Technical Report No. 2006–516
Quantum Key Distribution Revisited

Marius Nagy and Selim G. Akl
School of Computing
Queen's University
Kingston, Ontario K7L 3N6
Canada
Email: {marius,akl}@cs.queensu.ca

Abstract

We propose a new approach to quantum key distribution under the assumption that the qubits received during the execution of a protocol can be stored for a pre-determined amount of time. This assumption, motivated by the ongoing research towards designing a quantum network, allows for the elaboration of conceptually new quantum key distribution schemes. The data dependencies brought about by the Quantum Fourier Transform can be harnessed to design novel protocols with improved performance. Such a protocol maximizes an eavesdropper's uncertainty over the information transmitted, while amplifying the disturbance caused by the act of eavesdropping, thus offering better chances of detecting the intrusion.

1 Introduction

Two of the most important problems in cryptography are concerned with the *security* and *authenticity* of exchanged messages. There are perfectly good ways to achieve these two goals, provided the two parties (generically referred to as Alice and Bob) wishing to communicate over an insecure (public) channel share a secret key. Therefore, the *key distribution* step, allowing

Alice and Bob to establish a secret key prior to exchanging any messages, is of capital importance for many areas of cryptography.

Various schemes have been proposed over time to ensure the security and authenticity of communications without resorting to a previously shared private key (Diffie-Hellman, Digital Signature Algorithm, RSA). Probably, the most successful example of such a public-key system is the RSA cryptographic system, based on the RSA algorithm [14]. The security of public-key cryptographic communication systems rests on unproved assumptions about the difficulty to compute the decryption key, even when the encryption key is known. The RSA algorithm, for example, so popular today, capitalizes on the presumed intractability of factoring large numbers in a reasonable amount of time, although nobody was able to prove that factoring is not in P.

With the advent of processing information at the quantum level, the security of cryptographic protocols was set on a firmer foundation. Quantum key distribution (QKD) schemes were proposed whose security is guaranteed by the very laws of physics (quantum mechanics, more precisely). What really distinguishes them from the classical cryptographic protocols is that they make the difference in terms of *intrusion detection*. In a classical scheme, one can only hope that the adversary simply does not have enough computational resources to gain knowledge of the information in transit. There is no protocol that allows for the detection of an eavesdropper. The ability to copy classical information without restriction is responsible for this situation. In contrast, since arbitrary quantum bits cannot be cloned [16], it is much more difficult for an eavesdropper to spy on a quantum communication without being detected.

Several techniques exist that exploit quantum effects for key distribution [2, 1, 10]. Their aim is to maximize the intrusion detection rate, upon which the security of the protocols rests. In these protocols, Alice conveys the secret information to Bob by encoding it into some quantum properties of photons. At the other end, Bob has to subject each photon to a quantum measurement, as soon as it is received, in order to agree with Alice on a common key.

In this paper we explore the feasibility and advantages offered by a novel approach to QKD. We consider the situation in which Bob stores the qubits received from Alice until he acquires more information about how to measure them. This is not only possible, in view of the recent advances in laying the foundation for quantum networks, but also allows for the creation of con-

ceptually new protocols for QKD. These new protocols have the potential to outperform the previous ones in terms of the total volume of communication required and (more important, perhaps) the intrusion detection rate. The price to pay for these benefits is a more complex processing of the qubits transmitted.

The remainder of the paper is structured as follows. Next section reviews the main existing techniques for QKD. Section 3 introduces and motivates the approach we take in this paper. Sections 4 and 5, each discusses a protocol developed under the new assumption allowing qubits to be stored for a relatively short period of time. The first one is based on the random application of a phase shift, while the second one is a bit more expensive computationally and exploits the data dependency present in the Quantum Fourier Transform and its inverse. Conclusions and prospects for future research are presented in section 6.

2 Previous work

This section is intended to provide a context for the discussion of the new protocols developed in sections 4 and 5. Thus, when analyzing their features and performance, we will use the work reviewed here for reference and comparison.

Generally, QKD protocols involve two stages. The first one is usually a one-way communication (from Alice to Bob) over a quantum channel. In this stage, a random sequence of bits generated by Alice is transmitted over to Bob, each 0 or 1 encoded in some quantum observable (photon polarization is the natural choice). Having measured each incoming qubit in one of the predefined bases, Bob must now communicate with Alice over a public channel to exchange information about the encoding of each qubit and eventually agree upon a common secret key. This two-way communication between Alice and Bob over a classical channel represents the second stage of QKD protocols. The above two-stage scenario forms the backbone of all schemes developed so far in order to distribute classical keys through quantum means. They differ only in the particular quantum mechanical features or principles chosen to achieve their goal.

The first quantum protocol for key distribution was developed in 1984 by Charles Bennett and Gilles Brassard and is hence known as BB84 [2]. It is characterized by the use of two quantum alphabets (orthonormal bases) for

Alice	0	1	1	0	0	1	0	0	0	1	0	0	1	1	0
	$\times$	$+$	$\times$	$+$	$+$	$+$	$\times$	$\times$	$+$	$+$	$\times$	$+$	$\times$	$\times$	$\times$
	$\nearrow$	$\uparrow$	$\nwarrow$	$\rightarrow$	$\rightarrow$	$\uparrow$	$\nearrow$	$\nearrow$	$\rightarrow$	$\uparrow$	$\nearrow$	$\rightarrow$	$\nwarrow$	$\nwarrow$	$\nearrow$
Bob	$+$	$+$	$\times$	$+$	$\times$	$\times$	$+$	$\times$	$\times$	$+$	$+$	$+$	$\times$	$+$	$\times$
	1	1	1	0	0	1	1	0	1	1	0	0	1	1	0
key		1	1	0				0		1		0	1		0

Figure 1: Quantum key distribution in the absence of eavesdropping.

encoding and decoding the bits transmitted. One consists of the vertical and horizontal polarization states of photons, while the other orthonormal basis corresponds to polarization directions formed respectively by 45° clockwise and counter-clockwise rotations off from the vertical. The convention used for the two quantum alphabets could be

$$\begin{cases} \text{“0”} & = & |\rightarrow\rangle \\ \text{“1”} & = & |\uparrow\rangle \end{cases}$$

in the case of the vertical/horizontal basis, and

$$\begin{cases} \text{“0”} & = & |\nearrow\rangle \\ \text{“1”} & = & |\nwarrow\rangle \end{cases}$$

for the oblique basis. In the first stage of BB84, Alice randomly chooses one of these two agreed-upon quantum alphabets for each bit transmitted. At the receiving end, Bob also selects one basis, at random, to measure each incoming photon and decode the bit carried. By comparing the alphabet used for encoding with that used for decoding, in the second stage of the protocol, Alice and Bob can reach an agreement for a common binary substring called the *raw key*, by keeping only those bits for which the encoding and decoding basis was the same and discarding all the others (roughly half of the total number of bits transmitted). Figure 1 illustrates this process.

Using a pair of conjugate (incompatible) observables, the BB84 protocol relies on Heisenberg's uncertainty principle coupled with the inevitable disturbance caused by quantum measurements to detect potential eavesdroppers. On average, 25% of the photons that Eve (the prototypical eavesdropper) chooses to tamper with will give rise to disagreements between Alice's

raw key and Bob's raw key. Things get more complicated when such disagreements can also be the result of imperfections or noise in the quantum channel. Consequently, Eve could adopt the strategy of gaining only partial knowledge about the key by trying to hide behind the noise level. To cope with such low levels of eavesdropping, Bennett et al. [4] have proposed the method of *privacy amplification*, a mathematical technique based on the principle of hashing functions that magnifies Eve's uncertainty over the final form of the key.

Using pairs of orthogonal polarization states as quantum alphabets for the transmitted bits is not a necessary condition. Bennett showed [1] that any two non-orthogonal quantum states can be used to achieve key distribution in a practical interferometric realization using low-intensity coherent light pulses. The protocol (known as B92) needs only one quantum alphabet, but with non-orthogonal polarization states. Therefore, Bob must be equipped with a POVM (positive operator value measure) receiver in order to interpret the incoming photons properly. As in the case of BB84, eavesdropping attempts are made apparent by an unusual error rate in Bob's raw key. Specific to B92 is the possibility of detecting eavesdroppers by an unusual erasure rate (inconclusive receptions) for Bob.

The protocols that offer the best security, at least from a theoretical viewpoint, are based on entanglement (EPR pairs). Inspired by EPR experiments designed to test Bell's inequality, Artur Ekert thought of a way of using entangled pairs for distributing cryptographic keys by quantum means [10]. In the first stage of his scheme, Alice and Bob receive entangled particles from a central source and perform independent measurements upon them. The shared secret key is established in the second stage, when Alice and Bob publicly confront the orientations they adopted for each measurement.

Similarly to BB84, the key will consist of only those bits that were measured in the same basis by both participants. Unlike the BB84 protocol, however, the remaining bits are not discarded, but the strength of their correlations is used to test for eavesdroppers. These correlations must exceed anything that is possible classically, according to Bell's theorem, if the original EPR pairs were untampered with. A related, but simpler EPR cryptographic scheme was described by Bennett, Brassard and Mermin [3] that is proved secure without the need to invoke Bell's theorem. They also show the equivalence between their scheme and the original BB84 key distribution protocol.

Protocols resorting to EPR pairs offer a qualitatively new level of secu-

rity, that becomes apparent by considering the scenario in which someone attempts to make measurements on the particles before they arrive at the legitimate receiver. For an entanglement-free protocol, such an eavesdropping strategy aims at gaining knowledge of the information encoded in the qubits transmitted. But in the case of schemes based on EPR pairs, Eve cannot elicit any information from the transiting particles simply because there is no information encoded there. The information about the secret key has yet to come into being once Alice and Bob perform their measurements.

Another advantage of entanglement-based schemes refers to the issue of privacy amplification. The limitations of the classical privacy amplification based on hashing algorithms are overcome in the quantum privacy amplification technique developed in 1996 [9]. The quantum procedure, which is applicable only to entanglement-based quantum cryptography, is in fact an entanglement purification process that can be repeatedly applied to impurely entangled particles to cleanse them of any signs of tampering by Eve.

However, these advantages of entanglement-based cryptography are rather theoretical at the moment because storing entangled particles is only possible for a fraction of a second as yet, and entanglement purification depends on quantum computational hardware that, although simple, has yet to be built. In contrast, implementations of the original BB84 protocol are well within the capabilities of current technology, reaching the point where they have become commercially viable.

3 Motivation

At an abstract level, a QKD protocol could be described in terms of qubits transmitted over a quantum channel. For practical implementations, the physical realization usually chosen to embody a qubit is the photon. Since it travels at the speed of light and its polarization can be easily manipulated, the photon is naturally suited for transmitting information. Still, in some cases, other realizations are equally possible, like manipulating the spin of an electron, for instance. Regardless of their possible implementations, all QKD protocols share one basic constraint: qubits are measured individually as soon as they are received. Storing the incoming qubits for later processing and/or measurement is not taken into consideration. This is quite intuitive, especially if we think about photons, who, by their nature, are made to travel and not to store information locally, in a static fashion.

This paper investigates the opportunities created by the relaxation of the aforementioned constraint. More explicitly, we are interested in what benefits can be gained and at what cost, if we allow the qubits transmitted over the quantum channel to be stored for a determined amount of time by the receiving party. In the following, we motivate the feasibility of this assumption, even if the qubits are realized as photons.

Two of the main proposals for building a practical quantum computer are based on "ion traps" and cavity QED (quantum electrodynamics), respectively. In the ion trap scheme imagined by Cirac and Zoller [6], a quantum memory register would be physically realized by using "fences" of electromagnetic fields to trap a number of ions within the central region of an evacuated chamber. Each imprisoned ion embodies a qubit, with the ground state representing $|0\rangle$ and a metastable state representing $|1\rangle$. The operation of a quantum gate is effected by shining a pulse of light from a laser beam of the appropriate frequency onto the target ion. Although very simple quantum algorithms have been implemented on an ion trap quantum computer [11], the technology's main drawback remains scalability.

In the other proposal, which goes by the name of "flying qubit"-based quantum computer, quantum information is encoded in the polarization states of photons. The interaction necessary to emulate the functionality of a controlled-NOT quantum gate can be mediated by a drifting cesium atom, when the photons are placed inside a small cavity with highly reflecting walls. Quantum-phase gates based on cavity QED have been successfully realized experimentally [8, 15], yet again, it is a very challenging endeavor to extend this technology to complicated quantum circuits.

One of the ideas that emerged in order to overcome the scalability problem is a hybrid approach that combines the advantages of both ion trap and cavity QED technologies. In this approach, ion traps of limited size each would be interconnected through fiber optics, forming a quantum network. Thus, photons could be used to transfer quantum information between distant trapped atoms, while each of the multibit ion traps is responsible for storing information and local processing. The cavity QED interactions can provide the necessary methods for exchanging quantum information between the two different carriers [7]. Alternatively, the same goal can be achieved by using entanglement between a trapped atom and a photon [5].

The techniques proposed to implement a quantum network can also be applied in a cryptographic context. The qubits "flying" through the quantum channel will still be realized as photons, but whenever the receiving party

wishes to store them (until it has better knowledge about their encoding, for example), the information they carry is transferred to a local ion trap quantum register, which is much more suited for storing information over an extended length of time. Hence, our working assumption is motivated practically by the advancements made on the way toward building a quantum computer.

The immediate benefit of storing qubits during a quantum protocol for a more "intelligent" processing/measurement is an important reduction in the communication volume required, both quantum and classical. In the case of BB84, for instance, if Bob can safely store the qubits received from Alice until the second stage of the protocol, when he is informed of the exact encoding for each of them, then an appropriate measurement can be performed for each qubit. In this way, no qubit has to be discarded due to a mismatch between the encoding and decoding alphabet. For a shared secret key of a specified length, this leads to a 50% reduction in the total number of qubits that have to be transmitted. With fewer qubits transmitted, the volume of the classical communication in stage 2 of the protocol is reduced too. The fact that an eavesdropper may gain knowledge about the correct measurement basis for each qubit is of no advantage to her, since the qubits are no longer in her possession.

But reducing the amount of communication between Alice and Bob is not the only advantage offered by temporarily storing qubits. This possibility opens the door for designing new QKD schemes that have higher rates of intrusion detection and are therefore more secure. In the next two sections we show explicitly how storing qubits for a limited time can be exploited to enhance security.

4 Random $\frac{\pi}{2}$ phase shift protocol

We first describe a BB84 equivalent protocol that we will use as a building block in designing a QKD scheme based on the Quantum Fourier Transform. The main idea of the protocol described in this section is to encode each transmitted bit (0 or 1) into the relative phase between the $|0\rangle$ and $|1\rangle$ components of a balanced superposition and then encrypt the resulting qubit by applying a random phase shift gate, as depicted in Figure 2. The Hadamard gate provides the encoding alphabet

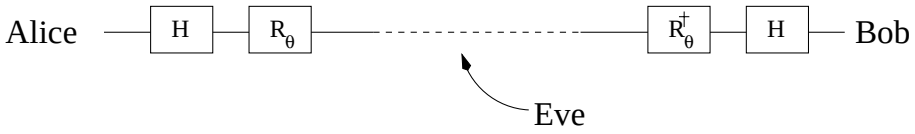

Figure 2: Schematics of random phase shift protocol for QKD.

$$\begin{cases} \text{“0”} & \mapsto & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ \text{“1”} & \mapsto & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$$

and the R_θ gate rotates the relative phase with an angle θ

$$R_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix},\ \theta \in \{0, \frac{\pi}{2}\}.$$

Note that R_0 does not affect the state of the qubit onto which the gate is applied, while $R_{\pi/2}$ rotates the qubit halfway between the two symbols of the encoding alphabet. The gate $R_\theta^\dagger$ denotes the inverse of R_θ. The protocol conforms to the generic two-stage structure, sketched in section 2.

Random $\frac{\pi}{2}$ phase shift protocol for QKD

Stage 1: Communication over a quantum channel

Step 1. Alice flips a fair coin to generate a random binary sequence that she intends to share with Bob.

Step 2. For each bit j in the sequence, Alice chooses , again at random, an angle $\theta = 0$ or $\theta = \pi/2$. She then prepares, accordingly, a qubit in the state $|\psi\rangle = R_\theta H|j\rangle$ that she sends over to Bob.

Step 3. Bob applies the necessary procedures for safely storing the qubits received from Alice until the second stage of the protocol, when he gains knowledge of which qubits have been phase shifted.

Stage 2: Communication over a public channel

Phase 1. Raw key extraction

Step 1. Alice informs Bob about her choice of θ for each transmitted bit.

Step 2. Knowing the relative phase shift θ for each stored qubit $|\psi\rangle$, Bob recovers the original bit transmitted, by computing $|j\rangle = HR_\theta^\dagger|\psi\rangle$ and then measuring $|j\rangle$ in the normal computational basis $\{|0\rangle, |1\rangle\}$. Following this procedure, Bob obtains a binary sequence that should be identical to the one randomly generated by Alice, provided no eavesdropping or errors interfered with the quantum transmission.

Phase 2. Error estimation

Step 1. Over the public channel, Alice and Bob compare portions of their raw keys to estimate the error rate Err. The bits tested are deleted from their raw keys. If $Err = 0$ the remaining bits form their final secret key.

Step 2. If $Err > 0$, but still sufficiently small, Alice and Bob may decide to apply privacy amplification techniques to minimize Eve's knowledge about their final secret key. Otherwise, if Err exceeds a certain threshold, they discard the whole sequence and start all over again.

The analogy with BB84 becomes apparent if we assimilate the encoding alphabet with the horizontal/vertical basis and the $\pi/2$ relative phase shift with the oblique basis. What are Eve's chances to break the above protocol and find a loophole that may allow her to elicit information about the secret key? In what follows, we analyze two main eavesdropping strategies that Eve may adopt.

Opaque eavesdropping The most straightforward way in which Eve could spy on the quantum communication between Alice and Bob would be to intercept Alice's information carriers and measure them in some appropriate basis. If she could undo the rotation (with angle θ) applied by Alice, then she could measure the intercepted qubit using the basis $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. Such a measurement is carried out by first passing the qubit through a Hadamard gate and then measuring it in the normal computational basis $\{|0\rangle, |1\rangle\}$.

Since Eve has no information about θ, trying to rotate the qubit back with $\pi/2$ (see Figure 3) is in no way a better strategy than applying the

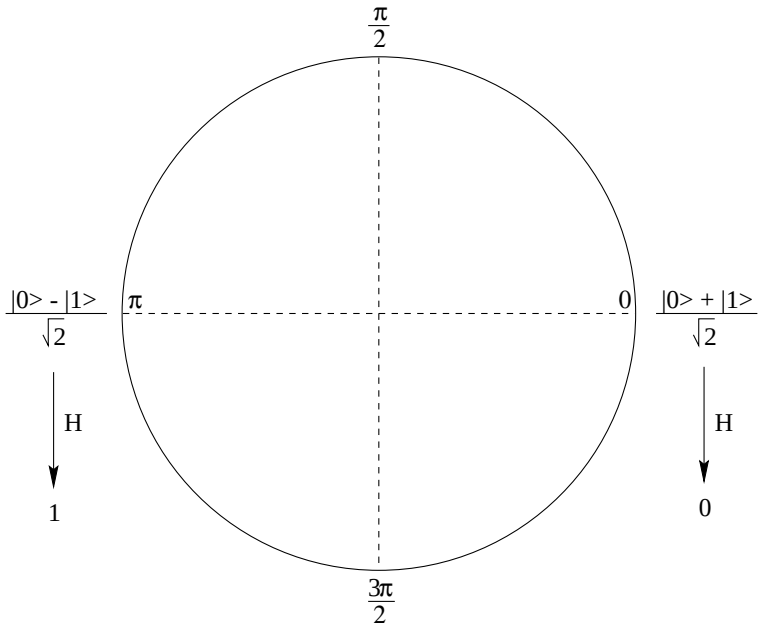

Figure 3: Bit encoding in the random $\frac{\pi}{2}$ phase shift protocol.

Hadamard gate directly. Without loss of generality, consider what happens if the qubit intercepted by Eve encodes the bit 0 (the other case proceeds in an analogous way yielding a symmetric result). Before is acted upon, its state is given by

$$|\psi^0\rangle = R_\theta H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}e^{i\theta}|1\rangle. \tag{1}$$

Eve is assumed to have knowledge of the encoding alphabet, so she reverses the effect of the Hadamard gate by also applying a Hadamard gate (which is its own inverse):

$$H|\psi^0\rangle = \frac{1}{2}(|0\rangle + |1\rangle) + \frac{e^{i\theta}}{2}(|0\rangle - |1\rangle) = \frac{1+e^{i\theta}}{2}|0\rangle + \frac{1-e^{i\theta}}{2}|1\rangle. \tag{2}$$

Upon observing the above state, Eve will see a 0 with probability

$$p^0_{Eve} = |\frac{1+e^{i\theta}}{2}|^2 = \frac{1+\cos\theta}{2}. \tag{3}$$

and a 1 with probability

$$p^1_{Eve} = |\frac{1 - e^{i\theta}}{2}|^2 = \frac{1 - \cos\theta}{2}. \quad (4)$$

where θ is either 0 or $\pi/2$ (see Figure 3). Next, Eve uses the Hadamard transform again to prepare a qubit in an encoded state compatible with the measurement's outcome and sends it to Bob. Bob keeps the qubit untouched until Alice informs him of the correct rotation angle θ. Then, he applies the $R^\dagger_\theta$ gate, thus inducing a relative phase of $-\theta$, since he received the qubit from Eve and not from Alice. Finally, Bob measures the qubit in the Hadamard basis, obtaining a 0 with the following probability:

$$p^0_{Bob} = p^0_{Eve} \cdot |\frac{1 + e^{-i\theta}}{2}|^2 + p^1_{Eve} \cdot |\frac{1 - e^{-i\theta}}{2}|^2 = \frac{1 + \cos^2\theta}{2}. \quad (5)$$

For $\theta = 0$, $p^0_{Bob} = 1$ and Eve gets undetected, but if $\theta = \pi/2$, p^0_{Bob} is only $1/2$, so, on average, there is a 25% probability of detecting Eve for each qubit she chooses to eavesdrop on (same as BB84). Of course, this probability can be made arbitrarily close to 1 by testing a sufficiently large number of qubits. In turn, this requires a large number of qubits to be transmitted through the quantum channel. If Bob can store these qubits until the second stage of the protocol, the cost of the total communication (both quantum and classical) is effectively halved. Parity checking techniques, to avoid discarding bits when testing for eavesdropping, are also applicable.

Translucent eavesdropping In order to avoid the inevitable disturbance caused by a measurement, Eve could decide for a more subtle eavesdropping technique. She could choose, for instance, to entangle Alice's information carrier with her own probe, sending half of the entangled pair to Bob while keeping the other half for herself. Then, upon finding about the correct θ angle, by listening in on the conversation between Alice and Bob on the classical channel, Eve can apply the $R^\dagger_\theta$ and Hadamard gates to the qubit in her possession, hoping to unlock the information hidden within it. We focus again on the case when Alice encodes a 0, with the observation that the analysis for the other case would proceed in a similar way. The entanglement operation, performed by Eve, is described by the following equation:

$$CNOT((\frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i\theta}}{\sqrt{2}}|1\rangle) \otimes |0\rangle) = \frac{1}{\sqrt{2}}|00\rangle + \frac{e^{i\theta}}{\sqrt{2}}|11\rangle. \quad (6)$$

where $CNOT$ denotes the application of a controlled-NOT operation, with the qubit intercepted from Alice acting as the control qubit. When Alice discloses to Bob whether she applied the $\pi/2$ relative phase shift or not, Eve can proceed to effect the $R_\theta^\dagger$ and Hadamard transformations on the qubit remained in her possession. This will change the state of the ensemble Eve-Bob as follows:

$$\begin{aligned} H \otimes I(R_\theta^\dagger \otimes I(\tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{e^{i\theta}}{\sqrt{2}}|11\rangle)) &= H \otimes I(\tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|11\rangle) \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle). \end{aligned} \tag{7}$$

Similarly, if a bit with the value 1 would have been transmitted by Alice, the state of the entangled ensemble would have been

$$\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle). \tag{8}$$

Although distinguishing among states (7) and (8) is possible by applying a two-qubit gate on the whole ensemble, no information can be elicited by acting only on one qubit. In particular, a quantum measurement in the normal computational basis will yield a 0 or a 1 with equal probability.

The description and analysis of the protocol assumed an error-free quantum channel. The issue of noise can be addressed by introducing an additional phase to the second stage of the protocol. During this phase, Alice and Bob remove all errors from their tentative final key, producing a common error-free key, called *reconciled key* (see [12], chapter III, for details).

We conclude the analysis of the random $\pi/2$ phase shift protocol with a few observations that, although formulated for the protocol presented in this section, can be generalized, in a suitable form, to probably any existing QKD scheme. For each qubit Eve decides to tamper with, there is a certain chance (25% in our case, as well as for BB84) that she will be caught. It is important to emphasize that this probability is independent of the actions performed on the other qubits transmitted through the quantum channel. The only way Eve can be detected is to test one of the qubits she decided to spy on. In half of the cases, when she is lucky, the quantum state retransmitted to Bob is identical to the one intercepted from Alice, so she gains knowledge of the bit transmitted without any possibility of being detected. On the other hand, if she gets unlucky, then her uncertainty about the bit transmitted is total and,

in addition, she disturbs the state of the qubit, introducing an error rate in Bob's raw key.

Consequently, Eve could settle for a low level of eavesdropping, trying to gain only partial knowledge of the secret key, while minimizing the chances of being detected. She could even take advantage of the imperfections in the quantum channel, trying to hide behind the "noise". In the next section, we propose a conceptually new kind of QKD scheme that aims to maximize Eve's uncertainty about the bits she eavesdropped on, even after the public discussion between Alice and Bob, while giving Bob higher chances of detecting Eve, even for a smaller number of bits tested. The main idea of the protocol is to propagate the disruption caused by Eve when measuring a qubit to other qubits in the sequence as well. To this end we take advantage of the data dependencies introduced by the application of the Quantum Fourier Transform.

5 QKD scheme based on the Fourier transform

The Quantum Fourier Transform (QFT) is a very powerful tool, allowing the design of quantum algorithms that are exponentially faster than their best classical counterparts, as in the case of Shor's quantum algorithms for factoring integers and computing discrete logarithms. We show herein that the QFT and its inverse can also be successfully used to build quantum key distribution protocols that offer improved eavesdropping detection rates while maximizing the eavesdropper's uncertainty about the binary sequence transmitted.

The QFT is a linear operator whose action on any of the computational basis vectors $|0\rangle, |1\rangle, \cdots, |2^n - 1\rangle$ associated with an n-qubit register is described by the following transformation:

$$|j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k/2^n} |k\rangle,\ 0 \leq j \leq 2^n - 1. \tag{9}$$

Equation (9) can be rewritten as a tensor product of the n qubits involved, as follows:

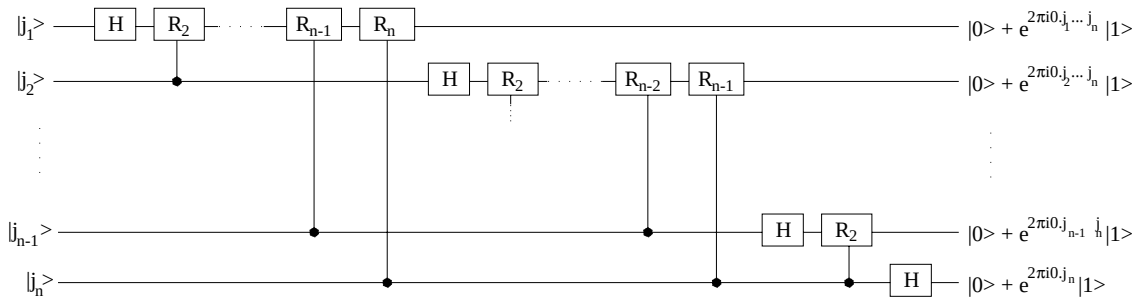

Figure 4: Quantum circuit performing the discrete Fourier transform.

$$|j_1 j_2 \cdots j_n\rangle \longrightarrow \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle) \otimes (|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle) \otimes \cdots \otimes (|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle)}{2^{n/2}}. \tag{10}$$

Equation (10) provides the blueprint for devising a circuit implementing the QFT that requires only $\Theta(n^2)$ elementary quantum gates (see Figure 4).

Note that each Fourier transformed qubit is in a balanced superposition of $|0\rangle$ and $|1\rangle$. They differ from one another only in the relative phase between the $|0\rangle$ and the $|1\rangle$ components. For the first qubit in the tensor product, j_n will introduce a phase shift of 0 or π, depending on whether its value is 0 or 1, respectively. The phase of the second qubit is determined (controlled) by both j_n and j_{n-1}. It can amount to $\pi + \pi/2$, provided j_{n-1} and j_n are both 1. This dependency on the values of all the previous qubits continues up to (and including) the last term in the tensor product. When $|j_1\rangle$ gets Fourier transformed, the coefficient of $|1\rangle$ in the superposition involves all the digits in the binary expansion of j.

In the case of each qubit, the 0 or π phase induced by its own binary value is implemented through a Hadamard gate. The dependency on the previous qubits is reflected in the use of controlled phase shifts, as depicted in Figure 4. Reversing each gate in Figure 4 gives us an efficient quantum circuit (depicted in Figure 5) for performing the inverse Fourier transform.

Getting back to the original $|j_1 j_2 \cdots j_n\rangle$ from its Fourier transformed expression has a certain particularity though. Because of the interdependencies introduced by the controlled rotations, the procedure must start by computing $|j_n\rangle$ and then work its way up to $|j_1\rangle$. The value of $|j_n\rangle$ is needed in the computation of $|j_{n-1}\rangle$. Both $|j_n\rangle$ and $|j_{n-1}\rangle$ are required in order to obtain

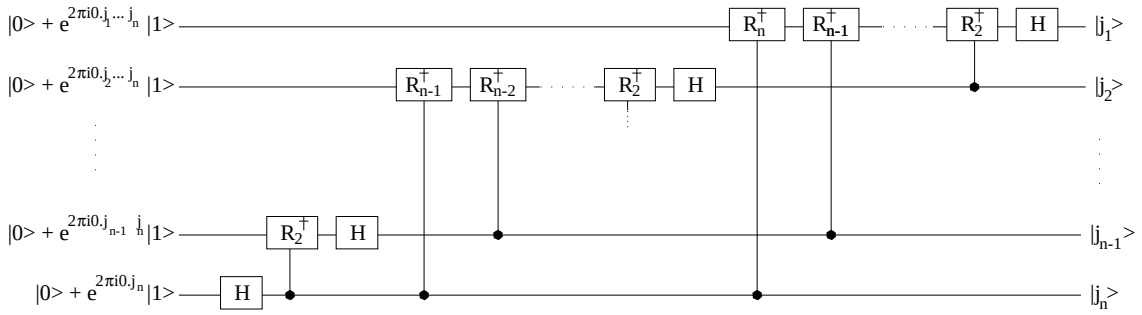

Figure 5: Quantum circuit performing the inverse Fourier transform.

$|j_{n-2}\rangle$. This continues in the same manner, until finally, the values of all the higher rank bits are used to determine $|j_1\rangle$ precisely.

This fixed order of execution can be exploited to design secure QKD schemes. The protocol that we describe in the following can be seen as a generalization of the random $\pi/2$ phase shift protocol, both relying on encapsulating information in the relative phase between the two components in a superposition. However, the Fourier transform brings into play the *rank* of a qubit in the sequence, thus giving a *context* to each qubit transmitted.

Employing the Fourier transform instead of the random $\pi/2$ phase shift as the encryption method does not alter the main structure of the protocol, so we will just point out the differences relative to the description we provided in the previous section. In step 2 of the quantum communication stage, Alice applies the QFT to the binary sequence generated in the previous step, by passing it through the quantum circuit depicted in Figure 4. Then, she scrambles the resulting qubit sequence by choosing an arbitrary permutation of the qubits and sends them to Bob.

In stage 2 of the protocol, Alice informs Bob of the correct order in which he must place the received qubits (in other words, the *rank* of each qubit is disclosed). Consequently, the raw key extraction step can proceed with Bob applying the inverse Fourier transform to the properly re-arranged qubit sequence. In the absence of any eavesdropping or transmission errors, Bob must end up with the same bit sequence that Alice randomly produced at the outset of the protocol.

When Eve decides to spy on an arbitrary qubit in the sequence, she doesn't know its rank and is therefore ignorant of the influence exerted on it by the previous qubits in the ordered sequence. Without access to this

additional information (the qubit's context), Eve can have no confidence in the outcome of an eventual measurement in the Hadamard basis pointing to a 0 or a 1.

Example Suppose that the bit string that Alice wants to convey to Bob is 10011010, so that $j_1 = 1$ and $j_8 = 0$. Consider what happens if Eve intercepts the qubit of rank 6 and measures it in the Hadamard basis. Since its state is

$$|0\rangle + e^{2\pi i 0.010}|1\rangle = |0\rangle + e^{\frac{\pi}{2}i}|1\rangle, \tag{11}$$

exactly halfway between $|0\rangle$ and $|1\rangle$ (relative phase $\pi/2$), there is an equal probability for either outcome to be realized. Consequently, even after learning it's context, Eve's uncertainty over this bit is total. Following her measurement, Eve can either send $H|0\rangle$ or $H|1\rangle$ to Bob. In any case, Bob will undo the $\pi/2$ rotation supposedly caused by $j_7 = 1$, therefore having a 50% chance of detecting Eve, provided he and Alice choose to test bit j_6. But if Bob measures bit j_6 as 1, then the error introduced by Eve's action is still detectable, even if the qubit whose state she disturbed is not checked by Alice and Bob. Thus, when applying the inverse Fourier transform on the qubit of rank 5, its quantum state becomes

$$|0\rangle + e^{(\pi + \frac{\pi}{4} - \frac{\pi}{4} - \frac{\pi}{2})i}|1\rangle \tag{12}$$

and in 50% of the cases Alice and Bob will discover a mismatch in their values for this bit. An erroneous bit j_6 will continue to influence the outcome of the following bits, up to j_1. The strength of this influence decreases with the rank and probably becomes negligible in a few steps. Nevertheless, if the error in j_6 propagates to one of its neighbors, then this bit acts as a new source of error, creating the mechanism for the initial disturbance to propagate indefinitely. So, unlike other QKD schemes, in this case, eavesdropping on one qubit has the potential to introduce a large number of errors. In general, for an arbitrary qubit of rank k ($0 < k \leq n$), the relative phase shift caused by errors in the previous bits (from n to $k+1$) varies between 0 and $\sum_{i=1}^{n-k} \pi/2^i$, as the errors induced may interfere with each other, adding up or canceling out.

Since Eve's uncertainty over an observed value is based on her ignorance about the context involved, it appears that the weak spot of the protocol lies in the high rank qubits. The highest rank qubit, for instance, is context-free (having no predecessors), so Eve can be certain of its value, provided she has

performed a measurement on it. But because she doesn't know the ranks of the qubits transmitted during the quantum communication stage, she must eavesdrop on many qubits to increase her chances of learning the value of j_n. This, in turn, will cause more disturbance and therefore increase the risk of being detected.

In our example, by learning that the value of j_8 equals 0, Eve also becomes aware that j_8 has no influence on j_7, so her measurement on j_7 (if performed) must have yielded its true value. However, since $j_7 = 1$, there is an equal probability that a hypothetical measurement on j_6 has revealed the correct or incorrect value. For an arbitrary bit string $j_1 \cdots j_n$, Eve can end up knowing the values of the last k bits, where $j_{n-k+1} = 1$ and $j_{n-k+2}, \cdots, j_{n-1}, j_n$ are all zeroes, assuming that she performed all the necessary measurements on the qubits in transit. In practice, since the binary sequence transmitted is chosen at random, the probability of it ending in more than two or three consecutive zeroes is very low.

One immediate solution is for Alice and Bob to discard those bits from their raw keys. Alternatively, the protocol described above, and based on the Fourier transform, could be combined with the random $\pi/2$ phase shift protocol presented in the previous section. In this way, each qubit may get an additional $\pi/2$ relative phase shift, increasing Eve's uncertainty about the trailing bits in the sequence while maintaining the uncertainty level for the others.

6 Conclusions

In this paper, we have addressed the quantum key distribution problem from the novel perspective allowed by the possibility of temporarily storing the qubits received through the quantum communications channel during a protocol. This assumption is well motivated by the progress achieved in quantum networks research. The immediate advantage is a significant decrease in the volume of quantum and classical communication required between the two parties. In addition, under the new assumption, conceptually new QKD schemes can be designed, with improved efficiency, security and eavesdropping detection.

One idea that we propose in this paper is to bring into play the dependencies between qubits created by the Quantum Fourier Transform in order to obtain a protocol with superior performance. When compared with existing

QKD schemes, the protocol using the QFT offer better eavesdropping detection rates by propagating the disruption caused to one qubit to the following qubits in the sequence. This makes the protocol more efficient in terms of the number of bits that have to be tested in order to achieve a certain level of security. Also, the lack of knowledge over a qubit's context, at the time of eavesdropping, maximizes Eve's uncertainty about the information encoded within its quantum state, thus making the protocol more secure.

These benefits come at the cost of a more complex processing required at both ends of the link. However, the computational power assumed to be available for Alice and Bob is not that of a quantum computer. Computing the QFT and its inverse in the special case of a sequence made up of classical bits requires only the application of single-qubit gates. Although all the phase shift gates in Figures 4 and 5 are controlled-rotations, the control qubit is in fact always classical. Consequently, the net effect of such a controlled-gate is the application of the phase shift rotation onto the target qubit, if the control is 1, or no transformation at all, if the control is 0. Therefore, Alice and Bob need only to be able to perform Hadamard and phase shift rotations of single-qubit quantum states. Parallel processing can also be applied in order to avoid decoherence [13].

The protocol for QKD developed in this paper demonstrates that the QFT is a versatile tool, with important applications not only in quantum algorithms, but also in quantum cryptography. It allows for the design of new QKD schemes with clear advantages over the existing ones, especially for low levels of eavesdropping. Furthermore, the results obtained herein suggest that the role of QFT in the general area of data security is much more important than previously believed. Finally, another possible direction for future research is to discover other ways in which to exploit the assumption of storing the transmitted qubits for a pre-determined amount of time.

References

[1] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121–3124, May 1992.

[2] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International*

Conference on Computers, Systems and Signal Processing, pages 175–179, IEEE, New York, 1984. Bangalore, India, December 1984.

[3] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without bell's theorem. *Physical Review Letters*, 68(5):557–559, Feb 1992.

[4] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, April 1988.

[5] B. B. Blinov, D. L. Moehring, L.-M. Duan, and Chris Monroe. Observation of entanglement between a single trapped atom and a single photon. *Nature*, 428:153–157, March 11, 2004.

[6] Ignazio Cirac and Peter Zoller. Quantum computations with cold trapped ions. *Physical Review Letters*, 74:4091–4094, 1995.

[7] Ignazio Cirac, Peter Zoller, H. J. Kimble, and H. Mabuchi. Quantum state transfer and entanglement distribution among distant nodes in a quantum network. *Physical Review Letters*, 78(16):3221–3224, April 21, 1997. http://arxiv.org/abs/quant-ph/9611017.

[8] L. Davidovich et al. Quantum switches and nonlocal microwave fields. *Physical Review Letters*, 71(15):2360–2363, October 11, 1993.

[9] David Deutsch, Artur Ekert, Richard Jozsa, Chiara Macchiavello, Sandu Popescu, and Anna Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Physical Review Letters*, 77:2818–2821, 1996. http://arxiv.org/abs/quant-ph/9604039.

[10] Artur Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, 1991.

[11] Stephan Gulde et al. Implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer. *Nature*, 421:48–50, January 2, 2003.

[12] Samuel J. Lomonaco Jr., editor. *Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium*, volume 58 of *Proceedings of Symposia in Applied Mathematics*. American Mathematical Society, Short Course, Washington, DC, January 17-18 2000.

[13] Marius Nagy and Selim G. Akl. Coping with decoherence: Parallelizing the Quantum Fourier Transform. Technical Report 2006-507, School of Computing, Queen's University, Kingston, Ontario, March 2006.

[14] Ronald L. Rivest, Adi Shamir, and Len M. Adleman. A method of obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[15] Q. Turchette et al. Measurement of conditional phase shifts for quantum logic. *Physical Review Letters*, 75(25):4710–4713, 1995.

[16] William K. Wootters and Wojciech H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.