Chapter 7
Provably Dwindling Three-Party Spurious Classical and Quantum Key Distribution Protocols

Sathya V.
Panimalar Engineering College, India

Kirankumar Manivannan
Easwari Engineering College, India

Prema P.
S.A. Engineering College, India

Saranya S.
Easwari Engineering College, India

Sanjay Misra
Covenant University, Nigeria

ABSTRACT

This chapter presents quantum key distribution protocols (QKDPs) to safeguard security in large networks, ushering in new directions in classical cryptography and quantum cryptography. Two three-party QKDPs, one with implicit user authentication and the other with explicit mutual authentication, are proposed to demonstrate the merits of the new combination, which include the following: 1) Security against such attacks as man-in-the-middle, eavesdropping, and replay, 2) Efficiency is improved as the proposed protocols contain the fewest number of communication rounds among existing QKDPs, and 3) Two parties can share and use a long-term secret (repeatedly). To prove the security of the proposed schemes, this work also presents a new primitive called the unbiased-chosen basis (UCB) assumption.

DOI: 10.4018/978-1-6684-6697-1.ch007

1.INTRODUCTION

Quantum Cryptography is a relatively recent arrival in the Information Security world. It harnesses the laws of Quantum Mechanics to create new cryptographic primitives that offer features either not achievable with 'classical' methods, or which improve on existing techniques. There is, however, one quantum cryptographic primitive which is achievable with today's technology – Quantum Key Distribution (QKD) – which is the focus of this report. Quantum key distribution is the creation of secret keys from quantum mechanical correlations is an example of how physical methods can be used to solve problems in classical information theory. Quantum Key Distribution (QKD) is a method of securely distributing cryptographic key material for subsequent cryptographic use. In particular, it is the sharing of random classical bit strings using quantum states. Its use of a set of non-orthogonal quantum states then requires this key material to be considered quantum information.

The quantum encoding of cryptographic keys for distribution is valuable, because the no-cloning theorem and the superposition principle governing quantum states confer a uniquely powerful form of information security during transmission of key bits as stated by Oleksandr Korchenko et al. (2010). For maximal security, it can be followed by one-time pad message encryption, which is the only cryptographic method that has been proven to be unbreakable once a random key has been securely shared. D. Gottesman et al. (2003) coined that in quantum cryptography, Quantum Key Distribution Protocols (QKDPs) employ quantum mechanisms to distribute quantum keys and public discussions to check for eavesdroppers and verify the correctness of a quantum key. However, public discussions require additional communication rounds between a sender and receiver and cost precious qubits. By contrast, classical cryptography provides convenient techniques that enable efficient key verification and user authentication. Key Distribution Protocols are used to facilitate sharing secret session keys between users on communication networks. By using these shared session keys, secure communication is possible on insecure public networks. However, various security problems exist in poorly designed key distribution protocols. Quantum cryptography easily resists replay and passive attacks, whereas classical cryptography enables efficient key verification and user authentication as described by Nur Atiqah Muhammad et al. (2009). By integrating the advantages of both classical and quantum cryptography, this work presents two QKDPs with the following contributions:

Man-in-the-middle attacks can be prevented, eaves-dropping can be detected, and replay attacks can be avoided easily.

User authentication and session key verification can be accomplished in one step without public discussions between a sender and receiver as the explanation verified from K.-Y. Lam et al. (1992).
The secret key pre shared by a TC and a user can be long term (repeatedly used); and
The proposed schemes are first provably secure QKDPs under the random oracle model.

In the proposed QKDPs, the TC and a participant synchronize their polarization bases according to a pre-shared secret key. During the session key distribution, the pre-shared secret key together with a random string are used to produce another encryption key to encipher the session key. A recipient will not receive the same polarization qubits even if an identical session key is retransmitted. Consequently, the secrecy of the preshared secret key can be preserved and, thus, this preshared secret key can be long term and repeatedly used between the TC and participant. The same idea can be extended to the design