QUANTUM COMPUTING

UNIT 5

SYLLABUS

ADVANCED TOPICS AND CASE STUDIES IN QUANTUM CYBERSECURITY:

Advanced Protocols

5.1 Device-independent QKD.

5.2 Quantum zero-knowledge proofs.

Ethics, Policy, and Future Trends

5.3 Security risks of quantum supremacy.

5.4 Governance, regulation, and standardization.

5.5 Ethical concerns in quantum cyber warfare.

5.6 Case study on NSA’s Post-Quantum Cryptography (PQC) initiatives.

5.1 DEVICE-INDEPENDENT QKD.

- DI-QKD is a highly advanced form of QKD that provides security **without trusting the internal workings of the quantum devices used**.
- Security is derived purely from the violation of Bell inequalities.
- Traditional QKD protocols (BB84, E91) assume that devices behave ideally. Real-world devices may be faulty, hacked, or maliciously built. DI-QKD removes these assumptions.

KEY PRINCIPLES:

- Uses **Bell experiments** to test quantum correlations.
- If Bell inequality is violated → Systems are entangled → No hidden classical variables → Secure key is possible.
- Security is guaranteed **even when devices are treated as “black boxes**

ADVANTAGES:

Immunity against side-channel attacks.

Highest known theoretical security guarantees.

CHALLENGES:

Requires near-perfect detection efficiency.

Difficult to implement over long distances.

Low key generation rate.

APPLICATIONS:

Ultra-secure communications for military, intelligence, finance.

Future quantum internet backbone.

STEPS IN PROTOCOL

DI-QKD PROTOCOL

STEP1:Alice and Bob receive entangled photon pairs.

STEP2:They randomly choose measurement bases.

STEP3:They record outcomes and check correlations.

STEP4:They calculate the Bell parameter (CHSH inequality).

STEP5:If Bell inequality is significantly violated → Entanglement is genuine → Key is secure.

STEP6:They generate a raw key from correlated outcomes.

STEP7:Error correction + privacy amplification → Final secret key.

NOTES

5.2 QUANTUM ZERO-KNOWLEDGE PROOFS.

DEFINITION

A **zero-knowledge proof** allows one party (Prover) to convince another (Verifier) that a statement

is true **without revealing any other information**.

QZKPs extend this idea using quantum states, offering stronger security.

CORE IDEA

Uses properties like **no-cloning**, quantum entanglement, and measurement disturbance.

The verifier cannot copy or analyze the proof in unintended ways.

ADVANTAGES

Resistant to quantum attacks.

Supports secure authentication without revealing secrets.

Enables privacy-preserving quantum identity schemes.

Quantum Zero-Knowledge Proof is an interactive protocol between:

Prover (P) → has quantum computing capability

Verifier (V) → may be quantum or classical

The prover wants to prove a fact *without revealing the secret* or allowing any quantum attack to extract information.

Need OF Quantum Zero-knowledge Proofs?

Because in a quantum world:

- Verifiers may have quantum computers
- Attackers can use **quantum algorithms** (like amplitude amplification or swapping tests)
- Classical ZK techniques such as **rewinding** do *not* work (no-cloning theorem blocks it)

QZKPs solve these issues.

1. No-Cloning Theorem

The verifier cannot copy a quantum witness → ensures strong secrecy.

2. Quantum Rewinding

Classical simulation techniques fail.QZKPs use:

- *Watrous rewinding*
- *Quantum simulators*

3. Completeness

If the prover is honest, verifier always accepts.

4. Soundness

If the prover cheats, the verifier detects it with high probability.

5. Zero-Knowledge

Verifier learns **nothing** except “statement is true”.

EXAMPLE USE-CASES

- Anonymous quantum digital signatures
- Authentication in quantum networks
- Privacy-preserving blockchain (Quantum blockchain verification)
- Secure multi-party computation in the quantum setting
- Key Challenge:
- Building scalable quantum circuits that support practical QZKPs.

5.3 SECURITY RISKS OF QUANTUM SUPREMACY.

5.5 ETHICAL CONCERNS IN QUANTUM CYBER WARFARE.

5.4 GOVERNANCE, REGULATION, AND STANDARDIZATION

5.6 CASE STUDY ON NSA'S POST-QUANTUM CRYPTOGRAPHY (PQC) INITIATIVES.

://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards?utm_source=chatgpt.com