Explicit Lower Bounds for Communication Complexity of PSM for Concrete Functions

Kazumasa Shinagawa[1,3] and Koji Nuida[2,3]

[1] Ibaraki University, Japan
kazumasa.shinagawa.np92@vc.ibaraki.ac.jp
[2] Institute of Mathematics for Industry (IMI), Kyushu University, Japan
nuida@imi.kyushu-u.ac.jp
[3] National Institute of Advanced Industrial Science and Technology (AIST), Japan

Abstract. Private Simultaneous Messages (PSM) is a minimal model of secure computation, where the input players with shared randomness send messages to the output player simultaneously and only once. In this field, finding upper and lower bounds on communication complexity of PSM protocols is important, and in particular, identifying the optimal one where the upper and lower bounds coincide is the ultimate goal. However, up until now, functions for which the optimal communication complexity has been determined are few: An example of such a function is the two-input AND function where $(2\log_2 3)$-bit communication is optimal. In this paper, we provide new upper and lower bounds for several concrete functions. For lower bounds, we introduce a novel approach using combinatorial objects called abstract simplicial complexes to represent PSM protocols. Our method is suitable for obtaining non-asymptotic explicit lower bounds for concrete functions. By deriving lower bounds and constructing concrete protocols, we show that the optimal communication complexity for the equality and majority functions with three input bits are $3\log_2 3$ bits and 6 bits, respectively. We also derive new lower bounds for the n-input AND function, three-valued comparison function, and multiplication over finite rings.

Keywords: secure multiparty computation; private simultaneous messages; communication complexity; lower bounds; concrete functions

1 Introduction

1.1 Background

Private Simultaneous Messages (PSM) is a minimal model of secure computation, initially proposed by Feige, Kilian, and Naor (hereafter, FKN) [8] and later generalized by Ishai and Kushilevitz [9]. A PSM protocol involves the input players $P_1, \ldots, P_n$ and the output player called the referee. Each input player P_i with input x_i sends a message m_i to the referee simultaneously and only once, and the referee computes the output value y based on the received messages $m_1, \ldots, m_n$.

Here, all players share a randomness r in advance, which is independent of the inputs and inaccessible to the referee, and each message m_i is computed from the input value x_i and the randomness r only. For a function f to be computed, a PSM protocol is said to be correct if $y = f(x_1, \ldots, x_n)$ holds with probability 1, and said to be secure if, when the output value y is fixed, the distribution of the tuple of the messages is independent from the input distribution. The communication complexity of a PSM protocol is defined as $\sum_{i=1}^{n} \log_2 |M_i|$, where M_i denotes the i-th message space and $|\cdot|$ denotes the cardinality of the set.

It is important to determine the upper and lower bounds for communication complexity of PSM protocols. So far, there is an exponential gap between these bounds for general two-input functions $f : \{0,1\}^k \times \{0,1\}^k \to \{0,1\}$: The best-known upper bound is $O(2^{k/2})$ from the PSM protocol constructed by Beimel, Ishai, Kumaresan, and Kushilevitz [5], while the lower bound for a random f is $3k - O(\log k)$ by Applebaum, Holenstein, Mishra, and Shayevitz [1] (see also Vaikuntanathan's survey [11]). The situation is similar for general n-input functions $f : (\{0,1\}^k)^n \to \{0,1\}$: The best-known upper bound is $O(poly(n) \cdot 2^{\frac{nk}{2}})$ by Beimel, Kushilevitz, and Nissim [6], the upper bound for infinitely many n is $O(poly(n) \cdot 2^{\frac{(n-1)k}{2}})$ by Assouline and Liu [2], and the lower bound with $n = \omega(k)$ for a random f is $\Omega(n^2 k / \log(nk))$ by Ball and Randolph [4].

On the other hand, for concrete functions, various PSM protocols had been proposed: the AND function [8], the three-valued comparison function [8], branching programs [9], symmetric functions [10], and so on. However, up until now, there are only few functions for which the optimal communication complexity has been determined. An example of such a function is the two-input AND function $x_1 \wedge x_2$, where the optimal communication complexity is shown to be $2 \log_2 3$ bits: The protocol is constructed by FKN [8], and the lower bound is given by Data, Prabhakaran, and Prabhakaran (hereafter, DPP) [7]. Another example is the multiplication $x_1 x_2 \cdots x_n$ over a finite group G, where the optimal communication complexity is shown to be $n \log_2 |G|$ bits: The protocol is constructed by FKN [8], and the lower bound follows from the trivial bound, i.e., the communication complexity without security. As the latter result on the lower bound did not concern the security, a new approach that fully utilizes the security condition is demanded towards non-trivial lower bounds for other functions.

1.2 Our Contribution

In this paper, we derive new upper and lower bounds on communication complexity of PSM protocols for several concrete functions, aiming to further identify the optimal communication complexity. The main technical contribution of this paper is to introduce a novel approach for proving lower bounds using combinatorial objects called abstract simplicial complexes (hereafter, simplicial complexes) to represent PSM protocols. Based on this approach, we derive lower bounds for the AND function, equality function, majority function, comparison function, and multiplication over finite rings. At the same time, we also provide upper bounds for the equality function, majority function, and multiplication

Table 1. Summary of our results and existing results

	upper/lower	communication complexity	condition
∘ AND: $x_1 \wedge \cdots \wedge x_n$			
FKN [8]	construction	$\lvert M_i\rvert = p$	$p > n$: prime
DPP [7]	lower bound	$\lvert M_i\rvert \geq 3$	$n = 2$
Sec. 4.2	lower bound	$\lvert M_1\rvert = 3 \Rightarrow \lvert M_{i(\neq 1)}\rvert \geq 6$	$n \geq 3$
∘ Equality: $(x_1 = \cdots = x_n)$?			
Sec. 4.3	construction	$\lvert M_i\rvert = p$	$p \geq n$: prime
Sec. 4.3	lower bound	$\lvert M_i\rvert \geq 3$	–
∘ Majority: $(x_1 + \cdots + x_n \geq \lceil n/2 \rceil)$?			
Sec. 4.4	construction	$\lvert M_i\rvert = 4$	$n = 3$
Sec. 4.4	lower bound	$\lvert M_i\rvert \geq 4$	–
∘ $(k+1)$-valued comparison: $(x_1 > x_2$ or $x_1 = x_2$ or $x_1 < x_2)$?			
FKN [8]	construction	$\lvert M_i\rvert = 7$	$k = 2$
Sec. 4.5	lower bound	$\lvert M_i\rvert \geq 2k + 1$	–
Sec. 4.5	lower bound	$\lvert M_1\rvert \geq 6$ or $\lvert M_2\rvert \geq 6$	$k = 2$
∘ Multiplication over a finite ring S: $x_1 \cdot x_2$			
Beaver Triple	construction	$\lvert M_i\rvert = \lvert S\rvert^2$	any S
Sec. 4.6	lower bound	$\lvert M_i\rvert \geq 2q - 1$	$S = \mathbb{F}_q$
Sec. 4.6	lower bound	$\lvert M_i\rvert \geq \sum_{j=1}^{q} \gcd(j, q)$	$S = \mathbb{Z}/q\mathbb{Z}$

over finite rings by constructing new protocols. As a result, we identify the optimal communication complexity for the equality function and majority function in the case of $n = 3$. Regarding the three-input AND function and three-valued comparison function, we specify all possibilities (eight for each function) for the optimal communication complexity. Our results are summarized in Table 1. In the following, we explain the details of each item.

- For the AND function $x_1 \wedge \cdots \wedge x_n$, FKN [8] proposed a PSM protocol with $|M_i| = p$ $(1 \leq i \leq n)$, where p is any prime number satisfying $p > n$, which currently provides the best-known upper bound. When $n = 2$, DPP [7] showed a lower bound $|M_i| \geq 3$ $(i \in \{1, 2\})$, which proves the optimality of the FKN protocol for $n = 2$. Based on our new approach for proving lower bounds, we provide an alternative proof for this result. When $n \geq 3$, as a new lower bound, we show that if $|M_1| = 3$, then $|M_i| \geq 6$ for all $i \neq 1$. In particular, when $n = 3$, there are only eight possibilities of the tuple $(|M_1|, |M_2|, |M_3|)$ (up to symmetry) for the protocol with the minimum value of $\sum_{i=1}^{3} \log_2 |M_i|$; we specify them explicitly.
- For the equality function, we propose a PSM protocol with $|M_i| = p$, where p is any prime number satisfying $p \geq n$, and prove a lower bound of $|M_i| \geq 3$ $(1 \leq i \leq n)$. When $n = 3$, the upper and lower bounds coincide, hence, the optimal communication complexity is determined as $3 \log_2 3$ bits.
- For the majority function, we prove a lower bound of $|M_i| \geq 4$ $(1 \leq i \leq n)$. When $n = 3$, we propose a PSM protocol with $|M_i| = 4$ $(1 \leq i \leq$

3). In this case, the upper and lower bounds coincide, hence, the optimal communication complexity for $n = 3$ is determined as 6 bits.
- For the $(k+1)$-valued comparison function $f : \{0, 1, \ldots, k\} \times \{0, 1, \ldots, k\} \to \{-1, 0, 1\}$, we prove a lower bound of $|M_i| \geq 2k + 1$ ($i \in \{1, 2\}$). When $k = 2$, FKN [8] proposed a PSM protocol with $|M_i| = 7$ ($i \in \{1, 2\}$), which currently provides the best-known upper bound. In this case, as a new lower bound, we show that either $|M_1| \geq 6$ or $|M_2| \geq 6$, which implies that there are only eight possibilities of $(|M_1|, |M_2|)$ (up to symmetry) attaining the minimum value of $\sum_{i=1}^{2} \log_2 |M_i|$; we specify them explicitly.
- For the multiplication function $x_1 \cdot x_2$ over a finite ring S, we propose a PSM protocol with $|M_i| = |S|^2$ ($i \in \{1, 2\}$) using the idea of Beaver multiplication triples. As for lower bounds, we prove that $|M_i| \geq 2q - 1$ if S is the field of order q and $|M_i| \geq a(q) := \sum_{j=1}^{q} \gcd(j, q)$ if S is the integer residue ring modulo q, where $a(q)$ is known as the Pillai's arithmetic function.

1.3 Technical Overview

Our new method of deriving lower bounds, which we call the *embedding method*, is a multi-input generalization of the idea by FKN [8] using edge-colored bipartite graphs. We start with recalling their idea. For a function $f : \{0, 1\}^k \times \{0, 1\}^k \to \{0, 1\}$, the bipartite graph G_f is constructed by joining vertices x_1 and x_2 with a black edge if $f(x_1, x_2) = 0$, and with a red edge if $f(x_1, x_2) = 1$. Similarly, the decoding function $\mathsf{Dec} : M_1 \times M_2 \to \{0, 1\}$ of a PSM protocol is represented by the bipartite graph G_{Dec}. In this context, a shared randomness of the PSM protocol can be regarded as an embedding map from G_f to G_{Dec} that preserves the coloring of edges. Based on this idea, FKN constructed PSM protocols and proved lower bounds.

To extend the idea of FKN to n-input functions $f : X_1 \times \cdots \times X_n \to Y$ with $n \geq 2$, we needed, instead of an edge joining two elements x_1 and x_2, a "higher-dimensional edge" joining n elements $x_1, \ldots, x_n$. We found that a combinatorial object called *simplicial complexes* (see Section 2.2) is suitable for the purpose. In our setting, the simplicial complex Δ_f representing the function f consists of $(n-1)$-dimensional faces $\{x_1, \ldots, x_n\}$ (called *facets*) having n vertices $x_i \in X_i$ (and their subfaces $\{x_{i_1}, \ldots, x_{i_d}\}$, $i_1 < \cdots < i_d$). Then a facet $\{x_1, \ldots, x_n\}$ of Δ_f has color $y \in Y$ if $f(x_1, \ldots, x_n) = y$. The simplicial complex Δ_{Dec} representing the decoding function Dec is defined in the same way. Now similarly to the case of $n = 2$, a key observation here is that any shared randomness can be interpreted as an embedding map from Δ_f to Δ_{Dec} that preserves the coloring of facets.

In order to explain our idea, here we demonstrate an alternative proof for DPP's lower bound $|M_i| \geq 3$ ($i \in \{1, 2\}$) for the two-input AND function $f(x_1, x_2) = x_1 \wedge x_2$. First, as mentioned above, any shared randomness $r = (r_1, r_2)$ can be regarded as a pair of injections $r_i : X_i = \{0, 1\} \to M_i$ ($i \in \{1, 2\}$). Take a randomness $r = (r_1, r_2)$ and write $\widehat{b} := r_i(b)$ ($b \in \{0, 1\}, i \in \{1, 2\}$). Here, the security of PSM protocols can be interpreted as stating that for any edge $\widehat{e}$ of G_{Dec}, the probability that an edge e of G_f with the same color as $\widehat{e}$

is mapped to $\widehat{e}$ by some randomness is independent of e. Thus, since the black edge $e = (0, 0)$ in G_f is mapped to the black edge $\widehat{e} = (\widehat{0}, \widehat{0})$ in G_{Dec}, there must exist another randomness $r' = (r'_1, r'_2)$ that maps another black edge $e' = (0, 1)$ in G_f to $\widehat{e}$. In this case, r' maps a red edge $e'' = (1, 1)$ to $\widehat{e'} = (r'_1(1), \widehat{0})$, which should be a red edge and hence be different from $(\widehat{0}, \widehat{0})$ and $(\widehat{1}, \widehat{0})$. Therefore, we have $r'_1(1) \neq \widehat{0}, \widehat{1}$ and hence M_1 must have at least three distinct elements, i.e., $|M_1| \geq 3$. By symmetry, we have $|M_2| \geq 3$.

In a general case, we establish useful lemmas for proving lower bounds (Lemmas 3 and 4) which we call *embedding lemmas*. These two versions have a trade-off that a strong version is only applicable to some restricted kind of functions f while a weak version is applicable to any f. In the previous paragraph, we derived the existence of a new embedding r' from the fact "the vertex 0 in X_1 is joined to two black edges" and the existence of the red edge $\widehat{e'}$ from the fact "the vertex 1 in X_2 is joined to both black and red edges." The idea of embedding lemmas is to derive a lower bound on the number of facets of Δ_{Dec} around a lower-dimensional face based on distributions of colors for facets in Δ_f.

Basic notations. For an integer $n \geq 1$, we write $[n] := \{1, 2, \ldots, n\}$. For any integer $q \geq 2$, we write $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$ and $\mathbb{Z}_q^\times := (\mathbb{Z}/q\mathbb{Z})^\times$ identified with $\{0, 1, \ldots, q-1\}$ and $\{1, 2, \ldots, q-1\}$, respectively. For a set S, we denote by $|S|$ the cardinality of S. For a bit string $m \in \{0,1\}^*$, we denote by $|m|$ the bit length of m. For two probability distributions $\mathcal{X}, \mathcal{Y}$, we write $\mathcal{X} \equiv \mathcal{Y}$ if they are the same probability distribution.

2 PSM Protocols and Simplicial Complexes

2.1 PSM Protocols

Definition 1. *Let $n \geq 2$ be a positive integer. Let X_i, M_i, R_i ($i \in [n]$), and Y be finite sets. Write $\vec{X} = X_1 \times \cdots \times X_n$, $\vec{M} = M_1 \times \cdots \times M_n$, and $\vec{R} = R_1 \times \cdots \times R_n$. Let $\mathsf{Enc}_i \colon X_i \times R_i \to M_i$ ($i \in [n]$) be functions and $\mathsf{Dec} \colon \vec{M} \to Y$ be a partial function. Let $\mathcal{R} = (\mathcal{R}_1, \ldots, \mathcal{R}_n)$ be a random variable over $\vec{R}$. A* private simultaneous messages (PSM) protocol for a function $f \colon \vec{X} \to Y$ *is a tuple $\Pi = (n, (X_i)_{i\in[n]}, Y, \mathcal{R}, (M_i)_{i\in[n]}, (\mathsf{Enc}_i)_{i\in[n]}, \mathsf{Dec})$ with the following conditions:*

- *(Correctness) For any $x = (x_1, \ldots, x_n) \in \vec{X}$,*

$$\Pr[\ \mathsf{Dec}(\mathsf{Enc}_1(x_1, \mathcal{R}_1), \ldots, \mathsf{Enc}_n(x_n, \mathcal{R}_n)) = f(x)\ ] = 1.$$

  Note that the correctness also claims that the partial function Dec *is defined over the arguments on the left-hand side.*
- *(Security) For any $x = (x_i)_{i\in[n]}, x' = (x'_i)_{i\in[n]} \in \vec{X}$ with $f(x) = f(x')$,*

$$(\mathsf{Enc}_1(x_1, \mathcal{R}_1), \ldots, \mathsf{Enc}_n(x_n, \mathcal{R}_n)) \equiv (\mathsf{Enc}_1(x'_1, \mathcal{R}_1), \ldots, \mathsf{Enc}_n(x'_n, \mathcal{R}_n)).$$

We call n the number of players, X_i the i-th input set, Y the output set, M_i the i-th message space, R_i the i-th randomness set, Enc_i the i-th encoding function, and Dec *the decoding function. We also define the effectiveness as follows:*

– *A random number* $r \in \vec{R}$ *is said to be* effective *if* $\Pr[r \leftarrow \mathcal{R}] > 0$. *We will denote by* R *the set of effective random numbers.*
– *A tuple of messages* $(m_{i_0}, \ldots, m_{i_d}) \in M_{i_0} \times \cdots \times M_{i_d}$ $(1 \leq i_0 < \cdots < i_d \leq n)$ *is said to be* effective *if there exist an input* $(x_1, \ldots, x_n) \in \vec{X}$ *and an effective random number* $(r_1, \ldots, r_n) \in R$ *such that* $\mathsf{Enc}_{i_j}(x_{i_j}, r_{i_j}) = m_{i_j}$ $(0 \leq j \leq d)$.

That is, a random number or a tuple of messages is said to be effective if it can appear during an execution of protocol Π. In Definition 1, an element r_i of R_i defines a function $X_i \to M_i$ that maps $x_i \in X_i$ to $\mathsf{Enc}_i(x_i, r_i) \in M_i$. This function is also denoted by r_i. We assume without loss of generality that any two elements $r_i \neq r_i'$ of R_i define different functions, since otherwise the correctness and security of the protocol are not affected by identifying r_i with r_i', hence reducing the size of R_i.

2.2 Simplicial Complexes

Let $\Delta \subseteq 2^S$ be a non-empty set of subsets of a finite set S. Δ is said to be a *simplicial complex* with *underlying set* S if $A \in \Delta$ and $B \subseteq A$ imply $B \in \Delta$ for any A, B. An element of Δ is called a *face* of Δ. The *dimension* of a face $A \in \Delta$ is defined by $\mathsf{dim}(A) := |A| - 1$. A maximal element A of Δ with respect to inclusion is called a *facet* of Δ. The set of all facets is denoted by $\mathsf{Facet}(\Delta)$. For a finite set C, a function $\mathsf{color} : \mathsf{Facet}(\Delta) \to C$ is said to be a C*-coloring* of Δ, and $\mathsf{color}(F)$ for a facet F is called the *color* of F.

Let $(S_1, \ldots, S_n)$ be a partition of S. A simplicial complex Δ is said to be n*-partite* with respect to $(S_1, \ldots, S_n)$ if $|A \cap S_i| \leq 1$ for any $A \in \Delta$ and $1 \leq i \leq n$. Moreover, Δ is said to be the *complete* n*-partite simplicial complex* with respect to $(S_1, \ldots, S_n)$ if $\{a_1, \ldots, a_n\} \in \Delta$ for any $a_i \in S_i$ $(1 \leq i \leq n)$. For an n-partite simplicial complex Δ, a face $\{a_{i_0}, a_{i_1}, \ldots, a_{i_d}\} \in \Delta$ $(1 \leq i_0 < i_1 < \cdots < i_d \leq n$, $a_{i_j} \in S_{i_j})$ is often represented by a sequence of length n formed by placing a_{i_j} in the i_j-th position and the symbol '$\perp$' in the remaining positions. For example, when $n = 5$, a face $\{a_1, a_3, a_4\}$ is represented by $(a_1, \perp, a_3, a_4, \perp)$ or $a_1 \perp a_3 a_4 \perp$.

Let Δ and Δ' be n-partite simplicial complexes with respect to $(S_1, \ldots, S_n)$ and $(S_1', \ldots, S_n')$, respectively. Let $\phi = (\phi_1, \ldots, \phi_n)$ be a tuple of n functions $\phi_i \colon S_i \to S_i'$ $(1 \leq i \leq n)$. For a face $A = \{a_{i_0}, \ldots, a_{i_d}\}$ $(a_{i_j} \in S_{i_j})$ of Δ, define $\phi(A) := \{\phi_{i_0}(a_{i_0}), \ldots, \phi_{i_d}(a_{i_d})\}$. We say that ϕ is a *morphism* from Δ to Δ', denoted by $\phi : \Delta \to \Delta'$, if $\mathsf{dim}(\phi(A)) = \mathsf{dim}(A)$ for any $A \in \mathsf{Face}(\Delta)$. If ϕ is injective, ϕ is said to be an *embedding* of Δ into Δ'. If ϕ is bijective, ϕ is said to be an *isomorphism* from Δ to Δ'. When each of Δ and Δ' has a C-coloring, we consider only morphisms ϕ that are consistent with the coloring, that is, those mapping a facet A of Δ onto a facet of Δ' with the same color as A.

2.3 Simplicial Complexes for PSM Protocols

Let $f' : X_1' \times \cdots \times X_n' \to Y'$ be a partial function, and Δ a Y'-colored n-partite simplicial complex with respect to a partition $(X_1', \ldots, X_n')$. Δ is said to be *the simplicial complex defined by* f' if for any $x_i' \in X_i'$ $(1 \leq i \leq n)$, $A = \{x_1', \ldots, x_n'\}$

is a facet of Δ if and only if $f'(x'_1, \ldots, x'_n)$ is defined, and in this case, the color of A coincides with $f'(x'_1, \ldots, x'_n)$.

For a PSM protocol as in Definition 1, let Δ_f and Δ_{Dec} be the simplicial complexes defined by f and Dec, respectively. Then we can observe that the correctness of the PSM protocol is equivalent to the following condition:

> For any effective randomness $r = (r_1, \ldots, r_n) \in R$ viewed as a tuple of functions $X_i \to M_i$, r is a (color-preserving) morphism from Δ_f to Δ_{Dec}.

Furthermore, the security of the PSM protocol can be rewritten as follows:

> For any facets F, F' of Δ_f with the same color and any facet $\widehat{F}$ of Δ_{Dec}, the following equation holds:
>
> $$\Pr_{r \leftarrow \mathcal{R}}[r(F) = \widehat{F}] = \Pr_{r \leftarrow \mathcal{R}}[r(F') = \widehat{F}].$$

We denote the left-hand side of the equation by $\Pr[F \mapsto \widehat{F}]$ and the right-hand side by $\Pr[F' \mapsto \widehat{F}]$. Note that we can remove any ineffective facets (and all faces included in the removed facets only) from Δ_{Dec} without affecting correctness or security. From now on, throughout this paper, we assume that all facets (and therefore all faces) of Δ_{Dec} are effective. In particular, the following is satisfied:

Lemma 1. *Let Π be a PSM protocol for a function f. Then for any facet $\widehat{F}$ of Δ_{Dec} and any facet F of Δ_f with the same color as $\widehat{F}$, there exists an effective randomness $r \in R$ satisfying that $r(F) = \widehat{F}$.*

Proof. Since $\widehat{F}$ is effective as mentioned above, there are a facet F' of Δ_f and an effective $r' \in R$ with $r'(F') = \widehat{F}$, hence $\Pr[F' \mapsto \widehat{F}] > 0$. By the correctness of Π, the color of F' is the same as that of $\widehat{F}$, hence of F as well. Now by the security of Π, we have $\Pr[F \mapsto \widehat{F}] = \Pr[F' \mapsto \widehat{F}] > 0$, implying the claim. □

3 Embedding Methods for Proving Lower Bounds

3.1 Injectivity of the Morphisms Defined by Randomness

In PSM protocols described by simplicial complexes, it is found that a morphism defined by a random number typically results in an embedding of Δ_f into Δ_{Dec}. To elaborate on this, we introduce the following definition.

Definition 2. *A function $f\colon X_1 \times \cdots \times X_n \to Y$ is said to have* no redundant inputs *if for any $i \in [n]$, there do not exist distinct $x_i, x'_i \in X_i$ such that*

$$f(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n) = f(x_1, \ldots, x_{i-1}, x'_i, x_{i+1}, \ldots, x_n)$$

for all $x_j \in X_j$ ($j \in [n]$, $j \neq i$).

Note that we can remove any redundant inputs without affecting correctness or security, hence, we will focus on functions having no redundant inputs.

We also define the following notation.

Definition 3. *The type* $\mathsf{type}(Z)$ *of a* d*-dimensional face* Z *of* Δ_f *is defined as the tuple of indices* $(i_0, \ldots, i_d)$ *with* $1 \leq i_0 < \cdots < i_d \leq n$ *such that* $Z \cap X_{i_j} \neq \emptyset$ *for any* $0 \leq j \leq d$*. The type of a face of* Δ_{Dec} *is defined in the similar way.*

Then the following lemma for the embedding holds.

Lemma 2. *Let* Π *be a PSM protocol for a function* f *having no redundant inputs. Then for any effective* $r = (r_1, \ldots, r_n) \in R$*, each* $r_i \colon X_i \to M_i$ *is injective, and* r *is an embedding from* Δ_f *to* Δ_{Dec}*.*

Proof. First, we show that each r_i is injective. Assume for contradiction that $r_i(x_i) = r_i(x_i')$ for different $x_i, x_i' \in X_i$. From the correctness of Π, we have

$$\begin{aligned} f(x_1, \ldots, x_i, \ldots, x_n) &= \mathsf{Dec}(r_1(x_1), \ldots, r_i(x_i), \ldots, r_n(x_n)) \\ &= \mathsf{Dec}(r_1(x_1), \ldots, r_i(x_i'), \ldots, r_n(x_n)) \\ &= f(x_1, \ldots, x_i', \ldots, x_n) \end{aligned}$$

for any $x_j \in X_j$ $(j \in [n],\ j \neq i)$. This contradicts the assumption that f has no redundant inputs. Therefore, r_i is injective.

It remains to show that $r(Z) \neq r(Z')$ for different faces $Z, Z' \in \Delta_f$ of the same type $(i_0, \ldots, i_d)$. Since $Z \neq Z'$, there is an index i_j such that $Z \cap X_{i_j} \neq Z' \cap X_{i_j}$. Since $r_{i_j} \colon X_{i_j} \to M_{i_j}$ is injective as above, it follows that $r(Z) \cap M_{i_j} \neq r(Z') \cap M_{i_j}$. Therefore, we have $r(Z) \neq r(Z')$. □

3.2 Embedding Lemmas

Let Δ be a simplicial complex with a C-coloring color. For any $j \in C$, we define a function $n_j : \Delta \to \mathbb{N}_{\geq 0}$ by $n_j(Z) := |\mathsf{Facet}(\Delta \mid j, Z)|$, where

$$\mathsf{Facet}(\Delta \mid j, Z) = \{F \in \mathsf{Facet}(\Delta) \mid Z \subseteq F,\ \mathsf{color}(F) = j\}.$$

We define a function $n : \Delta \to (\mathbb{N}_{\geq 0})^{|C|}$ as follows:

$$n(Z) = (n_j(Z))_{j \in C}.$$

We refer to this vector as the *color degree* of the face Z.

Here, we use the same notations as in Section 2.3. Let $Z \in \Delta_f$. We define a subset $\mathcal{F}(Z)$ of Δ_f as the set of all $Z' \in \Delta_f$ such that $\mathsf{type}(Z') = \mathsf{type}(Z)$ and there exists a color $j \in C$ such that $n_j(Z) > 0$ and $n_j(Z') > 0$.

Lemma 3 (Embedding lemma (weak form)). *Let* Π *be a PSM protocol for a function* $f \colon X_1 \times \cdots \times X_n \to Y$ *having no redundant inputs. For any face* Z *of* Δ_f*, there exists a face* $\widehat{Z}$ *of* Δ_{Dec} *such that* $\mathsf{type}(\widehat{Z}) = \mathsf{type}(Z)$ *and for any* $j \in Y$*, the following equation holds:*

$$n_j(\widehat{Z}) \geq N_j := \max\{n_j(Z') \mid Z' \in \mathcal{F}(Z)\}.$$

Proof. Let $r \in R$ be an effective embedding and set $\widehat{Z} := r(Z)$. Let $j \in Y$. Fix any face $Z' \in \mathcal{F}(Z)$. By the definition of $\mathcal{F}(Z)$, $\mathsf{type}(Z') = \mathsf{type}(Z)$ and there exists a color $j' \in Y$ such that $n_{j'}(Z) > 0$ and $n_{j'}(Z') > 0$, hence, there exist facets $F_1, F_2 \in \mathsf{Facet}(\Delta_f)$ with $Z \subseteq F_1,\ Z' \subseteq F_2$ such that $f(F_1) = j' = f(F_2)$. Writing $\widehat{F} := r(F_1)$, we have $\Pr[F_1 \mapsto \widehat{F}] > 0$. From the security of Π, we have $\Pr[F_2 \mapsto \widehat{F}] > 0$, i.e., there exists an effective embedding $r' \in R$ such that $r'(F_2) = \widehat{F}$. Since $\mathsf{type}(Z') = \mathsf{type}(Z)$ and $\widehat{Z} = r(Z) \subseteq r(F_1) = \widehat{F}$, it must hold $r'(Z') = \widehat{Z}$. Since r' is an embedding from Δ_f to Δ_{Dec} by Lemma 2, it gives an injection from $\mathsf{Facet}(\Delta_f \mid j, Z')$ to $\mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid j, \widehat{Z})$, therefore $n_j(\widehat{Z}) \geq n_j(Z')$. Since $Z' \in \mathcal{F}(Z)$ is arbitrary, we have $n_j(\widehat{Z}) \geq N_j$. □

Corollary 1. *Under the same notations as Lemma 3, if* $\mathsf{type}(Z) = (i_0, \ldots, i_d)$, *then the following equation holds:*

$$\prod_{a \in [n] \setminus \{i_0, \ldots, i_d\}} |M_a| \geq \sum_{j \in Y} N_j.$$

Proof. For the face $\widehat{Z} \in \Delta_{\mathsf{Dec}}$ as in Lemma 3, the number of facets of Δ_{Dec} containing $\widehat{Z}$ is $\prod_{a \in [n] \setminus \{i_0, \ldots, i_d\}} |M_a|$, and this value is also written as $\sum_{j \in Y} n_j(\widehat{Z})$. This relation and Lemma 3 proves the claim. □

The following lemma is a strengthened version of Lemma 3, which holds for a certain type of function f.

Lemma 4 (Embedding lemma (strong form)). *Let* Π *be a PSM protocol for a function* f *having no redundant inputs. Fix a type* t *of* Δ_f. *Define*

$$N_j^* := \max\{n_j(Z) \mid Z \in \Delta_f,\ \mathsf{type}(Z) = t\}$$

for $j \in Y$. *Furthermore, assume that there exists a face* $Z \in \Delta_f$ *of type* t *such that all components of the color degree* $n(Z)$ *are positive. Then, for any face* $\widehat{Z}$ *of* Δ_{Dec} *of type* t, *we have* $n_j(\widehat{Z}) \geq N_j^*$ *(*$j \in Y$*).*

Proof. Fix a facet $\widehat{F}_1$ of Δ_{Dec} with color, say j_1, containing $\widehat{Z}$. From the assumption on Z, there exists a facet $F_1 \in \mathsf{Facet}(\Delta_f \mid j_1, Z)$. By Lemma 1, there exists an effective morphism that maps F_1 to $\widehat{F}_1$, hence maps Z to $\widehat{Z}$ since $\mathsf{type}(\widehat{Z}) = \mathsf{type}(Z)$. From the assumption that all components of $n(Z)$ are positive, all components of $n(\widehat{Z})$ are also positive. Now let Z' be any face of Δ_f of type t, and fix a facet F_2 of Δ_f with color, say j_2, containing Z'. Since $n_{j_2}(\widehat{Z}) > 0$ as above, there is a facet $\widehat{F}_2 \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid j_2, \widehat{Z})$. By Lemmas 1 and 2, there exists an effective embedding that maps F_2 to $\widehat{F}_2$ (and hence Z' to $\widehat{Z}$) and gives an injection $\mathsf{Facet}(\Delta_f \mid j, Z') \to \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid j, \widehat{Z})$ for any $j \in Y$, implying $n_j(\widehat{Z}) \geq n_j(Z')$. As Z' is arbitrary, $n_j(\widehat{Z}) \geq N_j^*$, which proves the claim. □

4 Communication Complexity for Concrete Functions

In this section, using the embedding method from Section 3, we provide lower bounds on the communication complexity for concrete functions. For some functions, we also provide upper bounds on it by constructing PSM protocols.

Since the functions f below have no redundant inputs, Lemma 2 implies that any PSM protocol for f must satisfy $|M_i| \geq |X_i|$ for each i (since there is an injection $X_i \to M_i$). Hereafter, we refer to this as the *trivial lower bound*.

4.1 Multiplication in Groups

For a finite group G, let $f\colon G^n \to G$ be the multiplication function $f(x_1, \ldots, x_n) = x_1 \cdots x_n$. As already noted in Section 1.1, the optimal communication complexity for f has been determined to $n \log_2 |G|$. Here, we give another proof of this fact using the embedding method.

Since f has no redundant inputs (by setting the remaining input components to be the identity element 1_G), we have the trivial lower bound $|M_i| \geq |X_i| = |G|$. Since FKN [8] designed a PSM protocol for the function f with $|M_i| = |G|$, it is optimal in terms of the communication complexity. For a special case, by letting $G = \mathbb{Z}_2$ with the group operation $\oplus$ (XOR operation), we can construct a PSM protocol for the n-input XOR function $x_1 \oplus \cdots \oplus x_n$ with $|M_i| = 2$ ($i \in [n]$), which is optimal in terms of the communication complexity.

4.2 AND Function

Let $f\colon \{0,1\}^n \to \{0,1\}$ be the AND function $f(x_1, \ldots, x_n) = x_1 \wedge \cdots \wedge x_n$. f has no redundant inputs (by setting the remaining input components to be 1). For $n = 2$, we gave in Section 1.3 another proof of the lower bound given by DPP [7]. For $n \geq 3$, by using the strong form of the embedding lemma (Lemma 4), we can derive a stronger lower bound in the following.

Theorem 1. *Let $n \geq 3$. For any PSM protocol computing the n-input AND function f, we have $|M_i| \geq 3$ for any i, and if $|M_i| = 3$ for some $i \in [n]$, then $|M_{i'}| \geq 6$ for any $i' \neq i$.*

Proof. As mentioned above, f has no redundant inputs. For any $1 \leq i \leq n$ and any $(n-2)$-dimensional face $Z \in \Delta_f$ with $Z \cap X_i = \emptyset$, the coloring degree of Z is $(n_0(Z), n_1(Z)) = (1, 1)$ if all components of Z are 1 and $(2, 0)$ otherwise. In particular, f satisfies the assumptions of Lemma 4 with $N_0^* = 2$ and $N_1^* = 1$. Hereafter, we will use Lemma 4 without explicit mention. Then the number $|M_i|$ of facets in Δ_{Dec} including any given face of type $(1, \ldots, i-1, i+1, \ldots, n)$ is at least $N_0^* + N_1^* = 3$, therefore the former claim holds. For the remaining claim, since f is symmetric, it suffices to assume $|M_1| = 3$ and $|M_2| \leq 5$ and derive a contradiction. We denote the set of all facets of a simplicial complex Δ of color j by $\mathsf{Facet}(\Delta \mid j)$.

By Lemma 2, we take an effective embedding (called "standard embedding") and denote its image of a vertex $a \in X_i = \{0,1\}$ ($i \in [n]$) by $\widehat{a} \in M_i$. Then,

for any facet $x_1 \cdots x_n$ of Δ_f, $\widehat{x_1} \cdots \widehat{x_n}$ is a facet of Δ_{Dec} of the same color. We specify the colors of the facets of Δ_{Dec}. Here, $a^{n-2} := aa \cdots a$ ($n-2$ a's).

(1). Take a face $\widehat{0}\bot\widehat{0}^{n-2}$ of Δ_{Dec}. By the standard embedding, $\widehat{\widehat{000}}^{n-2}, \widehat{\widehat{010}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$, hence there must exist another facet in $\mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 1)$ including the face $\widehat{0}\bot\widehat{0}^{n-2}$ (since $n_1(\widehat{0}\bot\widehat{0}^{n-2}) \geq N_1^* = 1$). Thus, there exists $\widehat{2} \in M_2 \setminus \{\widehat{0}, \widehat{1}\}$ such that $\widehat{\widehat{020}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 1)$.

(2). Take a face $\bot\widehat{2}\widehat{0}^{n-2}$ of Δ_{Dec}. From (1), $\widehat{0\widehat{2}\widehat{0}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 1)$. Since $|M_1| = 3$ and $n_0(\bot\widehat{2}\widehat{0}^{n-2}) \geq N_0^* = 2$, $\widehat{\widehat{120}}^{n-2}, \widehat{\widehat{220}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$ where we set $M_1 = \{\widehat{0}, \widehat{1}, \widehat{2}\}$.

(3). Take two faces $\bot\widehat{0}\widehat{0}^{n-2}$ and $\bot\widehat{1}\widehat{0}^{n-2}$ of Δ_{Dec}. By the standard embedding, $\widehat{\widehat{000}}^{n-2}, \widehat{\widehat{100}}^{n-2}, \widehat{\widehat{010}}^{n-2}, \widehat{\widehat{110}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$. (Here, we used the condition $n \geq 3$ for $\widehat{\widehat{110}}^{n-2}$.) Thus, $\widehat{\widehat{200}}^{n-2}, \widehat{\widehat{210}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 1)$.

(4). From (2), $\widehat{1\widehat{2}\widehat{0}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$, hence by Lemmas 1 and 2, there exists an effective $r = (r_1, \ldots, r_n) \in R$ such that r maps $000^{n-2} \in \mathsf{Facet}(\Delta_f \mid 0)$ to $\widehat{\widehat{120}}^{n-2}$. This r maps $100^{n-2} \in \mathsf{Facet}(\Delta_f \mid 0)$ to $r_1(1)\widehat{\widehat{20}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$ different from $r(000^{n-2}) = \widehat{\widehat{120}}^{n-2}$. From (1), $\widehat{\widehat{020}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 1)$ and $r_1(1) \neq \widehat{0}, \widehat{1}$, hence, $r_1(1) = \widehat{2}$ and $r(100^{n-2}) = \widehat{\widehat{220}}^{n-2}$.

(5). r maps $110^{n-2} \in \mathsf{Facet}(\Delta_f \mid 0)$ to $\widehat{2}r_2(1)\widehat{0}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$ different from $r(100^{n-2}) = \widehat{\widehat{220}}^{n-2}$. From (3), $\widehat{\widehat{200}}^{n-2}, \widehat{\widehat{210}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 1)$, hence, $r_2(1) \neq \widehat{0}, \widehat{1}, \widehat{2}$. Thus, there exists $\widehat{3} \in M_2 \setminus \{\widehat{0}, \widehat{1}, \widehat{2}\}$ such that $r_2(1) = \widehat{3}$. Therefore, we have $\widehat{2\widehat{3}\widehat{0}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$, and since $r(000^{n-2}) = \widehat{1\widehat{2}\widehat{0}}^{n-2}$ as in (4), we have $r(010^{n-2}) = \widehat{1\widehat{3}\widehat{0}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$.

(6). Take a face $\bot\widehat{3}\widehat{0}^{n-2}$ of Δ_{Dec}. From (5), $\widehat{1\widehat{3}\widehat{0}}^{n-2}, \widehat{2\widehat{3}\widehat{0}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$, hence, $\widehat{0\widehat{3}\widehat{0}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 1)$.

(7). Take a face $\widehat{1}\bot\widehat{0}^{n-2}$ of Δ_{Dec}. From the standard embedding and (2) and (5), we have $\widehat{1\widehat{0}\widehat{0}}^{n-2}, \widehat{1\widehat{1}\widehat{0}}^{n-2}, \widehat{1\widehat{2}\widehat{0}}^{n-2}, \widehat{1\widehat{3}\widehat{0}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$. Thus, there exists $\widehat{4} \in M_2 \setminus \{\widehat{0}, \widehat{1}, \widehat{2}, \widehat{3}\}$ such that $\widehat{1\widehat{4}\widehat{0}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 1)$. Since $|M_2| \leq 5$, we have $M_2 = \{\widehat{0}, \widehat{1}, \widehat{2}, \widehat{3}, \widehat{4}\}$.

(8). Take a face $\bot\widehat{4}\widehat{0}^{n-2}$ of Δ_{Dec}. From (7), $\widehat{1\widehat{4}\widehat{0}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 1)$, hence, $\widehat{0\widehat{4}\widehat{0}}^{n-2}, \widehat{2\widehat{4}\widehat{0}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$.

(9). From (8), $\widehat{0\widehat{4}\widehat{0}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$, hence by Lemmas 1 and 2, there exists an effective $r' = (r'_1, \ldots, r'_n) \in R$ such that r' maps $000^{n-2} \in \mathsf{Facet}(\Delta_f \mid 0)$ to $\widehat{\widehat{040}}^{n-2}$. This r' maps $100^{n-2} \in \mathsf{Facet}(\Delta_f \mid 0)$ to $r'_1(1)\widehat{\widehat{40}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$ different from $r'(000^{n-2}) = \widehat{0\widehat{4}\widehat{0}}^{n-2}$. From (7), $\widehat{1\widehat{4}\widehat{0}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 1)$ and $r'_1(1) \neq \widehat{0}, \widehat{1}$, hence we have $r'_1(1) = \widehat{2}$.

(10). r' maps $010^{n-2} \in \mathsf{Facet}(\Delta_f \mid 0)$ into $\widehat{0}r'_2(1)\widehat{0}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$ different from $r'(000^{n-2}) = \widehat{\widehat{040}}^{n-2}$. From (1) and (6), $\widehat{\widehat{020}}^{n-2}, \widehat{\widehat{030}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 1)$, hence, $r'_2(1) \neq \widehat{2}, \widehat{3}, \widehat{4}$ and $r'_2(1) \in \{\widehat{0}, \widehat{1}\}$. Thus, r' maps $110^{n-2} \in \mathsf{Facet}(\Delta_f \mid 0)$ to $\widehat{2}r'_2(1)\widehat{0}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$, which must be either $\widehat{\widehat{200}}^{n-2}$ or $\widehat{\widehat{210}}^{n-2}$. However, from (3), we have $\widehat{\widehat{200}}^{n-2}, \widehat{\widehat{210}}^{n-2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 1)$, yielding a contradiction.

This completes the proof. □

Corollary 2. *For the PSM protocol for the three-input AND with* $|M_1| \leq |M_2| \leq |M_3|$ *attaining the minimum value of* $\sum_{i=1}^{3} \log_2 |M_i|$, $(|M_1|, |M_2|, |M_3|)$ *is one of* $(3,6,6)$, $(4,4,4)$, $(4,4,5)$, $(4,4,6)$, $(4,4,7)$, $(4,5,5)$, $(4,5,6)$, *and* $(5,5,5)$.

Proof. Since the protocol in [8] satisfies $|M_i| = 5$ for any i, the optimal case satisfies $\prod_{i=1}^{3} |M_i| \leq 5^3 = 125$. Now the claim follows from Theorem 1. □

4.3 Equality Function

Let $f\colon \{0,1\}^n \to \{0,1\}$ be the n-input equality function that outputs 1 if and only if all bits are the same. From the embedding method, we obtain the following lower bound for f.

Theorem 2. *Any PSM protocol for the* n*-input equality function* f *satisfies* $|M_i| \geq 3$ *for any* $i \in [n]$.

Proof. By symmetry, it suffices to show that $|M_n| \geq 3$. Similarly to Section 4.2, f has no redundant inputs. Now the color degrees of faces $Z := 0^{n-1}\perp$ and $Z' := 0^{n-2}1\perp$ of Δ_f are $n(Z) = (1,1)$ and $n(Z') = (2,0)$, respectively. Therefore $Z, Z' \in \mathcal{F}(Z)$ and we have $N_0 \geq \max\{1,2\} = 2$ and $N_1 \geq \max\{1,0\} = 1$ in Corollary 1. Hence $|M_n| \geq N_0 + N_1 \geq 3$ by Corollary 1. □

Let $p \geq n$ be any prime number. We design a PSM protocol for the n-input equality function as follows.

Shared randomness:
- $r_i = (b, c_i)$ $(i \in [n])$, where $b \in \mathbb{Z}_p^\times$ and $c_1, \ldots, c_{n-1} \in \mathbb{Z}_p$ are chosen uniformly at random and $c_n = -\sum_{i=1}^{n-1} c_i \in \mathbb{Z}_p$.

The protocol:
1. P_i, holding $x_i \in \{0,1\}$, computes $m_i = bx_i + c_i \pmod p$ for $i \in [n-1]$ and $m_n = b(p-n+1)x_n + c_n \pmod p$, and sends it to the referee.
2. The referee outputs 1 if $\sum_{i=1}^{n} m_i = 0 \pmod p$ and 0 otherwise.

Communication complexity: $|M_i| = p$.

Proposition 1. *The above protocol is a correct and secure PSM protocol for the* n*-input equality function with* $|M_i| = p$ *for any prime* $p \geq n$.

Proof. Let $\overline{x} := \sum_{i=1}^{n-1} x_i + (p-n+1)x_n \in \mathbb{Z}$. Then $0 \leq \overline{x} \leq p$, and we have $\overline{x} = 0$ (resp., p) if and only if all x_i are 0 (resp., 1). Hence, since $b \in \mathbb{Z}_p^\times$ is uniformly random, $\sum_{i=1}^{n} m_i = b\overline{x} \pmod p$ is 0 if all x_i are equal, and is uniformly random over $\mathbb{Z}_p^\times$ otherwise, implying the correctness. Moreover, due to the uniform choices for the c_i's, $(m_1, \ldots, m_n)$ is uniformly random over all those tuples with $\sum_{i=1}^{n} m_i$ being 0 (resp., uniformly random over $\mathbb{Z}_p^\times$) if $f(x_1, \ldots, x_n) = 1$ (resp., 0). This implies the security. □

Corollary 3. *When* $n = 3$, *the protocol above with* $|M_i| = p := 3$ *is optimal in terms of the communication complexity for the three-input equality function.*

Proof. This follows from Theorem 2 and Proposition 1.

4.4 Majority Function

Let $f\colon \{0,1\}^n \to \{0,1\}$ be the n-input majority function that outputs 1 if and only if $\sum_{i=1}^{n} x_i \geq \lceil n/2 \rceil$. We obtain the following lower bound.

Theorem 3. *Any PSM protocol for the n-input majority function f satisfies $|M_i| \geq 4$ for any $i \in [n]$.*

Proof. By symmetry, we focus on the case $i = n$. Set $m := \lceil n/2 \rceil$. By considering the inputs where except for x_n, $m-1$ bits are 1 and the others are 0, we see that f has no redundant inputs. Then, the color degrees of $Z := 0^{n-m}1^{m-1}\perp$, $Z' := 0^{n-1}\perp$, and $Z'' := 1^{n-1}\perp$ are $(1,1)$, $(2,0)$, and $(0,2)$, respectively. Therefore, by applying Corollary 1 to this Z, since $Z, Z', Z'' \in \mathcal{F}(Z)$, we have $N_0 \geq \max\{1,2,0\} = 2$ and $N_1 \geq \max\{1,0,2\} = 2$, hence $|M_n| \geq N_0 + N_1 \geq 4$. □

We design a PSM protocol for the three-input majority function as follows.

Shared randomness:

- $r_i = (b, c_i)$ $(i \in [3])$, where $b \in \{0,1\}$ and $c_1, c_2 \in \mathbb{Z}_4$ are chosen uniformly at random and $c_3 = -c_1 - c_2 \in \mathbb{Z}_4$.

The protocol:

1. If $b = 0$, P_i, holding $x_i \in \{0,1\}$, computes $m_i = x_i + c_i \pmod 4$. If $b = 1$, P_1 computes $m_1 = 1 - x_1 + c_1 \pmod 4$ and P_i $(i \in \{2,3\})$ computes $m_i = -x_i + c_i$. Each party P_i sends m_i to the referee.
2. The referee computes $m = m_1 + m_2 + m_3 \pmod 4$ and outputs 0 if $m \in \{0,1\}$ and 1 if $m \in \{2,3\}$.

Proposition 2. *The above protocol is a correct and secure PSM protocol for the three-input majority function with $|M_i| = 4$ for $i \in [3]$.*

Proof. A direct calculation shows that when $\overline{x} := \sum_{i=1}^{3} x_i$ is 0, 1, 2, or 3, we have $m = 0$, 1, 2, or 3 if $b = 0$, and $m = 1$, 0, 3, or 2 if $b = 1$, respectively. Then by the uniformly random choices of b and (c_1, c_2, c_3) with $\sum_{i=1}^{3} c_i = 0 \pmod 4$, if $\overline{x} \leq 1$ (resp., $\overline{x} \geq 2$), the tuple (m_1, m_2, m_3) is uniformly random over all those satisfying $m \in \{0,1\}$ (resp., $\{2,3\}$). This implies the claim. □

Corollary 4. *The protocol above with $|M_1| = |M_2| = |M_3| = 4$ is optimal in terms of the communication complexity for the three-input majority function.*

Proof. This follows from Theorem 3 and Proposition 2.

4.5 Comparison Function

Let $k \geq 2$ be an integer. Let $f\colon \{0,1,\ldots,k\}^2 \to \{0,1,2\}$ be the $(k+1)$-valued comparison function $f(x_1, x_2)$ that outputs 0 if $x_1 < x_2$, 1 if $x_1 = x_2$, and 2 if $x_1 > x_2$. When $k = 2$, FKN [8] constructed a PSM protocol satisfying $|M_1| = |M_2| = 7$. From the weak form of the embedding lemma (Lemma 3), we obtain the following lower bound for any $k \geq 2$.

Theorem 4. *Any PSM protocol for the $(k+1)$-valued comparison function f satisfies $|M_i| \geq 2k+1$ for any $i \in [2]$.*

Proof. By comparing inputs of the form (x, x) with (x', x) where $x \neq x'$, we see that f has no redundant inputs. The color degrees of $Z := 0\bot$, $Z' := 1\bot$, and $Z'' := k\bot$ are $n(Z) = (k, 1, 0)$, $n(Z') = (1, 1, k-1)$, and $n(Z'') = (0, 1, k)$, respectively. Therefore, by applying Corollary 1 to Z, since $Z, Z', Z'' \in \mathcal{F}(Z)$, we have $N_0 \geq \max\{k, 1, 0\} = k$, $N_1 \geq \max\{1, 1, 1\} = 1$, and $N_2 \geq \max\{0, k-1, k\} = k$, hence $|M_2| \geq N_0 + N_1 + N_2 = 2k+1$. The case of M_1 is similar.

When $k = 2$, by using the strong form of the embedding lemma (Lemma 4), we can derive a stronger lower bound in the following.

Theorem 5. *When $k = 2$, any PSM protocol for the three-valued comparison function f satisfies either $|M_1| \geq 6$ or $|M_2| \geq 6$.*

Proof. Assume for contradiction that $|M_1| = |M_2| = 5$. As in the proof of Theorem 4, f has no redundant inputs. For Δ_f, since $n(0\bot) = (2, 1, 0)$, $n(1\bot) = (1, 1, 1)$, and $n(2\bot) = (0, 1, 2)$, it satisfies the assumptions of Lemma 4 with $(N_0^*, N_1^*, N_2^*) = (2, 1, 2)$. Thus, from $|M_2| = 5$, it must hold that $n(Z) = (2, 1, 2)$ for any face Z of type (1). Similarly, we have $n(Z) = (2, 1, 2)$ for any face Z of type (2). We use the same notation $\mathsf{Facet}(\Delta \mid j)$ as the proof of Theorem 1.

Similarly to the proof of Theorem 1, for each $i \in [2]$, we write the image of $a \in X_i = \{0, 1, 2\}$ by a fixed ("standard") effective embedding as $\widehat{a} \in M_i$. By Lemmas 1 and 2, there exists an effective $r = (r_1, r_2) \in R$ such that r maps $01 \in \mathsf{Facet}(\Delta_f \mid 0)$ to $\widehat{0}\widehat{2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$. This maps $11 \in \mathsf{Facet}(\Delta_f \mid 1)$ to $r_1(1)\widehat{2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 1)$. From $n_1(\bot\widehat{2}) = 1$ as in the previous paragraph and $\widehat{2}\widehat{2} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 1)$, we have $r_1(1) = \widehat{2}$. Also, r maps $02 \in \mathsf{Facet}(\Delta_f \mid 0)$ to $\widehat{0}r_2(2) \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 0)$, which is different from $r(01) = \widehat{0}\widehat{2}$. From $n_0(\widehat{0}\bot) = 2$, $\widehat{0}r_2(2)$ must be $\widehat{0}\widehat{1}$, i.e., $r_2(2) = \widehat{1}$. Then r maps $12 \in \mathsf{Facet}(\Delta_f \mid 0)$ to $r_1(1)r_2(2) = \widehat{2}\widehat{1} \in \mathsf{Facet}(\Delta_{\mathsf{Dec}} \mid 2)$, a contradiction. This implies the claim. □

Corollary 5. *For the PSM protocol for the three-valued comparison function with $|M_1| \leq |M_2|$ attaining the minimum value of $\sum_{i=1}^{2} \log_2 |M_i|$, we have*

$$(|M_1|, |M_2|) \in \{(5,6), (5,7), (5,8), (5,9), (6,6), (6,7), (6,8), (7,7)\}.$$

Proof. Since the protocol in [8] mentioned above satisfies $|M_1| = |M_2| = 7$, the optimal case satisfies $|M_1| \cdot |M_2| \leq 7^2 = 49$. Now the claim follows from Theorem 4 (with $k = 2$) and Theorem 5. □

4.6 Multiplication over Finite Rings

For any (not necessarily commutative) finite ring S, let $f\colon S^2 \to S$ be the multiplication function $f(x_1, x_2) = x_1 x_2$. In the following, we design a PSM protocol for f by using the idea of Beaver multiplication triples.

Shared randomness:

– $r_1 = (a, b, c_1)$, $r_2 = (a, b, c_2)$, where a, b, c_1 are uniformly random elements of S and $c_2 = -c_1$.

The protocol:

1. P_1, holding $x_1 \in S$, computes $m_1 = (m_{1,1}, m_{1,2}) = (x_1 - a, x_1 b - ab + c_1)$. P_2, holding $x_2 \in S$, computes $m_2 = (m_{2,1}, m_{2,2}) = (x_2 - b, ax_2 + c_2)$. Each party P_i sends m_i to the referee.
2. The referee outputs $m_{1,1}m_{2,1} + m_{1,2} + m_{2,2} \in S$.

Proposition 3. *The above protocol is a correct and secure PSM protocol for the multiplication function f over a finite ring S with $|M_i| = |S|^2$ for $i \in [2]$.*

Proof. The correctness follows from the following computation:

$$\begin{aligned} m_{1,1}m_{2,1} + m_{1,2} + m_{2,2} &= (x_1 - a)(x_2 - b) + (x_1 b - ab + c_1) + (ax_2 + c_2) \\ &= x_1x_2 - x_1b - ax_2 + ab + x_1b - ab + c_1 + ax_2 + c_2 \\ &= x_1x_2 + c_1 + c_2 = x_1x_2. \end{aligned}$$

To prove the security, we compute the probability that given $m'_{1,1}$, $m'_{1,2}$, $m'_{2,1}$, $m'_{2,2} \in S$ with $m'_{1,1}m'_{2,1} + m'_{1,2} + m'_{2,2} = x_1x_2$, both $m_1 = (m'_{1,1}, m'_{1,2})$ and $m_2 = (m'_{2,1}, m'_{2,2})$ hold. First, from $m_{1,1} = m'_{1,1}$ and $m_{2,1} = m'_{2,1}$, we must have $a = x_1 - m'_{1,1}$ and $b = x_2 - m'_{2,1}$, which hold with probability $|S|^{-2}$. Then, under the condition that these a, b are chosen, we have

$$\begin{aligned} m_{1,2} &= x_1 b - ab + c_1 \\ &= x_1(x_2 - m'_{2,1}) - (x_1 - m'_{1,1})(x_2 - m'_{2,1}) + c_1 \\ &= x_1x_2 - x_1m'_{2,1} - x_1x_2 + x_1m'_{2,1} + m'_{1,1}x_2 - m'_{1,1}m'_{2,1} + c_1 \\ &= m'_{1,1}x_2 - m'_{1,1}m'_{2,1} + c_1, \\ m_{2,2} &= ax_2 + c_2 = (x_1 - m'_{1,1})x_2 + c_2 = x_1x_2 - m'_{1,1}x_2 + c_2. \end{aligned}$$

Therefore, from $m_{1,2} = m'_{1,2}$ and $m_{2,2} = m'_{2,2}$, we must have

$$c_1 = m'_{1,2} - m'_{1,1}x_2 + m'_{1,1}m'_{2,1}\,,\ c_2 = m'_{2,2} - x_1x_2 + m'_{1,1}x_2.$$

Since they satisfy

$$c_1 + c_2 = m'_{1,1}m'_{2,1} + m'_{1,2} + m'_{2,2} - x_1x_2 = 0,$$

the probability that these c_1, c_2 are chosen is $|S|^{-1}$. In summary, the probability that $m_1 = (m'_{1,1}, m'_{1,2})$ and $m_2 = (m'_{2,1}, m'_{2,2})$ is $|S|^{-3}$, which does not depend on the inputs (x_1, x_2). This proves the security. □

Let $q \geq 2$ be a prime power. When $S = \mathbb{F}_q$, the field of order q, we obtain the following lower bound.

Theorem 6. *Any PSM protocol for the multiplication function f over the finite field $\mathbb{F}_q$ satisfies $|M_1|, |M_2| \geq 2q - 1$.*

Proof. The color degrees of faces $Z := 1\perp$ and $Z' := 0\perp$ of Δ_f are $n(Z) = (1, 1, \ldots, 1)$ and $n(Z') = (q, 0, \ldots, 0)$, respectively. From the strong version of the embedding lemma, since $N_0^* \geq \max\{q, 1\} = q$ and $N_j^* \geq \max\{1, 0\} = 1$ $(j \neq 0)$, we have $|M_2| \geq q + (q-1) \cdot 1 = 2q - 1$. By symmetry, $|M_1| \geq 2q - 1$. □

Let $q \geq 2$ be any integer. When $S = \mathbb{Z}_q$, the integer residue ring modulo q, we obtain the following lower bound.

Theorem 7. *Any PSM protocol for the multiplication function f over $\mathbb{Z}_q$ satisfies $|M_1|, |M_2| \geq \sum_{i=1}^{q} \gcd(i, q)$.*

Proof. By symmetry, we focus on M_2. For $j \in \mathbb{Z}_q$ and a face $x\perp$ of Δ_f with $x \in \mathbb{Z}_q$, we have $n_j(x\perp) = |A_{j,x}|$ where $A_{j,x} := \{c \in \mathbb{Z}_q \mid c \cdot x = j \pmod q\}$. In particular, $n_j(1\perp) = 1$ for any j. Hence by the strong version of the embedding lemma, we have $|M_2| \geq \sum_{j \in \mathbb{Z}_q} N_j^* \geq \sum_{j \in \mathbb{Z}_q} \max_{x \in \mathbb{Z}_q} |A_{j,x}|$. Therefore, it suffices to show that $\gcd(j, q) = \max_{x \in \mathbb{Z}_q} |A_{j,x}|$ for any $j \in \mathbb{Z}_q$.

We write $d := \gcd(j, q)$ and $\delta_x := \gcd(x, d)$. Then any $c \in A_{j,x}$ satisfies that $c \cdot x = 0 \pmod d$ and hence $c \cdot (x/\delta_x) = 0 \pmod{d/\delta_x}$, therefore $c = 0 \pmod{d/\delta_x}$ since $\gcd(d/\delta_x, x/\delta_x) = 1$. Hence $c \mapsto c/(d/\delta_x)$ gives an injection $A_{j,x} \to A_{j,x \cdot d/\delta_x}$, and d divides $x \cdot d/\delta_x = d \cdot x/\delta_x$. Therefore, to show the claim, it suffices to consider $x \in \mathbb{Z}_q$ that is a multiple of d. Write $q = dq_0$, $j = dj_0$, and $x = dx_0$. Now $c \in \mathbb{Z}_q$ belongs to $A_{j,x}$ if and only if $c \cdot x_0 = j_0 \pmod{q_0}$. Since $\gcd(j_0, q_0) = 1$ by the definition of d, the condition for c is equivalent to $\gcd(x_0, q_0) = 1$ and $c = j_0 \cdot (x_0)^{-1} \pmod{q_0}$ where $(x_0)^{-1}$ is the inverse of x_0 modulo q_0. Hence we have $\max_{x \in \mathbb{Z}_q} |A_{j,x}| = q/q_0 = d = \gcd(j, q)$, as desired. □

Acknowledgments

This work was supported by JSPS KAKENHI Grant Numbers JP19H01109, JP21K17702, JP22K11906, and JP23H00479, and JST CREST Grant Number JPMJCR22M1, Japan. This work was supported by Institute of Mathematics for Industry, Joint Usage/Research Center in Kyushu University. (FY2022 Short-term Visiting Researcher "On Minimal Construction of Private Simultaneous Messages Protocols" (2022a006) and FY2023 Short-term Visiting Researcher "On the Relationship between Physical and Non-physical Secure Computation Protocols" (2023a009).)

References

1. B. Applebaum, T. Holenstein, M. Mishra, and O. Shayevitz. The communication complexity of private simultaneous messages, revisited. *Journal of Cryptology*, volume 33, number 3, pages 917–953, 2020.
2. L. Assouline and T. Liu. Multi-party PSM, revisited. In *TCC 2021*, pages 194–223. Springer, 2021.
3. M. Ball, J. Holmgren, Y. Ishai, T. Liu, and T. Malkin. On the complexity of decomposable randomized encodings, or: how friendly can a garbling-friendly PRF be? In *ITCS 2020*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2020.

4. M. Ball and T. Randolph. A note on the complexity of private simultaneous messages with many parties. In *ITC 2022*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2022.
5. A. Beimel, Y. Ishai, R. Kumaresan, and E. Kushilevitz. On the Cryptographic Complexity of the Worst Functions. In *TCC 2014*, pages 317–342. Springer, 2014.
6. A. Beimel, E. Kushilevitz, and P. Nissim. The complexity of multiparty PSM protocols and related models. In *EUROCRYPT 2018*, pages 287–318. Springer, 2018.
7. D. Data, M. Prabhakaran, and V. M. Prabhakaran. On the communication complexity of secure computation. In *CRYPTO 2014*, volume 8617 of *Lecture Notes in Computer Science*, pages 199–216. Springer, 2014.
8. U. Feige, J. Killian, and M. Naor. A minimal model for secure computation. In *Proceedings of the 26th ACM STOC*, pages 554–563, 1994.
9. Y. Ishai and E. Kushilevitz. Private simultaneous messages protocols with applications. In *Proceedings of the 5th Israeli Symposium on Theory of Computing and Systems (ISTCS 1997)*, pages 174–183. IEEE, 1997.
10. K. Shinagawa, R. Eriguchi, S. Satake, and K. Nuida. Private simultaneous messages based on quadratic residues, *Designs, Codes and Cryptography* (to appear).
11. V. Vaikuntanathan. Some open problems in information-theoretic cryptography. In *37th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2017)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.