Side Channel Attack using Machine Learning

Amina Amrouche[1,2], Larbi Boubchir[1] and Said Yahiaoui[2]

[1]*LIASD research Lab., University of Paris 8, France*
[2]*Research Center on Scientific and Technical Information (CERIST), Algiers, Algeria*
{amina_amrouche@outlook.fr, larbi.boubchir@univ-paris8.fr, syahiaoui@cerist.dz}

***Abstract*—The overwhelming majority of significant security threats are hardware-based, where the attackers attempt to steal information straight from the hardware that our secure and encrypted software operates on. Unquestionably, side-channel attacks are one of the most severe risks to hardware security. Rather than depending on bugs in the program itself, a side-channel attack exploits information leaked from the program implementation in order to exfiltrate sensitive secret information such as cryptographic keys. A side channel assault could manifest in different ways including electromagnetic radiation, power consumption, timing data, or even acoustic emanation. Ever since the side-channel attacks were introduced in the 1990s, a number of significant attacks on cryptographic implementations utilizing side-channel analysis have emerged, such as template attacks, and attacks based on power analysis and electromagnetic analysis. However, Artificial Intelligence has become more prevalent. Attackers are now more interested in machine learning and deep learning technologies that enable them to interpret the extracted raw data. The aim of this paper is to highlight the main methods of machine learning and deep learning that are used in the most recent studies that deal with different types of side-channel attacks.**

***Index Terms*—Side-channel attacks, Power analysis, Electromagnetic analysis, Machine learning, Deep learning.**

I. Introduction

Cryptanalysis refers to the process of decrypting ciphertext without the use of the actual key and to the process of analyzing cryptosystems to comprehend their functions. An alternative way to explain it : cryptanalysis is a method for getting at the plain text in transmission when you don't have access to the decryption key. A field in cryptanalysis that has grown in popularity recently is the Side-Channel Analysis (SC-Anal) [1]. The latter brings the issue of revealing secret information out of the domain of mathematics into the domain of physical implementation. Researchers have noticed that by focusing on the implementation of cryptosystems rather than their specifications, they can conduct attacks that are low-cost in terms of the time and resources needed, and extremely successful in obtaining valuable results. A side-channel attack (SCA) is a security vulnerability that relies on information obtained from the hardware implementation of a program instead of the programming errors. A SCA may include power consumption, electromagnetic emanations, and acoustic emissions, among other varieties. The security community has been very interested in physical attack vectors ever since P. Kocher released the first side channel attack back in 1996 [2]. Several side-channel attacks such as Simple (SPA), Differential power analysis (DPA), ElectroMagnetic analysis (EMA), and Template attacks, have long been the main subject of research. The idea of using machine learning techniques for side-channel analysis, however, became actively investigated as a result of recent advancements in machine learning (ML) and deep learning (DL) technologies.

This paper aims to review a number of new studies on side-channel attacks using ML and DL techniques. Each study will be briefly discussed to explain its main ideas and demonstrate how researchers approached each specific SCA class.

The structure of this article will be as follows: Section II will include background information on side-channel attacks, machine learning, and deep learning. The studies on ML and DL applications used in side-channel attacks are examined in Section III. In Section IV we wrap up our research with a brief review and outline of potential future work.

II. Background

A. Side-Channel Attacks

The vast majority of serious security threats are hardware-based, where the attacker can steal information directly from the hardware that our secure and encrypted software runs on. Side channel attacks are considered one of the most severe risks to hardware security.

a) Types of side-channel attacks: Malicious hackers can perform side-channel attacks in a number of ways, including the following:

- **Electromagnetic:** One of the earliest side-channel attacks, measures and analyzes the radio waves or electromagnetic radiation emitted from a target device in attempt to reconstruct the internal signals of that device. Van Eck phreaking [3] is an example of an EM attack.
- **Power:** Measures or influences the power consumption of a device or subsystem. In order to determine the input of the computation, a power-based SCA examines how power consumption changes during the course of the computation. An attacker can determine the activity of a system by watching the amount and timing of power used by that system or one of its components.
- **Acoustic:** Measures the sounds produced by a device. By listening to the sounds that electronic components generate, hackers can obtain information.
- **Timing:** Analyzes the time a system spends running cryptographic algorithms. The total time can provide data

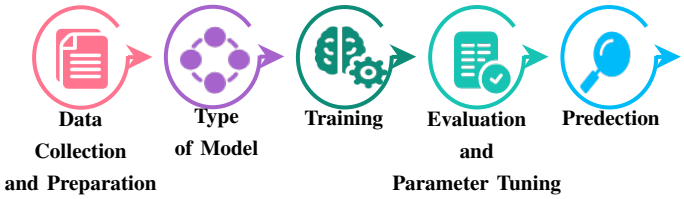

Fig. 1. Steps of machine learning.

about a system state or the type of process running. To create precise predictions, the attacker can compare the duration of a known system with that of the victim system.

b) Categories of side-channel attacks: They are usually divided into two categories: Profiling SCAs and Non-Profiling SCAs.

- **Profiling side-channel attacks:** The strongest variety of SCA. When executing a profiling SCA, two steps are taken into account. The attacker initially obtains a clone of the target device in order to determine the relationship between the modified data and the device behavior. He then launches a key-recovery attack against the target device. This kind of attack includes stochastic models, template attacks, which are acknowledged to be one of the most powerful profiled attacks, and machine & deep learning-based SCAs.
- **Non-Profiling side-channel attacks:** This corresponds to a significantly less effective attack, where an adversary can only access the physical leakage that the target device has let out. In order to retrieve the secret information, the attacker can gather and measure a set of side-channel traces and then apply statistical methods to map the traces to the sensitive intermediate values being processed by the device. Non-profiling SCAs include differential power analysis (DPA), correlation power analysis (CPA), and mutual information analysis (MIA).

Approaches from machine learning have already been used in cryptanalysis. In [4], Rivest noticed the similarity between cryptographic ”secret key” and ”target function” in machine learning. Based on this work the idea of employing machine learning in side-channel attacks has been introduced. The earliest application of ML in SCA was in the study involving a printer acoustic emission.

B. Machine learning

An application of Artificial Intelligence (AI) that allows computers to learn from experience and develop without being explicitly programmed. The goal of machine learning is to create computer programs that can access data and use it to acquire knowledge on their own [5].

a) Steps of Machine Learning:

- **Data collection and preparation:** This is the first step in machine learning. This is essential since the quantity and quality of the data collected will have a significant impact on the results. Second, the gathered data must be prepared for use in the machine learning training phase. To prevent the order of the data from affecting the training, the data will be randomized. The last step in data collection is splitting the cleaned data into two sets: a training set and a testing set.
  - The training set is the set the model learns from
  - The testing set is used to evaluate your model's accuracy following training.
- **Type of model:** The next step is to select a model based on the issue at hand, such as logistic regressions, decision trees, and linear models.
- **Training:** This is the most important step in ML. The ML model will receive the prepared data and use it to search for patterns and generate predictions. As a result, the model gains knowledge from the data to complete the given task. The model improves in prediction over time with training.
- **Evaluation and parameter tuning:** The effectiveness of the model will be evaluated using the second data set that was set aside. The model's performance when dealing with fresh data serves as an indicator of how it will perform in reality. Once the evaluation is done, the training phase will be tested to see whether there is still room for improvement through parameter tuning.
- **Prediction:** In the end, the model will be used on unseen data to make precise predictions.

b) Categories of machine learning: Modern machine learning algorithms can be divided into three primary categories: (i) supervised learning, (ii) unsupervised learning, and (iii) reinforcement learning. Casting Reinforced Learning aside, Supervised and Unsupervised learning are the primary two categories of machine learning problems.

- **Supervised machine learning**: It uses labeled datasets to train algorithms that reliably classify data or predict outcomes. Under the umbrella of supervised learning falls two major fields: classification and regression.
  - **Classification:** From observed values, the machine learning program must make a conclusion and decide which category a new observations fall within.
  - **Regression:** Machine learning estimates and comprehends the relationships among variables when doing regression tasks.
- **Unsupervised machine learning:** It analyzes and clusters unlabeled datasets. These algorithms identify hidden patterns or data clusters without the assistance of a human. Based on that, much like in supervised learning, we also distinguish between two fields: clustering and association rule.
  - **Clustering:** It involves assembling groups of related data based on predetermined criteria. Which can be useful for segmenting data into several groups and performing analysis on each data set to find patterns.
  - **Association rule:** Generally speaking, the association rule is a method for uncovering interesting relations or associations among the variables of the

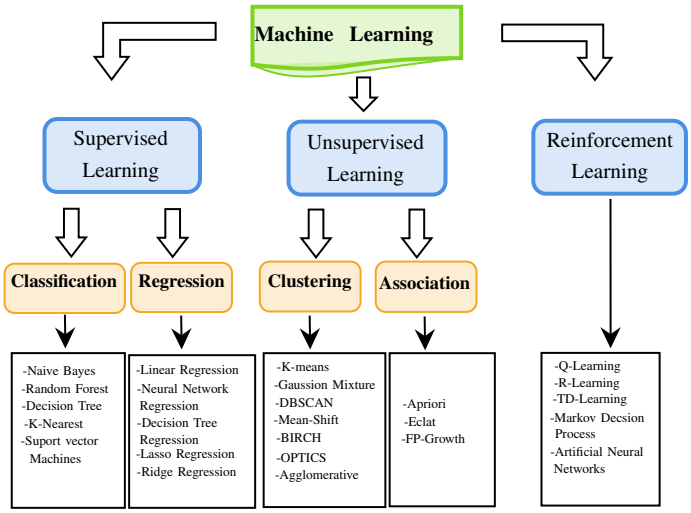

Fig. 2. Algorithms of machine learning.

dataset by determining whether one data item depends on another and then creating maps that are more profitable as a result.

- **Reinforcement Learning:** This is the process of teaching machine learning models to make a sequence of decisions. Artificial intelligence encounters a scenario similar to a game in reinforcement learning. In order to solve the problem, the computer uses trial and error; where the AI is rewarded or punished for the actions it takes. The goal is to maximize the overall rewards.

In figure 2, a number of machine learning algorithms are listed.

The two main concepts in making AI possible are machine learning and deep learning. The two terms are often conflated, although they actually describe two fundamentally different methodologies, each with a particular range of applications. ML relies on humans to select the features, while DL architectures can automatically extract features and generate models that are more comprehensive.

C. Deep learning

Formally speaking, deep learning is a machine learning technique that trains computers to do what comes easily to humans: learn by example. Deep learning is a subset of machine learning that is entirely founded on artificial neural networks, much like an artificial neural network is a form of imitation of the human brain.

In figure 3, a number of deep learning algorithms are listed.

III. Machine Learning in Side-Channel Attacks

Ever since Rivest [4] first introduced the principle of using machine learning in cryptography a lot of scientists have expressed interest in this domain.

In a 2010 study [5], machine learning was used for the first time in a side-channel attack to demonstrate the feasibility of

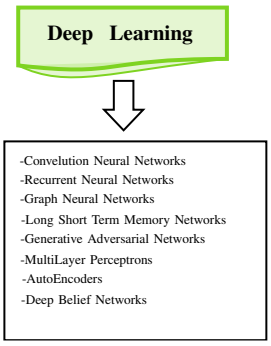

Fig. 3. Algorithms of deep learning.

recovering printed text by listening to the sound of a printer at work. By using machine learning techniques, the authors were able to recover up to 95% of English text just from a previously recorded sound of a printer at work. However, according to to [6], side-channel attacks typically target cryptography and attempt to recover secret information, such as keys, through side signals. Several power attacks attempted to recover the AES key using Least Squares Support Vector Machines (LS-SVM), but it wasn't until 2014 [7] that a successful assault against AES using SVM was established.

A comparison between ML and DL approaches in side-channel attacks was established in [8]. The authors concluded that even though recent studies have shifted their focus to DL, and DL models may outperform the conventional ML models. ML algorithms are not entirely replaceable and can perform at a similar level or even surpass DL algorithms. This concept was made abundantly clear in the 2018 publication [9] which compared several ML techniques and CNN architecture on a profiled SCA. [8] also brought to light some limitations of DL in side-channel attacks, for instance, the limited number of DL models that can be used for side-channel attacks. AE, MLP, CNN, and RNN are some of them. The limited number of studies on non-profiled side-channel attacks and the insufficiency of work on encryption techniques that defend against profiled attacks. Another point to note in [8] is that all the works discussed are concerned with power analysis.

[10] presented an overview of the use of traditional machine learning techniques -excluding deep learning techniques- in the field of side-channel analysis. It provided an overview of the historical application of machine learning techniques in side-channel analysis, as well as a brief discussion of certain machine learning methodologies that have been used in relevant studies. These studies examine numerous scenarios where the proper application of ML approaches could improve SCAs.

Deep learning-based side-channel analysis has drawn increasing attention. To improve the effectiveness of SCAs, numerous DL networks or models have been developed. Few studies, however, have investigated the impact of the different models on attack outcomes and the precise link between power consumption traces and intermediate values. [11] suggested a

Template Analysis Pre-trained DL classification model, called TAPDC, which is a three-layer subnetwork based on the convolutional neural network and the autoencoder. The TAPDC model analyzes the power trace to determine its periodicity, link power to intermediate values, and explore deeper features using a multi-layered convolutional network. In [11], the TAPDC model was implemented, and it was compared with two classical models. The experiment results showed that data may be extracted from the power consumption trace more effectively using the TAPDC model with an autoencoder and deep convolution feature extraction structure in the SCA.

The ability of a machine to solve issues that humans might find insurmountable due to biases or limited capacity is the main advantage of unsupervised learning. The latter is the best method for investigating unstructured data. A 2013 study [12] is one of the initial pieces of research to propose employing unsupervised learning for power analysis.

Model-based attacks and stochastic attacks are combined with the novel unsupervised key recovery method known as the Evil Machine Attack (Evil-MA) [13] (based on a GAN-Like structure) to show that it only requires one network training regardless of the number of key hypotheses. Thus, Evil-MA resolves the two main drawbacks of unsupervised deep learning attacks.

The two techniques that are typically employed in side-channel attacks are electromagnetic and power analysis. They have attracted a lot of attention from researchers. However, further consideration must be given to EM analysis based on ML. [14] established a comparison between several ML strategies after determining the best feature extraction/selection and pre-processing techniques for the leaked EM data collected while AES is running on Kintex-7 FPGA board. In contrast, [15] has developed a tool for Deep Learning Side-Channel Analysis (DLSCA). It demonstrated the steps involved in training and testing a Multiple Layer Perceptron (MLP) model trained on EM side-channel traces using DLSCA.

Another interesting concept of EM analysis is far-field EM emissions. [16] is the first side-channel attack on AES-128 based on deep learning using EM emissions in the far field. It showed that it is possible to train a neural network to recover the key from a separate device that is identical to the profiling ones by using a trace set that contains traces taken from various profiling devices at different distances from the target.

On the flip side, acoustic SC, much like power and electromagnetic analysis, is another interesting SCA concept. Acoustic CSAs are based on the noise made by the target device. Despite not being employed in key recovery attacks yet, Acoustic SC has been used to recover other kinds of valuable data. For instance, [17] suggested a brand-new technique for building a classifier to categorize a multi-tenant server's power consumption. It employed frequency features based on acoustic side-channels from a multi-tenant server to classify the data. On the other hand, a 2021 publication [18] captured the acoustic SCA from a set of similar devices, then used DL techniques to analyze the recordings and distinguish one device from another.

IV. Conclusion and perspectives

The aim of this paper is to highlight the various research projects done in each SCA category individually. Using ML and DL methods to obtain confidential data, we offered an overview of the major SCA categories in this work. First, we provided fundamental knowledge about SCAs, ML, and DL technologies. Then, we discussed the scientific papers and gave a brief summary of each. The conclusion and a list of future perspectives came last.

Putting this study's findings in perspective, SCAs and ML strategies pose a severe threat to cryptographic implementations. When employed in SCAs deep learning models might outperform ML. However, ML algorithms can perform on par with or even better than DL algorithms, thus ML techniques are not completely replaceable. Another point to consider is the need for additional research on unsupervised learning in SCAs.

Future research may investigate the usage of GNN technologies for SCAs. Another intriguing aspect would be recovering secret keys using information leaked from acoustic SCAs. Furthermore, ML and DL methods can also be used to defeat equipment with stronger side-channel countermeasures. Since ML and DL are currently dynamic fields in SCAs, many new concepts and methods should emerge in the near future.

References

[1] Nigel Smart, P., "Physical Side-Channel Attacks On Cryptographic Systems", Software Focus, vol. 1, no 2, pp. 6–13, 2001.

[2] Kocher, P. C., "Timing Attacks on Implementations of diffie-hellman, RSA, DSS, and Other Systems", In: Koblitz, N. (eds) Advances in Cryptology — CRYPTO '96. CRYPTO 1996. Lecture Notes in Computer Science, vol 1109, pp. 104–113, Springer, Berlin, Heidelberg, 1996.

[3] Wim van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?", Computers & Security, vol. 4, no. 4, pp. 269–286, 1985.

[4] Rivest, R. L., "Cryptography and machine learning", In: Imai, H., Rivest, R.L., Matsumoto, T. (eds) Advances in Cryptology — ASIACRYPT '91. ASIACRYPT 1991. Lecture Notes in Computer Science, vol 739, pp. 427–439, Springer, Berlin, Heidelberg, 1991.

[5] Backes, M., Dürmuth, M., Gerling, S., Pinkal, M., Sporleder, C., "Acoustic side-channel attacks on printers", USENIX, p. 20, USENIX Association, USA, 2010.

[6] Levina, A., Sleptsova, D., Zaitsev, O., "Side-channel attacks and machine learning approach", The 2016 18th Conference of Open Innovations Association and Seminar on Information Security and Protection of Information Technology (FRUCT-ISPIT), pp. 181–186, 2016.

[7] Zeng, Z., Gu, D., Liu, J., Guo, Z., "An improved side-channel attack based on support vector machine", In 2014 Tenth International Conference on Computational Intelligence and Security, pp. 676-680, 2014.

[8] Shaikh, M., Arain, Q. A., Saddar, S., "Paradigm Shift of Machine Learning to Deep Learning in Side Channel Attacks – A Survey", In 2021 6th International Multi-Topic ICT Conference (IMTIC), pp. 1–6, 2021.

[9] Picek, S., Samiotis, I. P., Kim, J., Heuser, A., Bhasin, S., Legay, A., "On the performance of convolutional neural networks for side-channel analysis", In: Chattopadhyay, A., Rebeiro, C., Yarom, Y. (eds) Security, Privacy, and Applied Cryptography Engineering. SPACE 2018. Lecture Notes in Computer Science(), vol 11348, pp. 157–176, Springer, Cham, 2018

[10] Jovic, A., Jap, D., Papachristodoulou, L., Heuser, A., "Traditional machine learning methods for side-channel analysis", In: Batina, L., Bäck, T., Buhan, I., Picek, S. (eds) Security and Artificial Intelligence. Lecture Notes in Computer Science, vol 13049, pp. 25–47, Springer, Cham, 2022.

[11] Ou, Y., Li, L., "Side-channel analysis attacks based on deep learning network", Frontiers of Computer Science, Springer, 16, 162303, 2022.
[12] Chou, J. W., Chu, M. H., Tsai, Y. L., Jin, Y., Cheng, C. M., Lin, S. D, "An Unsupervised Learning Model to Perform Side Channel Attack", In: Pei, J., Tseng, V.S., Cao, L., Motoda, H., Xu, G. (eds) Advances in Knowledge Discovery and Data Mining. PAKDD 2013. Lecture Notes in Computer Science(), vol 7818, pp. 414–425, Springer, Berlin, Heidelberg, 2013.
[13] Cristiani, V., Lecomte, M., Maurine, P., "The EVIL Machine: Encode, Visualize and Interpret the Leakage", Cryptology ePrint Archive, 2022.
[14] Mukhtar, N., Kong, Y., "Hyper-parameter optimization for machine-learning based electromagnetic side-channel analysis", In 2018 26th International Conference on Systems Engineering (ICSEng), pp. 1–7, 2018.
[15] Brisfors, M., Forsmark, S., "DLSCA: a tool for deep learning side channel analysis", Cryptology ePrint Archive, 2019.
[16] Wang, R., Wang, H., Dubrova, E., "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, pp. 35–44, 2020.
[17] Karimi, M., Arab, F., "Machine Learning Based Framework for Estimation of Data Center Power Using Acoustic Side Channel", arXiv preprint arXiv:2008.02481, 2020.
[18] Adhin, V. S., Maliekkal, A., Mukilan, K., Sanjay, K., Chitra, R., James, A. P., "Acoustic Side Channel Attack for Device Identification using Deep Learning Models", In 2021 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 857–860, 2021.