Abstract—Secure multi-party computation (MPC) is a fundamental problem in secure distributed computing. An MPC protocol allows a set of $n$ mutually distrusting parties to carry out any joint computation of their private inputs, without disclosing any additional information about their inputs. MPC with information-theoretic security (also called unconditional security) provides the strongest security guarantees and remains secure even against computationally unbounded adversaries. Perfectly-secure MPC protocols are a class of information-theoretically secure MPC protocols, which provide all the security guarantees in an error-free fashion. The focus of this work is perfectly-secure MPC. Known protocols are designed assuming a synchronous or asynchronous communication network. It is well known that perfectly-secure synchronous MPC is possible as long as the adversary can corrupt any $t_a < n/3$ parties. On the other hand, perfectly-secure asynchronous MPC protocols can tolerate up to $t_a < n/4$ corrupt parties. A natural question is does there exist a single MPC protocol for the setting where the parties are not aware of the exact network type and which can tolerate up to $t_a < n/3$ corruptions in a synchronous network and up to $t_a < n/4$ corruptions in an asynchronous network. We design such a best-of-both-worlds perfectly-secure MPC protocol, provided $3t_a + t_s < n$ holds. For designing our protocol, we design two important building blocks which are of independent interest. The first building block is a best-of-both-worlds Byzantine agreement (BA) protocol tolerating $t < n/3$ corruptions which remains secure both in a synchronous as well as asynchronous network. The second building block is a polynomial-based best-of-both-worlds verifiable secret-sharing (VSS) protocol, which can tolerate up to $t_s$ and $t_a$ corruptions in a synchronous and in an asynchronous network respectively.

I. INTRODUCTION

Consider a set of $n$ mutually distrusting parties $P = \{P_1, \ldots, P_n\}$, where each $P_i$ has some private input. The distrust among the parties is modelled as a centralized adversary, who can control any $t$ out of the $n$ parties in a Byzantine (malicious) fashion and force them to behave arbitrarily during the execution of any protocol. An MPC protocol [17], [28], [42], [45], [58], [60] allows the parties to securely compute any known function of their private inputs, such that the honest parties (who are not under the adversary’s control) obtain the correct output, irrespective of the behaviour of the adversary. Moreover, the adversary does not learn any additional information about the inputs of the honest parties, beyond what can be revealed by the function output and the inputs of the corrupt parties. If the adversary is computationally bounded then the notion of security achieved is called conditional security (also known as cryptographic security) [42], [45], [60]. On the other hand, unconditionally secure protocols (also known as information-theoretically secure protocols) provide security against computationally unbounded adversaries [17], [28]. Unconditionally secure protocols provide ever-lasting security, as their security is not based on any computational-hardness assumptions. Moreover, compared to conditionally secure protocols, the protocols are simpler and faster by several orders of magnitude, as they are based on very simple operations, such as polynomial interpolation and polynomial evaluation over finite fields. Unconditionally secure protocols can be further categorized as perfectly-secure MPC protocols [2], [14], [17], [34], [42], [46], where all security properties are achieved in an error-free fashion. On the other hand, statistically-secure MPC protocols [12], [18], [33], [47], [58] allow for a negligible error in the achieved security properties.

Traditionally, MPC protocols are designed assuming either a synchronous or asynchronous communication model. In synchronous MPC (SMPC) protocols, parties are assumed to be synchronized with respect to a global clock and there is a publicly-known upper bound on message delays. Any SMPC protocol operates as a sequence of communication rounds where, in each round, every party performs some computation, sends messages to other parties and receives messages sent by the other parties, in that order. Consequently, if during a round a receiving party does not receive an expected message...
from a designated sender party by the end of that round, then the receiving party has the assurance that the sender party is definitely corrupt. Though the synchronous communication model is highly appealing in terms of its simplicity, in practice, it might be very difficult to guarantee such strict time-outs over the channels in real-world networks like the Internet. Such networks are better modelled through the asynchronous communication model [24].

An asynchronous MPC (AMPC) protocol operates over an asynchronous network, where the messages can be arbitrarily, yet finitely delayed. The only guarantee in this model is that every sent message is eventually delivered. Moreover, the messages need not be delivered in the same order in which they were sent. Furthermore, to model the worst-case scenario, the sequence of message delivery is assumed to be under the control of the adversary. Unlike SMPC protocols, the protocol execution in an AMPC protocol occurs as a sequence of events, which depend upon the order in which the parties receive messages. Comparatively, AMPC protocols are more challenging to design than SMPC protocols. This is because inherently, in any AMPC protocol, a receiving party cannot distinguish between a slow sender party (whose messages are arbitrarily delayed in the network) and a corrupt sender party (who does not send any messages). Consequently, in any AMPC protocol with up to \( t_a \) corruptions, at any stage of the protocol, no party can afford to receive messages from all the parties. This is because the corrupt parties may never send their messages and hence the wait could turn out to be endless. Hence, as soon as a party receives messages from any subset of \( n - t_a \) parties, it has to proceed to the next stage of the protocol. However, in this process, messages from up to \( t_a \) potentially slow, but honest parties, may get ignored. In fact, in any AMPC protocol, it is impossible to ensure that the inputs of all honest parties are considered for the computation and inputs of up to \( t_a \) (potentially honest) parties may have to be ignored, since waiting for all \( n \) inputs may turn out to be an endless wait. The advantage of AMPC protocols over SMPC protocols is that the time taken to produce the output depends upon the actual speed of the underlying network. In more detail, for an SMPC protocol, the participants have to pessimistically set the global delay \( \Delta \) on the message delivery to a large value to ensure that the messages sent by every party at the beginning of a round reach their destination within time \( \Delta \). But if the actual delay \( \delta \) in the network is such that \( \delta \ll \Delta \), then the protocol fails to take advantage of the faster network and its running time will still be proportional to \( \Delta \).

The focus of this work is perfectly-secure MPC. It is well known that perfectly-secure SMPC is possible if and only if the adversary can corrupt up to \( t_s < n/3 \) parties [17]. On the other hand, perfectly-secure AMPC is possible if and only if the adversary can corrupt up to \( t_a < n/4 \) parties [16].

**Our Motivation and Results:** As discussed above, known SMPC and AMPC protocols are designed under the assumption that the parties are aware of the exact network type. We envision a scenario where the parties are not aware of the exact network type and aim to design a single MPC protocol, which remains secure both in a synchronous, as well as an asynchronous network. We call such a protocol a best-of-both-worlds protocol, since it offers the best security properties, both in the synchronous and the asynchronous communication model. While there exist best-of-both-worlds conditionally-secure MPC protocols [22], [35], to the best of our knowledge, no prior work has ever addressed the problem of getting a best-of-both-worlds perfectly-secure MPC protocol. Motivated by this, we ask the following question:

**Is there a best-of-both-worlds perfectly-secure MPC protocol that remains secure under \( t_s \) corruptions in a synchronous network, and under \( t_a \) corruptions in an asynchronous network, where \( t_a < t_s \)?**

We show the existence of a perfectly-secure MPC protocol with the above guarantees, provided \( 3t_a + t_s < n \) holds.\(^1\)

Note that we are interested in the case where \( t_a < t_s \) as otherwise, the question is trivial to solve. More specifically, if \( t_a = t_s \), then the necessary condition of AMPC implies that \( t_a < n/4 \) holds. Hence, one can use any existing perfectly-secure AMPC protocol, which will be secure under \( t_s \) corruptions even in a synchronous network. Moreover, by ensuring appropriate time-outs, it can be guaranteed that in the protocol, the inputs of all honest parties are considered for the computation, if the network is synchronous. Our goal is to achieve a resilience strictly greater than \( n/4 \) and close to \( n/3 \), if the underlying network is synchronous. For example, if \( n = 8 \), then existing perfectly-secure SMPC protocols can tolerate up to 2 corrupt parties, while existing perfectly-secure AMPC protocols can tolerate up to 1 fault. On the other hand, using our best-of-both-worlds protocol, one can tolerate up to 2 faults in a synchronous network and up to 1 fault in an asynchronous network, even if the parties are not aware of the exact network type.

**A. Technical Overview**

We assume that the function to be securely computed is represented by some arithmetic circuit \( cir \) over a finite field \( \mathbb{F} \), consisting of linear and non-linear (multiplication) gates. Following [17], the goal is then to securely “evaluate” \( cir \) in a secret-shared fashion, such that all the values during the circuit-evaluation are \( t \)-shared as per the Shamir’s secret-sharing scheme [59], where \( t \) is the maximum number of corrupt parties.\(^2\) Intuitively, this guarantees that an adversary controlling up to \( t \) parties does not learn any additional information during the circuit-evaluation, as the shares of the corrupt parties do not reveal anything additional about the actual shared values. The degree-of-sharing \( t \) is set to \( t < n/3 \) and \( t < n/4 \) in SMPC and AMPC protocols respectively. Since, in our best-of-both-worlds protocol, the parties will not be aware of the exact network type, we need to ensure that all the values during circuit-evaluation are always secret-shared with the degree-of-sharing being \( t = t_s \), even if the network is asynchronous.

\(^1\)This automatically implies that \( t_s < n/3 \) and \( t_a < n/4 \) holds, which are necessary for designing perfectly-secure MPC protocol in a synchronous and an asynchronous network respectively.

\(^2\)A value \( s \in \mathbb{F} \) is said to be \( t \)-shared, if there is some \( t \)-degree polynomial \( f_s(\cdot) \) over \( \mathbb{F} \) with \( f_s(0) = s \) and every (honest) \( P_i \) has a distinct point on \( f_s(\cdot) \), which is called \( P_i \’s \) share of \( s \).
For shared circuit-evaluation, we follow Beaver’s paradigm [11], in which multiplication gates are evaluated using random \( t_s \)-shared multiplication-triples of the form \( (a, b, c) \), where \( c = a \cdot b \) (due to the linearity of Shamir’s secret-sharing, linear gates can be evaluated non-interactively). The shared multiplication-triples are generated in a circuit-independent preprocessing phase, using the framework of [30], which shows how to use any polynomial-based verifiable secret-sharing (VSS) [29] and a Byzantine agreement (BA) protocol [56] to generate shared random multiplication-triples. The framework works both in a synchronous as well as in an asynchronous network, where the parties are aware of the exact network type. However, there are several challenges in adapting the framework if the parties are unaware of the exact network type, which we discuss next.

a) First Challenge — A Best-of-Both-Worlds Byzantine Agreement (BA) Protocol: Informally, a BA protocol [56] allows parties with private inputs to reach an agreement on a common output (consistency), where the output is the input of the honest parties, if all honest parties participate in the protocol with the same input (validity). Perfectly-secure BA protocols can be designed tolerating \( t < n/3 \) corruptions, both in a synchronous network [56], as well as in an asynchronous network [3], [10], [26]. However, the termination (also called liveness) guarantees are different for synchronous BA (SBA) and asynchronous BA (ABA). (Deterministic) SBA protocols ensure that all honest parties obtain their output after some fixed time (guaranteed liveness). On the other hand, to circumvent the FLP impossibility result [39], ABA protocols are randomized and provide what is called almost-surely liveness [3], [10]. Namely, the parties obtain an output asymptotically with probability 1 if they continue running the protocol. SBA protocols become insecure when executed in an asynchronous network, even if a single expected message from an honest party is delayed. On the other hand, ABA protocols when executed in a synchronous network, can provide only almost-surely liveness, instead of guaranteed liveness.

The first challenge to adapt the framework of [30] in the best-of-both-worlds setting is to get a perfectly-secure BA protocol which provides security both in a synchronous as well as in an asynchronous network. Namely, apart from providing the consistency and validity properties in both types of networks, the protocol should provide guaranteed liveness in a synchronous network and almost-surely liveness in an asynchronous network. We are not aware of any BA protocol with the above properties. Hence, we present a perfectly-secure BA protocol tolerating \( t < n/3 \) corruptions, with the above properties. Since our BA protocol is slightly technical, we defer the details to Section III.

b) Second Challenge — A Best-of-Both-Worlds VSS Protocol: Informally, in a polynomial-based VSS protocol, there exists a designated dealer \( D \) with a \( t \)-degree polynomial, where \( t \) is the maximum number of corrupt parties, possibly including \( D \). The protocol allows \( D \) to distribute points on this polynomial to the parties in a “verifiable” fashion, such that the view of the adversary remains independent of \( D \)’s polynomial for an honest \( D \). In a synchronous VSS (SVSS) protocol, every party has the correct point after some known time-out, say \( T \) (correctness property). The verifiability guarantees that even a corrupt \( D \) is bound to distribute points on some \( t \)-degree polynomial within time \( T \) (strong-commitment property). Perfectly-secure SVSS is possible if and only if \( t < n/3 \) [37]. For an asynchronous VSS (AVSS) protocol, the correctness property guarantees that when \( D \) is honest, the honest parties eventually receive points on \( D \)’s polynomial. However, a corrupt \( D \) may not invoke the protocol in the first place and the parties cannot distinguish this scenario from the case when \( D \)’s messages are arbitrarily delayed. This is unlike the strong-commitment of SVSS where, if the parties do not obtain an output within time \( T \), then the parties publicly conclude that \( D \) is corrupt. Hence, the strong-commitment of AVSS guarantees that if \( D \) is corrupt and if some honest party obtains a point on \( D \)’s polynomial, then all honest parties eventually obtain their respective points on this polynomial. Perfectly-secure AVSS is possible if and only if \( t < n/4 \) [4], [16].

Existing SVSS protocols [27], [40], [41], [49] become completely insecure in an asynchronous network, even if a single expected message from an honest party is delayed. On the other hand, existing AVSS protocols [13], [16], [27], [54] only work when \( D \)’s polynomial has degree \( t < n/4 \) and become insecure if there are more than \( n/4 \) corruptions (which can happen in our context, if the network is synchronous).

The second challenge to adapt the framework of [30] in our setting is to get a perfectly-secure VSS protocol, which provides security against \( t_s \) and \( t_a \) corruptions in a synchronous and in an asynchronous network respectively, where \( D \)’s polynomial is always a \( t_s \)-degree polynomial, irrespective of the network type. We are not aware of any VSS protocol with these guarantees. We present a best-of-both-worlds perfectly-secure VSS protocol satisfying the above properties, provided \( 3t_s + t_a < n \) holds. Our VSS protocol satisfies the correctness requirement of SVSS and AVSS in a synchronous and an asynchronous network respectively. However, it only satisfies the strong-commitment requirement of AVSS, even if the network is synchronous. This is because a potentially corrupt \( D \) may not invoke the protocol and the parties will not be aware of the exact network type. We stress that this does not hinder us from deploying our VSS protocol in the framework of [30]. Since our VSS protocol is slightly technical, we defer the details to Section IV.

B. Related Work

Best-of-both-worlds protocols have been studied very recently. The work of [20] shows that the condition \( 2t_s + t_a < n \) is necessary and sufficient for best-of-both-worlds conditionally-secure BA, tolerating computationally bounded adversaries. Using the same condition, the works of [22] and [35] present conditionally-secure MPC protocols. Moreover, the same condition has been used in [21] to design a best-of-both-worlds protocol for atomic broadcast (a.k.a. state machine

3Hence the protocol allows \( D \) to generate a \( t \)-sharing of the constant term of the polynomial, which is also called as \( D \)’s secret.
repetition). Furthermore, the same condition has been used recently in [43] to design a best-of-both-worlds approximate agreement protocol against computationally-bounded adversaries.

A recent work [36] has studied the problem of perfectly-secure message transmission (PSMT) [37] over incomplete graphs, in the best-of-both-worlds setting. Along with the results in this paper, they note that best-of-both-worlds protocols— a protocol with quadratic communication complexity. Recently, they also provide a conditionally-secure protocols - a protocol with quadratic communication complexity. Recently, in a follow-up paper [6], we extend our results in this paper to the setting of non-threshold (general) adversaries [48].

A common principle used in [22] and [35] to design best-of-both-worlds MPC protocols is to have two different MPC protocols - a synchronous protocol \( \Pi_{\text{SMPC}} \) with threshold \( t_s \) which also provides certain security guarantees in an asynchronous environment while tolerating \( t_a \) corruptions, and an asynchronous MPC protocol \( \Pi_{\text{AMPC}} \) with threshold \( t_a \). The idea is then to first run the protocol \( \Pi_{\text{SMPC}} \) assuming a synchronous network. After the known “time-out” of the synchronous protocol, the parties decide and agree on whether any output has been obtained from the protocol \( \Pi_{\text{SMPC}} \). If the network is synchronous, then the parties will definitely obtain their desired output by this time-out and will agree to terminate with the output obtained from \( \Pi_{\text{SMPC}} \). However, in case the parties do not obtain an output (implying that the network is asynchronous), the parties decide to run the protocol \( \Pi_{\text{AMPC}} \) to obtain the desired output. This means that if the network is asynchronous, then the parties may end up evaluating the underlying circuit twice. Our MPC protocol does not follow this design principle. Rather, the parties need to evaluate the circuit only once, irrespective of the network type.

II. PRELIMINARIES AND DEFINITIONS

We follow the pairwise secure-channel model, where the parties in \( \mathcal{P} = \{ P_1, \ldots, P_n \} \) are connected by pairwise private and authentic channels. The distrust in the system is modelled by a computationally unbounded Byzantine (malicious) adversary \( \text{Adv} \), who can corrupt a subset of the parties and force them to behave in any arbitrary fashion during the execution of a protocol. We assume a static adversary, who decides the set of corrupt parties at the beginning of the protocol execution. The underlying network can be synchronous or asynchronous, with parties being unaware of the exact type. In a synchronous network, every sent message is delivered in the same order, within some known fixed time \( \Delta \). The adversary \( \text{Adv} \) can control up to \( t_s \) parties in a synchronous network.

In an asynchronous network, messages are sent with an arbitrary, yet finite, delay and need not be delivered in the same order. The only guarantee is that every message sent is eventually delivered. The exact sequence of message delivery is decided by a scheduler and, to model the worst-case scenario, the scheduler is assumed to be under the control of \( \text{Adv} \). The adversary can control up to \( t_a \) parties in an asynchronous network.

We assume that \( t_a < t_s \) and \( 3t_s + t_a < n \) holds. This automatically implies that \( t_a < n/3 \) and \( t_a < n/4 \) hold, which are necessary for any SMPC and AMPC protocol respectively. All computations in our protocols are done over a finite field \( \mathbb{F} \), where \( |\mathbb{F}| > 2n \) and where \( \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \) are publicly-known, distinct, non-zero elements from \( \mathbb{F} \). For simplicity and without loss of generality, we assume that each \( P_i \) has a private input \( x^{(i)} \in \mathbb{F} \), and that the parties want to securely compute a function \( f : \mathbb{F}^n \rightarrow \mathbb{F} \). Without loss of generality, \( f \) is represented by an arithmetic circuit \( cir \) over \( \mathbb{F} \) consisting of linear and non-linear (multiplication) gates [44], where \( cir \) has \( c_M \) number of multiplication gates and has a multiplicative depth of \( D_M \).

On the Security Definition and Adversarial Model Used in Our Protocols: In the literature, there are two main approaches used to define the security of unconditionally-secure protocols, a property-based approach and a simulation-based approach. In the former, security is defined by enumerating a list of desired properties. The main properties which are desired are correctness (meaning that the output of the computation is correct) and privacy (meaning that the adversary cannot obtain any additional information about the honest parties’ inputs, other than what can be inferred from the corrupted parties’ inputs and outputs). A list of other desired properties, such as input independence (meaning that the corrupt parties cannot decide their inputs based on the outputs of the honest parties) can be found in [52]. In the latter approach [25], the security of a protocol \( \Pi \) is defined more precisely and rigorously with respect to a so-called ideal-specification (also called as ideal-world), which is a protocol between the protocol participants and a trusted third party (TTP) who performs the actual computation. The goal of \( \Pi \) is the simulation of the trusted party. We say that protocol \( \Pi \) securely implements a given specification if the protocol achieves the same as the specification and the adversary cannot achieve more than what it could achieve in the specification.

In this paper, we keep the formalisms to a minimum and prove the security of our protocols using the property-based approach. This is to prevent deviating from the main focus of the paper (which is to show the existence of a perfectly-secure best-of-both-worlds MPC protocol), since proving the security according to the simulation paradigm will bring in additional technicalities (especially to deal with two different types of networks) and which will make the protocols unreadable. However, we confirm that our protocols can be proved to be secure in the simulation paradigm as well, without affecting its efficiency, by using standard ideas from the literature (see for instance [8], [31]).

Similarly, for simplicity, we consider static adversaries. However, we confirm that our protocols can be proved to be

---

Footnote: We stress that even though simulation-based security is preferred in the context of MPC, there are other definitional frameworks which can be explored for proving the security of cryptographic protocols. For instance, [50] shows how to cast property-based definitions into existing composable frameworks, achieving composable guarantees.
secure even against a more powerful adaptive adversary, who decides the set of corrupt parties at run time.

**Termination Guarantees of Our Sub-Protocols:** For simplicity, we will not be specifying any termination criteria for our sub-protocols. The parties will keep on participating in these sub-protocol instances even after receiving their outputs. The termination criteria of our MPC protocol will ensure that once a party terminates the MPC protocol, it terminates all underlying sub-protocol instances. We will use existing randomized ABA protocols which ensure that the honest parties obtain some output almost-surely. This means that the probability that an honest party obtains its output after participating for infinitely many rounds approaches 1 asymptotically [3], [10], [53]. That is:

$$\lim_{T \to \infty} \Pr[\text{An honest } P_i \text{ obtains its output by local time } T] = 1,$$

where the probability is over the random coins of the honest parties and the adversary in the protocol. The property of almost-surely obtaining the output carries over to the “higher” level protocols, where ABA is used as a building block. We will say that the “honest parties obtain some output almost-surely from (an asynchronous) protocol II” to mean that every honest $P_i$ asymptotically obtains its output in $\Pi$ with probability 1, in the above sense.

We next discuss the properties of polynomials over $\mathbb{F}$, which are used in our protocols.

**Polynomials Over a Field:** A $d$-degree univariate polynomial over $\mathbb{F}$ is of the form

$$f(x) = a_0 + \ldots + a_d x^d,$$

where each $a_i \in \mathbb{F}$. An $(\ell, \ell)$-degree symmetric bivariate polynomial over $\mathbb{F}$ is of the form

$$F(x, y) = \sum_{i,j=0}^{i=\ell, j=\ell} r_{ij} x^i y^j,$$

where each $r_{ij} \in \mathbb{F}$ and $r_{ij} = r_{ji}$ holds for all $i, j$. This automatically implies that $F(\alpha, \alpha) = F(\alpha, \alpha)$ holds, for all $\alpha_i, \alpha_j$. Moreover, $F(x, \alpha_i) = F(x, \alpha_i)$ also holds, for every $\alpha_i$. Given an $i \in \{1, \ldots, n\}$ and an $\ell$-degree polynomial $F_i(x)$, we say that $F_i(x)$ lies on an $(\ell, \ell)$-degree symmetric bivariate polynomial $F(x, y)$, if $F(x, \alpha_i) = F_i(x)$ holds.

We now state some standard results related to polynomials over $\mathbb{F}$. It is a well-known fact that there always exists a unique $d$-degree univariate polynomial, passing through $d + 1$ distinct points. A generalization of this result for bivariate polynomials is that if there are “sufficiently many” univariate polynomials which are “pair-wise consistent”, then together they lie on a unique bivariate polynomial. Formally:

**Lemma II.1 ([8], [32]):** Let $f_i(x), \ldots, f_m(x)$ be $\ell$-degree univariate polynomials over $\mathbb{F}$, where $q \geq \ell + 1$ and $i_1, \ldots, i_q \in \{1, \ldots, n\}$, such that $f_{i_1}(\alpha_1) = f_{i_2}(\alpha_1)$ holds for all $i, j \in \{1, \ldots, q\}$. Then $f_{i_1}(x), \ldots, f_{i_q}(x)$ lie on a unique $(\ell, \ell)$-degree symmetric bivariate polynomial, say $F^*(x, y)$.

In existing (as well as our) VSS protocols, D, on having a $t$-degree polynomial $q(\cdot)$ as input, embeds $q(\cdot)$ into a random $(t, t)$-degree symmetric bivariate polynomial $F(x, y)$ at $x = 0$. Each party $P_i$ then receives the $t$-degree univariate polynomial $f_i(x) = F(x, \alpha_i)$. Here $t$ is the maximum number of parties which can be under the control of Adv. This ensures that Adv, by learning at most $t$ polynomials lying on $F(x, y)$, does not learn anything about $F(0, 0)$. Intuitively, this is because Adv will fall short of at least one point on $F(x, y)$ to uniquely interpolate it. In fact, it can be shown that for every pair of $t$-degree polynomials $q_1(\cdot), q_2(\cdot)$ such that $q_1(\alpha_i) = q_2(\alpha_i) = f_i(0)$ holds for every $P_i \in C$ (where $C$ is the set of parties under Adv), the distribution of the polynomials $\{f_i(x)\}_{P_i \in C}$ when $F(x, y)$ is chosen based on $q_1(\cdot)$ is identical to the distribution when $F(x, y)$ is chosen based on $q_2(\cdot)$.

Formally: **Lemma II.2 ([8], [32]):** Let $C \subseteq P$ and $q_1(\cdot) \neq q_2(\cdot)$ be $d$-degree polynomials where $d \geq |C|$ such that $q_1(\alpha_i) = q_2(\alpha_i)$ for all $P_i \in C$. Then the probability distributions $\{\{F(x, \alpha_i)\}_{P_i \in C}\}$ and $\{\{F'(x, \alpha_i)\}_{P_i \in C}\}$ are identical, where $F(x, y)$ and $F'(x, y)$ are random $(d, d)$-degree symmetric bivariate polynomials, such that $F(0, y) = q_1(\cdot)$ and $F'(0, y) = q_2(\cdot)$ holds.

We next give the definition of $d$-sharing, which is central to our protocols.

**Definition II.3 (d-Sharing):** A value $s \in \mathbb{F}$ is said to be $d$-shared, if there exists a $d$-degree sharing-polynomial, say $f_s(\cdot)$, with $f_s(0) = s$, such that every (honest) $P_i$ has the share $s_i = f_s(\alpha_i)$. The vector of shares of $s$ corresponding to the (honest) parties $P_i$ is called a $d$-sharing of $s$, denoted by $[s]_d$. We will omit the degree $d$ from the notation $[\cdot]$ if it is clear from the context.

It is easy to see that $d$-sharing satisfies the linearity property; i.e. given $[a]_d$ and $[b]_d$, then $[c_1 \cdot a + c_2 \cdot b]_d = c_1 \cdot [a]_d + c_2 \cdot [b]_d$ holds, where $c_1, c_2 \in \mathbb{F}$ are publicly-known. In general, consider any arbitrary linear function $g : \mathbb{F}^\ell \to \mathbb{F}^{m}$ and let $u^{(1)}, \ldots, u^{(t)}$ be $d$-shared. When we say that parties locally compute $([v^{(1)}], \ldots, [v^{(m)}]) = g([u^{(1)}], \ldots, [u^{(t)}])$, we mean that the parties locally apply the function $g$ on their respective shares of $u^{(1)}, \ldots, u^{(t)}$, to get their respective shares of $v^{(1)}, \ldots, v^{(m)}$.

A. Existing Primitives

We next discuss the existing primitives used in our protocols.

a) **Online Error-Correction (OEC) [16]:** Let $P'$ be a subset of parties, containing at most $t$ corrupt parties. Let there exist some $d$-degree polynomial $q(\cdot)$ with every (honest) $P_i \in P'$ having a point $q(\alpha_i)$. The goal is to make some designated party, say $P_R$, reconstruct $q(\cdot)$. For this, each $P_i \in P'$ sends $q(\alpha_i)$ to $P_R$, who keeps waiting till it receives $d + t + 1$ points, all of which lie on a unique $d$-degree polynomial. This step requires $P_R$ to repeatedly apply the Reed-Solomon (RS) error-correction procedure [51] and try to recover $q(\cdot)$, upon receiving a new point from the parties in $P'$. Once $P_R$ receives $d + t + 1$ points lying on a $d$-degree polynomial, say $q'(\cdot)$, then $q'(\cdot) = q(\cdot)$. This is because among these $d + t + 1$ points, at least $d + 1$ are from honest parties in $P'$, which uniquely determine $q(\cdot)$. If $d < \lfloor |P'|-2t \rfloor$, then, in an asynchronous network, $P_R$ eventually receives $d + t + 1$ points (from the honest parties in $P'$) lying on $q(\cdot)$ and recovers $q(\cdot)$. Moreover, in a synchronous network, it will
take at most $\Delta$ time for $P_n$ to recover $q(\cdot)$, since the points of the honest parties will be delivered within $\Delta$ time. We denote the above procedure by $OEC(d, t, F)$, which is presented in Appendix A, along with its properties.

b) Finding $(n, t)$-star [16]: Let $G$ be an undirected graph over $P$. Then a pair $(\mathcal{E}, \mathcal{F})$ where $\mathcal{E} \subseteq \mathcal{F} \subseteq P$ is called an $(n, t)$-star, if all the following hold:
- $|\mathcal{E}| \geq n - 2t$;
- $|\mathcal{F}| \geq n - t$;
- There exists an edge between every $P_i \in \mathcal{E}$ and every $P_j \in \mathcal{F}$.

The work of [16] presents an efficient algorithm (whose running time is polynomial in $n$), which we denote as $\text{asgStar}$. The algorithm always outputs an $(n, t)$-star $(\mathcal{E}, \mathcal{F})$, provided $G$ contains a clique of size at least $n - t$.

c) Asynchronous Reliable Broadcast (Acast): We use Bracha’s Acast protocol [23] where there exists a designated sender $S \in P$ with input $m \in \{0, 1\}^t$. The protocol allows $S$ to send $m$ identically to all the parties, in the presence of any $t < n/3$ corruptions, possibly including $S$. While the protocol has been primarily designed for an asynchronous network, it also provides certain guarantees in a synchronous network, as stated in Lemma II.4. Notice that the protocol does not provide any liveness if $S$ is corrupt, irrespective of the network type. This is because a corrupt $S$ may not invoke the protocol in the first place. Moreover, in a synchronous network, if $S$ is corrupt and if the honest parties compute an output, then they may not get the output at the same time. More precisely, the times at which honest parties obtain their outputs may differ by at most $2\Delta$. The Acast protocol and proof of Lemma II.4 are available in Appendix A.

Lemma II.4: Bracha’s Acast protocol $\Pi_{\text{Acast}}$ achieves the following in the presence of up to $t < n/3$ corruptions, where $S$ has an input $m \in \{0, 1\}^t$ for the protocol:
- Asynchronous Network:
  - (a) $t$-Liveness: If $S$ is honest, then all honest parties eventually obtain an output.
  - (b) $t$-Validity: If $S$ is honest, then every honest party with an output, outputs $m$.
  - (c) $t$-Consistency: If $S$ is corrupt and some honest party outputs $m^*$, then every honest party eventually outputs $m^*$.
- Synchronous Network:
  - (a) $t$-Liveness: If $S$ is honest, then all honest parties obtain an output within time $3\Delta$.
  - (b) $t$-Validity: If $S$ is honest, then every honest party with an output, outputs $m$.
  - (c) $t$-Consistency: If $S$ is corrupt and some honest party outputs $m^*$ at time $T$, then every honest $P_i$ outputs $m^*$ by the end of time $T + 3\Delta$.
- Irrespective of the network type, $O(n^2t)$ bits are communicated by the honest parties.

We next discuss few terminologies with respect to $\Pi_{\text{Acast}}$, which we use throughout the paper.

Terminologies for Using $\Pi_{\text{Acast}}$: We will say that “$P_i$ Acasts $m$” to mean that $P_i$ acts as a sender $S$ and invokes an instance of $\Pi_{\text{Acast}}$ with input $m$ and the parties participate in this instance. Similarly, we will say that “$P_j$ receives $m$ from the Acast of $P_i$” to mean that $P_j$ outputs $m$ in the corresponding instance of $\Pi_{\text{Acast}}$.

III. Best-of-Both-Worlds Perfectly-Secure Byzantine Agreement

In this section, we present our best-of-both-worlds perfectly-secure Byzantine agreement (BA) protocol. We begin with the definition of BA, which is a modified version of [20], as we do not require any termination guarantees. In the definition, we consider the case where the inputs of the parties are a single bit. However, the definition can be easily extended for the case when the inputs are bit strings.

Definition III.1 (Byzantine Agreement (BA) [20]): Let $\Pi$ be a protocol for the parties in $\mathcal{P}$ with up to $t$ corrupt parties, where every $P_i$ has an input $b_i \in \{0, 1\}$ and a possible output from $\{0, 1, \bot\}$.
- $t$-Guaranteed Liveness: $\Pi$ has $t$-guaranteed liveness if all honest parties obtain an output.
- $t$-Almost-Surely Liveness: $\Pi$ has $t$-almost-surely liveness if, almost-surely, all honest parties obtain some output.
- $t$-Validity: $\Pi$ has $t$-validity, if the following hold: if all honest parties have input $b$, then every honest party with an output, outputs $b$.
- $t$-Weak Validity: $\Pi$ has $t$-weak validity, if the following hold: if all honest parties have input $b$, then every honest party with an output, outputs $b$ or $\bot$.
- $t$-Consistency: $\Pi$ has $t$-consistency, if all honest parties with an output, output the same value.
- $t$-Weak Consistency: $\Pi$ has $t$-Weak Consistency, if all honest parties with an output, output either a common $v \in \{0, 1\}$ or $\bot$.

Protocol II is called a $t$-perfectly-secure synchronous-BA (SBA) protocol, if in a synchronous network, it achieves all the following:
- $t$-guaranteed liveness;
- $t$-Validity;
- $t$-Consistency.
Protocol II is called a $t$-perfectly-secure asynchronous-BA (ABA) protocol, if in an asynchronous network, it achieves the following:
- $t$-almost-surely liveness;
- $t$-Validity;
- $t$-Consistency.

To design our best-of-both-worlds BA protocol, we will be using an existing perfectly-secure SBA and a perfectly-secure ABA protocol, whose properties we review next.

a) Existing $t$-Perfectly-Secure SBA: We assume the existence of a $t$-perfectly-secure SBA protocol tolerating $t < n/3$ corruptions, which also provides $t$-guaranteed liveness in an asynchronous network.\footnote{We stress that we do not require any other property from the SBA protocol in an asynchronous network.} For the sake of communication efficiency, we choose the recursive phase-king based $t$-perfectly-secure SBA protocol $\Pi_{BGP}$ of [19]. The protocol incurs a communication of $O(n^2\ell)$ bits, if the inputs of the parties are of size $\ell$ bits. If the network is synchronous, then in protocol $\Pi_{BGP}$, at time $T_{BGP} = (12n - 6) \cdot \Delta$, all honest parties

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
have an output (see Lemma 10.7 of [1]). To ensure guaranteed liveness in an asynchronous network, the parties can simply run the protocol and then check if any output is obtained at local time \((12n - 6) \cdot \Delta\). In case no output is obtained, then \(\bot\) is taken as the output. The properties of \(\Pi_{BGP}\) are summarized in Lemma III.2.

**Lemma III.2 ([1], [19]):** Let \(t < n/3\). Then there exists a protocol \(\Pi_{BGP}\) with the following properties, where all parties participate with an input of size \(\ell\) bits.

- The protocol incurs a communication of \(O(n^2 \ell)\) bits from the honest parties.
- The protocol is a \(t\)-perfectly-secure SBA protocol, where all honest parties have an output within time \(T_{BGP} = (12n - 6) \cdot \Delta\).
- In an asynchronous network, all honest parties have an output from \(\{0, 1\}^\ell \cup \{\bot\}\), within local time \((12n - 6) \cdot \Delta\).

b) **Existing \(t\)-Perfectly-Secure ABA:** Existing perfectly-secure ABA protocols achieve the following properties.

**Lemma III.3 ([3], [10]):** Let \(t < n/3\). Then there exists a randomized protocol \(\Pi_{ABA}\), achieving the following properties, where the input of each party is a bit.

- **Asynchronous Network:** The protocol is a \(t\)-perfectly-secure ABA protocol and provides the following liveness guarantees.
  - If the inputs of all honest parties are same, then \(\Pi_{ABA}\) achieves \(t\)-guaranteed liveness;
  - Else \(\Pi_{ABA}\) achieves \(t\)-almost-surely liveness.
- **Synchronous Network:** The protocol achieves \(t\)-validity, \(t\)-consistency and the following liveness guarantees.
  - If the inputs of all honest parties are same, then \(\Pi_{ABA}\) achieves \(t\)-guaranteed liveness and all honest parties obtain their output within time \(T_{ABA} = k \cdot \Delta\) for some constant \(k\).
  - Else \(\Pi_{ABA}\) achieves \(t\)-almost-surely liveness and requires \(\mathcal{O}(\text{poly}(n) \cdot \Delta)\) expected time to generate the output.
  - Irrespective of the network type, the protocol incurs the following amount of communication from the honest parties.
  - If the inputs of all honest parties are the same, then the protocol incurs a communication of \(\mathcal{O}(\text{poly}(n) \log |F|)\) bits;
  - Else, it incurs an expected communication of \(\mathcal{O}(\text{poly}(n) \log |F|)\) bits.\(^6\)

Protocol \(\Pi_{ABA}\) is designed using a weaker “variant” of AVSS called *shunning AVSS (SAVSS)* [3], [10], which cannot be used for circuit-evaluation. We provide a brief overview of the ABA protocols of [3] and [10] and a brief outline of the proof of Lemma III.3 in Appendix B.

From the above discussion, we note that protocol \(\Pi_{ABA}\) cannot be considered as a best-of-both-worlds BA protocol. This is because the protocol achieves \(t\)-guaranteed liveness in a synchronous network, only when all honest parties have the same input. In case the parties have a mixed bag of inputs, then the parties may end up running the protocol forever without obtaining an output, even if the network is synchronous. However, the probability of this event is asymptotically 0. We design a perfectly-secure BA protocol, which solves this problem and which is secure in any network. To design the protocol, we need a special type of broadcast protocol, which we design first.

### A. Synchronous Broadcast With Asynchronous Guarantees

We begin with the definition of broadcast, adapted from [20], where we do not put any termination requirement.

**Definition III.4 (Broadcast [20]):** Let \(\Pi\) be a protocol for the parties in \(\mathcal{P}\) consisting of up to \(t\) corrupt parties, where a sender \(S \in \mathcal{P}\) has input \(m \in \{0, 1\}^\ell\), and parties obtain a possible output from \(\{0, 1\}^\ell \cup \{\bot\}\).

- **t-Liveness:** \(\Pi\) has \(t\)-liveness, if all honest parties obtain some output.
- **t-Validity:** \(\Pi\) has \(t\)-validity, if the following holds: if \(S\) is honest, then every honest party with an output, outputs \(m\).
- **t-Weak Validity:** \(\Pi\) has \(t\)-validity, if the following holds: if \(S\) is honest, then every honest party outputs either \(m\) or \(\bot\).
- **t-Consistency:** \(\Pi\) has \(t\)-consistency, if the following holds: if \(S\) is corrupt, then every honest party with an output, has a common output.
- **t-Weak Consistency:** \(\Pi\) has \(t\)-weak consistency, if the following holds: if \(S\) is corrupt, then every honest party with an output, outputs a common \(m^* \in \{0, 1\}^\ell\) or \(\bot\).

Protocol \(\Pi\) is called a \(t\)-perfectly-secure broadcast protocol, if it has the following properties:

- **t-Liveness**;
- **t-Validity**;
- **t-Consistency**.

We next design a special broadcast protocol \(\Pi_{BC}\), which is a \(t\)-perfectly-secure broadcast protocol in a synchronous network. Additionally, in an asynchronous network, the protocol achieves \(t\)-liveness, \(t\)-weak validity and \(t\)-weak consistency. Looking ahead, we will combine the protocols \(\Pi_{BC}, \Pi_{BGP}\) and \(\Pi_{ABA}\) to get our best-of-both-worlds BA protocol.

Before proceeding to design \(\Pi_{BC}\), we note that the existing Bracha’s Acast protocol \(\Pi_{Acast}\) does not guarantee the same properties as \(\Pi_{BC}\). Specifically, for a corrupt \(S\), there is no liveness guarantee (irrespective of the network type). Moreover, in a synchronous network, if \(S\) is corrupt and honest parties obtain an output, then they may not obtain an output within the same time (see Lemma II.4).\(^7\) Interestingly, our instantiation of \(\Pi_{BC}\) is based on \(\Pi_{Acast}\), by carefully “stitching” it with the protocol \(\Pi_{BGP}\).

The idea behind \(\Pi_{BC}\) is the following: sender \(S\) first Acasts its message. If the network is synchronous and \(S\) is honest, then within time \(3\Delta\), every honest party should have received \(S\)’s message. To verify this, the parties start participating in an instance of \(\Pi_{BGP}\) at (local) time \(3\Delta\), with their respective inputs being the output obtained from \(S\)’s Acast at time \(3\Delta\). If there is no output at time \(3\Delta\) from \(S\)’s Acast, then the input for \(\Pi_{BGP}\) is \(\bot\). Finally, at time \(3\Delta + T_{BGP}\), parties output \(m^*\),

\(\text{Looking ahead}, \text{this property from } \Pi_{BC} \text{ will be crucial when we use it in our best-of-both-worlds BA protocol.}\)
if it has been received from the Acast of S and if it is the output of Π_BGP as well; otherwise the parties output ⊥.

It is easy to see that the protocol has now guaranteed liveness in any network (irrespective of S), since all parties will have some output at (local) time $3Δ + T_{BGP}$. Moreover, consistency is achieved for a corrupt S in a synchronous network, with all honest parties obtaining a common output at the same time. This is because if any honest party obtains an output $m^* \neq ⊥$ at time $3Δ + T_{BGP}$, then at least one honest party must have received $m^*$ from S’s Acast by time $3Δ$. And so by time $3Δ + T_{BGP}$, all honest parties will receive $m^*$ from S’s Acast.

**Eventual Consistency and Validity in Asynchronous Network:** In Π_BG, the parties set a “time-out” of $3Δ + T_{BGP}$, due to which it provides weak validity and weak consistency in an asynchronous network. This is because some honest parties may receive S’s message from the Acast of S within the timeout, while others may fail to do so. The time-out is essential, as we need liveness from Π_BG in both synchronous and asynchronous network, when Π_BG is used later in our best-of-both-worlds BA protocol.

Looking ahead, we will use Π_BG in our VSS protocol as a broadcast protocol. Due to the weak validity and weak consistency properties, we may end up in a scenario where one subset of honest parties may output a common value different from ⊥ at the end of the time-out, while others may output ⊥. For the security of the VSS protocol, we would require even the latter subset of (honest) parties to eventually output the common non-⊥ value, if the parties continue participating in Π_BG. To achieve this goal, every party who outputs ⊥ at time $3Δ + T_{BGP}$, “switches” its output to $m^*$, if it eventually receives $m^*$ from S’s Acast. We stress that this switching is only for the parties who obtained ⊥ at time $3Δ + T_{BGP}$. To differentiate between the two ways of obtaining output, we use the terms regular-mode and fallback-mode. The regular-mode refers to the process of deciding the output at time $3Δ + T_{BGP}$, while the fallback-mode refers to the process of deciding the output beyond time $3Δ + T_{BGP}$.

If the network is asynchronous and S is honest, then from the liveness and validity of Π_Acast, every honest party eventually obtains m from S’s Acast. Hence, through the fallback-mode, every honest party who outputs ⊥ at the time-out of $3Δ + T_{BGP}$ eventually outputs m. Moreover, even if S is corrupt, the fallback-mode will not lead to different honest parties obtaining different non-⊥ outputs due to the consistency property of Π_Acast.

We next prove the properties of the protocol Π_BG.

**Theorem III.5:** Protocol Π_BG achieves the following properties in the presence of any $t < n/3$ corruptions, where S has an input $m \in \{0, 1\}^t$ and where $T_{BGP} = (12n - 3) \cdot Δ$.

- (a) t-Liveness: At local time $T_{BC}$, every honest party has an output, through regular-mode.
- (b) t-Validity: If S is honest, then at time $T_{BC}$, each honest party outputs m through regular-mode.
- (c) t-Consistency: If S is corrupt, then the output of every honest party is the same at time $T_{BC}$ through regular-mode.
- (d) t-Fallback Consistency: If S is corrupt and some honest party outputs $m^* \neq ⊥$ at time T through fallback-mode, then every honest party outputs $m^*$ by time $T + 2Δ$ through fallback-mode.

**Asynchronous Network:**

- (a) t-Liveness: At local time $T_{BC}$, every honest party has an output through regular-mode.
- (b) t-Weak Validity: If S is honest, then at local time $T_{BC}$, each honest party outputs m or ⊥ through regular-mode.
- (c) t-Fallback Validity: If S is honest, then each honest party who outputs ⊥ at local time $T_{BC}$ through regular-mode eventually outputs m through fallback-mode.
- (d) t-Weak Consistency: If S is corrupt, then at local time $T_{BC}$, each honest party outputs either a common $m^* \neq ⊥$ or ⊥ through regular-mode.
- (e) t-Fallback Consistency: If S is corrupt and some honest party outputs $m^* \neq ⊥$ at local time T, either through regular or fallback-mode, then every honest party eventually outputs $m^*$, either through regular or fallback-mode.

Irrespective of the network type, the protocol incurs a communication of $O(n^2t)$ bits from the honest parties.

**Proof:** The liveness (both for the synchronous as well asynchronous network) simply follows from the fact that every honest party outputs something (including ⊥) at (local) time $T_{BC} = 3Δ + T_{BGP}$, where $T_{BGP} = (12n - 6) \cdot Δ$. We next prove the rest of the properties of the protocol in the synchronous.

---

*The fallback-mode is never triggered when Π_BG is used in our best-of-both-worlds BA protocol. It will be triggered (along with the regular-mode) in our VSS protocol.*
network, for which we rely on the properties of Acast and Π_{BGP} in the synchronous network.

If S is honest, then due to the liveness and validity properties of Π_{Acast} in the synchronous network, at time 3∆, every honest party P_i receives m from the Acast of S. Hence, every honest party participates with input m in the instance of Π_{BGP}. From the guaranteed liveness and validity properties of Π_{BGP} in synchronous network, at time 3∆ + T_{BGP}, every honest party will have m as the output from Π_{BGP}. Hence, each honest party has the output m at time T_{BC}, thus proving that validity is achieved.

For consistency, we consider a corrupt S. We first note that each honest party will have the same output from the instance of Π_{BGP} at time T_{BC}, which follows from the consistency property of Π_{BGP} in synchronous network. If all honest parties have the output m for Π_{BGP} at time T_{BC}, then consistency holds trivially. So consider the case when some honest party, say P_i, has the output m' ≠ m for Π_{BGP} at time T_{BC}. This implies that the output of Π_{BGP} is m' for every honest party. Moreover, it also implies that at time 3∆, at least one honest party, say P_h, has received m' from the Acast of S. Otherwise, all honest parties would participate with input m in the instance of Π_{BGP} and, from the validity of Π_{BGP} in the synchronous network, every honest party would compute m as the output during Π_{BGP}, which is a contradiction. Since P_h has received m' from S’s Acast at time 3∆, it follows from the consistency property of Π_{Acast} in the synchronous network that all honest parties will receive m' from S’s Acast at time 5∆. Moreover, 5∆ < (12n−3)·∆ holds. Consequently, by time (12n−3)·∆, all honest parties will receive m' from S’s Acast and will have m as the output of Π_{BGP} and hence, output m' for Π_{BGP}.

For fallback consistency, we have to consider a corrupt S. Let P_h be an honest party who outputs m' ≠ m at time T through fallback-mode. Since the steps of fallback-mode are executed after time T_{BC}, it follows that T > T_{BC}. We first note that this implies that every honest party has output m at time T_{BC} through regular-mode. This is because, from the proof of the consistency property of Π_{BGP}, if any honest party has an output m' ≠ m at time T_{BC}, then all honest parties (including P_h) also must have computed the output m' at time T_{BC}, through regular-mode. And hence, P_h will never change its output to m'. Since P_h has computed the output m', it means that at time T, it has received m' from the Acast of S. It then follows from the consistency of Π_{Acast} in the synchronous network that every honest party will also receive m' from the Acast of S, latest by time T + 2∆ and output m' through fallback-mode.

We next prove the properties of the protocol Π_{BC} in an asynchronous network, for which we depend upon the properties of Π_{Acast} in the asynchronous network. The weak-validity property follows from the validity property of Π_{Acast} in the asynchronous network, which ensures that no honest party P_i ever receives an m' from the Acast of S where m' ≠ m. So if at all P_i outputs a value different from m at time T_{BC}, it has to be m. The weak-consistency property follows using arguments similar to what was used to prove consistency in the synchronous network, but relying instead on the validity and consistency properties of Π_{Acast} in the asynchronous network. The latter property ensures that even if the adversary has full control over message scheduling in the asynchronous network, it cannot ensure that for a corrupt S, two different honest parties end up receiving m_1 and m_2 from the Acast of S, where m_1 ≠ m_2.

For fallback validity, consider an honest S and let P_i be an honest party who outputs m' at time T where T ≥ T_{BC}. This implies that P_j has obtained m' from the Acast of S. Now, consider an arbitrary honest P_i. From the liveness and weak consistency properties of Π_{BC} in asynchronous network, it follows that P_i outputs either m' or m at local time T_{BC}, through the regular-mode. If P_i has output m, then from the consistency property of Π_{Acast} in the asynchronous network, it follows that P_i will also eventually obtain m' from the Acast of S through the fallback-mode of Π_{BC}. Consequently, party P_i eventually changes its output from m to m'.

The communication complexity follows from the communication complexity of Π_{BGP} and Π_{Acast}.

We next discuss a few terminologies for Π_{BC}, which we use in the rest of the paper.

Terminologies for Π_{BC}: When we say that “P_i broadcasts m”, we mean that P_i invokes Π_{BC} as S with input m and the parties participate in this instance. Similarly, when we say that “P_i receives m from the broadcast of P_j through regular-mode”, we mean that P_i has the output m at time T_{BC} during the instance of Π_{BC}. Finally, when we say that “P_i receives m from the broadcast of P_j through fallback-mode”, we mean that P_i has the output m after time T_{BC} during the instance of Π_{BC}.

B. Π_{BC} + Π_{ABA} ⇒ Best-of-Both-Worlds BA

We now show how to combine the protocols Π_{BC} and Π_{ABA} to get our best-of-both-worlds BA protocol Π_{ABA}. For this, we use an idea used in [20] to get a best-of-both-worlds BA protocol with conditional security. In the protocol, every party first broadcasts its input bit through an instance of Π_{BC}. If the network is synchronous, then all honest parties should have received the inputs of all the (honest) sender parties from their broadcasts through regular-mode, within time T_{BC}. Consequently, at time T_{BC}, the parties decide an output for all the n instances of Π_{BC}. Based on these outputs, the parties decide their respective inputs for an instance of the Π_{ABA} protocol. Specifically, if “sufficiently many” outputs from the Π_{BC} instances are found to be the same, then the parties consider it as their input for the Π_{ABA} instance. Else, they stick
Protocol $\Pi_{BA}$

- On having input $b_i \in \{0,1\}$, broadcast $b_i$.
- For $j = 1, \ldots, n$, let $b_{i}^{(j)} \in \{0,1\}$ be received from the broadcast of $P_j$. Include $P_j$ to a set $R$, if $b_{i}^{(j)} \neq \bot$. Compute the input $v_i^*$ for an instance of $\Pi_{ABA}$ as follows.
- If $|R| \geq n - t$, set $v_i^*$ to the majority bit among the $b_{i}^{(j)}$ values of the parties in $R$.
- Else set $v_i^* = b_i$.
- At time $T_{BC}$, participate in an instance of $\Pi_{ABA}$ with input $v_i^*$. Output the result of $\Pi_{ABA}$.

*If there is no majority, then set $v_i^* = 1$.

Fig. 2. The best-of-both-worlds BA protocol. The above code is executed by every $P_i \in P$.

to their original inputs. The overall output of the protocol is then set to be the output from $\Pi_{ABA}$.

We next prove the properties of the protocol $\Pi_{BA}$. We note that protocol $\Pi_{BA}$ is invoked only $O(n^3)$ times in our MPC protocol, which is independent of $|P|$. Consequently, we do not focus on the exact communication complexity of $\Pi_{BA}$.

**Theorem III.6:** Let $t < n/3$ and let $\Pi_{BA}$ be a randomized protocol, satisfying the conditions as per Lemma III.3. Then $\Pi_{BA}$ achieves the following, where every party participates with an input bit.

- **Synchronous Network:** The protocol is a $t$-perfectly-secure SBA protocol, where all honest parties obtain an output within time $T_{BA} = T_{BC} + T_{ABA}$. The protocol incurs a communication of $O(poly(n) \log |P|)$ bits from the honest parties.

- **Asynchronous Network:** The protocol is a $t$-perfectly-secure ABA protocol with an expected communication of $O(poly(n) \log |P|)$ bits.

**Proof:** We start with the properties in a synchronous network. The $t$-liveness property of $\Pi_{BC}$ in the synchronous network guarantees that all honest parties will have some output, from each instance of $\Pi_{BC}$ through regular-mode, at time $T_{BC}$. Moreover, the $t$-validity and $t$-consistency properties of $\Pi_{BC}$ in the synchronous network guarantee that irrespective of the sender parties, all honest parties will have a common output from each individual instance of $\Pi_{BC}$, at time $T_{BC}$. Now since the parties decide their respective inputs for the instance of $\Pi_{ABA}$ deterministically based on the individual outputs from the $n$ instances of $\Pi_{BC}$ at time $T_{BC}$, it follows that all honest parties participate with a common input in the protocol $\Pi_{ABA}$. Hence, all honest parties obtain an output by the end of time $T_{BC} + T_{ABA}$, thus ensuring $t$-guaranteed liveness of $\Pi_{ABA}$. Moreover, the $t$-consistency property of $\Pi_{ABA}$ in the synchronous network guarantees that all honest parties have a common output from the instance of $\Pi_{ABA}$, which is taken as the output of $\Pi_{BA}$, thus proving the $t$-consistency of $\Pi_{BA}$.

For proving the validation in the synchronous network, let all honest parties have the same input bit $b$. From the $t$-consistency of $\Pi_{BC}$ in the synchronous network, all honest parties will receive $b$ as the output at time $T_{BC}$ in all the $\Pi_{BC}$ instances, corresponding to the honest sender parties. Since there are at least $n - t$ honest parties, it follows that all honest parties will find a common subset $R$ in the protocol, as the set of honest parties constitutes a candidate $R$. Moreover, all honest parties will be present in $R$, as $n - t > t$ holds. Since the set of honest parties constitutes a majority in $R$, it follows that all honest parties will participate with input $b$ in the instance of $\Pi_{ABA}$ and hence output $b$ at the end of $\Pi_{ABA}$, which follows from the $t$-validity of $\Pi_{ABA}$ in the synchronous network. This proves the $t$-validity of $\Pi_{BA}$.

We next prove the properties of $\Pi_{BA}$ in an asynchronous network. The $t$-consistency of the protocol $\Pi_{BA}$ follows from the $t$-consistency of the protocol $\Pi_{ABA}$ in the asynchronous network, since the overall output of the protocol $\Pi_{BA}$ is same as the output of the protocol $\Pi_{ABA}$. The $t$-liveness of the protocol $\Pi_{BC}$ in the asynchronous network guarantees that all honest parties will have some output from all the $n$ instances of $\Pi_{BC}$ at local time $T_{BC}$ through regular-mode. Consequently, all honest parties will participate with some input in the instance of $\Pi_{ABA}$. The $t$-almost-surely liveness of $\Pi_{ABA}$ in the asynchronous network then implies the $t$-almost-surely liveness of $\Pi_{BA}$.

For proving the validity in an asynchronous network, let all honest parties have the same input bit $b$. We claim that all honest parties participate with input $b$ during the instance of $\Pi_{ABA}$. The $t$-validity of $\Pi_{ABA}$ in the asynchronous network then automatically implies the $t$-validity of $\Pi_{BA}$.

To prove the above claim, consider an arbitrary honest party $P_h$. There are two possible cases. If $P_h$ fails to find a subset $R$ satisfying the protocol conditions, then the claim holds trivially, as $P_h$ participates in the instance of $\Pi_{ABA}$ with its input for $\Pi_{BA}$, which is the bit $b$. So consider the case when $P_h$ finds a subset $R$, such that $|R| \geq n - t$ and where corresponding to each $P_j \in R$, party $P_h$ has computed an output $b_{i}^{(j)} \in \{0,1\}$ at local time $T_{BC}$ during the instance $\Pi_{BC}$, through regular-mode. Now consider the subset of honest parties in the set $R$. Since $t < n/3$, it follows that $n - 2t > t$ and hence the majority of the parties in $R$ will be honest. Moreover, $P_h$ will compute the output $b$ at local time $T_{BC}$ in the instance of $\Pi_{BC}$, corresponding to every honest $P_j$ in $R$, which follows from the $t$-weak validity of $\Pi_{BC}$ in the asynchronous network. From these arguments, it follows that $P_h$ will set $b$ as its input for the instance of $\Pi_{ABA}$, thus proving the claim.

The communication complexity, both in a synchronous as well as in an asynchronous network, follows easily from the protocol steps and from the communication complexity of $\Pi_{SBA}$ and $\Pi_{ABA}$.

**IV. Best-of-Both-Worlds Perfectly-Secure VSS**

In this section, we present our best-of-both-worlds VSS protocol. In the protocol, there exists a designated dealer $D \in P$. The input for $D$ consists of $L$ number of $t$-degree polynomials $q^{(1)}(\cdot), \ldots, q^{(L)}(\cdot)$, where $L \geq 1$. Each (honest) $P_i$ is supposed to “verifiably” receive the shares $\{q^{(i)}(\alpha_k)\}_{k=1,\ldots,L}$. Hence, the goal is to generate a $t$-sharing
of \(\{q^{(t)}(0)\}_{t=1,...,L}\). If \(D\) is honest, then in an asynchronous network, each (honest) \(P_i\) eventually gets its shares, while in a synchronous network, \(P_i\) gets its shares after some fixed time, such that the view of the adversary remains independent of \(D\)’s polynomials. The verifiability here ensures that if \(D\) is corrupt, then either no honest party obtains any output (if \(D\) does not invoke the protocol), or there exist \(L\) number of \(t_s\)-degree polynomials, such that \(D\) is “committed” to these polynomials and each honest \(P_i\) gets its shares lying on these polynomials. Note that in the latter case, we cannot bound the time within which honest parties will have their shares, even if the network is synchronous. This is because a corrupt \(D\) may delay sending the messages arbitrarily and the parties will not know the exact network type. Formally, a best-of-both-worlds VSS protocol should achieve the following properties.

**Definition IV.1:** (Best-of-Both-Worlds Perfectly-Secure VSS): Let \(\Pi\) be a protocol for the parties in \(\mathcal{P}\), tolerating up to \(t_s\) and \(t_a\) corruptions in a synchronous and asynchronous network respectively, where a designated party \(D\) \(\in \mathcal{P}\) has \(L\) number of \(t_s\)-degree polynomials \(q^{(1)}(\cdot), \ldots, q^{(L)}(\cdot)\) as input, where \(L\) is publicly-know with \(L \geq 1\). Then \(\Pi\) is called a best-of-both-worlds perfectly-secure VSS protocol if it achieves the following properties.

- If \(D\) is honest, then the following should hold.
  - \(t_s\)-correctness: In a synchronous network, after some fixed time, each honest \(P_i \in \mathcal{P}\) outputs its shares \(\{q^{(t)}(\alpha_i)\}_{t=1,...,L}\).
  - \(t_a\)-correctness: In an asynchronous network, almost-surely, each honest \(P_i \in \mathcal{P}\) eventually outputs its shares \(\{q^{(t)}(\alpha_i)\}_{t=1,...,L}\).
  - \(t_s\)-privacy: Irrespective of the network type, the view of the adversary remains independent of the polynomials \(q^{(1)}(\cdot), \ldots, q^{(L)}(\cdot)\).
  - If \(D\) is corrupt, then either no honest party computes any output or there exists \(L\) number of \(t_s\)-degree polynomials, say \(\{q^{(t)}(\cdot)\}_{t=1,...,L}\), such that the following hold.
    - Strong commitment: irrespective of the network type, almost-surely, at least \(t_s + 1\) honest parties \(P_i\) eventually output their shares \(\{q^{(t)}(\alpha_i)\}_{t=1,...,L}\). Moreover, if any honest \(P_i \in \mathcal{P}\) outputs shares \(s_j^{(1)}, \ldots, s_j^{(L)} \in \mathbb{F}\), then \(s_j = q^{(t)}(\alpha_j)\) holds for \(t = 1, \ldots, L\).

A. The Best-of-Both-Worlds Weak Polynomial-Sharing (WPS) Protocol

In this section, we present our best-of-both-worlds WPS protocol \(\Pi_{\text{WPS}}\). For simplicity, we explain the protocol \(\Pi_{\text{WPS}}\), assuming \(D\) has a single \(t_s\)-degree polynomial \(q(\cdot)\) as input. Later we discuss the modifications needed to handle \(L\) polynomials efficiently. Looking ahead, protocol \(\Pi_{\text{WPS}}\) provides “stronger” commitment guarantees in the asynchronous network than what is required as per Definition IV.2. In more detail, if the network is asynchronous, then the commitment guarantees of \(\Pi_{\text{WPS}}\) are the same, as required from that of a VSS protocol and every honest party will eventually get its desired shares, provided if any honest party receives its shares. Protocol \(\Pi_{\text{WPS}}\) is obtained by carefully “stitching” a synchronous WPS protocol with an asynchronous WPS protocol. We first explain these two individual protocols, followed by the procedure to stitch them together, where the parties will be not knowing the exact network type.

WPS in an Asynchronous Network: In an asynchronous network, one can consider the following protocol \(\Pi_{\text{WPS}}\): \(D\) embeds \(q(\cdot)\) in a random \((t_s, t_a)\)-degree symmetric bivariate polynomial \(Q(x, y) = z = 0\) and distributes univariate polynomials lying on \(Q(x, y)\) to respective parties. To verify whether \(D\) has distributed “consistent” polynomials, the parties check the pair-wise consistency of their supposedly common points and make the results public through \(\mathcal{OK}\) messages, if the tests are “positive”. Based on the \(\mathcal{OK}\) messages, the parties prepare a consistency graph and look for an \((n, t_a)\)-star, say \((\mathcal{E}', \mathcal{F}')\). If \(D\) is honest, then \((\mathcal{E}', \mathcal{F}')\) will be obtained eventually, since the honest parties eventually form a clique of size at least \(n - t_a\). The existence of \((\mathcal{E}', \mathcal{F}')\) guarantees that the polynomials of the honest parties in \(\mathcal{F}'\) lie
on a single \((t_s, t_s)\)-degree symmetric bivariate polynomial \(Q^*(x, y)\), where \(Q^*(x, y) = Q(x, y)\) for an honest \(D\). This is because \(E\) has at least \(t_s + 1\) honest parties with pair-wise consistent polynomials, defining \(Q^*(x, y)\). Moreover, the polynomial of every honest party in \(F\) is pair-wise consistent with the polynomials of every honest party in \(E\). The parties outside \(F\) obtain their polynomials lying on \(Q^*(x, y)\) by applying OEC on the common points on these polynomials received from the parties in \(F\). Every \(P_i\) then outputs \(Q^*(0, \alpha_i)\) as its share, which is same as \(q^*(\alpha_i)\), where \(q^*(\cdot) = Q^*(0, y)\). Note that \(\Pi_{\text{WPS}}\) actually constitutes a VSS in the asynchronous network as, for an honest \(D\), every honest party eventually gets its share. On the other hand, for a corrupt \(D\), every honest party eventually gets its share if some honest party gets its share.

**WPS for Synchronous Network:** \(\Pi_{\text{WPS}}\) fails in a synchronous network if there are \(t_s\) corruptions. This is because only \(n - t_s\) honest parties are guaranteed and hence the parties may fail to find an \((n, t_a)\)-star. The existence of an \((n, t_a)\)-star, say \((E, F)\), in the consistency graph is not “sufficient” to conclude that \(D\) has distributed consistent polynomials lying on a \((t_s, t_s)\)-degree symmetric bivariate polynomial. This is because if \(D\) is corrupt, then \(E\) is guaranteed to have only \(n - 2t_s - t_s > t_s\) honest parties with pair-wise consistent polynomials. Whereas to define a \((t_s, t_s)\)-degree symmetric bivariate polynomial, we need more than \(t_s\) pair-wise consistent polynomials. On the other hand, if \(D\) is corrupt, then the honest parties in \(F\) need not constitute a clique. As a result, the polynomials of the honest parties in \(F\) need not be pair-wise consistent and hence, need not lie on a \((t_s, t_s)\)-degree symmetric bivariate polynomial.

To get rid of the above problem, the parties instead look for a "special" \((n, t_s)\)-star \((E, F)\), where the polynomials of all honest parties in \(F\) are guaranteed to lie on a single \((t_s, t_s)\)-degree symmetric bivariate polynomial. Such a special \((E, F)\) is bound to exist for an honest \(D\). Based on the above idea, protocol \(\Pi_{\text{SWPS}}\) for a synchronous network proceeds as follows. For ease of understanding, we explain the protocol as a sequence of communication phases, with the parties being synchronized in each phase.

In the first phase, \(D\) distributes the univariate polynomials, during the second phase the parties perform pair-wise consistency tests and during the third phase, the parties make the results of positive tests public. Additionally, the parties also make the results of "negative" tests public through \(\text{NOK}\) messages and their respective versions of the disputed points (the \(\text{NOK}\) messages were not required for \(\Pi_{\text{WPS}}\)). The parties then construct the consistency graph. Next, \(D\) removes all the parties who have made public "incorrect" \(\text{NOK}\) messages with incorrect disputed points from consideration in its consistency graph. Among the remaining parties, \(D\) checks for the presence of a set of at least \(n - t_s\) parties \(W\), such that the polynomial of every party in \(W\) is publicly confirmed to be pair-wise consistent with the polynomials of at least \(n - t_s\) parties within \(W\). If a \(W\) is found, then \(D\) checks for the presence of an \((n, t_s)\)-star, say \((E, F)\) among \(W\) and broadcasts \((W, E, F)\) during the fourth phase, if \(D\) finds \((E, F)\). The parties upon receiving \((W, E, F)\) verify if \(W\) is of size at least \(n - t_s\) and every party in \(W\) has an edge with at least \(n - t_s\) parties within \(W\) in their local copy of the consistency graph. The parties also check whether indeed \((E, F)\) constitutes an \((n, t_s)\)-star among the parties within \(W\). Furthermore, the parties now additionally verify whether any pair of parties \(P_j, P_k\) from \(W\) have made public "conflicting" \(\text{NOK}\) messages during the third phase. That is, if there exists any \(P_j, P_k \in W\) who made public \(\text{NOK}\) messages with \(q_{jk}\) and \(q_{kj}\) respectively during the third phase such that \(q_{jk} \neq q_{kj}\), then \(W\) is not accepted. The idea here is that if \(D\) is honest, then at least one of \(P_j, P_k\) is bound to be corrupt, whose corresponding \(\text{NOK}\) message is incorrect. Since \(D\) also would have seen these public \(\text{NOK}\) messages during the third phase, it should have discarded the corresponding corrupt party, before finding \(W\). Hence, if a \((W, E, F)\) is accepted at the end of the fourth phase, then the polynomials of all honest parties in \(W\) are guaranteed to be pair-wise consistent and lie on a single \((t_s, t_s)\)-degree symmetric bivariate polynomial, say \(Q^*(x, y)\), where \(Q^*(x, y) = Q(x, y)\) for an honest \(D\). This will further guarantee that the polynomials of all honest parties in \(F\) also lie on \(Q^*(x, y)\), as \(F \subseteq W\).

If a \((W, E, F)\) is accepted, then each \(P_i \in W\) outputs the constant term of its univariate polynomial as its share. On the other hand, the parties outside \(W\) attempt to obtain their corresponding polynomials lying on \(Q^*(x, y)\) by applying OEC on the common points on these polynomials received from the parties in \(F\). And if a \(t_s\)-degree polynomial is obtained, then the constant term of the polynomial is set as the share. For an honest \(D\), each honest \(P_i\) will be present in \(W\) and hence, will have the share \(q(\alpha_i)\). On the other hand, if a \(W\) is accepted for a corrupt \(D\), then all the honest parties in \(W\) (which are at least \(t_s + 1\) in number) will have their shares lying on \(q^*(\cdot) = Q^*(0, y)\). Moreover, even if an honest party \(P_i\) outside \(W\) is able to compute its share, then it is the same as \(q^*(\alpha_i)\) due to the OEC mechanism. However, for a corrupt \(D\), all the honest parties outside \(W\) may not be able to obtain their desired share, as \(F\) is guaranteed to have only \(n - 2t_s > t_s + t_a\) honest parties and OEC may fail. It is precisely for this reason that \(\Pi_{\text{SWPS}}\) fails to qualify as a VSS.

\(\Pi_{\text{SWPS}} + \Pi_{\text{WPS}} \Rightarrow \text{Best-of-Both-Worlds WPS Protocol}\)

**\(\Pi_{\text{WPS}}\):** Next discuss how to combine protocols \(\Pi_{\text{SWPS}}\) and \(\Pi_{\text{WPS}}\) to get our best-of-both-worlds WPS protocol \(\Pi_{\text{WPS}}\). In protocol \(\Pi_{\text{WPS}}\) (Fig 3), the parties first run \(\Pi_{\text{SWPS}}\) assuming a synchronous network, where \(\Pi_{\text{BC}}\) is used to make any value public by setting \(t = t_s\) in the protocol \(\Pi_{\text{BC}}\). If \(D\) is honest then in a synchronous network, the first, second, third and fourth phase of \(\Pi_{\text{SWPS}}\) would have been over by the time \(\Delta, 2\Delta, 2\Delta + T_{\text{BC}}\) and \(2\Delta + 2T_{\text{BC}}\) respectively and by time \(2\Delta + 2T_{\text{BC}}\), the parties should have accepted some \((W, E, F)\). However, in an asynchronous network, parties may have different “opinions” regarding the acceptance of some \((W, E, F)\). This is because it may be possible that only a subset of the honest parties accept some \((W, E, F)\) within local time \(2\Delta + 2T_{\text{BC}}\). Hence at time \(2\Delta + 2T_{\text{BC}}\), the parties run an instance of our best-of-both-worlds BA protocol \(\Pi_{\text{BA}}\), to check whether any of \((W, E, F)\) is accepted.

If the parties conclude that some \((W, E, F)\) is accepted, then the parties compute their WPS-shares as per \(\Pi_{\text{SWPS}}\). However, we need to ensure that for a corrupt \(D\) in a synchronous
network, if the polynomials of the honest parties in W are not pair-wise consistent, then the corresponding conflicting messages are received within time $2\Delta + T_{BC}$ (the time required for the third phase of $\Pi_{SWPS}$ to be over), so that $(W, E, F)$ is not accepted. This is ensured by enforcing even a corrupt D to send the respective polynomials of all the honest parties in W by time $\Delta$, so that the pair-wise consistency test between every pair of honest parties in W is over by time $2\Delta$. For this, the parties are asked to wait for some “appropriate” time before starting the pair-wise consistency tests and also, before making public the results of pair-wise consistency tests. The idea is to ensure that if the polynomials of the honest parties in W are not delivered within time $\Delta$ (in a synchronous network), then the results of the pair-wise consistency tests also get delayed beyond time $2\Delta + T_{BC}$ (the time-out of the third phase of $\Pi_{SWPS}$). This in turn will ensure that no W is accepted within time $2\Delta + 2T_{BC}$.

If the parties conclude that no $(W, E, F)$ is accepted within time $2\Delta + 2T_{BC}$, then it implies that either D is corrupt or the network is asynchronous and hence, the parties resort to $\Pi_{AWPS}$. However, D need not have to start afresh and distribute polynomials on a “fresh” bivariate polynomial. Instead, D continues with the consistency graph formed using the OK messages received as part of $\Pi_{SWPS}$ and searches for an $(n, t_a)$-star. If D is honest and the network is asynchronous, then the parties eventually obtain their shares.

Notice that in an asynchronous network, it might be possible that the parties (through $\Pi_{BA}$) conclude that $(W, E, F)$ is accepted, if some honest party(ies) accepts a $(W, E, F)$ within the time-out $2\Delta + 2T_{BC}$. Even in this case, the polynomials of all honest parties in W lie on a single $(t_s, t_s)$-degree symmetric bivariate polynomial $Q^*(x, y)$ for a corrupt D. This is because there will be at least $n - 2t_s - t_a > t_s$ honest parties in E with pair-wise consistent polynomials, defining $Q^*(x, y)$, and the polynomial of every honest party in F will be pair-wise consistent with the polynomials of all honest parties in E and hence lie on $Q^*(x, y)$ as well. Now consider any honest $P_i \in (W \setminus F)$. As part of $\Pi_{SWPS}$, it is ensured that the polynomial of $P_i$ is consistent with the polynomials of at least $n - t_s$ parties among W. Among these $n - t_s$ parties, at least $n - 2t_s - t_a > t_s$ will be honest parties from F. Thus, the polynomial of $P_i$ will also lie on $Q^*(x, y)$.

We next proceed to prove the properties of the protocol $\Pi_{WPS}$. We begin with showing that if D is honest, then the adversary does not learn anything additional about $q(\cdot)$, irrespective of the network type.

**Lemma IV.3 ($t_s$-Privacy):** In protocol $\Pi_{WPS}$, if D is honest, then irrespective of the network type, the view of the adversary remains independent of $q(\cdot)$.

**Proof:** Let D be honest. We consider the worst-case scenario, when the adversary controls up to $t_s$ parties. We claim that throughout the protocol, the adversary learns at most $t_s$ univariate polynomials lying on $Q(x, y)$. Since $Q(x, y)$ is a random $(t_s, t_s)$-degree symmetric-bivariate polynomial, it then follows from Lemma II.2 that the view of the adversary will be independent of $q(\cdot)$. We next proceed to prove the claim.

---

**Protocol $\Pi_{WPS}(D, q(\cdot))$:**

- **Phase I — Sending Polynomials:** D, on having the input $q(\cdot)$, chooses a random $(t_s, t_s)$-degree symmetric bivariate polynomial $Q(x, y)$ such that $Q(0, y) = q(\cdot)$ and sends $q_i(x) = Q(x, a_i)$ to each party $P_i \in \mathcal{P}$.

- **Phase II — Pair-Wise Consistency:** Each $P_i \in \mathcal{P}$ on receiving a $t_s$-degree polynomial $q_i(x)$ from D does the following.
  - Wait till the local time becomes a multiple of $\Delta$ and then send $q_j = q_i(a_j)$ to $P_j$ for $j = 1, \ldots, n$.

- **Phase III — Publicly Declaring the Results of Pair-Wise Consistency Test:** Each $P_i \in \mathcal{P}$ does the following.
  - Upon receiving $q_j$ from $P_j$, wait till the local time becomes a multiple of $\Delta$. If a $t_s$-degree polynomial $q_i(x)$ has been received from D, then do the following.
    - Broadcast $\text{OK}(i, j)$, if $q_j = q_i(a_j)$ holds.
    - Broadcast $\text{NOK}(i, j, q_i(a_j))$, if $q_j \neq q_i(a_j)$ holds.

- **Local computation — Constructing Consistency Graph:** Each $P_i \in \mathcal{P}$ does the following.
  - Construct a consistency graph $G_i$ over $\mathcal{P}$, where the edge $(P_j, P_k)$ is included in $G_i$, if $\text{OK}(j, k)$ and $\text{OK}(k, j)$ is received from the broadcast of $P_j$ and $P_k$ respectively, either through the regular-mode or fall-back mode.

- **Phase IV — Checking for an $(n, t_s)$-star:** D does the following in its consistency graph $G_D$ at time $2\Delta + T_{BC}$.
  - Remove edges incident with $P_i$, if $\text{NOK}(i, j, q_i)$ is received from the broadcast of $P_i$ through regular-mode and $q_j \neq Q(a_j, a_i)$.
  - Set $W = \{P_i : \deg(P_i) \geq n - t_s\}$, where $\deg(P_i)$ denotes the degree of $P_i$ in $G_D$.
  - Remove $P_i$ from $W$, if $P_i$ is not incident with at least $n - t_s$ parties in $W$. Repeat this step till no more parties can be removed from $W$.
  - Run algorithm $\text{AlgStar}$ on $G_D[W]$, where $G_D[W]$ denotes the subgraph of $G_D$ induced by the vertices in $W$. If an $(n, t_s)$-star, say $(E, F)$, is obtained, then broadcast $(W, E, F)$.

- **Local Computation — Verifying and Accepting** $(W, E, F)$:
  - Each $P_i \in \mathcal{P}$ does the following at time $2\Delta + 2T_{BC}$.
    - There exist no $P_j, P_k \in W$, such that $\text{NOK}(j, k, q_k)$ and $\text{NOK}(k, j, q_j)$ messages were received from the broadcast of $P_j$ and $P_k$ respectively through regular-mode, where $q_j, q_k \neq q_{ij}$.
    - In the consistency graph $G_i$, $\deg(P_i) \geq n - t_s$ for all $P_i \in W$.
    - In the consistency graph $G_i$, every $P_j \in W$ has edges with at least $n - t_s$ parties from $W$.
    - $(E, F)$ was an $(n, t_s)$-star in the induced graph $G_i[W]$.
    - For every $P_j, P_k \in W$ where the edge $(P_j, P_k)$ is present in $G_i$, the $\text{OK}(j, k)$ and $\text{OK}(k, j)$ messages were received from the broadcast of $P_j$ and $P_k$ respectively through regular-mode.

- **Phase V — Deciding Whether to Go for an $(n, t_s)$-star:** At time $2\Delta + 2T_{BC}$, each $P_i \in \mathcal{P}$ participates in an instance of $\Pi_{BA}$ with input $b_i = 0$ if a $(W, E, F)$ was accepted, else with input $b_i = 1$, and waits for time $T_{BA}$.

- **Local Computation — Computing WPS-share** through $W$: If the output of $\Pi_{BA}$ is 0, then each $P_i \in \mathcal{P}$ computes its $\text{WPS-Share}$ $s_i$ (initially set to 1) as follows.
  - If a $(W, E, F)$ is not yet received then wait till a $(W, E, F)$.
is received from D’s broadcast through fall-back mode.
- If $P_i \in W$, then output $s_i = q_i(0)$.
- Else, initialise a support set $SS_i$ to $\emptyset$. If $q_{ij}$ is received from $P_j \in F$, include $q_{ij}$ to $SS_i$. Keep executing $OE_C(t_{ij}, t_{jk}, SS_i)$, till a $t_{ij}$-degree polynomial, say $q_{ij}(\cdot)$, is obtained. Then, output $s_i = q_i(0)$.

- **Phase VI — Broadcasting an $(n, t_a)$-star:** If the output of $\Pi_{BA}$ is 1, then D does the following.
- After every update in the consistency graph $G_D$, run AlgStar on $G_D$. If an $(n, t_a)$-star, say $(E', F')$, is obtained, then broadcast $(E', F')$.

- **Local Computation — Computing WPS-share Through $(n, t_a)$-star:** If the output of $\Pi_{BA}$ is 1, then each $P_i$ does the following to compute its WPS-Share.
- Waits till an $(n, t_a)$-star $(E', F')$ is obtained from the broadcast of D, either through regular or fall-back mode. Upon receiving, wait till $(E', F')$ becomes an $(n, t_a)$-star in $G_t$.
- If $P_i \in F'$, then output $s_i = q_i(0)$.
- Else, initialise a support set $SS_i$ to $\emptyset$. If $q_{ij}$ is received from $P_j \in F'$, include $q_{ij}$ to $SS_i$. Keep executing $OE_C(t_{ij}, t_{jk}, SS_i)$, till a $t_{ij}$-degree polynomial, say $q_{ij}(\cdot)$, is obtained. Then, output $s_i = q_i(0)$.

Fig. 3. (Continued.) The best-of-both-worlds weak polynomial-sharing protocol for a single polynomial.

Corresponding to every corrupt $P_i$, the adversary learns $Q(x, \alpha_i)$. Corresponding to every honest $P_i$, the adversary learns $t_a$ distinct points on $P_i$’s univariate polynomial $Q(x, \alpha_i)$, through the pair-wise consistency checks. However, these points were already included in the view of the adversary (through the univariate polynomials under the adversary’s control). Hence, no additional information about the polynomials of the honest parties is revealed during the pair-wise consistency checks. Furthermore, no honest $P_i$ ever broadcasts $NK(i, j, q_i(\alpha_j))$, corresponding to any honest $P_j$. This is because the pair-wise consistency check will always pass for every pair of honest parties.

We next prove the correctness property in a synchronous network.

**Lemma IV.4 ($t_a$-Correctness):** In protocol $\Pi_{WPS}$, if D is honest and the network is asynchronous, then each honest $P_i$ eventually outputs $q_i(\alpha_i)$.

**Proof:** Let D be honest and network be asynchronous with up to $t_a$ corruptions. We first note that every honest party participates with some input in the instance of $\Pi_{BA}$ at local time $2\Delta + 2T_{BC}$. Hence, from the $t_a$-almost-surely liveliness and $t_a$-consistency of $\Pi_{BA}$ in an asynchronous network, it follows that, almost-surely, the instance of $\Pi_{BA}$ eventually generates some common output for all honest parties. Now there are two possible cases:

- **The output of $\Pi_{BA}$ is 0:** From the $t_a$-validity of $\Pi_{BA}$ in the synchronous network, it follows that at least one honest party, say $P_h$, participated with input 0 during the instance of $\Pi_{BA}$. This implies that $P_h$ has accepted a $(W, E, F)$ at local $2\Delta + 2T_{BC}$, which is received from the broadcast of D, through regular-mode. Hence, by the $t_a$-validity and $t_a$-liveness properties of $\Pi_{BA}$ in the synchronous network, all honest parties will eventually receive $(W, E, F)$ from the broadcast of D and accept the triplet. This is because the consistency graphs of all honest parties will eventually have all the edges which were present in the consistency graph $G_{BA}$ of $P_h$ at time $2\Delta + 2T_{BC}$. We claim that every honest $P_i$ will eventually get $Q(x, \alpha_i)$. This will imply that eventually, every honest $P_i$ outputs $s_i = Q(0, \alpha_i) = q_i(\alpha_i)$. To prove the claim, consider an arbitrary honest party $P_i$. There are two possible cases:
  - $P_i \in W$: In this case, $P_i$ has already received $Q(x, \alpha_i)$ from D.
  - $P_i \notin W$: In this case, there will be at least $n - t_a > 2t_a + t_a$ parties in $F$, of which at most $t_a$ could be corrupt. Since $Q(x, \alpha_i)$ is a $t_a$-degree polynomial and $t_a < |F| - 2t_a$, from Lemma A.1, it follows that by applying the OEC procedure to the common points on the polynomials $Q(x, \alpha_i)$ received from the parties in $F$, party $P_i$ will eventually obtain $Q(x, \alpha_i)$.

- **The output of $\Pi_{BA}$ is 1:** Since D is honest, every pair of honest parties $P_j, P_k$ eventually broadcast $NK(j, k)$ and $NK(k, j)$ messages respectively, as the pair-wise consistency check between them will eventually be successful.
From the $t_a$-weak validity and $t_a$-fallback validity of $\Pi_{BC}$, these messages are eventually delivered to every honest party. Also from the $t_a$-weak consistency and $t_a$-fallback consistency of $\Pi_{BC}$ in the asynchronous network, any OK message which is received by $\mathcal{D}$ from the broadcast of any corrupt party will eventually be received by every other honest party as well. As there will be at least $n-t_a$ honest parties, a clique of size at least $n-t_a$ will eventually form in the consistency graph of every honest party. Hence, $\mathcal{D}$ will eventually find an $(n, t_a)$-star, say $(\mathcal{E'}, \mathcal{F}')$, in its consistency graph and broadcast it. From the $t_a$-weak validity and $t_a$-fallback validity of $\Pi_{BC}$, this star will eventually be delivered to every honest party. Moreover, $(\mathcal{E'}, \mathcal{F}')$ will eventually be an $(n, t_a)$-star in every honest party’s consistency graph. We claim that every honest $P_i$ will eventually get $Q(x, \alpha_i)$. This will imply that eventually, every honest $P_i$ outputs $s_i = Q(0, \alpha_i) = q(\alpha_i)$. To prove the claim, consider an arbitrary honest party $P_i$. There are two possible cases.

- $P_i \in \mathcal{F}':$ In this case, $P_i$ already has $Q(x, \alpha_i)$, received from $\mathcal{D}$.

- $P_i \notin \mathcal{F}':$ In this case, there will be at least $n-t_a > 3t_s$ parties in $\mathcal{F}'$, of which at most $t_a$ could be corrupt, where $t_a < t_s$. Since $Q(x, \alpha_i)$ is a $t_s$-degree polynomial and $t_s < |\mathcal{F}'| - 2t_a$, from Lemma A.1 it follows that, by applying the OEC procedure to the common points on the polynomial $Q(x, \alpha_i)$ received from the parties in $\mathcal{F}'$, party $P_i$ will eventually obtain $Q(x, \alpha_i)$.

We next proceed to prove the weak commitment properties for a corrupt $\mathcal{D}$. However, before that, we prove a helping lemma.

**Lemma IV.6:** Let the network be synchronous and let $\mathcal{D}$ be corrupt in the protocol $\Pi_{WPS}$. If any honest party receives a $(\mathcal{W}, \mathcal{E}, \mathcal{F})$ from the broadcast of $\mathcal{D}$ through regular-mode and accepts it at time $2\Delta + 2T_{BC}$, then all the following hold.

- All honest parties in $\mathcal{W}$ receive their respective $t_s$-degree univariate polynomials from $\mathcal{D}$, within time $\Delta$.
- The univariate polynomials $q_j(x)$ of all honest parties $P_i$ in the set $\mathcal{W}$ lie on a unique $(t_s, t_s)$-degree symmetric bivariate polynomial, say $Q^*(x, y)$. So consider an arbitrary pair of honest parties $P_j, P_k \in \mathcal{W}$. From the first part of the lemma, both $P_j$ and $P_k$ must have received their respective univariate polynomials $q_j(x)$ and $q_k(x)$ by time $\Delta$. This further implies that $P_j$ and $P_k$ must have received the points $q_{kj} = q_j(\alpha_k)$ and $q_{jk} = q_j(\alpha_k)$ respectively by time $2\Delta$. If $q_{kj} \neq q_{jk}$, then $P_j$ and $P_k$ would broadcast $NOK(j, k, q_{jk})$ and $NOK(k, j, q_{kj})$ messages respectively, at time $2\Delta$. Consequently, from the $t_s$-validity property of $\Pi_{BC}$ in the synchronous network, $P_i$ will receive these messages through regular-mode at time $2\Delta + T_{BC}$. Consequently, $P_i$ will not accept $(\mathcal{W}, \mathcal{E}, \mathcal{F})$, which is a contradiction.

To prove the third part of the lemma, we note that since $P_i$ has received $(\mathcal{W}, \mathcal{E}, \mathcal{F})$ from the broadcast of $\mathcal{D}$ through regular-mode at time $2\Delta + 2T_{BC}$, it implies that $\mathcal{D}$ must have started broadcasting $(\mathcal{W}, \mathcal{E}, \mathcal{F})$ latest at time $2\Delta + T_{BC}$. This is because it takes $T_{BC}$ time for the regular-mode of $\Pi_{BC}$ to produce an output. From the $t_s$-consistency property of $\Pi_{BC}$ in the synchronous network, it follows that every honest party will also receive $(\mathcal{W}, \mathcal{E}, \mathcal{F})$ from the broadcast of $\mathcal{D}$ through regular-mode, at time $2\Delta + 2T_{BC}$. Since, at time $2\Delta + T_{BC}$, party $P_i$ has received the $OK(j, k)$ and $OK(k, j)$ messages through regular-mode from the broadcast of every $P_j, P_k \in \mathcal{W}$ where $(P_j, P_k)$ is an edge in $P_i$’s consistency graph, it follows
that these messages started getting broadcast, latest at time $2\Delta$. From the $t_s$-validity and $t_s$-consistency properties of $\Pi_{BC}$ in the synchronous network, it follows that every honest party receives these broadcast messages through regular-mode at the time $2\Delta + T_{BC}$. Hence $(E, F)$ will constitute an $(n, t_s)$-star in the induced subgraph $G_t[\mathcal{W}]$ of every honest party $P_i$'s consistency-graph at time $2\Delta + T_{BC}$ and consequently, every honest party accepts $(\mathcal{W}, E, F)$.

Now based on the above helping lemma, we proceed to prove the weak commitment properties of the protocol $\Pi_{WPS}$.

Lemma IV.7 ($t_s$-Weak Commitment): In protocol $\Pi_{WPS}$, if $D$ is corrupt and the network is synchronous, then either no honest party computes any output or there exists some $t_s$-degree polynomial, say $q^*(\cdot)$, such that all the following hold.

- There are at least $t_s + 1$ honest parties $P_i$ who output the WPS-shares $q^*(\alpha_i)$.
- If any honest $P_j$ outputs a WPS-share $s_j \in \mathcal{F}$, then $s_j = q^*(\alpha_j)$ holds.

Proof: Let $D$ be corrupt and network be synchronous with up to $t_s$ corruptions. If no honest party outputs any WPS-share, then the lemma holds trivially. So consider the case when some honest party outputs a WPS-share, which is an element of $\mathcal{F}$. Now, there are two possible cases.

- At time $2\Delta + 2T_{BC}$, at least one honest party, say $P_i$, accepts a $(\mathcal{W}, E, F)$, received from the broadcast of $D$ through regular-mode: In this case, from Lemma IV.6, at time $2\Delta + 2T_{BC}$, every honest party will accept $(\mathcal{W}, E, F)$. Hence every honest party participates in the instance of $\Pi_{BA}$ with input 0. From the $t_s$-validity and $t_s$-guaranteed liveness properties of $\Pi_{BA}$ in the synchronous network, all honest parties will get the output 0 during the instance of $\Pi_{BA}$ by time $T_{WPS} = 2\Delta + 2T_{BC} + T_{BA}$. From Lemma IV.6, the univariate polynomials of all the honest parties in $\mathcal{W}$ will lie on some $(t_s, t_s)$-degree symmetric bivariate polynomial, say $Q^*(x, y)$. Let $q^*(\cdot) \equiv Q^*(0, 0)$. Now consider an arbitrary honest party $P_i$, who outputs a WPS-share $s_i \in \mathcal{F}$. We want to show that the condition $s_i = q^*(\alpha_i)$ holds. And there are at least $t_s + 1$ such honest parties $P_i$ who output their WPS-share. There are two possible cases.

  - $P_i \in \mathcal{W}$: From the protocol steps, $P_i$ sets $s_i = Q^*(0, \alpha_i)$, which is the same as $q^*(\alpha_i)$. Since $\mathcal{W}$ contains at least $t_s + t_a + 1$ honest parties, this also shows that at least $t_s + 1$ honest parties $P_i$ output their respective WPS-share $s_i \in \mathcal{F}$, which is the same as $Q^*(\alpha_i)$.

  - $P_i \notin \mathcal{W}$: In this case, $P_i$ sets $s_i = q_i(0)$, where $q_i(\cdot)$ is a $t_s$-degree univariate polynomial, obtained by applying the OEC procedure with $d = t = t_s$, on the values $q_{ji}$, received from the parties $P_j \in \mathcal{F}$, during the pair-wise consistency checks. Note that as part of OEC (see the proof of Lemma A.1), party $P_i$ verifies that at least $2t_s + 1$ $q_{ji}$ values from the parties in $\mathcal{F}$ lie on $q_i(\cdot)$. Now out of these $2t_s + 1$ $q_{ji}$ values, at least $t_s + 1$ values are from the honest parties in $\mathcal{F}$. Furthermore, these $q_{ji}$ values from the honest parties in $\mathcal{F}$ are the same as $Q^*(\alpha_i, \alpha_j)$, which is equal to $Q^*(\alpha_i, \alpha_j)$ and uniquely determine $Q^*(x, y)$; the last property holds since $Q^*(x, y)$ is a symmetric bivariate polynomial.

At time $2T_{BC} + 2\Delta$, no honest party has accepted any $(\mathcal{W}, E, F)$: This implies that all honest parties participate in the instance of $\Pi_{BA}$ with input 1. So by the $t_s$-validity and $t_s$-guaranteed liveness of $\Pi_{BA}$ in the synchronous network, all honest parties obtain the output 1 in the instance of $\Pi_{BA}$. Let $P_h$ be the first honest party who outputs a WPS-share, consisting of an element from $\mathcal{F}$. This means that $P_h$ has received a pair $(E', F')$, from the broadcast of $D$, such that $(E', F')$ constitutes an $(n, t_s)$-star in $P_h$'s consistency graph. By the $t_s$-consistency and $t_s$-fallback consistency properties of $\Pi_{BC}$ in the synchronous network, all honest parties receive $(E', F')$ from the broadcast of $D$. Moreover, since $(E', F')$ constitutes an $(n, t_s)$-star in $P_h$’s consistency graph, it will also eventually constitute an $(n, t_s)$-star in every other honest party’s consistency graph as well. This is because the OEC messages, which are received by $P_h$ from the broadcast of the various parties in $E'$ and $F'$, are also received by every other honest party, either through regular-mode or fallback-mode. The last property follows from the $t_s$-validity, $t_s$-consistency and $t_s$-fallback consistency properties of $\Pi_{BC}$ in the synchronous network. Since $|E'| \geq n - 2t_a > 2t_s + (t_s - t_a) > 2t_s$, it follows that $E'$ has at least $t_s + 1$ honest parties $P_i$, whose univariate polynomials $q_i(x)$ are pair-wise consistent. Hence, from Lemma II.1, these univariate polynomials lie on a unique $(t_s, t_s)$-degree symmetric bivariate polynomial, say $Q^*(x, y)$. Similarly, since the univariate polynomial $q_i(x)$ of every honest party in $F'$ is pair-wise consistent with the univariate polynomials $q_j(x)$ of the honest parties in $E'$, it implies that the univariate polynomials $q_i(x)$ of all the honest parties in $F'$ also lie on $Q^*(x, y)$. Let $q^*(\cdot) \equiv Q^*(0, 0)$. We show that every honest $P_i$ eventually outputs a WPS-share, which is the same as $q^*(\alpha_i)$. For this it is enough to show that each honest $P_i$ eventually gets $q_i(x) = Q^*(x, \alpha_i)$, as $P_i$ outputs $q_i(0)$ as its WPS-share, which will be then same as $q^*(\alpha_i)$. Consider an arbitrary honest party $P_i$. There are two possible cases.

- $P_i \in F'$: In this case, $P_i$ already has $Q^*(x, \alpha_i)$, received from $D$.
- $P_i \notin F'$: In this case, there will be $n - t_a > 3t_s$ parties in $F'$, of which at most $t_s$ could be corrupt. Moreover, $Q^*(x, \alpha_i)$ is a $t_s$-degree polynomial and $t_s < |F'| - 2t_s$ holds. Hence from the properties of OEC (Lemma A.1), by applying the OEC procedure to the common points on the polynomial $Q^*(x, \alpha_i)$ received from the parties in $F'$, party $P_i$ will compute $Q^*(x, \alpha_i)$.
We finally prove the commitment property in an asynchronous network.

**Lemma IV.8 (tₐ-Strong Commitment):** In protocol Π_{WPS}, if D is corrupt and the network is asynchronous, then either no honest party computes any output or there exists some tₐ-degree polynomial, say \( q^*(\cdot) \), such that almost-surely, every honest \( P_i \) eventually outputs a WPS-share \( q^*(\alpha_i) \).\(^{12}\)

**Proof:** Let D be corrupt and network be asynchronous with up to \( t_a \) corruptions. If no honest party computes any output, then the lemma holds trivially. So consider the case when some honest party outputs a WPS-share, consisting of an element of \( F \). We note that every honest party participates with some input in the instance of \( \Pi_{BA} \) at local time \( 2\Delta + 2T_{BC} \). Hence, from the \( t_a \)-almost-surely liveness and \( t_a \)-consistency properties of \( \Pi_{BA} \) in the asynchronous network, almost-surely, all honest parties eventually compute a common output during the instance of \( \Pi_{BA} \). Now there are two possible cases:

- **The output of \( \Pi_{BA} \) is 0:** From the \( t_a \)-validity of \( \Pi_{BA} \) in the asynchronous network, it implies that at least one honest party, say \( P_h \), participated with input 0 during the instance of \( \Pi_{BA} \). This further implies that at local time \( 2\Delta + 2T_{BC} \), party \( P_h \) has accepted a \( (W, E, F) \), which has been received by \( P_h \) from the broadcast of D, through regular-mode. Hence, by the \( t_a \)-weak consistency and \( t_a \)-fallback consistency of \( \Pi_{BC} \) in the asynchronous network, all honest parties will eventually receive \( (W, E, F) \) from the broadcast of D. There will be at least \( n - 2t_a > t_a \) honest parties in \( E \), whose univariate polynomials \( q_i(x) \) are pair-wise consistent and hence from Lemma II.1 lie on a unique \((t_s, t_a)\)-degree symmetric bivariate polynomial, say \( Q^*(x, y) \). Similarly, the univariate polynomial \( q_i(x) \) of every honest \( P_j \in F \) will be pair-wise consistent with the univariate polynomials \( q_i(x) \) of all the honest parties in \( E \) and hence lie on \( Q^*(x, y) \) as well. Let \( q^*(\cdot) \overset{df}{=} Q^*(0, y) \). We claim that every honest \( P_i \) will eventually get \( Q^*(x, \alpha_i) \). This will imply that eventually every honest \( P_i \) outputs the WPS-share \( s_i = Q^*(0, \alpha_i) = q^*(\alpha_i) \). To prove the claim, consider an arbitrary honest \( P_i \). There are three possible cases.

- \( P_i \in W \) and \( P_i \in F \): In this case, \( P_i \) already has \( q_i(x) \), received from D. And since \( P_i \in F \), the condition \( q_i(x) = Q^*(x, \alpha_i) \) holds.

- \( P_i \in W \) and \( P_i \notin F \): In this case, \( P_i \) already has \( q_i(x) \), received from D. Since \( |W| \geq n - t_a \) and \( |F| \geq n - t_a \), \( |W \cap F| \geq n - 2t_a > t_a + t_a \). From the protocol steps, the polynomial \( q_i(x) \) is pair-wise consistent with the polynomial \( q_j(x) \) of at least \( n - t_a \) parties \( P_j \in W \) (since \( P_i \) has edges with at least \( n - t_a \) parties \( P_j \) within \( W \)). Now among these \( n - t_a \) parties, at least \( n - 2t_a \) parties will be from \( F \), of which at least \( n - 2t_a > t_a \) parties will be honest. Hence, \( q_i(x) \) is pair-wise consistent with the \( q_j(x) \) polynomials of at least \( t_a + 1 \) honest parties \( P_j \in F \). Now since the \( q_j(x) \) polynomial of all the honest parties in \( F \) lie on \( Q^*(x, y) \), it implies that \( q_i(x) = Q^*(x, \alpha_i) \) holds.

- \( P_i \notin W \): In this case, there will be \( n - t_a \) parties in \( F \), of which at most \( t_a \) could be corrupt. Since \( Q^*(x, \alpha_i) \) is a \( t_a \)-degree polynomial and \( t_a < |F| - 2t_a \), from Lemma A.1 it follows that by applying the OEC procedure to the common points on the polynomial \( Q^*(x, \alpha_i) \) polynomial received from the parties in \( F \), party \( P_i \) will eventually obtain \( Q^*(x, \alpha_i) \).

**The output of \( \Pi_{BA} \) is 1:** Let \( P_h \) be the first honest party, who outputs a WPS-share. This means that \( P_h \) has received a pair, say \( (E', F') \), from the broadcast of D, such that \( (E', F') \) constitutes an \((n, t_a)\)-star in \( P_h \)'s consistency graph. By the \( t_a \)-weak consistency and \( t_a \)-fallback consistency properties of \( \Pi_{BC} \) in the asynchronous network, all honest parties eventually receive \( (E', F') \) from the broadcast of D. Moreover, since the consistency graphs are constructed based on the broadcasted \( OK \) messages and since \( (E', F') \) constitutes an \((n, t_a)\)-star in \( P_h \)'s consistency graph, from the \( t_a \)-weak validity, \( t_a \)-fallback validity, \( t_a \)-weak consistency and \( t_a \)-fallback consistency properties of \( \Pi_{BC} \) in the asynchronous network, the pair \( (E', F') \) will eventually constitute an \((n, t_a)\)-star in every honest party's consistency graph. Since \( |E'| \geq n - 2t_a > 2t_a + (t_a - t_a) > 2t_a \), it follows that \( E' \) has at least \( t_a + 1 \) honest parties, whose univariate polynomials \( q_i(x) \) are pair-wise consistent and hence, from Lemma II.1, lie on a unique degree-(\( t_a, t_a \)) symmetric bivariate polynomial, say \( Q^*(x, y) \). Similarly, the univariate polynomial \( q_i(x) \) of every honest party \( P_j \in F' \) is pair-wise consistent with the univariate polynomials \( q_i(x) \) of the honest parties in \( E' \), it implies that the univariate polynomial \( q_j(x) \) of all the honest parties in \( F' \) also lie on \( Q^*(x, y) \). Let \( q^*(\cdot) \overset{df}{=} Q^*(0, y) \). We show that every honest \( P_i \) eventually outputs \( q^*(\alpha_i) \) as its WPS-share. For this, it is enough to show that each honest \( P_i \) eventually gets \( q_i(x) = Q^*(x, \alpha_i) \), as \( P_i \) outputs \( q_i(0) \) as its WPS-share, which will be the same as \( q^*(\alpha_i) \). Consider an arbitrary honest \( P_i \). There are two possible cases.

- \( P_i \in F' \): In this case, \( P_i \) already has \( Q^*(x, \alpha_i) \), received from D.

- \( P_i \notin F' \): In this case, \( F' \) has at least \( n - t_a > 3t_a \) parties, of which at most \( t_a \) could be corrupt. Since \( Q^*(x, \alpha_i) \) is a \( t_a \)-degree polynomial and \( t_a < |F'| - 2t_a \), from Lemma A.1, it follows that by applying the OEC procedure to the common points on the polynomial \( Q^*(x, \alpha_i) \) received from the parties in \( F' \), party \( P_i \) will eventually obtain \( Q^*(x, \alpha_i) \).

**Lemma IV.9** Protocol \( \Pi_{WPS} \) incurs a communication of \( O(n^4 \log |F|) \) bits from the honest parties and invokes 1 instance of \( \Pi_{BA} \).

**Proof:** In the protocol, D sends a \( t_s \)-degree univariate polynomial to every party. As part of the pair-wise consistency checks, each pair of parties exchange 2 field elements.
In addition, an honest party may broadcast an NOK message, corresponding to every other party. As part of the NOK message, the honest party also broadcasts the corresponding common point on its univariate polynomial. Each such common point can be represented by $\log |F|$ bits. The communication complexity now follows from the communication complexity of the protocol $\Pi_{BC}$ (see Theorem III.5).

We next discuss the modifications needed in the protocol $\Pi_{WPS}$, if the input for $D$ consists of $L$ number of $t_s$-degree polynomials.

$\Pi_{WPS}$ for L Polynomials: If $D$ has $L$ polynomials as input in protocol $\Pi_{WPS}$, then it embeds them into $L$ random $(t_s, t_s)$-degree symmetric bivariate polynomials and distributes the univariate polynomials lying on these bivariate polynomials, to the respective parties. The parties then perform the pair-wise consistency tests by exchanging their supposedly common points on the bivariate polynomials. However, $P_i$ broadcasts a single OK$(i, j)$ message for $P_j$ if the pair-wise consistency test is positive for all the $L$ supposedly common values between $P_i$ and $P_j$. On the other hand, if the test fails for any of the $L$ supposedly common values, then $P_i$ broadcasts a single NOK message, corresponding to the least indexed common value for which the test fails. Hence, instead of constructing $L$ consistency graphs, a single consistency graph is constructed by each party. As a result, $D$ finds a single $(W, E, F)$ triplet and broadcasts it. Similarly, a single instance of $\Pi_{BA}$ is used to decide whether any $(W, E, F)$ is accepted. Finally, if no $(W, E, F)$ triplet is found and broadcast, then $D$ looks for a single $(n, t_s)$-star $(E', F')$ and broadcasts it.

To avoid repetition, we skip the formal details of the modified protocol and the proof of its properties, as stated in Theorem IV.10.

Theorem IV.10: Let $n > 3t_s + t_n$ and let $D$ has $L$ number of $t_s$-degree polynomials $q^{(1)}(\cdot), \ldots, q^{(L)}(\cdot)$ as input for $\Pi_{WPS}$, where $L \geq 1$. Moreover, let $T_{WPS} = 2\Delta + 2T_{BC} + T_{BA}$. Then protocol $\Pi_{WPS}$ achieves the following properties.

- If $D$ is honest then the following hold.
  - $t_s$-correctness: In a synchronous network, each (honest) $P_i$ outputs $\{q_i^{(1)}(\alpha_i)\}_{t=1,...,L}$ at time $T_{WPS}$.
  - $t_s$-correctness: In an asynchronous network, almost-surely, each (honest) $P_i$ eventually outputs $\{q_i^{(1)}(\alpha_i)\}_{t=1,...,L}$.
  - $t_s$-privacy: Irrespective of the network type, the view of the adversary remains independent of the polynomials $q^{(1)}(\cdot), \ldots, q^{(L)}(\cdot)$.
  - If $D$ is corrupt, then either no honest party computes any output or there exists $L$ number of $t_s$-degree polynomials, say $\{q_i^{(1)}(\cdot)\}_{t=1,...,L}$, such that the following hold.
    - $t_s$-Weak Commitment: In a synchronous network, at least $t_s + 1$ honest parties $P_i$ output WPS-shares $\{q_i^{(1)}(\alpha_i)\}_{t=1,...,L}$. Moreover, if any honest $P_j$ outputs WPS-shares $s_j^{(1)}, \ldots, s_j^{(L)} \in F$, then $s_j = q_i^{(1)}(\alpha_j)$ holds for $t = 1, \ldots, L$.
    - $t_s$-Strong Commitment: In an asynchronous network, almost-surely, each (honest) $P_i$ eventually outputs $\{q_i^{(1)}(\alpha_i)\}_{t=1,...,L}$ as WPS-shares.

- Irrespective of the network type, the protocol incurs a communication of $O(n^2 L \log |F| + n^4 \log |F|)$ bits from the honest parties and invokes 1 instance of $\Pi_{BA}$.

B. The VSS Protocol

Protocol $\Pi_{WPS}$ fails to serve as a VSS because if $D$ is corrupt and the network is synchronous, then the (honest) parties outside $W$ may not obtain their required shares, lying on $D$’s committed polynomials. Protocol $\Pi_{VSS}$ (see Fig 4) fixes this shortcoming. For ease of understanding, we present the protocol assuming $D$ has a single $t_s$-degree polynomial as input and later discuss the modifications needed when $D$ has $L$ such polynomials. The protocol has two “layers” of communication involved. The first layer is similar to $\Pi_{WPS}$ and identifies whether the parties accepted some $(W, E, F)$ within a specified time-out, such that the polynomials of all honest parties in $W$ lie on a single $(t_s, t_s)$-degree symmetric bivariate polynomial, say $Q^*(x, y)$. If some $(W, E, F)$ is accepted, then the second layer of communication (which is coupled with the first layer) enables even the (honest) parties outside $W$ to get their corresponding polynomials lying on $Q^*(x, y)$.

In more detail, to perform the pair-wise consistency check of the polynomials received from $D$, each $P_j$ upon receiving $q_j(x)$ from $D$, shares the polynomial $q_j(x)$ by invoking an instance of $\Pi_{WPS}$ as a dealer. Any party $P_i$ who computes a WPS-Share in this instance of $\Pi_{WPS}$ either broadcasts an OK or NOK message for $P_j$, depending on whether the WPS-share lies on the polynomial which $P_i$ has received from $D$. The rest of the steps for computing $(W, E, F)$ and accepting it remain the same. If some $(W, E, F)$ is accepted, then any $P_j$ outside $W$ computes its polynomial lying on $Q^*(x, y)$ as follows: $P_i$ checks for a subset $SS_i \subseteq F$ of $t_s + 1$ parties $P_j$, such that $P_j$ is able to compute its WPS-share in the $\Pi_{WPS}$ instance invoked by $P_j$ as a dealer. Such an $SS_i$ is bound to exist as there are at least $t_s + 1$ honest parties in $F$ who are always included in $SS_i$. While the WPS-shares corresponding to the honest parties in $SS_i$ will be the common points on $Q^*(x, \alpha_i)$, the same holds even for corrupt parties in $SS_i$. This is because in order to be included in $F$, such parties are “forced” to share polynomials lying on $Q^*(x, y)$, in their respective instances of $\Pi_{WPS}$. Now using the WPS-shares corresponding to the parties in $SS_i$, party $P_i$ will be able to compute $Q^*(x, \alpha_i)$ and hence, its share.

We next proceed to prove the properties of the protocol $\Pi_{VSS}$. We first start by showing that if $D$ is honest, then the view of the adversary remains independent of dealer’s polynomial.

Lemma IV.11 ($t_s$-Privacy): In protocol $\Pi_{VSS}$, if $D$ is honest, then irrespective of the network type, the view of the adversary remains independent of $q(\cdot)$.

Proof: Let $D$ be honest. We consider the worst-case scenario when the adversary controls up to $t_s$ parties. We claim that throughout the protocol, the adversary learns at most $t_s$ univariate polynomials lying on $Q(x, y)$. Since $Q(x, y)$ is a random $(t_s, t_s)$-degree symmetric-bivariate polynomial, it then follows from Lemma II.2, that the view of the adversary will be independent of $q(\cdot)$. We next proceed to prove the claim.
The best-of-both-worlds VSS protocol for a single polynomial.

- **Phase I** — Sending Polynomials: D on having the input $q(\cdot)$, chooses a random $(t_s, t_s)$-degree symmetric bivariate polynomial $Q(x, y)$ such that $Q(0, y) = q(\cdot)$ and sends $q_i(x) = Q(x, \alpha_i)$ to each party $P_i \in \mathcal{P}$.
- **Phase II** — Exchanging Common Values: Each $P_i \in \mathcal{P}$, upon receiving a $t_s$-degree polynomial $q_i(x)$ from D, waits till the current local time becomes a multiple of $\Delta$ and then does the following.
  - Act as a dealer and invoke an instance $\Pi_{WPS}^{(i)}$ of $\Pi_{WPS}$ with input $q_i(x)$.
  - For $j = 1, \ldots, n$, participate in the instance $\Pi_{WPS}^{(i)}$ if invoked by $P_i$ as a dealer, and wait for time $T_{WPS}$.
- **Phase III** — Publicly Declaring the Results of Pair-Wise Consistency Test: Each $P_i \in \mathcal{P}$ waits till the current local time becomes a multiple of $\Delta$ and then does the following.
  - If a WPS-share $q_{ij}$ is computed during the instance $\Pi_{WPS}^{(i)}$ and $q_i(x)$ has been received from D, then:
    - Broadcast $\text{OK}(i, j)$, if $q_{ij} = q_i(\alpha_j)$ holds.
    - Broadcast $\text{NOK}(i, j, q_i(\alpha_j))$, if $q_{ij} \neq q_i(\alpha_j)$ holds.
  - **Local Computation** — Constructing Consistency Graph: Each $P_i \in \mathcal{P}$ does the following.
    - Construct a consistency graph $G_i$ over $\mathcal{P}$, where the edge $(P_j, P_k)$ is included in $G_i$, if $\text{OK}(j, k)$ and $\text{OK}(k, j)$ is received from the broadcast of $P_j$ and $P_k$ respectively, either through the regular-mode or fall-back mode.
  - **Phase IV** — Constructing $(n, t_s)$-star: D does the following in its consistency graph $G_D$ at time $\Delta + T_{WPS} + T_{BC}$.
    - Remove edges incident with $P_i$, if $\text{NOK}(i, j, q_{ij})$ is received from the broadcast of $P_i$ through regular-mode and $q_{ij} \neq q_i(\alpha_j)$.
    - Set $\mathcal{W} = \{ P_j : \text{deg}(P_i) \geq n - t_s \}$, where $\text{deg}(P_i)$ denotes the degree of $P_i$ in $G_D$.
    - Remove $P_i$ from $\mathcal{W}$, if $P_i$ is not incident with at least $n - t_s$ parties in $\mathcal{W}$. Repeat this step till no more parties can be removed from $\mathcal{W}$.
    - Run algorithm AlgStar on $G_D[\mathcal{W}]$, where $G_D[\mathcal{W}]$ denotes the subgraph of $G_D$ induced by the vertices in $\mathcal{W}$. If an $(n, t_s)$-star, say $(\mathcal{E}, F)$, is obtained, then broadcast $(\mathcal{W}, \mathcal{E}, F)$.
  - **Local Computation** — Verifying and Accepting $(\mathcal{W}, \mathcal{E}, F)$: Each $P_i \in \mathcal{P}$ does the following at time $\Delta + T_{WPS} + T_{BC}$.
    - If $(\mathcal{W}, \mathcal{E}, F)$ is received from D’s broadcast through regular-mode, then accept it if following were true at time $\Delta + T_{WPS} + T_{BC}$:
      - There exist no $P_j, P_k \in \mathcal{W}$, such that $\text{NOK}(j, k, q_{jk})$ and $\text{NOK}(k, j, q_{kj})$ messages were received from the broadcast of $P_j$ and $P_k$ respectively through regular-mode, where $q_{jk} \neq q_{kj}$.
      - In the consistency graph $G_i$, $\text{deg}(P_i) \geq n - t_s$ for all $P_j \in \mathcal{W}$.
      - In the consistency graph $G_i$, every $P_j \in \mathcal{W}$ has edges with at least $n - t_s$ parties from $\mathcal{W}$.
      - $(\mathcal{E}, F)$ was an $(n, t_s)$-star in the induced graph $G_i[\mathcal{W}]$.
    - For every $P_j, P_k \in \mathcal{W}$ where the edge $(P_j, P_k)$ is present in $G_i$, the $\text{OK}(j, k)$ and $\text{OK}(k, j)$ messages were received from the broadcast of $P_j$ and $P_k$ respectively, through regular-mode.
  - **Phase V** — Deciding Whether to Go for $(n, t_s)$-star: At time $\Delta + T_{WPS} + 2T_{BC}$, each party $P_i$ participates in an instance of $\Pi_{BA}$ with input $b_i = 0$ if $(\mathcal{W}, \mathcal{E}, F)$ is accepted, else with input $b_i = 1$ and waits for time $T_{BA}$.
  - **Local Computation** — Computing VSS-Share Through $(W, E, F)$: If 0 is the output during the instance of $\Pi_{BA}$, then each $P_i$ does the following.
    - If a $(W, E, F)$ is not yet received, then wait till it is received from D’s broadcast through fall-back mode.
    - If $P_i \in W$, then output $q_i(0)$.
    - Else, initialize $SS_i \rightarrow \emptyset$. Include $P_j \in F$ to $SS_i$, if a WPS-share $q_{ij}$ is computed during $\Pi_{WPS}$. Wait till $|SS_i| \geq t_s + 1$. Then interpolate $\{ (\alpha_j, q_{ij}) \}_{j \in SS_i}$ to get a $t_s$-degree polynomial, say $q_i(x)$, and output $q_i(0)$.
  - **Phase VI** — Broadcasting $(n, t_s)$-star: If the output during the instance of $\Pi_{BA}$ is 1, then D runs AlgStar after every update in its consistency graph $G_D$ and broadcasts $(E', F')$, if it finds an $(n, t_s)$-star $(E', F')$.
  - **Local Computation** — Computing VSS-Share Through $(n, t_s)$-star: If the output during the instance of $\Pi_{BA}$ is 1, then each $P_i$ does the following.
    - Participate in any instance of $\Pi_{BC}$ invoked by D for broadcasting an $(n, t_s)$-star only after time $\Delta + T_{WPS} + 2T_{BC} + T_{BA}$. Wait till some $(E', F')$ is obtained from D’s broadcast (through any mode), which constitutes an $(n, t_s)$-star in $G_i$.
    - If $P_i \in F'$; then output $q_i(0)$, Else, include $P_j \in F'$ to $SS_i$ (initialized to $\emptyset$) if a WPS-share $q_{ij}$ is computed in $\Pi_{WPS}$. Wait till $|SS_i| \geq t_s + 1$. Then interpolate $\{ (\alpha_j, q_{ij}) \}_{j \in SS_i}$ to get a $t_s$-degree polynomial $q_i(x)$ and output $q_i(0)$.

Corresponding to every corrupt $P_i$, the adversary learns $Q(x, \alpha_i)$. Corresponding to every honest $P_i$, the adversary learns $t_s$ number of $q_i(\alpha_j)$ values through pair-wise consistency tests, as these values are computed as WPS-shares, during the instance $\Pi_{WPS}^{(i)}$. However, these values are already included in the view of the adversary (through the univariate polynomials under the adversary’s control). Additionally, from the $t_s$-privacy property of $\Pi_{WPS}$, the view of the adversary remains independent of $q_i(x)$ during $\Pi_{WPS}^{(i)}$, if $P_i$ is honest. Hence no additional information about the polynomials of the honest parties is revealed during the pair-wise consistency checks. Furthermore, no honest $P_i$ ever broadcasts $\text{NOK}(i, j, q_{ij})$ corresponding to any honest $P_j$, since the pair-wise consistency check will always pass for every pair of honest parties.

We next prove the correctness property in a synchronous network.

**Lemma IV.12 (Correctness):** In protocol $\Pi_{VSS}$, if D is honest and network is synchronous, then each honest $P_i$ outputs $q_i(\alpha_i)$ within time $T_{VSS} = \Delta + T_{WPS} + 2T_{BC} + T_{BA}$.

**Proof:** Let D be honest and network be synchronous with up to $t_s$ corruptions. During phase I, all honest parties receive $q_i(x) = Q(x, \alpha_i)$ from D within time $\Delta$. Consequently during phase II, each honest $P_i$ invokes the instance $\Pi_{WPS}^{(i)}$ with input $q_i(x)$. From the $t_s$-correctness of $\Pi_{WPS}$ in the synchronous network, corresponding to each honest $P_i$, every honest $P_j$ computes the WPS-share $q_{ij} = q_i(\alpha_j)$, at time $\Delta + T_{WPS}$. Consequently, during phase III, every honest party broadcasts an OK message for every other honest party, since $q_{ij} = q_i(\alpha_j)$ holds, for every pair of honest parties $P_i, P_j$ from the

![Fig. 4. The best-of-both-worlds VSS protocol for a single polynomial.](image-url)
Note that every honest party participates with some input during the instance of the synchronous network. Moreover, if D receives a corrupt message from any party P_i, it will eventually broadcast the correct message to D’s consistency graph G_D. D then computes the set W and all honest parties will be present in W. Moreover, the honest parties will form a clique of size at least n - t_s in the subgraph G_D[W] at time \Delta + T_WPS + T_BC. Hence, D will find an (n, t_a) - star (E, F) in G_D[W] and broadcast (W, E, F) during phase IV. By the t_s-validity of \Pi_{BC} in the synchronous network, all honest parties will receive (W, E, F) through regular-mode at time \Delta + T_WPS + 2T_BC. Moreover, all honest parties will accept (W, E, F) and participate with input 0 in the instance of \Pi_{BA}. By the t_s-validity and t_s-guaranteed liveness of \Pi_{BA} in the synchronous network, the output of the \Pi_{BA} instance will be 0 for every honest party at time \Delta + T_WPS + 2T_BC. Now consider an arbitrary honest party P_i. Since P_i \in W, P_i outputs s_i = q_i(0) = Q(0, \alpha_i) = q(\alpha_i). □

We next prove the correctness property in the asynchronous network.

Lemma IV.13 (t_a-Correctness): In protocol \Pi_{VSS}, if D is honest and the network is asynchronous, then almost-surely, each honest P_i eventually outputs q(\alpha_i).

Proof: Let D be honest and network be asynchronous with up to t_a corruptions. We first note that every honest P_i eventually broadcasts OK(i, j) message, corresponding to every honest P_j. This is because both P_i and P_j eventually receive q_j(x) = Q(x, \alpha_i) and q_i(x) = Q(x, \alpha_j) respectively from D. Moreover, P_j participates with input 0 during \Pi_{WPS}. From the t_a-correctness of \Pi_{WPS} in the asynchronous network, party P_i eventually computes the WPS-share q_{ji} = q_j(\alpha_i) during \Pi_{WPS}. Moreover, q_{ji} = q_{ij} holds. Note that any honest party participates with some input in the instance of \Pi_{BA} at local time \Delta + T_WPS + 2T_BC. Hence, from the t_a-almost-surely liveness and t_a-consistency properties of \Pi_{BA} in the asynchronous network, almost-surely, all honest parties eventually compute a common output during the instance of \Pi_{BA}. Now there are two possible cases:

- The output of \Pi_{BA} is 0: From the t_a-validity of \Pi_{BA} in the asynchronous network, this means that at least one honest party, say P_h, participated with input 0 during the instance of \Pi_{BA}. This implies that P_h has received (W, E, F) from the broadcast of D through regular-mode and accepted it. Hence, by the t_a-weak validity and t_a-fallback validity of \Pi_{BC} in the asynchronous network, all honest parties will eventually receive (W, E, F) from the broadcast of D. We claim that every honest P_i will eventually get Q(x, \alpha_i). This will imply that eventually every honest P_i outputs s_i = Q(0, \alpha_i) = q(\alpha_i). To prove the claim, consider an arbitrary honest party P_i. There are two possible cases:

  - P_i \in W: In this case, P_i already has Q(x, \alpha_i), received from D.
  - P_i \notin W: In this case, we first note that there will be at least t_s + 1 parties, who are eventually included in SS_i. This follows from the fact that there are at least t_s + 1 honest parties P_i in F. And corresponding to every honest P_i = F, party P_i will eventually compute the WPS-share q_{ji} in the instance \Pi_{WPS}, which follows from the t_a-correctness of \Pi_{WPS} in the asynchronous network. We next claim that corresponding to every P_i \in SS, the value q_{ji} computed by P_i is the same as Q(x, \alpha_i).

The claim is obviously true for every honest P_i \in SS, so consider a corrupt P_i \in SS. We first note that the input polynomial q_j(x) of P_j during \Pi_{WPS} is the same as Q(x, \alpha_j). This is because P_j \in W, since F \subseteq W. Thus, P_j has edges with at least n - t_s parties in W and with at least n - t_a \geq t_s honest parties from W in G_D[W]. Let H be the set of honest parties in W with which P_j has edges in G_D[W]. This implies that every P_k \in H has broadcasted the OK(j, s) message after verifying that q_{jk} = q_k(\alpha_j) holds, where the polynomial q_{x}(\alpha_j) held by P_k is the same as Q(x, \alpha_k) and where the WPS-share q_{jk} computed by P_k during \Pi_{WPS} is the same as q_j(\alpha_k); the last property follows from the t_a-strong commitment of \Pi_{WPS} in the synchronous network. Since |H| > t_s, it implies that at least t_a + 1 honest parties P_k have verified that q_{j}(\alpha_k) = Q(\alpha_i, \alpha_k) holds. This further implies that q_j(x) = Q(x, \alpha_j), since two different t_a-degree polynomials can have at most t_a common values. Since P_i has computed the WPS-share q_{ji} during \Pi_{WPS}, from the t_a-strong commitment of \Pi_{WPS} in synchronous network, it follows that q_{ji} = q_j(\alpha_i) = Q(\alpha_i, \alpha_j) = Q(\alpha_i, \alpha_i). The last equality follows since each Q(x, y) is a symmetric bivariate polynomial.

- The output of \Pi_{BA} is 1: As mentioned earlier, since D is honest, every pair of honest parties eventually broadcasts OK messages corresponding to each other, as the pairwise consistency check between them will be eventually positive. From the t_a-weak validity and t_a-fallback validity of \Pi_{BC} in the asynchronous network, these messages are eventually delivered to every honest party. Also, from the t_a-weak consistency and t_a-fallback consistency of \Pi_{BC} in the asynchronous network, any OK message which is received by D, will be eventually received by every other honest party as well. As there will be at least n - t_a honest parties, a clique of size at least n - t_a will eventually form in the consistency graph of every honest party. Hence, D will eventually find an (n, t_a) - star, say (E', F'), in its consistency graph and broadcast it. From the t_a-weak validity and t_a-fallback validity of \Pi_{BC} in the asynchronous network, (E', F') will be eventually received by every honest party. Moreover, (E', F') will be eventually an (n, t_a) - star in every honest party’s consistency graph. We now claim that every honest P_i will eventually get Q(x, \alpha_i). This will imply that eventually
every honest $P_i$ outputs $s_i = Q(0, \alpha_i) = q(\alpha_i)$. To prove the claim, consider an arbitrary honest party $P_i$. There are two possible cases.

- $P_i \in \mathcal{F}^1$: In this case, $P_i$ already has $Q(x, \alpha_i)$ received from $D$.

- $P_i \notin \mathcal{F}^1$: In this case, we note that there will be at least $t_s + 1$ parties, who are eventually included in $SS_t$, such that corresponding to every $P_j \in SS_t$, the value $q_{ji}$ computed by $P_j$ during $\Pi_{WPS}^{(j)}$ is the same as $Q(x, \alpha_i)$. The proof for this will be similar to the case when $P_i \notin \mathcal{W}$ and the output of $\Pi_{BA}$ is 0 and so we skip the proof.

Before we proceed to prove the strong commitment property in the synchronous network, we prove a helping lemma.

**Lemma IV.14:** Let $D$ be corrupt and the network be synchronous. If any honest party receives a $(\mathcal{W}, \mathcal{E}, \mathcal{F})$ from the broadcast of $D$ through regular-mode and accepts $(\mathcal{W}, \mathcal{E}, \mathcal{F})$ at time $\Delta + T_{WPS} + 2T_{BC}$, then all the following hold:

- All honest parties in $\mathcal{W}$ have received their respective $t_s$-degree univariate polynomials from $D$ within time $\Delta$.

- The univariate polynomials $q_j(x)$ of all honest parties $P_i$ in $\mathcal{W}$ lie on a unique $(t_s, t_s)$-degree symmetric bivariate polynomial, say $Q^*(x, y)$.

- At time $\Delta + T_{WPS} + 2T_{BC}$, every honest party accepts $(\mathcal{W}, \mathcal{E}, \mathcal{F})$.

**Proof:** Let $D$ be corrupt and network be synchronous with up to $t_s$ corruptions. As per the lemma condition, let $P_h$ be an honest party who receives some $(\mathcal{W}, \mathcal{E}, \mathcal{F})$ from the broadcast of $D$ through regular-mode and accepts it at time $\Delta + T_{WPS} + 2T_{BC}$. From the protocol steps, it then follows that the following must be true for $P_h$ at time $\Delta + T_{WPS} + T_{BC}$:

- There does not exist any $P_j, P_k \in \mathcal{W}$, such that $\text{NO}\text{K}(j, k, q_{jk})$ and $\text{NO}\text{K}(k, j, q_{kj})$ messages were received from the broadcast of $P_j$ and $P_k$ respectively through regular-mode, such that $q_{jk} \neq q_{kj}$.

- In $P_h$’s consistency graph $G_h$, $\deg(P_j) \geq n - t_s$ for all $P_j \in \mathcal{W}$ and $P_j$ has edges with at least $n - t_s$ parties from $\mathcal{W}$.

- $(\mathcal{E}, \mathcal{F})$ was an $(n, t_s)$-star in the induced subgraph $G_h[\mathcal{W}]$, such that for every $P_j, P_k \in \mathcal{W}$ where the edge $(P_j, P_k)$ is present in $G_h$, the $\text{OK}(j, k)$ and $\text{OK}(k, j)$ messages were received from the broadcast of $P_j$ and $P_k$ respectively through regular-mode.

We prove the first part of the lemma through a contradiction. So let $P_j \in \mathcal{W}$ be an honest party who receives its $t_s$-degree univariate polynomial from $D$, say $q_j(x)$, at time $\Delta + \delta$, where $\delta > 0$. Moreover, let $P_k \in \mathcal{W}$ be an honest party such that $P_k$ has an edge with $P_h$ (note that $P_j$ has edges with at least $n - 2t_s > t_s + t_h$ honest parties in $\mathcal{W}$). As stated above, at time $\Delta + T_{WPS} + T_{BC}$, party $P_h$ has received the message $\text{OK}(k, j)$ from the broadcast of $P_k$ through regular-mode. From the protocol steps, $P_j$ waits till its local time becomes a multiple of $\Delta$, before it participates with input $q_j(x)$ in the instance $\Pi_{WPS}^{(j)}$. Hence, $P_j$ must have invoked $\Pi_{WPS}^{(j)}$ at time $c\cdot\Delta$, where $c \geq 2$. Since the network is synchronous, from the $t_s$-correctness of $\Pi_{WPS}$ in the synchronous network, party $P_k$ will compute its WPS-share $q_j$ during $\Pi_{WPS}^{(j)}$ at time $c \cdot \Delta + T_{WPS}$. Hence the result of the pair-wise consistency test with $P_j$ will be available to $P_k$ at the time $c \cdot \Delta + T_{WPS}$. As a result, $P_k$ starts broadcasting $\text{OK}(k, j)$ message only at time $c \cdot \Delta + T_{WPS}$.

Since $P_k$ is honest, from the $t_s$-validity property of $\Pi_{BC}$ in the synchronous network, it will take exactly $T_{BC}$ time for the message $\text{OK}(k, j)$ to be received through regular-mode, once it is broadcast. This implies that $P_h$ will receive the message $\text{OK}(k, j)$ at time $c \cdot \Delta + T_{WPS} + T_{BC}$, where $c \geq 2$. However, this is a contradiction, since the $\text{OK}(k, j)$ message has been received by $P_h$ at time $\Delta + T_{WPS} + T_{BC}$.

To prove the second part of the lemma, we will show that the univariate polynomials $q_j(x)$ of all the honest parties $P_i \in \mathcal{W}$ are pair-wise consistent. Since there will be at least $n - 2t_s > t_s$ honest parties in $\mathcal{W}$, from Lemma II.2, this will imply that all these polynomials lie on a unique $(t_s, t_s)$-degree symmetric bivariate polynomial, say $Q^*(x, y)$. So consider an arbitrary pair of honest parties $P_j, P_k \in \mathcal{W}$. From the first part of the claim, both $P_j$ and $P_k$ must have received their respective univariate polynomials $q_j(x)$ and $q_k(x)$ by time $\Delta$. Moreover, from the $t_s$-correctness property of $\Pi_{WPS}$ in the synchronous network, $P_j$ and $P_k$ will compute the WPS-shares $q_{jk} = q_k(\alpha_j)$ and $q_{kj} = q_j(\alpha_k)$ at time $\Delta + T_{WPS}$ during $\Pi_{WPS}^{(k)}$ and $\Pi_{WPS}^{(j)}$ respectively. Since $P_j$ and $P_k$ are honest, if $q_{jk} \neq q_{kj}$, they would broadcast $\text{NO}\text{K}(j, k, q_{jk})$ and $\text{NO}\text{K}(k, j, q_{kj})$ messages respectively at time $\Delta + T_{WPS}$. From the $t_s$-validity property of $\Pi_{BC}$ in the synchronous network, $P_h$ will receive these messages through regular-mode at time $\Delta + T_{WPS} + T_{BC}$. Consequently, $P_h$ will not accept $(\mathcal{W}, \mathcal{E}, \mathcal{F})$, which is a contradiction.

To prove the third part of the lemma, we note that since $P_h$ receives $(\mathcal{W}, \mathcal{E}, \mathcal{F})$ from the broadcast of $D$ through regular-mode at time $\Delta + T_{WPS} + 2T_{BC}$, it implies that $D$ must have started broadcasting $(\mathcal{W}, \mathcal{E}, \mathcal{F})$ latest at time $\Delta + T_{WPS} + T_{BC}$. This is because it takes $T_{BC}$ time for the regular-mode of $\Pi_{BC}$ to generate an output. From the $t_s$-consistency property of $\Pi_{BC}$ in the synchronous network, it follows that every honest party will also receive $(\mathcal{W}, \mathcal{E}, \mathcal{F})$ from the broadcast of $D$ through regular-mode at time $\Delta + T_{WPS} + 2T_{BC}$. Similarly, since at time $\Delta + T_{WPS} + T_{BC}$, party $P_h$ has received the $\text{OK}(j, k)$ and $\text{OK}(k, j)$ messages through regular-mode from the broadcast of every $P_j, P_k \in \mathcal{W}$ where $(P_j, P_k)$ is an edge in $P_h$’s consistency graph, it follows that these messages started getting broadcasted latest at time $\Delta + T_{WPS}$. From the $t_s$-validity and $t_s$-consistency properties of $\Pi_{BC}$ in the synchronous network, it follows that every honest party receives these broadcast messages through regular-mode at time $\Delta + T_{WPS} + T_{BC}$. Hence $(\mathcal{E}, \mathcal{F})$ will constitute an $(n, t_s)$-star in the induced subgraph $G_h[\mathcal{W}]$ of every honest party $P_i$’s consistency-graph at time $\Delta + T_{WPS} + T_{BC}$ and consequently, every honest party accepts $(\mathcal{W}, \mathcal{E}, \mathcal{F})$.

We next prove the strong commitment property in the synchronous network.

**Lemma IV.15** ($t_s$-Strong Commitment): In protocol $\Pi_{WPS}$, if $D$ is corrupt and the network is synchronous, then either no honest party computes any output or there exists a $t_s$-degree
polynomial, say \( q^*(\cdot) \), such that each honest \( P_i \) eventually outputs \( q^*(\alpha_i) \), where the following hold.

- If any honest \( P_i \) computes its output at time \( T_{VSS} = \Delta + T_{WPS} + 2T_{BC} + T_{BA} \), then every honest party obtains its output at time \( T_{VSS} \).
- If any honest \( P_i \) computes its output at time \( T \) where \( T > T_{VSS} \), then every honest party computes its output by time \( T + 2\Delta \).

**Proof:** Let \( D \) be corrupt and network be synchronous with up to \( t_s \) corruptions. If no honest party computes any output, then the lemma holds trivially. So consider the case when some honest party computes an output. Now, there are two possible cases.

- **At least one honest party, say \( P_h \), has received some \((W, E, F)\) from the broadcast of \( D \) through regular-mode and accepted \((W, E, F)\) at time \( \Delta + T_{WPS} + 2T_{BC} \):** In this case, from Lemma IV.14, the polynomials \( q_i(x) \) of all honest parties in \( W \) are guaranteed to lie on a unique \((t_s, t_s)\)-degree symmetric bivariate polynomial, say \( Q^*(x, y) \). As per the protocol steps, \( P_h \) has also verified that \( F \subseteq W \), by checking that \((E, F)\) constitutes an \((n, t_s)\)-star in the induced subgraph \( G_{\mathcal{h}}[W] \). Hence the polynomials \( q_i(x) \) of all honest parties in \( F \) also lie on \( Q^*(x, y) \). Moreover, from Lemma IV.14, all honest parties accept \((W, E, F)\) at time \( \Delta + T_{WPS} + 2T_{BC} \). Hence, every honest party participates in the instance of \( \Pi_{BA} \) with input 0. Consequently, by the \( t_s\)-validity and \( t_s\)-guaranteed linearity properties of \( \Pi_{BA} \) in the synchronous network, all honest parties compute the output 0 during the instance of \( \Pi_{BA} \) at time \( T_{VSS} = \Delta + T_{WPS} + 2T_{BC} + T_{BA} \). Let \( q^*(\cdot) = Q^*(0, y) \) and consider an arbitrary honest party \( P_i \). We wish to show that \( P_i \) has \( q_i(x) = Q^*(x, \alpha_i) \) at time \( T_{VSS} \), which will imply that \( P_i \) outputs \( s_i = q_i(0) \) at time \( T_{VSS} \), which will be the same as \( q^*(\alpha_i) \). For this, we consider the following two possible cases.

- **\( P_i \in W \):** In this case, \( P_i \) has already received \( q_i(x) \) from \( D \) within time \( \Delta \). This follows from Lemma IV.14.

- **\( P_i \notin W \):** In this case, we claim that, at time \( T_{VSS} \), there will be at least \( t_s + 1 \) parties from \( F \) who are included in \( SS_i \), such that, corresponding to every \( P_j \in SS_i \), party \( P_i \) will have the value \( q_j \), which will be the same as \( Q^*(\alpha_j, \alpha_i) \). Namely, there are at least \( t_s + 1 \) honest parties in \( F \), who will be included in \( SS_i \) and the claim will trivially be true for those parties, due to the \( t_s\)-correctness property of \( \Pi_{WPS} \) in the synchronous network. On the other hand, if any corrupt \( P_j \in F \) is included in \( SS_i \), then the input polynomial of \( P_j \) during \( \Pi_{WPS} \) will be pair-wise consistent with the polynomials of at least \( t_s + 1 \) honest parties in \( W \) and hence will be the same as \( Q^*(x, \alpha_j) \).

Moreover, from the \( t_s\)-weak commitment of \( \Pi_{WPS} \) in the synchronous network, the WPS-share \( q_{ji} \) computed by \( P_i \) during \( \Pi_{WPS}^{(j)} \) will be the same as \( Q^*(\alpha_j, \alpha_i) \), which will be the same as \( Q^*(\alpha_j, \alpha_i) \), since \( Q^*(x, y) \) is a symmetric bivariate polynomial. Hence, \( P_i \) will interpolate \( q_i(x) \).

- **No honest party has received any \((W, E, F)\) from the broadcast of \( D \) through regular-mode and accepted \((W, E, F)\) at time \( \Delta + T_{WPS} + 2T_{BC} \):** This implies that all honest parties participate in the instance of \( \Pi_{BA} \) with input 1. Hence, by the \( t_s\)-validity and \( t_s\)-guaranteed linearity of \( \Pi_{BA} \) in the synchronous network, all honest parties obtain the output 1 during the instance of \( \Pi_{BA} \) at time \( \Delta + T_{WPS} + 2T_{BC} + T_{BA} \). Let \( P_h \) be the first honest party who computes an output. This means that \( P_h \) has received a pair \((E', F')\) from the broadcast of \( D \), such that \((E', F')\) constitutes an \((n, t_s)\)-star in \( P_h \)'s consistency graph. Let \( T \) be the time when \((E', F')\) constitutes an \((n, t_s)\)-star in \( P_h \)'s consistency graph. This implies that, at time \( T \), party \( P_h \) has received \((E', F')\) from \( D \)'s broadcast and also all the \( OK(\star, \star) \) messages from the broadcast of respective parties in \( E' \) and \( F' \). From the protocol steps, \( T > T_{VSS} \), since the honest parties participate in the instance of \( \Pi_{BC} \) through which \( D \) has broadcast \((E', F')\) only after time \( T_{VSS} \). By the \( t_s\)-consistency and \( t_s\)-fallback consistency properties of \( \Pi_{BC} \) in the synchronous network, all honest parties will receive \((E', F')\) from the broadcast of \( D \) by time \( T + 2\Delta \). Moreover, \((E', F')\) will constitute an \((n, t_s)\)-star in every honest party’s consistency graph by time \( T + 2\Delta \). This is because all the \( OK \) messages which are received by \( P_h \) from the broadcast of various parties in \( E' \) and \( F' \) are guaranteed to be received by every honest party by time \( T + 2\Delta \). Since \( |E'| \geq n - 2t_a > 2t_s + (t_s - t_a) > 2t_s \), it follows that \( E' \) has at least \( t_s + 1 \) honest parties. Moreover, the univariate polynomials \( (q_j(x), q_k(x)) \) of every pair of honest parties \( P_j, P_k \in E' \) will be pair-wise consistent and hence, lie on a unique \((t_s, t_s)\)-degree symmetric bivariate polynomial, say \( Q^*(x, y) \). Similarly, the univariate polynomial \( q_i(x) \) of every honest party \( P_i \) in \( F' \) is pair-wise consistent with the univariate polynomials \( q_j(x) \) of all the honest parties in \( E' \) and hence lie on \( Q^*(x, y) \) as well. Let \( q^*(\cdot) \triangleq Q^*(0, y) \). We show that every honest \( P_i \) outputs \( q^*(\alpha_i) \), by time \( T + 2\Delta \). For this it is enough to show that each honest \( P_i \) has \( q_i(x) = Q^*(x, \alpha_i) \) by time \( T + 2\Delta \), as \( P_i \) outputs \( q_i(0) \), which will be the same as \( q^*(\alpha_i) \). Consider an arbitrary honest party \( P_i \). There are two possible cases.

- **\( P_i \in F' \):** In this case, \( P_i \) has already received \( Q^*(x, \alpha_i) \) from \( D \), well before time \( T + 2\Delta \).

- **\( P_i \notin F' \):** In this case, we claim that by time \( T + 2\Delta \), there will be at least \( t_s + 1 \) parties from \( F' \), who are included in \( SS_i \), such that, corresponding to every \( P_j \in SS_i \), party \( P_i \) will have the value \( q_j \), which will be the same as \( Q^*(\alpha_j, \alpha_i) \). The proof for this is very similar to the previous case when \( P_i \notin W \) and the output of \( \Pi_{BA} \) is 0. Namely every honest \( P_j \in F' \) will be included in \( SS_i \). This is because \( P_i \) starts broadcasting \( OK \) messages for other parties in \( E' \) only after invoking instance \( \Pi_{WPS}^{(j)} \) with input \( q_j(x) \). Hence, by time \( T + 2\Delta \), the WPS-share \( q_{ji} \) from the instance \( \Pi_{WPS}^{(j)} \) will be available with \( P_i \). On the other hand, if a corrupt \( P_j \in F' \) is included in \( SS_i \), then also the claim
holds (the proof for this is similar to the proof of the \( t_a \)-correctness property in the asynchronous network in Lemma IV.13).

We finally prove the strong commitment property in an asynchronous network.

**Lemma IV.16 (\( t_a \)-Strong Commitment):** In protocol \( \Pi_{\text{VSS}} \), if \( D \) is corrupt and the network is asynchronous, then either no honest party computes any output or there exists some \( t_a \)-degree polynomial, say \( q^*(\cdot) \), such that almost-surely, every honest \( P_i \) eventually outputs \( q^*(\alpha_i) \).

**Proof:** Let \( D \) be corrupt and the network be asynchronous with up to \( t_a \) corruptions. If no honest party computes any output, then the lemma holds trivially. So, consider the case with up to \( t_a \) corruptions. If no honest party computes an output, we note that every honest party participates with some input in the instance of \( \Pi_{\text{BA}} \) at local time \( \Delta + T_{\text{WPS}} + 2T_{\text{BC}} \). Hence, from the \( t_a \)-almost-surely liveness and \( t_a \)-consistency properties of \( \Pi_{\text{BA}} \) in the asynchronous network, almost-surely, all honest parties eventually compute a common output during the instance of \( \Pi_{\text{BA}} \). Now there are two possible cases:

- **The output of \( \Pi_{\text{BA}} \) is 0:** From the \( t_a \)-validity of \( \Pi_{\text{BA}} \) in the asynchronous network, it follows that at least one honest party, say \( P_i \), participated with input 0 during the instance of \( \Pi_{\text{BA}} \). This means that \( P_i \) has received some \( (W, E, F) \) from the broadcast of \( D \) through regular-mode and accepted it at local time \( \Delta + T_{\text{WPS}} + 2T_{\text{BC}} \). Hence, by the \( t_a \)-weak consistency and \( t_a \)-fallback consistency of \( \Pi_{\text{BC}} \) in the asynchronous network, all honest parties will eventually receive \( (W, E, F) \) from the broadcast of \( D \). There will be at least \( n - 2t_a - t_a > t_a \) honest parties \( P_i \) in \( E \), whose univariate polynomials \( q_i(x) \) are pair-wise consistent and hence lie on a unique \( (t_s, t_a) \)-degree symmetric bivariate polynomial, say \( Q^*(x, y) \). Similarly, the univariate polynomial \( q_i(x) \) of every honest \( P_i \in F \) will be pair-wise consistent with the univariate polynomials \( q_j(x) \) of all the honest parties \( P_j \in E \) and hence lie on \( Q^*(x, y) \) as well. Let \( q^*(\cdot) \triangleq Q^*(0, y) \). We claim that every honest \( P_i \) will eventually have \( Q^*(x, \alpha_i) \). This will imply that eventually every honest \( P_i \) outputs \( s_i = Q^*(0, \alpha_i) = q^*(\alpha_i) \). To prove the claim, consider an arbitrary honest party \( P_i \). There are three possible cases:

- \( P_i \in W \) and \( P_i \in F \): In this case, \( P_i \) has received the polynomials \( q_j(x) \) from \( D \) and since \( P_i \in F \), the condition \( q_i(x) = Q^*(x, \alpha_i) \) holds.

- \( P_i \in W \) and \( P_i \notin F \): In this case, \( P_i \) has received the polynomial \( q_j(x) \) from \( D \). Since \( |W| \geq n - t_a \) and \( |F| \geq n - t_s \), \( |W \cap F| \geq n - 2t_s > t_a + t_s \). From the protocol steps, the polynomial \( q_i(x) \) is pair-wise consistent with the polynomials \( q_j(x) \) at least \( n - t_s \) parties \( P_j \in W \), since \( P_i \) has edges with at least \( n - t_s \) parties \( P_j \) within \( W \). Now among these \( n - t_s \) parties, at least \( n - 2t_s \) parties will be from \( F \), of which at least \( n - 2t_s \) parties will be honest. Hence, \( q_i(x) \) is pair-wise consistent with the \( q_j(x) \) polynomials of at least \( t_s + 1 \) honest parties \( P_j \in F \). Now since the \( q_j(x) \) polynomials of all the honest parties in \( F \) lie on \( Q^*(x, y) \), it implies that \( q_i(x) = Q^*(x, \alpha_i) \) holds.

- \( P_i \notin W \): In this case, similar to the proof of Lemma IV.13, one can show that \( P_i \) eventually includes at least \( t_a + 1 \) parties from \( F \) in \( SS_i \). And the value computed by \( P_i \) corresponding to any \( P_j \in SS_i \) will be the same as \( Q^*(\alpha_j, \alpha_i) \). Hence, \( P_i \) will eventually interpolate \( Q^*(x, \alpha_i) \).

**The output of \( \Pi_{\text{BA}} \) is 1:** Let \( P_h \) be the first honest party who computes an output in \( \Pi_{\text{VSS}} \). This means that \( P_h \) has received some \( (E', F') \) from the broadcast of \( D \), such that \( (E', F') \) constitutes an \((n, t_a)\)-star in \( P_h \)'s consistency graph. By the \( t_a \)-weak consistency and \( t_a \)-fallback consistency properties of \( \Pi_{\text{BC}} \) in the asynchronous network, all honest parties eventually receive \( (E', F') \) from the broadcast of \( D \). Moreover, since the consistency graphs are constructed based on the broadcast \( OK \) messages and since \( (E', F') \) constitutes an \((n, t_a)\)-star in every honest party's consistency graph, as the corresponding \( OK \) messages are eventually received by every honest party. Since \( |E'| \geq n - 2t_a > 2t_a + (t_a - t_a) > 2t_a \), it follows that \( E' \) at least \( t_a + 1 \) honest parties \( P_i \), whose univariate polynomials \( q_i(x) \) are pair-wise consistent and hence lie on a unique \((t_s, t_a)\)-degree symmetric bivariate polynomial, say \( Q^*(x, y) \). Similarly, since the univariate polynomials \( q_j(x) \) of every honest party \( P_i \) in \( F' \) is pair-wise consistent with the univariate polynomials \( q_j(x) \) of all the honest parties \( P_j \) in \( E' \), it implies that the polynomials \( q_j(x) \) of all the honest parties \( P_j \) in \( F' \) also lie on \( Q^*(x, y) \) as well. Let \( q^*(\cdot) \triangleq Q^*(0, y) \). We show that every honest \( P_i \) eventually outputs \( q^*(\alpha_i) \). For this it is enough to show that each honest \( P_i \) eventually gets \( q_i(x) = Q^*(x, \alpha_i) \), as \( P_i \) outputs \( q_i(0) \), which will be the same as \( q^*(\alpha_i) \). Consider an arbitrary honest party \( P_i \). There are two possible cases:

- \( P_i \in F' \): In this case, \( P_i \) already has received \( Q^*(x, \alpha_i) \) from \( D \).

- \( P_i \notin F' \): Again in this case, one can show that \( P_i \) eventually includes at least \( t_a + 1 \) parties from \( F' \) in \( SS_i \). And the value computed by \( P_i \) corresponding to any \( P_j \in SS_i \) will be the same as \( Q^*(\alpha_j, \alpha_i) \). Hence, \( P_i \) will eventually interpolate \( Q^*(x, \alpha_i) \).

**Lemma IV.17:** Protocol \( \Pi_{\text{VSS}} \) incurs a communication of \( O(n^5 \log |F|) \) bits and invokes \( n + 1 \) instance of \( \Pi_{\text{BA}} \).

**Proof:** The proof follows from Lemma IV.9 and the fact that each party acts as a dealer and invokes an instance of \( \Pi_{\text{WPS}} \) with a \( t_a \)-degree polynomial. Hence, the total communication cost due to the instances of \( \Pi_{\text{WPS}} \) in \( \Pi_{\text{VSS}} \) will be \( O(n \cdot n^4 \log |F|) = O(n^5 \log |F|) \) bits, along with \( n \) instances of \( \Pi_{\text{BA}} \). Additionally, there is an instance of \( \Pi_{\text{BA}} \) invoked in \( \Pi_{\text{VSS}} \) to agree on whether some \( (W, E, F) \) is accepted.
We next discuss the modifications needed in the protocol \( \Pi_{\text{VSS}} \), if the input for \( D \) consists of \( L \) number of \( t_s \)-degree polynomials.

**Protocol \( \Pi_{\text{VSS}} \) for \( L \) Polynomials:** If \( D \) has \( L \) polynomials as input for \( \Pi_{\text{VSS}} \), then we make similar modifications as done for \( \Pi_{\text{VPS}} \) handling \( L \) polynomials, with each party broadcasting a single OK/NOK message for every other party. To void repetition, we skip the formal details of the modified protocol and the proof of its properties, as stated in Theorem IV.18.

**Theorem IV.18:** Let \( n > 3t_s + t_a \) and let \( D \) has \( L \) number of \( t_s \)-degree polynomials \( q^{(1)}(\cdot), \ldots, q^{(L)}(\cdot) \) as input for \( \Pi_{\text{VSS}} \) where \( L \geq 1 \). Moreover, let \( T_{\text{VSS}} = \Delta + T_{\text{VPS}} + 2T_{\text{BC}} + T_{\text{BA}} \). Then protocol \( \Pi_{\text{VSS}} \) achieves the following properties:

- If \( D \) is honest, then the following hold.
  - \( t_s \)-correctness: In a synchronous network, each (honest) \( P_i \) eventually outputs \( \{q^{(i)}(\alpha_i)\}_{i=1,\ldots,L} \) at time \( T_{\text{VSS}} \).
  - \( t_s \)-correctness: In an asynchronous network, almost surely, each (honest) \( P_i \) eventually outputs \( \{q^{(i)}(\alpha_i)\}_{i=1,\ldots,L} \).
  - \( t_s \)-privacy: Irrespective of the network type, the view of the adversary remains independent of the polynomials \( q^{(1)}(\cdot), \ldots, q^{(L)}(\cdot) \).
  - If \( D \) is corrupt, then either no honest party computes any output or there exist \( t_s \)-degree polynomials \( \{q^{(i)}(\cdot)\}_{i=1,\ldots,L} \) such that the following hold.
  - \( t_s \)-strong commitment: each honest \( P_i \) eventually outputs \( \{q^{(i)}(\alpha_i)\}_{i=1,\ldots,L} \), such that one of the following holds.
    - If any honest \( P_i \) computes its output at time \( T_{\text{VSS}} \), then all honest parties compute their output at time \( T_{\text{VSS}} \).
    - If any honest \( P_i \) computes its output at time \( T \) where \( T > T_{\text{VSS}} \), then every honest party computes its output by time \( T + 2\Delta \).
  - Irrespective of the network type, the protocol incurs a communication of \( O(n^3\log |F| + n^5 \log |F|) \) bits from the honest parties and invokes \( n + 1 \) instances of \( \Pi_{\text{BA}} \).

**V. Agreement on a Common Subset (ACS)**

In this section, we present a best-of-all-worlds protocol for agreement on a common subset, which will later be used in our preprocessing phase protocol, as well as in our circuit-evaluation protocol. In the protocol, each party \( P_i \in \mathcal{P} \) has \( L \) number of \( t_s \)-degree polynomials as input for an instance of \( \Pi_{\text{VSS}} \), which \( P_i \) is supposed to invoke as a dealer.\(^{13}\) As corrupt parties may not invoke their instances of \( \Pi_{\text{VSS}} \) as dealers, the parties may obtain points lying on the polynomials of only \( n - t_s \) parties (even in a synchronous network). However, in an asynchronous network, different parties may obtain points on the polynomials of different subsets of \( n - t_s \) parties. The ACS protocol allows the parties to agree on a common subset \( \mathcal{C} \) of at least \( n - t_s \) parties, such that all (honest) parties are guaranteed to receive points lying on the polynomials of the parties in \( \mathcal{C} \). Additionally, the protocol guarantees that in a synchronous network, all honest parties are present in \( \mathcal{C} \). Looking ahead, this property will be very crucial when the ACS protocol is used during circuit-evaluation, as it will ensure that in a synchronous network, the inputs of all honest parties are considered for the circuit-evaluation.

The ACS protocol is presented in Fig 5, where, for simplicity, we assume that \( L = 1 \). Later, we discuss the modifications required for \( L > 1 \). In the protocol, each party acts as a dealer and invokes an instance of \( \Pi_{\text{VSS}} \) to verifiably distribute points on its polynomial. If the network is synchronous then, after time \( T_{\text{VSS}} \), all honest parties would have received points corresponding to the polynomials of the honest dealers. Hence, after (local) time \( T_{\text{VSS}} \), the parties locally check for the instances of \( \Pi_{\text{VSS}} \) in which they have received an output. Based on this, the parties start participating in \( n \) instances of \( \Pi_{\text{BA}} \), where the \( j^{th} \) instance is used to decide whether \( P_j \) should be included in \( \mathcal{C} \). The input criteria for these \( \Pi_{\text{BA}} \) instances is the following: if a party has received an output in the \( \Pi_{\text{VSS}} \) instance with \( P_j \) as the dealer, then the party starts participating with input 1 in the corresponding \( \Pi_{\text{BA}} \) instance. Now, once an output is obtained from all the \( n \) instances of \( \Pi_{\text{BA}} \), then the parties start participating with input 0 in any of the remaining \( \Pi_{\text{BA}} \) instances for which the parties may have not provided any input yet. Finally, once an output is obtained from all the \( n \) instances of \( \Pi_{\text{BA}} \), party \( P_j \) is included in \( \mathcal{C} \) if and only if the output of the corresponding \( \Pi_{\text{BA}} \) instance is 1. Since the parties wait for time \( T_{\text{VSS}} \) before starting the \( \Pi_{\text{BA}} \) instances, it is ensured that all honest dealers are included in \( \mathcal{C} \) in a synchronous network.

We next prove the properties of the protocol \( \Pi_{\text{ACS}} \).

**Lemma VI.1:** Protocol \( \Pi_{\text{ACS}} \) achieves the following properties, where every party \( P_i \) has a \( t_s \)-degree polynomial \( f_i(\cdot) \) as input.

- **Synchronous Network:** The following is achieved in the presence of up to \( t_s \) corruptions.
  - \( t_s \)-Correctness: at time \( T_{\text{ACS}} = T_{\text{VSS}} + 2T_{\text{BA}} \), the parties output a common subset \( \mathcal{C} \) of size at least \( n - t_s \), such that all the following hold:
    - All honest parties will be present in \( \mathcal{C} \).
Corresponding to every honest $P_j \in \mathcal{CS}$, every honest $P_i$ has $f_j(\alpha_i)$.

Corresponding to every corrupt $P_j \in \mathcal{CS}$, there exists some $t_a$-degree polynomial, say $f_j^i(\cdot)$, such that every honest $P_i$ has $f_j^i(\alpha_i)$.

Asynchronous Network: The following is achieved in the presence of up to $t_a$ corruptions.

$t_a$-Correctness: almost-surely, the honest parties eventually output a common subset $\mathcal{CS}$ of size at least $n-t_a$, such that all the following hold:
- Corresponding to every honest $P_j \in \mathcal{CS}$, every honest $P_i$ eventually has $f_j^i(\alpha_i)$.
- Corresponding to every corrupt $P_j \in \mathcal{CS}$, there exists some $t_a$-degree polynomial, say $f_j^i(\cdot)$, such that every honest $P_i$ eventually has $f_j^i(\alpha_i)$.

$t_a$-Privacy: Irrespective of the network type, the view of the adversary remains independent of the $f_i(\cdot)$ polynomials of the honest parties.

Irrespective of the network type, the protocol incurs a communication of $\mathcal{O}(n^6 \log |\mathcal{P}|)$ bits from the honest parties and invokes $\mathcal{O}(n^2)$ instances of $\Pi_{BA}$.

Proof: The $t_a$-privacy property simply follows from the $t_a$-privacy property of $\Pi_{VSS}$, while communication complexity follows from the communication complexity of $\Pi_{VSS}$ and the fact that $\mathcal{O}(n)$ instances of $\Pi_{VSS}$ are invoked. We next prove the correctness property.

We first consider a synchronous network with up to $t_a$ corruptions. Let $\mathcal{H}$ be the set of parties, where $|\mathcal{H}| \geq n-t_a$. Corresponding to each $P_j \in \mathcal{H}$, every honest $P_i$ computes the output $f_j(\alpha_i)$ at time $T_{VSS}$ during $\Pi_{VSS}^{(j)}$, which follows from the $t_a$-correctness of $\Pi_{VSS}$ in the synchronous network. Consequently, at time $T_{VSS}$, the set $\mathcal{C}_i$ will be of size at least $n-t_a$ for every honest $P_i$. Now corresponding to each $P_j \in \mathcal{H}$, each honest $P_j$ participates with input 1 in the instance $\Pi_{BA}^{(j)}$ at time $T_{VSS}$. Hence, from the $t_a$-validity and $t_a$-guaranteed liveness of $\Pi_{BA}$ in the synchronous network, it follows that, at time $T_{VSS} + T_{BA}$, every honest $P_i$ computes the output 1 during the instance $\Pi_{BA}^{(j)}$, corresponding to every $P_j \in \mathcal{H}$. Consequently, at time $T_{VSS} + T_{BA}$, every honest party will start participating in the remaining $\Pi_{BA}$ instances for which no input has been provided yet (if there are any). And from the $t_a$-guaranteed liveness and $t_a$-consistency of $\Pi_{BA}$ in the synchronous network, these $\Pi_{BA}$ instances will produce common outputs for every honest party at time $T_{ACS} = T_{VSS} + 2T_{BA}$. Since the set $\mathcal{CS}$ is determined deterministically based on the outputs computed from the $n$ instances of $\Pi_{BA}$, it follows that all the honest parties eventually output the same $\mathcal{CS}$ of size at least $n-t_a$, such that each $P_j \in \mathcal{H}$ will be present in $\mathcal{CS}$. We next wish to show that corresponding to every $P_j \in \mathcal{CS}$, every honest party has received its point on $P_j$’s polynomial.

Consider an arbitrary party $P_j \in \mathcal{CS}$. If $P_j$ is honest, then as argued above, every honest $P_i$ gets $f_j(\alpha_i)$ at time $T_{VSS}$ itself. Next, consider a corrupt $P_j \in \mathcal{CS}$. Since $P_j \in \mathcal{CS}$, it follows that the instance $\Pi_{BA}^{(j)}$ produces the output 1. From the $t_a$-validity property of $\Pi_{BA}$ in the synchronous network, it follows that at least one honest $P_i$ must have participated with input 1 in the instance $\Pi_{BA}^{(j)}$. This implies that $P_i$ must have computed some output during the instance $\Pi_{VSS}^{(j)}$ by time $T_{VSS} + T_{BA}$ and $P_j \in \mathcal{C}_i$. This is because if at time $T_{VSS} + T_{BA}$, party $P_j$ does not belong to the $\mathcal{C}_i$ set of any honest $P_i$, then it implies that all honest parties participate with input 0 in the instance $\Pi_{BA}^{(j)}$ from time $T_{VSS} + T_{BA}$. Then, from the $t_a$-validity of $\Pi_{BA}$ in the synchronous network, every honest party would compute the output 0 in the instance $\Pi_{BA}^{(j)}$ and hence $P_j$ will not be present in $\mathcal{CS}$, which is a contradiction. Now if $P_i$ has computed some output during $\Pi_{VSS}^{(j)}$ at time $T_{VSS} + T_{BA}$, then from the $t_a$-strong-commitment of $\Pi_{VSS}$, it follows that $P_i$ has some $t_a$-degree polynomial, say $f_j^i(\cdot)$, such that every honest party $P_i$ computes $f_j^i(\alpha_i)$ by time $T_{VSS} + T_{BA} + 2\Delta$. Since $2\Delta < T_{BA}$, it follows that at time $T_{ACS}$, every honest $P_i$ has $f_j^i(\alpha_i)$, thus proving the $t_a$-correctness property in a synchronous network.

We next consider an asynchronous network, with up to $t_a$ corruptions. Let $\mathcal{H}$ be the set of parties, where $|\mathcal{H}| \geq n-t_a$. From the above, irrespective of the way messages are scheduled, there will be at least $n-t_a$ instances of $\Pi_{BA}$ in which all honest parties eventually participate with input 1. This is because, corresponding to every $P_j \in \mathcal{H}$, every honest $P_i$ eventually computes the output $f_j(\alpha_i)$ during the instance $\Pi_{VSS}^{(j)}$, which follows from the $t_a$-correctness of $\Pi_{VSS}$ in the asynchronous network. So even if the corrupt parties $P_j$ do not invoke their respective $\Pi_{VSS}^{(j)}$ instances, there will be at least $n-t_a$ instances of $\Pi_{BA}$ in which all honest parties eventually participate with input 1. Consequently, from the $t_a$-almost-surely liveness and $t_a$-validity properties of $\Pi_{BA}$ in the asynchronous network, almost-surely, all honest parties eventually compute the output 1 during these $\Pi_{BA}$ instances. Hence, all honest parties eventually participate with some input in the remaining $\Pi_{BA}$ instances. Consequently, from the $t_a$-almost-surely liveness and $t_a$-consistency properties of $\Pi_{BA}$ in the asynchronous network, almost-surely, all honest parties will compute some common output in these $\Pi_{BA}$ instances as well. Since the set $\mathcal{CS}$ is determined deterministically based on the outputs computed from the $n$ instances of $\Pi_{BA}$, it follows that all the honest parties eventually output the same $\mathcal{CS}$.

Now consider an arbitrary party $P_j \in \mathcal{CS}$. It implies that the honest parties compute the output 1 during the instance $\Pi_{BA}^{(j)}$. From the $t_a$-validity of $\Pi_{BA}$ in the asynchronous network, it follows that at least one honest $P_i$ participated with input 1 during $\Pi_{BA}^{(j)}$ after computing some output in the instance $\Pi_{VSS}^{(j)}$. Now if $P_j$ is honest, then the $t_a$-correctness of $\Pi_{VSS}$ in the asynchronous network guarantees that every honest party $P_i$ eventually computes the output $f_j(\alpha_i)$ during $\Pi_{VSS}^{(j)}$. On the other hand, if $P_j$ is corrupt, then the $t_a$-strong commitment of $\Pi_{VSS}^{(j)}$ in the asynchronous network guarantees that there exists some $t_a$-degree polynomial, say $f_j^i(\cdot)$, such that every honest party $P_i$ eventually computes the output $f_j^i(\alpha_i)$ during the instance $\Pi_{VSS}^{(j)}$.

We end this section by discussing the modifications needed in the protocol $\Pi_{ACS}$ if each party has $L$ number of polynomials as input.

**Protocol $\Pi_{ACS}$ for Multiple Polynomials:** Protocol $\Pi_{ACS}$ can be easily extended if each party has $L$ number of
The properties of OEC in the synchronous network, within time $\Delta$, every honest $P_i$ will have $d$ and $e$ and hence the parties output a $t_s$-sharing of $z$ within time $\Delta$. On the other hand, if the network is asynchronous, then from the properties of OEC in the asynchronous network, every honest $P_i$ eventually reconstructs $d$ and $e$ and hence the honest parties eventually output a $t_s$-sharing of $z$

In the protocol, $z = (x-a) \cdot (y-b) + (x-a) \cdot b + (y-b) \cdot a + c = x \cdot y - a \cdot b + c$ holds. Hence it follows that $z = x \cdot y$ holds if and only if $c = a \cdot b$ holds.

In the protocol, the adversary learns the values $d$ and $e$, as they are publicly reconstructed. However, if $a$ and $b$ are random from the point of view of the adversary, then $d$ and $e$ leak no information about $x$ and $y$. Namely, for every candidate $x$ and $y$, there exist unique $a$ and $b$, consistent with $d$ and $e$.

The communication complexity follows from the fact each party needs to send 2 field elements to every other party.

B. Best-of-Both-Worlds Triple-Transformation Protocol

Protocol $\Pi_{Tri}^T$ takes input a set of $2d + 1$ $t_s$-shared triples $\{(x^{(i)}, y^{(i)}, z^{(i)})\}_{i=1,...,2d+1}$, where the triples may not be “related”. The output of the protocol are “co-related” $t_s$-shared triples $\{(x^{(i)}, y^{(i)}, z^{(i)})\}_{i=1,...,2d+1}$, such that all the following hold (irrespective of the network type):

- There exist $d$-degree polynomials $X(\cdot)$, $Y(\cdot)$ and $2d$-degree polynomial $Z(\cdot)$, such that $X(\alpha_i) = x^{(i)}$, $Y(\alpha_i) = y^{(i)}$ and $Z(\alpha_i) = z^{(i)}$ holds for $i = 1, \ldots, 2d + 1$.

- The triple $(x^{(i)}, y^{(i)}, z^{(i)})$ is a multiplication-triple if and only if $(x^{(i)}, y^{(i)}, z^{(i)})$ is a multiplication-triple. This further implies that $Z(\cdot) = X(\cdot) \cdot Y(\cdot)$ holds if and only if all the $2d + 1$ input triples are multiplication-triples.

- Adversary learns the triple $(x^{(i)}, y^{(i)}, z^{(i)})$ if and only if it knows the input triple $(x^{(i)}, y^{(i)}, z^{(i)})$.

The idea behind $\Pi_{Tri}^T$ is as follows: the polynomials $X(\cdot)$ and $Y(\cdot)$ are “defined” by the first and second components of the first $d+1$ input triples. Hence the first $d+1$ points on these polynomials are already $t_s$-shared. The parties then compute $d$ “new” points on the polynomials $X(\cdot)$ and $Y(\cdot)$ in a shared fashion. This step requires the parties to perform only local computations. This is because, from the property of Lagrange’s interpolation, computing any new point on $X(\cdot)$ and $Y(\cdot)$ involves computing a publicly-known linear function (which we call Lagrange’s linear function) of “old” points on these polynomials. Since the old points are $t_s$-shared, by applying corresponding Lagrange’s functions, the parties can compute a $t_s$-sharing of the new points. Finally, the parties compute a $t_s$-sharing of the product of the $d$ new points using Beaver’s technique, making use of the remaining $d$ input triples. The $Z(\cdot)$ polynomial is then defined by the $d$ computed products and the third component of the first $d+1$ input triples. The protocol is formally presented in Fig 7.

We next prove the properties of the protocol $\Pi_{Tri}^T$.

Lemma VI.2: Let $\{(x^{(i)}), (y^{(i)}), (z^{(i)})\}_{i=1,...,2d+1}$ be a set of $t_s$-shared triples. Then protocol $\Pi_{Tri}^T$ achieves the following properties in the presence of up to $t_s$ corruptions.
Protocol $\Pi_{\text{TripTrans}}(d, \{ [x(i)], [y(i)], [z(i)] \}_{i=1,\ldots,2d+1})$

- **Defining $\mathcal{X}(\cdot)$ and $\mathcal{Y}(\cdot)$ Polynomials** — The parties locally do the following:
  - For $i = 1,\ldots,d + 1$, set
    - $[x(i)] = [x(i)]$;
    - $[y(i)] = [y(i)]$;
    - $[z(i)] = [z(i)]$.
  - Let $X(i)$ be the unique $d$-degree polynomial, passing through the points $\{ (x(i), x(i)) \}_{i=1,\ldots,d+1}$. And let $Y(i)$ be
    the unique $d$-degree polynomial, passing through $\{ (x(i), y(i)) \}_{i=1,\ldots,d+1}$.
  - For $i = d+2,\ldots,2d+1$, locally compute
    $X(i) = Y(x(i))$ from $\{ X(i) \}_{i=1,\ldots,d+1}$, by applying the corresponding Lagrange’s linear function.
  - For $i = d+2,\ldots,2d+1$, locally compute
    $[y(i)] = [Y(x(i))]$ from $\{ [y(i)] \}_{i=1,\ldots,d+1}$, by applying the corresponding Lagrange’s linear function.

- **Computing Points on the $Z(\cdot)$ Polynomial** — The parties do the following:
  - For $i = d+2,\ldots,2d+1$, participate in the instance
    $\Pi_{\text{Beaver}}([x(i)], [y(i)], [x(i)], [z(i)])$ of $\Pi_{\text{Beaver}}$.
    Let $[z(i)]$ be the output obtained from this instance.
  - Output $\{ [x(i)], [y(i)], [z(i)] \}_{i=1,\ldots,2d+1}$.

Fig. 7: Protocol for transforming a set of $t_s$-shared triples into a set of correlated $t_s$-shared triples.

- If the network is synchronous, then the parties output $t_s$-shared triples $\{ [x(i)], [y(i)], [z(i)] \}_{i=1,\ldots,2d+1}$, within time $\Delta$.
- If the network is asynchronous, then the parties eventually output $t_s$-shared triples $\{ [x(i)], [y(i)], [z(i)] \}_{i=1,\ldots,2d+1}$.
- Irrespective of the network type, there exist $d$-degree polynomials $X(i), Y(i)$ and $2d$-degree polynomial $Z(i)$, such that
  $X(\alpha(i)) = x(i), Y(\alpha(i)) = y(i)$ and $Z(\alpha(i)) = z(i)$ holds for $i = 1,\ldots,d+1$.
- Irrespective of the network type, $(x(i), y(i), z(i))$ is a multiplication-triple if and only if $(z(i), y(i), z(i))$ is a
  multiplication-triple.
- For $i = 1,\ldots,2d+1$, no additional information about $(x(i), y(i), z(i))$ is revealed to the adversary if the triple
  $(x(i), y(i), z(i))$ is random from the point of view of the adversary.
- The protocol incurs a communication of $O(dn^2 \log |F|)$ bits from the honest parties.

**Proof:** Consider an adversary who controls up to $t_s$ parties. In the protocol, irrespective of the network type, the parties
locally compute the $t_s$-sharings $\{ [x(i)], [y(i)] \}_{i=1,\ldots,2d+1}$ and $t_s$-sharings $\{ [z(i)] \}_{i=1,\ldots,d+1}$. If the network is synchron-
ous, then from the properties of $\Pi_{\text{Beaver}}$ in the synchronous network, it follows that after time $\Delta$, all honest parties
will have their respective output in all the $d$ instances of $\Pi_{\text{Beaver}}$. Hence after time $\Delta$, the parties have $t_s$-sharings
$\{ [z(i)] \}_{i=d+2,\ldots,2d+1}$. On the other hand, if the network is asynchronous, then from the properties of $\Pi_{\text{Beaver}}$ in the
asynchronous network, all honest parties eventually compute their output in all the $d$ instances of $\Pi_{\text{Beaver}}$. Hence the parties
eventually compute the $t_s$-sharings $\{ [z(i)] \}_{i=d+2,\ldots,2d+1}$ and eventually compute their output in the protocol.

Next consider an arbitrary $i \in \{ 1,\ldots,d+1 \}$. Since $(x(i), y(i), z(i)) = (x(i), y(i), z(i))$, it follows that
$(x(i), y(i), z(i))$ will be a multiplication-triple if and only if $(x(i), y(i), z(i))$ is a multiplication-triple. Now consider an arbitrary
$i \in \{ d+2,\ldots,2d+1 \}$. Since $[z(i)]$ is the output of the instance $\Pi_{\text{Beaver}}([x(i)], [y(i)], [z(i)])$, it follows from the properties of $\Pi_{\text{Beaver}}$ that $z(i) = x(i), y(i)$ holds, if and only if $(x(i), y(i), z(i))$ is a multiplication-triple.

From the protocol steps, it is easy to see that the polynomials $X(i)$ and $Y(i)$ defined in the protocols are $d$-degree polynomials, as they are defined through $d+1$ distinct points $\{ (x(i), x(i)) \}_{i=1,\ldots,d+1}$ and $\{ (x(i), y(i)) \}_{i=1,\ldots,d+1}$ respectively. On the other hand, $Z(i)$ is a $2d$-degree polynomial, as it is defined through the $2d+1$ distinct points
$\{ (x(i), x(i), x(i)) \}_{i=1,\ldots,2d+1}$.

For any $i \in \{ 1,\ldots,d+1 \}$, if $(x(i), y(i), z(i))$ is random from the point of view of the adversary, then $(x(i), y(i), z(i))$ is also random from the point of view of the adversary, since $(x(i), y(i), z(i)) = (x(i), y(i), z(i))$. On the other hand for any
$i \in \{ d+2,\ldots,2d+1 \}$, if $(x(i), y(i), z(i))$ is random from the point of view of the adversary, then from the properties of $\Pi_{\text{Beaver}}$, it follows that no additional information is learnt about $(x(i), y(i), z(i))$.

The communication complexity follows from the fact that there are $d$ instances of $\Pi_{\text{Beaver}}$, invoked in the protocol.

C. Best-of-Both-Worlds Triple-Sharing Protocol

We next present a triple-sharing protocol $\Pi_{\text{TripSh}}$, which allows a dealer $D$ to verifiably $t_s$-share $L$ multiplication-
triples. If $D$ is honest, then the triples remain random from the point of view of the adversary and all honest parties
output the shares of $D$’s multiplication-triples. On the other hand, if $D$ is corrupt, then the protocol need not produce any
output, even in a synchronous network, as a corrupt $D$ may not invoke the protocol at the first place and the parties will
not be aware of the network type. However, the “verifiability” of $\Pi_{\text{TripSh}}$ guarantees that if the honest parties compute any
output corresponding to a corrupt $D$, then $D$ has indeed $t_s$-shared multiplication-triples.

For simplicity, we present the protocol assuming $D$ has a single multiplication-triple to share and the protocol can be
easily generalized for any $L > 1$. The idea behind the protocol is as follows: $D$ picks a random multiplication-triple and
$t_s$-shares it by invoking an instance of $\Pi_{\text{VSS}}$. To prove that it has indeed shared a multiplication-triple, $D$ actually $t_s$-shares
$2t_s+1$ random multiplication-triples. The parties then run an instance of $\Pi_{\text{TripTrans}}$ and “transform” these shared triples into
“co-related” shared triples, constituting distinct points on the triplet of polynomials $\{ X(i), Y(i), Z(i) \}$, which are guaranteed
to exist during $\Pi_{\text{TripTrans}}$. Then, to check if all the triples shared by $D$ are multiplication-triples, it is sufficient to verify
if $Z(\alpha(i)) = X(\alpha) \cdot Y(\alpha)$ holds. To verify the latter, we incorporate a mechanism which enables the parties to publicly
learn if $Z(\alpha(i)) = X(\alpha(i)) \cdot Y(\alpha(i))$ holds under $P_j$’s “supervision” in such a way that if $P_j$ is honest, then the supervised verification of the triplet $(X(\alpha(i)), Y(\alpha(i)), Z(\alpha(i)))$ is “successful” if and only if
the triplet is a multiplication-triple. Moreover, the privacy of the triplet will be maintained during the supervised verification
for an honest $D$ and $P_j$. The goal is to check whether there are
at least $2t_+ + 1$ successful supervised-verifications, performed under the supervision of honest supervisors $P_j$, which will then confirm that indeed $Z(\cdot) = X(\cdot) \cdot Y(\cdot)$ holds. This is because $Z(\cdot)$ is a $2t_+$-degree polynomial. Upon confirming that $Z(\cdot) = X(\cdot) \cdot Y(\cdot)$ holds, the parties compute a “new” point on the polynomials (in a shared fashion), which is taken as the output triple shared on behalf of $D$. We stress that the output triple is well defined and will be “known” to $D$, as it is deterministically determined from the triples shared by $D$. If $D$ is honest, then the privacy of the output triple is guaranteed from the fact that during the supervised verification, an adversary may learn at most $t_+$ distinct points on the polynomials $X(\cdot), Y(\cdot)$ and $Z(\cdot)$, corresponding to the corrupt supervisors.

The supervised verification of the (shared) points on the polynomials is performed as follows: the parties invoke an instance of $\Pi_{ACS}$, where the input for each party is a triplet of random $t_+$-degree polynomials, whose constant terms constitute a random multiplication-triple, called verification-triple. The instance of $\Pi_{ACS}$ is invoked in parallel with D’s invocation of $\Pi_{VSS}$. Through the instance of $\Pi_{ACS}$, the parties agree upon a set $W$ of at least $n - t_+$ supervisors, whose shared verification-triples are used to verify the points on the polynomials $X(\cdot), Y(\cdot)$ and $Z(\cdot)$. Namely, if $P_j \in W$ has shared the verification-triple $(u(j), v(j), w(j))$, then in the supervised verification under $P_j$, parties publicly reconstruct and check if $Z(\alpha_j) - X(\alpha_j) \cdot Y(\alpha_j) = 0$ holds. For this, the parties reconstruct $X(\alpha_j), Y(\alpha_j)$ in a shared fashion using Beaver’s method, by deploying the shared verification-triple $(u(j), v(j), w(j))$. If $Z(\alpha_j) - X(\alpha_j) \cdot Y(\alpha_j)$ does not turn out to be 0 (implying that either D is corrupt or $P_j$’s verification-triple is not a multiplication-triple), then the parties publicly reconstruct and check if $(X(\alpha_j), Y(\alpha_j), Z(\alpha_j))$ is a multiplication-triple and discard D if the triple does not turn out to be a multiplication-triple.

An honest $D$ will never be discarded. Moreover, in a synchronous network, all honest parties $P_j$ are guaranteed to be present in $W$ (follows from the $t_+$-correctness of $\Pi_{ACS}$ in the synchronous network) and hence, there will be at least $n - t_+ > 2t_+ + 1$ honest supervisors in $W$. On the other hand, even in an asynchronous network, there will be at least $n - t_+ - t_0 > 2t_+$ honest supervisors in $W$. Hence if a corrupt $D$ is not discarded, then it is guaranteed that $D$ has shared multiplication-triples.

We next prove the properties of the protocol of $\Pi_{TripSh}$.

**Lemma VI.3:** Protocol $\Pi_{TripSh}$ achieves the following properties.

- If $D$ is honest, then the following hold:
  - $t_+$-Correctness: If the network is synchronous, then after time $T_{TripSh} = T_{ACS} + 4\Delta$, the honest parties output a $t_+$-shared multiplication-triple on the behalf of $D$.
  - $t_+$-Correctness: If the network is asynchronous, then almost-surely, the (honest) parties eventually output a $t_+$-shared multiplication-triple on the behalf of $D$.
  - $t_+$-Privacy: Irrespective of the network type, the view of the adversary remains independent of the output multiplication-triple, shared on the behalf of $D$.

---

**Fig. 8.** A protocol for verifiably sharing a single multiplication triple.
For every $P_t \in \mathcal{W}$ such that $\text{flag}_{i_t} = 1$, apply the OEC($t, t, \mathcal{P}$) procedure on the received shares corresponding to $[x^{(j)}], [y^{(j)}]$ and $[z^{(j)}]$, to reconstruct the triple $(x^{(j)}, y^{(j)}, z^{(j)})$.

For every $P_t \in \mathcal{W}$ such that $\text{flag}_{i_t} = 1$, reset $\text{flag}_{i_t}$ to 0 if $(x^{(j)}, y^{(j)}, z^{(j)})$ is a multiplication-triple.

If $\text{flag}_{i_t} = 0$, corresponding to every $P_t \in \mathcal{W}$, then set $\text{flag}_{i_t} = 0$. else set $\text{flag}_{i_t} = 1$.

\textbf{Output Computation:} Each party $P_t \in \mathcal{P}$ does the following.

If $\text{flag}_{i_t} = 0$ then output shares corresponding to $t_s$-shared triple $(\alpha, [b], [c])$ on behalf of $D$, where $\alpha = X(\beta)$, $b = Y(\beta)$ and $c = Z(\beta)$ and where $[a]$, $[b]$ and $[c]$ are locally computed from $\{x^{(j)}\}_{j=1, \ldots, t_s+1}$, $\{y^{(j)}\}_{j=1, \ldots, t_s+1}$ and $\{z^{(j)}\}_{j=1, \ldots, t_s+1}$ respectively, by using appropriate Lagrange’s linear functions. Here $\beta$ is a zero element of $\mathbb{F}$, distinct from $\alpha_1, \ldots, \alpha_{2t_s+1}$.

If $\text{flag}_{i_t} = 1$ then output default-shares (namely all shares being 0) corresponding to $t_s$-shared triple $([0], [0], [0])$ on behalf of $D$.

\begin{itemize}
  \item $t_s$-Strong Commitment: If the network is synchronous, then the (honest) parties eventually output a $t_s$-shared multiplication-triple on behalf of $D$. Moreover, if some honest party computes its output shares at time $T$, then by time $T + 2\Delta$, all honest parties will compute their respective output shares.
  \item $t_s$-Strong Commitment: The (honest) parties eventually output a $t_s$-shared multiplication-triple on the behalf of $D$.
\end{itemize}

The protocol incurs a communication of $O(n^6 \log |\mathbb{F}|)$ bits from the honest parties and invokes $O(n^2)$ instances of $\Pi_{BA}$.

\textbf{Proof:} We first consider an honest $D$ and prove the corresponding properties. We first consider a synchronous network with up to $t_a$ corruptions. At time $T_{VSS}$, the multiplication-triples $\{(x^{(j)}, y^{(j)}, z^{(j)})\}_{j=1, \ldots, t_s+1}$ will be $t_s$-shared. This follows from the $t_s$-correctness property of $\Pi_{VSS}$ in the synchronous network. Moreover, these triples will be random from the point of view of the adversary. On the other hand, if $P_t \in \mathcal{W}$ is corrupt, then $\gamma^{(j)}$ may not be 0. However, in this case each honest $P_t$ will reset $\text{flag}_{i_t}$ to 0 after reconstructing the corresponding suspected-triple $(x^{(j)}, y^{(j)}, z^{(j)})$, since it will be a multiplication-triple. The process of computing $\gamma^{(j)}$ and the difference $\gamma^{(j)}$ will take $2\Delta$ time and additionally $\Delta$ time might be required to publicly reconstruct suspected-triples corresponding to corrupt $P_t \in \mathcal{W}$. Hence, at time $T_{ACS} + 4\Delta$, each honest $P_t$ sets $\text{flag}_{i_t} = 1$ and hence, the honest parties output $t_s$-shared triple $(a, b, c)$. Moreover, the triple will be a multiplication-triple, since $(a, b, c)$ is the same as $(X(\beta), Y(\beta), Z(\beta))$. Since at most $t_s$ triples $(x^{(j)}, y^{(j)}, z^{(j)})$ may be publicly reconstructed corresponding to the corrupt parties $P_t \in \mathcal{W}$, it follows that the adversary will learn at most $t_s$ distinct points on the $X(\cdot), Y(\cdot)$ and $Z(\cdot)$ polynomials. This further implies that $(X(\beta), Y(\beta), Z(\beta))$ will be random from the point of view of the adversary, since $X(\cdot), Y(\cdot)$ and $Z(\cdot)$ are $t_s$-degree polynomials. This completes the proof of the $t_s$-correctness in the synchronous network, as well as the proof of the $t_s$-privacy property.

If $D$ is honest and the network is asynchronous with up to $t_a$ corruptions, then the proof of the $t_a$-correctness property is similar to the above proof, except that now we now use the $t_a$-correctness property of $\Pi_{VSS}$ and the properties of $\Pi_{ACS}$, $\Pi_{Beaver}$ in the asynchronous network. Moreover, the privacy property holds since the adversary now corrupts $t_a < t_s$ parties.

We next consider a corrupt $D$ and prove the strong-commitment properties. We first consider a synchronous network with up to $t_a$ corruptions. Note that irrespective of whether $D$ shares any triples through the instance of $\Pi_{VSS}$ or not, all honest parties will output a set $\mathcal{W}$ at time $T_{ACS}$ during the instance of $\Pi_{ACS}$, with every honest $P_t$ being present in the $\mathcal{W}$. This follows from the properties of $\Pi_{ACS}$ in the synchronous network. If no honest party computes any output in the protocol, then strong-commitment holds trivially. So consider the case when some honest party computes an output. This implies that at least one honest party, say $P_h$, must have computed an output during the instance of $\Pi_{VSS}$ invoked by $D$, as otherwise, no honest party computes any output in the protocol. Let $T$ be the time at which $P_h$ has the output for the instance of $\Pi_{VSS}$ invoked by $D$. Note that $T \geq T_{VSS}$ and $T$ could be greater than $T_{ACS}$, as a corrupt $D$ may delay the start of the instances of $\Pi_{VSS}$. From the $t_s$-strong commitment property of $\Pi_{VSS}$ in the synchronous network, it then follows that by time $T + 2\Delta$, all honest parties compute their output in the instance of $\Pi_{VSS}$ invoked by $D$. Hence at time $T + 2\Delta$, there are $2t_s + 1$ triples which are $t_s$-shared by $D$.

If $T \leq T_{ACS} - 2\Delta$, then at time $T_{ACS}$, all honest parties will have their respective shares corresponding to the $t_s$-shared triples of $D$, as well as the set $\mathcal{W}$ and the shares corresponding to the verification-triples, shared by the parties in $\mathcal{W}$. The instance of $\Pi_{TripTrans}$ will produce its output at time $T_{ACS} + \Delta$. The follow-up instances of $\Pi_{Beaver}$ to recompute the triple $(x^{(j)}, y^{(j)}, z^{(j)})$. Moreover, in this case, no additional information about $(x^{(j)}, y^{(j)}, z^{(j)})$ is revealed, which follows from the properties of $\Pi_{Beaver}$ and the fact that the verification-triple $(w^{(j)}, v^{(j)}, w^{(j)})$ remains random from the point of view of the adversary. On the other hand, if $P_t \in \mathcal{W}$ is corrupt, then $\gamma^{(j)}$ may not be 0. However, in this case each honest $P_t$ will reset $\text{flag}_{i_t}$ to 0 after reconstructing the corresponding suspected-triple $(x^{(j)}, y^{(j)}, z^{(j)})$, since it will be a multiplication-triple. The process of computing $\gamma^{(j)}$ and the difference $\gamma^{(j)}$ will take $2\Delta$ time and additionally $\Delta$ time might be required to publicly reconstruct suspected-triples corresponding to corrupt $P_t \in \mathcal{W}$. Hence, at time $T_{ACS} + 4\Delta$, each honest $P_t$ sets $\text{flag}_{i_t} = 1$ and hence, the honest parties output $t_s$-shared triple $(a, b, c)$. Moreover, the triple will be a multiplication-triple, since $(a, b, c)$ is the same as $(X(\beta), Y(\beta), Z(\beta))$. Since at most $t_s$ triples $(x^{(j)}, y^{(j)}, z^{(j)})$ may be publicly reconstructed corresponding to the corrupt parties $P_t \in \mathcal{W}$, it follows that the adversary will learn at most $t_s$ distinct points on the $X(\cdot), Y(\cdot)$ and $Z(\cdot)$ polynomials. This further implies that $(X(\beta), Y(\beta), Z(\beta))$ will be random from the point of view of the adversary, since $X(\cdot), Y(\cdot)$ and $Z(\cdot)$ are $t_s$-degree polynomials. This completes the proof of the $t_s$-correctness in the synchronous network, as well as the proof of the $t_s$-privacy property.
products will take $\Delta$ time, followed by $\Delta$ time for publicly reconstructing the difference values $\gamma^{(j)}$. Additionally, the parties may take $\Delta$ time to publicly reconstruct any suspected triples. Hence in this case, all honest parties will have their respective output shares at time $T_{ACS} + 4\Delta$.

On the other hand, if $T > T_{ACS} - 2\Delta$, then each honest party computes its output during the instance of $P_{TripTrans}$, either at time $T + \Delta$ or at time $T + 3\Delta$. Then, each honest party computes its output from the instances of $P_{Beaver}$, either at time $T + 2\Delta$ or at time $T + 4\Delta$. This implies that the difference values $\gamma^{(j)}$ are available with the honest parties, either at time $T + 3\Delta$ or $T + 5\Delta$. Consequently, the suspected triples (if any) will be available with the honest parties, either at the time $T + 4\Delta$ or $T + 6\Delta$. Hence each honest party computes its output share in the protocol either at time $T + 4\Delta$ or $T + 6\Delta$. Notice that in this case there might be a difference of at most $2\Delta$ time within which the honest parties compute their output in the protocol, due to a possible difference of $2\Delta$ time in getting the output in the instances of $P_{VSS}$ invoked by the corrupt $D$.

If the triples shared by $D$ during the instances of $P_{VSS}$ are all multiplication-triples, then similar to the proof of the correctness property for an honest $D$, it follows that the honest parties will output a $t_s$-shared multiplication-triple on behalf of $D$. So consider the case when all the triples shared by $D$ are not multiplication-triples. This implies that $Z(\cdot) \neq X(\cdot) \cdot Y(\cdot)$, where $X(\cdot), Y(\cdot)$ are the $t_s$-degree polynomials and $Z(\cdot)$ is the $2t_s$-degree polynomial, which are guaranteed to exist from the protocol $P_{TripTrans}$. Let $P_j$ be an honest party, such that $Z(\alpha_j) \neq X(\alpha_j) \cdot Y(\alpha_j)$. This further implies that the transformed triple $(x^{(j)}, y^{(j)}, z^{(j)})$ is not a multiplication-triple. Such a $P_j$ is bound to exist. This is because there are at least $2t_s + 1$ honest parties $P_j$. And if $Z(\alpha_j) = X(\alpha_j) \cdot Y(\alpha_j)$ holds corresponding to every honest $P_j$, then it implies that $Z(\cdot) = X(\cdot) \cdot Y(\cdot)$ holds (due to the degrees of the respective polynomials), which is a contradiction.

We next show that each honest $P_i$ will set $flag_i^{(j)} = 1$ and hence $flag_i = 1$. For this, we note that if $P_j \in W$. This follows from the properties of $P_{ACS}$ in the synchronous network, which guarantees that all honest parties (and not just $P_j$) will be present in $W$. Since the verification-triple $(u^{(j)}, v^{(j)}, w^{(j)})$ shared by $P_j$ will be a multiplication-triple, from the properties of $P_{Beaver}$ in the synchronous network, it follows that $\gamma^{(j)} = x^{(j)} \cdot y^{(j)}$ holds. However, since $z^{(j)} \neq x^{(j)} \cdot y^{(j)}$, it follows that $\gamma^{(j)} = z^{(j)} - (z^{(j)} - \gamma^{(j)}) \neq 0$. Consequently, the parties will publicly reconstruct the suspected-triple $(x^{(j)}, y^{(j)}, z^{(j)})$ and find that it is not a multiplication-triple. Hence each honest $P_i$ will set $flag_i^{(j)} = 1$ and hence $flag_i = 1$. So the parties output a default $t_s$-sharing of the multiplication-triple $(0, 0, 0)$ on behalf of $D$.

The proof for the $t_s$-strong-commitment property in the asynchronous network is similar to the above proof, except that we now use the $t_s$-strong-commitment property of $P_{VSS}$ and the properties of $P_{ACS}$ and $P_{Beaver}$ in the asynchronous network. Moreover, there will be at least $n - t_s - t_a \geq 2t_s + 1$ honest parties in $W$, who will lead the verification of at least $2t_s + 1$ distinct points on the polynomials $X(\cdot), Y(\cdot)$ and $Z(\cdot)$, through their respective verification-triples.

The communication complexity follows from the communication complexity of $P_{ACS}, P_{VSS}, P_{TripTrans}$ and $P_{Beaver}$. $\Box$

We next discuss the modifications needed in the protocol $P_{TripSh}$ to handle $L$ multiplication-triples.

**Protocol $P_{TripSh}$ for Sharing $L$ Multiplication-Triples:**

Protocol $P_{TripSh}$ can be easily generalized so that $L$ multiplication-triples are shared on behalf of $D$. Namely, $D$ now has to share $L \cdot (2t_s + 1)$ random multiplication-triples through $P_{VSS}$, while each party $P_j$ will need to select $L$ verification-triples during the instance of $P_{ACS}$. Moreover, there will be $L$ instances of $P_{TripTrans}$ to transform $D$’s shared triples, resulting in $L$ triplets of shared polynomials $(X(\cdot), Y(\cdot), Z(\cdot))$, each of which is independently verified by performing supervised verification. To avoid repetition, we do not provide the formal details. The modified $P_{TripSh}$ protocol will incur a communication of $O(n^4 L \log |F| + n^6 \log |F|)$ bits from the honest parties and invokes $O(n^2)$ instances of $P_{BA}$.

**D. Best-of-Both-Worlds Triple-Extraction Protocol**

Protocol $P_{TripExt}$ (Fig 9) takes as input a publicly-known subset $CS$ of $2d + 1$ parties, where $d \geq t_s$ and where it will be ensured that each party $P_j \in CS$ has $t_s$-shared a multiplication-triple. It will also be ensured that if $P_j$ is honest, then the multiplication-triple is random from the point of view of the adversary. The protocol outputs $d + 1 - t_s$ number of $t_s$-shared multiplication-triples, which will be random from the point of view of the adversary. The high-level idea of the protocol is very simple. The parties first invoke an instance of $P_{TripTrans}$ to “transform” the input triples into a set of correlated triples. Since all the input triples are multiplication-triples, the output triples will also be multiplication-triples. Let $(X(\cdot), Y(\cdot), Z(\cdot))$ be the triplet of shared polynomials which is guaranteed to exist after $P_{TripTrans}$. From the properties of $P_{TripTrans}$, it follows that adversary will know at most $t_s$ distinct points on these polynomials and hence at least $d + 1 - t_s$ points on these polynomials are random for the adversary. Hence, the parties output $d + 1 - t_s$ “new” points on these polynomials (in a $t_s$-shared fashion), which are guaranteed to be random from the point of view of the adversary. This requires the parties to perform only local computation.

**Lemma VI.4:** Let $CS$ be a set of $2d + 1$ parties where $d \geq t_s$, such that each party $P_j \in CS$ has a multiplication-triple $(x^{(j)}, y^{(j)}, z^{(j)})$ which is $t_s$-shared. Moreover, if $P_j$ is honest, then the multiplication-triple is random from the point of view of the adversary. Then protocol $P_{TripExt}$ achieves the following properties.

- $t_s$-Correctness: If the network is synchronous, then after time $\Delta$, the parties output $t_s$-shared multiplication-triples $(a^{(j)}, b^{(j)}, c^{(j)})$ for $j = 1, \ldots, d + 1 - t_s$.
- $t_s$-Correctness: If the network is asynchronous, then the parties will eventually output $t_s$-shared multiplication-triples $(a^{(j)}, b^{(j)}, c^{(j)})$ for $j = 1, \ldots, d + 1 - t_s$.
- $t_s$-Privacy: Irrespective of the network type, the triples $(a^{(j)}, b^{(j)}, c^{(j)})$ for $j = 1, \ldots, d + 1 - t_s$ will be random from the point of view of the adversary.
- The protocol incurs a communication of $O((dn^2 \log |F|)$ bits from the honest parties.
follows that the honest parties output the polynomials respectively, which are guaranteed to exist from \( \{z(j)\}_j \) properties of \( d \) multiplication-triples from a set of \( d \) holds, where \( t \) is unknown multiplication-triples in the set \( d \) point of view of the adversary. Namely, there will be \( \{z(j)\}_j \) as \( t \) and \( \{z(j)\}_j \) holds for every \( P_j \in CS \).

- For \( j = 1, \ldots, d + 1 - t_s \), locally compute \( [a(j)], [b(j)], \) and \( [c(j)] \) from \( \{x(j), y(j), z(j)\}_j \) respectively by applying the corresponding Lagrange's linear function. Here \( a(j) = x(\beta_j), b(j) = Y(\beta_j) \) and \( c(j) = Z(\beta_j) \), where \( \beta_1, \ldots, \beta_{d + 1 - t_s} \) are distinct, non-zero elements from \( F \), different from \( \alpha_1, \ldots, \alpha_n \).

- Output \( \{[a(j)], [b(j)], [c(j)]\}_{j=1,\ldots,d+1-t_s} \).

\[ \text{Proof:} \] If the network is \textit{synchronous}, then from the properties of \( \Pi_{\text{TripTrans}} \) in the \textit{synchronous} network, it follows that after time \( \Delta \), the honest parties have \( t_s \)-shared multiplication-triples \( \{x(j), y(j), z(j)\}_P \in CS \). Moreover, all these triples will be \textit{multiplication-triples}, since all the input triples \( \{x(j), y(j), z(j)\}_P \in CS \) are guaranteed to be multiplication-triples. This further implies that the condition \( Z(\cdot) = X(\cdot)Y(\cdot) \) holds, where \( X(\cdot), Y(\cdot) \) and \( Z(\cdot) \) are the \( d \) and \( 2d \)-degree polynomials respectively, which are guaranteed to exist from \( \Pi_{\text{TripTrans}} \), such that \( X(\alpha_j) = x(j), Y(\alpha_j) = y(j) \) and \( Z(\alpha_j) = z(j) \) holds for every \( j \), such that \( P_j \in CS \). It now follows that the honest parties output the \( t_s \)-shared multiplication-triples \( \{a(j), b(j), c(j)\}_{j=1,\ldots,d+1-t_s} \) after time \( \Delta \), where \( X(\beta_j) = a(j), Y(\beta_j) = b(j) \) and \( Z(\beta_j) = c(j) \). Moreover, the triples will be multiplication-triples, because \( Z(\cdot) = X(\cdot)Y(\cdot) \) holds.

If the network is \textit{asynchronous}, then the proof of \( t_s \)-\textit{correctness} property will be similar as above, except that we now depend upon the properties of \( \Pi_{\text{TripTrans}} \) in the \textit{asynchronous} network.

For \textit{privacy}, we note that there will be at most \( t_s \) \textit{corrupt} parties in \( CS \) and hence adversary will know at most \( t_s \) multiplication-triples in the set \( \{x(j), y(j), z(j)\}_P \in CS \), which follows from the properties of \( \Pi_{\text{TripTrans}} \). This implies that the adversary will know at most \( t_s \) distinct points on the polynomials \( X(\cdot), Y(\cdot) \) and \( Z(\cdot) \), leaving \( d + 1 - t_s \) degrees of freedom on the these polynomials. This further implies that the multiplication-triples \( \{X(\beta_j), Y(\beta_j), Z(\beta_j)\}_{j=1,\ldots,d+1-t_s} \), which are the same as \( \{a(j), b(j), c(j)\}_{j=1,\ldots,d+1-t_s} \) will be random from the point of view of the adversary. Namely, there will be a one-to-one correspondence between the \( d + 1 - t_s \) multiplication-triples in the set \( \{x(j), y(j), z(j)\}_P \in CS \) which are \textit{unknown} to the adversary and the output multiplication-triples \( \{a(j), b(j), c(j)\}_{j=1,\ldots,d+1-t_s} \). Hence adversary's view will be consistent with every candidate value of the output \( d + 1 - t_s \) multiplication-triples.

The communication complexity simply follows from the fact that the protocol requires one instance of \( \Pi_{\text{TripTrans}} \).

\[ E. \text{ The Best-of-Both-Worlds Preprocessing Phase Protocol} \]

We finally present our best-of-both-worlds preprocessing phase protocol \( \Pi_{\text{PreProcessing}} \), which generates \( c_M \) number of \( t_s \)-shared multiplication-triples which will be random from the point of view of the adversary. The protocol is formally presented in Fig 10. In the protocol, each party acts as a dealer and invokes an instance of \( \Pi_{\text{TripSh}} \), so that \( \left( \frac{c_M}{s \cdot t_s \cdot (t_s + 1 - t_s)} \right) \) random multiplication-triples are shared on its behalf. As \textit{corrupt} dealers may not invoke their instances of \( \Pi_{\text{TripSh}} \) (even in a \textit{synchronous} network), the parties agree on a common subset \( CS \) of \( n - t_s \) parties, who have shared multiplication-triples, by executing instances of \( \Pi_{\text{BA}} \) (similar to the protocol \( \Pi_{\text{ACS}} \)). The multiplication-triples shared on the behalf of \( t_s \) \textit{corrupt} triple-providers in \( CS \) will be known to the adversary, while the multiplication-triples shared on the behalf of the \textit{honest} triple-providers in \( CS \) will be random for the adversary. Since the exact identity of the \textit{honest} triple-providers in \( CS \) will not be known, the parties execute \( \frac{c_M}{s \cdot t_s \cdot (t_s + 1 - t_s)} \) instances of \( \Pi_{\text{TripExt}} \) to securely extract \( c_M \) shared multiplication-triples, which will be random for the adversary. In the protocol, for simplicity and without loss of generality, we assume that \( n - t_s \) is of the form \( 2d + 1 \).

\[ \text{Theorem VI.5:} \text{ Protocol } \Pi_{\text{PreProcessing}} \text{ achieves the following properties.} \]

- In a \textit{synchronous} network, by time \( T_{\text{TripGen}} = T_{\text{TripSh}} + 2T_{\text{BA}} + \Delta \), the honest parties output a \( t_s \)-sharing of \( c_M \) multiplication-triples.
- In an \textit{asynchronous} network, almost-surely, the honest parties eventually output a \( t_s \)-sharing of \( c_M \) multiplication-triples.
- Irrespective of the network type, the view of the adversary remains independent of the output multiplication-triples.
- The protocol incurs a communication of \( O\left( \frac{n^2}{2} \cdot \log |F| + n^2 \log |F| \right) \) bits from the honest parties and invokes \( O(n^3) \) instances of \( \Pi_{\text{BA}} \).

\[ \text{Proof:} \text{ Let the network be } \textit{synchronous} \text{ with up to } t_s \text{ corruptions. Let } \mathcal{H} \text{ be the set of parties, where } |\mathcal{H}| \geq n - t_s. \text{ Corresponding to each } P_j \in \mathcal{H}, \text{ at time } T_{\text{TripSh}}, L \text{ multiplication-triples } \{x(j), y(j), z(j)\}_{j=1,\ldots,L} \text{ will be } t_s \text{-shared on the behalf of } P_j \text{ during the instance } \Pi_{\text{TripSh}}(j), \text{ which follows from the } t_s \text{-correctness of } \Pi_{\text{TripSh}} \text{ in the } \textit{synchronous} \text{ network. Consequently, the set } \mathcal{C}_t \text{ will be size at least } n - t_s \text{ for every honest } P_j. \text{ After time } T_{\text{TripSh}}, \text{ corresponding to each } P_j \in \mathcal{H}, \text{ each honest } P_j \text{ participates with input } 1 \text{ in the instance } \Pi_{\text{BA}}(j). \text{ It then follows from the } t_s \text{-validity and } t_s \text{-guaranteed liveness of } \Pi_{\text{BA}} \text{ in the } \textit{synchronous} \text{ network that corresponding to every } P_j \in \mathcal{H}, \text{ every honest } P_j \text{ computes the output } 1 \text{ during the instance } \Pi_{\text{BA}}(j), \text{ at time } T_{\text{TripSh}} + T_{\text{BA}}. \text{ Consequently, after time } T_{\text{TripSh}} + T_{\text{BA}}, \text{ every honest party will start participating in the remaining } \Pi_{\text{BA}} \text{ instances for which no input has been provided yet (if there are) } \]
Let $L \overset{def}{=} \left\lceil \frac{c_M d}{1+\frac{1}{s}} \right\rceil$.

- **Phase I — Sharing Random Multiplication-Triples:** Each $P_i \in \mathcal{P}$ does the following.
  - Act as a dealer $D$ and invoke an instance $\Pi^{(j)}_{\text{TripSh}}$ of $\Pi_{\text{TripSh}}$, so that $L$ random multiplication-triples are shared on $P_i$’s behalf.
  - For $j = 1, \ldots, n$, participate in the instance $\Pi^{(j)}_{\text{TripSh}}$ invoked by $P_j$ and wait for time $T_{\text{TripSh}}$.
  - Initialize a set $C_i = \emptyset$ and include $P_j$ in $C_i$, if an output is obtained from $\Pi^{(j)}_{\text{TripSh}}$.

- **Phase II — Agreement on a Common Subset of Triple-Providers:** Each $P_i \in \mathcal{P}$ does the following.
  - For $j = 1, \ldots, n$, participate in an instance of $\Pi^{(j)}_{\text{BA}}$ of $\Pi_{\text{BA}}$ with input 1, if $P_j \in C_i$.
  - Once $n - t_s$ instances of $\Pi_{\text{BA}}$ have produced an output 1, then participate with input 0 in all the $\Pi_{\text{BA}}$ instances $\Pi^{(j)}_{\text{BA}}$, such that $P_j \not\in C_i$.
  - Once a binary output is computed in all the $n$ instances of $\Pi_{\text{BA}}$, set $CS$ to be the set of first $n - t_s$ parties $P_j$, such that 1 is computed as the output in the instance $\Pi^{(j)}_{\text{BA}}$.

- **Phase III — Extracting Random Multiplication-Triples:** The parties do the following.
  - For every $P_j \in CS$, let $\{[x^{(j)},y^{(j)},z^{(j)}]\}_{t=1,\ldots,L}$ be the $t_s$-shared multiplication-triples, shared on $P_j$’s behalf, during the instance $\Pi^{(j)}_{\text{TripSh}}$.
  - For $t = 1, \ldots, L$, the parties participate in an instance $\Pi^{(t)}_{\text{TripExt}}(CS, \{[x^{(j)},y^{(j)},z^{(j)}]\}_{P_j \in CS})$ of $\Pi_{\text{TripExt}}$ and compute the output $\{[a^{(j)},b^{(j)},c^{(j)}]\}_{j=1,\ldots,M} = \frac{n-1}{2} - 1 - t_s$.
  - Output the $t_s$-shared multiplication-triples $\{[a^{(j)},b^{(j)},c^{(j)}]\}_{j=1,\ldots,M}$.

\[ \{ (x^{(j)}, y^{(j)}, z^{(j)}) \}_{t=1, \ldots, L} \] which will be $t_s$-shared among the parties on behalf of $P_j$ by time $(T_{\text{TripSh}} + T_{\text{BA}} + 2\Delta) < (T_{\text{TripSh}} + 2T_{\text{BA}})$; the latter follows because $2\Delta < T_{\text{BA}}$.

From the above discussion, it follows that there will be $L$ multiplication-triples which will be $t_s$-shared on behalf of each $P_j \in CS$ by time $T_{\text{TripSh}} + 2T_{\text{BA}}$. Hence, each instance of $\Pi_{\text{TripExt}}$ will output $\frac{n-1}{2} + 1 - t_s$ number of $t_s$-shared multiplication-triples by time $T_{\text{TripGen}} = T_{\text{TripSh}} + 2T_{\text{BA}} + \Delta$.

This follows from the $t_s$-correctness property of $\Pi_{\text{TripExt}}$ in the synchronous network by substituting $|CS| = n - t_s$ and $d = \frac{n-1}{2}$ in Lemma VI.4. Since there is $L = \begin{cases} c_M \cdot (t_s^2 - \frac{1}{2}t_s^2 + 1 - t_s) \end{cases}$ instances of $\Pi_{\text{TripExt}}$, it follows that at time $T_{\text{TripGen}}$, the parties have $L \cdot (\frac{n-1}{2} + 1 - t_s) = c_M$ number of $t_s$-shared multiplication-triples. This completes the proof of the $t_s$-correctness property in the synchronous network.

The proof of the $t_s$-privacy property in the asynchronous network is similar to above, except that we now use the $t_s$-correctness and $t_s$-strong-commitment properties of $\Pi_{\text{TripSh}}$ in the asynchronous network, the $t_s$-correctness property of $\Pi_{\text{TripExt}}$ in the asynchronous network and the properties of $\Pi_{\text{BA}}$ in the asynchronous network.

From the $t_s$-privacy property of $\Pi_{\text{TripSh}}$, it follows that the multiplication-triples which are $t_s$-shared on behalf of the honest parties $P_j \in CS$ will be random from the point of view of the adversary under the presence of up to $t_s$ corrupt parties, irrespective of the network type. It then follows from the $t_s$-privacy property of $\Pi_{\text{TripExt}}$ that the $t_s$-shared multiplication-triples generated from each instance of $\Pi_{\text{TripExt}}$ will be random from the point of view of the adversary. This proves the $t_s$-privacy property.

The communication complexity follows from the communication complexity of $\Pi_{\text{TripSh}}$ and $\Pi_{\text{TripExt}}$, and from the fact that $\frac{n-1}{2} - 1 - t_s \geq \frac{L}{2} + 1$.

### VII. THE BEST-OF-both-WORLDS CIRCUIT-EVALUATION PROTOCOL

The best-of-both-worlds protocol $\Pi_{\text{CirEval}}$ for evaluating cir has four phases. In the first phase, the parties generate $t_s$-sharing of $c_M$ random multiplication-triples through $\Pi_{\text{PreProcessing}}$. The parties also invoke an instance of $\Pi_{\text{ACs}}$ to generate $t_s$-sharing of their respective inputs for $f$ and agree on a common subset $CS$ of at least $n - t_s$ parties, whose inputs for $f$ are $t_s$-shared, while the remaining inputs are set to 0. In a synchronous network, all honest parties will be in $CS$, thus ensuring that the inputs of all honest parties are considered for the circuit-evaluation. In the second phase, each gate is evaluated in a $t_s$-shared fashion after which the parties publicly reconstruct the secret-shared output in the third phase. The fourth phase is the termination phase, where the parties check whether “sufficiently many” parties have obtained the same output, in which case the parties “safely” take that output and terminate the protocol (and all the underlying sub-protocols). Protocol $\Pi_{\text{CirEval}}$ is formally presented in Fig. 11.

We now prove the properties of the protocol $\Pi_{\text{CirEval}}$.

**Theorem VII.1:** Let $t_s < t_h$, such that $3t_s + t_s < n$. Moreover, let $f : \mathbb{F}^n \to \mathbb{F}$ be a function represented by an arithmetic circuit cir over $\mathbb{F}$ consisting of $c_M$ number of...
![Protocol](image)

**Preprocessing and Input-Sharing** — The parties do the following:

- Each $P_i \in \mathcal{P}$ on having the input $x^{(i)}$ for $f$, selects a random $t_s$-degree polynomial $f_s^{(i)}(\cdot)$ where $f_s^{(i)}(0) = x^{(i)}$ and participates in an instance of $\Pi_{ACS}$ with input $f_s^{(i)}(\cdot)$. Let $\mathcal{CS}$ be the common subset of parties, computed as an output during the instance of $\Pi_{ACS}$, where $|\mathcal{CS}| \geq n - t_s$. Corresponding to every $P_i \notin \mathcal{CS}$, set $x^{(i)} = 0$ and set $x^{(i)}$ to a default $t_s$-sharing of 0.

- In parallel, participate in an instance of $\Pi_{PreProcessing}$. Let $\langle \{a^{(j)}\}, \{b^{(j)}\}, \{c^{(j)}\} \rangle_{j=1,\ldots,\mathcal{CS}}$ be the $t_s$-shared multiplication-triples, computed as an output during the instance of $\Pi_{PreProcessing}$.

**Circuit Evaluation** — Let $G_1, \ldots, G_m$ be a publicly-known topological ordering of the gates of cir. For $k = 1, \ldots, m$, the parties do the following for gate $G_k$:

- If $G_k$ is an addition gate: the parties locally compute $[w] = [u] + [v]$, where $u$ and $v$ are gate-outputs and $w$ is the gate-output.

- If $G_k$ is a multiplication-with-a-constant gate with constant $c$: the parties locally compute $[v] = c \cdot [u]$, where $u$ is the gate-input and $v$ is the gate-output.

- If $G_k$ is an addition-with-a-constant gate with constant $c$: the parties locally compute $[v] = c + [u]$, where $u$ is the gate-input and $v$ is the gate-output.

- If $G_k$ is a multiplication gate: Let $G_k$ be the $f^{th}$ multiplication gate in cir in which $f \in \{1, \ldots, \mathcal{CS}\}$ and let $\langle \{a^{(j)}\}, \{b^{(j)}\}, \{c^{(j)}\} \rangle$ be the $f^{th}$ shared multiplication-triple, generated from $\Pi_{PreProcessing}$. Moreover, let $[u]$ and $[v]$ be the shared gate-outputs of $G_k$. Then the parties participate in an instance $\Pi_{Beaver}([u], [v], \langle \{a^{(j)}\}, \{b^{(j)}\}, \{c^{(j)}\} \rangle)$ of $\Pi_{Beaver}$ and compute the output $[w]$.

**Output Computation** — Let $[y]$ be the $t_s$-shared circuit-output. The parties exchange their respective shares of $y$ and apply the $\text{OE}(t_s, t_s, \mathcal{P})$ procedure on the received shares to reconstruct $y$.

**Termination:** Each $P_i$ does the following:

- If $y$ has been computed during output computation phase, then send $\text{ready}, y$ message to all the parties.

- If the message $(\text{ready}, y)$ is received from at least $t_s + 1$ distinct parties, then send $\text{ready}, y$ message to all the parties, if not sent earlier.

- If the message $(\text{ready}, y)$ is received from at least $2t_s + 1$ distinct parties, then output $y$ and terminate all the sub-protocols.

---

Fig. 11. A best-of-both-worlds perfectly-secure protocol for securely evaluating the arithmetic circuit cir.

multiplication gates, and whose multiplicative depth is $D_M$. Moreover, let party $P_h$ have input $x^{(j)}$ for $f$. Then, $\Pi_{CirEval}$ achieves the following.

- In a synchronous network, all honest parties output $y = f(x^{(1)}, \ldots, x^{(n)})$ at time $(120n + D_M + 6k - 20) \cdot \Delta$, where $x^{(j)} = 0$ for every $P_j \notin \mathcal{CS}$, such that $|\mathcal{CS}| \geq n - t_s$ and every honest party $P_j \in \mathcal{P}$ is present in $\mathcal{CS}$. Here $k$ is the constant from Lemma III.3, as determined by the underlying (existing) perfectly-secure ABA protocol $\Pi_{ABA}$.

- In an asynchronous network, almost-surely, the honest parties eventually output $y = f(x^{(1)}, \ldots, x^{(n)})$ where $x^{(j)} = 0$ for every $P_j \notin \mathcal{CS}$ and where $|\mathcal{CS}| \geq n - t_s$.

- Irrespective of the network type, the view of the adversary will be independent of the inputs of the honest parties in $\mathcal{CS}$.

- The protocol incurs a communication of $O\left(\frac{n^3}{n^2 + 1}c_M \log |\mathcal{F}| + n^7 \log |\mathcal{F}| \right)$ bits from the honest parties and invokes $O(n^3)$ instances of $\Pi_{BA}$.

**Proof:** Consider a synchronous network with up to $t_s$ corruptions. From the properties of $\Pi_{PreProcessing}$ in the synchronous network, at time $T_{TripGen}$, the (honest) output $c_M$ number of $t_s$-shared multiplication-triples, during the instance of $\Pi_{PreProcessing}$. From the $t_s$-correctness property of $\Pi_{ACS}$ in the synchronous network, at time $T_{ACS}$, the (honest) parties output a common subset of parties $\mathcal{CS}$ during the instance of $\Pi_{ACS}$, where all honest parties will be present in $\mathcal{CS}$ and where $|\mathcal{CS}| \geq n - t_s$. Moreover, corresponding to every $P_j \in \mathcal{CS}$, there will be some $x^{(j)}$ available with $P_j$ (which will be the same as $P_j$’s input for $f$ for an honest $P_j$), such that $x^{(j)}$ will be $t_s$-shared. As $\mathcal{CS}$ will be known publicly, the parties take a default $t_s$-sharing of 0 on the behalf of the parties $P_j$ outside $\mathcal{CS}$ by considering $x^{(j)} = 0$. Since $\mathcal{ACS} < T_{TripGen}$, it follows that at time $T_{TripGen}$, the parties will hold $t_s$-sharing of $c_M$ multiplication-triples and $t_s$-sharing of $x^{(1)}, \ldots, x^{(n)}$.

The circuit-evaluation will take $D_M \cdot \Delta$ time. This follows from the fact that linear gates are evaluated locally, while all the independent multiplication gates can be evaluated in parallel by running the corresponding instances of $\Pi_{Beaver}$ in parallel, where each such instance requires $\Delta$ time. From the properties of $\Pi_{Beaver}$ in the synchronous network, the multiplication-gates will be evaluated correctly and hence, during the output-computation phase, the parties will hold a $t_s$-sharing of $y$, where $y = f(x^{(1)}, \ldots, x^{(n)})$. From the properties of $\text{OE}$, it will take $\Delta$ time for every party to reconstruct $y$. Hence, during the termination phase, all honest parties will send a $\text{ready}$ message for $y$. Since there are at least $2t_s + 1$ honest parties, every honest party will then terminate with output $y$ at the time $T_{TripGen} + (D_M + 20) \cdot \Delta$. By substituting the values of $T_{TripGen}, T_{TripSh}, T_{ACS}, T_{WPS}, T_{BC}, T_{BA}, T_{SBA}$ and $T_{ABA}$ and by noting that all instances of $\Pi_{BC}$ in $\Pi_{CirEval}$ are invoked with $t = t_s$, we get that the parties terminate the protocol at time $(120n + D_M + 6k - 20) \cdot \Delta$, where $k$ is the constant from Lemma III.3, as determined by the underlying (existing) perfectly-secure ABA protocol $\Pi_{ABA}$.

The proof of the properties in an asynchronous network is similar to above, except that we now use the security properties of the building blocks $\Pi_{PreProcessing}, \Pi_{ACS}, \Pi_{Beaver}$ and $\Pi_{RecPriv}$ in the asynchronous network. During the termination phase, at most $t_s$ corrupt parties can send $\text{ready}$ messages for $y \neq y$ and there will be at least $2t_s + 1$ honest parties, who eventually send $\text{ready}$ messages for $y$. Moreover, if some honest party $P_h$ terminates with output $y$, then every honest party eventually terminates the protocol with output $y$. This is because $P_h$ must have received $\text{ready}$ messages for $y$ from at least $t_s + 1$ honest parties before termination, which are eventually delivered to every honest party. Consequently, irrespective of which stage of the protocol an honest party is in, every honest party (including $P_h$) eventually sends a...
ready message for $y$ which is eventually delivered. As there are at least $2t_s + 1$ honest parties, this implies that every honest party eventually terminates with output $y$.

From the $t_s$-privacy property of $\Pi_{ACS}$, corresponding to every honest $P_i \in CS$, the input $x^{(j)}$ will be random from the point of view of the adversary. Moreover, from the properties of $\Pi_{PreProcessing}$, the multiplication-triples generated through $\Pi_{PreProcessing}$ will be random from the point of view of the adversary. During the evaluation of linear gates, no interaction happens among the parties and hence, no additional information about the inputs of the honest parties is revealed. The same is true during the evaluation of multiplication-gates as well, which follows from the properties of $\Pi_{Beaver}$.

The communication complexity of the protocol follows from the communication complexity of $\Pi_{PreProcessing}, \Pi_{ACS}$ and $\Pi_{Beaver}$.

VIII. CONCLUSION AND OPEN PROBLEMS

In this work, we presented the first best-of-both-worlds perfectly-secure MPC protocol, which remains secure both in a synchronous as well as in an asynchronous network. To design the protocol, we presented a best-of-both-worlds perfectly-secure VSS protocol and a best-of-both-worlds perfectly-secure BA protocol. Our work leaves the following interesting open problems.

- We could not prove whether the condition $3t_s + t_a < n$ is also necessary for any best-of-both-worlds perfectly-secure MPC protocol and conjecture that it is indeed the case.

- Our main focus in this work is on the existence of best-of-both-worlds perfectly-secure MPC protocols. Improving the efficiency of the protocol is left open for future work.

APPENDIX A

PROPERTIES OF THE EXISTING (ASYNCHRONOUS) PRIMITIVES

In this section we discuss the existing asynchronous primitives in detail.

A. Online Error-Correction (OEC)

The OEC procedure uses a Reed-Solomon (RS) error-correcting procedure $\text{RSDec}(d, r, W)$, that takes as input a set $W$ of distinct points on a $d$-degree polynomial and tries to output a $d$-degree polynomial, by correcting at most $r$ incorrect points in $W$. Coding theory [51] says that RS-Dec can correct up to $r$ errors in $W$ and correctly interpolate back the original polynomial if and only if $|W| \geq d + 2r + 1$ holds. There are several efficient implementations of RSDec (for example, the algorithm of Berlekamp-Welch).

Suppose $P' \subseteq P$ contains at most $t$ corrupt parties and let there exist some $d$-degree polynomial $q(\cdot)$, with every (honest) $P_i \in P'$ having a point $q(\alpha_i)$. The goal is to make some designated party $P_R$ reconstruct $q(\cdot)$. For this, each $P_i \in P'$ sends $q(\alpha_i)$ to $P_R$, who then applies the OEC procedure OEC as described in Fig 12.

Lemma A.1 [24]: Let $P' \subseteq P$ contain at most $t$ corrupt parties and let there exist some $d$-degree polynomial $q(\cdot)$, with every (honest) $P_i \in P'$ having a point $q(\alpha_i)$. Then the OEC protocol prescribed in Fig 12 achieves the following for an honest $P_R$ in the presence of up to $t$ corruptions.

- **Output Computation** — For $r = 0, \ldots, t$, party $P_R$ does the following in iteration $r$:
  - Let $W$ denote the set of parties in $P'$ from whom $P_R$ has received the points and let $I_r$ denote the points received from the parties in $W$, where $|W|$ contains exactly $d + t + 1 + r$ parties.
  - Wait until $W \geq d + t + 1 + r$. Execute $\text{RSDec}(d, r, I_r)$ to get a $d$-degree polynomial, say $q_r(\cdot)$. If no polynomial is obtained, then skip the next step and proceed to the next iteration.
  - If for at least $d + t + 1$ values $v_i \in I_r$ it holds that $q_r(\alpha_i) = v_i$, then output $q_r(\cdot)$. Otherwise, proceed to the next iteration.

Fig. 12. The online error-correction procedure.
Protocol $\Pi_{\text{Acast}}$

1. If $P_i = S$, then on input $m$, send $(\text{init}, S, m)$ to all the parties.
2. Upon receiving the message $(\text{init}, S, m)$ from $S$, send $(\text{echo}, S, m)$ to all the parties. Do not execute this step, more than once.
3. Upon receiving $(\text{echo}, S, m^*)$ from $n - t$ parties, send $(\text{ready}, S, m^*)$ to all the parties.
4. Upon receiving $(\text{ready}, S, m^*)$ from $t + 1$ parties, send $(\text{ready}, S, m^*)$ to all the parties.
5. Upon receiving $(\text{ready}, S, m^*)$ from $n - t$ parties, output $m^*$.

Fig. 13. Bracha’s Acast protocol. The above code is executed by every $P_i \in \mathcal{P}$ including the sender $S$.

B. Bracha’s Acast Protocol

Bracha’s Acast protocol [23] tolerating $t < n/3$ corruptions is presented in Fig 13.

We now prove the properties of the protocol $\Pi_{\text{Acast}}$.

Lemma II.4: Bracha’s Acast protocol $\Pi_{\text{Acast}}$ achieves the following in the presence of up to $t < n/3$ corruptions, where $S$ has an input $m \in \{0, 1\}^t$ for the protocol.

- Asynchronous Network:
  - (a) $t$-Liveness: If $S$ is honest, then all honest parties eventually obtain some output.
  - (b) $t$-Validity: If $S$ is honest, then every honest party with an output, outputs $m$.
  - (c) $t$-Consistency: If $S$ is corrupt and some honest party outputs $m^*$, then every honest party eventually outputs $m^*$.

- Synchronous Network:
  - (a) $t$-Liveness: If $S$ is honest, then all honest parties obtain an output within time $3\Delta$.
  - (b) $t$-Validity: If $S$ is honest, then every honest party with an output, outputs $m$.
  - (c) $t$-Consistency: If $S$ is corrupt and some honest party outputs $m^*$ at time $T$, then every honest $P_i$ outputs $m^*$ by the end of time $T + 3\Delta$.

Irrespective of the network type, $O(n^2 \ell)$ bits are communicated by the honest parties.

Proof: We first prove the properties assuming an asynchronous network with up to $t$ corruptions. We start with the validity and liveness properties, for which we consider an honest $S$. We show that all honest parties eventually output $m$. This is because all honest parties complete steps $2 - 5$ in the protocol, even if the corrupt parties do not send their messages. This is because there are at least $n - t$ honest parties, whose messages are eventually selected for delivery. Moreover, the adversary may send at most $t$ echo messages for $m'$, where $m' \neq m$, on behalf of corrupt parties. Similarly, the adversary may send at most $t$ ready messages for $m^*$, where $m' \neq m$, on behalf of corrupt parties. Consequently, no honest party ever generates a ready message for $m'$, neither in step 3, nor in step 4. This is because $n - t > t$, as $t < n/3$.

For consistency, we consider a corrupt $S$ and let $P_h$ be an honest party, who outputs $m^*$. We next show that all honest parties eventually outputs $m^*$. Since $P_h$ outputs $m^*$, it implies that it receives $n - t$ ready messages for $m^*$ during step 5 of the protocol. Let $\mathcal{H}$ be the set of honest parties whose ready messages are received by $P_h$ during step 5.

It is easy to see that $|\mathcal{H}| \geq t + 1$. The ready messages of the parties in $\mathcal{H}$ are eventually delivered to every honest party and hence each honest party (including $P_h$) eventually executes step 4 and sends a ready message for $m^*$. As there are at least $n - t$ honest parties, it follows that eventually $n - t$ ready messages for $m^*$ are delivered to every honest party (irrespective of whether adversary sends all the required messages). This guarantees that all honest parties eventually obtain some output. To complete the proof, we show that this output is $m^*$.

On contrary, let $P_h'$ be another honest party, different from $P_h$, who outputs $m'' \neq m^*$. This implies that $P_h'$ received ready messages for $m''$ from at least $t + 1$ honest parties during step 5 of the protocol. Now from the protocol steps, it follow that an honest party generates a ready message for some potential $m$, only if it either receives $n - t$ echo messages for the $m$ during step 3 or $t + 1$ ready messages for $m$ (one of which has to come from an honest party) during step 4. So all in all, in order that $n - t$ ready messages are eventually generated for some potential $m$ during step 5, it must be the case that some honest party has to receive $n - t$ echo messages for $m$ during step 2 and generate a ready message for $m$. Now since $P_h$ receives $n - t$ ready messages for $m^*$, some honest party must have received $n - t$ echo messages for $m^*$, at most $t$ of which could come from the corrupt parties. Similarly, since $P_h'$ receives $n - t$ ready messages for $m''$, some honest party must have received $n - t$ echo messages for $m''$. However, since $n - t > 2t$, it follows that in order that $n - t$ echo messages are produced for both $m^*$ as well as $m''$, it must be the case that some honest party must have generated an echo message, both for $m^*$, as well as $m''$ during step 2, which is impossible. This is because an honest party executes step 2 at most once and hence generates an echo message at most once.

The proofs of the properties in the synchronous network closely follow the proofs of the properties in the asynchronous network. If $S$ is honest, then it will send the init message for $m$ to all the parties, which will be delivered within time $\Delta$. Consequently, every honest party will send an echo message for $m$ to all the parties, which will be delivered within time $2\Delta$. Hence every honest party will send a ready message for $m$ to all the parties, which will be delivered within time $3\Delta$. As there are at least $n - t$ honest parties, every honest party will receive ready messages for $m$ from at least $n - t$ parties within time $3\Delta$ and output $m$.

If $S$ is corrupt and some honest party $P_h$ outputs $m^*$ at time $T$, then it implies that $P_h$ has received ready messages for $m^*$ during step 5 of the protocol at time $T$ from a set $\mathcal{H}$ of at least $t + 1$ honest parties. These ready messages are guaranteed to be received by every other honest party within time $T + \Delta$. Consequently, every honest party who has not yet executed step 4 will do so and will send a ready message for $m^*$ at time $T + \Delta$. Consequently, by the end of time $T + \Delta$, every honest party would have sent a ready message for $m^*$ to every other honest party, which will be delivered within
time $T + 2\Delta$. Hence, every honest party will output $m^*$ latest at time $T + 2\Delta$.

The communication complexity (both in a synchronous as well as asynchronous network) simply follows from the fact that every party may need to send an echo and ready message for $m$ to every other party.

\section*{Appendix B

An Overview of the Existing ABA Protocols \cite{ABB00, AAB00}}

In this section, we give a very high level overview of the existing $t$-perfectly-secure ABA protocols of \cite{ABB00} and \cite{AAB00}. Both these protocols are perfectly-secure and can tolerate up to $t < n/3$ corruptions. The protocols follow the standard framework of Rabin and Ben-Or \cite{AB91, B91}, which uses two building-blocks to get a BA protocol. The first building-block is a voting protocol (often called gradecast or graded consensus in the literature) and which is a deterministic protocol. The second building-block is a coin-flipping protocol which is a randomized protocol. In the sequel, we review these building blocks and discuss how they are “combined” to get an ABA protocol. While presenting these building-blocks, unless it is explicitly stated, we assume an asynchronous network. Also, for simplicity, we present these building-blocks without specifying any termination criteria and hence, the parties may keep on running these building-blocks (as well as the ABA protocol) even after obtaining an output.\footnote{Recall that we do not put any termination criteria for any of our sub-protocols, as the termination of the MPC protocol will automatically ensure that all the underlying sub-protocols also get terminated.}

\subsection*{A. The Voting Protocol}

Informally, the voting protocol does “whatever can be done deterministically” to reach agreement. In a voting protocol, every party has a single bit as input. The protocol tries to find out whether there is a detectable majority for some value among the inputs of the parties. In the protocol, each party’s output can have five different forms:

- For $\sigma \in \{0, 1\}$, the output $(\sigma, 2)$ stands for “overwhelming majority for $\sigma$”;
- For $\sigma \in \{0, 1\}$, the output $(\sigma, 1)$ stands for “distinct majority for $\sigma$”;
- The output $(\Lambda, 0)$ stands for “non-distinct majority”.

The protocol code of the voting protocol taken from \cite{ABB00} is presented in Fig. 14.

The properties of the voting protocol are stated in Lemma B.1. While these properties hold in an asynchronous network, it automatically implies that they hold even for a synchronous network. We refer the readers to \cite{AAB00} and \cite{ABB00} for the proof of these properties.

\begin{lemma} [[[\cite{AAB00}, \cite{ABB00}]: Protocol $\Pi_{\text{vote}}$ achieves the following properties, both in the synchronous as well as asynchronous network, if the adversary corrupts up to $t < n/3$ parties, where all the parties participate with an input bit.

- If each honest party has the same input $\sigma$, then each honest party outputs $(\sigma, 2)$;
- If some honest party outputs $(\sigma, 2)$, then every other honest party outputs either $(\sigma, 2)$ or $(\sigma, 1)$;
- If some honest party outputs $(\sigma, 1)$ and no honest party outputs $(\sigma, 2)$ then each honest party outputs either $(\sigma, 1)$ or $(\Lambda, 0)$.
- The protocol incurs a communication of $O(n^3)$ bits from the honest parties.

An additional property which protocol $\Pi_{\text{vote}}$ achieves in a synchronous network is that all honest parties will have their output by the end of the time $9\Delta$. Intuitively, this is because the protocol involves three different “phases” of Acast, each of which will produce an output within time $3\Delta$ for honest sender parties in a synchronous network. Moreover, from Lemma B.1, this output will be $(\sigma, 2)$, if all the honest parties have the same input $\sigma$. We will require this property later while claiming the properties of the resultant ABA protocol in a synchronous network. Hence, we prove this property.

\begin{lemma}

If the network is synchronous and if the adversary corrupts up to $t < n/3$ parties, then in protocol $\Pi_{\text{vote}}$, all honest parties obtain their output within time $9\Delta$. Moreover, the output will be $(\sigma, 2)$, if all the honest parties have the same input $\sigma$.

\begin{proof}

Consider an arbitrary honest $P_j$. Party $P_j$ will Acast its input $x_j$ and from the $t$-liveness and $t$-validity properties of Acast in the synchronous network, every honest party will receive the output $x_j$ from the corresponding Acast instance within time $3\Delta$. As there are at least $n - t$ honest parties, it implies that every honest $P_i$ will obtain a set $X_i$ of size $n - t$ within time $3\Delta$. Hence each honest $P_i$ will Acast a $(\text{vote}, P_i, X_i, a_i)$ message latest at time $3\Delta$ and every honest party receives this message from the corresponding Acast instance within time $6\Delta$. We also note that if there is a corrupt $P_j$ such that $(P_j, x_j)$ is included by an honest $P_i$ in its set $X_i$ when $P_i$ Acasts $X_i$, then from the $t$-consistency property of

\begin{figure}[h]

\centering

\begin{tabular}{|c|}
\hline
\textbf{Protocol $\Pi_{\text{vote}}$} \\
\hline
\hline
- On having the input $x_i$, Acast $(\text{input}, P_i, x_i)$.
- Create a dynamic set $X_i$ which is initialized to $\emptyset$. Add $(P_j, x_j)$ to $X_i$ if $(\text{input}, P_i, x_i)$ is received from the Acast of $P_j$.
- Wait until $|X_i| = n - t$. Then assign $x_i = X_i$, set $a_i$ to the majority bit among $\{x_j \mid (P_j, x_j) \in X_i\}$. Acast $(\text{vote}, P_i, X_i, a_i)$.
- Create a dynamic set $Y_i$, which is initialized to $\emptyset$. Add $(P_j, x_j, a_j)$ to $Y_i$ if $(\text{vote}, P_i, x_i, a_i)$ is received from the Acast of $P_j$. $Y_i \subseteq X_i$, and $a_i$ is the majority bit of $X_i$.
- Wait until $|Y_i| = n - t$. Then assign $y_i = Y_i$, set $b_i$ to the majority bit among $(a_j \mid (P_j, x_j, a_j) \in Y_i)$ and Acast $(\text{re-vote}, P_i, Y_i, b_i)$.
- Create a set $Z_i$, which is initialized to $\emptyset$. Add $(P_j, y_j, b_j)$ to $Z_i$ if $(\text{re-vote}, P_i, Y_i, b_i)$ is received from the Acast of $P_j$, $Y_i \subseteq Y_i$, and $b_i$ is the majority bit of $Y_i$.
- Wait until $|Z_i| = n - t$. Then compute the output as follows.
\begin{itemize}
\item If all the parties $P_j \in Y_i$ have the same vote $a_j = \sigma$, then output $(\sigma, 2)$.
\item Else if all the parties $P_j \in Z_i$ have the same re-vote $b_j = \sigma$, then output $(\sigma, 1)$.
\item Else output $(\Lambda, 0)$.
\end{itemize}
\end{tabular}
\end{figure}
Acast in the synchronous network, every honest party \( P_k \) will include \((P_j, x_j)\) in its set \( X_k \), latest by time \( 5\Delta \). This further implies that upon receiving the message \((\text{vote}, P_i, X_i, a_i)\) from the Acast of any honest \( P_i \), all honest parties \( P_k \) will be able to verify this message and include \((P_i, X_i, a_i)\) in their respective \( Y_k \) sets within time \( 6\Delta \).

As there are at least \( n - t \) honest parties \( P_i \) whose vote messages are received and verified by all honest parties \( P_k \) within time \( 6\Delta \), it follows that every honest party Acasts a re-vote message, latest at time \( 6\Delta \), which is received by every honest party within time \( 9\Delta \). Moreover, as argued for the case of vote messages, every honest party will be able to verify these re-vote messages and include in their respective \( Z_i \) sets within time \( 9\Delta \). Since there are at least \( n - t \) honest parties, it follows that the \( Z_i \) sets of every honest party will attain the size of \( n - t \) within time \( 9\Delta \) and hence every honest party will obtain an output, latest at time \( 9\Delta \).

If all the honest parties have the same input \( \sigma \), then there will be at most \( t \) corrupt parties who may Acast \( 1 - \sigma \). Hence every party (both honest as well as corrupt) will send a vote message only for \( \sigma \). Consequently, every honest party will output \((\sigma, 2)\).\(^{15}\)

### B. Coin-Flipping Protocol

The coin-flipping protocol denoted by \( \Pi_{\text{CoinFlip}} \) (also called as the common-coin protocol) is an \( n \)-party (asynchronous) protocol, where the parties have local random inputs and the protocol outputs a bit for all the parties. The protocol achieves the following properties in an asynchronous (and hence synchronous) network in the presence of any \( t < n/3 \) corruptions:

- In an asynchronous network, all honest parties eventually obtain an output, while in a synchronous network, the honest parties obtain an output within some fixed time \( c \cdot \Delta \), where \( c \) is a publicly-known constant.
- One of the following holds:
  - If no party deviates from the protocol, then with probability at least \( p \), the output bits of all the honest parties are same and random. The probability \( p \) where \( p < 1 \) is often called as the success-probability of the protocol and is a parameter of the protocol.
  - Else, all honest parties will have the same output bit with probability less than \( p \). But in this case, the protocol allows some honest party(ies) to locally identify and shun a (subset of) corrupt party(ies) from any future communication. Namely, the protocol locally outputs ordered pairs of the form \((P_i, P_j)\), where \( P_i \) is some honest party and \( P_j \) is some corrupt party, such that \( P_i \) identifies \( P_j \) as a corrupt party and does not consider any communication from \( P_j \) for the rest of the protocol execution. Such pairs are called as local-conflicts. We stress that the local-conflicts are identified only locally. For instance, if an honest \( P_i \) has shunned a corrupt \( P_j \) during an instance of the coin-flipping protocol, then it is not necessary that every other honest party \( P_k \) also shuns \( P_j \) during the same instance, as \( P_j \) may decide to behave “honestly” towards \( P_k \).

The coin-flipping protocol of [3] guarantees that at least one new local-conflict is identified if, during an instance of the coin-flipping protocol, the parties obtain the same output bit with probability less than \( p \). On the other hand, the coin-flipping protocol of [10] guarantees that \( \Theta(n) \) number of new local-conflicts are identified, if the parties obtain the same output bit with probability less than \( p \).

Protocol \( \Pi_{\text{CoinFlip}} \) is designed using a weaker variant of perfectly-secure AVSS called shunning AVSS (SAVSS), introduced in [3]. The SAVSS primitive is weaker than AVSS in the following aspects:

- It is not guaranteed that every honest party obtains a point on \( D \)’s sharing-polynomial (and hence a share of \( D \)’s secret), even if \( D \) is honest;
- If \( D \) is corrupt, then it may not participate with a \( t \)-degree polynomial and hence, the underlying shared value could be \( \perp \), which is different from every element of \( \mathbb{F} \);
- Irrespective of \( D \), depending upon the behaviour of the corrupt parties, the honest parties later may either reconstruct the same secret as shared by \( D \) or an all-together different value. However, in the latter case, the protocol ensures that at least one new local-conflict is identified.

In [3], a perfectly-secure SAVSS protocol is designed with \( t < n/3 \). By executing \( n^2 \) instances of this protocol in parallel using the framework of [24] and [38], a coin-flipping protocol is presented in [3], where the success-probability \( p \) is \( \frac{1}{2} \). The protocol incurs a communication of \( O(poly(n) \log |\mathbb{F}|) \) bits from the honest parties.

The coin-flipping protocol of [10] also uses the same framework of [24] and [38], but substitutes the SAVSS of [3] with a “better” and more efficient SAVSS with \( t < n/3 \). Their SAVSS ensures that \( \Theta(n) \) number of new local-conflicts are identified, if the value reconstructed by the parties is different from the one shared by \( D \). The success-probability \( p \) remains \( \frac{1}{2} \) and the communication complexity of the protocol is \( O(poly(n) \log |\mathbb{F}|) \) bits.

### C. Vote + Coin-Flipping ⇒ ABA

We now show how to “combine” protocols \( \Pi_{\text{Vote}} \) and \( \Pi_{\text{CoinFlip}} \) to get the protocol \( \Pi_{\text{ABA}} \) (see Fig. 15). The current description of \( \Pi_{\text{ABA}} \) is taken from [20]. The protocol consists of several iterations, where each iteration consists of two instances of \( \Pi_{\text{Vote}} \) protocol and one instance of \( \Pi_{\text{CoinFlip}} \), which are carefully “stitched” together.

In the first instance of \( \Pi_{\text{Vote}} \), the parties participate with their “current input”, which is initialized to their respective bits for ABA in the first iteration. Then, independent of the output received from the instance of \( \Pi_{\text{Vote}} \), the parties participate in an instance of \( \Pi_{\text{CoinFlip}} \). Next, the parties decide their respective inputs for the second instance of \( \Pi_{\text{Vote}} \) protocol, based on the output they received from the first instance. If a party has received the highest grade (namely 2) during

\(^{15}\)If a corrupt party \( P_j \) sends a vote message for \( 1 - \sigma \), then it will never be accepted and no honest party \( P_i \) will ever include \((P_j, X_j, 1 - \sigma)\) in its \( Y_i \) set. This is because \( 1 - \sigma \) will not be the majority among the inputs of the honest parties in \( X_j \).
The ABA protocol from \(\Pi_{\text{Vote}}\) and \(\Pi_{\text{CoinFlip}}\). The above code is executed by every \(P_i \in P\).

Fig. 15. The ABA protocol from \(\Pi_{\text{Vote}}\) and \(\Pi_{\text{CoinFlip}}\). The above code is executed by every \(P_i \in P\).

the first instance of \(\Pi_{\text{Vote}}\), then the party continues with the bit received from that \(\Pi_{\text{Vote}}\) instance for the second \(\Pi_{\text{Vote}}\) instance. Otherwise, the party switches to the output received from \(\Pi_{\text{CoinFlip}}\). The output from the second instance of \(\Pi_{\text{Vote}}\) is then set as the modified input for the next iteration, if it is obtained with a grade higher than 0. Otherwise, the output of \(\Pi_{\text{CoinFlip}}\) is taken as the modified input for the next iteration.

If during any iteration a party obtains the highest grade from the second instance of \(\Pi_{\text{Vote}}\), then it indicates this publicly by sending a ready message to every party, along with the bit received. The ready message is an indication for the others about the “readiness” of the sender party to consider the corresponding bit as the output. Finally, once a party receives this readiness indication for a common bit, it will take as the modified input for the next iteration.

The idea behind the protocol is the following. In the protocol there can be two cases. The first case is when all the honest parties start with the same input bit, say \(b\). Then, they will obtain the output \(b\) from all the instances of \(\Pi_{\text{Vote}}\) protocol in all the iterations and the outputs from \(\Pi_{\text{CoinFlip}}\) will be never considered. Consequently, each honest party will eventually send a ready message for \(b\). Moreover, there can be at most \(t\) corrupt parties who may send a ready message for \(1 - b\) and hence no honest party ever sends a ready message for \(1 - b\). Hence, each honest party eventually outputs \(b\).

The second case is when the honest parties start the protocol with different input bits. In this case, the protocol tries to take the help of \(\Pi_{\text{CoinFlip}}\) to ensure that all honest parties reach an iteration with a common input bit for that iteration. Once such an iteration is reached, this second case gets “transformed” to the first case and hence all honest parties will eventually output that common bit. In more detail, in each iteration \(k\), it will be ensured that either every honest party have the same input bit for the second instance of \(\Pi_{\text{Vote}}\) with probability at least \(p \cdot \frac{1}{2}\) or else certain number of new local-conflicts are identified.\(^{16}\) This is because the input for second instance of \(\Pi_{\text{Vote}}\) is either the output bit of the first instance of \(\Pi_{\text{Vote}}\) or the output of \(\Pi_{\text{CoinFlip}}\), both of which are independent of each other. Hence if the output of \(\Pi_{\text{CoinFlip}}\) is same for all the parties with probability \(p\), then with probability \(p \cdot \frac{1}{2}\), this bit will be the same as output bit from the first instance of \(\Pi_{\text{Vote}}\). If in any iteration \(k\), it is guaranteed that all honest parties have the same inputs for the second instance of \(\Pi_{\text{Vote}}\), then the parties will obtain a common output with and highest grade from the second instance of \(\Pi_{\text{Vote}}\). And then from the next iteration onward, all parties will stick to that common bit and eventually output that common bit.

One can show that it requires \(O(\text{poly}(n))\) number of iterations in expectation before a “good” iteration is reached, where an iteration is considered good, if it is guaranteed that all honest parties have the same input for the second instance of \(\Pi_{\text{Vote}}\). Intuitively, this is because there can be \(O(\text{poly}(n))\) number of “bad” iterations in which the honest parties may have different outputs from the corresponding instances of \(\Pi_{\text{CoinFlip}}\). This follows from the fact that the corrupt parties may deviate from the protocol instructions during the instances of \(\Pi_{\text{CoinFlip}}\). There can be at most \((n - t)\) local-conflicts which may occur \((t\) potentially corrupt parties getting in conflict with \(n - t\) honest parties) overall during various “failed” instances of \(\Pi_{\text{CoinFlip}}\) (where a failed instance means that different honest parties obtain different outputs) and only after all these local-conflicts are identified, the parties may start witnessing “clean” instances of \(\Pi_{\text{CoinFlip}}\) where all honest parties shun communication from all corrupt parties and where it is ensured that all honest parties obtain the same output bit with probability \(p\). Now depending upon the number of new local-conflicts which are revealed from a single failed instance of \(\Pi_{\text{CoinFlip}}\), the parties may witness \(O(\text{poly}(n))\) number of bad iterations.\(^{17}\) Now, once all the bad iterations are over and all potential local-conflicts are identified, in each subsequent iteration, all honest parties will then have the same output from \(\Pi_{\text{CoinFlip}}\) (and hence, same input for the second instance of \(\Pi_{\text{Vote}}\)) with probability at least \(\frac{1}{2}\). Consequently, if \(p\) is a constant, then it will take \(O(1)\) expected number of such iterations before the parties reach a good iteration where it is guaranteed that all honest parties have the same inputs for the second instance of \(\Pi_{\text{Vote}}\).\(^{18}\)

Lemma III.3 now follows easily from the above discussion. Let \(c \cdot \Delta\) be the time within which the protocol \(\Pi_{\text{CoinFlip}}\) generates output for the honest parties in a synchronous network, where \(c\) is some publicly-known constant. Note that

\begin{itemize}
  \item[\(^{16}\)] The number of local-conflicts identified will depend upon the \(\Pi_{\text{CoinFlip}}\) protocol: while the \(\Pi_{\text{CoinFlip}}\) protocol of \([3]\) will ensure that at least 1 new local-conflict is identified, the \(\Pi_{\text{CoinFlip}}\)protocol of \([10]\) will ensure that \(\Theta(n)\) number of new local-conflicts are identified.
  \item[\(^{17}\)] Since each failed instance of the \(\Pi_{\text{CoinFlip}}\) protocol of \([3]\) may reveal only 1 new local-conflict, the number of bad iterations could be \(O(n^2)\). On the other hand, each failed instance of the \(\Pi_{\text{CoinFlip}}\) protocol of \([10]\) reveals \(\Theta(n)\) new local-conflicts and hence there can be \(O(n)\) number of bad iterations.
  \item[\(^{18}\)] One can show that if one sets \(p = \frac{1}{2}\) as done in \([3, 10,\) and \([26]\), then it takes expected 16 iterations after all the local-conflicts are identified to reach a good iteration.
\end{itemize}
The authors would like to thank the anonymous reviewers of PODC 2022 for their excellent reviews of the earlier version of the current article, which helped them significantly improve the article. Anirudh Chandramouli would like to thank Google Research for the travel support to attend and present the preliminary version of the paper at PODC 2022.

REFERENCES

[1] (2019). Lecture 10: Consensus. [Online]. Available: https://www.mpib-inf.mpg.de/fileadmin/inf/I1/teaching/summer19/kds/Lec10.pdf
[2] I. Abraham, G. Asharov, and A. Yanai, “Efficient perfectly secure computation with optimal resilience,” in Theory of Cryptography (Lecture Notes in Computer Science), vol. 13043. Cham, Switzerland: Springer, 2021, pp. 66–96.
[3] I. Abraham, D. Dolev, and J. Y. Halpern, “An almost-surely terminating polynomial protocol for asynchronous Byzantine agreement with optimal resilience,” in Proc. PODC, 2008, pp. 405–414.
[4] I. Abraham, D. Dolev, and G. Stern, “Revisiting asynchronous fault tolerant computation with optimal resilience,” in Proc. PODC, 2020, pp. 139–148.
[5] A. Appan, A. Chandramouli, and A. Choudhury, “Perfectly-secure synchronous MPC with asynchronous fallback guarantees,” in Proc. PODC, 2022, pp. 92–102.
[6] A. Appan, A. Chandramouli, and A. Choudhury, “Revisiting the efficiency of asynchronous multi-party computation against general adversaries,” in Proc. IACR, 2022, pp. 651.
[7] B. Applebaum, E. Kachlon, and A. Patra, “The round complexity of perfect MPC with active security and optimal resiliency,” in Proc. FOCS, 2020, pp. 1277–1284.
[8] G. Asharov and Y. Lindell, “A full proof of the BGW protocol for perfectly secure multiparty computation,” J. Cryptol., vol. 30, no. 1, pp. 58–151, Aug. 2017.
[9] R. Bacho, D. Collins, C. Liu-Zhang, and J. Loss, “Network-agnostic security comes for free in DKG and MPC,” in Proc. IACR, 2022, p. 1369.
[10] L. Bangalore, A. Choudhury, and A. Patra, “The power of shunning: Efficient asynchronous Byzantine agreement revisited,” J. ACM, vol. 67, no. 3, p. 14, 2020.
[11] D. Beaver, “Efficient multi-party protocols using circuit randomization,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 576. Berlin, Germany: Springer, Aug. 1992, pp. 420–432.
[12] Z. Beerliová-Trubíniová and M. Hirt, “Efficient multi-party computation with dispute control,” in Theory of Cryptography (Lecture Notes in Computer Science), vol. 3876. Berlin, Germany: Springer, 2006, pp. 305–328.
[13] Z. Beerliová-Trubíniová and M. Hirt, “Simple and efficient perfectly-secure asynchronous MPC,” in Advances in Cryptology—ASIACRYPT (Lecture Notes in Computer Science), vol. 4833. Berlin, Germany: Springer, 2007, pp. 376–392.
[14] Z. Beerliová-Trubíniová and M. Hirt, “Perfectly-secure MPC with linear communication complexity,” in Theory of Cryptography (Lecture Notes in Computer Science), vol. 4948. Berlin, Germany: Springer, 2008, pp. 213–230.
[15] M. Ben-Or, “Another advantage of free choice: Completely asynchronous agreement protocols (extended abstract),” in Proc. PODC, 1983, pp. 27–30.
[16] M. Ben-Or, R. Canetti, and O. Goldreich, “Asynchronous secure computation,” in Proc. STOC, 1993, pp. 52–61.
[17] M. Ben-Or and A. Wigderson, “Completeness theorems for non-cryptographic fault-tolerant distributed computation,” in Proc. 26th Ann. ACM Symp. Theory Comput. (STOC), 1988, pp. 1–10.
[18] E. Ben-Sasson, S. Fehr, and R. Ostrovsky, “Near-linear unconditionally-secure multiparty computation with a dishonest minority,” in Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science), vol. 7417. Berlin, Germany: Springer, 2012, pp. 663–680.
[19] P. Berman, J. A. Garay, and K. J. Perry, “Bit optimal distributed consensus,” in Computer Science Research. Boston, MA, USA: Springer, 1992, pp. 313–322.
[20] E. Blum, J. Katz, and J. Loss, “Synchronous consensus with optimal asynchronous fallback guarantees,” in Theory of Cryptography (Lecture Notes in Computer Science), vol. 11891. Cham, Switzerland: Springer, 2019, pp. 131–150.
[21] E. Blum, J. Katz, and J. Loss, “Tardigrade: An atomic broadcast protocol for arbitrary network conditions,” in Advances in Cryptology—ASIACRYPT (Lecture Notes in Computer Science), vol. 13091. Cham, Switzerland: Springer, 2020, pp. 707–731.
[22] G. Bracha, “An asynchronous [t < |F|]3-resilient consensus protocol,” in Proc. 3rd Annu. ACM Symp. Princ. Distrib. Comput. (PODC), 1984, pp. 154–162.
[23] R. Canetti, “Studies in secure multiparty computation and applications,” Ph.D. thesis, Weizmann Inst., Rehovot, Israel, 1995.
[24] R. Canetti, “Security and composition of multiparty cryptographic protocols,” J. Cryptol., vol. 13, no. 1, pp. 143–202, Jan. 2000.
[25] R. Canetti and T. Rabin, “Fast asynchronous Byzantine agreement with optimal resilience,” in Proc. 25th Annu. ACM Symp. Theory Comput. (STOC), 1993, pp. 42–51.
[26] A. Chandramouli, A. Choudhury, and A. Patra, “A survey on perfectly secure verifiable secret-sharing,” ACM Comput. Surveys, vol. 54, no. 11s, pp. 1–36, Jan. 2022.
[27] D. Chaum, C. Crépieux, and I. Damgård, “Multiparty unconditionally secure protocols (extended abstract),” in Proc. STOC, 1988, pp. 11–19.
[28] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, “Verifiable secret sharing and achieving simultaneity in the presence of faults,” in Proc. 26th Annu. Symp. Found. Comput. Sci. (SFCS), 1985, pp. 383–395.
[29] A. Choudhury and A. Patra, “An efficient framework for unconditionally secure multiparty computation,” IEEE Trans. Inf. Theory, vol. 63, no. 1, pp. 428–468, Jan. 2017.
[30] A. Choudhury and A. Patra, “On the communication efficiency of statistically-secure asynchronous MPC with optimal resilience,” in Proc. IACR, 2022, p. 913.
[31] R. Cramer and I. Damgård, Multiparty Computation, an Introduction. Contemporary Cryptography. Basel, Switzerland: Birkhäuser, 2005.
[32] R. Cramer, I. Damgård, S. Dziembowski, M. Hirt, and T. Rabin, “Efficient multiparty computations secure against an adaptive adversary,” in Advances in Cryptology—EUROCRYPT (Lecture Notes in Computer Science), vol. 1592. Berlin, Germany: Springer, Aug. 1993, pp. 52–61.
[33] R. Cramer, I. Damgård, S. Dziembowski, M. Hirt, and T. Rabin, “Synchronous perfectly secure message transmission with optimal asynchronous fallback guarantees,” in Proc. IACR, 2022, p. 1397.
[34] D. Dolev, C. Dwork, O. Waarts, and M. Yung, “Perfectly secure message transmission,” J. ACM, vol. 40, no. 1, pp. 17–47, Jan. 1993.
[35] G. Deligios and C. Liu-Zhang, “Round-efficient Byzantine agreement and multi-party computation with asynchronous fallback,” in Theory of Cryptography (Lecture Notes in Computer Science), vol. 13042. Cham, Switzerland: Springer, 2021, pp. 623–653.
[36] G. Deligios and C. Liu-Zhang, “Synchronous perfectly secure message transmission with optimal asynchronous fallback guarantees,” in Proc. IACR, 2022, p. 1397.
[40] M. Fitzi, J. A. Garay, S. Gollakota, C. P. Rangan, and K. Srinathan, “Round-optimal and efficient verifiable secret sharing,” in Theory of Cryptography (Lecture Notes in Computer Science), vol. 3876. Berlin, Germany: Springer, 2006, pp. 329–342.

[41] R. Gennaro, Y. Ishai, E. Kushilevitz, and T. Rabin, “The round complexity of verifiable secret sharing and secure multicast,” in Proc. 33rd Annu. ACM Symp. Theory Comput., Jul. 2001, pp. 580–589.

[42] R. Gennaro, M. O. Rabin, and T. Rabin, “Simplified VSS and fast-track multiparty computations with applications to threshold cryptography,” in Proc. 17th Annu. ACM Symp. Princ. Distrib. Comput. (PODC), 1998, pp. 101–111.

[43] D. Ghinea, C.-D. Liu-Zhang, and R. Wattenhofer, “Optimal synchronous approximate agreement with asynchronous fallback,” in Proc. ACM Symp. Principles of Distributed Computing, Jul. 2002, pp. 70–80.

[44] O. Goldreich, The Foundations of Cryptography—Volume 2: Basic Applications. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[45] O. Goldreich, S. Micali, and A. Wigderson, “How to play any mental game or a completeness theorem for protocols with honest majority,” in Proc. STOC, 1987, pp. 218–229.

[46] V. Goyal, Y. Liu, and Y. Song, “Communication-efficient unconditional MPC with guaranteed output delivery,” in Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science), vol. 11693. Berlin, Germany: Springer, 2019, pp. 85–114.

[47] V. Goyal, Y. Song, and C. Zhu, “Guaranteed output delivery comes free in honest majority MPC,” in Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science), vol. 12171. Berlin, Germany: Springer, 2020, pp. 618–646.

[48] M. Hirt and U. Maurer, “Player simulation and general adversary structures in perfect multiparty computation,” J. Cryptol., vol. 13, no. 1, pp. 31–60, Jan. 2000.

[49] J. Katz, C.-Y. Koo, and R. Kunaresan, “Improving the round complexity of VSS in point-to-point networks,” Inf. Comput., vol. 207, no. 8, pp. 889–899, Aug. 2009.

[50] C. Liu-Zhang and U. Maurer, “Synchronous constructive cryptography,” in Theory of Cryptography (Lecture Notes in Computer Science), vol. 12551. Springer, 2020, pp. 439–472.

[51] R. J. McEliece and D. V. Sarwate, “On sharing secrets and Reed–Solomon codes,” Commun. ACM, vol. 24, no. 9, pp. 583–584, Sep. 1981.

[52] S. Micali and P. Rogaway, “Secure computation,” in Advances in Cryptology—CRYPTO, vol. 576. Berlin, Germany: Springer, 1991, pp. 392–404.

[53] A. Mostéfaoui, H. Mounen, and M. Raynal, “Signature-free asynchronous binary Byzantine consensus with t < n/3, O(n2) messages, and O(1) expected time,” J. ACM, vol. 62, no. 4, p. 31, 2015.

[54] A. Patra, A. Choudhury, and C. F. Rangan, “Efficient asynchronous verifiable secret sharing and multiparty computation,” J. Cryptol., vol. 28, no. 1, pp. 49–109, 2015.

[55] A. Patra and D. Ravi, “On the power of hybrid networks in multi-party computation,” IEEE Trans. Inf. Theory, vol. 64, no. 6, pp. 4207–4227, Jun. 2018.

[56] M. Pease, R. Shostak, and L. Lamport, “Reaching agreement in the presence of faults,” J. ACM, vol. 27, no. 2, pp. 228–234, 1980.

[57] M. O. Rabin, “Randomized Byzantine generals,” in Proc. FOCS, 1983, pp. 403–409.

[58] T. Rabin and M. Ben-Or, “Verifiable secret sharing and multiparty protocols with honest majority (extended abstract),” in Proc. STOC, 1989, pp. 73–85.

[59] A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[60] A. C. Yao, “Protocols for secure computations (extended abstract),” in Proc. FOCS, 1982, pp. 160–164.

Ananya Appan received the integrated M.Tech. degree in computer science from the International Institute of Information Technology, Bengaluru. She is currently a Developer with the SAP Laboratories, India. She was advised by Prof. Ashish Choudhury during her master’s thesis, where she focused on designing unconditionally-secure protocols for multi-party computation under varying network conditions. Her research interests include theoretical cryptography.

Anirudh Chandramouli received the bachelor’s and master’s degrees in computer science from the International Institute of Information Technology, Bengaluru. He is currently pursuing the Ph.D. degree with Bar-Ilan University, Israel, under the guidance of Prof. Gilad Asharov. His master’s thesis was under the guidance of Prof. Ashish Choudhury.

Ashish Choudhury received the M.S. (by Research) and Ph.D. degrees from the Computer Science and Engineering Department, Indian Institute of Technology (IIT) Madras. Post Ph.D. degree, he was a Visiting Researcher with the Indian Statistical Institute (ISI) Kolkata for a year, and then, a Research Assistant (a Post-Doctoral Researcher) with the University of Bristol for two years. He joined the International Institute of Information Technology (IIIT) Bengaluru in 2014, where he is currently an Associate Professor. He has coauthored a book on the topic of A Pragmatic Introduction to Secure Multiparty Computation, published as part of the synthesis lecture series on distributed computing. His research interests include theoretical cryptography, with an emphasis on secure multi-party computation (MPC). His work has appeared in the Journal of the ACM (JACM), Journal of Cryptology (JoC), Journal of Parallel and Distributed Computing (JPDC), Distributed Computing (DC), IEEE TRANSACTIONS ON INFORMATION THEORY, CRYPTO, PODC, ASIACRYPT, DISC and ICDCN. He has offered a number of MOOCs on various topics in cryptography which are offered as part of the national programme on technology enhanced learning (NPTEL), a project funded by the Government of India, offering free online courses in various disciplines of science and engineering.