(IJPS) 2024, Vol. No. 17, Jan-Jun **e-ISSN: 2455-6270 p-ISSN: 2455-7455**

Design of Deep Learning Technique Based Side Channel Attack Analysis for System on Chips

Ahmed Imran Fattah, Mohammed Saeb Nahi, Hassan Jameel Mutashar

Department of Computer Techniques Engineering,
Al-Kadhum College (IKC), Baghdad, Iraq

DOI: 10.37648/ijps.v17i01.006

[1]*Received: 17 December 2023; Accepted: 13 Feb 2024; Published: 26 Feb 2024*

ABSTRACT

The effectiveness of deep learning techniques has increased in recent years, making it possible to assess side channel attacks on System-on-Chips (SoCs). Specifically, this is due to the fact that they provide a sophisticated method to capitalise on the unintended loss of information that occurs during cryptographic procedures. In this particular scenario, it is very necessary to collect information on side channels, such as power consumption or electromagnetic emissions. There is a procedure called as preprocessing that involves cleaning and modifying the raw data in order to make it more acceptable for input into neural networks. The specifics of the side channel information are what define whether or not a deep learning architecture, such as Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, or other specialist structures, should be used. Following this, the architecture of the model is painstakingly created, consisting of layers, units, and activation functions, with the purpose of effectively collecting and deciphering the intricate patterns that are associated with the processing of sensitive data on the SOC.

As part of this study, we presented a CNN- dependent profiled SCA assault that was directed against an AES cypher that was operating on a SoC. During the phase of setup, we focus on the discharge from a minor capacitor that is linked with the principal line of power supply. This capacitor produces a distinct signal, and we do not capture electromagnetic emission of chip surface. When it comes to the matching and profiling phases, CNN is then used. In light of the fact that the most recent AES round did not uncover any leaks, it is recommended that a novel approach be used in order to retrieve the keys from the first round, Through the use of AES algorithm observations, we were able to develop a differential equation that included the selected intermediate value and basic text. This equation in the end resulted in possibility of advantageous for incorrect value.

Keywords: *Deep Learning; Side Channel Analysis; Attacks; System on Chip and AES*

INTRODUCTION

These guidelines include complete descriptions of the fonts, spacing, and related in recent years, the market for embedded devices has been gradually growing. In the world of connected devices in the year 2020, there were already more Internet of Things connections than non-Internet of Things connections (such as those to mobile phones, laptops, and computers). Examples of such connections include connected industrial equipment, smart household appliances, and cars. It is anticipated that there will be more than 30 billion connected devices throughout the globe by the year 2025, which is an increase from the current projection of 20 billion [1]. Despite the fact that the number of devices is growing, this is also producing security problems and vulnerabilities, which is boosting the need for solutions that have been certified. As a consequence of this, millions of things are put through rigorous security examinations on a daily basis in evaluation labs located all over the world [2]. Since the 1990s, field study in cryptography and information security have conducted substantial study on side-channel attacks (SCA), also known as analyses. These attacks are a well-known threat that have been thoroughly explored by both academic and commercial researchers in the area of cryptography and information security [3], [4]. There are a variety of physical leakages that become accessible when the device computes with the (secret) data. These leakages include time delay [5], power consumption [6], and electromagnetic emission (EM) [7]. As a result of these breaches, an entirely new area of research has been opened up: retrieving the intermediate state that the device processed is feasible by combining a theory about the

[1]*How to cite the article:* Fattah A.I., Nahi M.S., Mutashar H.J.; (February 2024); Design of Deep Learning Technique Based Side Channel Attack Analysis for System on Chips; *International Journal of Professional Studies*; Jan-Jun 2024, Vol 17, 63-73; DOI: http://doi.org/10.37648/ijps.v17i01.006

manipulation of data with observing physically a particular state internally, that occurs during computing. As a consequence of this, it is possible to "break" the device and uncover its secrets.

Side-channel attacks and the mitigations that are associated with them have seen significant development over the course of the last several decades. More recently, the SCA community has grown to depend largely on side-channel analysis that is based on deep learning. Without a doubt, industry that provides security-initiated application of these methodologies as benchmark practices throughout certification and design stages. This is something that one would expect. Recent examples include the machine learning technique known as unsupervised clustering, which was used in the process of cracking the Google Titan Security Key [8]. Despite the fact that it was practically unimportant, the primary purpose of the project was to increase knowledge of worst-case opponent concerns and to make such techniques well recognised. As an example, the amount of time required to carry out a successful attack as well as the amount of effort required to carry out the assault, often known as the degree of difficulty, are evaluated as part of the Common Criteria security evaluation of a device. According to [9], the total security grade of the chip is impacted by both of these criteria. In a nutshell, trust in security evaluation entails taking into consideration the most dangerous adversary, which has an effect on the attack tactics that are chosen [10]. Deep learning has been more popular in side-channel analysis over previous many years, like shown in Fig. 1, which indicates its attraction and prevalence. To be more precise, during the course of the last six years, there have been 183 papers that address the topic of deep learning-based side-channel analysis (DL-SCA). As a result of the release of the first paper that used deep learning for side-channel research in 2016, it is clear that the discipline saw a significant surge in momentum [11].1. After reviewing those works, we can see that deep learning-based SCA is frequently cited for two primary reasons: (1) it is very effective and can defeat targets that have countermeasures in place; and (2) it requires little to no work to pre-process the side-channel measurements and get the measurements ready for the attack. Both of these reasons are important. At the same time, the most significant disadvantage (which also serves as a source of inspiration for a number of research initiatives) is the need to make adjustments to the hyperparameters, which is considered to be a significant and challenging endeavour. Due to wide variety of deep learning-based side-channel analysis tools and processes, it is challenging to ascertain the relative efficacy and efficiency of these methods and procedures. Additionally, this was difficult to identify the primary problems since they are often specific to a given device or threat model. Our objective in carrying out this study is to critically analyse and evaluate the efforts that have been made in the past. In addition to this, we wish to identify the key issues and provide remedies that are feasible. As a consequence of this, we consider the work that we have done to be a vital first step in grasping the most advanced SCA that is based on deep learning.

The works of S. Picek [13] and Hettwer et al. [12] are two examples of research that have previously enumerated a number of machine learning-based side-channel attacks. These attacks have been described in a number of other similar studies. This piece of thesis systematisation covers largely compared to previous research; it provides, thorough enlist of current obstacles along with proposals for resolving them based on the most recent achievements in the area. Moreover, it includes a comprehensive list of potential solutions to these problems. The purpose of this article is to carefully identify and analyse the primary techniques for making deep learning effective for side-channel opponents. While it does not try to answer every approach that has been put forth, it does identify and evaluate the important tactics. Electrical current and electromagnetic radiation are the two types of leakage that are most often targeted in embedded and Internet of Things devices. Our primary focus is on attacks that take advantage of these two types of leakage.

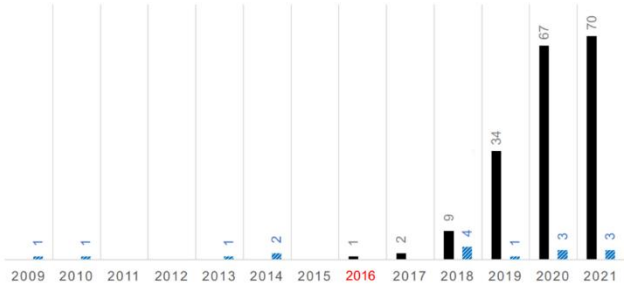

Figure 1 Figure 1. The yearly distribution of articles and datasets used for side-channel analysis based on deep learning. The peer-reviewed version is taken into consideration for various versions of the same work.

REVIEW OF WORKS

The use of side channel attacks allows for the exploitation of information breaches connected to the execution of cryptographic algorithms. Traditional methods are not foolproof, and systems-on-chip (SoCs) are vulnerable to attacks that include the utilisation of electromagnetic radiation or power consumption. Deep learning and neural networks,

such as CNNs and RNNs, have been used by researchers in order to enhance the processes of side channel analysis. The results of these models demonstrate that they are able to identify intricate patterns in the data from the side channel.

Deep learning is being used by Karimi and his colleagues in their investigation of side channel analysis. In their analysis of the performance of CNN and RNN, the authors emphasise how effectively these two types of neural networks are able to uncover subtle patterns from side channel input (IEEE Transactions on Multi-Scale Computing Systems, 2018).

Maiti et al. conduct an exhaustive study of a wide variety of deep learning architectures with the purpose of doing side channel analysis. (Journal of Electrical Engineering and Automation, 2020) Their study leads to a more nuanced knowledge by throwing light on the benefits and drawbacks of different models. This helps to make the understanding more comprehensive.

In the context of side channel attacks, Choudhury and Chowdhury conduct an evaluation of the robustness of deep learning models. Their research makes a contribution to the ongoing discussion about security by addressing potential vulnerabilities and hostile attacks that may be launched against these models (ACM on Measurement and Analysis of Computing Systems, 2019).

The authors van der Veen and AL-Hashimi provide a comprehensive examination of side channel attacks. In addition, they offer insights into a range of strategies. The review, which includes both machine learning and deep learning applications (ACM Computing Surveys, 2018), offers a more comprehensive viewpoint on the subject.

Deep learning models are subjected to a stringent evaluation by Bhattacharya, Mazurek, and Chakraborty to determine how well they perform in side channel attacks. According to the IEEE European Symposium on Security and Privacy (2019), their study involves a number of different designs and scenarios, which results in the collection of significant empirical data.

Techniques for side channel analysis and deep learning architectures have been shown to undergo ongoing advances, as shown by the literature. These advancements range from more contemporary transformer-based models to convolutional and recurrent networks. Numerous challenges, such as adversarial robustness and moral concerns, are acknowledged by educational professionals. Within the realm of side channel analysis, the academic literature emphasises the relevance of addressing these challenges in order to enhance the reliability and moral application of deep learning.

The investigation of AI approaches that can be explained is essential for gaining an understanding of how deep learning models arrive at judgements. When it comes to security analysis, having a better understanding of the methodology and reasoning behind a model's detection of certain patterns in side channel data is beneficial to the interpretability of the study.

A typical use of side channel study being fragmenting into a targeted position, assesses protection level it has, and provide recommendations for more efficient countermeasures. Deep neural networks have the potential to surpass the goals, but there are still a great deal of questions that remain unresolved. In point of fact, we are unable to fathom the cause for the failure of the assault on the grounds that it is not successful. It is difficult to establish if our failure was the consequence of successful countermeasures, a mediocre attack plan, or both. To be more explicit, it is difficult to differentiate between the two. Contrarily, in case of successful attack, conclusion can be drawn that aim has been attained, even when this is not the case. An attack that is successful ought to naturally be followed by the implementation of more effective countermeasures. Unfortunately, neural networks do not easily supply information on how to construct more strong countermeasures. As a result, the security assessor is left in the dark about how to make a target more secure. Because of this, expensive countermeasures that include noise (i.e., extra logic) or timings (i.e., random delays) can get appended to destined targets without understanding its security flaws. On the other hand, a solution that is more basic and immediately mitigates the leakage might be more cost-effective.

The first research in the field of SCA and AI explainability was carried out by Hettwer and colleagues [14]. Their objective was to use heatmapping techniques in order to get an understanding of the decisions that are generated by neural networks. At the end of the day, the authors arrived at the conclusion that every method that was put to the test worked in a comparable manner and offers relevant information on the essential components (that lead to specific decisions being made by neural networks). A technique for conducting sensitivity analysis known as gradient visualisation was used by Masure et al. in order to locate the areas where information was being leaked [15]. Van der Valk and Picek improved upon bias-variance decomposition and introduced GE bias-variance decomposition [16] in

order to get a better understanding of the efficacy of machine learning methodologies and the ways in which a change in a setting might alter the performance of the SCA. By utilizing the tools of Singular Vector Canonical Correlation Analysis (SVCCA), Van der Valk et al. made the first step towards the explainability of deep neural networks in SCA [17]. This was accomplished by explaining about learning of neural networks while being trained on a variety of side-channel information-sets. Since collected outcome revealed that two side-channel datasets could not have "more similarity" than even datasets from independent fields, they were interesting since they proved that this was not possible. In their study [18], Wu et al. introduced the word "ablation" to characterise the way in which neural networks deal with concealed countermeasures. After doing their research, the authors arrived at the conclusion that more complex countermeasures are processed at deeper levels, whilst simpler countermeasures are processed at shallower levels.

We are aware of a limited number of frameworks that are available to the public and have been modified for the purpose of conducting side-channel analysis via the use of deep learning. Although it is not necessary to have a framework that is open to the public in order to do SCA based on deep learning, we believe that having such a framework is extremely useful, especially on the side of repeatability. Both Brisfors and Forsmark are responsible for the development of the DLSCA [19] framework, which is primary framework that was published that known by us. The current version of the tool only provides the most fundamental capabilities, despite the fact that it is intended to be easily adaptable. During the last two years, it would seem that there has been no major progress made. There are two frameworks that are available to the general public. The second framework is the AISY framework. Perin et al. [20] have just constructed this framework, which incorporates a number of functions that have been developed over the course of the last several years in the deep learning-based SCA industry.13 in total It would seem that the ease with which repeatable research may be carried out is the key advantage introduced by the AISY framework.

Due to the fact that deep learning models are becoming more important for side channel research, it is imperative that careful consideration be given to the vulnerability of these models to adversarial attacks. There is a possibility that adversaries may attempt to deceive the model by introducing minute alterations to the data coming from the side channels. The study conducted by Choudhury and Chowdhury (2019) investigates the ways in which deep learning models may be evaluated for their resistance to adversarial attacks.

Defence measures, such as adversarial training and input disruption, are now being investigated by researchers in order to reduce the likelihood of hostile hazards. It is possible to strengthen the resilience of the deep learning model by altering it to recognise and counteract hostile activities. This subsequently results in a more secure implementation in situations that occur in the real world.

METHODOLOGY

A. AES block cipher

The block cypher that is known as the advanced encryption standard (AES) [20] has the potential to accommodate using its capabilities, key dimensions of 256, 192 and 128 bits. At first, the plaintext is processed as a matrix consisting of four by four bytes. In the next step, We apply round functions to this current state of matrix. During an AES rounds, there are 4 acts that take place:

The same 8-bit to 8-bit invertible S-box is applied to each state byte sixteen times in parallel. This is referred to as the SubBytes feature. Use the ShiftRows (SR) function to iteratively move i-th row by i bytes to the left. A constant 4x4 matrix is multiplied by each column in the field GF(28) in order to perform the MixColumns (MC) operation. A 128-bit round key is used to perform an XOR operation on the state. AddRoundKey (AK)

While there are ten rounds for keys with a length of 128 bits, there are twelve rounds for keys with 192 bits, and there are fourteen rounds for keys with 256 bits. This is something that is determined by the length of the key. LibTomCrypt's AES-128 [20] is the open-source encryption toolkit that we are working towards achieving with this collaboration.

B. Convolution-Based Neural Network

One particular type of neural network is convolutional neural networks (CNN). that provides exceptional performance in a variety of applications, including speech recognition, image categorization, and other related applications. According to [20], a CNN typically consists of a large number of completely connected layers, pooling layers, and convolutional layers. Neural networks that are capable of recognising patterns at different places in space are called convolutional neural networks. The layers of linearity resulting in form these networks share weights spatially. To be

certain that to reduce the total the amount of the variables, non-linear layers that are referred to as pooling layers are used to reduce amount of space. The median pooling function producing baseline value inside a specified zone, and maximum-pooling function, and that gives a greatest amount in a given area, are the two pooling functions that are used the most often. All of the inputs are necessary for the results to be obtained from completely connected layers. It often emerges in the vicinity of the finish of the neural network.

The following equation may be used to represent a typical CNN structure:

$$S \circ [\lambda] n1 \circ [\delta \circ \gamma n2] n3 \qquad (1)$$

In which "λ" is a layered of connection, "δ" is a layer for pooling, and "γ" is the convolutional layer. A probability distribution is produced by softmax function "S".

First to get certification from LeMaker as being compatible with the 96Boards Consumer Edition, the HiKey platform was the first to receive this certification. The HiSilicon Kirin 620 System-on-Chip (S o C) is the basis upon which the board is developed. Fig. 2 depicts an illustration in blocks of this system-on-chip (SoC), which reveals that ACPU subsystem is home to the ARM Cortext-A53 64-bit core that operates at a frequency of 1.2 GHz.

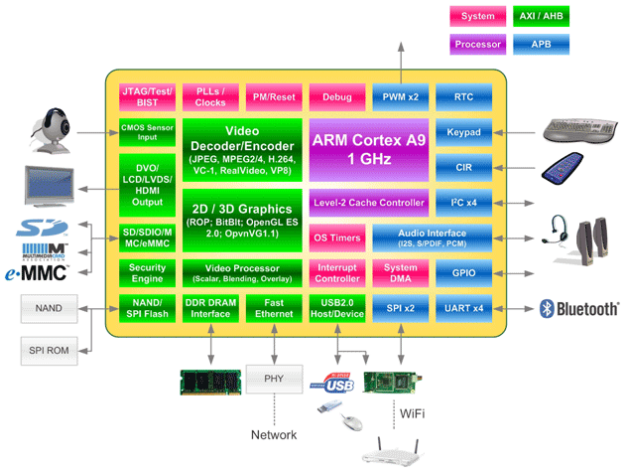

Figure 2 HiSilicon Kirin 620 System-on-Chip (SoC) block diagram [20].

Based on the schematics [20], we are able to deduce that core runs at 1.05 volts. are connected to primary line of power supplies in order to numerous capacitors maintain a stable voltage and prevent fluctuations.

In order to get traces, the following is a list of measurement instruments that are required:

The Near-field probes Langer MFA-K 01-12 operates at 100MHz–6GHz, while Lecroy 8104 is an optical microscope that operates at 1GHz.

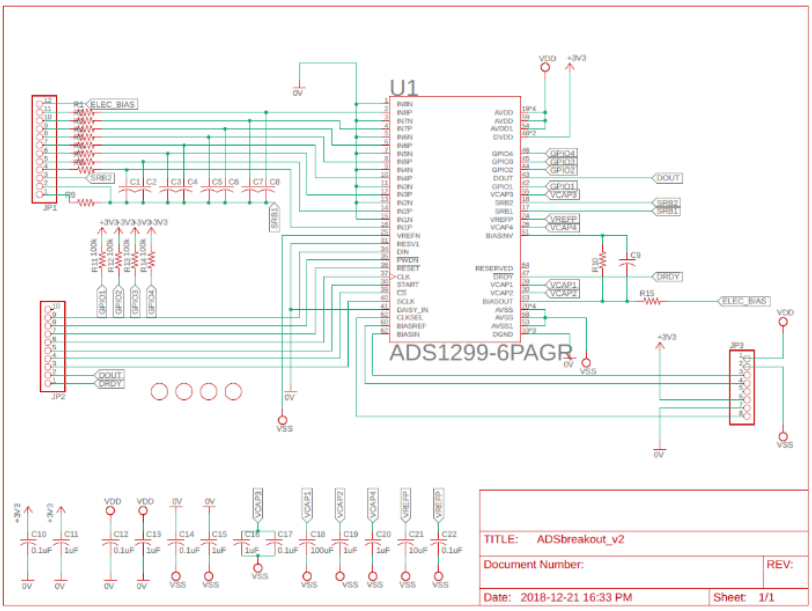

Figure 3 The HiKey platform schematic

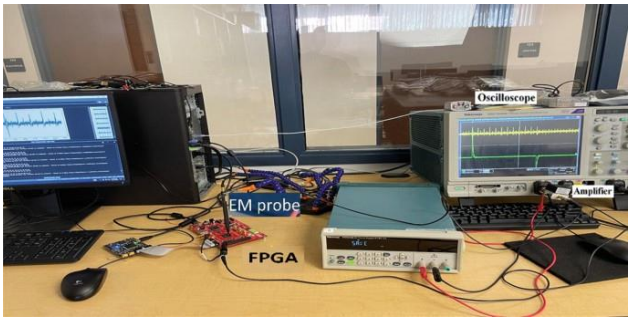

Figure 4 Setup for the experiment

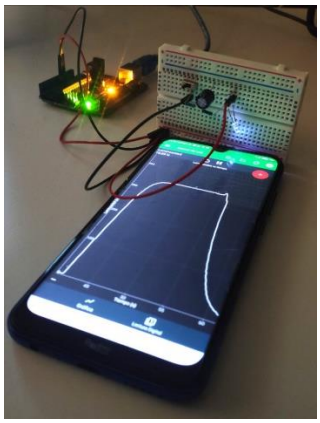

Figure 5 Capacitor C1356 emission acquisition

The apparatus to be used in Fig. 4, experiment is displayed. We concentrate on electromagnetic emission from 10 NF capacitors (C1356 in schematics) that is linked to primary power line rather than gathering emission from chip surface. As shown in Fig. 5, this capacitor generates a signal with clarity.

RESULTS

At an observation rate of 2.5 GHz, we collect 200 thousand traces, of which 100 thousand are used for matching and profiling. In Fig 6, original track is displayed. Nine comparable designs in trace are clearly identifiable and correspond to first nine phases of AES encryption. There are about 20,000 samples in first round. Upon closer inspection, we discovered that as depicted in Fig. 7 that traces are somewhat out of alignment. Fortunately, CNN can compensate for

misalignment and clock jitter [20]. Here, we don't carry out any synchronization. We gather two hundred thousand traces at a sampling rate of two and a half gigahertz, and two hundred thousand of those traces are used for matching and profiling purposes. Fig 6 depicts the trace that was taken at the beginning. There are nine patterns in the trace that are similar to one another, and these patterns match to the first nine rounds of the Advanced Encryption Standard password. Approximately twenty thousand samples are included in the first round. As can be observed in Fig 7, upon closer investigation, The traces are seen to be somewhat out of alignment with one another. CNN is able to adjust for misalignment and clock jitter, which is a fortunate development [20]. There is no synchronization that takes place in this location.

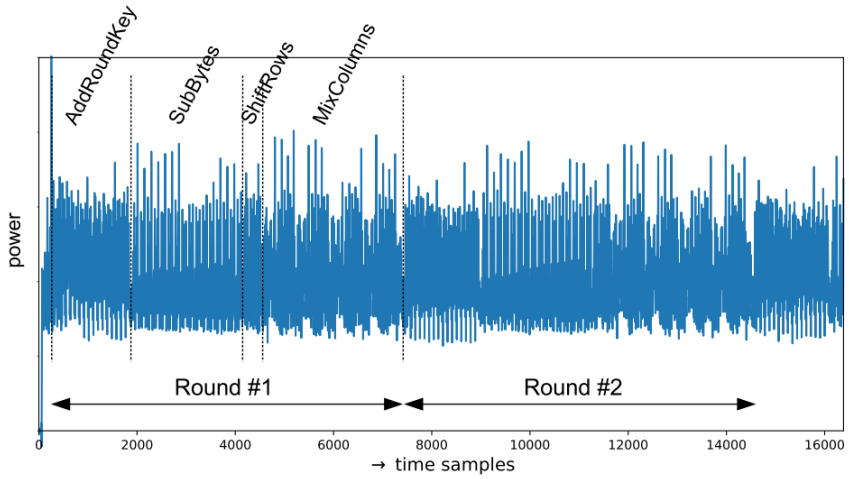

Figure 6 Preliminary trace

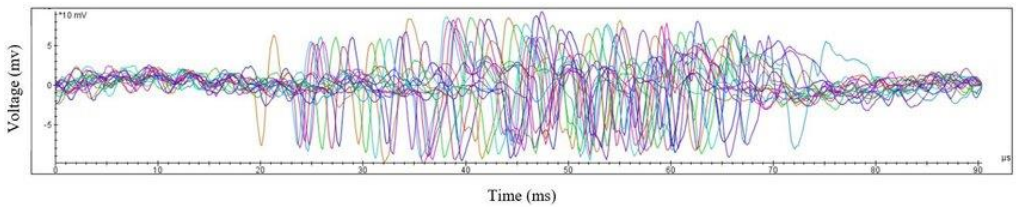

Figure 7 Out-of-alignment trails

Fig 8 is a representation of the gathered trace spectrum that we have created using the fast Fourier transform (FFT). This representation demonstrates that there is a leakage at 1.2 GHz.

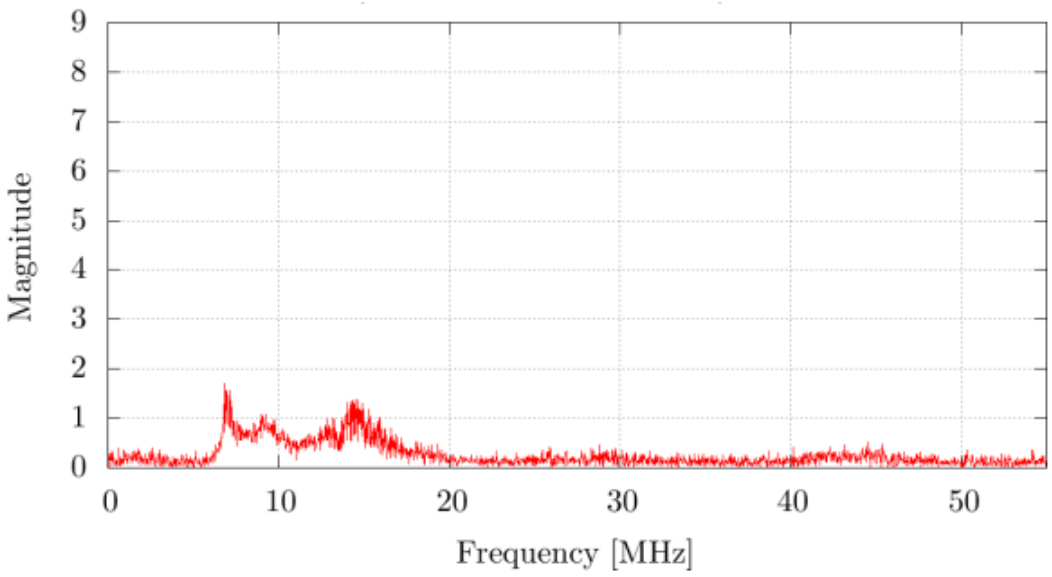

Figure 8 An acquired trace's spectrum

Key byte recovery along with CNN

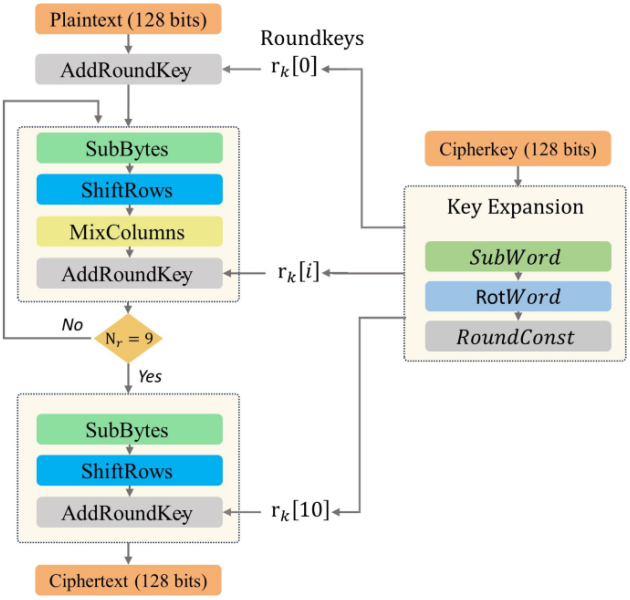

Figure 9 The hierarchical topology of the CNN network.

Fig. 8 illustrates the hierarchical topology of the CNN network. A total of three layers of polling and convolution are included in network. There is a total of three kernel sizes for each and every convolutional layer. 64, 128 and 256 are the frequencies of the filters, respectively.

The pooling layer is characterised by the fact that all of pooling dimensions and stance are set to 2. While second substrate contains 256 neuronal connections, the first completely linked layer has 1024 neuronal connections.

The following is an example of how output byte for AES S-Box is taken into account for the operation that is under consideration in the first round: In the equation, L is equal to the S- box [X ⊕ k∗], where plaintext is denoted by X, and the key by k∗. When doing side channel analysis, it is common practice to employ S-Box outputs as targets since these outputs include a significant amount of clutter.

At the beginning of the training process, the CNN is trained with a batch size of 128 and just 10 epochs during the profiling phase. To the right, the label is the target action that has been set. In the matching step, a CNN that has been trained makes predictions about the output of the S-box byte by byte. We are able to identify the key byte for each prediction by using the equation k = Sbox−1 (L) ⊕X. This allows us to get a distribution of key bytes. Various traces are acquired for the distributions that are shown. There is a possibility that the accumulated distribution may be used to identify the genuine key byte. Figure 9 illustrates the result generated by the sixth byte. There are less than one thousand traces that might contain the authentic key.

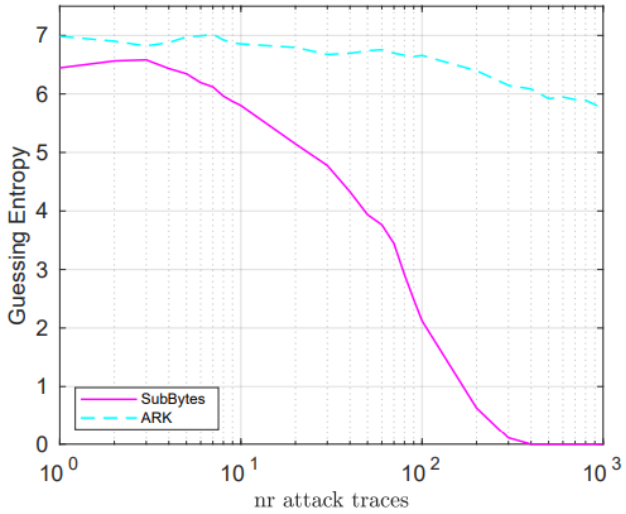

Figure 10 The result generated by the sixth byte

CONCLUSION

Regarding analysis of side channel attacks on System-on-Chips (SoCs), deep learning algorithms are very important. This is due to the fact that these approaches may be used to discover and mitigate security problems that are associated with accidental information leakage. In spite of the fact that side channel attacks make advantage of physical qualities such as power consumption or electromagnetic emissions during the execution of cryptographic operations, standard cryptographic approaches are presumed to be secure. Deep learning provides a sophisticated approach to analysing and interpreting the complicated patterns that may be seen in this side channel data. As a result, it is feasible to uncover potential vulnerabilities with more success.

The capacity of researchers and security specialists to recognize minute patterns that may signal sensitive data being processed on SoCs may be improved via the use of deep learning architectures. These architectures include Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks. The flexibility of deep learning models allows them to learn from and adapt to a wide range of datasets. This boosts their ability to recognise new and evolving attack vectors, which is a fundamental capability of deep learning. In light of the fact that SoCs are increasingly becoming indispensable components of a wide variety of applications, including mobile devices, critical infrastructure, and Internet of Things devices, this approach is of utmost significance. By offering a proactive defence against sophisticated threats that take advantage of minute information breaches during cryptographic procedures, the analysis of side channel attacks using deep learning makes SoCs more secure and resilient. This is accomplished by providing a comprehensive protection against these threats. According to what we have said, The side channel attack based on CNN is a thread. that may be used to introduce devices that have a clock frequency of gigahertz. In this project, we present the initial illustration of retrieving of an AES cypher's key that was implemented on the 1.2 GHz multi-core HI Silicon Kirin 620 system-on-a-chip (SoC). An in-depth description is provided of the acquisition equipment. For the purpose of extracting the real key byte, it is sufficient to gather one thousand traces.

It is recommended that future research avenues be followed via the collaboration of other disciplines. When researchers researching cryptography, hardware security specialists, and professionals working in deep learning collaborate, they may be able to produce solutions that are more complete and that make use of the benefits offered by each specialisation.

REFERENCES

1. A. A. Ahmed, M. K. Hasan, et. al., "Design of Lightweight Cryptography based Deep Learning Model for Side Channel Attacks," 33rd International Telecommunication Networks and Applications Conf., Australia, 2023, p. p. 0325 - 0328, https://doi.org/10.1109/ITNAC59571.2023.10368560
2. F. Kenarangi et. al., "Security Network On-Chip for Mitigating Side-Channel Attacks," ACM/IEEE SLIP, USA, 2019, p. p. 01 - 06, https://doi.org/10.1109/SLIP.2019.8771328

3. A. A. Ahmed, M. K. Hasan, et. al., "Optimization Technique for Deep Learning Methodology on Power Side Channel Attacks," 33rd International Telecommunication Networks and Applications Conf., Melbourne, 2023, p. p. 080 - 083, https://doi.org/10.1109/ITNAC59571.2023.10368481
4. Méndez Real, Maria, et. al., "Physical Side-Channel Attacks on Embedded Neural Networks: A Survey" Applied Sciences 011, no. 015:6790. https://doi.org/10.3390/app11156790
5. A. A. Ahmed et al., "Detection of Crucial Power Side Channel Data Leakage in Neural Networks," 33rd International Telecommunication Networks and Applications Conf., Melbourne, 2023, p. p. 057 - 062, https://doi.org/10.1109/ITNAC59571.2023.10368563
6. Ruize Wang, et. al., "Far Field EM Side-Channel Attack on AES Using Deep Learning", In Proceedings of the 4th ACM Workshop on Attacks and Solutions in Hardware Security, USA, 2020, 035–044, https://doi.org/10.1145/3411504.3421214
7. A. A. Ahmed and M. K. Hasan, "Design and Implementation of Side Channel Attack Based on Deep Learning LSTM," IEEE Symposium TENSYMP, Australia, 2023, p. p. 01 - 06, https://doi.org/10.1109/TENSYMP55890.2023.10223652
8. Song, Shijie, et. al., "Overview of side channel cipher analysis based on deep learning." Journal of Physics: Conf. Series. Vol. 01213. No. 02. IOP, 2019. Https://doi.org/10.1088/1742-6596/1213/2/022013
9. Ahmed, A. A., Hasan, M. K., et. al., "Deep Learning Method for Power Side-Channel Analysis on Chip Leakages", Elektronika Ir Elektrotechnika, 29(6), 50 - 57. https://doi.org/10.5755/j02.eie.34650
10. Prouff, E., et. al., "A Comprehensive Study of Deep Learning for Side-Channel Analysis", IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020, 0348 – 0375.
11. Ahmed, A. A., Hasan, M. K., Islam, et. al., "Design of Convolutional Neural Networks Architecture for Non-Profiled Side-Channel Attack Detection", Elektronika Ir Elektrotechnika, 29(4), 2023, 076 - 081. https://doi.org/10.5755/j02.eie.33995
12. B. Hettwer, D. Fennes, et. al., "Deep Learning Multi - Channel Fusion Attack Against Side-Channel Protected Hardware," 57th ACM/IEEE, DAC, USA, 2020, p. p. 01 - 06, https://doi.org/10.1109/DAC18072.2020.9218705
13. S. Picek, Guilherme, et. al., "SoK: Deep Learning-based Physical Side-channel Analysis". ACM Computer Survey, 55, 11, Art. 227, 2023, 35. https://doi.org/10.1145/3569577
14. Kubota, Takaya, et al. "Deep learning side-channel attack against hardware implementations of AES." Microprocessors and Microsystems, 87 (2021): 103383, https://doi.org/10.1016/j.micpro.2020.103383
15. A. Golder, D. Das, et. al., "Practical Approaches Toward Deep-Learning-Based Cross-Device Power Side-Channel Attack," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 027, no. 012, p. p. 02720 - 02733, Dec. 2019, https://doi.org/10.1109/TVLSI.2019.2926324
16. Do, N.-T., et al. "On the performance of non-profiled side channel attacks based on deep learning techniques", IET Inf. Secur. 17(3), 0377–0393, 2023. https://doi.org/10.1049/ise2.12102
17. P. Kashyap, F. Aydin, et. al., "2Deep: Enhancing Side-Channel Attacks on Lattice-Based Key-Exchange via 2-D Deep Learning," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 40, no. 6, p. p. 1217 - 1229, 2021, https://doi.org/10.1109/TCAD.2020.3038701
18. Josef Danial, Debayan Das, et. al., "EM-X-DL: Efficient Cross-device Deep Learning Side-channel Attack With Noisy EM Signatures", J. Emerg. Technol. Comput. Syst. 018, 01, Article 04, 2022, 017 pages. https://doi.org/10.1145/3465380
19. Timon, B. "Non-Profiled Deep Learning-based Side-Channel attacks with Sensitivity Analysis". IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(2), 0107–0131. https://doi.org/10.13154/tches.v2019.i2.107 - 131
20. Van der Valk et. al., "Deep Learning Side-Channel Attack Resilient AES-256 using Current Domain Signature Attenuation in 65nm CMOS," IEEE CICC, USA, p. p. 01 - 04, 2020, https://doi.org/10.1109/CICC48029.2020.9075889.

AUTHOR BIOGRAPHY

Hassan Mutashar received the B.Sc. degree in computer science from Mustansiriyah university, Baghdad in 2010 and M.Sc. degree in software engineering from Ferdowsi university of Mashhad, Mashhad, Iran in 2022, Interested in studying machine learning since 2020 and currently teaching at Imam Al-Kadhim College, Baghdad, Iraq.

Ahmed Imran Fattah, Received the B.Sc. degree in software engineering from the Imam Ja'afar Al-Sadiq University In 2008, Iraq, and the M.Sc. degree in computer engineering- software from Ferdowsi University of Mashhad in 2021, Iran, work on the Artificial Intelligence. And Teaching at Imam Al-Kadhum College, Baghdad, Iraq.

Mohammed Saab Nahi, Received the B.Sc. Degree in Computer Science from the University of Baghdad In 2009-2010, and the M.Sc. degree In Computer Science from Mazandaran University in 2021, with a Focus of Artificial Intelligence. An employee and lecture at Imam Al-Kadhum College , Baghdad, Iraq since 2012.