Deterministic quantum-public-key encryption: forward search attack and randomization

Georgios M. Nikolopoulos
Institute of Electronic Structure & Laser, FORTH, P.O. Box 1527, Heraklion 71110, Crete, Greece

Lawrence M. Ioannou
Center for Quantum Computation, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WA, UK

(Dated: November 5, 2018)

In the classical setting, public-key encryption requires randomness in order to be secure against a forward search attack, whereby an adversary compares the encryption of a guess of the secret message with that of the actual secret message. We show that this is also true in the information-theoretic setting — where the public keys are quantum systems — by defining and giving an example of a forward search attack for any deterministic quantum-public-key bit-encryption scheme. However, unlike in the classical setting, we show that any such deterministic scheme can be used as a black box to build a randomized bit-encryption scheme that is no longer susceptible to this attack.

PACS numbers: 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum-public-key cryptography, where the public keys are quantum-mechanical systems, was introduced by Gottesman and Chuang in Ref. [1], which contains an information-theoretically secure quantum digital signature scheme for signing classical messages. Other explorations within this information-theoretic framework include a no-go theorem for signing arbitrary quantum states [2], "lock and key" systems and distribution of quantum public keys [3], identification schemes [4], and — our focus in this paper — encryption schemes [5, 6, 7, 8, 9].

Roughly put, the purpose of an encryption scheme is to facilitate the communication of some secret information over an insecure channel, from a sender to a receiver, such that an adversary, who has access to this channel, cannot obtain anything close to a meaningful representation of the secret information. This secret information is called the *plaintext*, while the actual signal sent over the channel, which somehow *encodes* the plaintext, is called the *ciphertext*. In the classical setting, public-key encryption requires randomness in order to be secure against a forward search attack, whereby an adversary compares the ciphertext encoding a guess of the plaintext or — *test-plaintext* — with the ciphertext she is trying to decrypt (see Ref. [10] for more details in the classical setting). We show that this is also true in our information-theoretic setting (defined in Section II), by defining and giving an example of a forward search attack for any deterministic bit-encryption scheme that uses quantum public keys. However, unlike in the classical setting, we show that any such deterministic scheme can be used as a black box to build a randomized bit-encryption scheme that is no longer susceptible to this attack.

II. QUANTUM-PUBLIC-KEY ENCRYPTION

The potential for information-theoretic security in the quantum-public-key setting arises from the existence of a quantum function, mapping classical private keys (binary strings) to corresponding quantum public keys (quantum-mechanical systems), that is impossible to invert. More precisely, we have the following general setup. All users of the cryptosystem agree on a classical description of a set

$$A(n) \equiv \{\, |\Psi_x\rangle : x \in \{0,1\}^n \} \tag{1}$$

of $\log_2(d)$-qubit pure states (in general, $d = d(n)$) such that, for any distinct x and x' in $\{0,1\}^n$,

$$|\langle \Psi_{x'} | \Psi_x \rangle| < \delta \tag{2}$$

for some positive constant $\delta < 1$. Any user can now choose a uniformly random *private key* $k \in \{0,1\}^n$ and then generate and distribute (at most) T quantum-mechanical systems in or — *copies of* — the state $|\Psi_k\rangle$; each copy of $|\Psi_k\rangle$ constitutes one *(quantum) public key*. We assume that each public key reaches its intended recipient in an authenticated fashion. The bijective map

$$x \mapsto (T \text{ copies of } |\Psi_x\rangle) \tag{3}$$

is a one-way (quantum) function in the sense that, for a given $x \in \{0,1\}^n$, the deterministic preparation of a system in the state $|\Psi_x\rangle$ is possible via the classical description of $A(n)$, while the inversion of the map (with non-negligible probability) is guaranteed impossible by the Holevo bound [11] when

$$n \gg T \log_2(d). \tag{4}$$

This inequality thus sets an upper bound on the number T of public keys that can be publicly distributed, in order to ensure the secrecy of the private key, which is the minimal requirement for security of any cryptographic scheme in this framework. Note that the notion of computational efficiency may be ignored in an information-theoretic setting; however, there do exist constructions of $A(n)$ such that n is large enough that the set is cryptographically useful and such that, for all $x \in \{0,1\}^n$, a copy of $|\Psi_x\rangle$ can be computed in (quantum-) polynomial time from input x [1, 12].

Within the above framework, a *deterministic* quantum-public-key bit-encryption scheme may be defined by further specifying (and publishing, along with the description of $A(n)$) two unitary encryption operators, $\hat{\mathcal{U}}_0$ and $\hat{\mathcal{U}}_1$, and a decryption procedure whose exact form does not concern us. If Bob wants to communicate the plaintext $b \in \{0,1\}$ to Alice, he obtains an authenticated copy of Alice's public key, which is, by definition, in the state $|\Psi_k\rangle$, creates the (quantum) ciphertext in the state $|\Phi_{k,b}\rangle \equiv \hat{\mathcal{U}}_b |\Psi_k\rangle$, and sends it to Alice, who then decrypts and recovers the plaintext. Note that $\hat{\mathcal{U}}_0$ and $\hat{\mathcal{U}}_1$ do not depend on the private key k, but Alice's decryption procedure does.

Of course, in general, in our quantum setting, the plaintext can also be quantum, i.e., it can be a quantum-mechanical system in a particular state. Thus, we are focussing on the case where (a classical description of) the set of all possible (quantum) plaintexts consists of just two orthogonal states, $|0\rangle$ and $|1\rangle$. This is in fact the most general case from a security point of view: it may be seen as corresponding to the case where the adversary has narrowed down the plaintext to one of two maximally-distinguishable possibilities (of course, the states of the corresponding ciphertexts need not be orthogonal, depending on the encryption scheme; but, in any reasonable scheme, orthogonal plaintext-states would give rise to maximally-distinguishable ciphertexts, for a given key-value). However, we do not formally define what it means for an encryption scheme to be secure, because we do not prove security of any scheme; we only ever refer to security against a particular attack, i.e., our forward search attack.

In the following, we may abuse terminology by referring to quantum public keys or ciphertexts by their classical descriptions, i.e., by their states.

III. FORWARD SEARCH ATTACK BASED ON A SYMMETRY TEST

Before defining "(quantum) forward search attack", we should remind ourselves of what is the most general attack for uncovering the plaintext encoded by a particular ciphertext (as opposed to an attack that tries to compute the private key). If an adversary, Eve, wants to decide what the plaintext b is, given the ciphertext $|\Phi_{k,b}\rangle$ and all $(T-1)$ possible copies of the public key $|\Psi_k\rangle$, then she is ultimately faced with the problem of deciding which of the following two states she has:

$$\rho_0 \equiv \frac{1}{2^n}\sum_x |\Psi_x\rangle\langle\Psi_x|^{\otimes(T-1)}|\Phi_{x,0}\rangle\langle\Phi_{x,0}| \tag{5}$$

$$\rho_1 \equiv \frac{1}{2^n}\sum_x |\Psi_x\rangle\langle\Psi_x|^{\otimes(T-1)}|\Phi_{x,1}\rangle\langle\Phi_{x,1}|. \tag{6}$$

The optimal procedure ("POVM") for solving this "binary quantum decision problem" is given in Refs. [13, 14] and depends on ρ_0, ρ_1, and the prior probability distribution $(p, 1-p)$ of the plaintext b (i.e. $P[b=0]=p$). We assume that Eve can implement this optimal procedure, since we do not place any computational resource-bounds on her. The probability of success of this optimal procedure, which is affinely related to the trace distance between $p\rho_0$ and $(1-p)\rho_1$, is in general difficult to calculate.

In this paper, we concentrate on a restricted class of attacks that attempt to uncover the plaintext encoded by a particular ciphertext.

Definition 1 (Forward search attack)**.** A *forward search attack* on a deterministic quantum-public-key bit-encryption scheme is any (quantum) algorithm — independent of the encryption and decryption operations and the structure of the set of public keys — that outputs the plaintext with some probability of error, given one copy of the actual ciphertext and all available copies of the ciphertext encoding a test-plaintext.

As an aside, we note that this definition subsumes the definition of "forward search attack" for computationally-secure, classical public-key bit-encryption schemes that are implemented quantum-mechanically [15]. In the following, we give a simple forward search attack that we suspect is near to the optimal forward search attack and whose probability of success is easily computed. To simplify our presentation, we assume that each plaintext is equally likely and thus always use the test-plaintext 0 without loss of generality.

Following Ref. [12], we first define a problem that captures the essence of Eve's task of determining the plaintext via forward search attack (i.e. ignoring all structure of the particular cryptosystem), and then we give a solution for it, based on a test for symmetry.

Definition 2 ($(1, N-1)$-copy state distinguishing problem)**.** Given one copy of $|\xi\rangle \in \mathbb{C}^d$ and $(N-1)$ copies of $|\chi\rangle \in \mathbb{C}^d$ such that either $|\xi\rangle = |\chi\rangle$ or $|\langle\xi|\chi\rangle| = \lambda < 1$, decide which case holds.

To solve this problem with some probability of error, we can use the *symmetry-test* procedure depicted in Fig. 1, which we now explain. Let S_N be the set of all $N!$ permutations on N objects and let $\sigma \in S_N$. The operator $\hat{\mathcal{F}}$ is the $(N!)$-dimensional quantum Fourier transform [12], so that, in particular,

$$\hat{\mathcal{F}}|0\rangle = \frac{1}{\sqrt{N!}}\sum_{\sigma\in S_N}|\sigma\rangle, \tag{7}$$

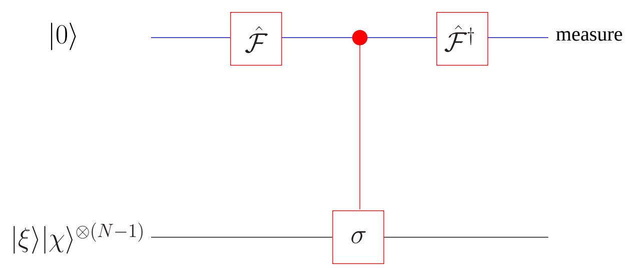

FIG. 1: (Color online) Symmetry-test for the $(1, N-1)$-copy state distinguishing problem. The top (blue) wire is a $N!$-dimensional quantum system, whose state-space is spanned by the computational basis states, each of which is labeled by a permutation $\sigma \in S_N$ (e.g. $|0\rangle$ corresponds to the identity permutation). The bottom wire represents N registers, each of dimension d.

and the controlled-σ operator permutes the N target registers according to the permutation σ encoded by the computational-basis-state of the control register. The probability of the final measurement in the computational basis of the top register resulting in outcome "0" is 1 when $|\xi\rangle = |\chi\rangle$. But when $\langle\xi|\chi\rangle = \lambda < 1$, this probability is

$$\left\| (|0\rangle\langle 0| \otimes I) \frac{1}{\sqrt{N!}} \sum_{\sigma \in S_N} \hat{\mathcal{F}}^\dagger \, |\sigma\rangle \sigma(\, |\xi\rangle \, |\chi\rangle^{\otimes(N-1)}) \right\|^2 \tag{8a}$$

$$= \left\| \frac{1}{\sqrt{N!}} \sum_{\sigma \in S_N} \langle 0| \, \hat{\mathcal{F}}^\dagger \, |\sigma\rangle \sigma(\, |\xi\rangle \, |\chi\rangle^{\otimes(N-1)}) \right\|^2$$

$$= \left\| \frac{1}{N!} \sum_{\sigma \in S_N} \sigma(\, |\xi\rangle \, |\chi\rangle^{\otimes(N-1)}) \right\|^2$$

$$= \frac{1}{N!^2} \sum_{\sigma, \tau \in S_N} \tau(\langle\xi| \, \langle\chi| \,^{N-1}) \sigma(\, |\xi\rangle \, |\chi\rangle^{N-1})$$

$$= \frac{1}{N!^2} \sum_{\sigma, \tau \in S_N} \langle\xi| \, \langle\chi| \,^{N-1} \tau^{-1} \sigma(\, |\xi\rangle \, |\chi\rangle^{N-1})$$

$$= \frac{1}{N!} \sum_{\sigma \in S_N} \langle\xi| \, \langle\chi| \,^{N-1} \sigma(\, |\xi\rangle \, |\chi\rangle^{N-1})$$

$$= \frac{(N-1)!(1!)}{N!} \left(\binom{N-1}{0}(1) + \binom{N-1}{1}(|\langle\xi|\chi\rangle|^2) \right)$$

$$= \frac{1}{N}(1 + (N-1)\lambda^2), \tag{8b}$$

which we denote $q_{N,\lambda}$. Thus, we only care whether the measurement outcome is "0" or not: in case it is "0", we guess that $|\xi\rangle = |\chi\rangle$ (but we might be wrong); otherwise, we know that $\langle\xi|\chi\rangle = \lambda < 1$. With this strategy, we can only make an error when $\langle\xi|\chi\rangle = \lambda < 1$, in which case the error probability is $q_{N,\lambda}$.

Thus, to perform a *forward search attack by symmetry-test*, Eve applies the above procedure (and decision strategy), with

$$|\xi\rangle \equiv |\Phi_{k,b}\rangle, \tag{9}$$
$$|\chi\rangle \equiv |\Phi_{k,0}\rangle, \tag{10}$$

and the maximum possible N. For a (non-classical) quantum-public-key bit-encryption scheme, Eve can use $N = T$, thus obtaining one-sided error $q_{T,\lambda}$ [16]. Although we only suspect that this forward search attack is nearly the optimal one, we note that the same symmetry-test procedure is nearly optimal for the "(N', N')-copy state distinguishing problem", where one is given N' copies each of $|\xi\rangle$ and $|\chi\rangle$ (and the procedure permutes $2N'$, instead of N, target registers) [12]. In the remainder of this work, we show that our assumption that Eve's probability of correctly guessing the plaintext (by forward search attack) is bounded away from 1 leads to a simple randomized encryption scheme that uses the original deterministic scheme as a black box and is resistant to our forward search attack.

IV. RANDOMIZATION AGAINST FORWARD SEARCH ATTACK

Any deterministic public-key bit-encryption scheme, quantum or classical, is susceptible to a forward search attack. However, if the scheme can be *nontrivially extended* to encrypting multiple-bit plaintexts — by which we mean that the multiple-bit scheme is not merely the concatenation of instances of the original single-bit scheme — one possible way to guard against a forward search attack is to use the following *parity encoding*. If the desired plaintext is $b \in \{0, 1\}$, Bob should first choose a uniformly random, binary-string *codeword* w, whose length is $s > 1$ and whose (Hamming) weight (sum of the bits) has parity b, and then encrypt b by using the s-bit version of the deterministic scheme to encrypt w, i.e., the new ciphertext encoding b is actually the ciphertext encoding w. Assuming Alice knows that the intended plaintext b is actually the parity of the weight of w, then this forms a randomized bit-encryption scheme that, for sufficiently large s, may not be susceptible to the forward search attack (of course, we do not claim that the use of the parity encoding results in a secure bit-encryption scheme, in general). The parameter s thus functions as a "security parameter".

Now consider the case where the original deterministic bit-encryption scheme has no nontrivial extension to multiple-bit plaintexts. Can it be used several times (under different key-values) as a black box, in order to create a randomized scheme that is potentially secure against a *compound forward search attack*, whereby Eve does a forward search attack on every instance of the original scheme? In the classical setting, the answer is clearly "no": Eve would learn the correct plaintext in every instance of the original scheme, so Alice would have no advantage over her. In our quantum setting, however, the answer to this question is "yes", as shown by the following randomized bit-encryption scheme, which just combines the above parity encoding with the trivial multiple-bit extension of the original scheme. Assume that Alice's public key is now $\otimes_{i=1}^{s}|\Psi_{k_i}\rangle$, where each k_i is uniformly randomly chosen from $\{0,1\}^n$. To encrypt plaintext $b \in \{0,1\}$, Bob again first chooses a uniformly random codeword w, whose length is $s > 1$ and whose weight has parity b. The ciphertext that encodes b is now simply $\otimes_{i=1}^{s}|\Phi_{k_i,w_i}\rangle$, where $w = w_1 w_2 \cdots w_s$. Alice decrypts to get w, and thus the intended plaintext b as the parity of the weight of w.

Consider Eve's compound forward search attack by symmetry-test on this new scheme, whereby Eve does s separate forward search attacks by symmetry-test as described in the previous section, one for each value of i. We now assume that distinct ciphertexts (under the same key-value) in the original bit-encryption scheme are orthogonal, i.e., $\lambda \equiv \langle\Phi_{k_i,0}|\Phi_{k_i,1}\rangle = 0$ for all i (this restricts to schemes where decryption is perfect). Assuming Eve uses $|\chi\rangle = |\Phi_{k_i,0}\rangle$ for all i, she can only fail in guessing w_i correctly when $w_i = 1$. Each codeword w has a weight α of well defined parity. Thus, a codeword will be decrypted correctly if, for some even $\gamma \in \{0,1,\ldots,\alpha\}$, γ out of α symmetry-tests give measurement outcome "0" and $(\alpha-\gamma)$ symmetry-tests give a different outcome. On average, the probabilities for Eve to decrypt successfully each of the bit values are

$$P^{(s)}(\text{success}|b=0) = \frac{1}{2^{s-1}} \sum_{\substack{\alpha=0 \\ \text{even}}}^{s} \sum_{\substack{\gamma=0 \\ \text{even}}}^{\alpha} \binom{s}{\alpha}\binom{\alpha}{\gamma} q^{\gamma}(1-q)^{\alpha-\gamma}, \tag{11}$$

$$P^{(s)}(\text{success}|b=1) = \frac{1}{2^{s-1}} \sum_{\substack{\alpha=1 \\ \text{odd}}}^{s} \sum_{\substack{\gamma=0 \\ \text{even}}}^{\alpha} \binom{s}{\alpha}\binom{\alpha}{\gamma} q^{\gamma}(1-q)^{\alpha-\gamma}, \tag{12}$$

where $q \equiv q_{T,0}$. Since we assume both plaintexts are equally probable, we have

$$\begin{aligned} & P^{(s)}(\text{success}) \\ &= \frac{1}{2}\left[P^{(s)}(\text{success}|b=0) + P^{(s)}(\text{success}|b=1)\right] \\ &= \frac{1}{2} + \frac{(1-q)^s}{2} \qquad (13) \\ &= \frac{1}{2} + \frac{(T-1)^s}{2T^s}, \qquad (14) \end{aligned}$$

where the second-last line follows by mathematical induction on s [17].

Assume now that Alice and Bob have agreed in advance on a security threshold $\epsilon \ll 1$, such that Eve's probability of success is restricted to slightly above random guessing, i.e., $P^{(s)}(\text{success}) \leq 1/2 + \epsilon$. This immediately implies that the plaintext b has to be encoded on

$$s \geq \left|\frac{1+\log_2(\epsilon)}{\log_2\left(\frac{T-1}{T}\right)}\right| \tag{15}$$

qubits. Working on the right-hand side of this inequality, we may derive a less tight, but simpler lower bound, namely

$$s \geq T|1+\log_2(\epsilon)|. \tag{16}$$

Assuming our forward search attack is the optimal one, this condition is sufficient to thwart Eve's compound forward search attack on the randomized bit-encryption scheme.

V. SUMMARY

We have introduced the forward search attack in the framework of quantum-public-key encryption, which aims at recovering the plaintext from the ciphertext without reference to the structure of the particular encryption scheme. As in the classical public-key setting, any deterministic encryption scheme that uses quantum public keys is susceptible to such an attack, unless some sort of randomization is used.

Several quantum-public-key encryption schemes have been proposed, the three most notable ones appearing in Refs. [5, 6, 9]. The schemes in Refs. [5, 6] are randomized, with nontrivial extensions to multiple-bit plaintexts, and thus they are not vulnerable to a forward search attack [18]. The scheme in Ref. [9] is randomized in the way we have presented in Sec. IV; our work places that scheme in the wider cryptographic context. In terms of computational efficiency, we note that the schemes in Refs. [5, 6] require scalable quantum computing in order to be secure against our forward search attack, whereas the scheme in Ref. [9] requires only single-qubit rotations about a fixed axis.

VI. ACKNOWLEDGEMENTS

We would like to thank Daniel Gottesman for helpful discussions. L. M. Ioannou acknowledges support from the EPSRC and SCALA. G. M. Nikolopoulos acknowledges partial support from the EC RTN EMALI (contract No. MRTN-CT-2006-035369).

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

[5] 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://www.perimeterinstitute.ca/personal/dgottesman/Public-key.ppt.

[6] 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.

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

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

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

[10] O. Goldreich, *Foundations of Cryptography* (Cambridge University Press, Cambridge, 2004), Vol. 2.

[11] A. S. Holevo, in *Proceedings of the Second Japan-USSR Symposium on Probability Theory*, edited by G. Maruyama and J. V. Prokhorov, Lect. Notes Math. Vol. 330 (Springer-Verlag, Berlin, 1973), pp. 104-119.

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

[13] C. A. Fuchs, PhD Thesis, University of New Mexico, 1995. See also e-print arXiv:quant-ph/9601020.

[14] C. W. Helstrom, *Quantum Detection and Estimation Theory*, Mathematics in Science and Engineering (Academic Press, New York, 1976), Vol. 123.

[15] For this to be true, the only assumption needed is that the set of ciphertexts of any such scheme is a subset of the computational basis, so that the outcome of a joint measurement with respect to the computational basis of the actual ciphertext and one copy of the test-ciphertext determines with certainty whether the two ciphertexts are identical.

[16] For a classical, computationally-secure scheme implemented quantum-mechanically, Eve can use arbitrarily large N so that her error is arbitrarily close to zero, as we would expect.

[17] The proof consists of two steps. First, it can be shown that Eq. (13) holds for $s=1$, i.e., $P^{(1)}(\text{success}) = [1+(1-q)]/2$. Second, assuming that Eq. (13) holds for s, one can show that it also holds for $s+1$. In this last step, one needs basic identities of binomial coefficients, including $\sum_{j=0}^{n}\binom{s}{j} = 2^n$ and Pascal's rule $\binom{n}{j}+\binom{n}{j+1} = \binom{n+1}{j+1}$.

[18] The mere fact that a (qu)bit-encryption scheme is randomized is not necessarily enough for our forward search attack to be ineffective: if the amount of randomness is dependent on (i.e. limited by) the size of the plaintext, then the s-(qu)bit extension of the scheme may have to be used in order to get a secure bit-encryption scheme (even though the single-qubit-encryption scheme may be secure for uniformly random qubit-plaintext with respect to the Haar measure), by encoding the intended plaintext $b \in \{0,1\}$ as the ciphertext that encodes the multi-qubit plaintext $|b\rangle^{\otimes s}$, for some $s>1$.