Single-Qubit Optical Quantum Fingerprinting

Rolf T. Horn,[1] S. A. Babichev,[1,2] Karl-Peter Marzlin,[1] A. I. Lvovsky,[1,2] and Barry C. Sanders[1]

[1]*Institute for Quantum Information Science, University of Calgary, Alberta T2N 1N4, Canada*

[2]*Fachbereich Physik, Universität Konstanz, D-78457 Konstanz, Germany*

(Received 23 September 2004; revised manuscript received 1 December 2004; published 4 October 2005)

We analyze and demonstrate the feasibility and superiority of linear optical single-qubit fingerprinting over its classical counterpart. For one-qubit fingerprinting of two-bit messages, we prepare "tetrahedral" qubit states experimentally and show that they meet the requirements for quantum fingerprinting to exceed the classical capability. We prove that shared entanglement permits 100% reliable quantum fingerprinting, which will outperform classical fingerprinting even with arbitrary amounts of shared randomness.

DOI: 10.1103/PhysRevLett.95.150502 PACS numbers: 03.67.Hk, 42.50.Dv

Introduction.—Quantum communication can significantly improve on the resource requirements compared to classical communication [1]. Fingerprinting, which enables an efficient way of inferring whether longer messages are identical or not, is a particularly striking example as quantum fingerprinting offers an exponential reduction of resources compared to classical fingerprinting [2]. In fact, even for single-qubit fingerprinting one can demonstrate an advantage of quantum protocols with respect to classical ones [3]. Here we establish the feasibility of single-qubit optical quantum fingerprinting, by theoretical analysis and also by experimentally generating and assessing the appropriate quantum optical states for encoding. In particular we (i) develop an optical protocol for single-qubit fingerprinting, (ii) show that two-photon coincidence measurements suffice as the experimental test for comparing fingerprints, (iii) prove that one shared entangled bit between Alice and Bob allows zero-error quantum fingerprinting which outperforms classical fingerprinting even with unlimited shared randomness between Alice and Bob, and (iv) present experimental results on the supply of fingerprint states that demonstrate the feasibility of the protocol. Our results open the prospect of experimental quantum communication complexity; although here we focus on single-qubit fingerprinting and correlated photon pairs, scalability will become possible as multiphoton entanglement capabilities improve [4].

Within the simultaneous message passing model [5], fingerprinting is constructed as follows. Two parties, Alice (A) and Bob (B), receive classical n-bit message inputs x and y from a supplier Sapna (S). Alice and Bob wish to test their messages for equality but are forbidden to communicate or share information with each other. They can, however, communicate with a third party Roger (R). Communication is expensive, so Alice and Bob create (classical or quantum) fingerprints of length g for their respective messages, which they send to Roger. Roger's goal is to generate a single-bit value z which provides the best inference of the function

$$\mathrm{EQ}\,(x,y) = \begin{cases} 0 & \text{if } x \neq y \\ 1 & \text{if } x = y \end{cases}, \tag{1}$$

and Roger is successful if $z = \mathrm{EQ}(x, y)$. If the inference is guaranteed to be successful for $x = y$, the protocol is a *one-sided error* protocol; a *two-sided error* protocol does not provide such a guarantee. Each message belongs to a set $M = \{0, \ldots, m-1\}$ comprised of m different messages represented as bit strings of length $n \equiv \lceil \log_2 m \rceil$ and each fingerprint to a set $F = \{0, \ldots, f-1\}$ of f different fingerprints. Classically, $g = \lceil \log_2 f \rceil$ and $F = \{0, 1\}^g$ while in the quantum case $F \subset \mathcal{H}_2^g$ for $\mathcal{H}_2 = \mathrm{span}\{|0\rangle, |1\rangle\}$. The protocol is evaluated according to the worst case scenario (WCS), in which Sapna, who is aware of other parties, always sends message pairs for which the probability for $z \neq \mathrm{EQ}(x, y)$ is maximized (i.e., performance in the WCS corresponds to the "guarantee" on the protocol). For example, when $n = 2$, $g = 1$, the WCS error probability is 1 for classical fingerprinting protocols with one-sided error and no shared information between Alice and Bob [3].

We consider two scenarios for $n = 2$, $g = 1$. In the first scenario, Alice and Bob simultaneously send to Roger unentangled single photons [6] with polarization states expressed in the logical basis $|0\rangle$ and $|1\rangle$. In the second scenario, we relax the condition that a shared resource is forbidden and provide Alice and Bob with a source of entangled photon pairs in the singlet Bell state $|\Psi^-\rangle \equiv (|0, 1\rangle - |1, 0\rangle)/\sqrt{2}$. In the first scenario we are able to show that a linear optical single-qubit quantum fingerprinting protocol outperforms single-bit classical fingerprinting. In the second scenario, we show that there exists a protocol that can yield perfect one-qubit fingerprinting, outperforming one-bit fingerprinting with an arbitrary amount of shared randomness.

Our first scenario is of special importance in the context of quantum communication complexity: as established by Buhrman *et al.* [2], without Alice and Bob sharing a common resource (for example, entanglement or random classical information) quantum fingerprinting requires exponentially less resources than its classical counterpart. Our second scenario, on the other hand, is a step forward with respect to a recent work by Massar [7] who proposed an interferometric fingerprinting protocol with Alice and Bob sharing a resource in the form of a single photon from

© 2005 The American Physical Society

a common source and demonstrated a two-sided error rate of 1/6 for $m = 3$. Horn *et al.* [8] provide a detailed comparison of entanglement-assisted quantum fingerprinting and its advantages over classical fingerprinting with shared randomness.

Encoding.—For any message $w \in M$ that Alice or Bob receive, they transform their qubit to a unique fingerprint state $|\Omega_w\rangle$ with $|\Omega \equiv (\theta, \phi)\rangle \equiv \cos(\theta/2)|0\rangle + \exp(i\phi) \times \sin(\theta/2)|1\rangle$. The state can be understood geometrically by identifying θ and ϕ with azimuthal and polar angles of the (Bloch) sphere. We assume that Alice and Bob employ the same mapping: $x = y \Leftrightarrow |\Omega_x\rangle = |\Omega_y\rangle$. Quantum fingerprinting allows m different qubit states so each message is distinctly encoded, but the distinguishability of these distinct states diminishes as m increases, with indistinguishability quantified by $\delta(\Omega', \Omega) \equiv |\langle\Omega'|\Omega\rangle|^2 = |\cos(\theta/2)(\theta'/2)\cos(\theta/2) + \exp[i(\phi - \phi')]\sin(\theta'/2) \times \sin(\theta/2)|^2$.

Single-qubit fingerprinting is especially interesting because of its current feasibility. To demonstrate this, we analyze the case $m = 4$ ($n = 2$). In this case the largest overlap between different states is minimized by the following set of four states,

$$F = \left\{|\Omega_w\rangle; \Omega_0 = (0, 0), \Omega_w = \left(2\cos^{-1}\frac{1}{\sqrt{3}}, \frac{2\pi}{3}w\right) \text{ for } w = 1, 2, 3\right\}, \tag{2}$$

and $\delta = \delta_{\text{diff}} \equiv 1/3$ for all pairs of different states [9,10]. We refer to the states (2) as "tetrahedral states" because the four states form the vertices of a tetrahedron on the Bloch sphere [10].

Protocol.—Alice and Bob map their two-bit messages to the tetrahedral states, and Roger's task is to assess $\text{EQ}(x, y)$ by measuring and inferring whether $|\Omega_x\rangle = |\Omega_y\rangle$. The original proposals [2,3] provided Roger with a controlled swap gate and an ancilla qubit [Fig. 1(a)]. The ancilla is prepared as $(|0\rangle + |1\rangle)/\sqrt{2}$ and entangled with the fingerprint states as follows: the two fingerprint states are not swapped if the ancilla is in the state $|0\rangle$ and swapped otherwise. The ancilla then passes through a Hadamard gate and is measured in the logical basis with outcome $r \in \{0, 1\}$ corresponding to the ancilla being in state $|r\rangle$. Roger uses the measurement result r to determine $z = 1 - r$, with outcome $z = 0$ and $z = 1$ yielding an inference of distinct and identical fingerprint states, respectively. We call such a strategy "pure" to signify that Roger is allowed no randomness in making his inference.

The encoding (2) yields a one-sided error protocol because Roger's error rate when Sapna sends $x = y$ is $p_{\text{err}}^{\text{same}} \equiv 1 - (1/2)[1 + \delta] = 0$. In the WCS, Sapna always sends different states so that, when Roger obtains $r = 0$, he infers $z = 1$ with error rate $p_{\text{err}}^{\text{diff}} = p_{\text{err}}^{\text{WCS}} = 1 - (1/2) \times [1 - \delta]$, which beats the classical result of $p_{\text{err}}^{\text{WCS}} = 1$. For $m = 4$ and tetrahedral encoding, we obtain $p_{\text{err}}^{\text{WCS}} = 2/3$.

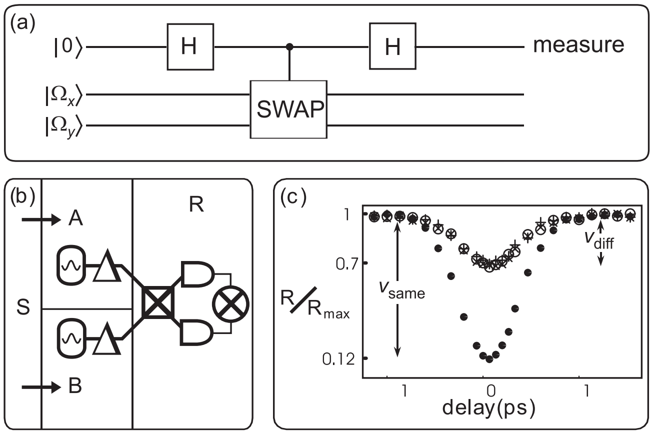

FIG. 1. (a) Quantum circuit of the original fingerprinting protocol [2,3]. (b) Linear optical implementation: Alice (A) and Bob (B) each receive a two-bit message from Sapna (S) and a single photon in a known polarization state from a source. The photons are transformed (represented by △) to particular tetrahedral states according to the received message. The photons are sent to Roger (R) who mixes them at a symmetric beam splitter ⊠ and uses coincidence detection (two detectors ⊂⊃ and a multiplier ⊗) to infer if the messages were the same or different. (c) Coincidence dip with state $|\Omega_1\rangle$ mixed with $|\Omega_0\rangle$ (○), $|\Omega_1\rangle$ (●), $|\Omega_2\rangle$ (+), and $|\Omega_3\rangle$ (×). The plots correspond to the normalized coincidence rate R/R_{max} (with $R_{\text{max}} = 474\ \text{s}^{-1}$ the maximum observed rate, or background rate, for the HOM dip) vs the relative delay between two photons. v_{same} and v_{diff} represent the dip depth $1 - R_{\text{min}}/R_{\text{max}}$ for photons in same or different states, respectively.

A controlled swap gate is not available in a deterministic linear optical system, but we show that it is not required. If Alice and Bob each send a single photonic qubit encoded in polarization to Roger, then Roger only needs to measure whether the photons are in the same polarization. This measurement can be accomplished with the Hong-Ou-Mandel effect according to which two photons entering a symmetric beam splitter in indistinguishable optical (including polarization) modes exit it through the same port [11]. These states produce a Hong-Ou-Mandel (HOM) dip in the coincidence rate [12] as the delay of the incidence photons is varied. For photons of nonidentical polarization, the dip depth is degraded according to the mode overlap δ.

For $n = 2$, Alice and Bob each receive two-bit messages from Sapna, which are used to encode their photonic qubit into one of the tetrahedral states. Their photons are transmitted to Roger who infers using a symmetric beam splitter whether the messages were the same or different. This protocol is depicted in Fig. 1(b). Ideally Alice and Bob would have separate single-photon–on-demand sources, but practically they will be supplied with correlated, unentangled photons from a down-conversion source. Later we consider the case in which Alice and Bob share entangled photons.

Roger assigns $r := 0$ for a no-coincidence and $r := 1$ for a coincidence event, then employs (as before) the strategy $z = 1 - r$. The result $r = 1$ guarantees that the two messages are distinct whereas $r = 0$ only indicates that the messages were possibly the same. In fact, this HOM dip protocol is equivalent to the controlled swap version of single-qubit quantum fingerprinting: if Sapna sends $x = y$, a definite no-coincidence event guarantees $p_{\rm err}^{\rm same} = 0$ whereas for $x \neq y$ the probability that Alice's and Bob's photons do not trigger a coincidence detection is identically $p_{\rm err}^{\rm diff} = [(1 + \delta)/2]$. Thus Sapna always sends different messages in the WCS, and for $m = 4$, and tetrahedral encoding, $p_{\rm err}^{\rm WCS} = 2/3$.

This error rate appears relatively high, yet it is superior to classical one-bit fingerprinting with one-sided error, in which failure is guaranteed for at least one pair of messages, resulting in $p_{\rm err}^{\rm WCS} = 1$ [3]. Of course a 100% failure rate for the classical case can be improved by allowing Roger a random (“mixed”) strategy, but then the quantum protocol can be improved in the same way, always maintaining its superiority over the classical case [3,8].

Experiment.—The feasibility of this protocol has been demonstrated by creating simultaneous pairs of tetrahedral states and analyzing the dip achieved by Roger's setup in Fig. 1(b). To create correlated photons, a Ti:Sapphire laser tuned to a wavelength of 790 nm emitted 170 fs pulses that were frequency doubled and then down-converted in a type I configuration via a 2 mm beta-barium borate crystal. Output photons were spectrally filtered with a 2 nm interference filter and transmitted through $\lambda/2$ and $\lambda/4$ wave plates which were rotated to convert the polarization state in each channel into one of the tetrahedral states. The two photons were then overlapped in free space on a symmetric beam splitter and subjected to measurements with single-photon counting modules; the experimental results are presented in Fig. 1(c) where state $|\Omega_1\rangle$ is mixed with itself and each of the other three states. The largest dip in Fig. 1(c) corresponds to the traditional HOM dip with two identical states, and the degree of distinguishability is varied by controlling the relative delay between the two photons. The experimental coincidence rates as a fraction of the maximum coincidence rate $R/R_{\rm max}$ for all 16 possible fingerprint pairs are given in Table I (first set of numbers) and are consistent with Clarke *et al.*'s experimental results for tetrahedral states [9].

Ideally, the dip depths should be $v_{\rm same} = \delta_{\rm same} = 1$ and $v_{\rm diff} = \delta_{\rm diff} = 1/3$. Because of an imperfect spatiotemporal overlap of the two single-photon wave packets, the depth of each dip is, however, degraded. Experimental values of $v_{\rm same}$ are consistently at 88% or higher, whereas those of $v_{\rm diff}$ approximate 30% and exhibit some additional variation due to birefringence in the beam splitter and systematic errors in wave plate setting.

The fingerprinting error rates can be determined from the empirical depths, bearing in mind that for ideal single-photon sources and detectors, the coincidence rate in the flat part of the HOM graph is half the photon pair production rate. Therefore, given a dip depth v, the probability for a pair of photons to generate a coincidence event is $p_{\rm coinc} = (1 - v)/2$. From a coincidence event, Roger will infer that the input states differ. If the input states were indeed not identical ($w \neq w'$), Roger will make a correct inference with a probability $p_{\rm coinc}$ and an error with a probability $p_{\rm err}^{ww'} = 1 - p_{\rm coinc} = (1 + v_{ww'})/2$. If, on the other hand, the input states are identical, the error probability for given w is $p_{\rm err}^{ww} = p_{\rm coinc} = (1 - v_{ww})/2$. The error rates calculated in this manner are displayed as the second set of numbers in Table I and are in good agreement with the theoretically expected $p_{\rm err}^{\rm same} = 0$, $p_{\rm err}^{\rm diff} = 2/3$ derived above.

TABLE I. Experimental HOM dip depths ($v_{ww'}$)/fingerprinting error rates ($p_{\rm err}^{ww'}$) for each pair of tetrahedral states.

	Bob			
Alice	0	1	2	3
0	0.88/0.06	0.31/0.66	0.24/0.62	0.26/0.63
1	0.30/0.65	0.88/0.06	0.25/0.63	0.40/0.70
2	0.44/0.72	0.30/0.65	0.89/0.06	0.25/0.63
3	0.20/0.60	0.30/0.65	0.35/0.63	0.89/0.06

In practice, parametric down-conversion is not sufficient as a photon production tool because Alice and Bob are not aware when a photon pair has been produced and sent to Roger. Practical quantum fingerprinting will be advantageous with respect to its classical counterpart only with deterministic (on-demand or heralded [13]) single-photon sources, loss-free communication channels, and highly efficient single-photon detectors. A further advantage can be gained by using number-resolving detectors [14] that can distinguish no-coincidence events from those in which one of the photons has been lost during transmission or detection.

Two-sided errors.—In the above theoretical analysis, we have established the superiority of quantum fingerprinting with respect to classical, assuming a one-sided error scheme. On the other hand, our experimental results exhibit two-sided errors (diagonal error terms in Table I are nonzero). In order to verify that the quantum advantage holds in spite of the experimental imperfection, we must compare classical and quantum WCS error rates assuming that Roger incorporates randomness and employs a mixed strategy aimed at minimizing these rates.

The mixed strategy is as follows. Roger makes an initial inference $z = 1 - r$ as before. He then generates a final inference z^* by randomly inverting the value of z with probabilities π_0 for $z = 1$ and π_1 for $z = 0$. The new error rates will be given by

$$\begin{aligned}(p_{\rm err}^{\rm diff})^* &= (1 - \pi_0)p_{\rm err}^{\rm diff} + \pi_1(1 - p_{\rm err}^{\rm diff}),\\ (p_{\rm err}^{\rm same})^* &= (1 - \pi_1)p_{\rm err}^{\rm same} + \pi_0(1 - p_{\rm err}^{\rm same}),\end{aligned} \tag{3}$$

for Sapna supplying $x \neq y$ and $x = y$ respectively. The WCS error rate corresponds to the higher of the above probabilities, so Roger must choose π_0 and π_1 so as to minimize it. Substituting our experimental values of $p_{\mathrm{err}}^{\mathrm{same}} \sim 0.06$ and $p_{\mathrm{err}}^{\mathrm{diff}} \sim 0.65$ into Eq. (3) we find that the optimum is achieved for $\pi_0 = 0.37$ and $\pi_1 = 0$, in which case the error rates are $(p_{\mathrm{err}}^{\mathrm{diff}})^* = (p_{\mathrm{err}}^{\mathrm{same}})^* = 0.41$. For this optimal mixed strategy, Sapna's choice of messages becomes irrelevant: all cases correspond to a WCS. For the classical case, the minimum WCS error rate equals 0.5, thus confirming the advantage of the quantum protocol.

Shared entanglement.—Thus far Alice and Bob have been denied any communication, but experimentally it is straightforward to provide Alice and Bob with an entangled pair of photons. In Ref. [7], Massar showed that a shared ebit (in the form of a single photon interferometrically split between Alice and Bob [15]) helps one achieve a fingerprinting error rate of $1/6$ for $m = 3$. Here we show that shared entanglement in fact allows perfect single-qubit quantum fingerprinting for $m = 4$ and, furthermore, exceeds the classical limit. The classical analog to this case corresponds to the performance in the WCS for Alice and Bob sharing random bits that are secret from Sapna.

We allow Alice and Bob to share the Bell singlet state $|\Psi^-\rangle$. Alice and Bob each receive a two-bit message from Sapna and apply one of the four Pauli operations according to which message has been sent. The result is that the state sent to Roger is one of the four Bell states. If Alice and Bob perform the same Pauli operation, $|\Psi^-\rangle$ is invariant (up to a global phase); if Alice and Bob apply different transformations, $|\Psi^-\rangle$ maps to a different Bell state. Thus, for Roger to infer whether the messages are the same or different, he needs only to detect whether he has received the state $|\Psi^-\rangle$ or not. The Bell state discriminator, in the form of a HOM dip apparatus discussed earlier, suffices as a discriminator between the Bell state $|\Psi^-\rangle$ and the other three Bell states [11]. For a perfectly efficient setup, a coincidence is guaranteed for an input Bell state $|\Psi^-\rangle$, and no coincidence occurs for the other Bell states. Therefore, the protocol can achieve $p_{\mathrm{err}}^{\mathrm{WCS}} = 0$ by consuming one ebit for each pair of two-bit messages delivered by Sapna.

The physics underlying this fingerprinting scheme resembles that employed in quantum dense coding [11], but the purposes that these two communication protocols serve are quite different. Whereas, in the latter case, a shared ebit is used to communicate a classical two-bit message from Alice to Bob, the former allows a third party (Roger) to compare two two-bit messages.

A 100% success rate is unachievable in classical one-bit fingerprinting regardless of how many random bits Alice and Bob share. If Alice and Bob share one random bit (in the case of a shared ebit, Alice and Bob could convert their ebit to a shared classical random bit if they wish), Roger's success rate for classical one-bit fingerprinting rises from zero to $1/2$ when Roger follows a pure strategy. If Alice and Bob share an arbitrarily large number of random bits, Roger's success rate improves but cannot exceed $2/3$ for any fixed number of random bits [8].

Conclusions.—We have proposed an optical protocol for single-qubit fingerprinting, experimentally demonstrated its functionality for the case $m = 4$, and shown that tetrahedral states can be produced that meet the requirements for beating the classical one-bit fingerprinting protocol for $m = 4$. We have also proven that single-qubit quantum fingerprinting with shared entanglement can succeed with a zero error rate, which beats the classical fingerprinting protocol with an arbitrary amount of shared randomness between Alice and Bob. The experimental results show that, in reality, two-sided errors must be accounted for, but we have shown that Roger's best strategy is to randomly vary his inference of whether the states are the same but not change his guesses as to whether they are different, and this approach yields a performance, given experimentally obtained parameters, that exceeds the classical error bound. Quantum fingerprinting is an excellent example of the new field of quantum communication complexity [1], and our results here open this field to experiments. Further work is now underway on quantum fingerprinting with two qubits and beyond, which will allow scaling and complexity issues to be fully investigated.

We appreciate valuable discussions with J. N. de Beaudrap, R. Cleve, and J. Watrous. This research has been supported by iCORE and the CIAR.

[1] G. Brassard, Found. Phys. **33**, 1593 (2003).
[2] H. Buhrman *et al.*, Phys. Rev. Lett. **87**, 167902 (2001).
[3] J. N. de Beaudrap, Phys. Rev. A **69**, 022307 (2004).
[4] M. Eibl *et al.*, Phys. Rev. Lett. **90**, 200403 (2003).
[5] A. C. C. Yao, in *Proceedings of the 11th Annual ACM Symposium on Theory of Computing* (ACM, New York, 1979), p. 209.
[6] Focus issue on Single Photons on Demand, edited by P. Grangier, B. C. Sanders, and J. Vuckovic [New J. Phys. **6**, (2004)]; http://www.iop.org/EJ/toc/1367-2630/6/1.
[7] S. Massar, quant-ph/0305112.
[8] R. T. Horn *et al.*, Quantum Inf. Comput. **5**, 258 (2005).
[9] R. B. M. Clarke *et al.*, Phys. Rev. A **64**, 012303 (2001).
[10] E. B. Davies, IEEE Trans. Inf. Theory **24**, 596 (1978).
[11] K. Mattle *et al.*, Phys. Rev. Lett. **76**, 4656 (1996).
[12] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
[13] C. K. Hong and L. Mandel, Phys. Rev. Lett. **56**, 58 (1986); P. Grangier, G. Roger, and A. Aspect, Europhys. Lett. **1**, 173 (1986); T. Aichele, A. I. Lvovsky, and S. Schiller, Eur. Phys. J. D **18**, 237 (2002).
[14] J. Kim *et al.*, Appl. Phys. Lett. **74**, 902 (1999).
[15] S. A. Babichev, J. Appel, and A. I. Lvovsky, Phys. Rev. Lett. **92**, 193601 (2004).