Soft Comput (2016) 20:87–101
DOI 10.1007/s00500-014-1555-7

FOCUS

Quantum-based secure communications with no prior key distribution

Marius Nagy · Naya Nagy

Published online: 18 December 2014

Abstract Current quantum cryptographic protocols aim to distribute a classical secret key to be used afterwards in classical encryption/decryption schemes. We show in this paper that quantum information processing can be used to do much more than just key distribution. Simple quantum transformations augmented with the ability to store qubits in a quantum memory are the building blocks of a class of protocols allowing two parties to communicate secretly by encoding/decoding the exchanged message directly through quantum means, without the need to establish a secret encryption/decryption key first. Consequently, our quantum mechanical process of securely transmitting a message through a public channel is conceptually simpler than the two-step scenario with a quantum distributed classical key. In addition, since the encrypted message is only transmitted through a quantum channel, copying and off-line analysis of the transmission is impossible. Our algorithms rely on the common assumption that public information can be authenticated. In terms of security, the protocol using three encoding bases achieves the maximum detection rate of 33 % per qubit tested. The probability of catching a potential eavesdropper can be brought as close to 1 as desired by increasing the length of the signature string attached to the message.

Communicated by C. M. Vide.

M. Nagy (✉) · N. Nagy
College of Computer Engineering and Science, Prince Mohammad Bin Fahd University, Al Azeziya, Eastern Province, KSA
e-mail: mnagy@pmu.edu.sa

M. Nagy · N. Nagy
School of Computing, Queen's University, Kingston, ON, Canada
e-mail: marius@cs.queensu.ca

N. Nagy
e-mail: nagy@cs.queensu.ca

Keywords Quantum gates · Quantum memory · Measurement · Cryptography · Quantum protocol · Key distribution · Security · Eavesdropping · Intruder detection · Bit rank

1 Introduction

Quantum cryptography has been mainly concerned with quantum key distribution (Bennett 1992; Bennett and Brassard 1984; Bennett et al. 1992; Ekert 1991). Regardless of whether they rely on quantum entanglement or not, all these quantum protocols are used with a single goal: to establish a classical secret key that is subsequently used to encrypt/decrypt a message using classical cryptographic algorithms. Actually, a large body of literature considers the quantum key distribution problem to be in fact a key enhancement (Lomonaco 2000), since a small secret key must already be available to the two communicating parties to authenticate the classical channel. 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.

As we have previously argued in Nagy et al. (2010), true key distribution is possible through quantum means using protected public information to guarantee the authenticity of exchanged messages. In our scheme, the public information that supports authentication is still classical, but an interesting area of research was opened by Gottesman and Chuang, when they proposed a quantum digital signature scheme, based on quantum one-way functions, that employs a public key made up of a set of quantum states (Gottesman and Chuang 2001). The scheme allows for a small number of quantum digital signatures to be shared among potential

recipients. It has the disadvantage of using several copies of the signatures, thus revealing more information about the actual signature to potential malevolent parties. The difficulty of using a quantum public key for a reduced number of times is discussed in Cao (2010). A scheme that does not use quantum memories is proposed in Dunjko et al. (2014). It uses only classical information when sending messages. Thus, signing a message is rather classical, but has good implementation prospects, as can be seen in the implementation-oriented version of the paper (Collins et al. 2014). Non-interactive quantum authentication schemes with classical keys are also studied in Barnum et al. (2002), where an efficient procedure to create purity-testing protocols is given. Finally, the original idea of Gottesman and Chuang was later enhanced by other researchers (Zeng and Keitel 2002; Lu and Feng 2005) to allow general quantum states to be signed, not just classical bitstrings.

After this brief detour on authentication techniques, we come back to the problem of encrypting a message directly through quantum means, which is the main focus of our paper. Although in the protocols developed herein, each physical message contains a signature along with the useful information, this signature plays the role of a sentinel, as it is used for detecting eavesdropping rather than for authentication purposes. The signature is unique for each message, that is, once used for a message it is not used again. Thus our protocols implement one-time signatures.

In any existing quantum key distribution protocol, an important characteristic of the classical secret key is that it is randomly generated. No quantum key distribution scheme can be used to distribute a key that is known a priori to any of the communicating parties. This randomness comes from the implicit randomness associated with the measurement postulate in quantum mechanics. In this paper, we distance ourselves from the very idea of using a key for encryption. We develop a class of protocols that transmit 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 classical bits.

Our protocols come with all the advantages of quantum cryptography. An intruder, Eve, listening to the message being transmitted, destroys the superposition state of the qubits and thus can gain knowledge about it only with a low probability. Also, the intruder is detected by Alice and Bob with an arbitrarily high probability. In addition, our protocols are equivalent to a one-time pad (Shannon 1949). As we use no key, information about the scrambling of the message is of the same order as the message itself. Eavesdropping on one application of the protocol provides no gain to the intruder for any subsequent protocol applications.

We first illustrate our idea with a simple protocol encoding bits in one of two complementary bases and show that the detection rate per qubit checked is 25 % (same as in Bennett and Brassard 1984; Bennett 1992). We then extend the encoding strategy to three complementary bases, which improves the detection rate per qubit to 33 %. Finally, we describe a general quantum protocol in which the encoding basis is arbitrary (not chosen from a pre-defined discrete set). In all three protocols, the step of establishing and distributing a cryptographic key is no longer needed. Together with the fact that we are using only simple unary quantum gates, the whole process of securely transmitting a message between two communicating parties becomes greatly simplified and streamlined. By comparison, the RSA algorithm (Rivest et al. 1978) used to just distribute the secret key needed to encrypt/decrypt the actual message through classical means is much more computationally intensive. Moreover, our protocols benefit from the level of security conferred by quantum mechanical properties when the encrypted message is transmitted. The no-cloning theorem makes it impossible for an eavesdropper to copy the transmission without disturbing it and then analyze the transmission off-line. Previous protocols benefit from this quantum level of security just for the key distribution step, the encrypted message is still transmitted through a classical channel, which is subject to all classical ways of attack.

Beside simple quantum gates, our scheme also relies on the use of a quantum memory capable of storing qubits (described by their quantum states) for a certain amount of time as detailed in the description of the protocol. Although building such a quantum memory is a challenging endeavor in practice, important steps in this direction have been recently reported (Gisin et al. 2011; Tittel et al. 2011; Lukin et al. 2012; Steger et al. 2012). Any practical implementation of a quantum protocol aimed at securing communications has to find an appropriate physical embodiment for the qubits transmitted over the quantum channel. The best choice in this respect seems to be photons, whose polarizations can easily be manipulated and which are, by definition, very fast, traveling at the speed of light. On the other hand, photons are not well suited for storage, where solid-state approaches seem to be the most promising technology.

Now, two separate teams, one led by Wolfgang Tittel at the University of Calgary in Alberta, Canada (Tittel et al. 2011) and another led by Nicolas Gisin at the University of Geneva in Switzerland (Gisin et al. 2011) are reporting advances on the road to make the two technologies work together. Experimenting with different types of crystals, they managed to have the quantum state of a photon being captured in solid crystals through entanglement. Furthermore, scientists at Harvard University have developed a room-temperature quantum memory that can hold information on the order of seconds by using the spin of the nucleus of an atom inside a diamond to physically realize a qubit (Lukin et al. 2012). But the record on how long a superposition state can be main-

tained definitely belongs to a team led by Professor Mike Thewalt of Simon Fraser University, Canada (Steger et al. 2012). Using the spins of atomic nuclei embedded in silicon, the research team was able to create a superposition state which lasted for 192 s (more than 3 min). These advances seem to hint to the possibility of practical realizations for protocols using quantum memories (like the one described in this paper) in the near future.

The remainder of the paper is organized as follows. Section 2 presents a simple keyless protocol that securely transmits a message from a source to a destination. It also analyzes the protocol's protection from the intruder's actions including a formal proof of security. 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 using an encoding in three complementary bases. A generalized encoding scheme where the encoding basis can be any ortho-normal basis spanning a two-dimensional Hilbert space is presented in Sect. 4. Finally, Sect. 5 offers some conclusions and highlights the main ideas that made the results in this paper possible.

2 Keyless quantum message transmission

In this section, we describe in detail the inner workings of a protocol that allows two parties (commonly referred to as 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. To communicate secretly, the two parties are assumed to have access to the following resources:

- a public quantum channel capable of delivering a block of qubits from Alice to Bob. This could be a fiber-optic cable or even air, depending on the particular physical embodiment chosen for a qubit. No particular restrictions are imposed on the quantum channel. In particular, it is open to any form of eavesdropping.
- a public classical channel that allows Alice and Bob to communicate with each other, exchanging classical information. Although this channel is also public and open to eavesdropping, it is authenticated. This means that Alice has the certainty of speaking to (communicating with) Bob and Bob has the certainty of speaking to Alice.
- a quantum memory required by Bob to store the qubits sent by Alice until the signature is verified and they can be decrypted.
- the ability to perform quantum information processing, namely applying single-qubit gates and measurements in the normal computational basis $\{|0\rangle, |1\rangle\}$. Note that this is not equivalent to the power of a general quantum computer, since two-qubit gates are required for universal quantum computation.

The main steps of the protocol are given next. Also, a graphical representation of the information flow during the unfolding of the protocol is depicted in Fig. 1.

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 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. The analysis below clearly shows that 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

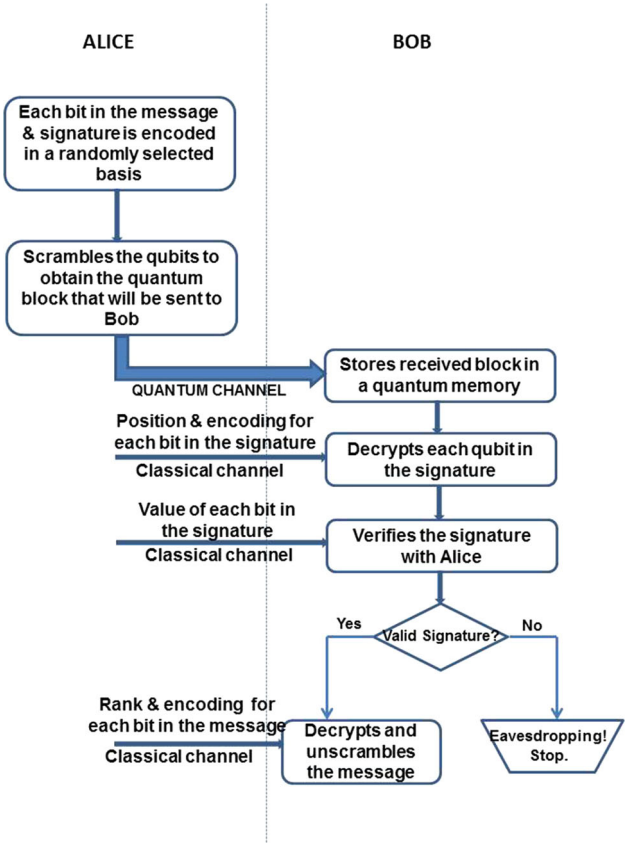

Fig. 1 Information flow diagram outlining the steps of the communication protocol using two bases

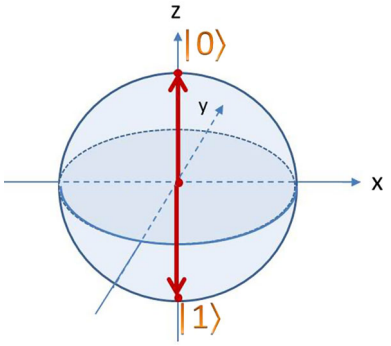

Fig. 2 Normal computational basis

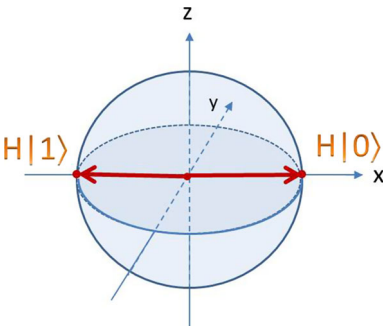

Fig. 3 Hadamard basis

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" $\left\{H|0\rangle = \frac{|0\rangle}{\sqrt{2}} + \frac{|1\rangle}{\sqrt{2}}, H|1\rangle = \frac{|0\rangle}{\sqrt{2}} - \frac{|1\rangle}{\sqrt{2}}\right\}$. We note in passing that the BB84 protocol (Bennett and Brassard 1984), which uses photon polarization as qubit embodiment, achieves complementarity 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 (see Fig. 2) and the Hadamard basis (see Fig. 3), 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, 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. 4). 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,

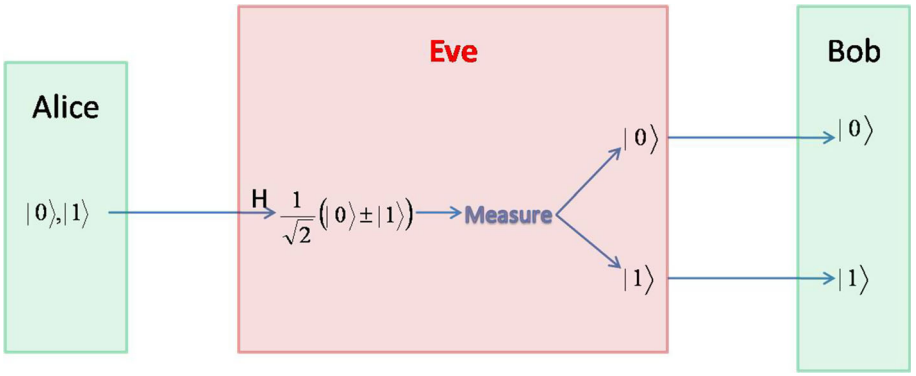

Fig. 4 Opaque eavesdropping. Eve wrongly measures in the Hadamard basis a qubit sent by Alice in the computational basis

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 $\left(\frac{3}{4}\right)^n$. Therefore, Bob's detection rate over n qubits is given by the formula

$$\text{Rate} = 1 - \left(\frac{3}{4}\right)^n . \tag{1}$$

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, to decode the qubit, he effectively transforms the state of the Bob–Eve ensemble as follows:

$$\begin{aligned} &H \otimes I \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) \\ &\quad = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle - |11\rangle\right), \end{aligned} \tag{2}$$

and

$$\begin{aligned} &H \otimes I \left(\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle\right) \\ &\quad = \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle + |11\rangle\right). \end{aligned} \tag{3}$$

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 description at the beginning of Sect. 2), the protocol is abandoned.

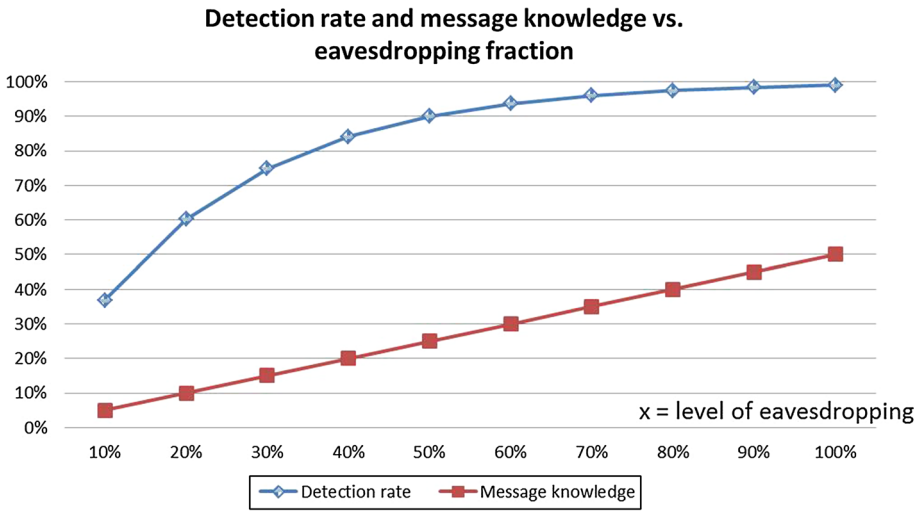

Fig. 5 The graph shows the detection rate together with Eve's information gain for a 16-bit signature. The Ox axis represents x, the percentage of the signature read by Eve. The Oy axis shows both the detection rate and the information gain

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 of the qubits in the quantum encrypted block transmitted, then the detection rate varies with x and with the signature length n as follows:

$$\text{rate} = 1 - \left(\frac{3}{4}\right)^{x \cdot n}, \tag{4}$$

where $0 \leq x \leq 1$ and n is the length of the signature, for example $n = 16$ bits long.

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. 5. 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?* To answer this question, we need to find the maximum of a benefit function that quantifies both these quantities. A suitable function is

$$f_{\text{benefit}} : [0, 1] \to [0, 1], \quad f_{\text{benefit}}(x) = \frac{x}{2}\left(\frac{3}{4}\right)^{x \cdot n}. \tag{5}$$

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. 6, 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.

2.4 Security proof

Having discussed the main eavesdropping strategies for Eve, we close this section with a formal proof of security for our keyless protocol in the special case of single-qubit eavesdropping. As in the case of BB84, the security of the protocol is guaranteed by the very laws of quantum mechanics, namely, the indistinguishability of non-orthogonal quantum states, the no-clonability theorem and the measurement postulate. Since the qubits passing through the quantum channel are encoded in complementary bases, there is no quantum circuit Eve can use to consistently make copies of them or entangle them with her measuring apparatus. To extract information, Eve has to perform a measurement that will inevitably alter the state of the qubit, an act which opens the possibility for Bob to detect the intrusion.

Formally, any signature qubit on which Eve decides to eavesdrop is in a state $|\varphi\rangle$ taken from the set $\{|0\rangle, |1\rangle, H|0\rangle, H|1\rangle\}$. In general, the act of eavesdropping on a qubit can be modeled by first applying some unitary transformation U followed by a von Neumann measurement in an orthonormal basis $\{|m_1\rangle, |m_2\rangle\}$. Note that this model is general enough to also cover strategies in which Eve may attempt to copy the quantum state of the qubit or entangle it with her measurement apparatus. According to the measurement postulate of quantum mechanics, the probability of obtaining result m_i is

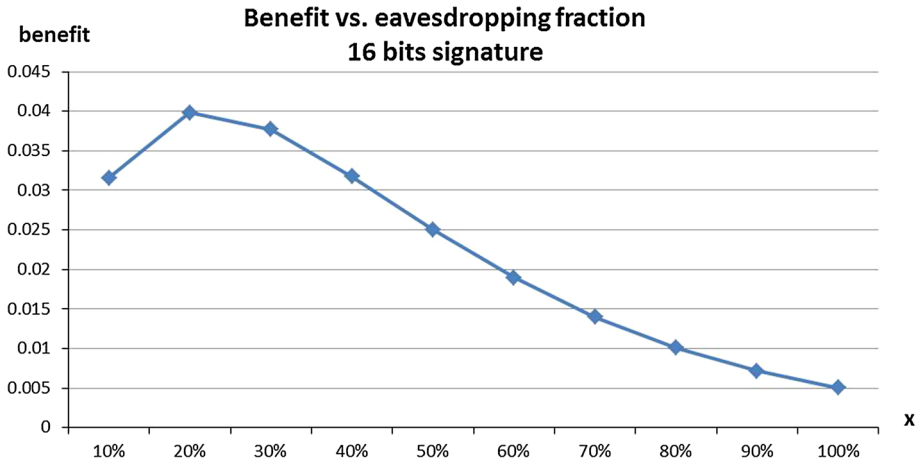

Fig. 6 The benefit of eavesdropping versus the detection rate

$$p(m_i) = \langle\varphi|U^\dagger P_{m_i} U|\varphi\rangle, \tag{6}$$

where $P_{m_i} = |m_i\rangle\langle m_i|$ is the projector associated with measurement outcome m_i.

The qubit eavesdropped upon, now in state $|m_i\rangle$, is again measured by Bob and the outcome verified with Alice. The measurement applied by Bob is again a projective measurement, either in the normal or Hadamard basis. This process can be viewed as a measurement of observable

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{7}$$

with eigenvectors $|0\rangle$ and $|1\rangle$ on the state $V|m_i\rangle$, where $V = I$, if Bob measures in the normal computational basis, and $V = H$, if Bob measures in the Hadamard basis.

The only chance for Eve to consistently pass the verification test between Alice and Bob is that state $|m_i\rangle$ coincides with the initial state $|\varphi\rangle$ prepared by Alice. In other words, the quantum state of the qubit is not altered by the eavesdropping action. However, according to the laws of quantum mechanics, the vectors in the normal computational basis $\{|0\rangle, |1\rangle\}$ cannot be reliably distinguished from the vectors in the Hadamard basis $H|0\rangle, H|1\rangle\}$ because they are non-orthogonal. Consequently, for each qubit "observed" by Eve, there is a non-zero probability that $|m_i\rangle \neq |\varphi\rangle$, which translates into a non-zero probability p_d that what Bob observes upon measuring this qubit is different from what Alice has prepared.

From the point of view of ensuring the security of the protocol, the actual value of p_d is irrelevant as long as $p_d > 0$. This is because the length of the signature string n acts as a security parameter that can bring the probability of catching Eve as close to 1 as desired:

$$\lim_{n\to\infty} (1 - (1 - p_d)^n) = 1. \tag{8}$$

Even if the exact value of p_d does not affect the security of the protocol, it affects its efficiency. Consequently, in the next section, we show how the efficiency of the protocol can be improved by encoding each bit in one of three complementary bases.

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 (Bennett and Brassard 1984; Bennett 1992). 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. Note that this detection rate is optimal, since we cannot select more than three pairwise complementary bases for the state space of a qubit. Expressing this in the geometry of the Bloch sphere, we cannot have more than three lines going through the center of the sphere that are perpendicular to each other.

While working with three bases may seem to increase the complexity in manipulating each qubit, the gates used for encoding are common and simple. More precisely, in the following protocol, 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 (see Fig. 7).

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.

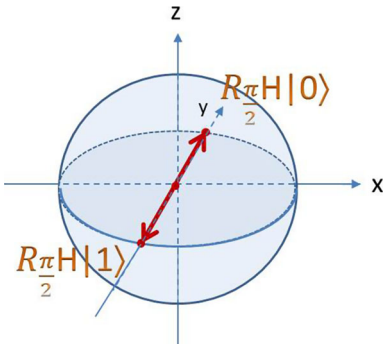

Fig. 7 The phase-shift Hadamard basis

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 she 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.

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 random encoding basis.

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 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 is represented in Fig. 4. 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. Figure 8 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 $\frac{1}{3}\left(\frac{1}{2}+\frac{1}{2}\right) = 33\,\%$. 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 obtained. 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:

$$\text{rate} = 1 - \left(\frac{2}{3}\right)^n. \tag{9}$$

Figure 9 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.

3.2 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.

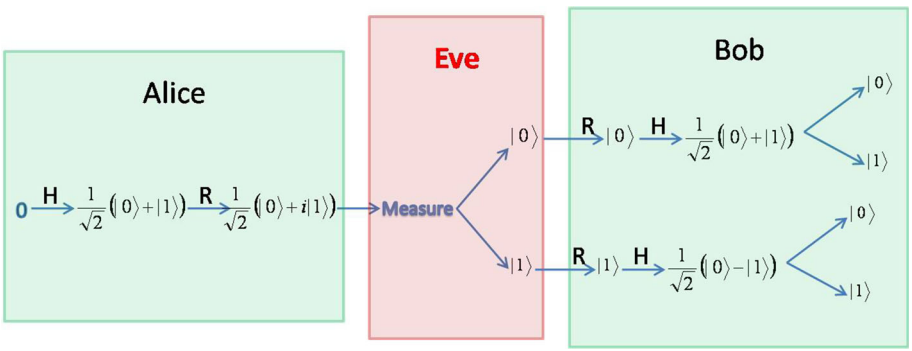

Fig. 8 Alice encodes her qubit in the phase-shift-Hadamard basis. Eve guesses the computational basis. Bob catches Eve with a 50 % chance

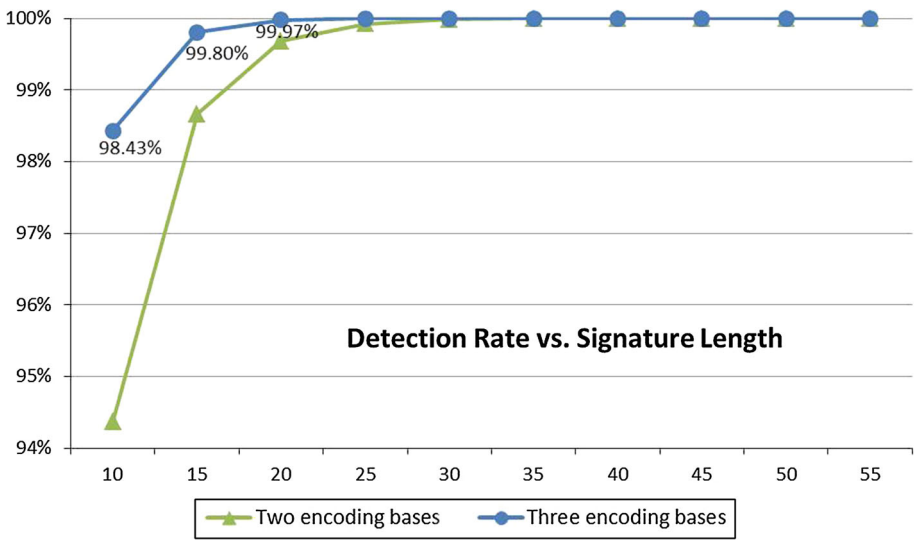

Fig. 9 The graph shows the detection rate versus the signature length for three encoding bases. The Ox axis represents the length of the signature string. The Oy axis shows the probability for Eve to be detected

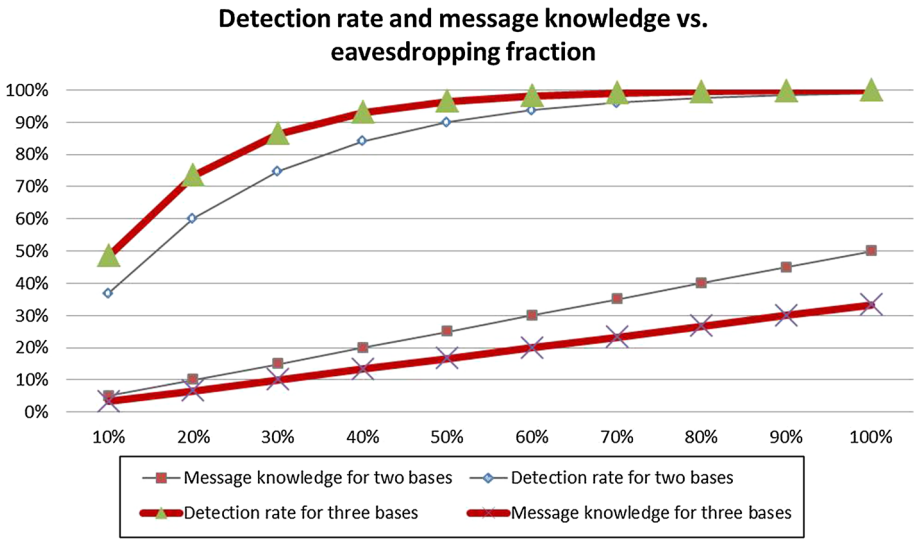

Fig. 10 The graph shows the detection rate together with Eve's information gain for a 16-bit signature. The Ox axis represents the percentage of the signature read by Eve. The Oy axis shows both the detection rate and the information gain

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

$$\text{rate} = 1 - \left(\frac{2}{3}\right)^{x \cdot n}. \tag{10}$$

Also, x affects the information gain, which will be the fraction $\frac{x}{3}$ of the message. Figure 10 represents both the detection rate and the information gain for the three bases encoding scheme, computed on a signature of 16 bits. In the figure, we also show with a thin line the graphs for encoding in two bases, for comparison purposes. It can be seen that the three bases protocol improves over the two bases protocol, both in terms of detection rate as well as information gain.

In Sect. 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

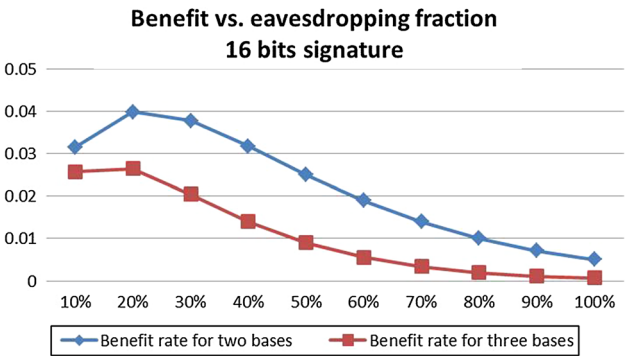

Fig. 11 The benefit of eavesdropping versus the detection rate

$$f_{\text{benefit}} : [0, 1] \to [0, 1], \quad f_{\text{benefit}}(x) = \frac{x}{3}\left(\frac{2}{3}\right)^{x \cdot n}. \tag{11}$$

Figure 11 shows the graph of this function juxtaposed with the graph for the two bases encoding defined in Sect. 2.3. By

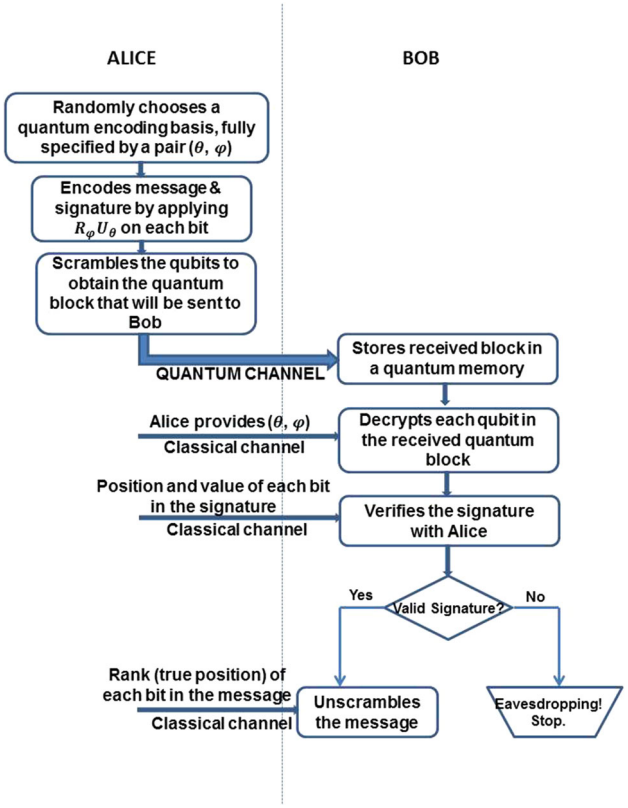

Fig. 12 Information flow diagram outlining the steps of the generalized communication protocol

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 Generalization to an arbitrary basis

In the previous two sections, we have described and analyzed two protocols sharing the same idea of a random choice for the encoding basis. The first protocol uses two complementary bases while the second protocol uses three complementary bases. In this section, we describe a general quantum communication protocol in which the encoding basis can be any ortho-normal basis spanning a two-dimensional Hilbert space.

The information flow diagram describing the steps of this generalized protocol is given in Fig. 12. The process starts with Alice choosing an encoding basis for the bitstring she wants to send to Bob. This bitstring is formed by the actual message to which a signature bitstring is appended. The signature will allow Alice and Bob to detect anyone trying to eavesdrop on the transmitted message. This means that every bit in the plaintext block (message and signature) will be converted to one of the two basis vectors of the quantum basis

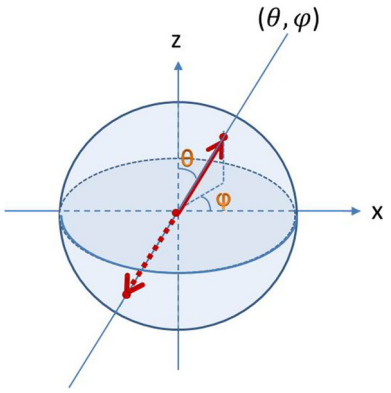

Fig. 13 Encoding basis is a straight line through the center of the Bloch sphere, specified by a pair (θ, φ)

chosen. An intuitive graphical representation of an encoding basis is a straight line going through the center of the Bloch sphere. Such a line is fully specified by two real-valued parameters: the angle θ between the line and the z axis, and the angle φ between the projection of the line on the equatorial plane and the x axis (see Fig. 13). In some sense, this encoding method is somewhat similar to anamorphosis, since the actual message can only be "seen" when viewed from the proper angle. With the major difference that attempting to "read" the message from any angle except the correct one is equivalent to a quantum measurement that will necessarily alter the message.

Therefore, to choose an encoding basis, Alice needs to decide on a pair (θ, φ). For example, the pair $(0, 0)$ specifies the computational basis, described by the two basis vectors $|0\rangle$ and $|1\rangle$ aligned along the z axis (see Fig. 2). Alternatively, pair $(\pi/2, 0)$ specifies the Hadamard basis, described by basis vectors $H|0\rangle = (1/\sqrt{2})|0\rangle + (1/\sqrt{2})|1\rangle$ and $H|1\rangle = (1/\sqrt{2})|0\rangle - (1/\sqrt{2})|1\rangle$, aligned along the x axis (see Fig. 3). As a last example, pair $(\pi/2, \pi/2)$ specifies an encoding basis whose base vectors are $(1/\sqrt{2})|0\rangle + (i/\sqrt{2})|1\rangle$ and $(1/\sqrt{2})|0\rangle - (i/\sqrt{2})|1\rangle$. Note that these two vectors are oriented in opposite directions along the y axis (see Fig. 7).

In general, for an arbitrarily chosen encoding basis (θ, φ), each 0 bit in the plaintext is embodied in a qubit with the quantum state

$$|\Psi_0\rangle = R_\varphi U_\theta |0\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle. \tag{12}$$

Similarly, a qubit in the quantum state

$$|\Psi_1\rangle = R_\varphi U_\theta |1\rangle = \sin\frac{\theta}{2}|0\rangle - e^{i\varphi}\cos\frac{\theta}{2}|1\rangle \tag{13}$$

will carry a value of 1. The quantum operations (gates) U_θ and R_φ are described by the following matrices:

$$U_\theta = \begin{bmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & -\cos\frac{\theta}{2} \end{bmatrix}; \; R_\varphi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}. \tag{14}$$

Once the plaintext is properly encoded, Alice will scramble the qubits so that signature qubits are scattered throughout and interspersed with message qubits. Consequently, the original ordering of bits in the message and in the signature (the rank of each bit) will no longer be preserved after the scrambling process. Whatever the scrambled quantum block is, Alice will send it through the quantum channel over to Bob, who will store each qubit received in a quantum memory, in the order they arrive. With this step, the quantum communication part of the protocol, that is, communication through the quantum channel is over. In the second phase, all communication between Alice and Bob is carried out through the public authenticated classical channel.

This second phase starts with Alice disclosing to Bob the exact encoding basis that she used to encrypt the plaintext. With this information Bob is able to decrypt each qubit (whether belonging to the message or to the signature) stored in his quantum memory. Next, Alice shares with Bob the position and value of each bit in the signature string. In this way, they can verify that the signature string received by Bob matches exactly the one sent by Alice. A perfect match will be taken as proof that the encoded quantum block was not tampered with while in transit, or at least not to a significant level. Of course, a potential eavesdropper may remain undetected if she is lucky enough not to disturb the quantum states of the qubits in the signature. But this probability can be made arbitrarily small by increasing the signature length.

Finally, if the verification step reveals no trace of an eavesdropper, Alice informs Bob about the rank (actual position) of each bit in the message string. This allows Bob to re-arrange the bits in the proper order and thus recover the original message.

4.1 Analysis

In what follows, we analyze the security of the protocol by investigating the effects of a possible eavesdropping act on the quantum and classical communication channels. Since the quantum channel is public, an eavesdropper (conventionally named Eve) may choose to act on any of the qubits passing by on their way from Alice to Bob. For concreteness, but without loss of generality, let us analyze the scenario in which Eve eavesdrops on a qubit encoding the value 0. The other case, in which a qubit encodes a 1 is perfectly similar.

The quantum state of a qubit embodying a 0 is $|\Psi_0\rangle$ (see Eq. 12). When Eve intercepts this qubit, she may try to measure it directly in the computational basis or try to guess what the encoding basis may have been, so that she can decrypt the qubit before measuring it. Let us denote the encoding basis (the one chosen by Alice) by (θ_A, φ_A) and label the basis guessed by Eve (θ_E, φ_E). Trying to decrypt the qubit, Eve applies $R_{-\varphi_E}$ followed by U_{θ_E} to $|\Psi_0\rangle$ altering the qubit state as follows:

$$
\begin{aligned}
U_{\theta_E} R_{-\varphi_E}|\Psi_0\rangle &= U_{\theta_E}\left(\cos\frac{\theta_A}{2}|0\rangle + e^{i(\varphi_A-\varphi_E)}\sin\frac{\theta_A}{2}|1\rangle\right)\\
&= \left(\cos\frac{\theta_E}{2}\cos\frac{\theta_A}{2} + e^{i(\varphi_A-\varphi_E)}\sin\frac{\theta_E}{2}\sin\frac{\theta_A}{2}\right)|0\rangle\\
&\quad + \left(\sin\frac{\theta_E}{2}\cos\frac{\theta_A}{2} - e^{i(\varphi_A-\varphi_E)}\cos\frac{\theta_E}{2}\sin\frac{\theta_A}{2}\right)|1\rangle \quad (15)
\end{aligned}
$$

Consequently, Eve will now measure a 0 with probability

$$
\begin{aligned}
p^0_{\text{Eve}} &= |\cos\frac{\theta_E}{2}\cos\frac{\theta_A}{2} + e^{i(\varphi_A-\varphi_E)}\sin\frac{\theta_E}{2}\sin\frac{\theta_A}{2}|^2\\
&= \cos^2\frac{\theta_A-\theta_E}{2} - \frac{1}{2}\sin\theta_E\sin\theta_A(1-\cos\Delta\varphi) \quad (16)
\end{aligned}
$$

and a 1 with probability

$$
\begin{aligned}
p^1_{\text{Eve}} &= |\sin\frac{\theta_E}{2}\cos\frac{\theta_A}{2} - e^{i(\varphi_A-\varphi_E)}\cos\frac{\theta_E}{2}\sin\frac{\theta_A}{2}|^2\\
&= \sin^2\frac{\theta_A+\theta_E}{2} - \frac{1}{2}\sin\theta_E\sin\theta_A(1+\cos\Delta\varphi) \quad (17)
\end{aligned}
$$

where $\Delta\varphi = \varphi_A - \varphi_E$.

Eve is aware that her actions may have modified the state of the qubit, so before sending it further on to Bob, she will try to undo the consequences of her eavesdropping by applying U_{θ_E} followed by R_{φ_E}. Therefore, what Bob receives (from Eve) is a qubit in the state

$$
|\Phi_0\rangle = \cos\frac{\theta_E}{2}|0\rangle + e^{i\varphi_E}\sin\frac{\theta_E}{2}|1\rangle \quad (18)
$$

with probability p^0_{Eve}, or in the state

$$
|\Phi_1\rangle = \sin\frac{\theta_E}{2}|0\rangle - e^{i\varphi_E}\cos\frac{\theta_E}{2}|1\rangle \quad (19)
$$

with probability p^1_{Eve}.

Assuming that the qubit comes straight from Alice, Bob now applies $R_{-\varphi_A}$ and U_{θ_A} to decode it:

$$
\begin{aligned}
U_{\theta_A} R_{-\varphi_A}|\Phi_0\rangle &= \left(\cos\frac{\theta_A}{2}\cos\frac{\theta_E}{2} + e^{i(\varphi_E-\varphi_A)}\sin\frac{\theta_A}{2}\sin\frac{\theta_E}{2}\right)|0\rangle\\
&\quad + \left(\sin\frac{\theta_A}{2}\cos\frac{\theta_E}{2} - e^{i(\varphi_E-\varphi_A)}\cos\frac{\theta_A}{2}\sin\frac{\theta_E}{2}\right)|1\rangle \quad (20)\\
U_{\theta_A} R_{-\varphi_A}|\Phi_1\rangle &= \left(\cos\frac{\theta_A}{2}\sin\frac{\theta_E}{2} - e^{i(\varphi_E-\varphi_A)}\sin\frac{\theta_A}{2}\cos\frac{\theta_E}{2}\right)|0\rangle\\
&\quad - \left(\sin\frac{\theta_A}{2}\sin\frac{\theta_E}{2} + e^{i(\varphi_E-\varphi_A)}\cos\frac{\theta_A}{2}\cos\frac{\theta_E}{2}\right)|1\rangle \quad (21)
\end{aligned}
$$

When measuring $U_{\theta_A} R_{-\varphi_A}|\Phi_0\rangle$, Bob will obtain 0 with probability p^0_{Eve}. Similarly, if the state of the qubit received by Bob is $|\Phi_1\rangle$, he will measure a 0 with probability p^1_{Eve}. Overall, the probability that Bob correctly decodes the qubit and obtains a 0 is $(p^0_{\text{Eve}})^2 + (p^1_{\text{Eve}})^2$. In this case, Eve's eavesdropping activity remains undetected. The probability of detection on a single qubit is therefore:

$$
p_{d,1} = 1 - ((p^0_{\text{Eve}})^2 + (p^1_{\text{Eve}})^2) = 2p^0_{\text{Eve}}p^1_{\text{Eve}} = 2p^0_{\text{Eve}}(1 - p^0_{\text{Eve}}) \quad (22)
$$

This probability achieves its maximum of 1/2 when $p^0_{\text{Eve}} = p^1_{\text{Eve}} = 1/2$. This happens when the basis guessed by Eve (θ_E, φ_E) is "maximally non-orthogonal" to the basis (θ_A, φ_A) chosen by Alice. In BB84 (Bennett and Brassard 1984), for example, this maximum non-orthogonality is realized by choosing horizontal/vertical together with diagonal polarization. In terms of the Bloch sphere representation, two bases are "maximally non-orthogonal" if the two straight lines corresponding to the two bases are perpendicular to each other. On the other hand, the detection probability is 0, when Eve chooses the same basis as Alice ($p^0_{\text{Eve}} = 1$) or an orthogonal basis in which the roles of the two basis vectors are reversed ($p^0_{\text{Eve}} = 0$).

When Alice uses a signature bitstring of length n, the probability of detecting the disruptions caused by eavesdropping on the qubits encoding the signature grows to

$$p_{d,n} = 1 - ((p^0_{\text{Eve}})^2 + (p^1_{\text{Eve}})^2)^n \tag{23}$$

Since $(p^0_{\text{Eve}})^2 + (p^1_{\text{Eve}})^2 = 2(p^0_{\text{Eve}})^2 - 2p^0_{\text{Eve}} + 1 \in (0, 1]$, it follows that

$$\lim_{n\to\infty} p_{d,n} = 1, \tag{24}$$

except for the particular case when Eve correctly guesses the encoding basis ($p^0_{\text{Eve}} = 1$ or $p^1_{\text{Eve}} = 1$) and remains undetected ($p_{d,1} = p_{d,n} = 0$). Consequently, the longer the signature string is, the larger the number of qubits that are tested for eavesdropping and the higher the probability to catch a potential eavesdropper.

4.2 Opaque eavesdropping

In the previous section, we have analyzed a rather elaborate scheme for Eve to hide her presence and make her eavesdropping actions transparent to Alice and Bob. Even with all those precautions, we have seen that the detection rate can be pushed as high as desired by increasing the number of bits tested for eavesdropping in the signature string. In this section, we investigate a more direct, opaque eavesdropping strategy in which Eve directly measures some or all of the qubits traveling through the quantum channel from Alice to Bob.

Again, without loss of generality, let us assume Eve intercepts a qubit encoding a value of 0. Such a qubit is described by quantum state $|\Psi_0\rangle$ (see Eq. 12). Upon measuring this qubit in the normal computational basis, Eve will observe a 0 with probability $p^0_{\text{Eve}} = \cos^2(\theta/2)$ and a 1 with probability $p^1_{\text{Eve}} = \sin^2(\theta/2)$, where θ is one of the two parameters characterizing the encoding basis chosen by Alice. According to the measurement postulate of quantum mechanics, the post-measurement state of the qubit must be compatible with the measurement outcome, so Eve will pass on to Bob a qubit in state $|0\rangle$ (with probability p^0_{Eve}) or a qubit in state $|1\rangle$ (with probability p^1_{Eve}).

During the second phase of the protocol, after Alice has disclosed the encoding basis, Bob can proceed to decrypt the received qubits. Note that at this time, although Eve can also eavesdrop on the classical communication channel and thus gain knowledge of θ and φ, the message qubits are no longer in her possession, so there is nothing else she can do to increase her knowledge about the transmitted message. By applying $R_{-\varphi}$ and U_θ to the received qubit, Bob will evolve its quantum state to

$$U_\theta R_{-\varphi}|0\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle \tag{25}$$

with probability p^0_{Eve}, or to

$$U_\theta R_{-\varphi}|1\rangle = U_\theta(e^{-i\varphi}|1\rangle) = e^{-i\varphi}(\sin\frac{\theta}{2}|0\rangle - \cos\frac{\theta}{2}|1\rangle) \tag{26}$$

with probability p^1_{Eve}. A measurement on these quantum states will yield a 0 (correct decoding) with probability

$$\cos^4\frac{\theta}{2} + \sin^4\frac{\theta}{2} = 1 - 2\sin^2\frac{\theta}{2}\cos^2\frac{\theta}{2} = 1 - \frac{\sin^2\theta}{2} \tag{27}$$

and a 1 (incorrect decoding) with probability $\frac{1}{2}\sin^2\theta$. Consequently, the eavesdropping detection probability per qubit varies between 0 (realized when $\theta = 0$) and 1/2 (achieved for $\theta = \pi/2$). In other words, Eve remains undetected when the encoding basis coincides with the normal computational basis; on the other hand, there is a 50 % probability of detecting the actions of Eve if the encoding basis is "maximally non-orthogonal" to the normal computational basis (like the Hadamard basis $\{H|0\rangle, H|1\rangle\}$, for example). Therefore, on average, the detection probability per qubit tested is given by

$$\frac{\frac{1}{2}\int_0^\pi \sin^2\theta d\theta}{\pi} = \frac{\int_0^{\frac{\pi}{2}} \sin^2\theta d\theta}{\pi} = \frac{1}{4} \tag{28}$$

As in the more complex scenario discussed before, this probability can be brought as close to 1 as desired by increasing the number of qubits tested for eavesdropping (the signature string).

Another interesting question in this analysis is: How much information from the transmitted message can Eve gain, assuming that she remains undetected? The condition to remain undetected is essential for Eve. Otherwise, Alice will not disclose to Bob the rank (correct position) of each qubit in the message and consequently, the information gain for Eve is null, even if she has correctly decoded each qubit.

A measure of the information gain is $1 - H_{bin}(p^0_{\text{Eve}})$, where $H_{bin}(p^0_{\text{Eve}})$ is the binary entropy associated with the probability of seeing a 0 when measuring a qubit that encodes a 0. We can express this information gain as a function of the

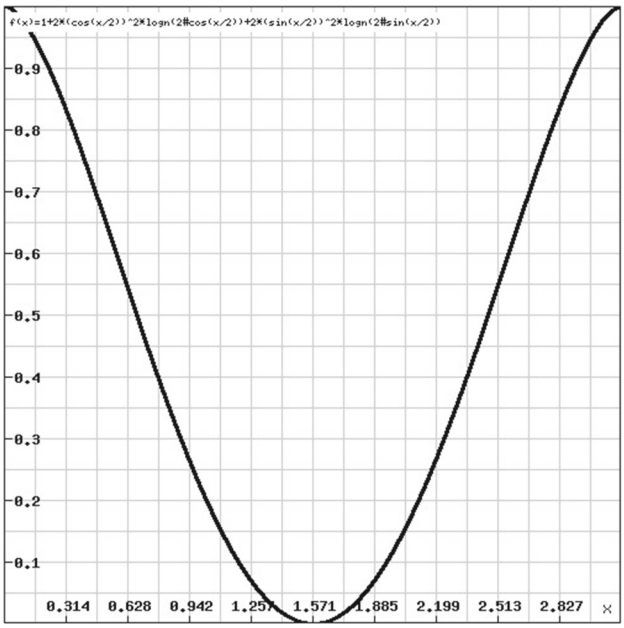

Fig. 14 Information gain as a function of the encoding angle θ

parameter θ as follows:

$$1 - H_{bin}(p^0_{\text{Eve}}) = 1 + p^0_{\text{Eve}} \log p^0_{\text{Eve}} + \left(1 - p^0_{\text{Eve}}\right) \times \log\left(1 - p^0_{\text{Eve}}\right) = 1 + \cos^2\frac{\theta}{2}\log\cos^2\frac{\theta}{2} + \sin^2\frac{\theta}{2} \times \log\sin^2\frac{\theta}{2} = 1 + 2\cos^2\frac{\theta}{2}\log\cos\frac{\theta}{2} + 2\sin^2\frac{\theta}{2}\log\sin\frac{\theta}{2} \tag{29}$$

The graph of this function is depicted in Fig. 14. When Eve performs a direct measurement in the normal computational basis on a qubit encoding a 0, she can be certain of the observed value for an encoding angle θ of 0 or π. On the other extremity, when $\theta = \frac{\pi}{2}$, the measurement provides no information gain whatsoever. From Eve's point of view, the message bit could still be a 0 or a 1, with equal probability. On average, the information gain is given by

$$\frac{\int_0^{\pi}\left(1 + 2\cos^2\frac{\theta}{2}\log\cos\frac{\theta}{2} + 2\sin^2\frac{\theta}{2}\log\sin\frac{\theta}{2}\right)d\theta}{\pi} \approx 0.44 \tag{30}$$

4.3 Variations

The role of the signature string in this general protocol is to ensure (with a certain probability, which can be made arbitrarily large) its security or, in other words, the secrecy of the communication between Alice and Bob. To this end, the bits forming the signature are treated in exactly the same way as the bits composing the actual message: they are scrambled together and encoded according to a chosen basis (θ, φ). Consequently, when attempting an eavesdropping, Eve has no knowledge whatsoever if the bit she tampers with is part of the signature or part of the message. Ideally, she would like to eavesdrop only on the message bitstring to avoid detection and maximize her knowledge on the message transmitted. Unfortunately for her, the information gain is directly proportional to the probability of being detected, so Eve has to think twice before deciding to eavesdrop on a particular qubit.

This property can be used to slightly simplify the protocol such that the bits in the signature string are not encoded (or equivalently, they are encoded in the normal computational basis: 0 becomes $|0\rangle$ and 1 becomes $|1\rangle$). Now Eve can completely avoid detection by choosing to measure the bypassing qubits directly in the standard computational basis. In this way, the quantum states of the signature qubits will not be altered, but the state of any message qubit will be projected to one of the two eigenvectors of the measurement basis: $|0\rangle$ or $|1\rangle$.

Consequently, Alice may pick as encoding basis for the message bitstring the Hadamard basis $(\frac{\pi}{2}, 0)$, which will maximize Eve's uncertainty over each measurement she performs on the message qubits. Effectively, the outcome of each such measurement has a 50 % probability of being correct, which is not better than tossing a fair coin. Therefore, we can confidently say that Eve has zero knowledge about the true value encoded in such a qubit, or equivalently, the binary entropy of such a qubit is 1.

This variant of the protocol, in which the message bits are encoded using the Hadamard basis while the bits in the signature are encoded in the normal computational basis, is reminiscent of BB84 Bennett and Brassard (1984) with its two encoding bases: horizontal/vertical and diagonal that are randomly applied by Alice. Here, as there, it is the "maximum non-orthogonality" of the two bases that keeps Eve in the dark, but this protocol has an important advantage: it can be used to directly encrypt any message without the need to establish a secret key first. Still, the classical channel needs to be authenticated, which is usually done with a small secret key, but it was shown that this requirement is too strong and all that is actually needed is protected public information (Nagy and Akl 2007).

Since the price for avoiding detection is total uncertainty about the transmitted message, Eve is forced to measure at least some of the qubits in the Hadamard basis, thus exposing herself to detection. The choice for Eve is a difficult one: either try as much as possible to remain hidden, but then she faces the prospect of gaining little information (if any at all) about the content of the message, or aiming at decrypting as much as possible from the transmitted message, which increases the risk of being caught. And in case of detection, no information is gained (zero knowledge), because Alice will no longer reveal the proper order of the bits in the message.

If the first variation discussed is one in which the complexity of the protocol is decreased, the second one involves an increase in complexity with the purpose of also decreasing the probability of the worst case. In the original protocol, the worst case happens when Eve gets so lucky that she guesses precisely the encoding basis (θ, φ) used by Alice. We can think of a variation in which Alice randomly chooses a pair (θ, φ) for every single bit transmitted. This will not change the average-case analysis, but will definitely make the worst-case much less probable, since Eve will have to get lucky N times now, where N is the total number of bits transmitted (message and signature together).

5 Conclusion

Quantum mechanical properties have been used before in cryptographic protocols, but only for key distribution purposes, or more precisely for key enhancement, if authentication is achieved through a small secret key already distributed to the parties involved. In this paper, we have shown that secret communication does not need an encryption 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. Our protocols are entanglement free and use only unary quantum transformations, which means that the computational power assumed is less than that of a universal quantum computer. Consequently, communicating securely through public channels can be performed simple, fast and efficient if we resort to quantum mechanics to directly encrypt the transmitted message into a sequence of qubits.

All protocols presented benefit from the capability of detecting an intruder, a trait which is unique to quantum 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 scheme has an improved intruder detection rate of 33 % (from 25 %) per intercepted qubit. This is achieved using three complementary encoding bases. Eve's presence is searched on a signature, as in all other protocols. Our paper also 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.

The two important ideas that made these results possible are the use of a quantum memory and bringing the rank (or position) of a bit in the message bitstring into play. The use of a quantum memory is essential to make "informed" measurements in the second phase of the protocols, after all the qubits have been received. Consequently, no qubits have to be discarded due to "incorrect" measurements, which translates into increased efficiency in terms of the number of qubits that need to be transmitted. Yet, storing qubits is rarely contemplated (if ever) in quantum protocols, perhaps due to their fragility and ephemeral nature. Nevertheless, experimental quantum physicists are making good progress towards making quantum memories a practical reality.

Scrambling the qubits encoding the message, on the other hand, guarantees that no knowledge whatsoever about the content of the message is gained by a potential eavesdropper, even in the highly unlikely eventuality of correctly decoding the individual bits in the message. It is our belief that the synergy of these two ideas working together may open the door for a whole new class of cryptographic protocols with superior characteristics.

References

Barnum H, Crépeau C, Gottesman D, Smith A, Tapp A (2002) Authentication of quantum messages. In: Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, pp 449–458

Bennett CH (1992) Quantum cryptography using any two nonorthogonal states. Phys Rev Lett 68(21):3121–3124

Bennett CH, Brassard G (1984) Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. IEEE, New York, pp 175–179 (Bangalore, India, December 1984)

Bennett CH, Brassard G, Mermin ND (1992) Quantum cryptography without Bell's theorem. Phys Rev Lett 68(5):557–559

Cao Z (2010) A note on Gottesman-Chuang quantum signature scheme. http://eprint.iacr.org/2010/317

Collins RJ, Donaldson RJ, Dunjko V, Wallden P, Clarke PJ, Andersson E, Jeffers J, Buller GS (2014) Realization of quantum digital signatures without the requirement of quantum memory. Phys Rev Lett 113:040502

Dunjko V, Wallden P, Andersson E (2014) Quantum digital signatures without quantum memory. Phys Rev Lett 112:040502–040506

Ekert A (1991) Quantum cryptography based on Bell's theorem. Phys Rev Lett 67:661–663

Gisin N et al (2011) Quantum storage of photonic entanglement in a crystal. Nature 469:508–511

Gottesman D, Chuang IL (2001) Quantum digital signatures. arXiv:quant-ph-0105032

Lu X, Feng DG (2005) Quantum digital signature based on quantum one-way functions. In: 7th International Conference on Advanced Communication Technology, ICACT 2005. IEEE, pp 514–517

Lomonaco Jr SJ (ed) (2000) Quantum computation: a grand mathematical challenge for the twenty-first century and the millennium. In: Proceedings of Symposia in Applied Mathematics, vol 58. American Mathematical Society, Short Course, Washington, DC

Lukin M et al (2012) Room-temperature quantum bit memory exceeding one second. Science 336:1283–1286

Nagy N, Akl SG (2007) Authenticated quantum key distribution without classical communication. Parallel Process Lett Special Issue Unconv Comput Probl 17(3):323–335

Nagy N, Nagy M, Akl SG (2010) Key distribution versus key enhancement in quantum cryptography. Parallel Process Lett 20(03): 239–250

Rivest RL, Shamir A, Adleman LM (1978) A method of obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126

Shannon C (1949) Communication theory of secrecy systems. Bell System Tech J 28(4):656–715

Steger M, Saeedi K, Thewalt MLW, Morton JJL, Riemann H, Abrosimov NV, Becker P, Pohl HJ (2012) Quantum information storage for over 180s using donor spins in a $Si^{2}8$ "Semiconductor Vacuum". Science 336(6086):1280–1283

Tittel W et al (2011) Broadband waveguide quantum memory for entangled photons. Nature 469:512–515

Zeng G, Keitel CH (2002) Arbitrated quantum-signature scheme. Phys Rev A 65:042312. http://link.aps.org/doi/10.1103/PhysRevA.65.042312