

# Communication Complexity of Private Simultaneous Quantum Messages Protocols

Akinori Kawachi ✉ 🏠 

Graduate School of Engineering, Mie University, Japan

Harumichi Nishimura ✉ 

Graduate School of Informatics/Institute for Advanced Study, Nagoya University, Japan

---

## Abstract

---

The private simultaneous messages (PSM) model is a non-interactive version of the multiparty secure computation (MPC), which has been intensively studied to examine the communication cost of the secure computation. We consider its quantum counterpart, the *private simultaneous quantum messages (PSQM)* model, and examine the advantages of quantum communication and prior entanglement of this model.

In the PSQM model,  $k$  parties  $P_1, \dots, P_k$  initially share a common random string (or entangled states in a stronger setting), and they have private classical inputs  $x_1, \dots, x_k$ . Every  $P_i$  generates a quantum message from the private input  $x_i$  and the shared random string (entangled states), and then sends it to the referee  $R$ . Receiving the messages from the  $k$  parties,  $R$  computes  $F(x_1, \dots, x_k)$  from the messages. Then,  $R$  learns nothing except for  $F(x_1, \dots, x_k)$  as the privacy condition.

We obtain the following results for this PSQM model. (i) We demonstrate that the privacy condition inevitably increases the communication cost in the two-party PSQM model as well as in the classical case presented by Applebaum, Holenstein, Mishra, and Shayevitz [*Journal of Cryptology* **33**(3), 916–953 (2020)]. In particular, we prove a lower bound  $(3 - o(1))n$  of the communication complexity in PSQM protocols with a shared random string for random Boolean functions of  $2n$ -bit input, which is larger than the trivial upper bound  $2n$  of the communication complexity without the privacy condition. (ii) We demonstrate a factor two gap between the communication complexity of PSQM protocols with shared entangled states and with shared random strings by designing a multiparty PSQM protocol with shared entangled states for a total function that extends the two-party equality function. (iii) We demonstrate an exponential gap between the communication complexity of PSQM protocols with shared entangled states and with shared random strings for a two-party *partial* function.

**2012 ACM Subject Classification** Theory of computation → Quantum computation theory; Theory of computation → Computational complexity and cryptography

**Keywords and phrases** Communication complexity, private simultaneous messages, quantum protocols, secure multi-party computation

**Funding** *Akinori Kawachi*: JSPS Grant-in-Aid for Scientific Research (A) Nos. 16H01705, 21H04879, (B) No. 17H01695, JSPS Grant-in-Aid for Young Scientists (B) No. 17K12640, and MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) Grant Number JPMXS0120319794.

*Harumichi Nishimura*: JSPS Grant-in-Aid for Scientific Research (A) Nos. 16H01705, 21H04879, (B) No. 19H04066, Grant-in-Aid for Transformative Research Areas No. 20H05966 and MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) Grant Number JPMXS0120319794.

**Acknowledgements** We thank the anonymous reviewers of ITC 2021 for helpful comments.

## 1 Introduction

**Background.** Communication complexity has been an important research area in theoretical computer science for more than four decades, aiming to understand the communication cost of computing functions in a distributed manner [31, 25]. Since the advent of quantum information science, quantum communication complexity has also been studied intensively to determine the advantage of quantum information processing over its classical counterparts. A number of studies have succeeded in demonstrating the quantum advantages from the early days of quantum complexity theory [7, 28, 8].

Recently, much attention has been given to studying the amount of communication overhead required to preserve privacy in the field of cryptography, particularly, multi-party secure computation (MPC), to explore the optimal communication cost for privacy from the viewpoint of communication complexity [13, 12]. MPC is commonly based on a general network model that has complex communication patterns (e.g., in which each of many parties can freely interact with the other parties bidirectionally) unlike standard models in communication complexity (e.g., in which two parties can exchange messages only with each other). Therefore, many studies have focused on a special class of MPC that has simpler communication patterns, such as *private simultaneous messages* (PSM) protocols [14, 21, 9, 2, 1].

The two-party version of the PSM model was first proposed by Feige, Kilian, and Naor [14], and was later extended by Ishai and Kushilevitz [21]. In the general setting of the PSM model, we consider  $k$  parties  $P_1, \dots, P_k$  and a unique referee  $R$ . The party  $P_i$  has its private input  $x_i$ , and all parties share a common random string  $r$ . Each  $P_i$  generates message  $m_i$  from  $x_i$  and  $r$ , and then, sends  $m_i$  to the referee  $R$  only once. Note that each party is not allowed to interact with other parties. The referee  $R$  receives the messages  $m_1, \dots, m_k$ , and computes an output value of a predetermined function  $F$ . The protocol generally has two properties *correctness* and *privacy*: Correctness signifies that the referee can compute  $F(x_1, \dots, x_k)$  correctly from the messages  $m_1, \dots, m_k$ , while privacy signifies that the referee  $R$  learns nothing except for  $F(x_1, \dots, x_k)$  from the received messages  $m_1, \dots, m_k$  in the information-theoretical sense.

In fact, the communication model of PSM protocols coincides with simultaneous message passing (SMP) protocols, which are known as traditional communication models in communication complexity [31, 25]. In the (number-in-hand) SMP model,  $k$  parties  $P_1, \dots, P_k$  that share a common random string  $r$  (and sometimes entangled states), send their messages  $m_1, \dots, m_k$  computed from individual inputs  $x_1, \dots, x_k$  and the referee computes  $F(x_1, \dots, x_k)$  from  $m_1, \dots, m_k$ , as performed in the PSM model. Note that the SMP model does not require the privacy condition unlike the PSM model. The communication complexity of SMP protocols has been widely studied from the viewpoint of classical/quantum information to demonstrate the power of quantum communication [8, 18, 16].

Two-party quantum SMP models were first studied by Buhrman, Cleve, Watrous, and de Wolf [8] in the setting that the two parties do not share any randomness or entanglement. In this model, they demonstrated that the quantum communication complexity of the equality function is exponentially smaller than in the classical case. This result has been strengthened in the literature [4, 15], and Gavinsky [16] demonstrated that there is a relational problem whose quantum communication complexity is exponentially smaller than that of the two-way classical communication model. However, the power of shared entanglement in the SMP model is unclear. In one of the few related studies, Gavinsky, Kempe, Regev, and de Wolf [18] demonstrated that there is a relational problem that has an exponential gap between quantum

SMP models with shared entanglement and without shared entanglement. However, the known maximum gap between them for *total functions* is only a constant multiplicative factor of 2 [20, 22].

Although various studies have examined quantum versions of MPC so far (e.g., [10, 29, 11]), to the best of the authors' knowledge, there has been no attempt to analyze quantum communication complexity under the privacy condition in a cryptographic setting, and such analysis is important to understand the advantages of quantum communication in a cryptographic setting.

**Contributions.** In this paper, we examine the power of quantum communication and shared entanglement under the information-theoretical privacy condition based on a standard communication model, namely, the PSM (or, equivalently, SMP) model. In particular, we propose a quantum counterpart of the classical PSM model called *private simultaneous quantum messages (PSQM)* model. In the PSQM model, parties  $P_1, \dots, P_k$  which have classical private inputs  $x_1, \dots, x_k$  share a common random string or entangled states in advance, and can send quantum messages to a quantum referee,  $R$ . Then,  $R$  computes a classical output value  $F(x_1, \dots, x_k)$  for a given function  $F$ .

In the PSM (and its related) model, there are few results on lower bounds of communication complexity [1, 13, 3]. As one of such results, Applebaum, Holenstein, Mishra, and Shayevitz [1] proved a lower bound  $(3 - o(1))n$  of the communication complexity for random functions  $F_n : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$  in the PSM model. In contrast, every function has the trivial upper bound  $2n$  in the SMP model (i.e., the PSM model without the privacy condition). This result implies that the privacy condition creates communication overhead in the PSM model for some functions. Our first result demonstrates that this communication overhead is inevitable even if the parties can send quantum messages as in the PSQM model.

► **Theorem 1.** *For a  $(1 - o(1))$  fraction of functions  $F_n : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ , the communication complexity of two-party PSQM protocols with shared randomness for  $F_n$  is at least  $3n - 2 \log n - O(1)$ .*

We also present a multiparty PSQM protocol for a total function that reduces the amount of quantum communication by half under the condition that the parties share entanglement compared to the case in which they do not share entanglement.

► **Theorem 2.** *For any even  $n$  and  $k$ , there is a total function  $F_n : (\{0, 1\}^n)^k \rightarrow \{0, 1\}$  such that the communication complexity of the  $k$ -party PSQM protocol with shared entanglement is at most  $kn/2$ , while that without shared entanglement is  $kn$ .*

Actually, this function matches the equality function for the two-party case. It is known that for the equality function, the two-party quantum SMP model with shared entanglement reduces the amount of quantum communication by half compared to the corresponding model without shared entanglement (e.g. [20]). Our result implies that this reduction still holds even if the privacy condition is required.

Moreover, we present a two-party PSQM protocol with shared entanglement for a *partial* function that reduces the amount of quantum communication exponentially compared to the case in which the parties do not share entanglement.

► **Theorem 3.** *There is a partial function  $F_n : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$  such that the communication complexity of the PSQM protocol with shared entanglement is  $O(\log n)$  while that without entanglement is  $\Omega(n)$ .*

**Related Work.** There have been several studies on quantum communication complexity with privacy conditions (e.g., [23, 17]), although they differed from a cryptographic setting.

For example, Gavinsky and Ito [17] considered the SMP model with privacy; however it considered the information leakage of quantum messages when the input was randomly chosen, while in the cryptographic setting, privacy should be retained for any input.

In a study related to the PSQM model, Brakerski and Yuen [6] constructed a quantum version of decomposable randomized encoding schemes. In fact, decomposable randomized encoding is equivalent to the PSM model from a communication-complexity perspective. They demonstrated how to garble a general quantum circuit on quantum inputs in a decomposable manner via a constant-depth quantum circuit. In contrast, our study focuses on the communication complexity of computing several classical functions on classical inputs in the communication model.

More recently, Morimae [27] investigated relationships between quantum randomized encoding and other quantum protocols including quantum computing verification and blind quantum computing. For example, he proved that a randomized encoding scheme of the BB84 state generation implies a two-round verification scheme of quantum computing with a classical verifier that additionally performs the encoding operation, and that a quantum randomized encoding scheme with a classical encoding operation implies violation of the no-cloning theorem. His target of quantum randomized encoding schemes is similar to that of [6], that is, encoding for quantum circuits on quantum inputs rather than classical functions on classical inputs.

## 2 Preliminaries

Let  $[n] := \{1, 2, \dots, n\}$ . For any two  $m$ -bit strings  $x = x_1 \cdots x_m$  and  $y = y_1 \cdots y_m$ , the product  $x \cdot y$  denotes  $\sum_{i \in [m]} x_i y_i \pmod{2}$ , and  $x \oplus y$  denotes the  $m$ -bit string whose  $i$ th bit is the XOR of  $x_i$  and  $y_i$ .

For any  $m$ -bit string  $x = x_1 x_2 \cdots x_m$ , let

$$\mathbf{p}(x) = x_1 + x_2 \alpha + \cdots + x_m \alpha^{m-1} \pmod{\mathfrak{q}_m} \quad (1)$$

be the corresponding polynomial over  $\mathbb{F}_2$ , where  $\mathfrak{q}_m$  is some irreducible polynomial of degree  $m$  over  $\mathbb{F}_2$ . Note that  $\mathbf{p}(x)$  is regarded as an element in  $\mathbb{F}_{2^m}$ , and  $\mathbf{p}$  is a one-to-one correspondence between  $\{0, 1\}^m \setminus \{0^m\}$  and the multiplicative group  $\mathbb{F}_{2^m}^*$ .

We assume the reader is familiar with the basics of quantum information and computation such as quantum states and quantum operations (see, e.g., [19, 26]). According to the standard notations, Pauli gates  $X$ ,  $Z$ , and the Hadamard gate  $H$  denote

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

respectively.

### 2.1 Private simultaneous quantum messages protocols

Private simultaneous quantum messages (PSQM) protocols are formally defined as follows.

► **Definition 4** (private simultaneous quantum messages (PSQM) protocols). *For positive integers  $n, k > 0$ , let  $n$  be the size parameter and  $k$  be the number of parties. Let  $F_n : \prod_{i=1}^k \mathcal{X}_{n,i} \rightarrow \mathcal{Y}_n$ . We say that a  $(k+1)$ -tuple  $\Pi = (P_1, \dots, P_k, R)$  of quantum algorithms is an  $\varepsilon$ -error  $k$ -party private simultaneous quantum messages (PSQM) protocol if the following holds: given an individual input  $x_i \in \mathcal{X}_{n,i}$  and shared random string  $r$  among  $P_1, \dots, P_k$ , the  $i$ th party  $P_i$  prepares a quantum message, represented as  $\rho_i = P_i(x_i, r)$ , in a Hilbert space*

$\mathcal{M}_{n,i}$  called a quantum register, and sends  $\mathcal{M}_{n,i}$  (or equivalently  $\rho_i$ ) to the party  $R$ , which is called the referee. Then, the following two properties hold:

1. **(Correctness)** The referee  $R$  outputs the classical value  $F_n(x_1, \dots, x_k) \in \mathcal{Y}_n$  using the received joint quantum register  $\mathcal{M}_n := \bigotimes_{i=1}^k \mathcal{M}_{n,i}$  with a probability of at least  $1 - \varepsilon$ .
2. **(Perfect Privacy)** There exists a quantum algorithm  $S_n$ , which is called the simulator, such that the output quantum state  $S_n(F_n(x_1, \dots, x_k))$  is identical to the quantum state in  $\mathcal{M}_n$  (before  $R$ ), namely,  $\bigotimes_{i=1}^k \rho_i$ .

We say that the protocol is exact when  $\varepsilon = 0$ .

If the shared random string  $r$  is replaced by a predetermined multipartite entangled quantum state  $|\Phi\rangle$  among the  $k$  parties, we say that  $\Pi$  is a PSQM protocol with a shared entangled state  $|\Phi\rangle$ , where the algorithms and the properties are similarly defined except that  $P_i$  prepares the message using its own part of  $|\Phi\rangle$  (instead of  $r$ ), and that the quantum state in  $\mathcal{M}_n$  is not a product state of the  $k$  local states in  $\mathcal{M}_{n,1}, \dots, \mathcal{M}_{n,k}$  any more.

The communication complexity of  $\Pi$  is defined by the total length  $\log \dim(\mathcal{M}_n)$  of the messages.

Let  $C_\varepsilon^{psm}(F_n)$  (resp.  $Q_\varepsilon^{psm}(F_n)$ ) be the  $\varepsilon$ -error classical (quantum) communication complexity of the problem  $F_n$  in the PSM (PSQM) model with a shared random string. Let  $C_\varepsilon^{psm,*}(F_n)$  (resp.  $Q_\varepsilon^{psm,*}(F_n)$ ) be the  $\varepsilon$ -error classical (quantum) communication complexity of  $F_n$  in the PSM (PSQM) model with shared entangled states (the PSM model with shared entangled states is defined similarly to the PSQM model with shared entangled states except that the messages sent to the referee are restricted to classical strings).

### 3 Communication Lower Bounds of Two-Party PSQM Protocols

In this section, we present the communication lower bounds of random functions for two-party PSQM protocols (Theorem 1).

The proof strategy is based on that of the classical case presented by Applebaum et al. [1]. The proof for the classical case considers two independent executions of a PSM protocol. It then evaluated the upper bounds of the collision probability, that is, the probability that the message in the first execution coincides with the one in the second execution, between two independent random messages. Because the collision probability is lower-bounded by the inverse of the size of the message domain, we can obtain the communication lower bound from the upper bound of the collision probability. Note that this argument is not available for quantum messages since they vary infinitely even over a finite number of qubits.

In order to extend the above argument to the case of quantum messages, we use the *purity*,  $\text{tr}\rho^2$ , of a quantum message  $\rho$  in a PSQM protocol instead of the collision probability. In accordance with its name, the purity is originally a measure of how pure a quantum state is. (For example, any pure state has a purity of 1, and the  $d$ -dimensional maximally mixed state has  $1/d$ .) It is easy to see that the purity of a quantum state  $\rho$  is lower-bounded by  $1/\dim(\rho)$ , and thus, we can obtain the communication lower bounds for a PSQM protocol by evaluating the upper bound of the purity of the quantum messages, similarly to the collision probability for a PSM protocol.

However, the purity of quantum messages is different from the collision probability between classical messages; thus, we must further adapt the proof technique in [1] to the purity. For example, while the collision probability is analyzed by combinatorial techniques in the proof of [1], we need to analyze the trace  $\text{tr}\rho^2$  combinatorially by extending the original proof (Claim 7). Also, the proof technique in [1] uses a unique collision (which is obtained from the property called non-degeneracy that random functions have with high probability) between

two messages in two independent executions with any fixed shared random string. Instead of the unique collision, we consider weighted collisions defined from the inner product of two quantum messages and extend the original argument for the weighted collisions (Lemma 9).

Before discussing the details of the proof, we provide several technical definitions and notation required for the proof of the lower bounds. In this section, we denote  $\mathcal{X}_{n,i}$  by  $\mathcal{X}_i$ . We use  $\rho(x_1, x_2; r) = \rho_1(x_1; r) \otimes \rho_2(x_2; r)$  to the entire quantum message sent from  $P_1$  and  $P_2$  on individual inputs  $x_1 \in \mathcal{X}_1$  and  $x_2 \in \mathcal{X}_2$  with a shared random string  $r$  to  $R$ , where  $\rho_1(x_1; r)$  denotes  $P_1$ 's message and  $\rho_2(x_2; r)$  denotes  $P_2$ 's message.

Let  $\mu$  be a distribution over  $\mathcal{X}_1 \times \mathcal{X}_2$  with marginal distributions  $\mu_1$  and  $\mu_2$ . We define  $\text{Supp}(\mu)$  for a distribution  $\mu$  as a set  $\{x : \Pr_{X \sim \mu}[X = x] > 0\}$ . We say that function  $F_n$  is non-degenerate under distribution  $\mu$  if for every distinct  $x_1 \in \text{Supp}(\mu_1)$  and  $x'_1 \in \text{Supp}(\mu_1)$ , there exists  $x_2 \in \text{Supp}(\mu_2)$  such that  $F_n(x_1, x_2) \neq F_n(x'_1, x_2)$  and for every distinct  $x_2 \in \text{Supp}(\mu_2)$  and  $x'_2 \in \text{Supp}(\mu_2)$  there exists  $x_1$  such that  $F_n(x_1, x_2) \neq F_n(x_1, x'_2)$ . We say that  $F_n$  is non-degenerate if the above holds when replacing  $\text{Supp}(\mu_1)$  and  $\text{Supp}(\mu_2)$  by  $\mathcal{X}_1$  and  $\mathcal{X}_2$ , respectively.

A rectangle  $\mathcal{R}$  of size  $k \times \ell$  over  $\mathcal{X}_1 \times \mathcal{X}_2$  is defined as  $((x_{1,1}, \dots, x_{1,k}), (x_{2,1}, \dots, x_{2,\ell}))$ , where  $x_{1,i} \in \mathcal{X}_1, x_{2,j} \in \mathcal{X}_2$  for every  $i, j$ ,  $x_{1,i} \neq x_{1,i'}$  for every distinct  $i, i'$ , and  $x_{2,j} \neq x_{2,j'}$  for every distinct  $j, j'$ . We say that two rectangles  $\mathcal{R} = ((x_{1,1}, \dots, x_{1,k}), (x_{2,1}, \dots, x_{2,\ell}))$  and  $\mathcal{R}' = ((x'_{1,1}, \dots, x'_{1,k}), (x'_{2,1}, \dots, x'_{2,\ell}))$  are  $\mathcal{X}_1$ -disjoint (resp.  $\mathcal{X}_2$ -disjoint) if  $x_{1,i} \neq x'_{1,i}$  for every  $i \in [k]$  (resp. if  $x_{2,j} \neq x'_{2,j}$  for every  $j \in [\ell]$ ). In particular, we say that  $\mathcal{R}$  and  $\mathcal{R}'$  are disjoint if they are either  $\mathcal{X}_1$ -disjoint or  $\mathcal{X}_2$ -disjoint.

For a rectangle  $\mathcal{R} = ((x_{1,1}, \dots, x_{1,k}), (x_{2,1}, \dots, x_{2,\ell}))$ , let  $F_n[\mathcal{R}]$  be a matrix whose  $(i, j)$ -entry is  $F_n(x_{1,i}, x_{2,j})$ , and let  $\mu(\mathcal{R}) = \sum_{i \in [k], j \in [\ell]} \mu(x_{1,i}, x_{2,j})$ . We say that  $\mathcal{R}$  is similar to  $\mathcal{R}'$  if  $F_n[\mathcal{R}] = F_n[\mathcal{R}']$ . We define

$$\alpha(\mu) := \max_{(\mathcal{R}_1, \mathcal{R}_2)} \min\{\mu(\mathcal{R}_1), \mu(\mathcal{R}_2)\},$$

where the maximum ranges over all pairs of similar disjoint rectangles  $(\mathcal{R}_1, \mathcal{R}_2)$ . In addition,

$$\beta(\mu) := \min_y \Pr_{(X_1, X_2), (X'_1, X'_2) \sim \mu} [(X_1, X_2) \neq (X'_1, X'_2) \mid F_n(X_1, X_2) = F_n(X'_1, X'_2) = y],$$

where  $(X_1, X_2)$  and  $(X'_1, X'_2)$  are independent.

We can demonstrate the communication lower bound in Theorem 1 from the following main technical lemma combined with an appropriate function  $F_n$ , which is provided in the study by Applebaum et al. [1].

► **Lemma 5.** *For every non-degenerate function  $F_n : \mathcal{X}_1 \times \mathcal{X}_2 \rightarrow \{0, 1\}$ , we have*

$$Q_0^{psm}(F_n) \geq \max_{\mu} (\log(\alpha(\mu)^{-1}) + H_{\infty}(\mu) - \log(\beta(\mu)^{-1})) - 1,$$

where  $\mu$  is taken over all distributions over  $\mathcal{X}_1 \times \mathcal{X}_2$  under which  $F_n$  is non-degenerate, and  $H_{\infty}(\mu)$  is the min-entropy of  $\mu$ .

From the previous study [1], we can obtain the appropriate function by selecting a function at random, as illustrated in the following theorem.

► **Theorem 6** (Applebaum et al. [1]). *For a  $(1 - o(1))$  fraction of the functions  $F_n : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ ,  $F_n$  is non-degenerate and  $|\mathcal{R}| \leq 2^n \cdot n^2$  holds for every pair  $(\mathcal{R}, \mathcal{R}')$  of similar disjoint rectangles.*

Considering the uniform distribution  $U$  over  $\{0, 1\}^n \times \{0, 1\}^n$ , the communication lower bound from Lemma 5 of PSQM protocols for  $F_n : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$  is bounded by  $\log(\alpha(U)^{-1}) + H_\infty(U) - \log(\beta(U)^{-1}) - 1$ . By Theorem 6, we can easily see that this bound is  $3n - 2 \log n - O(1)$  for a  $(1 - o(1))$  fraction of the functions  $\{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ , as given in Theorem 1.

Now, we provide the proof of the main technical lemma.

**Proof of Lemma 5.** From the correctness, the referee  $R$  outputs  $F_n(x_1, x_2)$  for the received quantum message  $\rho(x_1, x_2; r)$  for every  $x_1, x_2$  and every  $r$ . Without loss of generality, we can assume that  $P_1$  and  $P_2$  generate pure states  $|\psi_1(x_1; r)\rangle$  and  $|\psi_2(x_2; r)\rangle$  with a shared randomness  $r$ , respectively.

This assumption is justified as follows. Suppose that  $P_1$  and  $P_2$  generate mixed states  $\rho_1(x_1; r)$  and  $\rho_2(x_2; r)$  as their messages on inputs  $x_1, x_2$  and a shared random string  $r$ . By the spectral decomposition, we have  $\rho_1(x_1; r) = \sum_i p_i |\psi_1^{(i)}(x_1; r)\rangle \langle \psi_1^{(i)}(x_1; r)|$  and  $\rho_2(x_2; r) = \sum_j q_j |\psi_2^{(j)}(x_2; r)\rangle \langle \psi_2^{(j)}(x_2; r)|$ . The joint message state is

$$\rho(x_1, x_2; r) := \sum_{i,j} p_i q_j |\psi_1^{(i)}(x_1; r), \psi_2^{(j)}(x_2; r)\rangle \langle \psi_1^{(i)}(x_1; r), \psi_2^{(j)}(x_2; r)|$$

and its probabilistic mixture over the shared random string  $r$  is

$$\rho(x_1, x_2) := \sum_r \pi(r) \rho(x_1, x_2; r) = \sum_{i,j,r} p_i q_j \pi(r) |\psi_1^{(i)}(x_1; r), \psi_2^{(j)}(x_2; r)\rangle \langle \psi_1^{(i)}(x_1; r), \psi_2^{(j)}(x_2; r)|.$$

Rephrasing the probability distribution  $\{\pi(r)p_i q_j\}_{i,j,r}$  and the pure message states  $|\psi_1^{(i)}(x_1; r)\rangle$ ,  $|\psi_2^{(j)}(x_2; r)\rangle$  to  $\{\pi(r)\}_r$  and  $|\psi_1(x_1; r)\rangle$ ,  $|\psi_2(x_2; r)\rangle$  respectively, we can assume that they generate pure states as their messages from the beginning.

We denote by  $|\psi(x_1, x_2; r)\rangle$  their joint state  $|\psi_1(x_1; r)\rangle \otimes |\psi_2(x_2; r)\rangle$ . Namely, we set

$$\rho(x_1, x_2; r) := |\psi(x_1, x_2; r)\rangle \langle \psi(x_1, x_2; r)| = |\psi_1(x_1; r)\rangle \langle \psi_1(x_1; r)| \otimes |\psi_2(x_2; r)\rangle \langle \psi_2(x_2; r)|. \quad (2)$$

In addition, we set

$$\rho(x_1, x_2) := \sum_r \pi(r) \rho(x_1, x_2; r), \quad (3)$$

where  $\pi(r)$  denotes the probability that  $r$  is selected as a shared random string under the uniform distribution.

As mentioned above, we use the purity as a collision measure of quantum messages in order to obtain lower bounds of quantum message length from upper bounds of the purity. We set  $\rho := \sum_{x_1, x_2} \mu(x_1, x_2) \rho(x_1, x_2)$ . We then have

$$\begin{aligned} \frac{1}{\dim(\mathcal{M})} &\leq \text{tr} \rho^2 = \text{tr} \left( \sum_{x_1, x_2} \mu(x_1, x_2) \rho(x_1, x_2) \right)^2 \\ &= \text{tr} \sum_{x_1, x_2, x'_1, x'_2} \mu(x_1, x_2) \rho(x_1, x_2) \mu(x'_1, x'_2) \rho(x'_1, x'_2). \end{aligned} \quad (4)$$

Then, the purity of  $\rho$  is upper-bounded as follows.

▷ **Claim 7.**

$$\text{tr} \rho^2 \leq \beta(\mu)^{-1} \text{tr} \sum_{(x_1, x_2) \neq (x'_1, x'_2)} \mu(x_1, x_2) \rho(x_1, x_2) \mu(x'_1, x'_2) \rho(x'_1, x'_2).$$

The proof of this claim is done by a combinatorial analysis of the trace as a quantum counterpart of the analysis of the collision probability in [1]. The detailed proof will be given in Appendix A.

Next, we consider an upper bound of

$$\text{tr} \sum_{(x_1, x_2) \neq (x'_1, x'_2)} \mu(x_1, x_2) \rho(x_1, x_2) \mu(x'_1, x'_2) \rho(x'_1, x'_2). \quad (5)$$

Actually, we show that for every  $r$  and  $r'$ ,

$$\text{tr} \sum_{(x_1, x_2) \neq (x'_1, x'_2)} \mu(x_1, x_2) \rho(x_1, x_2; r) \mu(x'_1, x'_2) \rho(x'_1, x'_2; r')$$

is at most  $2\alpha(\mu)2^{-H_\infty(\mu)}$  as this implies that Eq. (5) is also at most  $2\alpha(\mu)2^{-H_\infty(\mu)}$  (by Eq. (3)). This completes the proof of Lemma 5 by Claim 7 and Eq. (4).

Now we fix any  $r$  and  $r'$ . From Eq. (2) and the union bound, we have

$$\begin{aligned} & \text{tr} \sum_{(x_1, x_2) \neq (x'_1, x'_2)} \mu(x_1, x_2) \rho(x_1, x_2; r) \mu(x'_1, x'_2) \rho(x'_1, x'_2; r') \\ &= \sum_{(x_1, x_2) \neq (x'_1, x'_2)} \mu(x_1, x_2) \mu(x'_1, x'_2) |\langle \psi_1(x_1; r) | \psi_1(x'_1; r') \rangle|^2 \cdot |\langle \psi_2(x_2; r) | \psi_2(x'_2; r') \rangle|^2 \\ &\leq \sum_{x_1 \neq x'_1, x_2, x'_2} \mu(x_1, x_2) \mu(x'_1, x'_2) |\langle \psi_1(x_1; r) | \psi_1(x'_1; r') \rangle|^2 \cdot |\langle \psi_2(x_2; r) | \psi_2(x'_2; r') \rangle|^2 \\ &\quad + \sum_{x_1, x'_1, x_2 \neq x'_2} \mu(x_1, x_2) \mu(x'_1, x'_2) |\langle \psi_1(x_1; r) | \psi_1(x'_1; r') \rangle|^2 \cdot |\langle \psi_2(x_2; r) | \psi_2(x'_2; r') \rangle|^2. \quad (6) \end{aligned}$$

It suffices to show that the first term of the right-hand of Eq. (6) is at most  $\alpha(\mu)2^{-H_\infty(\mu)}$  from the symmetry of  $P_1$  and  $P_2$ .

Note that we can regard the referee as a POVM  $R = \{R_y\}_{y \in \{0,1\}}$ . The following claim demonstrates that the referee is projective in the two-party PSQM setting. (Its proof will be given in Appendix A.)

▷ **Claim 8.** The referee  $R = \{R_y\}_{y \in \{0,1\}}$  is a PVM.

In the classical case of [1], Applebaum et al. used the fact that for every  $x_1$  and every  $r, r'$  there exists at most one  $z$  such that  $|\psi_1(x_1; r)\rangle = |\psi_1(z; r')\rangle$  if  $|\psi_1(x_1; r)\rangle, |\psi_1(z; r')\rangle$  are classical; that is, either  $\langle \psi_1(x_1; r) | \psi_1(z; r') \rangle = 0$  or  $\langle \psi_1(x_1; r) | \psi_1(z; r') \rangle = 1$ , which can be derived from the non-degeneracy of  $F_n$ . However, we cannot demonstrate the same fact for quantum messages. Instead, we can prove the following relaxed version of the fact for quantum messages.

► **Lemma 9.** *If  $F_n$  is non-degenerate, we have*

$$\sum_{z \neq x_1} |\langle \psi_1(x_1; r) | \psi_1(z; r') \rangle|^2 \leq 1$$

for every  $r, r'$  and every  $x_1$ . Similarly

$$\sum_z |\langle \psi_2(x_2; r) | \psi_2(z; r') \rangle|^2 \leq 1$$

for every  $r, r'$  and every  $x_2$ .



The proof of this lemma will be given in Appendix A.

Let  $w_1(x_1, x'_1) := |\langle \psi_1(x_1; r) | \psi_1(x'_1; r') \rangle|^2$  and let  $w_2(x_2, x'_2) := |\langle \psi_2(x_2; r) | \psi_2(x'_2; r') \rangle|^2$ . We say that  $x_1$  collides with  $x'_1$  if  $w_1(x_1, x'_1) > 0$ . Similarly, we say that  $x_2$  collides with  $x'_2$  if  $w_2(x_2, x'_2) > 0$ .

Now, our final goal is to upper-bound

$$\sum_{x_1 \neq x'_1, x_2, x'_2} \mu(x_1, x_2) \mu(x'_1, x'_2) w_1(x_1, x'_1) w_2(x_2, x'_2). \quad (7)$$

Let  $C(x_1)$  be the set of the elements in  $\mathcal{X}_1$  with which  $x_1$  collides except for  $x_1$  itself. Similarly, let  $C(x_2)$  be the set of the elements in  $\mathcal{X}_2$  with which  $x_2$  collides (note that  $C(x_2)$  may contain  $x_2$ ).

Let  $\mathbf{x}_1 := (x_1 : C(x_1) \neq \emptyset)$  with an arbitrary (e.g., lexicographical) order in  $\mathcal{X}_1$ . We denote  $\mathbf{x}_1 = (u_1, u_2, \dots, u_k)$ . Then, we select any element  $\mathbf{x}'_1 = (u'_1, u'_2, \dots, u'_k)$  from  $C(u_1) \times \dots \times C(u_k)$ . Note that  $u_i$  collides with  $u'_i$  and  $u_i \neq u'_i$  for every  $i$ . Similarly, let  $\mathbf{x}_2 := (x_2 : C(x_2) \neq \emptyset) = (v_1, v_2, \dots, v_\ell)$  with an arbitrary order in  $\mathcal{X}_2$ , and we then select any element  $\mathbf{x}'_2 = (v'_1, v'_2, \dots, v'_\ell)$  from  $C(v_1) \times \dots \times C(v_\ell)$ .

Then, we can show that for every choice of  $\mathbf{x}'_1$  and  $\mathbf{x}'_2$ , we have

$$\sum_{i,j} \mu(u_i, v_j) \mu(u'_i, v'_j) \leq \alpha(\mu) 2^{-H_\infty(\mu)}.$$

The reason is as follows. We consider two rectangles  $\mathcal{R} := (\mathbf{x}_1, \mathbf{x}_2)$  and  $\mathcal{R}' := (\mathbf{x}'_1, \mathbf{x}'_2)$ . We observe that  $R(|\psi_1(x_1; r)\rangle |\psi_2(x_2; r)\rangle) = R(|\psi_1(x'_1; r')\rangle |\psi_2(x'_2; r')\rangle)$  (where  $R(|\varphi\rangle)$  denotes the classical value that  $R$  outputs on input  $|\varphi\rangle$ ) if  $x_1$  collides with  $x'_1$  and  $x_2$  collides with  $x'_2$  from the perfect correctness. Therefore,  $\mathcal{X}_1$ -disjoint rectangles  $\mathcal{R}$  and  $\mathcal{R}'$  are similar; that is,  $F_n[\mathcal{R}] = F_n[\mathcal{R}']$ . Without loss of generality, we can assume that  $\mu(\mathcal{R}) \leq \mu(\mathcal{R}')$ . Hence, we have  $\mu(\mathcal{R}) \leq \alpha(\mu)$ . Thus, we can see that for random variables  $X_1, X_2, X'_1, X'_2$

$$\begin{aligned} \sum_{i,j} \mu(u_i, v_j) \mu(u'_i, v'_j) &= \sum_{i,j} \Pr [(X_1, X_2) = (u_i, v_j) \wedge (X'_1, X'_2) = (u'_i, v'_j)] \\ &\leq \max_{(x_1, x_2)} \mu(x_1, x_2) \sum_{i,j} \Pr [(X_1, X_2) = (u_i, v_j)] \\ &\leq 2^{-H_\infty(\mu)} \alpha(\mu). \end{aligned}$$

Furthermore, it holds for every  $i, j$  that

$$\begin{aligned} \sum_{u'_i \in C(u_i), v'_j \in C(v_j)} w_1(u_i, u'_i) w_2(v_j, v'_j) &= \sum_{u'_i \in C(u_i)} w_1(u_i, u'_i) \left( \sum_{v'_j \in C(v_j)} w_2(v_j, v'_j) \right) \\ &\leq \sum_{u'_i \in C(u_i)} w_1(u_i, u'_i) \leq 1 \end{aligned}$$

from Lemma 9. Thus, we have

$$\begin{aligned}
 & \sum_{x_1 \neq x'_1, x_2, x'_2} \mu(x_1, x_2) \mu(x'_1, x'_2) w_1(x_1, x'_1) w_2(x_2, x'_2) \\
 &= \sum_{i,j} \sum_{u'_i \in C(u_i), v'_j \in C(v_j)} \mu(u_i, v_j) \mu(u'_i, v'_j) w_1(u_i, u'_i) w_2(v_j, v'_j) \\
 &\leq \sum_{i,j} \mu(u_i, v_j) \mu(\hat{u}_i, \hat{v}_j) \sum_{u'_i \in C(u_i), v'_j \in C(v_j)} w_1(u_i, u'_i) w_2(v_j, v'_j) \\
 &\leq \sum_{i,j} \mu(u_i, v_j) \mu(\hat{u}_i, \hat{v}_j) \\
 &\leq \alpha(\mu) 2^{-H_\infty(\mu)},
 \end{aligned}$$

where  $\mu(\hat{u}_i, \hat{v}_j) = \max_{u'_i \in C(u_i), v'_j \in C(v_j)} \mu(u'_i, v'_j)$ . Eventually, an upper bound of Eq. (7) is  $\alpha(\mu) 2^{-H_\infty(\mu)}$ . ◀

#### 4 Power of Shared Entanglement for Total Functions

In this section, we prove Theorem 2, which implies a factor two gap between PSQMs with shared entanglement and without shared entanglement for a total function. The main part of Theorem 2 provides a  $k$ -party PSQM protocol for a total function  $GEQ_{2l} : (\{0, 1\}^{2l})^k \rightarrow \{0, 1\}$  defined by

$$GEQ_{2l}(x_1, x_2, \dots, x_k) = \begin{cases} 1 & (\sum_{j=1}^k x_j^1 = \sum_{j=1}^k x_j^2 = \dots = \sum_{j=1}^k x_j^{2l-1} = \sum_{j=1}^k x_j^{2l} = 0), \\ 0 & (\text{otherwise}), \end{cases}$$

where each  $x_j = x_j^1 x_j^2 \dots x_j^{2l-1} x_j^{2l}$  is an element of  $\{0, 1\}^{2l}$ , and the summation is taken over  $\mathbb{F}_2$ . To reduce the communication complexity from the trivial  $2kl$  qubits to  $kl$  qubits, we encode half of the input bits by bit flipping of the shared state  $\frac{1}{\sqrt{2}}(|0^k\rangle + |1^k\rangle)$  (called the  $k$ -qubit GHZ state) among the  $k$  parties, and the other half by phase flipping of the state, by a method similar to superdense coding (e.g., see [26]). More precisely, we exploit an encoding similar to two-party quantum SMP protocols with shared entangled states to compute the equality function [20]. However, this is not sufficient for PSQM protocols. To convert quantum SMP protocols into PSQM protocols, we further use shared randomness among the  $k$  parties, and hide the input strings from the referee except for the output of the function  $GEQ_{2l}$ . This hiding can be shown to be possible by multiplying a random element in  $\mathbb{F}_{2^{2l}}^*$  by the element in  $\mathbb{F}_{2^{2l}}^*$  that corresponds to the input  $x_j$ .

For the proof of Theorem 2, we first consider a PSQM protocol for a finite function. Let  $Sum_2 : (\{0, 1\}^2)^k \rightarrow \{0, 1\}^2$  be

$$Sum_2(x_1, x_2, \dots, x_k) = \left( \sum_{j=1}^k x_j^1, \sum_{j=1}^k x_j^2 \right),$$

where each  $x_j = x_j^1 x_j^2$  is an element of  $\{0, 1\}^2$ , and the summation is taken over  $\mathbb{F}_2$ .

► **Lemma 10.** *For any even (resp. odd)  $k$ ,  $Q_0^{psm,*}(Sum_2) \leq k$  (resp.  $\leq k + 1$ ).*

**Proof.** First, we consider the case in which  $k$  is even. The quantum protocol is as follows.

**Protocol  $\mathcal{P}_{Sum_2}$ :**

0. All the parties share the entangled state

$$\frac{1}{\sqrt{2}} \left( \bigotimes_{j=1}^k |0\rangle_{Q_j} + \bigotimes_{j=1}^k |1\rangle_{Q_j} \right),$$

where the single-qubit register  $Q_j$  is owned by party  $P_j$ . Moreover, the parties share a  $k$ -bit string  $r = r_1 r_2 \cdots r_k$  such that  $\sum_{j=1}^k r_j = 0$ .

1. Each party  $P_j$  applies  $Z$  on  $Q_j$  if  $x_j^2 = 1$ . The resulting state is

$$\frac{1}{\sqrt{2}} \left( \bigotimes_{j=1}^k |0\rangle_{Q_j} + \bigotimes_{j=1}^k (-1)^{\sum_{j=1}^k x_j^2} |1\rangle_{Q_j} \right).$$

2. Each party  $P_j$  applies  $X$  on  $Q_j$  if  $x_j^1 \oplus r_j = 1$ . The resulting state is

$$\frac{1}{\sqrt{2}} \left( \bigotimes_{j=1}^k |x_j^1 \oplus r_j\rangle_{Q_j} + (-1)^{\sum_{j=1}^k x_j^2} \bigotimes_{j=1}^k |x_j^1 \oplus r_j \oplus 1\rangle_{Q_j} \right). \quad (8)$$

3. Each party  $P_j$  sends  $Q_j$  to the referee  $R$ .

4.  $R$  measures quantum registers  $Q_1, Q_2, \dots, Q_k$  in the basis

$$\left\{ |\Phi(y_1, y_2, \dots, y_{k-1}, z)\rangle := \frac{1}{\sqrt{2}} (|y_1, y_2, \dots, y_{k-1}, 0\rangle + (-1)^z |y_1 \oplus 1, y_2 \oplus 1, \dots, y_{k-1} \oplus 1, 1\rangle) \right\},$$

and let  $y_1 y_2 \cdots y_{k-1} z$  be the measurement result.

5.  $R$  outputs the two bits  $\sum_{j=1}^{k-1} y_j$  and  $z$ .

**Correctness:** The second bit of the output of  $R$  is  $z = \sum_{j=1}^k x_j^2$ , as desired. For the first bit, we consider two cases: (i)  $x_k^1 \oplus r_k = 0$  and (ii)  $x_k^1 \oplus r_k = 1$ . We first consider case (i). Then,  $y_j = x_j^1 \oplus r_j$  for  $j = 1, 2, \dots, k-1$ , and we thus obtain the desired output

$$\sum_{j=1}^{k-1} y_j = \sum_{j=1}^{k-1} x_j^1 \oplus r_j = \sum_{j=1}^k x_j^1 \oplus r_j = \sum_{j=1}^k x_j^1,$$

where the second inequality originates from  $x_k^1 \oplus r_k = 0$ , and the last equality originates from  $\sum_{j=1}^k r_k = 0$ . For case (ii),  $y_j = x_j^1 \oplus r_j \oplus 1$  for  $j = 1, 2, \dots, k-1$ , and we thus obtain the desired output

$$\sum_{j=1}^{k-1} y_j = \sum_{j=1}^{k-1} x_j^1 \oplus r_j \oplus 1 = \left( \sum_{j=1}^{k-1} x_j^1 \oplus r_j \right) \oplus 1 = \sum_{j=1}^k x_j^1 \oplus r_j = \sum_{j=1}^k x_j^1,$$

where the second equality originates from the fact that  $k$  is even, the third equality originates from  $x_k^1 \oplus r_k = 1$ , and the last equality originates from  $\sum_{j=1}^k r_k = 0$ .

**Privacy:** Let the output of  $Sum_2$  be  $(b_1, b_2)$ , where  $b_1 = \sum_{j=1}^k x_j^1$  and  $b_2 = \sum_{j=1}^k x_j^2$ . As  $R$  has no knowledge about  $r_1, \dots, r_k$  except that the sum is 0, we can observe that the quantum state that  $R$  receives (represented by Eq. (8)) is taken from the set of  $2^{k-2}$  orthogonal pure states

$$\left\{ |\Phi(y_1, \dots, y_{k-1}, b_2)\rangle : \sum_{j=1}^{k-1} y_j = b_1 \right\}$$

(up to the total phase) uniformly at random. Thus, the simulator can simulate the distribution of the message given the output of  $Sum_2$ .

In the case in which  $k$  is odd, the last party  $P_k$  prepares an extra two-bit string  $x_{k+1} = 00$ , and  $\mathcal{P}_{Sum_2}$  is run for the  $(k+1)$ -party case, where  $P_k$  also plays the role of the party  $P_{k+1}$ .  $\blacktriangleleft$

Next, we present the main lemma for Theorem 2.

► **Lemma 11.** *For any even (resp. odd)  $k$ ,  $Q_0^{psm,*}(GEQ_{2l}) \leq kl$  (resp.  $\leq (k+1)l$ ).*

**Proof.** We only demonstrate the case in which  $k$  is even (as the odd case is considered similarly to the proof of Lemma 10). The quantum protocol is as follows.

**Protocol  $\mathcal{P}_{GEQ_{2l}}$ :**

0. All parties share the entangled state

$$\bigotimes_{i=1}^l \left( \frac{1}{\sqrt{2}} \left( \bigotimes_{j=1}^k |0\rangle_{Q_j^i} + \bigotimes_{j=1}^k |1\rangle_{Q_j^i} \right) \right),$$

where the single-qubit registers  $Q_j^1, \dots, Q_j^l$  are owned by party  $P_j$ . Moreover, they share  $l$   $k$ -bit strings  $r^i := r_1^i r_2^i \dots r_k^i$  such that  $\sum_{j=1}^k r_j^i = 0$  ( $i = 1, 2, \dots, l$ ), and a non-zero  $2l$ -bit string  $r' = r'_1 r'_2 \dots r'_{2l-1} r'_{2l}$ .

1. Each party  $P_j$  computes the  $2l$ -bit string  $a_j = a_j^1 a_j^2 \dots a_j^{2l}$  defined as  $\mathbf{p}(a_j) = \mathbf{p}(r')\mathbf{p}(x_j)$ .
2. Each party  $P_j$  applies  $Z$  on  $Q_j^i$  if  $a_j^{2i} = 1$ . The resulting state is

$$\bigotimes_{i=1}^l \left( \frac{1}{\sqrt{2}} \left( \bigotimes_{j=1}^k |0\rangle_{Q_j^i} + \bigotimes_{j=1}^k (-1)^{\sum_{j=1}^k a_j^{2i}} |1\rangle_{Q_j^i} \right) \right).$$

3. Each party  $P_j$  applies  $X$  on  $Q_j^i$  if  $a_j^{2i-1} \oplus r_j^i = 1$ . The resulting state is

$$\bigotimes_{i=1}^l \left( \frac{1}{\sqrt{2}} \left( \bigotimes_{j=1}^k |a_j^{2i-1} \oplus r_j^i\rangle_{Q_j^i} + (-1)^{\sum_{j=1}^k a_j^{2i}} \bigotimes_{j=1}^k |a_j^{2i-1} \oplus r_j^i \oplus 1\rangle_{Q_j^i} \right) \right). \quad (9)$$

4. Each party  $P_j$  sends  $l$  quantum registers  $Q_j^1, \dots, Q_j^l$  to  $R$ .
5.  $R$  measures  $kl$  quantum registers  $Q_1^1, \dots, Q_k^1, \dots, Q_1^l, \dots, Q_k^l$  in the basis

$$B := \left\{ \bigotimes_{j=1}^l |\Phi(y_1^i, \dots, y_{k-1}^i, z^i)\rangle : y_1^i \dots y_{k-1}^i z^i \in \{0, 1\}^k \text{ for every } i \in [l] \right\},$$

and let  $y_1^i y_2^i \dots y_{k-1}^i z^i$  ( $i = 1, \dots, l$ ) be the measurement results.

6.  $R$  accepts if  $\left( \sum_{j=1}^{k-1} y_j^i \right) = z^i = 0$  for all  $i = 1, \dots, l$  and rejects otherwise.

**Correctness:** Note that  $(\sum_{j=1}^k x_j^1, \dots, \sum_{j=1}^k x_j^{2l}) = (0, \dots, 0)$  if and only if  $(\sum_{j=1}^k a_j^1, \dots, \sum_{j=1}^k a_j^{2l}) = (0, \dots, 0)$ , since

$$\mathbf{p} \left( \left( \sum_{j=1}^k a_j^1, \dots, \sum_{j=1}^k a_j^{2l} \right) \right) = \mathbf{p}(r') \mathbf{p} \left( \left( \sum_{j=1}^k x_j^1, \dots, \sum_{j=1}^k x_j^{2l} \right) \right). \quad (10)$$

Now, the correctness of  $\mathcal{P}_{Sum_2}$  in Lemma 10 also guarantees the correctness of  $\mathcal{P}_{GEQ_{2l}}$ .

**Privacy:** First, we consider the case in which  $GEQ_{2l}(x_1, x_2, \dots, x_k) = 0$ : that is,  $(\sum_{j=1}^k x_j^1, \dots, \sum_{j=1}^k x_j^{2l}) = (0, \dots, 0)$ . Then, as demonstrated in Eq. (10),  $(a_1, a_2, \dots, a_k)$  satisfies  $(\sum_{j=1}^k a_j^1, \dots, \sum_{j=1}^k a_j^{2l}) = (0, \dots, 0)$ . Moreover,  $(a_1^{2^{i-1}}, a_2^{2^{i-1}}, \dots, a_k^{2^{i-1}})$  is uniformly randomized by  $r^i$  in Step 3 under the restriction that the sum is 0. Thus, the quantum state that  $R$  receives (represented by Eq. (9)) is taken from the set of  $2^{(k-2)l}$  orthogonal pure states

$$\left\{ \bigotimes_{i=1}^l |\Phi(y_1^i, \dots, y_{k-1}^i, 0)\rangle : \sum_{j=1}^{k-1} y_j^i = 0 \text{ for every } i \in [l] \right\}$$

(up to the total phase) uniformly at random. Second, we consider the case in which  $GEQ_{2l}(x_1, x_2, \dots, x_k) = 1$ , i.e.,  $(\sum_{j=1}^k x_j^1, \dots, \sum_{j=1}^k x_j^{2l})$  is in the set

$$S := \{(b_1, \dots, b_{2l}) : b_1 \cdots b_{2l} \in \{0, 1\}^{2l} \setminus \{(0, \dots, 0)\}\}.$$

Then, by Eq. (10),  $(a_1, a_2, \dots, a_k)$  is taken so that  $(\sum_{j=1}^k a_j^1, \dots, \sum_{j=1}^k a_j^{2l})$  can be distributed from  $S$  uniformly at random. Moreover,  $(a_1^{2^{i-1}}, a_2^{2^{i-1}}, \dots, a_k^{2^{i-1}})$  is uniformly randomized by  $r^i$  in Step 3 under the restriction that the sum remains the same (since  $\sum_{j=1}^k r_j^i = 0$ ). Thus, the quantum state that  $R$  receives (represented by Eq. (9)) is taken from the set of  $(2^{2l} - 1)2^{(k-2)l}$  orthogonal pure states

$$B \setminus \left\{ \bigotimes_{i=1}^l |\Phi(y_1^i, \dots, y_{k-1}^i, 0)\rangle : \sum_{j=1}^{k-1} y_j^i = 0 \text{ for every } i \in [l] \right\}$$

(up to the total phase) uniformly at random. ◀

Now Lemma 11 provides the upper bound  $kn/2$  of Theorem 2. The lower bound  $kn$  of Theorem 2 originates from the lower bound  $n$  of the exact (two-party) one-way quantum communication complexity with no shared entanglement of the  $n$ -bit equality function (see, e.g., [24, Theorem 5.11]) as it implies that for any  $j \in [k]$ , the  $j$ th party must send  $n$  qubits (considering the one-way communication setting from the  $j$ th party with input  $x \in \{0, 1\}^n$  to the group of the referee and the other  $k - 1$  parties in which one party has input  $y \in \{0, 1\}^n$  and the  $k - 2$  remaining parties have input  $0^n$ , the length of the message of the  $j$ th party must be  $n$ ). This completes the proof of Theorem 2.

Actually, the upper bound  $kl$  of Lemma 11 for  $GEQ_{2l}$  is tight when  $k$  is even. The matching lower bound  $kl$  originates from the lower bound  $l$  of the exact one-way quantum communication complexity with shared entanglement of the  $2l$ -bit equality function shown by Klauck [24, Theorem 5.12] as it implies that each party must send  $l$  qubits.

## 5 Power of Shared Entanglement for Partial Functions

In this section, we prove Theorem 3. We consider the so-called distributed Deutsch-Jozsa problem  $DJ_n$  introduced by Brassard, Cleve, and Tapp [5]. First we show that  $C_0^{psm,*}(DJ_n) = O(\log n)$ . Our PSM protocol is based on the protocol provided in [5], which we modify so that the privacy condition can be satisfied. Second we show  $Q_0^{psm}(DJ_n) = \Omega(n)$  by observing that the fact that the exact classical and quantum SMP communication complexities are the same for total functions can be extended to the case of partial functions.

Let  $n$  be any power of 2. The distributed Deutsch-Jozsa problem  $DJ_n : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ , introduced in [5], is defined as

$$DJ_n(x, y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \Delta(x, y) = n/2, \end{cases}$$

where  $\Delta(x, y)$  denotes the Hamming distance between  $x = x_0x_1 \cdots x_{n-1}$  and  $y = y_0y_1 \cdots y_{n-1}$ .

► **Lemma 12.** *There is a PSM protocol with shared entanglement that solves  $DJ_n$  with probability 1, and the classical communication complexity is  $2 \log n$ .*

**Proof.** The PSM protocol is as follows.

**Protocol  $\mathcal{P}_{DJ}$ :** Let  $n = 2^m$ .

0.  $P_1$  and  $P_2$  share the entangled state

$$\frac{1}{\sqrt{n}} \sum_{i \in \{0, 1\}^m} |i\rangle_A |i\rangle_B$$

and the two prearranged random  $m$ -bit strings  $r \in \{0, 1\}^m \setminus \{0^m\}$  and  $r' \in \{0, 1\}^m$ .

1.  $P_1$  (resp.  $P_2$ ) adds phase  $(-1)^{x_i}$  ( $(-1)^{y_i}$ ) to the  $m$ -qubit register  $A$  ( $B$ ) if the content of  $A$  ( $B$ ) is  $i$  (where  $i \in \{0, 1\}^m$  is identified as the corresponding non-negative integer). The resulting state is

$$\frac{1}{\sqrt{n}} \sum_{i \in \{0, 1\}^m} (-1)^{x_i} |i\rangle_A (-1)^{y_i} |i\rangle_B.$$

2.  $P_1$  and  $P_2$  apply the Hadamard gate  $H$  for each qubit of their registers  $A$  and  $B$ , respectively. The resulting state is

$$\frac{1}{n\sqrt{n}} \sum_{i \in \{0, 1\}^m} \left( (-1)^{x_i} \sum_{k \in \{0, 1\}^m} (-1)^{i \cdot k} |k\rangle_A \right) \left( (-1)^{y_i} \sum_{l \in \{0, 1\}^m} (-1)^{i \cdot l} |l\rangle_B \right). \quad (11)$$

3.  $P_1$  and  $P_2$  measure  $A$  and  $B$  in the computational basis, respectively, and let  $K$  and  $L$  be the resulting bit strings in  $\{0, 1\}^m$ .

4.  $P_1$  and  $P_2$  send classical messages  $m_A$  and  $m_B$  defined as  $\mathbf{p}(m_A) = \mathbf{p}(r)\mathbf{p}(K) + \mathbf{p}(r')$  and  $\mathbf{p}(m_B) = \mathbf{p}(r)\mathbf{p}(L) + \mathbf{p}(r')$  to  $R$ , respectively.

5.  $R$  accepts if  $m_A = m_B$  and rejects otherwise.

**Correctness:** Note that the amplitude of  $|k\rangle_A |l\rangle_B$  in Eq. (11) is

$$\frac{1}{n^{3/2}} \sum_{i \in \{0, 1\}^m} (-1)^{x_i \oplus y_i} (-1)^{i \cdot (k \oplus l)}. \quad (12)$$

When  $x = y$ , Eq. (12) is 0 if  $K \neq L$ . Thus, the event  $K = L$  occurs with probability 1; therefore,  $R$  always accepts. When  $\Delta(x, y) = n/2$ , Eq. (12) is 0 if  $K = L$ . Thus, the event  $K \neq L$  occurs with probability 1; therefore,  $R$  always rejects.

**Privacy:** Again, by Eq. (12), if  $x = y$ , then  $K = L = k$  is obtained with  $1/n$  for each  $k \in \{0, 1\}^m$ . Thus, the simulator can simulate the messages by generating the same  $m$ -bit string chosen uniformly at random as  $P_1$ 's and  $P_2$ 's messages. If  $\Delta(x, y) = n/2$ , the element  $\mathbf{p}(K) - \mathbf{p}(L)$  in  $\mathbb{F}_2^m$  is nonzero; thus, the difference between  $\mathbf{p}(r)\mathbf{p}(K) + \mathbf{p}(r')$  and

$p(r)p(L) + p(r')$  is distributed uniformly at random in  $\mathbb{F}_{2^m}^*$ . Moreover,  $p(K)$  (and  $p(L)$ ) is distributed uniformly at random in  $\mathbb{F}_{2^m}$  by multiplying  $p(r)$  and adding  $p(r')$ . Thus, the simulator can simulate the messages by choosing two different  $m$ -bit non-zero strings uniformly at random as  $P_1$ 's and  $P_2$ 's messages. ◀

Using the result in [7] that  $DJ_n$  has the exact classical communication complexity  $\Omega(n)$  (even in the two-way communication model), we can show that  $DJ_n$  provides the following exponential separation between exact PSMs with shared entanglement and exact PSQMs without shared entanglement. (Note that Theorem 13 implies Theorem 3, namely, an exponential gap between  $Q_0^{psm,*}(DJ_n)$  and  $Q_0^{psm}(DJ_n)$ , as well as between  $C_0^{psm,*}(DJ_n)$  and  $C_0^{psm}(DJ_n)$ .)

► **Theorem 13.**  $C_0^{psm,*}(DJ_n) = O(\log n)$  and  $Q_0^{psm}(DJ_n) = \Omega(n)$ .

**Proof.** The upper bound  $C_0^{psm,*}(DJ_n) = O(\log n)$  is shown by Lemma 12.

The lower bound comes from the fact that both the exact quantum and classical SMP communication complexities of a total function  $f$  over  $X \times Y$  are equal to the sum of the number of the different row vectors of the communication matrix of  $f$ ,  $M_f$ , and the number of the different column vectors of  $M_f$  (this fact can be found in [30, p.142]). The proof idea is that any two (classical or quantum) messages  $m_x$  and  $m_{x'}$  corresponding to different row vectors indexed with input  $x$  and  $x'$  must be perfectly distinguished since there is some column input  $y$  such that  $M_f(x, y) \neq M_f(x', y)$  (and a similar argument holds for different column vectors), and choosing different messages for such different row vectors or column vectors is sufficient for the referee to compute  $f$  exactly. This proof idea also holds for a partial function by replacing the number of the different row (resp. column) vectors by the size of the maximum clique of the graph  $G_1(M_f) = (X, E_{1,f})$  (resp.  $G_2(M_f) = (Y, E_{2,f})$ ) defined as follows: two rows  $x$  and  $x'$  (resp. columns  $y$  and  $y'$ ) have an edge in  $E_{1,f}$  (resp.  $E_{2,f}$ ) if and only if there is a column  $y$  (resp. row  $x$ ) such that  $(x, y)$  and  $(x', y)$  (resp.  $(x, y)$  and  $(x, y')$ ) are in the domain of the partial function  $f$  and  $M_f(x, y) \neq M_f(x', y)$  (resp.  $M_f(x, y) \neq M_f(x, y')$ ).

The above observation implies that the exact quantum and classical SMP communication complexities of the partial function  $DJ_n$  are the same. By the result in [7],  $DJ_n$  has the exact classical communication complexity  $\Omega(n)$ . This concludes the desired lower bound  $Q_0^{psm}(DJ_n) = \Omega(n)$ . ◀

Theorem 13 provides an exponential gap between PSMs with shared entanglement and PSQMs without shared entanglement for partial functions; however, it is obtained only in the exact setting, and we do not know whether this exponential gap can be obtained in the bounded-error setting for partial or total functions. However, we can observe that there is a relational problem that has an exponential gap between PSMs with shared entanglement and PSQMs without shared entanglement in the bounded-error setting from the result by Gavinsky et al. [18]. They demonstrated that the problem has an exponentially smaller communication complexity of a classical SMP protocol with shared entanglement than the communication complexity of quantum SMP protocols only with shared randomness, while it is easy to see that their protocol is in fact a PSQM.

## 6 Conclusion

This paper introduced a quantum analogue of the well-studied PSM model which was called the PSQM model, and provided several initial results in the exact setting. Here we list a number of open problems.

- Can the lower bound of Theorem 1 be extended to the bounded-error setting or to the shared entanglement case?
- Can any non-trivial communication complexity gap between the PSM model and the PSQM model for some function in the bounded-error setting? How about any non-trivial communication complexity gap between the PSQM model with shared entanglement and the PSQM model without it in the bounded-error setting?
- The PSQM model in this paper was defined only for perfect privacy. What results are obtained for imperfect privacy? To extend the lower bound of Theorem 1 to imperfect privacy, a quantumly tailored modification of [1, Section 5] might be worth considering, while it seems much more complicated than the proof of Theorem 1.

---

## References

- 1 Benny Applebaum, Thomas Holenstein, Manoj Mishra, and Ofer Shayelevitz. The communication complexity of private simultaneous messages, revisited. *Journal of Cryptology* **33**(3), 916–953 (2020).
- 2 Amos Beimel, Eyal Kushilevitz, and Pnina Nissim. The complexity of multiparty PSM protocols and related models. Proceedings of 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2018), Part II, 287–318 (2018).
- 3 Marshall Ball, Justin Holmgren, Yuval Ishai, Tianren Liu and Tal Malkin. On the complexity of decomposable randomized encodings, or: how friendly can a garbling-friendly PRF be? Proceedings of the 11th Innovations in Theoretical Computer Science Conference (ITCS 2020), 86:1–86:22 (2020).
- 4 Ziv Bar-Yossef, T. S. Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. *SIAM Journal on Computing* **38**(1), 366–384 (2008).
- 5 Gilles Brassard, Richard Cleve, and Alain Tapp. Cost of exactly simulating quantum entanglement with classical communication. *Physical Review Letters* **83**, 1874–1877 (1999).
- 6 Zvika Brakerski and Henry Yuen. Quantum garbled circuits. arXiv:2006.01085 (2020).
- 7 Harry Buhrman, Richard Cleve, and Avi Wigderson. Quantum vs. classical communication and computation. Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC 1998), 63–68 (1998).
- 8 Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Physical Review Letters* **87**, 167902 (2001).
- 9 Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. Proceedings of the 11th IACR Theory of Cryptography Conference (TCC 2014), 317–342 (2014).
- 10 Claude Crépeau, Daniel Gottesman, and Adam Smith. Secure multi-party quantum computation. Proceedings of the 34th Annual Symposium on Theory of Computing (STOC 2002), 643–652 (2002).
- 11 Yfke Dulek, Alex B. Grilo, Stacey Jeffery, Christian Majenz, and Christian Schaffner. Secure multi-party quantum computation with a dishonest majority. Proceedings of the 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2020) Part III, 729–758 (2020).
- 12 Ivan Damgård, Kasper Green Larsen, and Jesper Buus Nielsen. Communication lower bounds for statistically secure MPC, with or without preprocessing. Proceedings of the 39th Annual International Cryptology Conference (CRYPTO 2019) Part II, 61–84 (2019).
- 13 Deepesh Data, Vinod M. Prabhakaran, and Manoj Prabhakaran. Communication and randomness lower bounds for secure computation. *IEEE Transactions on Information Theory* **62**(7), 3901–3929 (2016).



- 14 Uriel Feige, Joe Kilian, and Moni Naor. A minimal model for secure computation (extended abstract). Proceedings of the 26th Annual ACM Symposium on Theory of Computing (STOC 1994), 554–563 (1994).
- 15 Dmitry Gavinsky. Quantum versus classical simultaneity in communication complexity. *IEEE Transactions on Information Theory* **65**(10), 6466–6483 (2019).
- 16 Dmitry Gavinsky. Bare quantum simultaneity versus classical interactivity in communication complexity. Proceedings of the 52nd Annual ACM Symposium on Theory of Computing (STOC 2020), 401–411 (2020).
- 17 Dmitry Gavinsky and Tsuyoshi Ito. Quantum fingerprints that keep secrets. *Quantum Information and Computation* **13**(7-8), 583–606 (2013).
- 18 Dmitry Gavinsky, Julia Kempe, Oded Regev, and Ronald de Wolf. Bounded-error quantum state identification and exponential separations in communication complexity. *SIAM Journal on Computing* **39**(1), 1–24 (2009).
- 19 Masahito Hayashi, Satoshi Ishizuka, Akinori Kawachi, Gen Kimura, and Tomohiro Ogawa. *Introduction to Quantum Information Science*, Springer (2015).
- 20 Rolf T. Horn, A. J. Scott, Jonathan Walgate, Richard Cleve, A. I. Lvovsky, and Barry C. Sanders. Classical and quantum fingerprinting with shared randomness and one-sided error. *Quantum Information and Computation* **5**(3), 258–271 (2005).
- 21 Yuval Ishai and Eyal Kushilevitz. Private simultaneous messages protocol with applications. Proceedings of the 5th Israel Symposium on Theory of Computing and Systems (ISTCS 1997), 174–183 (1997).
- 22 Roy Kasher and Julia Kempe. Two-source extractors secure against quantum adversaries. *Theory of Computing* **8**(1), 461–486 (2012).
- 23 Hartmut Klauck. Quantum and approximate privacy. *Theory of Computing Systems* **37**(1), 221–246 (2004).
- 24 Hartmut Klauck. One-way communication complexity and the Nečiporuk lower bound on formula size. *SIAM Journal on Computing* **37**(2), 552–583 (2007).
- 25 Eyal Kushilevitz and Noam Nisan. *Communication Complexity*, Cambridge University Press (1997).
- 26 Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000).
- 27 Tomoyuki Morimae. Quantum randomized encoding, verification of quantum computing, no-cloning, and blind quantum computing. arXiv:2011.03141 (2020).
- 28 Ran Raz. Exponential separation of quantum and classical communication complexity. Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC 1999), 358–367 (1999).
- 29 Dominique Unruh. Universally composable quantum multi-party computation. Proceedings of 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2010), 486–505 (2010).
- 30 Ronald de Wolf. *Quantum Computing and Communication Complexity*, University of Amsterdam (2001).
- 31 Andrew Chi-Chih Yao. Some complexity questions related to distributive computing (preliminary report). Proceedings of the 11th Annual ACM Symposium on Theory of Computing (STOC 1979), 209–213 (1979).

## **A** Proofs of Claim 7, Claim 8, and Lemma 9

In this appendix, we give the detailed proofs of the technical claims and lemma used in the proof of Lemma 5.

**Proof of Claim 7.** For any two quantum states  $\rho, \sigma$ , the condition  $\rho\sigma = 0$  is necessary (and sufficient) for perfect discrimination of the two states (see, e.g., Proposition 5.13 in [19]). Since

the referee  $R$  perfectly discriminates  $\rho(x_1, x_2)$  and  $\rho(x'_1, x'_2)$  for which  $F_n(x_1, x_2) \neq F_n(x'_1, x'_2)$  from the correctness, it must hold that  $\rho(x_1, x_2)\rho(x'_1, x'_2) = 0$ . Then, we have

$$\begin{aligned} & \text{tr} \sum_{(x_1, x_2) \neq (x'_1, x'_2)} \mu(x_1, x_2) \rho(x_1, x_2) \mu(x'_1, x'_2) \rho(x'_1, x'_2) \\ &= \sum_y \text{tr} \sum_{\substack{(x_1, x_2) \neq (x'_1, x'_2) \\ F_n(x_1, x_2) = F_n(x'_1, x'_2) = y}} \mu(x_1, x_2) \rho(x_1, x_2) \mu(x'_1, x'_2) \rho(x'_1, x'_2). \end{aligned}$$

From the privacy, there exists a quantum state  $\rho_y$  for each  $y$  such that  $\rho_y = \rho(x_1, x_2)$  for every  $(x_1, x_2)$  for which  $F_n(x_1, x_2) = y$ . Therefore,

$$\begin{aligned} & \sum_y \text{tr} \sum_{\substack{(x_1, x_2) \neq (x'_1, x'_2) \\ F_n(x_1, x_2) = F_n(x'_1, x'_2) = y}} \mu(x_1, x_2) \rho(x_1, x_2) \mu(x'_1, x'_2) \rho(x'_1, x'_2) \\ &= \sum_y \text{tr} \rho_y^2 \sum_{\substack{(x_1, x_2) \neq (x'_1, x'_2) \\ F_n(x_1, x_2) = F_n(x'_1, x'_2) = y}} \mu(x_1, x_2) \mu(x'_1, x'_2) \\ &= \sum_y \frac{\sum_{\substack{(x_1, x_2) \neq (x'_1, x'_2) \\ F_n(x_1, x_2) = F_n(x'_1, x'_2) = y}} \mu(x_1, x_2) \mu(x'_1, x'_2)}{\sum_{F_n(x_1, x_2) = F_n(x'_1, x'_2) = y} \mu(x_1, x_2) \mu(x'_1, x'_2)} \text{tr} \rho_y^2 \sum_{F_n(x_1, x_2) = F_n(x'_1, x'_2) = y} \mu(x_1, x_2) \mu(x'_1, x'_2) \\ &= \sum_y \Pr[(X_1, X_2) \neq (X'_1, X'_2) \mid F_n(X_1, X_2) = F_n(X'_1, X'_2) = y] \text{tr} \rho_y^2 \\ & \quad \times \sum_{F_n(x_1, x_2) = F_n(x'_1, x'_2) = y} \mu(x_1, x_2) \mu(x'_1, x'_2) \\ &\geq \beta(\mu) \sum_y \text{tr} \rho_y^2 \sum_{F_n(x_1, x_2) = F_n(x'_1, x'_2) = y} \mu(x_1, x_2) \mu(x'_1, x'_2) \\ &= \beta(\mu) \text{tr} \sum_{x_1, x_2, x'_1, x'_2} \mu(x_1, x_2) \rho(x_1, x_2) \mu(x'_1, x'_2) \rho(x'_1, x'_2). \end{aligned}$$

◀

**Proof of Claim 8.** From the privacy, there exists  $\rho_y$  such that  $\rho_y = \rho(x_1, x_2)$  for every  $y \in \{0, 1\}$  and every  $(x_1, x_2)$  for which  $F_n(x_1, x_2) = y$ . From the correctness and the necessary condition of the perfect quantum state discrimination,  $\rho_0 \rho_1 = 0$  must hold. From the spectral decomposition we have  $\rho_y = \sum_i \lambda_{y,i} |\phi_{y,i}\rangle \langle \phi_{y,i}|$  for some orthonormal basis  $\{|\phi_{y,i}\rangle\}_i$  ( $\lambda_{y,i} > 0$ ). Then, we have  $\langle \phi_{0,i} | \phi_{1,j} \rangle = 0$  for every  $i, j$  since  $\rho_0 \rho_1 = 0$ . Therefore, we can assume  $R_0 = \sum_i |\phi_{0,i}\rangle \langle \phi_{0,i}|$  and  $R_1 = I - R_0$  without loss of generality. This  $R = \{R_y\}_{y \in \{0,1\}}$  is a PVM. ◀

**Proof of Lemma 9.** We demonstrate that  $|\langle \psi_1(z; r') | \psi_1(z'; r') \rangle|^2 = 0$  for every distinct  $z, z'$  and every  $r'$ . Assuming this, we can decompose

$$|\psi_1(x_1; r)\rangle = \sum_{z'} \alpha_{z'} |\psi_1(z'; r')\rangle + \alpha^\perp |\psi_1^\perp\rangle$$

with orthonormal vectors  $\{|\psi_1(z'; r')\rangle\}_{z'} \cup \{|\psi_1^\perp\rangle\}$  for some coefficients  $\alpha_{z'}$  and  $\alpha^\perp$ . Then, it

holds that

$$\begin{aligned} \sum_{z \neq x_1} |\langle \psi_1(x_1; r) | \psi_1(z; r') \rangle|^2 &= \sum_{z \neq x_1} \left| \sum_{z'} \alpha_{z'}^* \langle \psi_1(z'; r') | \psi_1(z; r') \rangle + \alpha^{\perp*} \langle \psi_1^\perp | \psi_1(z; r') \rangle \right|^2 \\ &= \sum_{z \neq x_1} |\alpha_z|^2 \leq 1. \end{aligned}$$

Therefore, it suffices to demonstrate  $|\langle \psi_1(z; r') | \psi_1(z'; r') \rangle|^2 = 0$  for every distinct  $z, z'$  and every  $r'$ . For contradiction, assume that  $|\langle \psi_1(z; r') | \psi_1(z'; r') \rangle|^2 > 0$  for some  $z, z'$  and some  $r'$ .

From this assumption, we have

$$|\psi_1(z'; r') \rangle = \beta |\psi_1(z; r') \rangle + \beta^\perp |\psi_1^\perp(z; r') \rangle,$$

where  $\beta \neq 0$  and  $|\psi_1^\perp(z; r') \rangle$  is orthogonal to  $|\psi_1(z; r') \rangle$ .

We fix  $x_2$  arbitrarily. Then, we have

$$|\psi_1(z'; r') \rangle |\psi_2(x_2; r') \rangle = \beta |\psi_1(z; r') \rangle |\psi_2(x_2; r') \rangle + \beta^\perp |\psi_1^\perp(z; r') \rangle |\psi_2(x_2; r') \rangle.$$

Since  $R$  is a PVM, we have

$$R_{F_n(z, x_2)} |\psi_1(z; r') \rangle |\psi_2(x_2; r') \rangle = |\psi_1(z; r') \rangle |\psi_2(x_2; r') \rangle$$

from the correctness. We also have

$$|\psi_1^\perp(z; r') \rangle = \gamma |\phi(z; r') \rangle + \gamma^\perp |\phi^\perp(z; r') \rangle,$$

where  $|\psi_1(z; r') \rangle, |\phi(z; r') \rangle, |\phi^\perp(z; r') \rangle$  are orthogonal to each other, and  $R_{F_n(z, x_2)} |\phi(z; r') \rangle |\psi_2(x_2; r') \rangle = |\phi(z; r') \rangle |\psi_2(x_2; r') \rangle, R_{F_n(z, x_2)} |\phi^\perp(z; r') \rangle |\psi_2(x_2; r') \rangle = 0$ .

Therefore, it holds that

$$|\langle \psi_1(z; r') | \langle \psi_2(x_2; r') | R_{F_n(z, x_2)} |\psi_1(z'; r') \rangle |\psi_2(x_2; r') \rangle|^2 = |\beta|^2 + |\gamma|^2 > 0.$$

The value  $|\beta|^2 + |\gamma|^2 > 0$  must be 1 from the correctness; therefore,  $R(|\psi_1(z'; r') \rangle |\psi_2(x_2; r') \rangle) = F_n(z', x_2)$  for every  $x_2$  and every  $r'$ . This implies that  $F_n(z, x_2) = F_n(z', x_2)$  holds for every  $x_2$ , which contradicts the non-degeneracy of  $F_n$ . The same argument also works for  $x_2$ . ◀