# Phase-covariant quantum cloning

Dagmar Bruß,[1] Mirko Cinchetti,[2] G. Mauro D'Ariano,[2] and Chiara Macchiavello[2]
[1]*Institut für Theoretische Physik, Universität Hannover, Appelstraße 2, D-30167 Hannover, Germany*
[2]*Dipartimento di Fisica ''A. Volta'' and INFM-Unità di Pavia, Via Bassi 6, 27100 Pavia, Italy*

(Received 14 September 1999; published 7 June 2000)

We consider an $N \to M$ quantum cloning transformation acting on pure two-level states lying on the equator of the Bloch sphere. An upper bound for its fidelity is presented, by establishing a connection between optimal phase-covariant cloning and phase estimation. We give the explicit form of a cloning transformation that achieves the bound for the case $N=1$, $M=2$, and find a link between this case and optimal eavesdropping in the quantum cryptographic scheme BB84.

PACS number(s): 03.67.Dd, 03.65.−w

## I. INTRODUCTION

Perfect quantum cloning of a set of input states that contains at least two nonorthogonal states is impossible [1]. However, it is interesting to study how well we can approximate a perfect cloning procedure. We can expect different results depending on the set of input states considered. In particular, we expect that the smaller the set of inputs, i.e., the more information about the input is given, the better one can clone each of its states.

We analyze the case of pure qubits, i.e., vectors of a two-dimensional Hilbert space $\mathcal{H} \simeq \mathbb{C}^2$. Optimal $N \to M$ cloning transformations (i.e., transformations which act on $N$ identical inputs and create $M$ outputs) for the largest set of input qubits, namely, for qubits belonging to the whole Hilbert space, have been recently proposed [2–4]. Since a crucial requirement for such transformations is that their efficiency is the same for all input states, they were called universal cloning transformations.

In this paper we will analyze cloning transformations that are optimal for a restricted set of input states, namely, pure states of the form

$$|\psi_\phi\rangle = \frac{1}{\sqrt{2}}[|0\rangle + e^{i\phi}|1\rangle], \tag{1}$$

where $\phi \in [0,2\pi)$ and $\{|0\rangle,|1\rangle\}$ represent a basis for a qubit. We call the qubits of this form ''equatorial'' because the $z$ component of their Bloch vector is zero, i.e., the Bloch vector is restricted to the intersection of the $x$-$y$ plane with the Bloch sphere. The parameter $\phi$ is the angle between the Bloch vector and the $x$ axis.

Studying the restriction of the input set to the equator is motivated by physical implementations of quantum communication ideas (all existing quantum cryptographic experiments are using states that are on the equator, rather than states that span the whole Bloch sphere) as well as by fundamental questions in quantum information processing. As we will show in this paper, restricting to equatorial states makes the cloning problem related to phase estimation. This connection can be exploited in order to derive bounds for the optimal cloning fidelity. As expected, restriction of the cloning symmetry improves the cloning performance.

The paper is organized as follows. In Sec. II we describe the general operation of a phase-covariant cloning transformation. In Sec. III we establish the connection between phase-covariant cloning and phase estimation, and prove an upper bound on the fidelity of an $N \to M$ phase-covariant cloner acting on equatorial qubits. In Sec. IV we derive the explicit form of the $1 \to 2$ cloning transformation for equatorial qubits that saturates the bound, and point out a connection to eavesdropping in quantum cryptography.

## II. PHASE-COVARIANT CLONING TRANSFORMATIONS

In this section we consider cloning transformations with the requirement that the fidelity is the same for any equatorial qubit, i.e., it does not depend on the value of the phase $\phi$. We call such cloners ''phase-covariant cloners'' (pcc).

We describe the action of an $N \to M$ phase-covariant cloner on the $N$ input qubits by means of a completely positive (CP) map $T_{NM}$ [5]. We will consider only pure input states of the form $|\psi_\phi\rangle\langle\psi_\phi|^{\otimes N}$, namely, product states made of $N$ identical copies. The output of the map is generally a mixed state $\rho_M$ of the $M$ output qubits. In order to guarantee that all the output copies are described by the same density operator we require that $\rho_M$ is supported on the symmetric subspace of the total Hilbert space of the $M$ output qubits (the symmetric subspace is defined as the space spanned by all pure states which are invariant under any permutation of the constituent qubits). The density operator describing the state of each output qubit is given by

$$\rho^{out} = R[T_{NM}(|\psi_\phi\rangle\langle\psi_\phi|^{\otimes N})], \tag{2}$$

where $R$ denotes the partial trace over all but one output qubits. The phase-covariance condition corresponds to imposing the following requirement on the operation of the cloning map:

$$U_\chi \rho^{out} U_\chi^\dagger = R[T_{NM}(U_\chi^{\otimes N}|\psi\rangle\langle\psi|^{\otimes N} U_\chi^{\dagger\otimes N})] \tag{3}$$

for any pure state $|\psi\rangle$ and all unitary phase-shift operators $U_\chi = \exp[-i/2(\sigma_z - \mathbb{1})\chi]$, where $\chi \in [0,2\pi)$ and $\sigma_z$ is the Pauli operator diag$\{1,-1\}$.

We define the quality of the cloning transformation in terms of the fidelity between the reduced density operator of each output copy and the input state $|\psi_\phi\rangle$

$$F=\langle \psi_\phi|\rho^{out}|\psi_\phi\rangle. \tag{4}$$

In the Appendix we show that without loss of generality any phase-covariant cloning transformation can be completely described in terms of two shrinking factors $\eta_{xy}(N,M)$ and $\eta_z(N,M)$. The former describes the shrinking of the component of the Bloch vector lying in the $x$-$y$ plane of the Bloch sphere, the latter the shrinking of the component along the $z$ direction, namely, the state of each output copy is

$$\rho^{out}=\frac{1}{2}[\mathbb{1}+\eta_{xy}(N,M)(s_x\sigma_x+s_y\sigma_y)+\eta_z(N,M)s_z\sigma_z], \tag{5}$$

where $s_i$ are the components of the Bloch vector of the initial state $|\psi\rangle$ of each of the $N$ input copies. Therefore, for equatorial qubits, the cloner leads to an isotropic shrinking, namely, the density operator of each output copy (2) is given by

$$\rho^{out}=\eta_{xy}(N,M)|\psi_\phi\rangle\langle\psi_\phi|+\frac{1}{2}[1-\eta_{xy}(N,M)]\mathbb{1}, \tag{6}$$

where $\mathbb{1}$ is the identity operator. Thus, for equatorial qubits the action of a phase-covariant cloner is completely specified in terms of the equatorial shrinking factor $\eta_{xy}(N,M)$ and the fidelity is $F_{pcc}(N,M)=[1+\eta_{xy}(N,M)]/2$.

## III. OPTIMAL CLONING OF EQUATORIAL QUBITS

In this section we derive an upper bound for the shrinking factor $\eta_{xy}(N,M)$ of a phase-covariant cloner for equatorial qubits. Our derivation is similar to the one of universal cloners [3]. It is based on the concatenation property of phase-covariant cloners and on the link to phase estimation, as shown in the following.

### A. Concatenation of phase-covariant cloners

We concatenate two phase-covariant cloners as follows. The first is an $N\rightarrow M$ cloner acting on $N$ equatorial qubits, the second one acts on the output state $\rho_M$ of the $M$ output qubits of the first cloner and gives $L$ output copies. We show in the following that the sequence of these two cloning transformations is a phase covariant cloner with a shrinking factor $\eta_{xy}$ for the $x$-$y$ plane that is the multiplication of the shrinking factors $\eta_{xy}$ of the two separate cloners, namely,

$$\eta_{xy}(N,L)=\eta_{xy}(N,M)\,\eta_{xy}(M,L). \tag{7}$$

In order to prove the above property we exploit the decomposition of a density operator supported on the symmetric subspace [4],

$$\rho_M=\sum_i \beta_i|\psi_i\rangle\langle\psi_i|^{\otimes M}, \tag{8}$$

with $\beta_i\in\mathbb{R}$ (not necessarily positive) and $\Sigma_i\beta_i=1$.

Using the shrinking character of the phase covariant cloning transformation described in the previous section and the linearity of the cloning map we can write the following conditions for the output of the $N\rightarrow M$ cloner acting on $N$ pure qubits in the generic pure state $|\psi\rangle$ with (unit-length) Bloch vector $\vec{s}$:

$$\sum_i \beta_i s_{xi}=\eta_{xy}(N,M)s_x,$$
$$\sum_i \beta_i s_{yi}=\eta_{xy}(N,M)s_y, \tag{9}$$
$$\sum_i \beta_i s_{zi}=\eta_z(N,M)s_z,$$

where $s_{xi}$ denotes the $x$ component of the Bloch vector of state $|\psi_i\rangle\langle\psi_i|$, and accordingly for $y,z$.

The reduced density operator describing each of the $L$ copies at the output of the second cloner is given by

$$\begin{aligned}R[T_{ML}(\rho_M)]&=\sum_i \beta_i R[T_{ML}(|\psi_i\rangle\langle\psi_i|^{\otimes M})]\\&=\sum_i \beta_i\biggl\{\frac{1}{2}[\mathbb{1}+\eta_{xy}(M,L)(s_{xi}\sigma_x+s_{yi}\sigma_y)\\&\quad+\eta_z(M,L)s_{zi}\sigma_z]\biggr\}.\end{aligned} \tag{10}$$

By using Eqs. (9) the above expression takes the form

$$\begin{aligned}R[T_{ML}(T_{NM}(|\psi\rangle\langle\psi|^{\otimes N}))]=\frac{1}{2}[&\mathbb{1}+\eta_{xy}(N,M)\,\eta_{xy}(M,L)\\&\times(s_x\sigma_x+s_y\sigma_y)\\&+\eta_z(N,M)\,\eta_z(M,L)s_z\sigma_z],\end{aligned} \tag{11}$$

namely the concatenation property holds. For input qubits from the equator the Bloch vector of each copy at the output of the two cloners is simply shrunk in the $x$-$y$ plane by the factor $\eta_{xy}(N,M)\,\eta_{xy}(M,L)$.

### B. Phase-covariant cloning and phase estimation

We will now prove the following connection between phase-covariant cloners and phase estimation of equatorial qubits:

$$\eta_{xy}^{opt}(N,\infty)=\overline{\eta}_{pe}^{opt}(N). \tag{12}$$

The quantity $\eta_{xy}^{opt}(N,M)$ is the shrinking factor in the $x$-$y$ plane of the optimal $N\rightarrow M$ phase-covariant cloner, while $\overline{\eta}_{pe}^{opt}(N)$ is the shrinking factor of the reconstructed reduced density operator after performing phase estimation (pe) on $N$ equatorial qubits.

The aim of phase estimation is to find the optimal strategy to estimate the value of the phase $\phi$ [6]. This is described in terms of a positive-operator valued measure (POVM), namely, $d\mu(\phi_*)$, where $\phi_*$ is the estimated value of the phase, $d\mu(\phi_*)\geqslant 0$, and $\int(d\phi_*/2\pi)d\mu(\phi_*)=\mathbb{1}$. The outcome of each instance of measurement provides, with probability $p(\phi|\phi_*)=\mathrm{Tr}[d\mu(\phi_*)|\psi_\phi\rangle\langle\psi_\phi|]$, the ''candidate'' $|\psi_{\phi*}\rangle$ for $|\psi_\phi\rangle$. The fidelity of phase estimation can be calculated from the outcomes of the measurement as

$$\overline{F}_{pe}(N)=\int\frac{d\phi_*}{2\pi}p(\phi|\phi_*)|\langle\psi_\phi|\psi_{\phi_*}\rangle|^2=\langle\psi_\phi|\overline{\varrho}_\phi|\psi_\phi\rangle, \tag{13}$$

where $\overline{\varrho}_\phi=\int(d\phi_*/2\pi)p(\phi|\phi_*)|\psi_{\phi_*}\rangle\langle\psi_{\phi_*}|$ is the reconstructed density operator. For covariant phase estimation the fidelity does not depend on $\phi$, thus for the optimal procedure $\overline{\varrho}_\phi$ can also be written as

$$\overline{\varrho}_\phi=\overline{\eta}_{pe}(N)|\psi_\phi\rangle\langle\psi_\phi|+\frac{1}{2}[1-\overline{\eta}_{pe}(N)]\mathbb{1}, \tag{14}$$

namely, the input state is shrunk by the factor $\overline{\eta}_{pe}(N)=2\overline{F}_{pe}(N)-1$.

The fidelity for optimal covariant phase estimation of equatorial qubits, derived in Ref. [7], takes the form

$$\overline{F}_{pe}^{opt}(N)=\frac{1}{2}+\frac{1}{2^{N+1}}\sum_{l=0}^{N-1}\sqrt{\binom{N}{l}\binom{N}{l+1}}. \tag{15}$$

In order to prove Eq. (12) we first notice that after performing optimal phase estimation on $N$ equatorial qubits all in state $|\psi_\phi\rangle$ we can prepare a state of $L$ qubits, supported on the symmetric subspace, where each qubit is described by the reduced density operator (14). This procedure can be viewed as a phase covariant cloner and therefore it cannot perform better than the optimal $N\rightarrow L$ phase covariant cloning transformation. Thus we can write the inequality

$$\overline{\eta}_{pe}^{opt}(N)\leqslant\eta_{xy}^{opt}(N,L), \tag{16}$$

which holds for any value of $L$, and in particular for $L\rightarrow\infty$.

We will now prove the opposite inequality (which holds for $L\rightarrow\infty$ only): we concatenate a phase-covariant $N\rightarrow L$ cloner, acting on equatorial qubits, with a subsequent optimal *state* estimation (se) procedure (note that state estimation on qubits includes also an estimate of their phase). The whole procedure can be seen as a *phase* estimation performed on the input $|\psi_\phi\rangle\langle\psi_\phi|^{\otimes N}$, with fidelity

$$\overline{F}_{pe}(N)=\langle\psi_\phi|\Lambda_L(\rho_L)|\psi_\phi\rangle,$$

$$\Lambda_L(\rho_L)=\sum_\mu \mathrm{Tr}[P_\mu\rho_L]|\psi_\mu\rangle\langle\psi_\mu|,$$

where $\rho_L$ is the output of the cloner and $\Lambda_L(\rho_L)$ is the CP map of the state estimation of $L$ qubits, $\{P_\mu\}$ represents the set of optimal POVM's for state estimation of $L$ qubits [8,7] and $|\psi_\mu\rangle$ denotes the candidate for $|\psi\rangle$ when performing the measurement $P_\mu$. Since $\rho_L$ is supported on the symmetric subspace, we use again the decomposition $\rho_L=\Sigma_i\beta_i|\psi_i\rangle\langle\psi_i|^{\otimes L}$ and obtain

$$\begin{aligned}\overline{F}_{pe}(N)&=\sum_i\langle\psi_\phi|\beta_i\Lambda_L(|\psi_i\rangle\langle\psi_i|)^{\otimes L}|\psi_\phi\rangle\\&=\sum_i\langle\psi_\phi|\beta_i\Bigg[\overline{\eta}_{se}^{opt}(L)|\psi_i\rangle\langle\psi_i|\\&\quad+\frac{1}{2}[1-\overline{\eta}_{se}^{opt}(L)]\mathbb{1}\Bigg]|\psi_\phi\rangle\end{aligned} \tag{17}$$

where the optimal shrinking factor for state estimation is given by $\overline{\eta}_{se}^{opt}(L)=[2\overline{F}_{se}^{opt}(L)-1]=L/(L+2)$ [8]. Taking the limit of Eq. (17) for $L\rightarrow\infty$ we have

$$\overline{F}_{pe}(N)\overset{L\rightarrow\infty}{\rightarrow}\sum_i\langle\psi_\phi|\beta_i|\psi_i\rangle\langle\psi_i|\psi_\phi\rangle=\frac{1}{2}[\eta_{xy}(N,\infty)+1]. \tag{18}$$

The concatenation of a phase-covariant cloner with a state estimation cannot perform better than the optimal phase estimation, thus we can write

$$\eta_{xy}^{opt}(N,\infty)\leqslant\overline{\eta}_{pe}^{opt}(N). \tag{19}$$

The inequalities (16) and (19) prove the equality (12).

### C. Bound for optimal phase-covariant cloning

We now prove an upper bound for the fidelity of an $N\rightarrow M$ phase-covariant cloning transformation acting on equatorial qubits. We consider a phase-covariant cloner $T_{N\infty}$ that results from concatenating the two phase-covariant cloners $T_{NM}$ and $T_{M\infty}$. In this way we cannot obtain an $N\rightarrow\infty$ cloner that works better than the optimal one. Thus, by using the concatenation property of phase-covariant cloners proven above we can write

$$\eta_{xy}(N,M)\,\eta_{xy}(M,\infty)\leqslant\eta_{xy}^{opt}(N,\infty). \tag{20}$$

In the sequence of the two cloners we take the $M\rightarrow\infty$ as the optimal one in order to find the tightest upper bound for the equatorial shrinking factor of a phase covariant $N\rightarrow M$ cloning transformation. We rewrite Eq. (20) as follows:

$$\eta_{xy}^{opt}(N,M)\leqslant\frac{\eta_{xy}^{opt}(N,\infty)}{\eta_{xy}^{opt}(M,\infty)}. \tag{21}$$

By exploiting the connection to phase estimation in Eq. (12), proven above, this bound takes the form

$$\begin{aligned}\eta_{xy}^{opt}(N,M)\leqslant\tilde{\eta}_{pcc}(N,M)&=\frac{\overline{\eta}_{pe}^{opt}(N)}{\overline{\eta}_{pe}^{opt}(M)}\\&=2^{(M-N)}\frac{\sum_{l=0}^{N-1}\sqrt{\binom{N}{l}\binom{N}{l+1}}}{\sum_{j=0}^{M-1}\sqrt{\binom{M}{j}\binom{M}{j+1}}}.\end{aligned} \tag{22}$$

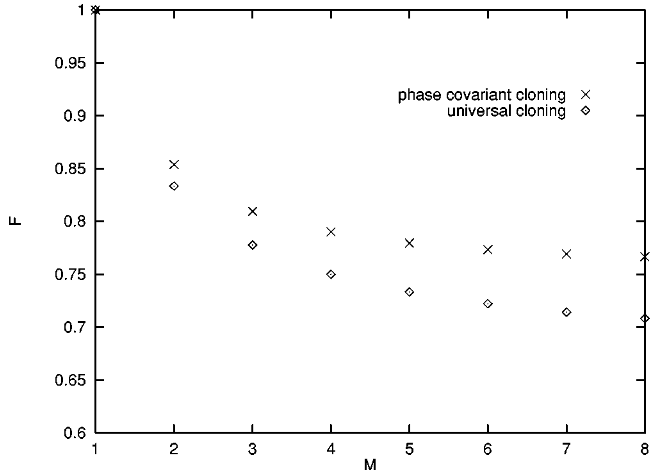

FIG. 1. Upper bound for the fidelity in phase-covariant cloning compared with the optimal fidelity for universal cloning of qubits. Both sets of points are shown for a fixed number of inputs, $N=1$, as a function of $M$, the number of outputs. For the limit $M\rightarrow\infty$ one finds from the formulas given in the text that $\tilde{F}_{pcc}(1,\infty)=3/4$ and $F^{opt}_{univ}(1,\infty)=2/3$.

In Fig. 1 we show the upper bound for the fidelity of phase-covariant cloning and the optimal fidelity for a universal cloner. The two quantities are shown as a function of $M$ for fixed $N=1$. By varying N it is possible to see that

$$\tilde{\eta}_{pcc}(N,M)>\eta^{opt}_{univ}(N,M)\ \ \forall N<M, \tag{23}$$

as expected. Note that while in the case of universal cloning the explicit form of the CP map which achieves the bound is known [2], in the case of phase-covariant cloners acting on equatorial qubits we do not know whether the bound (22) can be achieved for general values of $N$ and $M$. In the next section we present the cloning transformation which achieves the bound in the particular case $N=1,\ M=2$.

## IV. OPTIMAL 1→2 CLONING OF EQUATORIAL QUBITS

In this section we present constructive proof for the best $1\rightarrow 2$ cloning transformation acting on equatorial qubits. For convenience we choose the equator in the $x$-$z$ plane instead of the $x$-$y$ equator. (Note that optimality of the fidelity must be independent from the choice of a particular basis.) Hence we consider equatorial states with real coefficients of the form

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle\ \ \text{with}\alpha,\beta\ \ \text{real},\ \ \alpha^2+\beta^2=1. \tag{24}$$

Our notation and method is inspired by Ref. [9]. We proceed as follows: first we derive the optimal cloner that takes only the four BB84 states as input. Here we use the acronym BB84 for the quantum cryptographic protocol described in Ref. [10]. Remember that the four BB84 states are given by

$$\begin{aligned}&|0\rangle,\quad |1\rangle,\quad |\overline{0}\rangle=\sqrt{\tfrac{1}{2}}(|0\rangle+|1\rangle),\\ &|\overline{1}\rangle=\sqrt{\tfrac{1}{2}}(|0\rangle-|1\rangle).\end{aligned} \tag{25}$$

Then we will show that this transformation leads to the same fidelity for *any* input from the equator. Therefore we have also found the best transformation that takes all states from the equator as input. (If we could find a better one on the whole equator it would have to be better than the optimal one for the BB84 states.)

We start from a general symmetric ansatz for the unitary transformation on the input qubit, blank qubit, and ancilla, written in this order:

$$\begin{aligned}U|0\rangle|0\rangle|X\rangle&=a|00\rangle|A\rangle+b(|01\rangle+|10\rangle)|B\rangle+c|11\rangle|C\rangle,\\ U|1\rangle|0\rangle|X\rangle&=\tilde{a}|11\rangle|\tilde{A}\rangle+\tilde{b}(|10\rangle+|01\rangle)|\tilde{B}\rangle+\tilde{c}|00\rangle|\tilde{C}\rangle.\end{aligned} \tag{26}$$

For convenience we include all phases in Eq. (26) into the ancilla states, so that the coefficients $a,b,c,\tilde{a},\tilde{b}$, and $\tilde{c}$ are real and positive. Furthermore, the transformation should not change under renaming the basis, i.e., exchange of $|0\rangle$ and $|1\rangle$—therefore we have $a=\tilde{a},\ b=\tilde{b}$, and $c=\tilde{c}$.

The normalization and unitarity conditions for Eq. (26) read

$$\begin{aligned}&a^2+2b^2+c^2=1,\\ &ac\langle\tilde{C}|A\rangle+2b^2\langle\tilde{B}|B\rangle+ac\langle\tilde{A}|C\rangle=0.\end{aligned} \tag{27}$$

Now we have to determine the free parameters in this transformation (coefficients and scalar products of ancillas) such that the fidelity $F=\langle\psi|\rho^{out}|\psi\rangle$, where $|\psi\rangle$ is one of the four BB84 states, is constant and optimal. Here $\rho^{out}$ is the reduced density matrix of the first or second bit at the output of the cloner.

It is straightforward to calculate the fidelities corresponding to the reduced output density matrices for the four BB84 states. From their equality we find the following constraints:

$$F=a^2+b^2, \tag{28}$$

$$\begin{aligned}F=\tfrac{1}{2}(1+ab\,\mathrm{Re}[\langle\tilde{A}|B\rangle+\langle\tilde{B}|A\rangle]\\ +bc\,\mathrm{Re}[\langle\tilde{B}|C\rangle+\langle\tilde{C}|B\rangle]),\end{aligned} \tag{29}$$

$$0=ab\,\mathrm{Re}[\langle\tilde{A}|\tilde{B}\rangle+\langle B|A\rangle]+bc\,\mathrm{Re}[\langle\tilde{B}|\tilde{C}\rangle+\langle C|B\rangle]. \tag{30}$$

As the scalar products of ancillas are independent parameters the real part of which varies between -1 and +1, we can maximize the fidelity in Eq. (29) to

$$F=\tfrac{1}{2}[1+2b(a+c)] \tag{31}$$

by an appropriate choice of ancillas. Similarly, we can always fulfill Eq. (30) by the right choice of ancillas. So, our task reduces to finding the maximum of the function

$$F=\tfrac{1}{2}(1+a^2-c^2), \tag{32}$$

with the constraint

$$F=\tfrac{1}{2}+\sqrt{\tfrac{1}{2}(1-a^2-c^2)}(a+c). \tag{33}$$

This can be done analytically with the help of Lagrange multipliers. The solution for the optimum is

$$a=\tfrac{1}{2}+\sqrt{\tfrac{1}{8}},\qquad b=\sqrt{\tfrac{1}{8}},\qquad c=\tfrac{1}{2}-\sqrt{\tfrac{1}{8}}. \tag{34}$$

This solution corresponds to an optimal fidelity of

$$F^{opt}(1,2)=\tfrac{1}{2}+\sqrt{\tfrac{1}{8}}=0.854, \tag{35}$$

which reaches the bound $\tilde{F}_{pcc}(1,2)=\frac{1}{2}[\tilde{\eta}_{pcc}(1,2)+1]$, given by Eq. (22).

The optimal cloning transformation for the BB84 states can be written explicitly as follows (we see that a two-dimensional ancilla is sufficient):

$$\begin{aligned}U|0\rangle|0\rangle|X\rangle&=(\tfrac{1}{2}+\sqrt{\tfrac{1}{8}})|00\rangle|0\rangle+\sqrt{\tfrac{1}{8}}(|01\rangle+|10\rangle)|1\rangle\\&\quad+(\tfrac{1}{2}-\sqrt{\tfrac{1}{8}})|11\rangle|0\rangle,\\U|1\rangle|0\rangle|X\rangle&=(\tfrac{1}{2}+\sqrt{\tfrac{1}{8}})|11\rangle|1\rangle+\sqrt{\tfrac{1}{8}}(|10\rangle+|01\rangle)|0\rangle\\&\quad+(\tfrac{1}{2}-\sqrt{\tfrac{1}{8}})|00\rangle|1\rangle.\end{aligned} \tag{36}$$

We still have to show that this transformation leads to the same fidelity for *any* pure input state taken from the equator. In fact, any unitary transformation of the kind

$$\begin{aligned}U|0\rangle|0\rangle|X\rangle&=a|00\rangle|0\rangle+b(|01\rangle+|10\rangle)|1\rangle+c|11\rangle|0\rangle,\\U|1\rangle|0\rangle|X\rangle&=a|11\rangle|1\rangle+b(|10\rangle+|01\rangle)|0\rangle+c|00\rangle|1\rangle,\end{aligned} \tag{37}$$

that leads to the same fidelity for the BB84 states has this property. This can be seen by calculating the fidelity when applying the transformation (37) to the state given in Eq. (24). We find

$$F(\alpha)=(\alpha^4+\beta^4)a^2+b^2+\alpha^2\beta^2 2c^2+4\alpha^2\beta^2 b(a+c), \tag{38}$$

which at first glance does not look like a constant, but can be shown easily to be independent of $\alpha$ by inserting Eq. (31) and the constraints from unitarity, given in Eq. (27). Thus we have shown that apart from the four BB84 states our cloner [Eq. (36)] is optimal for *any* state from the equator.

It is worth pointing out that there is a link between optimal cloning of equatorial qubits and optimal eavesdropping in the BB84 scheme, see Ref. [11]: the intersection of the curve for the mutual information between Alice and Bob and the curve for the optimal mutual information between Alice and Eve occurs at a disturbance $D=1-F$ which corresponds to our optimal equatorial cloning fidelity. If Eve performs a symmetric attack where she gets as much information as Bob, she cannot find a better strategy than applying the best cloner. We could have actually proved an upper bound for our cloner from a contradiction: let us assume the cloner could have a higher fidelity than the one indicated by the intersection of the information curves. Then Eve could use it to eavesdrop and would have found a better spying device than the optimal one. Therefore, the best cloner cannot have a higher fidelity than the best symmetric eavesdropping attack. In this section we have shown a constructive proof for the corresponding optimal cloning transformation.

## V. CONCLUSIONS

In this paper we have pointed out a connection between optimal cloning of equatorial qubits and phase estimation. We exploited this connection to establish an upper bound for the fidelity of a phase covariant $N\rightarrow M$ cloning transformation acting on equatorial qubits. Our results for this restricted set of inputs are qualitatively similar to the ones for universal cloning, in the sense that in both cases the concatenation property holds. Quantitatively our upper bound is higher than the one for universal cloning, as expected. The bound for phase-covariant cloning was shown to be reached for $N=1,M=2$ by constructing the optimal cloning transformation explicitly. In this particular case we also found a link between phase-covariant cloning and optimal eavesdropping strategies in the quantum cryptographic scheme BB84. Finding the explicit optimal phase-covariant cloning transformation for general $N$ and $M$ remains to be achieved.

## ACKNOWLEDGMENTS

This work was supported in part by Deutsche Forschungsgemeinschaft under Grant SFB 407, by Ministero dell'Università e della Ricerca Scientifica e Tecnologica under the project ''Amplificazione e rivelazione di radiazione quantistica,'' and by the ESF-QIT program.

## APPENDIX: MAP OF THE PHASE COVARIANT CLONER

We use the Kraus decomposition [5] of a CP map [the map $RT_{N,M}$ in Eq. (2) is CP since it is the partial trace of the CP map $T_{N,M}$]

$$R[T_{N,M}(|\psi\rangle\langle\psi|^{\otimes N})]=\sum_k A_k|\psi\rangle\langle\psi|A_k^\dagger, \tag{A1}$$

where $A_k$ are operators on $\mathcal{H}$ depending on $N$ and $M$, satisfying the condition

$$\sum_k A_k^\dagger A_k=\mathbb{1}. \tag{A2}$$

By introducing the following basis for the $\mathbb{C}$ algebra of the operators on $\mathcal{H}$

$$\sigma_0=\frac{1}{2}(\sigma_x+i\sigma_y),\quad \sigma_1=\frac{1}{2}(\sigma_x-i\sigma_y), \tag{A3}$$

$$\sigma_2=\frac{1}{2}(1+\sigma_z),\quad \sigma_3=\frac{1}{2}(1-\sigma_z), \tag{A4}$$

we can write in general

$$A_k=\sum_{\alpha=0}^{3} c_k^{\alpha}\sigma_{\alpha}, \tag{A5}$$

with $c_k^{\alpha}\in\mathbb{C}$. It follows that

$$\begin{aligned}R[T_{N,M}(|\psi\rangle\langle\psi|^{\otimes N})]&=\sum_k\sum_{\alpha,\beta=0}^{3} c_k^{\alpha}c_k^{\beta *}\sigma_{\alpha}|\psi\rangle\langle\psi|\sigma_{\beta}^{\dagger}\\&=\sum_{\alpha,\beta=0}^{3}\Gamma^{\alpha\beta}\Sigma_{\alpha\beta}(|\psi\rangle\langle\psi|),\end{aligned} \tag{A6}$$

with $\Sigma_{\alpha\beta}(|\psi\rangle\langle\psi|)\equiv\sigma_{\alpha}|\psi\rangle\langle\psi|\sigma_{\beta}^{\dagger}$ and $\Gamma^{\alpha\beta}\equiv\Sigma_k c_k^{\alpha}c_k^{\beta *}$.

Imposing the phase-covariance condition (3) to the above CP map and using Eq. (A6) we find

$$\sum_{\alpha,\beta}\Gamma^{\alpha\beta}\Sigma_{\alpha\beta}(U_{\chi}|\psi\rangle\langle\psi|U_{\chi}^{*})=\sum_{\alpha,\beta}\Gamma^{\alpha\beta}U_{\chi}\Sigma_{\alpha\beta}(|\psi\rangle\langle\psi|)U_{\chi}^{*}. \tag{A7}$$

Writing down explicitly each term of Eq. (A7) and imposing that the equality holds $\forall\chi\in[0,2\pi)$ we obtain the following constraints on the coefficients $\Gamma^{\alpha\beta}$:

$$\begin{aligned}&\Gamma^{01}=\Gamma^{02}=\Gamma^{03}=0,\\&\Gamma^{10}=\Gamma^{12}=\Gamma^{13}=0,\\&\Gamma^{20}=\Gamma^{21}=0,\\&\Gamma^{30}=\Gamma^{31}=0.\end{aligned} \tag{A8}$$

In order to obtain Eq. (A8) we have written a general density matrix in $\mathcal{H}$ as

$$\varrho=\begin{pmatrix}\delta & \gamma\\ \gamma^{*} & 1-\delta\end{pmatrix} \tag{A9}$$

with $\delta\in[0,1]$ and $\gamma\in\mathbb{C}$. Condition (A2) takes the form

$$\sum_{\alpha,\beta=0}^{3}\Gamma^{\beta\alpha}\sigma_{\alpha}^{\dagger}\sigma_{\beta}=\mathbb{1}, \tag{A10}$$

which gives

$$\Gamma^{11}=1-\Gamma^{22},\quad \Gamma^{00}=1-\Gamma^{33}. \tag{A11}$$

Note that $\Gamma^{\alpha\alpha}=\Sigma_k|c_k^{\alpha}|^2\geqslant 0\ \ \forall\alpha$ and $\Gamma^{\alpha\beta}=(\Gamma^{\beta\alpha})^{*}$. Using Eq. (A11) we have $0\leqslant\Gamma^{\alpha\alpha}\leqslant 1$ and $|c_k^{\alpha}|\leqslant 1\forall\alpha$, from which we obtain

$$|\Gamma^{32}|^2=\left|\sum_k c_k^3 c_k^{2*}\right|^2\leqslant\sum_k|c_k^3 c_k^{2*}|^2\leqslant\Gamma^{22}\Gamma^{33}\leqslant 1. \tag{A12}$$

Using conditions (A8) and (A11) we can now write Eq. (A6) in matrix form as follows:

$$R[T_{N,M}(|\psi\rangle\langle\psi|^{\otimes N})]=\begin{pmatrix}(1-\Gamma^{33})(1-\delta)+\Gamma^{22}\delta & \gamma\Gamma^{32}\\ \gamma^{*}(\Gamma^{32})^{*} & (1-\Gamma^{22})\delta+\Gamma^{33}(1-\delta)\end{pmatrix}. \tag{A13}$$

Let us now use the notation $\eta_{xy}\equiv|\Gamma^{32}|$, $\varphi\equiv\arg(\Gamma^{32})$ and $\eta_z=(\Gamma^{33}+\Gamma^{22}-1)$. Note that $0\leqslant\eta_{xy}\leqslant 1$, $-1\leqslant\eta_z\leqslant 1$, and $\eta_{xy,z}=\eta_{xy,z}(N,M)$: the dependence on $N$ and $M$ is included in the coefficients $c_k^{\alpha}$.

Comparing the Bloch vector of an input generic qubit $\vec{s}^{in}=[2|\gamma|\cos\phi,-2|\gamma|\sin\phi,2\delta-1)$ where $\phi=\arg(\gamma)$ with the Bloch vector of the one-particle reduced density matrix of the output $\vec{s}^{out}=(2\eta_{pcc}|\gamma|\cos(\phi+\varphi),-2\eta_{pcc}|\gamma|\sin(\phi+\varphi),s_z^{in}\eta_z+(\Gamma^{22}-\Gamma^{33})]$, we notice that for

$$\varphi=0\quad\text{and}\quad\Gamma^{22}=\Gamma^{33} \tag{A14}$$

the map $T_{N,M}$ is completely determined by the factors $\eta_{xy}(N,M)$ and $\eta_z(N,M)$: $\eta_{xy}(N,M)$ describes the shrinking of the Bloch vector in the $x$-$y$ plane, while $\eta_z$ gives the shrinking along the $z$ axis. For initial equatorial qubits ($\delta=1/2$, $\gamma=e^{i\phi}/2$) we find with the conditions (A14):

$$R[T(|\psi_{\phi}\rangle\langle\psi_{\phi}|^{\otimes N})]=\frac{1}{2}\begin{pmatrix}1 & \eta_{xy}(N,M)e^{i\phi}\\ \eta_{xy}(N,M)e^{-i\phi} & 1\end{pmatrix} \tag{A15}$$

$$=\eta_{xy}(N,M)|\psi_{\phi}\rangle\langle\psi_{\phi}|+\frac{1}{2}[1-\eta_{xy}(N,M)]\mathbb{1}, \tag{A16}$$

i.e., the action of of the phase-covariant cloner $T_{N,M}$ on equatorial qubits is completely determined by the shrinking factor $\eta_{xy}(N,M)$ in the $x$-$y$ plane.

Let us now show that without loss of generality we can impose the conditions (A14) to describe the map of an optimal phase-covariant cloner for equatorial qubits. For $\varphi\neq 0$ the fidelity for equatorial qubits is given by

$$\begin{aligned}F_{pcc}(N,M)&=|\langle\psi_{\phi}|R[T_{N,M}(|\psi_{\phi}\rangle\langle\psi_{\phi}|^{\otimes N})]|\psi_{\phi}\rangle|^2\\&=\frac{1}{2}[1+\eta_{xy}(N,M)\cos\varphi].\end{aligned} \tag{A17}$$

By definition the optimal cloner $T_{N,M}$ is the one which maximizes $F_{pcc}(N,M)$. From Eq. (A17) we see that maximizing $F_{pcc}(N,M)$ is equivalent to setting $\varphi=0$ and maximizing

$\eta_{xy}(N,M)$, which is independent of $\varphi$.

Let us now analyze the condition $\Gamma^{22}=\Gamma^{33}$. Let us suppose that we can find an optimal phase-covariant cloner $T_{N,M}$ with $\eta_{xy}^{opt}(N,M)$ and $\Gamma^{22}\neq\Gamma^{33}$. From the explicit form of $\sigma_2$ and $\sigma_3$, given in Eq. (A4), one can see that renaming the basis (i.e., exchanging $|0\rangle\leftrightarrow|1\rangle$) is equivalent to exchanging $\sigma_2\leftrightarrow\sigma_3$ and $\sigma_0\leftrightarrow\sigma_1$, while leaving the basis vectors unchanged. The exchange $2\leftrightarrow3$ leaves $\eta_{xy}(N,M)$ and $\eta_z(N,M)$ invariant. Now consider a cloner $\hat{T}_{N,M}$ such that its single-particle reduced density operator is the matrix $R[T_{N,M}(|\psi_\phi\rangle\langle\psi_\phi|^{\otimes N})]$ written in the form (A6) with the exchange $2\leftrightarrow3$. The map $\hat{T}_{N,M}$ must also be optimal: in fact, optimality of $T_{N,M}$ cannot depend on the particular choice of the basis, and the fidelity (A17) is invariant under the exchange $2\leftrightarrow3$. Now consider the cloner described by the map $T_s=\frac{1}{2}(T_{N,M}+\hat{T}_{N,M})$. This cloner has the same shrinking factor $\eta_{xy}^{opt}(N,M)$ for equatorial qubits. Therefore we can always construct an optimal cloner with $\Gamma^{22}=\Gamma^{33}$.

[1] W.K. Wootters and W.H. Zurek, Nature (London) **299**, 802 (1982); H.P. Yuen, Phys. Lett. **A113**, 405 (1986).

[2] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).

[3] D. Bruß, A. Ekert, and C. Macchiavello, Phys. Rev. Lett. **81**, 2598 (1998).

[4] R. Werner, Phys. Rev. A **58**, 1827 (1998).

[5] K. Kraus, Ann. Phys. (N.Y.) **64**, 311 (1971).

[6] A.S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North Holland, Amsterdam, 1982).

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

[8] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).

[9] D. Bruß, D. DiVincenzo, A. Ekert, C. Fuchs, C. Macchiavello, and J. Smolin, Phys. Rev. A **57**, 2368 (1998).

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

[11] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).