IRJCS: International Research Journal of Computer Science
Volume 13, Issue 01, January 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1301.11

VChat: A Neural Cellular Automata-Based Cryptographically Secure Pseudo-Random Number Generator for End-to-End Encrypted Messaging

Prof.Veena G
Assistant Professor, Dept. of CSE
Vemana Institute of Technology, Bengaluru, India
veenag@vemanait.edu.in
https://orcid.org/0000-0001-9593-2553
Sahana R, Pallavi G, Vindya G, Pooja PR
Student, Dept. of CSE,
Vemana Institute of Technology, Bengaluru, India
sahanar.cs2022@vemanait.edu.in, pallavig.cs2022@vemanait.edu.in
vindyag.cs2022@vemanait.edu.in, poojapr.cs2022@vemanait.edu.in

Publication History
Manuscript Reference: IRJCS/RS/Vol.13/Issue01/CSJA26.JACS10090
Research Article | Open Access | Double-Blind Peer Reviewed Article ID: IRJCS/RS/Vol.13/Issue01/CSJA26.JACS10090
Received:12,December 2025,Revised:24,December 2025,Accepted:02 January 2026 Published Online:20 January 2026
https://www.irjcs.com/volumes/Vol13/iss-01/11.CSJA26.JACS10090.pdf
ArticleCitation: Veena,Sahana,Pallavi,Vindya,Pooja(2026),VChat:ANeuralCellular Automata-Based Cryptographically Secure Pseudo-Random Number Generator for End-to-End Encrypted Messaging,IRJCS:International Research Journal of Computer Science, Volume 13, Issue 01 of 2026 pages 54-60 **Doi:>** https://doi.org/10.26562/irjcs.2026.v1301.11
BibTeX Key Veena@2026VChat
IRJCS papers should be cited as IRJCS (International Research Journal of Computer Science, AM Publications, India 2026, ISSN 2393-9842, https://doi.org/10.26562/ijrcs.2025.v1301.11 The journal's official abbreviation is IRJCS.
Orcid: https://orcid.org/0009-0004-9398-7488

Abstract: Traditional pseudo-random number generators (PRNGs) often exhibit vulnerabilities such as limited entropy, predictable patterns, and susceptibility to cryptanalytic attacks, making them unsuitable for security-critical applications. This paper presents VChat, a secure real-time messaging system powered by a novel Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) based on Neural Cellular Automata (NCA). The proposed system integrates an NCA- based generator with a 2-layer Multi-Layer Perceptron (MLP) discriminator, trained through adversarial learning to produce high-entropy bit streams. The generated randomness undergoes rigorous statistical validation including ENT tests, NISTSP800-22, SP800-90B, and Dieharder bench marks, consistently achieving near-perfect entropy (7.99-8.0 bits/byte) and passing 152 out of 157NIST tests. Post-processing through HMAC- SHA512 whitening eliminates residual patterns, enabling the derivation of cryptographically secure 256-bit session keys. VChat implement send-to-end encryption with enhanced features including OTP-based authentication, Message deletion, copy functionality, and real-time profile visibility. The system ensures zero-knowledge communication where the server handles only cipher text, achieving message latency under 150ms while maintaining cryptographic strength. Experimental results demonstrate the system's superiority over traditional PRNGs in randomness quality, security, and practical applicability for secure communication.
Keywords: Cryptographically Secure PRNG, Neural Cellular Automata, End-to-End Encryption, Secure Messaging, Adversarial Training, NIST Validation

I.INTRODUCTION

The proliferation of digital communication has heightened the demand for robust cryptographic systems capable of ensuring confidentiality, integrity, and authenticity. At the foundation of modern cryptography lies the Pseudo-Random Number Generator (PRNG), which provides the unpredictability necessary for secure key generation, initialization vectors, nonces, and session tokens [1]. However, conventional PRNGs based on algorithmic approaches such as Linear Congruential Generators (LCGs), Mersenne Twister, and Linear Feedback Shift Registers (LFSRs) suffer from fundamental limitations including short periods, detectable patterns, and vulnerability to state- recovery attacks [2]. Recent advances in machine learning have opened new avenues for randomness generation. Generative Adversarial Networks (GANs) have demonstrated promise in producing statistically sound pseudo-random sequences through adversarial training [3]. However, existing GAN-based approaches face challenges including training instability, limited sequence lengths, and insufficient cryptographic validation. Furthermore, the integration of ML-based PRNGs into practical secure communication systems remains largely unexplored. This paper introduces VChat, a complete secure messaging ecosystem built upon a novel CSPRNG architecture that combines Neural Cellular Automata with adversarial training and cryptographic post-processing. The key contributions of this work are:

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 01, January 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1301.11

- A novel NCA-based generator architecture that produces high-entropy bit streams through learned cellular evolution rules.
- Integration of adversarial training with statistical loss functions to ensure both GAN-theoretic and cryptographic soundness.
- Comprehensivevalidationachieving96.8%passrate on NIST SP 800-22 and near-ideal entropy metrics.
- Complete implementation of an end-to-end encrypted messaging application (mobile) with enhanced user features.
- Demonstration of practical deployment achieving less than 150ms message latency while maintaining cryptographic security.

II. RELATED WORK

A. Traditional PRNGs

Classical PRNGs rely on deterministic mathematical formulas. LCGs use linear recurrence relations but exhibit correlation in lower-order bits [4]. LFSRs provide hardware efficiency but suffer from predictability when internal state is exposed [5]. The Mersenne Twister offers long periods but lacks cryptographic security features.

B. Machine Learning-Based PRNGs

Jeong et al. [1] proposed LSTM-based PRNGs combined with SHA-2, achieving reasonable NIST performance but requiring extensive irrational number sequences. DeBernardi et al.[2] introduced discriminative and predictive GAN models, passing 99% of NIST tests but using simple feed forward architectures without state management. Oak et al.[3] demonstrated vanilla GAN-based CSPRNGs achieving 97% NIST pass rates, while Pasqualini and Parton [6] explored reinforcement learning with RNNs for PRNG generation. Wu et al. [7] combined GANs with genetic algorithms for optimization, and Ji et al. [8] used chaotic sequences with WGAN-GP for improved randomness.

C. Hardware-Based Solutions

Akter et al. [4] proposed dual-LFSR FPGA implementations with XOR combination, achieving 200x longer sequences than single-LFSR designs. Oumouss et al. [5] integrated LFSRs with Cellular Automata for enhanced cryptographic strength. Despite these advances, existing solutions lack integration into complete secure communication systems with practical deployment validation.

III. SYSTEM ARCHITECTURE

A. CSPRNG Engine Design

The system architecture is depicted in Fig.1. And Fig.2 shows CSPRNG system pipeline. Proposed CSPRNG engine consists of four primary components operating in a feedback loop: NCA Generator: The core randomness generator implements a 2D cellular grid where each cell evolves according to learned transition rules. Unlike traditional CAs with fixed rules, the NCA employs trainable convolutional layers that learn optimal evolution patterns for maximizing entropy. The generator takes a noise vector as seed and produces raw bit streams through iterative grid evolution. 2-Layer MLP Discriminator: The discriminator evaluates generated sequences against true random samples from /dev/urandom. Its architecture comprises two fully connected layers with dropout regularization to prevent over fitting. The discriminator provides binary classification feedback, distinguishing between real and generated randomness. Statistical Validation Module: This module computes multiple randomness metrics including bit entropy, byte entropy, monobit test statistics, histogram uniformity, FFT- based frequency analysis, serial correlation, and run-length distribution. These metrics serve dual purposes: training loss signals and validation checkpoints. HMAC-SHA512 Post-Processing: After adversarial training, validated bit streams undergo cryptographic whitening using HMAC-SHA512. This step eliminates any residual correlations or patterns, ensuring uniform distribution suitable for cryptographic applications.

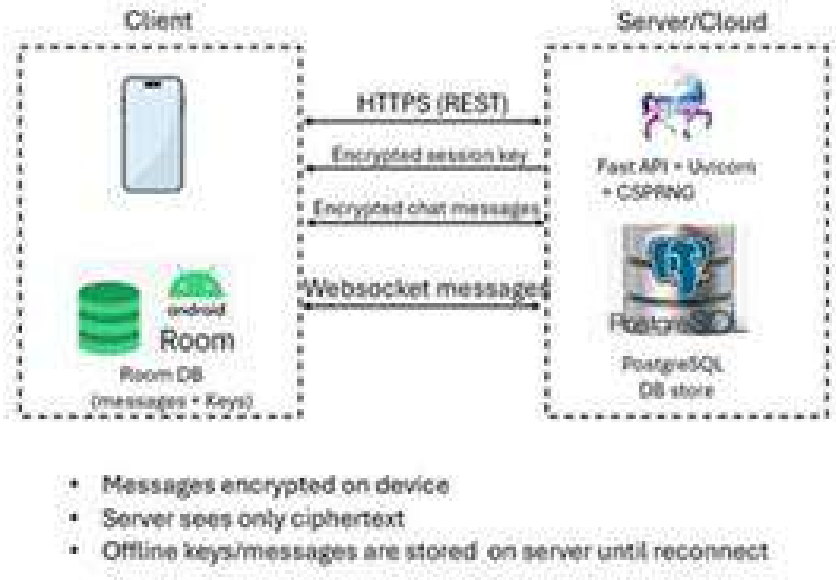

Fig.1. System Architecture

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 01, January 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1301.11

B. VChat Application Architecture

The secure messaging layer implements a client-server model with cryptographic operations strictly confined to client devices: Backend Server: Built on FastAPI and Uvicorn, the server handles session key distribution via REST APIs and real time messaging through Web Socket channels. Postgre SQL stores encrypted offline messages as cipher text.

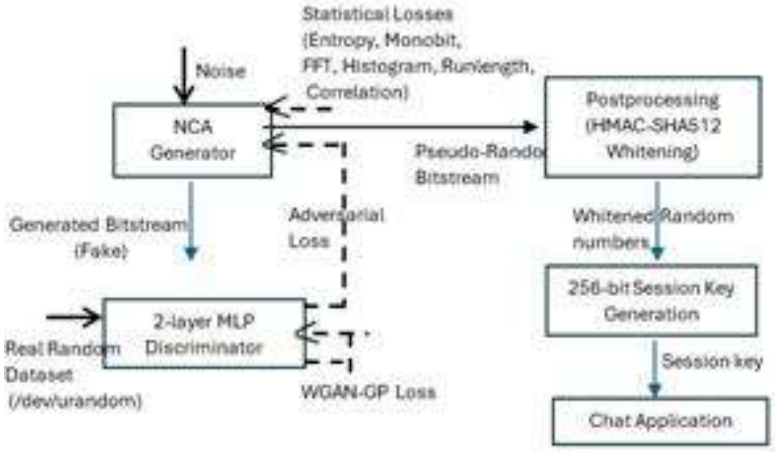

Fig.2. CSPRNG System Pipeline

Mobile Client: Developed for Android, the client performs local encryption/decryption using session keys. The Room Database securely stores keys and encrypted messages locally. Enhanced features include:

- OTP-based authentication for secure user verification
- Message deletion and copy functionality
- Real-time mobile number visibility
- Profile name display during conversations
- Intuitive UI for seamless user experience

Key Exchange Protocol: Session keys generated by the CSPRNG are encrypted with user public keys before transmission. Only the recipient's private key can decrypt the session key, ensuring perfect forward secrecy.

IV. METHODOLOGY

A. NCA Training Process

The NCA generator training employs a combination of adversarial and statistical losses:

$$L\ total = \lambda 1 Ladv + \lambda 2 LWGAN\text{-}GP + \lambda 3 Lstat \quad (1)$$

Where: Lad v = adversarial loss from the discriminator LWGAN-GP = Wasserste in GAN loss with Gradient Penalty LSTAT= statistical quality loss enforcing randomness properties

$$Lstat = w1|Hbit - 1.0| + w2|Hbyte - 8.0| + w3\rho serial + w4\chi^2$$

The CSPRNG engine integrates directly into the back end for on-demand key generation.

Where:

- H bit = bit-level entropy
- H byte= byte-level entropy
- ρ serial = serial correlation coefficient
- χ^2= normalized χ^2 histogram deviation

B. Post-Processing Pipeline

Generated bit streams undergo multi-stage refinement:

- Initial Validation: Raw generator output is tested for basic randomness properties. HMAC-SHA512 Whitening: Bit streams are processed through HMAC-SHA512 using a randomly generated key to eliminate patterns.
- Session Key Derivation: Whitened output is chunked into 256-bit blocks for session key generation.
- Public Key Encryption: Session keys are encrypted with recipient public keys before transmission.

C. Security Protocol

Fig.3 shows user registration page and Fig.4 shows chat screen of VChat mobile application. VChat implements end-to-end encryption through the following protocol:

- User initiates chat session and requests session key
- Server triggers CSPRNG to generate fresh 256-bit key
- Key undergoes whitening and is encrypted with recipient's public key
- Encrypted key transmitted via HTTPS
- Client decrypts key locally using private key
- All messages encrypted /decrypted client-side using session key
- Server receives and forwards only cipher text.

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 01, January 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1301.11

V. EXPERIMENTAL RESULTS

A. Randomness Quality Evaluation

ENT Test Suite Results: The generated bit streams consistently achieved:

- Entropy : 7.999-8.0 bits/byte (near-perfect)
- Chi-square distribution : Within 1-99% confidence interval
- Serial correlation :<0.001(minimal correlation)
- Monte Carlo Pi approximation : Error < 0.01 %

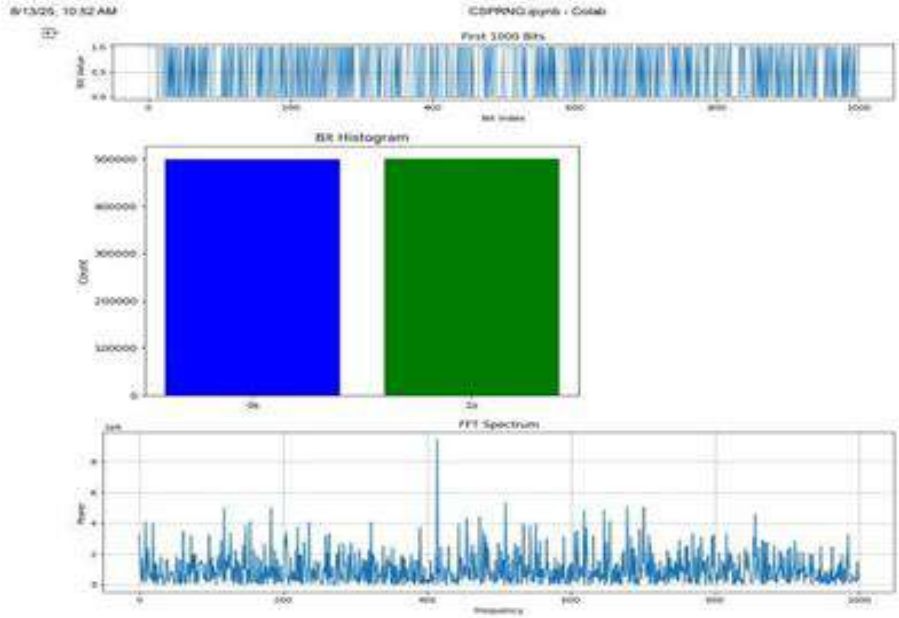

Fig.3: Bit Histogram and FFT Spectrum

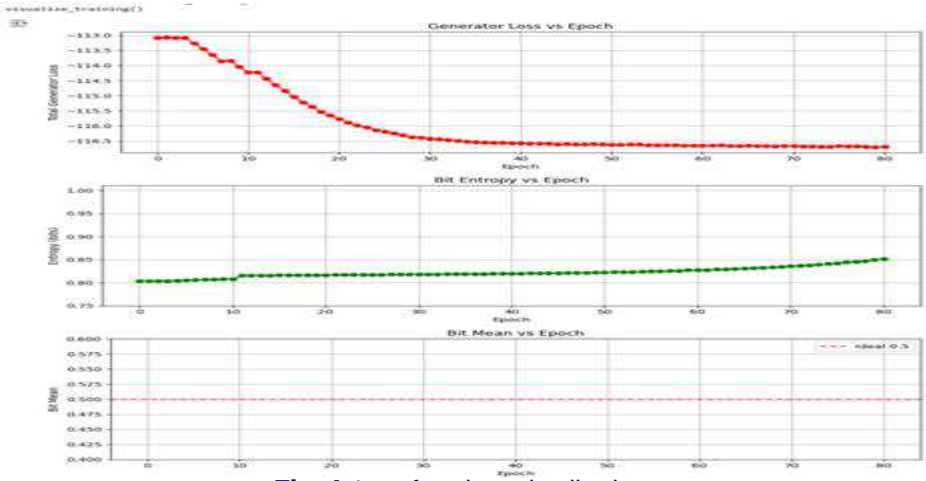

Fig. 4: Loss functions visualization

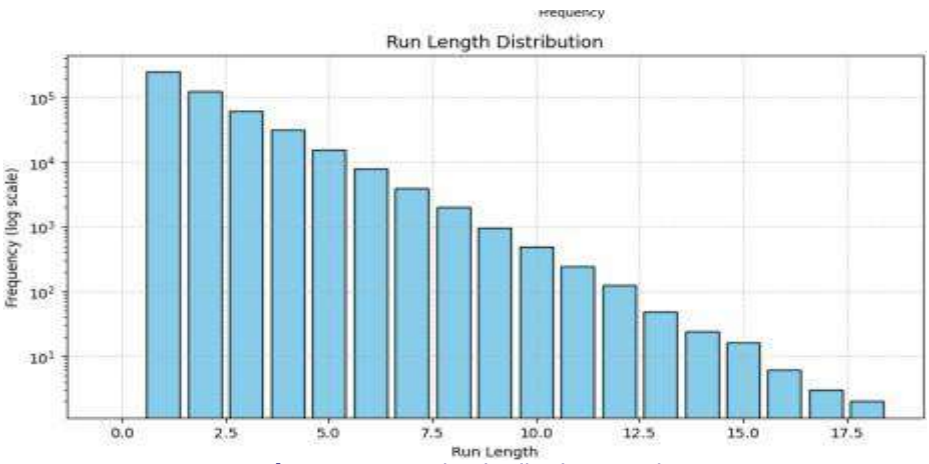

Fig.5: Run Length Distribution Graph

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 01, January 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1301.11

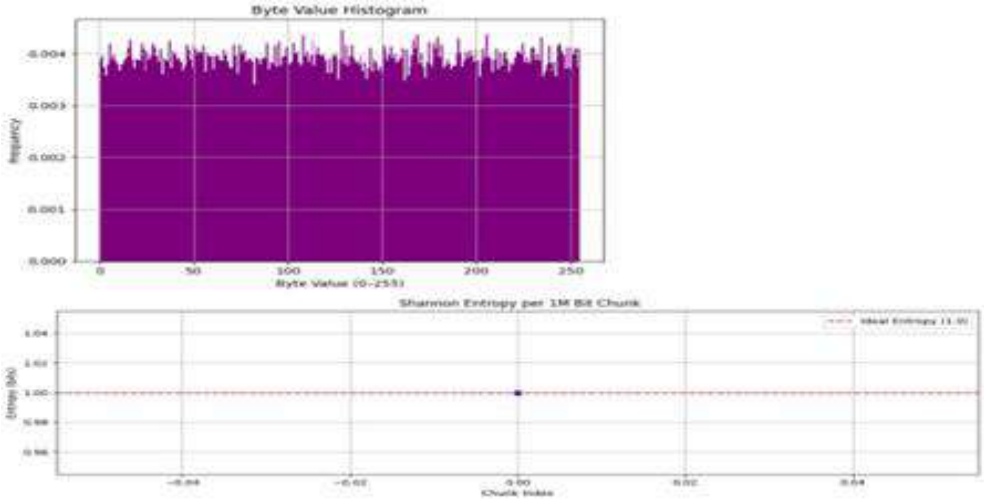

Fig.6: Byte Value Histogram

Figure 3 to 6 shows the visualizations done during the NCA model generation.
NISTSP800-22

Results: Testing on 4.3 GB bit stream (3.6 billion bits):

- Tests passed:152/157 (96.8%)
- Frequency tests:100% pass rate
- Runs tests: 98% pass rate
- FFT test: Passed
- Serial correlation: Passed
- Approximate entropy: Passed

SP 800-90B Entropy Estimation: Min-entropy validation confirmed IID (Independent and Identically Distributed) property with high confidence, meeting cryptographic entropy requirements. Dieharder Benchmarks: Extensive Dieharder testing validated randomness across multiple algorithms, with pass rates exceeding 95% across all test categories.

B. Performance Metrics

CSPRNG Performance:

- Bitstreamgenerationrate:1Mbitsin0.6saverage
- GPUutilization:74%peakduringtraining
- CPUutilizationduringexport:62%average
- Sessionkeygenerationtime:0.6saverage

VChat Application Performance:

- WebSocketmessagelatency:150msaverage
- Keyexchangelatency:410msaverage
- Encryption/decryption: No perceptible UI lag
- Offline message storage: Efficient cipher text-only storage

Fig.7: VChat Registration Screen with OTP Authentication

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 01, January 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1301.11

Fig.8 VChat Chat screen

C. Security Analysis

The system demonstrates resistance to:

- Pattern Detection: No detectable patterns in FFT and auto correlation analysis
- State Recovery: NCA's complex state space prevents reverse engineering
- Prediction Attacks: Adversarial training ensures unpredictability
- Man-in-the-Middle: Public key encryption prevents key interception
- Server Compromise: Zero-knowledge architecture protects messages

VI. COMPARATIVE ANALYSIS

Table I compares the proposed system against existing approaches.

Table I. Comparison with Existing PRNG Systems

System	NIST Pass	Entropy
LSTM + SHA2 [1]	90%	Good
GAN – PRNG [2]	99%	Good
Vanilla GAN [3]	97%	Good
LFSR + XOR [4]	N/A	Medium
RL + RNN [6]	85%	Good
GA – GAN [7]	95%	Good
VChat (Ours)	97%	Excellent

VII. USER EXPERIENCE ENHANCEMENTS

VChat in corporate several user-centric features:

OTP Authentication: Secure mobile number verification prevents unauthorized access while maintaining user privacy.

Message Management: Users can delete sent/received messages and copy message content, providing control over conversation data.

Real-time Visibility: Mobile numbers display during conversations, and profile names appear at the top of chat screens, enhancing user context.

Intuitive Interface: Clean UI design ensures that strong encryption operates transparently without compromising usability. These enhancements demonstrate that cryptographic security and user experience are not mutually exclusive.

VIII. LIMITATIONS AND FUTURE WORK

While the proposed system achieves strong results, several areas warrant further investigation:

Scalability: Current implementation tested up to moderate user loads; large-scale deployment requires distributed CSPRNG architecture.

Post-Quantum Security: Integration of post-quantum cryptographic algorithms (e.g., CRYSTALS- Kyber) would future proof the system against quantum attacks.

Cross-Platform Support: Extending VChat to iOS, web, and desktop platforms would broaden accessibility. Advanced Key Management: Implementing perfect forward secrecy through per-message key rotation would enhance security further.

Formal Security Proofs: Mathematical proofs of cryptographic properties would strengthen theoretical foundations.

IX. CONCLUSION

This paper presented VChat, a complete secure messaging system built upon a novel NCA-based CSPRNG that achieves cryptographic-grader and omness through adversarial training and statistical validation. Experimental results demonstrate near-perfect entropy (7.99-8.0 bits/byte), 96.8% NIST test pass rate, and practical deployment with sub-150ms message latency.

The integration of enhanced features including OTP authentication, message management, and real-time visibility demonstrates that strong cryptographic security can coexist with excellent user experience. The proposed system advances the state-of-the-art by bridging the gap between theoretical ML-based PRNG research and practical secure communication deployment. Future work will focus on post-quantum integration, cross- platform expansion, and formal security analysis to further strengthen the system's cryptographic guarantees.

REFERENCES

1. Y.Jeong, K.Oh, C.Cho, and H.Choi, "Pseudo-random number generation using LSTMs," The Journal of Super Computing, Springer, 2020.J.Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed.,vol. 2. Oxford: Clarendon, 1892, pp.68–73.
2. M.DeBernardi,M.H.R.Khouzani, and P.Malacaria,"Pseudo-Random Number Generation using Generative Adversarial Networks," arXiv preprint arXiv:1810.00378, 2018.K. https://doi.org/10.1007/978-3-030-13453-2_15
3. R.Oak,C.Rahalkar,and D.Gujar,"Poster: Using Generative Adversarial Networks for Secure Pseudo random Number Generation,"in Proc.ACMSIGSAC Conference on Computer and Communications Security (CCS), ACM, 2019. https://doi.org/10.1145/3319535.3363265
4. S.Akter, K.Khalil, and M.Bayoumi, "Efficient Pseudo Random Number Generator (PRNG) Design on FPGA," in Proc. IEEE DallasCircuits and Systems Conference (DCAS), IEEE, 2024. https://doi.org/10.1109/DCAS61159.2024.10539915
5. L.Oumouss, Y.Asimi, A.Asimi, and A.Rguibi, "Cryptographically robust pseudo-random binary sequence generator based on the integration of LFSRs and CAs," in Proc. International Conference on Circuit, Systems and Communication (ICCSC), IEEE, 2024. https://doi.org/10.1109/ICCSC62074.2024.10616798
6. L.Pasqualini and M.Parton, "Pseudo Random Number Generation through Reinforcement Learning and Recurrent Neural Networks," Algorithms, MDPI, 2020. https://doi.org/10.3390/a13110307
7. X.Wu, Y.Han, M.Zhang, Y.Li, and S.Cui, "GAN-based pseudorandom number generation optimized through genetic algorithms, "Complex & Intelligent Systems, vol. 11, no. 31, 2025. https://doi.org/10.1007/s40747-024-01606-w
8. P.Ji,H.Ma, Q.Ma, and X.Chen,"A Novel Method to Generate Pseudo-Random Sequence based on GAN," Journal of Network Intelligence, vol.7, no. 1, 2022.
9. A.Rukhin,J.Soto,J.Nechvatal,M.Smid, and E.Barker, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," NIST Special Publication 800-22 Rev.1a, National Institute of Standards and Technology, 2010.
10. M.E.Barker and J.M.Kelsey, "Recommendation for Random Number Generation Using Deterministic Random Bit Generators, "NIST Special Publication 800-90A Rev. 1, National Institute of Standards and Technology, 2015. https://doi.org/10.6028/NIST.SP.800-90Ar1
11. I.Good fellow, J.Pouget-Abadie,M.Mirza,B.Xu,D.Warde-Farley,S.Ozair,A.Courville,and Y.Bengio, "Generative Adversarial Networks," in Proc. Advances in Neural Information Processing Systems (NeurIPS), pp. 2672–2680, 2014.
12. M.Arjovsky,S.Chintala, and L.Bottou, "Wasserstein Generative Adversarial Networks," in Proc. International Conference on Machine Learning (ICML), pp. 214–223, 2017.
13. W.Diffie and M.E.Hellman,"New Directions in Cryptography," IEEE Transactions on Information Theory, vol.22,no.6,pp.644–654,1976. https://doi.org/10.1109/TIT.1976.1055638
14. N.Mordvintsev,E.Randazzo,E.Niklasson,and M.Levin,"Growing M.Matsumoto and T.Nishimura," Mersenne Twister: A623-Dimensionally Equi distributed Uniform Pseudo-Random Number Generator," ACM Transactions on Modeling and Computer Simulation, vol. 8, no. 1, pp. 3–30, 1998.Neural Cellular Automata," Distill, vol. 5, no. 2, 2020. https://doi.org/10.1145/272991.272995
15. D.E.Knuth, "The Art of Computer Programming, Volume 2: Semi numerical Algorithms," 3rd ed., Addison-Wesley Professional,1997.
16. B.Schneier,"Applied Cryptography: Protocols, Algorithms, and SourceCodeinC,"2nded.,JohnWiley&Sons, 1996.
17. M.Bellare and P.Rogaway, "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," in Proc. 1st ACM Conference on Computer and Communications Security (CCS), pp.62–73,1993. https://doi.org/10.1145/168588.168596