The Round Complexity of Statistical MPC with Optimal Resiliency

Benny Applebaum
Tel-Aviv University, Tel-Aviv, Israel
bennyap@post.tau.ac.il

Eliran Kachlon
Tel-Aviv University, Tel-Aviv, Israel
elirn.chalon@gmail.com

Arpita Patra
Indian Institute of Science, Bangalore
India
arpita@iisc.ac.in

ABSTRACT

In STOC 1989, Rabin and Ben-Or (RB) established an important milestone in the fields of cryptography and distributed computing by showing that every functionality can be computed with statistical (information-theoretic) security in the presence of an active (aka Byzantine) rushing adversary that controls up to half of the parties. We study the round complexity of general secure multiparty computation and several related tasks in the RB model.

Our main result shows that every functionality can be realized in only four rounds of interaction which is known to be optimal. This completely settles the round complexity of statistical actively-secure optimally-resilient MPC, resolving a long line of research.

Along the way, we construct the first round-optimal statistically-secure verifiable secret sharing protocol (Chor, Goldwasser, Micali, and Awerbuch; STOC 1985), show that every single-input functionality (e.g., multi-verifier zero-knowledge) can be realized in 3 rounds, and prove that the latter bound is optimal. The complexity of all our protocols is exponential in the number of parties, and the question of deriving polynomially-efficient protocols is left for future research.

Our main technical contribution is a construction of a new type of statistically-secure signature scheme whose existence was open even for smaller resiliency thresholds. We also describe a new statistical compiler that lifts up passively-secure protocols to actively-secure protocols in a round-efficient way via the aid of protocols for single-input functionalities. This compiler can be viewed as a statistical variant of the GMW compiler (Goldreich, Micali, Wigderson; STOC, 1987) that originally employed zero-knowledge proofs and public-key encryption.

CCS CONCEPTS

• **Theory of computation → Cryptographic protocols**.

KEYWORDS

Information-Theoretic Cryptography, Cryptographic protocols, Round Complexity, Verifiable Secret Sharing

ACM Reference Format:
Benny Applebaum, Eliran Kachlon, and Arpita Patra. 2023. The Round Complexity of Statistical MPC with Optimal Resiliency. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC '23), June 20–23, 2023, Orlando, FL, USA.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3564246.3585228

STOC '23, June 20–23, 2023, Orlando, FL, USA

ACM ISBN 978-1-4503-9913-5/23/06.
https://doi.org/10.1145/3564246.3585228

1 INTRODUCTION

The round complexity of interactive protocols is one of their most important efficiency measures. Consequently, a huge amount of research has been devoted towards characterizing the round complexity of various distributed tasks (e.g., Byzantine agreement [29, 31, 46], coin flipping [26, 47], zero-knowledge proofs [21, 38], verifiable secret sharing [36, 45] and general secure multiparty computation [15, 17, 35, 53]) under different security models.

In this work, we focus on the round complexity of protocols that achieve *full information-theoretic* security, including *guaranteed output delivery* in the presence of an active (aka Byzantine or malicious), static, computationally-unbounded, rushing adversary. We assume that there are n parties that communicate over *secure point-to-point channels*, and also that they have an access to a *broadcast* channel. Feasibility results in this model were first proved in the classic works of Ben-Or, Goldwasser, and Wigderson [16] and Chaum, Crépeau and Damgård [23]. Specifically, it is known that *perfect security* is achievable if and only if the adversary corrupts less than a third of the parties, i.e., the best-achievable *resiliency threshold* is $t = \lfloor (n-1)/3 \rfloor$. Quite remarkably, Rabin and Ben-Or [51] later showed that, by compromising on *statistical security*, the resiliency can be improved to $t = \lfloor (n-1)/2 \rfloor$. Put differently, a standard "honest majority" is sufficient if one is willing to tolerate a negligible statistical error in privacy and correctness. This is the best that one can hope for since an honest majority is known to be necessary even for weaker notions like *passive* statistical security [25] or active *computational* security with guaranteed output delivery [26].

Our goal in this paper is to determine the round complexity of general multiparty computation (MPC) in the statistical setting (aka the Rabin-Ben-Or setting). Indeed, following recent results that settled the round complexity of MPC for the perfect (aka BGW) setting [2, 4, 5, 7, 33] and for different variants of the computational setting [1, 3, 10, 12, 13, 17, 18, 34, 35, 40, 41, 52], the statistical setting is arguably the last main challenge in this domain. We therefore ask:

> What is the optimal round complexity of general MPC with full statistical security, including guaranteed output delivery, and optimal resiliency?

Indeed, the round complexity of statistically-secure protocols has remained wide open for any resiliency t larger than $n/3$, let alone for the central case of *optimal resiliency* of $t = \lfloor (n-1)/2 \rfloor$. In fact, in this setting, we do not even know what is the exact round

complexity of much more basic primitives, such as statistically-secure *verifiable secret sharing*.

In this work, we settle the round complexity of general MPC, verifiable secret sharing, and several related primitives. Details follow.

1.1 Verifiable Secret Sharing

Verifiable secret sharing (VSS) [24] is arguably the most basic primitive in information-theoretic multiparty computation, and it is known to be necessary for the construction of general MPC protocols both in the perfect setting (see [7]), and in the statistical setting (see [6]).[1] At a high level, a VSS scheme consists of two phases: a sharing phase, which allows a dealer to share a secret s among the parties, and a reconstruction phase, which allows the parties to recover the secret s. For an honest dealer, VSS has the same guarantees as robust secret sharing, that is, the adversary learns no information about s in the sharing phase (privacy), and the secret s will always be reconstructed properly in the reconstruction phase despite the misbehavior of the adversary (correctness). In addition, for a corrupt dealer, we require commitment, which means that at the end of the sharing phase there is some value s' that will always be reconstructed in the reconstruction phase.

While the round complexity of perfect VSS is well-understood (see [32, 36, 44]), this problem is still open in the statistical settings. The best-known scheme [45] achieves 3 rounds of sharing and 2 rounds of reconstruction. It is known that 3 rounds are necessary for the sharing phase [6, 49], but it is unclear whether 2 rounds of reconstruction are necessary. In fact, as shown by [28], one can derive a VSS in which the reconstruction phase consists of a single round by first constructing such a protocol under the assumption that the dealer is honest (aka robust secret sharing) [51], and then using statistical MPC to emulate the honest dealer. This approach suffers, however, from a large number of rounds in the sharing phase, which is inherently sub-optimal since it employs a VSS with multiple rounds of reconstruction as a building block (as part of the MPC protocol). Apart from the MPC-based approach, it is unknown how to achieve a single round of reconstruction even when more than 3 rounds of sharing are being employed [27, 45, 51]. Let us note that single-round reconstruction has a qualitative advantage due to its non-interactive nature (parties can just "speak" once without waiting for others).

Overall, the existence of a statistical VSS that *simultaneously* achieves 3 rounds of sharing and a single round of reconstruction is open. In fact, the question is not fully resolved even if one adds another round of reconstruction (as in [45]) since the known construction [45] lacks some important properties that are typically employed as part of MPC protocols. Most notably, it is not *linearly homomorphic*, i.e., parties cannot locally combine shares of different secrets into a new share of a linear combination of the underlying secrets.

In this work, we provide the first construction of a round-optimal VSS scheme, that requires three rounds of sharing, and only *one round of reconstruction*. Our construction is also linearly-homomorphic (and has other "MPC-friendly" features, see the full version [9] for more details).

Theorem 1.1. *For a security parameter κ, number of parties n, and number of corrupt parties $t < n/2$, there exists a protocol for verifiable secret sharing with three rounds of sharing and one round of reconstruction, that provides statistical security against an active, static, rushing unbounded adversary that corrupts up to t parties, with error $2^{-\kappa}$. The running time of the protocol is* $\mathrm{poly}(\kappa, 2^n)$.

Remark 1.2 (On the exponential dependency on n). *Our VSS protocol, as well as the rest of our protocols, have exponential dependency on the number of parties n, so they are only efficient when $n = O(\log \kappa)$. We emphasize that in the settings of statistical security, even inefficient protocols are meaningful, since the protocols are secure even against a* computationally-unbounded *adversary. We also mention that the question of an efficient VSS scheme with three rounds of sharing is open even if we allow more than one round of reconstruction. Indeed, the construction of [45] also has exponential dependency on the number of parties, even though it allows two rounds of reconstruction.*

1.2 Single Input Functionalities

Before moving to the case of MPC for general functionalities, it is useful to consider the special case of *single input functionalities* [37], whose output depends on the input of a single party, called the dealer. Single input functionalities capture a large class of non-trivial tasks, including secure multicast and multi-verifier zero-knowledge. In the perfect setting, the sharing phase of VSS can be also captured by SIF. However, in the statistical setting, where there is merely an honest majority, it can be shown that SIF *cannot* capture VSS. (See the full version [9] for more details.)

Augmented SIF. We present a stronger notion of SIF, called *augmented SIF*, that captures VSS as well as other related tasks (that will be useful later as building blocks for general MPC). Intuitively, it allows the computation of a single input functionality together with some verification information that will allow every party to publicly open its output, and convince the rest of the parties of its validity. Formally, for a single input functionality $\mathcal{F}$, the corresponding augmented single input functionality is a two-phase functionality $\mathcal{F}'$. The first phase, the computation phase, consists merely of the computation of $\mathcal{F}$. That is, the dealer inputs $\mathbf{x}$ to the functionality $\mathcal{F}'$, and the i-th party receives the value y_i as an output, where $\mathcal{F}(\mathbf{x}) = (y_1, \ldots, y_n)$. In the second phase, the opening phase, every P_i can input a command "open" to $\mathcal{F}'$, and the functionality will return y_i to the rest of the parties. It is not hard to verify that an augmented SIF of any $(t+1)$-out-of-n secret sharing scheme is indeed a VSS scheme.

The round complexity of SIF. Not much is known about the round complexity of SIF and augmented SIF. The three-round lower bound for the sharing phase of VSS [6, 49] implies that the computation phase of an augmented SIF requires at least three rounds. First, we extend this lower bound to hold for standard SIF as well.

[1] Unless stated otherwise, whenever we refer to the *perfect* setting and *statistical* setting, we assume that the resiliency threshold is taken to be optimal, i.e., $t_{\text{perfect}} = \lfloor (n-1)/3 \rfloor$ and $t_{\text{stat}} = \lfloor (n-1)/2 \rfloor$, respectively.

Theorem 1.3 (Lower Bound for SIF). *Let $n \geq 3$ and $t \geq n/3$ be positive integers. Then there exists an n-party single input functionality that cannot be computed in two rounds with resiliency t and error $1/12$.*

The exact round complexity of both, SIF and augmented SIF, is open, and the best upper bound is some large constant [37, 42, 43].[2] We fully resolve this question and provide tight upper bounds. We show that every augmented SIF can be realized in three rounds for the computation phase, and one round for the opening phase. This implies that every SIF can be realized in three rounds (ignoring the opening phase).

Theorem 1.4 (Upper Bound for augmented SIF and SIF). *For a security parameter κ, number of parties n, and number of corrupt parties $t < n/2$, for every single input functionality $\mathcal{F}$, the* augmented single input functionality *$\mathcal{F}'$ can be realized in three rounds for the computation phase, and one round for the opening phase, with statistical security against an active, static, rushing unbounded adversary that corrupts up to t parties, with error $2^{-\kappa}$. The running time of the protocol is $\mathrm{poly}(\kappa, 2^n, s)$, where s is the size of the boolean circuit computing $\mathcal{F}$. Consequently, the single-input functionality $\mathcal{F}$ can be realized in three rounds with similar complexity in the same setting.*

Previously, the best 3-round SIF protocol with active information-theoretic security achieved a threshold of $t \leq \lfloor (n-1)/4 \rfloor$ [5]. We also mention that if one is willing to relax the security to computational then the protocols of [8] provide a 2-round SIF based on cryptographic assumptions (essentially non-interactive commitments).

Application: Multi-verifier zero-knowledge. In multi-verifier zero-knowledge [19] for an NP relation R, there is a single prover and k verifiers, all holding the same statement x. The prover wants to prove that she is holding a secret witness w so that $R(x, w) = 1$, without revealing any information about w. Observe that this task is captured by a single input functionality, that takes (x, w) from the prover, and returns $(x,$ "true") to all the parties if $R(x, w) = 1$, and $(x,$ "false") otherwise. Therefore, when there is an honest majority among the $k + 1$ parties, we can use our SIF protocol to derive the first multi-verifier zero-knowledge proof system that runs in three rounds and achieves statistical security. We highlight the special case of a single prover and two verifiers (i.e., $k = 2$), allowing a single corruption. That is, by adding just a single verifier to the standard zero-knowledge settings, we obtain, for the first time, an efficient zero-knowledge proof with *statistical security* under no cryptographic assumptions. As a bonus, we even provide UC-security [20], which implies *straight-line black-box simulation*, as well as *knowledge extraction*. In comparison, in the standard settings of (single-verifier) zero-knowledge proofs three rounds protocols require non-black box simulation [38].

[2] The obvious approach is to use some MPC-friendly VSS, e.g., the VSS of [45] whose sharing takes 4 rounds and reconstruction takes 2 rounds. Then we can use the protocol of [27] to compute a degree-2 SIF (which is complete for general SIF [37]). Computing one multiplication takes more than 10 rounds in [27], and so the protocol requires more than 14 rounds. By using standard tricks (sharing random multiplication triples [14]) this can probably be improved to 7 rounds (4 rounds for sharing, 1 round for generating random challenges that are needed for the generation of random multiplication triples, and 2 rounds for opening).

1.3 General Multiparty Computation

The round complexity of statistical-MPC for general functionalities is a long-standing open problem. For a long time, it is known that constant-round protocols exist [42, 43], where the exact number of rounds is some large constant. More recently, [6] proved that at least four rounds are required for general statistical MPC. In this work, we close the gap and prove that four rounds are also sufficient.

Theorem 1.5 (General MPC in four rounds). *For a security parameter κ, number of parties n, and number of corrupt parties $t < n/2$, every functionality $\mathcal{F}$ can be realized in four rounds with statistical security against an active, static, rushing unbounded adversary that corrupts up to t parties, with error $2^{-\kappa}$. The running time of the protocol is $\mathrm{poly}(\kappa, 2^n, s, 2^d)$, where s is the size of the boolean circuit computing $\mathcal{F}$, and d is the depth of the circuit.*

As in all known constructions of constant-round information-theoretic MPC, there is an exponential dependency on the depth of the circuit. Getting rid of this dependency, even in weaker adversarial models (e.g., passive adversary and resiliency of $t = 1$), is a famous open problem that goes back to [15]. A potentially more accessible goal is to get-rid of the exponential dependency in the number of parties n (see Remark 1.2). Based on current techniques, $\mathrm{poly}(n)$-time protocols seem to require at least 7 rounds, and so the gap between efficient and inefficient solutions is quite large in this case.

Overall, our protocol is only efficient for $n = O(\log \kappa)$ and for NC^1 functionalities.[3] Nevertheless, even for general functions, for which our construction is inefficient, the result remains meaningful since the protocol resists computationally unbounded adversaries. More generally, ignoring efficiency aspects, one can view our theorems as *computability results* that characterize the minimal computational model (in terms of rounds of interactions) in which universal computation can be carried out with statistical security and optimal resiliency.

2 TECHNICAL OVERVIEW

In this section, we provide a detailed technical overview of our construction. We denote the parties by $P_1, \ldots, P_n$, and we assume that at most $t < n/2$ of the parties are corrupt. We denote the security parameter by κ, and throughout, we think of $\mathbb{F}$ as a finite field of size $\exp(n, \kappa)$, and of $1, \ldots, n$ as n distinct non-zero field elements.

At a high level, our construction consists of two main parts: the construction of a round-optimal VSS scheme, and a transformation from VSS to general MPC. In Section 2.1 we provide a detailed overview of our VSS scheme, that constitutes our main technical contribution. In Section 2.2 we provide a short overview of the transformation from VSS to general MPC via augmented SIF.

2.1 Verifiable Secret Sharing

Background. We begin with some background on the qualitative difference between VSS in the perfect setting and VSS in the statistical setting. It will be instructive to start with the simpler task

[3] As in similar cases, this can be pushed up to log-space functionalities since they securely reduce to NC^1 functionalities via non-interactive reductions [43].

of *robust secret sharing* where an *honest* dealer $\mathcal{D}$ shares a secret s among n players. We require t-privacy, i.e., t shares reveal no information about s, and also perfect t-robustness, which means that if all the parties send their shares to a receiver $\mathcal{R}$, then $\mathcal{R}$ can recover s even if t shares are maliciously chosen and might depend on the honest shares. When $n = 3t + 1$, it is known that Shamir's secret sharing satisfies those requirements since Reed-Solomon codes allow to recover the secret from t errors. On the other hand, when $n = 2t + 1$, it is not hard to see that this task is impossible. Indeed, if $(s_1, \ldots, s_n)$ are shares of 0, and $(s'_1, \ldots, s'_n)$ are shares of 1, then the Hamming distance between the two vectors has to be at least $2t + 1 = n$, or otherwise t-robustness is violated. But this means that we can distinguish a secret sharing of 0 from a secret sharing of 1 based on a single share, so t-privacy is violated. In fact, this argument shows that perfect robustness is possible only when $n \geq 3t + 1$. We will see that this qualitative difference propagates up to the more challenging task of VSS.

In the perfect setting, when $n \geq 3t + 1$, the canonical approach [7, 11, 16, 32, 36, 44] is to design an MPC protocol for the single input functionality that takes an input s and randomness r from the dealer, generates the shares $s_1, \ldots, s_n$ according to Shamir's scheme, and delivers s_i to P_i. Privacy follows from the privacy of the secret sharing scheme, while commitment (and correctness) follows from the perfect robustness property: Even if the dealer is dishonest, and therefore knows all the shares of the honest parties and has full control of the shares of t corrupt parties, perfect robustness guarantees that there *exists* exactly one valid opening in the reconstruction phase. Indeed, this approach leads to VSS protocols with an optimal round complexity [7, 32, 36, 44] (3 rounds of sharing and a single round of reconstruction) and so the problem in the perfect setting is well understood.

The situation in the statistical setting is more subtle. As already observed, we cannot hope for perfect robustness whenever $t \geq n/3$, and so the commitment property cannot be based on the nonexistence of ambiguous openings. Instead, one has to argue that it is infeasible to find such ambiguous openings given the adversary's view. That is, we have to inject some *private* randomness into the shares of the honest parties.[4] Indeed, following [51], the canonical approach here is to augment each share s_i with a private "proof-of-validity", that allows P_i to convince the rest of the parties in the validity of its share s_i. If P_i tries to open an invalid share $s'_i \neq s_i$, then with high probability P_i will fail to generate a proof-of-validity for s'_i, and the rest of the parties will set the share of P_i to an *erasure*. Since t erasures can be handled when $n \geq 2t + 1$, such proofs-of-validity suffices. Of course, some of the randomness used to generate the proofs-of-validity has to come from the honest parties and should remain hidden from the adversary. Furthermore, the use of interactive reconstruction (which allows for interactive verification of validity) seems to be of significant help. (See, e.g., the discussions in [22, 28, 30] in the context of robust secret sharing.) In contrast, in the perfect setting, it can be shown that interaction is useless in the reconstruction phase [37].)

[4] Consequently, in the honest majority statistical setting, VSS cannot be realized by a single input functionality. This is true even if multiple rounds of reconstruction are allowed (see the full version [9] for full details).

Interactive signatures. The main tool for constructing the proofs-of-validity is some form of *information-theoretic interactive signatures* (aka information-checking protocols [51]). This is essentially a weak version of VSS in which the opening is conducted by some designated party $\mathcal{I}$. Following the definition of [48, 50], an interactive signature is a protocol involving n parties, where two of them are distinguished: the dealer $\mathcal{D}$ and the intermediary $\mathcal{I}$. (Say that P_1 is $\mathcal{D}$ and that P_2 is $\mathcal{I}$.) The protocol consists of 3 phases as follows:

(1) *Distribution phase*: $\mathcal{D}$ sends to $\mathcal{I}$ a secret s together with some authentication information, and some verification information to the rest of the parties.
(2) *Verification phase*: The parties verify that the information that $\mathcal{D}$ sent is "valid" and "consistent" with the secret s that $\mathcal{I}$ holds, and terminate the phase with a public decision on success or failure that is taken based on public information (i.e., broadcasts).
(3) *Selective opening phase*: Assuming that the verification phase succeeds, $\mathcal{I}$ can publicly open the value s to all the parties. The parties decide whether to accept or reject this opening. Crucially, the decision of whether to open the value is in the hands of $\mathcal{I}$ and may depend on external reasons. (Hence the term "selective".)

Correctness and *privacy* are defined in a natural way: When $\mathcal{D}$ and $\mathcal{I}$ are honest, the verification succeeds, the opening of $\mathcal{I}$ is accepted by all honest parties (correctness), and the adversary learns no information about s in the distribution phase and verification phase (privacy). The commitment property from the VSS is replaced with the following three fine-grained requirements that are all conditioned on the success of the verification phase: (a) *unforgeability*: If $\mathcal{D}$ is honest and $\mathcal{I}$ is corrupt, the honest parties will reject an opening of $s' \neq s$ by $\mathcal{I}$; (b) *nonrepudiation*: If $\mathcal{D}$ is corrupt and $\mathcal{I}$ is honest, then the honest parties will accept the opening of s by $\mathcal{I}$; and (c) *agreement*: All honest parties agree on whether to accept or reject the opening of $\mathcal{I}$, even if both $\mathcal{I}$ and $\mathcal{D}$ are corrupt. If verification fails, unforgeability, nonrepudiation, and agreement are vacuously satisfied.

VSS from signatures. The work of [45] implicitly shows a VSS scheme with three rounds of sharing and one round of reconstruction (which is also MPC friendly) can be based on any signature scheme with one round of distribution, two rounds of verification, and a single round of selective opening that can be executed in *parallel* to the second round of the verification phase. We call such a signature scheme a $(1, 2, 1)$-signature. Unfortunately, all known constructions of interactive signatures [27, 45, 50, 51], regardless of the round-complexity of the distribution phase and the verification phase, require an interactive (two-round) sub-protocol for selective opening. To bypass this barrier, let us first take a fresh look at existing constructions [48, 50] which originally rely on polynomials, and abstract them by using general linear secret-sharing schemes.

Abstraction of previous constructions. Consider a linear secret-sharing scheme over $\mathbb{F}$ for N secret-sharing players $Q_1, \ldots, Q_N$. Linearity means that in order to share a secret $s \in \mathbb{F}$, we sample a random vector $\boldsymbol{\rho}_s$ whose first entry is s, and set the i-th share to $L_i(\boldsymbol{\rho}_s)$ where L_i is some public non-degenerate linear operator that

is associated with the i-th player Q_i. The scheme is parameterized by a threshold $T > n$ and we assume that any coalition of size n learns nothing about the secret and coalitions of size T can recover the secret and *the randomness vector* $\boldsymbol{\rho}_s$. The latter property implies that the mapping $L : \boldsymbol{\rho}_s \mapsto (L_i(\boldsymbol{\rho}_s))_{i\in[N]}$ forms a linear code of distance $\Delta = N - T + 1$. Jumping ahead, we will have exponentially many "virtual" secret-sharing players, i.e., $N = \exp(n, \kappa)$, but the threshold T is polynomial in n and κ. We will employ only n (randomly chosen) sharing players, so the overall complexity can be, in principle, $\text{poly}(n, \kappa)$.[5] An interactive signature (with 2 rounds of selective opening) can be constructed as follows.

(1) *Single-round Distribution phase*: Given a secret $s \in \mathbb{F}$, the dealer samples a random mask $r \in \mathbb{F}$, and random vectors $\boldsymbol{\rho}_s$ and $\boldsymbol{\rho}_r$ whose first entry is s and r, respectively. All these random values are sent to $\mathcal{I}$. In addition, for every P_i, the dealer picks a random index $\alpha_i \in [N]$ that represents some (virtual) secret-sharing player, and sends to party P_i the index α_i together with the corresponding shares $s_i := L_{\alpha_i}(\boldsymbol{\rho}_s)$ and $r_i := L_{\alpha_i}(\boldsymbol{\rho}_r)$, which will be used as "authenticators". This step reveals no information about s and r since the adversary can see at most n shares.

(2) *2-round Verification phase*: $\mathcal{I}$ broadcasts a random linear combination of the randomizers $\boldsymbol{\rho}_s$ and $\boldsymbol{\rho}_r$, i.e., $\mathcal{I}$ samples a non-zero scalar $c \in \mathbb{F}$ and broadcasts $(c, \quad \boldsymbol{\rho} := \boldsymbol{\rho}_s + c \cdot \boldsymbol{\rho}_r)$. This equation is being checked by the dealer who broadcasts a public complaint if $\boldsymbol{\rho}_s + c \cdot \boldsymbol{\rho}_r \neq \boldsymbol{\rho}$. If such a complaint is issued verification fails, otherwise verification succeeds. These messages do not violate privacy since $\boldsymbol{\rho}_r$ masks the value of $\boldsymbol{\rho}_s$.

(3) *2-round Selective opening phase*: In order to open the secret $\mathcal{I}$ broadcasts $\boldsymbol{\rho}_s$. We say that P_i *votes* for the opening if either (a) $L_{\alpha_i}(\boldsymbol{\rho}_s) = s_i$ or (b) $L_{\alpha_i}(\boldsymbol{\rho}) \neq s_i + c \cdot r_i$ and $\mathcal{D}$ did not broadcast a complaint.[6] In the second round, every party broadcasts its vote, and the parties accept if a majority of the parties vote for the opening. (If the verification phase failed, then the parties simply ignore the selective opening phase.)

Analysis (sketch). Correctness, privacy, and agreement are straightforward. For unforgeability, we assume that $\mathcal{D}$ is honest, $\mathcal{I}$ is corrupt, verification passes and $\mathcal{I}$ opens $\boldsymbol{\rho}'_s \neq \boldsymbol{\rho}_s$. Since the code L has distance Δ, the probability that $L_{\alpha_i}(\boldsymbol{\rho}_s) \neq L_{\alpha_i}(\boldsymbol{\rho}'_s)$, for a random $\alpha_i \in [N]$, is at least $\Delta/N > 1 - T/N$, and so every honest party is likely to vote against the opening. Here we crucially relied on the fact that the adversary does not know α_i. For nonrepudiation, assume that $\mathcal{D}$ is corrupt, $\mathcal{I}$ is honest, verification passes but $\mathcal{I}$ is rejected, i.e., at least one honest party P_i voted against the opening. Thus, $L_{\alpha_i}(\boldsymbol{\rho}_s) \neq s_i$ but $L_{\alpha_i}(\boldsymbol{\rho}) = s_i + c \cdot r_i$. By linearity, this happens iff $c \cdot (r_i - L_{\alpha_i}(\boldsymbol{\rho}_r)) = (L_{\alpha_i}(\boldsymbol{\rho}_s) - s_i)$, and since the RHS is non-zero, this happens with a probability of at most $1/(|\mathbb{F}| - 1)$ over the choice of the random non-zero scalar c.

[5] To achieve such a complexity, the secret sharing should be strongly explicit, i.e., the ith share should be computable in time $\text{poly}(T, \log(N)) = \text{poly}(n, \kappa)$. For example, one can use Shamir's $(n+1)$-out-of-N secret sharing scheme with a field of size $|\mathbb{F}| = N + 1$ and $T = n + 1$.

[6] In the latter case, P_i thinks that $\mathcal{D}$ is corrupt and so he shouldn't worry about unforgeability and there is no harm in accepting the opening.

Reducing a round? We can try to reduce one round of the selective opening by letting each party decide locally based on his own vote. However, in this case, an adversary that corrupts both $\mathcal{D}$ and $\mathcal{I}$ can violate the agreement property by generating vectors $\boldsymbol{\rho}_s, \boldsymbol{\rho}, (\alpha_i, s_i, r_i)$ and (α_j, s_j, r_j), so that an honest P_i accepts the opening while an honest P_j rejects the opening. One could also try to let every P_i broadcast the authentication values (α_i, s_i, r_i) in the first round of the selective opening phase, so the rest of the parties will be able to compute the vote of P_i based on $\boldsymbol{\rho}_s$ and (α_i, s_i, r_i). However, given this information, a corrupt rushing $\mathcal{I}$ can efficiently find an invalid opening that will be accepted by the honest parties, violating the unforgeability requirement. This problem can be fixed by increasing the distance of the code and setting the privacy threshold below n. But in this case, the authenticators (α_i, s_i, r_i) prematurely reveal the secret before we even know whether the intermediate wishes to open the secret, thus violating privacy. Overall, the challenge is to reveal enough information that allows the parties to reach an agreement (in case the secret is opened), while keeping enough uncertainty about the secret and its "authenticators" (for privacy and unforgeability).[7]

At a high level, we solve the problem by letting each party spread some partial, randomized, pieces of information about his local authenticators. In particular, each party P_i will receive *many* secret shares from the dealer and will spread random linear combinations of these shares to the other parties. Crucially, P_i will use a local private source of randomness. (This deviates from all previous approaches in which only $\mathcal{D}$ and $\mathcal{I}$ were randomized). The actual implementation of this approach requires some care. We will start with a simplified model that includes additional (virtual) verifiers (Section 2.1.1), and then explain how to emulate the verifiers in a round-preserving way (Section 2.1.2), in order to obtain a $(1, 2, 1)$-signature in the standard model.

2.1.1 Step I: Signature Scheme with Virtual Verifiers.

A simplified model. In previous constructions, every P_i had a dual role: P_i acted both as a verifier, that had to vote for/against the opening of $\mathcal{I}$, and also as a receiver, that had to accept/reject the opening of $\mathcal{I}$. We consider a *simplified model* where this role is divided between two entities: a verifier $\mathcal{V}_i$ and a receiver P_i. Formally, the model consists of m verifiers $\mathcal{V}_1, \ldots, \mathcal{V}_m$, and n receivers $P_1, \ldots, P_n$ and we assume that the dealer $\mathcal{D}$ is P_1 and the intermediary $\mathcal{I}$ is P_2. The adversary can corrupt any number of the receivers, and can *weakly corrupt* any subset of the verifiers with one limitation: When $\mathcal{D}$ is honest and $\mathcal{I}$ is corrupt there must be at least one honest verifier. The notion of weak corruption is non-standard: A weakly corrupted verifier passes all her incoming messages to the adversary but keeps her internal state (i.e., her random tape) and the messages that she sends to the other honest parties hidden. In addition, the adversary is allowed to abort a weakly corrupted verifier at any time. If a verifier is not aborted, it plays its role honestly.

[7] In contrast, in the reconstruction phase in VSS we do not care about the privacy of the secret, since the opening is not selective and all the parties know that the secret should be revealed. In this sense, signatures (with a single round of opening) are more challenging than VSS. Indeed, to the best of our knowledge, the question is open even when the resiliency threshold t is smaller than $n/3$ and perfect-VSS is available.

Hadamard-based secret sharing. Recall that we employ a linear secret-sharing scheme over $\mathbb{F}$ that is defined by N distinct linear mappings $\{L_i\}_{i\in[N]}$, one for each virtual party. We will need the (highly non-standard) property that this set of functions forms a linear space $\mathcal{L}$. For this, we will take $\mathcal{L}$ to be the space of *all* linear functions from $\mathbb{F}^v$ to $\mathbb{F}$ and think of each function as a vector in $\mathbb{F}^v$ (so $N = |\mathbb{F}|^v$). This is not a valid threshold secret sharing since some small coalitions (that span the vector $\mathbf{e}_1 = (1, 0, \ldots, 0)$) can recover the secret, and some huge coalitions (that do not span $\mathbf{e}_1$) may not be able to recover the secret. However, for a randomly chosen coalition of size $\gg v$ (resp., $\ll v$) correctness (resp., privacy) holds with high probability. These relaxed properties suffice (since privacy and correctness will only be needed when the dealer is honest and in this case the virtual parties will be selected at random). From a coding perspective, this secret sharing corresponds to the Hadamard code over a large field. Let u be polynomially larger than $\kappa \cdot m \cdot n$ and let v be polynomially larger than um. We modify the previous construction as follows:

(1) *Single-round distribution phase:* As before, the dealer samples the randomizers $\boldsymbol{\rho}_s$ and $\boldsymbol{\rho}_r$ and sends them to $\mathcal{I}$. In addition, $\mathcal{D}$ allocates to each verifier u random virtual secret-sharing parties by sampling a random $u \times v$ matrix A_i, and sends to $\mathcal{V}_i$ the "names" of the virtual parties and their shares, $(A_i, \quad \mathbf{s}_i := A_i \cdot \boldsymbol{\rho}_s, \quad \mathbf{r}_i := A_i \cdot \boldsymbol{\rho}_r)$. Since $v \gg um$, with a very high probability the row-span $(A_i)_{i\in[m]}$ does not include the unit vector $\mathbf{e}_1 = (1, 0, \ldots, 0)$, which means that all the messages that the verifiers receive from $\mathcal{D}$ reveal no information about s and r.

(2) *2-round verification phase:* As in the previous protocol, the intermediate publishes a random non-zero scalar c and a linear combination of the secret sharing randomizers $\boldsymbol{\rho} := \boldsymbol{\rho}_s + c \cdot \boldsymbol{\rho}_r$, and the dealer $\mathcal{D}$ announces whether verification succeeds by verifying the above equality. In addition, in the second round, every verifier $\mathcal{V}_i$ does the following: (a) broadcasts a public complaint if its local authenticators are inconsistent with the published information, i.e., if $A_i \cdot \boldsymbol{\rho} \neq \mathbf{s}_i + c \cdot \mathbf{r}_i$; and (b) privately sends to each receiver P_j, $j \in [n]$, a random linear combination of his s-shares $(\mathbf{t}_{i,j}, \quad \mathbf{a}_{i,j} := \mathbf{t}_{i,j} \cdot A_i, \quad s_{i,j} := \mathbf{t}_{i,j} \cdot \mathbf{s}_i)$, where $\mathbf{t}_{i,j} \leftarrow \mathbb{F}^u$ is a random row vector.

(3) *Single-round selective opening phase*: To open the secret s, the intermediate $\mathcal{I}$ broadcasts the vector $\boldsymbol{\rho}_s$ to all the parties. After this, each receiver P_i locally computes a vote for each verifier $\mathcal{V}_j$ and rejects the opening if at least one verifier votes against the opening. The receiver P_i thinks that the verifier $\mathcal{V}_j$ votes against the opening if the following conditions hold: (1) $\mathcal{V}_j$ did not broadcast a complaint[8], (2) $\mathcal{V}_j$ did not abort, and (3) there is an inconsistency $\mathbf{a}_{i,j} \cdot \boldsymbol{\rho}_s \neq s_{i,j}$. Observe that this phase can be executed in parallel to the second round of the verification phase, so that if the verification phase failed the opening is simply ignored.

Analysis (sketch). It is not hard to see that correctness and privacy hold even if none of the verifiers are honest. For unforgeability, assume that $\mathcal{D}$ is honest, $\mathcal{I}$ is corrupt, some verifier, say $\mathcal{V}_1$ is honest, and the verification phase succeeds. By following the previous argument, unforgeability boils down to showing that the vector $\mathbf{a}_{1,j}$ that an honest receiver P_j gets from $\mathcal{V}_1$ is (almost) uniformly distributed. Moreover, this should hold even when conditioning on the adversary's view that consists of all the vectors $\mathbf{a}_{1,\ell}$ that $\mathcal{V}_1$ sent to the corrupted receivers. To see this, observe that the vectors $\mathbf{a} = (\mathbf{a}_{1,1}, \ldots, \mathbf{a}_{1,n})$ were generated by taking n random linear combinations $T = (\mathbf{t}_{1,1}, \ldots, \mathbf{t}_{1,n})$ of the rows of a random matrix A_1. Since T is likely to be linearly independent (as each $\mathbf{t}_{1,j}$ is of dimension $u \gg n$) and since A_1 is uniform, the outcome $\mathbf{a}$ is also uniform.

For nonrepudiation, assume that $\mathcal{D}$ is corrupt and $\mathcal{I}$ is honest, and let $\mathcal{V}_i$ be any verifier that did not abort. If $A_i \cdot \boldsymbol{\rho}_s \neq \mathbf{s}_i$ then even weakly-corrupt $\mathcal{V}_i$ is likely to broadcast a public complaint (the argument is similar to the one used in the previous scheme); Otherwise, $A_i \cdot \boldsymbol{\rho}_s = \mathbf{s}_i$ and all the local authenticators that were sent by $\mathcal{V}_i$ will be consistent. In any case, no honest party rejects due to $\mathcal{V}_i$.

Finally, for agreement, we show that even if $\mathcal{D}$ and $\mathcal{I}$ are corrupt, if the verification phase succeeds, then all the honest receivers are likely to see, for every (possibly weakly-corrupt) verifier $\mathcal{V}_i$, the *same* vote. This is trivially true if $\mathcal{V}_i$ aborts or broadcast a complaint. If this is not the case, then, except with probability of $1/|\mathbb{F}| = \mathrm{negl}(n, \kappa)$ over the choice of the linear combination $\mathbf{t}_{i,j}$, the local equation tested by an honest receiver P_j, which can be written as $\mathbf{t}_{i,j} \cdot (A_i \cdot \boldsymbol{\rho}_s) = \mathbf{t}_{i,j} \cdot (\mathbf{s}_i)$ holds if and only if $\mathcal{V}_i$'s equation $A_i \cdot \boldsymbol{\rho}_s = \mathbf{s}_i$ holds.

Multiple-authenticators variant. It will be useful to consider a variant of the protocol in which every $\mathcal{V}_i$ sends multiple authenticators $(\mathbf{t}^k_{i,j}, \quad \mathbf{a}^k_{i,j} := \mathbf{t}^k_{i,j} \cdot A_i, \quad s^k_{i,j} := \mathbf{t}^k_{i,j} \cdot \mathbf{s}_i)_{k\in[\ell]}$ to every receiver P_j. Accordingly, in the opening phase, P_j will treat any inequality of the form $\mathbf{a}^k_{i,j} \cdot \boldsymbol{\rho}_s \neq s^k_{i,j}$ for some $k \in [\ell]$, as an inconsistency, and will reject accordingly (unless $\mathcal{V}_i$ aborted or issued a public complaint). We think of the random tape of $\mathcal{V}_i$ as composed of ℓ blocks where the kth block consists of all the vectors $(\mathbf{t}^k_{i,j})_{j\in[n]}$. By slightly modifying the parameters u and v, we can securely support this extension even if the adversary partially controls the choice of the linear combinations $\mathbf{t}^k_{i,j}$ of non-honest verifiers $\mathcal{V}_i$. Specifically, if either $\mathcal{D}$ or $\mathcal{I}$ is corrupt, the adversary will be allowed to choose, for every non-honest $\mathcal{V}_i$, all the random tape except for one block that is sampled uniformly at random and remains unknown to the adversary. (If $\mathcal{D}$ and $\mathcal{I}$ are honest then we allow the adversary to pick all the vectors $\mathbf{t}^k_{i,j}$ that are generated by $\mathcal{V}_i$.)

2.1.2 Step II: Emulating the Verifiers. We return to the standard model with n parties $P_1, \ldots, P_n$ where at most $t < n/2$ of them are corrupt. We consider the multiple-authenticators variant of the protocol in the simplified model as the *outer protocol*, and we use a virtualization technique to emulate the verifiers in a round-preserving way. For ease of presentation, we assume that the parties have an access to an idealized single-round signature scheme which is also *linearly homomorphic*. That is, if a signer A *signs* to B over secrets $(s_1, \ldots, s_q)$ then B can pick any vector of coefficients $\boldsymbol{\beta}_j = (\boldsymbol{\beta}_j[1], \ldots, \boldsymbol{\beta}_j[q])$ and *privately open* the vector of coefficients and linear combination $(\boldsymbol{\beta}, \quad \sum_{i\in[q]} \boldsymbol{\beta}_j[i] \cdot s_i)$ to some party P_j while

[8] Again, in case of a complaint the verifier (who always operates honestly) claims that the dealer is cheating, and so it's safe to accept the opening without worrying about forgery.

certifying that these values were "signed" by A. The opening is *designated* to P_j, and so we use the terms *A signs to B* and *B opens to P_j*. While it may seem paradoxical to make this assumption at this point, we will later see that it can be replaced with a weak form of interactive signatures, and thus can be easily realized.

The emulation. We identify the verifiers with all subsets of t parties that do not include $\mathcal{D}$ and $\mathcal{I}$, so $m = \binom{n-2}{t}$.[9] In a nutshell, messages that will be sent to the virtual verifier $\mathcal{V}_i$ will be delivered to all the parties in the corresponding committee, and whenever $\mathcal{V}_i$ sends a message, we let each party in the committee send the message as well where the message will be computed with respect to his own independent randomness. We think of $\mathcal{V}_i$ as weakly corrupt if it contains a corrupt party P_j. If all the parties in $\mathcal{V}_i$ are honest, the virtual party will be viewed as an honest party.

In more detail, we think of the distribution phase and verification phase as a three-round protocol. In the first round of the outer protocol, i.e., in the distribution phase, $\mathcal{D}$ sends every $\mathcal{V}_i$ a vector $(A_i, \mathbf{s}_i, \mathbf{r}_i)$. We emulate this step by letting $\mathcal{D}$ pass these values to every P_j in $\mathcal{V}_i$ together with linear private-opening (LPO) signatures. To make sure that $\mathcal{D}$ sent the same vector to all parties in $\mathcal{V}_i$, we let the parties perform a public secure pairwise comparison of those values in the following way. For every $\mathcal{V}_i$ and every P_j and P_k in $\mathcal{V}_i$, we let P_j sign a random pad $\mathbf{r}_{i,j,k}$ to P_k in the first round using the LPO signature, and both parties broadcast $(A_i, \mathbf{s}_i, \mathbf{r}_i) + \mathbf{r}_{i,j,k}$ in the second round. Any inconsistency in the broadcasts implies that the comparison failed, in which case we think of $\mathcal{V}_i$ as an aborting verifier.

In the third round of the outer protocol, i.e., in the second round of the verification phase, every $\mathcal{V}_i$ verifies that $A_i \cdot \boldsymbol{\rho} = \mathbf{s}_i + c \cdot \mathbf{r}_i$, and also generates ℓ authenticators and sends them to the receivers. We emulate this step by letting every P_j in $\mathcal{V}_i$, verify that $A_i \cdot \boldsymbol{\rho} = \mathbf{s}_i + c \cdot \mathbf{r}_i$, using the vector $(A_i, \mathbf{s}_i, \mathbf{r}_i)$ that P_j received from $\mathcal{D}$, and broadcast a public complaint if equality does not hold. If any P_j in $\mathcal{V}_i$ broadcasts a complaint, we think of $\mathcal{V}_i$ as a complaining verifier. We set the number of authenticators generated by every verifier $\mathcal{V}_i$ to be $\ell = t$, and we let every P_k in $\mathcal{V}_i$ generate a random vector $\mathbf{t}^k_{i,j}$ for every P_j, and *privately open* to P_j the values $(\mathbf{t}^k_{i,j}, \quad \mathbf{a}^k_{i,j} := \mathbf{t}^k_{i,j} \cdot A_i, \quad s^k_{i,j} := \mathbf{t}^k_{i,j} \cdot \mathbf{s}_i)$ which are linear combinations of the values on which $\mathcal{D}$ signed to P_k. That is, every party in $\mathcal{V}_i$ generates a single authenticator for P_j. (If P_j rejects the opening of P_k, then P_j simply ignores the authenticator of P_k.)

Analysis. For honest $\mathcal{D}$ and $\mathcal{I}$, we allowed all the verifiers to be non-honest in the outer protocol. Observe that every verifier $\mathcal{V}_i$ contains a corrupt party, that can broadcast a false complaint. However, since a complaining $\mathcal{V}_i$ is equivalent to an aborting $\mathcal{V}_i$ in the outer protocol, this behavior is allowed. In addition, when $\mathcal{D}$ is honest, the unforgeability of the LPO signature implies that for every non-aborting $\mathcal{V}_i$, all authenticators generated by the parties in $\mathcal{V}_i$ are of the correct form $(\mathbf{t}^k_{i,j}, \mathbf{t}^k_{i,j} \cdot A_i, \mathbf{t}^k_{i,j} \cdot \mathbf{s}_i)$. If, in addition, $\mathcal{I}$ is corrupt, then there exists a verifier that contains only honest parties that acts exactly like an honest verifier in the outer protocol, and the adversary has no information about the internal state of this verifier. Moreover, every verifier $\mathcal{V}_i$ contains at least one honest party P_k, for which the authenticators $(\mathbf{t}^k_{i,j})_{j\in[n]}$ are uniformly distributed, and the adversary has no information about the vectors corresponding to the honest parties.

When $\mathcal{D}$ is corrupt, every $\mathcal{V}_i$ contains at least one honest party, and if $\mathcal{V}_i$ did not abort then the honest parties in $\mathcal{V}_i$ agree on the values $(A_i, \mathbf{s}_i, \mathbf{r}_i)$. This means that for every $\mathcal{V}_i$ at least one authenticator is honestly generated. However, the authenticators that the corrupt parties generate are not necessarily consistent with the values $(A_i, \mathbf{s}_i, \mathbf{r}_i)$ that the honest parties hold. To solve this problem, we observe that each pair of parties P_ℓ and P_k in a non-aborting $\mathcal{V}_i$ already publicly agreed (via broadcast) on the masked values $\mathbf{b}_{i,\ell,k} = (A_i, \mathbf{s}_i, \mathbf{r}_i) + \mathbf{r}_{i,\ell,k}$. Also P_ℓ signed the random pad $\mathbf{r}_{i,\ell,k}$ to P_k, and since $\mathbf{b}_{i,\ell,k}$ is public, this signature is effectively a signature on the "plaintext" $(A_i, \mathbf{s}_i, \mathbf{r}_i)$. In particular, P_k can prove to any party P_j that her authenticator, $(\mathbf{t}^k_{i,j}, \quad \mathbf{a}^k_{i,j} := \mathbf{t}^k_{i,j} \cdot A_i, \quad s^k_{i,j} := \mathbf{t}^k_{i,j} \cdot \mathbf{s}_i)$, is consistent with P_ℓ, by opening to P_j the linear combinations of the random pad $\mathbf{r}_{i,\ell,k}$ that correspond to $\mathbf{t}^k_{i,j}$. (See the full version [9] for details.)

Realizing the linear private-opening signatures. So far we assumed that we have an idealized version of the linear private-opening signatures. To replace these signatures we construct information-theoretic linear private-opening signatures. Since the openings are private, we do not require agreement and show that such a scheme can be realized with a single round of distribution, two rounds of verification, and a single round of opening that can be executed in parallel to the second round of verification. Our construction follows the blueprints presented in previous works [48, 50]. (Full details appear in the full version of this paper [9].) Despite their interactive nature, our signatures can be employed in the above protocol without increasing the round complexity. The distribution phase is executed in the first round, and the verification phase is executed in the second and third round. A failures of an LPO verification, which is a public event, is translated to an "abort" of the corresponding virtual verifier. The final construction of the $(1, 2, 1)$-signature scheme satisfies several additional properties (e.g., linearity and refined versions of openings) that are needed later for the other constructions. See the full version [9]for details.

2.2 From VSS to General MPC

At a high level, our (long and winding) road to round-optimal general MPC has few additional steps. First, we note that our VSS scheme satisfies some useful properties for the construction of round-optimal general MPC protocol. We then use those properties to construct (standard) single-input functionalities, and show how to enhance SIF to augmented SIF. Finally, we use augmented single input functionalities for the construction of round-optimal general MPC. We continue with a short explanation about each step.

2.5-rounds VSS.. In order to obtain round-optimal protocols, we need to perform operations on the shares *before* the execution of VSS terminated. This idea can be traced back to [5], and was used in several papers on round-optimal MPC [7, 8]. We call the shares that the parties received in the first round of the VSS protocol *tentative shares*, and we observe that in some special cases we can perform linear operations over those shares. In the first special case, a single dealer shared many secrets $s_1, \ldots, s_m$, and the parties

[9] This is the point where complexity becomes exponential in n.

securely compute a linear function $\sum_{i\in[m]} \alpha_i \cdot s_i$ of the secrets already in the third round of VSS. In the second special case there are two dealers $\mathcal{D}_1$ and $\mathcal{D}_2$ that share the secrets s_1 and s_2, respectively, and the parties securely compute the value $s_1 - s_2$ already in the third round. See the full version [9] for more details.

Single input functionalities. Recently, [8] implicitly showed a round-preserving transformation from a VSS scheme that allows performing linear operations over the tentative shares into a protocol for single input functionalities. We follow this blueprint and show that it can be adopted to the statistical setting as well. Roughly, the transformation has two steps: (1) Based on VSS, we construct a three-round protocol for *triple secret sharing* (TSS) that allows a dealer $\mathcal{D}$ to share a triple (a, b, c) among the parties via VSS, and also prove in zero-knowledge that the triple satisfies $c = ab$; and (2) We use the TSS protocol in order to construct a three-round SIF protocol for a degree-2 functionality by letting the dealer shares its inputs and all the degree-2 monomials (via TSS) and then let the parties compute linear operations over the tentative shares. Since general SIF non-interactively reduces to degree-2 SIF [37], we get a 3-round SIF protocol.

While this approach is sufficient for the construction of SIF, it is insufficient for the construction of an augmented SIF, since a party P_i cannot convince the other parties of the validity of its outputs. In order to obtain an augmented SIF, we first present a new primitive, called *verifiable sharing and transferring* (VST), that allows a dealer $\mathcal{D}$ to share a secret s among the parties via VSS, while delegating the ability to perform the verifiable opening of s to a designated receiver R (who also gets to learn the secret). The protocol follows similar ideas to VSS. Now given a SIF functionality f, we realize an augmented SIF as follows. Instead of delivering the ith output, $f_i(\mathbf{x})$, privately to P_i, we use SIF to send to all the parties a masked version of the output $f_i(\mathbf{x}) + r_i$, and share the mask r_i via VST while delegating the opening to P_i as the receiver. As a result, P_i learns the output $f_i(\mathbf{x})$ and gets the ability to verifiably open r_i, and let all the parties learn $f_i(\mathbf{x})$.[10] For more details, see the full version [9].

From Single Input Functionality to General Multiparty Computation. To construct a 4-round MPC protocol for general functionalities, we begin with 2-round perfectly secure protocol Π^{sm} against passive adversaries (e.g., [4]), and use a 3-round augmented SIF to force an honest behavior while increasing the total round complexity by only one round. This can be viewed as a new round-efficient statistical realization of the GMW paradigm [39]. Since the underlying protocol Π^{sm} uses private channels, we face a consistency problem: How should Alice convince Bob and Charlie that she behaves well when they have different views on her behavior? To solve this problem GMW eliminate all private communication and pass it, encrypted under public-key encryption, over a broadcast channel, thus providing a common "point of reference" for all the parties. This public-key assumption was carried to round-efficient realizations of the GMW compiler [1, 40], and was recently relaxed to a symmetric assumption (the existence of commitments) in [10]. We get rid of computational assumptions and present a statistical variant of this round-efficient compiler. For this, we exploit the full power of the augmented SIF protocol and some of its special properties such as the ability to compute the difference between the outputs of two single input functionalities with different dealers. For more details, see the full version [9].

[10] In order to construct augmented single input functionalities, we need to execute multiple instances of VSS, TSS and VST, and perform linear operations over the shares. All these calls should be correlated, i.e., for every pair of parties (P_i, P_j), all instances of VSS, TSS, and VST should use the same underlying instance of linear (1,2,1)-signature with P_i in the role of $\mathcal{D}$ and P_j in the role of $\mathcal{I}$. In order to handle this correlation, it will be convenient to capture the execution of *all* VSS, TSS and VST instances by a *single* ideal functionality $\mathcal{F}_{\text{sh-comp}}$, that will formalize both the task of sharing values by the parties and of computing linear operations over the shares.

ACKNOWLEDGMENTS

B. Applebaum and E. Kachlon are supported by the Israel Science Foundation grant no. 2805/21. A. Patra is supported by DST National Mission on Interdisciplinary Cyber-Physical Systems (NM-ICPS) 2020-2025, SONY Faculty Innovation Award and JPM Faculty Research Award.

REFERENCES

[1] Prabhanjan Ananth, Arka Rai Choudhuri, Aarushi Goel, and Abhishek Jain. 2018. Round-Optimal Secure Multiparty Computation with Honest Majority. In *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part II.* 395–424. https://doi.org/10.1007/978-3-319-96881-0_14

[2] Prabhanjan Ananth, Arka Rai Choudhuri, Aarushi Goel, and Abhishek Jain. 2019. Two Round Information-Theoretic MPC with Malicious Security. In *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part II.* 532–561. https://doi.org/10.1007/978-3-030-17656-3_19

[3] P. Ananth, A. R. Choudhuri, and A. Jain. 2017. A New Approach to Round-Optimal Secure Multiparty Computation. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I (Lecture Notes in Computer Science, Vol. 10401).* Springer, 468–499. https://doi.org/10.1007/978-3-319-63688-7_16

[4] Benny Applebaum, Zvika Brakerski, and Rotem Tsabary. 2018. Perfect Secure Computation in Two Rounds. In *Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part I.* 152–174. https://doi.org/10.1007/978-3-030-03807-6_6

[5] Benny Applebaum, Zvika Brakerski, and Rotem Tsabary. 2019. Degree 2 is Complete for the Round-Complexity of Malicious MPC. In *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part II.* 504–531. https://doi.org/10.1007/978-3-030-17656-3_18

[6] Benny Applebaum, Eliran Kachlon, and Arpita Patra. 2020. The Resiliency of MPC with Low Interaction: The Benefit of Making Errors (Extended Abstract). In *Theory of Cryptography - 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, Proceedings, Part II.* 562–594. https://doi.org/10.1007/978-3-030-64378-2_20

[7] Benny Applebaum, Eliran Kachlon, and Arpita Patra. 2020. The Round Complexity of Perfect MPC with Active Security and Optimal Resiliency. In *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020.* 1277–1284. https://doi.org/10.1109/FOCS46700.2020.00121

[8] Benny Applebaum, Eliran Kachlon, and Arpita Patra. 2022. Verifiable Relation Sharing and Multi-verifier Zero-Knowledge in Two Rounds: Trading NIZKs with Honest Majority. In *Advances in Cryptology – CRYPTO 2022*, Yevgeniy Dodis and Thomas Shrimpton (Eds.). Springer, 33–56. https://doi.org/10.1007/978-3-031-15985-5_2

[9] Benny Applebaum, Eliran Kachlon, and Arpita Patra. 2023. The Round Complexity of Statistical MPC with Optimal Resiliency. Cryptology ePrint Archive, Paper 2023/418. (2023). The full version of this paper. https://eprint.iacr.org/2023/418.

[10] Benny Applebaum, Eliran Kachlon, and Arpita Patra. 2023. Round-optimal honest-majority mpc in minicrypt and with everlasting security. In *Theory of Cryptography: 20th International Conference, TCC 2022, Chicago, IL, USA, November 7–10, 2022, Proceedings, Part II.* Springer, 103–120. https://doi.org/10.1007/978-3-031-22365-5_4

[11] Gilad Asharov and Yehuda Lindell. 2017. A Full Proof of the BGW Protocol for Perfectly Secure Multiparty Computation. *J. Cryptology* 30, 1 (2017), 58–151. https://doi.org/10.1007/s00145-015-9214-4

[12] Saikrishna Badrinarayanan, Vipul Goyal, Abhishek Jain, Yael Tauman Kalai, Dakshita Khurana, and Amit Sahai. 2018. Promise zero knowledge and its applications to round optimal MPC. In *Annual International Cryptology Conference.* Springer, 459–487. https://doi.org/10.1007/978-3-319-96881-0_16

[13] Saikrishna Badrinarayanan, Aayush Jain, Nathan Manohar, and Amit Sahai. 2020. Secure MPC: Laziness Leads to GOD. In *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part III (Lecture Notes in Computer Science, Vol. 12493)*, Shiho Moriai and Huaxiong Wang (Eds.). Springer, 120–150. https://doi.org/10.1007/978-3-030-64840-4_5

[14] D. Beaver. 1991. Efficient Multiparty Protocols Using Circuit Randomization. In *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15*. 420–432. https://doi.org/10.1007/3-540-46766-1_34

[15] Donald Beaver, Silvio Micali, and Phillip Rogaway. 1990. The Round Complexity of Secure Protocols (Extended Abstract). In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, Maryland, USA*. 503–513. https://doi.org/10.1145/100216.100287

[16] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. 1988. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation (Extended Abstract). In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*. 1–10. https://doi.org/10.1145/62212.62213

[17] Fabrice Benhamouda and Huijia Lin. 2018. k-Round Multiparty Computation from k-Round Oblivious Transfer via Garbled Interactive Circuits. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*. 500–532. https://doi.org/10.1007/978-3-319-78375-8_17

[18] Zvika Brakerski, Shai Halevi, and Antigoni Polychroniadou. 2017. Four Round Secure Computation without Setup. In *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part I (Lecture Notes in Computer Science, Vol. 10677)*. Springer, 645–677. https://doi.org/10.1007/978-3-319-70500-2_22

[19] Mike Burmester and Yvo Desmedt. 1991. Broadcast Interactive Proofs (Extended Abstract). In *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings*. 81–95. https://doi.org/10.1007/3-540-46416-6_7

[20] Ran Canetti. 2001. Universally Composable Security: A New Paradigm for Cryptographic Protocols. In *42nd Annual Symposium on Foundations of Computer Science, FOCS 2001, 14-17 October 2001, Las Vegas, Nevada, USA*. 136–145. https://doi.org/10.1109/SFCS.2001.959888

[21] Ran Canetti, Joe Kilian, Erez Petrank, and Alon Rosen. 2001. Black-box concurrent zero-knowledge requires Omega~(log n) rounds. In *Proceedings on 33rd Annual ACM Symposium on Theory of Computing, July 6-8, 2001, Heraklion, Crete, Greece*. 570–579. https://doi.org/10.1145/380752.380852

[22] Alfonso Cevallos, Serge Fehr, Rafail Ostrovsky, and Yuval Rabani. 2012. Unconditionally-Secure Robust Secret Sharing with Compact Shares. In *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*. 195–208. https://doi.org/10.1007/978-3-642-29011-4_13

[23] David Chaum, Claude Crépeau, and Ivan Damgård. 1988. Multiparty Unconditionally Secure Protocols (Extended Abstract). In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*. 11–19. https://doi.org/10.1145/62212.62214

[24] Benny Chor, Shafi Goldwasser, Silvio Micali, and Baruch Awerbuch. 1985. Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults (Extended Abstract). In *26th Annual Symposium on Foundations of Computer Science, Portland, Oregon, USA, 21-23 October 1985*. 383–395. https://doi.org/10.1109/SFCS.1985.64

[25] B. Chor and E. Kushilevitz. 1989. A Zero-One Law for Boolean Privacy. In *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing* (Seattle, Washington, USA) *(STOC '89)*. Association for Computing Machinery, New York, NY, USA, 62–72. https://doi.org/10.1145/73007.73013

[26] Richard Cleve. 1986. Limits on the Security of Coin Flips when Half the Processors Are Faulty (Extended Abstract). In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing, May 28-30, 1986, Berkeley, California, USA*. 364–369. https://doi.org/10.1145/12130.12168

[27] Ronald Cramer, Ivan Damgård, Stefan Dziembowski, Martin Hirt, and Tal Rabin. 1999. Efficient Multiparty Computations Secure Against an Adaptive Adversary. In *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*. 311–326. https://doi.org/10.1007/3-540-48910-X_22

[28] Ronald Cramer, Ivan Damgård, and Serge Fehr. 2001. On the Cost of Reconstructing a Secret, or VSS with Optimal Reconstruction Phase. In *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*. 503–523. https://doi.org/10.1007/3-540-44647-8_30

[29] Danny Dolev and Rüdiger Reischuk. 1985. Bounds on Information Exchange for Byzantine Agreement. *J. ACM* 32, 1 (1985), 191–204. https://doi.org/10.1145/2455.214112

[30] Serge Fehr and Chen Yuan. 2020. Robust Secret Sharing with Almost Optimal Share Size and Security Against Rushing Adversaries. In *Theory of Cryptography - 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, Proceedings, Part III*. 470–498. https://doi.org/10.1007/978-3-030-64381-2_17

[31] Paul Feldman and Silvio Micali. 1985. Byzantine Agreement in Constant Expected Time (and Trusting No One). In *26th Annual Symposium on Foundations of Computer Science, Portland, Oregon, USA, 21-23 October 1985*. 267–276. https://doi.org/10.1109/SFCS.1985.14

[32] Matthias Fitzi, Juan A. Garay, Shyamnath Gollakota, C. Pandu Rangan, and K. Srinathan. 2006. Round-Optimal and Efficient Verifiable Secret Sharing. In *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006, Proceedings*. 329–342. https://doi.org/10.1007/11681878_17

[33] Sanjam Garg, Yuval Ishai, and Akshayaram Srinivasan. 2018. Two-Round MPC: Information-Theoretic and Black-Box. In *Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part I*. 123–151. https://doi.org/10.1007/978-3-030-03807-6_5

[34] Sanjam Garg and Akshayaram Srinivasan. 2017. Garbled protocols and two-round MPC from bilinear maps. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, 588–599. https://doi.org/10.1109/FOCS.2017.60

[35] Sanjam Garg and Akshayaram Srinivasan. 2018. Two-Round Multiparty Secure Computation from Minimal Assumptions. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*. 468–499. https://doi.org/10.1007/978-3-319-78375-8_16

[36] Rosario Gennaro, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin. 2001. The round complexity of verifiable secret sharing and secure multicast. In *Proceedings of the thirty-third annual ACM symposium on Theory of computing*. 580–589. https://doi.org/10.1145/380752.380853

[37] Rosario Gennaro, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin. 2002. On 2-Round Secure Multiparty Computation. In *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*. 178–193. https://doi.org/10.1007/3-540-45708-9_12

[38] Oded Goldreich and Hugo Krawczyk. 1996. On the Composition of Zero-Knowledge Proof Systems. *SIAM J. Comput.* 25, 1 (1996), 169–192. https://doi.org/10.1137/S0097539791220688

[39] Oded Goldreich, Silvio Micali, and Avi Wigderson. 1987. How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*. 218–229. https://doi.org/10.1145/28395.28420

[40] S. Dov Gordon, Feng-Hao Liu, and Elaine Shi. 2015. Constant-Round MPC with Fairness and Guarantee of Output Delivery. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*. 63–82. https://doi.org/10.1007/978-3-662-48000-7_4

[41] Shai Halevi, Carmit Hazay, Antigoni Polychroniadou, and Muthuramakrishnan Venkitasubramaniam. 2021. Round-optimal secure multi-party computation. *Journal of Cryptology* 34, 3 (2021), 1–63. https://doi.org/10.1007/s00145-021-09382-3

[42] Yuval Ishai and Eyal Kushilevitz. 2000. Randomizing Polynomials: A New Representation with Applications to Round-Efficient Secure Computation. In *41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12-14 November 2000, Redondo Beach, California, USA*. 294–304. https://doi.org/10.1109/SFCS.2000.892118

[43] Yuval Ishai and Eyal Kushilevitz. 2002. Perfect Constant-Round Secure Computation via Perfect Randomizing Polynomials. In *Automata, Languages and Programming, 29th International Colloquium, ICALP 2002, Malaga, Spain, July 8-13, 2002, Proceedings*. 244–256. https://doi.org/10.1007/3-540-45465-9_22

[44] Jonathan Katz, Chiu-Yuen Koo, and Ranjit Kumaresan. 2009. Improving the round complexity of VSS in point-to-point networks. *Inf. Comput.* 207, 8 (2009), 889–899. https://doi.org/10.1016/j.ic.2009.03.007

[45] Ranjit Kumaresan, Arpita Patra, and C. Pandu Rangan. 2010. The Round Complexity of Verifiable Secret Sharing: The Statistical Case. In *Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings*. 431–447. https://doi.org/10.1007/978-3-642-17373-8_25

[46] Leslie Lamport and Michael Fischer. 1982. *Byzantine generals and transaction commit protocols*. Technical Report. Technical Report 62, SRI International.

[47] Tal Moran, Moni Naor, and Gil Segev. 2016. An Optimally Fair Coin Toss. *J. Cryptology* 29, 3 (2016), 491–513. https://doi.org/10.1007/s00145-015-9199-z

[48] Arpita Patra, Ashish Choudhary, and Chandrasekharan Pandu Rangan. 2009. Simple and efficient asynchronous byzantine agreement with optimal resilience. In *Proceedings of the 28th ACM symposium on Principles of distributed computing*. 92–101. https://doi.org/10.1145/1582716.1582736

[49] Arpita Patra, Ashish Choudhary, Tal Rabin, and C. Pandu Rangan. 2009. The Round Complexity of Verifiable Secret Sharing Revisited. In *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*. 487–504. https://doi.org/10.1007/978-3-642-03356-8_29

[50] Arpita Patra, Ashish Choudhary, and C Pandu Rangan. 2008. Round Efficient Unconditionally Secure Multiparty Computation Protocol. In *Progress in Cryptology-INDOCRYPT 2008: 9th International Conference on Cryptology in India, Kharagpur, India, December 14-17, 2008. Proceedings*, Vol. 5365. Springer, 185. https://doi.org/10.1007/978-3-540-89754-5_15

[51] Tal Rabin and Michael Ben-Or. 1989. Verifiable Secret Sharing and Multiparty Protocols with Honest Majority (Extended Abstract). In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washigton, USA*. 73–85. https://doi.org/10.1145/73007.73014

[52] Arka Rai Choudhuri, Michele Ciampi, Vipul Goyal, Abhishek Jain, and Rafail Ostrovsky. 2020. Round optimal secure multiparty computation from minimal assumptions. In *Theory of Cryptography Conference*. Springer, 291–319. https://doi.org/10.1007/978-3-030-64378-2_11

[53] Andrew Chi-Chih Yao. 1986. How to Generate and Exchange Secrets (Extended Abstract). In *27th Annual Symposium on Foundations of Computer Science, Toronto, Canada, 27-29 October 1986*. 162–167. https://doi.org/10.1109/SFCS.1986.25

Received 2022-11-07; accepted 2023-02-06