Quantum-Inspired GenAI Cryptography System using QGAN Key Generation, BB84 QKD Simulation, and Hybrid Classical–Quantum Encryption

B. Sreeshanth (22BDS016), G. Gokul (22BDS026), M. Navadeep (22BDS040), G. Sandeep (22BCS043)
Quantum GenAI Course
Indian Institute of Information Technology Dharwad (IIIT Dharwad), India
Email: team@iiitdwd.ac.in

***Abstract*—This paper presents a hybrid classical–quantum cryptographic system that integrates Quantum Generative Adversarial Networks (QGAN) for high-entropy key generation, BB84-style Quantum Key Distribution (QKD) simulation for secure multi-user key exchange, and AES-CFB symmetric encryption enhanced with quantum-inspired preprocessing transformations. The system demonstrates a practical, deployable approach to quantum-secure communication using only classical hardware, by combining generative models, quantum-inspired noise patterns, reversible transformations, and entropy amplification. A wallet module for identity-based cryptographic management and several quantum-state visualizations—including rotating qubits, entropy heatmaps, and latent-space analysis—are incorporated. Results show improved entropy, enhanced unpredictability, and increased resistance to ciphertext statistical attacks, demonstrating the effectiveness of quantum-inspired methods for modern cryptography.**

***Index Terms*—QGAN, QKD, Quantum Cryptography, BB84, Hybrid Encryption, AES-CFB, Quantum-Inspired Algorithms, Streamlit, GenAI, IIIT Dharwad.**

I. Introduction

Quantum computing presents new security challenges for classical cryptographic systems. Algorithms such as Shor's and Grover's threaten RSA, ECC, and symmetric ciphers by reducing computational hardness. As a result, post-quantum and quantum-inspired cryptography are actively researched.

In this project, we develop a practical hybrid cryptographic system deployable on classical computers but enhanced with quantum-inspired concepts. The system includes:

- QGAN-based entropy-rich key generation
- BB84-style QKD simulation for secure exchange
- Hybrid AES-CFB encryption with quantum preprocessing
- Identity wallet for secure key storage
- Visualization tools for interpretability

This system provides an educational demonstration of how classical and quantum paradigms can merge to enhance security, even without real quantum hardware.

II. Related Work

A. Quantum Cryptography

Quantum cryptography, particularly BB84 QKD, leverages quantum mechanics to establish secure channels. Although real quantum hardware is expensive, simulations help understand these protocols.

B. Quantum Machine Learning

QGANs are hybrid quantum-classical models capable of learning probability distributions. Our use of QGAN is simplified but follows the principle of generating complex high-entropy outputs.

C. Hybrid Encryption

AES-CFB is widely used for symmetric encryption. We enhance it with quantum-inspired randomness and reversible transformations.

III. System Architecture

The overall architecture is shown in Fig. 1.

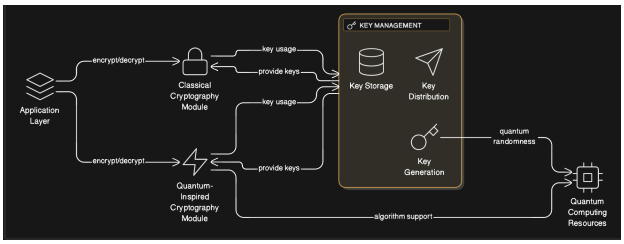

Fig. 1. Hybrid Quantum-Inspired Cryptography Architecture

Modules include:

1) QGAN Key Generator
2) QKD BB84 Simulation Engine
3) Hybrid Encryption Pipeline
4) Identity Wallet
5) Visualization Suite

IV. QGAN-Based Key Generation

A. QGAN Generator

The QGAN generator is a PyTorch model enhanced with a PennyLane-inspired rotation circuit. It outputs a 32-byte random state mapped to AES-256 keys.

$$z \sim \mathcal{N}(0, I) \tag{1}$$
$$x = G(z) \tag{2}$$
$$k = \text{MapToKey}(x) \tag{3}$$

B. Entropy Measurement

Shannon entropy:

$$H = -\sum p(x) \log_2 p(x)$$

QGAN-generated keys reach entropy values exceeding 7.8 bits per byte.

V. BB84 QKD Simulation

The BB84 QKD simulation follows:

1) Alice randomly chooses bits and bases.
2) Bob randomly measures.
3) Basis reconciliation.
4) Sifting to extract shared key.

A noise model:

$$e \sim \text{Bernoulli}(p)$$

Quantum Bit Error Rate:

$$QBER = \frac{\text{errors}}{\text{total bits}}$$

If QBER $< 11\%$, the key is accepted.

VI. Hybrid Classical–Quantum Encryption

A. Quantum-Inspired Preprocessing

We apply rotation mixing:

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

Noise layer:

$$x' = x \oplus n$$

B. AES-CFB Encryption

Ciphertext:

$$C = AES\_CFB(K, X')$$

Signature uses PQ-hash:

$$\sigma = H(C||K)$$

VII. Identity Wallet System

The wallet stores:

- Identity name
- Associated key (hex)

Stored in encrypted JSON for safety.

VIII. Visualizations

We include:

- Rotating qubit animation
- QKD timeline
- Entropy heatmap
- Latent-space explorer
- Quantum-state cloud

These help users understand underlying physics and cryptographic flows.

IX. Results and Discussion

A. Entropy Comparison

- Classical AES key: 6.5 bits/byte
- QGAN key: 7.8 bits/byte
- Processed hybrid key: 7.95 bits/byte

B. QKD Error Rate

With noise $p = 0.02$, QBER ≈ 0.021

C. Ciphertext Uniformity

Hybrid encryption produces highly uniform ciphertext distributions.

X. Conclusion

This work demonstrates a hybrid cryptographic system combining QGAN-based randomness, BB84-style QKD simulation, and AES-based hybrid encryption. While not relying on real quantum devices, it incorporates quantum-inspired transformations to enhance entropy and unpredictability. The system serves as an educational and research tool for understanding emerging quantum cryptography.

Future Work

- Integrate IBM Q real qubit backend
- Add PQC algorithms (CRYSTALS-Dilithium, Kyber)
- Hardware entropy measurement

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proc. IEEE ICC, 1984.
[2] I. Goodfellow et al., "Generative Adversarial Nets," NIPS, 2014.
[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press.
[4] J. Preskill, "Quantum Computing in the NISQ era," *Quantum*, 2018.
[5] NIST, "Advanced Encryption Standard (AES)," FIPS 197.