Quantum Fingerprinting Over AWGN Channels With Power-Limited Optical Signals

Michał Lipka, Marcin Jarzyna, and Konrad Banaszek, *Senior Member, IEEE*

***Abstract*— Quantum fingerprinting reduces communication complexity of determination whether two n-bit long inputs are equal or different in the simultaneous message passing model. Here we quantify the advantage of quantum fingerprinting over classical protocols when communication is carried out using optical signals with limited power and unrestricted bandwidth propagating over additive white Gaussian noise (AWGN) channels with power spectral density (PSD) much less than one photon per unit time and unit bandwidth. We identify a noise parameter whose order of magnitude separates near-noiseless quantum fingerprinting, with signal duration effectively independent of n, from a regime where the impact of AWGN is significant. In the latter case the signal duration is found to scale as $O(\sqrt{n})$, analogously to classical fingerprinting. However, the dependence of the signal duration on the AWGN PSD is starkly distinct, leading to quantum advantage in the form of a reduced multiplicative factor in $O(\sqrt{n})$ scaling.**

***Index Terms*— Communication channels, complexity theory, optical signal detection, coherence.**

I. Introduction

EXPLOITING the quantum nature of physical signals used for information transmission enables new functionalities, such as quantum key distribution [1]–[3]. It can also reduce communication complexity of certain distributed information-processing tasks. An example of the latter can be demonstrated in the simultaneous message passing model introduced by Yao [4]. Suppose that two parties, Alice and Bob, receive inputs in the form of n-bit long strings $x, y \in \{0,1\}^n$. While they cannot communicate with each other, they are supposed to use as little communication as possible with a third party, the referee, to facilitate computation of a certain Boolean function $f(x,y)$. In the specific scenario of the equality problem, the function reads

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

which corresponds to a test whether the input strings are equal or different. In order to reduce the amount of information transmitted to the referee, Alice and Bob can send only fingerprints of their inputs at the expense of tolerating a non-zero probability of error. Classically, the fingerprints have the form of bit strings shorter than inputs. If Alice and Bob do not have access to shared randomness, the fingerprints must be at least $O(\sqrt{n})$ bits long for an arbitrarily low probability of error [5]–[7]. On the other hand, when quantum states are used to carry fingerprints, it is sufficient that Alice and Bob communicate to the referee $O(\log_2 n)$ qubits [8]–[12]. Because according to Holevo's theorem [13], [14] a qubit can carry at most one bit of classical information, this presents a scaling advantage over classical fingerprinting. A key ingredient to attain this advantage is joint detection of quantum signals received from Alice and Bob by the referee.

Interestingly, quantum fingerprints can be efficiently generated as trains of coherent states of light with joint detection implemented using optical interference and photon counting [15], [16]. Coherent states are routinely used in conventional optical communication, which facilitated recent experimental proof-of-principle demonstrations of quantum fingerprinting [17], [18]. This naturally leads to a question about the advantage of quantum fingerprinting over its classical counterpart in terms of physical resources required to transmit optical signals carrying fingerprints rather than by the number of bits or qubits that need to be communicated.

This paper presents an analysis of quantum fingerprinting when optical signals sent from Alice and Bob to the referee are power-limited, but no restrictions on their bandwidth are in place. Our model includes contribution from background radiation described by additive white gaussian noise (AWGN). Motivated by recent studies of photon-starved communication [19]–[21], we consider regime when the noise power spectral density (PSD) ν expressed in photons per unit time per unit bandwidth is much less than one. The principal objective is to minimize the signal duration, which defines the transmission time required to execute the protocol. We show that because the impact of AWGN becomes more severe with increasing signal bandwidth, there exists an optimal operating point that is determined by a combination of the input length n, the noise PSD ν and the desired probability of error ε which is not to be exceeded when executing the protocol.

The obtained results are compared with a scenario when classical fingerprints are transmitted from Alice and Bob to the referee over optical channels with matching signal power and AWGN strength. This allows us to express quantum advantage in terms of reduction of the signal duration. We find that the performance of the quantum fingerprinting protocol

Manuscript received July 15, 2019; revised December 15, 2019; accepted January 6, 2020. Date of publication January 23, 2020; date of current version April 3, 2020. This work is a part of the "Quantum Optical Technologies" project carried out within the International Research Agendas programme of the Foundation for Polish Science co-financed by the European Union under the European Regional Development Fund. *(Corresponding author: Michał Lipka.)*

Michał Lipka and Konrad Banaszek are with the Centre for Quantum Optical Technologies, Centre of New Technologies, University of Warsaw, 02-097 Warsaw, Poland, and also with the Faculty of Physics, University of Warsaw, 02-093 Warsaw, Poland (e-mail: m.lipka@cent.uw.edu.pl).

Marcin Jarzyna is with the Centre for Quantum Optical Technologies, Centre of New Technologies, University of Warsaw, 02-097 Warsaw, Poland.

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSAC.2020.2968996

changes qualitatively with increasing input size n. When $n \ll 2\nu^{-1}\log[1/(2\varepsilon)]$, the effects of channel AWGN are insignificant and one remains close to the noiseless regime analyzed in [15]. On the other hand, for sufficiently long inputs, when $n \gg 2\nu^{-1}\log[1/(2\varepsilon)]$, the transmission time for quantum fingerprints scales as $O(\sqrt{n})$, which is the same as in the classical scenario. However, the proportionality constant has a starkly distinct dependence on the noise PSD ν. While in the classical scenario the noise PSD enters through a multiplicative factor $[\log_2(1+\nu^{-1})]^{-1}$, which follows directly from the Holevo capacity of an AWGN channel [22], [23], in the case of quantum fingerprinting the dependence is of the form $\sqrt{\nu}$. This difference becomes substantial for ν many orders below one photon per unit time and unit bandwidth, as is the case e.g. in space optical communication links [24].

This paper is organized as follows. Sec. II describes the optical layer of quantum fingerprinting based on coherent states of light. The complete quantum fingerprinting protocol is described in Sec. III for the noiseless case, and in Sec. IV for a general AWGN scenario using the framework of hypothesis testing. Optimization of the operating point is discussed in Sec. V. Sec. VI compares the performance of optimized quantum fingerprinting with classical protocols. Finally, Sec. VII concludes the paper.

II. Optical Layer

Let us start with the description of the optical layer of the quantum fingerprinting protocol using coherent states proposed by Arrazola and Lütkenhaus [15]. Alice and Bob use phase shift keying (PSK) to generate optical signals sent to the referee. As shown in Fig. 1, each of the two signals is a train of L optical pulses occupying consecutive temporal slots. A single pulse will be represented by a normalized mode function $u(s)$ parameterized with dimensionless time s. It is assumed that the mode function is orthogonal to its replica displaced by any integer number l of temporal slots:

$$\int_{-\infty}^{\infty} ds\, u^*(s-l)u(s) = \delta_{0l}, \quad l = \dots,-1,0,1,\dots \tag{2}$$

For a modulation bandwidth B, the duration of a single slot is equal to $1/B$ and the physical time is $t = s/B$. Hence the overall duration of each of the signals is L/B. Note that in general the signal spectral support can exceed B [25].

We will assume that the optical receiver used by the referee accepts only temporal modes matching those in the generated signals. Such selectivity can be achieved without any signal loss using the technique of quantum pulse gating [26]–[29]. In this case, the optical fields $\mathcal{E}^x(t)$ and $\mathcal{E}^y(t)$ received by the referee respectively from Alice and Bob can be described by

$$\mathcal{E}^z(t) = \sqrt{B}\sum_{l=1}^{L}\alpha_l^z u(Bt-l), \quad z = x, y. \tag{3}$$

Individual pulses are phase modulated by Alice and Bob according to L-tuples $\boldsymbol{\theta}^z = (\theta_1^z, \dots, \theta_L^z)$, $z = x, y$, that depend on the input strings x and y. The map $z \mapsto \boldsymbol{\theta}^z$ will be specified in Sec. III. The complex amplitudes α_l^x and α_l^y in (3) read

$$\alpha_l^x = \sqrt{\frac{S}{B}}e^{i\theta_l^x} + \xi_l, \quad \alpha_l^y = \sqrt{\frac{S}{B}}e^{i\theta_l^y} + \zeta_l, \tag{4}$$

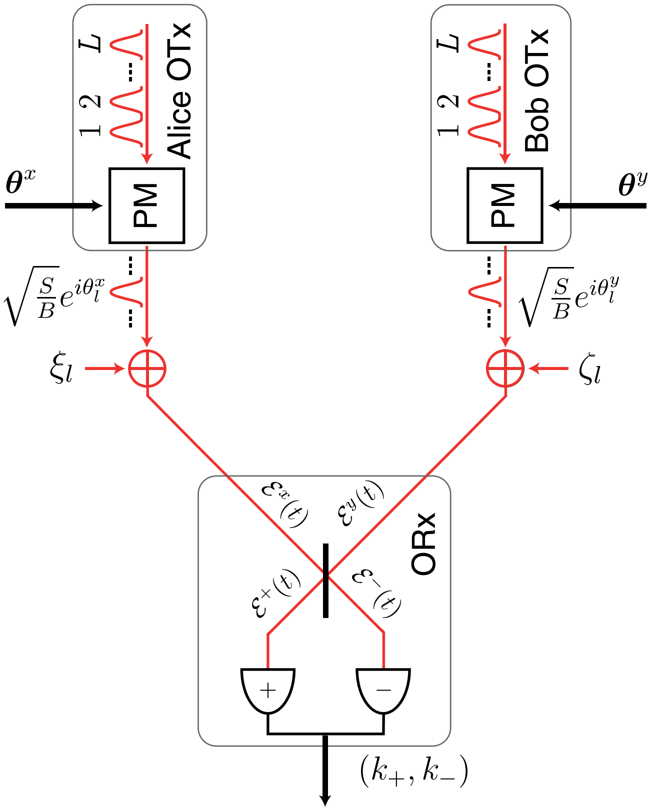


Fig. 1. Optical layer of the quantum fingerprinting protocol. Alice and Bob use optical transmitters OTx which imprint phase L-tuples $\boldsymbol{\theta}^z = (\theta_1^z, \dots, \theta_L^z)$ depending on inputs $z = x, y$ onto trains of L light pulses using phase modulators PM. In the course of propagation, individual pulse amplitudes acquire random AWGN components ξ_l and ζ_l. The optical receiver ORx used by the referee combines the received signals, described by time-dependent fields $\mathcal{E}^x(t)$ and $\mathcal{E}^y(t)$, on a balanced 50/50 beam splitter which produces superpositions $\mathcal{E}^\pm(t) = [\mathcal{E}^x(t) \pm \mathcal{E}^y(t)]/\sqrt{2}$. The output ports of the beam splitter are monitored by photon counting detectors which yield the total photocount numbers k_+ and k_- registered over the signal duration.

where S is the optical power, in photons per unit time, of the signal received from either Alice or Bob. Linear attenuation of the signal amplitude in the course of propagation can be taken into account in a straightforward manner by rescaling S. The complex variables ξ_l and ζ_l describe contributions from AWGN acquired by the signals and will be assumed to have equal variance

$$\mathrm{Var}[\xi_l] = \mathrm{Var}[\zeta_l] = \nu \tag{5}$$

that specifies noise PSD expressed in photons per unit time per unit bandwidth. Because broadband noise is assumed, its contribution to field amplitudes α_l^z in (4) is independent of the modulation bandwidth B.

The referee brings the received optical signals to interfere on a balanced $50/50$ beam splitter. The fields $\mathcal{E}^+(t)$ and $\mathcal{E}^-(t)$ at the two ± output ports of the beam splitter, described by superpositions

$$\mathcal{E}^\pm(t) = \frac{1}{\sqrt{2}}[\mathcal{E}^x(t) \pm \mathcal{E}^y(t)], \tag{6}$$

are subsequently measured by a pair of photon counting detectors that return the total numbers of photocounts k_+ and

k_- registered over the entire signal duration. According to the semiclassical theory of photodetection [23], [30], the probability distribution for the pair (k_+, k_-) reads

$$p(k_+, k_-) = \mathbb{E}\left[e^{-I_+} \frac{I_+^{k_+}}{k_+!} e^{-I_-} \frac{I_-^{k_-}}{k_-!} \right], \tag{7}$$

where

$$I_\pm = \int_{-\infty}^{\infty} dt \, |\mathcal{E}^\pm(t)|^2 \tag{8}$$

is the total optical energy incident on an individual detector over the signal duration and the expectation value $\mathbb{E}[\ldots]$ is calculated over all AWGN variables ξ_l and ζ_l, $l = 1, \ldots, L$. The characteristic function for the probability distribution $p(k_+, k_-)$ reads

$$\begin{aligned} Z(\lambda_+, \lambda_-) &= \sum_{k_+, k_- = 0}^{\infty} e^{i\lambda_+ k_+ + i\lambda_- k_-} p(k_+, k_-) \\ &= \mathbb{E}\left[\exp\left((e^{i\lambda_+} - 1)I_+ + (e^{i\lambda_-} - 1)I_-\right)\right]. \end{aligned} \tag{9}$$

The analysis will be carried out for $\nu \ll 1$. Further, terms of the order $O(\nu L S/B)$ and higher will be neglected. As shown in Appendix A, under these assumptions the characteristic function after averaging over the noise variables can be recast as

$$\begin{aligned} Z(\lambda_+, \lambda_-) &= \exp[(e^{i\lambda_+} - 1)\mu(1 + V)] \\ &\quad \times \exp[(e^{i\lambda_-} - 1)\mu(1 - V)], \end{aligned} \tag{10}$$

where

$$\mu = L(S/B + \nu) \tag{11}$$

is the total number of photocounts generated on both the detectors by the noisy signal coming from one sender, and

$$V = \frac{1}{L(1 + B\nu/S)} \sum_{l=1}^{L} \cos(\theta_l^x - \theta_l^y). \tag{12}$$

has the physical interpretation of interference visibility. The characteristic function derived in (10) indicates Poissonian distributions for the photocount numbers $k_\pm$ with respective means $\mu(1 \pm V)$:

$$\begin{aligned} p(k_+, k_- | V) &= e^{-\mu(1+V)} \frac{[\mu(1+V)]^{k_+}}{k_+!} \\ &\quad \times e^{-\mu(1-V)} \frac{[\mu(1-V)]^{k_-}}{k_-!}. \end{aligned} \tag{13}$$

We have written explicitly the conditional dependence of the photocount statistics on the visibility V, as this parameter contains information about the relation between the inputs x and y. The pair of photocount numbers (k_+, k_-) produced by the detectors serves as the basis for testing by the referee whether the input strings x and y are different or equal.

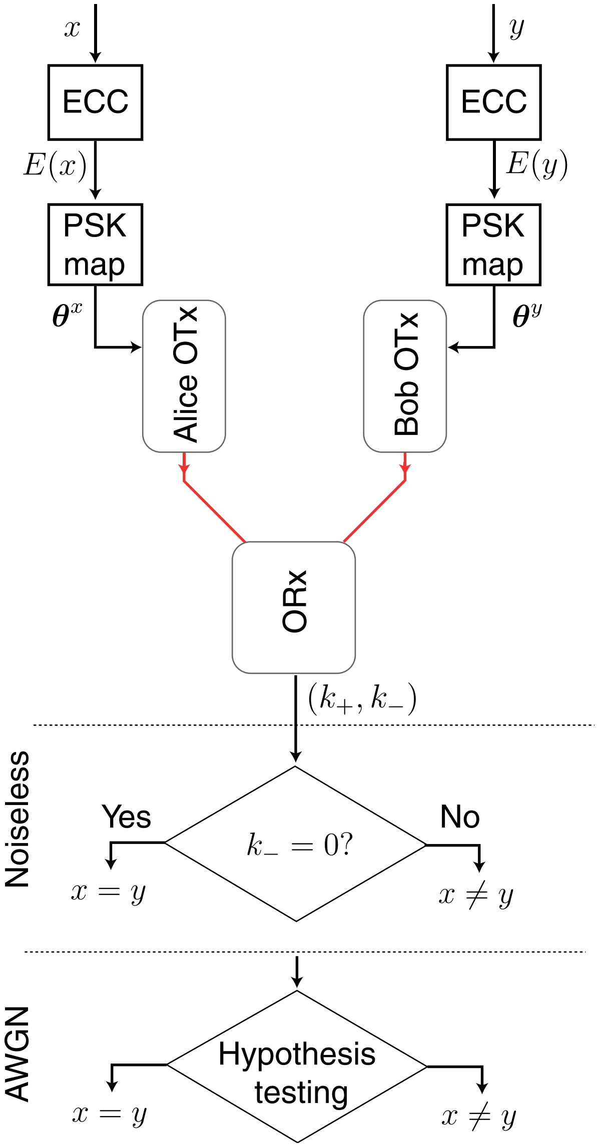


Fig. 2. Complete implementation of the quantum fingerprinting protocol based on coherent states of light. Inputs x and y are mapped onto codewords $E(x)$ and $E(y)$ using an error correcting code ECC. The codewords define via a PSK map phase L-tuples $\boldsymbol{\theta}^x$ and $\boldsymbol{\theta}^y$ that feed into optical transmitters OTx. The optical receiver ORx produces a pair of integers k_+, k_- that serves as the basis for the equality test. In the noiseless case the test has the form of a check whether $k_- = 0$ or not, whereas in the presence of noise a more complex test described in Sec. IV is required.

III. Noiseless Scenario

The optical layer described in the preceding section is used to implement the quantum fingerprinting protocol as shown in Fig. 2. The inputs x and y are mapped onto phase L-tuples $\boldsymbol{\theta}^x$ and $\boldsymbol{\theta}^y$ that define modulation of signals generated by Alice and Bob using optical transmitters OTx. Joint detection of these signals with an optical receiver ORx returns a pair of integers (k_+, k_-) that is used by the referee to infer the value of the equality function defined in (1).

We will begin with a discussion of a simplified scenario when there is no background noise, $\nu = 0$. In order to gain intuition about the workings of the fingerprinting protocol, suppose for a moment that the binary input strings x and y of length n are used directly to generate optical signals composed of $L = n$ pulses using a binary PSK map. In this setting, the two bit values $z_l = 0, 1$ are mapped onto phases $\theta_l^z = \pi z_l$, where z stands for x or y and $l = 1, \ldots, n$. For equal inputs, $x = y$, the two signals are identical, completely destructive interference occurs at the '$-$' output port of the beam splitter, and $\mathcal{E}^-(t) = 0$ over the entire signal duration given absence of background noise. As a result, no photocounts can be registered by the detector monitoring the '$-$' port and $k_- = 0$. Conversely, registering $k_- \geq 1$ photocounts heralds unambiguously that the inputs were different, $x \neq y$, as in this case $\mathcal{E}^-(t)$ is not identically equal to zero. However, because photon counting is a Poissonian process, it may happen that different strings will not produce any counts on the detector monitoring the '$-$' port. According to (13) the probability of such an event is $p(k_- = 0) = \exp[-\mu(1-V)]$. In the worst-case scenario, when the input strings differ at just one location, the visibility calculated according to (12) reads $V = 1 - 2/n$ and $p(k_- = 0) = \exp(-2S/B)$. In order to keep this probability below a desired level, one would need to maintain sufficiently high ratio S/B which specifies the mean photon number per temporal slot. For power-limited signals this would imply an upper bound on the bandwidth B. Consequently, the entire signal duration given by $L/B = n/B$ would scale linearly with n.

Quantum fingerprinting offers dramatically improved performance compared to the simple scenario described above by using an error correcting code (ECC) to define the map $z \mapsto \boldsymbol{\theta}^z$, $z = x, y$ and exploiting bandwidth as a free resource. Specifically, consider a binary ECC $E : \{0,1\}^n \rightarrow \{0,1\}^m$, which guarantees that any two different inputs $x \neq y$ are mapped onto codewords $E(x)$ and $E(y)$ for which the Hamming distance satisfies

$$D\big(E(x), E(y)\big) = \sum_{j=1}^{m} E_j(x) \oplus E_j(y) \geq m\delta. \tag{14}$$

Here $\delta \in [0, 1/2[$ is a constant specifying the minimum relative Hamming distance between any two different codewords. It will be assumed that the ECC E operates at the asymptotic Gilbert-Varshamov bound given by [31]

$$\frac{n}{m} = r(\delta) = 1 - H_2(\delta), \tag{15}$$

where $H_2(x) = -x \log_2 x - (1-x)\log_2(1-x)$ is the binary entropy. There exist efficient ECCs operating close to the Gilbert-Varshamov bound, such as the random Toeplitz matrix ECC employed in a recent experimental demonstration of quantum fingerprinting [18].

The codewords $E(x)$ and $E(y)$ are mapped onto L-tuples of phases $\boldsymbol{\theta}^x$ and $\boldsymbol{\theta}^y$ that are used to modulate optical signals. We shall take $L = m/2$ and employ a quadrature PSK map so that an individual phase depends on a block of two consecutive codeword bits according to

$$\theta_l^z = \pi E_{2l-1}(z) + \frac{\pi}{2}[E_{2l-1}(z) \oplus E_{2l}(z)], \quad z = x, y, \tag{16}$$

where $l = 1, \ldots, L = m/2$. Compared to binary PSK, quadrature PSK allows for a two-fold reduction of the pulse train length without altering otherwise the performance of the protocol [16]. This would no longer be the case for higher PSK constellations. Calculation of the interference visibility (12) is aided by the following straightforward observation:

$$\cos(\theta_l^x - \theta_l^y) = 1 - E_{2l-1}(x) \oplus E_{2l-1}(y) - E_{2l}(x) \oplus E_{2l}(y). \tag{17}$$

Assuming absence of noise, one obtains:

$$\begin{aligned} V &= \frac{1}{L}\sum_{l=1}^{L} \cos(\theta_l^x - \theta_l^y) = 1 - \frac{2}{m}\sum_{j=1}^{m} E_j(x) \oplus E_j(y) \\ &= 1 - \frac{2}{m} D\big(E(x), E(y)\big) \leq 1 - 2\delta, \end{aligned} \tag{18}$$

where in the last step (14) has been used. The probability of obtaining $k_- = 0$ for different inputs, $x \neq y$, is consequently upper bounded by $\exp(-2\delta LS/B)$. Given that L/B specifies the signal duration, it is now possible to execute the quantum optical fingerprinting protocol in a constant time by increasing the modulation bandwidth in line with L which grows with the input size n as $L = n/[2r(\delta)]$. Without any bandwidth limitations, it is optimal to approach $\delta \rightarrow 1/2$. In this limit the code rate $r(\delta) \rightarrow 0$ and the number of temporal slots $L \rightarrow \infty$. With unlimited bandwidth these slots can be accommodated in a constant time L/B.

It is worth noting that the ECC is used in quantum fingerprinting *not* to ensure faithful recovery of the messages fed into the communication channel, but rather to augment differences between received optical signals in order to guarantee sufficiently low interference visibility when $x \neq y$ which results in photocounts on the '$-$' detector.

IV. Hypothesis Testing

In the remainder of the paper, the fingerprinting protocol will be required to operate at or below a desired average probability of error ε for the equality test, assuming equiprobable hypotheses of equal and different inputs, and considering for the latter hypothesis the worst-case scenario of the minimum relative Hamming distance δ between the codewords. The objective will be to minimize the overall duration of signals sent by Alice and Bob given by L/B. For a fixed signal power S, the signal duration can be equivalently characterized by the signal optical energy expressed as the mean photon number received from Alice or Bob that is equal to $N_Q = SL/B$. In the noiseless case discussed in the preceding section, assuming unlimited bandwidth and taking $\delta \rightarrow 1/2$ yields the average probability of error equal to $\varepsilon = \exp(-N_Q)/2$, which can be recast as:

$$N_Q = \log[1/(2\varepsilon)], \qquad \nu = 0. \tag{19}$$

This expression is independent of the input length n implying constant signal duration. As expected, a lower probability of error requires higher photon number or, equivalently for power-limited signals, longer transmission time.

The above analysis becomes much more nuanced when background noise is present. First, the simple test based on whether $k_- = 0$ or not no longer guarantees minimum probability of error. Second, while in the noiseless case there was no penalty for increasing the bandwidth in order to accommodate more temporal slots within a constant transmission time, higher bandwidth boosts the AWGN contribution to the received signals, which may make the equality test based on interference visibility increasingly more difficult.

In the general scenario with background noise, the visibilities corresponding to hypotheses of equal and different inputs, assuming for the latter the worst-case scenario with the minimum relative Hamming distance δ, are given respectively by

$$V_e = \frac{1}{1 + B\nu/S}, \qquad V_d = \frac{1-2\delta}{1 + B\nu/S}. \tag{20}$$

The referee needs to decide whether the pair of integers (k_+, k_-) produced by the joint detection of optical signals received from Alice and Bob was generated by the probability distribution $p_e(k_+, k_-|V_e)$ or $p_d(k_+, k_-|V_d)$. We will use the Neyman-Pearson criterion for *a priori* equiprobable hypotheses, which yields the decision rule

$$\begin{aligned} p(k_+, k_-|V_e) > p(k_+, k_-|V_d): &\quad x = y \\ p(k_+, k_-|V_e) < p(k_+, k_-|V_d): &\quad x \neq y \end{aligned}$$

and a random draw when $p(k_+, k_-|V_e) = p(k_+, k_-|V_d)$. The probability of error for such a test is upper bounded by the Chernoff bound [32]

$$\varepsilon \leq \frac{1}{2}\exp[-C(V_e, V_d; \mu)], \tag{21}$$

where $C(V_e, V_d; \mu)$ is Chernoff information given by

$$C(V_e, V_d; \mu) = -\min_{0\leq\lambda\leq 1} \log\left\{ \sum_{k_+, k_-=0}^{\infty} [p(k_+, k_-|V_e)]^\lambda \right. \\ \left. \times [p(k_+, k_-|V_d)]^{1-\lambda} \right\}. \tag{22}$$

As specified in (13), the joint probability distributions $p(k_+, k_-|V_e)$ and $p(k_+, k_-|V_d)$ are products of Poissonian distributions with respective means $\mu(1 \pm V_e)$ and $\mu(1 \pm V_d)$. In such a case, Chernoff information is proportional to the total photocount number 2μ,

$$C(V_e, V_d; \mu) = 2\mu \mathsf{C}(V_e, V_d). \tag{23}$$

The multiplicative factor $\mathsf{C}(V_e, V_d)$ can be interpreted as *Chernoff information per count* and is given by the expression

$$\mathsf{C}(V_e, V_d) = 1 - \frac{1}{2}\min_{0\leq\lambda\leq 1}[(1+V_e)^\lambda(1+V_d)^{1-\lambda} \\ +(1-V_e)^\lambda(1-V_d)^{1-\lambda}]. \tag{24}$$

Fig. 3 depicts $\mathsf{C}(V_e, V_d)$ as a function of visibilities V_e and V_d for $0 \leq V_e, V_d \leq 1$. In this range, Chernoff information per count attains maximum at $\mathsf{C}(1, 0) = \mathsf{C}(0, 1) = 1/2$ and becomes zero for equal arguments. It will be useful to note that for a fixed V_e, $\mathsf{C}(V_e, V_d)$ is a decreasing function on an interval $V_d \in [0, V_e]$. The intuition behind this is that the closer V_d becomes to V_e, the more difficult it is to discriminate between the two visibilities based on the photocount statistics.

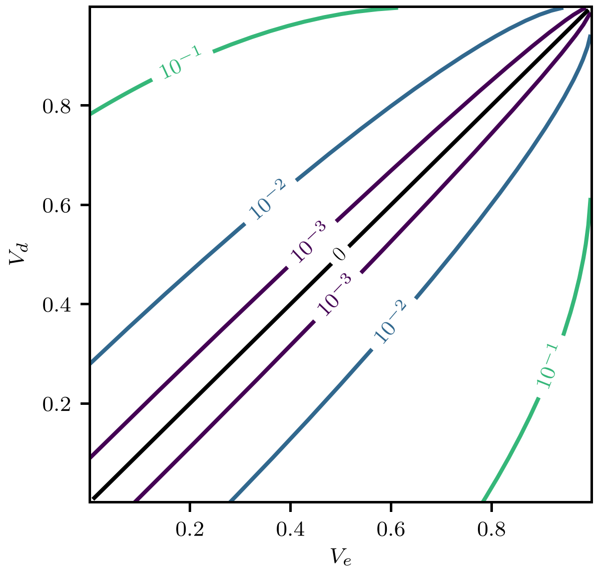


Fig. 3. Chernoff information per count $\mathsf{C}(V_e, V_d)$ as a function of interference visibilities V_e and V_d corresponding respectively to hypotheses of equal and different inputs.

As derived in Appendix B, for $V_e, V_d \ll 1$ the Chernoff information per count is well approximated by the expression

$$\mathsf{C}(V_e, V_d) \approx \frac{1}{8}(V_e - V_d)^2. \tag{25}$$

This simple formula will greatly simplify the analysis of the performance of the quantum fingerprinting protocol in the limit of large input size n.

V. Optimization

The task now is to identify the operating point achieving the minimum transmission time equal to L/B or equivalently—owing to the power constraint—the number of signal photons $N_Q = SL/B$ that need to be received by the referee from Alice and Bob. The operating point depends on the input bit string length n, the noise strength ν and the desired average probability of error ε which is not to be exceeded. It will be convenient to use as independent variables in the optimization problem the minimum relative Hamming distance δ of the ECC used in the protocol and the rescaled bandwidth

$$\beta = \frac{B\nu}{S}. \tag{26}$$

Note that the inverse β^{-1} specifies the signal-to-noise ratio. The range of the variables is $0 \leq \delta < 1/2$ and $\beta > 0$.

Transforming the Chernoff bound (21) with the help of definitions (11), (20), and (23) implies that the photon number

$$N_Q \geq \frac{\log[1/(2\varepsilon)]}{2(1+\beta)\mathsf{C}\left(\frac{1}{1+\beta}, \frac{1-2\delta}{1+\beta}\right)} \tag{27}$$

is sufficient to ensure operation below a desired error probability ε. At the same time, the transmission time must be sufficiently long to accommodate $L = n/[2r(\delta)]$ temporal slots each of duration $1/B = \nu/(\beta S)$. This condition translated for the number of received signal photons yields the inequality

$$N_Q \geq \frac{SL}{B} = \frac{n\nu/2}{\beta r(\delta)}. \tag{28}$$

For a fixed β the expressions on the right hand sides of (27) and (28) exhibit opposite monotonicity as functions of δ over the interval $0 \leq \delta < 1/2$. This is because in (27), Chernoff information per count $\mathsf{C}\left(\frac{1}{1+\beta}, \frac{1-2\delta}{1+\beta}\right)$ is monotonically increasing in δ as noted in Sec. IV, while the code rate $r(\delta)$ in the denominator of (28) is monotonically decreasing in δ. Consequently, if one seeks minimum N_Q that satisfies both inequalities (27) and (28), it is sufficient to consider the case when the expressions on the right hand sides of these inequalities are equal to each other. This yields an implicit relation between β and δ in the form

$$\frac{\beta r(\delta)}{2(1+\beta)\mathsf{C}\left(\frac{1}{1+\beta}, \frac{1-2\delta}{1+\beta}\right)} = \mathcal{N}, \tag{29}$$

where

$$\mathcal{N} = \frac{n\nu/2}{\log[1/(2\varepsilon)]}. \tag{30}$$

The ratio defined in (30) admits a simple interpretation. The enumerator is the total number of noise photons if the inputs were mapped onto quadrature PSK signals without an ECC. The denominator is the number of signal photons required to implement the quantum fingerprinting protocol for the desired probability of error ε in the noiseless scenario. Hence $\mathcal{N}$ can serve as a simple estimate of how severely the background noise would impact the protocol designed for the noiseless case. In the following we will refer to $\mathcal{N}$ as the *noise parameter*.

Equation (29) provides a relation between β and δ that can be used to reduce the number of independent optimization variables to one and to find the optimum operating point by minimizing the right hand side of either (27) or (28) over the remaining variable. Fig. 4 depicts numerically found optimal δ^* and the corresponding β^* as a function of the noise parameter $\mathcal{N}$. Two operating regimes can be identified depending on the order of magnitude of $\mathcal{N}$. When $\mathcal{N} \ll 1$ it is possible to attain $\delta^* \approx 1/2$ and $\beta^* \ll 1$. This corresponds to large ECC expansion with the code rate approaching $r(\delta^*) \approx 0$, as shown in Fig. 4(a). In this regime the minimum photon number N_Q^* can be conveniently calculated using the right hand side of (27) as a product of $\log[1/(2\varepsilon)]$ and a factor $1/\left[2(1+\beta^*)\mathsf{C}\left(\frac{1}{1+\beta^*}, \frac{1-2\delta^*}{1+\beta^*}\right)\right]$, plotted in Fig. 4(b). For $\mathcal{N} \leq 10^{-1}$ this factor remains between 1 and 6.6. Thus the fingerprinting protocol requires transmission time that depends primarily on the desired probability of error and the minimum number of signal photons

$$N_Q^* \approx \log[1/(2\varepsilon)], \qquad \mathcal{N} \ll 1. \tag{31}$$

is within one order of magnitude the same as in the noiseless scenario.

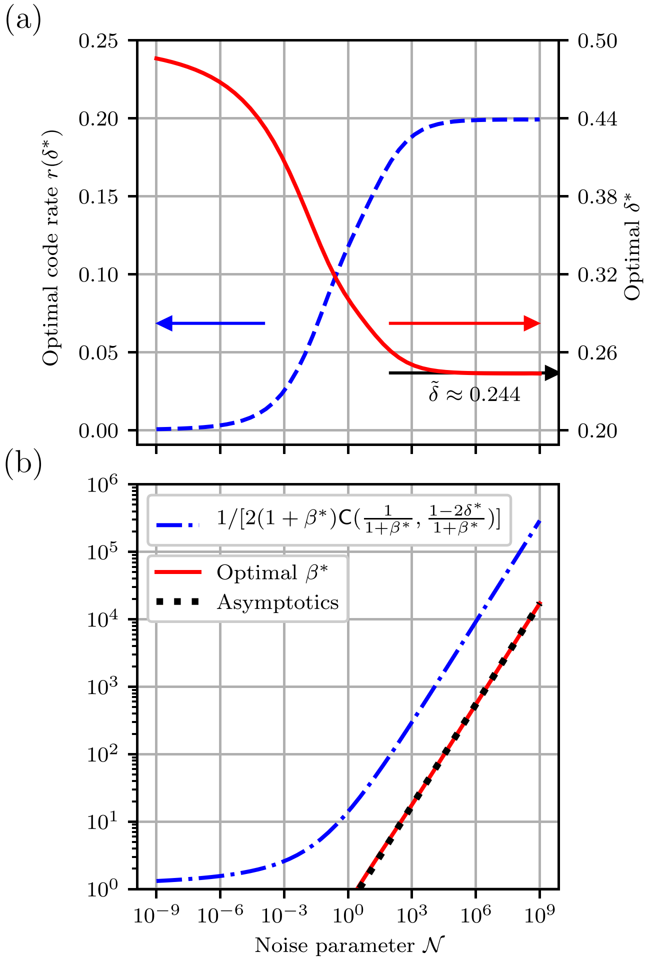


Fig. 4. (a) Optimal Hamming distance δ^* (solid line, right scale) and the corresponding code rate $r(\delta^*)$ (dashed line, left scale) minimizing the signal duration, or equivalently the signal photon number, as a function of the noise parameter $\mathcal{N}$ defined in (30). (b) Optimal rescaled bandwidth β^* (solid line) compared with the asymptotic expression (dotted line) derived in (33). The dash-dotted line depicts the proportionality factor between the minimum signal photon number and $\log_2[1/(2\varepsilon)]$, where ε is the desired average probability of error.

Fig. 4(b) indicates that in the opposite regime, when $\mathcal{N} \gg 1$, the rescaled bandwidth becomes $\beta \gg 1$, which corresponds to low signal-to-noise ratio. This allows one to apply the low-visibility approximation of the Chernoff information per count according to (25). This approximation expressed in presently used variables takes the form:

$$\mathsf{C}\left(\frac{1}{1+\beta}, \frac{1-2\delta}{1+\beta}\right) \approx \frac{\delta^2}{2(1+\beta)^2}. \tag{32}$$

Using the above closed formula in (29) and solving it with respect to β yields $\beta = \sqrt{\mathcal{N}\delta^2/r(\delta) + 1/4} - 1/2 \approx \sqrt{\mathcal{N}\delta^2/r(\delta)}$, where the second approximate expression can be applied when $\beta \gg 1$. Inserting the latter expression for β into the right hand side of (28) yields $n\nu/[2\sqrt{\mathcal{N}\delta^2\ r(\delta)}]$ that needs to be optimized over δ. The product $\delta^2\ r(\delta)$ appearing in the denominator has a single maximum over the interval $0 \leq \delta < 1/2$ at the argument whose numerically found value is equal to $\tilde{\delta} \approx 0.244$. As seen in Fig. 4(a), this value agrees very well with the results of numerical optimization for $\mathcal{N} \gg 1$. Consequently, one can take

$$\beta^* \approx \sqrt{\mathcal{N}\tilde{\delta}^2/r(\tilde{\delta})}, \qquad \mathcal{N} \gg 1, \tag{33}$$

and express the minimum photon number using the right hand side of (28) as:

$$N_Q^* \approx 6.51\sqrt{n\nu \log[1/(2\varepsilon)]}, \qquad \mathcal{N} \gg 1, \tag{34}$$

where the numerical multiplicative factor is given by the inverse of $\sqrt{2\tilde{\delta}^2\ r(\tilde{\delta})} \approx 0.154$.

VI. Comparison

The performance of the optimized quantum fingerprinting protocol can be compared directly with a scenario when optical channels are used to transmit classical fingerprints of inputs x and y. Based on results obtained by Babai and Kimmel [7] one can specify a classical protocol that uses fingerprints of length

$$I_C = 2\sqrt{n}\left[\frac{1}{2}\log_2\frac{1}{\varepsilon}\right] \tag{35}$$

bits each. It is also possible to devise a lower bound on the classical fingerprint length in the form [18]

$$I_B = \sqrt{\frac{n}{2\log 2}}\left(\frac{1}{2} - \sqrt{\varepsilon}\right) - \frac{1}{2}. \tag{36}$$

It is worth noting that I_B retains $O(\sqrt{n})$ scaling in the limit $\varepsilon \to 0$, which suggests that this bound is not tight. When the desired probability of error is equal to zero, it should be necessary to transmit entire inputs, leading to a breakdown of $O(\sqrt{n})$ scaling. This is the case of I_C defined in (35).

The maximum attainable rate R in bits per unit time for transmission of classical information over an AWGN channel, allowing for the most general detection strategies, follows from the Holevo capacity and is given by [22]

$$R = B[g(S/B + \nu) - g(\nu)], \tag{37}$$

where

$$g(x) = (x+1)\log_2(x+1) - x\log_2 x \tag{38}$$

is the entropy of a thermal state of a quantized harmonic oscillator with the mean number of excitations equal to x. For a given signal power S and noise PSD ν the information rate is maximized in the limit $B \to \infty$. The first term in (37) can be then expanded around ν up to the first order in S/B. This yields $R = Sg'(\nu)$, where $g'(x) = \log_2(1 + x^{-1})$ is the first derivative of $g(x)$. The coefficient $g'(\nu)$ has the interpretation of photon information efficiency (PIE), which specifies how many bits of information can be encoded in one photon [21], [33]. Consequently, I_C and I_B defined respectively in (35) and (36) divided by PIE characterize the performance of classical fingerprinting in terms of total photon numbers carried by optical signals sent from Alice and Bob to the referee. Specifically,

$$N_C = \frac{I_C}{\log_2(1+\nu^{-1})} = \frac{2\sqrt{n}}{\log_2(1+\nu^{-1})}\left[\frac{1}{2}\log_2\frac{1}{\varepsilon}\right] \tag{39}$$

is sufficient to implement a constructive classical fingerprinting protocol, and

$$\begin{aligned} N_B &= \frac{I_B}{\log_2(1+\nu^{-1})} \\ &= \frac{1}{\log_2(1+\nu^{-1})}\left[\sqrt{\frac{n}{2\log 2}}\left(\frac{1}{2} - \sqrt{\varepsilon}\right) - \frac{1}{2}\right] \end{aligned} \tag{40}$$

defines a lower bound on the total signal photon number required by any classical fingerprinting protocol.

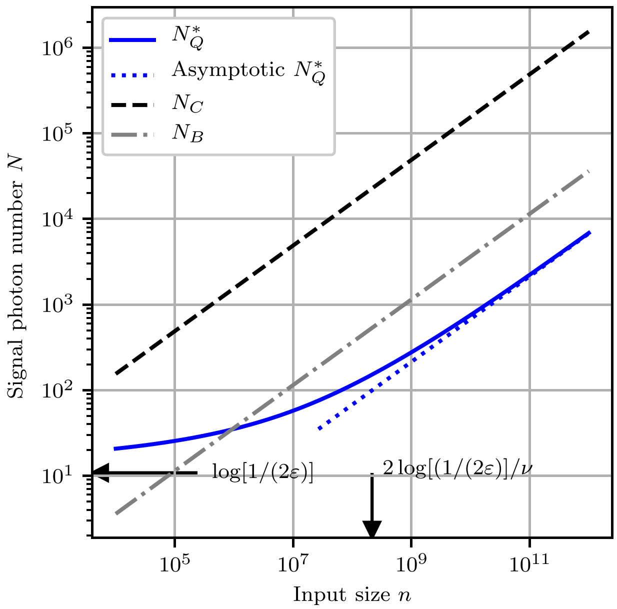


Fig. 5. The minimum signal photon number N_Q^* required by the quantum fingerprinting protocol (solid line) as a function of the input size n for the noise PSD $\nu = 10^{-7}$ and the desired average error probability $\varepsilon = 10^{-5}$. The horizontal arrow indicates the minimum signal photon number in the noiseless scenario and the vertical arrow corresponds to the noise parameter value $\mathcal{N} = 1$. The dotted line is the asymptotic expression given in (34). The dashed line depicts the performance of a classical fingerprinting protocol specified in (39) and the dash-dotted line indicates the known classical bound given by (40).

Fig. 5 compares N_C and N_B specified above with the numerically found minimum photon number N_Q^* used by the quantum fingeprinting protocol for the input size n in the range $10^4 \leq n \leq 10^{12}$, the desired probability of error $\varepsilon = 10^{-5}$, and the noise PSD $\nu = 10^{-7}$ photons per unit time and unit bandwidth. The noise parameter $\mathcal{N}$ defined in (30) becomes equal to one for $n = 2\nu^{-1}\log[1/(2\varepsilon)] \approx 2.2 \times 10^8$. It is seen that below this threshold N_Q^* exhibits weak dependence on n, staying within factor of 20 from the noiseless figure given according to (19) by $\log[1/(2\varepsilon)] \approx 10.8$ photons. Well above the threshold corresponding to $\mathcal{N} = 1$, the signal photon number N_Q follows $O(\sqrt{n})$ scaling with the asymptotic expression (34) that approximates well numerical results as seen in Fig. 5. In this regime the quantum advantage has the form of a reduced multiplicative factor compared to (39) and (40). The principal reason behind this reduction is distinct dependence on the AWGN strength ν: the factor $1/\log_2(1 + \nu^{-1})$, corresponding to the inverse of the PIE, is replaced by $\sqrt{\nu}$ in the quantum case. In the numerical example considered here with $\nu = 10^{-7}$ the ratio between these two factors exceeds two orders of magnitude and it would grow further for lower ν.

VII. Conclusion

We have presented a theoretical analysis of a quantum fingerprinting protocol using power-limited optical signals transmitted over AWGN channels with noise strength much less than one photon per unit time and unit bandwidth. Although for large input size no scaling advantage over classical fingerprinting is retained, the quantum protocol allows one to shorten the transmission time by a multiplicative factor that depends on the noise strength. The improvement offered by quantum fingerprinting is rooted in the joint detection of the received signals. Statistics provided by such detection allows one to perform the equality test more efficiently compared to a scenario when classical fingerprints need to be recovered faithfully after signal detection. The advantage of the quantum fingerprinting protocol over the classical one can be also phrased in terms of the amount of information about the input bit strings revealed to the referee by Alice and Bob [15].

It is worth noting that joint detection used in quantum fingerprinting exploits both wave and particle properties of light: the received optical fields interfere as waves on the beam splitter, but subsequently produce discrete photocounts which at the fundamental level correspond to absorption of individual particles—photons—from light incident on photodetectors. The process of generating photocounts by an incident electromagnetic field is inherently random. In the case of the quantum fingerprinting protocol described here, generation of a photocount by one of the photodetectors in a given temporal slot provides certain information on the phase relation between pulses transmitted in that slot. In turn, this phase relation depends on specific bits in codewords $E(x)$ and $E(y)$ encoding inputs. Informally speaking, photon counting selects randomly, through the physics of the photodetection process, a small subset of codeword bits that are effectively compared by the referee. Signals sent by Alice and Bob are so weak that they generate photocounts only in very few slots out of their total number.

It is insightful to juxtapose the above observation with a classical fingerprinting protocol which uses shared randomness between Alice and Bob [8]. In such a protocol Alice and Bob send only subsets of codeword bits that are specified by a shared random key. It is then sufficient to send classical fingerprints of constant length for a given probability of error. Quantum fingerprinting can be viewed as a method to replace the random key shared between Alice and Bob by the randomness of the photodetection process. In the quantum case, selection of codeword bits to be compared occurs only at the detection stage and does not require any ancillary resource to be shared between Alice and Bob.

The quantum fingerprinting protocol described here requires setting a proper phase relation between the fields received from Alice and Bob that are interfered at the beam splitter on the referee side. This requirement can be satisfied by transmitting additional reference signals that are measured by the referee to estimate the relative phase between the received optical fields and to adjust their phase relation with the help of a phase modulator inserted before the receiver beam splitter. Implementation of this strategy requires only a minor overhead in terms of the total transmitted optical energy, enabling one to maintain the advantage of the quantum fingerprinting protocol. To give a quantitative example, $N_{\text{est}} = 18/(\Delta\phi)^2$ photons is sufficient to estimate the relative phase with the uncertainty below $\Delta\phi$ and 99.7% confidence [34]. Assuming Gaussian phase fluctuations, the uncertainty $(\Delta\phi)^2$ contributes a multiplicative factor $W = \exp[-(\Delta\phi)^2/2]$ to the visibilities defined in (20). Taking for concreteness $W = 0.95$ yields $N_{\text{est}} \approx 180$ photons. This figure is substantially lower than the gap between N_Q^* and N_B for the numerical example depicted in Fig. 5, in the regime $n \gg 2\log[(1/(2\varepsilon)]/\nu$ which corresponds to the noise parameter $\mathcal{N} \gg 1$. Importantly, in this regime both visibilities V_e and V_d for the optimal bandwidth β^* are substantially below one, as implied by Fig. 4. Therefore, their rescaling by W can be included in a straightforward manner in the approximation (32) leading to (34). This produces an additional multiplicative factor W^{-1} in the expression for N_Q^* derived in (34). In the present example $W^{-1} \approx 1.05$ which implies that the assumed phase uncertainty does not alter noticeably N_Q^* in Fig. 5 when $\mathcal{N} \gg 1$.

A practical limitation when implementing the quantum fingerprinting protocol with phase estimation described above is the number of temporal slots that can be accommodated within the coherence time of the generated optical signals. Using state-of-the-art sub-Hz linewidth lasers [35] and phase modulators reaching 100 GHz bandwidth [36] yields the available number of slots up to 10^{11}. Given that the required code rate is above 0.1 in the regime $\mathcal{N} \gg 1$, this number of slots should be sufficient to achieve the quantum advantage for the input size $n \sim 10^9$–10^{10} and other parameters as in Fig. 5, even when taking into account the overhead required for phase estimation. A more universal strategy, applicable also for longer inputs, is to interleave the fingerprint signal with the reference signal at intervals shorter than the coherence time so that the referee can track the relative phase between the received signals. In terms of the required optical energy, such phase tracking adds an overhead scaling linearly with the transmission time and hence proportional to N_Q^*, which retains a constant separation between N_Q^* and N_B for large input size n in the logarithmic scale of Fig. 5. Yet another option to implement the quantum fingerprinting protocol is to exploit higher-order optical interference for signals without a defined phase relation [37], [38]. For this scenario, a preliminary analysis of the quantum advantage in terms of transmitted information has been recently presented [39].

On an ending note, the problem of comparing weak optical signals carrying classical or quantum information occurs in a number of quantum information protocols. Two relevant classes are quantum digital signatures [40], which provide a secure method to sign a message preventing impersonation, repudiation, or message tampering, and communication complexity protocols based on the so-called quantum switch [41]. Quantum fingerprinting can be viewed as a generic example of efficient extraction of information via optical interference and its thorough characterization may come in useful when analyzing other protocols based on a similar paradigm.

Appendix A

Using the orthogonality properties of the pulse mode function given in (2), the integrals (8) can be brought to the form

$$\begin{aligned} I_\pm &= \int_{-\infty}^{\infty} |\mathcal{E}^\pm(t)|^2 = \sum_{l=1}^{L} \left| \frac{\alpha_l^x \pm \alpha_l^y}{\sqrt{2}} \right|^2 \\ &= \sum_{l=1}^{L} \left[|\gamma_l^\pm|^2 + \left| \frac{\xi_l \pm \zeta_l}{\sqrt{2}} \right|^2 + 2\mathrm{Re}\left(\gamma_l^\pm \frac{\xi_l \pm \zeta_l}{\sqrt{2}} \right) \right], \quad (41) \end{aligned}$$

where

$$\gamma_l^\pm = \sqrt{\frac{S}{2B}} (e^{i\theta_l^x} \pm e^{i\theta_l^y}). \quad (42)$$

Note that linear combinations $(\xi_l \pm \zeta_l)/\sqrt{2}$ are Gaussian random variables with zero mean and variance $\mathrm{Var}[(\xi_l \pm \zeta_l)/\sqrt{2}] = \nu$. This allows one to calculate directly the expectation value in (9) which yields:

$$\begin{aligned} &Z(\lambda_+, \lambda_-) \\ &= \exp\Bigg[(e^{i\lambda_+} - 1)\left(1 + \frac{(e^{i\lambda_+}-1)\nu}{1-(e^{i\lambda_+}-1)\nu}\right) \sum_{l=1}^{L} |\gamma_l^+|^2 \\ &\quad + (e^{i\lambda_-} - 1)\left(1 + \frac{(e^{i\lambda_-}-1)\nu}{1-(e^{i\lambda_-}-1)\nu}\right) \sum_{l=1}^{L} |\gamma_l^-|^2 \Bigg] \\ &\quad \times \left(\frac{1}{1-(e^{i\lambda_+}-1)\nu} \right)^L \left(\frac{1}{1-(e^{i\lambda_-}-1)\nu} \right)^L. \quad (43) \end{aligned}$$

The terms in the exponent involving ν produce expressions of the order $O(\nu LS/B)$ and will be neglected. Sums over l can be written as

$$\sum_{l=1}^{L} |\gamma_l^\pm|^2 = \frac{LS}{B} \left(1 \pm \frac{1}{L} \sum_{l=1}^{L} \cos(\theta_l^x - \theta_l^y) \right). \quad (44)$$

Furthermore, for $\nu \ll 1$ and large L the power factors in (43) can be approximated by exponents $1/[1-(e^{i\lambda_\pm}-1)\nu]^L \approx \exp[(e^{i\lambda_\pm}-1)\nu L]$. Combining these steps together yields

$$\begin{aligned} &Z(\lambda_+, \lambda_-) \\ &= \exp\Bigg[(e^{i\lambda_+}-1)L\left(\frac{S}{B} + \nu + \frac{1}{L}\sum_{l=1}^{L} \cos(\theta_l^x - \theta_l^y) \right) \\ &\quad + (e^{i\lambda_-}-1)L\left(\frac{S}{B} + \nu - \frac{1}{L}\sum_{l=1}^{L} \cos(\theta_l^x - \theta_l^y) \right) \Bigg] \quad (45) \end{aligned}$$

which is identical with (10) when expressed in terms of μ and V defined respectively in (11) and (12).

Appendix B

The argument λ^* optimizing the right hand side of (24) can be found by solving equation $df/d\lambda = 0$, where

$$f(\lambda) = 1 - \frac{1}{2}[(1+V_e)^\lambda (1+V_d)^{1-\lambda} + (1-V_e)^\lambda (1-V_d)^{1-\lambda}]. \quad (46)$$

The solution is given by the following closed expression:

$$\lambda^* = \frac{\log\left[\frac{1-V_d}{1+V_d} \frac{\log\frac{1-V_d}{1-V_e}}{\log\frac{1+V_e}{1+V_d}} \right]}{\log\left(\frac{1+V_e}{1-V_e} \frac{1-V_d}{1+V_d} \right)}. \quad (47)$$

For $V_e, V_d \ll 1$ the above formula can be approximated up to the second order by

$$\lambda^* \approx \frac{1}{2} + \frac{V_d^2 - V_e^2}{24}. \quad (48)$$

Inserting this expression into (46) yields up to the second order in V_e, V_d:

$$\mathsf{C} \approx \frac{1}{8}(V_e - V_d)^2. \quad (49)$$

The same result is obtained by using the zeroth order expansion $\lambda^* \approx 1/2$ in (46).

Acknowledgment

Insightful discussions with B. A. Bash, N. Lütkenhaus, F. Xu, and Q. Zhang are gratefully acknowledged.

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sep. 2009.

[3] F. Xu, X. M. Q. Zhang, H.-K. Lo, and J.-W. Pan, "Quantum cryptography with realistic devices," Mar. 2019, *arXiv:1903.09051*. Accessed: Jul. 10, 2019. [Online]. Available: https://arxiv.org/abs/1903.09051

[4] A. C.-C. Yao, "Some complexity questions related to distributive computing (preliminary report)," in *Proc. 11th Annu. ACM Symp. Theory Comput.* Atlanta, GA, USA: ACM, 1979, pp. 209–213.

[5] A. Ambainis, "Communication complexity in a 3-computer model," *Algorithmica*, vol. 16, no. 3, pp. 298–301, Sep. 1996.

[6] I. Newman and M. Szegedy, "Public vs. private coin flips in one round communication games," in *Proc. 28th ACM Symp. Theory Comput.* New York, NY, USA: ACM, 1996, p. 596.

[7] L. Babai and P. Kimmel, "Randomized simultaneous messages: Solution of a problem of Yao in communication complexity," in *Proc. 12th Annu. IEEE Conf. Comput. Complex.*, Nov. 1997, p. 239.

[8] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, "Quantum fingerprinting," *Phys. Rev. Lett.*, vol. 87, no. 16, p. 167902, Sep. 2001.

[9] H. Buhrman and R. De Wolf, "Communication complexity lower bounds by polynomials," in *Proc. 16th Annu. IEEE Conf. Comput. Complex.*, 2001, pp. 120–130.

[10] S. Aaronson, "Limitations of quantum advice and one-way communication," in *Proc. 19th IEEE Annu. Conf. Comput. Complex.*, Nov. 2004, pp. 320–332.

[11] A. C.-C. Yao, "On the power of quantum fingerprinting," in *Proc. 35th ACM Symp. Theory Comput. (STOC)*, 2003, pp. 77–81.

[12] D. Gavinsky, J. Kempe, and R. De Wolf, "Strengths and weaknesses of quantum fingerprinting," in *Proc. 21st Annu. IEEE Conf. Comput. Complex. (CCC)*, Los Alamitos, CA, USA, Jul. 2006, pp. 288–298.

[13] A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum channel," *Problems Inf. Transm.*, vol. 9, no. 3, pp. 177–183, 1973.

[14] A. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 269–273, Jan. 1998.

[15] J. M. Arrazola and N. Lütkenhaus, "Quantum fingerprinting with coherent states and a constant mean number of photons," *Phys. Rev. A, Gen. Phys.*, vol. 89, no. 6, Jun. 2014, Art. no. 062305.

[16] B. Lovitz and N. Lütkenhaus, "Families of quantum fingerprinting protocols," *Phys. Rev. A, Gen. Phys.*, vol. 97, no. 3, 2018, Art. no. 032340.

[17] F. Xu *et al.*, "Experimental quantum fingerprinting with weak coherent pulses," *Nature Commun.*, vol. 6, no. 1, p. 8735, Dec. 2015.

[18] J. Y. Guan *et al.*, "Observation of quantum fingerprinting beating the classical limit," *Phys. Rev. Lett.*, vol. 116, no. 24, Jun. 2016, Art. no. 240502.

[19] D. M. Boroson, "On achieving high performance optical communications from very deep space," *Proc. SPIE, Free-Space Laser Commun. Atmos. Propag.*, vol. 10524, Feb. 2018, Art. no. 105240B.

[20] W. Zwoliński, M. Jarzyna, and K. Banaszek, "Range dependence of an optical pulse position modulation link in the presence of background noise," *Opt. Express*, vol. 26, no. 20, p. 25827, Oct. 2018.

[21] K. Banaszek, L. Kunz, M. Jarzyna, and M. Jachura, "Approaching the ultimate capacity limit in deep-space optical communication," *Proc. SPIE, Free-Space Laser Commun.*, vol. 10910, Mar. 2019, Art. no. 109100A.

[22] V. Giovannetti, R. García-Patrón, N. J. Cerf, and A. S. Holevo, "Ultimate classical communication rates of quantum optical channels," *Nature Photon*, vol. 8, no. 10, pp. 796–800, Oct. 2014.

[23] J. Shapiro, "The quantum theory of optical communications," *IEEE J. Sel. Topics Quantum Electron.*, vol. 15, no. 6, pp. 1547–1569, Aug. 2009.

[24] H. Hemmati, *Deep Space Optical Communications*. Hoboken, NJ, USA: Wiley, 2006.

[25] R.-J. Essiambre, G. Kramer, P. J. Winzer, G. J. Foschini, and B. Goebel, "Capacity limits of optical fiber networks," *J. Lightw. Technol.*, vol. 28, no. 4, pp. 662–701, Feb. 15, 2010.

[26] B. Brecht, A. Eckstein, A. Christ, H. Suche, and C. Silberhorn, "From quantum pulse gate to quantum pulse shaper–engineered frequency conversion in nonlinear optical waveguides," *New J. Phys.*, vol. 13, no. 6, Jul. 2011, Art. no. 065029.

[27] B. Brecht, D. V. Reddy, C. Silberhorn, and M. G. Raymer, "Photon temporal modes: A complete framework for quantum information science," *Phys. Rev. X*, vol. 5, no. 4, 2015, Art. no. 041017.

[28] A. Shahverdi, Y. M. Sua, L. Tumeh, and Y.-P. Huang, "Quantum parametric mode sorting: Beating the time-frequency filtering," *Sci. Rep.*, vol. 7, no. 1, Jul. 2017, Art. no. 6495.

[29] D. V. Reddy and M. G. Raymer, "High-selectivity quantum pulse gating of photonic temporal modes using all-optical Ramsey interferometry," *Optica*, vol. 5, no. 4, p. 423, Apr. 2018.

[30] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*. Cambridge, U.K.: Cambridge Univ. Press, 1995, ch. 9.

[31] J. H. van Lint, *Introduction to Coding Theory*, 3rd ed. Berlin, Germany: Springer, 1987.

[32] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, D. L. Schilling, Ed. Hoboken, NJ, USA: Wiley, 1991.

[33] S. Guha, Z. Dutton, and J. H. Shapiro, "On quantum limit of optical communications: Concatenated codes and joint-detection receivers," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2011, pp. 274–278.

[34] V. Makarov, A. Brylevski, and D. R. Hjelme, "Real-time phase tracking in single-photon interferometers," *Appl. Opt.*, vol. 43, no. 22, pp. 4385–4392, 2004.

[35] *OEwaves HI-Q 1.5 MICRON LASER SUB-HERTZ OE4030 Datasheet*. Accessed: Dec. 10, 2019. [Online]. Available: https://oewaves.com/hi-q-1-5-micron-lasers-1

[36] K. Noguchi, O. Mitomi, and H. Miyazawa, "Millimeter-wave Ti:LiNbO$_3$ optical modulators," *J. Lightw. Technol.*, vol. 16, no. 4, pp. 615–619, Apr. 1998.

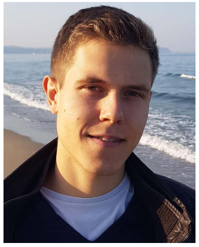
[37] M. Jachura, M. Lipka, M. Jarzyna, and K. Banaszek, "Quantum fingerprinting using two-photon interference," *Opt. Express*, vol. 25, no. 22, Oct. 2017, Art. no. 27475.

[38] M. Jachura, M. Jarzyna, M. Lipka, W. Wasilewski, and K. Banaszek, "Visibility-based hypothesis testing using higher-order optical interference," *Phys. Rev. Lett.*, vol. 120, no. 11, Mar. 2018, Art. no. 110502.

[39] M. Lipka, M. Jarzyna, and K. Banaszek, "Feasibility of quantum fingerprinting using optical signals with random global phase," in *Proc. SPIE, Quantum Inf. Sci. Technol. IV*, vol. 10803, Oct. 2018, Art. no. 108030K.

[40] P. L. Clarke, R. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light," *Nature Commun.*, vol. 3, p. 1174, 2012.

[41] K. Wei *et al.*, "Experimental quantum switching for exponentially superior quantum communication complexity," *Phys. Rev. Lett.*, vol. 122, Mar. 2019, Art. no. 120504.



Michał Lipka received the B.Sc. degree in physics from the University of Warsaw, Poland, in 2018. He is currently pursuing the M.Sc. degree in physics with the University of Warsaw and since 2015 works there in the Quantum Memories Laboratory, which is part of the Centre for Quantum Optical Technologies, University of Warsaw.

In 2019, he has been awarded National (Poland) Ministry of Science and Higher Education's "Diamond Grant" to develop real-time single photon localization technologies.

Marcin Jarzyna received the M.Sc. and Ph.D. degrees in physics from the University of Warsaw, Warsaw, Poland, in 2011 and 2016, respectively.

He has been with the Centre of New Technologies, University of Warsaw, since 2016. Research leading to his Ph.D. was focused mainly on quantum metrology and the impact of entanglement on the asymptotic precision limits under decoherence. His current research interests include low power limits of communication, impact of signal amplification, superresolution effects in optical imaging, and optical realizations of communication complexity problems

Konrad Banaszek (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in physics from the University of Warsaw, Poland in 1997 and 2000, respectively.

He held postdoctoral positions at the University of Rochester, NY, USA, and the University of Oxford, U.K., followed by a Junior Research Fellowship at St. John's College, Oxford, U.K., and faculty appointments at the Nicolaus Copernicus University, Toruń, Poland, from 2005 to 2009, and at the University of Warsaw, since 2009. His field of research is quantum physics and optical sciences with a focus on novel approaches to communication, sensing, and imaging that enable operation beyond the standard quantum limits. He is currently the Director of the Centre for Quantum Optical Technologies established in 2018 by the University of Warsaw in partnership with the University of Oxford under the International Research Agendas Programme operated by the Foundation for Polish Science.

Dr. Banaszek has served as an Associate Editor of *Optics Express* and a Guest Editor of a focus issue of the *New Journal of Physics* on quantum tomography. In 2001, he received the European Physical Society Fresnel Prize for his contributions to the understanding of non-classical light and its applications in quantum information processing.