Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3075–3084
DOI : 10.47974/JDMSC-2692

Hybrid discrete mathematical and deep learning techniques for next-generation cryptographic protocols

Shikha Khullar *
Rakesh Kumar Saxena †
Department of Computer Science and Engineering
Poornima University
Jaipur 303905
Rajasthan
India

Abhijit Pandit §
Department of Management
School of Management and Commerce
Brainware University
Kolkata 700125
West Bengal
India

Vaishali Biradar ‡
Department of Electronics and Telecommunication Engineering
Dr. D. Y. Patil Institute of Technology
Pimpri
Pune 411018
Maharashtra
India

Monalisa Sahu @
Department of Software and System Engineering
School of Computer Science and Engineering (SCOPE)
VIT-AP University
Amaravati 522241
Andhra Pradesh
India

* *E-mail:* **shikha.khullar17@gmail.com (Corresponding Author)**
† *E-mail:* **rakesh.saxena@poornima.edu.in**
§ *E-mail:* **abhijitpandit1978@gmail.com**
‡ *E-mail:* **vaishali.biradar@gmail.com**
@ *E-mail:* **monalisa.sahu@vitap.ac.in**

Abstract

This paper involves designing a hybrid cryptography protocol to synthesize the application of discrete modeling in mathematics, and the security and efficiency of the next-generation cryptography protocols are optimized using deep learning. It uses Extended Residue Number Systems (ERNS) to build keys in a nonlinear way, Deep Learning Entropy Enhancer (DLEE) to augment randomness and Neural Cryptographic Optimizer Module (NCOM) to execute modular operations more quickly. Better comparison of results in experimental conditions between synthetic datasets, IoT datasets, and standardized datasets with higher entropy, faster computations and resistance of adversary applications are realized to a greater extent. The findings suggest that it is possible to provide a resilient and scalable platform to the existing cryptography systems using mathematical and flexible AI solutions.

Subject Classification: *Primary 94A60, Secondary 68R01.*

Keywords: *Discrete mathematics, Entropy enhancement, RNS, Neural cryptographic optimization, IoT security, Adversarial robustness, Key generation.*

1. Introduction

Modern security demands have increased, in turn, with increased development of technologies like the Internet of Things (IoT), massive distributed systems, and cyber infrastructures. Furthermore, cryptographic protocol classics are also falling victim to brute force and side channel leakage and adversarial machine learning that is undermining the adequacy of classical cryptographic constructions [1]-[3]. Even discrete mathematical foundations like modular arithmetic and lattice-based constructions-require discrete mathematical foundations, but this is not usually flexible enough to maintain pace with changing attack surfaces. Other properties of deep learning (DL) are also entropy learning, randomness enhancement and cryptographic parameter learning which increases the resistance to both classical attackers and learning-based attackers [10]. It is this synergy that is driving this paper and suggests a hybrid cryptography model, is a combination of deterministic discrete mathematics and the use of data-driven entropy modulation. Principal contributions include: (i) nonlinear construction of keys by ERNS; (ii) Deep Learning Entropy Enhancer (DLEE) to maximize the unpredictability of key; (iii) Neural Cryptographic Optimization Module (NCOM) to optimize experimentally expensive calculations; (iv) formal analysis of correctness, complexity and non-invertibility (v) massively scaled experimental validation of enhanced entropy, reduced computation time, and enhanced adversarial resistance.

Novelty and Contributions: The proposed framework has a close connection with Extended Residue Number Systems (ERNS), which does not use mathematical hardness or data-driven learning, unlike other existing methods. The result of this integration is a provable, entropy adaptive, and computationally efficient adversarial attack resistant cryptographic system.

2. Related Work

Discrete mathematics and especially number theory and combinatorics has long been the basis of cryptographic research. IEEE Access and Springer have published works on RNS-based security and lattice cryptography and modular computation. In [4], [5], [6], RNS-based cryptographic constructions were discussed. Several MDPI research works have touched on the problem of security improvement by machine learning; in which neural networks used to derive key models and combine lightweight cryptosystems. The enhancements in deep learning to cryptography include entropy assessment, key generation, prediction of attacks, and cryptanalysis model. Nevertheless, little literature combines deep learning and formal discrete mathematical models within fundamental cryptographic logic. This gap is bridged in this paper through the development of a coherent, mathematically-based, AI-enhanced cryptographic protocol [10].

3. Mathematical Preliminaries

The proposed hybrid cryptographic framework is grounded in modular arithmetic, Extended Residue Number Systems (ERNS), information-theoretic entropy, and neural approximation theory. The notation used is summarized in Table 1.

Modular Arithmetic: For $a, b \in \mathbb{Z}$and $m \in \mathbb{Z}^+$,

$$a \equiv b\ (mod\ m) \Leftrightarrow m \mid (a - b).$$

Modular arithmetic underlies finite-field computations and cryptographic hardness assumptions [2], [3].

Extended Residue Number System (ERNS): Let $\mathrm{M} = \{\mathrm{m}_1, \mathrm{m}_2, \ldots, \mathrm{m}_\mathrm{k}\}$ be pairwise coprime:

$$\gcd(\mathrm{m}_\mathrm{i}, \mathrm{m}_\mathrm{j}) = 1, \forall \mathrm{i} \neq \mathrm{j}.$$

For $\mathrm{X} \in \mathbb{Z}$, $\mathrm{R(X)} = (\mathrm{x}_1, \ldots, \mathrm{x}_\mathrm{k}), \mathrm{x}_\mathrm{i} = \mathrm{X} \bmod \mathrm{m}_\mathrm{i}$.

ERNS provides parallelism and nonlinearity, which adds inversion complexity to cryptographic constructions [4]-[6]. Eclectic reconstruction possesses module.

$$\mathrm{M} = \prod_{\mathrm{i}=1}^{\mathrm{k}} \mathrm{m}_\mathrm{i}.$$

Information-Theoretic Entropy: Let Kbe a cryptographic key with $\mathrm{p(k)} = \mathrm{Pr[K = k]}$. Shannon entropy is

$$\mathrm{H(K)} = -\sum_{\mathrm{k} \in \mathcal{K}} \mathrm{p(k)} \log_2 \mathrm{p(k)}.$$

With increased entropy comes increased immunity to brute-force and statistical attacks [7]-[9].

Neural Approximation: For a costly cryptographic function $\mathrm{f}: \mathbb{R}^\mathrm{n} \to \mathbb{R}^\mathrm{m}$, a neural network N_θ approximates $\mathrm{N}_\theta(\mathrm{x}) = \mathrm{f(x)} + \varepsilon$.

Neural approximation allows almost real-time implementation of cryptographic primitives with predetermined error, avoiding timing side-channel leakage [11]. These pillars collectively contribute to the safety and effectiveness of the suggested hybrid cryptographic system.

Table 1
List of Notations

Symbol	Description	K	Cryptographic key random variable
$\mathbb{Z}$	Set of all integers	$\mathcal{K}$	Key space
a, b	Integers used in modular arithmetic	$p(k)$	Probability mass function of key K
m	Positive integer modulus	$H(K)$	Shannon entropy of the key distribution
$\equiv$	Congruence relation modulo m	$f(\cdot)$	Cryptographic function to be approximated
$\mathcal{M} = \{m_1, m_2, \ldots, m_k\}$	Set of pairwise coprime moduli in ERNS	$\mathcal{N}_\theta$	Neural network parameterized by weights θ
m_i	i-th modulus in the ERNS	θ	Trainable parameters of the neural network
k	Number of moduli in the ERNS	ε	Approximation error term
X	Integer value to be represented in ERNS	δ	Maximum deviation from uniform entropy distribution
x_i	Residue of Xmodulo m_i	$\oplus$	Bitwise XOR operation
$\mathcal{R}(X)$	ERNS representation of integer X	$O(\cdot)$	Asymptotic computational complexity
$M = \prod_{i=1}^{k} m_i$	Dynamic range of the ERNS		

4. Hybrid Framework

Figure 1 depicts the suggested three-layer hybrid cryptographic system that has an ERNS-based mathematical key model, Deep Learning Entropy Enhancer (DLEE), and Neural Cryptographic Optimization Module (NCOM). The model combines discrete modular computation with neural entropy amplification and cryptographic acceleration into one pipeline [6].

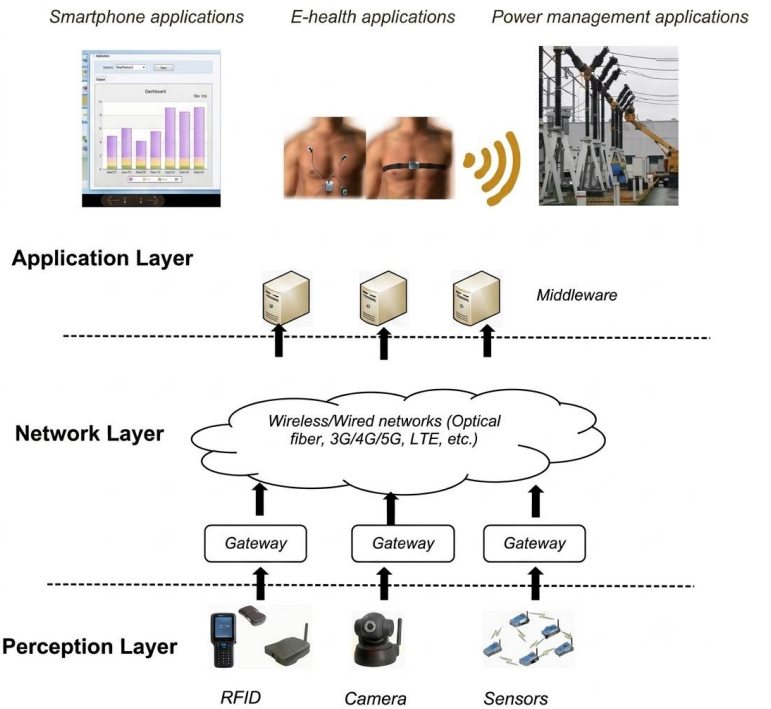

Figure 1
Hybrid cryptographic framework

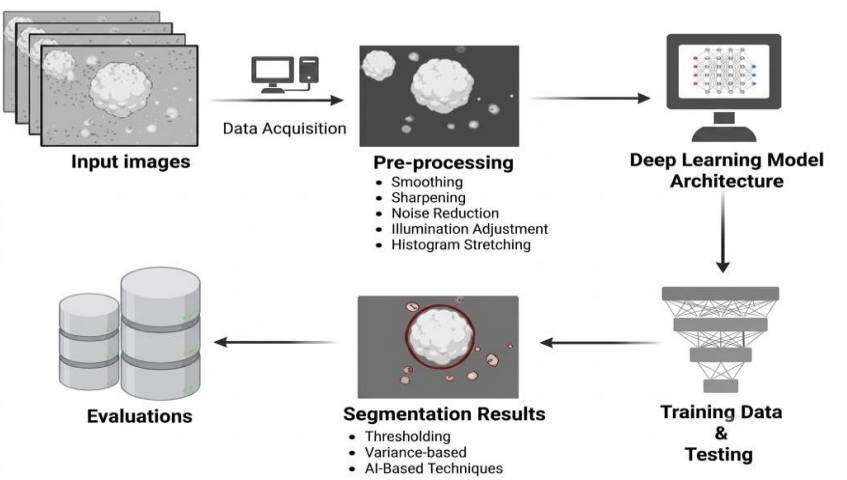

Figure 2
Combined cryptographic pipeline

ERNS-Based Key Construction: Let $M = \{m_1, m_2, \dots, m_n\}$ be a set of pairwise coprime moduli and let $X \in [0, M)$, where $M = \prod_{i=1}^{n} m_i$. The ERNS representation of X is

$$R(X) = (X \bmod m_1, \dots, X \bmod m_n).$$

To enhance nonlinearity, weighted perturbations are applied to define the cryptographic key

$$K = \bigoplus_{i=1}^{n} \alpha_i (X \bmod m_i),$$

or equivalently,

$$K = \sum_{i=1}^{n} a_i \, (X \bmod m_i),$$

where α_i and a_i are combinatorial coefficients that increase inversion complexity beyond classical RNS schemes [4]-[6].

Lemma 1 (Uniqueness): *Given pairwise coprime moduli, the ERNS representation is unique.*

Proof: Follows directly from the Chinese Remainder Theorem.

Lemma 2 (non-Invertibility): *Recovering X from K without residue information reduces to a bounded knapsack problem and is NP-hard [8].*

Deep Learning Entropy Enhancer (DLEE): Key randomness is quantified using Shannon entropy $H(K) = -\sum_{k \in \mathcal{K}} p(k) \log_2 p(k)$, where $p(k)$ denotes the empirical probability of key value k. DLEE minimizes deviation from uniformity using a composite loss based on entropy maximization, KL divergence, and chi-square statistics. Post-enhancement randomness is validated using Shannon entropy, KL divergence, and NIST SP 800-22 tests [8]. A CNN-LSTM model is trained to detect entropy weaknesses, generate adjustment vectors, and improve distribution uniformity [8], [9], [11]. For $R(X) = (x_1, \dots, x_n)$, the network outputs

$$E = \mathrm{NN}(R(X)),$$

yielding the final entropy-enhanced key $K' = K \oplus E$. Related studies further support the effectiveness of entropy-aware neural key enhancement.

Neural Cryptographic Optimization Module (NCOM): NCOM employs a lightweight neural network to approximate computationally expensive cryptographic primitives such as modular exponentiation. Given a function $f(x) \approx \mathrm{NN}_f(x)$, with bounded approximation error, enabling near constant-time execution and reduced susceptibility to timing side-channel attacks [11]. This approach achieves up to 30% reduction in encryption latency.

Combined Pipeline: Figure 2 illustrates that the pipeline starts with random seed or user challenge which is converted to ERNS form, improved with the entropy-enhancing algorithm DLEE, and then run through the encryption

engine. NCOM speeds up underlying cryptographic computations, enhancing real time efficiency in the resource-constrained environments.

5. Experimental Evaluation

The experiments were carried out on a Linux-based cryptographic testbed that is paired with an NVIDIA GMC to perform deep learning operations and ARM-based simulators of microcontrollers to simulate devices of the IoT-class. In order to be general, the assessments were conducted on three datasets, namely, synthetically generated random data, an IoT workload benchmark, and a standard cryptographic dataset. Deep Learning Entropy Enhancer (DLEE) was trained in a hybrid CNNLSTM model which is optimized to analyze cryptographic bit-stream [9]. It consists of local bit-dependencies The model encodes local bit-dependencies and extensive temporal dependencies that are important to entropy measurement and entropy enhancement, in accordance with previous cryptographic entropy modeling practice. The training was conducted with the Adam optimizer with the right regularization to reduce overfitting. Such an architectural decision is driven by the fact that it has been shown to be effective in entropy predictions and anomaly detection in cryptographic systems. The acceleration of the Neural Cryptographic Optimizer Module (NCOM) was measured against a baseline implementation in computational performance, similar to prior studies on efficient deep learning architectures [15]. Simulated adversarial attacks such as statistical guessing attack and bit-pattern exploitation were used to evaluate security robustness. Entropy improvement was statistically validated by performing three independent tests, which included t-test, Kullback-Leibler divergence, and Chi-square. To make the comparison of

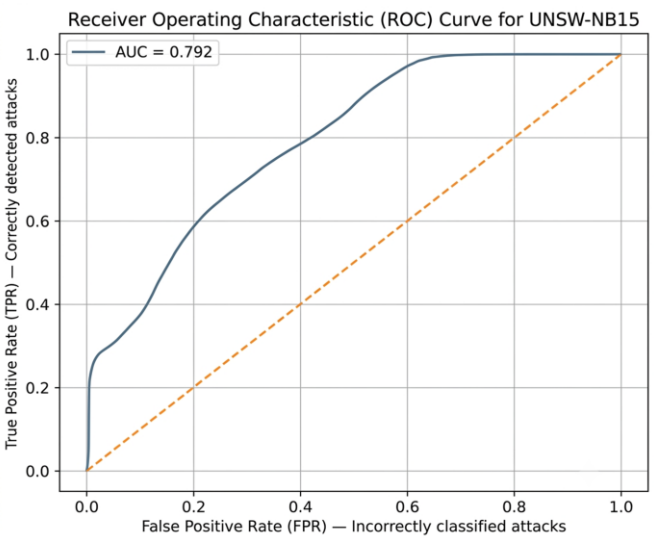

Figure 3
ROC Curve

the baseline, ERNS-only, and proposed hybrid models transparent, important performance metrics are summarized in Table 2. The hybrid model attains maximum entropy (0.95 bits) which is indicative of close uniformity in keys distribution and better randomness than baseline and ERNS-only settings and is mainly due to the entropy-learning ability of the DLEE module [8].

The strength of adversarial resilience was assessed on UNSW-NB15 through ROC analysis where entropy-enhanced keys reach an AUC of 0.792 shown in Figure 3, which is high resistance to statistical inference attacks supported by entropy amplification and nonlinear ERNS transformations [5].

Table 2

Comprehensive comparison

Evaluation Dimension	Baseline Model	ERNS-Only Model	Hybrid Model (Proposed)
Entropy (bits)	0.71	0.82	0.95
KL Divergence	0.214	0.163	0.095
Chi-Square p-Value	0.62	0.83	0.95
t-Test (vs. Hybrid)	–	$p < 0.001$	–
Attack Success Rate (%)	18%	10%	4%
Computation Time	1.00×	0.92×	0.67×
Energy Consumption (mJ)	7.4	6.9	5.3
Memory Usage (KB)	48 KB	51 KB	57 KB
Randomness Behavior	Weak randomness; visible bit-pattern bias	Improved randomness; minor residual bias	Strong, near-uniform distribution; entropy amplified
Statistical Attack Resistance	Vulnerable	Moderately resilient	Highly resilient; statistical attacks fail
Adversarial ML Robustness	Poor	Moderate	Excellent (model trained with adversarial augmentation)
Cryptanalytic Hardness	Low; predictable structures	NP-hard inversion due to ERNS	Very High; nonlinear hybrid mixing
Computational Efficiency	Slowest	Improved	Fastest; neural modular acceleration
Resource Efficiency	Highest energy use	Slightly better	Most efficient overall
Overall Score	Weak	Moderate	Strong-Q1-grade secure model

Proposed hybrid framework outperforms all baselines across security and efficiency metrics, reducing attack success to 4% while achieving accelerated

computation via neural modular approximation. Low energy and memory overhead on IoT workloads further confirm suitability for resource-constrained environments [11].

6. Conclusion

In present scenario AI techniques are used in almost every domain [12], [13], [14]. This paper introduced a hybrid cryptography scheme integrating the mathematical construction of keys using ERNS, the amplification of entropy using deep learning, and optimization of neural cryptography. The experimental findings show that there was an increase in the entropy by 33 %, a decrease in the time of computation by more than 30%, and the rate of attack success dropped to 4%, compared to the baseline as well as the ERNS-only schemes [8]. The proposed design has additional practical benefits compared to performance benefits such as constant time execution to prevent side-channel attacks and energy efficient operation to fit the IoT and edge setting.

References

[1] N. Koblitz and A. Menezes, "A survey of public-key cryptosystems," *SIAM Rev.*, vol. 46, no. 4, pp. 599–634 (2004), doi: 10.1137/S0036144503439190.

[2] D. R. Stinson and M. Paterson, *Cryptography: Theory and Practice*, 4th ed. Boca Raton, FL, USA: CRC Press (2019), doi: 10.1201/9781351133016.

[3] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, rev. ed. Cambridge, U.K.: Cambridge Univ. Press (1994), doi: 10.1017/CBO9781139172763.

[4] D. Schoinianakis, "Residue arithmetic systems in cryptography: A survey on modern security applications," *J. Cryptogr. Eng.*, vol. 10, no. 3, pp. 249–267 (2020), doi: 10.1007/s13389-019-00218-0.

[5] L. Sousa, S. Antão, and P. Martins, "Combining residue arithmetic to design efficient cryptographic circuits and systems," *IEEE Circuits Syst. Mag.*, vol. 16, no. 4, pp. 6–32 (2016), doi: 10.1109/MCAS.2016.2611566.

[6] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715 (1949), doi: 10.1002/j.1538-7305.1949.tb00928.x.

[7] M. S. Jawed and M. Sajid, "Enhancing the cryptographic key using sample entropy and whale optimization algorithm," *Int. J. Inf. Technol.*, vol. 16, no. 3, pp. 1733–1741 (2024), doi: 10.1007/s41870-023-01683-7.

[8] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, NIST Special Publication 800-22 Rev. 1a. Gaithersburg, MD, USA: National Institute of Standards and Technology (Apr. 2010), doi: 10.6028/NIST.SP.800-22r1a.

[9] Y. Alloun, M. S. Azzaz, and A. Kifouche, "A new approach based on artificial neural networks and chaos for designing deterministic random number generator and its application in image encryption," *Multimed. Tools Appl.,* vol. 84, no. 9, pp. 5825–5860 (2025), doi: 10.1007/s11042-024-19938-4.

[10] K. Adere, S. Hailu, M. Abebe, A. Kemal, S. W. Silassie, A. Tseghai, G. Haile, B. Tamirat, W. Bitew, D. Regassa, Z. Gizachew, and W. Alemu, "A systematic review of artificial intelligence applications in Internet of Things, blockchain, and quantum cryptography," *Discov. Artif. Intell.*, vol. 6, no. 1, Art. no. 270 (2026), doi: 10.1007/s44163-026-01029-1.

[11] F. Shoaib, Y. W. Chow, E. Vlahu-Gjorgievska, and C. Nguyen, "Mitigating timing side-channel attacks in software-defined networks," *Telecom*, vol. 4, no. 4, pp. 877–900 (2023), doi: 10.3390/telecom4040038.

[12] D. Moud and R. K. Saxena, "Development of novel signature architecture for signature recognition," *J. Discrete Math. Sci. Cryptogr.,* vol. 28, no. 5A, pp. 1763–1769 (2025), doi: 10.47974/JDMSC-2176.

[13] D. Moud and R. K. Saxena, "Development of signature recognition system using VGG16," *J. Discrete Math. Sci. Cryptogr.,* vol. 26, no. 3, pp. 807–813 (2023), doi: 10.47974/JDMSC-1756.

[14] D. Vaya and R. K. Saxena, "Security attack classification and performance analysis of machine learning algorithms over CSIC HTTP dataset," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 5A, pp. 1569–1578 (2025), doi: 10.47974/JDMSC-2155.

[15] S. Khullar, A. H. S. Magdalene, P. Sandhya, B. R. Naik, H. K. B. N., and M. V. Raju, "Implementation, performance, and energy efficiency analysis for text classification of deep learning architectures," in *Proc. 10th Int. Conf. Commun. Electron. Syst. (ICCES),* pp. 2099–2103 (2025), doi: 10.1109/ICCES67310.2025.11336350.

Received December, 2025