Quantum-Inspired GenAI Cryptography

Concepts & Architecture Overview · IIIT Dharwad ·

B Sreeshanth,
G Gokul,
M Navadeep,
G Sandeep.

Motivation: Securing Communication in the Post-Quantum Era

Why quantum-inspired cryptography matters for current systems

Quantum computers threaten **RSA** and **ECC**, breaking current confidentiality guarantees

Urgent need to protect integrity and trust as adversaries gain quantum access

Classical hardware cannot run full quantum protocols; solutions must be compatible with existing systems

Quantum-inspired cryptography leverages quantum principles to enhance security without full quantum infrastructure

Bridge current systems to post-quantum resilience while enabling practical deployment

Key Concepts in Quantum-Inspired Cryptography

Core components that boost resilience against classical and quantum adversaries

Quantum Generative Adversarial Networks (QGAN) — generate high-entropy keys for superior randomness

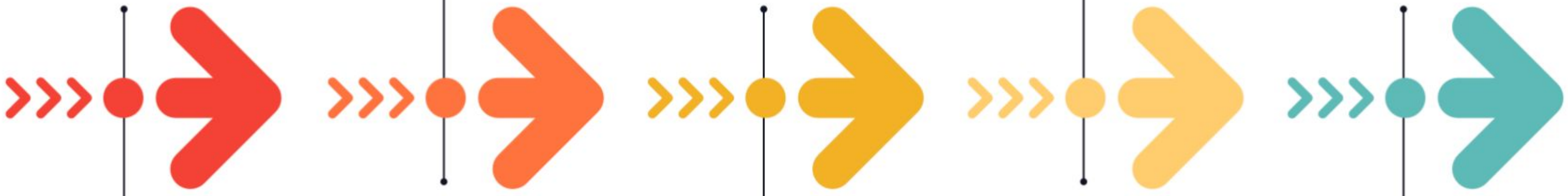
BB84 Quantum Key Distribution (QKD) — secure key exchange using quantum mechanics principles

Hybrid Encryption (AES-CFB + quantum preprocessing) — AES in Cipher Feedback mode enhanced by quantum-inspired preprocessing

Components integrate to increase **resilience** against classical and quantum adversaries

System Architecture Overview

Modular pipeline for quantum-inspired keying, secure exchange, hybrid encryption, key management, and visualization



QGAN Key Generator

Generates **quantum-inspired random keys** using a QGAN model

QKD Simulation

Models **secure quantum key exchange** for key agreement and testing

Hybrid Encryption

Applies **quantum preprocessing** then **AES-CFB** encryption for payloads

Secure Wallet

Stores and manages **keys and identities** with access controls

Interactive Visualization

Provides interactive views of **quantum states** and cryptographic operations

QGAN Key Generation Process & Advantages

Quantum-inspired rotations turn latent vectors into high-entropy AES keys, boosting unpredictability and resistance to cryptanalysis

- Input: latent vector fed into a **quantum-inspired rotation circuit**
- Circuit simulates **quantum transformations** via rotations and superposition-like mixing
- Measurement of outputs produces **highly entropic** data
- Derived data used as **AES keys**, preserving entropy for cryptographic use
- Advantage: greater **unpredictability and entropy** than classical PRGs
- Security impact: harder cryptanalysis and improved overall key robustness

BB84 Quantum Key Distribution Simulation

Stepwise flow from qubit exchange to error-corrected shared key; highlights sifting, noise estimation, and security basis

01

Qubit Preparation & Transmission

Alice encodes random bits in random bases and sends qubits to Bob over the channel

02

Random Basis Measurement

Bob measures each received qubit using randomly chosen bases independent of Alice

03

Sifting

Alice and Bob publicly compare bases and keep only bits measured in matching bases

04

Noise Estimation

They disclose a sample of sifted bits to estimate channel error rate and detect eavesdropping

05

Error Correction

Participants reconcile remaining key using error-correcting codes to ensure consistency

06

Privacy Amplification

Apply hashing to reduce any leaked information, yielding the final shared secret key

Hybrid Encryption Scheme

Quantum preprocessing + AES-CFB + post-quantum signatures for classical deployment

Rotation mixing preprocessing to increase diffusion

Noise injection preprocessing to harden against analysis

AES-CFB used as the conventional encryption mode

Post-quantum hashing for secure digital signatures

Layered approach: enhances diffusion and quantum resistance; suitable for near-term classical hardware

Wallet and Identity Management

Secure storage and reuse of identity–key bindings for encrypted messaging

01 **Store** identity names with associated **hexadecimal keys** securely

02 **Load** keys into memory for runtime cryptographic operations

03 **List** stored identities and their metadata for management

04 **Reuse** keys for encrypted messaging workflows

05 **Organize** identity–key bindings for distributed secure communications

Visualization Components

Interactive tools for teaching, debugging, and analyzing quantum-inspired cryptography

State & Structure

Rotating **qubit animations** illustrating quantum state behaviors for intuition and demo

Quantum **state cloud** mapping complex state spaces to reveal overlaps and trajectories

Encryption **pipeline diagram** explaining procedural flow and component interactions

Generative & Analytic

QGAN **latent-space explorer** to monitor key generation distributions and mode collapse

Entropy **heatmaps** highlighting randomness levels for key quality analysis and debugging

Value Delivered

Enhances **understanding**, supports **debugging**, and strengthens **education** on abstract quantum and cryptographic phenomena

Benefits and Applications

Security gains, research value, and future real-world impact

- Generates **high-entropy, unpredictable keys** to boost cryptographic strength
- Strengthens resistance to **classical statistical attacks**
- Serves as an **educational and research tool** linking quantum theory to applied cryptography
- Lays groundwork for **future real quantum implementations**
- Supports development of **post-quantum secure communication systems** resilient to emerging quantum threats

Thank you !