A Note on the Complexity of Private Simultaneous Messages with Many Parties

Marshall Ball
Courant Institute of Mathematical Sciences, New York University, NY, USA

Tim Randolph
Columbia University, New York, NY, USA

Abstract

For $k = \omega(\log n)$, we prove a $\Omega(k^2 n / \log(kn))$ lower bound on private simultaneous messages (PSM) with k parties who receive n-bit inputs.

This extends the $\Omega(n)$ lower bound due to Appelbaum, Holenstein, Mishra and Shayevitz [Journal of Cryptology, 2019] to the many-party ($k = \omega(\log n)$) setting. It is the first PSM lower bound that increases quadratically with the number of parties, and moreover the first *unconditional, explicit* bound that grows with both k and n. This note extends the work of Ball, Holmgren, Ishai, Liu, and Malkin [ITCS 2020], who prove communication complexity lower bounds on decomposable randomized encodings (DREs), which correspond to the special case of k-party PSMs with $n = 1$. To give a concise and readable introduction to the method, we focus our presentation on perfect PSM schemes.

2012 ACM Subject Classification Theory of computation → Cryptographic protocols; Theory of computation → Communication complexity; Security and privacy → Information-theoretic techniques

Keywords and phrases Secure computation, Private Simultaneous Messages

Digital Object Identifier 10.4230/LIPIcs.ITC.2022.7

Funding *Marshall Ball*: Part of this work was performed while the author was a student at Columbia University and a postdoc at University of Washington. This material is based upon work supported by the National Science Foundation under Grant #2030859 to the Computing Research Association for the CIFellows Project. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation nor the Computing Research Association.
Tim Randolph: This material is based upon work supported by the following grants: NSF CCF-1563155, NSF IIS-1838154, NSF CCF-1814873, NSF CCF-1703925, NSF CCF-2106429, and NSF CCF-2107187.

Acknowledgements The authors thank Tal Malkin for helpful discussion, and several anonymous reviewers for helpful comments on an earlier draft.

1 Introduction

In this note, we consider *private simultaneous message* (PSM) protocols. In this setting, we are given as public input a function $f : [N]^k \to \{0,1\}$.[1] There are k parties, each with private inputs $x_1, x_2, \ldots, x_k$ and access to a shared random string. Each party sends a single message to a referee in such a way that the referee can reconstruct $f(x_1, x_2, ..., x_k)$ but learns no other information about the private inputs. The communication complexity, or size, of a PSM protocol is the total number of bits sent by all parties.

[1] We write $f : \{\{0,1\}^n\}^k \to \{0,1\}$, where $n = \log_2(N)$, interchangeably.

The (2-party) PSM model was introduced as an elegant variant of secure computation by Feige, Kilian, and Naor in 1994 [8], and readily extended to the k-party case by Ishai and Kushilevitz [11]. The simple protocol structure makes the model an attractive proving ground for understanding the "cost of privacy" (i.e., communication complexity) in secure computation over distributed protocols with no privacy or security guarantees.

In addition to their theoretical importance, PSM protocols have practical import because they readily decompose into an expensive offline phase and an efficient single-message online phase.[2]

Significant progress on upper and lower bounds on the communication complexity of PSM has occurred since its introduction. In 2019, Assouline and Liu, building on the work of Beimel, Kushilevitz, and Nissim [5, 6], demonstrated a general PSM protocol with complexity $O_k(N^{(k-1)/2})$ for infinitely many k [2]. Also in 2019, Applebaum, Holenstein, Mishra, and Shayevitz [1] patched up a hole in the original PSM paper to establish a $3n - O(\log(n))$ lower bound for the two party case. This bound can be trivially extended to the k-party case by dividing the input of a boolean function on kn bits between k parties, in which case the bound becomes $3kn - O(\log(n))$.

The PSM setting can also be viewed as the addition of a security requirement to simultaneous multi-party communication complexity. Although the *number-on-forehead* model, in which players can see every input but their own, is more common in this setting, perfect multi-party PSM corresponds well to the deterministic *number-in-hand* model, in which k parties receive inputs $x_1, x_2, \cdots, x_k$ and send messages that allow a referee to compute $f(x_1, x_2, \cdots, x_k)$. $\Omega(kn)$ lower bounds exist in this setting (see, for example, [9]). Every multi-party PSM protocol with perfect correctness can be converted to a deterministic simultaneous number-in-hand communication protocol by fixing a shared random string, so these lower bounds apply to our setting.

A final related notion is that of *randomized encodings*, which originate from Yao's garbled circuits [15] and were elaborated by Ishai and Kushilevitz [12]. A randomized encoding of a function $f : \{0,1\}^k \to \{0,1\}$ is a function $\hat{f}$ that takes as input $x \in \{0,1\}^k$ and a random string r. For any r, given $\hat{f}(x, r)$ it must be possible to recover $f(x)$ but no other information about x. A randomized encoding is *decomposable* if $\hat{f}(x, r)$ can be written $(\hat{f}_1(x_1, r), \hat{f}_2(x_2, r), ..., \hat{f}_n(x_k, r))$; that is, if every bit of the output depends only on a single bit of x. Thus a DRE immediately implies a PSM protocol: parties compute the relevant portions of $\hat{f}$ using their shared randomness and send them to the referee. Moreover, a k-party PSM scheme in which every party receives exactly one bit is a DRE. A recent paper by Ball, Holmgren, Ishai, Liu, and Malkin establishes $\Omega(k^2/log(k))$ lower bounds on the communication complexity of DREs, implying corresponding lower bounds on PSM protocols [3]. Their result relies on a measure of function complexity first introduced by Nečiporuk in 1966 [13] and subsequently used to prove lower bounds on the sizes of formulas, branching programs and span programs [4, 7].

In this note, we introduce a new variant of Nečiporuk's measure of function complexity (as defined in [3]) and show it suffices to extend the approach of [3]: demonstrating that PSM complexity is lower-bounded by our modified Nečiporuk measure. We give two natural examples of explicit functions with modified Nečiporuk measure $\Omega(k^2 n/\log(kn))$ and additionally show that nearly all functions have such measure. Our main result is the following theorem:

[2] This paradigm has gained significant traction in recent years. However, typical use cases require stronger security requirements than that provided by PSM, such as resilience to the referee colluding with senders (Non-Interactive Secure Multiparty Computation). Note that lower bounds on the communication complexity of PSM protocols immediately extend to lower bounds on its stronger cousins.

▶ **Theorem 1.** *As long as $k = \omega(\log(n))$, there exist (explicit) functions $f : [N]^k \to \{0,1\}$ such that any perfect PSM $\mathcal{X}$ for f has size*

$$|\mathcal{X}| \geq \frac{k^2 n}{2\log_2(kn)} - O(kn).$$

To the best of our knowledge, this is the first unconditional, explicit[3] lower bound on the communication of PSM that increases with k and n, the first to grow quadratically with k, as well as the best in the many-party ($k = \omega(\log(n))$) setting.

In Appendix B, we argue that significantly better bounds (i.e., $\omega(k^2 n)$) will likely require very different techniques due a certain kind of natural proof barrier [14] which may be of independent interest.

2 Preliminaries

▶ **Definition 2** (PSM Protocol). *A PSM protocol $(M, R, (\Pi)_{i\in[k]}, \texttt{Ref})$ for a function $f : [N]^k \to \{0,1\}$ specifies a message space M, a randomness space R, a tuple of functions, $\Pi_i : [N] \times R \to M$ for $i \in [k]$, and a referee $\texttt{Ref} : [M]^k \to \{0,1\}$. It must satisfy that for every input $x \in [N]^k$ and every $r \in R$,*

$$\texttt{Ref}\big((\Pi_i(x_i, r))_{i\in[k]}\big) = f(x)$$

(perfect correctness), and that for all $x, y \in [N]^k$ such that $f(x) = f(y)$, when r is sampled uniformly from R,

$$\{(\Pi_i(x_i, r))_{i\in[k]}\}_{r\sim R} \equiv \{(\Pi_i(y_i, r))_{i\in[k]}\}_{r\sim R}$$

(perfect security).

Informally, each function Π_i captures the behavior of one of the k agents. Given an input in $[N]$ and a shared random string drawn from R, each agent produces a private message $m \in M$ that is sent to the referee. The referee evaluates f based on the messages she receives. Correctness and security requirements ensure that the referee always evaluates f correctly but never learns any other information about the input.

For this note, we consider perfect correctness and security. This choice keeps our presentation tidy while focusing on our contribution, which is a modification of Nečiporuk's measure and the extension of [3] to the multiparty PSM setting. The perfect security case highlights the core conceptual techniques of [3]. The result extends to multiparty PSMs with statistical or even (nonuniform) computational security, following the presentation of [3].

The traditional definition of the PSM setting is provided for completeness and comparison. For our investigation, it will be convenient to use the following equivalent definition of a PSM.

▶ **Definition 3** (Random Family Definition of PSM). *A PSM protocol for a function $f : [N]^k \to \{0,1\}$ is a family of random variables*

$$\mathcal{X} = (\mathcal{X}_j^i)_{j\in[N]}^{i\in[k]}$$

[3] Applebaum et al. [1] show a random function requires high communication unconditionally. They only construct an explicit function with high communication *under a hardness assumption on co-nondeterministic circuits*. In contrast, we give an unconditional explicit lower bound.

supported on M and a referee function $\texttt{Ref}$ *such that for all* $x \in [N]^k$,

$$\Pr[\texttt{Ref}((\mathcal{X}^i_{x_i})^{i\in[k]}) = f(x)] = 1$$

(correctness) and for all x, y *such that* $f(x) = f(y)$, *we have*

$$(\mathcal{X}^i_{x_i})^{i\in[k]} \equiv (\mathcal{X}^i_{y_i})^{i\in[k]}$$

(security).

▶ **Definition 4** (PSM size [3]). *The* size *of a PSM* $\mathcal{X}$ *is*

$$|\mathcal{X}| = \max_{x\in[N]^k} \sum_{i\in[k]} \lceil \log_2(|\texttt{Supp}(\mathcal{X}^i_{x_i})|)\rceil,$$

where $\texttt{Supp}(\mathcal{Y})$ *indicates the support of* $\mathcal{Y}$.

This coincides with the multiparty extension of Applebaum et al.'s definition of size as $\log|A| + \log|B|$, where A and B are the message spaces of the two parties, in the two party case. This notion of size corresponds to the sum of the channel widths required by the sending parties.

3 A Measure of the Complexity of a Function

To lower bound PSM size, we use Nečiporuk's measure of function complexity, which counts the maximum number of distinct nonzero restrictions of a boolean function over any partition of the input. For any subset $S \subseteq [k]$, we write $\overline{S}$ to denote $[k] \setminus S$, and $f_{S|z}$ to indicate the restriction of f to S in which the coordinates corresponding to $\overline{S}$ are fixed to the vector $z \in \{0,1\}^{\overline{S}}$.

▶ **Definition 5** (Nečiporuk's Measure [13, 3]). *Let* $f : \{0,1\}^k \to \{0,1\}$ *be any boolean function. For any subset* $S \subseteq [k]$, *define*

$$g_S(f) := \log_2(|\{f_{S|z} : z \in \{0,1\}^{\overline{S}}, f_{S|z} \not\equiv 0\}|).$$

For any positive integer $m \leq k$, *let* $V = (V_1, V_2, ..., V_m)$ *denote an* m*-partition of* $[k]$. *The measure is* $G(f) := \max_V \sum_{V_i\in V} g_{V_i}(f)$.

We are interested in functions that take boolean input in $\{\{0,1\}^n\}^k$. Unlike in the DRE setting, each message sent to the referee depends collectively on n bits of the input. Thus, when we restrict functions, we will need to carefully distinguish between inputs in $\{0,1\}^n$ in which all bits are restricted and inputs in $\{0,1\}^n$ in which only some bits are restricted. This requires a corresponding modification of Nečiporuk's measure.

▶ **Definition 6** (First-Bit Restriction). *For any function* $f : \{\{0,1\}^n\}^k \to \{0,1\}$ *and any set* $S \subseteq [k]$, *the* first-bit restriction of f to S using (α, β) *is the function*

$$f_{S|(\alpha,\beta)} : \{0,1\}^S \to \{0,1\}$$

defined by restricting the inputs as follows:

1. *Fix the* n*-bit inputs corresponding to* $\overline{S}$ *to* $\alpha \in \{\{0,1\}^n\}^{\overline{S}}$.
2. *Fix the last* $n-1$ *bits of each* n*-bit input corresponding to* S *to the values described by* $\beta \in \{\{0,1\}^{n-1}\}^S$.

Thus a first-bit restriction of f to the set S is a boolean function on $|S|$ bits.[4]

▶ **Definition 7** (Modified Nečiporuk's Measure). *Let $f : \{\{0,1\}^n\}^k \to \{0,1\}$ be a function. For any subset $S \subseteq [k]$, define*

$$g_S^*(f) := \max_{\beta \in \{\{0,1\}^{n-1}\}^S} \log_2(|\{f_{S|(\alpha,\beta)} : \alpha \in \{\{0,1\}^n\}^{\overline{S}}, f_{S|(\alpha,\beta)} \not\equiv 0\}|).$$

For any positive integer $m \leq k$, let $V = (V_1, V_2, ..., V_m)$ denote an m-partition of $[k]$. The measure is $G^*(f) := \max_V \sum_{V_i \in V} g_{V_i}^*(f)$.

We can easily bound the largest possible Modified Nečiporuk Measure for any boolean function.

▶ **Proposition 8.** *For any boolean function $f : \{\{0,1\}^n\}^k \to \{0,1\}$,*

$$G^*(f) \leq \frac{k^2 n}{\log_2(kn)}.$$

Proof. For any $S \subseteq [k]$, $g_S^*(f) \leq (k - |S|)n$ as α can take no more than $2^{(k-|S|)n}$ different values. Moreover, $g_S^*(f) \leq 2^{|S|}$, the log of the number of distinct $|S|$-bit boolean functions. Balancing these two restrictions gives the upper bound. ◀

In Section 4, we show examples of functions with large modified Nečiporuk measure. Then, in Section 5, we show that modified Nečiporuk measure is a lower bound on PSM complexity. Together, these results imply Theorem 1.

4 Functions with Large Modified Nečiporuk Measure

For $k = \omega(\log(n))$, many functions have modified Nečiporuk measure that is asymptotically optimal. For instance:

▶ **Proposition 9** (Modified Nečiporuk Measure of Random Functions). *As long as $k = \omega(\log(n))$, a random function $f : \{\{0,1\}^n\}^k \to \{0,1\}$ has*

$$G^*(f) \geq \frac{k^2 n}{\log_2(kn)} - kn - 1$$

with probability at least $1 - \exp(-N^{\log_2(kn)})$.

We prove Proposition 9 in Appendix A. In addition to most randomly sampled functions, we describe two explicit functions with optimal modified Nečiporuk measure. The first is a straightforward generalization of the distinct elements function.

[4] One can consider a generalization of first bit restrictions by allowing α to specify a sequence of pairs from some partitioning of the input domains $\{0,1\}^n$ into pairs, and allowing "free variables" in the restricted function to correspond to evaluating f on either the first or second string in the pair. Suitably modifying G^* with such restrictions should yield identical bounds on PSM complexity. However, the present definition is more intelligible and sufficient for our purposes.

▶ **Definition 10** (Set Disjointness). *The* (k, n) set disjointness function *is defined for* k *such that* $k = \omega(\log n)$ *as follows:*

1. $DISJ_{k,n}$ *takes as input* kn *bits, parsed as bit strings of length* n*. We fix* m *such that* $2m\log_2(mn) = k$,[5] *and divide the* k *input strings into* m *"blocks", each containing* $2\log_2(mn)$ n*-bit strings.*
2. *We interpret each block* $i \in [m]$ *as a multiset* $S_i \subset [(mn)^2]$ *as follows. Let* $x_i^1, \cdots, x_i^{2\log(mn)}$ *denote the* n*-bit strings in block* i*. We consider* $x_i^1, \ldots, x_i^{2\log(mn)}$ *as the columns of an* $n \times 2\log(mn)$*-matrix, and read the* $2\log(mn)$ *elements of* S_i *off the rows. (That is, we concatenate the first bits of each* n*-bit string to get the first element of* S_i*, the second bits to get the second element, etc.)*
3. $DISJ_{k,n}$ *outputs 1 if all sets are pairwise disjoint (*$S_i \cap S_j = \emptyset$ *for all* $i \neq j$*).*

▶ **Proposition 11.** $G^*(\mathrm{DISJ}_{k,n}) = \Omega(k^2 n/\log(kn))$.

Proof. For $i \in [m]$, let V_i denote the ith block of bit strings, which corresponds to the subset $S_i \subset [(mn)^2]$. We will show $g^*_{V_i}(\mathrm{DISJ}) = \Omega(mn\log(mn)) = \Omega(kn)$. As $k = 2m\log_2(mn)$ implies $m > \frac{k}{2\log_2(kn)}$, this implies the result by symmetry on the m other choices for V_i.

Consider building first-bit restrictions as follows. Set $\beta \in \{\{0,1\}^{n-1}\}^{V_i}$ so that all but the first element of S_i take the value $(mn)^2$. (By the definition of first-bit restrictions, the first element of S_i is unrestricted.)

Then consider values for α, which specifies each S_j, $j \neq i$, that select *disjoint* subsets of $[(mn)^2 - 1]$. Each such α yields a restriction with respect to β: namely, the function that evaluates to 1 whenever the free element of S_i is not a member of $\bigcup_{S_j, j\neq i} S_j$. Thus, every choice of α that specifies a distinct set $\bigcup_{S_j, j\neq i} S_j$ composed of disjoint members corresponds to a distinct restriction.

Finally, we can bound the choices of α via

$$\#\alpha = \binom{(mn)^2 - 1}{n(m-1)} \geq \left(\frac{(mn)^2 - 1}{n(m-1)}\right)^{n(m-1)} \geq (mn)^{n(m-1)}.$$

Thus, $g^*_{V_i}(\mathrm{DISJ}) \geq n(m-1)\log_2(mn) = \Omega(kn)$. ◀

We additionally show a variation on the Indirect Storage Access function has maximal modified Nečiporuk measure.

▶ **Definition 12** (First-bit Indirect Storage Access). *The* (k, n) *first-bit indirect storage access (FISA) function is defined for* k *such that* $k = \omega(\log n)$ *as follows:*

1. $FISA_{k,n}$ *takes as input* $\log_2(k) + kn$ *bits. The first* $\log_2(k)$ *bits are parsed as an integer* $y \in [k]$ *and the remainder as the matrix* $A \in \{0,1\}^{k\times n}$*.*
2. $FISA_{k,n}$ *first identifies the* n*-bit string* A^y *(i.e., the* y^{th} *row of* A*), and then identifies an index in* $[kn]$ *corresponding to the bit string* $x = A_0^y A_0^{y+1} ... A_0^{y+\log(kn)-1}$*. (If we overflow the boundaries of* A*, we continue from* A^0*.) It then returns the* x*th bit of* A *(i.e.,* $A^{\lfloor x/n \rfloor}_{x \pmod n}$*).*

▶ **Proposition 13.** $G^*(FISA_{k,n}) = \Omega(k^2 n/\log(kn))$.

[5] Strictly speaking, this limits us to pairs (k, n) such that some integer m satisfies our condition. In order to define the function for arbitrary k, we might choose the largest m such that $2m\log_2(mn) \leq k$, set $k' := 2m\log_2(mn)$, and compute the (k', n) set disjointness function on the first k' input strings.

Proof. For simplicity, we treat $FISA_{k,n}$ as a kn-bit boolean function when calculating $G^*(FISA_{k,n})$, as the additional $\log_2(k)$ bits of input are absorbed by Ω. Consider a partition $V = (y, V_1, V_2, ..., V_{k/\log_2(kn)})$, in which each V_i contains $\log_2(kn)$ contiguous n-bit strings in A.

Fix $i \in [k/\log_2(kn)]$ and consider $g^*_{V_i}(FISA_{k,n})$. In particular, consider the first-bit restrictions of $FISA_{k,n}$ to V_i in which y is set so that the bit string x is read from the first bit of each n-bit string in V_i. Fixing the remaining bits of A to every possible string results in $2^{kn-n\log(kn)} - 1$ distinct non-zero restrictions. Summing over each set in the partition of A gives $G^*(f_{k,n}) = \Omega(k^2 n/\log(kn))$. ◀

5 A New Lower Bound for Many-Party PSM

We conclude by showing that the modified Nečiporuk measure provides a lower bound on PSM size. To prove this fact, we use an "information squeezing" argument enabled by the following observation that follows from the perfect security requirement in Definition 3 and is further elaborated in the proof of Lemma 15 below.

▶ **Observation 14.** *Let $f : \{\{0,1\}^n\}^k \to \{0,1\}$ be a kn-bit boolean function and $S \subseteq [k]$ denote a subset of parties. If there exist two first-bit restrictions $f_{S|(\alpha,\beta)}$ and $f_{S|(\alpha',\beta)}$ to S such that for some $x \in \{0,1\}^S$, $f_{S|(\alpha,\beta)}(x) = f_{S|(\alpha',\beta)}(x)$, the distribution over messages sent by $\overline{S}$ must be identical on α and α' in any PSM with perfect security.*

In other words, if two first-bit restrictions agree on at least one input, the perfect security requirement implies that the distribution over messages sent by $\overline{S}$ must be identical. Thus, in order to ensure correctness, the messages sent by a subset of parties S must contain enough information to distinguish between the distinct first-bit restrictions of f to S created by setting the inputs $\overline{S}$ to different values. The precise amount of information required is captured by the modified Nečiporuk measure.

▶ **Lemma 15** (Nečiporuk Lower Bounds PSM Size). *Let $\mathcal{X}$ be a PSM for any function $f : \{\{0,1\}^n\}^k \to \{0,1\}$. Then*

$$|\mathcal{X}| \geq G^*(f)/2.$$

Combining Lemma 15 with Proposition 9 yields Theorem 1 as an immediate consequence. In Appendix B, we argue that stronger lower bounds are beyond a certain kind of natural proof barrier.

5.1 Proof of Lemma 15: Nečiporuk Lower Bounds PSM Size

Proof. Fix $f : \{\{0,1\}^n\}^k \to \{0,1\}$, and let V be a partition of $[k]$ that maximizes our modified Nečiporuk measure for f; that is,

$$V \in \arg\max_U \sum_{U_i \in U} g^*_{U_i}(f)$$

Consider an arbitrary set $S \in V$. Select $\beta \in \{\{0,1\}^{n-1}\}^S$ to fix all but the first bits of S and maximize $|\{f_{S|(\alpha,\beta)} : \alpha \in \{\{0,1\}^n\}^{\overline{S}}, f_{S|(\alpha,\beta)} \not\equiv 0\}|$. Let $\mathcal{D}$ denote the uniform distribution over a minimal set T such that

$$\{f_{S|(\alpha,\beta)} | \alpha \in T\} = \{f_{S|(\alpha,\beta)} : \alpha \in \{\{0,1\}^n\}^{\overline{S}}, f_{S|(\alpha,\beta)} \not\equiv 0\}.$$

We observe that $H(\mathcal{D}) = g^*_S(f)$, where H denotes the entropy function. Given a PSM $\mathcal{X}$ for f, we proceed to define two subfamilies of random variables that will capture the information in $\mathcal{D}$.

$$\mathcal{A} := (\mathcal{X}^i_{\{0\}\times\beta_i}, \mathcal{X}^i_{\{1\}\times\beta_i})_{i\in S}$$

$$\mathcal{B} := (\mathcal{X}^i_{d_i})_{i\in\overline{S}, d\sim\mathcal{D}}.$$

Consider drawing $(a, b) \sim \mathcal{A} \times \mathcal{B}$, conditioned on a particular $d \in \mathtt{Supp}(\mathcal{D})$. Given any $y \in \{0,1\}^{|S|}$, the referee can use the appropriate members of a and b to compute $f_{S|(d,\beta)}(y)$. Computing $f_{S|(d,\beta)}(y)$ for each $y \in \{0,1\}^{|S|}$ uniquely identifies d because each member of T corresponds to a unique restriction; thus $H(\mathcal{D}|\mathcal{A}, \mathcal{B}) = 0$.

Furthermore, for any distinct $d, d' \in \mathtt{Supp}(\mathcal{D})$, there exist y and y' such that $f_{S|(d,\beta)}(y) = f_{S|(d',\beta)}(y') = 1$. (This follows by definition, as every $d \in \mathtt{Supp}(\mathcal{D})$ corresponds to a restriction that is not the zero function.) Thus, by the security property of PSM, we know that $(\mathcal{X}^i_{d_i})_{i\in\overline{S}} \equiv (\mathcal{X}^i_{d'_i})_{i\in\overline{S}}$. In other words, $\mathcal{B}$ contains no information about $\mathcal{D}$: $H(\mathcal{D}|\mathcal{B}) = H(\mathcal{D})$.

Using fundamental properties of the entropy function, we have that

$$H(\mathcal{A}) \geq H(\mathcal{A}|\mathcal{B}) = H(\mathcal{A}, \mathcal{D}|\mathcal{B}) - H(\mathcal{D}|\mathcal{A}, \mathcal{B}). \tag{1}$$

As $H(\mathcal{D}|\mathcal{A}, \mathcal{B}) = 0$ and $H(\mathcal{A}, \mathcal{D}|\mathcal{B}) \geq H(\mathcal{D}|\mathcal{B}) = H(\mathcal{D})$, we have

$$H(\mathcal{A}) \geq H(\mathcal{D}) = g^*_S(f). \tag{2}$$

Partition $\mathcal{A}$ into $\mathcal{A}_0 := (\mathcal{X}^i_{\beta_i\times\{0\}})_{i\in S}$ and $\mathcal{A}_1 := (\mathcal{X}^i_{\beta_i\times\{1\}})_{i\in S}$. As $H(\mathcal{A}) = H(\mathcal{A}_0, \mathcal{A}_1) \leq H(\mathcal{A}_0) + H(\mathcal{A}_1)$, $H(\mathcal{A}_b) \geq H(\mathcal{A})/2$ for some $b \in \{0,1\}$. Thus

$$2 \cdot \log_2(|\mathtt{Supp}(\mathcal{A}_b)|) \geq g^*_S(f).$$

Repeating this argument for each $S \in V$ demonstrates the existence of $x \in \{\{0,1\}^n\}^k$ for which $\sum_{i=1}^k \log_2(|\mathtt{Supp}(\mathcal{X}^i_{x_i})|) \geq G^*(f)/2$. ◀

References

1. Benny Applebaum, Thomas Holenstein, Manoj Mishra, and Ofer Shayevitz. The communication complexity of private simultaneous messages, revisited. *Journal of Cryptology*, pages 1–37, 2019.
2. Leonard Assouline and Tianren Liu. Multi-party PSM, revisited. Technical report, Cryptology ePrint Archive, Report 2019/657, 2019. URL: `https://eprint.iacr.org/2019/657`.
3. Marshall Ball, Justin Holmgren, Yuval Ishai, Tianren Liu, and Tal Malkin. On the complexity of decomposable randomized encodings, or: How friendly can a garbling-friendly PRF be? In *11th Innovations in Theoretical Computer Science Conference (ITCS 2020)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2020.
4. Paul Beame, Nathan Grosshans, Pierre McKenzie, and Luc Segoufin. Nondeterminism and an abstract formulation of Nečiporuk's lower bound method. *ACM Transactions on Computation Theory (TOCT)*, 9(1):1–34, 2016.
5. Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. In *Theory of Cryptography Conference*, pages 317–342. Springer, 2014.
6. Amos Beimel, Eyal Kushilevitz, and Pnina Nissim. The complexity of multiparty PSM protocols and related models. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 287–318. Springer, 2018. `doi:10.1007/978-3-319-78375-8_10`.

7 I Nečiporuk Eduard. On a boolean function. In *Soviet Math. Dokl*, volume 7, pages 999–1000, 1966.

8 Uri Feige, Joe Killian, and Moni Naor. A minimal model for secure computation. In *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*, pages 554–563, 1994.

9 Orr Fischer, Rotem Oshman, and Uri Zwick. Public vs. private randomness in simultaneous multi-party communication complexity. In *International Colloquium on Structural Information and Communication Complexity*, pages 60–74. Springer, 2016.

10 Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions (extended abstract). In *25th Annual Symposium on Foundations of Computer Science, West Palm Beach, Florida, USA, 24-26 October 1984*, pages 464–479. IEEE Computer Society, 1984. doi:10.1109/SFCS.1984.715949.

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

12 Yuval Ishai and Eyal Kushilevitz. Randomizing polynomials: A new representation with applications to round-efficient secure computation. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pages 294–304. IEEE, 2000.

13 Edward I Nechiporuk. A boolean function. *Engl. transl. in Sov. Phys. Dokl.*, 10:591–593, 1966.

14 Alexander A. Razborov and Steven Rudich. Natural proofs. *J. Comput. Syst. Sci.*, 55(1):24–35, 1997. doi:10.1006/jcss.1997.1494.

15 Andrew Chi-Chih Yao. How to generate and exchange secrets. In *27th Annual Symposium on Foundations of Computer Science (sfcs 1986)*, pages 162–167. IEEE, 1986.

A Proof of Proposition 9: Random Functions have Large Nečiporuk Measure

With $k = \omega(\log(n))$, let $f : [N]^k \to \{0,1\}$ be a random function. Recall that

$$2^{g^*_S(f)} := \max_{\beta \in \{\{0,1\}^{n-1}\}^S} |\{f_{S|(\alpha,\beta)} : \alpha \in \{\{0,1\}^n\}^{\overline{S}}, f_{S|(\alpha,\beta)} \not\equiv 0\}|.$$

For a given S, we define the convenient function

$$z^*_S(f,\beta) := |\{f_{S|(\alpha,\beta)} : \alpha \in \{\{0,1\}^n\}^{\overline{S}}\}|.$$

Thus $2^{g^*_S(f)} \geq \max_\beta z^*_S(f,\beta) - 1$, where the -1 arises because $z^*_S(f,\beta)$ may also count the zero function.

Fix b, the parameter that will specify the fixed bits of the inputs in S, arbitrarily. For every function $\phi : \{0,1\}^{|S|} \to \{0,1\}$, define the indicator random variable $\mathcal{Y}_{\phi,b}$ as follows:

$$\mathcal{Y}_{\phi,b} = \begin{cases} 1, & \text{if } \exists a \in \{\{0,1\}^n\}^{\overline{S}} : f_{S|(a,b)} = \phi \\ 0, & \text{otherwise} \end{cases}$$

Thus we have

$$z^*_S(f,b) = \sum_\phi \mathcal{Y}_{\phi,b}.$$

For any fixed ϕ, we can lower bound $\mathbb{E}[\mathcal{Y}_{\phi,b}]$ as follows using the fact that $(1+x)^n \leq \frac{1}{1-nx}$ for $x \in [-1,0]$, $n \in \mathbb{N}$.

$$\mathbb{E}[\mathcal{Y}_{\phi,b}] = 1 - (1 - 2^{-2^{|S|}})^{2^{n|\overline{S}|}} \geq 1 - \frac{1}{1 + 2^{n|\overline{S}| - 2^{|S|}}} = \frac{2^{n|\overline{S}|}}{2^{2^{|S|}} + 2^{n|\overline{S}|}}$$

Rewriting using linearity of expectation, we get

$$\mathbb{E}[z^*_S(f,b)] = \mathbb{E}[\sum_\phi \mathcal{Y}_{\phi,b}] = \sum_\phi \mathbb{E}[\mathcal{Y}_{\phi,b}] \geq 2^{2^{|S|}} \cdot \frac{2^{n|\overline{S}|}}{2^{2^{|S|}} + 2^{n|\overline{S}|}}.$$

Furthermore, we note that we can upper bound $\mathbb{E}[z^*_S(f,b)]$ by $2^{n|\overline{S}|}$, the number of ways to fix values for $\overline{S}$.

We can consider $z^*_S(f,b)$ as a doob martingale on the independent random variables $f_{S|(a,b)}$ for $a \in \{\{0,1\}^n\}^{\overline{S}}$. As $z^*_S(f,b)$ counts the number of distinct restrictions, changing $f_{S|(a,b)}$ for a single value of a changes $z^*_S(f,b)$ by at most 1. As a result, we can apply McDiarmid's inequality to get

$$\Pr_f[\mathbb{E}[z^*_S(f,b)] - z^*_S(f,b) \geq t] \leq \exp(\frac{-2t^2}{\mathbb{E}[z^*_S(f,b)]}).$$

Substituting our lower and upper bounds for $\mathbb{E}[z^*_S(f,b)]$ on the left and right, and using the fact that $2^{g^*_S(f)} \geq z^*_S(f,b) - 1$ for any choice of b by definition, we have

$$\Pr_f[2^{g^*_S(f)} \leq \frac{2^{2^{|S|}+n|\overline{S}|}}{2^{2^{|S|}} + 2^{n|\overline{S}|}} - t - 1] \leq \exp(\frac{-2t^2}{2^{n|\overline{S}|}}).$$

Finally, setting $|S| = \log_2(kn)$ and $t = 2^{kn/2}$ yields

$$\Pr_f[2^{g^*_S(f)} \leq \frac{2^{kn}}{2^{n\log_2(kn)} + 1} - 2^{kn/2} - 1] \leq \exp(-2N^{\log_2(kn)}).$$

Taking a union bound over $k/\log_2(kn)$ choices of S, it follows that $G^*(f) > \frac{k^2 n}{\log_2(kn)} - kn - 1$ for all but an exponentially small fraction of functions.

B On the Possibility of $\omega(k^2 n)$ PSM Lower Bounds

We conclude by observing that the existence of strong pseudo-random functions[6] (PRFs) with efficient PSM schemes would rule out the possibility of proving $\omega(k^2 n)$ lower bounds using a natural class of arguments. Specifically, if there exists an exponentially strong PRF that admits a PSM of size $O(k^2 n)$, an argument due to Razborov and Rudich rules out the possibility that any natural proof with sublinear-time constructivity can prove an $\omega(k^2 n)$ lower bound. We conjecture that a candidate PRF presented by Ball et al. [3] meets these requirements.

Ball et al. conjecture that taking the quadratic residue of the sum of an input with the secret key in prime fields is exponentially secure, if the input domain is slightly restricted.

▶ **Conjecture 16** ([3]). *Let $p(m)$ be a sequence of primes such that $p > 2^{2m+1}$, for all $m \in \mathbb{N}$. Let $f : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}$ denote the function,*

$$f : (k,x) \to (k+x+1)^{\frac{p-1}{2}} \qquad \textit{(where } k,x \textit{ are interpreted as integers.)}$$

Then, for some $s(m) = 2^{\Omega(m)}$, any size-$s(m)$ circuit can distinguish oracle access to either f_k where k is sampled uniformly from $\{0,1\}^m$ or a truly random function with advantage at most $2^{-s(m)}$.

[6] For definitions and further discussion on pseudo-random functions we refer the reader to [10].

▶ **Proposition 17.** *The DRE for f (with $m = kn/2$ and $p(m) \in (2^{2m+1}, 2^{2m+2}]$ as defined in Conjecture 16) outlined in [3] can be extended to give a PSM with size $O(k^2 n)$.*

Proof. The ith component of the DRE for f is

$$\hat{f}_i(x_i; s, r_1, \ldots, r_k) = s^2 \cdot (x_i \cdot 2^{i-1}) + r_i,$$

where s is sampled uniformly from $\mathbb{Z}_p^*$ and $r_1, \ldots, r_k$ are sampled uniformly from $\mathbb{Z}_p$ conditioned on the fact that $\sum r_i = 0$.

Note that $\sum \hat{f}_i(x_i; s, r) = s^2 \cdot x$. Consequently, if $f(x) = 1$ the sum is uniformly distributed over residues and if $f(x) = -1$ the sum is distributed over non-residues. Moreover, any sum of an incomplete subset of DRE components is uniform over $\mathbb{Z}_p$. Thus, in the PSM setting, k parties can consolidate the $\hat{f}_i$'s corresponding to their input into an $O(kn)$-bit message to create a PSM with size $O(k^2 n)$. ◀

We recall Razborov and Rudich's concept of natural proofs of explicit circuit lower bounds [14]. They observed that all known explicit circuit lower bounds proceeded by defining a natural combinatorial property, showing a certain complexity class cannot compute functions with such a property, and then exhibiting an explicit function that does have the property. Their ingenious contribution was to *formalize* the notion of a natural property P as a subset of all boolean functions with following properties:

1. (Largeness) A random function is in P with high probability.
2. (Constructivity) Given its truth table, it is possible to decide if a function is in P in polynomial time.
3. (Useful) P does not contain functions from the class one wishes to prove a lower bound against. For us, this means P does not contain functions with DREs of size $ck^2 n$ for any constant c (and large enough k, n).

The definition can be naturally extended to capture *sublinear-time*[7] natural properties. We note all examples of natural properties that we are aware of can be made to admit sublinear-time constructivity, including that of Applebaum et al. [1].

▶ **Definition 18.** *$\Pi = (\Pi_Y, \Pi_N)$ is a* natural property with sublinear-time constructivity, useful against a class C *if Π_Y, Π_N are disjoint subsets of boolean functions such that*

1. *(Largeness) A random n-bit function is in Π_Y with probability 2/3.*
2. *(Sublinear-Time Constructivity) The promise problem Π admits a randomized oracle machine, $A^{(\cdot)}$ that runs in time $o(2^n)$ such that*
   - *$f \in \Pi_Y \implies \Pr[A^f = 1] > 2/3$.*
   - *$f \in \Pi_N \implies \Pr[A^f = 0] > 2/3$.*
3. *(C-useful) $C \subseteq \Pi_N$.*

We now conjecture that the PRF candidate of Ball et al. is resilient to any *uniform* attack that runs in slightly less than exponential time.

▶ **Conjecture 19.** *Let $p(m)$ be a sequence of primes such that $p > 2^{2m+1}$, for all $m \in \mathbb{N}$. Let $f : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}$ denote the function,*

$$f : (k, x) \to (k + x + 1)^{\frac{p-1}{2}} \qquad \textit{(where } k, x \textit{ are interpreted as integers).}$$

[7] In this case "sublinear" refers to the size of the truth table of the function.

Then, any randomized oracle-algorithm A that runs in time $o(2^m)$ on input parameter 1^m cannot distinguish between f_k where $k \xleftarrow{u} \{0,1\}^m$ and a truly random function with non-negligible probability.

Following Razborov and Rudich's argument in this new setting yields the following proposition.

▶ **Proposition 20.** *If Conjecture 19 is true, then sublinear-time-natural proofs of size $\omega(k^2 n)$ PSM lower bounds do not exist.*

Proof. Suppose for contradiction the existence of a natural property Π with sublinear-time constructivity, useful against some class C containing functions that admit PSMs of size $O(k^2 n)$. As most random functions are contained in Π_Y, and our candidate PRF is contained in Π_N, we can distinguish our PRF candidate from random in time $o(2^n)$ using constructivity. This violates Conjecture 19. ◀