BB84 Quantum Key Distribution

1.Introduction-to-classical-and-quantum-computing-1e4p-281-284.pdf
PDF

I dont know anything about bb84, explain me

Great 😄 Samyak, let's start from **absolute zero** and build BB84 step by step.

🔐 BB84 Protocol (Simple Explanation)

BB84 is a **Quantum Key Distribution (QKD)** protocol.

It was proposed in 1984 by:

- Charles H. Bennett
- Gilles Brassard

Its goal is simple:

> 🧠 Allow Alice and Bob to create a **secret key**
> 🚨 And detect if someone (Eve) is spying

⚡ Why Do We Need BB84?

In classical cryptography:

- Keys are shared using math.
- Security depends on hard problems (like factoring in RSA).

In quantum cryptography:

- Security depends on **laws of physics**.
- If Eve measures a qubit → she **disturbs it**.
- That disturbance can be detected.

🧩 Step 1: The Two Bases

BB84 uses **two measurement bases**.

1️⃣ Z-basis (Computational basis)

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \; |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

The difference between classical probabilities and quantum amplitudes arises in how the object's state changes when we perform an operation on it. Classically, we can multiply a vector of probabilities by a *stochastic matrix*, which is a matrix of nonnegative real numbers each of whose columns sums to 1. Quantum-mechanically, we multiply the vector of amplitudes by a *unitary matrix*, which is a matrix of complex numbers that maps any unit vector to another unit vector. (Equivalently, U is unitary if and only if its inverse U^{-1} equals its conjugate transpose U^*.) As an example, suppose we start with the state $|0\rangle$, which corresponds to the vector of amplitudes

$$\begin{bmatrix}1\\0\end{bmatrix}.$$

We then left-multiply this vector by the unitary matrix

$$U = \begin{bmatrix}\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{bmatrix},$$

which maps the vector to

$$\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix},$$

and therefore the state $|0\rangle$ to

$$U|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

If we now measured, we would see $|0\rangle$ with probability $1/2$ and $|1\rangle$ with probability $1/2$. The interesting part is what happens if we apply the same operation U a second time, without measuring. We get

$$\begin{bmatrix}\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix}$$

which is $|1\rangle$ with certainty (see Figure 4.1). Applying a "randomizing" operation to a "random" state produces a deterministic outcome! The reason is that, whereas probabilities are always nonnegative, amplitudes can be positive, negative, or even complex, and can therefore cancel each other out. This interference of amplitudes can be considered the source of all "quantum weirdness."

https://www.researchgate.net/publication/335845744/figure/fig1/AS%3A842502001135616%401577879538953/The-Bloch-sphere-representation-of-a-qubit-state-The-north-pole-is-the-ground-state-0.png

States:

- |0⟩
- |1⟩

This is like normal binary (0 and 1).

2️⃣ X-basis (Diagonal basis)

$$H\left|+\right\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix} = \begin{bmatrix}1\\ 0\end{bmatrix} = \left|0\right\rangle$$

The difference between classical probabilities and quantum amplitudes arises in how the object's state changes when we perform an operation on it. Classically, we can multiply a vector of probabilities by a *stochastic matrix*, which is a matrix of nonnegative real numbers each of whose columns sums to 1. Quantum-mechanically, we multiply the vector of amplitudes by a *unitary matrix*, which is a matrix of complex numbers that maps any unit vector to another unit vector. (Equivalently, U is unitary if and only if its inverse U^{-1} equals its conjugate transpose U^*.) As an example, suppose we start with the state $|0\rangle$, which corresponds to the vector of amplitudes

$$\begin{bmatrix}1\\ 0\end{bmatrix}.$$

We then left-multiply this vector by the unitary matrix

$$U = \begin{bmatrix}\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{bmatrix},$$

which maps the vector to

$$\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix},$$

and therefore the state $|0\rangle$ to

$$U|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

If we now measured, we would see $|0\rangle$ with probability $1/2$ and $|1\rangle$ with probability $1/2$. The interesting part is what happens if we apply the same operation U a second time, without measuring. We get

$$\begin{bmatrix}\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix} = \begin{bmatrix}0\\ 1\end{bmatrix}$$

which is $|1\rangle$ with certainty (see Figure 4.1). Applying a "randomizing" operation to a "random" state produces a deterministic outcome! The reason is that, whereas probabilities are always nonnegative, amplitudes can be positive, negative, or even complex, and can therefore cancel each other out. This interference of amplitudes can be considered the source of all "quantum weirdness."

https://www.researchgate.net/publication/232905933/figure/fig1/AS%3A1132493709291521%401647018949173/The-Bloch-sphere-showing-a-p-rotation-about-the-x-axis-transforming-an-initial-state.jpg

States:

- $|+\rangle$
- $|-\rangle$

Where:

- $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$
- $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$

🧪 Step 2: What Alice Does

Alice:

1. Generates **random bits**
   Example:
   `0 1 0 1 1 0 1`
2. For each bit, she randomly chooses a basis:
   - Z or X
3. She sends qubits according to this rule:

Bit	Z basis	X basis
0		0⟩
1		1⟩

So she sends qubits to Bob.

🧪 Step 3: What Bob Does

Bob:

- For each received qubit,
- Randomly chooses a basis (Z or X)
- Measures the qubit.

🎯 Important Rule

If Bob uses:

- ✅ Same basis as Alice → He gets correct bit
- ❌ Different basis → Result is random (50% chance)

📞 Step 4: Public Discussion

After transmission:

1. Alice and Bob publicly tell each other:
   - Which basis they used
     (NOT the bit!)
2. They keep only the bits where:
   - Their bases matched

3. These remaining bits become the:
   🔑 **Shared Secret Key**

🚨 What If Eve Is Spying?

Suppose Eve intercepts qubits.

She:

- Doesn't know correct basis.
- Randomly chooses a basis.
- Measures.
- Sends qubit to Bob.

Problem:

If she chooses wrong basis:
→ She disturbs the qubit.
→ Bob might get wrong result.
→ Alice & Bob will detect errors.

🎲 Detection Probability

If Alice and Bob reveal `n` bits to check:

Probability Eve is NOT detected:

$$(3/4)^n$$

Probability she IS detected:

$$1 - (3/4)^n$$

So if they check 50 bits:

Detection probability ≈ 99.999999%

Very close to certain.

(From your textbook section 6.6 1.Introduction-to-classical-and…)

🔥 Why Is BB84 Powerful?

Because:

- Measuring a quantum state **changes it**
- Eve cannot copy qubits (No-Cloning Theorem)
- Any eavesdropping introduces errors

Security comes from **physics**, not math.

🧠 Big Picture Summary

BB84 does:

1. Alice sends random qubits
2. Bob measures randomly
3. They compare bases publicly
4. Keep matching bits
5. Reveal a few bits to detect Eve
6. Remaining bits → Secret key

If you want, next I can explain:

- 🔢 A full numerical example (exam style)
- 🧮 Probability derivation
- 🧬 Why measuring wrong basis gives 50%
- 🔐 Compare BB84 vs E91
- 📝 6-mark exam answer format

Tell me what you want next 👀

Sources

(b) Explain the BB84 Quantum Key Distribution protocol with the help of a suitable example. [5] [5]

Perfect 👍 This is a **5-mark theory question**, so I'll give you a clean, exam-ready answer with example.

BB84 Quantum Key Distribution Protocol

The **BB84 protocol** was proposed in 1984 by
Charles H. Bennett and
Gilles Brassard.

It is a **Quantum Key Distribution (QKD)** protocol that allows two parties (Alice and Bob) to generate a shared secret key securely using quantum mechanics.

The security of BB84 is based on:

- Measurement disturbs a quantum state
- No-cloning theorem (qubits cannot be copied)

Step 1: Two Bases Used

BB84 uses two bases:

Z-basis (Computational Basis):

- $|0\rangle \rightarrow$ bit 0
- $|1\rangle \rightarrow$ bit 1

X-basis (Diagonal Basis):

- $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \rightarrow$ bit 0
- $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2} \rightarrow$ bit 1

Step 2: Protocol Working (With Example)

1️⃣ Alice's Preparation

Suppose Alice chooses:

Bits:
1 0 1 0 1 1 0 1

Bases:
Z X Z X X Z Z X

She sends:

Bit	Basis	Qubit Sent
1	Z	
0	X	
1	Z	
0	X	
1	X	
1	Z	
0	Z	
1	X	

2️⃣ Bob's Measurement

Bob randomly chooses bases:

Z Z Z X X X Z X

If Bob uses:

- Same basis → correct bit
- Different basis → random result (50%)

After measurement, suppose Bob obtains:

1 1 1 0 1 0 0 1

3️⃣ Public Discussion

Alice and Bob publicly compare only the **bases**, not the bits.

They keep bits where bases match:

Matching positions → 1, 3, 4, 5, 7, 8

Shared key becomes:

1 1 0 1 0 1

This is the **secret key**.

Step 3: Detecting Eavesdropper (Eve)

If Eve intercepts:

- She does not know correct basis.
- Wrong measurement disturbs the qubit.
- This introduces errors in Bob's results.

Alice and Bob reveal a few bits of their key.

If error rate is high → Eve is detected.

Probability of detecting Eve after revealing n bits:

$$P = 1 - (3/4)^n$$

Thus, security is guaranteed by the laws of quantum mechanics.

Conclusion

The BB84 protocol allows secure key distribution by:

1. Sending qubits in random bases
2. Measuring in random bases
3. Keeping only matching basis results
4. Detecting eavesdropping through error checking

Hence, BB84 provides unconditional security based on quantum physics.

If you want, I can also give you:

- 🔹 Ultra-perfect 6-mark version
- 🔹 Short 3-mark version
- 🔹 Only final bullet points (for last-minute revision)

similarly Explain E91 protocol also

Perfect 👍 this is also a **5-mark theory question**, so here is a clean, exam-ready answer.

E91 Quantum Key Distribution Protocol

The **E91 protocol** was proposed in 1991 by
Artur Ekert.

Unlike BB84, E91 is based on **quantum entanglement** and Bell's Theorem.

It is also a **Quantum Key Distribution (QKD)** protocol used to establish a secure shared key between Alice and Bob.

🔷 Basic Idea

E91 uses **entangled qubit pairs**.

A source generates entangled particles (usually Bell states) and sends:

- One particle to Alice
- One particle to Bob

Example Bell State used:

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

In an entangled pair:

- If Alice measures 0 → Bob gets 1
- If Alice measures 1 → Bob gets 0
  (Perfect anti-correlation)

🔷 Step-by-Step Working

OpenAI

Step 1: Distribution of Entangled Pairs

A quantum source sends entangled qubits:

- Alice receives one qubit
- Bob receives the other

They do not know outcomes yet.

Step 2: Random Measurements

Alice and Bob independently choose random measurement directions (different bases).

For example:

Alice chooses from: A1, A2, A3
Bob chooses from: B1, B2, B3

They measure their qubits.

Because of entanglement:

- Their results are correlated.

Step 3: Public Discussion

They publicly announce:

- Which measurement basis they used
  (Not the results)

For certain compatible measurement combinations:

- Their results are perfectly correlated or anti-correlated.
- These are used to generate the secret key.

Other combinations are used to test security.

🔷 Security Using Bell's Inequality

E91 uses **Bell's inequality test**.

If no eavesdropper is present:

- Measurements violate Bell's inequality.
- Strong quantum correlations are observed.

If Eve intercepts:

- Entanglement is disturbed.

- Bell inequality will NOT be violated.
- Alice and Bob detect eavesdropping.

Thus, security is guaranteed by:

- Quantum entanglement
- Violation of Bell inequalities

🔷 Example

Suppose:

Alice's Result → 0
Bob's Result → 1

If they used compatible bases:
→ They record this as secret bit.

After many measurements:
→ They keep correlated bits.
→ Discard others.
→ Perform Bell test.
→ If test passes → Key is secure.

🔷 Difference Between BB84 and E91

BB84	E91
Does NOT use entanglement	Uses entanglement
Security from measurement disturbance	Security from Bell inequality violation
Alice prepares qubits	Entangled source prepares qubits

🔷 Conclusion

The E91 protocol establishes a secure key by:

1. Distributing entangled qubits
2. Performing random measurements
3. Checking Bell inequality violation
4. Extracting correlated results as secret key

Thus, E91 provides unconditional security based on quantum entanglement and fundamental laws of quantum mechanics.

If you want, I can also give:

- 🔥 A direct BB84 vs E91 comparison answer (very good for exams)
- 📊 Numerical/Bell inequality based explanation
- 🧠 3-mark short version
- 📝 Combined 10-mark answer format