Quantum Cryptography Protocols for Information Security

Göran Pulkkis
Arcada Polytechnic, Finland

Kaj J. Grahn
Arcada Polytechnic, Finland

INTRODUCTION

Quantum cryptography will have a severe impact on information security technology. The objective of this article is to present state-of-the-art and future possibilities of two quantum cryptography protocol types. These protocols are for absolutely secure distribution of symmetric encryption/decryption keys and for creating secure digital signatures.

BACKGROUND

In the early 1980s, it was observed that the stochastic parallelism of quantum states cannot be simulated efficiently on a classical computer (Feynman, 1982). This observation started research on using quantum mechanical effects for more efficient information processing than is achievable with classical computers. During the 1980s, the operating principles and implementation possibilities of quantum computing were outlined at Oxford University (Deutsch, 1985). In 1984, a quantum protocol for information transfer with provable confidentiality was proposed (Bennett & Brassard, 1984). This protocol, called the BB84 protocol, uses quantum states implemented by randomly polarized photons.

In the 1990s, efficient algorithms based on the operating principles of quantum computing were proposed. Shor's quantum algorithm for integer factorization (Shor, 1994) has polynomial (cubic) computational complexity and has been experimentally verified in a quantum computer with seven qubits implemented using nuclear magnetic resonance (Vandersypen, Steffen, Breyta, Yannoni, Sherwood, & Chang, 2001). Search with Grover's (1996) quantum algorithm in an unsorted database has only square root computational complexity. The BB84 protocol has been used for secure distribution of symmetric encryption/decryption keys (Quantum Key Distribution, QKD) in research networks (BBN Technologies, 2005; Elliot, 2004; Quellette, 2005;). For some years also commercial QKD technology has been available (id Quantique Portal, 2005; MagiQ, 2005).

The RSA algorithm is often used to create digital signatures. RSA is secure because the best known factorization method for large integers has superpolynomial computational complexity in a classical computer. False signed messages could however be created with a sufficiently large quantum computer since the private signing key could easily be computed with Shor's algorithm from the corresponding public key. On the other hand, secure digital signatures could be created by manipulation and measurements of quantum states (Gottesman & Chuang, 2001; Lu & Feng, 2005).

INFORMATION REPRESENTATION WITH QUANTUM STATES

Quantum states are energy levels of molecules, atoms, and photons. Two quantum states for which a state transition exists can be used to represent an information bit, if the energy levels of both states can be measured. A bit defined by quantum states is called a quantum bit or qubit. However, quantum states are probabilistic. When the energy level of a molecule, an atom, or a photon is measured, the outcome is one of all possible energy levels, and each possible outcome is associated with a probability. The sum of the probabilities of all possible measurement outcomes is, of course, 1. A qubit is thus also probabilistic. The binary values 0 and 1 are represented by two possible quantum states of a qubit. If the measurement probabilities of these two quantum states are p_0 and p_1, then $p_0+p_1=1$.

Properties of Quantum Bits (Qubits)

A qubit can be treated mathematically by linear algebra as a 2-dimensional vector. The orthogonal base vectors $(1,0)^T$ and $(0,1)^T$ represent the quantum states associated with the binary values 0 and 1, respectively. Usually the **Dirac Notation** is used for qubits as well as for these two orthogonal base vectors, thus $(1,0)^T = |0\rangle$ and $(0,1)^T = |1\rangle$.

A qubit is a superposition of $|0\rangle$ and $|1\rangle$ and both values are simultaneously present. A measured qubit is set to the measured value, which is $|0\rangle$ or $|1\rangle$. Let $|\psi\rangle$ be a qubit in Dirac Notation. Then

$$|\psi> = a\cdot|0> + b\cdot|1> \quad (1)$$

where a and b are complex numbers for which

$$<\psi||\psi> = (a^*,b^*)\cdot(a,b)^T = a^*\cdot a + b^*\cdot b = |a|^2 + |b|^2 = 1, \quad (2)$$

{a*,b*} are complex conjugates of {a,b}, and $\{|a|^2,|b|^2\}$ are the probabilities to measure the values 0,1, respectively. A qubit has thus three dimensions because complex numbers have two dimensions. From this follows further, that a qubit can be presented geometrically as a point on a 3-dimensional unit sphere.

A fundamental qubit property is the No Cloning Property, according to which it is impossible to clone an unknown quantum state (Nielsen & Chuan, 2002).

Multiple Qubits

The quantum state of **2 qubits** is a column vector with $2^2 = 4$ components. For the qubits

$$|\psi_1> = a\cdot|0> + b\cdot|1> \text{ and } |\psi_2> = c\cdot|0> + d\cdot|1> \quad (3)$$

the quantum state is

$$|y_1y_2> = |\psi_1> \otimes |\psi_2> = a\cdot c\cdot|00> + a\cdot d\cdot|01> + b\cdot c\cdot|10> + b\cdot d\cdot|11> \quad (4)$$

where $\otimes$ is the **tensor product** of two column vectors. In such a product, the result vector is obtained by multiplying the latter vector with each component in the first vector, see the following examples: $|00> = |0>\otimes|0> = (1,0,0,0)^T$, $|01> = |0>\otimes|1> = (0,1,0,0)^T$, $|10> = |1>\otimes|0> = (0,0,1,0)^T$, and $|11> = |1>\otimes|1> = (0,0,0,1)^T$ are called the **base vectors** of the 2 qubit state.

An **N qubit** quantum state $|\psi_1\psi_2\ldots\psi_N>$ is a superposition of 2^N base vectors. For a three qubit quantum state $|\psi_1\psi_2\psi_3>$ the 2^3 base vectors are {|000>,|001>,|010>,|011>, |100>,|101>, |110>,|111>}, where $|001> = |0>\otimes|0>\otimes|1> = (0,1,0,0,0,0,0,0)^T$, and so forth.

The qubit state $|\psi_1\psi_2\ldots\psi_N>$ is an **entangled state** if there exists no $|\psi_1>,|\psi_2>,\ldots,|\psi_N>$ for which $|\psi_1\psi_2\ldots\psi_N> = |\psi_1>\otimes|\psi_1>\otimes\ldots\otimes|\psi_N>$.

Example: The 2 qubit state $2^{-½}$ (|00> + |11>) is entangled.

Proof: $(a\cdot|0>+b\cdot|1>)\otimes(c\cdot|0>+d\cdot|1>) = a\cdot c\cdot|00>+a\cdot d\cdot|01>+b\cdot c\cdot|10>+b\cdot d\cdot|11> \neq 2^{-½}\cdot(|00> + |11>)$, since one of {a,d} and one of {b,c} must be 0.

Physical Implementation of Qubits

Qubits have been implemented by ion traps, by cavity quantum electrodynamics (QED), by nuclear magnetic resonance (NMR), and by quantum dots (Nielsen & Chuang, 2002).

A qubit is implemented by the **polarization state** of a photon in practical quantum cryptography. A polarization state consists of all planes in which the electromagnetic wave of a photon propagates. The polarization of a randomly polarized photon is a superposition of any pair of orthogonal states. Examples of orthogonal polarization state pairs are:

- horizontal and vertical polarization;
- +45° and -45° diagonal polarization.

The polarization of a photon can thus be modeled by a qubit $|\psi>$ for which

$$|\psi> = a\cdot|horis> + b\cdot|vert> = c\cdot|+45°> + d\cdot|-45°> \quad (5)$$

where a,b,c,d are complex numbers and $|a|^2 + |b|^2 = |c|^2 + |d|^2 = 1$. One polarization state must be interpreted as |0> and the other state as |1> for a chosen orthogonal state pair. For example,

- |horis> = |0> and |vert> = |1>
- |+45°> = |0> and |-45°> = |1>.

Notice also that (c,d) can be calculated from (a,b) and vice versa since

$$|+45°> = 2^{-½}(|horis> + |vert>), \; |-45°> = 2^{-½}(|horis> - |vert>). \quad (6)$$

The polarization of a photon is measured with a filter. After measurement, only the component defined by the filter can pass through. For example, the polarization will change to $|\psi> = |horis>$ when a photon with polarization $|\psi> = a\cdot|horis> + b\cdot|vert>$ passes through a horizontal filter. If a=0 and b=1, then the photon is absorbed by a horizontal filter.

A consequence of the No Cloning Property of a qubit is that an unknown polarization state of a photon cannot be copied to any other photon.

QUANTUM INFORMATION PROCESSING

Quantum Gates and Circuits

Qubit states are changed with quantum gates. Basic single qubit quantum gates are: