Quantum authentication of classical messages

Marcos Curty* and David J. Santos[†]

ETSIT, Universidad de Vigo, Campus Universitario s/n, E-36200 Vigo, Spain
(Received 22 March 2001; published 14 November 2001)

Although key distribution is arguably the most studied context on which to apply quantum cryptographic techniques, message authentication, i.e., certifying the identity of the message originator and the integrity of the message sent, can also benefit from the use of quantum resources. Classically, message authentication can be performed by techniques based on hash functions. However, the security of the resulting protocols depends on the selection of appropriate hash functions, and on the use of long authentication keys. In this paper, we propose a quantum authentication procedure that, making use of just one qubit as the authentication key, allows the authentication of binary classical messages in a secure manner.

PACS number(s): 03.67.Dd, 03.67.Hk, 03.67.Lx

I. INTRODUCTION

As computer networks spread worldwide with users accessing them via millions of different terminals, information protection becomes more-and-more relevant. This challenge of providing adequate information protection is closely related to the basic tasks of cryptography, authentication and secrecy [1,2]. During the last decade it has been shown that information has a physical, not only mathematical, dimension and, as such, can be studied making use of quantum theory. This has given birth to the research field known as quantum-information theory (QIT) (see, e.g., [3–5]). Quantum cryptography (QC), first introduced by Wiesner [6] and Bennett and co-workers [7], is, with quantum computation, one of the most remarkable applications of QIT. The information security provided by QC is based on fundamental properties of quantum mechanics, instead of an unproven assumption concerning the computational complexity of some algorithms (as it is the case of most of the classical cryptography), and therefore brings a whole new dimension to security in communications. Over the last few years, there have been several experimental demonstrations of the feasibility of QC [8–15] that seem to indicate that the prospects for its future mainstream use are good.

QC involves several topics, and although quantum key distribution (QKD) [16–18] is arguably the most studied one, the necessity to combine QKD protocols with classical authentication methods has motivated recent investigations on the achievement of key verification [19,20] and user authentication [21–26] in a quantum-mechanical secure manner. Key verification consists of assuring that the parties of a key-distribution scheme are the legitimate ones, and that the key established is authentic. User authentication (also called user identification) allows a communicator to prove his/her identity, often as the first step to log into a system. One potential insecurity of user authentication consists of assuming that once the log-in process has concluded, the transmission remains authentic for the rest of the communication. This assumption strongly depends on the level of security provided by the channel used. Classical cryptography solves this weakness employing message authentication codes (MACs), which enable parties owning a shared secret key to achieve data integrity. MAC, also known as a data authentication code, is essentially a scheme specified by two algorithms, an encoding or tagging algorithm (possibly stochastic), and a decoding or verification algorithm. When the sender (Alice) wants to send a certified message to a recipient (Bob), she computes, employing the encoding algorithm, a tag (as a function of the message and a secret key previously shared) and appends it to the message. On the reception side, Bob verifies the authenticity of the tag by means of the specified decoding procedure, which depends on the message, tag, and shared key. This algorithm returns a bit indicating when Bob must regard the message as authentic and accept it as coming from Alice, and when he must discard it. Wegman and Carter [27,28] described a message-authentication scheme whose security is information theoretic, rather than based on computational assumptions. Their technique uses a hash function, selected from a universal hash family, to compress the message to be certified into a smaller string of bits. Then this string is encrypted to produce the tag.

Recently, Barnum [29] has addressed the problem of authenticating quantum messages. In his protocols the authentication key is used to select a quantum error-detection code (QEDC) from a given set. A quantum state is encoded in one of these codes, and the state is rejected as inauthentic if an error is detected by the recipient. The geometry of the set of QEDCs is chosen such that it ensures that the probability of undetected forgery is less than the classical bound (inverse of the square root of the number of keys).

In this paper we study how the use of quantum resources can improve the authentication of classical messages. Specifically, we present a broad class of quantum authentication schemes that, unlike classical MACs, which need at least two secret bits to achieve a probability of forgery less than 1, provide secure data integrity when only one-qubit key is shared between the communicating partners.

The paper is organized as follows. In Sec. II we describe a class of quantum message-authentication codes that requires just one qubit as the key to authenticate binary messages. In Sec. III, we analyze the security of these protocols

————
*Email address: mcurty@com.uvigo.es
[†]Email address: dsantos@com.uvigo.es

against various attacks of increasing severity. First, we analyze the no-message attack, in which the sender has not initiated the transmission (there is no message in the channel), and the adversary (Eve) attempts to prepare a message with the goal of passing Bob's verification test. Then, we analyze more subtle attacks, those in which Eve has access to what is transmitted. We also discuss, in Sec. III, how the security of the protocol is modified if the authentication keys are reused. Finally, we present our conclusions in Sec. IV.

II. QUANTUM MESSAGE-AUTHENTICATION CODES

Suppose Alice needs to send a certified classical message to Bob. The goal is to make Bob confident about the authenticity of the message and sender. The protocols described in this section require a quantum channel, so the first task consists of assigning a quantum state to each possible classical message. This decision needs no secrecy and can be made openly. We will discuss the simple case of binary messages (one-bit long). Thus, there are only two possible messages, "0" and "1," to which we assign the pure quantum states $|\phi_0\rangle$ and $|\phi_1\rangle$, respectively. In order to guarantee Bob's perfect extraction of information from these states and to make authentication possible, they cannot be selected arbitrarily, but must be orthogonal, $\langle \phi_i | \phi_j \rangle = \delta_{ij}$, with $i,j \in \{0,1\}$; and must contain, as in any authentication method, some tag information to be checked by Bob. We will assume that they belong to a two-qubit state space (a four-dimensional Hilbert space) $\mathcal{E}$. This can be seen as if the first qubit carried the message information, and the second qubit carried the tag. As for the secret authentication key, we will assume that Alice and Bob share a two-qubit maximally entangled state. Each owns one qubit of a publicly known singlet state $|\psi\rangle_{AB} = 1/\sqrt{2}(|01\rangle_{AB} - |10\rangle_{AB})$.

The authentication procedure goes as follows. When Alice wants to send a certified bit i, she prepares two qubits in the state $|\phi_i\rangle$ and performs the following encoding operation on her part of $|\psi\rangle_{AB}$ and on the message

$$E_{A\mathcal{E}} = |0\rangle\langle 0|_A 1_{\mathcal{E}} + |1\rangle\langle 1|_A U_{\mathcal{E}}, \tag{2.1}$$

where $U_{\mathcal{E}}$ is some publicly known unitary quantum operation. Basically, the result of this encoding operation can be seen as performing [second term in Eq. (2.1)] or not [first term in Eq. (2.1)], depending on the state of Alice's qubit of the shared key, a unitary operation, $U_{\mathcal{E}}$, on the quantum state $|\phi_i\rangle$. This could also be accomplished with a previously shared classical bit acting as a key. The singlet can be seen as a superposition of all possible classical key states.

After performing this tagging operation, the state of the global system (Alice+Bob+message) is

$$\frac{1}{\sqrt{2}}(|01\rangle_{AB}|\phi_i\rangle - |10\rangle_{AB}U_{\mathcal{E}}|\phi_i\rangle). \tag{2.2}$$

Using the density-operator formalism, the state of the authenticated message that Alice sends to Bob can be obtained

from Eq. (2.2) performing the partial trace over the Alice and Bob variables. In density-operator terms, this state is given by

$$\rho' = \frac{1}{2}(\rho_i + U_{\mathcal{E}}\rho_i U_{\mathcal{E}}^{\dagger}), \tag{2.3}$$

where $\rho_i = |\phi_i\rangle\langle\phi_i|$. On the reception side, Bob decodes the information sent by Alice performing the decoding operation

$$D_{B\mathcal{E}} = |0\rangle\langle 0|_B U_{\mathcal{E}}^{\dagger} + |1\rangle\langle 1|_B 1_{\mathcal{E}} \tag{2.4}$$

on his part of $|\psi\rangle_{AB}$ and the message received. Finally, Bob performs an orthogonal measurement on the space $\mathcal{E}$. Since this space is four dimensional, and we have imposed the states $|\phi_0\rangle$ and $|\phi_1\rangle$ to be orthonormal, we can perform this measurement on the orthonormal set $\{|\phi_i\rangle; i = 0, \dots, 3\}$, where $|\phi_2\rangle$ and $|\phi_3\rangle$ are two extra orthonormal states. If the result of such a measurement is one of the two first elements of the set, Bob should assume that no forgery has taken place, and therefore obtain the classical message sent to him. If this is not the case, he rejects the message received.

III. SECURITY ANALYSIS

The class of quantum protocols of the preceding section provides perfect deterministic decoding, i.e., the quantum key $|\psi\rangle_{AB}$ and the quantum ciphertext ρ' uniquely determine the classical message sent, ρ_i. This means that these protocols would fail only if Bob accepted a message as an authenticated one when that is not the case (due to the unnoticed action of Eve). When dealing with forgery strategies we must consider two main types of attacks, the no-message attack and the message attack. The first one is the simplest. Before Alice's sending any message to Bob, Eve attempts to prepare a quantum state that passes the decoding algorithm. The message attack is more subtle and severe. Eve could access authentic messages transmitted, and try to produce a forged message based on the information gained. The purpose of this section is to analyze both families of attacks, and obtain the class of unitary operations $U_{\mathcal{E}}$ that makes them unsuccessful. In the following discussion we will consider the ideal scenario of an error-free quantum channel.

A. No-message attack

Suppose Eve prepares a normalized pure quantum state $|\epsilon\rangle \in \mathcal{E}$ and sends it to Bob trying to impersonate Alice. In the most general case, this inauthentic pure quantum message can be described as $|\epsilon\rangle = \Sigma_{i=0}^{3} e_i |\phi_i\rangle$. When Bob receives this quantum message he cannot know that it comes from a forger, so he follows the procedure explained in the preceding section. He performs a decoding operation and then an orthogonal measurement over the set $\{|\phi_i\rangle; i = 0, \dots, 3\}$. Before this measurement takes place, the state of the message can be described by $\rho'_E = (\rho_E + U_{\mathcal{E}}^{\dagger}\rho_E U_{\mathcal{E}})/2$, where $\rho_E = |\epsilon\rangle\langle\epsilon|$. As we have seen, Bob rejects the message if the result of his measurement is one of the last-two elements of this basis; therefore, the probability P_f that Eve deceives Bob is

$$P_f = \sum_{i=0}^{1} \langle \phi_i | \rho'_E | \phi_i \rangle = \frac{1}{2} \sum_{i=0}^{1} (|e_i|^2 + |\langle \epsilon | U_{\mathcal{E}} | \phi_i \rangle|^2). \qquad (3.1)$$

This quantity depends both on Eve's strategy and on the quantum operation $U_{\mathcal{E}}$. The normalization of $|\epsilon\rangle$ and the unitarity of $U_{\mathcal{E}}$ make both terms on the right side of Eq. (3.1) to be less or equal to 0.5. The first term depends entirely on Eve's decision, and, to be 0.5, e_2 and e_3 must be zero. We will assume that Eve selects $|\epsilon\rangle$ such as this condition is fulfilled. Let us focus on the second term, $1/2\Sigma_{i=0}^{1}|\langle\epsilon|U_{\mathcal{E}}|\phi_i\rangle|^2$. First, let us write the matrix representation of $U_{\mathcal{E}}$ in the block form

$$U_{\mathcal{E}} = \begin{pmatrix} M_0 & M_1 \\ M_2 & M_3 \end{pmatrix}, \qquad (3.2)$$

where the M_i are 2×2 complex matrices. With this notation, the second term in the right side of Eq. (3.1) can be written as

$$\frac{1}{2}[(|\bar{M}_0^0|^2 - |\bar{M}_0^1|^2)|e_0|^2$$
$$+ 2|\bar{M}_0^1\bar{M}_0^{0\dagger}||e_0|\sqrt{1-|e_0|^2}\cos\theta_E + |\bar{M}_0^1|^2],$$
$$(3.3)$$

where $\bar{M}_i^j$ represents the j row of the i block of $U_{\mathcal{E}}$, and θ_E is an angle that depends entirely on Eve's choice of her state. Eve's goal is to make P_f as big as possible, so the worst case for Alice and Bob occurs when Eve chooses $\theta_E = 2\pi k$ with k any integer, and a $|e_0|$ that maximizes (3.3) for a given $U_{\mathcal{E}}$. We can distinguish between two cases

1. If $|\bar{M}_0^1\bar{M}_0^{0\dagger}| = 0$, the maximum of Eq. (3.3) is strictly less than 0.5 when $|\bar{M}_0^0|^2 < 1$ and $|\bar{M}_0^1|^2 < 1$.

2. If $|\bar{M}_0^1\bar{M}_0^{0\dagger}| \neq 0$, the maximum of Eq. (3.3) is strictly less than 0.5 when

$$\frac{1}{2}x\left\{1+\left(\frac{x}{y}\right)\left[1+\left(\frac{x}{y}\right)^2\right]^{-1/2}\right\} + \frac{1}{2}y\left[1+\left(\frac{x}{y}\right)^2\right]^{1/2} + z < 1, \qquad (3.4)$$

where the real variables x, y, and z are $|\bar{M}_0^0|^2 - |\bar{M}_0^1|^2$, $2|\bar{M}_0^1\bar{M}_0^{0\dagger}|$, and $|\bar{M}_0^1|^2$, respectively. Note that, in both cases, Alice and Bob can select $U_{\mathcal{E}}$ such that its M_0 block makes $P_f < 1$ independently of Eve's choice of $|\epsilon\rangle$.

Finally, in this subsection we have assumed that Eve prepares a pure state $|\epsilon\rangle$. However, she could have prepared a general mixed state $\rho_E = \Sigma_{i=0}^{3} p_i |\epsilon_i\rangle\langle\epsilon_i|$, with $\Sigma_{i=0}^{3} p_i = 1$. From what we have shown in this subsection, it is straightforward to see that if $U_{\mathcal{E}}$ is selected satisfying the conditions above, then also in this case $P_f < 1$. In fact, we can further show that, with the appropriate selection of $U_{\mathcal{E}}$, P_f can be made at the most $1/2$. According to Eq. (3.1), P_f can be written as $P_f = \text{Tr}(\rho'_E P)$, where $\rho'_E = (\rho_E + U_{\mathcal{E}}^{\dagger}\rho_E U_{\mathcal{E}})/2$ and $P = |\phi_0\rangle\langle\phi_0| + |\phi_1\rangle\langle\phi_1|$. Using the properties of the trace operator,

$$P_f = \text{Tr}(\rho_E Q)/2, \qquad (3.5)$$

where $Q = U_{\mathcal{E}} P U_{\mathcal{E}}^{\dagger} + P$ is a positive operator known to Eve, and with maximum eigenvalue $\lambda_{max} \geq 1$. Therefore, the maximizing ρ_E is any eigenvector corresponding to λ_{max}, and thus $P_f = \lambda_{max}/2$. Finally, it is easy to see (see, e.g., [30]) that choosing $U_{\mathcal{E}}$ such that it takes P to its orthogonal complement makes $\lambda_{max} = 1$, and therefore, as predicted, $P_f = 1/2$.

B. Message attack

As we have seen, this is a more subtle and severe class of attacks. Instead of directly forging a quantum message and send it to Bob, Eve could wait for Alice's original messages and try to manipulate them. Thus, Eve's goal is to convert authentic messages into others passing Bob's test. In the simple case we are dealing with binary messages, this implies converting $|\phi_0\rangle$ into $|\phi_1\rangle$ and vice versa.

In order to simplify the analysis, and without loss of generality, we will distinguish between two types of message attacks. In the first one, Eve, based on the knowledge of all the public aspects of the quantum authentication scheme used, determines a quantum operation and applies it to any message sent by Alice. This quantum operation can be described by a trace-preserving completely positive (TPCP) map. In the second class of attacks, Eve also tries to extract information, by means of the appropriate measurement of the message in the channel, that allows her to prepare a different message that Bob regards as authentic.

1. TPCP map

Consider that Alice sends to Bob a quantum message $|\phi_i\rangle$, with $i \in \{0,1\}$, and Eve performs an arbitrary TPCP map, $\mathcal{M}$, on it. The new state in the channel is $\rho'_E = \mathcal{M}(\rho')$, with ρ' given by Eq. (2.3). Eve chooses $\mathcal{M}$ such that the decoding procedure performed by Bob on the resulting state lead to the state $|\phi_j\rangle$, with $j \in \{0,1\}$, and $j \neq i$. Owing to the pure character of the states $|\phi_0\rangle$ and $|\phi_1\rangle$, this can only be done with certainty if $\mathcal{M}$ is a unitary operation, that we will write as U_E. For this kind of operation, the probability, $P'_f(i)$, of Eve achieving her goal is $\langle\phi_j|\rho''_E|\phi_j\rangle$, where ρ''_E, Bob's decoded state, is

$$\rho''_E = \frac{1}{2}(U_E\rho_i U_E^{\dagger} + U_{\mathcal{E}}^{\dagger}U_E U_{\mathcal{E}}\rho_i U_{\mathcal{E}}^{\dagger}U_E^{\dagger}U_{\mathcal{E}}), \qquad (3.6)$$

with $\rho_i = |\phi_i\rangle\langle\phi_i|$. Therefore,

$$P'_f(i) = \frac{1}{2}(|\langle\phi_j|U_E|\phi_i\rangle|^2 + |\langle\phi_j|U_{\mathcal{E}}^{\dagger}U_E U_{\mathcal{E}}|\phi_i\rangle|^2). \qquad (3.7)$$

If Alice prepares the state $|\phi_i\rangle$ with probability p_i, the overall probability of, employing a TPCP, substituting an authentic message with a different one that passes Bob's test is $P'_f = \Sigma_i p_i P'_f(i)$. This probability is 1 if U_E simultaneously satisfies, up to some arbitrary global phase factors, the following two pairs of conditions

$$|\phi_j\rangle = U_E|\phi_i\rangle, \qquad (3.8)$$

and

$$|\phi_j\rangle = U_{\mathcal{E}}^{\dagger} U_E U_{\mathcal{E}}|\phi_i\rangle, \qquad (3.9)$$

$\forall \ i,j \in \{0,1\}$, with $i \neq j$. The orthogonality between $|\phi_0\rangle$ and $|\phi_1\rangle$ allows Eve to always fulfill one of the two pairs of conditions independently of the particular $U_{\mathcal{E}}$ employed by Alice and Bob. Let us assume that Eve selects U_E such that Eq. (3.8) is satisfied. This selection makes U_E to have, in the orthonormal base $\{|\phi_i\rangle; i=0,\dots,3\}$, the following block representation:

$$U_E = \begin{pmatrix} M_0^E & 0 \\ 0 & M_1^E \end{pmatrix} \qquad (3.10)$$

with $M_0^E = e^{i\alpha} S(\beta)\sigma_x$, where α is an arbitrary phase, σ_x is the standard Pauli matrix, and $S(\beta)$ is a phase-shift operation, whose matrix representation is

$$S(\beta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\beta} \end{pmatrix}, \qquad (3.11)$$

and M_1^E is any 2×2 unitary matrix. Now, if we further demand the fulfillment of Eq. (3.9), the matrix elements of $U_{\mathcal{E}}$ and U_E must obey $\langle \phi_k | U_{\mathcal{E}} | \phi_i \rangle = \Sigma_{l=0}^{3} \langle \phi_k | U_E | \phi_l \rangle \times \langle \phi_l | U_{\mathcal{E}} | \phi_j \rangle \ \forall k \in \{0,\dots,3\}$. With the notation of U_E introduced in Eq. (3.10), this implies that M_0^0, M_0^1, M_2^0, and M_2^1, where M_i^j represents the j column of the i block of $U_{\mathcal{E}}$, must satisfy $M_0^0 = e^{i\gamma} S(\delta)\sigma_x M_0^1$ and, $M_2^{0\dagger} M_2^1 = 0$ or $M_2^0 = e^{i\chi} M_2^1$, where γ, δ, and χ are such that $U_{\mathcal{E}}$ is a unitary operation. If Alice and Bob choose $U_{\mathcal{E}}$ such that all these requirements are not verified, then the probability of successful tampering will be strictly less than 1, independently of Eve's TPCP map.

2. Measurement

Let us assume now that, instead of performing a predetermined quantum operation on the message sent by Alice, Eve makes a measurement on it trying to gain information about the key. If she were able to collapse the state of the key in a known unentangled pure state, she could throw away Alice's message and prepare and send to Bob an unauthentic new one that would pass his test with certainty. Since Eve knows how the protocol works, she would achieve this if she could distinguish perfectly between the two terms on the right-hand side of Eq. (2.3).

In order to avoid this attack, Alice and Bob must choose $U_{\mathcal{E}}$ such that the set of states $\{|\phi_i\rangle, U_{\mathcal{E}}|\phi_i\rangle\}$, with $i=0,1$, is not orthogonal. Owing to the orthogonality of $|\phi_0\rangle$ and $|\phi_1\rangle$, this requirement can be rewritten as $\langle \phi_i | U_{\mathcal{E}} | \phi_j \rangle \neq 0$ for, at least, one i and j, with $i,j \in \{0,1\}$. With the block-notation introduced in precedings sections, this condition can be expressed as $|M_0^0| > 0$ or $|M_0^1| > 0$. Although no secrecy is necessary for secure authentication, note that if $\langle \phi_i | U_{\mathcal{E}} | \phi_j \rangle \neq 0$, with $i \neq j$, the quantum authentication scheme also provides, in some sense, data encryption, since there is a probability

greater than zero, of Eve not determining the message that Alice sent.

C. Discussion

MACs are used to detect any attempt to modify the transmitted data by an undesired third party. In this section we have concentrated on several types of attacks which, we believe, are the most demanding. We have shown that, in order to avoid the forgery strategies studied, Alice and Bob should agree to choose $U_{\mathcal{E}}$ such that the following conditions are satisfied:

1. If $|\bar{M}_0^1 \bar{M}_0^{0\dagger}| = 0$, then $|\bar{M}_0^0|^2 < 1$ and $|\bar{M}_0^1|^2 < 1$.
2. If $|\bar{M}_0^1 \bar{M}_0^{0\dagger}| \neq 0$, then Eq. (3.4) must be verified.
3. $M_0^0 \neq e^{i\gamma} S(e^{i\delta})\sigma_x M_0^1$, or $M_2^{0\dagger} M_2^1 \neq 0$ and $M_2^0 \neq e^{i\chi} M_2^1$.
4. $|M_0^0| > 0$ or $|M_0^1| > 0$.

Of these four conditions, it is straightforward to see, however, that the last one, obtained in order to avoid the determination of the key by measurement, is redundant, since the fulfillment of the third condition leads to the fourth one.

After examining the three remaining conditions, two questions arise: (i) Can a unitary operation simultaneously fulfill these three restrictions? and, (ii) If the answer is yes, what is the optimum $U_{\mathcal{E}}$? Perhaps the easiest way to answer the first question is with a trivial example. If, for instance, $\bar{M}_0^0 = (0.5 \ 0.5)$ and $\bar{M}_0^1 = (0 \ 0)$, it is straightforward to construct a unitary operation with its first block equal to M_0. Moreover, it is evident that all the above conditions are satisfied by this matrix. As for the second question, it is an important open issue that we plan to address in the future. First one should establish some appropriate criterion according to which obtain such an optimum $U_{\mathcal{E}}$. When we analyzed no-message attacks, we showed that, selecting an appropriate $U_{\mathcal{E}}$, P_f can be made half regardless of Eve's strategy. Nevertheless, it is straightforward to see that this particular unitary quantum operation makes P_f' one, thus making the protocol vulnerable. Therefore, it seems that the optimization should result from a balance of the different forgery strategies considered.

Finally, one interesting property of this class of quantum authentication protocols is that it provides the possibility of reusing the authentication keys. If there is no forgery, then after Alice's encoding and Bob's decoding processes the state of the key remains intact. Thus, if the authentication procedure is successful, in principle Alice and Bob could retain the entangled key and reuse it in the next run of the protocol. The presence of Eve, however, cannot be despised. She could try to entangle an ancilla system with the quantum authentication key generating a global state of the form

$$|\phi\rangle_{ABE} = \alpha|01\rangle_{AB}|\phi\rangle_E - \beta|10\rangle_{AB}|\phi_\perp\rangle_E, \qquad (3.12)$$

with $|\phi\rangle_{ABE} \in \mathcal{K} \otimes \mathcal{A}$, where $\mathcal{K}$ and $\mathcal{A}$ denote the state spaces of the key and the ancilla systems, respectively, $|\phi\rangle_E$ and $|\phi_\perp\rangle_E$ represent two-arbitrary orthonormal states in $\mathcal{A}$, and α and β are two-arbitrary complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$. If Eq. (3.12) is verified, Eve could always forge

messages when the key is reused, just reproducing Alice's encoding process, but employing her ancilla as the control of the quantum operation.

If we assume that Eve has access only to the quantum channel between Alice and Bob, which we believe is a reasonable assumption, then Eve could try to obtain Eq. (3.12) in two different ways. She could prepare a quantum message and send it to Bob, or she could manipulate the message sent by Alice. The first possibility can be neglected, since, if $U_\mathcal{E}$ satisfies the conditions enumerated above, Eve cannot know when a run of the protocol has been successful. As for the second possibility, it must not be confused with the one previously analyzed when dealing with TPCP maps. Now Eve does not need to convert $|\phi_0\rangle$ into $|\phi_1\rangle$ and vice versa. She can prepare $|\psi\rangle_E \in \mathcal{A}$ and apply a unitary operation $U_{\mathcal{E}\otimes\mathcal{A}}$ of the form

$$U_{\mathcal{E}\otimes\mathcal{A}}\left[\frac{1}{\sqrt{2}}(|\phi_i\rangle|01\rangle_{AB} - U_\mathcal{E}|\phi_i\rangle|10\rangle_{AB}) \otimes |\psi\rangle_E\right],$$
(3.13)

trying to achieve $U_{\mathcal{E}\otimes\mathcal{A}}(|\phi_i\rangle|\psi\rangle_E) = (\alpha|\phi_i\rangle + \beta|\phi_j\rangle)|\phi\rangle_E$ and $U_{\mathcal{E}\otimes\mathcal{A}}(U_\mathcal{E}|\phi_i\rangle|\psi\rangle_E) = (\gamma U_\mathcal{E}|\phi_i\rangle + \delta U_\mathcal{E}|\phi_j\rangle)|\phi_\perp\rangle_E$, with $i,j \in \{0,1\}$, and $\alpha, \beta, \gamma, \delta$ some complex parameters such that $|\alpha|^2 + |\beta|^2 = |\gamma|^2 + |\delta|^2 = 1$. If $U_\mathcal{E}$ is chosen such that $\langle\phi_i|U_\mathcal{E}|\phi_i\rangle \neq 0$, for some $i \in \{0,1\}$, then $|\phi_i\rangle$ and $U_\mathcal{E}|\phi_i\rangle$ are not orthogonal for at least one value of i. Therefore, and since the inner product of states is preserved by any unitary operation, these conditions are impossible to fulfill. This means that Eq. (3.12) cannot be achieved with certainty.

Nevertheless, and although key recycling is in principle possible, it should be noticed that the security of the authentication protocols presented may be drastically reduced. As suggested in [31], security does not depend on the use of entanglement, but on the possibility of detecting Eve's presence in the quantum ciphertext. As we have seen, these authentication schemes can detect Eve with a certain probability, but there is also a chance that Eve remains undetected.

IV. CONCLUSION

We have presented a broad class of quantum authentication protocols that, making use of just one qubit as the authentication key, allow the authentication of binary classical messages with a probability of successful forgery less than 1. All parties, including the forger, may have full knowledge about all aspects of the protocol. However, it requires sharing a previous secret (in the form of an entangled pair of particles, or a classical bit), and an ideal quantum channel between the partners.

We have described several types of possible attacks and shown that careful selection of the quantum transformation performed by the communicating parties makes the protocol secure against these attacks. However, a further more extensive security analysis in a more realistic scenario (a nonperfect channel), as well as the derivation of the optimum $U_\mathcal{E}$ in such circumstances, is needed.

Finally, we have also shown that the protocol authentication keys can be reused. However, this reduces the security of the protocol.

[1] D. E. R. Denning, *Cryptography and Data Security* (Addison-Wesley, Reading, MA, 1983).

[2] B. Schneier, *Applied Cryptography*, 2nd ed. (Wiley, New York, 1996).

[3] J. Gruska, *Quantum Computing* (McGraw-Hill, New York, 1999).

[4] H. Lo, S. Popescu, and T. Spiller, *Introduction to Quantum Computation and Information* (World Scientific, Singapore, 1999).

[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[6] S.J. Wiesner, SIGACT News **15**, 78 (1983), original manuscript written ca. 1970.

[7] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, in *Advances in Cryptology* (Plenum Press, New York, 1982), pp. 267–275.

[8] C.H. Bennett and J. Smolin, J. Cryptology **5** (1), 3 (1992).

[9] A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23** (6), 383 (1993).

[10] C. Marand and P.D. Townsend, Opt. Lett. **20**, 1695 (1995).

[11] R.J. Hughes, D.M. Alde, P. Dyer, G.G. Luther, G.L. Morgan, and M. Schauer, Contemp. Phys. **36** (3), 149 (1995).

[12] W.T. Buttler, R.J. Hughes, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt, and C.G. Peterson, Phys. Rev. Lett. **84**, 5652 (2000).

[13] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).

[14] D.S. Naik, C.G. Peterson, A.G. White, A.J. Berglund, and P.G. Kwiat, Phys. Rev. Lett. **84**, 4733 (2000).

[15] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000).

[16] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE Press, New York, 1984), pp. 175–179.

[17] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[18] C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[19] D. Ljunggren, M. Bourennane, and A. Karlsson, Phys. Rev. A **62**, 022305 (2000).

[20] G. Zeng and W. Zhang, Phys. Rev. A **61**, 022303 (2000).

[21] C. Crépeau and L. Salvail, in *Advances in Cryptology* (Springer-Verlag, Berlin, 1995), pp. 133–146.

[22] M. Dusek, O. Haderka, M. Hendrych, and R. Myska, Phys. Rev. A **60**, 149 (1999).

[23] H. Barnum, e-print quant-ph/9910072.

[24] G. Zeng and G. Guo, e-print quant-ph/0001046.

[25] J.G. Jensen and R. Schack, e-print quant-ph/0003104.

[26] Y.-S. Zhang, C.-F. Li, and G.-C. Guo, e-print quant-ph/0008044.

[27] J.L. Carter and M.N. Wegman, J. Comput. Syst. Sci. **18**, 143 (1979).

[28] M.N. Wegman and J.L. Carter, J. Comput. Syst. Sci. **22**, 265 (1981).

[29] H. Barnum, e-print quant-ph/0103123.

[30] R. A. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, 1985).

[31] D.W. Leung, e-print quant-ph/0012077.