Optimal quantum-programmable projective measurements with coherent states

Niraj Kumar,[1,*] Ulysse Chabaud,[2,†] Elham Kashefi,[1,2,‡] Damian Markham,[2,3,§] and Eleni Diamanti[2,‖]

[1]*School of Informatics, 10 Crichton St., University of Edinburgh, Edinburgh EH8 9AB, United Kingdom*

[2]*CNRS, LIP6, Sorbonne Université, 4 Place Jussieu, 75005 Paris, France*

[3]*JFLI, CNRS, National Institute of Informatics, University of Tokyo, Tokyo, Japan*

(Received 9 February 2021; accepted 26 May 2021; published 14 October 2021)

We consider a device which can be programed using coherent states of light to approximate a given projective measurement on an input coherent state. We provide and discuss three practical implementations of this programmable projective measurement device with linear optics, involving only balanced beam splitters and single photon threshold detectors. The three schemes optimally approximate any projective measurement onto a program coherent state. We further extend these to the case where there are no assumptions on the input state. In this setting, we show that our scheme enables an efficient verification of an unbounded untrusted source with only local coherent states, balanced beam splitters, and threshold detectors. Exploiting the link between programmable measurements and generalized swap test, we show as a direct application that our schemes provide an asymptotically quadratic improvement in existing quantum fingerprinting protocol to approximate the Euclidean distance between two unit vectors.

DOI: 10.1103/PhysRevResearch.3.043035

I. INTRODUCTION

A typical experiment with measurement of a quantum state involves preparing a circuit, which is often classically controlled, to perform a vast range of operations on the state. The choice of measurement typically depends on the task at hand and is usually fixed beforehand. In some cases, one could alternatively use a measurement device which is classically (re)programmable to obtain a wide variety of measurement scenarios. Recent developments on this front involve a programmable optical circuit that can implement all possible linear optical protocols up to the size of that circuit [1]. The circuit involves Mach–Zehnder interferometers and thermo-optic phase shifters which are electronically and optically controlled.

In this paper, we investigate an alternative scenario where a quantum input—rather than a classical program—controls the choice of measurement. This setting has applications in several quantum protocols for solving communication complexity problems. These include quantum fingerprinting protocols to check for equality between two given strings [2–5], Euclidean distance of two real vectors [6], and matching-based one-way communication complexity problems [7,8]. The choice of measurement being driven by an input quantum state has also been extensively used in cryptography settings such as private quantum money schemes [5,9–12]. In these works, a central issue is to test whether two unknown quantum states are equal. Such a quantum state comparison can be performed using a programmable projective measurement device, where multiple copies of one of the two states to be compared act as program states encoding the direction of the measurement, which is then performed on the other state: if the projection succeeds, the states are considered equal, otherwise they are considered different.

The comparison of two states is trivial in the classical world, where two bit strings can be bit-wise checked and thus the maximum number of operations that are needed equals the size of the strings. However, comparing two quantum states is nontrivial since a quantum state is typically in a superposition over multiple possible basis states. If we simply follow the above classical procedure of individually measuring the quantum states in some fixed basis and comparing the measurement outcomes, then the basis measurement only reveals partial information about each quantum state, i.e., the amplitude corresponding to the specific basis state onto which the quantum state has collapsed. Hence, this measure-and-compare approach does not work for comparing two unknown quantum states. Buhrman *et al.* [2] introduced a simple test, the so-called swap test, to compare two unknown quantum states with one-sided error probability, i.e., the test succeeds with certainty if the two quantum states are the same, however, there is a nonzero probability of failing the test if the two states are different. This test uses a controlled-swap operation and is optimal under one-sided error probability, if one only has a single copy of the two quantum states [13]. However, to succeed with an arbitrarily small desired error probability ϵ, this technique needs to perform independent tests on at-least logarithm of inverse-ϵ number of copies of both quantum states.

*nkumar@exseed.ed.ac.uk
†ulysse.chabaud@gmail.com
‡ekashefi@exseed.ed.ac.uk
§damian.markham@lip6.fr
‖eleni.diamanti@lip6.fr

Generalizing this scenario, Chabaud *et al.* [14] introduced a version of the swap test when one is provided with just a single copy of one of the states in some *input* register and multiple copies of the other state in the *program* registers. They investigated the probability of a successful projective measurement on the input state in the basis of the program register state by constructing a circuit that takes as inputs the states in the input and program registers. They showed that this probability increases with the number of copies of the state in the program register. In particular, they proposed an implementation of a state comparison test, where all output states are measured, with generic quantum states encoded in single photons. They showed that the same implementation provides a programmable projective measurement scheme involving balanced beam splitters and photon number-resolving detectors, in which the states in the program registers approximate the direction of the measurement, which is performed on the state in the input register.

Their proposal, however, requires the creation and manipulation of high-dimensional superposition states, which is out of the reach of current experimental photonic technologies required for implementing quantum communication tasks. A major step in overcoming the difficulty in experimental realizations for such protocols requiring high-dimensional states was proposed by the theoretical work of Arrazola and Lütkenhaus [3]: Their work maps any protocol involving pure states of many qubits, unitary transformations, and projective measurement to protocols based on coherent states of light in multiple optical modes, passive linear optical transformations and single-photon threshold detection. Since coherent states of light are natural realizations of states produced by lasers, these are highly efficient to produce and manipulate experimentally. This model was subsequently used to demonstrate quantum advantage in quantum communication tasks [4,8,15].

Motivated by the coherent state mapping of quantum protocols, we extend the results of Ref. [14] and introduce a programmable device which uses coherent states of light to perform a given projective measurement onto program coherent states, with commercially available passive linear optics components such as balanced beam splitters and single-photon threshold detectors. Our scheme takes as input a single-mode coherent state (*the input* register) and $M-1$ copies of some coherent state $|\beta\rangle$ (the *program* registers) and approximates the projective measurement $\{|\beta\rangle\langle\beta|, 1-|\beta\rangle\langle\beta|\}$ on the state in the input register in a single run. We provide and discuss three practical implementations of our programmable projective measurement scheme. The three schemes, which we will refer to as the *Hadamard scheme*, the *amplifier scheme*, and the *looped amplifier scheme*, respectively, all provide an optimal projective measurement with one-sided error probability given a single copy of the input register and $M-1$ copies of the program registers, in the sense that they achieve the best possible approximation of the projective measurement using $M-1$ program states. The schemes differ, however, in the number of linear optics components. While all three schemes are efficient, the *looped amplifier scheme* is the most practical scheme requiring a single balanced beam splitter and a single threshold detector—with the counterpart that it requires an optical switch.

In addition to substantially reducing the experimental requirements, we obtain two additional advantages in our scheme compared to the original scheme of Ref. [14]. First, our scheme leaves a remaining output state after the projective measurement, which can be used as a resource for subsequent tasks. The second advantage is that from the use of coherent states, we obtain a more faithful projective measurement than using a single-photon encoding, implying better probability in carrying out a successful projective measurement.

Next, we extend our scheme to allow the input register to be obtained from an untrusted source: Instead of requiring that the state in the input register is a coherent state, we allow any generic quantum state as an input, while the states in the program registers are still obtained from a trusted coherent state source. This setting is very natural in quantum cryptography and in verification of quantum state preparation [10,12]. In this setting, we also show an optimal approximate projective measurement on the input state, thus finding relevance when such a measurement is a part of some verification protocol. Our result enables an efficient verification of an unbounded untrusted source with only trusted coherent states, balanced beam splitters, and threshold detectors.

As a final result, we give an application of our generalized scheme by showing an at-most quadratic improvement in soundness of an existing quantum fingerprinting protocol to approximate the Euclidean distance between two unit vectors [6].

The paper is organized as follows. In Sec. II, we review the existing state comparison techniques for qubit states and coherent states. Following Ref. [14], we then consider the setting of a single input register state and multiple program register states, where both the input register state and the program register states are coherent states, in Sec. III. We introduce and compare three different schemes for performing state comparison and programmable projective measurement with coherent states. Further, in Sec. IV, we give the proof of the optimality of our projective measurement for all three schemes, under the one-sided error requirement. We then analyze the robustness of our schemes by considering experimental imperfections in Sec. V. In Sec. VI, we drop the assumption that the incoming input register state is a coherent state. We further prove that our projective measurement scheme is also optimal in this case. We conclude with Sec. VII by giving a concrete improvement of the quantum fingerprinting protocol to solve the Euclidean distance problem [6].

II. QUANTUM STATE COMPARISON

A circuit for comparing two unknown qubit states, known as the swap test, was first introduced by Buhrman *et al.* [2]. The analog of this test when the states are unknown coherent states was introduced in Ref. [3]. We briefly review these two tests here. Throughout this paper, we use logarithm in base 2.

A. The swap test

The swap test uses a controlled-swap gate applied on two unknown qubit states $|\phi\rangle$ and $|\psi\rangle$, and controlled by an ancilla qubit, as shown in Fig. 1. Applying the circuit and measuring the ancilla qubit gives output 1 with a probability

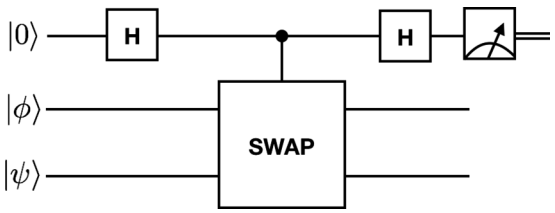

FIG. 1. Controlled-swap circuit employed to compare the incoming qubit states. The ancilla qubit is measured in the computational basis and this relates to the probability of telling the two qubit states apart.

$\mathbb{P}(1) = \frac{1}{2}(1 - |\langle\phi|\psi\rangle|^2)$, and output 0 with probability $\mathbb{P}(0) = 1 - \mathbb{P}(1)$.

We define the completeness and soundness of this test as follows:

Completeness: If the states $|\phi\rangle$ and $|\psi\rangle$ are the same, then there is a zero probability of the outcome being 1. We say that the test has perfect completeness $c_2 = 1$, where the completeness is defined as $c_2 = 1 - \mathbb{P}(1)$, when the input states are the same. The subscript denotes that two states have been used for testing. Alternatively, we say that the test meets the *one-sided error requirement* when it has perfect completeness.

Soundness: If the states are different, then with finite probability $\mathbb{P}(1)$, one is able to tell the states apart. Thus the soundness, defined as $s_2 = \mathbb{P}(1)$, is strictly greater than 0. The soundness of this scheme can be increased to any desired $1 - \delta$, by repeating the test $O(\log \frac{1}{\delta})$ times, using new copies of the states each time.

We note that this test provides an optimal comparison between two unknown states for the one-sided error probability.

B. Comparing two coherent states

The above swap test compares two unknown qubit states. If the unknown states are coherent states instead, then an analogous test can be performed by simply mixing the states on a balanced beam splitter and observing a photon click with a single-photon threshold detector (detector D_0 in Fig. 2).

This can be seen as follows. The beam splitter transforms the input mode creation operators $\{\hat{a}^\dagger, \hat{b}^\dagger\}$ into the output mode creation operators $\{\hat{c}^\dagger, \hat{d}^\dagger\}$. This input to output conversion is given by

$$\hat{a}^\dagger \to \frac{1}{\sqrt{2}}(\hat{c}^\dagger + \hat{d}^\dagger),$$
$$\hat{b}^\dagger \to \frac{1}{\sqrt{2}}(\hat{c}^\dagger - \hat{d}^\dagger). \tag{1}$$

The input state at the beam splitter is

$$|\alpha\rangle_a \otimes |\beta\rangle_b\,, \tag{2}$$

where the subscripts denote the mode in which the coherent states enter the beam splitter. In the absence of experimental imperfections, this yields the output state

$$\left|\frac{\alpha+\beta}{\sqrt{2}}\right\rangle_c \otimes \left|\frac{\alpha-\beta}{\sqrt{2}}\right\rangle_d. \tag{3}$$

The probability of obtaining a click in the detector D_0 (mode d) is

$$\mathbb{P}_{D_0} = 1 - \exp\left(-\frac{|\alpha-\beta|^2}{2}\right) = 1 - |\langle\alpha|\beta\rangle|. \tag{4}$$

We can relate the completeness c_2 and soundness s_2 of the test to the trace distance of the tested states $|\alpha\rangle$ and $|\beta\rangle$. The trace distance for two coherent states $\{|\alpha\rangle, |\beta\rangle\}$ is

$$\| |\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta| \|_{\rm tr} = \sqrt{1 - |\langle\alpha|\beta\rangle|^2} = \sqrt{1 - e^{-|\alpha-\beta|^2}}. \tag{5}$$

We assign the detection event (obtaining a click in D_0) the value 1 and to the other detection event (no click in detector D_0) the value 0. The completeness and soundness for this test are:

Completeness: If the states are the same, then their trace distance is 0, since $|\alpha\rangle = |\beta\rangle$. This implies that $|\langle\alpha|\beta\rangle| = 0$, thus leading to $\mathbb{P}(1) = 0$. This ensures perfect completeness $c_2 = 1$, where the subscript denotes the size of the interferometer.

Soundness: Suppose the states $|\alpha\rangle$ and $|\beta\rangle$ are ϵ far in trace distance, i.e.,

$$\| |\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta| \|_{\rm tr} \geqslant \epsilon \Rightarrow |\langle\alpha|\beta\rangle| \leqslant \sqrt{1-\epsilon^2}. \tag{6}$$

From this, we can lower bound the soundness s_2 as

$$s_2 = \mathbb{P}(1) \geqslant 1 - \sqrt{1-\epsilon^2}, \tag{7}$$

where ϵ is any lower bound to the trace distance between the program and tested states. This implies that the soundness is strictly greater than 0 for a nonzero ϵ. The soundness can be decreased to any desired δ by repeating the measurement procedure for $O(\log \frac{1}{\delta})$ runs. Further, this method provides an optimal comparison between two unknown coherent states under one-sided error probability. We prove this more generally in Sec. IV.

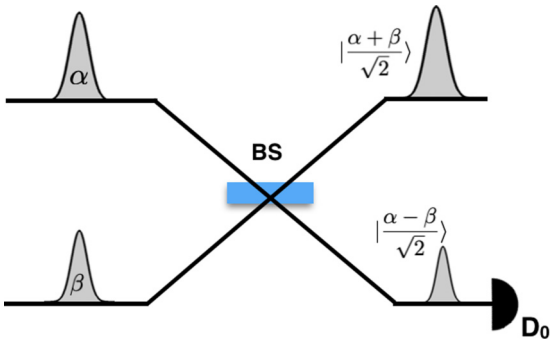

FIG. 2. Balanced beam splitter (BS) operation acting on input coherent states $|\alpha\rangle$ and $|\beta\rangle$. The lower output mode of the BS is measured with a single-photon threshold detector D_0. The probability of obtaining a click in D_0 relates to the projective measurement test of distinguishing the two coherent states.

III. GENERALIZED SINGLE RUN COHERENT STATE COMPARISON

Having briefly reviewed existing unknown state comparison techniques, we now consider the scenario where we have a single copy of an unknown coherent state $|\alpha\rangle$ in the input register and multiple copies of the coherent state $|\beta\rangle$ in the

TABLE I. Differences between coherent state comparison schemes in terms of number of optical elements. The first two schemes take as input a single copy of a coherent state $|\alpha\rangle$ and $M-1$ copies of a coherent state $|\beta\rangle$, where M is a power of 2, while the looped amplifier scheme is independent of M. The optical elements are balanced beam splitters, single-photon threshold detectors, and the switch is an optical switch element, only required for the looped amplifier scheme.

Scheme	Beam splitters	Detectors	Switch
Hadamard	$\frac{1}{2}M\log M$	$M-1$	0
Amplifier	$M-1$	$\log M$	0
Looped amplifier	1	1	1

program register. The task is to check if the state in the input register is equal to the state in the program register.

In the simplest case, the state comparison can be performed with a single copy of the state in the program register, like in the previous section. This succeeds with a probability given by Eq. (4). In this section, we prove that having multiple copies of $|\beta\rangle$ increases the success probability of state comparison with state $|\alpha\rangle$. For this, we first provide a generalized interferometer construction, the *Hadamard scheme*, based on Hadamard-Walsh transforms, following Ref. [14]. We then derive the *amplifier scheme*, requiring much less optical gates and detectors than the previous scheme. Finally, we modify the amplifier scheme using an optical switch to obtain a scheme with even less optical elements, the *looped amplifier scheme*. The differences between all three schemes are summarised in Table I.

A. The Hadamard scheme

In Ref. [14], it is shown how to perform state comparison and programmable measurements with linear optics using generic quantum states encoded in degrees of freedom of single photons. These photons are fed into an specific interferometer, the Hadamard interferometer, which we review below. All output modes of the interferometer are then measured with photon number-resolving detectors and the classical outcomes are postprocessed to retrieve the statistics of a projective measurement. In what follows, we adapt and simplify their approach to the case where the input states are coherent states. We show that single-photon threshold detectors are sufficient for our needs, obtaining a practical scheme.

Input state: Suppose the input is M coherent states, where M is a power of 2,

$$|\alpha\rangle_0 \otimes |\beta\rangle_1 \cdots \otimes |\beta\rangle_{M-1}, \tag{8}$$

where the subscript denotes the mode in which the coherent state enters the generalized interferometer (indexed from 0 to $M-1$). For brevity, we address this state as $|\alpha\beta\ldots\beta\rangle$. This input state is then fed in an interferometer of size M. For $M=4$ spatial modes, this interferometer is described by the Hadamard-Walsh transform of order 2,

$$H_2 := H^{\otimes 2} = \frac{1}{\sqrt{2}}\begin{pmatrix} H & H \\ H & -H \end{pmatrix}, \tag{9}$$

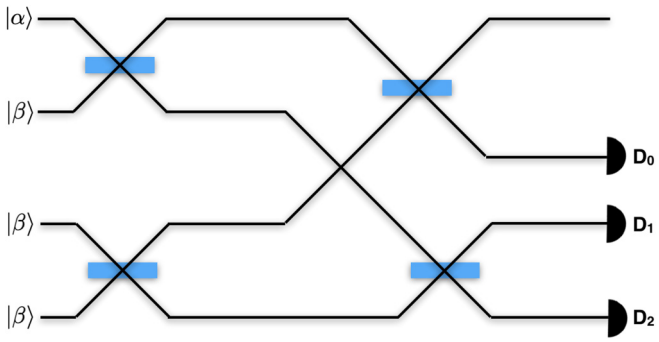

FIG. 3. Hadamard interferometer with four input modes.The input states are one input register state $|\alpha\rangle$ and three local states $|\beta\rangle$, one in each mode. The detectors D_i are single-photon threshold detectors, $\forall i \in \{0, 2\}$.

where H is a Hadamard matrix. The corresponding interferometer for $M=4$ is depicted in Fig. 3.

In the general case, the Hadamard interferometer of order M is described by the Hadamard-Walsh transform of order $n = \log M$, which is defined by

$$H_n := H^{\otimes n}, \tag{10}$$

with $H_0 = 1$ and $H_1 = H$.

Output state: The input coherent states $|\alpha\beta\ldots\beta\rangle$ upon interaction with the interferometer of order n transforms as

$$|\alpha\beta\ldots\beta\rangle \mapsto H_n\,|\alpha\beta\ldots\beta\rangle = |\delta_0\delta_1\ldots\delta_{M-1}\rangle\,, \tag{11}$$

where, with a simple induction, we obtain $\delta_0 = \frac{\alpha+(M-1)\beta}{\sqrt{M}}$ and $\delta_k = \frac{\alpha-\beta}{\sqrt{M}}$ for $k>0$. Thus the last $M-1$ modes have the same probability of a click when we detect with single-photon threshold detectors. The probability $\mathbb{P}_\emptyset$ that none of the $M-1$ detectors clicks is

$$\begin{aligned}\mathbb{P}_\emptyset(\alpha,\beta,M) &= \prod_{k=1}^{M-1}[1-\mathbb{P}(\text{click in } k\text{th mode})] \\ &= \prod_{k=1}^{M-1}[1-(1-\exp(-|\delta_k|^2))] \\ &= \exp\left(-\frac{M-1}{M}|\alpha-\beta|^2\right) \\ &= (|\langle\alpha|\beta\rangle|^2)^{1-\frac{1}{M}}.\end{aligned} \tag{12}$$

In particular, for all $\alpha,\beta\in\mathbb{C}$, $\mathbb{P}_\emptyset(\alpha,\beta,+\infty) = |\langle\alpha|\beta\rangle|^2$, which corresponds to a perfect projective measurement of the states $|\alpha\rangle$ and $|\beta\rangle$. Assigning to this detection event (none of the detectors clicks) the value 0, and to other detection events (at least one of the $M-1$ detectors clicks) the value 1, we obtain a device whose statistics mimic those of a projective measurement, with

$$\mathbb{P}_M(0) = 1-\mathbb{P}_M(1) = (|\langle\alpha|\beta\rangle|^2)^{1-\frac{1}{M}}. \tag{13}$$

The test based on single-photon encoding from Ref. [14] requires using M number-resolving detectors. On the contrary, the encoding with coherent states requires $M-1$ single-photon threshold detectors. Experimentally, this is much more

cost effective and relatively easier to implement. The test based on coherent state encoding has the following characteristics:

Completeness: If the states are the same, then the trace distance $\| |\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta| \|_{\mathrm{tr}} = 0$, and hence the probability of having the detection event 1 is 0. Thus, the completeness of this scheme is $c_M = 1$.

Soundness: If the states $\{|\alpha\rangle, |\beta\rangle\}$ are ϵ far apart in trace distance, then using Eq. (5), and the fact that the soundness is $s_M = 1 - \mathbb{P}(0)$, we obtain

$$s_M \geqslant 1 - (1-\epsilon^2)^{1-\frac{1}{M}}. \tag{14}$$

Moreover, contrary to single-photon encoding, the Hadamard scheme with coherent state encoding leaves a remaining single-mode output state, as the first output mode is not measured.

Another advantage with coherent state encoding is that it gives a more faithful projective measurement than the single-photon encoding in Ref. [14]. Indeed,the statistics corresponding to a perfect projective measurement are

$$\mathbb{P}(0) = 1 - \mathbb{P}(1) = |\langle\alpha|\beta\rangle|^2, \tag{15}$$

where $|\langle\alpha|\beta\rangle|^2$ is the overlap between the input state and the program state, while for the single-photon encoding, with an M-mode input state $|\alpha\beta\ldots\beta\rangle$, the corresponding statistics as obtained in Ref. [14] are

$$\mathbb{P}(0) = 1 - \mathbb{P}(1) = \frac{1}{M} + \left(1 - \frac{1}{M}\right)|\langle\alpha|\beta\rangle|^2, \tag{16}$$

and for any given value of the overlap $|\langle\alpha|\beta\rangle|^2$ we have

$$|\langle\alpha|\beta\rangle|^2 \leqslant (|\langle\alpha|\beta\rangle|^2)^{1-\frac{1}{M}} \leqslant \frac{1}{M} + \left(1 - \frac{1}{M}\right)|\langle\alpha|\beta\rangle|^2, \tag{17}$$

where the term on the left-hand side corresponds to a perfect projective measurement [Eq. (15)], the central term corresponds to our coherent state scheme [Eq. (13)] and the term on the right-hand side corresponds to the single-photon scheme [Eq. (16)]. In particular, for a given size M, the maximal statistical gap with a perfect projective measurement is

$$\begin{aligned} e_{\mathrm{SP}}(M) &= \max_{x\in[0,1]} \left| \left[\frac{1}{M} + \left(1 - \frac{1}{M}\right)x\right] - x \right| \\ &= \frac{1}{M}, \end{aligned} \tag{18}$$

for the single-photon encoding, and

$$\begin{aligned} e_{\mathrm{CS}}(M) &= \max_{x\in[0,1]} \left| \left(x^{1-\frac{1}{M}}\right) - x \right| \\ &= \frac{(M-1)^{M-1}}{M^M} \\ &\sim \frac{1}{e}\cdot\frac{1}{M}, \end{aligned} \tag{19}$$

for the coherent state encoding, which is lower than the single-photon encoding gap. This happens because, for the single-photon encoding, no assumption is made about the input states, while in our case states $|\alpha\rangle$ and $|\beta\rangle$ are assumed to be coherent states. This additional information about the states allows us to better approximate a perfect projective measurement with the same number of input states. A related question would be, Is the generalized Hadamard scheme optimal or can a better measurement setting improve the state comparison? We show in Sec. IV that the generalized Hadamard interferometer is actually optimal for approaching perfect projective measurements with coherent states under the one-sided error requirement. However, we already show in the next paragraph that there exists a simpler measurement setting than the Hadamard interferometer, achieving the same performance in the test.

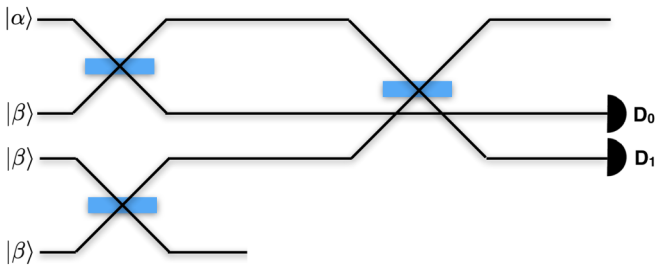

FIG. 4. Amplifier scheme with four input modes. The input states are one tested state $|\alpha\rangle$ and three local states $|\beta\rangle$, one in each mode. The detectors D_i are single-photon threshold detectors. This scheme may be contrasted with the one in Fig. 3

B. The amplifier scheme

The Hadamard scheme of size M described in the previous section uses $(M\log M)/2$ balanced beam splitters and $M-1$ single-photon threshold detectors. We introduce a simplified scheme of the same size, which only uses $M-1$ balanced beam splitters and $\log M$ detectors, and show that it achieves the same performance than the Hadamard scheme. We refer to this scheme as the *amplifier* scheme, since it maps identical input coherent states to an amplified coherent state in the first output mode and the vacuum in all other modes.

For $M = 4$ spatial modes, this interferometer acting on modes $\{0, 1, 2, 3\}$ is described by the following unitary matrix:

$$U_2 = H_{0,2} \times (H_{0,1} \oplus H_{2,3}), \tag{20}$$

where $H_{i,j}$ corresponds to the balanced beam splitter operation acting on modes i and j (where the modes are indexed from 0 to $M-1$) and identity on the other modes (Fig. 4).

The generalized amplifier interferometer is defined by induction,

$$U_n = H_{0,M/2} \times (U_{n-1} \oplus U_{n-1}), \tag{21}$$

where $n = \log M$ and where $U_1 = H_{0,1} = H$ is a Hadamard matrix. This induction relation is illustrated in Fig. 5. Indexing the spatial modes from 0 to $M-1$, the 2^k output modes are measured with single-photon threshold detectors, for $k = 0\ldots n-1$. A simple induction shows that the output state in the 2^k output mode is $|\frac{\alpha-\beta}{2^{\frac{k+1}{2}}}\rangle$.

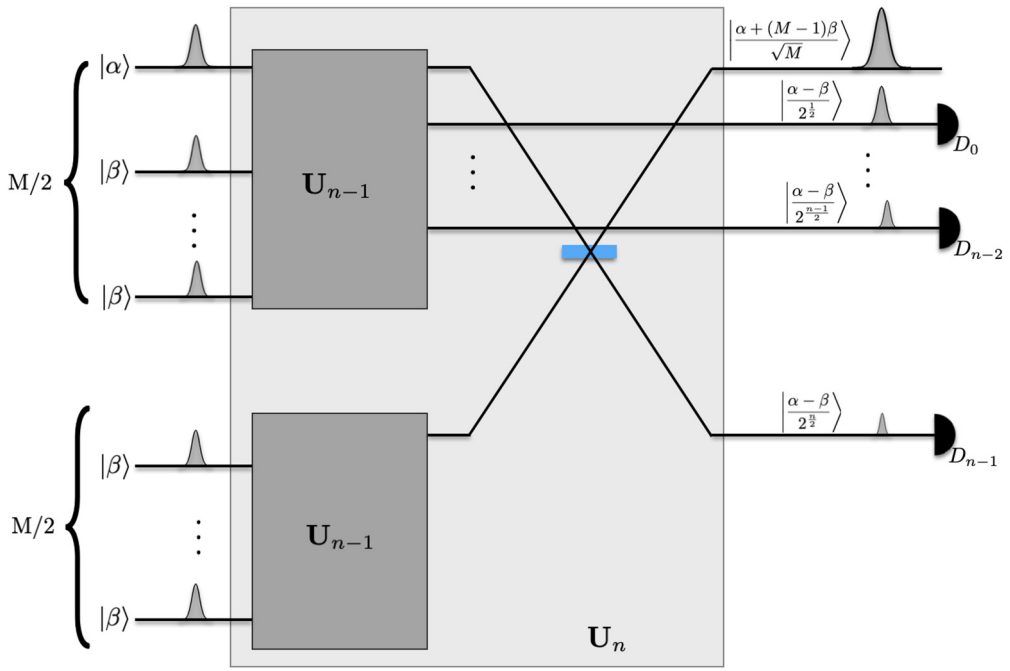

FIG. 5. General amplifier scheme of size M, with one copy of $|\alpha\rangle$ and $M-1$ copies of $|\beta\rangle$: The first output modes of two interferometers described by U_{n-1} are mixed on a balanced beam splitter. The input states are one tested state $|\alpha\rangle$ and $M-1$ local states $|\beta\rangle$, one in each mode. Indexing the spatial modes from 0 to $M-1$, the 2^k output modes are measured with single-photon threshold detectors labeled D_k, for $k=0\ldots n-1$.

Hence, the probability that none of the $n=\log M$ detectors clicks is given by

$$\begin{aligned} P_{\emptyset}(\alpha,\beta,M) &= \prod_{k=0}^{n-1}[1-\mathbb{P}(\text{click in the } 2^k\text{th mode})] \\ &= \prod_{k=0}^{n-1}\left[1-\left(1-\exp\left(-\left|\frac{\alpha-\beta}{2^{\frac{k+1}{2}}}\right|^2\right)\right)\right] \\ &= \exp\left(-\sum_{k=0}^{n-1}\left(\frac{1}{2}\right)^{k+1}|\alpha-\beta|^2\right) \\ &= \exp\left(-\frac{M-1}{M}|\alpha-\beta|^2\right) \\ &= (|\langle\alpha|\beta\rangle|^2)^{1-\frac{1}{M}}, \end{aligned} \tag{22}$$

thus retrieving the statistics obtained with the Hadamard scheme, using only $n=\log M$ detectors. Moreover, another simple induction shows that the amplifier interferometer can be implemented with only $M-1$ balanced beam splitters.

C. Looped amplifier scheme

Noting the recursive character of the amplifier scheme, we present another possible implementation of the amplifier scheme using a looped beam splitter interaction, one single-photon threshold detector, and an active optical element, namely, an optical switch (Fig. 6).

This setup now uses an active optical element and a constant number of passive linear optical elements, and approximates a perfect projective measurement up to arbitrary precision. It works in the following manner. Initially, the states $|\alpha\rangle$ and $|\beta\rangle$ are mixed on a balanced beam splitter. This results in a probability of not obtaining a click in the detector D_0 given by

$$P_{\emptyset}(\alpha,\beta,1) = |\langle\alpha|\beta\rangle|. \tag{23}$$

If a click is detected in D_0, then one immediately concludes that $|\alpha\rangle \neq |\beta\rangle$. Otherwise, in the next iteration, the switch connects to the upper arm and the next interaction with the beam splitter results in

$$\left|\frac{\alpha+\beta}{\sqrt{2}}\right\rangle \otimes |\sqrt{2}\beta\rangle \rightarrow \left|\frac{\alpha+3\beta}{2}\right\rangle \otimes \left|\frac{\alpha-\beta}{2}\right\rangle_{D_0}, \tag{24}$$

where in the lower arm the amplitude of the new coherent pulse has been multiplied by $\sqrt{2}$. The coherent state $|\sqrt{2}\beta\rangle$ is produced using variable optical attenuator (VOA): an active optical element to prepare coherent states with desired amplitude by the varying the intensity in the attenuator. Iterating this over $n=\log M$ runs, where at the kth run, the upper arm corresponding the unmeasured output state interacts with the local state $|2^{(k-1)/2}\beta\rangle$ (produced using VOA) in the beam splitter, the probability that there is no click obtained D_0 over all the runs is the same as Eq. (22). Hence, by construction, the statistics of the setup after $n-1$ pulses $\{|\beta\rangle, \cdots |2^{(n-1)/2}\beta\rangle\}$ sent reproduce those of the amplifier scheme of size M.

The three schemes discussed provide experimentally friendly devices to perform a variety of quantum information processing tasks using coherent states, ranging from state comparison to programmable projective measurements. We show in the next section that these schemes are optimal for

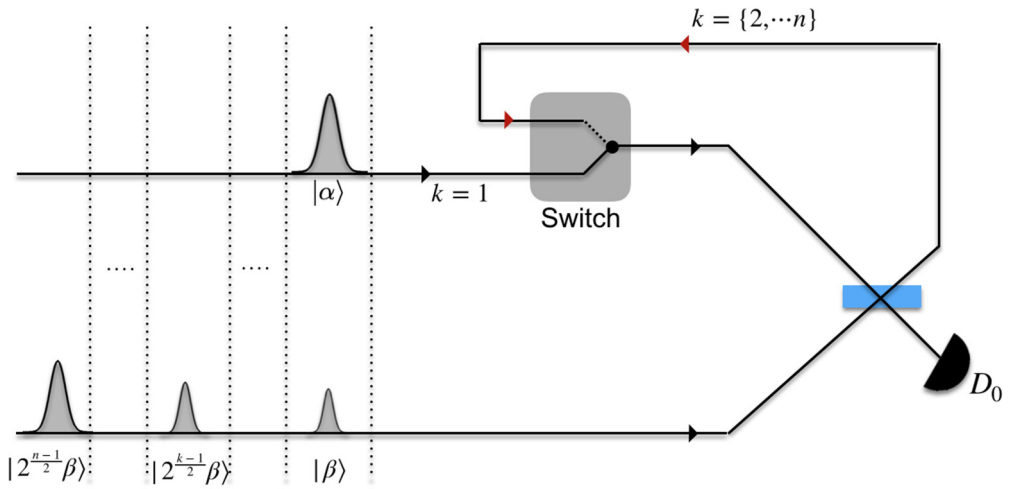

FIG. 6. The looped amplifier scheme. The coherent state $|\alpha\rangle$ is sent once, while at each loop a new coherent state $|2^{(k-1)/2}\rangle\,\beta$ for $k = \{1, ..n\}$, with $n = \log M$. The switch ensures a closed loop after the input state $|\alpha\rangle$ passes through. The clicks are collected in the detector D_0 for all the n instances of the beam-splitter interaction. In the ideal case, when $|\alpha\rangle = |\beta\rangle$, the detector D_0 does not click across any of the n instances. If the two states are different, however, there is a finite probability of a click across the n instances.

coherent state comparison under the one-sided error requirement.

IV. OPTIMALITY OF THE GENERALIZED TEST

An extension of the results in Ref. [16], which studies the problem of unambiguous comparison of unknown coherent states, proves the optimality of both the Hadamard scheme and the amplifier scheme for coherent state comparison, under the one-sided error requirement. In other terms, since these schemes satisfy the promise of perfect completeness, we show that they achieve minimal soundness.

A. Optimal POVM for comparing coherent states under the one-sided error requirement

Let $\{\Pi_0, \Pi_1\}$ be a POVM for comparing coherent states $|\alpha\rangle$ and $|\beta\rangle$ under the one-sided error requirement, when provided a single copy of $|\alpha\rangle$ and $M-1$ copies of $|\beta\rangle$ (the proof of Ref. [16] assumes $M = 2$). The operator Π_0 corresponds to saying that the states $|\alpha\rangle$ and $|\beta\rangle$ are the same, while the operator Π_1 corresponds to saying that they are different. These operators thus verify the following conditions:

$$\Pi_0, \Pi_1 \succeq 0, \;\; \Pi_0 + \Pi_1 = \mathbb{I}, \tag{25}$$

where $\mathbb{I}$ is the identity operator and

$$\forall \alpha \in \mathbb{C}, \;\; \mathrm{Tr}[\Pi_1 \, |\alpha\rangle \, \langle\alpha|^{\otimes M}] = 0, \tag{26}$$

where the last condition is the one-sided error requirement. Integrating this condition over $\mathbb{C}$ yields

$$0 = \int d^2\alpha \mathrm{Tr}[\Pi_1 \, |\alpha\rangle \, \langle\alpha|^{\otimes M}] = \mathrm{Tr}[\Pi_1 \Delta_M], \tag{27}$$

where we have defined

$$\Delta_M = \int d^2\alpha \, |\alpha\rangle \, \langle\alpha|^{\otimes M} \succeq 0. \tag{28}$$

Note that the condition in Eq. (27) is equivalent to the one-sided requirement in Eq. (26) because the operators Π_1 and $|\alpha\rangle \, \langle\alpha|^{\otimes M}$ are positive.

The operator $\frac{M}{\pi}\Delta_M$ is actually a projector. This result can be obtained by writing state $|\alpha\rangle$ in the Fock basis and an integration in polar coordinates, where $\alpha = re^{i\theta}$ (the derivation is detailed in Appendix A). From Eq. (28), we obtain

$$\Delta_M = \frac{\pi}{M} \sum_{N=0}^{\infty} \left|\chi_N^M\right\rangle\left\langle\chi_N^M\right|, \tag{29}$$

where we have defined for all $N \geqslant 0$,

$$\left|\chi_N^M\right\rangle := M^{-N/2} \sum_{\sum_j k_j = N} \sqrt{\frac{N!}{k_1! \ldots k_M!}} \, |k_1 \ldots k_M\rangle. \tag{30}$$

With the multinomial formula, we obtain $\langle\chi_N^M|\chi_N^M\rangle = 1$ for all $N \geqslant 0$, and since the states $|\chi_N^M\rangle$ have exactly N photons, we have $\langle\chi_N^M|\chi_{N'}^M\rangle = \delta_{N,N'}$ for all $N, N' \geqslant 0$. The states $|\chi_N^M\rangle$ thus are orthonormal and with Eq. (29), the operator $\frac{M}{\pi}\Delta_M$ is a projector.

By Eq. (27), the supports of Π_1 and $\frac{M}{\pi}\Delta_M$ are disjoint, and by Eq. (25) we see that $\Pi_0 + \Pi_1 = \mathbb{I}$, so the support of $\frac{M}{\pi}\Delta_M$ is included in the support of Π_0. The optimal POVM $\{\Pi_0^{\mathrm{opt}}, \Pi_1^{\mathrm{opt}}\}$ for state comparison minimizes the error probability, hence with the one-sided error requirement, Π_0^{opt} must have minimal support, meaning that

$$\Pi_0^{\mathrm{opt}} = \frac{M}{\pi}\Delta_M = \sum_{N=0}^{+\infty} \left|\chi_N^M\right\rangle\left\langle\chi_N^M\right| \quad \text{and} \quad \Pi_1^{\mathrm{opt}} = \mathbb{I} - \Pi_0^{\mathrm{opt}}. \tag{31}$$

Note that, with the same proof, this choice of POVM is also optimal in the generalized setting where one is given one unknown generic state (not necessarily a coherent state) and $M-1$ unknown coherent states, and is asked to test if all the states are identical or not.

B. The Hadamard interferometer is optimal for coherent state comparison

We now show that the Hadamard interferometer is optimal for coherent state comparison under the one-sided error requirement. Let $\{\Pi_0^h, \Pi_1^h\}$ be the POVM corresponding to the Hadamard interferometer with threshold detection of the last $M-1$ modes. Then,

$$\Pi_0^h = \hat{H}_n^\dagger \Pi_0^d \hat{H}_n, \tag{32}$$

where $\hat{H}_n$ is the unitary evolution corresponding to the action of the interferometer of order M defined in Eq. (10) in the M-mode infinite-dimensional Hilbert space, with $n = \log M$, and where

$$\Pi_0^d = \mathbb{I} \otimes |0\rangle\langle 0|^{\otimes(M-1)} \tag{33}$$

is the POVM operator corresponding to the event where none of the $M-1$ threshold detectors clicks. We obtain

$$\begin{aligned}\Pi_0^h &= \hat{H}_n^\dagger(\mathbb{I} \otimes |0\rangle\langle 0|^{\otimes(M-1)})\hat{H}_n \\ &= \sum_{N=0}^{+\infty} \hat{H}_n^\dagger(|N\rangle\langle N| \otimes |0\rangle\langle 0|^{\otimes(M-1)})\hat{H}_n. \end{aligned} \tag{34}$$

For $k = 1, \ldots, M$, we write $\hat{a}_k^\dagger$ the creation operator for the kth mode. For all $N \geqslant 0$, we have

$$\begin{aligned}\hat{H}_n^\dagger(|N\rangle \otimes |0\rangle^{\otimes(M-1)}) &= \frac{1}{\sqrt{N!}}\hat{H}_n^\dagger(\hat{a}_1^\dagger)^N|0\rangle^{\otimes M} \\ &= \frac{M^{-N/2}}{\sqrt{N!}}(\hat{a}_1^\dagger + \cdots + \hat{a}_M^\dagger)^N|0\rangle^{\otimes M} \\ &!= \left|\chi_N^M\right\rangle, \end{aligned} \tag{35}$$

where we have used $\hat{H}_n|0\rangle^{\otimes M} = |0\rangle^{\otimes M}$, $\hat{H}_n^\dagger\hat{H}_n = \mathbb{I}$, $\hat{H}_n^\dagger\hat{a}_1^\dagger\hat{H}_n = \frac{\hat{a}_1^\dagger+\cdots+\hat{a}_M^\dagger}{\sqrt{M}}$, the multinomial formula, and Eq. (30). With Eqs. (31) and (34), we obtain $\Pi_0^h = \Pi_0^{\text{opt}}$, which concludes the proof.

Given that the statistics obtained with the amplifier scheme and the looped amplifier scheme mimic those of the Hadamard scheme, these schemes are also optimal for the same state comparison task.

V. ANALYSIS WITH EXPERIMENTAL IMPERFECTIONS FOR $M = 4$ MODES

While these devices are relatively easy to implement, any implementation would suffer from experimental imperfections. In this section, we analyze the performance of the amplifier scheme in presence of such imperfections. There are three major sources of error: (i) limited detector efficiency and channel transmission loss, characterized by a parameter $0 \leqslant \eta \leqslant 1$. This changes the coherent state α to $\sqrt{\eta}\alpha$, thus reducing the probability of obtaining a click using a single-photon threshold detector by a factor η; (ii) limited beam splitter visibility $0 \leqslant \nu \leqslant 1$, which may lead to a click in the wrong detector; (iii) dark counts in the detectors characterized by a probability p_{dark}. For our analysis, the click probability due to the coherent states is $O(1)$ and thus significantly larger than the dark count probability p_{dark} ($\sim 10^{-8}$) observed in the standard commercially available superconducting nanowire single photon detectors. The effects of dark count can thus be safely ignored and we only consider the effects of limited detector efficiency and channel transmission loss together with limited beam splitter visibility.

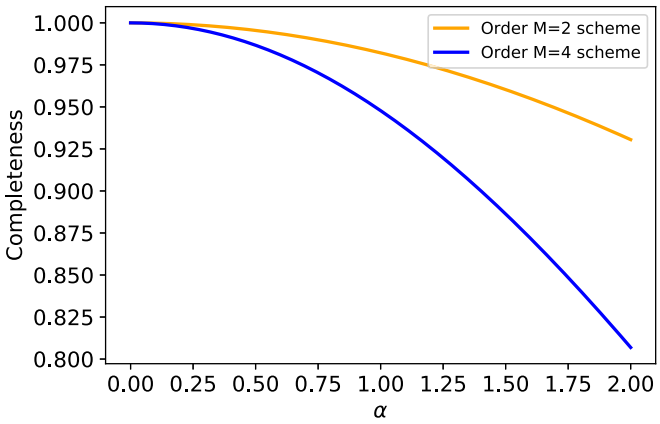

FIG. 7. Comparison of the completeness for $M = 2$ and $M = 4$ schemes in presence of experimental noise, as a function of the amplitude of the measured state. Here, we have chosen the experimental imperfection parameters $\eta = 0.9$, $\nu = 0.99$ as observed in standard optical setups.

For $M = 2$, when the input $|\alpha\rangle$, $|\beta\rangle$ is fed in an imperfect beam splitter, the transformation from input modes to output modes is the following:

$$|\alpha\rangle \otimes |\beta\rangle \mapsto |\sqrt{\nu}k_+ + \sqrt{1-\nu}k_-\rangle \otimes |\sqrt{\nu}k_- + \sqrt{1-\nu}k_+\rangle\,, \tag{36}$$

where $k_+ = (\alpha+\beta)/\sqrt{2}$ and $k_- = (\alpha-\beta)/\sqrt{2}$. The corresponding unitary transformation is

$$H' = \frac{1}{\sqrt{2}}\begin{pmatrix} A & B \\ A & -B \end{pmatrix}, \tag{37}$$

where $A = \sqrt{\nu} + \sqrt{1-\nu}$, and $B = \sqrt{\nu} - \sqrt{1-\nu}$.

Next, we consider the case of $M = 4$ spatial modes (Fig. 4), indexed from 0 to 3. We apply the imperfect transformation on the input $|\alpha\beta\beta\beta\rangle$. This results in

$$|\alpha\beta\beta\beta\rangle \mapsto U_2'|\alpha\beta\beta\beta\rangle = |\delta_0\delta_1\delta_2\delta_3\rangle\,, \tag{38}$$

where from Eq. (20) we derive

$$\begin{aligned} U_2' &= H_{0,2}' \times (H_{0,1}' \oplus H_{2,3}') \\ &= \begin{pmatrix} \frac{1}{2}A^2 & \frac{1}{2}AB & \frac{1}{2}AB & \frac{1}{2}B^2 \\ \frac{1}{\sqrt{2}}A & -\frac{1}{\sqrt{2}}B & 0 & 0 \\ \frac{1}{2}A^2 & \frac{1}{2}AB & -\frac{1}{2}AB & -\frac{1}{2}B^2 \\ 0 & 0 & \frac{1}{\sqrt{2}}A & -\frac{1}{\sqrt{2}}B \end{pmatrix}, \end{aligned} \tag{39}$$

with $A = \sqrt{\nu} + \sqrt{1-\nu}$ and $B = \sqrt{\nu} - \sqrt{1-\nu}$. We thus obtain

$$\delta_1 = \frac{A\alpha - B\beta}{\sqrt{2}} \quad \text{and} \quad \delta_2 = \frac{A^2\alpha - B^2\beta}{2}. \tag{40}$$

Adding the channel and detector losses η, the output is mapped as $\delta_k \mapsto \sqrt{\eta}\delta_k$, for all k.

Similar to the analysis without experimental imperfections, the output modes 1 and 2 of the imperfect amplifier

interferometer are measured, with the coherent state input being $|\alpha\beta\beta\beta\rangle$. The probability $\mathbb{P}_\emptyset$ that none of the two detectors clicks is

$$\mathbb{P}_\emptyset(\alpha, \beta, \nu, \eta, M = 4) = \exp(-\eta(|\delta_1|^2 + |\delta_2|^2)). \quad (41)$$

Assigning to the detection event *no detector clicks*, the value 0, and to other detection events, i.e., *at least one of the detectors clicks*, the value 1, we obtain a device whose statistics mimic those of a projective measurement.

Completeness: When the states are the same, the correctness, which is the probability of not obtaining the detection event 1 is

$$c_4^{\text{exp}} = \mathbb{P}_\emptyset(\alpha, \alpha, \nu, \eta, 4) = \exp(-2\eta(1-\nu)(1+2\nu)|\alpha|^2). \quad (42)$$

We observe that if $\nu = 1$ (no imperfections), then $c_4^{\text{exp}} = 1$, thus we obtain perfect completeness.

Comparison of completeness with the $M = 2$ scheme: The analogous completeness in $M = 2$ scheme is

$$c_2^{\text{exp}} = \mathbb{P}_\emptyset(\alpha, \alpha, \nu, \eta, 2) = \exp(-2\eta(1-\nu)|\alpha|^2). \quad (43)$$

From Eqs. (43) and (42), we observe that $c_2^{\text{exp}} \leqslant c_4^{\text{exp}}$, which implies that the completeness in the $M = 4$ scheme is less than the completeness in $M = 2$ scheme. This is illustrated in Fig. 7, which compares the $M = 2$ and $M = 4$ settings for experimental parameters $\eta = 0.9$ and $\nu = 0.99$. The reduction in completeness probability for the $M = 4$ scheme is precisely what accounts for an increase in soundness probability (when the input and program register states are different), which we detail in the next paragraph.

Soundness: If the states are different, the probability of obtaining the detection event 1 (soundness) is computed in Appendix B and given by

$$s_4^{\text{exp}} = 1 - \exp\Big[-\eta\big(\nu^2 - \tfrac{1}{4}\big)|\alpha-\beta|^2 - \eta((1+2\nu)(1-\nu) + 2\sqrt{\nu(1-\nu)})|\alpha|^2 - \eta((1+2\nu)(1-\nu) - 2\sqrt{\nu(1-\nu)})|\beta|^2\Big]. \quad (44)$$

The analogous soundness for the $M = 2$ scheme with experimental imperfections reads

$$s_2^{\text{exp}} = 1 - \exp\Big[-\eta\big(\nu - \tfrac{1}{2}\big)|\alpha-\beta|^2 - \eta(1-\nu+\sqrt{\nu(1-\nu)})|\alpha|^2 - \eta(1-\nu-\sqrt{\nu(1-\nu)})|\beta|^2\Big]. \quad (45)$$

In the absence of any experimental imperfections, it is straightforward to see that s_4 is always greater than s_2. We observe in Fig. 8 that this also holds in the presence of experimental imperfections with parameters $\eta = 0.9$ and $\nu = 0.99$, for a fixed program coherent state amplitude $\beta = 1$. Further, we also analytically show that, even with experimental imperfections, $s_4^{\text{exp}} \geqslant s_2^{\text{exp}}$ for all values of quantum efficiency η, visibility factor ν, and program coherent state amplitude β (see Appendix C). Thus, the $M = 4$ scheme outperforms the $M = 2$ scheme in soundness. We note the similar gain in the soundness is expected when comparing $M = 2$ scheme with the scheme involving any arbitrary M value. For simplicity, we have shown the comparison for $M = 2$ and $M = 4$ schemes.

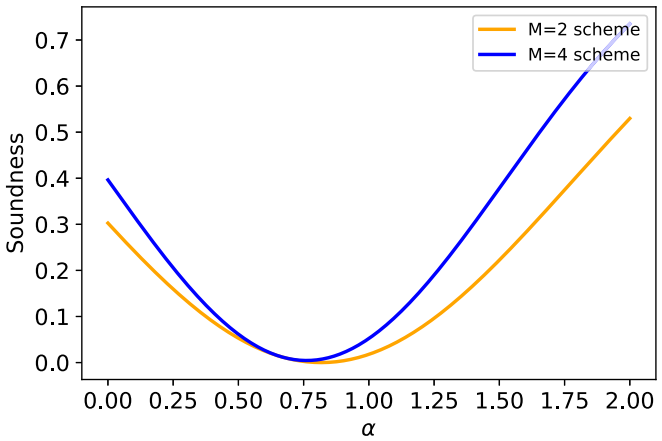

FIG. 8. Comparison of the soundness for $M = 2$ and $M = 4$ schemes in presence of experimental noise parameters $\eta = 0.9$, $\nu = 0.99$, for a fixed program state amplitude $\beta = 1$.

VI. STATE COMPARISON FOR AN UNTRUSTED SOURCE

We now consider an adversarial scenario where the unknown state in the input register is not restricted to being a coherent state but can be any generic (mixed) quantum state produced by some untrusted party, while the states in the program register are coherent states obtained from a trusted source. The task is then to check whether the states in the input and program registers are equal. We first analyze this state comparison task under one-sided error when the program register contains a single coherent state $|\beta\rangle$. Subsequently, we generalize the state comparison procedure by allowing multiple copies of $|\beta\rangle$ in the program register. We note that in both settings, we receive only a single unknown state from the untrusted source. We conclude this section by proving that our scheme is optimal for state comparison even when we do not make any assumption whatsoever about the state in the input register.

A. State comparison with a single copy of the test and program register states

We consider the scenario where the input register state is a generic quantum state τ and the program register state is a coherent state $|\beta\rangle$. Any single-mode state τ can be expressed in the Fock basis as

$$\tau = \sum_{k,l \geqslant 0} \tau_{kl} |k\rangle \langle l|, \quad (46)$$

with the normalization condition $\sum_{n\geqslant 0} \tau_{nn} = 1$, coming from from $\text{Tr}(\tau) = 1$.

Let us look at the completeness and soundness arguments again:

Completeness: If the states τ and $|\beta\rangle$ are the same, then their trace distance is 0. Thus, the probability of having the detection event 1 is zero. This ensures perfect completeness again, i.e., $c_2 = 1$.

Soundness: Trace distance. Suppose $\|\tau - |\beta\rangle\langle\beta|\|_{\rm tr} \geqslant \epsilon$. This implies

$$\sqrt{1 - \langle\beta|\tau|\beta\rangle} \geqslant \epsilon, \tag{47}$$

so $\langle\beta|\tau|\beta\rangle \leqslant 1 - \epsilon^2$. We show in Appendix D that the probability of obtaining a click in the detector D_0 after the interaction of the states τ and $|\beta\rangle$ in the balanced beam splitter is tightly lower bounded as

$$\begin{aligned}\mathbb{P}_{D_0} &\geqslant \frac{1}{2}(1 - \langle\beta|\tau|\beta\rangle) \\ &\geqslant \frac{\epsilon^2}{2}.\end{aligned} \tag{48}$$

Thus the soundness in this case is $s_2 \geqslant \frac{\epsilon^2}{2}$, where ϵ is any lower bound to the trace distance between the program and tested states.

B. Generalized single run state comparison

The generalized single run state comparison scheme is run on a single unknown state τ [Eq. (46)] in the input register and $M - 1$ coherent states $|\beta\rangle$ in the program register. Here we analyze the completeness and soundness of the *amplifier scheme* used for comparison as described in Sec. III B.

Completeness: If states τ and $|\beta\rangle$ are the same, then their trace distance is 0 and the probability of a click in at least one of the detectors in output modes 2^k is 0. Thus, we obtain perfect completeness $c_M = 1$.

Soundness: Suppose $\|\tau - |\beta\rangle\langle\beta|\|_{\rm tr} \geqslant \epsilon$, so $\langle\beta|\tau|\beta\rangle \leqslant 1 - \epsilon^2$. We show in Appendix E that the probability that at least one of the detectors in output modes 2^k clicks after the interaction of the states τ and $|\beta\rangle$ in the balanced beam splitter is tightly lower bounded as

$$\begin{aligned}\mathbb{P}_D &\geqslant \left(1 - \frac{1}{M}\right)(1 - \langle\beta|\tau|\beta\rangle) \\ &\geqslant \left(1 - \frac{1}{M}\right)\epsilon^2.\end{aligned} \tag{49}$$

Thus, the soundness in this case is $s_M \geqslant (1 - \frac{1}{M})\epsilon^2 > s_2$ for $M > 2$. The bound improves by adding more copies of the program register states, as can be expected.

C. Test optimality

The proof of optimality derived in Sec. IV holds even when the input register state is a generic mixed state, as long as the program register states are coherent states. Indeed, the optimal POVM for state comparison, when one has a single copy of input register state and $M - 1$ copies of the program register states is derived, assuming it satisfies the completeness relation in Eq. (26), which is also the case here. This implies that the optimal POVM when the tested state is generic, while the program register states are coherent states, is the same as the one constructed in Sec. IV. This proves the optimality of our proposed projective schemes in this generalized setting.

VII. IMPROVED QUANTUM FINGERPRINTING

Our schemes allow us to improve the soundness of quantum information protocols which use swap tests of coherent states as a subroutine. As a concrete example of an application of our generalized state comparison schemes, we consider the improvement in performance of a specific quantum communication protocol: the quantum fingerprinting protocol for estimating the Euclidean distance of two real vectors within a constant factor. Our model of study is the simultaneous message passing model of communication complexity [6].

The communication task is as follows. Two parties, Alice and Bob, receive data sets x and y, respectively, which are unit vectors in $\mathbb{R}^n$. They are interested in checking the similarity of their data sets, through a referee, by estimating the (square of the) Euclidean distance of their vectors, $||x - y||_2^2 = \sum_{j=1}^n (x_j - y_j)^2$ within some multiplicative constant ϵ with a probability at least $1 - \delta$.

A trivial solution to this problem would be Alice and Bob transmitting the strings x and y, respectively, to the referee. This, however, is a nonoptimal protocol in terms of communication resources (number of bits sent to referee) when the task is only to approximate the Euclidean distance. As we show, the task can be solved with much lower communication resources when Alice and Bob send the fingerprints of their data sets, which would typically be of much shorter lengths while still allowing the referee to estimate the Euclidean distance within some constant. When we restrict the model to Alice and Bob sharing no randomness, the classical fingerprint size necessary to solve this problem is $\Omega(\sqrt{n})$ (the lower bound in the classical communication complexity needed to solve the Euclidean distance within a constant ϵ with an error probability at most $\delta \in [0, \frac{1}{2}]$ is $2\sqrt{g(\delta)\sqrt{n} - g(\delta)} - 6$, where $g(x) = 2(0.5 - x)^2 \log e$) [17–20].

Motivated by the original quantum fingerprinting protocol of Buhrman *et al.* [2] to check for the equality of two n-bit strings, Kumar *et al.* [6] proposed a coherent state quantum fingerprinting protocol to estimate the Euclidean distance with $O(\log n)$ qubits, which is asymptotically exponentially shorter in size compared to the classical fingerprints. We note that a similar improvement in resources for approximately checking the equality of the two bit strings problem was proposed by Ref. [3] in the coherent state framework and subsequently demonstrated in Refs. [4,15].

A. Quantum fingerprinting protocol to approximate the Euclidean distance

Here we review the coherent state fingerprinting protocol proposed by Ref. [6] to approximate the Euclidean distance. Alice and Bob prepare quantum fingerprints of their data sets, which are a sequence of coherent pulses in n modes, and send these to the referee. Alice (similarly, Bob) prepares her state $|1_x\rangle$ by applying the displacement operator $\hat{D}_x(1) = \exp(\hat{a}_x^\dagger - \hat{a}_x)$ to the vacuum state, where $\hat{a}_x = \sum_{j=1}^n x_j \hat{b}_j$ is the superposed annihilation operator [3] and $\hat{b}_j$ is the photon annihilation operator of the jth mode. The coherent state fingerprint of Alice is then

$$|1_x\rangle = \hat{D}_x(1)|0\rangle = \otimes_{j=1}^n |x_j\rangle_j, \tag{50}$$

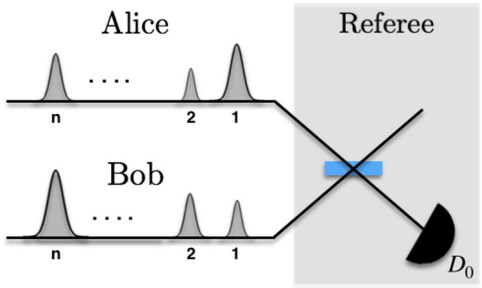

FIG. 9. Alice and Bob prepare coherent state fingerprints, $|1_x\rangle$ and $|1_y\rangle$, as a sequence of coherent pulses in n modes, with the jth mode amplitude encoding the information of jth component of the vector. This is then interfered sequentially in the balanced beam splitter and the results are analyzed in single-photon threshold detector D_0.

where $|x_j\rangle_j$ is a coherent state of amplitude x_j occupying the jth mode. The mean photon number for state $|1_x\rangle$ is given by $\mu = \sum_j |x_j|^2 = 1$, independent of the input size. This scheme is illustrated in Fig. 9.

The referee interacts the coherent fingerprints from Alice and Bob sequentially using a balanced beam splitter and observes the single-photon clicks in a threshold detector D_0. The input of the interaction is

$$|1_x\rangle \otimes |1_y\rangle = \bigotimes_{j=1}^{n} |x_j\rangle_j \otimes |y_j\rangle_j . \tag{51}$$

The output in the mode corresponding to the detector D_0 at the jth pulse is $|\frac{x_j - y_j}{\sqrt{2}}\rangle_j$. Let Z_j be the binary random variable which equals 1 with the probability that the detector D_1 clicks at the jth pulse, namely, $p_j = 1 - \exp(-\frac{(x_j-y_j)^2}{2}) \approx \frac{(x_j-y_j)^2}{2}$. The latter approximation holds true since x and y are unit vectors in $\mathbb{R}^n$ and for large n the terms $(x_j - y_j)^2$ are typically of the order of $1/n$. The Euclidean distance ($\tilde{E}$) is equal to

$$\tilde{E} = 2 \cdot \mathbb{E}\left[\sum_{j=1}^{n} Z_j\right]. \tag{52}$$

The Chernoff-Hoeffding inequality [21] can then be used to estimate $\tilde{E}$ with $\sum_{j=1}^{n} Z_j$ within a mutiplicative precision $\epsilon > 0$:

$$\mathbb{P}\left[\left|\sum_{i=1}^{n} Z_j - \frac{\tilde{E}}{2}\right| \geqslant \epsilon \frac{\tilde{E}}{2}\right] \leqslant 2\exp\left(-\frac{\epsilon^2 \tilde{E}}{6}\right). \tag{53}$$

Equation (53) provides the referee with the estimation of the Euclidean distance between two unit vectors x and y within a desired multiplicative precision ϵ, with a success probability at least $1 - 2\delta$, with $\delta = \exp(-\frac{\epsilon^2 \tilde{E}}{6})$ in a single run.

For the coherent state fingerprint with an average photon number $\mu = 1$ across n time modes, the fingerprint size (transmitted information) is $O(\log n)$. Thus, the estimation of the Euclidean distance within (ϵ, δ) requires Alice and Bob each to send exponentially smaller sized fingerprints to the referee than the classical analog of $O(\sqrt{n})$.

B. Improved quantum fingerprint protocol

Here we consider the performance of our generalized state comparison method and demonstrate that, in a single run, the referee is able to estimate the Euclidean distance of two vectors $x, y \in \mathbb{R}^n$ with substantially better probability than the original fingerprinting protocol.

The setting is as follows: Similar to the protocol of Ref. [6], Alice and Bob prepare their quantum fingerprints $|1_x\rangle$ and $|1\rangle_y$, respectively, as a sequence of coherent pulses in n modes. Here, one of the parties, say Alice, sends a single copy of the fingerprint state to the referee, while Bob sends multiple, $M - 1$, copies of the fingerprint state to the referee. Figure 10 illustrates the setting where, upon receiving the fingerprint states, the referee applies the projective measurement scheme. Here we showcase the *amplifier scheme* but the same results are obtained using the *Hadamard* and *looped amplifier* schemes.

The referee applies the generalized amplifier interferometer $U_{\log M}$ of Eq. (21) to the incoming states. The clicks are then collected in the $\log M$ threshold detectors indexed as $D : \{D_0, D_1, \ldots, D_{\log M - 1}\}$.

Let $Z_{j,k}$ be the binary random variable that is 1 with the probability that the detector indexed D_k clicks at the jth pulse, with $j \in \{1, \ldots, n\}$ and $k \in \{0, \ldots, \log M - 1\}$, namely, $p_{j,k} = 1 - \exp(-\frac{(x_j-y_j)^2}{2^{k+1}}) \approx \frac{(x_j-y_j)^2}{2^{k+1}}$. Again the approximation holds true since x and y are unit vectors in $\mathbb{R}^n$ and for large n the terms $(x_j - y_j)^2$ are typically of the order of $1/n$. The Euclidean distance ($\tilde{E}$) in this case is equal to

$$\tilde{E} = \frac{1}{1 - \frac{1}{M}} \cdot \mathbb{E}\left[\sum_{j=1,k=0}^{n,\log M-1} Z_{j,k}\right]. \tag{54}$$

Once again, the Chernoff-Hoeffding inequality can be used to estimate $\tilde{E}$ with $\sum_{j=1,k=0}^{n,\log M-1} Z_{j,k}$ within a multiplicative precision $\epsilon > 0$:

$$\begin{aligned}\mathbb{P}\left[\left|\sum_{j=1,k=0}^{n,\log M-1} Z_{j,k} - \left(1 - \frac{1}{M}\right)\tilde{E}\right| \geqslant \epsilon\left(1 - \frac{1}{M}\right)\tilde{E}\right] &\leqslant 2\exp\left(-\epsilon^2\left(1 - \frac{1}{M}\right)^2 \frac{\tilde{E}}{3}\right) \\ &\leqslant 2\delta^{2(1-\frac{1}{M})},\end{aligned} \tag{55}$$

where 2δ is the failure probability in estimating the Euclidean distance in the original fingerprint protocol.

With the improved quantum fingerprinting protocol, we conclude with Eq. (55) that the Euclidean distance between two vectors x and y can be estimated within an additive factor ϵ with a probability $1 - 2\delta^{2(1-\frac{1}{M})}$, which is better than the original protocol by a factor $2(1 - \frac{1}{M}) > 1$ for all $M > 2$. For example, $M = 4$ already provides a power 1.5 improvement in the probability of successfully estimating the Euclidean distance.

We note that when Bob sends $M - 1$ coherent state fingerprints to the referee, this leads to the total transmitted information to be $M \times O(\log n)$. As long as M is independent of n, we still achieve an asymptotic exponential reduction in

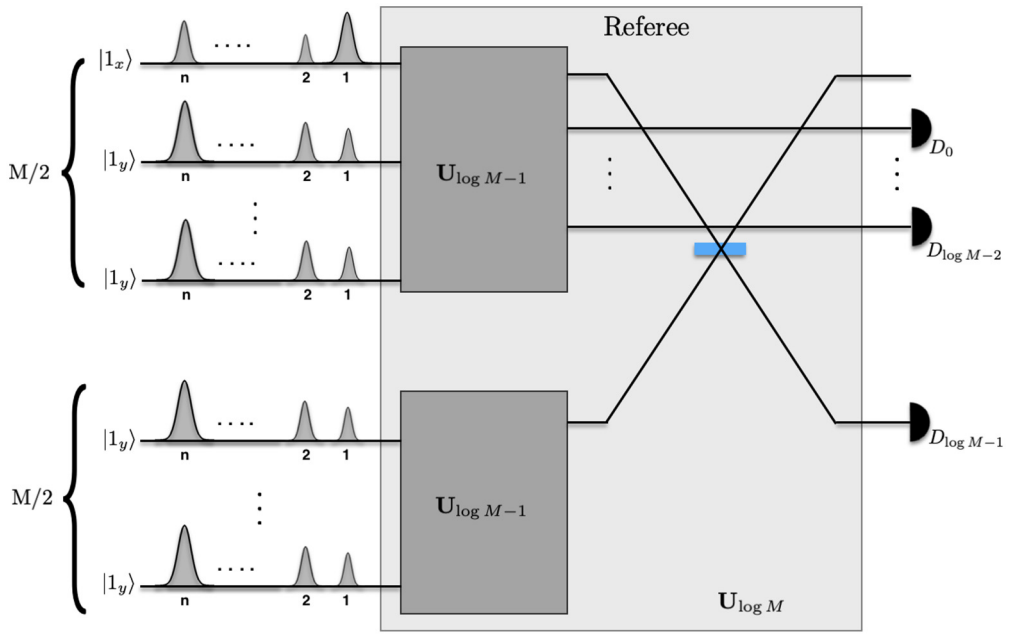

FIG. 10. Improved quantum fingerprinting protocol where Alice sends a single copy of $|1\rangle_x$ to the referee while Bob sends $M-1$ copies of the fingerprint $|1_y\rangle$ to the referee. Here the referee employs the *amplifier scheme* with $M-1$ beam splitters and $\log M$ threshold detectors $\{D_0, D_1, \ldots, D_{\log M-1}\}$.

transmitted information compared to the classical analog of $O(\sqrt{n})$.

VIII. DISCUSSION

We have presented an optimal programmable measurement scheme that projects the incoming single-mode state in the input register onto a local coherent state in the program register. Our scheme is implemented using balanced beam splitters and single-photon threshold detectors. Our implementation of this interferometer is efficient, and threshold detectors with high efficiency and low dark counts are commercially available [22]. Our most efficient scheme in terms of optical components, the *looped amplifier scheme*, requires only a single beam splitter and a single threshold detector, together with an optical switch. We have further generalized our schemes to a cryptographic setting where the input register state is obtained from an untrusted source and is no longer assumed to be a coherent state.

This universal implementation using coherent states as program states can act as a backbone in improving the performance of a range of quantum protocols in communication complexity [2,23], cryptography, and computational regimes [24–29]. For example, it has been shown that communication protocols using coherent state fingerprints provide an asymptotic exponential advantage in communication resources in estimating the Euclidean distance between two vectors compared to any classical protocol [6]. For this protocol, we show a further quadratic improvement in the probability of correctly estimating the Euclidean distance compared to the original protocol.

The general applicability of our optimal state comparison schemes makes them attractive and easy to implement. Another feature that we bring is that the output quantum states are not completely destroyed after the performing the comparison test. Further, the output states carry the overlap information of the unknown quantum test.

ACKNOWLEDGMENTS

We thank Frédéric Grosshans for useful discussions. N.K. and E.K. acknowledge the support of UK Engineering and Physical Sciences Research Council Grant No. EP/N003829/1. D.M. acknowledges the funding from the ANR through the ANR-17-CE24-0035 VanQuTe project. E.D. acknowledges financial support from the European Research Council QUSCO, Starting Grant (StG), PE7, ERC-2017-STG.

N.K. and U.C. conceptualized the idea and wrote the proofs. All authors contributed in preparing the paper.

APPENDIX A: COMPUTING THE EXPRESSION OF THE OPERATOR Δ_M IN FOCK BASIS

Using the notations of the main text, and writing

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{+\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \tag{A1}$$

we obtain

$$\begin{aligned}
\Delta_M &= \int d^2\alpha\ \exp[-M|\alpha|^2] \sum_{\substack{k_j,\,l_j=0\\ \forall j\in[M]}}^{\infty} \frac{\alpha^{\sum_j k_j}(\alpha^*)^{\sum_j l_j}}{\sqrt{k_1!\ldots k_M! l_1!\ldots l_M!}}\,|k_1\ldots k_M\rangle\langle l_1\ldots l_M| \\
&= \sum_{k_j,\,l_j=0}^{\infty} \frac{|k_1\ldots k_M\rangle\langle l_1\ldots l_M|}{\sqrt{k_1!\ldots k_M! l_1!\ldots l_M!}} \int_{r=0}^{\infty} dr\ \exp[-Mr^2] r^{1+\sum_j k_j+l_j} \int_{\theta=0}^{2\pi} d\theta\ \exp\left[i\theta\sum_j (k_j-l_j)\right] \\
&= \frac{\pi}{M}\sum_{k_j,\,l_j=0}^{\infty} \frac{\delta_{\sum_j k_j,\sum_j l_j}}{M^{\frac{\sum_j k_j}{2}} M^{\frac{\sum_j l_j}{2}}} \sqrt{\frac{\left(\sum_j k_j\right)!\left(\sum_j l_j\right)!}{k_1!\ldots k_M! l_1!\ldots l_M!}}\,|k_1\ldots k_M\rangle\langle l_1\ldots l_M| \\
&= \frac{\pi}{M}\sum_{N=0}^{\infty} \sum_{\substack{\sum_j k_j=N\\ \sum_j l_j=N}} M^{-N} \sqrt{\frac{N!}{k_1!\ldots k_M!}}\sqrt{\frac{N!}{l_1!\ldots l_M!}}\,|k_1\ldots k_M\rangle\langle l_1\ldots l_M| \\
&= \frac{\pi}{M}\sum_{N=0}^{\infty} \left|\chi_N^M\right\rangle\!\left\langle\chi_N^M\right|,
\end{aligned} \tag{A2}$$

where we have defined for all $N \geqslant 0$,

$$\left|\chi_N^M\right\rangle = M^{-N/2} \sum_{\sum_j k_j=N} \sqrt{\frac{N!}{k_1!\ldots k_M!}}\,|k_1\ldots k_M\rangle. \tag{A3}$$

APPENDIX B: COMPUTING THE SOUNDNESS FOR $M = 4$

When the states are different, the probability of obtaining the detection event 0 (failure probability) is

$$P_f(M=4) = 1 - s_4 = \exp\left(-\frac{\eta}{4}A\right), \tag{B1}$$

where

$$\begin{aligned}
A &= 2|\sqrt{\nu}(\alpha-\beta) + \sqrt{1-\nu}(\alpha+\beta)|^2 + |\alpha-\beta+2\sqrt{\nu(1-\nu)}(\alpha+\beta)|^2 \\
&= (1+2\nu)|\alpha-\beta|^2 + 2(1+2\nu)(1-\nu)|\alpha+\beta|^2 + 8\sqrt{\nu(1-\nu)}(|\alpha|^2-|\beta|^2),
\end{aligned} \tag{B2}$$

where we used $(\alpha-\beta)(\alpha+\beta)^* + (\alpha-\beta)^*(\alpha+\beta) = 2|\alpha|^2 - 2|\beta|^2$. Using $|\alpha+\beta|^2 = 2|\alpha|^2 + 2|\beta|^2 - |\alpha-\beta|^2$, we obtain

$$A = (4\nu^2-1)|\alpha-\beta|^2 + 4[(1+2\nu)(1-\nu) + 2\sqrt{\nu(1-\nu)}]|\alpha|^2 + 4[(1+2\nu)(1-\nu) - 2\sqrt{\nu(1-\nu)}]|\beta|^2. \tag{B3}$$

APPENDIX C: COMPARING THE SOUNDNESS FOR $M = 2$ TO THE SOUNDNESS FOR $M = 4$

We show in this section that $s_2^{\exp} \leqslant s_4^{\exp}$ for all α, β. We have

$$\begin{aligned}
s_2^{\exp} &= 1 - \exp\big[-\eta\big(\nu-\tfrac{1}{2}\big)|\alpha-\beta|^2 - \eta(1-\nu+\sqrt{\nu(1-\nu)})|\alpha|^2 \\
&\quad - \eta(1-\nu-\sqrt{\nu(1-\nu)})|\beta|^2\big] \\
&\equiv 1 - \exp[-\eta A_2],
\end{aligned} \tag{C1}$$

and

$$\begin{aligned}
s_4^{\exp} &= 1 - \exp\big[-\eta\big(\nu^2-\tfrac{1}{4}\big)|\alpha-\beta|^2 \\
&\quad - \eta((1+2\nu)(1-\nu) + 2\sqrt{\nu(1-\nu)})|\alpha|^2 \\
&\quad - \eta((1+2\nu)(1-\nu) - 2\sqrt{\nu(1-\nu)})|\beta|^2\big] \\
&\equiv 1 - \exp[-\eta A_4].
\end{aligned} \tag{C2}$$

Since the function $x \mapsto 1 - e^{-x}$ is increasing, it is sufficient to show that $A_2 \leqslant A_4$ for all α, β. Writing $\alpha = re^{i\phi}$ and $\beta = te^{i\psi}$, where $r, t \geqslant 0$ and $\phi, \psi \in [0, 2\pi]$, we obtain

$$A_4 - A_2 = \big(\tfrac{1}{4} + \nu(1-\nu) + \sqrt{\nu(1-\nu)}\big)r^2 + \big(\tfrac{1}{4} + \nu(1-\nu) - \sqrt{\nu(1-\nu)}\big)t^2 - 2rt\big(\tfrac{1}{4} - \nu(1-\nu)\big)\cos(\phi-\psi). \tag{C3}$$

This last expression is a polynomial of degree 2 in r, with a positive leading coefficient. Thus, if its discriminant is negative, then the expression is always positive. The discriminant is

$$\begin{aligned}\Delta &= 4t^2\Big[\big(\tfrac{1}{4}-\nu(1-\nu)\big)^2\cos(\phi-\psi)^2-\big(\tfrac{1}{4}+\nu(1-\nu)+\sqrt{\nu(1-\nu)}\big)\big(\tfrac{1}{4}+\nu(1-\nu)-\sqrt{\nu(1-\nu)}\big)\Big]\\ &\leqslant -6t^2\nu(1-\nu)\\ &\leqslant 0,\end{aligned} \tag{C4}$$

where the third line is obtained by using $\cos(\phi-\psi)\leqslant 1$. Hence, for all experimental parameters within the error model we consider, we have $s_2^{\exp}\leqslant s_4^{\exp}$.

APPENDIX D: SOUNDNESS FOR A GENERIC INPUT STATE WITH $M = 2$

By linearity of the probabilities, it is sufficient to prove Eq. (48) when τ is a pure state.

Let us write $\tau = |\psi\rangle\langle\psi|$, where $|\psi\rangle = \sum_{n\geqslant 0}\psi_n|n\rangle$, where $\sum_{n\geqslant 0}|\psi_n|^2 = 1$. We first show Eq. (48) for $\beta = 0$. In that case, the two-mode input state is

$$\begin{aligned}|\psi\rangle_a\otimes|0\rangle_b &= \sum_{n\geqslant 0}\psi_n|n\rangle_a\otimes|0\rangle_b\\ &= \sum_{n\geqslant 0}\frac{\psi_n}{\sqrt{n!}}(\hat{a}^\dagger)^n|0\rangle_a\otimes|0\rangle_b,\end{aligned} \tag{D1}$$

where $\hat{a}^\dagger$ is the creation operator corresponding to the input mode of $|\psi\rangle$. Writing $\hat{c}^\dagger$ and $\hat{d}^\dagger$, the creation operators of the output modes after the balanced beam splitter evolution $\hat{H}$, the output state is given by

$$\begin{aligned}\hat{H}|\psi\rangle_a\otimes|0\rangle_b &= \sum_{n\geqslant 0}\frac{\psi_n}{\sqrt{n!}}\left(\frac{\hat{c}^\dagger+\hat{d}^\dagger}{\sqrt{2}}\right)^n|0\rangle_c\otimes|0\rangle_d\\ &= \sum_{n\geqslant 0}\frac{\psi_n}{2^{n/2}\sqrt{n!}}\sum_{k=0}^{n}\binom{n}{k}(\hat{c}^\dagger)^k(\hat{d}^\dagger)^{n-k}|0\rangle_c\otimes|0\rangle_d\\ &= \sum_{n\geqslant 0}\frac{\psi_n}{2^{n/2}}\sum_{k=0}^{n}\sqrt{\binom{n}{k}}|k\rangle_c\otimes|n-k\rangle_d.\end{aligned} \tag{D2}$$

The probability that the detector D_0, corresponding to the output mode d, does not click is given by

$$\begin{aligned}\mathbb{P}_\emptyset &= \mathrm{Tr}[(\mathbb{I}_c\otimes|0\rangle\langle 0|_d)\hat{H}|\psi\rangle\langle\psi|_a\otimes|0\rangle\langle 0|_b\hat{H}^\dagger]\\ &= \sum_{n,m\geqslant 0}\frac{\psi_n\psi_m^*}{2^{(n+m)/2}}\sum_{k=0}^{n}\sum_{l=0}^{m}\sqrt{\binom{n}{k}\binom{m}{l}}\mathrm{Tr}[(\mathbb{I}_c\otimes|0\rangle\langle 0|_d)(|k\rangle\langle l|_c\otimes|n-k\rangle\langle m-l|_d)]\\ &= \sum_{n\geqslant 0}\frac{|\psi_n|^2}{2^n}\\ &\leqslant |\psi_0|^2+\frac{1}{2}\sum_{n\geqslant 1}|\psi_n|^2\\ &= |\psi_0|^2+\frac{1}{2}(1-|\psi_0|^2)\\ &= \frac{1}{2}+\frac{1}{2}|\psi_0|^2.\end{aligned} \tag{D3}$$

Note that this inequality is an equality whenever $\psi_n = 0$ for $n > 1$. Given that $\mathbb{P}_{D_1} = 1-\mathbb{P}_\emptyset$, this yields

$$\mathbb{P}_{D_0}\geqslant\tfrac{1}{2}(1-|\langle\psi|0\rangle|^2), \tag{D4}$$

which concludes the proof when $\beta = 0$.

Now if $\beta\neq 0$, we define

$$|\phi\rangle := \hat{D}^\dagger(\beta)|\psi\rangle, \tag{D5}$$

where $\hat{D}$ is a displacement operator, with $|\beta\rangle = D(\beta)\,|0\rangle$, so $|\psi\rangle = D(\beta)\,|\phi\rangle$ and $|\langle\psi|\beta\rangle|^2 = |\langle\phi|0\rangle|^2$. The input state is given by

$$|\psi\rangle_a \otimes |\beta\rangle_b = \hat{D}_a(\beta) \otimes \hat{D}_b(\beta)\,|\phi\rangle_a \otimes |0\rangle_b\,, \tag{D6}$$

where the subscript indicates the modes onto which the displacement operator acts. The probability that the detector D_0 does not click after the beam splitter interaction is then given by

$$\begin{aligned}\mathbb{P}_\emptyset &= \mathrm{Tr}[(\mathbb{I}_c \otimes |0\rangle\langle 0|_d)\hat{H}\,|\psi\rangle\langle\psi|_a \otimes |0\rangle\langle 0|_b \hat{H}^\dagger] \\ &= \mathrm{Tr}[(\mathbb{I}_c \otimes |0\rangle\langle 0|_d)\hat{H}(\hat{D}_a(\beta) \otimes \hat{D}_b(\beta))\,|\phi\rangle\langle\phi|_a \otimes |0\rangle\langle 0|_b (\hat{D}_a^\dagger(\beta) \otimes \hat{D}_b^\dagger(\beta))\hat{H}^\dagger].\end{aligned} \tag{D7}$$

Now we have

$$\hat{H}(\hat{D}_a(\beta) \otimes \hat{D}_b(\beta)) = (\hat{D}_c(\sqrt{2}\beta) \otimes \mathbb{I}_d)\hat{H}. \tag{D8}$$

Hence,

$$\begin{aligned}\mathbb{P}_\emptyset &= \mathrm{Tr}[(\mathbb{I}_c \otimes |0\rangle\langle 0|_d)(\hat{D}_c(\sqrt{2}\beta) \otimes \mathbb{I}_d)\hat{H}\,|\phi\rangle\langle\phi|_a \otimes |0\rangle\langle 0|_b \hat{H}^\dagger(\hat{D}_c^\dagger(\sqrt{2}\beta) \otimes \mathbb{I}_d)] \\ &= \mathrm{Tr}[(\mathbb{I}_c \otimes |0\rangle\langle 0|_d)\hat{H}\,|\phi\rangle\langle\phi|_a\,|0\rangle\langle 0|_b \hat{H}^\dagger],\end{aligned} \tag{D9}$$

and the previous proof for $\beta = 0$ gives

$$\mathbb{P}_{D_0} \geqslant \tfrac{1}{2}(1 - |\langle\phi|0\rangle|^2). \tag{D10}$$

Finally, since $|\langle\psi|\beta\rangle|^2 = |\langle\phi|0\rangle|^2$, we obtain

$$\mathbb{P}_{D_0} \geqslant \tfrac{1}{2}(1 - |\langle\psi|\beta\rangle|^2), \tag{D11}$$

and this inequality is an equality whenever $\langle\phi|n\rangle = 0$ for $n > 1$, with $|\phi\rangle = \hat{D}^\dagger(\beta)\,|\psi\rangle$.

APPENDIX E: SOUNDNESS FOR A GENERIC INPUT STATE FOR ANY M

By linearity of the probabilities, it is sufficient to prove Eq. (49) when τ is a pure state.

Let us write $\tau = |\psi\rangle\langle\psi|$, where $|\psi\rangle = \sum_{m\geqslant 0} \psi_m\,|m\rangle$, where $\sum_{m\geqslant 0} |\psi_m|^2 = 1$. We first show Eq. (49) for $\beta = 0$. In that case, the M-mode input state is

$$|\psi\,0\ldots 0\rangle = \sum_{m\geqslant 0} \psi_m\,|m0\ldots 0\rangle. \tag{E1}$$

The probability that none of the detectors in output modes 2^k clicks (the modes being indexed from 0 to $M-1$) after the amplifier interferometer evolution $\hat{U}_n$ is given by

$$\mathbb{P}_\emptyset = \mathrm{Tr}\left[\left(\bigotimes_{i=0}^{M-1} \hat{E}_i\right)\hat{U}_n\,|\psi\,0\ldots 0\rangle\langle\psi\,0\ldots 0|\,\hat{U}_n^\dagger\right], \tag{E2}$$

where $E_i = |0\rangle\langle 0|$ if $i = 2^k$ and $E_i = \mathbb{I}$ otherwise. From Sec. IV, since the amplifier scheme U_n reproduces the statistics of the Hadamard scheme H_n, this probability can be written as

$$\mathbb{P}_\emptyset = \mathrm{Tr}\big[\Pi_0^{\mathrm{opt}}\,|\psi\,0\ldots 0\rangle\langle\psi\,0\ldots 0|\big], \tag{E3}$$

where

$$\Pi_0^{\mathrm{opt}} = \sum_{N=0}^{\infty} \big|\chi_N^M\big\rangle\big\langle\chi_N^M\big|, \tag{E4}$$

with

$$\big|\chi_N^M\big\rangle := M^{-N/2} \sum_{\sum_j k_j = N} \sqrt{\frac{N!}{k_1!\ldots k_M!}}\,|k_1\ldots k_M\rangle. \tag{E5}$$

Expanding Eq. (E3) in Fock basis using Eq. (E1) yields

$$\begin{aligned}\mathbb{P}_{\emptyset} &= \sum_{N=0}^{\infty} \sum_{\sum_i k_i = N} \sum_{\sum_j l_j = N} \sum_{p,q \geqslant 0} M^{-N} \sqrt{\frac{N!}{k_1! \dots k_M!}} \sqrt{\frac{N!}{l_1! \dots l_M!}} \psi_p \psi_q^* \mathrm{Tr}[(|k_1 \dots k_M\rangle \langle l_1 \dots l_M|)(|p\,0 \dots 0\rangle \langle q\,0 \dots 0|)] \\ &= \sum_{p \geqslant 0} \frac{|\psi_p|^2}{M^p} \\ &\leqslant |\psi_0|^2 + \frac{1}{M} \sum_{p \geqslant 1} |\psi_p|^2 \\ &= |\psi_0|^2 + \frac{1}{M}(1 - |\psi_0|^2) \\ &= \frac{1}{M} + \left(1 - \frac{1}{M}\right)|\psi_0|^2. \end{aligned} \tag{E6}$$

Note that this inequality is an equality whenever $\psi_n = 0$ for $n > 1$. Given that $\mathbb{P}_D = 1 - \mathbb{P}_{\emptyset}$, this gives

$$\mathbb{P}_D \geqslant \left(1 - \frac{1}{M}\right)(1 - |\langle \psi | 0 \rangle|^2), \tag{E7}$$

which concludes the proof when $\beta = 0$.

Now if $\beta \neq 0$, we define

$$|\phi\rangle := \hat{D}^{\dagger}(\beta)\,|\psi\rangle\,, \tag{E8}$$

as in the previous section, where $\hat{D}$ is a displacement operator, with $|\beta\rangle = D(\beta)\,|0\rangle$, so that $|\psi\rangle = D(\beta)\,|\phi\rangle$ and $|\langle\psi|\beta\rangle|^2 = |\langle\phi|0\rangle|^2$. The input state is given by

$$|\psi\ \beta \dots \beta\rangle = \hat{D}(\beta)^{\otimes M}\,|\phi\,0 \dots 0\rangle\,. \tag{E9}$$

The probability that none of the detectors in output modes 2^k clicks is given by

$$\begin{aligned}\mathbb{P}_{\emptyset} &= \mathrm{Tr}\left[\left(\bigotimes_{i=0}^{M-1} \hat{E}_i\right) \hat{U}_n\,|\psi\ \beta \dots \beta\rangle\,\langle\psi\ \beta \dots \beta|\,\hat{U}_n^{\dagger}\right] \\ &= \mathrm{Tr}\left[\left(\bigotimes_{i=0}^{M-1} \hat{E}_i\right) \hat{U}_n \hat{D}(\beta)^{\otimes M}\,|\phi\,0 \dots 0\rangle\,\langle\phi\,0 \dots 0|\,\hat{D}^{\dagger}(\beta)^{\otimes M} \hat{U}_n^{\dagger}\right], \end{aligned} \tag{E10}$$

where $\hat{E}_i = |0\rangle\,\langle 0|$ if $i = 2^k$ and $\hat{E}_i = \mathbb{I}$ otherwise. We have

$$\hat{U}_n \hat{D}(\beta)^{\otimes M} = \left(\bigotimes_{i=0}^{M-1} \hat{D}(\delta_i)\right) \hat{U}_n, \tag{E11}$$

where $(\delta_0, \dots, \delta_{M-1})^T = U_n(\beta, \dots, \beta)^T$. In particular, $\delta_i = 0$ if $i = 2^k$, so for all $i = 0, \dots, M-1$,

$$\hat{D}^{\dagger}(\delta_i) \hat{E}_i \hat{D}(\delta_i) = \hat{E}_i. \tag{E12}$$

Hence,

$$\begin{aligned}\mathbb{P}_{\emptyset} &= \mathrm{Tr}\left[\left(\bigotimes_{i=0}^{M-1} \hat{E}_i\right)\left(\bigotimes_{i=0}^{M-1} \hat{D}(\delta_i)\right) \hat{U}_n\,|\phi\,0 \dots 0\rangle\,\langle\phi\,0 \dots 0|\,\hat{U}_n^{\dagger}\left(\bigotimes_{i=0}^{M-1} \hat{D}^{\dagger}(\delta_i)\right)\right] \\ &= \mathrm{Tr}\left[\left(\bigotimes_{i=0}^{M-1} \hat{D}^{\dagger}(\delta_i) \hat{E}_i \hat{D}(\delta_i)\right) \hat{U}_n\,|\phi\,0 \dots 0\rangle\,\langle\phi\,0 \dots 0|\,\hat{U}_n^{\dagger}\right] \\ &= \mathrm{Tr}\left[\left(\bigotimes_{i=0}^{M-1} \hat{E}_i\right) \hat{U}_n\,|\phi\,0 \dots 0\rangle\,\langle\phi\,0 \dots 0|\,\hat{U}_n^{\dagger}\right]. \end{aligned} \tag{E13}$$

The previous proof for $\beta = 0$ gives

$$\mathbb{P}_D \geqslant \left(1 - \frac{1}{M}\right)(1 - |\langle\phi|0\rangle|^2). \tag{E14}$$

Finally, since $|\langle\psi|\beta\rangle|^2 = |\langle\phi|0\rangle|^2$, we obtain

$$\mathbb{P}_D \geqslant \left(1 - \frac{1}{M}\right)(1 - |\langle\psi|\beta\rangle|^2), \tag{E15}$$

and this inequality is an equality whenever $\langle\phi|n\rangle = 0$ for $n > 1$, with $|\phi\rangle = \hat{D}^\dagger(\beta)\,|\psi\rangle$.

[1] J. Carolan, C. Harrold, C. Sparrow, E. Martín-López, N. J. Russell, J. W. Silverstone, P. J. Shadbolt, N. Matsuda, M. Oguma, M. Itoh *et al.*, Universal linear optics, Science **349**, 711 (2015).

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

[3] J. M. Arrazola and N. Lütkenhaus, Quantum communication with coherent states and linear optics, Phys. Rev. A **90**, 042335 (2014).

[4] J.-Y. Guan, F. Xu, H.-L. Yin, Y. Li, W.-J. Zhang, S.-J. Chen, X.-Y. Yang, L. Li, L.-X. You, T.-Y. Chen *et al.*, Observation of Quantum Fingerprinting Beating the Classical Limit, Phys. Rev. Lett. **116**, 240502 (2016).

[5] J.-Y. Guan, J. M. Arrazola, R. Amiri, W. Zhang, H. Li, L. You, Z. Wang, Q. Zhang, and J.-W. Pan, Experimental preparation and verification of quantum money, Phys. Rev. A **97**, 032338 (2018).

[6] N. Kumar, E. Diamanti, and I. Kerenidis, Efficient quantum communications with coherent state fingerprints over multiple channels, Phys. Rev. A **95**, 032337 (2017).

[7] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis, Exponential separation of quantum and classical one-way communication complexity, in *Proceedings of the Thirty-sixth Annual ACM Symposium on Theory of Computing* (ACM, New York, NY, United States, 2004), pp. 128–137.

[8] N. Kumar, I. Kerenidis, and E. Diamanti, Experimental demonstration of quantum advantage for one-way communication complexity surpassing best-known classical protocol, Nat. Commun. **10**, 4152 (2019).

[9] M. Georgiou and I. Kerenidis, New constructions for quantum money, in *LIPIcs-Leibniz International Proceedings in Informatics*, Vol. 44 (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2015).

[10] R. Amiri and J. M. Arrazola, Quantum money with nearly optimal error tolerance, Phys. Rev. A **95**, 062334 (2017).

[11] M. Bozzio, A. Orieux, L. T. Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti, Experimental investigation of practical unforgeable quantum money, npj Quantum Inf. **4**, 5 (2018).

[12] N. Kumar, Practically feasible robust quantum money with classical verification, Cryptography **3**, 26 (2019).

[13] S. M. Barnett, A. Chefles, and I. Jex, Comparison of two unknown pure quantum states, Phys. Lett. A **307**, 189 (2003).

[14] U. Chabaud, E. Diamanti, D. Markham, E. Kashefi, and A. Joux, Optimal quantum-programmable projective measurement with linear optics, Phys. Rev. A **98**, 062318 (2018).

[15] F. Xu, J. M. Arrazola, K. Wei, W. Wang, P. Palacios-Avila, C. Feng, S. Sajeed, N. Lütkenhaus, and H.-K. Lo, Experimental quantum fingerprinting with weak coherent pulses, Nat. Commun. **6**, 8735 (2015).

[16] M. Sedlák, M. Ziman, O. Přibyla, V. Bužek, and M. Hillery, Unambiguous identification of coherent states: Searching a quantum database, Phys. Rev. A **76**, 022326 (2007).

[17] A. Ambainis, Communication complexity in a 3-computer model, Algorithmica **16**, 298 (1996).

[18] L. Babai and P. G. Kimmel, Randomized simultaneous messages: Solution of a problem of Yao in communication complexity, in *Computational Complexity, 1997. Proceedings, Twelfth Annual IEEE Conference on (Formerly: Structure in Complexity Theory Conference)* (IEEE, Piscataway, New Jersey, 1997), pp. 239–246.

[19] I. Newman, Private vs. common random bits in communication complexity, Inform. Processing Lett. **39**, 67 (1991).

[20] I. Newman and M. Szegedy, Public vs. private coin flips in one round communication games, in *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, New York, NY, United States, 1996), pp. 561–570.

[21] E. Upfal and M. Mitzenmacher, *Probability and Computing: Randomized Algorithms and Probabilistic Analysis* (Cambridge University Press, Cambridge, UK, 2005).

[22] L. Schweickert, K. D. Jöns, K. D. Zeuner, S. F. Covre da Silva, H. Huang, T. Lettner, M. Reindl, J. Zichi, R. Trotta, A. Rastelli *et al.*, On-demand generation of background-free single photons from a solid-state source, Appl. Phys. Lett. **112**, 093106 (2018).

[23] J. N. de Beaudrap, One-qubit fingerprinting schemes, Phys. Rev. A **69**, 022307 (2004).

[24] A. K. Ekert, C. M. Alves, D. K. L. Oi, M. Horodecki, P. Horodecki, and L. C. Kwek, Direct Estimations of Linear and Nonlinear Functionals of a Quantum State, Phys. Rev. Lett. **88**, 217901 (2002).

[25] F. Mintert, M. Kuś, and A. Buchleitner, Concurrence of Mixed Multipartite Quantum States, Phys. Rev. Lett. **95**, 260502 (2005).

[26] S. P. Walborn, P. H. S. Ribeiro, L. Davidovich, F. Mintert, and A. Buchleitner, Experimental determination of entanglement with a single measurement, Nature (London) **440**, 1022 (2006).

[27] S. Aaronson, S. Beigi, A. Drucker, B. Fefferman, and P. Shor, The power of unentanglement, in *CCC'08. 23rd Annual IEEE Conference on Computational Complexity, 2008* (The University of Chicago, Chicago, Illinois, United States, 2008), pp. 223–236.

[28] A. W. Harrow and A. Montanaro, Testing product states, quantum merlin-arthur games and tensor optimization, J. ACM **60**, 1 (2013).

[29] S. Lloyd, M. Mohseni, and P. Rebentrost, Quantum algorithms for supervised and unsupervised machine learning, arXiv:1307.0411.