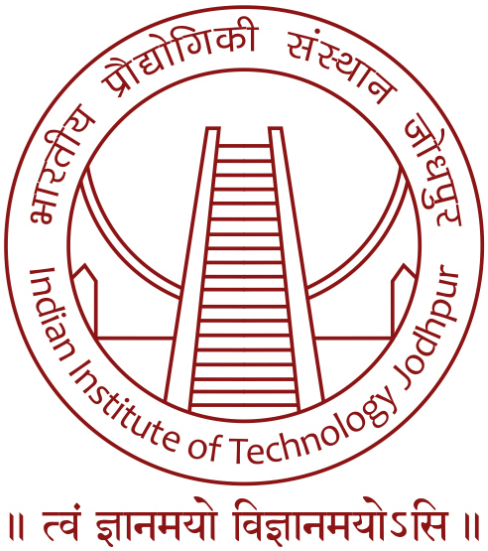
Quantum Cryptography and Coding

Report On LM05 QKD Protocol



Name: **SUMIT KUMAR**
Roll Number: **(M23IQT007)**
Program: **MTech(QUANTUM TECHNOLOGIES)**

0.1 Introduction

Quantum key distribution (QKD) allows two parties, traditionally called Alice and Bob, to share a secret random key with unconditional security guaranteed by the laws of quantum mechanics. The first and most well-known QKD protocol is the BB84 protocol proposed by Bennett and Brassard in 1984. Since then, many other QKD protocols have been developed, each with its own advantages and trade-offs.

One class of QKD protocols are the "two-way" protocols, where the qubits travel back and forth between Alice and Bob during the protocol, rather than just one-way from the sender to the receiver as in BB84. The LM05 protocol, proposed by Lucamarini and Mancini in 2005, is an important example of a two-way QKD protocol with some desirable properties compared to BB84.

This report will provide a detailed explanation of the LM05 protocol, its underlying principles, the protocol steps, security considerations, and recent experimental implementations.

0.2 The LM05 Protocol

0.2.1 Protocol Steps

The LM05 protocol consists of the following steps:

1. **Preparation:** Bob prepares a single qubit in one of four possible states: $|0\rangle$, $|1\rangle$, $|+\rangle$, or $|-\rangle$. These states belong to two complementary bases: the Z-basis ($|0\rangle$, $|1\rangle$) and the X-basis ($|+\rangle$, $|-\rangle$).

2. **Transmission:** Bob sends the prepared qubit to Alice through a quantum channel.

3. **Encoding:** Upon receiving the qubit, Alice encodes her secret bit (either 0 or 1) by applying one of two operators:

   - If she wants to encode 0, she applies the identity operator (I), leaving the qubit unchanged.
   - If she wants to encode 1, she applies the Pauli-Y operator (iY), which flips the state of the qubit.

4. **Retransmission:** After encoding her bit, Alice sends the qubit back to Bob through the quantum channel.

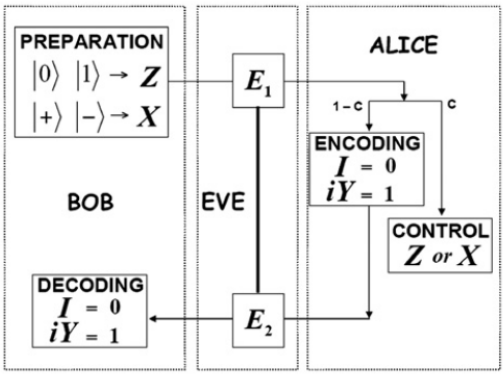
5. **Measurement and Key Generation:** Upon receiving the qubit from Alice, Bob measures it in the same basis he originally prepared it. By comparing the measurement outcome with his initial preparation, Bob can deterministically infer Alice's encoded bit (0 or 1) without the need for basis reconciliation.

0.2.2 Key Features of LM05

Some of the key advantages and features of the LM05 protocol include:

1. Deterministic Basis Reconciliation: Unlike BB84 where Alice and Bob must discard approximately 50% of the transmitted qubits due to basis mismatch, in LM05 there is no such loss since Bob simply measures in the basis he prepared the qubit in originally.

2. No Need for Public Discussion of Bases: In BB84, Alice and Bob must discuss their basis choices over an authenticated public channel to perform basis reconciliation, leaking some information to an eavesdropper. LM05 avoids this.



3. Efficiency: As Bob can deterministically read Alice's bit value, a higher fraction of the transmitted qubits contribute to the final key compared to BB84.

4. Robustness: LM05 is robust against photon number splitting attacks for signals containing up to two photons per pulse. This is better than BB84 which is only secure for single-photon signals.

5. Two-Way Advantage: By leveraging the two-way nature, LM05 extracts more key from the same channel compared to one-way protocols like BB84.

However, LM05 is not without drawbacks. It requires a higher degree of technological complexity to implement the various operations like the Y gate. The protocol is also more sensitive to flawed implementation compared to BB84.

0.3 Conclusion

The LM05 protocol offers several advantages over traditional QKD protocols like BB84, particularly in terms of efficiency, robustness against certain attacks, and eliminating the need for public discussion of bases. While it presents some challenges in implementation, its benefits make it a promising option for secure communication in quantum networks.

0.4 Reference

1. Can Two-Way Direct Communication Protocols Be Considered Secure?Mladen Pavicic

2. Implementation of two way Quantum Key Distribution protocol with decoy state - M.F. Abdul Khir a,c,∗, M.N. Mohd Zain c, Iskandar Bahari d, Suryadi b, S. Shaari a