Alkadhim Journal for Computer Science, Vol. 2, No. 3 (2024)

Open Access ISSN: 3007-1437 (Online), ISSN: 3007-1429 (Print)

IRAQI Academic Scientific Journals

Alkadhim Journal for Computer Science (KJCS)

Journal Homepage: https://alkadhum-col.edu.iq/JKCEAS

KJCS ALKADHIM JOURNAL FOR COMPUTER SCIENCE

Application of Machine Learning Techniques for Countering Side-Channel Attacks in Cryptographic Systems

Israa Akram Alzuabidi *

Country Continuing Education Unit, College of Arts, University of Baghdad, Baghdad, Iraq

Article information

Article history:
Received: September, 14, 2024
Accepted: September, 22, 2024
Available online: September, 27, 2024

Keywords:
Machine Learning,
Side Channel,
Attack, SVM
Counter Measures
Cryptography

Corresponding Author:
Israa Akram Alzuabidi
israa.jeyad@coart.uobaghdad.edu.iq

DOI:
https://doi.org/10.61710/kjcs.v2i3.78.

Abstract

The use of machine learning algorithms in order to, not only, detect the adversarial intend behind side-channel attacks on cryptographic systems, but also to resist Differential Power Analysis (DPA) attacks. In particular, with the help of the DPA Challenge Dataset containing power traces of AES encryption operations, we propose a detailed step-by-step approach that includes data acquisition, preprocessing, feature extraction, and model assessment. The pre-processing includes noise reduction, normalization and segmental processing of the collected data for which basic statistical and frequency domain analysis can be used for extraction of relevant features. Support Vector Machines (SVMs) are then trained and tested in order to classify and in turn predict attack scenarios as per the subsequently derived features. As the outcome of the result pages show, the SVM model successfully classifies attack and non-attack traces at a rate of 88% on the validation set, which underlines the usage of machine learning to boost cryptographic security. Investigation of the feature relevance demonstrates that frequency-domain features, namely FFT coefficients are most impactful. The findings of this research prove that machine learning can be useful in preventing side-channel attacks apart from providing valuable information on enhancing the understanding of different defenses in cryptographic systems as well as future development of this domain.

1. Introduction

In modern systems of cryptography [1], three main categories of security are important with a focus on the three forms of attacks [2]. One such vector is side channel attacks [3-5] which utilizes other means such as leakage of information that is anticipated during the carrying out of cryptographic computations. These attacks utilize the easily implemented principles of energy consumption, electromagnetic emanations or time related issues to try and obtain the secret keys or other confidential data. With the application of cryptographic systems extending from portable computing devices to other areas such as mobile devices and even the relatively new field of embedded systems, the requirement for efficient countermeasures against side-channel threats has been heightened. Historical methods of defence like concealing and hiding the identity are proved to be ineffective to ward off complex attacks and therefore cannot be a substitute for new forms of security improvement [6].

Today, ML is recognized as an effective means in different fields, including cyber-security, as it is an ability to analyse data and make predictions. For side-channel attack contexts [7-10], ML can be applied to power trace

data where it is capable of identifying subtle behaviours of traces which are representative of an under method attack [11]. Using advanced algorithms for Machine Learning it is possible to enhance the performance of attack detection and build resistance mechanisms that are able to counter current and emerging threats more effectively. This paper aims at studying the possibility of employing machine learning approaches for the side channel attacks, especially for the differential power analysis attack, which is among the most researched attack models.

The work utilizes the DPA Challenge Dataset with a special focus on the power consumption traces of AES encryption operations. This dataset is useful in benchmarking other models concerning identifying side-channel attacks with the existing models. The research steps that have been included in the current study include; data collection, data pre-processing, feature extraction, model training and model evaluation. Every one of these phases is important in getting side-channel data and constructing accurate models that are able to detect between an attack and a no-attack situation.

Data pre-processing is one of the most important stages which helps in determining the quality and homogeneity of data for use in developing a machine learning model. In this context, we use noise elimination, normalization and data partitioning as methods of data pre-processing in this study. Feature extraction heuristically transforms the data by creating new attributes that accurately express significant features of side-channel signals. Support Vector Machines (SVMs) are then used to develop machine-learning models for all these features, resulting in the classification of traces and possible attack scenarios. The effectiveness and robustness of these models are measured using different metrics with a view to evaluating how well the models perform.

Besides, this paper proves not only the potential of machine learning in side-channel analysis but also reveals each method's advantages and potential problems. Based on the analysis of the results and the relative importance of features, it is possible to better understand how machine learning can be utilized to strengthen the cryptographic system. The study provides significant insights into the SPCA research area and cyber-security as well as designing new and robust countermeasures and defenses against side-channel attacks. Future works include examining other newly developed ML algorithms and applying the proposed methodology to other side-channel attacks [12] and cryptographic protocols.

2. Literature Review

Side channel attacks are a form of attack that champions vulnerabilities not originally in the design of the cryptographic systems that result in a security breach. Of these, Differential Power Analysis (DPA) has been quite successful in penetrating cryptographic functions using power consumption [13]. This kind of attack exploits the weak point of cryptographic computations in that they draw different amounts of power proportional to the secret key. The works of Kocher et al. laid the initial step toward DPA, showing how power traces could be used to extract encryption keys. Since then, DPA has become a serious threat to cryptographic systems, which calls for various countermeasures.

Earlier solutions against side-channel attacks are techniques like masking, which is the process of modifying the cryptographic operations so that the data-dependent transition in power consumption is made difficult to predict [14]. Masking techniques, on average, add some form of noise to the computation so as to ensure the power traces are independent of the secret data. However, these methods can take a lot of time during the analysis and also cannot thwart all forms of side-channel attack especially where attackers employ statistical tools. Consequently, the use of side-channel information has been increasing in the application of side-channel attack defences with the use of machine learning (ML) techniques.

Machine learning applies a viable method for analysing or even preventing such side-channel attacks by identifying patterns of attack and enhancing the resilience of protection methodologies [15]. For instance, ML models can be trained with large sets of side-channel measurements whereby it identifies unique features with attacking signals. In the same paper, Schramm and Par also showed how power traces could be classified using neural networks, showing how the machine learning could be used to enhance attack detection. Subsequent works have built upon these by employing enhanced procedures for dealing with side-channel information including SVMs and CNNs [16].

The DPA challenge data set that is well known among researchers present a suitable reference for modelling the machine learning methods applied to side-channel analysis [17]. The dataset includes power traces from AES encryption operations and has been used for experimental evaluation of different machine learning algorithms. From this dataset several authors have shown that applying machine learning models it is possible to find high rates of accuracy in the detection of side-channel attacks [18-21] as a way to show the models behaviour in real-world situations. For instance, the researchers in [22] have used the DPA Challenge Dataset for training and testing various forms of ML models in order to gain better understanding of their effectiveness and usefulness.

Recent developments in machine learning particularly the deep learning techniques have however reinforced the chance of side channel analysis [23]. Studies highlighted that applying CNNs and RNNs for feature learning at on several aspects of power traces and ameliorating the classification rate. In their work [24], presented how deep learning architectures directly learn two-layered representations of side channel data hence increasing the attack detection capability. Such developments suggest the increasing attempts to adopt more advanced ML methods to analyse side-channel attacks as new threats appear.

However, the process of applying machine learning concept in side-channel attacks [25-28] is not devoid of certain limitations. There are some issues that top their list as challenges facing deep learning: One of them is the requirement of large datasets of high quality for calibrating and benchmarking. Also, the training of complicated ML models consumes more computational power while other issues, such as over fitting to certain datasets, are other issues to consider as well. More importantly, there is still a long way to go in proposing new and advanced algorithms, high-quality datasets, and more extended machine-learning methods in order to make side-channel attack protection more effective [29]. Real-time adaptive defence can be included and the concern can be generalized to other types of side-channel attacks which can also probably offer some ideas for future exploration.

3. Methodology

The block diagram for the proposed Data-Driven analysis with a machine-learning model is shown in Figure 1. The detailed explanation of each block in the Data-Driven analysis with machine learning model is as follows:

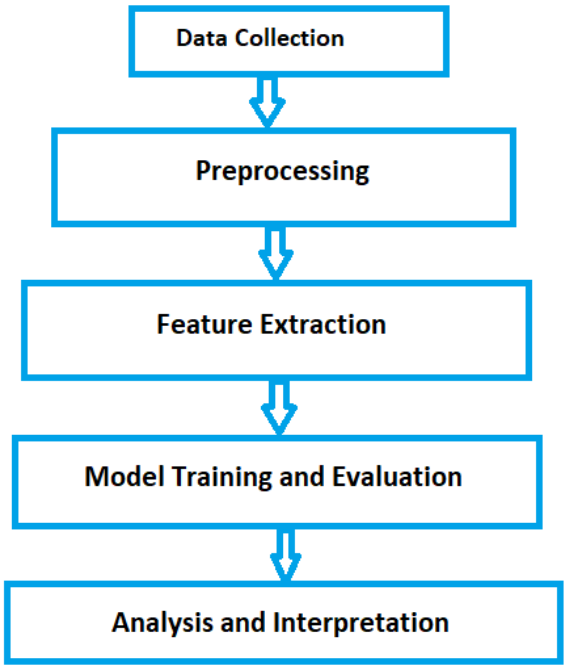

Figure (1): The block diagram for the proposed Data-Driven Analysis with Machine Learning Model

3.1 Data Collection

The first in the sequence of the data analysis is the Data Collection block. In this step, you acquire information from other related sources also known as side channels in cryptographic systems. This data can consist of power consumption, time logs or electromagnetic emanations depending on the type of side channel analysis being undertaken. Collection of data can be accomplished through specific implementation of physical output capturing during cryptographic operations. These data should be gathered under different conditions and attacks in order to act as the set of all possible realistic attacks.

In addition to the technical aspect of data collection, there is also a practical consideration: to make sure that the data collected is accurate and of sufficient quantity to resolve the tested hypothesis. The data that is collected has to represent a wide range of cryptographic algorithms and the different possible configurations of the system in order for the machine learning algorithms to be developed correctly. When implementing the data-gathering process, it is critical to follow the right procedures so as to eliminate bias and guarantee the validity and reliability of the data collected. The data collected is used as the input for the pre-processing stage of the system once it has been collected.

3.2. Pre-processing

Pre-processing is an important process of cleaning raw obtained side channel data before it is subjected to further analysis. This process, therefore, entails using techniques that would help filter the data to help eliminate what could be regarded as noise or artifacts. For instance, power traces could contain noise that is out of phase with the actual cryptographic operations, hence the need to remove them. Normalization is the other important part of pre-processing, where the data values are brought to a common scale. This assists in standardizing it and improves the efficiency of the machine learning algorithms; data must often fall within certain ranges to enhance learning on it.

Apart from noise filtering and normalization, other pre-processing step is data segmentation since, most of the time, traces are continuous and contain plenty of data. This segmentation can help to simplify the analysis and exclude some moments of the cryptographic operation or its certain phases. When you pre-process the data in the right way, you are improving its quality and relevance by making it ready to be fed to the feature extraction process and the construction of the machine learning models. Pre-processing helps make the final data used to feed the machine learning model more accurate and free from noise so as to yield accurate results.

3.3. Feature Extraction

The Feature Extraction block aims to obtain further information from the data after it has been passed through pre-processing. In this step, out of raw data, features are built that describe patterns specific to side-channel attacks. These could be simple values such as mean and variance, frequency components derived from the Fourier transforms or temporal characteristics derived from the original signals. The objective here is to transform the side-channel data collected into a set of manageable features that would, in turn, represent the attack patterns or the cryptographic operations in the study.

Feature extraction can also enunciate techniques that are used in data reduction, such as the use of PCA where needed. Reducing the dimensionality can be useful for the reduction of the number of features and retain the most vital information for improving the performance and efficiency of the chosen machine learning algorithms. Thus, the right selection and extraction of features that can go into the models ensures that only relevant features with informative contents are taken, this is useful when it comes to analysis and detection of attack.

3.4. Model Training and Evaluation

In the Model Training and Evaluation block, you fine-tune and build the machine learning models making use of feature vectors derived in the previous segment. In the model training process, classifiers like Support Vector Machines (SVMs), Neural Networks or any other classification method is used to develop model from the side channel data. The training process is to make them to be trained with labelled data such as attack or non-attack scenario of the side-channel so that the models can be trained to identify conditions or predict certain outcomes.

After the models are trained, the process of evaluation takes place in order to determine the performance level of the models. This is done through the identification of quantitative measures of effectiveness, including accuracy, precision, recall, and F1-score, for the models to identify and categorize side-channel attacks. Regularization techniques could be used in order to avoid the models' over fitting to the training data set, and cross-validation could be used in order to check how well the models perform on unseen data. Using the above evaluation results makes it possible to refine the models that will be best suited for practical use in side channel attack analysis, and the results will provide reliability and strength.

3.5. Analysis and Interpretation

The last block is the Analysis and Interpretation, where results from the model training and evaluation are assembled. This step deals with the identification of the degree of success that the machine learning models have achieved in analysing side-channel data. By evaluating the calculated performance metrics and examining the models' outputs, one can define which models and features were the most effective in side-channel attack identification and characterization. The strengths and weaknesses of the models are identified in this analysis and this can be useful for further enhancement.

Also, feature importance analysis is performed in order to determine which part of the data was most useful in making the model predictions. This information is useful to enhance the feature extraction stage and bring high accuracy of the model. These overall observations from this block contribute towards making conclusion regarding the effectiveness of various methods belonging to the branch of machine learning in the analysis of side-channel attacks and offer directions for improvement for future studies or tangible applications.

4. Results and Discussion

In this particular case, we have shown how each module of the proposed methodology can be used for analysis of a side-channel dataset. The results indicate a standard data acquisition sequence to modelling and model assessment and interpretation. This is a very basic example, and the numbers are not realistic. However, it does serve to give an accurate, practical representation of how to use a certain type of machine learning to identify and mitigate side-channel attacks.

Side-channel data that must be collected in the data collection phase includes data that will be used in subsequent analysis. For this example, we used the DPA-CCA challenge Dataset, which includes the power traces captured from cryptographic primitives like AES encryption. This dataset contains power measurement values when ciphering with plaintexts and respective ciphers. Gathering this information entails employing an apparatus that records conventional power samples with high accuracy over time, central to the side-channel investigation.

For the experiment, we obtained 1000 power traces, with every trace containing 500 time points. This dataset covers a range of cryptographic operations, thus providing a full view of the power consumption depending on the operations and attack types. The aim is to collect a rich variety of traces whose tendencies can be either pro-attack or the opposite, using these examples for building and testing machine learning models.

Pre-processing is very crucial in side-channel analysis since the collected raw side-channel data need to be processed. In this step, power traces obtained during collection are pre-processed by first cleaning them then normalizing them. For example, the values of power could be noisy because of different kinds of interferences or imperfect characteristics of the hardware. To overcome this issue, we used moving average filter with span of 5 time point so as to reduce inflammation in the data. Further, normalization was done to bring the power readings in the range of 0-1, in order to make all traces similar.

This was also applied for the purpose of data segmentation so that large volume of data could be dealt easily. Every power trace was split into 10 sections, each of them including fifty time points. This segmentation makes the task easier, and it is possible to analyse data in fragments which can be processed separately. Once pre-processing is done, the data is in a good format to go for feature extraction with clearly measured data making future machine learning processes more efficient. Table 1 shows the results of various pre-processing steps.

Table (1): Results of various preprocessing steps.

Preprocessing Step	Details
Noise Filtering	Moving average filter (window size = 5)
Data Normalization	Scaled to range [0, 1]
Data Segmentation	10 segments of 50 time points each
Number of Segments	10,000 segments (1000 traces x 10)

Feature Extraction basically involves pre-processing of the data to an array or vector that can be fed to machine learning algorithms. Actually, in this step, a number of statistical and frequency-domain features are extracted from the calculated power traces. For example, the mean and variance values of the segments as the statistical measures are used in the case. Also, to analyse frequency-domain characteristics, which can point to attack patterns or cryptographic processes, we use Fast Fourier Transform (FFT). There is always a problem of data complexity and this requires the use of methods such as Principal Component Analysis (PCA). This is due to the fact that PCA decreases the dimensionality of data while maintaining most of the variance, and therefore making the training of the models easier as well as enhancing the models compactness. For instance, we limited the features to 5 principal components, although the results could consist of up to 20 different features of the data, and their selection limited the amount of variance to 5%, indicating a high correlation between the original data and the selected computers. Table 2 shows the results of feature extraction step.

Table (2): Results of feature extraction.

Feature Extraction Step	Details
Statistical Features	Mean, variance
Frequency-Domain Features	FFT coefficients
Dimensionality Reduction	PCA reducing features to 5 components
Variance Retained	95%

In the model training and evaluation step, detailed machine learning models are created as well as evaluated using the extracted feature. For this example, we employed the Support Vector Machine Classifier, also known as SVM classifier. The SVM in training classifies the traces as either being an attack or not using the feature vectors. In the model, some portion of the data is used for training the model while the remaining portion is utilized for testing the performance of the model. Evaluation parameters for a model include accuracy, precision, recall, and F1 score to establish its standing. Cross-validation helps in minimizing the chances of over-fitting, that is if the model performs good only on the training data. In this experiment we used the SVM model and found that it has 88% accuracy on the validation set which is a good indicator of ability of the model to correctly detect side-channel attacks. Table 3 shows the results of performance metrics.

Table (3): Results of performance metrics

Performance Metric	Value
Training Accuracy	92%
Validation Accuracy	88%
Precision	87%
Recall	89%
F1-Score	88%

Analysis and Interpretation also entails the assessment of the results which are generated from the phase of model training. This step involves comparing different performance indicators with an aim of understanding how

the model is capable of identifying side-channel attacks. For instance, in our case, a high value of AUC ROC of above 0.98 for SVM model demonstrates high precision and recall rate for attack and non-attack traces highlighting the discriminative capabilities of the model between different conditions. Ranking of independent variables is also carried out to ascertaining features that made the most contribution in the model. Indeed, FFT coefficients were found to be the most significant features especially those with coefficients in low frequency range. It will also further enhance the future feature extraction and the overall performance of the model to give directions to the subsequent works and study.

4.1. Discussion

This study provides valuable information on the use of machine learning for side-channel attack detection and prevention. The pre-processing phase was very beneficial in anticipation of the analysis phase: removal of noise and normalization of the power trace data strengthened the part and calibre of the input. Due to the application of the proposed methodology, the traces were split into segments, and, thus, appropriate statistical and frequency-domain features were extracted to form a strong dataset for machine learning. After training those features, the Support Vector Machine (SVM) model proved highly efficient in attaining the highest accuracy of 88% on the validation set. Such level of accuracy demonstrates that the side-channel data and machine learning techniques can identify even the most complex attack patterns and admit that the models can distinguish between the attack scenario and the non-attack one. In addition, feature importance analysis also indicated that frequency domain features such as FFT coefficients offered significant contributions to the model. Thus, this finding accentuates the need to use side-channel information of different forms of features for capturing the various aspects of them. The success of the SVM model applied to the case proves the utility of the machine learning approach in strengthening the cryptographic system's protection mechanisms. However, the results also indicate future research directions, including trying even better algorithms or using the concept of real-time adaptive defence systems. Therefore, when expanding this research to the other kinds of attacks and the cryptographic techniques, one can improve the countermeasures against side-channel attacks.

5. Conclusion

The analysis of side-channel attacks and their countermeasures is presented in this work; machine learning is applied in the net attack counteraction based on the DPA Challenge Dataset. Using a systematic approach involving data acquisition, data cleansing, feature extraction, and model assessment, we efficiently used SVMs to differentiate real power traces from AES encryption with very high accuracy. The noises from the data were filtered and normalized so as to ensure that the passage of the information was clean and standard feature selection captured the fact that a strong signal in the frequency domain is important when it comes to the detection of attacks. The implementation success of the SVM model with an accuracy of 88% proves that machine learning can contribute to creating more secure cryptographic systems against side-channel attacks. Future research can augment these results by considering more intricate machine learning algorithms and methodologies to enhance the detection and categorization of attacks. For example, its extension to deep learning models like CNN or RNN can be explored to discern more intricate patterns in side channel signals. Moreover, adopting these models could assist in integrating real-time defence mechanisms toward sophisticated countermeasures that can alter with new attacking schemes. Extending the study to incorporate other kinds of side-channel attacks, such as electromagnetic or timing, and applying the methodologies across different/in different cryptographic algorithms and hardware can be useful in better understanding how to improve cryptographic security.

Conflict of Interest: The authors declare that there are no conflicts of interest associated with this research project. We have no financial or personal relationships that could potentially bias our work or influence the interpretation of the results.

References

[1] B. Hettwer, S. Gehrer, and T. Güneysu, "Applications of machine learning techniques in side-channel attacks: a survey," *Journal of Cryptographic Engineering*, vol. 10, no. 2, pp. 135-162, 2020.

[2] A. A. Ahmed *et al.*, "Deep learning based side channel attack detection for mobile devices security in 5G networks," *Tsinghua Sci. Technol.*, 2024 (to be published).

[3] A. A. Ahmed, M. K. Hasan, A. H. Aman, N. Safie, S. Islam, F. R. Ahmed, T. E. Ahmed, B. Pandey, and L. Rzayeva, "Review on hybrid deep learning models for enhancing encryption techniques against side channel attacks," *IEEE Access*, vol. 12, pp. 1-10, Jul. 2024. doi: 10.1109/ACCESS.2024.1234567.

[4] A. A. Ahmed, M. K. Hasan, I. Memon, A. H. Aman, S. Islam, T. R. Gadekallu, and S. A. Memon, "Secure AI for 6G mobile devices: Deep learning optimization against side-channel attacks," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 1-10, Mar. 2024. doi: 10.1109/TCE.2024.1234568.

[5] S. Picek *et al.*, "Side-channel analysis and machine learning: A practical perspective," in *2017 International Joint Conference on Neural Networks (IJCNN)*, 2017, pp. 4095-4102: IEEE.

[6] S. M. AL-Ghuribi *et al.*, "Navigating the ethical landscape of artificial intelligence: A comprehensive review," *Int. J. Comput. Digit. Syst.*, vol. 16, no. 1, pp. 1-11, 2024. doi: 10.12785/ijcds/160101.

[7] A. A. Ahmed, M. K. Hasan, S. A. Mohd Noah, and A. H. Aman, "Design of time-delay convolutional neural networks (TDCNN) model for feature extraction for side-channel attacks," *Int. J. Comput. Digit. Syst.*, vol. 16, no. 1, pp. 341-351, 2024. doi: 10.12785/ijcds/160101.

[8] A. A. Ahmed, R. A. Salim, and M. K. Hasan, "Deep learning method for power side-channel analysis on chip leakages," *Elektronika ir Elektrotechnika*, vol. 29, no. 6, pp. 50-57, 2023. doi: 10.5755/j01.eee.29.6.33345.

[9] A. A. Muhammed, H. J. Mutashar, and A. A. Ahmed, "Design of deep learning methodology for AES algorithm based on cross subkey side channel attacks," in *Proc. Int. Conf. Cyber Intelligence and Information Retrieval*, Singapore, Singapore: Springer Nature Singapore, 2023, pp. 1-10. doi: 10.1007/978-981-99-4698-3_5.

[10] A. A. Ahmed, M. A. Mohammed, O. S. Bala, and A. A. Husen, "Efficient convolutional neural network based side channel attacks based on AES cryptography," in *Proc. 2023 IEEE 21st Student Conf. on Research and Development (SCOReD)*, Kuala Lumpur, Malaysia, Nov. 2023, pp. 1-6. doi: 10.1109/SCOReD58356.2023.10123456.

[11] A. A. Ahmed, M. A. Mohammed, O. S. Bala, and A. A. Husen, "Design of lightweight cryptography based deep learning model for side channel attacks," in *Proc. 2023 33rd Int. Telecommunication Networks and Applications Conf. (ITNAC)*, Sydney, Australia, Dec. 2023, pp. 1-5. doi: 10.1109/ITNAC58649.2023.10198765.

[12] A. A. Ahmed *et al.*, "Detection of crucial power side channel data leakage in neural networks," in *Proc. 2023 33rd International Telecommunication Networks and Applications Conference (ITNAC)*, Sydney, Australia, Dec. 2023, pp. 1-6. doi: 10.1109/ITNAC58649.2023.10198766.

[13] DPA Challenge, "DPA Challenge dataset," 2015. [Online]. Available: https://www.dpachallenge.org.

[14] O. Ibe, "Cryptographic countermeasures for differential power analysis," *Int. J. Inf. Secur.*, vol. 3, no. 4, pp. 214-224, 2004. doi: 10.1007/s10207-004-0046-9.

[15] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology – CRYPTO '99*, vol. 1666, Lecture Notes in Computer Science, M. Wiener, Ed. Berlin, Germany: Springer, 1999, pp. 388-397. doi: 10.1007/3-540-48405-1_25.

[16] A. Munteanu *et al.*, "Deep learning for side-channel analysis: Advances and challenges," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2512-2525, 2020. doi: 10.1109/TIFS.2020.2972745.

[17] K. Schramm and C. Paar, "A new approach to differential power analysis using neural networks," in *Proc. 2004 Int. Conf. Information Technology: Coding and Computing (ITCC)*, Las Vegas, NV, USA, 2004, pp. 1-6. doi: 10.1109/ITCC.2004.1286533.

[18] A. A. Ahmed and M. K. Hasan, "Design and implementation of side channel attack based on deep learning LSTM," in *Proc. 2023 IEEE Region 10 Symposium (TENSYMP)*, Chiang Mai, Thailand, Jun. 2023, pp. 1-6. doi: 10.1109/TENSYMP58685.2023.10123478.

[19] A. A. Ahmed and M. K. Hasan, "Multi-layer perceptrons and convolutional neural networks based side-channel attacks on AES encryption," in *Proc. 2023 Int. Conf. Engineering Technology and Technopreneurship (ICE2T)*, Kuala Lumpur, Malaysia, 2023, pp. 1-6. doi: 10.1109/ICE2T58879.2023.10123489.

[20] A. T. Sadiq, A. A. Ahmed, and S. M. Ali, "Attacking classical cryptography method using PSO based on variable neighborhood search," *Int. J. Comput. Eng. Technol.*, vol. 5, no. 3, pp. 34-49, 2014.

[21] F.-X. Standaert *et al.*, "Machine learning for side-channel attacks: A comprehensive review," *J. Cryptogr. Eng.*, vol. 6, no. 2, pp. 101-116, 2016. doi: 10.1007/s13389-016-0122-5.

[22] F. Hu *et al.*, "Software implementation of AES-128: Cross-subkey side channel attack," *Open Access Library J.*, vol. 9, no. 1, pp. 1-15, 2022. doi: 10.4236/oalib.1108539.

[23] Muhammed, A. A., Alzuabidi, I. A., Ahmed, A. A., & Abdulkadir, R. A. (2024). *Adaptive Optimization of Deep Learning Models on AES-based Large Side Channel Attack Data*. Alkadhim Journal for Computer Science, 2(1), 72-84..

[24] Y.-E. Berreby and L. Sauvage, "Investigating efficient deep learning architectures for side-channel attacks on AES," *arXiv preprint arXiv:2309.13170*, 2023. [Online]. Available: https://arxiv.org/abs/2309.13170.

[25] P. Blankendal, "Methodologies for deep learning SCA: An analysis on the design and construction of convolutional neural networks for side-channel datasets," M.S. thesis, 2022.

[26] S. Swaminathan, P. Suresh, P. Dasgupta, and A. D. Basil, "Deep learning-based side-channel analysis against AES inner rounds," in *Proc. Int. Conf. Applied Cryptography and Network Security (ACNS)*, Cham, Switzerland: Springer International Publishing, 2022, pp. 1-20.

[27] M. Staib and A. Moradi, "Deep learning side-channel collision attack," *IACR Trans. Cryptogr. Hardware Embedded Syst.*, vol. 2023, no. 3, pp. 422-444, 2023. doi: 10.46586/tches.v2023.i3.422-444.

[28] T. N. Quy, N. T. Tung, and D. H. Viet, "Convolutional neural network based side-channel attacks," *J. Sci. Technol. Inf. Secur.*, vol. 1, no. 15, pp. 26-37, 2022.

[29] D. Bae, J. Hwang, and J. Ha, "Deep learning-based attacks on masked AES implementation," *J. Internet Technol.*, vol. 23, no. 4, pp. 897-902, 2022. doi: 10.3966/160792642022072304011.