Experimental demonstration of an efficient quantum phase-covariant cloning and its possible applications to simulating eavesdropping in quantum cryptography

Jiangfeng Du,1,2,3,4 Thomas Durt,4 Ping Zou,1 L.C. Kwek,5 C.H. Lai,2 C.H. Oh,2 and Artur Ekert3,2

1Structural Research Laboratory and Department of Modern Physics, University of Science and Technology of China, Hefei, 230027, P.R. China
2Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542
3Centre for Quantum Computation, DAMTP, University of Cambridge, Wilberforce Road, Cambridge CB3 0WA U.K.
4TONA-TENA Free University of Brussels, Pleinlaan 2, B-1050 Brussels, Belgium.
5Department of Natural Sciences, National Institute of Education, Nanyang Technological University, 1 Nanyang Walk, Singapore 637616

We describe a nuclear magnetic resonance (NMR) experiment which implements an efficient one-to-two qubit phase-covariant cloning machine (QPCCM). In the experiment we have achieved remarkably high fidelities of cloning, 0.848 and 0.844 respectively for the original and the blank qubit. This experimental value is close to the optimal theoretical value of 0.854. We have also demonstrated how to use our phase-covariant cloning machine for quantum simulations of bit by bit eavesdropping in the four-state quantum key distribution protocol.

PACS numbers:

The “no-cloning” result1, 2 asserts that due to the linearity of quantum mechanics unknown quantum states cannot be copied perfectly. This notwithstanding one can design approximate quantum cloning machines and address their optimality. The most notable example is the universal quantum cloner (UQC) proposed by Bužek and Hillery 3. It has been studied in great details 4, 5, 6 and a number of experimental implementations of a 1 → 2 qubit UQC have been proposed 7, 8, 9, 10, 11. Another important example is the optimal quantum phase-covariant cloning machine (QPCCM) 3, 10, 11. Unlike the UQC, it clones only subsets of states for which we have some a priori information. In the special case of the QPCCM operating on qubits it has been shown that a class of states |ψ⟩ = 1/√2 (|0⟩ + e^{i\phi} |1⟩), called equatorial states, can be cloned up to the fidelity 0.854. As expected this value is slightly higher than the optimal fidelity of the UQC (0.833). This is because even partial information about the original state allows to optimize the cloning process and to obtain higher fidelities of the clones. The phase-covariant cloners, which are the subject of this paper, are of significant importance in quantum cryptography as they provide the optimal eavesdropping technique for a large class of attacks on the four state protocol (BB84) 12. The properties of the QPCCM have been extensively studied from the theoretical perspective 12, 13, however, on the experimental side, apart from an interesting recent optical proposal by Fiurasek 14, no actual realization of the QPCCM has been reported.

Here we describe the first experimental implementation of the QPCCM. We use the NMR technology to implement a modified two qubit network originally designed by Niu and Griffiths 10 (see Fig. 1). The simplicity of the network allows to reduce the effects of decoherence and to obtain remarkably high fidelities of the clones.

FIG. 1: Quantum network of the efficient phase-covariant cloning. It consists of two controlled-NOT gates together with one controlled-rotation gate, where R(θ) = e^{-iθσ_y/2} is a rotation by an angle θ about the y axis in Bloch-sphere. The upper and the lower horizontal lines correspond to the original and the blank qubits respectively.

This is in contrast with earlier approaches which were based on more complicated three qubit networks 15. The complexity of related three qubits experiments is of any guidance here, e.g. the NMR implementation of the UQC 8, then substantial losses due to inhomogeneities of the magnetic field and decoherence cannot be avoided with the current state of the art technology. This, together with the stringent precision requirements, lowers the fidelity (to about inconclusive 58% in 15). A three qubit network for for the 1 → 2 QPCCM, for example the one proposed by Fuchs et al. 8, would face similar problems.

Our version of the network is shown in Fig. 1. The net unitary operator has the form

\[ U(\theta) = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & \cos \theta & \sin \theta & 0 \\
0 & -\sin \theta & \cos \theta & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}. \]

When \( \theta = \frac{\pi}{4} \), this unitary transform defined as \( U^{\text{opt}} \) corresponds to an efficient optimal QPCCM. In fact, \( U^{\text{opt}} \) is just a 2-qubit square root of SWAP gate. Consider now an equatorial state of a qubit, i.e., a state with a definite spin in the direction \( n = (\cos \varphi, \sin \varphi, 0) \). This
state has the form \( |n\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{i\varphi} |1\rangle) \), whereas the \( b \) qubit is in the state \( |0\rangle \). \( U^{opt} \) transforms the input state to \( \rho_{ab}^{\text{out}} = U^{opt} |n\rangle \langle n| U^{opt\dagger} \). The reduced density matrix of two copies can be calculated (by tracing out another qubit) as

\[
\rho_{a}^{\text{out}} = \rho_{b}^{\text{out}} = \begin{pmatrix}
3/4 & \sqrt{2} e^{-i\varphi}/4 \\
\sqrt{2} e^{i\varphi}/4 & 1/4
\end{pmatrix}.
\]

Note that the two copies are in fact symmetric. We describe the free procession of spin \( a \) \((^{13}C)\) and \( b \) \((^{1}H)\) around the static magnetic field with frequencies 100MHz and 400 MHz. \( I_{a}^z (I_{b}^z) \) is the angular moment operator of \( a \) \((b)\) in direction \( \hat{z} \), and the third term is the \( J \) coupling of the two spins with \( J = 214.5\) Hz. \(^{13}C\) nucleus’s \( T_1 \) relaxation time is 17.2s and it’s \( T_2 \) relaxation time is 0.35s. \(^{1}H\) nucleus’s \( T_1 \) relaxation time is 4.8s and it’s \( T_2 \) relaxation time is 3.3s. In the following, we describe how we experimentally realize the optimal \( 1 \rightarrow 2 \) QPCCM shown in Fig. 1.

(E1) Prepare the initial state: Initially the two qubits are in thermal equilibrium with the environment and their state is described by the density operator \( \rho_{th} \propto \sigma_{a}^{z} + 4\sigma_{b}^{z} \). We use the spatial averaging technique [19] to create the effective pure state \(| \uparrow \rangle_{a} \otimes | \uparrow \rangle_{b} \), or, in the density operator form, \( \frac{1}{2}(1 + \sigma_{a}^{x}) \otimes \frac{1}{2}(1 + \sigma_{b}^{x}) \). The sequence of operations leading to this state is shown in Fig. 2(a). We then perform a single hard \( \frac{\pi}{2} \) radio frequency (\( rf \)) pulse on \( a \) qubit to generate one of the desired equatorial state \( |n(\varphi)\rangle_{ab}^{in} = (\cos \varphi, \sin \varphi, 0) \) with \( \varphi = \cos(n\pi/12), n = \{0, 1, \ldots, 23\} \).

(E2) Clone the input equatorial state: The quantum circuit of optimal \( 1 \rightarrow 2 \) QPCCM is described in Fig. 1 by fixing \( \theta = \frac{\pi}{4} \). This corresponds to a 2-qubit square root of SWAP gate. NMR pulse sequences are developed by replacing this operation with an idealized sequence of NMR pulses and delays. The resulting sequences are then simplified by combining \( rf \) pulses appropriately. Figure 2(b) shows the final pulse sequence to demonstrate the optimal \( 1 \rightarrow 2 \) QPCCM. All the \( rf \) pulses are hard pulses which hardly affect the state of \( b \) qubit due to the heteronuclear sample we used.

(E3) Measure and analyze: In principle, the quality of the copies, defined as fidelity, can be calculated by \( F = \langle n | \rho_{a(b)}^{\text{out}} | n \rangle \), where \( \rho_{a(b)}^{\text{out}} \) is the reduced density matrix of a single qubit and can be obtained from the density matrix \( \rho_{ab}^{out} \). In NMR, one can use state tomography technique to get \( \rho_{ab}^{out} \) by applying a set of readout pulses, but this has the disadvantage of requiring separate experiments. In our experiment, we use a simpler method described in Ref.[3]: we measure the two spectra of two output qubits individually, here the receiver phase are set with the same phase as that of the input qubit measurement. Therefore, the tracing out process can be implemented by integrating the entire multiplet in each spectrum, comparing to the integration of the input state spectrum, we can get the relative length of the output state vector \( r'_{a(b)} \) in the same orientation as its input state vector, so the fidelity between the input and output state can be calculated as \( F_{a(b)} = \frac{1}{2}(1 + r'_{a(b)}) \). Figure 3 shows the experimental results from cloning the input equatorial state \( |n(0)\rangle_{ab}^{in} = (1, 0, 0) \). There are three spectra, corresponding to the observable NMR signals of one input state and its two copies, that are measured by setting the same receiver phase experimentally. The spectra do have similar expected form (in-phase absorption signals at the outmost positions of each multiplet).

An important feature of QPCCM is that all equatorial states are cloned equally well and so it is necessary to study the behavior of pulse sequence when applied to a wide range of states on equator. We have prepared a total of 24 input equatorial states \( |n(\varphi)\rangle_{ab}^{in} = (\cos \varphi, \sin \varphi, 0) \) by changing the value \( \varphi \) with a spacing of \( 15^{\circ} \) as shown in (E1). For each input state, we measure its spectrum and denote it as a reference to calculate the quality of the two copies after the cloning transformation described in (E2). Finally we measure each copy and calculate the fidelity. Experimentally, we get the mean fidelity of this phase-covariant cloning as \( F_{c} = 0.848 \pm 0.015 \) for a qubit.
and $F_b = 0.844 \pm 0.015$ for $b$ qubit, which are both close to the optimal theoretical value 0.854.

Compared to the low fidelity of the NMR experiment for UQCM [2], our near-optimal fidelity arises from the following reasons: (1) Less decoherence effect – the time used for cloning in our experiment is about 5.3 ms, which is well within the decoherence time (about 350 ms for $^{13}$C nucleus and 3.3 s for $^1$H nucleus); while the time used for UQCM in Ref. [2] was estimated about 400 ms, which is close to the decoherence time with the value 720 ms for two $^1$H nuclei; (2) Simplicity – it is simpler to realize our economic 2-qubit QPCCM than to realize the 3-qubit UQCM in Ref. [2]; (3) Pulses – in our experiment all the $rf$ pulses are hard pulses, which are more perfect than selective pulses, which is simply achieved by using heteronuclear sample. In our experiments, small errors arise as a result of the inhomogeneity of the static with $rf$ magnetic fields as well as the variability of the magnetic fields as well as the variability of the static

One important application of our efficient QPCCM is the quantum simulator of a bit by eavesdropping on the fidelities of the two copies, $F_0 = 0.842$ and $F_1 = 0.839$.

FIG. 3: Experimental spectra of cloning the input state $\ket{n(0)}_a = (1, 0, 0)$. The left and middle spectra are the carbon spectra corresponding to the input and output state of a qubit, where the vertical scales are the same arbitrary units. The right spectrum is for the hydrogen nucleus representing the output of $b$ qubit, where the vertical scale does not share the same arbitrary units with those of the carbon spectra. From the integration of the each multiplet, we obtain the fidelities of the two copies, $F_0 = 0.842$ and $F_1 = 0.839$.

and $F_b = 0.844 \pm 0.015$ for $b$ qubit, which are both close to the optimal theoretical value 0.854.

Compared to the low fidelity of the NMR experiment for UQCM [2], our near-optimal fidelity arises from the following reasons: (1) Less decoherence effect – the time used for cloning in our experiment is about 5.3 ms, which is well within the decoherence time (about 350 ms for $^{13}$C nucleus and 3.3 s for $^1$H nucleus); while the time used for UQCM in Ref. [2] was estimated about 400 ms, which is close to the decoherence time with the value 720 ms for two $^1$H nuclei; (2) Simplicity – it is simpler to realize our economic 2-qubit QPCCM than to realize the 3-qubit UQCM in Ref. [2]; (3) Pulses – in our experiment all the $rf$ pulses are hard pulses, which are more perfect than selective pulses, which is simply achieved by using heteronuclear sample. In our experiments, small errors arise as a result of the inhomogeneity of the static with $rf$ magnetic fields as well as the variability of the magnetic fields as well as the variability of the static

One important application of our efficient QPCCM is the quantum simulator of a bit by eavesdropping on the fidelities of the two copies, $F_0 = 0.842$ and $F_1 = 0.839$.

FIG. 4: The normalized observable NMR signals (σ) versus the rotation angle $\theta$ of the phase-covariant cloning machine, for two bases, $X$-base (at Left) and $Y$-base (at right). The lines correspond to theoretical calculation. The filled and empty boxes (circles) correspond to the experimental measurement from a qubit ($b$ qubit), while the filled (empty) circles and boxes correspond to the input state is $\ket{+}$ ($\ket{-}$).

A main concern of the eavesdropping is to determine how much information an eavesdropper can obtain from a given level of noise. For the above optimal eavesdropping attack, regardless of the input BB84 state, Bob guesses correctly the state sent by Alice with probability $F_{Bob} = \frac{1}{2} + \langle \sigma_{x\theta}^{Bob} \rangle$ and makes an error $D_{Bob} = 1 - F_{Bob} = \frac{1}{2} - \langle \sigma_{x\theta}^{Bob} \rangle$, where $i \in \{x, y\}$ is one of the maximally conjugate bases; while Eve guesses correctly the state sent by Alice with probability $F_{Eve} = \frac{1}{2} + \langle \sigma_{x\theta}^{Eve} \rangle$ and makes an error $D_{Eve} = \frac{1}{2} - \langle \sigma_{x\theta}^{Eve} \rangle$. As we know, the mutual information is defined as $I = \frac{1}{2} + D_{Bob} + (1 - D_{Bob})_{Bob}$. From our experimental dates shown in Fig. 4, we extract the Alice-Bob and Alice-Eve mutual information as a function of the
value of noise (QBER) defined as $QBER = \frac{1 - \cos \theta}{2}$. Here $\theta \in [0, \pi/2]$ characterize the strength of Eve’s attack. The experimental results are shown in Fig. 5. We show the relation between the mutual information and QBER, in agreement with the theoretical results.

In summary, we provide the first experimental demonstration of an efficient and nearly optimal $1 \rightarrow 2$ QPCCM by using a 2-qubit NMR quantum computer. Our approach cannot be extended to the UQC as it is known that a 3-qubit $1 \rightarrow 2$ UQC cannot be reduced to an efficient 2-qubit network. However, our efficient QPCCM has potential applications as a simulator of eavesdropping techniques in quantum key distributions.

This project was supported by the National Nature Science Foundation of China (Grants. No. 10075041 and No. 10075044) and Funded by the National Fundamental Research Program (2001CB309300). We also thank supports from the ASTAR Grant No. 012-104-0040 and Temasek Project in Quantum Information Technology (Grant No. R-144-000-071-305). T.D. thanks supports from the Flemish Fund for Scientific Research, the Inter-University Attraction Pole Program of the Belgian government under grant V-18, the Concerted Research Action Photonics in Computing, and the research council (OZR) of the VUB.

* Electronic address: djf@ustc.edu.cn

[1] W.K. Wootters and W.H. Zurek, Nature (London) 299, 802.
[2] G.C. Ghirardi and T. Weber, Nuovo Cimento Soc. Ital. Fis. B 78, 9 (1983). The impossibility of Exact cloning was first mentioned in a report by G.C. Ghirardi (1981) in response to a paper submitted to Found. Phys.
[3] V. Bužek and M. Hillery, Phys. Rev. A 54, 1844 (1996).
[4] N. Gisin and S. Massar, Phys. Rev. Lett. 79, 2153 (1997); D. Bruss et al., Phys. Rev. Lett. 81, 2598 (1998); L.M. Duan and G.C. Guo, Phys. Rev. Lett. 80, 4999 (1998); C. Simon et al., Phys. Rev. Lett. 84, 2993 (2000); V. Bužek and M. Hillery, Phys. Rev. Lett. 81, 5003 (1998); S.L. Braunstern, N.J. Cerf et al., Phys. Rev. Lett. 86, 4938 (2001); G.M. D’Ariano et al., Phys. Rev. Lett. 86, 914 (2001).
[5] H.K. Cummins et al., Phys. Rev. Lett. 88, 187901 (2002).
[6] A. Lamas-Linares et al., Science 296, 712 (2002).
[7] S. Fasel et al., Phys. Rev. Lett. 89, 107901 (2002).
[8] Y. F. Huang, Phys. Rev. A 64, 012315 (2001).
[9] C. A. Fuchs et al., Phys. Rev. A 56, 1163 (1997); R. B. Griffiths and C.-S. Niu, Phys. Rev. A 56, 1173 (1997).
[10] C.-S. Niu and R.B. Griffiths, Phys. Rev. A 60, 2764 (1999).
[11] D. Bruss et al., Phys. Rev. A 62 012302 (2000).
[12] G. M. D’Ariano and C. Macchiavello, Phys. Rev. A 64 042308 (2001); H. Fan et al., Phys. Rev. A 65 012304 (2002).
[13] T. Durt and J. Du, e-print quant-ph/0309072.
[14] J. Fiurasek, Phys. Rev. A 67, 052314 (2003).
[15] N. Gisin et al., Rev. Mod. Phys. 74, 145 (2002).
[16] C.H. Bennett and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984) p. 175.
[17] V. Scarani and N. Gisin, Phys. Rev. Lett. 87, 117901 (2001).
[18] D. Bruss, Phys. Rev. Lett. 81, 3018 (1998); H. Bechmann-Pasquinucci and N. Gisin Phys. Rev. A 59, 4238 (1999).
[19] D.G. Cory et al., Physica D 120, 82 (1998); J. Du et al., Phys. Rev. Lett. 81, 100403 (2003).