Symmetries and security of a quantum-public-key encryption based on single-qubit rotations

U. Seyfarth,[1] G. M. Nikolopoulos,[2] and G. Alber[2]

[1]*Institut für Angewandte Physik, Technische Universität Darmstadt, Darmstadt D-64289, Germany*
[2]*Institute of Electronic Structure & Laser, FORTH, P. O. Box 1385, Heraklion 71110, Crete, Greece*

(Dated: February 17, 2012)

Exploring the symmetries underlying a previously proposed encryption scheme which relies on single-qubit rotations, we derive an improved upper bound on the maximum information that an eavesdropper might extract from all the available copies of the public key. Subsequently, the robustness of the scheme is investigated in the context of attacks that address each public-key qubit independently. The attacks under consideration make use of projective measurements on single qubits and their efficiency is compared to attacks that address many qubits collectively and require complicated quantum operations.

PACS numbers: 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum-public-key cryptography, where the public keys are quantum-mechanical systems, is a largely unexplored area of problems. Various cryptographic primitives can be defined in this context (e.g., digital signatures, identification schemes, encryption schemes, etc) which aim at different goals (e.g., integrity, confidentiality, etc) [1–10]. Of particular interest are quantum-public-key encryption (QPKE) schemes [6–10] which facilitate the communication between many users over insecure channels. Typically, a legitimate user participating in such a QPKE scheme has to choose a random secret (private) key, and prepare the public key in a state that is in accordance with the private key. Many copies of the public-key state can be created in this manner and become available to any potential sender in an authenticated manner, e.g. via a key-distribution center, whereas the corresponding private key is never revealed and is used by the receiver for decryption only. In a nutshell, QPKE combines the provable security of quantum-key distribution (QKD) protocols [11] with the flexibility of conventional public-key encryption schemes, facilitating thus the *key distribution* and the *key management* in large networks [10, 12]. Key distribution and key management are crucial issues associated with the security and the efficient operation of large networks, and cannot be solved efficiently in the context of QKD (followed by a classical symmetric cryptosystem) or quantum direct communication (QDC) protocols such as [13–15]. The main reason is that, by construction, the protocols of QKD and QDC are point-to-point protocols, and thus the total number of secure links and keys scales quadratically with the number of users in the network. This power law can be improved if the communications are performed via a key distribution center (KDC) which possesses all the secret keys. In this case, however, the center becomes an attractive target, while a compromised KDC renters immediately all communications insecure. In QPKE schemes on the other hand, the KDC deals with the public keys only, whereas the private keys are in posession of the legitimate users [16]. The study of QPKE schemes is also of fundamental importance for the field of quantum cryptography because of the quantum trapdoor one-way functions, which are essential ingredients not only for the development of efficient encryption schemes, but also for many other cryptographic primitives (digital signatures, fingerprinting, zero-knowledge protocols, etc) [1, 3–5, 12, 17].

The mere fact that in QPKE schemes many copies of the public keys become available, allows an eavesdropper to launch new strategies that go beyond QKD and QDC protocols (e.g., see [18]). Although the actual state of the public key is unknown to an adversary, the multiple copies, when processed judiciously, may reveal more information on this state than a single copy. Hence, a security analysis of a particular QPKE scheme has to address questions related to the lengths of the private and the public keys, as well as the number of public-key copies that can become available before the entire cryptosystem is compromised. Clearly, such questions are intimately connected to specific aspects of QPKE, which are not present neither in QKD nor in QDC protocols.

The QPKE scheme of [10] is rather intuitive as it relies on single-qubit rotations. The public key consists of a number of qubits that are prepared at random and independently in some unknown state. A message can be encrypted in one of the public keys by rotating appropriately the corresponding qubit states and the resulting cipher-state is subsequently sent for decryption. Due to its simplicity, this scheme may serve as a theoretical framework for addressing questions pertaining to the power and limitations of QPKE as well as its robustness against various types of attacks. In this context it has been shown recently that any deterministic QPKE requires randomness in order to be secure against a forward-search attack [18]. Furthermore, in contrast to the classical setting, a QPKE scheme can be used as a black box to build a new randomized bit-encryption scheme that is no longer susceptible to this attack.

Here we discuss for the first time a symmetry that underlies the scheme of [10] and that reduces considerably the information that an eavesdropper might extract from the copies of the public key. Subsequently, we analyze the security of the protocol against attacks that aim at the encrypted message and that rely on individual projective measurements on the qubits of the public key(s) and of the cipher state. It is shown that the performance of such attacks can be slightly worse than the performance of the forward-search attack [18] which requires complicated quantum transformations that are beyond today's technology.

We like to emphasize, that discussions on the scheme of [10] with an appropriate choice of the parameters also apply on a specific so-called ping-pong protocol [14] that pertains to the category of the so-called quantum direct communication (QDC) protocols. The different context has to be taken into account to achieve meaningful statements.

This paper is organized as follows: In Sec. II basic aspects of the recently introduced quantum-public-key protocol of [10] are summarized. The influence of symmetric eavesdropping strategies on upper bounds of the probability for an eavesdropper to guess correctly the private key or the encrypted message are investigated in Sec. III. Security aspects of the private key are discussed in Sec. III A on the basis of Holevo's bound. In Sec. III B an attack on encrypted messages is studied, which pertains to individual projective measurements on the qubits involved. As a main result it is shown that Eve's success probability converges to the value of one half exponentially with the numbers of qubits in which the message is encrypted with a scale depending on the number of its publicly available copies of the public key. Furthermore, it turns out that the success probability of this attack differs only slightly from the already known optimal probability of successful state estimation by means of collective measurements. In addition, as discussed in III C, the resulting lower bound of the security parameter of the public-key protocol is also close to the previously derived security parameter of the forward-search attack of Ref. [18]. Finally, in Sec. III D a symmetry-test attack with projective measurements is explored, which attacks the message directly and makes use of only a single copy of the public-key quantum state and the corresponding cipherstate.

II. THE PROTOCOL

For the sake of completeness, let us summarize briefly the main ingredients of the protocol proposed in [10]. Each user participating in the cryptosystem generates a key consisting of a private part and a public part, as determined by the following steps.

1. Choice of a random positive integer $n \gg 1$. Additional limitations on n will be derived in the following section.

2. Choice of a random integer string $\mathbf{k}$ of length N i.e., $\mathbf{k} = (k_1, k_2, \ldots, k_N)$. Each integer k_j is chosen at random and independently from $\mathbb{Z}_{2^n}$, and thus it has a uniform distribution over $\mathbb{Z}_{2^n}$.

3. The classical key $\mathbf{k}$ is used for the preparation of the N-qubit public-key state

$$|\Psi_{\mathbf{k}}(\theta_n)\rangle = \bigotimes_{j=1}^{N} |\psi_{k_j}(\theta_n)\rangle \tag{1a}$$

where

$$|\psi_{k_j}(\theta_n)\rangle \equiv \cos\left(\frac{k_j\theta_n}{2}\right)|0_z\rangle + \sin\left(\frac{k_j\theta_n}{2}\right)|1_z\rangle, \tag{1b}$$

while $\{|0_z\rangle, |1_z\rangle\}$ denote the eigenstates of the Pauli operator $\hat{\sigma}_z \equiv |0_z\rangle\langle 0_z| - |1_z\rangle\langle 1_z|$, which form an orthonormal basis in the Hilbert space of a qubit. The Bloch vector associated with (1b) is given by $\mathbf{R}_j(\theta_n) = \cos(k_j\theta_n)\hat{z} + \sin(k_j\theta_n)\hat{x}$ with $\hat{x}$, $\hat{z}$ denoting unit vectors and with

$$\theta_n = \pi/2^{n-1} \tag{1c}$$

denoting the elementary angle of rotations around the axis with unit vector $\hat{y}$.

4. The private (secret) part of the key is $\mathbf{k}$, while the public part is $\{n, N, |\Psi_{\mathbf{k}}(\theta_n)\rangle\}$.

Note that, since each k_j is distributed uniformly and independently over $\mathbb{Z}_{2^n}$, the random state $|\psi_{k_j}(\theta_n)\rangle$ is uniformly distributed over the set of states

$$\mathbb{H}^{(n)} = \{|\psi_{k_j}(\theta_n)\rangle | k_j \in \{0, \ldots, 2^n - 1\}\}. \tag{2}$$

The state of the jth public-key qubit $|\psi_{k_j}(\theta_n)\rangle$ is known if the corresponding Bloch vector (or equivalently the angle $k_j\theta_n$) is known. The full characterization of the angle $k_j\theta_n$ requires n bits of information.

In general, a legitimate user should never reveal his private key, whereas he can produce at will as many copies of the public key as needed. The number of public-key copies T' [19], however, should be kept sufficiently small relative to n (the precise relation will be discussed in Sec. III A), so that the map

$$\mathbf{k} \mapsto \{T' \text{ copies of } |\Psi_{\mathbf{k}}(\theta_n)\rangle\} \tag{3}$$

is a quantum one-way function by virtue of Holevo's theorem [10, 18]. The one-way property of the map (3) is essential for the definition of the public-key encryption in the present framework.

Suppose now that Bob wants to communicate a binary plaintext $\mathbf{m}$ to Alice. The users have agreed in advance on two encryption operators $\hat{\mathcal{E}}_0$ and $\hat{\mathcal{E}}_1$ for encryption of bit $''0''$ and $''1''$, respectively. The key point here is that the bits of the plaintext (message) are assumed to be encrypted independently on public qubits that have been prepared at random and independently (see discussion above). Hence, for the sake of simplicity and without loss of generality, we can focus on the encryption of a one-bit message $m \in \{0, 1\}$. As discussed in [10, 18], in this case the protocol is not secure when the bit is encrypted on the state of a single qubit. However, it has been shown in the context of a forward-search attack, that the robustness of the protocol increases considerably if m is encoded in a randomly chosen s-bit codeword $\mathbf{w}$ with Hamming weight of parity m which is subsequently encrypted on s public qubits [20]. Correspondingly, the analysis of the following section pertains to a one-bit message, which is encrypted in the parity of an s-bit codeword with s playing the role of a security parameter.

For the encryption of the one-bit message $m \in \{0, 1\}$, Bob chooses at random a codeword $\mathbf{w} \equiv (w_1, w_2, \ldots, w_s)$ of parity m, and obtains an authenticated copy [21] of Alice's public key ($T' - 1$ public keys still remain publicly available).

The codeword is encrypted by applying independent successive encryption operations on the first s public qubits. The resulting (quantum) ciphertext is thus the s-qubit state

$$|X_{\mathbf{k},m}(\theta_n)\rangle = \bigotimes_{j=1}^{s} \hat{\mathcal{E}}_{w_j} |\psi_{k_j}(\theta_n)\rangle = \bigotimes_{j=1}^{s} |\chi_{k_j,w_j}(\theta_n)\rangle, \quad (4)$$

to be referred to hereafter as cipherstate. In this spirit, for the encryption of an L-bit message requires a public-key of length $N \geq Ls$. The cipherstate is sent to Alice who can obtain the message by means of a decryption procedure whose details are not essential for our purposes in this work. We only note here the crucial property that the encryption operations do not depend on Alice's private key, but the decryption operators do. Moreover, to allow for a simple decoding we assume that

$$\hat{\mathcal{E}}_{w_j} |\psi_{k_j}(\theta_n)\rangle \rightarrow |\psi_{k_j}(\theta_n + w_j\pi)\rangle, \quad (5)$$

for $w_j \in \{0, 1\}$ [22].

The primary objective of an eavesdropper (Eve) in the context of QPKE is to recover the plaintext from the cipher state intended for Alice. On the other hand, there is always a more ambitious objective pertaining to the recovery of the private key from Alice's public key. A cryptosystem is considered to be broken with accomplishment of either of the two objectives, but in the latter case the adversary has access to all of the messages sent to Alice (see also related discussion in [10, 12]). It is essential therefore to ensure secrecy of the private key, before we discuss the secrecy of a message. In Sec. III A, we derive restrictions on the parameters n and T' so that the map (3) is a quantum one-way function, and thus the recovery of the private key from the public keys is prevented.

As far as the encryption of the message (or equivalently the codeword) is concerned, we note that, in view of Eqs. (1b) and (5), the two possible values of the jth bit of the codeword $w_j \in \{0, 1\}$ are essentially encrypted in orthogonal eigenstates of a basis, which is rotated relative to the basis $\{|0_z\rangle, |1_z\rangle\}$ by an unknown angle $k_j\theta_n$. This means that the cipher-qubit state is parallel ($w_j = 0$) or antiparallel ($w_j = 1$) to the corresponding public-qubit state. Thus, in the following analysis we consider two different classes of eavesdropping strategies, which aim at the encrypted message. The first class involves attacks that explore the symmetry between the public-key state and the cipher state to reveal the message. The other class pertains to attacks that extract information on the public key (and thus on the basis on which the message has been encoded), so that the message can be recovered by means of a projective measurement on the estimated basis. Clearly, for this second class of attacks the probability of successful decryption is expected to increase with the information gain on the public-key state.

III. SYMMETRIC EAVESDROPPING STRATEGIES

In a single run of the protocol the fixed quantities are the secret key $\mathbf{k}$ (and thus the public key), as well as the codeword $\mathbf{w}$. In general, for a given eavesdropping strategy, the probability of successful eavesdropping in a single run of the protocol $P(\text{suc}|\mathbf{k}, \mathbf{w})$ differs from the corresponding probability obtained by averaging over all possible values of $\mathbf{k}$, i.e.,

$$\begin{aligned} \bar{P}(\text{suc}|\mathbf{w}) &= \sum_{\mathbf{k}} P(\mathbf{k}) P(\text{suc}|\mathbf{k}, \mathbf{w}) \\ &= \frac{1}{2^{nN}} \sum_{\mathbf{k}} P(\text{suc}|\mathbf{k}, \mathbf{w}), \end{aligned} \quad (6)$$

where for the last equation we have used the fact that $\mathbf{k}$ is uniformly distributed over $\{0, 1\}^{nN}$. The one-bit message m is encoded at random on one of the 2^{s-1} possible s-bit codewords with parity m (examples are given in [10, 18]). Hence, the conditional probability for the codeword $\mathbf{w}$ to occur, given a particular value of $m \in \{0, 1\}$, is $P(\mathbf{w}|m) = 2^{-(s-1)}$. However, from the point of view of an adversary, both values of $m \in \{0, 1\}$ are equally probable and thus $P(\mathbf{w}) = \sum_m P(\mathbf{w}|m)2^{-1} = 2^{-s}$ i.e., the codewords have a uniform distribution over $\{0, 1\}^s$. Therefore, the eavesdropping strategies we are going to discuss are symmetric with respect to all possible codewords [23], and thus we also have $\bar{P}(\text{suc}) \equiv 2^{-s} \sum_{\mathbf{w}} P(\text{suc}|\mathbf{w}) = P(\text{suc}|\mathbf{w})$.

A. Eve's point of view

Our first task is to find out how much information Eve may extract from τ available copies of the jth public qubit, and investigate the conditions under which the security of the private key is guaranteed.

From Eve's point of view, the state of the jth public qubit is uniformly distributed over $\mathbb{H}^{(n)}$, with the corresponding *a priori* probability being 2^{-n}. Hence, the density operator describing the state of τ copies of the jth public qubit is

$$\begin{aligned} \rho_{j,\text{prior}}^{(\tau)} &= \frac{1}{2^n} \sum_{k'_j=0}^{2^n-1} \Big[|\psi_{k'_j}(\theta_n)\rangle\langle\psi_{k'_j}(\theta_n)| \Big]^{\otimes\tau} \\ &= \frac{1}{2^n} \sum_{k'_j=0}^{2^n-1} |\Phi_{k'_j}^{(\tau)}(\theta_n)\rangle\langle\Phi_{k'_j}^{(\tau)}(\theta_n)|, \end{aligned} \quad (7)$$

where $|\Phi_{k'_j}^{(\tau)}(\theta_n)\rangle := |\psi_{k'_j}(\theta_n)\rangle^{\otimes\tau}$. In the space of τ-qubit states we have $\tau + 1$ different subspaces each of which is spanned by all $\mathcal{B}(\tau, l) = \binom{\tau}{l}$ eigenstates with the same Hamming weight l, i.e. the same number of qubits which are in the state $|1_z\rangle$. Within one of these subspaces, say $\mathcal{S}_l$, we can define the fully symmetric state

$$|l\rangle = \sum_{i=1}^{\mathcal{B}} |i\rangle_l / \sqrt{\mathcal{B}(\tau, l)},$$

where the sum runs over all the τ-qubit eigenstates with the same Hamming weight l. The problem can be formulated entirely in terms of these $(\tau + 1)$-symmetric states $\{|l\rangle : l = 0, 1, \ldots, \tau\}$ [24].

Using Eq. (1b), we have

$$|\Phi_{k'_j}^{(\tau)}(\theta_n)\rangle \;=\; \sum_{l=0}^{\tau} \sqrt{\mathcal{B}(\tau,l)} f_{\tau,l}(k_j\theta_n)\,|l\rangle, \qquad (8a)$$

with

$$f_{\tau,l}(k_j\theta_n) = \left[\cos\left(\frac{k_j\theta_n}{2}\right)\right]^{\tau-l}\left[\sin\left(\frac{k_j\theta_n}{2}\right)\right]^{l}. \qquad (8b)$$

Thus the density operator of Eq. (7) reads

$$\rho_{j,\mathrm{prior}}^{(\tau)} \;=\; \sum_{l,l'=0}^{\tau} C_{l,l'}\,|l\rangle\langle l'| \qquad (9a)$$

with

$$C_{l,l'} \;=\; \frac{1}{2^n}\sqrt{\mathcal{B}(\tau,l)\mathcal{B}(\tau,l')}\sum_{k'_j=0}^{2^n-1} f_{\tau,l}(k_j\theta_n) f^{\star}_{\tau,l'}(k_j\theta_n). \qquad (9b)$$

In the appendix A we provide additional information on the form of the *a priori* density operator $\rho_{j,\mathrm{prior}}^{(\tau)}$ as well as on some observations regarding its rank and eigenvalues. What we have so far, however, suffices to provide an upper bound on the von Neumann entropy $S[\rho_{j,\mathrm{prior}}^{(\tau)}]$ for any values of τ and n. In particular, instead of saying that τ copies of the jth public-key qubit are distributed, we can say that one copy of a larger $(\tau+1)$-dimensional system becomes publicly available. Hence, we have

$$S[\rho_{j,\mathrm{prior}}^{(\tau)}] \leq \log_2(\tau+1). \qquad (10)$$

The state described in Eq. (7) is a convex "classical" mixture of quantum states $\{\,|\Phi_{k_j}^{(\tau)}(\theta_n)\rangle\}$ which are distributed with probabilities $p_j = 2^{-n}$. Albeit pure, the states $|\Phi_{k_j}^{(\tau)}(\theta_n)\rangle$ are not mutually orthogonal. As a result the von Neumann entropy for the density operator $\rho_{j,\mathrm{prior}}^{(\tau)}$ is strictly smaller than the Shannon entropy of the corresponding probability distribution $H(p_j) = n$ [17]. The Holevo bound restricts Eve's average information gain I_{av} on the unknown state for τ copies. In particular, the information gain is upper bounded by $S[\rho_{j,\mathrm{prior}}^{(\tau)}]$, and in view of inequality (10) we obtain the result

$$I_{\mathrm{av}} \leq \log_2(\tau+1). \qquad (11)$$

On the other hand, one still needs n bits of information to characterize completely the state of the jth qubit (which of course implies knowledge on the private key as well). So, as long as

$$n \gg \log_2(\tau+1), \qquad (12)$$

the one-way property of the map (3) is guaranteed [25]. Thus one can be confident that no matter what strategy Eve may choose, her information on each public-key qubit is very low. Despite the fact that Eve has almost no knowledge about the public key she may be able to decrypt an encrypted message successfully. This will be demonstrated in the next sections.

In closing, we would like to emphasize that in [10, 18] the symmetries underlying the particular encryption scheme have not been taken into account and thus a larger upper bound on I_{av} was obtained suggesting that Eve can get up to τ bits of information from τ copies of the public key. However, this section demonstrates that the actual upper bound turns out to scale logarithmically with τ so that secrecy of the private key can be guaranteed already for significantly smaller values of n. Intuitively, this originates from the fact that the protocol restricts Eve by construction on the $(\tau+1)$-dimensional subspace of symmetric states for the τ copies of the jth public-key qubit. In appendix A we provide a tighter upper bound on Eve's information gain based on basic properties of the eigenvalues of $\rho_{j,\mathrm{prior}}^{(\tau)}$.

B. Incoherent Projective Measurements

Eve knows that all of the qubit states lie on the $x-z$ plane of the Bloch sphere. Thus, she may try to deduce the message by means of projective measurements on the cipherstate as well as on all of the remaining $(T'-1)$ copies of the public key [26]. In the following, we assume that each qubit of the public key or of the cipher is measured independently. Indeed, given that the random state of each public-key qubit is chosen independently and that it is distributed uniformly over $\mathbb{H}^{(n)}$, it is reasonable to assume that there are no hidden patterns that Eve can take advantage of by attacking many qubits collectively.

One possible strategy for Eve is to obtain an estimate of the public-key state (1) by measuring half of the public keys on the (eigen)basis $\{\,|0_z\rangle,\,|1_z\rangle\}$ of the Pauli operator $\hat{\sigma}_z$ and the other half on the (eigen)basis $\{\,|0_x\rangle,\,|1_x\rangle\}$ of the Pauli operator $\hat{\sigma}_x \equiv |0_z\rangle\langle 1_z| + |1_z\rangle\langle 0_z|$. In this way she can obtain an estimation on the jth public-qubit state or equivalently on its Bloch vector $\mathbf{R}_j$. It should be emphasized that such an attack essentially aims at the private key which, by construction, is in one-to-one correspondence with the public key. Although, condition (12) restricts Eve's information gain on the private key to negligible values, it cannot guarantee secrecy of the encrypted message. Hence, in an attempt to reveal the message she can measure the cipherstate on a basis defined by her guess on the corresponding public-qubit state. The main purpose of this section is to analyze this attack.

Since all public-key qubits are equivalent and independent, let us start by focusing on one of them, i.e., the jth qubit which is measured in the basis $b \in \{z,x\}$ with $b = z(x)$ referring to the eigenbasis of the operator $\hat{\sigma}_z(\hat{\sigma}_x)$. The two possible outcomes of these measurements are "0" and "1" and they occur with probabilities

$$p_{j,0}^{(b)}(k_j) = \cos^2\left(\beta\frac{\pi}{4} - \frac{k_j\theta_n}{2}\right), \quad p_{j,1}^{(b)} = 1 - p_{j,0}^{(b)}. \qquad (13)$$

In this equation, $\beta \in \{0,1\}$ with the correspondences $b = z \rightarrow \beta = 0$ and $b = x \rightarrow \beta = 1$. Without loss of generality let us also assume that $T'-1 = 2T$ [26], so that T

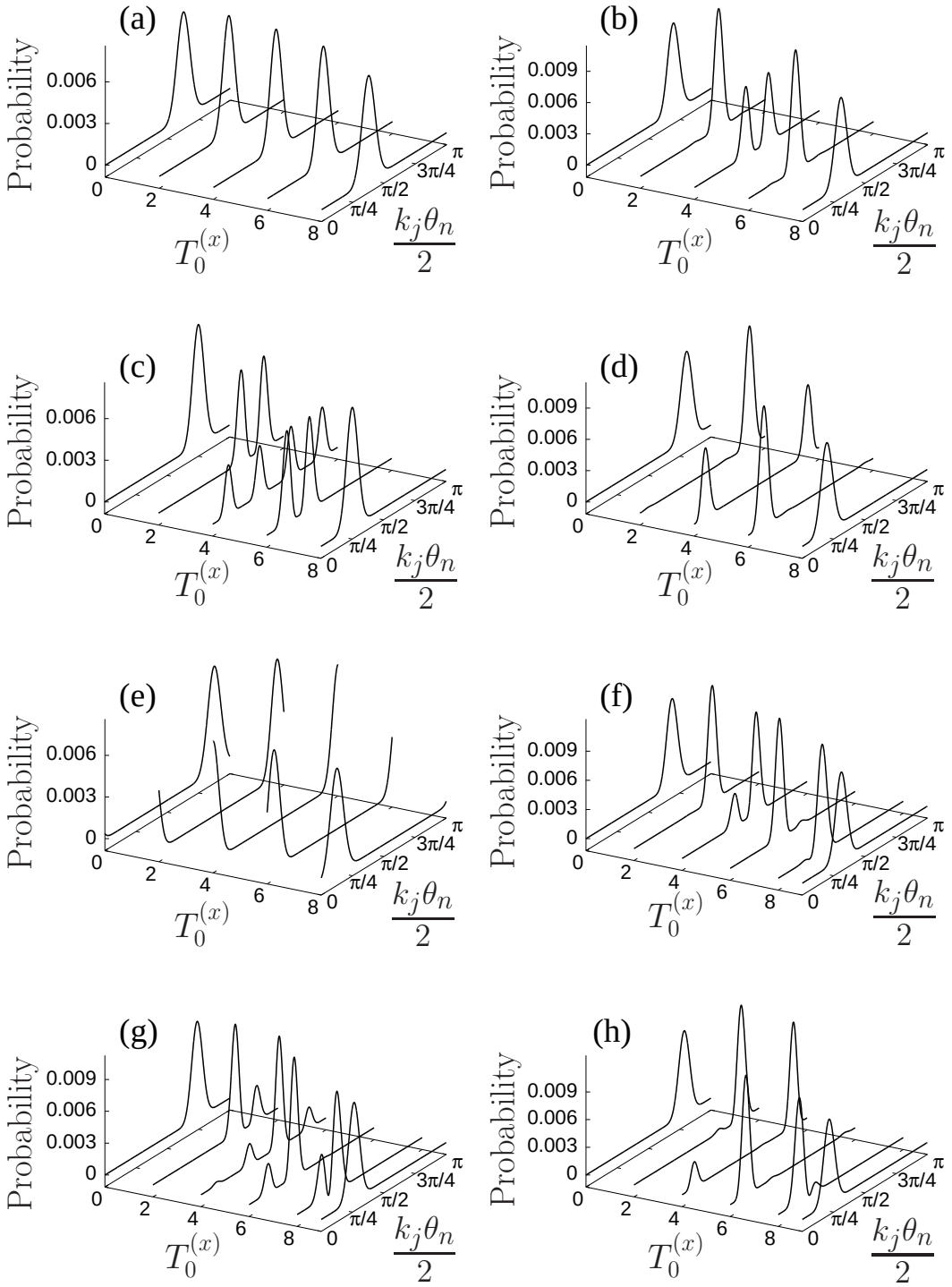

FIG. 1. A posteriori probability distributions (given by Eqs. 14) for $T = 8$ (a-e), $T = 9$ (f-h), and various events $\{T_0^{(z)}, T_0^{(x)}\}$: (a) $T_0^{(z)} = 0$; (b,f) $T_0^{(z)} = 2$; (c,g) $T_0^{(z)} = 4$; (d,h) $T_0^{(z)} = 6$; (e) $T_0^{(z)} = 8$.

measurements are performed on the basis b. Let $T_0^{(b)}$ denote the number of outcomes "0" from measurements in the b basis. In a single run of the protocol Eve obtains a particular set of outcomes $\{T_0^{(z)}, T_0^{(x)}\}$ out of T^2 different possible combinations. We will first discuss how much information she can obtain about the public-qubit state (or equivalently the private key).

1. *Information gain on the public-qubit state*

The *a posteriori* probability for the j-th qubit state is given by Bayes law

$$p_j(k_j'|T_0^{(z)}, T_0^{(x)}) = \frac{q_j(T_0^{(z)}, T_0^{(x)}|k_j')}{2^n q(T_0^{(z)}, T_0^{(x)})}. \tag{14a}$$

The probability for the outcome $\{T_0^{(z)}, T_0^{(x)}\}$ to occur given the input state $|\psi_{k_j'}(\theta_n)\rangle$ is

$$q_j(T_0^{(z)}, T_0^{(x)}|k_j') = \binom{T}{T_0^{(z)}}\binom{T}{T_0^{(x)}} \times \times \prod_b \left[p_{j,0}^{(b)}(k_j')\right]^{T_0^{(b)}} \left[p_{j,1}^{(b)}(k_j')\right]^{T-T_0^{(b)}}, \tag{14b}$$

and

$$q(T_0^{(z)}, T_0^{(x)}) = \frac{1}{2^n}\sum_{k_j'=0}^{2^n-1} q_j(T_0^{(z)}, T_0^{(x)}|k_j'). \tag{14c}$$

A sample of *a posteriori* probability distributions is depicted in Fig. 1, for $T = 8$, $T = 9$, and various events $\{T_0^{(z)}, T_0^{(x)}\}$. Different public-qubit states may give rise to a certain combination $\{T_0^{(z)}, T_0^{(x)}\}$ albeit with different probabilities. Hence, given a particular combination of "0" outcomes in the two bases, the conditional *a posteriori* probability distribution exhibits peaks for public-qubit states (as determined by $k_j\theta_n$), which are consistent with the particular event under consideration.

Eve's information gain is given by the difference of the Shannon entropies of the distributions before and after the measurements, i.e.,

$$\begin{aligned} I_{\rm av} &= H_{\rm prior} - \langle H_{\rm post}\rangle \\ &= n + \sum_{T_0^{(z)}}\sum_{T_0^{(x)}} q(T_0^{(z)}, T_0^{(x)}) \times \\ &\quad \times \sum_{k_j'=0}^{2^n-1} p_j(k_j'|T_0^{(z)}, T_0^{(x)}) \log[p_j(k_j'|T_0^{(z)}, T_0^{(x)})] \end{aligned} \tag{15}$$

where we have summed over all possible outcomes for a given state. The entropy of the *a priori* uniform probability distribution is equal to the entropy of the private-key bit k_j. As depicted in Fig. 2, this information gain is slightly below the

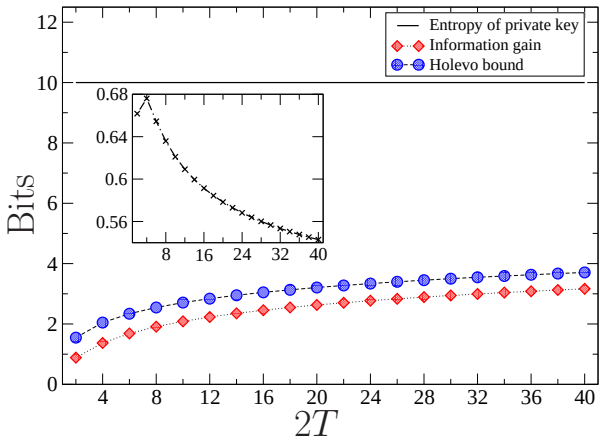

FIG. 2. (Color online) Entropy of *a priori* probability distribution (=entropy of private key), Holevo bound and information gain as functions of the number of public-key copies $2T$ that become available. The value of n affects considerably the *a priori* probability distribution. The inset shows the difference between the Holevo bound and the information gain.

Holevo bound of Eq. (A2) for $\tau = 2T$, which is tighter than the bound of Eq. (10). It is worth mentioning that although the information gain depends weakly on n the Holevo bound does not. In the subsequent discussion the choices of n and T are such that the inequality (A2) and thus also inequality (10) are satisfied for $\tau = 2T$.

2. *Probability of correct guessing the message*

As we have seen in the previous subsection, a particular outcome $\{T_0^{(z)}, T_0^{(x)}\}$ of a single run of the protocol allows Eve to update her knowledge on the public-qubit state she may have been given. From her point of view the *a posteriori* state pertaining to τ public-key copies is given by

$$\rho_{j,\rm post}^{(\tau)}(T_0^{(z)}, T_0^{(x)}) = \sum_{k_j'=0}^{2^n-1} p(k_j'|T_0^{(z)}, T_0^{(x)}) \times \times |\Phi_{k_j'}^{(\tau)}(\theta_n)\rangle\langle\Phi_{k_j'}^{(\tau)}(\theta_n)|\,. \tag{16}$$

Tracing out $\tau - 1$ copies, we obtain for the single-copy density operator the expression

$$\rho_{j,\rm post}^{(1)} = \sum_{k_j'} p(k_j'|T_0^{(z)}, T_0^{(x)})\,|\psi_{k_j'}(\theta_n)\rangle\langle\psi_{k_j'}(\theta_n)| \tag{17}$$

and the corresponding (estimated) Bloch vector

$$\tilde{\mathbf{R}}_j = \sum_{k_j'} p(k_j'|T_0^{(z)}, T_0^{(x)})[\cos(k_j'\theta_n)\hat{z} + \sin(k_j'\theta_n)\hat{x}] \tag{18}$$

with $||\tilde{\mathbf{R}}_j|| \neq 1$.

Recall now that the one-bit message m is encoded in the parity of an s-bit codeword $\mathbf{w}$ which is subsequently en-

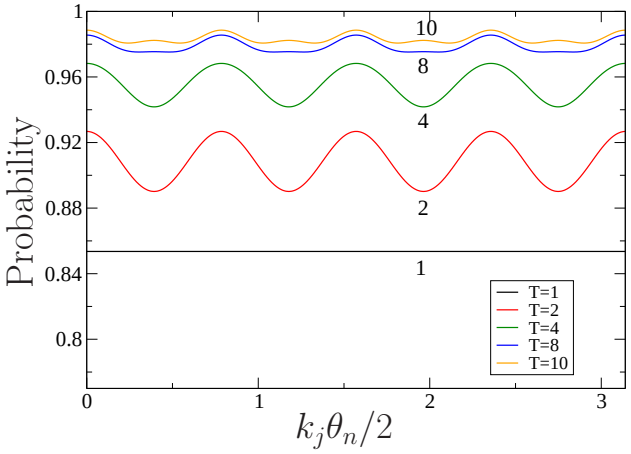

FIG. 3. (Color online) Conditional probability $P(\text{suc}|w_j, k_j)$ for $n = 10$ and various values of T.

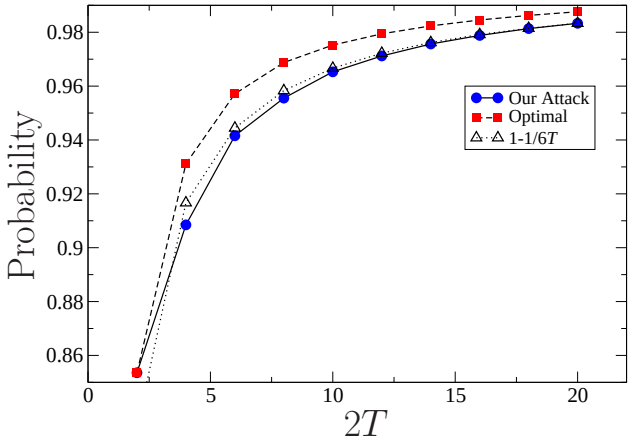

FIG. 4. (Color online) Conditional probability $P(\text{suc}|w_j)$ for $n = 10$ and various values of T.

crypted on s public qubits. Let us calculate first Eve's probability to recover the bit w_j in a single run of the protocol by measuring the corresponding cipher qubit in the basis defined by $\tilde{\mathbf{R}}_j$. For the particular encryption under consideration (see Sec. II) her probability of success is $P(\text{suc}|w_j, k_j, T_0^{(z)}, T_0^{(x)}) = \cos^2(\Omega_j/2)$ with Ω_j denoting the angle between the actual Bloch vector $\mathbf{R}_j$ and its estimation $\tilde{\mathbf{R}}_j$. Hence, we obtain

$$P(\text{suc}|w_j, k_j, T_0^{(z)}, T_0^{(x)}) = \frac{1}{2} + \frac{\tilde{\mathbf{R}}_j \cdot \mathbf{R}_j}{2||\tilde{\mathbf{R}}_j||}$$
$$= \frac{1}{2} + \frac{1}{2||\tilde{\mathbf{R}}_j||} \sum_{k_j'} p(k_j'|T_0^{(z)}, T_0^{(x)}) \cos[(k_j' - k_j)\theta_n] \quad (19)$$

with $\mathbf{R}_j$ defined in Sec. II. For a given public-qubit state various outcomes may occur albeit with different probabilities

$$P(\text{suc}|w_j, k_j) = \sum_{T_0^{(z)}} \sum_{T_0^{(x)}} P(\text{suc}|w_j, k_j, T_0^{(z)}, T_0^{(x)}) \times$$
$$\times q(T_0^{(z)}, T_0^{(x)}|k_j). \quad (20)$$

The typical behavior of $P(\text{suc}|w_j, k_j)$ with k_j (or equivalently $k_j\theta_n$) is depicted in Fig. 3 where we have an oscillation around the mean value

$$\bar{P}(\text{suc}|w_j) = \frac{1}{2^n} \sum_{k_j} P(\text{suc}|w_j, k_j). \quad (21)$$

As we increase the number of public-key copies the amplitude of the oscillations becomes smaller and the mean value increases. In particular, we find that for $T > 1$

$$\bar{P}(\text{suc}|w_j) \lesssim 1 - \frac{1}{6T} := U(T). \quad (22)$$

As depicted in Fig. 4, this performance is very close to the *optimal* probability of successful state estimation by means of collective measurements [27]

$$\bar{P}_{\text{opt}}(\text{suc}|w_j) = \frac{1}{2} + \frac{1}{2^{2T+1}} \sum_{i=0}^{2T-1} \sqrt{\binom{2T}{i}\binom{2T}{i+1}} \quad (23)$$

which scales like

$$\bar{P}_{\text{opt}}(\text{suc}|w_j) \sim 1 - \frac{1}{8T}. \quad (24)$$

Bagan *et al.* [28] have demonstrated that this upper bound can be saturated by means of individual measurements and our attack has similarities to their approach. Finally, for our subsequent discussion it is worth keeping in mind that $P(\text{suc}|w_j)$ does not depend on the actual value of the bit w_j i.e., $P(\text{suc}|w_j = 0) = P(\text{suc}|w_j = 1)$.

Up to now our results are referring to one bit of the codeword only and our task is to obtain the probability of success in guessing correctly the bit-message m from the s-bit codeword $\mathbf{w}$. Since the message is encoded on the parity of the codeword, Eve succeeds even if she fails to predict correctly α out of s bits with α even. Instead of considering her probability of success in a single run of the protocol, which is a rather complicated task, we concentrate in the following on her probability of success averaged over all possible public-qubit states (or equivalently private keys $\mathbf{k}$). As depicted in Fig. 3, for large T the amplitude of the oscillations is at least an order of magnitude smaller than the mean. Hence, any conclusions based on the average probability of success are also expected to apply with good accuracy to a single run of the protocol. Since each bit of the codeword is encrypted separately in independently prepared public qubits, the averaging over all possible values $\mathbf{k}$ is straightforward. Thus, one obtains for the average probability of successful eavesdropping for a given message m and codeword $\mathbf{w}$

$$\bar{P}_s(\text{suc}|m, \mathbf{w}) = \sum_{\substack{\alpha=0 \\ \text{even}}}^{s} \binom{s}{\alpha} [1 - \bar{P}(\text{suc}|w_j)]^\alpha \times$$
$$\times [\bar{P}(\text{suc}|w_j)]^{s-\alpha}. \quad (25a)$$

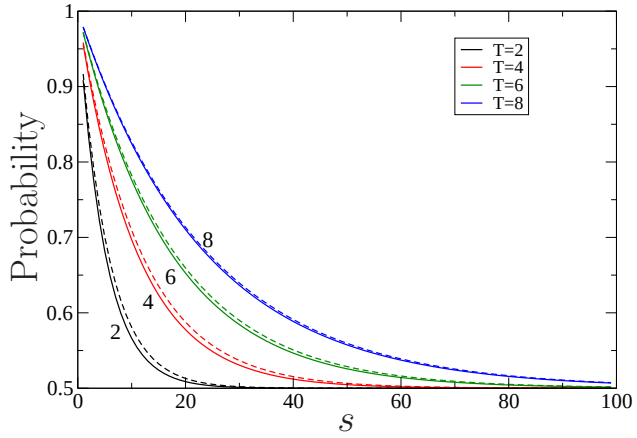

FIG. 5. (Color online) Average probability of success $\bar{P}_s(\text{success})$ as a function of codeword length s, for $n = 10$ and various values of T. The solid lines are numerical results obtained from Eqs. (25), whereas the dashed lines are for the upper bound defined in Eq. (26).

Averaging over all possible equally probable codewords and messages we finally find

$$\bar{P}_s(\text{suc}) = \bar{P}_s(\text{suc}|m, \mathbf{w}). \tag{25b}$$

In Fig. 5, $\bar{P}_s(\text{suc})$ is depicted as a function of the codeword length s for various numbers of public-key copies (solid lines). Clearly, the average probability of success decreases with increasing s whereas this drop becomes slower and slower as we increase the number of public-key copies. For $T > 1$ a rather tight upper bound for $\bar{P}_s(\text{suc})$ is given by the expression

$$\frac{1}{2} + \frac{1}{2}\left(1 - \frac{1}{3T}\right)^s \tag{26}$$

which is also plotted in Fig. 5 with dashed lines. A sketch of the proof of this upper bound is provided in Appendix B.

Now, let us assume that the users participating in the protocol have agreed in advance on a security parameter $\varepsilon \ll 1$ so that Eve's probability of success $\bar{P}_s(\text{suc})$ has to fulfill the relation $\bar{P}_s(\text{suc}) \leq 1/2 + \varepsilon$. This implies that the message bit m has to be encrypted in

$$s \geq \left| \frac{1 + \log_2(\varepsilon)}{\log_2\left(\frac{3T-1}{3T}\right)} \right| \tag{27}$$

qubits which is always fulfilled if

$$s \geq 3T|1 + \log_2(\varepsilon)|. \tag{28}$$

C. Comparison to the forward-search attack

The robustness of the present public-key encryption scheme against a forward-search attack based on a symmetry test in which Eve compares the cipher state with the public-key state is discussed in Ref. [10, 18]. The symmetry test of Ref. [10, 18] takes into account all the copies of the public keys but in contrast to the attacks discussed here it requires rather complicated quantum operations and gates, such as Fourier transformations and permutations on large numbers of qubits. Due to the nature of the attack the probability for successful eavesdropping does not vary from run to run and the probability for an eavesdropper to deduce the parity of the s-bit codeword and hence the message from the cipherstate is given by [18]

$$\bar{P}_s(\text{suc}) = \frac{1}{2} + \frac{1}{2}\left(1 - \frac{1}{2T}\right)^s. \tag{29}$$

It is rather surprising how close this exact expression is to the upper bound (26), which is slightly below the optimal probability of success. For a given security threshold ε the length of the codeword has to satisfy

$$s \geq T|1 + \log_2(\varepsilon)|. \tag{30}$$

which differs from Eq. (28) by a factor of three only.

D. A symmetry-test attack with projective measurements

In contrast to the previous attack we will consider here an attack which aims directly at the message rather than the private key and makes use of one copy of the public-key state and the cipherstate only. Eve pairs up the corresponding qubits of the public key and the cipher state i.e., the jth pair pertains to the jth qubits. The qubits of the jth pair are projected independently onto the same randomly chosen eigenbasis $\{|0_{\varphi_j}\rangle\}, |1_{\varphi_j}\rangle\}$ where

$$|\zeta_{\varphi_j}\rangle \;=\; (-1)^{\zeta}\cos\left(\frac{\varphi_j}{2}\right)|0_z\rangle + \sin\left(\frac{\varphi_j}{2}\right)|1_z\rangle \tag{31}$$

and φ_j is uniformly distributed over $[0, 2\pi)$. The probability of correct guessing either of the qubits is given by

$$F(k_j\theta_n, \varphi_j) \equiv |\langle\psi_{k_j}(\theta_n)|\zeta_{\varphi_j}\rangle|^2 = \cos^2\left(\frac{k_j\theta_n - \varphi_j}{2}\right). \tag{32}$$

However, since for a fixed value of k_j the angle φ_j is chosen at random, we can introduce a new random variable $\omega_{j,n} \equiv k_j\theta_n - \varphi_j$ uniformly distributed over the interval $[0, 2\pi)$. For later convenience let us also denote the number of wrong outcomes for the jth pair by e_j with $0 \leq e_j \leq 2$. As discussed in the last paragraph of Sec. II, the question that Eve has to answer is whether the states of the qubits in the jth pair are parallel or antiparallel. She obtains the correct answer if the outcomes of the measurements on the corresponding two qubits are either both correct $(e_j = 0)$ or both wrong $(e_j = 2)$. Thus, the probability of success in a single run of this protocol is given by

$$P(\text{suc}|w_j, k_j) = [F(\omega_{j,n})]^2 + [1 - F(\omega_{j,n})]^2. \tag{33}$$

If the one-bit message is encoded in the parity of an s-bit codeword which is subsequently encrypted on s qubits, Eve's strategy succeeds provided the total number of incorrect outcomes $e = \sum_{j=1}^{s} e_j$ is an even integer (e.g., see Table I for

public key	t,t	t,f	t,t	t,f	f,t	f,f	f,t	f,f
cipher state	t,t	t,f	f,f	f,t	t,f	t,t	f,t	f,f
e_1,e_2	0,0	0,2	1,1	1,1	1,1	1,1	2,0	2,2
e	0	2	2	2	2	2	2	4

TABLE I. Encryption of a single bit, on the state of two qubits ($s = 2$). Possible combinations of true (t) and false (f) outcomes that lead to correct estimation of the message.

$s = 2$). The total probability of success in a single run can be obtained by means of an iteration of the form (B3), where $Q^{(s)}$ is a multivariable function, i.e., $Q^{(s)}(\omega_{1,n}, \ldots \omega_{s,n}) \equiv P_s(\text{suc}|\mathbf{k}, \mathbf{w})$). Hence, Eve's probability of success in getting the correct parity and thus the correct message consists of two parts pertaining to possible combinations of outcomes from a single pair and the remaining $s-1$ pairs. More precisely, the first term refers to the case where the overall result on $s-1$ pairs as well as the result on the single pair are correct whereas for the second term Eve has failed in both cases.

Given that the probability $P_s(\text{suc}|\mathbf{k}, \mathbf{w})$ is a function of s uncorrelated random variables $\omega_{j,n}$, its analysis for $s > 2$ is rather cumbersome. Nevertheless, it is straightforward to obtain an analytic expression for the average probability of success $\bar{P}_s(\text{suc})$ by averaging over all possible keys and codewords which is equivalent to averaging over all possible combinations of $\{\omega_{s,j}\}$. Along the lines of Appendix B it can be proven that

$$\bar{P}_s(\text{suc}) = \frac{1}{2} + \frac{1}{2^{s+1}}. \tag{34}$$

Again, the average probability of success drops exponentially with increasing values of s. In contrast to Eqs. (26) and (29), this expression does not depend on T since the attack under consideration uses only one copy of the public key. It is, however, equivalent to the corresponding expression for the forward-search attack, i.e. Eq. (29) for $T = 1$. Hence, for a given security threshold ε the length of the codeword has to satisfy inequality (30) for $T = 1$.

IV. CONCLUSIONS

We have analyzed the security of a quantum-public-key encryption (QPKE) scheme that relies on single-qubit rotations. For a given number of public keys the symmetry underlying the protocol has been shown to restrict considerably the information gain that an eavesdropper might gain on the private key. This result suggests that new more efficient QPKE schemes could rely on quantum one-way functions, which explore symmetries in the involved quantum states. It is also worth recalling here the pivotal role of symmetries in quantum-key-distribution protocols, as a result of which qudit-based protocols can tolerate higher error rates than qubit-based ones [30].

The robustness of the protocol under consideration was mainly analyzed in the framework of an attack which takes into account all the public-key copies and is based on projective measurements on single qubits. As a main result it has been shown that the performance of this attack is comparable to the performance of optimal collective measurements [27] as well as to the forward-search attack of [18] which involves rather complicated quantum operations. Variants of the attack are expected to be applicable to other types of QPKE schemes as well.

ACKNOWLEDGEMENTS

This work is supported by CASED. We are grateful to Joe Renes for useful suggestions and discussions.

Appendix A: Properties of the density operator (9).

As for the matrix elements of the density operator of Eq. (9), we can distinguish two different cases:
Case 1: If $l + l'$ is an even number, the function $f_{\tau,l}(k_j\theta_n)f^{\star}_{\tau,l'}(k_j\theta_n)$ has even parity and does not change sign as we sum over all possible values of $k_j \in \mathbb{Z}_{2^n}$. Hence, we expect a non-zero contribution of $C_{l,l'}$ in this case.

Case 2: If $l+l'$ is an odd number, the element $C_{l,l'}$ vanishes since the parity of the overall trigonometric function in the sum is odd.

Another important property of the density operator (9) is that for fixed value of τ there seems to exist a critical value of n, let us say n_{c}, for which it is n-independent for all $n \geq n_{\text{c}}$. Furthermore, we have studied the rank of the density operator as well as the form of its eigenvalues for various values of n and τ. Our simulations show that for fixed τ, $\text{rank}[\rho^{(\tau)}_{\text{j,prior}}] < \tau + 1$ for all $n < n_{\text{c}}$ and thus the density operator is singular, whereas for $n \geq n_{\text{c}}$, $\text{rank}[\rho^{(\tau)}_{\text{j,prior}}] = \tau + 1$.

The von Neumann entropy of a quantum state is bounded from above by $\log_2(D)$ with D denoting the dimension of the support of the relevant density operator. In view of the hermiticity of $\rho^{(\tau)}_{j,\text{prior}}$ we have $D = \text{rank}[\rho^{(\tau)}_{j,\text{prior}}]$ and thus for a given pair of (τ, n) the entropy of the density operator is bounded from above by the corresponding entropy for (τ, n_{c}). Hence, we arrive again at the upper bound for the entropy provided in (10).

In order to obtain a tighter bound we can investigate eigenvalues of the density operator for (τ, n_{c}). Our simulations suggest that in this case the eigenvalues of (9) are given by

$$\lambda_i = \frac{1}{2^\tau}\binom{\tau}{i}. \tag{A1}$$

So, $S[\rho^{(\tau)}_{j,\text{prior}}]$ can be calculated as the entropy of the binomial distribution with mean $\tau/2$ and variance $\tau/4$. This entropy is bounded from above by the entropy of the the normal (Gaussian) distribution with the same mean and variance [29]. Thus, we obtain the result

$$S[\rho^{(\tau)}_{j,\text{prior}}] \leq \frac{1}{2}\log_2(\tau) + \frac{1}{2}\log_2(\pi e/2) \tag{A2}$$

and this bound is below the one of (10). Accordingly, the information gain is upper bounded by

$$I_{\rm av} \leq \frac{1}{2}\log_2(\tau) + \frac{1}{2}\log_2(\pi e/2). \quad \text{(A3)}$$

Appendix B: Proof of the upper bound (26).

The quantity we want to bound from above, i.e. $\bar{P}_s(\mathrm{suc})$, is a monotonously increasing function of $\bar{P}(\mathrm{suc}|w_j)$ for $\bar{P}(\mathrm{suc}|w_j) > 1/2$. Thus, in view of (22) we have

$$\bar{P}_s(\mathrm{suc}) = \sum_{\substack{\alpha=0 \\ \text{even}}}^{s} \binom{s}{\alpha} [1-\bar{P}(\mathrm{suc}|w_j)]^{\alpha} [\bar{P}(\mathrm{suc}|w_j)]^{s-\alpha} \quad \text{(B1)}$$

$$\leq \sum_{\substack{\alpha=0 \\ \text{even}}}^{s} \binom{s}{\alpha} [1-U(T)]^{\alpha} [U(T)]^{s-\alpha}. \quad \text{(B2)}$$

Let us denote the r.h.s of inequality (B2) by $Q^{(s)}(T)$. It can be shown by induction that $Q^{(s)}$ is equal to (26). To this end we note that $Q^{(s)}$ can be written alternatively in the form of an iteration, i.e.

$$Q^{(s)} = Q^{(1)}Q^{(s-1)} + \left[1-Q^{(1)}\right]\left[1-Q^{(s-1)}\right]. \quad \text{(B3)}$$

For $s=1$ the equality we want to show holds, i.e. we have

$$Q^{(1)} = U(T) = \frac{1}{2} - \frac{1}{2}\left(1 - \frac{1}{3T}\right) := \frac{1}{2} + \frac{\lambda}{2}. \quad \text{(B4)}$$

Assuming that it holds for s, i.e.

$$Q^{(s)} = \frac{1}{2} + \frac{\lambda^s}{2}, \quad \text{(B5)}$$

we can prove also that it holds for $s+1$, because

$$Q^{(s+1)} = \left(\frac{1}{2}+\frac{\lambda}{2}\right)\left(\frac{1}{2}+\frac{\lambda^s}{2}\right) + \left(\frac{1}{2}-\frac{\lambda}{2}\right)\left(\frac{1}{2}-\frac{\lambda^s}{2}\right) \quad \text{(B6)}$$

$$= \frac{1}{2} + \frac{\lambda^{s+1}}{2}. \quad \text{(B7)}$$

[1] D. Gottesman and I. L. Chuang, e-print arXiv:quant-ph/0105032.

[2] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, in *Proceedings of the 43rd Annual IEEE Symposium on the Foundations of Computer Science — FOCS '02*, (IEEE Computer Society Press, Washington, DC, 2002) pp. 449-458.

[3] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006).

[4] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001).

[5] L. M. Ioannou and M. Mosca, e-print arXiv:0810.2780.

[6] D. Gottesman, *Quantum public key cryptography with information-theoretic security*, Workshop on classical and quantum information security, Caltech, 15 - 18 December (2005), http://www.cpi.caltech.edu/quantum-security/program.html. See also http://perimeterinstitute.ca/personal/dgottesman/Public-key.ppt

[7] A. Kawachi, T. Koshiba, H. Nishimura, and T. Yamakami, in *Advances in Cryptology EUROCRYPT 2005*, Lect. Notes Comput. Sci. Vol. 3494 (Springer, 2005), pp. 268-284. See also arXiv:quant-ph/0403069.

[8] M. Hayashi, A. Kawachi, and H. Kobayashi, Quantum Inf. Comput. **8**, 0345 (2008).

[9] S. Kak, Found. Phys. Lett. **19**, 293 (2006).

[10] G. M. Nikolopoulos, Phys. Rev. A **77**, 032348 (2008); **78**, 019903(E) (2008).

[11] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[12] A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography* (CRC Press, 1996).

[13] K. Boström, and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).

[14] M. Lucamarini, and S. Mancini, Phys. Rev. Lett. **94**, 140501 (2005).

[15] W.-H. Kye, C.-M. Kim, M. S. Kim, and Y.-J. Park , Phys. Rev. Lett. **95**, 040501 (2005).

[16] For more information on the advantages of QPKE over protocols with point-to-point links the reader may look at chapter 1 of [12].

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

[18] G. M. Nikolopoulos and L. M. Ioannou , Phys. Rev. A **79**, 042327 (2009).

[19] The T' copies of the public key that are available can be used for up to T' encryptions (one key per encryption). In general, multiple copies can be issued by the same user at the purpose of encryptions or eavesdropping.

[20] The purpose of the parity encoding is to randomize our encryption scheme [18]. The encoding is publicly known, and the security parameter s has to be chosen judiciously so that security is guaranteed for a given number of public-key copies. Other types of randomization beyond parity encoding may be possible and equally efficient. A new security analysis of the protocol is required, if the accompanied encoding scheme differs from the one used here. Note also that analogous randomization techniques are used in conventional public-key encryption [12].

[21] In modern cryptography [12], confidentiality (secrecy) and authenticity are considered as distinct and independent cryptographic goals which are treated separately. Adopting the same attitude throughout this work we analyze the security of a par-

ticular public-key encryption scheme against certain types of attacks assuming that the possibility of an impersonation attack is prohibited by a reliable authentication scheme. The analysis of such an authentication scheme is beyond the scope of this work.

[22] Other encryption operations are also possible (e.g., mapping the different bit values on non-orthogonal qubit states), but they do not allow for a deterministic decoding. The following security analysis does not apply to this case.

[23] Strategies that do not respect this symmetry are not expected to offer anything more.

[24] This is essentially equivalent to the Schwinger representation of a spin-$\tau/2$ system in terms of two harmonic oscillators pertaining to $|0_z\rangle$ and $|1_z\rangle$.

[25] The robustness of the protocol (with respect to security of the private key), may be increased considerably if n is part of the private key and/or a random permutation is applied on the public qubits before they become publicly available [10].

[26] One public key has been issued by Bob for encryption of the message.

[27] R. Derka, V. Buzek and A. K. Ekert, Phys. Rev. Lett **80**, 1571 (1998).

[28] E. Bagan, M. Baig, and R. Munoz-Tapia, Phys. Rev. Lett **89**, 277904 (2002).

[29] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (John Wiley & Sons, New York, 1991).

[30] G. M Nikolopoulos and G. Alber, Phys. Rev. A **72**, 032320 (2005); G. M. Nikolopoulos, K. S. Ranade, G. Alber, Phys. Rev A **73**, 032325 (2006).