Uncovering Algebraic Structures in the MPC Landscape

Navneet Agarwal[1], Sanat Anand[1], and Manoj Prabhakaran[1⋆]

Indian Institute of Technology Bombay
{navneet,sanat,mp}@cse.iitb.ac.in

Abstract. A fundamental problem in the theory of secure multi-party computation (MPC) is to characterize functions with *more than 2 parties* which admit MPC protocols with information-theoretic security against passive corruption. This question has seen little progress since the work of Chor and Ishai (1996), which demonstrated difficulties in resolving it. In this work, we make significant progress towards resolving this question in the important case of aggregating functionalities, in which m parties $P_1, \ldots, P_m$ hold inputs $x_1, \ldots, x_m$ and an aggregating party P_0 must learn $f(x_1, \ldots, x_m)$.

We uncover a rich class of algebraic structures that are closely related to secure computability, namely, "Commuting Permutations Systems" (CPS) and its variants. We present an extensive set of results relating these algebraic structures among themselves and to MPC, including new protocols, impossibility results and separations. Our results include a necessary algebraic condition and slightly stronger sufficient algebraic condition for a function to admit information-theoretically secure MPC protocols.

We also introduce and study new models of minimally interactive MPC (called UNIMPC and UNIMPC*), which not only help in understanding our positive and negative results better, but also open up new avenues for studying the cryptographic complexity landscape of multi-party functionalities. Our positive results include novel protocols in these models, which may be of independent practical interest.

Finally, we extend our results to a definition that requires UC security as well as semi-honest security (which we term *strong security*). In this model we are able to carry out the characterization of *all* computable functions, except for a gap in the case of aggregating functionalities.

1 Introduction

Secure Multi-Party Computation (MPC) is a central and unifying concept in modern cryptography. The foundations, as well as the applications, of MPC have been built up over a period of almost four decades of active

⋆ Supported by the Dept. of Science and Technology, India via the Ramanujan Fellowship and an Indo-Israel Joint Research Project grant, 2018.

research since the initial ideas emerged [SRA79,Blu81,Yao82]. Yet, some of the basic questions in MPC remain open. Specifically, the following basic problem remains open to this day for various standard notions of security (when there are no restrictions like honest majority):

Which multi-party functions admit information-theoretically secure MPC?

Indeed, one of the most basic forms of this problem remains wide open: for the case of security against passive corruption, a characterization of securely realizable functions is known only for 2-party functions [Kus89]. Chor and Ishai pointed out the difficulty of this problem, by disproving a natural conjecture for characterizing securely realizable k-party functionalities in terms of functionalities involving fewer parties [CI96]. Since then, very little progress has been made on this problem.

In this work, we make significant progress towards resolving this question in the important case of *aggregating functionalities*: In an aggregating functionality, there are m parties $P_1, \ldots, P_m$ with inputs $x_1, \ldots, x_m$ and an aggregating party P_0 must learn $f(x_1, \ldots, x_m)$. Aggregating functionalities form a practically and theoretically important class. In particular, it has been the subject of an influential line of study that started with the *minimal model for secure computation* of Feige, Kilian and Naor [FKN94]. This model – also referred to as the Private Simultaneous Messages (PSM) model [IK97] – served as a precursor of important concepts like randomized encodings [IK00] that have proven useful in a variety of cryptographic applications. Recently, a strengthening of this model, called Non-Interactive MPC (NIMPC) was introduced by Beimel et al. [BGI+14], which is closer to standard MPC in terms of the security requirements.[1] However, these models do not address the question of secure realizability in the standard model, because due to weakened security requirements, all aggregating functions are securely realizable in these models.

Towards characterizing secure realizability under (the standard model of) MPC, we uncover and examine a rich class of algebraic structures of aggregating functionalities. We exploit these structures to give new positive

[1] Both PSM and NIMPC consider protocols of the following form: a coordinator sends a private message to each of $P_1, \ldots, P_m$; each P_i uses this message and its input to compute a single message which it sends to P_0; P_0 computes an output. PSM has a corruption model in which only P_0 could be corrupted, whereas NIMPC allows any subset of the parties (other than the coordinator) to be corrupted. But when such corruption takes place, NIMPC allows the adversary to learn the *residual function* determined by the honest parties' inputs – i.e., the output for each possible setting of the inputs for the corrupt parties (unlike in MPC, where the output for only a given input of the corrupt parties is learned).

and negative results for MPC. Further, we also put forth new minimalistic, yet natural models of secure computation that arise from these results. These new models and algebraic structures, in tandem, open up new avenues for investigating the landscape of secure multiparty computation involving many parties.

Commuting Permutations Systems. We identify an algebraic-combinatorial structure called Commuting Permutations System (CPS) and interesting sub-classes thereof. CPS generalizes the function of abelian group summation to a less structured class of functions. Indeed, as a function of two inputs (denoted as $m = 2$), a CPS can be identified with a *quasigroup* operation, or equivalently the function specified by a minor of a Latin square. (For $m > 2$ inputs, CPS imputes more structure than m-dimensional Latin hypercubes.)

We define **CPS** as the class of all aggregating functions which *embed* into a CPS functionality (Definition 2). We also identify two interesting sub-classes of CPS that (as we shall see) are closely related to secure computability, corresponding to Commuting Permutation *Subgroup* Systems (CPSS) and *Complete* CPS (CCPS).

Minimal Models of MPC. In a parallel thread, we develop new minimalistic models of MPC, that help us study feasibility of information-theoretic MPC. These models (called UNIMPC* and UNIMPC) admit secure protocols only for functions which have secure protocols in the standard MPC model. We remark that ours is perhaps the first significant minimalistic model with this property, as previous minimalistic models – PSM [FKN94] and NIMPC [BGI+14] – admit secure protocols for all functions.

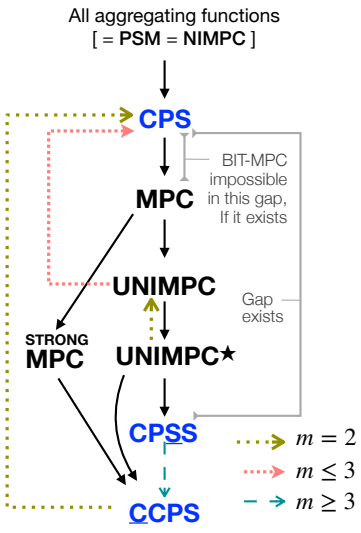

Fig. 1. The m-PC landscape of aggregating functions. The classes in blue typeface are defined in terms of algebraic/combinatorial properties, and the others in terms of secure computability. Arrow **A** → **B** indicates **A** ⊇ **B**.

UNIMPC stands for *Unassisted NIMPC* and, as the name suggests, removes the assistance from the trusted party in NIMPC: Instead the parties should securely compute the correlated randomness by themselves, in an offline phase. Unlike PSM and NIMPC, which have an incorruptible party, *UNIMPC retains the standard security model of MPC*, allowing corrup-

tion of any set of parties, and requiring the adversary to learn nothing more than the output of the function.

> *A UNIMPC protocol is an MPC protocol and can also be immediately interpreted as an NIMPC protocol.*[2]

Note that MPC and NIMPC are incomparable in the sense that an MPC protocol does not yield an NIMPC protocol (because of the general communication pattern) and an NIMPC protocol does not yield an MPC protocol (because of the use of a trusted party, and because the adversary is allowed to learn potentially more than the output of the function). Thus UNIMPC could be seen as a common denominator of these two secure computation models.

UNIMPC* corresponds to a minimalistic version of UNIMPC, with protocols which have a single round of (simultaneous) communication among the parties before they get their inputs, followed by a single message from each party to the aggregator after they receive their input. (UNIMPC allows arbitrarily many rounds of communication prior to receiving inputs.)

Strongly Secure MPC. We also study feasibility under a *stronger* model of MPC, which requires both UC security and passive security to hold simultaneously (information theoretically). Traditionally, UC security refers to the setting of active corruption, in which the security guarantees are relative to an ideal model where too the corrupt parties are actively corrupt. While stronger in general, this gives a weaker guarantee than security against passive corruption, when the corrupt parties are indeed only passively corrupt.[3] From a practical point of view, strong security (possibly weakened to hold only against PPT adversaries) is important, and arguably the "right" notion in many cases. Here we initiate the study of characterizing multi-party functionalities that are strongly securely realizable.

Relating Secure Computation to the Algebraic Classes. Our results show the rich connections between the cryptographic complexity landscape of MPC and the combinatorial/algebraic structures of the functions, as summarized in Figure 1. We briefly point out the several

[2] Replacing the views from the pre-processing phase of a UNIMPC protocol with correlated randomness from a trusted party turns it into an NIMPC protocol.

[3] E.g., a 2-party functionality in which Bob receives $a \vee b$, where $a, b \in \{0, 1\}$ are inputs to Alice and Bob respectively, has no protocol secure against passive corruption; but a protocol in which Alice simply sends a to Bob is UC secure. Also see $\mathcal{F}_{\text{AND}}$ discussed in Section 8.1.

results that go into making this map. All results relate to the information-theoretic setting with finite functions.

- **MPC** $\subseteq$ **CPS**: This result hinges on characterizing the following cryptographic property algebraically: given any subset of the inputs and the output of the function, the *residual function* of the remaining inputs can be determined. (Theorem 2.)
- **CPSS** $\subseteq$ **UNIMPC***: We establish this by developing a novel MPC protocol that generalizes the simple abelian group summation protocol to a certain class of (non-abelian) group actions (Theorem 3).
- **CPSS** $\subsetneq$ **CPS**: We give a concrete family of functions that fall into the gap between these two classes (Theorem 1). Combined with the above results, this separation leaves an intriguing gap between the necessary and sufficient conditions for MPC. (But we show in Theorem 4, that this gap disappears/reduces for a small number of input parties.)
- **CCPS** $\subseteq$ **UNIMPC***: The class **CCPS** (for Complete CPS) consists of the "Latin Hypercube" functionalities that fall within **CPS**. We show that all such functions, in more than two dimensions, are highly structured and in particular fall within **CPSS** (Theorem 5). For two dimensions, i.e., Latin squares, this is not true; but in this case a UNIMPC* protocol can be directly given for all Latin squares. Further, in this case, due to a classical result of Ryser [Rys51], **CPS** = **CCPS** (see Section 1.2).
- **UC security results**: The characterization of UC securely realizable functions has been resolved for *2 and 3-party functionalities* [CKL06,PR08], but remains open for more than 3 parties. Prabhakaran and Rosulek [PR08] showed that there are only two classes of secure function evaluation functionalities – aggregating and disseminating – that can possibly have UC secure protocols. They also gave a UC secure protocol for the "disseminated OR" functionality for 3 parties. We build on this further to show that:

  – Disseminated OR functionality with any number of players is UC securely realizable. Further, every disseminating functionality is UC securely realizable by a reduction to the disseminated OR functionality (Section 8.2).

  – Every aggregating functionality in **CCPS** has a UC secure protocol; this relies on a compiler from a strongly secure protocol for $\mathcal{F}$ (which exists only if $\mathcal{F}$ is a CPS functionality) to one for $\mathcal{F}$ restricted to a domain D (Section 8.1).

– In both these positive results, we obtain strong security (Theorem 7). Combined with the negative results (Theorem 6), this shows that

$$\mathbf{CCPS} \cup \mathbf{DISS} \subseteq \textsc{strong}\mathbf{MPC} \subseteq \mathbf{CPS} \cup \mathbf{DISS}$$

where $\textsc{strong}\mathbf{MPC}$ denotes the class of *all* functionalities (not just aggregating functionalities) that have strongly secure protocols, and **DISS** and **CCPS** are interpreted as all functionalities "isomorphic" to functionalities that are disseminating or functionalities that embed into a CCPS functionality. In Figure 1, this relationship is indicated restricted to aggregating functionalities (in which, case the extension to isomorphism – which allows all parties to have inputs and outputs – can be ignored).

□ **Additional Results and Implications:**

– Recently, Halevi et al. introduced the notion of "Best Possible Information-Theoretic MPC" (BIT-MPC) [HIKR18], by removing the trusted party and the non-interactive structure in the NIMPC model, but retaining the provision that (in the ideal-world) the adversary is allowed to learn the residual function of the honest parties' inputs. While the set of functions for which BIT-MPC is possible is a strict superset of **MPC**, the main open problem posed in [HIKR18] is whether all functions have BIT-MPC protocols. We note that for all functions in **CPS**, BIT-MPC protocols are automatically MPC protocols (because for them the residual function can be deduced from the output and the corrupt parties' own inputs). Thus if $\mathbf{CPS} \setminus \mathbf{MPC} \neq \emptyset$, then there exist functions which do not have a BIT-MPC protocol.

– Our necessity result – that $\mathbf{MPC} \subseteq \mathbf{CPS}$ – can be extended in a couple of ways (Section 5.1): Firstly, the necessity condition continues to hold even if the corruption model allowed the corruption of at most one party other than the aggregating party, if we require a UNIMPC protocol (this model could be called 1-Robust UNIMPC). Secondly, the necessity condition holds even for NIMPC (even 1-Robust NIMPC), if we required an additional security property that the adversary learns only what the output reveals (like in MPC) rather than the residual function of the honest parties (as NIMPC does).

– While our focus is on aggregating functionalities, our positive results for passive-secure MPC do yield new protocols for *symmetric functionalities* wherein all parties get the same output – as considered in [CI96]. This is because a passive-secure MPC protocol for an aggregating functionality can be readily converted into one for a symmetric functionality computing the same function.

– Since one of our results (Theorem 4) depends on the existence of NIMPC protocols, we present a simple NIMPC protocol for general functionalities in the full version. This protocol is a generalization of an NIMPC protocol in [HIJ+16] to arbitrary input domains, presented more directly in terms of the function matrix. This NIMPC protocol is more efficient and much simpler than the earlier ones in the literature [BGI+14,OY16].

We present more details of our results and techniques in Section 1.2. In the full version, we also discuss several problems that are left open by this work.

1.1 Related Work

There has been a large body of work aimed at characterizing functionalities with MPC protocols in various models (see, e.g., a survey [MPR13]). For some important classes, exact characterizations are known: this includes passive and active (stand-alone) security for 2-party deterministic functions [Kus89,KMR09,MPR09], multi-party functions with restricted adversary structures [BGW88,CCD88,HM97], multi-party functions with binary alphabet [CK91], multi-party protocols which only have public communication [KMR09], and UC security for 2-party functions [CKL06,PR08].

The characterization question for the multi-party setting (with point-to-point channels and no honest majority, for passive security) was explicitly considered in [CI96]. It was shown there that there exist m-party functions which do not have any passive-secure protocol such that the $m-1$-party function obtained by merging any two parties results in a securely realizable functionality. This problem in the context of UC security was studied in [PR08], where the terms aggregating functionality and disseminating functionality were coined.

The NIMPC model was introduced by Beimel et al. [BGI+14], inspired by the earlier work of Feige et al. [FKN94]. This was generalized to other patterns of interaction in [HIJ+16]. A computational version of UNIMPC (but with a public-key infrastructure) was recently explored in [HIJ+17].

A recent independent and concurrent work by Halevi et al. [HIKR18] overlaps with some of our results. Specifically, they also observe the fact that an MPC protocol must reveal the residual function of the honest parties to an adversary corrupting the output party, which is the staring point of our proof of Theorem 2 (they do not derive the combinatorial characterization of CPS). The transformation from NIMPC to UNIMPC

we use to prove Theorem 4 is a special case of the NIMPC to MPC compiler of [HIKR18], which forms the main tool for their positive results. Finally, as pointed out above, the main open problem left in [HIKR18] is whether there are functions with no BIT-MPC protocol, and this relates to an open problem we leave, namely whether **CPS** = **MPC**: A negative answer to our question answers that of [HIKR18] in the negative.

1.2 Technical Overview

We give a brief overview of CPS functions, and a couple of our protocols that exploit this structure.

An $m+1$ aggregating functionality involves parties $P_1, \cdots, P_m$ with inputs and an aggregator P_0 who learns the output. A classical example of an aggregating functionality that admits secure computation is the summation operation in an abelian group. As a starting point to understanding all securely computable functions, one could try to generalize this function. Consider the 3-party version of this problem, involving two input parties P_1, P_2 and an output party P_0. W.l.o.g. we can consider computing a function $f : [n_1] \times [n_2] \to [n]$, given an as a matrix M with $M_{ij} = f(i, j)$. Suppose there is a passive secure protocol Π for computing f. From the results on 2-party MPC we know that an adversary which passively corrupts $\{P_0, P_1\}$ must learn P_2's input fully (up to equivalent inputs). Then, for this protocol to be secure, even given an ideal functionality, an adversary who passively corrupts $\{P_0, P_1\}$ should be able to learn P_2's input. A passive adversary is not allowed to change the parties' inputs. Hence, for any inputs $x_1 \in [n_1], x_2 \in [n_2]$, it must be the case that $(x_1, f(x_1, x_2))$ uniquely determines x_2. Symmetrically, $(x_2, f(x_1, x_2))$ uniquely determines x_1. We refer to this as the *Latin property* of M, named after Latin squares. (Latin squares are $n \times n$ square matrices in which each row and each column is a permutation of $[n]$. Note that a square matrix with the Latin property is the same as a Latin square.)

It is easy to see that any 3-party aggregating functionality $f : [n] \times [n] \to [n]$ which is a Latin square has a passive secure protocol: P_1 and P_2 privately agree on a random permutation σ over $[n]$, and then P_1 sends P_0 the row indexed by its input x_1, but with positions permuted according to σ: i.e., a vector $(z_1, \cdots, z_n)$ where $z_{\sigma(j)} = M_{x_1,j}$. P_2 sends $k = \sigma(x_2)$ to P_0, and P_0 outputs $z_k = M_{x_1,x_2}$. Note that the security of this protocol relies on not only the Latin property, but also on the fact that each row has all n elements. However, since any rectangle with the Latin property can be embedded into an (at most quadratically larger) Latin square [Rys51],

any function f which has the Latin property does indeed have a passive secure protocol.

This might suggest that for arbitrary number of parties, an analogous Latin hypercube property would be a tight characterization of secure computability. Interestingly, this is not the case. With m input clients, the 2-party results imply that an adversary corrupting a subset of the m input parties and the aggregator P_0 can learn the *residual function* of the honest parties' inputs. Since the passive adversary cannot change the input of the corrupt parties even in the ideal world, this means that any choice of the corrupt parties' inputs should reveal the residual function of the honest parties. We identify an algebraic formulation in terms of a "Commuting Permutation System" (CPS) that captures this condition tightly.

A CPS over the output alphabet $[n]$ has input sets $X_i \subseteq S_n$, for $i = 1$ to m, where S_n is the group of all permutations of $[n]$. On input $(\pi_1, \cdots, \pi_m) \in X_1 \times \cdots \times X_m$, the output is defined as $\pi_1 \circ \cdots \circ \pi_m(1)$. The "commuting" property is the requirement that this output is invariant to the order in which the m permutations are applied to 1. Note that the commutativity needs to hold only when applied to 1. Also, it holds only *across* the sets $X_1, \cdots, X_m$. That is if $\pi, \pi' \in X_i$, it is not necessary that $\pi \circ \pi'(1)$ equals $\pi' \circ \pi(1)$. The function table of a CPS functionality is indeed a Latin hypercube, but the converse does not hold.

Being a CPS functionality is necessary to have an MPC protocol (let alone a UNIMPC protocol). Unfortunately, we do not know if this is also a sufficient condition. But given some additional structure in a CPS, we are able to give a new protocol. The additional structure that we can exploit is that each X_i is a *subgroup* of S_n, in which case we call the system a Commuting Permutation *Subgroups* System or CPSS. Exploiting this property, we design a protocol for computing CPSS functions, as discussed below.

UNIMPC Protocol for CPSS Functionalities. We present a novel protocol with perfect, information-theoretic security against passive corruption for all CPSS functionalities (and, further, is in fact, UC secure for a sub-class). Recall that the goal is to let P_0 learn $\pi_1 \circ \cdots \circ \pi_m(1)$, where π_i is a permutation that P_i receives as input. At first glance, our protocol may appear similar in structure to a protocol for an abelian group sum: each party P_i shares its input π_i as $\pi_i = \sigma_{i,0} \circ \sigma_{i,1} \circ \cdots \circ \sigma_{i,m}$, where each of the shares itself belongs to X_i. It will be helpful to visualize these shares as forming the i^{th} row in a matrix of shares. The shares in each column $(\sigma_{1,j}, \cdots, \sigma_{m,j})$ for $j \in [m]$ will be correlated with each other in some manner, so that the output can be reconstructed by aggregating

only the shares $(\sigma_{1,0}, \cdots, \sigma_{m,0})$. (An analogy for the case of the abelian group would be to choose the shares in each column to sum up to the identity element.) These shares will be sent to P_0.

But there are a couple of major differences. Firstly, permutations do not commute in general, and it is not clear how the shares can be meaningfully combined. Secondly, we *must not reveal* the composition of the inputs – i.e., the permutation $\pi_1 \circ \cdots \circ \pi_m$ – to the aggregator; only the result of applying this composition to 1 should be revealed. So, choosing the column shares to "add up to" the identity permutation would be problematic, not to mention that there may not be any such choice other than choosing all the shares to be the identity element.

In our protocol, we choose the column shares such that their composition has 1 as a fixed point (there is at least one such choice, since the each entry can be chosen as the identity permutation). Then, using the CPSS property, it can be shown that $(\prod_{i\in[m]} \sigma_{i,0})(1) = (\prod_{i\in[m]} \pi_i)(1)$ (see Figure 2). It turns out that we can use the subgroup structure in CPSS to argue that if the shares are chosen uniformly at random subject to the above constraint, then $(\sigma_{1,0}, \cdots, \sigma_{m,0})$ reveals nothing more than $\pi_1 \circ \cdots \circ \pi_m(1)$.

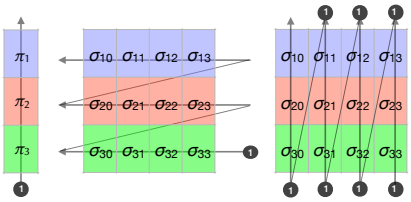

Fig. 2. Elements in the i^{th} row belong to a subgroup X_i in a CPSS. The subgroup structure enables secret-sharing as $\pi_i = \prod_{j=m}^{0} \sigma_{i,j}$. Then the illustrated quantities are equal: $(\prod_{i\in[m]} \pi_i)(1) = (\prod_{i\in[m]} \prod_{j=m}^{0} \sigma_{i,j})(1) = (\prod_{j=m}^{0} \prod_{i\in[m]} \sigma_{i,j})(1)$. The last equality relies on the closure property in the subgroup, as well as the commutativity guarantee (when applied to 1). In our protocol, for each $j > 0$, $(\prod_{i\in[m]} \sigma_{i,j})(1) = 1$, and hence this also equals $(\prod_{i\in[m]} \sigma_{i,0})(1)$.

Further, even if we consider all the shares $\sigma_{i,j}$ *except for* $(i,j) \in S \times S$ for some $S \subseteq [m]$, we show that they reveal nothing more than the residual function $\left(\prod_{i\in S} \pi_i\right)(1)$. The need to consider revealing this set of shares comes from the fact that our protocol is not an NIMPC protocol (where a trusted dealer could compute $\sigma_{i,j}$ for all $(i,j) \in [m]^2$ and send only $(\sigma_{i,1}, \cdots, \sigma_{i,m})$ to each party P_i); instead we require the parties to compute all the shares themselves, which is achieved by each party P_j computing the j^{th} column of shares, and distributing it among all the parties P_i. Thus when we consider a set S of honest parties, only the shares $\sigma_{i,j}$ where $(i,j) \in S^2$ remain hidden from the adversary.

UC-secure Protocols. It turns out that the above protocol for aggregating functions is UC secure if the function is a Complete CPSS (CCPSS) function. For $m \geq 3$, a Complete CPS is always a Complete CPSS, and

hence this gives a UC secure (in fact, strongly secure) protocol for all CCPS functionalities. (The case of $m = 2$ is handled separately.)

However, for a function that is only *embedded in* a CCPS functionality, this protocol is not necessarily UC secure (because nothing prevents an adversary from using an input from the full domain of the CCPS functionality). We give a compiler that can take a UC secure protocol for a CCPS functionality, and transform it into a UC secure protocol for the functionality restricted to a smaller domain. The main idea of the compiler is to run several instances of the original protocol with the parties using random inputs from the restricted domain. That they used inputs from the restricted domain is then verified using a cut-and-choose phase. Then, an aggregated AND functionality is used to identify instances among the unopened executions to obtain the output. Plugging in a simple UC secure protocol for aggregated AND, this compiler yields a UC secure protocol. Interestingly, though aggregated AND itself has no strongly secure protocol (or passive-secure protocol, for that matter) as it is not a CPS functionality, the resulting protocol above is a strongly secure protocol.

We remark that this is a feasibility result that relies on the domains being finite (small) as the compiler's overhead is polynomial in the domain size.

We also present a reduction from any disseminating function to the disseminated-OR functionality. This is also a feasibility result that relies on the number of parties being finite (small) as the protocol is exponential in the number of parties. To complete establishing the realizability of all disseminating functions, we give a UC secure protocol for the disseminated-OR functionality (extending a 3-party protocol for the same functionality in [PR08]).

2 Preliminaries

We write $[n]$ to denote the set $\{1, \cdots, n\}$. S_n denotes the symmetric group over $[n]$, namely, the group of all permutations of $[n]$. In our proofs, we shall use the product notation $\prod$ to denote the composition operation of permutations. Note that composition of permutations is a non-commutative operation in general, and hence the order of the indices is important (as in $\prod_{i=1}^{t} \rho_i$). When the order is not important, we denote the indices by a set (as in $\prod_{i \in [t]} \rho_i$).

Below we define notions referred to through out the paper. Additional notions relevant to strong security are deferred to Section 8.

We adapt the definition of an *aggregating functionality* from [PR08].[4]

Definition 1 (Aggregating Functionality). *An* $(m+1)$ *party* Aggregating functionality *accepts inputs* $x_i \in X_i$ *from* P_i *for* $i = 1$ *to* m*, and sends* $f(x_1, \cdots, x_m)$ *to party* P_0*, where* $f : X_1 \times \cdots \times X_m \to \Omega$ *is a fixed function.*

Consistent with the literature on feasibility questions, we consider the functions to have constant-sized domains (rather than infinite domains or domains expanding with the security parameter). Also, in all our positive results, the security obtained is perfect and hence the protocols themselves do not depend on the security parameter. Our negative results do allow protocols to have a negligible statistical error in security.

Definition 2 (Embedding). *An aggregating functionality* $f : X_1 \times \cdots \times X_m \to [n]$ *is said to* embed *into a functionality* $g : X'_1 \times \cdots \times X'_m \to [n']$ *if there exist functions* $\phi_i : X_i \to X'_i$ *for* $i \in [m]$*, and an injective function* $\phi_0 : [n] \to [n']$ *such that for all* $(x_1, \cdots, x_m) \in X_1 \times \cdots \times X_m$*,*

$$\phi_0(f(x_1, \cdots, x_n)) = g(\phi_1(x_1), \cdots, \phi_m(x_m)). \tag{1}$$

Below, $\mathcal{A} \cong \mathcal{B}$ denotes that the statistical difference between the two distributions $\mathcal{A}$ and $\mathcal{B}$ is negligible as a function of a (statistical) security parameter.

Definition 3 (Passive Secure MPC). *An* $(m+1)$*-party protocol* Π *with parties* $P_1, \cdots, P_m, P_0$ *is said to be an information-theoretically secure MPC protocol for an* $(m+1)$*-party aggregating functionality* f *against passive corruption, if for any subset* $T \subseteq [m] \cup \{0\}$*, there exists a simulator* S *s.t. for any input* $x \in X$*:*

$$\text{VIEW}_{\Pi(x)}(\{P_i | i \in T\}) \cong \begin{cases} S(x_T, f(x)) & \text{if } 0 \in T \\ S(x_T, \perp) & \text{otherwise} \end{cases}$$

where $\text{VIEW}_{\Pi(x)}(\{P_i | i \in T\})$ *represents the view of the parties* $\{P_i | i \in T\}$ *in an execution of* Π *with input* x *and* $\perp$ *represents an empty input.*

We shall use the following result for 2-party MPC, obtained from the general characterization in [KMR09].

[4] We allow only the aggregating party P_0 to have an output. The original definition in [PR08] allows all the parties to have outputs, but requires that for each party other than P_0, its output is a function only of its own input. Such a function is "isomorphic" to an aggregated functionality as we define here.

Lemma 1 (2-Party MPC with one-sided output [KMR09]). *If a finite 2-party functionality which takes inputs $x \in X$ and $y \in Y$ from Alice and Bob respectively and outputs $f(x, y)$ to Bob for some function $f : X \times Y \to Z$ has a statistically secure protocol against passive adversaries, then $\forall x, x' \in X$ it holds that $\exists y \in Y, f(x, y) = f(x', y) \Rightarrow \forall y \in Y, f(x, y) = f(x', y)$.*

We refer the reader to [BGI+14] for a definition of NIMPC and PSM.

3 New Models

In this section we define UNIMPC and UNIMPC*, which are models of secure computation, as well as combinatorial objects CPS and CPSS. For simplicity, we define UNIMPC and UNIMPC* for fixed functions rather than function families (though the definitions can be easily extended to function families, where all the input players receive the function as an input).

Definition 4 (UNIMPC). *We define an* Unassisted Non-Interactive Secure Multi-party Computation (UNIMPC) protocol Π *for an $(m+1)$-party aggregating functionality $f : X \to \Omega$ as $\Pi = (\mathcal{R}, \mathrm{Enc}, \mathrm{Dec})$ where:*

- *$\mathcal{R}$ is an m-party randomized protocol (without inputs), generating correlated views $(r_1, \cdots, r_m) \in R_1 \times \cdots \times R_m$.*
- *Enc is an m-tuple of deterministic functions $(\mathrm{Enc}_1, \cdots, \mathrm{Enc}_m)$ where $\mathrm{Enc}_i : X_i \times R_i \to M_i$.*
- *$\mathrm{Dec} : M_1 \times \cdots \times M_m \to \Omega$ is a deterministic function satisfying the following correctness requirement: for any $(x_1, \cdots, x_m) \in X$ and any view $(r_1, \cdots, r_m)$ which $\mathcal{R}$ generates with positive probability,*

$$\mathrm{Dec}((\mathrm{Enc}_1(x_1, r_1), \cdots, \mathrm{Enc}_m(x_m, r_m)) = f(x_1, \cdots, x_m).$$

It is identified with a two-phase MPC protocol where:

1. **Offline Phase:** *The parties $P_i : i \in [m]$ run $\mathcal{R}$ (without any input) so that each P_i obtains the view r_i.*
2. **Online Phase:** *Every P_i encodes its input x_i as $z_i = \mathrm{Enc}_i(x_i, r_i)$ and sends it to the aggregator P_0. P_0 outputs $\mathrm{Dec}(z_1, \cdots, z_m)$.*

Security: A UNIMPC protocol Π for $f : X \to \Omega$ is said to be T-secure *(for $T \subseteq [m]$) if there exists a simulator S s.t. for any $x \in X$:*

$$\textsc{view}_{\Pi(x)}(\{P_i | i \in T\} \cup \{P_0\}) \cong S(x_T, f(x))$$

where $\text{VIEW}_{\Pi(x)}(\cdot)$ *represents the view of a given set of parties in the two-phase protocol above, with input* x.

For any $t \in [m]$, Π *is said to be* t-robust *if it is* T*-secure* $\forall T \subseteq [m]$ *s.t.* $|T| \leq t$. *A UNIMPC protocol* Π *is said to be* secure *if it is* m*-robust.*

We point out that a secure UNIMPC protocol as defined above is a passive secure MPC protocol for f (as in Definition 3). Note that in defining T-security we considered only the case when the set of corrupt parties includes the aggregator. But when the aggregator is honest, security is automatically guaranteed by the structure of the UNIMPC protocol (the view of the adversary being derived completely from the offline phase).

Definition 5 (UNIMPC*). *We define an* Unassisted Non-Interactive Secure Multi-party Computation protocol with Non-Interactive Pre-Processing *(UNIMPC* protocol)* Π *for a functionality* $f : X \to \Omega$ *as a UNIMPC protocol* $\Pi = (\mathcal{R}, \text{Enc}, \text{Dec})$ *for* f *where* $\mathcal{R}$ *consists of a single round (i.e., each party simply sends messages to the others, and then receives all the messages sent to it).*

We define classes **MPC**, **UNIMPC**, **UNIMPC*** as the class of aggregating functionalities that have (information-theoretically) passive secure MPC, UNIMPC and UNIMPC* protocols, respectively.

4 Commuting Permutations System

In this section, we define the new algebraic-combinatorial classes.

Definition 6 (CPS and CPSS). *An* (n, m)-Commuting Permutations System *(CPS) is a collection* $(X_1, \cdots, X_m)$ *where for all* $i \in [m]$, $X_i \subseteq S_n$ *contains the identity permutation, and for any collection* $(\pi_1, \cdots .\pi_m)$ *with* $\pi_i \in X_i$, *and* $\rho \in S_m$, $\pi_1 \circ \cdots \circ \pi_m(1) = \pi_{\rho(1)} \circ \cdots \circ \pi_{\rho(m)}(1)$.[5]

It is called an (n, m)-Commuting Permutation Subgroups System *(CPSS) if each* X_i *is a subgroup of* S_n.

Note that given a CPS $(X_1, \cdots, X_m)$, for any $(\pi_1, \cdots, \pi_m) \in X_1 \times \cdots \times X_m$, the expression $(\prod_{i \in [m]} \pi_i)(1)$ is well-defined as the order of composition is not important.

Definition 7 (CCPS). *An* (n, m)*-CPS* $(X_1, \cdots, X_m)$ *is said to be* complete in dimension i *if* $\{\pi(1) \mid \pi \in X_i\} = [n]$. *If it is complete in all* m *dimensions, it is called a* Complete CPS *(CCPS).*

[5] Choice of 1 is arbitrary. Requiring identity permutation to always be part of each X_i is w.l.o.g., as a CPS without it will remain a CPS on adding it.

Definition 8. *An $(m+1)$-party aggregating functionality $f : X_1 \times \cdots \times X_m \to [n]$ is said to be a* CPS functionality *(resp.,* CPSS and CCPS functionality*) if $(X_1, \cdots, X_m)$ is an (n, m)-CPS (resp., (n, m)-CPSS and (n, m)-CCPS), and for all $(\pi_1, \cdots, \pi_m) \in X_1 \times \cdots \times X_m$, $f(\pi_1, \cdots, \pi_m) = (\prod_{i\in[m]} \pi_i)(1)$.*

CPS *(resp.,* **CPSS** *and* **CCPS***) is defined as the class of all aggregating functionalities that embed into a CPS functionality (resp., CPSS functionality and CCPS functionality).*

A CPSS enjoys a certain (non-abelian) group structure. More specifically, the CPSS $(G_1, \cdots, G_m)$ can be identified with a group, with the set of elements $G_1 \times \cdots \times G_m$ and group operation $*$ defined as $(\sigma_1, \ldots, \sigma_m) * (\sigma'_1, \ldots, \sigma'_m) = (\sigma_1 \circ \sigma'_1, \ldots, \sigma_m \circ \sigma'_m)$. This is captured in the following lemma.

Lemma 2. *Suppose $(G_1, \cdots, G_m)$ is a CPSS. Then, for any set of mt permutations $\{\sigma_{i,j} \mid i \in [m], j \in [t]\}$ such that $\sigma_{i,j} \in G_i$, it holds that*

$$\Big(\prod_{j=1}^{t}\prod_{i=1}^{m}\sigma_{i,j}\Big)(1) = \Big(\prod_{i\in[m]}\prod_{j=1}^{t}\sigma_{i,j}\Big)(1).$$

Proof: Consider $\rho \circ \prod_{i=1}^{m} \rho_i(1)$, where $\rho_i \in G_i$ for each i, and $\rho \in G_{i_0}$ for some $i_0 \in [m]$. Note that the order of composition is not important in $\prod_{i=1}^{m} \rho_i(1)$, since $(G_1, \cdots, G_m)$ is a CPS(S), and we may write it as $\prod_{i\in[m]} \rho_i(1)$. Also, define ρ'_i as

$$\rho'_i = \begin{cases} \rho \circ \rho_{i_0} & \text{if } i = i_0 \\ \rho_i & \text{otherwise.} \end{cases}$$

Since G_{i_0} is a group, we have $\rho'_i \in G_i$ for all $i \in [m]$ (including i_0). Then,

$$\Big(\rho \circ \prod_{i=1}^{m} \rho_i\Big)(1) = \Big(\rho \circ \rho_{i_0} \circ \prod_{i\in[m]\setminus\{i_0\}} \rho_i\Big)(1) = \Big(\rho'_{i_0} \circ \prod_{i\in[m]\setminus\{i_0\}} \rho'_i\Big)(1) = \Big(\prod_{i\in[m]} \rho'_i\Big)(1)$$

where in the last step, we again used the CPS property. The claim follows by repeatedly using the above equality. □

Our first result is a separation:

Theorem 1. **CPSS** $\subsetneq$ **CPS**.

Proof: We prove this by giving an explicit $(5,3)$-CPS (X_1, X_2, X_3), and showing that the corresponding CPS functionality does not embed into any $(n,3)$-CPSS functionality. (In the full version we give instances of (n,m)-CPS that cannot be embedded into a CPSS, for every value of $m \geq 2$.) Let

$$X_1 = \{\pi_0, \pi_1\}, X_2 = \{\pi_0, \pi_2\}, X_3 = \{\pi_0, \pi_3\},$$

where (using the standard cycle notation for permutations), $\pi_0 = (1)(2)(3)(4)(5)$, $\pi_1 = (1\ 2\ 5)(3\ 4)$, $\pi_2 = (1\ 3\ 5)(2\ 4)$ and $\pi_3 = (1\ 4\ 5)(2\ 3)$. It can be verified that this is a CPS by computing all non-trivial applications of these permutations on 1: $\prod_{i\in\{1,2,3\}} \pi_i(1) = 5$, $\prod_{i\in\{1,2\}} \pi_i(1) = 4$, $\prod_{i\in\{1,3\}} \pi_i(1) = 3$, and $\prod_{i\in\{2,3\}} \pi_i(1) = 2$.

We argue that this cannot be embedded into a CPSS. Suppose, for some n, there is an $(n,3)$-CPSS, (G_1, G_2, G_3), and functions $\phi_i : X_i \to G_i$ and an injective function $\phi_0 : [5] \to [n]$, as specified in Definition 2. Let $\phi_i(\pi_0) = \sigma_i$ and $\phi_i(\pi_i) = \rho_i$. First, we argue that w.l.o.g., we can require all σ_i to be the identity function. This is because, otherwise, $\hat{\phi}_i(\pi) = \sigma_i^{-1} \circ \phi_i(\pi)$ and $\hat{\phi}_0 = (\sigma_1 \circ \sigma_2 \circ \sigma_3)^{-1} \circ \phi_0$ is a valid embedding, with $\hat{\phi}_i(\pi_0)$ being the identity function. This follows from the fact (see Lemma 2) that in a CPSS with $\{\alpha_i, \beta_i\} \subseteq G_i$,

$$(\alpha_1 \circ \beta_1) \circ \cdots \circ (\alpha_m \circ \beta_m)(1) = (\alpha_1 \circ \cdots \circ \alpha_m) \circ (\beta_1 \circ \cdots \circ \beta_m)(1).$$

Next we argue that (with σ_i being identity), w.l.o.g., ϕ_0 is the identity function as well. This is because $\hat{\phi}_i(\pi) = \phi_0 \circ \phi_i(\pi)\phi_0^{-1}$, along with $\hat{\phi}_0$ being the identity function yields an embedding. This relies on the fact that $\phi_0(1) = 1$ (as implied by Equation 1 of Definition 2, by considering $x_1 = x_2 = x_3 = \pi_0$).

Now, we derive a contradiction from the following two requirements:

- From Equation 1, we get that $\pi_i(a) = \rho_i(a)$ for all i and $a \in \{1,2,3,4\}$ (but not necessarily for $a = 5$).
- Since (G_1, G_2, G_3) is a CPSS, we require that $\rho_2^2 \in G_2$. Then, we require that $\rho_2^2 \circ \rho_3(1) = \rho_3 \circ \rho_2^2(1)$.

Using the first condition, we derive three equalities: $\rho_3(1) = 4$, $\rho_2^2 \circ \rho_3(1) = 4$ and $\rho_3 \circ \rho_2^2(1) = \rho_3(5)$. From the last two equalities, and the second condition, we find that $\rho_3(5) = 4$, yielding a contradiction with the first equality. □

5 Only CPS Functionalities have (UNI)MPC Protocols

We show that if an aggregating functionality has a statistically secure MPC protocol against semi-honest adversaries (without honest majority or setups), then it must be a CPS functionality. Since UNIMPC protocols are MPC protocols, this applies to UNIMPC as well.

Theorem 2. *If an aggregating functionality has an information-theoretically secure MPC protocol against semi-honest adversaries, then it embeds into a CPS functionality.*

Proof: Suppose an $(m+1)$-party aggregating functionality $f : X_1 \times \cdots \times X_m \to [n]$ is semi-honest securely realizable. Denote the aggregating party as P_0 and for each $i \in [m]$, the party with input domain X_i as P_i.

Firstly, w.l.o.g., we may assume that no party has two *equivalent inputs*, by considering an embedding if necessary. Further, we may let $X_i = [n_i]$ for each i, and $f(1, \cdots, 1) = 1$, by relabeling the inputs and the outputs.

Now, for each $i \in [m]$, consider the 2-party SFE functionality obtained by grouping parties $\{P_j | j \in [m] \setminus \{i\}\}$ as a single party Alice, and the parties $\{P_i, P_0\}$ as a single party Bob. This functionality has the form in Lemma 1, namely, only Bob has any output. Then applying the lemma, we get the following (where the notation $\mathbf{x}[i : \ell]$ denotes the vector obtained from $\mathbf{x}$ by setting x_i to ℓ): $\forall \mathbf{x}, \mathbf{x}' \in X_1 \times \cdots \times X_m$,

$$f(\mathbf{x}) = f(\mathbf{x}') \text{ and } x_i = x'_i \;\Rightarrow\; \forall \ell \in X_i, f(\mathbf{x}[i : \ell]) = f(\mathbf{x}'[i : \ell]). \quad (2)$$

We use this to prove the following claim.

Claim. For each $i \in [m]$ and $\ell \in X_i$, there exists a permutation $\pi_\ell^{(i)}$ such that, for all $\mathbf{x} \in X_1 \times \cdots \times X_m$ with $x_i = 1$,

$$\pi_\ell^{(i)}(f(\mathbf{x})) = f(\mathbf{x}[i : \ell]). \quad (3)$$

Proof: Fix $i \in [m]$, $\ell \in X_i$. Now, consider defining a (partial) function $\pi_\ell^{(i)}$ using Equation 3. This is well-defined thanks to Equation 2: Even though there could be multiple $\mathbf{x}$ with $x_i = 1$ and the same value for $f(\mathbf{x})$, Equation 2 ensures that they all lead to the same value for $f(\mathbf{x}[i : \ell])$.

Further, with this definition, if $\pi_\ell^{(i)}(a) = \pi_\ell^{(i)}(b)$, this means that there exist $\mathbf{x}, \mathbf{x}'$ with $x_i = x'_i = 1$, $f(\mathbf{x}) = a$, $f(\mathbf{x}') = b$ and $f(\mathbf{x}[i : \ell]) = f(\mathbf{x}'[i : \ell])$. But by considering $\mathbf{z} = \mathbf{x}[i : \ell]$, $\mathbf{z}' = \mathbf{x}'[i : \ell]$, we have $z_i = z'_i$ and $f(\mathbf{z}) = f(\mathbf{z}')$. Hence, by Equation 2, we have $f(\mathbf{z}[i : 1]) = f(\mathbf{z}'[i : 1]$. But

since $\mathbf{x} = \mathbf{z}[i:1]$ and $\mathbf{x}' = \mathbf{z}'[i:1]$, this means that $a = f(\mathbf{x}) = f(\mathbf{x}') = b$. Hence, $\pi_\ell^{(i)}$ is a one-to-one function, from $\{a | \exists \mathbf{x}, x_i = 1, f(\mathbf{x}) = a\} \subseteq [n]$ to $[n]$. We can arbitrarily extend this to be a permutation over $[n]$ to meet the condition in the claim. □

Finally, for any $\mathbf{x}$ such that $x_{i_1} = \cdots = x_{i_t} = 1$, and distinct $i_1, \cdots, i_t$, by iteratively applying Equation 3, $\pi_{\ell_t}^{(i_t)} \circ \cdots \circ \pi_{\ell_1}^{(i_1)}(f(\mathbf{x})) = f(\mathbf{x}[i_1 : \ell_1] \cdots [i_t : \ell_t])$. Taking $(i_k, \ell_k) = (\rho(k), z_{\rho(k)})$ for any permutation $\rho \in S_m$ and any $\mathbf{z} \in X_1 \times \cdots \times X_m$, we have $\mathbf{x}[i_1 : \ell_1] \cdots [i_m : \ell_m] = \mathbf{z}$, for any $\mathbf{x}$. Then, with $\mathbf{x} = (1, \cdots, 1)$ we get that

$$f(\mathbf{z}) = \pi_{z_{\rho(1)}}^{(\rho(1))} \circ \cdots \circ \pi_{z_{\rho(m)}}^{(\rho(m))}(1),$$

where we substituted $f(\mathbf{x}) = 1$. This concludes the proof that f embeds into the CPS functionality with input domains $\hat{X}_i = \{\pi_\ell^{(i)} | \ell \in [n_i]\}$. □

5.1 Extensions to 1-Robust UNIMPC and NIMPC

Since every secure UNIMPC protocol is a secure MPC protocol, Theorem 2 applies to UNIMPC as well. But it extends to UNIMPC in a stronger manner than it holds for MPC. Note that if we restrict the number of corrupt parties to be at most $m/2$, then every $m+1$ party functionality has a passive secure MPC protocol, even if the functionality is a non-CPS aggregating functionality. But we show that as long as the adversary can corrupt just two parties (the aggregator and one of the input parties), the only aggregating functionalities that have secure UNIMPC protocols are CPS functionalities.

To see this, we consider how Equation 2 was derived in the proof of Theorem 2 (the rest of the argument did not rely on the protocol). We used the given $(m+1)$-party protocol to derive a secure 2-party protocol to which Lemma 1 was applied. In arguing that this 2-party protocol is secure we considered two corruption patterns in the original protocol: the adversary could corrupt $\{P_0, P_i\}$ (Bob) or $\{P_j \mid j \in [m] \backslash \{i\}\}$ (Alice). Now, if we allow only corruption of up to two parties, we cannot in general argue that the resulting two party protocol is secure when Alice is corrupted. However, if the starting protocol was a UNIMPC protocol, then in the resulting 2-phase protocol, there is an offline phase when Alice and Bob interact without using their inputs, and after that Alice sends a single message to Bob in the second phase. *Any such protocol* is secure against the corruption of Alice, as Alice's view can be perfectly simulated without Bob's input. Thus, when the starting protocol is a UNIMPC protocol that

is T-secure for every T of the form $\{0, i\}$ ($i \in [m]$), then Lemma 1 applies to the 2-party protocol constructed, and the rest of the proof goes through unchanged. Thus, an aggregating functionality f has a 1-robust UNIMPC protocol only if it is a CPS functionality.

The above argument extends in a way to 1-robust NIMPC as well. Of course, every function has a secure NIMPC protocol [BGI+14], and we cannot require all such functions to be CPS. But we note that NIMPC turned out to be possible for all functions not only because a trusted party is allowed (to generate correlated randomness), but also because NIMPC allows the adversary (corrupting the aggregator and some set of parties) to learn the residual function of the honest parties' inputs. So, one may ask for which functionalities does the adversary *learn nothing more than the output of the function* on any input (just as in the security requirement for MPC), even as we allow a trusted party to generate correlated randomness. Here, we note that the above argument in fact extends to the NIMPC setting with the trusted party: We simply include the trusted party as part of Alice in the above 2-party protocol. Since the security of the 2-party protocol relied only on security against Bob (and the 2-phase nature of the protocol), including the trusted party as part of Alice does not affect our proof. Thus we conclude that only CPS functionalities have 1-robust NIMPC where the simulator takes only the input of the corrupt parties and the output of the function (rather than the residual function of the honest parties' inputs).

6 UNIMPC Protocols

In this section we present our positive results for UNIMPC* and UNIMPC (Theorem 3 and Theorem 4).

Theorem 3. *Any function embeddable in a CPSS function has a UNIMPC* protocol with perfect security.*

To prove Theorem 3 it is enough to present a perfectly secure protocol for a CPSS function: the protocol retains security against passive corruption when the input domains are restricted to subsets.

UNIMPC* Protocol for CPSS Function.

For $i \in [m]$, party P_i has input $\pi_i \in G_i$, where $(G_1, \cdots, G_m)$ is an (n, m)-CPSS. Party P_0 will output $\pi_1 \circ \cdots \circ \pi_m(1)$.

1. **Randomness Computation:** For each $j \in [m]$, P_j samples $(\sigma_{1j}, \cdots, \sigma_{mj})$ uniformly at random from $G_1 \times \cdots \times G_m$, conditioned on
$$\sigma_{1j} \circ \sigma_{2j} \circ \cdots \circ \sigma_{mj}(1) = 1. \tag{4}$$
For each $i, j \in [m]$, P_j sends σ_{ij} to P_i.
2. **Input Encoding:** P_i computes $\sigma_{i0} := \pi_i \circ (\sigma_{i1} \circ \cdots \circ \sigma_{im})^{-1}$, and sends it to P_0. Note that $(\sigma_{i0}, \cdots, \sigma_{im})$ is an additive secret-sharing of π_i in the group G_i.
3. **Output Decoding:** P_0 outputs $\sigma_{1,0} \circ \sigma_{2,0} \circ \cdots \circ \sigma_{m,0}(1)$.

By construction, the protocol has the structure of a UNIMPC* protocol. Indeed, it is particularly simple for a UNIMPC* protocol in that the randomness computation protocol in offline phase is a single round protocol. Below we argue that this protocol is indeed a perfectly secure protocol for computing $\left(\prod_{i\in[m]} \pi_i\right)(1)$ against passive corruption of any subset of parties.

Perfect Correctness: The output of P_0 is $\prod_{i=0}^m \sigma_{i,0}(1)$. By Equation 4 (applied to $j = 1$) we may write $1 = \prod_{i=1}^m \sigma_{i1}(1)$. We further expand 1 in this expression again by applying Equation 4 successively for $j = 2, \cdots, m$ to obtain $1 = \prod_{j=1}^m \prod_{i=1}^m \sigma_{ij}(1)$. Hence, the output of P_0 may be written as $\prod_{j=0}^m \prod_{i=1}^m \sigma_{i,j}(1)$. By Lemma 2, this equals $\prod_{i\in[m]} \prod_{j=0}^m \sigma_{ij}(1)$. By the definition of $\sigma_{i,0}$ this in turn equals $\prod_{i\in[m]} \pi_i(1)$, as desired.

Perfect Semi-Honest Security: A protocol with the UNIMPC structure is always perfectly semi-honest secure as long as the aggregator is honest, or if all the input parties are corrupt. Hence we focus on the case when the aggregator P_0 is corrupt and there is at least one honest party. Suppose the adversary corrupts P_0 and $\{P_i \mid i \in S\}$ for some set $S \subsetneq [m]$. Below, we write $\overline{S} := [m] \setminus S$ to denote the set of indices of the honest parties. Recall that an execution of the protocol (including the inputs) is fully determined by the $m \times (m+1)$ matrix $\boldsymbol{\sigma}$, with $(i,j)^{\text{th}}$ entry $\sigma_{ij} \in G_i$, for $(i,j) \in [m] \times ([m] \cup \{0\})$. The input determined by $\boldsymbol{\sigma}$ is defined by $\mathsf{input}(\boldsymbol{\sigma}) = (\pi_1, \cdots, \pi_m)$, where $\pi_i = \prod_{j=0}^m \sigma_{ij}$. We say that $\boldsymbol{\sigma}$ is valid if for every $j \in [m]$, $\prod_{i\in[m]} \sigma_{ij}(1) = 1$.

When the functionality is invoked with inputs $\boldsymbol{\pi} = (\pi_1, \cdots, \pi_m)$, in the ideal world, the adversary learns only the corrupt parties' inputs $\boldsymbol{\pi}|_S$ and the residual function of the honest parties' inputs $\pi_{\overline{S}}(1)$, where $\pi_{\overline{S}} := \left(\prod_{i\in\overline{S}} \pi_i\right)$. But in the real world its view consists also $\langle\boldsymbol{\sigma}\rangle_S := \{\sigma_{ij} \mid i \in S \vee j \in S \cup \{0\}\}$. We need to show that for any two input vectors $\boldsymbol{\pi}, \boldsymbol{\pi}'$ with identical ideal views for the adversary – i.e., $\boldsymbol{\pi}|_S = \boldsymbol{\pi}'|_S$, and $\pi_{\overline{S}}(1) = \pi'_{\overline{S}}(1)$ – the distribution of $\langle\boldsymbol{\sigma}\rangle_S$ is also identical. For this we

shall show a bijective map $\phi_S^{\boldsymbol{\pi}'}$ between valid matrices $\boldsymbol{\sigma}$ consistent with $\boldsymbol{\pi}$ and those consistent with $\boldsymbol{\pi}'$, which preserves $\langle \boldsymbol{\sigma} \rangle_S$. Since $\boldsymbol{\sigma}$ is distributed uniformly over all valid matrices consistent with the input in the protocol, this will establish that the distribution of $\langle \boldsymbol{\sigma} \rangle_S$ is identical for $\boldsymbol{\pi}$ and $\boldsymbol{\pi}'$. More precisely, the following claim completes the proof.

Claim. For any $S \subsetneq [m]$, and any $\boldsymbol{\pi}, \boldsymbol{\pi}' \in G_1 \times \cdots \times G_m$ such that $\boldsymbol{\pi}|_S = \boldsymbol{\pi}'|_S$ and $\boldsymbol{\pi}_S(1) = \boldsymbol{\pi}'_S(1)$, there is is a bijection $\phi_S^{\boldsymbol{\pi}'}$ from $\{\boldsymbol{\sigma} \mid \mathsf{input}(\boldsymbol{\sigma}) = \boldsymbol{\pi} \wedge \boldsymbol{\sigma} \text{ valid}\}$ to $\{\boldsymbol{\sigma} \mid \mathsf{input}(\boldsymbol{\sigma}) = \boldsymbol{\pi}' \wedge \boldsymbol{\sigma} \text{ valid}\}$, such that $\langle \boldsymbol{\sigma} \rangle_S = \langle \phi_S^{\boldsymbol{\pi}'}(\boldsymbol{\sigma}) \rangle_S$.

Proof: Let $S, \boldsymbol{\pi}, \boldsymbol{\pi}'$ be as in the lemma. We shall first define $\phi_S^{\boldsymbol{\pi}'}$ for all $m \times (m+1)$ matrices $\boldsymbol{\sigma}$, with $\sigma_{ij} \in G_i$, and then prove the claimed properties when restricted to the domain in the claim. Fix $h \in \overline{S}$ as (say) the smallest index in $\overline{S}$. Given $\boldsymbol{\sigma}$, $\phi_S^{\boldsymbol{\pi}'}$ maps it to $\boldsymbol{\sigma}'$ as follows.

$$\sigma'_{ij} = \begin{cases} \sigma_{ij} & \text{if } j \neq h \\ \alpha_i^{-1} \circ \pi'_i \circ \beta_i^{-1} & \text{if } j = h \end{cases}$$

where $\alpha_i := \prod_{j=0}^{h-1} \sigma_{ij}$ and $\beta_i := \prod_{j=h+1}^{m} \sigma_{ij}$. Note that like $\boldsymbol{\sigma}$, $\boldsymbol{\sigma}'$ also satisfies the condition that $\sigma'_{ij} \in G_i$ for all $j = 0 \cup [m]$, because $\alpha_i, \beta_i, \pi'_i \in G_i$.

By construction, $\prod_{j=0}^{m} \sigma'_{ij} = \pi'_i$, and hence the image of $\phi_S^{\boldsymbol{\pi}'}$ is contained in $\{\boldsymbol{\sigma}' \mid \mathsf{input}(\boldsymbol{\sigma}') = \boldsymbol{\pi}'\}$. Also, when the domain is $\{\boldsymbol{\sigma} \mid \mathsf{input}(\boldsymbol{\sigma}) = \boldsymbol{\pi}\}$, the mapping is invertible since $\phi_S^{\boldsymbol{\pi}}(\phi_S^{\boldsymbol{\pi}'}(\boldsymbol{\sigma})) = \boldsymbol{\sigma}$, when $\mathsf{input}(\boldsymbol{\sigma}) = \boldsymbol{\pi}$. Hence, by symmetry, this is a bijection from $\{\boldsymbol{\sigma} \mid \mathsf{input}(\boldsymbol{\sigma}) = \boldsymbol{\pi}\}$ to $\{\boldsymbol{\sigma} \mid \mathsf{input}(\boldsymbol{\sigma}) = \boldsymbol{\pi}'\}$. Further, for $i \in S$, $\pi_i = \pi'_i$ and hence $\sigma'_{ih} = \sigma_{ih}$, so that $\langle \boldsymbol{\sigma}' \rangle_S = \langle \boldsymbol{\sigma} \rangle_S$.

It remains to prove that the map is a bijection when the domain and range are restricted to *valid* matrices. So, suppose $\boldsymbol{\sigma}$ is a valid matrix. Then we have

$$(\prod_{i \in [m]} \sigma_{ij})(1) = 1 \qquad \forall j \in [m] \tag{5}$$

$$(\prod_{i \in [m]} \beta_i)(1) = (\prod_{j=h+1}^{m} \prod_{i \in [m]} \sigma_{ij})(1) = 1. \tag{6}$$

where the first equality in (6) is obtained by applying Lemma 2, and the second by applying the validity condition (5) successively for $j = m, \cdots, h+1$.

To verify that $\boldsymbol{\sigma'} = \phi_S^{\boldsymbol{\pi}'}(\boldsymbol{\sigma})$ is valid, we only need to verify that $(\prod_{i\in[m]} \sigma'_{ih})(1) = 1$ (as the other columns of $\boldsymbol{\sigma'}$ are the same as in $\boldsymbol{\sigma}$). This we show as follows (where for brevity, we write $\alpha := \prod_{i\in[m]} \alpha_i$ and $\beta := \prod_{i\in[m]} \beta_i$):

$$
\begin{aligned}
&\prod_{i\in[m]} \pi'_i(1) = \prod_{i\in[m]} \pi_i(1) \\
&\quad\Rightarrow (\prod_{i\in[m]} \alpha_i \circ \sigma'_{ih} \circ \beta_i)(1) = (\prod_{i\in[m]} \alpha_i \circ \sigma_{ih} \circ \beta_i)(1) \\
&\quad\Rightarrow \alpha \circ (\prod_{i\in[m]} \sigma'_{ih}) \circ \beta(1) = \alpha \circ (\prod_{i\in[m]} \sigma_{ih}) \circ \beta(1) && \text{by Lemma 2} \\
&\quad\Rightarrow (\prod_{i\in[m]} \sigma'_{ih}) \circ \beta(1) = (\prod_{i\in[m]} \sigma_{ih}) \circ \beta(1) && \alpha \text{ a permutation} \\
&\quad\Rightarrow (\prod_{i\in[m]} \sigma'_{ih})(1) = (\prod_{i\in[m]} \sigma_{ih})(1) = 1 && \text{by (6) and (5).}
\end{aligned}
$$

□

Theorem 4. *Any CPS functionality with 4 or fewer parties has a UNIMPC protocol with perfect security. Further, any CPS functionality with 3 or fewer parties has a UNIMPC* protocol with perfect security.*

We present the full proof in the full version. In particular, for the case of 4 parties, we describe a UNIMPC protocol, which uses an NIMPC scheme $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$, but implements Gen using a 3-party perfectly secure protocol for general functions that is secure against passive corruption of 1 party (e.g., the passive-secure protocol in [BGW88]). This transformation has appeared in a recent, independent work [HIKR18].

7 Latin Hypercubes

CPS functions are closely related to Latin Squares, and more generally, *Latin Hypercubes*. An n-ary Latin Square is an $n \times n$ matrix with entries from $[n]$ such that each row and column has all elements of $[n]$ appearing in it. The m-dimensional version is similarly a tensor indexed by m-dimensional vectors, so that every "row" (obtained by going through all values for one coordinate of the index, keeping the others fixed) is a permutation of $[n]$. We can associate an m-input functionality with a Latin hypercube, which maps the index vector to the corresponding entry in the hypercube.

In the case of $m = 2$, an n-ary Latin square functionality f always is (or, technically, embeds into) an $(n, 2)$-CPS (X_1, X_2).[6] However, this is not true in higher dimensions (see the full version for an explicit counter example). So not all Latin hypercube functions can have MPC protocols. We obtain an exact characterization of all Latin hypercube functionalities that have UNIMPC* (or MPC) protocols. Recall that by Theorem 2 only CPS functionalities can have UNIMPC* (or even MPC) protocols. We show that *all Latin hypercube functionalities that are CPS functionalities indeed have UNIMPC* protocols*. To prove this, we relate this class — Latin hypercube functionalities that are CPS functionalities — to CPSS functionalities (which have UNIMPC* protocols). Firstly, a Latin hypercube functionality that is a CPS functionality forms a Complete CPS (CCPS) functionality, as defined in Definition 7. Then we use the following theorem:

Theorem 5. *For $m > 2$, an (n, m)-CCPS is an (n, m)-CPSS.*

The proof of this theorem, given in the full version, has two parts: Firstly, we show that for $m > 2$, the permutations in an (n, m)-CCPS enjoy "*full*-commutativity," rather than commutativity when applied to 1. Then we show that any (n, m)-CPS functionality with such full-commutativity embeds into an (n, m)-CPSS. Further, since a CCPS has the maximal number of possible inputs for every party in a CPS (namely, n), this embedding must use a surjective mapping for the inputs, making the original CCPS itself a CPSS.

The following can be stated as a corollary of the above theorems (see the full version).

Corollary 1. *A Latin hypercube functionality has a UNIMPC* protocol if and only if it is a CPS functionality.*

8 Towards a Characterization of Strong Security

While security against active corruption is often stronger than security against passive corruption, this is not always the case. This is because, in the ideal world model for active corruption, the adversary (i.e., simulator) is allowed to send any inputs of its choice to the functionality, the

[6] We let $X_1 = \{\pi_i \mid \pi_i(f(1, j)) = f(i, j)\ \forall j \in [n]\}$, and $X_2 = \{\rho_j \mid \rho_j(f(i, 1)) = f(i, j)\ \forall i \in [n]\}$. These functions are well-defined permutations because of f being a Latin square functionality, and it is a CPS because, $\pi_i \circ \rho_j(f(1, 1)) = \rho_j \circ \pi_i(f(1, 1)) = f(i, j)$. With a bijective embedding that relabels the outputs of f so that $f(1, 1) = 1$, this meets the definition of a CPS.

adversary in the passive corruption setting is required to send the same input as the corrupt parties received. To reconcile this discrepancy, one could weaken the notion of passive security by allowing the simulator to change the input sent to the functionality. However, the resulting security guarantee is quite pessimistic, as it assumes that even passively corrupt parties will alter their inputs, and may not be appropriate in scenarios where the passively corrupt parties will not do so (see Footnote 3). Instead, we propose using a stronger definition – which we simply call *strong security* – which requires the simulator to not alter the inputs if the parties are corrupted passively, but allows it to use arbitrary inputs if they are corrupted actively. Formally, we use the following information-theoretic security definition:

Definition 9 (Strong security). *A protocol Π is said to be a* strongly secure *protocol for a functionality $\mathcal{F}$ if it is both passive secure and UC secure (with selective abort) for $\mathcal{F}$ against computationally unbounded adversaries.*

Note that strong security admits composition as both semi-honest security and UC security are composable. From a practical point of view, strong security (possibly weakened to hold only against PPT adversaries) is important, and arguably the "right" notion in many cases. Here we initiate the study of characterizing multi-party functionalities that are strongly securely realizable. Clearly, the impossibility results for both UC security and passive security apply to strong security.

To state our results for *all* multi-party functions, we need to go beyond aggregating functionalities. Firstly, we shall need the notion of disseminating functionalities: An $(m+1)$-party disseminating functionality $f = (f_1, \cdots, f_m)$ has a single party P_0 with an input x, so that every other party P_i receives the output $f_i(x)$. The class of disseminating functions is denoted by **DISS**. Secondly, we need to consider functions which are "essentially" aggregating or disseminating, but not strictly so because of the presence of additional information in each party's local output which is derived solely from its own inputs. The idea that a function can be *essentially the same* as another function is captured using the notion of isomorphism among functionalities, as defined in [MPR13]. We reproduce this below, adapted to strong security. Here, a protocol $\pi^{\mathcal{G}}_{\mathcal{F}}$ for $\mathcal{F}$, using $\mathcal{G}$ as a setup, is said to be *local* if each party (deterministically) maps its input to an input for the functionality $\mathcal{G}$, then calls $\mathcal{G}$ once with that input and, based on their private input and the output obtained from $\mathcal{G}$, locally computes the final output (deterministically), without any other communication.

Definition 10 (Isomorphism [MPR13]). *We say $\mathcal{F}$ and $\mathcal{G}$ are* isomorphic *to each other if there exist two local protocols $\pi_{\mathcal{F}}^{\mathcal{G}}$ and $\pi_{\mathcal{G}}^{\mathcal{F}}$ that strongly securely realize $\mathcal{F}$ and $\mathcal{G}$ respectively.*

Now we are ready to state and prove our main results regarding strongly secure MPC.

Theorem 6. *If a functionality has a strongly secure protocol, then it is isomorphic to a functionality in* **DISS** $\cup$ **CPS**.

Proof: It follows from [PR08] that all strongly securely realizable functionalities are isomorphic to a *disseminating* functionality (i.e., a functionality in **DISS**), or an *aggregating* functionality (as defined in here).Further, if a functionality $\mathcal{F}$ that has a strongly secure protocol is isomorphic to an aggregating functionality $\mathcal{F}'$, then from the definition of isomorphism, $\mathcal{F}'$ too has a strongly secure (and in particular, a passive secure) protocol. Then, by Theorem 2, $\mathcal{F}' \in$ **CPS**. □

We contrast this with our positive result below, which refers to **CCPS** (Definition 7), instead of **CPS**. We point out that our protocols below are efficient in the sense of having polynomial complexity in the statistical security parameter, but can be polynomial (rather than logarithmic) in the domain sizes or exponential in the number of parties.

Theorem 7. *If a functionality is isomorphic to one in* **DISS** $\cup$ **CCPS**, *then it has a strongly secure protocol.*

Proof: We show in Section 8.2 that every disseminating functionality has a UC secure protocol. A UC secure protocol for a disseminating functionality is always passive secure as well: only the disseminator has any input, and if the disseminator is passively corrupt, the correctness guarantee under UC security (when no party is corrupt) ensures that the simulator can send the disseminator's actual input to the functionality.

In the full version, we prove that the UNIMPC* protocol in Section 6 is UC secure for every Complete CPSS functionality. By Theorem 5, this covers all Complete CPS functionalities of more than 2 dimensions. For 2-dimensional Complete CPS functionalities (which are precisely Latin Squares), we give a UC secure protocol in the full version. In Section 8.1, we show a compiler that extends these results to functionalities embedded in a CCPS functionality.

Finally, we note that for aggregating CPS functionalities too, UC security implies strong security: If the aggregator is honest, the correctness guarantee under UC security allows the simulator to send the corrupt

parties' actual input to the functionality; if the aggregator is corrupt, a simulator which sends the correct inputs of the passively corrupt players obtains the honest parties' residual function, and can internally execute the UC simulator (which may send arbitrary inputs to the functionality and expect the output). □

8.1 Restricting Input Domains While Retaining UC Security

In this section we give a compiler to transform a UC secure protocol for a CPS functionality $\mathcal{F}$ to a UC secure protocol for the same functionality, but with restricted input domains for each party. To illustrate the need for this compiler, suppose m input parties wish to total their votes (0 or 1) and provide it to an aggregator, securely. We do have a UC secure protocol for addition modulo $m+1$, and this functionality can correctly compute the total of m bits. However, this is not a UC secure protocol for our functionality, as the corrupt parties can provide inputs other than 0 or 1. Nevertheless, we show that the original protocol can be transformed into one which restricts the domain as desired.

Definition 11 (Domain Restriction). *Given a functionality $\mathcal{F}$ with input domain $X = X_1 \times \cdots \times X_m$, we define a* domain restriction of $\mathcal{F}$ to $D = D_1 \times \cdots \times D_m \subseteq X$ *as a functionality $\mathcal{F}_D$ which is defined only on inputs in D, where it behaves identically as $\mathcal{F}$.*

We give a compiler that transforms a UC secure protocol for a CPS functionality $\mathcal{F}$ to a UC secure protocol for $\mathcal{F}_D$ for any $D = D_1 \times \cdots \times D_m$. Our compiler can be presented as a protocol $\mathsf{RDom}_D^{\mathcal{F},\mathcal{F}_{\mathrm{AND}}}$ – a protocol in a hybrid model with access to the ideal functionalities $\mathcal{F}$ and (m-input) aggregating functionality $\mathcal{F}_{\mathrm{AND}}$. We note that while $\mathcal{F}_{\mathrm{AND}}$ is not a CPS functionality (and hence cannot have a passive secure protocol), it does have a UC secure protocol. Specifically, one can reduce $\mathcal{F}_{\mathrm{AND}}$ to summation over an exponentially large abelian group, where each party P_i maps its input x_i to a group element g_i as follows: if $x_i = 0$, let g_i be random, and if $x_i = 1$, let $g_i = 0$. The aggregator receives $\sum_i g_i$ and outputs 1 if the sum is 0, and 0 otherwise.

Protocol $\mathsf{RDom}_D^{\mathcal{F},\mathcal{F}_{\mathrm{AND}}}$ The high-level idea of this protocol is to first invoke $\mathcal{F}$ on random inputs from the domain D, and use a cut-and-choose phase to verify that indeed most of the invocations used inputs in the domain D. Then, using access to $\mathcal{F}_{\mathrm{AND}}$, the executions involving the correct input from all the parties are isolated, and the aggregator P_0 outputs what

it received from $\mathcal{F}$ in those executions (if there is a consistent output). The formal description follows.

Let $\mathcal{F}$ represent the functionality to be realized and k be the security parameter. Let $\mathcal{E}$ be the input domain of $\mathcal{F}$ and D be the desired domain. Let $P_i, i \in [m] \cup \{0\}$ be the set of parties with inputs $\{x_i\}_{i\in[m]}$. Let P_0 be the aggregator with output space $[n]$.

1. **Random Execution:** Invoke k sessions of the functionality $\mathcal{F}$ with domain $\mathcal{E}$. Each honest party $P_i, i \in [m]$ chooses input uniformly at random from domain D. Let u_{ij} be the input used by party P_i in the j^{th} execution and let v_j be its output.
2. **Opening:** P_0 chooses $S \subseteq [k]$, where every element has a probability of 0.5 of being picked up (thus $\mathbb{E}(|S|) = k/2$), and announces it. Every party $P_i, i \in [m]$ sends $u_{ij}, \forall j \in S$ to P_0. Then, P_0 checks the consistency of all the inputs and outputs it received: i.e., if $\forall j \in S$, $\mathcal{F}(\{u_{ij}\}_{i\in[m]}) = v_j$. It also confirms that each input is chosen from the domain D. Otherwise P_0 aborts.
3. **Tallying with actual inputs:** Invoke $k - |S|$ sessions of the $\mathcal{F}_{\text{AND}}$ functionality, indexed by $\bar{S} = [m] \setminus S$. Each honest party P_i sets its input to session j of $\mathcal{F}_{\text{AND}}$ a_{ij} as

$$a_{ij} = \begin{cases} 1 & \text{if } v_{ij} = x_i \\ 0 & \text{otherwise} \end{cases}$$

   and let the output for j^{th} $\mathcal{F}_{\text{AND}}$ be b_j. Also let $T = \{j : b_j = 1\}$.
4. **Computing the result:** If $|T| \geq t/2$ where $t = k/(2 \cdot \prod_{i\in[m]} |X_i|)$ is the expected size of T, and if $\exists v \forall j \in T$, $v_j = v$, then P_0 outputs v. Otherwise P_0 Aborts.

In the full version, we prove the following.

Theorem 8. *If $\mathcal{F}$ is an m-input CPS functionality, and $D = D_1 \times \cdots \times D_m$ is a subset of its domain, then $\mathsf{RDom}_D^{\mathcal{F},\mathcal{F}_{\text{AND}}}$ is a UC secure protocol for $\mathcal{F}_D$.*

8.2 Disseminating Functionalities

We rely on the disseminated-OR functionality $\mathcal{D}_{\text{OR}}$ to show that all disseminated functionalities are UC secure. The functionality $\mathcal{D}_{\text{OR}}$ takes $(x_1, \cdots, x_m)$ from the disseminator P_0 and outputs (b, x_i) to P_i where $b = x_1 \vee \cdots \vee x_m$. We start by giving a UC secure protocol for $\mathcal{D}_{\text{OR}}$.

Protocol for $\mathcal{D}_{\mathrm{OR}}$. In [PR08] a UC secure protocol for 3-party $\mathcal{D}_{\mathrm{OR}}$ was given. We present a variant that works for all values of m (please see the full version for the proof).

1. P_0 broadcasts (UC-securely [GL02]) $b := \bigvee_{i>0} x_i$ to all P_i.
2. If $b = 0$, for each $i > 0$, P_i outputs $(0, 0)$ and halts. Else, they continue.
3. P_0 sends x_i to each P_i.
4. For $i \in [m]$, $j \in [k]$, P_0 samples r_{ij} from a large group (e.g., k-bit strings) s.t. $\forall j$, $\sum_i r_{ij} = 0$.
5. For each i, if $x_i = 0$, P_0 sends r_{ij} for all j to P_i (and otherwise sends nothing to P_i).
6. Cut-and-choose:
   (a) P_1 picks a random subset $S \subset [k]$ of size $k/2$ and sends it to P_0.
   (b) For all $j \in S$, P_0 broadcasts r_{ij} for all i, and all parties verify that $\sum_i r_{ij} = 0$. P_1 verifies that the set S used is what it picked.
   (c) Any P_i with $x_i = 0$ aborts if it sees that for some j, r_{ij} broadcast by P_0 is not equal to r_{ij} it received.
7. For each $j \notin S$, $P_1, \cdots, P_m$ do the following:
   (a) For each i, if $x_i = 0$, P_i sets $s_{ij} = r_{ij}$, and otherwise samples s_{ij} randomly.
   (b) They use the standard semi-honest secure protocol to compute $\sum_i s_{ij}$.
   (c) Each P_i aborts if it gets the sum as 0.
8. If no abort has been observed, each P_i outputs $(1, x_i)$, where x_i is as received from P_0 in the beginning. Otherwise it aborts.

In the full version we prove that this protocol is secure. The interesting cases are when (1) a corrupt P_0 attempts to make all (honest) P_i's output $(1, 0)$ (thwarted by the summation evaluating to 0, or the cut-and-choose failing), and (2) when P_0 is honest and a set of corrupt P_i's may learn *all* s_{ij} (thwarted by s_{ij} being distributed uniformly, either because a corrupt P_i does not know r_{ij} as $x_i = 1$, or because an honest P_i used a random s_{ij}).

Protocol for any disseminating functionality. A disseminating functionality $\mathcal{F}$ with m output parties is specified by a function $F : X \to Y_1 \times \cdots \times Y_m$, for some finite domains X and Y_i. We consider a boolean function $\mathrm{Inv}^F_{[m]} : Y_1 \times \cdots \times Y_m \to \{0, 1\}$ (for "invalid") as follows: $\mathrm{Inv}^F_{[m]}(y_1, \cdots, y_n) = 1$ iff $\nexists x \in X$ s.t. $F(x) = (y_1, \ldots, y_n)$.

More generally, for any $S \subseteq [m]$, define $\mathrm{Inv}^F_S : Y_S \to \{0, 1\}$ as follows (denoting by Y_S the input combinations of parties indexed by S): for

$y_S \in Y_S$, $\mathrm{Inv}_S^F(y) = 1$ iff $\nexists x \in X, y_{\overline{S}} \in Y_{\overline{S}}$ s.t. $F(x) = (y_S, y_{\overline{S}})$ (with the output tuple understood as being sorted appropriately by the indices).

Protocol $\mathsf{Diss}_{\mathcal{F}}^{\mathcal{D}_{\mathrm{OR}}}$ (for disseminating functionality $\mathcal{F}$ computing F):

1. On input x, P_0 sends y_i to each P_i, where $F(x) = (y_1, \cdots, y_m)$.
2. For each subset $S \subseteq [m]$
   - For each $\tilde{y}_S \in Y_S$ such that $\mathrm{Inv}_S^F(\tilde{y}_S) = 1$:
     (a) Invoke $\mathcal{D}_{\mathrm{OR}}$, with P_0's input being $(a_1, \cdots, a_m)$, where $a_i = 0$ iff $\tilde{y}_i = y_i$ and 1 otherwise.
     (b) Each P_i receives (b, a_i). If $b = 0$, or if $a_i = 1$ but $\tilde{y}_i = y_i$, then abort.
3. If no abort has been observed, each P_i outputs y_i, and else aborts.

We point out that it is important to have the protocol consider all subsets $S \subseteq [m]$ (which makes it take time exponential in m), and not just the whole set $[m]$, as otherwise P_0 can collude with a corrupt P_{i^*} (who never aborts), and ensure that $b = 1$ always, by setting $a_{i^*} = 1$. Then P_0 can make the honest parties accept any combination of outputs, valid or not. In the full version we prove that the above protocol UC securely realizes $\mathcal{F}$.

References

BGI+14. Amos Beimel, Ariel Gabizon, Yuval Ishai, Eyal Kushilevitz, Sigurd Meldgaard, and Anat Paskin-Cherniavsky. Non-interactive secure multiparty computation. In *Advances in Cryptology - CRYPTO 2014, Proceedings, Part II*, pages 387–404, 2014.

BGW88. Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proc. 20th STOC*, pages 1–10, 1988.

Blu81. Manuel Blum. Three applications of the oblivious transfer: Part I: Coin flipping by telephone; part II: How to exchange secrets; part III: How to send certified electronic mail. Technical report, University of California, Berkeley, 1981.

CCD88. David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols. In *Proc. 20th STOC*, pages 11–19, 1988.

CI96. Benny Chor and Yuval Ishai. On privacy and partition arguments. In *Fourth Israel Symposium on Theory of Computing and Systems, ISTCS 1996, Jerusalem, Israel, June 10-12, 1996, Proceedings*, pages 191–194, 1996. Journal version appears in Information and Computation, 167(1).

CK91. Benny Chor and Eyal Kushilevitz. A zero-one law for boolean privacy. *SIAM J. Discrete Math.*, 4(1):36–47, 1991.

CKL06. Ran Canetti, Eyal Kushilevitz, and Yehuda Lindell. On the limitations of universally composable two-party computation without set-up assumptions. *J. Cryptology*, 19(2):135–167, 2006.

FKN94. Uriel Feige, Joe Kilian, and Moni Naor. A minimal model for secure computation (extended abstract). In *STOC*, pages 554–563, 1994.

GL02. Shafi Goldwasser and Yehuda Lindell. Secure computation without agreement. In *DISC*, pages 17–32, 2002.

HIJ+16. Shai Halevi, Yuval Ishai, Abhishek Jain, Eyal Kushilevitz, and Tal Rabin. Secure multiparty computation with general interaction patterns. In *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science, Cambridge, MA, USA, January 14-16, 2016*, pages 157–168, 2016.

HIJ+17. Shai Halevi, Yuval Ishai, Abhishek Jain, Ilan Komargodski, Amit Sahai, and Eylon Yogev. Non-interactive multiparty computation without correlated randomness. In *ASIACRYPT 2017, Proceedings, Part III*, pages 181–211, 2017.

HIKR18. Shai Halevi, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin. Best possible information-theoretic mpc. In *To appear in the Proceedings of Theory of Cryptography - 16th Theory of Cryptography Conference, TCC*, 2018.

HM97. Martin Hirt and Ueli M. Maurer. Complete characterization of adversaries tolerable in secure multi-party computation (extended abstract). In *PODC*, pages 25–34, 1997.

IK97. Yuval Ishai and Eyal Kushilevitz. Private simultaneous messages protocols with applications. In *Israel Symp. Theory of Comp. and Systems, ISTCS*, pages 174–184, 1997.

IK00. Yuval Ishai and Eyal Kushilevitz. Randomizing polynomials: A new representation with applications to round-efficient secure computation. In *FOCS*, pages 294–304, 2000.

KMR09. Robin Künzler, Jörn Müller-Quade, and Dominik Raub. Secure computability of functions in the IT setting with dishonest majority and applications to long-term security. In *TCC*, pages 238–255, 2009.

Kus89. Eyal Kushilevitz. Privacy and communication complexity. In *FOCS*, pages 416–421, 1989.

MPR09. Hemanta Maji, Manoj Prabhakaran, and Mike Rosulek. Complexity of multi-party computation problems: The case of 2-party symmetric secure function evaluation. In *TCC*, pages 256–273, 2009.

MPR13. Hemanta Maji, Manoj Prabhakaran, and Mike Rosulek. *Complexity of Multi-Party Computation Functionalities*, volume 10 of *Cryptology and Information Security Series*, pages 249 – 283. IOS Press, Amsterdam, 2013.

OY16. Satoshi Obana and Maki Yoshida. An efficient construction of non-interactive secure multiparty computation. In *Cryptology and Network Security, CANS*, pages 604–614, 2016.

PR08. Manoj Prabhakaran and Mike Rosulek. Cryptographic complexity of multi-party computation problems: Classifications and separations. In *CRYPTO*, pages 262–279, 2008. Full version available as ECCC Report TR08-050 from https://eccc.weizmann.ac.il.

Rys51. H. J. Ryser. A combinatorial theorem with an application to latin rectangles. *Proceedings of the American Mathematical Society*, 2(4):550–552, August 1951.

SRA79. Adi Shamir, R. L. Rivest, and Leonard M. Adleman. Mental poker. Technical Report LCS/TR-125, Massachusetts Institute of Technology, April 1979.

Yao82. Andrew Chi-Chih Yao. Protocols for secure computation. In *Proc. 23rd FOCS*, pages 160–164, 1982.