DETERMINISTIC AND EFFICIENT THREE-PARTY QUANTUM KEY DISTRIBUTION

Muneer Alshowkan, Advisor. Prof. Khaled Elleithy

Department of Computer Science and Engineering, University of Bridgeport, Bridgeport, CT, USA
malshowk@my.bridgeport.edu, elleithy@bridgeport.edu

ABSTRACT

The field of quantum computing is based on the laws of quantum mechanics, including states superposition and entanglement. Quantum cryptography is amongst the most surprising applications of quantum mechanics in quantum information processing. Remote state preparation allows a known state to a sender to be remotely prepared at a receiver's location when they prior share entanglement and transmit one classical bit. A trusted authority in a network where every user is only authenticated to the third party distributes a secret key using quantum entanglement parity bit, controlled gates, ancillary states, and transmit one classical bit. We also show it is possible to distribute entanglement in a typical telecom metropolitan optical network.

Index Terms— Quantum, Cryptography, EPR, Security

1. Introduction and Original Idea

Cryptography is the most fundamental element of computer and network security. Security services including confidentiality, authentication, and privacy depend on the techniques of cryptography. Communication security is a subfield which provides a private communication channel between a sender and a receiver. Also, it deters possible intruders from message content. Throughout the history, the invented cryptographic techniques got broke sometime later. In 1926 Vernam invented the one-time pad encryption technique [1] which also called the Vernam cipher. The algorithm is based on symmetric encryption with a long secret key known to the sender and the receiver. Moreover, the one-time pad encryption achieves perfect secrecy when the secret key is not reused. A few decades later, Shannon proved that the one-time pad encryption is ideal and sufficient when the length of the secret key is as long as the plaintext [2]. However, distant parties need a secure method to share the long secret key. The security of current cryptographic techniques is based on hard to solve mathematical problems, but not secure in principle. Current algorithms are adjustable to use more computational power than that available. Hence, a computer with significant power puts the current algorithms at risk. In the past few decades, quantum physics introduced a new type of cryptography. Bennett and Brassard were the first to propose secret key distribution using the properties of quantum mechanics in 1984 [3]. Then, Ekert's idea in 1991 [4] was the trigger of quantum key distribution. As a result, quantum cryptography became an active research topic in theory and experiments. Ten years later, Peter Shor found out manipulating coherent quantum states make it possible to factor large numbers [5]. Hence, factoring large number is a mathematical problem hard to solve using classical computing and public key cryptography such as RSA specifically depends on that problem. Therefore, the abilities of quantum computing put the current cryptographic techniques at risk.

The basic building block of quantum key distribution comprises two distanced parties (traditionally known as Alice and Bob) cooperating together to set up a secret key Fig. 1. Both have access to insecure quantum and authenticated classical channels. Compromising the quantum channel is possible with no limit on the attacker (traditionally known as Eve) who obeys the laws of quantum physics. However, only eavesdropping is possible on the classical channel. Alice and Bob need to protect their quantum channel from Eve during data transmission. For this reason, they either form a secret key with high confidence or they abort the channel. The confidence is based on estimating the quantity of information Eve gained during the communication process. The concept of information leakage from eavesdropping is not available in the classical channels because it goes undetected. In contrast, quantum physics quantifies the information leakage in the quantum channel which making it possible to be detected.

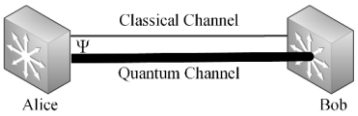

Figure 1. The building block of QKD.

Quantum computing introduces new theories to information security, for instance, measuring quantum bit (qubit) disturbs the original. Unlike copying in classical signals, it is impossible to copy a qubit by no-cloning theorem because measurement affects the original system [7]. Another approach considers separated measurement on entangled states and Bell's inequalities for quantum security. Measurement on correlated qubits violates Bell's theorem and it is impossible to prove that they were created in an earlier agreement. So, measurement did not occur before and an eavesdropper cannot have prior information [4]. Therefore, quantum cryptography provides unconditional without power limitation.

2. The original key idea and Hypothesis

Secure communication by teleporting an unknown quantum state from a sender to a receiver is known to consume two bits of classical communication, given that the sender and the receiver prior share an Einstein-Podolsky-Rosen (EPR) pair. Remote state preparation allows a known quantum state to a sender to be securely prepared at a remote receiver is using one bit of classical communication given that the parties prior shared an EPR pair. Therefore, in a network where every user is authenticated to a trusted authority, but not to each other, establishing a secret key between two users costs the trusted different amount of classical bits EPR pairs. A three-party quantum secret key distribution protocol can be created using parity bits of the EPR pairs, controlled gates, and ancillary states.

Moreover, we study the architecture of metropolitan optical networks (MON) and how to distribute entanglement in a typical telecommunication infrastructure. We analyze the MON architecture to allow simultaneous transmission of classical and quantum signals in the network and provides a dynamic routing mechanism to serve the entire network. The strong launch power of the classical signals impairs the weak quantum signals when they coexist in the same optical fiber. Raman scattering Stokes shift is the major physical impairment on the higher wavelength quantum signals which, caused by the lower wavelength classical signals. Therefore, we also study the physical impairments in the network to reduce the nonlinear effects and improve the quality of the signals. We show an architecture where quantum and classical signals travel in the same optical fiber, but in different spectral bands. Also, we show Raman Stokes-shift wavelength range and the peak power gain when simultaneous transmission of both signals occurs in the same optical fiber. Reducing the physical impairments increases the traveling distance of the signals and the number of the access networks in the MON.

3. Domain and the Specific Problem

Quantum key distribution is the domain of this thesis. The specific problem we are investigating is finding a secure and efficient entanglement-assisted three-party quantum key distribution protocol between two untrusted to each other parties. Also, we investigate the problem of distributing entanglement in typical telecom metropolitan optical network. A centralized EPR source creates then distributes entanglement to users in different access networks. We need to create a dynamic network using reconfigurable optical add/drop multiplexers to serve the entire network. Classical and quantum signals will be travelling in the same network.

4. Methodological Approach

In this thesis, we study quantum cryptography in network communications for secret key distribution. Specifically, the security and efficacy of entanglement-assisted three-party quantum key distribution. Using the formal methodological approach, we study how the entanglement-assisted quantum key distribution protocols consume the communication resource. Then, we create a three-party quantum key distribution protocol to establish secret keys between two users unauthenticated to each other. The parity bit of the shared EPR pairs is used by quantum controlled gates and ancillary states to reduce the classical bit communication. We show that the parity bits and the ancillary states provide a secure communication channel and reduce the classical communication consumption in the key distribution process. Any action from the attacker Eve over the channel presents noise which can be unambiguously detected. Also, using privacy amplification passive leakage is eliminated. The distribution process between the parties provides secure key distribution and with efficient classical communication.

5. Current research and Expected Result

Our preliminary results in three-party quantum key distribution have several conferences. Recently, in [6] we presented a MON architecture for dynamic entanglement distribution. Also, in [7] quantum mutual authentication and key distribution using entanglement swapping and Bell's state measurement. In [8] we presented a three-party QKD protocol based on the BB84. In [9] we presented a protocol based on entanglement swapping which consumed six classical bits per qubit. The protocol in [10] is based on RSP and entanglement swapping with classical bit consumption of five bits per qubit. In the remaining work, using EPR parity bit, controlled states and ancillary states in a three-party QKD we are expecting to achieve classical consumption of one classical bit of communication for each qubit in the secret key.

6. REFERENCES

[1] G. S. Vernam, "Cipher printing telegraph systems: For secret wire and radio telegraphic communications," AIEE, vol. 45, pp. 109-115, 1926.

[2 C. E. Shannon, "Communication theory of secrecy systems," Bell system technical journal, vol. 28, pp. 656-715, 1949.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theor. Comput. Sci., vol. 560, no. P1, pp. 7–11, Dec. 2014.

[4] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Physical review letters, vol. 67, pp. 661, 1991.

[5] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM journal on computing, vol. 26, pp. 1484-1509, 1997.

[6] M. Alshowkan and K. Elleithy, "Quantum Entanglement Distribution for Secret Key Establishment in Metropolitan Optical Networks," in IEEE International Conference (NAS), Long Beach, pp. 1-8, 2016.

[7] M. Alshowkan and K. Elleithy, "Quantum mutual authentication scheme based on Bell state measurement," in IEEE Long Island Conference (LISAT), Long Island, pp. 1-6, 2016.

[8] M. Alshowkan, K. Elleithy, A. Odeh, and E. Abdelfattah, "A new algorithm for three-party quantum key distribution," in IEEE Third International Conference (INTECH), London, pp. 208-212, 2013.

[9] M. Alshowkan and K. Elleithy, "Authenticated multiparty secret key sharing using quantum entanglement swapping," in American Society for Engineering Education, Bridgeport, pp. 1-6, 2014.

[10] M. Alshowkan and K. Elleithy, "Secret key sharing using entanglement swapping and remote preparation of quantum state," in IEEE Long Island Conference (LISAT), Long ISland, pp. 1-6, 2014.