LM05: A Deterministic Two-way Quantum Key Distribution Protocol

Aditya Kumar
M.TECH, M25IQT002

What is LM05?

- A simple two-way Quantum Key Distribution protocol.
- **Bob prepares** the qubits, not Alice.
- Alice chooses:
  - **Control Mode (CM)** – check for Eve.
  - **Message Mode (MM)** – encode a key bit.
- Bob measures again and recovers Alice's bit.
- LM05 is **deterministic** — no basis mismatch, no bit loss.

Step-by-Step LM05 (Simple)

1. **Bob prepares a qubit**
   - Random basis: Z or X.
   - Random bit: 0 or 1.
   - Sends qubit to Alice.
2. **Alice chooses a mode**
   - CM: measure the qubit (used to detect Eve).
   - MM: encode a bit and send back.

Control Mode vs Message Mode

Control Mode (CM)

- Alice measures the qubit.
- Results later compared with Bob.
- High errors $\Rightarrow$ Eve detected.

Message Mode (MM)

- Alice encodes:
  - $0 \rightarrow$ apply I
  - $1 \rightarrow$ apply iY
- Sends qubit back to Bob.

Bob's Measurement (Deterministic)

- Bob measures in the **same basis** he used earlier.
- Bob initial bit $= b$ Bob final result $= b'$
- He recovers Alice's bit:

$$\text{Alice bit} = b \oplus b'$$

- Works every time — no basis mismatch.

Example (Very Simple)

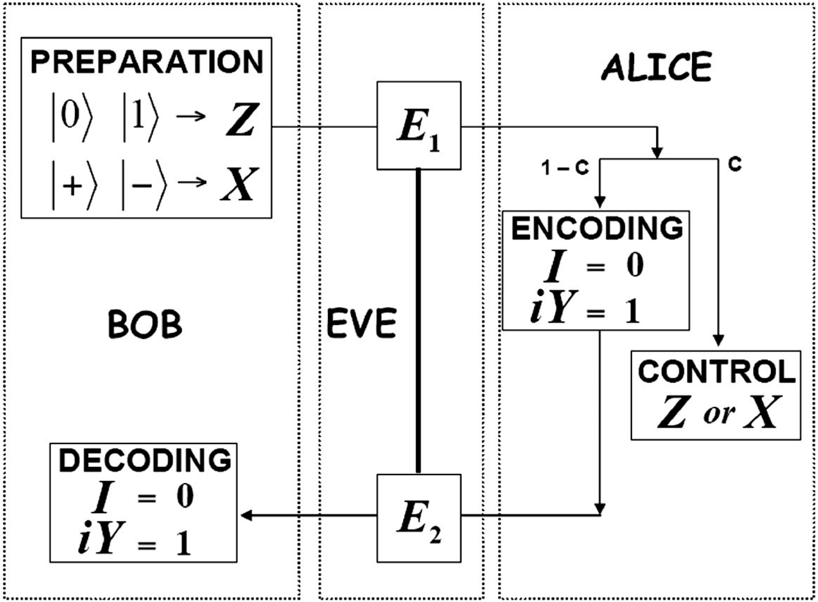
- Bob prepares $|0\rangle$ in Z basis.
- Alice chooses MM and wants to send bit 1.
- She applies iY: $|0\rangle \rightarrow |1\rangle$.
- Bob measures in Z: gets 1.
- Recovers: $0 \oplus 1 = 1$
- Shared bit $= 1$

Final Steps

After many rounds:

- Alice reveals which rounds were CM.
- Bob & Alice check errors (detect Eve).
- MM rounds form the raw key.
- Apply error correction & privacy amplification.

Diagram (LM05)



Decoy States in LM05 Protocol

What is a Decoy State?

- A decoy state is a **fake or dummy quantum pulse** sent by Bob.
- Not used for key generation.
- Used only to **detect photon-number-splitting (PNS) attacks**.
- Different mean photon numbers:
  - Signal pulses: $\mu \approx 0.5$
  - Decoy pulses: $\nu \approx 0.1$
  - Vacuum pulses: 0
- Same encoding, same probability, but **different expected detection rates**.
- Eve does not know which pulses are decoys.

Why Decoy States Are Needed

- LM05 uses weak laser pulses $\rightarrow$ sometimes multi-photon pulses.
- Eve can perform a **PNS attack**:
  - Splits off one photon from multi-photon pulses.
  - Learns Alice's encoding without introducing errors.
  - LM05 is two-way $\rightarrow$ Eve has two opportunities.

How Decoy States Work in LM05

Step-by-step:

1. Bob randomly sends:
   - Signal pulses (μ)
   - Weak decoy pulses (ν)
   - Vacuum pulses
2. Alice performs LM05 normally:
   - Message Mode: apply I or iY
   - Control Mode: measurement
3. After transmission:
   - Bob announces which pulses were decoys.
   - Alice and Bob compare detection rates.
4. If Eve performs PNS:
   - She steals photons from multi-photon signals.
   - But must treat decoy pulses similarly.
   - Detection statistics change significantly.
5. If statistics mismatch $\rightarrow$ **Eve is detected** $\rightarrow$ abort.

Why Decoy States Are Effective

Key Idea:

- Eve does not know which pulses are real vs decoy.
- Any PNS attack changes the detection probability of decoy pulses.
- These statistical deviations are easy to detect.
- Ensures LM05 remains secure even with weak coherent sources.

Advantages:

- Protects LM05 from PNS attacks.
- Improves security over long distances.
- Allows higher photon intensity (better key rates).
- Works very well with two-way QKD protocols.

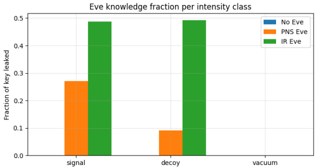
Security highlights

- Any eavesdropper (Eve) interacting with the qubit disturbs it; control rounds detect this via elevated QBER.
- Two-way channel forces Eve to attack both forward and backward channels or use memory — both detectable in principle.
- Authentication of the classical channel is mandatory to prevent man-in-the-middle attacks.

Attacks and countermeasures

- **Intercept-resend:** detected by control rounds (increased error rate).
- **Photon-number splitting (PNS):** mitigate with decoy states or single-photon sources.
- **Trojan-horse attacks:** use monitoring detectors and optical isolators.
- **Quantum memory attacks:** theoretical threat; practical countermeasures include randomness and privacy amplification.

Eve Knowledge for Signal, Decoy, and Vacuum Pulses

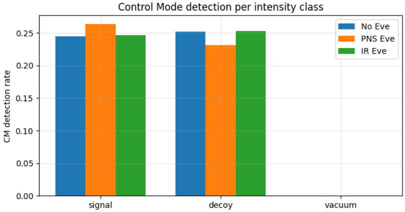


What this graph shows:

- **No Eve (Blue):** Eve learns nothing. This is the normal, safe case.
- **PNS Eve (Orange):** Eve learns more from **signal pulses** because they have more photons. She learns much less from **decoy pulses**, since decoys are very weak.
- **IR Eve (Green):** Eve learns about **50%** of the key for both signal and decoy. This is because IR Eve measures the qubit and guesses the basis.

Takeaway: Decoy pulses help detect PNS attacks (less leakage in decoys), but they cannot stop IR attacks, since IR works by measuring, not by photon number.

Control Mode Detection (Signal, Decoy, Vacuum)

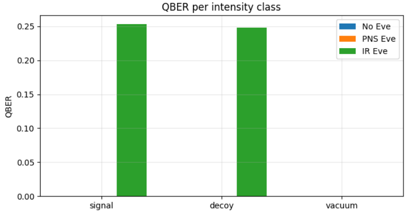


What this graph shows:

- **No Eve:** Signal and decoy pulses have almost the same detection rate. This is what a normal, safe channel looks like.
- **PNS Eve:** Signal detection goes **up** and decoy detection goes **down**. This difference is a strong sign of a PNS attack. (Because PNS affects strong pulses more than weak ones.)
- **IR Eve:** Detection looks almost the same as No Eve. IR does not change the intensity pattern, so decoys cannot catch it.

Takeaway: Comparing signal and decoy detection rates helps find **PNS attacks**, but it cannot detect **IR attacks**.

QBER per intensity class



What this graph shows:

- **No Eve:** QBER is almost zero. This means the channel is clean and safe.
- **PNS Eve:** QBER is still very low. PNS attacks do not cause measurement errors, so QBER cannot detect PNS.
- **IR Eve:** QBER jumps to around **25%**. This is because IR Eve measures in the wrong basis half the time, creating many errors.

Takeaway:

- Use **decoy pulses** to catch PNS attacks.
- Use **QBER (error rate)** to catch IR attacks.

Final Conclusion from All Three Results

Overall Security Insight:

- **PNS attacks** change the detection pattern of **signal vs decoy** pulses.
  - More leakage on signal than decoy.
  - Detection rates become uneven.
  - QBER stays low (silent attack).
- **IR attacks** do **not** change signal–decoy patterns, but introduce **high QBER**.
  - Eve learns about half the key.
  - Detection rates look normal.
  - Error rate becomes very large.

Conclusion:

- **Decoy-state analysis detects PNS attacks.**
- **QBER/Control Mode detects IR attacks.**
- Both checks together make LM05 secure against silent (PNS) and noisy (IR) attacks.

Advantages vs Limitations

Advantages

- Deterministic raw key generation (no basis reconciliation loss).
- Simpler operations (no entanglement).

Limitations

- Two-way channel doubles exposure to noise and loss.
- Requires robust authentication and additional engineering for practical deployment.

LM05 vs BB84 (summary)

Feature	LM05	BB84
Key type	Deterministic	Probabilistic
Channel	Two-way	One-way
Basis reconciliation	Not required	Required
Wastage	Low	High
Entanglement	No	No

Conclusion

- LM05 is an attractive deterministic QKD protocol for short-range networks with lower raw-key wastage.
- Security rests on standard quantum principles and additional practical countermeasures (decoy states, authentication).
- For practical deployment, noise, loss and two-way vulnerabilities must be carefully mitigated.