

# The Relevance of Quantum Cryptography in Modern Cryptographic Systems

Christoph Guenther

# The Relevance of Quantum Cryptography in Modern Cryptographic Systems



Christoph Guenther
GSEC Practical Requirements (v1.4b)
Submitted: December 16, 2003

## Abstract

This paper explains the basic principles of quantum cryptography and how these principles apply to quantum key distribution. One specific quantum key distribution protocol called BB84 is described in detail and compared to traditional (non-quantum) cryptographic systems. It is explained how BB84 addresses some of the shortcomings of traditional cryptographic systems. The remaining technical limitations of BB84 are listed. A short overview of commercial implementations of quantum cryptography is given. The paper concludes with a brief discussion of the relevance and future viability of quantum cryptography in today's information security environment.

# 1 Introduction

Quantum cryptography has made a few (small) headlines last year [18,19,23,29,32,33,37,41]. This interest was fueled mainly by the introduction of two commercial products [16,27] that are based on a quantum key distribution protocol and the announcement of a Swiss partnership to develop a quantum key infrastructure [17]. Since quantum cryptography has made the leap from basic research to commercial product, it is time to take a closer look at this promising new security technology.
The purpose of this paper, therefore, is to gain a better understanding of quantum cryptography, in particular, its benefits and limitations. More specifically, this paper will

- introduce quantum cryptography in a non-technical way,
- compare it with traditional (non-quantum) cryptographic systems,
- list its current strengths and limitations, and
- provide an overview of current commercial efforts at implementing quantum cryptosystems.

At the end of this paper, I hope to provide the reader with a better understanding of the viability and relevance of quantum cryptography in today's information security environment.

The remainder of this paper is organized as follows: Section 2 will give a brief overview of traditional (non-quantum) cryptographic systems and its shortcomings; Section 3 will introduce the basic principles of quantum cryptography, describe what is known as the BB84 quantum key distribution protocol [3] in detail, and list the strengths and weaknesses of quantum cryptography; Section 4 will give a brief overview of commercial efforts at exploiting this technology; and in Section 5 I will list my conclusions.

# 2 Cryptography

In the last ten years, the Internet has enjoyed tremendous success connecting a large number of households and businesses with each other. This has created enormous economic possibilities. However, this economic potential can only be fully realized if the need for secure (i.e., safe against eavesdropping) transmission of data over the inherently insecure and open Internet can be satisfied. Cryptography addresses this need.
According to the Merriam-Webster Dictionary OnLine the term cryptography can mean "secret writing", "the enciphering and deciphering of messages in secret code or cipher", or "cryptanalisys" [30] (which in turn is defined as "the solving of cryptograms or cryptographic systems" or "the theory of solving cryptograms or cryptographic systems **:** the art of devising methods for this" [31].)

In the remainder of this paper I will be concerned with the last two aspects of cryptography. More specifically, I will describe different algorithms of enciphering and deciphering messages - also called ciphers - and the vulnerabilities of the various ciphers to cryptanalysis.
Throughout this paper, I will make continued use of the following standard scenario: Alice and Bob wish to exchange messages without eavesdropper Eve, who has complete access to the communication channel between Alice and Bob, being able to discern the content of these messages. This is called a secure exchange of messages.

## 2.1 The One-Time Pad

Suppose Alice wants to send a secure message to Bob. She can do so by first converting her message into binary code and then performing an exclusive-OR (XOR) between each bit of the message and a random binary key that is of the length of the message. Alice will then send this enciphered message to Bob and destroy the binary key. Assuming Bob is in possession of the same key that Alice used to encipher the message, he can perform another XOR operation on the enciphered message and recover the original message. Once Bob has deciphered the message he also destroys the key. Bob can send a secure reply to Alice using the same method with a *different* random key [12,38].
The cipher just described is completely safe to eavesdropping. Since each key is used only once, this cipher is an example of what is called a “one-time pad” [12,38].
The following requirements have to be satisfied for a one-time pad to be secure [12,38]:

1) Each key needs to be generated randomly.
2) Each key can be used only once.
3) Each key has to be at least of the length of the message to be enciphered.
4) Alice and Bob have to be in possession of the same key.

In reality, to satisfy all of these requirements is at least highly impractical, if not entirely impossible. This severely limits the use of the one-time pad.
To illustrate this point, consider what it would mean in practice to satisfy these requirements. According to the first requirement each key needs to be generated randomly. This precludes the use of pseudo-random number generators on today’s computers to generate the keys, since these algorithms are inherently deterministic and the computers that they run on are finite-state machines. The key generation would therefore need to be tied to some truly random process such as the decay of radioactive atoms. Just consider the number of daily transactions on the Internet that require a secure communication channel and it will be apparent that for most situations this is highly impractical.
The second and fourth requirements place an even greater limit on the usefulness of the one-time pad. Even if a set of keys could initially be exchanged securely between Alice and Bob, possibly in a face-to-face meeting, once that initial set has

been used up (due to the second requirement), a new set of keys would have to be exchanged. This can only be accomplished in a guaranteed secure manner by another face-to-face meeting between the two. This problem is called the key distribution problem [12]. It all but prohibits the use of the one-time pad for secure communications in practice. Again just consider the Internet, where, in general, the participants in a communication will never meet face-to-face.
Due to the impracticalities of the one-time pad, ciphers that are widely used today violate at least some of the requirements for the one-time pad. As with the one-time pad, the effectiveness of these ciphers rests in large part on the strength of their keys. That means that even though the underlying cryptographic algorithms for these ciphers are known publicly, to recover the key is considered computationally impractical. "Computationally impractical" here means that using known algorithms running on the most powerful computers it will take millions of years to calculate the correct key. It is worth noting that the security of these ciphers depends on the following:

1) They have withstood the test of time, i.e., although many of the brightest minds in the field of cryptography have tried, no one has as yet found (or rather published) and implemented an algorithm that will provide a shortcut to breaking the cipher.
2) Due to the continuous increase in computing power what is considered a secure cipher today might not be secure in tomorrow's computing environment.

In the next section I will briefly describe two types of cryptographic algorithms: symmetric encryption and asymmetric encryption. I will concentrate on those aspects of these algorithms that make them - at least in principle - vulnerable to attack. This will then provide the motivation for the introduction of quantum cryptography.
For completeness, it should be mentioned here that there is a third type of cryptographic algorithm: the one-way hash function. Since it does not necessarily require a key, like symmetric and asymmetric encryption algorithms, it is not relevant for the remainder of this paper and will not be further discussed. The interested reader is referred to [20,38] and references therein.

## 2.2 Types of Cryptographic Algorithms

The two types of cryptographic algorithms that I will briefly discuss in this section are: symmetric key encryption and asymmetric key encryption. Both schemes utilize trapdoor one-way functions [38] to encipher and decipher messages.
One-way functions are mathematical functions that are easy to compute in one direction but are (believed) to be very difficult to inverse. Here, the inverse of a function is considered difficult (easy) to calculate if the time it takes to accomplish this task grows exponentially (polynomially) with the size (often expressed as the number of bits) of the input [10,38].

Since one-way functions do not discriminate between friend and foe, the concept of a trapdoor has to be introduced. The same as with ordinary one-way functions, trapdoor one-way functions are also hard to inverse unless one is in possession of a (secret) key which facilitates the calculation of the inverse.
In symmetric and asymmetric key encryption the concept of trapdoor one-way functions is applied as follows: A key and a cleartext message are used as the input to a trapdoor one-way function to generate ciphertext. A key (not necessarily the same key as before) and the ciphertext are then used as input to the inverse of the trapdoor one-way function to recover the cleartext message.
The major difference between symmetric and asymmetric key encryption lies in the way the necessary keys are generated and distributed.

### 2.2.1 Symmetric Key Encryption

Symmetric key encryption uses the same cryptographic algorithm and the same key to encipher and decipher messages [20]. The key is chosen pseudo-randomly[1] from a subset of all possible key values[2].
As opposed to the one-time pad, symmetric key encryption uses the same key repeatedly to encipher and decipher messages. This makes it inherently less secure than the one-time pad since in its most straightforward implementation the same plaintext will result in the same ciphertext. Special care has to be taken to circumvent this problem (see Chapter 9 in [38] for more details).
Other problems with symmetric key encryption include [20] the secure generation of keys and, since the same key is used to encipher and decipher messages, the secure distribution of keys to both Alice and Bob.
Examples of commonly used symmetric key encryption algorithms are [20] Data Encryption Standard (DES), 3DES, Rivest Cipher (RC-4), and International Data Encryption Algorithm (IDEA). For details about these algorithms and many others, the interested reader is referred to [38].

### 2.2.2 Asymmetric Key Encryption

Asymmetric key encryption is also known as public key encryption. As the name implies, it requires two different but mathematically related keys, one to encipher a message and the other corresponding key to decipher the message. Since one of the keys is known publicly, it is called the public key. The other key has to be kept private with one or the other party to the secure communication. It is therefore referred to as the private key. The same or separate but complementary cryptographic algorithms are used to encipher and decipher messages,

[1] The term "pseudo-random" was used here to emphasize the fact that the keys are chosen using deterministic, finite-state computers which inherently are unable to produce truly random sequences [4].

[2] Some of the possible key values might not be very suitable for use in a secure cipher because they are considered too weak [4].

respectively [20]. The public/private key pairs are generated using one-way functions.
A very popular asymmetric key encryption algorithm is RSA [36]. For both, key generation and encryption of messages, it relies on the difficulty of factorizing a large integer (• 200 digits) into two prime numbers as opposed to the ease with which these same prime numbers can be multiplied [38].
A most basic secure exchange of messages between Alice and Bob using asymmetric key encryption will proceed as follows [20,38]:

1) Alice and Bob agree on a particular asymmetric key encryption method.
2) Both Alice and Bob generate their own, separate public/private key pairs.
3) Alice and Bob exchange their public keys.
4) Alice uses Bob's public key to encipher a message and sends it to Bob.
5) Bob uses his private key to decipher the message.
6) Bob enciphers a reply using Alice's public key.
7) Alice deciphers the reply using her private key.

The advantage of asymmetric key encryption is that it solves the key distribution problem that plagues symmetric key algorithms. No secret keys are ever exchanged - only public keys. However, the private keys are still vulnerable to compromise. Also asymmetric key encryption is too slow for many high bandwidth communications [20,38].
Besides RSA, other examples of commonly used asymmetric key encryption algorithms include [20,38] El Gamal and Rabin. For details about these and other asymmetric key encryption algorithms, the interested reader is referred to [38].

### 2.2.3 Hybrid cryptographic algorithms

Since asymmetric key encryption is often too slow for high-bandwidth communications, cryptographic systems combining both asymmetric key encryption and symmetric key encryption are often employed. They are called hybrid cryptosystems and use asymmetric key encryption to generate and distribute a session key that is then used for the remainder of the communication session in a symmetric key encryption [38].
A most basic secure exchange of messages between Alice and Bob under a hybrid cryptosystem proceeds as follows [38]:

1) Alice and Bob agree on the particular asymmetric and symmetric key encryption methods to be used.
2) Bob generates a public/private key pair and sends Alice the public key.
3) Alice generates a random session key and uses Bob's public key to encipher it in a message to Bob.
4) Bob recovers the session key with his private key.
5) For the remainder of the communication session, Alice and Bob use the session key with the symmetric key encryption method they initially agreed on.

Widely used algorithms for the initial session key exchange [20,38] are RSA (see Section 2.2.2) and the Diffie-Hellman key exchange algorithm [8]. The one-way function used in the latter is exponentiation in a finite field whose inverse, the discrete logarithm in the same field, is believed to be very difficult to calculate [38]. It should be noted here that the Diffie-Hellman algorithm can only be used for key exchange and not for message encryption [38] as opposed to RSA which can be used for both.

## 2.3 Shortcomings of Cryptographic Algorithms

The features of all of the cryptographic algorithms discussed in Section 2.2 can be summarized as follows:

1) They all employ at least one secret key.
2) The key is either chosen randomly from a suitably chosen set of possible values (as in DES and its variants) or generated using one-way functions (as in Diffie-Hellman and RSA).
3) The cleartext message and the key are used as input to a trapdoor one-way function to generate ciphertext. The ciphertext and a key (not necessarily the same but at least a mathematically related one) are used as input to calculate the inverse of the previously used trapdoor one-way function to recover the original message.
4) Both, the trapdoor one-way functions utilized in the various cryptographic algorithms to encipher and decipher messages as well as the one-way functions that are used to generate the keys are public knowledge and have undergone public scrutiny.

From this summary, it is clear that the security of a given cryptosystem rests on the secrecy of its (private) key and the difficulty with which the inverse of its one-way function(s) can be calculated. Recall that it is considered difficult to inverse a function if the time it takes to calculate the inverse depends exponentially on the size of the input. Unfortunately, there is no mathematical prove that will establish whether it is difficult to find the inverse of a given one-way function [10,38]. The fact that an efficient algorithm has not yet been found (or rather published) does not mean that such an algorithm does not exist.
As a case in point, consider RSA and the Diffie-Hellman key exchange. As mentioned earlier, the security of these cryptosystems is based on the factorization into prime numbers of large integers and the calculation of the discrete logarithm in a finite field, respectively. Both of these functions are believed to be mathematically difficult to calculate. However, this has never been proven mathematically. Furthermore, in 1994 Peter Shor discovered algorithms to be run on quantum computers that will factor a large integer and calculate the discrete logarithm, respectively, in polynomial time [39]. And, although the implementation of these algorithms has to wait for the transition of quantum computers from a mere concept to a physical reality, it still casts doubts on the non-existence of

polynomial algorithms on classical computers that will efficiently calculate the inverse of the one-way functions that are most widely used in today's cryptosystems [10].
The shortcomings of today's most commonly used cryptographic systems are as follows:

1) The security of a one-way function against implementation of more efficient (but as yet unpublished) algorithms for calculating its inverse has not been proven.
2) All one-way functions are (at least in principle) vulnerable to an increase in computing power which makes brute-force attacks more feasible.
3) The security of the key during key generation cannot be absolutely guaranteed.
   This is true regardless of whether the key is chosen at random from a suitable chosen set of possible values or generated using a one-way function.
   If the key is chosen randomly the randomness of that choice has to be guaranteed. Using today's deterministic, finite state computers, this can, in principle, only be achieved approximately [38].
   If the key is generated using a one-way function, it is vulnerable to compromise by either item 1 or item 2 in this list.
4) The security of the key during key distribution cannot be absolutely guaranteed.
   As mentioned in Section 2.2.3, in today's cryptographic systems, the key distribution problem is solved using one-way functions which are vulnerable to compromise by item 1 or item 2 in this list.
5) The security of the key during key storage cannot be absolutely guaranteed.
6) Once a cipher has been compromised, there is no apparent method by which the participants in the secure communication can determine that a breach has occurred [24].

Some of these shortcomings can be overcome by using Quantum Cryptography which will be discussed in the next section.

# 3 Quantum Cryptography

Quantum cryptography was first proposed in 1970 by Wiesner in a paper that remained unpublished until 1983 [43] and by Bennett and Brassard in 1984 [3,4]. It constitutes the first application of the field of quantum information theory which itself is founded on the fundamental axioms of quantum physics.
More specifically, quantum cryptography provides a secure protocol to exchange cryptographic keys. This protocol is called quantum key distribution or quantum key exchange.

## 3.1 Quantum Key Distribution Part 1: The Basics

Quantum key distribution rests on two principles [10]. The first principle is itself one of the fundamental principles in quantum mechanics. The second principle is purely classical in nature.

First principle of quantum cryptography: [10,24]

> *Every measurement of the unknown state of a quantum system irreversibly perturbs the original state of the system, except if the system was prepared in a state that is compatible with the measurement.*

To illustrate how this principle is used to secure a communication channel, imagine Alice and Bob are communicating using a quantum system. Such a communication channel could, e.g., consist of an optical fiber that allows for the transmission of individual photons between Alice and Bob. In order for Alice to transmit a message to Bob, she prepares the quantum system in a certain state which represents the contents of Alice's message. Alice then sends that quantum system to Bob. In order for eavesdropper Eve to discern the information contained in Alice's message, she needs to find out what the state of the quantum system is that is being transmitted from Alice to Bob. The only way for her to accomplish that is by performing a measurement on the quantum system which according to the first principle will perturb the state of that system and thereby alter the message itself. Once Bob receives the message, Alice and Bob need to ascertain whether it had been perturbed by Eve or not. They can achieve that by comparing a randomly chosen subset of the information contained in the message over a regular, i.e. non-quantum, public communication channel.
The drawback of the quantum cryptosystem described above is that Alice and Bob find out whether a security breach has occurred only after the message has already been exchanged. In order to avoid this problem, the second (purely classical) principle of quantum cryptography is invoked.

Second principle of quantum cryptography: [10]

> *Before exchanging real information through a communication link, use quantum cryptography to only exchange random keys.*

This random key could, e.g., consist of a random sequence of bits. That way, if Alice and Bob find that the key has been perturbed in transit they discard it. Alice then retransmits another random key until no perturbation is found.
The tactic Eve employs in the scenario described above is to read a message (by measuring the state of the quantum system that Alice is sending to Bob) while it is being transmitted. This violates the first principle of quantum cryptography and can therefore not go undetected.
However, what if Eve did not try to read the message right away but instead just made a copy of it? She could then read the copy later; after the original was received by Bob and after Alice and Bob convinced themselves that no

perturbation occurred during transmission of the original message. As it turns out, however, there is a corollary to the first principle of quantum cryptography, called the no-cloning theorem, which prevents Eve from being successful in this scenario. Specifically, the no cloning theorem states that an unknown quantum state cannot be copied or cloned [24].
Finally, one needs to ensure that Eve does not impersonate Bob (or Alice) in the classical communication that is used to decide whether the previously exchanged key was perturbed during transmission or not. This can be done using classical authentication schemes (that, if necessary, can be information-theoretically secure [24,42]) to convince Alice (Bob) of the authenticity of the other party in the communication.

## 3.2 Quantum Key Distribution Part 2: Implementations

A number of quantum key distribution protocols have been proposed. I will only describe one protocol first introduced in 1984 by Bennett and Brassard [3] called BB84. The motivation for concentrating on BB84 is twofold:

1) It is the oldest quantum key distribution protocol and has been proven to be secure under a large number of circumstances [6,10,13,21,25,28,40].
2) To my knowledge, BB84 is the only quantum key distribution protocol that has been used successfully to launch commercial implementations of quantum key distribution [15,26].

The BB84 quantum key distribution protocol uses photons as quantum systems. In order to understand this protocol, we need to first illustrate what it means for a photon to be a quantum system. The following discussion will closely follow [11].

### 3.2.1 The Photon as a Quantum System

Photons have an intrinsic property called polarization. A photon can either be polarized perpendicular or circular to its direction of motion. Here we consider photons that are only polarized in the perpendicular direction.
Suppose we prepare a stream of photons that are vertically polarized by sending them through a vertical polarization filter. Further suppose that we want to subsequently measure the polarization of the photons by sending them through a second polarization filter. This “measurement filter” differs from the first filter in that it allows us to control its angle of orientation with respect to the vertical direction. If we were not aware of quantum physics, we would expect that only when the measurement filter is in the vertical position will the photons pass through it. What we actually find however, is that only when the measurement filter is in the horizontal position will the photons not pass through it. For all its other orientations we will actually find photons behind it.
In fact, quantum physics states that for each photon in the stream there is a certain probability p that it will pass through the measurement filter. This probability p depends on the orientation of the measurement filter and varies continuously from 1, when the filter is in the vertical position, through ½, when the filter is at a 45° angle, to 0, when the filter is in the horizontal position.

Furthermore, according to quantum physics, all one can say about the measurement of the polarization of the photon is that it was in a vertically polarized state with probability p and in a horizontally polarized state with probability 1-p before it entered the measurement filter. That means that unless the measurement filter happens to be in the vertical or horizontal position, the polarization of the photons before they entered the measurement filter is always uncertain. This uncertainty is largest when the angle of orientation of the measurement filter is 45°.
Quantum physics actually goes beyond what we have stated so far. Not only is it generally impossible to gain any precise information about the polarization state of a photon. But, once the polarization of a photon is measured, its polarization is irreversibly altered. Therefore, had we not known the exact polarization of the photon before it was measured, a measurement, will, in general, not reveal that exact polarization either. This is just the first principle of quantum cryptography introduced in Section 3.1 applied to the polarization of photons.

### 3.2.2 The BB84 Quantum Key Distribution Protocol

In this section we will use the following notation:

- "|" denotes a photon in a vertically polarized state.
- "• " denotes a photon in a horizontally polarized state.
- "/" denotes a photon in a 45° polarized state.
- "\" denotes a photon in a 135° polarized state.
- "+" denotes the pair of states {|, • }, also called the +-basis.
- "x" denotes the pair of states {\, /}, also called the x-basis

Let us further assume that Alice and Bob have agreed to associate the binary digit 1 with the states | and \, respectively, and the binary digit 0 with the states • and /, respectively.
As explained in Section 3.1, any quantum key distribution protocol requires two communication channels: a quantum communication channel which transmits the photons, such as a standard fiber-optic cable, and a classical communication channel, such as a phone line, e-mail, etc. Here, the classical communication channel is used to ascertain whether confidentiality on the quantum channel has been breached (see Section 3.1) and to facilitate error correction and privacy amplification (see below).
It is assumed that Eve has unlimited computing power and complete access to both communication links, except that she cannot impersonate either Alice or Bob on the classical communication channel (see Section 3.1).
With this setup in place, the BB84 quantum key distribution protocol proceeds through the following steps [24]:

1) Alice sends a stream of individual photons in one of the four polarization states |, • , /, or \ to Bob. Alice picks each photon's polarization state randomly and independently.
2) For each photon, Bob randomly chooses either the +-basis or the x-basis and measures the polarization of the photon in that basis.

3) For each photon, Bob records the basis he used and the result of the polarization measurement.
4) Through the classical communication channel, Bob communicates to Alice for each photon his choice of basis, but not the result of his polarization measurement.
5) Still through the classical communication channel, Alice tells Bob which photon was measured in the correct basis.
6) Both, Alice and Bob, discard the polarization data that correspond to those photons that were not measured in the correct basis.
7) Both, Alice and Bob, translate the valid polarization data into a string of bits according to the association of polarization states with the binary digits 0 and 1 that they agreed to earlier. This way Bob and Alice arrive at what is called the sifted key [9]. Note that neither Alice nor Bob actually picked a key before their communication took place. Rather, the key is the result of the combined random choices that Alice and Bob make during the course of their communication.
   Since Bob's chance of picking the correct basis is about 50%, the length of the sifted key is about ½ of the total number of photons that Alice sent to Bob.

The following table provides an illustration of the BB84 protocol in use [11,24].

| Alice sends to Bob: | / | • | • | \| | \ | • | \ | / | \| | / | \| | \| |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bob measures with: | + | + | X | + | X | X | + | + | + | X | + | X |
| Bob's results: | • | • | \ | \| | \ | / | \| | \| | \| | / | \| | \ |
| Valid data: | | • | | \| | \ | | | | \| | / | \| | |
| Sifted key: | | 0 | | 1 | 1 | | | | 1 | 0 | 1 | |

### 3.2.3 BB84 in the Presence of Noise and Eavesdropping: Reconciliation and Privacy Amplification

So far I have assumed that there is no eavesdropping or noise on the communication channels between Alice and Bob. In that case, Alice's and Bob's sifted keys will exactly match. However, in practice, to make these assumptions is unrealistic. In fact, one of the reasons for using a quantum key distribution protocol in the first place is to be able to tell if the security of the communications link between Alice and Bob has been breached. In this sub-section I will therefore deal with the effects that eavesdropping and noisy communication channels might have. I will also sketch a procedure consisting of what is called reconciliation (or error correction) and privacy amplification that one can apply to mitigate to arbitrarily low levels the effects of eavesdropping and noise. This procedure is purely classical [10]. It was first introduced in 1992 by Bennet *et al*. [5]. My discussion of the subject follows [10,11,24].
First consider the presence of an eavesdropper Eve in the absence of any noise. Any realistic eavesdropping by Eve will consist of some kind of intercept-resend strategy [10], whereby Eve intercepts the photons Alice is sending to Bob and then

either makes a copy of them or measures the polarization of these photons directly before sending them on to Bob.
Assuming that Alice chose the polarizations of the photons completely at random, Eve will not have any more knowledge about their polarization state than Bob. According to the no-cloning theorem introduced in Section 3.1 above, this lack of knowledge about the state of each photon will prevent Eve from making an exact copy of all the photons that Alice is sending to Bob. All Eve can do is (like Bob) to pick a basis for each photon, measure the photon polarization in that basis, and send the photon on to Bob. Like Bob, Eve has a 50% chance of picking the correct basis in which case Eve's intrusion goes undetected by Alice and Bob. In the remaining 50% of the photons however, Eve picks the wrong basis thereby changing the polarization of these photons irreversibly through her measurement. That means that approximately 50% of the photon that will eventually constitute the sifted key will have the wrong polarization. When Bob performs a measurement on these 50% of photons with the wrong polarization, he will have a 50% chance of finding the same polarization as before and a 50% chance of finding a different polarization. In total therefore, about 25% of the bits in Alice's and Bob's sifted key will be different.
Bob and Alice can find out about this difference by comparing the bits in a randomly chosen (but for Alice and Bob identical) subset of their respective sifted key over the classical communication channel. If about 25% of the bits are different, Alice and Bob discard the sifted key completely and start over. If the difference is smaller than 25%, Alice and Bob only discard the bits that they shared over the classical communication channel which leaves them with a smaller key.
So far we have assumed that Eve intercepts and resends every photon that Alice sent. However, Eve might decide to eavesdrop only on a subset of photons. This will result in a difference between Alice's and Bob's key that can be considerably smaller than 25%.
Up until now, we have completely ignored the effect noise can have on the key exchange. Noise can be caused by technical imperfections of the equipment that implements the communication link, such as the photon transmitter and receiver, the photon polarizers and analyzers, or the actual physical medium that constitutes the communication link. The total effect of noise is to randomly change Bob's polarization data for some of the photons. That will introduce additional differences between Alice's and Bob's key. For Alice and Bob the effects of noise are indistinguishable from the effects of Eve's interference.
In summary, Alice's and Bob's key will be different due to the combined effects of Eve's tampering and noise. In order for a key to be useful in a transmission of enciphered messages, however, Alice and Bob have to be in possession of exactly identical keys. By adopting a strategy called reconciliation or error correction, over the classical communication channel, Alice and Bob can reduce the difference in their keys to an arbitrarily small level.
A simple scheme for reconciliation proceeds through the following steps [5,24]:

1) Alice and Bob agree on a random permutation of the bit positions in their respective keys.

2) They then partition their key into blocks of k bits each. The size k of the blocks is chosen in such a way that each of the blocks, on average, just contains one difference, also called an error.
3) Alice and Bob then calculate and compare the parity for each block. (The parity of a block is defined as the sum modulo 2 over the bits in the block.)
    - If the parity agrees the block will contain no errors or an even number of errors. Since it is expected that the probability that the block will contain more than one error is small, the block is tentatively accepted, but only after one of its bits (e.g., the last one) is discarded. The last step is performed in order to minimize the information Eve can obtain on the final key from this reconciliation procedure.
    - If the parity does not agree at least one error is present in the block. In order to find the error, a binary search is performed, using parity as a guide to finally locate and correct the error. In each step of this binary search one of the bits of the sub-blocks for which the parity was compared is discarded. This is done in order to minimize the information about the final key that Eve can gain.
4) Since this procedure will not take care of the case when there are two errors in one block, steps 1) through 3) are repeated several times. In every iteration, a larger block size is chosen, such that on average there is only one error in each block.
5) At some point the number of errors will fall below a threshold for which the procedure described thus far will become inefficient. In that case Alice and Bob agree on a randomly chosen subset of bits from their respective key. Again computing and comparing the parity on the subset will reveal whether it contains an error or not.
    - If the parity agrees there are either zero errors or an even number of errors in the subset. In this case, the subset is tentatively accepted after one of its bits has been discarded.
    - If the parity does not agree at least one error is present in the subset. It is corrected using the same binary search method described in step 3).
6) Once the error is corrected or if no error is found, another random subset is chosen and step 5) is repeated.
7) The procedure terminates when no new errors are found in a large number (• 20) of consecutive iterations of step 5) [24].

After reconciliation Alice and Bob very likely will share identical copies of the same key. However, in general, Eve will still have some information about that key. Eve could have obtained that information, for example, from those photons whose polarization she - by chance - measured in the correct basis.
In order to reduce Eve's information of the shared key to arbitrarily low levels another entirely classical procedure called privacy amplification is applied [5,10,11,24].

A very basic privacy amplification procedure works as follows [10]. Alice and Bob agree on a pair of randomly chosen bits. They then replace this pair of bits with one bit whose value is equal to the XOR value of the pair. Without introducing new errors into the key, this procedure will lead to a smaller key that Eve knows less about than the original key. (Just consider the case in which Eve knows the value of only one of the bits in the pair which gives her no information about the XOR value of the pair.) With every iteration of this procedure the information Eve has about the resulting key becomes smaller and smaller until it has fallen to for Alice and Bob acceptable levels. (For more efficient algorithms than the one described here, see, e.g., [7].)

## 3.3 Advantages of Quantum Cryptography over Traditional Cryptography

In Section 3.2 I have introduced a quantum key distribution protocol that is proven to be secure under a wide variety of circumstances [6,10,13,21,25,28,40]. If one combines this quantum key distribution protocol with the one-time pad as described in Section 2.1[1], one obtains a cryptographic system that is, in principle, unbreakable. Some caution is still in order here (hence my use of the qualifying "in principle"), since certain limitations arising from technical implementations of this protocol have to still be overcome. I will mention some of these limitations in the next Section.

However, as opposed to the fundamental mathematical problems that one is faced with in traditional cryptographic protocols, it is my opinion, that the limitations arising from the implementation of quantum cryptographic protocols are of a "mere" technical nature and can be overcome with time.

In the remainder of this section, I will run through the list of shortcomings of traditional cryptographic systems that was presented in Section 2.3 and describe how each one is addressed in a quantum cryptographic system such as the QKD one-time pad.

Items 1 and 2 in the list of shortcomings of traditional cryptosystems (see Section 2.3) deal with fundamental vulnerabilities of mathematical one-way functions. However, those one-way functions are not used in a QKD one-time pad. Items 1 and 2 are therefore not an issue in the QKD one-time pad.

However, so far, quantum cryptography cannot be used in practice to encipher and decipher messages but only to generate and distribute a cryptographic key securely. Therefore, if one combines a quantum key distribution system with a traditional cryptographic algorithm that uses the quantum cryptographic key and a trapdoor one-way function to encipher and decipher messages, then items 1 and 2 remain an issue. One can, however, mitigate this risk by changing the quantum cryptographic key frequently.

[1] In the following I will call such a cryptographic system a "QKD one-time pad".

Since key generation and distribution are inextricably linked in quantum key distribution protocols items 3 and 4 in the list of shortcomings of traditional cryptosystems have to be addressed together. Both of them are not an issue provided that

1) Alice chooses the polarizations of the photons in a truly random fashion. If she uses pseudo-random number generators, this might not be guaranteed. However, there are implementations of the quantum key distribution protocol that use truly random physical processes for this task [16].
2) The classical communication channel between Alice and Bob can be secured against impersonation by Eve of either Alice or Bob. This can be achieved since information-theoretically secure authentication schemes exist [24,42].

Item 5 in the list of shortcomings of traditional cryptosystems is still an issue if one uses a key generated and distributed by a quantum key distribution protocol to encipher and decipher messages more than once.
Item 6 in the list of shortcomings of traditional cryptosystems is not an issue since eavesdropping can be detected and controlled in quantum key distribution protocols.

## 3.4 Limitations of Quantum Cryptography

A number of technical challenges still remain in quantum cryptography. The following discussion will be brief and follow [10,24]. For a more detailed discussion the interested reader is referred to [24].

1) Photon sources
   The security of the BB84 quantum key protocol depends on Alice's and Bob's ability to generate and process single photons. To illustrate this point, imagine Alice sent two photons in the same polarization state at the same time. It would then be possible for Eve to use a beam splitter to extract and analyze one of the photons while the other travels on to Bob. Such an eavesdropping strategy would go undetected.
   To generate single photons, however, turns out to be difficult to accomplish. Today's implementations therefore rely on faint laser pulses for which the probability of sending two photons at the same time is known and small. Since this probability is known one can account for the amount of eavesdropping that can occur due to this effect and correct for it during the privacy amplification stage of the quantum key distribution protocol.
2) Random number generators
   In order to minimize the amount of information Eve can gain about the key in a quantum key distribution protocol, Alice has to choose the polarization states of the photons she sends completely at random. If Alice uses a computer to generate random numbers, complete randomness cannot be achieved due to the deterministic nature of finite-state computers.

However, there are implementations of the quantum key distribution protocol that use truly random physical processes for this task [16].

3) Quantum repeaters
   Due to detector noise and fiber loss, the range of current quantum key distribution systems is limited to 40-60miles [10,15,26]. Traditional repeaters to increase this range cannot be used because they would perturb the polarization state of the photons in much the same way eavesdropper Eve does.
   Several technologies still under development, such as long distance free space quantum key distribution [14,22] which could lead to quantum key distribution via low-orbit satellites [10,14,35], or quantum key distribution protocols using quantum entanglement [10], might eventually solve this problem.
4) Low transmission rate
   Here the transmission rate is defined as the number of corrected secret bits (i.e., after reconciliation and privacy amplification has been applied) that can be transmitted per second. Transmission rates on the order of Gigahertz that are common with today's fiber-optic communication systems are not attainable with current quantum key distribution technology [10]. This limits the use of a QKD one-time pad to all but the most confidential transmissions.
   However, if one combines a quantum key distribution protocol with frequent key changes and a symmetric key encryption cipher, such as 3DES or AES, one can still greatly enhance the security of traditional cryptographic protocols [10].
5) Security
   Despite the fact that quantum key distribution protocols have successfully been proven to be secure, in general, a particular technical implementation will always be suspect [10]. However, a security breach caused by a flaw in a particular technical implementation is much easier to deal with than a security breach due to the breakdown of an unproven mathematical assumption. The latter is what one potentially faces with traditional cryptographic protocols.

# 4 Commercial Implementations of Quantum Cryptography

During the past year two commercial products implementing the BB84 quantum key distribution protocol have been launched [15,26].
One of the products is providing a VPN gateway claiming a 70mile transmission distance through standard fiber-optic cable with a key refresh rate of up to 100 new keys per second [27].
The other product is providing a point-to-point quantum key distribution hardware system. It claims a 40mile key distribution distance over standard optical fiber with

a key distribution rate of up to 1Mbit/s [16]. However, the key distribution performance degrades over long distances, being only 100bits/s for distances of 50km. This device also offers a random number generator that is based on a random physical process.
Commercial efforts are also under way to develop a quantum key distribution network infrastructure. Companies that are active in this arena include BBN Technologies [1] and a Swiss partnership formed between Wisekey SA [44], OISTE [34], and idQuantique [15].
More specifically, BBN Technologies is working on prototype components and a network architecture that can be used in a fiber-optic based quantum key distribution network [2]. The goal is to overcome the current 60 mile range limit on quantum key distribution networks and to make the quantum key distribution network completely compatible with the Internet.
The Swiss partnership between Wisekey, OISTE, and idQuantique is developing a quantum key infrastructure based on the OISTE root and idQuantique's commercially available quantum key distribution hardware appliance [17].
Another technology that seems poised to make the leap from basic research to commercial product development is free-space quantum cryptography [14,22]. Great strides have been made in recent years to extend the range of this technology. It has the potential to be soon put to use in a ground to low-orbit satellite quantum key distribution infrastructure [35] which itself could be incorporated into the quantum key distribution infrastructure currently under commercial development by BBN technologies and the Wisekey/idQuantique/OISTE partnership.

# 5 Conclusions

What is the relevance of quantum cryptography in today's information security environment?
It is my belief that the only thing that might stand in the way of an eventual widespread adoption of quantum cryptography is its apparent strength. Since, if properly implemented, it is inherently unbreakable, governmental security agencies might want to restrict its use.
Barring governmental intervention, it is my opinion that quantum cryptography is here to stay. There is no doubt that there are still quite difficult technical problems to overcome, such as its limited range and low transmission rate, before it will find widespread use in today's network infrastructure. However, the technology has developed to a point where its deployment in environments that require the highest level of security, e.g., in certain governmental agencies or in financial institutions, is possible with commercially available, of-the-shelf products. This should fuel more interest in this technology providing an even greater impetus to find solutions to its remaining limitations.

## References


[1] BBN Technologies, Camebridge, MA. Website at http://bbn.com. ( 15 December 2003).

[2] "Quantum Cryptography". BBN Technologies. 2003. URL: http://www.bbn.com/networking/quantumcryptography.html. (15 December 2003).

[3] Bennett, C. H. and G. Brassard. "Quantum cryptography: public key distribution and coin tossing" Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (1984), Bangalore, India, 175-179.

[4] Bennett, C. H. and G. Brassard. "Quantum Public Key Distribution System" IBM Technical Disclosure Bulletin **28** (1985): 3153-3163.

[5] Bennett, C. H., F. Bessette, F. Brassard, L. Salvail, and J. Smolin. "Experimental Quantum Cryptography" Journal of Cryptology **5** no. 1 (1992): 3-28.

[6] Biham, E., *et al.* "A Proof of the Security of Quantum Key Distribution" in Proceedings of the 32nd Annual ACM Symposium on the Theory of Computing. New York: ACM Press, 2000. 715. URL: http://arxiv.org/PS_cache/quant-ph/pdf/9912/9912053.pdf. (10 December 2003).

[7] Brassard, G. and L. Salvail. "Secrete-key reconciliation by public discussion" Advances in Cryptology - EUROCRYPT '93. T. Helleseth (editor), Lecture Notes in Computer Science **765**, Springer-Verlag 1994. 410--423

[8] Diffie, W. and M.E. Hellman. "New Directions in Cryptography" IEEE Transactions on Information Theory **IT-22** no. 6 (1976): 644-654.

[9] Ekert, A. K. and B. Huttner. "Eavesdropping Techniques in Quantum Cryptosystems" J. Modern Optics **41** (1994): 2455-2466.

[10] Gisin, N., G. Ribordy, W. Tittel and H. Zbinden. "Quantum Cryptography" Reviews of Modern Physics **74** (2002):145. URL: http://arxiv.org/PS_cache/quant-ph/pdf/0101/0101098.pdf. (13 December 2003)

[11] Goldwater, S. "Quantum Cryptography and Privacy Amplification". 10 December 1996.

URL: http://www.ai.sri.com/~goldwate/quantum.html.
(13 December 2003).

[12] Gottesman, D. and H.-K. Lo. "From Quantum Cheating to Quantum Security" Physics Today **53** no. 11 (2000): 22-27.
URL: http://arxiv.org/PS_cache/quant-ph/pdf/0111/0111100.pdf
(4 December 2003).

[13] Gottesman, D., H.-K. Lo, N. Luetkenhaus, and J. Preskill. "Security of quantum key distribution with imperfect devices". (2002)
URL: http://arxiv.org/PS_cache/quant-ph/pdf/0212/0212066.pdf.
(12 December 2003).

[14] Hughes, R.J., J. E. Nordholt, D. Derkacs and C. G. Peterson. (2002) "Practical free-space quantum key distribution over 10 km in daylight and at night" New Journal of Physics **4** (2002): 43.1-43.14.
URL: http://arxiv.org/ftp/quant-ph/papers/0206/0206092.pdf. (15 December 2003)

[15] idQuantique SA, Geneva, Switzerland. Website at http://www.idquantique.com/qkd.html. (13 December 2003).

[16] "Quantum Security… At Last". idQuantique SA. 2003.
URL: http://www.idquantique.com/files/spec-qkd.pdf. (14 December 2003).

[17] "Breakthrough in Quantum Cryptography – Swiss partnership to release world's first integrated Quantum Key Infrastructure". idQuantique SA, Wisekey SA. 2003.
URL: http://www.idquantique.com/files/wise-press-engl.pdf. (15 December 2003).

[18] Johnson, R. Colin. "Hackers beware: quantum encryption is coming" EETimes. 12 November 2002.
URL: http://www.eet.com/story/OEG20021111S0036. (15 December 2003).

[19] Johnson, R. Colin. "Quantum Is Key To New Security Alliance". Security Pipeline. 20 October 2003.
URL:
http://www.securitypipeline.com/news/showArticle.jhtml;jsessionid=2J0O3IXQL4MR0QSNDBCSKHY?articleId=15500200&printableArticle=true.
(15 December 2003).

[20] Kaeo, M. Designing Network Security. Indianapolis: Cisco Press, 1999. Chapter 1.

[21] Koashi, M. and J. Preskill. "Secure quantum key distribution with an uncharacterized source". Phys. Rev. Lett. **90** (2003): 057902.
URL: http://arxiv.org/PS_cache/quant-ph/pdf/0208/0208155.pdf.

(12 December 2003).

[22] Kurtsiefer, C., P. Zardaa, M. Haldera, P.M. Gorman, P.R. Tapster, J.G. Rarity and H. Weinfurter. "Long Distance Free Space Quantum Cryptography". URL: http://scotty.quantum.physik.uni-muenchen.de/publ/42106762.pdf. (15 December 2003)

[23] LaMonica, Martin. "Cryptography - A quantum leap over short distances". RedHerring. 13 January 2003.
URL:
http://www.redherring.com/Article.aspx?f=Articles/Archive/insider/2003/01/quantum011303.xml&hed=Cryptography. (15 December 2003).

[24] Lo, H.-K. "Quantum Cryptology" Hewlett Packard Technical Report. 1997. URL: http://fg.hpl.external.hp.com/techreports/97/HPL-97-151.pdf. (13 December 2003)
Appeared as Chapter 4 of H.-K. Lo, S. Popescu and T. Spiller (editors) Introduction to Quantum Computation and Information. World Scientific Press, 1998.

[25] Lo, H.-K. and H. F. Chau. "Unconditional security of quantum key distribution over arbitrarily long distances" Science **283** (1999): 2050–2056.
URL: http://arxiv.org/PS_cache/quant-ph/pdf/9803/9803006.pdf.
(13 December 2003).

[26] MagiQ Technologies, Inc., New York, NY. Website at http://www.magiqtech.com. (13 December 2003).

[27] "Navajo Security Gateway – Uncompromising VPN Security". MagiQ Technologies, Inc. 2003
URL: http://www.magiqtech.com/press/navajo.pdf. (13 December 2003).

[28] Mayers, D. "Quantum key distribution and string oblivious transfer in noisy channels" in N. Koblitz (editor) Advances in Cryptology – Proceedings of Crypto '96. New York: Springer Verlag, 1996. 343.

[29] McCullagh, Declan. "Start-up makes quantum leap into cryptography" CNet News.com. 6 November 2003.
URL: http://news.com.com/2100-1029-5103373.html. (15 December 2003).

[30] Merriam-Webster Dictionary OnLine.

URL: http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=cryptography. (4 December 2003).

[31] Merriam-Webster Dictionary OnLine.
URL: http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=cryptanalysis (4 December 2003).

[32] Metz, Cade. "Special Report: Quantum Cryptography Arrives" PC Magazine. 6 August 2002.
URL: http://www.pcmag.com/article2/0,4149,440474,00.asp.
(15 December 2003).

[33] "Encoding takes a quantum leap". Miami Herald. November 17, 2003.

[34] OISTE Foundation, Geneva, Switzerland. Website at http://www.iseto.ch/master.htm. (15 December 2003).

[35] Rarity, J. G., P. R. Tapster, P. M. Gorman and P. Knight. "Ground to satellite secure key exchange using quantum cryptography". New Journal of Physics **4** (2002): 82.1–82.21.
URL: http://ej.iop.org/links/q20/zjwnFUkQowfSgDBqQY6sLQ/nj2182.pdf.
(15 December 2003).

[36] Rivest, R.L., A. Shamir and L.M. Adleman. "A Method of Obtaining Digital Signatures and Public-Key Cryptosystems" Communications of the ACM **21** no. 2 (1978): 120-126.

[37] Salkever, Alex. "A quantum leap in cryptography" BusinessWeek Online. 15 July 2003.
URL:
http://www.businessweek.com/technology/content/jul2003/tc20030715_5818_tc047.htm. (15 December 2003).

[38] Schneier, B. Applied Cryptography Second Edition. New York: John Wiley & Sons, 1996.

[39] Shor, P. W. "Algorithms for quantum computation: discrete logarithms and factoring". S. Goldwasser (editor). Proceedings of the 35th Symposium on Foundations of Computer Science, Los Alamos: IEEE Computer Society Press, 1994. 124-134.
Online version: Shor, P. W. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". SIAM Journal on Computing **26** no. 5 (1997): 1484-1509.
URL: http://arxiv.org/PS_cache/quant-ph/pdf/9508/9508027.pdf
(10 December 2003).

[40] Shor, P. W. and J. Preskill. "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol". Phys. Rev. Lett. **85** (2000): 441—444. URL: http://arxiv.org/PS_cache/quant-ph/pdf/0003/0003004.pdf. (13 December 2003).

[41] "Uncrackable beams of light". The Economist. 4 September 2003. URL: http://www.magiqtech.com/press/Economist_Uncrackable_Beams_Of_Light.pdf. (15 December 2003).

[42] Wegman, M. N. and J. L. Carter. "New Hash Functions and Their Use in Authentication and Set Equality" Journal of Computer and System Sciences **22** no. 3 (1981): 265-279.

[43] Wiesner, S. (1983) SIGACT News **15** no. 1 (1983): 78; original manuscript written *circa* 1970.

[44] Wisekey SA, Geneva, Switzerland. Website at http://wisekey.com/pages/home.htm. (15 December 2003).