Mutual Authentication Mechanism using Pre-Shared Key and BB84 Quantum Key Distribution for Quantum Cryptography Communication

Minyoung Bae, Hana Kang, Ju-Sung Kang, Yongjin Yeom,
Department of Financial Information Security
Kookmin University, 77 Jeongneung-Ro, Seongbuk-Gu, Seoul, 02707, Republic of Korea
{mypaar, adr1145, jskang, salt}@kookmin.ac.kr

Abstract. It is believed that the quantum cryptography based on quantum key distribution achieves unconditional security. However, the additional authentication mechanism applied to the quantum cryptography needs to be studied since it is difficult for the quantum cryptography alone to prevent man-in-the-middle attacks. Thus, we propose two authentication mechanisms combined with modern cryptography that can solve the authentication problems of quantum cryptography using pre-shared key and quantum key distribution. The proposed mechanisms can be efficiently applied to current quantum cryptographic devices, and are more secure than the modern cryptographic authentication method.

Keywords: Entity Authentication; BB84 Quantum Key Distribution; Deterministic Random Bit Generator

1 Introduction

In recent decades, the quantum cryptography based on the quantum mechanical properties have been studied. Even though quantum cryptography theoretically achieves unconditional security, the quantum cryptography itself does not provide entity authentication to prevent man-in-the-middle attacks in which Eve pretends to be one of both entities in the middle of the communication channel. In order to solve this problem, researches on quantum authentication have been studied, but it is hard to find practical mechanisms well matched with quantum key distribution such as BB84 protocol. Consequently, it is natural to consider authentication protocols combined with modern cryptography.

In this paper, we introduce several previous efforts to solve the authentication problem, and propose a mutual authentication mechanism that can prevent man-in-the-middle attack without TTP (Trusted Third Party) and hindering the security of quantum cryptography. In addition, the authentication mechanism we propose is designed so that mutual authentication is possible even when only one party is able to transmit a qubit stream.
2 Related Works

- **Standard authentication mechanism**
  In modern cryptography [1], the authentication is performed on challenge-response method using either symmetric-key algorithm or asymmetric-key algorithm. The standard authentication mechanism requires either TTP or pre-shared secret key. For instance, if one party sends a random number as the challenge to the other party, then the receiver responds the encrypted random number with pre-shared secret key.

- **Authentication using universal hash family**
  Van Assche [2] proposes a cryptosystem based on QKD in his book which describes the authentication protocol that uses a pre-shared key (or bootstrap key) and the information-theoretic MAC (called one-time MAC; OTM). The MAC for authentication protocol is designed using the families of universal hash functions. This scheme provides unconditional security using the OTM. However, the key consumption of this mechanism is exceptionally high and the processing speed is extremely slow.

- **Authentication within BB84 QKD**
  In ICQNM 2015, Rass et al. [3] presented a protocol to authenticate entity’s identity within the process of BB84 protocol. Their protocol, generates a pseudorandom sequence by the private key and insert it into the qubit streaming data via quantum channel. After finishing BB84 QKD successfully, each participant reveals their private keys via special auxiliary public channel and verifies opponent’s pseudorandom sequence. For mutual authentication, their protocol repeats the authentication process in the reverse direction.

3 Authentication mechanism proposal

We propose two mutual authentication mechanisms to solve authentication problems in quantum cryptography. The common features of the two proposed authentication mechanisms are as follows:

- Use pre-shared keys and symmetric-key algorithms to avoid using TTP
- Authentication information is generated using PRNG (pseudorandom number generator; Deterministic random bit generator; DRBG)
- Comply with the international standard according to ISO/IEC 9798 mutual authentication mechanism as much as possible
- The authentication information is inserted in the qubit stream on QKD
  We observe that the authentication information inserted into quantum channel in [3] is fully determined by Alice only.

In order to avoid using arbitrarily generated the authentication information by one party only, we propose authentication mechanisms which generate authentication information from the data exchanged with each other through the challenge-response method and the symmetric-key algorithm. In terms of implementation efforts, with the help of pre-shared key, we are going to solve the inefficiency problem that both parties have to transmit the qubit stream for mutual authentication. The pre-shared key used in the initial entity authentication is refreshed using the output of QKD. The key used once
is always refreshed using the output of QKD. Thus, since the key after the initial entity authentication depends on QKD, the security of the authentication mechanism relies on the security of the quantum cryptography.

The proposed authentication protocols are based on the authentication information generated from DRBG with pre-shared secret so that they are secure against an impersonation attack. The authentication information inserted in the qubit stream is generated using DRBG as follows:

- The length of the interval between adjacent inserted data: \(2^t\) (\(t \in \mathbb{N}\))
- The maximum interval between authentication information: \(m (m \mid 2^t)\)
- Generation seed: \(K_v, K_p, v_0, p_0 = DRBG_{AK}(R_A || R_B)\)
- Authentication information: The value to insert \(v_n\), The position of this to insert \(p_n\)

\[
v_{n+1} = DRBG_{K_v}(v_n) \mod 2^t, \quad p_{n+1} = p_n + 1 + [DRBG_{K_p}(p_n) \mod m]
\]

The main difference between two mechanisms is whether or not additional auxiliary public channel other than the two basic channels (quantum channel, public channel) is required. Fig. 1 shows a model without additional channel, and Fig. 2 depicts a model with additional channel.

**Fig. 1. Mutual authentication without additional channel**

On Fig. 1, step 1-5 is that Alice authenticates Bob by means of a symmetric-key algorithm to verify that Bob possesses the pre-shared secret AK. In Step 6 Alice and Bob generate seed to authenticate Alice using DRBG. In Step 7 Alice inserts its authentication information into a qubit stream. During Step 8-11 Bob authenticates Alice by means of reproduction to verify the Alice’s authentication information in the qubit stream. Because this model does not require additional channel, it has the advantage of being easy to implement.

Most of the steps on Fig. 2 are the same as the steps on Fig. 1. The difference is that \(v_0, p_0\) is not publicly disclosed, so \(v_0, p_0\) must be shared via additional public channel later for authenticating Alice. This model prevents the potential weakness that Bob is already known Alice’s authentication information before receiving the transmission. The additional channel is referred as the auxiliary channel in [3].
4 Conclusion

We propose two mutual entity authentication mechanisms using pre-shared key and QKD. In order to achieve mutual authentication, the proposed mechanism inserts the authentication information into quantum channel. Since the information derived from both participants, we can prevent replay attack, one party’s collusion with outsider, and man-in-the-middle attack. Our proposal provides a solution to authentication problem in quantum cryptography. In addition, this is easy implemented on BB84 QKD by simple modification during the process of Alice’s random encoding.

Acknowledgments. This work was supported by IT R&D program of MSIP/IITP. [10044559, 2014-044-014-002]

References

4. M. Bae, J.S. Kang, Y. Yeom,: A Study on the One-To-Many Authentication Scheme for Cryptosystem Based on Quantum Key Distribution. PlatCon. Korea (to appear)