Evaluating AES Security: Correlation Power Analysis Attack Implementation using the Switching Distance Power Model

Hassen Mestiri
Department of Computer Engineering, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
h.mestiri@psau.edu.sa (corresponding author)

Received: 26 November 2024 | Revised: 21 December 2024 | Accepted: 6 January 2025

 DOI: https://doi.org/10.48084/etasr.9728

ABSTRACT

Cryptographic circuits play a critical role in safeguarding confidential information and ensuring secure communication, contributing to the resilience of digital infrastructure under SDG 9 (Industry, Innovation, and Infrastructure). These circuits store encryption keys for the Advanced Encryption Standard (AES) algorithm, including AES-128, AES-192, and AES-256, which are widely used in applications such as online banking and secure messaging platforms. This paper examines the effectiveness of Correlation Power Analysis (CPA), a side-channel attack technique that exploits power consumption patterns in cryptographic circuits, to highlight the challenges of implementing secure encryption systems. The study illustrates the CPA attack procedure against AES implemented on the SASEBO-GII FPGA platform. Experimental results reveal that while the CPA attack based on the Hamming Weight (HW) power consumption model fails to extract the encryption key, the Switching Distance (SD) power consumption model successfully recovers the entire key with a 100% success rate using approximately 4000 power traces. These findings underscore the vulnerability of cryptographic circuits to advanced side-channel attacks and emphasize the need for robust countermeasures to ensure secure data protection, thereby advancing secure and sustainable digital environments under SDG 11 (Sustainable Cities and Communities).

Keywords-cryptographic circuits; power consumption model; switching distance; CPA attack

I. INTRODUCTION

It is common for embedded systems to employ electronic cryptographic devices to safeguard confidential information. The cryptographic algorithm is performed in conjunction with the secret key, which is stored in such devices. This vulnerability highlights the importance of implementing strong security measures in embedded systems to prevent unauthorized access to sensitive data [1, 2]. Additionally, continuous monitoring and updating of encryption algorithms and key storage methods are essential to mitigate potential security risks. Algorithms have been developed to guarantee protection against mathematical attacks. However, such an algorithm may result in side channel leakages when it is implemented on hardware systems, which are used to disclose additional information about the computed secret. Attacks that use information derived from the physical implementation of a cryptosystem are known as side channel attacks, e.g. electromagnetic emanation [3], power consumption [4], and time execution [5].

Power analysis attacks are executed by exploiting the correlation between the internal data and the power consumption of cryptographic equipment. The Simple Power Analysis (SPA) attack [6] relies on a comprehensive understanding of the cryptographic method and a visual examination of power consumption to determine the secret cryptographic keys. The Differential Power Analysis (DPA) attack is more potent than SPA attack and requires less comprehensive knowledge of the cryptographic algorithm's - implementation. It employs statistical methods [7-9].

The Correlation Power Analysis (CPA) attack is a method that uses the correlation between real and predicted power consumption models of cryptographic circuits to extract encryption keys, requiring less detailed knowledge of the algorithm hardware implementation [10-12]. CPA is particularly effective in situations where DPA may not be feasible due to noise or other factors. By exploiting the power consumption patterns of cryptographic devices, CPA poses a significant threat to the security of sensitive information [13, 15]. Furthermore, CPA attacks can be conducted remotely, making them a serious concern for devices connected to the internet. Implementing countermeasures such as randomizing power consumption patterns or using secure hardware can help mitigate the risk of CPA attacks.

Cryptographic algorithms implemented on ASICs and FPGAs have been successfully employed with SD and HW

power consumption models [16, 17]. These models allow for the analysis of power consumption during cryptographic operations, helping to detect and prevent potential CPA attacks. By incorporating these models into the design and implementation of cryptographic devices, security vulnerabilities can be significantly reduced.

Side-channel attacks, which exploit unintended physical information leakage, have emerged as a significant threat to the security of cryptographic circuits [18, 19]. Among these attacks, CPA has been widely studied and demonstrated as an effective technique for extracting encryption keys by analyzing the power consumption patterns of cryptographic hardware. Several studies have investigated the application of CPA attacks against AES implementations, revealing the vulnerabilities of straightforward hardware and software implementations. Authors in [18, 19] explored the use of more advanced power models, such as the Switching Distance (SD) model, as an alternative to the commonly used Hamming Weight (HW) model, in an effort to enhance the effectiveness of these attacks. By utilizing more sophisticated power models, researchers aim to improve the success rate of CPA attacks on AES implementations and ultimately strengthen the security of cryptographic hardware. This ongoing research highlights the importance of continuously evolving countermeasures to protect against potential vulnerabilities in encryption systems. Additionally, the literature highlights the critical need for robust countermeasures to mitigate side-channel attacks.

To evaluate the robustness of AES implementations, we successfully conducted a CPA attack on AES deployed on the FPGA SASEBO-GII board [20], utilizing the SD power model. Additionally, we analyzed the efficiency of the CPA attack by determining the number of power traces required to reliably extract the correct encryption key. This research underscores the importance of understanding vulnerabilities in cryptographic systems to strengthen digital security, contributing to resilient infrastructure and innovation in line with SDG 9 and SDG 11.

II. BACKGROUND

A. AES Block Cipher

The AES algorithm is a symmetric block cipher that is widely used for securing sensitive data in various applications. This research highlights the importance of evaluating cryptographic devices against CPA attacks to ensure the confidentiality of information. The AES performs four basic operations: SubBytes (SB), ShiftRows (SR), MixColumns (MC), and AddRoundKey (ARK). These operations are repeated multiple times in different rounds depending on the key size [21, 22]. In addition, the AES algorithm has been standardized by the National Institute of Standards and Technology (NIST) and is considered to be highly secure against various cryptographic attacks. Furthermore, the AES algorithm is widely used in securing sensitive information. Its robust encryption techniques make it a trusted choice for protecting data at rest and in transit. Overall, the AES algorithm's versatility and strength have made it a popular choice for ensuring data confidentiality and integrity. Its widespread adoption in various sectors speaks to its reliability and effectiveness in safeguarding sensitive information from unauthorized access. The efficiency and security of ASIC and FPGA implementations of AES can be further enhanced by considering the resistance against CPA attacks during the design phase. By analyzing the performance of these devices under such attacks, potential vulnerabilities can be identified and mitigated to strengthen data protection measures.

B. CPA Attacks

The CPA attack capitalizes on the power consumption leaks during cryptographic processes to acquire the secret keys. An attacker might possibly retrieve the key used for data encryption by studying the power traces produced during AES encryption. The CPA attack necessitates a power model to comprehend the power consumption characteristics of the cryptographic equipment. By analyzing the relationship between the anticipated and actual power usage, cryptanalysts may deduce the confidential information. The Pearson correlation function is used to calculate the correlation coefficient (ρ), which is is calculated as:

$$\rho(W,P)=\frac{Cov(W,P)}{\sqrt{Var(W)}\sqrt{Var(P)}} \quad (1)$$

where W and P represent the actual and anticipated power consumption, respectively. The operations of covariance and variance are denoted by the symbols *Cov* and *Var*, respectively. Values ranging from -1 to +1 are possible for the Pearson correlation coefficient. When the value is +1, W and P have an increasing relationship, a decreasing relationship when the value is -1, and a non-linear relationship when the value is 0. The process of conducting a CPA attack is:

- Select an intermediate stage in the processing procedure. This point must depend on the secret keys and the known variable.
- During the execution of the processing algorithm, employ a digital oscilloscope to quantify the actual power consumption of the cryptographic device.
- Use a particular leakage model, like the HW, Hamming Distance, or SD, to forecast the power consumption.
- Ascertain the link between the presumed power and the recorded power trace. The correlation coefficient with the greatest value signifies the precise critical estimate.

Exploring how noise and environmental factors impact the success rate of the CPA attack could provide valuable insights for improving the effectiveness of side-channel attacks. Noise and environmental factors can introduce unpredictability and variability in the leakage signals, potentially making it more challenging for attackers to extract sensitive information accurately. Understanding these variables can help develop more accurate models and strategies for breaking encryption systems.

C. Source of Power Consumption

CMOS technology is the most prevalent contemporary digital design application. The aggregate of static and dynamic

power is the entire power consumption of a CMOS gate, as illustrated in (2):

$$P_{total} = P_{static} + P_{dynamic} \quad (2)$$

The leakage currents in transistors are the cause of P_{static} power consumption. However, the $P_{dynamic}$ power consumption is a result of the CMOS circuits executing an output transition. The $P_{dynamic}$ definition is:

$$P_{dynamic} = \alpha_{0\to1} C_L V_{DD}^2 f \quad (3)$$

The output transition probability of a CMOS gate from 0 to 1 is denoted by $\alpha_{0\to1}$, whereas C_L is the load capacitance, V_{DD} is the power voltage, and f is the working frequency.

The total power consumption of a CMOS device can be estimated in proportion to the frequency of output transitions from 0 to 1 as demonstrated by (3). Consequently, the power consumption of CMOS circuits is contingent upon the data set. In addition, researchers are exploring new techniques such as power analysis resistant logic styles to further enhance the security of devices against CPA attacks. By continuously improving hardware and software defenses, the industry can stay ahead of potential threats and protect sensitive information effectively.

III. POWER CONSUMPTION MODELS

The power consumption models used in CPA attacks can vary depending on the specific device and implementation, making it crucial for developers to stay informed about potential vulnerabilities and best practices for securing cryptographic devices. In addition, power models can be used to analyze and exploit weaknesses in cryptographic implementations, allowing attackers to recover sensitive information such as encryption keys. Staying updated on advancements in side-channel attack techniques and countermeasures is essential for maintaining the security of cryptographic devices. Developers should also consider implementing additional security measures, such as randomizing power consumption patterns or using masking techniques, to further protect cryptographic devices from side-channel attacks. Regularly testing devices for vulnerabilities and staying vigilant against emerging threats can help mitigate the risk of successful CPA attacks. In this study, we employed HW and SD power consumption models to forecast the power consumption of cryptographic circuits.

A. Switching Distance Model

The SD model is predicated on the fact that the power consumption of 0 to 1 and 1 to 0 transitions in a CMOS device varies. The SD factor, which is denoted as φ, is allocated to the transition from 0 to 1, while the SD factor for the transition from 1 to 0 is assigned 1, as shown in Table I [21].

B. Hamming Weight Model

The HW model represents the fundamental power consumption model. This is particularly relevant for predicting a circuit's power usage when the attacker lacks knowledge of the sequential data values at certain stages of the operation. This concept posits that a 0 does not result in excessive power consumption, but a 1 entails considerable power consumption. In this approach, it is posited that power consumption is directly proportional to the quantity of bits activated in the processed data [23, 24].

TABLE I. HW AND SD POWER CONSUMPTION MODELS

Transitions	HW	SD
0→0	0	0
0→1	1	1
1→0	0	φ
1→1	1	0

The HW model assumes power consumption is proportional to the number of bits set in the data, while the SD model accounts for different power consumption during $0\to1$ and $1\to0$ transitions in CMOS devices. The HW model may overestimate power consumption for certain types of data patterns, leading to discrepancies with the SD model. By considering the unique characteristics of CMOS devices, such as the differing power consumption during transitions, the SD model provides a more accurate representation of power consumption in digital circuits. This difference in the approach may explain the performance variation observed between the two models. The limitations of the SD model include its inability to accurately predict power consumption when sequential data values are unknown, as well as its reliance on the assumption that power consumption is solely determined by the number of activated bits in the data. Additionally, the SD model may not account for other factors that could influence power usage in a circuit.

IV. CPA ATTACK PROCESS

This part will explain how to use the HW and SD models to launch a CPA attack on the AES hardware on the FPGA SASEBO-GII board. We used the power traces accessible at [25]. Power measurements were executed on the SASEBO-GII FPGA.

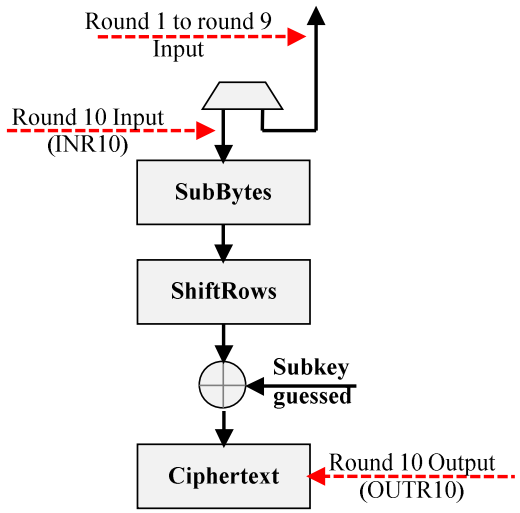

Fig. 1. CPA attack against the last AES round.

The AES encryption technique utilizes a 128-bit plaintext and a 128-bit encryption key to produce a 128-bit ciphertext. Each round of AES encryption entails the alteration of the encryption key via the XOR operation between an intermediate value and the round key. Every round of the AES makes use of a round key, which is obtained from the initial K_0. These round keys are K_1-K_{10}. In the 10th (last) round of the AES encryption algorithm, the MC transformation is not performed. This results in a reduction in the complexity of the encryption process. For the purpose of accomplishing this goal, we will focus on the last round of AES, as shown in Figure 1.

Let $OUTR_{10}$ represent the ciphertext output and INR_{10} denote the input of round 10. The $OUTR_{10}$ computes INR_{10} by using 256 potential key values (guessed K_{10}) along with the inverse transformations of ShiftRows and SubBytes (*Inv_SR* transformation and *Inv_SB* transformation). The INR_{10} is calculated as follows:

$$INR_{10} = Inv\_SB\left(Inv\_SR\left(K_{10(\text{guess})} \oplus OUTR_{10}\right)\right) \quad (4)$$

The SD between INR_{10} and $OUTR_{10}$, as defined in (5), can then be used to calculate the prediction of the power consumption of the previous AES round.

$$P_{\text{exp}} = SD\left(INR_{10} \oplus OUTR_{10}\right) \quad (5)$$

Following that, we proceed to compute the correlation coefficient ρ that exists between the expected power consumption P_{exp} and the measured power consumption P_{meas}. Equation (6) may be used to compute the correlation coefficient ρ.

$$\rho\left(\text{exp}, P_{meas}\right) = \frac{Cov\left(P_{\text{exp}}, P_{meas}\right)}{\sqrt{Var\left(P_{\text{exp}}\right)}\sqrt{Var\left(P_{meas}\right)}} \quad (6)$$

As ρ quantifies the linear connection between expected and actual power consumption, its value must range from -1 to 1. The accurate key estimate aligns with the maximum absolute value of the correlation coefficient ρ. By carefully analyzing power consumption patterns and implementing secure hardware, devices can better protect against CPA attacks. The correlation coefficient ρ plays a crucial role in accurately estimating cryptographic keys and must fall within the range of -1 to 1 for optimal security measures.

V. RESULTS AND DISCUSSION

The results of the CPA attack on AES-128 that was carried out on SASEBO-GII are presented in this section. The SD model was used to anticipate how much electricity will be used. There is a factor of 1.5 for the φ. Authors in [26] show that the 16-byte keys of AES may be retrieved with minimum power traces if the value of φ is equal to 1.5.

In the case that a CPA attack is successful, we predict that just one value, which is known to be connected with the right key hypothesis, will have a high correlation coefficient. This is because we know that this value is the only one that makes sense. Figure 2 is a representation of the experimental data related to the correlation power traces. In a straightforward manner, the peak that is believed to be associated with the appropriate subkey hypothesis may be seen.

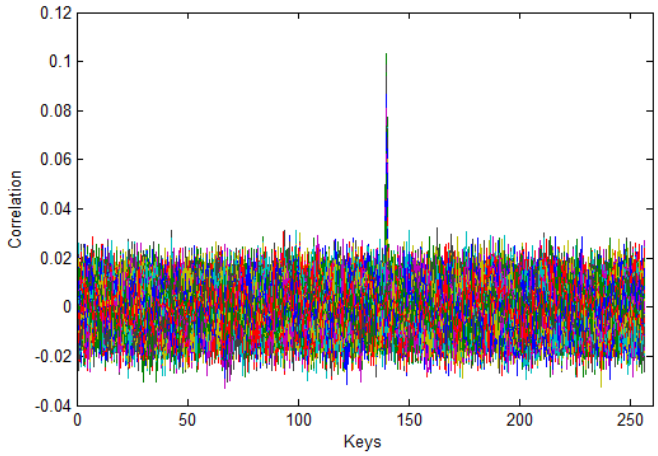

Fig. 2. Successful CPA attack against SASEBO-GII AES implementation.

The original key bytes (Round key 0) and their corresponding in round 10 (in decimal notation) are presented in Table II.

TABLE II. AES ROUND 10 KEY

Key Bytes (R0)	1	2	3	4	5	6	7	8
Key Bytes (R10)	19	17	29	127	227	148	74	23
Key Bytes (R0)	9	10	11	12	13	14	15	16
Key Bytes (R10)	243	07	167	139	77	43	48	197

Initially, for the purpose of extracting a single key byte from the AES keys, we make use of the SD power model. As shown in Figure 3, the correlation peak of the fourth AES encryption key byte is the greatest of all the correlation peaks. On the other hand, the correlation peaks of the incorrect encryption key byte estimations vary from -0.03281 to 0.03179. These results indicate that the SD power model can effectively extract AES key bytes, but further analysis is needed to improve accuracy and reliability. Additional research may focus on refining the methodology to enhance the precision of key byte extraction in AES encryption. By using CPA and basing it on the SD model, it is possible to correctly obtain the precise AES key bytes. The SD model is able to provide an accurate prediction about the amount of power that the AES implementation on the FPGA SASEBO-GII board would use. This information is crucial for optimizing power consumption in AES implementations and ensuring the security of cryptographic systems. Additionally, the SD power model can be further utilized to enhance side-channel attack resistance in FPGA-based cryptographic systems.

The second case involves the use of the HW power model for the purpose of extracting a single key byte from the AES keys. The correlation findings for the 256 hypotheses for the ninth byte of AES keys are presented in Figure 4.

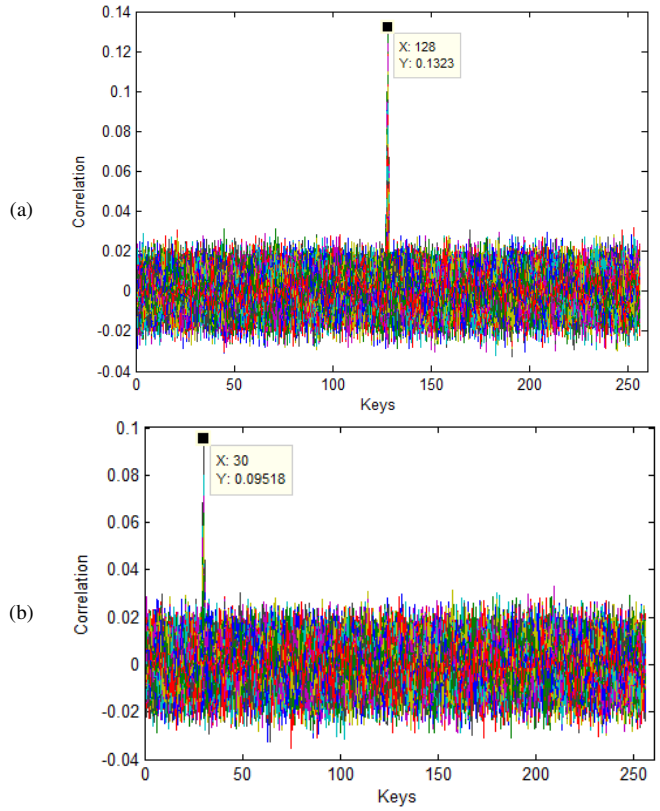

Fig. 3. Successful CPA attack against SASEBO-GII AES implementation using SD power model: (a) fourth key, (b) thrid key.

Figure 4 illustrates that, after using 30,000 power measurements, the accurate AES key cannot be extracted. This indicates that CPA attacks using a HW model are unable of retrieving the accurate encryption key. This model is incapable of accurately predicting the power consumption of the FPGA SASEBO-GII board.

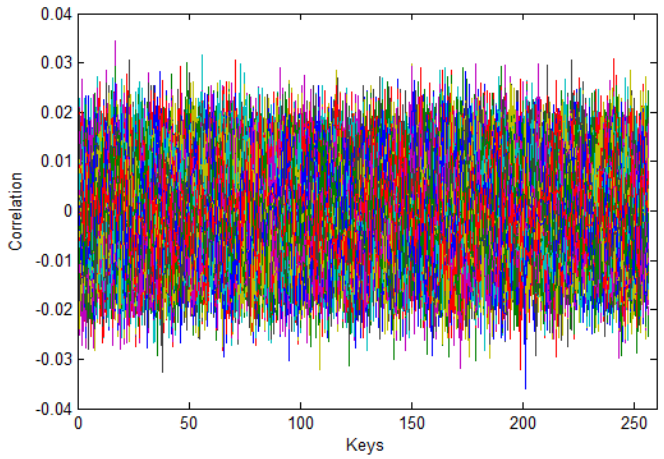

Fig. 4. Failed CPA attack against SASEBO-GII AES implementation using the HW power model.

To assess the quality of the correlation coefficient using the SD power model, the ordering of the three initial key suppositions are provided in Table II. In absolute value, the three suppositions are categorized according to their decreasing correlation coefficients. Table III demonstrates that the correlation coefficient with the maximum value is readily identifiable. The appropriate key can be readily extracted as a result. The fourth byte key, for example, can be readily identified by a difference of 426% between the first and the second peak.

Using the SD model, the final experiment in this section aims to ascertain the successful rate of the CPA attack. The CPA attack is re-conducted for all critical bytes in order to achieve this objective. For each test, we adjusted the number of power traces from 300 to 4500. Figure 5 illustrates the success rates of CPA attacks against AES. Figure 5 illustrates that the SD model allows for the appearance of 100% of AES keys at approximately 4000 power traces. This demonstrates the effectiveness of the SD model in successfully recovering AES keys through CPA attacks. The results indicate that with a sufficient number of power traces, the SD model can reliably identify cryptographic keys.

TABLE III. SD IDENTIFICATION OF THE CORRELATION PEAK

Key bytes	1	2	3	4	5	6	7	8
Correlation	19 11.8%	17 10.6%	29 9.52%	127 13.2%	227 10.2%	148 18.4%	74 11.3%	29 9.1%
	25 3.5%	129 3.8%	56 3.3%	102 3.1%	42 3.9%	235 3.8%	48 3.7%	189 4%
	203 3.1%	251 3.6%	167 3.13%	55 3.1%	46 3.6%	25 3.5%	156 3.4%	254 3.7%
Key bytes	9	10	11	12	13	14	15	16
Correlation	243 12.5%	7 11.5%	167 8.4%	139 10.4%	77 10.4%	43 10.1%	48 10.3%	197 9%
	18 3.5%	58 3.9%	245 3.7%	74 3.5%	224 3.6%	187 3.8%	16 3.4%	163 3.8%
	129 3.3%	145 3.7%	12 3.6%	163 3.3%	25 3.3%	155 3.5%	209 3.1%	24 3.6%

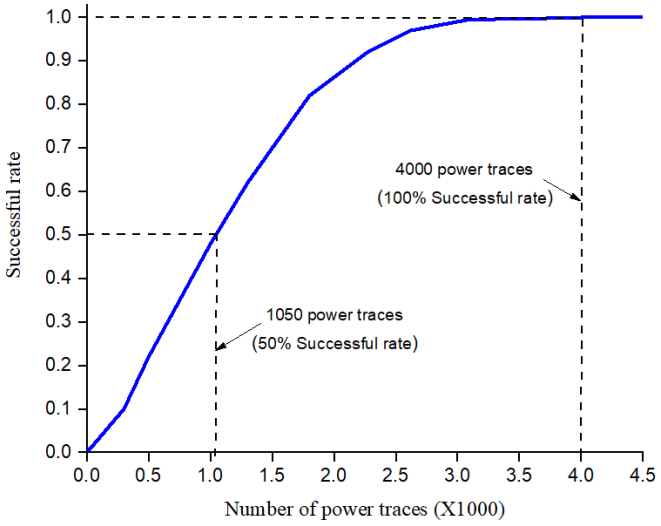

Fig. 5. CPA attack against AES using the SD power model: Success rate.

Further analysis of the relationship between the number of power traces and the success rate of key recovery could provide valuable insights into the practical implications of using the SD model for CPA attacks. Additionally, exploring potential limitations or vulnerabilities of the SD model in certain scenarios would enhance the overall understanding of its effectiveness in cryptographic key recovery.

VI. CONTREMESAURE METHODOLOGY AGAINST CPA ATTACKS

One advanced cryptographic technique that can be implemented to enhance the security of AES against CPA attacks is the use of authenticated encryption modes such as Galois Counter Mode (GCM) or CBC counter mode (CCM). The GCM principle provides both confidentiality and integrity protection, making it more resistant to CPA attacks compared to traditional modes like Cipher-Block Chaining (CBC) or Electronic Codebook (ECB). Additionally, incorporating random IVs and key diversification techniques can also help mitigate potential vulnerabilities in AES implementations. The CCM is another authenticated encryption mode that combines Counter Mode with CBC-MAC, providing both confidentiality and integrity protection in a single operation. By using these advanced cryptographic techniques, the security of AES can be significantly improved against CPA attacks. These modes not only provide confidentiality but also ensure data integrity, protecting against chosen plaintext attacks more effectively. Additionally, incorporating key diversification techniques such as using unique keys for different encryption sessions can further strengthen the resistance of AES against CPA attacks.

Machine learning algorithms have shown promise in predicting power consumption patterns with high accuracy. Developing sophisticated countermeasures such as randomizing power consumption or adding noise to the measurements can help mitigate power analysis attacks based on HW models. The results showed that machine learning algorithms are highly effective in predicting power consumption patterns.

VII. CONCLUSION

This study investigated the effectiveness of Correlation Power Analysis (CPA) attacks against an AES-128 implementation on the SASEBO-GII FPGA board. We compared the SD model and HW power models. Our results demonstrate that the SD model accurately predicts power consumption and enables successful key recovery. Using the SD model, we achieved a 100% success rate in extracting all key bytes with approximately 4000 power traces. Conversely, the HW model failed to predict power consumption accurately, rendering it ineffective for key extraction. The significant difference in performance between the two models highlights the importance of selecting an appropriate power model for CPA attacks. The SD model's success underscores its potential for evaluating the vulnerability of cryptographic implementations to side-channel attacks. Future research could explore the application of the SD model to other cryptographic algorithms and platforms, and investigate countermeasures to mitigate CPA attacks based on this model.

This research highlights the importance of selecting appropriate power consumption models for successful side-channel attacks and emphasizes the critical need for robust cryptographic countermeasures. By addressing vulnerabilities in encryption systems, this work contributes to advancing secure and resilient digital infrastructures, supporting SDG 9 and SDG 11.

ACKNOWLEDGMENT

The authors extend their appreciation to Prince Sattam bin Abdulaziz University for funding this research work through the project number (PSAU/2024/01/31267)

REFERENCES

[1] H. Mestiri and I. Barraj, "High-Speed Hardware Architecture Based on Error Detection for KECCAK," *Micromachines*, vol. 14, no. 6, May 2023, Art. no. 1129, https://doi.org/10.3390/mi14061129.

[2] H. Mestiri, I. Barraj, T. Saidani, and M. Machhout, "A PRESENT Lightweight Algorithm High-Level SystemC Modeling using AOP Approach," *Engineering, Technology & Applied Science Research*, vol. 14, no. 5, pp. 16772–16777, Oct. 2024, https://doi.org/10.48084/etasr.8417.

[3] O. A. Sosa, Z. Dyka, I. Kabin, and P. Langendörfer, "Simulation of Electromagnetic Emanation of Cryptographic ICs: Tools, Methods, Problems," in *IEEE East-West Design & Test Symposium*, Batumi, Georgia, Sep. 2021, pp. 1–5, https://doi.org/10.1109/EWDTS52692.2021.9581013.

[4] M. Lipp *et al.*, "PLATYPUS: Software-based Power Side-Channel Attacks on x86," in *IEEE Symposium on Security and Privacy*, San Francisco, CA, USA, Dec. 2021, pp. 355–371, https://doi.org/10.1109/SP40001.2021.00063.

[5] Z. H. Jiang, Y. Fei, and D. Kaeli, "A Novel Side-Channel Timing Attack on GPUs," in *Great Lakes Symposium on VLSI*, Alberta, Canada, Dec. 2017, pp. 167–172, https://doi.org/10.1145/3060403.3060462.

[6] Y.-S. Won, B.-Y. Sim, and J.-Y. Park, "Key Schedule against Template Attack-Based Simple Power Analysis on a Single Target," *Applied Sciences*, vol. 10, no. 11, Jan. 2020, Art. no. 3804, https://doi.org/10.3390/app10113804.

[7] B.-A. Dao, T.-T. Hoang, A.-T. Le, A. Tsukamoto, K. Suzaki, and C.-K. Pham, "Exploiting the Back-Gate Biasing Technique as a Countermeasure Against Power Analysis Attacks," *IEEE Access*, vol. 9, pp. 24768–24786, Jan. 2021, https://doi.org/10.1109/ACCESS.2021.3057369.

[8] J. Chen, J.-S. Ng, K.-S. Chong, Z. Lin, and B.-H. Gwee, "A Novel Normalized Variance-Based Differential Power Analysis Against Masking Countermeasures," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3767–3779, 2021, https://doi.org/10.1109/TIFS.2021.3093783.

[9] M. Asfand Hafeez, M. Mazyad Hazzazi, H. Tariq, A. Aljaedi, A. Javed, and A. R. Alharbi, "A Low-Overhead Countermeasure against Differential Power Analysis for AES Block Cipher," *Applied Sciences*, vol. 11, no. 21, Jan. 2021, Art. no. 10314, https://doi.org/10.3390/app112110314.

[10] J.-S. Ng *et al.*, "A Highly Efficient Power Model for Correlation Power Analysis (CPA) of Pipelined Advanced Encryption Standard (AES)," in *IEEE International Symposium on Circuits and Systems*, Seville, Spain, Oct. 2020, pp. 1–5, https://doi.org/10.1109/ISCAS45731.2020.9180778.

[11] Y. Jeon, J. H. Jung, and J. W. Yoon, "Efficient Correlation Power Analysis (CPA) Focusing on Byte-Wise Calculation Points," *IEEE Access*, vol. 9, pp. 74275–74285, Jan. 2021, https://doi.org/10.1109/ACCESS.2021.3079960.

[12] J. Han, Y.-J. Kim, S.-J. Kim, B.-Y. Sim, and D.-G. Han, "Improved Correlation Power Analysis on Bitslice Block Ciphers," *IEEE Access*, vol. 10, pp. 39387–39396, Jan. 2022, https://doi.org/10.1109/ACCESS.2022.3163852.

[13] N.-T. Do and V.-P. Hoang, "An Efficient Side Channel Attack Technique with Improved Correlation Power Analysis," in *International Conference on Industrial Networks and Intelligent Systems*, Hanoi, Vietnam, Aug. 2020, pp. 291–300, https://doi.org/10.1007/978-3-030-63083-6_22.

[14] Z. Zhang, I. Miketic, E. Salman, and Q. Yu, "Assessing Correlation Power Analysis (CPA) Attack Resilience of Transistor-Level Logic Locking," in *Great Lakes Symposium on VLSI*, Jun. 2021, pp. 415–420, https://doi.org/10.1145/3453688.3461508.

[15] R. D. Silva, I. Navarathna, M. Kumarasiri, C. W. Chuah, and J. Alawatugoda, "Correlation power analysis attack on software implementation of TRIVIUM stream cipher," *International Journal of Information and Computer Security*, vol. 19, no. 3–4, pp. 379–401, Jan. 2022, https://doi.org/10.1504/IJICS.2022.127156.

[16] T.-H. Tran, B.-A. Dao, T.-T. Hoang, V.-P. Hoang, and C.-K. Pham, "Transition Factors of Power Consumption Models for CPA Attacks on Cryptographic RISC-V SoC," *IEEE Transactions on Computers*, vol. 72, no. 9, pp. 2689–2700, Sep. 2023, https://doi.org/10.1109/TC.2023.3262926.

[17] S. D. Putra, A. D. W. Sumari, I. Asrowardi, and E. Subyantoro, "Power Analysis in Hamming Weight Model: Attacking IoT Encryption Devices," in *4th International Conference on Signal Processing and Information Security*, Dubai, United Arab Emirates, Nov. 2021, pp. 41–44, https://doi.org/10.1109/ICSPIS53734.2021.9652185.

[18] K. Coelho, D. Damião, G. Noubir, A. Borges, M. Nogueira, and J. Nacif, "Cryptographic Algorithms in Wearable Communications: An Empirical Analysis," *IEEE Communications Letters*, vol. 23, no. 11, pp. 1931–1934, Aug. 2019, https://doi.org/10.1109/LCOMM.2019.2937782.

[19] K.-L. Tsai, F.-Y. Leu, I. You, S.-W. Chang, S.-J. Hu, and H. Park, "Low-Power AES Data Encryption Architecture for a LoRaWAN," *IEEE Access*, vol. 7, pp. 146348–146357, Jan. 2019, https://doi.org/10.1109/ACCESS.2019.2941972.

[20] Y. Nomata, M. Matsubayashi, K. Sawada, and A. Satoh, "Comparison of side-channel attack on cryptographic cirucits between old and new technology FPGAs," in *5th Global Conference on Consumer Electronics*, Kyoto, Japan, Oct. 2016, pp. 1–4, https://doi.org/10.1109/GCCE.2016.7800555.

[21] M. Bedoui, H. Mestiri, B. Bouallegue, M. Marzougui, M. Qayyum, and M. Machhout, "An improved and efficient countermeasure against fault attacks for AES," in *2nd International Conference on Anti-Cyber Crimes*, Abha, Saudi Arabia, Mar. 2017, pp. 209–212, https://doi.org/10.1109/Anti-Cybercrime.2017.7905292.

[22] H. Mestiri, I. Barraj, A. Alsir Mohamed, and M. Machhout, "An Efficient AES 32-Bit Architecture Resistant to Fault Attacks," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 3667–3683, 2022, https://doi.org/10.32604/cmc.2022.020716.

[23] W. Cao, F. Huang, M. Zheng, and H. Hu, "Attacking FPGA-based Dual Complementary AES Implementation Using HD and SD Models," in *16th International Conference on Computational Intelligence and Security*, Guangxi, China, Nov. 2020, pp. 278–282, https://doi.org/10.1109/CIS52066.2020.00066.

[24] X. Fan, J. Tong, Y. Li, X. Duan, and Y. Ren, "Power Analysis Attack Based on Hamming Weight Model without Brute Force Cracking," *Security and Communication Networks*, vol. 2022, no. 1, 2022, Art. no. 7375097, https://doi.org/10.1155/2022/7375097.

[25] "NSF IUCRC." https://chest.coe.neu.edu/.

[26] H. Liu, G. Qian, S. Goto, and Y. Tsunoo, "AES Key Recovery Based on Switching Distance Model," in *Third International Symposium on Electronic Commerce and Security*, Nanchang, China, Jul. 2010, pp. 218–222, https://doi.org/10.1109/ISECS.2010.55.