Quantum Cryptology

Hoi-Kwong Lo
Networked Systems Department
HP Laboratories Bristol
HPL-97-151
December, 1997

cryptography;
cryptanalysis; quantum
cryptography; quantum
cryptology

The contest between code-makers and code-breakers has been going on for thousands of years. Recently, quantum mechanics has made a remarkable entry in the field. On the one hand, it is generally accepted that quantum cryptography can provide absolute security for communications between two users. On the other hand, code-breakers in possession of a quantum computer can easily break popular encryption schemes such as RSA and Data encryption Standard (DES) which are essentially intractable by any classical computer.

Quantum Cryptology*†

Hoi-Kwong Lo
Hewlett-Packard Labs,
Filton Road, Stoke Gifford,
Bristol BS12 6QZ,
United Kingdom
email: hkl@hplb.hpl.hp.com
(November 17, 1997)

Abstract

The contest between code-makers and code-breakers has been going on for thousands of years. Recently, quantum mechanics has made a remarkable entry in the field. On the one hand, it is generally accepted that quantum cryptography can provide absolute security for communications between two users. On the other hand, code-breakers in possession of a quantum computer can easily break popular encryption schemes such as RSA and Data Encryption Standard (DES) which are essentially intractable by any classical computer.

I. INTRODUCTION

Coded messages have a long history in military applications. [1] With the proliferation of the Internet and electronic mail, the importance of achieving secrecy in communications by cryptography [2]—the art of using coded messages—is growing each day. Amazingly, quantum mechanics has now provided the foundation stone to a new approach to cryptography—quantum cryptography. [3] It has been claimed that quantum cryptography can solve many problems that are impossible from the perspective of conventional cryptography. Here I survey the physical principles behind quantum cryptography together with its triumphs and defeats. This is followed by a discussion of the power of a quantum computer in code-breaking. Finally, I give some thoughts for the future.

* *Cryptology* is the art of secure communications. It consists of *cryptography*, the art of code-making and *cryptanalysis*, the art of code-breaking.

†To appear as Chapter 4 of *Introduction to Quantum Computation and Information*, eds. H.-K. Lo, S. Popescu and T. Spiller, World Scientific Press (1998), http://www.wspc.com.sg/.

II. NOVEL PROPERTIES OF QUANTUM INFORMATION

In my opinion, the essence of quantum cryptography can be understood by considering a single question: Given a *single* photon [1] in one of the four possible polarizations: horizontal, vertical, 45 degrees and 135 degrees, can you distinguish between these four possibilities with *certainty*? Surprisingly, the answer is *no*. This is due to the novel properties [4] of quantum information. First, there is a physical law in quantum mechanics known as the quantum 'no-cloning' theorem [5] which states that an unknown quantum state cannot be cloned. Second, given a quantum system prepared in one of two prescribed non-orthogonal states, any attempt to distinguish between the two possibilities necessarily leads to disturbance. Third, a measurement on an arbitrary unknown quantum state is an *irreversible* process which introduces disturbance to the state. As a result of these three properties, passive monitoring of quantum signals is impossible. Therefore, eavesdroping on quantum channels necessarily disturbs the signal and is exceedingly likely to be detected. In what follows, I will discuss these three properties [4] in more detail.

A. Quantum No-Cloning Theorem

Owing to the linearity of quantum mechanics, there is a quantum no-cloning theorem [5] which states that an unknown quantum state cannot be copied.[2] A proof by contradiction goes as follows: Suppose the contrary. Then a quantum Xerox machine exists and can copy an unknown state. Considering the unitary evolution of the composite system with two orthogonal states $|0\rangle$ and $|1\rangle$ respectively as the input, one finds that

$$|0\rangle \otimes |u\rangle \rightarrow |0\rangle \otimes |0\rangle \otimes |v_0\rangle \tag{1}$$

and

$$|1\rangle \otimes |u\rangle \rightarrow |1\rangle \otimes |1\rangle \otimes |v_1\rangle \tag{2}$$

where $|u\rangle$ is the initial state [3] of the Xerox machine, $|v_0\rangle$ and $|v_1\rangle$ are the final states of the system excluding the original and the duplicate. $|v_0\rangle$ and $|v_1\rangle$ may be non-orthogonal. Now suppose that the input is, in fact, a linear superposition $a|0\rangle + b|1\rangle$ $(a, b \neq 0)$ of the two orthogonal states. Then by the *linearity* of quantum mechanics, one obtains from Eqs. (1) and (2) that

[1] Just like matter is made up of indivisible atoms, light is made up of photons, which are indivisible without a change of frequency. A photon is the smallest unit or quantum of light which can be thought of as a tiny, oscillating electromagnetic field. The direction of the electric oscillation is known as its polarization, which can be probed by using a polarizer or a calcite crystal.

[2] Andy Steane says: "Even though one can clone a sheep, one cannot clone a single photon."

[3] $|u\rangle$ is independent of the input state ($|0\rangle$ or $|1\rangle$) because the Xerox machine is assumed to have no prior knowledge of the state.

$$(a|0\rangle + b|1\rangle) \otimes |u\rangle \rightarrow a|0\rangle \otimes |0\rangle \otimes |v_0\rangle + b|1\rangle \otimes |1\rangle \otimes |v_1\rangle. \tag{3}$$

Notice that the state of the original is now entangled with the duplicate. However, for quantum cloning the resulting state should be a direct product

$$(a|0\rangle + b|1\rangle) \otimes (a|0\rangle + b|1\rangle) \otimes |v'\rangle \tag{4}$$

instead. Since

$$\begin{aligned} &a|0\rangle \otimes |0\rangle \otimes |v_0\rangle + b|1\rangle \otimes |1\rangle \otimes |v_1\rangle \\ &\neq (a|0\rangle + b|1\rangle) \otimes (a|0\rangle + b|1\rangle) \otimes |v'\rangle \end{aligned} \tag{5}$$

whenever $a, b \neq 0$,[4] one concludes that an unknown quantum state cannot be cloned.[5]

B. Information Gain $\Longrightarrow$ Disturbance

Another unusual property of quantum mechanics is that, in any attempt to distinguish between two non-orthogonal states, information gain is possible only at the expense of introducing disturbance to the signal. A proof goes as follows: Suppose one is given a particle in one of two possible non-orthogonal states $|\phi\rangle$ and $|\psi\rangle$. The most general evolution involves the attachment of an ancillary quantum system say in a prescribed state $|u\rangle$ and a unitary transformation of the composite system. Assuming that the evolution leaves the state of the particle unchanged, one finds that

$$|\phi\rangle \otimes |u\rangle \rightarrow |\phi\rangle \otimes |v\rangle \tag{6}$$

and

$$|\psi\rangle \otimes |u\rangle \rightarrow |\psi\rangle \otimes |v'\rangle \tag{7}$$

where $|v\rangle$ and $|v'\rangle$ denote the final states of the ancilla in the two situations. Since the inner product is preserved by unitary transformations, one takes the inner product between the above two equations and finds that

[4] This can be verified by considering a simple example, say $a = b = 1/\sqrt{2}$.

[5] The above discussion shows that cloning violates the linearity of quantum mechanics. Since unitary transformations are linear, cloning also violates unitarity. Furthermore, cloning violates causality. Historically, it was suggested by Herbert [6] that cloning can be used to transmit signals faster than the speed of light. Suppose Alice and Bob share an EPR pair of photons. If Alice would like to send a '0', she measures the polarization of her photon along the rectilinear basis. If she would like to send a '1', she measures it along the diagonal basis. Now her measurement will project Bob's photon into one of the four possible polarizations—vertical, horizontal, 45-degree and 135-degree. If cloning were possible, immediately after Alice's measurement Bob could generate a sequence of photons *all* in one of the four possible polarizations. Bob could determine the polarization of his photons and thus the basis measured by Alice immediately, thus implying transmission of signals faster than the speed of light.

$$\begin{aligned}
(\langle u| \otimes \langle \phi|)\,(|\psi\rangle \otimes |u\rangle) &= (\langle v| \otimes \langle \phi|)\,(|\psi\rangle \otimes |v'\rangle) \\
\langle u|u\rangle \cdot \langle \phi|\psi\rangle &= \langle v|v'\rangle \cdot \langle \phi|\psi\rangle \\
1 &= \langle v|v'\rangle
\end{aligned} \tag{8}$$

where the last line follows from the fact that $\langle \phi|\psi\rangle \neq 0$ for non-orthogonal states. Therefore, one concludes that $|v\rangle$ is the same as $|v'\rangle$. In other words, any process that causes no disturbance to any two non-orthogonal states must give no information in distinguishing between the two. Thus, information gain in distinguishing between two non-orthogonal states is possible only at the expense of disturbing the state of the system.

These two properties—the quantum no-cloning theorem and the tradeoff between information gain and disturbance—imply that, given a photon in one of the four polarizations (horizontal, vertical, 45-degree and 135-degree), there is no way to distinguish between the four possibilities with certainty.

C. Irreversibility of Measurements

One might ask: What if one makes a measurement and copies the result of the measurement? Doesn't it allow one to make copies? The answer is *no* because measurements generally disturb the state of an object under observation. Consequently, the result of a measurement is generally different from the initial state and the copying will be unfaithful. To understand this point, it suffices to consider the above example of a photon in one of the four possible polarizations.[6] A birefringent calcite crystal can be used to distinguish with certainty between horizontally and vertically polarized photons. As shown in Fig. 1a, horizontally polarized photons pass straight through whereas in Fig. 1b vertically polarized photons are deflected to a new path. Photons originally in these two polarizations are, therefore, deterministically routed. However, the law of quantum mechanics says that if a photon polarized at some other direction enters the crystal (Fig. 1c), it will have some *probability* of going into either beam. It will then be repolarized according to which beam it goes into and permanently forget its original polarization. For instance, a diagonally (i.e., 45- or 135-degree) polarized photon is equally likely to go into either beam, revealing nothing about its original polarization.

If a photon is known to be rectilinearly (horizontally or vertically) polarized, by a simple modification—adding two detectors, such as photomultiplier tubes, that can record single photons along the two paths—an observer Bob can reliably distinguish between the two possibilites. This set up will, however, randomize the polarizations of diagonal (45- or 135-degree) photons, thus failing to distinguish between the two possibilities. In order to distinguish between diagonal photons, one should rotate the whole apparatus (calcite crystal and detectors) by 45 degrees. The rotated apparatus is, however, powerless in distinguishing between vertical and horizontal photons.

In conclusion, when a photon in one of the four polarizations (horizontal, vertical, 45-degree and 135-degree) is received, a naive process of measure-and-copy will disturb

[6] The discussion here is based on an excellent exposition in Ref. [3].

FIGURES

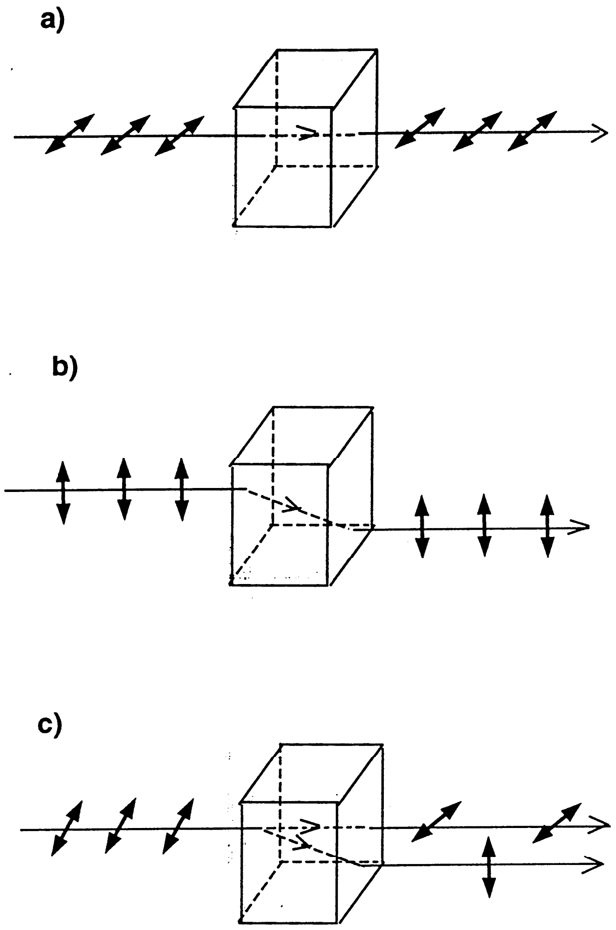

FIG. 1. A calcite crystal is used to distinguish between horizontal and vertical photons. (a) Horizontally polarized photons pass straight through. (b) Vertical polarized photons are deflected to a new path. (c) Diagonally polarized photons will have equal probability of coming out vertically or horizontally polarized.

the signal and fail to distinguish between the four possibilities: A measurement that distinguishes rectilinear photons will disturb diagonal photons. Similarly, a measurement that distinguishes diagonal photons will disturb rectilinear photons. As the last two subsections demonstrate, this fundamental limitation in distingushing between non-orthogonal states is due to the basic principles of quantum mechanics and thus it applies not only to the particular measuring apparatus described here, but also to *any* measuring apparatus.

I remark that these three novel properties of quantum information—1) no cloning, 2) information gain implies disturbance and 3) measurements are irreversible—are closely related. Indeed, the first and third properties can be regarded as corollaries of the second. It would, thus, be interesting to work out a quantitative theory of the second property. [7]

III. AN ILLUSTRATIVE EXAMPLE: QUANTUM MONEY

It was first appreciated by Stephen Wiesner [8] that quantum mechanics may be useful for cryptography. In a seminal manuscript written in about 1970 which remained unpublished until 1983, Wiesner showed that quantum mechanics can, in principle, be used to make bank notes [7] that are physically impossible to counterfeit. The idea is that, in addition to a unique serial number in a bank note, one stores on it a sequence of isolated two-state physical systems. For instance, one can imagine trapping photons with perfectly reflecting mirrors. Each of the trapped photons should be randomly and independently chosen to be in one of the four polarizations (vertical, horizontal, 45-degree and 135-degree). In the bank, a record of the serial numbers together with the actual polarizations is kept. See Fig. 2. Now the key point is that the polarization basis (rectilinear or diagonal) used for each photon is kept secret. When a customer deposits a bank note, the bank with its knowledge of the polarization basis can verify the polarizations of the sequence of photons without introducing any disturbance. On the contrary, a counterfeiter who is ignorant of the polarization basis has absolutely no way of counterfeiting a bank note faithfully.

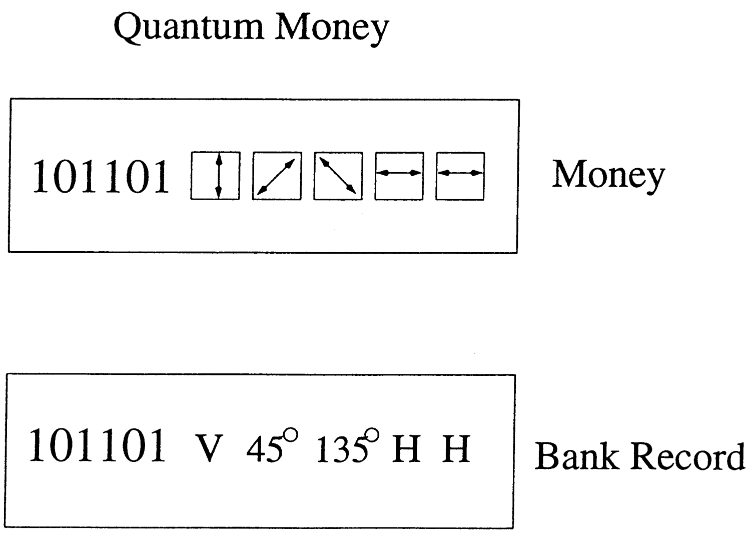

FIG. 2. In addition to a serial number, a sequence of single photons are kept in a bank note. The polarizations of those photons are a secret which is kept in the bank record.

For illustration, let me consider a simple measure-and-copy strategy. Suppose that, for each photon, a counterfeiter simply chooses one of the two (rectilinear or diagonal) bases to perform a measurement and makes copies according to his measurement result. There is a probability 1/2 that a wrong basis is chosen in which case the polarization of the photon will be randomized. Each of those randomized photons has only a probability

[7] Actually, it is more appropriate to call it a quantum check because a verification step with the bank is needed for each transaction.

1/2 of passing the bank's subsequent verification step. For each photon a measure-and-copy strategy, therefore, gives a total probability $1/2 + 1/2(1/2) = 3/4$ of success for the counterfeiter. If the total number of photons in each bank note is N, a duplicate has only a probability $(3/4)^N$ of passing the bank's verification step. When N is large, this probability becomes exponentially small. For this reason, a measure-and-copy strategy fails miserably for counterfeiting quantum money. The security of quantum money against more sophisticated counterfeiting strategies is guaranteed by the quantum no-cloning theorem.

Wiesner's work was so far ahead of his time that it was largely ignored in the 1970s. However, in the 1980s and 90s, various quantum cryptographic protocols including quantum key distribution were proposed. Before I come to them, I shall first introduce the subject of cryptography.

IV. CRYPTOGRAPHY

Suppose a sender, Alice, would like to send a receiver, Bob, a message. A basic problem in *cryptography* [2] is to make sure that an evil eavesdropper, Eve, cannot read it. (See Fig. 3.) This can be done by encryption. The idea is to scramble the message so that it becomes unintelligible to anyone except the intended recipient. In modern cryptography, the encryption algorithm itself is public information and the security lies on the users' knowledge of a *secret* string of information, known as the 'key'. Everyone can make copies of the encrypted message, but only the intended recipient who possesses the correct key can unlock form it the original message. See Fig. 4a.

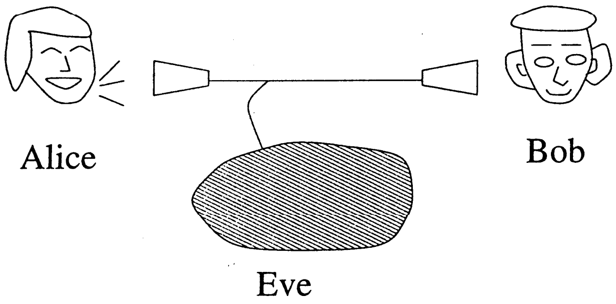

FIG. 3. Alice sends a message to Bob through a channel while the eavesdropper Eve is listening to their conversation.

If Alice and Bob share a key of the same length as the message, a *perfectly* secure scheme of communications is the one-time pad shown in Fig. 4b. It was invented by Vernam in 1918: For ease of discussion, the message is converted to binary. Suppose both the sender and the receiver possess a copy of a random sequence of 0's and 1's. The sender Alice can encode a message by combining the message and the key using the exclusive OR operation bitwise. See Fig. 4b. In other words, each message bit is flipped if and only if the corresponding key bit is 1. The encrypted form of the message is then transmitted to Bob. Bob decodes by combining the encrypted message and the key with a similar application of the exclusive OR operation bitwise.

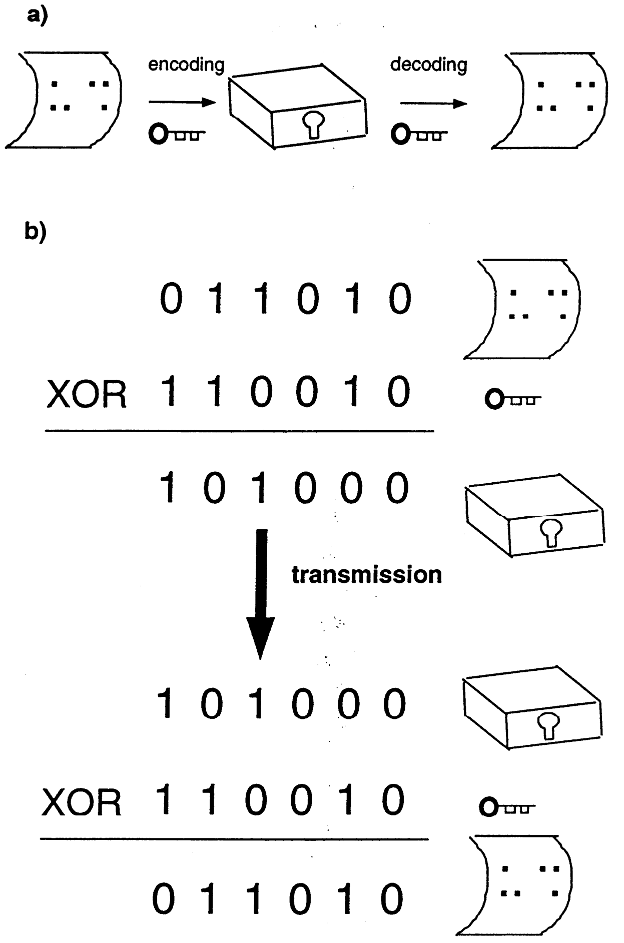

FIG. 4. (a) A message is encrypted by Alice using a key into a 'ciphertext', which is unintelligable to the eavesdropper. Bob, sharing the same key with Alice, can, however, decrypt the ciphertext to recover the original message. (b) One-time pad.

The one-time pad is secure because the encrypted message, being formed by the exclusive OR of the message with the random secret key, is itself totally random. Anyone intercepting the message and not having the encryption key knows that the message exists and how long it is, but will not be able to know anything about its meaning. It is crucial to the security of the one-time pad that the length of the key is the same as the message. In other words, the key in a one-time pad should never been re-used.[8] Otherwise, an eavesdropper Eve can reduce her ignorance of the message to that of the key.

So, what is the catch with the one-time pad? The catch is the following: The above

[8] Encryption schemes with key lengths shorter than those of the messages also exist and are widely used. They do not give perfect security.

discussion presupposes the possession of a common secret key by Alice and Bob. In practice, Alice and Bob need a second channel to transmit the key. A key problem in conventional cryptography is the key distribution problem. In classical physics, an evil eavesdropper can always passively monitor the key distribution channel and make copies of the transmitted key. Consequently, she can decode the message successfully. Worse still, there is, in principle, no way for the users to detect such a passive eavesdropping attack.

In conventional cryptography, the key distribution problem can be solved through either 1) trusted couriers or 2) 'public key' schemes.[9] At the conceptual level, both methods are unsatisfactory: In the first case, the danger in the deflection or capture of couriers by the adversaries cannot be under-estimated. In the second case, the security of public key schemes is based on computational assumptions, i.e., on the difficulty of solving certain hard problems such as the factoring of large integers. [See Appendix A for a discussion on RSA, which is the most popular public key crypto-system. The security of RSA is based on the difficulty of factoring large integers.] These computational assumptions may be defeated by exhaustive computer analysis or by the discovery of better algorithms for solving the problems on which they are based. For instance, Shor [10] has constructed efficient *quantum* algorithms for both factoring [10] and the 'discrete logarithm problem'. Therefore, if a quantum computer is ever built, many public key cryptosystems in use today will become unsafe. Worse still, this will lead to a *retrospective* total security break with catastrophic consequences.

Ironically, quantum mechanics also comes to the rescue. As remarked earlier, an attack that is notoriously difficult to defeat in conventional cryptography is passive eavesdropping. The strength of this attack lies in the ability of the eavesdropper Eve to make identical copies of the transmitted messages in order to perform extensive subsequent computer analysis *off-line*. In conventional cryptography there is, in principle, nothing to prevent this attack. In contrast, the quantum 'no-cloning' theorem forbids passive eavesdropping. As discussed in the Section 2, information gain generally leads to disturbance. Consequently, eavesdropping on a quantum channel will almost surely be detected due to the disturbance introduced to

[9] So far, I have assumed that the encryption key is the same as the decryption key. As shown in Fig. 4a, one can think of such a 'symmetric' algorithm as a safe and the key as the combination. "Someone who knows the combination can open the safe, put a document inside and close it again. Someone else with the combination can open the safe and take the document out. Anyone without the combination is forced to learn safecracking." [2] As the sender and the receiver must agree on a secret key in using a symmetric key algorithm, the key distribution problem is inevitable. However, there exist schemes in which the sender and the receiver do *not* need to agree on a secret key before they send messages. Indeed, in 1976 W. Diffie and M. Hellman [9] invented public key cryptography. In a public key crypto-system, two different keys are used. The encryption key is made public whereas the decryption key is kept private. It is supposed to be computationally hard to deduce the decryption key from the encryption key. Therefore, one can think of a public key crypto-system as a mailbox. Everyone can easily put mail in it, but getting the mail out is much harder unless one has the (secret) private key. Public key crypto-systems avoid the key distribution problem, but their security is based on some unproven computational assumptions.

[10] See Chapter Six for details on Shor's efficient quantum algorithm for factoring.

the signals. This is the basic idea behind quantum key distribution, a subject that I will come to in the next section.

V. QUANTUM KEY DISTRIBUTION

Quantum key distribution cannot prevent eavesdropping. However, it can detect eavesdropping. If eavesdropping is found (from the abnormally high error rate), the transmitted random string of numbers is discarded. On the other hand, if the error rate is sufficiently small, the two users have the peace of mind that the transmitted random string of numbers is most likely to be secure and can be used as a secure key for subsequent communications. Notice that, even in the case when the error rate is large, no useful information is leaked to the eavesdropper. This is because, in this case, the string is simply discarded. Alice and Bob postpone sending any valuable information until the security of the key is ascertained.

Notice that there is nothing, in principle, to prevent an adversary from jamming a quantum channel. In this case, the two users will be forced to abandon using the key distribution channel for the time being. However, the big advantage of quantum key distribution is to avoid a false sense of security. When substantial eavesdropping has occurred, the two users of a quantum key distribution scheme will be exceedingly unlikely to be fooled into believing the security of the key.

A. Bennett and Brassard's Scheme (BB84)

Various schemes for quantum key distribution have been proposed. For simplicity, I will consider mainly the first and the most well-known quantum key distribution scheme BB84, proposed by Bennett and Brassard [11] in 1984. The idea of BB84 scheme is *not* for Alice to prepare a particular key and send it to Bob. Heuristically, Alice and Bob each independently generate a random string of numbers. Afterwards, they go through some public discussion to decide on the key.

Two channels between Alice and Bob are needed for BB84: First of all, a *classical* communications channel is needed. It is assumed to be public but unjammable.[11] In other

[11] An unjammable channel is, in principle, impossible to achieve. If one allows the eavesdropper to attack the classical channel, some form of authentication process must be implicitly used in order to verify that the two users are talking to each other rather than an eavesdropper in disguise. Notice that authentication is needed even in conventional key distribution schemes. It can be done only if the two users initially share some small amount of secret information. If Alice and Bob have seen each other before, the information can be their outward appearances. In the case that they have not met before, it can be a short secret password. There are information-theoretically secure authentication schemes. [13] Notice that without sharing some secret information or an unjammable channel with Bob, it is totally symmetric whether Alice is talking to Bob or to an enemy Eve and it would be impossible for her to distinguish between the two cases. Barring unjammable channels, what quantum key distribution can achieve is only to *expand* this initially shared key information. Perhaps, a more appropriate name for quantum key distribution is quantum key

words, while anyone can read all the transmitted messages, no one can alter the messages sent by Alice or Bob. In peacetime, the New York Times or the BBC Radio would be good approximations to an unjammable classical channel. This classical channel will be useful for public discussion between Alice and Bob. (See below.) Second, a quantum communications channel is needed. Experiments have been done in free air [12,14] and on optical fibers [15] and ground to satellite experiments [16] have been proposed. The quantum channel is assumed to be insecure and the eavesdropper can manipulate the quantum signals in any way she desires.

Let me introduce a *refined* procedure of the BB84 scheme. [11] Suppose Alice and Bob would like to establish a secret key. Before the execution of the protocol, Alice and Bob first decide on the maximal acceptable error rate $e_{\max}$ for the transmission.[12] Refering to Figs. 5 and 6, the steps of BB84 are as follows:

(1) Alice sends Bob a sequence of photons, each of which is chosen randomly and independently to be in one of the four polarizations (horizontal, vertical, 45 degrees and 135 degrees). (Fig. 5, Step 1.)

(2) For each photon, Bob randomly chooses either the rectilinear or diagonal bases to perform a measurement. (Fig. 5, Step 2.)

(3) Bob records his bases used and the results of the measurements. (Fig. 5, Step 3.)

(4) Subsequently, Bob announces his bases (but *not* the results) publicly through the public unjammable channel that he shares with Alice. (Fig. 5, Step 4.)

Notice that it is crucial that Bob publicly announces his basis of measurement only *after* the measurement is made. This ensures that the eavesdropper, Eve, does not know the right basis during eavesdropping. If Bob were to announce his basis before the measurement, Eve could simply eavedrop along the announced basis without being detected.

(5) Alice tells Bob which measurements are done in the correct bases. (Fig. 5, Step 5.)

(6) Alice and Bob divide up their polarization data into four classes according to the bases used by them. See Fig. 7. In cases (a) and (b), Bob has performed the wrong type of measurement (i.e., Alice and Bob have used different bases). They should throw away those polarization data. On the other hand, in cases (c) and (d), Bob has performed the correct type of measurement (i.e., Alice and Bob have used the same bases).

Notice that if no eavesdropping has occurred, all the photons that are measured by Bob in the correct bases should give the same polarizations as prepared by Alice. Bob can determine those polarizations by his own detector without any communications from Alice. Therefore, Alice and Bob can use those polarization data as their raw key. Of course, before they proceed any further, they should sacrifice a small number of those photons to test for eavesdropping. For instance, they can do the following:

---

expansion. [12] Conventional methods for key expansion are necessarily insecure because a passive eavesdropper can always make copies of the communications and crack the key expansion scheme *off-line* by exhaustive computing analysis. The quantum no-cloning theorem forbids such a passive eavesdropping attack in quantum key expansion schemes.

[12] In current experiments something like $e_{\max} = 1\%$ is reasonable.

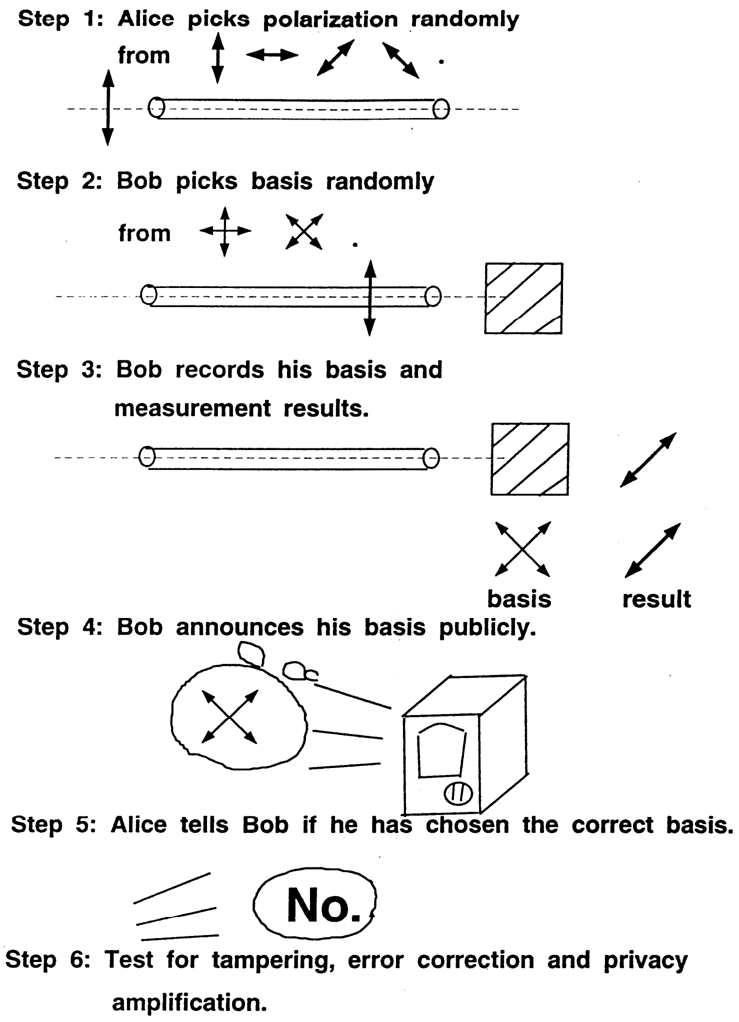
Step 1: Alice picks polarization randomly
from .
Step 2: Bob picks basis randomly
from .
Step 3: Bob records his basis and
measurement results.
basis
result
Step 4: Bob announces his basis publicly.
Step 5: Alice tells Bob if he has chosen the correct basis.
No.
Step 6: Test for tampering, error correction and privacy
amplification.

FIG. 5. Procedure of the BB84 scheme for quantum key distribution.

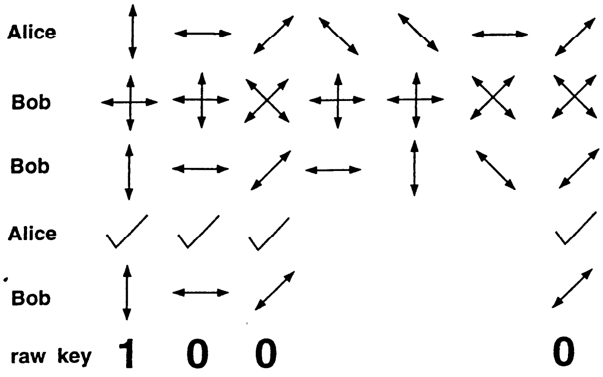

FIG. 6. A sequence of photons are sent by the BB84 scheme. For each photon, Alice chooses its polarizations randomly from horizontal, vertical, 45-degree and 135-degree. Bob then randomly chooses the rectilinear or diagonal basis to perform a measurement. He writes down the result of his measurement. Alice and Bob public compare their basis. Whenever they have used the same basis, they can convert their polarization data into a single raw bit. Of course, they need to test for tampering and go through error correction and privacy amplification as described in the text.

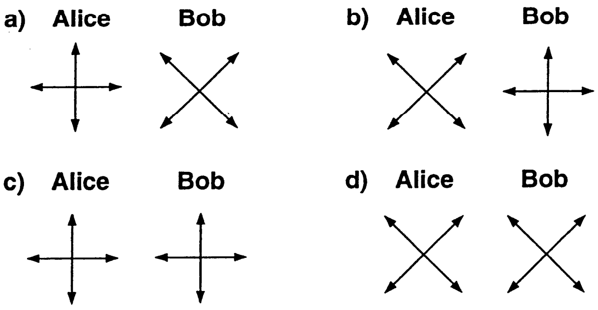

FIG. 7. Alice and Bob divide their polarization data into four cases according to the bases used by them.

(7) Alice and Bob randomly pick a fixed number say m_1 photons from case (c) and compute its experimental error rate, e_1. Similarly, they randomly pick m_2 photons from case (d) and compute its experimental error rate, e_2.[13]

If either e_1 or e_2 is larger than the maximal tolerable error rate e_{max}, either substantial eavesdropping has occurred or the channel is unexpectedly noisy. Alice and Bob should,

[13] m_1 and m_2 are chosen to be large enough for accurate estimation of the true error rates of the transmission. A simple protocol may take $m_1 = m_2$. In the original BB84, cases (c) and (d) are combined to estimate a single error rate. Here, I refine the error estimation to compute two error rates, in anticipation of my subsequent discussion of an improved scheme in Section 5.3.

therefore, discard all the data and start with a fresh batch of photons. On the other hand, if both e_1 and e_2 are smaller than $e_{\max}$, they proceed to step 8.

(8) Reconciliation and privacy amplification: Alice and Bob can independently convert the polarizations of the remaining photons into a raw key by, for example, regarding a horizontal or 45-degree photon as denoting a '0' and a vertical or 135-degree photon a '1'.

There are still two problems, namely noise and leakage of information to Eve, in the raw key that Alice and Bob share. Indeed, the raw key that Alice has may differ slightly from that of Bob. Moreover, Eve may have partial information on the raw key. A realistic scheme must include error correction and privacy amplification—the distillation of perfectly secret key out of a sequence of raw key that Eve may have partial knowledge of. Privacy amplification schemes that are secure against single-photon measurements by Eve have been devised. [12,17] However, despite immense efforts, [18]– [24] a complete widely accepted proof of the security of quantum key distribution against *coherent* attacks [14] is, in my opinion, still missing. I relegate an elementary discussion of error correction and privacy amplification to Appendix B.

B. Other Schemes

Even though BB84 solves the key distribution problem, it does not solve the key storage problem: Once Alice and Bob have established their classical key, they must store it before it is used. In principle, an eavedropper may break into their laboratories to steal it. Ekert [25] proposed an Einstein-Podolsky-Rosen-based scheme which solves the key storage problem.

The well-known Einstein-Podolsky-Rosen (EPR) [26] effect occurs when a pair of entangled (i.e., quantum mechanically correlated) photons is emitted from a source. The entanglement may arise out of conservation of angular momentum. As a result, each photon is in an undefined polarization. Yet, the two photons always give opposite polarizations when measured along the same basis. For example, if Alice and Bob both measure along the rectilinear basis, their photons are each equally likely to be horizontally or vertically polarized. But if Alice's photon is horizontal, Bob's will certainly be vertical and vice versa.

A simplified version of Ekert's scheme goes as follows: A source emits such pairs of entangled photons. Alice and Bob each keep a member of each pair. They measure some of their polarizations immediately to test for eavesdropping. The remainder is stored without being measured. When they need to use the key, they measure and compare some of the stored pairs. If no tampering has occurred, the polarizations of the two members of each pair should be opposite. They verify that, for the test pairs, this is indeed the case. They can then measure the polarizations of the reminder randomly and independently along two bases and subsequently go through privacy amplification in the same way as in BB84.

[14] In a coherent attack, Eve regards the whole sequence of photons as a single entity and couples it with an ancilla and evolves the combined system. Afterwards, she keeps her ancilla and listens to the public discussion between Alice and Bob before deciding on what information to extract from her ancilla.

Another interesting quantum key distribution scheme, B92, was proposed in 1992 by Bennett [27] who showed that any two non-orthogonal states suffice to distribute a key. Suppose a photon is chosen randomly from two non-orthogonal polarizations say $|u_0\rangle$ and $|u_1\rangle$. Let me consider the projections $P_{\text{not } 0} = 1 - |u_0\rangle\langle u_0|$ and $P_{\text{not } 1} = 1 - |u_1\rangle\langle u_1|$. Notice that $P_{\text{not } 0}|u_0\rangle = 0$. Therefore, if a measurement of $P_{\text{not } 0}$ gives an eigenvalue 1, Bob can be sure that the state before the observation must be $|u_1\rangle$. On the other hand, if a measurement $P_{\text{not } 0}$ gives an eigenvalue 0, the initial state may be either $|u_0\rangle$ or $|u_1\rangle$.

The procedure of B92 goes as follows: Alice sends a random sequence of photons to Bob, using $|u_0\rangle$ to represent a 0 and $|u_1\rangle$ to represent a 1. Bob performs a random measurement of either $P_{\text{not } 0}$ or $P_{\text{not } 1}$. Bob publicly announces the eigenvalue of his measurement for each photon, but not the type of measurement that he has performed. Alice and Bob discard all the instances when the eigenvalue is 0. Notice that, in the absence of noise, when the eigenvalue is 1, the type of measurement performed by Bob will tell him the bit chosen by Alice. The eigenvalue 1 should appear with a probability $(1 - |\langle u_0|u_1\rangle|^2)/2$. In this case, they share a common bit. Of course, just like in BB84, they need to test for tampering. They can do so by selecting and sacrificing a subset of photons for the case when the eigenvalue is 1 to check that their sub-strings agree with each other. Besides, they also need to check that the proportion of 1's is, indeed, a fraction around $(1 - |\langle u_0|u_1\rangle|^2)/2$. A malicious Eve who measures the signals in transit using an apparatus similar to Bob's and destroys them whenever the measurement outcome is 0 will decrease the proportion of 1's in Bob's result and thus be caught. (See also [28].)

Other quantum key distribution schemes have also been proposed. Townsend and collaborators have discussed a practical implementation of quantum cryptography in a communications network with many users. [29] A quantum cryptographic network based on quantum memories was proposed. [30] Goldenberg and Vaidman [31] showed that, rather surprisingly, orthogonal states can be used for quantum key distribution. A proposal to use quantum cryptography without public announcement of bases has also been made. [32]

C. Efficient Quantum Key Distribution

Another interesting question is the efficiency of quantum key distribution. Since Alice and Bob choose the two bases randomly and independently in BB84, on average Bob performs a wrong type of measurement half of the time. Therefore, half of the photons are thrown away immediately. However, Lo and Chau [33] proposed a modification of BB84 which essentially doubles its efficiency. The basic idea is that Alice and Bob pick a number $0 < \epsilon \leq 1/2$. The value of ϵ can be made public.[15] Now for each photon Alice chooses the two bases, rectilinear or diagonal, with probability ϵ and $1 - \epsilon$. Similarly, Bob measures the polarization of his received photon along the two bases, rectilinear or diagonal, with probability ϵ and $1 - \epsilon$. Clearly, their bases agree with a probability $\epsilon^2 + (1 - \epsilon)^2$ which goes

[15] Notice that ϵ is supposed to be small but *non-zero*. As I will argue later, the limit $\epsilon \to 0$ is *singular*. The constraint on the value ϵ will be discussed near the end of this Section.

to 1 as ϵ goes to zero.[16] Hence, the efficiency is asymptotically doubled when compared to BB84.

What about security? Naively, one might think that the eavesdropper can use the knowledge of ϵ to devise an attack that defeats the scheme. This naive expectation is, however, incorrect. As far as single-photon measurements by Eve are concerned, the improved scheme is as secure as BB84. The important modification is a refined error estimation. In the original BB84 scheme, it was proposed that cases (c) and (d) in Fig. 7 are combined to estimate a *single* error rate. In the improved scheme, a separate estimation of the *two* error rates is made. To see how this modification guarantees security, it is instructive to consider a simple intercept-resend eavesdropping strategy by Eve. Suppose, for each photon, Eve measures its polarization along the rectilinear axis with probability p_1, along the diagonal axis with probability p_2 and does nothing to the photon with probability $1 - p_1 - p_2$. Whenever Eve performs a measurement, the original polarization of the photon is irreversibly lost. In an attempt to avoid the users detecting her tampering, Eve then resends a photon with its polarization given by the result of her measurement. Now, for such a strategy, consider the error rate in case (c) where both Alice and Bob use the rectilinear basis. The errors occur when Eve uses the diagonal basis. See Fig. 8. This happens with a *conditional* probability p_2. In this case, the polarization of the photon is randomized, thus giving an error rate $e_1 = p_2/2$ for case (c). Similarly, errors in case (d) occur when Eve is measuring along the rectilinear basis. See Fig. 8. This happens with a conditional probability p_1 and when it happens, the photon polarization is randomized. Therefore, the error rate for case (d) is $e_2 = p_1/2$.

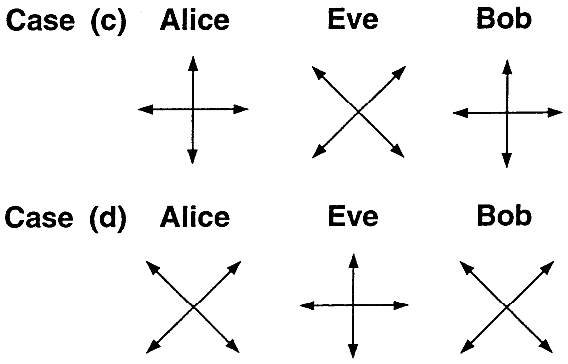

FIG. 8. In case (c) of Fig. 7 where both Alice and Bob use the rectilinear basis, errors occur when Eve uses the diagonal basis. Similarly, in case (d) of Fig. 7 where both users employ the diagonal basis, errors occur when Eve uses the rectilinear basis.

The key point to note is that these two error rates e_1 and e_2 only depend on Eve's eavesdropping strategy, but *not* on the value of ϵ! This is so because they are *conditional* probabilities. This fact is valid not only for the above simple example, but also for *any*

[16] See the preceding footnote.

single-photon eavesdropping strategy by Eve: Indeed, any single-photon-measurement eavesdropping strategy gives characteristic error rates e_1 and e_2 *independent* of the value of ϵ. Consequently, Eve cannot exploit her knowledge of ϵ to avoid detection of her tampering.

I remark that it is absolutely crucial to compute the two error rates separately. Otherwise, the scheme is insecure. Had a single error rate be computed as in the original BB84, Alice and Bob would have found that the average error rate

$$\bar{e} = \frac{\epsilon^2 e_1 + (1-\epsilon)^2 e_2}{\epsilon^2 + (1-\epsilon)^2}. \tag{9}$$

For the intercept-resend strategy,

$$\bar{e} = \frac{\epsilon^2 p_2 + (1-\epsilon)^2 p_1}{2[\epsilon^2 + (1-\epsilon)^2]}. \tag{10}$$

Suppose Eve always eavesdrops solely along the diagonal basis (i.e., $p_1 = 0$ and $p_2 = 1$), then

$$\bar{e} = \frac{\epsilon^2}{2[\epsilon^2 + (1-\epsilon)^2]} \rightarrow 0 \tag{11}$$

as ϵ tends to 0. Hence, with the original error estimation method in BB84, Alice and Bob will fail to detect eavesdropping by Eve. Yet, Eve will have much information about Alice and Bob's raw key as she is always eavesdropping along the dominant (diagonal) basis.

Apparently, the possibility of having more efficient quantum key distribution schemes was first raised by Ardehali. [34] Unfortunately, the crucial importance of a refined error analysis was not recognized and consequently the security of his scheme remained unproven. The use of a refined error analysis was first discussed by Barnett and Phoenix [35] for *rejected* data. Lo and Chau, however, noted the important fact that when a refined error analysis is applied to *accepted* data, an improved scheme can be made secure.

D. Constraint on ϵ.

Of course, if ϵ is actually zero, the improved scheme is insecure because Eve can simply eavesdrop along the diagonal axis. However, I emphasize that the limit $\epsilon \rightarrow 0$ is *singular* and that for non-zero ϵ, secure schemes do exist. A natural question to ask is: What is the constraint on ϵ? The key constraint is that one needs to make sure that there are enough photons for an accurate estimation of the two error rates e_1 and e_2. Suppose N photons are transmitted from Alice to Bob. On average, only $N\epsilon^2$ photons belong to case (c) where both Alice and Bob use the rectilinear basis. To estimate e_1 reasonably accurately, one needs to make sure that this number is larger than some number m_0. The key point to note is that the number m_0 may depend on e_1 but *not* on N. In summary, one needs:

$$\begin{aligned} N\epsilon^2 &\geq m_0 \\ \epsilon &\geq \sqrt{m_0/N}. \end{aligned} \tag{12}$$

As N tends to infinity, ϵ can be made to go to zero but never quite reach it.. (See footnote p.) Notice that the asymptotic limit $\epsilon \rightarrow 0$ corresponds to 100 percent efficiency. In conclusion, the improved scheme is asymptotically the most efficient scheme that one can possibly devise.

I remark that this type of efficient schemes of quantum key distribution applies also to Ekert's scheme and Biham, Huttner and Mor's scheme based on quantum memories. [33]

VI. PRACTICAL CONSIDERATIONS

Quantum key distribution is not just a theoretical subject. The first experimental demonstration of the feasibility of quantum key distribution was done with open air over 32 cm. [12] By now, experiments over 20 km of optical fibers [15] as well as 205m of free air [14] have been performed. Besides, there have been proposals for performing quantum key distribution experiment from the ground to a satellite. [16] Such capability is of immense value for re-programming satellites currently in orbit around the earth as well as for long distance relay of cryptographic keys via satellites. These exciting experiments will be the subject matter of the next chapter. Here I will give some simple practical considerations for the experiments.

A. Photon Source

As it turns out, it is difficult to prepare single photon sources. Most of the current experiments are, therefore, done with faint light pulses, rather than single photons. On average, there can be only 1/10 photon per pulse. Even so, there are still some chances of having two or more photons. This gives rise to a new eavesdropping strategy. Eve may use a beamsplitter to try to divide up the beam into two pieces, measuring the state of one beam and sending the second to Bob. Notice that such an attack is possible only when the beam contains more than one photon and is, therefore, divisible. By using very weak light pulses, the probability of success of the beamsplitting attack can be kept small. Hence, Alice and Bob can put some bounds to the information leakage to Eve due to such an attack and use privacy amplification to distill a perfectly secure key as discussed in Section 5.1.

A better source to use is EPR pairs from so-called parametric down conversion experiments. When a photon passes through a non-linear crystal, it can be converted into two entangled photons of *lower* frequencies.[17] One of the two photons can, then, be used as a trigger to signal the creation of *at least* one EPR pair. Since the input to the non-linear crystal is often a faint laser pulse rather than a single photon, parametric down conversion still gives two or more EPR pairs with non-zero probabilities. However, the case of having no photon pairs can be eliminated from consideration due to non-triggering of the sender's device. This helps to cut down an important source of error in the experiment—the photon dark count rates, which will be introduced in Subsection 6.4.

Finally, I remark that other methods [36,37] such as carefully tailored atomic emission in cavity quantum electrodynamics [36] may give still a better photon source in future.

[17] This does not violate the fact that a photon cannot be divided *without* a change in frequency.

B. Coding Schemes

There are two main types of coding schemes in experimental quantum cryptography—polarization coding and phase coding. The idea of phase coding is to send a photon into two different arms of an interferometer. The two paths then represent two orthogonal states in the coding scheme. By passing a photon through a 50-50 beam-splitter (i.e., a half-reflecting mirror), one can launch it into a coherent superposition of the two paths:

$$|u\rangle = \frac{1}{\sqrt{2}}|Path\ 1\rangle + \frac{i}{\sqrt{2}}|Path\ 2\rangle. \tag{13}$$

One can encode information by introducing a phase difference

$$|u\rangle = \frac{e^{i\phi}}{\sqrt{2}}|Path\ 1\rangle + \frac{i}{\sqrt{2}}|Path\ 2\rangle. \tag{14}$$

By picking ϕ randomly between 0 and $\pi/2$, the scheme is equivalent to the B92 scheme introduced in the last Section. Bob can read off information using a similar interferometer. See the next chapter for details.

C. Frequency

Commercial single-photon counting modules employing silicon avalanche photo-diodes (APDs) are available around wavelengths of 800 nm. Such devices have high efficiencies (about 50%) and low noise rates. Unfortunately, the losses in optical fibers are quite high (2 dB/km) at this frequency range. Therefore, for long-distance optical fiber experiments, it is preferable to use commercial Telecom wavelengths, either 1300 nm or 1550 nm where the losses are 0.35 dB/km and 0.2 dB/km respectively. At such frequencies, no efficient commercial single-photon counting modules are available and cooled Ge or InGaAs avalanche photo-dioded have to be built in the laboratories.

D. Noise

Even when the same basis is used by both Alice and Bob, the transmitted data of Alice and Bob may still be different because of various sources of errors. One of them is the *dark counts* in the detector: A detector may click accidentally even when there are no photons. To eliminate this source of error, the clicking of the detector is ignored unless it falls into specific time windows when a photon pulse is expected to arrive. Incidentally, an advantage of a parametric down conversion EPR source over a weak light pulse is that a member of the EPR pair will provide the 'trigger' to the sender Alice's detector. Only then will Bob consider his data. Therefore, the receiver Bob will discard the dark counts in cases when there are no triggering. Other sources of errors will be discussed in more detail in the next chapter.

VII. BEYOND QUANTUM KEY DISTRIBUTION?

Beside quantum key distribution, other applications of quantum cryptography have also been proposed. The underlying theme of those applications is the protection of private information during public discussion. "In this scenario, there are no enemies, but you must negotiate with everyone and you don't entirely trust them," Charles Bennett says. Indeed, there have been reports [38] of fake teller machines stealing PIN (Personal Identification Number) from customers. Next time when you type your PIN to an unknown teller machine, maybe you should worry about this possibility. To solve this problem, it would be useful to have some means of identification without revealing the actual password. i.e., comparing whether the customer's private password x matches the password y stored by the machine without revealing x itself. More generally, in a two-party secure computation, Alice has a *private* input x and Bob a *private* input y. Alice would like to help Bob to compute a prescribed (i.e., public) function $f(x, y)$ without revealing anything to Bob about x more than what follows logically from $f(x, y)$ and y.

Either trusted intermediaries or computational assumptions may be used to achieve two-party secure computations. In the first case, Alice and Bob send their private inputs to a trusted third party (or a machine) Charles, who performs the computation for them and tells them the result afterwards. Of course, the problem here is that Charles may cheat by telling one party the other party's input. In the second case, assumptions such as the hardness of factoring large integers can be used. However, an adversary may crack such system by exhaustive computer analysis or by more efficient algorithms. In particular, an adversary with a quantum computer can use Shor's algorithm [10] to factor large integers efficiently. See footnote k.

The impossibility of *unconditionally* secure schemes for two-party secure computations in *conventional* cryptography has sparked much interest in quantum protocols. Until recently, there had been a widespread belief that quantum two-party secure computations can be made unconditionally secure. [39]⁻ [43] However, this optimism was recently shattered [44] following the demonstration of the insecurity of quantum bit commitment by Mayers [45,46] and also by Lo and Chau [47,48]. This is a severe setback to quantum cryptography. In what follows, I will introduce the concept of bit commitment, describe a simple quantum bit commitment scheme and explain why unconditionally secure quantum bit commitment is impossible.

A. Bit Commitment

Bit commitment is a crucial primitive for implementing secure computations.[18] A bit commitment scheme involves two parties, a sender, Alice and a receiver, Bob. It is executed in two steps—1) the commit phase and 2) the opening phase. In the commit phase, Alice chooses a bit ($b = 0$ or 1) and commits it to Bob. That is, she gives a piece of evidence to Bob that she has chosen a bit and that she cannot change it. At that moment, the scheme should prevent Bob from learning the value of the bit from that evidence. At a later time, however, Alice and Bob must be able to execute the opening phase in which Alice *opens* the commitment. That is, she tells Bob which bit she has chosen and proves to him that this is indeed the genuine bit that she chose during the commit phase.

As an example of bit commitment, Alice writes down her bit in a piece of paper, places it in a box and locks it. She then hands over the box to Bob. Now she can no longer change her mind about the value of the bit. Meanwhile, Bob, without the key to the lock, cannot learn the value of the committed bit himself. At a later time, Alice gives the key to Bob who opens the box to recover the value of the committed bit. Unfortunately, the security of this scheme relies solely on the physical security of the box and the lock. Therefore, it is not applicable in the electronic age.

What is cheating? Both Alice and Bob may attempt to cheat. On the one hand, a dishonest Bob tries to find out the value of the bit before the opening phase. On the other hand, a dishonest Alice may choose 0 during the commit phase and yet in the opening phase claims that it was 1 that she had in mind. For a bit commitment scheme to be secure, both forms of cheating must be foiled.

B. A Simple Quantum Bit Commitment Scheme

For concreteness, I will describe a simple quantum bit commitment scheme proposed by Bennett and Brassard. [11] As before photons in four possible polarizations, horizontal (0 degrees), vertical (90 degrees), 45 degrees and 135 degrees, are used. If Alice has 0 in mind, she sends a sequence of photons chosen randomly from the rectilinear basis. i.e., each photon is independently and randomly chosen from horizontal and vertical polarizations. On the other hand, if Alice has 1 in mind, she sends a sequence of photons chosen randomly from the diagonal basis. i.e., each photon is independently and randomly chosen from 45-degree and 135-degree polarizations. Notice that independent of the value of the bit chosen by Alice, the density matrix ρ of the entire sequence of photons received by Bob is the same.

[18] Yao [49] has shown that quantum bit commitment can be used to implement quantum oblivious transfer. Besides, it has been shown by Kilian [50] that in conventional cryptography oblivious transfer can be used to achieve two-party secure computations. These two results combined together seem to suggest that quantum bit commitment leads directly to unconditionally secure two-party secure computations, thus achieving what is impossible from the perspective of conventional cryptography.

It is just the tensor product of the density matrices of the individual photons. Indeed, $\rho = \rho_{\text{single}} \otimes \rho_{\text{single}} \otimes \cdots \otimes \rho_{\text{single}}$ with

$$\begin{aligned} \rho_{\text{single}} &= \frac{1}{2} \left(|0^\circ\rangle\langle 0^\circ| + |90^\circ\rangle\langle 90^\circ| \right) \\ &= \frac{1}{2} \left(|45^\circ\rangle\langle 45^\circ| + |135^\circ\rangle\langle 135^\circ| \right) \\ &= \frac{1}{2} I, \end{aligned} \tag{15}$$

where I is the two-dimensional identity matrix. Consequently, there is absolutely no way for Bob to learn Alice's committed bit.

What an honest Bob should do is, for each photon, to choose randomly between the rectilinear or diagonal basis to measure its polarization. During the opening phase, Alice tells Bob her committed bit and the polarizations of all the photons. Bob accepts Alice's committed bit if her announced polarizations are consistent with his measurement results. Suppose, for instance, N photons are transmitted and Alice opens the commitment by telling Bob that she has committed to a 0. Since Bob has choosen the two bases at random, Bob would have performed measurements along the rectilinear basis for an average of $N/2$ photons. For those photons, Bob can then check if Alice's announced polarizations are the same as what he has got from his measurements. If the answer is yes, he believes that Alice is honest. Otherwise, Alice must be cheating.

I remark that a naive cheating strategy by Alice is likely to be caught by Bob. Suppose Alice prepares a sequence of rectilinear photons and claims that they are diagonally polarized during the opening phase. For an average of $N/2$ photons that Bob has measured along the diagonal basis, Alice's photons give random results to Bob's detector. Now Alice has to blindly guess those results. The probability that she will be successful is, therefore, approximately $(1/2)^{N/2}$.

A fatal problem in Bennett and Brassard's scheme, as noted by the inventors themselves in their paper, [11] is that it is insecure against an Einstein-Podolsky-Rosen (EPR) type of attack. Recall from Section 5.2 that an EPR correlated pair of photons always shows opposite polarizations when measured along the same basis. For instance, when measured along the rectilinear basis, if one photon is horizontal, the other will necessarily be vertical and vice versa. Suppose that each of the photons sent by Alice is, in fact, a member of an EPR pair and that Alice keeps the other member herself. Alice decides on the value of her bit only during the opening phase. If she decides it to be 0, she performs her measurement along the rectilinear basis. On the other hand, if she decides it to be 1, she performs her measurement along the diagonal basis instead. This strategy will totally fool Bob and defeat the security requirement of the scheme: During the commit phase, Bob's photons are described by a density matrix $\rho = \rho_{\text{single}} \otimes \rho_{\text{single}} \otimes \cdots \otimes \rho_{\text{single}}$ with ρ_{single} given by Eq. (15), just like in an honest protocol. Yet, for each pair of photons shared between Alice and Bob, the EPR paradox allows Alice's photon to give opposite polarization to that of Bob's whenever the two are measured along the same basis. There is no way for Bob to defeat such an attack.

While this EPR type of attack was well-known, its power and generality was not fully appeciated. Indeed, after Bennett and Brassard's scheme, many other quantum bit commitment protocols [40,42] had been proposed. Until recently, it had been widely claimed that *unconditionally* secure quantum bit commitment is possible. The fatal flaw of all those schemes was independently discovered by Mayers [45] and by Lo and Chau. [47] By now, it has been shown that unconditionally secure quantum bit commitment is impossible. [46,48] I will sketch the key point of the argument here.

C. Unconditionally Secure Quantum Bit Commitment Is Impossible

Recall the two security requirements for bit commitment: (A) Bob cannot learn the value of the bit b during the commit phase; and yet (B) Alice cannot change it during the opening phase. I now show that they are inconsistent. If Bob cannot learn the value of the committed bit, then Alice can almost always cheat successfully (i.e., she can change her bit from 0 to 1 during the opening phase without being caught by Bob) *even if* Bob has a quantum computer! Then, it is quite clear that she can cheat against a Bob without a quantum computer.[19] Consequently, quantum bit commitment is always insecure.

Here is the proof. Imagine that both Alice and Bob use quantum computers to execute a quantum bit commitment scheme. (See footnote *t*.) At the beginning, Alice chooses her committed bit $b = 0$ or 1 and inputs the state $|0\rangle$ or $|1\rangle$ accordingly. Alice and Bob are supposed to go through a multi-step procedure of sending classical and quantum signals to and fro as well as performing local unitary transformations, attaching ancillas and performing measurements in each step. With quantum computers, they preserve the coherence of the state under manipulation perfectly. One can then argue that all actions (classical [20] and quantum communications, unitary transformations, measurements and attachments of ancillas) by Alice and Bob can be regarded as a unitary transformation applied to the input state. The basic idea of this point was noted in [46]. A more concrete discussion was made in [48]. For a review, see [51].[21] Therefore, at the end of the commit phase, their composite quantum system $H_A \otimes H_B$ [where H_A (H_B respectively) is the Hilbert space of Alice's (Bob's

[19] Any bit commitment procedure followed by Bob can be re-phrased as one in which Bob does has a quantum computer but simply fails to make full use of it. Therefore, by showing that Alice can defeat a Bob who makes full use of his quantum computer, Mayers and also Lo and Chau proved that all bit commitment schemes based on quantum mechanics—classical, quantum, or quantum but with measurements—are insecure. There is no need to consider *decoherence*.

[20] Any classical communications may be regarded as a special case of quantum communications and there is no need to distinguish between the two.

[21] Let H_A and H_B denote the Hilbert spaces of Alice and Bob's quantum machine respectively and let H_C be the Hilbert space of the quantum communications channel. Consider the combined Hilbert space $H = H_A \otimes H_B \otimes H_C$. In the beginning, Alice chooses the bit b to be zero or one and prepares the state $|0\rangle$ or $|1\rangle$ accordingly. Bob always prepares $|v\rangle$. Alice and Bob now take turns to perform operations (including measurements, unitary transformation and attachment of ancillas) on the system. The key point to note is that the operation applied at each step can be regarded as a *unitary* transformation. Indeed, one can imagine that Alice and Bob have quantum computers. It is then well-known all operations can be done without any actual measurement. See [48,51] for

respectively) quantum machine] is in a *pure* state $|\psi_0\rangle$ or $|\psi_1\rangle$ depending on the value of b. Now the security requirement (A)—that Bob cannot learn the value of b—implies that Bob's quantum machine is described by essentially the same density matrix [22] independent of the value of b. i.e.,

$$\mathrm{Tr}_A|\psi_0\rangle\langle\psi_0| = \rho_0^B = \rho_1^B = \mathrm{Tr}_A|\psi_1\rangle\langle\psi_1|, \tag{16}$$

where Tr_A denotes the partial trace operation over the subsystem A controlled by Alice. Notice that I am considering the state of the *whole* quantum machine of Bob rather than its individual components. This greatly simplifies my discussion and avoids fallacies in classical reasoning.

But then, there is a mathematical result (see below) which says that $|\psi_0\rangle$ and $|\psi_1\rangle$ are related by a *local* unitary transformation by Alice *alone.* i.e., $|\psi_1\rangle = U^A|\psi_0\rangle$ for some U^A acting on H_A only. Consequently, Alice can cheat successfully by executing the protocol for $b = 0$ during the commit phase. It is only at the beginning of the opening phase that she makes up her mind. If she decides b to be zero, of course, she can execute the protocol honestly. If she decides b to be one instead, she simply applies U^A to her state $|\psi_0\rangle$ to change it to $|\psi_1\rangle$ and executes the protocol for $b = 1$ instead. Since U^A is a local unitary transformation on Alice's machine, she can clearly apply it without Bob's help and there is no way for Bob to defeat such cheating. Therefore, unconditionally secure quantum bit commitment is impossible.

D. Schmidt Decomposition

All that is left to prove is the existence of U^A used in the last paragraph. For this, I need a mathematical result—Schmidt decomposition. [52] The following discussion is largely based on [52]. Given Hilbert spaces H_A and H_B with dimensions p and q respectively, consider a normalized state $|\Phi\rangle$ in $H_A \otimes H_B$. Let $\rho = |\Phi\rangle\langle\Phi|$ be the density matrix and $\rho^A = \mathrm{Tr}_B\rho$ and $\rho^B = \mathrm{Tr}_A\rho$ be the reduced density matrices. Then the Schmidt decomposition theorem says that $|\Phi\rangle$ can be written as

$$|\Phi\rangle = \sum_{i=1}^{r} \sqrt{\lambda_i}|a_i\rangle \otimes |b_i\rangle, \tag{17}$$

where $|a_i\rangle$ ($|b_i\rangle$ respectively) are orthonormal eigenstates of ρ^A (ρ^B respectively), and $r \leq \min(p, q)$ is the total dimension of the non-zero eigenspaces of ρ^A.

details. In other words, in each step, a party $D \in \{A, B\}$ applies a unitary transformation on $H_A \otimes H_C$, which can then be regarded as a unitary transformation on H. Therefore, the whole procedure of the commit phase can be regarded as a product of unitary transformations, which is thus a unitary transformation, applied to the initial state. Hence, the final state can be considered as *pure*.

[22] The case when ρ_0^B and ρ_1^B are slightly different will be briefly discussed later. The physics there is essentially the same.

The proof goes as follows: Let me write $|\Phi\rangle$ in terms of the orthonormal eigenbasis $|a_1\rangle, |a_2\rangle, \cdots, |a_p\rangle$ of ρ^A as

$$|\Phi\rangle = \sum_{i=1}^{p} |a_i\rangle \otimes |b'_i\rangle, \tag{18}$$

where $|b'_i\rangle$'s are not necessarily orthogonal. Tracing over H_B, one finds

$$\begin{aligned} \mathrm{Tr}_B|\Phi\rangle\langle\Phi| &= \mathrm{Tr}_B \sum_{i=1}^{p}\sum_{j=1}^{p} |a_j\rangle \otimes |b'_j\rangle\langle a_i| \otimes \langle b'_i| \\ &= \sum_{i=1}^{p}\sum_{j=1}^{p} \langle b'_i|b'_j\rangle |a_j\rangle\langle a_i|. \end{aligned} \tag{19}$$

On the other hand, since $|a_i\rangle$'s are the eigenstates of ρ^A, one must have

$$\rho^A = \sum_{i=1}^{r} \lambda_i |a_i\rangle\langle a_i| \tag{20}$$

where λ_i's are the eigenvalues of ρ^A. Equating these two equations, one finds $\langle b'_i|b'_j\rangle = \lambda_i \delta_{ij}$. Hence, $|b_i\rangle = \lambda_i^{-\frac{1}{2}}|b'_i\rangle$ is an orthonormal set in H_B and

$$|\Phi\rangle = \sum_{i=1}^{r} \sqrt{\lambda_i}|a_i\rangle \otimes |b_i\rangle. \tag{21}$$

Now, by taking the trace over H_A, it is easy to see that

$$\rho^B = \sum_{i=1}^{r} \lambda_i |b_i\rangle\langle b_i|. \tag{22}$$

Therefore, $|b_i\rangle$ is an eigenvector of ρ^B corresponding to the eigenvalue λ_i. Q.E.D.

Let me apply this result to quantum bit commitment. At the end of the commit phase, if $b = 0$, the wavefunction $|\psi_0\rangle$ can be written in Schmidt decomposition as

$$|\psi_0\rangle = \sum_{i=1}^{r} \sqrt{\lambda_i}|a_i\rangle \otimes |b_i\rangle. \tag{23}$$

Similarly, if $b = 1$, the wavefunction $|\psi_1\rangle$ can be written as

$$|\psi_1\rangle = \sum_{i=1}^{r} \sqrt{\lambda'_i}|a'_i\rangle \otimes |b'_i\rangle. \tag{24}$$

The first security requirement—that Bob does not know the bit—demands that *ideally* Bob has the same density matrix for $b = 0$ and $b = 1$. That is,

$$\rho_0^B = \sum_{i=1}^{r} \lambda_i |b_i\rangle\langle b_i| = \sum_{i=1}^{r} \lambda'_i |b'_i\rangle\langle b'_i| = \rho_1^B. \tag{25}$$

Without much loss of generality,[23] this implies that $\lambda_i = \lambda'_i$ and $|b_i\rangle = |b'_i\rangle$. In other words,

$$|\psi_1\rangle = \sum_{i=1}^{r} \lambda_i |a'_i\rangle \otimes |b_i\rangle. \tag{26}$$

Observe that the only possible difference between $|\psi_0\rangle$ and $|\psi_1\rangle$ lies in the eigenvectors $|a_i\rangle$ and $|a'_i\rangle$ (of ρ_0^A and ρ_1^A respectively). Let me consider the unitary transformation U^A that maps $|a_i\rangle$ to $|a'_i\rangle$. As asserted, it acts on Alice's quantum machine H_A only and yet maps $|\psi_0\rangle$ to $|\psi_1\rangle$. This shows the existence of a cheating unitary transformation U^A and thus completes the proof of insecurity of *ideal* quantum bit commitment where Bob's density matrices ρ_0^B and ρ_1^B corresponding to $b = 0$ and $b = 1$ are exactly the same.

E. Non-ideal Quantum Bit Commitment

However, in general, one can allow ρ_0^B and ρ_1^B to be slightly different. This will only give Bob a small probability of distinguishing between 0 and 1. Using the concept of *fidelity*, [53] it has been shown rigorously by Mayers [45,46] (see also [47,48]) that even then Alice can almost always cheat successfully. Therefore, one concludes that even non-ideal quantum bit commitment is impossible. For a review on quantum bit commitment, see [51].

F. Aftermath of the Fall of Quantum Bit Commitment

In conclusion, the fatal flaw in quantum bit commitment protocols is that they all involve an *implicit* assumption that some measurements are performed by the two users. However, with quantum computers and quantum storage devices, a cheater, Alice, can almost always cheat successfully with entanglement. The significance of this discovery lies in its generality: Not only existing quantum bit commitment schemes, but also *any* quantum bit commitment scheme that one can possibly devise, are necessarily insecure.

Furthermore, as noted in footnote *t*, this 'no-go theorem' applies not only to fully quantum bit commitment schemes, but to all bit commitment schemes based on quantum mechanics—classical, quantum and quantum but with measurements.

Moreover, one cannot bypass this 'no-go theorem' by assuming that the decoherence time involved is short. This is because a cheater can, in principle, perform quantum error correction [54] and fault-tolerant quantum computation [55] to defeat decoherence.

Following the surprising discovery of the insecurity of quantum bit commitment, other quantum protocols such as *ideal* quantum coin tossing, [48] quantum 'one-out-of-two oblivious transfer' and 'one-sided' two-party secure computation [24] were also shown [44] to be

[23] Here I assume that the eigenvalues are non-degenerate. The case of having degenerate eigenvalues can be dealt with in a similar manner.

[24] A *one-sided* two-party secure computation allows only one of the two parties to learn the result $f(x, y)$. In other words, Alice with a private input x and Bob with a private input y cooperate to

impossible. By now, the big hope of unconditionally secure two-party computations has been totally shattered. [44,51]

There is, however, an important caveat in what I am saying. Even though quantum two-party secure computations are impossible *in theory*, they may still be possible *in practice.* The point is, to break those quantum protocols, a cheater generally needs a quantum computer. Therefore, quantum cryptographic protocols allow one to replace classical computational assumptions by quantum computational assumptions. Since it is a huge technological challenge to actually build a quantum computer, quantum two-party computations may still have practical value. Hrubý [56] has worked on a quantum smart card for identification purposes.

Finally, it cannot be over-emphasized that those 'no-go theorems' do not apply to quantum key distribution or quantum money. Quantum cryptography should remain a fertile and challenging subject in the foreseeable future. This is particularly so in view of the recent dramatic advances in experiments.

VIII. QUANTUM CRYPTANALYSIS

The subject of cryptology consists of two parts—cryptography, the art of code-making, and cryptanalysis, the art of code-breaking. In this section, I will turn to cryptanalysis. As remarked earlier, the cheating strategy in quantum bit commitment generally requires a quantum computer. The insecurity of quantum bit commitment, therefore, demonstrates the power of a quantum computer in cryptanalysis against *quantum* cryptography. Here I remark that quantum computer is also a powerful weapon for cryptanalysis against *conventional* cryptography. This is so because quantum computers can crack a number of hard problems that underlie the security of many conventional crypto-systems. For instance, Shor has devised efficient quantum algorithms [10,58] for factoring and for the so-called 'discrete logarithm problem'. [10] Boneh and Lipton [57] have generalized Shor's algorithm to attack any crypto-system with a 'hidden linear form'. In particular, even the discrete logarithm problem in 'elliptic curves' can be solved efficiently by a quantum computer. In conclusion, if a quantum computer is ever built, many widely used public key crypto-systems will be unsafe. What is even more worrying is the fact that this total security break by quantum computers is *retrospective.* By keeping copies of the current transmission, an eavesdropper can, in principle, wait for the construction of a quantum computer in future to decode any top secret message encoded by those breakable public key schemes. In this aspect, quantum cryptography has the advantage of avoiding this retrospective security break.

What about private key or symmetric systems? Grover's efficient algorithm [59] for database search can reduce the time needed for exhaustive key search from $O(N)$ to $O(\sqrt{N})$, where N is the total number of possible keys. For instance, it can speed up millionfold the exhaustive key search against DES (Data Encryption Standard), [2] the most popular

compute a prescribed function $f(x,y)$ in such a way that at the end of the computation, 1) Alice learns nothing about y or $f(x,y)$; 2) Bob learns $f(x,y)$ and 3) Bob learns nothing about x except for what logically follows from y and $f(x,y)$.

computer encryption algorithm. [60] The successful construction of a large scale quantum computer would be the end of DES.[25]

In conclusion, quantum computation can have potentially shattering effect on cryptography. To many conventional cryptographers, this is an unwelcome possibility that is too catastrophic to ignore. For a review on quantum algorithms including Shor's amd Grover's, see chapter six.

IX. THOUGHTS FOR THE FUTURE

Many challenging questions in quantum cryptology remain to be answered. Let me mention a few here.

At the conceptual level, there are now reasonably solid foundations to both quantum cryptography and quantum cryptanalysis. On the one hand, quantum key distribution is generally believed to be secure because of the quantum no-cloning theorem. On the other hand, quantum bit commitment has been shown to be impossible due to cheating by using the EPR effect. The important conceptual questions are: What is the exact boundary to the power of quantum cryptography? And why is there such a boundary?

At a phenomenological level, it would be interesting to see if quantum error correction, a subject to be introduced in chapter seven, can be used in *practice* to increase the range of quantum key distribution from the state-of-the-art tens of kilometers to a futuristic range of thousands of kilometers. This would be an important milestone in the feasibility study of a practical quantum key distribution system.

For experimental quantum cryptography, the proposed ground to satellite experiment is a major challenge. Improvements in photon sources, transmission channels as well as detector technology will ultimately determine the competitiveness of quantum cryptography against its conventional counterparts in military and commercial applications.

Finally, I remark that quantum cryptology is an integrated component of the general field of quantum information processing, whose ultimate goal is the unification of quantum mechanics with subjects such as information theory, computer science and cryptology. Ex-

[25] As a side remark, quantum computer can also solve the 'collision problem' efficiently. Let me first introduce the latter. Given a function $F : X \to Y$, the collision problem is to find a collision in F, i.e., two distinct elements x_0 and x_1 in X such that $F(x_0) = F(x_1)$, assuming that such a pair exists. This problem is important in cryptography because it is commonly assumed that the collision problem is computationally infeasible for a class of functions known as hash functions. Indeed, a brute force attack known as the birthday attack requires $O(\sqrt{N})$ evaluations of the function for a two-to-one function, where $N = |X|$. (The name birthday attack comes from the fact that on average it requires a group of less than 30 persons to find a *pair* of persons having the same birthday. The key point is that there are $r(r-1)/2$ *pairs* to consider.) However, using Grover's algorithm as a subroutine, Brassard, Høyer and Tapp [61] have found a quantum algorithm that finds collisions in arbitrary r-to-one functions after only $O(\sqrt[3]{N/r})$ expected evalutions of the function. Furthermore, there also exist some superfast quantum algorithms [62,63] for complex quantum queries. Their impact to cryptography is, however, unclear to me.

citing unexpected developments will most likely arise out of the interplay of the concepts from quantum cryptology, quantum computing and quantum information and out of inspirations from the classical theory. A closer look at those related subjects may, therefore, give new insights to the development of quantum cryptology.

ACKNOWLEDGMENTS

I am indebted to the generous support from colleagues and mentors at the Calfornia Institute of Technology, Pasadena, U.S.A., at the Institute for Advanced Study, Princeton, U.S.A, and at the Hewlett-Packard Laboratories, Bristol, U.K. Much of this chapter is based on other sources, in particular, an enlightening talk given by C. H. Bennett. Stimulating discussions on the subject with numerous colleagues including M. Ardehali, C. H. Bennett, G. Brassard, R. Cleve, C. Crépeau, D. P. DiVincenzo, L. Goldenberg, J. Hrubý, R. J. Hughes R. Jozsa, J. Kilian, H. J. Kimble, D. Mayers, T. Mor, J. G. Rarity, P. Shor, T. Toffoli and L. Vaidman are gratefully acknowledged. I particularly thank H. F. Chau for fruitful collaborations on the subject, D. W. Leung, T. Spiller and H. Zbinden for helpful comments on this chapter.

APPENDIX A: RSA PUBLIC KEY CRYPTO-SYSTEM

The most well-known public key encryption scheme was invented by Rivest, Shamir and Adleman. [2,64] The security of RSA is based on the difficulty of factoring large numbers. A user, say Bob, first chooses two large primes p and q and computes $N = pq$. He then randomly chooses the encryption key e such that e and $(p-1)(q-1)$ have no common factors. Afterwards, he computes the unique decryption key, d, such that

$$ed = 1 \quad [\mathrm{mod}(p-1)(q-1)]. \tag{27}$$

This computation can be done efficiently by the Euclidean algorithm. Now e and N are made public: They can be published in a public key directory in the same manner as a telephone directory. The decryption key, d, must be kept secret. As p and q are no longer needed, they can be discarded, but never revealed. Suppose a person Alice, who may or may not have met Bob before, would like to send Bob a message $m \pmod N$. She can do so by raising it to the power e, i.e.,

$$c = m^e \pmod N \tag{28}$$

and sending c to Bob. Bob can recover the message m by raising c to the power d. This is because, from elementary number theory, $m^{(p-1)(q-1)} = 1 \pmod N$ for any $m \pmod N$ and, therefore,

$$c^d = m^{ed} = m^{k(p-1)(q-1)+1} = m^{k(p-1)(q-1)} \times m = m \quad \text{all} \pmod N. \tag{29}$$

For a long message, Alice may, for example, expand it in power of N and encrypt each entry in the N-ary expansion individually.

An eavesdropper Eve who does not know d nor the factorization of N will generally have a hard time in deducing m from c, e and N alone. On the other hand, if Eve can factor N into p times q, then she can trivially find the decryption key d by using the Euclidean algorithm with d and $(p-1)(q-1)$ as the inputs.

APPENDIX B: ERROR CORRECTION AND PRIVACY AMPLIFICATION

Here I review a simple but non-optimal procedure for error correction and privacy amplification as introduced in [12]. Recall that Alice and Bob's polarization data may be different due to noise and eavesdropping by Eve. Upon the completion of the quantum transmission, Alice and Bob need to exchange public messages in order to reconcile the difference between their data. I will assume that Eve can listen to all public discussion. Therefore, Alice and Bob should make sure that the public discussion reveals as little information as possible on their data.

A simple scheme of reconciliation is for Alice and Bob to first agree on a random permutation of the bit positions in their strings. They then partition their string into blocks of size k such that each block is highly unlikely to contain more than one error. For each block, Alice and Bob compare its parity publicly. If the parities computed by Alice and Bob respectively are the same, a block is tentatively accepted as correct. If the parities are different, a binary search will now be applied to the block. This will disclose $\log_2 k$ bits of parities about the sub-blocks before the error is finally located and corrected. To prevent Eve from gaining information through the public discussion, Alice and Bob should discard the last bit of each block or sub-block whose parity has been announced.

Notice that if two or more errors occur in the same block, some of them may remain undetected. To correct those errors, random permutation and block parity disclosure (with increasing block size) is repeated several times. Once Alice and Bob have reached the stage in which there are probably only a few errors left, it will be inefficient for them to continue the block parity disclosure process. Therefore, a new process is now adapted: they can apply an iterative process of comparing the parity of a publicly chosen random subset of their data. Whenever there is some disagreement between their shared string, the random subset parities will disagree with a probability 1/2. If a disagreement is found, a bisective search is applied to locate and correct the error. As before, the last bit of each set whose parity is announced should be discarded in order to avoid Eve from getting additional information from the public discussion.

This iterative process is repeated until Alice and Bob fail to find any disagreement in many (say 20) consecutive comparisons. In this case, it is highly likely that they share the same string.

This completes the process of error correction. Alice and Bob can now convert their polarization data into a raw key. The remaining problem is that Eve may have partial information on this raw key. Therefore, Alice and Bob perform *privacy amplification*, i.e., they distill a shorter but perfectly secure key from such a partly secure raw key. Bennett *et al.* presented a procedure for achieving this distillation process: Suppose that there are n bits in the raw key and Eve has at most l deterministic bits of information about it. A *hash* function h should be chosen randomly from an appropriate class of functions $\{0,1\}^n \rightarrow \{0,1\}^{n-l-s}$ where $s > 0$. At the end, the raw key x will be mapped into $h(x)$ such that Eve's expected information on it is less than $2^{-s}/\ln 2$ bit. Alice and Bob can now each compute the value $h(x)$ and keep it as a secret key for subsequent communications.

REFERENCES

[1] D. Kahn, *The Codebreakers: The Story of Secret Writing*, New York, Macmillan Publishing Co., 1967.

[2] B. Schneier, *Applied Cryptography*, New York, John Wiley and Sons, Inc., 1996.

[3] For an excellent but perhaps outdated review, see C. H. Bennett, G. Brassard and A. K. Ekert, *Sci. Am.* (Oct. 1992), 50.

[4] The following discussion is based on a talk delivered by C. H. Bennett.

[5] W. K. Wootters and W. Zurek, *Nature* **299**, 802 (1982); D. Dieks, *Phys. Lett.* A **92**, 271 (1982).

[6] N. Herbert, *Found. Physics* **12**, 1171 (1982).

[7] C. A. Fuchs, Los Alamos preprint archive quant-ph/9611010.

[8] S. Wiesner, *Sigact News* **15**, 78 (1983).

[9] W. Diffie and M. E. Hellman, *IEEE Transactions on Information Theory*, v. IT-22, n. 6, 644 (1976).

[10] P. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, (USA, Nov. 1994), IEEE Press; "Polynominal-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Computing*, to appear, also Los Alamos preprint archive quant-ph/9508027.

[11] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, p. 175-179. IEEE, 1984.

[12] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, *J. Cryptol.* **5**, 3 (1992).

[13] M. N. Wegman and J. L. Carter, *Journal of Computer and System Sciences* **22**, 265 (1981).

[14] B. C. Jacobs and J. D. Franson, *Opt. Lett.* **21**, 1854 (1996); W. T. Buttler *et al.*, "Free-Space Quantum Key Distribution," to be published.

[15] P. D. Townsend, J. G. Rarity, P. R. Tapster, *Electronic Letters* **29** # 14, 1291 (1993); A. Muller, H. Zbinden and N. Gisin, *Nature* **378**, 449 (1995); R. J. Hughes *et al.*, in *Advances in Cryptology: Proceedings of Crypto '96*, Lecture Notes in Computer Science, Vol. 1109, Springer-Verlag, Berlin, p. 329.

[16] B. C. Jacobs and J. D. Franson, "Feasibility of Global Systems for Quantum Cryptography," to be published. R. Hughes has also made a similar proposal.

[17] C. H. Bennett, G. Brassard and J.-M. Robert, *SIAM J. Computing* **17**, 210 (1988).

[18] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, *Phys. Rev. Lett.* **77**, 2818 (1996).

[19] D. Mayers, in *Advances in Cryptology: Proceedings of Crypto' 96*, Lecture Notes in Computer Science, Vol. 1109 (Springer-Verlag, Berlin, 1996) p. 343.

[20] N. Lütkenhaus, *Phys. Rev.* A **54**, 97 (1996).

[21] C. H. Bennett, T. Mor, and J. A. Smolin, *Phys. Rev.* A **54**, 2675 (1996).

[22] E. Biham, and T. Mor, *Phys. Rev. Lett.* **78**, 2256 (1997).

[23] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Los Alamos preprint archive quant-ph/9701039.

[24] R. B. Griffiths, and C.-S. Niu, Los Alamos preprint archive quant-ph/9702015.

[25] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).

[26] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777 (1935); J. S. Bell, *Physics* **1**, 195 (1964); J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Phys. Rev. Lett.* **23**, 880 (1969). These three papers are reprinted in J. A. Wheeler and W. H. Zurek, *Quantum Theory and Measurement* (Princeton University Press, Princeton, 1983), p. 138, p. 403 and p. 409 respectively.

[27] C. H. Bennett, *Phys. Rev. Lett.* **68**, 3121 (1992).

[28] M. Koashi, and N. Imoto, *Phys. Rev. Lett.* **77**, 2137 (1996).

[29] P. D. Townsend, *Nature* **385**, 47 (1997).

[30] E. Biham, B. Huttner, and T. Mor, *Phys. Rev.* A **54**, 2651 (1996).

[31] L. Goldenberg and L. Vaidman, *Phys. Rev. Lett.* **75**, 1239 (1995). A comment to this paper appeared in A. Peres, *Phys. Rev. Lett.* **77**, 3264 (1996). A reply was made in L. Goldenberg and L. Vaidman, *Phys. Rev. Lett.* **77**, 3265 (1996).

[32] W. Y. Hwang, I. G. Koh, and Y. D. Han, Los Alamos preprint archive quant-ph/9702009.

[33] H.-K. Lo and H. F. Chau, "Quantum Cryptographic System with Reduced Data Loss" U. S. Patent pending.

[34] M. Ardehali, "Efficient Quantum Cryptography" unpublished manuscript written in 1992.

[35] S. M. Barnett and S. J. D. Phoenix, *J. Mod. Optics* **40**, 2501 (1993).

[36] H. J. Kimble, Private Communications.

[37] J. S. Kim, Private Communications.

[38] "One Less Thing to Believe in: Fraud at Fake Cash Machine," *New York Times*, 13 May 1993, pp. A1 and B9 as cited in [39].

[39] C. Crépeau and L. Salvail, in *Advances in Cryptology: Proceedings of Eurocrypto '95*, (Springer-Verlag) 133.

[40] G. Brassard and C. Crépeau, "Quantum bit commitment and coin tossing protocols," in *Advances in Cryptology: Proceedings of Crypto '90*, Lecture Notes in Computer Science, Vol. 537, p. 49-61. Springer-Verlag, 1991.

[41] B. Huttner, N. Imoto and S. M. Barnett, *Journal of Nonlinear Optical Physics and Materials* **5**, No. 4 (1996) 823.

[42] G. Brassard, C. Crépeau, R. Jozsa and D. Langlois, "A quantum bit commitment scheme provably unbreakable by both parties," in *Proceedings of the 34th annual IEEE Symposium on the Foundation of Computer Science*, Nov. 1993, p.362-371.

[43] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, "Practical quantum oblivious transfer," in *Advances in Cryptology: Proceedings of Crypto '91*, Lecture Notes in Computer Science, Vol. 576, p. 351-366. Springer-Verlag, 1992.

[44] H.-K. Lo, *Phys. Rev.* A **56**, 1154 (1997).

[45] D. Mayers, "The trouble with quantum bit commitment," Los Alamos preprint archive quant-ph/9603015, to be published.

[46] D. Mayers, *Phys. Rev. Lett.* **78**, 3414 (1997).

[47] H.-K. Lo and H. F. Chau, *Phys. Rev. Lett.* **78**, 3410 (1997).

[48] H.-K. Lo and H. F. Chau, in *Proceedings of the Fourth Workshop on Physics and Computation, PhysComp' 96*, Boston 1996 (New England Complex Systems Institute, Boston, 1996), p. 76, also Los Alamos preprint archive quant-ph/9605026, full paper to appear in a special issue of *Physica* D.

[49] A. C.-C. Yao, in *Proceedings of 26th Annual ACM Symposium on the Theory of Computing*, 1995, p. 67.

[50] J. Kilian in *Proceedings of 1988 ACM Annual Symposium on Theory of Computing*, (May, 1988), p. 20.

[51] H. F. Chau and H.-K. Lo, Los Alamos preprint archive quant-ph/9709053, to appear in a special issue of *Fortschritte der Phys.*

[52] See, for example, the Appendix of L. P. Hughston, R. Jozsa and W. K. Wootters, *Phys. Lett.* **A183**, 14 (1993).

[53] R. Jozsa, *J. Mod. Opt.* **41**, 2315 (1994).

[54] P. W. Shor, *Phys. Rev.* A **52**, R2493 (1995); A. M. Steane, *Phys. Rev. Lett.* **77**, 793 (1996). See also chapter 7 by Andy Steane.

[55] P. W. Shor, in *Proc. 37th Symposium on Foundations of Computer Science*, IEEE Computer Society Press, 1996, p. 56, also Los Alamos preprint archive quant-ph/9605011; J. Preskill, Los Alamos preprint archive quant-ph/9705031. See also chapter 8 by John Preskill.

[56] J. Hrubý, in *Proceedings of International Conference on Cryptography: Policy and Algorithms*, Lecture Notes in Computer Science, Vol. 1029, Springer-Verlag, 1995, p. 282.

[57] D. Boneh and R. J. Lipton, in *Advances in Cryptology: Proceedings of Crypto' 95*, Lecture Notes in Computer Sciences Vol. 963, 424 (1995).

[58] A. Y. Kitaev, Los Alamos preprint archive quant-ph/9511026.

[59] L. K. Grover, in *Proceedings of 28th Annual ACM Symposium on the Theory of Computing* (ACM Press, New York, 1996), p. 212; *Phys. Rev. Lett.* **79**, 325 (1997).

[60] For a survey article on the impact of Grover's algorithm on cryptanalysis, see G. Brassard, *Science* **275**, 627 (1997).

[61] G. Brassard, P. Høyer and A. Tapp, Los Alamos preprint archive quant-ph/9705002.

[62] B. M. Terhal and J. A. Smolin, Los Alamos preprint archive quant-ph/9705041.

[63] L. K. Grover, Los Alamos preprint archive quant-ph/9706005.

[64] R. L. Rivest, A. Shamir and L. M. Adleman, *Communications of the ACM* **21**, # 2, 120 (1978).