QUANTUM INFORMATION THEORY FUNDAMENTALS

QUANTUM KEY DISTRIBUTION

Information-Theoretic Cryptographic Security

An executive technical overview of unconditionally secure key exchange mechanics.

1. THE CORE PARADIGM: BB84 MECHANICS

The BB84 protocol leverages the impossibility of perfectly distinguishing non-orthogonal quantum states without introducing irreversible perturbation.

State Encoding in Hilbert Space $\mathcal{H}_2$:

$$\begin{aligned} \text{Rectilinear Basis } (+) \quad &\rightarrow \quad |0_+\rangle = |0\rangle\,, \quad |1_+\rangle = |1\rangle \\ \text{Diagonal Basis } (\times) \quad &\rightarrow \quad |0_\times\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |1_\times\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{aligned}$$

Constant Overlap Vector: $|\langle i_+ | j_\times \rangle|^2 = \frac{1}{2} \quad \forall\, i, j \in \{0, 1\}$

- **Sifting Phase:** Alice and Bob publicly match encoding/measurement bases via a classical channel.
- **Key Filtering:** Non-matching basis indices are permanently discarded, yielding perfectly correlated raw outcomes where $\theta = \hat{\theta}$.

2. ENTANGLEMENT-BASED SECURITY (E91)

Instead of prepare-and-measure state streams, the **E91 Protocol** distributes maximally entangled Einstein-Podolsky-Rosen (EPR) pairs from a central source.

$$|\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

The CHSH Inequality Test: Security validation relies strictly on verifying non-local correlations. Any active eavesdropping collapses the global coherence, dropping the correlation parameter S from the quantum bound toward classical limits:

Local Realism Bound: $|S| \leq 2$ $\quad\longleftrightarrow\quad$ **Quantum Tsirelson Bound:** $\mathbf{|S| = 2\sqrt{2} \approx 2.828}$

3. INFORMATION-THEORETIC SECURITY BOUNDS

Under the Csiszár-Körner framework, the asymptotic secret key rate R represents the mathematical net information advantage Alice and Bob maintain relative to Eve:

$$R = I(A:B) - \min\{I(A:E), I(B:E)\}$$

Mapping this advantage against the **Quantum Bit Error Rate (QBER)**, denoted as D, defines the operational boundary for secure key distillation:

Mutual Information (Alice/Bob): $I(A:B) = 1 - H_2(D)$
Where $H_2(D) = -D\log_2 D - (1-D)\log_2(1-D)$ is the classical binary entropy function.

Holevo Bound (Eve's Information): $I(A:E) \leq H_2(D)$
Assuming optimal collective intercept attacks executed in a symmetric noise channel.

CRITICAL SECURITY BOUNDARY: $R \geq 1 - 2H_2(D) = 0 \implies \mathbf{D_{\text{threshold}} \approx 11.0\%}$
If the measured channel QBER exceeds 11%, the entire raw string must be aborted.

4. CLASSICAL POST-PROCESSING PIPELINE

1. **Information Reconciliation:** Interactive cascade protocols or Low-Density Parity-Check (LDPC) codes purge physical transmission discrepancies, leaking $f(D) \cdot H_2(D)$ bits.
2. **Privacy Amplification:** Universal 2-hash functions compress the reconciled key down to absolute security limits based on the **Quantum Leftover Hash Lemma**:

$$\ell = n\left[1 - H_2(D) - f(D)H_2(D)\right] - 2\log_2\left(\frac{1}{\varepsilon}\right)$$