Understanding BB84 and BBM92 Protocol

June 10, 2025

BB84 Protocol: Basic Overview

- Proposed in 1984, BB84 is a foundational Quantum Key Distribution (QKD) protocol.
- Goal: Securely generate and share a secret cryptographic key between two parties — Alice and Bob.
- **How it works:**
  - Alice prepares a random string of qubits in one of four states:

$$|0\rangle, |1\rangle, |+\rangle, |-\rangle$$

  - Alice sends these qubits to Bob over a quantum channel.
  - Bob randomly chooses to measure each qubit in either:
    - Standard basis: $|0\rangle, |1\rangle$
    - Hadamard basis: $|+\rangle, |-\rangle$
  - Bob publicly announces which basis he used for each measurement.
  - Alice tells Bob which measurements used the matching basis.
  - Only qubits measured in matching bases are kept; the rest are discarded.
- On average, Bob's basis matches Alice's basis 50% of the time.
- Retained qubits form the raw key, which should be identical for both.

BB84 Protocol: Key Verification

- To verify correctness and detect eavesdropping:
  - Bob selects a random subset of the raw key (verification string).
  - Bob publicly announces the measurement results and positions of these qubits.
  - Alice compares with her own bits.
- If the error rate exceeds a tolerable threshold, the key is discarded — potential eavesdropping detected.
- Otherwise, Alice and Bob share a perfectly symmetric, random, and unconditionally secure quantum key.

BBM92 Protocol: Basic Overview

- BBM92 is an **entanglement-based** QKD protocol proposed in 1992.
- Uses pairs of entangled particles called EPR pairs, shared between Alice and Bob.
- **Protocol steps:**
  - Alice generates EPR pairs and sends one particle from each pair to Bob.
  - Bob randomly measures each incoming particle in either:
    - Standard (Z) basis
    - Hadamard (X) basis
  - Alice publicly reveals the basis she used for each particle.
  - Bob discards measurements done in the wrong basis, keeping only the rest (the sifted key).
  - **On average, bases match with probability $\frac{1}{2}$.**
  - Alice and Bob publicly compare a subset of remaining bits to estimate the error rate.
  - They apply reconciliation and privacy amplification to distill a secure secret key.

Security and Significance of BBM92

- Security comes from **quantum entanglement**:
  - Any eavesdropping attempt disturbs the entanglement, detectable as errors.
  - Cloning entangled particles is impossible (no-cloning theorem), so attacks are detected.
- Ensures unconditional security under ideal conditions.
- The entanglement link provides intrinsic correlation for generating a shared secret key.
- Widely studied and forms the basis for many modern entanglement-based QKD implementations.

QBER Formula

Quantum Bit Error Rate (BB84)

$$e_{84} = \frac{c \cdot p_{\text{signal}} + \frac{1}{2}(p_{\text{dark}} + p_{\text{straycounts}})}{p_{\text{click}}}$$

- Estimates the fraction of detected bits that are erroneous.
- Includes both signal-based and noise-based contributions to error.

Term Definitions

- c: Intrinsic error rate (e.g., imperfect preparation, polarization drift, basis mismatch).
- p_{signal}: Probability of photon detection originating from Alice.
- p_{dark}: Probability of detection due to internal detector noise.
- $p_{\text{straycounts}}$: Probability of detection due to external photons (environmental).
- p_{click}: Overall probability of any detection:

$$p_{\text{click}} = p_{\text{signal}} + p_{\text{dark}} + p_{\text{straycounts}}$$

Why Do Errors Happen in QKD?

- **Signal Error (c):**
  - Decoherence of quantum states in fiber.
  - Misalignment between Alice's and Bob's polarization bases.
  - Imperfect detectors or waveplates.
- **Dark Counts (p_{dark}):**
  - Thermal noise or spontaneous electron emission inside detector.
  - Unrelated to any incoming signal.
- **Stray Counts ($p_{\text{straycounts}}$):**
  - Ambient light leakage (daylight, moonlight).
  - Reflected photons from atmosphere or surroundings.
  - More dominant in free-space QKD.

Contribution from Valid Signal

$$\text{Signal Error} = c \cdot p_{\text{signal}}$$

- Even valid photons may be incorrectly measured.
- c is typically a small number (1–2%).
- Models inherent system imperfections.

Contribution from Noise Sources

$$\text{Noise Error} = \frac{1}{2}(p_{\text{dark}} + p_{\text{straycounts}})$$

- These events are uncorrelated with Alice's signal.
- Bob assigns a random bit $\rightarrow$ 50% chance of error.
- Noise dominates when p_{signal} is weak (e.g., over long distance or in bad weather).

Normalization by p_{click}

Interpretation

$$e_{84} = \frac{\text{Errors from signal and noise}}{\text{Total detection events}}$$

- p_{click} ensures QBER reflects actual error rate *among observed events*.
- Allows accurate estimation of key loss due to noise and imperfections.

Signal Detection Probability in QKD

Formula:

$$p_{\text{signal}} = 1 - \exp(-\eta_d \eta_T \mu)$$

Where:

- η_d = Detector efficiency
- η_T = Channel transmittance efficiency
- μ = Average number of photons per pulse

Physical Meaning:

- Models the probability that Bob detects at least one photon from Alice.
- The term $\exp(-\eta_d \eta_T \mu)$ is the probability of *zero* detections.

Photon emission is Poisson-distributed:

$$P(n) = \frac{\mu^n e^{-\mu}}{n!}, \quad P(0) = e^{-\mu}$$

After transmission and detection losses:

$$\lambda = \eta_d \eta_T \mu$$

$$P(0 \text{ photons detected}) = e^{-\lambda} = e^{-\eta_d \eta_T \mu}$$

Thus,

$$p_{\text{signal}} = 1 - \exp(-\eta_d \eta_T \mu)$$

Intuition: Detection = "at least one photon survives and is detected."

Dark Count Probability in QKD

Formulas:

$$p_{\text{dark}} = 4d \qquad d = D \cdot t_w$$

Where:

- D = Dark count rate (counts per second per detector)
- t_w = Detection time window (in seconds)
- d = Probability of a dark count in one detector during one window
- p_{dark} = Total dark count probability across 4 detectors

Intuition Behind Dark Count Formula

Why does this happen?

- Detectors can click even without a photon—due to thermal noise or electronics.
- These are called **dark counts** and occur randomly.

Explanation of Terms:

- $d = D \cdot t_w$: probability that one detector fires during a time window.
- $4d$: there are 4 detectors in BB84's passive detection module (2 bases $\times$ 2 outcomes).

Impact:

- When p_{signal} is low (due to high loss or low μ), p_{dark} becomes significant.

- This increases the QBER because dark count detections are random $\Rightarrow$ 50% error chance.

Why Stray Photons Matter in QKD

- QKD detectors cannot distinguish between photons sent by Alice and **stray photons** (environmental noise).
- Stray photons cause **false detections**, increasing the **Quantum Bit Error Rate (QBER)**.
- Managing stray photons is crucial to maintain secure key rates.

Stray Photons in Uplink (Ground $\rightarrow$ Satellite) at Night

- Background photons mainly come from sunlight reflected by the Moon and Earth:

$$\text{Sun} \rightarrow \text{Moon} \rightarrow \text{Earth} \rightarrow \text{Telescope}$$

- Number of stray photons entering the detector:

$$N_{\text{up, night}} = A_E A_M R_M^2 \frac{a^2 \Omega_{\text{fov}}}{d_{EM}^2} \cdot B_f \cdot \Delta t \cdot H_{\text{sun}}$$

Parameter significance:

- H_{sun}: Solar brightness — sets total background light level
- A_M, A_E: Reflectivity (albedo) — how much light the Moon and Earth reflect
- a: Telescope radius — larger aperture collects more photons
- Ω_{fov}: Field of view — wider FOV lets in more background light
- B_f: Filter bandwidth — wider bandwidth lets in more wavelengths (more noise)
- Δt: Detection time window — longer window accumulates more stray photons

Stray Photon Detection Probability (Uplink)

$$p_{\text{straycounts}} = \eta_d \cdot N_{\text{up, night}}$$

- η_d: Detector efficiency — probability to register an incoming stray photon.
- Stray photons increase **false click rate**, raising QBER.

Stray Photons in Downlink (Satellite $\rightarrow$ Ground)

- Background photons depend on sky brightness H_b, affected by moon phase, weather, city lights.
- Background power at telescope:

$$P_b = H_b \cdot \Omega_{\text{fov}} \cdot \pi a^2 \cdot B_f$$

- Convert to photon counts in time window Δt:

$$N_{\text{down}} = \frac{P_b}{h\nu} \cdot \Delta t = \frac{H_b}{h\nu} \cdot \Omega_{\text{fov}} \cdot \pi a^2 \cdot B_f \cdot \Delta t$$

Where:

- $h\nu$: photon energy (Planck constant $\times$ frequency)

Stray Photon Detection Probability (Downlink)

$$p_{\text{straycounts}} = \eta_d \cdot N_{\text{down}}$$

- Increased background brightness or wider FOV increases stray photon noise.
- This directly affects QBER and the security of the key.

Summary: Controlling Stray Photons

- **Minimize Field of View** (Ω_{fov}): narrower FOV reduces background light.
- **Use narrow spectral filters** (B_f): blocks out-of-band light.
- **Optimize detection window** (Δt): short window limits noise accumulation.
- **Improve detector efficiency** (η_d) carefully — more efficiency means more signal but also more stray photon detection.

Proper balance ensures secure QKD operation with low QBER.

QBER for BBM92 Protocol: Overview

- QBER depends on:
  - Losses in the quantum channel (fiber, free-space)
  - Detector quality (efficiency, noise)
  - Environmental noise and stray photons
- Define combined channel and detector efficiency:

$$\alpha_L = \eta_{\text{det}} \times \eta_T$$

  where

  - η_{det}: Detector efficiency (probability detector clicks if photon arrives)
  - η_T: Channel transmittance (fraction of photons reaching detector)

Coincidence Probability Breakdown

The total coincidence probability at Bob's side:

$$p_{\text{coin}} = p_{\text{true}} + p_{\text{false}} + p_{\text{straycounts}}$$

- p_{true}: Probability of detecting genuine entangled photon pairs.
- p_{false}: Probability of false coincidences caused by detector noise and accidental detections.
- $p_{\text{straycounts}}$: Probability of counts caused by stray environmental photons (e.g., background light).

True Coincidence Probability

$$p_{\text{true}} = \alpha_x \times \alpha_{L-x} = \eta_{\text{det}} \times \alpha_L$$

- Represents the chance both entangled photons successfully reach and are detected by Alice and Bob.
- Depends on channel loss on each path (α_x, α_{L-x}).
- Detector efficiency η_{det} accounts for imperfect photon detection.
- True coincidences carry useful quantum information.

False Coincidence Probability: Physical Origins

$$p_{\text{false}} = 4\alpha_x d + 4\alpha_{L-x} d + 16d^2$$

where d is the dark count probability per detector.

- **Dark Counts:** False detections caused by thermal noise or electronics in detectors.
- **Accidental Coincidences:** Random overlaps of independent dark counts or noise events.
- Terms explained:
  - $4\alpha_x d$: One genuine photon at Alice's side coincides with a dark count at Bob's detectors.
  - $4\alpha_{L-x} d$: One genuine photon at Bob's side coincides with a dark count at Alice's detectors.
  - $16d^2$: Both detections are dark counts occurring simultaneously by chance.
- False coincidences introduce errors because they do not carry entangled photon information.

Why Does Source Position Affect False Coincidences?

- α_x and α_{L-x} depend on distance losses — placing the source closer to one party reduces their channel loss but increases it for the other.
- p_{false} depends on these efficiencies multiplied by dark count probabilities.
- Minimizing false coincidences means balancing the losses:

$$\text{Optimal source position: } x = \frac{L}{2}$$

- At halfway, losses are balanced, minimizing false coincidence probability:

$$p_{\text{false}} = 8\alpha_{L/2}d + 16d^2$$

QBER Formula for BBM92

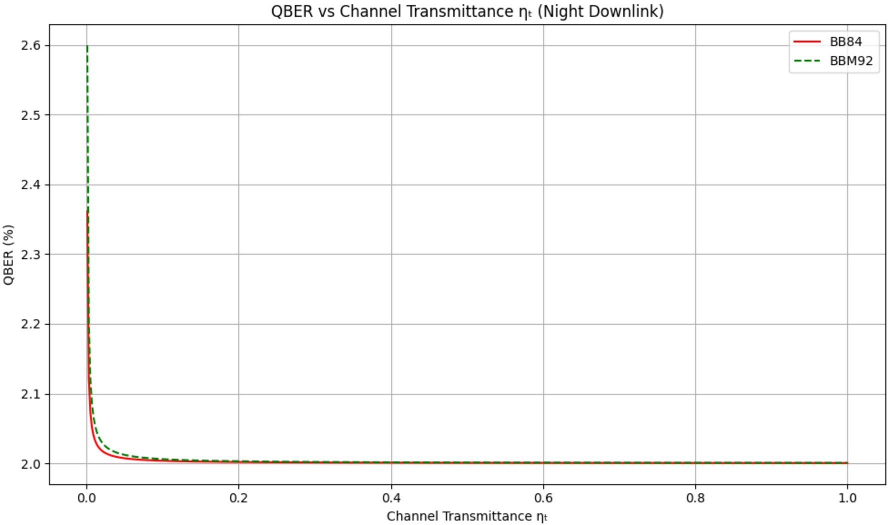
$$e_{\text{BBM92}} = \frac{c \cdot p_{\text{true}} + \frac{1}{2}(p_{\text{false}} + p_{\text{straycounts}})}{p_{\text{coin}}}$$

- c: intrinsic error rate from imperfect entanglement or alignment errors.
- p_{true} errors contribute fully (scaled by c).
- False and stray counts are random and cause errors with 50% probability (random bit values).
- Numerator = total error contribution.
- Denominator = total detected coincidences (signal + noise).

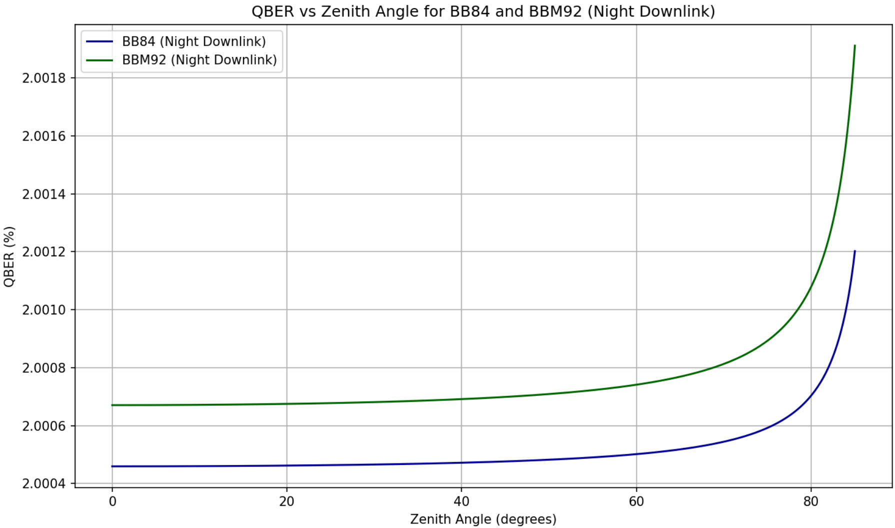
Summary: Physical Significance

- **True coincidences** are desired events carrying secure quantum info.
- **False coincidences** arise from detector noise and accidental overlaps:
  - Detector dark counts cause fake clicks.
  - Imbalance in source placement changes how losses affect noise.
- **Stray photons** add environmental noise, increasing error rates.
- Minimizing false and stray counts is crucial for low QBER and secure key generation.

Graph of QBER with transmittance



Graph of QBER with zenith angle



Conclusion from QBER Graphs

- **QBER vs Channel Transmittance η_t:**
  - QBER for both BB84 and BBM92 decreases rapidly as transmittance increases.
  - At high η_t, both protocols asymptotically approach a minimum QBER close to the intrinsic error (around 2%).
  - BB84 and BBM92 show nearly identical performance at higher transmittance levels.
- **QBER vs Zenith Angle:**
  - As zenith angle increases (i.e., link becomes more oblique), QBER increases for both protocols.
  - BBM92 shows slightly higher QBER than BB84 across all zenith angles.
  - The steep increase in QBER at high zenith angles is due to increased atmospheric attenuation and background noise.

Conclusion: BB84 vs BBM92

- In theory, **BB84 and BBM92 are equivalent** in ideal conditions — same QBER and SKR.
- In practice, BBM92 uses **entangled photon pairs**, which are:
  - More sensitive to **channel loss** and **timing jitter**.
  - Affected by **coincidence detection inefficiency** and **multi-photon noise**.
- BB84, based on **single-photon preparation**, is more robust in lossy and noisy environments.
- In the simulated night-time downlink:
  - BBM92 shows slightly higher QBER due to degraded entanglement fidelity.
  - BB84 maintains marginally lower QBER across zenith angles and transmittance.
- **Conclusion:** BB84 performs marginally better under realistic conditions with noise and attenuation.

Secure Key Rate for BB84 and Parameters

The secure key rate under photon number splitting (PNS) attack for BB84:

$$R_{BB84} = \frac{1}{2} p_{\text{click}} \left[(1 - \tau') + f(e_{84}) \left(e_{84} \log_2(e_{84}) + (1 - e_{84}) \log_2(1 - e_{84}) \right) \right]$$

Key Parameters:

- p_{click}: Total probability of detector clicks (signal + noise).
- e_{84}: Quantum Bit Error Rate (QBER).
- $f(e_{84})$: **Error correction inefficiency factor.**
  - Accounts for the *extra* bits revealed during classical error correction beyond the Shannon limit.
  - Typical values: 1.15–1.22, meaning actual error correction leaks 15–22% more information than ideal.
- τ': Effective privacy amplification term, quantifying bits to discard for security.

This formula accounts for sifting, error correction, and privacy amplification.

Privacy Amplification Term τ'

$$\tau' = \tau\left(\frac{e_{84}}{\beta}\right)$$

$$\tau(e) = \begin{cases} \log_2(1 + 4e - 4e^2), & \text{if } e < \frac{1}{2} \\ 1, & \text{if } e \geq \frac{1}{2} \end{cases}$$

Origin of the τ formula:

- Derived from information-theoretic security bounds on Eve's maximum knowledge.
- The term inside the logarithm estimates Eve's guessing probability based on error rate.
- For $e \geq 0.5$, the key is considered insecure; all bits must be discarded.

Privacy Amplification Term τ'

Why bits are discarded in privacy amplification:

- To eliminate any partial information Eve might have about the key.
- Privacy amplification shortens the raw key, sacrificing bits for unconditional security.
- The function $\tau'(e)$ sets how many bits must be removed based on effective error rate and security parameter.

Security Parameter β

$$\beta = \frac{p_{\text{click}} - p'}{p_{\text{click}}}$$

- β is the fraction of detection events considered secure (not vulnerable to multiphoton attacks).
- p' is the probability of insecure multiphoton pulses that an eavesdropper could exploit.
- Bits corresponding to insecure multiphoton pulses must be discarded or treated carefully to maintain security.
- Therefore, β reduces the effective error rate used in privacy amplification, reflecting the realistic secure fraction of the key.

Why bits are discarded due to β:

- Multiphoton pulses can leak information to Eve without detection.
- To be conservative, bits from these insecure pulses are excluded from the final key.
- This ensures only detections from single-photon (secure) pulses contribute to the final secure key.

Insecurity from Multiphoton Pulses

The term p' accounts for multi-photon pulses:

$$p' = 1 - \left(1 + \mu + \frac{\mu^2}{2} + \frac{\mu^3}{12}\right) e^{-\mu}$$

Where:

- μ: mean photon number per pulse.
- This models the probability of pulses with ≥ 4 photons.

Significance of pulses with ≥ 4 photons:

- In weak coherent sources, photon number follows a Poisson distribution.
- Multiphoton pulses are vulnerable to Photon Number Splitting (PNS) attacks.
- Pulses with 4 or more photons provide Eve multiple copies, increasing information leakage risk.
- Including these pulses in p' offers a conservative estimate of insecure pulses.
- Bits from such pulses must be discarded or treated cautiously to maintain security.

Summary

- The key rate R_{BB84} combines detection, error correction, and security bounds.
- Multiphoton pulses are considered insecure due to vulnerability to PNS attacks.
- Privacy amplification compensates for leaked information, quantified by τ'.
- Error correction leakage is accounted for by $f(e)$.
- The goal is to maximize secure key generation while bounding Eve's knowledge.

BBM92 Key Rate under Double Blinding Attack

The secure key rate is given by:

$$R_{BBM92} = \frac{p_{\text{coin}}}{2} \left\{ \tau(e_{M92}) + f(e_{M92}) \left[e_{M92} \log_2(e_{M92}) + (1 - e_{M92}) \log_2(1 - e_{M92}) \right] \right\}$$

- p_{coin}: Coincidence probability (both detectors click simultaneously).
- $\frac{1}{2}$: Basis sifting factor — only matched basis outcomes count.
- $\tau(e_{M92})$: Privacy amplification term.
- $f(e_{M92})$: Error correction inefficiency factor.
- e_{M92}: Quantum Bit Error Rate (QBER).

Privacy Amplification Term $\tau(e_{M92})$

- Quantifies bits that must be discarded to eliminate Eve's partial knowledge.
- Depends on measured QBER e_{M92}.
- Under **double blinding attack**, Eve's presence is undetectable:

$$\tau(e_{M92}) = 0$$

- No bits are discarded for privacy amplification — security is compromised.

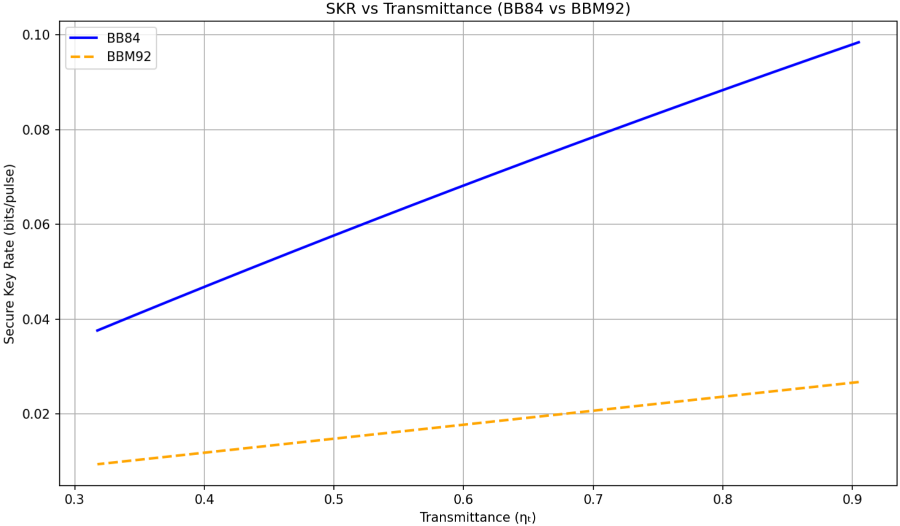
Error Correction and QBER Terms

- $f(e_{M92})$: Efficiency factor accounting for overhead in practical error correction.
- $e_{M92}\log_2(e_{M92}) + (1 - e_{M92})\log_2(1 - e_{M92})$: Shannon entropy of error distribution.
- Represents the fraction of bits lost during error correction.
- Overall, this term reduces the key rate due to noise/errors.

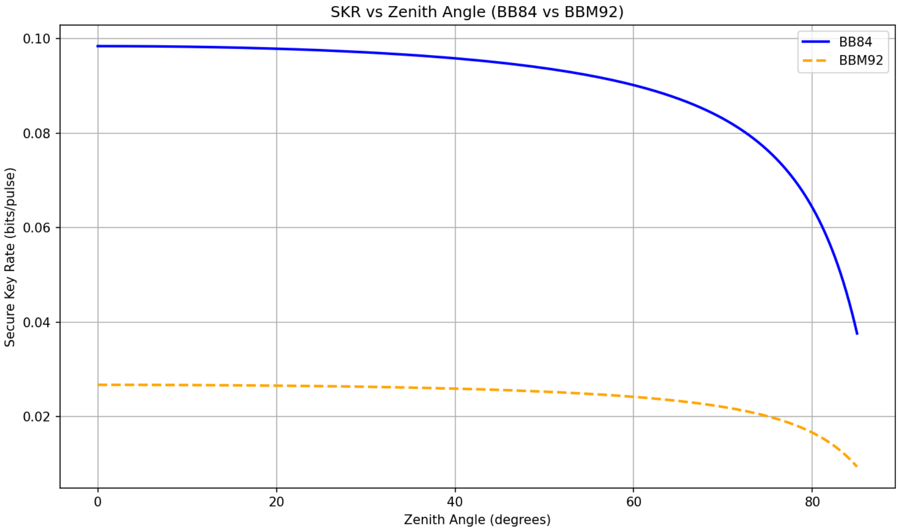
Summary and Security Implications

- The formula combines raw detection rates and bits lost to error correction and privacy amplification.
- Double blinding attack leads to $\tau = 0$, meaning Eve's presence is invisible.
- No privacy amplification means Eve can potentially know the entire key.
- Security of BBM92 is severely compromised under such an attack.

Graph of SKR with transmittance



Graph of SKR with zenith angle



Conclusion from SKR Graphs

- **SKR vs Transmittance:**
  - BB84 shows significantly higher secure key rate than BBM92 across all values of channel transmittance η_t.
  - SKR for both protocols increases with transmittance, but BB84 scales more efficiently.
- **SKR vs Zenith Angle:**
  - As zenith angle increases (i.e., more atmospheric attenuation), SKR for both protocols decreases.
  - BB84 consistently outperforms BBM92, especially at lower zenith angles.
  - SKR for BBM92 drops more sharply near high zenith angles.
- **Overall:** BB84 achieves higher secure key rates than BBM92 for the same channel conditions.

Conclusion: BB84 vs BBM92 (Key Rate Perspective)

- Although both protocols are theoretically secure, their **practical efficiency** differs.
- BBM92 is based on **coincidence detection of entangled photon pairs**, which results in:
  - Lower raw detection rates due to photon-pair splitting.
  - More susceptibility to background noise and timing errors.
  - Sifting factor of 1/2 further reduces SKR.
- BB84 benefits from:
  - Direct single-photon detection with higher transmission probability.
  - Lower overhead in detection and post-processing.
- **Conclusion:** BB84 provides a higher SKR than BBM92 in realistic conditions, especially under free-space loss.

BB84 Protocol over FSO Channel

Introduction to FSO-QKD

- **Free-Space Optical (FSO) QKD** uses open-air or satellite links instead of optical fibers.
- Although many QKD protocols have been implemented over optical fiber, the achievable distance is limited to a few hundred kilometers due to exponential fiber loss.
- In contrast, FSO channels (both terrestrial and satellite) allow global-scale secure quantum communication.
- FSO QKD overcomes the distance limitation of fiber-based QKD, making it suitable for long-distance quantum communication.
- However, the main challenge for FSO-QKD is **atmospheric losses**, such as turbulence, scattering, and absorption.
- **Protocols discussed**:
  - BB84 (Prepare-and-measure)
  - BBM92 (Entanglement-based)

Free-Space Losses in QKD

- **Geometric Losses**: Due to beam spreading between transmitter and receiver.
  - Expressed as:
$$\left(\frac{d_r}{d_t + DL}\right)^2$$
  - Where d_r, d_t: diameters of receiver/transmitter apertures
    D: beam divergence (mrad), L: channel length (m).
- **Atmospheric Losses**: Due to absorption and scattering in the atmosphere.
  - Modeled using Beer-Lambert Law:
$$\tau = \exp(-\alpha L)$$
  - α: atmospheric attenuation coefficient (in dB/km)

Total Free-Space Transmittance

Combined Loss Formula

$$T = \left(\frac{d_r}{d_t + DL} \right)^2 \exp(-\alpha L)$$

- Combines both geometric and atmospheric attenuation.
- **Interpretation**:
  - At short range (e.g., lab): geometric loss dominates.
  - At long range (e.g., ground-satellite): exponential atmospheric loss dominates.

BB84 QBER Formula:

Quantum Bit Error Rate (QBER):

$$Q = P_{\text{opt}} + \frac{\beta \cdot P_{\text{nc}} \cdot n}{T\eta q\mu}$$

Parameter Explanations:

- P_{opt}: Probability of incorrect detections due to imperfect polarization contrast or interference (e.g., optical misalignment).
- P_{nc}: Probability of noise counts — includes detector dark counts and background light from the environment.
- β: Protocol-dependent factor.
  - For BB84: $\beta = \frac{1}{2}$
  - For six-state protocol: $\beta = \frac{2}{3}$
- n: Number of detectors (typically 4 for BB84).
- T: Total channel transmittance (geometric $\times$ atmospheric).

BB84 QBER Formula:

Remaining Parameters:

- η: Detector quantum efficiency (typical value: 0.6–0.7).
- q: Correction factor due to non-interfering basis combinations; $q = 0.5$ for BB84.
- μ: Mean photon number; $\mu = 1$ for single-photon sources.

Interpretation:

- As the transmittance T decreases (i.e., under higher loss), the noise term becomes dominant and QBER increases.
- High QBER means less secure key bits. A typical security threshold for BB84 is $Q < 11\%$.
- Optimizing all these parameters is critical to achieving secure key generation in FSO links.

BB84 Secret Key Rate (SKR)

Secret Key Rate Formula:

$$S_{\mathrm{BB84}} = \frac{1}{2}\nu_s T \left[1 + 2Q\log_2 Q + 2(1-Q)\log_2(1-Q)\right]$$

Parameters:

- ν_s: Heralded single-photon count rate at the sender's side.
    - For this study: $\nu_s = 0.64 \times 10^6$ counts per second per mW (from SPDC source brightness).
- T: Channel transmittance (includes geometric and atmospheric loss).
- Q: QBER, affects the binary entropy and hence the extractable key.

Key Points:

- The SKR decreases sharply as QBER increases due to increased redundancy from error correction.
- High transmittance and low QBER maximize SKR.

Impact of Detector Efficiency and Noise on BB84 Performance

Observation from QBER and SKR analysis for BB84:

- Detector efficiency values analyzed: $\eta = 0.4,\ 0.6,\ 0.8$
- Noise count probabilities considered: $P_{nc} = 10^{-5},\ 10^{-4},\ 10^{-3}$
- Fixed parameters: $q = 0.5$, $\mu = 1$, $P_{\text{opt}} = 0.001$, $\nu_S = 0.64 \times 10^6$ cps, $n = 4$

Key Results for BB84:

- **Threshold QBER:** 11%
- **Noise Tolerance:** BB84 tolerates up to **33 dB channel loss** at $\eta = 0.4$.
- **Trends:**
  - Increasing $\eta \Rightarrow$ reduces QBER and extends secure distance.
  - Decreasing $P_{nc} \Rightarrow$ reduces background-induced errors.
  - SKR remains high under low loss, but drops sharply near the QBER threshold.
- **Inference:** Use **high-efficiency, low-noise detectors** to support longer secure communication distances in BB84-based FSO QKD.

BBM92 Protocol over FSO Channel

Two-Photon Interference and Visibility in BBM92

Entangled photon quality is characterized by:

- **Visibility in polarization bases:**

$$V_{\text{tot}} = \frac{V_{HV} + V_{\pm 45}}{2}$$

- V_{HV}: visibility in the horizontal/vertical (rectilinear) basis
- $V_{\pm 45}$: visibility in the diagonal basis
- **Intrinsic QBER due to source imperfection:**

$$q_i = \frac{1 - V_{\text{tot}}}{2}$$

- High-quality entangled sources yield $V_{\text{tot}} \to 1$ and hence $q_i \to 0$

Physical meaning:

- Visibility measures how strongly the detection outcomes are correlated.
- Any deviation from perfect correlation indicates decoherence, loss, or experimental error.
- q_i sets the lower bound of error even in ideal conditions (without Eve).

Coincidence Rate and Signal Detection in BBM92

Coincidence rate r_c:

- Number of simultaneous photon detections at Alice and Bob's detectors.
- Dependent on:
  - Source rate: $r_1 = r_2 = \nu_s$
  - Detector efficiency: η
  - Collection efficiency into fibers: η_c
- Modeled as:

$$r_c = \eta^2 \eta_c^2 r_1$$

Signal coincidence rate (raw key rate):

$$r_{\text{sig}} = \frac{1}{2} r_c T$$

- Represents valid, correlated detections from entangled pairs.
- The factor $1/2$ arises from basis matching probability.

Accidental Coincidence Rate in BBM92

Accidental coincidence rate r_a:

- Results from false coincidences — not from entangled pairs.
- Caused by dark counts and external background (e.g., stray light).
- **Source at Alice's side:**

$$r_a = \frac{1}{2}(r_1 - Tr_c)(r_{\text{bg}} + T(r_2 - r_c))\tau_c$$

- **Source in the middle (both arms exposed):**

$$r_a = \frac{1}{2}(r_{\text{bg}} + T(r_1 - r_c))(r_{\text{bg}} + T(r_2 - r_c))\tau_c$$

Parameters:

- $r_{\text{bg}} = P_{nc} \cdot r_1$: background count rate
- $\tau_c = 2$ ns: coincidence timing window

Impact: Accidental coincidences increase QBER and reduce key generation rate. Positioning the source in the middle increases their contribution.

BBM92 QBER Formula and Interpretation

Total QBER:

$$Q = \frac{1}{r_{\text{sig}} + r_a} \left(q_i r_{\text{sig}} + \frac{1}{2} r_a \right)$$

Interpretation:

- First term: QBER contribution from source imperfections (via q_i)
- Second term: QBER contribution from accidental coincidences
- When accidental rate r_a is large (due to high P_{nc}), QBER increases sharply
- Entanglement-breaking by eavesdropper also manifests as a QBER rise
- Source in the middle increases accidental coincidences in both arms

BBM92 Secret Key Rate (SKR)

Formula:

$$S_{\text{BBM92}} = \frac{1}{2}\nu_s T\left[1 - f(Q)h_2(Q) - h_2(Q)\right]$$

Where:

- ν_s: photon pair rate from the source (e.g., 0.64×10^6 cps)
- $f(Q)$: bidirectional error correction efficiency
- $h_2(Q) = -Q\log_2 Q - (1-Q)\log_2(1-Q)$: binary entropy function

Insight:

- SKR decreases as QBER increases.
- BBM92 tolerates up to $\sim 11\%$ QBER at threshold.
- Best performance with low QBER, high η, and low P_{nc}.

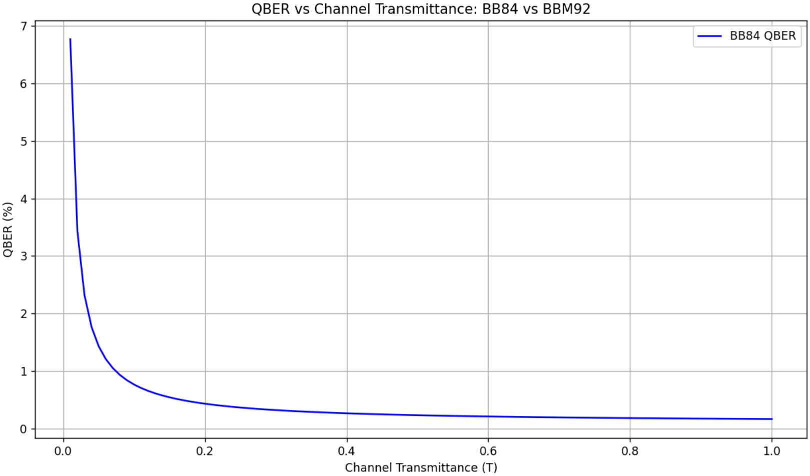
Effect of Source Placement in BBM92

- **Case 1: Source at Alice's side**
  - Only Bob's channel faces losses and noise.
  - Lower QBER, better performance.
- **Case 2: Source in the middle**
  - Both arms face free-space losses and noise.
  - QBER increases significantly.
- Detector noise and background impact are effectively **doubled**.

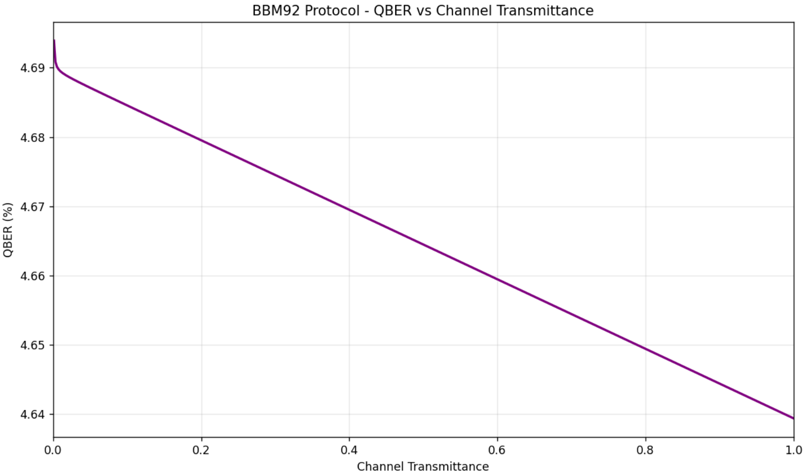
Recommendation: For long-distance FSO-QKD, prefer source placement strategies that minimize exposure to background noise and loss on both arms.

Note: We have used Case - 2 for plotting the graphs.

Graph of QBER with transmittance for BB84 protocol

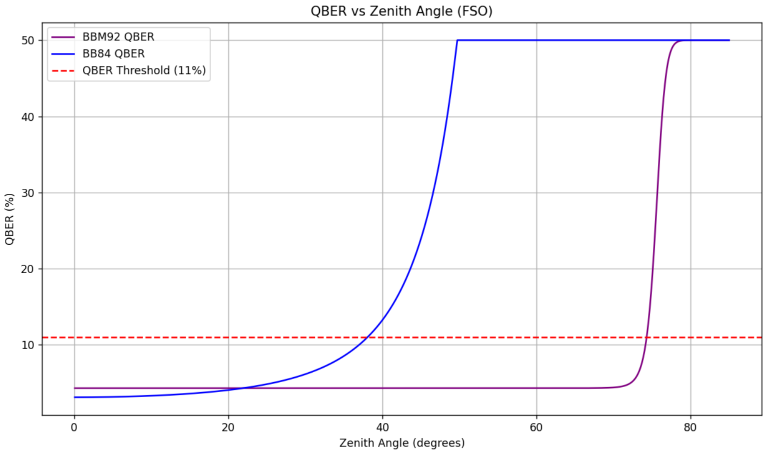


Graph of QBER with transmittance for BBM92 protocol



QBER vs Transmittance :BB84 and BBM92

QBER vs Zenith Angle :BB84 and BBM92



QBER Trends for BB84 and BBM92 over FSO

Observation Summary:

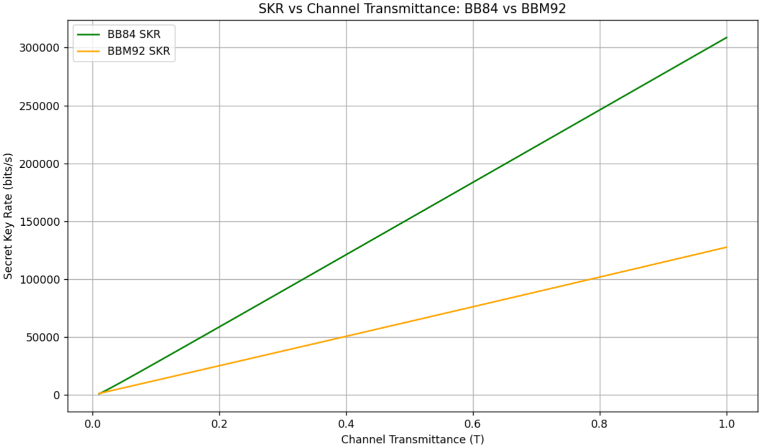
- **Transmittance Graph:**
  - QBER is high at low transmittance due to noise; drops rapidly with increasing T and stabilizes.
  - BB84 shows lower QBER than BBM92 across all T.
  - Secure region: $T > 0.04$ (approx) where $QBER < 11\%$.
- **Zenith Angle Graph:**
  - QBER increases steeply with zenith angle due to atmospheric losses.
  - BB84 becomes insecure ($QBER > 11\%$) beyond 42°, while BBM92 remains below threshold until 78°.
  - BBM92 is more robust against atmospheric path length increase than BB84 in this setting.

Interpretation

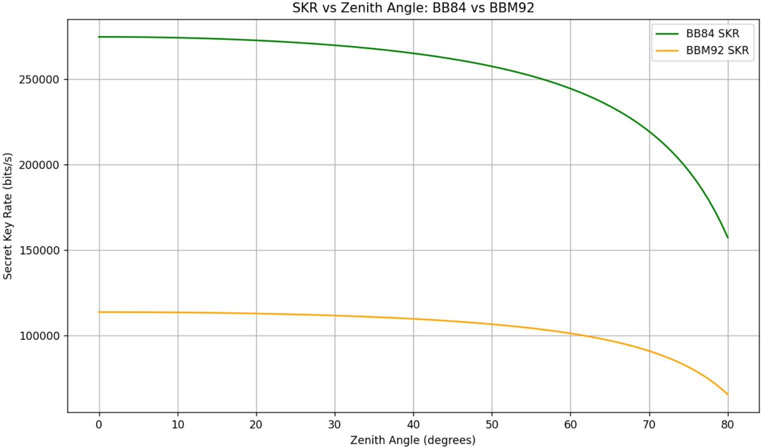
Underlying Physics and Security Implications:

- At low transmittance or high zenith angles, signal photons are attenuated, and dark counts dominate, increasing QBER.
- BB84 and BBM92 respond differently to noise and losses based on their protocol design.
- The QBER threshold (11%) is a critical boundary for secure key generation — defined by privacy amplification limits.
- **FSO performance:**
  - BB84 is more efficient at lower zenith angles or higher transmittance.
  - BBM92 tolerates higher zenith angles due to entanglement-based resilience but has slightly higher QBER at optimal conditions.
- Overall, protocol selection for FSO QKD depends on operating conditions (e.g., elevation, noise, distance).

SKR vs Transmittance :BB84 and BBM92



SKR vs Zenith Angle :BB84 and BBM92



Conclusion from SKR Graphs (BB84 vs BBM92 over FSO)

- **SKR vs Channel Transmittance:**
  - Secure key rate (SKR) increases approximately **linearly** with transmittance T for both BB84 and BBM92.
  - This is because SKR $\propto T$ when QBER is nearly constant and other factors (e.g., dark counts, multi-photon noise) are small.
  - BB84 consistently outperforms BBM92, achieving over twice the SKR across all T values.
- **SKR vs Zenith Angle:**
  - SKR drops as zenith angle increases, due to rising atmospheric losses.
  - BB84 remains significantly more robust under angular degradation.
- **Summary:** In free-space optical links, BB84 provides higher and more stable key rates across all transmittance and angular ranges.

Conclusion: BB84 vs BBM92 in FSO Channels

- The SKR for both BB84 and BBM92 scales approximately as:

$$\text{SKR} \propto T \times (1 - h(Q)) \quad \text{when QBER } Q \approx \text{constant}$$

- Since QBER is low and stable in the FSO case, SKR becomes a **linear function of transmittance**.
- **BB84 is more efficient because:**
  - It uses single-photon detection (not coincidences).
  - Has a higher raw detection probability.
  - Lower sifting loss (no need for pairwise correlations).
- **BBM92 limitations:**
  - Entanglement-based, requiring photon-pair coincidences.
  - Coincidence probability scales as T^2, but sifting and post-selection reduce it further.
- **Conclusion:** BB84 achieves a better SKR slope and higher overall key rates in realistic FSO links due to lower loss and greater detection efficiency.

BB84 Protocol over Optical Fiber

QKD over Optical Fibre

- Optical fibre is the most practical channel due to telecom infrastructure.
- Decoy-state BB84 helps detect photon number splitting (PNS) attacks in weak coherent pulse sources.
- Goal: Minimize Quantum Bit Error Rate (QBER) and maximize Secure Key Rate (SKR).

Decoy-State BB84 Protocol

- Alice randomly chooses basis (Z/X) and bit (0/1), encodes using weak coherent pulses.
- Uses multiple intensities: signal (e.g., $\mu = 0.5$), decoy (e.g., $\nu = 0.1$), vacuum.
- Bob randomly chooses basis and measures incoming photon.
- Only events where bases match contribute to sifted key.
- Decoy states allow estimation of single-photon events.

Experimental Parameters

- Wavelength: 1550 nm
- Clock rate: 1 GHz, Pulse flux: $\sim$0.5 photons/pulse
- Detection efficiency: $\eta_{\text{Bob}} = 0.2$
- Dark count probability: P_d
- Temporal filtering: gate width $\sim$ 100 ps
- Fibre loss: $\sim$ 0.2 dB/km

Quantum Bit Error Rate (QBER) - Formula

QBER measures the error rate in the sifted key. It is defined as:

Basic QBER Formula:

$$e = e_{\text{intrinsic}} + e_{\text{noise}}$$

Where:

- $e_{\text{intrinsic}} = e_{\text{opt}} + \frac{1}{2} P_{\text{a}}$
- e_{noise}: error from dark counts and Raman noise

Typical values:

- $e_{\text{intrinsic}} \approx e_{\text{opt}} + 0.5 \cdot P_{\text{a}} \approx 2.8\%$
- e_{opt}: due to phase errors, modulation imperfections
- $P_{\text{a}} \approx 0.01$: detector afterpulse probability

Interpretation:

- $e_{\text{intrinsic}}$ is independent of distance.
- e_{noise} increases with distance as signal weakens and noise becomes dominant.

QBER Noise Term e_{noise} Explanation

Noise Error Model:

$$e_{\text{noise}} = \frac{1}{2} \cdot \frac{P_d + P_R(L)}{\mu e^{-\alpha L}\eta_{\text{Bob}} + P_d + P_R(L)}$$

Parameter details:

- P_d: dark count probability per gate. For 500 cps and 1 GHz clock:

$$P_d = \frac{500}{10^9} = 5 \times 10^{-7}$$

- $P_R(L)$: Raman-scattered photon probability per gate.
  - Increases with fibre length due to scattering from classical data channels.
  - Modeled from measured Raman coefficients (see paper Appendix C).
- μ: mean photon number per pulse (e.g., 0.5 for signal states)
- α: fibre attenuation (e.g., 0.2 dB/km)
- η_{Bob}: detector efficiency at Bob (e.g., 0.2)

Secure Key Rate (SKR) - Formula

Based on Koashi's proof and decoy-state estimation:

$$R = \frac{1}{t}\left[Q_1(1 - H(e_1)) - Qf_{\mathrm{EC}}(e)H(e) + Q_0\right]$$

Where:

- R: secure key rate (bits per unit time)
- t: time duration of the key session
- Q_1: gain of single-photon states
- e_1: error rate of single-photon states
- Q: total gain (i.e., fraction of pulses where a detection occurs)
- $f_{\mathrm{EC}}(e)$: error correction efficiency factor (≈ 1.1)
- Q_0: contribution from vacuum states (usually small)

Secure Key Rate (SKR) - Term Significance

Explanation of Terms:

- Q_1: Estimated from decoy-state protocol. Represents the secure contribution.
- $H(e) = -e \log_2 e - (1-e) \log_2(1-e)$: binary Shannon entropy.
- $f_{\text{EC}}(e)$: Accounts for inefficiency in practical error correction.
- Q_0: Zero-photon (vacuum) contribution. Important in decoy analysis.

Dependence on Distance (L):

- Q_1 and Q decrease with L due to fibre attenuation: $e^{-\alpha L}$
- e_1 increases with L due to higher QBER
- $R \to 0$ beyond a certain distance (QBER threshold exceeded)

Note: Optimal μ, f_{EC}, and decoy intensities are crucial for maximizing R.

Fibre Transmittance and Noise

- Fibre transmittance:

$$T = 10^{-\alpha L/10}, \quad \text{where } \alpha = 0.2 \text{ dB/km}$$

- Noise sources:
  - Dark counts: P_d
  - Raman photons: $P_R(L)$ (from bidirectional data channels)

Results

- Secure key rate:
  - 935 kbps over 35 km
  - 507 kbps over 50 km
  - 7.6 kbps over 90 km
- QBER increases with length:
  - $\sim$3% at $<$ 50 km
  - $\sim$8% at 90 km
  - No key beyond 100 km due to QBER $>$10%

Conclusion

- Decoy-state BB84 over fibre enables long-distance QKD with high bit rates.
- Key challenges:
  - Fibre attenuation
  - Raman noise from classical channels
- Filtering and power control are critical for noise mitigation.
- Practical deployment possible in metropolitan networks.

BBM92 Protocol over Optical Fiber

Quantum Bit Error Rate (QBER)

QBER quantifies the fraction of incorrect bits in the raw key:

$$\text{QBER} = \frac{R_{\text{opt, err}} + R_{\text{acc, err}}}{R_{\text{key, raw}}}$$

- $R_{\text{opt, err}} = \frac{1}{2} R_{\text{coin}} \cdot p_o$ — error rate due to imperfections in the optical setup, where p_o is the intrinsic bit-flip probability from misalignment, drift, or source noise.
- $R_{\text{acc, err}} = \frac{1}{4} R_{\text{acc}}$ — error rate from accidental coincidences (random or dark-count-induced events), with only half yielding bits and half of those being incorrect.
- $R_{\text{key, raw}}$ — raw key rate after basis sifting.

Note: A low QBER ensures high fidelity of the entangled state and the security of the BBM92 protocol.

Raw Key Rate (Post-sifting)

Raw key rate is the number of bits retained after basis sifting (but before error correction):

$$R_{\text{key, raw}} = \frac{1}{2} R_{\text{coin}}$$

- The factor $\frac{1}{2}$ accounts for sifting — only the events where Alice and Bob choose the same basis are kept.
- $R_{\text{coin}} = R_{\text{coin, pairs}} + R_{\text{acc}}$ is the total coincidence rate:
  - $R_{\text{coin, pairs}}$: True coincidences from entangled pairs.
  - R_{acc}: Accidental coincidences (e.g., noise or unrelated detections).
- $R_{\text{coin, pairs}} = B\eta_A \eta_B \eta_D^2 \eta_{\text{dt},A} \eta_{\text{dt},B} \eta_r$

Secure Key Rate

$$R_{\text{key, sec}} = R_{\text{key, raw}} \left[1 - 2.1 H(\text{QBER})\right]$$
$$H(x) = -x \log_2 x - (1 - x) \log_2 (1 - x)$$

- $H(x)$: Binary Shannon entropy
- 2.1: Efficiency factor for finite-key error correction

Parameter Definitions

- B: Pair emission rate (brightness)
- η_A, η_B: Link efficiencies
- η_D: Detector quantum efficiency
- $\eta_{\text{dt},i}$: Efficiency due to dead time:

$$\eta_{\text{dt},i} = \frac{1}{1 + (B\eta_i\eta_D + D_i)t_d/n_d}$$

- D_i: Dark counts per second at party i

Parameter Definitions

- t_c: Coincidence window — time interval in which a detection at Alice and Bob is considered a valid coincidence.
- t_r: Detection resolution (FWHM) — combined timing uncertainty from detector jitter, dispersion, and photon coherence time.
- η_r: Coincidence timing efficiency:

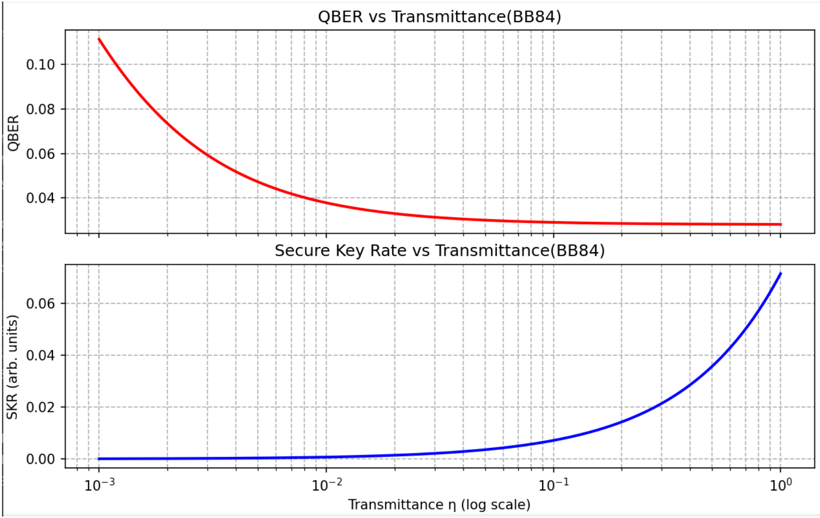
$$\eta_r = \text{erf}\left(\sqrt{\ln(2)} \cdot \frac{t_c}{t_r}\right)$$

  Approaches 1 when $t_c \gg t_r$ (i.e., negligible jitter).
- S_A, S_B: Singles count rates at Alice and Bob — total photon detection rate (signal + noise) at each side.
- $P_{\text{acc},t_c} \approx (1 - e^{-S_A t_c})(1 - e^{-S_B t_c})$: Probability that an accidental coincidence occurs within t_c.
- $R_{\text{acc}} = \frac{P_{\text{acc},t_c}}{t_c}$: Accidental coincidence rate — uncorrelated detection events falsely appearing as coincidences.

Experiment Parameters from Paper

- Visibility: 94%
- Wavelength: 810 nm, Bandwidth: 3 nm
- $B = 1.5 \times 10^6$ cps
- $\eta_D = 0.6$, $t_r = 1600$ ps
- Dark counts: Alice = 500 cps, Bob = 1800 cps
- Link Loss: 12 dB (both)
- Detector Dead Time: 45 ns

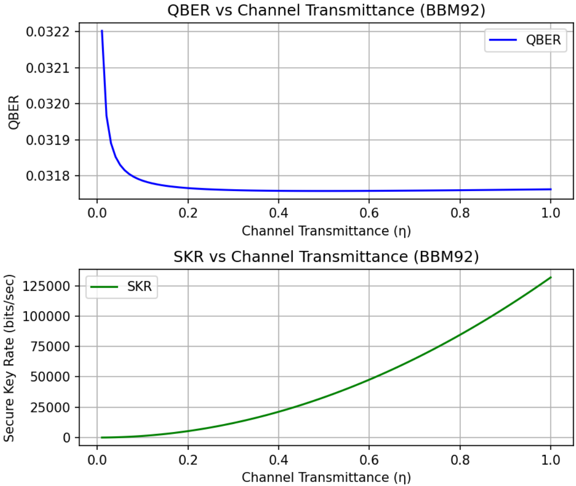
Graph of QBER and SKR with transmittance for BB84 protocol



BB84 Protocol Observations

- QBER decreases significantly with increasing transmittance
- SKR remains low at low transmittance, improves only at high values
- QBER increases sharply with zenith angle, showing sensitivity to misalignment and atmospheric effects
- More affected by detector inefficiencies and channel imperfections
- Best suited for stable, high-quality optical links such as fiber

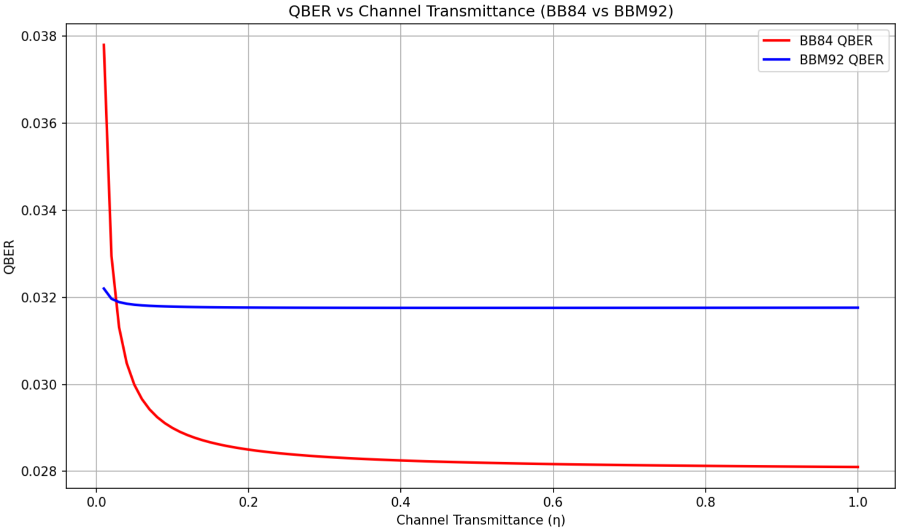
Graph of QBER and SKR with transmittance for BBM92 protocol



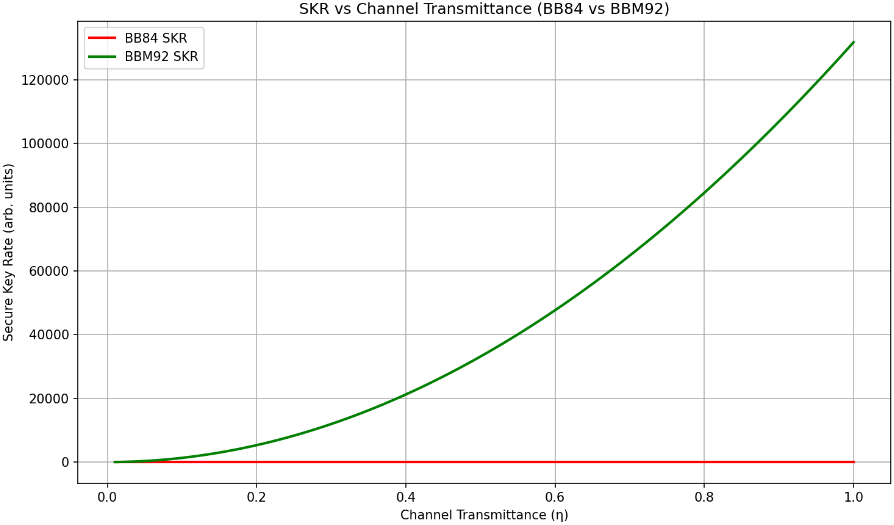
BBM92 Protocol Observations

- QBER remains nearly constant across all transmittance values
- SKR increases steadily with increasing transmittance
- QBER also shows minimal variation with zenith angle
- Indicates strong robustness to noise and channel loss
- Suitable for dynamic or lossy environments such as free-space or satellite QKD

Graph of QBER with transmittance



Graph of SKR with transmittance



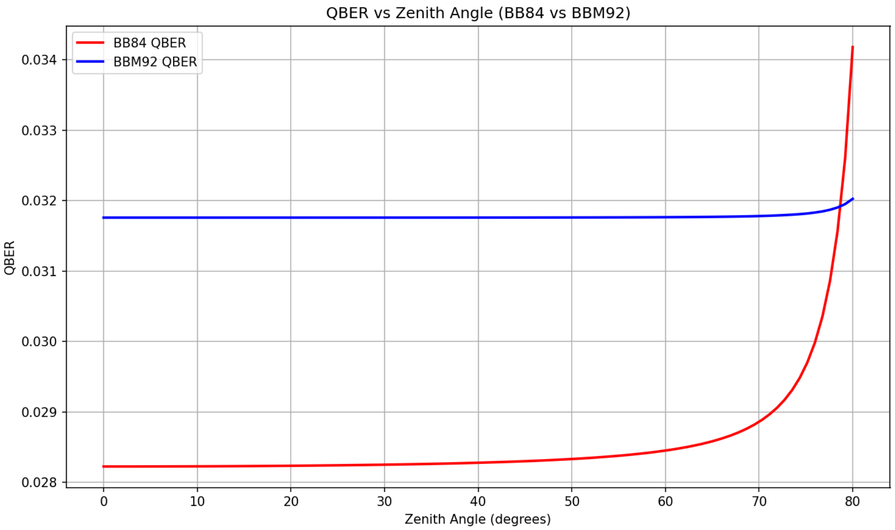
BB84 vs BBM92: QBER and SKR Behavior

- **QBER Comparison:**
  - **BB84:** QBER varies significantly with both transmittance and zenith angle
  - **BBM92:** QBER remains nearly constant across parameters
  - **Justification:** BBM92 uses entangled photon pairs—more resilient to noise; BB84 relies on basis reconciliation, more prone to errors
- **SKR Comparison:**
  - **BBM92:** Achieves higher SKR consistently, even at low transmittance
  - **BB84:** SKR improves only at high transmittance; remains low otherwise
  - **Justification:** Entanglement in BBM92 ensures better sifting and lower QBER; BB84 suffers from basis mismatch and losses

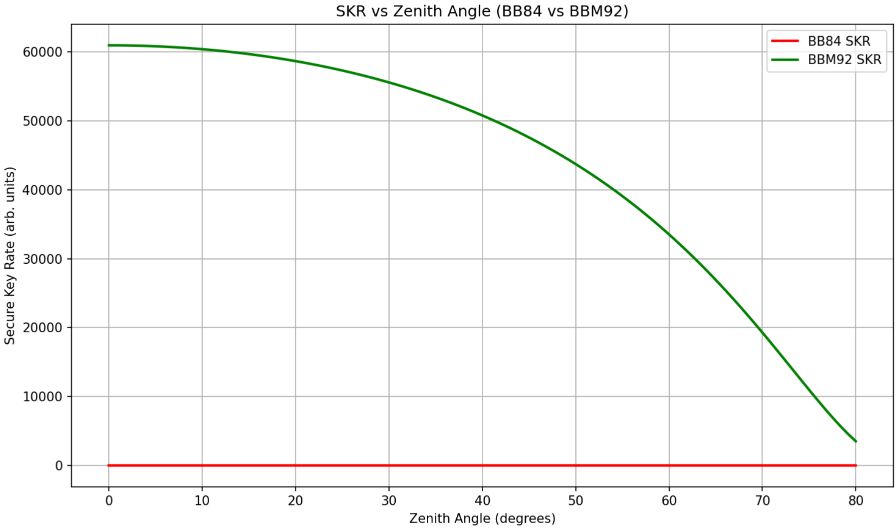
Conclusion and Recommendation

- **BB84:**
  - Suitable for high-transmittance, low-noise conditions (e.g., optical fiber channels)
  - Highly sensitive to zenith angle and atmospheric variations
- **BBM92:**
  - Robust across a wide range of transmittance and zenith angles
  - Consistently low QBER and high SKR make it suitable for dynamic environments
  - Ideal for free-space QKD, satellite communication, or mobile applications
- **Recommendation:** Use BB84 for stable, high-quality links; prefer BBM92 for noisy, lossy, or mobile channels

Graph of QBER with zenith angle



Graph of SKR with zenith angle



References

- **Analysing QBER and Secure Keyrate under Various Losses for Satellite Based Free Space QKD**
  Muskan, Ramniwas Meena, Subhashish Banerjee
  arXiv:2308.01036 [quant-ph]
  `https://arxiv.org/abs/2308.01036`

- **FSO-QKD Protocols Under Free-Space Losses and Device Imperfections: A Comparative Study**
  Mitali Sisodia, Omshankar, Vivek Venkataraman, Joyee Ghosh
  arXiv:2309.09994 [quant-ph]
  `https://arxiv.org/abs/2309.09994`

- **Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber**
  K.A. Patel, J.F. Dynes, I. Choi, A.W. Sharpe, A.R. Dixon, Z.L. Yuan, R.V. Penty, A.J. Shields

References

*Phys. Rev. X, 2, 041010 (2012)*https://doi.org/10.1103/PhysRevX.2.041010

- **Realistic Quantum Network Simulation for Experimental BBM92 Key Distribution**
  Michelle Chalupnik, Brian Doolittle, Suparna Seshadri, et al.
  arXiv:2505.24851 [quant-ph]
  https://arxiv.org/abs/2505.24851

- **Decoy State Quantum Key Distribution**
  Hoi-Kwong Lo, Xiongfeng Ma, Kai Chen
  Phys. Rev. Lett. 94, 230504 (2005)
  https://doi.org/10.1103/PhysRevLett.94.230504