On The Communication Complexity of Perfectly Secure Message Transmission in Directed Networks

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

Abstract

In this paper, we re-visit the problem of *perfectly secure message transmission* (PSMT) in a *directed network* under the presence of a threshold adaptive Byzantine adversary, having *unbounded computing power*. Desmedt et.al [5] have given the characterization for *three* or more phase PSMT protocols over directed networks. Recently, Patra et. al. [15] have given the characterization of *two phase* PSMT over directed networks. Even though the issue of tradeoff between phase complexity and communication complexity of PSMT protocols has been resolved in *undirected networks*, nothing is known in the literature regarding directed networks. In this paper, we completely settle down this issue. Specifically, we derive the lower bounds on communication complexity of (a) two phase PSMT protocols and (b) *three or more phase* PSMT protocols in directed networks. Moreover, we show that our lower bounds are *asymptotically tight*, by designing *communication optimal* PSMT protocols in directed networks, which are first of their kind.

We re-visit the problem of *perfectly reliable message transmission* (PRMT) as well. Any PRMT protocol that sends a message containing ℓ field elements, has a trivial lower bound of $\Omega(\ell)$ (field elements) on its communication complexity. Thus any PRMT protocol that sends a message of ℓ field elements by communicating $\mathcal{O}(\ell)$ field elements, is referred as *communication optimal PRMT* or *PRMT with constant factor overhead*. Here, we characterize the class of directed networks over which *communication optimal* PRMT or PRMT *with constant factor overhead* is possible. Moreover, we design a communication optimal PRMT over a directed network that satisfies the conditions stated in our characterization.

Our communication optimal PRMT/PSMT protocols employ several new techniques based on coding theory, which are of independent interest.

Keywords: Information Theoretic Security, Unbounded Computing Power, Directed Networks, Byzantine Adversary.

1 Introduction

Consider the following problem: a sender **S** and a receiver **R** are part of a directed synchronous network and are connected by uni-directional node disjoint paths/channels, which are directed either from **S** to **R** or vice-versa. Each channel is abstracted as a directed edge, also called as *wire*. Moreover, **S** and **R** do not share any information in advance. An adversary $\mathcal{A}_t$ having *unbounded computing power* controls at most t wires between **S** and **R** in Byzantine fashion; i.e., the adversary can read and corrupt the communication through the wires under its control in any arbitrary fashion. **S** intends to communicate a message m containing ℓ field elements from a finite field $\mathbb{F}$ to **R**. The challenge is to design a protocol such that after interacting in phases [1], as per the protocol, **R** should correctly output m, without any error, irrespective of the behaviour of $\mathcal{A}_t$. This problem is called *perfectly reliable message transmission* (PRMT)[6, 5]. The problem of *perfectly secure message transmission* (PSMT)[6, 5] has an additional restriction that at the end of the protocol, $\mathcal{A}_t$ should have *no* information about m what so ever, in *information theoretic* sense.

PRMT and PSMT problem are among the most basic and foundation problems in fault tolerant distributed computing. Many fault tolerant distributed computing tasks like Byzantine Agreement (BA) [18, 9] and Multiparty Computation (MPC) [3, 26, 4, 19] are mostly designed over *complete* networks, where every two processors/nodes are connected by direct channel. The assumption on the availability of a complete graph is impractical in most scenarios. Thus given an incomplete graph, PRMT (PSMT) can be used to simulate reliable (secure) channel between every pair of nodes.

Existing Literature: PRMT/PSMT was first introduced and studied in undirected networks by Dolev et.al in [6]. Dolev et.al abstracted the underlying undirected graph and assumed that **S** and **R** are connected by n bi-directional vertex disjoint paths, also called as *wires* and $\mathcal{A}_t$ may corrupt any t out of the n wires in Byzantine fashion. Such an abstraction is justified because by Menger's theorem [12], a graph which is (n)-(**S, R**)-connected has n vertex disjoint paths connecting **S** and **R** and each such path may be abstracted as a wire connecting **S** and **R**. Using *wire abstraction*, Dolev et.al [6] have shown that PRMT/PSMT between **S** and **R** tolerating $\mathcal{A}_t$ is possible iff there exists $2t + 1$ bidirectional wires between **S** and **R**.

PRMT and PSMT in directed networks was first studied by Desmedt et.al [5]. Modelling the underlying network as a directed graph is well motivated because in practice not every communication channel admits bi-directional communication. For instance, a base-station may communicate to even a far-off hand-held device but the communication may not be possible in reverse direction. Extending the *wire abstraction* approach of Dolev et.al [6] over undirected network, the authors in [5] have abstracted the underlying directed network in the form of vertex disjoint paths/wires, which are directed either from **S** to **R** or vice-versa. Specifically, the authors in [5] have assumed that there exists u wires from **R** to **S**, also referred as *bottom band* and n wires from **S** to **R**, also referred as *top band*.

Desmedt et.al [5] have shown that (a) PRMT tolerating $\mathcal{A}_t$ is possible iff there are at least $2t + 1$ wires in the *top band*, (b) PSMT tolerating $\mathcal{A}_t$ is possible iff there are at least $n = \max(3t-2u+1, 2t+1)$ wires in the *top band*. Desmedt et.al [5] have shown the sufficiency of their characterization for PSMT by designing a PSMT protocol that requires *exponential* number of phases and has *exponential* communication complexity. Recently, PSMT protocols with *polynomial* phase (*three phase* in [13, 16, 17]; polynomial phase in [25]) and communication complexity have been proposed, satisfying the characterization of Desmedt et.al. Recently, Patra et.al [15] have shown that *two* phase PSMT over a directed network, tolerating $\mathcal{A}_t$ is possible iff there exists $n = \max(3t - u + 1, 2t + 1)$ wires in the top band. This clearly shows that the characterization of PSMT given by Desmedt et.al [5] holds for only *three or more* phase PSMT protocols (and is not sufficient for two phase).

A variant of PRMT (PSMT) problem is called URMT (USMT) problem. The problem of URMT (USMT) is same as PRMT (PSMT) except that at the end of the protocol, **R** should output m with very high probability of $(1 - 2^{\kappa})$ where κ is an error parameter. In [14], Patra et.al have derived *tight* bounds on the communication complexity of URMT and USMT protocols. Furthermore, in [24, 21] the authors have studied the URMT problem considering a generalized directed graph. Since the main

[1] A phase is a send from **S** to **R** or vice-versa.

theme of this paper is PRMT and PSMT, we avoid comparing our results with URMT and USMT.

Our Network Model: In this work, we study PRMT and PSMT in directed network $G = (V, E)$, where $\mathbf{S}$ and $\mathbf{R}$ are two special honest nodes in V. We follow the network model of [5] and assume that there are n directed wires $f_1, f_2, \ldots, f_n$ from $\mathbf{S}$ to $\mathbf{R}$, called as *top band* and u directed wires $b_1, b_2, \ldots, b_u$ from $\mathbf{R}$ to $\mathbf{S}$, called as *bottom band*. A centralized Byzantine adversary $\mathcal{A}_t$ with unbounded computing power, can actively control at most t wires out of the $n+u$ wires, in a colluded fashion. The adversary is *adaptive*; i.e., he can *incrementally* corrupt additional wires during the protocol execution depending on the data obtained so far from the currently corrupted wires. A wire once under the control of $\mathcal{A}_t$, will remain so for the rest of the protocol. Once a wire is corrupted, the communication over the wire is fully eavesdropped and dictated by $\mathcal{A}_t$. A wire which is *not* under the control of $\mathcal{A}_t$, is called *honest*. The network is synchronous and a protocol is executed in terms of *phases*, where a phase denotes a communication either from $\mathbf{S}$ to $\mathbf{R}$ or vice-versa. For ease of exposition, we assume that if $\mathbf{S}$ ($\mathbf{R}$) is expecting some value(s) in some specific format from $\mathbf{R}$ ($\mathbf{S}$) along a wire and if nothing (or some syntactically incorrect value(s)) comes, then $\mathbf{S}$ ($\mathbf{R}$) substitutes predefined value(s) from $\mathbb{F}$ in the desired specific format and continues the protocol. Any information which is sent over entire top (bottom) band is said to be *broadcast*. If some information is broadcast over at least $2t+1$ wires (out of which at most t are corrupted), then the information will be always recovered correctly at the receiving end by taking majority of the received information. Our protocols work on a finite field $\mathbb{F}$ where $|\mathbb{F}| \geq (n+u)$. We use m to denote the message that $\mathbf{S}$ intends to send to $\mathbf{R}$, where m is a sequence of element(s) from $\mathbb{F}$.

Motivation of Our Work and Our Contributions: A key parameter of any PSMT protocol is its communication complexity, which is the number of field elements communicated by $\mathbf{S}$ and $\mathbf{R}$ in the protocol. Though the PSMT protocols over directed networks, reported in [13, 16, 25, 17] are *communication efficient* (i.e. require communication complexity which is polynomial in n), they are not *communication optimal*. Over the past one decade, lot of research has been carried out to derive tight bounds on the communication complexity of PRMT/PSMT protocols in undirected networks [23, 1, 7, 8, 2]. Unfortunately, there is no complexity bounds for PRMT/PSMT protocols in directed networks. The existing bounds on the communication complexity of PRMT/PSMT in undirected networks cannot be extended to directed networks. So in this paper, we derive the lower bound on the communication complexity of both two phase and *three or more* phase PSMT protocols[2]. Moreover, we show that our bounds are *asymptotically tight* by presenting polynomial time and *communication optimal* PSMT protocols which are first of their kind.

Any PRMT protocol that sends ℓ field elements, has a trivial lower bound of $\Omega(\ell)$ on its communication complexity. Thus any PRMT protocol that sends a message of ℓ field elements by communicating $\mathcal{O}(\ell)$ field elements, is referred as *communication optimal PRMT* or *PRMT with constant factor overhead*. Here, we characterize the class of directed networks over which communication optimal PRMT is possible. Moreover, we design a communication optimal PRMT over a graph that satisfies the conditions stated in our characterization. Our communication optimal PRMT is used as a building block to design communication optimal PSMT protocol. To design our protocols, we use several new techniques based on coding theory, which are of independent interest.

2 Preliminaries

As all the protocols that we present in this paper are heavily based on the properties of Reed-Solomon (RS) encoding and decoding from coding theory [10] and the concept of pseudo-basis, an idea introduced by Kurosawa et.al [8], we briefly recall the ideas related to them in the sequel.

Definition 1 (RS Codes [10]:) *For a message block $M = (m_1\ m_2\ \ldots\ m_k)$ over $\mathbb{F}$, define Reed − Solomon polynomial as $P_M(x) = m_1 + m_2x + m_3x^2 + \ldots + m_kx^{k-1}$. Let $\alpha_1, \alpha_2, ..., \alpha_L, L > k$, denote*

[2] Any single phase PSMT in directed network is no different from a single phase PSMT in undirected networks. Hence, from [6], any single phase PSMT in directed networks requires $n \geq 3t+1$ wires in the *top* band. Also, from [22, 7], any single phase PSMT over $n \geq 3t+1$ wires communicates $\Omega(\frac{n\ell}{n-3t})$ field elements to securely send a message containing ℓ field elements. Moreover, these bounds are asymptotically tight.

a sequence of L distinct and fixed elements from $\mathbb{F}$. Then vector $C = (c_1\ c_2\ \ldots\ c_L)$ where $c_i = P_M(\alpha_i), 1 \leq i \leq L$ is called the Reed-Solomon (RS) codeword of size L for the message block M.

Given a message block $M = (m_1\ m_2\ \ldots\ m_k)$ of size k over $\mathbb{F}$, the method of computing the RS codeword C for M is called RS encoding. So we write $C = RS - ENC(M, k, L)$. Now let $\mathbf{A}$ and $\mathbf{B}$ are two specific nodes and are connected by L wires of which at most t can be under the influence of $\mathcal{A}_t$. Let $\mathbf{A}$ send the i^{th} component of C over the i^{th} wire. Let $\mathbf{B}$ receive C' where C and C' differs in at most t locations. Under this scenario, the error correction and detection capability of $\mathbf{B}$ in C' is given by the error correction and detection capability of RS decoding which is stated as follows:

Theorem 1 ([10, 5]) *RS decoding can correct up to c Byzantine errors and simultaneously detect additional d Byzantine errors ($c + d \leq t$) in C' iff $L - k \geq 2c + d$.*

2.1 Pseudo-basis and Pseudo-dimension

Kurosawa et.al [8] have first introduced the concept of pseudo-basis for designing a two phase communication optimal PSMT protocol over undirected network where $\mathbf{S}$ and $\mathbf{R}$ are connected by at least $2t + 1$ bidirectional paths/wires. So, we take the current description of pseudo-basis and pseudo-dimension from [8]. Let $\mathcal{C}$ be the set of all possible L length RS codewords over $\mathbb{F}$, which are RS encoded using polynomials of degree $k - 1$ over $\mathbb{F}$. Also we assume that the hamming distance [10, 8] of code $\mathcal{C}$ is $t+1$ i.e. $L-(k-1) \geq t+1$ [8]. We may call the individual codewords in $\mathcal{C}$ as L-dimensional vectors. Though any L length codeword is an L length vector, the reverse is not true.

Now let us return back to the settings where $\mathbf{A}$ and $\mathbf{B}$ are connected by L wires, among which t are controlled by $\mathcal{A}_t$. Let $\mathbf{A}$ sends several codewords, say γ codewords $C_1, \ldots, C_\gamma \in \mathcal{C}$ over these wires, by transmitting i^{th} component of all the codewords over i^{th} wire. Then the locations at which error occurs in these codewords are not random. This is because for all the codewords the errors always occur at the same t (or less) locations. Based on this simple and interesting observation, Kurosawa et. al. [8] introduced the concept of pseudo-basis. Let $\mathbf{B}$ receive the L length vectors $Y_1 \ldots, Y_\gamma$ such that for $i = 1, \ldots, \gamma$, $Y_i = C_i + E_i$, where $E_i = (e_{i1}, \ldots, e_{iL})$ is an error vector caused by $\mathcal{A}_t$. Notice that each E_i has at most t non-zero components. Let

$$support(E_i) = \{j \mid e_{ij} \neq 0\}.$$

Then there exist some t-subset $\{j_1, \ldots, j_t\}$ of L wires that are corrupted by $\mathcal{A}_t$ such that each error vector E_i satisfies $support(E_i) \subseteq \{j_1, \ldots, j_t\}$. This means that the space $\mathcal{E}$ spanned by $E_1, \ldots, E_\gamma$ has dimension at most t. The notion of pseudo-basis exploits this idea. Let $\mathcal{V}$ denote the L-dimensional vector space over $\mathbb{F}$. For two vectors $Y, E \in \mathcal{V}$, we write $Y = E\ mod\ \mathcal{C}$ if $Y - E \in \mathcal{C}$. Notice that for $1 \leq i \leq \gamma$, for every triplet (Y_i, C_i, E_i), $Y_i = E_i\ mod\ \mathcal{C}$ holds since $Y_i - E_i = C_i \in \mathcal{C}$. We now recall the definition of pseudo-span on $\mathcal{Y} = \{Y_1 \ldots, Y_\gamma\}$, pseudo-dimension and pseudo-basis of $\mathcal{Y}$.

Definition 2 (Pseudo-span [8]) *: We say that $\{Y_{a_1} \ldots, Y_{a_p}\} \subset \mathcal{Y}$ pseudo-spans $\mathcal{Y}$ if each $Y_i \in \mathcal{Y}$ can be written as $Y_i = (b_1 Y_{a_1} + \ldots + b_p Y_{a_p})\ mod\ \mathcal{C}$, for some non-zero vector $(b_1, \ldots, b_p) \in \mathbb{F}^p$.*

Definition 3 (Pseudo-dimension and pseudo-basis [8]) *: Let p be the dimension of the space $\mathcal{E} = \{E_1, \ldots, E_\gamma\}$ and let $\{E_{a_1}, \ldots, E_{a_p}\} \subset \mathcal{E}$ be a basis of $\mathcal{E}$. We then say that $\mathcal{Y}$ has pseudo-dimension p and $\{Y_{a_1}, \ldots, Y_{a_p}\} \subset \mathcal{Y}$ is a pseudo-basis of $\mathcal{Y}$.*

We now recall the following theorems from [8] (the proofs are available in [8]):

Theorem 2 ([8]) *$\mathcal{B} = \{Y_{a_1}, \ldots, Y_{a_p}\}$ is a pseudo-basis of $\mathcal{Y}$ iff $\mathcal{B}$ is a minimal subset of $\mathcal{Y}$ which pseudo-spans $\mathcal{Y}$.*

Theorem 3 ([8]) *The pseudo-dimension of $\mathcal{Y}$ is at most t.*

Let $\mathcal{B} = \{Y_{a_1}, \ldots, Y_{a_p}\}$ be a pseudo-basis of $\mathcal{Y}$ and let $CORRUPTED = \cup_{i=1}^{p} support(E_{a_i})$. Then $CORRUPTED$ is the set of wires that the adversary $\mathcal{A}_t$ has corrupted. So,

Theorem 4 ([8]) *For each i, $support(E_i) \subseteq CORRUPTED$.*

Finally, Kurosawa et. al [8] also have provided a polynomial time algorithm which finds the pseudo-dimension p (which is at most t) and a pseudo-basis $\mathcal{B}$ of $\mathcal{Y} = \{Y_1, \ldots, Y_\gamma\}$. We denote the algorithm as: $(p, \mathcal{B}, \mathcal{I}) =$ **FindPseudo-basis**$(\mathcal{Y})$. So **FindPseudo-basis** takes the set of received (by $\mathbf{B}$) vectors $\mathcal{Y}$ as input and finds the pseudo-basis $\mathcal{B} = \{Y_{a_1}, \ldots, Y_{a_p}\} \subset \mathcal{Y}$, pseudo-dimension $p = |\mathcal{B}| \leq t$ and an index set $\mathcal{I} = \{a_1, \ldots, a_p\} \subset \{1, \ldots, \gamma\}$ containing the indices of the vectors selected in $\mathcal{B}$.

2.2 Extracting Randomness

Suppose by some means, $\mathbf{S}$ and $\mathbf{R}$ agree on L random numbers $x = [x_1\ x_2\ \ldots\ x_L] \in \mathbb{F}^L$ such that $\mathcal{A}_t$ knows $L - f$ components of x, but has no information about the other f components of x. However $\mathbf{S}$ and $\mathbf{R}$ do not know which values are known to $\mathcal{A}_t$. The goal of $\mathbf{S}$ and $\mathbf{R}$ is to agree on a sequence of f elements $[y_1\ y_2\ \ldots\ y_f]$, such that $\mathcal{A}_t$ has no information about $[y_1\ y_2\ \ldots\ y_f]$. This is done as follows [23]:

Algorithm EXTRAND$_{L,f}(x)$ [23]: Let V be an $L \times f$ Vandermonde matrix with members in $\mathbb{F}$ and which is known publicly. Then $\mathbf{S}$ and $\mathbf{R}$ both locally compute the product $[y_1\ y_2\ \ldots\ y_f] = [x_1\ x_2\ \ldots\ x_L]V$.

3 PRMT with Constant Factor Overhead

In this section, we characterize the class of digraphs over which *communication optimal PRMT* protocol is possible tolerating $\mathcal{A}_t$. To be more clear, we answer the following question: *what is the necessary and sufficient condition for the possibility of communication optimal PRMT protocol over a directed network / digraph?* The following theorem completely resolves the above question.

Theorem 5 *Communication optimal PRMT protocol, tolerating $\mathcal{A}_t$ is possible over a digraph iff there are $n \geq 2t + 1$ wires in the top band and u wires in the bottom band where $(n - 2t) + 2u = \Omega(n)$.*

Proof: **Sufficiency:** To prove the sufficiency, in the sequel we design a *communication optimal* PRMT protocol **OPRMT**, which reliably sends a message m containing $\ell = \Omega(nt)$ field elements by communicating $\mathcal{O}(nt)$ field elements and terminates in three phases, provided $n = 2t + 1$ and $(n - 2t) + 2u = \Omega(n)$.

Before describing **OPRMT**, we present a special type of single phase PRMT called **SP-REL** where $\mathbf{S}$ is connected to $\mathbf{R}$ by $n \geq 2t+1$ wires $f_1, \ldots, f_n$. **SP-REL** either sends m to $\mathbf{R}$ or it may fail because $\mathcal{A}_t$ have done corruptions exceeding some limit (but not more than t). In the later case, $\mathbf{R}$ will *only* be able to detect but cannot correct the errors to recover m. Thus **SP-REL** creates a win-win situation: if $\mathcal{A}_t$ does at most $(t - b)$ corruptions then m is recovered; else $\mathbf{R}$ detects that more than $(t - b)$ wires are corrupted. Protocol **SP-REL** is based on RS codes. Let $X = n - 2t$.

Protocol SP-REL(m, ℓ, n, t, b)**:** $n \geq 2t + 1, 0 \leq b \leq t$

1. $\mathbf{S}$ breaks up m into blocks $\mathbf{B_1}, \mathbf{B_2}, \ldots, \mathbf{B_z}$, each consisting of k field elements, where $k = X + b$. If ℓ is not an exact multiple of k, a default padding is used to make ℓ mod $k = 0$.
2. For each block $\mathbf{B_i}$, $\mathbf{S}$ computes $(c_{i1}c_{i2}\ldots c_{in}) = RS{-}ENC(B_i, k, n)$ and sends c_{ij}, along the wire $f_j, 1 \leq j \leq n$.
3. $\mathbf{R}$ receives c'_{ij} (possibly corrupted) over f_j for $1 \leq j \leq n$ and $1 \leq i \leq z$ and applies RS decoding to each of the received n length vectors and tries to correct $t - b$ errors and simultaneously detect additional b errors.
4. If after correcting $t - b$ errors, the RS decoding algorithm does not detect additional errors in any of the z received vectors, then $\mathbf{R}$ correctly recovers $\mathbf{B_i}$, $1 \leq i \leq z$ and concatenates these blocks to recover m.
5. If $\exists e \in \{1, 2, \ldots, z\}$ such that after correcting $t - b$ errors, the decoding algorithm detects additional errors in the e^{th} received vector, then $\mathbf{R}$ generates "ERROR" which means he has detected that more than $t - b$ faults has occurred.

We request the reader to refer **APPENDIX A** for the proof of the properties of **SP-REL**. We now design a *communication optimal* PRMT protocol **OPRMT** using **SP-REL** as a black-box. The proofs of the properties of **OPRMT** are provided in **APPENDIX A** due to space constraint.

It should be noted that **OPRMT** sends ℓ field elements by communicating $\mathcal{O}(\ell)$ field elements for all $\ell = \Omega(nt)$. *It will be interesting to find a communication optimal PRMT for any message size.*

Protocol OPRMT (m, ℓ, n, u, t)**;** $|m| = \ell = (nt)$

Phase I: S to R: **S** executes **SP-REL**(m, ℓ, n, t, b) with $b = \min(\frac{u}{2}, \frac{t}{2})$, $n = 2t+1$. In **SP-REL**, let $B_1^S, \ldots, B_z^S$ be the message blocks and C_i^S be the n length RS codeword corresponding to B_i^S, sent by **S**.

Phase II: R to S: Let **R** receive $C_1^R, \ldots, C_z^R$. If **R** recovers m after the execution of **SP-REL**, then he sends `SUCCESS` to **S** through the entire *bottom band*. Else **R** sends `ERROR` and the tuple (α, C_α^R) to **S** through entire *bottom band*, where **R** has detected more than $t-b$ faults in C_α^R.

Phase III: S to R: Let **S** receive `SUCCESS` along $u_s \geq 0$ wires and `ERROR` along with an tuple of the form **(index,** n **length vector)** through $u_e \geq 0$ wires. **S** now considers the following two cases:

- *Case 1.* $u_s \geq \frac{u}{2}$: **S** does nothing and terminates the protocol (see Theorem 11).
- *Case 2.* $u_e \geq \frac{u}{2}$: **S** checks whether it has received the same **(index,** n **length vector)** over at least $\frac{u}{2}$ wires out of the u_e wires. If not, then **S** does nothing and terminates the protocol (see Theorem 11). Otherwise, let **S** receive the same tuple (β, Γ) through at least $\frac{u}{2}$ wires out of u_e wires and do the following:
  1. Compute $\mathcal{E} = support(C_\beta^S - \Gamma)$ and the number of mismatches between C_β^S and Γ as $E = |\mathcal{E}|$.
  2. If $E \leq t-b$, then do nothing and terminate the protocol (see Theorem 11).
  3. If $E > t-b$, then consider the wires in $\mathcal{E}$ as faulty and add them to a list L_{fault}. Ignore all the wires in L_{fault} from the *top band* for further communication. For simplicity, let these be the last $|L_{fault}|$ wires in the *top* band. Re-send m by executing **SP-REL**$(m, \ell, n-|L_{fault}|, t-|L_{fault}|, |L_{fault}|)$ over the first $n-|L_{fault}|$ wires. In addition, broadcast L_{fault} to **R** over entire *top band*.

Message Recovery by R: If **R** had sent `ERROR` and a tuple (index, n length vector) to **S** during **Phase II**, then **R** will always correctly receive L_{fault}. Now ignoring all information received over the wires in L_{fault}, **R** correctly recovers m by executing the steps of **SP-REL**$(m, \ell, n-|L_{fault}|, t-|L_{fault}|, |L_{fault}|)$.

Necessity: First of all, irrespective of the value of u, by the results of [6], any PRMT from **S** to **R** is possible iff there exist $n \geq 2t+1$ wires from **S** to **R**. Hence the digraph must have $n \geq 2t+1$ wires in the *top band* for the existence of any PRMT that is *communication optimal*. Next we show that u must satisfy $(n-2t)+2u = \Omega(n)$ for the existence of *communication optimal* PRMT protocol. We have to prove this when $u < t$ because if $u \geq t$ then $(n-2t)+2u = \Omega(n)$ is satisfied.

So let $u < t$. Suppose both **S** and **R** in advance know that the entire bottom band is corrupted. Under this assumption, any multiphase PRMT protocol virtually reduces to a single phase PRMT protocol, where **S** is connected to **R** by $n \geq 2t+1$ wires, of which at most $t-u$ are corrupted. Now by the results of [23], any single phase protocol must communicate $\Omega(\frac{n\ell}{n-2t})$ field elements for reliably sending ℓ field elements, where **S** is connected to **R** by $n \geq 2t+1$ wires, of which at most t are corrupted. This implies that any single phase protocol must communicate $\Omega(\frac{n\ell}{n-2(t-u)})$ field elements for reliably sending ℓ field elements, where **S** is connected to **R** by $n \geq 2t+1$ wires, of which at most $t-u$ are corrupted. Thus any multiphase PRMT protocol must communicate $\Omega(\frac{n\ell}{n-2(t-u)})$ fields elements for reliably sending ℓ field elements over a digraph. Therefore $\Omega(\frac{n\ell}{n-2(t-u)})$ defines a lower bound on the communication complexity of any multiphase PRMT protocol sending ℓ field elements. Note that this lower bound is derived by assuming that **S** and **R** in advance know that the entire bottom band is corrupted. Any lower bound derived under this assumption is trivially a lower bound for the more general case, where **S** and **R** do not have this information in advance. By definition, any *communication optimal* PRMT protocol transmits $\mathcal{O}(\ell)$ field elements for sending ℓ field elements. It is easy to see that $\Omega(\frac{n\ell}{n-2(t-u)})$ will turn out to be $\mathcal{O}(\ell)$ only if $(n-2t)+2u = \Omega(n)$. □

4 Lower Bound on Communication Complexity of Two Phase PSMT

For the rest of the paper, we will concentrate on PSMT problem, where we require the message to be delivered *reliably as well as securely* to **R**. This is in contrast to PRMT, where we require the message to be delivered only *reliably* to **R**. In this section, we derive the lower bound on the communication complexity of any two phase PSMT protocol in directed networks. We then show that the bound is *asymptotically tight*. We first recall the characterization of two phase PSMT in directed networks tolerating $\mathcal{A}_t$ from [15].

Theorem 6 ([15]) *Suppose there are disjoint set of n wires in the top band and u wires in the bottom band such that $\mathcal{A}_t$ controls at most t of these $n+u$ wires. Then there exists a two phase PSMT tolerating $\mathcal{A}_t$ iff $n \geq max(3t-u+1, 2t+1)$.*

The necessity proof of the above theorem is divided in two cases: if $u > t$, then the necessity condition says that there should exist $n \geq 2t+1$ wires in the top band. From [6, 5], $n \geq 2t+1$ wires from **S** to **R** are necessary for any reliable communication from **S** to **R**. Hence, it is obviously necessary for PSMT. On the other hand, if $u \leq t$, then the necessity condition says that there should exist $n \geq 3t-u+1$ wires in the top band. This is proved by contradiction. Specifically, the authors of [15] showed that if there exists a two phase PSMT tolerating $\mathcal{A}_t$ with $u \leq t$ wires in bottom band and $n = 3t-u$ wires in the top band, then one can design a single phase PSMT with $N = n+u = 3t$ wires directed from **S** to **R**, tolerating $\mathcal{A}_t$, which is impossible according to [6]. We recall the necessity proof of the above theorem from [15] and present it in **APPENDIX B**. Our derivation of the lower bound on the communication complexity of two phase PSMT (which is presented below), heavily bases on the necessity proof of above theorem.

Theorem 7 *Suppose there exists u wires in the bottom band and $n = \max(3t-u+1, 2t+1)$ wires in the top band. Then any two phase PSMT protocol which securely sends a message $m \in \mathbb{F}^\ell$ containing ℓ field elements must communicate*

(a) $\Omega\left(\frac{N\ell}{N-3t}\right)$ field elements where $0 \leq u \leq t$, $n \geq 3t-u+1$ and $N = n+u \geq 3t+1$.

(b) $\Omega\left(\frac{n\ell}{n-2t}\right)$ field elements where $u > t$ and $n \geq 2t+1$.

The proof of Theorem 7 is presented in **APPENDIX C** due to space constraint. □

In [15], a two phase polynomial time PSMT protocol is reported for showing sufficiency of Theorem 6. The protocol sends a message of size $\ell = 1$ field element by communicating $\mathcal{O}(N) = \mathcal{O}(n+u)$ field elements, where $n = \max(3t-u+1, 2t+1)$. Though the protocol of [15] satisfies the lower bound given in Theorem 7(a) for the case $u \leq t$, it fails to satisfy the lower bound given in Theorem 7(b) for the case $u > t$. So, in the next section, we modify the PSMT protocol of [15], to obtain a generic two phase PSMT protocol, that satisfies the lower bound given in Theorem 7(a), as well as Theorem 7(b).

4.1 Two Phase Communication Optimal PSMT Protocol

Let $n = \max(3t-u+1, 2t+1)$ and $u > 0$. Also let $\delta = \max(u, t)$ and $N = n+u$. We now design a two phase PSMT protocol called **O2PSMT**, which securely sends a message m, containing $\ell = (\delta+1-t)$ field elements by communicating $(N+n(\delta+1-t))$ field elements. *In* **O2PSMT**, *$\mathcal{C}$ is the set of all possible RS codewords of length N, encoded using all possible polynomials of degree δ over $\mathbb{F}$, for fixed $\alpha_1, \ldots, \alpha_{n+u}$. Here α_i is associated with wire f_i for $1 \leq i \leq n$ and α_{n+j} is associated with b_j for $1 \leq j \leq u$. The hamming distance* [10] between any two codeword in $\mathcal{C}$ is $N-\delta = n+u-\delta \geq 2t+1$. Briefly, **O2PSMT** works as follows: **S** and **R** communicate with each other to agree on a random polynomial of degree δ, ensuring that $\mathcal{A}_t$ knows t points on it. Once this is done, both **S** and **R** generate a common information theoretic secure pad of length $(\delta+1-t)$, which is completely unknown to $\mathcal{A}_t$. Then, **S** blinds the message with the pad and reliably sends the blinded message to **R**. **O2PSMT** is presented below and its proofs are differed in **APPENDIX D**.

Protocol O2PSMT

Phase I: R to S: **R** selects a random vector $R = (r_1, \ldots, r_u)$ over $\mathbb{F}$ and sends r_j to **S** along wire b_j.

Phase II: S to R:

1. Let **S** receive $\overline{R}$. **S** then select a codeword C from $\mathcal{C}$ such that last u components of C is same as $\overline{R}$. This is always possible because $\delta \geq u$ and every RS codeword in $\mathcal{C}$ corresponds to a unique δ degree polynomial. Let C correspond to polynomial $F(x)$. **S** sends j^{th} component of C over wire f_j in *top band*.
2. **S** computes $\Gamma = m \oplus Z$ where $Z = \textbf{EXTRAND}_{N,\delta+1-t}(C_{(\delta+1)})$ and $C_{(\delta+1)}$ denotes the first $\delta+1$ components of C. **S** then broadcasts the blinded message Γ over the entire *top band*.

Local Computation by R At The End of Phase II:

1. After receiving information over the *top band*, **R** possesses $N = n+u$ length vector Y (by combining the values received over the top band and values sent over the bottom band) corresponding to codeword C, such that Y is different from C at most at t locations. **R** applies RS decoding algorithm on Y to recover C by correcting t errors. Once C is obtained, **R** computes Z in the same way as done by **S**.
2. **R** also receives Γ correctly. Now **R** recovers m by computing $m = \Gamma \oplus Z$.

5 Lower Bounds for Three or More Phase PSMT

Recall that from [5], any three or more phase PSMT requires $n = \max(3t - 2u + 1, 2t + 1)$ wires in the *top* band to tolerate $\mathcal{A}_t$. To build our lower bound argument for three or more phase PSMT protocol, we need a few concepts from secret sharing and Maximum Distance Separable (MDS) codes. Hence we briefly recall them before presenting our lower bound result.

5.1 Secret Sharing Schemes and Maximum Distance Separable (MDS) Codes

Definition 4 (x-out-of-n Secret Sharing Scheme (SSS) [20]) *: An x-out-of-n Secret Sharing Scheme (SSS) is a probabilistic function $S : \mathbb{F} \rightarrow \mathbb{F}^n$ with the property that for any $M \in \mathbb{F}$ and $S(M) = (s_1, \ldots, s_n)$, no information on M can be inferred from any x elements of $(s_1, \ldots, s_n)$ and M can be recovered from any $x + 1$ elements in $(s_1, \ldots, s_n)$.*

The set of all possible $(s_1, \ldots, s_n)$ can be viewed as a code and its elements as codewords [5]. If the code is a Maximum Distance Separable (MDS) code [10, 5] (e.g RS code), then it can correct c errors and simultaneously detect d additional errors iff $n - x > 2c + d$ [10, 5]. An x-out-of-n SSS is called MDS x-out-of-n SSS if it is constructed from a MDS code. MDS SSSs can be constructed from any MDS codes, for example RS codes [10, 11, 5]. So we have the following theorem on the error correction and detection capability of MDS x-out-of-n SSS:

Theorem 8 ([10, 5]) *Any MDS x-out-of-n SSS can correct c errors and detect d additional errors in a codeword iff $n - x > 2c + d$.*

5.2 The Lower Bound on Communication Complexity

We now derive the lower bound on the communication complexity of any three or more phase PSMT protocol tolerating $\mathcal{A}_t$. We first give the following definition:

Definition 5 ($(\alpha, \beta, \gamma, m, \ell)$-SSS:) *Given a secret m containing ℓ field elements from $\mathbb{F}$, an $(\alpha, \beta, \gamma, m, \ell)$-SSS generates α shares of m, such that any set of β shares have full information about the secret m, while any set of γ shares have no information about the secret m with $\alpha > \beta > \gamma$.*

Theorem 9 *Suppose there exists u wires in the bottom band and $n = \max(3t - 2u + 1, 2t + 1)$ wires in the top band. Then any three or more phase PSMT protocol that securely sends a message m containing ℓ field elements from $\mathbb{F}$ tolerating $\mathcal{A}_t$ must communicate*

(a) $\Omega(\frac{n\ell}{n-(3t-2u)})$ field elements when $0 < u \leq t$.

(b) $\Omega(\ell)$ field elements when $u > t$.

Important Note: Note that when $u = 0$, then any multiphase PSMT turns out to be a single phase PSMT. From results of [6], any single phase PSMT requires $n \geq 3t + 1$ wires from **S** to **R**. In [7, 22] it is shown that any single phase PSMT must communicate $\Omega(\frac{n\ell}{n-3t})$ field elements for sending ℓ field elements. This resolves the issue of lower bound for $u = 0$.

Proof: We first prove part (a) of the theorem. The outline of the proof strategy is as follows: we first show that the communication complexity of any three or more phase PSMT protocol tolerating $\mathcal{A}_t$ to send a message $m \in \mathbb{F}^\ell$ is not less than the share complexity (sum of all the shares) of an $(n, (n - 2(t - u)), t, m, \ell)$-SSS (see Lemma 1). We then show that the share complexity of any $(n, (n - 2(t - u)), t, m, \ell)$-SSS is $\Omega(\frac{n\ell}{n-(3t-2u)})$ field elements (see Lemma 2). Part (a) of Theorem 9 will follow from Lemma 1 and Lemma 2. So we now proceed to prove Lemma 1.

Lemma 1 *Let $0 < u \leq t$ and $n = max(3t - 2u + 1, 2t + 1)$. Then the communication complexity of any 3 or more phase PSMT protocol tolerating $\mathcal{A}_t$ to send a message $m \in \mathbb{F}^\ell$ is not less than the share complexity (sum of all the shares) of an $(n, (n - 2(t - u)), t, m, \ell)$-SSS.*

PROOF: Let Π be a PSMT protocol which runs for $p \geq 3$ phases. W.l.o.g the view of $\mathbf{S}$ in Π, denoted by $view_{\Pi}^{\mathbf{S}}$ is drawn from a probability distribution that depends on the message m, the coin flips $\mathcal{R}^{\mathbf{S}}$ of $\mathbf{S}$, the coin flips $\mathcal{R}^{\mathbf{R}}$ of $\mathbf{R}$, the coin flips $\mathcal{R}^{\mathcal{A}}$ of $\mathcal{A}_t$ (w.l.o.g, we assume that the value of $\mathcal{R}^{\mathcal{A}}$ will determine the choice of faulty wires controlled by $\mathcal{A}_t$). W.l.o.g, we assume that $\mathbf{S}$ is silent in even phases and $\mathbf{R}$ is silent in odd phases [6, 5]. Now consider the following possible strategy for $\mathcal{A}_t$ in Π:

1. First $\mathcal{A}_t$ uses $\mathcal{R}^{\mathcal{A}}$ to choose a value r.
2. If $r = 0$, then $\mathcal{A}_t$ uses $\mathcal{R}^{\mathcal{A}}$ to choose t wires $f_{j_1}, f_{j_2}, \ldots, f_{j_t}$ from the top band and behaves passively over these paths. This means the adversary proceeds according to protocol Π.
3. If $r = 1$, then $\mathcal{A}_t$ uses $\mathcal{R}^{\mathcal{A}}$ to choose $t-u$ wires $f_{j_1}, f_{j_2}, \ldots, f_{j_{t-u}}$ from the *top* band and all the u wires from the *bottom* band. In this case $\mathcal{A}_t$ corrupts all the u wires in the bottom band and the $t-u$ wires $f_{j_1}, f_{j_2}, \ldots, f_{j_{t-u}}$ from the top band. $\mathcal{A}_t$ also uses $\mathcal{R}^{\mathcal{A}}$ to choose a message $\overline{m} \in \mathbb{F}$ according to the same probability distribution from which the actual message m was drawn. Now over the corrupted wires, $\mathcal{A}_t$ behaves in the following way: (i) Over the wires $f_{j_1}, f_{j_2}, \ldots, f_{j_{t-u}}$, it ignores what $\mathbf{S}$ sends in odd phases of Π and simulates what $\mathbf{S}$ would send to $\mathbf{R}$ if $\overline{m}$ would have been the message. (ii) Over the paths in the bottom band, it ignores what $\mathbf{R}$ sends to $\mathbf{S}$ in even phases of Π and simulates what $\mathbf{R}$ would send to $\mathbf{S}$ when $r = 0$.

$\mathcal{A}_t$ can behave in the above manner with non-zero probability. Now let $\alpha_{i,j}^{\mathbf{S}}$ be the values that $\mathbf{S}$ sends on wire f_i in phase j of protocol Π. Let $\alpha_i^{\mathbf{S}} = (\alpha_{i,1}^{\mathbf{S}}, \ldots, \alpha_{i,p}^{\mathbf{S}})$ i.e. $\alpha_i^{\mathbf{S}}$ is the concatenation of the values sent by $\mathbf{S}$ over wire f_i during the execution of Π. We can view $\alpha_i^{\mathbf{S}}$'s as the shares of message m. Now if $r = 0$, due to the fact that Π is a PSMT protocol, $\mathcal{A}_t$ should not get any information on m from any t shares from the set $\{\alpha_1^{\mathbf{S}}, \ldots, \alpha_n^{\mathbf{S}}\}$. This implies that $(\alpha_1^{\mathbf{S}}, \ldots, \alpha_n^{\mathbf{S}})$ is an x-out-of-n SSS for $x \geq t$. Note that when $x > t$, it is still ensured that t shares from the set $\{\alpha_1^{\mathbf{S}}, \ldots, \alpha_n^{\mathbf{S}}\}$ do not reveal any information on m. Now if $r = 1$, due to the fact that Π is also a PRMT protocol, $\mathbf{R}$ must be able to correct any $t-u$ errors in the shares $(\alpha_1^{\mathbf{S}}, \ldots, \alpha_n^{\mathbf{S}})$ and thus recover the message m. Summing up, $(\alpha_1^{\mathbf{S}}, \ldots, \alpha_n^{\mathbf{S}})$ is an MDS x-out-of-n SSS with the capability of correcting $t-u$ error where $x \geq t$. Now by Theorem 8, an MDS x-out-of-n SSS can correct $(t-u)$ errors if

$$n - x > 2(t-u) \;\Rightarrow\; x < n - 2(t-u) \Rightarrow\; x + 1 \leq n - 2(t-u). \tag{1}$$

This shows that the communication done by $\mathbf{S}$ (alone) is equivalent to the share complexity (sum of all the shares) of an $(n, (n-2(t-u)), t, m, \ell)$-SSS. Thus ignoring the communication done by $\mathbf{R}$, we can say that the communication done in protocol Π is not less than the share complexity (sum of all the shares) of an $(n, (n-2(t-u)), t, m, \ell)$-SSS. □

Lemma 2 *The share complexity of any $(n, (n-2(t-u)), t, m, \ell)$-SSS is $\Omega(\frac{n\ell}{n-(3t-2u)})$ field elements.*

PROOF: We define the following notations:

1. $\mathcal{M}$ denotes the message space from where the message m is selected. In our context, $\mathcal{M} = \mathbb{F}^{\ell}$.
2. For $i = 1, \ldots, n$, $\mathbf{X}_i^m$ denotes the set of all possible i^{th} share corresponding to message $m \in \mathcal{M}$, that could be generated by any $(n, (n-2(t-u)), t, m, \ell)$-SSS.
3. For $j \geq i$, $\mathbf{M}_{i,j}^m \subseteq \mathbf{X}_i^m \times \mathbf{X}_{i+1}^m \times \ldots \times \mathbf{X}_j^m$ denotes the set of all possible $\{i^{th}, (i+1)^{th}, \ldots, j^{th}\}$ shares, corresponding to message $m \in \mathcal{M}$, that could be generated by any $(n, (n-2(t-u)), t, m, \ell)$-SSS.
4. $\mathbf{M}_{i,j} = \bigcup_{m \in \mathcal{M}} \mathbf{M}_{i,j}^m$ and $\mathbf{X}_i = \bigcup_{m \in \mathcal{M}} \mathbf{X}_i^m$. We call $\mathbf{X}_i$ as the *capacity* of i^{th} share and $\mathbf{M}_{i,j}$ as the *capacity* of the set of $\{i^{th}, (i+1)^{th}, \ldots, j^{th}\}$ shares.

To generate n shares for message m, any $(n, (n-2(t-u)), t, m, \ell)$-SSS would select one element from the set $\mathbf{X}_i$, as the i^{th} share of m, for $i = 1, \ldots, n$. Each element of the set $\mathbf{X}_i$ can be represented by $\log |\mathbf{X}_i|$ bits. Thus, the share complexity corresponding to message m will be $\Sigma_{i=1}^{n} \log |\mathbf{X}_i|$ bits. In the sequel, we show that $\Sigma_{i=1}^{n} \log |\mathbf{X}_i| \geq \left(\frac{n\ell \log(|\mathbb{F}|)}{n-(3t-2u)}\right)$.

From the property of a $(n, (n-2(t-u)), t, m, \ell)$-SSS, any set of t shares is *independent* of the message. Thus, for any two messages $m_1, m_2 \in \mathcal{M}$, the following should hold:

$$\mathbf{M}_{2t-2u+1,3t-2u}^{m_1} = \mathbf{M}_{2t-2u+1,3t-2u}^{m_2}. \tag{2}$$

Though we focussed on specific set of t shares, namely $\{(2t-2u+1)^{th},\ldots,(3t-2u)^{th}\}$, the above relation should hold for any selection of t shares. Also, from the property of a $(n,(n-2(t-u)),t,m,\ell)$-SSS, any set of $n-2(t-u)$ shares have *full* information about m and uniquely determine m. Thus,

$$\mathbf{M}^{m_1}_{2t-2u+1,n} \cap \mathbf{M}^{m_2}_{2t-2u+1,n} = \emptyset. \tag{3}$$

As above, though we focussed on specific set of $n-(2t-2u)$ shares, namely $\{(2t-2u+1)^{th},\ldots,n^{th}\}$, the above relation should hold for any selection of $n-(2t-2u)$ shares. From (2), $\mathbf{M}^{m}_{2t-2u+1,3t-2u}$ will be same for all m. Thus, (3) will hold only if $\mathbf{M}^{m}_{3t-2u+1,n}$ is *unique* for every m. Hence,

$$|\mathbf{M}_{3t-2u+1,n}| = |\mathcal{M}|. \tag{4}$$

From the definition of $\mathbf{X}_i$ and $\mathbf{M}_{i,j}$, we get $\Pi^{n}_{i=3t-2u+1}|\mathbf{X}_i| \geq |\mathbf{M}_{3t-2u+1,n}|$. Combining this with (4), we get

$$\Pi^{n}_{i=3t-2u+1}|\mathbf{X}_i| \geq |\mathcal{M}|. \tag{5}$$

Let $g = n-(3t-2u)$. The inequality in (5) holds for any set of of g shares $\mathcal{D}$, where $|\mathcal{D}| = g$; i.e., $\Pi_{i\in\mathcal{D}}|\mathbf{X}_i| \geq |\mathcal{M}|$. In particular, we consider n such sets (consisting of g shares), namely $\mathcal{D}_0,\ldots,\mathcal{D}_{n-1}$ where $\mathcal{D}_k$ consists of $\{(kg+1)^{th} \bmod n, (kg+2)^{th} \bmod n,\ldots,(kg+g)^{th} \bmod n\}$ shares. Thus for each $\mathcal{D}_k$, $\Pi_{i\in\mathcal{D}_k}|\mathbf{X}_i| \geq |\mathcal{M}|$ holds. Taking product over all $\mathcal{D}_k$'s, we obtain $\Pi^{n-1}_{k=0}\Pi_{j\in\mathcal{D}_k}|\mathbf{X}_j| \geq |\mathcal{M}|^n$. Now notice that the i^{th} share is accounted exactly g times in total in $\mathcal{D}_0,\ldots,\mathcal{D}_{n-1}$. Thus, we get $|\mathcal{M}|^n \leq \Pi^{n-1}_{k=0}\Pi_{j\in\mathcal{D}_k}|\mathbf{X}_j| = (\Pi^{n}_{i=1}|\mathbf{X}_i|)^g$. Taking log, we obtain

$$n\log(|\mathcal{M}|) \leq g\Sigma^{n}_{i=1}\log(|\mathbf{X}_i|) \Rightarrow \Sigma^{n}_{i=1}\log(|\mathbf{X}_i|) \geq \left(\frac{n\ell\log(|\mathbb{F}|)}{g}\right)$$

As $\log(|\mathcal{M}|) = \ell\log(|\mathbb{F}|)$ and $g = n-(3t-2u)$, from the above inequality, we get $\Sigma^{n}_{i=1}\log(|\mathbf{X}_i|) \geq \left(\frac{n\ell\log(|\mathbb{F}|)}{n-(3t-2u)}\right)$. As mentioned earlier, $\Sigma^{n}_{i=1}\log(|\mathbf{X}_i|)$ denotes the share complexity in bits of distributing n shares of a message m using any $(n,(n-2(t-u)),t,m,\ell)$-SSS. From the above inequality, the share complexity of $(n,(n-2(t-u)),t,m,\ell)$-SSS is $\Omega\left(\frac{n\ell\log(|\mathbb{F}|)}{n-(3t-2u)}\right)$ bits. Now each field element from $\mathbb{F}$ can be represented by $\log(|\mathbb{F}|)$ bits. Thus the share complexity is $\Omega\left(\frac{n\ell}{n-(3t-2u)}\right)$ field elements.

Part (a) of Theorem 9 now follows from Lemma 1 and Lemma 2. Now part (b) simply follows from the fact that any PSMT protocol has to at least send the message and hence $\Omega(\ell)$ field elements. □

In the next section, we show that our lower bounds on the communication complexity of any three or more phase PSMT are *asymptotically* tight.

6 Upper Bounds for Three or More Phase PSMT

From Theorem 9, we get the following implications: Any three or more phase PSMT protocol which wishes to send a message m containing ℓ field elements, has to communicate (i) $\Omega(\frac{n\ell}{n-(3t-2u)})$ field elements when $0 < u < \frac{t}{2}$ and $n \geq 3t-2u+1$, (ii) $\Omega(\frac{n\ell}{2u-t})$ field elements when $\frac{t}{2} \leq u \leq t$ and $n \geq 2t+1$, (iii) $\Omega(\ell)$ field elements when $u > t$ and $n \geq 2t+1$.

To show that the lower bounds in (i), (ii) and (iii) are *asymptotically tight*, we present three different protocols in the sequel. All our protocols use the concept of pseudo-basis and properties of Reed-Solomon encoding-decoding (see Section 2).

6.1 Communication Optimal PSMT with $0 < u < \frac{t}{2}$ and $n = 3t-2u+1$

In this section, we present a three phase communication optimal PSMT protocol called **O3PSMT**, which securely sends $\ell = n^2u$ field elements by communicating $\mathcal{O}(n^3u) = \mathcal{O}(n\ell)$ field elements. Informally the protocol works as follows: **S** tries to correctly establish an information theoretic secure one time pad of size n^2u with **R**. *Let $\mathcal{C}$ denote the set of all RS codewords of length $n = 3t-2u+1$ over $\mathbb{F}$, encoded using all possible polynomials of degree t over $\mathbb{F}$, for fixed $\alpha_1,\ldots,\alpha_n$. Here α_i is associated*

with wire f_i. Hence the hamming distance between any two codeword is $n - t = 2t - 2u + 1 \geq t + 1$. In protocol **O3PSMT**, **S** selects a number of random codewords from $\mathcal{C}$ and sends them across the n wires. **R** receives the codewords and finds the pseudo-basis of the received codewords. **R** then sends the pseudo-basis, pseudo-dimension and index set through the *bottom band*. We say that a pseudo-basis, pseudo-dimension and index set triple received over a wire in bottom band is **valid** iff all the codewords listed in pseudo-basis differs from the corresponding original codewords (sent by **S**) at most at t locations. Note that **S** has no knowledge on whether the original pseudo-basis generated by **R** is received by him. So **S** broadcasts all the valid triple of (pseudo basis, pseudo-dimension and index set) as received by him along with the corresponding list of corrupted wires. Now **R** correctly receives all the pseudo-basis, pseudo-dimension and index set, along with their corresponding list of corrupted wires. **R** checks whether the pseudo-basis generated by him is present in the received list of pseudo-basis. If yes then he knows the set of corrupted wires and can recover all the original codewords (sent by **S**) by neglecting the values received over those corrupted wires during first phase. Otherwise **R** learns that entire *bottom band* is corrupted and hence in the *top band* there are at most $t - u$ Byzantine faults. So **R** can correct these $t - u$ errors in each of the codeword, received during first phase and thus can recover all the original codewords. Hence in any case **S** and **R** will agree on all the codewords chosen by **S**.

Protocol O3PSMT(m, ℓ, n, u, t)

Phase I: S to R: **S** selects $P = n^2u + ut = \ell + ut$ random codewords $C_1, \ldots, C_P$ from $\mathcal{C}$. Let $C_i = (c_{i1}, \ldots, c_{in})$. Also let $F_1(x), \ldots, F_P(x)$ be the t degree polynomials corresponding to the codewords. Now **S** sends j^{th} component of all the codewords along wire f_j in *top band*.

Phase II: R to S

1. Let **R** receive $Y_i = C_i + E_i$ corresponding to codeword C_i and let $\mathcal{Y} = \{Y_1, \ldots, Y_P\}$.
2. **R** invokes $(p, \mathcal{B}, \mathcal{I}) =$ **FindPseudo-basis**$(\mathcal{Y})$ to find pseudo-basis $\mathcal{B} = \{Y_{a_1}, \ldots, Y_{a_p}\} \subset \mathcal{Y}$, pseudo-dimension $p = |\mathcal{B}|$ and index set $\mathcal{I} = \{a_1, \ldots, a_p\} \subset \{1, \ldots, P\}$. **R** then broadcasts $(\mathcal{B}, p, \mathcal{I})$ through the *bottom band*.

Phase III: S to R

1. **S** may receive different triples over different wires. Let **S** receive $(\mathcal{B}^j, p^j, \mathcal{I}^j)$ over wire b_j in *bottom band*. Let $\mathcal{B}^j = \{Y^j_{a^j_1}, \ldots, Y^j_{a^j_{p^j}}\}$ and $\mathcal{I}^j = \{a^j_1, \ldots, a^j_{p^j}\}$.
2. **S** considers the triple $(\mathcal{B}^j, p^j, \mathcal{I}^j)$ as **valid** iff $p^j = |\mathcal{B}^j|$ and every n length vector listed in $\mathcal{B}^j$ is different from the corresponding original codeword at most at t locations. For every **valid** triple $(\mathcal{B}^j, p^j, \mathcal{I}^j)$, **S** finds $E^j_{a^j_1} = Y^j_{a^j_1} - C_{a^j_1}$ ..., $E^j_{a^j_{p^j}} = Y^j_{a^j_{p^j}} - C_{a^j_{p^j}}$ and computes $CORRUPTED^j = \cup_{\alpha=1}^{p^j} support(E^j_{a^j_\alpha})$.
3. **S** computes $\Lambda = \cup_j \{\mathcal{I}^j | (\mathcal{B}^j, p^j, \mathcal{I}^j)$ is a valid triple$\}$. Then **S** concatenates all the $F_i(0)$'s such $i \notin \Lambda$ and forms an information theoretic secure pad Z of length at least n^2u (since $|\Lambda| \leq ut$ and $P = n^2u + ut$).
4. Now **S** broadcasts the following to **R**: (i) every valid triple $(\mathcal{B}^j, p^j, \mathcal{I}^j)$ and corresponding list of corrupted wires $CORRUPTED^j$ (ii) If there is no **valid** triple, then the message **"Entire Bottom band is corrupted"**, (iii) blinded message $\Gamma = Z_\ell \oplus m$ where Z_ℓ contains first ℓ elements from Z.

Local Computation by R at the End of Phase III:

1. **R** correctly receives all information sent by **S** in **Phase III** and computes Λ in same way as done by **S**.
2. If either **R** gets the message **"Entire Bottom band is corrupted"** or if **R** finds his original triple $(\mathcal{B}, p, \mathcal{I})$ is not present in the list of **valid** triples sent by **S**, then **R** does the following:
   (a) Conclude that entire *bottom band* is corrupted and hence in the top band there are at most $t - u$ faults.
   (b) Recover all $F_i(x)$ such that $i \notin \Lambda$ by applying RS decoding algorithm on Y_i and correcting $t - u$ faults.
   (c) Recover pad Z (and hence Z_ℓ) by concatenating $F_i(0)$ for all $i \notin \Lambda$ and hence the message $m = \Gamma \oplus Z_\ell$.
3. If **R** finds that his original triple $(\mathcal{B}, p, \mathcal{I})$ is present in the list of **valid** triples sent by **S** and let $(\mathcal{B}^j, p^j, \mathcal{I}^j)$ is same as $(\mathcal{B}, p, \mathcal{I})$, then **R** does following:
   (a) Identify all the wires in $CORRUPTED^j$ ($|CORRUPTED^j| \leq t$) as the corrupted wires in **Phase I**.
   (b) Ignore all information received over the wires in $CORRUPTED^j$ ($|CORRUPTED^j| \leq t$) during **Phase I**. Reconstruct all the polynomial $F_i(x)$ such that $i \notin \Lambda$ by considering the correct values on $F_i(x)$ received over remaining wires (which are at least $t + 1$) during **Phase I**.
   (c) Recover the message m in the same way as described in step 2.

But during the transmission of pseudo-basis over u wires, $\mathcal{A}_t$ can generate u distinct **valid** pseudo-basis each containing at most t disjoint codewords (this he can do by guessing with very non-zero probability). Therefore initially **S** should send sufficient number of codewords such that after removing all the ut codewords appearing in the received list of valid pseudo-basis, the remaining codewords can be used to construct an information theoretic secure pad of size n^2u. Once the pad is established, **S** uses the pad to blind the message and sends the blinded message reliably to **R**. The proofs for **O3PSMT** are presented in **APPENDIX E**.

6.2 Six Phase Communication Optimal PSMT when $\frac{t}{2} \leq u \leq t$ and $n \geq 2t+1$

In this section, we present a six phase communication optimal PSMT protocol called **O6PSMT** where $n = 2t+1$ and $\frac{t}{2} \leq u \leq t$. Protocol **O6PSMT** securely sends $\ell = n^2u$ field elements by communicating $O\left(\frac{n^3u}{2u-t}\right) = O\left(\frac{n\ell}{2u-t+1}\right)$ field elements, thus *asymptotically* satisfying the lower bound given in Theorem 9. Interestingly, when $u = \frac{t}{2} + \Theta(t)$, then Protocol **O6PSMT** sends ℓ field elements securely by communicating $\mathcal{O}(\ell)$ field elements. Protocol **O6PSMT** achieves it's goal by allowing **S** and **R** to share $\frac{n^2u}{2u-t+1}$ common polynomials each of degree $2u$, such that $\mathcal{A}_t$ knows only t points on each of them. Once this is done, both **S** and **R** can generate an information theoretic pad of length n^2u by using **EXTRAND** algorithm. **S** can then blind the message and sends it to **R**. However, note that **S** cannot send the blinded message to **R** by sending it over the entire *top* band, as done in protocol **O3PSMT**. Because the communication complexity will then become $\mathcal{O}(n^3u)$ and hence, it will no longer satisfy the lower bound of Theorem 9. So **S** reliably sends the blinded message by using protocol **OPRMT** given in Section 3, which takes 3 phases. Since here $n = 2t+1$ and $(n-2t)+2u = \Omega(n)$, we can execute **OPRMT**. **R** can recover the message since he knows the pad. *In* **O6PSMT**, $\mathcal{C}$ *denotes the set of all possible RS codewords of length* $N = n+u = 2t+1+u$ *encoded using all possible polynomials of degree* $2u \geq t$ *over* $\mathbb{F}$. *Hence the hamming distance between any two codeword is* $N - 2u = 2t - u + 1 \geq t + 1$. Protocol **O6PSMT** and the proofs of its properties are provided in **APPENDIX E** due to space constraints.

6.3 Six Phase Communication Optimal PSMT when $u > t$ and $n \geq 2t+1$

If $u = t$ and $n = 2t+1 = \Theta(t)$, then from Theorem 22, protocol **O6PSMT** securely sends $\ell = n^2u = \Theta(n^3)$ field elements by communicating $\mathcal{O}(n^3)$ field elements. Hence, if $u > t$ and $n \geq 2t+1$, then **S** and **R** can execute **O6PSMT** by considering the first $2t+1$ wires in the *top* band and first t wires in the *bottom* band. Thus, we have the following theorem:

Theorem 10 *Suppose* $n \geq 2t+1$ *and* $u > t$. *Then there exists a six phase PSMT protocol tolerating* $\mathcal{A}_t$, *which securely sends* ℓ *(*$\ell = n^3$*) field elements by communicating* $\mathcal{O}(\ell)$ *field elements.*

7 Conclusion and Open Problems

In this paper, we have derived the necessary and sufficient condition for the existence of communication optimal PRMT protocols in directed networks.

In the context of PSMT, we have derived *tight* bounds on the communication complexity of PSMT protocols in directed networks, which are first of their kind. The summary of our results for PSMT (marked with *) is given below.

# Phases	Characterization	Lower Bound on Communication Complexity
1	$n \geq 3t+1$ [6, 5]	$\Omega(\frac{n\ell}{n-3t})$ [7]
2	If $0 < u \leq t$ then $n \geq 3t-u+1$*	$\Omega(\frac{N\ell}{N-3t})$; $N = n+u$*
	If $u > t$ then $n \geq 2t+1$*	$\Omega(\frac{n\ell}{n-2t})$*
3	If $0 < u \leq t$ then $n \geq \max(3t-2u+1, 2t+1)$ [5]	$\Omega(\frac{n\ell}{n-(3t-2u)})$*
	If $u > t$ then $n \geq 2t+1$ [5]	$\Omega(\ell)$*

It would be interesting to reduce the phase complexity of our *six phase* PSMT protocol. Our protocols achieve optimality only if the message is of some minimum specific length. It would be interesting to design PRMT and PSMT protocols, which are communication optimal for message of any length.

References

[1] S. Agarwal, R. Cramer, and R. de Haan. Asymptotically optimal two-round perfectly secure message transmission. In C. Dwork, editor, *Proc. of Advances in Cryptology: CRYPTO 2006*, LNCS 4117, pages 394–408. Springer-Verlag, 2006.

[2] B. V. Ashwinkumar, A. Patra, A. Choudhary, K. Srinathan, and C. Pandu Rangan. On trade-off between network connectivity, phase complexity and communication complexity of reliable communication tolerating mixed adversary. In *PODC*, pages 115–124, 2008.

[3] 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.

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

[5] Y. Desmedt and Y. Wang. Perfectly secure message transmission revisited. Cryptology ePrint Archive, Report 2002/128. A preliminary version appeared in Proc. of EUROCRYPT 2002, 2002.

[6] D. Dolev, C. Dwork, O. Waarts, and M. Yung. Perfectly secure message transmission. *JACM*, 40(1):17–47, 1993.

[7] Matthias Fitzi, Matthew K. Franklin, Juan A. Garay, and S. Harsha Vardhan. Towards optimal and efficient perfectly secure message transmission. In *TCC*, volume 4392 of *LNCS*, pages 311–322. Springer Verlag, 2007.

[8] K. Kurosawa and K. Suzuki. Truly efficient 2-round perfectly secure message transmission scheme. In *Proc. of EUROCRYPT*, pages 324–340, 2008.

[9] N. A. Lynch. *Distributed Algorithms*. Morgan Kaufmann, 1998.

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

[11] R. J. McEliece and D. V. Sarwate. On sharing secrets and Reed-Solomon codes. *Communications of the ACM*, 24(9):583–584, 1981.

[12] K. Menger. Zur allgemeinen kurventheorie. *Fundamenta Mathematicae*, 10:96–115, 1927.

[13] A. Patra, A. Choudhary, and C. Pandu Rangan. Constant phase efficient protocols for secure message transmission in directed networks. In *ACM PODC*, pages 322–323, 2007.

[14] A. Patra, A. Choudhary, and C. Pandu Rangan. Unconditionally reliable and secure message transmission in directed networks revisited. Cryptology ePrint Archive, Report 2008/262. A preliminary version appeared in Proc. of SCN 2008, 2008.

[15] A. Patra, A. Choudhary, and C. Pandu Rangan. Brief announcement: Perfectly secure message transmission in directed networks revisited. To appear in Proc. of PODC 2009, 2009.

[16] A. Patra, A. Choudhary, K. Srinathan, and C. Pandu Rangan. Perfectly reliable and secure communication in directed networks tolerating mixed adversary. In *DISC*, pages 496–498, 2007.

[17] Arpita Patra, Bhavani Shankar, Ashish Choudhary, K. Srinathan, and C. Pandu Rangan. Perfectly secure message transmission in directed networks tolerating threshold and non threshold adversary. In *CANS*, pages 80–101, 2007.

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

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

[20] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[21] B. Shanker, P. Gopal, K. Srinathan, and C. Pandu Rangan. Unconditional reliable message transmision in directed networks. In *SODA 2008*, pages 1048–1055, 2008.

[22] K. Srinathan. Secure distributed communication. PhD Thesis, IIT Madras, 2006.

[23] K. Srinathan, A. Narayanan, and C. Pandu Rangan. Optimal perfectly secure message transmission. In *Proc. of Advances in Cryptology: CRYPTO 2004*, LNCS 3152, pages 545–561. Springer-Verlag, 2004.

[24] K. Srinathan and C. Pandu Rangan. Possibility and complexity of probabilistic reliable communication in directed networks. In *Proc. of 25th PODC*, pages 265–274. ACM Press, 2006.

[25] Y. Wang and Y. Desmedt. Perfectly secure message transmission revisited. *IEEE Transactions on Information Theory*, 54(6):2582–2595, 2008.

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

APPENDIX A: Properties of Protocols SP-REL and OPRMT

Lemma 3 *In* **SP-REL***, if at most $t-b$ wires are corrupted by the adversary, then* $\mathbf{R}$ *recovers m. Otherwise,* $\mathbf{R}$ *detects that more than $t-b$ wires have been corrupted in the top band.*

PROOF: In the protocol, $\mathbf{R}$ receives $L = n \geq 2t+1$ values for each $\mathbf{B}_i$, each of which is RS encoded using a polynomial of degree $k-1 = X+b-1$. Now substituting these values in Theorem 1, we find that RS decoding can correct $c = t-b$ errors and simultaneously detect additional $d = b$ errors in each of the received n length vectors. If at most $t-b$ errors occur in the *top band*, then decoding algorithm will correct them and hence $\mathbf{R}$ will be able to recover m. On the other hand if more than $t-b$ wires are corrupted in the *top band*, then more than $t-b$ values will be corrupted in at least one of the received vectors. After correcting $t-b$ errors in that vector, the RS decoding algorithm will detect additional errors in the vector. So $\mathbf{R}$ will know that more than $t-b$ wires are corrupted in the *top band* (though he will not know the identity of the corrupted wires). In this case, $\mathbf{R}$ will fail to recover m. □

Lemma 4 SP-REL *communicates $\mathcal{O}\left(\frac{n\ell}{(n-2t)+b}\right)$ field elements where $|m| = \ell$.*

PROOF: Follows from the working of the protocol. □

Theorem 11 OPRMT *reliably sends m in at most three phases.*

PROOF: The proof is divided into two cases: (a) more than $t-b$ errors take place during **Phase I** and (b) at most $t-b$ errors take place during **Phase I**. If more than $t-b$ errors take place during **Phase I** then $\mathbf{R}$ detects it (see Lemma 3) and sends `ERROR` along with the tuple (α, C_α^R) through the *bottom band* where C_α^R is the received n tuple in which $\mathbf{R}$ has detected more than $t-b$ errors. In this case, in the *bottom band*, there can be at most $b-1$ faults. Now since $b = min(\frac{t}{2}, \frac{u}{2})$, irrespective of whether $b = \frac{u}{2}$ or $\frac{t}{2}$, $\mathbf{R}$ will correctly receive (α, C_α^R) and `ERROR` over at least $\frac{u}{2}$ wires. So $\mathbf{S}$ will locally find the number of mismatches between what $\mathbf{R}$ had received and what $\mathbf{S}$ had sent during **Phase I**. Thus $\mathbf{S}$ will know the identity of more than $t-b$ Byzantine faults and adds them to the list L_{fault}. $\mathbf{S}$ then broadcasts L_{fault} to $\mathbf{R}$ through entire *top band*. So $\mathbf{R}$ also comes to know the identity of these faults. Finally, $\mathbf{S}$ re-sends the message by executing **SP-REL**$(m, \ell, n-|L_{fault}|, t-|L_{fault}|, |L_{fault}|)$ over the first $n-|L_{fault}|$ wires. Now since there can be indeed $t-|L_{fault}|$ faults in the *top band*, by Lemma 3 $\mathbf{R}$ will be able to recover the message after correcting $t-|L_{fault}|$ faults.

On the other hand, if during **Phase I**, at most $t-b$ Byzantine faults occur, then from Lemma 3, **R** will be able to recover the message correctly after **Phase I**. **R** then sends `SUCCESS` through the *bottom band*. Since it has recovered m, it will simply neglect whatever it receives from **S** during **Phase III**. Hence the theorem holds. □

Theorem 12 *The protocol* **OPRMT** *is a communication optimal PRMT protocol which sends* $\Omega(nt)$ *field elements by communicating* $\mathcal{O}(nt)$ *field elements.*

PROOF: Since $n = 2t+1, \ell = \Omega(nt)$, $n - 2t + 2u = \Omega(n)$ and $b = \min(\frac{u}{2}, \frac{t}{2})$, from Lemma 4, the communication complexity of **Phase I** is $\mathcal{O}(nt)$. During **Phase II**, **R** either sends `SUCCESS` or a tuple **(index,** n **length vector)**, along with `ERROR` over all the u wires in bottom band. This involves communication of at most $nu = \mathcal{O}(nt)$ field elements. During **Phase III**, **S** either sends nothing or re-sends the message. Communication complexity of re-sending the message is $\mathcal{O}(\frac{(n-|L_{fault}|)|m|}{X+|L_{fault}|})$. Since $|L_{fault}| > t - b > \frac{t}{2}$, the following holds: $|L_{fault}| = \Theta(t)$ and $n - |L_{fault}| = \Theta(t)$. Hence re-sending m incurs a communication complexity of $\mathcal{O}(nt)$. Thus the total communication complexity is $\mathcal{O}(nt)$. □

APPENDIX B: Necessity Proof of Existing Characterization of Two Phase PSMT

Theorem 6 [15]: *Suppose there are disjoint set of* n *wires in the top band and* u *wires in the bottom band such that* $\mathcal{A}_t$ *controls at most* t *of these* $n+u$ *wires. Then there exists a two phase PSMT tolerating* $\mathcal{A}_t$ *only if* $n \geq max(3t-u+1, 2t+1)$.

PROOF: The proof is divided into two cases: (a) $0 < u \leq t$ and (b) $u > t$. If $u > t$, then the necessary condition says that there should exist $n = 2t+1$ wires in the *top band*. By [6, 5], $n = 2t+1$ wires from **S** to **R** are necessary for *reliably* sending m tolerating $\mathcal{A}_t$. So it is obviously necessary for PSMT.

Now if $0 < u \leq t$, then $n = 3t - u + 1$ wires in the *top band* are necessary for the existence of any two phase PSMT protocol tolerating $\mathcal{A}_t$. The proof is by contradiction. So assume that there exists a two phase PSMT protocol with $0 < u \leq t$ wires in the *bottom band* and $n = 3t - u$ wires in the *top band*, tolerating $\mathcal{A}_t$. Let Π^{2Phase} be an *execution* of the two phase PSMT protocol where **S** sends message m. Let $\mathcal{A}_t^{2Phase}$ be an adversarial strategy in Π^{2Phase}. Given Π^{2Phase} and $\mathcal{A}_t^{2Phase}$, we show that there exist an *execution* Π^{1Phase} of a single phase PSMT protocol over $N = n+u = 3t$ wires from **S** to **R** and an adversarial strategy $\mathcal{A}_t^{1Phase}$ in Π^{1Phase}, such that the views of **S** and **R** in Π^{2Phase} are identical to the views of **S** and **R** (respectively) in Π^{1Phase}. Now by the property of two phase PSMT, **R** will recover m in Π^{2Phase} tolerating any strategy $\mathcal{A}_t^{2Phase}$. Since the views are identical, **R** should also recover m in Π^{1Phase} tolerating $\mathcal{A}_t^{1Phase}$. But by results of [6], we show that **R** can not recover m in Π^{1Phase} tolerating $\mathcal{A}_t^{1Phase}$. This in turn implies that **R** will fail to recover m in Π^{2Phase} tolerating $\mathcal{A}_t^{2Phase}$, thus showing a contradiction.

We now describe the executions Π^{2Phase}, Π^{1Phase} and the adversary strategies $\mathcal{A}_t^{2Phase}$ and $\mathcal{A}_t^{1Phase}$. The random coin flips of **S**, **R** and $\mathcal{A}_t$ in Π^{2Phase} as well as in Π^{1Phase} are $\mathcal{R}^{\mathbf{S}}$, $\mathcal{R}^{\mathbf{R}}$ and $\mathcal{R}^{\mathcal{A}}$ respectively. Since Π^{2Phase} is an instance of a two phase PSMT, without loss of generality, the computation and communication during Π^{2Phase} are as follows:

1. **Phase I: R to S**: R uses $\mathcal{R}^{\mathbf{R}}$ to generate $\beta_1, \ldots, \beta_u$ and sends β_i to **S** through wire $b_i, 1 \leq i \leq u$.
2. **Phase II: S to R**: Let **S** receive β_i' through wire b_i. Based on the received information, message m and coin flips $\mathcal{R}^{\mathbf{S}}$, **S** computes $\alpha_1, \alpha_2, \ldots, \alpha_n$ and sends α_i to **R** through wire $f_i, 1 \leq i \leq n$.
3. **Computation by R at the end of Phase II**: Let **R** receive α_i' through wire f_i. Thus the view of **R** at the end of **Phase II** is $[\alpha_1', \ldots, \alpha_n', \beta_1, \ldots, \beta_u]$, while view of **S** is $[\alpha_1, \ldots, \alpha_n, \beta_1', \ldots, \beta_u']$. **R** performs local computation according to the protocol specification and correctly recovers m.

Now we present Π^{1Phase} where there exists $N = n + u = 3t$ wires $w_1, \ldots, w_N$ from **S** to **R**.

1. **Phase I: S to R**: $\mathbf{S}$ uses $\mathcal{R}^{\mathbf{S}}$ to generate $\beta'_1, \ldots, \beta'_u$ (which he can do with non-zero probability). Now assuming that $\beta'_1, \ldots, \beta'_u$ would have been received through the bottom band in Π^{2Phase}, $\mathbf{S}$ performs the same computation as in Π^{2Phase} and generates $\alpha_1, \ldots, \alpha_n$. Finally, $\mathbf{S}$ sends α_i to $\mathbf{R}$ through wire $w_i, 1 \leq i \leq n$ and β'_i through wire $w_{n+i}, 1 \leq i \leq u$.

2. **Computation by R at the end of Phase I**: Let $\mathbf{R}$ receive α''_i through wire $w_i, 1 \leq i \leq n$ and β''_i through wire $w_{n+i}, 1 \leq i \leq u$. Now $\mathbf{R}$ performs the same computation as in Π^{2Phase} to recover m.

Now consider the following strategy $\mathcal{A}_t^{2Phase}$ in Π^{2Phase}: $\mathcal{A}_t$ corrupts entire bottom band and first $t-u$ wires from top band and ensures that $\beta'_i \neq \beta_i$ for $1 \leq i \leq u$ and $\alpha'_i \neq \alpha_i$ for $1 \leq i \leq t-u$. So, the views of $\mathbf{S}$ and $\mathbf{R}$ are $(\alpha_1, \ldots, \alpha_{t-u}, \alpha_{t-u+1}, \ldots, \alpha_n, \beta'_1, \ldots, \beta'_u)$ and $(\alpha'_1, \ldots, \alpha'_{t-u}, \alpha_{t-u+1}, \ldots, \alpha_n, \beta_1, \ldots, \beta_u)$ respectively. Now consider the following strategy $\mathcal{A}_t^{1Phase}$ in Π^{1Phase}: $\mathcal{A}_t$ corrupts last u wires and first $t-u$ wires and ensures that $\beta''_i = \beta_i$ for $1 \leq i \leq u$ and $\alpha''_i = \alpha'_i$, for $1 \leq i \leq (t-u)$. Since all other wires are honest, it holds that $\alpha''_i = \alpha_i$ for $t-u+1 \leq i \leq n$. Hence in this case, the views of $\mathbf{S}$ and $\mathbf{R}$ will be exactly same as in the execution Π^{2Phase} where $\mathcal{A}_t^{2Phase}$ is the adversary strategy. If in Π^{2Phase}, $\mathbf{R}$ is able to recover m, same should hold for Π^{1Phase}. But from [6], single phase PSMT over $3t$ wires is impossible tolerating t faults done by $\mathcal{A}_t$. Hence by the argument given before, this leads to a contradiction to our assumption that Π^{2Phase} is an execution of two phase PSMT. Therefore for $0 < u \leq t$, the condition $n \geq 3t - u + 1$ should hold for two phase PSMT. □

APPENDIX C: Lower Bound on The communication Complexity of Two Phase PSMT

Theorem 7: *Suppose there exists u wires in the bottom band and $n = \max(3t-u+1, 2t+1)$ wires in the top band. Then any two phase PSMT protocol which securely sends a message $m \in \mathbb{F}^\ell$ containing ℓ field elements must communicate*

(a) $\Omega\left(\frac{N\ell}{N-3t}\right)$ field elements where $0 \leq u \leq t$, $n \geq 3t-u+1$ and $N = n+u \geq 3t+1$.

(b) $\Omega\left(\frac{n\ell}{n-2t}\right)$ field elements where $u > t$ and $n \geq 2t+1$.

Proof : We first prove part (a) of this theorem. This proof is heavily based on the necessity proof of Theorem 6. Following the same line of argument, we can show that when $n = 3t-u+1$ and $0 < u \leq t$, then for every possible pair of Π^{2Phase} and $\mathcal{A}_t^{2Phase}$ there exist a pair Π^{1Phase} and $\mathcal{A}_t^{1Phase}$ (with non-zero probability) such that the view of $\mathbf{S}$ and $\mathbf{R}$ are same in both the scenarios. It is easy to see that the communication cost are also same in Π^{1Phase} and Π^{2Phase}. It implies that for every two phase PSMT protocol sending m with $n \geq 3t-u+1$ and $0 < u \leq t$ wires in *top* and *bottom* band respectively, there exist a single phase PSMT sending m with $N = n+u$ wires (from $\mathbf{S}$ to $\mathbf{R}$) with same communication cost. Now any single phase PSMT sending m over $N \geq 3t+1$ wires must communicate $\Omega\left(\frac{N\ell}{N-3t}\right)$ field elements [7, 22]. Hence any two phase PSMT with $u < t$ and $n \geq 3t-u+1$ must communicate $\Omega\left(\frac{N\ell}{N-3t}\right)$ field elements for sending m.

We now proceed to prove part (b) of the theorem. Any PSMT protocol has to deliver the message correctly. Thus any PSMT protocol is also a PRMT protocol. Now neglecting the communication from $\mathbf{R}$ to $\mathbf{S}$, any two phase PRMT can be reduced to single phase PRMT by following the conversion shown in [23] (see proof of Theorem 2). Now from [23], any single phase PRMT protocol over $n = 2t+1$ wires has to communicate $\Omega(\frac{n\ell}{n-2t})$ field elements. So any two phase PSMT protocol with $u > t$ and $n \geq 2t+1$ has to communicate $\Omega(\frac{n\ell}{n-2t})$ field elements as well. □

APPENDIX D: Properties of Protocols O2PSMT

Theorem 13 *In protocol* **O2PSMT**, $\mathbf{R}$ *will correctly recover m at the end of* **Phase II**.

PROOF: From the description of the protocol, it is easy to see that **S** and **R** will agree on $N-t$ values (components) among N values in C. In other words, C and Y will differ at most at t locations. From Theorem 1, by substituting $d=0$, we find that the maximum number of errors c that can be corrected in Y is t. Hence by applying RS decoding on Y, **R** can recover C. Thus at the end of **Phase II**, both **S** and **R** will share the common pad Z (which is computed from C). Now since the blinded message Γ is broadcast over $n \geq 2t+1$ wires, it reaches to **R** correctly. Hence **R** will recover m correctly. □

Theorem 14 *In protocol* **O2PSMT**, $\mathcal{A}_t$ *will get no information about* m.

PROOF: In the protocol, m will be secure iff the pad Z is secure. Z is computed from C which is a RS codeword encoded using a polynomial of degree δ. Thus though C is of length N, any $\delta+1$ values on C are independent and uniquely defines C (the rest of the values of C are dependent on the selected set of $\delta+1$ values). So, consider the first $\delta+1$ values on C, denoted by $C_{(\delta+1)}$. Since those $\delta+1$ values were transmitted over $f_1,\ldots,f_{\delta+1}$, $\mathcal{A}_t$ may know t of them by corrupting t wires among $f_1,\ldots,f_{\delta+1}$. But the remaining $\delta+1-t$ values will not be known to $\mathcal{A}_t$. Hence $EXTRAND$ can extract an information theoretically secure pad Z of length $\delta+1-t$ from $C_{(\delta+1)}$. □

Theorem 15 *Protocol* **O2PSMT** *sends a message* m *containing* $\ell=(\delta+1)-t$ *field elements by communicating* $(n+u)+n(\delta+1-t)$ *field elements.*

PROOF: During first phase, **R** sends u field elements to **S** through the bottom band. During second phase, **S** sends n field elements for sending n components of C to **R**. In addition, **S** broadcasts Γ over the top band, incurring a communication complexity of $n(\delta+1-t)$ field elements. □

Theorem 16 *Protocol* **O2PSMT** *is a communication optimal two phase PSMT protocol, satisfying the lower bound given in Theorem 7.*

PROOF: We consider the following two cases:

1. **Case I:** $u \leq t$: In this case, $\delta=t$ and hence $|m|=\ell=1$. So from Theorem 15, the communication complexity of protocol **O2PSMT** will be $n+u=\mathcal{O}(N)$. Moreover, $N=3t+1$. By substituting these values in part (a) of Theorem 7, we find that the communication complexity of protocol **O2PSMT** satisfies the lower bound given in Theorem 7(a).

2. **Case I:** $u > t$: In this case, $\delta=u$ and hence $|m|=\ell=(u+1-t)$. Moreover, $n=2t+1$. So $n+u=\mathcal{O}(n(u-t))$ will hold. Hence from Theorem 15, the communication complexity of protocol **O2PSMT** will be $\mathcal{O}(n(u-t))$. By substituting the values of n and ℓ in part (b) of Theorem 7, we find that the communication complexity of protocol **O2PSMT** satisfies the lower bound given in Theorem 7(b).

APPENDIX E: Proof of the Properties of O3PSMT

Theorem 17 *In Protocol* **O3PSMT**, **R** *will correctly recover* m.

PROOF: First note that since $n=3t-2u+1>2t+1$, any information broadcast by **S** over the *top band* will be received by **R** correctly. This implies that **R** correctly receives blinded message Γ and either one of the two (depending upon what **S** has sent during **Phase III**): all quadruples $(\mathcal{B}^j, p^j, \mathcal{I}^j, CORRUPTED^j)$ or the message **"Entire Bottom band is corrupted"**. Now to prove that **R** recovers the message m sent by **S**, we show that **S** and **R** shares the same pad Z. **S** and **R** will share Z if (i) Λ is same at both ends and (ii) **R** is able to recover polynomials $F_i(x)$ for $i \notin \Lambda$. Since **S** sends all valid triples to **R** over all wires in *top band*, Λ will be same at both ends. Now we show that irrespective of the behavior of $\mathcal{A}_t$, **R** will always recover all the polynomials.

If $\mathcal{A}_t$ spares (either does not control or behave passively) at least one wire, say b_j, in the *bottom band*, then **S** will correctly receive $(\mathcal{B}^j, p^j, \mathcal{I}^j)=(\mathcal{B}, p, \mathcal{I})$ and hence $CORRUPTED^j$ will contain all the wires which were corrupted during first phase. In this case, **R** will correctly receive $CORRUPTED^j$, from which it identifies all wires which were corrupted during first phase. **R** ignores

the values received over those wires during **Phase I** and with the remaining values all the polynomials can be recovered correctly. On the other hand, if $\mathcal{A}_t$ corrupts the entire bottom band such that either **S** detects that all the received triples are invalid or **R** detects that his original triple is not present in the list of triples received by **S** (at the end of **Phase II**), then **R** concludes that entire *bottom band* is corrupted. Hence **R** applies RS decoding on the received vector Y_i to correct $t-u$ errors (see Theorem 1) and reconstruct polynomial $F_i(x)$ for $i \notin \Lambda$. Hence the theorem. □

Theorem 18 *In Protocol* **O3PSMT**, *m is information theoretically secure.*

PROOF: The message m will be information theoretically secure from $\mathcal{A}_t$ if the pad Z is information theoretically secure. According to the protocol, Z contains $F_i(0)$ iff $i \notin \Lambda$. Notice that $\Lambda = \cup_j \{\mathcal{I}^j | (\mathcal{B}^j, p^j, \mathcal{I}^j)$ is a valid triple$\}$. Now a valid triple $(\mathcal{B}^j, p^j, \mathcal{I}^j)$ can be either the original triple $(\mathcal{B}, p, \mathcal{I})$ sent by **R** or it may be different from $(\mathcal{B}, p, \mathcal{I})$ and generated by $\mathcal{A}_t$ (who can guess with non-zero probability). In the former case $(\mathcal{B}^j, p^j, \mathcal{I}^j)$ may be eavesdropped by $\mathcal{A}_t$ during its transmission over the *bottom band*. In later case, $\mathcal{A}_t$ knows $(\mathcal{B}^j, p^j, \mathcal{I}^j)$ since he himself has generated them. Hence it is possible that all $F_i(0)$'s with $i \in \Lambda$ are already exposed to $\mathcal{A}_t$. But for remaining polynomials $\mathcal{A}_t$ knows at most t points on them (by listening during first phase) and hence constant term of each $F_i(x)$ with $i \notin \Lambda$ is information theoretically secure. □

Theorem 19 *Protocol* **O3PSMT** *sends a message m containing $\ell = n^2u$ field elements by communicating $\mathcal{O}(n^3u) = \mathcal{O}\left(\frac{n\ell}{n-(3t-2u)}\right) = \mathcal{O}(n\ell)$ field elements. Moreover, the protocol is communication optimal.*

PROOF: During **Phase I**, **S** communicates $P = n^2u + ut$ codewords to **R** which has communication complexity of $Pn = n^3u + nut = \mathcal{O}(n^3u)$ field elements. In **Phase II**, **R** sends triple $(\mathcal{B}, p, \mathcal{I})$ through the *bottom band*. This incurs a communication cost of $\mathcal{O}(nt.u + 1.u + t.u) = \mathcal{O}(n^2u)$. In the worst case, it may happen that over every wire in *bottom band*, **S** receives a distinct valid triple $(\mathcal{B}^j, p^j, \mathcal{I}^j)$. Then communication complexity of **Phase III** for sending the triples will be $\mathcal{O}(n^2u.n) = \mathcal{O}(n^3u)$. Since message is of size n^2u, sending blinded message Γ results in a communication cost of $\mathcal{O}(n^3u)$. Hence overall communication complexity of Protocol is $\mathcal{O}(n^3u)$. Thus from Theorem 9, Protocol **O3PSMT** is a communication optimal PSMT protocol. □

APPENDIX F: Protocol O6PSMT and The Proof of its Properties

Protocol **O6PSMT** is given in Table 1.

Theorem 20 *In Protocol* **O6PSMT**, **R** *correctly recovers m.*

PROOF: First note that for each codeword C_i, the corresponding N length vector Y_i, possessed by **R**, differs from C_i only at t locations. This is because $\mathcal{A}_t$ controls at most t wires from top band and bottom band. With this observation, the correctness proof of this theorem simply follows from the correctness proof of Protocol **O3PSMT** (see theorem 17), **OPRMT** and **EXTRAND**. □

Theorem 21 *In Protocol* **O6PSMT**, *m will be information theoretically secure.*

PROOF: The secrecy of the message follows using similar argument as in Theorem 18 and the properties of **EXTRAND** algorithm. □

Theorem 22 *Protocol* **O6PSMT** *sends a message m containing $\ell = n^2u$ field elements by communicating $O\left(\frac{n^3u}{2u-t}\right) = O\left(\frac{n\ell}{n-(3t-2u)}\right) = O\left(\frac{n\ell}{2u-t+1}\right)$ field elements and hence is communication optimal.*

PROOF: During **Phase I**, **R** sends $Q = \frac{n^2u}{2u-t+1} + ut$ vectors, each of size u, thus communicating $Qu = \mathcal{O}(\frac{n^2u^2}{2u-t+1} + u^2t)$ field elements. During **Phase II**, **S** communicates $Q = \frac{n^2u}{2u-t+1} + ut$ codewords to **R** which incurs a communication cost of $Qn = \frac{n^3u}{2u-t+1} + nut$ field elements. In **Phase III**, **R** sends triple $(\mathcal{B}, p, \mathcal{I})$ through the bottom band. This incurs a communication cost of $\mathcal{O}(nt.u + 1.u + t.u) =$

$\mathcal{O}(n^2u)$. In worst case it may happen that over every wire in *bottom band*, **S** receives a distinct valid triple $(\mathcal{B}^j, p^j, \mathcal{I}^j)$. Then communication complexity of **Phase IV** for sending the triples using Protocol **OPRMT** will be $\mathcal{O}(n^2u)$. Similarly sending the blinded message Γ of size n^2u using protocol **OPRMT** results in a communication cost of $\mathcal{O}(n^2u)$. Hence overall communication complexity of Protocol **O6PSMT** is $\mathcal{O}(\frac{n^3u}{2u-t+1})$. Since the total communication complexity of **O6PSMT** satisfies the lower bound given in Theorem 9, it is a communication optimal PSMT protocol. □

Protocol O6PSMT(m, ℓ, n, u, t)

Phase I: R to S **R** selects $Q = \frac{n^2u}{2u-t+1} + ut = \frac{\ell}{2u-t+1} + ut$ random u length vectors $R_1, \ldots, R_Q$ such that $R_i = (r_{i1}, \ldots, r_{iu})$. Now **R** sends j^{th} component of all the vectors along wire b_j in *bottom band*.

Phase II: S to R **S** receives $\bar{R}_1, \ldots, \bar{R}_Q$ and selects Q codewords $C_1, \ldots, C_Q$ from $\mathcal{C}$ such that last u components of C_i is same as $\bar{R}_i$. This is always possible because every codeword C_i corresponds to a $2u$ degree polynomial $F_i(x)$. Now **S** sends j^{th} component of all the codewords over wire f_j in the *top band*.

Phase III: R to S

1. After receiving information over *top band*, **R** possesses N length vector (by combining the values sent over bottom band and the values received over top band) $Y_i = C_i + E_i$ corresponding to codeword C_i such that Y_i is different from C_i at most at t locations. Let $\mathcal{Y} = \{Y_1, \ldots, Y_Q\}$.
2. Now **R** does same computation and communication as in **Phase II** of Protocol **O3PSMT**. The only difference is that here $\mathcal{Y}$ contains $N = 2t + 1 + u$ length vectors $\{Y_1, \ldots, Y_Q\}$ whereas in **O3PSMT** $\mathcal{Y}$ contains $n = 3t - 2u + 1$ length vectors $\{Y_1, \ldots, Y_P\}$. Notice that **FindPseudo-basis** will still be able to find out pseudo-basis. This is because the code $\mathcal{C}$ used here has a hamming distance of at least $t + 1$.

Phase IV: S to R

1. With respect to the triples received through the bottom band, **S** performs the same computation (not communication) as done in **Phase III** of Protocol **O3PSMT**. That means **S** identifies the valid triples and for each valid triple $(\mathcal{B}^j, p^j, \mathcal{I}^j)$ finds list of corrupted wires $CORRUPTED^j$. But here there are following differences: (i) the pad Z is generated in a different manner, (ii) the valid triples, their corresponding list of corrupted wires and the blinded message are sent in a different manner.
2. **Generation of pad Z:**
   (a) **S** computes $\Lambda = \cup_j \{\mathcal{I}^j | (\mathcal{B}^j, p^j, \mathcal{I}^j)$ is a valid triple$\}$.
   (b) **S** computes $Z^i = (z^i_1, \ldots, z^i_{2u-t+1}) = \mathbf{EXTRAND}_{N,2u-t+1}(C_i)$ for each $i \notin \Lambda$.
   (c) Since $|\Lambda| \leq ut$ and $Q = \frac{n^2u}{2u-t+1} + ut$, **S** has generated at least $\frac{n^2u}{2u-t+1}$ Z^is. Hence concatenating all Z^i, **S** obtains a pad Z of length at least n^2u.
3. **Communication done by S:**
   (a) **S** merges all the quadruples $(\mathcal{B}^j, p^j, \mathcal{I}^j, CORRUPTED^j)$ such that $(\mathcal{B}^j, p^j, \mathcal{I}^j)$ is a valid triple into a list called L and sends it to **R** reliably by executing Protocol **OPRMT**.
   (b) If there is no **valid** triple, then **S** simply sends the message **"Entire Bottom band is corrupted"** over all the wires in *top band*.
   (c) **S** sends the blinded message $\Gamma = Z_\ell \oplus m$ by executing another instance of Protocol **OPRMT** where Z_ℓ contains first ℓ elements from Z.
   (d) Since $n = 2t + 1$ and $n - 2t + 2u = \Omega(n)$, **OPRMT** sends message in three phases. **R** receives all information communicated by **S** during **Phase IV** at the end of **Phase VI**.

Local Computation by R At The End of Phase VI:

1. **R** correctly receives all the information that **S** had sent during **Phase IV** and computes Λ in the same manner as done by **S**.
2. If either **R** gets the message **"Entire Bottom band is corrupted"** or if **R** finds his original triple $(\mathcal{B}, p, \mathcal{I})$ is not present in the list of **valid** triples sent by **S**, then **R** does the following:
   (a) Conclude that entire *bottom band* is corrupted and hence in the *top band* there are at most $t - u$ faults.
   (b) Neglect last u components of all Y_i and then recover all C_i such that $i \notin \Lambda$ by applying RS decoding algorithm on truncated Y_i and correcting $t - u$ Byzantine faults.
   (c) Compute pad Z in the same way as done by **S** and recovers $m = \Gamma \oplus Z_\ell$.
3. If **R** finds that his original triple $(\mathcal{B}, p, \mathcal{I})$ is present in the list of **valid** triples sent by **S** and let $(\mathcal{B}^j, p^j, \mathcal{I}^j)$ be same as $(\mathcal{B}, p, \mathcal{I})$, then **R** does the following:
   (a) Identify all the wires in $CORRUPTED^j$ as the corrupted wires (including *top* and *bottom* band). Notice that in protocol **O3PSMT**, a valid $CORRUPTED^j$ contains only the corrupted wires in the *top band* while in **O6PSMT**, it contains all the corrupted wires including *top* as well as *bottom band*.
   (b) Ignore all information communicated over the wires in $CORRUPTED^j$. Reconstruct all C_i such that $i \notin \Lambda$. This is possible because $|CORRUPTED^j| \leq t$. Hence $N - |CORRUPTED^j| \geq (t+1+u) \geq 2u+1$ and each codeword C_i is encoded using a polynomial of degree $2u$.
   (c) Recover the message m in the same way as described in step 2.

Table 1: **Protocol O6PSMT**(m, ℓ, n, u, t): $n = 2t + 1$, $\frac{t}{2} \leq u \leq t$, $\ell = n^2u$