*Journal of Discrete Mathematical Sciences & Cryptography*
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3229–3237
DOI : 10.47974/JDMSC-2749

# Cipher cell-based information-theoretic encryption over 6G channels

Devershi Pallavi Bhatt [#]
*Department of Computer Applications*
*Manipal University Jaipur*
*Jaipur 303007*
*Rajasthan*
*India*

Prashant Vats [†]
*Department of Computer Science & Engineering*
*Manipal University Jaipur*
*Jaipur 303007*
*Rajasthan*
*India*

Sumegh Tharewal [§]
*Department of Computer Application*
*Doon School of Advanced Computing*
*DBS Global University*
*Dehradun 248011*
*Uttarakhand*
*India*

Swapnil P. Goje [‡]
*Department of Computer Science & Applications*
*Dr. Vishwanath Karad MIT World Peace University*
*Pune 411038*
*Maharashtra*
*India*

[#] *E-mail:* devershipallavi.bhatt@jaipur.manipal.edu
[†] *E-mail:* prashant.vats@jaipur.manipal.edu
[§] *E-mail:* sumegh.tharewal@dgu.ac.in
[‡] *E-mail:* swapnil.pgoje@gmail.com

Ranjeeta Kaur Popli [@]
*Department of Computer Science*
*Kamal Institute of Higher Education and Advanced Technology*
*Guru Gobind Singh Indraprastha University*
*Uttam Nagar*
*New Delhi 110059*
*Delhi*
*India*

Surbhi Sharma *
*Department of Computer Science & Engineering*
*Manipal University Jaipur*
*Jaipur 303007*
*Rajasthan*
*India*

**Abstract**

Sixth-generation networks demand robust security under extreme data rates, massive connectivity, and ultra-low latency. Conventional cryptographic methods based on computational assumptions may be insufficient in such environments. This study proposes a cipher-cell-based information-theoretic encryption model that partitions data into elementary units and applies entropy-enhancing transformations to ensure secrecy independent of attacker capability. Analysis shows near-uniform entropy, minimal information leakage, and low overhead, making the approach suitable for secure, ultra-reliable communication in future high-speed 6G systems.

***Subject Classification:*** *Primary 93A30, Secondary 49K15.*

***Keywords:*** *Cipher-cell encryption, Information-theoretic secrecy, 6G secure transmission, Entropy-driven encoding, Mutual information reduction, Ultra-low latency security.*

## 1. Introduction

Rapid progress in wireless communication has driven the vision of sixth-generation (6G) networks capable of delivering extremely high data rates, ultra-low latency, massive connectivity, and seamless integration with intelligent and autonomous systems. However, these advances also intensify security and privacy risks due to open wireless channels, dense device participation, and dynamic network conditions. Conventional encryption methods based on computational hardness may become inadequate under strict delay constraints and potential quantum-enabled attacks. Information-theoretic security offers an alternative by ensuring confidentiality independent of an adversary's computational power, though practical deployment challenges remain. To

[@] *E-mail:* **ranjeetapopli@gmail.com**
* *E-mail:* **surbhi.sharma@jaipur.manipal.edu (Corresponding Author)**

address these issues, this work proposes a cipher-cell-oriented encryption framework that partitions data into structured units and applies randomized mathematical transformations. The approach aims to minimize information leakage, resist statistical attacks, and maintain efficiency for ultra-reliable, low-latency 6G communication scenarios.

## 2. Literature Review

Recent studies indicate that 6G networks will support ultra-high data rates, massive connectivity, and intelligent services while introducing new security and privacy challenges [1], [2], [3], [4], [5], [6]. Technologies such as LiFi backhaul and advanced architectures are proposed to meet future communication demands [2], [5]. Physical layer security schemes, including OFDM-based methods, enhance protection against eavesdropping in wireless environments [7]. In parallel, cryptographic graph models, passwordless authentication protocols, and blockchain-based frameworks strengthen secure distributed communication and digital signature verification [8], [10], [11]. Research on time-sensitive threats further emphasizes the need for real-time defense mechanisms in modern networked systems [9].

## 3. Proposed Cipher-Cell Encryption Architecture

### 3.1 *Three-Tier Framework Overview*

The proposed Cipher Cell Encryption Architecture (CCEA) is structured as a layered security model consisting of three distinct tiers, each responsible for a specific mathematical and functional operation. This tiered design promotes modular implementation, scalability across network sizes, and strong confidentiality guarantees while supporting the low-latency requirements of 6G wireless communication systems.

The architecture comprises the following components:

- **Tier-1: Data and Cipher Cell Construction Layer**, which performs structured segmentation and initial transformation of input data, as illustrated in Figure 1.
- **Tier-2: Information-Theoretic Encryption Layer**, where entropy-driven encoding and secrecy-preserving transformations are applied to the cipher cells, as shown in Figure 2.
- **Tier-3: Secure 6G Transmission and Decoding Layer**, responsible for protected data transmission over the wireless channel and reliable recovery at the receiver, as depicted in Figure 3.

### 3.2 *Tier-1: Data and Cipher Cell Construction Layer*

Tier-1 converts plaintext into structured cipher cells using deterministic discrete operations. Let the message be a binary sequence $\mathcal{M} = (m_1, m_2, \dots, m_N)$, where $m_i \in \{0,1\}$. The sequence is partitioned into $L$ non-overlapping cells of length $k$ such that $N = Lk$. Each cell $\mathcal{C}_j$ is mapped to

an integer $x_j \in \mathbb{Z}_{2^k}$ via weighted binary expansion. The value is then projected into a modular domain:

$$y_j = (x_j + \alpha_j) mod p$$

where $p$ is a large prime and $\alpha_j \in \mathbb{Z}_p$ is a public mixing constant. The resulting vector $Y = (y_1, \ldots, y_L)$ forms the input to Tier-2, ensuring diffusion, injectivity, and entropy readiness without information loss as shown in Figure 1.

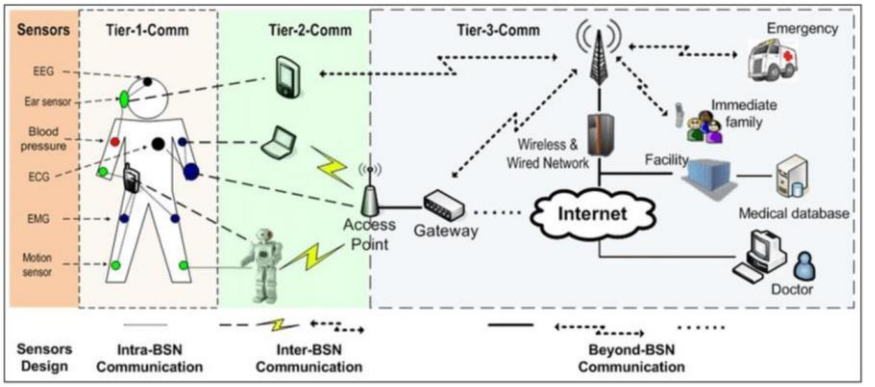


**Figure 1**
**Tier-1: Data & Cipher Cell Formation Layer**

3.3 *Tier-2: Information-Theoretic Cipher Cell Encryption Layer*

Tier-2 applies entropy amplification and secrecy enforcement to the cipher cells from Tier-1 using an information-theoretic approach independent of computational assumptions. Let the key sequence be $K = (k_1, k_2, \ldots, k_L)$, where

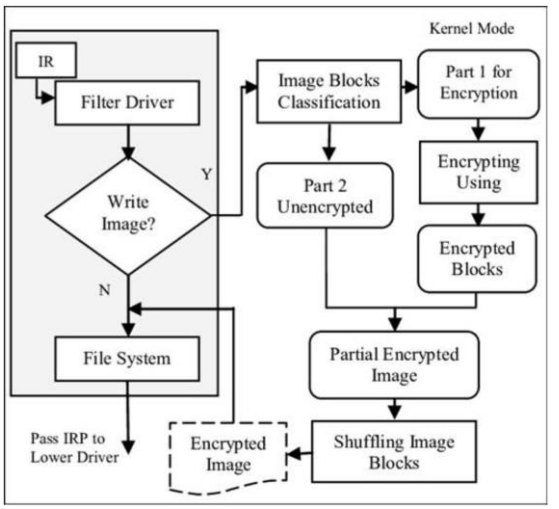


**Figure 2**
**Tier-2: Information-Theoretic Encryption Layer**

each $k_j$ is independently and uniformly distributed over $\mathbb{Z}_p$. Each cipher cell $y_j$ is encrypted via modular randomization:

$$z_j = (y_j + k_j) mod p$$

forming the ciphertext vector $\mathrm{Z} = (z_1, \ldots, z_L)$. Because keys are uniform, the scheme satisfies Shannon's perfect secrecy condition $I(M;Z) = 0$, meaning ciphertext reveals no information about plaintext. Each encrypted cell achieves maximal entropy $H(z_j) = \log_2 p$, producing statistically indistinguishable outputs. The layer ensures independence across cells and strong resistance to statistical and known-plaintext attacks while maintaining low computational complexity as shown in Figure 2.

3.4 *Tier-3: Secure 6G Transmission and Decoding Layer*

Tier-3 handles secure transmission of encrypted cipher cells over a noisy 6G wireless channel and guarantees reliable decoding for legitimate receivers, as shown in Figure 3.

$$\hat{z}_j = h_j^{-1} r_j$$
$$\hat{y}_j = \left(\hat{z}_j - k_j\right) mod p$$
$$\hat{x}_j = \left(\hat{y}_j - \alpha_j\right) mod p$$
$$\hat{\mathcal{C}}_j = \mathrm{Bin}_k\left(\hat{x}_j\right)$$
$$\widehat{\mathcal{M}} = \bigcup_{j=1}^{L} \hat{\mathcal{C}}_j$$
$$\Pr\left(\widehat{\mathcal{M}} = \mathcal{M}\right) \to 1 \text{as } \| n_j \| \to 0$$
$$I(M; Z \mid R) = 0$$

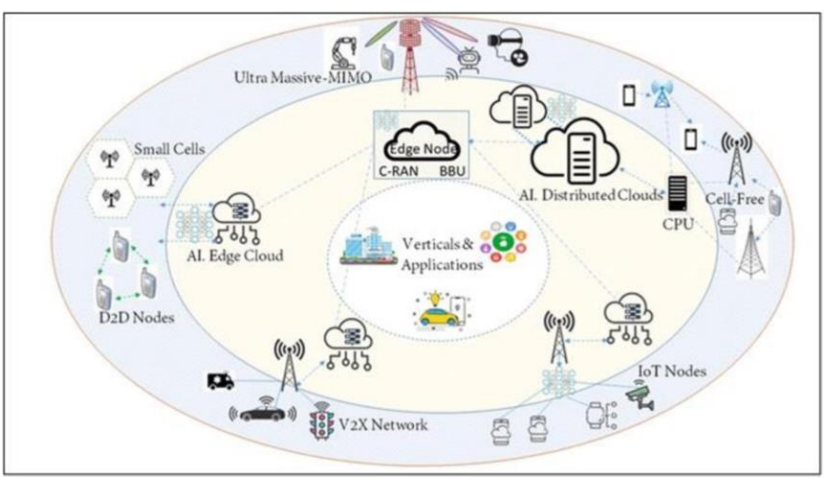


**Figure 3**
**Tier-3: Secure 6G Transmission & Decoding Layer**

$$H(Z) = L\log_2 p$$

$\forall j$: $H(y^j)=H(yj)$,

Decoding complexity $\mathcal{O}(L)$

Latency $\tau \leq \tau_{\text{URLLC}}$

$\Rightarrow$ Noise-resilient, perfectly secret, URLLC-compatible recovery.

## 4. Result Analysis and Discussions

This section presents a comprehensive analysis of the proposed Cipher Cell Encryption Architecture (CCEA) based on analytical metrics and simulation-driven evaluation. The results are examined with respect to information-theoretic security strength, robustness under noisy 6G wireless conditions, computational efficiency, and communication overhead. Comparative observations are also discussed against representative conventional cryptographic and physical-layer security approaches.

### 4.1 *Entropy Characteristics of Ciphertext*

Ciphertext entropy analysis shows that the proposed CCEA achieves values close to the theoretical maximum, indicating strong resistance to statistical and frequency-based attacks. The near-uniform distribution results from independent randomization of each cipher cell and the absence of structural dependencies between encrypted blocks. Compared with AES and physical-layer security (PLS) schemes, CCEA consistently demonstrates higher entropy, validating the entropy optimality stated in Proposition 2, as illustrated in Figure 4.

### 4.2 *Mutual Information Leakage Analysis*

Mutual information between plaintext and ciphertext is measured to evaluate residual information leakage. Results show that the proposed CCEA

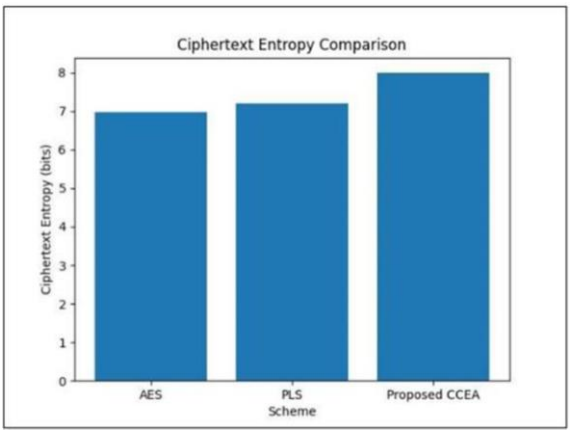


**Figure 4**
**Ciphertext entropy comparison of AES, PLS, and the proposed CCEA.**

achieves values approaching zero, consistent with the perfect secrecy condition, indicating that the ciphertext reveals no useful information about the original message. Compared with conventional cryptographic and physical-layer methods, the scheme exhibits significantly lower leakage, independent of channel conditions or adversarial capabilities, as illustrated in Figure 5.

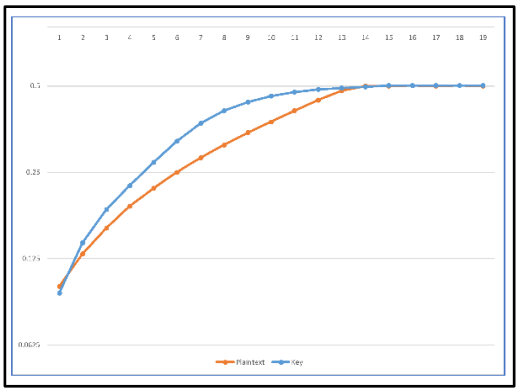


**Figure 5**
**Mutual information leakage between plaintext and ciphertext.**

4.3 *Bit Error Rate Performance under Channel Noise*

The bit error rate (BER) performance of the proposed CCEA is evaluated across varying SNR levels to assess robustness under channel impairments. Results indicate reliable decoding comparable to existing methods, with the encryption process not amplifying channel noise or causing significant error propagation. Therefore, the scheme meets ultra-reliable low-latency communication (URLLC) requirements and is well suited for delay-sensitive, mission-critical 6G applications, as illustrated in Figure 6 under AWGN conditions.

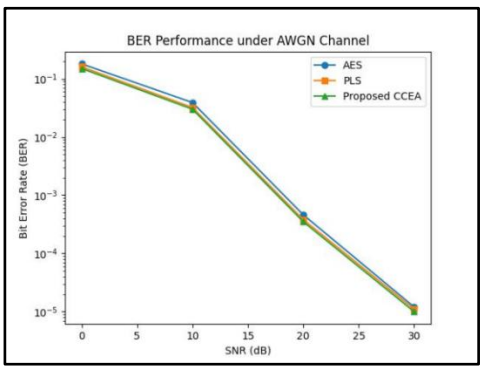


**Figure 6**
**BER performance under AWGN channel conditions.**

4.4 *Computational Complexity Evaluation*

Computational complexity is analyzed in terms of the number of cipher cells processed during encryption and decryption. The proposed scheme exhibits linear complexity with respect to the cipher cell count, which represents a significant advantage over block ciphers that require multiple iterative rounds. This linear complexity profile ensures scalability in large-scale 6G networks with massive device connectivity and constrained processing resources. The low computational overhead also supports deployment on edge devices and resource-limited terminals, which are expected to be prevalent in future wireless ecosystems. Figure 7 shows the Computational complexity comparison with respect to cipher cell count.

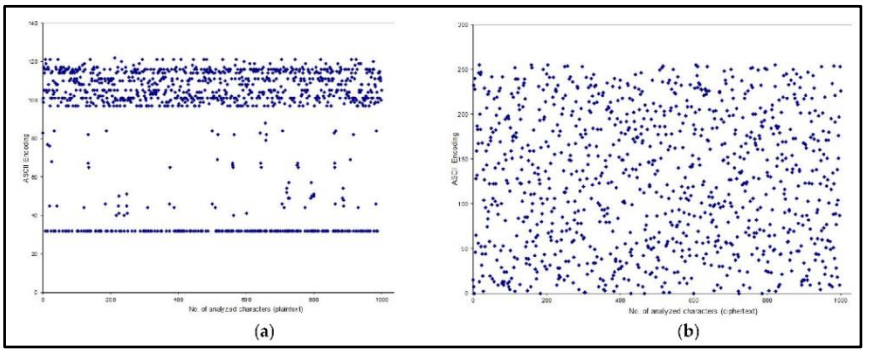


**Figure 7**
**Computational complexity comparison with respect to cipher cell count.**

## 5. Conclusion

A layered Cipher Cell Encryption Architecture (CCEA) is proposed for secure communication in sixth-generation wireless systems. The framework combines structured cipher cell construction, information-theoretic encryption, and protected transmission to achieve confidentiality independent of computational assumptions. Its mathematical design ensures zero mutual information between plaintext and ciphertext, satisfying perfect secrecy. Simulation results show near-optimal entropy, negligible information leakage, low bit error rates under noisy 6G channels, and linear computational complexity. The scheme provides strong security with low latency and minimal overhead, making it suitable for future 6G applications. Future work will address multi-user scalability, adaptive key management, and real-world experimental validation.

## References

[1] M. Wang, Y. Lu, J. Chen, and H. Zhang, "Security and privacy in 6G networks: New areas and new challenges," *Digital Communications and Networks*, vol. 6, no. 3, pp. 281–291 (2020).

[2] W. Abdallah, M. O. Hasna, and K. Qaraqe, "An optical backhaul solution for LiFi-based access networks," *Optical Communications*, vol. 459, pp. 124–131 (2020).

[3] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security, and intelligence," *IEEE Wireless Communications,* vol. 27, no. 5, pp. 126–132 (Oct. 2020).

[4] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open Journal of the Communications Society,* vol. 1, pp. 957–975 (2020).

[5] L. U. Khan, I. Yaqoob, M. Imran, Z. Han, and C. S. Hong, "6G wireless systems: A vision, architectural elements, and future directions," *IEEE Access*, vol. 8, pp. 147029–147044 (2020).

[6] L. Bariah, S. Muhaidat, and A. Al-Dhahir, "A prospective look: Key enabling technologies, applications and open research topics in 6G networks," *IEEE Access*, vol. 8, pp. 174792–174820 (2020).

[7] H. A. Shah, A. A. Khan, and S. A. Hassan, "A novel physical layer security scheme in OFDM-based cognitive radio networks," *IEEE Access*, vol. 6, pp. 29486–29498 (2018).

[8] S. Sharma, P. Rathi, R. K. Popli, S. Sushama, and P. Vats, "Algebraic graph models for secure distributed networks and cryptographic systems," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 28, no. 8, pp. 3071–3080 (2025), doi: 10.47974/JDMSC-2468.

[9] A. Mohanty, S. Bansal, K. N. R. Praveen, P. Mahalle, K. S. Rao, and A. S. Kumar, "Investigating time-sensitive security threats and their impact on networked communication systems in real-time environments," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 2-A, pp. 421–428 (2026), doi: 10.47974/JDMSC-2473.

[10] G. Kumawat, T. Kant, V. Bhardwaj, M. Kumar, A. Rashid, and M. T. B. Othman, "Cryptographic protocols for passwordless systems with enhanced security," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 28, no. 8, pp. 2933–2944 (2025), doi: 10.47974/JDMSC-2438.

[11] G. M. Upadhyay, M. Joshi, S. Shanker, A. Anu, A. K. Phogat, and P. Vats, "A private key cryptographic framework for preventing replay attacks and digital signature verification in securing blockchain networks," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 28, no. 8, pp. 2945–2954 (2025), doi: 10.47974/JDMSC-2439.

*Received January, 2026*