

Quantum Copiers

Howard E. Brandt

U.S. Army Research Laboratory, Adelphi, MD, U.S.
hbrandt@arl.army.mil

According to the no-cloning theorem of quantum information theory, arbitrary quantum states cannot be cloned because of the linearity of quantum mechanics [1]. The security of quantum key distribution in quantum cryptography depends on this physical fact. The implication is that one cannot produce an exact copy of an arbitrary qubit. This does not mean however that an approximate copy cannot be made. The function of one type of quantum copier is to produce an approximate copy of a qubit that is as close to being an exact copy as possible, and with the original qubit changed as little as possible in the process. A variety of quantum copiers have been considered in the literature on quantum information processing.

A universal quantum copier is one that produces two identical copies whose quality is independent of the input state. The universal quantum copier must copy an arbitrary pure state $|\psi\rangle_i$ which can be written in a chosen basis, $\{|0\rangle_i, |1\rangle_i\}$, as follows:

$$|\psi\rangle_i = \alpha |0\rangle_i + \beta |1\rangle_i, \quad (1)$$

for which a general parameterization of the coefficients is given by

$$\alpha = \sin \theta \exp(i\phi), \quad \beta = \cos \theta, \quad (2)$$

in which $i = \sqrt{-1}$, and θ and ϕ are angles on the Bloch sphere (not to be confused with the index i in Eq. (1)). The universal quantum copier must satisfy three basic requirements [2]: (1) If the state of the original qubit at the output of the quantum copier is denoted by the density operator ρ_i^{out} , and that of the quantum copy is ρ_f^{out} , one requires that

$$\rho_i^{out} = \rho_f^{out}, \quad (3)$$

(2) If the measure of distance between two states with density operators ρ_1 and ρ_2 is taken to be the Hilbert-Schmidt norm, namely, $d(\rho_1, \rho_2) = \text{Tr}[(\rho_1 - \rho_2)^2]$, then the requirement that pure states be copied equally well can be expressed by

$$d(\rho_i^{out}, \rho_i^{id}) = d(\rho_f^{out}, \rho_f^{id}) = C, \quad (4)$$

where the superscript *id* denotes the ideal density operator describing the input state, and C is a constant, independent of the input state; and (3) Equation (4) should be minimized with respect to all unitary transformations within the Hilbert space of the two qubits and the quantum copier.

It can be shown that the unitary transformation that implements the universal quantum copier by satisfying requirements (1)-(3) is given by [3]:

$$|0\rangle_i |Q\rangle_x \implies (3/2)^{-1/2} |0\rangle_i |0\rangle_f |\uparrow\rangle_x + 3^{-1/2} |+\rangle_{if} |\downarrow\rangle_x, \quad (5)$$

and

$$|1\rangle_i |Q\rangle_x \implies (3/2)^{-1/2} |1\rangle_i |1\rangle_f |\downarrow\rangle_x + 3^{-1/2} |+\rangle_{if} |\uparrow\rangle_x, \quad (6)$$

where

$$|+\rangle_{if} = 2_i^{-1/2} (|1\rangle_i |0\rangle_f + |0\rangle_i |1\rangle_f). \quad (7)$$

Here indices i , f , and x designate the original qubit, the copy, and the copier, respectively. The copier has a two-dimensional state space with basis vectors $|\uparrow\rangle_x$ and $|\downarrow\rangle_x$, and $|Q\rangle_x$ denotes the initial state of the copier. The implication of Eqs. (5)-(7) is that the copy contains 5/6 of the desired state and 1/6 of the undesired. The

universal quantum copier can be implemented with a network of simple quantum gates. It can be shown that owing to residual correlations between the copy and the quantum copier, quantum copying degrades entanglement. Also, it is important to stress that quantum decoherence is an obstacle to useful implementations of quantum copying because it limits the state storage time [4].

Quantum copiers can be utilized in eavesdropping on quantum key distribution in quantum cryptography by obtaining at least part of an unknown quantum key. An alternative approach to obtaining at least part of a secret quantum key exploits quantum entanglement of an eavesdropping device with the key during its transit between the legitimate users [5], [6]. If the error rate of the legitimate users is sufficiently high, then a prohibitive amount of key must be sacrificed during key distillation.

References

- [1] M. A. Nielsen and I. C. Chuang, Quantum Computing and Quantum Information, Cambridge University Press (2010).
- [2] V. Buzek and M. Hillery, Quantum copying: Beyond the no-cloning theorem, Phys. Rev. A **54**, 1844-1852 (1996).
- [3] V. Buzek, S. Braunstein, M. Hillery, and D. Bruss, Quantum copying: A network, Phys. Rev A **56**, 3446-3452 (1997)
- [4] H. E. Brandt, Qubit devices and the issue of quantum decoherence, Progress in Quantum Electronics **22**, 257-370 (1998).
- [5] H. E. Brandt, Systems and methods for obtaining information on a key in BB84 protocol of quantum key distribution, U.S. Patent Pub. No, US2009/0175450, (2009).
- [6] H. E. Brandt, Alternative design for quantum cryptographic entangling probe, U. S. Patent 7,876,901 B2 (2011).