Summary and Analysis on

DEEP LEARNING-BASED POWER ANALYSIS ATTACK FOR EXTRACTING AES KEYS ON ATMEGA328P MICROCONTROLLER

by **R.Kirthika** *(23MCS001)*

Department of Computer Science and Engineering

National Institute of Technology, Hamirpur

This article analyses and summarizes the research paper titled as above written by "*Ismail Negabi1, Smail Ait El Asri, Samir El Adib, Naoufal Raissouni*" and published in *Arabian Journal for Science and Engineering* in the year 2023. Further study on this subject has been discussed under *Appendix.*

ABSTRACT OF THE PAPER

The abstract of the paper provides an excerpt on the power analysis attack (PAA) using Deep-Learning methods on ATmega328P microcontroller. The approach discussed in the paper extracts AES keys using CNN trained on power consumption traces and efficiently recovers AES-128 keys with only about 1200 traces, outperforming other methods by a margin of 100 power consumption traces.

SUMMARY

The paper discusses the DL-based power analysis attack (PAA) to extract AES keys from the ATmega328P microcontroller using a CNN trained on power consumption traces. Deep learning approaches, such as CNN and RNN, have been utilized for side-channel attacks on cryptographic systems, particularly on resource-constrained devices like microcontrollers and demonstrates the effectiveness of DL-based SCAs in recovering secret keys from cryptographic devices with a small number of traces.

The paper highlights the vulnerability of various cryptographic systems to side-channel attacks. It also emphasises the significant threats on rapid developing technologies such as Internet of Things (IoT) which eventually increases the demand for data processing devices. Understanding these vulnerabilities are crucial to improve the security of IoT devices and other devices like microcontrollers and sensors. Despite the strength of advanced encryption algorithms like AES, they are susceptible to attacks like side-channel attacks, compromising the security of the device.

Side-channel attacks (SCA) exploit unintended leaks of information on physical characteristics of a device or system can reveal the device's internal information such as energy consumption, runtime, network traffic data, or memory during cryptographic algorithm implementation.

The paper focuses on one such type of Side Channel Attack known as Power analysis attack (PAA). It is a passive method of SCA that aims to infer sensitive information, such as passwords or encryption keys, by analysing the energy consumption fluctuations of a device. PAA uses real-time energy consumption data to build mathematical models that can uncover a secret key. Conventionally, there are three techniques to carry out and analyse the PAA namely *Simple power analysis (SPA)*, *Differential power analysis (DPA)* and *Correlation power analysis (CPA)*.

The paper introduces a Deep Learning based power analysis attack (PAA) to extract AES keys from the ATmega328P

microcontroller using a CNN trained on power consumption traces. The DL-based side-channel attacks analyse power consumption data to improve the efficiency and accuracy of attacks on target devices.

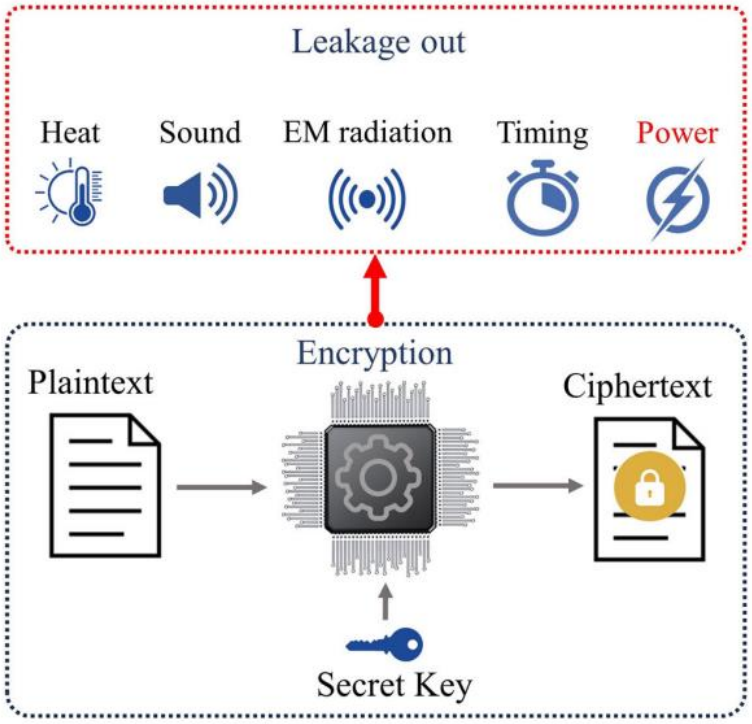

Fig.1 Side-Channel monitoring

CONTRIBUTION OF THE PAPER

The paper presented a DL-based power analysis attack for extracting AES keys on an ATmega328P microcontroller. Utilized a CNN trained on energy consumption traces to perform side-channel attacks. It details the use of DL-based power analysis attacks to exploit information leakage from cryptographic devices. The author then compares the performance of the DL-based attack method with other techniques targeting cryptographic devices and demonstrated an improved performance in extracting secret keys from power traces compared to other attacks on the ATmega328P microcontroller. The research demonstrates the effectiveness of DL models in recovering secret keys through side-channel analysis, particularly focusing on power consumption traces.

ANALYSIS

Literature Survey of the Paper:

Previous related works and research also provide various methods including DL Models to counter SCA in cryptographic algorithm-based implementations and have been effective in recovering of the secret key. The author refers such existing studies that have similar objectives.

The highlights of the paper's literature survey are as follows:

- Renauld et al.[2009] : Demonstrated that through algebraic power analysis attacks, it is possible to extract the AES key from implementations, revealing vulnerabilities in the security of the cryptographic system.

- Jayasinghe et al. [2014]: Explored how power analysis attacks could be used to uncover sensitive information by targeting the vulnerabilities in the energy consumption of hardware circuits.
- Hnath et al. [2010]: Highlighted differential power analysis (DPA) technique and utilized mathematical models to study the relationship between cryptographic protocols and the energy consumption patterns. He demonstrated the aforementioned by training Neural Network models on leak traces and exploring multiple-input models.
- Lo et al. [2017]: Introduced the concept of Correlation Power Analysis (CPA), which involves analysing the correlation between power consumption and the data being processed. He also explores data augmentation methods to enhance the success rates of side-channel attacks, demonstrating the effectiveness of techniques like MIXUP in improving attack performance.
- Wang et al. [2020]: Pioneered the use of DL-models, specifically CNNs, in side-channel attacks against AES-128, utilizing electromagnetic emissions as the side channel for extracting the secret key.

Methods used in the Paper:

To implement the attack described in the paper the author uses hardware/software setups involving ATmega328p microcontrollers, oscilloscope, DELL computer, and software like Arduino IDE and Python for data collection and analysis.

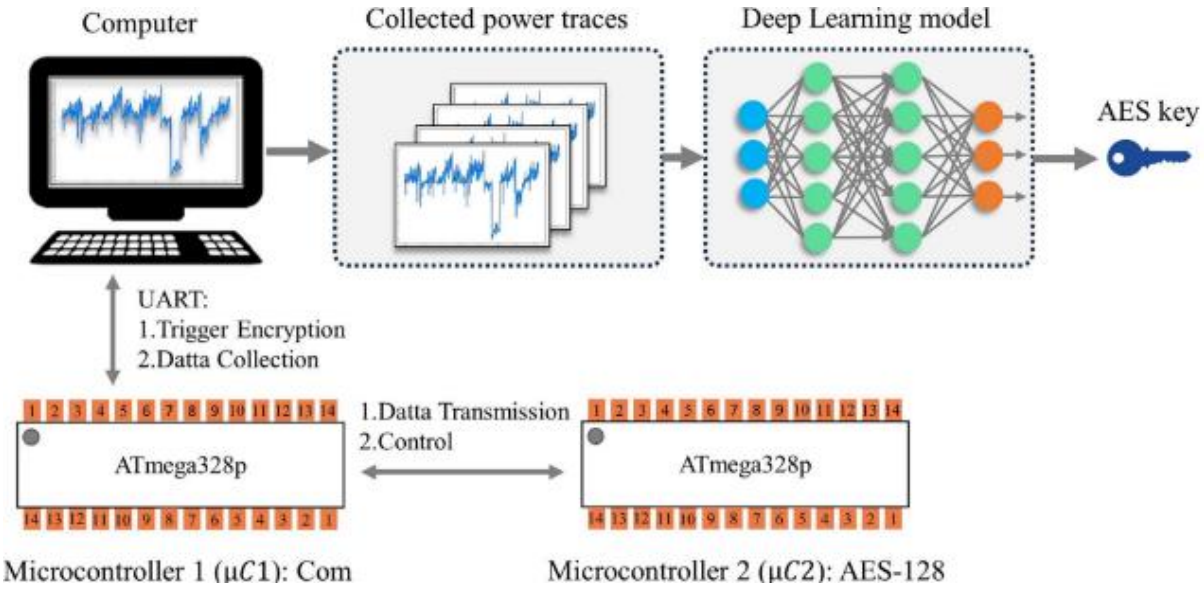

Fig.2 Block diagram of the power-based side-channel Attacks on AES-128

Data capture workflow involves generating random text and key values, transmitting data between microcontrollers, and capturing power traces for analysis. Power consumption traces collected during AES-128 execution on the ATmega328P microcontroller were used for the DL-based power analysis attack.

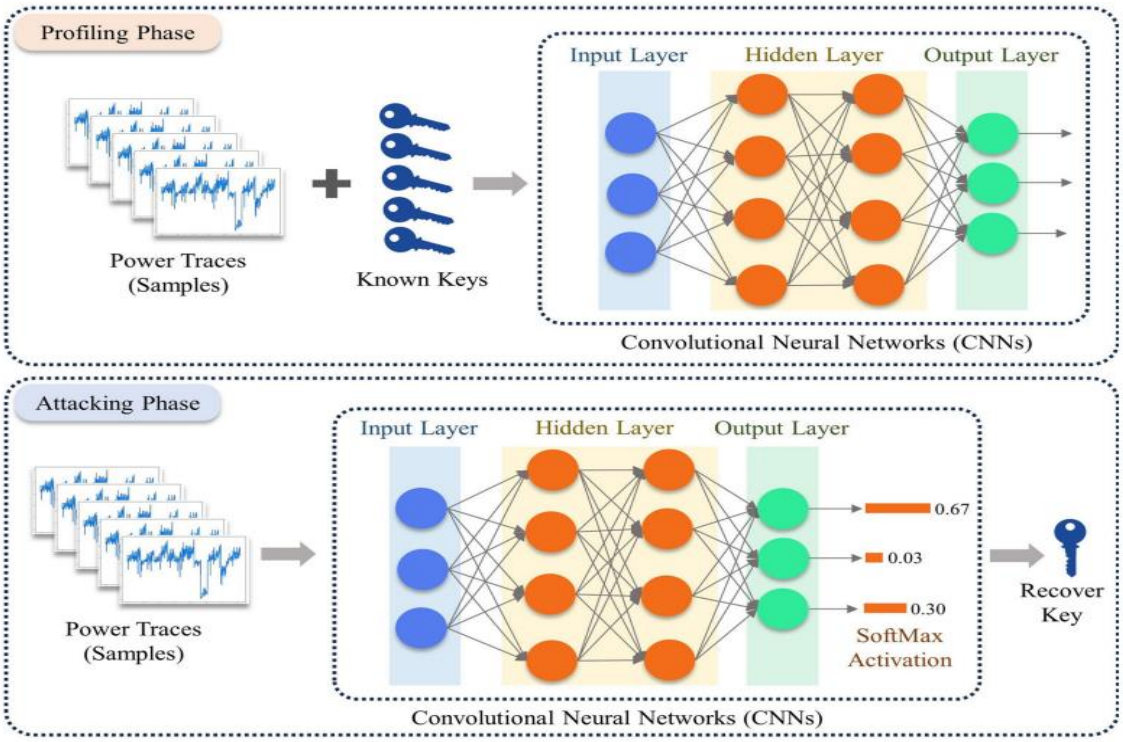

Fig.3 Profiling and attacking phase of deep learning-based side-channel attacks.

The purposed CNN architecture developed for power analysis attacks includes two contraction paths with five convolution blocks each. Each convolution block consists of a 1D convolution layer, ReLu activation function, and Max Pooling 1D function. The 1D convolution layer uses a kernel size of 3 x 3, and the number of filters in each layer is specified. The architecture processes different types of input data: power consumption traces and plaintext, extracting features and patterns relevant for determining the secret key.

The data from both input paths are concatenated and fed into fully connected layers, results in producing a probability vector generated by the Softmax function after analysing the combined data from both input paths to extract the secret key.

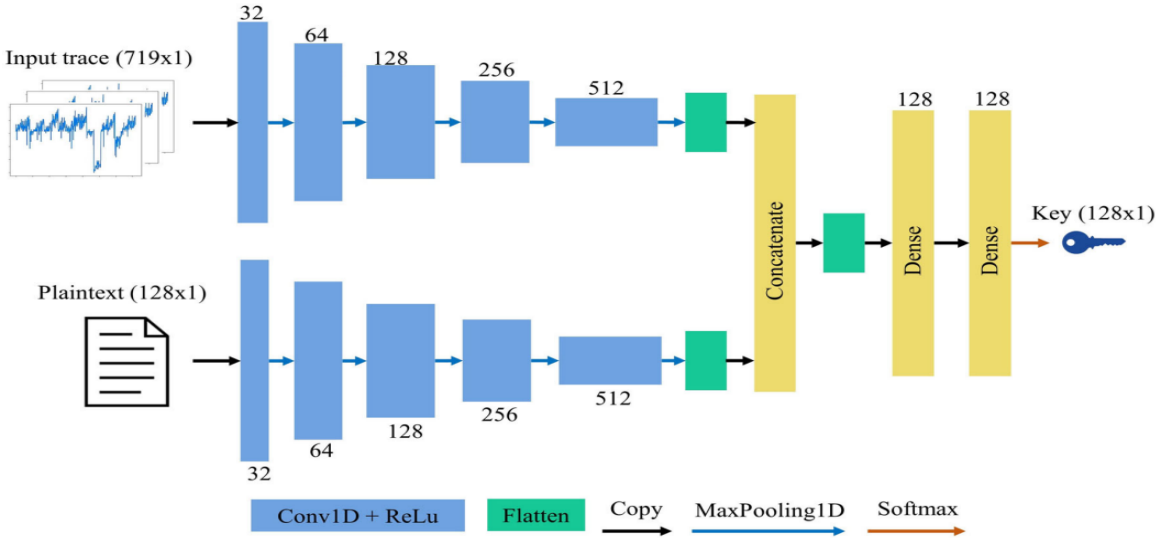

Fig.4 An overview of the proposed CNN architecture

RESULT AND CONCLUSION OF THE PAPER

The experimentation results included specific dataset usage, evaluation metrics, training setup details, and performance assessment of the AES-128 implementation on the ATmega328p.

The results show that the approach described in the paper uses only 1200 power traces to recover the AES key, which is an 8% decrease in number of traces required when compared with previous similar studies and experiments.

The DL-based power analysis attack successfully extracted AES keys from the ATmega328P microcontroller with high efficiency and robustness. The model trained on power traces achieved classification accuracy using the cross-entropy loss function and RMSProp optimization. The study demonstrated the effectiveness of DL-based side-channel attacks for extracting AES keys on the microcontroller.

SCA analysis	Algorithm	Hardware	Technology (nm)	Model DL	Target bytes	Required traces
Wang et al. [2019]	AES	FPGA	45	CNN	16	approx. 3700
Picek.S et al. [2018]	AES	FPGA	65	CNN	Single	$\geq$ 2000
Kubota et al. [2021]	AES	ASIC	180	CNN	16	$\geq$ 1300
This Paper	AES	ASIC	130	CNN	16	approx. 1200

Table.1 Summary of deep learning-based SCA on hardware implementation of AES-128

FUTURE WORKS SUGGESTED IN THE PAPER

The author suggests to extend the study to other popular microcontrollers to determine generalizability.

The author recommends exploration of other commonly used encryption algorithms in microcontrollers for key extraction using the proposed technique.

The author encourages to investigate and study countermeasures like white noise or signal distortion to protect such devices against this type of attacks.

LIMITATION OF THE PAPER

As mentioned in the paper the accuracy of DL Model used in the study may limit the effectiveness of the attack. Overall, while the paper provides valuable insights into DL-based SCAs on the ATmega328P microcontroller, further research is needed to address these limitations and strengthen the security of devices against such attack.

APPENDIX

Key Update Countermeasure for Correlation-Based Side-Channel Attacks
Gui, Y.; Tamore, S.M.; Siddiqui, A.S.; Saqib, (2020)

Side-channel attacks exploit leaked physical information from cryptographic devices, unlike traditional attacks targeting encryption algorithms. The proposed key update scheme in this paper aims to counter power and electromagnetic analysis-based attacks by utilizing a secure coprocessor for key generation and storage in a trusted environment. The paper demonstrates the vulnerability of hardware-based AES-128 to correlation power analysis (CPA) and correlation electromagnetic analysis (CEMA) attacks, successfully revealing the secret key. It introduces a flexible key update scheme that enhances resilience to side-channel attacks through experiments. The key update scheme reduces correlation and dependence between leaked information and the secret key by updating keys at short intervals. This mitigates the risk of power and EM analysis attacks, ensuring key protection. Keys are securely generated and stored on the Trusted Platform Module (TPM), supporting various encryption standards with flexible security strength. Integration of the TPM chip with FPGA fabric enhances key security by providing a secure environment for key generation and storage, safeguarding keys used for encryption.

Multi-Leak Deep-Learning Side-Channel Analysis
Hu, F.; Wang, H.; Wang (2022).

The paper addresses Deep Learning Side-Channel Attacks (DLSCAs) on cryptographic algorithms like AES, focusing on scenarios with multiple leakage intervals at a specific attack point. Existing works often train neural networks directly on traces with multiple leakages, leading to noise and reduced profiling quality. To combat this, the paper proposes a multi-input model that divides traces into leakage intervals, trains models on each interval separately, and then concatenates these models for improved performance. The study uses traces from STM32F3 microcontroller implementations of AES-128, showcasing a 2-fold enhancement over single-input attacks with the proposed multi-input model. The research investigates the impact of different fusion techniques on the multi-input model's classification accuracy, highlighting the superiority of parallel concatenation of leakage intervals.

Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA)
Lo, O.; Buchanan, W.J.; Carson, D.: Power analysis at-tacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA)(2017).

The paper focuses on power analysis attacks, specifically Differential Power Analysis (DPA) and Correlation Power Analysis (CPA), on the Arduino Uno microcontroller implementing AES-128 encryption. The authors successfully demonstrate the effectiveness of both DPA and CPA attacks on the Arduino Uno, with CPA being easier to interpret analytically.

No conflicts of interest were reported, and the work was supported by The Data Lab. The methodology provided in the paper serves as a valuable resource for researchers interested in power analysis attacks on AES-128, offering insights into the Difference of Means and Hamming Weight Power Model attacks. The paper addresses challenges in applying the methodology to real-life cryptographic devices running AES-128, suggesting solutions like monitoring power consumption during the final round of encryption to predict the cipher key values.

How Diversity Affects Deep-Learning Side-Channel Attacks

Huanyu Wang, Martin Brisfors, Sebastian Forsmark, Elena Dubrova(2019)

Deep learning side-channel attacks pose a significant threat to cryptographic algorithm implementations, where an attacker can recover unknown keys using trained models on side-channel traces. The paper emphasizes the importance of training and testing neural network models on diverse traces captured from different boards to avoid overestimating classification accuracy. Training and testing on the same board can lead to misleadingly high accuracy results. Side-channel attacks exploit information leakage like power consumption, with power analysis being a successful method to breach cryptographic algorithms. The paper highlights the vulnerability of implementations like AES to such attacks. It discusses the architecture of Multiple Layer Perceptron (MLP) networks, their components like neurons, activation functions, and training process involving weight and bias parameter updates. Additionally, Convolutional Neural Networks (CNNs) are introduced as variants of MLPs, particularly effective for recognizing patterns in multi-dimensional data like images through convolution and pooling layers.

Tandem Deep Learning Side-Channel Attack Against FPGA Implementation of AES

Huanyu Wang, Elena Dubrova (2021)

The paper introduces a novel approach in deep-learning side-channel attacks by proposing a tandem-model technique that combines multiple CNN classifiers trained on different attack points. By utilizing this tandem model, the researchers were able to significantly reduce the number of traces required to recover the key from an FPGA implementation of AES through power analysis, achieving over 40% reduction on average. The study emphasizes the importance of using diverse attack points for building the tandem model to ensure efficient classification results. Failure to do so may lead to unsatisfactory performance**.** The research also delves into the comparison between hardware and software implementations of AES, followed by an exploration of deep-learning techniques and CNNs**.** The paper concludes by highlighting the potential for further enhancement of the tandem model by incorporating more deep-learning classifiers trained on different attack points, posing an interesting open problem for future research.

Side Channel Power Analysis of an AES-256 Bootloader

Colin O'Flynn and Zhizhang (David) Chen(2015)

The paper focuses on conducting a side-channel power analysis attack on a secure bootloader encrypted with AES-256-CBC. It aims to demonstrate the vulnerability of cryptographic algorithms, specifically AES, to such attacks.
The study utilizes a Correlation Power Analysis (CPA) attack to recover the complete 32-byte key used in the encryption process. Additionally, a CPA attack is also employed to try to retrieve the initialization vector (IV) used in the encryption.
The AES algorithm involves special functions like Sub(), Shift(), and Mix() to perform substitution, row shifting, and column mixing operations. The decryption process mirrors the encryption process but in reverse, with specific rounds denoted as r14, r13, etc. The input ciphertext consists of 16 bytes.
The research demonstrates the relevance of side-channel power analysis attacks in real systems, emphasizing the need for countermeasures to secure cryptographic implementations effectively. It highlights that using strong encryption like AES-256 alone is insufficient to guarantee security against such attacks.
The paper also discusses the synchronization of power traces during the execution of the algorithm, showcasing how traces may become unsynchronized and the importance of resynchronization for the attack to continue successfully.

Differential Power Analysis
Kocher, P, Jaffe, Jun (1999)

The paper focuses on the vulnerability of cryptographic systems to Differential Power Analysis (DPA) attacks, where information leaks through power consumption during cryptographic operations.
Asymmetric operations leak stronger signals compared to symmetric algorithms due to factors like computational complexity and microprocessor characteristics.
Implementing effective DPA countermeasures can be challenging, especially for systems with large power consumption variations and operand-dependent features.
The paper discusses the leakage rate of functions as oracles providing information about computational processes and data, emphasizing the importance of leak reduction and masking techniques for security.
It also highlights the significance of preventing Simple Power Analysis (SPA) techniques, which are generally simpler to execute compared to DPA attacks.
This paper delves into the methods for analysing power consumption to extract secret keys from tamper-resistant devices and proposes strategies for developing secure cryptosystems in the presence of information leakage from hardware.

RSA Power Analysis Obfuscation: A Dynamic Algorithmic Hardware Countermeasure
Todd R. Andel, John W. Barron, J. Todd McDonald, Jeffrey W. Humphries(2014)

The paper focuses on developing a dynamic countermeasure to protect against side channel analysis (SCA) attacks on RSA encryption**.** Current SCA countermeasures are static and can be defeated with enough power traces, so the paper proposes a dynamic approach that constantly varies timing and power consumption to make

correlation between traces more difficult. By randomizing the radix of encoding for Booth multiplication and window size for exponentiation, the countermeasure increases RSA SCA attack protection up to at least 100,000 encryption cycles. The research introduces a dynamic countermeasure that incorporates run-time algorithmic randomness into operations, intermediate values, power consumption, and timing**.** This dynamic signature forces attackers to perform a 'brute force' search to achieve the correlation needed for successful attacks. The paper discusses the background on RSA, Booth multiplication, and modular exponentiation methods, introduces the dynamic algorithmic countermeasure, presents well-known side channel attacks and existing countermeasures, and provides results and metrics of implementing the countermeasures**.**

Frequency Throttling Side-Channel Attack

Liu, C.; Chakraborty, A.; Chawla, N.; Roggel(2022)

The research paper focuses on a novel type of side-channel attack called the Frequency Throttling Side-Channel Attack, which exploits CPU frequency adjustments made by power management systems in modern processors. The attack converts power side-channel information into a timing side-channel, allowing attackers to infer secret data from a victim workload, such as cryptographic keys like AES, by measuring execution times of cryptographic operations. The paper details the three phases of the attack: configuration, online, and analysis, demonstrating how reactive limits trigger frequency throttling side-channels, affecting system performance and security. Experimental evaluations showcase successful extraction of AES keys through the attack methodology, highlighting the security implications of such side-channel vulnerabilities. Mitigation strategies to counter frequency throttling side-channel attacks are discussed, providing insights into necessary conditions for such attacks and effective countermeasures to enhance system security. The paper also delves into related work, presenting options to mitigate the side-channel attack and concludes with a comprehensive analysis of the findings.

REFERENCES

- Luo, Z.; Zheng, M.; Wang, P.; Jin, M.; Zhang, J.; Hu, H.: Towards strengthening deep learning-based side channel attacks with mixup, In: Proceedings IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications Trust, pp. 791–801 (2021).
- Wang, H.; Dubrova, E.: Tandem deep learning side-channel attack against FPGA implementation of AES, In: 2020 IEEE International Symposium on Smart Electronic Systems (Formerly INiS), IEEE, pp. 147–150 (2020).
- Renauld, M.; Standaert, F.X.; Veyrat-Charvillon, N.: Algebraic side-channel attacks on the AES: Why time also matters in DPA, Lect. Notes Comput. Sci.
- Jayasinghe, D.; Ragel, R.; Ambrose, J.A.; Ignjatovic, A.; Parameswaran, S.: Advanced modes in AES: Are

they safe from power analysis based side channel attacks. In: 2014 32nd IEEE International Conference on Computer and Design, ICCD.
- Hnath, W.: Differential Power Analysis Side-Channel Attacks in Cryptography, p. 42 (2010)
- Pammu, A.A.; Chong, K.S.; Ho, W.G.; Gwee, B.H.: Interceptive side channel attack on AES-128 wireless communi-cations for IoT applications
- Dinur, I.; Shamir, A.: Side channel cube attacks on block ciphers, IACR Cryptol. EPrint Arch. 1–15 (2009)
- Wang, H.; Dubrova, E.: Tandem deep learning side-channel attack on FPGA implementation of AES. SN Comput. Sci.
- Samir, E.A.; Naoufal, R.: Compactrio based real time implementation of AES algorithm for embedded applications. Int. J. Embed. Real-Time Commun. Syst. 10, 19–36 (2019)
- Wang, H.; Brisfors, M.; Forsmark, S.; Dubrova, E.: How diversity affects deep-learning side-channel attacks (2019).
- O'Flynn, C.; David Chen, Z.: Side channel power analysis of an AES-256 bootloader. In: Canadian Conference on Electrical and Computer Engineering, pp. 750–755 (2015).
- Kocher, P.; Jaffe, J.; Jun, B.: Differential power analysis. Encycl. Cryptogr. Secur. (1999).
- Samir, E.A.; Naoufal, R.: Compactrio based real time implementation of AES algorithm for embedded applications (2019).
- Wang, H.; Brisfors, M.; Forsmark, S.; Dubrova, E.: How diversity affects deep-learning side-channel attacks(2019)
- Lo, O.; Buchanan, W.J.; Carson, D.: Power analysis at-tacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA)(2017).
- Gui, Y.; Tamore, S.M.; Siddiqui, A.S.; Saqib, F.: Key update countermeasure for correlation-based side-channel attacks. (2020).
- Hu, F.; Wang, H.; Wang, J.: Multi-leak deep-learning side-channel analysis. IEEE Access (2022).