Theoretical concept : BB84

1**) State Preparation via Control Hamiltonian**

Each qubit (photon polarization) is prepared as a rotation on the Bloch sphere driven by a control Hamiltonian

Hctrl=ħ /2 *(π. σ),

where σ = (**σ**x, **σ**y, **σ**z) and omega(Ω) determines rotation axis and rate.

The corresponding unitary is

$$U(\theta,\hat{n}) = \exp\left(-\frac{i}{\hbar}H_{\text{ctrl}}t\right) = \exp\left(-\frac{i\theta}{2}\,\hat{n}\cdot\boldsymbol{\sigma}\right), \qquad \theta = |\boldsymbol{\Omega}|t.$$

Choosing n cap = z cap yields the Z-basis I0>,I 1>.
Choosing n cap = x cap gives the X-basis |±) = (I0>) ± I1>))/√2.

These are mutually unbiased bases-measurement in one reveals no information about the other.

2 Environment / Eavesdropper Coupling and QBER

When the channel couples to an environment or an eavesdropper, we model the total Hamiltonian as

$$H = H_{\text{sys}} + H_{\text{env}} + H_{\text{int}}, \qquad H_{\text{int}} = g\,\sigma_{\hat{n}} \otimes B,$$

where **g** is coupling strength and **B** an environmental operator.
Tracing out the bath gives dephasing of the qubit density matrix:

Theoretical concept : BB84

$$\rho(t) = \begin{pmatrix} \rho_{00}(0) & \rho_{01}(0)\,\chi(t) \\ \rho_{10}(0)\,\chi^*(t) & \rho_{11}(0) \end{pmatrix}, \qquad \chi(t) = e^{-\Gamma t + i\phi(t)}.$$

The coherence factor $\chi(t)$ controls measurement errors.
The quantum bit error rate (QBER) for measurements in the conjugate basis is

QBER=(1-Re $\chi(t)$) /2

In the depolarizing-channel picture

$$\mathcal{E}(\rho) = (1-p)\rho + p\,I/2,$$

the QBER reduces to

QBER=p/2 p≈1-e^*y*t

Thus, decoherence (or Eve's interaction) directly raises QBER—physically equivalent to adding "energy" or entropy to the system

3 Intercept–Resend Attack → 25 % QBER

Eve randomly chooses a measurement basis.

Event	Probability
Eve guesses wrong basis	½
Bob (after sifting) uses Alice's correct basis	½

Theoretical concept : BB84

Bob's bit wrong when Eve guessed wrong	½

Hence the conditional QBER on the sifted key is:

QBER (intercept-resend)=½ * ½ = ¼ =25%

This fixed value is the unmistakable "fingerprint" of an intercept–resend eavesdropper.

4 Security Threshold

a secure key can be distilled if

QBER < 11%

Concept	Physical Interpretation	Observable Signature
Mutually unbiased bases	Orthogonal control Hamiltonians x cap,z cap)	Random outcomes if measured in wrong basis
No-cloning theorem	Measurement–induced collapse	Irrecoverable disturbance
Decoherence	Energy/entropy inflow from (**H***int*)	QBER ↑ with (\Gamma)
Intercept–resend	Effective projective coupling to Eve's basis	QBER ≈ 25 %
Security bound	Shor–Preskill limit	Abort if QBER > 11 %