Unconditionally Secure Asynchronous Multiparty Computation with Quadratic Communication Per Multiplication Gate

Arpita Patra * **Ashish Choudhary** † **C. Pandu Rangan** ‡
Department of Computer Science and Engineering
Indian Institute of Technology Madras
Chennai India 600036
Email:{ arpita,ashishc }@cse.iitm.ernet.in, rangan@iitm.ernet.in

Abstract

Secure multiparty computation (MPC) allows a set of n parties to securely compute an agreed function, even if up to t parties are under the control of an adversary. In this paper, we propose a new *Asynchronous secure multiparty computation* (AMPC) protocol that provides information theoretic security with $n = 4t + 1$, where t out of n parties can be under the influence of a *Byzantine (active)* adversary $\mathcal{A}_t$ having *unbounded computing power*. Our protocol communicates $\mathcal{O}(n^2 \log |\mathbb{F}|)$ bits per *multiplication gate* and involves a negligible error probability of $2^{-\Omega(\kappa)}$, where κ is the error parameter and $\mathbb{F}$ is the field over which the computation is carried out. The best known information theoretically secure AMPC with $n = 4t+1$ communicates $\mathcal{O}(n^3 \log |\mathbb{F}|)$ bits per multiplication and does not involve any error probability in computation. Though a negligible error probability is involved, our AMPC protocol provides the best communication complexity among all the known AMPC protocols providing information theoretic security. Moreover, the communication complexity of our AMPC is same as the communication complexity of the best known AMPC protocol with *cryptographic assumptions*.

As a tool for our AMPC protocol, we propose a new method of efficiently generating *d-sharing* of multiple secrets concurrently in asynchronous setting, where $t \leq d \leq 2t$. In the literature, though there are protocols for generating t-sharing and $2t$-sharing separately, there is no generic protocol for generating *d-sharing* for the range $t \leq d \leq 2t$. Comparing our protocol with the existing protocols for generating t-sharing and $2t$-sharing, we find that: (i) our protocol requires no extra cost in communication complexity in comparison to the best known method for generating t-sharing; (ii) it provides better communication complexity than the existing methods for generating $2t$-sharing.

Keywords: Multiparty Computation, Byzantine Adversary, Asynchronous Networks.

1 Introduction

Secure Multiparty Computation (MPC): Secure multiparty computation (MPC) [37] allows a set of n parties to securely compute an agreed function f, even if some of the parties are under the control of a centralized adversary. More specifically, assume that the agreed function f can be expressed as $f : \mathbb{F}^n \rightarrow \mathbb{F}^n$ and party P_i has input $x_i \in \mathbb{F}$, where $\mathbb{F}$ is a finite field. At the end of the computation of f, each honest P_i gets $y_i \in \mathbb{F}$, where $(y_1, \ldots, y_n) = f(x_1, \ldots, x_n)$, irrespective of the behavior of the corrupted parties (correctness). Moreover, the adversary should not get any information about the input and output of the honest parties, other than what can be inferred from the input and output of the corrupted parties (secrecy). MPC is one of the most important and fundamental problems in secure distributed computing. The problem has been studied extensively in different settings, depending upon whether the network is synchronous [37, 20, 7, 13, 33, 1, 22, 19, 21, 24, 3, 17, 26, 5, 25] or asynchronous [6, 8, 36, 32, 10, 27, 4, 30], the adversary is threshold [37, 20, 7, 13, 33, 1, 19, 21, 3, 17, 5, 22] or non-threshold [22, 16, 27, 2, 23], the adversary behavior is static [37, 20, 7, 13, 33, 1, 22, 19] or mobile [29], the security is cryptographic [20, 24, 25] or information theoretic [37, 7, 13, 33], whether the protocol is perfect (i.e., without any

*Financial Support from Microsoft Research India Acknowledged
†Financial Support from Infosys Technology India Acknowledged
‡Work Supported by Project No. CSE/05-06/076/DITX/CPAN on Protocols for Secure Communication and Computation, Sponsored by Department of Information Technology, Govt. of India

error) [7, 21, 5] or allows a negligible error probability [34, 33, 14, 15, 17, 3, 31] etc. In any general MPC protocol, the function f is specified by an arithmetic circuit over $\mathbb{F}$, consisting of input, linear (e.g. addition), multiplication, random and output gates. *Among all the different types of gate, the evaluation of a multiplication gate requires the most communication complexity. So the communication complexity of any general MPC is usually given in terms of the communication complexity per multiplication gate.*

The MPC problem has been studied extensively over synchronous networks which assumes that there is a global clock and the delay of any message in the network channels is bounded. However, though theoretically impressive, such networks do not model adequately real life networks like Internet. So in this paper, we study MPC in asynchronous networks, tolerating a threshold adversary, having unbounded computing power, who can corrupt t out of the n parties in Byzantine fashion.

Asynchronous Networks: Asynchronous networks model real life networks like Internet much better than their synchronous counterpart. Here the communication channels between the parties have arbitrary, yet finite delay (i.e the messages are guaranteed to reach eventually). To model this, the adversary is given the power to schedule the delivery of messages in the network. The inherent difficulty in designing a protocol in asynchronous network, comes from the fact that when a party does not receive an expected message then he cannot decide whether the sender is corrupted (and did not send the message at all) or the message is just delayed in the network. Therefore it is impossible to consider the inputs of all uncorrupted parties. So input of up to t (potentially honest) parties may get ignored because waiting for them could turn out to be endless. Moreover the tools used in synchronous settings, cannot be deployed in asynchronous settings in a straight forward manner. Hence, designing asynchronous protocols requires completely new set of primitives. For an excellent introduction to asynchronous protocols, see [11].

Asynchronous Multiparty Computation (AMPC): Unlike MPC in synchronous networks, designing AMPC protocols has received very less attention due to their inherent difficulty. It is known that AMPC under *cryptographic assumptions* [24, 25] is possible iff $n \geq 3t + 1$. In information theoretic settings, AMPC with *zero error* (i.e., *perfectly secure* AMPC) is possible iff $n \geq 4t + 1$ [6], whereas AMPC with *negligible error probability* is possible iff $n \geq 3t + 1$ [8]. The communication complexities *per multiplication* (denoted as "CC in bits/ Multiplication Gate" in the table given below) of the best known AMPC protocols are given in the following table, where IT denotes Information Theoretic security. Furthermore, for cryptographic AMPC, κ is the security parameter, while for information theoretic AMPC with negligible error probability, κ is the error parameter. Finally, c_M denotes the number of multiplication gates in the circuit representing the function f.

Reference	Type of Security	Resilience	CC in bits/ Multiplication Gate
[24]	Cryptographic	$t < n/3$ (optimal)	$\mathcal{O}(c_M n^3 \kappa)$
[25]	Cryptographic	$t < n/3$ (optimal)	$\mathcal{O}(c_M n^2 \kappa)$
[36]	IT (no error)	$t < n/4$ (optimal)	$\Omega(c_M n^5 \log(\lvert\mathbb{F}\rvert))$
[4]	IT (no error)	$t < n/4$ (optimal)	$\mathcal{O}(c_M n^3 \log(\lvert\mathbb{F}\rvert))$
[8]	IT (negligible error)	$t < n/3$ (optimal)	$\Omega(c_M n^{11} \kappa^4)$
[30]	IT (negligible error)	$t < n/3$ (optimal)	$\mathcal{O}(c_M n^5 \kappa)$
[32]	IT (negligible error)	$t < n/4$ (non-optimal)	$\mathcal{O}(c_M n^4 \kappa)$

Recently in [38], the authors have designed communication efficient MPC protocols over networks that exhibit partial asynchrony (where the network is synchronous up to certain point and becomes completely asynchronous after that). In another work, Damgaard et. al [18] have reported efficient MPC protocol over a network that assumes the concept of synchronization point; i.e,. the network is asynchronous before and after the synchronization point.

Our Contribution: We design an efficient information theoretic secure AMPC protocol with $n = 4t + 1$ satisfying : (a) TERMINATION: Every honest party terminates the protocol except with negligible probability of $2^{-\Omega(\kappa)}$, where κ is the error parameter, (b) CORRECTNESS: Every honest party receives the correct output at the end, except with negligible error probability of $2^{-\Omega(\kappa)}$, (c) SECRECY: The adversary gets no information about the inputs and outputs of *honest* parties apart from what can be computed from the inputs and outputs of the corrupted parties. Our protocol communicates $\mathcal{O}(n^2 \log \lvert\mathbb{F}\rvert)$ bits per multiplication and involves a negligible error probability of $2^{-\Omega(\kappa)}$ in **correctness** and **termination**, where $\mathbb{F}$ is the field over which the computation is carried out. Our AMPC is to be compared with the best known AMPC with $n = 4t + 1$ that communicates $\mathcal{O}(n^3 \log \lvert\mathbb{F}\rvert)$ bits per multiplication [4] and satisfies all the three properties, namely **termination**, **secrecy** and **correctness** perfectly (i.e without any error probability). Moreover, the communication complexity of our AMPC protocol is same as the communication complexity of the best known AMPC protocol with *cryptographic assumptions* [25].

As a tool for our AMPC protocol, we propose an efficient and generic method of generating *d-sharing* of secrets in asynchronous settings, for any d in the range $t \leq d \leq 2t$. Even though there are asynchronous protocols to generate t-sharing as well as $2t$-sharing separately, there is no generic protocol to generate d-sharing, for $t \leq d \leq 2t$, in asynchronous settings. Comparing our protocol with the existing protocols for generating t-sharing and $2t$-sharing, we find that: (i) our protocol requires no extra cost in communication complexity in comparison to the best known method for generating t-sharing; (ii) it provides better communication complexity than the existing methods [4] for generating $2t$-sharing.

2 Preliminaries

Model: We follow the network model of [6], where there is a set of n parties denoted by $\mathcal{P} = \{P_1, \ldots, P_n\}$, who are pairwise connected by secure asynchronous channels. An adversary $\mathcal{A}_t$ with *unbounded computing power* can control at most $t < \frac{n}{4}$ parties in Byzantine fashion and can force the corrupted parties to deviate from the protocol in any arbitrary manner. Moreover, the adversary is given the power to schedule messages over each channel. But he will have no access to the messages sent by honest parties. The function to be computed is specified by an arithmetic circuit over a finite field $\mathbb{F}$, consisting of input, linear (e.g. addition), multiplication, random and output gates. We denote the number of gates of each type by c_I, c_L, c_M, c_R and c_O respectively.

The Ground Field and The Extension Field: For the rest of the paper, we fix a finite field $\mathbb{F}$ with $|\mathbb{F}| \geq n$ over which most of our computations will be performed. We call $\mathbb{F}$ as the *Ground Field*. Any element from $\mathbb{F}$ can be represented by $\log |\mathbb{F}|$ bits. We also fix an extension field $\mathbb{E} \supset \mathbb{F}$ to be the smallest extension for which $|\mathbb{E}| \geq 2^{\kappa}$. Each element of $\mathbb{E}$ can be written down using $\mathcal{O}(\kappa)$ bits. We call $\mathbb{E}$ as *Extension Field*. Moreover, without loss of generality, we assume that $n = \text{poly}(\kappa)$.

A-cast, Agreement on a Core Set (ACS)

A-Cast[12]: It is an asynchronous broadcast primitive, introduced and elegantly implemented by Bracha [9] with $n \geq 3t + 1$. A-Cast of b bits incurs a private communication of $\mathcal{O}(n^2 b)$ bits [9]. Let Π be an asynchronous protocol initiated by a special party (called the sender), having input m (the message to be broadcast). We say that Π is a t-resilient A-cast protocol if the following hold:

- **Termination**: (1) If the sender is honest and all the honest parties participate in the protocol, then each honest party will eventually terminate the protocol. (2) Irrespective of the behavior of the sender, if any honest party terminates the protocol then each honest party will eventually terminate the protocol.
- **Correctness**: If the honest parties terminate the protocol then they have a common output m^*. Furthermore, if the sender is honest then $m^* = m$.

Agreement on Core Set (ACS)[4, 8]: It is a primitive presented in [6, 8]. It is used to determine a set of $n - t$ parties that correctly shared their values. More concretely, every party P_i starts the ACS protocol with an accumulative set of parties who from P_i's view point correctly shared their values. The output of the protocol is a set of at least $n - t$ parties, who correctly shared their values. The communication cost of ACS protocol is $\Omega(n^4 \log n)$ bits [4].

Definition 1 (d-Sharing [3]) : *A value $s \in \mathbb{F}$ is said to be d-shared among a set of parties $\overline{\mathcal{P}} \subseteq \mathcal{P}$ with $|\overline{\mathcal{P}}| \geq d + 1$ if* **every honest** *$P_i \in \overline{\mathcal{P}}$ is holding a share s_i of s, such that there exists a degree-d polynomial $f(x)$ over $\mathbb{F}$ with $f(0) = s$ and $f(i) = s_i$ for every honest $P_i \in \overline{\mathcal{P}}$. The vector of shares is called a d-sharing of s and is denoted by $[s]_d$.*

Definition 2 ($(t, 2t)$-Sharing [5]:) *A value s is said to be $(t, 2t)$-shared among the parties in $\mathcal{P}$, denoted as $[s]_{(t,2t)}$, if s is both t-shared and $2t$-shared among the parties in $\mathcal{P}$.*

3 AMPC Protocol Overview

Our AMPC protocol proceeds in three phases: preparation phase, input phase and computation phase. Every honest party will eventually complete each phase with very high probability. In the preparation phase, $(t, 2t)$-sharing of $c_M + c_R$ random values will be generated. For this, we use our proposed efficient protocol for d-sharing. Each multiplication gate and random gate of the circuit will be associated with a $(t, 2t)$-sharing. In the input phase the parties t-share (commit) their inputs and agree on a core set of $n - t$ parties who correctly t-shared their inputs (every honest party will eventually get a share of the inputs of the parties in the core set). In the computation phase, based on the inputs of the parties in core set, the actual circuit will be computed gate by gate, such that the outputs of the intermediate gates are always kept as secret and are properly t-shared among the parties. Due to the linearity of the used t-sharing, the linear gates can be computed locally without requiring any communication. Each multiplication gate will be evaluated with the help of the $(t, 2t)$-sharing associated with it. For evaluating multiplication gate, we adapt a technique from [17] used in synchronous settings. The same technique is also adapted in the AMPC protocol of [4].

4 Reconstruction of d-Sharing

Assume that a secret $s \in \mathbb{F}$ is d-shared among the parties in $\mathcal{P}$ by a degree-d polynomial $f(x)$, such that $f(0) = s$ and $d < n - 2t$. Let $P_\alpha \in \mathcal{P}$ be a *receiver*. We now give a protocol **Rec-Private**, which allows P_α to privately reconstruct $f(x)$ and hence $s = f(0)$ in asynchronous settings. Moreover, if P_α is honest then s remains secure. The high level idea of the protocol is as follows: Every party P_i sends his share s_i of s to P_α. The shares may reach P_α in any arbitrary order. Moreover, up to t of the shares may be incorrect or missing. To reconstruct $f(x)$, P_α applies OEC (Online Error Correcting) technique [6] on the received s_i's to get the polynomial $f(x)$ and reconstructs $s = f(0)$. Roughly speaking, the online error correcting method enables P_α to recognize when the received shares define a unique degree-d interpolation polynomial. We call the reconstruction of s by P_α as the P_α-Private-Reconstruction of s.

Protocol Rec-Private($\mathcal{P}, d, s, P_\alpha$): P_α-Private-Reconstruction of s by Receiver P_α

CODE FOR P_i: Send s_i to P_α.

CODE FOR P_α: Apply On-line Error Correcting (OEC) technique on the received s_i's to interpolate a unique degree-d polynomial $f(x)$ and output $s = f(0)$.

Theorem 1 ([11]) *For any secret s which is correctly d-shared among a set of n parties, with $d < n-2t$, protocol Rec-Private achieves the following properties tolerating any $\mathcal{A}_t$:*

– TERMINATION: *If P_α is honest, then P_α will eventually terminate Rec-Private.*

– CORRECTNESS: *An honest P_α will always output s correctly at the end of the protocol.*

– SECRECY: *If P_α is honest then $\mathcal{A}_t$ obtains no information about s.*

– COMMUNICATION COMPLEXITY: *Protocol Rec-Private privately communicates $\mathcal{O}(n \log |\mathbb{F}|)$ bits.*

Theorem 2 *(i) Protocol Rec-Private can be used to reconstruct $2t$-sharing of some secret s which is shared among the parties in $\mathcal{P}$, where $|\mathcal{P}| = 4t + 1$.*

(ii) If $\overline{\mathcal{P}}$ is any $3t + 1$ sized subset of $\mathcal{P}$, such that s is t-shared among the parties in $\overline{\mathcal{P}}$, then Rec-Private($\overline{\mathcal{P}}, t, s, P_\alpha$) ensures successful P_α-Private-Reconstruction of s.

(iii) Let s be correctly d-shared among a set of n parties, except with probability $2^{-\Omega(\kappa)}$, where $d < n-2t$. Then Rec-Private satisfies the TERMINATION *and* CORRECTNESS *properties mentioned in Theorem 1, except with probability $2^{-\Omega(\kappa)}$.*

For the description of OEC and proof of Theorem 2, see **APPENDIX A**.

5 Generating d-Sharing with $d < n - 2t$

We now present a novel protocol, called d-Share-MS, that allows a dealer $D \in \mathcal{P}$ (dealer can be any party from $\mathcal{P}$) to concurrently d-share $\ell \geq 1$ secrets from $\mathbb{F}$, among the parties in $\mathcal{P}$, except with error probability of $2^{-\Omega(\kappa)}$, where $t \leq d \leq 2t$. Protocol d-Share-MS achieves the following properties:

Property 1

1. TERMINATION: *(a) If D is honest, then every honest party will eventually terminate the protocol. (b) If D is corrupted and some honest party has terminated the protocol, then all the honest parties will eventually terminate the protocol, except with probability $2^{-\Omega(\kappa)}$.*

2. CORRECTNESS: *(a) If D is honest, then all the ℓ secrets will be correctly d-shared among the honest parties in $\mathcal{P}$. (b) If D is corrupted and the honest parties in $\mathcal{P}$ terminate the protocol, then there are ℓ secrets that are properly d-shared among the honest parties in $\mathcal{P}$, except with probability $2^{-\Omega(\kappa)}$.*

3. SECRECY: *If D is honest, then $\mathcal{A}_t$ obtains no information about the secrets of D.*

Comparison with Existing Protocols for t-sharing and $2t$-sharing in Asynchronous Settings: In [4], the authors have presented a protocol for generating t-sharing of ℓ secrets concurrently (the protocol is a simple extension of Canetti's [11] protocol for generating t-sharing of a single secret). The protocol of [4] requires private communication of $\mathcal{O}(\ell n^2 \log |\mathbb{F}|)$ bits and A-cast of $\mathcal{O}(n^2 \log |\mathbb{F}|)$ bits. But protocol of [4] is not extendible to generate d-sharing for $d > t$. In order to generate $2t$-sharing of a *single* secret, [4] have used another protocol, which uses t-sharing of $2t+1$ random secrets to generate $2t$-sharing of a *single* secret. This incurs a private communication of $\mathcal{O}(n^3 \log |\mathbb{F}|)$ bits and A-cast of $\mathcal{O}(n^2 \log |\mathbb{F}|)$ bits, for a *single* secret. Our protocol for generating d-sharing with $t \leq d \leq 2t$ is *generic* and can generate d-sharing of ℓ secrets concurrently, with a private communication of $\mathcal{O}((\ell n^2 + n^3) \log |\mathbb{F}|)$ bits and A-cast of $\mathcal{O}(n^3 \kappa)$ bits. If ℓ is significantly large, then instead of generating $2t$-sharing of the individual secrets by executing ℓ instances of the protocol of [4], we can generate the $2t$-sharing of all the secrets concurrently by executing a single instance of our protocol, which will result in less communication overhead. Specifically, if $\ell = \Omega(n)$, then our protocol gains a factor of $\Omega(n)$, in generating $2t$-sharing of ℓ secrets, in comparison to the protocol of [4].

For the ease of understanding, we first present a protocol, called d-Share-SS, that allows D to d-share a single secret among the parties in $\mathcal{P}$ except with error probability of $2^{-\Omega(\kappa)}$. Later we present protocol d-Share-MS which is simple extension of d-Share-SS. Our discussion will clearly show, that executing a *single* instance of d-Share-MS dealing with multiple secrets *concurrently*, is advantageous over executing *multiple* instances of d-Share-SS, dealing with single secret, in terms communication complexity (see Remark 1 at the end of this section). Thus protocol d-Share-MS harnesses the advantages offered by dealing with multiple secrets *concurrently*. The sole purpose of presenting d-Share-SS is to simplify the overall presentation of d-Share-MS. We divide the structure of d-Share-SS into three main phases:

1. **Distribution by D:** As the name suggests, in this phase, D on having a secret s, distributes information to the parties in $\mathcal{P}$ in order to generate d-sharing of s.

2. **Verification & Agreement on CORE:** Here the parties in $\mathcal{P}$ jointly perform some computation and communication in order to verify consistency of the information distributed by D in **Distribution by** D phase. In case of successful verification, all the honest parties agree on a set of at least $3t+1$ parties, called $CORE$, satisfying certain properties.

3. **Generation of d-sharing of Secret:** In this phase, *only* the parties in $CORE$ communicate to every party in $\mathcal{P}$ and every party performs local computation (on the data received from the parties in $CORE$) to finally generate the d-sharing of secret s.

We now focus on the details of each of these phases.

5.1 Distribution by D

In this phase, D on having a secret s, selects a random bivariate polynomial $F(x,y)$ of degree d in x and t in y, such that $F(0,0) = s$. Let $f_i(x) = F(x,i)$, $p_i(y) = F(i,y)$. While all $f_i(x)$ polynomials are of degree-d, all $p_i(y)$ polynomials are of degree-t. We will call the $f_i(x)$ polynomials as *row polynomials* and $p_i(y)$ polynomials as *column polynomials*. Now D sends $f_i(x)$ to party P_i. In this phase, D also distributes some more information which will be used to keep his secret secure during **Verification & Agreement on CORE** phase. Precisely, D distributes the shares of $(t+1)n$ random polynomials of degree-t which will be used for *blinding* purpose in **Verification & Agreement on CORE** phase. We refer these polynomials as *blinding polynomials*, so that its purpose and role is clear to the reader. The reason for taking $(t+1)n$ blinding polynomials will be clear in the next section.

Protocol Distr-SS($D, \mathcal{P}, s, d$)

CODE FOR D:

1. Select a random bivariate polynomial $F(x,y)$ of degree-d in x and degree-t in y, such that $F(0,0) = s$. Let $f_i(x) = F(x,i)$, $p_i(y) = F(i,y)$ for $0 \leq i \leq n$.
2. Select $(t+1)n$ degree-t, random, distinct *blinding polynomials*, over $\mathbb{F}$, denoted by $b^{(P_i,1)}(y), \ldots, b^{(P_i,t+1)}(y)$ for $i = 1, \ldots, n$.
3. Send the following to party P_i: (i) $f_i(x)$; (ii) $b^{(P_j,1)}(i), \ldots, b^{(P_j,t+1)}(i)$ for $j = 1, \ldots, n$.

Before proceeding further, we would like to mention few interesting points about the above protocol. The bivariate polynomial $F(x, y)$, selected by D, has degree d in x and degree t in y. This results in each row polynomial to be of degree-d and each column polynomial to be of degree-t. On the other hand, all the existing protocols for generating t-sharing, based on the approach of bivariate polynomial, selects the degree of both x and y to be t [11, 4]. In subsequent phases, we create a situation, where the parties have to only reconstruct the column polynomials, to complete the d-sharing. So even though, the row polynomials are of degree more than t, the parties need not have to bother about reconstructing them.

In the sequel, we describe **Verification & Agreement on CORE** phase. If **Verification & Agreement on CORE** phase is successful, then at the end of **Generation of d-sharing of Secret** phase, the secret s will be d-shared using polynomial $f_0(x)$.

5.2 Verification & Agreement on CORE

As it is clear from the description of **Distribution by** D phase, if D behaves honestly in protocol Distr-SS, then j^{th} points on *all row polynomial* $f_i(x)$, corresponding to honest P_i's (i.e $f_i(j)$'s), should define degree-t *column polynomial* $p_j(y)$. For an honest D, this is obviously true. But for a corrupted D, we must ensure the above condition by enforcing some verification mechanism. While it may be difficult to ensure that the j^{th} points on *all* honest P_i's row polynomial $f_i(x)$ define a degree-t polynomial $p_j(y)$ (due to asynchrony of the network), it is easier to ensure the same for the honest parties in a set of at least $3t + 1$ parties, say $CORE$ ($CORE \subseteq \mathcal{P}$). In fact, this is what our protocol attempts to achieve. Specifically, the protocol tries to identify a set of parties, called $CORE$, having the following property:

Desired Properties of $CORE$: $CORE \subseteq \mathcal{P}$, such that $|CORE| \geq 3t + 1$. Moreover, for $j = 1, \ldots, n$, the j^{th} points on all honest P_i's row polynomial $f_i(x)$ of degree-d, where $P_i \in CORE$, should define a degree-t column polynomial $p_j(y)$.

Hence, we do not care about $f_i(x)$ possessed by P_i, for $P_i \notin CORE$. The verification mechanism and the construction of $CORE$ is the crux of protocol d-Share-SS.

An Informal Description: In our verification mechanism, every party has dual responsibility: (a) it acts as a verifier to verify certain consistency of the information distributed by D to the parties; (b) it also co-operates as a party, with other verifiers, in order to make the verification mechanism initiated by them, finishes successfully. So, we first concentrate on the part of communications and computations that is to be carried out with respect to a single verifier, say V (here V can be any party from $\mathcal{P}$). The goal of this part of communications and computations is to decide on a set of at least $3t + 1$ parties, say $AgreeSet^V$, such that if V is honest, then $AgreeSet^V$ should satisfy all the desirable properties of $CORE$. That is $AgreeSet^V$ could be a eligible candidate for $CORE$, when V is honest. To implement this, we use the following protocol. In the protocol, we use the following notation:

Notation 1 *Given ρ polynomials, $C = \{c_1(x), \ldots, c_\rho(x)\}$ and a vector $R = (\zeta_1, \ldots, \zeta_\rho)$ of length ρ, we define $c(x)$ as the polynomial obtained by the linear combination of the polynomials in C with respect to R. That is, $c(x) = \sum_{i=1}^{\rho} \zeta_i . c_i(x)$. We capture this by: $c(x) = \mathsf{LinCombPoly}(C, R)$. Similarly, we define $c = \mathsf{LinCombValue}(C, R)$, where $C = \{c_1, \ldots, c_\rho\}$ and c is the linear combination of C, with respect to R.*

Protocol Single-Verifier-SS$(V, \mathcal{P}, s, d)$

i. CODE FOR P_i:

1. Wait to receive $f_i(x)$ and $b^{(P_j,1)}(i), \ldots, b^{(P_j,t+1)}(i)$ for $j = 1, \ldots, n$ from D.
2. After receiving, check whether $f_i(x)$ is a degree-d polynomial. If yes, then send a `Received-From-D` signal to V.

ii. CODE FOR V:

1. Wait to obtain `Received-From-D` signal from at least $3t+1$ parties. Put the identities of the $3t+1$ parties in a set $ReceivedSet^{(V,1)}$. Select a random $r^{(V,1)}$ from extension field $\mathbb{E}$ and A-cast $(r^{(V,1)}, ReceivedSet^{(V,1)})$.
2. For β^{th} ($\beta > 1$) receipt of `Received-From-D` from $P_\alpha \notin ReceivedSet^{(V,\beta-1)}$, construct $ReceivedSet^{(V,\beta)} = ReceivedSet^{(V,\beta-1)} \cup \{P_\alpha\}$, select a random $r^{(V,\beta)} \in \mathbb{E} \setminus \{r^{(V,1)}, \ldots, r^{(V,\beta-1)}\}$ and A-cast $(r^{(V,\beta)}, ReceivedSet^{(V,\beta)})$.

iii. CODE FOR D:

1. If $(r^{(V,\beta)}, ReceivedSet^{(V,\beta)})$ is received from the A-cast of V, then A-cast the polynomial $E^{(V,\beta)}(y)$, where $E^{(V,\beta)}(y) =$ LinCombPoly$(\mathcal{E}, R)$. Here $\mathcal{E} = \{b^{(V,\beta)}(y), p_1(y), \ldots, p_n(y)\}$ and $R = (1, r^{(V,\beta)}, \left(r^{(V,\beta)}\right)^2, \ldots, \left(r^{(V,\beta)}\right)^n)$.

iv. CODE FOR P_i:

1. If $(r^{(V,\beta)}, ReceivedSet^{(V,\beta)})$ is received from the A-cast of V, then check if $P_i \in ReceivedSet^{(V,\beta)}$. If yes, then A-cast $e_i^{(V,\beta)} =$ LinCombValue(Δ_i, R), where $\Delta_i = \{b^{(V,\beta)}(i), f_i(1), \ldots, f_i(n)\}$ and $R = (1, r^{(V,\beta)}, \left(r^{(V,\beta)}\right)^2, \ldots, \left(r^{(V,\beta)}\right)^n)$.
2. Say that **party P_j agrees with D with respect to** $(r^{(V,\beta)}, ReceivedSet^{(V,\beta)})$ if all the following hold:
   (a) $E^{(V,\beta)}(y)$ is a degree-t polynomial, (b) $P_j \in ReceivedSet^{(V,\beta)}$ and (c) $e_j^{(V,\beta)} = E^{(V,\beta)}(j)$
   where $e_j^{(V,\beta)}$, $E^{(V,\beta)}(y)$ and $(r^{(V,\beta)}, ReceivedSet^{(V,\beta)})$ are received from the A-casts of P_j, D and V respectively.
3. With respect to $(r^{(V,\beta)}, ReceivedSet^{(V,\beta)})$, when there are $3t+1$ P_j's who agree with D, add them in a set $AgreeSet^{(V,\beta)}$.

Lemma 1 *In protocol Single-Verifier-SS, if V is honest, then for all $j = 1, \ldots, n$, the j^{th} points on the row polynomials, held by the honest parties in $AgreeSet^{(V,\beta)}$ (with $|AgreeSet^{(V,\beta)}| \geq 3t+1$), define degree-$t$ column polynomial, with very high probability. Moreover, the points on blinding polynomial $b^{(V,\beta)}(y)$ held by the honest parties in $AgreeSet^{(V,\beta)}$ will lie on a degree-t polynomial with very high probability.*

PROOF: If D is honest, then the condition in the lemma will be true, without any error. Hence we consider the case when D is corrupted. Let $H^{(V,\beta)}$ denote the set of honest parties in $AgreeSet^{(V,\beta)}$. First of all, since V is honest, he A-casts random $r^{(V,\beta)}$ only after listening `Received-From-D` signal from all the parties in $ReceivedSet^{(V,\beta)}$. Thus D has no knowledge of $r^{(V,\beta)}$, when he distributes the row polynomials and points on blinding polynomial $b^{(V,\beta)}(y)$ to the (honest) parties in $ReceivedSet^{(V,\beta)}$. Let $\overline{b^{(V,\beta)}(y)}$ denote the *minimum degree* polynomial, defined by the points on $b^{(V,\beta)}(y)$, held by the honest parties in $H^{(V,\beta)}$. Similarly, let $\overline{p_1(y)}, \ldots, \overline{p_n(y)}$ denote the *minimum degree* polynomials, defined by the points on the row polynomials, held by the parties in $H^{(V,\beta)}$. For convenience, we use an uniform notation for these $n+1$ polynomials. We denote them by $h^0(y), \ldots, h^n(y)$, respectively. Then the value $e_i^{(V,\beta)}$, A-casted by $P_i \in ReceivedSet^{(V,\beta)}$ is defined as $e_i^{(V,\beta)} = \sum_{j=0}^{n} \left(r^{(V,\beta)}\right)^j h^j(i)$.

We now claim that with very high probability, $h^0(y), \ldots, h^n(y)$ have degree-t. On the contrary, if we assume that at least one of the polynomials has degree more than t, then we can show that the minimum degree polynomial, say $h^{min}(y)$, defined by $e_i^{(V,\beta)}$'s for $P_i \in H^{(V,\beta)}$ will be of degree more than t, with very high probability. This will clearly imply $E^{(V,\beta)}(y) \neq h^{min}(y)$ and hence $e_i^{(V,\beta)} \neq E^{(V,\beta)}(i)$ for at least one $P_i \in H^{(V,\beta)}$. This is a contradiction as $e_i^{(V,\beta)} = E^{(V,\beta)}(i)$ holds for every $P_i \in Agree^{(V,\beta)}$ and $H^{(V,\beta)} \subseteq Agree^{(V,\beta)}$. This shows that our claim is true.

So we proceed to prove that $h^{min}(y)$ will be of degree more than t with very high probability, when one of $h^0(y), \ldots, h^n(y)$ has degree more than t. For this, we show the following:

1. We first show that $h^{def}(y) = \Sigma_{j=0}^{n} \left(r^{(V,\beta)}\right)^j h^j(y)$ will of degree more than t with very high probability, if one of $h^0(y), \ldots, h^n(y)$ has degree more than t.
2. We then show that $h^{min}(y) = h^{def}(y)$, implying that $h^{min}(y)$ will be of degree more than t with very high probability

The first claim is easy to prove. If at least one of $h^0(y), \ldots, h^n(y)$, has degree more than t, then the linear combination of these polynomials, namely $h^{def}(y)$, can be written as $h^{def}(y) = h_1^{def}(y) + h_2^{def}(y)$. Here

$h_1^{def}(y)$ contains all the coefficients of $h^{def}(y)$, having exponent more than t, while $h_2^{def}(y)$ contains all the remaining coefficients of $h^{def}(y)$. Now $h^{def}(y)$ will be of degree-t, if $h_1^{def}(y) = 0$, which can happen for at most n possible values of $r^{(V,\beta)}$ (for details see **APPENDIX C**). Since $r^{(V,\beta)}$ is selected randomly from $\mathbb{E} \setminus \{r^{(V,1)}, \ldots, r^{(V,\beta-1)}\}$, independent of $h^0(y), \ldots, h^n(y)$, the probability that $h_1^{def}(y) = 0$ is at most $\frac{n}{|\mathbb{E}|-(\beta-1)} \approx 2^{-\Omega(\kappa)}$ (which is negligible), where $\beta \leq t+1$ (see Lemma 2).

For the second point, consider the polynomial $dp(y) = h^{def}(y) - h^{min}(y)$. Clearly, $dp(y) = 0$, for all $y = i$, where $P_i \in H^{(V,\beta)}$. Thus $dp(y)$ will have at least $|H^{(V,\beta)}|$ roots. On the other hand, maximum degree of $dp(y)$ could be $|H^{(V,\beta)}| - 1$. These two facts together imply that $dp(y)$ is the zero polynomial, implying $h^{def}(y) = h^{min}(y)$. The complete formal proof of the lemma is given in **APPENDIX C**. □

Lemma 2 *In Single-Verifier-SS, V will A-Cast $(r^{(V,\beta)}, ReceivedSet^{(V,\beta)})$ at most $t+1$ times. Hence the maximum value of β is $t+1$. Moreover, each $ReceivedSet^{(V,\beta)}$ will be unique.*

PROOF: Easy. For complete proof, see **APPENDIX C**. □

Lemma 3 *In protocol Single-Verifier-SS, if both V and D are honest, then for some β $(1 \leq \beta \leq t+1)$ $AgreeSet^{(V,\beta)}$ with $|AgreeSet^{(V,\beta)}| \geq 3t+1$ will be generated.*

PROOF: When D is honest, every honest party in $\mathcal{P}$ will eventually send `Received-From-D` signal to V. From the protocol step, $|ReceivedSet^{(V,1)}| = 3t+1$. Moreover, from Lemma 2, V will A-Cast $ReceivedSet^{(V,\beta)}$ at most $t+1$ times. These facts together imply that eventually there will be a $\beta \in \{1, \ldots, t+1\}$, such that $ReceivedSet^{(V,\beta)}$ is bound to contain all the $3t+1$ honest parties. Moreover, each honest party from $ReceivedSet^{(V,\beta)}$ containing $3t+1$ honest parties, will eventually enter into $AgreeSet^{(V,\beta)}$. Hence $|AgreeSet^{(V,\beta)}|$ will be at least $3t+1$ eventually. □

Lemma 4 *In protocol Single-Verifier-SS, if D is honest, then $\mathcal{A}_t$ will have no information about s.*

PROOF: Without loss of generality, let $\mathcal{A}_t$ controls $P_1, \ldots, P_t$. So $\mathcal{A}_t$ will know $f_1(x), \ldots, f_t(x)$. Since $F(x,y)$ is of degree d and t in x and y respectively, its constant term $F(0,0)$ will remain information theoretically secure. $\mathcal{A}_t$ may learn $E^{(V,\beta)}(y)$ for $\beta = 1, \ldots, t+1$. But each $E^{(V,\beta)}(y)$ is the linear combination of polynomials $b^{(V,\beta)}(y), p_1(y), \ldots, p_n(y)$. As $b^{(V,\beta)}(y)$ is completely random and independent of $p_1(y), \ldots, p_n(y)$, $E^{(V,\beta)}(y)$ will be completely random for $\mathcal{A}_t$. Moreover for every $\beta \in \{1, \ldots, t+1\}$, distinct $b^{(V,\beta)}(y)$ is used. Hence $\mathcal{A}_t$ obtains no information about s in Single-Verifier-SS. □

So far, we have concentrated on the part of the communications that is to be carried out with respect to a single V. We proved that if V is honest then Single-Verifier-SS can provide with a candidate solution for $CORE$. But as we do not know the exact identities of the honest parties in $\mathcal{P}$, we can not pick a $AgreeSet^{(V,*)}$ for an honest V as $CORE$. Thus $CORE$ construction requires a special trick. Informally, we execute Single-Verifier-SS for every $V \in \mathcal{P}$ and compute $CORE$ based on $AgreeSet^{(*,*)}$'s.

Need for $n(t+1)$ Blinding Polynomials: Recall that in Distr-SS, D has selected $n(t+1)$ *blinding polynomials*. The reason for this is as follows: From Lemma 2, a single verifier V will A-Cast at most $t+1$ $(r^{(V,\beta)}, ReceivedSet^{(V,\beta)})$'s. Hence β will be at most $t+1$ for V. Now, from Lemma 4, in order to maintain the secrecy of s for every $\beta \in \{1, \ldots, t+1\}$, distinct $b^{(V,\beta)}(y)$ should be used for computing $E^{(V,\beta)}(y)$. Now in **Verification and Agreement on** $CORE$ phase, each of the n parties will act as a verifier and execute protocol Single-Verifier-SS. Hence D should select $n(t+1)$ blinding polynomials. □

Before presenting our protocol for **Verification & Agreement on CORE** phase, we prove the following lemmas which will help to grasp the part of code used for constructing $CORE$.

Lemma 5 *For an* **honest** *V, the row polynomials held by honest parties in $AgreeSet^{(V,\beta)}$ and $AgreeSet^{(V,\gamma)}$ with $\beta \neq \gamma$, define the same degree-t column polynomials, say $p_1(y), \ldots, p_n(y)$, with very high probability.*

PROOF: By Lemma 1, for an honest V, the row polynomials held by the honest parties in $AgreeSet^{(V,\beta)}$, define degree-t column polynomials, say $\overline{p_1(y)}, \ldots, \overline{p_n(y)}$, with very high probability. Similarly, by Lemma 1, the row polynomials held by the honest parties in $AgreeSet^{(V,\gamma)}$, define degree-t column polynomials, say $\widehat{p_1(y)}, \ldots, \widehat{p_n(y)}$, with very high probability. We claim that these two sets of polynomials are identical. Since $AgreeSet^{(V,\beta)}$ and $AgreeSet^{(V,\gamma)}$ are of size at least $3t+1$, there are at least $2t+1$ common parties between them out of which at least $t+1$ are honest. Since all the polynomials are of degree t, any $t+1$ points completely and uniquely define them and hence these two set of polynomials can not be different while having $t+1$ common values. □

Lemma 6 *For any two* **honest** *verifiers V_α and V_δ, with $\alpha \neq \delta$, the column polynomials, defined by the points on the row polynomials of the honest parties in any two sets $AgreeSet^{(V_\alpha,\beta)}$ and $AgreeSet^{(V_\delta,\gamma)}$ are same, with very high probability.*

PROOF: Follows using similar argument as in Lemma 5. □

The protocol for **Verification & Agreement on CORE** phase is as follows:

Protocol Ver-Agree-on-CORE-SS($D, \mathcal{P}, s, d$)

<u>VERIFICATION AND $CORE$ CONSTRUCTION:</u>

i. CODE FOR P_i:

1. Start executing Protocol Single-Verifier-SS($P_\alpha, \mathcal{P}, s, d$) for every verifier $P_\alpha \in \mathcal{P}$ parallely.
2. Add a verifier P_α to a set $ValidVerifier$ if at least one $AgreeSet^{(P_\alpha,\beta)}$ has been generated.
3. Check whether $|ValidVerifier| \geq t+1$ and in case of 'yes' perform the following computation:
   (a) For every $P_\alpha \in ValidVerifier$, compute $AgreeSet^{P_\alpha} = \cup_\beta AgreeSet^{(P_\alpha,\beta)}$.
   (b) Compute $CORE_i = \{P_j \mid P_j$ belongs to $AgreeSet^{P_\alpha}$ for at least t+1 $P'_\alpha s$ in $ValidVerifier\}$.
   (c) Wait for new updates (such as generation of new set $AgreeSet^{(P_\alpha,\beta)}$, expansion of $AgreeSet^{(P_\alpha,\beta)}$ etc.) and repeat the same computation (i.e steps 2-3((a),(b)) to update $CORE_i$ for every new update.

ii. CODE FOR D:

1. A-cast $CORE = CORE_D$ as soon as $|CORE_D| = 3t+1$.

<u>AGREEMENT ON CORE:</u> CODE FOR P_i:

1. Wait to receive $CORE$ from the A-cast of D. Wait until $CORE \subseteq CORE_i$. Once this holds, agree on the $CORE$ and terminate.

Lemma 7 *If D is honest, then the points on the row polynomials held by honest parties in $CORE$ define degree-t column polynomials. If D is corrupted, then the same holds except with negligible error probability. Moreover there can not be another set $\overline{CORE}$ containing $3t+1$ parties such that the row polynomials held by honest parties in $\overline{CORE}$ define a different set of degree-t column polynomials.*

PROOF: The complete proof is moved to **APPENDIX C**, due to space constraints. □

Once the parties agree on a $CORE$ set, generation of d-sharing requires n private reconstructions. We do that in **Generation of d-sharing of Secret** phase which is discussed in the sequel.

5.3 Generation of d-sharing of Secret

Assuming that the honest parties in $\mathcal{P}$ have agreed upon a $CORE$, our protocol achieves d-sharing of s in the following way: Since $|CORE| \geq 3t+1$ and each $p_i(0)$ is t-shared among the parties in $CORE$, from the property (ii) of Theorem 2, each $p_i(0)$ can be P_i-Private-Reconstructed for $i = 1, \ldots, n$. Every P_i can then output $p_i(0)$ as the shares of D's secret s and this will complete the d-sharing. As $f_0(i) = p_i(0)$, D's secret s (which is equal to $F(0,0)$) is d-shared using degree-d polynomial $f_0(x) = F(x, 0)$.

Protocol Gen-d-Share-SS($D, \mathcal{P}, s, d$)

<u>FOR $j = 1, \ldots, n$, P_j-PRIVATE-RECONSTRUCTION OF $p_j(0)$:</u> CODE FOR P_i:

1. If $P_i \in CORE$, participate in Rec-Private($CORE, t, p_j(0), P_j$) for P_j-Private-Reconstruction of $p_j(0)$, for $j = 1, \ldots, n$.
2. As a receiver, participate in Rec-Private($CORE, t, p_i(0), P_i$) for P_i-Private-Reconstruction of $p_i(0)$.
3. Output $f_0(i) = p_i(0)$ as the i^{th} share of secret s and terminate. s is now d-shared using polynomial $f_0(x)$.

5.4 Final Protocol for Generating d-sharing: Protocol d-Share-SS

Protocol d-Share-SS($D, \mathcal{P}, s, d$)

I. CODE FOR D:

1. Execute Distr-SS($D, \mathcal{P}, s, d$).

II. CODE FOR P_i:

1. Participate in Ver-Agree-on-CORE-SS($D, \mathcal{P}, s, d$).
2. Upon termination of Ver-Agree-on-CORE-SS($D, \mathcal{P}, s, d$), participate in Gen-d-Share-SS($D, \mathcal{P}, s, d$).

Lemma 8 *In protocol d-Share-SS, if D is honest, then every honest party will eventually terminate Ver-Agree-on-CORE-SS and Gen-d-Share-SS.*

PROOF: When D is honest, then eventually for every honest verifiers P_α, the set $AgreeSet^{P_\alpha}$ will contain all the honest parties in $\mathcal{P}$. Since there are at least $3t+1$ honest verifiers, $CORE$ will eventually contain all the honest parties in $\mathcal{P}$. Thus when D is honest, every honest party will eventually terminate Ver-Agree-on-CORE-SS. Moreover, each honest party in $CORE$ will hold correct points on degree-t column polynomials. The rest now follows from property (ii) of Theorem 2. □

Lemma 9 *In protocol d-Share-SS, if D is corrupted and some honest party has terminated Ver-Agree-on-CORE-SS, then all the honest parties will eventually terminate Ver-Agree-on-CORE-SS. Furthermore, if some honest party terminates Ver-Agree-on-CORE-SS, then every honest party will eventually terminate Gen-d-Share-SS, with very high probability.*

PROOF: If D is corrupted and some honest P_i has terminated Ver-Agree-on-CORE-SS, then he must have checked the validity of $CORE$ received from the A-cast of D. In the same way, every other honest P_j will check the validity of $CORE$ and terminate Ver-Agree-on-CORE-SS. This proves the first part. Once all the honest parties terminate Ver-Agree-on-CORE-SS, they will agree on $CORE$ of size $3t+1$. Moreover, with very high probability, the honest parties in $CORE$ will hold correct points on degree-t column polynomials. The rest now follows from property (iii) of Theorem 2. □

Theorem 3 *The protocol d-Share-SS satisfies* TERMINATION*,* CORRECTNESS *and* SECRECY *conditions of Property 1, with respect to a single secret. The protocol privately communicates $\mathcal{O}(n^3\log(|\mathbb{F}|))$ bits and A-Cast $\mathcal{O}(n^3\kappa)$ bits, where $\kappa = \log(|\mathbb{E}|)$.*

PROOF: TERMINATION: The proof follows from Lemma 8 and Lemma 9.

CORRECTNESS: Part (a) follows from the proof of Lemma 8 and Lemma 7. For part(b), if D is corrupted and the honest parties in $\mathcal{P}$ terminates d-Share-SS, then from Lemma 7, the row polynomials held by honest parties in $CORE$ define degree-t column polynomials, say $p_1(y),\ldots,p_n(y)$ with very high probability. Now by Theorem 2-(iii), P_i-Private-Reconstruction of $p_i(0)$ is possible for all $i=1,\ldots,n$ with very high probability. This implies every $P_i \in \mathcal{P}$ will compute $f_0(i) = p_i(0)$. So s will be d-shared among the parties in $\mathcal{P}$ using $f_0(x)$ with very high probability.

SECRECY: We have to consider the case when D is honest. By Lemma 4, the polynomials $E^{(P_\alpha,\beta)}$ A-casted in Ver-Agree-on-CORE are completely random to $\mathcal{A}_t$ and hence can be ignored. Without loss of generality, let $\mathcal{A}_t$ controls $P_1,\ldots,P_t$. So at the end of d-Share-SS, $\mathcal{A}_t$ will know $f_1(x),\ldots,f_t(x),p_1(y),\ldots,p_t(y)$. The bivariate polynomial $F(x,y)$ can be interpolated using $t+1$ $f_i(x)$'s or $d+1$ $p_i(y)$'s. $\mathcal{A}_t$ knows $f_1(x),\ldots,f_t(x)$ and t more points on each of $f_i(x)$ for $t+1 \le i \le n$ from $p_1(y),\ldots,p_t(y)$. But the t points on $f_{t+2}(x),\ldots,f_n(x)$ are linearly dependent on the t points on $f_1(x),\ldots,f_{t+1}(x)$. As $f_{t+1}(x)$ is a degree-d polynomial, $\mathcal{A}_t$ requires $d+1-t$ more points to completely interpolate $f_{t+1}(x)$. Thus $d+1-t$ coefficients of $F(x,y)$ (and hence $f_0(x)$) remain secure. Therefore $F(0,0) = f_0(0)$ is secure.

COMMUNICATION COMPLEXITY: In Distr-SS, D privately communicates $\mathcal{O}((nd+n^3)\log(\mathbb{F}))$ bits. Since $t \le d \le 2t$, $d = \mathcal{O}(n)$. In Ver-Agree-on-CORE-SS, the parties A-Cast $\mathcal{O}(n^3\log(|\mathbb{F}|)+n^2\kappa)$ bits. In Gen-d-Share-SS, the parties privately communicates $\mathcal{O}(n^2\log|\mathbb{F}|)$ bits. As $\log(|\mathbb{F}|) \le \kappa$, overall the protocol involves a private communication of $\mathcal{O}(n^3\log(\mathbb{F})$ bits and A-Cast of $\mathcal{O}(n^3\kappa)$ bits. □

We now give the details of protocol d-Share-MS, that allows a dealer $D \in \mathcal{P}$ to concurrently generate d-sharing of $\ell \ge 1$ secrets from $\mathbb{F}$, denoted as $S = (s^1,\ldots,s^\ell)$. We need to extend protocol Distr-SS, Single-Verifier-SS, Ver-Agree-on-CORE-SS, and Gen-d-Share-SS for multiple (ℓ) secrets. We refer them as Distr-MS, Single-Verifier-MS, Ver-Agree-on-CORE-MS and Gen-d-Share-MS. We present the protocols in **APPENDIX D**. The proofs for the properties of the protocols dealing with multiple secrets will be similar to the proofs of the protocols dealing with single secret. We now have the following theorem, whose proof is given in **APPENDIX D**, due to space constraints.

Theorem 4 *Protocol d-Share-MS satisfies* TERMINATION*,* CORRECTNESS *and* SECRECY *condition of Property 1. The protocol privately communicates $\mathcal{O}((\ell n^2+n^3)\log|\mathbb{F}|)$ bits and A-cast $\mathcal{O}(n^3\kappa)$ bits.*

Remark 1 (Advantage of Concurrently Sharing Multiple Secrets) *Note that, had we executed ℓ times the protocol* d-Share-SS *for single secret, the communication complexity would turn out to be $\mathcal{O}(\ell n^3 \log|\mathbb{F}|)$ bits of private communication plus $\mathcal{O}(\ell n^3 \kappa)$ bits of* A-cast*. However, the communication complexity of* d-Share-MS *treating all the ℓ secrets simultaneously is $\mathcal{O}((\ell n^2 + n^3)\log|\mathbb{F}|)$ bits of private communication and $\mathcal{O}(n^3\kappa)$ bits of* A-cast*. This shows that executing a single instance of* d-Share-MS *dealing with multiple secrets concurrently is advantageous over executing multiple instances of* d-Share-SS *dealing with single secret. The same principle holds for other primitives described in the sequel.*

6 Generating $(t, 2t)$-Sharing

We now present a novel protocol, called (t,2t)-Share-MS that allows a dealer $D \in \mathcal{P}$ (dealer can be any party from $\mathcal{P}$) to concurrently generate $(t, 2t)$-sharing of $\ell \geq 1$ secrets from $\mathbb{F}$. The idea is as follows: D, on having ℓ secrets $S = (s^1, \ldots, s^\ell)$, invokes two instances of d-Share-MS, to t-share and $2t$-share S respectively. For an honest D, this is enough to generate $(t, 2t)$-sharing of S. But a corrupted D may t-share $\widehat{S} = (\widehat{s^1}, \ldots, \widehat{s^\ell})$ and $2t$-share $\overline{S} = (\overline{s^1}, \ldots, \overline{s^\ell})$ where $\widehat{S} \neq \overline{S}$. To verify whether $\widehat{S} = \overline{S}$, each $d^l = \widehat{s^l} - \overline{s^l}$, for $l = 1, \ldots, \ell$, is P_i-Private-Reconstructed for every P_i. P_i then check whether $d^l = 0$ for $l = 1, \ldots, \ell$ and in case if all the d^l values are 0, every P_i knows that S is correctly $(t, 2t)$-shared. We now prove the properties of (t,2t)-Share-MS.

Theorem 5 *Protocol (t,2t)-Share-MS achieves the following properties:*

1. Termination: *(a) If D is honest, then every honest party will eventually terminate (t,2t)-Share-MS. (b) If D is corrupted and some honest party terminates (t,2t)-Share-MS, then all the honest parties will also terminate the protocol, except with probability $2^{-\Omega(\kappa)}$.*
2. Correctness: *(a) If D is honest, then all the ℓ secrets are correctly $(t, 2t)$-shared among the parties in $\mathcal{P}$. (b) If D is corrupted and the honest parties terminate (t,2t)-Share-MS, then there are ℓ secrets, that are correctly $(t, 2t)$-shared among the parties in $\mathcal{P}$, except with probability $2^{-\Omega(\kappa)}$.*
3. Secrecy: *$\mathcal{A}_t$ will have no information about the secrets of an honest D.*
4. Communication Complexity: *The protocol privately communicates $\mathcal{O}((\ell n^2 + n^3)\log|\mathbb{F}|)$ bits and A-cast $\mathcal{O}(n^3\kappa)$ bits.*

Proof: Follows from the properties of d-Share-MS. The complete proof is given in **APPENDIX E**. □

Protocol (t,2t)-Share-MS($D, \mathcal{P}, S = (s^1, \ldots, s^\ell)$)

Code for D:

1. Invoke d-Share-MS($D, \mathcal{P}, \widehat{S} = (\widehat{s^1}, \ldots, \widehat{s^\ell}), t$) and d-Share-MS($D, \mathcal{P}, \overline{S} = (\overline{s^1}, \ldots, \overline{s^\ell}), 2t$), such that $\widehat{S} = \overline{S}$.

Code for P_i:

1. Participate in d-Share-MS($D, \mathcal{P}, \widehat{S}, t$) and d-Share-MS($D, \mathcal{P}, \overline{S}, 2t$).
2. Wait until both d-Share-MS($D, \mathcal{P}, \widehat{S}, t$) and d-Share-MS($D, \mathcal{P}, \overline{S}, 2t$) terminate. Participate in Rec-Private($\mathcal{P}, 2t, \widehat{s^l} - \overline{s^l}, P_j$) for P_j-Private-Reconstruction of $\widehat{s^l} - \overline{s^l}$ for $j = 1, \ldots, n$ and $l = 1, \ldots, \ell$.
3. As a receiver participate in Rec-Private($\mathcal{P}, 2t, \widehat{s^l} - \overline{s^l}, P_i$) for P_i-Private-Reconstruction of $\widehat{s^l} - \overline{s^l}$, for $l = 1, \ldots, \ell$.
4. If $\widehat{s^l} - \overline{s^l} = 0$ for all $l = 1, \ldots, \ell$, then output φ_i^l and χ_i^l, where φ_i^l and χ_i^l are the i^{th} shares of secret s^l, obtained during d-Share-MS($D, \mathcal{P}, \widehat{S}, t$) and d-Share-MS($D, \mathcal{P}, \overline{S}, 2t$) respectively and terminate.

Protocol (t,2t)-Share-MS is to be compared with the best known asynchronous protocol of [4] that requires a private communication of $\mathcal{O}(n^3 \log|\mathbb{F}|)$ bits and A-Cast of $\mathcal{O}(n^2 \log(|\mathbb{F}|))$ bits to generate $(t, 2t)$-sharing of a *single* secret. This shows that (t,2t)-Share-MS provides better complexity than the protocol of [4] (though, the protocol of [4] does not involve any error probability in correctness and termination). A brief account on the existing protocols for generating $(t, 2t)$-sharing is presented in **APPENDIX B**.

7 Preparation Phase

The goal of the preparation phase is to generate correct $(t, 2t)$-sharing of $c_M + c_R$ *secret* random values. We now present a protocol called PreparationPhase which achieves the same.

Protocol PreparationPhase($\mathcal{P}$)

SECRET SHARING: CODE FOR P_i:

1. Select $L = \frac{c_M+c_R}{n-2t}$ random secret elements $(s^{(i,1)},\ldots,s^{(i,L)})$ from $\mathbb{F}$. As a dealer, invoke **(t, 2t)-Share-MS($P_i, \mathcal{P}, S^i$)** to generate $(t,2t)$-sharing of $S^i = (s^{(i,1)},\ldots,s^{(i,L)})$.
2. For $j = 1,\ldots,n$, participate in **(t, 2t)-Share-MS($P_j, \mathcal{P}, S^j$)**.

AGREEMENT ON A CORE-SET: CODE FOR P_i

1. Create an accumulative set $C^i = \emptyset$. Upon terminating **(t,2t)-Share-MS($P_j, \mathcal{P}, S^j$)**, include P_j in C^i.
2. Take part in ACS with the accumulative set C^i as input.

GENERATION OF RANDOM $(t,2t)$-SHARING: CODE FOR P_i:

1. Wait until ACS completes with output C containing $n-t$ parties. Obtain the i^{th} shares $\varphi_i^{(j,1)},\ldots,\varphi_i^{(j,L)}$ corresponding to t-sharing of S^j and i^{th} shares $\phi_i^{(j,1)},\ldots,\phi_i^{(j,L)}$ corresponding to $2t$-sharing of S^j for every $P_j \in C$. Without loss of generality, let $C = \{P_1,\ldots,P_{n-t}\}$.
2. Let V denote a $(n-t)\times(n-2t)$ publicly known *Vandermonde Matrix*.
   (a) For every $k \in \{1,\ldots,L\}$, let $(r^{(1,k)},\ldots,r^{(n-2t,k)}) = (s^{(1,k)},\ldots,s^{(n-t,k)})V$.
   (b) Locally compute i^{th} shares corresponding to t-sharing of $r^{(1,k)},\ldots,r^{(n-2t,k)}$ as $(\varsigma_i^{(1,k)},\ldots,\varsigma_i^{(n-2t,k)}) = (\varphi_i^{(1,k)},\ldots,\varphi_i^{(n-t,k)})V$.
   (c) Locally compute i^{th} shares corresponding to $2t$-sharing of $r^{(1,k)},\ldots,r^{(n-2t,k)}$ as $(\sigma_i^{(1,k)},\ldots,\sigma_i^{(n-2t,k)}) = (\phi_i^{(1,k)},\ldots,\phi_i^{(n-t,k)})V$ and terminate.

The values $r^{(1,1)},\ldots,r^{(n-2t,1)},\ldots,r^{(1,L)},\ldots,r^{(n-2t,L)}$ denotes the c_M+c_R random secrets which are $(t,2t)$-shared.

PreparationPhase asks individual party to act as a dealer and $(t,2t)$-share $\frac{c_M+c_R}{n-2t}$ random secrets. Then an instance of ACS protocol is executed to agree on a core set of $n-t$ parties who have correctly $(t,2t)$-shared $\frac{c_M+c_R}{n-2t}$ random secrets. Now out of these $n-t$ parties, at least $n-2t$ are honest. Hence the random secrets that are $(t,2t)$-shared by these $n-2t$ honest parties are truly random and unknown to $\mathcal{A}_t$. So if we consider the $(t,2t)$-sharing done by the honest parties (each of them has done $\frac{c_M+c_R}{n-2t}$ $(t,2t)$-sharing) in core set, then we will get $\frac{c_M+c_R}{n-2t}*(n-2t) = c_M+c_R$ random $(t,2t)$-sharing. For this, we use *Vandermonde Matrix* [17] and its ability to extract randomness which has been exploited in [35, 17, 4].

Vandermonde Matrix and Randomness Extraction [17]: Let $\beta_1,\ldots,\beta_c$ be distinct and publicly known elements from $\mathbb{F}$. We denote an $(r\times c)$ Vandermonde matrix by $V^{(r,c)}$, where for $1\le i\le c$, the i^{th} column of $V^{(r,c)}$ is $(\beta_i^0,\ldots,\beta_i^{r-1})^T$. The idea behind extracting randomness using $V^{(r,c)}$ is as follows: without loss of generality, assume that $r > c$. Moreover, let $(x_1,\ldots,x_r)$ be such that (a) *any* c elements of it are chosen uniformly at random from $\mathbb{F}$ and are unknown to adversary $\mathcal{A}_t$, (b) the remaining $r-c$ elements are chosen with an arbitrary distribution from $\mathbb{F}$, independent of the c elements, and are also known to $\mathcal{A}_t$. Now if we compute $(y_1,\ldots,y_c) = (x_1,\ldots,x_r)V$, then $(y_1,\ldots,y_c)$ is an random vector of length c unknown to $\mathcal{A}_t$, extracted from $(x_1,\ldots,x_r)$ [35, 17, 4].

Lemma 10 *Each honest party will eventually terminate PreparationPhase, except with probability $2^{-\Omega(\kappa)}$. The protocol correctly generates $(t,2t)$-sharing of c_M+c_R secret random values, except with error probability of $2^{-\Omega(\kappa)}$ by privately communicating $O(((c_M+c_R)n^2+n^4)\log|\mathbb{F}|)$ bits, A-Casting $\mathcal{O}(n^4\kappa)$ bits and executing one invocation to ACS. Moreover, $\mathcal{A}_t$ will have no information about the random values.*

PROOF: Easy. For complete proof, see **APPENDIX F**. □

8 Input Phase

In protocol InputPhase, each $P_i \in \mathcal{P}$ acts as a dealer to t-share his input X_i containing c_i elements from $\mathbb{F}$. So total number of inputs $c_I = \sum_{i=1}^n c_i$. To achieve this, party P_i t-share his input X_i by acting as a dealer and executing d-Share-MS. The asynchrony of the network does not allow the parties to wait for more than $n-t = 3t+1$ parties to complete their instance of d-Share-MS. In order to agree on a core set of parties whose instance of d-Share-MS have terminated and whose inputs will be taken into consideration for computation (of the circuit), one instance of ACS is invoked. At the end, everyone considers the t-sharing of all the inputs shared by parties, only in the core set. As the protocol is very straight forward, we present it in **APPENDIX F**.

Lemma 11 *Each honest party will eventually terminate InputPhase and will correctly output t-sharing of the inputs of the parties in core set C with high probability. The protocol privately communicates*

$O((c_I n^2 + n^4)\log|\mathbb{F}|)$ *bits, A-Casts* $\mathcal{O}(n^4\kappa)$ *bits and requires one invocation to ACS. Furthermore,* $\mathcal{A}_t$ *will have no information about the inputs of the honest parties in* C.

9 Computation Phase

Once the input phase is over, in the computation phase, the circuit is evaluated gate by gate, where all inputs and intermediate values are t-shared among the parties. As soon as a party holds his shares of the input values of a gate, he joins the computation of the gate.

Due to the linearity of the t-sharing, linear gates can be computed locally, simply by applying the linear function to the shares, i.e. for any linear function $c = f(a, b)$, the sharing $[c]_t$ is computed by letting every party P_i to compute $c_i = f(a_i, b_i)$, where a_i, b_i and c_i are the i^{th} shares of a, b and c respectively. With every random gate, one random $(t, 2t)$-sharing (from the preparation phase) is associated, whose t-sharing is directly used as outcome of the random gate. With every multiplication gate, one random $(t, 2t)$-sharing (from the preparation phase) is associated, which is then used to compute t-sharing of the product, following the technique of Damgard et. al. [17] in synchronous settings, which is as follows: Let $z = xy$, where x, y are the inputs of the multiplication gate, where x, y are t-shared, i.e. $[x]_t, [y]_t$. Moreover, let $[r]_{(t,2t)}$ be the $(t, 2t)$-sharing associated with the multiplication gate, where r is a secret random value. Now for computing $[z]_t$, the t-sharing of z, the parties compute $[\Lambda]_{2t} = [x]_t.[y]_t + [r]_{2t}$. Then Λ is P_i-Private-Reconstructed for every $P_i \in \mathcal{P}$. Now every party defines $[\Lambda]_t$ as the default sharing of Λ, e.g., the constant degree-0 polynomial Λ and computes $[z]_t = [\Lambda]_t - [r]_t$. The secrecy of z follows from the fact that r is random and independent of x and y [17, 4]. As the protocol for **Computation Phase** is very straight forward, we present it in **APPENDIX F**.

Lemma 12 *Each honest party will eventually terminate ComputationPhase with very high probability. Given* $(t, 2t)$*-sharing of* $c_M + c_R$ *secret random values, the protocol computes the outputs of the circuit securely by privately communicating* $O(n^2(c_M + c_O)\log|\mathbb{F}|)$ *bits. The outputs of the circuit will be correct except with probability* $2^{-\Omega(\kappa)}$

10 The AMPC Protocol

Now our new AMPC protocol AMPC for evaluating function f is: (1). Invoke PreparationPhase (2). Invoke InputPhase (3). Invoke ComputationPhase.

Theorem 6 *For every coalition of up to* $t < n/4$ *corrupted parties, the protocol AMPC securely computes the circuit representing function* f*, satisfying (i)* Termination: *Except with probability* $2^{-\Omega(\kappa)}$*, each honest party will terminate the protocol; (ii)* Correctness: *The protocol correctly computes the circuit except with error probability of* $2^{-\Omega(\kappa)}$. *The protocol privately communicates* $\mathcal{O}(((c_I + c_M + c_R + c_O)n^2 + n^4)\log|\mathbb{F}|)$ *bits, A-Casts* $\mathcal{O}(n^4\kappa)$ *bits and requires 2 invocations to ACS.*

11 Open Problems

It would be interesting to see whether it is possible to further reduce the communication complexity of AMPC protocol with $n = 4t+1$ by using techniques such as player elimination [21]. Our AMPC protocol have a negligible probability of non-termination and negligible probability of error in correctness. It is an interesting and challenging problem to design an AMPC protocol with $n = 4t+1$ that is perfect (errorless) in all respects, namely termination, secrecy and correctness while maintaining quadratic communication complexity per multiplication gate.

References

[1] D. Beaver. Efficient multiparty protocols using circuit randomization. In *Proc. of CRYPTO 1991*, volume 576 of *LNCS*, pages 420–432. Springer Verlag, 1991.

[2] Z. Beerliová-Trubíniová, M. Fitzi, M. Hirt, U. M. Maurer, and V. Zikas. MPC vs. SFE: Perfect security in a unified corruption model. In *TCC*, pages 231–250, 2008.

[3] Z. Beerliová-Trubíniová and M. Hirt. Efficient multi-party computation with dispute control. In *Proc. of TCC*, pages 305–328, 2006.

[4] Z. Beerliová-Trubíniová and M. Hirt. Simple and efficient perfectly-secure asynchronous MPC. In *ASIACRYPT*, pages 376–392, 2007.

[5] Z. Beerliová-Trubíniová and M. Hirt. Perfectly-secure MPC with linear communication complexity. In *Proc. of TCC 2008*, volume 4948 of *LNCS*, pages 213–230. Springer Verlag, 2008.

[6] M. Ben-Or, R. Canetti, and O. Goldreich. Asynchronous secure computation. In *STOC*, pages 52–61, 1993.

[7] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proc. of 20th ACM STOC*, pages 1–10, 1988.

[8] M. BenOr, B. Kelmer, and T. Rabin. Asynchronous secure computations with optimal resilience. In *PODC*, pages 183–192, 1994.

[9] G. Bracha. An asynchronous $\lfloor (n-1)/3 \rfloor$-resilient consensus protocol. In 3^{rd} *ACM PODC*, pages 154 – 162, 1984.

[10] C. Cachin, K. Kursawe, A. Lysyanskaya, and R. Strobl. Asynchronous verifiable secret sharing and proactive cryptosystems. In *ACM Conference on Computer and Communications Security*, pages 88–97, 2002.

[11] R. Canetti. *Studies in Secure Multiparty Computation and Applications*. PhD thesis, Weizmann Institute, Israel, 1995.

[12] R. Canetti and T. Rabin. Fast asynchronous Byzantine agreement with optimal resilience. In *Proc. of STOC 1993*, pages 42–51. ACM, 1993.

[13] D. Chaum, C. Crpeau, and I. Damgård. Multiparty unconditionally secure protocols (extended abstract). In *Proc. of FOCS 1988*, pages 11–19, 1988.

[14] R. Cramer, I. Damgård, S. Dziembowski, M. Hirt, and T. Rabin. Efficient multiparty computations secure against an adaptive adversary. In *Proc. of EUROCRYPT 1999*, volume 1592 of *LNCS*, pages 311–326. Springer Verlag, 1999.

[15] R. Cramer, I. Damgård, and S. Fehr. On the cost of reconstructing a secret, or VSS with optimal reconstruction phase. In *CRYPTO*, pages 503–523, 2001.

[16] R. Cramer, I. Damgård, and U. M. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In *EUROCRYPT*, pages 316–334, 2000.

[17] I. Damgård and J. B. Nielsen. Scalable and unconditionally secure multiparty computation. In *Proc. of CRYPTO*, volume 4622 of *LNCS*, pages 572–590. Springer Verlag, 2007.

[18] I. Damgrd, M. Geisler, M. Krigaard, and J. Buus Nielsen. Asynchronous multiparty computation: Theory and implementation. Cryptology ePrint Archive, Report 2008/415, 2008.

[19] R. Gennaro, M. O. Rabin, and T. Rabin. Simplified VSS and fact-track multiparty computations with applications to threshold cryptography. In *PODC*, pages 101–111, 1998.

[20] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *Proc. of 19th ACM STOC*, pages 218–229, 1987.

[21] M. Hirt, U. Maurer, and B. Przydatek. Efficient secure multiparty computation. In *Proc. of ASIACRYPT 2000*, volume 1976 of *LNCS*, pages 143–161. Springer Verlag, 2000.

[22] M. Hirt and U. M. Maurer. Complete characterization of adversaries tolerable in secure multi-party computation. In *PODC*, pages 25–34, 1997.

[23] M. Hirt, U. M. Maurer, and V. Zikas. MPC vs. SFE : Unconditional and computational security. In *ASIACRYPT*, pages 1–18, 2008.

[24] M. Hirt, J. B Nielsen, and B. Przydatek. Cryptographic asynchronous multi-party computation with optimal resilience (extended abstract). In *EUROCRYPT*, pages 322–340, 2005.

[25] M. Hirt, J. B Nielsen, and B. Przydatek. Asynchronous multi-party computation with quadratic communication. In *ICALP (2)*, pages 473–485, 2008.

[26] J. Katz and C. Y. Koo. Round-efficient secure computation in point-to-point networks. In *Proc. of EUROCRYPT 2007*, volume 4515 of *LNCS*, pages 311–328. Springer Verlag, 2007.

[27] M. V. N. Ashwin Kumar, K. Srinathan, and C. Pandu Rangan. Asynchronous perfectly secure computation tolerating generalized adversaries. In *ACISP*, pages 497–512, 2002.

[28] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error Correcting Codes*. North-Holland Publishing Company, 1978.

[29] R. Ostrovsky and M. Yung. How to withstand mobile virus attacks. In *Proc. of 10th PODC*, pages 51–61. ACM Press, 1991.

[30] A. Patra, A. Choudhary, and C. Pandu Rangan. Efficient asynchronous multiparty computation with optimal resilience. Cryptology ePrint Archive, Report 2008/425, 2008.

[31] A. Patra, A. Choudhary, and C. Pandu Rangan. Round efficient unconditionally secure multiparty computation protocol. In *INDOCRYPT*, pages 185–199, 2008.

[32] B. Prabhu, K. Srinathan, and C. Pandu Rangan. Trading players for efficiency in unconditional multiparty computation. In *SCN*, pages 342–353, 2002.

[33] T. Rabin. Robust sharing of secrets when the dealer is honest or cheating. *J. ACM*, 41(6):1089–1109, 1994.

[34] Tal Rabin and Michael Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority (extended abstract). In *STOC*, pages 73–85, 1989.

[35] K. Srinathan, A. Narayanan, and C. Pandu Rangan. Optimal perfectly secure message transmission. In *Proc. of Advances in Cryptology: CRYPTO 2004*, pages 545–561, 2004.

[36] K. Srinathan and C. Pandu Rangan. Efficient asynchronous secure multiparty distributed computation. In *INDOCRYPT*, pages 117–129, 2000.

[37] A. C. Yao. Protocols for secure computations. In *Proc. of 23rd IEEE FOCS*, pages 160–164, 1982.

[38] Jesper Buus Nielsen Zuzana Beerliova-Trubiniova, Martin Hirt. Almost-asynchronous MPC with faulty minority. Cryptology ePrint Archive, Report 2008/416, 2008.

APPENDIX A: Online Error Correction and Properties of Protocol Rec-Private

The current description of OEC is taken from [11]. Consider the following scenario: Let s be a secret, which is d-shared among the n parties in $\mathcal{P}$, by a degree-d polynomial $f(x)$, where $d < n - 2t$. Thus, each honest party P_i has the share $s_i = f(i)$. Let $P_\alpha \in \mathcal{P}$ be a specific party in $\mathcal{P}$, which we call as *receiver*. P_α wants to reconstruct the polynomial $f(x)$ and get $s = F(0)$. For this, he expects the honest parties, to send their shares of s to him. Due to asynchronity of the network, the shares may arrive in any arbitrary order. Moreover, t of the shares may be wrong or missing. In such a scenario, *online error correction* (OEC) [11] allows P_α to recover $f(x)$ from the received shares in an *online* fashion. Informally, the procedure allows P_α to identify, when the received shares define a unique degree-d polynomial.

Before describing OEC, we recall the definition of *generalized Reed-Solomon* (GRS) code [28]. Consider the following code over $\mathbb{F}$: A word $W = \{(i_1, a_1), \ldots, (i_l, a_l)\}$ over $\mathbb{F}$ is a codeword iff there exists a degree-d polynomial $F(x)$ over $\mathbb{F}$, such that $F(i_j) = a_j$, for $j = 1, \ldots, l$. This code is called GRS code. GRS codes have an efficient error correcting procedure, which can correct r errors in an input word $\overline{W}$, provided that $|\overline{W}| \geq d + 2r + 1$ (see [28]). Let EC be such a procedure.

We now describe the procedure for OEC, using the above notions of GRS codes. Informally, the procedure will run for at most $t+1$ iterations. In r^{th} iteration, P_α will wait to receive shares of s from $d+t+r+1$ parties. P_α will now assume that at most r shares are corrupted in the received shares and try to correct them using procedure EC. Now there are two possible cases:

1. **There are at most r corrupted shares in the received set of shares**. So in this case, EC will correctly output the original degree-d polynomial $f(x)$ and hence s by correcting at most r corrupted shares present in the received set of shares. P_α can check the validity of output polynomial $f(x)$ by verifying that at least $d+t+1$ received shares (other than the wrong shares that are corrected by EC) lie on $f(x)$. Finally, in this case, P_α terminates the OEC procedure.

2. **There are more than r corrupted shares in the received shares**. In this case, EC may either fail to output any degree-d polynomial or may output an incorrect degree-d polynomial, say $f'(x)$. In the former case, P_α can easily identify that more than r shares are corrupted in the received set of shares. However, even in the later case, P_α will identify that more than r shares are corrupted in the received set of shares. This is because $d+t+1$ received shares (other than the ones which are corrected by EC) will not lie on $f'(x)$. Thus P_α will know that more honest shares will eventually come from the honest parties and hence proceed to the next iteration.

The protocol is formally given in the following table:

Protocol OEC

For $0 \leq r \leq t$, in iteration r, P_α does the following:

1. Let $\mathcal{W}$ denote the set of shares received by P_α and I_r denote the received shares in $\mathcal{W}$, when $\mathcal{W}$ contains $d+t+r+1$ shares.
2. Wait until $|\mathcal{W}| \geq d+t+r+1$. Then apply EC to I_r to get the polynomial $\overline{f(x)}$ of degree d. If no polynomial is output, then skip the next step and proceed to next iteration.
3. If at least $d+t+1$ shares in I_r (other than the ones which are corrected by EC) lie on $\overline{f(x)}$, then output $\overline{s} = \overline{f(0)}$ as the secret and terminate. Otherwise, proceed to the next iteration.

Theorem 7 ([11]) *In protocol OEC, if s is correctly d-shared among a set of n parties, where $d < n-2t$, then P_α will eventually output s without any error.*

PROOF: Suppose $\mathcal{A}_t$ corrupts $\hat{r} \leq t$ shares of s, during their transmission to P_α. Since $d < n-2t$, during $\hat{r}^{th}$ iteration, P_α will receive $d+t+\hat{r}+1$ shares of s, of which at most $\hat{r}$ are corrupted. So from the properties of GRS codes [28] (as mentioned above), EC will correct $\hat{r}$ errors in the received set of shares and will output $\overline{f(x)}$ of degree d. Moreover, $d+t+1$ shares in I_r (other than the ones which are corrected by EC) will lie on $\overline{f(x)}$. Since out of these $d+t+1$ shares, at least $d+1$ are honest and uniquely define the original polynomial $f(x)$ ($d+1$ honest shares are $d+1$ correct points on a degree-d polynomial and hence uniquely define a degree-d polynomial), the output polynomial $\overline{f(x)}$ is same as $f(x)$. Thus $f(x)$ will be the output in $\hat{r}^{th}$ iteration. □

Theorem 8 *In protocol OEC, if s is not d-shared among the parties in $\mathcal{P}$, then any of the following events may happen:*

1. *P_α may output an incorrect degree-d polynomial.*
2. *P_α may be waiting indefinitely and may not terminate.*

PROOF: The first case may occur if s is d'-shared among the parties in $\mathcal{P}$, where $d' > d$. On the other hand, second case may occur if the shares of the honest parties in $\mathcal{P}$ do not lie on a degree-d polynomial and t corrupted parties do not send their shares to P_α. □

Theorem 2: (i) Protocol Rec-Private can be used to reconstruct $2t$-sharing of s which is shared among the parties in $\mathcal{P}$, where $|\mathcal{P}| = 4t+1$.

(ii) If $\overline{\mathcal{P}}$ is any $3t+1$ sized subset of $\mathcal{P}$, such that s is t-shared among the parties in $\overline{\mathcal{P}}$, then $\mathsf{Rec\text{-}Private}(\overline{\mathcal{P}}, t, s, P_\alpha)$ ensures successful P_α-Private-Reconstruction of s.

(iii) Let s be correctly d-shared among a set of n parties, except with probability $2^{-\Omega(\kappa)}$, where $d < n-2t$. Then Rec-Private satisfies the TERMINATION and CORRECTNESS properties mentioned in Theorem 1, except with probability $2^{-\Omega(\kappa)}$.

PROOF: Part (i) and (ii) follows from Theorem 7. Part (iii) follows from Theorem 8 and Theorem 7. □.

APPENDIX B: Existing Protocols for Generating $(t, 2t)$-sharing

In [17], Damgard et. al. have proposed a protocol that generates $(t, 2t)$-sharing of ℓ secrets concurrently in *synchronous settings* with $n = 3t+1$ parties, *conditioned on the event that all the parties correctly follow the protocol steps*; i.e., behave honestly. If at least one party behaves in a corrupted manner, then the protocol of [17] fails to generate the $(t, 2t)$-sharing and terminates with a pair of parties, in which at least one is corrupted. By allowing such susceptibility to the bad behavior of the corrupted parties, their protocol involves a communication complexity of $\mathcal{O}(\ell n \log|\mathbb{F}| + poly(n, \kappa))$ bits, where κ is the error probability of the protocol. The protocol of [17] cannot be directly adapted to asynchronous settings.

Later in [4], the authors have generated $(t, 2t)$-sharing of a single secret in *asynchronous settings* from t-sharing of $3t+1$ random values in asynchronous settings. Briefly, the authors have done the following: Let $[r^0]_t, \ldots, [r^{3t}]_t$ be the t-sharing of $3t+1$ random values. Let $p(x)$ be the t-degree polynomial defined by the $t+1$ coefficients $r^0, \ldots, r^t$. Let $q(x)$ be the $2t$-degree polynomial defined by the $2t+1$ coefficients $r^0, r^{t+1} \ldots, r^{3t}$. It is to be noted that both $p(x)$ and $q(x)$ have common constant term (which is r^0). Now the parties jointly perform some computation such that every party P_i receives $p(i)$ and $q(i)$ at the end. This ensures that r^0 is $(t, 2t)$-shared among the parties. To generate t-sharing of $3t+1$ random values, the authors in [4] have used a protocol, which involves a private communication of $\mathcal{O}(n^3 \log|\mathbb{F}|)$ bits and A-Cast of $\mathcal{O}(n^2 \log(|\mathbb{F}|))$ bits. Thus the protocol of [4] requires a private communication of $\mathcal{O}(n^3 \log|\mathbb{F}|)$ bits and A-Cast of $\mathcal{O}(n^2 \log(|\mathbb{F}|))$ bits to generate $(t, 2t)$ sharing of a *single* secret. The protocol of [4] does not involve any error probability in CORRECTNESS and TERMINATION.

APPENDIX C: Properties of Protocol d-Share-SS

Lemma 1: In protocol Single-Verifier-SS, if V is honest, then for all $j = 1, \ldots, n$, the j^{th} points on the row polynomials, held by the honest parties in $AgreeSet^{(V,\beta)}$ (with $|AgreeSet^{(V,\beta)}| \geq 3t+1$), define degree-$t$ column polynomial, with very high probability. Moreover, the points on blinding polynomial $b^{(V,\beta)}(y)$ held by the honest parties in $AgreeSet^{(V,\beta)}$ will lie on a degree-t polynomial with very high probability.

PROOF: The condition in the lemma will be true, without any error, when D is honest. Hence we consider the case when D is corrupted. Let $H^{(V,\beta)}$ denote the set of honest parties in $AgreeSet^{(V,\beta)}$. First of all, since V is honest, he A-casts random $r^{(V,\beta)}$ only after listening `Received-From-D` signal from all the parties in $ReceivedSet^{(V,\beta)}$. Thus D has no knowledge of $r^{(V,\beta)}$, when he distributes the row polynomials and points on blinding polynomial $b^{(V,\beta)}(y)$ to the (honest) parties in $ReceivedSet^{(V,\beta)}$. Let $\overline{b^{(V,\beta)}(y)}$ denote the *minimum degree* polynomial, defined by the points on $b^{(V,\beta)}(y)$, held by the honest parties in $H^{(V,\beta)}$. Similarly, let $\overline{p_1(y)}, \ldots, \overline{p_n(y)}$ denote the *minimum degree* polynomials, defined by the points on row polynomials, held by the parties in $H^{(V,\beta)}$. For convenience, we use an uniform notation for these $n+1$ polynomials. We denote them by $h^0(y), \ldots, h^n(y)$, respectively. Then the value $e_i^{(V,\beta)}$ A-casted by P_i is defined as $e_i^{(V,\beta)} = \sum_{j=0}^{n} \left(r^{(V,\beta)}\right)^j h^j(i)$.

We now claim that with very high probability, $h^0(y), \ldots, h^n(y)$ have degree-t. On the contrary, if we assume that at least one of the polynomials has degree more than t, then we can show that the minimum degree polynomial, say $h^{min}(y)$, defined by $e_i^{(V,\beta)}$'s for $P_i \in H^{(V,\beta)}$ will be of degree more than t, with very high probability. This will clearly imply $E^{(V,\beta)}(y) \neq h^{min}(y)$ and hence $e_i^{(V,\beta)} \neq E^{(V,\beta)}(i)$ for at least one $P_i \in H^{(V,\beta)}$. This is a contradiction as $e_i^{(V,\beta)} = E^{(V,\beta)}(i)$ holds for every $P_i \in Agree^{(V,\beta)}$ and $H^{(V,\beta)} \subseteq Agree^{(V,\beta)}$. This shows that our claim is true.

So we proceed to prove that $h^{min}(y)$ will be of degree more than t with very high probability, when one of $h^0(y), \ldots, h^n(y)$ has degree more than t. For this, we show the following:

1. We first show that $h^{def}(y) = \Sigma_{j=0}^{n} \left(r^{(V,\beta)}\right)^{j} h^{j}(y)$ will of degree more than t with very high probability, if one of $h^0(y), \ldots, h^n(y)$ has degree more than t.

2. We then show that $h^{min}(y) = h^{def}(y)$, implying that $h^{min}(y)$ will be of degree more than t with very high probability

To prove the first point, assume that at least one of $h^0(y), \ldots, h^n(y)$, has degree more than t. Let m be such that $h^m(y)$ has maximal degree among $h^0(y), \ldots, h^n(y)$, and let t_m be the degree of $h^m(y)$. Then according to the condition, $t_m > t$. Note that $t_m < |H^{(V,\beta)}|$. This is because given $|H^{(V,\beta)}|$ values (recall that $h^0(y), \ldots, h^n(y)$ are defined by the points on the row polynomials, held by the honest parties in $H^{(V,\beta)}$), the maximum degree polynomial that can be defined using them is $|H^{(V,\beta)}| - 1$. Now each polynomial $h^i(y)$ can be written as $h^i(y) = c^i_{t_m} y^{t_m} + \widehat{h^i(y)}$ where $\widehat{h^i(y)}$ has degree lower than t_m. Thus the polynomial $h^{def}(y)$ can be written as:

$$\begin{aligned} h^{def}(y) &= [c^0_{t_m} y^{t_m} + \widehat{h^0(y)}] + r^{(V,\beta)}[c^1_{t_m} y^{t_m} + \widehat{h^1(y)}] + \ldots + \left(r^{(V,\beta)}\right)^n [c^n_{t_m} y^{t_m} + \widehat{h^n(y)}] \\ &= y^{t_m}(c^0_{t_m} + \ldots + \left(r^{(V,\beta)}\right)^n c^n_{t_m}) + \Sigma_{j=0}^{n} \left(r^{(V,\beta)}\right)^j \widehat{h^j(y)} \\ &= y^{t_m} c_{t_m} + \Sigma_{j=0}^{n} \left(r^{(V,\beta)}\right)^j \widehat{h^j(y)} \end{aligned}$$

By assumption $c^m_{t_m} \neq 0$. It implies that the vector $(c^0_{t_m}, \ldots, c^n_{t_m})$ is not a complete 0 vector. Hence $c_{t_m} = c^0_{t_m} + \ldots + \left(r^{(V,\beta)}\right)^n c^n_{t_m}$ will be zero with probability $\frac{n}{|\mathbb{E}|-(\beta-1)} \approx 2^{-\Omega(\kappa)}$ (which is negligible), where $\beta \leq t+1$ (see Lemma 2). This is because the vector $(c^0_{t_m}, \ldots, c^n_{t_m})$ may be considered as the set of coefficients of a n degree polynomial, say $\mu(x)$, and hence the value c_{t_m} is the value of $\mu(x)$ evaluated at $r^{(V,\beta)}$. Now c_{t_m} will be zero if $r^{(V,\beta)}$ happens to be one of the n roots of $\mu(x)$ (since degree of $\mu(x)$ is at most n). Now since $r^{(V,\beta)}$ is chosen randomly from $\mathbb{E} \setminus \{r^{(V,1)}, \ldots, r^{(V,\beta-1)}\}$ by V, independent of the polynomials $h^0(y), \ldots, h^n(y)$, the probability that it is a root of $\mu(x)$ is $\frac{n}{|\mathbb{E}|-(\beta-1)} \approx 2^{-\Omega(\kappa)}$. So with very high probability c_{t_m}, which is the t_m^{th} coefficient of $h^{def}(y)$ is non-zero. This implies that $h^{def}(y)$ will be of degree at least $t_m > t$. Notice that each $e_i^{(V,\beta)}$ (A-casted by P_i), corresponding to every $P_i \in H^{(V,\beta)}$ will lie on $h^{def}(y)$.

Now we will show that $h^{min}(y) = h^{def}(y)$ and thus $h^{min}(y)$ has degree at least t_m which is greater than t. So consider the difference polynomial $dp(y) = h^{def}(y) - h^{min}(y)$. Clearly, $dp(y) = 0$, for all $y = i$, where $P_i \in H^{(V,\beta)}$. Thus $dp(y)$ will have at least $|H^{(V,\beta)}|$ roots. On the other hand, maximum degree of $dp(y)$ could be t_m, which is at most $|H^{(V,\beta)}| - 1$. These two facts together imply that $dp(y)$ is the zero polynomial, implying that $h^{def}(y) = h^{min}(y)$ and thus $h^{min}(y)$ has degree $t_m > t$. □

Lemma 2: *In Single-Verifier-SS, V will A-Cast $(r^{(V,\beta)}, ReceivedSet^{(V,\beta)})$ at most $t+1$ times. Hence the maximum value of β is $t+1$. Moreover, each $ReceivedSet^{(V,\beta)}$ will be unique. .*

Proof: First note that $ReceivedSet^{(V,1)} \geq 3t+1$. In the worst case $ReceivedSet^{(V,1)}$ may be exactly equal to $3t+1$ and potentially t honest parties may not be present in it. But for every β^{th} ($\beta > 1$) receipt of `Received-From-D` signal, from a new party $P_\alpha \notin ReceivedSet^{(V,\beta-1)}$, V will construct $ReceivedSet^{(V,\beta)} = ReceivedSet^{(V,\beta-1)} \cup \{P_\alpha\}$. Since $n = 4t+1$, V will A-Cast $(r^{(V,\beta)}, ReceivedSet^{(V,\beta)})$ at most $t+1$ times. Hence the maximum value of β can be $t+1$. The uniqueness of $ReceivedSet^{(V,\beta)}$'s follows from the fact that $ReceivedSet^{(V,\beta-1)} \subset ReceivedSet^{(V,\beta)}$. □

Lemma 7: *If D is honest, then the row polynomials held by honest parties in $CORE$ define degree-t column polynomials. If D is corrupted, then the same holds except with negligible error probability. Moreover there can not be another set $\overline{CORE}$ containing $3t+1$ parties such that the row polynomials held by honest parties in $\overline{CORE}$ define a different set of degree-t column polynomials..*

Proof: If D is honest then the lemma is trivially true. We now prove the lemma for the case of a corrupted D. By the construction of $CORE$, every party in $CORE$ is guaranteed to be present in *AgreeSet* of at least one honest verifier. By Lemma 5, corresponding to an honest verifier P_α, the row polynomials held by the honest parties in $AgreeSet^{P_\alpha}$ define t-degree column polynomials, say $p_1(y), \ldots, p_n(y)$, with very high probability. Moreover, by Lemma 6, the row polynomials held by the honest parties in the union of $AgreeSet^{P_\alpha}$'s, corresponding to all *honest* P_α's, also define $p_1(y), \ldots, p_n(y)$

with very high probability. This implies that the values held by the honest parties in $CORE$, define $p_1(y), \ldots, p_n(y)$.

Now we prove the second part of the lemma. Assume that there is another set, $\overline{CORE}$ containing $3t+1$ parties such that the row polynomials held by honest parties in $\overline{CORE}$ define a different set of degree-t column polynomials, say $\overline{p_1(y)}, \ldots, \overline{p_n(y)}$. Now since both $CORE$ and $\overline{CORE}$ are of size at least $3t+1$, they have $2t+1$ parties in common of which $t+1$ are honest. This implies that for $i = 1, \ldots, n$ polynomial $p_i(y)$ and $\overline{p_i(y)}$ has $t+1$ points in common. As both $p_i(y)$ and $\overline{p_i(y)}$ are of degree t, the above fact implies that $p_i(y) = \overline{p_i(y)}$. Hence $p_i(y) = \overline{p_i(y)}$ for $i = 1, \ldots, n$. Hence the lemma. □

APPENDIX D: Protocol d-Share-MS

Protocol Distr-MS$(D, \mathcal{P}, S = (s^1, \ldots, s^\ell), d)$

CODE FOR D:

1. Select ℓ random bivariate polynomials $F^1(x,y), \ldots, F^\ell(x,y)$ of degree d and t in x and y respectively, such that $F^l(0,0) = s^l$ for $l = 1, \ldots, \ell$. Let $f_i^l(x) = F^l(x,i)$, $p_i^l(y) = F^l(i,y)$ for $0 \leq i \leq n$ and $l = 1, \ldots, \ell$.
2. Select $(t+1)n$ degree-t, random, distinct *blinding polynomials* over $\mathbb{F}$, denoted by $b^{(P_j,1)}(y), \ldots, b^{(P_j,t+1)}(y)$ for $j = 1, \ldots, n$.
3. Send the following to party P_i: (i) $f_i^l(x)$ for $l = 1, \ldots, \ell$; (ii) $b^{(P_j,1)}(i), \ldots, b^{(P_j,t+1)}(i)$ for $j = 1, \ldots, n$.

Protocol Single-Verifier-MS$(V, \mathcal{P}, S, d)$

i. CODE FOR P_i:

1. Wait to receive (a) $f_i^l(x)$ for $l = 1, \ldots, \ell$ and (b) $b^{(P_j,1)}(i), \ldots, b^{(P_j,t+1)}(i)$ for $j = 1, \ldots, n$ from D.
2. After receiving, check whether $f_i^l(x)$ is a degree-d polynomial for all $l = 1, \ldots, \ell$. If yes, then send a `Received-From-D` signal to V.

ii. CODE FOR V:

1. Wait to obtain `Received-From-D` signal from at least $3t+1$ parties. Put the identities of the $3t+1$ parties in a set $ReceivedSet^{(V,1)}$. Select a random $r^{(V,1)} \in \mathbb{E}$ and A-cast $(r^{(V,1)}, ReceivedSet^{(V,1)})$.
2. For β^{th} ($\beta > 1$) receipt of `Received-From-D` signal from a new party $P_\alpha \notin ReceivedSet^{(V,\beta-1)}$, construct $ReceivedSet^{(V,\beta)} = ReceivedSet^{(V,\beta-1)} \cup \{P_\alpha\}$, select a random $r^{(V,\beta)} \in \mathbb{E} \setminus \{r^{(V,1)}, \ldots, r^{(V,\beta-1)}\}$ and A-cast $(r^{(V,\beta)}, ReceivedSet^{(V,\beta)})$.

iii. CODE FOR D:

1. If $(r^{(V,\beta)}, ReceivedSet^{(V,\beta)})$ is received from the A-cast of V, then A-cast the polynomial $E^{(V,\beta)}(y) = \mathsf{LinCombPoly}(\mathcal{E}, R)$. Here $\mathcal{E} = \{b^{(V,\beta)}(y), p_1^1(y), \ldots, p_n^1(y), \ldots, p_1^\ell(y), \ldots, p_n^\ell(y)\}$ and $R = (1, r^{(V,\beta)}, \left(r^{(V,\beta)}\right)^2, \ldots, \left(r^{(V,\beta)}\right)^{\ell n})$.

iv. CODE FOR P_i:

1. If $(r^{(V,\beta)}, ReceivedSet^{(V,\beta)})$ is received from the A-cast of V, then do the following:
   (a) Check if $P_i \in ReceivedSet^{(V,\beta)}$. If yes, then A-cast $e_i^{(V,\beta)} = \mathsf{LinCombValue}(\Delta_i, R)$, where $\Delta_i = \{b^{(V,\beta)}(i), f_i^1(1), \ldots, f_i^1(n), \ldots, f_i^\ell(1), \ldots, f_i^\ell(n)\}$ and $R = (1, r^{(V,\beta)}, \left(r^{(V,\beta)}\right)^2, \ldots, \left(r^{(V,\beta)}\right)^{\ell n})$.
2. Say that **party P_j agrees with D with respect to** $(r^{(V,\beta)}, ReceivedSet^{(V,\beta)})$ if all the following holds:
   (a) $E^{(V,\beta)}(y)$ is a degree-t polynomial, (b) $P_j \in ReceivedSet^{(V,\beta)}$ and (c) $e_j^{(V,\beta)} = E^{(V,\beta)}(j)$
   where $e_j^{(V,\beta)}$, $E^{(V,\beta)}(y)$ and $(r^{(V,\beta)}, ReceivedSet^{(V,\beta)})$ are received from the A-casts of P_j, D and V respectively.
3. With respect to $(r^{(V,\beta)}, ReceivedSet^{(V,\beta)})$, when there are $3t+1$ P_j's who agree with D, add all of them in a set $AgreeSet^{(V,\beta)}$.

Protocol Ver-Agree-on-CORE-MS$(D, \mathcal{P}, S, d)$

Here, in step i(1), P_i invokes Single-Verifier-MS$(P_\alpha, \mathcal{P}, S, d)$ instead of Single-Verifier-SS. The rest of the protocol is same as in Protocol Ver-Agree-on-CORE-SS.

Protocol Gen-d-Share-MS($D, \mathcal{P}, S = (s^1, \ldots, s^\ell), d$)

For $j = 1, \ldots, n$, P_j-Private-Reconstruction of $p_j^1(0), \ldots, p_j^\ell(0)$: Code for P_i:

1. If $P_i \in CORE$, participate in Rec-Private($CORE, t, p_j^l(0), P_j$) for P_j-Private-Reconstruction of $p_j^l(0)$ for $l = 1, \ldots, \ell$ and $j = 1, \ldots, n$.
2. As a receiver participate in Rec-Private($CORE, t, p_i^l(0), P_i$) for P_i-Private-Reconstruction of $p_i^l(0)$ for $l = 1, \ldots, \ell$.
3. Output $f_0^l(i) = p_i^l(0)$ as the i^{th} share of secret s^l and terminate. For $l = 1, \ldots, \ell$, s^l is now d-shared using polynomial $f_0^l(x)$.

Protocol d-Share-MS($D, \mathcal{P}, S = \{s^1, \ldots, s^\ell\}, d$)

i. Code for D:

1. Execute Distr-MS($D, \mathcal{P}, S, d$).

ii. Code for P_i:

1. Participate in Ver-Agree-on-CORE-MS($D, \mathcal{P}, S, d$).
2. Upon termination of Ver-Agree-on-CORE-MS($D, \mathcal{P}, S, d$), participate in Gen-d-Share-MS($D, \mathcal{P}, S, d$).

Theorem 4: *Protocol d-Share-MS satisfies* Termination, Correctness *and* Secrecy *conditions of Property 1. The protocol privately communicates $\mathcal{O}((\ell n^2 + n^3)\log|\mathbb{F}|)$ bits and A-cast $\mathcal{O}(n^3\kappa)$ bits.*

Proof: The proof of termination, correctness and secrecy follows using similar arguments as in Theorem 3. We now do the communication complexity analysis of d-Share-MS.

In Distr-MS, D privately communicates $\mathcal{O}((\ell nd + n^3)\log(\mathbb{F}))$ bits. Since $t \leq d \leq 2t$, $d = \mathcal{O}(n)$. In Ver-Agree-on-CORE-MS, the parties A-Cast $\mathcal{O}(n^3 \log(|\mathbb{F}|) + n^2\kappa)$ bits. In Gen-d-Share-MS, the parties privately communicates $\mathcal{O}(\ell n^2 \log|\mathbb{F}|)$ bits. As $\log(|\mathbb{F}|) \leq \kappa$, overall the protocol involves a private communication of $\mathcal{O}((\ell n^2 + n^3)\log|\mathbb{F}|)$ bits and A-cast $\mathcal{O}(n^3\kappa)$ bits. □

APPENDIX E: Properties of Protocol (t,2t)-Share-MS

Theorem 5: *Protocol (t,2t)-Share-MS achieves the following properties:*

1. Termination: *(a) If D is honest, then every honest party will eventually terminate (t,2t)-Share-MS. (b) If D is corrupted and some honest party terminates (t,2t)-Share-MS, then all the honest parties will also terminate the protocol, except with probability $2^{-\Omega(\kappa)}$.*
2. Correctness: *(a) If D is honest, then all the ℓ secrets are correctly $(t, 2t)$-shared among the parties in $\mathcal{P}$. (b) If D is corrupted and the honest parties terminate (t,2t)-Share-MS, then there are ℓ secrets, that are correctly $(t, 2t)$-shared among the parties in $\mathcal{P}$, except with probability $2^{-\Omega(\kappa)}$.*
3. Secrecy: *$\mathcal{A}_t$ will have no information about the secrets of an honest D.*
4. Communication Complexity: *The protocol privately communicates $\mathcal{O}((\ell n^2 + n^3)\log|\mathbb{F}|)$ bits and A-cast $\mathcal{O}(n^3\kappa)$ bits.*

Proof: The termination, correctness and communication complexity follows from Theorem 4. We now prove the secrecy property. We have to consider the case when D is honest. We show that the secrets $s^1, \ldots, s^\ell$ are information theoretically secure. The argument for the security of s^l is as follows. Let s^l be t-shared and $2t$-shared using polynomial $f_0^l(x)$ and $g_0^l(x)$ of degree t and $2t$ respectively. Then from the secrecy proof of Theorem 4 and Theorem 3, $\mathcal{A}_t$ will have no information about *one* and $t+1$ coefficients of $f_0^l(x)$ and $g_0^l(x)$ respectively. This is because $\mathcal{A}_t$ knows t distinct points on $g_0^l(x)$ and $f_0^1(x)$ during the execution of d-Share-MS. But, in (t,2t)-Share-MS, $\gamma^l(x) = g_0^l(x) - f_0^l(x)$ is privately reconstructed towards each party. By this $\mathcal{A}_t$ will know the higher order t coefficients of $g_0^l(x)$ as the higher order t coefficients of $\gamma^l(x)$ are same as the higher order t coefficients of $g_0^l(x)$. So, now $\mathcal{A}_t$ has no information about one coefficient of both $f_0^l(x)$ and $g_0^l(x)$, namely their constant terms. But notice that $\gamma^l(0) = g^l(0) - f^l(0) = 0$ for honest D. The remaining information that is obtained from $\gamma^l(x)$ is linearly dependent on the information that $\mathcal{A}_t$ possesses already. So s^l remains information theoretically secure. □

APPENDIX F: **Preparation Phase, Input Phase** and **Computation Phase**

lemma 10: *Each honest party will eventually terminate PreparationPhase, except with probability* $2^{-\Omega(\kappa)}$. *The protocol correctly generates* $(t, 2t)$*-sharing of* $c_M + c_R$ *secret random values, except with error probability of* $2^{-\Omega(\kappa)}$ *by privately communicating* $O(((c_M + c_R)n^2 + n^4) \log |\mathbb{F}|)$ *bits, A-Casting* $\mathcal{O}(n^4\kappa)$ *bits and executing one invocation to ACS. Moreover,* $\mathcal{A}_t$ *will have no information about the random values.*

PROOF: The termination and correctness property follow from the termination and correctness property of **(t,2t)-Share-MS**. The secrecy follows from the secrecy of **(t,2t)-Share-MS** and randomness extraction property of Vandermonde matrix [35, 17, 4]. We now prove the communication complexity. In the protocol, each party executes an instance of **(t,2t)-Share-MS**, by acting as a dealer, to $(t, 2t)$ share $L = \frac{c_M + c_R}{n-2t}$ secrets. So substituting $\ell = L$ in Theorem 5, the total private communication of the protocol is $\mathcal{O}\left(\left(Ln^3 + n^4\right) \log(|\mathbb{F}|)\right)$ bits. Since $L = \frac{c_M + c_R}{n-2t}$ and $n - 2t = \Theta(n)$, the total private communication of the protocol will be $O(((c_M + c_R)n^2 + n^4) \log |\mathbb{F}|)$ bits. Moreover, the protocol will A-Cast $\mathcal{O}(n^4\kappa)$ bits. □

Protocol InputPhase($\mathcal{P}$)

<u>SECRET SHARING:</u> CODE FOR P_i

1. Having input X_i, invoke **d-Share-MS(**$P_i, \mathcal{P}, X_i, t$**)**, as a dealer, to generate t-sharing of X_i.
2. For every $j = 1, \ldots, n$, participate in **d-Share-MS(**$P_j, \mathcal{P}, X_j, t$**)**.

<u>AGREEMENT ON A CORE-SET:</u> CODE FOR P_i

1. Create an accumulative set $C^i = \emptyset$. Upon terminating **d-Share-MS(**$P_j, \mathcal{P}, X_j, t$**)** with dealer P_j, add P_j in C^i.
2. Participate in ACS with the accumulative set C^i as input.

<u>OUTPUT GENERATION:</u> CODE FOR P_i:

1. Waits until ACS completes with output C containing $n - t$ parties. Output the the shares corresponding to t-sharing of the inputs of the parties in C and terminate.

Protocol ComputationPhase($\mathcal{P}$)

<u>FOR EVERY GATE IN THE CIRCUIT:</u> CODE FOR P_i

Wait until the i^{th} share of each of the inputs of the gate is available. Now depending on the type of the gate, proceed as follows:

1. **Input Gate:** $[s]_t = \mathsf{IGate}([s]_t)$: There is nothing to be done here.
2. **Linear Gate:** $[z]_t = \mathsf{LGate}([x]_t, [y]_t, \ldots)$: Compute $z_i = \mathsf{LGate}(x_i, y_i, \ldots)$, the i^{th} share of $z = \mathsf{LGate}(x, y, \ldots)$, where $x_i, y_i, \ldots$ denotes i^{th} share of $x, y, \ldots$.
3. **Multiplication Gate:** $[z]_t = \mathsf{MGate}([x]_t, [y]_t, [r]_{(t,2t)})$:
   (a) Let $[r]_{(t,2t)}$ be the random $(t, 2t)$-sharing associated with the multiplication gate. Also let $(\varphi_1, \ldots, \varphi_n)$ and $(\phi_1, \ldots, \phi_n)$ denote the t-sharing and $2t$-sharing of r, respectively.
   (b) Compute $\Lambda_i = x_i.y_i - \phi_i$ the i^{th} share of Λ which is now $2t$-shared.
   (c) Participate in Rec-Private($\mathcal{P}, 2t, \Lambda, P_j$) for P_j-Private-Reconstruction of Λ for all $j = 1, \ldots, n$.
   (d) Participate in Rec-Private($\mathcal{P}, 2t, \Lambda, P_i$) as a receiver to reconstruct Λ. Compute $z_i = \Lambda - \varphi_i$, the i^{th} share of z.
4. **Random Gate:** $[R]_t = \mathsf{RGate}([r]_{(t,2t)})$: Let $[r]_{(t,2t)}$ be the random $(t, 2t)$-sharing associated with the random gate. Also let $(\varphi_1, \ldots, \varphi_n)$ denote the t-sharing of r. Assign $R_i = \varphi_i$ as the i^{th} share of $R(= r)$.
5. **Output Gate:** $x = \mathsf{OGate}([x]_t)$: Participate in Rec-Private($\mathcal{P}, t, x, P_j$) for every $P_j \in \mathcal{P}$. Participate in Rec-Private($\mathcal{P}, t, x, P_i$) as a receiver to reconstruct x. Output x.