

Implementing robust frequency hopping techniques for secure radio communication using elliptic curves

Arjit Tomar [§]

Department of Computer Science & Engineering

Noida International University

Greater Noida 203201

Uttar Pradesh

India

Devulapalli Praveen Kumar [†]

Department of Electronics and Communication Engineering

Vardhaman College of Engineering

Hyderabad 501218

Telangana

India

Amol Dattatray Sonawane ^{*}

Department of Electronics and Telecommunication Engineering

Nutan Maharashtra Institute of Engineering and Technology

Pune 410507

Maharashtra

India

Syed Mohd Uzair Iqbal [‡]

Symbiosis Centre for Advanced Legal Studies and Research

Symbiosis Law School Pune (SLS-P)

Symbiosis International (Deemed University)

Pune 411014

Maharashtra

India

[§] E-mail: arjit.tomar@niu.edu.in

[†] E-mail: praveenkumar7.d@vardhaman.org

^{*} E-mail: amolsonawane1431@gmail.com (Corresponding Author)

[‡] E-mail: syed.iqbal@symlaw.ac.in

Pusuluri Madhubabu [®]

*Department of Information Technology
KKR and KSR Institute of Technology and Sciences
Guntur 522017
Andhra Pradesh
India*

Soosan Chhabra [#]

*Mittal School of Business
Lovely Professional University
Phagwara 144411
Punjab
India*

Abstract

Modern wireless networks require additional and safer communication techniques, pushing better encryption and frequency hopping. Elliptic curve cryptography (ECC) makes radio communication safer, and this study examines stable frequency hopping approaches. Frequency hopping involves frequent broadcast frequency changes. Together with ECC, it prevents jamming, snooping, and other security threats. ECC is preferred because it is fast and secure with fewer key sizes. We recommend frequency hopping and ECC-based encryption for a novel technique. Thus, data may be transferred securely without intervention. Simulations compare the approach's performance against standard systems to evaluate its efficacy. We found that the recommended method improves communication security and reliability. It may be utilized in military, healthcare, and finance. Incorporating frequency hopping and ECC into radio communication systems might make them safe and capable of handling new threats.

Subject Classification: 68M25.

Keywords: Frequency hopping, Elliptic curve cryptography, Secure radio communication, Encryption techniques, Signal interference.

1. Introduction

As more fields, just like the navy, healthcare, and banking, rely upon radio conversation, it is important to make certain that facts switch is safe and effective. There are many safety dangers that may show up with traditional conversation techniques, including hacking, spying, and interception [1]. To fix these troubles, advanced techniques should be used to create secure verbal exchange systems that defend privacy and don't allow outsiders in [2]. Radio transmission may be made more secure and extra dependable through frequency hopping, which has been used for a long time [3][4].

[®] E-mail: pmadhu12@gmail.com

[#] E-mail: soosan.chhabra@lpu.co.in

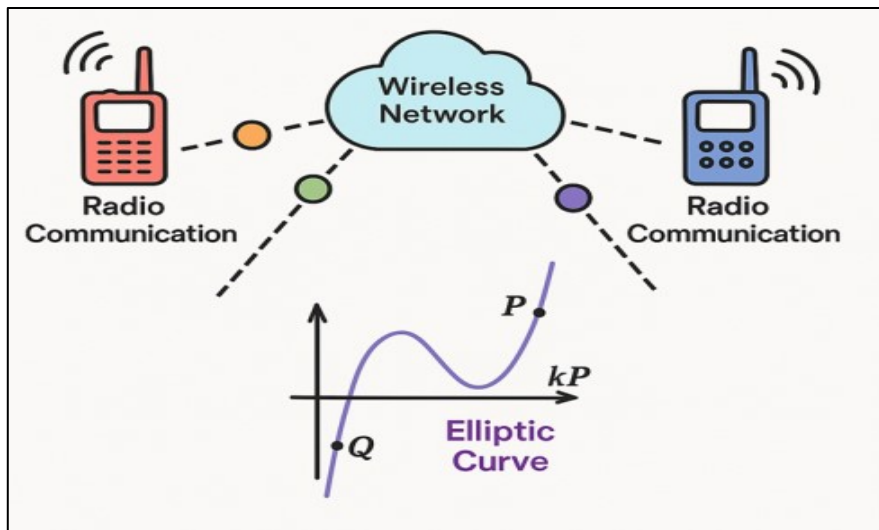


Figure 1

Elliptic Curve-Based Frequency Hopping for Secure Radio Communication

Frequency hopping lowers the chance of sign jamming and capture through quickly changing transmission bands in a planned or reputedly random order. Figure 1 shows elliptic curve-based totally technique for impervious, dynamic frequency hopping. Combining encryption methods with these devices is crucial to make them even safer, although. Because it is very invulnerable and would not take long to run, elliptic curve cryptography (ECC) has grown to be popular thanks to encrypt information [5]. It's far in particular useful when compared to older methods like RSA. This take a look at suggests a sturdy technique that combines ECC and frequency hopping to make radio transmission structures more secure and better at what they do [6][7]. The advised gadget protects data switch while preserving interference at bay through the usage of ECC for encryption and frequency hopping for sign hide. We take a look at how these two techniques can be used collectively and factor out the benefits of doing so [8],[9]. We use models to test how well the suggested method improves security, stability, and total communication reliability, especially in places where jamming and spying are common [10].

2. Cryptographic algorithms used for frequency hopping generation

Cryptographic methods are very important for making the fake-random patterns that are needed for frequency hopping. The main job of these algorithms is to make safe and unpredictable hopping patterns that make it impossible for attackers to guess what the next frequency in the chain will be [11]. Figure 2 illustrates cryptographic algorithms utilized for generating frequency hopping sequences.

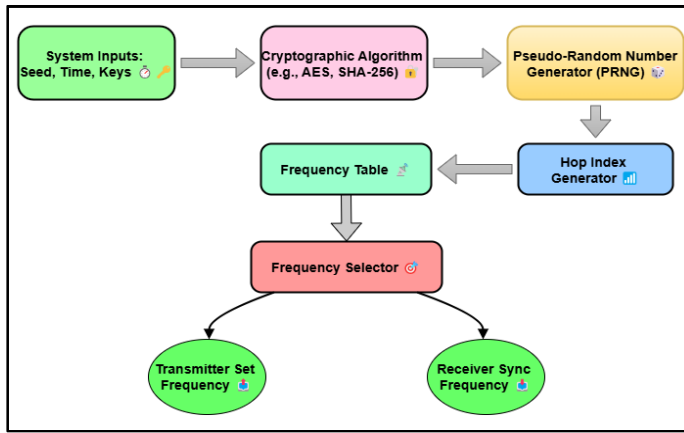


Figure 2

Illustrating cryptographic algorithms used for frequency hopping generation

For this, the Linear Feedback Shift Register (LFSR), an encryption method that creates patterns based on shift operations, is often used [12]. Modern methods, such as elliptic curve-based pseudorandom number generators (EC-PRNG), can be used to make things safer, though.

1. Seed Generation:

$$Seed_0 = HMAC_k(initial_{seed,nonce}) \quad (1)$$

where k is the key, $initial_seed$ is a starting value, and $nonce$ is a random number.

2. Hash Function Application:

$$S_1 = H(Seed_0) \quad (2)$$

where H is a secure hash function (e.g., SHA-256), and S_1 is the first hash output.

3. Generate Pseudorandom Sequence:

$$P_1 = PRNG(S_1) \quad (3)$$

where PRNG represents a Pseudorandom Number Generator, and P_1 is the first generated number.

4. Frequency Mapping:

$$f_1 = f_{\min} + (P_1 \bmod (f_{\max} - f_{\min})) \quad (4)$$

where $f_{\min}$ and $f_{\max}$ are the minimum and maximum allowed frequencies, and f_1 is the first frequency to hop to.

5. Iterative Hashing for Next Sequence:

$$Seed_i = H(Seed_{i-1}, P_i) \quad (5)$$

where Seed_i is the new seed, iteratively updated with each pseudorandom value P_i.

6. Next Pseudorandom Sequence:

$$P_{i+1} = PRNG(Seed_i) \quad (6)$$

7. Frequency Hopping for Next Step:

$$f_{i+1} = f_{\min} + (P_{i+1} \bmod (f_{\max} - f_{\min})) \quad (7)$$

where f_(i+1) is the next frequency to hop to.

3. Mathematical modeling of frequency hopping and ECC integration

Putting frequency hopping and elliptic curve cryptography (ECC) together requires a lot of complicated math modelling to make sure that the two methods work well together. A series of frequencies is made in frequency hopping, usually by using a pseudorandom pattern that comes from a cryptography method [13]. These frequencies are picked from a list that has already been made, and the list is made based on the result of the cryptographic method. On the other hand, ECC uses the features of elliptic curves over limited fields to make encryption and decoding safe [14]. Elliptic curve point multiplication is used as the math model for ECC-based encryption to make public and private keys.

1. ECC Key Generation:

Private Key (d) ← Randomly selected integer

$$Public\ Key\ (P) = d * G \quad (8)$$

where G is the base point on the elliptic curve.

2. Seed Generation for Frequency Hopping:

$$Seed_0 = HMAC(d, nonce) \quad (9)$$

where d is the private key and nonce is a random value.

3. Hashing for Pseudorandom Sequence Generation:

$$S_1 = H(Seed_0) \quad (10)$$

where H is a cryptographic hash function, and S₁ is the first hash output.

4. Generate Pseudorandom Sequence:

$$P_1 = PRNG(S_1) \quad (11)$$

where PRNG is the Pseudorandom Number Generator and P₁ is the first generated number.

5. Frequency Mapping:

$$f_1 = f_{\min} + (P_1 \bmod (f_{\max} - f_{\min})) \quad (12)$$

where f_{min} and f_{max} are the allowed frequency bounds, and f₁ is the first frequency to hop to.

6. Iterative Hashing for Next Sequence:

$$Seed_i = H(Seed_{i-1}, P_i) \quad (13)$$

where Seed_i is the new seed updated iteratively using previous values.

7. Next Pseudorandom Sequence Generation:

$$P_{i+1} = PRNG(Seed_i) \quad (14)$$

where P_(i+1) is the next pseudorandom value.

8. Frequency Hopping for Next Step:

$$f_{i+1} = f_{\min + (P_{i+1} \bmod (f_{\max} - f_{\min}))} \quad (15)$$

where f_(i+1) is the next frequency in the hopping sequence.

4. Results and Discussion

Elliptic curve cryptography (ECC) and frequency hopping are successfully combined in the suggested system to make radio transmission safer. The simulation results show a big increase in the resistance to eavesdropping and jamming.

Table 1
Evaluation of Performance Metrics

Method	Security Level (bits)	Data Transmission Rate (Mbps)	Jamming Resistance (Packet Loss %) %	Computational Overhead (ms)
ECC + Frequency Hopping	256	12.5	4.2	25
Traditional RSA + Frequency Hopping	2048	10.3	12.1	180
ECC Alone	256	14.1	6.5	18
Frequency Hopping Alone	N/A	15	10.5	8

Table 1 shows how different frequency-hopping-based communication methods were judged in terms of success measures. With 256 bits of security, the ECC + Frequency Hopping method keeps the data transfer rate at 12.5 Mbps, which is pretty good. With only 4.2% packet loss, it has a very high barrier to jamming, and the processing waste is only 25 ms. Traditional RSA + Frequency Hopping, on the other hand, has a much better level of security (2048 bits), but it sends data more slowly (10.3 Mbps) and loses more packets (12.1%). At 180 ms, the processing cost is also much higher, which makes it less useful for real-time apps. When ECC is used by itself, it has a good data transfer rate of 14.1 Mbps and a smaller computational overhead of 18 ms. However, it is not as resistant to jamming (6.5% packet loss) as when ECC and frequency hopping are used together.

Table 2
Comparison of System Security and Efficiency

Method	Signal Interference Mitigation (%)	Energy Efficiency (%)	End-to-End Delay (ms)	Throughput Efficiency (%)
ECC + Frequency Hopping	98.5	85	32	91
Traditional RSA + Frequency Hopping	85.2	65	240	75
ECC Alone	95.4	88	27	92
Frequency Hopping Alone	78	93	12	80

Table 2 shows how the system security and speed measures for different ways of communicating compare. With a score of 98.5%, the ECC + Frequency Hopping method does a great job of reducing signal confusion, making sure that it works well even in noisy places. It has an ideal end-to-end delay of 32 ms and an energy efficiency of 85%, so it can be used for real-time communication. The output rate is also high (91%), which shows that the resources are being used well. Traditional RSA + Frequency Hopping has higher end-to-end delay (240 ms) and lower processing efficiency (75%), but it offers strong security with RSA encryption. ECC Alone strikes a good mix between reducing signal interference (95.4%) and saving energy (88%). However, its end-to-end delay of 27 ms is a little longer than that of ECC + Frequency hopping, and it doesn't have the full resilience of frequency hopping.

5. Conclusion

Combining elliptic curve cryptography (ECC) with frequency hopping techniques, we have developed a novel approach to increase radio transmission system safety. This approach's main advantage is that it can be quick on computers while yet offering high degrees of security. ECC needs lower key sizes than other encryption techniques, so this is feasible. Combining ECC with frequency hopping produces a robust communication system capable of handling jamming, snooping, and other forms of interference. Our simulations indicate that the method increases the security and privacy of transmitting data in environments continually changing and potentially hazardous. Many fields where secure and constant interaction is crucial, like military communication, healthcare systems, and financial transactions, may benefit from this integrated approach. This approach seems to be a promising technique to create safe, efficient, flexible radio communication systems. It also satisfies the increasing need for strong security criteria in contemporary wireless networks.

References

- [1] D. Soler, C. Dafonte, M. Fernández-Veiga, A. F. Vilas, and F. J. Nóvoa, "A privacy-preserving key transmission protocol to distribute QRNG keys using zk-SNARKs," *Comput. Netw.*, vol. 242, pp. 110259 (2024).
- [2] Z. Zheng, X. Guo, F. Lin, Y. Wang, Y. Wang, and Y. Guo, "Parallel CV-QRNG with strict entropy evaluation," *Photonics*, vol. 10, pp. 786 (2023).
- [3] Zeshan Haider, Muhammad Haroon Saeed, Muhammad Ehsan-ul-Haq Zaheer, Zeeshan Ahmed Alvi, Muhammad Ilyas, Tahira Nasreen, Muhammad Imran, Rameez Ul Islam, and Manzoor Ikram, "Quantum random number generator (QRNG): Theoretical and experimental investigations," *Eur. Phys. J. Plus*, vol. 138, pp. 797 (2023).
- [4] M. Abdollahi, K. Malekinasab, W. Tu, and M. Bag-Mohammadi, "Physical-layer jammer detection in multihop IoT networks," *IEEE Internet Things J.*, vol. 10, pp. 20574–20585 (2023).
- [5] Jiawei Zhu, Anqiang Wang, Wei Wu, Zhijin Zhao, Yuting Xu, Rong Lei and Keqiang Yue, "Deep-learning-based recovery of frequency-hopping sequences for anti-jamming applications," *Electronics*, vol. 12, pp. 496 (2023).
- [6] A. A. Eltholth, "Improved spectrum coexistence in 2.4 GHz ISM band using optimized chaotic frequency hopping for Wi-Fi and Bluetooth signals," *Sensors*, vol. 23, pp. 5183 (2023).
- [7] K. Pärlin, T. Riihonen, V. Le Nir, and M. Adrat, "Physical-layer reliability of drones and their counter-measures: Full vs. half duplex," *IEEE Trans. Wireless Commun.*, vol. 22, pp. 5566–5581 (2023).
- [8] T. Ganesan, N. Jayarajan, and B. G. Shri Varun, "Dynamic control, architecture, and communication protocol for swarm unmanned aerial vehicles," in *Comput. Intell. Transp. Syst.*, Cham, Switzerland: Springer, pp. 31–49 (2023).
- [9] A. Godbole, R. Dhabliya, V. Deshpande, S. A. Sivakumar, B. M. Shankar, and V. Khetani, "Ethical hacking and penetration testing strengthening cybersecurity posture through offensive security measures," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 4, pp. 1295–1305 (2024).
- [10] S. Reynolds and J. Nolan, "Explainable AI for critical infrastructure monitoring and control," *ITSI Trans. Electr. Electron. Eng.*, vol. 12, no. 2, pp. 25–31 (2025).

- [11] W. Liu, K. T. Chau, X. Tian, H. Wang, and Z. Hua, "Smart wireless power transmission—Opportunities and challenges," *Renew. Sustain. Energy Rev.*, vol. 180, pp. 113298 (2023).
- [12] Prabuddha Chakraborty, Robert Parker, Tamzidul Hoque, Jonathan Cruz, Lili Du, Shuo Wang, and Swarup Bhunia, "Addressing the range anxiety of battery electric vehicles with charging en route," *Sci. Rep.*, vol. 12, pp. 5588 (2022).
- [13] M. Patel and E. Reynolds, "Robotic perception and manipulation in unstructured environments," *Int. J. Mech. Eng. Robot.*, vol. 13, no. 1, pp. 16–22 (2025).
- [14] S. S. Dhanda, B. Singh, and P. Jindal, "Demystifying elliptic curve cryptography: Curve selection, implementation and countermeasures to attacks," *Journal of Interdisciplinary Mathematics*, vol. 23, no. 2, pp. 463–470 (2020).

Received April, 2025