Privacy and correctness trade-offs for information-theoretically secure quantum homomorphic encryption

Yanglin Hu (胡杨林)[1], Yingkai Ouyang[1], and Marco Tomamichel[1,2]

[1] Centre of Quantum Technologies, National University of Singapore, Singapore
[2]Department of Electrical and Computer Engineering, National University of Singapore

Quantum homomorphic encryption, which allows computation by a server directly on encrypted data, is a fundamental primitive out of which more complex quantum cryptography protocols can be built. For such constructions to be possible, quantum homomorphic encryption must satisfy two privacy properties: data privacy which ensures that the input data is private from the server, and circuit privacy which ensures that the ciphertext after the computation does not reveal any additional information about the circuit used to perform it, beyond the output of the computation itself. While circuit privacy is well-studied in classical cryptography and many homomorphic encryption schemes can be equipped with it, its quantum analogue has received little attention. Here we establish a definition of circuit privacy for quantum homomorphic encryption with information-theoretic security. Furthermore, we reduce quantum oblivious transfer to quantum homomorphic encryption. By using this reduction, our work unravels fundamental trade-offs between circuit privacy, data privacy and correctness for a broad family of quantum homomorphic encryption protocols, including schemes that allow only the computation of Clifford circuits.

1 Introduction

Given the difficulty of building reliable quantum computers at scale, it is reasonable to expect the first such quantum computers to be controlled by a few service providers with the prerequisite infrastructure and resources [1]. In such a scenario, individual users will, in contrast, only hold quantum computers with far more limited capabilities and must delegate complex computations to large servers. However, there is also an inherent lack of trust between the service providers and the users: individuals would like to keep their data private from large corporations, while the service providers would like to keep their exact implementation private from competitors. Protocols such as blind quantum computing [2, 3, 4, 5, 1, 6] are proposed to help with the situation; they require only minimal quantum capabilities of the client but require extensive communication. Quantum homomorphic encryption [7, 8, 9, 10, 11, 12, 13], which allows a server to compute on encrypted data of a client without first decrypting it, offers an alternative solution to this problem. Here, all communication can be done in one round, but the client needs a quantum computer for encoding the input and decoding the output.

Because classical homomorphic encryption [14, 15, 16] can build a broad range of more complex classical cryptographic primitives such as multiparty secure computation and private information retrieval, it has been called the "Swiss army knife" of classical cryptography [17, 18, 19]. These reductions[1] rely crucially on the data and circuit privacy of homomorphic encryption schemes. While data privacy is inherent in homomorphic encryption, circuit privacy encapsulates the property that no additional information about the computation circuit is leaked beyond its action on the encoded data.

It is natural to conjecture a quantum analogue of the classical reduction, i.e. reducing quantum oblivious transfer to quantum homomorphic encryption. In this paper, we progress in understanding the extent to which quantum homomorphic encryption can be analogously a "Swiss army knife" of quantum cryptography. In particular, we explore the limitations of quantum homomorphic encryption in the paradigm of information-theoretic security.

Quantum homomorphic encryption that allows the delegation of an *arbitrary* quantum computation while also assuring the privacy of the client's encrypted data cannot exist because its existence would violate well-known information-theoretic bounds, such as Nielsen's no-programming bound [7] or fundamental coding-type bounds [21, 22] such as Nayak's bound [23] which bounds the amount of classical information that can be stored in a quantum state. On the other hand, if we consider quantum homomorphic encryption schemes that support only Clifford computations, such schemes exist with asymptotically perfect data privacy and correctness [11]. Hence, there is the hope that, by restricting ourselves to quantum homomorphic encryption schemes that support a limited set of operations [10, 24, 11, 21, 25, 13], such schemes can still have enough functionality (data privacy, correctness and circuit privacy) to serve as a Swiss army knife. Here we show that this is not possible. Namely, even if we restrict ourselves to quantum homomorphic encryption protocols that can perform only two-qubit Clifford gates, we find that data privacy, circuit privacy and correctness cannot be simultaneously achieved. In particular, we obtain non-trivial trade-offs between these parameters for such computationally-restricted quantum homomorphic encryption schemes.

Our main contributions are as follows:

- We introduce a formal definition of circuit privacy for quantum homomorphic encryption schemes. (See Definition 4.) We achieve this by introducing a quantum counterpart of the simulation paradigm [18] in classical cryptography. Roughly speaking, the simulation paradigm is a pattern of using a simulator to compare a possibly insecure actual protocol with a naturally secure ideal protocol.

- We give an explicit reduction from quantum oblivious transfer to quantum homomorphic encryption by constructing a quantum oblivious transfer protocol with a quantum homomorphic encryption protocol. In this reduction, we use only quantum homomorphic encryption protocols that perform delegated Clifford circuits and additionally utilize genuine random classical bits. (See Theorem 21).

- The reduction allows us to inherit no-go results for quantum oblivious transfer [26, 27, 28] to quantum homomorphic encryption. We find that, for any information-theoretically secure quantum homomorphic encryption scheme support (at least)

[1] Suppose that we have two protocols, protocol A and protocol B. If we can use protocol B to realise protocol A, then we can reduce protocol A to protocol B [20]. If protocol A is impossible, then protocol B is also impossible. Thus limitations of protocol A also apply to protocol B.

Clifford operations, it holds that

$$\epsilon_d + \epsilon_c + 4\sqrt{\epsilon} \geq \frac{1}{2}, \tag{1}$$

where ϵ_d, ϵ_c and ϵ are parameters describing data privacy, circuit privacy and correctness, respectively, and ideally, we would want them to all be small.

It is worth emphasizing that our results apply only to quantum homomorphic encryption schemes with information-theoretic security. In particular, quantum homomorphic encryption schemes based on computational hardness assumptions [8, 9, 12] might be able to support better trade-offs for these parameters. Notably, circuit privacy for computational-secure semi-honest quantum homomorphic encryption was discussed in [9].

Our paper is structured as follows. In Section 2, we give formal definitions of quantum cryptographic primitives. In Section 2.3, we give the scheme of quantum homomorphic encryption and define the correctness, data privacy and circuit privacy. In Section 2.4, we discuss two types of quantum oblivious transfer, standard and semi-random oblivious transfer, and show their equivalence. In Section 4, we reduce standard oblivious transfer to quantum homomorphic encryption. In Section 3, we present a bound for semi-random oblivious transfer. In Section 5, we present bounds for quantum homomorphic encryption. In Section 5.1, we obtain our lower bound for quantum homomorphic encryption by reduction. In Section 5.2, we derive our upper bound.

2 Quantum homomorphic encryption and oblivious transfer

2.1 Notations

When $x \in \{0,1\}$ denotes a bit, we let $\overline{x} = x \oplus 1 \in \{0,1\}$ denote its complement. An n-bit string is a binary vector $(x_1, ..., x_n) \in \{0,1\}^n$. A random bit is denoted by \$. We use Latin capital letters in a sans serif font, such as X, to denote the system and also its Hilbert space. The set of density matrices of a system X is denoted by $\mathscr{S}(\mathsf{X})$. The set of completely positive trace-preserving maps from a system X to a system Y is denoted by $\mathrm{CPTP}(\mathsf{X},\mathsf{Y})$. The set of unitary channels on X is denoted by $\mathscr{U}(\mathsf{X})$. The adjoint channel $\mathcal{N}^* \in \mathrm{CPTP}(\mathsf{Y},\mathsf{X})$ of a channel $\mathcal{N} \in \mathrm{CPTP}(\mathsf{X},\mathsf{Y})$ is defined by the relation $\mathrm{Tr}(\rho\mathcal{N}(\sigma)) = \mathrm{Tr}(\mathcal{N}^*(\rho)\sigma)$ for all $\rho \in \mathscr{S}(\mathsf{Y})$ and $\sigma \in \mathscr{S}(\mathsf{X})$. The identity channel of n dimensions is denoted by $\mathcal{I}_n$. The identity channel on X is denoted by $\mathcal{I}_{\mathsf{X}}$. For simplicity, we will omit identity channels $\mathcal{I}_{\mathsf{X}}$ and $\mathcal{I}_{\mathsf{X}}$ if it does not cause any confusion. The set of unitary operators on X is denoted by $\mathrm{U}(\mathsf{X})$. The identity operator acting on n dimensions and on X are denoted by $\mathbb{I}_n$ and $\mathbb{I}_{\mathsf{X}}$, respectively. The Schatten 1-norm is defined by $\|A\|_1 = \sqrt{A^\dagger A}$. The trace distance is defined by $\Delta(A,B) = \frac{1}{2}\|A - B\|_1$. The fidelity is defined by $F(A,B) = \|\sqrt{A}\sqrt{B}\|_1$. The Hermitian conjugate of a term in an equation is denoted by a h.c. following the term. Table 1 summarizes the notations.

2.2 Classical homomorphic encryption

For the formal definition of classical homomorphic encryption, interested readers may refer to [15, 18]. Here we only introduce classical homomorphic encryption informally, emphasising its scheme and circuit privacy. In a classical homomorphic encryption protocol, Alice, the user, encrypts the input and sends the ciphertext to Bob, the server. Next, Bob evaluates a function on the ciphertext without decryption and sends the evaluated ciphertext back to Alice. Finally, Alice decrypts the evaluated ciphertext and obtains the output.

Notation	Description
$	A random bit.
X	The system and also its Hilbert space.
$\mathscr{S}(\mathsf{X})$	The set of density matrices on X.
$\mathrm{CPTP}(\mathsf{X},\mathsf{Y})$	The set of CPTP maps from X to Y.
$\mathscr{U}(\mathsf{X})$	The set of unitary channels on X.
$\mathcal{N}^*$	The adjoint channel of $\mathcal{N}$.
$\mathcal{I}_n$	The identity channel of n dimensions.
$\mathcal{I}_{\mathsf{X}}$	The identity channel on X.
$\mathrm{U}(\mathsf{X})$	The set of unitary matrices on X.
$\mathbb{I}_n$	The identity operator of n dimensions.
$\mathbb{I}_{\mathsf{X}}$	The identity operator on X.
$\|\cdot\|_1$	The Schatten 1-norm.
$\Delta(\cdot,\cdot)$	The trace distance between two states.
$F(\cdot,\cdot)$	The fidelity between two states.
h.c.	The Hermitian conjugate of a term.

Table 1: Notations

The correctness of classical homomorphic encryption requires that the output is the same as the function computed on the input. Data privacy requires that Bob cannot distinguish the ciphertexts corresponding to different inputs.

Circuit privacy is defined in a simulation paradigm. It is defined by comparing a possibly insecure actual protocol to a naturally secure ideal protocol. Alice knows the input, the ciphertext, and the modified ciphertext in the actual protocol. In the ideal protocol, Alice knows the input and the function computed by the input. Bob's circuit is private if Alice does not learn more information about the circuit in the actual protocol than in the ideal protocol. This happens when a simulator can simulate the results of the actual protocol with the results of the ideal protocol. Hence, circuit privacy quantifies the simulator's performance.

In classical cryptography, we can reduce classical oblivious transfer to classical homomorphic encryption. For a generic but simple classical reduction from classical oblivious transfer to classical homomorphic encryption, interested readers may refer to [19]. The essence of the reduction is that classical homomorphic encryption ensures not only data privacy but also circuit privacy. We will use this idea in the quantum analogue of classical reduction.

2.3 Quantum homomorphic encryption

In this subsection, we introduce relevant definitions of quantum homomorphic encryption. The scheme of quantum homomorphic encryption is similar to that of classical homomorphic encryption, which is presented in Definition 1. Both data privacy and circuit privacy are essential if we treat quantum homomorphic encryption as a "Swiss army knife" primitive. We formally define correctness, data privacy and circuit privacy as a quantum analogue of their classical counterparts in Definition 2, Definition 3 and Definition 4, respectively.

Figure 1 describes a quantum homomorphic encryption scheme. In a quantum homomorphic encryption protocol, Alice computes a function `KeyGen` to obtain the key, uses the key and encryption map `Enc` to encrypt Alice's input and then sends the encryption

to Bob. Bob applies $\texttt{Eval}$ to evaluate Bob's channel $\mathcal{F}$ on the encryption and sends the evaluated encryption back to Alice. Alice decrypts the evaluated encryption with the key and a decryption map $\texttt{Dec}$ and obtains Alice's output.

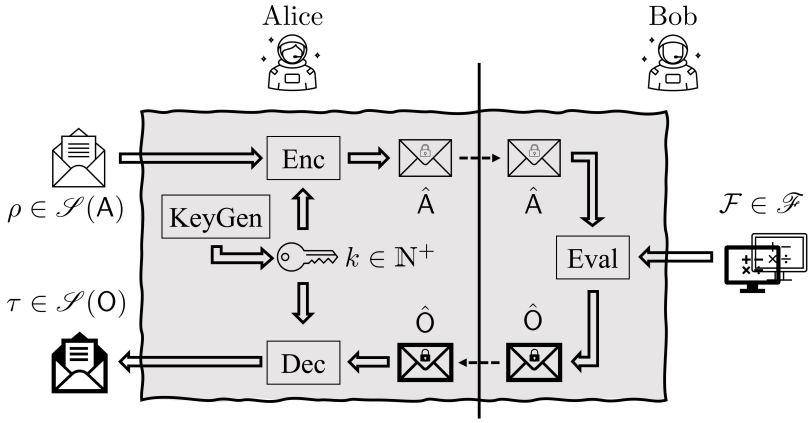


Figure 1: The scheme of quantum homomorphic encryption.

Definition 1 (Scheme for quantum homomorphic encryption)**.** *A quantum homomorphic encryption protocol is a secure two-party computation protocol where Alice requires Bob to evaluate a channel in one round of communication. It is characterized by a set of channels and four maps* $(\mathscr{F}, \texttt{KeyGen}, \texttt{Enc}, \texttt{Eval}, \texttt{Dec})$*.*

- $\mathscr{F} \subset \mathrm{CPTP}(\mathsf{A}, \mathsf{O})$ *is a set of channels that Alice would like to delegate.*
- $\texttt{KeyGen} : \emptyset \to \{0,1\}^L$ *is the key generation map which generates a random key* $k \in \{0,1\}^L$ *where* L *is the length of the key. Without loss of generality, we define the space of all keys as the space of all* L*-bit strings* $\{0,1\}^L$*.*
- $\texttt{Enc} : \{0,1\}^L \times \mathscr{S}(\mathsf{A}) \to \mathscr{S}(\hat{\mathsf{A}})$ *is the encryption map which takes the key* k *and Alice's unencrypted input* $\rho \in \mathscr{S}(\mathsf{A})$ *and gives out Alice's encrypted message* $\sigma \in \mathscr{S}(\hat{\mathsf{A}})$*.*
- $\texttt{Eval} : \mathscr{F} \times \mathscr{S}(\hat{\mathsf{A}}) \to \mathscr{S}(\hat{\mathsf{O}})$ *is the evaluation map which takes in a channel* $\mathcal{F} \in \mathscr{F}$ *and Alice's encrypted message* $\sigma \in \mathscr{S}(\hat{\mathsf{A}})$ *and gives out Bob's encrypted message* $\theta \in \mathscr{S}(\hat{\mathsf{O}})$*.*
- $\texttt{Dec} : \{0,1\}^L \times \mathscr{S}(\hat{\mathsf{O}}) \to \mathscr{S}(\mathsf{O})$ *is the decryption map which takes in the key* k *and Bob's encrypted message* $\theta \in \mathscr{S}(\hat{\mathsf{O}})$ *and gives out Alice's unencrypted output* $\tau \in \mathscr{S}(\mathsf{O})$*.*

For simplicity, we will denote $\texttt{Enc}(k, \cdot)$ *by* $\texttt{Enc}_k$*,* $\texttt{Eval}(\mathcal{F}, \cdot)$ *by* $\hat{\mathcal{F}}(\cdot)$*,* $\{\texttt{Eval}(\mathcal{F}, \cdot) : \mathcal{F} \in \mathscr{F}\}$ *by* $\hat{\mathscr{F}}$ *and* $\texttt{Dec}(k, \cdot)$ *by* $\texttt{Dec}_k(\cdot)$*.*

For a quantum homomorphic encryption protocol to be meaningful, it needs to return the correct output. This is quantified by a property known as correctness.

Definition 2 (Correctness of quantum homomorphic encryption)**.** *A quantum homomorphic encryption protocol* $(\mathscr{F}, \texttt{KeyGen}, \texttt{Enc}, \texttt{Eval}, \texttt{Dec})$ *is* ϵ*-correct if, for every channel* $\mathcal{F} \in \mathscr{F}$*, every Alice's input and its purification* $|\psi'\rangle \in \mathsf{AR}_\mathsf{A}$ *and every key* $k \in \{0,1\}^L$*,*

$$\Delta\left(((\texttt{Dec}_k \hat{\mathcal{F}} \texttt{Enc}_k) \otimes \mathcal{I}_{\mathsf{R}_\mathsf{A}})[|\psi'\rangle\langle\psi'|_{\mathsf{AR}_\mathsf{A}}], (\mathcal{F} \otimes \mathcal{I}_{\mathsf{R}_\mathsf{A}})(|\psi'\rangle\langle\psi'|_{\mathsf{AR}_\mathsf{A}})\right) \leq \epsilon. \tag{2}$$

Specifically when $\epsilon = 0$*, we say that the protocol is perfectly correct.*

Function	Input	Output
$\texttt{KeyGen}$	$\emptyset$	$k \in \{0,1\}^L$
$\texttt{Enc}$	$k \in \{0,1\}^L$, $\rho \in \mathscr{S}(\mathsf{A})$	$\sigma \in \mathscr{S}(\hat{\mathsf{A}})$
$\texttt{Enc}_k$	$\rho \in \mathscr{S}(\mathsf{A})$	$\sigma \in \mathscr{S}(\hat{\mathsf{A}})$
$\texttt{Eval}$	$\mathcal{F} \in \mathscr{F}$, $\sigma \in \mathscr{S}(\hat{\mathsf{A}})$	$\theta \in \mathscr{S}(\hat{\mathsf{O}})$
$\hat{\mathcal{F}}$	$\sigma \in \mathscr{S}(\hat{\mathsf{A}})$	$\theta \in \mathscr{S}(\hat{\mathsf{O}})$
$\texttt{Dec}$	$k \in \{0,1\}^L$, $\theta \in \mathscr{S}(\hat{\mathsf{O}})$	$\tau \in \mathscr{S}(\mathsf{O})$
$\texttt{Dec}_k$	$\theta \in \mathscr{S}(\hat{\mathsf{O}})$	$\tau \in \mathscr{S}(\mathsf{O})$

Table 2: channels in the quantum homomorphic encryption protocol

Quantum homomorphic encryption needs to protect an honest Alice's data when a malicious Bob strives to learn it, as is shown in Figure 2. A quantum homomorphic encryption protocol is data private if a malicious Bob cannot distinguish different inputs of an honest Alice. The trace distance between encrypted states describes their indistinguishability.

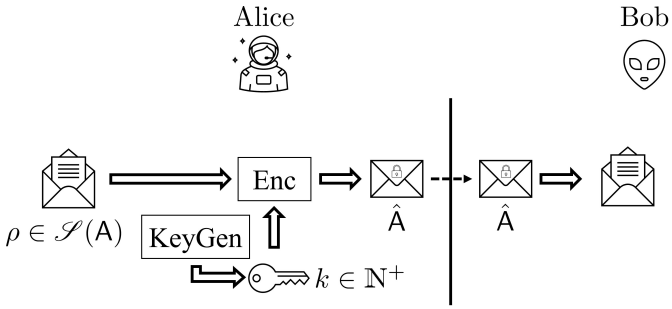


Figure 2: An honest Alice and malicious Bob in quantum homomorphic encryption

Definition 3 (Information-theoretic data privacy of quantum homomorphic encryption)**.** *A quantum homomorphic encryption protocol* $(\mathscr{F}, \texttt{KeyGen}, \texttt{Enc}, \texttt{Eval}, \texttt{Dec})$ *is* ϵ_d*-data private if for any two Alice's inputs* $\rho \in \mathscr{S}(\mathsf{A})$ *and* $\rho' \in \mathscr{S}(\mathsf{A})$*, the trace distance between the averages of Alice messages* $\mathbb{E}(\texttt{Enc}_k[\rho])$ *and* $\mathbb{E}(\texttt{Enc}_k[\rho'])$ *over the distribution over keys* $k \in \{0,1\}^L$ *is bounded by* ϵ_d

$$\Delta(\mathbb{E}(\texttt{Enc}_k[\rho]), \mathbb{E}(\texttt{Enc}_k[\rho'])) \leq \epsilon_d, \tag{3}$$

Specifically when $\epsilon_d = 0$*, we say that the protocol is perfectly data private.*

Quantum homomorphic encryption needs to protect an honest Bob's circuit when a malicious Alice strives to learn Bob's circuit more than what an honest Alice's output indicates, as is shown in Figure 3. However, even an honest Alice can learn some information about Bob's circuit. Therefore, we identify the information indicated by an honest Alice's output with an ideal protocol in Figure 4. In the ideal protocol, we imagine a trusted Charlie. Alice sends the input, and Bob sends the channel to Charlie. Charlie applies Bob's channel to Alice's input and sends the output to Alice. Alice ought to learn no more information in the actual protocol than what Alice can learn in the ideal protocol in a circuit private protocol. This circuit private case happens if a channel can turn Alice's output in the ideal protocol into Alice's output in the actual protocol. The trace distance between the two states can quantify the channel's performance.

Now we describe the actual protocol and the ideal protocol in detail. In the actual protocol, Alice sends her message $\sigma \in \mathscr{S}(\hat{\mathsf{A}})$ (whose purification is $|\psi\rangle \in \hat{\mathsf{A}}\mathsf{R}_{\hat{\mathsf{A}}}$) to Bob. Bob

applies $\hat{\mathcal{F}} \in \hat{\mathscr{F}}$ on σ according to Bob's channel $\mathcal{F}$, and sends Bob's message $\hat{\mathcal{F}}(\sigma) \in \mathscr{S}(\hat{\mathsf{O}})$ to Alice. Alice finally possesses the joint state $\hat{\mathcal{F}}[|\psi\rangle\langle\psi|] \in \mathscr{S}(\hat{\mathsf{O}}\mathsf{R}_{\hat{\mathsf{A}}})$ of Bob's message and Alice's referencing system.

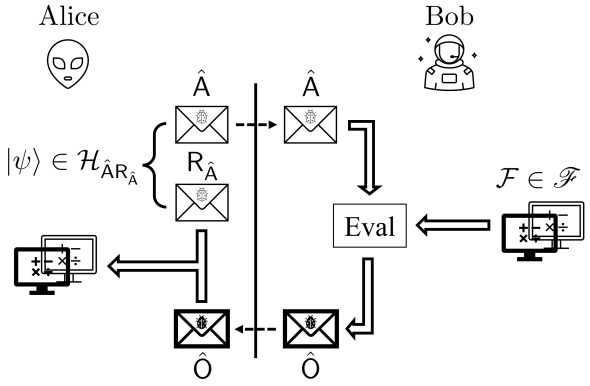


Figure 3: The actual protocol with a malicious Alice and an honest Bob

In the ideal protocol, Alice sends Alice's input $\rho' \in \mathscr{S}(\mathsf{A})$ (whose purification is $|\psi'\rangle \in \mathsf{A}\mathsf{R}_{\mathsf{A}}$) and Bob sends Bob's channel $\mathcal{F} \in \mathscr{F}$ to Charlie. Charlie applies $\mathcal{F}$ on ρ' according to Bob's channel $\mathcal{F}$ and sends Charlie's message $\mathcal{F}(\rho') \in \mathscr{S}(\mathsf{O})$ to Alice. Alice finally possesses the joint state $\mathcal{F}(|\psi'\rangle\langle\psi'|) \in \mathscr{S}(\mathsf{O}\mathsf{R}_{\mathsf{A}})$ of Charlie's message and Alice's referencing system. Alice further applies a post-processing channel $\mathcal{N} \in \mathrm{CPTP}(\mathsf{O}\mathsf{R}_{\mathsf{A}}, \hat{\mathsf{O}}\mathsf{R}_{\hat{\mathsf{A}}})$ on $\mathcal{F}(|\psi'\rangle\langle\psi'|)$ and obtains Alice's output $\mathcal{N}(\mathcal{F}(|\psi'\rangle\langle\psi'|)) \in \mathscr{S}(\hat{\mathsf{O}}\mathsf{R}_{\hat{\mathsf{A}}})$.

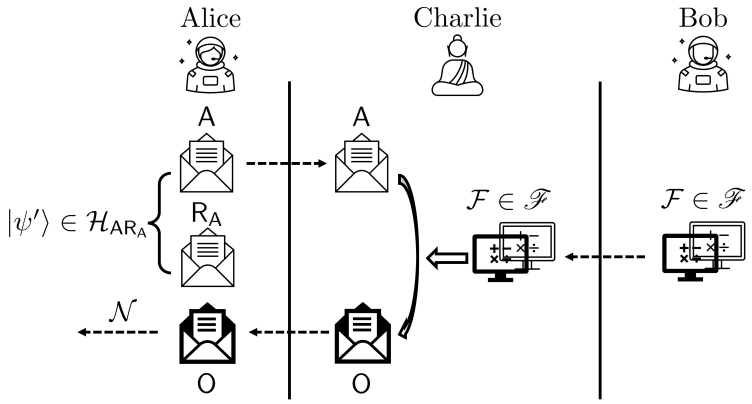


Figure 4: The ideal protocol with a trusted Charlie

Definition 4 (Information-theoretic circuit privacy of quantum homomorphic encryption)**.** *A quantum homomorphic encryption protocol* $(\mathscr{F}, \mathtt{KeyGen}, \mathtt{Enc}, \mathtt{Eval}, \mathtt{Dec})$ *is* ϵ_c*-circuit private if for any purification of Alice's message* $|\psi\rangle \in \hat{\mathsf{A}}\mathsf{R}_{\hat{\mathsf{A}}}$ *in the actual protocol, there exists a purification of Alice's input* $|\psi'\rangle \in \mathsf{A}\mathsf{R}_{\mathsf{A}}$ *and a post-processing channel* $\mathcal{N} \in \mathrm{CPTP}(\mathsf{O}\mathsf{R}_{\mathsf{A}}, \hat{\mathsf{O}}\mathsf{R}_{\hat{\mathsf{A}}})$ *in the ideal protocol such that for any* $\mathcal{F} \in \mathscr{F}$

$$\Delta\left((\hat{\mathcal{F}} \otimes \mathcal{I}_{\mathsf{R}_{\hat{\mathsf{A}}}})[|\psi\rangle\langle\psi|_{\hat{\mathsf{A}}\mathsf{R}_{\hat{\mathsf{A}}}}], \mathcal{N}\left((\mathcal{F} \otimes \mathcal{I}_{\mathsf{R}_{\mathsf{A}}})(|\psi'\rangle\langle\psi'|_{\mathsf{A}\mathsf{R}_{\mathsf{A}}})\right)\right) \leq \epsilon_c, \tag{4}$$

Specifically when $\epsilon_c = 0$*, we call that the protocol is perfectly circuit private.*

Our definition of circuit privacy is a good definition for the trivial protocol where Alice sends plaintexts to Bob. The trivial protocol where Alice sends plaintexts to Bob has no data privacy and perfect circuit privacy. We can write circuit privacy in terms of an optimization problem which is useful both theoretically and numerically.

Remark 5. *The circuit privacy can be written in the form of an optimization problem.*

$$\epsilon_c = \max_{|\psi\rangle\in\hat{A}\mathsf{R}_{\hat{A}}} \min_{\substack{|\psi'\rangle\in\mathsf{AR}_{\mathsf{A}} \\ \mathcal{N}\in\mathrm{CPTP}(\mathsf{OR}_{\hat{A}},\hat{\mathsf{O}}\mathsf{R}_{\hat{A}})}} \max_{\mathcal{F}\in\mathscr{F}} \Delta\left((\hat{\mathcal{F}}\otimes\mathcal{I}_{\mathsf{R}_{\hat{A}}})[|\psi\rangle\langle\psi|_{\hat{A}\mathsf{R}_{\hat{A}}}], \mathcal{N}((\mathcal{F}\otimes\mathcal{I}_{\mathsf{R}_{\mathsf{A}}})(|\psi'\rangle\langle\psi'|_{\mathsf{AR}_{\mathsf{A}}}))\right). \tag{5}$$

2.4 Quantum oblivious transfer

Quantum oblivious transfer is a vital quantum cryptographic primitive. Following [26, 27, 28], we consider two types of quantum oblivious transfer protocols, namely standard oblivious transfer and semi-random oblivious transfer in our work which we define in Definition 6 and Definition 7, respectively. In Theorem 8, we prove that standard oblivious transfer and semi-random oblivious transfer are equivalent by constructing reductions between them in both directions.

In standard oblivious transfer, Bob possesses two data bits, and Alice interacts with Bob to learn one specific data bit, as shown in Figure 5. Furthermore, Alice does not want Bob to know which data bit Alice desires. Bob does not want Alice to know both data bits. Next, we define standard oblivious transfer with δ-completeness and soundness against a cheating Alice or Bob following Ref. [26, Definition 6].

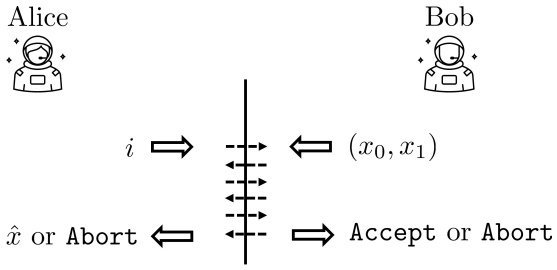


Figure 5: Standard oblivious transfer. Alice inputs i and Bob inputs (x_0, x_1). Then Alice and Bob perform rounds of communication. Alice outputs $\hat{x}$ or `Abort` and Bob outputs `Accept` or `Abort`.

Definition 6 (Standard oblivious transfer)**.** *A standard oblivious transfer protocol with δ-completeness, $P_A^\star$-soundness against a cheating Alice and $P_B^\star$-soundness against a cheating Bob is a two-party protocol where Alice begins with $i \in \{0,1\}$ and Bob begins with $(x_0, x_1) \in \{0,1\}^2$, and Alice ends with $\mathrm{output}_A \in \{0,1\} \cup \{\texttt{Abort}\}$, and Bob ends with $\mathrm{output}_B \in \{\texttt{Accept}, \texttt{Abort}\}$. If Alice does not output `Abort`, we say that Alice accepts and outputs $\hat{x} \in \{0,1\}$.*

$$\begin{array}{rccc} \mathrm{StandardOT}: & \mathrm{Alice}\times\mathrm{Bob} & \to & \mathrm{Alice}\times\mathrm{Bob} \\ & \{0,1\}\times\{0,1\}^2 & \to & \{0,1\}\cup\{\texttt{Abort}\}\times\{\texttt{Accept},\texttt{Abort}\}\ . \\ & i\times(x_0,x_1) & \mapsto & \mathrm{output}_A\times\mathrm{output}_B \end{array} \tag{6}$$

The following properties should be satisfied

- *Completeness: If Alice and Bob are both honest, then both parties accept, and with a probability of at least $1-\delta$, $\hat{x} = x_i$. That is, when both are honest,*

$$\Pr[(\text{Both accept})] = 1, \tag{7}$$

and

$$\Pr[(\hat{x} = x_i)] \geq 1 - \delta. \tag{8}$$

Note that the above equations should hold for any choice (x_0, x_1).

- *Soundness against a cheating Alice: Suppose that Bob's (x_0, x_1) is uniformly random. With a probability of at most $P_A^\star$, a cheating Alice can guess $(\hat{x}_0, \hat{x}_1)$ for an honest Bob's (x_0, x_1) correctly and Bob accepts. That is, when only Bob is honest,*

$$\Pr[((\hat{x}_0, \hat{x}_1) = (x_0, x_1)) \wedge (\text{Bob accepts})] \leq P_A^\star. \tag{9}$$

- *Soundness against a cheating Bob: Suppose that Alice's i is uniformly random. With a probability of at most $P_B^\star$, a cheating Bob can guess $\hat{i}$ for an honest Alice's i correctly and Alice accepts. That is, when only Alice is honest,*

$$\Pr[(\hat{i} = i) \wedge (\text{Alice accepts})] \leq P_B^\star. \tag{10}$$

In semi-random oblivious transfer, Bob possesses two data bits, and Alice interacts with Bob to learn one data bit uniformly at random and the index of the data bit, as is shown in Figure 6. Furthermore, Alice does not want Bob to know the index of the data bit. Bob does not want Alice to know both data bits. We formally define semi-random oblivious transfer with δ-completeness by extending [28, Definition 2].

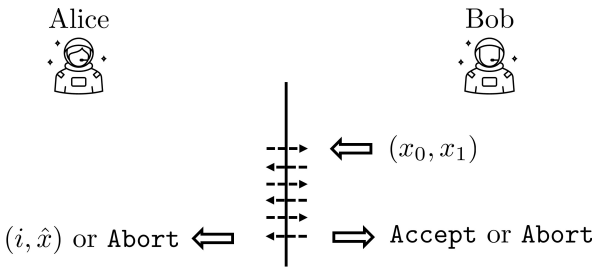


Figure 6: Semi-random oblivious transfer. Bob inputs (x_0, x_1). Then Alice and Bob perform rounds of communication. Alice outputs $(i, \hat{x})$ or `Abort` and Bob outputs `Accept` or `Abort`.

Definition 7 (Semi-random oblivious transfer)**.** *A semi-random oblivious transfer protocol is a two-party protocol where Bob begins with $(x_0, x_1) \in \{0,1\}^2$, Alice ends with $\text{output}_A \in \{0,1\}^2 \cup \{\texttt{Abort}\}$, and Bob ends with $\text{output}_B \in \{\texttt{Accept}, \texttt{Abort}\}$. If Alice does not output `Abort`, we say that Alice accepts and outputs $(i, \hat{x}) \in \{0,1\}^2$.*

$$\begin{array}{rccc} \text{SemirandomOT}: & \text{Bob} & \to & \text{Alice} \times \text{Bob} \\ & \{0,1\}^2 & \to & \{0,1\}^2 \cup \{\texttt{Abort}\} \times \{\texttt{Accept}, \texttt{Abort}\} \\ & (x_0, x_1) & \mapsto & \text{output}_A \times \text{output}_B \end{array}, \tag{11}$$

The protocol has δ-completeness, $P_A^\star$-soundness against a cheating Alice and $P_B^\star$-soundness against a cheating Bob if the following holds.

- *Completeness: If Alice and Bob are both honest, then both parties accept, i is uniformly random and with a probability of at least $1 - \delta$, $\hat{x} = x_i$. That is, when both parties are honest,*

$$\Pr[(\text{Both accept})] = 1, \tag{12}$$

$$\Pr[(i = 0)] = \Pr[(i = 1)] = \frac{1}{2}, \tag{13}$$

and

$$\Pr[(\hat{x} = x_i)] \geq 1 - \delta. \tag{14}$$

Note again that above equations should hold for any (x_0, x_1).

- *Soundness against a cheating Alice: Suppose that Bob's (x_0, x_1) is uniformly random. With a probability of at most $P_A^\star$, a cheating Alice can guess $(\hat{x}_0, \hat{x}_1)$ for an honest Bob's (x_0, x_1) correctly and Bob accepts. That is, when only Bob is honest,*

$$\Pr[((\hat{x}_0, \hat{x}_1) = (x_0, x_1)) \wedge (\text{Bob accepts})] \leq P_A^\star. \tag{15}$$

- *Soundness against a cheating Bob: With a probability of at most $P_B^\star$, a cheating Bob can guess $\hat{i}$ for an honest Alice's i correctly and Alice accepts. That is, when only Alice is honest,*

$$\Pr[(\hat{i} = i) \wedge (\text{Alice accepts})] \leq P_B^\star. \tag{16}$$

Following the same technique in [26, Proposition 9,10] and [28, Proposition 1], we prove that standard oblivious transfer is equivalent to semi-random oblivious transfer in Theorem 8.

Theorem 8. *A standard oblivious transfer protocol with δ-completeness, $P_A^\star$-soundness against a cheating Alice and $P_B^\star$-soundness against a cheating Bob is equivalent to a semi-random oblivious transfer protocol with δ-completeness, $P_A^\star$-soundness against a cheating Alice and $P_B^\star$-soundness against a cheating Bob.*

The proof works by constructing reductions between semi-random and standard oblivious transfer. We can easily reduce semi-random oblivious transfer to standard oblivious transfer. A semi-random oblivious transfer protocol can be viewed as Alice chooses the index of the data bit Alice wants to learn and performs a standard oblivious transfer protocol with Bob. It is trickier to reduce standard oblivious transfer to semi-random oblivious transfer. A semi-random oblivious transfer protocol can work as a subprotocol to generate keys in a standard oblivious transfer protocol. Initially, Bob holds two keys. After a semi-random oblivious transfer protocol, Alice learns one key uniformly at random and the key index, while Bob does not know the index of the key. Alice can then encrypt Alice's request with the key index, and Bob can encrypt Bob's two data bits with two keys. In this way, Alice can only decrypt one data bit, and Bob cannot decrypt Alice's request. We provide the detailed proof in Appendix A.

3 Bounds for quantum oblivious transfer

In this section, we extend the bound for quantum oblivious transfer in [28, Eq. (27)] to δ-correctness with the same technique. We first describe the general scheme of semi-random oblivious transfer and then bound Alice's and Bob's cheating probabilities by proposing their cheating strategies.

The general scheme of semi-random oblivious transfer with N rounds of communication [28, Section IIIA] is illustrated in Figure 7. Alice and Bob keep their memories private and exchange their messages publicly. Each time either Alice or Bob receives the message, they apply a unitary that acts jointly on the memory and the message. In the last step, they measure their state to obtain their output. Any semi-random oblivious transfer can be described by such a general scheme.

Protocol 1 formally describes the general scheme depicted in Figure 7. Alice begins with the state $|\psi\rangle \in \mathsf{R_A A}$, where $\mathsf{R_A}$ is Alice's referencing system and A is Alice's message. Bob begins with the state $|0\rangle \in \mathsf{R_B}$ and the data bits $(x_0, x_1) \in \{0,1\}^2$, where $\mathsf{R_B}$ is Bob's referencing system. The joint state of Alice and Bob is $|\psi\rangle|0\rangle|x_0, x_1\rangle \in \mathsf{AR_A BR_B}$.

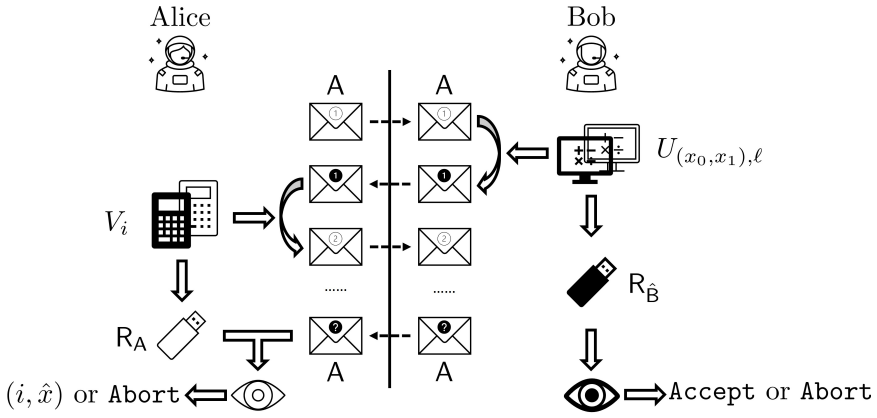


Figure 7: The scheme of quantum oblivious transfer.

Bob prepares the program $|x_0, x_1\rangle \in \mathsf{B}$. Then Alice and Bob repeat N rounds of communication: Alice sends A to Bob; Bob applies a unitary $U_{(x_0,x_1),\ell} \in \mathrm{U}(\mathsf{AR_B})$ that acts trivially on $\mathsf{R_A}$ and depends on (x_0, x_1); Bob sends A back to Alice; Alice applies a unitary $V_\ell \in \mathrm{U}(\mathsf{AR_A})$ that acts trivially on $\mathsf{R_B}$. After N iterations, Alice and Bob's joint state is $|\psi^{(x_0,x_1)}\rangle = V_N U_{(x_0,x_1),N} ... V_1 U_{(x_0,x_1),1} |\psi\rangle \in \mathscr{S}(\mathsf{AR_A R_B})$. Alice's final state is $\sigma_{(x_0,x_1)} = \mathrm{Tr}_{\mathsf{R_B}}(|\psi^{(x_0,x_1)}\rangle\langle\psi^{(x_0,x_1)}|) \in \mathscr{S}(\mathsf{AR_A})$. We denote the maximum fidelity between distinct pairs of Alice's final states by f, i.e.

$$f = \max\left\{F(\sigma_{(x_0,x_1)}, \sigma_{(x_0',x_1')}), (x_0, x_1) \neq (x_0', x_1')\right\}. \tag{17}$$

Alice measures a projective measurement $\{\Pi_{\text{Alice}}^{\texttt{Accept}}, \Pi_{\text{Alice}}^{\texttt{Abort}}\}$ on $\mathsf{AR_A}$ to determine if Alice accepts, where $\Pi_{\text{Alice}}^{\texttt{Accept}}$ is the projector onto Alice's accepting subspace while $\Pi_{\text{Alice}}^{\texttt{Abort}}$ is the projector onto Alice aborting subspace. Similarly, Bob measures $\{\Pi_{\text{Bob}}^{\texttt{Accept}}, \Pi_{\text{Bob}}^{\texttt{Abort}}\}$ on $\mathsf{R_B}$ to determine if Bob accepts, where $\Pi_{\text{Bob}}^{\texttt{Accept}}$ is the projector onto Bob's accepting subspace while $\Pi_{\text{Bob}}^{\texttt{Abort}}$ is the projector onto Bob aborting subspace. If both accept, Alice performs a positive operator valued measure $\{N_{(i,\hat{x})} = E_{(i,\hat{x})}^\dagger E_{(i,\hat{x})}\}_{i,\hat{x}\in\{0,1\}}$ on $\mathsf{R_A}$, where $E_{(i,\hat{x})}$ relates the post-measurement state to the pre-measurement state. Alice's output is the measurement outcome $(i, \hat{x})$.

Applying a similar method as in [28, Section IIIB,C,D], we can obtain a bound for the semi-random oblivious transfer protocol.

Theorem 9. *Any semi-random oblivious transfer protocol and any standard oblivious transfer protocol with δ-completeness, $P_A^\star$-soundness against a cheating Alice and $P_B^\star$-soundness against a cheating Bob satisfies*

$$P_A^\star + 2P_B^\star + 4\sqrt{\delta} \geq 2. \tag{18}$$

In order to show a violation of soundness, it suffices to exhibit a specific cheating strategy. Therefore, we will only deal with certain strategies of cheating Alice and Bob in the proof. Alice's cheating strategy involves performing a pretty-good measurement in the last step to try to learn Bob's input. Bob can input a well-chosen superposition at the beginning and measure at the end to try to learn Alice's input.

Proof. Here we prove a bound for semi-random oblivious transfer, and due to the equivalence between semi-random oblivious transfer and standard oblivious transfer in Theorem 8, the same bound applies to standard oblivious transfer. Consider a semi-random

Protocol 1 Scheme of semi-random oblivious transfer with N rounds of communication

Input: $(x_0, x_1) \in \{0,1\}^2$. ▷ Bob's input

Output: $\text{output}_A \in \{0,1\}^2 \cup \{\texttt{Abort}\}$, $\text{output}_B \in \{\texttt{Accept}, \texttt{Abort}\}$. ▷ Alice's and Bob's outputs

1: Alice: Prepare $|\psi\rangle \in \mathsf{R_A A}$
2: Bob: Prepare $|0\rangle \in \mathsf{R_B}$.
3: **for** $\ell = 1$ to $\ell = N$ **do** ▷ Alice and Bob performs N rounds of communication.
4: Alice: Send A to Bob.
5: Bob: Perform $U_{(x_0,x_1),\ell} \in \mathrm{U}(\mathsf{AR_B})$.
6: Bob: Send A back to Alice.
7: Alice: Perform $V_\ell \in \mathrm{U}(\mathsf{AR_A})$.
8: **end for**
9: Alice: Measure $\{\Pi_{\text{Alice}}^{\texttt{Accept}}, \Pi_{\text{Alice}}^{\texttt{Abort}}\}$ on $\mathsf{AR_A}$ with outcome A. ▷ Alice measures to determine whether to accept.
10: Bob: Measure $\{\Pi_{\text{Bob}}^{\texttt{Accept}}, \Pi_{\text{Bob}}^{\texttt{Abort}}\}$ on $\mathsf{R_B}$ with outcome B. ▷ Bob measures to determine whether to accept.
11: Bob: $\text{output}_B \leftarrow B$.
12: **if** $A = \texttt{Abort}$ **then**
13: Alice: $\text{output}_A \leftarrow \texttt{Abort}$.
14: **else**
15: Alice: Measure $\{N_{(i,\hat{x})}\}_{i,\hat{x}\in\{0,1\}}$ on $\mathsf{AR_A}$ with outcome $(i,\hat{x})$. ▷ Alice measures to determine $(i,\hat{x})$.
16: Alice: $\text{output}_A \leftarrow (i,\hat{x})$.
17: **end if**

oblivious transfer protocol with δ-completeness described by Protocol 1. The positive operator valued measure $\{N_{(i,\hat{x})}\}_{i,\hat{x}\in\{0,1\}}$ must satisfy

$$\Pr[(\text{Alice output } (i,\hat{x}))|\text{Bob input } (x_0,x_1)] = \mathrm{Tr}(N_{(i,\hat{x})}\sigma_{(x_0,x_1)}) = \begin{cases} \frac{1-\theta_{i,(x_0,x_1)}}{2} & \hat{x} = x_i \\ \frac{\theta_{i,(x_0,x_1)}}{2} & \hat{x} \neq x_i \end{cases}. \tag{19}$$

where $\theta_{i,(x_0,x_1)}$ is the error probability that depends on i and (x_0,x_1). In order to satisfy the δ-completeness of standard oblivious transfer, $\theta_{i,(x_0,x_1)}$ must satisfy for any (x_0,x_1)

$$0 \leq \sum_{i\in\{0,1\}} \theta_{i,(x_0,x_1)} \leq 2\delta. \tag{20}$$

We first discuss the soundness against Alice. Suppose that Alice is malicious and Bob is honest. Alice can follow Protocol 1 through Step 14 while performing the pretty good measurement $\{N^{\mathrm{PGM}}_{(\hat{x}_0,\hat{x}_1)} = S^{-\frac{1}{2}}\sigma_{(\hat{x}_0,\hat{x}_1)}S^{-\frac{1}{2}}\}_{\hat{x}_0,\hat{x}_1\in\{0,1\}}$ where $S = \sum_{x_0,x_1\in\{0,1\}}\sigma_{(x_0,x_1)}$ instead of the required measurement $\{N_{(i,\hat{x})}\}_{i,\hat{x}\in\{0,1\}}$ in Step 15 and guess $(\hat{x}_0,\hat{x}_1)$ for (x_0,x_1). A cheating Alice will not be caught by an honest Bob since Alice follows the protocol until Bob accepts. If (x_0,x_1) is uniformly random, then the probability that Alice can guess correctly is bounded in [29, Theorem 3.1], and satisfies the inequality

$$\Pr[(\hat{x}_0,\hat{x}_1) = (x_0,x_1)] \geq 1 - \frac{1}{8}\sum_{\substack{x_0,x_1,x_0',x_1'\in\{0,1\} \\ (x_0,x_1)\neq(x_0',x_1')}} F(\sigma_{(x_0,x_1)},\sigma_{(x_0',x_1')}). \tag{21}$$

As shown in Eq. (19), the required measurement $\{N_{(i,\hat{x})}\}_{i,\hat{x}\in\{0,1\}}$ distinguishes $\sigma_{(x_0,x_1)}$ and $\sigma_{(\overline{x}_0,\overline{x}_1)}$ with a probability of at least $1-\delta$. Therefore, the Holevo-Helstrom theorem [30, 31] (see [32, Theorem 3.4] for a modern version) implies that

$$\frac{1}{2}(1+\Delta(\sigma_{(x_0,x_1)},\sigma_{(\overline{x}_0,\overline{x}_1)}))\geq 1-\delta. \tag{22}$$

Applying the Fuchs-van de Graaf inequality in [33, Theorem 1]

$$\Delta(\sigma_{(x_0,x_1)},\sigma_{(\overline{x}_0,\overline{x}_1)})\leq\sqrt{1-F(\sigma_{(x_0,x_1)},\sigma_{(\overline{x}_0,\overline{x}_1)})^2}, \tag{23}$$

we obtain

$$F(\sigma_{(x_0,x_1)},\sigma_{(\overline{x}_0,\overline{x}_1)})\leq 2\sqrt{\delta(1-\delta)}. \tag{24}$$

Recall the maximum fidelity f defined in (17). By reordering terms in Eq. (21), we obtain

$$\begin{aligned}\Pr[(\hat{x}_0,\hat{x}_1)=(x_0,x_1)]\geq 1&-\frac{1}{8}\sum_{\substack{x_0,x_1,x_0',x_1'\in\{0,1\}\\(\overline{x}_0,\overline{x}_1)=(x_0',x_1')}}F(\sigma_{(x_0,x_1)},\sigma_{(x_0',x_1')})\\&-\frac{1}{8}\sum_{\substack{x_0,x_1,x_0',x_1'\in\{0,1\}\\(x_0,x_1)\neq(x_0',x_1')\\(\overline{x}_0,\overline{x}_1)\neq(x_0',x_1')}}F(\sigma_{(x_0,x_1)},\sigma_{(x_0',x_1')}).\end{aligned} \tag{25}$$

Applying Eq. (24), we obtain

$$\Pr[(\hat{x}_0,\hat{x}_1)=(x_0,x_1)]\geq 1-f-\sqrt{\delta(1-\delta)}. \tag{26}$$

Therefore, a cheating Alice can guess an honest Bob's (x_0,x_1) and both parties accept with a probability of at least $1-f-\sqrt{\delta(1-\delta)}$, and thus

$$P_A^\star\geq 1-f-\sqrt{\delta(1-\delta)}. \tag{27}$$

Second we discuss the soundness against Bob. Suppose that Alice is honest and Bob is malicious. Let (x_0,x_1) and (x_0',x_1') be the two data bit strings corresponding to the maximum fidelity f defined in (17), i.e. $f=F(\sigma_{(x_0,x_1)},\sigma_{(x_0',x_1')})$. There is at least one different bit between (x_0,x_1) and (x_0',x_1'). Let us assume that $x_1=0$ and $x_1'=1$, and other cases follow analogously. According to Uhlmann's theorem [34] (or see a textbook e.g. [32, Theorem 3.22]), we can find a purification $|\phi^{(x_0,0)}\rangle\in\mathsf{AR_AR_B}$ of $\sigma_{(x_0,0)}$ and a purification $|\phi^{(x_0',1)}\rangle\in\mathsf{AR_AR_B}$ of $\sigma_{(x_0',1)}$ such that $f=|\langle\phi^{(x_0',1)}|\phi^{(x_0,0)}\rangle|$. Due to the unitary equivalence of purifications [32, Theorem 2.12], Bob can perform local unitaries $U_{(x_0,0)}\in\mathrm{U}(\mathsf{R_B})$ and $U_{(x_0',1)}\in\mathrm{U}(\mathsf{R_B})$ such that $|\phi^{(x_0,0)}\rangle=U_{(x_0,0)}|\psi^{(x_0,0)}\rangle$ and $|\phi^{(x_0',1)}\rangle=U_{(x_0',1)}|\psi^{(x_0',1)}\rangle$.

Based on the above facts, Bob can cheat by considering the two inputs $(x_0,0)$ and $(x_0',1)$, preparing the program in superposition and otherwise honestly following the protocol, and making a measurement on his state in the end to try to learn Alice's input. More precisely, instead of following Protocol 1, Bob will prepare the superposition $|(x_0,0)\rangle+|(x_0',1)\rangle\in\mathsf{B}$ and apply the controlled unitary $\sum_{x_0'',x_1''\in\{0,1\}}U_{(x_0'',x_1''),\ell}\otimes|x_0'',x_1''\rangle\langle x_0'',x_1''|_{\mathsf{B}}\in\mathrm{U}(\mathsf{ABR_B})$ in Step 5 of each round of communication. Before Step 9, the joint state of both parties is the superposition $|\psi^{(x_0,0)}\rangle|x_0,0\rangle+|\psi^{(x_0',1)}\rangle|x_0',1\rangle$. A cheating Bob will not be caught by an honest Alice because $\Pi_{\text{Alice}}^{\texttt{Accept}}|\psi^{(x_0,0)}\rangle=|\psi^{(x_0,0)}\rangle$ and $\Pi_{\text{Alice}}^{\texttt{Accept}}|\psi^{(x_0',1)}\rangle=|\psi^{(x_0',1)}\rangle$, hence $\Pi_{\text{Alice}}^{\texttt{Accept}}\left(|\psi^{(x_0,0)}\rangle|x_0,0\rangle+|\psi^{(x_0',1)}\rangle|x_0',1\rangle\right)=|\psi^{(x_0,0)}\rangle|x_0,0\rangle+|\psi^{(x_0',1)}\rangle|x_0',1\rangle$.

After Step 15, Bob wants to learn i. This can be done by a unitary $U_{(x_0,0)} \otimes |x_0,0\rangle\langle x_0,0|_{\mathsf{B}} + U_{(x'_0,1)} \otimes |x'_0,1\rangle\langle x'_0,1|_{\mathsf{B}} + \mathbb{I}_{\mathsf{R_B}} \otimes (\mathbb{I}_{\mathsf{B}} - |x_0,0\rangle\langle x_0,0|_{\mathsf{B}} - |x'_0,1\rangle\langle x'_0,1|_{\mathsf{B}}) \in \mathrm{U}(\mathsf{BR_B})$ followed by a measurement $\{N^{\mathrm{OPT}}_{\hat{i}}\}_{\hat{i}\in\{0,1\}}$ on B. This can bound the probability that the estimate $\hat{i}$ is equal to i. The joint state of Alice and Bob $|\Phi\rangle \in \mathsf{AR_ABR_BE}$ before Alice and Bob measure in Step 15 is

$$|\Phi\rangle = \frac{1}{\sqrt{2}} \left(|\phi^{(x_0,0)}\rangle |x_0,0\rangle + |\phi^{(x'_0,1)}\rangle |x'_0,1\rangle \right). \tag{28}$$

The reduced density matrix $\rho_{\mathsf{B}} \in \mathscr{S}(\mathsf{B})$ is

$$\rho_{\mathsf{B}} = \frac{1}{2} \left(|x_0,0\rangle\langle x_0,0|_{\mathsf{B}} + |x'_0,1\rangle\langle x'_0,1|_{\mathsf{B}} \right) + \frac{1}{2} \left(\langle \phi^{(x'_0,1)} | \phi^{(x_0,0)} \rangle |x_0,0\rangle\langle x'_0,1|_{\mathsf{B}} + \text{h.c.} \right). \tag{29}$$

where h.c. stands for the Hermitian conjugate of the previous term. After Alice performs the required measurement $\{N_{i,\hat{x}}\}_{i,\hat{x}\in\{0,1\}}$ on $\mathsf{AR_A}$ to obtain $(i,\hat{x})$ in Step 15, the post-measurement reduced density matrices $\rho^{(i)}_{\mathsf{B}} \in \mathscr{S}(\mathsf{B})$ given i is

$$\rho^{(i)}_{\mathsf{B}} = \sum_{\hat{x}\in\{0,1\}} \mathrm{Tr}_{\mathsf{AR_AR_B}} (E_{(i,\hat{x})} |\Phi\rangle\langle\Phi| E^{\dagger}_{(i,\hat{x})}), \tag{30}$$

or more explicitly

$$\begin{aligned} \rho^{(i)}_{\mathsf{B}} = {} & \frac{1}{2} \left(|x_0,0\rangle\langle x_0,0|_{\mathsf{B}} + |x'_0,1\rangle\langle x'_0,1|_{\mathsf{B}} \right) \\ & + \sum_{\hat{x}\in\{0,1\}} \left(\langle \phi^{(x'_0,1)} | N_{(i,\hat{x})} | \phi^{(0,0)} \rangle |(x_0,0)\rangle\langle(x'_0,1)|_{\mathsf{B}} + \text{h.c.} \right). \end{aligned} \tag{31}$$

The difference between $\rho^{(0)}_{\mathsf{B}}$ and $\rho^{(1)}_{\mathsf{B}}$ is

$$\rho^{(0)}_{\mathsf{B}} - \rho^{(1)}_{\mathsf{B}} = \begin{pmatrix} 0 & \sum_{\hat{x}\in\{0,1\}} \langle \phi^{(x'_0,1)} | N_{(0,\hat{x})} - N_{(1,\hat{x})} | \phi^{(x_0,0)} \rangle \\ \sum_{\hat{x}\in\{0,1\}} \langle \phi^{(x_0,0)} | N_{(0,\hat{x})} - N_{(1,\hat{x})} | \phi^{(x'_0,1)} \rangle & 0 \end{pmatrix}. \tag{32}$$

The trace norm of a two-dimensional Hermitian matrix with only off-diagonal elements is just the absolute value of its off-diagonal elements. Hence we obtain

$$\Delta(\rho^{(0)}_{\mathsf{B}}, \rho^{(1)}_{\mathsf{B}}) = \left| \sum_{\hat{x}\in\{0,1\}} \langle \phi^{(x'_0,1)} | N_{(0,\hat{x})} | \phi^{(x_0,0)} \rangle - \sum_{\hat{x}\in\{0,1\}} \langle \phi^{(x'_0,1)} | N_{(1,\hat{x})} | \phi^{(x_0,0)} \rangle \right|. \tag{33}$$

Since $\sum_{i,\hat{x}\in\{0,1\}} N_{(i,\hat{x})} = \mathbb{I}_{\mathsf{AR_A}}$, we obtain

$$\Delta(\rho^{(0)}_{\mathsf{B}}, \rho^{(1)}_{\mathsf{B}}) = \left| \langle \phi^{(0,1)} | \phi^{(0,0)} \rangle - 2 \sum_{\hat{x}\in\{0,1\}} \langle \phi^{(0,1)} | N_{(1,\hat{x})} | \phi^{(0,0)} \rangle \right|. \tag{34}$$

Applying the reverse triangle inequality, we obtain

$$\Delta(\rho^{(0)}_{\mathsf{B}}, \rho^{(1)}_{\mathsf{B}}) \geq \left| \langle \phi^{(x'_0,1)} | \phi^{(x_0,0)} \rangle \right| - 2 \sum_{\hat{x}\in\{0,1\}} \left| \langle \phi^{(x'_0,1)} | N_{(1,\hat{x})} | \phi^{(x_0,0)} \rangle \right|. \tag{35}$$

Furthermore, applying the Cauchy-Schwarz inequality, we obtain

$$\left| \langle \phi^{(x'_0,1)} | N_{(1,\hat{x})} | \phi^{(x_0,0)} \rangle \right| \leq \sqrt{ \left| \langle \phi^{(x_0,0)} | N_{(1,\hat{x})} | \phi^{(x_0,0)} \rangle \right| \cdot \left| \langle \phi^{(x'_0,1)} | N_{(1,\hat{x})} | \phi^{(x'_0,1)} \rangle \right| } \leq \frac{\sqrt{2\delta}}{2}, \tag{36}$$

where the last inequality follows from Eq. (19). Substituting into Eq. (35), we find

$$\Delta(\rho_{\mathsf{B}}^{(0)}, \rho_{\mathsf{B}}^{(1)}) \geq f - 2\sqrt{2\delta}. \tag{37}$$

Therefore, we obtain $\Pr[\hat{i} = i] \geq \frac{1}{2}(1 + f - 2\sqrt{2\delta})$. Hence, a cheating Bob can guess an honest Alice's i and both parties accept with a probability of at least

$$P_B^\star \geq \frac{1}{2}(1 + f - 2\sqrt{2\delta}). \tag{38}$$

Combining Eq. (27) with Eq. (38) and eliminating F, we obtain a bound for semi-random oblivious transfer

$$P_A^\star + 2P_B^\star + \sqrt{\delta(1-\delta)} + 2\sqrt{2\delta} \geq 2. \tag{39}$$

By further using

$$\sqrt{\delta(1-\delta)} + 2\sqrt{2\delta} \leq 4\sqrt{\delta}, \tag{40}$$

we have

$$P_A^\star + 2P_B^\star + 4\sqrt{\delta} \geq 2. \tag{41}$$

□

4 Reduction from quantum oblivious transfer to quantum homomorphic encryption

In this section, we reduce quantum oblivious transfer to quantum homomorphic encryption. We construct a set of channels which can realize quantum oblivious transfer in Definition 10. We then use a quantum homomorphic encryption protocol with the set of channels as a black-box subprotocol to construct a quantum oblivious transfer protocol, as shown in Figure 8. Alice inputs the index of the data bit, Bob inputs two data bits to the black-box subprotocol, and the black-box subprotocol outputs the desired data bit to Alice. We complete the reduction by translating the correctness, data privacy and circuit privacy of quantum homomorphic encryption into the completeness, soundness against Bob and soundness against Alice of quantum oblivious transfer in Lemma 16, Lemma 17 and Lemma 20, respectively.

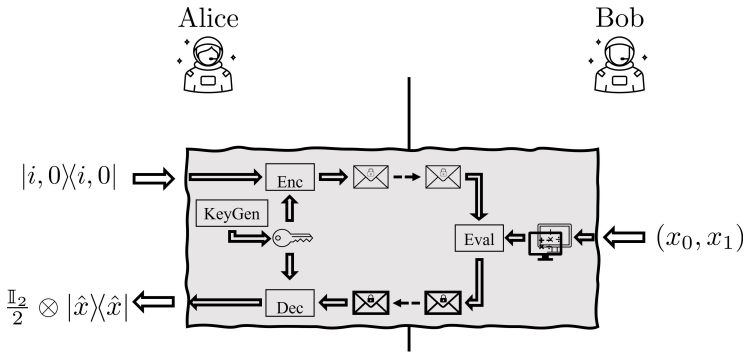


Figure 8: The reduction from quantum oblivious transfer to quantum homomorphic encryption

We now define the set of strong oblivious transfer channels. Roughly speaking, the set of strong oblivious transfer channels can realize standard oblivious transfer in a classical manner.

Definition 10 (Strong oblivious transfer channels)**.** *Strong oblivious transfer channels* $\mathcal{F}_{(x_0,x_1)} \in \mathrm{CPTP}(\mathsf{A},\mathsf{O})$*, where* $(x_0,x_1)\in\{0,1\}^2$*, can be compactly given by*

$$\mathcal{F}_{(x_0,x_1)}(\rho) = \sum_{i,i'\in\{0,1\}} \mathrm{Tr}\left(|i,i'\rangle\langle i,i'|_{\mathsf{A}}\rho\right)\frac{\mathbb{I}_2}{2}\otimes|x_{i\oplus i'}\oplus i'\rangle\langle x_{i\oplus i'}\oplus i'|_{\mathsf{O}_2}. \tag{42}$$

where O_2 *denotes the second qubit in the output.*

Remark 11. *Strong oblivious transfer channels* $\mathcal{F}_{(x_0,x_1)}$ *can be explicitly expressed as*

$$\mathcal{F}_{(0,0)}(\rho) = \frac{\mathbb{I}_2}{2}\otimes\left(\mathrm{Tr}\left(\mathbb{I}_2\otimes|0\rangle\langle 0|_{\mathsf{A}_2}\rho\right)|0\rangle\langle 0|_{\mathsf{O}_2} + \mathrm{Tr}\left(\mathbb{I}_2\otimes|1\rangle\langle 1|_{\mathsf{A}_2}\rho\right)|1\rangle\langle 1|_{\mathsf{O}_2}\right), \tag{43}$$

$$\mathcal{F}_{(0,1)}(\rho) = \frac{\mathbb{I}_2}{2}\otimes\left(\mathrm{Tr}\left(|0\rangle\langle 0|_{\mathsf{A}_1}\otimes\mathbb{I}_2\rho\right)|0\rangle\langle 0|_{\mathsf{O}_2} + \mathrm{Tr}\left(|1\rangle\langle 1|_{\mathsf{A}_1}\otimes\mathbb{I}_2\rho\right)|1\rangle\langle 1|_{\mathsf{O}_2}\right), \tag{44}$$

$$\mathcal{F}_{(1,0)}(\rho) = \frac{\mathbb{I}_2}{2}\otimes\left(\mathrm{Tr}\left(|0\rangle\langle 0|_{\mathsf{A}_1}\otimes\mathbb{I}_2\rho\right)|1\rangle\langle 1|_{\mathsf{O}_2} + \mathrm{Tr}\left(|1\rangle\langle 1|_{\mathsf{A}_1}\otimes\mathbb{I}_2\rho\right)|0\rangle\langle 0|_{\mathsf{O}_2}\right), \tag{45}$$

$$\mathcal{F}_{(1,1)}(\rho) = \frac{\mathbb{I}_2}{2}\otimes\left(\mathrm{Tr}\left(\mathbb{I}_2\otimes|0\rangle\langle 0|_{\mathsf{A}_2}\rho\right)|1\rangle\langle 1|_{\mathsf{O}_2} + \mathrm{Tr}\left(\mathbb{I}_2\otimes|1\rangle\langle 1|_{\mathsf{A}_2}\rho\right)|0\rangle\langle 0|_{\mathsf{O}_2}\right). \tag{46}$$

where A_1 *and* A_2 *denotes the first and second qubit in the input, respectively.*

Remark 12. *When* $\rho = |i,0\rangle\langle i,0|_{\mathsf{A}}$*, then* $\mathcal{F}_{(x_0,x_1)}$ *satisfies*

$$\mathcal{F}_{(x_0,x_1)}(\rho) = \frac{\mathbb{I}_2}{2}\otimes|x_i\rangle\langle x_i|_{\mathsf{O}_2} \tag{47}$$

or

$$\mathcal{F}_{(0,0)}(\rho) = \frac{\mathbb{I}_2}{2}\otimes|0\rangle\langle 0|_{\mathsf{O}_2}, \tag{48}$$

$$\mathcal{F}_{(0,1)}(\rho) = \frac{\mathbb{I}_2}{2}\otimes|i\rangle\langle i|_{\mathsf{O}_2}, \tag{49}$$

$$\mathcal{F}_{(1,0)}(\rho) = \frac{\mathbb{I}_2}{2}\otimes|\bar{i}\rangle\langle\bar{i}|_{\mathsf{O}_2}, \tag{50}$$

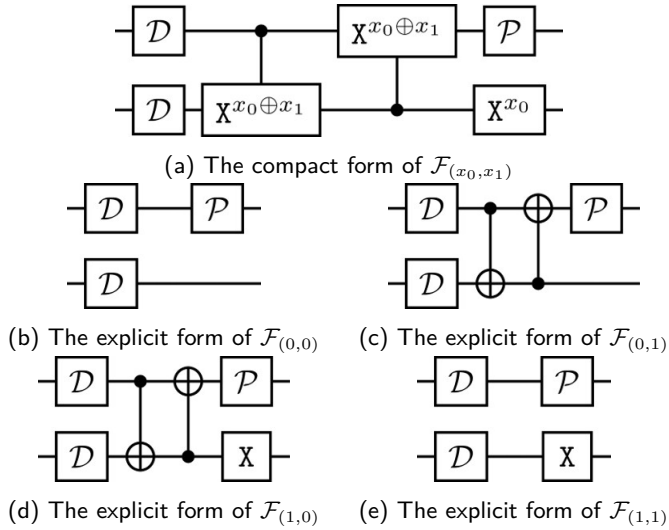
$$\mathcal{F}_{(1,1)}(\rho) = \frac{\mathbb{I}_2}{2}\otimes|1\rangle\langle 1|_{\mathsf{O}_2}. \tag{51}$$

We explicitly construct $\mathcal{F}_{(x_0,x_1)}$ with Cliffords $\mathtt{CL}$, completely dephasing channels $\mathcal{D}$ and completely depolarising channels $\mathcal{P}$ in Figure 9.

The completely dephasing channel $\mathcal{D}$ can further be constructed by applying $\mathbb{I}_2$ and $\mathtt{Z}$ uniformly at random. The completely depolarising channel $\mathcal{P}$ can be constructed by applying $\mathbb{I}_2$, $\mathtt{Z}$, $\mathtt{X}$ and $\mathtt{XZ}$ uniformly at random. That motivates us to define the set of strong oblivious transfer Cliffords. Equivalently, strong oblivious transfer Cliffords can realize strong oblivious transfer channels.

Definition 13 (Strong oblivious transfer Cliffords)**.** *Strong oblivious transfer Cliffords* $\mathcal{F}^{(r_0,r_1,r_2,r_3)}_{(x_0,x_1)} \in \mathtt{CL}$*, where* $(x_0,x_1,r_0,r_1,r_2,r_3)\in\{0,1\}^6$*, are given by circuits in Figure 10.*

Lemma 14. *A quantum homomorphic encryption protocol that allows to delegate* $\mathcal{F}^{(r_0,r_1,r_2,r_3)}_{(x_0,x_1)}$ *and with* ϵ*-correctness,* ϵ_d*-data privacy,* ϵ_c*-circuit privacy can simulate a quantum homomorphic encryption protocol that allows to delegate* $\mathcal{F}_{(x_0,x_1)}$ *with* ϵ*-correctness,* ϵ_d*-data privacy and* ϵ_c*-circuit privacy.*



(a) The compact form of $\mathcal{F}_{(x_0,x_1)}$

(b) The explicit form of $\mathcal{F}_{(0,0)}$ (c) The explicit form of $\mathcal{F}_{(0,1)}$

(d) The explicit form of $\mathcal{F}_{(1,0)}$ (e) The explicit form of $\mathcal{F}_{(1,1)}$

Figure 9: (a) The compact form of $\mathcal{F}_{(x_0,x_1)}$ and (b)–(e) the explicit form of $\mathcal{F}_{(0,0)}$, $\mathcal{F}_{(0,1)}$, $\mathcal{F}_{(1,0)}$, and $\mathcal{F}_{(1,1)}$ of strong oblivious transfer channels. We apply the two CNOT gates if and only if $x_0 \neq x_1$ and apply the X gate if and only if $x_0 = 1$ in both (a) and (b)–(e). Thus (a) is a compact form of (b)–(e).

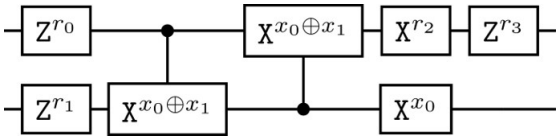


Figure 10: Strong oblivious transfer Cliffords $\mathcal{F}_{(x_0,x_1)}^{(r_0,r_1,r_2,r_3)}$.

Proof. Suppose that there is a quantum homomorphic encryption protocol Q that delegates $\mathcal{F}_{(x_0,x_1)}^{(r_0,r_1,r_2,r_3)}$ with ϵ-correctness, ϵ_d-data privacy, ϵ_c-circuit privacy. The quantum homomorphic encryption protocol Q' that delegates $\mathcal{F}_{(x_0,x_1)}$ can be constructed from Q as follows. The key generation, encryption and decryption maps of Q' are the same as that of Q'. The evaluation map of Q' requires further randomization, i.e. Bob fixes (x_0, x_1), generates (r_0, r_1, r_2, r_3) uniformly at random and evaluates $\mathcal{F}_{(x_0,x_1)}^{(r_0,r_1,r_2,r_3)}$. Namely,

$$\mathcal{F}_{(x_0,x_1)} = \frac{1}{16} \sum_{r_0,r_1,r_2,r_3\in\{0,1\}} \mathcal{F}_{(x_0,x_1)}^{(r_0,r_1,r_2,r_3)}, \tag{52}$$

and hence

$$\hat{\mathcal{F}}_{(x_0,x_1)} = \frac{1}{16} \sum_{r_0,r_1,r_2,r_3\in\{0,1\}} \hat{\mathcal{F}}_{(x_0,x_1)}^{(r_0,r_1,r_2,r_3)}. \tag{53}$$

The correctness of Q implies that for any $\mathcal{F}_{(x_0,x_1)}^{(r_0,r_1,r_2,r_3)}$, any $|\psi'\rangle \in \mathsf{AR_A}$ and any key $k = \mathtt{KeyGen}(\kappa)$

$$\epsilon \geq \Delta\left(\mathtt{Dec}_k \hat{\mathcal{F}}_{(x_0,x_1)}^{(r_0,r_1,r_2,r_3)} \mathtt{Enc}_k(|\psi'\rangle\langle\psi'|_{\mathsf{AR_A}}), \mathcal{F}_{(x_0,x_1)}^{(r_0,r_1,r_2,r_3)}(|\psi'\rangle\langle\psi'|_{\mathsf{AR_A}})\right). \tag{54}$$

Averaging over the uniform distribution of (r_0, r_1, r_2, r_3), applying the convexity of the trace distance in [35, Theorem 9.3] and substituting Eq. (52) and Eq. (53), we conclude that for any $\mathcal{F}_{(x_0,x_1)}$, any $|\psi'\rangle \in \mathsf{AR_A}$ and any key $k = \mathtt{KeyGen}(\kappa)$

$$\epsilon \geq \Delta\left(\mathtt{Dec}_k \hat{\mathcal{F}}_{(x_0,x_1)} \mathtt{Enc}_k(|\psi'\rangle\langle\psi'|_{\mathsf{AR_A}}), \mathcal{F}_{(x_0,x_1)}(|\psi'\rangle\langle\psi'|_{\mathsf{AR_A}})\right), \tag{55}$$

which is exactly the correctness of Q'.

The data privacy of Q translates directly to the data privacy of Q', because both the key generation and encryption maps are identical. That is, for any $\rho \in \mathscr{S}(\mathsf{A})$

$$\epsilon_d \geq \Delta\left(\mathbb{E}(\mathtt{Enc}_k(\rho)), \mathbb{E}(\mathtt{Enc}_k(\rho'))\right), \tag{56}$$

for both Q and Q'.

The circuit privacy of Q requires that for any $|\psi\rangle \in \hat{\mathsf{A}}\mathsf{R}_{\hat{\mathsf{A}}}$, there must exist $|\psi'\rangle \in \mathsf{A}\mathsf{R}_{\mathsf{A}}$ and $\mathcal{N} \in \mathrm{CPTP}(\mathsf{A}\mathsf{R}_{\hat{\mathsf{A}}}, \hat{\mathsf{A}}\mathsf{R}_{\hat{\mathsf{A}}})$ such that for any $\mathcal{F}_{(x_0,x_1)}^{(r_0,r_1,r_2,r_3)}$

$$\epsilon_c \geq \Delta\left(\hat{\mathcal{F}}_{(x_0,x_1)}^{(r_0,r_1,r_2,r_3)}[|\psi\rangle\langle\psi|_{\hat{\mathsf{A}}\mathsf{R}_{\hat{\mathsf{A}}}}], \mathcal{N}(\mathcal{F}_{(x_0,x_1)}^{(r_0,r_1,r_2,r_3)}(|\psi'\rangle\langle\psi'|_{\mathsf{A}\mathsf{R}_{\mathsf{A}}}))\right). \tag{57}$$

Similar to the technique we use for the correctness, averaging over the uniform distribution of (r_0, r_1, r_2, r_3), applying the convexity of the trace distance in [35, Theorem 9.3] and substituting Eq. (52) and Eq. (53), we conclude that for any $|\psi\rangle \in \hat{\mathsf{A}}\mathsf{R}_{\hat{\mathsf{A}}}$, there must exist $|\psi'\rangle \in \mathsf{A}\mathsf{R}_{\mathsf{A}}$ and $\mathcal{N} \in \mathrm{CPTP}(\mathsf{A}\mathsf{R}_{\hat{\mathsf{A}}}, \hat{\mathsf{A}}\mathsf{R}_{\hat{\mathsf{A}}})$ such that for any $\mathcal{F}_{(x_0,x_1)}$

$$\epsilon_c \geq \Delta\left(\hat{\mathcal{F}}_{(x_0,x_1)}[|\psi\rangle\langle\psi|_{\hat{\mathsf{A}}\mathsf{R}_{\hat{\mathsf{A}}}}], \mathcal{N}(\mathcal{F}_{(x_0,x_1)}(|\psi'\rangle\langle\psi'|_{\mathsf{A}\mathsf{R}_{\mathsf{A}}}))\right). \tag{58}$$

This shows that Q' has ϵ_c-circuit privacy.

□

Remark 15. *We can reduce quantum homomorphic encryption which allows the delegation of $\mathcal{F}_{(x_0,x_1)}$ to quantum homomorphic encryption which allows the delegation of $\mathcal{F}_{(x_0,x_1)}^{(r_0,r_1,r_2,r_3)}$. However, the converse is not necessarily true. Quantum homomorphic encryption allowing $\mathcal{F}_{(x_0,x_1)}$ is weaker than quantum homomorphic encryption allowing $\mathcal{F}_{(x_0,x_1)}^{(r_0,r_1,r_2,r_3)}$.*

In the following part, we will prove that one can construct a standard oblivious transfer protocol by a quantum homomorphic encryption protocol with $\{\mathcal{F}_{(x_0,x_1)}\}_{x_0,x_1\in\{0,1\}} \subset \mathscr{F}$. The ϵ-correctness, ϵ_d-data privacy and ϵ_c-circuit privacy of quantum homomorphic encryption translates to the ϵ-completeness, $\frac{1}{2}(1+\epsilon_d)$-soundness against a cheating Bob and $\frac{1}{2}+\epsilon_c$-soundness against a cheating Alice of standard oblivious transfer.

Now we clarify once more the notations before we state the lemmas. Recall the notations in the actual protocol. Alice's message is $\sigma \in \mathscr{S}(\hat{\mathsf{A}})$ and the purification of Alice's message is $|\psi\rangle \in \hat{\mathsf{A}}\mathsf{R}_{\hat{\mathsf{A}}}$. Bob's program is $|x_0, x_1\rangle\langle x_0, x_1|_{\mathsf{B}} \in \mathscr{S}(\mathsf{B})$. Bob's channel is $\hat{\mathcal{F}}_{(x_0,x_1)} \in \mathrm{CPTP}(\hat{\mathsf{A}}, \hat{\mathsf{O}})$ which maps Alice's message $\sigma \in \mathscr{S}(\hat{\mathsf{A}})$ to Bob's message $\hat{\mathcal{F}}_{(x_0,x_1)}(\sigma) \in \mathscr{S}(\hat{\mathsf{O}})$. Alice obtains $\hat{\mathcal{F}}_{(x_0,x_1)}(|\psi\rangle\langle\psi|_{\hat{\mathsf{A}}\mathsf{R}_{\hat{\mathsf{A}}}}) \in \mathscr{S}(\hat{\mathsf{O}}\mathsf{R}_{\hat{\mathsf{A}}})$.

Recall the notations in the ideal protocol. Alice's input is $\rho' \in \mathscr{S}(\mathsf{A})$ and the purification of Alice's input is $|\psi'\rangle \in \mathsf{A}\mathsf{R}_{\mathsf{A}}$. Charlie's channel is $\mathcal{F}_{(x_0,x_1)} \in \mathrm{CPTP}(\mathsf{A}, \mathsf{O})$ which maps Alice's input ρ' to Charlie's message $\mathcal{F}_{(x_0,x_1)}(\rho')$. Alice post-processes $\mathcal{F}_{(x_0,x_1)}(|\psi'\rangle\langle\psi'|_{\mathsf{A}\mathsf{R}_{\mathsf{A}}}) \in \mathscr{S}(\mathsf{O}\mathsf{R}_{\mathsf{A}})$ with $\mathcal{N} \in \mathrm{CPTP}(\mathsf{O}\mathsf{R}_{\mathsf{A}}, \hat{\mathsf{O}}\mathsf{R}_{\hat{\mathsf{A}}})$ and obtains $\mathcal{N}(\mathcal{F}_{(x_0,x_1)}(|\psi'\rangle\langle\psi'|_{\mathsf{A}\mathsf{R}_{\mathsf{A}}})) \in \mathscr{S}(\hat{\mathsf{O}}\mathsf{R}_{\hat{\mathsf{A}}})$.

We sketch the proof of the reduction from quantum oblivious transfer to quantum homomorphic encryption. In Protocol 2, we show how one can realize the standard oblivious transfer protocol using quantum homomorphic encryption. In Lemma 16, we translate the ϵ-correctness of quantum homomorphic encryption to the ϵ-completeness of standard oblivious transfer. In Lemma 17, we translate the ϵ_d-data privacy to the $\frac{1}{2}(1+\epsilon_d)$-soundness against a cheating Bob. In Lemma 20, we translate the ϵ_c-circuit privacy of a quantum homomorphic encryption protocol to the $(\frac{1}{2}+\epsilon_c)$-soundness of a quantum oblivious transfer protocol against a cheating Alice. We piece these lemmas together in Theorem 21, where

we show how a quantum homomorphic encryption protocol can apply a standard oblivious transfer protocol while taking into account the properties of completeness and soundness.

In Protocol 2, we reduce standard oblivious transfer to quantum homomorphic encryption. Alice inputs $i \in \{0,1\}$ and Bob inputs $(x_0, x_1) \in \{0,1\}^2$ in standard oblivious transfer. Now Alice and Bob make use of a black-box quantum homomorphic encryption protocol $(\mathscr{F}, \mathtt{KeyGen}, \mathtt{Enc}, \mathtt{Eval}, \mathtt{Dec})$ with $\{\mathcal{F}_{(x_0,x_1)}\}_{x_0,x_1\in\{0,1\}} \subset \mathscr{F}$. Alice generates Alice's key k with $\mathtt{KeyGen}$ and prepares Alice's input state $|i,0\rangle\langle i,0|_{\mathsf{A}} \in \mathscr{S}(\mathsf{A})$. Alice then encrypts and sends Alice's message $\sigma = \mathtt{Enc}_k(|i,0\rangle\langle i,0|_{\mathsf{A}}) \in \mathscr{S}(\hat{\mathsf{A}})$ to Bob. Bob evaluates and sends Bob's message $\theta = \hat{\mathcal{F}}_{(x_0,x_1)}(\sigma) \in \mathscr{S}(\hat{\mathsf{O}})$ back to Alice. Alice decrypts and obtains Alice's output state $\tau = \mathtt{Dec}_k(\theta) \in \mathscr{S}(\mathsf{O})$. Finally, Alice performs the optimal positive operator valued measure $\{M_{\hat{x}}\}_{\hat{x}\in\{0,1\}}$ on O to guess $\hat{x}$ for x_i and outputs $\hat{x}$.

Protocol 2 Applying standard oblivious transfer with quantum homomorphic encryption

Input: $i \in \{0,1\}$, $(x_0, x_1) \in \{0,1\}^2$. ▷ Alice's and Bob's inputs
Output: $\text{output}_A \in \{0,1\}$. ▷ Alice's output.

1: Alice: $k \leftarrow \mathtt{KeyGen}$.
2: Alice: Encode $\sigma \leftarrow \mathtt{Enc}_k(|i,0\rangle\langle i,0|_{\mathsf{A}})$ and send it to Bob.
3: Bob: Evaluate $\theta \leftarrow \mathcal{F}_{(x_0,x_1)}(\sigma)$ and send it to Alice.
4: Alice: Decrypt $\tau \leftarrow \mathtt{Dec}_k(\theta)$.
5: Alice: Measure $\{M_x\}_{x\in\{0,1\}}$ with outcome $\hat{x}$. ▷ Alice measures to determine $\hat{x}$.
6: Alice: $\text{output}_A \leftarrow \hat{x}$.

Lemma 16. *If the quantum homomorphic encryption in Protocol 2 has ϵ-correctness, then the constructed standard oblivious transfer has ϵ-completeness.*

Proof. From Definition 6, the correctness of the standard oblivious transfer requires that the output is approximately correct if both Alice and Bob are honest. Note that for any $|i,0\rangle \in \mathsf{A}$ and any $(x_0,x_1) \in \{0,1\}^2$, we have

$$\mathcal{F}_{(x_0,x_1)}(|i,0\rangle\langle i,0|_{\mathsf{A}}) = \frac{\mathbb{I}_2}{2} \otimes |x_i\rangle\langle x_i|_{\mathsf{O}_2}. \tag{59}$$

Due to the ϵ-correctness of the quantum homomorphic encryption protocol defined in Definition 2, we have

$$\Delta\left(\mathtt{Dec}_k\hat{\mathcal{F}}_{(x_0,x_1)}\mathtt{Enc}_k[|i,0\rangle\langle i,0|_{\mathsf{A}}], \frac{\mathbb{I}_2}{2} \otimes |x_i\rangle\langle x_i|_{\mathsf{O}_2}\right) \leq \epsilon. \tag{60}$$

According to [35, Eq. (9.22)], the trace distance can be written as

$$\begin{aligned}&\Delta\left(\mathtt{Dec}_k\hat{\mathcal{F}}_{(x_0,x_1)}\mathtt{Enc}_k[|i,0\rangle\langle i,0|_{\mathsf{A}}], \frac{\mathbb{I}_2}{2} \otimes |x_i\rangle\langle x_i|_{\mathsf{O}_2}\right)\\ &= \sup_{0\leq Q\leq \mathbb{I}_4} \mathrm{Tr}\left[Q\left(\frac{\mathbb{I}_2}{2} \otimes |x_i\rangle\langle x_i|_{\mathsf{O}_2} - \mathtt{Dec}_k\hat{\mathcal{F}}_{(x_0,x_1)}\mathtt{Enc}_k[|i,0\rangle\langle i,0|_{\mathsf{A}}]\right)\right].\end{aligned} \tag{61}$$

Let $Q = \mathbb{I}_2 \otimes |x_i\rangle\langle x_i|_{\mathsf{O}_2}$, we obtain

$$\begin{aligned}&\Delta\left(\mathtt{Dec}_k\hat{\mathcal{F}}_{(x_0,x_1)}\mathtt{Enc}_k[|i,0\rangle\langle i,0|_{\mathsf{A}}], \frac{\mathbb{I}}{2} \otimes |x_i\rangle\langle x_i|_{\mathsf{O}_2}\right)\\ &\geq 1 - \mathrm{Tr}\left(\frac{\mathbb{I}}{2} \otimes |x_i\rangle\langle x_i|_{\mathsf{O}_2}\mathtt{Dec}_k\hat{\mathcal{F}}_{(x_0,x_1)}\mathtt{Enc}_k[|i,0\rangle\langle i,0|_{\mathsf{A}}]\right).\end{aligned} \tag{62}$$

Suppose that Alice performs the positive operator valued measure $\{|0\rangle\langle 0|_{\mathsf{O}}, |1\rangle\langle 1|_{\mathsf{O}}\}$ and obtains the measurement outcome $\hat{x}'$. Thus

$$\Pr[(\hat{x}' = x_i)] = \mathrm{Tr}\left(\frac{\mathbb{I}}{2} \otimes |x_i\rangle\langle x_i|_{\mathsf{O}_2} \mathtt{Dec}_k \hat{\mathcal{F}}_{(x_0,x_1)} \mathtt{Enc}_k[|i,0\rangle\langle i,0|_{\mathsf{A}}]\right) \geq 1-\epsilon. \tag{63}$$

Since the optimal measurement performs better than the above measurement, we have

$$\Pr[\hat{x} = x_i] \geq \Pr[\hat{x}' = x_i] \geq 1-\epsilon. \tag{64}$$

Hence the standard oblivious transfer protocol in Definition 6 has ϵ-completeness. □

Lemma 17. *In Protocol 2, if the quantum homomorphic encryption protocol has ϵ_d-data privacy, then the constructed standard oblivious transfer protocol has $\frac{1}{2}(1+\epsilon_d)$-soundness against Bob.*

Proof. Suppose that the quantum homomorphic encryption protocol has ϵ_d-data privacy. Consider an honest Alice and a malicious Bob. Suppose that Alice's input is $|i,0\rangle\langle i,0|_{\mathsf{A}}$. Because Bob does not know Alice's key, Bob perceives Alice's message as $\mathbb{E}(\mathtt{Enc}_k[|i,0\rangle\langle i,0|_{\mathsf{A}}])$ where the expectation is taken over a uniform distribution over all keys k. From the ϵ_d-data privacy of the quantum homomorphic encryption protocol defined in Definition 3, we have

$$\Delta\left(\mathbb{E}(\mathtt{Enc}_k[|0,0\rangle\langle 0,0|_{\mathsf{A}}]), \mathbb{E}(\mathtt{Enc}_k[|1,0\rangle\langle 1,0|_{\mathsf{A}}])\right) \leq \epsilon_d. \tag{65}$$

Now Bob measures Alice's message and guesses $\hat{i}$ for i. Using the Holevo-Helstrom theorem in [30, 31] (or in a textbook, e.g. [32, Theorem 3.4]), the cheating probability of Bob, i.e., the probability that Bob guesses the given state correctly when Bob is given either of two states, each with a probability of $\frac{1}{2}$, is at most

$$\Pr[\hat{i} = i] \leq \frac{1}{2}(1+\epsilon_d). \tag{66}$$

Thus, the standard oblivious transfer protocol in Definition 6 has $\frac{1}{2}(1+\epsilon_d)$-soundness against a cheating Bob. □

Before we proceed to Lemma 20, we prove two more claims. In Claim 18, we show that the Schmidt basis of Alice's input can be chosen as the computational basis in Protocol 2 in the ideal protocol.

Claim 18. *Consider Protocol 2 in the ideal protocol. Suppose that the input $|\psi'\rangle \in \mathsf{AR}_{\mathsf{A}}$ is of the form*

$$|\psi'\rangle = \sum_{i,i',j,j' \in \{0,1\}} a_{ii'jj'} |i,i'\rangle_{\mathsf{A}} |j,j'\rangle_{\mathsf{R}_{\mathsf{A}}}, \tag{67}$$

and $\mathcal{N} \in \mathrm{CPTP}(\mathsf{OR}_{\mathsf{A}}, \hat{\mathsf{O}}\mathsf{R}_{\hat{\mathsf{A}}})$ is any channel. Then there exists an input $|\psi''\rangle \in \mathsf{AR}_{\mathsf{A}}$ of the form

$$|\psi''\rangle = \sum_{i,i' \in \{0,1\}} \sqrt{p_{ii'}} |i,i'\rangle_{\mathsf{A}} |i,i'\rangle_{\mathsf{R}_{\mathsf{A}}}, \tag{68}$$

and a post-processing channel $\mathcal{N}' \in \mathrm{CPTP}(\mathsf{OR}_{\mathsf{A}}, \hat{\mathsf{O}}\mathsf{R}_{\hat{\mathsf{A}}})$ such that for any $x_0, x_1 = 0, 1$,

$$\mathcal{N}\left(\mathcal{F}_{(x_0,x_1)}(|\psi'\rangle\langle\psi'|_{\mathsf{AR}_{\mathsf{A}}})\right) = \mathcal{N}'\left(\mathcal{F}_{(x_0,x_1)}(|\psi''\rangle\langle\psi''|_{\mathsf{AR}_{\mathsf{A}}})\right). \tag{69}$$

Proof. Here, we construct $\mathcal{N}'$ explicitly. Consider an input $|\psi'\rangle \in \mathsf{AR_A}$ of the form Eq. (67). Using the definition of $\mathcal{F}_{(x_0,x_1)}$ in Definition 10, we have

$$\mathcal{F}_{(x_0,x_1)}(|\psi'\rangle\langle\psi'|_{\mathsf{AR_A}}) = \sum_{i,i'\in\{0,1\}} p_{ii'} \frac{\mathbb{I}_2}{2} \otimes |x_{i\oplus i'} \oplus i'\rangle\langle x_{i\oplus i'} \oplus i'|_{\mathsf{O}_2} \otimes \rho_{ii'}, \tag{70}$$

where $\tau_{ii'} = \mathrm{Tr}_{\mathsf{A}}(|i,i'\rangle\langle i,i'|_{\mathsf{A}}|\psi'\rangle\langle\psi'|_{\mathsf{AR_A}}) \in \mathscr{S}(\mathsf{R_A})$, and $p_{ii'} = \mathrm{Tr}(\tau_{ii'})$ and $\rho_{ii'} = \frac{\tau_{ii'}}{p_{ii'}}$. Consider an input $|\psi''\rangle \in \mathsf{AR_A}$ of the form Eq. (68). Hence,

$$\mathcal{F}_{(x_0,x_1)}(|\psi''\rangle\langle\psi''|) = \sum_{i,i'\in\{0,1\}} p_{ii'} \frac{\mathbb{I}_2}{2} \otimes |x_{i\oplus i'} \oplus i'\rangle\langle x_{i\oplus i'} \oplus i'|_{\mathsf{O}_2} \otimes |i,i'\rangle\langle i,i'|_{\mathsf{R_A}}. \tag{71}$$

By observation, we can construct $\mathcal{N}'' \in \mathrm{CPTP}(\mathsf{OR_A}, \mathsf{OR_A})$ such that

$$\mathcal{N}''(\rho) = \sum_{i,i'\in\{0,1\}} \mathrm{Tr}_{\mathsf{R_A}}(|i,i'\rangle\langle i,i'|_{\mathsf{R_A}}\rho) \otimes \rho_{ii'}, \tag{72}$$

which satisfies

$$\mathcal{F}_{(x_0,x_1)}(|\psi'\rangle\langle\psi'|_{\mathsf{AR_A}}) = \mathcal{N}''(\mathcal{F}_{(x_0,x_1)}(|\psi''\rangle\langle\psi''|_{\mathsf{AR_A}})). \tag{73}$$

Hence we can construct $\mathcal{N}' = \mathcal{N} \circ \mathcal{N}''$ which satisfies

$$\mathcal{N}(\mathcal{F}_{(x_0,x_1)}(|\psi'\rangle\langle\psi'|_{\mathsf{AR_A}})) = \mathcal{N}'(\mathcal{F}_{(x_0,x_1)}(|\psi''\rangle\langle\psi''|_{\mathsf{AR_A}})). \tag{74}$$

Therefore, for any input $|\psi'\rangle \in \mathsf{AR_A}$ and any channel $\mathcal{N} \in \mathrm{CPTP}(\mathsf{OR_A}, \hat{\mathsf{OR}}_{\hat{\mathsf{A}}})$, there exist $|\psi''\rangle \in \mathsf{AR_A}$ and $\mathcal{N}' \in \mathrm{CPTP}(\mathsf{OR_A}, \hat{\mathsf{OR}}_{\hat{\mathsf{A}}})$ such that for any $\mathcal{F}_{(x_0,x_1)}$, Eq. (74) holds. □

In Claim 19 we show that the cheating probability of Alice is at most $\frac{1}{2}$ in the ideal protocol if the Schmidt basis of Alice's input is the computational basis.

Claim 19. *Consider Protocol 2 in the ideal protocol. For any input $|\psi''\rangle \in \mathsf{AR_A}$ of the form Eq. (68), any channel $\mathcal{N}' \in \mathrm{CPTP}(\mathsf{OR_A}, \hat{\mathsf{OR}}_{\hat{\mathsf{A}}})$, and any positive operator valued measure $\{M_{(\hat{x}_0,\hat{x}_1)}\}_{\hat{x}_0,\hat{x}_1\in\{0,1\}}$ on $\hat{\mathsf{OR}}_{\hat{\mathsf{A}}}$ where $(\hat{x}_0,\hat{x}_1) \in \{0,1\}^2$ are Alice's guesses for (x_0,x_1), the probability that Alice guesses correctly satisfies*

$$\Pr[(\hat{x}_0,\hat{x}_1) = (x_0,x_1)] \leq \frac{1}{2}, \tag{75}$$

when (x_0,x_1) are chosen uniformly at random.

Proof. Suppose that in the ideal protocol, Alice inputs $|\psi''\rangle \in \mathsf{AR_A}$ of the form Eq. (68). Alice applies $\mathcal{N}' \in \mathrm{CPTP}(\mathsf{OR_A}, \hat{\mathsf{OR}}_{\hat{\mathsf{A}}})$. Let B denotes Bob's register. The definition of soundness against Alice requires Bob to input (x_0,x_1) uniformly at random, or equivalently to input $\frac{1}{4}\sum_{x_0,x_1} |x_0,x_1\rangle\langle x_0,x_1|_{\mathsf{B}}$. The state of both Alice and Bob in the ideal protocol is

$$\rho_{\text{ideal}} = \frac{1}{4} \sum_{x_0,x_1\in\{0,1\}} \mathcal{N}'(\mathcal{F}_{(x_0,x_1)}(|\psi''\rangle\langle\psi''|_{\mathsf{AR_A}})) \otimes |x_0,x_1\rangle\langle x_0,x_1|_{\mathsf{B}}. \tag{76}$$

Suppose that Alice measures $\{M_{(\hat{x}_0,\hat{x}_1)}\}_{\hat{x}_0,\hat{x}_1\in\{0,1\}}$ and guesses $(\hat{x}_0,\hat{x}_1)$ for (x_0,x_1). The probability that Alice guesses correctly is

$$\Pr[(\hat{x}_0,\hat{x}_1) = (x_0,x_1)] = \sum_{x_0,x_1\in\{0,1\}} \mathrm{Tr}\left(M_{(x_0,x_1)} \otimes |x_0,x_1\rangle\langle x_0,x_1|_{\mathsf{B}}\rho_{\text{ideal}}\right) \tag{77}$$

$$= \frac{1}{4} \sum_{x_0,x_1\in\{0,1\}} \mathrm{Tr}\left(M_{(x_0,x_1)}\mathcal{N}'(\mathcal{F}_{(x_0,x_1)}(|\psi''\rangle\langle\psi''|_{\mathsf{AR_A}}))\right), \tag{78}$$

where we substituted Eq. (76) and took the trace over B. Let $\mathcal{N}'^*$ be the adjoint of $\mathcal{N}'$ and $M'_{(x_0,x_1)} = \mathcal{N}'^*(M_{(x_0,x_1)})$. $\mathcal{N}'$ is trace preserving, thus $\mathcal{N}'^*$ is unital. Since $\{M_{(x_0,x_1)}\}_{x_0,x_1\in\{0,1\}}$ is a positive operator valued measure on $\hat{\mathsf{OR}}_{\hat{\mathsf{A}}}$, $\{M_{(x_0,x_1)}\}_{x_0,x_1\in\{0,1\}}$ is also a positive operator valued measure on OR_{A}. By replacing $\mathcal{N}'$ and $\{M_{(x_0,x_1)}\}_{x_0,x_1\in\{0,1\}}$ with $\mathcal{N}'^*$ and $\{M'_{(x_0,x_1)}\}_{x_0,x_1\in\{0,1\}}$, we obtain

$$\Pr[(\hat{x}_0,\hat{x}_1)=(x_0,x_1)] = \frac{1}{4}\sum_{x_0,x_1\in\{0,1\}} \mathrm{Tr}\left(M'_{(x_0,x_1)}\mathcal{F}_{(x_0,x_1)}(|\psi''\rangle\langle\psi''|_{\mathsf{AR}_{\mathsf{A}}})\right). \tag{79}$$

Recall that $|\psi''\rangle$ has the form Eq. (68) and thus $\mathcal{F}_{(x_0,x_1)}(|\psi''\rangle\langle\psi''|_{\mathsf{AR}_{\mathsf{A}}})$ has the form Eq. (71). Substituting both Eq. (68) and Eq. (71) into Eq. (79), we obtain

$$\begin{aligned}&\Pr[(\hat{x}_0,\hat{x}_1)=(x_0,x_1)|\rho_{\text{ideal}}]\\ &= \frac{1}{4}\sum_{x_0,x_1,i,i'\in\{0,1\}} \mathrm{Tr}\left(p_{ii'}M'_{(x_0,x_1)}\frac{\mathbb{I}_2}{2}\otimes|x_{i\oplus i'}\oplus i'\rangle\langle x_{i\oplus i'}\oplus i'|_{\mathsf{O}_2}\otimes|i,i'\rangle\langle i,i'|_{\mathsf{R}_{\mathsf{A}}}\right).\end{aligned} \tag{80}$$

To upper bound the probability, we replace $|x_{i\oplus i'}\oplus i'\rangle\langle x_{i\oplus i'}\oplus i'|_{\mathsf{O}_2}$ with $\mathbb{I}_2$. Substituting $\sum_{x_0,x_1\in\{0,1\}} M'_{(x_0,x_1)} = \mathbb{I}_{\mathsf{OR}_{\mathsf{A}}}$ as well as $\sum_{i,i'\in\{0,1\}} p_{ii'} = 1$, we obtain that the probability that Alice guesses correctly is at most $\frac{1}{2}$ in the ideal protocol

$$\Pr[(\hat{x}_0,\hat{x}_1)=(x_0,x_1)|\rho_{\text{ideal}}] \le \frac{1}{2}\sum_{i,i'\in\{0,1\}} p_{ii'} = \frac{1}{2}, \tag{81}$$

which completes the proof.

□

With Claim 18 and Claim 19 in hand, we are ready to prove the bound on soundness against Alice in Lemma 20. The circuit privacy bounds the trace distance between Alice's state in the ideal protocol and that in the actual protocol. The trace distance further bounds the difference between Alice's cheating probability in the actual model and the ideal model. Note that Alice's cheating probability in the ideal protocol is $\frac{1}{2}$. Hence we can upper-bound Alice's cheating probability in the actual protocol.

Lemma 20. *If the quantum homomorphic encryption protocol In Protocol 2 has ϵ_c-circuit privacy, then the constructed standard oblivious transfer protocol has $(\frac{1}{2}+\epsilon_c)$-soundness against Alice.*

Proof. Suppose that in the actual protocol, Alice inputs $|\psi\rangle \in \hat{\mathsf{AR}}_{\hat{\mathsf{A}}}$. Again Let B denote Bob's register. The definition of soundness against Alice requires Bob to input (x_0,x_1) uniformly at random, or equivalently Bob to input $\frac{1}{4}\sum_{x_0,x_1}|x_0,x_1\rangle\langle x_0,x_1|_{\mathsf{B}}$. Bob applies $\hat{\mathcal{F}}_{(x_0,x_1)}$ according to his values for (x_0,x_1). Alice and Bob's joint state in the actual protocol is

$$\rho_{\text{actual}} = \frac{1}{4}\sum_{x_0,x_1\in\{0,1\}} \hat{\mathcal{F}}_{(x_0,x_1)}[|\psi\rangle\langle\psi|_{\hat{\mathsf{AR}}_{\hat{\mathsf{A}}}}]\otimes|x_0,x_1\rangle\langle x_0,x_1|_{\mathsf{B}}. \tag{82}$$

Suppose that Alice measures $\{M_{(\hat{x}_0,\hat{x}_1)}\}_{\hat{x}_0,\hat{x}_1\in\{0,1\}}$ and guesses $(\hat{x}_0,\hat{x}_1)$ for (x_0,x_1). The probability that Alice can guess correctly is

$$\Pr[(\hat{x}_0,\hat{x}_1)=(x_0,x_1)|\rho_{\text{actual}}] = \sum_{x_0,x_1\in\{0,1\}} \mathrm{Tr}\left(M_{(x_0,x_1)}\otimes|x_0,x_1\rangle\langle x_0,x_1|_{\mathsf{B}}\rho_{\text{actual}}\right). \tag{83}$$

The absolute value of Eq. (77) minus Eq. (83) can be bounded by the trace distance between ρ_{ideal} and ρ_{actual}, as shown in the Holevo-Helstrom theorem in [30, 31] (or a modern version in [32, Theorem 3.4])

$$|\Pr[(\hat{x}_0,\hat{x}_1)=(x_0,x_1)|\rho_{\text{actual}}]-\Pr[(\hat{x}_0,\hat{x}_1)=(x_0,x_1)|\rho_{\text{ideal}}]|\leq\Delta(\rho_{\text{actual}},\rho_{\text{ideal}}). \tag{84}$$

Substituting Eq. (76) and Eq. (82) into Eq. (84) and applying the convexity of the trace distance in [35, Theorem 9.3], we obtain

$$\Delta\left(\rho_{\text{actual}},\rho_{\text{ideal}}\right)\leq\frac{1}{4}\sum_{x_0,x_1\in\{0,1\}}\Delta\left(\hat{\mathcal{F}}_{(x_0,x_1)}[|\psi\rangle\langle\psi|_{\hat{\mathsf{A}}\mathsf{R}_{\hat{\mathsf{A}}}}],\mathcal{N}'\left(\mathcal{F}_{(x_0,x_1)}(|\psi''\rangle\langle\psi''|_{\mathsf{A}\mathsf{R}_{\mathsf{A}}})\right)\right)\leq\epsilon_c, \tag{85}$$

where the last inequality is due to the ϵ_c-circuit privacy of the quantum homomorphic encryption protocol defined in Definition 4, which implies that for any $|\psi\rangle$ we can find $|\psi''\rangle$ and $\mathcal{N}'$ such that for any (x_0,x_1)

$$\Delta\left(\hat{\mathcal{F}}_{(x_0,x_1)}[|\psi\rangle\langle\psi|_{\hat{\mathsf{A}}\mathsf{R}_{\hat{\mathsf{A}}}}],\mathcal{N}'\left(\mathcal{F}_{(x_0,x_1)}(|\psi''\rangle\langle\psi''|_{\mathsf{A}\mathsf{R}_{\mathsf{A}}})\right)\right)\leq\epsilon_c. \tag{86}$$

Thus,

$$|\Pr[(\hat{x}_0,\hat{x}_1)=(x_0,x_1)|\rho_{\text{actual}}]-\Pr[(\hat{x}_0,\hat{x}_1)=(x_0,x_1)|\rho_{\text{ideal}}]|\leq\epsilon_c. \tag{87}$$

Substituting Eq. (81) in Claim 19 into Eq. (87), we obtain that the cheating probability of Alice is at most

$$\Pr[(\hat{x}_0,\hat{x}_1)=(x_0,x_1)|\rho_{\text{actual}}]\leq\frac{1}{2}+\epsilon_c. \tag{88}$$

Hence, the oblivious transfer protocol in Definition 6 has $(\frac{1}{2}+\epsilon_c)$-soundness. □

We can immediately prove Theorem 21 with Protocol 2, Lemma 16, Lemma 17 and Lemma 20.

Theorem 21. *Suppose that there is a quantum homomorphic encryption protocol Q with ϵ-correctness, ϵ_d-data privacy and ϵ_c-circuit privacy that delegates $\mathcal{F}_{(x_0,x_1)}$. Then one can use Q to execute standard oblivious transfer with ϵ-completeness, $(\frac{1}{2}+\epsilon_c)$-soundness against a cheating Alice and $\frac{1}{2}(1+\epsilon_d)$-soundness against a cheating Bob.*

Proof. Suppose that we apply Protocol 2 with a quantum homomorphic encryption protocol with ϵ-correctness, ϵ_d-data privacy and ϵ_c-circuit privacy. Lemma 16 shows that the ϵ-completeness of the standard oblivious transfer is satisfied, Lemma 17 shows that the $\frac{1}{2}(1+\epsilon_d)$-soundness against a cheating Bob is satisfied, and Lemma 20 shows that the $\frac{1}{2}+\epsilon_c$-soundness against a cheating Alice is satisfied, which completes the proof. □

5 Bounds for quantum homomorphic encryption

5.1 Lower bounds for quantum homomorphic encryption

Here, we prove a lower bound for a broad family of quantum homomorphic encryption protocols. The reduction in Theorem 21 can translate a bound on quantum oblivious transfer to the bound on quantum homomorphic encryption that can delegate $\mathcal{F}_{(x_0,x_1)}$. Lemma 14 shows that quantum homomorphic encryption allowing Cliffords can simulate quantum homomorphic encryption allowing $\mathcal{F}_{(x_0,x_1)}$. Combining Theorem 21, Theorem 9 and Lemma 14, we obtain a lower bound for quantum homomorphic encryption with Cliffords.

Corollary 22. *A quantum homomorphic encryption protocol with ϵ-correctness, ϵ_d-data privacy and ϵ_c-circuit privacy that allows the delegated computation of $\mathcal{F}_{(x_0,x_1)}$ satisfies*

$$\epsilon_c + \epsilon_d + 4\sqrt{\epsilon} \geq \frac{1}{2}. \tag{89}$$

Moreover, the above bound also applies to quantum homomorphic encryption allowing $\mathcal{F}_{(x_0,x_1)}^{(r_0,r_1,r_2,r_3)}$ or with Cliffords.

5.2 Upper bounds for quantum homomorphic encryption

In this section, we relate the circuit privacy of quantum homomorphic encryption that delegates a set of channels to the maximal error probability of multi-channel quantum hypothesis testing over the set of channels. In this way, we can prove upper bounds on circuit privacy of quantum homomorphic encryption.

We first introduce the multi-channel quantum hypothesis testing problem. Suppose that we are given a quantum channel $\mathcal{F}$ which is chosen from a set $\mathscr{F}$ of quantum channels. We apply the quantum channel $\mathcal{F}$ on an input $|\psi'\rangle \in \mathsf{AR_A}$, perform a positive operator valued measure $\{M_{\mathcal{F}'}\}_{\mathcal{F}'\in\mathscr{F}}$ on the output $\mathcal{F}(|\psi'\rangle\langle\psi'|_{\mathsf{AR_A}}) \in \mathscr{S}(\mathsf{OR_A})$ and use the measurement outcome $\mathcal{F}'$ to guess for $\mathcal{F}$. The maximal error probability of multi-channel quantum hypothesis testing over $\mathscr{F}$ is

$$p_{\max}(\mathscr{F}) = \min_{|\psi'\rangle\in\mathsf{AR_A},\{M_{\mathcal{F}'}\}_{\mathcal{F}'\in\mathscr{F}}} \max_{\mathcal{F}\in\mathscr{F}} \mathrm{Tr}\left((\mathbb{I} - M_{\mathcal{F}})\mathcal{F}(|\psi'\rangle\langle\psi'|_{\mathsf{AR_A}})\right). \tag{90}$$

Now, consider the circuit privacy of quantum homomorphic encryption that allows the delegation of a set of channels $\mathscr{F}$. Suppose that Alice is malicious and Bob is honest. Recall the actual protocol in Figure 3 and the ideal protocol in Figure 4. In the actual protocol and the ideal protocol, Alice's final state is $\hat{\mathcal{F}}(|\psi\rangle\langle\psi|_{\hat{\mathsf{AR}}_{\hat{\mathsf{A}}}}) \in \mathscr{S}(\hat{\mathsf{OR}}_{\hat{\mathsf{A}}})$ and $\mathcal{F}(|\psi'\rangle\langle\psi'|_{\mathsf{AR_A}}) \in \mathscr{S}(\mathsf{OR_A})$ respectively. The circuit privacy quantifies how well Alice in the ideal protocol can simulate Alice in the actual protocol. There is always a possible strategy for the simulation: Alice in the ideal protocol performs multi-channel quantum hypothesis testing and then uses the measurement outcome to simulate Alice in the actual protocol. More precisely, first, Alice in the ideal protocol sends $|\psi'\rangle \in \mathsf{AR_A}$ to Charlie, obtains $\mathcal{F}(|\psi'\rangle\langle\psi'|_{\mathsf{AR_A}}) \in \mathscr{S}(\mathsf{OR_A})$, measures $\{M_{\mathcal{F}'}\}_{\mathcal{F}'\in\mathscr{F}}$ on $\mathcal{F}(|\psi'\rangle\langle\psi'|_{\mathsf{AR_A}})$ and guesses $\mathcal{F}'$ for $\mathcal{F}$; second, Alice in the ideal protocol use $\hat{\mathcal{F}}'(|\psi\rangle\langle\psi|_{\hat{\mathsf{AR}}_{\hat{\mathsf{A}}}})$ to simulate $\hat{\mathcal{F}}(|\psi\rangle\langle\psi|_{\hat{\mathsf{AR}}_{\hat{\mathsf{A}}}})$. We can then use this strategy to upper bound the circuit privacy of quantum homomorphic encryption.

Theorem 23. *The circuit privacy of a quantum homomorphic encryption protocol that delegates a set $\mathscr{F}$ of channels is upper bounded by the maximal error probability of multi-channel quantum hypothesis testing over a set $\mathscr{F}$ of channels*

$$\epsilon_c \leq p_{\max}(\mathscr{F}). \tag{91}$$

Proof. Suppose that Alice in the actual protocol obtains $\hat{\mathcal{F}}(|\psi\rangle\langle\psi|_{\hat{\mathsf{AR}}_{\hat{\mathsf{A}}}})$ and that Alice in the ideal protocol obtains $\mathcal{F}(|\psi'\rangle\langle\psi'|_{\mathsf{AR_A}})$. Alice in the ideal protocol performs the multi-channel quantum hypothesis testing and uses the measurement outcome to simulate Alice in the actual protocol. That is, Alice in the ideal protocol sends a state $|\psi'\rangle \in \mathsf{AR_A}$ to Charlie, obtains $\mathcal{F}(|\psi'\rangle\langle\psi'|_{\mathsf{AR_A}}) \in \mathscr{S}(\mathsf{OR_A})$, measures the positive operator valued measurement $\{M_{\mathcal{F}'}\}_{\mathcal{F}'\in\mathscr{F}}$, obtains the measurement outcome $\mathcal{F}'$ and then constructs $\hat{\mathcal{F}}(|\psi\rangle\langle\psi|_{\hat{\mathsf{AR}}_{\hat{\mathsf{A}}}})$. The corresponding quantum channel $\mathcal{N} \in \mathrm{CPTP}(\mathsf{OR_A}, \hat{\mathsf{OR}}_{\hat{A}})$ is given by

$$\mathcal{N}(\rho) = \sum_{\mathcal{F}'\in\mathscr{F}} \mathrm{Tr}(M_{\mathcal{F}'}\rho)\hat{\mathcal{F}}'(|\psi\rangle\langle\psi|_{\hat{\mathsf{AR}}_{\hat{\mathsf{A}}}}). \tag{92}$$

Substituting Eq. (92) into Eq. (4), applying the convexity of the trace distance in [35, Theorem 9.3] and note that trace distance is upper-bounded by 1, we obtain

$$\Delta(\hat{\mathcal{F}}(|\psi\rangle\langle\psi|_{\hat{\mathsf{AR}}_{\hat{\mathsf{A}}}}), \mathcal{N}(\mathcal{F}(|\psi'\rangle\langle\psi'|_{\mathsf{AR}_{\mathsf{A}}}))) \leq \mathrm{Tr}((\mathbb{I} - M_{\mathcal{F}})\mathcal{F}(|\psi'\rangle\langle\psi'|_{\mathsf{AR}_{\mathsf{A}}})), \tag{93}$$

which holds for all possible $\mathcal{F} \in \mathscr{F}$, $|\psi'\rangle \in \mathsf{AR}_{\mathsf{A}}$, $\{M_{\mathcal{F}'}\}_{\mathcal{F}'\in\mathscr{F}}$, and $|\psi\rangle \in \hat{\mathsf{AR}}_{\hat{\mathsf{A}}}$. We now maximize over all possible $\mathcal{F} \in \mathscr{F}$, minimize over all possible $|\psi'\rangle \in \mathsf{AR}_{\mathsf{A}}$ and $\{M_{\mathcal{F}'}\}_{\mathcal{F}'\in\mathscr{F}}$, and maximize over all possible $|\psi\rangle \in \hat{\mathsf{AR}}_{\hat{\mathsf{A}}}$. Recall Remark 5 and Eq. (90), we obtain

$$\epsilon_c \leq p_{\max}(\mathscr{F}), \tag{94}$$

which completes the proof. □

By applying a trivial positive operator valued measure $\{M_{\mathcal{F}} = \frac{1}{|\mathscr{F}|}\mathbb{I}_{\mathsf{OR}_{\mathsf{A}}}\}_{\mathcal{F}\in\mathscr{F}}$, we can immediately obtain a trivial upper bound $\epsilon_c \leq 1 - \frac{1}{|\mathscr{F}|}$ for an arbitrary $\mathscr{F}$. We can further derive a better upper bound for $\mathscr{F} = \{\mathcal{F}_{(x_0,x_1)}\}_{x_0,x_1\in\{0,1\}}$.

Corollary 24. *For any quantum homomorphic encryption which only allows the delegated computation of $\mathcal{F}_{(x_0,x_1)}$, the circuit privacy is bounded by*

$$\epsilon_c \leq \frac{1}{2}. \tag{95}$$

Proof. Let $|\psi'\rangle = |0,0\rangle|0,0\rangle$ and $\{M_{(x_0,x_1)} = \mathbb{I}_2 \otimes \frac{1}{2}|x_0\rangle\langle x_0|_{\mathsf{O}_2}\}_{0,x_1\in\{0,1\}}$. Hence

$$\mathcal{F}_{(x_0,x_1)}(|\psi'\rangle\langle\psi'|_{\mathsf{AR}_{\mathsf{A}}}) = \frac{\mathbb{I}_2}{2} \otimes |x_0\rangle\langle x_0|_{\mathsf{O}_2} \otimes |0,0\rangle\langle 0,0|_{\mathsf{R}_{\mathsf{A}}}. \tag{96}$$

Thus we have

$$p_{\max}(\mathscr{F}) \leq \max_{x_0,x_1\in\{0,1\}} \mathrm{Tr}\left((\mathbb{I}_4 - M_{(x_0,x_1)})\mathcal{F}_{(x_0,x_1)}(|\psi'\rangle\langle\psi'|_{\mathsf{AR}_{\mathsf{A}}})\right) = \frac{1}{2}. \tag{97}$$

We then immediately obtain Corollary 24 from Theorem 23. □

6 Conclusion

In conclusion, we formally define quantum homomorphic encryption and its information-theoretic circuit privacy, correctness and data privacy. We then reduce quantum oblivious transfer to quantum homomorphic encryption with strong oblivious transfer channels. We show our reduction works for a broad class of quantum homomorphic encryption by further reducing quantum homomorphic encryption with strong oblivious transfer channels to quantum homomorphic encryption with Cliffords. Combining our reduction and a lower bound for quantum oblivious transfer, we obtain a lower bound for a broad class of quantum homomorphic encryption

$$\epsilon_d + \epsilon_c + 4\sqrt{\epsilon} \geq \frac{1}{2}. \tag{98}$$

To be complete, we also prove an upper bound for quantum homomorphic encryption by constructing a simulation strategy for Alice from multi-channel quantum hypothesis testing. We show that the circuit privacy of quantum homomorphic encryption that delegates

a set $\mathscr{F}$ of channels is upper bounded by the maximal error probability of multi-channel quantum hypothesis testing

$$\epsilon_c \leq p_{\max}(\mathscr{F}). \tag{99}$$

As a corollary, we find $\epsilon_c \leq \frac{1}{2}$ for quantum homomorphic encryption that only delegates $\mathcal{F}_{(x_0,x_1)}$.

In Figure 11, we present lower bounds for quantum homomorphic encryption protocols that only allow the delegation of $\mathcal{F}_{(x_0,x_1)}$ with perfect correctness. Each point in Figure 11 is denoted by (ϵ_d, ϵ_c). The line corresponds to the lower bound, and the shaded area indicates the impossible region. The diamond point $(0, \frac{1}{2})$ can be achieved using [11] asymptotically. The square point $(1, 0)$ can be trivially achieved by Alice sending her input to Bob without encryption. It is still unknown whether the line is reachable at points other than the diamond point. In particular, we do not have quantum homomorphic encryption protocols which trade some data privacy for some circuit privacy, and thus we cannot achieve other points on the line without additional resources. (If Alice and Bob have shared randomness or can use weak coin flipping, then interpolation would be possible.)

We note that the impossible region could potentially be enlarged if we consider more powerful function classes so that, for example, 1-out-of-n oblivious transfer can be reduced to homomorphic encryption, reducing the probability that Alice and Bob correctly guess their opponent's inputs by chance. We leave this for future work.

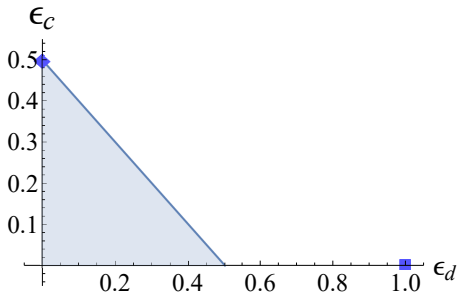


Figure 11: The lower bound for quantum homomorphic encryption that only allows to delegate $\mathcal{F}_{(x_0,x_1)}$ with perfect correctness. Each point is denoted by (ϵ_d, ϵ_c). The line corresponds to the lower bound. The diamond point $(0, \frac{1}{2})$ and the square point $(1, 0)$ are known to be achievable. The shaded area is impossible.

Our definitions and techniques can also apply to reductions from other cryptographic primitives (e.g. secure multi-party computation [36, 37], coin-flipping [38, 39, 40, 41], bit commitment [42, 43]) to quantum homomorphic encryption, which may allow better privacy and correctness trade-offs.

7 Acknowledgements

We thank Christopher Portmann for useful discussions on security definitions. MT, YO and YH are supported by the National Research Foundation, Singapore and A*STAR under its CQT Bridging Grant. They are also funded by the Quantum Engineering programme grant NRF2021-QEP2-01-P06.

A Equivalence between standard oblivious transfer and semi-random oblivious transfer

In this subsection, we give the detailed proof for Theorem 8.

Proof. First, we reduce semi-random oblivious transfer to standard oblivious transfer, as is shown in Protocol 3. Bob inputs two data bits $(x_0, x_1) \in \{0,1\}^2$ in semi-random oblivious transfer. Alice generates $i \in \{0,1\}$ uniformly at random. Then Alice and Bob perform standard oblivious transfer in which Alice inputs i and Bob inputs (x_0, x_1) and from which Alice obtains A and Bob obtains B. Each party accepts in semi-random oblivious transfer if and only if she or he accepts in standard oblivious transfer. If Alice accepts, Alice's output is $\text{output}_A = (i, A)$.

Protocol 3 Semi-random oblivious transfer from standard oblivious transfer

Input: $(x_0, x_1) \in \{0,1\}^2$. ▷ Bob's input.

Output: $\text{output}_A \in \{0,1\}^2 \cup \{\texttt{Abort}\}$, $\text{output}_B \in \{\texttt{Accept}, \texttt{Abort}\}$. ▷ Alice's and Bob's outputs.

1: Alice: Generate $i \leftarrow \$$. ▷ Alice generates a bit uniformly at random
2: Alice and Bob: Perform $(A, B) \leftarrow \text{StandardOT}(i, (x_0, x_1))$.
3: **if** $A = \texttt{Abort}$ **then**
4: Alice: $\text{output}_A \leftarrow \texttt{Abort}$.
5: **else**
6: Alice: $\text{output}_A \leftarrow (i, A)$. ▷ Alice accepts in SemirandomOT iff Alice accepts in StandardOT.
7: **end if**
8: Bob: $\text{output}_B \leftarrow B$. ▷ Bob accepts in SemirandomOT iff Bob accepts in StandardOT.

Now we show that the δ-completeness, $P_A^\star$-soundness against Alice and $P_B^\star$-soundness against Bob also translate from standard oblivious transfer to semi-random oblivious transfer in the reduction.

- Completeness: Suppose that both Alice and Bob are honest. Then i is uniformly at random. Due to the δ-completeness of standard oblivious transfer, both parties accept, and with a probability of at least $1-\delta$, $y = x_i$. Hence the δ-completeness of semi-random oblivious transfer is satisfied.

- Soundness against a cheating Alice: Suppose that Alice is malicious while Bob is honest. Due to the $P_A^\star$-soundness against a cheating Alice of standard oblivious transfer, with a probability of at most $P_A^\star$, Alice can guess Bob's (x_0, x_1) correctly and both parties accept. Therefore, the $P_A^\star$-soundness against a cheating Alice of semi-random oblivious transfer is satisfied.

- Soundness against a cheating Bob: Suppose that Alice is honest while Bob is malicious. Due to the $P_B^\star$-soundness against a cheating Alice of standard oblivious transfer, with a probability of at most $P_B^\star$, Bob can guess Alice's i correctly and both parties accept. Thus, the $P_B^\star$-soundness against a cheating Alice of semi-random oblivious transfer is satisfied.

Second, we reduce standard oblivious transfer to semi-random oblivious transfer, as is shown in Protocol 4. Alice inputs $i \in \{0,1\}$ and Bob inputs $(x_0, x_1) \in \{0,1\}^2$ in standard

oblivious transfer. Bob generates $(y_0, y_1) \in \{0,1\}^2$ uniformly at random. Then Alice and Bob perform semi-random oblivious transfer in which Bob inputs (y_0, y_1) and from which Alice obtains A and Bob obtains B. They then declare if they have aborted to the other party. Each party accepts in standard oblivious transfer if and only if both accept in semi-random oblivious transfer. If both accept, Alice sets $(j, \hat{y}) = A$. Then Alice encrypts and sends the request $r = i \oplus j$ to Bob, Bob encrypts and sends the data bits $s_0 = x_r \oplus y_0$ and $s_1 = x_{\overline{r}} \oplus y_1$ to Alice. Alice decrypts the data and Alice's output is $\text{output}_A = s_j \oplus \hat{y}$.

Protocol 4 Standard oblivious transfer from semi-random oblivious transfer

Input: $i \in \{0,1\}$, $(x_0, x_1) \in \{0,1\}^2$. ▷ Alice's and Bob's inputs.

Output: $\text{output}_B \in \{0,1\} \cup \{\texttt{Abort}\}$, $\text{output}_B \in \{\texttt{Accept}, \texttt{Abort}\}$. ▷ Alice's and Bob's outputs.

1: Bob: Generate $y_0, y_1 \leftarrow \$$. ▷ Bob generates two bits uniformly at random.
2: Alice and Bob: Perform $(A, B) \leftarrow \text{SemirandomOT}(y_0, y_1)$.
3: Alice and Bob: Declare if they have aborted to the other party.
4: **if** $(A = \texttt{Abort}) \vee (B = \texttt{Abort})$ **then**
5: Alice: $\text{output}_A \leftarrow \texttt{Abort}$.
6: Bob: $\text{output}_B \leftarrow \texttt{Abort}$.
7: **else**
8: Alice: $(j, \hat{y}) \leftarrow A$.
9: Alice: Send $r \leftarrow i \oplus j$ to Bob.
10: Bob: Send $s_0 \leftarrow x_r \oplus y_0$ and $s_1 \leftarrow x_{\overline{r}} \oplus y_1$ to Alice.
11: Alice: $\text{output}_A \leftarrow s_j \oplus \hat{y}$. ▷ Alice accepts in StandardOT iff both accept in SemirandomOT.
12: Bob: $\text{output}_B \leftarrow \texttt{Accept}$. ▷ Bob accepts in StandardOT iff both accept in SemirandomOT.
13: **end if**

Now we show that the δ-completeness, $P_A^\star$-soundness against Alice and $P_B^\star$-soundness against Bob also translate from semi-random oblivious transfer to standard oblivious transfer in the reduction.

- Completeness: Suppose that both Alice and Bob are honest. Due to the δ-completeness of semi-random oblivious transfer, both parties accept, and with a probability of at least $1 - \delta$, $\hat{y} = y_j$. Considering that $\hat{x} = x_i \oplus y_j \oplus \hat{y}$, thus with a probability of at least $1 - \delta$, $\hat{x} = x_i$. Therefore, the δ-completeness of standard oblivious transfer is satisfied.

- Soundness against a cheating Alice: Suppose that Alice is malicious and Bob is honest. Due to the $P_A^\star$-soundness against a cheating Alice of semi-random oblivious transfer, with a probability of at most $P_A^\star$, Alice can guess Bob's (y_0, y_1) and both parties accept. Since $y_0 y_1$ is uniformly random and $x_r = s_0 \oplus y_0$ and $x_{\overline{r}}) = s_1 \oplus y_1$, with a probability of at most $P_A^\star$, Alice can guess Bob's (x_0, x_1) and both parties accept. Hence, the $P_A^\star$-soundness against a cheating Alice of standard oblivious transfer is satisfied.

- Soundness against a cheating Bob: Suppose that Alice is honest and Bob is malicious. Due to the $P_B^\star$-soundness against a cheating Bob of semi-random oblivious transfer, with a probability of at most $P_0^\star$, Bob can guess Alice's j and both parties accept. Considering that j is uniformly random and that $i = r \oplus j$, with a probability of

at most $P_B^\star$, Bob can guess Alice's i and both parties accept. Therefore, the $P_B^\star$-soundness against a cheating Bob of standard oblivious transfer is satisfied.

□

References

[1] Joseph F Fitzsimons. "Private quantum computation: an introduction to blind quantum computing and related protocols". npj Quantum Information **3**, 1–11 (2017).

[2] Dorit Aharonov, Michael Ben-Or, and Elad Eban. "Interactive proofs for quantum computations" (2008) arXiv:0810.5375.

[3] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. "Universal blind quantum computation". In 2009 50th Annual IEEE Symposium on Foundations of Computer Science. Pages 517–526. (2009).

[4] Tomoyuki Morimae and Keisuke Fujii. "Blind quantum computation protocol in which alice only makes measurements". Phys. Rev. A **87**, 050301 (2013).

[5] Ben W Reichardt, Falk Unger, and Umesh Vazirani. "Classical command of quantum systems". Nature **496**, 456–460 (2013).

[6] Atul Mantri, Tommaso F. Demarie, Nicolas C. Menicucci, and Joseph F. Fitzsimons. "Flow ambiguity: A path towards classically driven blind quantum computation". Phys. Rev. X **7**, 031004 (2017).

[7] Li Yu, Carlos A. Pérez-Delgado, and Joseph F. Fitzsimons. "Limitations on information-theoretically-secure quantum homomorphic encryption". Phys. Rev. A **90**, 050303 (2014).

[8] Anne Broadbent and Stacey Jeffery. "Quantum homomorphic encryption for circuits of low t-gate complexity". In Rosario Gennaro and Matthew Robshaw, editors, Advances in Cryptology – CRYPTO 2015. Pages 609–629. Berlin, Heidelberg (2015). Springer Berlin Heidelberg.

[9] Yfke Dulek, Christian Schaffner, and Florian Speelman. "Quantum homomorphic encryption for polynomial-sized circuits". In Matthew Robshaw and Jonathan Katz, editors, Advances in Cryptology – CRYPTO 2016. Pages 3–32. Berlin, Heidelberg (2016). Springer Berlin Heidelberg.

[10] Si-Hui Tan, Joshua A. Kettlewell, Yingkai Ouyang, Lin Chen, and Joseph F. Fitzsimons. "A quantum approach to homomorphic encryption". Scientific Reports **6**, 33467 (2016).

[11] Yingkai Ouyang, Si-Hui Tan, and Joseph F. Fitzsimons. "Quantum homomorphic encryption from quantum codes". Phys. Rev. A **98**, 042334 (2018).

[12] Urmila Mahadev. "Classical homomorphic encryption for quantum circuits". SIAM Journal on Computing **0**, FOCS18–189 (2020).

[13] Yingkai Ouyang and Peter P. Rohde. "A general framework for the composition of quantum homomorphic encryption & quantum error correction" (2022) arXiv:2204.10471.

[14] Craig Gentry. "Fully homomorphic encryption using ideal lattices". In Proceedings of the 41st annual ACM Symposium on Theory of computing. Pages 169–178. (2009).

[15] Craig Gentry. "A fully homomorphic encryption scheme". PhD thesis. Stanford University. (2009). url: crypto.stanford.edu/craig.

[16] Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. "I-hop homomorphic encryption and rerandomizable yao circuits". In Proceedings of the 30th Annual Conference on Advances in Cryptology. Pages 155–172. CRYPTO'10Berlin, Heidelberg (2010). Springer-Verlag.

[17] Baoz Barak and Zvika Brakerski. "The swiss army knife of cryptography" (2012) url: windowsontheory.org/2012/05/01/the-swiss-army-knife-of-cryptography/.

[18] Yehuda Lindell. "Tutorials on the foundations of cryptography: Dedicated to oded goldreich". Springer Publishing Company, Incorporated. (2017). 1st edition.

[19] Saeid Esmaeilzade, Nasrollah Pakniat, and Ziba Eslami. "A generic construction to build simple oblivious transfer protocols from homomorphic encryption schemes". The Journal of Supercomputing **78**, 72–92 (2022).

[20] Omer Reingold, Luca Trevisan, and Salil Vadhan. "Notions of reducibility between cryptographic primitives". In Moni Naor, editor, Theory of Cryptography. Pages 1–20. Berlin, Heidelberg (2004). Springer Berlin Heidelberg.

[21] Ching-Yi Lai and Kai-Min Chung. "On statistically-secure quantum homomorphic encryption". Quantum Info. Comput. **18**, 785–794 (2018).

[22] Michael Newman. "Further limitations on information-theoretically secure quantum homomorphic encryption" (2018) arXiv:1809.08719.

[23] Ashwin Nayak. "Optimal lower bounds for quantum automata and random access codes". In 40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039). Pages 369–376. (1999).

[24] Si-Hui Tan, Yingkai Ouyang, and Peter P. Rohde. "Practical somewhat-secure quantum somewhat-homomorphic encryption with coherent states". Phys. Rev. A **97**, 042308 (2018).

[25] Yingkai Ouyang, Si-Hui Tan, Joseph Fitzsimons, and Peter P. Rohde. "Homomorphic encryption of linear optics quantum computation on almost arbitrary states of light with asymptotically perfect security". Physical Review Research **2**, 013332 (2020).

[26] André Chailloux, Iordanis Kerenidis, and Jamie Sikora. "Lower bounds for quantum oblivious transfer". Quantum Info. Comput. **13**, 158–177 (2013).

[27] André Chailloux and Jamie Sikora. "Optimal bounds for semi-honest quantum oblivious transfer". Chicago Journal of Theoretical Computer Science **2016** (2016).

[28] Ryan Amiri, Robert Stárek, David Reichmuth, Ittoop V. Puthoor, Michal Mičuda, Ladislav Mišta, Jr., Miloslav Dušek, Petros Wallden, and Erika Andersson. "Imperfect 1-out-of-2 quantum oblivious transfer: Bounds, a protocol, and its experimental implementation". PRX Quantum **2**, 010335 (2021).

[29] Koenraad M. R. Audenaert and Milán Mosonyi. "Upper bounds on the error probabilities and asymptotic error exponents in quantum multiple state discrimination". Journal of Mathematical Physics **55**, 102201 (2014).

[30] Carl W. Helstrom. "Detection theory and quantum mechanics". Information and Control **10**, 254–291 (1967).

[31] Alexander S. Holevo. "Bounds for the quantity of information transmitted by a quantum communication channel". Problems of Information Transmission **9**, 177–183 (1973). url: http://mi.mathnet.ru/ppi903.

[32] John Watrous. "The theory of quantum information". Cambridge University Press. (2018).

[33] C.A. Fuchs and J. van de Graaf. "Cryptographic distinguishability measures for quantum-mechanical states". IEEE Transactions on Information Theory **45**, 1216–1227 (1999).

[34] A. Uhlmann. "The "transition probability" in the state space of a *-algebra". Reports on Mathematical Physics **9**, 273–279 (1976).

[35] Michael A Nielsen and Isaac Chuang. "Quantum computation and quantum information: 10th anniversary edition". Cambridge University Press. (2010).

[36] Hoi-Kwong Lo. "Insecurity of quantum secure computations". Phys. Rev. A **56**, 1154–1162 (1997).

[37] Roger Colbeck. "Impossibility of secure two-party classical computation". Phys. Rev. A **76**, 062308 (2007).

[38] Carlos Mochon. "Quantum weak coin flipping with arbitrarily small bias" (2007) arXiv:0711.4114.

[39] André Chailloux and Iordanis Kerenidis. "Optimal quantum strong coin flipping". In 2009 50th Annual IEEE Symposium on Foundations of Computer Science. Pages 527–533. IEEE (2009).

[40] Dorit Aharonov, André Chailloux, Maor Ganz, Iordanis Kerenidis, and Loïck Magnin. "A simpler proof of the existence of quantum weak coin flipping with arbitrarily small bias". SIAM Journal on Computing **45**, 633–679 (2016).

[41] Carl A. Miller. "The impossibility of efficient quantum weak coin flipping". In Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing. Pages 916–929. New York, NY, USA (2020). Association for Computing Machinery.

[42] Hoi-Kwong Lo and H. F. Chau. "Is quantum bit commitment really possible?". Phys. Rev. Lett. **78**, 3410–3413 (1997).

[43] Dominic Mayers. "Unconditionally secure quantum bit commitment is impossible". Phys. Rev. Lett. **78**, 3414–3417 (1997).