt = subBytes( Statemt, round ) ;
                Statemt = shiftRows( Statemt );
                Statemt = (( round == 9 )) ? Statemt : mixcolimns( Statemt )) ;
                Statemt = addRoundKey( Statemt, RoundKey ) ;
        }
        Statemt = remaskOutput( Statemt, MaskIn, MaskOut ) ;
        return Statemt ;
}
```

(a)

```
sbox_t  sBox_Masked[2][SBOX_COUNT][SBOX_RANGE] ;
block_t  sLayer( block_t  Statemt, round_idx_t  round ) {
        block_t  NewState ;
        for( int i = 0; i < 16; i++ ) {
                NewState( i *4 + 3, i * 4 ) = sBox_Masked[round%2][state( i * 4 + 3, i * 4)] ;
        }
        return NewState ;
}
```

(b)

```
void reconfigure ( block_t  MaskIn, block_t  MaskOut ) {
        block_t  mask1[2] = { MaskOut, MaskIn } ;
        block_t  mask2InvP[2] = { pInvLayer( MaskIn ), pInvLayer( MaskOut ) } ;
        for( int i = 0; i < 2; i++) {
                for( int j = 0; j < SBOX_RANGE; j++ ) {
                        for( int k = 0; k < SBOX_COUNT; k++ ) {
                                sbox_t  idx = mask1[ i ]( 4 * k + 3, 4 + k ) ^ j ;
                                sbox_t  val = sBoxClean[ j ] ^ mask2InvP[ i ]( 4 * k + 3, 4 * k ) ;
                                sBox_Masked[ i ][ k ][ idx ] = val ;
                        }
                }
        }
}
```

(c)

Figure 3. The masked AES algorithm, (a) top function, (b) sbox layer, and (c) reconfiguration of sboxes

Table 1. Optimization without masking

Parameter	Description
Default	The circuit without optimization
Inline and pipeline (II = 2)	The circuit with inlining and pipelining with initial interval = 2 for FOR loop
Pipeline (II = 2)	The circuit with pipelining of initiation interval = 2 for FOR loop
Pipeline (II = 3)	The circuit with pipelining of initiation interval = 3 for FOR loop
Pipeline (II = 4)	The circuit with pipelining of initiation interval = 4 for FOR loop
Pipeline (func)	The circuit with pipelining of initiation interval = 2 for each function

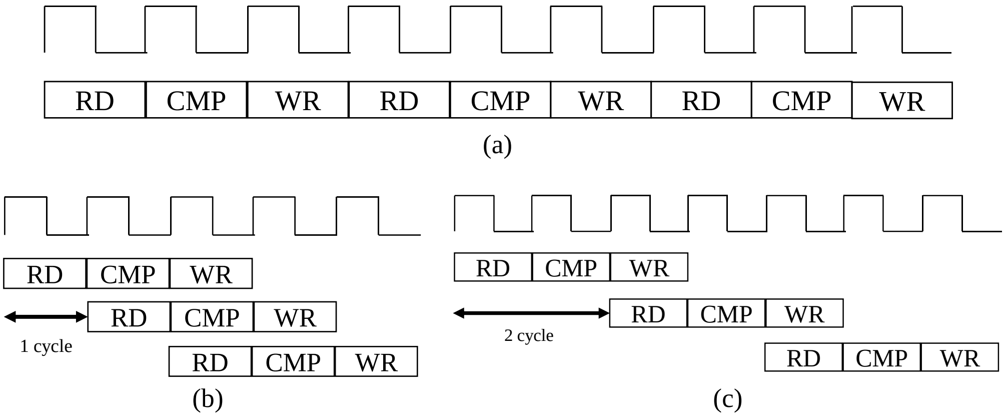


Figure 4. Description of pipelining initial interval, (a) without pipelining, (b) pipelining with initial interval=1, and (c) pipelining with initial interval =2

Table 2. Optimization with masking

Parameter	Description
Default	The circuit without optimization
Pipeline (function, II = 1)	The circuit with pipelining of initiation interval = 1 for each function
Pipeline (II = 1)	The circuit with pipelining of initiation interval = 1 for FOR loop
Pipeline (II = 2)	The circuit with pipelining of initiation interval = 2 for FOR loop
Inline and Pipeline (II = 3)	The circuit with inlining and pipelining with initial interval = 3 for FOR loop

3.2. Synthesis result

After high-level synthesis, we design AES circuits using logic synthesis. Logic synthesis is the process of implementing logic circuits from very high speed integrated circuit hardware description language (VHDL) or hardware description language (HDL). This study uses logic synthesis on FPGAs, and the target FPGA board is the Zynq 7,000. FPGAs are well researched in that they are reprogrammable, but they have characteristics that make them vulnerable to power analysis attacks [26]. We use Vivado as the logic synthesis tool. Vivado can simulate implemented circuits in FPGAs. Therefore, the AES circuits in this study are not mounted on the actual hardware but run entirely on the simulation. Since there is no effect from the external environment, the experiment has an advantage, as it is conducted in an ideal environment. The number of clock cycles and resources after logic synthesis for each AES circuit is shown in Table 3 and Figure 5. Figure 5(a) shows the relationship between clock cycles and resources for the AES circuits without masking countermeasures. Figure 5(b) shows the relationship for the AES circuits with masking countermeasures. Resources refer to the number of slices. Slices are fundamental hardware resources in FPGAs, typically consisting of look up tables (LUTs) and flip flops. In case of the FPGA used in our work, a slice contains six 6 input LUTs. We use the number of slices to evaluate the circuit size. Therefore, the larger the resources, the larger the circuits area. In Table 3 the upper rows show the number of AES circuits without a masking countermeasure and Table 4 the lower rows show the number of AES with a masking countermeasure. In Figure 5, the horizontal axis is the number of clock cycles and the vertical axis is the number of resources. We can see the relationship between clock cycles and resources from Figure 5. AES circuits without masking are inversely proportional and AES circuits with masking are close to proportional. Since the source codes for high-level synthesis are different, the impact of the optimization of the two types of AES circuits is very different. In terms of improving circuit performance, the AES circuit with masking is superior, allowing for the implementation of a circuit with higher performance and smaller area. For designers, it is essential to devise a method of writing source code.

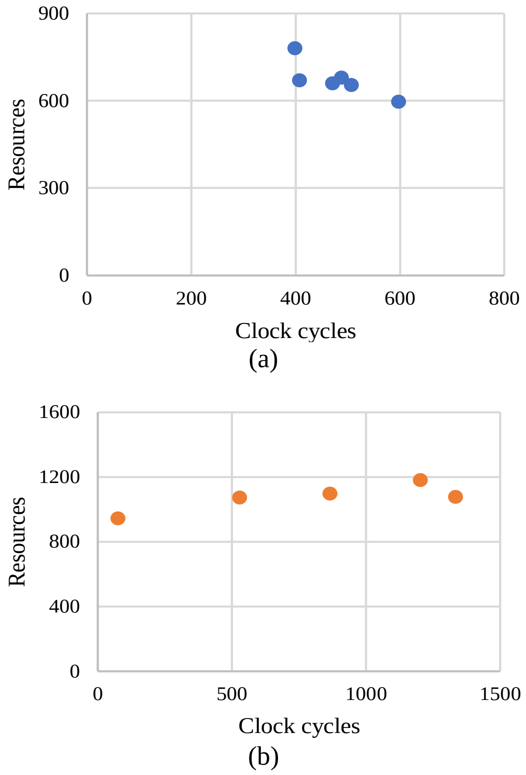


Figure 5. Relationship between clock cycles and resources, (a) AES circuits without masking countermeasures and (b) AES circuits with masking countermeasures

Table 3. Number of clock cycles and resources (slices) for AES circuit without mask

Parameter	Default	Pipeline (func, II=2)	Inline and pipeline (II = 2)	Pipeline (II=2)	Pipeline (II=3)	Pipeline (II=4)
Clock cycles	487	597	398	407	470	506
Resources	679	596	780	670	660	654

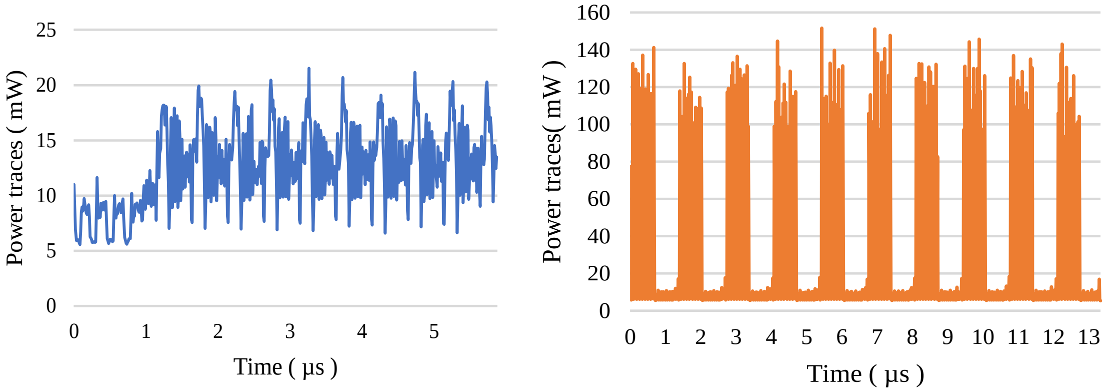
Table 4. Number of clock cycles and resources (slices) for masked AES circuit

Parameter	Default	Pipeline (func, II = 1)	Inline and pipeline (II=3)	Pipeline (II=1)	Pipeline (II=2)
Clock cycles	1334	76	1203	530	866
Resources	1076	944	1180	1073	1098

4. EVALUATION OF POWER SIDE-CHANNEL LEAKAGE

4.1. Power analysis and T-test

We analyze the power traces and evaluate side-channel attack resistance for the AES circuit designed in section 3. T-test is employed to evaluate side-channel attack resistance [27]. To carry out the power analysis, we use Vivado and the power analysis tool developed in [28]. In Figure 1, the right block shows power analysis and T-test method. In this study, power traces are also measured on the simulation. This environment removes human error or minute differences in measurement methods. Therefore, the evaluation considers severe conditions for cryptographic circuits, which tend to result in higher side-channel attack resistance. Power traces are analyzed from switching activity. Switching activity records changes in signals as the circuit operates, and these recorded changes can analyze power traces. Switching activity interface format (SAIF) files can record the switching activity. The power analysis tool [28] can generate a lot of SAIF files from value change dump (VCD) file. VCD file records whole signal changes and it can be generated by synthesis simulation. The SAIF files are obtained in the same amount of clock cycles. Each SAIF file holds power values. The waveforms obtained from the power values are shown in Figure 6. Figure 6(a) shows the power trace for an AES circuit without masking countermeasures and Figure 6(b) shows the power trace for an AES circuit with masking countermeasures by simulation. The horizontal axis depicts the time and the vertical axis depicts the power traces. The results are for the AES circuit with default performance; this means no optimization options are used. The shape of waveforms is slightly different; however, we can see the ten cryptographic operations.



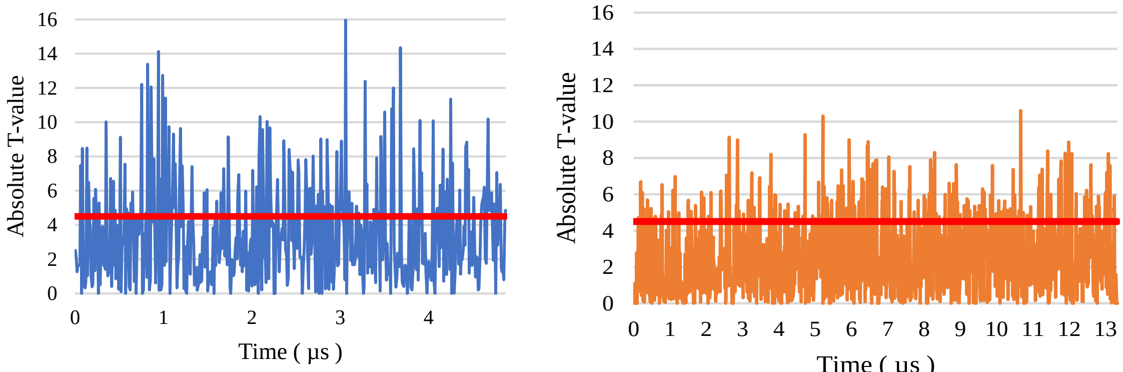
(a) (b)

Figure 6. Power traces obtained by simulation, (a) power trace of AES circuit without masking and (b) power trace of masked AES circuit

Next, we discuss the T-test [21]. As mentioned in section 2.4, the T-test is a method used to evaluate the side-channel attack resistance. The T-test as shown in.

$$T = \frac{|X_A - X_B|}{\sqrt{\frac{S_A^2}{N_A} + \frac{S_B^2}{N_B}}}$$

T-values are computed at 10 ns intervals, which is the same as the clock cycle. Therefore, the same number of T-values are gathered as the number of clock cycles in AES circuits. First, 30 power traces from 30 encryptions are obtained to compute the T-value. Then, 20 power traces are obtained from random 128-bit plaintexts (as shown above in Eq. A) and 10 power traces (B in the above formula) from fixed 128-bit plaintexts. The 128-bit cryptographic key is fixed. The amount of traces used in the experiments looks low, but we conduct experiments by simulation that is considered ideal noiseless environments. Therefore 30 power traces are not so little. Also, simulation time is extremely slower than real experiments time. We cannot obtain a lot of traces. The T-test results are shown in Figure 7. Figure 7(a) shows the result for the AES circuit without masking countermeasures and Figure 7(b) shows the result for the AES circuit with masking countermeasures. The horizontal axis depicts the time and the vertical axis depicts the absolute T-value.



(a) (b)

Figure 7. T-test results, (a) T-test of AES circuit without masking and (b) T-test of AES masked circuit

The results are for the AES circuit with default performance. There is a red line at the T-value threshold of 4.5, because the T-value threshold is set at 4.5. From Figure 7, we can see that even AES circuits do not secure circuits. Most literature focuses on whether the absolute T-value exceeds 4.5 of the T-value threshold. However, the purpose of this paper is to compare side-channel attack resistance based on the performance of each AES circuit. Satoh *et al*. [29] and Francois [30] discuss the importance of security evaluation. The tools used in this study is as:

- Vivado HLS: Optimization and high-level synthesis;
- Vivado: synthesis simulation and exporting VCD file;
- Power analysis tool [28]: Generating SAIF files.

In this paper, to compare AES circuits equally, we evaluate side-channel attack resistance based on the following four metrics:

- $P_{t\leq 4.5}$: percentage of T-values lower than or equal to 4.5;
- $N_{t\geq 4.5}$: number of times T-values is 4.5 or higher;
- T_{max}: maximum T-value;
- T_{ave}: average T-value.

$P_{t\leq 4.5}$ shows the percentage of T-values distributed below 4.5 for the entire AES circuit. In Figure 7, the percentage below the red line is shown; since the T-value threshold is 4.5, $P_{t\leq 4.5}$ is higher. The higher the T-value, the higher the side-channel attack resistance. $N_{t\geq 4.5}$ indicates the number of times the T-value is greater than 4.5. In Figure 7, the red line $N_{t\geq 4.5}$ indicates the number of times that the distribution is above the red line. $N_{t\geq 4.5}$ The smaller T-value is 4.5, the higher the side-channel attack resistance. T_{max} indicates the maximum value of T. Since the T value indicates the variation of the power of 30 encryptions, the larger the T value, the lower the side-channel attack resistance. Therefore, the smaller T_{max} is smaller, the higher the side-channel attack resistance. T_{ave} indicates the average value of the T-value. Similarly, the smaller T_{ave}, the higher the side-channel attack resistance. We evaluate the side-channel attack resistance of AES circuits from the above four metrics. One of the contributions of this paper is that security is now evaluated based on the above four metrics.

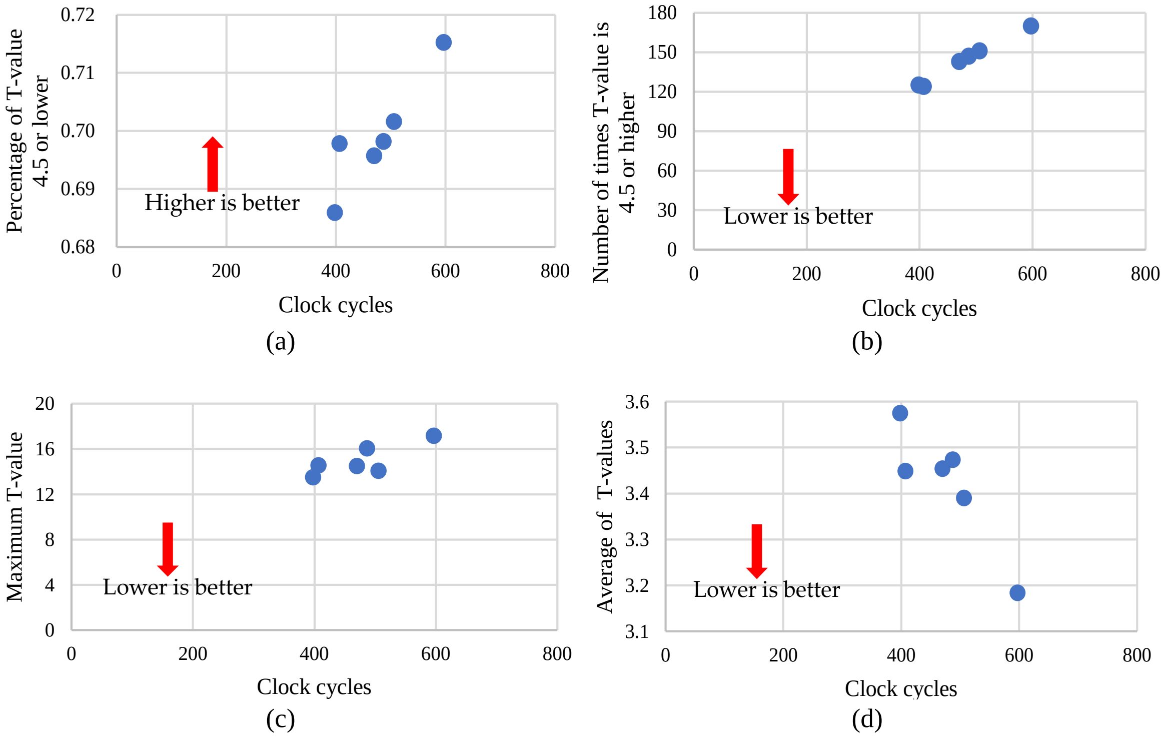
4.2. Evaluation of AES circuits without masking

As mentioned in section 4.1, the side-channel attack resistance is evaluated from four metrics based on a T-test. Figures 8 and 9 show the evaluation of side-channel attack resistance of AES circuits without masking countermeasures. Figure 9 shows the number of clock cycles and the results of the four metrics. The horizontal axis is the number of clock cycles, and the vertical axes are $P_{t\leq 4.5}$, $N_{t\geq 4.5}$, T_{max} and T_{ave}, respectively. Figure 9 shows the number of resources and the results of the four metrics. The horizontal axis is the number of resources, and the vertical axes are $P_{t\leq 4.5}$, $N_{t\geq 4.5}$, T_{max} and T_{ave}, respectively. Table 5 shows the correlation coefficient between the performance and side-channel attack resistance of AES circuits without masking countermeasures.

Figure 8(a) shows a positive correlation between the number of clock cycles and $P_{t\leq 4.5}$. The higher the $P_{t\leq 4.5}$, the higher the side-channel attack resistance. Therefore, the smaller the number of clock cycles, the lower the side-channel attack resistance. Figure 8(b) shows a positive correlation between the number of clock cycles and $N_{t\geq 4.5}$. The higher the $N_{t\geq 4.5}$, the lower the side-channel attack resistance. Therefore, the smaller the number of clock cycles, the higher the side-channel attack resistance. Figure 8(c) shows a positive number of clock cycles and $T_{\max}$. The higher the $T_{\max}$, the lower the side-channel attack resistance. Therefore, the smaller the number of clock cycles, the higher the side-channel attack resistance. Figure 8(d) shows a negative correlation between the number of clock cycles and T_{ave}. The higher the T_{ave}, the lower the side-channel attack resistance. Therefore, the smaller the number of clock cycles, the lower the side-channel attack resistance.

Figure 9(a) shows a negative correlation between the number of resources and $P_{t\leq 4.5}$. Therefore, the smaller the number of resources, the higher the side-channel attack resistance. Figure 9(b) shows a negative correlation between the number of resources and $N_{t\geq 4.5}$. Therefore, the smaller the number of resources, the lower the side-channel attack resistance. Figure 9(c) shows a slight negative correlation between the number of resources and T_{max}. Therefore, the smaller the number of resources, the lower the side-channel attack re sistance. Figure 9(d) shows a positive correlatio n between the number of resources and T_{ave}. Therefore, the smaller the number of resources, the higher the side-channel attack resistance.

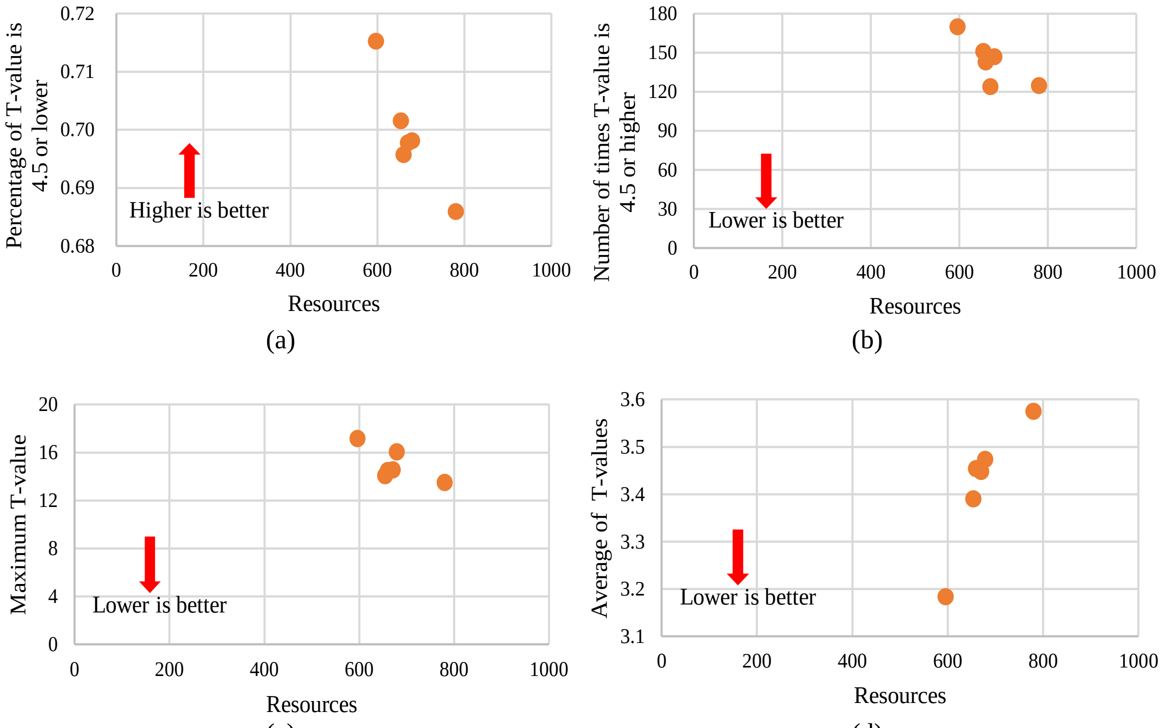
The results in Figures 8 and 9 show a correlation between the performance (number of clock cycles and nu mber of resources) and side-channel attack resistance of AES circuits without masking countermeasures. However, the strength of side-channel attack resistance varies depending on the security evaluation metrics. For example, the results in Figures 8(a) and 8(d) show that the higher the number of clock cycles, the higher the side-channel attack resistance. In contrast, Figures 8(b) and 8(c) show that the smaller the number of clock cycles, the higher the side-channel attack resistance. The graphs in Figure 9 show contrasting results, as there is a trade-off between the number of clock cycles and resources.



(a) (b)

(c) (d)

Figure 8. Clock cycles and side-channel attack resistance for AES without masking, (a) relationship of clock cycles and $P_{t \leq 4.5}$, (b) relationship of clock cycles and $N_{t \geq 4.5}$, (c) relationship of clock cycles and T_{max}, and (d) relationship of clock cycles and T_{ave}



(a) (b)

(c) (d)

Figure 9. Resources and side-channel attack resistance for AES without masking, (a) relationship of resources and $P_{t \leq 4.5}$, (b) relationship of resources and $N_{t \geq 4.5}$, (c) relationship of resources and T_{max}, and (d) relationship of resources and T_{ave}

Table 5. Correlation coefficient between performance and different security metrics for AES without masking

Parameter	$P_{t\leq4.5}$	$N_{t\geq4.5}$	T_{max}	T_{ave}
Clock cycles	0.66	0.98	0.58	-0.81
Resources	-0.79	-0.74	-0.27	0.98

Table 6 summarizes the results of Figures 8 and 9. Higher performance indicates a smaller number of clock cycles, and lower cost indicates a smaller number of resources. In general, high performance and low cost should be designers' main targets. Additionally, since there is a trade-off between performance and cost, higher performance circuits tend to have a larger cost. Table 6 shows that when we try to design higher performance circuits, the circuits are more secure in terms of $N_{t\geq4.5}$ and T_{max}, but less secure in terms of $P_{t\leq4.5}$ and T_{ave}. On the other hand, when we try to design lower cost circuits, the circuits are less secure in terms of $N_{t\geq4.5}$ and the T_{max}, but more secure in terms of $P_{t\leq4.5}$ and T_{ave}. The results for AES circuits without masking countermeasures show that side-channel attack resistance varies depending on the security metrics. When we design AES circuits without masking countermeasures and consider security, the design method may differ depending on which metrics are important.

Table 6. Side-channel attack resistance with different security metrics for AES without masking

Parameter	$P_{t\leq4.5}$	$N_{t\geq4.5}$	T_{max}	T_{ave}
Higher performance	×	○	○	×
Lower cost	○	×	×	○

4.3. Evaluation of masked AES

Figures 10 and 11 show the evaluation of side-channel attack resistance of masked AES circuits. Figure 10 shows the number of clock cycles and the results of the four metrics. The horizontal axis is the number of clock cycles, and the vertical axes are $P_{t\leq4.5}$, $N_{t\geq4.5}$, T_{max} and T_{ave} respectively. Figure 11 shows the number of resources and the results of the four metrics. The horizontal axis is the number of resources, and the vertical axes are $P_{t\leq4.5}$, $N_{t\geq4.5}$, T_{max} and T_{ave}, respectively. Table 7 shows the correlation coefficient between the performance (number of clock cycles and number of resources) and the side-channel attack resistance of masked AES circuits.

Table 7. Correlation coefficient between performance and different security metrics for masked AES

Parameter	$P_{t\leq4.5}$	$N_{t\geq4.5}$	T_{max}	T_{ave}
Clock cycles	-0.20	0.99	0.74	0.89
Resources	0.12	0.78	0.87	0.49

Figure 10(a) shows that there is no correlation between the number of clock cycles and $P_{t\leq4.5}$. Figure 10(b) shows a positive correlation between the number of clock cycles and $N_{t\geq4.5}$. The higher the $N_{t\geq4.5}$, the lower the side-channel attack resistance. Therefore, the smaller the number of clock cycles, the higher the side-channel attack resistance. Figure 10(c) shows a positive correlation between the number of clock cycles and T_{max}. The higher the T_{max}, the lower the side-channel attack resistance. Therefore, the smaller the number of clock cycles, the higher the side-channel attack resistance. Figure 10(d) shows positive correlation between the number of clock cycles and T_{ave}. The higher the T_{ave}, the lower the side-channel attack resistance. Therefore, the smaller the number of clock cycles, the higher the side-channel attack resistance.

Figure 11(a) shows that there is no correlation between the number of resources and $P_{t\leq4.5}$. Figure 11(b) shows a positive correlation between the number of resources and $N_{t\geq4.5}$. The smaller the number of resources, the higher the side-channel attack resistance. Figure 11(c) shows a positive correlation between the number of resources and T_{max}. The smaller the number of resources, the higher the side-channel attack resistance. Figure 11(d) shows a slight positive correla tion between the number of resources and T_{ave}. The smaller the number of resources, the higher the side-channel attack resistance.

The results in Figures 10 and 11 show that the performance (number of clock cycles and number of resources) of masked AES circuits and side-channel attacks have $P_{t\leq4.5}$. There is some correlation between them, except for $P_{t\leq4.5}$. In contrast with the AES circuits without masking countermeasures, there is no change in side-channel attack resistance in terms of security metrics.

Similarly, Table 8 summarizes the results of Figures 10 and 11. According to Table 8, in terms of $N_{t\geq4.5}$, T_{max}, and T_{ave}, we can see that the higher performance or the lower cost of the masked AES circuits have higher side-channel attack resistance. The results for masked AES circuits show that the safest circuit is the most ideal.

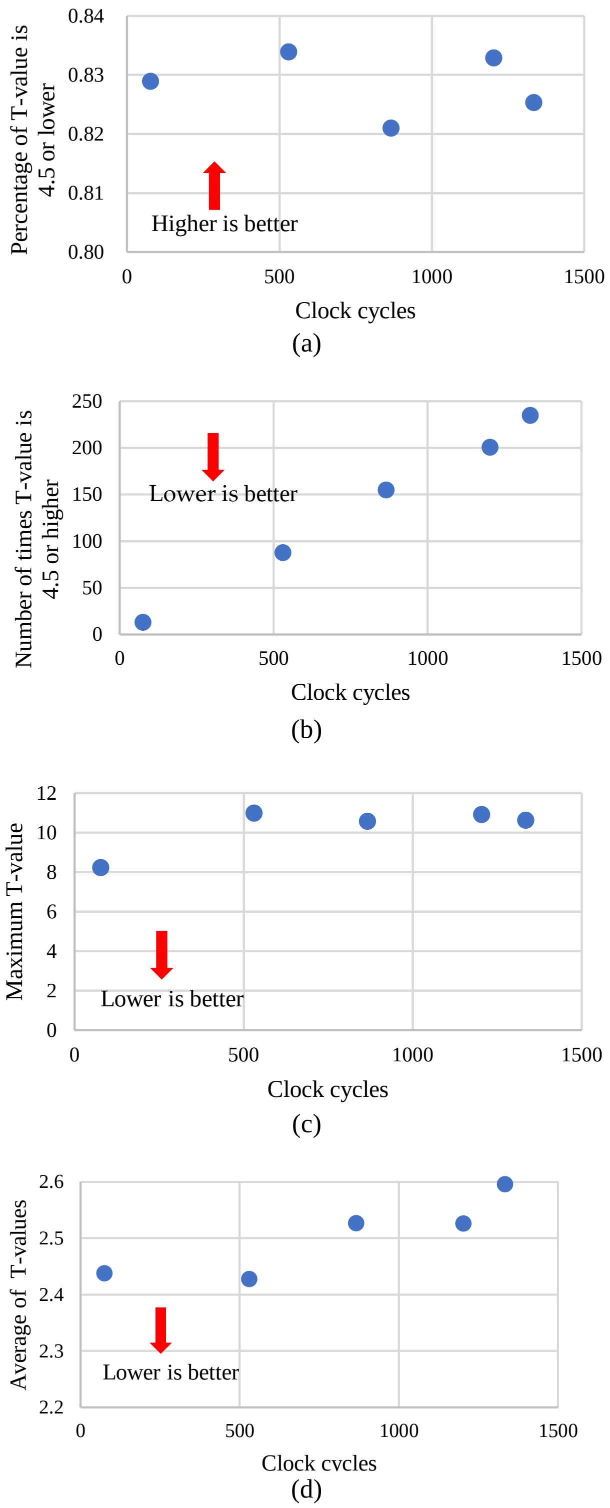


Figure 10. Clock cycles and side-channel attack resistance for masked AES, (a) relationship of clock cycles and $P_{t\leq4.5}$, (b) relationship of clock cycles and $N_{t\geq4.5}$, (c) relationship of clock cycles and T_{max}, and (d) relationship of clock cycles and T_{ave}

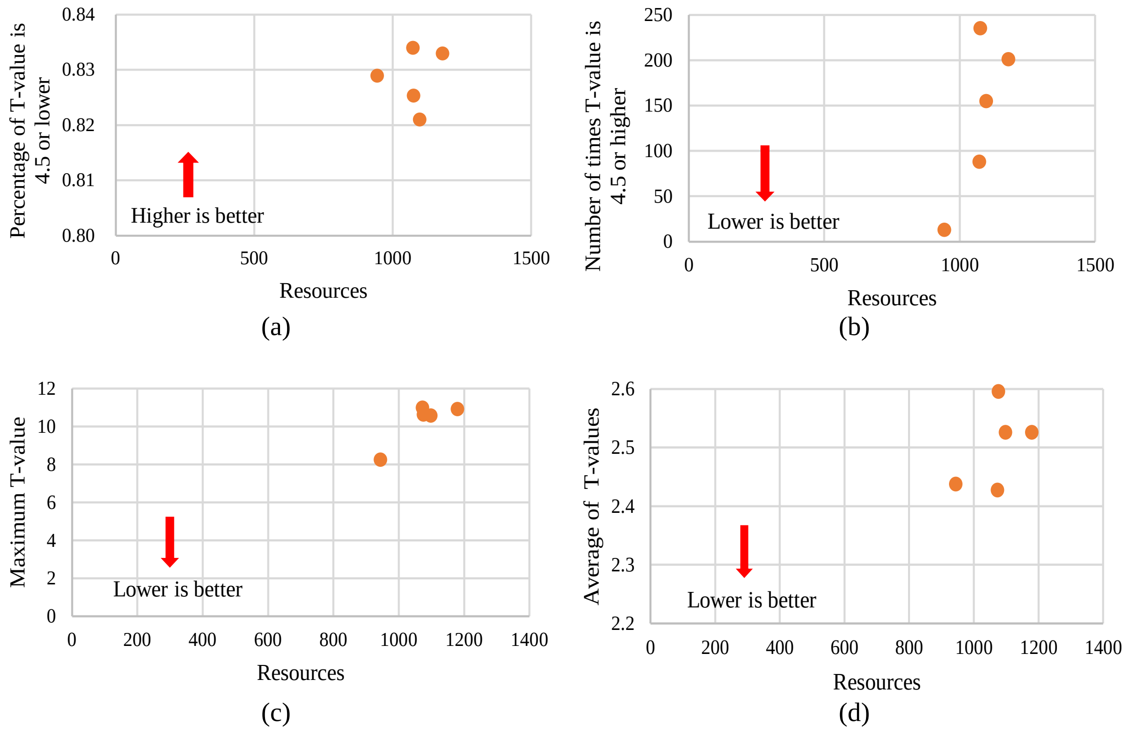


Figure 11. Resources and side-channel attack resistance for masked AES, (a) relationship of resources and $P_{t\leq 4.5}$, (b) relationship of resources and $N_{t\geq 4.5}$, (c) relationship of resources and T_{max}, and (d) relationship of resources and T_{ave}

Table 8. Side-channel attack resistance with different security metrics for masked AES

Parameter	$P_{t\leq 4.5}$	$N_{t\geq 4.5}$	T_{max}	T_{ave}
Higher performance	-	○	○	○
Lower cost	-	○	○	○

The results for masked AES circuits show that side-channel attack resistance depends on the circuits' performance. When we design masked AES circuits and consider security, a better performing circuit provides higher side-channel attack resistance. Additionally, in this study, the masked AES circuits do not possess sufficient security features, which is different from the observations in previous work such as [23]-[25]. One reason for this is that our evaluation is based on simulation. Simulation is a noiseless ideal environment that is severe for cryptographic circuits. Although the masked AES circuits are not perfectly safe, we observe that the masked circuits tend to be safer than the circuits without masking. It should be noted that the goal of this work is not evaluation of masking, but studying the impacts of high-level optimizations on the side-channel leakage. In future, we plan to conduct more extensive experiments based on not only simulation but also actual implementation.

5. CONCLUSIONS

This study investigates the relationship between the performance (number of clock cycles and number of resources) and side-channel attack resistance of AES circuits. We design and evaluate AES circuits without masking countermeasures and AES circuits with masking countermeasures. From four metrics based on a T-test, we evaluate the side-channel attack resistance. There are correlations between performance and side-channel attack resistance in both types of AES circuits, but the relationship is different. For AES circuits without masking countermeasures, the results differ depending on the evaluation metrics, and designers must change their design approach depending on which evaluation metrics are important.

ACKNOWLEDGEMENTS

This work is supported partly by KAKENHI 20H00590, 20K23333, 21K19776 and 22K21276.

REFERENCES

[1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A survey on IoT security: Application areas, security threats, and solution architectures,” *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[2] J. Persial, M. Prabhu, and R. Shanmugalaksmi, “Side channel attack-survey,” *International Journal of Advanced Scientific Research and Review*, vol. 1, no. 4, pp. 54–57, 2011.

[3] M. Randolph and W. Diehl, “Power side-channel attack analysis: A review of 20 years of study for the Layman,” *Cryptography*, vol. 4, no. 2, p. 15, May 2020, doi: 10.3390/cryptography4020015.

[4] S. Mangard, “A simple power-analysis (SPA) attack on implementations of the AES key expansion,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2587, pp. 343–358, 2003, doi: 10.1007/3-540-36552-4_24.

[5] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 1666, Berlin/Heidelberg: Springer-Verlag, 1999, pp. 388–397, doi: 10.1007/3-540-48405-1_25.

[6] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, “Introduction to differential power analysis,” *Journal of Cryptographic Engineering*, vol. 1, no. 1, pp. 5–27, Apr. 2011, doi: 10.1007/s13389-011-0006-y.

[7] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 3156, 2004, pp. 16–29, doi: 10.1007/978-3-540-28632-5_2.

[8] S. B. Örs, F. Gürkaynak, E. Oswald, and B. Preneel, “Power-analysis attack on an ASIC AES implementation,” in *International Conference on Information Technology: Coding Computing, ITCC*, 2004, vol. 2, pp. 546–552, doi: 10.1109/itcc.2004.1286711.

[9] F. Dassance and A. Venelli, “Combined fault and side-channel attacks on the AES key schedule,” in *Proceedings - 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2012*, Sep. 2012, pp. 63–71, doi: 10.1109/FDTC.2012.10.

[10] M. C. McFarland, A. C. Parker, and R. Camposano, “Tutorial on high-level synthesis.,” in *Proceedings - Design Automation Conference*, 1988, pp. 330–336.

[11] G. Martin and G. Smith, “High-level synthesis: Past, present, and future,” *IEEE Design and Test of Computers*, vol. 26, no. 4, pp. 18–25, Jul. 2009, doi: 10.1109/MDT.2009.83.

[12] G. D. Micheli, *Synthesis and optimization of digital circuits*, vol. 32, no. 02. McGraw-Hill Science/Engineering/Math, 1994.

[13] L. Zhang *et al.*, “Examining the consequences of high-level synthesis optimizations on power side-channel,” in *Proceedings of the 2018 Design, Automation and Test in Europe Conference and Exhibition, DATE 2018*, Mar. 2018, vol. 2018-January, pp. 1167–1170, doi: 10.23919/DATE.2018.8342189.

[14] T. Mizuno, Q. Zhang, H. Nishikawa, X. Kong, and H. Tomiyama, “Impacts of HLS optimizations on side-channel leakage for AES circuits,” in *Proceedings - International SoC Design Conference 2021, ISOCC 2021*, Oct. 2021, pp. 53–54, doi: 10.1109/ISOCC53507.2021.9613900.

[15] T. Balihar and M. Novotny, “Influence of synthesis parameters on vulnerability to side-channel attacks,” in *2021 10th Mediterranean Conference on Embedded Computing, MECO 2021*, Jun. 2021, pp. 1–6, doi: 10.1109/MECO52532.2021.9460288.

[16] M. L. Akkar and C. Giraud, “An implementation of DES and AES, secure against some attacks,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2162, 2001, pp. 309–318, doi: 10.1007/3-540-44709-1_26.

[17] E. Oswald, S. Mangard, N. Pramstaller, and V. Rijmen, “A side-channel analysis resistant description of the AES S-box,” in *Lecture Notes in Computer Science*, vol. 3557, 2005, pp. 413–423, doi: 10.1007/11502760_28.

[18] J. Nechvatal *et al.*, “Report on the development of the advanced encryption standard (AES),” *Journal of Research of the National Institute of Standards and Technology*, vol. 106, no. 3, pp. 511–577, 2001, doi: 10.6028/jres.106.023.

[19] S. Chhabra and K. Lata, “Enhancing data security using obfuscated 128-bit AES algorithm - an active hardware obfuscation approach at RTL level,” in *2018 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2018*, Sep. 2018, pp. 401–406, doi: 10.1109/ICACCI.2018.8554562.

[20] T. S. Messerges, “Securing the AES finalists against power analysis attacks,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 1978, 2001, pp. 150–164, doi: 10.1007/3-540-44706-7_11.

[21] G. Goodwill, B. Jun, J. Jaffe, and P. Rohatgi, “A testing methodology for side-channel resistance validation,” *NIST non-invasive attack testing workshop*, vol. 7, pp. 115–136, 2011.

[22] Y. Hara, H. Tomiyama, S. Honda, and H. Takada, “Proposal and quantitative analysis of the CHStone benchmark program suite for practical c-based high-level synthesis,” *Journal of Information Processing*, vol. 17, pp. 242–254, 2009, doi: 10.2197/ipsjjip.17.242.

[23] P. Socha, “hls-crypto,” *github*, 2020, Accessed: Dec. 10, 2022. [Online]. Available: https://github.com/petrsocha/hls-crypto.

[24] J. Blömer, J. Guajardo, and V. Krummel, “Provably secure masking of AES,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 3357, 2004, pp. 69–83, doi: 10.1007/978-3-540-30564-4_5.

[25] P. Socha, V. Miškovský, and M. Novotný, “High-level synthesis, cryptography, and side-channel countermeasures: A comprehensive evaluation,” *Microprocessors and Microsystems*, vol. 85, p. 104311, Sep. 2021, doi: 10.1016/j.micpro.2021.104311.

[26] F. X. Standaert, L. V. O. T. Oldenzeel, D. Samyde, and J. J. Quisquater, “Power analysis of FPGAs: How practical is the attack?,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2778, 2003, pp. 701–711, doi: 10.1007/978-3-540-45234-8_68.

[27] W. Lei, L. Wang, W. Shan, K. Jiang, and Q. Li, “A frequency-based leakage assessment methodology for side-channel evaluations,” in *Proceedings - 13th International Conference on Computational Intelligence and Security, CIS 2017*, Dec. 2018, vol. 2018-January, pp. 590–593, doi: 10.1109/CIS.2017.00137.

[28] Q. Zhang, X. Kong, and H. Tomiyama, “A toolkit for power behavior analysis of hls-designed FPGA circuits,” in *Low-Power and High-Speed Chips and Systems (COOL Chips)*, 2021.

[29] A. Satoh, T. Katashita, and H. Sakane, “Secure implementation of cryptographic modules,” *Synthesiology English edition*, vol. 3, no. 1, pp. 86–95, 2010, doi: 10.5571/syntheng.3.86.

[30] D. Francois, “Towards fair side-channel security evaluations,” Ph.D. Thesis, Université Catholique de Louvain, 2015.

BIOGRAPHIES OF AUTHORS

Takumi Mizuno received his B.E. degree in electronic and computer engineering from Ritsumeikan University in 2021. He is in the Master's degree program at Ritsumeikan University. His research interests include design methodologies for embedded systems. He can be contacted at email: takumi.mizuno@tomiyama-lab.org.

Hiroki Nishikawa received his B.E., M.E. and Ph.D. degrees from Ritsumeikan University in 2018, 2020, and 2022, respectively. In 2022, he joined the Graduate School of Information Science and Technology, Osaka University as an assistant professor. His research interests include system-level design methodologies, design methodologies for cyber-physical systems. He is a member of IEEE, IEICE, and IPSJ. He can be contacted at email: nishikawa.hiroki@ist.osaka-u.ac.jp.

Xiangbo Kong received B.E. degree from Nankai University in 2012 and he received M.E. and Ph.D. degrees from Ritsumeikan University in 2018 and 2020, respectively. In 2020, he joined the College of Science and Engineering, Ritsumeikan University as an assistant professor. His research interests include artificial intelligence, and image processing, embedded system. He is a member of IEEE and IPSJ. He can be contacted at email: kong@fc.ritsumei.ac.jp.

Hiroyuki Tomiyama received his B.E., M.E., and D.E. degrees in computer science from Kyushu University in 1994, 1996, and 1999, respectively. He worked as a visiting researcher at UC Irvine, as a researcher at ISIT/Kyushu, and as an associate professor at Nagoya University. Since 2010, he has been a full professor with the College of Science and Engineering, Ritsumeikan University. He has served on program and organizing committees for several premier conferences including DAC, ICCAD, DATE, ASP-DAC, CODES+ISSS, CASES, ISLPED, RTCSA, FPL, and MPSoC. He has also served as an editor-in-chief for IPSJ TSLDM; an associate editor for ACM TODAES, IEEE ESL, and Springer DAEM; and a chair for the IEEE CS Kansai Chapter and IEEE CEDA Japan Chapter. His research interests include, but are not limited to, design methodologies for embedded and cyber-physical systems. He can be contacted at email: ht@fc.ritsumei.ac.jp.