J Cryptol (2015) 28:161–175
DOI: 10.1007/s00145-014-9180-2

Journal of
CRYPTOLOGY

# Quantum Private Information Retrieval has Linear Communication Complexity

Ämin Baumeler
Faculty of Informatics, Università della Svizzera italiana, Lugano, Switzerland
amin.baumeler@usi.ch

Anne Broadbent
Department of Mathematics and Statistics, University of Ottawa, Ottawa, ON, Canada
abroadbe@uottawa.ca

Communicated by Stefan Wolf

Received 15 May 2013
Online publication 17 April 2014

**Abstract.** In private information retrieval (PIR), a client queries an $n$-bit database in order to retrieve an entry of her choice, while maintaining privacy of her query value. Chor et al. [J ACM 45(6):965–981, 1998] showed that, in the information-theoretical setting, a linear amount of communication is required for classical PIR protocols (thus the trivial protocol is optimal). This linear lower bound was shown by Nayak [FOCS 1999, pp. 369–376, 1999] to hold also in the quantum setting. Here, we extend Nayak's result by considering approximate privacy, and requiring security only against *specious* adversaries, which are, in analogy to classical honest-but-curious adversaries, the weakest reasonable quantum adversaries. We show that, even in this weakened scenario, quantum private information retrieval (QPIR) requires $n$ qubits of communication. From this follows that Le Gall's recent QPIR protocol with sublinear communication complexity [Theory Comput. 8(1):369–374, 2012] is not information-theoretically private, against the weakest reasonable cryptographic adversary.

**Keywords.** Private information retrieval, Quantum cryptography, Specious adversaries, Quantum semi-honest.

## 1. Introduction

The cryptographic scheme of private information retrieval (PIR) describes the problem of querying a database without suffering a loss in privacy. It was formally defined in 1998 by Chor et al. [4]. Intuitively, not losing privacy through a query means that the database server does not learn anything about the client's input. An interesting question is as follows: how much communication does a PIR protocol require? Sending the whole database to the client is a trivial PIR protocol, but it seems unsatisfactory with respect to the amount of communication. Are there better solutions? In the setting of one database

server and information-theoretic privacy, the trivial protocol is optimal (even against honest-but-curious adversaries). This result was shown by Chor et al. [4].

Quantum computation and quantum communication, compared to the classical model, allow for improved solutions to cryptographic tasks [2,17]. A natural question thus arises: *does quantum information allow PIR protocols with sublinear communication complexity?* We call a PIR protocol where we make use of quantum resources a quantum private information retrieval (QPIR) protocol. Nayak answered this question in the negative [16], with a proof sketch establishing a reduction to *random access encoding*.[1] There are also other fields where allowing quantum computation and communication failed to qualitatively improve the classical result. An example is bit commitment: as we know, perfect bit commitment is not possible in the classical setting; in the quantum setting it is also not possible [14,15] (but see Chailloux and Kerenidis [3] for some quantum improvements that *are* possible).

Recently, Le Gall [13] presented a QPIR protocol with a sublinear amount of communication. This result holds for a database that exactly follows the protocol specification. Motivated by this seemingly contradictory result, we study here the communication complexity of QPIR protocols that are secure against *specious* adversaries. As defined by Dupuis et al. [5], specious adversaries may deviate from the protocol, but only in a way that is essentially indistinguishable from the honest behavior—they are a quantum analog of classical honest-but-curious adversaries, thus corresponding to the weakest reasonable cryptographic adversaries.

*a. Main Result* We show that, even in the case of approximate privacy and approximate correctness, QPIR against specious adversaries has linear communication complexity.[2] This establishes that the adversarial model in Le Gall's analysis does not fulfill the weakest reasonable security definition and closes the topic of single-server, information-theoretic QPIR.

*b. Related Work* Nayak's lower bound was generalized by Jain et al. [8], who showed a trade-off for the loss in privacy between the client and database. QPIR has also been studied in the scenario of multiple servers [10,11], in the scenario of symmetric privacy [11], as well as in the scenario where a cheating server is detected [6]. Recently, a practical symmetric QPIR protocol which is not unconditionally secure was developed [9].

### 1.1. *Specious Adversaries*

We call a party which follows a protocol *honest*. A *correct* protocol is a protocol that achieves its task, given that all the parties are honest. Clearly, every meaningful protocol has to be correct. If we now try to restrict the actions of an adversary as much as possible, we cannot violate the correctness requirement. This means, the weakest adversary has to *appear* honest.

[1] It has been claimed [13] that Nayak proved a lower bound for two-message quantum protocols only, when in fact, his claim encompasses protocols with arbitrary interaction. We attribute this misunderstanding to the succinctness of Nayak's original write-up (the result and proof are only a few sentences long).

[2] This result has appeared as part of the M.Sc. thesis of one of the authors [1].

In classical cryptography, there exists a notion of *honest-but-curious* adversaries, which models the above description. Such adversaries follow the protocol (honesty), but record everything they see and try to extract a secret (curiosity). A classical honest-but-curious adversary can do nothing more to break the privacy property of a protocol.

Dupuis et al. [5] followed this spirit and introduced the quantum analog to the honest-but-curious adversaries, and called them *specious*. The honesty property, as well as the curiosity property cannot be translated one-to-one from the classical to the quantum case. To get a meaningful model, the definition needs to capture the essence of being the weakest adversary, as described above.

Attempting a translation from the classical to the quantum case, we see that a quantum adversary can also follow the protocol to be honest. Curiosity means to copy everything the adversary sees and extracting a secret from it. In general, copying is not possible because of the no-cloning theorem [18]. Therefore, a protocol can force a quantum honest-but-curious adversary to forget. This motivates the need for a security guarantee not only at the end of the protocol, but also *during* the interaction.

Quantum adversaries, on the other hand, can act in a way indistinguishable from an honest party. As an example, in some protocols, it may be possible to delay measurements. This means, the adversary skips a measurement instruction and continues in superposition. At a later point in the protocol, if required, the adversary can perform the measurement, making it look like it was honest all the time. In other words, at any step during the execution of the protocol, we specify that the adversary should be able to provide some state that, when joined with the state held by the honest party, is indistinguishable from the joint state of an honest interaction. This is the essence of the definition of specious adversaries, which we define formally in Sect. 2.3.

While the concept of specious adversaries is not yet in widespread use in the quantum cryptographic community, *purification* attacks and the related *purified adversaries* have long been known to present subtle challenges unique to the quantum world. Bennett and Brassard [2] were among the first to draw attention to this type of attack, proposing a quantum bit commitment scheme, together with an explicit purification attack. Purified adversaries (who can be seen as delaying their input choices by sending entangled states) are easily seen to be a special case of specious adversaries.

### 1.2. *Le Gall's QPIR Protocol*

Recently, Le Gall [13] presented a QPIR protocol with information-theoretic privacy. His protocol achieves a communication complexity of $\mathcal{O}\left(\sqrt{n}\right)$, where $n$ is the database size in bits. At first glance, this result seems to beat Nayak's lower bound of $n$. However, the price for this lower communication complexity is that the server must follow the protocol precisely. Hence, Le Gall considers a different model of adversaries. One naturally wonders if such gains can be achieved by specious adversaries. Our main result (Theorem 4) rules out this possibility.

## 2. Formal Model and Security Definitions

In this section, we formally define our model and notions of correctness and privacy. First, we give some basic notation.

### 2.1. *Notation*

We use calligraphic symbols to describe Hilbert spaces. Subscripts of quantum states and quantum operations usually denote the associated Hilbert spaces. Let $\mathcal{A}$ and $\mathcal{B}$ be two Hilbert spaces. By $\mathcal{A} \otimes \mathcal{B}$, we denote the joint Hilbert space. The set $L(\mathcal{A}, \mathcal{B})$ is the set of all linear maps from $\mathcal{A}$ to $\mathcal{B}$. The set $L(\mathcal{A}) = L(\mathcal{A}, \mathcal{A})$ is the set of all linear maps on $\mathcal{A}$. A quantum state is either expressed as a ket $|x\rangle$ or as a density operator $\rho$. Every state that can be written as $|x\rangle$ is pure, with corresponding density operator $|x\rangle\langle x|$. The set $S(\mathcal{A})$ is the set of all density operators on $\mathcal{A}$. The identity operator on the space $\mathcal{A}$ is $\mathbb{1}_{\mathcal{A}} \in L(\mathcal{A})$, for a joint space $\mathcal{A} \otimes \mathcal{B}$ we use $\mathbb{1}_{\mathcal{A},\mathcal{B}}$. An operator $\mathsf{U} \in L(\mathcal{A})$ is called unitary, if $\mathsf{U}^\dagger \mathsf{U} = \mathbb{1}$. In the expression $\mathcal{A} \approx \mathcal{B}$, the symbol $\approx$ denotes that the dimension of $\mathcal{A}$ equals the dimension of $\mathcal{B}$ (i.e., $\dim(\mathcal{A}) = \dim(\mathcal{B})$). The measurement outcome of a measurement $\mathcal{M}$ of a density operator $\rho$ is expressed by $\mathcal{M}(\rho)$.

Let $\rho, \sigma \in S(\mathcal{A})$ be two density operators. We denote by $\|\rho\|_1 = \operatorname{tr}|\rho|$ the *trace norm* of the density operator $\rho$. The *trace distance* between the two density operators $\rho$ and $\sigma$ is defined as

$$\Delta(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_1 . \tag{1}$$

If $\rho = |x\rangle\langle x|$ and $\sigma = |y\rangle\langle y|$ are pure, then we use the compact notation $\Delta(|x\rangle, |y\rangle)$ interchangeably with $\Delta(|x\rangle\langle x|, |y\rangle\langle y|)$.

### 2.2. *Protocol Definition*

As mentioned in Sect. 1.1, when defining security against specious adversaries, we must examine the system held by the adversary *during* the protocol. To this end, we first formally define a two-party quantum *protocol*. We base our definition on the strategy formalism of Gutoski and Watrous [7], as well as on a definition from Dupuis et al. [5] (our scenario is simpler, since our protocols do not make any explicit oracle calls). Without loss of generality, we assume that party $\mathscr{A}$ sends the first and last messages.

**Definition 1** (Two-party quantum protocol). An *s-round, two-party protocol* denoted $\Pi = (\mathscr{A}, \mathscr{B}, s)$ consists of:

1. input spaces $\mathcal{A}_0$ and $\mathcal{B}_0$ for parties $\mathscr{A}$ and $\mathscr{B}$, respectively,
2. memory spaces $\mathcal{A}_1, \ldots, \mathcal{A}_s$ for $\mathscr{A}$ and $\mathcal{B}_1, \ldots, \mathcal{B}_s$ for $\mathscr{B}$ and communication spaces $\mathcal{X}_1, \ldots, \mathcal{X}_s, \mathcal{Y}_1, \ldots, \mathcal{Y}_{s-1}$,
3. an $s$-tuple of quantum operations $(\mathscr{A}_1, \ldots, \mathscr{A}_s)$ for $\mathscr{A}$, where $\mathscr{A}_1 : L(\mathcal{A}_0) \mapsto L(\mathcal{A}_1 \otimes \mathcal{X}_1)$, and $\mathscr{A}_i : L(\mathcal{A}_{i-1} \otimes \mathcal{Y}_{i-1}) \mapsto L(\mathcal{A}_i \otimes \mathcal{X}_i)$, $(2 \leq i \leq s)$,
4. an $s$-tuple of quantum operations $(\mathscr{B}_1, \ldots, \mathscr{B}_s)$ for $\mathscr{B}$, where $\mathscr{B}_i : L(\mathcal{B}_{i-1} \otimes \mathcal{X}_i) \mapsto L(\mathcal{B}_i \otimes \mathcal{Y}_i)$, $(1 \leq i \leq s-1)$, and $\mathscr{B}_s : L(\mathcal{B}_{s-1} \otimes \mathcal{X}_s) \mapsto L(\mathcal{B}_s)$.

If $\Pi = (\mathscr{A}, \mathscr{B}, s)$ is an $s$-round two-party protocol, we define the state after the $i$-th step $(1 \leq i \leq 2s)$, and upon input state $\rho_{\text{in}} \in S(\mathcal{A}_0 \otimes \mathcal{B}_0 \otimes \mathcal{R})$, where $\mathcal{R}$ is a system of dimension $\dim(\mathcal{R}) = \dim(\mathcal{A}_0)\dim(\mathcal{B}_0)$ as

$$\rho_i\left(\rho_{\text{in}}\right) := \left(\mathscr{A}_{(i+1)/2} \otimes \mathbb{1}_{\mathcal{B}_{(i-1)/2},\mathcal{R}}\right) \ldots \left(\mathscr{B}_1 \otimes \mathbb{1}_{\mathcal{A}_1,\mathcal{R}}\right)\left(\mathscr{A}_1 \otimes \mathbb{1}_{\mathcal{B}_0,\mathcal{R}}\right)\left(\rho_{\text{in}}\right), \quad (2)$$

for $i$ odd, and

$$\rho_i\left(\rho_{\text{in}}\right) := \left(\mathscr{B}_{i/2} \otimes \mathbb{1}_{\mathcal{A}_{i/2},\mathcal{R}}\right) \ldots \left(\mathscr{B}_1 \otimes \mathbb{1}_{\mathcal{A}_1,\mathcal{R}}\right)\left(\mathscr{A}_1 \otimes \mathbb{1}_{\mathcal{B}_0,\mathcal{R}}\right)\left(\rho_{\text{in}}\right), \quad (3)$$

for $i$ even. Note that the last round (round $s$) is only partial, since $\mathscr{B}_s : L(\mathcal{B}_{s-1} \otimes \mathcal{X}_s) \mapsto L(\mathcal{B}_s)$. We define the final state of protocol $\Pi = (\mathscr{A}, \mathscr{B}, s)$, upon input state $\rho_{\text{in}} \in S(\mathcal{A}_0 \otimes \mathcal{B}_0 \otimes \mathcal{R})$ as:

$$[\mathscr{A} \circledast \mathscr{B}]\left(\rho_{\text{in}}\right) := \rho_{2s}\left(\rho_{\text{in}}\right). \quad (4)$$

The *communication complexity* of $\Pi = (\mathscr{A}, \mathscr{B}, s)$ is the total amount of quantum communication in the protocol (counted in terms of qubits), as given by $\sum_{i=1}^{s} \log(\dim(\mathcal{X}_i)) + \sum_{i=1}^{s-1} \log(\dim(\mathcal{Y}_i))$.

Given a protocol $\Pi = (\mathscr{A}, \mathscr{B}, s)$, an *adversary* $\tilde{\mathscr{A}}$ *for* $\mathscr{A}$ is an $s$-tuple of quantum operations $(\tilde{\mathscr{A}_1}, \ldots, \tilde{\mathscr{A}_s})$, where $\tilde{\mathscr{A}_1} : L(\mathcal{A}_0) \mapsto L(\tilde{\mathcal{A}}_1 \otimes \mathcal{X}_1)$ and $\tilde{\mathscr{A}_i} : L(\tilde{\mathcal{A}}_{i-1} \otimes \mathcal{Y}_{i-1}) \mapsto L(\tilde{\mathcal{A}}_i \otimes \mathcal{X}_i)$, $(2 \leq i \leq s)$, with $\tilde{\mathcal{A}}_1, \ldots, \tilde{\mathcal{A}}_s$ being $\tilde{\mathscr{A}}$'s memory spaces. We denote the final state of a protocol run with an adversary $\tilde{\mathscr{A}}$ by $[\tilde{\mathscr{A}} \circledast \mathscr{B}]\left(\rho_{\text{in}}\right)$. The state after the $i$-th step of a protocol run with an adversary $\tilde{\mathscr{A}}$ is $\tilde{\rho}_i(\tilde{\mathscr{A}}, \rho_{\text{in}})$.

A special type of adversary for a protocol $\Pi = (\mathscr{A}, \mathscr{B}, s)$ is a *purified adversary*, $\bar{\mathscr{A}}$ *for* $\mathscr{A}$ that is described by *unitaries* $(\bar{\mathscr{A}_1}, \ldots, \bar{\mathscr{A}_s})$, where $\bar{\mathscr{A}_1} : L(\mathcal{A}_0 \otimes \bar{\mathcal{A}}_0) \mapsto L(\mathcal{A}_1 \otimes \bar{\mathcal{A}}_1 \otimes \mathcal{X}_1)$ and $\bar{\mathscr{A}_i} : L(\mathcal{A}_{i-1} \otimes \bar{\mathcal{A}}_{i-1} \otimes \mathcal{Y}_{i-1}) \mapsto L(\mathcal{A}_i \otimes \bar{\mathcal{A}}_i \otimes \mathcal{X}_i)$, $(2 \leq i \leq s)$, with auxiliary space $\bar{\mathcal{A}}_0$ of sufficiently large dimension being initialized to the zero state. We refer to $\bar{\mathcal{A}}_1, \ldots, \bar{\mathcal{A}}_s$ as the purifying spaces and specify that tracing out the purifying space reverts the state to a state from the original protocol; in particular, this holds for the final state of the protocol: $\text{tr}_{\bar{\mathcal{A}}_s}[\bar{\mathscr{A}} \circledast \mathscr{B}]\left(\rho_{\text{in}}\right) = [\mathscr{A} \circledast \mathscr{B}]\left(\rho_{\text{in}}\right)$ for all $\rho_{\text{in}}$. It is not hard to see that such adversaries always exist (see, for instance Gutoski and Watrous [7]). The definition of a *purified adversary*, $\bar{\mathscr{B}}$ *for* $\mathscr{B}$ is obtained similarly as the definition for $\bar{\mathscr{A}}$. In particular, $\Pi = \left(\bar{\mathscr{A}}, \bar{\mathscr{B}}, s\right)$ denotes the protocol where both parties $\mathscr{A}$ and $\mathscr{B}$ are purified.

### 2.3. *Specious Adversaries*

Recall the intuition that a specious adversary should be able, at each step of the protocol, to produce a state that, when joined with the honest party's state, is close (in trace distance) to the joint state of an honest execution of the protocol. Dupuis et al. [5] give a definition for specious adversaries in the most general context. For the purposes of QPIR in our model, the following is an equivalent definition. Below we also define *ultimately specious* adversaries, which are adversaries that satisfy the criteria for speciousness at the last step of the protocol.

**Definition 2** (Specious adversaries). Let $\Pi = (\mathscr{A}, \mathscr{B}, s)$ be an $s$-round two-party protocol. We say that an adversary $\tilde{\mathscr{A}}$ for $\mathscr{A}$ is $\varepsilon$-*specious*, if there exists a sequence of quantum operations $(\mathscr{F}_1, \ldots, \mathscr{F}_{2s})$, such that for all $1 \leq i \leq 2s$ and for all $\rho_{\text{in}} \in S(\mathcal{A}_0 \otimes \mathcal{B}_0 \otimes \mathcal{R})$,

1.
$$\mathscr{F}_i : \begin{cases} L(\tilde{\mathcal{A}}_{(i+1)/2}) \mapsto L(\mathcal{A}_{(i+1)/2}), & i \text{ even} \\ L(\tilde{\mathcal{A}}_i \otimes \mathcal{X}_{i/2+1}) \mapsto L(\mathcal{A}_i \otimes \mathcal{X}_{i/2+1}), & i \text{ odd} \end{cases} \tag{5}$$

2. for every input state $\rho_{\text{in}} \in S(\mathcal{A}_0 \otimes \mathcal{B}_0 \otimes \mathcal{R})$,

$$\Delta\left(\left(\mathscr{F}_i \otimes \mathbb{1}_{\mathcal{B}_i,\mathcal{R}}\right)\left(\tilde{\rho}_i\left(\tilde{\mathscr{A}}, \rho_{\text{in}}\right)\right), \rho_i\left(\rho_{\text{in}}\right)\right) \leq \varepsilon\,. \tag{6}$$

We call an adversary $\tilde{\mathscr{A}}$ for $\mathscr{A}$ *ultimately* $\varepsilon$*-specious*, if there exists a quantum operation $\mathscr{F} : L(\tilde{\mathcal{A}}_s) \mapsto L(\mathcal{A}_s)$, such that for every input state $\rho_{\text{in}} \in S(\mathcal{A}_0 \otimes \mathcal{B}_0 \otimes \mathcal{R})$,

$$\Delta\left(\left(\mathscr{F} \otimes \mathbb{1}_{\mathcal{B}_s,\mathcal{R}}\right)\left(\left[\tilde{\mathscr{A}} \circledast \mathscr{B}\right](\rho_{\text{in}})\right), \left[\mathscr{A} \circledast \mathscr{B}\right](\rho_{\text{in}})\right) \leq \varepsilon\,. \tag{7}$$

### 2.4. *Definitions for QPIR*

Using the formalism developed so far, we now define QPIR protocols. In particular, we define a notion of approximate correctness, together with a notion of approximate privacy against specious servers; *correctness* refers to the notion that the client should obtain the correct outcome at the end of the protocol, while *privacy* refers to the notion that the server should learn essentially nothing about the client's input via its interaction with the client. For specious adversaries, this corresponds to the intuitive notion that the server's local density matrix at each step of the protocol should be independent of the client's input $i$; in other words, there must exist at each step of the protocol, a quantum map $\mathscr{S}$ that has access only to the server's input register and that reproduces, or *simulates* the server's local view. This is the standard ideal-real world simulation-based security notion that is simplified to the QPIR setting and required only for specious adversaries.

We also consider *ultimate* privacy (i.e., the privacy condition holds at the end of the protocol) against purified servers, which is sufficient in order to show our result.

**Definition 3** (QPIR protocol). An $s$*-round*, $n$*-bit QPIR protocol* is a two-party protocol $\Pi_{\mathsf{QPIR}} = (\mathscr{A}, \mathscr{B}, s)$, where $\mathscr{A}$ is the server and $\mathscr{B}$ is the client.

We call $\Pi_{\mathsf{QPIR}}$ $(1-\delta)$*-correct* if for all inputs $\rho_{\text{in}} = |x\rangle\langle x|_{\mathcal{A}_0} \otimes |i\rangle\langle i|_{\mathcal{B}_0}$, with $x = x_1, \ldots, x_n \in \{0,1\}^n$ and $i \in \{1, \ldots, n\}$, there exists a measurement $\mathcal{M}$ with outcome 0 or 1, such that:

$$\Pr\left[\mathcal{M}\left(\text{tr}_{\mathcal{A}_s}\left[\mathscr{A} \circledast \mathscr{B}\right](\rho_{\text{in}})\right) = x_i\right] \geq 1 - \delta\,. \tag{8}$$

We call $\Pi_{\mathsf{QPIR}}$ $(1-\varepsilon)$*-private against* $\gamma$*-specious servers* if for every $\gamma$-specious server $\tilde{\mathscr{A}}$, there exists a sequence of quantum operations $\mathscr{S}_1, \ldots, \mathscr{S}_{s-1}$ where $\mathscr{S}_i : L(\mathcal{A}_0) \mapsto L(\tilde{\mathcal{A}}_i \otimes \mathcal{Y}_i)$, such that for all $1 \leq i \leq s-1$ and for all $\rho_{\text{in}} \in S(\mathcal{A}_0 \otimes \mathcal{B}_0 \otimes \mathcal{R})$,

$$\Delta\left(\text{tr}_{\mathcal{B}_0}\left(\left(\mathscr{S}_i \otimes \mathbb{1}_{\mathcal{B}_0,\mathcal{R}}\right)(\rho_{\text{in}})\right), \text{tr}_{\mathcal{B}_i}\left(\tilde{\rho}_i\left(\tilde{\mathscr{A}}, \rho_{\text{in}}\right)\right)\right) \leq \varepsilon\,, \tag{9}$$

We call $\Pi_{\mathsf{QPIR}}$ *ultimately* $(1-\varepsilon)$*-private against purified servers* if for every purification $\tilde{\mathscr{A}}$ of the server $\mathscr{A}$, there exists a quantum operation $\mathscr{S} : L(\mathcal{A}_0) \mapsto L(\mathcal{A}_s \otimes \bar{\mathcal{A}}_s)$, such that for all $\rho_{\text{in}} \in S(\mathcal{A}_0 \otimes \mathcal{B}_0 \otimes \mathcal{R})$,

$$\Delta\Big(\mathrm{tr}_{\mathcal{B}_0}\left(\mathscr{S}\otimes \mathbb{1}_{\mathcal{B}_0,\mathcal{R}}\right)(\rho_{\mathrm{in}}),\, \mathrm{tr}_{\mathcal{B}_s}\left[\bar{\mathscr{A}}\circledast\mathscr{B}\right](\rho_{\mathrm{in}})\Big)\leq\varepsilon\,. \tag{10}$$

## 3. Tools

In this section, we present definitions and results that are used in the proof of our main result.

### 3.1. *Entropy*

**Definition 4** (Shannon entropy). Let $P_X$ be a probability distribution over the alphabet $X$. Then, the Shannon entropy $H(P_X)$ of $P_X$ is

$$H(P_X) := -\sum_{x\in X} P_X(x)\log\left(P_X(x)\right)\,. \tag{11}$$

The Shannon entropy of a binary random variable is called *binary entropy*.

**Definition 5** (Binary entropy). Let $p$ be the probability of an event of a binary random variable. Then, the binary entropy $H_{\mathrm{bin}}(p)$ of $p$ is

$$H_{\mathrm{bin}}(p) := -p\log p-(1-p)\log(1-p)\,. \tag{12}$$

### 3.2. *Trace distance and fidelity*

We have already encountered the *trace norm* and *trace distance* in Sect. 2.1. Another measure of distance between two density operators $\rho$ and $\sigma$ is the *fidelity* defined as

$$F(\rho,\sigma) := \left\|\rho^{\frac{1}{2}}\sigma^{\frac{1}{2}}\right\|_1\,. \tag{13}$$

For pure states $|x\rangle$ and $|y\rangle$, we define $F(|x\rangle,|y\rangle)$ as $F(|x\rangle\langle x|,|y\rangle\langle y|)$. The following Lemma simplifies the calculation of the fidelity.

**Lemma 1** (Uhlmann's Lemma). *The fidelity between $\rho_{\mathcal{A}}\in S(\mathcal{A})$ and $\sigma_{\mathcal{A}}\in S(\mathcal{A})$ is*

$$F(\rho_{\mathcal{A}},\sigma_{\mathcal{A}}) = \max_{|\varphi\rangle_{\mathcal{A},\mathcal{B}},|\psi\rangle_{\mathcal{A},\mathcal{B}}} F\left(|\varphi\rangle_{\mathcal{A},\mathcal{B}},|\psi\rangle_{\mathcal{A},\mathcal{B}}\right) \tag{14}$$

$$= \max_{|\varphi\rangle_{\mathcal{A},\mathcal{B}},|\psi\rangle_{\mathcal{A},\mathcal{B}}} \left|\langle\varphi|\psi\rangle_{\mathcal{A},\mathcal{B}}\right|\,, \tag{15}$$

*where the maximum is taken over all purifications of $\rho_{\mathcal{A}}=\mathrm{tr}_{\mathcal{B}}|\varphi\rangle\langle\varphi|_{\mathcal{A},\mathcal{B}}$ and over all purifications of $\sigma_{\mathcal{A}}=\mathrm{tr}_{\mathcal{B}}|\psi\rangle\langle\psi|_{\mathcal{A},\mathcal{B}}$.*

Recall the Fuchs-van de Graaf inequalities, relating the fidelity to the trace distance:

**Lemma 2** (Fuchs-van de Graaf inequalities). *Let $\rho, \sigma \in S(\mathcal{A})$ be density operators, then*

$$1 - F(\rho, \sigma) \leq \Delta(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}\,. \tag{16}$$

The following lemma states that given two density matrices that are close in trace distance, it is possible, by acting only on the purifying subspace, to transform a purification of one of the density matrices into an approximate version of a purification of the other.

**Lemma 3.** *Let $\rho_{\mathcal{A}}, \sigma_{\mathcal{A}} \in S(\mathcal{A})$ be two $\varepsilon$-close density operators, such that*

$$\Delta(\rho_{\mathcal{A}}, \sigma_{\mathcal{A}}) \leq \varepsilon \tag{17}$$

*with respective purifications $|\varphi\rangle_{\mathcal{A},\mathcal{B}}$ and $|\psi\rangle_{\mathcal{A},\mathcal{B}}$. Then, there exists a unitary $\mathsf{U}_{\mathcal{B}}$ acting solely on $\mathcal{B}$, such that*

$$\Delta\left(|\varphi\rangle_{\mathcal{A},\mathcal{B}}, (\mathbb{1}_{\mathcal{A}} \otimes \mathsf{U}_{\mathcal{B}})\,|\psi\rangle_{\mathcal{A},\mathcal{B}}\right) \leq \sqrt{\varepsilon(2-\varepsilon)}\,. \tag{18}$$

*Proof of Lemma 3.* Let $\rho_{\mathcal{A}}, \sigma_{\mathcal{A}} \in S(\mathcal{A})$ be two density operators, with $\Delta(\rho_{\mathcal{A}}, \sigma_{\mathcal{A}}) \leq \varepsilon$. By the first inequality of Lemma 2 we get

$$F(\rho_{\mathcal{A}}, \sigma_{\mathcal{A}}) \geq 1 - \varepsilon\,. \tag{19}$$

Let the state $|\varphi\rangle_{\mathcal{A},\mathcal{B}}$ be an arbitrary purification of the density operator $\rho_{\mathcal{A}}$. By Lemma 1, there exists a purification $|\psi'\rangle_{\mathcal{A},\mathcal{B}}$ of the density operator $\sigma_{\mathcal{A}}$, such that

$$F(\rho_{\mathcal{A}}, \sigma_{\mathcal{A}}) = F(|\varphi\rangle_{\mathcal{A},\mathcal{B}}, |\psi'\rangle_{\mathcal{A},\mathcal{B}})\,. \tag{20}$$

Therefore, the fidelity lower bound (19) is also a lower bound for the fidelity between the pure states $|\varphi\rangle_{\mathcal{A},\mathcal{B}}$ and $|\psi'\rangle_{\mathcal{A},\mathcal{B}}$. Using this in the second inequality of Lemma 2 yields

$$\Delta(|\varphi\rangle_{\mathcal{A},\mathcal{B}}, |\psi'\rangle_{\mathcal{A},\mathcal{B}}) \leq \sqrt{1 - F(|\varphi\rangle_{\mathcal{A},\mathcal{B}}, |\psi'\rangle_{\mathcal{A},\mathcal{B}})^2}\,. \tag{21}$$

By squaring both sides and plugging in inequality (19), we get

$$\begin{aligned}
\Delta(|\varphi\rangle_{\mathcal{A},\mathcal{B}}, |\psi'\rangle_{\mathcal{A},\mathcal{B}})^2 &\leq 1 - F(|\varphi\rangle_{\mathcal{A},\mathcal{B}}, |\psi'\rangle_{\mathcal{A},\mathcal{B}})^2 && (22)\\
&\leq 1 - (1-\varepsilon)^2 && (23)\\
&= \varepsilon(2-\varepsilon)\,. && (24)
\end{aligned}$$

Because purifications are equivalent up to unitary transformations on the purifying system, we thus get

$$\Delta\left(|\varphi\rangle_{\mathcal{A},\mathcal{B}}, (\mathbb{1}_{\mathcal{A}} \otimes \mathsf{U}_{\mathcal{B}})\,|\psi\rangle_{\mathcal{A},\mathcal{B}}\right) \leq \sqrt{\varepsilon(2-\varepsilon)}\,, \tag{25}$$

where

$$(\mathbb{1}_{\mathcal{A}} \otimes \mathsf{U}_{\mathcal{B}})\,|\psi\rangle_{\mathcal{A},\mathcal{B}} = |\psi'\rangle_{\mathcal{A},\mathcal{B}}\,. \tag{26}$$

□

### 3.3. *The Schmidt Decomposition and its Properties*

The Schmidt compression allows for a lossless compression of a quantum state. We first describe the Schmidt decomposition.

**Theorem 1** (Schmidt decomposition). *Let $|\psi\rangle_{\mathcal{A},\mathcal{B}}$ be a pure state shared between party $\mathscr{A}$ and party $\mathscr{B}$. Then, there exists a set of orthonormal pure states $\{|a_i\rangle_{\mathcal{A}}\}$ for party $\mathscr{A}$, a set of orthonormal pure states $\{|b_i\rangle_{\mathcal{B}}\}$ for party $\mathscr{B}$, a set of real coefficients $\{\lambda_i\}$ called* Schmidt coefficients*, and a positive integer $r$ called* Schmidt rank*, such that*

$$|\psi\rangle_{\mathcal{A},\mathcal{B}} = \sum_{i=1}^{r} \lambda_i |a_i\rangle_{\mathcal{A}} |b_i\rangle_{\mathcal{B}}\,. \tag{27}$$

Because the spaces $\mathcal{A}$ and $\mathcal{B}$ use only $r$ different orthonormal pure states, both spaces can be compressed independently to spaces of dimension $r$ with $\lceil \log r \rceil$ qubits. This is known as *Schmidt compression*.

The following theorem states that we can bound the Schmidt rank of a bipartite state resulting from a purified two-party protocol. This theorem is attributed to Kremer [12] (see Lemma 5).

**Theorem 2** (Bound on Schmidt rank). *Let $\Pi = \left(\bar{\mathscr{A}}, \bar{\mathscr{B}}, s\right)$ be a two-party quantum protocol with purified parties $\bar{\mathscr{A}}$ and $\bar{\mathscr{B}}$, and let $\rho_{in} = |\phi_0\rangle_{\mathcal{A},\mathcal{B}}$ be a pure product state. Suppose $\Pi$ has communication complexity $c$. Then, $[\bar{\mathscr{A}} \circledast \bar{\mathscr{B}}]\,(\rho_{in})$ has Schmidt rank at most $2^c$.*

*Proof of Theorem 2.* In the following, we ignore unitary operations on either side during the protocol, because such operations do not increase the Schmidt rank.

Let $|\phi_d\rangle_{\mathcal{A},\mathcal{B}}$ be the shared state after $d$ qubits have been communicated and let

$$|\phi_d\rangle_{\mathcal{A},\mathcal{B}} = \sum_{i=1}^{r} \lambda_i |a_i\rangle_{\mathcal{A}} |b_i\rangle_{\mathcal{B}} \tag{28}$$

be the corresponding Schmidt decomposition. The terms belonging to party $\mathscr{A}$ from the Schmidt decomposition (28) can be expanded as

$$|a_i\rangle_{\mathcal{A}} = \alpha_i |a_i^0\rangle_{\mathcal{A}_\ell} |0\rangle_{\mathcal{A}_r} + \beta_i |a_i^1\rangle_{\mathcal{A}_\ell} |1\rangle_{\mathcal{A}_r}\,. \tag{29}$$

Without loss of generality, assume that in the next step in the protocol, the qubit from the space $\mathcal{A}_r$ is sent from party $\mathscr{A}$ to party $\mathscr{B}$. By plugging in the expanded expression (29) into the Schmidt decomposition (28), we get

$$|\phi_d\rangle_{\mathcal{A},\mathcal{B}} = \sum_{i=1}^{r} \lambda_i \left(\alpha_i |a_i^0\rangle_{\mathcal{A}_\ell} |0\rangle_{\mathcal{A}_r} + \beta_i |a_i^1\rangle_{\mathcal{A}_\ell} |1\rangle_{\mathcal{A}_r}\right) |b_i\rangle_{\mathcal{B}} \tag{30}$$

$$= \sum_{i=1}^{r} \lambda_i \alpha_i |a_i^0\rangle_{\mathcal{A}_\ell} |0\rangle_{\mathcal{A}_r} |b_i\rangle_{\mathcal{B}} + \lambda_i \beta_i |a_i^1\rangle_{\mathcal{A}_\ell} |1\rangle_{\mathcal{A}_r} |b_i\rangle_{\mathcal{B}} \,. \tag{31}$$

Hence the transmission of one qubit at most doubles the number of summands, which is an upper bound of the Schmidt rank of the new Schmidt decomposition into the spaces $\mathcal{A}_\ell$ and $\mathcal{A}_r \otimes \mathcal{B}$. By assumption, the initial state $|\phi_0\rangle_{\mathcal{A},\mathcal{B}}$ has Schmidt rank 1. Therefore, after communicating $c$ qubits, the Schmidt rank is at most $2^c$. □

### 3.4. *Random Access Encoding*

A random access encoding is an encoding of classical database as a density operator, such that any database item can be extracted with a certain probability using a measurement which is independent of the database. It is easy to see that the message of a single-message QPIR protocol is a random access encoding of the server's database. We state the definition of random access encoding and a theorem on their size; here, we consider the average case scenario, which follows from Nayak's work [16] (see also Kerenidis and de Wolf [10], Appendix B).

**Definition 6** (Random access encoding). An $(n, m, p)$-*random access encoding* is a function $f$ that maps $n$-bit strings to density operators over $m$ qubits, such that, for every $i \in \{1, \ldots, n\}$, there exists a measurement $\mathscr{M}_i$ with outcome 0 or 1 that has the property that on average over all $x \in \{0, 1\}^n$,

$$\Pr\left[\mathscr{M}_i\left(f\left(x\right)\right) = x_i\right] \geq p \,. \tag{32}$$

**Theorem 3** (Size of random access encoding). *Any* $(n, m, p)$-*random access encoding satisfies* $m \geq \left(1 - H_{bin}\left(p\right)\right) n$.

## 4. Main Theorem

In this section, we present our main result and related corollaries. The proof is given in Sect. 4.2.

### 4.1. *Results*

Our main result is the following.

**Theorem 4.** *Let* $\Pi_{\mathsf{QPIR}} = (\mathscr{A}, \mathscr{B}, s)$ *be an* $s$*-round,* $n$*-bit QPIR protocol, that is* $(1-\delta)$*-correct and ultimately* $(1-\varepsilon)$*-private against purified servers. Then,* $\Pi_{\mathsf{QPIR}}$ *has communication complexity of at least*

$$\left(1 - H_{bin}\left(1 - \delta - 2\sqrt{\varepsilon(1-\varepsilon)}\right)\right) n\,. \tag{33}$$

The above theorem is an extension of Nayak's result on QPIR [16] to approximate privacy, and requiring security only against a purified server at the end of the protocol. It is easy to see that a purified server is specious (see Sect. 2.2). Therefore, any QPIR protocol that is $(1-\varepsilon)$-private against $\gamma$-specious servers is also $(1-\varepsilon)$-private against purified serves. Trivially such a protocol is ultimately $(1-\varepsilon)$-private against purified servers. Hence, by Theorem 4 we get the following.

**Corollary 1.** *Let $\Pi_{\mathsf{QPIR}} = (\mathscr{A}, \mathscr{B}, s)$ be an $s$-round, $n$-bit QPIR protocol that is $(1-\delta)$-correct and $(1-\varepsilon)$-private against $\gamma$-specious servers. Then, for any $\gamma$, $\Pi_{\mathsf{QPIR}}$ has communication complexity of at least*

$$\left(1 - H_{bin}\left(1 - \delta - 2\sqrt{\varepsilon(1-\varepsilon)}\right)\right) n\,. \tag{34}$$

Let $\delta$ and $\varepsilon$ be non-negative and negligible functions[3] with respect to $n$. Then, for any $\gamma$, the communication complexity as given in Corollary 1 is at least $n - o(1)$. In sharp contrast to this, in Le Gall's model (that considers an adversary that follows the protocol exactly), the communication complexity is $\mathcal{O}\left(\sqrt{n}\right)$; we, therefore, obtain the following corollary.

**Corollary 2.** *Le Gall's QPIR protocol is not private against $\gamma$-specious adversaries, for any $\gamma$.*

An alternate proof of Corollary 2, via an explicit specious attack, can be found in the thesis of Baumeler [1].

### 4.2. *Proof of Theorem 4*

The main technique used in the proof of Theorem 4 is to reduce a given QPIR protocol to a random access encoding, and then apply Nayak's lower bound as established by Theorem 3. This is the same technique as used by Nayak in his lower bound proof for QPIR, which we extend here to the case of approximate privacy against ultimately specious servers.

As a starting point to understanding the reduction, note that any single-message QPIR protocol (where one message is sent from the server to the client) implements a random access encoding. Hence, the lower bound on the size of the random access encoding is also a lower bound on the communication complexity for the single-message QPIR protocol. We generalize this idea to ultimately $(1-\varepsilon)$-private against purified servers, multi-round QPIR protocols by reducing the multi-round protocol to a single-message protocol, and hence to a random access encoding. Taking care that this procedure does not increase the amount of communication allows us to apply the lower bound on the

[3] A non-negative function $\mu$ is called *negligible with respect to $n$* if for all $c > 0$ and all sufficiently large $n$, $\mu(n) < n^{-c}$.

size of the random access encoding to the communication complexity of the multi-step QPIR protocol, thus establishing the result.

*Proof of Theorem 4.* Let $\Pi_{\mathsf{QPIR}}$ be an $s$-round, $n$-bit, $(1-\delta)$-correct QPIR protocol that is ultimately $(1-\varepsilon)$-private against purified servers and that has communication complexity $c$.

Consider $\Pi_{\mathsf{QPIR}}(\bar{\mathscr{A}}, \bar{\mathscr{B}})$, the modification of $\Pi_{\mathsf{QPIR}}$, where both parties, $\mathscr{A}$ and $\mathscr{B}$, are purified, as described in Sect. 2.2. We denote by $\mathcal{S} \approx \mathcal{A}_s \otimes \bar{\mathcal{A}}_s$ the server's subspace, and by $\mathcal{C} \approx \mathcal{B}_s \otimes \bar{\mathcal{B}}_s$ the client's subspace at the end of the protocol. Furthermore, let

$$|\bar{\psi}_{x,i}\rangle\langle\bar{\psi}_{x,i}|_{\mathcal{S},\mathcal{C}} := \left[\bar{\mathscr{A}} \circledast \bar{\mathscr{B}}\right]\left(|x\rangle\langle x| \otimes |i\rangle\langle i|\right); \tag{35}$$

that is, $|\bar{\psi}_{x,i}\rangle_{\mathcal{S},\mathcal{C}}$ is the global state at the end of the protocol $\Pi_{\mathsf{QPIR}}(\bar{\mathscr{A}}, \bar{\mathscr{B}})$, with inputs $x \in \{0,1\}^n$ for the database and $i \in \{1,\ldots,n\}$ for the index.

**Encoding.** Given $\Pi_{\mathsf{QPIR}}(\bar{\mathscr{A}}, \bar{\mathscr{B}})$, we derive a random access encoding in the following way: the server simulates the purified version $\Pi_{\mathsf{QPIR}}(\bar{\mathscr{A}}, \bar{\mathscr{B}})$ of the protocol $\Pi_{\mathsf{QPIR}}$ with inputs $|x\rangle$ as database input and index $|i\rangle = |1\rangle$. The joint output is $|\bar{\psi}_{x,1}\rangle_{\mathcal{S},\mathcal{C}}$.

Consider $|\xi\rangle_{\mathcal{D}}$, the uniform superposition of all possible databases

$$|\xi\rangle_{\mathcal{D}} := \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_{\mathcal{D}}\,, \tag{36}$$

and let

$$|\nu_i\rangle\langle\nu_i|_{\mathcal{S},\mathcal{C}} := \left[\bar{\mathscr{A}} \circledast \bar{\mathscr{B}}\right]\left(|\xi\rangle\langle\xi|_{\mathcal{D}} \otimes |i\rangle\langle i|\right). \tag{37}$$

Since we consider the case where both parties are purified, the final global state is

$$|\nu_i\rangle_{\mathcal{S},\mathcal{C}} = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\bar{\psi}_{x,i}\rangle_{\mathcal{S},\mathcal{C}}\,. \tag{38}$$

By Theorem 2, the Schmidt decomposition of $|\nu_i\rangle_{\mathcal{S},\mathcal{C}}$ into the subspace $\mathcal{S}$ and $\mathcal{C}$ has Schmidt rank at most $2^c$. Hence there exists a Schmidt compression of the subspace $\mathcal{C}$ into at most $c$ qubits. By linearity, this map can be used to compress (and decompress) $|\bar{\psi}_{x,1}\rangle_{\mathcal{S},\mathcal{C}}$ for any $x \in \{0,1\}^n$. The server applies this compression on system $\mathcal{C}$ of $|\bar{\psi}_{x,1}\rangle_{\mathcal{S},\mathcal{C}}$. Let the result of the compression be $|\bar{\psi}^c_{x,1}\rangle_{\mathcal{S},\mathcal{C}'}$. The server outputs as encoding of database $x$ the state of the subsystem $\mathcal{C}'$:

$$\mathrm{tr}_{\mathcal{S}}|\bar{\psi}^c_{x,1}\rangle\langle\bar{\psi}^c_{x,1}|_{\mathcal{S},\mathcal{C}'}\,. \tag{39}$$

**Decoding.** Given the output of the Encoding algorithm, the client applies the inverse operation of the Schmidt compression obtained above in order to recover the joint state corresponding to the input $i = 1$:

$$|\bar{\psi}_{x,1}\rangle_{\mathcal{S},\mathcal{C}}\,. \tag{40}$$

However, the client would like to recover the joint state for an arbitrary $i$. To this end, consider again $|\xi\rangle_{\mathcal{D}}$, the uniform superposition of databases as database input, and fix $i \in \{1,\ldots,n\}$ as index input. Let the corresponding input state be $\rho_{\text{in}}^{\xi,i}$. By the privacy condition (Eq. 10), there exists a quantum map $\mathscr{S} : L(\mathcal{A}_0) \mapsto L(\mathcal{A}_s \otimes \bar{\mathcal{A}}_s)$, such that

$$\Delta\left(\text{tr}_{\mathcal{B}_0}\left(\mathscr{S}\otimes \mathbb{1}_{\mathcal{B}_0,\mathcal{R}}\right)\left(\rho_{\text{in}}^{\xi,i}\right), \text{tr}_{\mathcal{B}_s}\left[\bar{\mathscr{A}}\circledast\mathscr{B}\right]\left(\rho_{\text{in}}^{\xi,i}\right)\right) \leq \varepsilon\,. \tag{41}$$

Since for all $i \in \{1,\ldots,n\}$

$$\text{tr}_{\mathcal{B}_0}\left(\mathscr{S}\otimes \mathbb{1}_{\mathcal{B}_0,\mathcal{R}}\right)\left(\rho_{\text{in}}^{\xi,1}\right) = \text{tr}_{\mathcal{B}_0}\left(\mathscr{S}\otimes \mathbb{1}_{\mathcal{B}_0,\mathcal{R}}\right)\left(\rho_{\text{in}}^{\xi,i}\right) \tag{42}$$

and

$$\begin{aligned}\text{tr}_{\mathcal{B}_s}\left[\bar{\mathscr{A}}\circledast\mathscr{B}\right]\left(\rho_{\text{in}}^{\xi,i}\right) &= \text{tr}_{\mathcal{C}}\left[\bar{\mathscr{A}}\circledast\bar{\mathscr{B}}\right]\left(\rho_{\text{in}}^{\xi,i}\right) &(43)\\ &= \text{tr}_{\mathcal{C}}|\nu_i\rangle\langle\nu_i|_{\mathcal{S},\mathcal{C}}\,, &(44)\end{aligned}$$

by the triangle inequality, we get that for all $i \in \{1,\ldots,n\}$,

$$\Delta\left(\text{tr}_{\mathcal{C}}|\nu_1\rangle\langle\nu_1|_{\mathcal{S},\mathcal{C}}, \text{tr}_{\mathcal{C}}|\nu_i\rangle\langle\nu_i|_{\mathcal{S},\mathcal{C}}\right) \leq 2\varepsilon\,. \tag{45}$$

Thus, by Lemma 3, for every $i \in \{1,\ldots,n\}$, there exists a unitary $\mathsf{U}_{\mathcal{C}}^{1\to i}$ acting only on the client's subspace, such that

$$\Delta\left(\left(\mathbb{1}_{\mathcal{S}}\otimes\mathsf{U}_{\mathcal{C}}^{1\to i}\right)|\nu_1\rangle_{\mathcal{S},\mathcal{C}}, |\nu_i\rangle_{\mathcal{S},\mathcal{C}}\right) \leq 2\sqrt{\varepsilon(1-\varepsilon)}\,. \tag{46}$$

Because the trace distance does not increase under measurements, we simply measure the space $\mathcal{D}$ of the states from the inequality (46) and obtain that for a uniform random $x \in \{0,1\}^n$

$$\Delta\left(\left(\mathbb{1}_{\mathcal{S}}\otimes\mathsf{U}_{\mathcal{C}}^{1\to i}\right)|\bar{\psi}_{x,1}\rangle_{\mathcal{S},\mathcal{C}}, |\bar{\psi}_{x,i}\rangle_{\mathcal{S},\mathcal{C}}\right) \leq 2\sqrt{\varepsilon(1-\varepsilon)}\,. \tag{47}$$

Hence, on average over all databases $x \in \{0,1\}^n$, this family $\left\{\mathsf{U}_{\mathcal{C}}^{1\to i}\right\}_i$ of unitary operators can be used to construct a $2\sqrt{\varepsilon(1-\varepsilon)}$-close approximation.

It remains to calculate the recovery probability of the constructed random access code. The QPIR protocol $\Pi_{\mathsf{QPIR}}$ is $(1-\delta)$-correct, and hence there exists a measurement that recovers the desired bit with a probability of at least $1-\delta$. The family of unitary approximation transformations $\left\{\mathsf{U}_{\mathcal{C}}^{1\to i}\right\}_i$, used to approximate the global state, induces a loss in the recovery probability. The approximation is $2\sqrt{\varepsilon(1-\varepsilon)}$-close.

Hence the QPIR protocol yields a random access encoding with recovery probability of at least $1-\delta-2\sqrt{\varepsilon(1-\varepsilon)}$. By applying Nayak's Theorem 3, we get that any $n$-bit,

$(1-\delta)$-correct, ultimately $(1-\varepsilon)$-private against purified servers QPIR protocol has communication complexity of at least

$$\left(1 - H_{\text{bin}}\left(1 - \delta - 2\sqrt{\varepsilon(1-\varepsilon)}\right)\right) n \,. \tag{48}$$

□

It is interesting to note that the reason why this lower bound proof is not applicable to the model in the work of Le Gall [13], is that there the privacy condition (10) does not hold. In other words, the *possibility* of Le Gall's result is a direct consequence of the fact that security is guaranteed only for classical inputs, that is, the adversary is forced to select a classical database at the beginning of the protocol, or equivalently, is forced to measure any superposition of databases that it might receive as input.

## 5. Conclusion and Open Questions

Using quantum computation and quantum communication, non-trivial information-theoretic single-server QPIR protocols secure against any reasonable adversary do not exist. This work closes the topic of single-server and information-theoretic QPIR.

An open question that remains is whether there exist other applications of the reduction from multi-step protocols to single-step protocols used in the proof of the lower bound (see Sect. 4). In the reduction, we show that any protocol with asymmetric privacy at the end of the protocol against one particular type of adversaries, can be transformed to a single-step protocol. The resulting single-step protocol preserves the communication complexity and the privacy property. This reduction could potentially be used to build offline protocols from multi-step protocols. An offline protocol is a protocol, where the parties are not required to be involved in the protocol at the same time. This could be advantageous under some circumstances.

## Acknowledgements

We are grateful to Gus Gutoski, Robert König, and Ashwin Nayak for helpful discussions, and to the anonymous referees for helpful comments. Furthermore, we thank Sébastien Gambs for introducing us to PIR. Ä. B. thanks the Institute for Quantum Computing (IQC) and the University of Waterloo for hosting him for a six-month visit, during which these results were established. This work was performed, while A. B. was at the Department of Combinatorics and Optimization, and at the Institute for Quantum Computing (IQC), University of Waterloo. This work was supported by the Canadian Institute for Advanced Research (CIFAR), NSERC Frequency and Industry Canada.

## References

[1] Ä. Baumeler, Quantum private information retrieval. Master's Thesis, ETH Zürich, 2012. http://e-collection.library.ethz.ch/view/eth:6297

[2] C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in *Proceedings of the International Conference on Computers, Systems, and Signal Processing 1984*, pp. 175–180

[3] A. Chailloux, I. Kerenidis, Optimal bounds for quantum bit commitment, in *Proceedings of the 52th Annual Symposium on Foundations of Computer Science, FOCS 2011*, pp. 354–362
[4] B. Chor, E. Kushilevitz, O. Goldreich, M. Sudan, Private information retrieval. *J. ACM* **45**(6), 965–981 (1998)
[5] F. Dupuis, J.B. Nielsen, L. Salvail, Secure two-party quantum evaluation of unitaries against specious adversaries, in *Proceedings of the 30th Annual Conference on Advances in Cryptology, CRYPTO '10*, (Springer, Berlin, 2010), pp. 685–706
[6] V. Giovannetti, S. Lloyd, L. Maccone, Quantum private queries. *Phys. Rev. Lett.* **100**(23), 230502 (2008)
[7] G. Gutoski, J. Watrous, Toward a general theory of quantum games, in *Proceedings of the 39th Annual ACM Symposium on Theory of Computing, STOC 2007*, pp. 565–574
[8] R. Jain, J. Radhakrishnan, P. Sen, A property of quantum relative entropy with an application to privacy in quantum communication, *J. ACM* **56**(6), 33 (2009). Preliminary version in FOCS '02
[9] M. Jakobi, C. Simon, N. Gisin, J.-D. Bancal, C. Branciard, N. Walenta, H. Zbinden, Practical private database queries based on a quantum-key-distribution protocol. *Phys. Rev. A* **83**, 022301 (2011)
[10] I. Kerenidis, R. de Wolf, Exponential lower bound for 2-query locally decodable codes via a quantum argument. *J. Comput. Syst. Sci.* **9**(3), 395–420 (2004)
[11] I. Kerenidis, R. de Wolf, Quantum symmetrically-private information retrieval, in *Inf. Process. Lett.* **90**, 109–114 (2004)
[12] I. Kremer, Quantum communication. Master's Thesis, The Hebrew University of Jerusalem, 1995. http://www.cs.huji.ac.il/noam/kremer-thesis.ps
[13] F. Le Gall, Quantum private information retrieval with sublinear communication complexity. *Theory Comput.* **8**(1), 369–374 (2012)
[14] H.-K. Lo, H.F. Chau, Is quantum bit commitment really possible? *Phys. Rev. Lett.* **78**(17), 3410–3413 (1997)
[15] D. Mayers, Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.* **78**(17), 3414–3417 (1997)
[16] A. Nayak, Optimal lower bounds for quantum automata and random access codes, in *Proceedings of the 40th Annual Symposium on Foundations of Computer Science, FOCS 1999*, pp. 369–376 (1999)
[17] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**(5), 1484–1509 (1997)
[18] W.K. Wootters, W.H. Zurek, A single quantum cannot be cloned. *Nature* **299**(5886), 802–803 (1982)