Quadratic Multiparty Randomized Encodings Beyond Honest Majority and Their Applications*

Benny Applebaum† Yuval Ishai‡ Or Karni* Arpita Patra§

Abstract

Multiparty randomized encodings (Applebaum, Brakerski, and Tsabary, SICOMP 2021) reduce the task of securely computing a complicated multiparty functionality f to the task of securely computing a simpler functionality g. The reduction is non-interactive and preserves information-theoretic security against a passive (semi-honest) adversary, also referred to as *privacy*. The special case of a degree-2 encoding g (2MPRE) has recently found several applications to secure multiparty computation (MPC) with either information-theoretic security or making black-box access to cryptographic primitives. Unfortunately, as all known constructions are based on information-theoretic MPC protocols in the plain model, they can only be private with an honest majority.

In this paper, we break the honest-majority barrier and present the first construction of general 2MPRE that remains secure in the presence of a dishonest majority. Our construction encodes every n-party functionality f by a 2MPRE that tolerates at most $t = \lfloor 2n/3 \rfloor$ passive corruptions.

We derive several applications including: (1) The first non-interactive client-server MPC protocol with perfect privacy against any coalition of a minority of the servers and up to t of the n clients; (2) Completeness of 3-party functionalities under non-interactive t-private reductions; and (3) A single-round t-private reduction from general-MPC to an ideal oblivious transfer (OT). These positive results partially resolve open questions that were posed in several previous works. We also show that t-private 2MPREs are necessary for solving (2) and (3), thus establishing new equivalence theorems between these three notions.

Finally, we present a new approach for constructing fully-private 2MPREs based on multi-round protocols in the OT-hybrid model that achieve *perfect privacy* against active attacks. Moreover, by slightly restricting the power of the active adversary, we derive an equivalence between these notions. This forms a surprising, and quite unique, connection between a non-interactive passively-private primitive to an interactive actively-private primitive.

*This is the full version of a paper published in Crypto 2022.

†Tel-Aviv University, Israel bennyap@post.tau.ac.il, orzkarni@gmail.com

‡Technion, Israel yuvali@cs.technion.ac.il

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

Contents

1 Introduction

Information-theoretic secure multiparty computation (IT-MPC) deals with the problem of jointly computing a function over distributed inputs while providing information-theoretic privacy against an adversary that may corrupt a subset of the parties. IT-MPC has several important features. It does not rely on unproven intractability assumptions and does not depend on the computational power of the adversary. This notion also tends to provide clean frameworks (e.g., in the form of idealized models) for studying more complicated cryptographic questions without facing our ignorance regarding the nature of efficient computation. Moreover, apart from being a playground for basic theoretical feasibility results, IT-based solutions often lead to highly efficient protocols with a good concrete computational complexity. Finally, IT-MPC solutions typically form the basis for efficient computational MPC solutions that make a black-box use of cryptographic primitives.

In this paper, we consider several basic questions in the domain of IT-MPC and reveal new connections between them. By default, we consider n parties and assume that at most t of them can be passively corrupted by a (semi-honest) computationally unbounded adversary.[1] We refer to this as *t-privacy*. The following questions are open for any $t \geq n/2$.

MPC in the client-server model. Suppose that $n \geq 2$ parties, called *clients*, wish to employ $m \geq 3$ external parties, called *servers*, in order to securely compute some (possibly complex) function of their inputs. We would like to obtain a non-interactive protocol in which each client sends a single message to each server, depending on its input and its local randomness, and gets a single message from each server in return without any additional interaction.

Q 1.1. *Is there a non-interactive client-server MPC protocol with privacy against any (semi-honest) adversary who corrupts a minority of the m servers and up to t of the n clients?*

This question dates back to the work of Barkol, Ishai and Weinreb [6], who noted that even the 3-server case is open. Earlier client-server protocols [29, 18] only apply to the settings where less than *one third* of the servers (and $t < n$ clients) can be corrupted. The work of Applebaum, Brakerski and Tsabary [4] presented a client-server protocol that can tolerate any minority of corrupted servers, but at the expense of tolerating only $t < n/2$ corrupted clients. The case $t \geq n/2$ remains open. In this context, even a computationally-private solution with good concrete efficiency would be useful. However, the only known computationally-secure solution (which is in fact secure against an arbitrary strict subset of

[1] For simplicity, here and throughout the paper, we think of functionalities as finite objects and accordingly derive protocols and simulators with finite fixed complexity. All our statements carry over to the asymptotic setting (possibly with a tiny loss of the privacy threshold) and yield constructions whose complexity is polynomial in the size of the formulas (or branching program) of the underlying functionality. Furthermore, if one is willing to make a black-box use of a PRG and relax privacy to computational, these results also extend to size-s *circuits*, where the complexity is linear in s [39, 8, 18]. In fact, all these "liftings" can be done automatically by using appropriate completeness results from [29, 2, 4, 3]. See Appendix A.3.

servers) makes a non-black-box use of OT. This solution is obtained by applying a general transformation from [24] to the 2-round (non-black-box) OT-based MPC protocols from [25, 11].

Completeness of 3PC under non-interactive reductions. Let us move to the standard model where no servers are available. Classical completeness results, by Yao [39] and Goldreich, Micali and Wigderson [27], show that, for an arbitrary corruption threshold $t \leq n$, the problem of securely computing a general n-party functionality t-privately reduces to the problem of securely computing the elementary finite 2-party *Oblivious Transfer* (OT) functionality [38, 22]. The OT functionality takes a bit x from the Receiver and a pair of bits (m_0, m_1) from the Sender, and delivers to the Receiver the message m_x while hiding m_{1-x} from the Receiver and x from the Sender. In the 2-party setting, Yao's reduction [39] is completely non-interactive and makes only parallel invocations of an ideal OT-oracle without any further interaction. In the multiparty setting, known reductions are either interactive (i.e., make sequential calls to the OT) [27] or make a non-black-box use of the underlying OT [25], leading to computational security and to a large, typically impractical, computational overhead. In [3] it was shown that this limitation is inherent: No 2-party functionality can be complete under *round-preserving black-box* (RPBB) reductions. The same paper also established the completeness of 4-party functionalities, and stated the case of 3-party functionalities as an open question:

Q 1.2. *What is the minimal primitive that is non-interactively complete for t-private MPC? Are 3-party functionalities complete?*

The round complexity of protocols based on ideal-OT. Let us move back to OT-based protocols. In light of the negative result of [3], it is natural to ask what is the best achievable round complexity given a black-box access to an OT oracle. A partial answer was recently given by Patra and Srinivasan [37] who showed that, given a black-box access to a 2-round OT protocol, general secure multiparty computation with full computational privacy ($t \leq n$) can be realized in 3 rounds. This result falls short of providing information-theoretic security and, more importantly, it strongly relies on an access to an OT *protocol*. Consequently, we do not know whether a 3-round protocol can be based on other realizations of 2-round OT such as ones that are based on physical means such as noisy channels or secure hardware, or on some limited form of a trusted party (e.g., [17, 16, 36, 34, 21, 20]).[2] To capture such scenarios, we consider a refined version of the OT-hybrid model in which the OT takes 2 rounds. That is, if both parties send their inputs to an OT in round i, the output is delivered to the receiver at the *end* of round $i + 1$. In addition, the parties are allowed to exchange messages via standard point-to-point private channels. We refer to this

[2]More generally, one may ask whether $k + 1$ round protocols can be based on k-round OT, i.e., is it possible to obtain a *single-round reduction*. We focus on the minimal case of $k = 2$ for simplicity, though all our results actually hold for the general case.

model as the *2-round OT hybrid* model.[3] (See Remark 6.2 for further discussion about the model.) Refining an open question from [3], we ask

Q 1.3. *What is the minimal number of rounds that are needed for t-private MPC in the 2-round OT hybrid model? Are 3-rounds achievable?*

MPC with active perfect privacy in the OT-hybrid model. Let us change gears and move to the problem of perfect privacy under active attacks in the (standard) OT-hybrid model without putting any limitation on the round complexity. The results of Kilian [33] and Ishai, Prabhakaran, and Sahai [32] show that in this model one can achieve information-theoretic security with abort against a computationally unbounded adversary that corrupts an arbitrary subset of the parties. However, unlike the passive case, where one can achieve perfect simulation, current constructions suffer from a negligible statistical simulation error. It is known that one cannot simultaneously achieve perfect correctness and perfect privacy (aka perfect security) unless NP is contained in BPP (see, e.g., [30]). Still one can hope for a protocol that achieves *perfect privacy* against active attacks (i.e., a perfect simulation of the adversary's view) together with some weak form of correctness. Partial positive results are known for special classes of functionalities either in the correlated randomness setting [30] or in the 2-party setting [1]. Remarkably, for general functionalities the following basic question is wide open:

Q 1.4. *Is general MPC feasible in the OT-hybrid model with perfect passive correctness and perfect active t-privacy feasible?*

The difference between prefect privacy to statistical privacy is analogous to the difference between perfect zero-knowledge and statistical zero-knowledge. Furthermore, since the communication complexity grows logarithmically with the inverse error, perfectly-private protocols may lead to more economical solutions.

2MPREs beyond honest majority. In the honest-majority setting ($t < n/2$), Questions 1.1–1.3 can be settled in the affirmative based on the existence of t-private quadratic *multiparty randomized encoding* (MPRE).[4] The MPRE notion was introduced in [4] as a multiparty generalization of the notion of randomized encoding of functions from [29, 2]. Roughly speaking, a functionality f has a t-private quadratic-MPRE (2MPRE) if the task of securely-computing f non-interactively reduces to a single call to a degree-2 functionality

[3] In the terminology of [3] the reduction of Patra and Srinivasan [37] is a "free Black-Box" reduction, whereas the (2-round) OT hybrid model corresponds to so-called "strict Black-box reduction". To illustrate the distinction between the two notions, note that in a free-BB reduction, party A can, for example, generate several different "first messages" of the OT protocol, manipulate them (e.g., encrypt them) and deliver them to B or to a third party. Moreover, the 2nd part of these OT invocations can be later continued or withdrawn based on additional information (e.g., the inputs of B). In a strict BB reduction there is no notion of "first message" and the parties can only feed their inputs into the OT functionality and obtain the output. Thus a strict-BB reduction implies a free-BB reduction. See further discussion in [37].

[4] To the best of our knowledge, for Question 1.4, no solution is known beyond the trivial case of $t < n/3$ in which perfect active security can be achieved in the plain model [10].

g via a t-private information-theoretic reduction. In [4] it was shown that every functionality can be realized by an honest-majority 2MPREs. Other constructions were also given in [24, 35]. All these constructions are essentially based on plain-model MPC protocols and are therefore limited to the honest-majority setting. In an attempt to understand whether this limitation is inherent, we ask:

Q 1.5 ([4]). *Is t-private 2MPRE feasible with $t > n/2$?*

2 Our Results

We construct new 2MPREs and derive new connections between Questions 1.1–1.5.

2.1 New 2MPREs beyond Honest-Majority

We present the first construction of perfect 2MPRE that achieves privacy against coalitions of size at most $\lfloor 2n/3 \rfloor$.

Theorem 2.1 (main theorem). *Every n-party functionality can be perfectly realized by $\lfloor 2n/3 \rfloor$-private 2MPRE.*

The theorem "separates" the model of 2MPRE from plain-model MPC, demonstrating the power of the former. We will later discuss the implications of Theorem 2.1. For now observe that for 3-party functionalities the theorem provides privacy against coalitions of size at most 2. Since privacy against 3-party functionalities vacuously hold, we derive the following corollary.

Corollary 2.2 (2MPRE for 3PC). *Every 3-party functionality can be perfectly realized by a 3-private 2MPRE.*

Note that any tiny improvement to Theorem 2.1, e.g., from $\lfloor 2n/3 \rfloor$-privacy to $\lceil 2n/3 \rceil$-privacy would allow us to obtain fully-private MPRE for 4-party functionalities. Since 4-party functionalities are known to be complete under non-interactive reductions [3], such an improvement would immediately yield n-private 2MPREs for any n-party functionality! Thus, the $\lfloor 2n/3 \rfloor$ bound is a natural intermediate point between the case of full corruption $t = n$ and the honest-majority setting $t < n/2$. This puts 2MPRE somewhere between the OT-hybrid model, in which n-privacy can be achieved, to the plain model that is restricted to $(n-1)/2$-privacy.

Indeed, while proving Theorem 2.1, we show that 2MPREs are equivalent to an MPC model where the parties are allowed to communicate via private point-to-point channels for an arbitrary number of rounds and at the end are allowed to make a single call to a degree-2 functionality. If we remove this last round, we get the standard plain model and if we allow to call degree-2 functionalities in every round we get the standard OT-hybrid model. In fact, by preprocessing OTs [7], the OT-hybrid model is equivalent to a model where all the OT-calls are performed in the first round and all other rounds use private point-to-point

channels. Thus, the "only difference" between the 2MPRE model and the OT-hybrid model is whether the degree-2 functionality is being invoked before the plain-model sub-protocol or after it.

2.2 Equivalences and Implications

Theorem 2.1 implies affirmative answers to Questions 1.2 and 1.3 with $t = \lfloor 2n/3 \rfloor$. We prove that 2MPREs are also necessary for the resolution of these questions.

Theorem 2.3 (Necessity of 2MPRE)**.** *The following holds for every n-party functionality f and privacy threshold $1 \leq t \leq n$.*

1. *If f non-interactively t-privately reduces to some 3-party functionality, then f has a t-private 2MPRE.*
2. *If f can be t-privately computed in 3 rounds in the 2-round OT hybrid model, then f has a t-private 2MPRE.*

The results of [3] imply that if f has t-private 2MPREs then it non-interactively t-privately reduces to the following 3-party variant of OT (hereafter referred to as TOT). Given a pair of bits (x_1, y_1) from Alice, and a pair of bits (x_2, y_2) from Bob, the functionality delivers to Carol the value $x_1x_2+y_1+y_2$ where addition and multiplication are computed over the binary field. Alice and Bob receive no output.[5] TOT takes its input from only 2 parties and deliver it to the third party and so it can be seen as an extremely simple variant of a 3-party functionality. Nevertheless, by combining Theorem 2.3 with the above implication, we conclude that TOT is complete for 3-party functionalities. Finally, we observe that TOT can be easily computed in 3 rounds in the 2-round OT hybrid model (see Section 6). We therefore derive the following equivalence.

Corollary 2.4. *Let f be an n-party functionality and let $1 \leq t \leq n$ be some integers. The following statements are equivalent:*

1. *f can be realized by t-private 2MPRE.*
2. *f non-interactively t-privately reduces to TOT.*
3. *f non-interactively t-privately reduces to some 3-party functionality.*
4. *f can be t-privately computed in 3 rounds in the 2-round OT hybrid model.*

The theorem yields an equivalence between Questions 1.2, 1.3 and 1.5. This equivalence is fairly strong: it holds for each functionality separately and carries to the statistical setting as well while preserving correctness and privacy errors.

[5] We refer to this as "3-party OT" since the 2-party version of this functionality, where the output is delivered to, say, Alice, is essentially equivalent to the standard 1-out-of-2 OT.

The client-server model. Let us get back to the client-server model (Question 1.1). It was shown in [4] that t-private 2MPREs imply non-interactive t-private client-server protocols. As an immediate corollary of Theorem 2.1, we derive the following statement.

Corollary 2.5. *Every n-party functionality has a non-interactive client-server MPC with privacy against any coalition that consists of a minority of the m servers and up to $\lfloor 2n/3 \rfloor$ of the n clients. For the case of 3 clients, we derive privacy against an arbitrary (mixed) coalition of clients and a minority of the servers.*

Being an information-theoretic protocol, our construction is fairly efficient and may turn to be useful in 3PC applications.

2.3 2MPREs vs Active Perfect-Privacy

In an attempt to obtain better 2MPREs with privacy threshold larger than $\lfloor 2n/3 \rfloor$, we reveal a new connection to the problem of achieving perfect-privacy under active attacks (Question 1.4). Specifically, we show that any protocol in the OT-hybrid model with perfect t-privacy under active attacks and passive perfect (or statistical) correctness can be turned into a t-private 2MPRE with statistical correctness error. We find this implication quite surprising; the protocol is an actively-secure primitive with no round-complexity requirements, whereas the 2MPRE is a passively-secure object whose main feature is low interaction. In fact, by weakening the notion of active attacks we derive a surprising equivalence between these 2 objects. Loosely speaking, we consider a *weakly-active* adversary that corrupts a subset T of the parties and deviates from the protocol as follows: For every OT-call between two corrupted parties, the adversary is allowed to replace the receiver's received message m with some arbitrary value m'. Once this value is replaced, the adversary must consistently use this fake value according to the instructions of the protocol. For example, if the protocol instructs the receiver to pass m to all the parties, then the adversary passes m' to all the parties. (See Section 7 for a formal definition.)

We prove the following theorem.

Theorem 2.6. *Let f be an n-party public-output functionality and let $0 \leq t \leq n$ be an arbitrary privacy threshold. The functionality f has a protocol in the OT-hybrid model with statistical (passive) correctness and t-perfect privacy against weakly-active adversaries if and only if f has a t-private 2MPRE with statistical correctness error.*

The error can be reduced to an arbitrarily small ϵ with $O(\log(1/\epsilon))$ overhead via standard error-reduction techniques. A public-output functionality is a functionality that delivers the same output to all the parties; it is known that general functionalities can be reduced to public-output functionalities via a non-interactive reduction.

Note that in the honest-majority setting, any protocol with perfect passive t-privacy is also t-perfectly private against a weakly-active adversary (since there are no calls to OT). In this setting, Theorem 2.6 yields a new alternative construction of 2MPREs. In fact, as a by-product, we derive a new completeness result in the honest-majority setting.

Theorem 2.7 (completeness of $\mathsf{AND} \circ \mathsf{EQ}$ for honest majority)**.** *In the honest majority setting, every n-party functionality f non-interactively reduces to multiple parallel calls to $\mathsf{AND} \circ \mathsf{EQ}$ functionality. The reduction has perfect privacy and an arbitrarily small 1-sided statistical correctness error.*

For parameters ℓ and k, the predicate $\mathsf{AND} \circ \mathsf{EQ}$ takes ℓ pairs of k-bit strings, computes for each pair an equality bit v_i that determines whether the ith pair is equal, and outputs the logical AND of all the bits $v_1, \ldots, v_\ell$. Specifically, we allocate a single equality for each pair of parties (i.e., $\ell = \binom{n}{2}$).

Features of the $\mathsf{AND} \circ \mathsf{EQ}$ predicate. Since $\mathsf{EQ}(x, y) = \bigwedge_i (x_i \oplus \bar{y}_i)$, the $\mathsf{AND} \circ \mathsf{EQ}$ predicate can be replaced by a conjunction of *parities* of *pairs* of bits. Another feature of this predicate is the following physical implementation: suppose each pair of parties are connected by pipes (alternatively, electrical wires), one for each comparison of two bits held by these parties. For each pipe (wire), one can ensure that water (electricity) flows through only if equality holds. For instance, an input bit may determine the position of a switch, where the two switches need to be aligned to enable flow. Finally, connecting all pipes via an Euler path, the output of the $\mathsf{AND} \circ \mathsf{EQ}$ predicate corresponds to whether or not the flow gets through the system.

2.4 Techniques

To illustrate some of our techniques, let us focus on the 2MPRE construction and on the implications of protocols that achieve perfect-privacy under active attacks.

2.4.1 Constructing 2MPREs

Our new construction (Theorem 2.1) is based on two components. First, we introduce a new round-collapsing lemma that turns a 2-round protocol that satisfies some "nice" form into a 2MPRE. Then, we design a nice protocol with $\lceil 2n/3 \rceil$-privacy and collapse it into a 2MPRE. Let us elaborate on these steps.

Round-collapsing lemma. Recall that a 2MPRE can be viewed as a non-interactive protocol that makes only parallel calls to some degree-2 functionalities (WLOG, we may use only TOT calls). Consider the seemingly more liberal model where the parties are allowed to make a single round of communication over private point-to-point channels before calling the TOT functionalities. We prove that such a *nice* protocol π can be turned into a 2MPRE. To explain the high-level idea, let us assume that the protocol π makes a single call to TOT where A and B are the senders with inputs f and g, respectively, and C receives $\mathsf{TOT}(f, g)$. The messages f and g are computed based on first-round messages that were sent to A and B during the first round by all the parties $P_1, \ldots, P_n$. Denote by $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ the vectors of these first-round messages. Our goal is to replace the second-round call to TOT with many first-round calls to TOT. All these TOTs are delivered to the

receiver C and the pair of senders range over all possible pairs of the form (A, B), (A, P_i) or (B, P_i). Let us imagine, for a moment, that the original TOT computation $\mathsf{TOT}(f, g)$ is replaced with some multi-output function $H(f, g)$ in which each output depends on a single bit either of f or of g. Moreover, let us assume that each bit of $f = f(a)$ and $g = g(b)$ depends on a single bit of the input. In this case, each output of H depends on some message, a_i or b_i, that some P_i have sent in the first round. Therefore, the corresponding bit of H could be delivered to C directly at the first round by some party P_i. Of course, we cannot really hope for such single-bit dependencies. Instead, we replace each of the above computation with a fully-decomposable randomized encoding [29, 2]. Such an encoding preserves the original information while maintaining privacy, at the expense of using some secret randomness. The crucial observation is that in our case the randomness can be chosen either jointly by A and B (for randomizing the TOT part), or solely by A (for randomizing the f part) or solely by B (for randomizing the g part). This is due to the fact that we do not need to hide f (resp., g) from A (resp., B). Overall, this allows us to collapse the computation to first-round calls to multiple 2-party functionalities.[6] The latter can be trivially encoded by 2MPRE, which, by a proper form of composition, leads to 2MPRE for the entire computation. For full details see Lemma 4.2 and its proof. By applying the reduction repeatedly, one can turn a multi-round plain-model protocol whose last round makes calls to degree-2 ideal functionalities into a 2MPRE, establishing the equivalence of these 2 models. The round-preserving lemma plays a central role in our constructions as well as in our negative results about the necessity of 2MPREs.

Nice protocols. Equipped with the round-collapsing lemma, we explore the power of nice protocols. To illustrate the power of the model, let us start by observing that for degree-3 computation (which is known to be complete [29]), the passive honest-majority version of the BGW protocol [10] gives rise to a nice protocol! In the standard description of the protocol, in (R1) the parties secret share their inputs, then the parties multiply their shares locally and (R2) apply a round of degree-reduction, then the parties apply another local multiplication and (R3) publish the randomized shares. Since degree reduction is a linear operation one can replace the last 2 rounds (including the second local multiplication) with a call to a degree-2 functionality, and derive a "nice" protocol. The resulting construction can be viewed as an abstract version of a recent algebraic construction of honest-majority arithmetic 2MPREs [35]. The round-collapsing lemma allows us to derive this result immediately in a conceptually clean way.

Observe that the BGW-based 2MPRE works even if the ideal degree-2 functionality is only private against a corrupted minority. Put differently, we did not use the full power of the degree-2 oracle that provides *privacy against an arbitrary coalition*. Our result for $t = \lfloor 2n/3 \rfloor$ is derived by making a stronger use of this resource. Following BGW, we dedicate

[6] A related observation is in the heart of other recent round reduction techniques [25, 11, 4], though we do not see a way to obtain our result based on their techniques. Specifically, [25, 11] makes a non-black-box use of OTs and [4] exploit the specific properties of Yao's based randomized encodings. In particular, the latter result does not seem to extend to arithmetic protocols while our result does.

the first round to input sharing, except that this time we use a CNF-based secret sharing scheme. That is, we additively share each input into $\binom{n}{t}$ shares where each share corresponds to some "unauthorized" t-subset T of the parties, and hand the corresponding share to all parties outside T. Now a degree-3 computation boils down to a sum of degree-3 monomials over the additive shares. A threshold of $t = \lfloor 2n/3 \rfloor - 1$ guarantees that for each monomial there must exists a party who holds 2 variables of the monomials. (A slightly modified version yields $t = \lfloor 2n/3 \rfloor$.) By locally computing these values, we can realize the remaining parts via a call to a degree-2 functionality. See Section 5. We note that a similar degree-reduction technique was previously used in the contexts of communication complexity [5] and information-theoretic private information retrieval [9]. The current application is unique in that it applies this technique in the context of *feasibility* rather than *efficiency*.

2.4.2 2MPREs from Perfect Active Privacy

Consider the following MPC-in-the-head type approach [31, 32] for transforming a plain-model (passively) t-private protocol π to a t-private 2MPRE. Each party P_i samples locally a random tape and guesses randomly a sequence of incoming messages. Then P_i computes, based on this random view, the vector of outgoing messages that should be sent in π given this view. Finally, P_i sends her guesses for the incoming messages together with the computed outgoing messages to an ideal functionality V. The functionality V checks that the local views match; namely, that each guessed incoming message is equal to the corresponding outgoing message. If all these tests pass, V returns the output of the protocol (assume wlog that this output appears in the transcript), say to all the parties. Otherwise, V outputs zero.

It can be shown that the resulting protocol σ is perfectly private. Correctness holds when all the guesses succeed which happens with probability 2^{-c} where c is the communication complexity of π. Since privacy is perfect we can arbitrarily reduce the correctness error via repetition. The ideal functionality V can be written as a conjunction of Equality tests. Since Equality of two bits is a linear function over $\mathbb{F}_2$, and since AND has a degree-2 RE (with statistical correctness error), V can be replaced with a degree-2 functionality. By instantiating π with a perfect plain-model honest majority protocol (e.g., BGW) we obtain another construction of honest-majority 2MPRE, this time with a statistical correctness error. (Note that so far π is only required to be passively private.)

In order to obtain an MPRE in the honest-minority setting, we start with a protocol π that operates in the OT-hybrid model and add pair-wise consistency checks over OT values. That is, each party guesses the incoming messages and incoming OT messages and computes the corresponding outgoing messages and OT-inputs. Now V verifies that the local views are pair-wise consistent. Unfortunately, an OT consistency check corresponds to a quadratic relation. Since these tests are being fed into a degree-2 function (the randomized encoding of AND), we get a degree-3 encoding of V. We bypass the problem by letting the pair of parties that use the OT call to locally sample part of the randomness of the RE. This allows us to reduce the degree at the expense of leaking some information about the inputs of V. We show that this leakage can still be simulated if the original protocol π is weakly-active

perfectly private. See Section 7 for more details.

Organization. Following some preliminaries in Section 3, we relate 2MPREs to non-interactive protocols in the TOT-hybrid model and prove the round-collapsing lemma in Section 4. We present our main construction in Section 5, and dedicate Section 6 to the equivalence between 2MPREs and protocols in the 2-round-OT hybrid model. Finally, in Section 7, we establish the equivalence between 2MPREs and perfect privacy under weakly-active attacks. Some MPC background appears in the appendix.

3 Preliminaries

We assume familiarity with standard MPC definitions. The relevant background appears in Appendix A.We will extensively use randomized encoding (RE) of functions and multiparty randomized encoding as means for transforming and manipulating protocols.

Definition 3.1 (Randomized Encoding of functions [29])**.** *Let $f : X \to Y$ be a function. We say that a function $\widehat{f} : X \times R \to Z$ is a δ-correct and ϵ-private* randomized encoding *(RE) of f if the following holds:*

- *(δ-correctness) There exists a randomized algorithm* Dec *such that for every input $x \in X$,*
$$\Pr_{r \leftarrow R}\left[\mathsf{Dec}(\widehat{f}(x;r)) \neq f(x)\right] \leq \delta$$
- *(ϵ-privacy) There exists a randomized algorithm* Sim *such that for every $x \in X$, the distributions*
$$\mathsf{Sim}\,(f(x)) \quad \textit{and} \quad \widehat{f}(x;r), \qquad \textit{where } r \leftarrow R,$$
are ϵ-close in statistical distance.

By default, we assume that both correctness and privacy are perfect*, i.e., ϵ and δ are both zero.*

By default, the set X (resp., R, Z) is a set of strings of some fixed length. An RE, $\widehat{f}$, is *fully decomposable* if each of its outputs $\widehat{f}_i(x;r)$ depends on at most a single input bit of x. The encoding $\widehat{f}$ has degree d if each of its outputs can be written as a degree-d polynomial over a field $\mathbb{F}$ (by default the binary field). If $X = \mathbb{F}^n, R = \mathbb{F}^\rho$ and $Z = \mathbb{F}^s$, then each output $\widehat{f}_i(x,r)$ can be written as a degree-d polynomial in the inputs $(x_1, \ldots, x_n, r_1, \ldots, r_\rho)$. The encoding is d-local if each output depends on at most d inputs $(x_1, \ldots, x_n, r_1, \ldots, r_\rho)$. The *complexity* of an encoding $\widehat{f}$ is s if the encoding can be computed, simulated, and decoded by s-size circuits. In the asymptotic setting, when f is treated as a polynomial-time uniform family of circuits, s is required to be polynomial-time bounded and the circuits for encoding, decoding and simulating should all be uniform. All known RE constructions satisfy these properties.

Functionalities. An n-party functionality is a function that maps the inputs of n parties to a vector of outputs that are distributed among the parties. Without loss of generality, we assume that the inputs and outputs of each party are taken from some fixed input and output domains X and Y (e.g., bit strings of fixed length). We will also make use of *randomized functionalities*. In this case, we let f take an additional random input r_0 that is chosen uniformly from some finite domain R, and view r_0 as an internal source of randomness that does not belong to any party. We typically write $f(x_1, \ldots, x_n; r_0)$ and use semicolon to separate the inputs of the parties from the internal randomness of the functionality.

Definition 3.2 (Multiparty Randomized Encoding (MPRE) [4])**.** *Let $f : X^n \to Y^n$ be an n-party functionality. We say that an n-party randomized functionality $\widehat{f} : (X \times R)^n \times R \to Z^n$ is a* multiparty randomized encoding *of f if the following holds:*

- *(δ-correctness): There exists a decoder* Dec *such that for every party $i \in [n]$, and every input $x = (x_1, \ldots, x_n)$ it holds that*

$$\Pr_{(r_0, r_1, \ldots, r_n) \leftarrow R^{n+1}} [\mathsf{Dec}(i, \widehat{y}[i], x_i, r_i) = y[i]] \leq \delta,$$

  where $y = f(x_1, \ldots, x_n), \widehat{y} = \widehat{f}((x_1, r_1), \ldots, (x_n, r_n); r_0)$, and $y[i]$ and $\widehat{y}[i]$ are the restrictions of y and $\widehat{y}$ to the coordinates delivered to party i by f and $\widehat{f}$, respectively.

- *((t, ϵ)-privacy): There exists a randomized simulator* Sim *such that for every t-subset $T \subseteq [n]$ of parties and every set of inputs $x = (x_1, \ldots, x_n)$ it holds that the distributions*

$$\mathsf{Sim}(T, x[T], y[T]), \quad \text{where } y = f(x_1, \ldots, x_n)$$

  and the distributions

$$(x[T], r[T], \widehat{y}[T])$$

  where

$$\widehat{y} = \widehat{f}((x_1, r_1), \ldots, (x_n, r_n); r_0), \text{ and } (r_0, r_1, \ldots, r_n) \leftarrow R^{n+1}$$

  are ϵ-close in statistical distance.

We say that $\widehat{f}$ is perfectly correct *if it has δ-correctness for $\delta = 0$, and* perfectly t-private *if it has (t, ϵ)-privacy for $\epsilon = 0$. We say that $\widehat{f}$ is* t-private *if it is both perfectly correct and perfectly t-private.*

Definition 3.3 (Effective degree and 2MPRE)**.** *A (possibly randomized) n-party functionality $f : X^n \times R \to \{0,1\}^m$ has effective degree d if there exist a tuple of local preprocessing functions $(h_1, \ldots, h_n)$ and a degree-d function h such that*

$$h(h_1(x_1), \ldots, h_n(x_n); r) = f(x_1, \ldots, x_n; r),$$

for every input $x_1, \ldots, x_n$ and internal randomness r.

A functionality f has a t-private quadratic MPRE (2MPRE) if it has a t-private MPRE with an effective degree of 2. Unless stated otherwise, we assume, by default, that the privacy and correctness errors are zero.

If f has a t-private 2MPRE $h\left(h_1(x_1),\ldots,h_n(x_n);r\right)$ then it can be computed by a non-interactive t-private reduction: First, the ith party locally computes h_i on her input and random tape; then she sends the result to the degree-2 functionality h; and finally she locally computes her output by using the MPRE decoder. In fact, the converse direction also holds, and so f has a t-private 2MPRE if and only if it reduces to a degree 2 functionality g via a non-interactive t-private reduction that makes a single call to g.[7] (See Proposition A.3 for a more general statement.)Despite this equivalence, the MPRE abstraction will be useful as it will allow us to conveniently manipulate protocols and gradually turn them into 2MPREs. Specifically, we will often use the composition lemma (Lemma A.5)that asserts that if f is encoded by an MPRE g, and g is encoded by an MPRE h then h encodes f. (This lemma together with few other useful properties of MPREs appear in Section A.2.) Finally, let us make the following simple, yet useful, observation.

Observation 3.4. *Let f be a 3-party functionality that takes its input from only 2 parties (aka 2-input functionality). Then, f has a 3-private 2MPRE.*

Proof. Let $\{P_0,P_1,P_2\}$ be the three parties and assume that only P_0 and P_1 give inputs to the functionality. Now write each output of f as a polynomial and note that each monomial can be broken into a product of P_0's inputs and P_1's inputs. These respective products can be computed locally by P_0 and P_1, leading to a trivial (deterministic) 2MPRE. □

4 2MPRE and TOT-hybrid model

The TOT-hybrid model. A protocol in the TOT-hybrid model consists of black-box calls to the TOT functionality. We assume that each 3-tuple of parties (A,B,C) can make a call to an ideal TOT functionality $\mathsf{TOT}:\{0,1\}^2\times\{0,1\}^2\times\{\perp\}\to\{\perp\}\times\{\perp\}\times\{0,1\}$ where

$$\mathsf{TOT}\big((x_1,y_1),(x_2,y_2),\perp\big)=(\perp,\perp,x_1x_2+y_1+y_2).$$

By letting $A=C$ or $A=B$ respectively, TOT calls can emulate OT calls as well as 2-wise private channels. Still, it will be sometimes convenient to make explicit use of private point-to-point channels. We will mainly be interested in non-interactive protocols in this model where the parties make a single round of parallel calls to the TOT functionality.

The following claim can be derived from [3] who studied a close variant of TOT known as $(2,3)$-MULTPlus. For completeness, we provide a self-contained proof in Section 4.1.

Claim 4.1. *If a functionality F has a t-private 2MPRE then it has a t-private non-interactive protocol in the TOT-hybrid model.*

The converse direction trivially holds since by definition, a non-interactive protocol in the TOT-hybrid model is also a non-interactive reduction to a degree-2 functionality. The following lemma provides a stronger converse: It shows that a 2MPRE can be derived even if

[7] The requirement for a single call is without loss of generality in the semi-honest setting, since multiple parallel calls can be packed in a single call.

we start from a 2-round protocol in the TOT-hybrid model whose first round only consists of private messages (carried over private point-to-point channels) and its second rounds consists of parallel calls to the TOT functionality.

Lemma 4.2 (Collapsing a round in TOT-hybrid model)**.** *Suppose that the n-party functionality f can be realized by a t-private protocol π in the TOT-hybrid model whose first round only consists of private messages (carried over private point-to-point channels) and its second round consists of parallel calls to the TOT functionality. Then f has a t-private 2MPRE f'. Moreover, f can be realized by a t-private non-interactive protocol σ in the TOT-hybrid model. The transformation holds even if π has a correctness error or a privacy error while preserving these errors.*

Before proving the lemma, we note that once we can collapse a single plain-model round, we can also collapse multiple plain-model rounds. Specifically,

Corollary 4.3 (Collapsing multiple rounds in TOT-hybrid model)**.** *Suppose that the n-party functionality f can be realized by a t-private multi-round protocol π in the TOT-hybrid model that makes TOT calls only in the last round (al;l other rounds are in the plain model). Then f has a t-private 2MPRE f'. Moreover, f can be realized by a t-private non-interactive protocol σ in the TOT-hybrid model. The transformation holds even if π has a correctness error or a privacy error while preserving these errors.*

Proof of Cor. 4.3. By induction on the round complexity k. For $k = 1$ the statement is trivial. Assume that the statement holds for k, and consider a $(k+1)$-round protocol π for f that makes calls to TOT only in the last round. We decompose π to a plain-model protocol π_1 that consists of the first $k-1$ rounds π and to a protocol π_2 that consists of the last 2 rounds of π. Accordingly, the first round of π_2 is a "plain-model" round and the second round makes TOT-calls. We can (artificially) define a functionality g that is being perfectly realized by π_2 with full security (e.g., g takes the state of each party and delivers the to her the messages that are delivered by g). By Lemma 4.2, g can be perfectly realized by a 2MPRE with full security, and so it admits a protocol π_2' that makes a single round of calls to TOTs. By appending π_2' to π_1 (and applying a proper local decoding in the end), we derive a k-round protocol π' that realizes f with correctness and privacy guarantees that are identical to π. By construction, π' makes TOT calls only in the last round, and so the corollary follows by the induction hypothesis. □

We move on and prove Lemma 4.2.

Proof of Lemma 4.2. Let $f : X^n \to \{0,1\}^m$ be an n-party functionality, and let π be δ-correct (t,ϵ)-private protocol in the TOT-hybrid model whose first-round only consists of private messages and its second-round consists of parallel calls to the TOT functionality. For each call to the TOT functionality with parties $A \in \mathcal{P}$ and $B \in \mathcal{P}$ and receiver $C \in \mathcal{P}$, the protocol π can be viewed as computing the following functionality o:

- Each party P_i locally computes messages a_i and b_i based on its private input and randomness and sends a_i to A and b_i to B. As part of this step, A (resp., B) sends her private input/randomness to herself.

- The receiver C gets the TOT output

$$\mathsf{TOT}((f_0(a), f_1(a)),\ (g_0(b), g_1(b))),$$

  where $a = (a_i)_{i\in[n]}$ and $b = (b_i)_{i\in[n]}$ and f_0, f_1, g_0, g_1 are some Boolean functions. (In π the party A computes f_0 and f_1 locally and the party B locally computes the functions g_0, g_1).

To prove the lemma it suffices to encode the functionality o by a perfect MPRE of effective degree-2. To gain some intuition, imagine the case where a and b are selected by A and B, respectively. Then the output that is delivered to C is a 2-party functionality that depends only on values that can be computed by either A or B. Such a function trivially has an effective degree of 2 as per Observation 3.4. Our setting is slightly more involved: While some inputs are neither chosen by A nor by B, each of these inputs is being leaked either to A or to B. We show that in this case one can still obtain a 2MPRE.

As our first step, we construct an MPRE for o based on degree-3 RE as follows. Let $\widehat{o}(a, b; r)$ be the standard degree-3 fully-decomposable RE from [29, 2] where $r = (r_1, \ldots, r_m)$ is the internal randomness of the RE. Consider the functionality $\widehat{o}_1$ in which party A randomly samples $\alpha = (\alpha_i)_{i\in[m]}$, party B randomly samples $\beta = (\beta_i)_{i\in[m]}$, and party P_i locally computes a_i and b_i as before. The functionality $\widehat{o}_1$ delivers the value

$$\widehat{o}(a, b; \alpha + \beta)$$

to C and the vector a to A and b to B. We claim that $\widehat{o}_1$ is an MPRE of o. Indeed, correctness follows from the correctness of the RE. As for privacy, fix a set $T \subseteq [n]$ that contains the receiver C (if $C \notin T$ simulation is trivial). Observe that if A or B are not in T, then privacy follows from the privacy of the RE (since, conditioned on the view of the parties in T, the distribution of C's output in $\widehat{o}_1$ is identical to the distribution of $\widehat{o}(a, b; \alpha + \beta)$). Finally, if both A and B are in T, then simulating C's output is trivial since we have both a and b as part of T's view in o.

Next, our goal is to construct a 2MPRE for $\widehat{o}_1$. First, let us take a step backward and recall that the degree-3 RE $\widehat{o}(a, b; r)$ is so-called *fully-decomposable* RE, which means that each of its outputs is either a degree-2 function (of the form $r_i + r_j + r_k$ or $r_i r_j + r_k$ or $x_i r_i + r_j$) or an expression of the form

$$x r_j r_k + r_\ell$$

where x is either a_i, b_i or r_i and r_i, r_j, r_k, r_ℓ are part of the internal random bits $r = (r_1, \ldots, r_m)$ of the RE. Recalling that $r = \alpha + \beta$, observe that each output bit that $\widehat{o}_1$ delivers to C is of the form

$$x(\alpha_j + \beta_j)(\alpha_k + \beta_k) + (\alpha_\ell + \beta_\ell) = x\alpha_j\alpha_k + x\alpha_j\beta_k + x\beta_j\alpha_k + x\beta_j\beta_k + (\alpha_\ell + \beta_\ell) \qquad (1)$$

where x is either a_i, b_i or $\alpha_i + \beta_i$. Let us start by breaking this sum to separate monomials. That is, we define the functionality $\widehat{o}_2$ that operates identically to $\widehat{o}_1$ except that each bit in (1) that $\widehat{o}_1$ delivers to C is replaced with the tuple

$$(x\alpha_j\alpha_k + s_1, x\alpha_j\beta_k + s_2, x\beta_j\alpha_k + s_3, x\beta_j\beta_k + (\alpha_\ell + \beta_\ell) - (s_1 + s_2 + s_3)) \tag{2}$$

where s_1, s_2 and s_3 are uniform bits that are sampled as part of the internal randomness of the functionality $\widehat{o}_2$.[8] The tuple in (2) is a tuple of 4 random bits whose sum equals to (1). Therefore, (2) perfectly encodes (1) and so $\widehat{o}_2$ perfectly encodes $\widehat{o}_1$.

Observe that the first entry of (2) has an effective degree of 2 since A can precompute $\alpha_j \cdot \alpha_k$. Similarly, the last entry has an effective degree 2 since B can precompute $\beta_j \cdot \beta_k$. Moreover if $x = \alpha_i + \beta_i$ then the second and third entries of (2) have also an effective degree of 2. It remains to handle the second and third entries in the case where x is either a_i or b_i. Let us focus on the second entry and assume that $x = a_i$ (the other cases are handled similarly). Consider the functionality $\widehat{o}_3$ that is identical to $\widehat{o}_2$ except that instead of delivering the second entry of (2) to C we deliver to C the tuple

$$(a_i + \alpha', \alpha_j\beta_k + s', a_i s' + \alpha'\alpha_j\beta_k + \alpha' s' - s_2)\,. \tag{3}$$

Here s' is sampled as part of the internal randomness of the functionality, and, crucially, α' is sampled uniformly by A. Therefore, (3) has an effective degree of 2. We claim that $\widehat{o}_3$ perfectly encodes $\widehat{o}_2$. Indeed, given an output (y_1, y_2, y_3) of (3), we can decode the second entry of (2) by outputting the value $y_1 y_2 - y_3$. As for privacy, consider a set $T \subsetneq [n]$ and assume that $C \in T$ (again the other case is trivial). If $A \notin T$, then simulation is simple: given y, the second entry of (2), sample y_1, y_2 uniformly at random and set $y_3 = y_1 y_2 - y$. If $A \in T$, then the simulator is given y,a_i and α' as part of A's private tape, accordingly we set $y_1 = a_i + \alpha'$, sample y_2 uniformly and set $y_3 = y_1 y_2 - y$. It is not hard to verify that the simulation is perfect.

By handling the third entry of (2) similarly, we derive an MPRE of effective degree 2 that encodes $\widehat{o}_2$. By the MPRE composition lemma (Lemma A.5),we conclude that the functionality o admits a perfect 2MPRE. Overall, we encoded f by a a δ-correct (t, ϵ)-private f'.

To prove the "Moreover" part, observe that, by Claim 4.1, f' can be perfectly realized by a non-interactive protocol π' in the TOT-hybrid model. By Proposition A.3,π' admits a non-interactive protocol σ in the TOT-Hybrid model that realizes f with δ-correctness and (t, ϵ)-privacy, as required. □

4.1 Proof of Claim 4.1

We present such a protocol for each output bit of F separately. For concreteness, let us focus on the first output bit F_1, and let us assume, wlog, that this output is delivered to a single

[8] In fact, we could take s_i to be the sum of a random bit that is sampled by A and a random bit that is sampled by B.

party denoted by P. By assumption, $F_1((x_1, r_1), \ldots, (x_n, r_n))$ can be written as a degree-2 function of the form

$$\sum_{i \leq j \in [n]} a_{i,j} a_{j,i}$$

where, for every $i, j \in [n]$, the value $a_{i,j} = a_{i,j}(x_i; r_i)$ is computed locally by the ith party. The protocol π' proceeds as follows.

1. Each party P_i computes locally the values $a_{i,i}, \ldots, a_{i,n}$ and, in addition, she samples, for each $j \in [n]$, a random pad $r_{i,j} \leftarrow \{0,1\}$ under the constraint that $\sum_j r_{i,j} = 0$ where addition is over the binary field.

2. For every $i \leq j \in [n]$, the parties P_i and P_j use a constant number of parallel calls to TOT to deliver to P the value $a_{i,j} a_{j,i} + r_{i,j} + r_{j,i}$.

3. The party P outputs the sum of all the values that were received by the TOT calls.

Clearly, the protocol can be realized by making only parallel calls to the TOT oracle. Correctness holds since P outputs

$$\sum_{i \leq j} a_{i,j} a_{j,i} + r_{i,j} + r_{j,i} = \sum_{i \leq j} a_{i,j} a_{j,i}.$$

For privacy, we describe a simulator for a subset $T \subset [n]$ as follows. If $P \notin T$, the view of the parties in T consists only of their inputs and their local randomness, and so it can be trivially simulated. If $P \in T$ we use the following simulator. Given the output y, and inputs/random tapes for the parties in T, the simulator defines the output, $y_{i,j}$, $\forall i \leq j \in [n]$, of the (i,j)th call to the TOT functionality as follows. If $i, j \in T$, the simulator computes $y_{i,j}$ as in the protocol based on the inputs and random tapes of P_i and P_j. Otherwise, the simulator samples a random $y_{i,j} \leftarrow \{0,1\}$ subject to the constraint that $\sum_{i,j} y_{i,j} = y$.

To analyze the simulator, let us assume, wlog, that the set of honest parties $[n] \setminus T$ contains exactly the first k parties $P_1, \ldots, P_k$. Fix some input to all parties, and random tapes for the parties in T, and assume that the output of F_1 is y. For $i \leq j \in [n]$, denote by $y_{i,j}$, the random variable that describes the output of the (i,j)th TOT call in the protocol. Since $(y_{i,j})_{i,j \in T}$ is computed just like in the simulation, it suffices to show that the vector

$$((y_{1,j})_{1 \leq j \leq n}, (y_{2,j})_{2 \leq j \leq n}, \ldots, (y_{k,j})_{k \leq j \leq n}) \tag{4}$$

is uniformly distributed subject to $\sum_{i \leq j} y_{i,j} = y$. Since the latter equality always holds (as shown by the correctness analysis) it suffices to show that the vector (4) with its last entry omitted,

$$Y = ((y_{1,j})_{1 \leq j \leq n}, (y_{2,j})_{2 \leq j \leq n}, \ldots, (y_{k,j})_{k \leq j \leq n-1}),$$

is uniform. Fix the random tapes of the parties in T and observe that each entry $y_{i,j}$ of Y can be written as the sum of some value z and some unique independent random bit $r_{i',j'}$. Specifically, for $i < k$ and $j \neq k$, we set (i', j') to (i, j). For $i < k$ and $j = k$ we set (i', j') to

(j,i). Finally, for $i=k$ and every $j \in [k, n-1]$, we set (i',j') to (i,j). We therefore defined a 1-1 mapping from the random bits

$$R = \left((r_{i,j})_{i\in[k-1],j\in[i,k-1]}, \quad (r_{k,j})_{j\in[n-1]}\right)$$

to the vector Y. (Here the notation $[a,b]$ stands for all the integers i for which $a \leq i \leq b$ and the notation $[b]$ stands for the interval $[1,b]$.) The claim follows since the vector R is uniformly distributed. This is true even though, for every i, the vector $(r_{i,1},\ldots,r_{i,n})$ was chosen subject to $\sum_j r_{i,j} = 0$; indeed, for every i, there exists at least a single j for which the random variable $r_{i,j}$ does not appear in R.

5 New 2MPRE Construction

In this section we present our main construction and prove Theorem 2.1.

5.1 2MPREs for 3-party functionalities

We begin with the following simple observation that deals with a degree-3 function whose output is delivered to one of the parties who owns one of the multiplicands as an input.

Claim 5.1. *The Boolean n-party functionality*

$$f\left((x_1,y_1),(x_2,y_2),(x_3,y_3),y_4,\ldots,y_n\right) = \left(x_1x_2x_3 + \sum_{i=1}^{n} y_i, \perp, \ldots, \perp\right)$$

(where additions and multiplications are in $\mathbb{F}_2$) that delivers the output to P_1 admits a 2MPRE with perfect correctness and perfect privacy against arbitrary coalitions.

Proof. The MPRE $\widehat{f}$ employs private randomness r that is sampled internally by the functionality. (By Proposition A.4,one can always replace it by the sum $\sum r_i$ where r_i is sampled locally by P_i.) The output of $\widehat{f}$ is delivered to P_1 and it consists of two entries:

$$\left(x_1 r + \sum_i y_i, \quad (1-x_1)r + x_2x_3 + \sum_i y_i\right).$$

Given the output (z_0,z_1), party P_1 decodes the value of f by outputting z_{x_1}. Indeed, if $x_1 = 0$ then the output z_0 is $\sum_i y_i$ and if $x_1 = 1$ then the output z_1 is $x_2x_3 + \sum_i y_i$, as required. To prove privacy, consider a set of corrupted parties $T \subsetneq [n]$ and assume that $P_1 \in T$ (the other case is trivial). Given the output y, the inputs x_1, y_1 and possibly the inputs of other parties, the simulator samples a random bit b and outputs the value (z_0,z_1) where $z_{x_1} = y$ and $z_{1-x_1} = b$. It is not hard to verify that this is a perfect simulator. □

As an immediate corollary we derive the following theorem which implies Corollary 2.2.

Theorem 5.2 (Corollary 2.2 restated)**.** *Every 3-party functionality f admits a 2MPRE with perfect correctness and perfect privacy against arbitrary coalitions.*

Proof. By the completeness of degree-3 REs [29], f can be perfectly encoded by a degree-3 RE f' where each of its outputs is of the form $x_1x_2x_3 + r_1 + r_2 + r_3$ where x_i is an input of P_i and r_i is a linear combination of the random inputs of P_i. Therefore, by composition (Lemma A.5),the theorem follows from Claim 5.1. □

Remark 5.3 (Arithmetic extension of Theorem 5.2)**.** *The MPRE of Claim 5.1 can be generalized to work over an arbitrary finite field $\mathbb{F}$. Indeed, if we treat the functionality f from Claim 5.1 as defined over $\mathbb{F}$, then we can construct an MPRE as follows. Sample internally $|\mathbb{F}|$ random elements $(r_c)_{c\in\mathbb{F}}$ from $\mathbb{F}$ and send to P_1 the vector $(z_c)_{c\in\mathbb{F}}$ where*

$$z_c = (x_c - c)r_c + c \cdot x_2 \cdot x_3 + \sum_i y_i.$$

The analysis is similar to the one presented in Theorem 5.2. A similar arithmetic extension applies to essentially all the results in this paper.

5.2 $\left\lfloor \frac{2n}{3} \right\rfloor$-private 2MPRE

Theorem 5.4 (Theorem 2.1 restated)**.** *Let n and t be positive integers for which $t < \frac{2n+1}{3}$. Then, every n-party functionality admits a t-private 2MPRE.*

Unfortunately, the complexity of the resulting MPRE is exponential in n. (This is the only result in this paper that suffers from this drawback.) However, by Theorem A.7, one can derive an efficient poly(n)-time version of the 2MPRE at the expense of reducing the privacy threshold to $\frac{2}{3} - \epsilon$ for an arbitrary small constant $\epsilon > 0$. (In fact, we can even take $\epsilon = o_n(1)$ by using Remark A.8.)

Proof. Consider the n-party functionality f that takes a pair of bits (a, α) from P_1, (b, β) from P_2 and (c, γ) from P_3 and delivers the value

$$abc + \alpha + \beta + \gamma$$

to some designated receiver $R \in \{ P_1, \ldots, P_n \}$. Since this functionality is known to be complete under non-interactive reductions [29, 2, 12] (for an arbitrary privacy threshold), it suffices to focus on f. Observe that if $R \in \{ P_1, P_2, P_3 \}$ the theorem follows from Claim 5.1, hence we will focus on the case where $R \notin \{ P_1, P_2, P_3 \}$. For concreteness, set $R = P_n$.

We will construct a t-perfect 2-round protocol π for f whose first round makes use of only private point-to-point channels and its second round makes parallel calls to TOT. By Lemma 4.2, such a protocol can be compiled back into an MPRE with an effective degree of 2.

Before presenting the protocol π, let us start with the following simple protocol π_0:

- At the first round, P_1 shares its input a via a t-private CNF secret sharing among the parties $\mathcal{P}$. That is, for each t-subset $S \subset \mathcal{P}$, party P_1 samples a random bit a_S conditioned on $a = \sum_S a_S$ and delivers a_S to all the parties $P_i, i \notin S$. Similarly, P_2 shares b into $b = \sum_{T \subset \mathcal{P}, |T|=t} b_T$ and sends b_T to every party $P_i, i \notin T$ and P_3 shares c into $c = \sum_{U \subset \mathcal{P}, |U|=t} c_U$ and sends c_U to every party $P_i, i \notin U$.

- At the second round, the parties make a call to an ideal functionality g that delivers the value

$$\left(\sum_{S \subset \mathcal{P}, |S|=t} a_S\right) \cdot \left(\sum_{T \subset \mathcal{P}, |T|=t} b_T\right) \cdot \left(\sum_{U \subset \mathcal{P}, |U|=t} c_U\right) + \alpha + \beta + \gamma$$

  to P_n.

It is not hard to verify that the protocol π_0 achieves perfect correctness and perfect t-privacy.

Our next protocol, π_1 is obtained by replacing the call to g by a call to a perfect MPRE for g (with full privacy) and by letting P_n apply the MPRE decoder. Specifically, the MPRE $\widehat{g}$ is defined via

$$(a_S \cdot b_T \cdot c_U + r_{S,T,U})_{S,T,U}\,, \qquad \alpha + \beta + \gamma - \sum_{S,T,U} r_{S,T,U},$$

where S, T, U range over all t-subsets of $\mathcal{P}$, and where each random bit $r_{S,T,U}$ is taken to the sum of random bits $r_{S,T,U,1}, \ldots, r_{S,T,U,n}$ that are sampled locally by $P_1, \ldots, P_n$, respectively. By Proposition A.3,the privacy and correctness of π_1 are inherited from π_0.

Next, we claim that each output of $\widehat{g}$ can be perfectly encoded by a functionality of effective degree-2 (with full privacy). Fix some S, T and U, and let us focus on the output $y = a_S \cdot b_T \cdot c_U + r_{S,T,U}$. Define the complement sets by

$$\overline{S} := \mathcal{P} \setminus S, \qquad \overline{T} := \mathcal{P} \setminus T, \qquad \overline{U} := \mathcal{P} \setminus U,$$

and let $V = \overline{S} \cup \overline{T} \cup \overline{U}$. Recall that a_S (resp., b_T, c_U) is known to all the parties in $\overline{S}$ (resp., $\overline{T}, \overline{U}$). We distinguish between two cases.

If $P_n \in V$, then the output y can be perfectly encoded by an MPRE of effective degree 2 by Claim 5.1. Next, suppose that $P_n \notin V$. We claim that in this case there must exist a party that owns at least 2 out of the 3 elements a_S, b_T, c_U, and so the effective degree is 2. Indeed, assume towards a contradiction, that such a party does not exist. That is, the sets $\overline{S}, \overline{T}, \overline{U}$ are pairwise disjoint. Since $|\overline{S}| = |\overline{T}| = |\overline{U}| = (n-t)$, it follows that $|V| = 3(n-t)$. Since $t < \frac{2n+1}{3}$, $|V| > n-1$. But $V \subset \{P_1, \ldots, P_{n-1}\}$ and so $|V| \leq n-1$, a contradiction.

Overall, the second round of π_1 can be realized by a call to a functionality $\widehat{g}$ of effective degree 2. Hence, by Claim 4.1, the second round can be replaced by parallel calls to TOT, and by Lemma 4.2, the resulting protocol can be compiled back into an MPRE with an effective degree of 2, as required. □

6 2MPREs vs. 2-round-OT-hybrid Model

The equivalence between t-private 2MPREs and the completeness of 3-party functionalities under non-interactive t-private reductions follows from Corollary 2.2 and Claim 4.1. In this section we establish an equivalence between 2MPREs and 3-round protocols in the 2-round-OT-hybrid Model. Recall that in the 2-round OT hybrid model we assume that OT takes 2 rounds. That is, if both parties send their inputs to an OT in round i, the output is delivered to the receiver at the *end* of round $i+1$. In addition, the parties are allowed to exchange messages via standard point-to-point private channels.

Remark 6.1 (On the 2-round-OT-hybrid Model)**.** *The 2-round-OT-hybrid Model attempts to capture an information-theoretic reduction to OT with the minimal possible interaction. (Recall that a single-round reduction in which the parties exchange messages over private channels and make parallel calls to OT was shown to be impossible in [3].) A natural suggestion is to consider a 2-round reduction that is allowed to make oracle calls to OT. However, this allows the reduction to make calls to OT both in the first round and in the second round, which leads to an actual round complexity of 4 when the OT is realized via a 2-round protocol. Our refined notion of 2-round-OT-hybrid Model is therefore stronger than 2-round reduction to OT. One could also consider a seemingly stronger model in which the reduction has 2 rounds but only the first round is allowed to make calls to an ideal OT. Our theorem shows that such a 2-round "OT-then-plain" reduction is actually equivalent to the 2-round-OT-hybrid Model.*

Theorem 6.2. *The following holds for every n-party functionality f and every privacy threshold $1 \leq t \leq n$. The functionality f can be t-privately computed by a 3-round protocol π in the 2-round OT hybrid model if and only if it has a t-private 2MPRE. Furthermore, for the "if" direction the resulting protocol makes OT calls only at the first round and no private messages are exchanged in the second round and so derive a 2-round "OT-then-plain" reduction. The transformation preserves the privacy and correctness errors.*

The "only if" direction establishes the second item of Theorem 2.3 (whose first item follows from Corollary 2.2.)

Proof. We begin with the easy "if" direction. It suffices to realize the TOT functionality with a 2-round protocol π' in the OT-hybrid model with perfect correctness and perfect privacy against any coalition, in which only the first round consists of OT calls. Consider a TOT between the parties, Alice, Bob and Carol, where Alice holds the inputs (x_1, y_1), Bob holds the inputs (x_2, y_2), and Carol should receive $z = x_1x_2 + y_1 + y_2$. The protocol proceeds as follows:

1. (Round 1) Alice samples a random bit α, she sends to Carol the value $a = y_1 - \alpha$ and initiates an OT with Bob.[9] In this invocation, Alice plays the Sender with inputs $(\alpha, x_1 + \alpha)$ and Bob uses x_2 as the selection bit.

[9]Despite the equivalence of addition and subtraction over the binary field, we use both signs to indicate that the construction generalizes to general fields.

2. (Round 3) Given the output $m = x_1x_2 + \alpha$ of the OT, Bob sends to Carol the value $b = m + y_2$.

3. (Output) Carol outputs the sum $a + b$.

Clearly, the protocol can be realized in 3 rounds in the 2-round OT-hybrid model (or, more generally in $k+1$ rounds given a k-round OT). Correctness can be easily verified. For privacy, consider any coalition that contains Carol and either Alice or Bob (all other cases are trivial). Given $z = x_1x_2 + y_1 + y_2$, sample a random bit a and set Carol's view to $(a, b = z - a)$. A corrupted Alice adds nothing to the view (except for her inputs). If Bob is corrupted, then we are also given the inputs (x_2, y_2) and we can simulate m by $b - y_2$. It is not hard to verify that the simulation is perfect.

We move on to prove the more interesting "only if" direction. We show that any 3-round protocol in the 2-round OT-hybrid model can be transformed into a protocol in which the party first exchanges private messages and then makes parallel calls to 3-party functionalities. These functionalities can be replaced by 2MPREs (based on Corollary 2.2) and the resulting 2-round protocol can be compiled into a 2MPRE via the aid of the round-collapsing lemma (Lemma 4.2). Details follow.

Consider the protocol π. For any round number $1 \leq R \leq 3$ and parties P_i, P_j, let $m^R_{i,j}$ be the private message sent from P_i to P_j on round R. Without loss of generality, we further assume that in each round each party P_i sends to herself her entire private view, including the input x_i and the private random tape ρ_i. Since the protocol has only 3 rounds and the OT takes 2 rounds, we may assume that OT calls are performed either on the first round or on the second round. Let us further assume that, both in round 1 and in round 2, each pair of parties (P_i, P_j) performs exactly ℓ OT-calls in which P_i is the sender and P_j is the receiver. Denote by $o^2_{i,j} = (o^2_{i,j,1}, \ldots, o^2_{i,j,\ell})$ and $o^3_{i,j} = (o^3_{i,j,1}, \ldots, o^3_{i,j,\ell})$ the vector of OT-outputs of the first-round calls and the second-round calls, respectively. Observe that $o^R_{i,j}$ arrives at the end of round R. For every round $R \in [3]$ and party i, let

$$m^R_i = \left(m^R_{1,i}, \ldots, m^1_{n,i}\right) \quad \text{and} \quad o^R_i = \left(o^R_{1,i}, \ldots, o^R_{n,i}\right).$$

By definition, for $R \in [3]$ and $i, j \in [n]$ there exist functions $f^R_{i,j}, g^R_{i,j}$ such that

$$\begin{aligned}
m^1_{i,j} &= f^1_{i,j}(x_j, \rho_i), \\
m^2_{i,j} &= f^2_{i,j}\left(m^1_i\right), & o^2_{i,j} &= g^2_{i,j}\left(m^1_{i,i}, m^1_{j,j}\right), \\
m^3_{i,j} &= f^3_{i,j}\left(m^2_i, o^2_i\right), & o^3_{i,j} &= g^3_{i,j}\left(m^1_i, m^1_j\right).
\end{aligned}$$

Note that the g functions "merge" together the OT computation with the local computation that is being used in order to generate the input to the OT. To prove the lemma it suffices to securely compute each of these values by a non-interactive TOT-hybrid protocol with perfect correctness and perfect privacy against an arbitrary coalition. In fact, by Lemma 4.2, it suffices to obtain a 2-round protocol π' that makes TOT calls only in the second round. First observe that the values $m^1_{i,j}, m^2_{i,j}$ can be easily computed by a 2-round protocol via private point-point channels in which $m^2_{i,j}$ can be transferred using a TOT call in the round

2. Moreover, since the messages $o^2_{i,j} = g^2_{i,j}\left(m^1_{ii}, m^1_{jj}\right)$ and $o^3_{i,j} = g^3_{i,j}\left(m^1_i, m^1_j\right)$ depend only on values that are known to P_i and P_j after the first round, we can use Observation 3.4, and deliver them to P_j by making parallel calls to TOT in the second round (where P_i is the sender and P_j is the selector and receiver). It is left to deliver the value $m^3_{i,j}$.

Fix some $i, j \in [n]$, and let $\widehat{f}$ be a fully decomposable RE of $f^3_{i,j}$, e.g., from [2]. Observe that it suffices to deliver the value of $\widehat{f}(m^2_i, o^2_i; w)$ to P_j where the randomness w is chosen *solely* by P_i. (Indeed, privacy for coalitions that do not contain P_i follows from the RE privacy and privacy for coalitions that contain P_i vacuously holds, since m^2_i and o^2_i are given to the simulator.) Being fully-decomposable, each output of $\widehat{f}$ depends on the randomness w, selected by P_i, and on at most a single input bit y of m^2_i or o^2_i. Thus, after some reordering of the outputs, we can write $\widehat{f}(m^2_i, o^2_i; w)$ as

$$\widehat{f}_1(m^2_{1,i}, o^2_{1,i}, w), \ldots, \widehat{f}_n(m^2_{n,i}, o^2_{n,i}, w)$$

where the functions $\widehat{f}_1, \ldots, \widehat{f}_n$ are multi-output functions. Note that $o^2_{k,i}$ itself is the result of $g^2_{k,i}(m^1_{k,k}, m^1_{i,i})$. Therefore there exist functions $h_1, \ldots, h_n$ such that for all $k \in [n]$ we can write $\widehat{f}_k(m^2_{k,i}, o^2_{k,i}, w) = h_k(m^1_{k,i}, m^1_{k,k}, m^1_{i,i}, w)$. Since the input to h_k is being held by only two parties, P_i and P_j, and is available at the end of the first round, it can be encoded by a 2MPRE (Observation 3.4). It follows, by Claim 4.1, that h_k can be computed by making parallel calls to TOT at the second round. The theorem follows. □

7 2MPREs vs Perfect Privacy under Active Attacks

In this section we will prove Theorem 2.6. Most of the work will be devoted to the construction of 2MPREs, the converse direction will be proved in Section 7.3. Along the way, we will also prove Theorem 2.7.

Recall that a public-output functionality is a function that delivers the same output to all the parties. We begin with the following basic construction.

Construction 7.1. *Let π be a protocol that realizes some Boolean public-output functionality $f(x_1, \ldots, x_n)$. The protocol π may have an arbitrary number of rounds, and may use OT calls as well as private channels. We construct a non-interactive protocol σ that realizes f and makes use of an ideal functionality V as follows.*

1. *(Local pre-computation) First, each party P_i uniformly samples a local view of π. That is, P_i samples a private random tape r_i, and randomly "guesses" a vector of incoming private messages, and a vector of incoming OT messages corresponding to all the OT calls in which P_i plays the receiver. Then, P_i appends her input x_i to the sampled view, and computes the corresponding outgoing messages that she would send in π either over private channels or as inputs to the OT functionality.*

2. *(Calling V) The parties send their sampled views and the computed outgoing messages to an ideal functionality V. We further assume that P_1 sends to V her final π-output.*

The functionality V verifies that for every pair of parties, (P_i, P_j), the sampled views are consistent *in the following sense:*

- *For every message m that is delivered from P_i to P_j it holds that the guess of P_j for m is equal to the value of the outgoing message m as computed by P_i.*
- *For every OT-call in which the sender P_i computes her inputs as (a_0, a_1) and the receiver P_j computes her input as s, it holds that the value a' that is guessed by the receiver equals to a_0 if $s = 0$ and to a_1 if $s = 1$.*

If all these pair-wise tests succeed and P_1's output is 1, the functionality V outputs 1 *to all the parties. Else, it outputs* 0*.*

3. *(Output) The parties terminate with the output that V passes.*

Lemma 7.2. *If π realizes f with perfect correctness, perfect privacy against a coalition T, and a total communication of c bits (where each OT call is counted as a single bit), then the protocol σ defined in Construction 7.1 realizes f with perfect privacy against T, and a 1-sided correctness error of $1 - 2^{-c}$.*

Proof. Fix an input $x = (x_1, \ldots, x_n)$ for f. It is not hard to see that if $f(x) = 0$, the protocol σ always outputs 0. On the other hand, when $f(x) = 1$ the protocol σ outputs the correct result only when the sampled views are consistent. Fix the local random tapes $r = (r_1, \ldots, r_n)$ in π. Under this fixing, all the communication in a real execution of π is fully determined, and can be represented by a *transcript string* $C_{x,r} \in \{0,1\}^c$ whose ith bit corresponds to the ith bit that is delivered in π from party $A = A(i)$ to party $B = B(i)$ either via OT or via a private channel. (We assume, wlog, that the communication in π is ordered in some canonical way). Since each bit of communication is being guessed by the receiving party uniformly and independently, the parties submit the consistent transcript $C_{x,r}$ with probability exactly 2^{-c}.

We move on to privacy. Fix some coalition T. Syntactically, the view of T in π consists of the input $x_T = (x_i)_{i \in T}$ the local random tapes $r_T = (r_i)_{i \in T}$ and all the incoming messages that a party in T receives. Let I_T denote the set of all indices $i \in [c]$, such that the ith message in π is received by a party in T. Given a full transcript $C \in \{0,1\}^c$, we denote by $C[I_T]$ the restriction of C to the messages that are delivered to members in the coalition T. For convenience, let us further assume that the final output of the protocol, y, appears as part of the view. Similarly, the view of T in σ consists of $(x_T, r_T, C'[I_T], v)$ where $C'[I_T]$ are the *guessed* incoming messages, and v is the bit that V delivers.

Consider the following randomized mapping g that maps a T-view $(x_T, r_T, C[I_T], y)$ under π to a T-view $(x_T, r_T, C'[I_T], v)$ under σ: First, uniformly sample a sequence $e = (e_1, \ldots, e_c)$ of random bits (where $e_i = 1$ indicates an "incorrect" guess for the ith bit in the full transcript). Then, copy $C[T]$ to $C'[T]$ and flip the value of the ith entry if $i \in I_T$ and $e_i = 1$. Finally, set v to zero if some e_i is‘ one, and otherwise set $v = y$.

We can define a simulator Sim' for σ as follows. Given x_T and an output y, use the simulator Sim of π to sample a view $(x_T, r_T, C[I_T], y)$ under π, apply the mapping g and

output the resulting σ view $(x_T, r_T, C'[I_T], v)$. To analyze the simulator, fix an input x to all the parties. By the privacy of π, the distribution generated by $\mathsf{Sim}'(x_T, f(x))$ is identically distributed to the distribution $g(x_T, r_T, C_{x,r}[I_T], f(x))$ where $C_{x,r}[I_T]$ is the vector of incoming messages to T in a *real execution* of π over the input x and fresh randomness $r = (r_1, \ldots, r_n)$, and $r_T = (r_i)_{i \in T}$.

We complete the argument by showing that $g(x_T, r_T, C_{x,r}[I_T], f(x))$ is distributed identically to the real execution of σ. We prove that this is the case for every fixing of r. Indeed, in σ the entire vector of guesses $C' \in \{0,1\}^c$ is chosen uniformly at random, and the coalition T receives the restricted transcript $C'[I_T]$ together with a bit v which is equal to 0 if $C' \neq C_{x,r}$ and to $f(x)$ otherwise. Equivalently, we could sample an error vector $e \leftarrow \{0,1\}^c$, set $C' = C_{x,r} \oplus e$ and deliver to T the restricted vector $C'[I_T]$ with the bit v which is set to 0 if some bit of e is 1, and otherwise takes the value $f(x)$. The resulting distribution is exactly the one that is sampled by g. The lemma follows. □

Remark 7.3 (Handling protocols with imperfect correctness)**.** *One can use a variant of Construction 7.1 in which V outputs an additional consistency bit b that indicates whether the views were consistent. (Our simulator can simulate this additional information.) At the post-processing stage, the parties output a special "I do not know", $\perp$, symbol when $b = 0$ and otherwise output the main output v of V. Assuming that the original protocol π is perfectly correct, the resulting protocol never errs and outputs a non-$\perp$ symbol with probability 2^{-c}.*

This variant also allows us to handle protocols that have imperfect correctness. Specifically, if the original protocol π suffers from some correctness error of $\delta < 0.5$ we get a protocol with similar correctness error (conditioned on not outputting $\perp$). Such an error can be reduced to an arbitrary ϵ by taking a majority vote over $k = O(\log(1/\epsilon)2^c/(1-2\delta))$ independent parallel copies of the new protocol. This new protocol σ_k is syntactically similar to σ except that it makes k calls to (the extended version of) V. This allows us to extend the above lemma (and all the subsequent results) to the case where π has a correctness error of $\delta < 0.5$. For simplicity, we omit these extensions from the current version.

7.1 2MPRE for protocols without OT calls

Observation 7.4. *If π does not use OT calls then the functionality V can be written as $\bigwedge_{i,j \in [n]} z_{i,j}$ where $z_{i,j}$ is computed by taking the equality between a string $a_{i,j}$, computed locally by P_i, and a string $b_{i,j}$ computed locally by P_j. The length of $a_{i,j}$ and $b_{i,j}$ equals to the number of bits that P_i delivers to P_j in π.*

Indeed, $a_{i,j}$ is the vector of messages that P_i should deliver to P_j according to her local computation (under the sampled view) and $b_{i,j}$ is vector of incoming messages that P_j receives from P_i according to her guesses.

Corollary 7.5 (Theorem 2.7 restated)**.** *In the honest majority setting, every n-party functionality f non-interactively reduces to multiple parallel calls to $\mathsf{AND} \circ \mathsf{EQ}$ functionality. The reduction has perfect privacy and an arbitrarily small 1-sided statistical correctness error of ϵ. The complexity of the protocol is $O(\log(m/\epsilon))$ where m is the number of outputs of f and the hidden constant in the O-notation depends on the complexity of f.*

Proof. Every n-party functionality f has a protocol in the plain model (i.e. does not use OT calls) that is perfectly correct and perfectly $\lfloor \frac{n-1}{2} \rfloor$-private [10]. Assuming that f is a Boolean public-output functionality, we can use Lemma 7.2 and Observation 7.4 to non-interactively reduce f to $\mathsf{AND} \circ \mathsf{EQ}$ with perfect privacy and a constant 1-sided correctness error δ against minority coalitions. (The constant δ depends on the description of f.) We can reduce the error to ϵ' by executing the reduction $\ell = O(\frac{\log(1/\epsilon')}{1-\delta})$ times in parallel and outputting 1 if and only if at least one of these executions outputs 1. (The latter step is computed locally, i.e., by the decoder). Since σ has perfect privacy, repeating it in parallel does not affect privacy. Finally, since every m-output functionality non-interactively reduces to m parallel calls to Boolean public-output functionalities, the statement extends to such functionalities as well, while the error grows to $\epsilon = m\epsilon'$ where m is the number of outputs. □

Remark 7.6 (The complexity of the construction)**.** *Recall that every n-party multi-output functionality f that is computable by s-size formula (or even s-size branching program) non-interactively n-privately reduces to a functionality g with* $\mathrm{poly}(s)$ *outputs and each of its output is a constant-size deterministic public-output functionality (that takes a constant number of input bits from a constant number of parties) [29, 2, 3]. Therefore, by Corollary 7.5, f reduces to* $\mathrm{poly}(s)\log(1/\epsilon)$ *calls to* $\mathsf{AND} \circ \mathsf{EQ}$ *over constant fan-in.*

Observe that the equality function over k-bit strings, $\mathsf{EQ}(x, y)$ can be written as a linear function $L(x, y) = (x_i - y_i + 1)_{i\in[k]}$ over an arbitrary finite field $\mathbb{F}$ such that $L(x, y) = 1^k$ iff $x = y$. In addition, the AND predicate admits a degree-2 statistical randomized encoding as follows.

Fact 7.7 (Encoding AND by Inner-Products [29])**.** *Fix an arbitrary finite field $\mathbb{F}$. Let $v = (v_1, \ldots, v_\ell)$ be a vector of 0-1 values. Consider the randomized function*

$$g(v; \rho) := \sum_{i\in[\ell]} \rho_i \cdot (1 - v_i),$$

where $\rho \leftarrow \mathbb{F}^\ell$ and the addition and multiplication are taken over $\mathbb{F}$. Then, g is a randomized encoding of $\bigwedge_{i\in[\ell]} v_i$ with perfect privacy and correctness error of $1/|\mathbb{F}|$. When all v_is are 1, we get 0 from g. So the output is decoded as (a) 1 when g outputs 0 and (b) 0 otherwise. Note that when we output 0, this is always correct. But when we output 1, it may not be correct, since the sum of ρ_i's can lead to zero. Since the sum is random, the probability that it can be 0 is $1/|\mathbb{F}|$. Lastly, in this case g is a degree-2 function over the binary field. By default, we let $\mathbb{F}$ be a binary extension field. In this case, g can be written as a degree-2 function over the binary field, and it can be computed by a Boolean circuit of size $\ell \log |\mathbb{F}|$. Unless stated otherwise, we assume that $\mathbb{F}$ is the field of size $2^{\ell+1}$.[10]

It follows that $\mathsf{AND} \circ \mathsf{EQ}$ reduces non-interactively to a degree-2 functionality (with statistical correctness error) and so Corollary 7.5 yields a new alternative construction of honest-majority 2MPRE, alas with statistical correctness.

[10] Alternatively, one can instantiate g over the binary field, and reduce the error to ϵ by repeating the encoding $\log(1/\epsilon)$ times with fresh independent randomness. See [29].

7.2 2MPRE for protocols with OT calls

Note that when the underlying protocol is the OT-hybrid channel, the functionality (also a predicate) V has a slightly more complicated form. In particular, it computes an AND over degree-2 functions. As a result, we cannot use Fact 7.7 directly to derive a 2MPRE. We bypass the problem by letting the pair of parties that use the ith OT call, to locally select the ith randomizer ρ_i of the AND in the inner-product based RE of Fact 7.7. (Note that previously we treated the randomizers as being part of the internal randomness of the MPRE.) Unfortunately, this leads to a "leaky" 2MPRE of V. We show that this leakage can still be simulated if the original protocol π is weakly-active private. Details follow.

Definition 7.8 (Weakly-active adversaries)**.** *Let π be an n-party protocol in the OT-hybrid model. A* weakly-active *adversary $\mathcal{A}$ that corrupts a subset T is defined by deviating from the protocol π as follows. For every OT-call between two* corrupted *parties, a sender S with values $(a_0, a_1) \in \{0,1\}^2$ and a receiver R with selector bit $s \in \{0,1\}$, the adversary sets the received value to be some fixed value $a' \in \{0,1\}$. After these modifications, the adversary honestly follows the protocol where a' is used as the received value of the OT instance with inputs (a_0, a_1) and s. Such a deviation can be fully specified by a vector $a' = (a'_i)_{i \in O_T}$ where $i \in O_T$ if the ith bit that is exchanged in π is delivered via an OT between 2 corrupted parties. We write $\pi_{a'}$ to denote the protocol that is obtained for a given fixing of a'.*

A protocol π in the OT-hybrid model computes a (deterministic) functionality f with t-perfect privacy against weakly-active adversaries *if for every t-bounded subset T, and every vector $a' = (a'_i)_{i \in O_T}$, it holds that*

$$\mathsf{Sim}(T, a', x_T, f_T(x)) \equiv \mathsf{View}_{T,\pi_{a'}}(x, r),$$

where $r = (r_1, \ldots, r_n)$ are chosen uniformly at random and $\mathsf{View}_{T,\pi_{a'}}(x, r)$ denotes the view of coalition T when running the protocol $\pi_{a'}$ with input $x = (x_1, \ldots, x_n)$ and randomness $r = (r_1, \ldots, r_n)$.

We also require either statistical or perfect correctness against a passive adversary, i.e.,

$$\Pr_{r_1,\ldots,r_n}[\pi(x_1, \ldots, x_n; r_1, \ldots, r_n) \neq f(x_1, \ldots, x_n)] \leq \delta,$$

where r_i is the randomness used by the ith party in π.

A leaky version of Construction 7.1. Before introducing the leaky 2MPRE of V, it will be useful to consider an intermediate case where V itself is leaky. Let $\widetilde{V}$ denote the corruption-aware predicate that takes the same input as V in Construction 7.1, delivers the same output as V to all the honest parties, but leaks some additional information to the adversary. Specifically, $\widetilde{V}$ leaks to the adversary the consistency bit that verifies consistency of the transcript without taking into account the OT-messages that are exchanged between pairs of corrupted parties. Formally, for a set of corrupted parties $T \subset [n]$, the functionality $\widetilde{V}$ is defined as follows.

- Input: For each index $i \in [c]$, (a) if the ith bit in π is a private-channel message from a sender $A(i)$ to a receiver $B(i)$, then $\widetilde{V}$ receives a bit m_i from $A(i)$ and m'_i from $B(i)$; (b) if the ith bit in π is transferred over an OT-channel then $\widetilde{V}$ receives $(a_{i,0}, a_{i,1})$ from the sender $A(i)$ and (s_i, a'_i) from the receiver $B(i)$. In addition, the functionality $\widetilde{V}$ receives from the first party P_1 her output v_{c+1} (computed based on her guesses).

- Output: The parties receive the output

$$V = \bigwedge_{i \in [c+1]} v_i$$

where for v_i is defined as follows. If the ith communication bit of π is delivered over a private-channel then $v_i = 1$ if and only if $m_i = m'_i$. If the ith communication bit of π is delivered over an OT-channel then $v_i = 1$ if and only if $a'_i = s_i \cdot a_{i,1} + (1 - s_i) \cdot a_{i,0}$. Lastly, recall that $v_{c+1} = 1$ if and only if the output of P_1 is 1. In addition, the adversary receives the value

$$V_T = \bigwedge_{i \notin O_T} v_i$$

where $i \in O_T$ if the ith communication bit in π is an OT-message that is delivered between a pair of corrupted parties $A(i), B(i) \in T$.

Claim 7.9. *Suppose that π realizes f with perfect passive correctness and t-perfect privacy against weakly-active adversaries. Let $\tilde{\sigma}$ denote the protocol that is obtained by instantiating Construction 7.1 with the functionality (predicate) $\widetilde{V}$ instead of V. Then, $\tilde{\sigma}$ realizes f with perfect t-privacy and 1-sided correctness error of $1 - 2^{-c}$.*

Proof. The proof of correctness is identical to the proof of Lemma 7.2. We move on to prove privacy. Fix a t-bounded corrupted coalition $T \subseteq [n]$. For each index $i \in O_T$, sample a random received bit a'_i, and consider the weakly-corrupted protocol $\pi_{a'}$ where $a' = (a'_i)_{i \in O_T}$. Observe that the output V_T given by the "leaky" functionality $\widetilde{V}$ to the adversary in $\tilde{\sigma}$ corresponds to the non-leaky value that is delivered by V in σ when the underlying protocol is $\pi_{a'}$. Now by Lemma 7.2, since we can perfectly simulate the view of T in $\pi_{a'}$ (due to the security of π against a weak-active), we can also simulate the view of T in $\tilde{\sigma}$. □

In order to obtain a 2MPRE we will need the following extension to the inner-product encoding from Fact 7.7.

Fact 7.10 (leaky inner products)**.** *Under the notation of Fact 7.7, the following holds. For every set $S \subseteq [\ell]$, let $\rho_S = (\rho_i)_{i \in S}$ and $v_S = (v_i)_{i \in S}$. There exists a simulator Sim_S that, for every $v \in \{0,1\}^\ell$, perfectly samples the distribution*

$$(g(v; \rho), \rho_S, v_S) \qquad \text{where } \rho \leftarrow \mathbb{F}^\ell$$

given ρ_S, v_S and $\bigwedge_{i \notin S} v_i$.

Lemma 7.11 (2MPRE from weak-active privacy)**.** *Suppose that the functionality f can be realized in the OT-hybrid model by a protocol π with t-perfect privacy against weakly-active adversaries and perfect passive correctness. Then f can be realized by t-private 2MPRE with an arbitrarily small correctness error of ϵ and with complexity of $\log(1/\epsilon)(n+T_\pi)2^{O(c)}$ where n is the number of parties and T_π is the computational complexity of π.*

Proof. Let f be a functionality that is realized by a protocol π in the OT-hybrid model that has perfect passive correctness and t-perfect privacy against weakly-active adversaries. From Claim 7.9, we get a non-interactive protocol $\tilde{\sigma}$ that makes use of the ideal functionality $\widetilde{V}$, and is perfectly t-private and has a 1-sided correctness error of $1-2^{-c}$, where c is the total number of bits of communication in π. Denote by M and O the set of indices that correspond to point-to-point messages and OT messages. That is, $i \in M$ (resp., $i \in O$) if the ith bit in π is a sent by party $A(i)$ to party $B(i)$ via a private channel (resp., over an OT-channel). We construct MPRE $\widehat{f}$ by modifying $\tilde{\sigma}$ as follows.

- Local preprocessing: Similarly to $\tilde{\sigma}$, the parties locally compute the values $(m_i, m'_i)_{i\in M}$ and $(a_{i,0}, a_{i,1}, s_i, a'_i)_{i\in O}$ and v_{c+1}. In addition, for every $i \in O$, the parties $A(i)$ and $B(i)$ randomly sample α_i and β_i respectively.
- The functionality outputs $g(v;\rho)$ where $v = (v_i)_{i\in[c+1]}$ is computed as in $\tilde{\sigma}$, for $i \in O$ the randomizer $\rho_i = \alpha_i + \beta_i$, and for $i \notin O$, the randomizer ρ_i is sampled uniformly at random internally by the functionality.
- Decoding: The parties decode g and output the result.

Before analyzing the correctness and privacy of $\widehat{f}$, we show that g has an effective degree of 2. Recall that g outputs the sum

$$Q_1 + \ldots + Q_{c+1} \quad \text{where } Q_i := \rho_i \cdot (1 - v_i) \quad \forall i \in [c+1].$$

We show that for every i, Q_i can be written as a degree-2 expression over some prepossessed inputs and the internal randomness of g.[11] Indeed, for $i = c+1$, this is trivial since v_{c+1} is given as an input to g; For $i \in M$ it holds that v_i is linear in m_i, m'_i, and so Q_i is quadratic in m_i, m'_i and the internal randomness ρ_i. For $i \in O$, both v_i and ρ_i depend on inputs that are delivered by $A(i)$ and $B(i)$, and so Q_i is a 2-input functionality, which can be written as a degree-2 function in the prepossessed inputs as shown in Observation 3.4. Specifically, since $v_i = 1 + a'_i - (s_i \cdot a_{i,1} + (1-s_i)\cdot a_{i,0})$ and $\rho_i = \alpha_i + \beta_i$ we can write Q_i as a quadratic expression in $a'_i, s_i, a_{i,1}, a_{i,0}, \alpha_i, \beta_i$ and in the pre-processed values $\alpha_i a_{i,0}, \alpha_i a_{i,1}$ and $s\beta_i$.

Next, we prove that $\widehat{f}$ achieves perfect t-privacy. Fix some t-bounded coalition T. Denote by $O_T \subset O$ the indices of the OT message that is sent between a pair of corrupted parties $A(i), B(i) \in T$. Our simulator, $\mathsf{Sim}(x_T)$, first applies the simulator $\mathsf{Sim}_{\tilde{\sigma}}(x_T)$ for $\tilde{\sigma}$ and

[11] The function g has degree-2 over $\mathbb{F}$. However, by taking $\mathbb{F}$ to be a binary extension field and by decomposing $\rho_i = (\rho_i[j])_j$ to bits, we can also write g as a vector of quadratic polynomials over the binary field.

gets a simulated $\tilde{\sigma}$-view that includes the local guesses, the final output V and a leaky output $V_T = \bigwedge_{i \notin O_T} v_i$. Based on the guesses of the parties in T, the simulator computes the consistency bits $v_{O_T} = (v_i)_{i \in O_T}$ of the corrupted OT's, and samples $(\rho_i)_{i \in O_T}$. Finally, the simulator samples the value of g using the leaky-RE simulator Sim_{O_T} applied to ρ_{O_T}, v_{O_T} and V_T. Since both, $\mathsf{Sim}_{\tilde{\sigma}}(x_T)$ and Sim_{O_T} are perfect, we get perfect simulation.

The correctness of $\widehat{f}$ follows from the correctness of $\tilde{\sigma}$ and the correctness of the MPRE in Fact 7.7. In more detail, if the output of f is 1, the protocol outputs 1 with probability exactly 2^{-c} (recall that when the AND evaluates to 1 the MPRE from Fact 7.7 does not err). When the function evaluates to 0 the output is 1 only if the MPRE errs. Let us set to error probability of the MPRE to $\epsilon_0 = 2^{-c}/2$. To reduce the error to ϵ, we can invoke $L = O(2^c \log(1/\epsilon))$ fresh copies of $\widehat{f}$ in parallel, and set the decoding to output 1 iff at least $\frac{3}{4}2^{-c}$-fraction of the executions output one. By a multiplicative Chernoff bound, an error occurs with probability of $\exp(-\Omega(L2^{-c})) = \epsilon$. The complexity of the protocol (without repetition) is similar to the complexity T_π of π plus the complexity of g which is $O(T_\pi + n2^c \log(1/\epsilon_0)) = O(T_\pi + n2^{2c})$, where n is the number of parties. Thus the overall complexity after repetition is $O((T_\pi + n2^{2c})L) = O((T_\pi + n2^{2c})2^c \log(1/\epsilon)$. □

7.3 2MPRE implies weak-active perfect privacy

We prove the converse of Theorem 2.6.

Lemma 7.12. *If the functionality f has t-private 2MPRE, then it can be realized in the OT-hybrid model with perfect (passive) correctness and t-perfect privacy against weakly active adversaries. The transformation carries to the statistical setting while preserving the error.*

Proof. Suppose that f has t-private 2MPRE. By Theorem 6.2, f can be computed by a protocol in which the result of OT messages only affect the last-round messages of the parties. This means that a deviation of a weakly-active adversary can only affect the view of an honest party after the last round of messages. Put differently, at the beginning of the last round the view of all honest parties is consistent with an honest execution of the protocol. Consequently, all the messages that are being sent to the adversary (including the last round messages) are consistent with an honest execution of the protocol, and so weak-active perfect privacy follows from passive perfect privacy, as required. □

Acknowledgements. B. Applebaum and O. Karni are supported by the Israel Science Foundation grant no. 2805/21. Y. Ishai is supported by ERC Project NTSC (742754), BSF grant 2018393, and ISF grant 2774/20. A. Patra is supported by DST National Mission on Interdisciplinary Cyber-Physical Systems (NM-CPS) 2020-2025 and SERB MATRICS (Theoretical Sciences) Grant 2020-2023.

References

[1] Bar Alon and Anat Paskin-Cherniavsky. On perfectly secure 2PC in the OT-hybrid model. *Theor. Comput. Sci.*, 891:166–188, 2021.

[2] B. Applebaum, Y. Ishai, and E. Kushilevitz. Cryptography in NC^0. In *45th Annual IEEE Symposium on Foundations of Computer Science*, pages 166–175, 2004.

[3] Benny Applebaum, Zvika Brakerski, Sanjam Garg, Yuval Ishai, and Akshayaram Srinivasan. Separating two-round secure computation from oblivious transfer. In *11th Innovations in Theoretical Computer Science Conference, ITCS*, volume 151 of *LIPIcs*, pages 71:1–71:18. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

[4] Benny Applebaum, Zvika Brakerski, and Rotem Tsabary. Perfect secure computation in two rounds. *SIAM J. Comput.*, 50(1):68–97, 2021.

[5] László Babai, Anna Gál, Peter G. Kimmel, and Satyanarayana V. Lokam. Communication complexity of simultaneous messages. *SIAM J. Comput.*, 33(1):137–166, 2003.

[6] Omer Barkol, Yuval Ishai, and Enav Weinreb. On d-multiplicative secret sharing. *J. Cryptol.*, 23(4):580–593, 2010.

[7] Donald Beaver. Precomputing oblivious transfer. In *Advances in Cryptology - CRYPTO '95, 15th Annual International Cryptology Conference, Santa Barbara, California, USA, August 27-31, 1995, Proceedings*, volume 963 of *Lecture Notes in Computer Science*, pages 97–109. Springer, 1995.

[8] Donald Beaver, Silvio Micali, and Phillip Rogaway. 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*, pages 503–513, 1990.

[9] Amos Beimel, Yuval Ishai, and Eyal Kushilevitz. General constructions for information-theoretic private information retrieval. *J. Comput. Syst. Sci.*, 71(2):213–247, 2005.

[10] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, page 1–10, 1988.

[11] Fabrice Benhamouda and Huijia Lin. k-round multiparty computation from k-round oblivious transfer via garbled interactive circuits. In *EUROCRYPT 2018*, pages 500–532, 2018.

[12] Elette Boyle, Niv Gilboa, Yuval Ishai, Huijia Lin, and Stefano Tessaro. Foundations of homomorphic secret sharing. In *ITCS 2018*, volume 94, pages 21:1–21:21.

[13] Gabriel Bracha. An asynchronou [(n-1)/3]-resilient consensus protocol. In *Proceedings of the Third Annual ACM Symposium on Principles of Distributed Computing, Vancouver, B. C., Canada, August 27-29, 1984*, pages 154–162, 1984.

[14] Ran Canetti. Security and composition of multiparty cryptographic protocols. *J. Cryptology*, 13(1):143–202, 2000.

[15] Ran Canetti. 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*, pages 136–145, 2001.

[16] Claude Crépeau. Efficient cryptographic protocols based on noisy channels. In *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*, pages 306–317. Springer, 1997.

[17] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *29th Annual Symposium on Foundations of Computer Science, White Plains, New York, USA, 24-26 October 1988*, pages 42–52. IEEE Computer Society, 1988.

[18] Ivan Damgård and Yuval Ishai. Constant-round multiparty computation using a black-box pseudorandom generator. In *CRYPTO 2005*, pages 378–394, 2005.

[19] Ivan Damgård, Yuval Ishai, Mikkel Krøigaard, Jesper Buus Nielsen, and Adam D. Smith. Scalable multiparty computation with nearly optimal work and resilience. In *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*, pages 241–261, 2008.

[20] Nico Döttling, Daniel Kraschewski, and Jörn Müller-Quade. Unconditional and composable security using a single stateful tamper-proof hardware token. In *Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011. Proceedings*, pages 164–181, 2011.

[21] Maria Dubovitskaya, Alessandra Scafuro, and Ivan Visconti. On efficient non-interactive oblivious transfer with tamper-proof hardware. *IACR Cryptol. ePrint Arch.*, page 509, 2010.

[22] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Commun. ACM*, 28(6):637–647, 1985.

[23] Matthias Fitzi, Matthew K. Franklin, Juan A. Garay, and Harsha Vardhan Simhadri. Towards optimal and efficient perfectly secure message transmission. pages 311–322, 2007.

[24] Sanjam Garg, Yuval Ishai, and Akshayaram Srinivasan. Two-round MPC: information-theoretic and black-box. In *TCC 2018*, pages 123–151, 2018.

[25] Sanjam Garg and Akshayaram Srinivasan. 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*, pages 468–499, 2018.

[26] Oded Goldreich. *The Foundations of Cryptography - Volume 2, Basic Applications*. Cambridge University Press, 2004.

[27] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game, or a completeness theorem for protocols with honest majority. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 307–328. 2019.

[28] Danny Harnik, Yuval Ishai, and Eyal Kushilevitz. How many oblivious transfers are needed for secure multiparty computation? pages 284–302, 2007.

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

[30] Yuval Ishai, Eyal Kushilevitz, Sigurd Meldgaard, Claudio Orlandi, and Anat Paskin-Cherniavsky. On the power of correlated randomness in secure computation. In *Theory of Cryptography - 10th Theory of Cryptography Conference, TCC 2013, Tokyo, Japan, March 3-6, 2013. Proceedings*, pages 600–620, 2013.

[31] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Zero-knowledge from secure multiparty computation. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, California, USA, June 11-13, 2007*, pages 21–30, 2007.

[32] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer - efficiently. In *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*, pages 572–591, 2008.

[33] Joe Kilian. Founding cryptography on oblivious transfer. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 20–31. ACM, 1988.

[34] Vladimir Kolesnikov. Truly efficient string oblivious transfer using resettable tamper-proof tokens. In *Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings*, pages 327–342, 2010.

[35] Huijia Lin, Tianren Liu, and Hoeteck Wee. Information-theoretic 2-round MPC without round collapsing: Adaptive security, and more. In *Theory of Cryptography - 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, Proceedings, Part II*, pages 502–531, 2020.

[36] Anderson C. A. Nascimento and Andreas J. Winter. On the oblivious transfer capacity of noisy correlations. In *Proceedings 2006 IEEE International Symposium on Information Theory, ISIT 2006, The Westin Seattle, Seattle, Washington, USA, July 9-14, 2006*, pages 1871–1875. IEEE, 2006.

[37] Arpita Patra and Akshayaram Srinivasan. Three-round secure multiparty computation from black-box two-round oblivious transfer. In *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part II*, pages 185–213, 2021.

[38] Michael O. Rabin. How to exchange secrets with oblivious transfer. Technical Report TR-81, Aiken Computation Lab, Harvard University, 1981.

[39] Andrew Chi-Chih Yao. How to generate and exchange secrets. In *27th Annual Symposium on Foundations of Computer Science*, pages 162–167, 1986.

A Omitted Preliminaries

A.1 Standard background on MPC

Through the paper, we focus on semi-honest (aka passive) secure computation hereafter referred to as *private* computation. (See, e.g., [14, 15, 26], for more detailed and concrete definitions.)

Definition A.1. (Private computation) *Let $f(x_1, \ldots, x_n)$ be a (possibly probabilistic) n-party functionality. Let π be an n-party protocol. We say that the protocol* t-privately computes f with perfect privacy *if there exists an efficient randomized simulator* Sim *for which the following holds. For any subset of corrupted parties $T \subseteq [n]$ of size at most t, and every tuple of inputs $x = (x_1, \ldots, x_n)$ the joint distribution of the simulated view of the corrupted parties together with the output of the honest parties in an ideal implementation of f,*

$$\mathsf{Sim}(T, x[T], y[T]), \quad y[\bar{T}], \qquad \text{where } y = f(x) \text{ and } \bar{T} = [n] \setminus T,$$

is identically distributed to

$$\mathsf{View}_{\pi,T}(x), \quad \mathsf{Output}_{\pi,\bar{T}}(x),$$

where $\mathsf{View}_{\pi,T}(x)$ and $\mathsf{Output}_{\pi,\bar{T}}(x)$ are defined by executing π on x with fresh randomness and concatenating the joint view of the parties in T (i.e., their inputs, their random coin tosses, and all the incoming messages), with the output that the protocol delivers to the honest parties in $\bar{T}$.

When the functionality is deterministic, the above definition scan be decomposed to privacy and correctness. That is, we require that the correctness error $\epsilon := \Pr[y \neq \mathsf{Output}_\pi(x)]$ and the t-privacy error $\delta := \mathsf{SD}(\mathsf{Sim}(T, x[T], y[T]),\ \mathsf{View}_{\pi,T}(x))$ will be both zero. (Here SD is the statistical distance). We can further relax the definition by allowing small non-zero correctness error or privacy error.

Secure Reductions. To define secure reductions, consider the following *hybrid* model. An n-party protocol augmented with an oracle to the n-party functionality g is a standard protocol in which the parties are allowed to invoke g, i.e., a trusted party to which they can securely send inputs and receive the corresponding outputs. The notion of t-security generalizes to protocols augmented with an oracle in the natural way.

Definition A.2. *Let f and g be n-party functionalities. A t* perfectly-private *reduction from f to g is an n-party protocol that given an oracle access to the functionality g, t-privately realizes the functionality f with perfect security. We say that the reduction is* non-interactive *if it involves a single call to g (and possibly local computations on inputs and outputs), but no further communication. The notions of t* computationally-private *reduction is defined analogously.*

Appropriate composition theorems, e.g., [26, Thms. 7.3.3, 7.4.3] and [14], guarantee that the call to g can be replaced by any protocol that t-privately realize g, without violating the security of the high-level protocol for f.

A.2 Properties of MPREs

Below we list some useful properties of MPREs that were proved in [4]. (The original statements refer to perfect MPREs but the same proofs apply to the statistical setting as well).

Proposition A.3 (Proposition 3.1 from [4])**.** *Let f be an n-party functionality. Let g be a δ-correct (t,ϵ)-private MPRE of f. Then the task of computing f with δ-correctness and (t,ϵ)-privacy reduces non-interactively to the task of computing g with δ-correctness and (t,ϵ)-privacy.*

Proposition A.4 (Removing internal randomness - Proposition 3.2 from [4])**.** *Let f be an n-party functionality. Suppose the functionality $\widehat{f}\left((x_1,r_1),\ldots,(x_n,r_n);r_0\right)$ is a δ-correct and (t,ϵ)-private MPRE of f. Then the functionality*

$$g\left((x_1,r_1,r_1'),\ldots,(x_n,r_n,r_n')\right) := \widehat{f}\left((x_1,r_1),\ldots,(x_n,r_n);\sum_i r_i'\right)$$

is a δ-correct (t,ϵ)-private MPRE of f.

Lemma A.5 (Composition - Lemma 3.3 from [4]). *Let f be an n-party functionality and assume the functionality g is a perfectly correct and perfectly t_1-private MPRE of f with no internal randomness. Further assume that the functionality h is a perfectly correct and t_2-perfectly private MPRE of g (viewed as a deterministic functionality over the domain $(X')^n$ where $X' = (X, R)$). Then, then functionality*

$$h'\left(\left(x_1,\left(r_1,r_1'\right)\right),\ldots,\left(x_n,\left(r_n,r_n'\right)\right);r_0'\right) := h\left(\left(\left(x_1,r_1\right),r_1'\right),\ldots,\left(\left(x_n,r_n\right),r_n'\right)\right),$$

is a perfectly correct and t_3-perfectly private MPRE of f with $t_3 = \min(t_1, t_2)$.

A.3 Non-Interactive Completeness of Finite Functionalities

Let $\mathsf{CubePlus}_n$ denote the n-party functionality that takes a pair of bits (x_1, z_1) from a party P_{i_1}, (x_2, z_2) from a party P_{i_2}, and (x_3, z_3) from a party P_{i_3} and delivers the value $x_1 \cdot x_2 \cdot x_3 + z_1 + z_2 + z_3$ to all the parties. The following theorem is taken from [3].

Theorem A.6 (Thm 6.4 in [3]). *Let f be an n-party functionality. There exists a protocol Π_f for privately computing f against a semi-honest adversary (corrupting an arbitrary subset of parties), where Π_f makes parallel calls to the $\mathsf{CubePlus}_n$ functionality and uses no further interaction. The protocol Π_f can either be: (1) computationally secure using a black-box PRG, where the complexity of the parties is polynomial in n, the security parameter* sec *and the circuit size of f, or alternatively (2) perfectly secure, where the complexity of the parties is polynomial in n and the branching program size of f.*

Therefore, an n-party protocol σ that t-privately computes $\mathsf{CubePlus}_n$ with perfect privacy can be "lifted" to a protocol π that t-privately computes f. One can also consider a 4-party variant of $\mathsf{CubePlus}$ in which the output is delivered to a designated receiver R. Let us denote this functionality by $\mathsf{CubePlusR}_4$. In the semi-honest setting, the public-output version perfectly reduces to n parallel calls to the designated-receiver variant where in each call we use a different receiver. Therefore, a protocol σ that 4-privately computes $\mathsf{CubePlusR}_4$ can be lifted to a protocol for f. However, this transformation works only if σ achieves a full privacy threshold of 4. Theorem A.6 therefore falls short of lifting a k'-private protocol σ for a finite k-party functionality to t-private protocol for general n-party functionality.

The following theorem establishes such a result at the expense of a minor loss in the threshold. Below, we model a k'-private realization of a functionality g by a k'-corruptible oracle that leaks all the information (i.e., inputs of the honest parties) to the adversary who corrupts more than k'-parties.

Theorem A.7. *Let f be an n-party functionality, and let $\alpha \leq \beta \in [0, 1]$ be some real numbers. There exists a constant $k = k(\alpha, \beta)$, a finite k-party functionality g, and a protocol Π_f for securely computing f against a semi-honest adversary corrupting αn-fraction of the parties where Π_f makes parallel calls to βk-corruptible version of g and uses no further interaction. Moreover, g can be taken to be $\mathsf{CubePlus}_k$. The protocol Π_f can either be: (1) computationally secure using a black-box PRG, where the complexity of the parties is*

polynomial in n, the security parameter sec *and the circuit size of f, or alternatively (2) perfectly secure, where the complexity of the parties is polynomial in n and the branching program size of f.*

The theorem is based on player virtualization. This technique was first introduced by the work of Bracha [13] in the context of Byzantine Agreement, and since then has been used several times in the MPC literature [23, 28, 19]. Nevertheless, to the best of our knowledge the above basic statement has not appeared in the literature before.

Proof. By Theorem A.6, it suffices to prove the theorem for the case where f is taken to be the n-party designated-receiver functionality $\mathsf{CubePlusR}_n$. Fix some finite field $\mathbb{F}$ of size at least $m+1$ for some parameter m that will be determined later. By using standard arithmetization, we can write $\mathsf{CubePlusR}_n$ as a degree-3 polynomial $x_1 \cdot x_2 \cdot x_3 + z_1 + z_2 + z_3$ over $\mathbb{F}$. Specifically, we assume that the inputs arrive from P_1, P_2 and P_3 and the receiver is P_4, and all other $n-4$ parties have no inputs or outputs. The idea is to first solve the problem in a client-server setting where a large fraction of the clients are honest, and then use party virtualization to replace the servers with calls to some finite g.

For starters, assume that we have m servers $Q_1, \ldots, Q_m$ that are all honest except for at most γm fraction, for, say, $\gamma = 0.3$. Consider the protocol π' in which P_i for $i = 1, 2, 3$, shares x_i among the servers via Shamir's secret sharing with degree γm and shares z_i over the servers via Shamir's secret sharing with degree $3\gamma m$. The servers can now run a non-interactive version of BGW [10] and send a single message to P_4 from which he can recover the output. Specifically, each server j locally computes the polynomial $x_1[j] \cdot x_2[j] \cdot x_3[j] + z_1[j] + z_2[j] + z_3[j]$ and sends the result to P_4 who uniquely interpolates the corresponding degree 3γ-polynomial and outputs its free coefficient as its output. Standard analysis shows that this protocol privately realizes f as long as the adversary does not corrupt more than γ fraction of the servers.

Let k be a sufficiently large constant whose value will be determined later. We now replace each server by a k-subset of the parties $P_1, \ldots, P_n$ that includes the parties P_1, P_2, P_3 and P_4, and take g to be the k-party functionality that realizes the operation of the jth server. That is, we enumerate over all k-subsets $S_1, \ldots, S_m$ that includes $\{P_1, P_2, P_3, P_4\}$, i.e., $m = \binom{n-4}{k}$. For every $j \in [m]$, we make a call to the functionality g that takes the jth shares $(x_1[j], z_1[j]), (x_2[j], z_2[j]), (x_3[j], z_3[j])$ from P_1, P_2 and P_3 and delivers the point $x_1[j] \cdot x_2[j] \cdot x_3[j] + z_1[j] + z_2[j] + z_3[j]$ to the receiver P_4. Note that the jth copy is applied over the set of parties S_j.

Suppose that g is instantiated by a βk-corruptible oracle. Then the resulting protocol π is private against a subset $T \subset [n]$ as long at most γ-fraction of the subsets S_i are *β-corrupted* in the sense that $|S_i \cap T| > \beta k$. By taking $k = k(\alpha, \beta)$ to be sufficiently larger constant, it can be guaranteed that the above condition holds for every αn-subset T. (It can be shown that $k = O(1/(\beta - \alpha)^2)$ suffices.) Observe that g is a k-party functionality that can be computed by a constant-size arithmetic formula over a field of size $m = O(n^k)$ which can be emulated by $\mathrm{polylog}(n^k)$ parallel calls to constant-size Boolean functionalities. Moreover, by Theorem A.6, we can non-interactively k-privately reduce g (with perfect privacy) to $\mathsf{CubePlus}_k$ (or to $\mathsf{CubePlusR}_k$). The theorem follows. □

Remark A.8 (Reducing the threshold loss $\beta - \alpha$)**.** *Suppose that, for every k, we have a protocol σ_k that βk-privately computes every k-party functionality with complexity* $\exp(k)$ *– as done in the proof of Theorem 5.4. Then, for some $\alpha_n = \beta - o_n(1)$, we can $\alpha_n n$-privately compute every n-party functionality by making parallel calls to σ_k for $k = O(\log n)$ while keeping the protocol efficient. The new protocol achieves the same features as in Theorem A.7. That is, the complexity is polynomial in n and in the branching program size (resp., circuit size) of f and it achieves perfect privacy (resp., computational privacy and black-box access to a PRG). This can be done by tweaking the above proof along the lines of [19]. Specifically, the committees $S_1, \ldots, S_m$ are chosen according to a bipartite expander graph over n left nodes, m right nodes, with right degree of $k = O(\log n)$, so that every αn-subset T of left nodes has at most* $0.3m$ *right neighbors that touch more than βk left nodes. Such graphs can be constructed efficiently in* $\mathrm{poly}(n)$ *time. See Lemma 5 in [19] for further details.*