Zero-Communication Reductions

Varun Narayanan[1], Manoj Prabhakaran[2], and Vinod M. Prabhakaran[1]

[1] TIFR, Mumbai {varun.narayanan,vinodmp}@tifr.res.in
[2] IIT Bombay mp@cse.iitb.ac.in

Abstract. We introduce a new primitive in information-theoretic cryptography, namely *zero-communication reductions* (ZCR), with different levels of security. We relate ZCR to several other important primitives, and obtain new results on upper and lower bounds.
In particular, we obtain new upper bounds for PSM, CDS and OT complexity of functions, which are exponential in the information complexity of the functions. These upper bounds complement the results of Beimel et al. [BIKK14] which broke the circuit-complexity barrier for "high complexity" functions; our results break the barrier of input size for "low complexity" functions.
We also show that lower bounds on secure ZCR can be used to establish lower bounds for OT-complexity. We recover the known (linear) lower bounds on OT-complexity [BM04] via this new route. We also formulate the lower bound problem for secure ZCR in purely linear-algebraic terms, by defining the *invertible rank* of a matrix.
We present an **Invertible Rank Conjecture**, proving which will establish super-linear lower bounds for OT-complexity (and if accompanied by an explicit construction, will provide explicit functions with super-linear circuit lower bounds).

1 Introduction

Modern cryptography has developed a remarkable suite of information-theoretic primitives, like secret-sharing and its many variants, secure multi-party computation (MPC) in a variety of information-theoretic settings, (multi-server) private information retrieval (PIR), randomness extractors, randomized encoding, private simultaneous messages (PSM) protocols, conditional disclosure of secrets (CDS), and non-malleable codes, to name a few. Even computationally secure primitives are often built using these powerful tools. Further, a rich web of connections tie these primitives together.

Even as these primitives are often simple to define, and even as a large body of literature has investigated them over the years, many open questions remain. For instance, the efficiency of secret-sharing, communication complexity in MPC, PIR, and CDS, characterization of functions that admit MPC (without honest majority or setups) all pose major open problems. Interestingly, recent progress in some of these questions have arisen from surprising new connections across primitives (e.g., MPC from PIR [BIKK14], CDS from PIR [LVW17], and secret-sharing from CDS [LVW18,AA18]).

In this work, we introduce a novel information-theoretic primitive called *Zero-Communication Reductions* (ZCR) that fits right into this toolkit, and provides a bridge to information theoretic tools which were so far not brought to bear on cryptographic applications. The goal of a ZCR scheme is to let two parties compute a function on their joint inputs, without communicating with each other! Instead, in a ZCR from a function f to a *predicate* $\boldsymbol{\Phi}$, each party locally produces an output candidate *along with an input to the predicate*. The correctness requirement is that when the predicate outputs 1 ("accepts"), then the output candidates produced by the two parties should be correct; when the predicate outputs 0, correctness is not guaranteed. The non-triviality requirement places a (typically exponentially small) lower bound on the acceptance probability. We also define a natural security notion for ZCR, resulting in a primitive that is challenging to realize, and requires predicates with cryptographic structure.

Thanks to its minimalistic nature, ZCR emerges as a fundamental primitive. In this work we develop a theory that connects it with other fundamental cryptographic and information-theoretic notions. We highlight two classes of important applications of ZCR to central questions in information-theoretic cryptography – one for upper bounds and one for lower bounds. On the former front, we derive new upper bounds for communication in PSM and CDS protocols and for "OT-complexity" of a function – i.e., the number of OTs needed by an information-theoretically secure 2-Party Computation (2PC) protocol for the function – in terms of (internal) *information complexity*, a fundamental complexity measure of a 2-party function closely related to its communication complexity. On the other hand, we present a new potential route for strong lower bounds for OT-complexity, via Secure ZCR (SZCR), which has a much simpler combinatorial and linear algebraic structure compared to 2PC protocols.

Barriers: Avoiding and Confronting. One of the key questions that motivates our work is that of lower bounds for "cryptographic complexity" of 2-party functions – i.e., the number of accesses to oblivious transfer (or any other finite complete functionality) needed to securely evaluate the function (say, against honest-but-curious adversaries). Proving such lower bounds would imply lower bounds on representations that can be used to construct protocols. Specifically, small circuits and efficient private information retrieval (PIR) schemes imply low cryptographic complexity. As such, establishing strong lower bounds for cryptographic complexity will entail showing breakthrough results on circuit complexity and also on PIR lower bounds (which in turn has implications to Locally Decodable Codes).

Nevertheless, there is room to pursue cryptographic complexity lower bound questions without necessarily breaking these barriers. Firstly, there are existential questions of cryptographic complexity lower bounds that remain open, while the corresponding questions for circuit lower bounds are easy and pose no barrier by themselves. Secondly, when perfect correctness is required, the cryptographic lower bound questions are interesting and remain open for *randomized functions* with very fine-grained probability values. In these cases, since the input

(or index) must be long enough to encode the random choice, the corresponding circuit lower bounds and PIR lower bounds are already implied.

Finally, cryptographic complexity provides a non-traditional route — though still difficult — to attack these barriers. In fact, this work could be seen as providing a step along this path. We formulate SZCR lower bounds as a linear algebraic question of lower bounding what we call the *invertible rank*, which in turn implies cryptographic complexity and hence circuit complexity and PIR lower bounds. We conjecture that there exist matrices (representing the truth table of functions) that have a high invertible rank. Attacking the circuit complexity lower bound question translates to finding such matrices explicitly.

1.1 Our Results

We summarize our main contributions, and elaborate on them below.

- **New Primitives.** We define zero-communication reductions with different levels of security (ZCR, WZCR, and SZCR). We kick-start a theory of zero-communication reductions with several basic feasibility and efficiency results.
- **New Upper Bounds via Information Complexity.** Building on results of [BW16,KLL+15] which related information complexity of functions to communication complexity and "partition" complexity, we obtain constructions of ZCR whose complexity is upper bounded by the information complexity of the function. This in turn lets us obtain new upper bounds for statistically secure PSM, CDS, and OT complexity, which are exponential in the information complexity of the functions. As a concrete illustration of our upper bounds based on information complexity, for the "*bursting noise function*" of Ganor, Kol and Raz [GKR15], we obtain an *exponential improvement* over all existing constructions.
- **A New Route to Lower Bounds.** We show that an upper bound on OT-complexity of a function f implies an upper bound on the complexity of a SZCR from f to a predicate corresponding to OT. Hence lower bounding the latter would provide a potential route to lower bounding OT-complexity.
- We motivate the feasibility of this new route in a couple of ways:
  - We recover the known (linear) lower bounds on OT-complexity [BM04] via this new route by providing lower bounds on SZCR complexity.
  - We formulate the lower bound problem for SZCR in purely linear-algebraic terms, by defining the *invertible rank* of a matrix. We present our **Invertible Rank Conjecture**, proving which will establish super-linear lower bounds for OT-complexity (and if accompanied by an explicit construction, will provide explicit functions with super-linear circuit lower bounds).

Defining ZCR and SZCR. Our first contribution is definitional. The zero-communication model that we introduce is a powerful framework that, on the one hand, is convenient to analyze and, on the other hand, has close connections to a range of cryptographic primitives. Our definition builds on a line of work that used zero-communication protocols for studying communication and

information complexity, in classical and quantum settings (see, e.g., [KLL+15] and references therein), but we extend the model significantly to enable the cryptographic connections we seek. In Section 2, we define three variants – ZCR, WZCR, and SZCR– with three levels of security (none, weak, and standard or strong). All these reductions relate a function f to a predicate $\boldsymbol{\Phi}$, and, optionally, a correlation $\boldsymbol{\Psi}$, with the primary complexity measure being "non-triviality" or "acceptance probability" of the reduction: A μ-ZCR (or μ-WZCR, or μ-SZCR) needs to *accept* the outputs produced by the non-communicating parties with probability at least $2^{-\mu}$, and may abort otherwise.

(In)Feasibility Results. We follow up on the definitions with several basic positive and negative results about SZCR, presented in Section 4. In particular, we show that every function f has a non-trivial SZCR to some predicate $\boldsymbol{\Phi}_f$ (using no correlation); also every function f has a SZCR to the AND predicate, using some correlation $\boldsymbol{\Psi}_f$. Complementing these results, we show that for many natural choices of the predicate (AND, OR, or XOR), there are functions f which *do not* have a SZCR to the predicate, if no correlation is used. In fact, we *completely characterize* all functions that have a SZCR to these predicates.

On the other hand, there are predicates which are *complete* in the sense that any function f has a SZCR to it (possibly using a common random string). In a dual manner, a correlation $\boldsymbol{\Psi}$ can be considered complete if any function f can be reduced to a constant-sized predicate like AND using $\boldsymbol{\Psi}$. Our results (discussed below) show that the predicate $\boldsymbol{\Phi}_{\mathsf{supp}(\mathsf{OT}^+)}$– which checks if its inputs are in the support of one or more instances of the oblivious transfer (OT) correlation – is a complete predicate (Theorem 3) and OT is a complete correlation (Theorem 12). These results rely on OT being complete for secure 2-party computation and having a "regularity" structure.

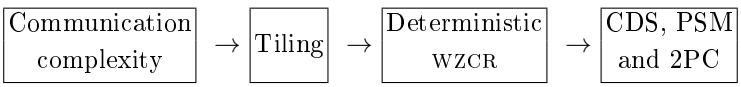
We also consider reducing *randomized functionalities without inputs* to *randomized predicates*; in this case, we characterize the optimal non-triviality achievable (Theorem 9).

Upper Bounds. Our upper bounds for CDS, PSM and 2PC for a function f are obtained by first constructing a ZCR (or WZCR) from f to a simple predicate. We offer two sets of results – perfectly secure constructions with complexity exponential in the communication complexity of f, and statistically secure constructions with complexity exponential in the information complexity.

The first set of results presented in Section 6.1, may be informally stated as follows.

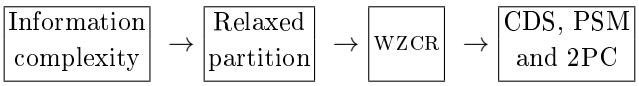
Theorem 1 (Informal). *For a deterministic function $f : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$, with communication complexity ℓ, there exist perfectly secure protocols for CDS, PSM and 2PC using OTs, all with communication complexity $O(2^\ell)$. Further, the 2PC protocol uses $O(2^\ell)$ invocations of OT.*

They follow from a sequence of connections illustrated below:



Here tiling refers to partitioning the function's domain $\mathcal{X}\times\mathcal{Y}$ into *monochromatic rectangles* – i.e., sets $\mathcal{X}'\times\mathcal{Y}'$ on which the function's value remains constant.

We significantly improve on these results (while sacrificing perfect security) in our second set of constructions presented in Section 6.2. They follow the outline below.



Note that now, instead of a tiling of f, we only require a (relaxed) *partition* of f [JK10,KLL+15], which allows overlapping monochromatic rectangles with fractional weights. The connection between information complexity and relaxed partition is a non-trivial result of Kerenidis et al. [KLL+15], that builds on [BW16]. We then construct a WZCR from a relaxed partition, and finally show how a WZCR (in fact, a ZCR) can be turned into a CDS, PSM or 2PC protocol. This leads us to the following theorem, stated in terms of the information complexity of f, $\mathsf{IC}_\epsilon(f)$, and statistical PSM, CDS and 2PC.

Theorem 2 (Informal). *Let $f:\mathcal{X}\times\mathcal{Y}\to\{0,1\}$ be a deterministic function. For any constant $\epsilon>0$, the communication complexity of ϵ-PSM of f, communication complexity of ϵ-CDS for predicate f, and OT and communication complexity of ϵ-secure 2PC of f are upperbounded by $2^{O\left(\mathsf{IC}_{\epsilon/8}(f)\right)}$.*

This result is all the more interesting because it is known that information complexity can be exponentially smaller than communication complexity. In particular, Ganor, Kol and Raz described an explicit (partial) function in [GKR15], called the "bursting noise function," which on inputs of size n, have a communication complexity lower bound of $\Omega(\log\log n)$ and an information complexity upper bound of $O(\log\log\log n)$. Note that the existing general 2PC techniques do not achieve sub-linear OT-complexity. Theorem 1 would allow $O(\log n)$ OT-complexity, whereas Theorem 2 brings it down to $O(\log\log n)$.

Our results can be seen as complementing [BIKK14] which offered improvements over the circuit size for "very high complexity" functions. We offer the best known protocols, improving over the input size, and even the communication complexity, for "very low complexity" functions.

Constructions of SZCR and Connection to Lower Bounds. We show that for a function f with OT-complexity m, there is a μ-SZCR from f to the constant-depth predicate $\mathbf{\Phi}_{\mathsf{supp}(\mathsf{OT}^+)}$(which checks if its inputs are in the support of oblivious transfer (OT) correlations), where μ is roughly m:

Theorem 3 (Informal). *If a deterministic functionality f with domain $\{0,1\}^n\times\{0,1\}^n$ and has OT-complexity m, then there exists an $(m+O(n))$-SZCR from f to $\mathbf{\Phi}_{\mathsf{supp}(\mathsf{OT}^{m+1})}$, possibly using a common random string.*

This result is proved more generally in Theorem 11, where it is also shown that the common random string can be avoided for a natural class of functions f (which are "common-information-free"). The results also extend to a "dual

version" where the reduction is to a simple AND predicate, but uses a *correlation* that provides m copies of OT (Theorem 12).

A consequence of Theorem 3 is that it can recover the best known lower bound for OT-complexity in terms of one-way communication complexity [BM04]. We show

$$\begin{array}{c}\text{One-way communication}\\ \text{complexity}\end{array} \leq \begin{array}{c}\text{Predicate-domain}\\ \text{complexity of SZCR}\end{array} \leq \text{OT-complexity}$$

where the first bound is shown using a simple support based argument (Lemma 2), and the second one follows from the upper bound on the *domain size of the predicate* $\boldsymbol{\Phi}_{\mathsf{supp}(\mathsf{OT}^k)}$ in Theorem 3. This is formally stated and proved as Corollary 2.

Invertible Rank. Theorem 3 provides a new potential route for lower bounding OT-complexity of f, by lower bounding μ or k in a μ-SZCR from f to $\boldsymbol{\Phi}_{\mathsf{supp}(\mathsf{OT}^k)}$. In turn, this problem can be formulated as a *purely linear-algebraic question* of what we term "invertible rank" (Section 5.1). Compared to previous paths for lower bounding OT-complexity [BM04,PP14], this new route is not known to be capped at linear bounds, and could even be seen as a stepping stone towards a fresh line of attack on circuit complexity lower bounds (as they are implied by OT-complexity lower bounds).

Invertible rank characterizes the best complexity – in terms of non-triviality *and* predicate-domain complexity – achievable by a SZCR from f to $\boldsymbol{\Phi}^+$ (conjunction of one or more instances of $\boldsymbol{\Phi}$). Specifically, for a matrix M_f encoding a function f and a matrix $P_{\boldsymbol{\Phi}}$ encoding a predicate, we have:

Theorem 4 (Informal). *If a function f has a perfect μ-SZCR to $\boldsymbol{\Phi}^k$ then the invertible rank of M_f w.r.t. $P_{\boldsymbol{\Phi}}$ is at most $\mu + k$.*

This characterization, combined with Theorem 3 implies that if a deterministic n-bit input functionality f has OT-complexity m, then its invertible rank w.r.t. P_{OT} is $O(m+n)$. Hence, a super-linear lower bound on invertible rank w.r.t. P_{OT} would imply super-linear OT-complexity, and consequently, super-linear circuit complexity for f. We conjecture the existence of function families f with super-linear invertible rank, and leave it as an important open problem to resolve it.

1.2 Related Work

As mentioned above, zero-communication protocols have been used to study communication and information complexity, in classical and quantum settings. The model can be traced back to the work of Gisin and Gisin [GG99], who proposed it as a local-hidden variable model (i.e., no quantum effects) that could explain apparent violation of the Bell inequality, when there is a significant probability of abort (i.e., missed detection) built into the system. More recently, Kerenidis et al. [KLL+15], using a compression lemma by Braverman and Weinstein [BW16], presented a zero-communication protocol with non-abort probability of at least $2^{-O(IC)}$, given a protocol for computing f with information complexity IC.

OT-complexity was explicitly introduced as a fundamental measure of complexity of a function f by Beimel and Malkin [BM04], who also presented a lower bound for f's OT-complexity in terms of the one-way communication complexity of f. In [PP14] an information-theoretic measure called tension was developed, and was shown to imply lower bounds for OT-complexity, among other things. Unfortunately, both these techniques can yield lower bounds on OT-complexity that are at most the length of the inputs. On the other hand, the best known feasibility result for OT-complexity, achieved via connections to PIR, by Beimel et al. [BIKK14], is sub-exponential (a.k.a. weakly exponential) in the input length. Closing this gap, even existentially, is an open problem.

In the PSM model, all functions are computable [FKN94] and efficient protocols are known when the function has small non-deterministic branching programs [FKN94,IK97]. Upper bounds on communication complexity were studied by Beimel et al. [BIKK14]. See [AHMS18] and references therein for lower bounds. In CDS, protocols have been constructed with communication complexity linear in the formula size [GIKM00]. Efficient protocols were later developed for branching programs [KN97] and arithmetic span programs [AR17]. Liu et al. [LVW17] obtained an upper bound of $2^{O(\sqrt{k \log k})}$ for arbitrary predicates with domain $\{0,1\}^k \times \{0,1\}^k$. Applebaum et al. [AA18] showed that amortized complexity over very long secrets can be brought down to a constant.

1.3 Technical Overview

We discuss some of the technical aspects of a few of our contributions mentioned above.

A New Model of Secure Computation. ZCR and its secure variants present a fundamentally new cryptographic primitive, highlighting aspects of secure computation common to many seemingly disparate notions like PSM, CDS and secure 2PC using correlated randomness.

Recall that in a ZCR from a function f to a predicate $\boldsymbol{\phi}$, each party locally produces an output candidate along with an input to the predicate. The output candidates produced by the two parties should be correct when the predicate outputs 1. Instances of zero-communication models have appeared in the communication complexity literature (see [KLL+15]), but they typically prescribed a specific predicate as part of the model (e.g., the equality predicate). By allowing an arbitrary predicate rather than one that is fixed as part of the model, we view our protocols as *reductions* from 2-party functionalities to predicates. This generalization is key to obtaining the various connections we develop.

Secondly, we add security requirements to the model. One may expect that a zero-communication protocol is naturally secure, as neither party receives *any* information about the other party's input or output. While that is the case for honest parties, we shall allow the adversary to learn the outcome of the predicate as well. This is the "right" definition, in that it allows interpreting a zero-communication protocol as a standard secure computation protocol when the predicate is implemented by a trusted party, who announces its result to the

two parties. The secure version of ZCR – called SZCR – admits stronger lower bounds (and even impossibility results), as discussed below.

We further generalize the notion of zero-communication reduction to allow the two parties access to a correlation $\boldsymbol{\psi}$, rather than just common randomness as in the original models in the literature.

In Figure 1, we illustrate a zero communication reduction from a functionality $f = (f_A, f_B)$ to a predicate $\boldsymbol{\phi}$, using a correlation $\boldsymbol{\psi}$.

The reduction is specified as a pair of randomized algorithms $(\mathfrak{A}, \mathfrak{B})$ executed by two parties, Alice and Bob. Alice, given input x and her part of the correlation R, samples $(A, U) \leftarrow \mathfrak{A}(x, R)$, where A is her proposed output for the functionality f, and U is her input to $\boldsymbol{\phi}$. Similarly, Bob computes $(B, V) \leftarrow \mathfrak{B}(y, S)$. The non-triviality guarantee is that $\boldsymbol{\phi}(U, V) = 1$ with a positive probability $2^{-\mu}$, and correctness guarantee is that conditioned on $\boldsymbol{\phi}(U, V) = 1$, the outputs of Alice and Bob are (almost always) correct.

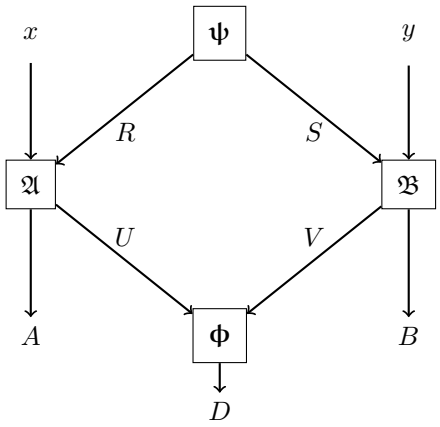


Fig. 1. The random variables involved in a ZCR.

The security definitions we attach to WZCR and SZCR could be seen as based on the standard simulation paradigm. However, when defining statistical (rather than perfect) security in the case of SZCR, a novel aspect emerges for us. Note that a μ-SZCR needs to accept an execution with probability only $2^{-\mu}$, which can be negligible. As such, allowing a negligible statistical error in security would allow one to have no security guarantees at all whenever the execution is not aborting, and would render SZCR no different from WZCR. The "right" security definition of SZCR with statistical security is to require security to hold *conditioned on acceptance* (as well as over all).

PSM, CDS, and 2PC from ZCR. Due to its minimalistic nature, a ZCR can be used as a reduction in the context of PSM, CDS, and 2PC. At a high-level, a ZCR from f to a predicated $\boldsymbol{\phi}$ could be thought of as involving a "trusted party" which implements $\boldsymbol{\phi}$. Since the reduction itself involves no communication, it can easily be turned into a PSM, CDS or 2PC scheme for the function f, if we can "securely implement" a trusted party for $\boldsymbol{\phi}$ in the respective model. One complication however, is that a ZCR can abort with a high probability. This is handled by repeating the execution several times (inversely proportional to the acceptance probability), and using the answer produced in an execution that is accepted.

While it may appear at first that ZCR with a security guarantee will be needed here, we can avoid it. This is done by designing the secure component (PSM, CDS, or 2PC) to not implement the predicate $\boldsymbol{\phi}$ directly, but to implement a *selector function* as described below. Recall that in an execution of the ZCR

protocol, Alice and Bob will generate candidate outputs (a, b) as well as inputs (u, v) for $\boldsymbol{\Phi}$. The parties will now carry out this protocol n times in parallel, to generate (a_i, b_i) and (u_i, v_i), for $i = 1$ to n. The selector function accepts all (a_i, b_i, u_i, v_i) as inputs and outputs a pair (a_i, b_i) such that $\boldsymbol{\Phi}(u_i, v_i) = 1$, without revealing i itself (we choose n sufficiently large as to guarantee that there will be at least one such instance, except with negligible probability; if multiple such i exist, then, say, the largest index is selected).

The overall communication complexity of the resulting protocol is exactly determined by the PSM, CDS, or 2PC protocol for the selector function (as the ZCR itself adds no communication overhead). By instantiating our results for the predicate $\boldsymbol{\Phi}_{\mathsf{AND}}$, the selector function has a small *formula complexity*, and hence efficient PSM, CDS, and 2PC protocols.

ZCR and Information Complexity. WZCR and the notion of relaxed partition [JK10,KLL+15] are intimately connected to each other. A relaxed partition of a 2-input function f could be seen as a tiling of the function table with fractionally weighted tiles such that each cell in the table is covered by (almost) 1 unit worth of tiles, (almost) all of them having the same color (i.e., output value) as the cell itself. The goal of a partition is to use as few tiles as possible – or more precisely, to minimize the total weight of all the tiles used. In Lemma 4, we show that a relaxed partition can be turned into a WZCR of f to the predicate $\boldsymbol{\Phi}_{\mathsf{AND}}$, with acceptance probability roughly equal to the reciprocal of the total weights of the tile. (In fact, if no error were to be allowed, a WZCR with maximum acceptance probability exactly corresponds to a partition with minimum total weight.) A result of [KLL+15] can then be used to relate this acceptance probability to the information complexity of f.

Thus, via ZCR, we can upper bound PSM, CDS, and OT-complexity of functions by a quantity exponential in their information complexity. While this upper bound is rather loose in the worst case, in general, it appears incomparable to all other known upper bounds.

SZCR from 2PC. Any boolean function f has a SZCR to a predicate $\boldsymbol{\Phi}_f$ with acceptance probability of at least 1/4 (Theorem 5). However, the computational complexity (measured in size or depth) of $\boldsymbol{\Phi}_f$ is as much as that of f. An important question is whether – and how well can – a function be reduced to a *universal, constant-depth* predicate.

We show that if the predicate is $\boldsymbol{\Phi}_{\mathsf{AND}}$, and no correlations are used (except possibly common randomness), then only *simple* functions have a SZCR to the predicate. (Simple functions are those that are not complete [MPR13].)

On the other hand, there is a *universal* constant-depth predicate $\boldsymbol{\Phi}_{\mathsf{supp}(\mathsf{OT}^+)}$, which simply checks if its inputs are in the support of several copies of oblivious transfer correlations, such that every function f has a SZCR to it. In fact, we show that f has a μ-SZCR (i.e., a SZCR with acceptance probability $2^{-\mu}$) to $\boldsymbol{\Phi}_{\mathsf{supp}(\mathsf{OT}^+)}$ where μ is at most the OT complexity of f. (Corollary 1). (In this result, OT can be replaced by a general class of correlations, called "regular correlations.")

The idea is to transform a 2-party protocol Π^{OT} that (against passive corruption) perfectly securely realizes f using OT correlations, into a SZCR from f

to $\boldsymbol{\Phi}_{\mathsf{supp}(\mathsf{OT}^+)}$. The transformation relies on the fact that any protocol admits *transcript factorization*: i.e., the probability of a transcript q occurring in an execution of Π^{OT}, given inputs (x, y) and OT correlation (u, v) to the two parties respectively, can be written as

$$\mathsf{Pr}_{\Pi^{\mathsf{OT}}}(q|x, y, u, v) = \rho(x, u, q) \cdot \sigma(y, v, q),$$

for some functions ρ and σ. This could be exploited by the parties to non-interactively sample an instance of the protocol execution, and derive their outputs from it. One issue here is that since the parties have access to OTs, the product structure on the transcript distribution applies only conditioned on their respective views from the OT. Thus, it is in fact the views in the OT, u and v that the two parties sample locally, conditioned on their own inputs and a transcript q that is determined by a common random string.[3] $\boldsymbol{\Phi}_{\mathsf{supp}(\mathsf{OT}^+)}$ is used to check if the two views of the OT correlations sampled thus are compatible with each other.

Several technical complications arise in the above plan. In particular, ensuring that the abort event does not reveal any information beyond the input and output to each party, requires a careful choice of probabilities with which each party selects its view of the OT correlations; also, each party unilaterally forces an abort with some probability (implemented using a couple of extra OTs included in the input to $\boldsymbol{\Phi}_{\mathsf{supp}(\mathsf{OT}^+)}$). For simplicity, here we summarize the scheme for a common-information-free function f. In this case, there will be no common random string. We fix an arbitrary transcript q^* (which has a non-zero probability of occurring), and define

$$\rho^\dagger := \max_x \sum_u \rho(x, u, q^*), \qquad \sigma^\dagger := \max_y \sum_v \sigma(y, v, q^*). \tag{1}$$

Recall that a SZCR is given by a pair of algorithms $(\mathfrak{A}, \mathfrak{B})$ which, respectively, take x and y as inputs, and output (U, A) and (V, B) (Figure 1). We define these algorithms below. In addition to the quantities mentioned above, we also refer to the algorithms Π_A^{out} and Π_B^{out} which are the output computation algorithms of the protocol Π.

$\mathfrak{A}(x)$**:** For each $u \in \mathcal{U}$, let $(U, A) = (u, \Pi_A^{\text{out}}(x, u, q^*))$ with probability $\frac{\rho(x,u,q^*)}{\rho^\dagger}$, and $(\perp, \perp)$ with remaining probability (if any).

$\mathfrak{B}(y)$**:** For each $u \in \mathcal{U}$, let $(V, B) = (v, \Pi_B^{\text{out}}(y, v, q^*))$ with probability $\frac{\sigma(y,v,q^*)}{\sigma^\dagger}$, and $(\perp, \perp)$ with remaining probability (if any).

Note that for x which maximizes the expression defining $\rho^\dagger$, $\mathfrak{A}(x)$ does not set $(u, a) = (\perp, \perp)$, but in general, this costs the SZCR in terms of non-triviality. This sacrifice in acceptance probability is needed for Alice to even out the acceptance probability across her different inputs, so that Bob's view combined with the acceptance event, does not reveal information about x (beyond $f(x, y)$). Nevertheless, we can show that the probability of acceptance is lower bounded by

[3] For secure protocols for common-information-free functions, a transcript can be fixed, avoiding the need for a common random string.

$2^{-(m+n)}$, where m is the number of OTs (so u, v are each $2m$-bit strings) and the combined input of f is n bits long.

The construction is somewhat more delicate when f admits common-information. This means that there is some common information that Alice and Bob could agree on if they are given $(x, f_A(x, y))$ and $(y, f_B(x, y))$ respectively. For such functions, the SZCR construction above is modified so that a candidate value for the common information is given as a common random string; it is arranged that the execution is rejected by the predicate if the common information in the common random string is not correct. Also, in this case, we can no more choose an arbitrary transcript (even after fixing the common information); instead we argue that there is a "good" transcript for each value of common information, that would let us still obtain a similar non-triviality guarantee as in the case of common-information-free f.

We give an analogous result for SZCR to $\boldsymbol{\Phi}_{\mathsf{AND}}$, but *using* OT correlations. Here, each party locally checks if their input is consistent with a given transcript (determined by common randomness) and their share of OT correlations. Here also, for the sake of security, even if it is consistent, the party aborts with a carefully calibrated probability.

In both the above transformations from a secure 2PC protocol Π for f to a SZCR, an important consideration is the probability of not aborting. To establish our connection with OT-complexity, we need a μ-SZCR where μ is directly related to the number of OTs used in Π, and *not the length of the transcripts*. One element in establishing such a SZCR is an analysis of the given 2PC protocol when it is run with correlations drawn using a wrong distribution. We refer the reader to Theorem 11 and its proof for further details.

Invertible Rank. The conditions of a SZCR (from a possibly randomized function to a possible randomized predicate) without correlations can be captured purely in linear algebraic terms, leading to the definition of a new linear-algebraic complexity measure for functions.

The correctness condition for μ-SZCR of f to $\boldsymbol{\Phi}$ has the form $A^\intercal P B = 2^{-\mu} M$, where M and P are matrices that encode the function f and the predicate $\boldsymbol{\Phi}$ in a natural way. If P were to be replaced with the identity matrix, and μ by 0, the smallest possible size of P would correspond to the rank of M. In defining invertible rank with respect to a finite matrix $P_{\boldsymbol{\Phi}}$, we let $P = P_{\boldsymbol{\Phi}}^{\otimes k}$ and ask for the smallest k possible, for a given μ (thus the invertible rank is analogous to *log-rank*). Also, A, B are required to satisfy natural stochasticity properties so that they correspond to valid probabilistic actions.

In addition to the correctness guarantees, we also incorporate the security guarantees of SZCR into our complexity measure. This takes the form of the existence of simulators, which are again captured using linear transformations. The "invertibility" in the term invertible rank refers to the existence of such simulators.

We remark that linear-algebraic complexity measures have been prevalent in studying the computational or communication complexity of functions – matrix rigidity [Val77], sign rank [PS86], the "rank measure" of Razborov [Raz90],

approximate rank [ALSV13] and probabilistic rank [AW17] have all led to important advances in our understanding of functions. In particular, Razborov's rank measure was instrumental in establishing exponential lower bounds for linear secret-sharing schemes [RPRC16,PR17]. Invertible rank provides a new linear-algebraic complexity measure that is closely related to *secure two-party computation*, via our results on SZCR; this is in contrast with the prior measures which were motivated by computational complexity, (insecure) two-party communication complexity, or secret-sharing (which does not address the issues of secure two-party computation),

Organization of the Rest of the Paper

We present the formal definitions of ZCR, WZCR and SZCR in Section 2. Before continuing to our results, we summarize relevant background information in Section 3. The basic feasibility results in our model are presented in Section 4. The connections with lower bounds are given in Section 5, and the upper bounds on CDS, PSM and 2PC are given in Section 6. Several proof details are given in in the full version [NPP20].

2 Defining Zero-Communication Secure Reductions

We refer the reader to Figure 1, which illustrates the random variables involved in a zero communication reduction from a functionality $f = (f_A, f_B)$ to a predicate $\boldsymbol{\Phi}$, using a correlation $\boldsymbol{\Psi}$. The reduction is specified as a pair of randomized algorithms $(\mathfrak{A}, \mathfrak{B})$ executed by two parties, Alice and Bob. Alice, given input x and her part of the correlation R, samples $(A, U) \leftarrow \mathfrak{A}(x, R)$, where A is her proposed output for the functionality f, and U is her input to $\boldsymbol{\Phi}$. Similarly, Bob computes $(B, V) \leftarrow \mathfrak{B}(y, S)$. The non-triviality guarantee is that $\boldsymbol{\Phi}(U, V) = 1$ with a positive probability $2^{-\mu}$, and correctness guarantee is that conditioned on $\boldsymbol{\Phi}(U, V) = 1$, the outputs of Alice and Bob are almost always correct.

We shall define three notions of such a reduction (ZCR, WZCR and SZCR) depending on the level of security implied (no security, weak security and standard security).

Notation: Below, $\mathfrak{p}(R)$ denotes the distribution of a random variable R, $\mathsf{Pr}(r, s)$ stands for $\mathsf{Pr}(R = r, S = s)$, where R, S are random variables, and $\mathsf{Pr}_{\mathfrak{A}}(\alpha|\beta)$ denotes the probability that a probabilistic process $\mathfrak{A}$ outputs α on input β. $|D_1 - D_2|$ denotes the statistical difference between two distributions D_1, D_2. (Further notes on notation are given in Section 3.)

Definition 1. *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{A} \times \mathcal{B}$ and $\boldsymbol{\Phi} : \mathcal{U} \times \mathcal{V} \to \{0, 1\}$ be randomized functions, and let $\boldsymbol{\Psi}$ be a distribution over $\mathcal{R} \times \mathcal{S}$. For any $\mu, \epsilon \geq 0$, a (μ, ϵ)-zero-communication reduction (ZCR) from f to the predicate $\boldsymbol{\Phi}$ using $\boldsymbol{\Psi}$ is a pair of probabilistic algorithms $\mathfrak{A} : \mathcal{X} \times \mathcal{R} \to \mathcal{U} \times \mathcal{A}$ and $\mathfrak{B} : \mathcal{Y} \times \mathcal{S} \to \mathcal{V} \times \mathcal{B}$ such that the following holds.*

Define jointly distributed random variables (R, S, U, V, A, B, D)*, conditioned on each* $(x, y) \in \mathcal{X} \times \mathcal{Y}$*, as*

$$\mathsf{Pr}(r, s, u, v, a, b, d|x, y) = \mathsf{Pr}_{\boldsymbol{\psi}}(r, s) \cdot \mathsf{Pr}_{\mathfrak{A}}(u, a|x, r) \cdot \mathsf{Pr}_{\mathfrak{B}}(v, b|y, s) \cdot \mathsf{Pr}_{\boldsymbol{\phi}}(d|u, v).$$

- ***Non-Triviality:*** $\forall (x, y) \in \mathcal{X} \times \mathcal{Y}$, $\mathsf{Pr}(D = 1|x, y) \geq 2^{-\mu}$.
- ***Correctness:*** $\forall (x, y) \in \mathcal{X} \times \mathcal{Y}$, $|\mathfrak{p}((A, B)|x, y, D = 1) - f(x, y)| \leq \epsilon$.

In other words, in a ZCR, Alice and Bob compute "candidate outputs" a and b, as well as two messages u and v, respectively, such that correctness (i.e., $f(x, y) = (a, b)$) is required only when $\boldsymbol{\phi}$ "accepts" (u, v). We allow Alice and Bob to coordinate their actions using the output of $\boldsymbol{\psi}$. We also allow a small error probability of ϵ. To be non-trivial, we require a lower bound $2^{-\mu}$ on the probability of $\boldsymbol{\phi}$ accepting. Note that as μ increases from 0 to ∞, the non-triviality constraint gets relaxed.

Next, we add a weak security condition to ZCR as follows: Consider an "eavesdropper" who gets to observe whether the predicate $\boldsymbol{\phi}$ accepts or not. We require that this reveals (almost) no information about the inputs (x, y) to the eavesdropper. Technically, we require the probability of accepting to remain within a multiplicative factor of $(1 - \epsilon)^{\pm 1}$ as the inputs are changed.

Definition 2. *For any* $\mu \geq 0$*,* $\epsilon \geq 0$*, a* (μ, ϵ)-ZCR $(\mathfrak{A}, \mathfrak{B})$ *from* f *to* $\boldsymbol{\phi}$ *using* $\boldsymbol{\psi}$ *is a* (μ, ϵ)-weakly secure zero-communication reduction *(*WZCR*) if the following condition holds.*

- ***Weak Security:*** $\forall (x, y), (x', y') \in \mathcal{X} \times \mathcal{Y}$,

$$\mathsf{Pr}(D = 1|x, y) \geq (1 - \epsilon)\mathsf{Pr}(D = 1|x', y'),$$

  where D *is the random variable corresponding to the output of* $\boldsymbol{\phi}$*, as defined in Definition 1.*

Finally, we present our strongest notion of security, SZCR. The definition corresponds to security against passive corruption of one of Alice and Bob in a secure computation protocol (using $\boldsymbol{\phi}$ and $\boldsymbol{\psi}$ as trusted parties) that realizes the following functionality $f_{\mu'}$ (for some $\mu' \leq \mu$): After computing $(a, b) \leftarrow f(x, y)$, with probability $2^{-\mu'}$ the functionality sends the respective outputs to the two parties ("accepting" case); with the remaining probability, it sends the output only to the corrupt party. The definition of SZCR involves a refinement not present in (statistical) security of secure computation: We require that even *conditioned on* the execution "accepting" – which could occur with a negligible probability – security holds. The formal definition of SZCR includes the correctness and (weak) security properties of a WZCR, and further requires the existence of two simulators $\hat{S}_A$ (for corrupt Alice) and $\hat{S}_B$ (for corrupt Bob), with separate conditions for the accepting and non-accepting cases. We formalize these conditions below.

Definition 3. *For any* $\mu \geq 0$*,* $\epsilon \geq 0$*, a* (μ, ϵ)-WZCR $(\mathfrak{A}, \mathfrak{B})$ *from* f *to* $\boldsymbol{\phi}$ *using* $\boldsymbol{\psi}$ *is a* (μ, ϵ)-secure zero-communication reduction *(*SZCR*) if the following conditions hold.*

– ***Security:*** $\forall x \in \mathcal{X}, y \in \mathcal{Y}$, *and* a, b *s.t.* $\mathsf{Pr}_f(a,b|x,y) > 0$

$$\left|\mathfrak{p}\left(R, U | x, y, a, b, D = 1\right) - \hat{S}_A(x, a, 1)\right| \leq \epsilon, \tag{2}$$

$$\left|\mathfrak{p}\left(S, V | x, y, a, b, D = 1\right) - \hat{S}_B(y, b, 1)\right| \leq \epsilon, \tag{3}$$

$$\left|\mathfrak{p}\left(R, U | x, y, D = 0\right) - \hat{S}_A(x, f_A(x,y), 0)\right| \leq \epsilon, \tag{4}$$

$$\left|\mathfrak{p}\left(S, V | x, y, D = 0\right) - \hat{S}_B(y, f_B(x,y), 0)\right| \leq \epsilon. \tag{5}$$

where the random variables R, S, U, V, D *are as defined in Definition 1, and* $\hat{S}_A : \mathcal{X} \times \mathcal{A} \times \mathcal{D} \to \mathcal{R} \times \mathcal{U}$ *and* $\hat{S}_B : \mathcal{Y} \times \mathcal{B} \times \mathcal{D} \to \mathcal{S} \times \mathcal{V}$ *are randomized functions.*

Above, (2) and (4) correspond to corrupting Alice, with the first one being the accepting case. (The other two equations correspond to corrupting Bob.) Note that in these cases the adversary's view consists of (R, U), in addition to the input x and the boolean variable D (accepting or not), which are given to the environment as well. In the accepting case, the environment also observes the outputs (a, b). In either case, $\hat{S}_A$ is given $(x, f_A(x,y), D)$ as inputs; in the accepting case, we naturally require that the simulated view has the same output a as $f_A(x,y)$ given to $\hat{S}_A$.

Special Cases. A few special cases of the above definitions will be of interest, and we use specialized notation for them. A perfect reduction guarantees *perfect* correctness and security, wherein $\epsilon = 0$. In this case instead of $(\mu, 0)$-ZCR (WZCR, SZCR), we simply say μ-ZCR (WZCR, SZCR).

For deterministic f, when $\epsilon = 0$, the security conditions (2)-(5) in Definition 3 can be replaced with the following equivalent conditions: $\forall x, y, r, s, u, v, d$,

$$\mathsf{Pr}(r, u, d | x, y_1) = \mathsf{Pr}(r, u, d | x, y_2), \text{ if } f_A(x, y_1) = f_A(x, y_2), \tag{6}$$

$$\mathsf{Pr}(s, v, d | x_1, y) = \mathsf{Pr}(s, v, d | x_2, y), \text{ if } f_B(x_1, y) = f_B(x_2, y). \tag{7}$$

A formal proof of this equivalence is provided in the full version [NPP20].

We would consider perfect SZCR of a functionality f to a predicate $\boldsymbol{\Phi}$ using no correlation. This notion of reduction still suffices for many of our connections (e.g., to lower bounds on OT complexity), while being simpler to analyze. A correlation $\boldsymbol{\Psi}$ which only offers a common random string to the two parties is denoted as $\boldsymbol{\Psi}^{\mathsf{CRS}}$. Indeed, for ZCR and WZCR, $\boldsymbol{\Psi}^{\mathsf{CRS}}$ is the only non-trivial correlation one may consider.

3 Preliminaries for the Remainder

Before proceeding further, we present background material and some notation needed for the remainder of the paper.

Probability Notation. The probability assigned by a distribution D (or a probabilistic process D) to a value x is denoted as $\mathsf{Pr}_D(x)$, or simply $\mathsf{Pr}(x)$,

when the distribution is understood. We write $x \leftarrow D$ to denote sampling a value according to the distribution D. Given two distributions D_1, D_2, we write $|D_1 - D_2|$ to denote the statistical difference (a.k.a. total variation distance) between the two.

For a random variable X, we write $\mathfrak{p}(X)$ to denote the probability distribution associated with it. We write $\mathfrak{p}(X|Y=y)$ (or simply $\mathfrak{p}(X|y)$, letting the lower case y signify that it is the value of the random variable Y), to denote the distribution of a random variable X, conditioned on the value y for a random variable Y that is jointly distributed with X.

Functionalities. We denote a 2-party functionality as $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{A} \times \mathcal{B}$, to indicate that the functionality accepts an input $x \in \mathcal{X}$ from Alice and $y \in \mathcal{Y}$ from Bob, computes $(a, b) = f(x, y)$, and sends a to Alice and b to Bob. We allow f to be a randomized function too, in which case $f(x, y)$ stands for a probability distribution over $\mathcal{A} \times \mathcal{B}$, for each $(x, y) \in \mathcal{X} \times \mathcal{Y}$; for readability, we write $\mathsf{Pr}_f(a, b|x, y)$ instead of $\mathsf{Pr}_{f(x,y)}(a, b)$ to denote the probability of $f(x, y)$ outputting (a, b). We write $f = (f_A, f_B)$, where $f_A : \mathcal{X} \times \mathcal{Y} \to \mathcal{A}$ and $f_B : \mathcal{X} \times \mathcal{Y} \to \mathcal{B}$ are such that (making the randomness ξ used by f explicit), $f(x, y; \xi) = (f_A(x, y; \xi), f_B(x, y; \xi))$. If f_B is a constant function, we identify f with f_A and refer to it as a *one-sided functionality*. Similarly, if $f_A = f_B$, then we may use f to refer to either of these functions; in this case, we refer to f as a *symmetric functionality*.

Correlations. A correlation $\boldsymbol{\psi}$ over a domain $\mathcal{R} \times \mathcal{S}$ is the same as a 2-party randomized functionality $\boldsymbol{\psi} : \{\perp\} \times \{\perp\} \to \mathcal{R} \times \mathcal{S}$ (i.e., a functionality with no inputs). $\mathsf{supp}(\boldsymbol{\psi}) = \{(r, s)|\mathsf{Pr}_{\boldsymbol{\psi}}(r, s) > 0\}$ is the support of $\boldsymbol{\psi}$. We say that a correlation is *regular* if (1) $\forall (r, s) \in \mathsf{supp}(\boldsymbol{\psi})$, $\mathsf{Pr}_{\boldsymbol{\psi}}(r, s) = \frac{1}{|\mathsf{supp}(\boldsymbol{\psi})|}$, (2) $\forall r \in \mathcal{R}$, $\sum_{s \in \mathcal{S}} \mathsf{Pr}_{\boldsymbol{\psi}}(r, s) = \frac{1}{|\mathcal{R}|}$, and (3) $\forall s \in \mathcal{S}$, $\sum_{r \in \mathcal{R}} \mathsf{Pr}_{\boldsymbol{\psi}}(r, s) = \frac{1}{|\mathcal{S}|}$. Common examples of regular correlations are those corresponding to Oblivious Transfer (OT) and Oblivious Linear Function Evaluation (OLE), and their n-fold repetitions. Another regular correlation of interest is the common randomness correlation $\boldsymbol{\psi}^{\mathsf{CRS}}$, in which $(r, s) \in \mathsf{supp}(\boldsymbol{\psi}^{\mathsf{CRS}})$ if only if $r = s$.

We denote t independent copies of a correlation $\boldsymbol{\psi}$ by $\boldsymbol{\psi}^t$. It will be convenient to denote $\boldsymbol{\psi}^t$ for an unspecified t by $\boldsymbol{\psi}^+$.

Predicates. We shall also refer to predicates of the form $\boldsymbol{\phi} : \mathcal{U} \times \mathcal{V} \to \{0, 1\}$. Again, as in the case of functionalities above, a predicate could be randomized. Given a correlation $\boldsymbol{\psi}$ over $\mathcal{U} \times \mathcal{V}$, we define the predicate $\boldsymbol{\phi}_{\mathsf{supp}(\boldsymbol{\psi})}$ so that $\boldsymbol{\phi}_{\mathsf{supp}(\boldsymbol{\psi})}(u, v) = 1$ iff $(u, v) \in \mathsf{supp}(\boldsymbol{\psi})$. The predicate $\boldsymbol{\phi}_{\mathsf{supp}^*(\boldsymbol{\psi})}$ is defined identically, except that we allow the domain of $\boldsymbol{\phi}_{\mathsf{supp}^*(\boldsymbol{\psi})}$ to be $(\mathcal{U} \cup \{\perp\}) \times (\mathcal{V} \cup \{\perp\})$ where $\perp$ is a symbol not in $\mathcal{U} \cup \mathcal{V}$.

It will also be convenient to define $\mathsf{supp}(\boldsymbol{\psi}^+) := \bigcup_{t=1}^{\infty} \mathsf{supp}(\boldsymbol{\psi}^t)$.

Evaluation Graph G_f. For a functionality f, it is useful to define a bipartite graph G_f [MPR13].

Definition 4. *For a randomized functionality $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{A} \times \mathcal{B}$, the weighted graph G_f is defined as the bipartite graph on vertices $(\mathcal{X} \times \mathcal{A}) \cup (\mathcal{Y} \times \mathcal{B})$ with weight on edge $((x, a), (y, b)) = \mathsf{Pr}_f(a, b|x, y)$.*

Note that for deterministic f, the graph G_f is unweighted (all edges have weight 1 or 0). If f is a correlation, with no inputs, the nodes in the graph G_f can be identified with $\mathcal{A} \cup \mathcal{B}$.

Definition 5. *In an evaluation graph G_f, a* connected component *is a set of edges that form a connected component in the unweighted graph consisting only of edges in G_f with positive weight. A function f is said to be* common-information-free *if all the edges in G_f belong to the same connected component.*

For each connected component C in G_f, we define $\mathcal{X}_C \subseteq \mathcal{X}$ as the set $\{x | \exists y, a, b \text{ s.t. } ((x,a),(y,b)) \in C\}$; $\mathcal{Y}_C \subseteq \mathcal{Y}$ is defined analogously. Also, we define $C|_{\mathcal{X}\times\mathcal{Y}} := \{(x,y) | \exists (a,b) \text{ s.t. } ((x,a),(y,b)) \in C\}$.

For a correlation $\boldsymbol{\psi}$, we will denote by $\boldsymbol{\psi}|_C$ the restriction of $\boldsymbol{\psi}$ to the connected component C. That is, $\mathsf{Pr}_{\boldsymbol{\psi}|_C}(a,b) \propto \mathsf{Pr}_{\boldsymbol{\psi}}(a,b)$ for $(a,b) \in C$ and 0 otherwise.

A simple functionality [MPR12,MPR13] is one whose graph G_f consists of connected components that are all *product graphs*. For deterministic functionalities, it can be defined as follows:

Definition 6. *A deterministic functionality $f = (f_A, f_B)$ with domain $\mathcal{X} \times \mathcal{Y}$ is a* simple functionality *if there exist no $x, x' \in \mathcal{X}$ and $y, y' \in \mathcal{Y}$ such that $f_A(x,y) = f_A(x,y')$ and $f_B(x,y) = f_B(x',y)$ but either $f_A(x',y) \neq f_A(x',y')$ or $f_B(x,y') \neq f_B(x',y')$.*

Simple functionalities satisfy the following (see [MPR12]).

Lemma 1. *If (f_A, f_B) is a simple deterministic functionality, then there exists a partition $\mathcal{X} \times \mathcal{Y}$ into k rectangles $(A_i \times B_i)_{i\in[k]}$ for some number k such that the following properties are satisfied.*

1. *For each $i \in [k]$, for any $x \in A_i$, whenever $y, y' \in B_i$, $f_A(x,y) = f_A(x,y')$. Similarly, for each $y \in B_i$ whenever $x, x' \in A_i$, $f_B(x,y) = f_B(x',y)$.*
2. *For distinct $i, j \in [k]$, if $A_i \cap A_j \neq \emptyset$ (in this case B_i and B_j are disjoint), if $x \in A_i \cap A_j$ and $y \in B_i$ and $y' \in B_j$ then $f_A(x,y) \neq f_A(x,y')$.*
3. *For distinct $i, j \in [k]$, if $B_i \cap B_j \neq \emptyset$, if $y \in B_i \cap B_j$ and $x \in A_i$ and $x' \in A_j$ then $f_B(x,y) \neq f_B(x',y)$.*

Secure Protocols and OT Complexity. A standard (interactive) 2-party protocol using a correlation $\boldsymbol{\psi}$, denoted as $\Pi^{\boldsymbol{\psi}}$, consists of a pair of computationally unbounded randomized parties Alice and Bob. We write $(r, s, q, a, b) \leftarrow \Pi^{\boldsymbol{\psi}}(x, y)$ to denote the outcome of an execution of $\Pi^{\boldsymbol{\psi}}$ on inputs (x, y), as follows: Sample $(r, s) \leftarrow \boldsymbol{\psi}$, and give r to Alice and s to Bob. Then they exchange messages to (probabilistically) generate a transcript q. Finally, Alice samples a based on her view (x, r, q) and outputs it; similarly, Bob outputs b based on (y, s, q).

We are interested in *passive secure* protocols for computing a 2-party function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{A} \times \mathcal{B}$, possibly with a statistical error. See the full version

[NPP20] for a formal definition of secure 2-party computation protocols that use correlations.

It is well-known that there are correlations – like *randomized oblivious transfer (OT) correlation* – that can be used to perfectly securely compute any function f using its circuit representation (see [Gol04]) or sometimes more efficiently using its truth table [BIKK14]. The *OT-complexity* of a functionality f is the smallest number of independent instances of OT-correlations needed by a perfectly secure 2-party protocol that securely realizes f against passive adversaries.

Transcript Factorization. An important and well-known property (e.g., [CK91]) of a protocol Π^{Ψ} is that the probability of generating the transcript, as a function of (x, y, r, s), can be factorized into separate functions of (x, r) and (y, s). More formally, there exist *transcript factorization functions* $\rho : \mathcal{X} \times \mathcal{R} \times \mathcal{Q} \to [0, 1]$ and $\sigma : \mathcal{Y} \times \mathcal{S} \times \mathcal{Q} \to [0, 1]$, such that

$$\mathsf{Pr}_{\Pi^{\Psi}}(q|x, y, r, s) = \rho(x, r, q) \cdot \sigma(y, s, q). \tag{8}$$

To see this, note that a transcript $q = (m_1, \ldots, m_N)$ is generated by $\Pi^{\Psi}(x, y)$, given (r, s) from $\boldsymbol{\psi}$, if Alice produces the message m_1 given (x, r), and then Bob produces m_2 given (y, s) as well as m_1, and so forth. That is,

$$\mathsf{Pr}_{\Pi^{\Psi}}(m_1, \ldots, m_N|x, y, r, s) = \mathsf{Pr}(m_1|x, r) \cdot \mathsf{Pr}(m_2|y, s, m_1) \cdot \mathsf{Pr}(m_3|x, r, m_1, m_2) \cdot \ldots.$$

We get (8) by collecting the products of odd factors and of even factors separately as $\rho(x, r, m_1, \ldots, m_N)$ and $\sigma(y, s, m_1, \ldots, m_N)$.

We remark that the only property regarding the nature of a protocol we shall need in our results is the transcript factorization property. As such, our results stated for protocols in Theorem 11 and Theorem 12 are applicable more broadly to "pseudo protocols" which are distributions over transcripts satisfying (8), without necessarily being realizable using protocols [PP16].

The following claim about protocols (which holds for pseudo protocols as well) would be useful in our proofs. The proof for the same is provided in the full version [NPP20].

Claim 1. *Let Π^{Ψ} be a perfectly secure protocol for computing a deterministic functionality f. For any two edges $((x_1, a_1), (y_1, b_1))$ and $((x_2, a_2), (y_2, b_2))$ in the same connected component of G_f, for all transcripts $q \in \mathcal{Q}$, it holds that $\mathsf{Pr}_{\Pi^{\Psi}}(q|x_1, y_1, a_1, b_1) = \mathsf{Pr}_{\Pi^{\Psi}}(q|x_2, y_2, a_2, b_2)$.*

Private Simultaneous Messages & Conditional Disclosure of Secrets We refer to the full version [NPP20] for a detailed description of private simultaneous messages (PSM) and conditional disclosure of secrets (CDS). In this paper, we use statistically secure variants of both these models of secure computation. An ϵ-secure PSM protocol (represented as ϵ-PSM) guarantees that for every input (x, y), Carol recovers $f(x, y)$ with at least $1 - \epsilon$ probability and that whenever f evaluates to the same value for two different inputs, Carol's view for these inputs are at most ϵ far in statistical distance. An ϵ-secure CDS protocol (represented as ϵ-CDS) is defined similarly.

4 Feasibility Results

In this section, we present several feasibility and infeasibility results for our various models. For want of space, we defer the proofs of these results to the full version [NPP20]. Note that all our feasibility results are backward compatible and all the the impossibility results are forward compatible. That is, a SZCR implies a WZCR which in turn implies a ZCR, whereas, impossibility of a ZCR implies impossibility of WZCR which implies impossibility of SZCR. We define a simple predicate of interest, $\boldsymbol{\Phi}_{\mathsf{AND}} : \{0,1\} \times \{0,1\} \to \{0,1\}$, which refers to the AND predicate. The following show that any functionality has a SZCR with $\epsilon = 0$, i.e., perfect correctness and security, to appropriate predicates using no correlation.

Theorem 5. *For every (possibly randomized) functionality $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{A} \times \mathcal{B}$, there exists a predicate $\boldsymbol{\Phi}_f$ such that f has a perfect $\log(|\mathcal{A}||\mathcal{B}|)$-SZCR to $\boldsymbol{\Phi}_f$ using no correlation.*

Following theorem establishes that any functionality has a perfect SZCR to $\boldsymbol{\Phi}_{\mathsf{AND}}$ using an appropriate correlation.

Theorem 6. *For every deterministic functionality $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{A} \times \mathcal{B}$, there exists a correlation $\boldsymbol{\Psi}_f$ such that f has a perfect $\log(|\mathcal{X}||\mathcal{Y}|)$-SZCR to $\boldsymbol{\Phi}_{\mathsf{AND}}$ using $\boldsymbol{\Psi}_f$.*

We next look at the computational power of the predicate $\boldsymbol{\Phi}_{\mathsf{AND}}$ in the context of reductions using common randomness ($\boldsymbol{\Psi}^{\mathsf{CRS}}$). As we shall see in Lemma 3, every deterministic functionality has a perfect WZCR to $\boldsymbol{\Phi}_{\mathsf{AND}}$. In contrast, the next theorem shows that only simple functionalities have perfect SZCR to $\boldsymbol{\Phi}_{\mathsf{AND}}$ using common randomness.

Theorem 7. *A deterministic functionality f has a perfect μ-SZCR to $\boldsymbol{\Phi}_{\mathsf{AND}}$ using $\boldsymbol{\Psi}^{\mathsf{CRS}}$, for some $\mu < \infty$, if and only if it is simple.*

An even simpler predicate $\boldsymbol{\Phi}_{\mathsf{XOR}} : \{0,1\} \times \{0,1\} \to \{0,1\}$ refers to the XOR predicate. The following theorem shows that it has very limited power and even the AND function does not have a reduction to $\boldsymbol{\Phi}_{\mathsf{XOR}}$.

Theorem 8. *A deterministic functionality $f = (f_A, f_B)$ has a perfect μ-SZCR to $\boldsymbol{\Phi}_{\mathsf{XOR}}$ using $\boldsymbol{\Psi}^{\mathsf{CRS}}$, for some $\mu < \infty$, if and only if there exists sets $A \subseteq \mathcal{X}$ and $B \subseteq \mathcal{Y}$ such that,*

1. *For all $x \in \mathcal{X}$, $f_A(x,y) = f_A(x,y')$ if and only if $y, y' \in B$ or $y, y' \in \bar{B}$.*
2. *For all $y \in \mathcal{Y}$, $f_B(x,y) = f_B(x',y)$ if and only if $x, x' \in A$ or $x, x' \in \bar{A}$.*

Finally, we consider reducing a randomized functionality without inputs (i.e., a correlation) to a randomized predicate. To state our result, we define a measure of "productness" of a correlation $\boldsymbol{\Psi}$ over $\mathcal{R} \times \mathcal{S}$:

$$K(\boldsymbol{\Psi}) = \max_{(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2)} \min_{r \in \mathcal{R}, s \in \mathcal{S}} \frac{\mathsf{Pr}_{\boldsymbol{\lambda}_1}(r)\mathsf{Pr}_{\boldsymbol{\lambda}_1}(s)}{\mathsf{Pr}_{\boldsymbol{\Psi}}(r,s)}, \tag{9}$$

where the maximum[4] is taken over all pairs of distributions $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2$ over $\mathcal{R}$ and $\mathcal{S}$ respectively.

Theorem 9. *For any correlation $\boldsymbol{\psi}$ there exists a predicate $\boldsymbol{\phi}_{\boldsymbol{\psi}}$ such that $\boldsymbol{\psi}$ has a perfect μ-SZCR to $\boldsymbol{\phi}_{\boldsymbol{\psi}}$ using no correlation, where $\mu = -\log(K(\boldsymbol{\psi}))$. Further, if $\boldsymbol{\psi}$ has a perfect μ'-SZCR to any predicate $\boldsymbol{\phi}$ using no correlation, then $\mu' \geq \mu$.*

5 Lower Bounds via SZCR

SZCR provides a new route for approaching lower bound proofs. The high-level approach, for showing a lower bound for a certain complexity measure is in two parts:

- First show that an upper bound on that complexity measure implies an upper bound on a complexity measure related to SZCR.
- Then showing a lower bound for SZCR implies the desired lower bound.

The complexity measure related to SZCR that we use is what we call the invertible rank of a matrix associated with the function. In Section 5.2, we upper bound invertible rank by OT complexity. While invertible rank of a matrix (with respect to another matrix) is easy to define, establishing super-linear lower bounds for it is presumably difficult (circuit complexity lower bounds being a barrier). But currently, even showing the existence of functions whose matrices have super-linear invertible rank remains open. One may wonder if invertible rank would turn out to not have interesting lower bounds at all. In Section 5.3, we present some evidence that invertible rank has non-trivial lower bounds, as it is an upper bound on communication complexity, and use it to recover the best known lower bounds on OT complexity.

5.1 Linear algebraic characterization of SZCR

Conditions for SZCR naturally yield a linear algebraic characterization. In this section, we focus on perfect SZCR using no correlation (i.e., $(\mu, 0)$-SZCR).

A brief introduction to invertible rank was given in Section 1.3. Below, we shall formally define this quantity. But first, we set up some notation. It will be convenient to consider matrices as having elements indexed by pairs of elements $(a, b) \in \mathcal{A} \times \mathcal{B}$ for arbitrary finite sets $\mathcal{A}$ and $\mathcal{B}$. Below, for clarity, we write $M(a, b)$ instead of $M_{a,b}$ to denote the element indexed by (a, b) in the matrix M. For a matrix M indexed by $\mathcal{A} \times \mathcal{B}$, $[M]_{\triangleright}$ be the matrix indexed by $\mathcal{A} \times (\mathcal{B} \times \mathcal{A})$ and $[M]_{\triangleleft}$ be the matrix indexed by $\mathcal{A} \times (\mathcal{A} \times \mathcal{B})$ defined as follows: For all $a, a' \in \mathcal{A}$ and $b \in \mathcal{B}$,

$$[M]_{\triangleright}(a, (b, a')) = [M]_{\triangleleft}(a, (a', b)) = \begin{cases} M(a, b) & \text{if } a = a', \\ 0 & \text{otherwise.} \end{cases}$$

[4] The supremum is achieved since we are maximizing a continuous function over a compact set.

A matrix M with non-negative entries indexed by $\mathcal{A}\times\mathcal{B}$, is said to be *stochastic* if $\forall a \in \mathcal{A}$, $\sum_{b\in\mathcal{B}} M(a,b) = 1$. A matrix M indexed by $\mathcal{A} \times (\mathcal{B} \times \mathcal{C})$, is said to be $\mathcal{B}$-*block stochastic* if $\forall b \in \mathcal{B}$, $\sum_{a\in\mathcal{A},c\in\mathcal{C}} M(a,(b,c)) = 1$.

Though we shall define invertible rank generally for a matrix (w.r.t. another matrix), our motivation is to use it as a complexity measure of a possibly randomized function (w.r.t. a predicate). Towards this, we represent a function f using a matrix M_f, and also define a 0-1 matrix $P_{\mathbf{\Phi}}$ for a predicate $\mathbf{\Phi}$.

Definition 7. *For a (possibly randomized) function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{A} \times \mathcal{B}$, M_f is the matrix indexed by $(\mathcal{X} \times \mathcal{A})\times(\mathcal{Y}\times\mathcal{B})$, defined as follows: For all $(x,a) \in \mathcal{X}\times\mathcal{A}$ and $(y,b) \in \mathcal{Y} \times \mathcal{B}$,*

$$M_f((x,a),(y,b)) = \mathsf{Pr}_f(a,b|x,y).$$

For a predicate $\mathbf{\Phi} : \mathcal{U} \times \mathcal{V} \to \{0,1\}$, the matrix $P_{\mathbf{\Phi}}$ indexed by $\mathcal{U} \times \mathcal{V}$ is defined as follows. For all $(u,v) \in \mathcal{U} \times \mathcal{V}$,

$$P_{\mathbf{\Phi}}(u,v) = \mathbf{\Phi}(u,v)$$

Given a matrix P indexed by $\mathcal{U}\times\mathcal{V}$, the tensor-power $P^{\otimes k}$ is a matrix indexed by $\mathcal{U}^k\times\mathcal{V}^k$, where $P^{\otimes k}((u_1,\ldots,u_k),(v_1,\ldots,v_k)) = \prod_{i=1}^k P(u_i,v_i)$. We note that for the k-fold conjunction $\mathbf{\Phi}^k$ of a predicate $\mathbf{\Phi}$, we have $P_{\mathbf{\Phi}^k} = P_{\mathbf{\Phi}}^{\otimes k}$.

Now, we are ready to define the invertible rank of a matrix M w.r.t. a matrix P. To motivate the definition, consider M to be of the form M_f for a function $f : \mathcal{X}\times\mathcal{Y} \to \mathcal{A}\times\mathcal{B}$, and P to be of the form $P_{\mathbf{\Phi}}$ for some predicate $\mathbf{\Phi} : \mathcal{U}\times\mathcal{V} \to \{0,1\}$. Suppose $(\mathfrak{A},\mathfrak{B})$ is a (perfect) μ-ZCR from f to $\mathbf{\Phi}$. Consider a $\mathcal{U}\times(\mathcal{X}\times\mathcal{A})$ dimensional matrix A and a $\mathcal{V}\times(\mathcal{Y}\times\mathcal{B})$ dimensional matrix B corresponding to $\mathfrak{A}$ and $\mathfrak{B}$, respectively, as follows:

$$A(u,(x,a)) = \mathsf{Pr}_{\mathfrak{A}}(u,a|x) \qquad B(v,(y,b)) = \mathsf{Pr}_{\mathfrak{B}}(v,b|y).$$

Note that A is $\mathcal{X}$-block stochastic and B is $\mathcal{Y}$-block stochastic. Given a 0-1 matrix Q indexed by $\mathcal{U}\times\mathcal{V}$, with $Q(u,v) = \mathbf{\Phi}(u,v)$ for a predicate $\mathbf{\Phi}$, we can write the function implemented by the ZCR as a matrix $W = A^\intercal QB$, indexed by $(\mathcal{X}\times\mathcal{A})\times(\mathcal{Y}\times\mathcal{B})$. The probability of the ZCR accepting, given input (x,y), is $\sum_{a,b} W((x,a),(y,b))$. If $(\mathfrak{A},\mathfrak{B})$ is a (perfect) μ-WZCR from f to $\mathbf{\Phi}$, then we have $W = 2^{-\mu'}M_f$ for some $\mu' \le \mu$. This corresponds to the condition (10) below.

Now, if $(\mathfrak{A},\mathfrak{B})$ is a SZCR, we also have a security guarantee when either party is corrupt. Note that when both parties are honest, the *environment's* view of the protocol, consisting of (x,y,a,b), is specified by the matrix W above. But when Bob, say, is corrupt, the view also includes the message v that Bob sends to $\mathbf{\Phi}$, and hence it would be specified by a matrix indexed by $(\mathcal{X}\times\mathcal{A})\times(\mathcal{Y}\times\mathcal{B}\times\mathcal{V})$. This matrix can be written as $A^\intercal\cdot Q\cdot[B]_\triangleright$ (where $[B]_\triangleright$ "copies" the row index information of B to the column index, corresponding to v becoming visible outside the protocol). On the other hand, the security condition says that this view can be simulated by having $\hat{S}_B$ sample v given (y,b); $\hat{S}_B$ can be encoded in

a stochastic matrix H indexed by $(\mathcal{Y}\times\mathcal{B})\times\mathcal{V}$. The view of the environment in the simulated execution, taking into account the fact that it aborts with probability $1-2^{-\mu}$, can be written as $2^{-\mu}\,M_f\cdot[H]_\triangleleft$ (where $[H]_\triangleleft$ is derived from H by adding the row index information (y,b) to the column index v). This aspect of SZCR is reflected in (12) in the definition below. Similarly, (11) corresponds to security against corruption of Alice.

Thus the linear algebraic conditions in the definition below correspond to the existence of a μ-SZCR from f to $\boldsymbol{\Phi}^k$. The invertible rank of M_f w.r.t. $P_{\boldsymbol{\Phi}}$ corresponds to minimizing μ and k simultaneously (or more concretely, their sum).

Definition 8. *Given a matrix M indexed by $(\mathcal{X}\times\mathcal{A})\times(\mathcal{Y}\times\mathcal{B})$ and matrix P indexed by $\mathcal{U}\times\mathcal{V}$, the* μ^*-invertible rank of M w.r.t. P *is defined as*

$$\mathsf{IR}_P^{(\mu^*)}(M)=\min_{A,B,G,H,\mu} k$$

subject to $\mu\le\mu^*$ and

$$A^\intercal\cdot P^{\otimes k}\cdot B=2^{-\mu}\,M, \tag{10}$$

$$[A]_\triangleright^\intercal\cdot P^{\otimes k}\cdot B=2^{-\mu}\,[G]_\triangleleft^\intercal\cdot M, \tag{11}$$

$$A^\intercal\cdot P^{\otimes k}\cdot[B]_\triangleright=2^{-\mu}\,M\cdot[H]_\triangleleft, \tag{12}$$

where A is a $\mathcal{X}$-block stochastic matrix indexed by $\mathcal{U}^k\times(\mathcal{X}\times\mathcal{A})$, B is a $\mathcal{Y}$-block stochastic matrix indexed by $\mathcal{V}^k\times(\mathcal{Y}\times\mathcal{B})$, G is a stochastic matrix indexed by $(\mathcal{X}\times\mathcal{A})\times\mathcal{U}^k$, and H is a stochastic matrix indexed by $(\mathcal{Y}\times\mathcal{B})\times\mathcal{V}^k$.

The invertible rank of M w.r.t. P *is defined as*

$$\mathsf{IR}_P(M)=\min_\mu\ \mathsf{IR}_P^{(\mu)}(M)+\mu.$$

As discussed above, a $(\mu,0)$-SZCR from f to $\boldsymbol{\Phi}^k$ (using no correlation) corresponds to the existence of matrices A,B,G,H that satisfy the conditions (10)-(12). Then the invertible rank of M_f w.r.t. $P_{\boldsymbol{\Phi}}$ would be upper bounded by $\mu+k$. This is captured in the following theorem (proven in the full version [NPP20].

Theorem 10. *For a (possibly randomized) functionality $f:\mathcal{X}\times\mathcal{Y}\to\mathcal{A}\times\mathcal{B}$ and a predicate $\boldsymbol{\Phi}:\mathcal{U}\times\mathcal{V}\to\{0,1\}$, f has a perfect μ-SZCR to $\boldsymbol{\Phi}$ using no correlation if and only if $\mathsf{IR}_{P_{\boldsymbol{\Phi}}}^{(\mu)}(M_f)\le 1$. Further, if f has a perfect μ-SZCR to $\boldsymbol{\Phi}^k$ using no correlation then $\mathsf{IR}_{P_{\boldsymbol{\Phi}}}(M_f)\le\mu+k$.*

Invertible Rank w.r.t. OT. Let P_{OT} denote the matrix that corresponds to the predicate $\boldsymbol{\Phi}_{\mathsf{supp}(\mathsf{OT})}$.[5] It can be written as the following circulant matrix:

$$P_{\mathsf{OT}}=\begin{bmatrix}1&0&0&1\\1&1&0&0\\0&1&1&0\\0&0&1&1\end{bmatrix}$$

[5] More generally, for a correlation $\boldsymbol{\Psi}$, the 0-1 matrix corresponding to the associated predicate $\boldsymbol{\Phi}_{\mathsf{supp}(\boldsymbol{\Psi})}$ will be denoted as $P_{\boldsymbol{\Psi}}$.

We present a conjecture on the existence of functions f which have super-linear invertible ranks with respect to P_{OT}.

*Conjecture 1 (**Invertible Rank Conjecture**).* There exists a family of functions $f_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\} \times \{0,1\}$ such that $\mathsf{IR}_{P_{\mathsf{OT}}}(M_{f_n}) = \omega(n)$.

Proving this conjecture, for a family of common-information-free functions, would imply super-linear lower bounds for OT complexity, thanks to Corollary 1 in the sequel. Finding such an explicit family f_n would be a major breakthrough, as it would give a function family with super-linear circuit complexity.

On the other hand, a weakly exponential upper bound of $2^{\tilde{O}(\sqrt{n})}$ exists on invertible rank of n-bit input functions, as implied by an upper bound on OT-complexity [BIKK14], re-instantiated using the 2-server PIR protocols of [DG16].

The following corollary of Theorem 10 and Theorem 3 gives a purely linear algebraic problem – namely, lower bounding invertible rank – that can yield OT complexity lower bounds.

Corollary 1. *If a deterministic common-information-free functionality $f : \{0,1\}^n \times \{0,1\}^n \to \mathcal{A} \times \mathcal{B}$ has OT-complexity m, then $\mathsf{IR}_{P_{\mathsf{OT}}}(M_f) = O(m+n)$.*

Proof: Recall that by Theorem 3, there exists a μ-SZCR from f to $\boldsymbol{\Phi}_{\mathsf{supp}(\mathsf{OT}^{m+1})}$, where $\mu = m + O(n)$. We will use the further guarantee that, since f is common-information-free, this SZCR does not use any correlation. Then, by Theorem 10, we have $\mathsf{IR}_{P_{\mathsf{OT}}}(M_f) \leq (m+1) + \mu = O(m+n)$.[6] □

5.2 SZCR vs. OT Complexity

In this section we prove Theorem 3 and its extensions, that show that SZCR lower bounds translate to lower bounds for OT-complexity, or more generally, 2PC complexity w.r.t. any *regular* correlation $\boldsymbol{\psi}$ (see Section 3). Our main result in this section is Theorem 11, where we transform a perfectly secure 2PC protocol for a general deterministic functionality f using a regular correlation $\boldsymbol{\psi}$, into a SZCR from f to the predicate $\boldsymbol{\Phi}_{\mathsf{supp}^*(\boldsymbol{\psi})}$. (Recall from Section 3 that $\boldsymbol{\Phi}_{\mathsf{supp}^*(\boldsymbol{\psi})}$ is a predicate that evaluates to 1 on inputs $(u,v) \in \mathsf{supp}(\boldsymbol{\psi})$; it allows u or v to be the symbol $\perp$, in which case it evaluates to 0.) Theorem 3 follows from this result when $\boldsymbol{\psi}$ is taken as OT^m.

Theorem 11. *If protocol Π^{Ψ} using regular correlation $\boldsymbol{\psi}$ distributed over $\mathcal{U} \times \mathcal{V}$ computes a deterministic functionality $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{A} \times \mathcal{B}$ with perfect security, then f has a μ-SZCR to $\boldsymbol{\Phi}_{\mathsf{supp}^*(\boldsymbol{\psi})}$ using $\boldsymbol{\psi}^{\mathsf{CRS}}$, where $\mu = \log \frac{|\mathcal{U}|\,|\mathcal{V}||\mathcal{X}|^2|\mathcal{Y}|^2}{|\mathsf{supp}(\boldsymbol{\psi})|}$.*

Additionally, if f is common-information-free, then f has a μ'-SZCR to $\boldsymbol{\Phi}_{\mathsf{supp}^*(\boldsymbol{\psi})}$ using no correlation, where $\mu' = \log \frac{|\mathcal{U}|\,|\mathcal{V}||\mathcal{X}||\mathcal{Y}|}{|\mathsf{supp}(\boldsymbol{\psi})|}$.

[6] Using the sharper statement from Theorem 11, we would have $\mu = m + 2n$, and hence we have $\mathsf{IR}_{P_{\mathsf{OT}}}(M_f) \leq 2(m+n) + 1$.

A proof of this theorem is provided in the full version [NPP20]. Theorem 3 is obtained by specializing the above result to the correlation of OT.

Proof: [Proof of Theorem 3] A single instance of OT is a regular correlation with its support being a 1/2 fraction of its entire domain (see the matrix P_{OT}). Hence m independent OTs form a regular correlation OT^m distributed over $\mathcal{U} \times \mathcal{V} = \{0,1\}^{2m} \times \{0,1\}^{2m}$ such that $\frac{|\mathsf{supp}(\mathsf{OT}^m)|}{|\mathcal{U}||\mathcal{V}|} = \frac{1}{2^m}$. Invoking Theorem 11 for $|\mathcal{X}| = |\mathcal{Y}| = 2^n$, we get a μ-SZCR from f to $\boldsymbol{\Phi}_{\mathsf{supp}^*(\mathsf{OT}^m)}$ using $\boldsymbol{\Psi}^{\mathsf{CRS}}$, where $\mu = \log \frac{|\mathcal{U}||\mathcal{V}||\mathcal{X}|^2|\mathcal{Y}|^2}{|\mathsf{supp}(\mathsf{OT}^m)|} = m + 4n$. (If f is common-information-free, i.e., it has a single connected component in G_f, then $\boldsymbol{\Psi}^{\mathsf{CRS}}$ is not needed and $\mu = m + 2n$.)

Recall that the domain of $\boldsymbol{\Phi}_{\mathsf{supp}^*(\mathsf{OT}^m)}$ contains a special symbol $\perp$, in addition to $2m$ bit long strings that are in the support of OT^m. It is not hard to see that we can implement the functionality of this symbol $\perp$ using an additional instance of OT. That is, every (u, v) in the domain of $\boldsymbol{\Phi}_{\mathsf{supp}^*(\mathsf{OT}^m)}$ can be encoded as $(\hat{u}, \hat{v})$ in the domain of $\boldsymbol{\Phi}_{\mathsf{supp}(\mathsf{OT}^{m+1})}$ so that $\boldsymbol{\Phi}_{\mathsf{supp}^*(\mathsf{OT}^m)}(u, v) = \boldsymbol{\Phi}_{\mathsf{supp}(\mathsf{OT}^{m+1})}(\hat{u}, \hat{v})$. Hence, f has a μ-SZCR to $\boldsymbol{\Phi}_{\mathsf{supp}(\mathsf{OT}^{m+1})}$ using a $\boldsymbol{\Psi}^{\mathsf{CRS}}$ (or, if f is common-information-free, using no correlation). □

We also prove Theorem 12, which is a "dual version" of Theorem 11: Here, when the protocol Π^{Ψ} is transformed into a SZCR, instead of $\boldsymbol{\Psi}$ transforming into the predicate, it remains a correlation that is used by the reduction; this reduction is to the constant-sized predicate $\boldsymbol{\Phi}_{\mathsf{AND}}$.

Theorem 12. *Suppose Π^{Ψ} is a perfectly secure protocol for a deterministic functionality $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{A} \times \mathcal{B}$, that uses a regular correlation $\boldsymbol{\Psi}$ over $\mathcal{R} \times \mathcal{S}$. Then f has a μ-SZCR to $\boldsymbol{\Phi}_{\mathsf{AND}}$ using $\boldsymbol{\Psi}$, where $\mu = \log |\mathcal{X}||\mathcal{Y}||\mathcal{R}||\mathcal{S}|$.*

The reduction and its analysis is similar to that in Theorem 11. A detailed proof is provided in the full version [NPP20].

5.3 Communication Complexity vs. SZCR

In this section, we lower bound the domain size of a predicate $\boldsymbol{\Phi}$ to which a functionality has a non-trivial SZCR. In combination with Theorem 11, which provides an upper bound on the domain size of the predicate in terms of OT complexity, we obtain a lower bound on OT complexity in terms of (one-way) communication complexity, reproducing a result of [BM04].

More precisely, the connection between the domain size of $\boldsymbol{\Phi}$ and the communication complexity of f is captured below. To be able to base the lower bound on the *one-way communication complexity* of f, we consider a one-sided functionality f.

Lemma 2. *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{A} \times \{\perp\}$ be a deterministic one-sided functionality such that for all y, y' there exists some x such that $f_A(x, y) \neq f_A(x, y')$. For any predicate $\boldsymbol{\Phi} : \mathcal{U} \times \mathcal{V} \to \{0,1\}$, and $\mu > 0$, f has a perfect μ-SZCR to $\boldsymbol{\Phi}$ using no correlation only if $|\mathcal{V}| \geq |\mathcal{Y}|$.*

Proof: We will show that if f has a perfect μ-SZCR to $\boldsymbol{\Phi}$ using no correlation, then there exists a one-way communication protocol for computing f_A, where the message is an element of the set $\mathcal{V}$. By our assumption, no two inputs of Bob are equivalent w.r.t. f_A. Hence in a one-way communication protocol for f_A, Bob must communicate his exact input to Alice. This implies that $|\mathcal{V}| \geq |\mathcal{Y}|$.

Suppose $(\mathfrak{A}, \mathfrak{B})$ is a μ-SZCR from f to the predicate $\boldsymbol{\Phi}$ using no correlation. Consider the jointly distributed random variables (U, A, V, D) (as described in Figure 1), conditioned on input (x, y). Since $f_B(x, y) = \perp$ for all (x, y), the security condition (3) (for $\epsilon = 0$) guarantees that $\mathsf{Pr}(v|x, y, D = 1) = \mathsf{Pr}(\hat{S}_B(y, \perp, 1) = v)$, for all x, y, v.

The one-way communication protocol for computing f when Alice and Bob have inputs x and y, respectively can be described as follows. Bob picks a v in the support of the distribution $\hat{S}_B(y, \perp, 1)$, and sends it to Alice. Alice, chooses $(u, a) \in \mathcal{U} \times \mathcal{A}$ such that $\mathsf{Pr}_{\mathfrak{A}}(u, a|x) > 0$ and $\boldsymbol{\Phi}(u, v) = 1$, and outputs a. Existence of such a pair (u, a) is argued as follows. By non-triviality of the SZCR, $\mathsf{Pr}(D = 1|x, y) > 0$ and since v is in the support of $\hat{S}_B(y, \perp, 1)$,

$$\mathsf{Pr}(v|x, y, D = 1) = \mathsf{Pr}(\hat{S}_B(y, \perp, 1) = v) > 0.$$

Hence, $\mathsf{Pr}(D = 1|x, y, v) > 0$. This implies that there exists (u, a) such that $\mathsf{Pr}(a, u, v, D = 1|x, y) > 0$. The new one-way communication protocol is correct since the perfect correctness of $(\mathfrak{A}, \mathfrak{B})$ implies that $a = f_A(x, y)$. □

Corollary 2. *If f is a deterministic functionality with one-sided output, such that for all y, y' there exists some x such that $f_A(x, y) \neq f_A(x, y')$, then its OT complexity is lower bounded by its one-way computation complexity.*

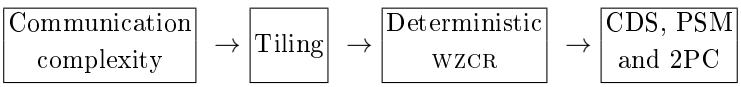
Proof: Since f is a one-sided (hence common-information-free) functionality, by Theorem 11 f has a perfect non-trivial SZCR to $\boldsymbol{\Phi}_{\mathsf{supp}(\mathsf{OT}^{m+1})}$ using no correlation if the OT complexity of f is m. Since f is one-sided, by Lemma 2, 2^{m+1} is at least the size of the domain of the non-computing user. This proves the claim. □

6 Upper Bounds

In this section, we show that ZCR provides a new path to protocols in different secure computation models. In Section 6.1, we obtain upper bounds on CDS, PSM and 2PC, in terms of the *communication complexity* of the functions being computed, followed by improved upper bounds in Section 6.2 which leverage ZCR and its connections to information complexity.

6.1 Upper Bounds using Communication Complexity

In this section, we follow the outline below to prove Theorem 1.



For a deterministic function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$, a k-tiling is the partition of $\mathcal{X} \times \mathcal{Y}$ into k monochromatic rectangles – i.e., sets $R_1, \ldots, R_k$ such that $R_i = \mathcal{X}_i \times \mathcal{Y}_i$ and $\exists z_i \in \mathcal{Z}$ s.t., $\forall (x, y) \in R_i$, $f(x, y) = z_i$. (Then, abusing the notation, we write $f(R_i)$ to denote z_i.) We refer to the smallest number k such that f has a k-tiling, as the tiling number of f. The first step above is standard: Communication complexity of ℓ implies a protocol with at most 2^ℓ transcripts, and the inputs consistent with each transcript corresponds to a monochromatic tile.

The last step requires a (non-trivial) perfect deterministic WZCR from f to (say) $\boldsymbol{\Phi}_{\mathsf{AND}}$ using $\boldsymbol{\Psi}^{\mathsf{CRS}}$. If ℓ is the length of the common random string supplied by $\boldsymbol{\Psi}^{\mathsf{CRS}}$, the resulting CDS, PSM or 2PC (in the OT-hybrid model) protocols for f, will have $O(2^\ell)$ communication complexity (as well as OT complexity, in the case of 2PC). Further, we show that such a WZCR can be readily constructed from a tiling for f, with 2^ℓ tiles. Lemma 3 summarizes the upperbounds we obtain using such constructions under different secure computation models. The detailed construction of all the protocols are relegated to the full version [NPP20].

Lemma 3. *For a deterministic function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$, if f admits a k-tiling, then the following exist.*

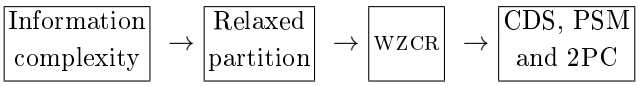
1. *A perfectly secure CDS for predicate f (when $\mathcal{Z} = \{0, 1\}$) with $O(k)$ communication.*
2. *A perfectly secure PSM for f with $O(k \log |\mathcal{Z}|)$ communication.*
3. *A perfectly secure 2-party symmetric secure function evaluation protocol for f, against passive corruption, with $O(k \log |\mathcal{Z}|)$ communication and OT invocations.*

Remark 1. In our proof of the above lemma, we show a $(\mu, 0)$-WZCR for *any* deterministic functionality $g : \mathcal{X} \times \mathcal{Y} \to \mathcal{A} \times \mathcal{B}$ to $\boldsymbol{\Phi}_{\mathsf{AND}}$ (with $\mu = \log(k_1 \cdot k_2)$ where k_1 and k_2 are the tiling numbers of g_A and g_B, respectively). This is in contrast with Theorem 7 where we showed that only simple functions have a $(\mu, 0)$-SZCR to $\boldsymbol{\Phi}_{\mathsf{AND}}$ for any $\mu > 0$.

Lemma 3, combined with the fact that a communication complexity of ℓ implies a tiling with at most 2^ℓ tiles, proves Theorem 1.

6.2 Upper Bounds using Information Complexity

In this section we follow the outline below to prove Theorem 2.



In Section 6.2.1, we present the definitions as well as the first step from [KLL+15], and show how a relaxed partition of f can be turned into a WZCR for f. Then, in Section 6.2.2, we show how a WZCR (in fact, a ZCR) can be transformed into (statistically secure) PSM, CDS, and 2PC protocols. A detailed form of the final result is presented in Theorem 13 (from which Theorem 2 follows).

6.2.1 Information Complexity and Relaxed Partition First, we define information complexity and relaxed partition bound.

Information Complexity. Consider a deterministic function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ and a possibly randomized non-secure protocol Π for computing f. When Π is executed with $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, respectively, as inputs of Alice and Bob, let $\Pi(x, y)$ be the random variable for the transcript of the protocol, and let A and B denote the outputs of Alice and Bob, respectively. For jointly distributed random variables (X, Y) over $\mathcal{X} \times \mathcal{Y}$, the error of the protocol $\mathsf{error}^f_{X,Y}(\Pi) = \mathsf{Pr}[A \neq f(X, Y) \text{ or } B \neq f(X, Y)]$. For $\epsilon \geq 0$, information complexity of a function is defined as

$$\mathsf{IC}_\epsilon(f) = \max_{\mathsf{p}(X,Y)} \min_{\Pi:\mathsf{error}^f_{X,Y}(\Pi)\leq\epsilon} I(X; \Pi(X, Y)|Y) + I(Y; \Pi(X, Y)|X).$$

Relaxed Partition. Relaxed partition bound was originally defined in [KLL+15], extending partition bound defined in [JK10]. Here we provide an equivalent definition of the relaxed partition bound that makes the connection with WZCR clearer.

Definition 9 (Relaxed partition bound). *Consider a deterministic function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$. For every rectangle $R \in 2^{\mathcal{X}} \times 2^{\mathcal{Y}}$ and $z \in \mathcal{Z}$, let $w(R, z) \in [0, 1]$. The* relaxed partition bound *for $\epsilon \geq 0$, denoted by $\bar{\mathsf{prt}}_\epsilon(f)$, is defined as $\min \frac{1}{\eta}$ subject to: $\sum_{R,z} w(R, z) = 1$,*

$$\sum_{R:(x,y)\in R} w(R, f(x, y)) \geq \eta(1 - \epsilon), \qquad \forall (x, y) \in \mathcal{X} \times \mathcal{Y}$$

$$\sum_{R:(x,y)\in R} \sum_{z\in\mathcal{Z}} w(R, z) \leq \eta, \qquad \forall (x, y) \in \mathcal{X} \times \mathcal{Y}$$

$$w(R, z) \geq 0. \qquad \forall R \in 2^{\mathcal{X}} \times 2^{\mathcal{Y}}, z \in \mathcal{Z}$$

The following proposition restates a theorem due to Kerenidis et al. [KLL+15] that gives a connection between relaxed partition bound and information complexity. The statement has been modified for our purposes.

Proposition 1 (Theorem 1.1 in [KLL+15]). *There is a positive constant C such that for every function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ and $\epsilon > 0$,*

$$\log \bar{\mathsf{prt}}_{2\epsilon}(f) \leq \left(\frac{9C \cdot \mathsf{IC}_\epsilon(f)}{\epsilon^2} + \frac{3C}{\epsilon} + \log |\mathcal{Z}| \right).$$

See the full version [NPP20] for details on the modification of [KLL+15, Theorem 1.1] which gives the above form. Interestingly, this result is established in [KLL+15] via a notion of *zero communication protocols*, which is similar to (albeit more restricted than) our notion of ZCR. This is not surprising given the close connection between relaxed partition bound and WZCR that we establish below. The following lemma is proved in the full version [NPP20].

Lemma 4. *For any $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$, functionality (f, f) has a (μ, ϵ)-WZCR to $\boldsymbol{\phi}_{\mathsf{AND}}$ using $\boldsymbol{\psi}^{\mathsf{CRS}}$, where $\mu = \log \frac{\bar{\mathsf{prt}}_\epsilon(f)}{1-\epsilon}$.*

6.2.2 From ZCR to Secure Computation In this section we use ZCR to construct protocols for statistically secure PSM, CDS and secure 2PC. To accomplish this, the parties carry out the ZCR protocol n times, for n sufficiently large as to guarantee (except with negligible probability) that there will be at least one instance which would accept. Amongst these n executions, a selector function selects the candidate outputs corresponding to a reduction in which the predicate is accepted, without revealing the the execution itself. For this we use the notion of selector functions, which we next define. We conclude this section with Theorem 13, which formally states and proves the claim in Theorem 2.

Definition 10. *For a predicate $\mathbf{\Phi} : \mathcal{U} \times \mathcal{V} \to \{0,1\}$, finite set $\mathcal{Z}$ and $t \in \mathbb{N}$, we define selector function $\mathsf{Sel}^{\mathbf{\Phi},\mathcal{Z},t} : \mathcal{U}^t \times \mathcal{Z}^t \times \mathcal{V}^t \to \mathcal{Z}$ as follows.*
For $u^t := (u_1, \ldots, u_t) \in \mathcal{U}^t, v^t := (v_1, \ldots, v_t) \in \mathcal{V}^t$ and $z^t := (z_1, \ldots, z_t) \in \mathcal{Z}^t$,

$$\mathsf{Sel}^{\mathbf{\Phi},\mathcal{Z},t}(u^t, v^t, z^t) = \begin{cases} z_i \text{ if } \exists i \text{ s.t. } \mathbf{\Phi}(u_i, v_i) = 1, \forall j > i, \mathbf{\Phi}(u_j, v_j) = 0, \\ z^* \text{ otherwise.} \end{cases}$$

Here, z^* is a fixed arbitrary member of $\mathcal{Z}$. For the specific case where $\mathcal{Z} = \{0,1\}$, we will set $z^* = 0$.

Selector function for the predicate $\mathbf{\Phi}_{\mathsf{AND}}$ is of special interest. The following lemma shows that for $t \in \mathbb{N}$ and finite set $\mathcal{Z}$, there is an efficient PSM protocol and a secure 2-party protocol that compute $\mathsf{Sel}^{\mathbf{\Phi}_{\mathsf{AND}},\mathcal{Z},t}$, when Alice and Bob get inputs $(u^t, z^t) \in \mathcal{U}^t \times \mathcal{Z}^t$ and $v^t \in \mathcal{V}^t$, respectively. When $\mathcal{Z} = \{0,1\}$, there is an efficient protocol for CDS with predicate $\mathsf{Sel}^{\mathbf{\Phi}_{\mathsf{AND}},\mathcal{Z},t}$. We use this to show upper bounds for communication complexity of statistically secure PSM and CDS protocols, and for OT complexity and communication complexity of statistically secure 2PC.

Lemma 5. *The following statements hold for the predicate $\mathbf{\Phi}_{\mathsf{AND}}$, $t \in \mathbb{N}$ and a finite set $\mathcal{Z}$.*

(i). $\mathsf{Sel}^{\mathbf{\Phi}_{\mathsf{AND}},\mathcal{Z},t} : (\mathcal{U}^t \times \mathcal{Z}^t) \times \mathcal{V}^t \to \mathcal{Z}$ *has perfect PSM with communication complexity $O(t^2 \cdot \log|\mathcal{Z}|)$.*

(ii). *CDS for the predicate* $\mathsf{Sel}^{\mathbf{\Phi}_{\mathsf{AND}},\{0,1\},t} : (\mathcal{U}^t \times \{0,1\}^t) \times \mathcal{V}^t \to \{0,1\}$ *and domain $\{0,1\}$ has communication complexity $O(t)$.*

(iii). *The functionality* $\left(\mathsf{Sel}^{\mathbf{\Phi}_{\mathsf{AND}},\mathcal{Z},t}, \mathsf{Sel}^{\mathbf{\Phi}_{\mathsf{AND}},\mathcal{Z},t}, \right) : (\mathcal{U}^t \times \mathcal{Z}^t) \times \mathcal{V}^t \to \mathcal{Z} \times \mathcal{Z}$ *has a perfectly secure 2PC protocol with communication complexity and OT complexity $O(t \cdot \log|\mathcal{Z}|)$.*

Since there are efficient PSM protocols for branching programs, the first statement is shown by providing a small branching program for $\mathsf{Sel}^{\mathbf{\Phi}_{\mathsf{AND}},\mathcal{Z},t}$. Statements (ii) and (iii) are proved by showing that $\mathsf{Sel}^{\mathbf{\Phi}_{\mathsf{AND}},\{0,1\},t}$ and $\mathsf{Sel}^{\mathbf{\Phi}_{\mathsf{AND}},\mathcal{Z},t}$, respectively, have small formulas [FKN94], [IK97]. The detailed proof is provided in the full version [NPP20].

We now proceed to give constructions for *statistically secure* PSM, CDS and 2PC using ZCR. All the three constructions follow the same framework. We start

with ZCR of a functionality f to predicate $\boldsymbol{\Phi}$. The ZCR is executed (independently) sufficiently many times to guarantee that at least one of the executions satisfy the predicate but with negligible probability. The output of a reduction in which the predicate was accepted is securely chosen using the selector function for the predicate. Following lemma summarizes the upper bounds we obtain for statistically secure PSM, CDS and 2PC *via.* constructions using ZCR. Detailed proof of the lemma is provided in the full version [NPP20].

Lemma 6. *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a deterministic function and $\perp$ be a constant function with the same domain If $(f, \perp)$ has a (μ, ϵ)-ZCR to $\boldsymbol{\Phi}$ using $\boldsymbol{\Psi}^{\mathsf{CRS}}$, then for $t = 2^{\mu} \ln \frac{1}{\epsilon}$, we obtain the following upper bound.*

1. *The 4ϵ-PSM complexity of f is at most the PSM complexity of the selector function $\mathsf{Sel}^{\boldsymbol{\Phi},\mathcal{Z},t} : (\mathcal{U}^t \times \mathcal{Z}^t) \times \mathcal{V}^t \to \mathcal{Z}$.*
2. *The communication complexity of 4ϵ-CDS for predicate f (when $\mathcal{Z} = \{0,1\}$) is at most that of CDS for predicate $\mathsf{Sel}^{\boldsymbol{\Phi},\mathcal{Z},t} : (\mathcal{U}^t \times \mathcal{Z}^t) \times \mathcal{V}^t \to \mathcal{Z}$.*
3. *The communication complexity (respectively, OT complexity) of 4ϵ-secure computation of the functionality (f, f) is at most the communication complexity (respectively, OT complexity) of perfectly secure computation of the symmetric functionality $\left(\mathsf{Sel}^{\boldsymbol{\Phi},\mathcal{Z},t}, \mathsf{Sel}^{\boldsymbol{\Phi},\mathcal{Z},t}\right) : (\mathcal{U}^t \times \mathcal{Z}^t) \times \mathcal{V}^t \to \mathcal{Z} \times \mathcal{Z}$.*

Theorem 13. *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a deterministic function and $\epsilon > 0$. There exists a positive constant C such that for*

$$K = 2^{\left(\frac{9C \cdot \mathsf{IC}_{\epsilon}(f)}{\epsilon^2} + \frac{3C}{\epsilon} + \log|\mathcal{Z}|\right)} \cdot \left(\frac{\ln(1/2\epsilon)}{1-2\epsilon}\right),$$

1. *The communication complexity of 8ϵ-PSM of f is $O\left(K^2 \log|\mathcal{Z}|\right)$.*
2. *The communication complexity of 8ϵ-CDS for predicate f (when $\mathcal{Z} = \{0,1\}$) and domain $\{0,1\}$ is $O(K)$.*
3. *The OT complexity and communication complexity of 8ϵ-secure computation of f is $O\left(K \log|\mathcal{Z}|\right)$.*

Proof: The statistically secure protocols described in the above lemma taken together with the connection between WZCR and information complexity allow us to prove our upper bounds on complexities in terms of information complexity for these models. Specifically, it follows from Proposition 1 and Lemma 4 that (f, f) (hence $(f, \perp)$) has a $(\mu, 2\epsilon)$-ZCR to $\boldsymbol{\Phi}_{\mathsf{AND}}$ using $\boldsymbol{\Psi}^{\mathsf{CRS}}$, where

$$\mu \leq \log \frac{1}{1-2\epsilon} \cdot \left(\frac{9C \cdot \mathsf{IC}_{\epsilon}(f)}{\epsilon^2} + \frac{3C}{\epsilon} + \log|\mathcal{Z}|\right).$$

Using the statement 1 in Lemma 6 along with Lemma 5, we can now show that there exists an 8ϵ-PSM protocol for f with communication complexity $O\left(\left(2^{\mu} \cdot \log \frac{1}{2\epsilon}\right)^2 \cdot \log|\mathcal{Z}|\right)$. Similarly, using statement 2 in Lemma 6 and Lemma 5, we can show that there is an 8ϵ-CDS protocol for predicate f with communication complexity $O\left(2^{\mu} \cdot \log \frac{1}{2\epsilon} \cdot \log|\{0,1\}|\right)$. And using statement 3 in Lemma 6 and Lemma 5, we can show that there is an 8ϵ-secure 2-party protocol for f with communication complexity $O\left(2^{\mu} \cdot \log \frac{1}{2\epsilon} \cdot \log|\mathcal{Z}|\right)$. This proves the theorem. □

Acknowledgements

This research was supported by Ministry of Science and Technology, Israel and Department of Science and Technology, Government of India, under Joint Indo-Israel Project DST/INT/ISR/P-16/2017. V. Narayanan and V. Prabhakaran were supported by the Department of Atomic Energy, Government of India, under project no. RTI4001; M. Prabhakaran was supported by the Dept. of Science and Technology, India via the Ramanujan Fellowship; V. Narayanan acknowledges the discussions with Tulasi Mohan Molli on various topics in communication complexity.

References

AA18. Benny Applebaum and Barak Arkis. On the power of amortization in secret sharing: d-uniform secret sharing and cds with constant information rate. In *Theory of Cryptography*, pages 317–344, 2018.

AHMS18. Benny Applebaum, Thomas Holenstein, Manoj Mishra, and Ofer Shayevitz. The communication complexity of private simultaneous messages, revisited. In *EUROCRYPT*, pages 261–286, 2018.

ALSV13. Noga Alon, Troy Lee, Adi Shraibman, and Santosh S. Vempala. The approximate rank of a matrix and its algorithmic applications. In *STOC*, pages 675–684, 2013.

AR17. Benny Applebaum and Pavel Raykov. From private simultaneous messages to zero-information arthur–merlin protocols and back. *Journal of Cryptology*, 30:961–988, 2017.

AW17. Josh Alman and R. Ryan Williams. Probabilistic rank and matrix rigidity. In *STOC*, pages 641–652, 2017.

BIKK14. Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. In *Theory of Cryptography*, pages 317–342, 2014.

BM04. Amos Beimel and Tal Malkin. A quantitative approach to reductions in secure computation. In *TCC*, pages 238–257, 2004.

BW16. Mark Braverman and Omri Weinstein. A discrepancy lower bound for information complexity. *Algorithmica*, pages 846–864, 2016.

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

DG16. Zeev Dvir and Sivakanth Gopi. 2-server PIR with subpolynomial communication. *J. ACM*, 63(4):39:1–39:15, 2016.

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

GG99. Nicolas Gisin and Bernard Gisin. A local hidden variable model of quantum correlation exploiting the detection loophole. *Physics Letters A*, 260(5):323–327, 1999.

GIKM00. Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. Protecting data privacy in private information retrieval schemes. *J. Comput. Syst. Sci.*, 60(3):592–629, 2000.

GKR15. Anat Ganor, Gillat Kol, and Ran Raz. Exponential separation of information and communication for boolean functions. In *STOC*, pages 557–566, 2015.

Gol04. Oded Goldreich. *Foundations of Cryptography: Basic Applications*. Cambridge University Press, 2004.

IK97. Yuval Ishai and Eyal Kushilevitz. Private simultaneous messages protocols with applications. In *ISTCS*, pages 174–184, 1997.

JK10. Rahul Jain and Hartmut Klauck. The partition bound for classical communication complexity and query complexity. In *CCC*, pages 247–258, 2010.

KLL+15. Iordanis Kerenidis, Sophie Laplante, Virginie Lerays, Jérémie Roland, and David Xiao. Lower bounds on information complexity via zero-communication protocols and applications. *SIAM Journal on Computing*, 44(5):1550–1572, 2015.

KN97. Eyal Kushilevitz and Noam Nisan. *Communication complexity*. Cambridge University Press, New York, 1997.

LVW17. Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Conditional disclosure of secrets via non-linear reconstruction. In *CRYPTO*, pages 758–790, 2017.

LVW18. Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Towards breaking the exponential barrier for general secret sharing. In *EUROCRYPT*, pages 567–596, 2018.

MPR12. Hemanta Maji, Manoj Prabhakaran, and Mike Rosulek. A unified characterization of completeness and triviality for secure function evaluation. In *INDOCRYPT*, pages 40–59, 2012.

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.

NPP20. V. Narayanan, M. Prabhakaran, and V. Prabhakaran. Zero-communication reductions. In *Cryptology ePrint Archive*, 2020.

PP14. Vinod Prabhakaran and Manoj Prabhakaran. Assisted common information with an application to secure two-party sampling. *Information Theory, IEEE Transactions on*, 60(6):3413–3434, 2014.

PP16. Manoj M. Prabhakaran and Vinod M. Prabhakaran. Rényi information complexity and an information theoretic characterization of the partition bound. In *ICALP*, pages 88:1–88:14, 2016.

PR17. Toniann Pitassi and Robert Robere. Strongly exponential lower bounds for monotone computation. In *STOC*, pages 1246–1255, 2017.

PS86. Ramamohan Paturi and Janos Simon. Probabilistic communication complexity. *J. Comput. Syst. Sci.*, 33(1):106–123, 1986.

Raz90. Alexander A. Razborov. Applications of matrix methods to the theory of lower bounds in computational complexity. *Combinatorica*, 10(1):81–93, 1990.

RPRC16. Robert Robere, Toniann Pitassi, Benjamin Rossman, and Stephen A. Cook. Exponential lower bounds for monotone span programs. In *FOCS*, pages 406–415, 2016.

Val77. Leslie G. Valiant. Graph-theoretic arguments in low-level complexity. In *Mathematical Foundations of Computer Science*, pages 162–176, 1977.