Probabilistic Verifiable Secret Sharing Tolerating Adaptive Adversary

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

Abstract

In this work we focus on two basic secure distributed computation tasks- Probabilistic Weak Secret Sharing (PWSS) and Probabilistic Verifiable Secret Sharing (PVSS). PVSS allows a dealer to share a secret among several players in a way that would later allow a unique reconstruction of the secret with negligible error probability. PWSS is slightly weaker version of PVSS where the dealer can choose not to disclose his secret later. Both of them are well-studied problems. While PVSS is used as a building block in every general probabilistic secure multiparty computation, PWSS can be used as a building block for PVSS protocols. Both these problems can be parameterized by the number of players (n) and the fault tolerance threshold (t) which bounds the total number of malicious (Byzantine) players having *unbounded computing power.* We focus on the standard *secure channel model*, where all players have access to secure point-to-point channels and a common broadcast medium. We show the following for PVSS: (a) 1-round PVSS is possible iff $t = 1$ and $n > 3$ (b) 2-round PVSS is possible if $n > 3t$ (c) 4-round PVSS is possible if $n > 2t$. For the PWSS we show the following: (a) 1-round PWSS is possible iff $n > 3t$ and (b) 3-round PWSS is possible if $n > 2t$. All our protocols are *efficient.* Comparing our results with the existing trade-off results for perfect (zero error probability) VSS and WSS, we find that probabilistically relaxing the conditions of VSS/WSS helps to increase fault tolerance significantly.

Keywords: Verifiable Secret Sharing, Error Probability, Round Complexity.

1 Introduction

This paper studies two basic secure computation primitives: Probabilistic Verifiable Secret Sharing (PVSS) and Probabilistic Weak Secret Sharing (PWSS). In *secret sharing* a dealer **D** wants to share a secret s among a set of n players, such that no set of t players will be able to reconstruct s while any set of $t + 1$ or more players will be able to reconstruct s by combining their shares. VSS extends ordinary secret sharing to work against active corruption. It is a stronger notion than standard secret sharing and provides robustness against t malicious players, possibly including **D**. In PVSS, each property of VSS holds, but with a negligible error probability. PVSS is essentially a

2-phase protocol, consisting of a sharing phase and reconstruction phase. In the sharing phase the dealer distributes a secret among n players in a way that no t of them can infer any information on the secret. In the reconstruction phase, the players pool together their information to reconstruct the secret. In PVSS, the following should be true with very high probability: (a) if **D** is honest, then collusion of t Byzantine corrupted players should not be able to prevent honest players from reconstructing the correct secret, (b) moreover, a collusion of dishonest **D** and additional $(t-1)$ dishonest players can not change the reconstructed value once it is decided in sharing phase. In some scenarios the strong requirement of PVSS specified in (b) can be loosened such that **D** may choose not to disclose the secret in reconstruction phase. This means either the committed secret or "NULL" will be output in reconstruction phase. A protocol that satisfies (a) and weaker form of (b) is called PWSS protocol. As in [5], we define the round complexity of PVSS/PWSS protocol as number of communication rounds in its sharing phase. Reconstruction can be done in a single round wherein every player reveals its entire view generated during sharing phase.

While PVSS is an useful building block in the design of general probabilistic multiparty computation protocols, PWSS being a "weaker" version of PVSS is used for constructing PVSS protocols [7, 3]. In this work, we study trade-offs between number of rounds and fault tolerance threshold for PVSS and PWSS and show that allowing a negligible error probability increases fault tolerance significantly in comparison to VSS and WSS respectively. Moreover our results shows noticeable improvements over existing PVSS and PWSS protocols [7, 3] in terms of number of rounds as well as communication complexity.

Existing Literature: There is extensive literature on VSS and WSS. In *secure channel* model (point-to-point private channel and Broadcast channel), perfect (zero error) VSS is first studied in [1, 2] where it is proved that perfect VSS is possible iff $n > 3t$. The exact round complexity of perfect VSS and tight trade-offs between the round complexity and fault tolerance threshold was established by Gennaro et. al. [5]. In their work, among many other important results, Gennaro et. al. has given a 3 round exponential time perfect VSS protocol (with $n > 3t$) which is later made polynomial time by Fitzi et. al. [4]. In summary, the trade-offs between the number of rounds and fault tolerance threshold for perfect VSS and WSS is presented in first two columns of Table 1.

Table 1: The first two columns shows existing characterization for WSS and VSS. The last two columns summarize results for PWSS and PVSS, where "iff" denotes that the condition is necessary and sufficient where as "sufficient" ("necessary") denotes that condition is only sufficient (necessary). "*" indicates the results given in this work

# Rounds	Characterization for WSS	Characterization for VSS	PWSS	PVSS
1	$n > 4t$ [4]	$t = 1$, $n > 4$ for $t > 1$, impossible [5]	$n > 3t$ (iff) *	$t = 1, n > 3$ (iff) for $t > 1$, impossible *
2	$n > 4t$ [4]	$n > 4t$ [5]	$n > 3t$ (sufficient)	$n > 3t$ (sufficient) *
3	$n > 3t$ [4]	$n > 3t$ [5]	$n > 2t$ (iff) *	$n > 2t$ (necessary)
4	$n > 3t$ [4]	$n > 3t$ [5]	$n > 2t$ (iff)	$n > 2t$ (iff) *

In VSS, it is possible to obtain better fault tolerance when negligible error probability is allowed. In [7], it is shown that unconditionally secure VSS with small probability of error (PVSS) can be realized iff $n > 2t$. In [7] a PWSS and a PVSS protocol is proposed. Later Cramer et. al. [3] proposed a more efficient PWSS and PVSS protocol which requires 5 and 9 rounds respectively.

Our Contribution: We bring out the power of allowing negligible error probability by significantly improving the fault tolerance for VSS and WSS problem in *secure channel model* (point-to-point channel + broadcast channel). Specifically, we show the following for PVSS: (a) single round PVSS is possible iff $t = 1$ and $n > 3$ (b) 2-round PVSS is possible if $n > 3t$ (c) 4-round PVSS is possible if $n > 2t$. For the PWSS we show the following: (a) single round PWSS is possible iff $n > 3t$ and (c) 3-round PWSS is possible if $n > 2t$. In traditional secret sharing scheme, **information rate** is defined as the ratio of size of the secret and size of a share [8]. However, in PVSS/PWSS protocols, since the players also communicate among themselves, we extend the definition of **information rate** for PVSS/PWSS protocol as the ratio of total number of bits communicated in the protocol (excluding the bits which are broadcasted) and the size of the secret(s). We observe that the first two steps of PVSS protocol of [3] along with some additional checking constitutes a five round PWSS (with $n = 2t + 1$) achieving an information rate of $O(n^3)$. However, our three round PWSS (with $n = 2t + 1$) attains an information rate of $O(n)$, which is a significant improvement over the PWSS protocol of [3]. Also, our *four* round PVSS with information rate of $O(n^3)$ is a significant improvement over the existing *nine* round PVSS with same information rate [3].

Note that as in the case of VSS, there exists a stronger definition of PVSS which guarantees that at the end of sharing phase, each player locally outputs a share such that the joint shares output by honest players are consistent with a specified secret sharing scheme, say Shamir's (see [5] for this stronger definition of VSS). This definition is convenient to use in the context of general secure multiparty computation. However, this stronger notion is not needed when VSS (PVSS) is viewed as a stand alone application. We though stress that all our protocols (with the exception of 1 round PVSS protocol) can be easily adapted to meet this stronger requirement. Recently in [6], Katz et.al have designed a perfect VSS protocol with $n = 3t + 1$ which optimizes the use of broadcast channel. All our protocols can be easily modified so that they optimize the use of broadcast channel.

Finally, comparing our results (last two columns of Table 1) with the existing trade-offs between the round complexity and the achievable fault tolerance for perfect VSS and WSS (first two columns of Table 1), we find that probabilistically relaxing the conditions of VSS/WSS helps significantly to increase fault tolerance. Note that for 2 round PVSS and PWSS, we do not know whether $n > 3t$ is necessary (we show it is sufficient). Similarly for three round PVSS, we do not know whether $n = 2t + 1$ is sufficient. We leave these questions as open problems.

2 Model and Definitions

We consider the standard *secure channel* settings where there are n players $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$, who are pairwise connected by perfectly secure channels and an additional broadcast channel is available to all the players. We assume the dealer $\mathbf{D}$ to be any one of the players from $\mathcal{P}$. Our protocol will *also* work for an external dealer where $\mathbf{D}$ is an entity outside the set $\mathcal{P}$. The system is synchronous and the protocol operates in a sequence of rounds, where in each round, a player performs some local computation, sends new messages to his neighbors through private channel and broadcast some information over the broadcast channel and receive message sent by his neighbor in the previous round and receive message sent over broadcast channel in previous round, in that order. The adversary model is same as in [3]. The adversary, denoted as $\mathcal{A}_t$ has *unbounded computing power* and can actively control at most t of the n players (possibly including $\mathbf{D}$) during the protocol. The adversary is centralized and can pool all the information from the players under its control and use them in any manner in its computation. The adversary is *adaptive* [3] and is allowed to corrupt players during protocol execution (and his choice may depend on the data seen so far). A player under the control of $\mathcal{A}_t$ will remain so throughout the protocol and can (mis)behave in an arbitrary manner during protocol execution. The error probability in our protocols is expressed in terms of an error parameter k and the field size $|\mathbb{F}|$ is selected appropriately as a function of k. Note that in [3], the field size $|\mathbb{F}|$ is fixed, which is 2^k and the error probability is of the form $2^{-k+O(\log n)}$. However, in this paper the error probability is fixed, which is 2^{-k} and the field size is $|\mathbb{F}| \geq n^2(n-1)2^k$.

Definition 1 ([3, 7]) *A (n,t)-PWSS scheme for sharing a secret $s \in \mathbb{F}$ is a pair of protocols (***Sh, Rec***) that satisfy the following properties with an negligible error probability (except* SECRECY *which is perfect) 2^{-k} (k is the error parameter), even in the presence of $\mathcal{A}_t$:*

1. TERMINATION: *If* $\mathbf{D}$ *is honest then all honest players will complete* **Sh** *and if the honest players invoke* **Rec***, then each honest player will complete* **Rec***.*

2. SECRECY: *If* $\mathbf{D}$ *is honest and no honest player has yet started* **Rec***, then $\mathcal{A}_t$ has no information about s in information theoretic sense.*

3. *Once all currently uncorrupted players complete protocol* **Sh***, there exists a value $r \in \mathbb{F} \cup \{NULL\}$, such that the following requirements hold:*
   CORRECTNESS: *If the dealer is uncorrupted throughout protocols* **Sh** *and* **Rec** *then r is the shared secret, i.e. $r = s$ and each honest players will output $r = s$ at the end of* **Rec***.*
   WEAK COMMITMENT: *If the dealer is corrupted, then all honest players output either same r or 'NULL' upon completion of protocol* **Rec***.*

Definition 2 *A (n,t)-PVSS scheme for sharing a secret $s \in \mathbb{F}$ is a pair of protocols (***Sh, Rec***) that satisfy the* TERMINATION, SECRECY *and* CORRECTNESS *property of PWSS and a stronger commitment property which is as follows: Once all currently uncorrupted players complete* **Sh***, there exists an $r \in \mathbb{F}$, such that the following requirement holds, with an error probability 2^{-k}:*
STRONG COMMITMENT: *If* $\mathbf{D}$ *is corrupted then each honest player outputs r upon completion of* **Rec***.*

ROUND COMPLEXITY AND EFFICIENCY: As in [5], we define the round complexity of PVSS and PWSS protocol as the number of rounds in its sharing phase. Reconstruction can always be done in a single round wherein every player reveals its entire view generated during sharing phase. A

PVSS (PWSS) protocol is called *efficient* if the total computation and communication performed by all honest players is polynomial in n (the number of players) and error parameter k.

Remark 1 *Using the convention of [5], we assume that if* $\mathbf{D}$ *is discarded in the protocol during sharing phase, then there exists a pre-defined value, say* $s' \in \mathbb{F}$*, which will be taken as* $\mathbf{D}$*'s secret.*

3 Secret Distribution Protocol

We now design a single round protocol called **Secret Distribution**, which we use as a black-box in our PWSS and PVSS protocols. In the protocol, n is at least $2t+1$.

Before proving the properties of protocol **Secret Distribution**, we first pictorially represent the values computed by $\mathbf{D}$.

$M(x), M(0) = s$					
$M(1)$	$M(2)$	$\dots$	$M(j)$	$\dots$	$M(n)$
$f_1(x)$	$f_2(x)$	$\dots$	$f_j(x)$	$\dots$	$f_n(x)$
$f_1(0) = M(1)$	$f_2(0) = M(2)$	$\dots$	$f_j(0) = M(j)$	$\dots$	$f_n(0) = M(n)$
$f_1(1)$	$f_2(1)$	$\dots$	$f_j(1)$	$\dots$	$f_n(1)$
$f_1(2)$	$f_2(2)$	$\dots$	$f_j(2)$	$\dots$	$f_n(2)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$f_1(i)$	$f_2(i)$	$\dots$	$f_j(i)$	$\dots$	$f_n(i)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$f_1(n)$	$f_2(n)$	$\dots$	$f_j(n)$	$\dots$	$f_n(n)$

$$\begin{aligned}
F_1(x) &= f_1(1) + f_2(1)x + f_3(1)x^2 + \dots + f_j(1)x^{j-1} + \dots + f_n(1)x^{n-1} \\
F_2(x) &= f_1(2) + f_2(2)x + f_3(2)x^2 + \dots + f_j(2)x^{j-1} + \dots + f_n(2)x^{n-1} \\
\dots \quad &\dots \quad \dots \\
F_i(x) &= f_1(i) + f_2(i)x + f_3(i)x^2 + \dots + f_j(i)x^{j-1} + \dots + f_n(i)x^{n-1} \\
\dots \quad &\dots \quad \dots \\
F_n(x) &= f_1(n) + f_2(n)x + f_3(n)x^2 + \dots + f_j(n)x^{j-1} + \dots + f_n(n)x^{n-1}
\end{aligned}$$

Lemma 1 *In protocol* **Secret Distribution***, any* $t+1$ *players can jointly reconstruct* s*.*

Proof: The proof follows from the fact that any $t+1$ players will know $t+1$ points on each $f_i(x)$, from the F polynomials given to them. Since each $f_i(x)$ is of degree t, the knowledge of $t+1$ points is sufficient to construct each $f_i(x)$ and hence each $M(i)$. Now using the $M(i)$'s, $M(x)$ and hence s can be reconstructed. □

Lemma 2 *In protocol* **Secret Distribution***, any* t *players will have no information about* $n-t$ *coefficients of* $M(x)$ *in information theoretic sense.*

Protocol Secret Distribution

- **D** selects a random polynomial $M(x)$ over $\mathbb{F}$ of degree $n-1$ such that $M(0) = s$, where s is a secret. **D** then computes $M(1), M(2), \ldots, M(n)$.
- **D** selects n random polynomials $f_1(x), f_2(x), \ldots, f_n(x)$ over $\mathbb{F}$, each of degree t, such that $f_i(0) = M(i), 1 \leq i \leq n$. **D** then evaluates each $f_i(x)$ at $x = 1, 2, \ldots, n$ to form a n tuple $f_i = [f_i(1)\ f_i(2)\ \ldots\ f_i(n)]$
- **D** now constructs an $n \times n$ matrix T where i^{th} column of T contains the n tuple f_i. Using the i^{th} row of T, **D** forms a $n-1$ degree polynomial $F_i(x) = f_1(i) + f_2(i)x + f_3(i)x^2 + \ldots + f_n(i)x^{n-1}$. **D** also selects n random and distinct elements from $\mathbb{F}$, denoted by $\alpha_1, \alpha_2, \ldots, \alpha_n$.
- To P_i, **D** privately delivers $F_i(x)$, α_i and n tuple $[v_{1i}\ v_{2i}\ \ldots\ v_{ni}]$ where $v_{ji} = F_j(\alpha_i), 1 \leq j \leq n$.

PROOF: From Lemma 1, the knowledge of any $t+1$ $F_i(x)$'s is enough to reconstruct $M(x)$. Without loss of generality, consider the set of first t players, denoted by $\mathcal{P}_t$. We now show that $n-t$ coefficients of $M(x)$ will be information theoretic secure, even if the players in $\mathcal{P}_t$ pool the information received during sharing phase.

From the protocol, the players in $\mathcal{P}_t$ will know $F_1(x), F_2(x), \ldots, F_t(x)$. Hence they will collectively know the first t points on each $f_i(x)$, each of degree t. Hence they fall short of one point to recover $f_i(x)$. The players in $\mathcal{P}_t$ will also know the random values $\alpha_1, \alpha_2, \ldots, \alpha_t$ and values of $F_i(x)$, $1 \leq i \leq n$ at $x = \alpha_1, \alpha_2, \ldots, \alpha_t$. The values $F_i(\alpha_j), 1 \leq i \leq t, 1 \leq j \leq t$ does not reveal any new information to these players. However, the values $F_{t+1}(\alpha_j), 1 \leq j \leq t$ gives t new independent equations on $F_{t+1}(x)$. But $F_{t+1}(x)$ is an $n-1$ degree polynomial, so the players in $\mathcal{P}_t$ fall short of $n-t$ points to completely know $F_{t+1}(x)$. Now, the remaining polynomials $F_j(x), t+2 \leq j \leq n$ are linearly dependent on $F_k(x), 1 \leq k \leq t+1$ because each $F_j(x), t+2 \leq j \leq n$ can be derived completely by the knowledge of first $t+1$ $F_k(x)$'s. Hence the points on $F_j(x), t+2 \leq j \leq n$ are linear combination of the points on $F_k(x), 1 \leq k \leq t+1$. So the knowledge of $F_i(\alpha_j), t+2 \leq i \leq n, 1 \leq j \leq t$ does not give any new information to the players in $\mathcal{P}_t$. We now formally prove this. Let us use the following notations:

- $g_i(x)$ is the $t-1$ degree polynomial defined by the first t values of $f_i(x)$. Since $\mathcal{P}_t$ knows first t values of each $f_i(x)$, he can compute each $g_i(x)$.
- $J(x) = (x-1) * (x-2) * \ldots * (x-t)$

Now $F_j(x) = \sum_{i=1}^{n} f_i(j) * x^{i-1}$. Let $k_i(x) = f_i(x) - g_i(x)$. Then

$$\forall x \in \{1, 2, \ldots, t\} : \qquad k_i(x) = 0 \tag{1}$$

As $k_i(x)$ is a t degree polynomial and $\{1, 2, \ldots, t\}$ are its roots, so we get

$$k_i(x) = c_i * (x-1) * (x-2) * \ldots * (x-t) \Longrightarrow k_i(x) = c_i \times J(x) \Longrightarrow c_i = \frac{k_i(x)}{J_i(x)} \tag{2}$$

Now

$$f_i(x) = g_i(x) + k_i(x) \Longrightarrow f_i(x) = g_i(x) + c_i \times J(x) \tag{3}$$

Now the players in $\mathcal{P}_t$ know the points $F_{t+1}(\alpha_j), 1 \leq j \leq t$. These points can be expressed as:

$$\begin{aligned} \forall j \in \{\alpha_1 \dots \alpha_t\} : \qquad F_{t+1}(j) & = \textstyle\sum_{i=1}^{n} f_i(t+1) * j^{i-1} \\ & = \textstyle\sum_{i=1}^{n} (g_i(t+1) + c_i * J(t+1)) * j^{i-1} \text{ From Equation (3)} \end{aligned}$$

We now show that the points $F_k(\alpha_j), t+2 \leq k \leq n, 1 \leq j \leq t$ does not give any new information to the players in $\mathcal{P}_t$. Consider any $k \in \{t+2, t+3, \dots, n\}$ and any $j \in \{\alpha_1, \alpha_2, \dots, \alpha_t\}$. Now similar to the last equation, we have

$$F_k(j) = \sum_{i=1}^{n} (g_i(k) + c_i * J(k)) * j^{i-1} \tag{4}$$

Now $F_k(j)$ can be expressed as

$$\begin{aligned} F_k(j) &= \sum_{i=1}^{n} g_i(k) * j^{i-1} - \frac{J(k)}{J(t+1)} * \sum_{i=1}^{n} g_i(t+1) * j^{i-1} \\ & \quad + \frac{J(k)}{J(t+1)} * \sum_{i=1}^{n} (g_i(t+1) + c_i * J(t+1)) * j^{i-1} && (5) \\ &= \sum_{i=1}^{n} g_i(k) * j^{i-1} - \frac{J(k)}{J(t+1)} * \sum_{i=1}^{n} g_i(t+1) * j^{i-1} \\ & \quad + \frac{J(k)}{J(t+1)} * F_{t+1}(j) && (6) \end{aligned}$$

We see that in (6) all the terms are known to the players in $\mathcal{P}_t$ and hence the t points on the polynomials $F_{t+2}(x), F_{t+3}(x), \dots, F_n(x)$ can be computed from the t points on $F_{t+1}(x)$ and the first t $F_i(x)$'s only. Hence the players in $\mathcal{P}_t$ fall short of $n-t$ values to completely recover $F_{t+1}(x)$ and hence $M(x)$. □

4 Single Round PWSS with $n = 3t + 1$

We now design a single round PWSS protocol called **1-Round-PWSS** with $n = 3t + 1$ and error probability bounded by 2^{-k}, where $|\mathbb{F}| \geq n^2(n-1)2^k$. From [4], one round perfect WSS is possible iff $n > 4t$. Thus probabilistically relaxing the conditions of WSS helps to increase the fault tolerance of 1-round WSS. The protocol uses protocol **Secret Distribution** given in Section 3 as black-box.

Remark 2 *Let $i_1, i_2, \dots, i_k$ denote the index of the rows which are filled in matrix T during step 4(b) of local computation of protocol* **1-Round-PWSS**. *Let $f'_j(i_1), f'_j(i_2), \dots, f'_j(i_k)$ denote the values in the j^{th} column of the matrix T. Then j^{th} column is said to be t-consistent if there exists a polynomial $w_j(x)$ of degree at most t such that $w_j(i_1) = f'_j(i_1), w_j(i_2) = f'_j(i_2), \dots, w_j(i_k) = f'_j(i_k)$.*

Protocol 1-Round-PWSS: A Single Round PWSS Protocol with $n = 3t + 1$

Sharing Phase: **D** executes protocol **Secret Distribution**. So P_i obtains the following from **D**: polynomial $F_i(x)$, the random secret value α_i and the n tuple $[v_{1i} \; v_{2i} \; \ldots \; v_{ni}]$ where $v_{ji} = F_j(\alpha_i), 1 \leq j \leq n$.
Reconstruction Phase: P_i broadcasts whatever it received during sharing phase; i.e., $F_i'(x), \alpha_i'$ and $[v_{1i}' \; v_{2i}' \; \ldots \; v_{ni}']$.
Local Computation (by each player)

1. Construct a directed graph G called *approval graph* over the set of n players, such that there exists an arc (P_k, P_j) (k can be equal to j) in G iff $F_j'(\alpha_k') = v_{jk}'$, which indicates that P_k approves the polynomial $F_j'(x)$ broadcasted by P_j. Since all information are broadcasted, every (honest) player constructs the same graph G.
2. Each player whose in-degree (in G) is at least $n - t$ are included in a set $CORE$. Next, players in $CORE$ whose polynomials are not approved by at least $n - t$ players in $CORE$ are removed from $CORE$. This process continues until no more players can be removed from $CORE$. Let $\overline{CORE} = \mathcal{P} \setminus CORE$.
3. Player $P_j \in CORE$, who has an arc (P_j, P_k) to player $P_k \in \overline{CORE}$ in G is removed from $CORE$, but not included in $\overline{CORE}$. If the removal of P_j from $CORE$ reduces the in-degree of some other player $P_l \in CORE$ to less than $n - t$ then remove P_l from $CORE$. This process continues, until no more player can be removed from $CORE$.
4. If $|CORE| < n - t$, then output NULL. Else try to reconstruct the original $n \times n$ matrix T (constructed by **D** during sharing phase) by doing the following:
   (a) Insert the coefficients of $F_j'(x)$ (in increasing power of x) as the j^{th} row of T, if $P_j \in CORE$. Since $|CORE| \geq n - t$, at least $2t + 1$ rows will be inserted in T.
   (b) Check if each column of T is t-consistent (**Remark 2**). If not then output NULL. Else recover $M'(1), M'(2), \ldots, M'(n)$ by interpolating the values of each column and recover $M'(x)$ and compute $s' = M'(0)$.

Claim 1 *Let* **D** *be honest. Assume that P_i is an honest player and some corrupted player P_j broadcasts $F_j'(x) \neq F_j(x)$ in reconstruction phase. Then the probability that the arc (P_i, P_j) may be present in G is at most 2^{-k}.*

PROOF: Let **D** be honest and a corrupted P_j broadcasts $F_j'(x)$ ($\neq F_j(x)$) during reconstruction phase, such that there exists an arc (P_i, P_j) in G, where P_i is honest. This implies that $F_j'(x) \neq F_j(x)$ broadcasted by P_j is approved by an honest P_i. Let π_{ij} be the probability that P_j is approved by honest P_i. This means that the adversary could ensure that $F_j(\alpha_i) = F_j'(\alpha_i)$ with probability π_{ij}. Since there are only $n - 1$ points at which $F_j(x)$ and $F_j'(x)$ intersect and α_i's are randomly selected from $\mathbb{F}$, we have $\pi_{ij} \leq \frac{n-1}{|\mathbb{F}|}$. Thus total probability that adversary can find P_i, P_j such that corrupted P_j will be approved by honest P_i is at most $\sum_{i,j} \pi_{ij} \leq \frac{n^2(n-1)}{|\mathbb{F}|}$. Since $\mathbb{F}$ is chosen such that $|\mathbb{F}| \geq n^2(n-1)2^k$, it follows that arc (P_i, P_j) may be present in G with a probability at most 2^{-k}. □

Claim 2 *If* **D** *is honest, then except with probability at most 2^{-k}, an honest P_i is present in $CORE$*

PROOF: If **D** is honest, then he will distribute consistent information to all the players. So a honest player will have an incoming arc in G from all the honest players (at least $n - t$). Now the only reason that an honest player P_i is removed from $CORE$ is that there exists an arc (P_i, P_j) in G, where P_j(corrupted) $\in \overline{CORE}$. However, from Claim 1, this can happen with a probability at most 2^{-k}. □

Lemma 3 **1-Round-PWSS** *satisfy correctness property with error probability at most* 2^{-k}.

Proof: If **D** is honest, then from Claim 2, each honest player will be present in $CORE$ with very high probability. Also by Claim 1, a corrupted P_j broadcasting incorrect $F'_j(x) \neq F_j(x)$, will be excluded from $CORE$, with probability more than $1-2^{-k}$. So with probability more than $1-2^{-k}$, all the columns of T will be t-consistent and hence m will be reconstructed. However, if a corrupted P_j who broadcasted $F'_j(x) \neq F_j(x)$, is included in $CORE$, then all the columns of partially filled matrix T will not be t-consistent. This is because at least one of the coefficients of $F'_j(x)$ will be different from $F_j(x)$ and each column of partially filled T contains at least $2t+1$ correct values, corresponding to honest players. This causes NULL to be output which happens with probability less than 2^{-k}. □

Claim 3 *If* **D** *is corrupted and* $|CORE| \geq n-t$, *then at the end of the sharing phase there exists a unique secret* $s' \in \mathbb{F} \cup \{NULL\}$ *defined by the honest players in CORE.*

Proof: If **D** is corrupted and $|CORE| \geq n-t$ then it contains at least $(n-t)-t \geq t+1$ honest players. Now polynomial $F'_i(x)$ possessed by honest player $P_i \in CORE$ can be used to fill up the i^{th} row of T. Since $CORE$ contains at least $t+1$ honest players, at least $t+1$ rows of T will be occupied. Now consider the matrix T with only the coefficients of the polynomials corresponding to the honest players inserted in it. There are two possible cases: **(a) The values along each of the** n **columns are** t**-consistent**: In this case, the values along each of the n columns on interpolation will result in a t degree polynomial, $f'_i(x), 1 \leq i \leq n$ for i^{th} column. Let $M'(i) = f'_i(0)$, then a unique $n-1$ degree polynomial $M'(x)$ can be interpolated from $M'(i), 1 \leq i \leq n$. The unique secret defined by the honest players in $CORE$ is $s' = M'(0)$. **(b) The values along at least one of the** n **columns is not** t**-consistent**: In this case, the defined value s' is NULL. □

Lemma 4 *Protocol* **1-Round-PWSS** *satisfies weak commitment property.*

Proof: If **D** is corrupted then the following cases can happen: (a) $|CORE| < n-t$: In this case **D** has not defined an unique secret and hence is discarded. (b) $|CORE| \geq n-t$: From Claim 3, $CORE$ contains a set $\mathcal{C}$ of at least $t+1$ honest players. Moreover all the honest players in $CORE$ define a unique value $s' \in \mathbb{F} \cup \{NULL\}$ at the end of sharing phase. Also, according to the protocol, any player in $CORE$ cannot have an outgoing arc to any other player outside $CORE$. But the corrupted players (at most t) in $CORE$, along with the players outside $CORE$ (which could be at most t) may define some other secret s'' during reconstruction phase. However, if this occurs then size of the $CORE$ would be at most $2t < (n-t)$. Hence, the corrupted players cannot change the commitment from s' to s'' during reconstruction phase. However, the corrupted players could behave such that $NULL$ gets reconstructed (this happens if the values broadcasted by the corrupted players in $CORE$ are not t-consistent with the values corresponding to the honest players in $CORE$). Hence weak commitment on s' holds. □

Theorem 1 *If* $|\mathbb{F}| \geq n^2(n-1)2^k$, *then protocol* **1-Round-PWSS** *is an* (n,t) *PWSS protocol with an error probability bounded by* 2^{-k}. *The protocol communicates* $O((k+\log n)n^2)$ *bits and broadcasts* $O((k+\log n)n^2)$ *bits.*

Proof: Properties of PWSS follows from Lemma 2, Lemma 3 and Lemma 4. During sharing phase, **D** communicates n^2 field elements. Since each field element can be represented by $\log(|\mathbb{F}|)$ bits and $|\mathbb{F}| = n^2(n-1)2^k$, the communication complexity is $O((k + \log n)n^2)$ bits. During reconstruction phase, n^2 field elements are broadcasted. So overall $O((k + \log n)n^2)$ bits are broadcasted. $\square$

Remark 3 *From Lemma 2, $n - t$ coefficients of $M(x)$ are information theoretically secure. So* **D** *can share $n - t = \Theta(n)$ secrets incurring the same communication complexity. Thus the information rate of our single round PWSS protocol is $O(n)$.*

5 Single Round PVSS with $n = 4$ and $t = 1$

In [5] it is shown that there exists a single round $(5, 1)$ perfect VSS. We now design a single round $(4, 1)$ PVSS protocol called **1-Round-PVSS**, thus showing that probabilistically relaxing the conditions of VSS helps to increase the fault tolerance. The protocol is designed using the protocol **Secret Distribution** given in Section 3 as a black-box and is similar to our single round PWSS.

Let the players be denoted by P_1, P_2, P_3, P_4, where P_1 is dealer and s is the secret. The secrecy of **1-Round-PVSS** follows from the secrecy of **1-Round-PWSS**. We now show that the protocol satisfies correctness and strong commitment property.

Protocol 1-Round-PVSS: A Single Round PVSS Protocol with $n = 4$ and $t = 1$

Sharing Phase: Same as the sharing phase of protocol **1-Round-PWSS**, with $n = 4$ and $t = 1$.
Reconstruction Phase: Player P_i, except P_1, who is the dealer, broadcasts $F'_i(x), \alpha'_i$ and $[v'_{1i}\ v'_{2i}\ v'_{3i}\ v'_{4i}]$.
Local Computation by players $P_i, 2 \leq i \leq 4$: Construct the *approval graph* G (as in protocol **1-Round-PWSS**) over P_2, P_3 and P_4, using the information broadcasted by P_2, P_3 and P_4 during reconstruction phase. All the players who have in-degree at least two in G are included in $CORE$. Remove all the players from $CORE$ who do not have an in-coming arc (in G) from at least two players in $CORE$. Then do the following:

1. If $|CORE| = 0$, then construct $M'(x)$ using $F'_2(x)$ and $F'_3(x)$, reconstruct $s' = M'(0)$ and terminate.
2. If $|CORE| = 2$, then construct $M'(x)$ using the $F'(x)$ polynomials broadcasted by the players in $CORE$, reconstruct $s' = M'(0)$ and terminate.
3. If $|CORE| = 3$ and each player in $CORE$ has an incoming arc from all the players in $CORE$, then construct $M'(x)$ using the $F'(x)$ polynomials broadcasted by the players in $CORE$ and reconstruct $s' = M'(0)$.
4. If $|CORE| = 3$, but at least one player in $CORE$ do not have an incoming arc from all the players in $CORE$, then construct $M'(x)$ using $F'_2(x)$ and $F'_3(x)$ and reconstruct $s' = M'(0)$.

Claim 4 *Protocol* **1-Round-PVSS** *satisfies correctness property with very high probability.*

Proof: If **D** is honest, then among the remaining three players at most one can be corrupted. Let P_4 be the corrupted player among P_2, P_3 and P_4. Then P_2 and P_3 will be present in $CORE$ (since P_2 (P_3) will have have incoming arcs from P_2 and P_3 in G). From Claim 1, if P_4 is also present in $CORE$, then with very high probability, it has broadcasted $F'_4(x) = F_4(x)$. The proof now follows using similar argument as in Lemma 3. $\square$

Claim 5 *Protocol* **1-Round-PVSS** *satisfies strong commitment property.*

PROOF: We have to only consider the case when **D** (P_1) is corrupted. In this case, P_2, P_3 and P_4 are honest and behave correctly in reconstruction phase (recall that **D** is not allowed to participate in reconstruction phase). Note that the $F'(x)$ polynomials corresponding to any two honest players define a unique secret s' because here $t = 1$. Now we divide our argument depending upon the size of $CORE$. If $|CORE| = 0$, then it implies that **D** has not given consistent values to anybody during sharing phase. So secret s' is reconstructed from $F'_2(x)$ and $F'_3(x)$, implying that s' is the unique secret defined by **D** in the sharing phase and is reconstructed (in reconstruction phase) irrespective of the behavior of the corrupted player (**D**). The similar argument holds for the case when $|CORE| = 3$ and at least one player in $CORE$ do not have an incoming arc from all the players in $CORE$. For the case when $|CORE| = 2$ or $|CORE| = 3$, with each player in $CORE$ having an incoming arc from all the players in $CORE$, the committed secret is the one defined by the polynomials of the players in $CORE$. □

6 Two Round PVSS with $n = 3t + 1$

We now design a two round PVSS protocol called **2-Round-PVSS** for $n = 3t + 1$. The upper bound for error probability is 2^{-k} and $|\mathbb{F}| = n^2(n-1)2^k$. The protocol uses protocol **1-Round-PWSS** of Section 4 as a black-box. In [5], it is shown that 2 round (n, t) perfect VSS exists iff $n \geq 4t + 1$. Thus allowing a negligible error probability significantly increases the fault tolerance of two round VSS.

The principle behind our *two* round PVSS protocol is similar to the *three* round *perfect* (where error probability is 0) VSS protocol proposed in [4]. The secret s is hidden by **D** in a bivariate polynomial $F(x, y)$ and each player P_i gets the univariate polynomials $F(x, i)$ and $F(i, y)$. Then every pair of players compare their common shares by "binding" them with a random pad and broadcasting them. In the reconstruction phase the random pads are revealed, allowing the players to compute the shares and finally reconstruct the secret. To ensure that P_i discloses the same random pads in reconstruction phase, P_i shares a random field element using **1-Round-PWSS** and chooses his random pads as *points on the respective polynomials* which are given to the individual players as part of protocol **1-Round-PWSS**. During reconstruction phase, players whose instance of protocol **1-Round-PWSS** fails, get disqualified from the main protocol. On the other hand, players whose instance of single round PWSS succeeds, disclose their original pads. Note that if **D** is corrupted, then he can distribute inconsistent values to the honest players during first round. So when the honest players compare their common shares during second round, they may find them to be inconsistent. In the three round perfect VSS protocol of [4], such inconsistencies are resolved by **D** during third round, which cannot be done here because sharing phase has now only two rounds. However, inspite of this, our protocol satisfies the requirement of PVSS. Before discussing the proofs of protocol **2-Round-PVSS**, we first give the following definition.

Definition 3 *In protocol* **2-Round-PVSS**, *we say that a player P_i is consistent with bivariate polynomial $F(x, y)$ if the polynomials given to P_i during sharing phase, namely $f_i(x)$ and $g_i(y)$ lie on $F(x, y)$; i.e., $f_i(x) = F(x, i)$ and $g_i(y) = F(i, y)$.*

Protocol 2-Round-PVSS: A Two Round PVSS with $n = 3t + 1$

Sharing Phase:

Round 1:

- $\mathbf{D}$ chooses a random bivariate polynomial $F(x, y)$ over $\mathbb{F}$ of degree t in each variable such that $F(0, 0) = s$. $\mathbf{D}$ privately sends to player P_i the polynomials $f_i(x) = F(x, i)$ and $g_i(y) = F(i, y)$.
- Player $P_i, 1 \leq i \leq n$, acting as a dealer, starts single round PWSS protocol **1-Round-PWSS**^{P_i} in order to share a random value $s_i \in \mathbb{F}$. Let the polynomials distributed by P_i to the n players in **1-Round-PWSS**^{P_i} be denoted by $F_1^{iW}(x), F_2^{iW}(x), \ldots, F_n^{iW}(x)$, where $P_j, 1 \leq j \leq n$ receives $F_j^{iW}(x)$.

Round 2: Player $P_i, 1 \leq i \leq n$ broadcasts the following: $a_{ij} = f_i(j) + F_j^{iW}(0)$ and $b_{ij} = g_i(j) + F_i^{jW}(0)$.
/* $F_j^{iW}(0)$ denotes constant term of the polynomial $F_j^{iW}(x)$ received by P_j from P_i in **1-Round-PWSS**^{P_i}. */

Local Computation (by each player):

- Player P_i and P_j are said to be consistent if $a_{ij} = b_{ji}$ and $b_{ij} = a_{ji}$. Form a consistency graph G over the set of n players, where there exists an edge between P_i and P_j if they are consistent with each other. Since a_{ij}'s and b_{ij}'s are public information, same G will be constructed by all (honest) players.
- Construct a set $CORE^{Sh}$ ($= \emptyset$ initially) and add P_i in $CORE^{Sh}$ if degree of P_i (in G) is at least $n-t$. Remove P_j from $CORE^{Sh}$ if P_j is not consistent with at least $n - t$ players in $CORE^{Sh}$. Continue this process till no more players can be removed. If $|CORE^{Sh}| < n - t$ then discard $\mathbf{D}$ and terminate the protocol.

Reconstruction Phase: Only the players in $CORE^{Sh}$ participate.

- For each $P_i \in CORE^{Sh}$, concurrently run the reconstruction phase of **1-Round-PWSS**^{P_i}. If reconstruction phase fails, then remove P_i from $CORE^{Sh}$.
- If the reconstruction phase of **1-Round-PWSS**^{P_i} does not fail, then the polynomials $F_j^{iW}(x), 1 \leq j \leq n$, distributed by P_i in **1-Round-PWSS**^{P_i} to the n players are recovered. Now compute $f_i(j) = a_{ij} - F_j^{iW}(0)$, $1 \leq j \leq n$ using the values a_{ij}, which P_i broadcasted during second round of sharing phase. If there exists a polynomial $f_i(x)$ of degree at most t passing through the $f_i(j)$'s, then include P_i in a set $CORE^{Rec}$ ($= \emptyset$ initially)
- Consider all players from $CORE^{Rec}$ and use their reconstructed $f_i(x)$'s to construct a bivariate polynomial $F'(x, y)$. If $F'(x, y)$ is of degree at most t in both x and y, then reconstruct $s' = F'(0, 0)$. Otherwise, output some standard (predefined) value $s^* \in \mathbb{F}$.

Lemma 5 *If* $\mathbf{D}$ *is honest then except with probability* 2^{-k}*,* $CORE^{Rec}$ *contains each honest player, consistent with the bivariate polynomial* $F(x, y)$ *defined by* $\mathbf{D}$*. Moreover even a dishonest player is in* $CORE^{Rec}$ *is consistent with* $F(x, y)$*.*

PROOF: If $\mathbf{D}$ is honest, then the information received by each honest player during sharing phase will be consistent with bivariate polynomial $F(x, y)$ and hence they will be pairwise consistent and will be included in $CORE^{Sh}$. From Lemma 3, for each honest player P_i, **1-Round-WSS**^{P_i} will succeed with probability at least $(1 - 2^{-k})$ and their corresponding recovered polynomials $f_i(x)$ will be t-consistent. So all the honest players (at least $2t + 1$) will be in $CORE^{Rec}$ and will define $F(x, y)$.

Now consider a dishonest player $P_j \in CORE^{Rec}$. This implies that P_j is consistent with at least $(n - t) - t \geq t + 1$ honest players in $CORE^{Rec}$, who define the bivariate polynomial $F(x, y)$. Also $P_j \in CORE^{Rec}$ implies that **1-Round-PWSS**^{P_j} is successful and the recovered $f_j(x)$ is t-

consistent. Since **1-Round-PWSS**^{P_j} is successful, it implies that the polynomials $F_i^{jW}(x), 1 \leq i \leq n$ given by P_j to the individual players during PWSS are recovered correctly. Since P_j is consistent with at least $t+1$ honest players in $CORE^{Rec}$, who define $F(x,y)$ and since recovered $f_j(x)$ is t-consistent, it follows that recovered $f_j(x)$ is consistent with $F(x,y)$. □

Claim 6 *If* **D** *is dishonest and does not get disqualified during sharing phase, then $CORE^{Sh}$ contains at least $t+1$ honest players. Moreover, except with probability 2^{-k}, each honest player in $CORE^{Sh}$ will be present in $CORE^{Rec}$.*

Proof: If **D** is dishonest and does not get disqualified during sharing phase then it implies that $CORE^{Sh}$ contains at least $n-t$ players, of which $(n-t)-t \geq t+1$ are honest. Now a player P_i gets removed from $CORE^{Rec}$ in only two cases: (a) the reconstruction phase of **1-Round-PWSS**^{P_i} fails or (2) the reconstruction phase of **1-Round-PWSS**^{P_i} is successful but the resulting polynomial $f_i(x)$ is of degree larger than t. However, from the properties of single round PWSS, for an honest P_i, the first event can occur with probability at most 2^{-k}, where as the second event cannot occur at all. Hence, each honest player (in fact at least $t+1$ honest players) present in $CORE^{Sh}$ will also be present in $CORE^{Rec}$ with very high probability. □

Lemma 6 *If* **D** *is dishonest and does not get disqualified during sharing phase, then except with probability 2^{-k}, the protocol satisfies strong commitment property.*

Proof: From Claim 6, if **D** is dishonest and does not get disqualified during sharing phase, then except with probability 2^{-k}, each honest player (at least $t+1$) of $CORE^{Sh}$ will also be present in $CORE^{Rec}$. Now there are three possible cases:

1. $CORE^{Sh}$ contains exactly $t+1$ honest players: In this case $|CORE^{Sh}| = 2t+1$ and it contains t corrupted players. It also implies that the honest players in $CORE^{Sh}$ are consistent with each other and define a bi-variate polynomial $F'(x,y)$ of degree at most t in both x and y. Moreover, the corrupted players in $CORE^{Sh}$ are also consistent with these $t+1$ honest players. From Claim 6, these $t+1$ honest players will be present in $CORE^{Rec}$. Now if the remaining t corrupted players in $CORE^{Sh}$ are also present in $CORE^{Rec}$, it implies that these corrupted players are also consistent with $F'(x,y)$ (following the argument provided for the second part of Lemma 5). So in reconstruction phase, $s' = F'(0,0)$ will be reconstructed.

2. $CORE^{Sh}$ contains more than $t+1$ honest players, who are all consistent with each other: Similar to previous case, here also all honest players in $CORE^{Sh}$ define a unique bi-variate polynomial $F'(x,y)$. Also if a corrupted player is present in $CORE^{Sh}$, then it implies that it is consistent with at least $(n-t)-t \geq t+1$ honest players in $CORE^{Sh}$ and hence with $F'(x,y)$. Now following the same argument given in the previous case $s' = F'(0,0)$ will be reconstructed.

3. $CORE^{Sh}$ contains more than $t+1$ honest players, but are not consistent with each other: Hence the $f_i(x)$ polynomials of all honest players in $CORE^{Sh}$ does not define a bivariate polynomial of degree at most t in both x and y. In this case, **D** has committed a secret which is a predefined (standard) value s^* from $\mathbb{F}$. From Claim 6, each honest player from

$CORE^{Sh}$ will be present in $CORE^{Rec}$, except with probability at most 2^{-k}. Now irrespective of whether the corrupted players in $CORE^{Sh}$ are present in $CORE^{Rec}$ or not, the $f_i(x)$ polynomials corresponding to the honest players in $CORE^{Rec}$ will not reconstruct a bivariate polynomial of degree at most t in both x and y. Hence s^* will be reconstructed and so the strong commitment on s^* is satisfied. □

Remark 4 *Note that the third case in the proof of Lemma 6 is different from the* WEAK COMMITMENT *property of PWSS. In the* WEAK COMMITMENT *property, there exists a $r \in \mathbb{F}$ which is defined after the sharing phase, such that depending upon the the behavior of corrupted players during reconstruction phase, either r or NULL is reconstructed. On the other hand, in the third case of Lemma 6, the shares given by* **D** *to the players in $CORE^{Sh}$ does not define a unique secret. So it can be viewed as* **D** *committing a fixed $s^* \in \mathbb{F}$. Now irrespective of the behavior of the corrupted players during reconstruction phase,* **D***'s commitment on s^* is not violated.*

Lemma 7 *Protocol* **2-Round-PVSS** *satisfies perfect secrecy.*

PROOF: We have to only consider the case when **D** is dishonest. The proof follows from the properties of bivariate polynomial of degree t. Without loss of generality, assume that the first t players are under the control of $\mathcal{A}_t$. Let $\text{View}^k_{\mathcal{A}}, 1 \leq k \leq 2$ denote the view of $\mathcal{A}_t$ at the end of round k of sharing phase. During first round of sharing phase, $\mathcal{A}_t$ will know about the polynomials $F(x,i), 1 \leq i \leq t$ and $F(i,y), 1 \leq i \leq t$. With these polynomials $\mathcal{A}_t$ can form $t(t+1)+t = t^2+2t$ independent equations on the coefficients of $F(x,y)$. Thus $\mathcal{A}_t$ falls short of one independent equation to completely know $F(x,y)$ and hence s.

Now during first round, each player P_i executes the protocol **1-Round-WSS**^{P_i}. Thus $\mathcal{A}_t$ also knows the polynomials $F^{jW}_1(x), F^{jW}_2(x), \ldots, F^{jW}_t(x), t+1 \leq j \leq n$ given by the honest players to the corrupted players. Note that for all $j, 1 \leq j \leq t$, the polynomials $F^{jW}_1(x), F^{jW}_2(x), \ldots, F^{jW}_t(x)$ are used by player P_j to blind values which are already known to $\mathcal{A}_t$ and hence does not add any new information to the knowledge of $\mathcal{A}_t$. Also from SECRECY property of **1-Round-PWSS** (see Theorem 1 and Lemma 2), at least $n-t$ coefficients of $F^{jW}_{t+1}(x)$ (and hence $F^{jW}_{t+2}(x), \ldots, F^{jW}_n(x)$), which are distributed by players $P_j, t+1 \leq j \leq n$ to players $P_k, t+1 \leq k \leq n$ during the execution of **1-Round-WSS**^{P_j} are information theoretically secure. Hence at the end of round 1 of sharing phase, it holds that for every $P_j, P_k, t+1 \leq j,k \leq n$, the entropy $H(F(x,j)|View^1_{\mathcal{A}}) = \log(|\mathbb{F}|) = H(F^{kW}_j(x)|View^1_{\mathcal{A}}) = H(F^{kW}_j(0)|View^1_{\mathcal{A}}) = \log(|\mathbb{F}|)$.

During round 2, each player $P_j, 1 \leq j \leq n$ reveals the values $F(k,j) + F^{jW}_k(0), 1 \leq k \leq n$. Since for each $t+1 \leq j,k \leq n$, the entropy $H(F^{kW}_j(0)|View^1_{\mathcal{A}}) = \log(|\mathbb{F}|)$ and $H(F(x,j)|View^1_{\mathcal{A}}) = \log(|\mathbb{F}|)$, it is still the case that for each $P_j, t+1 \leq j \leq n$, the entropy $H(F(x,j)|View^2_{\mathcal{A}}) = \log(|\mathbb{F}|)$ and hence $H(F(0,0)|View^2_{\mathcal{A}}) = \log(|\mathbb{F}|)$. Hence perfect secrecy follows. □

Theorem 2 *If $|\mathbb{F}| = n^2(n-1)2^k$, then protocol* **2-Round-PVSS** *is an efficient two round (n,t) PVSS protocol, with an error probability of at most 2^{-k}. The protocol communicates $O((k+\log n)n^3)$ bits and broadcasts $O((k+\log n)n^3)$ bits.*

PROOF: The secrecy of **2-Round-PVSS** follows from Lemma 7. The "correctness" and "Strong Commitment" properties follow from Lemma 5 and Lemma 6 respectively. Protocol **2-Round-PVSS** runs n instances of protocol **1-Round-PWSS**. Now from Theorem 1, each execution of protocol **1-Round-PWSS** communicates $O((k + \log n)n^2)$ bits and broadcasts $O((k + \log n)n^2)$ bits. Hence protocol **2-Round-PVSS** communicates $O((k+\log n)n^3)$ bits and broadcasts $O((k+\log n)n^3)$ bits. Hence the information rate is $O(n^3)$. □

7 Three Round PWSS with $n = 2t + 1$

We design a three round PWSS protocol called **3-Round-PWSS** which works with error probability of 2^{-k}, where $n = 2t+1$ and $|\mathbb{F}| \geq n^2(n-1)2^k$. From [4], 3 round perfect WSS is possible iff $n > 3t$. Thus, probabilistically relaxing the conditions of WSS helps to increase the fault tolerance of three round WSS protocols significantly. In the protocol, we use the following definition:

Definition 4 (α_j-consistent) *Let $F(x)$ be a polynomial of degree $n-1$ over $\mathbb{F}$. Let α_j and v be two elements in $\mathbb{F}$. Then v is said to be α_j consistent with $F(x)$ if $F(\alpha_j) = v$.*

Theorem 3 *In protocol* **3-Round-PWSS***, the following holds:*

1. **D** *is honest and*
   (a) If P_i is honest, then $P_i \in NB$ and V_i^{Sh} and $V_{FR_i}^{Rec}$ are same atleast at $(t+1)$ locations.
   (b) If P_i is dishonest, $P_i \in NB$ and broadcasted at least one of the polynomial $F_i(x)$ or $R_i(x)$ incorrectly in reconstruction phase, then V_i^{Sh} and $V_{FR_i}^{Rec}$ mismatches atleast at $(t+1)$ locations with probability more than $(1-2^{-k})$.

2. **D** *is dishonest and if P_i is honest and $P_i \in NB$ then V_i^{Sh} and $V_{FR_i}^{Rec}$ matches atleast at $(t+1)$ locations with probability more than $(1-2^{-k})$.*

Proof: Since $n = 2t+1$, among n players at least $(t+1)$ are honest players. It is obvious that when both **D** and P_i are honest then $P_i \in NB$ because P_i will broadcast correct information during second round. Also V_i^{Sh} and $V_{FR_i}^{Rec}$ will have 1 at $(t+1)$ locations corresponding to $(t+1)$ honest players. Hence they will match at atleast $(t+1)$ locations. This proves 1(a).

Now consider the case when **D** is honest, P_i is dishonest and $P_i \in NB$. This implies that **D** is satisfied by the values broadcasted by P_i during second round and hence all the honest players (at least $t+1$) will respond with "Accept". So V_i^{Sh} will contain 1 at least at $(t+1)$ locations corresponding to honest players. Now if P_i discloses at least one of the polynomials $F_i(x)$ and $R_i(x)$ incorrectly during reconstruction phase, then with very high probability, at least one of the vector $V_{F_i(x)}^{Rec}$ or $V_{R_i(x)}^{Rec}$ will contain zero at a location corresponding to an honest player. Specifically, if P_i broadcasts incorrect $F_i'(x) \neq F_i(x)$ $(R_i'(x) \neq R_i(x))$, then $V_{F_i(x)}^{Rec}$ $(V_{R_i(x)}^{Rec})$ may contain 1 at the j^{th} position, corresponding to an honest player P_j, provided $F_i'(\alpha_j) = F_i(\alpha_j) = v_{ij}$. However, this can happen with probability $\pi_{ij} \leq \frac{n-1}{|\mathbb{F}|-n}$. Thus total probability that adversary can find P_i, P_j such that a corrupted player P_i will be approved by an honest player P_j is at most $\sum_{i,j}\pi_{ij} \leq \frac{n^2(n-1)}{|\mathbb{F}|-n}$. Since $\mathbb{F}$ is chosen such that $|\mathbb{F}| = n^2(n-1)2^k$, it follows that if P_i discloses incorrect $F_i(x)$ $(R_i(x))$ then each of the $(t+1)$ locations corresponding to the honest player will contain zero in $V_{F_i(x)}^{Rec} \otimes V_{R_i(x)}^{Rec}$

Protocol 3-Round-PWSS: A Three Round PWSS Protocol with $n = 2t + 1$

Sharing Phase

Round 1: - **D** executes protocol **Secret Distribution** of Section 3 with a restriction that each random $\alpha_i \in \mathbb{F} - \{0, 1, \ldots, n-1\}$. Hence P_i gets the polynomial $F_i(x)$ of degree $n-1$, the random value α_i and the n tuple $[v_{1i}, v_{2i}, \ldots, v_{ni}]$ from **D**, where $v_{ji} = F_j(\alpha_i),\ 1 \leq j \leq n$. In addition, **D** also gives another random $n-1$ degree polynomial $R_i(x)$ and n tuple $[r_{1i}, r_{2i}, \ldots, r_{ni}]$ to P_i, where $r_{ji} = R_j(\alpha_i),\ 1 \leq j \leq n$.

Round 2: Player P_i chooses a random $d_i \in \mathbb{F} \setminus \{0\}$ and broadcasts $B_i(x) = d_i F_i(x) + R_i(x)$, along with d_i.

Round 3: With respect to the values broadcasted by P_i in **Round 2**, **D** along with the n players do the following:

- **D** checks the correctness of the P_i's broadcasted information. **D** also checks $d_i v_{ij} + r_{ij} \overset{?}{=} B_i(\alpha_j)$, for $1 \leq j \leq n$. If **D** finds any inconsistency, he broadcasts $F_i(x)$.

- Player P_j, $1 \leq j \leq n$ broadcasts "Accept" or "Reject", depending upon whether $d_i v_{ij} + r_{ij} = B_i(\alpha_j)$ or not.

Local Computation (by each player):

1. Divide the set of players in two sets. Each player P_i whose $F_i(x)$ is broadcasted by **D** during third round are included in a set B. The remaining players are included in another set NB.
2. If $|B| > t$ then discard **D** and terminate the protocol.
3. For each $P_i \in NB$, construct an n length bit vector, denoted by V_i^{Sh}, where the $j^{th}, 1 \leq j \leq n$ bit is 1(0), if P_j has broadcasted "Accept" ("Reject") during **Round 3** in response to $B_i(x)$ broadcasted by P_i during second round. The vectors V_i^{Sh} are public as they are constructed using broadcasted information. If there exist $P_i \in NB$ such that V_i^{Sh} contains at least $t+1$ 0's, then discard **D** and terminate the protocol.

Reconstruction Phase: Each $P_i \in NB$ broadcasts $F_i'(x)$, $R_i'(x)$, $[v_{1i}', v_{2i}', \ldots, v_{ni}']$, $[r_{1i}', r_{2i}', \ldots, r_{ni}']$ and α_i'.

Local Computation (by each player):

1. For the polynomial $F_i'(x)$ broadcasted by $P_i \in NB$, construct an n bit response $V_{F_i(x)}^{Rec}$ where the j^{th} bit of $V_{F_i(x)}^{Rec}$ contains 1(0) if $F_i'(\alpha_j') = v_{ij}'$ $(F_i'(\alpha_j') \neq v_{ij}')$. Similarly, construct the response vector $V_{R_i(x)}^{Rec}$ corresponding to $R_i(x)$. Finally compute $V_{FR_i}^{Rec} = V_{F_i(x)}^{Rec} \otimes V_{R_i(x)}^{Rec}$, where $\otimes$ denotes bit wise AND.
2. Construct a set $CORE^{Rec}$ ($= \emptyset$ initially). $P_i \in NB$ is included in $CORE^{Rec}$ if V_i^{Sh} matches with $V_{FR_i}^{Rec}$ atleast at $t+1$ locations.
3. Set $CORE = B \cup CORE^{Rec}$. If $|CORE| < n - t$, then output NULL and terminate. Else try to reconstruct the original $n \times n$ matrix T constructed by **D** in protocol **Secret Distribution** during first round by doing the following:

   (a) If $P_j \in NB$ and included in $CORE$ then insert the coefficients of $F_j'(x)$ (in increasing power of x) as the j^{th} row of T. Similarly, if $P_i \in B$, insert the coefficients of $F_i(x)$ broadcasted by **D** in third round as i^{th} row of T. Since $|CORE| > n - t$, at least $t+1$ rows will be inserted in T.

   (b) Check if each column of T is t-consistent (see Remark 2 for the meaning of t-consistency here). If not, output NULL. Else if all the n columns are t consistent, then reconstruct $M'(1), M'(2), \ldots, M'(n)$ by interpolating the values of each column and recover $M'(x)$ and finally compute $s' = M'(0)$.

with probability at least $1 - 2^{-k}$. Hence $V_{FR_i}^{Rec}$ and V_i^{Sh} will mismatch at those $(t+1)$ locations. This proves 1(b).

Now consider the case when **D** is dishonest and $P_i \in NB$ is an honest player. So P_i will broadcast correct information during second round, using $F_i(x), R_i(x)$ and d_i. In this case, V_i^{Sh} and $V_{F_i(x)}^{Rec} \otimes V_{R_i(x)}^{Rec}$ will match at least at $(t+1)$ locations corresponding to $(t+1)$ honest players. For this, consider an honest player P_j. Now there are two possible cases: (a) V_i^{Sh} **contains 0 at** j^{th} **position**. It implies that $d_i v_{ij} + r_{ij} \neq B_i(\alpha_j)$. This further implies that either v_{ij} is not α_j-

consistent with $F_i(x)$ or r_{ij} is not α_j-consistent with $R_i(x)$ or both. So during reconstruction phase when P_i broadcasts $F_i(x), R_i(x)$ and P_j broadcasts r_{ij}, v_{ij}, then the j^{th} location in $V^{Rec}_{F_i(x)} \otimes V^{Rec}_{R_i(x)}$ will contain 0. Hence j^{th} location in both V^{Sh}_i and $V^{Rec}_{F_i(x)} \otimes V^{Rec}_{R_i(x)}$ will match. (b) V^{Sh}_i **contains 1 at j^{th} position**. It implies that $d_i v_{ij} + r_{ij} = B_i(\alpha_j)$. Notice that j^{th} location in V^{Sh}_i is 1 iff either both v_{ij} and r_{ij} are α_j-consistent with $F_i(x)$ and $R_i(x)$ or both v_{ij} and r_{ij} are not α_j-consistent with $F_i(x)$ and $R_i(x)$. The problem comes in later case, when both v_{ij} and r_{ij} are not α_j-consistent with $F_i(x)$ and $R_i(x)$ but still j^{th} location in V^{Sh}_i is 1. We claim that this can happen for an unique $d_i \in \mathbb{F} - \{0\}$ for the pair $F_i(x)$ and $R_i(x)$, which the dishonest **D** must guess with probability $\frac{1}{|\mathbb{F}|-1} \approx 2^{-k}$ during first round. For otherwise, let there exist another $e_i \in \mathbb{F} - \{0\}$, such that $e_i v_{ij} + r_{ij}$ is also α_j consistent with $e_i F_i(x) + R_i(x)$. This implies $(d_i - e_i)v_{ij}$ is α_j consistent with $(d_i - e_i)F_i(x)$ or v_{ij} is α_j consistent with $F_i(x)$ which is a contradiction. Hence if V^{Sh}_i contains 1 at j^{th} position, then except with probability 2^{-k}, $V^{Rec}_{F_i(x)} \otimes V^{Rec}_{R_i(x)}$ will also contain 1 at j^{th} location. Hence, we have shown that with very high probability, V^{Sh}_i and $V^{Rec}_{F_i(x)} \otimes V^{Rec}_{R_i(x)}$ will match at the $(t+1)$ locations corresponding the honest players. This proves 2. □

Lemma 8 *If* **D** *is not discarded in sharing phase then the probability that an honest player P_i will be included in $CORE$ is at least $1 - 2^{-k}$.*

Proof: Since $CORE = B \cup CORE^{Rec}$, all honest players in B will be included in $CORE$. We now show that all honest players in NB are included in $CORE^{Rec}$ and hence in $CORE$, with very high probability. Now $P_i \in NB$ is included in $CORE^{Rec}$ if V^{Sh}_i matches with $V^{Rec}_{F_i} \otimes V^{Rec}_{R_i}$ atleast at $t+1$ locations. From Theorem 3, for an honest P_i, this condition will be satisfied with probability 1 for an honest **D** and with probability at least $(1 - 2^{-k})$ for a dishonest **D**. Hence except with probability 2^{-k}, an honest $P_i \in NB$ will be added in $CORE^{Rec}$ and hence in $CORE$. □

Lemma 9 *If* **D** *is honest then B will contain all corrupted players and $CORE^{Rec}$ will contain all players who disclose correct $F_i(x)$ and $R_i(x)$ (as given by* **D***) in reconstruction phase. Moreover, players in NB who disclose incorrect $F_i(x)$ or $R_i(x)$ or both during reconstruction phase, will not be included in $CORE^{Rec}$ with probability at least $(1 - 2^{-k})$.*

Proof: It is easy to see that when **D** is honest, B contains only corrupted players. Now a player $P_i \in NB$ is included in $CORE^{Rec}$ if V^{Sh}_i matches with $V^{Rec}_{F_i(x)} \otimes V^{Rec}_{R_i(x)}$ at least at $t+1$ locations. Now according to Theorem 3, when **D** is honest, this property is always true if P_i is honest, where as it may hold with probability at most 2^{-k} if P_i is corrupted and broadcasted incorrect $F_i(x)$ or $R_i(x)$ during reconstruction phase. Hence the lemma. □

Theorem 4 **Protocol 3-Round-PWSS** *is an efficient three round (n,t)-PWSS protocol for $n = 2t+1$, with error probability at most 2^{-k}.*

Proof: Number of rounds and efficiency is evident from the working of the protocol. Now we prove each of the three required property of PWSS in turn:

1. Secrecy: We only need to consider the case when **D** is honest. Without loss of generality let $\mathcal{A}_t$ controls the first t players. The proof will be similar to the proof of Lemma 2, where

the secrecy is shown by proving that $n-t$ coefficients of $F_{t+1}(x)$ are information theoretically secure. We now prove that same holds here also. Note that $n-t$ coefficients of $R_{t+1}(x)$ are information theoretically secure because $\mathcal{A}_t$ knows only t points on $n-1$ degree polynomial $R_{t+1}(x)$. Since $F_{t+1}(x)$ and $R_{t+1}(x)$ are independent of each other and d_{t+1} is randomly selected, it implies that $B_{t+1}(x) = d_{t+1}F_{t+1}(x) + R_{t+1}(x)$ has a completely independent distribution from $F_{t+1}(x)$ and $R_{t+1}(x)$. So even the knowledge of $B_{t+1}(x)$ keeps $n-t$ coefficients of $F_{t+1}(x)$ and $R_{t+1}(x)$ information theoretically secure.

2. Correctness: If **D** is honest, then from Lemma 9, all the honest players will be present in $CORE^{Rec}$. Also set B will contain only corrupted players P_j and they will be included in $CORE^{Rec}$ along with the corresponding correct polynomial $F_j(x)$, broadcasted by **D** during third round. Moreover, if a player $P_k \in NB$ broadcasts incorrect $F'_k(x)$ during reconstruction phase, then from Lemma 9, it might be present in $CORE^{Rec}$ with probability at most 2^{-k}. The property now follows from the working of the protocol.

3. Weak Commitment: We need to consider the case when **D** is dishonest. If **D** is not discarded at the end of sharing phase, then from Lemma 8, except with probability 2^{-k}, an honest player will be present in $CORE^{Rec}$, along with its corresponding $F_i(x)$ polynomial. If $F_i(x)$'s corresponding to the honest players in $CORE^{Rec}$ does not define a unique secret s', then irrespective of the polynomials broadcasted by corrupted players in $CORE^{Rec}$ during reconstruction phase, NULL will be output. On the other hand, if the $F_i(x)$'s corresponding to the honest players in $CORE^{Rec}$ define a unique secret s', then depending upon whether the $F_i(x)$'s broadcasted by corrupted players in $CORE^{Rec}$ are consistent with s' or not, either s' or NULL is output. Thus weak commitment on s' is satisfied. □

□

Theorem 5 *Protocol* **3-Round-PWSS** *communicates* $O((k+\log n)n^2)$ *bits and broadcasts* $O((k+\log n)n^2)$ *bits.*

Proof: During sharing phase, **D** gives two polynomials of degree $n-1$ and two n tuples to each player. This incurs a communication complexity of $O(n^2)$ field elements. Since $|\mathbb{F}| = n^2(n-1)2^k$, the communication complexity of the protocol is $O((k+\log n)n^2)$ bits. □

Remark 5 *As in protocol* **1-Round-PWSS**, **D** *can share* $n-t = \Theta(n)$ *secrets using protocol* **3-Round-PWSS** *by communicating* $O((k+\log n)n^2)$ *bits. Thus, the information rate of our protocol is* $\Theta(n)$. *We observe that the first two steps of PVSS protocol of [3] along with some additional checking constitutes a five round PWSS (with* $n = 2t+1$*) achieving an information rate of* $\Theta(n^3)$. *Thus our PWSS protocol is a significant improvement over the PWSS protocol of [3] in terms of round complexity as well as the information rate.*

8 Information Checking Protocol with $n = 2t+1$

We now describe a generalized Information Checking (IC) protocol which is a slight modification of the one described in [3]. The **GenIC** protocol is used in our four round PVSS protocol to generate

D's signature on a secret value s. In the protocol INT is a player, who wants **D**'s signature on a secret value s, such that at least $t+1$ receivers from the set $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ will accept the signature except with error probability 2^{-k}. To bound the error probability by 2^{-k}, it is enough that $|\mathbb{F}| \geq 2^k$. Before describing the protocol, we recall the following definition from [3].

Definition 5 (1_α-consistent [3]) *A vector $(x, y, z) \in \mathbb{F}^3$ is 1_α-consistent if there exists a degree one polynomial w over $\mathbb{F}$ such that $w(0) = x$, $w(1) = y$ and $w(\alpha) = z$.*

Protocol GenIC(D, $INT, \mathcal{P}, s$) - Generalized Information Checking Protocol with $n = 2t+1$

Protocol GenDistr($D, INT, \mathcal{P}, s$)

Round 1: Corresponding to each receiver $P_i \in \mathcal{P}$, **D** chooses a random value $\alpha_i \in \mathbb{F} - \{0, 1\}$ and additional random values $y_i, z_i \in \mathbb{F}$, such that the three tuple (s, y_i, z_i) is 1_{α_i}-consistent. In addition, corresponding to each $P_i \in \mathcal{P}$, **D** choose a random 1_{α_i}-consistent vector (s'_i, y'_i, z'_i). **D** sends s, y_i, s'_i, y'_i to INT and α_i, z_i, z'_i to the receiver P_i. The n tuple $[y_1\ y_2\ \ldots\ y_n]$ held by INT is called **authentication information**. The two n tuples $[y'_1\ y'_2\ \ldots\ y'_n]$ and $[s'_1\ s'_2\ \ldots, s'_n]$ held by INT are called as **auxiliary information**, where as the values (α_i, z_i) held by receiver P_i are called **verification information**.

Protocol GenAuthVal($D, INT, \mathcal{P}, s$):

Round 2: INT randomly selects n random elements $d_i, 1 \leq i \leq n$ from $\mathbb{F} - \{0\}$ and broadcasts the tuples $(d_i, s'_i + d_i s, y'_i + d_i y_i)$.

Round 3: In response to INTs broadcast in **Round 2**, **D** checks the correctness of the broadcasted information and also checks whether $(s'_i + d_i s, y'_i + d_i y_i, z'_i + d_i z_i)$ is 1_{α_i}-consistent for $1 \leq i \leq n$. **D** broadcasts s, along the n tuple $[y_1\ y_2\ \ldots\ y_n]$ if he finds any inconsistency. Each $P_i \in \mathcal{P}$ then adjusts his **verification information** (α_i, z_i), such that (s, y_i, z_i) is 1_{α_i}-consistent and the protocol ends here.

Parallely, $P_i \in \mathcal{P}$ checks if $(s'_i + d_i s, y'_i + d_i y_i, z'_i + d_i z_i)$ is 1_{α_i}-consistent and broadcasts "Accept" or "Reject", depending upon whether $(s'_i + d_i s, y'_i + d_i y_i, z'_i + d_i z_i)$ is 1_{α_i}-consistent or not.

Round 4: If **D** has not broadcasted s, along with the tuple $[y_1\ y_2\ \ldots\ y_n]$ in the previous round, then **D** broadcasts (α_i, z_i) corresponding to all receivers $P_i \in \mathcal{P}$, whose response was "Reject" in the previous round. Accordingly INT will adjust his y_i so that (s, y_i, z_i) becomes 1_{α_i}-consistent.

Protocol GenRevealVal($D, INT, \mathcal{P}, s$):

INT broadcasts s and $[y_1\ y_2\ \ldots\ y_n]$, whereas each receiver $P_i \in \mathcal{P}$ broadcasts (α_i, z_i).

If there exists at least $t+1$ distinct j's such that (s, y_j, z_j) is 1_{α_j}-consistent then **D**'s signature on s is "valid". Otherwise the signature is "invalid".

Theorem 6

1. *If **D** is honest, then except with probability 2^{-k}, a corrupted INT will not be able to forge **D**'s signature on some arbitrary value $s' \neq s$.*
2. *If INT is honest, then except with probability 2^{-k}, **D**'s signature on s which is given to INT, will be accepted during **GenRevealVal**.*
3. *If **D** and INT are honest, then at the end of **GenAuthVal**, the receivers in $\mathcal{P}$ will have no information about s in information theoretic sense.*

PROOF: Even though **GenIC** protocol is a slight modification of generalized IC protocol of [3], the properties of **GenIC** protocol is similar to the properties of generalized IC protocol of [3] (see

Lemma 1, Page 318-319). □

Important Observation: In protocol **GenIC**, if **D** does not broadcast s and $[y_1\ y_2\ \dots\ y_n]$ during **Round 3**, then the signing process will be over at the end of **Round 4** and INT will be able to produce the signature during fifth round (in protocol **RevealVal**). So the signature can be verified locally at the end of fifth round. However a careful observation shows that *INT can produce the signature and can get it verified in fourth round itself.* This is because if **D** has not broadcasted s during **Round 3**, then it implies that **D** does not want to change his commitment on s. The only information which is going to be changed (in **Round 4**) is the **authentication information** (y values) corresponding to the players for which **D** broadcasts **verification information** (α and z values) during **Round 4**. But s remains same. So INT can reveal (broadcast) s and the "old" **authentication information** during **Round 4** itself. Parallely, the receivers in $\mathcal{P}$ can also broadcast their "old" **verification information**. Now **D** will broadcast the "new" **verification information** during fourth round. So at the end of **Round 4**, each player can locally change INT's "old" **authentication information** according to the "new" **verification information** and can check the validity of **D**'s signature on s with "new" **verification** and "new" **authentication information** as in **GenIC** protocol. Thus, we have the following theorem:

Theorem 7 *In protocol* **GenIC***, if* **D** *does not broadcast s during* **Round 3***, then INT gets a signature on s, which can be produced (by INT) and verified (by n players) during* **Round 4***.*

9 Four Round PVSS with $n = 2t + 1$

We now design a four round PVSS protocol called **4-Round-PVSS**, with error probability 2^{-k} and $n = 2t + 1$. This is a significant improvement over the existing nine round PVSS protocol with $n = 2t + 1$ players given in [3]. The field size $|\mathbb{F}| \geq n^2(n-1)2^k$. In the protocol, **D** uses the **GenIC** protocol to provide its signature on the values which he gives to individual players. Parallely, each player in $\mathcal{P}$ executes the three round PWSS protocol **3-Round-PWSS**. We overlap the execution of **GenIC** and PWSS protocol, so that the sharing phase takes only four rounds. If a player (including **D**) is asked to broadcast some information during any round but he fails to do so, then he will be discarded.

Claim 7 *If $|\mathbf{D}^B| > t$ then it implies that* **D** *is corrupted.*

Proof: Obvious because for an honest **D**, $|\mathbf{D}^B| \leq t$. □

Claim 8 *If the players in $\mathbf{D}^B$ are not consistent with each other with respect to the polynomials which* **D** *broadcasted for them during* **Round 3** *then it implies that* **D** *is corrupted.*

Proof: Obvious because for an honest **D**, this can never happen. □

Implication 1 **D** *has broadcasted $f_i(x)$ and $f_i(y)$ for all $P_i \in \mathbf{D}^B$, during* **Round 3** *and hence the shares corresponding to these polynomials are public. So the execution of* **3-Round-PWSS**^{P_i}*, which was initiated by P_i, to distribute random pad to each player and check the consistency of*

Protocol 4-Round-PVSS: A Four Round PVSS Protocol with $n = 2t + 1$

Sharing Phase: **Round 1**

1. **D** chooses a random bivariate polynomial $F(x, y)$ of degree t in each variable, such that $F(0, 0) = s$. **D** computes $f_i(x) = F(x, i)$ and $g_i(y) = F(i, y)$ for $1 \leq i \leq n$. Considering player P_i as INT, **D** executes **Round 1** of **GenIC(**$D, P_i, \mathcal{P}, f_i(j)$**)** and **GenIC(**$D, P_i, \mathcal{P}, g_i(j)$**)** for $1 \leq j \leq n$.
2. Each $P_i \in \mathcal{P}$, acting as a dealer, starts the three round PWSS protocol **3-Round-PWSS**^{P_i} in order to share a random value $s_i \in \mathbb{F}$. Let the polynomials distributed by player P_i in **3-Round-PWSS**^{P_i} to the n players be denoted by $F_1^{iW}(x), F_2^{iW}(x), \ldots, F_n^{iW}(x)$, where player $P_j, 1 \leq j \leq n$ receives $F_j^{iW}(x)$.

Round 2:

1. In response to the protocols **GenIC(D,**$P_i, \mathcal{P}, f_i(j)$**)** and **GenIC(D,**$P_i, \mathcal{P}, g_i(j)$**)** initiated by **D** in **Round 1**, P_i acting as INT, executes **Round 2** of **GenIC(**$D, P_i, \mathcal{P}, f_i(j)$**)** and **GenIC(**$D, P_i, \mathcal{P}, g_i(j)$**)** for $1 \leq j \leq n$.
2. Each player $P_i, 1 \leq i \leq n$ broadcasts: (a) $a_{ij} = f_i(j) + F_j^{iW}(0)$, (b) $b_{ij} = g_i(j) + F_i^{jW}(0)$. /* $F_j^{iW}(0)$ denotes the constant term of $F_j^{iW}(x)$ received by player P_j from P_i in protocol **3-Round-PWSS**^{P_i}. */
3. Players in $\mathcal{P}$ executes the second round of **3-Round-PWSS**^{P_i} protocol for $1 \leq i \leq n$.

Round 3:

1. If **D** is not satisfied by the broadcast of P_i (as INT) in previous round (during the execution of **Round 2** of **GenIC(**$D, P_i, \mathcal{P}, f_i(j)$**)** and **GenIC(**$D, P_i, \mathcal{P}, g_i(j)$**)** for $1 \leq j \leq n$), then **D** broadcast $f_i(x) = F(x, i)$ and $g_i(y) = F(i, y)$.
2. Third round of **3-Round-PWSS**$^{P_i}, 1 \leq i \leq n$ is executed.

Local Computation At The End of Round 3:

1. Divide the set of players $\mathcal{P}$ into two sets $\mathbf{D}^B$ and $\mathbf{D}^{NB}$. Include P_i in $\mathbf{D}^B$ if **D** has broadcasted $f_i(x)$ and $g_i(y)$ during third round. If $|\mathbf{D}^B| > t$, then discard **D** and terminate **(see Claim 7)**.
2. Check whether all the players in $\mathbf{D}^B$ are pair-wise consistent with respect to the polynomials corresponding to them which are broadcasted by **D** during **Round 3** (two players P_i and P_j are said to be consistent if $f_i(j) = g_j(i)$ and $g_i(j) = f_j(i)$). If not, then discard **D** and terminate **(see Claim 8)**
3. For each $P_i \in \mathbf{D}^B$, terminate the execution of protocol **3-Round-PWSS**^{P_i}, **GenIC(**$D, P_i, \mathcal{P}, f_i(j)$**)** and **GenIC(**$D, P_i, \mathcal{P}, g_i(j)$**)** for $1 \leq j \leq n$ **(see Implication 1)**.

common shares on $f_i(x)$ can be terminated. Similarly, the execution of **GenIC(**$D, P_i, \mathcal{P}, f_i(j)$**)** *and* **GenIC(**$D, P_i, \mathcal{P}, g_i(j)$**)** *(to obtain* **D***'s signature on $f_i(j)$ and $g_i(j), 1 \leq j \leq n$) can be terminated, since* **D** *has publicly committed $f_i(x)$ and $f_i(y)$ to everybody by broadcasting them.*

Before giving description of **Round 4**, we prove the following claim, which is useful in the fourth round.

Claim 9 *If* **D** *has not broadcasted $Ff_i(x)$ and $g_i(y)$ during third round, then during fourth round, an honest P_i can produce signature on the values $f_i(j)$ and $g_i(j), 1 \leq j \leq n$, which will be accepted by an honest player at the end of fourth round with probability more than $(1 - 2^{-k})$.*

Proof: Follows from Theorem 7. □

We now give implication of each step of **Round 4**.

Implication 2 *Since $P_i \in \mathbf{D}^{NB}$,* **D** *has not broadcasted $f_i(x)$ and $g_i(y)$ during third round. Now if P_i finds that the values $f_i(j)$ ($g_i(j)$) given by* **D** *to him during first round are not t-consistent,*

Round 4:

1. For each $P_i \in \mathbf{D}^{NB}$, $\mathbf{D}$ executes **Round 4** of **GenIC**$(D, P_i, \mathcal{P}, f_i(j))$ and **GenIC**$(D, P_i, \mathcal{P}, g_i(j))$, $1 \leq j \leq n$.
2. Each $P_i \in \mathbf{D}^{NB}$ checks whether the values $f_i(j)$ and $g_i(j)$ given to it during first round are t-consistent. If not then P_i broadcasts $f_i(j)$ and $g_i(j), 1 \leq j \leq n$, along with $\mathbf{D}$'s signature on them.

   Local Computation by Each Player at the end of Round 4 with respect to this step: Every player checks whether $f_i(j), g_i(j), 1 \leq j \leq n$ are t-consistent. If not then check whether $\mathbf{D}$'s signature on them are valid. If yes, then discard $\mathbf{D}$. On the other hand, if either $f_i(j)$ $(g_i(j))$'s are found to be t-consistent or $\mathbf{D}$'s signature on them are found to be in-valid (or both) then discard P_i **(see Implication 2)**.
3. Each $P_i \in \mathbf{D}^{NB}$ checks whether they are consistent with all the players in $\mathbf{D}^B$. If not then P_i broadcasts $f_i(j)$ and $g_i(j), 1 \leq j \leq n$, along with $\mathbf{D}$'s signature on them.

   Local Computation by Each Player at the end of Round 4 with respect to this step: Every player checks whether $f_i(j)$'s and $g_i(j)'s$ broadcasted by P_i are consistent with the polynomials corresponding to the players in $\mathbf{D}^B$ and checks whether $\mathbf{D}$'s signature on $f_i(j)$'s and $g_i(j)$'s are valid. Now there are following cases: (a) If $f_i(j)$'s or $g_i(j)$'s (or both) are inconsistent with players in $\mathbf{D}^B$ and if $\mathbf{D}$'s signature on these values is valid, then discard $\mathbf{D}$ and terminate. (b) If $f_i(j)$'s and $g_i(j)$'s are consistent with $\mathbf{D}^B$ or if $\mathbf{D}$'s signature is invalid (or both), then discard P_i **(see Implication 3)**.
4. If $\exists P_i, P_j \in \mathbf{D}^{NB}$, such that $a_{ij} \neq b_{ji}$ or $b_{ij} \neq a_{ji}$ (these values were broadcasted by P_i, P_j during second round), then P_i broadcasts $f_i(j)$ and $g_i(j), 1 \leq j \leq n$ along with $\mathbf{D}$'s signature on them. Parallely, P_j broadcasts $f_j(i)$ and $g_j(i)$ along with $\mathbf{D}$'s signature on them.

   Local Computation by Each Player at the end of Round 4 with respect to this step: Every player checks $f_i(j) \stackrel{?}{=} g_j(i)$ and $g_i(j) \stackrel{?}{=} f_j(i)$ and checks validity of $\mathbf{D}$'s signature on these values. Now the following can occur: (a) The values are inconsistent and have valid signature from $\mathbf{D}$ on them. In this case discard $\mathbf{D}$ and terminate. (b) The values are inconsistent but $\mathbf{D}$'s signature on them are invalid. In this case, discard P_i (P_j) if $\mathbf{D}$'s signature on $f_i(j)$ or $g_i(j)$ $(f_j(i)$ or $g_j(i))$ is found to be invalid. (c) The values are consistent and have valid signature of $\mathbf{D}$ on them. In this case, everybody accepts $f_i(j)$ and $f_j(i)$ as j^{th} and i^{th} share of $f_i(x)$ and $f_j(x)$ respectively and these become public points on $f_i(x)$ and $f_j(x)$ **(see Implication 4)**.
5. If $\exists P_i, P_j \in \mathbf{D}^{NB}$, such that during the execution of third round of **3-Round-PWSS**^{P_i}, P_i (acting as a dealer) has broadcasted $F_j^{iW}(x)$ (the polynomial received by P_j from P_i during first round of PWSS), then P_i and P_j broadcast $f_i(j)$ and $g_j(i)$ respectively along with $\mathbf{D}$'s signature on them.

   Local Computation by Each Player at the end of Round 4 with respect to this step: Every player checks $f_i(j) \stackrel{?}{=} g_j(i)$. In addition, check the validity of $\mathbf{D}$'s signature on these values. Now the following cases can occur: (a) If the values are inconsistent and have got $\mathbf{D}$'s valid signature on them then discard $\mathbf{D}$ and terminate. (b) If the values are inconsistent but $\mathbf{D}$'s signature on them is invalid then discard P_i (P_j) if $\mathbf{D}$'s signature on $f_i(j)$ $(g_j(i))$ is invalid. (c) If the values are consistent and $\mathbf{D}$'s signature on them are valid then accept $f_i(j)$ as the j^{th} share of $f_i(x)$ and it becomes public point on $f_i(x)$ **(see Implication 5)**.

   If more than t players are discarded during **Local Computation**, then $\mathbf{D}$ is discarded and the protocol terminates.

then P_i broadcasts these values along with $\mathbf{D}$'s signature on them. Now this can happen in two scenarios: (a) $\mathbf{D}$ is corrupted and P_i is honest: From Claim 9, if P_i is honest and belongs to $\mathbf{D}^{NB}$, then P_i has got a signature on each $f_i(j)$ and $g_i(j)$, which can be produced and verified during fourth round. Moreover the signature will be accepted by every honest players (in fact at least $t+1$ honest players) with probability more than $1 - 2^{-k}$. In this case $\mathbf{D}$ will be discarded at the end of **Round 4**. *(b) $\mathbf{D}$ is honest and P_i is corrupted: A corrupted P_i can produce $f_i(j)$'s ($g_i(j)$'s) which are not t consistent and might forge a valid signature of $\mathbf{D}$ on these values with probability at most 2^{-k}.*

So an honest $\mathbf{D}$ *might be discarded with very low probability. Essentially step 2 (during* **Round 4***) ensures that if* $\mathbf{D}$ *is not discarded then every honest player in* $\mathbf{D}^{NB}$ *has t-consistent* $f_i(x)$*'s and* $g_i(y)$*'s.*

Implication 3 *The condition in step3 can occur in two scenarios: (a)* $\mathbf{D}$ *is corrupted and* P_i *is honest: Since* P_i *is honest and belongs to* $\mathbf{D}^{NB}$*, then* P_i *has got a signature on each* $f_i(j)$ *and* $g_i(j)$*, which can be produced and verified during fourth round. Moreover the signature will be accepted by every honest players (at least* $t+1$*) with probability more than* $1-2^{-k}$*. Hence* $\mathbf{D}$ *will be discarded at the end of* **Round 4***. (b)* $\mathbf{D}$ *is honest and* P_i *is corrupted: A corrupted player* P_i *might forge* $\mathbf{D}$*'s signature on* $f_i(j)$*'s or* $g_i(j)$*'s with probability at most* 2^{-k}*, and can broadcast some different values which are not consistent with the polynomials corresponding to the players in* $\mathbf{D}^B$*. Hence an honest* $\mathbf{D}$ *might be discarded with probability at most* 2^{-k}*. Essentially step 3 (during* **Round 4***) ensures that if* $\mathbf{D}$ *is not discarded then every honest player in* $\mathbf{D}^{NB}$ *is consistent with every player in* $\mathbf{D}^B$*.*

Implication 4 *During* **Round 2***, the situation* $a_{ij} \neq b_{ji}$ *or* $a_{ji} \neq b_{ij}$ *(or both) can happen when (a)* $\mathbf{D}$ *in corrupted and* P_i, P_j *can be honest/dishonest, (b)* $\mathbf{D}$ *is honest and at least one of* P_i *and* P_j *is corrupted. Now both* P_i *and* P_j *are asked to broadcast their common shares, along with* $\mathbf{D}$*'s signature on them.*

If $\mathbf{D}$ *is dishonest and given inconsistent values to honest players* P_i *and* P_j*, then except with probability at most* 2^{-k}*, everybody (at least honest players) will accept* $\mathbf{D}$*'s signature on these inconsistent values and discard* $\mathbf{D}$*. Similarly, if* $\mathbf{D}$ *is honest, then with probability at most* 2^{-k}*, a corrupted player* P_i *might forge* $\mathbf{D}$*'s signature on inconsistent* $f_i(j)$ *or* $g_i(j)$*. So an honest* $\mathbf{D}$ *might be discarded with probability at most* 2^{-k}*. Note that it is possible that a corrupted* P_i *purposely broadcast conflicting value against* P_j *(who also might have behaved incorrectly) during second round. But during fourth round, both* P_i *and* P_j *produce consistent values along with valid signature of* $\mathbf{D}$ *on them. In this case, everybody will accept these consistent values as the shares of* $f_i(x)$ *and* $g_j(y)$*. Essentially, step4 (during* **Round 4***) ensures that if* $\mathbf{D}$ *is not discarded then the honest players in* $\mathbf{D}^{NB}$ *are pair-wise consistent.*

Implication 5 *If* P_i *and* P_j *are two honest players in* $\mathbf{D}^{NB}$ *then both will behave honestly during the execution of* **3-Round-PWSS**^{P_i} *and so* P_i *(acting as a dealer) will never broadcast* $F_j^{iW}(x)$ *(the polynomial which* P_j *received from* P_i *during first round of PWSS). However, if* P_i *broadcasts* $F_j^{iW}(x)$ *then it implies that at least one of* P_i *or* P_j *is corrupted. Again this case is similar to the cases explained before. Essentially step5 (during* **Round 4***) ensures that if* $\mathbf{D}$ *is not discarded then every corrupted player* P_i *in* $\mathbf{D}^{NB}$ *commits* $f_i(j) = g_j(i)$ *to honest player* P_j *in* $\mathbf{D}^{NB}$*.*

Lemma 10 *During local computation (at the end of* **Round 4***) an honest* $\mathbf{D}$ *might get discarded with probability at most* 2^{-k}*.*

Proof: Follows from Implication 2, Implication 3, Implication 4 and Implication 5. □

Theorem 8 *Let* $\mathbf{D'}^{NB}$ *be the set of players in* $\mathbf{D}^{NB}$ *who are not discarded during local computation (at the end of* **Round 4***). If* $\mathbf{D}$ *is not discarded, then the following holds:*

1. *The probability that an honest player in $\mathbf{D}^{NB}$ might be absent in $\mathbf{D'}^{NB}$ is at most 2^{-k}.*

2. *All the players in $\mathbf{D}^{B}$ are consistent with each other.*

3. *All the honest players in $\mathbf{D'}^{NB}$ are consistent with each other. Moreover, they are also consistent with all the players in $\mathbf{D}^{B}$.*

4. *Every corrupted player P_i in $\mathbf{D'}^{NB}$ commits $f_i(j)$ to honest player P_j in $\mathbf{D'}^{NB}$ (by agreeing with $g_j(i)$).*

5. *Every corrupted player $P_i \in \mathbf{D'}^{NB}$ commits $f_i(k)$ to everybody by agreeing with $g_k(y)$, where $P_k \in \mathbf{D}^{B}$ and $g_k(y)$ is broadcasted by $\mathbf{D}$ during third round.*

PROOF: The first property follows from Implication 2, Implication 3, Implication 4 and Implication 5.

From Claim 8, if the players in $\mathbf{D}^{B}$ are in-consistent with each other then $\mathbf{D}$ is corrupted and hence would have been discarded during fourth round itself. So if $\mathbf{D}$ is not discarded then it implies that the players in $\mathbf{D}^{B}$ are consistent with each other. So the second property holds.

If P_i, P_j are two honest players in $\mathbf{D'}^{NB}$ and if they are not consistent with each other, then from Implication 4, they would have broadcasted their common shares along with $\mathbf{D}$'s signature on them. Moreover, with very high probability, during local computation, every player would have seen these inconsistent common shares, along with $\mathbf{D}$'s signature on them and would have discarded $\mathbf{D}$. But since $\mathbf{D}$ is not discarded, it implies that all the honest players in $\mathbf{D'}^{NB}$ are consistent with each other. Moreover, each honest player P_i in $\mathbf{D'}^{NB}$ is also consistent with all the players in $\mathbf{D}^{B}$. If not, then from Implication 3, P_i would have broadcasted all his shares along with $\mathbf{D}$'s signature on them and $\mathbf{D}$ would have been discarded. But since $\mathbf{D}$ is not discarded, each honest player P_i in $\mathbf{D'}^{NB}$ is also consistent with all the players in $\mathbf{D}^{B}$. Hence third property holds.

If $P_i, P_j \in \mathbf{D'}^{NB}$, such that P_i is corrupted and P_j is honest and the values broadcasted by P_i, P_j during second round contradict each other, then from Implication 4, P_i and P_j would have broadcasted their common shares along with $\mathbf{D}$'s signature on them and either $\mathbf{D}$ or P_i would have been discarded. But since neither $\mathbf{D}$ nor P_i is discarded, it implies that the corrupted players in $\mathbf{D'}^{NB}$ have broadcasted correct information during second round, that matches the corresponding information broadcasted by the honest players in $\mathbf{D'}^{NB}$ during second round. Hence fourth property holds.

If $P_k \in \mathbf{D}^{B}$, then it implies that $\mathbf{D}$ has broadcasted $g_k(y) = F(k, y)$. It also implies that $\mathbf{D}$ is committing the shares $g_k(j), 1 \leq j \leq n$. Now if a corrupted $P_i \in \mathbf{D'}^{NB}$ also agrees with $F(k, y)$, it implies that he is committing $g_k(i) = f_i(k) = F(k, i)$ to everybody. □

Theorem 9 *If $\mathbf{D}$ is not discarded at the end of sharing phase, then with very high probability, all the honest players are consistent with each other and define a bivariate polynomial $F^H(x, y)$ of degree at most t in each variable.*

PROOF: From Theorem 8, except with probability 2^{-k}, each honest player in $\mathbf{D}^{NB}$ is present in $\mathbf{D'}^{NB}$. Also from Theorem 8, all the honest players in $\mathbf{D'}^{NB}$ are consistent with each other. Moreover, each honest player in $\mathbf{D'}^{NB}$ is consistent with all the players (and hence with the honest players) in $\mathbf{D}^B$. This implies that all the honest players are consistent with each other. Since there are at least $t+1$ honest players, they define a bi-variate polynomials $F^H(x,y)$ of degree at most t in each variable. □

We now describe the reconstruction phase.

Protocol 4-Round-VSS: A Four Round PVSS Protocol with $n = 2t+1$

Reconstruction Phase: Only the players from the set $\mathbf{D}^B$ and $\mathbf{D}'^{NB}$ participate where $\mathbf{D}'^{NB}$ denotes the set of players in $\mathbf{D}^{NB}$ who are not discarded during local computation at the end of **Round 4**.

1. Set $CORE = \mathbf{D}'^{NB}$. Run the reconstruction phase of **3-Round-PWSS**^{P_i} if $P_i \in CORE$. If the reconstruction phase of **3-Round-PWSS**^{P_i} fails then remove P_i from $CORE$.
2. If reconstruction phase of **3-Round-PWSS**^{P_i} is successful then the polynomials $F_j^{iW}(x), 1 \leq j \leq n$, distributed by P_i in **3-Round-PWSS**^{P_i} to the n players are recovered correctly. Now the $j^{th}, 1 \leq j \leq n$ share of $f_i(x)$, denoted by f_{ij} is computed as follows:
$$\begin{aligned} f_{ij} &= g_j(i) \quad \text{if } P_j \in \mathbf{D}^B \\ &= f_i(j) \quad \text{if } f_i(j) \text{ is known publicly during } \textbf{Round 4} \\ &= a_{ij} - F_j^{iW}(0) \quad \text{otherwise} \end{aligned}$$
Remove P_i from $CORE$, if f_{ij}'s are not t-consistent. Otherwise reconstruct $f_i(x)$ by interpolating f_{ij}'s.
3. Take the recovered $f_i(x)$'s corresponding to the players in $CORE$, along with the $f_i(x)$'s corresponding to the players in $\mathbf{D}^B$. Using them, interpolate $F^H(x,y)$, reconstruct $s' = F^H(0,0)$ and terminate (see Theorem 10).

Theorem 10 *Protocol* **4-Round-PVSS** *is an efficient four round* (n,t) *PVSS, where* $n = 2t+1$. *The error probability of the protocol is* 2^{-k} *where* $|\mathbb{F}| = n^2(n-1)2^k$. *The communication complexity of the protocol is* $O((k+\log n)n^3)$ *bits.*

Proof: To prove the theorem, we prove each of the desirable properties of PVSS separately.

Lemma 11 *Protocol* **4-Round-PVSS** *satisfies perfect secrecy.*

Proof: We have to only consider the case when $\mathbf{D}$ is honest. Without loss of generality, let $\mathcal{A}_t$ controls the first t players. It is easy to see that if $\mathbf{D}$ is honest then $\mathbf{D}^B$ will contain only corrupted players. So the polynomials corresponding to these players which are broadcasted by $\mathbf{D}$ gives no new information to $\mathcal{A}_t$. The proof now follows from the properties of a bivariate polynomial of degree t and using similar arguments as in Lemma 7 (to prove the secrecy of **2-Round-PVSS**). □

Lemma 12 *Protocol* **4-Round-PVSS** *satisfies correctness property except with an error probability* $\leq 2^{-k}$.

Proof: We have to only consider the case when $\mathbf{D}$ is honest. From Lemma 10, the probability that a honest $\mathbf{D}$ might get discarded during sharing phase is at most 2^{-k}. Moreover, from Theorem 9, all the honest players will be consistent with each other and define a unique bivariate polynomial $F(x,y)$ (originally defined by $\mathbf{D}$) of degree t in both x and y. Also, only corrupted players will be present in $\mathbf{D}^B$ and hence all the honest players (at least $t+1$) will be present in $\mathbf{D}'^{NB}$. Now consider a corrupted player $P_i \in \mathbf{D}'^{NB}$. From property 4 of Theorem 8, P_i is consistent with all the honest players in $\mathbf{D}'^{NB}$, who in turn are consistent with $F(x, y)$. So if during reconstruction phase, the recovered $f_i(x)$ is t-consistent then it implies that it is consistent with $F(x, y)$ also. Hence the lemma holds. □

Lemma 13 *Protocol* **4-Round-PVSS** *satisfies strong commitment property except with an error probability* $\leq 2^{-k}$*.*

Proof: We have to only consider the case when $\mathbf{D}$ is dishonest. If $\mathbf{D}$ is discarded during sharing phase, then the lemma holds. On the other hand if $\mathbf{D}$ is not discarded, then from Theorem 9, except with an error probability of 2^{-k}, each pair of honest players will be consistent. Hence all honest players will define a bivariate polynomial $F^H(x, y)$ of degree at most t in both x and y. Since $\mathbf{D}$ is corrupted, the honest players may be distributed in sets $\mathbf{D}^B$ and $\mathbf{D}'^{NB}$. However, by property 3, 4 and 5 of Theorem 8, each corrupted player (either in $\mathbf{D}^B$ or in $\mathbf{D}'^{NB}$) is consistent with all the honest players, who in turn are consistent with $F^H(x, y)$. So if a corrupted $P_i \in \mathbf{D}'^{NB}$ is not discarded in the reconstruction phase, then the recovered $f_i(x)$ will be consistent with $F^H(x, y)$. Hence the strong commitment on $s' = F^H(0, 0)$ is satisfied. □

Lemma 14 *Protocol* **4-Round-PVSS** *communicates* $O((k+\log n)n^3)$ *bits where* $|\mathbb{F}| = n^2(n-1)2^k$

Proof: From Theorem 5, a single execution of **3-Round-PWSS** incurs a communication overhead of $O((k+\log n)n^2)$ bits. In our protocol, there are n such executions thus incurring a communication overhead of $O((k + \log n)n^3)$ bits. It is easy to see that other steps also incur a communication overhead is $O((k + \log n)n^3)$ bits. Hence the lemma holds. □

Theorem 10 now follows from Lemma 11, Lemma 12, Lemma 13 and Lemma 14. □

10 Lower Bound on Single Round PWSS

In this section, we prove that any single round PWSS is possible only if $n > 3t$.

Theorem 11 *There is no single round* (n, t)*-PWSS protocol when* $n \leq 3t$*.*

Proof: By using a standard player-partitioning argument [4, 5], Theorem 11 can be reduced to the following lemma.

Lemma 15 *There is no single round* $(3, 1)$*-PWSS protocol.*

Proof: Let Π be a $(3, 1)$-PWSS protocol with players P_1, P_2, P_3, with P_1 as dealer ($\mathbf{D}$). We start with a formal description of Π:

1. **Sharing Phase:** $\mathbf{D}$, on input secret s and random input r_D, sends α, β, γ to P_1, P_2 and P_3 respectively and broadcasts b_D. Each other player $P_i, i \in \{2, 3\}$, on random input r_i, sends a message p_{ij} to each player P_j and broadcasts b_i.

2. **Reconstruction Phase:** Every player broadcasts it's entire view generated in sharing phase.

In Π, the broadcasts done by dealer and individual players have no information about the secret s, otherwise Π violates the secrecy property of PWSS. The secrecy property also implies that when $\mathbf{D}$ is honest, any one of α, β and γ must not have any information about s. According to the correctness property of Π, when $\mathbf{D}$ is honest, if either P_2 or P_3 deviates from the protocol during reconstruction phase (and broadcasts a view which is different from the acquired view in sharing phase), then all the honest players must output $\mathbf{D}$'s secret s with very high probability.

Let s_1 and s_2 be two independent secrets and $(\alpha_1, \beta_1, \gamma_1)$ and $(\alpha_2, \beta_2, \gamma_2)$ be the share corresponding to s_1 and s_2 respectively. Consider two execution E_1^h and E_2^h of Π, where $\mathbf{D}$ is honest. In E_1^h, secret is s_1 and $\mathbf{D}$ distributes α_1, β_1 and γ_1 to P_1, P_2 and P_3 respectively. Assume that in E_1^h, P_2 is corrupted and further assume that P_2 broadcasts β_2 in reconstruction phase. So according to correctness property of Π, each honest player should reconstruct s_1 with very high probability.

In E_2^h, secret is s_2 and $\mathbf{D}$ distributes α_2, β_2 and γ_2 to P_1, P_2 and P_3 respectively. Assume that in E_2^h, P_3 is corrupted and further assume that P_3 broadcasts γ_1 in reconstruction phase. So according to correctness property of Π, each honest player should reconstruct s_2 with very high probability.

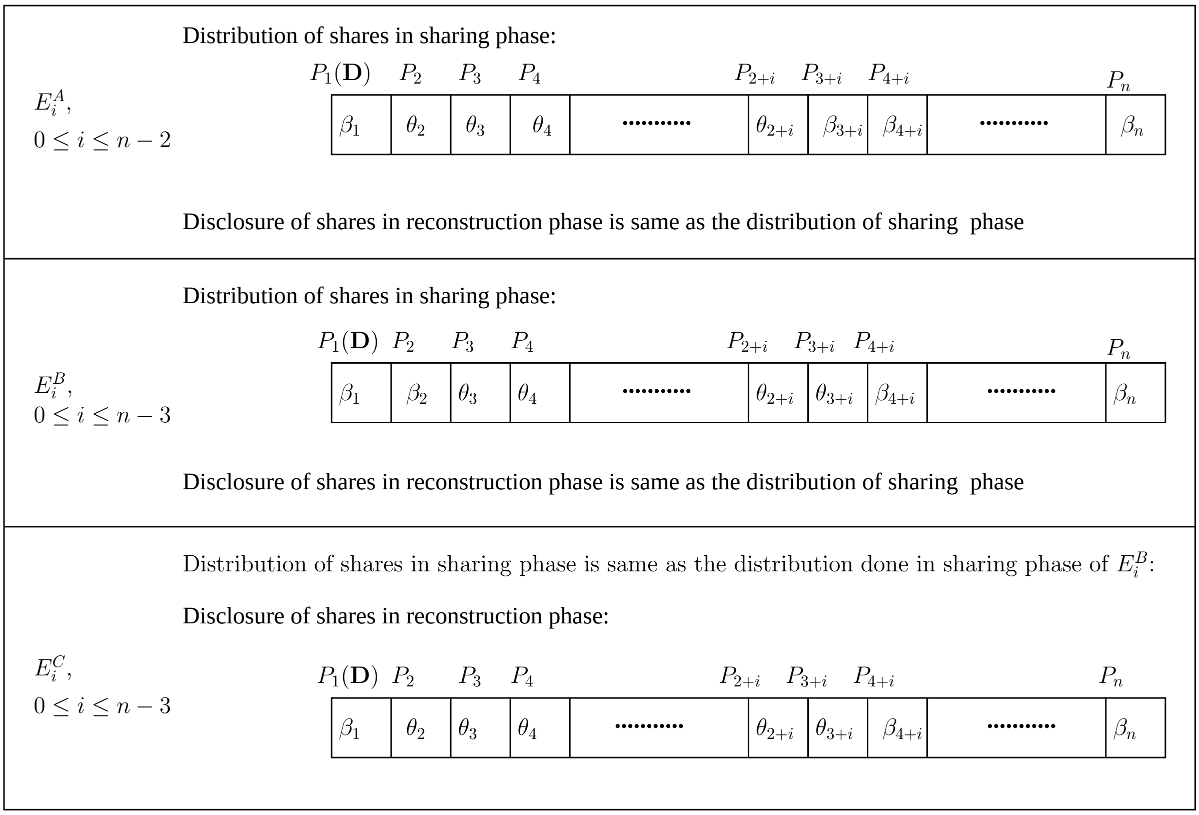
Now consider another execution E_3^c of Π where $\mathbf{D}$ is corrupted and distributes α_1, β_2 and γ_1 to P_1, P_2 and P_3 respectively. Now in reconstruction phase if every player behaves honestly, then view of the honest players in the reconstruction phase of E_3^c will exactly match with the view of the honest players in the reconstruction phase of E_1^h. Since the honest players reconstructs s_1 in E_1^h, they do the same in E_3^c also. Now according to the weak commitment property, if in E_3^c, the corrupted player (which is $\mathbf{D} = P_1$) deviates from the protocol and broadcasts α_2 during reconstruction phase, then with very high probability all honest players must reconstruct either s_1 or $NULL$. But notice that now, the view of the honest players will be identical as in E_2^h and thus s_2 should be reconstructed with very high probability. This is a contradiction. Hence Π does not exist. Thus there is no single round $(3, 1)$-PWSS and hence single round $(3t, t)$ PWSS protocol. □

11 Lower Bound on Single Round PVSS

Theorem 12 *There is no one round PVSS protocol with with ($t = 1$ and $n < 4$) or with $t > 1$.*

Proof: From Theorem 11, we know that there is no single round (n, t)-PWSS protocol when $n \leq 3t$. For $t = 1$, this implies there is no PWSS for $n \leq 3$. Since PVSS is stronger problem that PWSS, the above implication holds for PWSS.

Now we prove that there is no single round PVSS protocol for $t > 1$ and $n \geq 4$. For that, we show that if there exist a single round $(n, 2)$ PVSS protocol, then its error probability P_{error} must satisfy $P_{error} \geq \frac{1}{n}$. But according to the definition of PVSS, P_{error} should be exponentially small. So this shows a contradiction. Let Π be a single round $(n, 2)$ PVSS, where P_1 is the dealer. According to secrecy property of Π, for an honest $\mathbf{D}$, the broadcasts done by $\mathbf{D}$ is independent of the secret. Since for a honest $\mathbf{D}$, other players do not know the secret in sharing phase (which has a single round), the broadcasts done by individual players and the private communications done between any two players from $\mathcal{P} - \{\mathbf{D}\}$ are completely independent of the secret. Hence, we can neglect all of the above mentioned communications and concentrate on the communications done by $\mathbf{D}$ to the players in $\mathcal{P}$. Since Π is single round PVSS, the values given by $\mathbf{D}$ to individual players can be thought as shares of $\mathbf{D}$'s secret s. Now, let s and s^* be two secrets where $(\beta_1, \beta_2, \ldots, \beta_n)$ and $(\theta_1, \theta_2, \ldots, \theta_n)$ be the n shares corresponding to s and s^*, respectively. Let in Π, P_1 $(= \mathbf{D})$ and P_2 be the two corrupted players. Now consider three different type of executions of Π. In each execution, the random coin tosses of all the players are same.



E_i^A, $0 \le i \le n-2$

Distribution of shares in sharing phase:

$P_1(\mathbf{D})$	P_2	P_3	P_4		P_{2+i}	P_{3+i}	P_{4+i}		P_n
β_1	θ_2	θ_3	θ_4	....	θ_{2+i}	β_{3+i}	β_{4+i}	....	β_n

Disclosure of shares in reconstruction phase is same as the distribution of sharing phase

E_i^B, $0 \le i \le n-3$

Distribution of shares in sharing phase:

$P_1(\mathbf{D})$	P_2	P_3	P_4		P_{2+i}	P_{3+i}	P_{4+i}		P_n
β_1	β_2	θ_3	θ_4	....	θ_{2+i}	θ_{3+i}	β_{4+i}	....	β_n

Disclosure of shares in reconstruction phase is same as the distribution of sharing phase

E_i^C, $0 \le i \le n-3$

Distribution of shares in sharing phase is same as the distribution done in sharing phase of E_i^B:

Disclosure of shares in reconstruction phase:

$P_1(\mathbf{D})$	P_2	P_3	P_4		P_{2+i}	P_{3+i}	P_{4+i}		P_n
β_1	θ_2	θ_3	θ_4	....	θ_{2+i}	θ_{3+i}	β_{4+i}	....	β_n

Figure 1: Pictorial Representation of three differerent type of executions E_i^A,E_i^B and E_i^C

1. In execution type E_i^A, $0 \le i \le n-2$, during sharing phase, $\mathbf{D}$ gives the shares corresponding to the secret s^* to $P_2, P_3, \ldots, P_{2+i}$. To the remaining players, $\mathbf{D}$ gives the shares corresponding to s. During reconstruction phase, each player behaves honestly and correctly broadcast the shares received during sharing phase.

2. In execution type $E_i^B, 0 \le i \le n-3$, during sharing phase, $\mathbf{D}$ gives the shares corresponding to s^* to $P_3, P_4, \ldots, P_{3+i}$. To the remaining players, $\mathbf{D}$ gives the shares corresponding to s. During reconstruction phase, each player behaves honestly and correctly broadcast the shares received during sharing phase.

3. In execution type $E_i^C, 0 \le i \le n-3$, the sharing phase is same as in E_i^B, but during reconstruction phase, P_2 (corrupted player) broadcasts share corresponding to s^*. This he can do because $\mathbf{D}$ is also corrupted and hence can collude with P_2.

Let $P(s, E)$ be the probability that secret s is reconstructed during reconstruction phase of an execution E. Notice that execution E_i^A and E_i^B are same in the sense that in both the executions, during sharing phase, **D** distributes $i+1$ shares corresponding to s^* and $n-i-1$ shares corresponding to s and during reconstruction phase, each player honestly broadcast the shares received during sharing phase. Hence

$$P(s, E_i^A) = P(s, E_i^B) \tag{7}$$

Next notice that E_i^B and E_i^C differs only in the behavior of faulty player (P_2) during reconstruction phase. So according to the strong commitment property of Π, if s can be reconstructed in E_i^B with probability p, then s should also be reconstructed with probability at least $(1 - P_{error}) \times p$ in E_i^C (from Baye's Theorem and neglecting the other terms which are positive). This implies that

$$P(s, E_i^C) \geq (1 - P_{error}) \times P(s, E_i^B) \tag{8}$$

Finally in E_i^C and E_{i+1}^A, the view of the honest players during reconstruction phase is same. Hence

$$P(s, E_{i+1}^A) = P(s, E_i^C) \tag{9}$$

$$\text{Now by correctness property of } \Pi, P(s, E_0^A) \geq 1 - P_{error} \tag{10}$$

$$\begin{aligned} \text{Now From Equation (9) , } \quad P(s, E_1^A) &= P(s, E_0^C) \qquad (11) \\ &\geq (1 - P_{error}) \times P(s, E_0^B) \text{ by (8)} \\ &= (1 - P_{error}) \times P(s, E_0^A) \text{ by (7)} \\ &\geq (1 - P_{error})^2 \text{ by (10)} \end{aligned}$$

Hence by induction, $P(s, E_{n-2}^A) \geq (1 - P_{error})^{n-1}$. However, E_{n-2}^A denotes an execution sequence, where during sharing phase, **D** has distributed $n-1$ shares corresponding to s^* and one share corresponding to s. Moreover, during reconstruction phase, all players honestly broadcast the shares received during sharing phase. From the correctness and commitment property of Π, we get

$$P(s^*, E_{n-2}^A) \geq (1 - P_{error}) \tag{12}$$

Notice that

$$\begin{aligned} 1 &\geq P(s, E_{n-2}^A) + P(s^*, E_{n-2}^A) \\ &\geq (1 - P_{error})^{n-1} + (1 - P_{error}) \\ &\geq 1 - (n-1) \times P_{error} + 1 - P_{error} \end{aligned}$$

This implies that $P_{error} \geq \frac{1}{n}$. But this is a contradiction because according to the definition of PVSS, P_{error} is exponentially small. Hence Π does not exist. □

12 Conclusion and Open Problems

In this work, we have shown that allowing a negligible probability of error in VSS and WSS, increases the the fault tolerance significantly (which is visible from the Table 1 in Section 1). The following are the challenging problems left open in this paper: (a) Is $n > 3t$ necessary for two round PVSS and two round PWSS? (we have proved only sufficiency) (b) Is $n > 2t$ is sufficient for three round PVSS? (necessity is obvious from [7]).

References

[1] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *STOC*, pages 1–10, 1988.

[2] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols (extended abstract). In *STOC*, pages 11–19, 1988.

[3] 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.

[4] M. Fitzi, J. Garay, S. Gollakota, C. Pandu Rangan, and K. Srinathan. Round-optimal and efficient verifiable secret sharing. In *Proc. of TCC 2006*, volume 3876 of *LNCS*, pages 329–342. Springer Verlag, 2006.

[5] Rosario Gennaro, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin. The round complexity of verifiable secret sharing and secure multicast. In *STOC*, pages 580–589, 2001.

[6] J. Katz, C. Y. Koo, and R. Kumaresan. Improving the round complexity of 'round-optimal' vss. Cryptology ePrint Archive, Report 2007/358, 2007. http://eprint.iacr.org/.

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

[8] D. R. Stinson. *Cryptography Theory and Practice.* Chapman and Hall, 2006.