

# The Round Complexity of Verifiable Secret Sharing Revisited

Arpita Patra<sup>1</sup>\*, Ashish Choudhary<sup>\*\*1</sup>, Tal Rabin<sup>2</sup>, and  
C. Pandu Rangan<sup>\*\*\*1</sup>

<sup>1</sup> Dept of Computer Science and Engineering  
IIT Madras, Chennai India 600036

arpitapatra10@gmail.com, partho\_31@yahoo.co.in, prangan55@gmail.com

<sup>2</sup> IBM T. J. Watson Research Center  
talr@us.ibm.com

**Abstract.** The round complexity of interactive protocols is one of their most important complexity measures. In this work we prove that existing lower bounds for the round complexity of VSS can be circumvented by introducing a negligible probability of error in the reconstruction phase. Previous results show matching lower and upper bounds of *three* rounds for VSS, with  $n = 3t + 1$ , where the reconstruction of the secrets always succeeds, i.e. with probability 1. In contrast we show that with a negligible probability of error in the reconstruction phase:

1. There exists an efficient 2-round VSS protocol for  $n = 3t + 1$ . If we assume that the adversary is non-rushing then we can achieve a 1-round reconstruction phase.
2. There exists an efficient 1-round VSS for  $t = 1$  and  $n > 3$ .
3. We prove that our results are optimal both in resilience and number of sharing rounds by showing:
  - (a) There does not exist a 2-round WSS<sup>1</sup> (and hence VSS) for  $n \leq 3t$ .
  - (b) There does not exist a 1-round VSS protocol for  $t \geq 2$  and  $n \geq 4$ .

## 1 Introduction

Verifiable Secret Sharing (VSS) [3] is a fundamental building block for many distributed cryptographic tasks. VSS is a two phase protocol (Sharing and Reconstruction) carried out among  $n$  parties in the presence of an adversary who can corrupt up to  $t$  parties. Informally, the goal of the VSS protocol is to share a secret,  $s$ , among the  $n$  parties during the sharing phase in a way that would

---

\* 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, Government of India.

<sup>1</sup> WSS is a weaker notion of VSS.

later allow for a unique reconstruction of this secret in the reconstruction phase, while preserving the secrecy of  $s$  until the reconstruction phase.

Due to the central importance of VSS in the context of many cryptographic protocols such as multiparty computation, Byzantine agreement, etc, the problem has drawn much attention over the years (e.g. [12, 1, 2, 7, 8, 18, 5, 4, 6]) and many aspects of the problem have been studied. Round complexity is one of the most important complexity measures of interactive protocols. The study of the round complexity of VSS in the information theoretic security setting, i.e. under the assumption of a *computationally unbounded adversary*, was initiated by Gennaro et al. [11]. Their investigation was conducted under the assumption that the protocols are error-free. They refer to the round complexity of VSS as the number of rounds in the sharing phase and prove that a 3-round error-free VSS is possible only if  $n \geq 3t + 1$ , and match it with an inefficient upper bound. Fitzi et al. [10] show an optimal efficient 3-round VSS protocol in this setting. The protocol of Fitzi et al. used the broadcast channel in more than one round of the sharing phase and Katz et al. [14] showed how to achieve the same result while using a single round of broadcast. The lower bound from [11] (and the matching upper bounds) consider *error-free* VSS, where the VSS properties are satisfied without any probability of error.

In this work we investigate the question of whether the lower bounds for the round complexity of VSS can be overcome by introducing a negligible probability of error.

**Our Results:** We prove that existing lower bounds for the round complexity of VSS can be circumvented by introducing a negligible probability of error in the reconstruction phase. Specifically, we show that:

1. There exists an efficient 2-round VSS protocol for  $n = 3t + 1$ . This protocol has a 2-round reconstruction phase. If we assume that the adversary is non-rushing then we can achieve a 1-round reconstruction phase. A rushing adversary can wait to hear the incoming messages in a given round prior to sending out its own messages.  
This matches the sharing phase round complexity of the best known protocols in the computational setting [9, 16] with no set-up assumptions (but note that these protocols use a one round reconstruction phase).
2. There exists an efficient 1-round VSS for  $t = 1$  and  $n \geq 4$ .
3. We prove that our results are optimal both in resilience and number of sharing rounds by proving:
  - (a) There does not exist a 2-round WSS (and hence VSS) for  $n \leq 3t$ .
  - (b) There is no 1-round VSS protocol for  $t \geq 2$  and  $n \geq 4^2$ .

Our protocols also achieve the design optimization of Katz et al. [14] and use a single round of broadcast in the sharing phase and no broadcasts at all in the reconstruction phase.

To achieve our goal of constructing a VSS protocol, we follow the structure of [18, 17], where we first design a Weak Secret Sharing (WSS) protocol and

---

<sup>2</sup> We note that there exists a 1-round WSS protocol with  $n > 3t$  (see Appendix A).

then use it as a building block for VSS. Informally WSS is a primitive which satisfies the same properties as VSS except for the commitment property. VSS has a *strong commitment*, which requires that at the end of the sharing, there is a fixed value  $s^*$  and that the honest parties output this value in the reconstruction phase. In contrast, WSS has a *weaker commitment* property which requires that at the end of the reconstruction phase, the honest parties output  $s^*$  or NULL. The novelty of our protocol is in the specific design of the WSS component and the way we use it to build the round optimal VSS.

**On the Definition of Round Complexity of VSS:** As we have stated earlier, the common definition for the round complexity of VSS is the number of rounds in the sharing phase. This is a natural definition for the perfect (i.e., zero error) setting, as the reconstruction can always be done in one round (by having all parties reveal their complete view generated at the end of sharing phase). However, in our protocols we have a reconstruction phase that cannot be collapsed into a single round. This indicates that a different definition for the round complexity of VSS may be needed, which is the total number of rounds in the sharing plus the number of rounds in the reconstruction. Both the previous VSS results [11, 10, 14] and our result exhibit a VSS with a *total* of four rounds<sup>3</sup>. This introduces the question of what is the lower bound on the total number of rounds for VSS.

## 2 Preliminaries

We follow the network model of [18, 11]. Specifically, we consider a setting with  $n$  parties  $\mathcal{P} = \{P_1, P_2, \dots, P_n\}$  that are pairwise connected by a private and authenticated channel. We further assume that all parties have access to a common broadcast channel and there exists a *malicious, computationally unbounded adversary*  $\mathcal{A}_t$ , that can corrupt up to  $t$  parties, out of  $n$  parties. The adversary controls and coordinates the actions of the corrupted/faulty parties. We further allow the adversary to be rushing, i.e. in every round of communication it can wait to hear the messages of the honest parties before sending his own messages. For simplicity we describe our protocols for a static adversary, who corrupts all the parties at the beginning of the protocol. However, our results also hold for a stronger adaptive adversary. Given a security parameter  $k$ , we assume that the protocols operate with values from a finite field  $\mathbb{F} = GF(q)$ , where  $q = 2^k$ . Thus, each element of  $\mathbb{F}$  can be represented by  $k$  bits. Moreover, without loss of generality, we assume that  $n = \text{poly}(k)$ . The error probability of our protocols will be  $2^{-\Omega(k)}$ . We say that our protocols are efficient if the communication and computation of the parties are polynomial in the security parameter  $k$ . All the protocols presented in this paper perform computation and communication which are  $\text{poly}(k)$ . We assume the system to be synchronous. Therefore the protocols operate in a sequence of rounds, where in each round, a party performs

<sup>3</sup> As the total number of rounds in both protocols is the same, the question of which protocol to use depends on the application. For applications where there is a need of more efficiency during the sharing, i.e. fewer number of rounds, the two round sharing protocol should be used.

some local computation, sends new messages to the other parties through the private channels and broadcasts some information over the broadcast channel, then it receives the messages that were sent by the other parties in this round on the private and broadcast channels.

## 2.1 Verifiable Secret Sharing (VSS)

We now present the definition of VSS [3]. In a VSS protocol there is a distinguished party  $D \in \mathcal{P}$ , that holds an input  $s \in \mathbb{F}$  referred to as the secret. The protocol consists of two phases, a sharing phase and a reconstruction phase. We call an  $n$  party protocol with adversary  $\mathcal{A}_t$  an  $(n, t)$ -VSS protocol if it satisfies the following conditions for dealer  $D$  holding secret  $s$  :

**Secrecy.** If  $D$  is honest then the adversary’s view during the sharing phase reveals no information on  $s$ .<sup>4</sup> More formally, the adversary’s view is *identically distributed* for all different values of  $s$ .

**Correctness.** If  $D$  is honest then the honest parties output  $s$  at the end of the reconstruction phase.

**Strong Commitment.** If  $D$  is *corrupted*, then at the end of the sharing phase there is a value  $s^* \in \mathbb{F} \cup \{NULL\}$ , such that at the end of the reconstruction phase all honest parties output  $s^*$ .

NOTE: This definition is equivalent to saying that  $s^* \in \mathbb{F}$ , by fixing a default value in  $\mathbb{F}$ , which may be output in case the reconstruction ends with a NULL. However, we prefer this presentation of the definition as to distinguish it from a stronger definition of VSS [13, 11]. The stronger definition also requires that at the end of the sharing there is a commitment to an actual value in  $\mathbb{F}$ , i.e. the dealer cannot commit to NULL, and furthermore that all parties hold a share of this actual value. Thus, using the above definition points to the fact that NULL is a possible value, instead of setting it to a default value in  $\mathbb{F}$ .

Protocols that do not satisfy the stronger VSS definition are not suitable for use in multiparty computations. The protocols in this paper satisfy the standard VSS definition, which leave the open question of whether a 2-round VSS protocol can be designed that satisfies the stronger definition. However, when examining the round complexity of VSS as a stand alone application, the above definition is sufficient and was used in [11] (with the variation  $s^* \in \mathbb{F}$ ) to prove the lower bounds.

**VSS in External Dealer Model:** In the external dealer model, the system is assumed to consist of a dealer and  $n$  parties. The dealer is considered as an external party. Moreover, the adversary  $\mathcal{A}_t$  is allowed to corrupt  $D$  and up to  $t$  *additional* parties. We stress that all the protocols and lower bounds presented in this paper will work for this model as well.

---

<sup>4</sup> If  $D$  is corrupted, then  $s$  will be known to the adversary. In such a case, the secrecy property does not apply.

## 2.2 Weak Secret Sharing (WSS)

In order to construct our VSS protocol we use another form of secret sharing called Weak Secret Sharing (WSS) [18, 17]. The setting is the same as for the VSS and the definition satisfies the Secrecy and Correctness properties. However, we relax the Commitment property as follows:

**Weak Commitment.** If  $D$  is faulty then at the end of the sharing phase there is a value  $s^* \in \mathbb{F} \cup \{NULL\}$  such that at the end of the reconstruction phase, each honest party will output either  $s^*$  or NULL.

Notice that it is not required that all honest parties output the same value, i.e. some may output  $s^*$  and some may output NULL. The above definition is standard and follows many of the existing definitions [17, 18, 14].

## 2.3 Statistical VSS and Statistical WSS

We say that a VSS (WSS) protocol is a  $(1-\epsilon)$  statistical VSS (WSS) if it achieves correctness and strong (weak) commitment with probability  $1-\epsilon$ , where given a security parameter  $k$  we have that  $\epsilon = 2^{-\Omega(k)}$ . Note that we assume secrecy to be perfect<sup>5</sup>.

## 3 Statistical-WSS, 2-Round Sharing, $n = 3t + 1$

In this section we present our 2-round share, 2-round reconstruct statistical-WSS protocol with  $n = 3t+1$ . The protocol appears in Figure 1. For ease of exposition, we describe our protocol using multiple rounds of broadcast. We follow this with a brief description on how to modify the protocol to a variation that uses a single round of broadcast.

NOTE: Following the notation of [11], whenever we say that dealer is disqualified during the sharing phase of WSS/VSS, we mean to say that all honest parties accept the sharing of NULL (or a default value from  $\mathbb{F}$ ) as the dealer's secret.

Before we turn to our proofs we draw the readers attention to the following interesting points that enable us to achieve the final result. The bi-variate polynomial  $F(x, y)$  (defined by  $D$ ) has a tweak, the  $x$  variable is of degree  $nk + 1$ , which results in the polynomials  $f_i(x)$  being of degree  $nk + 1$  (where as this degree is typically  $t$  in other protocols). We further create a situation where these polynomials never need to be reconstructed and thus the parties need not hold large number of points on the polynomials to interpolate them. These two properties put together, enable us to give each party many evaluation points and values on these polynomials and to further allow them to expose a portion of them without exposing the underlying polynomial. In addition, we adapt an interesting technique from Tompa and Woll [20] and use *secret* evaluation points.

The fact that we can expose points on the high degree polynomials and that the evaluation points are secret, facilitates the cut-and-choose proof, carried out

---

<sup>5</sup> We conjecture that the lower bounds in this paper hold also for the case when the secrecy is statistical.

## Protocol WSS

### Sharing Phase

**Local Computations:**  $D$  does the following:

1. Picks a random bivariate polynomial  $F(x, y)$  over  $\mathbb{F}$  of degree  $t$  in the variable  $y$  and degree  $nk + 1$  in the variable  $x$ , such that  $F(0, 0) = s$ .
2. Defines  $f_i(x) = F(x, i)$  for  $1 \leq i \leq n$ .
3. Picks random polynomials  $r_i(x)$  over  $\mathbb{F}$ ,  $\deg(r_i(x)) = nk + 1$  for  $1 \leq i \leq n$ .
4.  $nk$  random, non-zero, distinct elements from  $\mathbb{F}$ , denoted by  $\alpha_{i,1}, \alpha_{i,2}, \dots, \alpha_{i,k}$  for  $1 \leq i \leq n$ .

**Round 1:**  $D$  sends to party  $P_i$ :

- The polynomials  $f_i(x), r_i(x)$ . Let  $f_i(0)$  be  $P_i$ 's share of  $D$ 's secret  $s$ .
- The random evaluation points  $\alpha_{i,\ell}$  for  $1 \leq \ell \leq k$ .
- $a_{j,i,\ell} = f_j(\alpha_{i,\ell})$  and  $b_{j,i,\ell} = r_j(\alpha_{i,\ell})$  for  $1 \leq \ell \leq k, 1 \leq j \leq n$ .

**Round 2:** Party  $P_i$  broadcasts the following:

- A random non-zero value  $c_i$  and polynomial  $g_i(x) = f_i(x) + c_i r_i(x)$ ,  $\deg(g_i(x)) = nk + 1$ .<sup>a</sup>
- For a random subset of indices  $\ell_1, \dots, \ell_{\frac{k}{2}}$ , the evaluation points  $\alpha_{i,\ell_1}, \dots, \alpha_{i,\ell_{\frac{k}{2}}}$  and  $a_{j,i,\ell_1}, \dots, a_{j,i,\ell_{\frac{k}{2}}}$  and  $b_{j,i,\ell_1}, \dots, b_{j,i,\ell_{\frac{k}{2}}}$  for  $1 \leq j \leq n$ .

**Local Computation:** For all parties:

1. Party  $P_i$  is *accepted* by party  $P_j$  if  $a_{i,j,\ell} + c_i b_{i,j,\ell} = g_i(\alpha_{j,\ell})$  for all  $\ell$  in the set of indices broadcasted by  $P_j$  in **Round 2**.
2. Initiate the set  $SH = \emptyset$ . Place  $P_i$  in  $SH$  if it is accepted by at least  $2t + 1$  parties.
3. If  $|SH| \leq 2t$  disqualify dealer  $D$ . Note that  $SH$  computed by all honest parties are identical.

### Reconstruction Phase, 2-rounds:

**Round 1:** Each  $P_i$  in  $SH$  broadcasts  $f_i(x)$ ,  $\deg(f_i(x)) = nk + 1$ .

**Round 2:** Each  $P_j \in \mathcal{P}$  broadcasts all the evaluation points  $\alpha_{j,\ell}$  which were not broadcasted in the sharing phase and  $a_{i,j,\ell}$  corresponding to those indices, for  $i = 1, \dots, n$ .

**Local Computation:** For all parties:

1. Party  $P_i \in SH$  is *re-accepted* by  $P_j \in \mathcal{P}$  if for one of the newly revealed points it holds that  $a_{i,j,\ell} = f_i(\alpha_{j,\ell})$ .
2. Initiate the set  $REC = \emptyset$ . Place  $P_i$  in  $REC$  if it is re-accepted by at least  $t + 1$  parties. If the shares of the parties in  $REC$  interpolate to a  $t$  degree polynomial  $g(y)$  then output  $s = g(0)$ . Otherwise output  $NULL$ .

<sup>a</sup> When ever we say that a party broadcasts a polynomial of a certain degree we assume that if this is not done then the party is disqualified.

**Fig. 1.** (2-Round Share, 2-Round Reconstruct) Statistical-WSS,  $n = 3t + 1$

by the parties in Round 2. It should be noted that if we allow rushing, then a cheating prover may try to foil the cut-and-choose proof during the sharing phase. However, surprisingly we show that this proof is sufficient for our needs and that we can deal with such faulty parties in the reconstruction phase.

**Lemma 1.** *Protocol WSS satisfies the  $(1-\epsilon)$ -correctness property.*

PROOF: It is easy to see that if  $D$  is honest, then every honest party  $P_i$  is present in  $SH$  as well as in  $REC$ . Given that all honest parties are present in  $SH$  the dealer will not be disqualified during the sharing phase. In order to show that the correct secret is reconstructed, we prove that if a faulty  $P_i$  broadcast a polynomial  $\bar{f}_i(x) \neq f_i(x)$ , then with high probability  $P_i$  will not be added to  $REC$ . In order for a faulty  $P_i$  to be included in  $REC$ , it needs to be re-accepted by  $t + 1$  parties and thus by at least one honest party. The polynomial  $\bar{f}_i(x)$  can agree with  $f_i(x)$  in at most  $nk + 1$  evaluation points. Without knowing the secret evaluation points of an honest party, say  $P_j$ , the probability that  $P_i$  will be re-accepted by  $P_j$  is at most  $\frac{nk}{|\mathbb{F}|}$ . Thus, the probability that any faulty party is in  $REC$  is  $\frac{(nk)(2t+1)(t)}{|\mathbb{F}|} \approx 2^{-\Omega(k)}$ . Hence with very high probability, the parties will reconstruct  $s = f(0)$ , which is  $D$ 's secret.  $\square$

Note that in the previous proof we did not claim, and in fact cannot claim, that there are no faulty parties in  $SH$ . As we allow the adversary to be rushing, it can cause faulty parties, i.e. parties that have broadcasted inconsistent polynomials (during the second round of the sharing phase), to be included in this set. This is done by waiting to hear the evaluation points of the honest parties (in the second round of the sharing phase). However, this does not affect the result of the reconstruction because the parties in  $SH$  broadcast their polynomials in the first round while the secret evaluation points of the parties are revealed only in the second round of the reconstruction.

**Lemma 2.** *Protocol WSS satisfies the  $(1-\epsilon)$ -weak commitment property.*

PROOF: To prove this lemma we need to show that in case that a faulty  $D$  was not disqualified, i.e.  $|SH| \geq 2t + 1$ , then with high probability, all the honest parties  $P_i$  that are in  $SH$  are also present in  $REC$ . If we prove this then the lemma follows immediately; we set  $D$ 's committed secrets  $s^*$  to be the constant term of the polynomial, which is defined by the interpolation of the shares of the honest parties in  $SH$  (note that  $s^*$  may be  $NULL$ ). As we require that shares of all the parties in  $REC$  define a polynomial of degree  $t$ , then either the value  $s^*$  or  $NULL$  will be reconstructed.

In order for an honest  $P_i$  to be in  $SH$  and not in  $REC$  it must be the case that at least  $2t + 1$  parties should have accepted  $P_i$  in the sharing phase but at most  $t$  of them re-accepted it in the reconstruction phase. This means that there is at least one honest  $P_j$  who accepted  $P_i$  but did not re-accept it. This implies that the data (evaluation points and values) that  $P_j$  exposed in the sharing phase satisfies the polynomial  $g_i(x)$  that  $P_i$  broadcasted during the sharing phase, but on the other hand, out of the remaining evaluation points that are used by  $P_j$  in the reconstruction phase, none satisfy the polynomial  $f_i(x)$  produced by  $P_i$ . That

is, for the selected  $\frac{k}{2}$  indices  $\ell_1, \dots, \ell_{\frac{k}{2}}$ , it holds that  $a_{i,j,\ell} + c_i b_{i,j,\ell} = g_i(\alpha_{j,\ell})$  for all  $\ell$  in the set of indices  $\{\ell_1, \dots, \ell_{\frac{k}{2}}\}$  and  $f_i(\alpha_{j,\ell}) \neq a_{i,j,\ell}$  for all  $\ell$  in the *remaining* set of indices. Notice that  $P_i$  chooses  $c_i$  independently of the values given by  $D$ . Also,  $P_j$  chooses the  $\frac{k}{2}$  indices randomly out of  $k$  indices. So the probability that the above event happens is  $\frac{1}{\binom{k}{\frac{k}{2}}} \approx 2^{-\Omega(k)}$ , which is negligible. This shows that with high probability all honest parties from  $SH$  will be included in  $REC$ , thus proving our lemma.  $\square$

**Lemma 3.** *Protocol WSS satisfies perfect secrecy.*

PROOF: The secrecy has to be argued when  $D$  is honest. For simplicity, assume that first  $t$  parties are corrupted. So in **Round 1** of the **Sharing Phase**, the adversary will know the polynomials  $f_1(x), \dots, f_t(x), r_1(x), \dots, r_t(x)$  and  $kt$  points on  $f_i(x)$  and  $r_i(x)$  for  $t+1 \leq i \leq n$ . In **Round 2** of the **Sharing Phase**, the adversary learns  $\frac{k}{2}(2t+1)$  additional points on  $f_i(x)$  and  $r_i(x)$  for  $t+1 \leq i \leq n$ . So in total the adversary will know  $kt + \frac{k}{2}(2t+1)$  points on each of  $f_i(x)$  and  $r_i(x)$  for  $t+1 \leq i \leq n$  which is less than the degree of the polynomials  $(nk+1)$ . Thus, the constant term of the polynomials  $f_i(x)$  for  $t+1 \leq i \leq n$  are information theoretically secure in the **Sharing Phase**, which further implies information theoretic security for  $s$ .  $\square$

**Theorem 1.** *There exists an efficient 2-round share, 2-round reconstruct  $(3t+1, t)$  statistical-WSS protocol.*

PROOF: Protocol WSS presented here achieves  $1-\epsilon$ -correctness,  $1-\epsilon$ -weak commitment and perfect secrecy. This follows from Lemma 1, 2 and 3.  $\square$

IMPORTANT NOTE: There is another interesting way to interpret the computation done in the Protocol WSS. We may view this as  $D$  sharing a  $t$  degree polynomial  $g(y)$  using protocol WSS. For this,  $D$  selects the bivariate polynomial  $F(x, y)$  as in protocol WSS, such that  $F(0, y) = g(y)$ . The polynomial  $g(y)$  is the polynomial that  $D$  used to share the secret  $g(0) = F(0, 0) = s$ . The polynomial  $g(y)$  is not random but only preserves the secrecy of the constant term. Yet, this distribution of polynomials is sufficient to provide the secrecy requirements needed by our protocols.

**Statistical WSS with One Round of Reconstruction:** It is interesting to note that if we restrict the adversary to a non-rushing adversary then the two rounds of the reconstruction phase can be collapsed into a single round. The two rounds are needed in order to force the adversary to commit to the polynomials  $f_i(x)$  of the faulty parties prior to seeing the evaluation points, as this knowledge can enable the adversary to publish a polynomial that is re-accepted by the honest parties, which would violate the correctness of the protocol. However, if the adversary is non-rushing then this property is achieved via the synchronicity of the step. We state this in the following theorem:

**Theorem 2.** *If the adversary is non-rushing then there exists an efficient 2-round share 1-round reconstruct  $(3t+1, t)$  statistical-WSS protocol.*



**Statistical WSS with One Round of Broadcast:** We now show how the protocol in Fig. 1 can be modified, so that it uses *only one* round of broadcast. Specifically, we modify the **Reconstruction Phase**, so that it requires no broadcast.

**Reconstruction Phase, 2-rounds:**

**Round 1:** Each  $P_i$  in  $SH$  privately sends  $f_i(x)$ ,  $\deg(f_i(x)) = nk + 1$  to every other party.

**Round 2:** Each  $P_j \in \mathcal{P}$  privately sends all the evaluation points  $\alpha_{j,\ell}$  which were not broadcasted in the sharing phase and  $a_{i,j,\ell}$  for those indices, to all other parties.

**Local Computation:** For all parties it is the same as in the Protocol WSS.

This modified version of WSS preserves the  $(1-\epsilon)$ -correctness and perfect secrecy properties. It will also satisfy  $(1-\epsilon)$ -weak commitment, but *without agreement*. That is, some honest party(ies) may output the committed secret  $s^*$  while some other may output *NULL*.

**4 Statistical-VSS, 2-Round Sharing,  $n = 3t + 1$**

We now design a 2-round share, 2-round reconstruct  $(3t + 1, t)$  statistical-VSS protocol. We follow the general idea of [1, 11, 10, 14] of sharing the secret  $s$  with a symmetric bivariate polynomial  $F(x, y)$  where each party  $P_i$  gets the univariate polynomial  $f_i(y) = F(i, y)$  and his share is  $f_i(0)$ . The next step is for every pair of parties to verify that they have received the correct values from the dealer. However, as we have only one more round available we cannot depend on  $D$  to resolve conflicts in a third round. Thus, instead of doing the verification point wise we carry out the verification on polynomials. More specifically, party  $P_i$  initiates an execution of the WSS protocol in the first round, to share a random polynomial  $g_i(y)$ . In the second round,  $P_i$  broadcasts the masked polynomial  $h_i(y) = f_i(y) + g_i(y)$ , while every other party broadcasts the corresponding point on  $h_i(y)$ . In fact, this verification can be viewed as an extension of the round reducing technique of pad sharing for a single value given in [11], to the sharing of polynomial, which is used as a pad for the verification of a polynomial. The VSS protocol appears in Figure 2.

**Lemma 4.** *Protocol VSS satisfies  $(1-\epsilon)$ -correctness property.*

PROOF: A simple examination of the Protocol VSS and the properties of Protocol WSS reveal that all honest parties will be in VSS- $SH$  and thus an honest  $D$  is not disqualified during the sharing phase. To prove this lemma we need to show that when  $D$  is honest, then very with high probability, for all faulty parties  $P_j$  in VSS- $SH$  the following holds: if at the end of WSS $^{P_j}$ , the fixed (weak committed) value is not NULL and the shared polynomial is  $g_j(y)$ , then  $h_j(y) - g_j(y)$  is in fact polynomial  $f_j(y)$ , received by  $P_j$  from  $D$ . If we prove this, then the lemma follows

## Protocol VSS

### Sharing Phase

#### **Round 1:**

- $D$  selects a random symmetric bivariate polynomial  $F(x, y)$  over  $\mathbb{F}$  of degree  $t$  in each variable such that  $F(0, 0) = s$  and sends the polynomial  $f_i(y) = F(i, y)$  to  $P_i$ .
- Party  $P_i$  initiates Round 1 of the WSS protocol to share a random  $t$  degree polynomial  $g_i(y)$ . Denote this execution by  $\text{WSS}^{P_i}$ .

#### **Round 2:**

- Party  $P_i$  broadcasts the polynomial  $h_i(y) = f_i(y) + g_i(y)$ ,  $\deg(h_i(y)) = t$ , and values  $a_{ji} = f_i(j) + g_j(i) = f_j(i) + g_j(i)$ , for  $1 \leq j \leq n$ .
- Execute Round 2 of the sharing phase of each  $\text{WSS}^{P_i}$ . Let  $SH_i$  denote the set  $SH$  from this execution.

#### **Local Computation:** For all parties

1. Party  $P_i$  is *accepted* by party  $P_j$  if  $h_i(j) = a_{ij}$ .
2. Let  $\text{Accept}_i$  denote the set of parties that accepted  $P_i$ .
3. Create the set  $\text{VSS-SH}$ . Place  $P_i$  in  $\text{VSS-SH}$  if  $|\text{Accept}_i| \geq 2t + 1$ .
4. Remove  $P_i$  from  $\text{VSS-SH}$  if  $|\text{VSS-SH} \cap \text{Accept}_i \cap SH_i| \leq 2t$ . Repeat, until no more parties can be removed.
5. If  $|\text{VSS-SH}| \leq 2t$  then disqualify  $D$ .

### Reconstruction Phase, 2-rounds:

For all  $P_i$  in  $\text{VSS-SH}$ , execute the 2-round reconstruction phase of  $\text{WSS}^{P_i}$ . If the output of the execution is not NULL then let  $g_i(y)$  be the output from this execution.

#### **Local Computation (for each party)**

1. Initialize  $\text{REC} = \text{VSS-SH}$ .
2. Remove  $P_i$  from  $\text{REC}$  if the output of  $\text{WSS}^{P_i}$  is *NULL*.
3. For each  $P_i \in \text{REC}$ , define its share as  $f_i(0) = h_i(0) - g_i(0)$ .
4. If the shares of the parties in  $\text{REC}$  define a unique polynomial  $f(x)$  of degree  $t$  then output  $f(0)$ , otherwise output NULL.

**Fig. 2.** (2-Round Share, 2-Round Reconstruct) Statistical VSS,  $n = 3t + 1$

immediately because, a faulty  $P_j$  in VSS-SH whose reconstruction of  $WSS^{P_j}$  fails is removed from  $REC$ . Furthermore, with high probability, a sufficient number of shares belonging to the parties in  $REC$  will be reconstructed successfully (due to the properties of WSS) and thus the correct secret of  $D$  will be reconstructed.

What this implies is that we cannot guarantee that all parties in VSS-SH are honest. But we can ensure that if they eventually remain in  $REC$  then they have shared the proper values. And this is sufficient to guarantee the correctness of the protocol. We now proceed to prove this claim.

Since  $P_j$  is present in VSS-SH, we know that  $|Accept_j \cap SH_j| \geq 2t + 1$ . This means that there are  $t + 1$  honest parties in this set. By the properties of WSS, this set of honest parties define the polynomial  $g_j(y)$  which  $P_j$  is committed to, at the end of the sharing phase of  $WSS^{P_j}$ . We now examine the polynomial  $h_j(y) - g_j(y)$  and show that it is equal to  $f_j(y)$ . The set of  $(t + 1)$  honest parties in  $(Accept_j \cap SH_j)$  verified that the sum of the share  $f_i(j) = f_j(i)$  (which they received from  $D$ ) and  $g_j(i)$  (which they received from  $P_j$ ), in fact lie on the polynomial  $h_j(y)$ . Moreover, the set of  $t + 1$  shares, corresponding to these honest parties define the polynomial  $f_j(y)$ . Thus,  $h_j(y) - g_j(y) = f_j(y)$ .  $\square$

**Lemma 5.** *Protocol VSS satisfies  $(1 - \epsilon)$ -strong commitment property.*

PROOF: If  $D$  is corrupted and does not get disqualified during the sharing phase, then VSS-SH is fixed at the end of sharing phase. Since  $VSS-SH \geq 2t + 1$ , it contains a set  $\mathcal{H}$  of honest parties of size at least  $t + 1$ . If  $f_j(y)$ 's corresponding to the parties  $\mathcal{H}$  define a unique symmetric bivariate polynomial  $F^*(x, y)$  of degree  $t$  in  $x$  and  $y$ , then  $D$ 's committed secret is  $s^* = F^*(0, 0)$ . Otherwise,  $s^* = \text{NULL}$ . We show that in the reconstruction phase  $s^*$  will be reconstructed.

It is easy to see that due to the WSS reconstruction properties, with high probability, all the honest parties in  $\mathcal{H} \subseteq VSS-SH$  will also be present in  $REC$ . We now divide our proof into two cases: (a)  $s^* \neq \text{NULL}$ : the proof for this case follows from the proof of Lemma 4 as this case is indistinguishable from the case when  $D$  is honest. (b)  $s^* = \text{NULL}$ : As  $\mathcal{H} \subseteq REC$ , during Step 4 of the reconstruction phase all parties will output  $\text{NULL}$  which is equal to  $s^*$ .  $\square$

**Lemma 6.** *Protocol VSS satisfies perfect secrecy.*

PROOF: This proof is similar to the entropy based argument, used to prove the secrecy of 3 round perfect VSS protocol of [10].  $\square$

**Theorem 3.** *There exists an efficient 2-round share, 2-round reconstruct  $(3t + 1, t)$  statistical-VSS protocol.*

As the reconstruction phase of the VSS protocol is simply the reconstruction phase of the WSS, we claim here as well, that the reconstruction phase can be collapsed into one round against a non-rushing adversary.

**Theorem 4.** *If the adversary is non-rushing then there exists an efficient 2-round share 1-round reconstruct  $(3t + 1, t)$  statistical-VSS protocol.*

We stress that in Protocol VSS,  $D$  can commit  $NULL$  at the end of the sharing phase. This makes Protocol VSS unsuitable for Multiparty Computation. It is an interesting problem to see whether there exists an efficient 2-round share,  $(3t + 1, t)$  statistical VSS protocol, which satisfies the stronger definition of VSS [13, 11], given in Section 2. In fact, if such a sharing exists then it would also imply that there is a one round reconstruction, as error correction can be used to interpolate the secret.

**Statistical VSS with One Round of Broadcast:** We now explain how Protocol VSS can be modified, so that the broadcast channel is used in only one round throughout the protocol, namely in the second round of the sharing phase. The reconstruction phase of the VSS protocol is simply the reconstruction phase of the WSS protocol. Moreover, in the previous section, we have seen how Protocol WSS can be modified, so as to have only one round of broadcast. Thus, if we can argue that the modified WSS is sufficient for the reconstruction of VSS, then we have a VSS protocol that does not use broadcast in the reconstruction phase. Examining the proof of the VSS protocol, we see that it is not mandatory that the set of shares, which the honest parties use in reconstruction is identical, but rather that it has a large enough intersection. As the shares of the honest parties provide this guarantee, it is irrelevant which shares of the faulty parties are included in the computation. Thus, by using the modified statistical WSS, we get a statistical VSS, with only one round of broadcast.

## 5 Lower Bounds

### 5.1 Lower Bound for 2-round statistical-VSS, $n \leq 3t$

We now prove the optimality of our 2-round share  $(3t + 1, t)$  statistical VSS protocol, with respect to the resiliency.

**Theorem 5.** *There is no 2-round share  $(n, t)$ -statistical-VSS protocol with  $n \leq 3t$ , irrespective of the number of rounds in the reconstruction phase.*

In fact we prove the following stronger result from which the above theorem follows immediately.

**Theorem 6.** *There is no 2-round share  $(n, t)$ -statistical-WSS protocol with  $n \leq 3t$ , irrespective of the number of rounds in the reconstruction phase.*

To prove the above theorem, we use standard player partitioning arguments and prove the following:

**Lemma 7.** *There is no 2-round share  $(3, 1)$ -statistical-WSS protocol, irrespective of the number of rounds in the reconstruction phase.*

Before proceeding to prove the above lemma, we recall the following result:

**Lemma 8 ([11]).** *Let  $\psi$  be any  $r$ -round protocol, where  $r \geq 2$ . Then there exists an  $r$ -round protocol  $\bar{\psi}$  with the same number of parties and same properties (as  $\psi$ ), such that all messages in rounds  $2, \dots, r$  of  $\bar{\psi}$  are broadcast messages.*

We now prove Lemma 7 by contradiction. Let  $\Pi$  be a 2-round share  $(3, 1)$  statistical WSS protocol, having  $r \geq 1$  rounds in the reconstruction phase. Let the three parties in  $\Pi$  be  $P_1, P_2$  and  $P_3$ , where  $P_1$  is the dealer ( $D$ ). We prove the lemma by constructing a sequence of executions of  $\Pi$  which allows to show that  $\Pi$  violates the  $(1-\epsilon)$ -weak commitment property. From Lemma 8, we can assume that in protocol  $\Pi$ , the private communication is done only in the first round, while in the remaining rounds, parties use only broadcast. The broadcasts done by  $P_2$  and  $P_3$  during first round of sharing phase will be independent of the messages received from  $D$  and hence can be ignored. Similarly, due to the secrecy property, the broadcast done by  $D$  during first round of sharing will be independent of the secret and can be ignored. Moreover, during first round of sharing phase, the private communication done between  $P_2, P_3$  will be independent of the secret. Also the private communication from  $P_2$  to  $P_1$  and from  $P_3$  to  $P_1$  will be independent of the secret.

We first consider the following two executions of  $\Pi$ , where  $D$  is honest:

1. In execution  $E_s$ ,  $D$  shares the secret  $s$ . In the first round of the sharing phase,  $D$  defines the shares  $s_1, s_2, s_3$  and sends them to  $P_1, P_2$  and  $P_3$  respectively. In the second round of sharing, the parties broadcast  $B_1, B_2$  and  $B_3$  respectively. During the reconstruction phase, the parties broadcast messages  $C_{1,1}, C_{2,1}$  and  $C_{3,1}$  respectively in the first round. For  $i = 2, \dots, r$ , in round  $i$  of the reconstruction phase, the parties broadcast the messages  $C_{1,i}, C_{2,i}$  and  $C_{3,i}$  respectively. As  $D$  is honest, due to correctness property of  $\Pi$ , the honest parties need to output  $s$  at the end of the reconstruction phase.
2. In execution  $E_{s^*}$ ,  $D$  shares the secret  $s^*$  and defines the shares  $\bar{s}_1, s_2$  and  $\bar{s}_3$  respectively and gives them to  $P_1, P_2$  and  $P_3$  respectively. Note that due to the secrecy property of  $\Pi$ , such a sharing always exists. Given different randomness, we can have the broadcast messages in round two of the sharing phase be identical to  $B_1, B_2$  and  $B_3$  respectively.<sup>6</sup> The broadcasts in the reconstruction phase are as follows: note that  $P_2$ 's view is identical to its view in  $E_s$  up to this step and thus the first round messages of  $P_2$  in the reconstruction phase are the same as in  $E_s$  (i.e.,  $C_{2,1}$ ). The broadcast messages in the first round of reconstruction are  $\bar{C}_{1,1}, C_{2,1}$  and  $\bar{C}_{3,1}$  respectively. For  $i = 2, \dots, r$ , in round  $i$  of the reconstruction phase, the parties broadcast the messages  $\bar{C}_{1,i}, \bar{C}_{2,i}$  and  $\bar{C}_{3,i}$  respectively. As  $D$  is honest, due to correctness property of  $\Pi$ , the honest parties need to output  $s^*$  at the end of the reconstruction phase.

Next we consider another execution of  $\Pi$ , namely  $E_s^*$ .

3. In  $E_s^*$ ,  $D$  is honest and  $P_3$  is faulty. Here  $D$ 's communication during the first round of sharing is the same as in  $E_s$  and the second round broadcast messages of the sharing phase are same as in  $E_s$ . However, during the reconstruction phase,  $P_3$  gets corrupted. In the first round of reconstruction,

<sup>6</sup> If this is not so, then it implies that  $B_1, B_2$  and  $B_3$  could be generated only for the shares  $s_1, s_2$  and  $s_3$  and a specific randomness, which violates the secrecy condition of protocol  $\Pi$ .

$P_3$  broadcasts the message  $\bar{C}_{3,1}$  (as if he is in execution  $E_{s^*}$ ), while  $P_1$  and  $P_2$  broadcasts  $C_{1,1}$  and  $C_{2,1}$  respectively, as in  $E_s$ . For  $i = 2, \dots, r$ , in round  $i$  of the reconstruction phase, the parties broadcast the messages  $C'_{1,i}, C'_{2,i}$  and  $C'_{3,i}$  respectively. As  $D$  is honest, due to correctness property of  $\Pi$ , the honest parties need to output  $s$  at the end of the reconstruction phase.

Finally, we consider another execution  $E$  of  $\Pi$ , where  $D (= P_1)$  is corrupted.

4. In  $E$ , during first round of the sharing phase,  $D$  gives to parties  $P_2$  and  $P_3$  the shares  $s_2$  and  $\bar{s}_3$  respectively. Due to different randomness, the broadcast messages in the second round of the sharing phase are  $B_1, B_2$  and  $B_3$  respectively. During the reconstruction phase, in the first round,  $P_2$  broadcasts  $C_{2,1}$  as its view at this point is identical to that in the execution  $E_s$ , and  $P_3$  broadcasts  $\bar{C}_{3,1}$  as its view is identical to the one in  $E_{s^*}$ . Now  $P_1$  can behave in one of the two ways:
  - 4.1  $P_1$  behaves as if he is in the reconstruction phase of execution  $E_{s^*}$  and broadcasts  $\bar{C}_{1,i}$  in  $i^{th}$  round of the reconstruction phase for  $i = 1, \dots, r$ . Thus the view of  $P_2$  and  $P_3$  at the end of the first round of reconstruction is identical to the view in  $E_{s^*}$ . Hence, for  $i = 2, \dots, r$ ,  $P_2$ 's and  $P_3$ 's broadcasts in the  $i^{th}$  round of the reconstruction will be the same as in  $E_{s^*}$ . Thus at the end of the reconstruction phase, the view of  $P_2$  and  $P_3$  will be same as in  $E_{s^*}$  and thus they will reconstruct  $s^*$ .
  - 4.2  $P_1$  behaves as if he is in the reconstruction phase of execution  $E_s^*$  and broadcasts  $C_{1,1}$  during first round of the reconstruction phase and  $C'_{1,i}$  during  $i^{th}$  round of reconstruction phase for  $i = 2, \dots, r$ . Now the views of  $P_2$  and  $P_3$  will be the same as in  $E_s^*$  at the end of the first round of reconstruction. Using the same arguments as in 4.1 we have that the subsequent rounds of the reconstruction phase will also be the same as in  $E_s^*$ , and thus at the end of the reconstruction phase, the parties will output  $s$ .

Thus we have shown that a corrupted  $D$  can always force during the reconstruction phase the output of the protocol to be one of two secrets, thus violating the weak commitment property. From the above proof, we conclude that there does not exist a 2-round share  $(3t, t)$  statistical WSS and hence such a statistical VSS protocol, with any number of rounds in the reconstruction phase.  $\square$

## 5.2 Lower Bound for 1-Round statistical-VSS

We now derive a non-trivial lower bound on the fault tolerance of any 1-round share statistical VSS (with any number of rounds in reconstruction).

**Theorem 7.** *1-round share statistical-VSS is possible iff  $((t = 1)$  and  $(n \geq 4))$ , irrespective of the number of rounds in reconstruction.*

PROOF: The impossibility of 1-round share  $(3, 1)$  statistical VSS with any number of rounds in reconstruction, follows from Theorem 5. Now we show that

for  $t \geq 2$  there does not exist any 1-round share  $(n, t)$  statistical VSS protocol with  $n \geq 4$ , irrespective of the number of rounds in the reconstruction phase. We prove the above the statement assuming  $t = 2$ .

To prove the above claim, we use a hybrid argument. More specifically, we assume that  $\Pi$  is a 1-round share  $(n, 2)$  statistical VSS with  $n \geq 4$ , with any number of rounds in the reconstruction phase. Without loss of generality, let the  $n$  parties in  $\Pi$  be denoted by  $P_1, \dots, P_n$  with  $D$  being any of these  $n$  parties, other than  $P_1$ . Before proceeding further, we make the following claim:

*Claim.* In any execution of  $\Pi$ , the messages broadcast by  $D$  and other parties during sharing phase will be independent of the secret. Moreover, private communication between any two honest parties (excluding the ones done from  $D$  to the parties) during the sharing phase, will be independent of the messages received from  $D$  during the sharing phase.

PROOF: From the secrecy property of  $\Pi$ , any message broadcasted by  $D$  during the sharing phase should be independent of the secret. Also, since  $\Pi$  has only one round in the sharing phase, the messages exchanged between any two honest parties (excluding the ones given by  $D$  to the parties) and the messages broadcasted by the parties during the sharing phase, will be independent of the messages that the parties have received from  $D$  during the sharing phase.  $\square$

Based on the above claim, we can simply ignore the broadcast done by  $D$  and the parties during the sharing phase. We can also ignore all private communication between any two parties (excluding the ones done from  $D$  to the parties) during the sharing phase and concentrate only on the messages which are privately communicated by  $D$  to the the parties. Thus, without loss of generality, any execution of protocol  $\Pi$  will have the following form:

(Sharing Phase):  $D$ , on having a secret  $Sec$ , generates messages  $Msg_1, \dots, Msg_n$  and privately communicates  $Msg_i$  to party  $P_i$ . Since  $\Pi$  is a 1-round share VSS, the sharing phase will take only one round.

(Reconstruction Phase): This may take several rounds. At the end of the reconstruction phase, each party outputs some secret.

Now consider an execution of  $\Pi$ , where an *honest*  $D$ , on input secret  $s$ , generates  $(\alpha_1, \dots, \alpha_n)$  during sharing phase and privately communicates  $\alpha_i$  to  $P_i$ . Now from the correctness property of  $\Pi$ , this distribution of messages should output  $s$  at the end of the reconstruction phase. We now prove the following claim:

*Claim.* Any execution of  $\Pi$ , where  $D$  (honest or corrupted) generates and distributes  $\alpha_1, \dots, \alpha_{n-1}, \beta_n$  (for any  $\beta_n$ ) during the sharing phase, should output the secret  $s$  at the end of the reconstruction phase.

PROOF: If  $\beta_n = \alpha_n$ , then the claim is true. Let  $\beta_n \neq \alpha_n$ , we prove the claim by contradiction. More specifically, let the distribution of messages  $\alpha_1, \dots, \alpha_{n-1}, \beta_n$  outputs secret  $s' \neq s$  during the reconstruction phase. Now consider another execution of  $\Pi$ , where  $D$  is corrupted and distributes  $\alpha_1, \dots, \alpha_n$  during the sharing phase. During the reconstruction phase, the adversary corrupts  $P_n$  and

asks him to behave as if  $P_n$  has received either  $\alpha_n$  or  $\beta_n$ . Accordingly, either  $s$  or  $s'$  will be reconstructed at the end of the reconstruction phase. This violates the commitment property of  $\Pi$ , which is a contradiction. Hence distribution of the messages  $\alpha_1, \alpha_2, \dots, \alpha_{n-1}, \beta_n$  (for any  $\beta_n$ ) during the sharing phase, should output the secret  $s$  at the end of the reconstruction phase.  $\square$

Now using similar arguments as in the above claim, we can prove the following lemma:

**Lemma 9.** *Any execution of  $\Pi$ , where  $D$  (honest or corrupted) generates and distributes  $\alpha_1, \beta_2, \dots, \beta_n$  (for any  $\beta_2, \dots, \beta_n$ ) during the sharing phase, should output the secret  $s$  at the end of the reconstruction phase.*

Finally the above lemma clearly shows a violation of the secrecy property of  $\Pi$  because it states that any execution, where  $D$  gives message  $\alpha_1$  to  $P_1$  will always output the secret  $s$  at the end of the reconstruction phase. So if  $D$  is honest and adversary passively corrupts  $P_1$  in such an execution, he will come to know that the shared secret is  $s$ , which is a violation of the secrecy property. Theorem 7 now follows from the above discussion.  $\square$

Note that the above proof does not hold for WSS due to the fact that WSS requires only weak commitment, this prevents the argument that all sequences of messages sent to the parties need to be reconstructed to the same secret. In fact we can design a 1-round share, 2-round reconstruct  $(3t + 1, t)$  statistical WSS protocol (see Appendix A.)

We provide without proof a Statistical VSS, 1-Round Sharing for  $n = 4, t = 1$ . Proofs are provided in the full version [15].

### **Sharing Phase**

**$D$  selects:** A random polynomial  $f(x)$  over  $\mathbb{F}$  of degree 1, such that  $f(0) = s$ . For  $i, 2 \leq i \leq 4$  the dealer chooses and sends to  $P_i$  the following:

1. A random polynomial  $f_i(x)$  over  $\mathbb{F}$ ,  $\deg(f_i) = 1$  and  $f_i(0) = f(i)$ .
2. Random non-zero element from  $\mathbb{F}$ , denoted by  $\alpha_i$ .
3.  $v_{ji} = f_j(\alpha_i)$  for  $2 \leq j \leq 4$ .

**Reconstruction Phase, 2-rounds:**  $D(P_1)$  is not allowed to participate

**Round 1:** Each  $P_i$  broadcasts  $f'_i(x)$ , for  $2 \leq i \leq 4$ .

**Round 2:** For  $2 \leq i \leq 4$ ,  $P_i$  broadcasts the evaluation point  $\alpha'_i$  and the values  $v'_{ji}$ , for  $2 \leq j \leq 4$ .

**Local Computation (by each party except  $P_1$ ):**

1. party  $P_i \in \mathcal{P} \setminus \{P_1\}$  is *confirmed* if there exists a  $P_j \in \mathcal{P} \setminus \{P_1, P_i\}$  for which  $f'_i(\alpha'_j) = v'_{ij}$ .
2. If the  $f'_i(0)$ s corresponding to the set of confirmed parties define a polynomial  $f(x)$  of degree one then output  $f(0)$  otherwise output NULL.



## Open Problems

This paper leaves an interesting open problem: What is the lower bound on the total number of rounds in VSS, i.e. sharing plus reconstruction? This problem is also closely connected to the question of whether we can design a 2-round statistical VSS protocol which satisfies the strong VSS definition. Such a protocol would immediately result in a total of 3-round VSS protocol.

**Acknowledgments:** We would like to thank the anonymous referees of CRYPTO 2009 for several helpful suggestions.

## References

1. M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation. *STOC*, pg 1–10, 1988.
2. D. Chaum, C. Crpeau, and I. Damgård. Multiparty Unconditionally Secure Protocols. In *FOCS*, pages 11–19, 1988.
3. B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults. In *STOC*, pages 383–395, 1985.
4. R. Cramer, I. Damgård, and S. Dziembowski. On the Complexity of Verifiable Secret Sharing and Multiparty Computation. In *STOC*, pages 325–334, 2000.
5. R. Cramer, I. Damgård, S. Dziembowski, M. Hirt, and T. Rabin. Efficient Multiparty Computations Secure Against an Adaptive Adversary. In *EUROCRYPT*, pages 311–326, 1999.
6. R. Cramer, I. Damgård, and U. M. Maurer. General Secure Multi-Party Computation from Any Linear Secret-Sharing Scheme. *EUROCRYPT'00*, pg 316–334.
7. D. Dolev, C. Dwork, O. Waarts, and M. Yung. Perfectly Secure Message Transmission. *JACM*, 40(1):17–47, 1993.
8. C. Dwork. Strong Verifiable Secret Sharing. In *WDAG*, pages 213–227, 1990.
9. P. Feldman. A Practical Scheme for Non-Interactive Verifiable Secret Sharing. In *FOCS*, pages 427–437, 1987.
10. M. Fitzi, J. Garay, S. Gollakota, C. Pandu Rangan, and K. Srinathan. Round-Optimal and Efficient Verifiable Secret Sharing. In *TCC*, pages 329–342, 2006.
11. R. Gennaro, Y. Ishai, E. Kushilevitz, and T. Rabin. The Round Complexity of Verifiable Secret Sharing and Secure Multicast. In *STOC*, pages 580–589, 2001.
12. O. Golderich, S. Micali, and A. Wigderson. How to Play a Mental Game— a Completeness Theorem for Protocols with Honest Majority. *STOC'87*, pg 218–229.
13. O. Goldreich. Secure Multiparty Computation. [www.wisdom.weizman.ac.il/~oded/pp.html](http://www.wisdom.weizman.ac.il/~oded/pp.html), 2007.
14. J. Katz, C. Koo, and R. Kumaresan. Improving the Round Complexity of VSS in Point-to-Point Networks. Cryptology ePrint 2007/358. Also in ICALP 2008.
15. A. Patra, A. Choudhary, T. Rabin and C. Pandu Rangan. The Round Complexity of Verifiable Secret Sharing Revisited. Cryptology ePrint 2008/172.
16. T. P. Pedersen. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In *CRYPTO*, pages 129–140, 1991.
17. T. Rabin. Robust Sharing of Secrets When the Dealer is Honest or Cheating. *J. ACM*, 41(6):1089–1109, 1994.
18. T. Rabin and M. Ben-Or. Verifiable Secret Sharing and Multiparty Protocols with Honest Majority. In *STOC*, pages 73–85, 1989.
19. A. Shamir. How to Share a Secret. *Comm. of the ACM*, 22(11):612–613, 1979.
20. M. Tompa and H. Woll. How to Share a Secret with Cheaters. In *CRYPTO*, pages 261–265, 1986.

## A 1-Round Statistical WSS

For (partial) completeness we present the 1-Round Statistical WSS for  $n = 3t + 1$ . Proofs appear in the full version [15].

### Sharing Phase

**Local computations:**  $D$  picks:

1. a random polynomial  $G(x)$  over  $\mathbb{F}$  of degree  $t$ , such that  $G(0) = s$ .
2.  $n$  random polynomials  $g_1(x), g_2(x), \dots, g_n(x)$  over  $\mathbb{F}$ , each of degree  $t$ , such that for  $1 \leq i \leq n$ ,  $g_i(0) = G(i)$ .
3.  $n$  random non-zero distinct elements from  $\mathbb{F}$ , denoted by  $\alpha_1, \alpha_2, \dots, \alpha_n$ .

**$D$ 's communication:**  $D$  sends to party  $P_i$ :

- the polynomial  $g_i(x)$ ,
- the random value  $\alpha_i$  and the  $n$  tuple  $[v_{1i} \ v_{2i} \ \dots \ v_{ni}]$  where for  $1 \leq j \leq n$ ,  $v_{ji} = g_j(\alpha_i)$ .

### Reconstruction Phase, 2-rounds:

**Round 1:** Each  $P_i \in \mathcal{P}$  broadcasts the polynomial  $g'_i(x)$ .

**Round 2:** Each  $P_i \in \mathcal{P}$  broadcasts the value  $\alpha'_i$  and the  $n$  tuple  $[v'_{1i} \ v'_{2i} \ \dots \ v'_{ni}]$ .

1. Party  $P_i$  *accepts* party  $P_j$  if  $v'_{ji} = g'_j(\alpha'_i)$ .
2. Party  $P_i$  is called *affirmed* if it is *accepted* by at least  $2t + 1$  parties (possibly including itself) where as  $P_i$  is called *semi-affirmed* if it is accepted by at least  $t + 1$  and by at most  $2t$  parties (possibly including itself).

**Local Computation:** (For all parties):

1. IF the number of *affirmed* parties is less than  $2t + 1$  OR the number of *semi-affirmed* parties is more than zero, then output *NULL*.
2. ELSE let *CORE* be the set of all *affirmed* parties. Consider  $g'_i(0)$ 's of all the parties in *CORE* and check whether they interpolate a unique  $t$  degree polynomial, say  $G'(x)$ . IF yes, then output  $s' = G'(0)$ , ELSE output *NULL*.