Prudent Engineering Practices for Quantum Communication Security

0.1 MiTM Attack

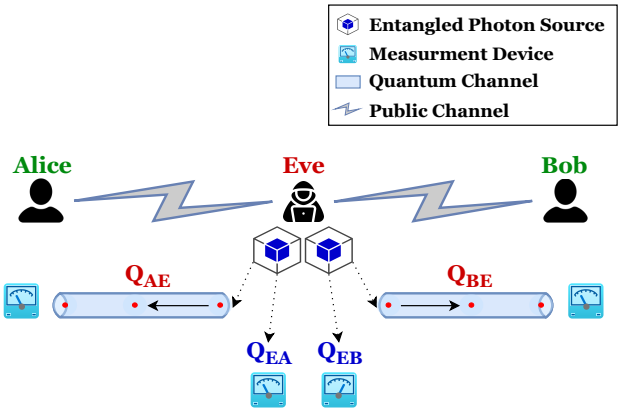
Quantum Key Distribution (QKD) protocols are vulnerable to Man-in-the-Middle (MiTM) Attacks due to the absence of pure quantum authentication procedures. These protocols currently depend on classical channels to identify any interference by attackers on the quantum channel. This allows an adversary to utilize two streams of entangled qubits to execute a MiTM attack against the involved parties, without detection. This leads to generation of compromised key pairs;allowing the adversary to intercept encrypted communication over the classical channel.

Adversary Model: In our analysis, we assume the adversary controls the entangled photon source ($\mathcal{S}$) and can transmit qubits over the quantum channel ($\mathcal{Q}$). On the classical channel ($\mathcal{N}$), the adversary is capable of impersonating a legitimate protocol participant. This means that the adversary can listen and transmit packet over the classical channel. These constraints define the scope within which the potential attack may succeed.

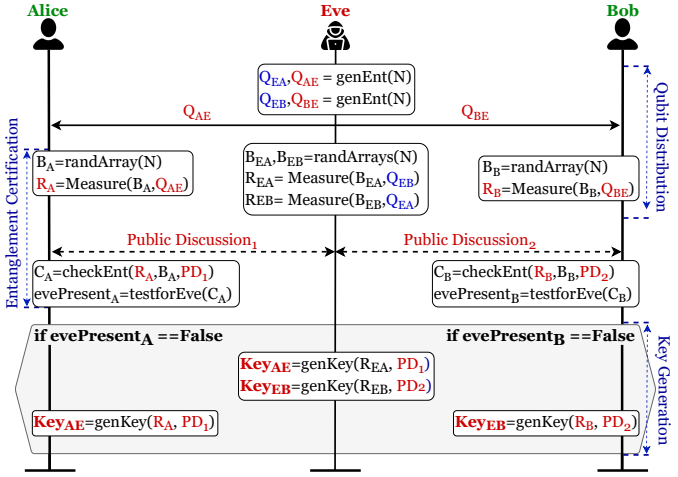
Protocol Setup: The network architecture (see figure 1a) consists of two communication channels, the quantum channel $\mathcal{Q}$ and the classical channel $\mathcal{N}$. Alice and Bob are legitimate users with access to both channels, for the purpose of generating a secure symmetric key pair. The quantum channel $\mathcal{Q}$ is used to distribute entangled qubits from an entangled qubit source $\mathcal{S}$ to the legitimate users. The classical channel $\mathcal{N}$ is used for public exchange between Alice and Bob. Eve is an adversary with the goal of compromising the generated quantum key pair.

Attack Description: The attack starts with Eve generating two streams of entangled qubit pairs using an Entangled Photon Source $\mathcal{S}$. We denote these entangled qubits as (Q_{AE}, Q_{EA}) and (Q_{BE}, Q_{EB}) The qubits Q_{AE} and Q_{BE} represent qubits transmitted to Alice and Bob over a quantum channel $\mathcal{Q}$. The other entangled qubits Q_{EA} and Q_{EB} are retained by Eve. This allows Eve to establish entanglement between herself and the users.

After both users receive the qubits over the quantum channel $\mathcal{Q}$, they conduct private measurements. This is achieved by utilizing randomly generated arrays of measurement bases $B_{A/B}$. Each measurement basis is designed to measure the orientation of the qubits along a specific dimension. Each measurement yields a binary value, denoted as $R_{A/B} = Measure(B_{A/B}, Q_{AE/BE})$, resulting in arrays of measurement results $R_{A/B}$.



(a) Network architecture for the MiTM attack scenario



(b) Message Sequence Diagram for MiTM attack.

An entanglement certification step is performed as both users need to verify if the qubits they received are entangled. This involves measuring the qubits using measurement bases, exchanging the choice of measurement bases ($B_{A/B}$), and partial information about measurement results ($R_{A/B}$). The exchange is facilitated by the classical channel $\mathcal{N}$, which allows Eve to send her own measurement basis and measurement results over the channel. The information revealed during the public discussion and information sent by Eve are represented by Public Discussion ($PD_{1/2}$).

Alice and Bob use ($R_{A/B}$, $B_{A/B}$, $PD_{1/2}$) to check entanglement between received qubits. As Eve shares entangled qubits over the quantum channel, and interferes with the classical channel, both users conclude that entanglement exists between the received qubits. They conclude that no eavesdropper is present and generate a key using the compromised measurement results $R_{A/B}$ and $PD_{1/2}$.

Root Cause: The root cause of this attack lies in the absence of

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
Conference'17, July 2017, Washington, DC, USA
© 2024 Association for Computing Machinery.
ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

a pure quantum authentication procedure in QKD protocols. This protocol relies on an insecure classical communication to authenticate qubits transmitted over the quantum channel. This makes these protocols vulnerable to a Man-in-the-Middle attacker with access to an entangled photon source.

While a vigilant reader might assert that Quantum Key Distribution (QKD) protocols are equipped to detect Man-in-the-Middle (MiTM) interference across the quantum channel, it is crucial to acknowledge that an adversary not directly manipulating the qubits may go undetected using this process.

Implication:

This leads to Alice and Bob unwittingly generating compromised key pairs, Key_{EA} and Key_{EB}, with Eve, without detecting her presence. Subsequently, all further communication is compromised, allowing Eve to remain undetected.