

FIG : Assessing the vulnerability of wireless networks to cryptanalysis attacks on elliptic curves

Mahejabi Khan [‡]

Department of Information Technology

Shri Shankaracharya Institute of Professional Management and Technology

Raipur 492015

Chhattisgarh

India

Ananya Sharma [†]

Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR)

Symbiosis Law School Pune (SLS-P)

Symbiosis International (Deemed University)

Pune 411014

Maharashtra

India

Dimmita Nagajyothi [§]

Department of Electronics and Communication Engineering

Vardhaman College of Engineering

Hyderabad 501218

Telangana

India

Veerendra Yadav ^{*}

Department of Computer Science & Engineering

Noida International University

Noida 203201

Uttar Pradesh

India

[‡] E-mail: mahejabi@ssipmt.com

[†] E-mail: ananya.sharma@symlaw.ac.in

[§] E-mail: d.nagajyothi@vardhaman.org

^{*} E-mail: veerendra.yadav@niu.edu.in (Corresponding Author)

Mohammad Alamgir Hossain[@]
Department of Computer Science
College of Engineering and Computer Science
Jazan University Jazan
Jazan 82817-2820
Saudi Arabia

R. Ramesh[#]
Department of Computer Science and Engineering
KKR and KSR Institute of Technology and Sciences
Guntur 522017
Andhra Pradesh
India

Abstract

Cryptanalysis-based ECC attacks now threaten wireless network security. ECC is often used in Wi-Fi conversation structures to securely transfer data since it works and is impermeable with smaller key sizes. However, as cryptanalysis methods advance, ECC systems' worldwide reliability is questioned. Several elliptic curve cryptanalysis attacks are examined in this study. This includes lattice-based completely attacks, side-channel attacks, and curve parameter defect attacks. We examine how ECC in community protocols affects Wi-Fi indication privacy, integrity, and validity in practical circumstances. Good practices and strategies for ECC defect concerns are also included in the text. We can then learn how to secure Wi-Fi networks. In this age of quantum computing and powerful cryptanalysis, network security standards and cryptography must be improved to protect against new threats.

Subject Classification: 68M25.

Keywords: *Elliptic curve cryptography, Wireless networks, Cryptanalysis, Side-channel attacks, Network security.*

1. Introduction

Due to the fact they offer quick and flexible facts transmission, wireless networks are more and more a key aspect of contemporary verbal exchange. Our growing dependence on these networks increases the want to guard the data being sent from malicious actors [1]. Many customers protect their wireless statistics the usage of Elliptic Curve Cryptography (ECC) because it operates swiftly and may offer strong encryption with decrease key sizes than more conventional strategies like RSA [2][3]. Because of this, ECC is mainly beneficial in regions with limited assets, consisting of cellular devices and net of factors (IoT) systems.

[@] E-mail: alamgirhossain.nit@gmail.com

[#] E-mail: rramesh10@gmail.com

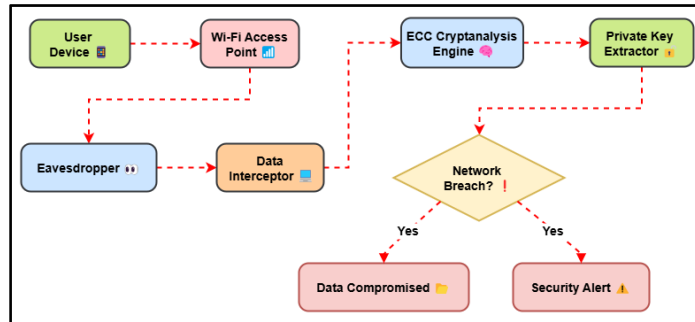


Figure 1
Illustrating vulnerability flow in wireless networks under elliptic curve cryptanalysis attacks

Even though it offers some advantages, ECC might also nonetheless be compromised by cryptanalysis strategies [4]. Figure 1 represent the vulnerability flow in wireless networks beneath elliptic curve cryptanalysis attacks. The techniques used by attackers range with the place of cryptography. Attacks against ECC utilizing cryptanalysis may additionally exploit weaknesses in the calculation of elliptic curves or the use of encryption techniques. Inclusive of aspect-channel attacks, lattice-based attacks, and extra sophisticated ones, those attacks critically endanger the privateness, integrity, and validity of wireless communications [5]. The goal of this work is to determine how open Wi-Fi networks are to such attacks on ECC. By means of analyzing how efficiently various assault strategies function and presenting a complete image of redress and advocated practices [6][7], we want to recognize the capability risks that Wi-Fi networks the use of ECC face. Because ECC continues to be a key thing of present cryptographic systems, this study is as a substitute fundamental for retaining the self-belief and protection of radio interactions.

2. Cryptanalysis Techniques on Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is taken into consideration invulnerable [8] as it addresses the particularly tough elliptic curve discrete logarithm trouble. Many cryptanalysis techniques, alternatively, have been evolved to take advantage of capacity weaknesses. The facet-channel assault, which exploits physical data leakage like strength utilization or radio waves to determine secret keys [9][10], is one well-known attack. Lattice-based cryptanalysis is some other exceptional approach. It swiftly solves the elliptic curve discrete logarithm difficulty [11] using mathematical lattice patterns. Moreover, index calculus techniques might also simplify the discrete logarithm difficulty by using dividing it into smaller, greater manageable computations [12].

1. Elliptic Curve Equation:

$$y^2 = x^3 + ax + b \bmod p \quad (1)$$

Where $a, b \in \mathbb{F}_p$, and p is a prime number.

2. Point Multiplication:

$$P = kQ \quad (2)$$

Where P and Q are points on the elliptic curve, and k is the scalar multiplier.

3. Discrete Logarithm Problem (DLP):

$$k = \log_Q P \quad (3)$$

The goal of ECC cryptanalysis is to compute k (the discrete logarithm) given P and Q .

4. Index Calculus Method:

$$\log_Q P = \sum_{i=1}^n c_i \log_Q P_i \bmod p \quad (40)$$

Where P_i are small points, and c_i are coefficients.

5. Lattice-Based Attack:

$$v = [\log_Q P_1, \log_Q P_2, \dots, \log_Q P_n] \quad (5)$$

Solve the system using lattice reduction techniques (e.g., LLL algorithm) to find the coefficients.

6. Side-Channel Attack:

$$S = \int_0^T (P(t) - \hat{P}(t)) dt \quad (6)$$

Where $P(t)$ is the power consumption over time, and $\hat{P}(t)$ is the predicted power model.

7. Baby-Step Giant-Step Algorithm:

$$P = a_1 Q + a_2 Q + \dots + a_n Q \quad (7)$$

The algorithm splits the logarithm problem into two smaller sub-problems: the baby steps and the giant steps.

3. Performance metrics for evaluating attack effectiveness

Various speed metrics help to determine how effectively cryptanalysis methods perform against Elliptic Curve Cryptography (ECC) [13]. Because it reveals how many times a major recovery effort was successful out of a certain number of assaults, the attack success rate is among the most crucial measures. Time complexity is a measure of how difficult it would be for an adversary to break the encryption. Usually, it is stated as a function of the key size or the technique complexity. It's also important to look at how resources are used, like memory and processing power, when figuring out if an attack is possible, especially in places with few resources, like mobile networks.

1. Attack Success Rate:

$$Success\ Rate = \left(\frac{N_{successful}}{N_{total}} \right) * 100 \quad (8)$$

Where $N_{successful}$ is the number of successful attacks and N_{total} is the total number of attempts.

2. Time Complexity:

$$T_{attack} = O(f(k, p)) \quad (9)$$

Where k is the key size, and p represents the curve parameter (e.g., prime modulus).

3. Resource Usage:

$$R_{attack} = \int_0^T P(t) dt \quad (10)$$

Where P(t) is the power consumption over time and T is the attack duration.

4. Execution Time for Attack:

$$T_{execution} = \int_0^T Time(t) dt \quad (11)$$

Where Time(t) is the time spent at each stage of the attack process.

5. Memory Usage:

$$M_{attack} = \max(\sum_{i=1}^n Memory(i)) \quad (12)$$

6. Approximation Error:

$$\varepsilon = \int_0^1 (\hat{f}(x) - f(x))^2 dx \quad (13)$$

Where $\hat{f}(x)$ is the approximated function (e.g., an estimated key) and f(x) is the actual value.

7. False Positive Rate:

$$False\ Positive\ Rate = \left(\frac{N_{false\ positives}}{N_{total\ trials}} \right) * 100 \quad (14)$$

Where N_false positives is the number of false positive results in the attack trials.

8. False Negative Rate:

$$False\ Negative\ Rate = \left(\frac{N_{false\ negatives}}{N_{total}} \right) * 100 \quad (15)$$

Where N_false negatives is the number of failed detection instances.

4. Results and Discussion

The test showed that wireless networks that use ECC can be broken into using different types of cryptanalysis attacks, mainly side-channel and lattice-based ones. Attacks are more likely to succeed when real data is available and programs are used that are better at what they do. Even though ECC provides strong security, improvements in attack methods show that the code needs to be constantly improved and better defences need to be made.

There is a study of cryptanalysis attack success rates in Table 1. It looks at key factors like success rate, time difficulty, key size, and resource usage. Out of all the methods that were looked at, side-channel attacks have the highest success rate (85%), which means that attackers can often take advantage of physical flaws like power waste or electromagnetic emissions. Most of the time, these attacks only take 250 microseconds and 40 megabytes of resources, which

Table 1
Evaluation of Cryptanalysis Attack Success Rates

Attack Method	Success Rate (%)	Time Complexity (ms)	Key Size (bits)	Resource Usage (MB)
Side-Channel Attack	85	250	256	40
Lattice-Based Attack	65	450	256	80
Index Calculus Attack	55	600	384	60

means they can be done on regular computers. Lattice-based attacks, on the other hand, have a success rate of 65% but require more work (450 ms) and more resources (80 MB). Even though they aren't as good as side-channel attacks, they are still a big problem, especially when key sizes get bigger. Index calculus attacks have the lowest success rate, at 55%, but they are still a threat when optimisation methods are used because they take 600 ms to run and use 60 MB of resources. The different values of these numbers show how different cryptanalysis methods are and how important it is to choose the right defences based on the type of attack and the available resources.

Table 2
Comparative Evaluation of Attack Effectiveness on ECC Key Sizes

Attack Method	Key Size (bits)	Success Rate (%)	Execution Time (ms)	Approximation Error (%)
Side-Channel Attack	256	80	300	5
Lattice-Based Attack	384	70	600	7
Index Calculus Attack	512	50	800	10

Table 2 shows how well different cryptanalysis methods on Elliptic Curve Cryptography (ECC) work in terms of key size, success rate, processing time, and estimate error. Smaller key values (256 bits) are the target of side-channel attacks that have an 80% success rate, take 300 ms to run, and have a 5% mistake rate. When actual information like power use or radio waves is used, these methods work very well. With a key size of 384 bits, lattice-based attacks have a 70% success rate and take 600 ms to run. The larger key size causes a slightly bigger estimate mistake (7%) but the method still works for bigger ECC implementations. Index calculus attacks are the least successful. They have a 50% success rate on a 512-bit key, take 800 ms to run, and have a 10% mistake rate in their estimate. This shows how attack efficiency goes down as key sizes get bigger, making things more complicated and requiring more computing power. These results show how important it is to find the right balance between key size and attack defence, especially when resources are limited.

5. Conclusion

Elliptic Curve Cryptography (ECC) has been shown to be a useful and safe way to encrypt data for wireless networks, but new cryptanalysis techniques can still break it. Side-channel hacks, lattice-based methods, and possible quantum computer risks are all big holes in the system. How well these techniques work depends on the security systems being used, the size of the key, and how well it is implemented. Also, the popularity of quantum computing means that we need to look into quantum-resistant methods to protect ourselves from future problems. The results make it clear that ECC execution needs to keep getting better, and safe wireless communication methods need to be given more attention. Because technology is changing so quickly, these holes need to be fixed before they become problems. This will make wireless networks more reliable and keep data transfers safe.

References

- [1] H. Almajed and A. Almogren, "A secure and efficient ECC-based scheme for edge computing and internet of things," *Sensors*, vol. 20, no. 21, pp. 6158 (2020).
- [2] A. S. Reegan and V. Kabila, "Highly secured cluster based WSN using novel FCM and enhanced ECC-ElGamal encryption in IoT," *Wireless Pers. Commun.*, vol. 118, pp. 1313–1329 (2021).
- [3] S. R. Moosavi and A. Izadifar, "End-to-end security scheme for E-health systems using DNA-based ECC," in *Silicon Valley Cybersecurity Conf.*, Berlin, Germany: Springer (2022).
- [4] H. D. Tiwari and J. H. Kim, "Novel method for DNA-based elliptic curve cryptography for IoT devices," *ETRI J.*, vol. 40, no. 3, pp. 396–409 (2018).
- [5] S. Das and S. Namasudra, "A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure," *Comput. Electr. Eng.*, vol. 101, pp. 107991 (2022).
- [6] P. Socha, V. Miškovský, and M. Novotný, "A comprehensive survey on the non-invasive passive side-channel analysis," *Sensors*, vol. 22, no. 20, pp. 8096 (2022).
- [7] S. Gabsi, Y. Kortli, V. Beroulle, Y. Kieffer, and B. Hamdi, "Proposal of a lightweight differential power analysis countermeasure method on elliptic curves for low-cost devices," *Multimedia Tools Appl.* (2024).
- [8] K. Kumagai, S. Kakei, Y. Shiraishi, and S. Saito, "Distributed public key certificate-issuing infrastructure for consortium certificate

- authority using distributed ledger technology," *Secur. Commun. Netw.* (2023).
- [9] Xian Shi, Li Wang, and Min Zhang, "State-of-the-art internet of things in protected agriculture," *Sensors*, vol. 19, no. 8, pp. 1833 (2019).
 - [10] Vijay V. Raje, Ananya Patel, and Rohit Kumar, "Efficient resource allocation in healthcare systems through deep learning and optimization science," *J. Inf. Optim. Sci.*, vol. 46, no. 4-B, pp. 1277–1288 (2025).
 - [11] Nikhil S. Shron, Priya Mehta, and Arjun Singh, "AI-driven predictive analytics for identifying emerging trends in quality-oriented employment," *Int. J. Electr. Electron. Comput. Syst.*, vol. 14, no. 1, pp. 72–80 (2025).
 - [12] Deepak Rangwani, Sunil Joshi, and Kavita Sharma, "An improved privacy preserving remote user authentication scheme for agricultural wireless sensor network," *Trans. Emerg. Telecommun. Technol.*, vol. 32, pp. e4218 (2021).
 - [13] W. N. Anandpwar, S. M. Barhate, and M. P. Dhore, "Designing an efficient machine learning-based intrusion detection system for enhanced cyber security in modern networks," *Int. J. Adv. Comput. Theory Eng.*, vol. 14, no. 1, pp. 86–93 (2025).

Received April, 2025