Quantum Private Queries: Security Analysis

Citation: Giovannetti, Vittorio, Seth Lloyd, and Lorenzo Maccone. “Quantum Private Queries: Security Analysis.” IEEE Transactions on Information Theory 56.7 (2010): 3465-3477. Web. 3 Feb. 2012. © 2010 Institute of Electrical and Electronics Engineers

As Published: http://dx.doi.org/10.1109/tit.2010.2048446

Publisher: Institute of Electrical and Electronics Engineers (IEEE)

Persistent URL: http://hdl.handle.net/1721.1/69027

Version: Final published version: final published article, as it appeared in a journal, conference proceedings, or other formally published context

Quantum Private Queries: Security Analysis

Vittorio Giovannetti, *Member, IEEE*, Seth Lloyd, *Fellow, IEEE, OSA*, and Lorenzo Maccone, *Life Fellow, IEEE*

***Abstract*—A security analysis of the recently introduced Quantum Private Query (QPQ) protocol is presented. The latter is a cheat sensitive quantum protocol to perform a private search on a classical database. It allows a user to retrieve an item from the database without revealing which item was retrieved, and at the same time it ensures data privacy of the database (the information that the user retrieves in a query is bounded). The security analysis is based on information-disturbance tradeoffs which show that whenever the provider tries to obtain information on the query, the query (encoded into a quantum system) is disturbed so that the person querying the database can detect the privacy violation. The security bounds are derived under the assumption that a unique answer corresponds to each query. To remove this assumption, some simple variants of the protocol are illustrated, and it is conjectured that analogous security bounds apply to them.**

***Index Terms*—Privacy, quantum algorithm, quantum communication, quantum information theory, security.**

I. Introduction

IN its most basic form, the scenario we consider can be described as follows. On one side we have a provider, Bob, who controls an ordered classical database composed of $N = 2^n$ memory cells. Each cell of the data-base contains an m bit string, so that the database consists of N strings $A_0, A_1, \ldots, A_{N-1}$. On the other side, we have the person querying the database, Alice, who wants to recover the string associated with a memory cell (say the jth one) but at the same time does not want Bob to know which cell she is interested in (*user privacy*). In a purely classical setting, the simplest strategy for Alice consists in placing a large number of decoy queries, i.e., she "hides" her query among a large number $M-1$ of randomly selected queries. In this case, she will be able to get the information she is looking for, while limiting Bob's intrusion in her privacy. (In fact, the mutual information between Alice's true query j and Bob's estimate of such value is upper bounded by $\log_2(N/M) - (M-1)/M \log_2((N-1)/(M-1)))$. The drawbacks associated with such procedures are evident. First of all, the method does not allow Alice to check whether Bob is retaining information on her queries. Moreover, to achieve a high level of privacy Alice is forced to submit large amounts of fake queries, increasing the communication cost of the transition: in particular, absolute privacy is obtained only for $M = N$, i.e., by asking Bob to send *all* his database. This may not be acceptable if the database is huge or if it is an asset for Bob (*data privacy*).

User and data privacy are apparently in conflict: the most straightforward way to obtain user privacy is for Alice to have Bob send her the entire database, leading to no data privacy whatsoever. Conversely, techniques for guaranteeing the server's data privacy typically leave the user vulnerable [1]. At the information theoretical level, this problem has been formalized as the Symmetrically-Private Information Retrieval (SPIR) [1] generalizing the Private Information Retrieval (PIR) problem [2]–[7] which deals with user privacy alone. SPIR is closely related to oblivious transfer [8]–[10], in which Bob sends to Alice N bits, out of which Alice can access exactly one—which one, Bob does not know. No efficient solutions in terms of communication complexity [11] are known for SPIR. Indeed, even rephrasing them at a quantum level [12], [13], the best known solution for the SPIR problem (with a single database server) employs $O(N)$ qubits to be exchanged between the server and the user, and ensures data privacy only in the case of *honest users* (i.e., users who do not want to compromise their chances of getting the information about the selected item in order to get more). Better performance is obtained for the case of multiple nonmutually communicating servers [2] (although the user cannot have any guarantee that the servers are not secretly cooperating to violate her privacy), while sub-linear communication complexity is possible under the some computational complexity assumption, e.g., [7]. PIR admits protocols that are more efficient in terms of communication complexity [2]–[7].

The Quantum Private Queries (QPQ) protocol we have introduced in [14] (a more didactical explanation is given in [15]) is a cheat sensitive strategy [16] which addresses both user and data privacy while allowing an exponential reduction in the communication and computational complexity with respect to the best (quantum or classical) single-server SPIR protocol proposed so far. Specifically QPQ provides a method to check whether or not Bob is cheating and does not need the exchange of the whole database (i.e., $O(N)$ qubits): in its simplest form it only requires Bob to transfer two database elements, identified by $O(\log N)$ qubits, for each query. It also requires that each query has a single answer that Alice can verify (although we argue that by slightly modifying the proposed scheme this assumption can be dropped without compromising the security, see Section VI). The QPQ protocol is ideally composed by a preliminary signaling stage where the user and the database provider exchange some quantum messages (specifically Alice addresses Bob receiving some feedback from him) and by a subsequent *retrieval&check* stage where Alice performs

Manuscript received September 22, 2008; revised August 25, 2009. Current version published June 16, 2010.

V. Giovannetti is with NEST, Scuola Normale Superiore and Istituto Nanoscienze-CNR, Piazza dei Cavalieri 7, I-56126, Pisa, Italy (e-mail: v.giovannett@sns.it).

S. Lloyd is with the Massachusetts Institute of Technology, RLE and Department of Mechanical Engineering, Cambridge, MA 02139 USA.

L. Maccone was with the Institute for Scientific Interchange, I-10133 Torino, Italy. He is now with the Massachusetts Institute of Technology, RLE and Department of Mechanical Engineering, Cambridge, MA 02139 USA.

Communicated by P. Hayden, Associate Editor for Quantum Information Theory.

Digital Object Identifier 10.1109/TIT.2010.2048446

some simple quantum information processing on the received messages to recover the information she is interested in and to check Bob's honesty. The user security relies on the fact that if Bob tries to infer the query Alice is looking for, she has a nonzero probability of discovering it. A similar trick was also exploited in [17] with the purpose of obtaining secure computation from a remote server. Such proposal, however, did not involve any sort of data security which instead is explicitly enforced in our scheme by limiting the number of exchanged signals between Alice and Bob—see Section II.

The main idea behind the QPQ protocol is the following. Alice submits her request to Bob using some quantum information carrier, so that she can either submit a plain query $|j\rangle$ or a quantum superposition of different queries $\alpha|j\rangle + \beta|j'\rangle$. Alice randomly alternates superposed queries and nonsuperposed queries. Thus, Bob does not know whether the request he is receiving at any given time is a superposition of queries or not, so that he does not know which measurement will leave the information carrier unperturbed: he cannot extract information without risking to introduce a disturbance that Alice can detect. Bob can, however, respond to Alice's request without knowing which kind of query was submitted. Depending on the form of Alice's queries, his response will be correspondingly either of the form $|j\rangle|A_j\rangle$ or $\alpha|j\rangle|A_j\rangle + \beta|j'\rangle|A_{j'}\rangle$, where the first ket is the register that Alice had sent him, the second ket is a register that contains Bob's answer (A_i being the answer to the ith query), and which may be entangled with the first. From these answers Alice can both obtain the reply to her query and check that Bob has not tried to breach her privacy.[1] This enforces user privacy, while data privacy follows from the limited (logarithmic) number of qubits Alice obtains by Bob in the process.

To provide a rigorous security proof for the QPQ protocol we will focus on its simpler version. Namely we will consider the case where Alice always prepares her superposed queries by coherently mixing them with a given reference query 0 (dubbed *rhetoric* query) which has a known standard answer A_0. As discussed in [14], this assumption is not fundamental, but it is very useful since it allows us to minimize the amount of exchanged signals in the protocol (as a matter of fact alternative versions of the QPQ protocol with higher security level can be devised which do not employ the rhetoric query or which employ multiple rhetoric queries). An assumption which on the contrary appears to be rather important for our derivation is that, for each database entry j, there exists a *unique* answer string A_j. In other words, we restrict our analysis to the case of *deterministic databases*, i.e., databases whose outcomes are deterministically determined by the value of j (This, however, does not prevent different queries from having the same answer: indeed we do admit the possibility to have $A_j = A_{j'}$ for $j \neq j'$). Examples are provided for instance by a database that associates to each Social Security Number the (legal) name of its owner, or by the one which associates to each national lottery ticket the name of the town where it was sold. As extensively discussed in Section VI, for the versions of the QPQ protocol we analyze here, the hypothesis of dealing with deterministic database is fundamental: by removing it, Bob will be able to spy on Alice with zero probability of being caught. This follows from the fact that for nondeterministic databases Bob needs not to commit on a given answer during the signaling process: instead he is allowed to construct quantum superpositions of the various *correct* answers, letting Alice's measurements to randomly pick up one of them. As will be evident in the following, such freedom is sufficient to circumvent Alice's honesty test. In the final sections of the paper, we will present some variants of the QPQ protocol which, to some extent, allow one to relax the deterministic-database constraint. Essentially, this is done by admitting the possibility that Alice or some external third party (a referee) which is monitoring Bob's activity on her behalf, submits sequences of random queries on the same database items. If we require that Bob should always answer the same way to such repeated queries, we force him to consider each query as effectively having a unique answer, as required by the protocol versions analyzed here. Then he is restricted by the protocol in not being able to cheat, if he wants to keep his record clean also in the face of possible future queries. Even though the rigorous security bounds we derived under the uniqueness assumption are not valid if it is dropped, we conjecture that similar bounds can be analogously derived also for nondeterministic databases.

The paper is organized as follows. In Section II, we describe the rhetoric version of QPQ in its basic form and introduce the notation. This is followed by the technical Section III, where we analyze in detail the most general transformations Bob can perform on Alice's queries. Section IV contains the main result of the paper: here, we introduce the trade-off between Bob's information on Alice's query and the success probability of him passing her honesty test. In Section V, we present some variations of the QPQ protocol discussed here, one of which exploits entanglement as a resource to strengthen Alice's privacy. Finally, in Section VI, we analyze what happens when relaxing some of the assumptions adopted in the security proof. In particular, we show that the basic version of the QPQ described here does not guarantee privacy if the database queries admit multiple answers, and we point out some possible solutions.

II. QPQ With Rhetoric Question: Preliminaries and Notation

In the rhetoric version of the QPQ protocol (see Fig. 1), Alice uses two quantum registers each time she needs to interrogate Bob's database. The first register contains $|j\rangle$, the address of the database memory cell she is interested in; the other register is prepared in a quantum superposition of the type $(|j\rangle + |0\rangle)/\sqrt{2}$, "0" being the address of the rhetoric query. Alice then *secretly* and *randomly* chooses one of the two registers and sends it to Bob. He returns the register Alice has sent to him, together with an extra register in which the corresponding answer is encoded. In order to reply to Alice's query without knowing whether it is the superposed query or not, Bob needs to employ the quantum random access memory (qRAM) algorithm [18]–[20]. This algorithm permits to coherently interrogate a database. It requires an address register $|j\rangle$ as input, and it returns the same address

[1] Note that, since Bob's cheats are detected only probabilistically, it is preferable that the whole database record is transferred during a single query (if the database elements are composed of more than one bit). In contrast, in an ideal PIR protocol the security is unvaried if Alice accesses a single bit of the database record at a time.

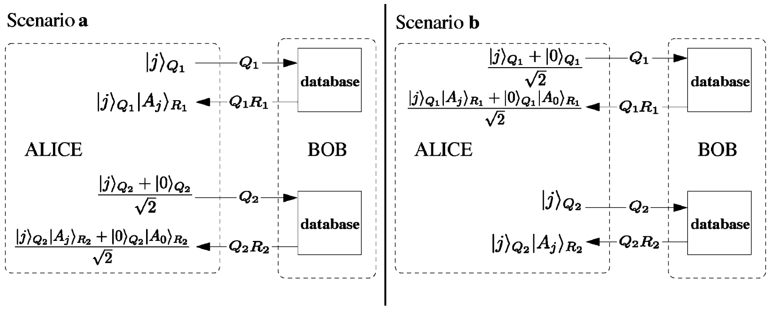
Scenario **a**
$|j\rangle_{Q_1}$
Q_1
$|j\rangle_{Q_1}|A_j\rangle_{R_1}$
Q_1R_1
database
ALICE
BOB
$\frac{|j\rangle_{Q_2}+|0\rangle_{Q_2}}{\sqrt{2}}$
Q_2
$\frac{|j\rangle_{Q_2}|A_j\rangle_{R_2}+|0\rangle_{Q_2}|A_0\rangle_{R_2}}{\sqrt{2}}$
Q_2R_2
database
Scenario **b**
$\frac{|j\rangle_{Q_1}+|0\rangle_{Q_1}}{\sqrt{2}}$
Q_1
$\frac{|j\rangle_{Q_1}|A_j\rangle_{R_1}+|0\rangle_{Q_1}|A_0\rangle_{R_1}}{\sqrt{2}}$
Q_1R_1
database
ALICE
BOB
$|j\rangle_{Q_2}$
Q_2
$|j\rangle_{Q_2}|A_j\rangle_{R_2}$
Q_2R_2
database

Fig. 1. Scheme of the QPQ protocol with rhetoric questions. Alice wants to find out the jth record of Bob's database (composed of $N=2^n$ records). She then prepares two n-qubit registers. The first contains the state $|j\rangle_Q$, while the second contains the quantum superposition $(|j\rangle_Q+|0\rangle_Q)/\sqrt{2}$ between her query and the rhetoric question "0", to which she knows the standard answer A_0. She then sends, in random order (i.e., randomly choosing either scenario **a** or scenario **b**), these two registers to Bob, waiting for his first reply before sending the next register. Bob uses each of the two registers to interrogate his database using a qRAM device [18]–[20], which records the reply to her queries in the two "reply" registers R. At the end of their exchange, Alice possesses the states $|j\rangle_Q|A_j\rangle_R$ and $(|j\rangle_Q|A_j\rangle_R+|0\rangle_Q|A_0\rangle_R)/\sqrt{2}$, where the A_j is the content of the jth record in the database. By measuring the first she obtains the value of A_j, with which she can check whether the superposition in the second state was preserved. If this is not the case, then she can be confident Bob that Bob has violated her privacy, and has tried to obtain information on what j was.

register together with a "reply" register $|A_j\rangle$ which contains the unique value A_j of the requested database element. Since the algorithm is coherent, it works also on superposed address registers, namely the state $\sum_j \alpha_j|j\rangle$ is evolved into $\sum_j \alpha_j|j\rangle|A_j\rangle$. The important aspect of the qRAM algorithm is that it can be executed without having knowledge of the state of the address register.

After Alice has received Bob's first reply, she sends her second register and waits for Bob's second reply. Again Bob applies the qRAM and returns her the result.

If Bob has followed the protocol without trying to cheat, Alice now should possess a state which encodes the information she is looking for and an entangled state involving the rhetoric query, whose coherence can be tested to check Bob honesty, i.e., the two states $|j\rangle|A_j\rangle$ and $(|j\rangle|A_j\rangle+|0\rangle|A_0\rangle)/\sqrt{2}$. Alice recovers the value of A_j by measuring the second register in the first state and validates it to make sure that what she got is indeed the correct answer connected to the jth query (see below for the validation procedure). Then she uses this value to prepare a measurement to test whether the superposition has been retained in the second state ("honesty test"). (This is simply a projective measurement on $(|j\rangle|A_j\rangle+|0\rangle|A_0\rangle)/\sqrt{2}$). If either the validating stage or the honesty test fails (i.e., if she finds out that A_j is not the correct answer or if she found that the state Bob has sent her back in reply to $(|j\rangle+|0\rangle)/\sqrt{2}$ is orthogonal to the one she is expecting), she can be confident that Bob has cheated and has violated her privacy. If, instead, the validating and the test pass, she cannot conclude anything. In fact, suppose that Bob has measured the state and collapsed it to the form $|j\rangle|A_j\rangle$ or to the form $|0\rangle|A_0\rangle$, it still has a probability 1/2 to pass Alice's test of it being of the form $(|j\rangle|A_j\rangle+|0\rangle|A_0\rangle)/\sqrt{2}$. So Alice's honesty test allows her to be confident that Bob has cheated if the test fails, but she can never be completely confident that Bob has not cheated if the test passes.

As mentioned above, before performing the honesty test Alice needs to validate the received message. Namely, Alice has to check whether the answer A_j she received from Bob is the unique one connected to the jth query (of course this can be done at any time during the protocol). Such test is mandatory in order to make sure that the received message originated from the deterministic database she is addressing. If not, Bob could have still cheated along the lines detailed in Section VI. In practice there are two scenarios which allows for such validation. If the relation $j \rightarrow A_j$ is determined by some computable function, she should be able to verify that the value A_j is the correct one *a posteriori* by direct computation.[2] If on the contrary $j \rightarrow A_j$ is not computable (e.g., as in the cases of the Social Security Number and national-lottery database discussed in the previous section), then she should at least be able to consult an external trusted party that certifies the reply A_j. It is important to note that, since she catches a cheating Bob only probabilistically, it is not necessary for her to validate every single answer she receives from him. She can verify only a random subset of them (otherwise one could argue that Bob's intervention would be useless, as Alice could refer only to the trusted third party).

As anticipated, another important aspect of the QPQ protocol is data privacy. Since Alice has access to any of Bob's database elements, data privacy should be intended in the sense that the *amount* of information that Bob is willing to release is limited. In the rhetoric version we discuss here this is automatically enforced by the fact that Alice and Bob exchange a number of bits logarithmic in the database size: Alice sends $2\log_2 N$ qubits, and receives from Bob the same $2\log_2 N$ qubits she had sent, plus two copies of the reply register R. Through the Holevo bound [21], this implies that she receives no more information on the database than twice the number of bits contained in the register R. This is a logarithmic quantity of information with respect to the database size: data privacy is strongly enforced. User privacy, on the other hand, is only enforced through cheat sensitivity, namely through the fact that Bob does not want to be caught cheating.

A. Notation

We now introduce the notation which will be used. We define $X \equiv \{0,1,\ldots,N-1\}$ the source space which contains the addresses j of the memory cells which compose Bob's determin-

[2] Note that this does not necessarily mean that she could have calculated the value of A_j from j in the first place (as in the NP complexity class problems [18]).

istic database, identifying with $j=0$ the address of the rhetoric query. For each j we define A_j to be the information associated with the jth address. As mentioned in the introduction the A_j are *classical messages* composed of m bits, and they need not to represent distinct messages (i.e., we allow the possibility that $A_j = A_{j'}$ for $j \neq j'$), but they are uniquely determined by the value of j. In this context, Bob's database is defined as the ordered set $\mathcal{D} \equiv \{A_j | j \in X\}$ formed by the strings A_j. We define $Q = Q_1, Q_2$ the two quantum registers Alice uses to submit her queries; according to the protocol, she will first send Q_1, wait for Bob's answer and then send Q_2. In this notation, for $k = 1, 2$, the vector $|j\rangle_{Q_k}$ is the state of the kth register which carries the address of the jth database memory. For all $j \neq 0$ we use the vector $|+j\rangle_{Q_k}$ to represent the superposition of the jth query and the rhetoric query, i.e.,

$$|+j\rangle_{Q_k} \equiv (|j\rangle_{Q_k} + |0\rangle_{Q_k})/\sqrt{2} \tag{1}$$

(for $j=0$, we set $|+0\rangle_{Q_k} \equiv |0\rangle_{Q_k}$). We define $R \equiv R_1, R_2$ the registers which Bob is supposed to use for communicating the database entries. After having received Q_1 from Alice, Bob encodes the necessary information on R_1 and sends back to her both Q_1 and R_1. Analogously, after having received Q_2, he will encode information on R_2 and send her back both Q_2 and R_2. It is useful to also define the vectors

$$|C_j\rangle_{Q_kR_k} \equiv |j\rangle_{Q_k}|A_j\rangle_{R_k} \tag{2}$$

$$|C_{\pm j}\rangle_{Q_kR_k} \equiv (|C_j\rangle_{Q_kR_k} \pm |C_0\rangle_{Q_kR_k})/\sqrt{2} \tag{3}$$

[as in (1) for $j=0$ we set $|C_{+0}\rangle_{Q_kR_k} \equiv |C_0\rangle_{Q_kR_k}$]. According to the protocol, the vectors $|C_j\rangle_{Q_kR_k}$ or $|C_{+j}\rangle_{Q_kR_k}$ are the states that an honest Bob should send back to Alice when she is preparing Q_k into the states $|j\rangle_{Q_k}$ or $|+j\rangle_{Q_k}$, respectively. In fact, the states $|C_j\rangle_{Q_kR_k}$ and $|C_{+j}\rangle_{Q_kR_k}$ are the result of the qRAM transformation [18]–[20] when it is fed $|j\rangle_{Q_k}$ and $|+j\rangle_{Q_k}$, respectively.[3] We also introduce an ancillary system B to represent any auxiliary systems that Bob may employ when performing his local transformation on the Alice queries, plus (possibly) an external environment.

Let us use this notation to better formalize the QPQ protocol described above. Suppose then that Alice wants to address the jth entry of the database. The protocol goes as follows.

1) Alice randomly chooses between the two alternative scenarios **a** and **b** (see Fig. 1). In the scenario **a**, she prepares the qubits Q_1 in $|j\rangle_{Q_1}$ and the qubits Q_2 in $|+j\rangle_{Q_2}$. Instead, in the scenario **b** she prepares the states $|+j\rangle_{Q_1}$ and $|j\rangle_{Q_2}$. This means that, in the scenario **a**, she first sends the plain query and then the superposed query. On the contrary, in the scenario **b**, she first sends the superposed query and then the plain query. Consequently, the input state of the system QRB is described by the vectors

$$\left|\Psi_j^{(\ell)}\right\rangle_{QRB} \equiv \begin{cases} |j\rangle_{Q_1}|+j\rangle_{Q_2}|000\rangle_{RB}, & \text{for } \ell = \mathbf{a} \\ |+j\rangle_{Q_1}|j\rangle_{Q_2}|000\rangle_{RB}, & \text{for } \ell = \mathbf{b} \end{cases} \tag{4}$$

where the index ℓ refers to the selected scenario and $|000\rangle_{RB}$ is the fiducial initial state of the systems $R = R_1R_2$ and B (it is independent on ℓ because Bob does not know which scenario Alice has chosen).

2) Now Alice sends Q_1 and waits until Bob gives her back Q_1 and R_1. Then, she sends Q_2 and waits until she gets back Q_2 and R_2.

3) *Honesty Test*: Alice checks the states she has received. If she had selected scenario **a**, she performs a von Neumann measurement to see if QR is in the state $|C_j\rangle_{Q_1R_1}|C_{+j}\rangle_{Q_2R_2}$—see (3). Of course, this can be done in two steps: first she measures Q_1R_1 to learn A_j; then, after having validated it, she uses such value to prepare an appropriate measurement on Q_2R_2. If the measurement fails, then Alice can definitely conclude that Bob was cheating, otherwise she can assume he was honest (although she has no guarantee of it). If she had chosen scenario **b**, she proceeds analogously, using a von Neumann measurement to check if QR is in the state $|C_j\rangle_{Q_2R_2}|C_{+j}\rangle_{Q_1R_1}$.

III. Bob's Transformations

In the QPQ protocol, Alice's privacy relies essentially on the fact that Bob is not allowed to operate jointly on Q_1 and Q_2. This a fundamental constraint: without it, Bob would be able to discover the index j without Alice knowing it. In fact, the subspaces $\mathcal{H}_j$ spanned by the two vectors $|j\rangle_{Q_1}|+j\rangle_{Q_2}$ and $|+j\rangle_{Q_1}|j\rangle_{Q_2}$ (associated to the two different scenarios **a** and **b** for the query j) are mutually orthogonal. Thus, such vectors (and then the corresponding queries) could be easily distinguished by performing on Q_1Q_2 a simple von Neumann measurement defined by the projectors associated with the spaces $\mathcal{H}_j$. This is a measurement that would allow Bob to recover Alice's query without disturbing the input states of Q_1Q_2. To prevent this cheating strategy, the QPQ protocol forces Bob to address Q_1 and Q_2 separately (i.e., he has to send the register Q_1 back, before Alice provides him the register Q_2).

Bob's action when he receives Alice's first register can be described by a unitary operator $U^{(1)}_{Q_1RB}$ which acts on the first register Q_1, on $R = R_1R_2$, and on B (and not on the second register Q_2 which is still in Alice's possession). Analogously, Bob's action when he receives the second register is described by the unitary operator $U^{(2)}_{Q_2R_2B}$ which acts on Q_2, R_2, and B (and not on Q_1 and R_1 which are now in Alice's possession). [Note that the above framework describes also the situation in which Bob is employing nonunitary transformations (i.e., completely positive, trace preserving maps), since the space B can be thought to contain also the Naimark extension [22] that transforms such operations into unitaries]. The above transformations cannot depend on the selected scenario ℓ (as Bob does not know which one, among $\ell = \mathbf{a}$ and $\ell = \mathbf{b}$, has been selected by Alice). Therefore, within the ℓth scenario, the global state at the end of the protocol is described by the vectors

$$\left|\Xi_j^{(\ell)}\right\rangle_{QRB} \equiv U^{(2)}_{Q_2R_2B}U^{(1)}_{Q_1RB}\left|\Psi_j^{(\ell)}\right\rangle_{QRB} \tag{5}$$

with $|\Psi_j^{(\ell)}\rangle_{QRB}$ given in (4).

[3] In particular, $|C_j\rangle_{Q_kR_k}$ is associated with the unique string A_j which on Alice side will pass the validation stage.

A. Some Useful Decompositions

Consider the transformation $U^{(1)}$. In the scenario **a** for all j we can always split the state $U^{(1)}_{Q_1RB}\,(|j\rangle_{Q_1}|000\rangle_{RB})$ as a vector which contains the unique correct answer (2) plus an orthogonal contribution, i.e.,

$$U^{(1)}_{Q_1RB}\,(|j\rangle_{Q_1}|000\rangle_{RB}) = \sqrt{\eta_j^{(1)}}\,\left|C_j;\Phi_j^{(1)}\right\rangle_{Q_1RB} + \sqrt{1-\eta_j^{(1)}}\,\left|V_j^{(1)}\right\rangle_{Q_1RB} \quad (6)$$

where $|C_j;\Phi_j^{(1)}\rangle_{Q_1RB}$ stands for the separable state $|C_j\rangle_{Q_1R_1}|\Phi_j^{(1)}\rangle_{R_2B}$ and where $|V_j^{(1)}\rangle_{Q_1RB}$ is a vector whose Q_1, R_1 components are orthogonal to $|C_j\rangle_{Q_1R_1}$, i.e.,

$${}_{Q_1R_1}\left\langle C_j \,\middle|\, V_j^{(1)} \right\rangle_{Q_1RB} = 0. \quad (7)$$

The separability of $|C_j;\Phi_j^{(1)}\rangle_{Q_1RB}$ with respect to the bipartition Q_1R_1/R_2B follows from the assumption that Bob's answer A_j is unique: he does not have any degree of freedom he can use to correlate the Q_1R_1 space with anything else. If this hypothesis is dropped the component $|C_j;\Phi_j^{(1)}\rangle_{Q_1RB}$ does not need to be separable as there are different possible "correct" answers to Alice's query. We will see in Section VI that when this happens, the QPQ scheme we are discussing here does not guarantee user privacy: in this case, Bob can in fact recover partial information on Alice's query undetected (i.e., with zero probability of being caught) by replying with quantum superpositions of the possible correct answers. This is the reason behind the necessity of the validation stage in which Alice (perhaps probabilistically) verifies that the A_j she is reading is indeed the unique correct answer to the query j.

From condition (7), it is clear that $\eta_j^{(1)}$ is the probability that the state (6) will be found in $|C_j\rangle_{Q_1R_1}$. In the scenario **b**, instead, for $j \neq 0$, we can write

$$U^{(1)}_{Q_1RB}(|+j\rangle_{Q_1}|000\rangle_{RB}) = \sqrt{\overline{\eta}_j^{(1)}}\,\left|C_{+j};\overline{\Phi}_j^{(1)}\right\rangle_{Q_1RB} + \sqrt{1-\overline{\eta}_j^{(1)}}\,\left|\overline{V}_j^{(1)}\right\rangle_{Q_1RB}. \quad (8)$$

As before $|C_{+j};\overline{\Phi}_j^{(1)}\rangle_{Q_1RB} \equiv |C_{+j}\rangle_{Q_1R_1}|\overline{\Phi}_j^{(1)}\rangle_{Q_1R_2B}$ (where again the separability is granted by the uniqueness of A_j) and $|\overline{V}_j^{(1)}\rangle_{Q_1RB}$ is a vector orthogonal to the "check state" $|C_{+j}\rangle_{Q_1R_1}$ Alice is expecting, i.e.,

$${}_{Q_1R_1}\left\langle C_{+j} \,\middle|\, \overline{V}_j^{(1)} \right\rangle_{Q_1RB} = 0. \quad (9)$$

Consequently $\overline{\eta}_j^{(1)}$ is the probability that the state (8) will pass the test of being in $|C_{+j}\rangle_{Q_1R_1}$. The state on the first line of (8) can be expanded on a basis of which the state on the first line of (6) is a component. Therefore, $\overline{\eta}_j^{(1)}$ and $\eta_j^{(1)}$ must be related. The security analysis given in the following sections is based on the study of this relation.

Analogous decompositions can be given for $U^{(2)}$: in this case, however, it is useful to describe them not in terms of the input states, but in terms of the state of the system *after it has passed the test on the subsystems* Q_1R_1. For $j \neq 0$, in the scenario **a** this gives

$$U^{(2)}_{Q_2R_2B}\left(|+j\rangle_{Q_2}\left|\Phi_j^{(1)}\right\rangle_{R_2B}\right) = \sqrt{\overline{\eta}_j^{(2)}}\,\left|C_{+j};\overline{\Phi}_j^{(2)}\right\rangle_{Q_2R_2B} + \sqrt{1-\overline{\eta}_j^{(2)}}\,\left|\overline{V}_j^{(2)}\right\rangle_{Q_2R_2B}. \quad (10)$$

Here $|C_{+j};\overline{\Phi}_j^{(2)}\rangle_{Q_2R_2B} \equiv |C_{+j}\rangle_{Q_2R_2} \otimes |\overline{\Phi}_j^{(2)}\rangle_B$, and $|\overline{V}_j^{(2)}\rangle_{Q_2R_2B}$ is a vector orthogonal to $|C_{+j}\rangle_{Q_2R_2}$ of (3), i.e.,

$${}_{Q_2R_2}\left\langle C_{+j} \,\middle|\, \overline{V}_j^{(2)} \right\rangle_{Q_2R_2B} = 0.$$

Thus, $\overline{\eta}_j^{(2)}$ is the probability that the state (10) will pass the test of being in $|C_{+j}\rangle_{Q_2R_2}$. Notice that the vector $|\Phi_j^{(1)}\rangle_{R_2B}$ in the first line of (10) is the state of R_2B one obtains in the scenario **a** if, after the first round, the state Q_1R_1 passes the test of being $|C_j\rangle_{Q_1R_1}$—see (6). In the scenario **b**, instead, we have

$$U^{(2)}_{Q_2RB}\left(|j\rangle_{Q_2}\left|\overline{\Phi}_j^{(1)}\right\rangle_{R_2B}\right) = \sqrt{\eta_j^{(2)}}\left|C_j;\Phi_j^{(2)}\right\rangle_{Q_2R_2B} + \sqrt{1-\eta_j^{(2)}}\,\left|V_j^{(2)}\right\rangle_{Q_2R_2B} \quad (11)$$

where $|C_j;\Phi_j^{(2)}\rangle_{Q_2R_2B}$ stands for $|C_j\rangle_{Q_2R_2} \otimes |\Phi_j^{(2)}\rangle_B$, and $|V_j^{(2)}\rangle_{Q_2R_2B}$ is a vector orthogonal to the state $|C_j\rangle_{Q_2R_2}$, i.e.,

$${}_{Q_2R_2}\left\langle C_j \,\middle|\, V_j^{(2)} \right\rangle_{Q_2R_2B} = 0$$

and $\eta_j^{(2)}$ is the probability that the state (11) will be found in $|C_j\rangle_{Q_2R_2}$.

The case $j=0$ has to be treated separately: indeed, if Alice sends this query then both Q_1 and Q_2 will be prepared into $|0\rangle$. In this case, it is then useful to define $U^{(2)}$ by considering its action on the vector $|0\rangle_{Q_2}|\Phi_0^{(1)}\rangle_{R_2B}$ with $|\Phi_0^{(1)}\rangle_{R_2B}$ defined as in (6), i.e.,

$$U^{(2)}_{Q_2RB}\left(|0\rangle_{Q_2}\left|\Phi_0^{(1)}\right\rangle_{R_2B}\right) = \sqrt{\eta_0^{(2)}}\,\left|C_0;\Phi_0^{(2)}\right\rangle_{Q_2R_2B} + \sqrt{1-\eta_0^{(2)}}\left|V_0^{(2)}\right\rangle_{Q_2R_2B} \quad (12)$$

where again one has $|C_0;\Phi_0^{(2)}\rangle_{Q_2R_2B} \equiv |C_0\rangle_{Q_2R_2} \otimes |\Phi_0^{(2)}\rangle_B$, and

$${}_{Q_2R_2}\left\langle C_0 \,\middle|\, V_0^{(2)} \right\rangle_{Q_2R_2B} = 0.$$

From the above equations, it follows that for $j \neq 0$ the final state (5), after Bob has finished his manipulations, can be written as follows for scenario **a**:

$$\begin{aligned}\left|\Xi_j^{(\mathbf{a})}\right\rangle = &\sqrt{\eta_j^{(1)}\overline{\eta}_j^{(2)}}|C_{+j}\rangle_{Q_2R_2}|C_j\rangle_{Q_1R_1}\left|\overline{\Phi}_j^{(2)}\right\rangle_B\\ &+\sqrt{\eta_j^{(1)}\left(1-\overline{\eta}_j^{(2)}\right)}|C_j\rangle_{Q_1R_1}\left|\overline{V}_j^{(2)}\right\rangle_{Q_2R_2B}\\ &+\sqrt{1-\eta_j^{(1)}}U^{(2)}_{Q_2R_2B}|+j\rangle_{Q_2}\left|V_j^{(1)}\right\rangle_{Q_1RB}\end{aligned} \quad (13)$$

where all the terms in the second and third line are orthogonal to $|C_{+j}\rangle_{Q_2R_2}|C_j\rangle_{Q_1R_1}$. Analogously, we have for scenario **b**

$$\begin{aligned}\left|\Xi_j^{(\mathbf{b})}\right\rangle = &\sqrt{\overline{\eta}_j^{(1)}\eta_j^{(2)}}|C_j\rangle_{Q_2R_2}|C_{+j}\rangle_{Q_1R_1}\left|\Phi_j^{(2)}\right\rangle_B\\ &+\sqrt{\overline{\eta}_j^{(1)}\left(1-\eta_j^{(2)}\right)}|C_{+j}\rangle_{Q_1R_1}\left|V_j^{(2)}\right\rangle_{Q_2R_2B}\\ &+\sqrt{1-\overline{\eta}_j^{(1)}}U^{(2)}_{Q_2R_2B}|j\rangle_{Q_2}\left|\overline{V}_j^{(1)}\right\rangle_{Q_1RB}\end{aligned} \quad (14)$$

where, again, the states in the last two lines are orthogonal to the state in the first. Instead, for $j = 0$, we have

$$\begin{aligned}\left|\Xi_0^{(\mathbf{a},\mathbf{b})}\right\rangle = &\sqrt{\eta_0^{(1)}\eta_0^{(2)}}|C_0\rangle_{Q_2R_2}|C_0\rangle_{Q_1R_1}\left|\Phi_0^{(2)}\right\rangle_B\\ &+\sqrt{\eta_0^{(1)}\left(1-\eta_0^{(2)}\right)}|C_0\rangle_{Q_1R_1}\left|V_0^{(2)}\right\rangle_{Q_2R_2B}\\ &+\sqrt{1-\eta_0^{(1)}}U^{(2)}_{Q_2R_2B}|0\rangle_{Q_2}\left|V_0^{(1)}\right\rangle_{Q_1RB}.\end{aligned} \quad (15)$$

IV. Information-Disturbance Tradeoff and User Privacy

In this section, we present an information-disturbance analysis of the QPQ protocol. This will yield a trade-off which shows that, if Bob tries to get some information on Alice's queries, then she has a nonzero probability of detecting that he is cheating. The same analysis can be easily reproduced for more complicated versions of the protocol. For instance Alice may hide her queries into superpositions of randomly selected queries. In this case, the derivation, although more involved, is a straightforward generalization of the one presented here.

According to (5), to measure Bob's information gain, it is sufficient to study how the final state of the ancillary subsystem B depends upon Alice's query j. Exploiting the decompositions introduced in Section III we can then show that one can force B to keep no track of Alice's query by bounding the success probabilities that Bob will pass the QPQ honesty test. Specifically, indicating with $P_j^{(\ell)}$ the success probability associated with Alice's query j in the ℓth scenario and defining $\rho_B^{(\ell)}(j)$ the corresponding output state of B, in Section IV-A, we will prove the following theorem

Theorem: Choose $\epsilon \in [0,1]$ so that $P_j^{(\ell)} > 1-\epsilon$ for all j and ℓ. Then there exists a state σ_B^* of B and a positive constant $c \leq 151.3$ such that the fidelities [23], [24] $F(\rho_B^{(\ell)}(j);\sigma_B^*)$ are bounded as follows:

$$\left|F\left(\rho_B^{(\ell)}(j);\sigma_B^*\right)-1\right| < c\epsilon^{1/4} \quad (16)$$

for all all j and ℓ.

This implies that, by requiring Bob's probabilities of passing the honesty test to be higher than a certain threshold $1-\epsilon$, then the final states of B will be forced in the vicinity of a common fixed state σ_B^*, which is independent from the choice of j and ℓ. This in turn implies that, for sufficiently small values of ϵ, Bob will not be able to distinguish reliably between different values of j using the states in his possession at the end of the protocol. In particular, if $\epsilon = 0$, i.e., if Bob wants to be sure that he passes the honesty test, then the final states for any choice of j will coincide with σ_B^*, i.e., they will be completely independent from j: he cannot retain any memory of what Alice's query was. It is also worth noticing that since the total number of queries, as well as the number of scenarios ℓ, is finite and randomly selected by Alice, then the requirement on $P_j^{(\ell)}$ in the theorem can be replaced by a similar condition on the *average probability* of success.[4]

In Section IV-B, we will employ the above theorem to bound the *mutual information* I [25] that connects the classical variable $j \in \{1,\ldots,N-1\}$, which labels Alice's query, and Bob's estimation of this variable. Assuming that initially Bob does not have any prior information on the value of j that Alice is interested in, we will determine the value I at the end of the protocol, showing that this quantity is upper-bounded by the parameter ϵ of (16). Specifically, we will show that by requiring that Bob passes the honesty test with a probability greater than $1-\epsilon$, then Alice can bound Bob's information as

$$I \leq c\,\epsilon^{1/4}\,\log_2 N \quad (17)$$

N being the number of database entries: his information is upper bounded by a quantity that depends monotonically on a lower bound to his probability $P_j^{(\ell)}$ of passing the honesty test. Thus, if he wants to pass the honesty test with high probability, he must retain little information on Alice's query.

The bounds (16) and (17) are rather weak as implied by the fourth root of ϵ in these equations. However, as is clear from the subsequent proof, the security parameters we derive are only loose (i.e., nontight) lower bounds to the actual values: to avoid further complicating the proof, we have not derived the optimal bounds. In other words, already the simple variant of the protocol discussed here is certainly more secure than the numbers we derive suggest. Furthermore, as discussed in Section V, better performance is expected by relaxing some of the hypothesis we have assumed on Alice's encodings. Finally we stress

[4] Since the number N of entries j is finite, the condition $P_j^{(\ell)} > 1-\epsilon$ can be imposed by requiring a similar condition on the *average probability* $P \equiv \sum_{\ell,j} P_j^{(\ell)}/(2N)$. Indeed, assume $P > 1-\epsilon'$ and let P_* be the minimum of the $P_j^{(\ell)}$ for all j and ℓ. Since there are $2N$ terms each contributing to P with probability $1/2N$, we have

$$1-\epsilon' < P \leq P_*/2N + (2N-1)/2N$$

that gives $P_* > 1-2N\epsilon'$. The condition $P_j^{(\ell)} > 1-\epsilon$ then follows by taking $\epsilon = 2N\epsilon'$.

that the while (16) and (17) refers to the information that Bob recovers on Alice's query (i.e., to the user privacy), the protocol entails also a strict data privacy due to the limited number of qubits Alice receives from the database, i.e., $O(\log N)$.

A. Proof of the Theorem

Assume that Alice randomly chooses the scenarios **a** and **b** with probability 1/2. From (13) and (14), it is easy to verify that the success probability that Bob will pass the honesty test when Alice is submitting the jth query is

$$P_j = \frac{1}{2}\left(P_j^{(\mathbf{a})} + P_j^{(\mathbf{b})}\right) = \frac{1}{2}\left(\eta_j^{(1)}\overline{\eta}_j^{(2)} + \eta_j^{(2)}\overline{\eta}_j^{(1)}\right) \tag{18}$$

where $P_j^{(\mathbf{a})} \equiv \eta_j^{(1)}\overline{\eta}_j^{(2)}$ and $P_j^{(\mathbf{b})} \equiv \eta_j^{(2)}\overline{\eta}_j^{(1)}$ refer to the success probabilities in the scenarios **a** and **b**, respectively (these expressions hold also for $j = 0$ by setting $\overline{\eta}_0^{(1,2)} \equiv \eta_0^{(1,2)}$). The corresponding output density matrix of the ancillary system B is given by

$$\rho_B(j) = \frac{1}{2}\left[\rho_B^{(\mathbf{a})}(j) + \rho_B^{(\mathbf{b})}(j)\right] \tag{19}$$

where, for $\ell = \mathbf{a}$ and $\mathbf{b}$, the state $\rho_B^{(\ell)}(j)$ are obtained by partial tracing on Alice's spaces the output vectors of (13) and (14), i.e.,

$$\begin{aligned}\rho_B^{(\ell)}(j) &\equiv \mathrm{Tr}_{QR}\left[\left|\Xi_j^{(\ell)}\right\rangle\left\langle\Xi_j^{(\ell)}\right|\right]\\ &= P_j^{(\ell)}\,\sigma_B^{(\ell)}(j) + \left[1 - P_j^{(\ell)}\right]\,\tilde{\sigma}_B^{(\ell)}(j) \qquad (20)\\ \text{where} \qquad \sigma_B^{(\mathbf{a})}(j) &\equiv \left|\overline{\Phi}_j^{(2)}\right\rangle_B\left\langle\overline{\Phi}_j^{(2)}\right| \qquad (21)\\ \sigma_B^{(\mathbf{b})}(j) &\equiv \left|\Phi_j^{(2)}\right\rangle_B\left\langle\Phi_j^{(2)}\right| \qquad (22)\end{aligned}$$

and where the state $\tilde{\sigma}_B^{(\ell)}(j)$ contains the contribution to the partial trace coming from the last two lines of (13) and (14). The quantities $\sigma_B^{(\ell)}(j)$ (for $\ell = \mathbf{a}$ and $\mathbf{b}$) are the density matrices obtained by projecting $|\Xi_j^{(\ell)}\rangle_{QRB}$ into the state of QR which allows Bob to pass the honesty test (i.e., $|C_j\rangle_{Q_1R_1}|C_{+j}\rangle_{Q_2R_2}$ for $\ell = \mathbf{a}$ and $|C_{+j}\rangle_{Q_1R_1}|C_j\rangle_{Q_2R_2}$ for $\ell = \mathbf{b}$).

In accordance with the theorem's hypothesis, we consider the case in which the probability of passing the test (18) for an arbitrary j is higher than a certain threshold, i.e.,

$$P_j^{(\ell)} > 1 - \epsilon \tag{23}$$

with $\epsilon \in [0, 1]$. We will then prove (16) by identifying the density matrix σ_B^* with the pure state $|\Phi_0^{(2)}\rangle_B$ defined as in (12) and showing that the following condition holds:

$$F\left(\rho_B^{(\ell)}(j), \left|\Phi_0^{(2)}\right\rangle_B\right) > 1 - 151.3\,\epsilon^{1/4} \tag{24}$$

where F is the fidelity [23], [24]. Such inequality is a consequence of the fact that we want Bob to preserve the coherence of the superposition $|+j\rangle$, and at the same time to answer correctly to query $|j\rangle$. To derive it we use (20) and the condition (23) to write

$$F\left(\rho_B^{(\ell)}(j), \left|\Phi_0^{(2)}\right\rangle_B\right) \geq (1-\epsilon)F\left(\sigma_B^{(\ell)}(j), \left|\Phi_0^{(2)}\right\rangle_B\right). \tag{25}$$

To prove (24), it is then sufficient to verify that for all j one has

$$\begin{aligned}F\left(\sigma_B^{(\mathbf{a})}(j), \left|\Phi_0^{(2)}\right\rangle\right) &= \left|\left\langle \Phi_j^{(2)} \,\middle|\, \Phi_0^{(2)}\right\rangle\right|^2 > 1 - 150.3\,\epsilon^{1/4}\\ F\left(\sigma_B^{(\mathbf{b})}(j), \left|\Phi_0^{(2)}\right\rangle\right) &= \left|\left\langle \overline{\Phi}_j^{(2)} \,\middle|\, \Phi_0^{(2)}\right\rangle\right|^2 > 1 - 150.3\,\epsilon^{1/4}\end{aligned} \tag{26}$$

(the label B on the vectors has been dropped for ease of notation). This part of the derivation is similar to the one used in [26] and can be split in two parts, which will be derived in the following:

i) First we use (23) and the definitions (6) and (8) to show that for all $j \neq 0$ one has

$$\left|\left\langle \Phi_j^{(1)} \,\middle|\, \Phi_0^{(1)}\right\rangle\right|^2 > 1 - 23.4\,\sqrt{\epsilon} \tag{27}$$

$$\left|\left\langle \overline{\Phi}_j^{(1)} \,\middle|\, \Phi_0^{(1)}\right\rangle\right|^2 > 1 - 13.7\,\sqrt{\epsilon}. \tag{28}$$

ii) Then we use (27), (28), and the definitions (10) and (11) to verify that for $j \neq 0$ one has

$$\left|\left\langle \Phi_j^{(2)} \,\middle|\, \Phi_0^{(2)}\right\rangle\right|^2 > 1 - 150.3\,\epsilon^{1/4} \tag{29}$$

$$\left|\left\langle \overline{\Phi}_j^{(2)} \,\middle|\, \Phi_0^{(2)}\right\rangle\right|^2 > 1 - 14.6\,\epsilon^{1/4} \tag{30}$$

which implies (26) and hence the theorem with $c = 151.3$.

Derivation of Part i): The condition (23) implies the following inequalities:

$$\eta_j^{(1,2)} > 1 - \epsilon, \qquad \overline{\eta}_j^{(1,2)} > 1 - \epsilon \tag{31}$$

for all $j \in \{0, 1, \ldots, N-1\}$. To obtain inequality (27), we compare (6) and (8) under the constraint imposed by (31). In particular, we notice that for $j \neq 0$ (6) gives

$$U_{Q_1RB}^{(1)}\ \left(|+j\rangle_{Q_1}|000\rangle_{RB}\right) = |W_j\rangle_{Q_1RB} + |\Delta W_j\rangle_{Q_1RB} \tag{32}$$

with

$$\begin{aligned}|W_j\rangle &= \frac{\sqrt{\eta_j^{(1)}}\,\left|C_j; \Phi_j^{(1)}\right\rangle + \sqrt{\eta_0^{(1)}}\,\left|C_0; \Phi_0^{(1)}\right\rangle}{\sqrt{2}}\\ |\Delta W_j\rangle &= \frac{\sqrt{1-\eta_j^{(1)}}\,\left|V_j^{(1)}\right\rangle + \sqrt{1-\eta_0^{(1)}}\left|V_0^{(1)}\right\rangle}{\sqrt{2}}.\end{aligned} \tag{33}$$

According to (31), the vector $|\Delta W_j\rangle_{Q_1RB}$ has a norm of the order ϵ. This implies that in the limit $\epsilon \to 0$ the vector (32) tends to $|W_j\rangle_{Q_1RB}$. Analogously, (8) and the second inequality of (31) tell us that in the limit $\epsilon \to 0$, the state $U^{(1)}_{Q_1RB}(|+j\rangle_{Q_1}|000\rangle_{RB})$ converges to the vector $|C_{+j};\overline{\Phi}^{(1)}_j\rangle_{Q_1RB}$. Combining these two observations, it follows that for $\epsilon \to 0$ the vectors $|W_j\rangle_{Q_1RB}$ and $|C_{+j};\overline{\Phi}^{(1)}_j\rangle_{Q_1RB}$ coincide. According to definition (3), this implies that $|\Phi^{(1)}_j\rangle_{R_2B}$, $|\Phi^{(1)}_0\rangle_{R_2B}$ and $|\overline{\Phi}^{(1)}_j\rangle_{R_2B}$ must converge for $\epsilon \to 0$. To make this statement quantitatively precise, evaluate the scalar product between (32) and (8), and obtain the identity

$$\begin{aligned}1 &= \sqrt{\overline{\eta}^{(1)}_j}\left\langle W_j \middle| C_{+j};\overline{\Phi}^{(1)}_j\right\rangle \\ &\quad + \sqrt{1-\overline{\eta}^{(1)}_j}\left\langle W_j \middle| \overline{V}^{(1)}_j\right\rangle \\ &\quad + \sqrt{\overline{\eta}^{(1)}_j}\left\langle \Delta W_j \middle| C_{+j};\overline{\Phi}^{(1)}_j\right\rangle \\ &\quad + \sqrt{1-\overline{\eta}^{(1)}_j}\left\langle \Delta W_j \middle| \overline{V}^{(1)}_j\right\rangle. \qquad (34)\end{aligned}$$

It can be simplified by using the following inequalities:

$$\begin{aligned}&\left|\left\langle W_j \middle| C_{+j};\overline{\Phi}^{(1)}_j\right\rangle\right| \\ &\quad\le \frac{\sqrt{\eta^{(1)}_j}\left|\left\langle \Phi^{(1)}_j \middle| \overline{\Phi}^{(1)}_j\right\rangle\right| + \sqrt{\eta^{(1)}_0}\left|\left\langle \Phi^{(1)}_0 \middle| \overline{\Phi}^{(1)}_j\right\rangle\right|}{2} \\ &\left|\left\langle W_j \middle| \overline{V}^{(1)}_j\right\rangle\right| \le 1 \\ &\left|\left\langle \Delta W_j \middle| C_{+j};\overline{\Phi}^{(1)}_j\right\rangle\right| < \sqrt{\epsilon}, \quad \left|\left\langle \Delta W_j \middle| \overline{V}^{(1)}_j\right\rangle\right| < \sqrt{2\epsilon}\end{aligned}$$

which can be easily derived from (33) by invoking the orthogonality conditions (9). Replacing the above expressions into (34), we get

$$\begin{aligned}1 < \frac{\sqrt{\overline{\eta}^{(1)}_j\eta^{(1)}_j}}{2}\left|\left\langle \Phi^{(1)}_j \middle| \overline{\Phi}^{(1)}_j\right\rangle\right| &+ \frac{\sqrt{\overline{\eta}^{(1)}_j\eta^{(1)}_0}}{2} \\ &\times\left|\left\langle \Phi^{(1)}_0 \middle| \overline{\Phi}^{(1)}_j\right\rangle\right| + 2\sqrt{\epsilon} + \sqrt{2}\epsilon \qquad (35)\end{aligned}$$

and thus

$$\frac{\left|\left\langle \Phi^{(1)}_j \middle| \overline{\Phi}^{(1)}_j\right\rangle\right| + \left|\left\langle \Phi^{(1)}_0 \middle| \overline{\Phi}^{(1)}_j\right\rangle\right|}{2} \ge 1 - (2\sqrt{\epsilon} + \sqrt{2}\epsilon)$$

which provides a bound for the average of $|\langle\Phi^{(1)}_j|\overline{\Phi}^{(1)}_j\rangle|$ and $|\langle\Phi^{(1)}_0|\overline{\Phi}^{(1)}_j\rangle|$. Therefore, we can conclude that

$$\begin{aligned}&\max\left\{\left|\left\langle \Phi^{(1)}_0 \middle| \overline{\Phi}^{(1)}_j\right\rangle\right|, \left|\left\langle \Phi^{(1)}_j \middle| \overline{\Phi}^{(1)}_j\right\rangle\right|\right\} \\ &\quad \ge 1 - (2\sqrt{\epsilon} + \sqrt{2}\epsilon) \qquad (36) \\ &\min\left\{\left|\left\langle \Phi^{(1)}_0 \middle| \overline{\Phi}^{(1)}_j\right\rangle\right|, \left|\left\langle \Phi^{(1)}_j \middle| \overline{\Phi}^{(1)}_j\right\rangle\right|\right\} \\ &\quad \ge 1 - 2(2\sqrt{\epsilon} + \sqrt{2}\epsilon) \qquad (37)\end{aligned}$$

where the second follows by using the fact that $|\langle\Phi^{(1)}_0|\overline{\Phi}^{(1)}_j\rangle|$ and $|\langle\Phi^{(1)}_j|\overline{\Phi}^{(1)}_j\rangle|$ can both be maximized by 1. We are almost there: indeed (28) follows via simple manipulations by squaring both terms of (37). To derive (27) we apply the triangular inequality[5] to the vectors $|\Phi^{(1)}_0\rangle$, $|\Phi^{(1)}_j\rangle$ and $|\overline{\Phi}^{(1)}_j\rangle$. This yields

$$\begin{aligned}\left|\left\langle \Phi^{(1)}_j \middle| \overline{\Phi}^{(1)}_0\right\rangle\right|^2 \ge 1 - &\left[\sqrt{1 - \left|\left\langle \Phi^{(1)}_0 \middle| \overline{\Phi}^{(1)}_j\right\rangle\right|^2}\right. \\ &\left. + \sqrt{1 - \left|\left\langle \Phi^{(1)}_j \middle| \overline{\Phi}^{(1)}_j\right\rangle\right|^2}\right]^2 \ge 1 - 23.4\sqrt{\epsilon} \qquad (38)\end{aligned}$$

where the last inequality follows from (36) and (37).

Derivation of Part II: The main difference between the set of (6), (8), and the set of (10), (11) is the fact that, in the former, $U^{(1)}$ acts on vectors with fixed RB component, while, in the latter, $U^{(2)}$ operates on vectors whose R_2B components may vary with j. We can take care of this by replacing $|\Phi^{(1)}_j\rangle_{R_2B}$ and $|\overline{\Phi}^{(1)}_j\rangle_{R_2B}$ with the constant vector $|\Phi^{(1)}_0\rangle_{R_2B}$. This is, of course, not surprising, given the inequalities of (27) and (28). To see it explicitly, evaluate the scalar product between $U^{(2)}_{Q_2RB}(|j\rangle_{Q_2}|\overline{\Phi}^{(1)}_j\rangle_{R_2B})$ and $U^{(2)}_{Q_2RB}(|j\rangle_{Q_2}|\Phi^{(1)}_0\rangle_{R_2B})$. For $j \neq 0$ it gives

$$\begin{aligned}\left\langle \overline{\Phi}^{(1)}_j \middle| \Phi^{(1)}_0\right\rangle = &\sqrt{\eta^{(2)}_j}\left\langle C_j;\Phi^{(2)}_j \middle| U^{(2)} \middle| j;\Phi^{(1)}_0\right\rangle \\ &+ \sqrt{1-\eta^{(2)}_j}\left\langle V^{(2)}_j \middle| U^{(2)} \middle| j;\Phi^{(1)}_0\right\rangle. \qquad (39)\end{aligned}$$

From the inequalities (31) and (28), it then follows that the modulus of $\kappa_j \equiv \langle C_j;\Phi^{(2)}_j|U^{(2)}|j;\Phi^{(1)}_0\rangle$ must be close to one. An estimation based on (37) yields the following bound:

$$|\kappa_j|^2 > 1 - 10.0\sqrt{\epsilon}. \qquad (40)$$

Proceeding analogously for the vectors $U^{(2)}|+j;\Phi^{(1)}_0\rangle$ and $U^{(2)}|+j;\Phi^{(1)}_j\rangle$, we obtain

$$|\overline{\kappa}_j|^2 \equiv \left|\left\langle C_{+j};\overline{\Phi}^{(2)}_j \middle| U^{(2)} \middle| +j;\Phi^{(1)}_0\right\rangle\right|^2 > 1 - 26.4\sqrt{\epsilon}. \qquad (41)$$

For all $j \neq 0$ we can then write the following decompositions:

$$\begin{aligned}U^{(2)}_{Q_2RB}\left(|j\rangle_{Q_2}\left|\Phi^{(1)}_0\right\rangle_{R_2B}\right) &= \kappa_j\left|C_j;\Phi^{(2)}_j\right\rangle_{Q_2R_2B} \\ &\quad + \sqrt{1-|\kappa_j|^2}|Z_j\rangle_{Q_2R_2B} \qquad (42) \\ U^{(2)}_{Q_2R_2B}(|+j\rangle_{Q_2}\left|\Phi^{(1)}_0\right\rangle_{R_2B}) &= \overline{\kappa}_j\left|C_{+j};\overline{\Phi}^{(2)}_j\right\rangle_{Q_2R_2B} \\ &\quad + \sqrt{1-|\overline{\kappa}_j|^2}\,|\overline{Z}_j\rangle_{Q_2R2B} \qquad (43)\end{aligned}$$

where $|Z_j\rangle$ and $|\overline{Z}_j\rangle$ are vectors orthogonal to $|C_j;\Phi^{(2)}_j\rangle$ and $|C_{+j};\overline{\Phi}^{(2)}_j\rangle$ respectively. The inequality (30) can now be de-

[5] This is the triangular inequality associated to the trace distance $D(|\psi\rangle,|\phi\rangle) = (1/2)\mathrm{Tr}[||\psi\rangle\langle\psi| - |\phi\rangle\langle\phi||] = \sqrt{1-|\langle\psi|\phi\rangle|^2}$.

rived by taking the scalar product between (43) and (12), remembering that $|V_0^{(2)}\rangle$ is orthogonal to $|C_0\rangle$ and using (31) and (41). To derive (29), instead, we first evaluate the scalar product between (42) and (43) obtaining

$$\left|\left\langle \overline{\Phi}_j^{(2)} \,\middle|\, \Phi_j^{(2)} \right\rangle\right|^2 > 1 - 23.5\, \epsilon^{1/4}$$

and then, as in (38), we impose the triangular inequality between the vectors $|\overline{\Phi}_j^{(2)}\rangle$, $|\Phi_j^{(2)}\rangle$ and $|\Phi_0^{(2)}\rangle$.

B. Bound on Bob's Information

Here, we give an upper bound to Bob's information on the variable j. This can be done by noticing that we can treat B as a *quantum source* which encodes the classical information produced by the classical random source X. Specifically, this quantum source will be characterized by the quantum ensemble $\mathcal{E} \equiv \{p_j = 1/N, \rho_B(j)\}$, where $p_j = 1/N$ is Alice's probability of selecting the jth query, and $\rho_B(j)$ is given by (19). We can then give an upper bound to Bob's information by considering the mutual information I associated with the ensemble $\mathcal{E}$. From the Holevo bound [21], we obtain

$$I \le \chi(\mathcal{E}) \equiv S(\rho_B) - \frac{1}{N}\sum_{j=0}^{N-1} S(\rho_B(j)) \qquad (44)$$

where $\rho_B \equiv \sum_{j=0}^{N-1} \rho_B(j)/N$ is the average state of B, assuming that each of Alice's queries is equiprobable. To simplify this expression, it is useful to express $\rho_B(j)$ as

$$\rho_B(j) = P_j\, \sigma_j + (1 - P_j)\, \tilde{\sigma}_j \qquad (45)$$

where P_j is the average probability (18) that Bob will pass the test while Alice is sending the jth query, and where σ_j and $\tilde{\sigma}_j$ are the density matrices

$$\begin{aligned} \sigma_j &\equiv \left(P_j^{(\mathbf{a})}\, \sigma_j^{(\mathbf{a})} + P_j^{(\mathbf{b})} \sigma_j^{(\mathbf{b})}\right) \Big/ (2P_j) \\ \tilde{\sigma}_j &\equiv \left[\left(1 - P_j^{(\mathbf{a})}\right)\, \tilde{\sigma}_j^{(\mathbf{a})} + \left(1 - P_j^{(\mathbf{b})}\right) \tilde{\sigma}_j^{(\mathbf{b})}\right] \Big/ [2(1 - P_j)]. \end{aligned} \qquad (46)$$

This allows us to write also

$$\rho_B = P\, \sigma + (1 - P)\, \tilde{\sigma}, \qquad (47)$$

with

$$\sigma \equiv \sum_{j=0}^{N-1} \frac{P_j}{NP} \sigma_j, \quad \tilde{\sigma} \equiv \sum_{j=0}^{N-1} \frac{1 - P_j}{N(1 - P)} \tilde{\sigma}_j \qquad (48)$$

where $P \equiv \sum_j P_j/N$ is Bob's average probability of passing the honesty test, which, according to (23), must be greater than $1 - \epsilon$. Equations (45) and (47) can then be exploited to produce the following inequalities [18]:

$$\begin{aligned} S(\rho_B) &\le H_2(P) + P\, S(\sigma) + (1 - P)\, S(\tilde{\sigma}) \\ S(\rho_B(j)) &\ge P_j\, S(\sigma_j) + (1 - P_j)\, S(\tilde{\sigma}_j) \end{aligned} \qquad (49)$$

where $H_2(x) \equiv -x \log x - (1 - x)\log(1 - x)$ is the binary entropy. Therefore, (44) gives

$$\begin{aligned} I \le H_2(P) + P\, \chi\left(\left\{\frac{P_j}{NP}; \sigma_j\right\}\right) \\ +(1 - P)\, \chi\left(\left\{\frac{1 - P_j}{N(1 - P)}; \tilde{\sigma}_j\right\}\right) \end{aligned}$$

where $\chi(\{\frac{1-P_j}{N(1-P)}; \tilde{\sigma}_j\})$ is the Holevo information associated with a source characterized by probabilities $\frac{1-P_j}{N(1-P)}$. This quantity can never be bigger than $\log_2 N$ (the same applies to $\chi(\{\frac{P_j}{NP}; \sigma_j\})$, but we are not going to use it). Therefore, we can write

$$I \le H_2(P) + P\, \chi\left(\left\{\frac{P_j}{NP}; \sigma_j\right\}\right) + (1 - P)\log_2 N \qquad (50)$$

which shows that, in the limit in which $P \to 1$, the upper bound is only given by $\chi(\{\frac{P_j}{NP}; \sigma_j\})$. For $P \to 1$ (i.e., $\epsilon \to 0$) this quantity vanishes. In fact, according to (26) we know that for $\epsilon \to 0$ the density matrices σ_j converge to the fixed state $|\Phi_0^{(2)}\rangle_B$; hence, $\chi(\{\frac{P_j}{NP}; \sigma_j\}) \to 0$. More generally, we now show that I can be bounded from above to any value > 0 for P sufficiently close to 1.

In order to exploit the above relations to give a bound on I, let us introduce the probabilities

$$q_j \equiv \left\langle \Phi_0^{(2)} \right| \sigma_j \left| \Phi_0^{(2)} \right\rangle \ge 1 - 150.3\, \epsilon^{1/4} \qquad (51)$$

$$q \equiv \left\langle \Phi_0^{(2)} \right| \sigma \left| \Phi_0^{(2)} \right\rangle = \sum_{j=0}^{N-1} \frac{P_j}{NP}\, q_j \ge 1 - 150.3\, \epsilon^{1/4} \qquad (52)$$

[the inequalities simply follow from (26)]. We can then write

$$\begin{aligned} \sigma_j &= q_j \left|\Phi_0^{(2)}\right\rangle \left\langle \Phi_0^{(2)}\right| + (1 - q_j)\, \tau_j + \Delta_j \\ \sigma &= q \left|\Phi_0^{(2)}\right\rangle \left\langle \Phi_0^{(2)}\right| + (1 - q)\, \tau + \Delta \end{aligned} \qquad (53)$$

where τ_j are density matrices formed by vectors $|v_\perp\rangle$ orthogonal to $|\Phi_0^{(2)}\rangle$, Δ_j are traceless operators containing off-diagonal terms of the form $|\Phi_0^{(2)}\rangle\langle v_\perp|$, and $\tau \equiv \sum_j P_j \tau_j/(NP)$. We now introduce a *unital*, completely positive trace preserving (CPT) map[6] $\mathcal{T}$ which destroys the off-diagonal terms $|\Phi_0^{(2)}\rangle\langle v_\perp|$ while preserving the corresponding diagonal terms, and observe that the von Neumann entropy always increases under the action of a unital map [27]. Therefore

$$\begin{aligned} \chi\left(\left\{\frac{P_j}{NP}; \sigma_j\right\}\right) &\le S(\sigma) \le S(\mathcal{T}(\sigma)) \\ &= S\left(q\left|\Phi_0^{(2)}\right\rangle \left\langle \Phi_0^{(2)}\right| + (1 - q)\, \tau\right) \\ &\le H_2(q) + (1 - q) S(\tau). \end{aligned} \qquad (54)$$

[6] A Unital CPT map by definition preserves the identity operator I, i.e., $\mathcal{T}[I] = I$.

Now, since τ is a density matrix in B, the quantity $S(\tau)$ can always be upper bounded by $\log_2 d_B$ with d_B the dimension of B. This is not very useful, as d_B can be arbitrarily large. However, a better solution can be obtained. Indeed, we can show that the following inequality holds:

$$S(\tau) \leq \log_2(2N). \tag{55}$$

To verify this, we note that the ensemble $\{\frac{P_j}{NP}; \sigma_j\}$ is composed by N density matrices of the form (46) where $\sigma_j^{(\mathbf{a})}$ and $\sigma_j^{(\mathbf{b})}$ are pure vectors satisfying the conditions given in (26) which, for $\epsilon \to 0$ becomes parallel. Since the density matrices $\sigma_j^{(\mathbf{a})}$ and $\sigma_j^{(\mathbf{b})}$ for $j = 1 \ldots N$ are $2N$ pure states, they span at most a $2N$-dimensional subspace of the Hilbert space B. Then there exists a partial isometry $\mathcal{I}$ connecting B to a Hilbert space B' of dimension $2N$ which maintains their relative distances intact. Applying such an isometry to all elements of $\{\frac{P_j}{NP}; \sigma_j\}$ we obtain a new ensemble $\{\frac{P_j}{NP}; \sigma'_j\}$ of B', whose elements satisfy to the same relations as the original one. In particular, the two ensembles possess the same value of χ (in fact, χ is an entropic quantity, whose value depends only on the relations among the ensemble elements), i.e.,

$$\chi\left(\left\{\frac{P_j}{NP}; \sigma_j\right\}\right) = \chi\left(\left\{\frac{P_j}{NP}; \sigma'_j\right\}\right) \tag{56}$$

We can now apply to $\chi(\{\frac{P_j}{NP}; \sigma'_j\})$ the inequalities (54): the only difference being that now τ is a density matrix of B', and, hence, it satisfies the condition (55). Therefore, we can conclude

$$\chi\left(\left\{\frac{P_j}{NP}; \sigma_j\right\}\right) \leq H_2(q) + (1-q)\log_2(2N).$$

Replacing this into (50), we finally find

$$I \leq H_2(P) + P\,H_2(q) + (1-q) + (2-P-q)\log_2 N. \tag{57}$$

which thanks to (52), for sufficiently large N yields (17). This means that Alice can limit Bob's information I, by employing in her tests a value of ϵ sufficiently small.

V. QPQ Variants and Entanglement Assisted QPQ

In this section, we discuss some simple variants of the QPQ protocol that can be used to improve the privacy of Alice. In particular we describe an entanglement assisted QPQ [28] in which Alice entangles her registers $Q_{1,2}$ with a local ancilla before sending them to Bob. As before, we will focus for simplicity on rhetoric versions of such variants, even though similar considerations can be applied also to other (nonrhetoric) QPQ versions.

An example of cheating strategy will allow us to put in evidence the aspects of QPQ that these variants are able to improve. Specifically, suppose that Bob performs a projective measure on all of Alice's queries to determine the value of the index j. As we have seen in the previous section, he will be by necessity disturbing Alice's state in average, so that she will have some nonzero probability to find out he is cheating. However, if she had chosen scenario **a** [see (4)], then Bob's first measurement on Q_1 will return j. Now, suppose that his second measurement on Alice's second request Q_2 returns the value "0" (this happens with probability $1/2$), then Bob will know that Alice had chosen scenario **a** and that her query was j. In this particular case, he will be able to evade detection if he re-prepares the system Q_2 in the state $|+j\rangle_{Q_2}$. (Of course, this does not mean that he will evade detection in general, as this is a situation that is particularly lucky for him, but that has only a small chance of presenting itself). A simple variant of the QPQ protocol can be used to reduce the success probability of this particular cheating strategy and in general to strengthen the security of the whole procedure. It consists in allowing Alice to replace the superposition $|+j\rangle_{Q_k}$ with states of the form $(|j\rangle_{Q_k} + e^{i\theta}|0\rangle_{Q_k})/\sqrt{2}$, the phase θ being a parameter randomly selected by Alice. Since Bob does not know the value of θ, it will be clearly impossible for him to re-prepare the correct reply state after his measurement: as a result his probability of cheating using the simple strategy presented above will be decreased.[7] Furthermore, since for each given choice of θ, the results of Section IV apply, one expects that the use of randomly selected θs will result in a general security enhancement of the QPQ protocol.

In the previous example, the parameter θ is a *secret parameter* whose value, unknown to Bob, prevents him from sending the correct answers to Alice. Another QPQ variant employs entanglement to enhance security. Suppose that, instead of presenting Bob with the states $|j\rangle_{Q_k}$ and $|+j\rangle_{Q_k} = (|j\rangle_{Q_k} + |0\rangle_{Q_k})/\sqrt{2}$, as requested by the QPQ protocol, Alice uses the states

$$|j\rangle_{Q_k} \quad \text{and} \quad |\wedge j\rangle_{Q_k A} \equiv \frac{1}{\sqrt{2}}[|j\rangle_{Q_k}|0\rangle_A + |0\rangle_{Q_k}|j\rangle_A] \tag{58}$$

where the system A is an ancillary system that Alice does not hand over to Bob. The protocol now follows the same procedure as the "canonical" QPQ described previously, but employing the state $|\wedge j\rangle$ in place of the state $|+j\rangle$. Of course, Alice's honesty test must be appropriately modified, as she has to test whether Bob's actions have destroyed the entanglement between the ancillary system A and the Q_k register. The main difference with the canonical QPQ is that here half of the times Bob has only access to a part of an entangled state: he is even more limited in re-preparing the states for Alice than in the canonical QPQ. It is easy to see that the security proof given in the previous sections can be straightforwardly extended to this version of the protocol, and that the security bounds derived above still apply: indeed they can be made even more stringent as Bob has only a limited capacity in his transformations on Alice's queries, since he does not have access to the ancillary space A. In the situations in which the information carriers employed in the queries can be put in a superposition of traveling in different directions [28], this version of the protocol can easily be reduced to the canonical QPQ by simply supposing that Alice is in the possession of the database element $j = 0$ corresponding to the rhetoric question, while, obviously, Bob is in possession of all the remaining database elements.

[7] Analogous improvements are obtained by allowing Alice to replace the states $|+j\rangle$ with superposition of the form $\alpha|j\rangle + \beta|0\rangle$ with randomly selected complex amplitudes α and β.

VI. What If Alice Cannot Check the Answer to Her Queries Independently From Bob?

In deriving the security thresholds of the QPQ protocol we have assumed the database to be deterministic, i.e., that for each query $j \in \{1, 2, \ldots, N\}$ there is a *unique* possible answer A_j (notice, however, that two distinct queries can have the same answer—i.e., A_j can coincides with $A_{j'}$). Such hypothesis explicitly enters our derivation at the very beginning of the proof: namely in the writing of the rhs of (6) where the *correct answer* component $|C_j; \Phi_j^{(1)}\rangle_{Q_1RB}$ is assumed to be separable with respect to the bipartition Q_1R_1/R_2B. As mentioned in the introductory sections, one way to enforce the deterministic-database condition in a realistic scenario is to require that Alice can independently validate the value A_j of Bob's answer after its reception (either by direct computation or by contacting an external referee). In this section we will show that if this is not the case, then the simple version of QPQ we have analyzed here does not prevent Bob to cheat without being discovered by Alice. In fact, in this case Bob is no longer forced to commit to a specific answer during the whole querying procedure, meaning that the Q_1R_1/R_2B separability of the component $|C_j; \Phi_j^{(1)}\rangle_{Q_1RB}$ is no longer guaranteed. On the contrary, he can exploit the existence of multiple queries to create quantum superposition of "correct" answers that allow him to pass Alice's honesty test with probability one while gathering some extra information on her query. In Section VI-B, we will discuss some methods one can apply to overcome these limitations by increasing the complexity of the protocol, e.g., allowing Alice (or third parties that collaborate with her) to reiterate her query at random times.

A. Successful Cheating Strategies for a Database With Multiple Valid Answers

Here, we drop the deterministic hypothesis on the database and give two examples of successful cheating strategies that allow Bob to spy on Alice's query, and pass the honesty test with probability 1.

Example 1: Let us start by considering the case of a nondeterministic database with $N = 3$ possible entries in which both the query $j = 1$ and the query $j = 2$ admit two distinguishable answers. In particular let $A_1^{(+)}$, $A_1^{(-)}$ be the answers for $j = 1$ and $A_2^{(+)}$, $A_2^{(-)}$ those for $j = 2$.

Now, suppose that the unitary $U^{(1)}_{Q_1RB}$ of (5) that Bob applies to Q_1RB performs the following mapping:

$$
\begin{aligned}
&|0\rangle_{Q_1}|0\rangle_{R_1}|0\rangle_B\\
&\quad\to |0\rangle_{Q_1}|A_0\rangle_{R_1}|0\rangle_B\\
&|1\rangle_{Q_1}|0\rangle_{R_1}|0\rangle_B\\
&\quad\to |1\rangle_{Q_1}\frac{\left|A_1^{(+)}\right\rangle_{R_1}|+1\rangle_B+\left|A_1^{(-)}\right\rangle_{R_1}|-1\rangle_B}{\sqrt{2}}\\
&|2\rangle_{Q_1}|0\rangle_{R_1}|0\rangle_B\\
&\quad\to |2\rangle_{Q_1}\frac{\left|A_2^{(+)}\right\rangle_{R_1}|+2\rangle_B+\left|A_2^{(-)}\right\rangle_{R_1}|-2\rangle_B}{\sqrt{2}}
\end{aligned}
$$

where $|A_0\rangle$ is the answer to the rhetoric query and where

$$|\pm 1\rangle_B \equiv \frac{|0\rangle_B \pm |1\rangle_B}{\sqrt{2}}, \quad |\pm 2\rangle_B \equiv \frac{|0\rangle_B \pm |2\rangle_B}{\sqrt{2}} \tag{59}$$

with $|0\rangle_B, |1\rangle_B$ and $|2\rangle_B$ being orthonormal states of Bob's space B. By a comparison with (6) it immediately follows that in this case when $j = 1, 2$ the vectors $|C_j; \Phi_j^{(1)}\rangle_{Q_1RB}$ are no longer separable with respect to the bipartition Q_1R_1/R_2B. Analogously define $U^{(2)}_{Q_2R_2B}$ as the unitary operator which performs the following transformation: $|0\rangle_{Q_2}|0\rangle_{R_2}|\psi\rangle_B \;\to\; |0\rangle_{Q_2}|A_0\rangle_{R_2}|\psi\rangle_B$ for all $|\psi\rangle_B$ of B and

$$
\begin{aligned}
|1\rangle_{Q_2}|0\rangle_{R_2}|\pm 1\rangle_B &\to |1\rangle_{Q_2}\left|A_1^{(\pm)}\right\rangle_{R_2}|\pm 1\rangle_B\\
|2\rangle_{Q_2}|0\rangle_{R_2}|\pm 2\rangle_B &\to |2\rangle_{Q_2}\left|A_2^{(\pm)}\right\rangle_{R_2}|\pm 3\rangle_B.
\end{aligned} \tag{60}
$$

According to the above assumptions, if Alice's query is the rhetoric one (i.e., $j = 0$) the final state (5) of the QPQ protocol is $|0\rangle_{Q_2}|A_0\rangle_{R_2}|0\rangle_{Q_1}|A_0\rangle_{R_1}|0\rangle_B$. In this case Bob passes the test and gets $|0\rangle_B$ as output state. For $j = 2, 3$, instead, we have two possibilities. In the scenario $\ell = \mathbf{a}$ the final state will be

$$
\begin{aligned}
&|j\rangle_{Q_1}\left|A_j^{(+)}\right\rangle_{R_1}\frac{|j\rangle_{Q_2}\left|A_j^{(+)}\right\rangle_{R_2}+|0\rangle_{Q_2}|A_0\rangle_{R_2}}{2}|+j\rangle_B\\
&\quad+|j\rangle_{Q_1}\left|A_j^{(-)}\right\rangle_{R_1}\frac{|j\rangle_{Q_2}\left|A_j^{(-)}\right\rangle_{R_2}+|0\rangle_{Q_2}|A_0\rangle_{R_2}}{2}|-j\rangle_B
\end{aligned}
$$

while in the scenario $\ell = \mathbf{b}$ it will be

$$
\begin{aligned}
&\frac{|j\rangle_{Q_1}\left|A_j^{(+)}\right\rangle_{R_1}+|0\rangle_{Q_1}|A_0\rangle_{R_1}}{2}|j\rangle_{Q_2}\left|A_j^{(+)}\right\rangle_{R_2}|+j\rangle_B\\
&\quad+\frac{|j\rangle_{Q_1}|A_j^{(-)}\rangle_{R_1}+|0\rangle_{Q_1}|A_0\rangle_{R_1}}{2}|j\rangle_{Q_2}|A_j^{(-)}\rangle_{R_2}|-j\rangle_B.
\end{aligned}
$$

This means that independently from the selected value of ℓ Alice will receive the answer $A_j^{(+)}$ half of the times and the answer $A_j^{(-)}$ in the other half of the times, while Bob will always pass the honesty test. Moreover in the case in which Alice receives the answer $A_j^{(+)}$, Bob will get the state $|+j\rangle_B$ while in the case in which Alice receives the answer $A_j^{(-)}$ Bob will get the state $|-j\rangle_B$. In average the state B is $(|0\rangle_B\langle 0| + |j\rangle_B\langle j|_B)/2$.

In conclusion, using $U^{(1)}$ and $U^{(2)}$ as in the previous paragraphs, Bob will always pass the honesty test. Furthermore, the output state of B he gets at the end of the protocol will be partially correlated with the query j as follows:

$$
\begin{array}{c|c}
\text{Query} & \text{output state } B\\
\hline
j=0 & |0\rangle_B\langle 0|\\
j=1 & (|0\rangle_B\langle 0|+|1\rangle_B\langle 1|)/2\\
j=2 & (|0\rangle_B\langle 0|+|2\rangle_B\langle 2|)/2
\end{array}. \tag{61}
$$

Therefore, by performing a simple von Neumann measurement on B, Bob will be able to extract some information on j, without Alice having any chance of detecting it.

Notice that, in the example presented here, Bob's info is limited by the partial overlap between the states $|0\rangle_B\langle 0|$, $(|0\rangle_B\langle 0| + |1\rangle_B\langle 1|)/2$ and $(|0\rangle_B\langle 0| + |2\rangle_B\langle 2|)/2$. However, this is not a fundamental limitation as one can construct more complex examples (e.g., databases with more than two possible answers for a single query) for which the amount of info that Bob acquires on j can be arbitrarily high. It is also important to stress that the above example can be used also to show that Bob will be able to cheat also in the case in which Alice adopts QPQ strategies more sophisticated then the simple rhetoric version discussed in this paper (e.g., instead of sending superpositions of the form $(|j\rangle + |0\rangle)/\sqrt{2}$ she sends arbitrary superpositions $\alpha|j\rangle + \beta|0\rangle$ with α and β arbitrary amplitudes that only she knows).

Example 2: Here we analyze how multiple valid answers may affect the performance of a nonrhetoric version of the QPQ protocol (i.e., where Alice is not using the rhetoric question $j = 0$). Again we give an example of a successful cheating strategy for a database with $N = 3$ queries. For the sake of simplicity, we will assume that $j = 0, 1$ have single answers A_0 and A_1 respectively, but that $j = 2$ is associated with two distinguishable answers $A_2^{(\pm)}$. As an example of a nonrhetoric QPQ protocol we consider the case in which Alice, to get the information associated with the j query, chooses another query (say the j'th one) and sends sequentially, in random order, states of the form $\alpha|j\rangle + \beta|j'\rangle$, $|j\rangle$ and $|j'\rangle$ (α and β being amplitudes that only she knows).

As in the case of the rhetoric version of the protocol, Bob's action can be described by unitaries. In this case, they are $U^{(1)}$, $U^{(2)}$ and $U^{(3)}$. Notice that the first acts on Q_1RB the second on $Q_2R_2R_3B$ and the third on Q_3R_3B, with obvious choice of the notation for the subspaces involved. For our present purpose, it is sufficient to assume that for $k = 1, 2, 3$, $U^{(k)}$ acts nontrivially only on Q_kR_kB (this is a particular instance of the general case). We can also assume that $U^{(1)}$,$U^{(2)}$ and $U^{(3)}$ are identical. We then define such operators according to the following rules:

$$U^{(k)}_{Q_kR_kB}(|j\rangle_{Q_k}|0\rangle_{R_k}|0\rangle_B) = |j\rangle_{Q_k}|A_j\rangle_{R_k}|0\rangle_B$$
$$U^{(k)}_{Q_kR_kB}(|j\rangle_{Q_k}|0\rangle_{R_k}|2\rangle_B) = |j\rangle_{Q_k}|A_j\rangle_{R_k}|2\rangle_B$$

if $j = 0, 1$ while, for $j = 2$

$$\begin{aligned} &U^{(k)}_{Q_kR_kB}(|2\rangle_{Q_k}|0\rangle_{R_k}|0\rangle_B) \\ &\quad = |2\rangle_{Q_k}\left(\left|A_2^{(+)}\right\rangle_{R_k}|+2\rangle_B + \left|A_2^{(-)}\right\rangle_{R_k}|-2\rangle_B\right)\Big/\sqrt{2} \\ &\qquad U^{(k)}_{Q_kR_kB}\left(|2\rangle_{Q_k}|0\rangle_{R_k}|2\rangle_B\right) = |2\rangle_{Q_k}\left|A_2^{(\pm)}\right\rangle_{R_k}|2\rangle_B \end{aligned}$$

where $|\pm 2\rangle_B$ are defined in (59). If initial state of the B is $|0\rangle_B$, one can easily verify that Bob will always pass Alice's honesty test (no matter which superposition $\alpha|j\rangle + \beta|j'\rangle$ she is using) and that he can recover part of the information associated with the query. In this simple example, for instance, he has a not null probability to identify the query $j = 2$. As before, this counterexample can be easily generalized and improved.

B. Possible Solutions for Nondeterministic Databases

The case of nondeterministic databases in which different answers may correspond to the same query is, of course, quite relevant, so that it is natural to ask if the QPQ protocol can be modified to apply also to this situation. At present, we do not have a formal security proof for a QPQ strategy that works if one drops the deterministic-database assumption. However, we suspect that this is only due to the complexity of the problem which makes the analysis technically cumbersome. Indeed we believe that secure QPQ strategies for nondeterministic database exist and conjecture that the uniqueness assumption for the A_j could be dropped without affecting the security. In support to the above conjecture, in this section we present some ideas that allow Alice to foil the cheating strategies described in the previous section temporarily, for as long as Bob is expecting further queries.

In the case in which Alice can independently check how many different replies correspond to the each query (and which they are), then there is a simple solution that prevents Bob from cheating: we must require Bob to provide all possible replies in a pre-established order (e.g., alphabetically) when he is presented the jth query. In this way, each query has again a unique *composite* answer (composed by the ordered succession of all the possible answers), so that we are reduced to the canonical QPQ protocol, and Bob is prevented from cheating.

If, however, Alice cannot independently establish the total number of different replies to each query, then a different strategy is necessary. First of all, we must require that each of the possible replies to the jth query is uniquely indexed by Bob. This means that there should be a unique answer to the question "What is the kth possible reply to the jth query?" Of course, this by itself is insufficient to guarantee that Bob cannot employ the cheating strategies of the previous section, as Alice cannot independently check the uniqueness of Bob's indexing. However, she can check whether Bob will always answer in the same way to repeated queries. From (60) and (61), it follows that, as soon as Bob measures his system B, he might gain information on the value of j, but at the same time he loses information on which one (among all the possible answers to the jth query) he had presented to Alice. If he wants to be sure that he keeps on providing always the same answer to repeated queries on Alice's part, he must preserve his system B (in order to prepare subsequent replies) without trying to extract information from it. He can measure the system B only when he is confident that Alice will not be asking him the same query anymore. In a multiparty scenario, we can also think of a situation where multiple cooperating parties ask Bob the same queries and compare the replies they receive from him. If they find that his answers when he is asked the kth reply to the jth query to do not match, then they can conclude that he has been cheating: he has not assigned a unique index to all the possible replies to the jth query, and he has taken advantage of the cheating strategies detailed in the previous section.

Note that it might seem that Bob can cheat undetected when he replies to the *first* query, since at that point the ordering has still not been established. (He cannot cheat in any of the successive queries since it could be a repeat of the first, and he cannot risk changing the order). However, the cheating strategy detailed in the previous section is probabilistic: if he is unlucky, he will not be able neither to determine which was Alice query, nor which among the possible answers was the one he provided her. In this case, he will risk getting caught if that query is repeated: he cannot provide the same answer again. Hence, if he does not want to risk getting caught, even at the first query he cannot use the cheating strategy of the previous section.

In conclusion, by requiring that Bob should answer in the same way to repeated queries, we can drop the requirement that Alice has to be able to independently check each answer. (Clearly, since Bob's cheats are only probabilistically revealed, she should not repeat her queries too often). Bob is thus placed in the awkward situation that he may be possessing information on Alice's query in the system B entirely in his possession, but he is prevented from accessing such information. This is a temporary solution, since, as soon as Bob is certain that he will not be asked the jth query anymore, he can measure the system B and extract the information stored on it. He is kept honest only as long as he is in business (and, of course, he is in business only as long as he is honest).

VII. Conclusion

In conclusion, we have given a security proof of the QPQ protocol introduced in [14]. In particular we focused on the simplest variant of such scheme, i.e., a rhetoric version of QPQ with a single rhetoric answer where to each query j there corresponds a unique, testable reply A_j (deterministic database assumption). The proof is based on quantitative information-disturbance tradeoffs which place an upper bound on the information Bob can retain on Alice's query in terms of the disturbance he is producing on the states that he is handing back to her (see Sections III and IV). A nonzero information retained by Bob implies a nonzero disturbance on Alice's states, which she can detect with a simple measurement (the "honesty test"). If the honesty test fails, she can conclude that Bob has certainly cheated. If, on the other hand, the test passes, she can tentatively conclude that Bob has not cheated (although she cannot be certain of it).

In addition, we have discussed some variants of the basic scheme which yields an increase Alice's security by reducing Bob's probability of evading detection when cheating. These variants either exploit secret parameters, or exploit entanglement with an ancillary system Alice retains in her possession (see Section V).

Finally, we have seen that Bob can successfully cheat without being detected if we drop the assumption that to each query there can be associated only a single answer A_j (see Section VI-A). In fact, if we assume that there exist two (or more) different replies $A_j \neq A'_j$ to the query j, then Bob can find out the value of j, evading detection by Alice with certainty. We discussed some strategies that allow Alice to protect herself also in this situation, at least as long as Bob can expect further queries from her or from other parties who may cooperate with her (see Section VI-B).

Acknowledgment

The authors would like to thank E. Kushilevitz, S. Micali, F. Sciarrino, and M. Sudan for discussions. S. Lloyd would like to thank S. Brin and L. Page for fruitful discussions.

References

[1] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, *J. Comput. Syst. Sci.*, vol. 60, p. 592, 2000.
[2] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," *J. ACM*, vol. 45, pp. 965–981, 1998.
[3] C. Cachin, S. Micali, and M. Stadler, *Advances in Cryptology-EUROCRYPT* 1999.
[4] C. Gentry and Z. Ramzan, in *Proc. 32nd ICALP*, 2005, pp. 803–815.
[5] S. Yekhanin, Tech. Rep. ECCC TR06-127, 2006.
[6] S. Yekhanin, *J. ACM*, vol. 55, p. 1, 2007.
[7] E. Kushilevitz and R. Ostrovsky, in *Proc. 38th IEEE Symp.*, 1997, p. 364.
[8] S. Wiesner, in *ACM SIGACT News*, Winter/Spring 1983, vol. 15, no. 1, pp. 78–88.
[9] M. O. Rabin, "How to Exchange Secrets With Oblivious Transfer," Tech. Rep. TR-81, 1981, Harvard Aiken Computational Lab..
[10] A. Jakoby, M. Liskiewicz, and A. Madry, arXiv: quant-ph/0605150v1 2006.
[11] A. Ambainis, in *Proc. 24ht ICALP, Lecture Notes in Computer Science*, 1997, vol. 1256, p. 401.
[12] I. Kerenidis and R. de Wolf, *J. Comput. Syst. Sci.*, vol. 69, p. 395, 2004.
[13] I. Kerenidis and R. de Wolf, *Inf. Process. Lett.*, vol. 90, p. 109, 2004.
[14] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum private queries," *Phys. Rev. Lett.*, vol. 100, no. 23, 2008, art. 230502.
[15] S. Lloyd, "Privacy and the quantum internet," *Sci. Amer.*, vol. 301, pp. 60–63, 2009.
[16] L. Hardy and A. Kent, "Cheat sensitive quantum bit commitment," *Phys. Rev. Lett.*, vol. 92, no. 95, 2004, art.157901.
[17] P. Arrighi and L. Salvail, "Blind quantum computation," *Int. J. Quant. Inf.*, vol. 4, no. 5, pp. 883–898, 2006.
[18] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.
[19] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum random access memory," *Phys. Rev. Lett.*, vol. 100, no. 16, 2008, art. 16050.
[20] V. Giovannetti, S. Lloyd, and L. Maccone, "Architectures for a quantum random access memory," *Phys. Rev. A*, vol. 78, no. 5, 2008, art. 052310.
[21] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*. Amsterdam, The Netherlands: North Holland, 1982.
[22] A. Peres, *Quantum Theory: Concepts and Methods*. Berlin, Germany: Springer, 1995.
[23] D. Bures, *Trans. Amer. Math. Soc.*, vol. 135, p. 199, 1969.
[24] A. Uhlmann, *Rep. Math. Phys.*, vol. 9, p. 273, 1979.
[25] T. Cover and J. Thomas, *Elements of Information Theory*. Hoboken, NJ: Wiley, 1991.
[26] V. Giovannetti and A. S. Holevo, "Quantum shared broadcasting," *Quant. Inf. Process.*, vol. 7, pp. 55–69, 2008.
[27] R. F. Streater, *Statistical Dynamics*. Singapore: Imperial College Press, 1995.
[28] F. De Martini, V. Giovannetti, S. Lloyd, L. Maccone, E. Nagali, L. Sansoni, and F. Sciarrino, "Experimental quantum private queries with linear optics," *Phys. Rev. A*, vol. 80, no. 1, 2009, art. 010302(R).

Vittorio Giovannetti, photograph and biography not available at the time of publication.

Seth Lloyd, photograph and biography not available at the time of publication.

Lorenzo Maccone, photograph and biography not available at the time of publication.