View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by IntechOpen

# We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

**4,800**
Open access books available

**122,000**
International authors and editors

**135M**
Downloads

Our authors are among the

**154**
Countries delivered to

**TOP 1%**
most cited scientists

**12.2%**
Contributors from top 500 universities

CLARIVATE ANALYTICS BOOK CITATION INDEX INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

## Interested in publishing with us?
## Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Chapter 5

# Introduction to Quantum Cryptography

Xiaoqing Tan

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/56092

## 1. Introduction

Broadly speaking, cryptography is the problem of doing communication or computation involving two or more parties who may not trust one another. The best known cryptographic problem is the transmission of secret messages. Suppose wish to communicate in secret. For example, you may wish to give your credit card number to a merchant in exchange for goods, hopefully without any malevolent third party intercepting your credit card number. The way this is done is to use a cryptographic protocol. The most important distinction is between private key cryptosystems and public key cryptosystems.

The way a private key cryptosystem works is that two parties, 'Alice' and 'Bob', wish to communicate by sharing a private key, which only they know. The exact form of the key doesn't matter at this point – think of a string of zeroes and ones. The point is that this key is used by Alice to encrypt the information she wishes to send to Bob. After Alice encrypts she sends the encrypted information to Bob, who must now recover the original information. Exactly how Alice encrypts the message depends upon the private key, so that to recover the original message Bob needs to know the private key, in order to undo the transformation Alice applied.

Unfortunately, private key cryptosystems have some severe problems in many contexts. The most basic problem is how to distribute the keys? In many ways, the key distribution problem is just as difficult as the original problem of communicating in private – a malevolent third party may be eavesdropping on the key distribution, and then use the intercepted key to decrypt some of the message transmission.

One of the earliest discoveries in quantum computation and quantum information was that quantum mechanics can be used to do key distribution in such a way that Alice and Bob's security cannot be compromised. This procedure is known as **quantum cryptography** or **quantum key distribution** (abbreviated QKD). The basic idea is to exploit the quantum mechanical principle that observation in general disturbs the system being observed. Thus, if

INTECH
open science | open minds

© 2013 Tan; licensee InTech. This is an open access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

there is an eavesdropper listening in as Alice and Bob attempt to transmit their key, the presence of the eavesdropper will be visible as a disturbance of the communications channel Alice and Bob are using to establish the key. Alice and Bob can then throw out the key bits established while the eavesdropper was listening in, and start over.

The first quantum cryptographic ideas were proposed by Stephen Wiesner wrote "Conjugate Coding"[1], which unfortunately took more than ten years to see the light of print. In the mean time, Charles H. Bennett (who knew of Wiesner's idea) and Gilles Brassard picked up the subject and brought it to fruition in a series of papers that culminated with the demonstration of an experimental prototype that established the technological feasibility of the concept [2]. Quantum cryptographic systems take advantage of Heisenberg's uncertainty principle, according to which measuring a quantum system in general disturbs it and yields incomplete information about its state before the measurement. Eavesdropping on a quantum communication channel therefore causes an unavoidable disturbance, alerting the legitimate users. This yields a cryptographic system for the distribution of a secret random cryptographic key between two parties initially sharing no secret information that is secure against an eavesdropper having at her disposal unlimited computing power. Once this secret key is established, it can be used together with classical cryptographic techniques such as the one-time-pad (OTP) to allow the parties to communicate meaningful information in absolute secrecy.

The second major type of cryptosystem is the public key cryptosystem. Public key cryptosystem don't rely on Alice and Bob sharing a secret key in advance. Instead, Bob simply publishes a 'public key', which is made available to the general public. Alice can make use of this public key to encrypt a message which she sends to Bob. The third party cannot use Bob's public key to decrypt the message. Public key cryptography did not achieve widespread use until the mid-1970s, when it was proposed independently by Whitfield Diffie and Martin Hellman, Rivest, Adi Shamir, and Leonard Adleman developed the RSA cryptosystem, which at the time of writing is the most widely deployed public key cryptosystem, believed to offer a fine balance of security and practical usability.

The key to the security of public key cryptosystems is that it should be difficult to invert the encryption stage if only the public key is available. For example, it turns out that inverting the encryption stage of RSA is a problem closely related to factoring. Much of the presumed security of RSA comes from the belief that factoring is a problem hard to solve on a classical computer. However, Shor's fast algorithm for factoring on cryptosystems which can be broken if a fast algorithm for solving the discrete logarithm problem – like Shor's quantum algorithm for discrete logarithm – were known. This practical application of quantum computers to the breaking of cryptographic codes has excited much of the interest in quantum computation and quantum information.

In addition to key distribution, quantum techniques may also assist in the achievement of subtler cryptographic goals, important in the post-cold war world, such as protecting private information while it is being used to reach public decisions. Such techniques, pioneered by Claude Crepeau [3] [4], allow two people to compute an agreed-upon function $f(x; y)$ on private inputs $x$ and $y$ when one person knows $x$, the other knows $y$, and neither is willing to disclose anything about their private input to the other, except for what follows logically from one's

http://dx.doi.org/10.5772/56092

private input and the function's output. The classic example of such discreet decision making is the "dating problem", in which two people seek a way of making a date if and only if each likes the other, without disclosing any further information. For example, if Alice likes Bob but Bob doesn't like Alice, the date should be called off without Bob finding out that Alice likes him, on the other hand, it is logically unavoidable for Alice to learn that Bob doesn't like her, because if he did the date would be on.

In general, the goal of quantum cryptography is to perform tasks that are impossible or intractable with conventional cryptography. Quantum cryptography makes use of the subtle properties of quantum mechanics such as the quantum no-cloning theorem and the Heisenberg uncertainty principle. Unlike conventional cryptography, whose security is often based on unproven computational assumptions, quantum cryptography has an important advantage in that its security is often based on the laws of physics. Thus far, proposed applications of quantum cryptography include QKD, quantum bit commitment and quantum coin tossing. These applications have varying degrees of success. The most successful and important application – QKD – has been proven to be unconditionally secure. Moreover, experimental QKD has now been performed over hundreds of kilometers over both standard commercial telecom optical fibers and open-air. In fact, commercial QKD systems are currently available on the market [5].

Classical secret sharing can be used in a number of ways besides for a joint checking account. The secret key could access a bank vault, or a computer account, or any of a variety of things. In addition, secret sharing is a necessary component for performing secure distributed computations among a number of people who do not completely trust each other. With the boom in quantum computation, it seems possible, even likely, that quantum states will become nearly as important as classical data. It might therefore be useful to have some way of sharing secret quantum states as well as secret classical data. Such a **quantum secret sharing** (abbreviated QSS) scheme might be useful for sharing quantum keys, such as those used in quantum key distribution or in other quantum cryptographic protocols. In addition, QSS might allow us to take advantage of the additional power of quantum computation in secure distributed computations.

Imagine that it is fifteen years from now and someone announces the successful construction of a large quantum computer. The New York Times runs a front-page article reporting that all of the public-key algorithms used to protect the Internet have been broken by quantum computer. Perhaps, after seeing quantum computers destroy RSA and DSA and ECDSA, Internet users will leap to the conclusion that cryptography is dead. For solving the problem, some researchers provided the idea about **post-quantum cryptography** which refers to research on cryptographic primitives (usually public-key cryptosystems) that are not breakable using quantum computers. This term came about because most currently popular public-key cryptosystems rely on the integer factorization problem or discrete logarithm problem, both of which would be easily solvable on large enough quantum computers using Shor's algorithm [6] [7]. Even though current publicly known experimental quantum computing is nowhere near powerful enough to attack real cryptosystems, many cryptographers are researching new algorithms, in case quantum computing becomes a threat in the future. This work is popularized by the PQCrypto conference series since 2006.

In the past few years, a remarkable surge of interest in the international scientific and industrial community has propelled quantum cryptography into mainstream computer science and physics. Furthermore, quantum cryptography is becoming increasingly practical at a fast pace. The first quantum key distribution prototype [2] worked over a distance of 32 centimeters in 1989. Two additional experimental demonstrations have been set up since, which work over significant lengths of optical fibre [8] [9]. The highest bit rate system currently demonstrated exchanges secure keys at 1 Mbit/s (over 20 km of optical fibre) and 10 kbit/s (over 100 km of fibre), achieved by a collaboration between the University of Cambridge and Toshiba using the BB84 protocol with decoy pulses.

As of March 2007 the longest distance over which quantum key distribution has been demonstrated using optic fibre is 148.7 km, achieved by Los Alamos National Laboratory/NIST using the BB84 protocol. Significantly, this distance is long enough for almost all the spans found in today's fibre networks. The distance record for free space QKD is 144 km between two of the Canary Islands, achieved by a European collaboration using entangled photons (the Ekert scheme) in 2006, and using BB84 enhanced with decoy states in 2007. The experiments suggest transmission to satellites is possible, due to the lower atmospheric density at higher altitudes. For example although the minimum distance from the International Space Station to the ESA Space Debris Telescope is about 400 km, the atmospheric thickness is about an order of magnitude less than in the European experiment, thus yielding less attenuation compared to this experiment.

## 2. Quantum cryptography fundamentals

On a wider context, quantum cryptography is a branch of quantum information processing, which includes quantum computing, quantum measurements, and quantum teleportation. Quantum computation and quantum information is the study of the information processing tasks that can be accomplished using quantum mechanical systems.

Quantum mechanics is a mathematical framework or set of rules for the construction of physical theories. The rules of quantum mechanics are simple but even experts find them counterintuitive, and the earliest antecedents of quantum computation and quantum information may be found in the long-standing desire of physicists to better understand quantum mechanics. Perhaps the most striking of these is the study of quantum entanglement. Entanglement is a uniquely quantum mechanical resource that plays a key role in many of the most interesting applications of quantum computation and quantum information; entanglement is iron to the classical world’s bronze age. In recent years there has been a tremendous effort trying to better understand the properties of entanglement considered as a fundamental resource of Nature, of comparable importance to energy, information, entropy, or any other fundamental resource. Although there is as yet no complete theory of entanglement, some progress has been made in understanding this strange property of quantum mechanics. It is hoped by many researchers that further study of the properties of entanglement will yield insights that facilitate the development of new applications in quantum computation and quantum information.

As we known, it is interesting to learn that one decade before people realized that a quantum computer could be used to break public key cryptography, they had already found a solution

against this quantum attack – quantum key distribution (QKD). Based on the fundamental principles in quantum physics, QKD provides an unconditionally secure way to distribute random keys through insecure channels. The secure key generated by QKD could be further applied in the OTP scheme or other encryption algorithms to enhance information security. In this chapter, we will introduce the fundamental principles behind various QKD or QSS and present the state-of-the art quantum cryptography technologies.

### 2.1. Entanglement state

The counterintuitive predictions of quantum mechanics about correlated systems were first discussed by Albert Einstein in 1935, in a joint paper with Boris Podolsky and Nathan Rosen [10]. They demonstrated a thought experiment that attempted to show that quantum mechanical theory was impossible.

But flowing the EPR paper, Erwin Schrodinger wrote letter (in German) to Einstein in which he used the word Verschrankung (translated by himself as entanglement) "to describe the correlations between two particles that interact and then separate, as in the EPR experiment" [11]. He shortly thereafter published a seminal paper defining and discussing the notion, and terming it "entanglement".

Entanglement is usually created by direct interactions between subatomic particles. These interactions can take numerous forms. One of the most commonly used methods is spontaneous parametric down-conversion to generate a pair of photons entangled in polarization [12]. Other methods include the use of a fiber coupler to confine and mix photons, the use of quantum dots to trap electrons until decay occurs, the use of the Hong-Ou-Mandel effect, etc. In the earliest tests of Bell's theorem, the entangled particles were generated using atomic cascades. It is also possible to create entanglement between quantum systems that never directly interacted, through the use of entanglement swapping.

Consider two noninteracting systems $A$ and $B$, with respective Hilbert spaces $H_A$ and $H_B$. The Hilbert space of the composite system is the tensor product $H_A \otimes H_B$. If the first system is in state $|\psi\rangle_A$ and the second in state $|\psi\rangle_B$, the state of the composite system is $|\psi\rangle_A \otimes |\psi\rangle_B$. States of the composite system which can be represented in this form are called separable states, or product states. Not all states are separable states. Fix a basis $\{|i\rangle_A\}$ for $H_A$ and a basis $\{|j\rangle_B\}$ for $H_B$. The most general state in $H_A \otimes H_B$ is the form of

$$|\psi\rangle_{AB} = \sum_{i,j} C_{ij} |i\rangle_A \otimes |j\rangle_B \tag{1}$$

This state is separable if $c_{ij} = c_i^A c_j^B$ yielding $|\psi\rangle_A = \sum_i c_i^A |i\rangle_A$ and $|\phi\rangle_B = \sum_j c_j^B |j\rangle_B$. It is inseparable if $c_{ij} \neq c_i^A c_j^B$ If a state is inseparable, it is called an entangled state. For example, given two basis vectors $\{|0\rangle_A, |1\rangle_A\}$ of $H_A$and two basis vectors $\{|0\rangle_B, |1\rangle_B\}$ of $H_B$, the following is an entangled state:

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \tag{2}$$

If the composite system is in this state, it is impossible to attribute to either system $A$ or system $B$ a definite pure state. Another way to say this is that while the von Neumann entropy of the whole state is zero, the entropy of the subsystems is greater than zero. In this sense, the systems are "entangled". This has specific empirical ramifications for interferometry [13]. It is worthwhile to note that the above example is one of four Bell states, which are maximally entangled pure states.

### 2.2. One-time-pad and key distribution problem

In conventional cryptography, an unbreakable code does exist. It is called the one-time-pad and was invented by Gilbert Vernam in 1918 [14]. In the one-time-pad method, a message (traditionally called the plain text) is first converted by Alice into a binary form (a string consisting of "0"s and "1"s) by a publicly known method. A key is a binary string of the same length as the message. By combining each bit of the message with the respective bit of the key using XOR (i.e. addition modulo two), Alice converts the plain text into an encrypted form (called the cipher text). i.e. for each bit

$$c_i \equiv m_i + k_i \pmod 2. \tag{3}$$

Alice then transmits the cipher text to Bob via a broadcast channel. Anyone including an eavesdropper can get a copy of the cipher text. However, without the knowledge of the key, the cipher text is totally random and gives no information whatsoever about the plain text. For decryption, Bob, who shares the same key with Alice, can perform another XOR (i.e. addition modulo two) between each bit of the cipher text with the respective bit of the key to recover the plain text. This is because

$$c_i \equiv m_i + k_i \equiv m_i + 2k_i \equiv m_i \pmod 2. \tag{4}$$

The one-time-pad method is unbreakable, but it has a serious drawback: it supposes that Alice and Bob initially share a random string of secret that is as long as the message. Therefore, the one-time-pad simply shifts the problem of secure communication to the problem of key distribution. This is the key distribution problem. The one of possible solution to the key distribution problem is public key cryptography.

Quantum mechanics can provide a solution to the key distribution problem. In quantum key distribution, an encryption key is generated randomly between Alice and Bob by using non orthogonal quantum states. In quantum mechanics there is a quantum no-cloning theorem, which states that it is fundamentally impossible for anyone including an eavesdropper to make an additional copy of an unknown quantum state. Therefore, any attempt by an eavesdropper

to learn information about a key in a QKD process will lead to disturbance, which can be detected by Alice and Bob who can, for example, check the bit error rate of a random sample of the raw transmission data.

### 2.3. Quantum no-cloning theorem

The quantum no-cloning theorem was stated by Wootters, Zurek, and Dieks in 1982, and has profound implications in quantum computing and related fields.

**Theorem (Quantum no-cloning theorem)** An arbitrary quantum state cannot be duplicated perfectly.

**Proof:** Suppose the state of a quantum system A, which we wish to copy, is $|\psi\rangle_A$. In order to make a copy, we take a system B with the same state space and initial state $|e\rangle_B$. The initial, or blank, state must be independent of $|\psi\rangle_A$, of which we have no prior knowledge. The composite system is then described by the tensor product, and its state is $|\psi\rangle_A|e\rangle_B$.

There are only two ways to manipulate the composite system. We could perform an observation, which irreversibly collapses the system into some eigenstate of the observable, corrupting the information contained in the qubit. This is obviously not what we want. Alternatively, we could control the Hamiltonian of the system, and thus the time evolution operator $U$ (for a time independent Hamiltonian, $U(t)=e^{-iHt/\hbar}$, where $-H/\hbar$ is called the generator of translations in time) up to some fixed time interval, which yields a unitary operator. Then $U$ acts as a copier provided that

$$U|\phi\rangle_A|e\rangle_B = |\phi\rangle_A|\phi\rangle_B, \tag{5}$$

for all possible states $|\phi\rangle$ in the state space (including $|\psi\rangle$). Since $U$ is unitary, it preserves the inner product:

$$\langle e|_B\langle\phi|_A|\psi\rangle_A|e\rangle_B = \langle e|_B\langle\phi|_A U^{\dagger}U|\psi\rangle_A|e\rangle_B = \langle\phi|_B\langle\phi|_A|\psi\rangle_A|\psi\rangle_B, \tag{6}$$

and since quantum mechanical states are assumed to be normalized, it follows that $\langle\phi|\psi\rangle=\langle\phi|\psi\rangle^2$.

This implies that either $\phi=\psi$ (in which case $\langle\phi|\psi\rangle=1$) or $\phi$ is orthogonal to $\psi$ (in which case $\langle\phi|\psi\rangle=0$ ). However, this is not the case for two arbitrary states. While orthogonal states in a specifically chosen basis $\{|0\rangle, |1\rangle\}$, for example, $|\phi\rangle=1/\sqrt{2}(|0\rangle+|1\rangle)$ and $|\psi\rangle=1/\sqrt{2}(|0\rangle-|1\rangle)$ fit the requirement that$\langle\phi|\psi\rangle=\langle\phi|\psi\rangle^2$, this result does not hold for more general quantum states. Apparently $U$ cannot clone a general quantum state.

Quantum no-cloning theorem is a direct result of the linearity of quantum physics. It is closely related to another important theorem in quantum mechanics, which states: if a measurement

allows one to gain information about the state of a quantum system, then in general the state of this quantum system will be disturbed, unless we know in advance that the possible states of the original quantum system are orthogonal to each other.

At first sight, the impossibility of making perfect copies of unknown quantum states seems to be a shortcoming. Surprisingly, it can also be an advantage. It turned out that by using this impossibility smartly, unconditionally secure key distribution could be achieved: any attempts by the eavesdropper to learn the information encoded quantum mechanically will disturb the quantum state and expose her existence. Specially, we can get the following characteristics about quantum no-cloning theorem:

- The no-cloning theorem prevents us from using classical error correction techniques on quantum states. For example, we cannot create backup copies of a state in the middle of a quantum computation, and use them to correct subsequent errors. Error correction is vital for practical quantum computing, and for some time this was thought to be a fatal limitation. In 1995, Shor and Steane revived the prospects of quantum computing by independently devising the first quantum error correcting codes, which circumvent the no-cloning theorem.

- Similarly, cloning would violate the no teleportation theorem, which says classical teleportation (not to be confused with entanglement-assisted teleportation) is impossible. In other words, quantum states cannot be measured reliably.

- The no-cloning theorem does not prevent superluminal communication via quantum entanglement, as cloning is a sufficient condition for such communication, but not a necessary one. Nevertheless, consider the EPR thought experiment, and suppose quantum states could be cloned. Assume parts of a maximally entangled Bell state are distributed to Alice and Bob. Alice could send bits to Bob in the following way: If Alice wishes to transmit a "0", she measures the spin of her electron in the z direction, collapsing Bob's state to either $|z+\rangle_B$ or $|z-\rangle_B$. To transmit "1", Alice does nothing to her qubit. Bob creates many copies of his electron's state, and measures the spin of each copy in the z direction. Bob will know that Alice has transmitted a "0" if all his measurements will produce the same result; otherwise, his measurements will have outcomes +1/2 and −1/2 with equal probability. This would allow Alice and Bob to communicate across space-like separations.

- The no-cloning theorem prevents us from viewing the holographic principle for black holes as meaning we have two copies of information lying at the event horizon and the black hole interior simultaneously. This leads us to more radical interpretations like black hole complementarity.

### 2.4. Heisenberg uncertainty principle

**Heisenberg's Uncertainty Principle** (abbreviated HUP) is one of the fundamental concepts of quantum physics, and is the basis for the initial realization of fundamental uncertainties in the ability of an experimenter to measure more than one quantum variable at a time. Attempting to measure an elementary particle's position to the highest degree of accuracy, for example,

leads to an increasing uncertainty in being able to measure the particle's momentum to an equally high degree of accuracy.

Suppose $A$ and $B$ are two Hermitian operators, and $|\psi\rangle$ is a quantum state. Suppose $\langle\psi|AB|\psi\rangle = x + iy$, where $x$ and $y$ are real. Note that $\langle\psi|[A, B]|\psi\rangle = 2iy$ and $\langle\psi|\{A, B\}|\psi\rangle = 2x$. This implies that

$$\left|\langle\psi|\left[A,B\right]|\psi\rangle\right|^2 + \left|\langle\psi|\{A,B\}|\psi\rangle\right|^2 = 4\left|\langle\psi|AB|\psi\rangle\right|^2. \tag{7}$$

By the Cauchy-Schwarz inequality $|\langle\psi|AB|\psi\rangle|^2 \leq \langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle$, which combined with the equation (1) and dropping a non-negative term gives

$$\left|\langle\psi|\left[A,B\right]|\psi\rangle\right|^2 \leq 4\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle. \tag{8}$$

Suppose $C$ and $D$ are two observables. Substituting $A = C - \langle C\rangle$ and $B = D - \langle D\rangle$ into the last equation, where the average value of the observable $C$ is often written $\langle C\rangle = \langle\psi|C|\psi\rangle$ and similar to $D$, we obtain Heisenberg's uncertainty principle as it is usually stated

$$\Delta(C)\Delta(D) \geq \frac{\left|\langle\psi|\left[C,D\right]|\psi\rangle\right|}{2}. \tag{9}$$

Quantum communication the sending of encoded messages that are un-hackable by any computer. This i allows s possible because the messages are carried by tiny particles of light called photons. If an eavesdropper attempts to read out the message in transit, they will be discovered by the disturbance their measurement causes to the particles as an inevitable consequence of the HUP. In the regime of quantum experiments, by contrast, we are uncertain about the results of experiments because the particle itself is uncertain. It has no position or speed until we measure it. We can design some protocol of quantum cryptography by using the property of quantum from HUP.

## 3. Quantum key distribution

The first attempt of using quantum mechanics to achieve missions impossible in classical information started in the early 70's. Stephen Wiesner proposed two communication modalities not allowed by classical physics: "quantum multiplexing" channel and counterfeit-free bank-note. Unfortunately, his paper was rejected and couldn't be published until a decade later. In 1980's, Charles H.Bennett and Gilles Brassard extended Wiesner's idea and applied it to solve the key distribution problem in classical cryptography. In 1984, the well known BB84 QKD protocol was published [15]. QKD is a new tool in the cryptographer's toolbox: it allows for secure key agreement over an untrusted channel where the output key is entirely inde-

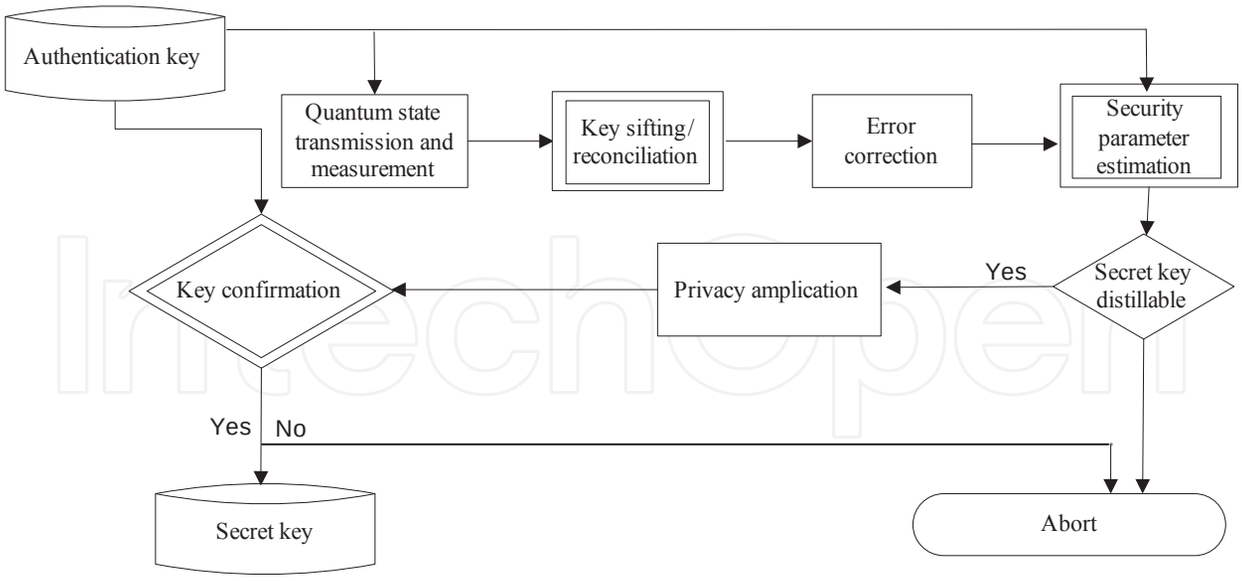


**Figure 1.** Flow chart of the stages of a quantum key distribution protocol. Stages with double lines require classical authentication. [18]

pendent from any input value, a task that is impossible using classical cryptography. QKD does not eliminate the need for other cryptographic primitives, such as authentication, but it can be used to build systems with new security properties.

To conquer the errors made by noise and wiretapping in the quantum channel, unconditionally secure secret-key agreement over a public channel was designed, information reconciliation and privacy amplification can be used to quantum key distribution, or otherwise, quantum entanglement purification should be used. The first general although rather complex proof of unconditional security was given by Mayers [16], which was followed by a number of other proofs. In Mayers' proof, the BB84 scheme proposed by Bennett and Brassard was proved to be unconditionally secure. Building on the quantum privacy amplification idea, Lo and Chau, proposed a conceptually simpler proof of security [17].

In QKD, two parties, Alice and Bob, obtain some quantum states and measure them. They communicate (all communication form this point onwards is classical) to determine which of their measurement results could lead to secret key bits; some are discarded in a process called sifting because the measurement settings were incompatible. They perform error correction and then estimate a security parameter which describes how much information an eavesdropper might have about their key data. If this amount is above a certain threshold, then they abort as they cannot guarantee any secrecy whatsoever. If it is below the threshold, then they can apply privacy amplification to squeeze out any remaining information the eavesdropper might have, and arrive at a shared secret key. Some of this classical communication must be authenticated to avoid man-in-the-middle attacks. Some portions of the protocol can fail with negligible probability.

A flow chart describing the stages of quantum key distribution is given in Figure 1.

| Alice's bit sequence | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|
| Alice's basis | + | × | + | + | × | + | × | × | + | × |
| Alice's photon polarization | → | ↖ | ↑ | ↑ | ↗ | ↑ | ↗ | ↗ | → | ↖ |
| Bob's basis | + | + | × | + | + | × | × | + | + | × |
| Bob's measured polarization | → | ↑ | ↖ | ↑ | → | ↗ | ↗ | ↑ | → | ↖ |
| Bob's sifted measured polarization | → | | | ↑ | | | ↗ | | → | ↖ |
| Bob's data sequence | 0 | | | 1 | | | 0 | | 0 | 1 |

**Table 1.** Procedure of BB84 protocol.

### 3.1. The BB84 QKD protocol

The best-known protocol for QKD is the Bennett and Brassard protocol (BB84). The procedure of BB84 is as follows (also shown in Table 1).

**1.** Quantum communication phase

**1.** In BB84, Alice sends Bob a sequence of photons through an *insecure quantum channel*, each independently chosen from one of the four polarizations-vertical, horizontal, 45-degrees and 135-degrees.

**2.** For each photon, Bob randomly chooses one of the two measurement bases (rectilinear and diagonal) to perform a measurement.

**3.** Bob records his measurement bases and results. Bob publicly acknowledge his receipt of signals.

**2.** Public discussion phase

**1.** Alice broadcasts her bases of measurements. Bob broadcasts his bases of measurements.

**2.** Alice and Bob discard all events where they use different bases for a signal.

**3.** To test for tampering, Alice randomly chooses a fraction, $p$, of all remaining events as test events. For those test events, she publicly broadcasts their positions and polarizations.

**4.** Bob broadcasts the polarizations of the test events.

**5.** Alice and Bob compute the error rate of the test events (i.e., the fraction of data for which their value disagree). If the computed error rate is larger than some prescribed threshold value, say 11%, they abort. Otherwise, they proceed to the next step.

**6.** Alice and Bob each convert the polarization data of all remaining data into a binary string called a raw key (by, for example, mapping a vertical of 45-degrees photon to "0" and a horizontal or 135-degrees photon to "1"). The can perform classical postprocessing such as error correction and privacy amplification to generate a final key.

The basic idea of the BB84 QKD protocol is beautiful and its security can be intuitively understood from the quantum no-cloning theorem. On the other hand, to apply QKD in practice, Alice and Bob need to find the upper bound of Eve's information quantitatively, given the observed quantum bit error rate (abbreviated QBER) and other system parameters. This is the primary goal of various QKD security proofs and it had turned out to be extremely difficult. One major challenge comes from the fact that Eve could launch attacks way beyond today's technologies and our imaginations. Nevertheless, QKD was proved to be unconditionally secure. This is most significant achievements in quantum information.

### 3.2. QKD based on EPR

An essentially equivalent protocol that utilizes Einstein-Podolsky-Rosen (EPR) correlations has been worked on by Artur Ekert [19] and Bennett, Brassard, and Mermin [20]. To take advantage of EPR correlations, particles are prepared in such a way that they are "entangled". This means that although they may be separated by large distances in space, they are not independent of each other. Suppose the entangled particles are photons. If one of the particles is measured according to the rectilinear basis and found to have a vertical polarization, then the other particle will also be found to have a vertical polarization if it is measured according to the rectilinear basis. If however, the second particle is measured according to the circular basis, it may be found to have either left-circular or right-circular polarization.

In his 1991 paper, Ekert [19] suggested basing the security of this two-qubit protocol on Bell's inequality, an inequality which demonstrates that some correlations predicted by quantum mechanics cannot be reproduced by the local theory. To do this, Alice and Bob can use a third basis. In this way the probability that they might happen to choose the same basis is reduced from $\frac{1}{2}$ to $\frac{2}{9}$, but at the same time as they establish a key, they collect enough data to test Bell's inequality. They can thus check that the source really emits the entangled state and not merely product states. The following year Bennett, Brassard, and Mermin [20] criticized Ekert's letter, arguing that the violation of Bell's inequality is not necessary for the security of quantum cryptography and emphasizing the close connection between the Ekert and the BB84 schemes. This criticism quantum cryptography might be missing an important point. Although the exact relation between security and Bell's inequality is not yet fully known, there are clear results establishing fascinating connections.

The steps of the protocol for developing a secret key using EPR correlations of entangled photons are explained below.

1. Alice creates EPR pairs of polarized photons, keeping one particle for herself and sending the other particle of each pair to Bob.

2. Alice randomly measures the polarization of each particle she kept according to the rectilinear or circular basis. She records each measurement type and the polarization measured.

3. Bob randomly measures each particle he received according to the rectilinear or circular basis. He records each measurement type and the polarization measured.

4. Alice and Bob tell each other which measurement types were used, and they keep the data from all particle pairs where they both chose the same measurement type.

5. They convert the remaining data to a string of bits using a convention such as: left-circular = 0, right-circular = 1, horizontal = 0, vertical = 1.

One important difference between the BB84 and the EPR methods is that with BB84, the key created by Alice and Bob must be stored classically until it is used. Therefore, although the key was completely secure when it was created, its continued security over time is only as great as the security of its storage. Using the EPR method, Alice and Bob could potentially store the prepared entangled particles and then measure them and create the key just before they were going to use it, eliminating the problem of insecure storage.

So the idea consists in replacing the quantum channel carrying two qubits from Alice to Bob by a channel carrying two qubits from a common source, one qubit to Alice and one to Bob. A first possibility would be that the source always emits the two qubits in the same state chosen randomly among the four states of the BB84 protocol. Alice and Bob would then both measure their qubit in one of the two bases, again chosen independently and randomly. The source then announces the bases, and Alice and Bob keep the data only when they happen to have made their measurements in the compatible basis. If the source is reliable, this protocol is equivalent to that of BB84: It is as if the qubit propagates backwards in time from Alice to the source, and then forward to Bob. But better than trusting the source, which could be in Eve's hand the Ekert protocol assumes that the two qubits are emitted in a maximally entangled state like $|\phi^+\rangle = {}^1\!/\!_{\sqrt{2}}(|00\rangle + |11\rangle)$.

Then, when Alice and Bob happen to use the same basis, either the $x$ basis or the $y$ basis, i.e., in about half of the cases, their results are identical, providing them with a common key.

### 3.3. Continuous variable QKD

In the BB84 QKD protocol, Alice's random bits are encoded in a two dimensional space like the polarization state of a single photon. More recently, QKD protocols working with continuous variables have been proposed. Among them, the Gaussian modulated coherent state (GMCS) QKD protocol has drawn special attention [21].

The protocol runs as follows. First, Alice draws two random numbers $x_A$ and $p_A$ from a gaussian distribution of mean zero and variance $V_A N_0$, where $N_0$ denotes the shot-noise variance. Then, she sends the coherent state $|x_A + ip_A\rangle$ to Bob, who randomly chooses to measure either quadrature $x$ or $p$. Later, using a public authenticated channel, he informs Alice about which quadrature he measured, so she may discard the irrelevant data. After many similar exchanges, Alice and Bob (and possibly the eavesdropper Eve) share a set of correlated gaussian variables, which we call 'key elements'.

The basic scheme of the GMCS QKD protocol can be shown in Figure 2.

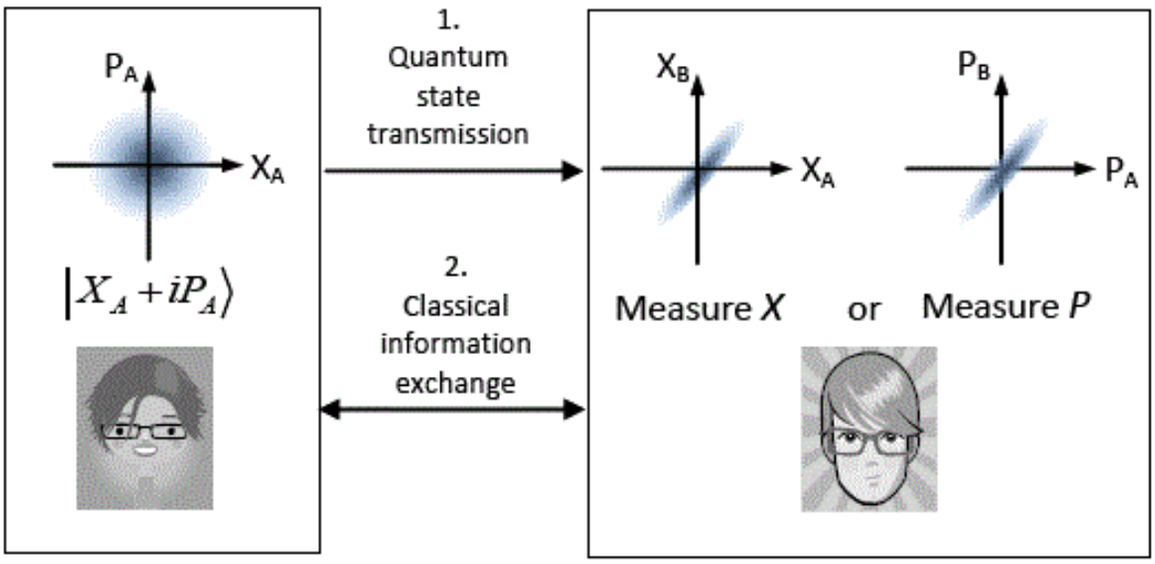


**Figure 2.** *The Gaussian modulated coherent state (GMCS) QKD. X: amplitude quadrature; P: phase quadrature.* [22]

Alice modulates both the amplitude quadrature and phase quadrature of a coherent state with Gaussian distributed random numbers. In classical electromagnetism, these two quadratures correspond to the in-phase and out-of-phase components of electric field, which can be conveniently modulated with optical phase and amplitude modulators. Alice sends the modulated coherent state together with a strong local oscillator (a strong laser pulse which serves as a phase reference) to Bob. Bob randomly measures one of the two quadratures with a phase modulator and a homodyne detector. After performing his measurements, Bob informs Alice which quadrature he actually measures for each pulse and Alice drops the irrelevant data. At this stage, they share a set of correlated Gaussian variables which are called the — raw key. Given the variances of the measurement results below certain thresholds, they can further work out perfectly correlated secure key by performing reconciliation and privacy amplification. Classical data processing is then necessary for Alice and Bob to obtain a fully secret binary key.

The security of the GMCS QKD can be comprehended from the uncertainty principle. In quantum optics, the amplitude quadrature and phase quadrature of a coherent state form a pair of conjugate variables, which cannot be simultaneously determined with arbitrarily high accuracies due to Heisenberg uncertainty principle. From the observed variance in one quadrature, Alice and Bob can upper bound Eve's information about the other quadrature. This provides a way to verify the security of the generated key. Recently, an unconditional security proof of the GMCS QKD appeared [23].

Different from the BB84 QKD, in GMCS QKD, homodyne detectors are employed to measure electric fields rather than photon energy. By using a strong local oscillator, high efficiency and fast photo diodes can be used to construct the homodyne detector which could result in a high secure key generation rate. However, the performance of the GMCS QKD is strongly dependent on the channel loss. Recall that in the BB84 QKD system, the channel loss plays a simple

http://dx.doi.org/10.5772/56092

role: it reduces the communication efficiency but it will not introduce QBER. A photon is either lost in the channel, in which case Bob will not register anything, or it will reach Bob's detector intact. On the other hand, in the GMCS QKD, the channel loss will introduce vacuum noise and reduce the correlation between Alice and Bob's data. As the channel loss increases, the vacuum noise will become so high that it is impossible for Alice and Bob to resolve a small excess noise (which is used to upper bound Eve's information) on the top of a huge vacuum noise.

Comparing with the BB84 QKD, the GMCS QKD could yield a high secure key rate over short distances [24] [25].

### 3.4. Decoy state QKD

The security of QKD has been rigorously proven in a number of recent papers. There has been tremendous interest in experimental QKD [26] [27]. Unfortunately, all those exciting recent experiments are, in principle, insecure due to real-life imperfections. More concretely, highly attenuated lasers are often used as sources. But, these sources sometimes produce signals that contain more than one photon. Those multi-photon signals open the door to powerful new eavesdropping attacks including photon splitting attack. For example, Eve can, in principle, measure the photon number of each signal emitted by Alice and selectively suppress single photon signals. She splits multi-photon signals, keeping one copy for herself and sending one copy to Bob. Now, since Eve has an identical copy of what Bob possesses, the unconditional security of QKD is completely compromised.

In summary, in standard BB84 protocol, only signals originated from single photon pulses emitted by Alice are guaranteed to be secure. Consequently, paraphrasing GLLP (Gottesman, Lo, Lutkenhaus, Preskill [28]), the secure key generation rate (per signal state emitted by Alice) can be shown to be given by:

$$S \geq Q_{\mu}\{-H_2(E_{\mu}) + \Omega\,[1 - H_2(e_1)]\}, \tag{10}$$

where $Q_{\mu}$ and $E_{\mu}$ are respectively the gain and quantum bit error rate (QBER) of the signal state (Here, the gain means the ratio of the number of Bob's detection events (where Bob chooses the same basis as Alice) to Alice's number of emitted signals. QBER means the error rate of Bob's detection events for the case that Alice and Bob use the same basis), $\Omega$ and $e_1$ are respectively the fraction and QBER of detection events by Bob that have originated from single-photon signals emitted by Alice and $H_2$ is the binary Shannon entropy. It is a prior very hard to obtain a good lower bound on $\Omega$ and a good upper bound on $e_1$. Therefore, prior art methods (as in GLLP [28], under (semi-) realistic assumptions, if imperfections are sufficiently small, then BB84 is unconditionally secure.) make the most pessimistic assumption that all multi-photon signals emitted by Alice will be received by Bob. For this reason, until now, it has been widely believed that the demand for unconditional security will severely reduce the performance of QKD systems.

In [29], they present a simple method that will provide very good bounds to $\Omega$ and $e_1$. The method is based on the decoy state idea first proposed by Hwang [12]. While the idea of Hwang was highly innovative, his security analysis was heuristic. Consequently, H.K. Lo etc's method for the first time makes most of the long distance QKD experiments reported in the literature unconditionally secure. And their method has the advantage that it can be implemented with essentially the current hardware. So, unlike prior art solutions based on single-photon sources, their method does not require daunting experimental developments. The key point of the decoy state idea is that Alice prepares a set of additional states — decoy states, in addition to standard BB84 states. Those decoy states are used for the purpose of detecting eavesdropping attacks only, whereas the standard BB84 states are used for key generation only. The only difference between the decoy state and the standard BB84 states is their intensities (i.e., their photon number distributions). By measuring the yields and QBER of decoy states, Alice and Bob can obtain reliable bounds to $\Omega$ and $e_1$, thus allowing them to surpass all prior art results substantially [30].

At first, we recall the original decoy state QKD by Hwang [12] in detail.

Define $Y_n$= yield = conditional probability that a signal will be detected by Bob, given that it is emitted by Alice as an $n$-photon state.

To design a method to test experimentally the yield (i.e. transmittance) of multi-photons, we can use two-photon states as decoys and test their yield. For example, Alice and Bob estimate the yield $Y_2 = x / N$ if Alice sends N two-photon signals to Bob and Bob detects $x$ signals. If Eve selectively sends multi-photons, $Y_2$ will be abnormally large. So Eve will be caught.

The two kinds of states are as follows for the decoy state QKD (Toy Model).

**a.** Signal state: Poisson photon number distribution $\mu$ (at Alice).

**b.** Decoy state: two-photon signals.

The procedure of decoy state QKD (Toy Model) is as following.

**1.** Alice randomly sends either a signal state or decoy state to Bob.

**2.** Bob acknowledges receipt of signals.

**3.** Alice publicly announces which are signal states and which are decoy states.

**4.** Alice and Bob compute the transmission probability for the signal states and for the decoy states respectively.

If Eve selectively transmits two-photons, an abnormally high fraction of the decoy state B) will be received by Bob. Eve will be caught. But the practical problem with toy model is making perfect two-photon state is hard. So the solution of Hwang's decoy state QKD is to make another mixture of good and bad photons with a different weight.

There is two kinds of states for Hwang's decoy state QKD.

**a.** Signal state: Poisson photon number distribution: $\alpha$ (at Alice) with mixture 1.

**b.** Decoy state: Poisson photon number distribution: $\mu \sim 2$ (at Alice) with mixture 2.

If Eve lets an abnormally high fraction of multi-photons go to Bob, then decoy states (which has high weight of multi-photons) will have an abnormally high transmission. Therefore, Alice and Bob can catch Eve.

But there are some drawbacks of Hwang's original idea:

**1.** Hwang's security analysis was heuristic, rather than rigorous.

**2.** "Dark counts"–an important effect–are not considered.

**3.** Final results (distance and key generation rate) are unclear.

Suppose that a decoy state and a signal state have the same characteristics (wavelength, timing information, etc) by H.K. Lo etc's methods [29]. Therefore, Eve cannot distinguish a decoy state from a signal state and the only piece of information available to Eve is the number of photons in a signal. Therefore, the yield, $Y_n$ (yield of an $n$-photon signal), and QBER, $e_n$ (quantum bit error rate of an $n$-photon signal), can depend on only the photon number,$n$, but not which distribution (decoy or signal) the state is from. If Eve cannot treat the decoy state any differently from signal state, then

$$Y_n(signal) = Y_n(decoy) = Y_n$$
$$e_n(signal) = e_n(decoy) = e_n.$$

Let us imagine that Alice varies over all non-negative values of $\mu$ randomly and independently for each signal, Alice and Bob can experimentally measure the yield $Q_\mu$ and the QBER $E_\mu$.

$$Q_\mu = Y_0 e^{-\mu} + Y_1 e^{-\mu}\mu + Y_2 e^{-\mu}(\mu^2/2) + \ldots + Y_n e^{-\mu}(\mu^n/n!) + \ldots. \tag{11}$$

$$Q_\mu E_\mu = Y_0 e^{-\mu} e_0 + Y_1 e^{-\mu}\mu e_1 + Y_2 e^{-\mu}(\mu^2/2) e_2 + \ldots + Y_n e^{-\mu}(\mu^n/n!) e_n + \ldots. \tag{12}$$

Since the relations between the variables $Q_\mu$'s and $Y_n$'s and between $E_\mu$'s and $e_n$'s are linear, given the set of variables $Q_\mu$'s and $E_\mu$'s measured from their experiments, Alice and Bob can deduce mathematically with high confidence the variables $Y_n$'s and $e_n$'s. This means that Alice and Bob can constrain simultaneously the yields, $Y_n$ and QBER $e_n$ simultaneously for all $n$. Suppose Alice and Bob know their channel property well. Then, they know what range of values of $Y_n$'s and $e_n$'s is acceptable. Any attack by Eve that will change the value of any one of the $Y_n$'s and $e_n$'s substantially will, in principle, be caught with high probability by decoy state method. Therefore, in order to avoid being detected, the eavesdropper, Eve, has very limited options in her eavesdropping attack. In summary, the ability for Alice and Bob to verify experimentally the values of $Y_n$ and $e_n$'s in the decoy state method greatly strengthens their

power in detecting eavesdropping, thus leading to a dramatic improvement in the performance of their QKD system. The decoy state method allows Alice and Bob to detect deviations from the normal behavior due to eavesdropping attacks.

In [29], they also give for the first time a rigorous analysis of the security of decoy state QKD. Moreover, they show that the decoy state idea can be combined with the prior art GLLP analysis. And we can get the comparison results with and without decoy state as the following Figure3.

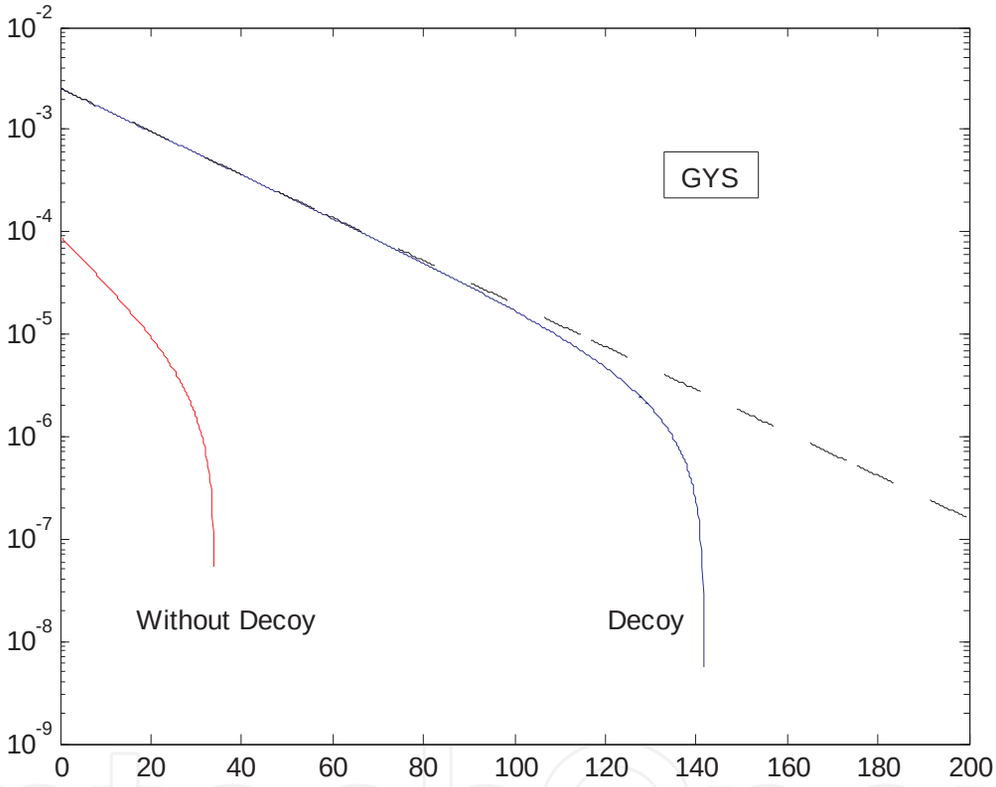


**Figure 3.** Compare results with and without decoy state.

## 4. The security of QKD

Bennett and Brassard have ever said that the most important question in quantum cryptography is to determine how secure it really is.

Security proofs are very important because a) they provide the foundation of security to a QKD protocol, b) they provide a formula for the key generation rate of a QKD protocol and c) they

http://dx.doi.org/10.5772/56092

may even provide a construction for the classical post-processing protocol (for error correction and privacy amplification) that is necessary for the generation of the final key. Without security proofs, a real-life QKD system is incomplete because we can never be sure about how to generate a secure key and how secure the final key really is.

After the qubit exchange and basis reconciliation, Alice and Bob each have a sifted key. Ideally, these keys are identical. But in real life, there are always some errors, and Alice and Bob must apply some classical information processing protocols, like error correction and privacy amplification to their data. The first protocol is necessary to obtain identical keys and the second to obtain a secret key. Essentially, the problem of eavesdropping is to find protocols which, given that Alice and Bob can only measure the QBER, either provide Alice and Bob with a verifiably secure key or stop the protocol and inform the users that the key distribution has failed. This is a delicate problem at the intersection of quantum physics and information theory. Actually, it comprises several eavesdropping problems, depending on the precise protocol, the degree of idealization one admits, the technological power one assumes Eve has, and the assumed fidelity of Alice and Bob's equipment. Let us immediately stress that a complete analysis of eavesdropping on a quantum channel has yet to be achieved.

### 4.1. Eavesdropping attacks

In order to simplify the problem, several eavesdropping strategies of limited generality have been defined ([31-33]) and analyzed. Of particular interest is the assumption that Eve attaches independent probes to each qubit and measures her probes one after the other. They can be classified as follows:

**Individual attacks**: In an individual attack, Eve performs an attack on each signal independently. The intercept-resend attack is an example of an individual attack. let us consider the simple example of an intercept-resend attack by an eavesdropper Eve, who measures each photon in a randomly chosen basis and then resends the resulting state to Bob. For instance, if Eve performs a rectilinear measurement, photons prepared by Alice in the diagonal bases will be disturbed by Eve's measurement and give random answers. When Eve resends rectilinear photons to Bob, if Bob performs a diagonal measurement, then he will get random answers. Since the two bases are chosen randomly by each party, such an intercept-resend attack will give a bit error rate of $0.5\times0.5+0.5\times0 = 25\%$, which is readily detectable by Alice and Bob. Sophisticated attacks against QKD do exist. Fortunately, the security of QKD has now been proven.

**Collective attacks**: A more general class of attacks is collective attack where for each signal, Eve independently couples it with an ancillary quantum system, commonly called an ancilla, and evolves the combined signal/ancilla unitarily. She can send the resulting signals to Bob, but keep all ancillas herself. Unlike the case of individual attacks, Eve postpones her choice of measurement. Only after hearing the public discussion between Alice and Bob, does Eve decide on what measurement to perform on her ancilla to extract information about the final key.

**Joint attacks**: The most general class of attacks is joint attack. In a joint attack, instead of interacting with each signal independently, Eve treats all the signals as a single quantum system. She then couples the signal system with her ancilla and evolves the combined signal and ancilla system unitarily. She hears the public discussion between Alice and Bob before deciding on which measurement to perform on her ancilla.

For joint and collective attacks, the usual assumption is that Eve measures her probe only after Alice and Bob have completed all public discussion about basis reconciliation, error correction, and privacy amplification. For the more realistic individual attacks, one assumes that Eve waits only until the basis reconciliation phase of the public discussion. With today's technology, it might even be fair to assume that in individual attacks Eve must measure her probe before the basis reconciliation [34]. The motivation for this assumption is that one hardly sees what Eve could gain by waiting until after the public discussion on error correction and privacy amplification before measuring her probes, since she is going to measure them independently anyway. About practical QKD, they summary some assumptions about security of QKD in [18]. We describe them in the next subsection 4.2.

### 4.2. Some assumptions about security of QKD

Quantum key distribution is often described by its proponents as "unconditionally secure" to emphasize its difference with computationally secure classical cryptographic protocols. While there are still conditions that need to be satisfied for quantum key distribution to be secure, the phrase "unconditionally secure" is justified because, not only are the conditions reduced, they are in some sense minimal necessary conditions. Any secure key agreement protocol must make a few minimal assumptions, for security cannot come from nothing: we must be able to identify and authenticate the communicating parties, we must be able to have some private location to perform local operations, and all parties must operate within the laws of physics.

The following statement describes the security of quantum key distribution, and there are many formal mathematical arguments for the security of QKD.

**Theorem 1 (Security statement for quantum key distribution)** If 1) quantum mechanics is correct, and 2) authentication is secure, and 3) our devices are reasonably secure, then with high probability the key established by quantum key distribution is a random secret key independent (up to a negligible difference) of input values.

**Assumption 1: Quantum mechanics is correct.** This assumption requires that any eavesdropper be bounded by the laws of quantum mechanics, although within this realm there are no further restrictions beyond the eavesdropper's inability to access the devices. In particular, we allow the eavesdropper to have arbitrarily large quantum computing technology, far more powerful than the current state of the art. Quantum mechanics has been tested experimentally for nearly a century, to very high precision. But even if quantum mechanics is superseded by a new physical theory, it is not necessarily true that quantum key distribution would be insecure: for example, secure key distribution can be achieved in a manner similar to QKD solely based on the assumption that no faster-than-light communication is possible [35].

**Assumption 2: Authentication is secure.** This assumption is one of the main concerns of those evaluating quantum key distributions. In order to be protected against man-in-the-middle attack, much of the classical communication in QKD must be authenticated. Authentication can be achieved with unconditional security using short shared keys, or with computational security using public key cryptography.

**Assumption 3: Our devices are secure.** Constructing a QKD implementation that is verifiably secure is a substantial engineering challenge that researchers are still working on. Although the first prototype QKD system leaked key information over a side channel (it made different noises depending on the photon polarization, and thus the "prototype was unconditionally secure against any eavesdropper who happened to be deaf" [36] ), experimental cryptanalysis leads to better theoretical and practical security. More sophisticated side-channel attacks continue to be proposed against particular implementations of existing systems (e.g., [37]), but so too are better theoretical methods being proposed, such as the decoy state method [38]. Device-independent security proofs [39, 40] aim to minimize the security assumptions on physical devices. It seems reasonable to expect that further theoretical and engineering advances will eventually bring us devices which have strong arguments and few assumptions for their security.

### 4.3. Security proofs for QKD

Proving the security of QKD against the most general attack was a very hard problem. It took more than 10 years, but the unconditional security of QKD was finally established in several papers in the 1990s. One approach by Mayers [16] was to prove the security of the BB84 directly. A simpler approach by Lo and Chau [17], mad use of the idea of entanglement distillation by Bennett, DiVincenzo, Smolin and Wootters (BDSW) [41] and quantum privacy amplification by Deutsch et al. [42] to solve the security of an entanglement-based QKD protocol. The two approaches have been unified by the work of Shor and Preskill [43], who provided a simple proof of security of BB84 using entanglement distillation idea. Other early security proofs of QKD include Biham, Boyer, Boykin, Mor, and Roychowdhury [44], and Ben-Or [45].

There are several approaches to security proof as following. [5]

#### *4.3.1. Entanglement distillation*

Entanglement distillation protocol (EDP) provides a simple approach to security proof [17, 42, 43]. The basic insight is that entanglement is a sufficient (but not necessary) condition for a secure key. In the noiseless case, suppose two distant parties, Alice and Bob, share a maximally entangled state of the form $|\phi\rangle_{AB}={}^{1}\!/\!_{\sqrt{2}}(|00\rangle_{AB}+|11\rangle_{AB})$. If each of Alice and Bob measure their systems, then they will both get "0"s or "1"s, which is a shared random key. Moreover, if we consider the combined system of the three parties—Alice, Bob and an eavesdropper, Eve, we can use a pure-state description (the "Church of Larger Hilbert space") and consider a pure state $|\psi\rangle_{ABE}$. In this case, the von Neumann entropy of Eve $S(\rho_E)=S(\rho_{AB})=0$. This means that Eve has absolutely no information on the final

key. In the noisy case, Alice and Bob may share $N$ pairs of qubits, which are a noisy version of $N$ maximally entangled states. Now, using the idea of entanglement distillation protocol (EDP) discussed in BDSW [41], Alice and Bob may apply local operations and classical communications (LOCCs) to distill from the $N$ noisy pairs a smaller number, say $M$ almost perfect pairs i.e., a state close to $|\phi\rangle_{AB}^{M}$. Once such a EDP has been performed, Alice and Bob can measure their respective system to generate an $M$-bit final key.

How can Alice and Bob be sure that their EDP will be successful? Whether an EDP will be successful or not depends on the initial state shared by Alice and Bob. In practice, Alice and Bob can never be sure what initial state they possess. Therefore, it is useful for them to add a verification step. By, for example, randomly testing a fraction of their pairs, they have a pretty good idea about the properties (e.g., the bit-flip and phase error rates) of their remaining pairs and are pretty confident that their EDP will be successful.

*4.3.2. Communication complexity/quantum memory*

The communication complexity/quantum memory approach to security proof was proposed by Ben-Or [45] and subsequently by Renner and Koenig [46]. See also [47]. They provide a formula for secure key generation rate in terms of an eavesdropper's quantum knowledge on the raw key: Let $Z$ be a random variable with range $\mathbb{Z}$, let $\rho$ be a random state, and let $F$ be a two-universal function on $\mathbb{Z}$ with range $S=\{0,\ 1\}^s$ which is independent of $Z$ and $\rho$. Then [46]

$$d(F(Z)|\{F\}\otimes\rho)\le\frac{1}{2}2^{-\frac{1}{2}(S_2([\{Z\}\otimes\rho])-S_0([\rho])-s)}. \tag{13}$$

Incidentally, the quantum de Finnetti's theorem [48] is often useful for simplifying security proofs of this type.

*4.3.3. Twisted state approach*

What is a necessary and sufficient condition for secure key generation? From the entanglement distillation approach, we know that entanglement distillation a sufficient condition for secure key generation. For some time, it was hoped that entanglement distillation is also a necessary condition for secure key generation. However, such an idea was proven to be wrong in [49] [50], where it was found that a necessary and sufficient condition is the distillation of a private state, rather than a maximally entangled state. A private state is a "twisted" version of a maximally entangled state. They proved the following theorem in [49]: a state is private in the above sense iff it is of the following form

$$\gamma_m=U\left|\psi_{2^m}^{+}\right\rangle_{AB}\left\langle\psi_{2^m}^{+}\right|\otimes\rho_{A'B'}U^{\dagger} \tag{14}$$

Where $|\psi_d\rangle = \sum_{i=1}^{d} |ii\rangle$ and $\rho_{A'B'}$ is an arbitrary state on $A'$, $B'$. $U$ is an arbitrary unitary controlled in the computational basis

$$U = \sum_{i,j=1}^{2^m} |ij\rangle_{AB} \langle ij| \otimes U_{ij}^{A'B'}. \tag{15}$$

The operation (15) will be called "twisting" (note that only $U_{ii}^{A'B'}$ matter here, yet it will be useful to consider general twisting later).

The main new ingredient of the above theorem is the introduction of a "shield" part to Alice and Bob's system. That is, in addition to the systems $A$ and $B$ used by Alice and Bob for key generation, we assume that Alice and Bob also hold some ancillary systems, $A'$ and $B'$, often called the shield part. Since we assume that Eve has no access to the shield part, Eve is further limited in her ability to eavesdrop. Therefore, Alice and Bob can derive a higher key generation rate than the case when Eve does have access to the shield part.

#### *4.3.4. Complementary principle*

Another approach to security proof is to use the complementary principle of quantum mechanics. Such an approach is interesting because it shows the deep connection between the foundations of quantum mechanics and the security of QKD. In fact, both Mayers' proof [16] and Biham, Boyer, Boykin, Mor, and Roychowdhury's proof [44] make use of this complementary principle. A clear and rigorous discussion of the complementary principle approach to security proof has recently been achieved by Koashi [51]. The key insight of Koashi's proof is that Alice and Bob's ability to generate a random secure key in the $Z$-basis (by a measurement of the Pauli spin matrix $\sigma_Z$) is equivalent to the ability for Bob to help Alice prepare an eigenstate in the complementary, i.e., $X$-basis ($\sigma_X$), with their help of the shield. The intuition is that an $X$-basis eigenstate, for example, $|+\rangle_A = {}^{1}\!/\!_{\sqrt{2}}(|0\rangle_A + |1\rangle_A)$, when measured along the $Z$-basis, gives a random answer.

#### *4.3.5. Other ideas for security proofs*

Here are two other ideas for security proofs, namely, a) device-independent security proofs and b) security from the causality constraint. Unfortunately, these ideas are still very much under development and so far a complete version of a proof of unconditional security of QKD based on these ideas with a finite key rate is still missing.

Let us start with a) device-independent security proofs. So far we have assumed that Alice and Bob know what their devices are doing exactly. In practice, Alice and Bob may not know their devices for sure. Recently, there has been much interest in the idea of device independent security proofs. In other words, how to prove security when Alice and Bob's devices cannot

be trusted. See, for example, [52]. The idea is to look only at the input and output variables. A handwaving argument goes as follows. Using their probability distribution, if one can demonstrate the violation of some Bell inequalities, then one cannot explain the data by a separable system. How to develop such a handwaving argument into a full proof of unconditional security is an important question.

The second idea b) security from the causality constraint is even more ambitious. The question that it tries to address is the following. How can one prove security when even quantum mechanics is wrong? In [53] and references cited therein, it was suggested that perhaps a more general physical principle such as the no-signaling requirement for space-like observables could be used to prove the security of QKD.

## 5. Quantum secret sharing

"Secret sharing" refers to an important family of multi-party cryptographic protocols in both the classical and the quantum contexts. A secret sharing protocol comprises a dealer and $n$ players who are interconnected by some set of classical or quantum channels. The "secret" to be shared is a classical string or quantum state and is distributed among the players by the dealer in such a way that it can only be recovered by certain subsets of players acting collaboratively. The access structure is the set of all subsets of players who can recover the secret, and the adversary structure corresponds to those subsets that obtain no knowledge of the secret. There may, in addition, be external eavesdroppers who should also gain no knowledge of the secret.

Quantum secret sharing (abbreviated QSS) is the generalization of quantum key distribution to more than two parties [54]. In this new application of quantum communication, Alice distributes a secret key to two other users, Bob and Charlie, in such a way that neither Bob nor Charlie alone has any information about the key, but together they have full information. As in traditional QC, an eavesdropper trying to get some information about the key creates errors in the transmission data and thus reveals her presence. The motivation behind quantum secret sharing is to guarantee that Bob and Charlie cooperate—one of them might be dishonest—in order to obtain a given piece of information. In contrast with previous proposals using three particle Greenberger-Horne-Zeilinger states [55], pairs of entangled photons in so-called energy-time Bell states were used to mimic the necessary quantum correlation of three entangled qubits, although only two photons exist at the same time. This is possible because of the symmetry between the preparation device acting on the pump pulse and the devices analyzing the downconverted photons. Therefore the emission of a pump pulse can be considered as the detection of a photon with 100% efficiency, and the scheme features a much higher coincidence rate than that expected with the initially proposed "triplephoton" schemes.

QSS which is based on the laws of quantum mechanics, instead of mathematical assumptions can share the information unconditionally securely. According to the form of sharing information, QSS can be divided into QSS of classical messages and QSS of quantum informa-

tion.QSS of classical messages can be divided into QSS of classical messages based on entanglement and QSS of classical messages without entanglement.

In 1999, Hillery et al. [55] used entangled three-photon GHZ states to propose the first QSS protocol, namely the HBB99 scheme. In their scheme, the dealer (Alice) prepares a three photons quantum system in the GHZ state $|\psi\rangle = {}^{1}\!/\!_{\sqrt{2}}(|000\rangle + |111\rangle)_{ABC}$ and sends the photon B and C to Bob and Charlie, respectively. The three parties all choose randomly one of two measuring bases to measure the photons in their hands independently. They keep the correlate results for generating the key $K_A$. In the same year, Cleve et al. utilized the properties of quantum error-correcting code to propose the first $(k, n)$ threshold of QSS protocol. In a $(k, n)$ threshold scheme, any subset of $k$ or more parties can reconstruct the secret, while any subset of $k-1$ or fewer parties can obtain no information [56]. In 2001, Tittel et al. used the experiment to realize quantum secret sharing for the first time [54]. In 2002, Tyc et al. developed the theory of continuous variable quantum secret sharing and propose its interferometric realization using passive and active optical elements [57]. In 2003, Gou et al. presented a quantum secret sharing scheme where only product states are employed [58]. Xiao et al. showed that in the Hillery-Bužek-Berthiaume QSS scheme [59], and the secret information is shared in the parity of binary strings formed by the measured outcomes of the participants in 2004. With the rapid development of QSS, people are researching to achieve unconditional security.

### 5.1. QSS based on entanglement states

Quantum entanglement is an indispensable physical resource in QSS. Many application fields of QSS such as this entanglement feature, so the study of entanglement is the core issue of quantum information theory.

Let's see the QSS based on entanglement. The entanglement states are all generated by the sender, and the order of two or more photons sent to the same agent is randomly changed. After the photons send to the receiver, for the detection mode, the order of the two photons is announced, so that the two parties detected the security of the quantum channel, for the information mode, the two receivers respectively does Bell measurement on the two photons they owned, and then communicate through classical channel to share the secret key with the sender. This protocol ensures the validity and security of the shared information.

We can see an example of QSS based on entanglement state GHZ [55].

Let us suppose that Alice, Bob, and Charlie each have one particle from a GHZ triplet that is in the state $|\psi\rangle = {}^{1}\!/\!_{\sqrt{2}}(|000\rangle + |111\rangle)$. They each choose at random whether to measure their particle in the x or y direction. They then announce publicly in which direction they have made a measurement, but not the results of their measurements. Half the time, Bob and Charlie, by combining the results of their measurements, can determine what the result of Alice's measurement was. This allows Alice to establish a joint key with Bob and Charlie, which she can then use to send her message. Let us see how this works in more detail. Define the $x$ and $y$ eigenstates

$$\begin{aligned} |+x\rangle &= 1/\sqrt{2}(|0\rangle + |1\rangle), \quad |+y\rangle = 1/\sqrt{2}(|0\rangle + i|1\rangle), \\ |-x\rangle &= 1/\sqrt{2}(|0\rangle - |1\rangle), \quad |-y\rangle = 1/\sqrt{2}(|0\rangle - i|1\rangle). \end{aligned} \tag{16}$$

We can see the effects of measurements by Alice and Bob on the state of Charlie's particle if we express the GHZ state in different ways. Noting that

$$|0\rangle = 1/\sqrt{2}(|+x\rangle + |-x\rangle), \quad |1\rangle = 1/\sqrt{2}(|+x\rangle - |-x\rangle), \tag{17}$$

we can write

$$\begin{aligned} |\psi\rangle = 1/2\sqrt{2}[&(|+x\rangle_a|+x\rangle_b + |-x\rangle_a|-x\rangle_b)(|0\rangle_c + |1\rangle_c) \\ &+ (|+x\rangle_a|-x\rangle_b + |-x\rangle_a|+x\rangle_b)(|0\rangle_c - |1\rangle_c)]. \end{aligned} \tag{18}$$

This decomposition of $|\psi\rangle$ tells us what happens if both Alice and Bob make measurements in the $x$ direction. If they both get the same result, then Charlie will have the state $1/\sqrt{2}(|0\rangle_c + |1\rangle_c)$; if they get different results, he will have the state $1/\sqrt{2}(|0\rangle_c - |1\rangle_c)$. He can determine which of these states he has by performing a measurement along the $x$ direction. The following table summarizes the effects of Alice's and Bob's measurements on Charlie's state:

| | | **Alice** | | | |
|---|---|---|---|---|---|
| | | *+x* | *-x* | *+y* | *-y* |
| Bob | *+x* | $\|0\rangle + \|1\rangle$ | $\|0\rangle - \|1\rangle$ | $\|0\rangle - i\|1\rangle$ | $\|0\rangle + i\|1\rangle$ |
| | *-x* | $\|0\rangle - \|1\rangle$ | $\|0\rangle + \|1\rangle$ | $\|0\rangle + i\|1\rangle$ | $\|0\rangle - i\|1\rangle$ |
| | *+y* | $\|0\rangle - i\|1\rangle$ | $\|0\rangle + i\|1\rangle$ | $\|0\rangle - \|1\rangle$ | $\|0\rangle + \|1\rangle$ |
| | *-y* | $\|0\rangle + i\|1\rangle$ | $\|0\rangle - i\|1\rangle$ | $\|0\rangle + \|1\rangle$ | $\|0\rangle - \|1\rangle$ |

**Table 2.** QSS based on entanglement state [55].

Alice's measurements are given in the columns and Bob's are given in the rows. Charlie's state, up to normalization, appears in the boxes. From the table it is clear that if Charlie knows what measurements Alice and Bob made (that is, $x$ or $y$), he can determine whether their results are the same or opposite and also that he will gain no knowledge of what their results actually

are. Similarly, Bob will not be able to determine what Alice's result is without Charlie's assistance because he does not know if his result is the same as Alice's or the opposite of hers.

To improve the efficiency of QSS, a protocol share the message directly among the users was proposed. The scheme made full use of entanglement swapping of Bell states and local operations. For detection of eavesdropping, the EPR pairs were divided into two parts: the checking parts and the encoding parts. After insuring the security of the quantum channel by measuring the checking particles in conjugate bases, the sender encoded her bits via the local unitary operations on the encoding parts. And the protocol is secure, and two Bell states can be used to share two bits message. And there is a scheme for multiparty quantum secret sharing which is based on EPR entangled state. In the scheme, the secret messages are imposed on the auxiliary particles, and the transmitted particles of EPR pairs do not carry any secret messages during the whole process of transmission. After both of the communicators reliably share the EPR entangled states, all the participants can securely share the secret messages of the sender. Because there is no particles that carrying the secret message being transmitted on the quantum channel during the process of transmission, the scheme can efficiently resist the eavesdropper's attack on secret message.

So, entanglement makes an important role in quantum secret sharing and many application fields of quantum information theory such as quantum teleportation, QKD, quantum computing need to use this entanglement feature. But the quantification of the entanglement receives a better solution only for bipartite quantum system, and the quantification of multipartite entanglement is still open even for a pure multipartite state. Until now, a variety of different entanglement measures have been proposed for multipartite setting, such as the robustness of entanglement, the relative entropy of entanglement, and the geometric measure.

However, all these methods involve variable complexity problem, which make the quantification of multipartite entanglement very difficult. Fortunately, it is hopeful to obtain the exact value of the multipartite entanglement of graph states, which are very useful multipartite quantum states in quantum information processing. Graph states are the specific algorithm resources for one-way quantum computing model, and they are subsets of stabilizer states which are widely used in quantum error correction.

### 5.2. QSS with qudit graph states

The quantification of entanglement has attracted wide attention in recent years, but the quantification of the entanglement receives a better solution only for bipartite quantum system. And the quantification of multipartite entanglement is still open even for a pure multipartite state. Until now, a variety of different entanglement measures have been proposed for multipartite setting, such as the robustness of entanglement, the relative entropy of entanglement, and the quantification of multipartite entanglement is still open even for a pure multipartite state. Fortunately, it is hopeful to obtain the exact value of the multipartite entanglement of graph states, which are useful multipartite quantum states in quantum information processing.

The entanglement quantification of graph state is relatively simple, for it can be described by graph language. So far, the study of graph state entanglement has just started, the latest research results is determining the upper and lower bounds of graph state entanglement by using local operation and classical communication, which can only confirm the entanglement of graph states that have equal bounds. But for graph states which have unequal bounds, it can only give a range of entanglement but not the exact value.

In quantum computing, a graph state is a special type of multi-qubit state that can be represented by a graph. Each qubit is represented by a vertex of the graph, and there is an edge between every interacting pair of qubits. In particular, they are a convenient way of representing certain types of entangled states.

Given a graph $G=(V, E)$with the set of vertices $V$ and the set of edges $E$, the corresponding graph

$$\left|G\right\rangle = \prod_{(a,b)\in E} U^{\{a,b\}} \left|+\right\rangle^{\otimes V}, \tag{19}$$

where the operator $U^{\{a,b\}}$ is the controlled-Z interaction between the two vertices (qubits) $a$, $b$,

$$U^{\{a,b\}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

And $|+\rangle = {}^{1}/_{\sqrt{2}}(|0\rangle + |1\rangle)$. With each graph $G=(V, E)$, we associate a graph state. A graph state is a certain pure quantum state on a Hilbert space $H_V = (C^2)^{\otimes V}$.

An alternative and equivalent definition is the following. Hence each vertex labels a two-level quantum system or qubit — a notion that can be extended to quantum systems of finite dimension $d$. To every vertex $a \in V$ of the graph $G=(V, E)$ is attached a Hermitian operator

$$K_G^{(a)} = \sigma_x^{(a)} \prod_{b\in N_a} \sigma_z^{(b)}. \tag{20}$$

In terms of the adjacency matrix, this can be expressed as

$$K_G^{(a)} = \sigma_x^{(a)} \prod_{b\in V} (\sigma_z^{(b)})^{\Gamma_{ab}}. \tag{21}$$

As usual, the matrices $\sigma_x^{(a)}$, $\sigma_y^{(a)}$, $\sigma_z^{(a)}$ are the Pauli matrices, where the upper index specifies the Hilbert space on which the operator acts $K_G^{(a)}$ is an observable of the qubits associated with

http://dx.doi.org/10.5772/56092

the vertex $a$ and all of its neighbors $b \in N_a$. The graph state $|G\rangle$ is then defined as the simultaneous eigenstate of the $N = |V|$ operators $\{K_G^{(a)}\}_{a \in V}$ with eigenvalue 1:

$$K_G^{(a)}|G\rangle = |G\rangle. \tag{22}$$

Here they consider three specific varieties of such schemes previously demonstrated in graph states. They note that all existing forms of secret sharing that have been proposed fall into one of these categories. [60]

1. CC scheme: The secret is classical, the dealer is connected to the player via private quantum channels and all players are connected by private classical channels.
2. CQ scheme: The secret is classical, the dealer shares public quantum channels with each player and the players are connected to each by private classical channels.
3. QQ scheme: The secret is quantum, the dealer shares either private or public quantum channels with each player and the players are connected to each other by private quantum or classical channels.

Now let's see an example of QSS with graph states. It is the third scenario presented in the previous QQ scheme. This QQ scheme proposed is readily generalisable to qudits. In this scheme, the secret to be shared is a quantum state $|s\rangle$ in a $d$-dimensional Hilbert space now, initially possessed by the dealer, who distributes it to the other parties via a joint operation on the secret state and parties' shared graph state, in a manner analogous to quantum teleportation. We describe the general protocol explicitly below.

Denoting the dealer's secret qudit as

$$|s\rangle_D = \sum_{i=0}^{d-1} \alpha_i |i\rangle_D. \tag{23}$$

The dealer prepares the state $|s\rangle_D |G\rangle_{D,V}$. Corresponding to some graph state $G$ for the dealer's qudit $D$ and all the players' qudits $V$. The dealer distributes the player's qudits to them. The dealer then measures her two qudits in the generalized Bell basis $\{|\psi\rangle_{mn}\}$, where

$$|\psi_{mn}\rangle := \frac{1}{\sqrt{d}} \sum_j \omega^{jn} |j\rangle |j+m\rangle \tag{24}$$

If the dealer's measurement result is $(m, n)$, corresponding to the state $|\psi\rangle_{mn}$, then it follows from the rules for projective measurement that the resultant state for all parties is

$$\begin{aligned} & |\psi_{mn}\rangle_D \langle\psi_{mn}||s\rangle_D |G\rangle_{D,V} \\ \propto \quad & |\psi_{mn}\rangle_D \sum \alpha_j \omega^{-jn} \left| g_{z=(j+m)(A_{D1},A_{D2},\cdots,A_{DN})} \right\rangle_V \end{aligned} \tag{25}$$

where $|g_z\rangle$ is the encoded reduced graph state on the players 1, ⋯, $n$ with labels $z$.

If the dealer informs the players of their measurement result ($m$, $n$), then a set of players $\in V$ can apply a correction operator

$$U_{mn} := K_a^{-nN_{D_a}^{-1}} Z^{-mA_D} \tag{26}$$

to obtain the state

$$\left| s_g \right\rangle^V = \sum_j \alpha_j \left| g_{z=j(A_{D1},A_{D2},\cdots,A_{DN})} \right\rangle_V . \tag{27}$$

The access properties of this final state depend on the graph state used. Qualitatively, for certain initial graph states, the state $|s_g\rangle^V$ can be regarded as a superposition of orthogonal labelled graph states whose labels have the same access structure as CC protocols. Thus, the ability to recover the quantum secret corresponds to the ability to recover these classical labels, providing a natural extension of the classical protocols to the quantum case.

## 6. Post-quantum cryptography

Post-quantum cryptography deals with cryptosystems that run on conventional computers and are secure against attacks by quantum computers. This field came about because most currently popular public-key cryptosystems rely on the integer factorization problem or discrete logarithm problem, both of which would be easily solvable on large enough quantum computers using Shor's algorithm. Even though current publicly known experimental quantum computing is nowhere near powerful enough to attack real cryptosystems, many cryptographers are researching new algorithms, in case quantum computing becomes a threat in the future.

In contrast, most current symmetric cryptography (symmetric ciphers and hash functions) is secure from quantum computers. The quantum Grover's algorithm can speed up attacks against symmetric ciphers, but this can be counteracted by increasing key size. Thus post-quantum cryptography does not focus on symmetric algorithms. Post-quantum cryptography is also unrelated to quantum cryptography, which refers to using quantum phenomena

to achieve secrecy. Currently post-quantum cryptography is mostly focused on four different approaches:

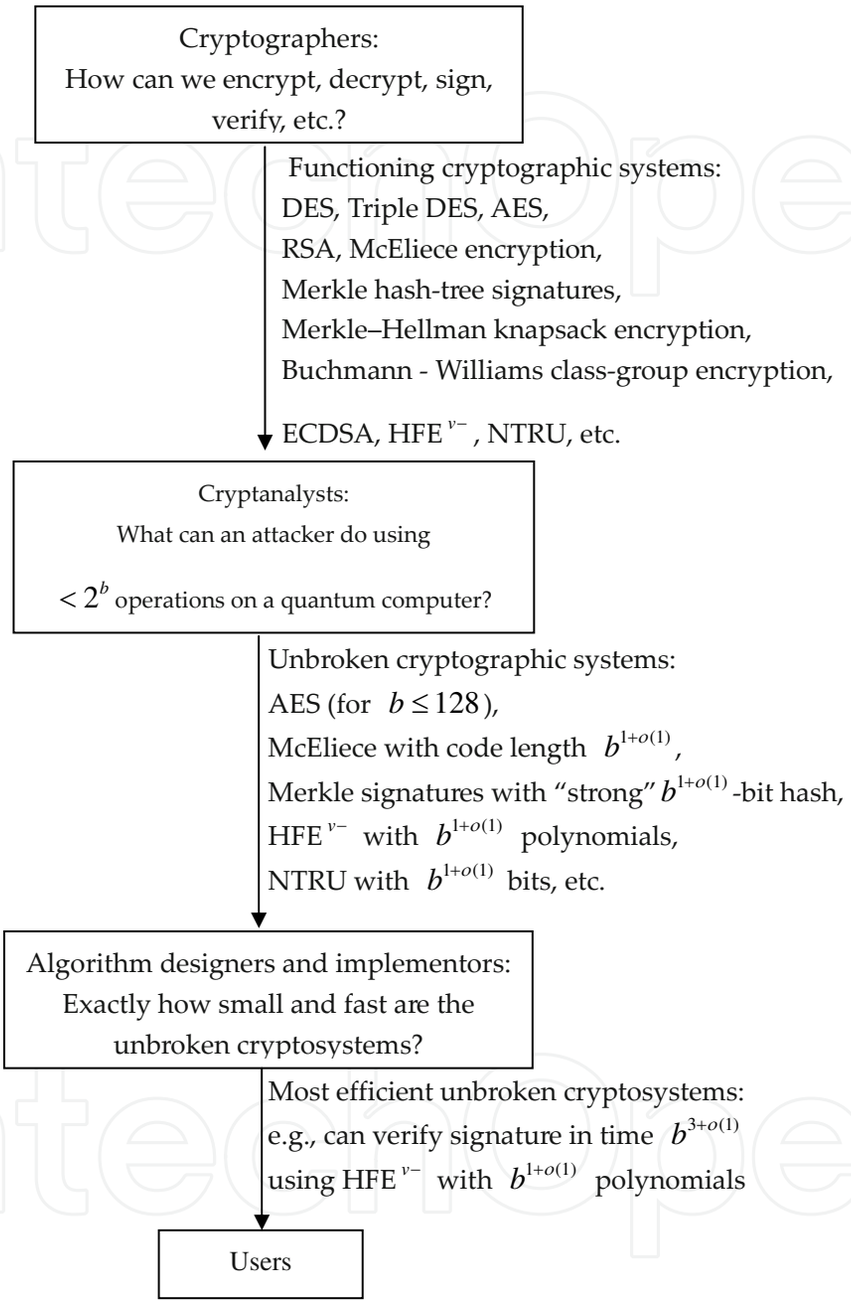


**Figure 4.** Post-quantum cryptography. Sizes and times are simplified to $b^{1+o(1)}$, $b^{2+o(1)}$, etc. Optimization of any specific b requires a more detailed analysis.

1. Lattice-based cryptography such as NTRU and GGH;
2. Multivariate cryptography such as unbalanced oil and vinegar;
3. Hash-based signatures such as Lamport signatures and Merkle signature scheme;

4. Code-based cryptography that relies on error-correcting codes, such McEliece encryption and Niederreiter signatures.

We can use the following figure to show the content of post-quantum cryptography clearly [7].

Post-quantum cryptography is, in general, a quite different topic from quantum cryptography:

- Post-quantum cryptography, like the rest of cryptography, covers a wide range of secure-communication tasks, ranging from secret-key operations, public-key signatures, and public-key encryption to high-level operations such as secure electronic voting. Quantum cryptography handles only one task, namely expanding a short shared secret into a long shared secret.
- Post-quantum cryptography, like the rest of cryptography, includes some systems proven to be secure, but also includes many lower-cost systems that are conjectured to be secure. Quantum cryptography rejects conjectural systems — begging the question of how Alice and Bob can securely share a secret in the first place.
- Post-quantum cryptography includes many systems that can be used for a noticeable fraction of today's Internet communication—Alice and Bob need to perform some computation and send some data but do not need any new hardware. Quantum cryptography requires new network hardware that is, at least for the moment, impossibly expensive for the vast majority of Internet users.

## Acknowledgements

This work was conducted when Xiaoqing Tan visited the University of Toronto and is supported by the NSFC 61003258. She especially thanks Hoi-Kwong Lo for the hospitality during her stay at the University of Toronto.

## Author details

Xiaoqing Tan*

Address all correspondence to: ttanxq@jnu.edu.cn

Dept. of Mathematics, Jinan University, Guangzhou, Guangdong, China

## References

[1] Wiesner, S. Conjugate coding," *Sigact News,* (1983). , 15(1), 78-88.

[2] Bennett, C. H, Bessette, F, & Brassard, G. *et al.*, "Experimental quantum cryptography," in Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology, Aarhus, Denmark, (1991). , 253-265.

[3] Bennett, C. H, Brassard, G, & Crepeau, C. *et al.*, "Practical Quantum Oblivious Transfer," in Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, (1992). , 351-366.

[4] Brassard, G, Crepeau, C, & Jozsa, R. *et al.*, "A quantum bit commitment scheme provably unbreakable by both parties," in Proceedings of the 1993 IEEE 34th Annual Foundations of Computer Science, (1993). , 362-371.

[5] Lo, H. -K, & Zhao, Y. Quantum Cryptography," http://arxiv.org/abs/0803.2507/.

[6] Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," http://arxiv.org/abs/quant-ph/9508027.

[7] Bernstein, D. J. Introduction to post-quantum cryptography " *Post-quantum cryptography*, (2009).

[8] Townsend, P. D, Rarity, J. G, & Tapster, P. R. Single photon interference in a 10 km long optical fibre interferometer," *Electronics Letters,* (1993). , 29(7), 634-635.

[9] Townsend, P. D, Rarity, J. G, & Tapster, P. R. Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel," *Electronics Letters,* (1993). , 29(14), 1291-1293.

[10] Einstein, A, Podolsky, B, & Rosen, N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?," *Physical Review,* (1935). , 47(10), 777-780.

[11] Kumar, M. *Quantum*: London : Icon books, (2009).

[12] Horodecki, R, Horodecki, P, & Horodecki, M. *et al.*, "Quantum entanglement," *Reviews of Modern Physics,* (2009). , 81(2), 865-942.

[13] Jaeger, G, Shimony, A, & Vaidman, L. Two interferometric complementarities," *Physical Review A,* (1995). , 51(1), 54-67.

[14] Vernam, G. S. Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications," *American Institute of Electrical Engineers, Transactions of the,* vol. XLV, (1926). , 295-301.

[15] Bennett, C. H, & Brassard, G. Quantum cryptography: Public key distribution and coin tossing},," in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, India, (1984). , 175.

[16] Mayers, D. Unconditional security in quantum cryptography," *J. ACM,* (2001). , 48(3), 351-406.

[17] Lo, H. -K, & Chau, H. F. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances," *Science,* March 26, 1999, (1999). , 283(5410), 2050-2056.

[18] Stebila, D, Mosca, M, & Lütkenhaus, N. The Case for Quantum Key Distribution," *Quantum Communication and Quantum Networking*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering A. Sergienko, S. Pascazio and P. Villoresi, eds., Springer Berlin Heidelberg, (2010). , 283-296.

[19] Ekert, A. K. Quantum cryptography based on Bell's theorem," *Physical Review Letters,* (1991). , 67(6), 661-663.

[20] Bennett, C. H, Brassard, G, & Mermin, N. D. Quantum cryptography without Bell's theorem," *Physical Review Letters,* (1992). , 68(5), 557-559.

[21] Grosshans, F, Van Assche, G, & Wenger, J. *et al.*, "Quantum key distribution using gaussian-modulated coherent states," *Nature,* Jan 16, (2003). , 421(6920), 238-241.

[22] Bing QiLi Qian, and H.-K. Lo. "A brief introduction of quantum cryptography for engineers," http://arxiv.org/abs/1002.1237.

[23] Renner, R, & Cirac, J. I. de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography," *Physical Review Letters,* Mar 20, (2009). , 102(11)

[24] Lodewyck, J, Bloch, M, & Garcia-patron, R. *et al.*, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Physical Review A,* Oct, (2007). , 76(4)

[25] Qi, B, Huang, L. -L, & Qian, L. *et al.*, "Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," *Physical Review A,* (2007). , 76(5), 052323.

[26] Ekert, A. Complex and unpredictable Cardano," *International Journal of Theoretical Physics,* Aug, (2008). , 47(8), 2101-2119.

[27] Van Dam, W, Ariano, G. M. D, & Ekert, A. *et al.*, "Optimal phase estimation in quantum networks," *Journal of Physics a-Mathematical and Theoretical,* Jul 13, (2007). , 40(28), 7971-7984.

[28] Christandl, M, Datta, N, & Ekert, A. *et al.*, "Perfect state transfer in quantum spin networks," *Physical Review Letters,* May 7, (2004). , 92(18)

[29] Lo, H. K, Ma, X. F, & Chen, K. Decoy state quantum key distribution," *Physical Review Letters,* Jun 17, (2005). , 94(23)

[30] Curty, M, Gühne, O, & Lewenstein, M. *et al.*, "Detecting two-party quantum correlations in quantum-key-distribution protocols," *Physical Review A,* (2005). , 71(2), 022306.

[31] Lütkenhaus, N. Security against eavesdropping in quantum cryptography," *Physical Review A,* (1996). , 54(1), 97-111.

[32] Biham, E, & Mor, T. Security of Quantum Cryptography against Collective Attacks," *Physical Review Letters,* (1997). , 78(11), 2256-2259.

[33] Biham, E, & Mor, T. Bounds on Information and the Security of Quantum Cryptography," *Physical Review Letters,* (1997). , 79(20), 4034-4037.

[34] Gisin, N, Ribordy, G, & Tittel, W. *et al.*, "Quantum cryptography," *Reviews of Modern Physics,* (2002). , 74(1), 145-195.

[35] Barrett, J, Hardy, L, & Kent, A. No signaling and quantum key distribution," *Physical Review Letters,* Jul 1, (2005). , 95(1)

[36] Brassard, G. Brief history of quantum cryptography: a personal perspective." , 19-23.

[37] Zhao, Y, Fung, C. -H. F, & Qi, B. *et al.*, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Physical Review A,* (2008). , 78(4), 042333.

[38] Hwang, W. -Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Physical Review Letters,* (2003). , 91(5), 057901.

[39] Mayers, D. Unconditionally Secure Quantum Bit Commitment is Impossible," *Physical Review Letters,* (1997). , 78(17), 3414-3417.

[40] Pironio, S, Acín, A, & Brunner, N. *et al.*, "Device-independent quantum key distribution secure against collective attacks," *New Journal of Physics,* (2009). , 11(4), 045021.

[41] Bennett, C. H, & Di, D. P. . Smolin *et al.*, "Mixed-state entanglement and quantum error correction," *Physical Review A,* vol. 54, no. 5, pp. 3824-3851, 1996.

[42] Deutsch, D, Ekert, A, & Jozsa, R. *et al.*, "Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels," *Physical Review Letters,* (1996). , 77(13), 2818-2821.

[43] Shor, P. W, & Preskill, J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters,* (2000). , 85(2), 441-444.

[44] Biham, E, Boyer, M, & Boykin, P. O. *et al.*, "A proof of the security of quantum key distribution (extended abstract)," in Proceedings of the thirty-second annual ACM symposium on Theory of computing, Portland, Oregon, United States, (2000). , 715-724.

[45] Ben-or, M. (2002). http://www.msri.org/publications/ln/msri/2002/qip/ben-or/1/index.html.

[46] Renner, R, & Koenig, R. Universally composable privacy amplification against quantum adversaries."

[47] Renner, R. Security of Quantum Key Distribution," http://arxiv.org/abs/quant-ph/0512258.

[48] Renner, R. Symmetry of large physical systems implies independence of subsystems," *Nat Phys,* (2007). , 3(9), 645-649.

[49] Horodecki, K, Horodecki, M, & Horodecki, P. *et al.*, "Secure Key from Bound Entanglement," *Physical Review Letters,* (2005). , 94(16), 160502.

[50] Karol HorodeckiMichal Horodecki, Pawel Horodecki *et al.* "Quantum key distribution based on private states: unconditional security over untrusted channels with zero quantum capacity," http://arxiv.org/abs/quant-ph/0608195.

[51] Koashi, M. Complementarity, distillable secret key, and distillable entanglement," (2007).

[52] Acín, A, Brunner, N, & Gisin, N. *et al.*, "Device-Independent Security of Quantum Cryptography against Collective Attacks," *Physical Review Letters,* (2007). , 98(23), 230501.

[53] LlMasanes, R. Renner, M. Christandl *et al.*, "Unconditional security of key distribution from causality constraints," (2006).

[54] Tittel, W, Zbinden, H, & Gisin, N. Experimental demonstration of quantum secret sharing," *Physical Review A,* (2001). , 63(4), 042301.

[55] Hillery, M, Bužek, V, & Berthiaume, A. Quantum secret sharing," *Physical Review A,* (1999). , 59(3), 1829-1834.

[56] Cleve, R, Gottesman, D, & Lo, H. -K. How to Share a Quantum Secret," *Physical Review Letters,* (1999). , 83(3), 648-651.

[57] Tyc, T, & Sanders, B. C. How to share a continuous-variable quantum secret by optical interferometry," *Physical Review A,* Apr, (2002). , 65(4)

[58] Guo, G. -P, & Guo, G. -C. Quantum secret sharing without entanglement," *Physics Letters A,* (2003). , 310(4), 247-251.

[59] Xiao, L, Lu, G, Long, F, & Deng, G. *et al.*, "Efficient multiparty quantum-secret-sharing schemes," *Physical Review A,* (2004). , 69(5), 052307.

[60] Keet, A, Fortescue, B, & Markham, D. *et al.*, "Quantum secret sharing with qudit graph states," *Physical Review A,* (2010). , 82(6), 062315.