BB84 Quantum Key Distribution
Complete Learning Guide

Generated: February 01, 2026

JNTUA ECE Department | Team Silicon

Table of Contents

1. Questions Asked & Comprehensive Answers

Q1: Error Suppression & SessionInfo Initialization Issues

Problem: Application showing "Bad message format" and "SessionInfo before it was initialized" errors.

Solution:
• Optimized error suppression to target only specific errors (SessionInfo, Bad message format)
• Removed aggressive stderr/stdout filtering that caused performance issues
• Implemented MinimalErrorFilter class for lightweight error handling
• Maintained early session state initialization at module level

Result: Clean startup, no error messages, improved app performance.

Q2: Transmitted Bits in Key Metrics Display

Question: Can we show transmitted bits in the key metrics?

Answer: Yes! Added two new metrics:
• **Transmitted Bits:** Total number of qubits Alice sent through the quantum channel
• **Sift Rate (Success Rate):** Percentage of transmitted bits that were successfully sifted

Expected Values:
• Normal: ~50% success rate (expected in BB84 due to random basis matching)
• With Eve: May decrease below 50% due to eavesdropping errors

Formula: Sift Rate = (Sifted Bits / Transmitted Bits) × 100%

Q3: Sifted Key Rate for Both Scenarios

Question: Add sifted key rate for both No Eve and With Eve scenarios.

Implementation:
• Calculate sifted key rate separately for each scenario
• No Eve scenario: Shows baseline sifting efficiency (blue color #1e40af)
• With Eve scenario: Shows reduced efficiency (red color #dc2626)
• Allows direct comparison of Eve's impact

Calculation:
Sift_Rate_No_Eve = (No_Eve_Sifted_Count / Transmitted_Bits) × 100%
Sift_Rate_With_Eve = (With_Eve_Sifted_Count / Transmitted_Bits) × 100%

Q4: Eve's Impact on Sifted Key Rate

Question: If Eve intercepts, does the sifted key decrease?

Answer: YES! Added three-column impact analysis:
• **Eve's Impact on Sift Rate (%):** Percentage decrease in sifting efficiency
• **Sifted Bits Lost to Eve:** Actual count of bits lost
• **Eve Detection Status:** Red (DETECTED) if QBER > threshold, Green (UNDETECTED) otherwise

Why Decrease Happens:
1. Eve measures in wrong basis ~50% of the time

2. Wrong-basis measurements alter quantum states
3. Eve re-sends corrupted qubits to Bob
4. Alice-Bob basis matching faces additional errors
5. Fewer bits pass verification → Lower sift rate

Q5: What is Success Rate?

Definition: Percentage of transmitted bits that were successfully sifted (basis-matched).

Why ~50% in BB84?
• Alice randomly chooses basis (Z or X) for each qubit: 50/50 probability
• Bob randomly measures in basis (Z or X): 50/50 probability
• They match only when both choose same basis: ~50% of the time
• This is NORMAL and EXPECTED in BB84 protocol

With Eve:
• Eve's eavesdropping may introduce errors
• Extra errors cause additional mismatches
• Success rate may drop below 50%
• Decrease reveals Eve's presence through QBER increase

Q6: Color Legend for Metrics

Question: Add color guide/legend for transmitted bits and success rate.

Color Scheme:
• **Cyan (#0891b2):** Transmitted bits, normal success rate
• **Blue (#1e40af):** No Eve scenario metrics
• **Red (#dc2626):** With Eve scenario, eavesdropping detected
• **Orange (#f59e0b):** Eve's impact percentage
• **Green (#16a34a):** Eve undetected (low QBER)

Visual Legend: Three colored boxes showing meaning of each color.

Q7: How Sifted Bits Are Lost to Eve

Mechanism:
1. Eve uses wrong basis: ~50% of Eve's choices don't match Alice's
2. Wrong-basis measurement collapses quantum state incorrectly
3. Eve re-sends incorrect state to Bob
4. Bob's measurement gives wrong result for these bits
5. During sifting, Alice & Bob find mismatches in their results
6. These bits are rejected as "sifted bits lost"

Mathematical View:
Bits_Lost = Sifted_No_Eve - Sifted_With_Eve
Impact_Rate = (Bits_Lost / Sifted_No_Eve) × 100%

Q8: Why Sifted Bits Lost Shows Zero

Possible Reasons:
1. **Low Eve Probability:** If Eve Probability ≤ 50%, Eve doesn't intercept all qubits
2. **Statistical Variance:** Eve's random basis sometimes aligns correctly with Alice
3. **Small Sample Size:** With limited transmitted bits, randomness dominates

To See Bits Lost:
• Increase Eve Probability slider to 80-100%
• Increase Transmitted Bits to 500-2000
• Run simulation multiple times (randomness matters)
• Watch Eve's Impact Rate (%) instead of bit count

Q9: Eve Detected Despite 0 Bits Lost

KEY INSIGHT: Eve is detected through QBER (error rate), NOT bit count!

The Difference:
• **Sifted Bits Lost:** Counts how many bits disappeared (quantity)
• **QBER:** Measures error rate in remaining sifted bits (quality)

Real Example:
No Eve: 100 sifted bits, 0 errors → QBER = 0% ■
With Eve: 100 sifted bits, 15 errors → QBER = 15% ■ DETECTED!

Why? Eve's wrong-basis measurements introduce BIT FLIPS in the remaining sifted bits!
These errors show up as QBER exceeding the threshold (typically 11%).

2. Mathematical Formulas & Equations

BB84 Protocol Mathematics

Sift Rate (Success Rate):

```
Sift_Rate = (Sifted_Bits / Transmitted_Bits) × 100%
```
Percentage of transmitted bits where Alice and Bob used same basis

Expected Sift Rate (No Eve):

```
Sift_Rate_Expected = 50%
```
Since each person randomly chooses basis independently

Sifted Key Rate:

```
Sifted_Rate = (Sifted_Count / Total_Transmitted) × 100%
```
Shows efficiency for each scenario (No Eve vs With Eve)

Eve's Impact on Sifting:

```
Impact = Sift_Rate_NoEve - Sift_Rate_WithEve
```
Percentage point difference showing eavesdropping effect

Bits Lost to Eve:

```
Bits_Lost = Sifted_Count_NoEve - Sifted_Count_WithEve
```
Absolute count of sifted bits lost due to eavesdropping

QBER (Quantum Bit Error Rate) Formulas

Basic QBER Calculation:
QBER = (Number_of_Errors / Total_Sifted_Bits) × 100%

Interpretation:
• QBER = 0-3%: Low errors (no eavesdropper detected) ■
• QBER = 3-11%: Medium errors (depends on threshold setting)
• QBER > 11%: High errors (eavesdropping DETECTED) ■

Theoretical QBER with Eve (Intercept-Resend):
QBER_theoretical = 0.25 (25%) for Intercept-Resend attack
• Eve guesses wrong basis 50% of the time
• Wrong guess causes measurement error 50% of time
• Total: 0.5 × 0.5 = 0.25 = 25%

Detection Threshold:
If QBER > Threshold → Eavesdropping Detected
If QBER ≤ Threshold → Key is considered Secure ■

Key Rate & Privacy Amplification

Key Rate (Efficiency):
Key_Rate = (Final_Key_Length / Transmitted_Bits)
Example: 25 bits final key / 200 transmitted = 0.125 = 12.5% efficiency

Final Secure Key Length:
Final_Key = Privacy_Amplification(Sifted_Key, QBER)

Shannon Entropy (Eve's Information):
H(E) = -e·log■(e) - (1-e)·log■(1-e)
where e = QBER
(Gives maximum information Eve could have learned)

Information-Theoretic Security:
If QBER < threshold:
Remaining_Eve_Info = 2^(-128) (exponentially small)
Final key is cryptographically secure

Quantum State Mathematics

Z-Basis (Rectilinear) States:
|0■_Z = |0■ (vertical polarization)
|1■_Z = |1■ (horizontal polarization)

X-Basis (Diagonal) States:
|0■_X = |+■ = (|0■ + |1■)/√2 (45° polarization)
|1■_X = |-■ = (|0■ - |1■)/√2 (135° polarization)

Measurement Probability:
If prepared in Z-basis but measured in X-basis:
P(correct) = |■+|0■|² = (1/√2)² = 0.5 = 50%
P(incorrect) = |■-|0■|² = (1/√2)² = 0.5 = 50%

This is why Eve introduces errors! Wrong basis measurement gives random result.

Bloch Sphere Representation

General Qubit State:
|ψ■ = cos(θ/2)|0■ + e^(iϕ)·sin(θ/2)|1■

Bloch Vector Coordinates:
x = sin(θ)·cos(ϕ)
y = sin(θ)·sin(ϕ)
z = cos(θ)

θ **(Polar Angle):** θ = 2·arccos(|■0|ψ■|)
ϕ **(Azimuthal Angle):** ϕ = arg(■1|ψ■) - arg(■0|ψ■)

Basis States on Bloch Sphere:
|0■ → (0, 0, 1) - North pole (Z-basis)
|1■ → (0, 0, -1) - South pole (Z-basis)
|+■ → (1, 0, 0) - +X axis (X-basis)
|-■ → (-1, 0, 0) - -X axis (X-basis)

3. Key Concepts Explained

Basis Matching: When Alice's basis equals Bob's basis for a particular qubit. Essential for BB84 sifting.

Sifting: Process of keeping only bits where Alice and Bob used the same measurement basis.

Eavesdropping Detection: Detected through QBER (error rate), not through missing bits. Eve's measurements introduce errors.

Quantum Measurement: Collapses superposition to definite state. Measuring in wrong basis gives random result.

Quantum Uncertainty: Cannot know arbitrary observable of quantum state without destroying it (Heisenberg principle).

Information-Theoretic Security: Security guaranteed by laws of physics, not computational complexity. Eve gains negligible information.

4. Practical Implementation Details

Simulation Parameters

Transmitted Bits (qubits): 50-2000 (configurable)
Range determines sample size for statistical analysis.

Eve Probability: 0-100%
Likelihood of Eve intercepting each qubit (0% = no eavesdropping, 100% = intercepts all).

QBER Threshold: Default 11%
If QBER exceeds this, eavesdropping is detected and key rejected.

Channel Noise: Default 1%
Environmental noise causing random bit flips (independent of Eve).

Eve Attack Type: Intercept-Resend (default)
Eve measures and re-transmits, introducing detectable errors.

Metrics Explained

Metric	Formula	Meaning
Transmitted	num_bits	Total qubits sent
Sift Rate	(sifted/transmitted)×100%	Success in basis matching
Sifted Bits	count where basis match	Usable bits for key
Errors	sifted_bits - correct_bits	Mismatches in sifted bits
QBER	(errors/sifted)×100%	Error rate indicator
Final Key	privacy_amplify(sifted)	Cryptographically secure key
Key Rate	final_key/transmitted	Protocol efficiency

==========

End of Learning Guide