Electronic Colloquium on Computational Complexity, Report No. 146 (2005)

Quantum Cryptography: A Survey[*]

Gábor Erdélyi[†] and Tobias Riege[‡] and Jörg Rothe[§]
Institut für Informatik
Heinrich-Heine-Universität Düsseldorf
40225 Düsseldorf, Germany

November 23, 2005

Abstract

We survey some results in quantum cryptography. After a brief introduction to classical cryptography, we provide the physical and mathematical background needed and present some fundamental protocols from quantum cryptography, including quantum key distribution and quantum bit commitment protocols.

1 Introduction

Cryptography is the science of keeping private information from unauthorized access. An algorithm, which is called a *cipher* in this context, scrambles the message via some rule such that restoring the original message is hard—if not impossible—without knowledge of the secret key. Cryptographic technology in use today relies on the hardness of certain mathematical problems. Classical cryptography faces the following two problems. First, the hardness of the problems on which the security of cryptosystems is based (e.g., integer factoring or the discrete logarithm problem) often is not a proven fact but rather a widely believed hypothesis. Second, the theory of quantum computation has yielded new methods to tackle these mathematical problems in a much more efficient way. Although there are still numerous challenges to overcome before a working quantum computer of sufficient power can be built, in theory all classical ciphers might be vulnerable to such a powerful machine. However, while quantum computation seems to be the coffin nail for classical cryptography in a possibly not so distant future, at the same time it offers new possibilities to build encryption methods that are safe even against attacks performed by a quantum computer. Quantum cryptography extends the power of classical cryptography by protecting the secrecy of messages using the physical laws of quantum mechanics.

[*] Presented at *A Magyar Tudomany Napja*, E¨otv¨os J´ozsef F¨oiskola, Baja, Hungary, November 2005. Work supported in part by the DFG under Grants RO 1202/9-1 and RO 1202/9-3.

[†] Email: `erdelyi@cs.uni-duesseldorf.de`.

[‡] Email: `riege@cs.uni-duesseldorf.de`.

[§] Email: `rothe@cs.uni-duesseldorf.de`.

ISSN 1433-8092

Looking back in the history of cryptography, one of the first encryption methods was the scytale. The first recorded use of the scytale dates back to the fivth century B.C. when the Spartans used it to exchange battle information between generals without revealing it to the enemy. To encrypt a message, which we call the *plaintext* in cryptography, a strip of leather or pergament was wrapped around a wooden cylinder, the scytale. The encrypted message, also called the *ciphertext*, was then written from left to right onto the leather, so that unravelling the strip would produce a meaningless alignment of seemingly random letters, see Figure 1 for the encryption of the plaintext "scytaleisatranspositioncipher" by "ssoicaspytihtrteaairlnoesnipc." The decryption of the ciphertext was achieved by using a scytale of the same diameter as the cylinder that was used for encryption.

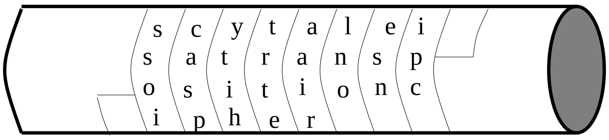

Figure 1: The Scytale

The scytale is a so-called transposition cipher, since only the order of the letters within the message is changed. Another type of encryption is the substitution cipher. Here, instead of swapping the positions of the letters, each plaintext letter is replaced by another letter according to some specific rule. The method of encryption and decryption is called a *cryptosystem*, whereas the particular information used for encryption or decryption in an individual communication is called a *key*. In the case of the scytale, the diameter of the cylinder represents the secret key. Obviously, this ancient cryptosystem has a very low level of security. Once the method of encryption is known to the eavesdropper, he can simply try all possible diameters to reveal the original message. The fact that the cryptosystem is publicly known is not the reason for the insecurity of the communication, but rather the small number of possible keys that can be used for encryption. In the 19th century, Auguste Kerckhoffs stated the principle that the security of a cryptosystem must be based solely on the secrecy of the key itself. Therefore, when designing new ciphers, one should always treat the algorithm as if it were publicly known.

Over time, the amount of information that needed to be encrypted exploded, making it impossible to use simple and insecure procedures like the scytale. At first, mechanical devices were built to speed up the encryption and the decryption process, and to increase the complexity of the keys used to scramble the message. An infamous example of a mechanical cryptosystem is the Enigma, which was used in World War II by the Germans to conceal their military communication. Not following Kerckhoff's principle, the Germans considered the Enigma unbreakable, assuming that the mechanical device used for secure communication was not known to the enemy. But during the war allied cryptanalysts in Bletchley Park near London often were able to decrypt the German military messages. One might argue that breaking the Enigma was one of the most crucial factors for the victory of the allied forces and for ending the war. After the war, it was the invention of the transistor that made the rise of the computer industry possible. The huge speed-up in executing mathematical calculations resulted in the need to create much more secure cryptosystems, among them symmetric block ciphers such as the Data Encryption Standard (DES) and the Advanced Encryption Standard

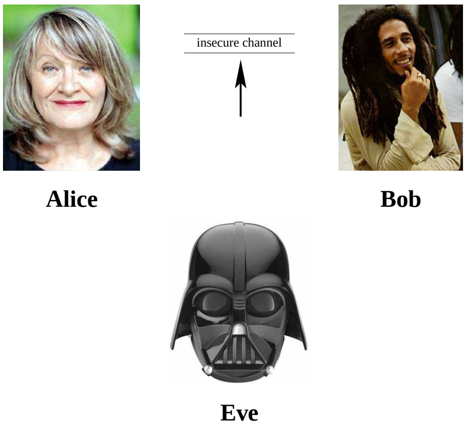

Figure 2: Communication between Alice and Bob, with Eve listening

(AES) and public-key cryptosystems such as RSA and others, which are integrated in modern cryptographic applications currently in use. With the theory of quantum computation, we seem to be at the beginning of yet another era of cryptography. A nice and easy-to-read overview of the history of cryptography is given by Singh [Sin99].

2 Classical Cryptography

Overviews of classical cryptography can be found in various text books, see, e.g., [Rot05,Sti02]. Here, we present just the basic definition of a cryptosystem and give one example of a classical encryption method, the one-time pad.

Definition 1 *A* cryptosystem *is a five-tuple* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *satisfying the following conditions:*

1. $\mathcal{P}$ *is a finite set of possible* plaintexts.

2. $\mathcal{C}$ *is a finite set of possible* ciphertexts.

3. $\mathcal{K}$*, the* keyspace*, is a finite set of possible* keys.

4. *For each* $k \in \mathcal{K}$*, there is an* encryption rule $e_k \in \mathcal{E}$ *and a corresponding* decryption rule $d_k \in \mathcal{D}$*. Every* $e_k : \mathcal{P} \to \mathcal{C}$ *and every* $d_k : \mathcal{C} \to \mathcal{P}$ *is a function satisfying* $d_k(e_k(x)) = x$ *for every plaintext element* $x \in \mathcal{P}$*.*

In the basic scenario in cryptography, we have two parties that wish to communicate over an insecure channel, such as a phone line or a computer network. Usually, these parties are referred to as Alice and Bob. Since the communication channel is insecure, an eavesdropper, called Eve, may intercept the messages that are sent over this channel. By agreeing on a secret key k via a secure communication method, Alice and Bob can make use of a cryptosystem to keep their information secret, even when sent over the insecure channel. This situation is illustrated in Figure 2.

The method of encryption works as follows. For her secret message m, Alice uses the key k and the encryption rule e_k to obtain the ciphertext $c = e_k(m)$. She sends Bob the ciphertext c over the insecure channel. Knowing the key k, Bob can easily decrypt the ciphertext by the decryption rule d_k: $d_k(c) = d_k(e_k(m)) = m$. Knowing the ciphertext c but missing the key k, there is no easy way for Eve to determine the original message m.

There exist many cryptosystems in modern cryptography to transmit secret messages. One early well-known system is the *one-time pad*, which is also known as the *Vernam cipher*. The one-time pad is a substitution cipher. Despite its advantageous properties, which we will discuss later on, the one-time pad's drawback is the costly effort needed to transmit and store the secret keys.

Example 2 (One-time Pad) *For our plaintext elements in $\mathcal{P}$, we restrict ourselves to capital letters and some punctuation marks, which we encode as numbers ranging from 0 to 29, see Figure 3. As is the case with most cryptosystems, the ciphertext space equals the plaintext space. Furthermore, the key space $\mathcal{K}$ also equals $\mathcal{P}$, and we have $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0, 1, \ldots, 29\}$.*

A	B	C	D	E	$\cdots$	X	Y	Z		!	-	.
00	01	02	03	04	$\cdots$	23	24	25	26	27	28	29

Figure 3: Letters and punctuation marks encoded by numbers from 0 to 29

Next, we describe how Alice and Bob use the one-time pad to transmit their messages. One concrete example is shown in Figure 4. Let $m = m_1 m_2 \ldots m_n$ be a given message of length n, which Alice wishes to encrypt. For each plaintext element m_i, where $1 \leq i \leq n$, Alice randomly and uniformly chooses a key element $k_i \in \{0, 1, \ldots, 29\}$ and adds the plaintext numbers to the key numbers. The result is taken modulo 30. For example, the last letter of the plaintext from Figure 4, "D," is encoded by "03." The corresponding key is "28," so we have $c = 3 + 28 = 31$. As $31 \equiv 1 \bmod 30$, our plaintext letter "D" is decrypted as "B." The encryption and decryption can be written as $c_i = (m_i + k_i) \bmod 30$ and $m_i = (c_i - k_i) \bmod 30$, respectively.

plaintext $p \in \mathcal{P}$	O	N	E	-	T	I	M	E		P	A	D
p encoded	14	13	04	28	19	08	12	04	26	15	00	03
key k	06	13	02	01	14	05	07	18	05	26	13	28
ciphertext $c \in \mathcal{C}$	20	26	06	29	03	13	19	22	01	11	13	01
c decoded	U		G	.	D	N	T	W	B	L	N	B

Figure 4: Encryption and decryption example for the one-time pad

To prove that the one-time pad is perfectly secure, we need a few notions from probability theory.

Definition 3 *Let $\mathbf{X}$ be a discrete random variable that can take on values from a finite set X according to a given probability distribution on X. We denote by $\Pr[\mathbf{X} = x]$ the probability that $\mathbf{X}$ takes on the value $x \in X$. If $\mathbf{X}$ is clear from the context, we just write $\Pr[x]$. For all $x \in X$, $\Pr[x] \geq 0$. Additionally, $\sum_{x \in X} \Pr[x] = 1$. For another random variable $\mathbf{Y}$ defined on the finite set Y, we define the conditional probability that $\mathbf{X}$ takes on the value $x \in X$ given that $\mathbf{Y}$ takes on the value $y \in Y$ by $\Pr[x|y]$.*

Suppose that a probability distribution on the finite plaintext space $\mathcal{P}$ is given. Thus, the plaintext element defines a random variable, which we denote by $\mathbf{p}$. The key chosen by Alice for communication with Bob also defines a random variable, which we call $\mathbf{k}$. Both probability distributions, for $\mathbf{p}$ and $\mathbf{k}$, induce a probability distribution on the ciphertext $\mathcal{C}$. Thus, we have another random variable $\mathbf{c}$ for the ciphertext element. We call a cryptosystem *perfectly secure* if $\Pr[p|c] = \Pr[p]$ for all $p \in \mathcal{P}$ and $c \in \mathcal{C}$. That means that the event that plaintext p occurs is independent of the ciphertext c being observed. In other words, knowing c yields no advantage when trying to retrieve the original plaintext p.

Shannon [Sha49] gave a characterization of when perfect secrecy can be guaranteed. Suppose that $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is a cryptosystem with $||\mathcal{K}|| = ||\mathcal{C}||$ and such that every plaintext element will be encrypted with a positive probability. Then, this cryptosystem achieves perfect secrecy if and only if (1) the probability distribution on the key space $\mathcal{K}$ is uniform, and (2) for each $p \in \mathcal{P}$ and for each $c \in \mathcal{C}$, there exists a unique key k such that $e_k(p) = c$. The proof of Shannon's theorem can be found, e.g., in [Sha49,Rot05,Sti02]. Using this theorem, it is easy to see that the one-time pad satisfies the property of perfect secrecy. As a new key element is created for each single plaintext element randomly under the uniform distribution, knowing the ciphertext is no advantage for an eavesdropper when trying to obtain the original message.

Although it provides perfect secrecy, the one-time pad also has severe disadvantages that make it impractical to use. Remember that the key has to be as large as the message itself. Thus, the number of bits that need to be exchanged over a secure channel for the key increases with the amount of information that Alice and Bob wish to transmit secretly. Therefore, one might ask why they don't use the secure channel for their communication directly. Using the same key for encryption more than one time is no alternative, as the one-time pad's perfect secrecy crucially depends on creating a new key for every single plaintext element.

The scytale and the one-time pad are two examples of a symmetric cryptosystem. That means that the same key is used for encryption and decryption (or, at least, that the decryption key can be easily determined from the encryption key). Thus, Alice and Bob have to agree on a joint secret key prior to their conversation via a secure channel. Secret-key agreement protocols were proposed by Diffie and Hellman [DH76], Rivest and Sherman (see [RS97,HR99]), and others. However, a major disadvantage of symmetric ciphers and the related issue of key distribution occurs when the communicating parties in a large network need to share joint secret keys. When n parties participate in a communication network, $n(n+1)/2$ different keys have to be exchanged and stored safely.

Public-key cryptosystems, also called asymmetric cryptosystems, circumvent the key distribution and storage problem. Instead of having one unique key for every pair of parties, only one key per party is needed to communicate securely. In 1976, Whitfield Diffie and Martin Hellman [DH76] proposed the principle idea of public-key cryptography, namely to use two distinct keys, a public key for encryption and a private key for decryption. The first public-key cryptosystem is the RSA system, named after its three inventors Ron Rivest, Adi Shamir, and Leonard Adleman [RSA78].[1] RSA is used in numerous cryptographic applications still today. Public-key cryptosystems are based on so-called *one-way functions*, functions that are easy to compute but hard to invert.

To communicate via a public-key cryptosystem, Alice creates two keys, k_{public} and k_{private}. Her encryption key k_{public} is public, but Alice keeps her private decryption key k_{private} secret. Each time Bob wishes to communicate with Alice, he looks up her public key and uses it to encrypt his message. Since only Alice knows her private key, she alone can (efficiently) compute the inverse of the encryption function.

The key issue is to find one-way functions that are safe enough to use for public-key cryptography. The first one-way function designed for this purpose (i.e., the RSA encryption function) was based on the problem of factoring large integers. Up to now, no efficient algorithm for computing the prime factors of some given integer is known. Other public-key cryptosystems—such as the ElGamal system [ElG85]—are based on the presumed hardness of computing discrete logarithms. One disadvantage of such systems is that they often lack a proof of security. Another disadvantage is that the directory storing the public keys has to be protected against manipulation. If eavesdropper Eve replaces Alice's public key with her own key, she can decrypt all messages sent to Alice.

Since the publication of Peter Shor about prime factorization and computing discrete logarithms with quantum computers [Sho97], all cryptosystems whose security is based on the hardness of solving these mathematical problems have become theoretically vulnerable. Although it will certainly take some time for the first practical quantum computers to emerge, it is advisable to look for alternative, new cryptosystems that do not solely build on the hardness of solving such mathematical problems with current computer technology. Quantum theory seems to be the perfect basis on which to build such a new cryptosystem that withstands an attack even by quantum computers.

3 From Bits to Qubits

The most important unit of information in computer science is the *bit*. Two possible values can be stored by a bit: it is either equal to "0" or equal to "1." These two distinct states can be represented in various ways, for example by a simple switch or a capacitor: if not charged, the capacitor holds the value zero; if charged, it contains the value "1."

The quantum analog of the bit is called *qubit*, which is derived from *qu*antum *bit*. Both entities are similar in the sense that they are represented by two states. For the qubit, the basic states are called $|0\rangle$ and $|1\rangle$. But unlike its classical counterpart, the qubit is represented by a two-dimensional quantum system and can be in a coherent superposition of the two states. Its general state is expressed by

$$|Q\rangle = \alpha|0\rangle + \beta|1\rangle,$$

[1] In 1997, the British Government Communications Headquarters revealed that its researchers James Ellis, William Cocks, and Malcolm Williamson had independently and even earlier discovered the principle idea of public-key cryptography, the cryptosystem now called RSA, and the secret-key agreement protocol now called Diffie–Hellman, see, e.g., [Sin99,Rot05].

with complex numbers α and β satisfying $||\alpha||^2 + ||\beta||^2 = 1$. Thus, we view a qubit $|Q\rangle$ as a vector of unit length in the two-dimensional Hilbert space over complex numbers. This does not mean that the value of the qubit is somewhere between zero and one, but rather that the probability that the qubit takes on the value $|0\rangle$ or the value $|1\rangle$ once measured is equal to respectively $||\alpha||^2$ or $||\beta||^2$. The most important property of the qubit is that any measurement performed on it alters its state, which makes it impossible to copy the contained quantum information. This fact is known as the no-cloning theorem in quantum mechanics.

There exist many possibilities to represent a qubit in practice, as every quantum system with at least two states can serve as a qubit. For example, the spin of an atom or the polarization of a light particle (called a photon) can represent the state of a qubit. Even a cat with its two basic states "dead" and "alive" might serve as a representation; see Schr¨odinger's well-known example of how to visualize the concept of quantum mechanics [Sch35]. The cat's problem—or fortune from the animal's point of view—when being used as a quantum system is its sheer size compared to that of an atom or a photon. There is no way to protect such a big quantum instance from interaction with its environment, which in turn will result in decoherence of the superposition of the cat. For the rest of the paper, we will leave the cat alone and use photons to represent qubits.

Photons can be viewed both as particles and as electromagnetical waves. Regarding the latter, a specific property of photons is their transversality, which means that the electrical and the magnetical fields are orthogonal to each other and to the propagation direction. The inclination of the electrical and magnetical fields to the axis of the propagation is called the polarization. To obtain photons with a desired polarization, one may use a filter that absorbs those photons with undesired polarization out of the light emerging from the source. Figure 5 shows such a polarization filter. Two things can happen: Either the photon passes through the filter and gets the desired polarization, or it will be absorbed by the filter and its energy is converted into heat. Let γ be the angle between the polarization filter and the electrical field of the photon. The probability that the photon passes the filter equals $\cos^2\gamma$. Thus, it will be absorbed with probability $1 - \cos^2\gamma$.

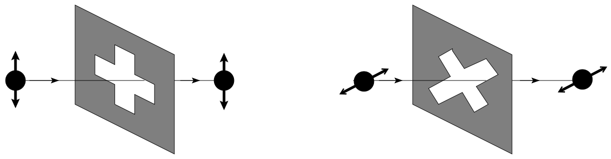

Figure 5: Polarization filters with rectilinear and diagonal basis

There are strict rules to get information out of a quantum state. This can be done by a mathematical structure called observable. Any observable can be mathematically represented by a so-called observable operator, which is a Hermitian matrix, i.e., A is self-adjoint: $A = \overline{A}^T$, where $\overline{A}^T$ denotes the conjugate transpose. All possible values of the observable are eigenvalues of the matrix. Let A be an observable. Define $\langle A\rangle$ to be the expected value we would obtain if we would measure A in the same quantum system again and again. $\Delta A = \sqrt{\langle A^2\rangle - \langle A\rangle^2}$ is the root of the average quadratic deviation with $A^2 = A \cdot A$. Let $[A, B] = AB - BA$ be the commutator of the two observables A and B.

Suppose we have a quantum state ρ, how can we identify the final value $x \in X$ of all outcomes? A positive operator valued measure (POVM) is a set of nonnegative Hermitian operators $\mathcal{E} = (E_x)_{x\in X}$ that act in the Hilbert space of a quantum system and sum to the identity operator, i.e., $\sum_{x\in X} E_x = 1$, where 1 is the identity matrix. The probability for the outcome x, if the system is in a state described by the density matrix ρ, is given by $p^{\mathcal{E}}(x) = Tr(\rho E_x)$. A brief history of POVMs in quantum theory is given in [Bra99].

It is impossible to do a proper measurement of specified observables simultaneously. If we define a state of an observable precisely, this will make it impossible to define the other state precisely as well. This principle is called the Heisenberg uncertainty relation. The general form of the Heisenberg uncertainty relation for observables A and B is $\Delta A \Delta B \geq \frac{1}{2}|\langle [A, B]\rangle|$. We can measure both values exactly only if the left-hand side is equal to 0, i.e., there is no uncertainty in the measurement. And this is possible only if the commutator can be reduced to a matrix with only 0 entries. In this case we say that A and B are commuting.

For example, suppose we want to simultaneously measure the position x and the momentum y of a particle. We need light with short wavelength to measure x strictly. The problem is that light with short wavelength increases the momentum of the particle. On the other hand, we need light with long wavelength to measure the momentum of the particle, but in this case we cannot determine its position precisely.

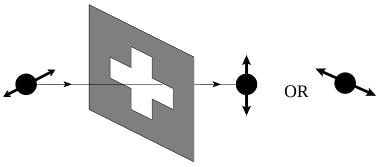

Figure 6: The Heisenberg uncertainty relation also holds for polarized photons

In quantum cryptography we generally use more than just one qubit. A quantum register is an ordered set of a finite number of qubits. The standard basis of a n-qubit register is

$$B = \{|i\rangle \mid i \text{ is a } n\text{-bit binary string }\}.$$

4 Quantum Key Distribution

Quantum cryptography exploits the quantum mechanical property that a qubit cannot be copied or amplified without disturbing its original state. Alice and Bob use a quantum channel to exchange a random sequence of bits, which will then be used to create a key for the one-time pad used for communication over an insecure channel. Any disturbance of the qubits, for example Eve trying to measure the qubits' state, can be detected with high probability.

In this section, we describe the BB84 protocol proposed by Charles Bennett and Gilles Brassard in 1984, see [BB84]. It was the first protocol suggested that uses quantum mechanics for two parties to agree on a joint secret key. After describing the protocol in detail, we show that it is secure against all collective attacks, which implies that it is secure against any attack.

4.1 The BB84 Protocol

In this protocol, Alice and Bob use a quantum channel by sending qubits. They are also connected by a classical channel, which is insecure against an eavesdropper but unjammable. Alice and Bob use four possible quantum states in two conjugate bases (say, the rectilinear basis $+$ and the diagonal basis $\times$). We use $|0\rangle_+$ and $|0\rangle_\times = (|0\rangle_+ + |1\rangle_+)/\sqrt{2}$ for 0, and $|1\rangle_+$ and $|1\rangle_\times = (|0\rangle_+ - |1\rangle_+)/\sqrt{2}$ for 1. The protocol works as follows.

1. Alice sends a n''-bit string to Bob.
2. For each qubit, Alice tells Bob via the classical channel whether she used the basis $+$ or the basis $\times$. They keep the bits where Bob has used the same basis for his measurement as Alice. Now they have n' qubits left.
3. Alice and Bob compare a few bits (say n_{test} many) for which they used the same basis. When the estimated error-rate p_{test} is less than a pre-agreed limiting value $p_{allowed}$, then the test succeeds. They now have an n-bit string $n = n' - n_{test}$.
4. Finally, Alice and Bob obtain a joint secret key from the remaining n bits by performing error correction and privacy amplification.

Alice's string	1	1	0	1	0	0	1	0	1	1	1	1	0	0
Alice's basis	$+$	$+$	$+$	$\times$	$\times$	$+$	$\times$	$\times$	$\times$	$\times$	$+$	$+$	$+$	$+$
Alice sends	—	—	|	\	/	|	\	/	\	\	—	—	|	|
Bob's basis	$+$	$\times$	$+$	$+$	$\times$	$+$	$\times$	$+$	$\times$	$\times$	$+$	$+$	$+$	$+$
Bob's string	1	0	0	1	0	0	1	1	1	1	1	1	0	0
Same basis?	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Bits to keep	1		0		0	0	1		1	1	1	1	0	0
Test	Y		N		N	Y	N		N	N	N	Y	Y	N
Key			0		0		1		1	1	1			0

Table 1: The BB84 Key Distribution Protocol

There is a simple method for error correction. Alice chooses two bits at random and tells Bob the XOR-value of the two bits. Bob tells Alice if he has the same value. In this case they keep the first bit and discard the second bit. If their values differ, they discard both bits. The remaining bits are added to the key.

The probability to detect an eavesdropper Eve is $1/4$ for every bit. Thus, with probability $3/4$, Eve is lucky and won't be detected. If Alice and Bob compare N bits, the probability to detect Eve is $1 - (3/4)^N$. When N increases, the probability that Eve's attack succeeds converges to zero.

4.2 Security of Quantum Key Distribution

In this section, we show the security of quantum key distribution against the most general attack, the so-called joint attack. Collective attacks are probably the strongest joint attacks. In a joint attack, Eve can delay her measurements until receiving all classical data, and she can manipulate the qubits without anyone noticing. An important subclass of the joint attacks is a collective attack where each qubit is attached to a separate probe, the measurement is delayed and performed collectively on all probes after all classical data is received.

In order to prove the security of quantum key distribution against all collective attacks we first have to introduce some definitions and notations. For two binary strings k and l, let $k \oplus l$ denote the bitwise XOR addition of k and l. We call $Tr|\rho_0 - \rho_1|$ the trace-norm of the Hermitian operator $(\rho_0 - \rho_1)$, where ρ_0 and ρ_1 are two density matrices. In this section, we use only Hermitian matrices, thus $Tr(A)$ is nothing else than the sum of the absolute values of the eigenvalues of A.

For random variables $\mathbf{X}$ and $\mathbf{B}$, we will write $p(x)$ for $p(\mathbf{X} = x)$ and $p(b)$ for $p(\mathbf{B} = b)$. We denote the conditional probability by $p_b(x) = p(\mathbf{X} = x|\mathbf{B} = b)$. We need a function that gives the increase of information about the input if the output is known. To this end, we introduce the entropy between the input and the output, which is defined as

$$H(\mathbf{X};\mathbf{B}) = -\sum_{b\in B} p(b)\log p(b) + \sum_{x\in X} p(x) \sum_{b\in B} p_x(b)\log p_x(b).$$

When the input probabilities are equal for a binary input $\mathbf{B}$, then the entropy is $H(\mathbf{B};\mathbf{X}) = \sum_{x\in X} p(x) H_2(p_x(0))$, with $H_2(p) = 1 + p\log p + (1-p)\log(1-p)$. Every probability distribution in the entropy can be computed with $p_0(x)$ and $p_1(x)$. Thus to define the input when the output is given is the same as to distinguish $p_0(x)$ and $p_1(x)$. We can define a new function for binary inputs with equal probabilities, $SD(p_0(x), p_1(x)) \equiv H(\mathbf{B};\mathbf{X})$, the Shannon Distinguishability.

We present only a proof sketch, a complete proof can be found in [BBB$^+$98]. Given two equiprobable states ρ_0, ρ_1, and a measurement procedure (POVM) $\mathcal{E}$, let $p_b^{\mathcal{E}}(x) = Tr(\rho_b E_x)$; for all $\mathcal{E}$, let $SD^{\mathcal{E}}(\rho_0, \rho_1) \equiv SD(p_0^{\mathcal{E}}(x), p_1^{\mathcal{E}}(x))$. The optimal Shannon Distinguishability $SD(\rho_0, \rho_1) \equiv \sup_{\mathcal{E}}[SD^{\mathcal{E}}(\rho_0, \rho_1)]$, where the supremum is taken over all measurement procedures on all possible sets X, gives us the maximum information we can obtain from a state. Unfortunately, we are not able to compute the exact value of the optimal Shannon Distinguishability, therefore we will give two bounds. The first bound shows that tracing out does not increase information, it merely leads to a useful upper bound in special cases.

The first bound: Let $\widetilde{\rho_0}$ and $\widetilde{\rho_1}$ be two density matrices defined on a space $\mathcal{H}_1 \otimes \mathcal{H}_2$. Further, let $\rho_i = Tr_2(\widetilde{\rho_i})$ be the density matrices on $\mathcal{H}_1$, obtained by tracing out $\mathcal{H}_2$. Then,

$$SD(\rho_0, \rho_1) = SD(Tr_2(\widetilde{\rho_0}), Tr_2(\widetilde{\rho_1})) \leq SD(\widetilde{\rho_0}, \widetilde{\rho_1}). \tag{4.1}$$

If $\widetilde{\rho_b}$ is a pure state, we call $\widetilde{\rho_b}$ the lift-up or purification of ρ_b.

The second bound: For any two density matrices ρ_0 and ρ_1,

$$SD(\rho_0, \rho_1) \leq \frac{1}{2} Tr|\rho_0 - \rho_1|. \tag{4.2}$$

The proof of the two bounds can be found in [BBB$^+$98].

We assume that Eve's probes are in an arbitrary but fixed initial pure state $|E\rangle$. In a collective attack, Eve can change the state $|b\rangle$ sent by Alice to the global states

$$\begin{aligned} |0\rangle_+ &\mapsto |E^+_{0,0}\rangle|0\rangle_+ + |E^+_{0,1}\rangle|1\rangle_+ \equiv |\phi^+_0\rangle; \\ |1\rangle_+ &\mapsto |E^+_{1,0}\rangle|0\rangle_+ + |E^+_{1,1}\rangle|1\rangle_+ \equiv |\phi^+_1\rangle, \end{aligned}$$

where the $|E^+_{i,j}\rangle$ are Eve's non-normalized states. We assume that Eve is strong enough to control the natural noise.

Now we can identify Bob's error probability (measuring $|0\rangle_+$ when $|1\rangle_+$ was sent etc.). We have $p_e^+ = \frac{1}{2}(\langle E^+_{0,1}|E^+_{0,1}\rangle + \langle E^+_{1,0}|E^+_{1,0}\rangle)$ for the rectilinear basis, and $p_e^\times = \frac{1}{2}(\langle E^\times_{0,1}|E^\times_{0,1}\rangle + \langle E^\times_{1,0}|E^\times_{1,0}\rangle)$ for the diagonal basis. Alice uses the two bases with the same probability, so Bob's overall probability of error is $p_e = \frac{1}{2}(p_e^\times + p_e^+)$, thus $p_e^\times \leq 2p_e$ and $p_e^+ \leq 2p_e$. In a few steps we can convert this result [BBB+98] into

$$p_e^\times = \frac{1 - \Re(\langle E^+_{0,0}|E^+_{1,1}\rangle + \langle E^+_{1,0}|E^+_{0,1}\rangle)}{2}, \tag{4.3}$$

where $\Re(z)$ denotes the real part of the complex number z. Everything we will say in the following for a basis holds by symmetry for the other basis too. Eve's goal is tracing-out Bob from the states ϕ^+_b if the $+$ basis was used:

$$\begin{aligned} \rho^+_0(E) &= |E^+_{0,0}\rangle\langle E^+_{0,0}| + |E^+_{0,1}\rangle\langle E^+_{0,1}|; \\ \rho^+_1(E) &= |E^+_{1,0}\rangle\langle E^+_{1,0}| + |E^+_{1,1}\rangle\langle E^+_{1,1}|. \end{aligned}$$

There are many purifications that also result in the same reduced density matrices for Eve, in particular

$$\begin{aligned} |\psi^+_0\rangle &= |E^+_{0,0}\rangle|0\rangle_+ + |E^+_{0,1}\rangle|1\rangle_+; \\ |\psi^+_1\rangle &= |E^+_{1,1}\rangle|0\rangle_+ + |E^+_{1,0}\rangle|1\rangle_+. \end{aligned}$$

Now, if there is no disturbance, the angle between the two purifications is zero. The states in Eve's hands are the trace-outs of these pure states. These states exist in some Hilbert space $\mathcal{H}^E \otimes \mathcal{H}^2$, and they are normalized. Here, $\mathcal{H}^2$ is the two-dimensional Hilbert space. Thus $|\langle\psi^+_0|\psi^+_1\rangle| = \cos(2\alpha_+)$, for some angle α_+, $0 \leq \alpha_+ \leq \pi/4$.

Let $|\Psi^+_0\rangle = |\psi^+_0\rangle$ and $|\Psi^+_1\rangle = e^{i\theta}|\psi^+_1\rangle$. There exist two normalized orthogonal states $|0^+_{\mathcal{H}}\rangle$ and $|1^+_{\mathcal{H}}\rangle$ with

$$\begin{aligned} |\Psi^+_0\rangle &= \cos(\alpha_+)|0^+_{\mathcal{H}}\rangle + \sin(\alpha_+)|1^+_{\mathcal{H}}\rangle; \\ |\Psi^+_1\rangle &= \cos(\alpha_+)|0^+_{\mathcal{H}}\rangle - \sin(\alpha_+)|1^+_{\mathcal{H}}\rangle. \end{aligned}$$

Since

$$1 - 2\sin^2(\alpha_+) = \langle\Psi^+_0|\Psi^+_1\rangle = |\langle\psi^+_0|\psi^+_1\rangle| = |\langle E^+_{0,0}|E^+_{1,1}\rangle + \langle E^+_{1,0}|E^+_{0,1}\rangle|,$$

we have $\Re(\langle E^+_{0,0}|E^+_{1,1}\rangle + \langle E^+_{1,0}|E^+_{0,1}\rangle) \leq 1 - 2\sin^2(\alpha_+)$.

We can deduce from (4.3) that Eves's state is a partial trace of the pure states $|\Psi_b^+\rangle$ with $\sin(\alpha_+) \leq \sqrt{p_e^\times}$. Because of the symmetry of the bases, $\sin(\alpha_\times) \leq \sqrt{p_e^+}$ also holds. We know that $p_e^\times \leq 2p_e$ and $p_e^+ \leq 2p_e$, so we can conclude that $\sin(\alpha_+) \leq \sqrt{2p_e}$ and $\sin(\alpha_\times) \leq \sqrt{2p_e}$.

In what follows, we omit the indices $\times$ and $+$ for the bases, since Alice and Bob use the same basis from now on. Eve detects which basis is used only after she retransmitted the particle towards Bob.

After the two parties discard the bits where they used different bases, and those bits they used to show that $p_{test} \leq p_{allowed}$, they have an n-bit string $\mathbf{x}$ left. From now on, we will use boldface letters to denote strings in $\{0,1\}^n$. We will use boldface letters also in the following meaning: If $\mathbf{j} = j_1 \cdots j_n$ is the concatenation of n bits, then $|\mathbf{j}\rangle = |j_1\rangle_1 \cdots |j_n\rangle_n$.

The global state of Eve's probes is a partial trace of $|\Psi_\mathbf{x}\rangle$, the tensor product of $|\Psi_{x_i}\rangle$, where $|\Psi_{x_i}\rangle = \cos(\alpha_i)|0\rangle_i + (-1)^{x_i}\sin(\alpha_i)|1\rangle_i$ is the purification of Eve's state after retransmitting the ith bit x_i to Bob. Let $d_\mathbf{j} = d_{j_1} \cdots d_{j_n}$, where $d_{j_i} = \cos(\alpha_i)$ if $j_i = 0$, and $d_{j_i} = \sin(\alpha_i)$ if $j_i = 1$. It follows that

$$|\Psi_\mathbf{x}\rangle = \otimes_{i=1}^n \left((\cos(\alpha_i)|0\rangle_i + (-1)^{x_i}\sin(\alpha_i)|1\rangle_i)\right) = \sum_{\mathbf{j}\in\{0,1\}^n} d_\mathbf{j}(-1)^{\mathbf{xj}}|\mathbf{j}\rangle,$$

where $\mathbf{xj} = \sum_{i=1}^n x_i j_i \bmod 2$.

At this point we are going to show an example for $|\Psi_\mathbf{x}\rangle$. Let $\mathbf{x} = 10$, then

$$\begin{aligned} |\Psi_{10}\rangle &= (\cos(\alpha_1)|0\rangle_1 - \sin(\alpha_1)|1\rangle_1) \otimes (\cos(\alpha_2)|0\rangle_2 + \sin(\alpha_2)|1\rangle_2) \\ &= \cos(\alpha_1)\cos(\alpha_2)|00\rangle + \cos(\alpha_1)\sin(\alpha_2)|01\rangle - \\ &\quad \sin(\alpha_1)\cos(\alpha_2)|10\rangle - \sin(\alpha_1)\sin(\alpha_2)|11\rangle \end{aligned}$$

Since $(-1)^{\mathbf{xj}}(-1)^{\mathbf{xk}} = (-1)^{\mathbf{x}(\mathbf{j}\oplus\mathbf{k})}$, the state in Eve's hands, i.e., the lift-up of Eve's density matrix, is

$$\widetilde{\rho_\mathbf{x}} = |\Psi_\mathbf{x}\rangle\langle\Psi_\mathbf{x}| = \sum_{\mathbf{j},\mathbf{k}\in\{0,1\}^n} d_\mathbf{j} d_\mathbf{k} (-1)^{\mathbf{x}\cdot(\mathbf{j}\oplus\mathbf{k})}|\mathbf{j}\rangle\langle\mathbf{k}|, \tag{4.4}$$

for all the strings $\mathbf{x}$ sent by Alice.

We still have to analyze the parity bit. The procedure to encode one key-bit $b \in \{0,1\}$ with a substring of the n bits that were sent by Alice looks as follows:

1. To define the relevant substring, Alice chooses a string $\mathbf{v} \in \{0,1\}^n$ and sends it to Bob.
2. Bob can calculate the bit b, as he knows that $b = \mathbf{x}\cdot\mathbf{v}$.

Now Eve has a problem, since only the value of $\mathbf{v}$ is known to her, so she has to guess $b = \mathbf{x}\cdot\mathbf{v}$. Only strings $\mathbf{x}$ with $\mathbf{x}\cdot\mathbf{v} = b$ satisfy

$$\widetilde{\rho_b^\mathbf{v}} \equiv 2^{-n+1} \sum_{\{\mathbf{x}|\mathbf{x}\cdot\mathbf{v}=b\}} |\Psi_\mathbf{x}\rangle\langle\Psi_\mathbf{x}|.$$

Eve has to distinguish between the two density matrices $\rho_b^\mathbf{v}$ in her hands to find out b, where the $\widetilde{\rho_b^\mathbf{v}}$ are lift-ups of $\rho_b^\mathbf{v}$.

Let $\Delta^{\mathbf{v}} \equiv \widetilde{\rho_0^{\mathbf{v}}} - \widetilde{\rho_1^{\mathbf{v}}}$. The trace-norm of $\Delta^{\mathbf{v}}$ can be calculated [BBB+98] by

$$Tr|\Delta^{\mathbf{v}}| \leq 2 \sum_{\mathbf{i}\oplus\mathbf{j}=\mathbf{v}} d_{\mathbf{i}} d_{\mathbf{j}} = 2 \sum_{\mathbf{j}} d_{\mathbf{j}} d_{\mathbf{j}\oplus\mathbf{v}} = 2 \prod_{i\in\mathbf{v}} \sin(2\alpha_i), \tag{4.5}$$

where v_i is the ith bit in $\mathbf{v}$. We write $i \in \mathbf{v}$ instead of $v_i = 1$ when looking at $\mathbf{v}$ as a characteristic function of a set also denoted $\mathbf{v}$, see [BBB+98]. Using the bounds (4.1) and (4.2), we notice that

$$SD(\rho_0^{\mathbf{v}}, \rho_1^{\mathbf{v}}) \leq SD(\widetilde{\rho_0^{\mathbf{v}}}, \widetilde{\rho_1^{\mathbf{v}}}) \leq Tr|\Delta^{\mathbf{v}}| \leq 2 \prod_{i\in\mathbf{v}} \sin(2\alpha_i)$$

if Eve does not know the error correction data.

Some remarks on error correction are in order here. For all $\mathbf{s} \in \{0,1\}^r$, let $\mathbf{v_s} = \sum_{i=1}^{r} s_i \mathbf{v}_i$. With a compatible error correction model as in [BBB+98], it can be shown using the two bounds (4.1) and (4.2) that

$$SD(\rho_0^{\mathbf{E},\mathbf{v}}, \rho_1^{\mathbf{E},\mathbf{v}}) \leq 2 \sum_{\mathbf{s}\in\{0,1\}^r} \left(\prod_{i\in(\mathbf{v}\oplus\mathbf{v_s})} (8p_i) \right)^{1/2},$$

where $\mathbf{E} = \{\mathbf{v}_1 \cdot \mathbf{x} = b_1, \mathbf{v}_2 \cdot \mathbf{x} = b_2, \ldots, \mathbf{v}_r \cdot \mathbf{x} = b_r\}$ is a system of r linear equations chosen by Alice such that the $r+1$ strings $\mathbf{v}, \mathbf{v}_1, \ldots, \mathbf{v}_r$ are linearly independent and $b_i \in \{0,1\}$. We write $\mathbf{E}(\mathbf{x})$ for $\mathbf{x}$ satisfying the system $\mathbf{E}$, so $\mathbf{x}$ is a code word.

For all $\mathbf{s}$, let $\widehat{n_{\mathbf{s}}}$ be the number of ones in $\mathbf{v} \oplus \mathbf{v_s}$. Let $p_{\mathbf{s}} = (\sum_{i\in(\mathbf{v}\oplus\mathbf{v_s})} p_i)/\widehat{n_{\mathbf{s}}}$ be the average error in the subset $\mathbf{s}$. Since the geometrical mean is always less than the arithmetical mean, it follows that

$$\left(\prod_{i\in(\mathbf{v}\oplus\mathbf{v_s})} 8p_i \right)^{1/2} \leq (8p_{\mathbf{s}})^{\widehat{n_{\mathbf{s}}}/2},$$

which implies

$$SD(\rho_0^{\mathbf{E},\mathbf{v}}, \rho_1^{\mathbf{E},\mathbf{v}}) \leq 2 \sum_{\mathbf{s}\in\{0,1\}^r} (8p_{\mathbf{s}})^{\widehat{n_{\mathbf{s}}}/2}. \tag{4.6}$$

With these equations at hand, one can prove that the BB84 protocol is secure against all collective attacks. Let us assume that the test was successful with probability $p_{test} \leq p_{allowed}$. The statistical analysis tells us that each of the error values $p_{\mathbf{s}}$ is bounded. Using bound (4.2), the two laws of large numbers of Hoeffding [Hoe63], and Equation (4.6), it follows for the average p_i of all n' relevant bits $p_{n'}$ that

$$p[p_{n'} > p_{test} + 2\delta] \leq 2e^{-2n_{test}\delta^2}.$$

Due to the fact that $p_{n'}$ is bounded, we can also bound $p_{\mathbf{s}}$ in the following way: Let Alice and Bob use $n_{test} = n = n'/2$ bits. Assume that n' is even, otherwise we can throw in another bit. Thus $p_{\mathbf{s}} \leq (n'/\widehat{n_{\mathbf{s}}})p_{n'}$. Eve's information is bounded by

$$2 \sum_{\mathbf{s}\in\{0,1\}^r} \left(\left(\frac{8n'}{\widehat{n_{\mathbf{s}}}} \right) (p_{test} + 2\delta) \right)^{\widehat{n_{\mathbf{s}}}/2},$$

except she has luck with probability $p_{luck} = 2e^{-2n_{test}\delta^2}$. In the case of Eve being lucky, her information is maximal, i.e., only one bit, and her total information is bounded by

$$2 \sum_{\mathbf{s}\in\{0,1\}^r} \left(\binom{16n}{\widehat{n_{\mathbf{s}}}} (p_{test} + 2\delta) \right)^{\widehat{n_{\mathbf{s}}}/2} + 2e^{-2n\delta^2}.$$

Thus, we can give a bound for the Shannon Distinguishability:

$$SD(\rho_0^{\mathbf{E},\mathbf{v}}, \rho_1^{\mathbf{E},\mathbf{v}}) \le 2^{r+1} \left(\binom{16}{\alpha} (p_{test} + 2\delta) \right)^{\alpha n/2} + 2e^{-2n\delta^2},$$

where $\alpha n = \widehat{n} = \min_{\mathbf{s}\in\{0,1\}^r} \widehat{n_{\mathbf{s}}}$.

For reasonable error rates, for example below 2%, there exist many codes where we can choose the parameters n, r, α, and δ such that Eve's information is negligible. In [BBB$^+$99], an asymptotic result of security and reliability using random linear codes is presented, and it is shown that such a code provides asymptotic reliability and security, for an allowed error-rate below 7.56%.

5 Quantum Bit Commitment

When talking about quantum cryptography everyone is thinking about key distribution. However, there are other cryptographic applications as well, such as bit commitment. In 1993, a bit commitment protocol based on quantum mechanics was introduced by Brassard et al. [BCJL93]. The unconditional security of the protocol (which means that the security of the protocol is independent of time, space, and technology of the cheater) has been accepted without proof [Yao95]. Two years later the protocol turned out to be wrong [May95].

A commitment protocol is a procedure in which one party, say Alice, deposits a message such that no one (and in particular not Alice) can either read or change it. A commitment protocol has two stages, the commit phase and the unveil phase. Alice commits herself to the data m by computing $c = f(m)$ and she sends c to Bob. Alice unveils the commitment by showing Bob the preimage m of c. Bit commitment is a special case of a commitment protocol, where the data m consists of only a single bit.

5.1 How to Realize Quantum Bit Commitment

For simplicity, we will use only two-dimensional quantum registers. Systems of higher dimension can be created from two-dimensional systems. The two parties, Alice and Bob, have their own corresponding areas H_A and H_B on their respective sides. They thus perform the protocol on the system $H_A \otimes H_B \otimes H_E$, where H_E corresponds to the environment. We allow any kind of quantum communication between Alice and Bob. The two parties can execute any unitary transformation on their own system. In particular, they can launch new quantum registers in a fixed state $|0\rangle$. Let H_S be the system that stores the classical bits that have been transmitted from Alice's system to Bob's system, or vice versa. Thus, the environment has the form $H_E = H_S \otimes H_{E,A} \otimes H_{E,B}$, where

$H_{E,A}$ and $H_{E,B}$ store untransmitted classical bits that are kept on Alice's side and on Bob's side, respectively.

In quantum bit commitment, the bit b that Alice has in mind must be changed with a procedure $commit(b)$ into a state $|\psi_b\rangle$ of $H_A \otimes H_B \otimes H_E$. The protocol also needs a procedure $unveil(|\psi_b\rangle)$ that returns the value of the bit b, or if Alice cheats, an inconclusive result denoted by $\perp$. We call the protocol correct if the procedure $unveil$ always returns b on $|\psi_b\rangle$ assuming that Alice and Bob are honest.

If one of the parties, say Alice, wishes to perform a binary outcome measurement, she proceeds as follows:

1. Alice launches a quantum register in a fixed state $|0\rangle$.

2. Next she entangles it with the measured system initially in a state $|\phi\rangle$ and receives the state in the form $\alpha|0\rangle|\phi_0\rangle + \beta|1\rangle|\phi_1\rangle$.

3. Alice sends this quantum register to a measuring device in $H_{E,P}$, which stores and amplifies the component $|x\rangle$ as a complex state $|x\rangle^{(E,P)}$. The new state is then of the form $\alpha|0\rangle^{(E,P)}|\phi_0\rangle + \beta|1\rangle^{(E,P)}|\phi_1\rangle$.

To generate a random bit, we can proceed in the same way. The transmission of a classical bit x from Alice to Bob is represented by a transformation that maps $|x\rangle^{(E,A)}|0\rangle^{(E,B)}$ to $|x\rangle^{(S,A)}|x\rangle^{(S,B)}$, see Mayers [May97].

The entire system is always in a state

$$\sum_{\xi_S,\xi_A,\xi_B} \alpha_{(\xi_S,\xi_A,\xi_B)}|\xi_S,\xi_A,\xi_B\rangle^{(E)}|\phi_{(\xi_S,\xi_A,\xi_B)}\rangle,$$

where ξ_S, ξ_A and ξ_B are random binary strings with joint probability $|\alpha_{(\xi_S,\xi_A,\xi_B)}|^2$, and $|\phi_{(\xi_S,\xi_A,\xi_B)}\rangle$ is the state of $H_A \otimes H_B$ combined with the appearance of ξ_S, ξ_A, and ξ_B when a collapse occurs. A party $P \in \{A, B\}$ knows ξ_P and ξ_S. P can choose the next action such that the transformations must behave as if a collapse into the state $|\phi_{(\xi_S,\xi_A,\xi_B)}\rangle$ had really occured.

Next, we will introduce some definitions and notations. Let us assume that Alice is cheating, namely that she has not any specific bit b in mind during the $commit$ phase, and that she chooses this bit later. Let $|\psi'\rangle$ be the state created by Alice's modified procedure $commit'$. Now, $p(b|\ not\ \perp)$ is the probability that $unveil$ returns b on $|\psi'\rangle$, given that it has not returned $\perp$. Alice can certainly choose the probability $p(b|\ not\ \perp)$, see Mayers [May97]. After the procedure $commit'$, Alice should not be able to change her mind about $p(b|\ not\ \perp)$. Analogously, let $unveil'$ be Alice's modified $unveil$ procedure, and define $p'(b|\ not\ \perp)$ accordingly. Thus, $p'(b|\ not\ \perp)$ is the probability that $unveil'$ returns b on $|\psi'\rangle$, given that it does not return $\perp$. The state $|\psi'\rangle$ is perfectly binding if every procedure $unveil'$ returns $\perp$ with probability one, or else returns b with probability $p'(b|\ not\ \perp) = p(b|\ not\ \perp)$. The state $|\psi'\rangle$ with a parameter n (for example, the number of the transmitted photons) is binding if with the increase of the parameter it can be made arbitrarily close to being perfectly binding.

In the following we want to explain what kind of security we expext from a quantum bit commitment protocol. We considered Alice to be dishonest above. Now, what if Alice is honest (otherwise, the encoding $b \mapsto |\psi_b\rangle$ would not make sense), but the encoding can be modified by a dishonest Bob. Let $\eta = (\xi_B, \xi_S)$ be the random classical information stored in $H_{E,B} \otimes H_S$ after the encoding. This classical information is available to Bob. Let $|\psi_{b,\eta}\rangle$ be the corresponding collapsed state of the system $H_A \otimes H_B \otimes H_{E,A}$. For given η, let $\rho_B(|\psi_{b,\eta}\rangle) = Tr_{H_A \otimes H_{E,A}}(|\psi_{b,\eta}\rangle\langle\psi_{b,\eta}|)$ denote the reduced density matrix of H_B. Next we need an expression for the accuracy of our encoding. For any given communication scheme, the fidelity is a quantitative measure of the accuracy of transmission, see Jozsa [Joz94]. Define $F(\eta)$ as follows: Set $F(\eta) = 0$ if η determines a single value of the bit b; otherwise, let $F(\eta)$ be the fidelity between $\rho_B(|\psi_{0,\eta}\rangle)$ and $\rho_B(|\psi_{1,\eta}\rangle)$, see Mayers [May97]. The value of the fidelity is always between 0 and 1. It is equal to 1 if and only if the two density matrices are identical.

We call the modified encoding *perfectly concealing* if the expected value of $F(\eta)$ is 1 and the random string η gives no information about the bit b. We can now define "concealing" the same way we defined "binding" above. Let us explain what kind of security we expect from a quantum bit commitment protocol. We call a protocol *perfectly secure* if

- the encoding is perfectly concealing, even if Bob is cheating, and
- if the state $|\psi\rangle$ returned by the $commit$ procedure is perfectly binding.

Analogously, define a protocol (with parameter n) to be *secure* if

- even for a dishonest Bob, the encoding is concealing, and
- even for a dishonest Alice , the encoding is binding.

It is widely believed that it is impossible to create a perfectly secure bit commitment protocol. In quantum cryptography, we want to design "only" secure protocols. Mayers has shown that unconditionally secure quantum bit commitment is impossible [May97]. A bit commitment protocol is unconditionally secure if any desired property holds even against a cheater with unlimited computational capacities, regarding technology, time, and space.

5.2 The BB84 Quantum Bit Commitment Protocol

If $b \mapsto |\psi_b\rangle$ is concealing and $|\psi_0\rangle$ and $|\psi_1\rangle$ bind Alice to 0 and 1, respectively, then we call the encoding a bit commitment encoding. The BB84 protocol was introduced in Section 4.1. We will create a bit commitment protocol from the BB84 quantum key distribution protocol with a few minor changes.

The commit procedure:

1. Alice creates a random binary string $w = w_1 \cdots w_n$.
2. Alice encodes each bit w_i by the rectilinear basis $\theta = +$ or the diagonal basis $\theta = \times$, if she wants to commit to 0 or to 1, respectively.
3. Alice sends the registers to Bob.
4. Bob chooses for each received register the basis to measure, so he has a string of random bases $\hat{\theta} = \hat{\theta}_1 \cdots \hat{\theta}_n \in \{+, \times\}^n$. He measures register i with basis $\hat{\theta}_i$, and denotes the outcome by w_i.

The unveil procedure:

1. Alice publishes the string w.
2. Bob can identify b by looking at the positions where $w_i \neq \hat{w}_i$. Bob knows that $\theta \neq \hat{\theta}_i$ must hold when $w_i \neq \hat{w}_i$. Thus he can determine θ and b at each of these positions. If two of these positions reveal different values for θ, Bob interprets this as an inconclusive result.

The protocol above is a bit commitment encoding, since it is concealing, and $b = 0$ and $b = 1$ correspond to the same density matrix on Bob's side. The commit procedure is also binding because if Alice wants to cheat, she has to guess the right bits obtained by Bob when $\widehat{\theta_i} \neq \theta$. As these bits are chosen at random, the probability of detecting that Alice is cheating increases with n.

There is a strategy Alice can use against the BB84 bit commitment protocol. In step two in the commit procedure, Alice creates for each random bit w_i the state

$$\frac{1}{\sqrt{2}}\left(|0\rangle_\theta^{(E,A)}|0\rangle_\theta^{(B)} + (|1\rangle_\theta^{(E,A)}|1\rangle_\theta^{(B)}\right). \tag{5.7}$$

If Alice is dishonest, she performs the commit procedure for $b = 0$, with the difference that she won't send any information to the environment. Thus, for each position i the state above is of the form

$$\frac{1}{\sqrt{2}}\left(|0\rangle_+^{(A)}|0\rangle_+^{(B)} + (|1\rangle_+^{(A)}|1\rangle_+^{(B)}\right). \tag{5.8}$$

The only difference between the two states (5.7) and (5.8) are the underlying systems. At this point, Alice can execute a unitary transformation on H_A, which transforms Alice's state into the state that she would have created at the beginning with $b = 1$:

$$\frac{1}{\sqrt{2}}\left(|0\rangle_\times^{(A)}|0\rangle_\times^{(B)} + (|1\rangle_\times^{(A)}|1\rangle_\times^{(B)}\right).$$

It seems that this transformation is the identity transformation, but in general the cheater has to launch a nontrivial transformation.

5.3 Unconditional Security of Quantum Bit Commitment

Unconditionally secure quantum bit commitment is impossible. However, a secure bit commitment protocol where the initial state is already the outcome of the encoding is easy to build [BCJL93]. There are no unconditional secure quantum bit commitment protocols, with initial quantum registers set to $|0\rangle$, without any entanglement of the environment.

We can act on the assumption that the protocol is secure against Bob, otherwise the protocol is not secure. Alice chooses in her modified $commit'$ procedure $b = 0$, and she does not send any register to the environment unless it is required for classical communication. Bob acts the same way in his $commit''$ procedure. So, the two systems $H_{E,A}$ and $H_{E,B}$ are not used in $commit'$ and $commit''$, respectively.

After the $commit'$ procedure, there is a random string γ stored in H_S. Let $|\psi'_{b,\gamma}\rangle$ be the corresponding collapsed state of the remaining system $H_A \otimes H_B \otimes H_{E,B}$. Mayers [May97] has shown that the expected value of $F'(\gamma)$ between the density matrices $\rho_B(|\psi'_{b,\gamma}\rangle)$ in the $commit'$ procedure is arbitrary close to 1.

We have two cases. First, $F'(\gamma) = 1$, so the density matrices are always identical. Second, $F'(\gamma) \neq 1$, but this is arbitrarily close to 1.

In the first case there exists a unitary transformation that maps $|\psi'_{0,\gamma}\rangle$ to $|\psi'_{1,\gamma}\rangle$. Thus, Alice can unveil the bit $b = 1$, so she can cheat if the two density matrices on Bob's side are identical.

Now, let $F'(\gamma) \neq 1$. If $\rho_B(|\psi_{01}\rangle) = \rho_B(|\psi'_{0,\gamma}\rangle)$, we call $|\psi_{01}\rangle$ the purification of the density matrix $\rho_B(|\psi'_{0,\gamma}\rangle)$. Uhlmann's Theorem (see Jozsa [Joz94]) says that there exists a purification $|\psi_{01}\rangle$ of $\rho_B(|\psi'_{0,\gamma}\rangle)$ with $\langle\psi_{01}|\psi'_{1,\gamma}\rangle \geq F'(\gamma)$. Therefore, Alice is able to transform $|\psi'_{0,\gamma}\rangle$ into $|\psi_{01}\rangle$ in her $unveil'$ procedure, just as in the case where the density matrices were identical. After this, she can continue with the honest $unveil$ procedure. From Uhlmann's Theorem it follows that Alice can change the bit b from 0 into 1 with probability arbitrarily close to one if the expected value of $F'(\gamma)$ is close to one, see Mayers [May95].

As we can see, a dishonest party uses the same algorithm in the $commit'$ and $commit''$ procedure as does an honest party in the $commit$ procedure. Thus, it is impossible for the honest party to detect the cheater in the $commit'$ and $commit''$ procedures.

Acknowledgments: The choice of Alice and Bob in Figure 2 was inspired by a talk by Dagmar Bruß at the University of D¨usseldorf in November, 2005.

References

[BB84] C. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, page 175. IEEE Press, 1984.

[BBB$^+$98] E. Biham, M. Boyer, G. Brassard, J. Graaf, and T. Mor. Security of quantum key distribution against all collective attacks. Technical Report quant-ph/9801022, Computing Research Repository (CoRR), 1998. Available on-line at http://arxiv.org/pdf/quant-ph/9801022.

[BBB$^+$99] E. Biham, M. Boyer, P. Boykin, T. Mo, and V. Roychowdhury. A proof of the security of quantum key distribution. Technical Report quant-ph/9912053, Computing Research Repository (CoRR), 1999. Available on-line at http://arxiv.org/pdf/quant-ph/9912053.

[BCJL93] G. Brassard, C. Crepeau, R. Jozsa, and D. Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In *Proceedings of the 34th IEEE Symposium on Foundations of Computer Science*, pages 362–371. IEEE Computer Society Press, 1993.

[Bra99] H. Brandt. Positive operator-valued measure in quantum information processing. *The American Journal of Physics*, 47:434–439, 1999.

[DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[ElG85] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, IT-31(4):469–472, 1985.

[Hoe63] W. Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, 1963.

[HR99] L. Hemaspaandra and J. Rothe. Creating strong, total, commutative, associative one-way functions from any one-way function in complexity theory. *Journal of Computer and System Sciences*, 58(3):648–659, June 1999.

[Joz94] R. Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics*, 41:2315–2323, 1994.

[May95] D. Mayers. The trouble with quantum bit commitment. Technical Report quant-ph/9603015v3, Computing Research Repository (CoRR), 1995. Available on-line at http://arxiv.org/pdf/quant-ph/9603015.

[May97] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78:3414–3417, 1997.

[Rot05] J. Rothe. *Complexity Theory and Cryptology. An Introduction to Cryptocomplexity*. EATCS Texts in Theoretical Computer Science. Springer-Verlag, Berlin, Heidelberg, New York, 2005.

[RS97] M. Rabi and A. Sherman. An observation on associative one-way functions in complexity theory. *Information Processing Letters*, 64(5):239–244, 1997.

[RSA78] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signature and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[Sch35] E. Schr¨odinger. Die gegenw¨artige Situation in der Quantenmechanik. *Die Naturwissenschaften*, 23:807–812, 823–828, 844–849, 1935.

[Sha49] C. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):657–715, 1949.

[Sho97] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[Sin99] S. Singh. *The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Fourth Estate, London, 1999.

[Sti02] D. Stinson. *Cryptography: Theory and Practice*. CRC Press, Boca Raton, second edition, 2002.

[Yao95] A. Yao. Security of quantum protocols against coherent measurements. In *Proceedings of the 27th ACM Symposium on Theory of Computing*, pages 67–75. ACM, New York, 1995.