Secure Ballots Using Quantum Cryptography

Lester Houston III [les45ismore@yahoo.com]

Abstract

Quantum cryptography is an emerging technology in the field of cryptographic systems where quantum mechanics is used to guarantee secure communication between two parties. In simple terms, quantum cryptography uses the principles of quantum mechanics to provide communication between two parties where eavesdropping can be detected by both the sender and the receiver. The first commercial application is applied towards securing electronic ballots. This paper will discuss what is needed to make electronic ballots secure, how quantum cryptography is used to make electronic ballots secure, the principles that make quantum cryptography secure and the quantum key distribution protocols used to perform quantum key distribution. This paper will also discuss the flaws of quantum cryptographic systems along with the plans for enhancing current quantum cryptographic systems.

Keywords

Quantum Cryptography, cryptography, secure ballots, electronic ballots, electronic voting, quantum key distribution, BB84 encoding scheme, B92 encoding scheme, Ekert encoding scheme, information reconciliation, privacy amplification, Heisenberg's uncertainty principle, denial of service, man-in-the-middle.

Table of Contents

---

1 Introduction

Quantum cryptography is an emerging technology in the field of cryptographic systems where quantum mechanics is used to guarantee secure communication between two parties. Quantum cryptographic systems seem to offer an unbreakable way to secure communication in a way that eavesdropping by a third party is detectable, if you can understand the quantum mechanics ensuring this guarantee, such as Heisenberg's Uncertainty Principle and quantum entanglement.QC systems encode information in the quantum properties of photons, using one of the three protocols discussed in later sections: BB83 encoding scheme, B92 encoding scheme or the Ekert encoding scheme.

Although quantum cryptography has great potential, it is not a good choice for encrypting and decrypting an entire conversation because of its range and payload limitations. As a result quantum cryptography's primary function is for exchanging secret keys where an encryption method such as AES or triple-DES is used to encrypt and decrypt the rest of the conversation. Also, the quantum mechanic principles used are based on the single photons, but current QC implementations send bursts of protons, so additional methods are used to increase the level of security offered, such as information reconciliation and privacy amplification.

Currently, the Swiss community is using quantum cryptographic systems to secure electronic ballots in public elections, although quantum cryptographics is still considered experimental. Advances in this field are still being made along with ways to implement this technology in a wireless environment. As promising as quantum cryptographics may be, before it can be used to secure electronic ballots, one must know what makes electronic ballots secure.

Back to Table of Contents

---

2 Quantum Cryptograpy

The basic quantum cryptography (QC) technology was originally developed by Charles Bennett, an IBM research staff member and IBM fellow, along with Giles Brassard of the University of Montreal in 1984. Their initially developed quantum cryptographic box was called BB84. The BB84 has been the basis for the majority of current implementations of quantum cryptographic systems. As implied in the name, quantum cryptographic technology uses quantum mechanics (specifically the Heisenberg Uncertainty Principle and Quantum Superposition or Quantum Entanglement). These fundamental quantum mechanic principles are used in combination with Privacy Amplification and Information Reconciliation to make quantum cryptography secure. Information exchange within a quantum cryptographic system consists of encoding information into protons in a way that interception or monitoring by a third party is detectable by the sender and recipient.

2.1. Quantum Key Distribution

The major difference between QC technology and traditional cryptographic technology is that the QC relies on the laws of physics, specifically the laws of quantum mechanics, to provide a secure system, while traditional cryptographic systems rely on the computational difficulty of the encryption methods employed to provide a secure system. The laws of quantum physics make QC secure because of the following principles [Llp07].

- Anyone directly trying to measure the bit value of a photon will introduce errors that can be detected by both the sender and the receiver.
- A single photon cannot be divided, which means that an eavesdropper cannot split a quantum photon to make measurements secretly.
- A single photon cannot be cloned, copied or duplicated so no one could clone a photon to measure it while passing another.

Quantum key distribution (QKD) involves observing quantum states, where photons are put in a particular state by the sender and observed by the recipient. There are two different approaches to creating a quantum cryptographic system, polarized photons and entangled photons. This two approaches result in three different types of quantum

cryptographic encoding protocols: BB84, B92 and the Ekert scheme.

2.1.1. BB84 Encoding Scheme

The typical way of encoding quantum information is by transmission of photons in some polarization states [Unk01]. Photon polarization is the quantum mechanical description of the classical polarized sinusoidal plane electromagnetic wave [Jones06]. Polarization in general, is the property of electromagnetic waves describing the direction of oscillation in the plane perpendicular to the direction of travel. The protocol developed using polarized photons, known as BB84, was developed by Charles Bennett and Giles Brassard, uses Heisenberg's Uncertainty Principle. The Heisenberg's Uncertainty Principle states that it's possible to encode information into the quantum properties of any substance particle in a way that any attempt to measure or monitor them would also disturb them in a detectable manner. In other words, information can be encoding into the quantum properties a particle, such as a photon, such that when the particle is measured, the quantum state of that particle will change in a detectable way. As stated before, in QKD, photons are placed into a particular state by the sender and observed by the recipient. Using Heisenberg's Uncertainty Principle, certain quantum information cannot be measured or observed at the same time [Ford96]. These pieces of quantum information that cannot be measured simultaneously are called conjugates, which are complimentary properties on a quantum photon. In polarization, these conjugates are expressed in three different bases, rectilinear, circular, and diagonal. Observing one these bases will randomize all other conjugates so the sender and the receiver must agree on the basis of the quantum system they will be using, otherwise the receiver may accidentally destroy the sender's information before using it.

The security of the BB84 protocol comes from encoding the quantum information in non-orthogonal states, where BB84 uses two pairs of states with each pair conjugate to the other and the two within a pair being orthogonal to each other. The typical polarization state pairs used are rectilinear basis of vertical (0°) and horizontal (90°), the diagonal basis of 45° and 135° or the circular basis of left- and right-handed. All three of these bases are conjugate to each other, so any two can be used together. The typical polarization state pairs are shown below in Table 1. The BB84 protocol uses the rectilinear and diagonal states.

Table 1: Typical Polarization State Pairs

Basis	Representation	Random Bit 0	Random Bit 1
Rectilinear	+		
Diagonal	X		
Circular	O		

When encoding with the BB84 protocol, Alice (the sender), creates a random bit 0 or 1 and then randomly selects one her two bases to transmit it in. She then creates a polarization state depending on both the random bit value chosen and the basis chosen. She then transmits a single photon to Bob, the receiver. The process is then repeated with Alice recording the state, basis and time of each photon sent. Bob does not know the basis the photons sent by Alice were encoded in so he selects a random basis to measure each photon, either rectilinear or diagonal. For each photon that Bob receives, he records the time and measurement basis used. After the photon transmission has ended, Alice broadcasts the basis used for each photon while Bob broadcasts the basis used to measure each photon. Both Alice and Bob discard the photons where Bob used a different basis for measurement then Alice used for encoding, which is half on average. The remaining bits are used as a shared key to encrypt and decrypt their conversation using some other cryptographic algorithm.