Dr. B. C. Roy Polytechnic

BCRP Journal of Innovative Research in Science and Technology (BJIRST)

A peer-reviewed open-access journal
ISSN: 2583-4290
Journal homepage: https://bcrpjournal.org/

BJIRST

Review on Performance Analysis of Deep Learning-Based Approaches in Elliptic Curve Cryptography (ECC)

Subhadeep Mondal
Dept. of Computer Science and Technology
Dr. B.C.Roy Polytechnic
Durgapur, India
subhadeep.mondal@bcrec.ac.in

ABSTRACT

Elliptic Curve Cryptography (ECC) has emerged as a fundamental element of contemporary digital security, providing strong protection with shorter key sizes and reduced computational requirements compared to traditional public-key systems like Rivest-Shamir-Adleman algorithm (RSA). Nevertheless, recent progress in machine learning, especially deep learning (DL), has presented new possibilities and challenges for ECC. Deep learning can be utilized both to enhance cryptographic calculations and to simulate potential attacks, including side-channel and fault-based vulnerabilities. This paper offers an in-depth performance evaluation of deep learning-based methods applied to ECC, concentrating on their efficacy, computational efficiency, and effects on cryptographic robustness. By examining recent research and experimental results, author assess various DL frameworks, such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and autoencoders, in the context of ECC-related tasks.

Keywords— Elliptic Curve Cryptography, Deep Learning, Side Channel Analysis, Cryptanalysis, Neural Networks, Performance Optimization.

1. INTRODUCTION

In today's era of ubiquitous computing, robust and efficient cryptographic techniques are crucial. Elliptic Curve Cryptography (ECC) has emerged as a key tool in numerous applications because it provides security comparable to traditional public key algorithms, such as RSA, while using shorter keys and requiring less computational effort [1]. ECC is widely utilized in mobile devices, Internet of Things (IoT) systems, secure communications, and blockchain technologies. However, a cryptographic algorithm's theoretical strength does not automatically translate to practical security. Implementation weaknesses—such as timing attacks, power consumption analysis, and electromagnetic leaks—can expose private keys [2].

Meanwhile, developments in machine learning, especially deep learning (DL), have revolutionized pattern recognition. Models like convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory (LSTM) networks excel at automatic feature extraction and classification. In cryptography, these methods have been employed both to carry out attacks, such as side-channel analysis, and to improve algorithm performance, for instance by accelerating ECC scalar multiplication. In light of these developments, a comprehensive evaluation of deep learning (DL) methods within the ECC domain is timely.

The author addresses reviewing recent literature, comparing DL architectures for ECC-related tasks, assessing performance in terms of accuracy, latency, resource utilization, and robustness, and highlighting open challenges and providing directions for future research.

2. LITERATURE REVIEW

Deep learning (DL) has seen extensive application in side-channel analysis (SCA) and cryptanalysis. For example, [3] examined evaluation metrics for DL-based side-channel attacks, noting that measures like guessing entropy may require adjustment when applied to DL systems. Similarly, [4] provided a comprehensive survey of DL in SCA, discussing challenges such as dataset size, countermeasures, and the relationship between model accuracy and cryptographic success rates. [5] investigated power side-channel attacks on RNS/GLV ECC cores using ML and DL models and proposed corresponding countermeasures. More recently, [2] highlighted the growing maturity of DL-based SCA frameworks. On the defensive and optimization side, fewer studies explore DL for enhancing ECC operations. For instance, [3] applied neural networks to optimize ECC scalar multiplication, achieving reduced computation times.

The evaluation of DL models in cryptographic settings has also attracted attention. [3] argued that conventional ML/DL metrics, such as accuracy, may not adequately capture cryptographic effectiveness and recommended refined metrics. [7,8] introduced AISY, a DL-based SCA framework emphasizing reproducibility.

Despite these advances, several gaps remain. Most research targets symmetric key cryptosystems like AES, with

comparatively fewer studies on asymmetric ECC implementations. Work on using DL to improve ECC performance, rather than attack it, is limited. Comparative benchmarking of DL architectures—CNNs, LSTMs, and transformers—within ECC is scarce, and evaluation metrics that jointly consider speed, resource usage, accuracy, and security robustness remain underdeveloped.

3. DISCUSSIONS

CNNs have emerged as the most effective architecture for side channel attacks on ECC. CNNs broke the target implementation with only a single measurement in some cases [9,10]. Misalignment and countermeasures still degrade performance for non-CNN models, whereas CNNs, combined with data augmentation (e.g., shifted traces), showed resilience [4]. The training and inference cost for DL models, however, poses a barrier for deployment in constrained devices (IoT). For example, feature engineering combined with ML (rather than heavy DL) sometimes performs comparably when dataset size is limited [5-7]. On the optimization side, fewer quantitative studies exist. The potential for DL to optimize ECC [11] operations remains under explored and lacks rigorous benchmarking. High accuracy in attack scenarios often correlates with deep, complex models and large datasets. But these impose higher computational cost, memory and energy usage—limiting applicability in real world embedded cryptographic modules. Furthermore, deploying DL [12] for optimization may introduce new risks: e.g., model leakage, adversarial DL attacks, and unforeseen side effects in algorithmic security. Benchmark dataset and implementation (e.g., a standardized ECC implementation with and without countermeasures), Architecture comparison (CNN vs. LSTM [12-14] vs. hybrid vs. transformer), Metrics: attack success / optimization gain + latency + resource usage + robustness, Deployment scenario evaluation: lab vs. embedded/IoT environment, Security risk assessment: adversarial model, model leakage, side effects. This framework allows for direct comparison of studies and helps highlight practical trade-offs.

TABLE 1 THE ESSENTIAL PARAMETERS FOR PERFORMANCE EVALUATION

Sl No.	Parameter	Role in performance evaluation
1	Attack Accuracy	Success rate of key recovery, guessing entropy, number of traces needed
2	Computation Time / Latency	Training time, inference time, number of traces required
3	Resource Usage	Model size, memory footprint, GPU/CPU cycles, suitability for embedded/IoT devices.
4	Robustness	Ability to handle misalignment, noise, countermeasures, variant ECC curves.
5	Optimization Gain	Performance enhancement

4. CONCLUSION

Deep learning–based approaches have considerably impacted the domain of ECC cryptography—both from the attack and optimization perspectives. On the attack side, DL models (especially CNNs) have demonstrated high success rates in side-channel analysis of ECC implementations, even under some counter-measures. On the optimization side, DL holds promise for accelerating ECC operations, though rigorous benchmarks and broad adoption are still lacking. Fig. 1 explains about the ECC with deep learning models. However, the adoption of DL in cryptographic contexts carries trade-offs: computational cost, resource constraints, robustness issues and new vulnerabilities. Future research should address these by developing lightweight models for embedded systems, creating standardized benchmarking datasets for ECC + DL, exploring adversarial-robust DL architectures, and ensuring transparency [13,14] and explainability in DL-based cryptographic modules. By adopting [15-17] the proposed evaluation framework and focusing on real-world deployments and risks, the community [18] can move toward mature, secure, and efficient DL-enhanced ECC systems.

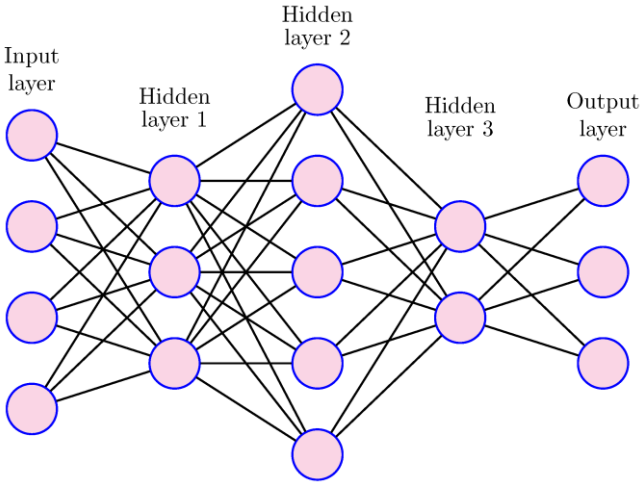

FIG. 1: ECC WITH DEEP LEARNING MODELS [19]

5. FUTURE SCOPES

This review highlights future studies could investigate the application of advanced deep learning models, including transformers and graph neural networks, to improve performance optimization and enhance anomaly detection within ECC systems. The development of real-time, AI-driven monitoring frameworks offers substantial potential for adaptive key management and strengthening overall cryptographic resilience. In addition, exploring hardware-accelerated solutions utilizing GPUs, TPUs, and FPGAs could significantly improve computational efficiency [14], particularly in IoT and edge-computing environments with constrained resources. Further research may focus on designing lightweight and energy-efficient models tailored for low-power cryptographic applications. Extending deep learning-assisted ECC [5] analysis to emerging domains such as blockchain, secure cloud computing, and next-generation communication networks provides additional avenues for innovation. Furthermore, integrating ECC with post-quantum cryptographic techniques may facilitate the creation of hybrid, quantum-resilient security frameworks. Finally, establishing standardized datasets and robust benchmarking

protocols is essential to enable consistent evaluation and comparison of deep learning-based ECC methodologies.

6. ACKNOWLEDGEMENT

The author would like to thank the Department of Computer Science and Technology, Dr. B. C. Roy Polytechnic, Durgapur for extending their support in the successful completion of this manuscript.

REFERENCES

[1] Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *IEEE communications surveys & tutorials*, *25*(1), 319-352.

[2] Vaezi, M., Azari, A., Khosravirad, S. R., Shirvanimoghaddam, M., Azari, M. M., Chasaki, D., & Popovski, P. (2022). Cellular, wide-area, and non-terrestrial IoT: A survey on 5G advances and the road toward 6G. IEEE Communications Surveys & Tutorials, 24(2), 1117-1174.

[3] Wu, L., Perin, G., & Picek, S. (2022, March). On the evaluation of deep learning-based side-channel analysis. In International Workshop on Constructive Side-Channel Analysis and Secure Design (pp. 49-71). Cham: Springer International Publishing.

[4] Baseri, Y., Hafid, A., Shahsavari, Y., Makrakis, D., & Khodaiemehr, H. (2025). Blockchain security risk assessment in quantum era, migration strategies and proactive defense. IEEE Communications Surveys & Tutorials.

[5] Parthasarathy, R., & Saravanan, P. (2025). Side-channel attack resilient implementation of homomorphic encryption using elliptic curve cryptography for secure cloud computing. Integration, 102439.

[6] Alqarni, M., & Azim, A. (2025). SecureLLAMA: Secure FPGAs using LLAMA Large Language Models. IEEE Transactions on Artificial Intelligence.

[7] Picek, S., Perin, G., Mariot, L., Wu, L., & Batina, L. (2023). Sok: Deep learning-based physical side-channel analysis. *ACM Computing Surveys*, *55*(11), 1-35.

[8] Kou, X., Yang, W., Li, L., & Zhang, G. (2025). Multi-Modal Side-Channel Analysis Based on Isometric Compression and Combined Clustering. Symmetry, 17(9), 1483.

[9] Park, C. (2025). *Interpolating Neural Networks for the Next-Generation Predictive Scientific Artificial Intelligence* (Doctoral dissertation, Northwestern University).

[10] Gill, S. S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., & Buyya, R. (2022). Quantum computing: A taxonomy, systematic review and future directions. Software: Practice and Experience, 52(1), 66-114.

[11] Karayalcin, S., Perin, G., & Picek, S. (2023). Resolving the doubts: On the construction and use of resnets for side-channel analysis. Mathematics, 11(15), 3265.

[12] Li, T., Qiao, F., Wang, Y., Lu, K., Lv, Y., & Wang, Y. (2025). TLD-SCA: A Transformer-LSTM Detection Model against Side-Channel Attack in Blockchain Payment Channel. *ACM Transactions on the Web*.

[13] Yuan, Y., Liu, Z., Deng, S., Chen, Y., Wang, S., Zhang, Y., & Su, Z. (2025, May). Ciphersteal: Stealing input data from tee-shielded neural networks with ciphertext side channels. In 2025 IEEE Symposium on Security and Privacy (SP) (pp. 4136-4154). IEEE.

[14] Xu, J., Li, M., Liang, L., Zhang, Y., Xiang, S., & Ma, Z. (2021, October). Profiling attacks against ecc: Side channel analysis based on deep learning for curve-25519. In 2021 IEEE 21st International Conference on Communication Technology (ICCT) (pp. 274-278). IEEE.

[15] Hettwer, B., Horn, T., Gehrer, S., & Güneysu, T. (2020, December). Encoding power traces as images for efficient side-channel analysis. In 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (pp. 46-56). IEEE.

[16] Gammell, J., Raghunathan, A., Hashemi, A., & Roy, K. (2025). Learning to Localize Leakage of Cryptographic Sensitive Variables. arXiv preprint arXiv:2503.07464.

[17] Kumar, M. V., Raju, K. S., Rajakumar, K., & Saravanakumar, S. (2025). A Study on Next-Generation Materials and Devices.

[18] Reddy, C. L., & Malathi, K. (2025). Revolutionary hybrid ensembled deep learning model for accurate and robust side-channel attack detection in cloud computing. *Scientific Reports*, *15*(1), 32949.

[19] Jebrane, J., Chhaybi, A., Lazaar, S., & Nitaj, A. (2025). Elliptic Curve Cryptography with Machine Learning. Cryptography, 9(1), 3.