New bounds on private simultaneous quantum message passing

Uma Girish[1], Alex May[2,3], Natalie Parham[1], and Henry Yuen[1]

[1]Columbia University
[2]Perimeter Institute for Theoretical Physics
[3]Institute for Quantum Computing, University of Waterloo

In the private simultaneous message (PSM) setting, k players obtain inputs $x_i \in \{0,1\}^n$ and then independently send messages to a referee, who should learn $f(x_1, ..., x_k)$ but no other information about $(x_1, ..., x_k)$. The PSM setting was introduced as a minimal model for secure multiparty computation. In the quantum setting, PSM has been related to non-local quantum computation (NLQC), and has several connections to the complexity of Boolean functions. The communication and correlation cost of implementing private simultaneous message passing may be much larger than the cost without privacy, and the cost of privacy in this setting remains poorly understood. Here, we give new upper and lower bounds on the PSM model, in both the quantum and classical settings. Concretely, we prove two lower bounds:

- Nečiporuk's measure lower bounds the entanglement required for k-player quantum PSM with perfect correctness. This can be evaluated to give quadratic lower bounds for some explicit functions.
- The rank of the communication matrix of $f(x_1, x_2)$ lower bounds 2-player quantum PSM with perfect privacy but imperfect correctness. This implies a previously unknown lower bound on classical PSM with imperfect correctness.

When allowing both quantum communication and shared entanglement, these two bounds are the first lower bounds on quantum PSM that make use of the privacy condition. Regarding upper bounds, we show:

- Letting s be the size of a quantum circuit computing f, d_f be the circuit depth, k the number of players, n the number of bits received by each player, and ϵ the correctness parameter of the PSM protocol, we obtain the upper bound $\mathsf{PSM}^*_k(f) \leq (kn + s) \cdot \log^{O(d_f)}(s/\epsilon)$.
- The square of the Fourier 1 norm of f, $\|\hat{f}\|_1^2$, upper bounds the classical PSM complexity, $\mathsf{PSM}(f) \leq O(\|\hat{f}\|_1^2)$.

In proving the first upper bound, we also generalize existing T-depth based techniques for NLQC from 2 to $k \geq 2$ parties, and consider cases where the Clifford layers are restricted to having small light cones. These generalizations may be of independent interest.

Contents

1 Introduction **2**

Uma Girish: ug2150@columbia.edu
Alex May: amay@perimeterinstitute.ca
Natalie Parham: natalie@cs.columbia.edu
Henry Yuen: hyuen@cs.columbia.edu

1.1 Related work . . . 2
1.2 Our results . . . 4

2 Model definitions and quantum information tools **6**
2.1 Quantum information tools . . . 6
2.2 Communication models . . . 6

3 Lower bound from Nečiporuk's measure **8**
3.1 Nečiporuk's measure . . . 8
3.2 Lower bound from Nečiporuk's measure . . . 10

4 Rank lower bound **12**
4.1 Lower bound . . . 12
4.2 Comparison to related bounds . . . 14

5 Upper bound from T-depth and quantum circuits **14**
5.1 Computational models . . . 15
5.2 Speelman's instantaneous computation technique . . . 15
5.3 T-depth and circuit depth PSM_k^* upper bounds . . . 16

6 Upper bound from the Fourier 1 norm **19**
6.1 Fourier transform for Boolean functions and the Fourier one-norm . . . 19
6.2 Upper Bound . . . 19

A k-player instantaneous computations based on the T-depth **21**
A.1 The garden-hose model . . . 21
A.2 A garden-hose gadget . . . 22
A.3 Instantaneous k-party computations from T-depth . . . 24

B Newman's Theorem for PSM **28**

1 Introduction

What is the cost of information-theoretic privacy? This is a fundamental question in cryptography which reappears across many settings, and which is closely related to understanding the complexity of Boolean functions. In this work, we make progress on understanding this problem in both the classical and quantum settings by giving several new upper and lower bounds on the private simultaneous message (PSM) model [1, 2].

The PSM setting is illustrated in Figure 1. The setting involves k parties, who we label player 1, player 2, etc, and a referee. Player i receives input $x_i \in \{0,1\}^n$. All parties including the referee agree in advance on a choice of Boolean function $f : \{0,1\}^{kn} \to \{0,1\}$. Classically, the players share randomness that is inaccessible to the referee, and send classical messages to the referee. The goal is for the referee to compute $f(x_1, ..., x_k)$ without learning anything further about the value of $(x_1, ..., x_k)$. We consider this model in both quantum and classical variants. When $n = 1$, so that each of k players receives a single bit of input, this setting is also an example of a *decomposable randomized encoding*. Another special case we often consider fixes $k = 2$.

1.1 Related work

The PSM model was introduced in a classical context in [1] as a simple toy model for secure multi-party computation. Since then, several applications and connections to other primitives in cryptography have appeared [2].

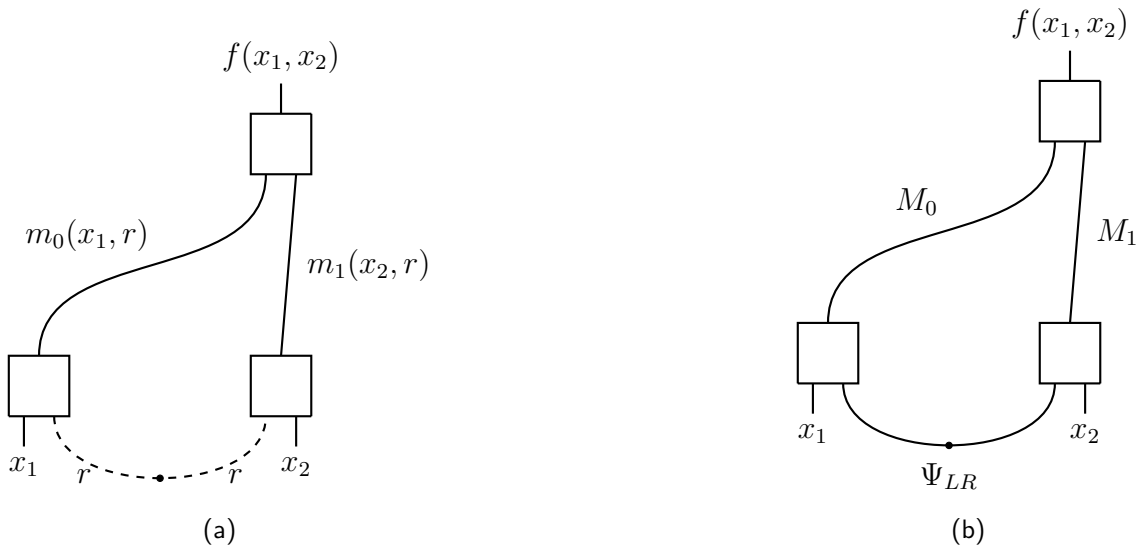


Figure 1: A private simultaneous message protocol (PSM). We show the case with two players for simplicity, but in general we consider $k \geq 2$ players. Players 1 and 2 do not communicate. Player i holds input $x_i \in \{0,1\}^n$. The referee should be able to learn $f(x_1, ..., x_k)$ but nothing else about $(x_1, ..., x_k)$. a) In the classical setting, the players share a random string r and send classical messages to the referee. b) In the quantum setting the randomness is replaced with an entangled state Ψ_{LR}, and the messages can be quantum.

The definition of PSM is information-theoretic and does not refer to complexity theory. Nonetheless, a relationship between PSM and complexity emerges: known protocols for implementing PSM have a communication and randomness cost set by the complexity of the function f. For instance, in [1] an efficient protocol for functions in NL was given, based on a reduction to a PSM protocol for group products. This was improved in [2] to give efficient protocols for functions in $\mathsf{Mod}_p\mathsf{L}$[1] as well as other 'counting' variants of log-space classes.

Without the privacy condition, PSM complexity would be at most linear, since Alice and Bob can simply send their inputs to the referee. Meanwhile, most notions of Boolean function complexity can be as large as exponential, so it is clear that without privacy PSM complexity and Boolean function complexity can only be loosely related. With privacy however, the relationship may be much tighter. Better understanding the relationship between privacy and the complexity of Boolean functions is one motivation for studying the cost of privacy in PSM.

Only a few lower bound techniques that make use of the privacy condition are known for PSM. In the classical setting, one such technique was proposed in [1] and then corrected in [3]. This technique, when we have $k = 2$ players, gives a lower bound in terms of a condition on rectangles in the communication matrix for f; for random functions, it leads to a $3n - o(1)$ lower bound. This can be seen to make non-trivial use of privacy in that without privacy, the cost is at most $2n$, the total input length.

In the classical context, a lower bound on k-party PSM was proven in [4, 5]. This lower bound is in terms of Nečiporuk's measure, an object previously known to lower bound formula size for Boolean functions. Concretely, [4, 5] prove that for perfectly correct and perfectly secure PSM,

$$\mathsf{PSM}(f) \geq \frac{1}{2} G^*(f) \tag{1}$$

where $G^*(f)$ is Nečiporuk's measure. A similar bound holds with perfect security relaxed. Heuristically, Nečiporuk's measure can be understood as the logarithm of the number of

[1] $\mathsf{Mod}_p\mathsf{L}$ contains NL, and this containment is believed to be strict.

distinct functions that appear when fixing subsets of the variables. In more detail, we sum over a partition of the variables and consider the number of distinct functions that arise when fixing all but the variables in the current subset of the partition. For some explicit functions on k inputs each of length n, Nečiporuk's measure evaluates to $\frac{k^2 n}{2\log(kn)}$, so when (for instance) $n = 1$, this is a nearly quadratic lower bound. This bound also necessarily uses privacy, since it is super-linear.

Recently [6, 7] a new perspective on PSM and related primitives has emerged, which considers quantum variants of these settings. This provides a new setting in which to explore the relationship between privacy, complexity, and communication cost. In [6], quantum PSM was first studied. In that context, with $k = 2$ players, a lower bound of $3n - o(1)$ for random functions was proven in the context of quantum communication but restricting to classical shared randomness. In [6] it was shown that for some relations, communication cost in PSM can be exponentially smaller when allowing shared entanglement; this was later proven for a partial function in [8].

Quantum PSM exhibits a relationship between privacy and notions of quantum complexity. In particular, in [7] it was pointed out that communication and entanglement cost in PSM with shared entanglement allowed is upper bounded in terms of the T-depth of any unitary that computes the relevant Boolean function. Later [9], similar techniques were used to observe that certain communication complexity protocols can be transformed into PSM protocols. In particular, let $\mathsf{PSM}^*(f)$ denote the communication cost of PSM when allowing shared entanglement but restricting to classical messages, and let $\mathsf{Q}\|^*$ be the communication cost in the simultaneous message model, allowing quantum communication and shared entanglement. Then [9] showed that

$$\mathsf{PSM}^*(f) \leq (\mathsf{Q}\|^*(f) + a)^{d_T} \tag{2}$$

where d_T is the T-depth of the unitary applied by the referee in the $\mathsf{Q}\|^*$ protocol, and a is the number of qubits of ancilla used by the referee. In practice, this leads to new efficient PSM* protocols constructed from existing $\mathsf{Q}\|^*$ protocols in several interesting cases, and in particular leads to new separations between communication complexity classes. Furthermore, this shows that a separation between PSM^* and $\mathsf{Q}\|^*$ implies a T-depth lower bound.

1.2 Our results

We contribute to the understanding of the cost of privacy in quantum and classical PSM by proving two new lower bounds on entanglement cost, and two new upper bounds. One of each of our lower and upper bounds is new to even classical PSM. Our lower bounds are the first lower bounds on fully quantum PSM which make use of the privacy condition, where by fully quantum we mean that both entanglement and quantum communication are allowed. Previously, lower bounds that used privacy only applied to the case where the messages are quantum, but no shared entanglement is allowed [6].

Our first lower bound is in terms of the rank of the communication matrix of the target function f, and applies to two player quantum PSM,

$$\boxed{\mathsf{pp}\overline{\mathsf{PSQM}}^*(f) \geq \frac{1}{4}\log \operatorname{rank} f - \frac{1}{4}.} \tag{3}$$

Here, the left hand side denotes the entanglement cost of fully quantum PSM (allowing entanglement and quantum messages), and requiring perfect privacy. The communication matrix M_f of f is a $2^n \times 2^n$ matrix with entries $f(x, y)$. We compute the rank over the complex numbers. Notice that this lower bound follows without using privacy if we assume perfect correctness, because quantum communication complexity with

perfect correctness is lower bounded by the log-rank [10]. Our result holds with imperfect correctness however, and relies instead on the perfect privacy condition. Because $\mathsf{pp}\overline{\mathsf{PSM}}(f) \geq \mathsf{pp}\overline{\mathsf{PSQM}}^*(f)$, we obtain the same lower bound on perfectly private classical PSM. This result appears to be new to the classical setting, but is proven from the quantum perspective.

Our second lower bound applies to k-player quantum PSM, with perfect correctness. Then, denoting the total entanglement shared among all players by $\mathsf{pc}\overline{\mathsf{PSQM}}^*_k(f)$, we find that

$$\boxed{\mathsf{pc}\overline{\mathsf{PSQM}}^*_k(f) \geq \frac{1}{2}\alpha_\delta G^*(f) - \beta_\delta.} \tag{4}$$

Here the object $G^*(f)$ appearing in the lower bound is *Nečiporuk's measure*, and the $\alpha_\delta, \beta_\delta$ are functions of the security parameter δ for the protocol. Because Nečiporuk's measure can be quadratic in k, and hence larger than the input size, it is clear that this bound also relies on the privacy condition.

For upper bounds, we prove two new results. First, we prove an upper bound in the k player setting based on a Clifford+T decomposition of any circuit computing the function f. We find the upper bound

$$\mathsf{PSM}^*_k(f) \leq O((K\ell)^{d_T - 1} \cdot kn \cdot \min\{k, \ell\}) \tag{5}$$

where d_T is the T-depth of the circuit computing f, k is the number of players, n is the number of input bits per player, and ℓ measures how much any single Clifford layer spreads the support of an operator. This result generalizes the T-depth upper bound of [11], to allow for $k > 2$ players and restricted Clifford layers.

As an application of this upper bound, we show that functions with low-depth quantum circuits [12] can be computed efficiently in the PSM^* model. In particular, we consider circuits with gates that only act on a constant number of qubits. Letting d_f be the minimal depth of any quantum circuit computing f, we find

$$\boxed{\mathsf{PSM}^*_k(f) \leq (kn + s) \cdot \log^{O(d_f)}(s/\epsilon).} \tag{6}$$

Thus we find that functions computable in depth $\log(nk)/\log\log(nk)$ can be computed by a polynomial-cost PSM^*_k protocol. It is interesting to compare this with the classical seting: a combination of Barrington's theorem [13] and the PSM construction of [1] for branching programs implies that there are polynomial-cost classical PSM protocols for all functions computable by logarithmic-depth (classical) circuits. We leave it as an interesting open question of improving our bound to get polynomial-cost PSM^* protocols for quantum circuits with depth $\Omega(\log n)$.

Our second upper bound is in terms of the Fourier 1 norm of f, denoted $\|\hat{f}\|_1$. Recall that we define the Fourier transform of f by defining functions $\chi_S(x) = (-1)^{S \cdot x}$ where S labels a subset of the bits of x, and then expressing $f(x)$ as

$$f(x) = \sum_S \hat{f}(S)\chi_S(x). \tag{7}$$

The Fourier 1 norm is then

$$\|\hat{f}\|_1 = \sum_S |\hat{f}(S)|. \tag{8}$$

The Fourier 1 norm appears in several contexts [14]; most relevantly [15] proved a $O(\|\hat{f}\|_1^2)$ upper bound on the simultaneous message passing (SMP) model (which is the same as PSM, but without privacy imposed). This was then used to prove a number of circuit

lower bounds. We upgrade this upper bound on the SMP model to the PSM model, proving

$$\boxed{\mathsf{PSM}(f) \leq O(\|\hat{f}\|_1^2).} \tag{9}$$

It may be interesting to explore applications of this upper bound to proving circuit lower bounds.

Acknowledgments. Research at the Perimeter Institute is supported by the Government of Canada through the Department of Innovation, Science and Industry Canada and by the Province of Ontario through the Ministry of Colleges and Universities. UG, NP, and HY are supported by AFOSR award FA9550-23-1-0363, NSF awards CCF-2530159, CCF-2144219, and CCF-2329939, and by the Sloan Foundation. NP is supported by the Google PhD Fellowship.

2 Model definitions and quantum information tools

2.1 Quantum information tools

Unless otherwise noted, by log we always mean the base 2 logarithm. We define the von Neumann entropy by

$$S(A)_\rho = -\operatorname{tr}(\rho_A \log \rho_A). \tag{10}$$

We define the mutual information as

$$I(A:B)_\rho = S(A)_\rho + S(B)_\rho - S(AB)_\rho. \tag{11}$$

We make use of the following continuity property of the mutual information, which follows from the Alicki-Fannes-Winter inequality [16, 17].

Theorem 1 *Suppose that* $||\sigma - \rho||_1 \leq 2\epsilon$, *and define*

$$h(\epsilon) = (\epsilon + 1)\log(\epsilon + 1) - \epsilon \log \epsilon. \tag{12}$$

Then

$$|I(A:B)_\sigma - I(A:B)_\rho| \leq 3\epsilon \log d_A + 2h(\epsilon). \tag{13}$$

2.2 Communication models

In this section we define the relevant classical and quantum communication models. In all cases we are interested in the simultaneous message passing scenario, so that the communication pattern allows only for the players to send messages to a referee. The models we consider can then be divided into models without privacy, and those with privacy. We begin by defining the non-private models.

Definition 2 *Let* $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ *be a (partial or total) Boolean function, and* $\epsilon \in [0,1]$ *be a parameter. A* ***simultaneous message passing*** *protocol* P *for* f *involves three parties, Alice, Bob, and a referee. Alice receives* $x \in \{0,1\}^n$ *as input and Bob receives* $y \in \{0,1\}^n$. *Alice and Bob send the referee (quantum or classical) message systems* M_A *and* M_B *respectively, and the referee subsequently outputs a bit* $c = P(x,y)$.

Messages. *The messages that Alice and Bob send to the referee can be quantum, denoted by* $\mathsf{Q}\|$ *or classical, denoted by* $\mathsf{R}\|$.

Correctness. *The protocol is ϵ-correct if for all (x, y) in the support of f,*

$$\Pr[P(x, y) = f(x, y)] \geq 1 - \epsilon \ .$$

By default we assume $\epsilon = 1/3$. Focusing on the case when Alice and Bob send classical messages and $\epsilon = 0$, we obtain the deterministic model of classical simultaneous communication, denoted by $\mathsf{D}\|$.

Cost of a protocol. *The cost of the protocol denoted by $\mathrm{cost}(P)$ is defined to be the total number of bits (resp. qubits) sent by Alice and Bob in the $\mathsf{R}\|$ (resp. $\mathsf{Q}\|$) model. The $\mathsf{R}\|_\epsilon$ complexity of f is defined as follows*

$$\mathsf{R}\|_\epsilon(f) = \min_{P:P \text{ is } \epsilon\text{-correct}} \mathrm{cost}(P)$$

and the $\mathsf{Q}\|_\epsilon$ complexity is analogously defined.

Randomness. *Alice and Bob typically have private randomness, but we also consider a variation of the simultaneous message model where we allow public randomness. In particular, we allow all three players (Alice, Bob and the referee) to hold a shared random string r of arbitrary length. They can then use r as an input to their local operations. We label the cost to compute f ϵ-correctly in this model by $\mathsf{R}\|_\epsilon^{\mathsf{pub}}(f)$ (resp. $\mathsf{Q}\|_\epsilon^{\mathsf{pub}}(f)$) when the messages are classical (resp. quantum).*

Entanglement. *We may allow Alice and Bob to share entanglement, denoted by the superscript $*$ and resulting in the models $\mathsf{Q}\|^*$ and $\mathsf{R}\|^*$ depending on whether the messages to the referee are quantum or classical.*

Next we take up the private variations of these models.

Definition 3 *A **private simultaneous message** task is defined by a choice of (partial or total) Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Let $\epsilon, \delta \in [0,1]$ be parameters. The inputs to the task are n-bit strings x and y given to Alice and Bob, respectively. Alice then sends a message system M_0 to the referee, and Bob sends a message system M_1. From the combined message system $M = M_0M_1$, the referee prepares an output bit z whose system is denoted by Z. We require the task be completed in a way that satisfies the following two properties.*

- *ϵ-**correctness:** There exists a decoding map $\boldsymbol{\mathcal{V}}_{M\to Z}$ such that, for all (x, y) in the support of f,*

$$\left\| \boldsymbol{\mathcal{V}}_{M\to Z} \left(\rho_M(x, y)\right) - |f_{x,y}\rangle\langle f_{x,y}|_Z \right\|_1 \leq \epsilon \tag{14}$$

  where $\rho_M(x, y)$ is the density matrix on M produced on inputs x, y and $f_{x,y} = f(x, y)$.

- *δ-**security:** There exists a simulator, which is a quantum channel $\boldsymbol{\mathcal{S}}_{Z\to M}(\cdot)$, such that for all (x, y) on which f is defined*

$$\left\| \rho_M(x, y) - \boldsymbol{\mathcal{S}}_{Z\to M}(|f_{x,y}\rangle\langle f_{x,y}|_Z) \right\|_1 \leq \delta. \tag{15}$$

  Stated differently, the state of the message systems is δ-close to one that depends only on the function value, for every choice of input.

Messages. *When the messages are quantum, we will refer to this model as PSQM and when the messages are classical, we refer to the model by PSM.*

Entanglement. *When Alice and Bob share entanglement, we denote it by the superscript $*$, obtaining the model PSQM^* when Alice and Bob send quantum messages and PSM^* when Alice and Bob send classical messages.*

Communication cost of a protocol. *The communication cost of the protocol is defined to be the total number of bits sent by Alice and Bob in the PSM or PSM^* models.*

We denote the minimal cost over all $\epsilon = 1/3$ correct, $\delta = 1/3$ secure protocols by $\mathsf{PSM}(f)$ *or* $\mathsf{PSM}^*(f)$. *The communication cost measures* $\mathsf{PSQM}(f)$ *and* $\mathsf{PSQM}^*(f)$ *are defined similarly, now counting qubits of communication.*

Correlation cost of a protocol. *The correlation cost of the protocol is defined to be the log dimension of the quantum state shared among Alice and Bob at the start of the protocol, which counts both classical randomness and shared entanglement. We use an overline to denote the correlation cost in various models,* $\overline{\mathsf{PSM}}(f)$, $\overline{\mathsf{PSQM}}(f)$, *etc.*

If we enforce that the protocol is perfectly correct we add the suffix pc; if we enforce that the protocol is perfectly private we add pp. Thus for example the communication cost of perfectly correct PSQM* protocol for function f is $\mathsf{pcPSQM}^*(f)$.

We also consider PSM settings where the input is split among k parties, rather than two. The definition is similar to the above, but we replace the input space $X \times Y$ with $X_1 \times ... \times X_k$, and have messages computed separately from each of the inputs. In this case we add a subscript k to the model designation, for instance PSQM_k^* is k-player PSM with quantum communication and shared entanglement. The k players may share a k-partite entangled state. To define the entanglement cost in this case, suppose that a protocol uses resource state $\Psi_{E_1E_2...E_k}$. Then we define the correlation cost to be the log dimension of this state. Note that we allow arbitrary isometries in the PSQM* protocol, so the correlation cost measure doesn't count any ancilla used.

3 Lower bound from Nečiporuk's measure

In this section we develop a lower bound technique on correlation cost in the PSQM* model, in the setting where we give each of k parties n bits of the input. We start by developing the definition of Nečiporuk's measure, which counts the number of distinct functions that appear when restricting a given function to a subset of its inputs. Our strategy is adapted from an analogous classical setting [5].

3.1 Nečiporuk's measure

The variant of Nečiporuk's measure that appears in our lower bounds involves the following notion of a restriction of a k input function.

Definition 4 ***(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*

$$f_{S|(\alpha,\beta)} : \{0,1\}^{|S|} \to \{0,1\} \tag{16}$$

defined by restricting the inputs as follows:

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

Now we can define the modified Nečiporuk's measure.

Definition 5 ***(Modified Nečiporuk's measure)*** *Let $f : \{\{0,1\}^n\}^k \to \{0,1\}$ be a function. For any subset $S \subseteq [k]$, define*

$$g_S^*(f) := \max_{\beta \in \{\{0,1\}^{n-1}\}^{|S|}} \log |\{f_{S|(\alpha,\beta)} : \alpha \in \{\{0,1\}^n\}^{|\bar{S}|}, f_{S|(\alpha,\beta)} \not\equiv 0\}|. \tag{17}$$

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

We will eventually prove a lower bound on the k party PSQM* complexity in terms of the Nečiporuk measure. First, we need the following claim, which restricts the number of orthogonal states on the AB Hilbert space assuming that all of the density matrices on B (nearly) agree.

Lemma 6 *Call d_X the number of states $\{\rho^i_{AB}\}_i$ satisfying*

$$F(\rho^i_{AB}, \rho^j_{AB}) = \delta_{ij} \quad \textit{and} \quad \|\rho^i_B - \rho_B\|_1 \leq \delta \tag{18}$$

with ρ_B a single fixed state. Then

$$\log d_X \leq \frac{1}{1 - 3\delta/2} \left[2 \log d_A + 2h(\delta/2)\right]. \tag{19}$$

where $h(x) = (1+x)\log(1+x) - x \log x$.

Proof. Consider the states

$$\begin{aligned} \sigma_{XAB} &= \frac{1}{d_X} \sum_{i=1}^{d_X} |i\rangle\langle i|_X \otimes \rho^i_{AB} \\ \tilde{\sigma}_{XB} &= \frac{1}{d_X} \sum_{i=1}^{d_X} |i\rangle\langle i|_X \otimes \rho_B \end{aligned} \tag{20}$$

Then we have

$$\|\sigma_{XB} - \tilde{\sigma}_{XB}\|_1 = \frac{1}{d_X} \sum_i \|\rho^i_B - \rho_B\|_1 \leq \delta \tag{21}$$

Using Theorem 1 and that $I(X:B)_{\tilde{\sigma}} = 0$, we can bound the mutual information $I(X:B)_\sigma$,

$$I(X:B)_\sigma = I(X:B)_\sigma - I(X:B)_{\tilde{\sigma}} \leq \frac{3}{2}\delta \log d_X + 2h(\delta/2). \tag{22}$$

But also, since the ρ^i_{AB} all have orthogonal support, we can measure AB and determine i so then also $I(AB:X) = \log d_X$. But then we use

$$\begin{aligned} \log d_X &= I(AB:X)_\sigma \\ &= I(A:X|B)_\sigma + I(B:X)_\sigma \\ &\leq 2S(A)_\sigma + I(B:X)_\sigma \\ &\leq 2S(A) + \frac{3}{2}\delta \log d_X + 2h(\delta/2) \\ &\leq 2\log d_A + \frac{3}{2}\delta \log d_X + 2h(\delta/2) \end{aligned} \tag{23}$$

which can be re-arranged to the desired inequality. ∎

For intuition, consider the case where $\delta = 0$ and A, B are both qubits. Then the bound says that any set of orthogonal states on AB which all have the same marginal on A must be of size at most 4. We can saturate this bound by for instance choosing the four Bell states on AB, which are orthogonal but all have $\rho_B = \mathcal{I}_B/2$.

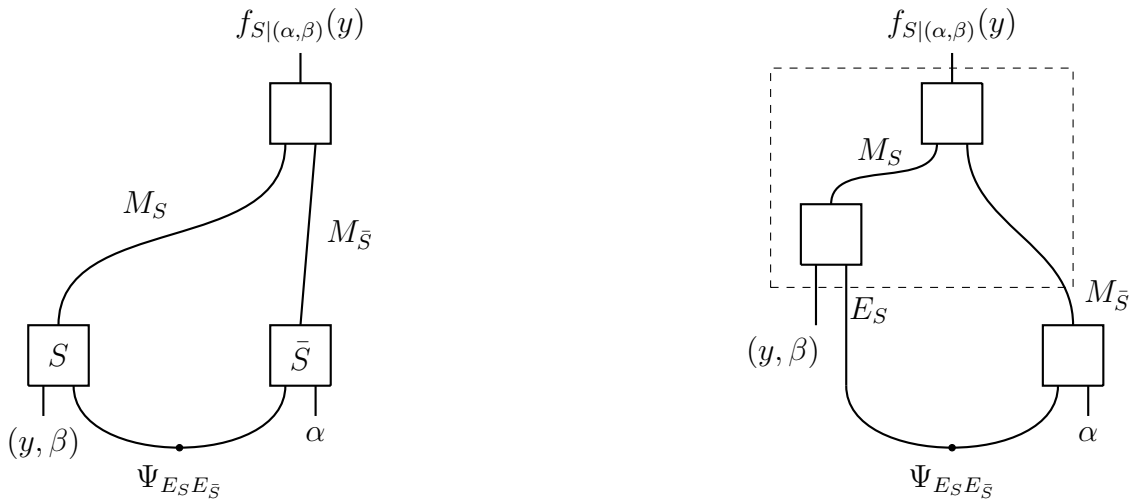


Figure 2: a) A PSQM* protocol. The n players have been divided into two subsets, S and $\bar{S}$. The input to the $\bar{S}$ players is set to α. The last $n-1$ bits of each of the players in S is set to β, while the first bit inputs are free, and the players can choose any string y to take as input. Correctness of the PSQM* protocol gives that the referee can compute $f_{S|(\alpha,\beta)}(y)$ from the message systems M_S, $M_{\bar{S}}$. b) In the proof of Theorem 7, we observe that given $E_S M_{\bar{S}}$, $f_{S|(\alpha,\beta)}(y)$ can be computed for any value of y. By computing this reversibly, this can be repeated for all values of y. This means the function $f_{S|(\alpha,\beta)}$ is determined by $E_S M_{\bar{S}}$.

3.2 Lower bound from Nečiporuk's measure

Finally, we are ready to prove the quantum PSM lower bound. The overall strategy is as follows. We partition the inputs into S and $\bar{S}$. The inputs to $\bar{S}$ are fixed to a string $\alpha \in \{\{0,1\}^n\}^{|\bar{S}|}$. The last $n-1$ bits of each input to the players in S is fixed to $\beta \in \{\{0,1\}^{(n-1)}\}^{|S|}$, while the remaining inputs are taken to be $y \in \{0,1\}^{|S|}$. We observe that the message $M_{\bar{S}}$ from players in $\bar{S}$, along with the initial entanglement on players in S, call it E_S, can be used to compute $f_{S|(\alpha,\beta)}(y)$ for any choice of y. See Figure 2. Further, when the protocol is perfectly correct, we can copy out the value of y, uncompute, and run forward again with a new choice of input. Thus in fact the state on $S\bar{S}$ determines all values of $f_{S|(\alpha,\beta)}$ and hence determines α. Naively, that means $E_S M_{\bar{S}}$ needs to have a dimension lower bounded by the number of distinct functions. Alone, this isn't strong enough to get our bound, and instead we want to lower bound the dimension of E_S alone. To achieve this, we use security to show that all the states on $E_S M_{\bar{S}}$ have density matrices that agree on $M_{\bar{S}}$, and then apply Lemma 6 to bound the dimension of E_S alone.

Theorem 7 *Consider a perfectly correct PSQM* protocol for function f with security parameter $\delta > 0$. Then, the correlation cost is lower bounded by*

$$\mathsf{pc}\overline{\mathsf{PSQM}}^*(f) \geq \frac{1}{2}(1-3\delta/2)G^*(f) - h(\delta/2)p \tag{24}$$

where p is the number of subsets in the partition V^* that maximizes the sum $\sum_{V_i \in V} g^*_{V_i}(f)$.

Proof. Consider a subset of players S and the complement set $\bar{S}$. Considering the modified Nečiporuk measure, fix β to its maximizing value. Then choose a set of distinct α that each lead to distinct first-bit restrictions $f_{S|(\alpha,\beta)}$. Denote the remaining inputs to $f_{S|(\alpha,\beta)}$ as y. Let the message system sent by S be M_S, and the message system sent by $\bar{S}$ be $M_{\bar{S}}$. Similarly, let the entangled resource systems held by S and $\bar{S}$, before they act with their local operators, be E_S and $E_{\bar{S}}$ respectively.

We claim that all the possible message density matrices (for each distinct input y) agree on $M_{\bar{S}}$, up to an error set by δ. This is because for all α, α' the functions we get

by restriction are still non-zero by assumption, so there exist choices of y, y' such that $f_{S|(\alpha,\beta)}(y) = f_{S|(\alpha',\beta)}(y')$, so then by privacy

$$\|\rho_{M_S M_{\bar{S}}}(y,\alpha,\beta) - \rho_{M_S M_{\bar{S}}}(y',\alpha',\beta)\|_1 \leq \delta. \tag{25}$$

But by causality the reduced density matrix on $M_{\bar{S}}$ can't depend on y, so we get

$$\|\rho_{M_{\bar{S}}}(\alpha) - \rho_{M_{\bar{S}}}(\alpha')\|_1 \leq \delta \tag{26}$$

as claimed. Define $\rho_{M_{\bar{S}}}(\alpha_0) \equiv \rho_{M_{\bar{S}}}$ for some fixed α_0, so all $\rho_{M_{\bar{S}}}(\alpha)$ are δ close to a fixed density matrix.

Next, we show that α can be determined from $E_S M_{\bar{S}}$, in other words we show that $F(\rho_{E_S M_{\bar{S}}}(\alpha,\beta), \rho_{E_S M_{\bar{S}}}(\alpha',\beta)) = \delta_{\alpha,\alpha'}$. To see this, consider a unitary extension of the operations of each of the S players acting on E_S and input I, followed by the referee's operations, to define a single unitary taking in $E_S M_{\bar{S}}$ and a copy of the inputs and producing

$$U_{IE_S M_{\bar{S}} \to \mathcal{O}R}(|y\rangle\langle y|_I \otimes \rho_{E_S M_{\bar{S}}}) U^\dagger_{IE_S M_{\bar{S}} \to \mathcal{O}R} = \left|f_{S|(\alpha,\beta)}(y)\right\rangle\!\left\langle f_{S|(\alpha,\beta)}(y)\right|_{\mathcal{O}} \otimes \sigma_R \tag{27}$$

for some state σ_R. We can CNOT the value of $f_{S|(\alpha,\beta)}(y)$ into a separate register, then invert the unitary to get what we started with. We then pick a new value of y and repeat. In this way we can determine the truth table of $f_{S|(\alpha,\beta)}$. Since there is just one α that leads to $f_{S|(\alpha,\beta)}$ by assumption, this determines α as needed. Since the α can be perfectly distinguished, we have $F(\rho_{E_S M_{\bar{S}}}(\alpha,\beta), \rho_{E_S M_{\bar{S}}}(\alpha',\beta)) = \delta_{\alpha,\alpha'}$ as claimed.

Now, we apply Lemma 6. In our setting, d_X is the total number of choices of α, so $\log d_X$ is $g^*_S(f)$. Thus we obtain

$$\frac{1}{2}(1 - 3\delta/2) g^*_S(f) - h(\delta/2) \leq n_{E_S}. \tag{28}$$

We find that the entanglement held by S must consist of at least $g^*_S(f)/2$ qubits, up to a multiplicative factor which is close to 1, and a small additive term. Then we consider a partition $V = (V_1, ..., V_m)$, use the above for each V_i, sum over the V_i, and optimize over partitions to get a lower bound in terms of $G^*(f)$. Doing so leads to the claimed lower bound. ■

We also remark that if PSQM^* protocols can be amplified, then the above lower bound technique can be adapted to apply to imperfectly correct protocols. To see why, suppose the PSQM^* protocol can be amplified in the sense that, with a factor of ℓ overhead in resources, we have $\epsilon \to 2^{-\ell}\epsilon$, and further that the security parameter is not increased by the amplification procedure. Then, we can consider a similar construction as used above, now applied to the amplified protocol. A complication arises when the referee wishes to determine α from $E_S M_{\bar{S}}$. To do so, they compute $f_{S|(\alpha,\beta)}(y)$ for a given value of y, measure the output qubit and store the value of $f_{S|(\alpha,\beta)}(y)$, then reverse the procedure to try and return to the initial state on $E_S M_{\bar{S}}$. With perfect correctness the measurement returns $f_{S|(\alpha,\beta)}(y)$ with probability 1 and doesn't change the state, so that the initial state on $E_S M_{\bar{S}}$ is reproduced perfectly. Repeating, the referee learns all the values $\{f_{S|(\alpha,\beta)}(y)\}_y$ correctly with probability 1. To ensure this works with probability of order 1 when the protocol is imperfectly correct, we need that each measurement fails to return $f_{S|(\alpha,\beta)}(y)$ with probability at most $2^{-|S|}$. Thus in the amplification step we should choose $k = \Theta(|S|)$. This means our lower bound is weakened by a factor of $|S|$, becoming,

$$n_{E_S} \gtrsim g^*_S(f)/|S|. \tag{29}$$

Thus on the total dimension of the entangled state we obtain a lower bound of $G^*(f)/\max_i |S_i|$ where the $\{S_i\}_i$ are the subsets in the optimizing partition used in computing $G^*(f)$.

Many functions have large Nečiporuk measure, and explicit functions can be identified with large Nečiporuk measure as well. A review of this can be found in [5]. To summarize briefly, we have that all functions have Nečiporuk measure bounded by

$$G^*(f) \leq \frac{k^2 n}{\log(kn)}. \tag{30}$$

Further, random functions nearly saturate this bound with high probability. Considering explicit functions, the (n, k) set disjointness function ($DISJ_{n,k}$) and first-bit indirect storage access ($FISA_{n,k}$) function[2] have

$$G^*(f) = \Omega\left(\frac{n^2 k}{\log(kn)}\right) \tag{31}$$

which saturates the upper bound on G^*. For these functions we obtain quadratic lower bounds on the entanglement cost of perfectly correct PSQM.

4 Rank lower bound

We will give a lower bound strategy based on the rank of the communication matrix for the function $f(x, y)$. This technique will only apply to the case where the PSM protocol is perfectly secure, but correctness errors are allowed. This is similar to a technique given in [18], which deals with the related (quantum) CDS primitive [7, 19, 20], but for quantum PSM the technique gives a stronger bound. In this section we deal with 2-player PSM, but note that for k-players we can apply the technique to any partition of the players into two subsets.

4.1 Lower bound

In this section we prove the rank lower bound on perfectly private PSM.

Theorem 8 *Consider an ϵ-correct, perfectly secure 2 party $PSQM^*$ protocol for the function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Then*

$$\mathsf{pp}\overline{\mathsf{PSQM}}^*(f) \geq \frac{1}{4} \log \operatorname{rank} f - \frac{1}{4} \tag{32}$$

where $\operatorname{rank}(f)$ *denotes the rank of the communication matrix for f, computed over the complex numbers.*

Proof. Consider a PSQM* protocol. Let the density matrix describing the message systems $M_A M_B = M$ be denoted $\rho_M(x, y)$. For a perfectly secure PSQM protocol, there are just two possible density matrices that can be realized for different values of (x, y); a 0 density matrix or a 1 density matrix,

$$\begin{aligned} \rho_M(x, y) &= \rho_0 \quad \text{if} \quad f(x, y) = 0, \\ \rho_M(x, y) &= \rho_1 \quad \text{if} \quad f(x, y) = 1. \end{aligned} \tag{33}$$

This follows because if $\rho(x, y) \neq \rho(x', y')$, the referee has some probability of distinguishing between (x, y) and (x', y'), which shouldn't be the case if $f(x, y) = f(x', y')$.

This lets us express $f(x, y)$ using the matrix valued function $\rho(x, y)$, in particular define

$$\alpha = \operatorname{tr}\left((\rho_1 - \rho_0)^2\right) = \|\rho_1 - \rho_0\|_2^2. \tag{34}$$

[2] See [5], section 4 for definitions of these functions.

This is non-zero, because by correctness it must be the case that $\rho_0 \neq \rho_1$. Then we can notice

$$f(x,y) = \frac{1}{\alpha} \operatorname{tr}(\rho(x,y) - \rho_0)^2. \tag{35}$$

To see why the above holds, note that when $f(x,y) = 1$ we have $\rho(x,y) = \rho_1$, so the right hand side is 1 as needed. Meanwhile, if $f(x,y) = 0$ then $\rho(x,y) = \rho_0$ so the above is 0, as needed.

Next, we use an expression for $\rho(x,y)$ that is constrained by the amount of entanglement used in the protocol. Suppose that the resource state used in the protocol is $\Psi_{L'R}$, and purify this to

$$|\Psi\rangle_{LR} = \sum_{i=1}^{r} \sqrt{\lambda_i} \, |i\rangle_L \, |i\rangle_R \, . \tag{36}$$

We will lower bound the log-dimension of the purified state, which never need be larger than twice the unpurified log-dimension. Thus beginning with a mixed state and purifying will loosen our bound by at most a factor of 1/2.

The mid-protocol density matrix $\rho_{M_A M_B}(x,y)$ is produced by Alice and Bob acting separately on each end of the entangled state, so is of the form

$$\begin{aligned}
\rho_{M_A M_B}(x,y) &= \sum_{i,j=1}^{r} \sqrt{\lambda_i \lambda_j} \mathcal{N}^x_{L \to M_A}(|i\rangle\langle j|) \otimes \mathcal{N}^y_{R \to M_B}(|i\rangle\langle j|) \\
&= \sum_{i,j=1}^{r} A^{i,j}_{M_A}(x) \otimes B^{i,j}_{M_B}(y) \\
&= \sum_{I=1}^{r^2} A^I_{M_A}(x) \otimes B^I_{M_B}(y).
\end{aligned} \tag{37}$$

The second line defines the matrices $A^{i,j}_{M_A}(x), B^{i,j}_{M_B}(y)$. Pick any input (x_0, y_0) with $f(x_0, y_0) = 0$. Then

$$\rho_0 = \sum_{I=1}^{r^2} A^I_{M_A}(x_0) \otimes B^I_{M_B}(y_0) \tag{38}$$

and we can write $f(x,y)$ as

$$\begin{aligned}
f(x,y) &= \frac{1}{\alpha} \operatorname{tr}(\rho(x,y) - \rho_0)^2 \\
&= \frac{1}{\alpha} \operatorname{tr}\left((\rho(x,y))^2 - 2\rho(x,y)\rho_0 + \rho_0^2 \right) \\
&= \frac{1}{\alpha} \operatorname{tr}\left(\sum_{I,J=1}^{r^2} A^I(x) A^J(x) \otimes B^I(y) B^J(y) - 2 \sum_{I,J=1}^{r^2} A^I(x) A^J(x_0) \otimes B^I(y) B^J(y_0) \right. \\
&\qquad \left. + \sum_{I,J=1}^{r^2} A^I(x_0) A^J(x_0) \otimes B^I(y_0) B^J(y_0) \right) \\
&= \sum_{K=1}^{2r^4} f_K(x) f'_K(y)
\end{aligned} \tag{39}$$

where the last line defines two functions $f_K(x)$ and $f'_K(y)$. Therefore, we have that the rank of f over the complex numbers is at most

$$\operatorname{rank}(f) \leq 2r^4. \tag{40}$$

Since r is the Schmidt rank of the purified state, $\log r$ lower bounds the dimension of R and L, which we want to translate to a bound on the dimension of $\rho_{L'R}$. We know that

$$\log d_{LR} \leq 2 \log d_{L'R} \tag{41}$$

and that $\log r \leq \log d_R, \log d_L$. Combining these statements we have

$$\log r \leq \frac{1}{2} \log d_{LR} \leq \log d_{L'R} = \mathsf{pp}\overline{\mathsf{PSQM}}^*(f). \tag{42}$$

Finally, by Equation (40) we have that $\log(r) \geq \frac{1}{4} \log \operatorname{rank}(f) - \frac{1}{4}$. Combining this with the previous equation we get

$$\boxed{\mathsf{pp}\overline{\mathsf{PSQM}}^*(f) \geq \frac{1}{4} \log \operatorname{rank} f - \frac{1}{4}.} \tag{43}$$

Here $\mathsf{pp}\overline{\mathsf{PSQM}}^*(f)$ is the minimal number of qubits of shared resource state needed to execute PSQM with perfect security. ■

Note that the rank lower bound does not apply to communication, but only to correlation cost. We could ask if the communication is also lower bounded by the rank, but considering the equality function shows such a bound cannot hold. To see this, consider that equality is full rank, so the log-rank is n. Using linear randomness in the resource, Alice and Bob can take $x \oplus r$ and $y \oplus r$ and then send a constant length hash of those strings. This is perfectly secure and approximately correct, so we can compute equality in the PSQM* model with perfect privacy and log communication, even while the log-rank is linear. Thus our bound cannot also apply to communication.

4.2 Comparison to related bounds

We should also compare the rank lower bound obtained here to similar lower bounds. We can notice first that the communication cost $\mathsf{PSQM}^*(f)$ is lower bounded by two-way quantum communication complexity of f. If we assume perfect correctness, this is lower bounded by the log-rank [10]. If we had assumed perfect correctness for our PSQM protocol then our lower bound would be immediate. Our result shows that perfect privacy (and relaxed correctness) also suffices to obtain a rank bound.

Note that our bound also applies to classical PSM, since classical PSM is lower bounded by quantum PSM. As well, our lower bound uses privacy — indeed our bound is on the shared randomness, which can be zero when there is no privacy requirement.

Another point of comparison are the similar lower bounds on quantum CDS obtained in [18]. There, the log Schmidt rank in perfectly private quantum CDS, denoted ppCDQS, is lower bounded according to

$$\mathsf{ppCDQS}^*(f) \geq \frac{1}{4} \log(\operatorname{nrank}(f)). \tag{44}$$

The non-deterministic rank is the minimal rank of any matrix over the complex numbers which has the same zeros as the communication matrix of f. In general this may be smaller than the usual notion of rank. Because CDS lower bounds PSM [7], we also obtain the same lower bound on perfectly private PSM, but since the nrank may be much smaller than the rank, our bound on PSM is stronger than the one inherited from CDS.

5 Upper bound from T-depth and quantum circuits

In this section we prove new upper bounds on the PSM_k^* model. Our main strategy is to adapt techniques from non-local quantum computation [11], which involves two separated

players, to the k-player setting. This gives an upper bound on $\mathsf{PSM}_k^*(f)$ related to the T-depth of any unitary computing f. With some further modifications to this technique, we show it can be used to realize an upper bound on PSM_k^* based on the size and depth of a quantum circuit computing f.

5.1 Computational models

Recall that the n-qubit Pauli group $\mathcal{P}_n$ consists of n-fold tensor products of the four Pauli operators, $\{I, X, Y, Z\}$, with an added overall phase of ± 1 or $\pm i$. A Clifford unitary C is a unitary such that for any $P \in \mathcal{P}_n$, there exists another $P' \in \mathcal{P}_n$ such that $CPC^\dagger = P'$.

Clifford unitaries are a subgroup of all possible unitaries. To generate the full unitary group, it suffices to consider the T-gate,

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \tag{45}$$

along with the Cliffords. T-gates are more difficult to apply in standard quantum computing architectures, and consequently understanding the number of T-gates required for a given computation has been a topic of interest.

We will be interested in decompositions of unitaries into Clifford layers interlaid with T-gate layers,

$$U = C_d \bar{T}_d C_{d-1} ... C_1 \bar{T}_1 C_0. \tag{46}$$

The operators $\bar{T}_i$ consist of parallel T-gates on a subset S_i of the qubits, and identity on the remaining qubits. The operators C_i are Clifford. We call d_T the T-depth of the circuit.

We are also interested in restricted variants of the above decomposition into Clifford+T layers. To specify these, we define a unitary V to have a backward light-cone of size at most ℓ if, taking a single qubit operator $\mathcal{O}_i$, we have that

$$V^\dagger \mathcal{O}_i V = \tilde{\mathcal{O}}_i \tag{47}$$

has support on at most ℓ qubits. Note that we do not require any notion of geometric locality in these operators; we only consider the size of the non-trivial support. Returning to Clifford+T decompositions, we say that a Clifford+T decomposition is ℓ-local if every Clifford C_i has backward light-cones of size at most ℓ.

5.2 Speelman's instantaneous computation technique

To prove our upper bounds in this section, we borrow techniques developed in the context of non-local quantum computation (NLQC) [11]. In both NLQC and in the context of PSM protocols, it is useful to be able to implement the following transformation.

Definition 9 *An* instantaneous computation *of a unitary $U_{AB_1...B_{k-1}}$ is the following transformation. k players, whom we call Alice and Bob$_1$, ..., Bob$_{k-1}$ each hold one of the systems A, B_1, ..., B_{k-1}. The choice of unitary $U_{AB_1...B_{k-1}}$ is known to all players. We say that Alice and Bob instantaneously implement $U_{AB_1...B_{k-1}}$ if they implement the transformation*

$$|\psi\rangle_{AB'} \to P_{AB'}[m_a, m_b^1, ...m_b^{k-1}] U_{AB'} |\psi\rangle_{AB'} \tag{48}$$

where $AB' = AB_1...B_{k-1}$ is held by Alice at the end of the protocol, $P[m_a, m_b]$ is a Pauli string determined by m_a, m_b, Alice holds m_a, and Bob$_i$ holds m_b^i.

The entanglement cost of instantaneous computations can be upper bounded in terms of the complexity of the unitary $U_{AB'}$. Consider a decomposition of $U_{AB'}$ into Clifford layers and layers of T-gates,

$$U = C_{d_T}\bar{T}C_{d_T-1}\bar{T}C_{d_T-2}...C_1\bar{T}C_0. \tag{49}$$

If we allow arbitrary Cliffords C_i at each layer, and consider only 2 players Alice and Bob_1, [11] shows that U can be computed instantaneously using $O((K_1 n)^{d_T})$ shared EPR pairs where d_T is the T-depth, n is the number of qubits of input, and K_1 is a constant. We will need an extension of this result.

Specifically, we consider the case where 1) We allow $k \geq 2$ players. 2) The Clifford layers are further restricted, to only allow Cliffords with backward light cones of size ℓ. This is equivalent to the statement that the ith output qubit of the Clifford is only influenced by at most ℓ input qubits.

Theorem 10 *Suppose that a unitary $U_{AB_1...B_{k-1}}$ on n_{tot} qubits is of the form*

$$U = C^{\ell}_{d_T}\bar{T}C^{\ell}_{d_T-1}\bar{T}C^{\ell}_{d_T-2}...C^{\ell}_1\bar{T}C^{\ell}_0. \tag{50}$$

where each C^{ℓ}_i is a Clifford unitary with backward light cones of size at most ℓ. Then U_{AB} can be computed instantaneously using $E(U)$ shared EPR pairs, where

$$E(U) \leq O((K\ell)^{d_T-1} \cdot n_{tot} \cdot \min\{k, \ell\}). \tag{51}$$

Here K is a constant independent of the choice of unitary.

We prove this theorem in Appendix A.

Next we proceed to apply this result to PSM^*_k upper bounds.

5.3 T-depth and circuit depth PSM^*_k upper bounds

We first of all show the following PSM^* upper bound from the T-depth.

Theorem 11 *Suppose that a Boolean function $f : X_1 \times ... \times X_k \to \{0,1\}$, $X_i = \{0,1\}^n$ can be computed from the inputs $|x_1, ..., x_k\rangle$ and advice state $|\psi\rangle$ ϵ-correctly by a unitary of the form*

$$U = C^{\ell}_{d_T}\bar{T}C^{\ell}_{d_T-1}\bar{T}C^{\ell}_{d_T-2}...C^{\ell}_1\bar{T}C^{\ell}_0. \tag{52}$$

with Clifford layers C^{ℓ}_i restricted to Cliffords with light cones of size at most ℓ. The total number of qubits of input plus advice is denoted n_{tot}. Then there is an ϵ-correct, $\delta = 2\epsilon$ secure PSM^* protocol for f with communication cost

$$\mathsf{PSM}^*_k(f) \leq O((K\ell)^{d_T-1} \cdot n_{tot} \cdot \min\{k, \ell\}) \tag{53}$$

and which uses a number of EPR pairs satisfying the same upper bound.

Proof. Let the unitary computing $f(x)$ be computed by applying a unitary $U_{AB_1...B_{k-1}}$ to the inputs and advice state followed by a computational basis measurement on the first output qubit. By assumption the circuit computes f with probability $1 - \epsilon$.

The PSM^* protocol is as follows. The players execute the instantaneous computation for U, which uses entanglement upper bounded as in Theorem 10. At this point, Alice holds the output of U, which has been corrupted by a Pauli string $P[m_a, m_{b_1}, ..., m_{b_{k-1}}]$ with the b_i held by Bob_i. Alice proceeds to measure the first qubit, obtaining outcome

s. All of the players then send the measurement outcomes m_a, m_{b_i} produced during the execution of the instantaneous computation protocol.

To see that this protocol is ϵ correct, notice that the Pauli operator acting on the measured qubit will not change the measurement outcome if it is an I or Z operator, and will invert the outcome if it is an X or Y operator. Thus if the referee receives this final measurement outcome along with the strings $m_a, m_{b_1}, ...m_{b_{k-1}}$, the referee can determine which Pauli acted on the measured qubit and inverts the result if it is X or Y, then the resulting bit will be distributed just as if it were the outcome from the original circuit with no Pauli corrections, so will equal $f(x, y)$ with probability at least $1 - \epsilon$.

Next we consider security. In the instantaneous computation protocol, all of the bits sent to the referee were from Bell basis measurements, call them $r = (r_1, ..., r_k)$, except one bit s, which came from Alice measuring the final output qubit. The Bell basis measurement outcomes r are distributed as a uniformly random bit-string in $\{0, 1\}^{|r|}$. To design a simulator, consider that the message is of the form

$$\begin{aligned} \rho_M(x, y) &= \frac{1}{2^{|r|}} \sum_r X^{p(r)} \sigma(x, y) X^{p(r)} \otimes |r\rangle\langle r| \,, \\ \sigma(x, y) &= \alpha(x, y) \, |f\rangle\langle f| + (1 - \alpha(x, y)) \, |f \oplus 1\rangle\langle f \oplus 1| \,. \end{aligned} \tag{54}$$

Here $p(r)$ is a function which determines if there is a Pauli X correction on the measured qubit. The probabilities $\alpha(x, y)$ can in general leak information about (x, y), but we have that $\alpha(x, y) \geq 1 - \epsilon$ for all (x, y) which will ensure this leaked information is small. In particular we define the simulator distribution to be

$$\mathrm{Sim}(f) = \frac{1}{2^{|r|}} \sum_r X^{p(r)} \, |f\rangle\langle f| \, X^{p(r)} \otimes |r\rangle\langle r| \,. \tag{55}$$

Then to check security, we just need to calculate the trace distance between the message distribution and the simulator distribution,

$$\begin{aligned} \|\rho_M(x, y) - \mathrm{Sim}_M(f)\|_1 &= \left\| \frac{1}{2^{|r|}} \sum_r X^{p(r)} (\sigma(x, y) - |f\rangle\langle f|) X^{p(r)} \otimes |r\rangle\langle r| \right\|_1 \\ &= \frac{1}{2^{|r|}} \sum_r \|\sigma(x, y) - |f\rangle\langle f| \, \|_1 \\ &= \frac{1}{2^{|r|}} \sum_r \|(\alpha(x, y) - 1) \, |f\rangle\langle f| + (1 - \alpha(x, y)) \, |f \oplus 1\rangle\langle f \oplus 1| \, \|_1 \\ &\leq \frac{1}{2^{|r|}} \sum_r 2|1 - \alpha(x, y)| \\ &\leq 2\epsilon \end{aligned} \tag{56}$$

so that the protocol is $\delta = 2\epsilon$ secure, as claimed. ■

As a special case of this result, it follows that low-depth quantum circuits, with gates of constant arity, provide a good upper bound on PSM^* complexity.

Corollary 12 *Suppose that a Boolean function $f : X_1 \times ... \times X_k \to \{0, 1\}$, $X_i = \{0, 1\}^n$ can be computed from the inputs $|x_1, ..., x_k\rangle$ by a depth d_f, size s quantum circuit (composed of gates acting on $O(1)$ qubits). Then, there is an ϵ-correct, $\delta = 2\epsilon$-secure PSM^* protocol for f with communication cost*

$$\mathsf{PSM}^*_k(f) \leq (kn + s) \cdot \log^{O(d_f)}(s/\epsilon) \tag{57}$$

and which uses a number of EPR pairs satisfying the same upper bound.

Proof. First we convert the gates from the given quantum circuit to the Clifford + T gate set that consists only of one and two-qubit gates, in particular our gate set consists of: Hadamard, Phase, T, and CNOT. Using Solovay-Kitaev [21, 22] we could do this with a depth overhead factor of $\log(s/\epsilon)$ where s is the size of the circuit. However, we will do better than this by making use of an additional *catalytic* [23] advice state. The catalytic advice state is provided as additional input to the circuit (does not depend on the input) and after the computation it must be returned to its original form so can be reused. Surprisingly, Kim showed that any Pauli Z-rotation can be η-approximated in depth 3 if a certain catalyst state is available, which has size $O(\log^2(1/\eta))$ [23]. Kim and Laakkonen later improved this to be depth 1 with size $O(\log(1/\eta))$ advice [23, 24][3]. We will use this construction to convert our circuit to a Clifford + T circuit with low T-depth.

For each gate in the original circuit we do the following. Let $b = O(1)$ be the bound on the number of qubits of fan-in the circuit's gates have. It's well-known that we can implement any unitary of dimension 2^b exactly with a circuit of size 4^b using only arbitrary single qubit rotations about Z and Y, and CNOT gates [26]. Note that the Y-rotation gate is just a Z-rotation gate conjugated by the single-qubit Clifford gate, SH. Thus, we can rewrite the gate with $O(4^b)$ gates consisting only of Clifford and Z-rotations. Using Kim's construction [23, 24] we then approximate each of the $O(4^b)$ Z-rotation gates to within approximation error η, which only requires T-depth 1 for each such Z-rotation. We implement each of the gates sequentially so that we can reuse the catalytic state. Now the overall T-depth for implementing this gate is $O(4^b)$, uses a catalytic state on $O(\log(1/\eta))$ qubits, and has approximation error $\eta \cdot O(4^b)$.

We do the above for each of the gates. Let s be the total number of gates in the original circuit. So our constructed Clifford + T circuit then has T-depth $d_T := O(d_f \cdot 4^b)$, approximation error $\epsilon = O(s\eta 4^b)$ and requires a catalytic advice state on $O(s \cdot \log(1/\eta))$ qubits.

Furthermore, note that each of the Clifford components act on at most $O(b+\log(1/\eta))$ qubits: the original b input qubits and the $\log(1/\eta)$ catalytic advice qubits. So each of the Clifford layers has lightcones bounded by $\ell := O(b + \log(1/\eta))$.

We set $\eta = \Theta(\epsilon s^{-1} 4^{-b})$ such that the total approximation error is ϵ, the catalytic state is on $a := O(s \cdot \log\left(s4^b/\epsilon\right)) = O(sb\log(s/\epsilon))$ qubits, and the lightcones are bounded by $\ell = O(b\log(s/\epsilon))$.

Let U be the unitary on $n'_{\text{tot}} := (n_{\text{tot}}+a) = nk+O(sb\log(s/\epsilon))$ qubits that implements this circuit, so it takes as input the input to the original circuit (nk-qubits) in addition to the (a-qubit) catalytic advice state, and it computes f to within approximation error ϵ. Using that $n_{\text{tot}} = kn$ we get the claimed bound.

We can implement this unitary instantaneously using Theorem 10. Now, Alice will receive n bits of input in addition to the a qubits of advice. Applying Theorem 10 with n'_{tot} as the total number of qubits, we see that there is an instantaneous protocol for implementing U with the number of EPR pairs used at most

$$\begin{aligned} E(U) &\leq O((K\ell)^{d_T-1} \cdot n'_{\text{tot}} \cdot \min\{k, \ell\}) && (58)\\ &= (b\log(s/\epsilon))^{O(d_f 4^b)} \cdot (n_{\text{tot}} + O(sb\log(s/\epsilon))) \cdot \min\{k, b\log(s/\epsilon)\} && (59)\\ &\leq (b\log(s/\epsilon))^{O(d_f 4^b)} \cdot (n_{\text{tot}} + s) && (60)\\ &\leq (n_{\text{tot}} + s) \cdot \log^{c\cdot d_f}(s/\epsilon) && (61) \end{aligned}$$

for some constant $c > 0$. In the last line we used that $b = O(1)$.

[3] Kim notes in v2 of [23] that after the release of the first version of the paper, Craig Gidney observed that it could be done in T-depth 2 [25].

Now for the PSM_k^* protocol, when each player is given the classical n-bit input, Alice can prepare the catalytic advice state herself, the players can apply the above protocol. Furthermore, following the same argument as in the proof of Theorem 11, this protocol is ϵ-correct and 2ϵ-secure, and both communication cost and number of EPR pairs at most $(n_{\text{tot}} + s) \cdot \log^{c \cdot d_f}(s/\epsilon)$.

■

6 Upper bound from the Fourier 1 norm

In this section we give an upper bound on classical PSM complexity based on the one-norm of the Fourier transformation of f. This upper bound appears to be new to the classical literature. As we discuss, the Fourier one-norm captures how the function f is related to parity functions.

6.1 Fourier transform for Boolean functions and the Fourier one-norm

We briefly introduce the Fourier transform of a Boolean function. Let x, S be n bit strings. We think of S as labelling a subset of the bits, where the ith bit of S is 1 iff bit i is included in the subset. Then define the parity function

$$\chi_S(x) = (-1)^{S \cdot x} = (-1)^{\sum_{i \in S} x_i} \tag{62}$$

which is -1 if the parity of the bits x_i in the subset S is odd, and $+1$ otherwise. We study a Fourier transform of f, which can also be understood as expressing $f(x)$ as a sum over parity functions. Specifically, the Fourier transform $\hat{f}(S)$ is defined such that

$$f(x) = \sum_S \hat{f}(S) \chi_S(x) \tag{63}$$

Alternatively, we can use that

$$\frac{1}{2^n} \sum_x \chi_S(x) \chi_T(x) = \delta_{S,T} \tag{64}$$

to express $\hat{f}(S)$ in terms of $f(x)$,

$$\hat{f}(S) = \frac{1}{2^n} \sum_x f(x) \chi_S(x). \tag{65}$$

Our upper bound will be expressed in terms of the Fourier 1 norm, which given a function f is defined from the Fourier coefficients $\hat{f}(S)$ according to

$$\|\hat{f}\|_1 = \sum_S |\hat{f}(S)| \tag{66}$$

The Fourier 1 norm captures, in a weighted sense, how many Fourier coefficients are needed to represent $f(x)$.

6.2 Upper Bound

Theorem 13 *For any function $f : X \times Y \to \{0, 1\}$, and any $\delta > 0$, the function f can be computed δ-correctly and perfectly securely in the PSM model using communication and randomness both of $O(\|\hat{f}\|_1^2 \ln(2/\delta))$.*

Proof. The starting point for the proof is the observation that $f(x, y)$ can be expressed as the expected value of a random variable from a certain fixed distribution depending on the function f. In more detail, define a probability distribution p from the Fourier coefficients of f,

$$p_S = \frac{|\hat{f}(S)|}{\|\hat{f}\|_1}. \tag{67}$$

Observe that $f(x, y)$ can be expressed in terms of the expectation of the random variable $\text{sign}(\hat{f}(S)) \cdot \chi_S(x, y)$ under this distribution. In more detail,

$$\begin{aligned} f(x, y) &= \sum_S \hat{f}(S)\chi_S(x, y) \\ &= \|\hat{f}\|_1 \cdot \sum_S p_S \cdot \text{sign}(\hat{f}(S)) \cdot \chi_S(x, y) \\ &= \|\hat{f}\|_1 \cdot \mathbb{E}_{S\sim p}[\text{sign}(\hat{f}(S)) \cdot \chi_S(x, y)]. \end{aligned} \tag{68}$$

Next, we note that $\chi_S(x, y) = \chi_S(x)\chi_S(y)$, as can be checked from its definition. Thus,

$$\frac{f(x, y)}{\|\hat{f}\|_1} = \mathbb{E}_{S\sim p}[\text{sign}(\hat{f}(S)) \cdot \chi_S(x) \cdot \chi_S(y)]. \tag{69}$$

This naturally motivates a strategy for Alice and Bob as follows. Firstly, using shared private randomness, they sample a set $S \sim p$ according to the aforementioned distribution p, secondly, they sample a uniformly random bit $b \in \{-1, 1\}$. Then, Alice sends $\chi_S(x) \cdot b$ to the referee and Bob sends $\chi_S(y) \cdot b \cdot \text{sign}(\hat{f}(S))$. We then have the referee multiply these two quantities to get $\text{sign}(\hat{f}(S)) \cdot \chi_S(x, y)$.

Firstly, we observe that the expected output of the referee is precisely $f(x, y)/\|\hat{f}\|_1$ from Equation (69). Furthermore, we will see that this protocol is perfectly private. But first, we would like to amplify the success probability to get perfect correctness. To determine whether $f(x, y)$ is 1 or -1 with probability $1-\delta$, the idea is to have the players repeat this protocol $m = 10\|\hat{f}\|_1^2 \ln(2/\delta)$ times in parallel (using independent randomness) and have the referee output 1 or -1 if the sum of all his outputs is positive or negative respectively. We now prove that this described protocol is correct. To do so, observe that expected sum of the outputs is $m \cdot f(x, y)/\|\hat{f}\|_1$. As each output is $\{\pm 1\}$-valued, by Hoeffding's inequality, the probability that the sum differs from its expectation by more than t is at most $2\exp(-t^2/2m)$, which is at most δ for $t = \sqrt{2m\ln(2/\delta)}$. Thus, with all but δ probability, the sum of all outputs is roughly $m \cdot f(x, y)/\|\hat{f}\|_1 \pm \sqrt{2m\ln(2/\delta)}$ which is roughly $10\|\hat{f}\|_1 \ln(2/\delta) \cdot f(x, y) \pm 5\|\hat{f}\|_1 \ln(2/\delta)$ by our choice of m. As the first term dominates, it is clear that this quantity is positive if and only if $f(x, y) = 1$. This completes the proof of correctness of the amplified protocol.

Perfect privacy of the original (not repeated) protocol, implies perfect privacy of the repeated protocol, so all that remains is to show that the original protocol is perfectly private. Recall that the referee receives a bit $b_1 \in \{-1, 1\}$ from Alice and a bit $b_2 \in \{-1, 1\}$ from Bob, where $b_1 = b \cdot \chi_S(x)$ for a uniformly random bit $b \in \{-1, 1\}$ and $b_2 = b \cdot \chi_S(y) \cdot \text{sign}(\hat{f}(S))$. The simulator for this protocol is as follows: Given $f(x, y)$, the simulator samples a uniformly random bit $b \in \{-1, 1\}$ and an independent random bit $c \in \{-1, 1\}$ with bias given by $f(x, y)/\|\hat{f}\|_1$ and outputs $b_1' := b$ for Alice's message and $b_2' := b \cdot c$ for Bob's message. We will show that the resulting distribution on (b_1', b_2') is identical to that of (b_1, b_2) in the original protocol. We will instead argue that the distribution of $(b_1', b_1' \cdot b_2')$ is identical to that of $(b_1, b_1 \cdot b_2)$ and since $b_1, b_1', b_2, b_2' \in \{-1, 1\}$, this suffices. Firstly, observe that these are product distributions as the random variables

$b_1 \cdot b_2$ and $b'_1 \cdot b'_2$ are independent of b_1 and b'_1 respectively. Thus, it suffices to argue that the marginal distributions are identical. Firstly, it is clear that b_1 and b'_1 are uniformly random bits. Secondly, observe that $b'_1 \cdot b'_2$ is by definition a random bit in $\{-1, 1\}$ with bias $f(x, y)/\|\hat{f}\|_1$. In the original protocol, we observe that $b_1 \cdot b_2$ is a bit obtained by sampling $S \sim p$ and returning $\chi_S(x, y) \cdot \text{sign}(\hat{f}(S))$ – this is simply a random bit whose expectation is $f(x, y)/\|\hat{f}\|_1$ by Equation (69). This completes the proof. ■

A k-player instantaneous computations based on the T-depth

In this appendix we give the proof of Theorem 10. Our techniques follow [11], but we make some generalizations to achieve the needed bound.

A.1 The garden-hose model

To give the proof, we first need to describe the garden-hose model and some associated instantaneous computation strategies. The garden-hose model [27] is most easily described in terms of the following setting. Alice and Bob are neighbours, and share a fence. Alice has an input string $x \in \{0, 1\}^n$, while Bob has an input string $y \in \{0, 1\}^n$. Alice has a tap, which she can turn on to produce a flow of water. Alice and Bob share a number of pipes which connect their yards, and they have hoses that they can use to connect pipes to one another, or the tap to a pipe. Alice and Bob wish to compute a Boolean function $f(x, y)$, with the outcome determined by where the water spills. Typically, the model is defined so that water spilling on Alice's side indicates $f(x, y) = 0$, while water spilling on Bob's side indicates $f(x, y) = 1$. The garden-hose model can also be formalized in terms of path connectivity in a particular form of graph, see [27]. We won't need this formalization though, and stick to the more informal water-based description.

We modify the definition of the garden-hose model somewhat and specify two pipes labelled "$f = 0$" and "$f = 1$", and require the water to spill on Alice's side out of the corresponding pipe. In fact, these models are not too different, as the following lemma from [28] shows.

Lemma 14 *Suppose there is a garden-hose protocol that computes $f(x, y)$ using m pipes in the sense that water spills on Alice's side if $f(x, y) = 0$, and on Bob's side if $f(x, y) = 1$. Then there is also a garden-hose protocol that computes $f(x, y)$ in the sense of water spilling on Alice's side from one of two designated pipes that uses at most $3m + 1$ pipes.*

The model where water spills from designated pipes will generalize better to the k player setting, so take the model with two designated pipes on Alice's side as the defining setting. We denote the number of pipes needed to compute f in (this variant of) the garden-hose model by $GH(f)$.

In the quantum context, the garden-hose model appears as a description of concatenated teleportations in some settings. In particular, consider an unknown quantum state $|\psi\rangle$, which plays the role of the tap in the garden-hose description. Alice and Bob share a set of EPR pairs between them, which play the role of the pipes. Alice and Bob can then make Bell basis measurements, which act on either two ends of EPR pairs they hold in their own labs, or (in Alice's case) on the input state plus the end of one EPR pair. To see why the water-flow analogy of the garden-hose model is relevant, consider that after the input state is measured with one EPR pair, the state has moved to the other end of the EPR pair, up to Pauli corrections. Each subsequent measurement moves the state to the other end of the measured EPR pair. To an observer with access to the measurement outcomes, it is as if the state is flowing along the path determined by the pipes in the garden-hose picture.

We generalize the garden-hose model to allow $k \geq 2$ players, in which case we name the players Alice, Bob_1, Bob_2,..., Bob_{k-1}. Each player receives a string of n bits, with x_0 the string held by Alice and x_i, $k-1 \geq i \geq 1$ held by Bob_i. In this setting, pairs of players share pipes, and the actions of the players is as before: Alice may connect the tap to a pipe, and all players may connect open ends of pipes they have access to using hoses. Again the result of the computation is determined by considering two labelled pipes shared with Alice. This model can be instantiated as before in the quantum context with the tap replaced by an input state and the pipes replaced by EPR pairs. We define the minimal number of pipes used in a k-party garden-hose protocol by $GH_k(f)$. Note that we allow any fixed configuration of pipe connections among the players.

We make use of the following lemma regarding the k-party garden-hose model. The proof is nearly the same as is given in [11, 28] for the case of two players. For completeness, we include the proof in our k-player setting.

Lemma 15 *The k-party garden-hose complexity satisfies the following:*

$$GH_k\left(\bigoplus_i f_i\right) \leq 4\sum_i GH_k(f_i) \tag{70}$$

Proof. Consider garden-hose protocols for each f_i, which we label P_i. We give a garden-hose protocol for $\oplus_i f_i$ by wiring copies of the P_i together in an appropriate way. Concretely, we take 4 copies of P_i, and connect them as shown in Figure 3. The gadget has four open hoses, which we wire together with further gadgets: we wire the 0 output of the f_i gadget to the 0 input of the f_{i+1} gadget, and the 1 output of the f_i gadget to the 1 input of the f_{i+1} protocol. By inspection, one can check that the gadget flips the parity of the input if $f_i = 1$, and leaves the input unchanged if $f_i = 0$. To compute $\oplus_i f_i$ then, we connect the tap to the 0 input of the f_1 gadget, and label the 0 and 1 outputs of the final f_i as the 0 and 1 labelled output hoses of the protocol. After the water flows through gadgets for each f_i, we've computed $\oplus_i f_i$. ■

A.2 A garden-hose gadget

Before stating the precise upper bound and its proof, we first need the following lemma, related to the garden-hose model. Specifically, we discuss the garden-hose complexity of implementing a controlled $P^\dagger$ gate instantaneously, up to Pauli corrections, and the garden-hose complexity of the resulting corrections. The lemma is very similar to one in [11]; the only change is to point out that the proof there continues to apply in the context of the $k > 2$ party setting.

Lemma 16 *Let f be a k-party function known to all parties. Assume Alice holds a single qubit state $S^{f(x)}|\psi\rangle$, where $x = (x_0, x_1, ..., x_{k-1})$ Alice knows x_0 and Bob_i knows x_i. Then the following two statements hold:*

1. *There exists an instantaneous protocol (no communication) which uses $2GH_k(f)$ EPR pairs after which Alice holds $X^{g(\hat{x})}Z^{h(\hat{x})}|\psi\rangle$, where $\hat{x}$ depends on x and $2GH(f)$ bits that describe Alice and Bob's measurement outcomes.*
2. *The garden hose complexities of g and h are at most linear in the complexity of f,*

$$\begin{aligned} GH_k(g) &\leq 4GH_k(f) \\ GH_k(h) &\leq 11GH_k(f) \end{aligned} \tag{71}$$

Proof. For the first part, run the garden hose protocol with $S^{f(x)}|\psi\rangle$ as input, have Alice do $S^\dagger$ to the $f = 1$ output hose, then wire the outputs to a copy of the protocol. The

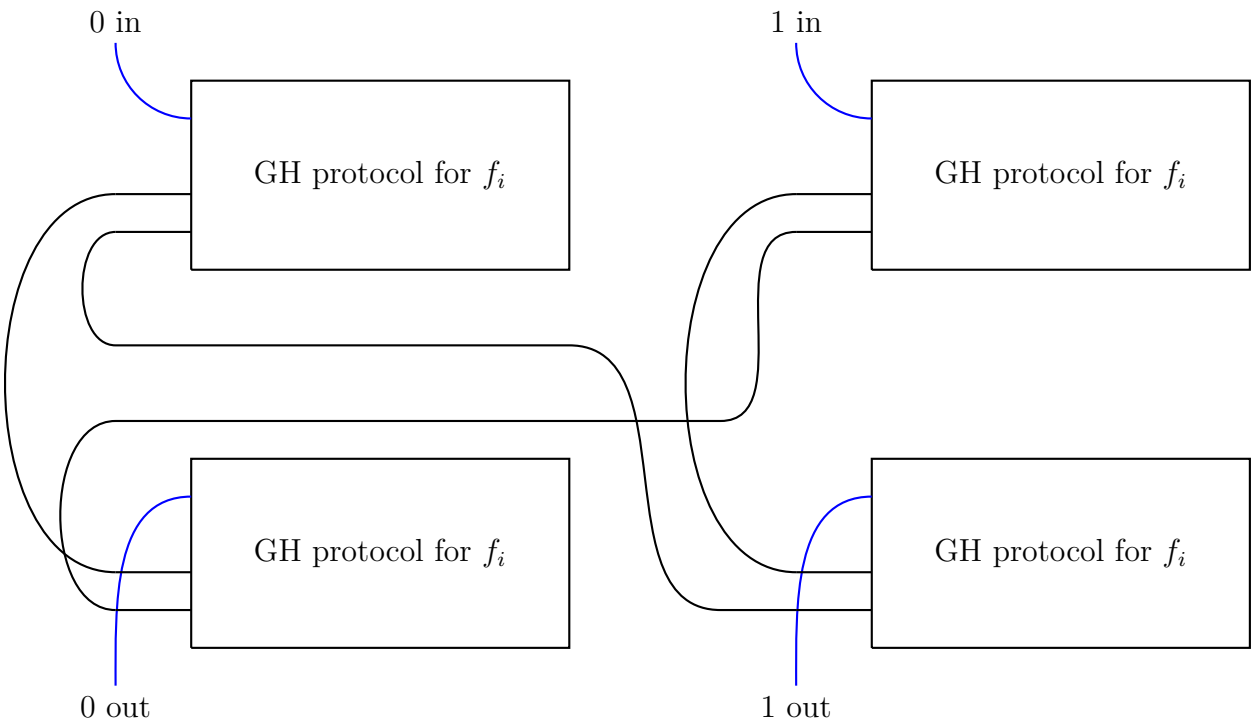


Figure 3: XOR gadget for computing $\oplus_i f_i$ in the garden-hose model. It can be checked directly that if water enters on the top left, it exits on the left if $f_i = 0$ and on the right if $f_i = 1$. Meanwhile if water enters from the top right, it exits from the bottom right if $f_i = 0$ and from the bottom left if $f_i = 1$. By wiring such gadgets together for each f_i then, we can compute $\oplus_i f_i$.

input qubit comes back out of the "input" wire of the second protocol, now with no S gate. This is illustrated in Figure 4. Note that we incur Pauli corrections accumulated from all the Bell basis measurements along the path of the qubit.

Note that in the garden-hose protocol used to apply the conditional $S^\dagger$ there is a sequence of teleportation measurements made, which create possible X and Z corrections. Call the bits determining if there is an X correction $b_x^{i,j}$, where i, j label the two EPR pairs involved in the measurement. Similarly, there are corrections $b_z^{i,j}$. Note that not all measurements contribute to these corrections, only those that occur in the unbroken chain of EPR pairs connected to the input state. Rather than obtain the input state with a $(S^\dagger)^{f(x,y)}$ applied, we actually end up applying, up to a global phase, the operator

$$X^{\sum_{i\in A} b_x^{i,j}} Z^{\sum_{i\in A} b_z^{i,j}} (S^\dagger)^{f(x,y)} X^{\sum_{i\in B} b_x^{i,j}} Z^{\sum_{i\in B} b_z^{i,j}} \tag{72}$$

where the pairs of indices $(i, j) \in B$ correspond to measurements in the chain that occur before $(S^{-1})^{f(x,y)}$, while pairs $(i, j) \in A$ occur after. Using that (again up to a global phase)

$$\begin{aligned} XZS^\dagger &= S^\dagger X \\ S^\dagger Z &= ZS^\dagger \end{aligned} \tag{73}$$

the above becomes

$$X^{g(\hat{x})} Z^{h(\hat{x})} (S^\dagger)^{f(x,y)} \tag{74}$$

where

$$\begin{aligned} g(\hat{x}) &= \sum_{(i,j)\in A\cup B} b_x^{i,j}, \\ h(\hat{x}) &= \sum_{(i,j)\in A\cup B} b_z^{i,j} + f(x,y) \sum_{(i,j)\in B} b_x^{i,j}. \end{aligned} \tag{75}$$

Thus to compute g, we just need to compute the parity of all of the $b_x^{i,j}$ that occur in the chain. Note that which measurements are actually a part of the chain depends on x, so this is a function of the original input x as well as the measurement outcomes $b_x^{(i,j)}$. The function h is somewhat more involved, in particular there is an additional correction based on the $b_x^{(i,j)}$ for measurements that occur before the conditional $S^\dagger$.

Let's begin with designing a garden-hose protocol to compute $g(\hat{x})$. To do this, we create a "rail", consisting of two EPR pairs, one for each EPR pair in the initial protocol. Then, we connect subsequent rails in the ordering defined by the sequence of EPR pairs used in the original protocol. We connect the rails end to end if $b_x^{i,j} = 0$, and we connect them cross-wise if $b_x^{i,j} = 1$. Thus after running over all (i, j), the input is crossed if the parity of the $b_x^{i,j}$ is odd, and left unchanged if the parity is even. This protocol uses twice the EPR pairs used in the protocol for applying $(S^{-1})^{f(x,y)}$, which itself was $2GH(f)$, so the cost is $4GH(f)$.

Now we consider the function $h(\hat{x})$. We need a somewhat more involved protocol that treats EPR pairs before and after the conditional $S^\dagger$ differently, and accounts for the value of $f(x, y)$. To do this, we first run a garden-hose protocol to compute $f(x, y)$, then feed the two output hoses into two different subsequent garden-hose protocols. The $f = 0$ pipe is input to a protocol computing the parity of just the Z corrections. We do this using the "rail" construction, just as in computing $g(\hat{x})$. The $f = 1$ pipe is input to a similar rail protocol, which flips the rails if $b_x^{(i,j)} \oplus b_z^{(i,j)} = 1$ for pipes occurring before the $S^\dagger$, and flips the pipes after the $S^\dagger$ if $b_z^{(i,j)} = 1$. The garden-hose complexity of this protocol is composed of:

- The complexity of computing $f(x, y)$, in a way that uses just two spilling pipes, which is $3GH_k(f)$.
- The complexity of computing the Z corrections only, in the sub-protocol that is used when $f(x, y) = 0$. This is $4GH_k(f)$, where the 4 comes from using the rail construction to double the pipes in the initial protocol, which itself was the protocol that involved computing f, applying $S^\dagger$, then running the protocol for f in reverse.
- The complexity of computing the parity of the $b_x^{(i,j)} \oplus b_z^{(i,j)}$ for the first part of the protocol (before $S^\dagger$) along with the parity of the $b_z^{(i,j)}$ in the later part of the protocol. This is $4GH_k(f)$ again.

In total then the garden hose complexity of $h(\hat{x})$ is $11GH_k(f)$. ∎

A.3 Instantaneous k-party computations from T-depth

We are ready to prove our upper bound on the entanglement cost of implementing a unitary based on the T-depth. Before delving into the detailed proof, we give a heuristic understanding of where the dominant scaling of the entanglement cost comes from. The protocol involves first having all of the Bobs perform Bell basis measurements using EPR pairs shared with Alice, as if teleporting their states to her. This gives the full state in Alice's lab, up to Pauli corrections which are determined by a distributed set of measurement outcomes. Alice then applies her first Clifford layer, then applies the first layer of T gates. We can conjugate the Pauli's through the Clifford to give new Pauli's, then through the T gates using the identities

$$\begin{aligned} ZT &= TZ, \\ TX &= SXT, \end{aligned} \tag{76}$$

which hold up to a global phase. This leaves us in a state where one layer of the unitary has been applied, up to S corrections. We then use Lemma 16 to correct the S gates. There is an entanglement cost to doing this set by the garden-hose complexity of the

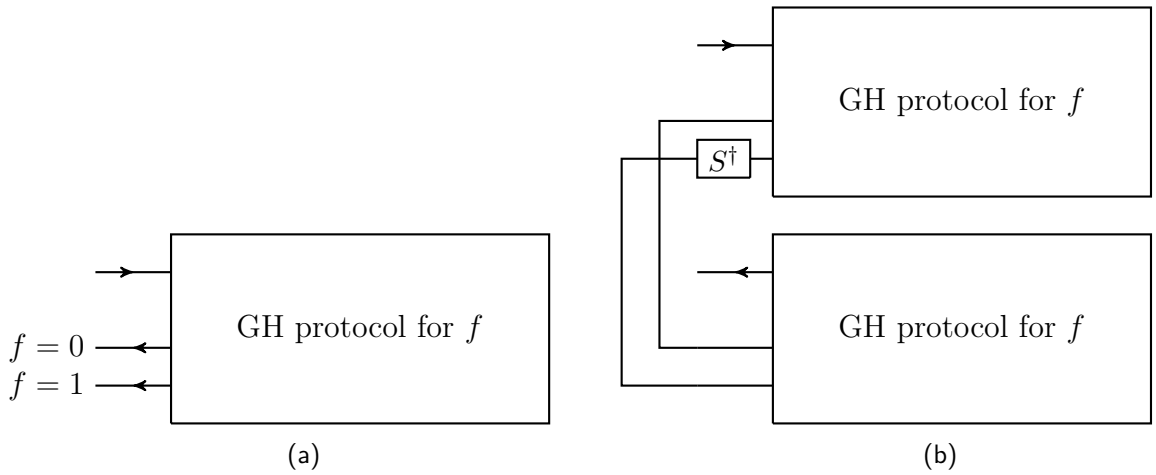


Figure 4: a) k-party garden-hose protocol for a function f. The water enters in the top left pipe, is redirected through a sequence of pipes represented abstractly as the white rectangle, then exits through one of two pipes, indicating the value of $f(x, y)$. The open input and both open outputs are held by Alice, while the remaining parties are involved in the intermediate steps. b) Protocol for applying a $(S^\dagger)^{f(x,y)}$. The input state is entered into a garden hose protocol that computes f, then $S^\dagger$ is applied only to the output pipe indicating $f(x, y) = 1$. Another instance of the protocol for f is then run, and the corresponding output pipes of the two protocols are connected. As a result water always runs out a single fixed pipe.

function determining if there is an S gate or not. After correcting the S gates as needed, we begin again in the situation we started in, trying to apply a Clifford+T layer to a state with unknown Pauli corrections applied to it. We repeat the above procedure to apply the next layer. After each layer, the garden-hose complexity of the needed S corrections grows, and this growth controls the entanglement cost.

To capture the form of the S corrections more precisely and understand how their garden-hose complexity grows, define $g_{i,j} = 1$ if there is an X correction on the jth input wire and 0 otherwise, along with $g_{i+1,j} = 1$ if an X correction appears on the jth output wire after conjugation. Similarly, we define $h_{i,j}$ and $h_{i+1,j}$ to be 1 to indicate a Z correction on the input or output jth wire, respectively. Then, we can see that the output wire functions are related to the input wire functions by

$$\begin{aligned} g_{i+1,k} &= \bigoplus_{j \in S_{g,k}} g_{i,j} \oplus \bigoplus_{j \in S'_{g,k}} h_{i,j}, \\ h_{i+1,k} &= \bigoplus_{j \in S_{h,k}} g_{i,j} \oplus \bigoplus_{j \in S'_{h,k}} h_{i,j}. \end{aligned} \tag{77}$$

The subsets $S^{(\prime)}_{g,k}$ and $S^{(\prime)}_{h,k}$ depend on the choice of Clifford and the wire k being considered. For Clifford with backward light cones of size at most ℓ, we have that these sets are not larger than ℓ. From Lemma 15, we know how the garden-hose complexity of the XOR of many functions behaves, and in particular we can bound it by something of order ℓ times the worst-case garden-hose complexity of the $g_{i,j}$ and $h_{i,j}$. The garden-hose complexity of the worst single qubit correction at layer $i+1$, call it t_{i+1}, then is related to the complexity at the previous layer by $t_{i+1} \lesssim \ell\, t_i$. An added complication is that these Pauli corrections move through the T gates at this layer to give S gates, and then to correct the S gates we apply Lemma 16. This increases the garden-hose complexity of the Pauli corrections on that wire, but only by a constant factor that contributes to the value of K. It is the XOR functions determined by the choice of Clifford that give the dominant scaling of the entanglement cost.

Finally, to solve the recursive relation $t_{i+1} \lesssim t_i \ell$ we need to know the garden-hose complexity at the 0th layer, which means the garden-hose complexity of the Pauli corrections right after the initial teleportation into Alice's lab. These have constant garden-hose

complexity, since they depend on just one bit held in one of the Bobs' labs. After the first Clifford, denoted C_0^ℓ then, the garden-hose complexity is at most ℓ, since the functions $g_{1,i}$, $h_{1,i}$ are XOR's of ℓ bits. However, it is possible some of those bits are held together in one lab, in which case the parity functions $g_{1,i}$, $h_{1,i}$ only depend on a parity of a subset of them, which the local party can pre-compute. For instance if we have k-parties, $g_{1,i}$, $h_{1,i}$ are XOR functions of at most k distributed bits. This means $t_1 = O(\min\{k,\ell\})$, and hence $t_d \lesssim \min\{k,\ell\}(K\ell)^{d-1}$. Letting n_{tot} be the total number of qubits the unitary acts on, the entanglement cost for each layer is then bounded by n_{tot}, the maximal number of possible S corrections at each layer, times t_i, the worst-case correction complexity. The total entanglement cost is then the sum of the cost for each layer,

$$E \leq \sum_{i=1}^{d} t_i n_{\text{tot}} \leq O((K\ell)^{d-1} \cdot n_{\text{tot}} \cdot \min\{k,\ell\}) \tag{78}$$

which is the claimed scaling. We give a formal proof and more detailed accounting in the theorem proof below.

Theorem 17 *Given a unitary $U_{AB_1\ldots B_{k-1}}$ that can be implemented in a Clifford+T decomposition using a circuit of T-depth d, we have that U can be computed instantaneously using*

$$E(U) \leq O((K\ell)^{d-1} \cdot n_{tot} \cdot \min\{k,\ell\}) \tag{79}$$

EPR pairs.

Proof. We first have each of the Bobs 'teleport'[4] their systems B to Alice, who then holds

$$X^{\vec{g}_0(y)} Z^{\vec{h}_0(y)} \left|\psi\right\rangle_{AB} \tag{80}$$

where, less succinctly, we mean

$$\begin{aligned} X^{\vec{g}_0(y)} &= X_1^{g_{0,1}(y)} \ldots X_n^{g_{0,n}(y)} \\ Z^{\vec{h}_0(y)} &= Z_1^{h_{0,1}(y)} \ldots Z_n^{h_{0,n}(y)} \end{aligned} \tag{81}$$

where X_i and Z_i act on the ith qubit. Note that the entries of both $\vec{h}$ and $\vec{g}$ all have constant garden-hose complexity, since they are functions of single bits held in one of the Bobs labs.

This will serve as our base case in an inductive argument. We induct on the level i, and assume Alice holds the state

$$X^{\vec{g}_i(x,y)} Z^{\vec{h}_i(x,y)} \bar{T}_i C_i \ldots \bar{T}_1 C_1 \left|\psi\right\rangle_{AB}. \tag{82}$$

where Alice holds x and Bob holds y, and the entries of $\vec{g}_i$ and $\vec{h}_i$ have known garden-hose complexities. Define

$$t_i = \max\{\max_j\{GH(g_{i,j})\}, \max_j\{GH(h_{i,j})\}\}. \tag{83}$$

In words t_i is the worst-case garden-hose complexity of any single X or Z correction in the ith layer. We have from above that $t_0 = 2$.

To induct have Alice apply $\bar{T}_{i+1} C_{i+1}$, obtaining

$$\bar{T}_{i+1} C_{i+1} X^{\vec{g}_i(x,y)} Z^{\vec{h}_i(x,y)} \bar{T}_i C_i \ldots \bar{T}_1 C_1 \left|\psi\right\rangle_{AB} = \bar{S}^{\vec{f}_i(x,y)} X^{\vec{g}'_i(x,y)} Z^{\vec{h}'_i(x,y)} \bar{T}_{i+1} C_{i+1} \ldots \bar{T}_1 C_1 \left|\psi\right\rangle_{AB}$$

[4] By this we mean have each Bob measure their system in the Bell basis along with one end of a maximally entangled state, with the other end held by Alice.

Then, we use the procedure of Lemma 16 to undo the phase gates, obtaining

$$X^{\vec{g}_i''(x,y)\oplus\vec{g}_i'(x,y)} Z^{\vec{h}_i''(x,y)\oplus\vec{h}_i'(x,y)} \bar{T}_{i+1} C_{i+1} ... \bar{T}_1 C_1 \left|\psi\right\rangle_{AB} . \tag{84}$$

The functions $\vec{g}_i', \vec{h}_i'$ arise from commuting the X, Z operators through $\bar{T}_{i+1}C_{i+1}$, while the $\vec{g}_i'', \vec{h}_i''$ operators appear when correcting the phase gates. The singly-primed operators are of the form

$$\begin{aligned} g'_{i,j} &= \bigoplus_{l\in S_{g,j}} g_{i,l} \oplus \bigoplus_{k\in S'_{g,j}} h_{i,k} \\ h'_{i,j} &= \bigoplus_{l\in S_{h,j}} g_{i,l} \oplus \bigoplus_{k\in S'_{h,j}} h_{i,k} \end{aligned} \tag{85}$$

where the subsets $S^{(\prime)}_{g/h,j}$ depend on the Clifford, and have size at most ℓ.

The functions $\vec{g}_i'', \vec{h}_i''$ appear when undoing the $S^{\vec{f}(x,y)}$ operator, which we do using the procedure in Lemma 16. We are also provided with upper bounds on the garden-hose complexity of these functions from that lemma. We want to determine the garden-hose complexity of $g_{i+1,j} = g''_{i,j} \oplus g'_{i,j}$ and $h_{i+1,j} = h''_{i,j} \oplus h'_{i,j}$. Starting with $g_{i+1,j}$, we have

$$\begin{aligned} GH(g_{i+1,j}) &= GH\left(\bigoplus_{l\in S_{g,j}} g_{i,l} \oplus \bigoplus_{k\in S'_{g,j}} h_{i,k} \oplus g''_{i,j}\right) \\ &\leq 4\left(\sum_l GH\left(g_{i,l}\right) + \sum_k GH(h_{i,k}) + GH(g''_{i,j})\right) \\ &\leq 4\left(\sum_l GH\left(g_{i,l}\right) + \sum_k GH(h_{i,k}) + 4GH(f_{i,j})\right) \\ &\leq 4\left(\ell t_i + \ell t_i + 4GH(f_{i,j})\right) \end{aligned} \tag{86}$$

where the first inequality uses Lemma 15 (the XOR lemma), the second line uses that $GH(g''_{i,j}) \leq 4GH(f_{i,j})$ which comes from Lemma 16, and the last uses the definition of t_i.

It remains to bound the garden-hose complexity of $f_{i,j}$. Notice that since $f_{i,j}$ is itself a parity function of the $g_{i,j}$ and $h_{i,j}$ (it is of the form (85)), so again its garden hose complexity is at most $4\ell t_i$ by a use of the XOR lemma. Overall then this gives

$$GH(g_{i+1,j}) \leq 4(\ell t_i + \ell t_i + 4 \cdot 4\ell t_i) = 72\ell t_i \tag{87}$$

An upper bound can be determined for $GH(h_{i+1,j})$ in a similar way. The only difference is that where before we used $GH(g''_{i,j}) \leq 4GH(f_{i,j})$, we now need $GH(h''_{i,j}) \leq 11GH(f_{i,j})$, which is given in Lemma 16. This changes the constant but gives a similar upper bound,

$$GH(h_{i+1,j}) \leq 184\ell t_i. \tag{88}$$

Using equations (87) and (88), we get that

$$t_{i+1} \leq 184\ell t_i. \tag{89}$$

Our numerical constant is not optimal, but we lose the optimal constants in favour of a simpler presentation. We will write $t_{i+1} = K\ell t_i$ to summarize the above. This relation and our earlier computation showing that $t_1 = \min\{\ell, k\}$ is solved by

$$t_d \leq O((K\ell)^{d-1} \min\{\ell, k\}). \tag{90}$$

Summing over the corrections at each of the d layers, which each involve n_{tot} qubits, leads to the claimed upper bound. ■

B Newman's Theorem for PSM

The following theorem shows that the randomness complexity in the PSM model is never much larger than the communication complexity. The proof is straightforward and similar to the well-known Newman's theorem in communication complexity [29]; however we have not seen it recorded explicitly for PSM, so we give a proof here for completeness. A similar statement for the related conditional disclosure of secrets setting was proven in [30].

Theorem 18 ***(Newman's theorem for PSM)*** *Consider an ϵ-correct and δ-secure PSM protocol for function f, with communication complexity c. Then, there exists an $\epsilon + \delta'$-correct and $\delta + 2\delta'$-secure PSM protocol for f using communication complexity c and randomness complexity $2c + O(\log(c+n) + \log(1/\delta'))$.*

Proof. Let D be the distribution from which the players sample their randomness (independently of their inputs). Sample $r_1, \ldots, r_K \sim D$ where we take $K = 2^c \cdot (c+n) \cdot \log(1/\delta')/\epsilon^2$. We will think of $r_1, \ldots, r_K$ being the common source of randomness for all inputs and in the new protocol, the players will instead sample $k \sim [K]$ and run the original protocol with r_k as the randomness. We will now analyze the correctness and privacy of this protocol.

Privacy. Fix any inputs x, y. Now, each fixed random string r_i induces a fixed transcript $m_{x,y}(r_i)$ and we consider the distribution $M'_{x,y}$ on transcripts obtained by sampling $i \sim [K]$ and outputting $m_{x,y}(r_i)$. Compare it to the ideal distribution $M_{x,y}$ on transcripts obtained by sampling a random $r \sim D$ and outputting $m_{x,y}(r)$. For any τ in the support of the message space, we want that with high probability, the probabilities assigned to τ by $M_{x,y}$ and by $M'_{x,y}$ differ very little — by at most $t = \delta'/2^c$. By Hoeffding's inequality, these probabilities differ by at least t with probability at most $\exp(-t^2K)$. This means, by a union bound over all possible transcripts τ, that the total variation distance between $M_{x,y}$ and $M'_{x,y}$, given by

$$\frac{1}{2}\sum_{\tau} |M_{x,y}[\tau] - M'_{x,y}[\tau]| \tag{91}$$

is at most $t \cdot 2^c/2$ with probability at least $1 - \exp(-t^2K) \cdot 2^c$. Further, we want that these distributions are δ'-close for all input pairs x, y, which (by the union bound again) occurs with probability at least $1 - \exp(-t^2K) \cdot 2^c \cdot 2^n$. If this happens, then it would follow from the Triangle Inequality that the new protocol is $(\delta + 2\delta')$-private. Setting $t = \delta'/2^c$ so that the total variation distance is at most δ', we obtain that the bad event has probability at most $\exp(-\delta'^2 K/2^{2c}) \cdot 2^c \cdot 2^n$. We want this to be strictly smaller than 1, so that by linearity of expectation, we can fix some random strings $r_1, \ldots, r_K$ such that the distributions $M'_{x,y}$ and $M_{x,y}$ are δ'-close in total variation distance for all x, y. To achieve this bound, we only need to set $K = \Theta(2^{2c} \cdot (c+n)/\delta'^2)$.

Correctness. The correctness of this protocol follows immediately from the guarantee from earlier that the distribution $M'_{x,y}$ is δ'-close to $M_{x,y}$ for all x, y – indeed, the referee's output only depends on the distribution of the transcript, and since the original protocol is ϵ-correct, the new protocol is $\epsilon + \delta'$-correct. ■

References

[1] 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.

[2] 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.

[3] 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.

[4] 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)*, pages 86–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2020.

[5] 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. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2022.

[6] Akinori Kawachi and Harumichi Nishimura. Communication complexity of private simultaneous quantum messages protocols. *arXiv preprint arXiv:2105.07120*, 2021.

[7] Rene Allerstorfer, Harry Buhrman, Alex May, Florian Speelman, and Philip Verduyn Lunel. Relating non-local quantum computation to information theoretic cryptography. *Quantum*, 8:1387, 2024.

[8] Uma Girish, Alex May, Leo Orshansky, and Chris Waddell. Comparing classical and quantum conditional disclosure of secrets. *arXiv preprint arXiv:2505.02939*, 2025.

[9] Uma Girish, Alex May, Natalie Parham, and Henry Yuen. Magic and communication complexity. *arXiv preprint arXiv:2510.07246*, 2025.

[10] Harry Buhrman and Ronald de Wolf. Communication complexity lower bounds by polynomials. In *Proceedings 16th Annual IEEE Conference on Computational Complexity*, pages 120–130. IEEE, 2001.

[11] Florian Speelman. Instantaneous non-local computation of low T-depth quantum circuits. *arXiv preprint arXiv:1511.02839*, 2015.

[12] A Chi-Chih Yao. Quantum circuit complexity. In *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*, pages 352–361. IEEE, 1993.

[13] David A Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in NC. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 1–5, 1986.

[14] Ryan O'Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014.

[15] Vince Grolmusz. On the power of circuits with gates of low l1 norms. *Theoretical computer science*, 188(1-2):117–128, 1997.

[16] Robert Alicki and Mark Fannes. Continuity of quantum conditional information. *Journal of Physics A: Mathematical and General*, 37(5):L55–L57, 2004.

[17] Andreas Winter. Tight uniform continuity bounds for quantum entropies: conditional entropy, relative entropy distance and energy constraints. *Communications in Mathematical Physics*, 347(1):291–313, 2016.

[18] Vahid R Asadi, Eric Culf, and Alex May. Rank lower bounds on non-local quantum computation. *arXiv preprint arXiv:2402.18647*, 2024.

[19] Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. Protecting data privacy in private information retrieval schemes. *Journal of Computer and System Sciences*, 60(3):592–629, 2000. ISSN 0022-0000. doi:https://doi.org/10.1006/jcss.1999.1689. URL https://www.sciencedirect.com/science/article/pii/S0022000099916896.

[20] Vahid R Asadi, Kohdai Kuroiwa, Debbie Leung, Alex May, Sabrina Pasterski, and Chris Waddell. Conditional disclosure of secrets with quantum resources. *Quantum*, 9:1885, 2025.

[21] A Yu Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997.

[22] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[23] Isaac H Kim. Catalytic z-rotations in constant t-depth. *arXiv preprint arXiv:2506.15147*, 2025.

[24] Isaac H Kim and Tuomas Laakkonen. Any Clifford+T circuit can be controlled with constant T-depth overhead. *arXiv preprint arXiv:2512.24982*, 2025.

[25] Craig Gidney. Post on X (Twitter). https://x.com/CraigGidney/status/1936285631359197210. Accessed: 2026-02-12.

[26] Mikko Möttönen, Juha J Vartiainen, Ville Bergholm, and Martti M Salomaa. Quantum circuits for general multiqubit gates. *Physical review letters*, 93(13):130502, 2004.

[27] Harry Buhrman, Serge Fehr, Christian Schaffner, and Florian Speelman. The garden-hose model. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, pages 145–158, 2013.

[28] Hartmut Klauck and Supartha Podder. New bounds for the garden-hose model. *arXiv preprint arXiv:1412.4904*, 2014.

[29] Ilan Newman. Private vs. common random bits in communication complexity. *Information processing letters*, 39(2):67–71, 1991.

[30] Benny Applebaum and Prashant Nalini Vasudevan. Placing conditional disclosure of secrets in the communication complexity universe. *Journal of Cryptology*, 34(2): 11, 2021.