KEY DISTRIBUTION BASED ON QUANTUM FOURIER TRANSFORM

Marius Nagy, Selim G. Akl and Sean Kershaw
School of Computing, Queen's University, Kingston, Ontario, Canada

Keywords: Key distribution, protocols, phase shift, quantum Fourier transform, disturbance amplification, eavesdropping detection.

Abstract: The data dependencies brought about by the Quantum Fourier Transform can be harnessed to design novel key distribution 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. This is due to the fact that a tested qubit may reveal the presence of an eavesdropper even if that particular qubit was not "touched" while in transit.

1 INTRODUCTION

In this paper we explore the feasibility and advantages offered by a novel approach to quantum key distribution (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 assumption is motivated by recent advances in laying the foundation for quantum networks (Cirac et al., 1997; Blinov et al., 2004) and allows for the creation of conceptually 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 is intended as a reference for the comparison we will make between the new protocol developed in this paper and the well-known BB84 quantum protocol for key distribution (Bennett and Brassard, 1984). The section describes a generic protocol based on phase manipulation, which can be seen as an abstraction of BB84. Section 3 takes the idea of phase shifts to a deeper level, as it appears in the computation of the Quantum Fourier Transform and shows how the interdependencies between qubits can be exploited to detect eavesdropping activity in a quantum key distribution protocol. Section 4 demonstrates the improvement in intrusion detection and security of the novel protocol with respect to BB84 through a series of simulations. Conclusions and prospects for future research are presented in section 5.

2 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 1. The Hadamard gate provides the encoding alphabet

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

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

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

Nagy M., G. Akl S. and Kershaw S. (2008).
KEY DISTRIBUTION BASED ON QUANTUM FOURIER TRANSFORM.
In *Proceedings of the International Conference on Security and Cryptography*, pages 263-269
DOI: 10.5220/0001916802630269

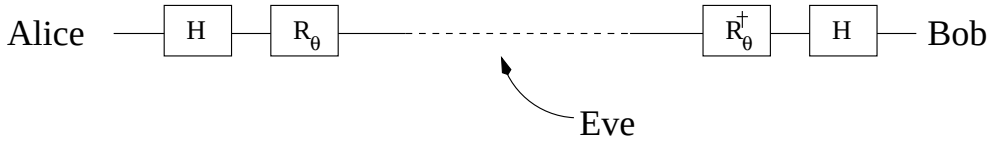

Figure 1: Schematics of random phase shift protocol for QKD.

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.

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. 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.

3 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 (Shor, 1997). 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:

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

Equation (1) can be rewritten as a tensor product of the n qubits involved, as follows:

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

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

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 2. Reversing each gate in Figure 2 gives us an efficient quantum circuit for performing the inverse Fourier transform.

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 $|j_{n-2}\rangle$. 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. Figure 3 gives a pictorial representation of the entire protocol, with time flowing downwards.

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 2. Then, she scrambles the resulting qubit sequence by choosing an arbitrary permutation of the qubits and sends them to Bob.

In the second stage of the protocol (involving classical communication), 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.

3.1 An 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

$$|0\rangle + e^{2\pi i 0.010}|1\rangle = |0\rangle + e^{\frac{\pi}{2}i}|1\rangle, \quad (3)$$

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 its 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

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

and in 50% of the cases Alice and Bob will discover a mismatch in their values for this bit. An erroneous

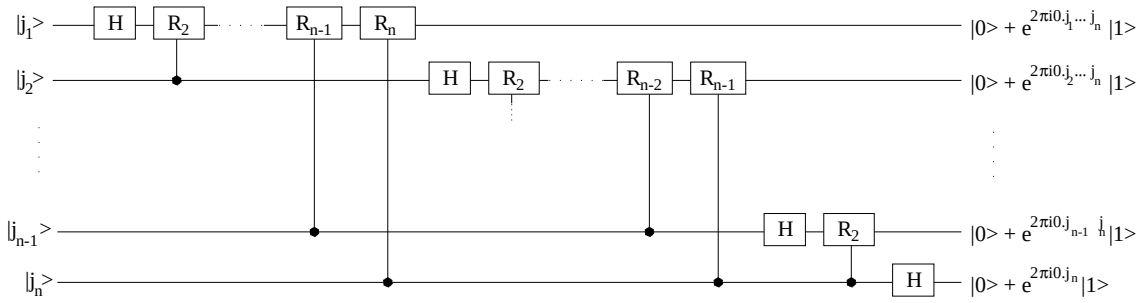

Figure 2: Quantum circuit performing the discrete Fourier transform.

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.

4 SIMULATIONS

In order to better assess the improvement in performance brought by the QFT-based protocol with respect to the traditional BB84 protocol, a series of simulations for various input parameters were performed. To ensure a fair comparison between the two protocols, we assumed that Bob has knowledge of the encoding bases chosen by Alice, such that no qubits are discarded in the BB84 protocol because of a mismatch between the encoding and decoding bases. A series of 1000 simulations were performed for each possible configuration allowed by varying the following input parameters:

- total number of qubits transmitted (128, 256, 512),
- percentage of qubits eavesdropped on by Eve (10, 25, 50),
- percentage of qubits checked for eavesdropping by Alice and Bob (10, 25, 50).

Figure 4 shows the results in terms of the number of times Eve managed to remain undetected during each batch of 1000 simulations of the two protocols. For the same number of qubits eavesdropped on and the same number of qubits checked, the QFT-based protocol consistently outperforms BB84 because the errors introduced by eavesdropping propagate to other qubits as well and thus Eve may get caught even if the bit checked was not eavesdropped on. We can see that the improvement is bigger for lower levels of eavesdropping and/or fewer bits checked.

Figure 5, on the other hand, shows the average number of qubits (out of 256) that were detected as

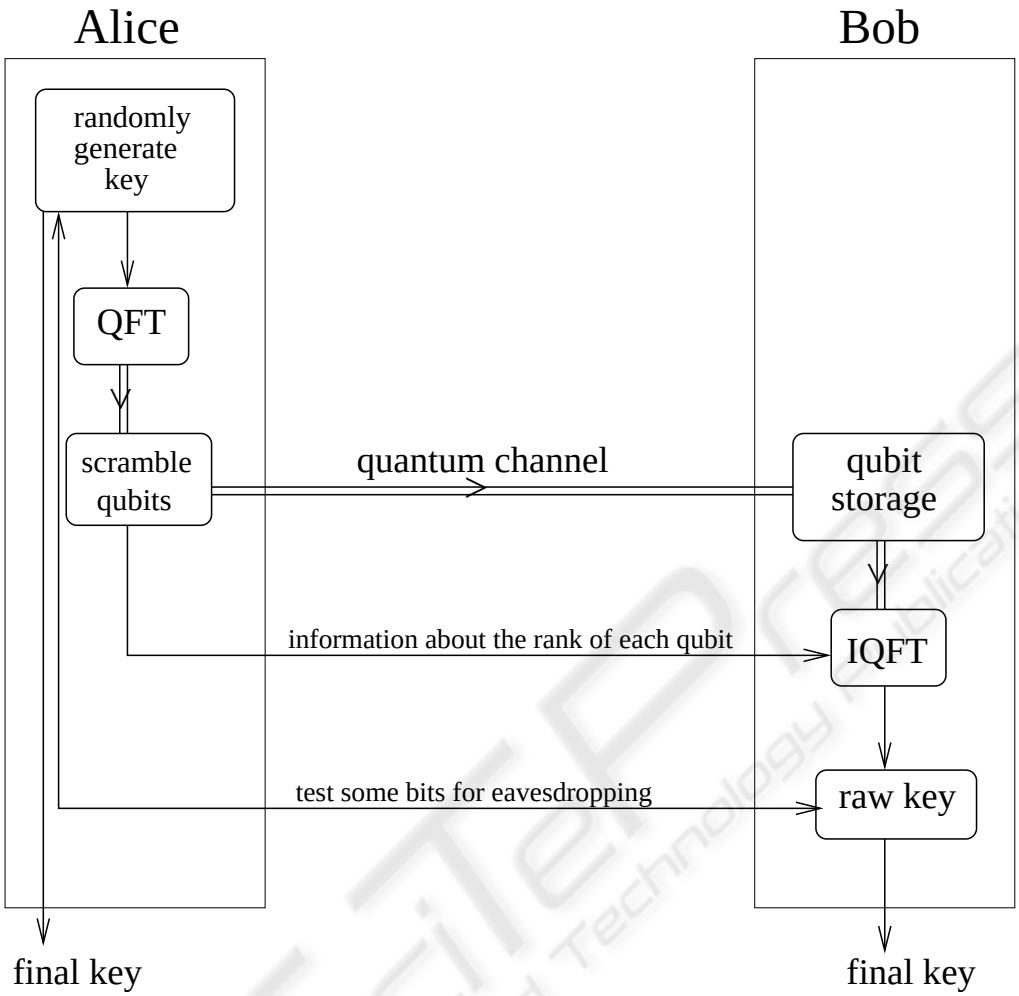

Figure 3: Schematics of a quantum key distribution protocol using the quantum Fourier transform (QFT) and its inverse (IQFT) as encoding and decoding algorithms. This is the first protocol that allows the detection of an eavesdropper even if the qubit tested was not "disturbed" while in transit.

corrupted by Eve in each 1000-trial batch. The improvement in performance in favor of the QFT-based protocol is evident for each combination of input variables.

5 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

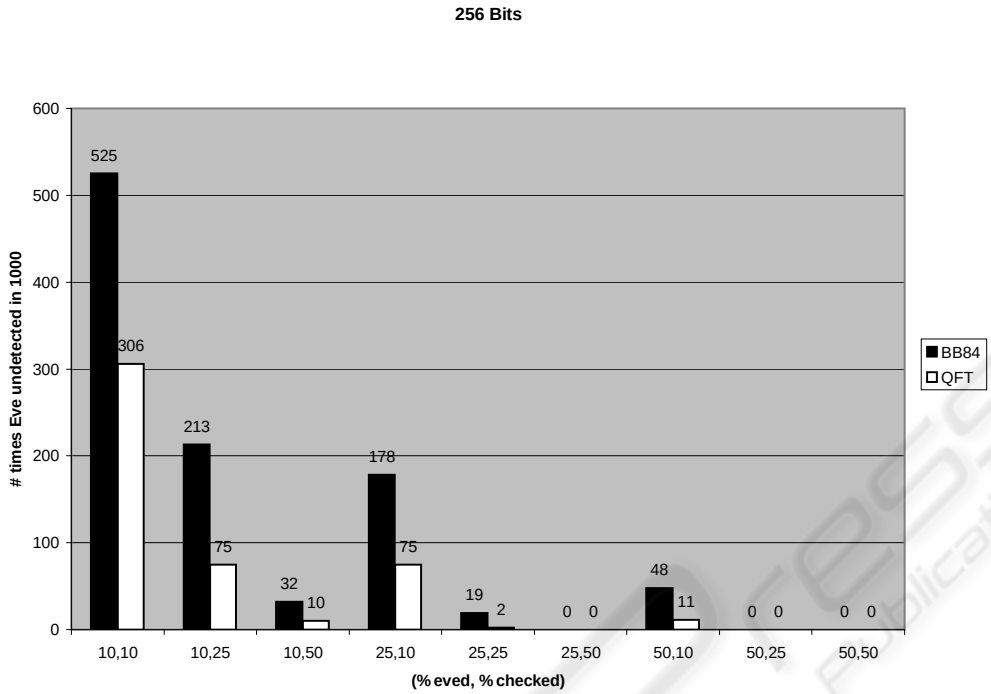

Figure 4: A comparison between the QFT-based and the BB84 protocol, in terms of the number of times Eve escapes detection in 1000 trials, for various percentages of bits eavesdropped on and checked.

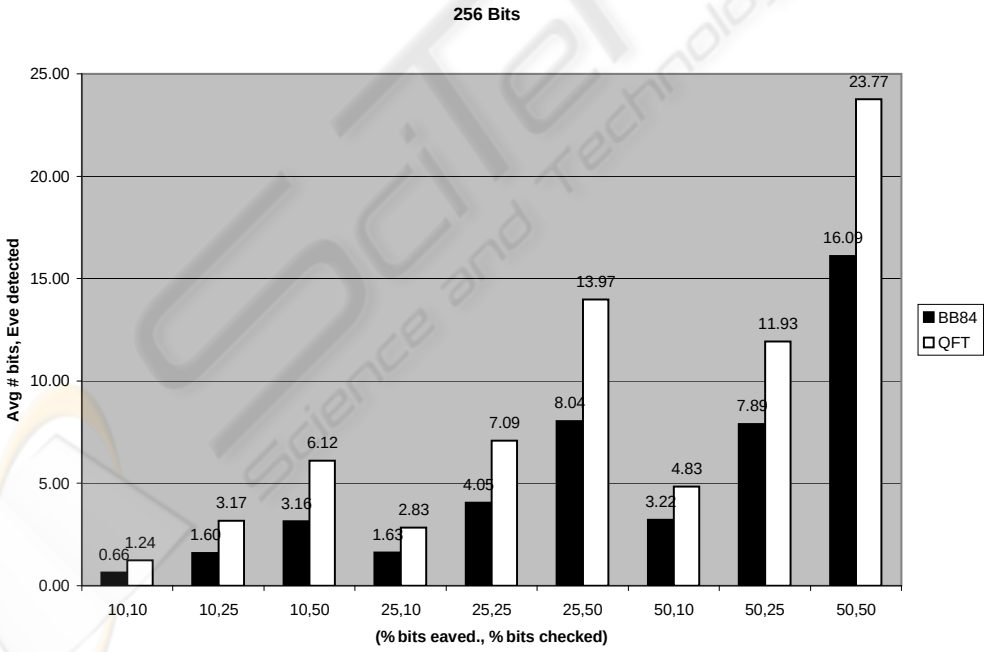

Figure 5: A comparison between the QFT-based and the BB84 protocol, in terms of the average number of corrupt bits detected in 1000 trials, for various percentages of bits eavesdropped on and checked.

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. 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 (Nagy and Akl, 2006).

The protocol for QKD developed in this paper demonstrates that the QFT is a versatile tool, with im-

portant 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.

REFERENCES

Bennett, C. H. and Brassard, G. (1984). 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. Bangalore, India, December 1984.

Blinov, B. B., Moehring, D. L., Duan, L.-M., and Monroe, C. (2004). Observation of entanglement between a single trapped atom and a single photon. *Nature*, 428:153–157.

Cirac, I., Zoller, P., Kimble, H. J., and Mabuchi, H. (1997). Quantum state transfer and entanglement distribution among distant nodes in a quantum network. *Physical Review Letters*, 78(16):3221–3224.

Nagy, M. and Akl, S. G. (2006). Coping with Decoherence: Parallelizing the Quantum Fourier Transform. In *19th International Conference on Parallel and Distributed Computing Systems*, pages 108–113, San Francisco, California.

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *Special issue on Quantum Computation of the SIAM Journal on Computing*, 26(5):1484–1509.