International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.281.04

An Analytical Study of Pseudorandom Generators and Stream Ciphers Using Elliptic Curve Cryptography

Sowmya T K
Department of Electronics and Communication Engineering
SDMIT, Dakshina Kannada, Karnataka, India

S. V. Sathyanarayana
Department of Electronics and Communication Engineering
JNNCE, Shimoga, Karnataka, India

Mohan Naik R
Department of Electronics and Communication Engineering
SDMIT, Dakshina Kannada, Karnataka, India

Abstract- As the demand for secure digital communication continues to grow, particularly over public networks, the generation of robust pseudorandom sequences has become a cornerstone of cryptographic systems like stream ciphers. This paper provides a detailed review of pseudorandom number generators (PRNGs), with particular emphasis on those developed using elliptic curves over finite structures such as fields and rings. It examines classic PRNG methods, cryptographically secure generators, and true random sources. Additionally, the study categorizes and compares elliptic curve-based approaches based on their mathematical frameworks, security attributes, computational efficiency, and statistical robustness. The work consolidates key contributions, underlying algorithms, implementation methodologies, and open challenges, offering guidance for advancing cryptographic research.

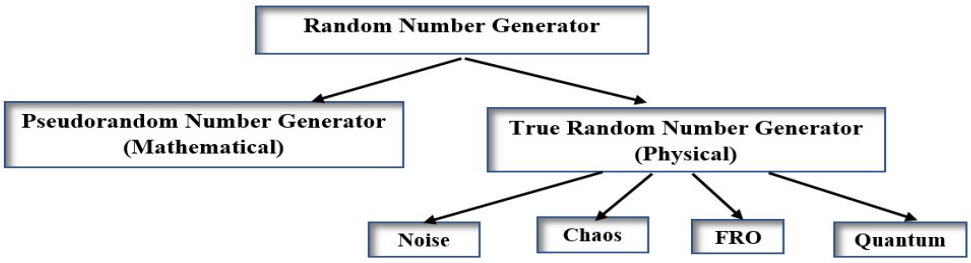
Keywords – PSNR Elliptic Curve Cryptography (ECC), Pseudorandom Number Generator (PRNG), Finite Fields, Finite Rings, Stream Cipher, Cryptographic Security, Linear Congruential Generator (LCG)

I. INTRODUCTION

Cryptography ensures the secure transmission of information by preventing unauthorized access, playing a vital role in maintaining confidentiality, integrity, authentication, and non-repudiation. Originally limited to military and diplomatic use, it is now integral to sectors such as digital communication, banking, and healthcare [1].

Central to most cryptographic mechanisms are pseudorandom number generators (PRNGs), which facilitate secure key generation and data randomization. PRNGs operate through deterministic algorithms that yield sequences resembling true randomness, often initialized with a specific seed. The effectiveness of cryptographic tools, especially stream ciphers, is highly dependent on the unpredictability of these sequences [2].

Elliptic Curve Cryptography (ECC) has emerged as an efficient cryptographic framework due to its strong security properties and low resource requirements. ECC-based PRNGs leverage the complex algebraic structure of elliptic curves defined over finite fields and rings to produce high-entropy random outputs. This paper surveys traditional and ECC-driven pseudorandom generation techniques, evaluating them on performance and security benchmarks



.

Figure 1:The tree of RNGs

II. LITERATURE REVIEW

A. Pseudorandom number generation

Pseudorandom number generation forms a fundamental component of contemporary cryptographic systems. This section provides a detailed survey of both classical and elliptic curve-based pseudorandom sequence generators (PRSGs), categorized by their structural foundation and cryptographic reliability.

1. Fan and Tian [3] introduced a technique to construct hyperelliptic covers for elliptic curves over quadratic extensions. Their approach offers improved efficiency in generating genus 2 curves by leveraging elliptic curve-based algorithms, particularly for secure point counting. The study supports curve generation strategies aimed at mitigating specific attacks like the cover-decomposition attack on elliptic curve discrete logarithms.
2. Pote and Lande [4] investigated elliptic curve arithmetic operations in extension fields, specifically F2pF_{2^p}F2p, to enhance encryption robustness. Their method, validated using SAGE software, demonstrated improved obfuscation in ciphertexts derived from elliptic curve operations, making it more difficult for adversaries to retrieve original messages.
3. El Marssi and El Marraki [5] offered a refinement of Koblitz's probabilistic mapping technique for elliptic curve cryptosystems. Their enhancements, such as eliminating double blocks and modifying loops, aimed to optimize encoding time without increasing computational complexity—especially useful in mapping plaintext blocks to curve points efficiently.
4. A novel pseudorandom generator inspired by the Lagged Fibonacci technique was proposed in [6], which integrates elliptic curves over finite fields. The generator achieved longer periods and fulfilled data encryption criteria through statistical validation.
5. Aung and Hla [7] applied complex number operations in elliptic curve cryptosystems over finite fields, facilitating secure computation over both prime and binary fields. Java's BigInteger class was employed to handle mathematical operations, revealing insights into elliptic curve cryptography across varying coordinate domains.
6. Rakhmatov and Ananyi [8] developed a reconfigurable ECC processor capable of handling modular arithmetic across five NIST-specified prime fields, with efficient implementation demonstrated on Xilinx FPGA platforms.
7. Babenko et al. [9] presented an optimized method of implementing elliptic curve cryptography using the Residue Number System (RNS), particularly improving the efficiency of point addition and doubling across multiple coordinate representations.
8. Gayoso Martínez et al. [10] analyzed the performance of elliptic curves in ECC using different curve forms—namely Weierstrass, Edwards, and Montgomery. Their comparison using the Safe Curves dataset highlighted trade-offs between performance and security.

B. Elliptic Curve PRNGs over Finite Fields and Rings

9. Huang and Xing [11] discussed critical computational challenges in elliptic curve cryptography over integer rings Zn. They introduced ECC analogs of RSA and Rabin cryptosystems and demonstrated reductions from integer factorization to elliptic curve-based security problems.
10. Gong et al. [14] proposed a pseudorandom sequence generator that employs elliptic curves over $GF(2^m)$, using trace functions. From a base point P, a sequence {P,2P,...,NP} is generated, with pseudorandom bits extracted via trace operations on coordinate values.
11. Sathyanarayana et al. [12] developed an image encryption system that derives symmetric key sequences from the random traversal of cyclic elliptic curve points. The method exploits ECC's natural randomness to improve encryption strength.
12. Reeyad and Kotulski [13] designed a pseudo-random binary sequence generator using elliptic curves over binary fields F2mF_{2^m}F2m, enhanced with S-box transformations and XOR logic. Out of 22 configurations, 14 passed multiple NIST tests and showed promising results in image encryption tasks.
13. Hassib [15] explored the mathematical properties of elliptic curves over a specialized ring $A_n=F_3[\varepsilon]$ with $\varepsilon^4=0$. The work introduced the j-invariant in this ring setting and its relevance to cryptographic designs
14. Hassiba et al. [16] generalized the findings for rings A_n, validating results for A2,A3, and A4. They uncovered unexpected algebraic behaviors, such as the emergence of subgroups based on projective coordinates, offering novel insights into ECC over rings.
15. Chillali [17] investigated elliptic curves over Fq[ε], focusing on structures where the discrete logarithm problem remains computationally difficult. The work provided optimized representations and operations tailored to cryptographic uses.
16. Chillali, Tadmori, and Ziane [18] focused on enhancing ECC over ring-based architectures, emphasizing their application in resource-constrained environments like wireless networks due to their security and efficiency advantages.
17. Bisson [19] developed a probabilistic method to compute the endomorphism rings of elliptic curves over finite fields. Assuming the Generalized Riemann Hypothesis, the algorithm runs in sub-exponential time and improves previous approaches by streamlining isogeny computations.
18. Chillali and El Fadil [20] analyzed elliptic curves defined over finite local rings Rn=Fq[X]/(Xn). They reviewed arithmetic properties and their potential in cryptographic systems across different field characteristics.

III. RESULTS AND DISCUSSION

i. Implementation of Pseudorandom sequence generator:

a. Linear Congruential Random Number Generator

The Linear Congruential Random Number Generator (LCRNG) is a widely used method for generating random numbers. It is called "linear congruential" because each number in the sequence is generated using a linear formula with modular arithmetic. The values are related through a simple mathematical relationship involving a modulus mmm. It works by using a sequence-generating formula.

$$\mathbf{X_i = (a*X_{i-1} + c) \bmod m} \qquad \mathbf{(1)}$$

b. BLUM BLUM SHUB GENERATOR

Blum Blum Shub (BBS) is a pseudo-random number generator, meaning it produces numbers that appear random but are actually determined by an initial value called a seed. Its randomness depends on this seed. The algorithm was developed in 1968 by Lenore Blum, Manuel Blum, and Michael Shub. BBS generates numbers using a specific mathematical formula.

$$x_{n+1}=x_n^2 ((mod M) \qquad (2)$$

c. Mersenne Twister

The algorithm is named after Marin Mersenne, a 17th-century French monk known for his work on prime numbers and for being regarded as the father of acoustics. The Mersenne Twister follows a specific mathematical structure to generate high-quality random numbers. The general form is

$$M_n=2_{n-1} \quad (3)$$

IV. EVALUATION METRICS

Table -1 EVALUATION METRICS

Author(s)	Technique	Field	Key Equation	NIST Test	Use Case
Gong et al. [26]	Trace function	GF(2^m)	Tr(x_n)	✓	Binary keystream
Reyad & Kotulski [29]	XOR + EC points + S-Box	GF(2^m)	x_n ⊕ S(x)	✓	Image encryption
Sathyanarayana et al.	EC point mapping from LFSR	GF(p)	k_iP	✓	Stream cipher
Payingat & Pattathil	Hash of EC x-coordinates	GF(p)	H(x(Q_i))	✓	Embedded systems
Chen & Li	Discrete log on EC	GF(p)	log_P(k_iP)	✓	Cryptographic PRNG
Hassib [31]	j-invariants in nilpotent ring	Ring	$\varepsilon^4 = 0$	Partial	Advanced ECC design
Huang & Xing [24]	EC over Zn, RSA-like	Ring	$y^2 = x^3 + ax + b \mod n$	✓	Public key systems

Evaluations typically use the NIST SP 800-22 test suite: - Frequency - Block frequency - Cumulative sums - Linear complexity. Table -1 shows the evaluation metrics for different techniques of pseudorandom generators.

Generators like those proposed by Reyad, Gong, and Payingat consistently pass these tests, indicating statistically sound sequences.

V. CONCLUSION

In today's world, where mobile networks and the internet are widely used, security has become more important than ever. Sensitive information shared over public networks must be protected from hackers. E-services like e-transfers, e-banking, emails, and e-business all require strong security measures.

The table shows that elliptic curve-based techniques are effective for generating secure random numbers. Most methods using finite fields (like GF(p) and GF(2^m)) pass the NIST tests and are used in real applications such as stream ciphers, image encryption, and embedded systems.

Some newer methods use elliptic curves over rings, which offer interesting possibilities for future cryptographic systems. While these may not fully pass all randomness tests yet, they are useful for exploring advanced ECC designs.

In summary, elliptic curves are powerful tools for creating secure and efficient random number generators, with strong potential in both current and future cryptographic applications.

In this paper, three types of pseudorandom number generators were studied and implemented. It also covers basic arithmetic operations related to finite fields, rings, and elliptic curves. A brief literature review was presented on pseudorandom generators and elliptic curves over finite fields and rings.

REFERENCES

[1] D.Stinson, "Cryptography Theory and Practice. Discrete Mathematics and its Applications", *3rd ed. Chapman Hall, 2006.*

[2] W. D. B. Junior, "Applications of frobenius expansions in elliptic curve cryptography," Ph.D. dissertation, Department of Mathematics Royal Holloway, *University of London, London, UK, September 2008*.

[3] Xuejun Fan and Song Tian, "Constructing Hyperelliptic Covers for Elliptic Curves over Quadratic Extension Fields," *ACISP 2019, LNCS 11547, pp. 630–638, 2019.*

[4] Santoshi Pote and B. K. Lande, "Elliptic Curve Arithmetic over Extension Field to Intensify Security and Privacy," *IEEE WiSPNET 2016 conference,978-1-4673-9338-6/16/2016 IEEE.*

[5] Karim El Marssi and Mohamed El Marraki, "Koblitz's Improved Probability Mapping Method in the Elliptic Curve Cryptosystem: A comparative study and results," *978-1-7281-0003-6/19/ © 2019 IEEE*.

[6] Shankar B R and Karuna Kamath K, "Lagged Fibonacci Generators Using Elliptic Curves over Finite Fields," *978-0-7695-3521-0/09/2009 IEEE, DOI 10.1109/ICCET.2009.103.*

[7] Tun Myat Aung and Ni Ni Hla "A Complex Number Approach to Elliptic Curve Cryptosystems over Finite Fields," 2019 International Conference on Computer Communication and Informatics (ICCCI -2019), *Jan. 23 – 25, 2019, Coimbatore, INDIA.*

[8] Kendall Ananyi and Daler Rakhmatov, "Design of a Reconfigurable Processor for NIST Prime Field ECC," 14th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM'06) *0-7695-2661-6/06 © 2006*.

[9] Mikhail Babenko, Aziz Salimovich Redvanov and Maxim Deryabin, "Efficient Implementation of Cryptography on Points of an Elliptic Curve in Residue Number System," 2019 International Conference on Engineering and Telecommunication (EnT), *12 March 2020*.

[10] V. GAYOSO MARTÍNEZ, L. HERNÁNDEZ ENCINAS AND A. MARTÍN MUÑOZ "Secure elliptic curves and their performance", *Vol. 00, No. 0, © The Author(s) 2018.*

[11] Ming-Deh A. Huang and Chaoping Xing, "Some Computational Problems of Cryptographic Significance Concerning Elliptic Curves over Rings", *Information and Computation 151, 92-99 (1999).*

[12] S. V. Sathyanarayana, M. A. Kumar, and K. N. H. Bhat, "Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve points," International Journal of Network Security, *vol. 12, no. 3, pp. 137–150, May 2011*.

[13] Kendall Ananyi and Daler Rakhmatov, "Design of a Reconfigurable Processor for NIST Prime Field ECC," 14th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM'06) *0-7695-2661-6/06 © 2006*.

[14] G. Gong, T. A. Berson, and D. R. Stinson, "Elliptic curve pseudorandom sequence generators,," Proceedings of the 6th Annual International Work- shop on Selected Areas in Cryptography, *pp. 34–48, 1999*.

[15] Hachem HASSIB, "Elliptic Curves over the Ring F_{3^d}[ε], ε4 = 0", International Mathematical Forum, *Vol. 9, 2014, no. 24, 1191 – 1196 HIKARI Ltd, www.m-hikari.com.*

[16] Moulay Hachem Hassiba, Abdelhakim Chillalib and Mohamed Abdou Elomary, "Elliptic curves over a chain ring of characteristic 3", *Journal of Taibah University for Science 9 (2015) 276–287.*

[17] Chillali Abdelhakim, "Elliptic Curve of the Ring Fq[\varepsilon] εn = 0", International Mathematical Forum, *Vol. 6, 2011, no. 31, 1501 – 1505.*

[18] A. Chillali, A Tadmori and M. Ziane, "Improved of Elliptic Curves Cryptography over a Ring", International Journal of Mathematical, Computational, Physical, *Electrical and Computer Engineering Vol:9, No:4, 2015.*

[19] [41] Gaetan Bisson, "Computing endomorphism rings of elliptic curves under the GRH" www.intechopen.com, Number Theory and Its Applications.

[20] Minoror thesis I: "Endomorphism rings of elliptic curves".Chao Li's HomepageHarvard UniversityMath DepartmentmaTHμ.

[21] Ivanov M.A., Chugunkov I.V. "Kriptograficheskie metody zashchity informatsii v komp'yuternykh sistemakh i setyakh" [Cryptographic Methods of Information Defense in the Computer Systems and Networks]. *Moscow, NIYaU MIFI Publ., 2012. 400 p*.