Hybrid-Secure MPC: Trading Information-Theoretic Robustness for Computational Privacy

Christoph Lucas*
Department of Computer Science, ETH Zurich
8092 Zurich, Switzerland
clucas@inf.ethz.ch

Dominik Raub† ‡
Department of Computer Science, University of Århus
8000 Århus, Denmark
raub@cs.au.dk

Ueli Maurer‡
Department of Computer Science, ETH Zurich
8092 Zurich, Switzerland
maurer@inf.ethz.ch

ABSTRACT

Most protocols for distributed, fault-tolerant computation, or multi-party computation (MPC), provide security guarantees in an *all-or-nothing* fashion. In contrast, a hybrid-secure protocol provides different security guarantees depending on the set of corrupted parties and the computational power of the adversary, without being aware of the actual adversarial setting. Thus, hybrid-secure MPC protocols allow for graceful degradation of security.

We present a hybrid-secure MPC protocol that provides an optimal trade-off between IT robustness and computational privacy: For any *robustness parameter* $\rho < \frac{n}{2}$, we obtain one MPC protocol that is simultaneously IT secure with robustness for up to $t \leq \rho$ actively corrupted parties, IT secure with fairness (no robustness) for up to $t < \frac{n}{2}$, and computationally secure with agreement on abort (privacy and correctness only) for up to $t < n - \rho$. Our construction is secure in the universal composability (UC) framework (based on a network of secure channels, a broadcast channel, and a common reference string). It achieves the bound on the trade-off between robustness and privacy shown by Ishai et al. [CRYPTO'06] and Katz [STOC'07], the bound on fairness shown by Cleve [STOC'86], and the bound on IT security shown by Kilian [STOC'00], and is the first protocol that achieves all these bounds simultaneously.

Categories and Subject Descriptors

D.4.6 [**OPERATING Systems**]: Security and Protection—*Cryptographic controls*

General Terms

Security, Theory, Reliability

Keywords

Multi-party computation, information-theoretic security, computational security, hybrid security, universal composability, party emulation.

1. INTRODUCTION

1.1 Secure Multi-Party Computation

The goal of *multi-party computation* (MPC) is to perform a computation in a distributed, private, and fault-tolerant way [33]. For this purpose, a fixed set of n parties runs a protocol that tolerates an adversary corrupting a subset of the participating parties. Actively corrupted parties may deviate arbitrarily from the protocol, whereas passively corrupted parties follow the protocol and, intuitively speaking, only try to violate privacy. Security requirements for MPC in the literature (e.g. [17]) include privacy, correctness, robustness, fairness, and agreement on abort. *Privacy* is achieved if the adversary cannot learn more about the honest parties' inputs than what can be deduced from the inputs and outputs of the corrupted parties. *Correctness* means that the protocol either outputs the intended value or no value at all. Privacy and correctness are the two basic requirements. Possible additional requirements are notions of output guarantees, which we discuss in order of decreasing strength: A protocol achieves *robustness* if an adversary cannot abort the computation, preventing the honest parties from obtaining output. *Fairness* is achieved if the honest parties obtain at least as much information about the output as the adversary. *Agreement on abort* means that all honest parties detect if one of them aborts (and then generally make no output).

Goldreich et al. [19] provide a first general solution to the MPC problem[1], based on computational (CO) intractability assumptions and a broadcast (BC) channel. They achieve full security against $t < \frac{n}{2}$ actively corrupted parties, or privacy and correctness only (no fairness or robustness) against $t < n$ actively corrupted parties. If no BC channel is available, privacy and correctness against $t < n$ actively corrupted parties can also be obtained using the BC construction from [15]. Robust MPC without BC channel is possible

*Supported by the Zurich Information Security Center.
†Work done while at ETH Zurich, Switzerland.
‡Supported by the Swiss National Science Foundation (SNF), SPP project no. 200020-113700/1.

[1]Essentially, [19] presents the general idea, while [18] gives a detailed protocol description and a proof of security.

PODC'10, July 25–28, 2010, Zurich, Switzerland.

if and only if $t < \frac{n}{3}$ parties are corrupted in both the CO and the IT setting [30]. The protocols of both [2] and [9] are IT secure, require no BC channel, and achieve this bound. When a BC channel is available [31], or if no robustness but only fairness is required [15], the bound for IT MPC can be improved to $t < \frac{n}{2}$.

The adversarial setting is defined by the combination of the computational power of the adversary and the cardinality of the set of corrupted parties. Impossibility proofs show that most security guarantees can be achieved simultaneously (i.e. by a single protocol) only in a subset of all adversarial settings. Cleve [11] shows that fairness for general MPC can be achieved only for $t < \frac{n}{2}$ actively corrupted parties. The same bound holds for IT security given a broadcast channel [26]. Ishai et al. [24] and Katz [25] show that a protocol which guarantees robustness for up to ρ corrupted parties can be secure with abort against at most $n - \rho$ corrupted parties, and describe CO secure protocols that match these bounds.

1.2 Hybrid Security and our Contribution

Conventional, non-hybrid MPC protocols distinguish only between adversarial settings in which they provide all specified security guarantees, and settings in which they provide no security guarantees at all. In contrast, MPC protocols with hybrid security provide different security guarantees for each adversarial setting, without being aware of the actual setting. Hence, they allow for graceful degradation of security.

Specifically, we discuss a protocol providing strong security guarantees for few corruptions in the IT setting, and weaker security guarantees for many corruptions in the CO setting. More precisely, for any robustness parameter $\rho < \frac{n}{2}$ and any static adversary actively corrupting t parties, we describe an MPC protocol π^ρ that simultaneously provides IT security with robustness, correctness and privacy for $t \leq \rho$, IT security with fairness, correctness, and privacy for $t < \frac{n}{2}$, and CO security with agreement on abort, correctness, and privacy for $t < n - \rho$. Hence, our protocol is optimal under the bounds on fairness [11], IT security [26], and the trade-off between robustness and privacy [24, 25].

Our protocol is based on a complete network of synchronous secure channels, a synchronous authenticated broadcast channel, and a common reference string (CRS). The security is proven in the universal composability model [5]. In [28, 32], we also present results for the stand-alone setting without CRS.

Furthermore, we present a modified version of the protocol with weaker security guarantees, which does not require a broadcast channel.

1.3 Related Work

Chaum [8] sketches a protocol construction secure against passive adversaries that simultaneously guarantees CO privacy for any number of corrupted parties, and IT privacy for a corrupted minority. In contrast to our work, [8] does not discuss the active setting, and hence does not guarantee correctness, fairness, or robustness in case of active corruptions. It is not evident how this protocol would be extended to the active setting. A crucial technique of both Chaum's approach and ours is *party emulation*, which allows a set of parties to implement an additional virtual party for a higher level protocol. This technique was first used in [4] to improve the threshold of broadcast protocols in a setting where privacy is not relevant. Damgård et al. [13] extend the technique to improve the threshold of general MPC protocols. In [23], this technique was discussed in the stand-alone setting for perfectly secure MPC and applied to general adversary structures.

Fitzi et al. [15] improve upon [2, 9] in the IT setting when no BC channel is available by allowing for two thresholds t_v and t_c, where $t_v = 0$ or $t_v + 2t_c < n$. For $t \leq t_v$ corrupted parties, fully secure MPC is achieved, while for $t_v < t \leq t_c$ corrupted parties, non-robust (but fair) MPC is accomplished.

Another work by Fitzi et al. [16] also combines IT and CO security: Up to a first threshold t_p, the security is IT. Between t_p and a second threshold t_σ, IT security is guaranteed if the underlying PKI is consistent. Finally, between t_σ and T, the protocol is as secure as the signature scheme in use. Fitzi et al. show that their notion of hybrid MPC is achievable for $(2T + t_p < n) \wedge (T + 2t_\sigma < n)$, which they prove to be tight.

Both [15] and [16] work in a setting without BC channel. When a BC channel is provided, our results improve substantially upon those of [15, 16]. As [15] only treats IT MPC and [16] only treats robust MPC, both [15, 16] do not reach beyond $t < \frac{n}{2}$ corrupted parties, nor are they easily extended. In contrast, we can guarantee CO security with agreement on abort for $t < n - \rho$. In the setting without BC channel and for $\rho > 0$, our results match those of [15] (which they prove optimal for this case). However, for the special case that $\rho = 0$ (i.e., no robustness is required) our construction achieves IT fairness for $t < \frac{n}{2}$, and CO security with agreement on abort for $t < n$ corrupted parties, which goes beyond [15].

2. SECURITY DEFINITIONS

2.1 Universal Composability

We follow the Universal Composability (UC) paradigm [5, 1], which uses a simulation-based security model. Here, we only give a high-level overview of the paradigm, see [5] for technical details. The security of a protocol (the real world) is defined with respect to a *Trusted Third Party* or *Ideal Functionality* F that correctly performs all computations (the ideal world). Informally, a protocol π is secure if whatever an adversary can achieve in the real world could also be achieved in the ideal world.

More precisely, let $\mathcal{P} = \{1, \ldots, n\}$ be the set of all parties. We only consider static corruptions and use $\mathcal{H} \subseteq \mathcal{P}$ to denote the set of honest parties, and $\mathcal{A} = \mathcal{P} \setminus \mathcal{H}$ to denote the set of corrupted parties. In the *real world*, there is a given set of resources R to which, for each honest party $i \in \mathcal{H}$, a protocol machine π_i is connected. Apart from interacting with the resources, protocol machines provide an interface to higher level protocols for input and output, called an I/O-channel. Corrupted parties access the resources directly which models that they do not adhere to the protocol. The complete real world is denoted by $\pi_{\mathcal{H}}(\mathsf{R})$. In [5], resources are modeled as ideal functionalities available in a hybrid model[2] (e.g., authentic or secure channels, broadcast channels). The *ideal world* consists of the ideal functionality F and an ideal ad-

[2]Note that the term "hybrid model" is not related to the notion of hybrid security.

versary (or simulator) σ connected to F via the interfaces of the corrupted parties $\mathcal{A}$. This ideal world is denoted by $\sigma_{\mathcal{A}}(\mathsf{F})$.

A protocol π is said to securely implement a functionality F if, for every possible set $\mathcal{A}$ of corrupted parties, there is a simulator σ such that no distinguisher D can tell the real world and the ideal world apart.[3] For this purpose, the distinguisher directly interacts either with the real or with the ideal world, by connecting to all open interfaces, and then outputs a decision bit. This interaction is denoted by $\mathsf{D}(X)$, where $X \in \{\pi_{\mathcal{H}}(\mathsf{R}), \sigma_{\mathcal{A}}(\mathsf{F})\}$.

In [5], all protocol machines, simulators, ideal functionalities, and distinguishers are modeled as interactive Turing machines (ITM). We define Σ^{all} as the set of *all* ITMs, and Σ^{eff} as the set of *polynomially bounded* ITMs. Note that, in this paper, ITMs are specified on a higher level of abstraction.

Definition 1. (Universally Composable (UC) Security) A protocol π *UC securely* implements an ideal functionality F if $\forall \mathcal{A}\ \exists \sigma_{\mathcal{A}} \in \Sigma^{\mathsf{eff}}\ \forall \mathsf{D} \in \Sigma^{\mathsf{eff}/\mathsf{all}}$:

$$|\Pr[\mathsf{D}(\sigma_{\mathcal{A}}(\mathsf{F})) = 1] - \Pr[\mathsf{D}(\pi_{\mathcal{H}}(\mathsf{R})) = 1]| \leq \varepsilon(\kappa)$$

where $\varepsilon(\kappa)$ denotes a negligible function in the security parameter κ. For $\mathsf{D} \in \Sigma^{\mathsf{eff}}$, the security is *computational* (CO). For $\mathsf{D} \in \Sigma^{\mathsf{all}}$, the security is *information-theoretic* (IT).

Simulators must be efficient not only in the CO, but also in the IT setting, since otherwise, IT security does not imply CO security. Our formalization of hybrid security uses ideal functionalities that are aware of both the set of corrupted parties and the computational power of the adversary. In other words, the behavior of the functionality, and hence the security guarantees, varies depending on both parameters. A protocol π UC securely implements an ideal functionality F with hybrid-security if π securely implements F in both the CO and the IT setting. Note that, in contrast to [5], we use a synchronous communication model with static corruption. The bounds for MPC mentioned in Section 1.1 apply to this model.

In the UC setting, a strong composition theorem can be proven [5, 1]. This theorem states that wherever a protocol π is used, we can indistinguishably replace this protocol by the corresponding ideal functionality F together with an appropriate simulator.[4]

2.2 Ideal Functionalities for MPC

MPC protocols implement ideal functionalities $\mathcal{E}$ that perform certain computations which are described in some specified language. We describe computations as *programs*[5], i.e. arbitrary sequences of operations on values from a predefined finite field, where each operation is one of input, addition, multiplication, or output.[6] Given such a program $\mathcal{C}$, an MPC functionality $\mathcal{E}[\mathcal{C}]$ evaluates the program operation-wise, and stores intermediate values internally in a vector of registers. Basically, it works as follows: In case of an input operation, $\mathcal{E}[\mathcal{C}]$ receives an input from a certain party over the corresponding I/O-channel and stores it internally in a new register. In case of an addition operation, $\mathcal{E}[\mathcal{C}]$ adds the two corresponding values internally, and stores the result in a new register. The case of a multiplication operation is handled analogously. In case of an output operation, $\mathcal{E}[\mathcal{C}]$ retrieves the corresponding value from the register, and outputs it to all parties.

The operations defined above capture only deterministic computations with symmetric output. However, probabilistic computations with asymmetric output can be reduced to these operations [3, 10]. Furthermore, note that such programs can also perform the computations necessary for realizing an arbitrary protocol machine, thereby allowing for party emulation.

In our work, we are interested in ideal functionalities that evaluate programs with various security guarantees (i.e. only with a subset of the security properties described in Section 1.1, but generally at least encompassing privacy and correctness), depending on the adversarial setting.

Full Security implies *privacy, correctness, and robustness.* Hence, given a program $\mathcal{C}$, an ideal functionality evaluating $\mathcal{C}$ with full security follows the program without deviation.

Fair Security implies *privacy, correctness, and fairness.* Given a program $\mathcal{C}$, an ideal functionality evaluating $\mathcal{C}$ with fair security executes input, addition, and multiplication operations without deviation. However, in case of an output operation, the functionality first requests an output flag $o \in \{0, 1\}$ from the adversary (default is $o = 1$ if the adversary makes no suitable input). Then, for $o = 1$ the functionality executes the output operation with output to *all* parties, for $o = 0$, the functionality halts.

Abort Security implies *privacy, correctness, and agreement on abort.* Given a program $\mathcal{C}$, an ideal functionality evaluating $\mathcal{C}$ with abort security executes input, addition, and multiplication operations without deviation. In case of an output operation, the functionality first outputs the corresponding value to the adversary and requests an output flag $o \in \{0, 1\}$ from the adversary (default is $o = 1$ if the adversary makes no suitable input). Then, for $o = 1$, the functionality executes the output operation with output to *all* parties, for $o = 0$, the functionality halts.[7]

No Security: Given a program $\mathcal{C}$, an ideal functionality evaluating $\mathcal{C}$ with no security forwards all inputs from the honest parties to the adversary and lets the adversary determine all outputs for honest parties. As a simulator σ^{noSec} can use the inputs of honest parties to simulate honest protocol machines, this already proves the following (rather trivial) lemma:

LEMMA 1. *Given a program $\mathcal{C}$, any protocol π UC securely implements the ideal functionality evaluating $\mathcal{C}$ with no security.*

We therefore omit this case from the description of the simulators in this work.

[3] In this model, the adversary is thought of as being part of the distinguisher. Canetti [5] shows that this model without adversary is essentially equivalent to a model with adversary, since the security definition quantifies over all distinguishers.

[4] This follows from the free interaction between the distinguisher and the system during the execution, which implicitly models that outputs of the system can be used in arbitrary other protocols, even before the execution ends. This is in contrast to a stand-alone definition of security where the distinguisher receives output only at the end.

[5] A computation could equivalently be modeled as a circuit.

[6] It is out of scope of this paper how the program is determined. We simply assume that all entities "know" what to do next.

[7] We could relax the definition further by allowing the adversary to send one output flag for each party, dropping agreement on abort. However, all our protocols will achieve agreement on abort.

3. A PROTOCOL OVERVIEW

Our result for hybrid-secure MPC is formalized by the ideal functionality $\mathcal{E}_\rho^{\mathsf{hyb}}[\mathcal{C}]$. This functionality evaluates a program $\mathcal{C}$ with IT full security for $t \leq \rho$ corrupted parties, with IT fair security for $t < \frac{n}{2}$ corrupted parties, and with CO abort security for $t < n - \rho$ corrupted parties (see Figure 1).

Given a robustness parameter $\rho < \frac{n}{2}$ and a program $\mathcal{C}$, the ideal functionality $\mathcal{E}_\rho^{\mathsf{hyb}}[\mathcal{C}]$ evaluates $\mathcal{C}$ according to the number t of corrupted parties and according to the computational power of the adversary (CO or IT).

Setting		Security Guarantees
$t \leq \rho$	IT/CO	evaluate $\mathcal{C}$ with full security
$\rho < t < \frac{n}{2}$	IT/CO	evaluate $\mathcal{C}$ with fair security
$\frac{n}{2} \leq t < n - \rho$	CO	evaluate $\mathcal{C}$ with abort security
$\frac{n}{2} \leq t < n$	IT	evaluate $\mathcal{C}$ with no security
$n - \rho \leq t < n$	CO	

Figure 1: The ideal functionality $\mathcal{E}_\rho^{\mathsf{hyb}}[\mathcal{C}]$.

We present a protocol π^ρ that UC securely implements the functionality $\mathcal{E}_\rho^{\mathsf{hyb}}[\mathcal{C}]$ from an n-party communication resource com^n (consisting of a complete network of synchronous secure channels and a synchronous authenticated n-party broadcast channel), and an n-party CRS crs^n drawn from a predefined distribution. A CRS (or an equivalent resource) is required to avoid the impossibility results of [5, 6].[8] The proof of Theorem 1 stating the security of the protocol π^ρ is an application of the UC composition theorem to Lemma 2, Lemma 3, Corollary 1, and Lemma 5.

THEOREM 1. *Given a program $\mathcal{C}$ and a robustness parameter $\rho < \frac{n}{2}$, protocol π^ρ UC securely implements the ideal functionality $\mathcal{E}_\rho^{\mathsf{hyb}}[\mathcal{C}]$ evaluating $\mathcal{C}$, from a complete and synchronous network of secure channels and an authenticated broadcast channel com^n, and a common reference string crs^n, in the presence of a static and active adversary.*

3.1 Overview and Key Design Concepts

Basically, the protocol π^ρ consists of three protocol layers: On the lowest layer, the n parties use a technique called *party emulation* to emulate another, $(n+1)^{\text{st}}$ party. The emulation of a party makes it harder for the adversary to control this party: It is not sufficient to corrupt a single party, but, in our case, it is necessary to corrupt at least $\frac{n}{2}$ real parties to control the emulated party. Hence, more trust can be placed in this emulated party. On the middle layer, an $(n+1)$-party MPC protocol is carried out among the n original parties and the emulated party. This protocol provides IT guarantees given that a designated party is honest (this designated party is the emulated party), and CO guarantees otherwise. While it already achieves the correctness, robustness, and fairness requirements (both IT and CO), only the input of the designated party is IT private. The remaining parties obtain only CO privacy. To additionally fulfill the privacy requirement, on the highest layer, the parties exploit this asymmetry: Each party splits its input into two halves, and provides one half as input via a regular party, and the other half as input via the designated party. Additional techniques are required here to maintain correctness and robustness.

More formally, the protocol π^ρ is modularized into three subprotocols: the emulation, the designated party, and the input subprotocol. Each subprotocol implements an ideal functionality on which the next subprotocol is based (see Figure 2).

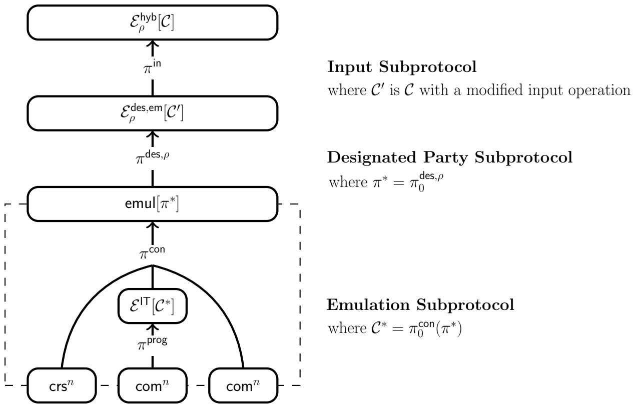

Figure 2: A visualization of the construction underlying our hybrid-secure MPC protocol π^ρ.

The goal of the *emulation subprotocol* (Section 4) is to implement a protocol machine π^* belonging to an $(n+1)^{\text{st}}$ party, as formalized by the ideal functionality $\mathsf{emul}[\pi^*]$ (Figure 4). This subprotocol is based on the given resources com^n and crs^n. On the one hand, a protocol machine performs certain computations that can be modeled as a program (see Section 2.2). On the other hand, it communicates with given resources. As a consequence, the subprotocol for party emulation is again modularized into two subprotocols π^{prog} and π^{con}. The subprotocol π^{prog} implements an MPC functionality to evaluate the program of π^* (Section 4.1). The subprotocol π^{con} enables the interaction between the emulated π^* and the resources com^{n+1} and crs^{n+1} (Section 4.2).

The *designated party subprotocol* $\pi^{\mathsf{des},\rho}$ (Section 5) is basically an $(n+1)$-party protocol and implements the ideal functionality $\mathcal{E}_\rho^{\mathsf{des,em}}[\mathcal{C}']$ that provides stronger security guarantees if a designated party is honest. This subprotocol is based on $\mathsf{emul}[\pi^*]$. While we think of protocol $\pi^{\mathsf{des},\rho}$ as an $n+1$ party protocol, one of the protocol machines ($\pi_0^{\mathsf{des},\rho}$) is actually emulated by the ideal functionality $\mathsf{emul}[\pi^*]$, i.e. in fact we set the parameter $\pi^* = \pi_0^{\mathsf{des},\rho}$ and run an n-party protocol $\pi_1^{\mathsf{des},\rho}, \ldots, \pi_n^{\mathsf{des},\rho}$ on a resource that emulates the $(n+1)^{\text{st}}$ party $\pi_0^{\mathsf{des},\rho}$.

Finally, the *input subprotocol* π^{in} (Section 6) implements the ideal functionality for hybrid security, $\mathcal{E}_\rho^{\mathsf{hyb}}[\mathcal{C}]$, based on $\mathcal{E}_\rho^{\mathsf{des,em}}[\mathcal{C}']$. For this purpose, we define the program $\mathcal{C}'$ evaluated by $\mathcal{E}_\rho^{\mathsf{des,em}}[\mathcal{C}']$ to be equivalent to the program $\mathcal{C}$ evaluated by $\mathcal{E}_\rho^{\mathsf{hyb}}[\mathcal{C}]$, however with a modified input operation taking into account the input splitting and the techniques to preserve correctness and robustness mentioned above.

[8]It is possible to minimize the reliance on the crs^n such that our protocols tolerate an adversarially chosen crs^n for few corrupted parties by applying techniques from [20, 21] and a $(t, 2t-1)$-combiner for commitments (e.g. [22]). However, this construction is beyond the scope of this paper.

4. PARTY EMULATION

In this section, we describe a technique for party emulation. This technique allows to emulate an arbitrary protocol machine π^* and to employ it in a higher level protocol. A protocol machine fulfills two tasks which we discuss separately: On the one hand, it performs certain computations (discussed in Section 4.1), on the other hand, it sends and receives messages over its interfaces (discussed in Section 4.2).

4.1 Emulating the Computation of π^*

A protocol machine π^* internally performs certain computations. These computations can be modeled as a program that can be evaluated by an MPC functionality, as discussed in Section 2.2. For the purpose of achieving hybrid-secure MPC, we require the emulation of π^* to be IT full secure for $t < \frac{n}{2}$ corrupted parties. This security requirement is captured by the ideal functionality $\mathcal{E}^{\mathsf{IT}}[\mathcal{C}^*]$ evaluating a program $\mathcal{C}^*$ (Figure 3). Note that in Section 4.2.2, we define $\mathcal{C}^*$ such that it contains not only the operations performed by π^*, but additional operations enabling communication over the interfaces of π^*.

Given a program $\mathcal{C}^*$, the ideal functionality $\mathcal{E}^{\mathsf{IT}}[\mathcal{C}^*]$ evaluates $\mathcal{C}^*$, according to the number t of corrupted parties:

Setting		Security Guarantees
$t < \frac{n}{2}$	IT/CO	evaluate $\mathcal{C}^*$ with full security
$\frac{n}{2} \leq t$	IT/CO	evaluate $\mathcal{C}^*$ with no security

Figure 3: The ideal functionality $\mathcal{E}^{\mathsf{IT}}[\mathcal{C}^*]$.

The subprotocol π^{prog} has to implement the ideal functionality $\mathcal{E}^{\mathsf{IT}}[\mathcal{C}^*]$ from a complete network of synchronous secure channels and a BC channel. As stated in Lemma 2, the protocol presented in [31] already fulfills all requirements.

LEMMA 2 ([31, 12, 5]). *Given an arbitrary program $\mathcal{C}^*$, there is a protocol that UC securely implements the ideal functionality $\mathcal{E}^{\mathsf{IT}}[\mathcal{C}^*]$ from a complete network of synchronous secure channels and a BC channel com^n, in the presence of a static and active adversary.*

4.2 Connecting π^* to the Resources

In the previous section, we described a protocol π^{prog} that emulates the computations of a protocol machine π^*. In this section, we describe a protocol π^{con} that enables the communication over the interfaces of the emulated π^*. This communication includes the interaction with the resources (i.e. a complete network of synchronous secure channels and a BC channel for $n+1$ parties, denoted by com^{n+1}, and an $(n+1)$-party CRS crs^{n+1}), as well as the input from and output to the emulating parties. Before we present the protocol π^{con}, we give a formal description of the ideal functionality $\mathsf{emul}[\pi^*]$ implemented by π^{con}.

4.2.1 The Ideal Functionality for Emulated Parties

We now give a description of the ideal functionality $\mathsf{emul}[\pi^*]$ (summarized in Figure 4). Basically, $\mathsf{emul}[\pi^*]$ internally emulates the resources com^{n+1} and crs^{n+1}, and a protocol machine π^*. This protocol machine is given to $\mathsf{emul}[\pi^*]$ as a parameter, and is an arbitrary protocol machine with the condition that it has a com^{n+1} and a crs^{n+1} interface, and n I/O-channels (instead of a single one as usual). These n I/O-channels belong to the n parties emulating π^*. Accordingly, the interface of $\mathsf{emul}[\pi^*]$ for each party consists of three subinterfaces: Each party has access to its corresponding interfaces of com^{n+1} and crs^{n+1}, and may provide input to and receive output from π^* over its corresponding I/O-channel to π^*.

For $t < \frac{n}{2}$ corrupted parties, $\mathsf{emul}[\pi^*]$ internally emulates the ideal functionalities com^{n+1} and crs^{n+1}, and the protocol machine π^*, and connects them accordingly. In this setting, the protocol machine π^* works according to its specification, i.e. can be considered honest. We denote this behavior of $\mathsf{emul}[\pi^*]$ with $[\mathsf{crs}^{n+1}, \mathsf{com}^{n+1}, \pi^*]$.

For $t \geq \frac{n}{2}$, $\mathsf{emul}[\pi^*]$ transfers control over the (emulated) protocol machine π^* to the adversary. Hence, $\mathsf{emul}[\pi^*]$ only emulates com^{n+1} and crs^{n+1}, and gives the adversary access not only to the interfaces of com^{n+1} and crs^{n+1} belonging to corrupted parties, but also to the interfaces belonging to the emulated protocol machine π^*. Furthermore, the I/O-channels from honest parties to π^* are directly connected to the adversary. We denote this behavior of $\mathsf{emul}[\pi^*]$ with $[\mathsf{crs}^{n+1}, \mathsf{com}^{n+1}]$.

Given a protocol machine π^*, the ideal functionality $\mathsf{emul}[\pi^*]$ evaluates a program either for $[\mathsf{crs}^{n+1}, \mathsf{com}^{n+1}, \pi^*]$ or for $[\mathsf{crs}^{n+1}, \mathsf{com}^{n+1}]$, according to the number t of corrupted parties:

Setting		Security Guarantees
$t < \frac{n}{2}$	IT/CO	evaluate the program for $[\mathsf{crs}^{n+1}, \mathsf{com}^{n+1}, \pi^*]$ with full security
$\frac{n}{2} \leq t$	IT/CO	evaluate the program for $[\mathsf{crs}^{n+1}, \mathsf{com}^{n+1}]$ with full security

Figure 4: The ideal functionality $\mathsf{emul}[\pi^*]$.

4.2.2 Protocol π^{con}

Here, we describe a protocol π^{con} that implements the ideal functionality $\mathsf{emul}[\pi^*]$, based on the ideal functionalities $\mathcal{E}^{\mathsf{IT}}[\mathcal{C}^*]$ (evaluating a program $\mathcal{C}^*$ to be defined below), com^n, and crs^n.[9] The task of π^{con} is twofold: On the one hand, it turns the n-party resources com^n and crs^n into resources for $n+1$ parties. On the other hand, it connects the emulated protocol machine π^* (running as part of $\mathcal{C}^*$ on $\mathcal{E}^{\mathsf{IT}}[\mathcal{C}^*]$) to these resources. The protocol π^{con} consists of the n protocol machines $\pi_1^{\mathsf{con}}, \ldots, \pi_n^{\mathsf{con}}$ run by the real parties, and an additional protocol machine denoted by π_0^{con} that runs as part of $\mathcal{C}^*$ on $\mathcal{E}^{\mathsf{IT}}[\mathcal{C}^*]$. In fact, π_0^{con} is a wrapper for π^*, and we parametrize $\mathcal{E}^{\mathsf{IT}}[\mathcal{C}^*]$ with the program that emulates π_0^{con} connected to all interfaces of π^*, which we denote by $\mathcal{C}^* = \pi_0^{\mathsf{con}}(\pi^*)$.

Each protocol machine π_i^{con} ($i \in \{1, \ldots, n\}$) is connected to the resources com^n, crs^n and $\mathcal{E}^{\mathsf{IT}}[\mathcal{C}^*]$. In turn, via its I/O-channel to higher level protocols, π_i^{con} provides access to a com^{n+1}, a crs^{n+1}, and one I/O-channel of π^*. The protocol machine π_0^{con} is connected to all interfaces of π^*. Furthermore, each one of the n interfaces of $\mathcal{E}^{\mathsf{IT}}[\mathcal{C}^*]$ (the ideal functionality evaluating $\mathcal{C}^* = \pi_0^{\mathsf{con}}(\pi^*)$) serves as a secure channel between π_0^{con} and a protocol machine π_i^{con} ($i \in \{1, \ldots, n\}$).

[9] As stated in Theorem 1, we assume a single resource com^n. However, for the emulation subprotocol, we require two independent copies of com^n, which can be achieved by multiplexing the given com^n.

Using these secure channels, protocol π^{con} enables the interaction between π^* and the resources com^n and crs^n, and thereby extends these resources to $(n+1)$-party resources.

Basically, the protocol machines π_i^{con} only receive messages and forward them on the correct interface and with the correct label. For broadcast messages and the CRS, consensus among all parties is guaranteed by additionally performing a majority vote on messages relating to π_0^{con}. Given that $t < \frac{n}{2}$ parties are corrupted, this results in a correct $(n+1)$-party broadcast and CRS. For $t \geq \frac{n}{2}$ corrupted parties, π^* is controlled by the adversary and it is not necessary to securely extend the resources. Figures 5 and 6 provide a technical description of the protocol machines π_0^{con} and π_i^{con} ($i \in \{1, \ldots, n\}$), respectively. A proof of the following Lemma can be found in [29].

LEMMA 3. *Protocol* π^{con} *UC securely implements* $\mathsf{emul}[\pi^*]$ *from* com^n*,* crs^n*, and the functionality* $\mathcal{E}^{\mathsf{IT}}[\mathcal{C}^*]$ *evaluating* $\mathcal{C}^* = \pi_0^{\mathsf{con}}(\pi^*)$*, in the presence of a static and active adversary.*

π_0^{con} connects to *all* interfaces of protocol machine π^*, i.e. to the com^{n+1} interface, the crs^{n+1} interface and to the n I/O-interfaces. In turn, π_0^{con} makes direct use of the n interfaces of $\mathcal{E}^{\mathsf{IT}}[\mathcal{C}^*]$ as secure channels to the π_i^{con} ($i \in \{1, \ldots, n\}$). π_0^{con} then processes messages as follows:

Secure Channels: Messages from π_i^{con} that are labeled as secret message from party i are forwarded to the com^{n+1}-interface of π^*. Messages for party i from the com^{n+1}-interface of π^* are labeled as secret message from the emulated party and sent to π_i^{con}.

I/O for π^*: Messages from π_i^{con} labeled as input to π^* are forwarded to the protocol machine π^* as input to the I/O-interface of party i. Outputs from π^* on the I/O-interface of party i are labeled as such and sent to π_i^{con}.

Broadcasts: Messages labeled as broadcast messages from party j, if received identically from more than $\frac{n}{2}$ protocol machines π_i^{con}, are forwarded to the com^{n+1}-interface of π^* as broadcast messages from party j. Otherwise, they are ignored. Broadcast messages from the com^{n+1}-interface of π^* are labeled as broadcast messages from the emulated party and sent to all π_i^{con} ($i \in \{1, \ldots, n\}$).

CRS: A message labeled as CRS, if received identically from more than $\frac{n}{2}$ protocol machines π_i^{con}, is forwarded to the crs^{n+1} interface of π^*. Otherwise, it is ignored.

Figure 5: The protocol machine π_0^{con}.

5. MPC WITH A DESIGNATED PARTY

In this section, we present an $(n+1)$-party protocol $\pi^{\mathsf{des},\rho}$ that implements an ideal functionality $\mathcal{E}_\rho^{\mathsf{des}}[\mathcal{C}']$ for designated party MPC from a common reference string crs^{n+1} and an $(n+1)$-party communication resource com^{n+1}. The behavior (and hence the provided security guarantees) of the ideal functionality $\mathcal{E}_\rho^{\mathsf{des}}[\mathcal{C}']$ depend in particular on a designated party. For ease of notation, we assume that this designated party is party 0, and that the remaining parties are numbered $1, \ldots, n$.

π_i^{con} connects to the interfaces of com^n, crs^n and $\mathcal{E}^{\mathsf{IT}}[\mathcal{C}^*]$ belonging to party i. The interface to $\mathcal{E}^{\mathsf{IT}}[\mathcal{C}^*]$ serves as a secure channel to π_0^{con}. Via its I/O-channel, π_i^{con} provides access to a com^{n+1}, a crs^{n+1}, and one I/O-channel of π^*. π_i^{con} then processes messages as follows:

Secure Channels: Messages arriving on the I/O-channel labeled as secret messages for party j ($j \in \{1, \ldots, n\}$) are forwarded to com^n. Messages from party j arriving on the com^n-interface are output over the I/O-channel as messages from party j. Messages arriving on the I/O-channel labeled as secret messages for π^* are forwarded to π_0^{con}. Messages from π_0^{con} labeled as secret message from π^* to party i are output over the I/O-channel as messages from π^*.

I/O for π^*: Messages arriving on the I/O-channel labeled as inputs to π^* are forwarded to π_0^{con}. In turn, messages from π_0^{con} labeled as outputs from π^* are output over the I/O-channel.

Broadcasts from party $i \in \{1, \ldots, n\}$: Broadcast messages arriving on the I/O-channel are forwarded to com^n and to π_0^{con}, labeled as broadcast messages from party i. Broadcast messages from party j arriving on the com^n-interface (unless labeled as originating from π^*) are both output over the I/O-channel and forwarded to π_0^{con}, labeled as broadcast from party j.

Broadcasts from π^*: Messages from π_0^{con} labeled as broadcast messages from π^* are forwarded as broadcast messages to com^n (including the label). Broadcast messages arriving on the com^n-interface labeled as originating from π^*, if received identically from more than $\frac{n}{2}$ parties j, are output over the I/O-channel as broadcast message from π^*.

CRS: On first activation, π_i^{con} retrieves the CRS from the crs^n functionality, labels it accordingly, and both outputs it over the I/O-channel and sends it to π_0^{con}.

Figure 6: The protocol machine π_i^{con}.

For the sake of simplicity, we describe the designated party protocol as a usual $(n+1)$-party protocol, without taking into account that one of the parties is emulated. The security of the corresponding subprotocol in our construction can easily be derived from the security of this $(n+1)$-party protocol, and is stated in Corollary 1.

5.1 The Ideal Functionality for Designated Party MPC

The ideal functionality $\mathcal{E}_\rho^{\mathsf{des}}[\mathcal{C}']$ for $n+1$ parties evaluates an arbitrary program $\mathcal{C}'$ and provides stronger security guarantees if the designated party 0 is honest. In the following descriptions, the number t of corrupted parties always pertains to the parties $1, \ldots, n$, and never includes the designated party 0, which is treated separately. If the designated party 0 is honest, functionality $\mathcal{E}_\rho^{\mathsf{des}}[\mathcal{C}']$ guarantees IT security with correctness and fairness for all parties, as well as IT privacy for the input from party 0, against any number of corrupted parties. Additionally, it guarantees IT robustness against $t \leq \rho$ corrupted parties. If the designated party 0 is corrupted, functionality $\mathcal{E}_\rho^{\mathsf{des}}[\mathcal{C}']$ still provides CO security with correctness and privacy to the honest parties

Given a robustness parameter $\rho < \frac{n}{2}$ and a program $\mathcal{C}'$, the ideal functionality $\mathcal{E}_\rho^{\mathsf{des}}[\mathcal{C}']$ evaluates $\mathcal{C}'$ according to the computational power of the adversary (CO or IT), the honesty of party 0, and the number t of corrupted parties in $\{1, \ldots, n\}$. $\mathcal{E}_\rho^{\mathsf{des}}[\mathcal{C}']$ provides one interface to each party $i \in \{1, \ldots, n\}$, and n interfaces to party 0.

Setting			**Security Guarantees**				
IT/CO	Party 0	t	Priv. party 0	Priv. party i	Cor.	Fair.	Rob.
IT	honest	$t \le \rho$	yes	no	yes[10]	yes	yes
		$\rho < t \le n$	yes	no	yes[10]	yes	no
	corrupted	$0 \le t \le n$	*(corrupted)*	no	no	no	no
CO	honest	$t \le \rho$	yes	yes	yes	yes	yes
		$\rho < t \le n$	yes	yes	yes	yes	no
	corrupted	$t \le n - \rho$	*(corrupted)*	yes	yes	no	no
		$n - \rho < t \le n$	*(corrupted)*	no	no[11]	no	no

Addition and multiplication operations are always executed without deviation. In contrast, the execution of input and output operations depend on the security guarantees:
Privacy for party $j \in \{0, \ldots, n\}$: Execute input operations for party j without deviation.
No privacy for party $j \in \{0, \ldots, n\}$: The input is additionally sent to the adversary.
Robustness: Execute output operations without deviation.
No robustness but fairness: In case of an output operation, request an output flag $o \in \{0, 1\}$ from the adversary (default is $o = 1$ if the adversary makes no suitable input). Then, for $o = 1$, execute the output operation with output to *all* parties, for $o = 0$ halt.
No fairness but correctness: In case of an output operation, output the corresponding value to the adversary and request an output flag $o \in \{0, 1\}$ from the adversary (default is $o = 1$ if the adversary makes no suitable input). Then, for $o = 1$, execute the output operation with output to *all* parties, for $o = 0$ halt.
No correctness: Receive a value from the adversary and output this value to all parties.

Figure 7: The ideal functionality $\mathcal{E}_\rho^{\mathsf{des}}[\mathcal{C}']$.

against $t < n-\rho$ corrupted parties. The functionality $\mathcal{E}_\rho^{\mathsf{des}}[\mathcal{C}']$ is described in Figure 7.

5.2 A Designated Party MPC Protocol

We now describe a designated party MPC protocol $\pi^{\mathsf{des},\rho}$ which implements the $(n+1)$-party functionality $\mathcal{E}_\rho^{\mathsf{des}}[\mathcal{C}']$ for designated party MPC from a common reference string crs^{n+1} and an $n+1$ party communication resource com^{n+1}. We obtain protocol $\pi^{\mathsf{des},\rho}$ by adapting the CO MPC protocol of [7] to our needs.

The protocol in [7] evaluates programs consisting of input, addition, multiplication, and output operations (see Section 2.2). During an *input* operation, the party providing input commits to its input and shares it among all parties according to a predefined secret sharing scheme. In [7], this is a simple XOR n-out-of-n sharing, but as described in [18] a different sharing can be used to trade privacy for robustness. *Addition* operations are evaluated locally. To evaluate a *multiplication* operation, [7] uses oblivious transfer (OT) primitives. All intermediate results are computed as sharings, and each party is committed to its shares. To achieve security against active adversaries, each party proves the correctness of the messages it sends using zero-knowledge (ZK) proofs. During *output* operations, each party opens the commitment to its share of the final result, which can then be reconstructed locally.

Essentially, to achieve the asymmetric security guarantees of $\mathcal{E}_\rho^{\mathsf{des}}[\mathcal{C}']$, we need to provide IT security guarantees to the designated party, without compromising the original CO security guarantees for the remaining parties. In the following, we describe how the components in [7] can be modified accordingly.

5.2.1 Summary of Modifications

The protocol in [7] is based on three primitives: OT, commitment, and ZK proofs. Basically, these primitives are two-party primitives, and each one can be implemented such that one of the two parties obtains IT security guarantees, while the other party still has CO guarantees. In [29], a detailed discussion of suitable primitives can be found. Hence, in each invocation between the designated party and a normal party, the designated party can be protected against an IT adversary. Using such primitives is merely a refinement of [7], so, in the CO setting, the original security guarantees are still valid.

Furthermore, we need to modify the sharing scheme and the output reconstruction in [7] in order to meet the robustness and fairness requirements. We have to robustly tolerate $t \le \rho$ corruptions among the parties $i \in \{1, \ldots, n\}$, while preserving the unconditional privacy of party 0. This can be accomplished by modifying the underlying sharing of [7] as described in [18, Section 7.5.5]. We use a sharing scheme where any set M of $n-\rho+1$ parties that *includes* party 0 is qualified, i.e., can reconstruct. Such a sharing can efficiently be implemented using a $(2n-\rho)$-out-of-$(2n)$ Shamir-sharing where party 0 receives n shares and each remaining party i obtains a single share. Here, we inherently trade privacy for

[10] Correctness is maintained in the sense that the ideal functionality still performs the desired computation. However, the adversary may make inputs dependent on the inputs of honest parties in the current and previous input phases.

[11] Our protocol $\pi^{\mathsf{des},\rho}$ could be modified to achieve correct and input-independent non-interactive MPC in this case. For our subsequent results, though, we need not demand correctness here.

robustness: Any qualified set M of parties can reconstruct the input of the remaining parties. So, on the one hand, any qualified set M of honest parties can recover the input of up to ρ corrupted parties $i \in \{1, \ldots, n\}$. This ensures robustness, when $t \leq \rho$ corrupted parties try to disrupt the computation. On the other hand, any such qualified set M of corrupted parties can violate the privacy of the remaining parties.

Finally, we have to guarantee fairness whenever party 0 is honest. As noted in [18], a party can violate fairness only if it holds the last share required for reconstruction and all other parties already opened their commitments. In our case, party 0 is always required for reconstruction. Hence, if we specify that party 0 opens last and only if it can contribute sufficiently many shares such that all parties can reconstruct the result, then the resulting protocol $\pi^{\mathsf{des},\rho}$ is fair in the IT setting as long as party 0 is honest.

5.3 The Security of the Designated Party Protocol

The modifications to the protocol from [7] result in a protocol $\pi^{\mathsf{des},\rho}$ that provides the designated party 0 with IT security guarantees, while protecting the remaining parties with CO security. In [29], we provide a proof sketch for the following lemma:

LEMMA 4. *Given an arbitrary program $\mathcal{C}'$ and a robustness parameter $\rho < \frac{n}{2}$, protocol $\pi^{\mathsf{des},\rho}$ UC securely implements the ideal functionality $\mathcal{E}^{\mathsf{des}}_{\rho}[\mathcal{C}']$ evaluating $\mathcal{C}'$, from a complete and synchronous network of secure channels and an authenticated broadcast channel com^{n+1}, and a common reference string crs^{n+1}, in the presence of a static and active adversary.*

Computational assumptions sufficient for implementing the necessary primitives for protocol $\pi^{\mathsf{des},\rho}$, in particular perfectly hiding or perfectly binding UC secure commitments [14], are, for instance, the p-subgroup assumption or the decisional composite residuosity assumption. A similar approach, where *all* parties use primitives that IT disclose no undesired information is used in [27] to achieve long-term security for specific functions.

The protocol $\pi^{\mathsf{des},\rho}$ does not fit directly into the setting of the overall protocol π^{ρ}: On the one hand, in protocol π^{ρ}, there are only n parties running a protocol based on the functionality $\mathsf{emul}[\pi^*]$ emulating $\pi^* = \pi_0^{\mathsf{des},\rho}$ and the resources com^{n+1} and crs^{n+1}. On the other hand, these n parties have to implement the ideal functionality $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$, and not $\mathcal{E}^{\mathsf{des}}_{\rho}[\mathcal{C}']$, where the only difference is that $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$ is specialized for a setting where the designated party 0 is emulated. That means, the security guarantees provided by $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$ do not depend on the honesty of party 0, but on the bound $t < \frac{n}{2}$ for a correct emulation (see Section 4.1). More to the point, IT privacy, correctness and fairness can be violated only by a corrupted majority. Furthermore, the input for party 0 is provided by the n real parties. For this purpose, $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$ provides a second interface to each party, corresponding to one of the n interfaces of party 0 to $\mathcal{E}^{\mathsf{des}}_{\rho}[\mathcal{C}']$. Inputs over these interfaces are treated as input from party 0 when evaluating the program $\mathcal{C}'$. That is, the privacy of these inputs is guaranteed even against IT adversaries.

A formal description of $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$ is obtained by replacing the condition on the honesty of party 0 in Figure 7 by the bound $t < \frac{n}{2}$, and adjusting the interfaces accordingly (see [29]).

Basically, the following corollary is only a technical modification of Lemma 4 to our needs:

COROLLARY 1. *Given an arbitrary program $\mathcal{C}'$ and a robustness parameter $\rho < \frac{n}{2}$, the protocol machines $\pi_1^{\mathsf{des},\rho}, \ldots, \pi_n^{\mathsf{des},\rho}$ UC securely implement the ideal functionality $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$ evaluating $\mathcal{C}'$, from the ideal functionality $\mathsf{emul}[\pi^*]$ parametrized with $\pi^* = \pi_0^{\mathsf{des},\rho}$, in the presence of a static and active adversary.*

6. REALIZING HYBRID-SECURE MPC

In this section, we describe an n-party protocol π^{in} implementing a hybrid-secure MPC functionality $\mathcal{E}^{\mathsf{hyb}}_{\rho}[\mathcal{C}]$ (Figure 1) based on the designated party MPC functionality $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$ (see Section 5.3 or [29]), and the program $\mathcal{C}'$ to be evaluated by $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$. We introduce one by one the three techniques used to (1) fulfill the privacy requirement of $\mathcal{E}^{\mathsf{hyb}}_{\rho}[\mathcal{C}]$, while (2) preserving the correctness and (3) the robustness provided by $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$.

(1) The functionality $\mathcal{E}^{\mathsf{hyb}}_{\rho}[\mathcal{C}]$ specifies *IT privacy* for $t < \frac{n}{2}$ and *CO privacy* for $t < n - \rho$. The protocol π^{in} achieves this requirement by having π_i^{in} share any input x_i as $x_i = x_i^{\mathsf{it}} \oplus x_i^{\mathsf{co}}$, where x_i^{it} is chosen uniformly at random over the input space.[12] Recall that $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$ provides each party with two interfaces: a regular one, and one that corresponds to one of the n interfaces of the designated party 0 (called party-0-interface). The protocol machine π_i^{in} inputs x_i^{co} at its regular interface to functionality $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$, while entering the share x_i^{it} via its party-0-interface to functionality $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$. Functionality $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$ guarantees IT privacy for inputs over a party-0-interface for $t < \frac{n}{2}$, and CO privacy for inputs over a regular interface for $t < n - \rho$. The input splitting combines the two privacy guarantees and, hence, accomplishes the privacy requirements of $\mathcal{E}^{\mathsf{hyb}}_{\rho}[\mathcal{C}]$.

(2) To preserve *CO correctness* for $t \geq \frac{n}{2}$, additional measures are needed: For $t \geq \frac{n}{2}$, the party-0-interfaces are controlled by the adversary, who could manipulate the input x_i^{it} at will, effectively manipulating the inputs x_i to produce *incorrect* results. This adversarial behavior can be prevented using commitments: Let commit and open denote the respective procedures of a UC secure IT hiding commitment scheme (see [14, 29]). First, π_i^{in} computes an IT hiding commitment to x_i^{it} together with its opening information $(c_i, o_i) = \mathsf{commit}(x_i^{\mathsf{it}})$. Then, it inputs the commitment c_i together with x_i^{co} at its regular interface to functionality $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$, while entering the matching opening information o_i together with x_i^{it} at its party-0-interface to functionality $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$. Functionality $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$ checks these commitments. The case where a commitment fails to open correctly is treated in the next paragraph. This construction achieves CO correctness, because a CO adversary controlling the party-0-interfaces cannot open such a commitment incorrectly. At the same time, the unconditional privacy of the x_i^{it} is unaffected as the commitments c_i are IT hiding.

(3) Finally, we need to preserve *IT robustness* for $t \leq \rho$. Essentially, this means that $\mathcal{E}^{\mathsf{des,em}}_{\rho}[\mathcal{C}']$ may not simply abort if a commitment c_i fails to open correctly. Instead, it outputs

[12] As mentioned in Section 2.2, we assume a field structure with operation $\oplus$ over the input space.

a complaint, requesting that party i inputs x_i directly via its regular interface to $\mathcal{E}_\rho^{\mathsf{des,em}}[\mathcal{C}']$. This procedure does not affect privacy, since commitments c_i fail to open correctly only if either party i is corrupted or if the party-0-interfaces are controlled by the adversary. In the first case, we need not guarantee privacy to party i. In the latter case, we have $t \geq \frac{n}{2}$ corrupted parties, so we only need to guarantee CO privacy of x_i, which $\mathcal{E}_\rho^{\mathsf{des,em}}[\mathcal{C}']$ already does. Correctness is maintained since privacy is maintained and a party can only replace its own input.

The IT fairness properties of $\mathcal{E}_\rho^{\mathsf{des,em}}[\mathcal{C}']$ are unaffected by the measures described above, so the resulting protocol is fair whenever $t < \frac{n}{2}$ parties are corrupted, i.e. whenever the designated party 0 is honest.

Summarizing the measures above, we obtain a protocol π^{in} (Figure 8) and a matching program $\mathcal{C}'$ (Figure 9) to be evaluated by functionality $\mathcal{E}_\rho^{\mathsf{des,em}}[\mathcal{C}']$. Protocol π^{in} takes care of sharing inputs, providing commitments and answering complaints. The program $\mathcal{C}'$ is merely a slight adaption of the (target) program $\mathcal{C}$ evaluated by $\mathcal{E}_\rho^{\mathsf{hyb}}[\mathcal{C}]$. It additionally reconstructs the inputs, checks commitments, makes complaints, and only then evaluates $\mathcal{C}$.

Protocol machine π_i^{in} connects over the regular and the party-0-interface belonging to party i to the functionality $\mathcal{E}_\rho^{\mathsf{des,em}}[\mathcal{C}']$. In turn π_i^{in} offers an I/O-interface to higher level protocols. The protocol machine π_i^{in} then proceeds as follows:

1. On receiving an input on the I/O-interface: Choose x_i^{it} uniformly at random and compute $x_i^{\mathsf{co}} := x_i \oplus x_i^{\mathsf{it}}$. Using the IT hiding commitment scheme compute $[c_i, o_i] = \mathsf{commit}(x_i^{\mathsf{it}})$. Pass input (x_i^{co}, c_i) to the regular interface and (x_i^{it}, o_i) to the party-0-interface of $\mathcal{E}_\rho^{\mathsf{des,em}}[\mathcal{C}']$. Receive a complaint bit e on the regular interface of $\mathcal{E}_\rho^{\mathsf{des,em}}[\mathcal{C}']$. If $e = 1$, then input x_i to the regular interface of $\mathcal{E}_\rho^{\mathsf{des,em}}[\mathcal{C}']$.
2. On receiving an output y on the regular interface of $\mathcal{E}_\rho^{\mathsf{des,em}}[\mathcal{C}']$, output y on the I/O-interface.

Figure 8: The protocol machine π_i^{in}.

The program $\mathcal{C}'$ is identical to the (target) program $\mathcal{C}$ except for the input operations. Addition, multiplication and output operations are executed unmodified.
In case of an input operation for party i in program $\mathcal{C}$, program $\mathcal{C}'$ takes an input (x_i^{co}, c_i) over the regular interface to party i, and an input (x_i^{it}, o_i) over the party-0-interface to party i. If $x_i^{\mathsf{it}} \neq \mathsf{open}(c_i, o_i)$, it outputs a complaint bit $e = 1$ to all parties, and takes a new input x_i over the regular interface to party i (default to $x_i = \perp$ if no input is provided). Otherwise, it outputs $e = 0$ and computes $x_i := x_i^{\mathsf{co}} \oplus x_i^{\mathsf{it}}$.[13]

Figure 9: The program $\mathcal{C}'$ to be evaluated by $\mathcal{E}_\rho^{\mathsf{des,em}}[\mathcal{C}']$.

A proof of the following Lemma can be found in [29].

Lemma 5. *Given an arbitrary program $\mathcal{C}$ and a robustness parameter $\rho < \frac{n}{2}$, protocol π^{in} UC securely implements the ideal functionality $\mathcal{E}_\rho^{\mathsf{hyb}}[\mathcal{C}]$ evaluating $\mathcal{C}$, from a designated party MPC functionality $\mathcal{E}_\rho^{\mathsf{des,em}}[\mathcal{C}']$, in the presence of a static and active adversary.*

[13]Note that the output of the complaint bit is a regular output. If robustness is not guaranteed, the adversary might interrupt the computation at this point.

7. PROTOCOLS WITHOUT BROADCAST CHANNEL

In this section, we discuss a protocol for hybrid secure MPC in a setting *without* BC channel. To be able to use our protocol π^ρ (which relies on a BC channel), we implement a BC channel from a complete network of synchronous secure channels. For this purpose, we use the construction from [15] that provides an IT secure BC channel $\mathsf{bc}_{\mathsf{extCons}}$ with extended consistency and validity detection. For two thresholds t_v and t_c, where $t_v \leq t_c$ and either $t_v = 0$ or $t_v + 2t_c < n$, $\mathsf{bc}_{\mathsf{extCons}}$ delivers a robust BC for $t \leq t_v$ and a BC with fairness (but without robustness) for $t_v < t \leq t_c$. The construction of $\mathsf{bc}_{\mathsf{extCons}}$ is based on a *detectable precomputation*, which either establishes a setup for a robust BC (for $t \leq t_v$ always) or aborts with agreement on abort (for $t \leq t_c$).

For a robustness bound $\rho > 0$, we let $t_v = \rho < \frac{n}{3}$ and $t_c = \lceil \frac{n-t_v}{2} \rceil - 1$. This choice of parameters achieves IT full security (with robustness) for $t \leq \rho$ and IT fair security (no robustness) for $t < \frac{n-\rho}{2}$. Unfortunately, these results do not (and cannot) go beyond those of [15], which they have proven optimal for this case.

However, for robustness bound $\rho = 0$, we let $t_v = \rho = 0$ and $t_c = n$. In this case we achieve IT fair security (no robustness) for $t < \frac{n}{2}$ and CO abort security for $t < n$. This choice of parameters yields a protocol that extends the existing results and actually matches the result in Theorem 1 for $\rho = 0$ in the case where a BC channel is provided. This construction, where protocol π^ρ is run with $\rho = 0$ on the BC implementation above, is denote by π^0.

Theorem 2. *Given an arbitrary program $\mathcal{C}$, protocol π^0 UC securely implements the ideal functionality $\mathcal{E}_0^{\mathsf{hyb}}[\mathcal{C}]$ evaluating $\mathcal{C}$, from a complete and synchronous network of secure channels (*without *BC channel), and a common reference string, in the presence of a static and active adversary. Let t be the number of corrupted parties. Then π^0 evaluates $\mathcal{C}$ with IT fair security for $t < \frac{n}{2}$, and with CO abort security, for $t < n$ corrupted parties.*

8. CONCLUSIONS

We describe a hybrid secure MPC protocol that provides a flexible and optimal trade-off between IT full security (with robustness), IT fair security (no robustness), and CO abort security (no fairness). More precisely, for an arbitrarily chosen robustness parameter $\rho < \frac{n}{2}$, the protocol is IT full secure for $t \leq \rho$, IT fair secure for $t < \frac{n}{2}$, and CO abort secure for $t < n - \rho$ actively and statically corrupted parties. These results are optimal with respect to the bounds stated in [11, 26, 25, 24]. We provide a security proof of the protocol in the UC setting based on synchronous secure channels, a broadcast channel, and a CRS.

Furthermore, we discuss the synchronous secure channels model *without* BC. Here we find that for robustness parameter $\rho > 0$ the results of [15] are already optimal, but for $\rho = 0$ our protocol achieves the same results as in the case where a BC is provided, indicating that a BC channel is required only for robustness.

9. ACKNOWLEDGEMENTS

We would like to thank Björn Tackmann and Stefano Tessaro for their valuable feedback and interesting discussions.

10. REFERENCES

[1] M. Backes, B. Pfitzmann, and M. Waidner. A general composition theorem for secure reactive systems. In *TCC'04*, pages 336–354. Springer, 2004.

[2] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *STOC'88*, pages 1–10. ACM, 1988.

[3] M. Blum. Coin flipping by telephone. In *CRYPTO'81*, pages 11–15. Springer, 1981.

[4] G. Bracha. An $O(\lg n)$ expected rounds randomized byzantine generals protocol. In *STOC'85*, pages 316–326. ACM, 1985.

[5] R. Canetti. Universally composable security: a new paradigm for cryptographic protocols. In *FOCS'01*, pages 136–145. IEEE, 2001.

[6] R. Canetti and M. Fischlin. Universally composable commitments. In *CRYPTO'01*, pages 19–40. Springer, 2001.

[7] R. Canetti, Y. Lindell, R. Ostrovsky, and A. Sahai. Universally composable two-party and multi-party secure computation. In *STOC'02*, pages 494–503. ACM, 2002.

[8] D. Chaum. The spymasters double-agent problem: Multiparty computations secure unconditionally from minorities and cryptographically from majorities. In *CRYPTO'89*, pages 591–602. Springer, 1989.

[9] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols. In *STOC'88*, pages 11–19. ACM, 1988.

[10] D. Chaum, I. Damgård, and J. Graaf. Multiparty computations ensuring privacy of each party's input and correctness of the result. In *CRYPTO'87*, pages 87–119. Springer, 1988.

[11] R. Cleve. Limits on the security of coin flips when half the processors are faulty. In *STOC'86*, pages 364–369. ACM, 1986.

[12] R. Cramer, I. Damgård, S. Dziembowski, M. Hirt, and T. Rabin. Efficient multiparty computations secure against an adaptive adversary. In *EUROCRYPT'99*, pages 311–326. Springer, 1999.

[13] I. Damgård, Y. Ishai, M. Krøigaard, J. B. Nielsen, and A. Smith. Scalable multiparty computation with nearly optimal work and resilience. In *CRYPTO'08*, pages 241–261. Springer, 2008.

[14] I. Damgård and J. B. Nielsen. Perfect hiding and perfect binding universally composable commitment schemes with constant expansion factor. In *CRYPTO'02*, pages 581–596. Springer, 2002.

[15] M. Fitzi, M. Hirt, T. Holenstein, and J. Wullschleger. Two-threshold broadcast and detectable multi-party computation. In *EUROCRYPT'03*, pages 51–67. Springer, 2003.

[16] M. Fitzi, T. Holenstein, and J. Wullschleger. Multi-party computation with hybrid security. In *EUROCRYPT'04*, pages 419–438. Springer, 2004.

[17] O. Goldreich. *Foundations of Cryptography: Basic Tools*, volume 1. Cambridge University Press, 2001.

[18] O. Goldreich. *Foundations of Cryptography: Basic Applications*, volume 2. Cambridge University Press, 2004.

[19] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *STOC'87*, pages 218–229. ACM, 1987.

[20] V. Goyal and J. Katz. Universally composable multi-party computation with an unreliable common reference string. In *TCC'08*, pages 142–154. Springer, 2008.

[21] J. Groth and R. Ostrovsky. Cryptography in the multi-string model. In *CRYPTO'07*, pages 323–341. Springer, 2007.

[22] A. Herzberg. On tolerant cryptographic constructions. In *CT-RSA'05*, pages 172–190. Springer, 2005.

[23] M. Hirt and U. Maurer. Player simulation and general adversary structures in perfect multiparty computation. *Journal of Cryptology*, 13(1):31–60, 2000. Extended abstract in *Proc. 16th of ACM PODC '97*.

[24] Y. Ishai, E. Kushilevitz, Y. Lindell, and E. Petrank. On combining privacy with guaranteed output delivery in secure multiparty computation. In *CRYPTO'06*, pages 483–500. Springer, 2006.

[25] J. Katz. On achieving the "best of both worlds" in secure multiparty computation. In *STOC'07*, pages 11–20. ACM, 2007.

[26] J. Kilian. More general completeness theorems for secure two-party computation. In *STOC'00*, pages 316–324. ACM, 2000.

[27] R. Künzler, J. Müller-Quade, and D. Raub. Secure computability of functions in the IT setting with dishonest majority and applications to long-term security. In *TCC'09*, pages 238–255. Springer, 2009.

[28] C. Lucas. Combining computational and information-theoretic security in multi-party computation. Master's thesis, ETH Zurich, 2008. Supervised by Ueli Maurer and Dominik Raub, see http://e-collection.ethbib.ethz.ch/view/eth:31131.

[29] C. Lucas, D. Raub, and U. Maurer. Optimally hybrid-secure MPC. 2010. Full version, see http://eprint.iacr.org/2009/009.

[30] M. Pease, R. Shostak, and L. Lamport. Reaching agreement in the presence of faults. *J. ACM*, 27(2):228–234, 1980.

[31] T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In *STOC'89*, pages 73–85. ACM, 1989.

[32] D. Raub. *Exploring the Limits of Multi-Party Computation*. PhD thesis, ETH Zürich, 2010.

[33] A. C. Yao. Protocols for secure computations (extended abstract). In *FOCS'82*, pages 160–164. IEEE, 1982.