

Timing issues on power side-channel leakage of advanced encryption standard circuits designed by high-level synthesis

Yuto Miura¹, Hiroki Nishikawa², Xiangbo Kong³, Hiroyuki Tomiyama¹

¹Graduate School of Science and Engineering, Ritsumeikan University, Kusatsu, Japan

²Graduate School of Information Science and Technology, Osaka University, Osaka, Japan

³Faculty of Information Engineering, Toyama Prefectural University, Toyama, Japan

Article Info

Article history:

Received Dec 7, 2023

Revised Feb 6, 2024

Accepted Mar 21, 2024

Keywords:

Advanced encryption standard

Clock period

High-level synthesis

Sampling interval

Side-channel attack

T-test

ABSTRACT

In recent years, field programmable gate array (FPGA) have been used in many internet of things (IoT) devices and are equipped with cryptographic circuits to ensure security. However, they are exposed to the risk of cryptographic keys being stolen by side-channel attacks. Countermeasures against side-channel attacks have been developed, but they are becoming more of a threat to IoT devices due to the diversity of attacks. Therefore, it is necessary to understand the basic characteristics of side-channel attacks. Therefore, this study clarifies the relationship between two timing issues, the clock period of the circuit and the power sampling interval, and the amount of side-channel leakage. We design seven advanced encryption standard (AES) circuits with different clock periods and conduct empirical experiments using logic simulations to clarify the correlation between the two timings and the amount of side-channel leakage. T-test is used to evaluate the leakage amount, which is evaluated based on four metrics. From the results, we argue that the clock period and sampling interval do not interfere with each other in the side-channel leakage amount.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Yuto Miura

Graduate School of Science and Engineering, Ritsumeikan University

1-1-1 Nojihigashi, Kusatsu, Shiga, 525-8577, Japan

Email: yuto.miura@tomiyama-lab.org

1. INTRODUCTION

In recent years, field programmable gate array (FPGA) have been used as internet of things (IoT) devices due to their low power consumption and low cost, and have greatly benefited our lives [1]–[3]. IoT devices are connected to the internet and used to communicate between devices and connect to the cloud. They handle some important sensitive information and can be attacked from outside. Therefore, they are equipped with cryptographic circuits such as AES to protect the information [4]. AES [5], [6] is an abbreviation for advanced encryption standard, an algorithm used to encrypt communication data in wireless local area network (LAN). AES was approved by National Institute of Standards and Technology (NIST) in 2001 and has been used as a standard ever since. A cryptographic circuit is a specific transformation applied to some information to make it difficult to infer the information. However, cryptographic circuits can have their cryptographic keys stolen through side-channel attacks. Side-channel attacks are attacks that identify cryptographic keys by applying statistical processing based on physical information leaked from cryptographic circuits. Among them, the power analysis attack, which estimates the cryptographic key from the power consumption caused by providing input to the cryptographic circuit, is one of the most dangerous side-channel attacks [7], [8]. Research on countermeasures against side-channel attacks has been widely conducted. Masking techniques [9] prevent attackers from observing sensitive information by inserting

random numbers during encryption. This technique makes the system resistant to existing side-channel attacks but vulnerable to new types of attacks [10]. On the attacker side, Schellenberg *et al.* [11] successfully analyzes power remotely, indicating the threat of diversifying side-channel attacks.

Therefore, side-channel attacks are a threat in IoT devices. In order to counter these attacks, it is necessary to clarify the basic characteristics of side-channel attacks. Timing issues are the basic characteristics of side-channel attacks that have not been elucidated. Timing issues are defined as timings of clock period and timings of sampling interval. Since power analysis attacks use a large number of power reports obtained at certain intervals, the amount of leakage differs with different power sampling intervals. In addition, since the power consumption of a circuit changes with the timing of clock changes, different clock periods will change the power reports, and side-channel attack leakage will change. Therefore, this paper evaluates the impact of two timings of the AES circuit on side-channel leakage. If this timing issue is not clarified, the cryptographic circuit designer cannot consider security when setting the clock.

On the other hand, when designing scalable circuits, high-level synthesis (HLS) techniques [12], [13] have attracted much attention. HLS is a technology to generate register transfer level (RTL) circuits from high-level languages such as C/C+. Generally, RTL circuits are difficult to understand, and HLS technology using a high-level language that can be easily handled is effective in circuit design. Research on HLS has been widely conducted, and it is known that circuit performance can be improved by optimization. However, it has also been found that optimization reduces side-channel attack resistance [14]. This paper is an extended version of [15], offering a broader range of experiments and more detailed analysis and results. In this experiment, AES circuits with different clock constraints are designed using HLS and simulated respectively. We evaluate the amount of side-channel leakage by performing T-tests from the power obtained from the simulations. We argue that the two timings, clock period and sampling interval, do not interfere with each other in the side-channel leakage quantities. The contributions of this paper are as follows.

- We designed seven AES circuits with different clock periods by HLS and proved that the amount of side-channel leakage varies
- We proved that the side-channel leakage amount of AES circuits varies with the sampling interval in power analysis;
- We proved that the clock period and the sampling interval do not interfere with each other in the side-channel leakage amount of an AES circuit.

The organization of this paper is as follows. Section 2 describes the design methodology of the AES circuit. In section 3, we evaluate the side-channel leakage of the designed AES circuit. Section 4 presents the conclusions of this paper and future work.

2. ADVANCED ENCRYPTION STANDARD CIRCUIT DESIGNS

This chapter describes the design and simulation methods for AES circuits. Section 2.1 describes the design of AES circuits and the previous knowledge required for this study. Section 2.2 describes the design procedure of the AES circuit and the constraints set. Section 2.3 describes the simulation method and results of the AES circuit.

2.1. Preliminaries

2.1.1. Advanced encryption standard

AES is also called a symmetric key cryptosystem, which uses the same key for encryption and decryption. Before AES, data encryption standard (DES), a symmetric key cryptosystem, was widely used. Bit is the smallest unit of information handled by a computer, and the higher the number of bits, the better the encryption performance. However, a key length of 56 bits is too short to prevent external attacks and is easily deciphered. AES, the successor to DES, allows users to choose from 128, 192, or 256 bit key lengths. AES also performs four types of conversions: SubBytes, ShiftRows, MixColumns, and AddRoundKey. The encryption process is performed by repeating these four types of transformations multiple times in a single round. This encryption process prevents external attacks and information leakage.

- SubBytes is a process that performs substitution in units of 1 byte according to the rule called S-box.
- ShiftRows is a process that shifts a matrix by 4 bytes to the left according to a certain rule.
- MixColumns is a process that performs matrix transformation in 4-byte units.
- AddRoundKey is a process that takes the exclusive OR (XOR) of a plaintext and a round key.

2.1.2. Side-channel attack

Since IoT devices and integrated circuit (IC) cards usually handle confidential information, they are equipped with cryptographic circuits such as AES to ensure security. However, side-channel attacks can lead to the theft of encryption keys. A side-channel attack is an attack to infer confidential information by

applying statistical processing based on physical information leaked from the device. There are various physical information such as power consumption, execution time, electromagnetic waves, cache, and noise [16]. Among them, power analysis attacks, which acquire and analyze power at certain intervals, have become mainstream because they are low-cost and easy to perform. Power analysis attacks include simple power analysis (SPA) [17], differential fault analysis (DFA) [18], and correlation power analysis (CPA) [19], [20]. CPA are particularly threatening in the IoT field. CPA is an attack technique to obtain a secret key by observing multiple power consumption waveforms of a cryptographic circuit in operation and statistically processing them. First, the attacker encrypts multiple prepared plaintexts with a cryptographic circuit and collects the power consumption waveforms at that time. Next, he calculates the hamming distance between the plaintext and its S-box after passing through it. The attacker assumes 256 keys for the calculation of the S-box transformation. Finally, the correlation coefficients are calculated for each assumed key value using the obtained power consumption waveform and the hamming distance. The correlation coefficient ranges from -1 to 1. The closer the absolute value is to 1, the stronger the correlation between the two values. Therefore, the value with the highest absolute value of the correlation coefficient can be inferred as the encryption key.

2.2. High-level synthesis on different clock constraints

This study uses HLS techniques for the design of AES circuits. The experimental flow of this study is shown in Figure 1. HLS is a technique to convert software programs such as C and C++ into RTL code. Compared to conventionally designed RTL code, software programs have a shorter description. Software programs also require less time for program verification. From these, a significant reduction in circuit design time can be expected [21]. We use Vivado HLS 2019.2 as our HLS tool. The circuits to be designed can be modified by setting constraints and optimizations. In this study, we focus on clock constraints. Clock constraint is a pre-set clock period that users want to operate and generates a circuit that operates at that clock period. Seven AES circuits were designed by setting clock constraints from 7.0 to 10.0 ns at 0.5 ns intervals. As a software program, we use the AES program that exists in CHStone [22], a benchmark program for HLS.

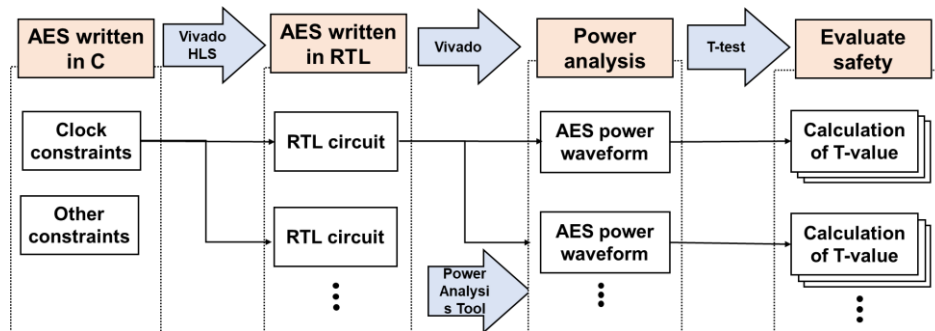


Figure 1. Flow from AES circuit design to side-channel leakage evaluation in this study

2.3. Synthesis result

Logic synthesis and logic simulation are performed using RTL code designed HLS. Logic synthesis is the implementation of logic circuits from RTL code written in Verilog hardware description language or VHDL. We employ Vivado 2019.2 for logic synthesis and logic simulation. We specify a Zynq XC7Z020 as the target device. Logic simulation of the seven synthesized AES circuits is to be performed in Vivado. Clock period of the circuits should run as fast as the set clock constraints. The reason for employing logic simulation in the experiment is that it allows for more accurate power analysis since there are no errors due to noise or environment. In this study, 20 encryptions of 128-bit random plaintexts and 10 encryptions of fixed plaintexts are performed. Logic simulation is performed in Vivado under these conditions to output value change dump (VCD) file containing information about the circuit. The number of clock cycles, execution time, number of slices, average power, and energy consumption obtained from the logic simulation are shown in Table 1.

Table 1 shows that power and energy consumption tend to decrease with larger clock constraints. They do not change when the clock constraint is larger than 9.0 ns. This is since the number of clock cycles does not change when the clock constraint becomes larger than 9.0 ns. AES circuit designed in this study did not show any correlation in the number of slices.

Table 1. Synthesis and simulation results of each AES circuit

Variable	Result						
Clock constraint [ns]	7.0	7.5	8.0	8.5	9.0	9.5	10.0
Clock cycles	5,889	5,825	5,359	5,223	4,559	4,559	4,544
Execution time [ns]	41,223	43,688	42,872	44,396	41,031	43,311	45,440
Slices	655	651	632	656	648	643	651
Average power [uW]	12,213	11,182	10,837	10,389	10,535	9,981	9,635
Energy consumption [nJ]	503	488	464	461	432	432	437

3. POWER SIDE-CHANNEL LEAKAGE ANALYSIS

This chapter provides an overview of the experiments. Section 3.1 describes the power analysis and evaluation methods. Section 3.2 describes the evaluation of the impact of clock constraints on the amount of side-channel leakage. Section 3.3 describes the evaluation of the impact of power sampling interval on side-channel leakage. Section 3.4 describes the evaluation of the impact of two timing factors on the amount of side-channel leakage.

3.1. Power analysis methods

In this study, power analysis is performed using VCD files obtained from Vivado and a power analysis tool [23]. This tool divides the VCD files output by Vivado with sampling interval and converts each into a switching activity interchange format (SAIF) file. The SAIF file is a file that contains the on/off state time of each signal. SAIF file can be input into Vivado to output power consumption. All of the divided SAIF files can be used in Python to obtain the power waveform of the circuit as shown in Figure 2. The horizontal axis is time and the vertical axis is the absolute value of T-value. These power waveforms are used to evaluate the side channel leakage.

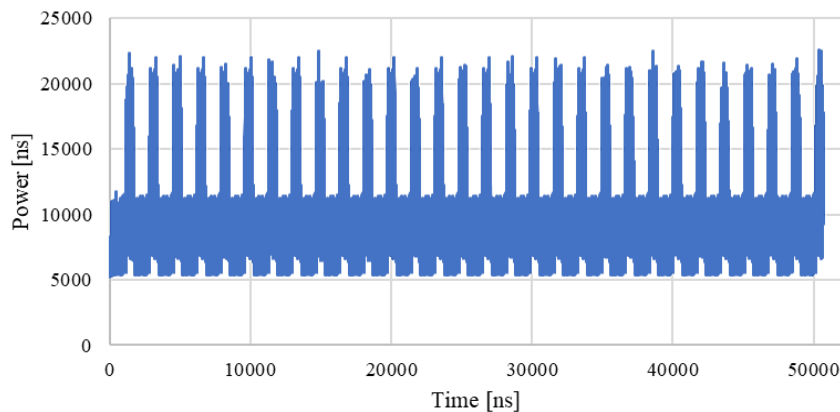


Figure 2. Power waveform obtained by simulation

In this study, Welch's T-test [24] is used to evaluate the amount of side-channel leakage. T-test is one of the metrics to evaluate the resistance to side-channel attacks. T value is calculated using the acquired power trace. T-value is a measure of the difference between the mean and variance of the two data sets to be compared and is obtained by the (1).

$$T = \frac{\overline{X_A} - \overline{X_B}}{\sqrt{\frac{S_A^2}{N_A} + \frac{S_B^2}{N_B}}} \quad (1)$$

In this paper, A and B are the two sets of data sets, N_A and N_B are the number of data sets, $\overline{X_A}$ and $\overline{X_B}$ are sample averages, and S_A and S_B are standard deviations. Datasets A and B in this experiment are random and fixed plaintexts. N is 20 and 10 times, respectively. X and S are calculated from 30 data sets. Basically, if there is variation in power consumption relative to input, the device is at risk. In other words, the higher the T value, the lower the side-channel attack resistance. The work in [25], in the telecommunications field, if the absolute value of T is greater than 4.5, the circuit is considered vulnerable to side-channel attacks. Therefore,

we adopt 4.5 as the T-value threshold. The comparison is made between fixed and random plaintexts. Since the T-value is calculated for each power, the number of T-values varies depending on the sampling interval. The results of the T test are shown in Figure 3. The horizontal axis shows time and the vertical axis shows T-values. This is the result of power analysis of an AES circuit with a clock period of 10.0 ns and sampling interval of 10.0 ns. Since FPGAs are used in a variety of situations, it is difficult to evaluate side-channel attack resistance using a single metric. Therefore, this study uses the following four metrics [26] to evaluate the amount of side-channel leakage in AES circuits. $N_{t \geq 4.5}$: Number of times T-values is 4.5 or higher; T_{ave} : Average of absolute T-values; $P_{t \geq 4.5}$: Percentage of T-values is 4.5 or higher; and T_{max} : Maximum absolute T-value.

This experiment was divided into three main parts: i) evaluating the effect of clock period on the AES circuit (clock period: 7.0 to 10.0 ns and sampling interval: 10 ns); ii) power at different sampling intervals (clock period: 10.0 ns and sampling interval: 1 to 1,000 ns); and iii) side channel leakage amount at two timings (clock period: 7.0 to 10.0 ns and sampling interval: 1 to 1,000 ns).

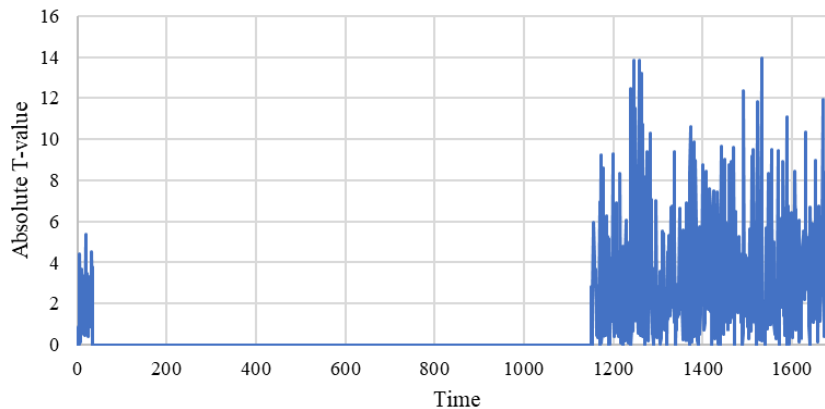


Figure 3. T-test result

3.2. Power analysis under different clock constraints

This experiment uses seven AES circuits with sampling intervals of 10 ns and clock periods of 7.0, 7.5, 8.0, 8.5, 9.0, 9.5, and 10 ns. The relationship between the clock period and the four metrics is shown in Figure 4. The vertical axis shows the result of each metrics, and the horizontal axis shows the clock period. From Figures 4(a) and (b), for T_{ave} and $P_{t \geq 4.5}$, a positive correlation is observed, and the larger the clock period, the larger the leakage. The leakage decreases when the clock period is decreased, but the energy consumption increases. There is also a critical value at which HLS becomes impossible. From Figure 4(c), for $N_{t \geq 4.5}$, a negative correlation is observed, and the smaller the clock period is, the larger the leakage is. Increasing the clock period decreases the amount of leakage but increases the execution time, which may degrade the performance of the circuit. Figure 4(d) shows that the correlation could not be confirmed for T_{max} . However, all are above 4.5, which proves that some leakage occurs.

3.3. Power analysis under different sampling intervals

This experiment measures the leakage of a single AES circuit with clock period of 10 ns at multiple sampling intervals from 1 to 1,000 ns. Figure 5 shows the relationship between the sampling intervals and four metrics. The logarithm is used for the sampling interval on the horizontal axis and the indicator $N_{t \geq 4.5}$ on the vertical axis. From Figure 5(a), for $N_{t \geq 4.5}$, a negative correlation is observed, and the narrower the sampling interval, the greater the side-channel leakage. It is expected that $N_{t \geq 4.5}$ increases when the sampling interval is small because the number of T values calculated increases. From Figures 5(b) and (c), for T_{ave} and $P_{t \geq 4.5}$, a positive correlation is observed, and the amount of side-channel leakage is larger for wider sampling intervals. Figure 5(d) shows that no correlation could be confirmed for T_{max} . However, similar to the results in 3.2, T_{max} is above 4.5 for all sampling intervals, proving that some information is leaked. For T_{ave} and $P_{t \geq 4.5}$, evaluated as a percentage of the total, the correlation was strong up to a sampling interval of 10 ns, but became weaker after that. The correlation coefficients for the four metrics from 1 to 1,000 ns, 1 to 10 ns, and 10 to 1,000 ns are shown in Table 2. These values indicate that the correlation changed greatly after 10 ns, which is the clock period. From this result, it is easy to determine the optimal sampling interval for leakage when conducting power analysis at sampling intervals smaller than the clock period.

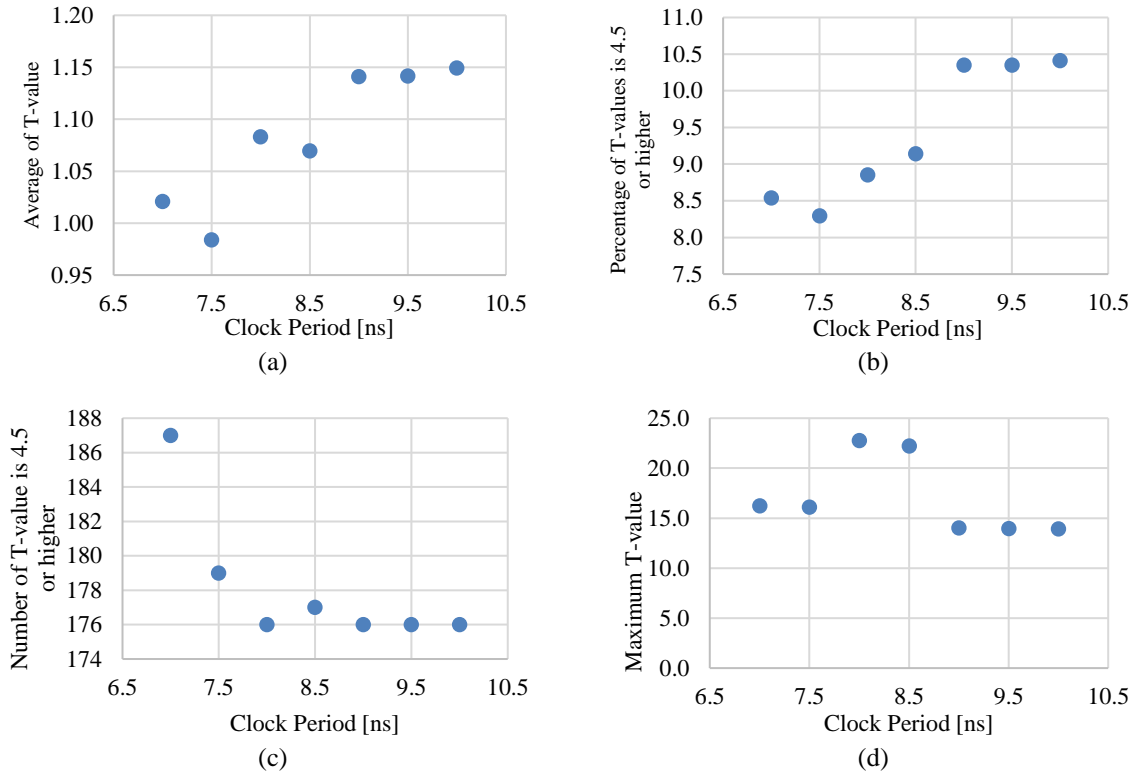


Figure 4. Correlation between energy consumption and side-channel attack resistance, (a) energy consumption and T_{ave} , (b) energy consumption and $P_{t \geq 4.5}$, (c) energy consumption and $N_{t \geq 4.5}$, and (d) energy consumption and T_{max}

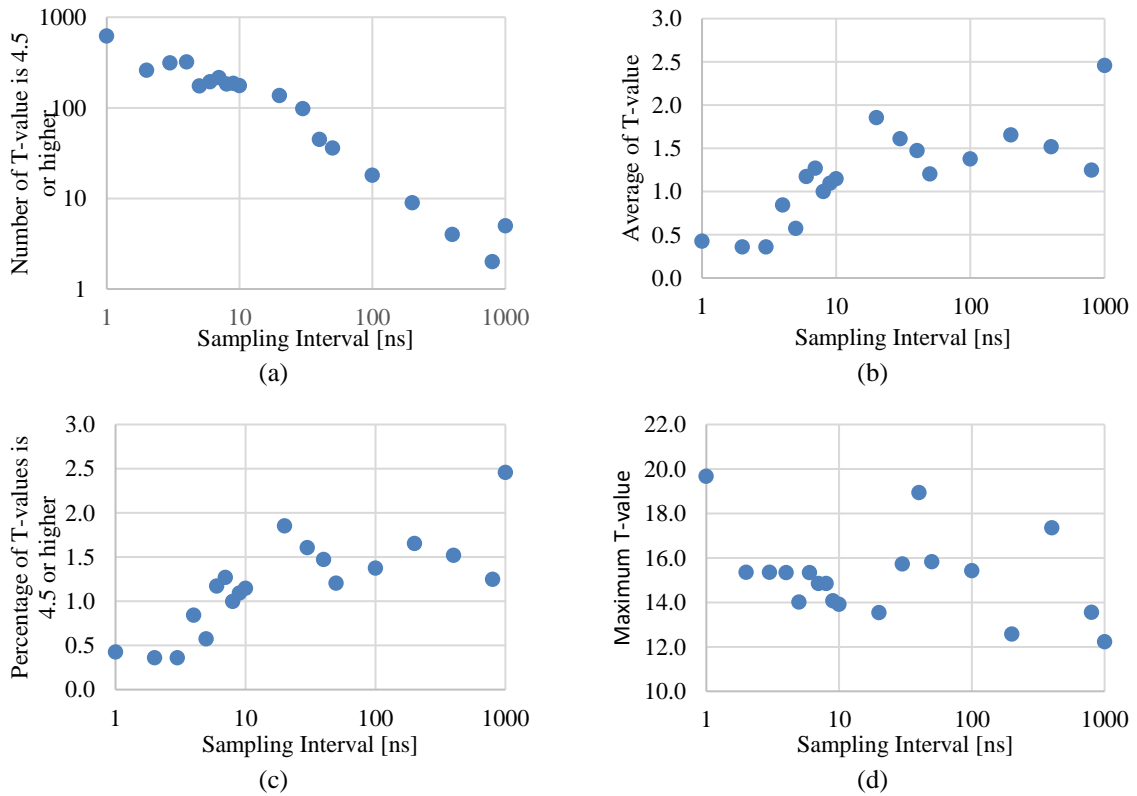


Figure 5. Correlation between sampling interval and side-channel leakage, (a) sampling interval and $N_{t \geq 4.5}$, (b) sampling interval and T_{ave} , (c) sampling interval and $P_{t \geq 4.5}$, and (d) sampling interval and T_{max}

Table 2. Correlation values at range of sampling interval

Sampling interval range [ns]	1 to 10	1 to 1,000	10 to 1,000
$N_{t \geq 4.5}$	-0.73	-0.49	-0.59
T_{ave}	0.85	0.57	0.51
$P_{t \geq 4.5}$	-0.93	-0.61	-0.49
T_{max}	-0.70	-0.37	-0.44

3.4. Evaluation of two timings for side-channel leakage

Figure 6 shows the relationship between clock period, sampling interval, and side-channel attack leakage. The horizontal axis shows the clock period, and the sampling interval is indicated by color coding. The vertical axis shows the evaluation of each metric. From Figure 6(a), for $N_{t \geq 4.5}$, the amount of side-channel leakage is higher when the clock period is larger and the sampling interval is smaller. Table 1 shows that $N_{t \geq 4.5}$ is affected by the higher clock period because the higher the clock period, the longer the execution time. Also, as in 3.3, it is expected that $N_{t \geq 4.5}$ increases when the sampling interval is small because the number of T values calculated increases. From Figures 6(b) and (c), for T_{ave} and $P_{t \geq 4.5}$, the side channel leakage is higher for larger sampling intervals and is less affected by the clock period. From Figure 6(d), for T_{max} , the side channel leakage varies, but no correlation can be observed. Since the power change in the circuit varies with the clock period, one would expect there to be a particular change in the side-channel leakage amount when it is equal to the sampling interval. However, the experimental results show that there is no special change in side-channel attack leakage.

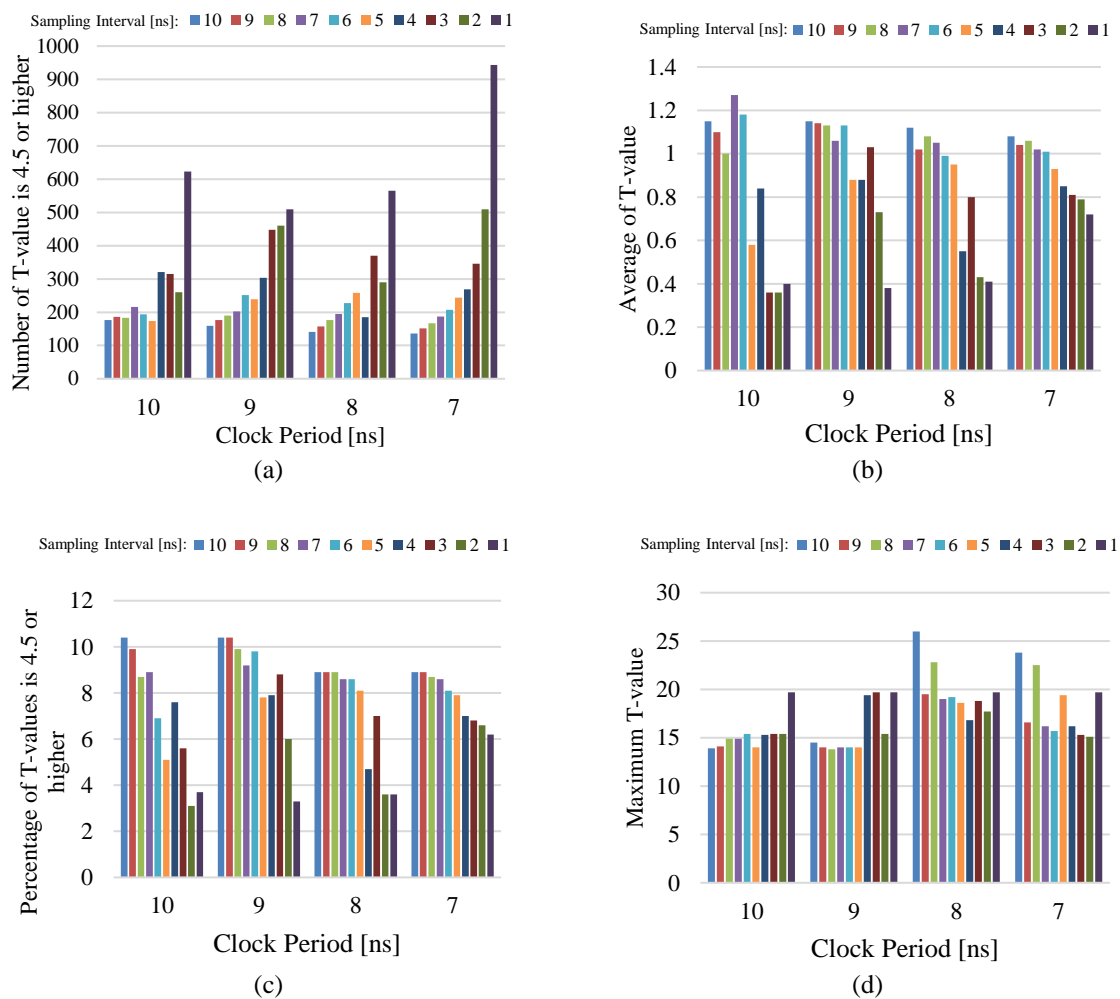


Figure 6. Correlation between clock frequency, sampling interval and side-channel attack leakage, (a) clock frequency, energy consumption, and $N_{t \geq 4.5}$, (b) clock frequency, energy consumption, and T_{ave} , (c) clock frequency, energy consumption, and $P_{t \geq 4.5}$, and (d) clock frequency, energy consumption and T_{max}

4. CONCLUSION

In this study, seven AES circuits with different clock constraints were designed from HLS, and side channel leakage amount of power analysis attack at different sampling intervals is evaluated. Correlations are confirmed between clock period and side channel leakage amount, and sampling interval and side channel leakage amount. However, the experimental results showed that clock period and sampling interval do not interfere with each other in the side-channel leakage quantities. In the future, we will establish a clock design methodology for cryptographic circuits. This will enable circuit design that allows designers to consider not only circuit performance but also security.

ACKNOWLEDGEMENTS

This work is partly supported by Japan Society for the Promotion of Science (JSPS) KAKENHI Grant Numbers 20H00590, 21K19776 and 22K21276.




REFERENCES

- [1] C. Bobda *et al.*, “The future of FPGA acceleration in datacenters and the cloud,” *ACM Transactions on Reconfigurable Technology and Systems*, vol. 15, no. 3, pp. 1–42, Sep. 2022, doi: 10.1145/3506713.
- [2] J. J. Rodriguez-Andina, M. D. Valdes-Pena, and M. J. Moure, “Advanced features and industrial applications of FPGAs—a review,” *IEEE Transactions on Industrial Informatics*, vol. 11, no. 4, pp. 853–864, Aug. 2015, doi: 10.1109/TII.2015.2431223.
- [3] E. Monmasson, L. Idkhajine, M. N. Cirstea, I. Bahri, A. Tisan, and M. W. Naouar, “FPGAs in industrial control applications,” *IEEE Transactions on Industrial Informatics*, vol. 7, no. 2, pp. 224–243, May 2011, doi: 10.1109/TII.2011.2123908.
- [4] Y. Kumar and P. Purohit, “Hardware implementation of advanced encryption standard,” in *2010 International Conference on Computational Intelligence and Communication Networks*, IEEE, Nov. 2010, pp. 440–442. doi: 10.1109/CICN.2010.89.
- [5] 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, p. 511, May 2001, doi: 10.6028/jres.106.023.
- [6] S. Hasan, A. Ghafouri, A. Dubey, G. Karsai, and X. Koutsoukos, “Vulnerability analysis of power systems based on cyber-attack and defense models,” in *2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, IEEE, Feb. 2018, pp. 1–5. doi: 10.1109/ISGT.2018.8403337.
- [7] M. Li, Z. Yang, L. He, and Y. Teng, “Research on typical model of network invasion and attack in power industrial control system,” in *2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, IEEE, Dec. 2019, pp. 2070–2073. doi: 10.1109/IAEAC47372.2019.8997649.
- [8] 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)*, IEEE, Sep. 2018, pp. 401–406. doi: 10.1109/ICACCI.2018.8554562.
- [9] Y. Zhao, H. Nishikawa, X. Kong, and H. Tomiyama, “Side channel power analysis resistance evaluation of masked adders on FPGA,” *International Journal of Reconfigurable and Embedded Systems (IJRES)*, vol. 12, no. 1, pp. 97–112, Mar. 2023, doi: 10.11591/ijres.v12.i1.pp97-112.
- [10] A. Gohr, F. Laus, and W. Schindler, “Breaking masked implementations of the clyde-cipher by means of side-channel analysis,” *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 397–437, Aug. 2022, doi: 10.46586/tches.v2022.i4.397-437.
- [11] F. Schellenberg, D. R. E. Gnad, A. Moradi, and M. B. Tahoori, “An inside job: remote power analysis attacks on FPGAs,” in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, IEEE, Mar. 2018, pp. 1111–1116. doi: 10.23919/DATE.2018.8342177.
- [12] G. Martin and G. Smith, “High-level synthesis: past, present, and future,” *IEEE Design & Test of Computers*, vol. 26, no. 4, pp. 18–25, Jul. 2009, doi: 10.1109/MDT.2009.83.
- [13] M. C. McFarland, A. C. Parker, and R. Camposano, “Tutorial on high-level synthesis,” in *Proceedings of the 25th ACM/IEEE Design Automation Conference*, 1988, pp. 330–336.
- [14] T. Mizuno, Q. Zhang, H. Nishikawa, X. Kong, and H. Tomiyama, “Impacts of HLS optimizations on side-channel leakage for AES Circuits,” in *2021 18th International SoC Design Conference (ISOCC)*, IEEE, Oct. 2021, pp. 53–54. doi: 10.1109/ISOCC53507.2021.9613900.
- [15] Y. Miura, H. Nishikawa, X. Kong, and H. Tomiyama, “Impacts of clock frequency and sampling intervals on power side-channel leakage of AES circuits,” in *International Conference on Electronics, Information, and Communication (ICEIC)*, 2024.
- [16] F. Koeune and F.-X. Standaert, “A tutorial on physical security and side-channel attacks,” in *Foundations of Security Analysis and Design III. FOSAD FOSAD 2005 2004. Lecture Notes in Computer Science*, Berlin, Heidelberg: Springer, 2005, pp. 78–108. doi: 10.1007/11554578_3.
- [17] S. Mangard, “A simple power-analysis (SPA) attack on implementations of the AES key expansion,” in *Information Security and Cryptology — ICISC 2002. ICISC 2002. Lecture Notes in Computer Science*, Berlin, Heidelberg: Springer, 2003, pp. 343–358. doi: 10.1007/3-540-36552-4_24.
- [18] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in *Advances in Cryptology — CRYPTO’ 99. CRYPTO 1999. Lecture Notes in Computer Science*, Berlin, Heidelberg: Springer, 1999, pp. 388–397. doi: 10.1007/3-540-48405-1_25.
- [19] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model,” in *Cryptographic Hardware and Embedded Systems - CHES 2004. CHES 2004. Lecture Notes in Computer Science*, Berlin, Heidelberg: Springer, 2004, pp. 16–29. doi: 10.1007/978-3-540-28632-5_2.
- [20] C. Rechberger and E. Oswald, “Practical template attacks,” in *Information Security Applications. WISA 2004. Lecture Notes in Computer Science*, Berlin, Heidelberg: Springer, 2005, pp. 440–456. doi: 10.1007/978-3-540-31815-6_35.
- [21] Y. Liang, K. Rupnow, Y. Li, D. Min, M. N. Do, and D. Chen, “High-level synthesis: productivity, performance, and software constraints,” *Journal of Electrical and Computer Engineering*, vol. 2012, pp. 1–14, 2012, doi: 10.1155/2012/649057.
- [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/ipsjip.17.242.




- [23] Q. Zhang, X. Kong, and H. Tomiyama, "A toolkit for power behavior analysis of HLS-designed FPGA circuits," in *Symposium on Low-Power and High-Speed Chips and Systems*, 2021.
- [24] G. Goodwill, B. Jun, J. Jaffe, and P. Rohatgi, "A testing methodology for side-channel resistance validation," *NIST Non-Invasive Attack Testing Workshop*, 2011.
- [25] ISO/IEC 17825, "Information technology – security techniques – testing methods for the mitigation of non-invasive attack classes against cryptographic modules" 2016.
- [26] T. Mizuno, H. Nishikawa, X. Kong, and H. Tomiyama, "Empirical analysis of side-channel attack resistance of HLS-designed AES circuits," in *2023 International Conference on Electronics, Information, and Communication (ICEIC)*, IEEE, Feb. 2023, pp. 1–4. doi: 10.1109/ICEIC57457.2023.10049904.

BIOGRAPHIES OF AUTHORS






Yuto Miura    received his B.E. degree in electronic and computer engineering from Ritsumeikan University in 2022. 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: yuto.miura@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, and so on. 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 his B.E. degree from Nankai University in 2012 and received his M.E. and Ph.D. degrees from Ritsumeikan University in 2018 and 2020, respectively. He worked as an assistant professor at Ritsumeikan University, and as a visiting researcher at the University of Tokyo. In 2023, he joined the Department of Intelligent Robotics, Faculty of Engineering, Toyama Prefectural University as a lecture. His research interests include artificial intelligence, image processing, and embedded system. He is a member of IEEE IEICE and IPSJ. He can be contacted at email: kong@pu-toyama.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 re-searcher 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.