Quantum fingerprinting with coherent states and a constant mean number of photons

Juan Miguel Arrazola and Norbert Lütkenhaus

Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo,
200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1

(Received 3 October 2013; published 4 June 2014)

We present a protocol for quantum fingerprinting that is ready to be implemented with current technology and is robust to experimental errors. The basis of our scheme is an implementation of the signal states in terms of a coherent state in a superposition of time-bin modes. Experimentally, this requires only the ability to prepare coherent states of low amplitude and to interfere them in a balanced beam splitter. The states used in the protocol are arbitrarily close in trace distance to states of $O(\log_2 n)$ qubits, thus exhibiting an exponential separation in abstract communication complexity compared to the classical case. The protocol uses a number of optical modes that is proportional to the size n of the input bit strings but a total mean photon number that is constant and independent of n. Given the expended resources, our protocol achieves a task that is provably impossible using classical communication only. In fact, even in the presence of realistic experimental errors and loss, we show that there exist a large range of input sizes for which our quantum protocol transmits an amount of information that can be more than two orders of magnitude smaller than a classical fingerprinting protocol.

DOI: 10.1103/PhysRevA.89.062305 PACS number(s): 03.67.Hk, 42.50.Ex, 89.70.Hj

I. INTRODUCTION

Communication complexity is the study of the amount of communication that is required to perform distributed information-processing tasks. This corresponds to the scenario in which two parties, Alice and Bob, respectively receive inputs $x,x' \in \{0,1\}^n$. Their goal is to collaboratively compute the value of a Boolean function $f(x,x')$ with as little communication as possible [1]. Although they can always do this by communicating their entire input, there are many situations in which they can succeed with significantly less communication [2].

Likewise, quantum communication complexity studies the case where the parties are allowed to employ quantum resources such as quantum channels and shared entanglement (see Refs. [3,4] for an overview). Remarkably, it has been proven that there exist various problems for which the use of quantum resources offer exponential savings in communication compared to their classical counterparts [5–9]. Unfortunately, these results are currently accompanied by only a few experimental demonstrations [10–12], and providing a method to facilitate their implementation is a pressing problem.

We focus on the *simultaneous message passing* model [1], in which Alice and Bob are not allowed to communicate with each other but instead send messages to a third party, the referee, who must determine the value of the function based only on the messages she receives. An important example is the equality problem, where $f(x,x')=1$ if and only if $x=x'$. In this case, Alice and Bob can achieve their goal by sending much shorter *fingerprints* of their original inputs. If they are restricted to classical messages and local randomness only, it has been shown that the optimal classical protocols require fingerprints of length at least $\Omega(\sqrt{n})$ when an arbitrarily small probability of error is allowed [13–15]. On the other hand, it was shown in Ref. [9] that if Alice and Bob are allowed to send quantum states, then they only need to send fingerprints of $O(\log n)$ qubits, thus demonstrating an exponential separation between classical and quantum communication complexity.

In this work, we present a protocol for quantum fingerprinting that uses quantum states that are arbitrarily close in trace distance with respect to states of $O(\log_2 n)$ qubits, thus exhibiting an exponential separation in abstract communication complexity compared to the classical case. The protocol is robust to experimental imperfections and is characterized by a probability of error which is tunable and can be made arbitrarily small. Moreover, in an ideal implementation, the mean photon number of the signals is independent of n, so that the energy cost of the protocol is constant regardless of the size of the messages.

In the remainder of this paper, we describe the results of Ref. [9], and based on them, we outline the protocol for implementing quantum fingerprinting with coherent states and a constant mean number of photons. We then show how the protocol can be adjusted to account for experimental errors, and we analyze its performance in realistic scenarios. Finally, we conclude by discussing further possible applications of our results as well as some of its limitations.

II. COHERENT-STATE QUANTUM PROTOCOL

Quantum fingerprinting, as introduced in Ref. [9], relies on the concept of error-correcting codes. A code can be expressed as a function $E:\{0,1\}^n \rightarrow \{0,1\}^m$, where $E(x)$ is the *codeword* associated with the input x and $m=cn$ for some $c>1$. The protocol makes use of codes that have the additional property that the minimum Hamming distance between any two codewords is at least $(1-\delta)m$ for some $\delta>0$. One example is Justesen codes [16], for which we can have $\delta < \frac{9}{10}+\frac{1}{15c}$ whenever $c>2$. In Ref. [9], a protocol is specified in which, for each possible input x and corresponding codeword $E(x)$, Alice and Bob prepare the fingerprint states

$$|h_x\rangle = \frac{1}{\sqrt{m}}\sum_{i=1}^{m}(-1)^{E(x)_i}\,|i\rangle\,, \tag{1}$$

where $E(x)_i$ is the ith bit of the codeword $E(x)$. This state has dimension m, so it can be associated with a system of $\log_2 m = O(\log_2 n)$ qubits.

An approach to implementing the fingerprint states is to decompose the underlying Hilbert space as a tensor product of

Hilbert spaces of smaller dimension [12,17,18]. For example, we could have a collection of $O(\log_2 n)$ two-level systems, such as photons in the polarization degree of freedom. As noted already in Ref. [12], a serious drawback of this strategy is that most fingerprint states must be highly entangled [19,20], so that even for low input sizes, the experimental requirements greatly exceed that which is possible to achieve with current technology, except for the case of single-qubit quantum fingerprinting [17,18].

Alternatively, we can consider the underlying Hilbert space as arising directly from a single m-dimensional physical system, such as a single photon distributed over m orthogonal optical modes, as has been considered in Refs. [21,22]. In that case, let b_i be the annihilation operator of the ith optical mode. We define the *fingerprint mode* as $a_x = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} (-1)^{E(x)_i} b_i$, so that a single-photon state in the fingerprint mode

$$a_x^\dagger |0\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} (-1)^{E(x)_i} |1\rangle_i \tag{2}$$

is *exactly* an implementation of the fingerprint state of Eq. (1). Here $|1\rangle_i$ denotes a one-photon state in the ith mode. Since these states are an exact implementation of the fingerprint states, they are equivalent to states of $O(\log_2 n)$ qubits, even if the number of modes employed is proportional to the input size n. This clearly indicates that the amount of abstract communication in a protocol is not given by the number of modes used.

In general, we must quantify the amount of communication by the smallest number of qubits that would be required, in principle, to replicate the performance of the protocol. More precisely, if a quantum communication protocol uses states in a Hilbert space of dimension d, this space can be associated with a system of $O(\log_2 d)$ qubits. Therefore, the amount of communication C in a quantum protocol is generally given by

$$C = \log_2[\dim(\mathcal{H})], \tag{3}$$

where $\mathcal{H}$ is the smallest Hilbert space containing all the states of the protocol, which may be a significantly smaller subspace of the entire Hilbert space associated with the physical systems. For example, a single photon in the polarization degree of freedom can be used as a qubit, but we require two polarization modes, each representing an infinite-dimensional Hilbert space. Moreover, Holevo's theorem [23] guarantees that no more than $\log_2 d$ classical bits of information could be transmitted, on average, by a quantum protocol that uses states in a Hilbert space of dimension d.

By quantifying communication carefully, we gain a better understanding of the different physical resources that are required to transmit a certain amount of information. For example, the fact that the same amount of information can be transmitted by a single photon in n optical modes, at most n photons in a single mode or $\log_2 n$ qubits, is understood because the smallest Hilbert space containing all possible states in each of the three cases has the same dimension.

In terms of an experimental demonstration, creating states of fixed photon number in a superposition of modes, as proposed in Refs. [21,22], is an extremely challenging task [24]. Instead, we opt for an alternative that is readily implementable in practice: a coherent state in the fingerprint mode. This *coherent fingerprint state* can be written as $|\alpha\rangle_x = D_x(\alpha)|0\rangle$, where $D_x(\alpha) = \exp(\alpha a_x^\dagger - \alpha^* a_x)$ is the displacement operator and α is a complex number. A straightforward calculation shows that this state can be equivalently expressed as a simple sequence of coherent pulses

$$|\alpha\rangle_x = \bigotimes_{i=1}^{m} \left| (-1)^{E(x)_i} \frac{\alpha}{\sqrt{m}} \right\rangle_i, \tag{4}$$

where $|\frac{\alpha}{\sqrt{m}}\rangle_i$ is a coherent state with amplitude $\frac{\alpha}{\sqrt{m}}$ in the ith mode. Notice that a projection of this state onto the single-photon subspace gives exactly the state of Eq. (2).

The phase of each individual state in the product depends on the corresponding bit of the codeword. Therefore, to implement the states correctly, Alice and Bob need a common phase reference, which can be established before the start of the protocol or may be available already from other contexts, without giving Alice and Bob access to shared randomness. On the other hand, the referee needs a measurement that allows her to verify whether the relative phases of the incoming pulses are equal or different. A way of achieving this consists of an interferometer in which the individual pulses enter a balanced beam splitter, and whenever there is a click in the output detectors, it is unambiguously revealed whether their phases are the same or not [25]. We call these outcomes "0" and "1," respectively, in accordance to the relative parity of the phases. In this way, we have established the basic ingredients for a quantum fingerprinting protocol in an ideal implementation:

(1) Alice and Bob fix a value c for the Justesen code and of α for the coherent fingerprint states.

(2) They prepare states $|\alpha\rangle_x, |\alpha\rangle_{x'}$ according to their respective inputs x, x' as in Eq. (4).

(3) They send these states to the referee, who performs an interference measurement on the individual signals using a balanced beam splitter and single-photon detectors.

(4) The referee concludes that the inputs are different if and only if she observes at least one click in the 1 detector.

An illustration of the protocol is shown in Fig. 1.

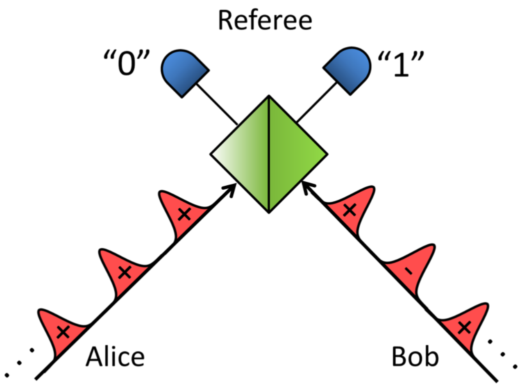

FIG. 1. (Color online) Coherent-state protocol: Alice and Bob send a train of m coherent pulses whose phases (+ or −) depend on the inputs they receive. The referee interferes the individual signals in a 50:50 beam splitter and concludes that the inputs are different if and only if at least one 1 click is observed.

As discussed before, the abstract communication cost of a quantum protocol, which is equal to the amount of information transmitted, is determined by the dimension of the quantum states used. In our case, the coherent fingerprint states are effectively contained in a Hilbert space of small dimension, as is formally summarized by the following statement:

Theorem 1. There exist a set of states $\{|v\rangle_x\}$ of dimension d satisfying $\log_2 d = O(\log_2 n)$, such that for any $\epsilon > 0$, it holds that $\| |v\rangle\langle v|_x - |\alpha\rangle\langle\alpha|_x \|_1 \leqslant \epsilon$ for all inputs x.

Proof. For a given Δ_N, let $\mathcal{H}_V$ be the subspace spanned by the Fock states $|N\rangle_x$ whose photon number N satisfies $|N - |\alpha|^2| \leqslant \Delta_N$. To calculate the dimension of this subspace, we use the fact that the dimension of the space of states with fixed a photon number N is equal to the number of distinct ways in which the photons can be distributed into the m different modes. Since the photons are indistinguishable, this quantity is given by the binomial factor $\binom{N+m-1}{m-1}$ [26]. In the case of $\mathcal{H}_V$, there are $2\Delta_N$ different possible values of N, the largest being $N = |\alpha|^2 + \Delta_N$. Thus, the dimension d of this subspace satisfies

$$\log_2 d \leqslant \log_2 \left[2\Delta_N \binom{|\alpha|^2 + \Delta_N + m - 1}{m-1} \right]$$
$$\leqslant (|\alpha|^2 + \Delta_N) \log_2(m + |\alpha|^2 + \Delta_N - 1) + \log_2(2\Delta_N), \tag{5}$$

which is $O(\log_2 n)$ for any fixed α and Δ_N.

Now let P_V be the projector unto $\mathcal{H}_V$ and define the $O(\log_2 n)$-qubit states $|v\rangle_x := P_V\,|\alpha\rangle_x / ||P_V\,|\alpha\rangle_x||$. Consider a measurement $\{P_V, \mathbb{1} - P_V\}$ that informs us whether the photon number lies within the range $|N - |\alpha|^2| \leqslant \Delta_N$. Since all of the coherent fingerprint states have the same Poissonian photon number distribution with mean $|\alpha|^2$, we can use the properties of this distribution to calculate the probability that the measured number of photons N deviates by an amount Δ_N from its expected value. This probability satisfies [27]

$$\Pr(|N - |\alpha|^2| \geqslant \Delta_N) \leqslant 2e^{-|\alpha|^2} \left(\frac{e|\alpha|^2}{|\alpha|^2 + \Delta_N} \right)^{|\alpha|^2 + \Delta_N} = \epsilon'. \tag{6}$$

This also implies that $1 - |\langle v|\alpha\rangle_x|^2 \leqslant \epsilon'$. Finally, using the Fuchs–van de Graaf inequality [28], we have that

$$\| |v\rangle\langle v|_x - |\alpha\rangle\langle\alpha|_x \|_1 \leqslant 2\sqrt{1 - |\langle v|\alpha\rangle_x|^2} \leqslant 2\sqrt{\epsilon'}, \tag{7}$$

and this can be made equal to any $\epsilon > 0$ by choosing Δ_N accordingly while keeping α fixed. ■

The above result implies that the statistics obtained from any measurement on the coherent fingerprint states can be made arbitrarily close to those obtained from states of $O(\log_2 n)$ qubits. Therefore, for sufficiently small ϵ, the two cases are operationally indistinguishable, and an exponential separation in communication complexity is maintained.

To calculate the error probability of the protocol, notice that whenever $x = x'$, the referee outputs the correct answer with certainty because the only possible outcomes are 0 or no clicks. For the case of $x \neq x'$, we need to calculate the probability that no 1 outcomes are observed. It can be shown (see the Appendix for details) that this probability of error satisfies

$$\Pr_m(\text{error}) \leqslant [1 - p_c(1 - \delta)]^m, \tag{8}$$

where p_c is the probability of obtaining a click at each time slot, which is given by

$$p_c = 1 - \exp\left(-2\frac{|\alpha|^2}{m}\right). \tag{9}$$

To illustrate the behavior of this quantity, note that for large m, we can make the approximation $p_c \approx \frac{2|\alpha|^2}{m}$, so that

$$\Pr_m(\text{error}) \approx \left(1 - \frac{2(1-\delta)|\alpha|^2}{m}\right)^m$$
$$\leqslant \exp[-2(1-\delta)|\alpha|^2]. \tag{10}$$

Therefore, for fixed δ, the probability of error can be made arbitrarily close to zero by fixing α accordingly, and this error decreases exponentially with α. Moreover, we can choose the total mean photon number of the coherent fingerprint states independently of the input size and still satisfy any demand on the error probability.

III. PROTOCOL IN THE PRESENCE OF EXPERIMENTAL ERRORS

So far, we have assumed an ideal scenario, but any practical implementation will invariably suffer from the presence of experimental errors. Our goal is now to show that the above protocol can be modified to become robust against these errors.

The main drawback of the previous protocol is that it is extremely sensitive to the error that occurs when the fingerprints are equal, but the 1 detector fires due to an imperfection. Nevertheless, it is natural to envision a situation in which the expected ratio of 0 to 1 clicks differs significantly for the cases of equal or different inputs, so that these situations can be statistically distinguished. Formally, let f_0 be the observed fraction of 0 outcomes and define the expectation values $q_E := \mathbb{E}(f_0|x = x')$, $q_D := \mathbb{E}(f_0|x \neq x')$, and $\Delta_q = (q_E - q_D)/2$. The modification to the protocol is then very simple: The referee concludes that the inputs are equal if and only if $f_0 > q_E - \Delta_q$. In this case, it can be shown (see the Appendix for details) that the probability of error satisfies

$$\Pr_m(\text{error}) \leqslant \left[1 - p_c'\left(1 - e^{-2\Delta_q^2}\right)\right]^m, \tag{11}$$

where $p_c' \approx p_c + p_{\text{dark}}$ is the effective click probability. Again, for large m, $p_c' \approx 2|\alpha|^2/m$, and we get

$$\Pr_m(\text{error}) \lesssim e^{-2|\alpha|^2(1 - e^{-2\Delta_q^2})}, \tag{12}$$

which can also be made arbitrarily close to zero by fixing α accordingly.

The values of the expectations q_E and q_D as well as the click probability p_c' are determined by the experimental errors. We consider a model of imperfections characterized by three parameters: the combined effect of channel loss and limited detector efficiency η, the limited visibility of the interferometer ν, and the dark count probability p_{dark}. The effect of loss and limited efficiency is equivalent to a transformation $|\alpha\rangle_x \rightarrow |\sqrt{\eta}\alpha\rangle_x$, which can always be compensated by increasing the initial value of α to α/η, without changing the scaling properties of the protocol.

Since $p_{\text{dark}} \ll 1$ and $p_c' \ll 1$ for large n, we neglect the occurrence of double clicks in one time slot. In this case the expected fractions of 0 outcomes can be shown to be

$$\begin{aligned} q_D =& \frac{p_c}{p_c + p_{\text{dark}}}[\nu\delta + (1-\nu)(1-\delta)] + \frac{p_{\text{dark}}}{2(p_c + p_{\text{dark}})}, \\ q_E =& \frac{p_c}{p_c + p_{\text{dark}}}\nu + \frac{p_{\text{dark}}}{2(p_c + p_{\text{dark}})}. \end{aligned} \tag{13}$$

From these expressions we can also calculate Δ_q to obtain

$$\Delta_q = \frac{p_c}{p_c + p_{\text{dark}}}(1-\delta)(2\nu - 1). \tag{14}$$

It is important to notice the crucial role played by the dark count probability, which sets a limit on the maximum input size the protocol can tolerate with a fixed mean photon number. When the click probability p_c becomes smaller than p_{dark}, most of the outcomes are random regardless of whether the inputs are equal or different, making the two situations increasingly difficult to distinguish. To put this into context, it is currently possible to achieve values as low as $p_{\text{dark}} \sim 10^{-8}$ [30]. In this case, the protocol can function for input sizes of up to $n \sim 10^{13}$ for a constant mean number of photons. This can be seen in Fig. 2, where a comparison of classical and quantum fingerprinting protocols is made. We also highlight that even in the presence of errors, our protocol surpasses the performance of a classical protocol [14] for a wide range of input sizes, with a reduction in the transmitted information that can be larger than two orders of magnitude, as depicted by the dotted lines in Fig. 2.

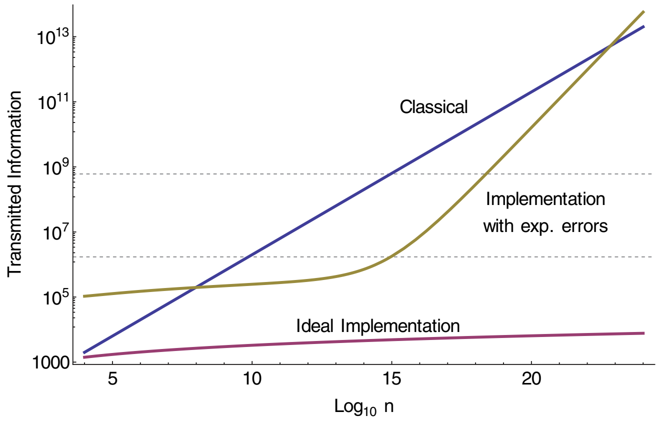

FIG. 2. (Color online) Logarithmic plot for the transmitted information as a function of the input size n for different fingerprinting protocols with probability of error of 10^{-6}. We adopt the classical protocol specified in [14], which requires $2\sqrt{n} + O(1)$ bits of communication and must be repeated ten times to ensure the desired probability of error. For the quantum case, we choose $c = 3$ for the Justesen code and portray the cost for the coherent-state protocol with an ideal implementation ($|\alpha|^2 = 88.8$) and for a nonideal implementation ($|\alpha|^2 = 6651$) suffering from experimental errors. The effective dimension of the states is chosen so that the trace distance between the fingerprint states and states of this dimension is smaller than 10^{-6}. The errors are characterized by the parameters $\eta = 0.1$, $\nu = 0.98$ as in the experiment of [29] and by $p_{\text{dark}} = 4 \times 10^{-8}$, as would occur with the Superconducting Nano-wire Single-Photon Detector (SNSPD) of Ref. [30]. For $n \sim 10^{13}$, it is not possible to maintain the desired error probability for fixed α, and increasing the mean photon number leads to a steeper increase in the transmitted information.

IV. DISCUSSION

We have outlined a quantum fingerprinting protocol that can be implemented with current technology [31], even in the presence of experimental imperfections, and demonstrates an exponential separation in communication complexity compared to the classical case. Previous work had proposed different paths towards the implementation of quantum fingerprinting, but none of them could be experimentally deployed to the point of exhibiting a gap in communication complexity compared to the classical case.

From a practical perspective, we are often interested in the expenditure of resources beyond the abstract amount of communication. For instance, we may be interested in the running time of the protocol or the amount of energy used. Since our protocol uses $O(n)$ optical modes, the total time required to carry the protocol is quadratically larger than what would be needed in a classical protocol. On the other hand, the total number of photons used is constant, whereas, classically, one would need $O(\sqrt{n})$ photons when restricted to using $O(\sqrt{n})$ modes. Thus, our protocol introduces an asymptotically unbounded reduction in energy consumption for the price of only a quadratic increase in running time. Moreover, by Theorem 1, any classical communication protocol using $O(n)$ modes and a constant photon number could only be used to transmit $O(\log_2 n)$ classical bits of information, which is insufficient to solve the equality problem in the simultaneous message passing model. This also means that only $O(\log_2 n)$ classical bits of the input bit strings are leaked to the referee (or anyone else). Overall, given the expended resources, our protocol achieves a task that is provably impossible with classical communication only.

The fact that the total mean photon number is constant has potential practical implications beyond the inherently vast reduction in energy consumption. The clock rate of a quantum communication protocol is usually limited by the dead times of the detectors. However, since in our case each individual mode carries very few photons on average, the expected time between detector clicks could be significantly larger than the dead times, allowing an increase of the clock rate by orders of magnitude. Moreover, time resolution is unnecessary in our scheme; only the click patterns matter regardless of the times at which they occur. Finally, the low photon numbers imply that nonlinear effects are not an issue in the transmission of the signals.

Most important, the fact that only a small subspace is employed in our scheme implies that, in principle, the unused sections of the entire Hilbert space can still be used for other purposes such as the transmission of additional information through multiplexing schemes. For example, it may be possible to conduct multiple quantum fingerprinting protocols in parallel or to perform them alongside classical communication. Although this multiplexing can be achieved in principle, practical methods for achieving it are a line for future research.

Generally, our results imply that any state $|\psi\rangle = \sum_{i=1}^{d} c_i\, |i\rangle$ can be approximately implemented by a sequence of coherent states $\otimes_{i=1}^{d} |\alpha c_i\rangle$. This could provide a promising route for the implementation of other quantum communication protocols. An example is existing schemes for quantum digital signatures [32,33] that also use sequences of phase-encoded coherent states. Our fingerprinting protocol also provides a new ground in which to explore fundamental aspects of quantum mechanics, such as the connection between entanglement and nonorthogonality, the information-carrying capacity of quantum states, and the regime of extremely low mean photon numbers. Overall, our results pave the way for experimental demonstrations of the gap between classical and quantum communication complexity and open a new window of opportunity for research in quantum communication in general.

ACKNOWLEDGMENTS

We thank R. Cleve, R. Koenig, M. Curty, H. Buhrman, and W. Tittel for fruitful discussions concerning this work. J.M.A. would like to thank A. Ignjatovic for her help in preparing this paper, and he acknowledges support from the Mike and Ophelia Lazaridis Fellowship. This work has been supported by Industry Canada, the NSERC Strategic Project Grant (SPG) FREQUENCY, and the NSCERC Discovery Program.

APPENDIX

1. Error probability for the ideal protocol

To calculate the error probability of the ideal protocol, notice that whenever the inputs to Alice and Bob satisfy $x = x'$, the referee outputs the correct answer with certainty because the only possible outcomes are 0 or no clicks. For the case of $x \neq x'$, we need to calculate the probability that no 1 outcomes are observed. After the individual signals interfere in the beam splitter, there will always be a coherent state entering one detector and the vacuum entering the other one. The probability p_c of obtaining a click can be calculated from the Poissonian statistics of the incoming coherent states and is given by

$$p_c = 1 - \exp\left(-2\frac{|\alpha|^2}{m}\right), \tag{A1}$$

where $p_c \approx 2\frac{|\alpha^2|}{m}$ for $\frac{|\alpha^2|}{m} \ll 1$. The total number of clicks in the m signals is therefore a binomial random variable, which we call C. We introduce another random variable Z, the number of 0 outcomes observed. When $x \neq x'$, the conditional probability distribution of Z given that k clicks are observed is a hypergeometric distribution satisfying

$$\Pr_m(Z = \ell | C = k) = \frac{\binom{m\,\delta}{\ell}\binom{m-m\,\delta}{k-\ell}}{\binom{m}{k}}. \tag{A2}$$

In this case, the probability of error is given by

$$\begin{aligned}\Pr_m(\text{error}) &= \sum_{k=0}^{m} P(C = k)P(Z = k|C = k)\\ &= \sum_{k=0}^{m} \binom{m}{k} p_c^k (1 - p_c)^{m-k} \frac{\binom{m\,\delta}{\ell}\binom{m-m\,\delta}{k-\ell}}{\binom{m}{k}}\\ &\leqslant \sum_{k=0}^{m} \binom{m}{k} (p_c\delta)^k (1 - p_c)^{m-k},\end{aligned}$$

where we have used the inequality

$$\frac{\binom{m\,\delta}{\ell}\binom{m-m\,\delta}{k-\ell}}{\binom{m}{k}} \leqslant \delta^k, \tag{A3}$$

which can be proven with a straightforward calculation. From the binomial theorem we conclude that for any two inputs

$$\Pr(\text{error})_m \leqslant [1 - p_c(1 - \delta)]^m. \tag{A4}$$

2. Error probability for the protocol in the presence of experimental errors

To bound the probability of error in this case, we consider first the case $x = x'$ and denote by $p_c' \approx p_c + p_{\text{dark}}$ the effective click probability. We then have

$$\begin{aligned}&\Pr(f_0 \leqslant q_E - \Delta_q | x = x')\\ &= \sum_{k=0}^{m} \Pr(C = k) \Pr(f_0 \leqslant q_E - \Delta_q | k, x = x')\\ &= \sum_{k=0}^{m} \binom{m}{k} (p_c')^k (1 - p_c')^{m-k} \Pr\left(\frac{Z}{k} \leqslant q_E - \Delta_q | k, x = x'\right)\\ &\leqslant \sum_{k=0}^{m} \binom{m}{k} \left(e^{-2\Delta_q^2} p_c'\right)^k (1 - p_c')^{m-k}\\ &= \left[1 - p_c'\left(1 - e^{-2\Delta_q^2}\right)\right]^m,\end{aligned}$$

where we have made use of Hoeffding's inequality [34]

$$\Pr\left(\frac{Z}{k} \leqslant q_E - \Delta_q | x = x'\right) \leqslant e^{-2k\Delta_q^2},$$

which holds when Z is hypergeometrically distributed. Since the Hoeffding bound for $\Pr(f_0 \leqslant q_E - \Delta_q | x = x')$ is equal to that of $\Pr(f_0 \geqslant q_D + \Delta_q | x \neq x')$, the bound on the probability of error is the same when the fingerprints are different. Therefore, we can conclude that

$$\Pr_m(\text{error}) \leqslant \left[1 - p_c'\left(1 - e^{-2\Delta_q^2}\right)\right]^m. \tag{A5}$$

[1] A. C.-C. Yao, in *Proceedings of the 11th ACM Symposium on the Theory of Computing* (ACM, New York, 1979), pp. 209–213.

[2] E. Kushilevitz and N. Nisan, *Communication Complexity* (Cambridge University Press, Cambridge, 2006).

[3] G. Brassard, Found. Phys. **33**, 1593 (2003).

[4] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Rev. Mod. Phys. **82**, 665 (2010).

[5] H. Buhrman, R. Cleve, and A. Wigderson, in *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing* (ACM, New York, 1998), pp. 63–68.

[6] R. Raz, in *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing* (ACM, New York, 1999), pp. 358–367.

[7] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis, in *Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing* (ACM, New York, 2004), pp. 128–137.

[8] D. Gavinsky, in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing* (ACM, New York, 2008), pp. 95–102.

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

[10] J. Zhang, X.-H. Bao, T.-Y. Chen, T. Yang, A. Cabello, and J.-W. Pan, Phys. Rev. A **75**, 022302 (2007).

[11] P. Trojek, C. Schmid, M. Bourennane, C. Brukner, M. Żukowski, and H. Weinfurter, Phys. Rev. A **72**, 050305 (2005).

[12] R. T. Horn, S. A. Babichev, K.-P. Marzlin, A. I. Lvovsky, and B. C. Sanders, Phys. Rev. Lett. **95**, 150502 (2005).

[13] A. Ambainis, Algorithmica **16**, 298 (1996).

[14] L. Babai and P. G. Kimmel, in *Proceedings: Twelfth Annual IEEE Conference on Computational Complexity* (IEEE Computer Society, Los Alamitos, 1997), pp. 239–246.

[15] I. Newman and M. Szegedy, in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing* (ACM, New York, 1996), pp. 561–570.

[16] J. Justesen, IEEE Trans. Inf. Theory **18**, 652 (1972).

[17] J. Du, P. Zou, X. Peng, D. K. L. Oi, L. C. Kwek, C. H. Oh, and A. Ekert, Phys. Rev. A **74**, 042319 (2006).

[18] J. N. de Beaudrap, Phys. Rev. A **69**, 022307 (2004).

[19] C. E. Mora, H. J. Briegel, and B. Kraus, Int. J. Quantum Inf. **05**, 729 (2007).

[20] C. E. Mora and H. J. Briegel, Phys. Rev. Lett. **95**, 200503 (2005).

[21] S. Massar, Phys. Rev. A **71**, 012310 (2005).

[22] J. C. Garcia-Escartin and P. Chamorro-Posada, Phys. Rev. A **87**, 052330 (2013).

[23] A. S. Holevo, Probl. Peredachi Inf. **9**, 3 (1973).

[24] D. Gauthier, H. Guilbert, Y. Zhu, M. Shi, K. McCusker, B. Christensen, P. Kwiat, T. Brougham, S. M. Barnett, and V. Chandar, in *Quantum Information and Measurement* (Optical Society of America, Washington, DC, 2012).

[25] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006).

[26] R. Sheldon, *A First Course in Probability*, 6th ed. (Pearson Education, Upper Saddle River, NJ, 2002).

[27] M. Franceschetti, O. Dousse, N. David, and P. Thiran, IEEE Trans. Inf. Theory **53**, 1009 (2007).

[28] C. Fuchs and J. Van De Graaf, IEEE Trans. Inf. Theory **45**, 1216 (1999).

[29] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003).

[30] F. Marsili, V. Verma, J. Stern, S. Harrington, A. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. Shaw, R. Mirin *et al.*, Nat. Photonics **7**, 210 (2013).

[31] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).

[32] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, Nat. Commun. **3**, 1174 (2012).

[33] V. Dunjko, P. Wallden, and E. Andersson, Phys. Rev. Lett. **112**, 040502 (2014).

[34] W. Hoeffding, J. Am. Stat. Assoc. **58**, 13 (1963).