Quantum Secret Communication without an Encryption Key

Marius Nagy and Naya Nagy

College of Computer Engineering and Science
Prince Mohammad Bin Fahd University, Al Khobar, Saudi Arabia
{mnagy,nnagy}@pmu.edu.sa

Abstract. Quantum cryptographic methods increase security over classical methods. To date, quantum algorithms aim to distribute a secret key to be used afterwards to encrypt messages. The method described in this paper does not use an encryption key at all. An array of qubits is transmitted from the source to the destination with the message encoded in the phase of the qubit. The secrecy of the message derives from the nonclonability principle. Our algorithm relies on the common assumption that public information can be authenticated. The alforithm shows an increased detection rate per qubit, 33%, which is higher than the one commonly used in literature, namely 25%.

Keywords: Quantum Key Distribution, Quantum Cryptography, Intruder Detection.

1 Introduction

Quantum cryptography has been mainly concerned with quantum key distribution. The two communicating parties, Alice and Bob, undergo a protocol to distribute a secret key. Alice and Bob aim to reach a consensus on the value of a secret key. This key is to be used **later** to encrypt/decrypt a message. Actually, a large body of literature considers the quantum key distribution problem to be in fact a key enhancement [5]. Nevertheless, the opposite opinion, which says that true key distribution can be achieved with quantum means only, also has its adepts [3]. Key enhancement means that Alice and Bob share already a small secret key, possibly obtained via a classical protocol, and then develop a large secret key. Key distribution starts from public information only and develops a secret key during the protocol.

In this paper, we distance ourselves from the very idea of using a **key** for encryption. We develop a protocol that transmits a message secretly by scrambling the order of the bits rather than explicitly encrypting the message with a key. The scrambled message is transmitted via a quantum channel and therefore consists of quantum bits (qubits) rather than binary bits.

Our protocol comes with all the advantages of quantum cryptography. An intruder, Eve, listening to the message being transmitted, destroys the superposition of the qubits and thus can gain knowledge about it only with a low

A.-H. Dediu et al. (Eds.): TPNC 2013, LNCS 8273, pp. 181–192, 2013.
© Springer-Verlag Berlin Heidelberg 2013

probability. Also, the intruder is detected by Alice and Bob with an arbitrarily high probability.

Additionally, our protocol is equivalent to a one-time-pad [6] protocol. As we use no key, information about the scrambling of the message is of the same length as the message itself. Eavesdropping one message provides no gain to the intruder for any subsequent messages.

Previous quantum key distribution protocols [1] [2] have a detection rate of 25% per checked qubit. We develop an encoding strategy in three complementary basis that improves the detection rate per qubit to 33%.

The rest of the paper is organized as follows. Section 2 presents the keyless protocol that securely transmits a message from a source to a destination. It also analyzes the protocol's protection to the intruder's actions. The analysis is formalized to measure the intruder's gain of knowledge for different levels of attack. Section 3 describes an improvement on the detection rate of the intruder by using an encoding in three complementary bases. Section 4 concludes the paper.

2 Keyless Quantum Message Transmission

Using Dirac's notation, a qubit is $q = \alpha|0\rangle + \beta|1\rangle$. α and β are complex numbers. Thus, $|\alpha|^2$ is the probability of the qubit to collapse to 0, and $|\beta|^2$ to 1. Qubits are said to be in a balanced superposition if the qubit has an equal chance 50% to collapse to 0 or 1. Quantum protocols use a small set of common gates. Three such gates are used in our protocols: the controlled-NOT (CNOT) gate. the Hadamard gate, and the phase-shift gate [4]. All these gates have a control qubit. If the control qubit is $|1\rangle$, the primary qubit is transformed according to the gate's definition. If the control qubit is $|0\rangle$, the primary qubit passes the gate undisturbed.

In this section, we describe in detail the inner workings of a protocol that allows two parties, Alice and Bob, to communicate secretly over an insecure, public quantum channel. The protocol relies on the fact that a quantum channel cannot be eavesdropped on without disturbing the quantum information transmitted over the channel. In addition to the quantum channel, the quantum protocol also requires an authenticated channel for classical communication and a quantum memory (i.e. the ability to store the states of a certain number of qubits for a certain amount of time). The main steps of the protocol are:

Phase I: Communication over the Quantum Channel

Step 1: Alice concatenates the two binary strings, one representing the message she intends to send over to Bob and the other representing the signature bitstring that will be used for eavesdropping.

Step 2: For each bit in the concatenated sequence, Alice uses one of the two bases, or alphabets (chosen randomly) to encode the value of the respective bit in the quantum state of the resulting qubit.

Step 3: Alice scrambles the order of the qubits forming the quantum encrypted block obtained in step 2, by choosing an arbitrary permutation of the qubits and then sends them over to Bob through the insecure, public quantum channel.

Step 4: Bob applies the necessary procedures to safely store the qubits received from Alice until the second phase of the protocol, when he will gain knowledge about each qubit's encoding basis and position in the original qubit sequence. The position, or index of the qubit in the original sequence is called the qubit's rank.

Phase II: Communication over the Classical Channel

Step 1: Alice discloses to Bob which of the qubits transmitted are part of the signature string and the encoding base of each.

Step 2: Following Alice's instructions, Bob reconstructs the signature bitstring.

Step 3: Alice and Bob proceed to verify, bit by bit, whether the signature bitstring was untampered with, during the transmission.

Step 4: If the discrepancy between Alice and Bob is discovered in the values of the signature bits, the presence of an eavesdropper is inferred and the protocol is abandoned.
Otherwise, Alice informs Bob about the correct position (rank) of each qubit in the original message and the encoding alphabet employed to obtain each qubit.

Step 5: Bob decodes and re-arranges the qubits he still has in storage in order to obtain the plain message sent to him by Alice.

Having presented the structure of the protocol, a few clarifications and an analysis of it are perhaps appropriate at this point. Generally, the length of the signature bitstring reflects the intended level of security for the transmitted message. As the analysis below clearly shows, a longer signature bitstring results in higher chances of detecting a potential eavesdropper. Consequently, the signature length can be varied according to the importance of the message.

The protocol above is described in general terms, abstracted away from any particular physical realizations for a qubit. Moreover, any two alphabets, i.e. encoding bases, can be used, as long as they are complementary. Complementary bases means that they correspond to conjugate quantum variables. In this situation, trying to measure (decode) a qubit using the other basis, and not the one used for encoding, will maximize the uncertainty over the value of the corresponding bit: equal chances to obtain 0 or 1. From a mathematical point of view, the simplest example to achieve complementarity would probably be the use of the regular computational basis $\{|0\rangle, |1\rangle\}$ together with the "Hadamard basis" $\{H|0\rangle = \frac{|0\rangle}{\sqrt{2}} + \frac{|1\rangle}{\sqrt{2}}, H|1\rangle = \frac{|0\rangle}{\sqrt{2}} - \frac{|1\rangle}{\sqrt{2}}\}$. We note in passing that the BB84 protocol [1], which uses photon polarization as qubit embodiment, achieves com-

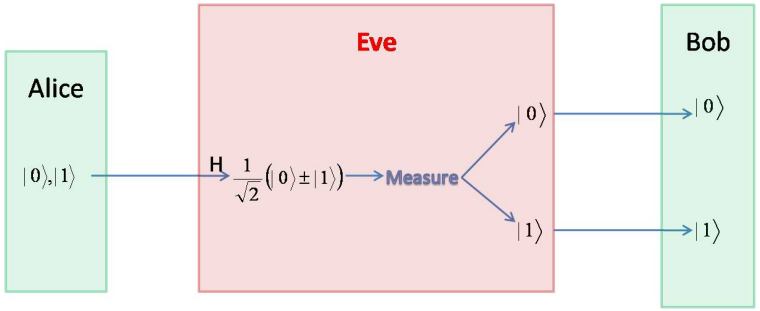

Fig. 1. Opaque eavesdropping. Eve wrongly measures in the Hadamard basis a qubit sent by Alice in the computational basis.

plementarity by choosing randomly between rectilinear polarization $\{|\rightarrow\rangle, |\uparrow\rangle\}$ and diagonal polarization $\{|\nearrow\rangle, |\nwarrow\rangle\}$ as the two possible encoding bases. In general, the precise meaning or interpretation of a certain basis depends entirely on the physical realization chosen for the qubit. To keep our discussion as general as possible, while still referring to a concrete pair of complementary bases, we assume henceforth that the two encoding alphabets are the computational basis and the Hadamard basis, as specified above. This basically means that Alice will create a $|0\rangle$ qubit for each 0 bit in the message and a $|1\rangle$ qubit for each 1 bit in the message, with a random choice to apply a Hadamard gate on the resulting qubit. What can Eve, the prototypical eavesdropper do, in order to elicit as much information as possible about the transmitted message, while the qubits are in transit from Alice to Bob? The two main possible eavesdropping strategies are discussed next.

2.1 Opaque Eavesdropping

Opaque eavesdropping refers to Eve's attempt to gain knowledge about the transmitted message by measuring each qubit passing through the quantum channel in one of the two possible bases. Eve knows the two bases that Eve has used: computational and Hadamard. Yet, for any specific qubit, Eve does not know the basis used, as Alice chooses the basis randomly. If Eve is lucky and chooses the same basis, she will be able to read the binary value of the qubit and will leave no trace of her interference. Nevertheless, if Eve chooses the wrong basis, she gains no knowledge about the binary value of the qubit, and also may disturb the correct measurement for Bob. There are two cases with similar results. First, Alice may send the qubit simply in the computational basis, see fig. 1. If Eve mistakenly applies a Hadamard gate prior to her own measurement, she will get either 0 or 1 with equal probability, regardless of Alice's original value. Therefore, Bob may measure the wrong value with a 50% chance. If this is a qubit that Alice and Bob check, again they have a 50% chance to catch Eve. Secondly, Alice may send a qubit in the Hadamard basis. If Eve mistakenly measures the qubit directly she again produces a qubit on which she may be caught with a chance

of 50%. Therefore, on each qubit that Eve wrongly disturbs, she is caught 50% of the times. As she is disturbing half the qubits on average, Eve is caught with a probability of 25% on each qubit she chooses to observe. Or else, on each qubit that Eve decides to observe and Bob decides to check, Eve remains undetected with a probability of $75\% = \frac{3}{4}$.

Suppose, there are n qubits in the signature string. They are observed by Eve and checked by Bob. Eve remains undetected with a probability of $(\frac{3}{4})^n$. Therefore Bob's detection rate over n qubits is given by the formula $rate = 1 - \left(\frac{3}{4}\right)^n$.

Nevertheless, if Eve gets lucky enough to remain undetected, then she will gain access to the rank and encoding basis of each bit in the message. This means that she can put the bits in the correct order, but she can only be certain about their value for half of them, the ones for which she correctly guessed the encoding basis. For example, if Eve listens to n qubits, she is certain of the value of $\frac{n}{2}$ qubits. Thus, her *information gain* is $50\% = \frac{1}{2}$.

Note that the probability for Eve to remain undetected may be very low; for example, if the signature string is 25 bits long, Eve remains undetected with a probability of about 0.075%.

2.2 Translucent Eavesdropping

Alternatively, Eve could try a more insidious eavesdropping strategy, avoiding a direct measurement on the qubits in transit through the quantum channel. This can be achieved by making a copy of each qubit or entangling each qubit to one of her own, before sending the original further on to Bob. Since the two encoding bases are complementary, no quantum circuit exists that can accurately duplicate all four base vectors (no-cloning theorem). For example, the Controlled-NOT (CNOT) gate acts as a cloning gate for qubits encoded in the computational basis, but creates as entangled pair $\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ whenever we push a quantum state like $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ through it. Consequently, each qubit originally encoded by Alice in the Hadamard basis, will arrive at Bob entangled with a corresponding qubit in Eve's possession. Now when Bob applies a Hadamard gate on his half of the entanglement, in order to decode the qubit, he effectively transforms the state of the Bob-Eve ensemble as follows: $H \otimes I \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$, and $H \otimes I \left(\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle\right) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)$.

When any of the two quantum states above is measured by Bob in the normal computational basis, the entanglement will collapse to one of the four basis vectors $\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$ and Bob will have a 50% chance to obtain the correct bit value, the one originally encoded by Alice. Consequently, the detection rate for translucent eavesdropping is the same as the one derived for opaque eavesdropping.

2.3 Lower Levels of Eavesdropping

The above analysis for eavesdropping consequences is based on the assumption that Eve tampers with all qubits transmitted through the quantum channel. Here, tampering with a qubit means either measuring or trying to clone it. If Eve is caught, she gains no knowledge whatsoever about the content of the message. This happens because whenever Eve is caught in Step 4 of Phase II of the protocol, see section 2, the protocol is abandoned. Alice does not reveal the correct order of the qubits and the scrambled message is meaningless both to Eve and Bob.

Consequently, Eve could settle for a more discrete strategy, according to the plan that partial information is better than no information at all. If Eve decides to eavesdrop on a fraction x for the qubits in the quantum encrypted block transmitted, then the detection rate varies with x and with the signature length n as follows:$rate = 1 - \left(\frac{3}{4}\right)^{x \cdot n}$,, where $0 \leq x \leq 1$ and n is the length of the signature, for example $n = 16$ bits long.

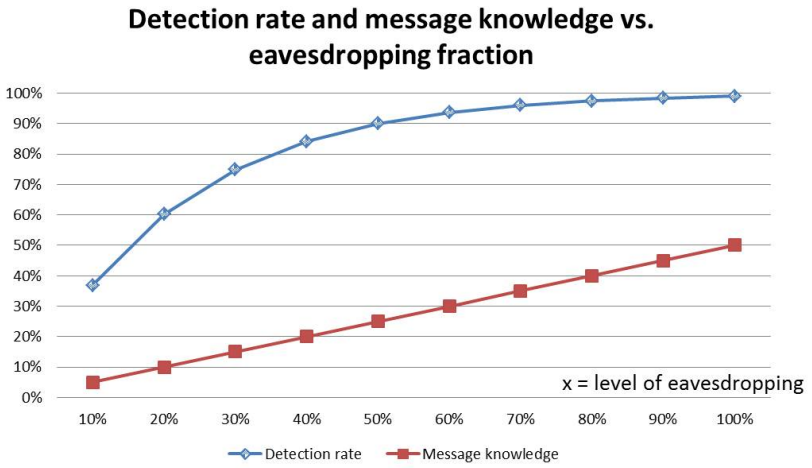

Fig. 2. The graph shows the detection rate together with Eve's information gain. The Ox axis represents x, the percentage of the signature read by Eve. The Oy axis shows both the detection rate and the information gain.

In the eventuality that she remains undetected, the percentage of the message that Eve is certain she has correctly decoded is 50%. Thus the *information gain* on a fraction x is $\frac{x}{2}$ A graph depicting the variation of the detection rate and information gain for various levels of eavesdropping is presented in fig. 2. The graph assumes a constant signature length of 16 bits. A longer signature will, of course, push the detection rates asymptotically closer to the 100% limit.

From Eve's point of view, probably the most pertinent question is: *What is the optimal level of eavesdropping such that the probability of escaping detection and the*

knowledge gained about the message are both maximized? In order to answer this question, we need to find the maximum of a benefit function that quantifies both these quantities. A suitable function is $f_{benefit} : [0,1] \rightarrow [0,1], \quad f_{benefit}(x) = \frac{x}{2}\left(\frac{3}{4}\right)^{x \cdot n}$.

This function was obtained by multiplying the two quantities, probability of escaping detection and the fraction of the message correctly decoded, normalized to the interval $[0,1]$. As it can be seen from fig. 3, this function reaches its maximum for a level of eavesdropping of about 22%, if the signature string consists of 16 bits. This maximum drops to 14% for a 24-bit signature and to around 11% for a 32-bit signature. These data suggest that the best strategy for Eve is to decrease the level of eavesdropping as the size of the signature increases. However, the length of the signature string is disclosed only during the second phase of the protocol, so Eve cannot use this information in planning her eavesdropping strategy.

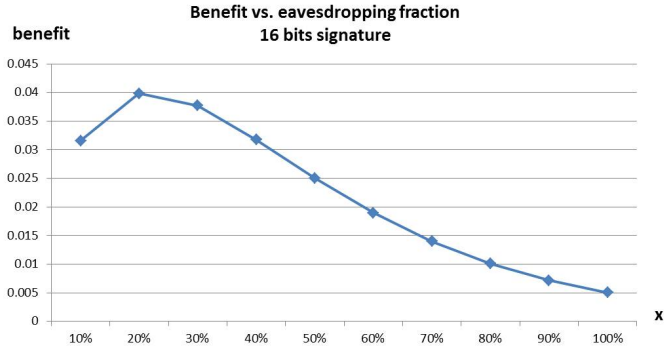

Fig. 3. The benefit of eavesdropping versus the detection rate

3 Encoding in Three Bases

We have discussed an algorithm that reveals the presence of Eve whenever the signature test fails. For each bit of the signature, Eve can be detected with a probability of 25%. This detection rate per qubit is common to all classical key distribution protocols [1] [2]. We hereby propose an encoding scheme that improves the detection rate per qubit to 33%. The improved detection rate comes from encoding each qubit in three complementary bases. While this may seem to increase the complexity in manipulating each qubit, yet the gates used for encoding are common and simple.

The three bases used for encoding are the computational basis, the Hadamard basis, and the phase-shift- Hadamard basis. The phase-shift- Hadamard basis has two gates applied to a qubit: a Hadamard gate and then a $R_{\frac{\pi}{2}}$ rotation.

When Alice wants to send a binary digit 0 or 1, she first prepares a qubit in the computational basis $|0\rangle$ or $|1\rangle$. Then Alice chooses randomly one of the three bases to encode her qubit:

1. The computational basis $|0\rangle$ and $|1\rangle$.
2. The Hadamard basis, $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle$ for 0 and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle$ for 1.
3. The $R_{\frac{\pi}{2}}$-Hadamard basis, $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle$ for 0 and $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle$ for 1.

If Alice chooses the computational basis, she simply sends the qubit to Bob. If Alice chooses the Hadamard basis, then Alice applies a Hadamard gate first and then sends the transformed qubit to Bob. If Alice chooses the $R_{\frac{\pi}{2}}$-Hadamard basis, Alice applies a Hadamard gate then a $\frac{\pi}{2}$ phase shift gate, and then sends the doubly transformed qubit to Bob.

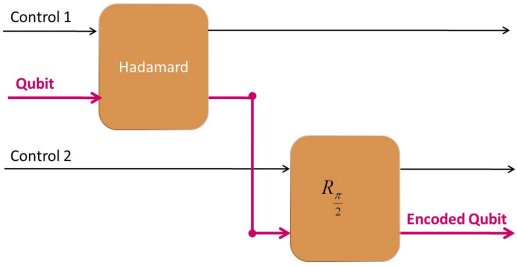

Fig. 4. Encoding of a qubit in three orthogonal bases. The random values of the control qubits 1 and 2 define the actual encoding basis.

As Alice has three options, the choice can be made by two control bits that are set on arbitrary values. Fig. 4 shows the quantum circuit that Alice uses to encode each qubit. The table below shows the encoding basis as given by the values of the two control bits.

Control 1	Control 2	Encoding Basis
0	0	computational basis
0	1	not used
1	0	Hadamard basis
1	1	phase-shift Hadamard basis

According to the protocol, when Bob receives a qubit from Alice, he waits to be informed on the classical channel what encoding basis was used. Then he applies the necessary gates in reverse order: the phase-shift gate first and then the Hadamard gate.

3.1 What Eve Can Do

The eavesdropper can be supposed to know the mechanism of encryption, while not knowing the values of the random control bits.

In opaque eavesdropping, Eve will try to measure the qubit intercepted from Alice and then will further transmit either the measured qubit or a qubit of her

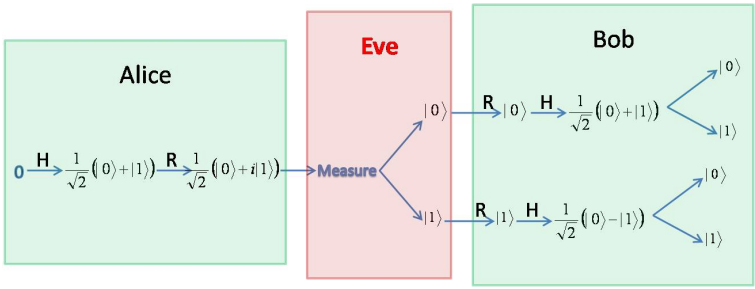

Fig. 5. Alice encodes her qubit in the phase-shift-Hadamard basis. Eve guesses the computational basis. Bob catches Eve with a 50% chance.

choice to Bob. Eve guesses one of the three encoding bases and treats the qubit intercepted from Alice accordingly.

Suppose Eve tries the computational basis. If Alice's qubit is encoded in the computational basis, Eve reads the correct value and remains undetected. If Alice's qubit is encoded in the Hadamard basis, Eve wrongly pushes Alice's qubit through a Hadamard gate and will be detected by Bob in 50% of the cases. This situation was represented in fig. 1. If Alice's qubit was encoded in the phase-shift -Hadamard basis and Eve measures the qubit in the computational basis, Eve destroys the balanced superposition. As in the previous case, Bob can catch Eve with a 50% chance. Fig. 5 shows an example of Alice encoding a binary 0 in the phase-shift-Hadamard basis. Bob, by applying the same steps that Alice did in reverse order will retrieve the initial 0 only 50% of the times. As Alice encodes a qubit randomly in one of the three bases, and Eve reads the stolen qubit in the computational basis, Eve will be caught in two situations with a chance of 50%. This yields an overall probability of $\frac{1}{3}(\frac{1}{2}+\frac{1}{2}) = 33\%$. This chance is considerably higher than 25% offered by two bases encoding.

We supposed that Eve decides to measure the intercepted qubit in the computational basis. If Eve chooses to measure in any other of the three bases, a similar result can be deducted. The detection probability is 33% no matter what basis Eve chooses.

If eavesdropping is tested on a larger signature, the detection rate increases sharply with the length of the signature n: $rate = 1 - \left(\frac{2}{3}\right)^n$.

Fig. 6 shows a comparison on the detection rate for the case of two encoding and three encoding bases respectively. The graph shows that for short signatures, the detection rate for three encoding bases is measurably larger, whereas signatures large than 25 qubits do not benefit from three encoding bases.

Lower Levels of Eavesdropping. Let us study the optimal level of eavesdropping on the three bases encoding scheme. Under the assumption that Eve is not caught, Eve gains the value of the qubits that she has luckily measured in the same basis as Bob. As there are three possible bases, Eve reads correctly $\frac{1}{3}$ of the qubits she intercepts.

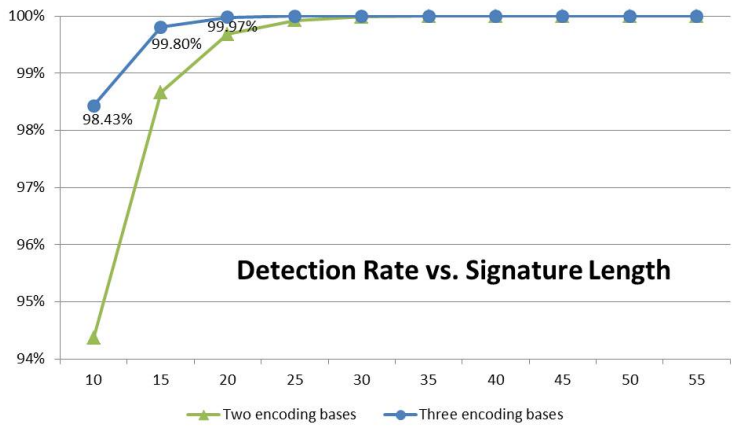

Fig. 6. The graph shows the detection rate versus the signature length for three encoding bases. The Ox axis represents the length of the signature string. The Oy axis shows the probability for Eve to be detected.

Fig. 7. The graph shows the detection rate together with Eve's information gain. The Ox axis represents the percentage of the signature read by Eve. The Oy axis shows both the detection rate and the information gain.

Suppose Eve does not listen to the entire qubit block, but eavesdrops a fraction x. Therefore, she will disturb a fraction x of the signature of length n. The detection rate varies with x according to the following formula $rate = 1 - \left(\frac{2}{3}\right)^{x \cdot n}$.

Also, x affects the information gain, which will be the fraction $\frac{x}{3}$ of the message. Fig. 7 represents both the detection rate and the information gain for the three bases encoding scheme, computed on a signature of 16 bits. The graphs for a two bases encoding are also shown for comparison in the figure, with a thin line. It can be seen that the three base protocol improves over the two base protocol, both in terms of detection rate as well as information gain.

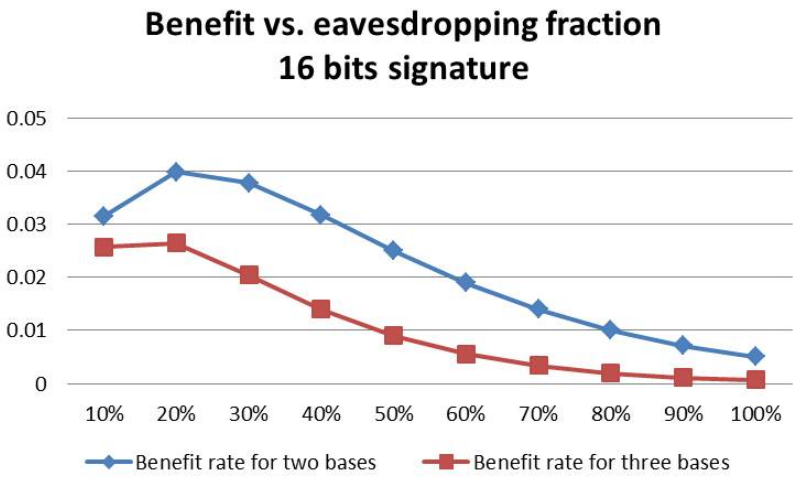

Fig. 8. The benefit of eavesdropping versus the detection rate

In section 2.3, we defined a benefit function that Eve uses to find the optimal level of eavesdropping. For the three bases encoding, the function becomes $f_{benefit} : [0,1] \to [0,1], \quad f_{benefit}(x) = \frac{x}{3}\left(\frac{2}{3}\right)^{x \cdot n}$.

Fig. 8 shows the graph of this function juxtaposed with the graph for the two bases encoding defined in section 2.3. By comparison, we see that the optimal level of eavesdropping is approximately the same, about 22%. Nevertheless, for a three bases encoding scheme the benefit is considerably lower .

4 Conclusion

We have shown that secret communication does not need an encryption key. The previous section contains a protocol that transmits a secret message without encoding the message with a key. The secrecy of the message ensues from randomly scrambling the order of the bits in the message. As the bits are sent in random

order, the scrambled message does not reveal anything about the content of the message. The correct order of the qubits is revealed publicly after the absence of an intruder is checked.

The protocol benefits from the capability of detecting an intruder. This is a major characteristic of all quantum key distribution protocols. The intruder, Eve, leaves an unmistakable mark on the qubits she read: she changes the intended value of the qubit with a certain probability. Our paper has an improved detection rate of Eve from 25% to 33% per intercepted qubit. This is achieved by using three orthogonal encoding bases. Eve's presence is searched on a signature, as in all other protocols.

Our paper gives an extensive analysis on what Eve can do: opaque and translucent eavesdropping, and also low levels of eavesdropping. It studies the advantages of Eve and the maximum benefit Eve can get from a certain signature length.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984, pp. 175–179. IEEE, New York (1984)
2. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Physical Review Letters 68(21), 3121–3124 (1992)
3. Nagy, N., Nagy, M., Akl, S.G.: Key distribution versus key enhancement in quantum cryptography. Parallel Processing Letters 20(03), 239–250 (2010)
4. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press (2000)
5. Lomonaco Jr., S.J.: A Talk on Quantum Cryptography or How Alice Outwits Eve. In: Proceedings of Symposia in Applied Mathematics, Washington, DC, vol. 58, pp. 237–264 (January 2002)
6. Shannon, C.: Communication theory of secrecy systems. Bell System Technical Journal 28(4), 656–715 (1949)