# Investigating Machine Learning-based Attacks on Random Frequency Tuning-based Countermeasures


Chandrasekara C.M.A
*Department of Computer Engineering*
*University of Peradeniya*
Sri Lanka
e17038@eng.pdn.ac.lk

Gunathilaka S.P.A.U
*Department of Computer Engineering*
*University of Peradeniya*
Sri Lanka
e17101@eng.pdn.ac.lk

Rilwan M.M.M
*Department of Computer Engineering*
*University of Peradeniya*
Sri Lanka
e17292@eng.pdn.ac.lk

Damayanthi Herath
*Department of Computer Engineering*
*University of Peradeniya*
Sri Lanka
damayanthiherath@eng.pdn.ac.lk

Darshana Jayasinghe
*dept. name of organization (of Aff.)*
*name of organization (of Aff.)*
City, Country
darshana.jayasinghe@gmail.com

Manjula Sandirigama
*Department fo Computer Engineering*
*University of Peradeniya*
Sri Lanka
manjula.sandirigama@eng.pdn.ac.lk


## I. Introduction

Side-channel attacks (SCAs) pose a significant threat to the security of cryptographic systems, as they exploit unintended information leakage through side channels such as power consumption, timing variations, or electromagnetic radiation. These attacks aim to extract sensitive information, like secret keys, by analyzing the physical implementations (as mentioned above) of a cryptographic device rather than directly breaking the algorithm.

In recent years, deep learning (DL) techniques have gained considerable attention and success in various fields, and domains. When we speak about Deep Learning algorithms, we have Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM), Generative Adversarial Networks (GANs), Reinforcement Learning (RL), Deep neural networks (DNNs), Convolutional neural networks (CNNs) etc. Each algorithm has its own strengths and applications. The choice of algorithm depends on the nature of the problem or issue and the characteristics of the data. But most of the cases have been captured by Deep neural networks (DNNs) and Convolutional Neural Networks (CNNs). Both algorithms have shown remarkable capabilities in capturing complex patterns and extracting meaningful features from high-dimensional data. When we went through related researches or publications Convolutional Neural Networks has played a major role.

Deep Learning based SCA attacks leverage the power of neural networks to learn the complex relationship between the observed side-channel leakage and the underlying secret key even without knowing the algorithm. By training DL models on large amount of datasets of side-channel measurements or traces, these attacks can enhance the efficiency and accuracy of information extraction, even in the presence of countermeasures.To train DL models, it requires substantial amounts of labeled training data, which may be costly or time-consuming to obtain. But, currently its not a big issue since some research in this field have already addressed these issues.

This field, Deep Learning based SCA attacks is rapidly evolving, and numerous research papers have been published.These papers explore various aspects, including the design and architecture of DL models, the impact of different network configurations on attack performance, and the effectiveness of DL-based attacks against different cryptographic devices and countermeasures.

In this paper, we expect to discuss the test results of RFTC against ASCAD, AISY and SCAAML frmework, about improved MLP andd CNN models to attack RFTC and also test results of attacking other block cipher circuit (PRESENT, Simon, Speck etc ...) using the developed CNN or MLP models.


Identify applicable funding agency here. If none, delete this.


## II. Literature Review

### A. Template Attack

Template attack requires a precomputation phase (attacker collects a set of side-channel traces, along with their corresponding known plaintexts and the secret keys), during this phase the attacker performs statistical analysis on the new set of side channel traces from the target device. As the number of side-channel features increases, the dimensionality of the data space also increases.This leads to several problems.So available data becomes sparse in high-dimensional spaces, making it difficult to estimate accurate statistical models or capture meaningful patterns.Analyzing the data increases exponentially with the number of dimensions, making it computationally expensive and time-consuming. In recent years, two

popular approaches to side-channel analysis have emerged: template attacks and machine learning-based attacks. Template attacks are the method of choice when a limited number of Points of Interest (POI) can be identified in leakage traces and contain most of the information. However, as the number of useless samples in leakage traces increases, then machine learning-based attacks gain interest [4].

### *B. Machine Learning based Attack*

As mentioned in the template attack, the dimensionality issue discussed as "curse of dimensionality" in publications or research papers.Dimension reduction techniques like PCA (Principal Component Analysis) and LDA (Linear Discriminant Analysis) can be used to overcome this problem [6]. But most papers [references to add] discuss the use of machine learning attacks on PRESENT and AES in the profiled channel analysis.

Classical machine learning techniques have been extensively studied and explored by researchers. These include popular methods such as Random Forest [5], Support Vector Machines, and Naive Bayes [6]. In addition, researchers in previous years frequently employed the use of multilayer perceptron.These techniques have garnered significant attention in the research community due to their efficacy in various domains. Random forest, for instance, employs an ensemble of decision trees to make predictions [5]. Naive Bayes, a probabilistic classifier based on Bayes' theorem, has been widely used for text classification and spam filtering tasks.By the growth of deep learning field, there are several algorithms have emerged but most of the papers discuss about Deep neural networks (DNNs) and Convolutional Neural Networks (CNNs)[aisy ref no]

### *C. Multiple Device Model*

Profiled side-channel attacks such as Correlation Power Analysis (CPA), Differential power analysis (DPA) have gained prominence due to their ability to exploit side-channel leakages to extract sensitive information.In these attacks, adversaries leverage knowledge gained from accessing a cloned device to infer the secrets of the target device. But here portability play a major role,the portability issue arises when the profiling information needs to be applied to the target device, which may be a separate device with potentially different characteristics, such as manufacturing variances or operating conditions.The challenge lies in accurately transferring the profiling information from the profiling device to the target device, accounting for these differences and ensuring the effectiveness of the attack.

To mitigate this issue, a novel Multiple Device Model (MDM) [1] that formally incorporates the variations between profiling and target devices was proposed. There, leveraging deep learning algorithms and the MDM approach, authors showcase the substantial enhancements in attack performance, effectively neutralizing the impact of portability.

### *D. Deep learning for side-channel analysis*

Even though many research papers have demonstrated the effectiveness of deep learning algorithms in evaluating the security of embedded systems and highlighted their advantages over other methods, authors of those papers have often kept their hyperparameter settings confidential, focusing only on the main design principles and attack efficiencies in specific contexts. ASCAD paper[7] addresses these limitations in multiple ways. Building upon previous work, authors examine the application of deep learning algorithms in the context of side-channel analysis and discuss their relationship with traditional template attacks. Also, they tackle the question of selecting appropriate hyperparameters for convolutional neural networks, specifically focusing on a challenging implementation of the AES algorithm with masking. Intriguingly, findings in this paper indicate that the methodology used to design the VGG-16 algorithm for image recognition also proves effective in devising an architecture for side-channel analysis

### *E. RFTC*

This section introduces Random Frequency Countermeasure (RFTC) to defend against power analysis attacks. Unlike previous methods that used limited clock frequencies or delays for randomization, RFTC leverages the dynamic reconfiguration ability of clock managers in Field-Programmable Gate Arrays (FPGAs) like Xilinx Mixed-Mode Clock Manager (MMCM). By changing the operating frequency at runtime, RFTC executes the Advanced Encryption Standard (AES) block cipher algorithm using randomly selected clock frequencies from a large set, thus mitigating power analysis vulnerabilities.

The effectiveness this clock randomization is tested by performing Correlation Power Analysis (CPA) attacks on collected power traces. Various preprocessing techniques such as Dynamic Time Warping (DTW), Principal Component Analysis (PCA), and Fast Fourier Transform (FFT) are applied to the power traces to assess the removal of random execution. In comparison to existing methods with only 83 distinct finishing times for each encryption, the RFTC approach achieves over 60,000 distinct finishing times, rendering it highly resistant to power analysis attacks. The method has been validated and demonstrated to be secure against up to four million traces.

## REFERENCES


[1] Bhasin, S., Chattopadhyay, A., Heuser, A., Jap, D., Picek, S., Shrivastwa, R.R.: Mind the portability: A warriors guide through realistic profiled side-channel analy- sis. In: 27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23-26, 2020. The Internet Society (2020), https://www.ndss-symposium.org/ndss2020/

[2] Choudary, O., Kuhn, M.G.: Efficient template attacks. In: Francillon, A., Rohatgi, P. (eds.) Smart Card Research and Advanced Applications. pp. 253–270. Springer International Publishing, Cham (2014) .

[3] Gilmore, R., Hanley, N., O'Neill, M.: Neural network based attack on a masked implementation of AES. In: 2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). pp. 106–111 (May 2015). https://doi.org/10.1109/HST.2015.7140247

[4] Lerman, L., Poussier, R., Bontempi, G., Markowitch, O., Standaert, F.X.: Tem-plate attacks vs. machine learning revisited (and the curse of dimensionality in side-channel analysis). In: International Workshop on Constructive Side-Channel Analysis and Secure Design. pp. 20–33. Springer (2015)

[5] Lerman, L., Medeiros, S.F., Bontempi, G., Markowitch, O.: A Machine Learning Approach Against a Masked AES. In: CARDIS. Lecture Notes in Computer Sci- ence, Springer (November 2013), berlin, Germany

[6] Heuser, A., Picek, S., Guilley, S., Mentens, N.: Side-channel analysis of lightweight ciphers: Does lightweight equal easy? In: Hancke, G.P., Markantonakis, K. (eds.) Radio Frequency Identification and IoT Security - 12th International Workshop, RFIDSec 2016, Hong Kong, China, November 30 - December 2, 2016, Revised Selected Papers. Lecture Notes in Computer Science, vol. 10155, pp. 91–104. Springer (2016). https://doi.org/10.1007/978-3-319-62024-4 7, https://doi.org/10.1007/ 978- 3- 319- 62024- 4_7

[7] Benadjila, R., Prouff, E., Strullu, R., Cagli, E., Dumas, C.: Deep learning for side-channel analysis and introduction to ASCAD database. J. Cryptographic Engineering 10(2), 163–188 (2020). https://doi.org/10.1007/s13389-019-00220-8, https://doi.org/10.1007/s13389-019-00220-8

[8] Hospodar, G., Gierlichs, B., Mulder, E.D., Verbauwhede, I., Vandewalle, J.: Ma- chine learning in side-channel analysis: a first study. J. Cryptogr. Eng. 1(4), 293–302 (2011). https://doi.org/10.1007/s13389-011-0023-x, https://doi.org/ 10.1007/s13389- 011- 0023- x

[9] Hettwer, B., Gehrer, S., G¨uneysu, T.: Profiled power analysis attacks using convolutional neural networks with domain knowledge. In: Cid, C., Jr., M.J.J. (eds.) Selected Areas in Cryptography - SAC 2018 - 25th International Conference, Calgary, AB, Canada, August 15-17, 2018, Revised Selected Papers. Lecture Notes in Computer Science, vol. 11349, pp. 479–498. Springer (2018). https://doi.org/10.1007/978-3-030-10970-7 22, https://doi.org/10.1007/978-3-030-10970-7_22

[10] i, H., Kr˘cek, M., Perin, G.: A comparison of weight initializers in deep learningbased side-channel analysis. In: Zhou, J., Conti, M., Ahmed, C.M., Au, M.H.,Batina, L., Li, Z., Lin, J., Losiouk, E., Luo, B., Majumdar, S., Meng, W., Ochoa,M., Picek, S., Portokalidis, G., Wang, C., Zhang, K. (eds.) Applied Cryptography and Network Security Workshops. pp. 126–143. Springer International Publishing,Cham (2020)

[11] Maghrebi, H., Portigliatti, T., Prouff, E.: Breaking cryptographic implementations using deep learning techniques. In: International Conference on Security, Privacy,and Applied Cryptography Engineering. pp. 3–26. Springer (2016)

[12] Masure, L., Dumas, C., Prouff, E.: Gradient visualization for general characterization in profiling attacks. In: Polian, I., St¨ottinger, M. (eds.) Constructive Side-Channel Analysis and Secure Design - 10th International Workshop, COSADE 2019, Darmstadt, Germany, April 3-5, 2019, Proceedings. Lecture Notes in Computer Science, vol. 11421, pp. 145–167. Springer (2019). https://doi.org/10.1007/978-3-030-16350-1 9, https://doi.org/10.1007/ 978-3-030-16350-1_9

[13] Timon, B.: Non-profiled deep learning-based side-channel attacks with sensitivity analysis. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2019(2), 107– 131 (2019). https://doi.org/10.13154/tches.v2019.i2.107-131, https://doi.org/ 10.13154/tches.v2019.i2.107-131

[14] Darshana Jayasinghe, Aleksandar Ignjatovic, and Sri Parameswaran. RFTC: Run?time Frequency Tuning Countermeasure Using FPGA Dynamic Reconfiguration to Mitigate Power Analysis Attacks. In Proceedings of the 56th Annual Design Automation Conference 2019, DAC '19, New York, NY, USA, 2019. Association for Computing Machinery.