On Communication Complexity of Perfectly Reliable and Secure Communication in Directed Networks

Arpita Patra[1] ⋆, Ashish Choudhary[1] ⋆⋆, Kannan Srinathan[2], and C. Pandu Rangan[1] ⋆⋆⋆

[1] Department of Computer Science and Engineering
IIT Madras, Chennai India 600036
Email:{ arpita,ashishc }@cse.iitm.ernet.in, rangan@iitm.ernet.in
[2] Center for Security, Theory and Algorithmic Research
IIIT Hyderabad
Gachibowli, Hyderabad India
srinathan@iiit.ac.in

Abstract. In this paper, we re-visit the problem of *perfectly reliable message transmission* (PRMT) and *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 [4] have given the necessary and sufficient condition for the existence of PSMT protocols in directed networks. In this paper, we first show that the necessary and sufficient condition (characterization) given by Desmedt et.al [4] does not hold for two phase[3] PSMT protocols. Hence we provide a different necessary and sufficient condition for two phase PSMT in directed networks. We also derive the lower bound on communication complexity of two phase PSMT and show that our lower bound is *asymptotically tight* by designing a two phase PSMT protocol whose communication complexity satisfies the lower bound. Though the characterization for three or more phase PSMT is resolved by the result of Desmedt et. al. [4], the lower bound on communication complexity for the same has not been investigated yet. Here we derive the lower bound on the communication complexity of three or more phase PSMT in directed networks and show that our lower bound is *asymptotically tight* by designing *communication optimal* PSMT protocols. Finally, we characterize the class of directed networks over which communication optimal PRMT or PRMT with constant factor overhead is possible. By communication optimal PRMT or PRMT with constant factor overhead, we mean that the PRMT protocol is able to send ℓ field elements by communicating $O(\ell)$ field elements from a finite field $\mathbb{F}$. To design our protocols, we use several techniques, which are of independent interest.

⋆ Financial Support from Microsoft Research India Acknowledged.

⋆⋆ Financial Support from Infosys Technology India Acknowledged.

⋆⋆⋆ Work Supported by Project No. CSE/05-06/076/DITX/CPAN on Protocols for Secure Communication and Computation Sponsored by Department of Information Technology, Govt. of India.

[3] A phase is a send from sender to receiver or vice-versa.

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 a part of directed synchronous network and are connected by uni-directional vertex disjoint paths/channels (also called as *wires*), which are directed either from **S** to **R** or vice-versa. 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 forge the communication through these wires in an 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, as per the protocol, **R** should output m correctly with probability one irrespective of the behavior of $\mathcal{A}_t$. This problem is called *perfectly reliable message transmission* (PRMT)[5, 4]. The problem of *Perfectly secure message transmission* (PSMT)[5, 4] has an additional restriction that at the end of the protocol, the adversary should have *no* information about m what so ever, in *information theoretic* sense.

If **S** and **R** are directly connected by a private channel, as assumed in generic secure multiparty computation protocols [1, 19, 2, 13], then reliable and secure communication between them is trivially guaranteed. However this assumption implies that the underlying network is a complete graph, which is impractical! In incomplete networks, where **S** and **R** are NOT directly connected, PRMT/PSMT protocols help to simulate a reliable/secure link. There is another motivation to study PSMT protocols. Currently, the security of all existing public key cryptosystems, digital signature schemes, etc are based on *unproven* hardness assumptions of certain number theoretic problems. However with increase in computing speed and advent of new computing paradigm (like Quantum computing) may render these assumptions to be baseless. In such a scenario, PSMT protocols will help to achieve information theoretic security against an all powerful adversary.

Existing Literature: In [5] Dolev et.al have shown that PRMT/PSMT between **S** and **R** tolerating $\mathcal{A}_t$ is possible in an undirected network iff there exists $2t+1$ bidirectional wires between **S** and **R**. The problem of PRMT and PSMT in directed networks was first studied by Desmedt et.al [4]. Modeling 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 other way round communication may not be possible. Following the approach of Dolev et.al [5], the authors in [4] have abstracted the underlying directed network in the form of directed vertex disjoint paths/wires, which are directed either from **S** to **R** or vice-versa. Under such settings, Desmedt et.al [4] have shown that PRMT tolerating $\mathcal{A}_t$ is possible iff there are at least $2t+1$ wires from **S** to **R**. Desmedt et.al [4] have also proved that PSMT tolerating $\mathcal{A}_t$ is possible iff there are at least $n = \max(3t - 2u + 1, 2t + 1)$ wires from **S** to **R** where u is the number of wires (disjoint from the n wires) directed from **R** to **S**. Noticeably, in this paper we show that this result does not hold good for two phase PSMT. Desmedt et.al [4] have shown the sufficiency of their characterization for PSMT by designing a PSMT protocol with exponential phase and communication complexity. Recently, PSMT protocols with polynomial phase and communication complexity, satisfying the characterization of Desmedt et.al in directed networks have been proposed in [12, 18].

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. URMT and USMT in the presence of $\mathcal{A}_t$ was first introduced and solved by Franklin et.al [7] in undirected synchronous networks, where they showed that URMT/USMT between **S** and **R** is possible iff there exists $2t + 1$ bi-directional wires between **S** and **R**. Over directed networks, Desmedt et.al [4] have shown that URMT/USMT tolerating $\mathcal{A}_t$ is possible iff there are total $2t+1$ wires between **S** and **R**, of which at least $t + 1$ should be directed from **S** to **R**. Recently, Patra et. al [11] have derived the lower bounds on communication complexity of URMT and USMT problems and have designed communication optimal URMT and USMT protocols over directed networks. Shankar et.al [15] have studied URMT in *arbitrary directed networks*, where they have given the complete characterization of URMT tolerating $\mathcal{A}_t$ by considering the underling directed network *as a whole*. Their characterization shows that it is inappropriate to model an underlying directed network in the form of directed wires between **S** and **R**. However, it is likely to take exponential time to verify whether a given directed network and $\mathcal{A}_t$ satisfies the conditions given in [15] for the possibility of URMT. Moreover, as a part of their sufficiency condition, the authors in [15] have given an exponential time URMT protocol. These two shortcomings "justifies" the use of *wire based* characterization of URMT and USMT given by Desmedt et.al, where we can afford to design efficient protocols [11]. Similarly, it can be shown that it is inappropriate to model a digraph in the form of directed wires between **S** and **R**, in the context of PSMT. But as far our knowledge is concerned, we are not aware of any work, which have considered the underlying directed network as a "whole" to study and characterize PSMT. Moreover, we strictly believe that any characterization of PSMT in *arbitrary* directed networks, derived by considering the entire network as a "whole", will have the same shortcomings as in the case of URMT/USMT. Nevertheless, finding the "exact" characterization of PSMT tolerating $\mathcal{A}_t$ in *arbitrary directed networks* is a theoretically challenging open problem.

Network Model and Definitions: Even though it might be inappropriate to model a directed graph in the form of directed wires, the characterization of PRMT and PSMT given by Desmedt et.al is advantageous if the network is densely connected and there are sufficient number of wires between **S** and **R**. For such networks, we can easily check whether PRMT/PSMT is possible tolerating $\mathcal{A}_t$ in polynomial time. So the moral is that for enough densely connected digraph, *wire based* abstraction of the network is preferable over the *graph based* one, where the digraph is considered as a whole. Hence, in this paper, we follow the model of Desmedt et.al [4] and abstract the underlying network in the form of a directed graph $G = (V, E)$, where **S** and **R** are two special honest nodes in V. We assume that there are n directed wires $f_1, f_2, \ldots, f_n$ from **S** to **R**, called as *top band* and u directed wires $b_1, b_2, \ldots, b_u$ from **R** to **S**, called as *bottom band*. Moreover, the wires in the *top band* are disjoint from the wires in the *bottom band*. A centralized adversary $\mathcal{A}_t$ with unbounded computing power actively controls at most t wires between **S** and **R**, including the *top* and *bottom band* in a colluded fashion. The adversary is *adaptive*; i.e., it can corrupt wires *dynamically* during the protocol execution and its choice of corrupting a wire depends upon the data seen so far from the already 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 compromised, the communication over the wire is fully eavesdropped and dictated by $\mathcal{A}_t$. We say that a wire is corrupted, if the value(s) sent over the wire is changed arbitrarily 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 **S** to **R** or vice-versa.

Our protocols work on a finite field $\mathbb{F}$ where $|\mathbb{F}| \geq (n + u)$. We use m to denote the message that **S** intends to send to **R**, where m is a sequence of $\ell \geq 1$ field elements from $\mathbb{F}$.

Our Contributions: Desmedt et.al [4] have shown that PSMT tolerating $\mathcal{A}_t$ is possible iff there are at least $n = \max(3t - 2u + 1, 2t + 1)$ wires from **S** to **R** where u is the number of wires directed from **R** to **S**. In this paper, we first show that the necessary and sufficient condition (characterization) given by Desmedt et.al [4] does not hold for two phase PSMT protocols. Specifically, we show that two phase PSMT tolerating $\mathcal{A}_t$ is possible iff there are at least $n = \max(3t - u + 1, 2t + 1)$ wires from **S** to **R** where u is the number of wires directed from **R** to **S**.

A key parameter of any PSMT protocol is its communication complexity, which is the number of field elements communicated by **S** and **R** in the protocol. Though the PSMT protocols of [18, 12] are efficient, they are not communication optimal. In this paper, we prove the lower bound on the communication complexity of both two phase and three or more phase PSMT protocols[4], which securely sends a message containing ℓ field elements. Moreover, we show that our bounds are *asymptotically tight* by giving efficient, polynomial time communication optimal PSMT protocols which are first of their kind. Specifically, for securely sending a message containing ℓ field elements, we show that (a) If $0 < u \leq t$, then any two phase PSMT requires $n \geq 3t - u + 1$ wires and commu-

[4] Any single phase PSMT protocol in directed network is no different from a single phase PSMT protocol in undirected networks. Hence, from [5], any single phase PSMT in directed networks requires $n \geq 3t + 1$ wires in the *top* band. Also, from [6], any single phase PSMT over $n \geq 3t + 1$ wires communicates $\Omega(\frac{n\ell}{n-3t})$ field elements to securely send ℓ field elements.

nicates $\Omega(\frac{N\ell}{N-3t})$ field elements where $N = n + u$. However, if $u > t$, then any two phase PSMT requires $n \geq 2t+1$ and communicates $\Omega(\frac{n\ell}{n-2t})$ field elements. (b) If $0 < u \leq t$, then $n \geq \max(3t - 2u + 1, 2t + 1)$ and any three or more phase PSMT must communicate $\Omega(\frac{n\ell}{n-(3t-2u)})$ field elements. However, if $u > t$, then $n \geq 2t + 1$ and any three or more phase PSMT must communicate $\Omega(\ell)$ field elements.

Finally, we characterize the class of directed networks over which communication optimal PRMT or PRMT with constant factor overhead is possible. By communication optimal PRMT or PRMT with constant factor overhead, we mean that the PRMT protocol is able to send ℓ field elements by communicating $O(\ell)$ field elements. Any such PRMT protocol is communication optimal because any PRMT protocol has a trivial lower bound of $\Omega(\ell)$ on communication complexity. Specifically, we show that any communication optimal PRMT protocol that transmits a message containing ℓ field elements by sending $O(\ell)$ field elements, tolerating $\mathcal{A}_t$ is possible over a digraph iff the digraph has $n \geq 2t + 1$ wires in the *top band* and u wires in the *bottom band* where $(n-2t)+2u = \Omega(t)$. To design our protocols, we use several techniques, which are of independent interest.

For ease of exposition, we assume that if **S** (**R**) is expecting some value(s) in some specific format from **R** (**S**) along a wire and if nothing (or some syntactically incorrect value(s)) comes, then **S** (**R**) substitutes predefined value(s) from $\mathbb{F}$ in the same specific format and continue the protocol. Thus, we separately do not consider the case when nothing or something syntactically incorrect comes along a wire. Any information which is sent over all the wires (either top or bottom band) is said to be broadcasted. If some information is broadcasted over at least $2t + 1$ wires, then it will always be received correctly at the receiving end by taking majority vote.

2 Preliminaries

All the protocols that we present in this paper are heavily based on the concept of pseudo-basis, a novel idea introduced by Kurosawa et.al [8] and on the properties of Reed-Solomon encoding and decoding from coding theory [9]. Kurosawa et.al [8] have first introduced the concept of pseudo-basis for designing a two phase communication optimal PSMT protocol over undirected graph where **S** and **R** are connected by at least $2t+1$ bidirectional vertex disjoint paths. In the sequel, we first briefly recall the ideas related to pseudo-basis and Reed-Solomon encoding and decoding.

2.1 Reed-Solomon (RS) Encoding and Decoding

We first define Reed-Solomon (RS) codes.

Definition 1 ([9]). *For 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 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.*

So 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 **A** and **B** are two specific nodes and there exists L wires from A to B. Let **A** sends an RS codeword $C = RS - ENC(M, k, L)$ of size L to **B** over the L wires. Specifically, **A** sends the i^{th} component of C over the i^{th} wire. Now assume that among the L wires, at most t can be under the influence of $\mathcal{A}_t$ who can arbitrarily change information flowing over the wires. Also let **B** receives C' where C and C' differs in at most t locations. Under this scenario, the error correction and detection capability of **R** in C' is given by the error correction and detection capability of RS decoding which is stated as follows:

Theorem 1 ([9, 4]). *Let C denotes the RS codeword for a message block of size k, where* $|C| = L$. *Let receiver receives* C' *where* C' *differs from C in at most t locations. Then RS decoding can correct upto c Byzantine errors in* C' *and simultaneously detect additional d Byzantine errors* $(c + d \leq t)$ *in* C' *iff* $L - k \geq 2c + d$.

2.2 Pseudo-basis and Pseudo-dimension

The current description of pseudo-basis and pseudo-dimension is taken from [8]. For full details, see [8]. Let $\mathcal{C}$ be the set of all possible codewords $C = (c_1\ c_2\ \ldots\ c_L)$. This implies that $\mathcal{C}$ is the set of all possible $(P_M(\alpha_1)\ \ldots\ P_M(\alpha_L))$, where $P_M(x)$ is a polynomial over $\mathbb{F}$ with degree of $P_M(x)$ being $k-1$. Also we assume that the hamming distance [9, 8] of code $\mathcal{C}$ is $t+1$. This implies that $L-(k-1) \geq t+1$ [8]. We may call the individual codewords in $\mathcal{C}$ as L-dimensional vectors. We would like to stress that any L length codeword is an L length vector but the reverse is not true.

Now let us return back to the same settings where **A** and **B** are connected by L wires, among which t are controlled by $\mathcal{A}_t$. Now if **A** sends γ codewords $C_1, \ldots, C_\gamma \in \mathcal{C}$ over these wires, 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. This important and brilliant observation is the incentive for Kurosawa et. al. [8] to introduce the concept of pseudo-basis which we briefly recall in the sequel. Let **B** receives 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 the adversary $\mathcal{A}_t$. Let

$$support(E_i) = \{j \mid e_{ij} \neq 0\}. \qquad (1)$$

Then there exist some t-subset $\{j_1, \ldots, j_t\}$ of L wires such that each error vector E_i satisfies $support(E_i) \subseteq \{j_1, \ldots, j_t\}$ where $\{j_1, \ldots, j_t\}$ is the set of wires that $\mathcal{A}_t$ has corrupted. 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 extensively.

Let $\mathcal{V}$ denotes 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 $Y_i - E_i = C_i \in \mathcal{C}$. Let us now recall the definition of pseudo-span on $\mathcal{Y} = \{Y_1 \ldots, Y_\gamma\}$ and definition of 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 $\mathcal{E} = \{E_1, \ldots, E_\gamma\}$ 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 whose 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 $\mathcal{B} = \{Y_{a_1}, \ldots, Y_{a_p}\}$ is a pseudo-basis of $\mathcal{Y}$. Then let $FORGED = \cup_{i=1}^{p} support(E_{a_i})$. Therefore $FORGED$ is the set of wires that the adversary $\mathcal{A}_t$ has corrupted. So,

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

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 $\mathcal{B} = \{Y_{a_1} \ldots, Y_{a_p}\}$ of $\mathcal{Y} = \{Y_1, \ldots, Y_\gamma\}$. For convenience, we use the following notation: $(p, \mathcal{B}, \mathcal{I}) =$ **FindPseudo-basis**$(\mathcal{Y})$. The interpretation is that the algorithm **FindPseudo-basis** takes set of received (by **R**) 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 codewords selected in $\mathcal{B}$, in polynomial time.

2.3 Extracting Randomness

For designing our PSMT protocols, we need another technique called **Extracting Randomness** which is described as follows. Suppose by some means, **S** and **R** agree on a sequence of 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 **S** and **R** do not know which values are known to $\mathcal{A}_t$. The goal of **S** and **R** is to agree on a sequence of f elements $[y_1 \ y_2 \ \ldots \ y_f] \in \mathbb{F}^f$, such that $\mathcal{A}_t$ has no information about $[y_1 \ y_2 \ \ldots \ y_f]$. This is done as follows [17]:

Algorithm EXTRAND$_{L,f}(x)$ [17]: Let V be an $L \times f$ Vandermonde matrix with members in $\mathbb{F}$ and which is known publicly. Then **S** and **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

Any PRMT protocol which reliably sends ℓ field elements by communicating $O(\ell)$ field elements, is called a *communication optimal* PRMT protocol. Essentially, a *communication optimal* PRMT protocol achieves reliability with *constant factor* overhead. In this section, we first 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 characterization of the digraphs over which a communication optimal PRMT is possible and how to design such communication optimal protocol over a sufficiently connected digraph? In other words what is the necessary and sufficient condition for the possibility of communication optimal PRMT protocol over a digraph?

The following theorem completely resolves the above question.

Theorem 5. *Any communication optimal PRMT protocol that transmits a message m containing ℓ field elements by communicating $O(\ell)$ field elements, tolerating $\mathcal{A}_t$ is possible over a digraph iff the digraph has $n \geq 2t+1$ wires in the top band and u wires in the bottom band where $(n-2t)+2u = \Omega(t)$.*

Proof: Necessity: First irrespective of the value of u, by the results of [5], any PRMT (may or may not be communication optimal) 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 *communication optimal* PRMT. Next we show that the u wires in the *bottom* band must satisfy $(n-2t)+2u = \Omega(t)$ for the existence of *communication optimal* PRMT protocol. We have to prove this when $u < t$ because if $u \geq t$ then $(n-2t)+2u = \Omega(t)$ is satisfied.

Suppose both **S** and **R** in advance knows 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 [17], any single phase protocol, where **S** is connected to **R** by $n \geq 2t+1$ wires, of which at most t are corrupted must communicate $\Omega(\frac{n\ell}{n-2t})$ fields elements for reliably sending ℓ field elements. This implies that any single phase protocol, where **S** is connected to **R** by $n \geq 2t+1$ wires, of which at most $t-u$ are corrupted must communicate $\Omega(\frac{n\ell}{n-2(t-u)})$ fields elements for reliably sending ℓ field elements. This in tern implies that 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 knows 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. Now the lower bound implies that any *communication optimal* PRMT protocol must communicate $\Omega(\frac{n\ell}{n-2(t-u)})$ field elements for sending ℓ field elements. By definition any *communication optimal* PRMT protocol transmits $O(\ell)$ 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 $O(\ell)$ iff $(n-2t)+2u = \Omega(t)$.

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

Before describing protocol **OPRMT**, we present a special type of single phase PRMT protocol called **SP-REL** where **S** is connected to **R** by $n \geq 2t+1$ wires (i.e. top band contains $n \geq 2t+1$ wires). **SP-REL** either sends the message m to **R** or it may fail to send the message due to some behavior of $\mathcal{A}_t$. In the later case, $\mathcal{A}_t$ must have done corruptions exceeding some limit which **R** will be able to detect. Protocol **SP-REL** is heavily 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. **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 $\mathbf{B_i}, 1 \leq i \leq z$ of m, **S** computes $(c_{i1}c_{i2}\ldots c_{in}) = RS{-}ENC(B_i, k, n)$ and sends $c_{ij}, 1 \leq i \leq z$ along the wire $f_j, 1 \leq j \leq n$.
3. **R** parallely receives c'_{ij}'s (possibly corrupted) over n wires. **R** then applies RS decoding algorithm to the received n length vectors and tries to correct $t-b$ errors and simultaneously detect additional b errors in each of the z received vectors.
4. If after correcting $t-b$ errors, the RS decoding algorithm does not detect additional errors in any of the z received vectors, then **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 **R** generates "ERROR" signal.

Lemma 1. *In* **SP-REL***, if at most $t-b$ wires are corrupted by the adversary, then* **R** *recovers m. Otherwise,* **R** *detects that more than $t-b$ wires have been corrupted in the top band.*

Proof: In the protocol, **R** receives $n \geq 2t+1$ 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 codeword. If at most $t-b$ errors occur in the *top band*, then decoding algorithm will correct them and will not detect any additional errors. So **R** will be able to recover m correctly. 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 codewords. After correcting $t - b$ errors in that codeword, the RS decoding algorithm will detect additional errors in the codeword. So **R** will come to know that more than $t - b$ wires are corrupted in the *top band* (though he does not know the identity of the corrupted wires). In this case, **R** fails to recover m. □

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

Proof: Follows from the working of the protocol. □

Thus protocol **SP-REL** creates a win-win situation with the adversary as follows: if $\mathcal{A}_t$ does at most $(t-b)$ errors then m is recovered; else **R** comes to know that more than $(t - b)$ wires are corrupted. We now design our *communication optimal* PRMT protocol **OPRMT** using **SP-REL** as a black-box. Though the protocol looks quite complex, we request the reader to read the protocol and go through the proof of Theorem 6, after which the protocol will be understood easily.

Theorem 6. **OPRMT** *reliably sends* m *in at most three phases.*

Proof: If more than $t-b$ errors take place during **Phase I**, then **R** detects it (see Lemma 1) and sends "ERROR" signal, along with the received n tuple for which it has detected more than $t - b$ errors, through the *bottom band*. In this case, in the *bottom band*, there can be at most $b - 1$ Byzantine faults. Now irrespective of whether $b = \frac{u}{2}$ or $\frac{t}{2}$, **R** will correctly receive the n tuple and "ERROR" signal over at least $\frac{u}{2}$ wires. **S** then locally find the number of mismatches between what **R** had received and what **S** had sent during **Phase I**. **S** then comes to know the identity of more than $t - b$ Byzantine faults and adds them to the list L_{fault}. **S** then sends L_{fault} to **R** through entire *top band*. So **R** also comes to know the identity of these faults. Finally, **S** resends the message by dividing it into blocks of size $k = X + |L_{fault}|$ and sending an $n - |L_{fault}|$ length RS codeword for each message block. Now from Theorem 1, by substituting $d = 0$, **R** will be able to recover the message after correcting $t - |L_{fault}|$ faults in each received vector.

On the other hand, if during **Phase I**, at most $t-b$ Byzantine faults occurred, then from Lemma 1, **R** will be able to recover the message correctly after **Phase I**. **R** then correctly broadcasts "SUCCESS" signal 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 7. *The protocol* **OPRMT** *is a communication optimal PRMT protocol which sends* $\Omega(nt)$ *field elements by communicating* $O(nt)$ *field elements.*

Proof: Since $n \geq 2t+1, \ell = \Omega(nt)$, $n-2t+2u = \Omega(t)$ and $b = \min(\frac{u}{2}, \frac{t}{2})$, from Lemma 2, the communication complexity of **Phase I** is $O(nt)$. During **Phase II**, **R** either sends an n tuple and "ERROR" signal or "SUCCESS" signal over all

Protocol OPRMT (m, ℓ, n, u, t)

Phase I: S to R: **S** executes **SP-REL**(m, ℓ, n, t, b) where $b = \min(\frac{u}{2}, \frac{t}{2})$, $n \geq 2t + 1$ and $|m| = \ell = (nt)$.

Phase II: R to S: If **R** recovers m after the execution of **SP-REL**, then he sends a "SUCCESS" message to **S** through the entire *bottom band.* Else **R** sends an "ERROR" message and the received n tuple (vector) for which **R** has detected more than $t - b$ faults.

Phase III: S to R: Let **S** receives "SUCCESS" signal along $u_s \geq 0$ wires and "ERROR" signal along with an n tuple through $u_e \geq 0$ wires. **S** now considers the following two cases:

– *Case 1.* $u_s \geq \frac{u}{2}$: In this case, **S** does nothing and terminates the protocol(see Theorem 6).
– *Case 2.* $u_e \geq \frac{u}{2}$: In this case, **S** checks whether it has received the same n tuple over at least $\frac{u}{2}$ wires out of the u_e wires through which it has received "ERROR" signal and n tuple. If not, then **S** does nothing and terminates the protocol (see Theorem 6). If **S** receives the same n tuple through at least $\frac{u}{2}$ wires out of u_e wires, then **S** does the following:

  S locally finds the number of mismatches between the n tuple received through at least $\frac{u}{2}$ wires and the corresponding original n tuple which it had sent during **Phase I**. If the number of mismatches is at most $t - b$, then **S** does nothing and terminates the protocol (see Theorem 6). If the number of mismatches is more than $t - b$, then **S** considers the corresponding wires (i.e., the wires, corresponding to which **S** has found a mismatch) as faulty and adds such wires to a list L_{fault}. Notice that $|L_{fault}| > t - b$. **S** eliminates all the wires in the list L_{fault} from the *top band.* For simplicity, let these be the last $|L_{fault}|$ wires in the *top* band. **S** then re-sends m by executing following steps:

  - First notice that now **S** considers only the first $n - |L_{fault}|$ wires. Also if indeed the received n tuple is correct then among the $n - |L_{fault}|$ wires there are at most $t - |L_{fault}|$ wires under the control of $\mathcal{A}_t$. Also note if the received n tuple is wrong then **R** already has got the message at the end of **SP-REL**.
  - **S** breaks up m into blocks $\mathbf{B_1}, \mathbf{B_2}, \ldots, \mathbf{B_z}$, each consisting of k field elements, where $k = X + |L_{fault}|$. If ℓ is not an exact multiple of k, a default padding is used to make ℓ mod $k = 0$.
  - For each block $\mathbf{B_i}, 1 \leq i \leq z$ of m, **S** compute an $(n - |L_{fault}|)$ length RS codeword $(c_{i1} \ldots c_{i(n-|L_{fault}|)})$ and sends $c_{ij}, 1 \leq i \leq z$ along the wire $f_j, 1 \leq j \leq (n - |L_{fault}|)$. In addition, **S** also sends L_{fault} to **R** over entire *top band.*

Message Recovery by R

If **R** had sent "ERROR" signal and an n tuple to **S** during **Phase II**, then **R** will correctly receive the list L_{fault}. After eliminating the wires in L_{fault} from the *top band*, **R** receives $(n - |L_{fault}|)$ length codeword for each block $\mathbf{B_i}$. **R** now correctly recovers each $\mathbf{B_i}$ by applying RS decoding algorithm and correcting $t - |L_{fault}|$ Byzantine errors in each codeword.

the u wires in bottom band. This involves communicating at most $nu = O(nt)$ field elements. During **Phase III**, **S** either sends nothing or resends the message. Communication complexity of resending the message is $O(\frac{(n-|L_{fault}|)|m|}{X+|L_{fault}|})$. 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 $O(nt)$. Thus the total communication complexity is $O(nt)$. □

4 Two Phase PSMT in Directed Networks

In this section, we prove the necessary and sufficient condition for the existence of any two phase PSMT protocol in directed networks tolerating $\mathcal{A}_t$. We then derive the lower bound on the communication complexity of any two phase PSMT protocol tolerating $\mathcal{A}_t$. Finally, we show that the bound is *asymptotically tight.*

4.1 Characterization of Two Phase PSMT in Directed Networks

The characterization for two phase PSMT in directed networks tolerating $\mathcal{A}_t$ is given by the following theorem:

Theorem 8. *Suppose there exists n wires from* **S** *to* **R** *in the top band and u wires from* **R** *to* **S** *in the bottom band, such that the wires in the top band are disjoint from the wires in the bottom band. Moreover, let $\mathcal{A}_t$ controls at most t of these $n + u$ wires. Then there exists a two phase PSMT tolerating $\mathcal{A}_t$ iff $n \geq max(3t - u + 1, 2t + 1)$.*

Proof: **Sufficiency**: The sufficiency proof is divided into two cases, namely when $0 < u \leq t$ and when $u > t$. If $0 < u \leq t$, then $n \geq 3t - u + 1$. So there will be total $n + u \geq 3t + 1$ wires between **S** and **R**. In this case, we design a two phase PSMT protocol called **O2PSMT-I**, given in Table 1. Protocol **O2PSMT-I** securely sends a secret message $m \in \mathbb{F}$ by communicating $O(n+u)$ field elements. So to send a message $m \in \mathbb{F}^\ell$ of size $\ell > 1$, we can parallely execute **O2PSMT-I** for each individual element of m, incurring a communication complexity of $O((n + u)\ell)$.

Protocol **O2PSMT-I** achieves it's goal by allowing **S** and **R** to share a common polynomial of degree t, such that $\mathcal{A}_t$ knows only t points on it. Once this is done, both **S** and **R** can generate an information theoretic pad of length one. **S** then can blind the message with the pad and sends it to **R**. Let $\mathcal{C}$ be the set of all RS codewords of length $N = n + u = 3t + 1$ encoded using polynomial of degree t. Hence the hamming distance between any two codeword in $\mathcal{C}$ is $N - t = 3t + 1 - t = 2t + 1$.

Theorem 9. *In protocol* **O2PSMT-I**, **R** *will correctly recover m at the end of* **Phase II**.

Proof: From the protocol, it is clear that **S** and **R** will agree on at least $2t + 1$ values (components) among $3t + 1$ 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 and corresponding polynomial $F(x)$ of degree t. Thus at the end of **Phase II**, both **S** and **R** will share the common pad $Z = F(0)$. Now since the blinded message Γ reaches to **R** correctly, **R** will recover message m correctly. □

Theorem 10. *In protocol* **O2PSMT-I**, *$\mathcal{A}_t$ will get no information about m.*

Proof: The proof follows from the fact that $\mathcal{A}_t$ will get at most t distinct points on $F(x)$. Thus $F(0)$ will be information theoretically secure. Since the pad is secure, so is the message m. □

Theorem 11. *Protocol* **O2PSMT-I** *sends a message $m \in \mathbb{F}^\ell$ of size ℓ by communicating $O((n + u)\ell)$ field elements.*

Proof: It is easy to check that protocol **O2PSMT-I** sends a single field element by communicating $O(n + u)$ field elements. So to send a message m containing

Protocol O2PSMT-I(m, n, u, t)

Phase I: R to S: **R** selects a random u length vector R such that $R = (r_1, \ldots, r_u)$. Now **R** sends j^{th} component of R along wire b_j in *bottom band*.

Phase II: S to R:

1. **S** receives $\bar{R}$ and selects a codeword C from $\mathcal{C}$ such that last u components of C is same as $\bar{R}$. This is always possible because every codeword $C \in \mathcal{C}$ corresponds to a t degree polynomial $F(x)$, where $t \geq u$. Now **S** sends j^{th} component of C over wire f_j in the *top band*.
2. **S** computes $\Gamma = m \oplus Z$ where $Z = F(0)$ and $F(x)$ is the t degree polynomial corresponding to codeword C. **S** sends 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 $N = 3t+1$ length vector $Y = C + E$ corresponding to codeword C such that Y is different from C at most at t locations. Hence by Theorem 1, **R** can recover C (and hence $F(x)$ and hence $Z = F(0)$) by applying RS decoding algorithm on Y and correcting t errors.
2. **R** also receives Γ correctly. Hence **R** recovers the message m by computing $m = \Gamma \oplus Z$

Table 1. Protocol **O2PSMT-I**: Two Phase PSMT with $n = 3t - u + 1$ and $0 < u \leq t$

$\ell > 1$ field elements, we can parallely execute **O2PSMT-I** for each individual field element of m, incurring a total communication complexity of $O((n + u)\ell)$ field elements. □

On the other hand, if $u > t$, then $n = 2t + 1$. So there will be total $N = n + u > 3t+1$ wires between **S** and **R**. In this case, we design a two phase PSMT protocol called **O2PSMT-II**, given in Table 2. Protocol **O2PSMT-II** securely sends a message m containing $(u-t)$ field elements from $\mathbb{F}$ by communicating $O(n(u-t))$ field elements. So to send a message $m \in \mathbb{F}^{\ell}$ of size $\ell > (u - t)$, we can divide m into several blocks of size $(u - t)$ and securely send each block by executing **O2PSMT-II**, incurring a communication complexity of $O(n\ell)$. Note that here at least $(u - t)$ wires in the *bottom* band are free from the influence of $\mathcal{A}_t$. Using this knowledge, **S** and **R** tries to establish an information theoretically secure one time pad of length $(u - t)$. Once this is done, the message can be send securely by blinding it with the pad. The idea of Protocol **O2PSMT-II** is very similar to Protocol **O2PSMT-I**. Let $\mathcal{C}$ be the set of all RS codewords of length $N = n + u > 3t + 1$ encoded using polynomial of degree u. Hence the hamming distance between any two codeword in $\mathcal{C}$ is $N - u = n = 2t + 1$.

Theorem 12. *In protocol* **O2PSMT-II**, **R** *will correctly recover m at the end of* **Phase II**.

Proof: The proof is similar to the proof of Theorem 9. Here again C and Y will differ at most at t locations. By Theorem 1, **R** can recover C by applying

RS decoding on Y and correcting t errors. The rest follows from the correctness of the **EXTRAND** and working of the protocol. □

Theorem 13. *In protocol* **O2PSMT-II**, $\mathcal{A}_t$ *will get no information about* m.

Proof: The secrecy of message m follows from the security of pad Z. Pad Z is secure from the security proof of the **EXTRAND**. □

Theorem 14. *Protocol* **O2PSMT-II** *can send a message* $m \in \mathbb{F}^{\ell}$ *of size* $\ell \geq (u-t)$ *by communicating* $O(n\ell)$ *field elements.*

Proof: From the protocol, it is clear that the protocol sends a message containing $(u-t)$ field elements by communicating $O(n(u-t))$ field elements. So to send a message m containing $\ell \geq (u-t)$ field elements, we can parallely execute **O2PSMT-II** for each sub-block of m of size $(u-t)$, incurring a total communication complexity of $O(n\ell)$ field elements. □

Protocol O2PSMT-II(m, ℓ, n, u, t)

Phase I: R to S: Same as in protocol **O2PSMT-I**.

Phase II: S to R:

1. **S** receives $\bar{R}$ and selects a codeword C from $\mathcal{C}$ such that last u components of C is same as $\bar{R}$. Now **S** sends j^{th} component of C over wire f_j in the *top band*.
2. **S** computes $\Gamma = m \oplus Z$ where $Z = [z_1, \ldots, z_{u-t}] = EXTRAND_{N,u-t}(C)$. **S** sends 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 $Y = C + E$ corresponding to codeword C such that Y is different from C at most at t locations. Hence by Theorem 1 **R** can recover C (and hence $F(x)$, the polynomial corresponding to C) by applying RS decoding algorithm on Y and correcting t errors. Once C is obtained, **R** gets Z in the same way as done by **S**.
2. **R** now recovers m in the same way as in protocol **O2PSMT-I**.

Table 2. Protocol **O2PSMT-II**: Two Phase PSMT with $n = 2t + 1$ and $u > t$.

Thus sufficiency of Theorem 8 is proved by protocols **O2PSMT-I** and **O2PSMT-II**. We now proceed to prove the necessity of Theorem 8.

Necessity: As in the case of sufficiency proof, the necessity proof is also divided into two cases, namely when $0 < u \leq t$ and when $u > t$. If $u > t$, then the necessary condition says that there should exist $n = 2t + 1$ wires from **S** to **R** in the *top band*. By [5, 4], $n = 2t + 1$ wires from **S** to **R** are necessary for any PRMT protocol tolerating $\mathcal{A}_t$. So it is obviously necessary for PSMT.

Next we show that if $0 < u \leq t$, then $n = 3t - u + 1$ wires from **S** to **R** in the *top band* is necessary for the existence of any two phase PSMT protocol tolerating $\mathcal{A}_t$. The proof is by contradiction. Let Π^{2Phase} be an instance of a two phase PSMT protocol sending message m with $0 < u \leq t$ wires in the *bottom band* and $n = 3t - u$ wires in the *top band*, tolerating $\mathcal{A}_t$. The random coin flips of **S**, **R** and $\mathcal{A}_t$ in Π^{2Phase} are $\mathcal{R}^{\mathbf{S}}_{\Pi^{2Phase}}$, $\mathcal{R}^{\mathbf{R}}_{\Pi^{2Phase}}$ and $\mathcal{R}^{\mathcal{A}}_{\Pi^{2Phase}}$ respectively. Then we show that there exists an instance of single phase PSMT protocol Π^{1Phase} (with non-zero probability), which sends m tolerating certain behavior of $\mathcal{A}_t$ with $N = n + u = 3t$ wires from **S** to **R**. But by results of [5], Π^{1Phase} can not deliver m tolerating that behavior of $\mathcal{A}_t$. This in turn implies that Π^{2Phase} also will fail to deliver m (with non-zero probability). But since Π^{2Phase} is an instance of PSMT, it must succeed in all cases. This shows contradiction. Let the random coin flips of **S**, **R** and $\mathcal{A}_t$ in Π^{1Phase} are $\mathcal{R}^{\mathbf{S}}_{\Pi^{1Phase}}$, $\mathcal{R}^{\mathbf{R}}_{\Pi^{1Phase}}$ and $\mathcal{R}^{\mathcal{A}}_{\Pi^{1Phase}}$ respectively.

Since Π^{2Phase} is a two phase PSMT, the first phase is from **R** to **S**, while the second phase is from **S** to **R**. Without loss of generality, the computation and communication during Π^{2Phase} are as follows:

1. **Phase I: R to S**: R uses $\mathcal{R}^{\mathbf{R}}_{\Pi^{2Phase}}$ to generate $\beta_1, \beta_2, \ldots, \beta_u$ and sends β_i to **S** through wire $b_i, 1 \leq i \leq u$.
2. **Phase II: S to R**: Let **S** receives β'_i through wire b_i. Based on the received information, m and $\mathcal{R}^{\mathbf{S}}_{\Pi^{2Phase}}$, **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** receives α'_i through wire f_i. Thus the combined view of **R** at the end of **Phase II** is $[\alpha'_1, \alpha'_2, \ldots, \alpha'_n, \beta_1, \beta_2, \ldots, \beta_u]$. On the other hand, the combined view of **S** at the end of **Phase II** is $[\alpha_1, \alpha_2, \ldots, \alpha_n, \beta'_1, \beta'_2, \ldots, \beta'_u]$. **R** performs local computation according to the protocol specification and correctly and securely recovers m.

Now we proceed to present an instance of a single phase PSMT Π^{1Phase} where there exists $N = n + u = (3t - u) + u = 3t$ wires $f_1, f_2, \ldots, f_N$. from **S** to **R**.

1. **Phase I: S to R**: **S** uses $\mathcal{R}^{\mathbf{S}}_{\Pi^{1Phase}}$ to generate $\beta'_1, \ldots, \beta'_u$ (which he can do with non-zero probability by simulating **R** in **Phase I** of Π^{2Phase}). **S** performs the same computation as in Π^{2Phase} and generates $\alpha_1, \ldots, \alpha_n$. Finally, **S** sends α_i to **R** through wire $f_i, 1 \leq i \leq n$ and β'_i through wire $f_i, n + 1 \leq i \leq 3t$.
2. **Computation by R at the end of Phase I**: Let **R** receives α'_i through wire $f_i, 1 \leq i \leq n$ and β''_i through wire $f_i, n + 1 \leq i \leq 3t$. Now **R** performs the same computation as in Π^{2Phase} to recover m.

Now we demonstrate two adversarial behavior; one in Π^{2Phase} and another in Π^{1Phase}, which allow the views of **S** and **R** in Π^{2Phase} to be identical to views of **S** and **R** in Π^{1Phase}, respectively. Consider the following adversarial behavior $\mathcal{A}^{2Phase}_t$ in Π^{2Phase}: $\mathcal{A}_t$ corrupts entire bottom band and first $t - u$ wires from top band. When **R** transmits β_i over b_i, $\mathcal{A}_t$ changes it to β'_i with $\beta'_i \neq \beta_i$ for $1 \leq i \leq u$. When **S** transmits α_i over f_i, $\mathcal{A}_t$ changes it to α'_i with $\alpha'_i \neq \alpha_i$ for $1 \leq i \leq t - u$. In this case views of **S** and **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 adversarial behavior $\mathcal{A}^{1Phase}_t$ in Π^{1Phase}: $\mathcal{A}_t$ corrupts last u wires and first

$t-u$ wires. When $\mathbf{S}$ transmits β_i' over f_i, $\mathcal{A}_t$ changes it to β_i for $n+1 \leq i \leq 3t$. When $\mathbf{S}$ transmits α_i over f_i, $\mathcal{A}_t$ changes it to α_i' for $1 \leq i \leq t-u$. Now notice that the views of both $\mathbf{S}$ and $\mathbf{R}$ in Π^{1Phase} against $\mathcal{A}_t^{1Phase}$ is same as in Π^{2Phase} against $\mathcal{A}_t^{2Phase}$. Hence if in Π^{2Phase}, $\mathbf{R}$ is able to get m, same should hold for Π^{1Phase}. But from the results of [5], it is easy to show that Π^{1Phase} can not recover m against $\mathcal{A}_t^{1Phase}$. Hence it implies that Π^{2Phase} also can not recover m against $\mathcal{A}_t^{2Phase}$. Since given Π^{2Phase}, the existence of $\mathcal{A}_t^{2Phase}$ is possible with non-zero probability, we conclude that Π^{2Phase} may fail to recover m against $\mathcal{A}_t^{2Phase}$ with non-zero probability. This is a contradiction, since Π^{2Phase} is an instance of two phase PSMT. Hence for $0 < u \leq t, n \geq 3t-u+1$ should hold. □

4.2 Lower Bound on Communication Complexity of Two Phase PSMT

We now prove the lower bound on the communication complexity of any two phase PSMT protocol in a directed network tolerating $\mathcal{A}_t$.

Theorem 15. *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* $n \geq 2t+1$.
Moreover, the bounds are asymptotically tight.

Proof : We first prove part (a) of this theorem. This proof is heavily based on the necessity proof of Theorem 8. 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 [6]. Hence any two phase PSMT must communicate $\Omega\left(\frac{N\ell}{N-3t}\right)$ field elements for sending m. The tightness of the bound follows from protocol **O2PSMT-I** and Theorem 11.

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. Such a conversion is possible [17]. Now from [17], 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 has to communicate $\Omega(\frac{n\ell}{n-2t})$ field elements. The tightness of the bound follows from protocol **O2PSMT-II** and Theorem 14. □

5 Lower Bounds on the Communication Complexity of Three or More Phase PSMT

Recall that from [4], any 3 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 and Maximum Distance Separable (MDS) Codes

Definition 4 (x-out-of-n Secret Sharing Scheme [14]). *: An x-out-of-n Secret Sharing scheme 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 $(s_1, \ldots, s_n)$ is called a code and its element a codeword. If the code is a Maximum Distance Separable (MDS) code [9, 4], then it can correct c errors and simultaneously detect d additional errors iff $n - x > 2c + d$ [9, 4]. An x-out-of-n Secret Sharing scheme is called MDS secret sharing scheme if it is constructed from a MDS code. MDS secret sharing schemes can be constructed from any MDS codes, for example Reed-Solomon codes [9, 10, 4]. So we have the following theorem on the error correction and detection capability of MDS x-out-of-n Secret Sharing scheme:

Theorem 16 ([9, 4]). *Any MDS x-out-of-n Secret Sharing scheme can correct c errors and detect d additional errors in a codeword iff $n - x > 2c + d$.*

5.2 The Lower Bound

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 ($(\alpha, \beta, \gamma, m, \ell)$-SecretSharingScheme:). *Given a secret m containing ℓ field elements from $\mathbb{F}$, an $(\alpha, \beta, \gamma, m, \ell)$-SecretSharingScheme 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 17. *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 $0 < u \leq t$ [5].

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

Proof: We first prove part (a) of the theorem. The outline of the proof 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 containing ℓ field elements from $\mathbb{F}$ is not less than the share complexity (sum of all the shares) of an $(n, (n-2(t-u)), t, m, \ell)$-SecretSharingScheme (see Lemma 3). We then show that the share complexity of any $(n, (n-2(t-u)), t, m, \ell)$-SecretSharingScheme is $\Omega(\frac{n\ell}{n-(3t-2u)})$ field elements (see Lemma 4). Part (a) of Theorem 17 now follows from Lemma 3 and Lemma 4. So we proceed to prove Lemma 3.

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

Proof: Let Π be a PSMT protocol which runs for p phases with $p \geq 3$. In the sequel we will give a possible behavior of $\mathcal{A}_t$ which proves the lemma statement. Now as in [4], without loss of generality, the view of $\mathbf{S}$ in protocol Π, denoted as $view_{\Pi}^{\mathbf{S}}$ 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 $\mathcal{A}_t$ (without loss of generality, we assume that the value of $\mathcal{R}^{\mathcal{A}}$ will determine the choice of faulty wires controlled by $\mathcal{A}_t$). Without loss of generality, we assume that the protocol proceeds in phases where $\mathbf{S}$ is silent in even phases and $\mathbf{R}$ is silent in odd phases [5, 4]. Now the strategy of the adversary $\mathcal{A}_t$ is as follows:

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 $f_{a_1}, f_{a_2}, \ldots, f_{a_{t-u}}$ 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)

[5] Note that when $u = 0$, then any multiphase PSMT turns out to be a single phase PSMT. From results of [5], any single phase PSMT requires at least $n = 3t + 1$ wires from $\mathbf{S}$ to $\mathbf{R}$. Fitzi et. al. [6] have proved 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 $u = 0$.

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 $r = 0$.

Since $\mathcal{A}_t$ has unbounded computing power, he can behave in the above manner. Now let $\alpha^{\mathbf{S}}_{i,j}$ be the values that $\mathbf{S}$ sends on wire f_i in phase j of protocol Π. Let $\alpha^{\mathbf{S}}_i = (\alpha^{\mathbf{S}}_{i,1}, \ldots, \alpha^{\mathbf{S}}_{i,p})$ i.e. $\alpha^{\mathbf{S}}_i$ is the concatenation of the values sent by $\mathbf{S}$ over wire f_i during the execution of Π. We can view $\alpha^{\mathbf{S}}_i$'s as the shares of message m. Similarly, let $\alpha^{\mathbf{R}}_{i,j}$ be the values that $\mathbf{R}$ sends on wire b_i in phase j. Let $\alpha^{\mathbf{R}}_i = (\alpha^{\mathbf{R}}_{i,1}, \ldots, \alpha^{\mathbf{R}}_{i,p})$. Now if we assume $r = 0$, 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 $\{\alpha^{\mathbf{S}}_1, \ldots, \alpha^{\mathbf{S}}_n\}$. Thus $(\alpha^{\mathbf{S}}_1, \ldots, \alpha^{\mathbf{S}}_n)$ is an x-out-of-n secret sharing scheme with $x \geq t$, since with $x > t$, we still maintain that t shares from the set $\{\alpha^{\mathbf{S}}_1, \ldots, \alpha^{\mathbf{S}}_n\}$ does not reveal any information on m. Now if we assume $r = 1$, 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 $(\alpha^{\mathbf{S}}_1, \ldots, \alpha^{\mathbf{S}}_n)$ and thus recover the message m. Thus in summary, $(\alpha^{\mathbf{S}}_1, \ldots, \alpha^{\mathbf{S}}_n)$ is an x-out-of-n (MDS) secret sharing scheme with the capability of correcting $t-u$ error where $x \geq t$. Now by Theorem 16, an x-out-of-n (MDS) secret sharing scheme can correct $(t-u)$ errors if

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

This shows that the communication done by $\mathbf{S}$ (alone) is equivalent to the share complexity (sum of all the shares) of an $(n, (n-2(t-u)), t, m, \ell)$-SecretSharingScheme. 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 $(n, (n-2(t-u)), t, m, \ell)$-Scheme. □

Next, we prove that the share complexity of any $(n, (n-2(t-u)), t, m, \ell)$-SecretSharingScheme is $\Omega(\frac{n\ell}{n-(3t-2u)})$ field elements. This along with Lemma 3 proves part (a) of Theorem 17. To prove Lemma 4, we use entropy based argument which is used in [16] to prove the lower bound on the communication complexity of PSMT protocols in undirected networks.

Lemma 4. *The share complexity of any $(n, (n-2(t-u)), t, m, \ell)$-SecretSharingScheme is $\Omega(\frac{n\ell}{n-(3t-2u)})$ field elements.*

Proof: Let X_i denotes the i^{th} share. For any subset $A \subseteq \{1, 2 \ldots n\}$, let X_A denotes the set of variables $\{X_i | i \in A\}$. Let m be a value drawn uniformly at random from $\mathbb{F}^\ell$. Then the secret m and the shares X_i are random variables. Let $H(X)$ for a random variable denote its entropy. Let $H(X|Y)$ denotes the entropy of X conditional on Y. The conditional entropy measures how much entropy a random variable X has remaining if we have already learned completely the value of a second random variable Y [3]. Since m is a value drawn uniformly at random from $\mathbb{F}^\ell$, we have $H(m) = \ell$. Since any set B consisting of $n - 2(t-u)$ correct shares has full information about m, we have $H(m|X_B) = 0$. Consider any subset $A \subset B$ such that $|A| = t$. Since any set of t shares has no information about m, we have $H(m|X_A) = H(m)$. From the chain rule of the entropy [3], for any two random variables X_1, X_2, we have $H(X_1, X_2) = H(X_2) + H(X_1|X_2)$. Substituting $X_1 = m|X_A$ and $X_2 = X_{B-A}$, we get

$$H(m|X_A, X_{B-A}) = H(X_{B-A}) + H(m|X_A|X_{B-A}) \tag{3}$$

From the properties of joint entropy [3], for any two variables X_1, X_2, we have $H(X_1, X_2) \geq H(X_1)$ and $H(X_1, X_2) \geq H(X_2)$. Thus, $H(m|X_A, X_{B-A}) \geq H(m|X_A)$. Substituting in the above equation, we get

$$\begin{aligned} H(m|X_A) &\leq H(m|X_A, X_{B-A}) + H(X_{B-A}) \\ &\leq 0 + H(X_{B-A}) \text{ because } m \text{ can be known completely from } X_A \text{ and } X_{B-A} \end{aligned}$$

Consequently, $H(m) \leq H(X_{B-A})$ because $H(m|X_A) = H(m)$. Since $|B| = n - 2(t-u)$ and $|A| = t$, we get $|B - A| = n - (3t - 2u)$. So for any set C of size $|B - A| = n - (3t - 2u)$,

$$H(X_C) \geq H(m) \Rightarrow \sum_{i \in C} H(X_i) \geq H(m)$$

Since there are $\binom{n}{n-(3t-2u)}$ possible subsets of cardinality $n-(3t-2u)$, summing the above equation over all possible subsets of cardinality $n - (3t - 2u)$ we get

$$\sum_{C} \sum_{i \in C} H(X_i) \geq \binom{n}{n - (3t - 2u)} H(m)$$

Now in all the possible $\binom{n}{n-(3t-2u)}$ subsets of size $n-(3t-2u)$, each of the term $H(X_i)$ appears $\binom{n-1}{n-(3t-2u)-1}$ times. So

$$\binom{n-1}{n - (3t - 2u) - 1} \sum_{i=1}^{n} H(X_i) \geq \binom{n}{n - (3t - 2u)} H(m)$$

$$\Rightarrow \quad \sum_{i=1}^{n} H(X_i) \geq \frac{n}{n - (3t - 2u)} H(m)$$

Since $H(m) = \ell$, we get $\sum_{i=1}^{n} H(X_i) \geq \frac{n}{n-(3t-2u)}\ell$. Thus the share-complexity of any $(n, (n - 2(t - u)), t, m, \ell)$-SecretSharingScheme is $\Omega\left(\frac{n\ell}{n-(3t-2u)}\right)$. □

Part (a) of Theorem 17 now follows from Lemma 3 and Lemma 4. We now proceed to prove part (b) of Theorem 17. We can prove part (b) by two different arguments. First argument goes as follows: since any PSMT protocol has to at least send the message, it must communicate $\Omega(\ell)$ field elements for sending ℓ field elements. The second argument is as follows. Notice that from the result of part (a), any PSMT must communicate $\Omega(\ell)$ field elements for sending ℓ field elements when $n \geq 2t+1$ and $u = t$. Hence increasing u beyond t can neither increase (because we may simply ignore any $u-t$ wires and consider the remaining t wires in the bottom band) nor decrease (because of first argument) the lower bound on the communication complexity. So if $u > t$, then $n \geq 2t+1$ and any three or more phase PSMT has to communicate $\Omega(\ell)$ field elements to securely send ℓ field elements. This proves part(b) of Theorem 17. □

In the next section, we show that our lower bounds on the communication complexity of any 3 or more phase PSMT are *asymptotically* tight.

6 Upper Bounds on the Communication Complexity of Three or More Phase PSMT

From Theorem 17, 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 $n \geq 2t+1$.

In this section, we show that the lower bounds in (i), (ii) and (iii) are *asymptotically tight*. Specifically, we provide a three phase PSMT protocol whose communication complexity satisfies the lower bound specified in (i) where $0 < u < \frac{t}{2}$ and $n \geq 3t-2u+1$. Then we provide a six phase PSMT protocol whose communication complexity satisfies the lower bound specified in (ii) where $\frac{t}{2} \leq u \leq t$ and $n \geq 2t+1$. Finally we show that a trivial modification of our second protocol leads to a six phase PSMT protocol which communicates $O(\ell)$ field elements for transmitting ℓ field elements when $u > t$ and $n \geq 2t+1$. All the protocols that we present here are heavily based on the concept of pseudo-basis, a novel idea introduced by Kurosawa et.al [8] and on the properties of Reed-Solomon encoding and decoding from coding theory (see Section 2). Designing a five or less phase PSMT protocol with $\frac{t}{2} \leq u \leq t$ ($u > t$) and $n \geq 2t+1$ wires in the bottom and top band respectively and with a communication complexity of $O(\frac{n\ell}{2u-t)})$ ($O(\ell)$) is left as an open problem.

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

In this section, we present a three phase communication optimal PSMT protocol called **O3PSMT** where there are $n = 3t-2u+1$ wires in the *top band* and u wires in the *bottom band* with $0 < u < \frac{t}{2}$. Protocol **O3PSMT** securely sends $\ell = n^2u$ field elements by communicating $O(n^3u) = O(n\ell)$ field elements. Informally the protocol works in the following way. **S** tries to securely and correctly establish an information theoretic secure one time pad of size n^2u with **R**. Let $\mathcal{C}$ denotes the set of all RS codewords of length $n = 3t-2u+1$ encoded using polynomials of degree t. 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. Notice that each random codeword from $\mathcal{C}$ corresponds to a polynomial of degree t. **R** receives (possibly) modified codewords (which are different from the original codewords at most at t locations) and finds the pseudo-basis of the received codewords using algorithm **FindPseudo-basis** (see section 2). **R** then sends the pseudo-basis, pseudo-dimension and index set over all the wires in *bottom band*. **S** first checks the validity of the pseudo-basis and index set received over a wire and then for each valid pseudo basis finds the set of corrupted wires. 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** sends all the valid triple of (pseudo basis, pseudo-dimension and index set) as received by him along with the corresponding list of corrupted wires through all the n 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. Now from Theorem 1, **R** can correct $t-u$ errors in each of the codeword and thus can recover all the original codewords. Hence in any case **S** and **R** will agree on all the codewords chosen by **S**. But during the transmission of pseudo-basis over u wires, $\mathcal{A}_t$ who may control all the u wires in the *bottom band* 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-basses, the remaining codewords can be used to construct an information theoretic secure pad of size n^2u. Once the pad is established between **S** and **R**, **S** can use the pad to blind the message and sends the blinded message reliably to **R**. The protocol **O3PSMT** is given in Table 3.

Theorem 18. *In Protocol* **O3PSMT**, **R** *will correctly recover m.*

Proof: First note that since $n = 3t - 2u + 1 > 2t + 1$, any information sent by **S** over all the wires in *top band* will be received by **R** reliably without any error. This implies **R** correctly receives blinded message Γ and either one of the two (depending upon what **S** has sent during **Phase III**): all quadruples $(\mathcal{B}^j, p^j, \mathcal{I}^j, FORGED^j)$ 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 $FORGED^j$ will contain all the wires which were corrupted during first phase. In this case, **R** will correctly receive $FORGED^j$, 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 19. *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 $\mathcal{A}_t$ by guessing (which is possible with non-zero probability). In the previous 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 $F_i(0)$ with $i \in \Lambda$ is 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 20. *Protocol* **O3PSMT** *sends a message m containing $\ell = n^2u$ field elements by communicating $O(n^3u) = O\left(\frac{n\ell}{n-(3t-2u)}\right) = O(n\ell)$ 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 $Pn = n^3u + nut = O(n^3u)$ field elements. In **Phase II**, **R** sends triple $(\mathcal{B}, p, \mathcal{I})$ through the *bottom band*. This incurs a communication cost of $O(nt.u + 1.u + t.u) = O(n^2u)$. 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 $O(n^2u).n = O(n^3u)$. Since message is of size n^2u, sending blinded message Γ results in a communication cost of $O(n^3u)$. Hence overall communication complexity of Protocol is $O(n^3u)$. Thus from Theorem 17, Protocol **O3PSMT** is a communication optimal PSMT protocol. □

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 there are $n = 2t+1$ wires in the *top band* and u wires in the *bottom band* with $\frac{t}{2} \leq u \leq t$. Protocol **O6PSMT** securely sends $\ell = n^2u$

Protocol O3PSMT(m, ℓ, n, u, t)

<u>Phase I: S to R</u> **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.*

<u>Phase II: R to S</u>

1. **R** receives $Y_i = C_i + E_i$ corresponding to codeword C_i such that Y_i is different from C_i at most at t locations. Let $\mathcal{Y} = \{Y_1, \ldots, Y_P\}$.
2. Now **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 $\mathcal{I} = \{a_1, \ldots, a_p\} \subset \{1, \ldots, P\}$.
3. **R** sends the triple $(\mathcal{B}, p, \mathcal{I})$ over all the wires in *bottom band.*

<u>Phase III: S to R</u>

1. **S** may receive different triples over different wires. Let **S** receives $(\mathcal{B}^j, p^j, \mathcal{I}^j)$ 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 atmost t locations.
3. Now for every **valid** triple $(\mathcal{B}^j, p^j, \mathcal{I}^j)$, **S** finds $E^j_{a^j_1} = Y^j_{a^j_1} - C_{a^j_1} \ldots, E^j_{a^j_{p^j}} = Y^j_{a^j_{p^j}} - C_{a^j_{p^j}}$ and computes $FORGED^j = \cup_{\alpha=1}^{p^j} support(E^j_{a^j_\alpha})$.
4. **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 $P = n^2u + ut$).
5. Now **S** communicates the following over all the wires in the *top band*: (i) every valid triple $(\mathcal{B}^j, p^j, \mathcal{I}^j)$ and corresponding list of corrupted wire $FORGED^j$ (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.

<u>Local Computation by R at the End of Phase III:</u>

1. **R** correctly receives all the information that are sent by **S** in **Phase III** 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** concludes that entire *bottom band* is corrupted. Hence in the top band there are at most $t - u$ Byzantine faults. **R** now recovers all the polynomials $F_i(x)$ such that $i \notin \Lambda$ by applying RS decoding algorithm on Y_i (received at the end of **Phase I**) and correcting $t - u$ Byzantine faults. Notice that according to Theorem 1, RS decoding can correct $t - u$ errors, since each codeword is RS encoded using a polynomial of degree t. Thus **R** recovers 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. Otherwise **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** identifies all the wires in $FORGED^j$ $(|FORGED^j| \leq t)$ as the corrupted wires in **Phase I**. Ignoring all information received over the wires in $FORGED^j$ during **Phase I**, **R** reconstruct all the polynomial $F_i(x)$ such that $i \notin \Lambda$ (actually he can reconstruct all polynomials sent by **S**). **R** can do this because now he has at least $t+1$ correct values for each $F_i(x)$. After this **R** recovers the message m in the same way as described in previous step.

Table 3. Protocol O3PSMT(m, ℓ, n, u, t): $\ell = n^2u, n = 3t - 2u + 1, 0 < u < \frac{t}{2}$

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 17. Interestingly, when $u = \frac{t}{2} + \Theta(t)$, then Protocol **O6PSMT** sends ℓ field elements securely with constant factor overhead. Protocol **O6PSMT** achieves it's goal by allowing **S** and **R** to share n^2u 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 $O(n^3u)$ and hence, it will no longer satisfy the lower bound of Theorem 17. 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 $(n - 2t) + 2u = \Omega(t)$, we can execute **OPRMT**. **R** can recover the message since he knows the pad. Let $\mathcal{C}$ denotes the set of all RS codewords of length $N = n + u = 2t + 1 + u$ encoded using polynomials of degree $2u \geq t$. Hence the hamming distance between any two codeword is $N - 2u = 2t - u + 1 \geq t + 1$. Protocol **O6PSMT** is given in Table 4.

Theorem 21. *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 18) and the correctness of **EXTRAND**. □

Theorem 22. *In Protocol* **O6PSMT**, *m will be information theoretically secure.*

Proof: The secrecy of the message follows using similar argument as in Theorem 19 and the correctness of **EXTRAND** algorithm. □

Theorem 23. *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 $Qu = O(\frac{n^2u^2}{2u-t+1} + u^2t)$ 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 $O(nt.u+1.u+t.u) = O(n^2u)$. 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 $O(n^2u)$. Similarly sending the blinded message Γ of size n^2u using protocol **OPRMT** results in a communication cost of $O(n^2u)$. Hence overall communication complexity of Protocol **O6PSMT** is $O(\frac{n^3u}{2u-t+1})$. Since the total communication complexity of **O6PSMT** satisfies the lower bound given in Theorem 17, 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 $Y_i = C_i + E_i$ 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 $FORGED^j$. 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**:** **S** computes $\Lambda = \cup_j \ \{\mathcal{I}^j | (\mathcal{B}^j, p^j, \mathcal{I}^j)$ is a valid triple$\}$. Then **S** executes $Z^i = (z^i_1, \ldots, z^i_{2u-t+1}) =$ **EXTRAND**$_{N,2u-t+1}(C_i)$ for each $i \notin \Lambda$. 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. **S** merges all the quadruples $(\mathcal{B}^j, p^j, \mathcal{I}^j, FORGED^j)$ 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**. If there is no **valid** triple, then **S** simply sends the message **"Entire Bottom band is corrupted"** over all the wires in *top band*. **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. Notice that if $n \geq 2t + 1$ and $n - 2t + 2u = \Omega(t)$, then **OPRMT** can send message reliably with constant factor overhead in three phases. Hence **R** receives all information communicated by **S** at the end of **Phase VI**.

Local Computation by R At The End of Phase VI:

1. **R** correctly receives all the information sent by **S** 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** concludes that entire *bottom band* is corrupted. Hence in the *top band* there are at most $t - u$ Byzantine faults. In this case, **R** neglects last u components of all Y_i and then recovers all the codewords C_i such that $i \notin \Lambda$ by applying RS decoding algorithm on truncated Y_i (of length n received at the end of **Phase II**) and correcting $t - u$ Byzantine faults. Notice that according to Theorem 1, RS decoding can correct $t - u$ errors in truncated Y_i, as each C_i is RS encoded using a polynomial of degree $2u$. Thus **R** computes pad Z in the same way as done by **S** and recovers $m = \Gamma \oplus Z_\ell$.
3. Else **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** identifies all the wires in $FORGED^j$ as the corrupted wires (including *top* and *bottom* band). Notice that in protocol **O3PSMT**, a valid $FORGED^j$ 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*. Now ignoring all information communicated over the wires in $FORGED^j$, **R** can easily reconstruct all the codewords C_i such that $i \notin \Lambda$. This is because $|FORGED^j| \leq t$. Hence $N - |FORGED^j| \geq (t + 1 + u) \geq 2u + 1$ and each codeword C_i is encoded using a polynomial of degree $2u$. After this **R** recovers the message m in the same way as described in previous step.

Table 4. Protocol O6PSMT(m, ℓ, n, u, t): $n = 2t + 1, \frac{t}{2} \leq u \leq t, \ell = n^2u$

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

In protocol **O6PSMT**, if $u = t$ and $n = 2t + 1 = \Theta(t)$, then from Theorem 23, the protocol securely sends $\ell = n^2 u = \Theta(n^3)$ field elements by communicating $O(n^3)$ field elements. Hence, if $u > t$ and $n \geq 2t + 1$, then **S** and **R** can execute protocol **O6PSMT** by considering only the first $2t + 1$ wires in the *top* band and first t wires in the *bottom* band, thus resulting in a six phase communication optimal PSMT protocol, which sends ℓ field elements with a communication complexity of $O(\ell)$. Thus, we have the following theorem:

Theorem 24. *Suppose there exists $n \geq 2t + 1$ wires in the top band and $u > t$ wires in the bottom band. Then there exists a six phase PSMT protocol tolerating $\mathcal{A}_t$, which securely sends ℓ ($\ell = n^3$) field elements by communicating $O(\ell)$ field elements.*

7 Conclusion and Open Problems

In this paper we have proved the lower bound on the communication complexity of PSMT protocols in directed networks, which is done for the first time. Moreover, we have shown that our bounds are *asymptotically tight* by designing communication optimal PSMT protocols, which are first of their kind. The summary of our results (marked with *) is given in the following Table. 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 PSMT protocols, which are communication optimal for message of any length.

# Phases	Characterization	Lower Bound
1	$n \geq 3t + 1$ [5, 4]	$\Omega(\frac{n\ell}{n-3t})$ [6]
2	If $0 < u \leq t$ then $n \geq 3t - u + 1$* If $u > t$ then $n \geq 2t + 1$*	$\Omega(\frac{N\ell}{N-3t})$; $N = n + u$* $\Omega(\frac{n\ell}{n-2t})$*
3	If $0 < u \leq t$ then $n \geq \max(3t - 2u + 1, 2t + 1)$ [4] If $u > t$ then $n \geq 2t + 1$ [4]	$\Omega(\frac{n\ell}{n-(3t-2u)})$* $\Omega(\ell)$*

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

3. T. H. Cover and J. A. Thomas. *Elements of Information Theory.* John Wiley & Sons, 2004.
4. 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.
5. D. Dolev, C. Dwork, O. Waarts, and M. Yung. Perfectly secure message transmission. *JACM*, 40(1):17–47, 1993.
6. 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.
7. M. Franklin and R. Wright. Secure communication in minimal connectivity models. *Journal of Cryptology*, 13(1):9–30, 2000.
8. K. Kurosawa and K. Suzuki. Truly efficient 2-round perfectly secure message transmission scheme. In *Proc. of EUROCRYPT*, pages 324–340, 2008.
9. F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error Correcting Codes.* North-Holland Publishing Company, 1978.
10. R. J. McEliece and D. V. Sarwate. On sharing secrets and Reed-Solomon codes. *Communications of the ACM*, 24(9):583–584, 1981.
11. 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.
12. 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.
13. Tal Rabin and Michael Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority (extended abstract). In *STOC*, pages 73–85, 1989.
14. A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.
15. B. Shanker, P. Gopal, K. Srinathan, and C. Pandu Rangan. Unconditional reliable message transmision in directed networks. In Proc. of SODA 2008.
16. K. Srinathan. Secure distributed communication. PhD Thesis, IIT Madras, 2006.
17. 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.
18. Y. Wang and Y. Desmedt. Perfectly secure message transmission revisited. IEEE Transactions on Information Theory. Manuscript. Available at www.sis.uncc.edu/∼yonwang/.
19. A. C. Yao. Protocols for secure computations. In *Proc. of 23rd IEEE FOCS*, pages 160–164, 1982.