Experimental quantum private queries with linear optics

The MIT Faculty has made this article openly available. Please share how this access benefits you. Your story matters.

| Citation       | De Martini, Francesco et al. “Experimental quantum private queries with linear optics.” Physical Review A 80.1 (2009): 010302. © 2009 The American Physical Society |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| As Published   | http://dx.doi.org/10.1103/PhysRevA.80.010302                                                                                                                                                       |
| Publisher      | American Physical Society                                                                                                                                                                         |
| Version        | Final published version                                                                                                                                                                          |
| Citable link   | http://hdl.handle.net/1721.1/51867                                                                                                                                                              |
| Terms of Use   | Article is made available in accordance with the publisher’s policy and may be subject to US copyright law. Please refer to the publisher’s site for terms of use.                                           |
I. INTRODUCTION

Quantum information technology has matured especially in the field of cryptography. Two distant parties can exploit quantum effects, such as entanglement, to communicate in a provably secure fashion. An interesting cryptographic primitive is the symmetrically private information retrieval (SPIR) [1]: it allows a user (say Alice) to recover an element from a database in possession of a provider (say Bob), without revealing which element was recovered (user privacy). At the same time it allows Bob to limit the total amount of information that Alice receives (data privacy). Since user and data privacy appear to be conflicting requirements, all existing classical protocols rely on constraining the resources accessible by the two parties [2]. However, using quantum effects, such constraints can be dropped: the quantum private query (QPQ) [3] is a quantum-cryptographic protocol that implements a cheat-sensitive SPIR. User privacy is indirectly enforced by allowing Alice to test the honesty of Bob: she can perform a quantum test to find out whether he is retaining any information on her queries, in which case Bob would disturb the states Alice is transmitting and she has some probability of detecting it [4]. Data privacy is strictly enforced since the number of bits that Alice and Bob exchange is too small to convey more than at most two database items.

In this Rapid Communication we present an optical scheme to carry out a variant of the QPQ protocol. In contrast to the original proposal of [3], it does not require a quantum random access memory (qRAM) [5] and can be implemented with linear optics, i.e., current technology, but it has suboptimal communication complexity. The qRAM’s absence implies that the binary-to-unary translation to route Alice’s query to the appropriate database memory element must be performed by Alice herself. Thus Alice and Bob must be connected by a number of communication channels equal to the number \( N \) of database elements [although \( O(\log_2 N) \) would suffice with a qRAM]. We present two conceptually equivalent QPQ implementations: in the first (more suited to explanatory purposes and proof-of-principle tests) each channel is a spatial optical mode, in the second (more suited to practical applications) it is a time slot in a fiber [6,7]. The Rapid Communication focuses mostly on the former implementation for which we provide an experimental test. For this setup we also consider the case in which Alice entangles her queries with ancillary systems that she keeps in her laboratory. With this choice the user privacy can only be enhanced with respect to original scheme [3] as Bob has only limited access to the states which encode Alice’s queries.

We start with a description of a scheme, focusing on how user and data privacy can be tested. Then we describe its experimental implementation and conclude with the time-slot implementation.

II. SCHEME

The optical QPQ scheme is sketched in Fig. 1(a). Bob controls an \( N \)-element database, where each element \( j \) is associated to a spatial optical mode and consists of one bit \( A_j \) of classical information. The bit \( A_j=1 \) (0) is encoded into the presence (absence) of a half-wave plate \( B_{pr} \) in the \( j \)th mode (it rotates the polarization by 90°). Alice probes this system with single photons either in one mode or in a superposition of modes. To recover the database element \( A_j \), Alice sends to Bob a single horizontally polarized photon \( H \) in the mode \( j \), i.e., the state \( |P_j\rangle=|H\rangle_j \), see Fig. 1(b). Bob employs the photon’s polarization as a “bus” qubit to communicate the query result: vertical \( V \) if \( A_j=1 \) or horizontal \( H \) if \( A_j=0 \). Namely, his transformation is

\[
|P_j\rangle \rightarrow |P_{\text{out}}\rangle = |A_j\rangle = \begin{cases} |H\rangle_j & \text{for } A_j=0 \\ |V\rangle_j & \text{for } A_j=1. \end{cases}
\]  

This exchange is clearly not private. To attain cheat sensitivity, Alice must randomly alternate two different kinds of queries: “plain” queries of the type \( |P_j\rangle \) described above and “superposed” queries

\[
|S_j\rangle = (|H\rangle_j \otimes |a\rangle + |V\rangle_j |\bar{a}\rangle_j)/\sqrt{2},
\]

where the \( j \)th mode is entangled with an ancillary spatial
mode $j_a$ and $|\varnothing\rangle$ is the vacuum state. According to original proposal [3] $j_a$ should be identified with one (say the first) of the $N$ spatial modes of the system, whose associated database entry is initialized in a known fiducial value $A_{ja}=0$. With this choice $j_a$ will play the role of the *rhetoric* query of the original QPO scheme whose user privacy has been formally proved in Ref. [4]. Here however we follow an alternative strategy that guarantees user privacy levels which are at least as good as the original scheme and that can be easily realized in the spatial mode implementation. Namely, as shown in Fig. 1(a), the $j_a$'s will be identified with extra modes that Alice keeps in her laboratory. With this choice Alice privacy can only increase with respect to the original scheme as Bob does not have access to the complete quantum system [Eq. (2)]—his cheating operations can only act on the subsystem that Alice has sent him, while the QPO security proof [4] assumes he can act on the full state system. To prepare such input state Alice simply shines an $H$ polarized photon onto a 50% beam-splitter sending one of the emerging beams to Bob and keeping the other in her laboratory as shown in Fig. 1(c). After having crossed Bob's laboratory (in the absence of cheating), the superposed query is evolved into

$$|S_j\rangle \rightarrow |S_{ja}^{\text{out}}\rangle = (|A_j\rangle\langle\varnothing| \otimes |\varnothing\rangle_j\langle H|j_a\rangle)\sqrt{2}. \quad (3)$$

The two types of queries $|P_j\rangle$ and $|S_j\rangle$ must be submitted in random order and *one at a time* (i.e., she must wait for Bob's first reply before sending him the second query): if Bob received both queries at the same time, he could cheat undetected with a joint measurement [3].

The random alternation of plain and superposed queries allows Alice to test Bob's honesty. Indeed, since he does not know whether her photon is in the state $|P_j\rangle$ or $|S_j\rangle$, if Bob measures its position he risks collapsing the superposed query $|S_j\rangle$, and Alice can easily find it out. In fact, she can first obtain the value of $A_j$ through a polarization readout from $|P_{ja}^{\text{out}}\rangle$, see Fig. 1(d). She can then use this value to prepare a projective measurement that tests whether the superposed query $|S_j\rangle$ has been preserved or collapsed (honesty test), i.e., a measurement that tests if the answer associated with $|S_j\rangle$ has been collapsed into the subspace orthogonal to the expected output $|S_{ja}^{\text{out}}\rangle$. As explained in more detail in the next section, this essentially amounts to the interferometric measurement of Fig. 1(e).] If this happened, she can confidently conclude that Bob has cheated. If this has not happened she cannot conclude anything: a cheating Bob still has some probability of passing the test. For instance, assume that Bob uses a measure-and-reprepare strategy on one of the two queries, he will be caught only with probability 1/4. Anyhow, whatever cheating strategy Bob may employ, the probability of passing the honesty test is bounded by the information he retains on Alice's query [4]; he can pass the test with certainty *if and only if* he does not retain any information from her.

### III. READOUT AND HONESTY TEST

Before proceeding, we analyze in more detail Alice's measurements. Consider first the case in which Alice *first* sends the plain query $|P_j\rangle$ and *then* the superposed query $|S_j\rangle$. In this case, she recovers $A_j$ with the polarization measurement of Fig. 1(d). Then, before sending the second query $|S_j\rangle$, she sets up an interferometer that couples the ancillary mode $j_a$ with the output of the mode $j$ as shown in Fig. 1(c), while the polarization rotator $A_{ja}$ is used to compensate the rotation induced by Bob's database, determined by the value of $A_j$ that she previously recovered. Therefore, if Bob has not cheated, the state in the interferometer just before the second beam splitter is $|S_j\rangle$ so that the “don’t know” detector $D_0$ must fire and the “cheat” detector $D_1$ cannot fire. If the cheat detector $D_1$ does fire, Alice knows that Bob must have cheated.

Consider now the case in which Alice sends first the superposed query $|S_j\rangle$ and then the plain query $|P_j\rangle$. In order to perform the honesty test, she must first recover the value of $A_j$. So she needs to store the answer to the superposed query $|S_{ja}^{\text{out}}\rangle$ until the answer to the plain query $|P_{ja}^{\text{out}}\rangle$ arrives, from which $A_j$ can be measured. It requires a quantum memory [8] and a fast feed-forward mechanism [9] to prepare the honesty test measurement depending on the value of $A_j$. Achieving this is possible but demanding. The same goal is reached with a less efficient but much simpler strategy. Alice chooses a random value $A(0)$ in place of $A_j$. She then performs the interferometric measurement of Fig. 1(c) inserting or not the polarization rotator $A_{ja}$ depending on the value of $A(0)$. This interferometer is then a projector on the state $|S_{ja}^{\text{guess}}\rangle = (|A(0)\rangle\langle\varnothing| \otimes |\varnothing\rangle_j\langle H|j_a\rangle)\sqrt{2}$. Later, when she receives the output of the plain query $|P_{ja}^{\text{out}}\rangle$, she finds out the value of $A_j$. If she had picked the right value $A(0)=A_j$, she will know that her first measurement was a valid honesty test since $|S_{ja}^{\text{guess}}\rangle = |S_{ja}^{\text{guess}}\rangle$. Otherwise, if $A(0) \neq A_j$, then the result of her honesty test is useless and she must discard it. Since Alice chooses $A(0)=A_j$ with probability 1/2, she performs the hon-
Let us now briefly summarize the protocol. (1) Alice randomly chooses one of the two scenarios: either send first the plain query $|P_j\rangle$ and then the superposed query $|S_i\rangle$, or vice versa. (2a) In the first case, she recovers $A_j$ from Bob’s first reply and uses it to prepare the honesty test to use on his second reply. (2b) In the second case, she chooses a random bit $A(R^j)$ and prepares the honesty test using it in place of $A_j$. Then she performs the honesty test on Bob’s first reply. When $A_j$ becomes available later (from Bob’s second reply), she finds out whether the honesty test result was meaningful (if $A_j=A(R^j)$) or not (if $A_j\neq A(R^j)$). (3) If the honesty test was meaningful and it has failed, she can conclude that Bob has cheated.

**IV. DATA PRIVACY**

In the original QPQ protocol [3], data privacy was ensured by the fact that only a limited number of qubits were exchanged between Alice and Bob: she had to send (and receive) a sequence of $O(\log_2 N)$ qubits to specify the address of the $j$th element. In contrast, in this version of the protocol Alice has direct access to all the entries of Bob’s database through the $N$ optical modes. She can then violate data privacy and recover multiple elements of Bob’s database by sending many photons, one per mode. Theoretically, Bob can foil Alice by preparing a joint measurement on the $N$ spatial modes that discriminates the subspace with zero or one photon from the rest. If he finds that the modes jointly contain more than one photon, he knows that Alice is trying to violate the data privacy, and stops the communication. If, instead, he finds that Alice is sending no more than one photon per query, he can be sure that she is recovering no more than one bit per transaction.

Unfortunately, the above measurement is practically unfeasible. An alternative solution that is feasible, although less efficient, is the following. After Alice has sent her first photon into his laboratory, Bob blocks the access to the database and partitions it into $X$ equal parts $P_1, P_2, \ldots, P_X$ containing $N/X$ random entries each. He then communicates to Alice the composition of the partitions asking to reveal $\log_2 X$ bits on her query to indicate which of the $P_i$s contains the database entry she is interested in [the fact that Alice has to reveal some bits should not be seen as a breach of the user privacy, since this is a (small) fixed quantity which is independent of the database size]. Bob now can perform a local photodetection on each of the modes of the $X-1$ partitions which according to Alice do not contain the message she is looking for. If he finds any photons there, he knows for sure that Alice has cheated and stops the communication. If he does not, he cannot conclude that Alice has cheated and allows her to complete her query sending the second photon, for which the above procedure is repeated.

As in the case of user privacy, the data privacy is thus enforced by means of a probabilistic, nonconclusive honesty test. In particular there is a tradeoff: the more bits Alice reveals on her query, the higher is the probability that Bob will be able to find out if she is cheating. For instance, consider the case in which Alice tries to recover some extra bits from the database by sending $t \approx 1$ photons per transmitted signal. Assuming random encodings, the probability that all of them will be found in the same subset of the database partition can be estimated as $X(1/X)'=(1/X)'^{-1}$. This is the only case in which Alice can safely pass Bob’s honesty test. In all remaining cases at least one of the $t$ photons will belong to one of the subsets on which Bob performs his photodetections. Alice’s probability of being caught is thus equal to $P=1-(1/X)'^{-1}$, which increases both with the number $(t-1)$ of cheating photons and with the number $\log_2 X$ of bits she reveals to Bob, see Fig. 2. The gating is also fundamental: Bob must open the access to the database only during the transit time of Alice’s photons prompted by a trigger signal. Otherwise, she can cheat sending photons at other times. Similar expedients are usually adopted in plug-and-play cryptographie schemes to avoid Trojan horse attacks [10]. These parts of the protocol are important only if data privacy is an issue. As done in the experiment below, it can be omitted when only user privacy is important.

**V. EXPERIMENTAL RESULTS**

In order to perform a proof-of-principle experiment, we have to show that Alice can recover the value of each database element and that she can detect Bob’s cheats. The single photon is created by starting from a biphoton generated through spontaneous parametric downconversion and using one of the two component photons as a trigger. A sequence of half-wave plates and polarizing beam splitters allows Alice to choose the mode $j$ (i.e., the database element) she wants to access with her $H$ polarized photon, see Fig. 1(b). In the experiment we employed $N=3$ modes. A standard polar-
TABLE I. (a) Experimental values of the fidelity of Alice’s measurement of each of the three elements of Bob’s database. The measurement is performed by sending queries of the form $|P_j\rangle$ and measuring the output polarization, see Fig. 1(d). (b) Comparison between theoretical (theor.) and experimental (expt.) fidelities of Alice’s honesty test of Fig. 1(c). The discrepancy with theory is due to unbalancement of the interferometer and slight misalignment.

| $j$ | $A_j$ | Fidelity | $A_j$ | Fidelity |
|-----|-------|----------|-------|----------|
| 1   | 0     | 99.84 ± 0.04% | 1     | 99.99 ± 0.01% |
| 2   | 0     | 99.81 ± 0.04% | 1     | 99.72 ± 0.05% |
| 3   | 0     | 99.99 ± 0.01% | 1     | 99.99 ± 0.01% |

(b)

| $A_j$ | $D_0$ theor. | $D_0$ expt. | $D_1$ theor. | $D_1$ expt. |
|-------|--------------|--------------|--------------|--------------|
| No cheat | 0 | 1 | 99.3 ± 0.2% | 0 | (0.7 ± 0.2)% |
| No cheat | 1 | 1 | 99.4 ± 0.2% | 0 | (0.6 ± 0.2)% |
| Cheat | 0 | 0.5 | 45.0 ± 0.1% | 0.5 | 55.0 ± 0.1% |
| Cheat | 1 | 0.5 | 45.4 ± 0.1% | 0.5 | 54.6 ± 0.1% |

VI. TIME-SLOT IMPLEMENTATION

We now describe a different implementation of the scheme based on [6,7]. To each database element $j$ we associate a unique time slot in an optical fiber: Alice places her query photon in the $j$th slot (i.e., the state $|P_j\rangle$) if she wants to access $A_j$. Bob’s database is encoded into a time-dependent polarization rotator: in the $j$th time slot the polarization is rotated only if $A_j=1$. To create the superposed $|S_j\rangle$ query, Alice places her photon in a superposition of two time slots [6]. This is achieved by sending it through a 50% beam splitter, at the two outputs of which she places a long and a short fiber. The length difference of the fibers corresponds to a delay proportional to $j$. The signals from the two fibers are then joined into a single fiber through an optical switch [6]. The same device (used in reverse) is used as cheat test on the superposed signal returning from Bob: the optical switch sends the first pulse through the long fiber and the second through the short fiber so that they interfere at the beam splitter. The photon then exits at one of the two “cheat” or “don’t know” ports of the beam splitter. It is simple to see that this implementation is conceptually equivalent to the previous one, but it is more suited to the case in which Alice and Bob are far apart, as this procedure has been tested experimentally with interferometers of many Km in length [7,10]. Our protocol can be easily scaled up considerably since the resources scale only linearly with the number of database elements. The number of database elements is ultimately limited only by the time-dependent noise the photons encounter along the fiber.

[1] Y. Gartner et al., J. Comput. Syst. Sci. 60, 592 (2000).
[2] A. Ambainis, in Proceedings of ICALP’97, Lecture Notes in Computer Science Vol. 1256 (Springer-Verlag, 1997), pp. 401–407; A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[3] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. 100, 230502 (2008).
[4] V. Giovannetti et al., arXiv:0809.1934.
[5] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. 100, 160501 (2008); Phys. Rev. A 78, 052310 (2008).
[6] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Phys. Rev. Lett. 82, 2594 (1999).
[7] R. T. Thew, S. Tanzilli, W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A 66, 062304 (2002).
[8] C.-S. Chuu et al., Phys. Rev. Lett. 101, 120501 (2008); Y.-A. Chen et al., Nat. Phys. 4, 103 (2008).
[9] F. Sciarrino, M. Ricci, F. De Martini, R. Filip, and L. Mista, Phys. Rev. Lett. 96, 020408 (2006).
[10] N. Gisin et al., Rev. Mod. Phys. 74, 145 (2002).
[11] J. L. O’Brien et al., Nature 426, 264 (2003).