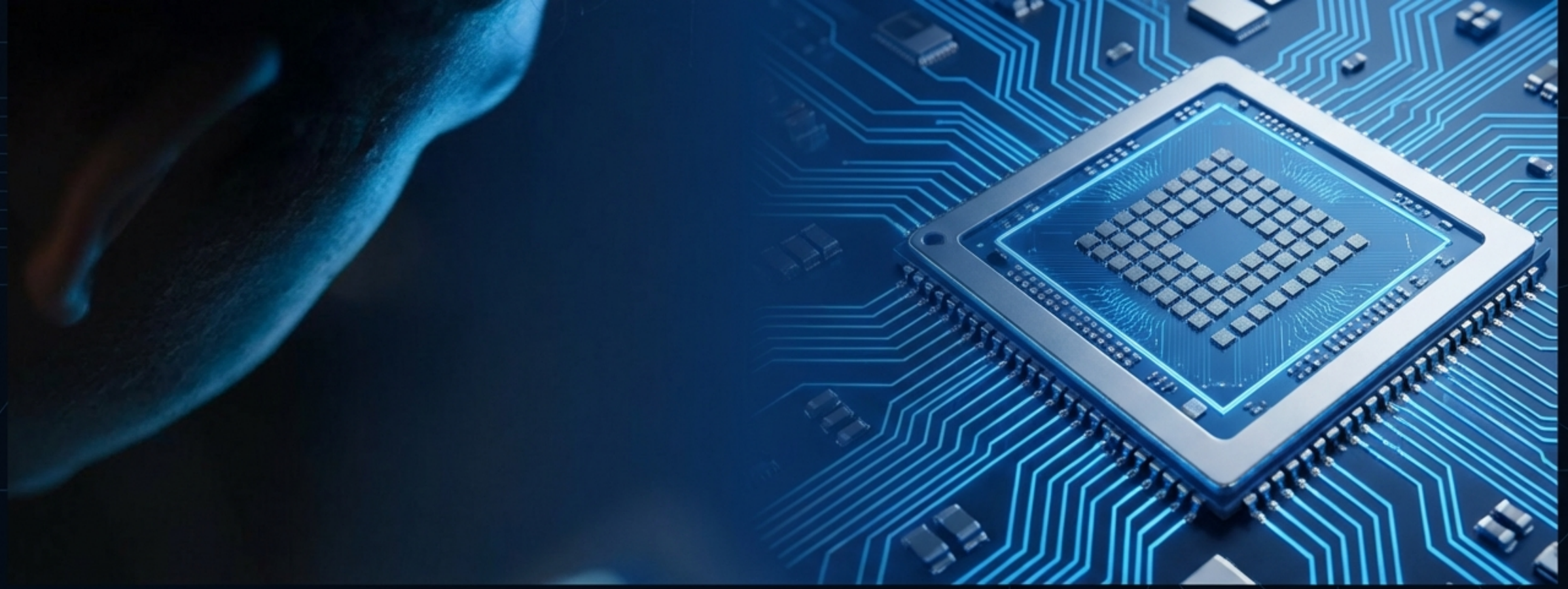


Foundations of Quantum Communication

From Computational Assumptions to Physical Security

EgQCC Presentation | Quantum Security Foundations

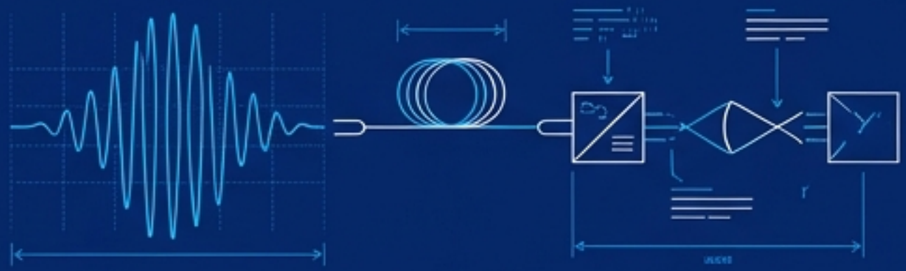
The Security Paradigm Shift

Computational Security

Classical systems (RSA, ECC, DH) rely on ‘computational hardness assumptions’. They assume mathematical factorisation problems are too hard to solve. Quantum computers threaten these widely deployed schemes.

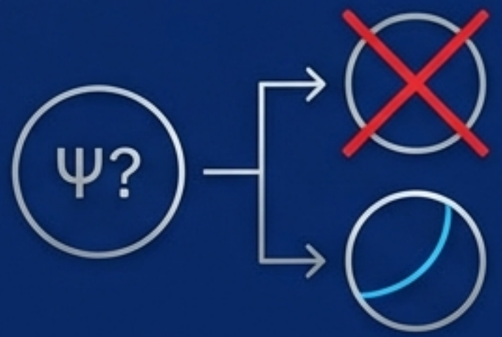
Physical Security

Quantum Communication offers ‘information-theoretic security’. Security is guaranteed by the fundamental laws of quantum mechanics, not by assumptions about computing power.



We are moving from security based on hard math to security based on hard physics.

Physics as the Ultimate Defence

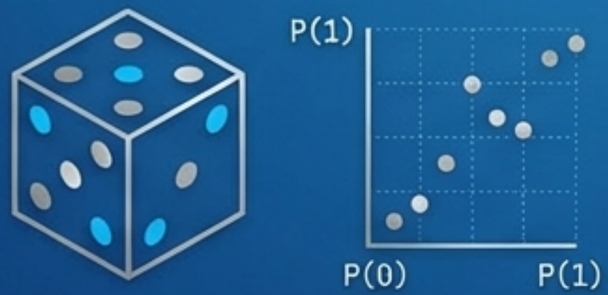


No-Cloning Theorem

It is physically impossible to create an identical copy of an arbitrary unknown quantum state.

Measurement Disturbance

Any measurement on an unknown state alters it, leaving a detectable trace.

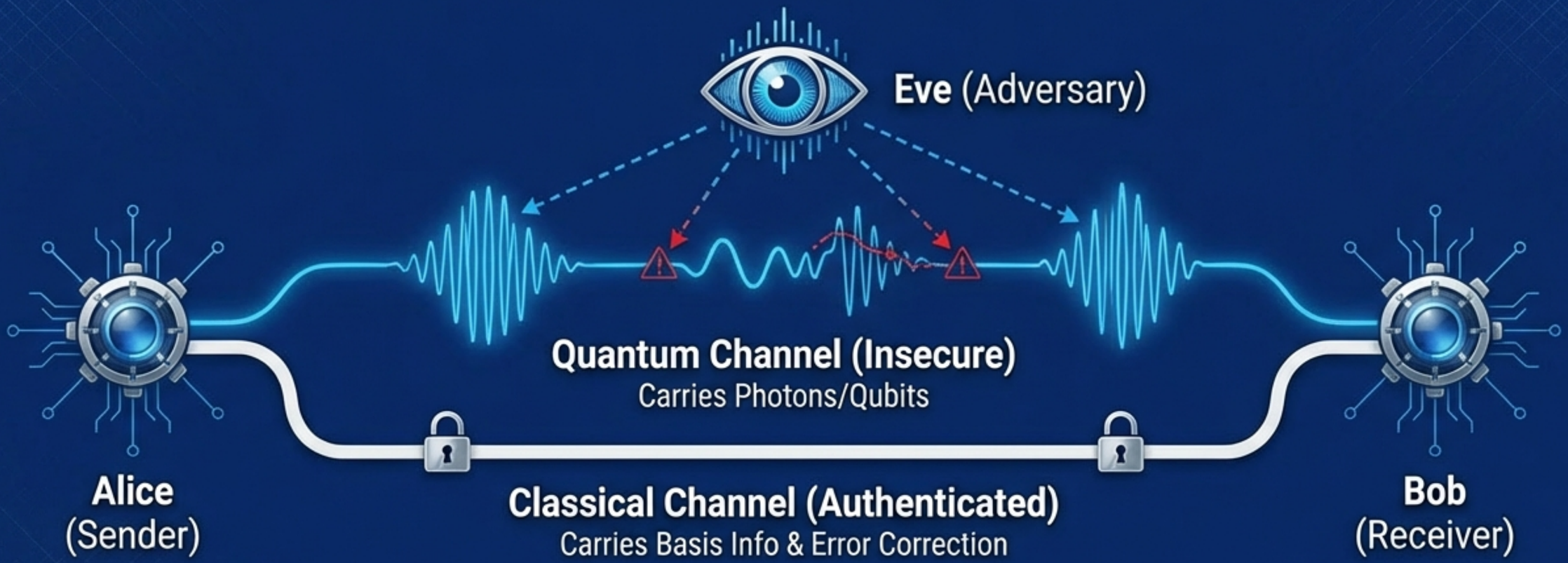


Intrinsic Randomness

Measurement outcomes are probabilistic, enabling true randomness.

Quantum security begins at the photon level. The hardware is the security.

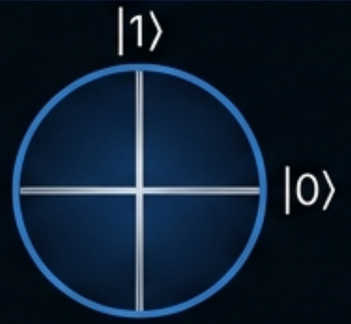
Quantum Key Distribution (QKD) Architecture



QKD allows two parties to establish a shared secret key. We assume Eve has unlimited computational power and full control over the channels, constrained only by the laws of physics.

The BB84 Protocol: Prepare and Measure

Mutually Unbiased Bases

Rectilinear Basis (+)	Diagonal Basis (x)
	

1. Preparation:

Alice selects random bits and random bases.

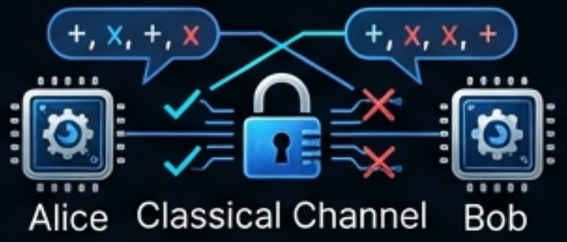
2. Transmission:

Alice sends photons encoded in these states.

3. Measurement:

Bob measures incoming photons using random bases.

4. Sifting:



Alice and Bob publicly compare bases. Matches are kept; mismatches are discarded.

The Tripwire: QBER and Intrusion Detection

- **The Mechanism:** If Eve intercepts and resends, she must guess the basis.
- **The Error:** She guesses wrong ~50% of the time, introducing a ~25% error rate into the signal.

- **The Error:** She guesses wrong ~50% of the time, introducing a ~25% error rate into the signal.
- **The Check:** Alice and Bob monitor the Quantum Bit Error Rate (QBER). If it exceeds the 11% threshold, they know Eve is listening.

$QBER_{measured}$

$QBER_{\_measured}$

= [1%] (noise)

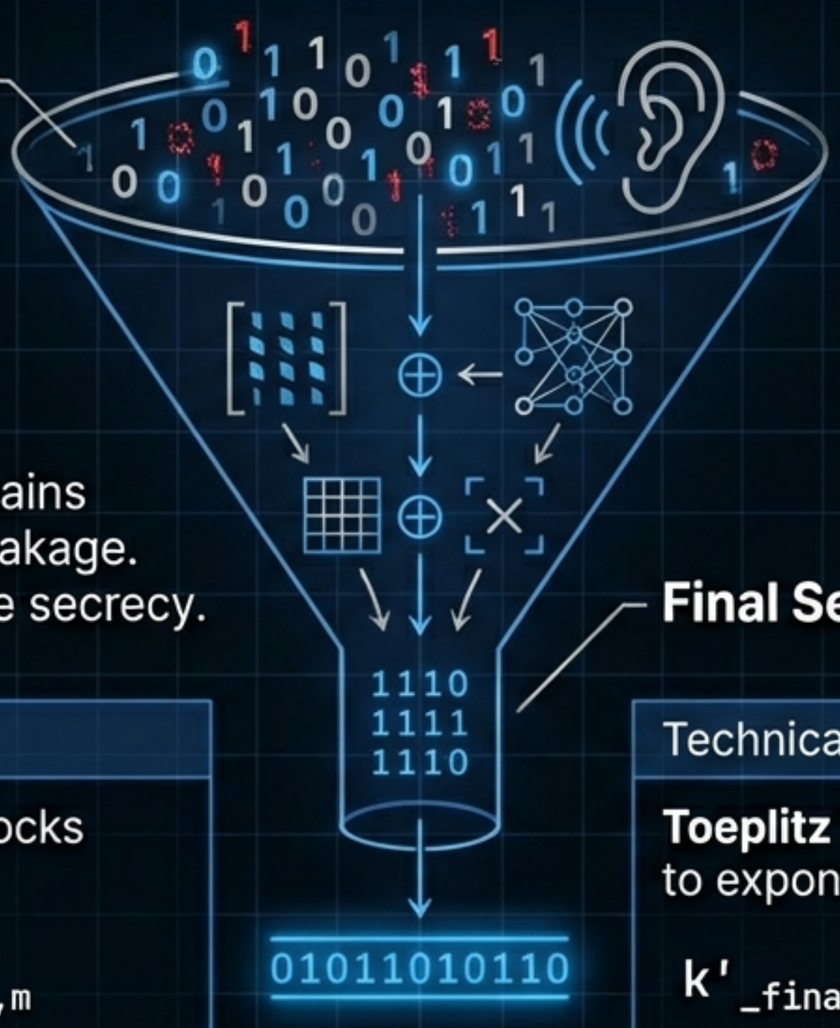
+ [25%] (Eve)

= [26%]

-> DETECTED

Distilling the Secret: Privacy Amplification

Raw Key
(Noisy, Potentially Leaked)



Even without Eve, the raw key contains noise and potential side-channel leakage. We must shrink the key to maximize secrecy.

Final Secret Key (Pure)

Technical Detail

Parity Checks: Dividing key into blocks and XORing to detect errors.

$$k'_i = k_{i,1} \oplus k_{i,2} \oplus \ldots \oplus k_{i,m}$$

Technical Detail

Toeplitz Matrices: Applying random matrices to exponentially reduce Eve's knowledge.

$$k'_{\text{final}} = T \cdot k_{\text{sifted}} \pmod 2$$

Engineering Realities and Limitations

Distance Limits

Signal loss in fibre optics limits transmission range without trusted repeaters.

Hardware Imperfections

Detectors have 'dark counts' (noise) and imperfect efficiency.

Key Rates

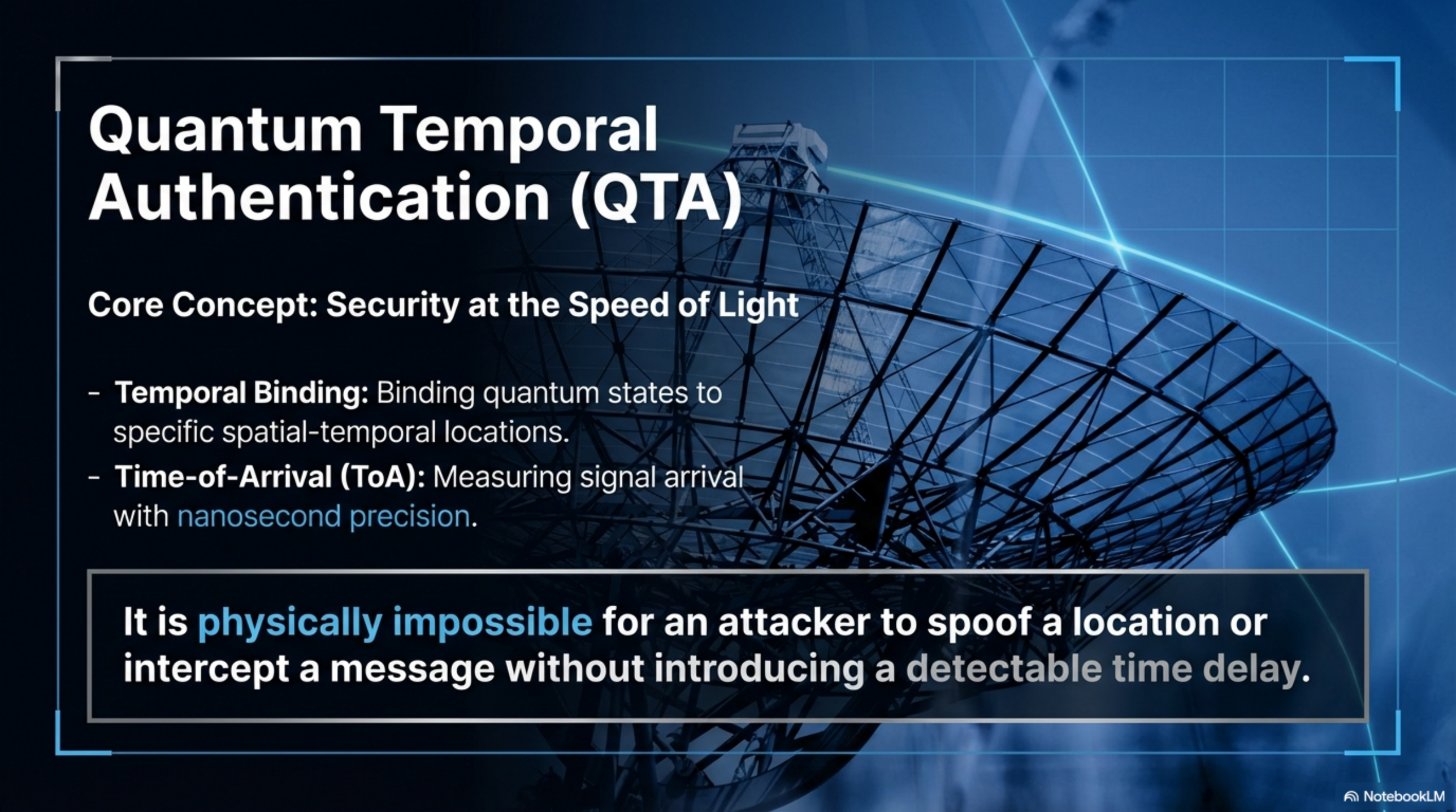
Finite key effects prevent instant high-volume key generation.

0111
010
100
1001

Authentication

The classical channel requires pre-authentication to prevent Man-in-the-Middle attacks.

Quantum Temporal Authentication (QTA)



Core Concept: Security at the Speed of Light

- **Temporal Binding:** Binding quantum states to specific spatial-temporal locations.
- **Time-of-Arrival (ToA):** Measuring signal arrival with nanosecond precision.

It is physically impossible for an attacker to spoof a location or intercept a message without introducing a detectable time delay.

Quantum Secure Direct Communication (QSDC)

Why exchange a key to encrypt a message if we can just send the message securely?

Definition:

Transmitting information directly over the quantum channel without prior key distribution.

No Key Management

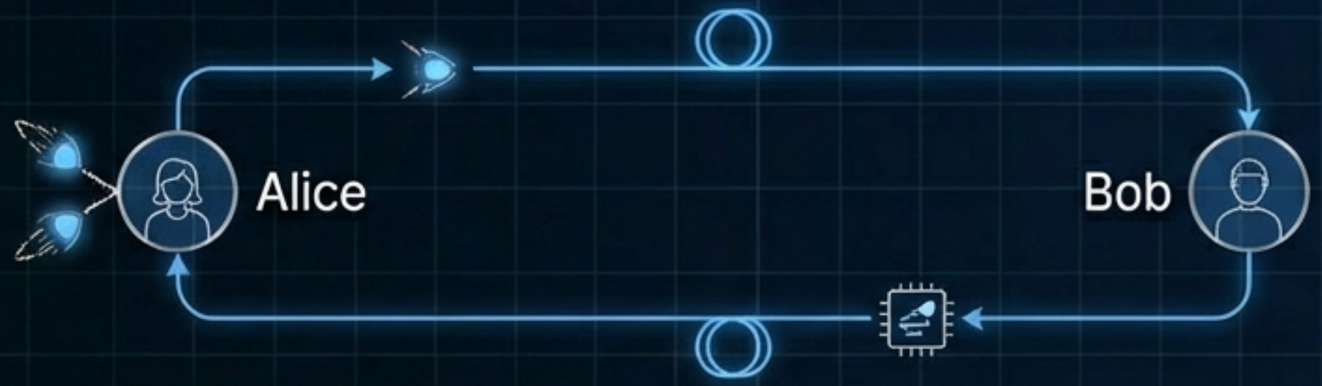
Forward Secrecy
(No stored keys to be decrypted later)

Efficiency
(Single protocol for transmission)

QSDC Protocols and Mechanics

Ping-Pong Protocol

Alice holds one qubit, sends one to Bob.



Bob encodes info by altering his qubit and sends it ‘back’ (Ping-Pong).

Two-Step Protocol

Phase 1: Check Security

(Send sequence to test for eavesdropping).

Phase 2: Direct Transmission

(Once channel is clear, encode message).

Current Throughput: 425–850 kbps.

Comparative Analysis: QKD vs. QSDC

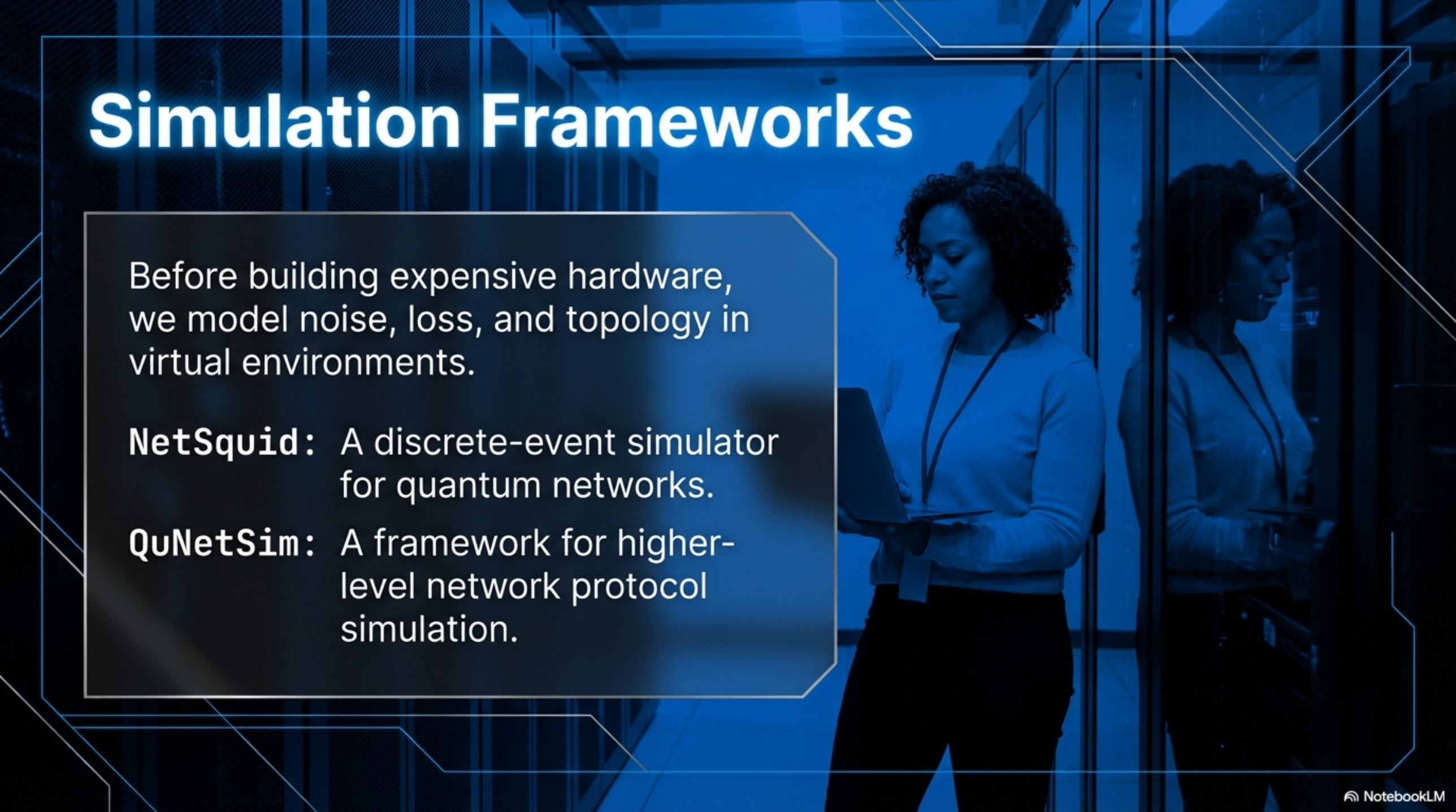
QKD (Quantum Key Distribution)	QSDC (Direct Communication)
Goal: Generate random keys.	**Goal:** Transmit actual data.
Requirement: Needs separate classical encryption for the message.	**Requirement:** No separate encryption step.
Storage: Requires secure key storage (O(n) memory).	**Storage:** Minimal (parameters only).
Workflow: Key Exchange -> Encryption -> Transmission.	**Workflow:** Check Channel -> Send Message.

Simulation Frameworks

Before building expensive hardware, we model noise, loss, and topology in virtual environments.

`NetSquid:` A discrete-event simulator for quantum networks.

`QuNetSim:` A framework for higher-level network protocol simulation.



The Future of Secure Communication

The Physical Layer is the ultimate frontier.
It is no longer just a pipe; it is the shield.

Sources & References

Primary Source:

EgQCC: Quantum Communication (QC) Foundations, Protocols, and Simulation Frameworks.

Key References:

- Bennett & Brassard (1984) - Quantum Cryptography: Public Key Distribution and Coin Tossing.
- Boström and Felbinger (2002) - Deterministic Secure Direct Communication using Entanglement (Ping-Pong Protocol).
- NetSquid & QuNetSim Technical Documentation.