# Quantum Information Protocols for Cryptography

**Bassem Abd-El-Atty, Salvador E. Venegas-Andraca and Ahmed A. Abd El-Latif**

**Abstract** Quantum cryptography is a robust field of quantum computation and quantum information that focuses on protecting data secrecy by using properties of quantum-mechanical systems. Over the last few years, quantum cryptography has evolved into an emergent high-tech market with companies capable of delivering off-the-shelf products. This chapter introduces a succinct overview of some fundamental concepts of quantum computation, quantum information protocols and their use on the development of quantum cryptography protocols. Key concepts include quantum key distribution, quantum secret sharing, quantum secure direct communication, and deterministic secure quantum communication.

## 1 Introduction to Quantum Cryptography

Nowadays, computers are key resources in all branches of science, engineering, commerce, and business in general. Indeed, computer science and computer engineering have pervaded every aspect of modern society. The complex relationship between computer science and computer engineering includes the following aspects:

- Computer science provides the fundamental mathematical structures required to build both specific- and general-purpose computers (automata theory) as well as to quantify the amount of resources needed to execute an algorithm (complexity theory). Computer science serves as a guide to understand and estimate the capacities and limits of practical computers and algorithm design.

B. Abd-El-Atty · A.A. Abd El-Latif (✉)
Faculty of Science, Department of Mathematics, Menoufia University,
Menofia Governorate 32511, Egypt
e-mail: a.rahiem@gmail.com; ahmed_rahiem@yahoo.com

S.E. Venegas-Andraca
Escuela de Ingenieria y Ciencias, Tecnologico de Monterrey,
Ave. Eugenio Garza Sada 2501, 64849 Monterrey, N.L., México, Mexico
e-mail: salvador.venegas-andraca@keble.oxon.org



A.E. Hassanien et al. (eds.), *Quantum Computing: An Environment for Intelligent Large Scale Real Application*, Studies in Big Data 33,
https://doi.org/10.1007/978-3-319-63639-9_1

- Open problems and engineering challenges faced at the development of computer technology usually become a decisive resource to produce new scientific questions, among them the need to develop new abstract models of computers.
- Ultimately, information is processed, stored and transmitted by physical systems. Indeed, theoretical computer science is a branch of mathematics but the actual manufacture and behavior of tangible computers and communications systems is fundamentally described by the laws of physics.
- Since the 1950s, the development of computer industry is based on transistor technology whose behavior, due to transistor size, has been largely described by classical physics.

The birth and evolution of quantum computation, the interdisciplinary scientific and engineering field devoted to build information processing systems using the quantum mechanical properties of Nature, is an example of the mutual fertilization of computer science and computer technology described above:

- On the one hand, the idea of using quantum mechanical systems in order to simulate other quantum mechanical systems is the very theoretical foundation of quantum computers as introduced by Feynman [1].
- On the other hand, current semiconductor-based transistors for computer technology are now at the nano scale level. The state-of-the-art of transistor technology has two important consequences for quantum computation: (a) the description and dynamics of nano-transistors require quantum mechanics [2] and (b) the end of Moore's law beseeches new technologies for the computer industry, being quantum computation a leading and most promising paradigm [3].

Physics and computer science have cross-fertilized each other for long time. For example, in trying to quantify the minimum amount of energy required to perform a computation, von Neumann [4] showed that "a minimum amount of energy required per elementary decision of a two-way alternative and the elementary transmittal of one unit of information" was close to $kT$, where $k$ is Boltzmann's constant and $T$ is the temperature of the system. Later on, Landauer studied the relationship between energy consumption and reversible computation [5] and Bennet presented a formal reversible version of a Universal Turing Machine [6]. Another famous side of this cross-fertilization is the field of algorithms inspired in the mathematical description of physical phenomena, e.g., simulated annealing [7] and percolation theory [8].

Quantum computation and quantum information are scientific and engineering disciplines devoted to the development of novel quantum algorithms and quantum information processing protocols and devices. Some key results in quantum computation include the discovery of quantum teleportation [9, 10] which consists of transmitting quantum information (originally contained in a qubit) via a quantum channel, quantum dense coding [11, 12] which allows sending two classical bits using only one qubit, quantum steganography [13–15] and quantum cryptography [16–44].

Quantum cryptography is a robust field of science and engineering that evolved in an emergent high-tech market with companies capable of delivering off-the-shelf

products [45, 46]. Quantum cryptography protocols can be categorized into quantum key distribution protocols (QKD) [16–18], quantum secret sharing protocols (QSS) [19–22], quantum secure direct communication protocols (QSDC) [23–38] and deterministic secure quantum communication protocols (DSQC) [39–44].

Let us now provide a succinct introduction to some fundamental concepts of quantum computation needed to formally describe quantum cryptography protocols.

## *1.1 Concise Introduction to Preliminary Mathematics and Fundamentals of Quantum Computation*

Section 1.1 is based on [47, 48].

### 1.1.1 The Qubit

In classical computation, information is stored and manipulated in the form of bits. The mathematical structure of a classical bit is rather simple. It suffices to define two logical values, traditionally labelled as $\{0, 1\}$ (i.e. a classical bit lives in a scalar space) and to relate those values to two different and mutually exclusive outcomes of a classical measurement.

In quantum computation, information is stored, manipulated and measured in the form of qubits. A qubit is a physical entity described by the laws of quantum mechanics. A qubit may be mathematically represented as a unit vector in a two-dimensional Hilbert space $|\psi\rangle \in \mathscr{H}^2$ (for the purposes of this chapter, a Hilbert space is a complex inner-product vector space, e.g., $\mathbb{C}^n$). A qubit $|\psi\rangle$ may be written in general form as

$$|\psi\rangle = \alpha|p\rangle + \beta|q\rangle \tag{1}$$

where $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$ and $\{|p\rangle, |q\rangle\}$ is an arbitrary basis spanning $\mathscr{H}^2$. Note that a most important consequence of the vectorial nature of a qubit is the possibility of writing it as a linear combination of elements of any basis (this is known as the principle of superposition.)

The choice of $\{|p\rangle, |q\rangle\}$ is often *the orthonormal* basis

$$\{|0\rangle, |1\rangle\}$$

known as **the computational basis**. In addition to the computational basis $\{|0\rangle, |1\rangle\}$, it is customary in quantum cryptography protocols to use **the diagonal basis**

$$\{|+\rangle, |-\rangle\}$$

defined as $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$.

### 1.1.2 Dirac Notation

The symbol $|\cdot\rangle$ is known as a ket. We can always represent kets $|\psi\rangle$ of $\mathscr{H}^2$ as column vectors by choosing a basis for $\mathscr{H}^2$. For example, let $\mathscr{H}^2 = \mathbb{C}^2$ be a 2-dimensional Hilbert space and let us choose the vector basis $\{|0\rangle, |1\rangle\}$, where

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2}$$

Then, every element $|\psi\rangle \in \mathscr{H}^2$ can be written as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \alpha, \beta \in \mathbb{C}.$$

We can also define bras, which formally speaking are functionals (i.e. functions of vector spaces into corresponding fields) and in practice can be thought of as row vectors:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \text{ if and only if } \langle\psi| = \alpha^*\langle 0| + \beta^*\langle 1|$$

For example, let

$$|\psi\rangle = \frac{i}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{i}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

The corresponding bra $\langle\psi|$ is

$$\langle\psi| = \frac{-i}{\sqrt{2}}(1,\ 0) + \frac{1}{\sqrt{2}}(0,\ 1) = (\frac{-i}{\sqrt{2}}, \frac{1}{\sqrt{2}}) = \frac{-i}{\sqrt{2}}\langle 0| + \frac{1}{\sqrt{2}}\langle 1|$$

Thus, if $\mathscr{H}$ is an n-dimensional Hilbert space then the ket $|\psi\rangle \in \mathscr{H}$ can be represented as an n-dimensional column vector, and its corresponding bra $\langle\psi| \in \mathscr{H}^*$ can be seen as an n-dimensional row vector; $|\psi\rangle \leftrightarrow \langle\psi|$ corresponds to transposition and conjunction. Kets and bras are succinctly referred to as **Dirac notation**.

### 1.1.3 Inner and Outer Products

We can use Dirac notation to make calculations. For example, $\langle\phi|\psi\rangle$ is the usual row-column matrix operator that computes the *inner product* in finite dimensional vector spaces.

Let us take the representations of $|0\rangle$ and $|1\rangle$ given in Eq. (2). Note that $|0\rangle \perp |1\rangle$ as well as the fact that both vectors have unitary norm. Consequently, the inner product of $|0\rangle$ and $|1\rangle$ must be zero and the inner product of each vector with itself must be equal to one:

$$\langle 0|1\rangle = (1,\ 0)\begin{pmatrix}0\\1\end{pmatrix} = (1\times 0 + 0\times 1) = 0 = (0\times 1 + 1\times 0) = (0,\ 1)\begin{pmatrix}1\\0\end{pmatrix} = \langle 1|0\rangle$$

Moreover

$$\langle 0|0\rangle = (1,\ 0)\begin{pmatrix}1\\0\end{pmatrix} = (1\times 1 + 0\times 0) = 1 = (0\times 0 + 1\times 1) = (0,\ 1)\begin{pmatrix}0\\1\end{pmatrix} = \langle 1|1\rangle$$

We may also use kets and bras to create linear operators (i.e. linear functions between vector spaces). Let $|\psi\rangle, |a\rangle \in \mathscr{H}_1$ and $|\phi\rangle \in \mathscr{H}_2$ then the *outer product* is the linear operator from $\mathscr{H}_1$ to $\mathscr{H}_2$ defined by

$$(|\phi\rangle\langle\psi|)|a\rangle \equiv (\langle\psi|a\rangle)|\phi\rangle$$

As it may be expected, the summation of outer products is also a linear operator. For example, let us define the Hadamard operator

$$\hat{H} = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$$

The action of $\hat{H}$ on the ket $|0\rangle$ is given by

$$\begin{aligned}\hat{H}|\psi\rangle &= (\tfrac{1}{\sqrt{2}}|0\rangle\langle 0| + \tfrac{1}{\sqrt{2}}|0\rangle\langle 1| + \tfrac{1}{\sqrt{2}}|1\rangle\langle 0| - \tfrac{1}{\sqrt{2}}|1\rangle\langle 1|)|0\rangle \\ &= \tfrac{\langle 0|0\rangle}{\sqrt{2}}|0\rangle + \tfrac{\langle 1|0\rangle}{\sqrt{2}}|0\rangle + \tfrac{\langle 0|0\rangle}{\sqrt{2}}|1\rangle - \tfrac{\langle 1|0\rangle}{\sqrt{2}}|1\rangle \\ &= \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\end{aligned}$$

### 1.1.4 Quantum Measurements

In quantum mechanics, measurement is a non-trivial and highly counter-intuitive process. Firstly, because measurement outcomes are probabilistic: regardless of the carefulness in the preparation of a measurement procedure, the possible outcomes of such measurement will be distributed according to a certain probability distribution. Secondly, once a measurement has been performed, a quantum system is unavoidably altered due to the interaction with the measurement apparatus. Consequently, for an arbitrary quantum system, pre-measurement and post-measurement quantum states are different in general. Thirdly, in order to perform a measurement it is needed to define a set of measurement operators. This set of operators must fulfill a number of rules that allows one to compute the actual probability distribution as well as post-measurement quantum states.

Quantum measurements are described by a set of measurement operators $\{\hat{M}_m\}$ where index $m$ labels the different measurement outcomes. Measurement outcomes correspond to values of *observable*, such as position, energy and momentum.

Let $|\psi\rangle$ be the state of the quantum system immediately before the measurement. Then, the probability that result $m$ occurs is given by

$$p(m) = \langle\psi|\hat{M}_m^\dagger \hat{M}_m|\psi\rangle \tag{3}$$

and the post-measurement quantum state is

$$|\psi\rangle_{pm} = \frac{\hat{M}_m|\psi\rangle}{\sqrt{\langle\psi|\hat{M}_m^\dagger \hat{M}_m|\psi\rangle}}. \tag{4}$$

Let us work out a simple example. Assume we have a polarized photon with associated polarization orientations 'horizontal' and 'vertical'. The horizontal polarization direction is denoted by $|0\rangle$ and the vertical polarization direction is denoted by $|1\rangle$.

Thus, an arbitrary initial state for our photon can be described by the quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha$ and $\beta$ are complex numbers constrained by the normalization condition $|\alpha|^2 + |\beta|^2 = 1$ and $\{|0\rangle, |1\rangle\}$ is the computational basis spanning $\mathscr{H}^2$.

Now, we construct two measurement operators $\hat{M}_0 = |0\rangle\langle 0|$ and $\hat{M}_1 = |1\rangle\langle 1|$ and two measurement outcomes $a_0, a_1$. Then, the full *observable* used for measurement in this experiment is $\hat{M} = a_0|0\rangle\langle 0| + a_1|1\rangle\langle 1|$. According to Eq. (3), the probabilities of obtaining outcome $a_0$ or outcome $a_1$ are given by $p(a_0) = |\alpha|^2$ and $p(a_1) = |\beta|^2$. Corresponding post-measurement quantum states (Eq. (4)) are as follows: if outcome $= a_0$ then $|\psi\rangle_{pm} = |0\rangle$; if outcome $= a_1$ then $|\psi\rangle_{pm} = |1\rangle$.

The following results shall be used in the next section:

### 1.1.5 Entanglement

Entanglement is a unique type of correlation shared between components of a quantum system. Entangled quantum systems are often best used collectively, i.e. an optimal use of entangled quantum systems for information storage and retrieval must manipulate and measure those systems as a whole, rather than on an individual basis.

The concept of correlation is deeply rooted in every branch of science. A typical and simple example is the following experiment: let us suppose we have two balls, one white and one black, as well as two boxes. If we randomly put a ball in each box and then close both boxes, we need to perform only one experiment, that is, to open one box, in order *to know which of the balls is in each box*. In other words, by means of one measurement, namely opening one box and seeing which ball was stored in it, we obtain two pieces of information, namely the colour of the ball stored in both boxes.

The former experiment is an example of classical correlation. Quantum entanglement is also a kind of correlation, but one that has been detected only in quantum phenomena so far.

For example, consider the following 2-particle state:

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{5}$$

Clearly, $|\Psi^-\rangle$ lives in a four-dimensional Hilbert space. It can be seen, after some calculations, that it is impossible to find quantum states $|a\rangle, |b\rangle \in \mathscr{H}^2$ such that $|a\rangle \otimes |b\rangle = |\Psi^-\rangle$, that is, $|\Psi^-\rangle$ is not a product state of $|a\rangle$ and $|b\rangle$. This is indeed a criterion to determine whether a quantum state is entangled or not, whether it is possible to express such a composite quantum state as a simple tensor product of quantum subsystems.

Another example is the tripartite entangled GHZ state

$$|GHZ\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}} \tag{6}$$

Again, it is not possible to find three quantum states $|a\rangle, |b\rangle, |c\rangle \in \mathscr{H}^2$ such that $|a\rangle \otimes |b\rangle \otimes |c\rangle = |GHZ\rangle$.

## 2 Quantum Key Distribution Protocols

The quantum key distribution protocols we shall review in this chapter are methodologies designed and implemented to produce and distribute private keys. The importance of (quantum) private keys is described in the following lines.

Cryptography is the branch of science and engineering devoted to the design and implementation of techniques for secure communication, under the assumption that a third party is interested in reading our messages. In other words, cryptography is the science of keeping information secure [49]. Encryption is the process of transforming plaintext (i.e. the actual message) into a ciphertext (i.e. a coded message) by using a cryptosystem. Decryption is the inverse process, i.e. transforming a ciphertext into a plain message. Cryptanalysis is the field focused on recovering the plain text breaking the encryption method used to produce the ciphertext [49].

Modern cryptography has two types of encryption: symmetric key and asymmetric key cryptosystems. Let us briefly describe each type.

- Symmetric key cryptosystems, also known as private key cryptosystems, are encryption algorithms that use a single key for both encryption and decryption of the ciphertext. In this field, algorithms for encryption and decryption are known while the key must remain private, i.e. secret [50].

- Asymmetric key cryptosystems use two keys: a public key and a private key, the public key is used for encryption and the private key for decryption. These cryptosystems work under the rationale of a safe with two keys: the key to lock the safe is known by everybody but the key for opening is available to only one person [49, 50].

Private key cryptosystems can be very powerful. For example, the cryptosystem known as the one-time pad (also known as the Vernam cipher) can be proved to be perfectly secured as long as the key is truly random, the length of the key is equal to the size of the message and the key is only used once [50]. Other private key cryptosystems include the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) [49, 50].

One of the most sensible issues with private key cryptosystems is safe key distribution, i.e. the process of establishing a private key between two users who cannot use a perfectly secure communication channel [50]. For example, this situation may arise if two users, who do not share secrete information a priori, need to contact each other urgently. The issue is the fact that, if the channel used to distribute a private key is governed by the laws of classical physics, then in principle any (classical) key can be passively eavesdropped, i.e. without users becoming aware of this vulnerability [50].

Quantum key distribution protocols use properties of quantum mechanical systems in order to significantly enhance the security of key distribution channels. Let us now introduce the BB84 and E91 quantum key distribution protocols.

### *2.1 BB84*

In 1984, Charles Bennett and Gilles Brassard [16] proposed a quantum key distribution protocol known as BB84. The key idea of BB84 is to produce a key by encoding bits in qubits that are taken from a set composed by the union of the computational and diagonal bases, i.e. a set of four *non-orthogonal* quantum states. Proofs of the security of BB84 against attacks of eavesdropping strategies have been presented in [51, 52].

Let us suppose the following setting: two people, usually referred to as Alice and Bob, want to create a key for encoding a message. The key, to be shared by Alice and Bob, must be random and secret. There is a third character in this scenario: Eve, an eavesdropper. The conflict in this story is: Alice and Bob's key need their key to be secret and Eve will do anything in her power to reveal at least some portions of the key. Note that the purpose of BB84 is to produce a key, i.e. actual encoded data transmission is *not* part of the BB84.

In the following lines, we present the BB84 protocol step by step. Hereinafter, we assume that:
(a) Alice has a source of individual photons as well as the experimental equipment and expertise to manipulate the polarization of her photons. Moreover, she has access to a source of random bits.
(b) There is a channel available to Alice and Bob that they can use to send quantum states (e.g., an optical fiber.)
(c) Bob has the experimental facilities and expertise required to measure quantum states using different bases.
(d) Finally, Alice and Bob have a classical channel (e.g., a telephone line) that may or may not be a secure line, it does not really matter.

The BB84 protocol is composed of the following steps [53]:

1. Alice starts by generating two sets of *random* bits $A = \{a_1, a_2, \ldots a_n\}$ and $B = \{b_1, b_2, \ldots b_n\}$
2. Alice uses the set of random bits $A$ to select the vector basis with which she will prepare the initial polarization state of her photons, according to the following criterion: Alice will read one bit at a time from set $A$ and, depending on her reading (either 0 or 1), she will choose the computational basis (+) or the diagonal basis (×) to prepare her photons. In computational terms, this step would be more or less equivalent to variable initialization.
   For instance, let us suppose that $A = \{0, 1, 0, 0, 1, 0, 1, 1, 1, 0\}$ and that Alice has *chosen* the following criterion: if 0 then use the computational basis; if 1 then use the diagonal basis. Then, Alice would initialize her qubits using the following list: $(+, \times, +, +, \times, +, \times, \times, \times, +)$.
3. So far, Alice has a random list of vector space bases $(+, \times)$ to initialize her photons. Now, Alice must *randomly* choose one vector from each basis to prepare the polarization initial state of each photon. To do so, Alice will use the elements of set $B$ according to the following function:

$$\text{initial polarization state} = \begin{cases} |0\rangle \text{ (or } |1\rangle) & \text{if } (+, 0) \\ |1\rangle (\text{ or } |0\rangle) & \text{if } (+, 1) \\ |+\rangle (\text{ or } |-\rangle) & \text{if } (\times, 0) \\ |-\rangle (\text{ or } |+\rangle) & \text{if } (\times, 1) \end{cases}$$

   Following the example presented in the previous step, let us suppose that $B = \{1, 0, 1, 0, 1, 0, 0, 1, 0, 1\}$ and that Alice's list for preparing the initial polarization state of her photons is $(+, \times, +, +, \times, +, \times, \times, \times, +)$. Moreover, let us suppose that she has decided to prepare her photons according to the following

$$\text{initial polarization state} = \begin{cases} |0\rangle & \text{if } +, 1) \\ |1\rangle & \text{if } +, 0) \\ |+\rangle & \text{if } \times, 0) \\ |-\rangle & \text{if } (\times, 1) \end{cases}$$

Then, her photons will have the following initial polarization states:

$$\{|0\rangle, |+\rangle, |0\rangle, |1\rangle, |-\rangle, |1\rangle, |+\rangle, |-\rangle, |+\rangle, |0\rangle\}$$

4. Alice sends her qubit sequence (step 3) to Bob via the quantum channel they both have access to. This step is Eve's chance to extract information from the quantum channel. We now describe two strategies that Eve may try to follow, together with an explanation of why such strategies would fail:

   a. To *perfectly* copy photon polarization states on the fly. Eve may try to design a device $D_{\hat{U}}(|\psi\rangle_i|0\rangle) = |\psi\rangle_i|\psi\rangle$ to allow her to perform the following operation:

   $$\hat{U}(|\psi\rangle_i|0\rangle) = |\psi\rangle_i|\psi\rangle$$

   where $\hat{U}$ must be a unitary operator (this is a requisite imposed by the mathematical structure of quantum mechanics), $|\psi\rangle_i$ is the polarization state of photon $i$ and $|0\rangle$ is the initial state of a qubit (e.g., the polarization state of a photon contained in the device). In this strategy, Eve intends to copy quantum states as photon travel along the quantum channel, it is *not* her intention to perturb the photons sent by Alice in any sense.
   The no-cloning theorem [54, 55], a most remarkable and counter-intuitive result of quantum mechanics, prevents the realization of a device that makes *clones*, i.e. perfect copies, of arbitrary quantum states. In other words, the no-cloning theorem makes Eve's device $D_U$ impossible to create.

   b. To measure photon polarization states followed by preparing new photons for Bob. In this case, Eve intercepts photon $i$ and measures its polarization state. Moreover and based on the information extracted from photon $i$, Eve prepares a new photon and sends it to Bob.
   In order to measure photon $i$, Eve must choose a basis to build the corresponding measurement operators. Eve may know that Alice has prepared her qubits using the computational and diagonal bases, but she does not know the order in which bases were picked, hence she does not know for sure which measurement operators she must use in order to extract information from the photon sequence; in fact, Eve can only *guess* which basis she should use for measuring each photon.
   Let us then suppose that Eve randomly chooses to use the computational basis or the diagonal basis to measure photon polarization states. Of course,

**Table 1** Probabilities and post-measurement quantum states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ and measurement operators $|0\rangle\langle 0|, |1\rangle\langle 1|$

| Qubit | Measurement operator | $p(0)$ | $\|\psi\rangle_{pm}^{0}$ | Measurement operator | $p(1)$ | $\|\psi\rangle_{pm}^{1}$ |
|---|---|---|---|---|---|---|
| $\|0\rangle$ | $\hat{M}_0 = \|0\rangle\langle 0\|$ | 1 | $\|0\rangle$ | $\hat{M}_1 = \|1\rangle\langle 1\|$ | 0 | $\nexists$ |
| $\|1\rangle$ | $\hat{M}_0 = \|0\rangle\langle 0\|$ | 0 | $\nexists$ | $\hat{M}_1 = \|1\rangle\langle 1\|$ | 1 | $\|1\rangle$ |
| $\|+\rangle$ | $\hat{M}_0 = \|0\rangle\langle 0\|$ | 1/2 | $\|0\rangle$ | $\hat{M}_1 = \|1\rangle\langle 1\|$ | 1/2 | $\|1\rangle$ |
| $\|-\rangle$ | $\hat{M}_0 = \|0\rangle\langle 0\|$ | 1/2 | $\|0\rangle$ | $\hat{M}_1 = \|1\rangle\langle 1\|$ | 1/2 | $\|1\rangle$ |

**Table 2** Probabilities and post-measurement quantum states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ and measurement operators $|+\rangle\langle +|, |-\rangle\langle -|$

| Qubit | Measurement operator | $p(+)$ | $\|\psi\rangle_{pm}^{0}$ | Measurement operator | $p(-)$ | $\|\psi\rangle_{pm}^{1}$ |
|---|---|---|---|---|---|---|
| $\|0\rangle$ | $\hat{M}_+ = \|+\rangle\langle +\|$ | 1/2 | $\|+\rangle$ | $\hat{M}_- = \|-\rangle\langle -\|$ | 1/2 | $\|-\rangle$ |
| $\|1\rangle$ | $\hat{M}_+ = \|+\rangle\langle +\|$ | 1/2 | $\|+\rangle$ | $\hat{M}_- = \|-\rangle\langle -\|$ | 1/2 | $\|-\rangle$ |
| $\|+\rangle$ | $\hat{M}_+ = \|+\rangle\langle +\|$ | 1 | $\|+\rangle$ | $\hat{M}_- = \|-\rangle\langle -\|$ | 0 | $\nexists$ |
| $\|-\rangle$ | $\hat{M}_+ = \|+\rangle\langle +\|$ | 0 | $\nexists$ | $\hat{M}_- = \|-\rangle\langle -\|$ | 1 | $\|-\rangle$ |

Eve will make right choices sometimes and will be wrong some other times. Let us analyze both cases:

i. Right choice of measurement operators. For example, let us suppose that the polarization state of photon $i$ is $|1\rangle$ and that Eve has chosen the computational basis $\{|0\rangle, |1\rangle\}$ to produce $\{\hat{M}_0, \hat{M}_1\}$. Hence, the probability of measuring outcome 0 is 1, i.e. $p(0) = 1$, and the corresponding post-measurement state is $|0\rangle$, i.e. $|\psi\rangle_{pm}^{0} = |0\rangle$, (please see Table 1). After learning that the polarization of photon $i$ is $|0\rangle$, Eve prepares a new photon $i'$ and sends it to Bob. Since Eve has sent to Bob the same quantum state that Alice prepared, her eavesdropping will go unnoticed (Table 2).

ii. Wrong choice of measurement operators. For example, Eve chooses the diagonal basis $\{|+\rangle, |-\rangle\}$ to measure photon $j$ whose polarization state is $|0\rangle$. Then, according to the rules of quantum mechanics, the probability of having $|+\rangle$ as post-measurement quantum state is $1/2$ and, correspondingly, the probability of having $|-\rangle$ as post-measurement quantum state is also $1/2$. Here, Eve faces two problems: she has not extracted any information from photon $j$ and the photon that she will prepare and send to Bob will be different from the photon sent by Alice, hence there is room for detecting her eavesdropping activity (remember that BB84 is about safely creating a private key, not about transmitting any message between Alice and Bob, so detecting Eve's activity does not jeopardize the message itself, it only renders the key unusable.)

So, if Eve randomly chooses between the computational basis and the diagonal basis to measure photon polarization states, it is reasonable to expect that she will be successful only half of the time, hence her chances of making a mistake are high (50%), an unacceptable scenario for a professional spy.

5. Let us now describe Bob's activities. Bob knows that Alice has prepared her qubits using either the computational basis or the diagonal basis but, just like Eve, he does not know the order in which Alice chose between those vector bases. So, Bob randomly selects the vector basis he will use to produce the corresponding measurement operators (i.e. he randomly chooses $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$) and measures the polarization states of the photons he receives at his end. The result of this procedure will be a list $C$ composed of ordered pairs (*basis*,*outcome*) where *basis* is either + or × and *outcome* is either 0 or 1.
6. Once the full photon sequence has been processed as described above, Alice and Bob use a classical channel (a telephone line or e-mail, for instance) to tell each other the sequence of basis they use to initialize and measure photon polarization states, respectively. Alice and Bob will discard those outcomes that correspond to disagreements of initialization and measurement bases (for instance, if Alice used $\{|0\rangle, |1\rangle\}$ to prepare photon $i$ and Bob used basis $\{|+\rangle, |-\rangle\}$ to measure the same photon $i$) and will keep the remaining outcomes. Let us label the remaining bit sequences os Alice and Bob as $R_A$ and $R_B$, respectively.
   Assuming no interference on the quantum channel, $R_A$ and $R_B$ must be identical, that is, Alice and Bob have succeeded at producing a private key $K(= R_A = R_B.)$ However, it is reasonable to assume some discrepancies between $R_A$ and $R_B$ due to errors in transmission and/or Eve's activity. In this case, Alice and Bob may follow error correction and privacy amplification procedures in order to produce two identical bit strings $R_A^{'}$ and $R_B^{'}$, that is, the private key $K(= R_A = R_B)$ they needed to generate.

A succinct example of BB84 is presented on Table 3.

**Table 3** Example of the BB84 protocol in action

| Alice's bits | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alice's bases | + | + | × | + | × | + | × | + | × | + | × | × |
| Alice's qubits | $\|0\rangle$ | $\|0\rangle$ | $\|+\rangle$ | $\|0\rangle$ | $\|+\rangle$ | $\|1\rangle$ | $\|-\rangle$ | $\|0\rangle$ | $\|-\rangle$ | $\|1\rangle$ | $\|+\rangle$ | $\|-\rangle$ |
| Eve's bases | + | × | + | + | × | × | + | × | + | + | + | + |
| Eve's measurements | $\|0\rangle$ | $\|+\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|+\rangle$ | $\|0\rangle$ | $\|0\rangle$ | $\|+\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|0\rangle$ |
| Bob's bases | × | + | + | + | × | × | × | + | + | + | + | × |
| Bob's measurements | $\|+\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|+\rangle$ | $\|-\rangle$ | $\|+\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|+\rangle$ |
| Bob's bits | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| Selection | | • | | • | • | | • | • | | • | | • |

### *2.2 E91*

In 1991, Ekert [17] proposed a quantum key distribution protocol based on Bell states and known as E91. Bell states, presented in Eqs. (7a–7d), constitute a widely used set of entangled states

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{7a}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{7b}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{7c}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{7d}$$

When Alice holds the first particle and Bob holds the second particle, this implies that the measurement results of Alice and Bob are completely correlated with each other when they used one of two bases (+, ×) to measure the state. Eve has no information about the particles (qubits) hold by Alice and Bob, due to the two particles are in entangled state and Eve cannot reach the two particles in the same time. To transmit the whole key, Alice and Bob generate a large numbers of Bell states and measure each particle in separate way. E91 is composed of the following steps:

1. Alice generates a sequence of Bell states.
2. Alice randomly selects a subset of this sequence and applies the Hadamard transformation on the first particle for each pair when the corresponding bit string is '1'.
3. Alice sends the sequence of second qubits to Bob and holds the sequence of first qubits.
4. Alice tells Bob the bits of string and which qubits are selected.
5. Bob applies the Hadamard transformation on the selected qubits where the bit string is '1'.
6. Both Alice and Bob measure the selected qubits with same bases and delete the bits which are of different bases and the remaining bits are called shifted key. Then they check the exiting of Eve by estimate the error-rate of choosing a subset of the sifted key. If the bits are differing, they abort the protocol.
7. Finally, by performing error correction Alice and Bob obtain the secret key.

Without performing Hadamard transformation on the first qubit (which is equivalent to transforming + into ×, Eve could easily attack the protocol via intercept-resend attack.

## 3 Quantum Secret Sharing Protocols (QSS)

Secret sharing, as one of the most important branches in cryptography, is a technique developed to distribute a secret message to several parties so that no participant can access and read the secret message without the collaboration of other parties. To further illustrate the observations, imagine Alice holding a secret message and want to gain access for both Bob and Charlie. She knows that one of them is dishonest and she does not know which the honest one is. So, Alice cannot send the secret message directly to both of them, because the dishonest one will steal the information, but she knows that if Bob and Charlie carry out it together, the honest one will keep the dishonest one from doing any damage.

Quantum secret sharing (QSS) firstly proposed by Hillery et al. [19] in 1999, namely Hillery's protocol. It's based on three-particle quantum entangled states and the classical secret sharing protocol presented by Shamir [56] in 1979. Then, Anders Karlsson et al. [20] presented a new QSS protocol based on entangled two-photon states. Thereafter, several QSS protocols have been proposed, for example, but not limited, [19, 20].

Herein, we shed the light to QSS protocol in [19]. This protocol uses Greenberger-Horne-Zeilinger (GHZ) three-particle states. Supposing that there are three participants Alice, Bob and Charlie, each of them in possession of one particle of the GHZ state presented in Eq. (8)

$$|\Psi\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}} \tag{8}$$

All participants randomly choose to measure their own particles using directions $x$ or $y$. Then they communicate with each other to declare which direction they used in measurement process, without announcing their measurement results. By combining the measurement results of Alice and Bob, they can determine the measurement result of Charlie. This allows Charlie to build up a joint key with Alice and Bob, which can be used to send the secret message. The directions of particles $x$ and $y$ are defined as follows:

$$|x^{\pm}\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}} \tag{9a}$$

$$|y^{\pm}\rangle = \frac{|0\rangle \pm i|1\rangle}{\sqrt{2}} \tag{9b}$$

If Alice and Bob perform their measurement in the $x$ direction and they want to get information about Charlie's particle. The GHZ state can be written as

$$|\Psi\rangle = \frac{(|x^{+}\rangle_a|x^{+}\rangle_b + |x^{-}\rangle_a|x^{-}\rangle_b)(|0\rangle_c + |1\rangle_c) + (|x^{+}\rangle_a|x^{-}\rangle_b + |x^{-}\rangle_a|x^{+}\rangle_b)(|0\rangle_c - |1\rangle_c)}{2\sqrt{2}} \tag{10}$$

From Eq. (10), if Alice and Bob have the same result of measurement, then they conclude that Charlie have the state $\frac{|0\rangle_c+|1\rangle_c}{\sqrt{2}}$, otherwise he have the state $\frac{|0\rangle_c-|1\rangle_c}{\sqrt{2}}$. Similarly, Bob and Charlie can determine the quantum state of Alice by combining their results of measurement. Generally, no one of the three participants can determine the quantum state of each other without combining their results.

Now, what happens if the participants choose to measure their own particles in any direction without announcing their measurement basis. In other words, how to determine whether the participant's measurements are correlated or not. The answer is, all participant's particles must be measured in the same direction. For example, if both Bob and Charlie measure their particles in the $x$ direction. Alice must also measure her particle in $x$ direction. Otherwise, she gains no information from her result. Therefore, all the three participants must announce their measurements basis to each other to decide whether measurement basis to keep or which to discard.

## 4 Quantum Secure Direct Communication Protocols (QSDC)

Quantum secure direct communication (QSDC) protocols differ from QKD, QSS and DSQC protocols as a secret message in QSDC protocols is transmitted by the quantum channel directly without having to share a private key between two legitimate users beforehand. There are three requirements should be satisfied in any secure QSDC protocol:

1. Before the sender (Alice) and the receiver (Bob) communicate to encode their secret message on the quantum states, they can detect the exiting of the eavesdropper (Eve).
2. Bob can read the secret message directly without establishing additional classical channels with Alice to exchange the secret key and ensure the security of the protocol.
3. In any type of attacks performed by Eve, no any useful information stolen about the transmitted secret message.

In 2002, Beige et al. [23] proposed the first QSDC protocol based on the exchange of single photons and each photon transmits one bit of the secret message. In the same year, Boström et al. [24] presented a ping-pong QSDC scheme based on EPR pairs. In 2003, Deng and Long [25] introduced a two-step QSDC scheme based on dense coding operations. In 2004, Deng and Long [26] introduced another QSDC protocol based on a sequence of single photons. Then, several QSDC protocols are proposed to carry the secret message based on single photons and entangled particles through a quantum channel. In the literature, there are several QSDC protocols utilized entangled particles in their internal structure such as EPR pairs [27, 28], Greenberger-Horne-Zeilinger (GHZ) [29], cluster states [30], W states [31] and $\chi$-type states [32]. EPR pairs are more easily prepared and therefore widely used. In fact, single photons have several advantages that lead to the development of quantum communication protocols such as flexible implementation, high efficiency as

well as simple operations. In 2004, Deng and Long [26] developed a QSDC scheme by using batches of single photons, which serves as quantum one-time pad cryptosystem. In 2006, Wang et al. [33] proposed a QSDC scheme based on order rearrangement of single photons, in which all single photons are used to encode the secret message except those used for eavesdropping check. In the same year, Li et al. [34] presented a deterministic QSDC scheme by using a sequence of single photons. In 2010, Quan et al. [35] proposed a one-way DQSDC scheme by using a sequence of single photons. In 2013, Chang et al. [36] proposed quantum secure direct communication and authentication protocol with single photons and XOR operation. In 2015, Zhao [37] proposed two quantum secure communication protocols based on single photon sequence and the XOR operation. Also, in the same year, Xin et al. [38] proposed a quantum authentication protocol based on Hash function and Bell states. Hereinafter, we introduce examples of these protocols.

### *4.1 QSDC Deng-Long Protocol*

As mentioned above, quantum communication protocols based on single photons are easier to implement than quantum protocols based on entangled states. Therefore, Deng and Long presented a QSDC protocol [26] based on QKD idea. In this protocol, Alice shares with Bob a sequence of single photon states, then Alice encodes the secret message and transmits the photon states to Bob. The detailed steps of QSDC Deng-Long protocol is given below:

1. Bob generates a sequence $S$ of single photons in one of the four polarized states $|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ which the polarized states $|0\rangle$ and $|+\rangle$ represent the binary value 0, the polarized states $|1\rangle$ and $|-\rangle$ represent the binary value 1 and sends these sequence $S$ to Alice. To check the security of the protocol, Bob selects a subset group of photons in sequence S and tells Alice the positions of the selected group. Alice measures the photons in the selected group using the same basis and compares the results of measurement with Bob. If their results are the same, there is no attack and the quantum channel is secure, otherwise, the connection is not secure and they abort from the quantum channel.
2. To encode the secret message, Alice performs the unitary transformation $U_0$ and $U_1$ which represent binary values 0 and 1, respectively on each photon in the selected positions according to the secret message. where

$$U_0 = |0\rangle\langle 0| + |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \tag{11a}$$

$$U_1 = |0\rangle\langle 1| - |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = i\sigma_Y \tag{11b}$$

3. Alice sends the result of the sequence $S$ to Bob. Bob knows the initial state of photon polarization and the selected positions, due to the sequence is generated by her. Then Bob measure each photon in the selected positions by the original basis and deduce the secret message from the unitary transformation Alice applied on the selected photons.

### *4.2 QSDC Deng Protocol*

Deng et al. [25] presented a two-step QSDC protocol, which the first QSDC protocol based on Bell states. In this protocol, Alice generates a sequence of entangled particles all in $|\Phi\rangle^+$ state. Alice separates the sequence of particles into two subsequences. The first subsequence called the message-carrier and labels it as SA. The second subsequence called the checking and labels it as SB. At first Alice and Bob agree that classical bits 00, 01, 10 and 11 correspond to the four Bell states $|\Psi\rangle^+, |\Psi\rangle^-, |\Phi\rangle^+, |\Phi\rangle^-$, respectively. Then, Alice sends the sequence SB to Bob. To check the security of the established quantum channel, Bob selects randomly a subset of photons in the sequence SB and measures this selected group by one of the two basis ($Z$ and $X$). Thus, Bob communicates with Alice via a classical channel to tells here the positions of photons in the selected group. Then, Alice measures the corresponding photons in sequence SA using the same basis. Alice's result is then compared with Bob's result via the classical channel. If two results are completely opposite, there is no attack performed by Eve, otherwise Eve performed attack and they must abort the connection. After that Alice encodes her secret message by applying unitary transformations ($\sigma_I, \sigma_z, \sigma_x, \sigma_{iy}$) on their own particles in the selected positions to transform the Bell state to another Bell state (see Table 4) according to the encoded secret message and sends the result sequence SA to Bob. Then Bob extract the secret message from the Bell states in the selected position utilizing Bell measurements.

where,

$$\sigma_I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{12a}$$

**Table 4** The relationship between the initial Bell states and the final Bell states

| | $\sigma_I$ | $\sigma_X$ | $\sigma_Z$ | $i\sigma_Y$ |
|---|---|---|---|---|
| $\|\Phi^+\rangle$ | $\|\Phi^+\rangle$ | $\|\Psi^+\rangle$ | $\|\Phi^-\rangle$ | $\|\Psi^-\rangle$ |
| $\|\Phi^-\rangle$ | $\|\Phi^-\rangle$ | $\|\Psi^-\rangle$ | $\|\Phi^+\rangle$ | $\|\Psi^+\rangle$ |
| $\|\Psi^+\rangle$ | $\|\Psi^+\rangle$ | $\|\Phi^+\rangle$ | $\|\Psi^-\rangle$ | $\|\Phi^-\rangle$ |
| $\|\Psi^-\rangle$ | $\|\Psi^-\rangle$ | $\|\Phi^-\rangle$ | $\|\Psi^+\rangle$ | $\|\Phi^+\rangle$ |

$$\sigma_X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{12b}$$

$$\sigma_Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{12c}$$

$$i\sigma_Y = |0\rangle\langle 1| - |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \sigma_Z\sigma_X \tag{12d}$$

## 5 Deterministic Secure Quantum Communication Protocols (DSQC)

The deterministic secure quantum communication (DSQC) protocols are designed to obtain deterministic information, not random information. It is similar to QKD protocols which at first generate a key to encrypt the secret message. In DSQC, Bob can extract the secret message by using for each transmitted qubit at least an additional classical bit. So the classical channels are needed besides the DSQC protocols. In 2004, Cai and Li [56] presented a DSQC protocol based on single qubit in a mixed state and its security based on the security of BB84 protocol. In 2005, Gao et al. [39] proposed a DSQC protocol based on GHZ states and entanglement swapping. In 2006, Shaari et al. [40] presented a two-way deterministic protocol using six mutually unbiased states in the Poincare sphere which the information are encoded by not-flip or flip operations on the states. Also, in the same year, Li et al. [41] presented two DSQC protocols, one based on d-dimensional single-photon states and the other based on pure entangled states which single-photon measurements are only used for the two participants in these two protocols. In 2012, Huang et al. [42] proposed two DSQC protocols with collective detection, one is a DSQC network and the other is a two-party DSQC scheme. Finally, in 2015, Yan et al. [43] presented a controlled DSQC protocol based on three-particle GHZ state in X-basis.

Let us now describe one of these DSQC protocols in details. Huang et al. [42] presented a two-party DSQC protocol using single photons with collective detection. In this protocol, Alice and Bob perform single-photon measurements on their photons and communicate via classical channel to exchange a certain classical information bits. This protocol based on collective detection strategy, which is used to detect any attack on the quantum protocol after the whole process of qubit transmission and reduces the cost of protocol realization.

At first in this protocol, Alice and Bob share a sequence of single photons, and then Alice encodes the message using two unitary operations then encrypts the encoded states using a tilt-adjustable phase plate. After receiving Bob the sequence of photons from Alice via quantum channel, he can decode the message with the help of transmitted classical information bits via classical channel. The steps of this protocol can be described as follows:

1. Bob prepares a sequence of single photons all in the state $|+\rangle$ and sends the sequence to Alice.
2. After receiving the sequence, Alice generates a random string $M$ with length equal to the number of elements in Bob's sequence of states $S$.
3. Alice apply on the photon sequence $S$ a phase shift $\psi_i \in \{0, \pi/2, \pi, 3\pi/2\}$ to encode 00, 01, 10 and 11, respectively.
4. Alice randomly chooses some polarized photons in sequence S as decoy states and performs unitary transformation $\sigma_i$ and $\sigma_z$ on the polarized photons in selected positions, then Alice sends the sequence to Bob.
5. To check eavesdropping via classical channel:
   - At first Alice tells Bob the positions of decoy photons and the corresponding values of $M$ for each decoy particle.
   - Then Bob measures each decoy photon using $\{|+\rangle, |-\rangle, |s\rangle, |t\rangle\}$ to obtain corresponding values, where $|s\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}$ and $|t\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$
   - Bob estimates the error rate and decides whether they abort the protocol; otherwise, they go to the next step.
6. Bob measures each photon in the sequence with measurement basis $\{|+\rangle, |-\rangle, |s\rangle, |t\rangle\}$ to reveal the encoded secret message $M$.

The main advantage of this protocol is that Alice and Bob can utilize all transferred polarized photons to transmit the secret message, except for the ones used for eavesdropping check.

## References


1. Feynman, R.P.: Simulating physics with computers. Int. J. Theor. Phys. **21**(6/7), 467–488 (1982)
2. Svizhenko, A., Anantram, M.P., Govindan, T.R., Biegel, B., Venugopal, R.: Two-dimensional quantum mechanical modeling of nanotransistors. J. Appl. Phys. **91**(4), 2343–2354 (2002)
3. IEEE. Rebooting Computing Initiative. http://rebootingcomputing.ieee.org/
4. von Neumann, J.: Fourth University of Illinois Lecture (Theory of self-reproducing Automata). University of Illinois Press (1966)
5. Landauer, R.: Irreversibility and heat generation in the computing process. IBM J. Res. Dev. **5**(3), 183–191 (1961)
6. Landauer, R.: Logical reversibility of computation. IBM J. Res. Dev. **17**(6), 525–532 (1973)
7. Kirkpatrick, S., Gelatt, C.D. Jr., Vecchi, M.P.: Optimization by simulated annealing. Science **220**(4598), 671–680 (1983)
8. Mertens, S., Moore, C.: Continuum percolation thresholds in two dimensions. Phys. Rev. E **86**, 061109 (2012)
9. Bennett, H.C., Brassard, G., Crpeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **70**(13), 1895–1899 (1993)
10. Lee, J., Kim, M.S.: Entanglement teleportation via werner states. Phys. Rev. Lett. **84**(18), 4236–4239 (2000)
11. Bennett, C.H., Wiesner, S.J.: Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys. Rev. Lett. **69**(20), 2881–2884 (1992)

12. Mermin, N.D.: Deconstructing dense coding. Phys. Rev. A. **66**, 032308 (2002)
13. Abd-El-Atty, B., Abd El-Latif, A.A., Amin, M.: New quantum image steganography scheme with Hadamard transformation. In: International Conference on Advanced Intelligent Systems and Informatics, pp. 342–352, Springer International Publishing (2016)
14. Jiang, N., Zhao, N., Wang, L.: LSB based quantum image steganography algorithm. Int. J. Theor. Phys. **55**(1), 107–123 (2015)
15. Wang, S., Sang, J., Song, X., Niu, X.: Least significant qubit (LSQb) information hiding algorithm for quantum images. Measurement **73**, 352–359 (2015)
16. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179, Bangalore, India (1984)
17. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6), 661–663 (1991)
18. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell's theorem. Phys. Rev. Lett. **68**(5), 557–559 (1992)
19. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**(3), 1829–1834 (1999)
20. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**(1), 162–168 (1999)
21. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum secret-sharing schemes. Phys. Rev. A **69**, 052307 (2004)
22. Chen, P., Long, G.L., Deng, F.G.: High-dimension multiparty quantum secret sharing scheme with Einstein-Podolsky-Rosen pairs. Chin. Phys. B **15**, 2228–2235 (2006)
23. Beige, A., Englert, B.G., Urtsiefer, C.K., Weinfurter, H.: Secure communication with a publicly known key. Acta Physica Polonica A **101**(3), 357–368 (2002)
24. Bostrom, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002)
25. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys. Rev. A **68**, 042317 (2003)
26. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**, 052319 (2004)
27. Yin, X., Ma, W., Shen, D., Hao, C.: Efficient three-party quantum secure direct communication with EPR pairs. Quantum Inf. Sci. **3**, 1–5 (2013)
28. Zhang, C., Long, G.F.: Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs. Sci. Chin. Phys. Mech. Astron. **57**(7), 1238 (2014)
29. Man, Z.X., Xia, Y.J., An, N.B.: Quantum secure direct communication by using GHZ states and entanglement swapping. J. Phys. B **39**(18), 3855–3863 (2006)
30. Chang, Y., Zhang, S.B., Yan, L.L.: A bidirectional quantum secure direct communication protocol based on five-particle cluster state. Chin. Phys. Lett. **30**, 090301 (2013)
31. Cao, H.J., Song, H.S.: Quantum secure direct communication with W state. Chin. Phys. Lett. **23**, 290–292 (2006)
32. Lin, S., Wen, Q.Y., Gao, F., Zhu, F.C.: Quantum secure direct communication with $\chi$-type entangled states. Phys. Rev. A **78**, 064304 (2008)
33. Wang, J., Zhang, Q., Tang, C.J.: Quantum secure direct communication based on order rearrangement of single photons. Phys. Lett. A **358**, 256–258 (2006)
34. Li, X.H., Deng, F.G., Li, C.Y., Liang, Y.J., Zhou, P., Zhou, H.Y.: Deterministic secure quantum communication without maximally entangled states. J. Korean Phys. Soc. **49**, 1354–1359 (2006)
35. Quan, D.X., Pei, C.X., Liu, D., Nan, Z.: One-way deterministic secure quantum communication protocol based on single photons. Acta. Phys. Sin. **59**, 2493–2497 (2010)
36. Chang, Y., Xu, C.X., Zhang, S.B., Yan, L.L.: Quantum secure direct communication and authentication protocol with single photons. Chin. Sci. Bull. **58**(36), 4571–4576 (2013)
37. Zhao, G.: Quantum secure communication protocol based on single-photon. Int. J. Sec. Appl. **9**(3), 267–274 (2015)

38. Xin, X., Hua, X., Song, J., Li, F.: Quantum authentication protocol for classical messages based on bell states and hash function. Int. J. Sec. Appl. **9**(7), 285–292 (2015)
39. Cai, Q.Y., Li, B.W.: Deterministic secure communication without using entanglement. Chin. Phys. Lett. **21**(4), 601 (2004)
40. Gao, T., Yan, F.L., Wang, Z.X.: Deterministic secure direct communication using GHZ states and swapping quantum entanglement. J. Phys. A Math. Gen. **38**(25), 5761 (2005)
41. Shaari, J.S., Lucamarini, M., Wahiddin, M.R.B.: Deterministic six states protocol for quantum communication. Phys. Lett. A **358**(2), 85–90 (2006)
42. Li, X., Deng, F.G., Li, C.Y., Liang, Y.J., Zhou, P., Zhou, H.Y.: Quantum secure direct communication without maximally entangled states. J. Korean Phys. Soc. **49**, 1354–1359 (2006)
43. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Chen, H.: Deterministic secure quantum communication with collective detection using single photons. Int. J. Theor. Phys. **51**(9), 2787–2797 (2012)
44. Yan, C., Shi-Bin, Z., Li-Li, Y., Gui-Hua, H.: Controlled deterministic secure quantum communication protocol based on three-particle GHZ states in X-basis. Commun. Theor. Phys. **63**(3), 285–290 (2015)
45. IID Quantique. http://www.idquantique.com/
46. IID Quantique. http://www.nucrypt.net/
47. Nielsen, M.A., Chuang, I.L.: Quantum computation and quantum information, Cambridge University Press (2000)
48. Venegas-Andraca, S.E.: Quantum walks and quantum image processing. DPhil Thesis, The University of Oxford (2005)
49. Andress, J.: The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, 2nd edn. Elsevier (2014)
50. Bouwmeester, D.: The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, 2nd edn. Elsevier (2014)
51. Mayers, D.: Unconditional security in quantum cryptography. J. ACM (JACM) **48**(3), 351–406
52. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441–444 (2000)
53. Loepp, S., Wootters, W., Zurek, W.: Protecting information: from classical error correction to quantum cryptography. Cambridge University Press (2006)
54. Wootters, W., Zurek, W.: A single quantum cannot be cloned. Nature **299**, 802–803 (1982)
55. Dieks, D.: Communication by EPR devices. Phys. Lett. A **92**(6), 271–272 (1982)
56. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)