FLAGSHIP SYSTEM · QUANTUM SECURITY

FPGA-Based Quantum Key Distribution Controller

With Two-Level Encryption & the B92 Quantum Cryptography Protocol

As cyber threats evolve, traditional encryption is becoming vulnerable to advanced computational attacks. This system demonstrates next-generation secure communication using quantum cryptography principles combined with high-speed FPGA hardware.

WHY QUANTUM CRYPTOGRAPHY MATTERS TODAY

Industries moving toward quantum security.

Modern cybersecurity relies on mathematical encryption. Future quantum computers are expected to break many of the algorithms banking, defense, cloud computing, and digital communications depend on today. Quantum Key Distribution (QKD) introduces a new approach — where the laws of physics protect information instead of computational complexity.

01
Defense & Military Communication

02
Banking & Financial Security

03
Government Communication Networks

04
Data Centers & Cloud Infrastructure

05
IoT & Smart Devices

06
Healthcare Data Protection

07
Aerospace & Satellite Communication

WHAT MAKES THIS SYSTEM UNIQUE

FPGA + Quantum Cryptography + Dual Encryption

This platform bridges the gap between theoretical quantum cryptography and real-world secure communication hardware.

FPGA-Based Hardware Architecture

High-speed and reconfigurable FPGA implementation for real-time quantum communication control and signal processing.

B92 Quantum Key Distribution Protocol

Demonstrates secure quantum key exchange using non-orthogonal quantum states for highly secure communication.

Two-Level Encryption Security

An additional layer of data protection, integrating classical encryption with quantum key-based encryption.

Real-Time Secure Communication

Visual demonstration of secure key transmission, encryption, decryption, and unauthorized access detection.

Eavesdropping Detection Mechanism

Shows how quantum systems detect interception attempts through quantum state disturbance.

Educational & Research Friendly

Designed for academic institutions, quantum security laboratories, and advanced communication research.

QUANTUM PROPERTIES & SECURITY CONCEPTS DEMONSTRATED

From key generation to intrusion detection.

QUANTUM KEY DISTRIBUTION

- ✓ Secure generation and distribution of cryptographic keys
- ✓ Quantum-state-based communication security
- ✓ Randomized quantum key generation

B92 PROTOCOL DEMONSTRATION

- ✓ Non-orthogonal quantum state encoding
- ✓ Quantum-based secure communication principles
- ✓ Photon polarization-based key exchange

QUANTUM SECURITY VERIFICATION

- ✓ Detection of eavesdropping attempts
- ✓ Measurement disturbance effects
- ✓ Quantum state collapse during interception

TWO-LEVEL ENCRYPTION ARCHITECTURE

- ✓ Quantum-generated secure keys
- ✓ Additional classical encryption layer
- ✓ Enhanced data confidentiality and authentication

APPLICATIONS

Educational, research, and industrial relevance.

EDUCATIONAL

- ✓ Quantum Cryptography Labs
- ✓ FPGA & Embedded Training
- ✓ Communication Demos
- ✓ Cybersecurity Courses

RESEARCH

- ✓ Secure Comms Research
- ✓ Quantum Networking Studies
- ✓ FPGA System Development
- ✓ Quantum-Safe Encryption

INDUSTRIAL

- ✓ Defense Comm Systems
- ✓ Secure IoT Networks
- ✓ Government Data Security
- ✓ Banking Security Systems

DESIGNED FOR

Engineering Colleges & Universities
Quantum Technology Research Centers
Cybersecurity Laboratories
Embedded Systems Training Labs
Innovation & Incubation Centers
Defense Technology Research Programs

PREPARE FOR THE FUTURE OF SECURE COMMUNICATION

Build quantum-secure innovation today.

Quantum-safe communication is rapidly becoming one of the most important technologies of the future. Our FPGA-Based Quantum Key Distribution Controller provides the perfect platform for institutions and researchers to explore the next generation of secure communication systems.
