Ideal Private Simultaneous Messages Schemes and Their Applications

Keitaro Hiwatashi[1]
National Institute of Advanced Industrial Science and Technology, Tokyo, Japan

Reo Eriguchi
National Institute of Advanced Industrial Science and Technology, Tokyo, Japan

Abstract

Private Simultaneous Messages (PSM) is a minimal model for secure computation, where two parties, Alice and Bob, have private inputs x, y and a shared random string. Each of them sends a single message to an external party, Charlie, who can compute $f(x, y)$ for a public function f but learns nothing else. The problem of narrowing the gap between upper and lower bounds on the communication complexity of PSM has been widely studied, but the gap still remains exponential. In this work, we study the communication complexity of PSM from a different perspective and introduce a special class of PSM, referred to as *ideal PSM*, in which each party's message length attains the minimum, that is, their messages are taken from the same domain as inputs. We initiate a systematic study of ideal PSM with a complete characterization, several positive results, and applications. First, we provide a characterization of the class of functions that admit ideal PSM, based on permutation groups acting on the input domain. This characterization allows us to derive asymptotic upper bounds on the total number of such functions and a complete list for small domains. We also present several infinite families of functions of practical interest that admit ideal PSM. Interestingly, by simply restricting the input domains of these ideal PSM schemes, we can recover most of the existing PSM schemes that achieve the best known communication complexity in various computation models. As applications, we show that these ideal PSM schemes yield novel communication-efficient PSM schemes for functions with sparse or dense truth-tables and those with low-rank truth-tables. Furthermore, we obtain a PSM scheme for general functions that improves the constant factor in the dominant term of the best known communication complexity. An additional advantage is that our scheme simplifies the existing construction by avoiding the hierarchical design of internally invoking PSM schemes for smaller functions.

2012 ACM Subject Classification Theory of computation → Cryptographic primitives

Keywords and phrases secure computation, private simultaneous messages, communication complexity

Digital Object Identifier 10.4230/LIPIcs.ITCS.2026.76

Related Version *Full Version*: `https://eprint.iacr.org/2025/2217`

Funding This work was supported in part by JST CREST Grant Number JPMJCR22M1, JST K Program Grant Number JPMJKP24U3, and JSPS KAKENHI Grant Numbers 24K20775.

Acknowledgements We would like to thank Koji Nuida for his helpful comments.

1 Introduction

Secure computation [49] is a fundamental cryptographic primitive which enables two parties, Alice and Bob, to evaluate a function f over their joint inputs without revealing information other than the output. This problem has been considered in several different models and settings (see, e.g., [12, 17, 20–22, 30]). In this work, we consider this problem in a minimal

[1] corresponding author

model for communication in the setting of information-theoretic security, referred to as *Private Simultaneous Messages (PSM)* model [29, 33]. In a (two-party) PSM scheme, Alice holds an input x, Bob holds an input y, and they both share common randomness. Each of them sends a message to an external party, Charlie, who can then compute $f(x, y)$ but learns nothing else.

The central research question is to determine the minimum communication complexity of PSM schemes for a given function f, where communication complexity is defined as the total bit-length of Alice's and Bob's messages. This question has been extensively studied for general functions as well as for functions with specific representations [2, 3, 6, 7, 9, 23, 25, 34, 47]. The currently best known construction for a general function $f : X \times X \to \{0, 1\}$ provides a PSM scheme with communication complexity $O(\sqrt{N})$, where N denotes the cardinality of X [7]. Whereas, the lower bound of $3 \log N - O(\log \log N)$ bits is derived for certain functions [2]. Despite all the progresses, however, there still remains an exponential gap between upper and lower bounds.

In this work, we depart from prior approaches aimed at narrowing the exponential gap and study the communication complexity of PSM from a different perspective. It is clear that a communication complexity of $2 \log N$ bits is trivially unavoidable in light of the input length[2]. Thus, if a PSM scheme has communication complexity equal to the input length of f, then it is necessarily communication-optimal. We will refer to such schemes as *ideal PSM schemes*. Due to the lower bounds by [2, 23, 47], not every function admits ideal PSM. Nevertheless, some special functions of interest admit ideal PSM. For example, the function that computes the sum $x + y$ over an abelian group is realized by a PSM scheme where Alice sends $x + r$ and Bob sends $y - r$ for a uniformly random element r. This scheme is ideal since messages are taken from the same domain as inputs. The main goal of this work is to give a complete characterization of functions that admit ideal PSM.

This research direction is inspired by a series of works on *ideal secret sharing schemes* [11, 15, 18, 26–28, 42, 48]. A secret sharing scheme is called ideal if the size of every share is equal to that of a secret, which is proven to be the optimal size [37]. While a complete characterization is not known, several classes of access structures are proven to admit ideal secret sharing schemes (see Section 1.2 for details). We are the first to conduct a systematic study of ideal PSM schemes, in analogy with ideal secret sharing schemes.

1.1 Our Results

In this work, we initiate a theory of ideal PSM schemes with a complete characterization, several positive results, and applications. As an interesting implication, our results provide a unified perspective on existing PSM constructions achieving the best known communication complexity, and moreover yield novel and more efficient constructions. First, we show a necessary and sufficient condition for functions to admit ideal PSM, using group-theoretic terminology. Specifically, we prove that such functions are essentially limited to a family of functions induced by certain permutation groups on the input domain. This characterization allows us to derive asymptotic upper bounds on the number of functions admitting ideal PSM and a complete list when the domain size N is small (e.g., up to $N \leq 23$ for boolean functions). We also provide several infinite families of functions of special interest that admit ideal PSM schemes, including the sum function mentioned above. As applications,

[2] Note that if a non-zero probability of failure is allowed in the reconstruction, this lower bound does not apply. Throughout this paper, we focus on PSM with perfect correctness.

we propose novel communication-efficient PSM schemes for functions with sparse/dense or low-rank truth-tables, improving upon the previous construction for functions with bounded tiling number [41]. Furthermore, we reduce the constant factor in the dominant term of the best known communication complexity for general functions [7], from $12\sqrt{N}$ to $8\sqrt{N}$. Below, we elaborate on our results.

1.1.1 Characterization

We say that a PSM scheme is ideal if the message space of each party i is the same as X_i. A function $f : X_0 \times X_1 \to Y$ is called an ideal PSM function if there exists an ideal PSM scheme for f. To formalize our characterization, we introduce the *invariant group* I_f of f, defined as the set of all pairs of permutations $\pi = (\pi_0, \pi_1)$, where each π_i acts on X_i, such that $f(\pi_0(x), \pi_1(y)) = f(x, y)$ for all $(x, y) \in X_0 \times X_1$. This group naturally acts on $X_0 \times X_1$. We show that f is an ideal PSM function if and only if I_f satisfies the following condition: for any pair of inputs $(x, y), (x', y') \in X_0 \times X_1$ such that $f(x, y) = f(x', y')$, there exists a permutation $\pi \in I_f$ such that $(x', y') = \pi(x, y)$. This characterization makes it easier to test if a given function admits ideal PSM, by finding an appropriate permutation that preserves the outputs of f.

A key technical idea in our characterization is that the class of ideal PSM functions is essentially restricted to a special subclass, that is, every ideal PSM function is equivalent to one of them[3]. Specifically, each function $f_{\mathcal{G}}$ in the subclass is parameterized by a tuple $\mathcal{G} = (G_0, G_1, \psi)$, where G_i is a subgroup of permutations on X_i and ψ is an isomorphism from G_0 to G_1, and $f_{\mathcal{G}}$ maps each input (x, y) to its *orbit* under the action of $\mathcal{G}$ on $X_0 \times X_1$. We show that any function f admitting ideal PSM is equivalent to $f_{\mathcal{G}}$ for some $\mathcal{G}$. This formalization is useful for the enumeration of ideal PSM functions since it reduces the problem to the enumeration of all such tuples $\mathcal{G}$.

1.1.2 Enumeration

We provide asymptotic upper bounds on the total number of connected functions $f : X_0 \times X_1 \to Y$ that admit ideal PSM. Here, we additionally assume that f is connected, meaning that there exists no partition of $X_0 \times X_1$ into rectangles each of which corresponds to disjoint values of f. In the boolean case $Y = \{0, 1\}$, this assumption excludes only a few trivial functions and does not affect the asymptotic results. Note that naively enumerating all tuples $\mathcal{G}$ cannot yield a non-trivial upper bound. This is because a permutation group of degree N contains at least $2^{\Omega(N^2)}$ subgroups [43], implying that such a naive enumeration cannot improve upon the trivial bound of 2^{N^2} given by the total number of functions. We leverage group-theoretic properties of ideal PSM functions to remove duplicate counts of $\mathcal{G}$'s that correspond to equivalent functions. As a result, we obtain a non-trivial upper bound of $2^{O(N \log^2 N)}$ on the number of ideal PSM functions, where $N = \max\{|X_0|, |X_1|\}$. Furthermore, if $|X_0|$ and $|X_1|$ are primes, we can significantly improve the upper bound to $2^{O(\log^3 N)}$. These bounds demonstrate that the fraction of ideal PSM functions is exponentially small compared to the set of all functions.

We provide a complete list of ideal PSM functions for small domains by enumerating all tuples $\mathcal{G}$ determining non-equivalent functions $f_{\mathcal{G}}$. We use an open software package called GAP to enumerate permutation groups[4]. For a general range Y, we obtain a list of

[3] We say that two functions are *equivalent* if they are identical up to permutations of inputs and outputs.
[4] `https://www.gap-system.org/about/`

such functions up to $N \leq 15$ except for the case of $|X_0| = |X_1| = 12$. For a boolean case $Y = \{0, 1\}$, we show that each equivalence class of ideal PSM functions corresponds to a connected component of a certain graph, leading to substantial reduction in computational cost. As a result, we obtain a larger list of functions up to $N \leq 23$ in the boolean case. The resulting lists are available in [1].

1.1.3 Infinite Families

We show that the following families of practically relevant functions admit ideal PSM schemes:

- *Group product.* This function computes the iterated product of a combined sequence of (possibly non-commutative) group elements held by two parties.
- *Index function.* This function takes a function $\phi : H \to G$ from a certain class and a pair $(x, r) \in H \times G$ as input, and outputs $\phi(x) - r$, where H and G are abelian groups. This family generalizes the original notion of the index function [29, 38], which outputs D_x on input a vector $D = (D_i)_{1 \leq i \leq N}$ and an index x. It also includes the inner product and multi-linear polynomials as special cases.
- *Private set intersection cardinality (PSIC).* This function takes two subsets A_0 and A_1 of a common set as input and outputs $|A_0 \cap A_1|$. This family particularly includes the equality function, which tests the equality of two elements.

In particular, we are the first to consider PSIC functions in the PSM setting and to show a communication-optimal construction for them.

Interestingly, by simply restricting the input domains of the above ideal PSM schemes, we can recover most of the existing PSM schemes that achieve the state-of-the-art communication complexity in various computation models. The best known schemes for branching programs [29] and arithmetic formulas [19, 34] are obtained by evaluating the group product over restricted inputs. The nearly optimal construction for polynomials [38] is also obtained by computing a generalized index function, where ϕ is taken to be a multi-linear polynomial. As explained below, the previous constructions [3, 7] can be even refined and simplified within our framework based on ideal PSM schemes.

1.1.4 Communication-efficient and Simplified Constructions

We demonstrate that ideal PSM schemes for the above function families induce more communication-efficient PSM schemes for several functions. First, we consider a function $f : X \times X \to \{0, 1\}$ such that the number of 1's in each row of its truth-table T_f (viewed as a matrix) is at most $d \ll N := |X|$. Prior to our work, the only general construction in [7] can apply, resulting in communication complexity of $O(\sqrt{N})$. In contrast, by embedding T_f to the truth-table of a PSIC function, we obtain a novel PSM scheme for f with communication complexity $O(d \log(N + d))$, implying a strict improvement when $d = o(\sqrt{N}/\log N)$. The same communication complexity can be attained when the columns are sparse as well as when the rows (or columns) are dense, that is, they contain at least $n - d$ ones for a small d.

Next, Narayanan et al. [41] showed that a function $f : X \times X \to Y$ can be realized by a PSM scheme with communication complexity $O(k_f \log |Y|)$, where k_f denotes the tiling number of f. Here, the tiling number refers to the smallest number of disjoint monochromatic rectangles covering the truth-table T_f. On the other hand, by embedding T_f to the truth-table of the inner product, we present a novel PSM scheme for f with communication complexity $O(r_f \log |Y|)$, where r_f denotes the rank of T_f as a matrix over some field of size at least $|Y|$. As is well known, it always holds that $k_f \geq r_f$ (e.g., [31]) and thus our scheme achieves a more refined communication complexity.

Finally, Beimel et al. [7] presented a PSM scheme for a general function $f : X \times X \to \{0,1\}$ with communication complexity $O(\sqrt{N})$, which is at least $12\sqrt{N}$, where $N = |X|$. In contrast, we adopt a different approach based on ideal PSM schemes to improve and simplify their construction. We show an ideal PSM function $G_f : X' \times X' \to \{0,1\}$ with $\log |X'| = 4\sqrt{N} + 1$ that contains f as a restriction. As a result, we obtain a PSM scheme for f with communication complexity $8\sqrt{N} + 2$ from the ideal PSM scheme for G_f, improving the constant factor in the dominant term of [7]. An additional benefit is that our construction is simpler and more direct: Alice and Bob can compute their messages simply by applying explicitly given permutations to their inputs. As a result, the message functions of our scheme can be expressed in closed form and avoid the hierarchical design of [3, 7], which relies on nested invocations of PSM schemes for smaller functions.

1.2 Related Work

We provide a brief history of the problem of determining the optimal communication complexity of PSM schemes. Feige et al. [29] formalized the notion of PSM schemes and presented the feasibility result of two-party PSM for general functions. Ishai and Kushilevitz [33] extended this to the multi-party setting and showed a k-party PSM scheme for functions represented by branching programs. These constructions, along with several variants including PSM for arithmetic formulas, are summarized in [34]. Subsequently, Beimel et al. [7] successfully devised a two-party PSM scheme for general functions $f : X \times X \to \{0,1\}$ with communication complexity $O(\sqrt{|X|})$. This result was later generalized and improved by [3,9], leading to k-party PSM schemes with communication complexity $O(|X|^{(k-1)/2})$, omitting factors that depend only on k. Another direction aims at obtaining more communication-efficient PSM schemes for functions of special interest. For example, a series of works [6, 13, 24, 25, 46] presented several "tailor-made" constructions for *symmetric* functions, whose outputs are independent of the order of inputs. PSM schemes have been used to obtain many other cryptographic primitives, e.g., secure computation with general interaction patterns [32], constant-round secure computation [35,36], and conditional disclosure of secrets [38,39]. The model of PSM schemes has also been generalized into different scenarios such as ad-hoc PSM [5,8] where only a subset of the parties actually send messages, and robust PSM (also known as non-interactive secure computation) [6, 13] where an external party may corrupt some parties.

There are known lower bounds on the communication complexity of PSM. Applebaum et al. [2] proved a lower bound of $3 \log N - O(\log \log N)$ for the two-party case, and Ball and Randolph [4] showed a lower bound that is roughly $k^2 \log N$ for k-party PSM when $k = \omega(\log \log N)$. Tighter upper and lower bounds are known for concrete functions with small input domains and/or a small number of parties, including the n-bit AND function [23,29,47], the multi-input equality function [47], and the majority function [47].

A secret sharing scheme [14, 45] is a cryptographic primitive, which divides a secret x into k shares in such a way that x can be recovered from any authorized set of shares while no information on x is revealed from any unauthorized set of shares. The collection of all authorized sets, namely sets of shares that can recover a secret, is called its access structure. A secret sharing scheme is called ideal if each share is taken from the same domain as secrets [15]. Since the size of each share cannot be smaller than the secret size [37], ideal secret sharing schemes necessarily achieve the optimal share size. A series of works have shown that several classes of access structures admit ideal secret sharing schemes [11, 18, 26–28, 42, 48], and found interesting connections to combinatorics and information theory [10, 16, 40]. Despite all these progresses, the exact characterization of access structures admitting ideal secret sharing schemes is a longstanding open problem.

2 Overview of Our Techniques

2.1 Ideal PSM: Definition and Characterization

In a (two-party) PSM scheme, each of two parties has common randomness $r \in R$ and an input $x_i \in X_i$. Then, each party sends a single message $m_i \in M_i$ to an external party, from which he learns $f(x_0, x_1)$ for a public function $f : X_0 \times X_1 \to Y$. The PSM scheme specifies a randomized algorithm Gen to sample r, message functions $\mathsf{Msg}_i : X_i \times R_i \to M_i$ that computes m_i from (x_i, r), and an evaluation function $\mathsf{Eval} : M_0 \times M_1 \to Y$ that outputs $f(x_0, x_1)$ from (m_0, m_1). The privacy requirement is that the distribution of messages does not leak any information on the inputs other than $f(x_0, x_1)$. We say that the PSM scheme is *ideal* if parties' messages are taken from the same domain as inputs, i.e., $M_i = X_i$. A function f is called an *ideal PSM function* if there exists an ideal PSM scheme for f. The communication complexity of ideal PSM schemes cannot be reduced further if f is non-degenerate, by which we mean that its truth-table has no identical rows or columns. Throughout the paper, we only consider non-degenerate functions as the computation of degenerate functions is reduced to the computation of a smaller non-degenerate function.

We introduce a special class of ideal PSM schemes. As will be shown later, these schemes are canonical in the sense that every function admitting ideal PSM can be realized by some ideal PSM scheme in this class. Each of them is parameterized by a tuple $\mathcal{G} = (G_0, G_1, \psi)$, where G_i is a subgroup of the group $\mathcal{S}_{X_i}$ of all permutations over X_i, and ψ is an isomorphism from G_0 to G_1, that is, ψ maps a permutation belonging to G_0 to another permutation belonging to G_1. We define a group $\Gamma_\mathcal{G}$ as $\Gamma_\mathcal{G} = \{(\pi_0, \pi_1) \in G_0 \times G_1 : \pi_1 = \psi(\pi_0)\}$. Then, $\Gamma_\mathcal{G}$ naturally acts on $X_0 \times X_1$ as it is a subgroup of $\mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$, and thus specifies the set of *orbits*, $Y_\mathcal{G} = \{\mathrm{Orb}_{\Gamma_\mathcal{G}}(x_0, x_1) : (x_0, x_1) \in X_0 \times X_1\}$, where $\mathrm{Orb}_{\Gamma_\mathcal{G}}(x_0, x_1) = \{(\pi_0(x_0), \pi_1(x_1)) : (\pi_0, \pi_1) \in \Gamma_\mathcal{G}\}$. We define $f_\mathcal{G} : X_0 \times X_1 \to Y_\mathcal{G}$ as a function that maps each input to its orbit, namely

$$f_\mathcal{G}(x_0, x_1) = \mathrm{Orb}_{\Gamma_\mathcal{G}}(x_0, x_1).$$

We can construct an ideal PSM scheme $\Pi_\mathcal{G}$ for $f_\mathcal{G}$ as follows:

- Gen samples a permutation $\pi = (\pi_0, \pi_1)$ chosen from $\Gamma_\mathcal{G}$ uniformly at random.
- Msg_i applies the permutation π to an input x_i, namely $\mathsf{Msg}_i(x_i, \pi) = \pi_i(x_i)$.
- Eval outputs the orbit of messages (m_0, m_1), namely $\mathsf{Eval}(m_0, m_1) = \mathrm{Orb}_{\Gamma_\mathcal{G}}(m_0, m_1)$.

Since an orbit of (x_0, x_1) is invariant under a permutation $\pi \in \Gamma_\mathcal{G}$, $\Pi_\mathcal{G}$ correctly computes $f_\mathcal{G}$. Furthermore, if $f_\mathcal{G}(x_0, x_1) = f_\mathcal{G}(x'_0, x'_1)$, then (x_0, x_1) and (x'_0, x'_1) are mapped to each other by some permutation $\pi \in \Gamma_\mathcal{G}$ as their orbits are identical, implying the privacy of $\Pi_\mathcal{G}$.

We show that every ideal PSM function $f : X_0 \times X_1 \to Y$ is equivalent (that is, identical up to permutations of inputs and outputs) to $f_\mathcal{G}$ for some $\mathcal{G}$. We obtain this characterization by proving that the following conditions are equivalent:

1. f is an ideal PSM function.
2. For any two inputs $(x_0, x_1), (x'_0, x'_1)$ such that $f(x_0, x_1) = f(x'_0, x'_1)$, there exists a pair of permutations $\pi = (\pi_0, \pi_1) \in \mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$ such that
   - $\pi(x_0, x_1) = (\pi_0(x_0), \pi_1(x_1)) = (x'_0, x'_1)$.
   - $\pi \in I_f$, i.e., the values of f are invariant under π.
3. f is equivalent to $f_\mathcal{G}$ for some $\mathcal{G}$.

We have already seen the implication $3 \Rightarrow 1$.

To prove the implication $1 \Rightarrow 2$, we observe that since $M_i = X_i$ in an ideal PSM scheme, the message function $\mathsf{Msg}_i(\cdot, r)$ induces a permutation π^i_r over X_i for a random string $r \in R$. We construct S as a group generated by all such permutations (π^0_r, π^1_r)'s. We also

observe that an ideal PSM scheme for f can be transformed into an ideal PSM scheme whose evaluation function is identical to f, namely $\mathsf{Eval}(m_0, m_1) = f(m_0, m_1)$. Then, the correctness property ensures that any permutation in S preserves the outputs of f since $f(\pi_r^0(x_0), \pi_r^1(x_1)) = \mathsf{Eval}(\mathsf{Msg}_0(x_0, r), \mathsf{Msg}_1(x_1, r)) = f(x_0, x_1)$. Furthermore, the privacy property ensures that if $f(x_0, x_1) = f(x_0', x_1')$, then there exist random strings $r, r' \in R$ such that $(\mathsf{Msg}_0(x_0, r), \mathsf{Msg}_1(x_1, r)) = (\mathsf{Msg}_0(x_0', r'), \mathsf{Msg}_1(x_1', r'))$. This implies that there exists a permutation $\pi \in S$ that maps (x_0, x_1) to (x_0', x_1').

To prove the implication $2 \Rightarrow 3$, we show a one-to-one correspondence between the set of orbits under the action of I_f and the range of f, that is,

$$\{\mathrm{Orb}_{I_f}(x_0, x_1) : (x_0, x_1) \in X_0 \times X_1\} \overset{\text{1-to-1}}{\longleftrightarrow} \{f(x_0, x_1) : (x_0, x_1) \in X_0 \times X_1\}.$$

Indeed, if $\mathrm{Orb}_{I_f}(x_0, x_1) = \mathrm{Orb}_{I_f}(x_0', x_1')$, then the values of f on them are identical since f is invariant under any permutation in I_f. Conversely, if $f(x_0, x_1) = f(x_0', x_1')$, then there exists a permutation $\pi \in I_f$ that maps (x_0, x_1) to (x_0', x_1'), and hence their orbits are identical. Furthermore, we can construct a tuple $\mathcal{G} = (G_0, G_1, \psi)$ such that $\Gamma_{\mathcal{G}} = I_f$. Indeed, if f is non-degenerate, then any permutation π_0 appearing in the first component of I_f uniquely determines its counterpart π_1 such that $(\pi_0, \pi_1) \in I_f$. In particular, I_f, $\mathsf{pr}_0(I_f)$, and $\mathsf{pr}_1(I_f)$ are isomorphic to each other, where $\mathsf{pr}_i : \mathcal{S}_{X_0} \times \mathcal{S}_{X_1} \to \mathcal{S}_{X_i}$ is a projection map. We set $G_0 = \mathsf{pr}_0(I_f)$, $G_1 = \mathsf{pr}_1(I_f)$, and $\psi = \mathsf{pr}_1 \circ \mathsf{pr}_0^{-1}$. Note that G_i forms a group as pr_i is a homomorphism. Then, we have $I_f = \Gamma_{\mathcal{G}}$ where $\mathcal{G} = (G_0, G_1, \psi)$. Therefore, we obtain that $f_{\mathcal{G}}(x_0, x_1) = \mathrm{Orb}_{I_f}(x_0, x_1)$ and hence $f_{\mathcal{G}}$ is equivalent to f.

As a demonstration, we consider the sum function $f(x_0, x_1) = x_0 + x_1$ over an abelian group X. For $r \in X$, let $\sigma_r : X \to X$ denote a permutation that shifts each element $x \in X$ by r. It is easy to verify that if $f(x_0', x_1') = f(x_0, x_1)$, then $(x_0', x_1') = (\sigma_r(x_0), \sigma_{-r}(x_1))$ and $(\sigma_r, \sigma_{-r}) \in I_f$, where $r := x_0' - x_0$. Thus, our characterization ensures that f is an ideal PSM function. Note that f is equivalent to $f_{\mathcal{G}} = f_{(G_0, G_1, \psi)}$ where both G_0 and G_1 are the set consisting of all σ_r's, and $\psi : G_0 \to G_1$ is defined as $\psi(\sigma_r) = \sigma_{-r}$. Interestingly, this argument does not require presenting any explicit PSM protocol for f.

2.2 Enumeration of Ideal PSM Functions

The above characterization reduces the enumeration of ideal PSM functions $f : X_0 \times X_1 \to Y$ to the enumeration of all tuples $\mathcal{G}$'s. For ease of exposition, we assume that $|X_0| = |X_1| =: N$. See Section 5 for a general case.

First, we provide asymptotic upper bounds on the total number of such functions. Here, we focus on connected functions, that is, there exists no partition of $X_0 \times X_1$ into rectangles each of which corresponds to disjoint sets of values of f. In the boolean case $Y = \{0, 1\}$, this assumption excludes only a few trivial functions and does not affect the asymptotic results. Thanks to our characterization, we can obtain an upper bound by counting the number of all $\mathcal{G} = (G_0, G_1, \psi)$, where G_i is a subgroup of $\mathcal{S}_{X_i}$ and ψ is an isomorphism between G_0 and G_1. However, since the total number of subgroups of $\mathcal{S}_N$ is $2^{\Theta(N^2)}$ [43], naively enumerating all subgroups cannot provide a non-trivial upper bound beyond the trivial bound of 2^{N^2}, which is the number of all functions with domain $X_0 \times X_1$. To remove duplicate counts of $\mathcal{G}$'s that correspond to equivalent functions, we first observe that if $\mathcal{G}$ and $\mathcal{G}'$ are conjugate, then the corresponding functions $f_{\mathcal{G}}$ and $f_{\mathcal{G}'}$ are equivalent. Hence, it suffices to enumerate only conjugacy classes. As a more effective technique, we consider a minimal subgroup $H_{\mathcal{G}}$ of $\Gamma_{\mathcal{G}}$ that induces the same set of orbits as $\Gamma_{\mathcal{G}}$. Then, $H_{\mathcal{G}}$ uniquely determines $f_{\mathcal{G}}$, that is, $f_{\mathcal{G}}$ and $f_{\mathcal{G}'}$ are equivalent if $H_{\mathcal{G}} = H_{\mathcal{G}'}$. It thus suffices to bound the number of all such

subgroups $H_{\mathcal{G}}$'s. A key observation is that $H_{\mathcal{G}}$ belongs to a special class of permutation groups called *orbit-minimal groups*. It is shown in [43] that any orbit-minimal group over a set X is generated by only $\log|X|$ permutations. As a result, any $H_{\mathcal{G}}$ is generated by at most $\log|X_0 \times X_1| = \log(N^2)$ pairs of permutations in $\mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$. We thus obtain a non-trivial upper bound on the number of ideal PSM functions as

$$\binom{|\mathcal{S}_{X_0}| \cdot |\mathcal{S}_{X_1}|}{\log|X_0 \times X_1|} = (N!)^{O(\log(N^2))} = 2^{O(N \log^2 N)}.$$

Furthermore, we obtain a tighter upper bound in the special case where both $|X_0|$ and $|X_1|$ are primes. We observe that it suffices to enumerate $\mathcal{G} = (G_0, G_1, \psi)$ such that G_0 and G_1 are transitive groups, when connected functions are considered. For a prime N, the total number of transitive subgroups of $\mathcal{S}_N$ is at most $2^{O(\log N)}$ [44]. Moreover, we show that the possible types of transitive groups relevant to our setting are limited, and in particular, their sizes are upper bounded by $2^{O(\log^2 N)}$. Consequently, in this special case, we obtain the following bound:

$$\sum_{G_0, G_1 : \text{transitive}} \binom{|G_0| \cdot |G_1|}{\log|X_0 \times X_1|} = 2^{O(\log N)} |G_0|^{\log(N^2)} |G_1|^{\log(N^2)} = 2^{O(\log^3 N)}.$$

Next, we provide a complete list of ideal PSM functions $f : X_0 \times X_1 \to Y$ for small domains. We use an open software package called GAP to enumerate all the conjugacy classes of $\mathcal{G}$. For a general range Y, we obtain a complete list up to $\max\{|X_0|, |X_1|\} \leq 15$ except for the case of $|X_0| = |X_1| = 12$. In the boolean case $Y = \{0, 1\}$, we devise a more computationally efficient method to enumerate $\mathcal{G}$. As a result, we obtain a list of boolean functions admitting ideal PSM up to $\max\{|X_0|, |X_1|\} \leq 23$. Specifically, if f is an ideal PSM function, i.e., $f = f_{\mathcal{G}}$ for some $\mathcal{G} = (G_0, G_1, \psi)$, then the truth-table T_f, viewed as a $|X_0|$-by-$|X_1|$ matrix, satisfies the following property: If $v \in \{0,1\}^{|X_1|}$ is a column of T_f, then so is a permuted vector $\pi_0(v)$ for any $\pi_0 \in G_0$. Conversely, for any pair of columns v, v' of T_f, there exists a permutation $\pi_0 \in G_0$ such that $v' = \pi_0(v)$. Leveraging this property, we can enumerate ideal PSM functions as follows: For each transitive group G_0, we construct a graph $\mathfrak{G}_{G_0} = (V_{G_0}, E_{G_0})$ where $V_{G_0} = \{0,1\}^n$ and $E_{G_0} = \{(v, v') \in V_{G_0} \times V_{G_0} : \exists \pi_0 \in G_0, v' = \pi_0(v)\}$. From the above property, the truth-table of any $f_{\mathcal{G}}$ with $\mathcal{G} = (G_0, G_1, \psi)$ corresponds to some connected component of $\mathfrak{G}_{G_0}$. We then collect the connected components of $\mathfrak{G}_{G_0}$ for all G_0's, which contain all desired functions.

2.3 Infinite Families of Ideal PSM Functions

We present several infinite families of ideal PSM functions. The simplest family is the *group product*, which computes

$$f((x_i)_{i \in S_0}, (y_i)_{i \in S_1}) = \prod_{i \in S_0 \cup S_1} z_i,$$

where each x_i and y_i are taken from a possibly non-abelian group G and we set $z_i = x_i$ for $i \in S_0$ and $z_i = y_i$ for $i \in S_1$. Feige et al. [29] constructed an ideal PSM scheme for this function by randomizing a sequence of group elements while preserving their product.

Next, we show that a function computing private set intersection cardinality admits ideal PSM. Specifically, for parameters $n, d_0, d_1 \in \mathbb{N}$, we define

$$\mathsf{PSIC}_{n,(d_0,d_1)}(A_0, A_1) = |A_0 \cap A_1|,$$

where A_i is taken from the set of all d_i-sized subsets of a common set U of n elements. To see that $\mathsf{PSIC}_{n,(d_0,d_1)}$ is an ideal PSM function, suppose that $|A_0 \cap A_1| = |A'_0 \cap A'_1|$ and let $B = A_0 \cap A_1$ and $B' = A'_0 \cap A'_1$. Then, we can choose a permutation π on U such that $\pi(A_0) = A'_0$ and $\pi(A_1) = A'_1$, and apply our characterization result. The existence of such π is guaranteed by the fact that both $A_0 \cup A_1$ and $A'_0 \cup A'_1$ admit partitions whose corresponding blocks have the same sizes, that is, $|A_0 \setminus B| = |A'_0 \setminus B'|$, $|A_1 \setminus B| = |A'_1 \setminus B'|$, and $|B| = |B'|$. In particular, $\mathsf{PSIC}_{n,(1,1)}$ is equivalent to the functionality of testing whether two given elements are identical, which implies that the equality function is an ideal PSM function.

Finally, we introduce a class of functions that generalizes the index function [29, 38]. Let H and G be abelian groups and let $\mathcal{F}$ be any set of families $\phi : H \to G$ that are closed under sums (that is, $\phi \pm \phi' \in \mathcal{F}$ for any $\phi, \phi' \in \mathcal{F}$) and are closed under input shifts (that is, $\phi_s \in \mathcal{F}$ for any $\phi \in \mathcal{F}, s \in H$, where $\phi_s(x) := \phi(x - s)$). We set $X_0 = H \times G$ and $X_1 = \mathcal{F}$, and define a function $f : (H \times G) \times \mathcal{F} \to G$ as

$$f((x, r), \phi) = \phi(x) - r.$$

This class of functions includes the original index function considered in [29], an augmented form of the inner product, and multi-linear polynomials as special instances. To show that these functions admit ideal PSM, we define two families of permutations over $X_0 \times X_1$:

- $\pi^s : ((x, r), \phi) \mapsto ((x + s, r), \phi_s)$ for any $s \in H$.
- $\sigma^\tau : ((x, r), \phi) \mapsto ((x, r + \tau(x)), \phi + \tau)$ for any $\tau \in \mathcal{F}$.

Intuitively, the first family of permutations allows us to freely move Alice's input (x, r) to any (x', r) while preserving the outputs of f. The second family allows us to freely move Bob's input ϕ to any ϕ'. Thus, for any pair of inputs $(x_0, x_1), (x'_0, x'_1)$ with $f(x_0, x_1) = f(x'_0, x'_1)$, we can find a permutation that maps (x_0, x_1) to (x'_0, x'_1) preserving the outputs of f and apply our characterization result.

2.4 Communication-efficient and Simplified PSM Schemes

In general, if we obtain a PSM scheme for a function $F : X'_0 \times X'_1 \to Y$, then the scheme naturally induces a PSM scheme for any function $f : X_0 \times X_1 \to Y$ that can be embedded into F, simply by restricting the input domains. Here, by saying that f is *embedded* into F, we mean that there are injections $\tau_i : X_i \to X'_i$ such that $f(x_0, x_1) = F(\tau_0(x_0), \tau_1(x_1))$ for all $(x_0, x_1) \in X_0 \times X_1$. Thus, the ideal PSM schemes described above particularly induce PSM schemes for functions that are embedded into the corresponding functions. We refer to such a construction template of PSM as the "embedding-to-ideal-PSM" construction. Interestingly, most of the existing PSM schemes achieving the state-of-the-art communication complexity in various computation models follow the embedding-to-ideal-PSM template. For example, the best known schemes for branching programs [29] and arithmetic formulas [19, 34] are obtained from the ideal PSM scheme for the group product. The nearly optimal scheme for polynomials [38] is obtained from the ideal PSM scheme for a generalized index function, where $\mathcal{F}$ is the set of all multi-linear polynomials.

By embedding target functions to ideal PSM functions, we obtain novel communication-efficient PSM schemes for functions with sparse/dense or low-rank truth-tables. First, we consider a function $f : X_0 \times X_1 \to \{0, 1\}$ whose truth-table T_f, viewed as a $|X_0|$-by-$|X_1|$ matrix, contains at most d ones in each row for a small $d \ll N_1 := |X_1|$. By appending each row with an appropriate number of ones, we can embed f into a function $f' : X_0 \times X'_1 \to \{0, 1\}$ whose truth-table contains exactly d ones in each row, where $N'_1 := |X'_1| = N_1 + d$. Note that the truth-table of $\mathsf{PSIC}_{N'_1,(d,1)}$ is a $\binom{N'_1}{d}$-by-N'_1 matrix, which

consists of all row vectors of weight d. We can then embed f' (and hence f) into $\mathsf{PSIC}_{N_1',(d,1)}$. The ideal PSM scheme for $\mathsf{PSIC}_{N_1',(d,1)}$ induces a PSM scheme for f with communication complexity $O(\log \binom{N_1'}{d}) = O(d \log(N_1 + d))$. Prior to this work, the only general construction in [7] can apply in this setting which results in communication complexity of $O(\sqrt{N_1})$. Thus, our construction achieves a strict improvement when $d = o(\sqrt{N_1}/\log N_1)$. Note that these schemes also apply to functions such that the rows (or the columns) are dense, that is, they contain at least $n - d$ ones for a small d.

Next, Narayanan et al. [41] showed a PSM scheme for a function $f : X_0 \times X_1 \to Y$ whose communication complexity is $O(k \log |Y|)$, where k is the tiling number of f. Here, the tiling number refers to the smallest number of disjoint monochromatic rectangles covering the truth-table T_f. Let q be the smallest prime power larger than $|Y|$ (we can choose q so that $q = O(|Y|)$). If the rank of the truth-table T_f is at most r over $\mathbb{F}_q$, then we can decompose $T_f = \mathbf{M}_0 \mathbf{M}_1^\top$ where $\mathbf{M}_i \in \mathbb{F}_q^{|X_i| \times r}$. Thus, by defining an injection

$$\tau_i : X_i \ni x_i \mapsto \mathbf{M}_i[x_i] \in \mathbb{F}_q^r,$$

where $\mathbf{M}_i[x]$ denotes the x-th row of $\mathbf{M}_i$, we can embed f into the inner product function over $\mathbb{F}_q^r$. The inner product is a special case of the generalized index function and hence admits ideal PSM. As a result, we obtain a PSM scheme for f with communication complexity $O(r \log |Y|)$. Since it holds that $k \geq r$ for any f, our construction achieves a more refined communication complexity than [41].

Finally, Beimel et al. [7] showed a PSM scheme for a general function $f : X \times X \to \{0,1\}$ with communication complexity $O(\sqrt{N})$, where $X = \{0, 1, \ldots, N-1\}$. According to the description in [3], the more precise communication complexity is at least $12\sqrt{N}$. In contrast, we show that any function f can be embedded into an ideal PSM function $G_f : X' \times X' \to \{0,1\}$ with $\log |X'| = 4\sqrt{N} + 1$. Precisely, we consider a multi-linear function $\hat{f} : (\{0,1\}^{\sqrt{N}})^4 \to \{0,1\}$ such that

$$\hat{f}(\mathbf{e}_{i_0}, \mathbf{e}_{j_0}, \mathbf{e}_{i_1}, \mathbf{e}_{j_1}) = f(i_0\sqrt{N} + j_0, i_1\sqrt{N} + j_1)$$

for any $i_0, j_0, i_1, j_1 \in \{0, 1, \ldots, \sqrt{N}-1\}$, where $\mathbf{e}_i$ denotes a one-hot vector whose i-th element is one. Then, we set $X' = (\{0,1\}^{\sqrt{N}})^4 \times \{0,1\}$ and define a function $G_f : X' \times X' \to \{0,1\}$ as

$$\begin{aligned} & G_f((\mathbf{x}_0, \mathbf{x}_1, \mathbf{i}_0, \mathbf{i}_1, a), (\mathbf{y}_0, \mathbf{y}_1, \mathbf{j}_0, \mathbf{j}_1, b)) \\ = \; & \hat{f}(\mathbf{x}_0, \mathbf{x}_1, \mathbf{y}_0, \mathbf{y}_1) \oplus \langle \mathbf{x}_0, \mathbf{j}_0 \rangle \oplus \langle \mathbf{x}_1, \mathbf{j}_1 \rangle \oplus \langle \mathbf{y}_0, \mathbf{i}_0 \rangle \oplus \langle \mathbf{y}_1, \mathbf{i}_1 \rangle \oplus a \oplus b \end{aligned}$$

for any $\mathbf{x}_0, \mathbf{x}_1, \mathbf{i}_0, \mathbf{i}_1, \mathbf{y}_0, \mathbf{y}_1, \mathbf{j}_0, \mathbf{j}_1 \in \{0,1\}^{\sqrt{N}}$ and $a, b \in \{0,1\}$. To show that G_f admits ideal PSM, we construct the following families of permutations over $X' \times X'$ under which the outputs of G_f are invariant:

- For any $\mathbf{t}_0, \mathbf{t}_1 \in \{0,1\}^{\sqrt{N}}$, $\pi^{\mathbf{t}_0, \mathbf{t}_1}$ freely shifts part of Alice's input $(\mathbf{x}_0, \mathbf{x}_1)$ by $(\mathbf{t}_0, \mathbf{t}_1)$.
- For any $\mathbf{s}_0, \mathbf{s}_1 \in \{0,1\}^{\sqrt{N}}$, $\sigma^{\mathbf{s}_0, \mathbf{s}_1}$ freely shifts part of Bob's input $(\mathbf{y}_0, \mathbf{y}_1)$ by $(\mathbf{s}_0, \mathbf{s}_1)$.
- For any $\mathbf{p}_0, \mathbf{p}_1, \mathbf{q}_0, \mathbf{q}_1 \in \{0,1\}^{\sqrt{N}}$, $\tau^{\mathbf{p}_0, \mathbf{p}_1, \mathbf{q}_0, \mathbf{q}_1}$ freely shifts part of Alice's and Bob's inputs, $(\mathbf{i}_0, \mathbf{i}_1)$ and $(\mathbf{j}_0, \mathbf{j}_1)$, by $(\mathbf{p}_0, \mathbf{p}_1)$ and $(\mathbf{q}_0, \mathbf{q}_1)$, respectively.
- For any $r \in \{0,1\}$, ρ^r maps part of Alice's and Bob's inputs (a, b) to $(a \oplus r, b \oplus r)$.

Thus, we can map an input to any other input by composing permutations from the above families as long as their corresponding outputs of G_f are equal, which shows the existence of ideal PSM for G_f. Since the communication complexity of the resulting ideal PSM scheme is $\log |X' \times X'| = 8\sqrt{N} + 2$, our construction improves the constant factor in the dominant term of the best known communication complexity. An additional benefit is that Alice and Bob can compute their messages simply by applying a composition of the permutations defined

above to their inputs. As a result, the message functions of our scheme can be expressed in closed form and simplifies the hierarchical design of [3, 7], which relies on nested invocations of PSM schemes for smaller functions.

3 Preliminaries

This section summarizes basic notations used in the paper. For $n \in \mathbb{N}$, we define $[n] = \{0, 1, 2, \ldots, n-1\}$. For a set X, let $\binom{X}{k}$ denote the set of all k-sized subsets of X. We write $x \leftarrow\!\$\ X$ if an element x is sampled uniformly at random from a set X. The statistical distance between two random variables X, Y over a set U is defined as $\mathsf{SD}(X, Y) = (1/2)\sum_{a \in U} |\Pr[X = a] - \Pr[Y = a]|$. For two vectors $\mathbf{u}, \mathbf{v}$, we denote their inner product by $\langle \mathbf{u}, \mathbf{v} \rangle$ and their tensor (or Kronecker product) by $\mathbf{u} \otimes \mathbf{v}$. Let $\mathbb{F}_q$ denote a finite field of size q.

3.1 Permutation Groups

If H is a subgroup of a group G, then we write $H \leq G$. We denote the group of all permutations over a finite set X by $\mathcal{S}_X$. If $|X| = N$, then we also denote it by $\mathcal{S}_N$ and call it the permutation group of degree N. We denote the inverse of a permutation π by π^{-1} and the composition of π and π' by $\pi' \circ \pi$. We say that G is generated by a subset $S \subseteq G$ if every element of G can be expressed by a composition of finitely many elements of S or their inverses. Each permutation $\pi \in \mathcal{S}_X$ naturally acts on the set X. If $n = |X|$, then π also acts on the set Y^n of n-dimensional vectors over a set Y: for each $v = (v_x)_{x \in X} \in Y^n$, define $\pi(v) = (v'_x)_{x \in X} \in Y^n$ as $v'_{\pi(x)} = v_x$ for all $x \in X$. For a subset $S \subseteq \mathcal{S}_X$, we define the *orbit* of $x \in X$ under the action of S on X by $\mathrm{Orb}_S(x) = \{\pi(x) : \pi \in S\}$. We say that $G \leq \mathcal{S}_X$ is *transitive* if for any $x, x' \in X$, there exists $\pi \in G$ such that $\pi(x) = x'$, that is, the orbit of any $x \in X$ is equal to X. A (not necessarily transitive) subgroup $G \leq \mathcal{S}_X$ is called *orbit-minimal* if for any proper subgroup $H \lneq G$, it holds that $|\{\mathrm{Orb}_H(x) : x \in X\}| > |\{\mathrm{Orb}_G(x) : x \in X\}|$. Let X_0, X_1 be sets. We naturally identify $\mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$ as a subgroup of $\mathcal{S}_{X_0 \times X_1}$ via $\tau(x_0, x_1) = (\tau_0(x_0), \tau_1(x_1))$ where $\tau = (\tau_0, \tau_1) \in \mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$ and $(x_0, x_1) \in X_0 \times X_1$. We denote a natural projection from $\mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$ onto $\mathcal{S}_{X_i}$ by pr_i. For $S \subseteq \mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$, we similarly define the orbit of (x_0, x_1) under the action of S on $X_0 \times X_1$, denoted by $\mathrm{Orb}_S(x_0, x_1)$.

3.2 Functions

Let $f : X_0 \times X_1 \to Y$ be a function. For subsets $A_0 \subseteq X_0$ and $A_1 \subseteq X_1$, we denote $f(A_0 \times A_1) = \{f(x_0, x_1) : (x_0, x_1) \in A_0 \times A_1\}$ and denote $\mathrm{Range}(f) = f(X_0 \times X_1)$. We also denote $f^{-1}(y) = \{(x_0, x_1) \in X_0 \times X_1 : f(x_0, x_1) = y\}$ for $y \in \mathrm{Range}(f)$. We define an equivalence relation $\simeq$ on the set of all functions whose domain is $X_0 \times X_1$ as follows:

$$f \simeq g \iff^{\mathrm{def}} \forall (x_0, x_1) \in X_0 \times X_1,\ \sigma(f(\tau_0(x_0), \tau_1(x_1))) = g(x_0, x_1)$$

for some pair of permutations $(\tau_0, \tau_1) \in \mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$ and some bijection $\sigma : \mathrm{Range}(f) \to \mathrm{Range}(g)$. The truth-table of $f : X_0 \times X_1 \to Y$ is defined as a matrix T_f whose rows and columns are indexed by X_0 and X_1 and whose (x_0, x_1)-th entry $T_f[x_0, x_1]$ is $f(x_0, x_1)$ for any $(x_0, x_1) \in X_0 \times X_1$. For each $x_0 \in X_0$, we denote the row vector of T_f corresponding to x_0 by $T_f[x_0, *] \in Y^{|X_1|}$. Similarly, we denote the column vector of T_f corresponding to $x_1 \in X_1$ by $T_f[*, x_1] \in Y^{|X_0|}$. We say that a function $f : X_0 \times X_1 \to Y$ is *degenerate* if there exist $i \in \{0, 1\}$ and $x_i \neq x'_i \in X_i$ such that $f(x_i, x_{1-i}) = f(x'_i, x_{1-i})$ for all $x_{1-i} \in X_{1-i}$, where the inputs are supposed to be sorted according to the index. We say that f is *non-degenerate* if f

is not degenerate. We say that $f : X_0 \times X_1 \to Y$ is *disconnected* if there exist $i \in \{0,1\}$ and a partition $X_i = A_i \cup B_i$ such that $f(A_i \times X_{1-i}) \cap f(B_i \times X_{1-i}) = \emptyset$. We say that f is *connected* if f is not disconnected. Note that if $Y = \{0,1\}$, then non-degenerate disconnected functions are limited to those whose truth tables are (1 0) or its transpose, or functions that are equivalent to them. For $\pi = (\pi_0, \pi_1) \in \mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$ and $x = (x_0, x_1) \in X_0 \times X_1$, we simply write $\pi(x) = (\pi_0(x_0), \pi_1(x_1))$ and $f(\pi(x)) = f(\pi_0(x_0), \pi_1(x_1))$. We define the *invariant group* of f, denoted by I_f, as the subgroup consisting of all pairs of permutations in $\mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$ under which the outputs of f are invariant, i.e., $I_f = \{\pi \in \mathcal{S}_{X_0} \times \mathcal{S}_{X_1} : f(\pi(x)) = f(x), \forall x \in X_0 \times X_1\}$.

3.3 Private Simultaneous Messages

We introduce Private Simultaneous Messages (PSM) schemes. Each of two parties holds an input x_i and they both share a common string r sampled by a randomized algorithm Gen. Then, each party runs an algorithm Msg to compute a message m_i. They send the messages to an external party, who then runs an algorithm Eval to obtain $f(x_0, x_1)$. The privacy requirement is that the joint distribution of messages leaks no extra information. We provide the formal definition below.

▶ **Definition 1.** *Let $f : X_0 \times X_1 \to Y$ be a function. A* Private Simultaneous Messages (PSM) *scheme Π for f is a tuple $(\mathsf{Gen}, \mathsf{Msg}, \mathsf{Eval})$ of three algorithms, where*

- $\mathsf{Gen}() \to r$*:* Gen *is a randomized algorithm that takes no input and outputs $r \in R$ sampled from a probability distribution over a set R.*
- $\mathsf{Msg}(i, x_i, r)$*:* Msg *is a deterministic algorithm that takes $i \in \{0,1\}$, $x_i \in X_i$, and $r \in R$ as input and outputs a message m_i.*
- $\mathsf{Eval}(m_0, m_1)$*:* Eval *is a deterministic algorithm that takes messages (m_0, m_1) as input and outputs $y \in Y$.*

satisfying the following properties:

Correctness. *For any $(x_0, x_1) \in X_0 \times X_1$ and $r \in R$, it holds that $\mathsf{Eval}(\mathsf{Msg}(0, x_0, r), \mathsf{Msg}(1, x_1, r)) = f(x_0, x_1)$.*

Privacy. *For any input $(x_0, x_1) \in X_0 \times X_1$, let $\mathcal{D}_{(x_0,x_1)}$ denote the probability distribution of $(\mathsf{Msg}(i, x_i, r))_{i\in\{0,1\}}$ induced by $r \leftarrow \mathsf{Gen}()$. For any pair of inputs $(x_0, x_1), (x'_0, x'_1) \in X_0 \times X_1$ with $f(x_0, x_1) = f(x'_0, x'_1)$, it holds that $\mathsf{SD}\left(\mathcal{D}_{(x_0,x_1)}, \mathcal{D}_{(x'_0,x'_1)}\right) = 0$.*

We call the set of all possible outcomes of Gen (i.e., R) the randomness space of Π. We call the set of all possible outcomes of $\mathsf{Msg}(i, \cdot, \cdot)$ the i-th message space and denote it by M_i. The communication complexity of Π is defined as $\log |M_0| + \log |M_1|$.

If a PSM scheme for a function f is given, then it immediately implies a PSM scheme with the same communication complexity for any function f' that is equivalent to f. Therefore, throughout this paper, we do not distinguish between equivalent functions and rather focus on equivalence classes of functions.

Furthermore, we focus on PSM schemes for non-degenerate functions. Suppose that $f : X_0 \times X_1 \to Y$ is degenerate, and that there exist $x_0, x'_0 \in X_0$ such that $f(x_0, x_1) = f(x'_0, x_1)$ for any $x_1 \in X_1$. Then, any PSM scheme Π' for the restriction f' of f to $X_0 \setminus \{x'_0\} \times X_1$ can be extended to a PSM scheme Π for f simply by letting party 0 "reuse" his message for x_0 when his input is x'_0. The communication complexity of Π is the same as that of Π'.

4 Ideal PSM

In this section, we introduce the notion of ideal PSM schemes, in which messages are taken from the same domain as inputs. Ideal PSM schemes are necessarily communication-optimal as communication complexity must be at least the input length of a function. We begin by presenting the formal definition.

▶ **Definition 2.** *We say that a PSM scheme* Π *for a function* $f : X_0 \times X_1 \to Y$ *is* ideal *if the message spaces satisfy*

$$M_0 = X_0 \text{ and } M_1 = X_1.$$

We say that a function f admits ideal PSM *or is an* ideal PSM function *if there exists an ideal PSM scheme for* f*.*

Suppose that Π is an ideal PSM scheme for a non-degenerate function f. Then, the communication complexity of Π cannot be reduced further. This is because otherwise, for some randomness r and some pair of inputs, say x_0, x_0', the corresponding messages coincide. Then, the perfect correctness of Π implies that $f(x_0, x_1) = f(x_0', x_1)$ for any x_1, which contradicts that f is non-degenerate.

4.1 Canonical Ideal PSM Schemes

We introduce a special class of ideal PSM schemes induced by permutation groups. Jumping ahead, we will show that the set of ideal PSM functions is essentially limited to those realized by this special type of ideal PSM schemes. In that sense, we refer to these ideal schemes as "canonical".

For sets X_0, X_1, we define

$$\Psi_{X_0,X_1} = \{(G_0, G_1, \psi) : G_0 \leq \mathcal{S}_{X_0}, G_1 \leq \mathcal{S}_{X_1},\ \psi : G_0 \to G_1 \text{ is an isomorphism}\}.$$

For each $\mathcal{G} = (G_0, G_1, \psi) \in \Psi_{X_0,X_1}$, we define a subgroup $\Gamma_{\mathcal{G}}$ of $\mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$ as

$$\Gamma_{\mathcal{G}} = \{(\pi_0, \pi_1) : \pi_0 \in G_0, \pi_1 = \psi(\pi_0)\}.$$

and $Y_{\mathcal{G}} = \{\mathrm{Orb}_{\Gamma_{\mathcal{G}}}(x_0, x_1) : (x_0, x_1) \in X_0 \times X_1\}$. Finally, we define a function $f_{\mathcal{G}} : X_0 \times X_1 \to Y_{\mathcal{G}}$ by

$$f_{\mathcal{G}}(x_0, x_1) = \mathrm{Orb}_{\Gamma_{\mathcal{G}}}(x_0, x_1)$$

for all $(x_0, x_1) \in X_0 \times X_1$.

We can see that each function $f_{\mathcal{G}}$ admits ideal PSM.

▶ **Proposition 3.** *For each* $\mathcal{G} = (G_0, G_1, \psi) \in \Psi_{X_0,X_1}$*, there exists an ideal PSM scheme* $\Pi_{\mathcal{G}}$ *for the function* $f_{\mathcal{G}}$*.*

Proof. We construct $\Pi_{\mathcal{G}}$ as follows. The randomness generation algorithm Gen outputs $\pi = (\pi_0, \pi_1)$ chosen uniformly at random from $\Gamma_{\mathcal{G}}$. The message function Msg is defined as $\mathsf{Msg}(i, x_i, \pi) = \pi_i(x_i)$. The evaluation function Eval is defined as $\mathsf{Eval}(m_0, m_1) = \mathrm{Orb}_{\Gamma_{\mathcal{G}}}(m_0, m_1)$. By definition, $\Pi_{\mathcal{G}}$ is ideal.

We have that

$$\mathsf{Eval}(\mathsf{Msg}(0, x_0, \pi), \mathsf{Msg}(1, x_1, \pi)) = \mathrm{Orb}_{\Gamma_{\mathcal{G}}}(\pi_0(x_0), \pi_1(x_1)) = \mathrm{Orb}_{\Gamma_{\mathcal{G}}}(x_0, x_1) = f_{\mathcal{G}}(x_0, x_1).$$

The second equality follows from $\pi = (\pi_0, \pi_1) \in \Gamma_{\mathcal{G}}$. Thus, the correctness of $\Pi_{\mathcal{G}}$ follows.

Let $(x_0, x_1), (x'_0, x'_1)$ be two inputs such that $f_{\mathcal{G}}(x_0, x_1) = f_{\mathcal{G}}(x'_0, x'_1)$. Then, $\mathrm{Orb}_{\Gamma_{\mathcal{G}}}(x_0, x_1) = \mathrm{Orb}_{\Gamma_{\mathcal{G}}}(x'_0, x'_1)$. It follows from the orbit-stabilizer theorem that the distribution of

$$(\mathsf{Msg}(0, x_0, \pi), \mathsf{Msg}(1, x_1, \pi)) = (\pi_0(x_0), \pi_1(x_1))$$

induced by $\pi \leftarrow\!\!\$\ \Gamma_{\mathcal{G}}$ is a uniform distribution over the orbit $\mathrm{Orb}_{\Gamma_{\mathcal{G}}}(x_0, x_1)$. Similarly, the distribution of $(\mathsf{Msg}(0, x'_0, \pi'), \mathsf{Msg}(1, x'_1, \pi'))$ induced by $\pi' \leftarrow\!\!\$\ \Gamma_{\mathcal{G}}$ is a uniform distribution over $\mathrm{Orb}_{\Gamma_{\mathcal{G}}}(x'_0, x'_1)$. Therefore, the distribution of $(\mathsf{Msg}(i, x_i, \pi))_{i\in\{0,1\}}$ is identical with that of $(\mathsf{Msg}(i, x'_i, \pi'))_{i\in\{0,1\}}$, from which the privacy of $\Pi_{\mathcal{G}}$ follows. ◀

4.2 Characterization

We show that the class of ideal PSM functions is essentially equal to those computed by the canonical ideal PSM schemes, namely the $f_{\mathcal{G}}$'s.

First, we prepare two lemmas, whose proofs are provided in the full version.

▶ **Lemma 4.** *Let $\Pi = (\mathsf{Gen}, \mathsf{Msg}, \mathsf{Eval})$ be a PSM scheme for a non-degenerate function $f : X_0 \times X_1 \to Y$ with randomness space R. Then, for any $r \in R$ and $i \in \{0, 1\}$, the function $\mathsf{Msg}(i, \cdot, r) \colon X_i \to M_i$ is injective. In particular, if Π is ideal, then $\mathsf{Msg}(i, \cdot, r) \colon X_i \to X_i$ is a bijection.*

▶ **Lemma 5.** *Assume that a non-degenerate function $f : X_0 \times X_1 \to Y$ admits ideal PSM. Then, there exists an ideal PSM scheme $\Pi' = (\mathsf{Gen}', \mathsf{Msg}', \mathsf{Eval}')$ for f such that $\mathsf{Eval}' = f$.*

Now, we show a characterization of ideal PSM functions.

▶ **Theorem 6.** *Let $f : X_0 \times X_1 \to Y$ be a non-degenerate function. Then, the following conditions are equivalent:*

1. *f admits ideal PSM.*
2. *There exists $\mathcal{G} \in \Psi_{X_0, X_1}$ such that $f \simeq f_{\mathcal{G}}$.*
3. *It holds that $\mathrm{Orb}_{I_f}(x_0, x_1) = f^{-1}(f(x_0, x_1))$ for any $(x_0, x_1) \in X_0 \times X_1$.*
4. *There exists a subset $S \subseteq I_f$ such that $\mathrm{Orb}_S(x_0, x_1) = f^{-1}(f(x_0, x_1))$ for any $(x_0, x_1) \in X_0 \times X_1$.*

Proof.

2 ⇒ 1. Let $\Pi_{\mathcal{G}} = (\mathsf{Gen}_{\mathcal{G}}, \mathsf{Msg}_{\mathcal{G}}, \mathsf{Eval}_{\mathcal{G}})$ be the ideal PSM scheme for $f_{\mathcal{G}}$ constructed in Proposition 3. Since $f \simeq f_{\mathcal{G}}$, there are a pair of permutations $\tau = (\tau_0, \tau_1) \in \mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$ and a bijection $\sigma : Y \to Y_{\mathcal{G}}$ such that $\sigma(f(\tau(x))) = f_{\mathcal{G}}(x)$ for all $x = (x_0, x_1) \in X_0 \times X_1$.

It suffices to construct an ideal PSM scheme $\Pi = (\mathsf{Gen}, \mathsf{Msg}, \mathsf{Eval})$ for f. We define Π as follows:

- $\mathsf{Gen} = \mathsf{Gen}_{\mathcal{G}}$, that is, Gen outputs $\pi = (\pi_0, \pi_1) \leftarrow\!\!\$\ \Gamma_{\mathcal{G}}$.
- $\mathsf{Msg}(i, x_i, \pi) = \mathsf{Msg}_{\mathcal{G}}(i, \tau_i^{-1}(x_i), \pi) = \pi_i(\tau_i^{-1}(x_i))$.
- $\mathsf{Eval}(m_0, m_1) = \sigma^{-1}(\mathsf{Eval}_{\mathcal{G}}(m_0, m_1))$.

The correctness follows since

$$\begin{aligned}\mathsf{Eval}(\mathsf{Msg}(0, x_0, \pi), \mathsf{Msg}(1, x_1, \pi)) &= \sigma^{-1}(\mathsf{Eval}_{\mathcal{G}}(\mathsf{Msg}_{\mathcal{G}}(0, \tau_0^{-1}(x_0), \pi), \mathsf{Msg}_{\mathcal{G}}(1, \tau_1^{-1}(x_1), \pi))\\ &= \sigma^{-1}(f_{\mathcal{G}}(\tau_0^{-1}(x_0), \tau_1^{-1}(x_1)))\\ &= f(x_0, x_1).\end{aligned}$$

The privacy of Π is implied by that of $\Pi_{\mathcal{G}}$ since $f(x_0, x_1) = f(x'_0, x'_1)$ if and only if $f_{\mathcal{G}}(\tau_0^{-1}(x_0), \tau_1^{-1}(x_1)) = f_{\mathcal{G}}(\tau_0^{-1}(x'_0), \tau_1^{-1}(x'_1))$. Clearly, Π is ideal.

1 ⇒ 4. Let Π be an ideal PSM scheme for f obtained via Lemma 5. Let R be the randomness space of Π. For each $r \in R$ and $i \in \{0,1\}$, we define $\pi_r^i : X_i \to X_i$ as $\pi_r^i(x_i) = \mathsf{Msg}(i, x_i, r)$. From Lemma 4, π_r^i is a permutation on X_i. Let S be a subgroup of $\mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$ generated by $\{(\pi_r^0, \pi_r^1) : r \in R\}$.

First, we prove that $S \subseteq I_f$. Let $(x_0, x_1) \in X_0 \times X_1$ and $(\pi_0, \pi_1) \in S$. Since S is generated by $\{(\pi_r^0, \pi_r^1) : r \in R\}$, there exists a sequence $(r_1, \ldots, r_m)$ such that

$$(\pi_0, \pi_1) = (\pi_{r_1}^0, \pi_{r_1}^1) \circ \cdots \circ (\pi_{r_m}^0, \pi_{r_m}^1). \tag{1}$$

Note that since S is a finite group, for any $(\pi_0, \pi_1) \in S$, there exists $k > 0$ such that $(\pi_0, \pi_1)^{-1} = (\pi_0, \pi_1)^k$. Hence, any $(\pi_0, \pi_1) \in S$ can be represented as in Eq. (1). Then, from the correctness of Π, we have $f(x_0, x_1) = f(\pi_{r_m}^0(x_0), \pi_{r_m}^1(x_1)) = f(\pi_{r_{m-1}}^0 \circ \pi_{r_m}^0(x_0), \pi_{r_{m-1}}^1 \circ \pi_{r_m}^1(x_1)) = \cdots = f(\pi_0(x_0), \pi_1(x_1))$ for all $(x_0, x_1) \in X_0 \times X_1$.

Next, we prove that $\mathrm{Orb}_S(x_0, x_1) = f^{-1}(f(x_0, x_1))$ for any $(x_0, x_1) \in X_0 \times X_1$. Since we have shown $S \subseteq I_f$, it holds that $\mathrm{Orb}_S(x_0, x_1) \subseteq f^{-1}(f(x_0, x_1))$. It remains to show that for any $(x_0', x_1') \in f^{-1}(f(x_0, x_1))$, there exists $(\pi_0, \pi_1) \in S$ such that $\pi_0(x_0) = x_0'$ and $\pi_1(x_1) = x_1'$. From the privacy requirement of Π, the distribution of $(\pi_r^0(x_0), \pi_r^1(x_1))$ induced by $r \leftarrow\!\$\, R$ is identical with that of $(\pi_{r'}^0(x_0'), \pi_{r'}^1(x_1'))$ induced by $r' \leftarrow\!\$\, R$, since $f(x_0, x_1) = f(x_0', x_1')$. This particularly implies that there exist $r, r' \in R$ such that $(\pi_r^0(x_0), \pi_r^1(x_1)) = (\pi_{r'}^0(x_0'), \pi_{r'}^1(x_1'))$. By the definition of S, $(\pi_0, \pi_1) := (\pi_{r'}^0, \pi_{r'}^1)^{-1} \circ (\pi_r^0, \pi_r^1)$ belongs to S and $(\pi_0(x_0), \pi_1(x_1)) = (x_0', x_1')$.

4 ⇒ 3. Let $(x_0, x_1) \in X_0 \times X_1$. By the definition of I_f, it holds that $\mathrm{Orb}_{I_f}(x_0, x_1) \subseteq f^{-1}(f(x_0, x_1))$. The converse inclusion follows from $f^{-1}(f(x_0, x_1)) = \mathrm{Orb}_S(x_0, x_1) \subseteq \mathrm{Orb}_{I_f}(x_0, x_1)$ as $S \subseteq I_f$.

3 ⇒ 2. Define $G_i = \mathsf{pr}_i(I_f)$ for $i \in \{0,1\}$. First, we prove that the restriction of the projection pr_i to I_f is an isomorphism, i.e., G_i and I_f are isomorphic. Since pr_i is surjective, it is enough to show that it is injective. Suppose on the contrary that there exist $\pi_0 \in G_0$ and $\pi_1 \neq \pi_1' \in G_1$ such that $(\pi_0, \pi_1) \in I_f$ and $(\pi_0, \pi_1') \in I_f$. Then, there exists $x_1 \in X_1$ such that $\pi_1(x_1) \neq \pi_1'(x_1)$. For any $x_0 \in X_0$, we have $f(\pi_0(x_0), \pi_1(x_1)) = f(x_0, x_1) = f(\pi_0(x_0), \pi_1'(x_1))$. Since π_0 is a bijection, this implies that for any $x_0 \in X_0$, we have $f(x_0, \pi_1(x_1)) = f(x_0, \pi_1'(x_1))$. This contradicts that f is non-degenerate. Thus, the projection $\mathsf{pr}_i : I_f \to G_i$ is an injection and hence is an isomorphism. In summary, G_0, G_1 and I_f are isomorphic to each other. Let ψ be an isomorphism from G_0 to G_1.

We set $\mathcal{G} = (G_0, G_1, \psi) \in \Psi_{X_0, X_1}$. Note that $\Gamma_{\mathcal{G}} = I_f$ and $Y_{\mathcal{G}} = \{\mathrm{Orb}_{I_f}(x_0, x_1) : (x_0, x_1) \in X_0 \times X_1\}$. We show that $f \simeq f_{\mathcal{G}}$. Define $\sigma : Y \to Y_{\mathcal{G}}$ as follows: For any $y \in Y$, pick any $(x_0, x_1) \in f^{-1}(y)$ and set $\sigma(y) = \mathrm{Orb}_{I_f}(x_0, x_1)$. We see that σ is well-defined. Indeed, the condition 3 ensures that for any $(x_0', x_1') \in f^{-1}(y)$, it holds that $\mathrm{Orb}_{I_f}(x_0', x_1') = f^{-1}(f(y)) = \mathrm{Orb}_{I_f}(x_0, x_1)$. We also see that σ is a bijection. We define $\sigma' : Y_{\mathcal{G}} \to Y$ as $\sigma'(\mathrm{Orb}_{I_f}(x_0, x_1)) = f(x_0, x_1)$ for any $\mathrm{Orb}_{I_f}(x_0, x_1) \in Y_{\mathcal{G}}$. We see that σ' is well-defined. Indeed, if $\mathrm{Orb}_{I_f}(x_0, x_1) = \mathrm{Orb}_{I_f}(x_0', x_1')$, then there is $\pi \in I_f$ such that $\pi(x_0, x_1) = (x_0', x_1')$, which implies that $f(x_0', x_1') = f(\pi(x_0, x_1)) = f(x_0, x_1)$. Since σ' is clearly the inverse of σ, σ is a bijection. Furthermore, $\sigma(f(x_0, x_1)) = \mathrm{Orb}_{I_f}(x_0, x_1) = \mathrm{Orb}_{\Gamma_{\mathcal{G}}}(x_0, x_1) = f_{\mathcal{G}}(x_0, x_1)$ for any $(x_0, x_1) \in X_0 \times X_1$. ◀

We note that the tuple $\mathcal{G} = (G_0, G_1, \psi)$ such that $f \simeq f_{\mathcal{G}}$ may not be uniquely determined by a function f. In other words, there may exist distinct $\mathcal{G} \neq \mathcal{G}' \in \Psi_{X_0, X_1}$ such that $f_{\mathcal{G}} \simeq f_{\mathcal{G}'}$.

5 Enumeration of Ideal PSM Functions

In this section, we give asymptotic upper bounds on the total number of non-degenerate connected functions $f : X_0 \times X_1 \to Y$ that admit ideal PSM. In addition, we provide a complete list of such functions for small domains by a brute-force search. Our approach for enumeration is based on Theorem 6, which ensures that it is sufficient to enumerate all possible tuples $(G_0, G_1, \psi) \in \Psi_{X_0,X_1}$ where $G_0 \leq \mathcal{S}_{X_0}$, $G_1 \leq \mathcal{S}_{X_1}$, and ψ is an isomorphism from G_0 to G_1.

5.1 Asymptotic Upper Bounds

We define C_{N_0,N_1} as the total number of non-degenerate connected functions f, up to the equivalence relation $\simeq$ (defined in Section 3.2), such that

- The domain of f is $X_0 \times X_1$ with $|X_0| = N_0$ and $|X_1| = N_1$.
- f admits ideal PSM.

From Theorem 6, a non-degenerate ideal PSM function f is equivalent to $f_{\mathcal{G}}$ for some $\mathcal{G} \in \Psi_{X_0,X_1}$. Thus, we can upper bound C_{N_0,N_1} by enumerating all $f_{\mathcal{G}}$'s up to equivalence.

Furthermore, it suffices to enumerate all orbit-minimal subgroups H of $\mathcal{S}_{X_0\times X_1}$ such that $H \leq \mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$. Indeed, given $f_{\mathcal{G}}$, let $H_{\mathcal{G}}$ be a minimal one among subgroups of $\Gamma_{\mathcal{G}}$ such that $\{\mathrm{Orb}_{H_{\mathcal{G}}}(x_0, x_1) : (x_0, x_1) \in X_0 \times X_1\} = \{\mathrm{Orb}_{\Gamma_{\mathcal{G}}}(x_0, x_1) : (x_0, x_1) \in X_0 \times X_1\}$. Then, $H_{\mathcal{G}}$ is an orbit-minimal subgroup of $\mathcal{S}_{X_0\times X_1}$ since otherwise, there is a proper subgroup $H' \lneq H_{\mathcal{G}}$ such that $|\{\mathrm{Orb}_{H'}(x_0, x_1) : (x_0, x_1) \in X_0 \times X_1\}| = |\{\mathrm{Orb}_{H_{\mathcal{G}}}(x_0, x_1) : (x_0, x_1) \in X_0 \times X_1\}| = |\{\mathrm{Orb}_{\Gamma_{\mathcal{G}}}(x_0, x_1) : (x_0, x_1) \in X_0 \times X_1\}|$, which contradicts the choice of $H_{\mathcal{G}}$. Furthermore, if $f_{\mathcal{G}}$ and $f_{\mathcal{G}'}$ lead to the same subgroup $H = H_{\mathcal{G}} = H_{\mathcal{G}'}$, then it holds that $\{\mathrm{Orb}_{\Gamma_{\mathcal{G}}}(x_0, x_1) : (x_0, x_1) \in X_0 \times X_1\} = \{\mathrm{Orb}_{H}(x_0, x_1) : (x_0, x_1) \in X_0 \times X_1\} = \{\mathrm{Orb}_{\Gamma_{\mathcal{G}'}}(x_0, x_1) : (x_0, x_1) \in X_0 \times X_1\}$ and hence $f_{\mathcal{G}} \simeq f_{\mathcal{G}'}$. Therefore, the total number of non-equivalent $f_{\mathcal{G}}$'s and hence C_{N_0,N_1} are upper bounded by the total number of orbit-minimal subgroups H of $\mathcal{S}_{X_0\times X_1}$ such that $H \leq \mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$. According to [43, Theorem 1.5], any orbit-minimal subgroup H with $H \leq \mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$ is generated by a set S of at most $\log(N_0N_1)$ elements. Furthermore, since each element of S is expressed as (π_0, π_1) for some $\pi_0 \in \mathcal{S}_{X_0}$ and $\pi_1 \in \mathcal{S}_{X_1}$, the total number of such H's is upper bounded by $\binom{|\mathcal{S}_{X_0}|\cdot|\mathcal{S}_{X_1}|}{\log(N_0N_1)}$.

▶ **Theorem 7.** *The total number of non-degenerate ideal PSM functions $f : X_0 \times X_1 \to Y$ with $|X_0| = N_0$ and $|X_1| = N_1$, up to equivalence, is at most*

$$\binom{N_0! \cdot N_1!}{\log(N_0N_1)} = 2^{O((N_0 \log N_0 + N_1 \log N_1) \log N_0N_1)}$$

If the message spaces of both parties are of prime size, i.e., N_0 and N_1 are primes, then we can obtain a better upper bound for C_{N_0,N_1}. See the full version for details.

▶ **Theorem 8.** *Let N_0 and N_1 be primes and $f : X_0 \times X_1 \to Y$ be a non-degenerate, connected, ideal PSM function with $|X_0| = N_0$ and $|X_1| = N_1$. Then, $N_0 = N_1$. Furthermore, the total number C_{N_0,N_1} of such functions is at most $2^{O(\log^3 p)}$, where $p := N_0 = N_1$.*

5.2 Complete Lists of Small Ideal PSM Functions

Finally, we provide a complete list of non-degenerate connected functions $f : X_0 \times X_1 \to Y$ that admit ideal PSM when $|X_0|$ and $|X_1|$ are small. Since we are interested in equivalence classes of ideal PSM functions, it is sufficient to enumerate $G_0 \leq \mathcal{S}_{X_0}$ and $G_1 \leq \mathcal{S}_{X_1}$ up to conjugacy, and isomorphism $\psi\colon G_0 \to G_1$. Furthermore, we observe that if connected

functions are considered, it suffices to enumerate such (G_0, G_1, ψ) assuming that G_0 and G_1 are transitive. For small domains, we do this by a brute-force search using an open software package called GAP. GAP has a list of all transitive permutation groups (up to conjugacy) of degree at most 30. GAP has a function that takes G_0 and G_1 as input and computes an isomorphism from G_0 to G_1 (if exists). GAP also has a function that takes G_0 as input and computes all automorphism of G_0. Using these functions, we can enumerate Ψ_{X_0,X_1} with $\max\{|X_0|, |X_1|\} \leq 15$ except for the case of $|X_0| = |X_1| = 12$. We were unable to deal with larger cases or $|X_0| = |X_1| = 12$ due to limited computational resources. There are possibilities that $f_{\mathcal{G}}$ is degenerate for some $\mathcal{G} \in \Psi_{X_0,X_1}$ or that $f_{\mathcal{G}} \simeq f_{\mathcal{G}'}$ for some $\mathcal{G} \neq \mathcal{G}' \in \Psi_{X_0,X_1}$. We manually eliminate such degenerate functions and duplicates. The resulting list and our source codes are available in [1] and the exact values of C_{N_0,N_1} are provided in the full version. It can be observed that the exact values of C_{N_0,N_1} seem to be much smaller than our asymptotic upper bounds. We leave the question of the tightness of our upper bounds on C_{N_0,N_1} to future work. In the full version, we also show a more efficient method to enumerate *boolean* functions $f : X_0 \times X_1 \to \{0,1\}$ that admit ideal PSM. This allows us to enumerate such functions with $\max\{|X_0|, |X_1|\} \leq 23$.

6 Infinite Families of Ideal PSM Functions

6.1 Group Product

The sum function $f : G \times G \to G$ over an abelian group G, defined as $f(x, y) = x + y$, admits ideal PSM: one party with input x computes a message $x + r$ and the other party with input y computes a message $y - r$.

More generally, let G be a possibly non-abelian group. Let $m \in \mathbb{N}$, (S_0, S_1) be a partition of $[m]$, and $s_i = |S_i|$ for $i \in \{0, 1\}$. We define a function $f : G^{s_0} \times G^{s_1} \to G$ as

$$f((x_i)_{i\in S_0}, (y_i)_{i\in S_1}) = \prod_{i\in[m]} z_i,$$

where we set $z_i = x_i$ for $i \in S_0$ and $z_i = y_i$ for $i \in S_1$. The PSM scheme for f presented in [29] is ideal and hence f is an ideal PSM function.

6.2 Private Set Intersection Cardinality

Let U be a set of size n and $d_0, d_1 \in \mathbb{N}$ be such that $d_0 \leq n$ and $d_1 \leq n$. Set $d = \min\{d_0, d_1\}$. Define a function $\mathsf{PSIC}_{n,(d_0,d_1)} : \binom{U}{d_0} \times \binom{U}{d_1} \to \{0, 1, \ldots, d\}$ as

$$\mathsf{PSIC}_{n,(d_0,d_1)}(A_0, A_1) = |A_0 \cap A_1|$$

for all $(A_0, A_1) \in \binom{U}{d_0} \times \binom{U}{d_1}$. We show that $\mathsf{PSIC}_{n,(d_0,d_1)}$ admits ideal PSM based on Theorem 6. Let $(A_0, A_1), (A'_0, A'_1) \in \binom{U}{d_0} \times \binom{U}{d_1}$ be two inputs such that $|A_0 \cap A_1| = |A'_0 \cap A'_1|$. Observe that both $A_0 \cup A_1$ and $A'_0 \cup A'_1$ admit partitions whose corresponding blocks have the same sizes, that is, $A_0 \cup A_1 = (A_0 \setminus A_1) \cup (A_0 \cap A_1) \cup (A_1 \setminus A_0)$ and $A'_0 \cup A'_1 = (A'_0 \setminus A'_1) \cup (A'_0 \cap A'_1) \cup (A'_1 \setminus A'_0)$. Thus, there exists a permutation σ over U such that $\sigma(A_0) = A'_0$ and $\sigma(A_1) = A'_1$. Furthermore, since σ is a permutation, $|\sigma(X) \cap \sigma(Y)| = |\sigma(X \cap Y)| = |X \cap Y|$ for any $(X, Y) \in \binom{U}{d_0} \times \binom{U}{d_1}$. Thus, the fourth condition in Theorem 6 is satisfied.

6.3 Index Function

We show that an index function, which takes a vector $D = (D_j)_{j\in[N]} \in \{0,1\}^N$ and an index $x \in [N]$ as input and outputs D_x, admits ideal PSM. The index function was implicitly used to prove the feasibility of PSM for general functions f in [29] by setting D as the truth-table of $f(x_0, \cdot)$ and $x = x_1$. It has played an important role to improve the worst-case communication complexity of PSM [3, 7, 9, 38].

We prove that a more general form of the index functions admit ideal PSM. Let H and G be abelian groups. Let $\mathcal{F}$ be a set of functions from H to G satisfying the following properties:

- For any $\phi, \phi' \in \mathcal{F}$, the function $\phi + \phi'$ (resp. $\phi - \phi'$), defined as $(\phi + \phi')(t) = \phi(t) + \phi'(t)$ (resp. $(\phi - \phi')(t) = \phi(t) - \phi'(t)$) for any $t \in H$, is also in $\mathcal{F}$.
- For any $\phi \in \mathcal{F}$ and $s \in H$, the function ϕ_s, defined as $\phi_s(t) = \phi(t - s)$ for any $t \in H$, is also in $\mathcal{F}$.

Set $X_0 = H \times G$ and $X_1 = \mathcal{F}$. Define $f : X_0 \times X_1 \to G$ as

$$f((x, r), \phi) = \phi(x) - r \tag{2}$$

for any $x \in H$, $r \in G$, and $\phi : H \to G \in \mathcal{F}$. The original index function can be viewed as a special instance by setting $G = \{0,1\}$, $H = \mathbb{Z}_N$, and $\mathcal{F}$ as the set of all functions from $[N]$ to $\{0,1\}$. We show that f admits ideal PSM if it is non-degenerate. For $s \in H$, we define $(\pi_0^s, \pi_1^s) \in \mathcal{S}_{X_0} \times \mathcal{S}_{X_1}$ as $\pi_0^s(x, r) = (x + s, r)$ and $\pi_1^s(\phi) = \phi_s$. For $\tau \in X_1$, we define $(\sigma_0^\tau, \sigma_1^\tau)$ as $\sigma_0^\tau(x, r) = (x, r + \tau(x))$ and $\sigma_1^\tau(\phi) = \phi + \tau$. Let S be a subgroup generated by $\{(\pi_0^s, \pi_1^s) : s \in H\} \cup \{(\sigma_0^\tau, \sigma_1^\tau) : \tau \in X_1\}$. Then, S satisfies the fourth condition in Theorem 6. See the full version for details.

We also show that an augmented form of the inner product can be expressed as a special instance of the index function f in Eq. (2) and hence admits ideal PSM. Formally, define $\mathsf{IP}_{q,r} : (\mathbb{F}_q^r \times \mathbb{F}_q) \times (\mathbb{F}_q^r \times \mathbb{F}_q) \to \mathbb{F}_q$ as

$$\mathsf{IP}_{q,r}((\mathbf{x}_0, a_0), (\mathbf{x}_1, a_1)) = \langle \mathbf{x}_0, \mathbf{x}_1 \rangle - a_0 - a_1$$

for any $\mathbf{x}_0, \mathbf{x}_1 \in \mathbb{F}_q^r$ and $a_0, a_1 \in \mathbb{F}_q$. Let $G = \mathbb{F}_q$ and $H = \mathbb{F}_q^r$. For $\mathbf{x}_1 \in \mathbb{F}_q^r$ and $a_1 \in \mathbb{F}_q$, define a function $\phi^{\mathbf{x}_1, a_1} : H \to G$ as $\phi^{\mathbf{x}_1, a_1}(\mathbf{x}_0) = \langle \mathbf{x}_0, \mathbf{x}_1 \rangle - a_1$ for any $\mathbf{x}_0 \in H$. Let $X_0 = H \times G$ and $X_1 = \mathcal{F} = \{\phi^{\mathbf{x}_1, a_1} : \mathbf{x}_1 \in \mathbb{F}_q^r, a_1 \in \mathbb{F}_q\}$. It then holds that $\mathsf{IP}_{q,r}((\mathbf{x}_0, a_0), (\mathbf{x}_1, a_1)) = f((\mathbf{x}_0, a_0), \phi^{\mathbf{x}_1, a_1})$. We have that $\phi^{\mathbf{x}_1, a_1} + \phi^{\mathbf{x}_1', a_1'} = \phi^{\mathbf{x}_1 + \mathbf{x}_1', a_1 + a_1'}$ and $\phi_{\mathbf{s}}^{\mathbf{x}_1, a_1}(\mathbf{x}_0) := \phi^{\mathbf{x}_1, a_1}(\mathbf{x}_0 - \mathbf{s}) = \phi^{\mathbf{x}_1, a_1 + \langle \mathbf{s}, \mathbf{x}_1 \rangle}(\mathbf{x}_0)$. Hence, X_1 satisfies the assumption in Section 6.3.

7 Communication-efficient and Simplified PSM Schemes

In this section, we improve the communication complexity of state-of-the-art PSM schemes for several functions. Our constructions follow the same template: We embed a target function f into a larger function f' that admits an ideal PSM scheme, from which we naturally derive a PSM scheme for f. Since the ideal PSM scheme is communication-optimal, the key question is how much we can restrict the domain of f' while still containing f as a restriction. Formally, we say that a function $f : X_0 \times X_1 \to Y$ is *embedded* into a function $f' : X_0' \times X_1' \to Y$ if there are injective functions $\tau_i : X_i \to X_i'$ such that $f(x_0, x_1) = f'(\tau_0(x_0), \tau_1(x_1))$ for all $(x_0, x_1) \in X_0 \times X_1$. If f is embedded into f', then a PSM scheme for f' naturally induces a PSM scheme for f.

7.1 Functions with Sparse/Dense Truth-tables

First, we consider functions with sparse truth-tables. Specifically, let $f : [N_0] \times [N_1] \to \{0,1\}$ be a function such that each row of the truth-table T_f has at most d ones for a small $d \ll N_1$. Prior to this work, the only general construction in [7] can apply, resulting in communication complexity of $O(\max\{\sqrt{N_0}, \sqrt{N_1}\})$.

We show an efficient PSM scheme for f with communication complexity $O(d \log(N_1 + d))$, resulting in a strict improvement over [7] when $d = o(\sqrt{N_1}/\log N_1)$. The same communication complexity can be attained when the columns of the truth-table are sparse. These schemes also apply to functions such that the rows (or the columns) are dense, that is, they contain at least $n - d$ ones for a small d, by taking the NOT of sparse functions.

▶ **Proposition 9.** *Let $f : [N_0] \times [N_1] \to \{0,1\}$ be a non-degenerate function such that for any $x_0 \in X_0$, the number of ones in the row $T_f[x_0, *]$ of the truth-table T_f is at most d. Then, there exists a PSM scheme for f such that $|M_0| = \binom{N_1+d}{d}$ and $|M_1| = N_1 + d$.*

Proof. We show that f is embedded into an ideal PSM function $f' : [N_0'] \times [N_1'] \to \{0,1\}$ with $N_0' = \binom{N_1+d}{d}$ and $N_1' = N_1 + d$. Then, an ideal PSM scheme for f' induces a PSM scheme Π for f with the stated communication complexity.

We define $f'' : [N_0] \times [N_1'] \to \{0,1\}$ by specifying its truth-table $T_{f''}$ as follows. For each $x_0 \in [N_0]$, define the row vector $T_{f''}[x_0, *]$ of length $N_1' = N_1 + d$ by appending $d - w_{x_0}$ ones and w_{x_0} zeros to the right of $T_f[x_0, *]$, where w_{x_0} denotes the number of ones in $T_f[x_0, *]$. Clearly, f is embedded into f'' and each row of $T_{f''}$ contains exact d ones.

We set $f' = \mathsf{PSIC}_{N_1',(d,1)}$. Note that f' has a domain $[N_0'] \times [N_1']$ with $N_0' = \binom{N_1+d}{d}$ and $N_1' = N_1 + d$. Then, f'' is embedded into f' since the rows of the truth-table of f' contains any row vector of weight d. Therefore, f is embedded into f'. ◀

7.2 Functions with Low-Rank Truth-tables

Narayanan et al. [41] showed PSM schemes for functions that have bounded tiling numbers. Specifically, a k-tiling of a function $f : X_0 \times X_1 \to Y$ is a partition of $X_0 \times X_1$ into k monochromatic rectangles, i.e., a tuple of rectangles $(R_i)_{i \in [k]}$ such that for every $i \in [k]$, there exists $y_i \in Y$ such that $f(x_0, x_1) = y_i$ for all $(x_0, x_1) \in R_i$. The tiling number of a function f is defined as the smallest number k such that f has a k-tiling. They showed a PSM scheme for f with communication complexity $O(k \log |Y|)$, where k is the tiling number of f.

Let q be the smallest prime power larger than $|Y|$ (we can choose q so that $q = O(|Y|)$). Then, the truth-table T_f of a function $f : X_0 \times X_1 \to Y$ can be viewed as a $|X_0|$-by-$|X_1|$ matrix over $\mathbb{F}_q$. In the following, we present a PSM scheme for f with communication complexity $O(r \log q) = O(r \log |Y|)$, where r is the rank of T_f over $\mathbb{F}_q$. As is well known, it holds that $k \geq r$ since T_f can be represented as a sum of k rank-1 matrices if f has a k-tiling (e.g. [31]). Our construction thus achieves a more refined communication complexity than [41].

▶ **Proposition 10.** *Let $f : [N_0] \times [N_1] \to \mathbb{F}_q$ be a non-degenerate function whose truth-table $T_f \in \mathbb{F}_q^{N_0 \times N_1}$ has rank r as a matrix over $\mathbb{F}_q$. Then, there exists a PSM scheme for f such that $|M_0| = |M_1| = q^r$.*

Proof. We show that f is embedded into the inner-product function $\mathsf{IP}_{q,r} : \mathbb{F}_q^r \times \mathbb{F}_q^r \to \mathbb{F}_q$. Then, the proposition follows since $\mathsf{IP}_{q,r}$ admits ideal PSM.

Since T_f has rank r, there exist two matrices $\mathbf{M}_0 \in \mathbb{F}_q^{N_0 \times r}$ and $\mathbf{M}_1 \in \mathbb{F}_q^{N_1 \times r}$ such that $T_f = \mathbf{M}_0 \mathbf{M}_1^\top$ as matrices over $\mathbb{F}_q$. In particular, it holds that $T_f[x_0, x_1] = \langle \mathbf{M}_0[x_0], \mathbf{M}_1[x_1] \rangle$ for any $(x_0, x_1) \in [N_0] \times [N_1]$, where $\mathbf{M}_i[x]$ denotes the x-th row vector of $\mathbf{M}_i$.

For each $i \in \{0, 1\}$, define $\tau_i : [N_i] \to \mathbb{F}_q^r$ by $\tau_i(x) = \mathbf{M}_i[x]$ for any $x \in [N_i]$. From the above, we have $f(x_0, x_1) = \mathsf{IP}_{q,r}(\tau_0(x_0), \tau_1(x_1))$ for any (x_0, x_1). Since f is non-degenerate, the rows of $\mathbf{M}_i$ are pairwise distinct and hence τ_i is injective. Therefore, f is embedded into $\mathsf{IP}_{q,r}$ via the τ_i's. ◀

7.3 Simplified PSM for General Functions

Beimel et al. [7] showed a PSM scheme for a general function $f : [N] \times [N] \to \{0, 1\}$ with communication complexity $O(\sqrt{N})$. According to the description in [3], the more precise communication complexity is at least $12\sqrt{N}$. In the following, we present a PSM scheme for f with communication complexity $8\sqrt{N} + 2$, improving the constant factor in the dominant term of the state-of-the-art construction. An additional benefit is that our construction is simpler and more direct: the message and evaluation functions are given in closed form, unlike the hierarchical designs of [3, 7], which rely on nested invocations of PSM schemes for smaller functions.

Let $f : [N] \times [N] \to \{0, 1\}$ be a non-degenerate function. We assume that N is a square number. Otherwise, we embed f into a function f' with domain $[N'] \times [N']$ for the smallest square number N' with $N' > N$. Let $n = \sqrt{N}$. We define a multi-linear function $\hat{f} \colon (\{0, 1\}^n)^4 \to \{0, 1\}$ as

$$\hat{f}(\mathbf{a}_0, \mathbf{b}_0, \mathbf{a}_1, \mathbf{b}_1) = \sum_{i_0, j_0, i_1, j_1 \in [n]} \mathbf{a}_0[i_0] \cdot \mathbf{b}_0[j_0] \cdot \mathbf{a}_1[i_1] \cdot \mathbf{b}_1[j_1] \cdot f(i_0 n + j_0, i_1 n + j_1)$$

for any $\mathbf{a}_0, \mathbf{b}_0, \mathbf{a}_1, \mathbf{b}_1 \in \{0, 1\}^n$, where we denote the i-th bit of a vector $\mathbf{v}$ by $\mathbf{v}[i]$. Let $X = Y = (\{0, 1\}^n)^4 \times \{0, 1\}$. We define $G_f \colon X \times Y \to \{0, 1\}$ as

$$\begin{aligned} &G_f((\mathbf{x}_0, \mathbf{x}_1, \mathbf{i}_0, \mathbf{i}_1, a), (\mathbf{y}_0, \mathbf{y}_1, \mathbf{j}_0, \mathbf{j}_1, b)) \\ &= \hat{f}(\mathbf{x}_0, \mathbf{x}_1, \mathbf{y}_0, \mathbf{y}_1) \oplus \langle \mathbf{x}_0, \mathbf{j}_0 \rangle \oplus \langle \mathbf{x}_1, \mathbf{j}_1 \rangle \oplus \langle \mathbf{y}_0, \mathbf{i}_0 \rangle \oplus \langle \mathbf{y}_1, \mathbf{i}_1 \rangle \oplus a \oplus b. \end{aligned}$$

Note that $\hat{f}(\mathbf{u}_x, \mathbf{v}_x, \mathbf{u}_y, \mathbf{v}_y) = f(x, y)$, where we let $\mathbf{e}_x \in \{0, 1\}^N$ denote a one-hot vector whose x-th element is one, and $\mathbf{u}_x, \mathbf{v}_x \in \{0, 1\}^n$ denote one-hot vectors such that $\mathbf{u}_x \otimes \mathbf{v}_x = \mathbf{e}_x$. Thus, we have $G_f((\mathbf{u}_x, \mathbf{v}_x, \mathbf{0}, \mathbf{0}, 0), (\mathbf{u}_y, \mathbf{v}_y, \mathbf{0}, \mathbf{0}, 0)) = f(x, y)$ and hence f is embedded into G_f. In the full version, we show that G_f admits ideal PSM, which implies that there exists a PSM scheme for f with communication complexity $8\lceil\sqrt{N}\rceil + 2$. This improves the dominant term $12\sqrt{N}$ of the best known PSM scheme for general functions [7].

References

1 `https://github.com/hiwatashi-keitaro/idealPSM`, 2025.

2 Benny Applebaum, Thomas Holenstein, Manoj Mishra, and Ofer Shayevitz. The communication complexity of private simultaneous messages, revisited. *Journal of Cryptology*, 33(3):917–953, 2020. `doi:10.1007/S00145-019-09334-Y`.

3 Léonard Assouline and Tianren Liu. Multi-party psm, revisited: Improved communication and unbalanced communication. In *Theory of Cryptography*, pages 194–223, 2021. `doi:10.1007/978-3-030-90453-1_7`.

4 Marshall Ball and Tim Randolph. A note on the complexity of private simultaneous messages with many parties. In *3rd Conference on Information-Theoretic Cryptography, ITC 2022*, pages 7:1–7:12, 2022. `doi:10.4230/LIPIcs.ITC.2022.7`.

5 Amos Beimel, Ariel Gabizon, Yuval Ishai, and Eyal Kushilevitz. Distribution design. In *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science*, ITCS '16, pages 81–92, 2016. doi:10.1145/2840728.2840759.

6 Amos Beimel, Ariel Gabizon, Yuval Ishai, Eyal Kushilevitz, Sigurd Meldgaard, and Anat Paskin-Cherniavsky. Non-interactive secure multiparty computation. In *Advances in Cryptology – CRYPTO 2014, Part II*, pages 387–404, 2014. doi:10.1007/978-3-662-44381-1_22.

7 Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. In *Theory of Cryptography*, pages 317–342, 2014. doi:10.1007/978-3-642-54242-8_14.

8 Amos Beimel, Yuval Ishai, and Eyal Kushilevitz. Ad hoc PSM protocols: Secure computation without coordination. In *Advances in Cryptology – EUROCRYPT 2017, Part III*, pages 580–608, 2017. doi:10.1007/978-3-319-56617-7_20.

9 Amos Beimel, Eyal Kushilevitz, and Pnina Nissim. The complexity of multiparty PSM protocols and related models. In *Advances in Cryptology – EUROCRYPT 2018, Part II*, pages 287–318, 2018. doi:10.1007/978-3-319-78375-8_10.

10 Amos Beimel, Noam Livne, and Carles Padró. Matroids can be far from ideal secret sharing. In *Theory of Cryptography*, pages 194–212, 2008. doi:10.1007/978-3-540-78524-8_12.

11 Amos Beimel, Tamir Tassa, and Enav Weinreb. Characterizing ideal weighted threshold secret sharing. *SIAM Journal on Discrete Mathematics*, 22(1):360–397, 2008. doi:10.1137/S0895480104445654.

12 Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 1–10, 1988.

13 Fabrice Benhamouda, Hugo Krawczyk, and Tal Rabin. Robust non-interactive multiparty computation against constant-size collusion. In *Advances in Cryptology – CRYPTO 2017, Part I*, pages 391–419, 2017. doi:10.1007/978-3-319-63688-7_13.

14 G. R. Blakley. Safeguarding cryptographic keys. In *1979 International Workshop on Managing Requirements Knowledge (MARK)*, pages 313–318, 1979. doi:10.1109/MARK.1979.8817296.

15 Ernest F. Brickell. Some ideal secret sharing schemes. In *Advances in Cryptology — EUROCRYPT '89*, pages 468–475, 1990.

16 Ernest F Brickell and Daniel M Davenport. On the classification of ideal secret sharing schemes. *Journal of Cryptology*, 4(2):123–134, 1991. doi:10.1007/BF00196772.

17 David Chaum, Claude Crépeau, and Ivan Damgard. Multiparty unconditionally secure protocols. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 11–19, 1988.

18 Qi Chen, Chunming Tang, and Zhiqiang Lin. Efficient explicit constructions of compartmented secret sharing schemes. *Designs, Codes and Cryptography*, 87(12):2913–2940, 2019. doi:10.1007/S10623-019-00657-2.

19 Richard Cleve. Towards optimal simulations of formulas by bounded-width programs. In *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, pages 271–277, 1990. doi:10.1145/100216.100251.

20 Ivan Damgård and Jesper Buus Nielsen. Scalable and unconditionally secure multiparty computation. In *Advances in Cryptology – CRYPTO 2007*, pages 572–590, 2007. doi:10.1007/978-3-540-74143-5_32.

21 Ivan Damgård, Valerio Pastro, Nigel Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. In *Advances in Cryptology – CRYPTO 2012*, pages 643–662, 2012. doi:10.1007/978-3-642-32009-5_38.

22 Ivan Damgård, Kasper Green Larsen, and Jesper Buus Nielsen. Communication lower bounds for statistically secure mpc, with or without preprocessing. In *Advances in Cryptology – CRYPTO 2019*, pages 61–84, 2019. doi:10.1007/978-3-030-26951-7_3.

23 Deepesh Data, Manoj Prabhakaran, and Vinod M. Prabhakaran. On the communication complexity of secure computation. In *Advances in Cryptology - CRYPTO 2014*, pages 199–216, 2014. doi:10.1007/978-3-662-44381-1_12.

24 Reo Eriguchi, Kazuma Ohara, Shota Yamada, and Koji Nuida. Non-interactive secure multiparty computation for symmetric functions, revisited: More efficient constructions and extensions. In *Advances in Cryptology – CRYPTO 2021*, pages 305–334, 2021. doi:10.1007/978-3-030-84245-1_11.

25 Reo Eriguchi and Kazumasa Shinagawa. Efficient multiparty private simultaneous messages for symmetric functions. In *Advances in Cryptology – EUROCRYPT 2025*, pages 240–269, 2025. doi:10.1007/978-3-031-91092-0_9.

26 Oriol Farràs, Jaume Martí-Farré, and Carles Padró. Ideal multipartite secret sharing schemes. *Journal of Cryptology*, 25(3):434–463, 2012. doi:10.1007/S00145-011-9101-6.

27 Oriol Farràs and Carles Padró. Ideal hierarchical secret sharing schemes. In *Theory of Cryptography*, pages 219–236, 2010. doi:10.1007/978-3-642-11799-2_14.

28 Oriol Farràs and Carles Padró. Ideal secret sharing schemes for useful multipartite access structures. In *Coding and Cryptology*, pages 99–108, 2011. doi:10.1007/978-3-642-20901-7_6.

29 Uri Feige, Joe Kilian, and Moni Naor. A minimal model for secure computation (extended abstract). In *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing*, STOC '94, pages 554–563, 1994.

30 O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, STOC '87, pages 218–229, 1987.

31 Mika Göös, Toniann Pitassi, and Thomas Watson. Deterministic communication vs. partition number. *SIAM Journal on Computing*, 47(6):2435–2450, 2018. doi:10.1137/16M1059369.

32 Shai Halevi, Yuval Ishai, Abhishek Jain, Eyal Kushilevitz, and Tal Rabin. Secure multiparty computation with general interaction patterns. In *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science*, ITCS '16, pages 157–168, 2016. doi:10.1145/2840728.2840760.

33 Y. Ishai and E. Kushilevitz. Private simultaneous messages protocols with applications. In *Proceedings of the Fifth Israeli Symposium on Theory of Computing and Systems*, pages 174–183, 1997.

34 Yuval Ishai. Randomization techniques for secure computation. *Secure Multi-Party Computation*, 10:222–248, 2013. doi:10.3233/978-1-61499-169-4-222.

35 Yuval Ishai, Ranjit Kumaresan, Eyal Kushilevitz, and Anat Paskin-Cherniavsky. Secure computation with minimal interaction, revisited. In *Advances in Cryptology – CRYPTO 2015*, pages 359–378, 2015. doi:10.1007/978-3-662-48000-7_18.

36 Yuval Ishai, Eyal Kushilevitz, and Anat Paskin. Secure multiparty computation with minimal interaction. In *Advances in Cryptology – CRYPTO 2010*, pages 577–594, 2010. doi:10.1007/978-3-642-14623-7_31.

37 E. Karnin, J. Greene, and M. Hellman. On secret sharing systems. *IEEE Transactions on Information Theory*, 29(1):35–41, 1983. doi:10.1109/TIT.1983.1056621.

38 Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Conditional disclosure of secrets via non-linear reconstruction. In *Advances in Cryptology – CRYPTO 2017*, pages 758–790, 2017. doi:10.1007/978-3-319-63688-7_25.

39 Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Towards breaking the exponential barrier for general secret sharing. In *Advances in Cryptology – EUROCRYPT 2018*, pages 567–596, 2018. doi:10.1007/978-3-319-78381-9_21.

40 Jaume Martí-Farré and Carles Padró. On secret sharing schemes, matroids and polymatroids. In *Theory of Cryptography*, pages 273–290, 2007. doi:10.1007/978-3-540-70936-7_15.

41 Varun Narayanan, Manoj Prabhakaran, and Vinod M. Prabhakaran. Zero-communication reductions. In *Theory of Cryptography*, pages 274–304, 2020. doi:10.1007/978-3-030-64381-2_10.

42 Carles Padró and Germán Sáez. Secret sharing schemes with bipartite access structure. *IEEE Transactions on Information Theory*, 46(7):2596–2604, 2000. doi:10.1109/18.887867.

43 László Pyber. Asymptotic results for permutation groups. In *Groups And Computation*, 1991.

44 László Pyber and Aner Shalev. Asymptotic results for primitive permutation groups. *Journal of Algebra*, 188(1):103–124, 1997.

45 A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979. doi:10.1145/359168.359176.

46 Kazumasa Shinagawa, Reo Eriguchi, Shohei Satake, and Koji Nuida. Private simultaneous messages based on quadratic residues. *Designs, Codes and Cryptography*, 91(12):3915–3932, 2023. doi:10.1007/S10623-023-01279-5.

47 Kazumasa Shinagawa and Koji Nuida. Explicit lower bounds for communication complexity of PSM for concrete functions. In *Progress in Cryptology - INDOCRYPT 2023*, pages 45–61, 2023. doi:10.1007/978-3-031-56235-8_3.

48 Tamir Tassa. Hierarchical threshold secret sharing. In *Theory of Cryptography*, pages 473–490, 2004. doi:10.1007/978-3-540-24638-1_26.

49 Andrew C. Yao. Protocols for secure computations. In *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, SFCS '82, pages 160–164, 1982.