Probabilistic Perfectly Reliable and Secure Message Transmission – Possibility, Feasibility and Optimality

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

[1] Dept of Computer Science and Engineering
IIT Madras, Chennai India 600036
arpita@cse.iitm.ernet.in, ashishc@cse.iitm.ernet.in, rangan@iitm.ernet.in
[2] Center for Security, Theory and Algorithmic Research
International Institute of Information Technology
Hyderabad India 500032
shankar@research.iiit.ac.in, srinathan@iiit.ac.in

Abstract. We study the interplay of network connectivity and the issues related to feasibility and optimality for *probabilistic perfectly reliable message transmission* (PPRMT) and *probabilistic perfectly secure message transmission* (PPSMT) in a *synchronous* network under the influence of a *mixed* adversary who possesses *unbounded* computing power and can corrupt different set of nodes in Byzantine, omission, failstop and passive fashion simultaneously. Our results show that that *randomness helps in the possibility of multiphase PPSMT and significantly improves the lower bound on communication complexity for both PPRMT and PPSMT protocols!!*

Keywords: Probabilistic Reliability, Information Theoretic Security, Fault Tolerance.

1 Introduction

We study the fundamental problem of *probabilistic perfectly reliable message transmission* (PPRMT), where two non-faulty players, the sender **S** and the receiver **R** are part of a synchronous network modeled as a undirected graph, a part of which may be under the influence of a unbounded computational powerful *mixed* adversary which is denoted by three tuple (t_b, t_o, t_f, t_p) and can corrupt t_b, t_o, t_f and t_p nodes in Byzantine, omission, failstop and passive fashion respectively. **S** intends to transmit a message m chosen from a finite field $\mathbb{F}$ to **R** using

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

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

K. Srinathan, C. Pandu Rangan, M. Yung (Eds.): Indocrypt 2007, LNCS 4859, pp. 101–122, 2007.

some protocol such that **R** should *correctly* obtain **S**'s message with probability at least $(1-\delta)$ for arbitrarily small $0 < \delta < 1/2$. The problem of *probabilistic perfectly secure message transmission* (PPSMT) is same as PPRMT except that the adversary should not get any information about the message.

Intuitively, the allowance of a small probability of error in the transmission should result in improvements in both the fault tolerance as well as the efficiency aspects of reliable and secure protocols. What exactly is the improvement? — this is the central question addressed in this paper. More specifically, we address the following in the context of PPRMT and PPSMT: (i) When is a protocol possible in the given network (Possibility) (ii) Once the existence of a protocol is ensured, what is the minimum communication complexity required by any protocol to reliably/securely send a message (Optimality), (iii) Finally, how to design such protocol which satisfies the proven minimum communication complexity bound (Feasibility). Finally, we compare our results with the existing results for *perfectly reliable message transmission* (PRMT) and *perfectly secure message transmission* (PSMT) and show that randomness and probabilistic approaches lead to improved communication, phase[1] and computational complexities. Moreover results on mixed adversaries reveal *higher* level of fault tolerance in the underlying network.

The problem of PPRMT and PPSMT in the presence of static[2] threshold Byzantine adversary was first defined and solved by Franklin *et al* [4]. As one of the key results, they have proved, that over undirected graphs PPRMT (PPSMT) is possible if and only if PRMT (PSMT) is possible!!! Subsequent works on PPRMT and PPSMT include [14,5].

1.1 Our Contribution

Any reliable/secure protocol is analyzed by the following parameters: the connectivity requirement of the network, the number of phases required by the protocol, the total number of field elements communicated by **S** and **R** throughout the protocol and the computation done by **S** and **R**. There is a *trade-off* among these parameter which is well studied in the literature for PRMT and PSMT [9,13]. In this paper we try to understand this trade-off for PPRMT and PPSMT in the presence of a *mixed* adversary, which is done for the *first* time in the literature of PPRMT and PPSMT[3]. The contribution of our paper is four-fold and can be summarized as follows: **(a)** We characterize single phase PPRMT and multiphase PPSMT protocols in the presence of mixed adversary and show that in many practical scenarios, our characterization shows higher level of fault tolerance in the underlying network, while the extant results offer no such insight. **(b)** We prove the lower bound on the communication complexity of any single phase PPRMT and multiple phase PPSMT protocol tolerating mixed adversary. **(c)** We also design

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

[2] By static adversary, we mean an adversary that decides on the set of players to corrupt before the start of the protocol.

[3] PRMT and PSMT in the presence of mixed adversary is studied in [7].

polynomial time *bit optimal* single phase PPRMT and four phase PPSMT protocols whose communication complexity satisfy our proven lower bounds. Our *single* phase PPRMT protocol has a *special* property that it achieves reliability with *constant* overhead when considered with *only* Byzantine adversary. Similarly our *four* phase PPSMT protocol has a *special* property that it achieves *secrecy* with *constant* overhead when considered with *only* Byzantine adversary. **(d)** Finally, we also compare our bit optimal PPRMT and PPSMT protocols with the existing bit optimal PRMT and PSMT protocols and cite many practical scenarios where no bit optimal PRMT or PSMT protocol exist but bit optimal PPRMT and PPSMT protocol do exists thus showing the power of allowing negligible error probability in the reliability of the protocols (without sacrificing secrecy).

1.2 Network Model

Following [3], we abstract away the network and concentrate on solving PPRMT and PPSMT problem for a single pair of processors, the *sender* **S** and the *receiver* **R**, connected by n parallel bi-directional channels $w_1, w_2, \ldots, w_n$ called wires such that an adversary having unbounded computing power can corrupt upto t_b, t_o, t_f and t_p wires in Byzantine, omission[4], failstop[5] and passive fashion respectively. Moreover, we assume that the wires that are under the control of the adversary in Byzantine, omission, failstop and passive fashion are mutually disjoint. Note that there is a difference between fail-stop and omission error[6]. If some value is sent over all the wires then it is said to be "broadcast"[7].

2 Probabilistic Perfectly Reliable Message Transmission

Here we completely characterize the set of tolerable adversaries, prove the lower bound for communication complexity of any single phase PPRMT protocol and present efficient/optimal protocol for single phase PPRMT.

[4] We say that a player P is under the control of an adversary in omission fashion, if the adversary can block the working of P at will at any time during the execution of the protocol. Also, as long as P is alive, it will follow the instructions of the protocol honestly. The adversary can eavesdrop the data/computation by P but cannot make P to deviate from the proper execution of the protocol. However, a blocked P can again become alive at some later stage of the protocol.

[5] We say that a player P is under the control of an adversary in a fail-stop manner, if the adversary can force P to *crash* at will at any time during the execution of the protocol. However, as long as P is alive, it will honestly follow the protocol. Also once P is crashed, it will not become alive again.

[6] The fail-stop error models a hardware failure caused by any natural calamity or manual shutdown. Also the nodes which are fail-stop corrupted cannot be passively listened by the adversary. On the other hand, nodes corrupted by omission adversary has listening capability. Thus omission adversary can be considered as a combination of fail-stop and passive adversary with the exception that unlike fail-stop error, a node which is crashed once by omission error may become alive during later stages of the protocol.

[7] Any information which is "broadcast" over at least $2t_b + t_o + t_f + 1$ wires will be recovered correctly at the receiving end (the receiver can output the majority).

2.1 Characterization for PPRMT

The existing characterization for PPRMT tolerating Byzantine adversary is:

Theorem 1 ([4]). *PPRMT between* **S** *and* **R** *against a* t_b *active Byzantine adversary is possible iff the network is* $(2t_b + 1)$*-(***S,R***)-connected.*

The characterization for PPRMT tolerating mixed adversary is as follows:

Theorem 2. *PPRMT between* **S** *and* **R** *against a mixed adversary* (t_b, t_o, t_p, t_f) *is possible iff the network is* $(2t_b + t_o + t_f + 1)$*-(***S,R***)-connected.*

Proof: If part: Consider a network which is $(2t_b + t_o + t_f + 1)$-(**S,R**)-connected. To send a message m, **S** simply *broadcasts* m to **R** over $2t_b + t_o + t_f + 1$ wires. It is easy to see that **R** will receive m with probability one by taking majority[8]. Only if part: Assume that a PPRMT protocol Π exists in a network $\mathcal{N}$ that is not $(2t_b + t_o + t_f + 1)$-(**S,R**)-connected. Consider the network $\mathcal{N}'$, induced by $\mathcal{N}$, on deleting $(t_o + t_f)$ vertices from a minimal vertex cutset of $\mathcal{N}$ (this can be viewed as an adversary blocking the communication over $t_o + t_f$ wires). It follows that $\mathcal{N}'$ is not $(2t_b + 1)$-(**S,R**)-connected. Evidently, if Π is a PPRMT protocol on $\mathcal{N}$, then Π' is a PPRMT protocol on $\mathcal{N}'$, where Π' is the protocol Π restricted to the players in $\mathcal{N}'$. However, from Theorem 1, Π' is non-existent. Thus Π is impossible too. □

Significance of Theorem 2: *Theorem 2* strictly generalizes *Theorem 1 because we obtain the latter by substituting* $t_o = t_f = 0$*. Now consider a network, which is 4-(***S,R***)-connected. From Theorem 1, on this network, any PPRMT protocol can tolerate* one *Byzantine fault. However, according to Theorem 2, it is possible to tolerate* one additional *faulty player, which can be either omission or fail-stop faulty. Thus our characterization shows more fault tolerance in comparison to the existing results.*

In the sequel, we show that allowance of negligible error probability in transmission reduces the communication lower bound markedly in comparison to perfect transmission.

2.2 Lower Bound on Communication Complexity of Single Phase PPRMT Protocol

We now prove the lower bound on the communication complexity of any single phase PPRMT protocol tolerating mixed adversary.

Theorem 3. *Any single phase PPRMT protocol, from* **S** *to* **R** *over* n *wires, communicates* $\Omega(\frac{n\ell}{n-(t_b+t_o+t_f)})$ *field elements to reliably transmit (with high probability)* ℓ *field elements.*

Proof: In any single phase PPRMT protocol, the concatenation of the information sent over n wires can be viewed as a (probabilistic) error correcting code

[8] The protocol described here is a naive protocol which does not take the advantage of allowing small error probability in the reliability.

which can correct t_b Byzantine errors and $t_o + t_f$ erasures with an arbitrarily high probability. Without loss of generality, the domain of the set of possible values of the data sent along the wire can be assumed to be the same for all the wires. Let $\mathbb{S}$ be the set of possible values of the data sent along the wires. Thus, each codeword can be viewed as concatenation of n elements from $\mathbb{S}$ which can be represented by $n \log |\mathbb{S}|$ bits. Now, the removal of any $(t_b + t_o + t_f)$ elements from each of the codewords which corresponds to an adversary blocking $t_b + t_o + t_f$ wires (a Byzantine adversary can also block communication) should result in shortened codewords that are all distinct. For if any two were identical, the original codewords could have differed only in at most $(t_b + t_o + t_f)$ elements implying that there exist two codewords c_1 and c_2 and an adversarial strategy such that the receiver's view is the *same* on the receipt of c_1 and c_2. Specifically, without loss of generality assume that c_1 and c_2 differ only in their last $(t_b + t_o + t_f)$ elements. That is, $c_1 = \alpha \circ \beta$ and $c_2 = \alpha \circ \gamma$, where $\circ$ denotes concatenation and $|\beta| = |\gamma| = (t_b + t_o + t_f)$ elements. Now, consider the two cases: (a) c_1 is sent and the adversary corrupts it to $\alpha \circ \perp$ by completely blocking the last $(t_b + t_o + t_f)$ elements (wires) and (b) c_2 is sent and the adversary again corrupts it to $\alpha \circ \perp$. Thus, $\mathbf{R}$ can not distinguish between the receipt of c_1 and c_2 with probability greater than $\frac{1}{2}$, which violates the PPRMT communication property (in any PPRMT protocol, receiver should be able to receive the message with probability more than $\frac{1}{2}$). Therefore, all shortened codewords containing $n - (t_b + t_o + t_f)$ elements from $\mathbb{S}$ are distinct. This implies that there are same number of shortened and original codewords. But the number of shortened codewords can be at most $C = |\mathbb{S}|^{(n-(t_b+t_o+t_f)}$. Now each shortened codeword can be represented by $\log C = (n - (t_b + t_o + t_f)) \log |\mathbb{S}|$ bits. Since, for error-correcting we need to communicate the longer codeword containing $n \log |\mathbb{S}|$, reliable communication of shortened codeword of $k = \log C$ bits incurs a communication cost of at least $n \log |\mathbb{S}|$ bits. Hence communicating a single bit incurs communicating $\frac{n}{(n-(t_b+t_o+t_f)}$ bits. So to communicate ℓ elements from a field $\mathbb{F}$, represented by $\ell \log |\mathbb{F}|$ bits, $\Omega(\frac{n\ell}{(n-(t_b+t_o+t_f))} \log |\mathbb{F}|)$ bits need to be sent. Since $\log |\mathbb{F}|$ bits represents one field element from $\mathbb{F}$, communicating ℓ elements from $\mathbb{F}$ requires a communication complexity of $\Omega(\frac{n\ell}{(n-(t_b+t_o+t_f)})$ field elements.

Note: *In any PPRMT protocol designed in a field $\mathbb{F}$, the size of the field depends upon the error probability δ of the protocol (we show this in next section)*[9].

Single Phase PRMT vs Single Phase PPRMT: *While the lower bound on the communication complexity of any single phase PRMT tolerating mixed*

[9] From Theorem 3, any PPRMT protocol to send ℓ field elements from $\mathbb{F}$ need to communicate $\Omega(\frac{n\ell}{(n-(t_b+t_o+t_f))} log|\mathbb{F}|)$ bits. Thus the communication complexity of any single phase PPRMT protocol is a function of δ (since $|\mathbb{F}|$ is a function of δ), though it is not explicitly mentioned in the expression derived in Theorem 3. It should also be noted that communication complexity explicitly depends upon the message size ℓ.

adversary is $\Omega(\frac{n\ell}{(n-(2t_b+t_o+t_f)})$ *[11], the same for PPRMT is* $\Omega(\frac{n\ell}{(n-(t_b+t_o+t_f)})$ *(Theorem 3). This clearly brings forth the power of randomization.*

2.3 Single Phase Bit Optimal PPRMT Protocol

We now present an optimal single phase PPRMT protocol **PPRMT_Single_Phase**, which delivers $(t_b+1)n$ field elements by communicating $O(n^2)$ field elements in single phase with (arbitrarily) high probability where $n=2t_b+t_o+t_f+1$. **PPRMT_Single_Phase** achieves reliability with *constant* overhead, when considered with only Byzantine adversary. The message block is represented by $\mathbf{M} = [m_1\ m_2\ \ldots\ m_n\ m_{n+1}\ m_{n+2} \ldots\ m_{2n} \ldots\ m_{t_bn+1}\ m_{t_bn+2} \ldots m_{t_bn+n}]$. Before the protocol, we describe a novel technique, called as **Extrapolation Technique** which we use in designing single phase PPRMT protocol **PPRMT_Single_Phase**.

Extrapolation Technique: We visually represent $\mathbf{M}$ as a rectangular array A of size $(t_b+1)\times n$ where the $j^{th}, 1 \le j \le t_b+1$ row contains the elements $m_{(j-1)n+1}\, m_{(j-1)n+2}\ \ldots\ m_{(j-1)n+n}$. For each column i of A, $1 \le i \le n$ we do the following: we construct the unique t_b degree polynomial $q_i(x)$ passing through the points $(1, m_i), (2, m_{n+i}), \ldots, (t_b+1, m_{t_bn+i})$ where $m_i, m_{n+i}, \ldots, m_{t_bn+i}$ belong to the i^{th} column A. Then $q_i(x)$ is evaluated at $t_b+t_o+t_f$ points namely, $x = t_b+2, t_b+3, \ldots n$ to obtain $c_{1i}, c_{2i}, \ldots, c_{(t_b+t_o+t_f)i}$. Finally, we obtain a square array D of size $n \times n$ containing n^2 elements, where

$$D = \begin{bmatrix} m_1 & m_2 & \ldots & m_i & \ldots & m_n \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ m_{(j-1)n+1} & m_{(j-1)n+2} & \ldots & m_{(j-1)n+i} & \ldots & m_{(j-1)n+n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ m_{t_bn+1} & m_{t_bn+2} & \ldots & m_{t_bn+i} & \ldots & m_{t_bn+n} \\ c_{11} & c_{12} & \ldots & c_{1i} & \ldots & c_{1n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ c_{j1} & c_{j2} & \ldots & c_{ji} & \ldots & c_{jn} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ c_{(t_b+t_o+t_f)1} & c_{(t_b+t_o+t_f)2} & \ldots & c_{(t_b+t_o+t_f)i} & \ldots & c_{(t_b+t_o+t_f)n} \end{bmatrix} = \begin{bmatrix} A \\ C \end{bmatrix} \text{ where}$$

C is the sub-matrix of D containing last $t_b+t_o+t_f$ rows. Thus D is the row concatenation of A of size $(t_b+1)\times n$ (containing elements of $\mathbf{M}$) and matrix C, whose elements are obtained from A by **Extrapolation Technique**. We now prove certain properties of the array D.

Lemma 1. *In D, all the n elements of any column can be uniquely generated from any t_b+1 elements of the same column.*

Proof: Without loss of generality, we prove this for i^{th} column of D. The elements in the i^{th} column are $m_i, m_{n+i}, \ldots, m_{t_bn+i}, c_{1i}, c_{2i}, \ldots, c_{ji}, , \ldots c_{(t_b+t_o+t_f)i}$. From the construction, the points $(1, m_i), (2, m_{n+i}), \ldots, (t_b+1, m_{t_bn+i})$, $(t_b+2, c_{1i}), (t_b+3, c_{2i}), \ldots, (n, c_{(t_b+t_o+t_f)i})$ lie on a unique t_b degree polynomial $q_i(x)$. Any t_b+1 points uniquely determines $q_i(x)$ and hence the remaining $t_b+t_o+t_f$ points. □

Lemma 2. *The elements of message* $\mathbf{M}$ *can be uniquely determined from any t_b+1 rows of D.*

Proof: From the construction of D, the elements of $\mathbf{M}$ are arranged in the first t_b+1 rows. If the first t_b+1 rows are known then the lemma holds trivially. On the other hand, if some other t_b+1 rows are known, then from Lemma 1, i^{th} $1 \leq i \leq n$ column of D can be completely generated from $t_b + 1$ elements of the same column. Hence, knowledge of any $t_b + 1$ rows can reconstruct the whole matrix D and hence the message (first t_b+1 rows of D). □

Lemma 3. *Modification of at most t_b elements along any column of D is detectable.*

Proof: Recall that in D, the points (corresponds to i^{th} column of D) $(1, m_i)$, $(2, m_{n+i}), \ldots, (t_b + 1, m_{t_b n+i}), (t_b + 2, c_{1i}), \ldots, (n, c_{(t_b+t_o+t_f)i})$ lie on a unique t_b degree polynomial $q_i(x)$. Now suppose t_b values are changed in such a manner that they lie on some other t_b degree polynomial $q'_i(x)$ where $q_i(x) \neq q'_i(x)$. Since both $q_i(x)$ and $q'_i(x)$ are of degree t_b, they can match on additional t_b common points. But still there are at least $n - 2t_b = t_o + t_f + 1$ points still passing only the original polynomial $q_i(x)$ (but not through $q'_i(x)$). Hence any attempt to interpolate a t_b degree polynomial passing through the elements of a column (in which at most t_b values has been changed) will clearly indicate that at most t_b values are changed along the column. Hence the lemma holds. □

We are now ready to describe our protocol. Let the set of n wires be denoted as $\mathcal{W} = \{w_1, w_2, \ldots, w_n\}$. Let δ be a bound on the probability that the protocol fails to deliver the correct message. We require the size of the field $\mathbb{F}$ be $\Omega(\frac{Q(n)}{\delta})$, for

Protocol PPRMT_Single_Phase - The Single Phase PPRMT Protocol

1. **S** generates a rectangular array D containing n^2 field elements, from the $(t_b + 1) \times n$ elements of message $\mathbf{M}$ using **Extrapolation Technique**. **S** then forms n polynomials $p_j(x), 1 \leq j \leq n$, each of degree $n-1$ where $p_j(x)$ is formed using the j^{th} row of D as follows: the coefficient of $x^i, 0 \leq i \leq n-1$ in $p_j(x)$ is the $(i+1)^{th}$ element of j^{th} row of D.

2. **S** chooses another n^2 field elements at random, say r_{ji}, $1 \leq i, j \leq n$. Over w_j, **S** sends the following to **R**: the polynomial $p_j(x)$ and the n ordered pairs $(r_{ji}, p_i(r_{ji}))$, for $1 \leq i \leq n$. Let $v_{ji} = p_i(r_{ji})$.

3. Let $\mathcal{F}$ denotes the set of wires that delivered nothing and let $\mathcal{B}$ denotes the set of wires that delivered invalid information (like higher degree polynomials etc.). Note that the wires in $\mathcal{B}$ are Byzantine corrupted because omission or fail-stop adversary is not allowed to modify the contents. **R** removes all the wires in $(\mathcal{F} \cup \mathcal{B})$ from $\mathcal{W}$ to work on the remaining wires in $\mathcal{W} \setminus (\mathcal{F} \cup \mathcal{B})$ out of which at most $t_b - |\mathcal{B}|$ could be Byzantine corrupted. Let **R** receives $p'_j(x)$ and (r'_{ji}, v'_{ji}) $1 \leq i \leq n$ over $w_j \in \mathcal{W} \setminus (\mathcal{F} \cup \mathcal{B})$. We say that w_j *contradicts* w_i if: $v'_{ji} \neq p'_i(r'_{ji})$ where $w_i, w_j \in \mathcal{W} \setminus (\mathcal{F} \cup \mathcal{B})$. Among all the wires in $\mathcal{W} \setminus (\mathcal{F} \cup \mathcal{B})$, **R** checks if there is a wire contradicted by at least $(t_b - |\mathcal{B}|) + 1$ wires. All such wires are Byzantine corrupted and removed (see Lemma 4).

4. To retrieve $\mathbf{M}$, **R** tries to reconstruct the array D as generated originally by **S** as follows: Corresponding to each $w_j \in \mathcal{W} \setminus (\mathcal{F} \cup \mathcal{B})$, which is not removed in step 3, **R** fills the j^{th} row of D in the following manner: coefficient of $x^i, 0 \leq i \leq n-1$ in $p'_j(x)$ occupies $(i+1)^{th}$ column in the j^{th} row of D; i.e., the coefficients of $p'_j(x)$ are inserted in j^{th} row of D such that the coefficient of x^i in $p'_j(x)$ occupies $(i+1)^{th}$ column in the j^{th} row of D.

5. After doing the above step for each $w_j \in \mathcal{W} \setminus (\mathcal{F} \cup \mathcal{B})$, which is not removed in step 3, **R** has at least $t_b + 1$ rows inserted in D (see Lemma 6). **R** then checks the validity of these rows as follows: corresponding to the $i^{th}, 1 \leq i \leq n$ column, **R** checks whether the points corresponding to the inserted elements of i^{th} column lie on a t_b degree polynomial.

6. If the above test fails for at least one column of D, then **R** outputs "FAILURE" and halts. Otherwise, **R** regenerates the complete D correctly and recovers $\mathbf{M}$ from the first $t_b + 1$ rows (see Lemma 6).

some polynomial $Q(n)$, but this is acceptable because complexity of the protocol increases logarithmically with field size.

Lemma 4. *In* **PPRMT_Single_Phase**, *if any* $w_j \in \mathcal{W} \setminus (\mathcal{F} \cup \mathcal{B})$ *is contradicted by at least* $(t_b - |\mathcal{B}|)+1$ *wires, then the polynomial* $p_j(x)$ *over* w_j *has been changed by adversary or in effect* w_j *is faulty.*

Proof: The wires in $\mathcal{B}$ are already identified to be Byzantine corrupted and hence neglected by $\mathbf{R}$. Also the wires in $\mathcal{F}$ delivers nothing and hence neglected by $\mathbf{R}$. So among the remaining $\mathcal{W} \setminus (\mathcal{F} \cup \mathcal{B})$ wires, at most $(t_b - |\mathcal{B}|)$ could be Byzantine corrupted. Also there cannot be any contradiction between two honest wires and hence any honest wire can be contradicted by at most $(t_b - |\mathcal{B}|)$ wires. Thus if a wire is contradicted by at least $(t_b - |\mathcal{B}|)+1$ wires then it is faulty. □

Lemma 5. *In the protocol, if the adversary corrupts a polynomial over wire* w_j *in such a way that* w_j *is not removed during step 3, then* $\mathbf{R}$ *will always be able to detect it at the end of step 5 and outputs "FAILURE".*

Proof: At the beginning of step 5, there are at least $t_b + 1$ rows present in the partially reconstructed D. This follows from the fact there always exist $t_b + 1$ honest wires which will deliver correct polynomials to $\mathbf{R}$. As mentioned in Lemma 4, any honest wire can be contradicted by at most $(t_b - |\mathcal{B}|)$ wires and hence is not be removed by $\mathbf{R}$ during step 4. So the coefficients of the polynomials corresponding to these honest wires will be present in partially reconstructed D.

Now if w_j (which has delivered a faulty polynomial) is not removed during step 3, then during step 4, the coefficients of $p'_j(x)$ are inserted in the j^{th} row of partially reconstructed D. Since $p_j(x) \neq p'_j(x)$, there is at least one coefficient in $p'_j(x)$ which is different from the corresponding coefficient in $p_j(x)$. Let $p_j(x)$ differs from $p'_j(x)$ in the coefficient of x^i. Then $(i+1)^{th}$ column of partially reconstructed D differs from the $(i+1)^{th}$ column of original D at j^{th} position. The proof now follows from Lemma 3. Hence $\mathbf{R}$ outputs "FAILURE". □

Lemma 6. *In* **PPRMT_Single_Phase**, *if the test in step 5 succeeds for all the* n *columns of partially constructed* D, *then* $\mathbf{R}$ *will never output "FAILURE" and always recovers* $\mathbf{M}$ *correctly.*

Proof: As explained in previous Lemma, at the beginning of step 5, there will be at least $t_b + 1$ rows present in the partially reconstructed D. Now if the test in step 5 succeeds for all the n columns of partially constructed D, it implies that all the rows present in the partially reconstructed D are same as the corresponding rows in the original D. From Lemma 1, $\mathbf{R}$ will be able to completely regenerate all the n columns of original D. The proof now follows from Lemma 2. It is easy to see that $\mathbf{R}$ does not outputs "FAILURE" in this case.

Theorem 4. PPRMT_Single_Phase *terminates with a non-"FAILURE" output with high probability.*

Proof: Since no honest wire contradicts another honest wire, from Lemma 4, all the wires removed by $\mathbf{R}$ during step 3 are indeed faulty. We need to show that

if a wire is corrupted (the polynomial over the wire is changed), then it will be contradicted by all the honest players with high probability. Let π_{ij} be the probability that a corrupted wire w_j will not be contradicted by a honest wire w_i. This means that the adversary can ensure that $p_j(r_{ij}) = p'_j(r_{ij})$ with a probability of π_{ij}. Since there are only $n-1$ points at which these two polynomials intersect, this allows the adversary to guess the value of r_{ij} with a probability of at least $\frac{\pi_{ij}}{n-1}$. But since r_{ij} was selected uniformly in $\mathbb{F}$, the probability of guessing it is at most $\frac{1}{|\mathbb{F}|}$. Therefore we have $\pi_{ij} \leq \frac{n-1}{|\mathbb{F}|}$ for each i, j. Thus the total probability that the adversary can find w_i, w_j such that corrupted wire w_j will not be contradicted by w_i is at most $\sum_{i,j} \pi_{ij} \leq \frac{n^2(n-1)}{|\mathbb{F}|}$. Since $\mathbb{F}$ is chosen such that $|\mathbb{F}| \geq \frac{Q(n)}{\delta}$, it follows that the protocol outputs a non-"FAILURE" value with probability $\geq 1-\delta$ if we set $Q(n) = n^3$. □

Note. PPRMT_Single_Phase *is a* special *kind of a probabilistic reliable message transmission protocol where* **R** *actually* knows *whether he outputs the correct message. But according to our definition of PPRMT, inability of* **R** *to "detect" every occurrence of an error is acceptable. Thus, our protocol has a strictly stronger property than that of necessary.*

Lemma 7. PPRMT_Single_Phase *reliably sends* $n(t_b+1)$ *field elements by communicating* $O(n^2)$ *field elements. In terms of bits, the protocol sends* $n(t_b+1)\log|\mathbb{F}|$ *bits by communicating* $O(n^2 \log|\mathbb{F}|)$ *bits.*

Proof: Over each wire, **S** sends a polynomial of degree $n-1$ and n ordered pair. Thus the total communication complexity is $O(n^2)$. Since each element from field $\mathbb{F}$ can be represented by $\log|\mathbb{F}|$ bits, the communication complexity of the protocol is $O(n^2 log|\mathbb{F}|)$ bits. □

Achieving PPRMT in Constant Factor Overhead in Single Phase
In the presence of Byzantine fault, ℓ *field elements can be transmitted by communicating* $O(\ell)$ *field elements in three phases [9] with perfect reliability. Also, achieving the same in single phase in the presence of Byzantine adversary is impossible [12]. However it is attainable in case of probabilistic reliability. In* **PPRMT_Single_Phase***, if* $t_o = t_f = 0$*, then* $(t_b+1)n = O(n^2)$ *field elements (when* $t_o = 0, t_f = 0$*,* $n = 2t_b+1$ *and so* $t_b = O(n)$*) can be sent by communicating* $O(n^2)$ *field elements. Thus, by allowing a small error probability in the reliability we can send* ℓ *field elements by communicating* $O(\ell)$ *field elements in only single phase.*

In Theorem 3, substituting $n = 2t_b + t_o + t_f + 1$ and $\ell = n(t_b+1)$, we find that any single phase PPRMT protocol must communicate $\Omega(n^2)$ elements to send $n(t_b+1)$ elements. Now, from Lemma 7, the communication complexity of **PPRMT_Single_Phase** is $O(n^2)$. Hence our protocol has **optimal communication complexity**. In terms of bits, **PPRMT_Single_Phase** sends $n(t_b+1)\log|\mathbb{F}|$ bits by communicating $n^2\log|\mathbb{F}|$ bits where $\mathbb{F} = \frac{Q(n)}{\delta}$, $Q(n) = n^3$ and $1-\delta$ is the least probability with which the protocol terminates without "FAILURE". So, our protocol is **bit-optimal**.

Finally, we would like to point out that single phase PPRMT protocols can also be designed using the idea of check vectors proposed by Rabin and Ben-Or [10] for VSS. However, simple extension of their idea does not leads to a **bit-optimal** single phase PPRMT protocol.

3 Multiphase PPSMT Protocol in Undirected Networks

In this section, we provide characterization, lower bound on the communication complexity of any multiphase PPSMT protocol and also design one such protocol whose communication complexity matches with the lower bound.

3.1 Characterization for Multiphase PPSMT Protocol

In the previous section, we have shown how randomization affects the possibility and optimality of PPRMT protocol in the presence of a mixed adversary. We now explore the effect of randomization on the possibility and optimality of PPSMT protocol tolerating a mixed adversary. Our first step towards this exploration is to characterize the possibility of any multiphase PPSMT protocol.

Theorem 5. *Multiphase PPSMT between* **S** *and* **R** *in an undirected network tolerating a mixed adversary characterized by 4-tuple* (t_b, t_o, t_f, t_p) *is possible if and only if the network is* $(t_b + \max(t_b, t_p) + t_o + t_f + 1)$*-(***S,R***)-connected.*

Proof: Necessity: We consider two cases for proving the necessity.

• **Case 1:** $t_p \leq t_b$: In this case, the network is $(2t_b + t_o + t_f + 1)$-(**S,R**) connected which is necessary for PPRMT (Theorem 2) and hence obviously for PPSMT.

• **Case 2:** $t_p > t_b$: Here, the network is $(t_b + t_p + t_o + t_f + 1)$-(**S,R**)-connected. This condition is necessary for PPSMT because, if the network is $(t_b + t_p + t_o + t_f)$-(**S,R**)-connected, then the adversary may strategize to simply block all message

Protocol SECURE - A Three Phase PPSMT Protocol

Phase I: S to R

• Along $w_i, 1 \leq i \leq n$, **S** sends to **R** two randomly picked elements ρ_{i1} and ρ_{i2} chosen from $\mathbb{F}$.

Phase II: R to S

• Suppose **R** receives values in syntactically correct form along $n' \leq n$ wires. **R** neglects the remaining $(n - n')$ wires. Let **R** receives ρ'_{i1} and ρ'_{i2} along wire w_i, where w_i is not neglected by **R**.

• **R** chooses uniformly at random an element $K \in \mathbb{F}$. **R** then broadcasts to **S** the following: identities of the $(n - n')$ wires neglected by him, the secret K and the values $(K\rho'_{i1} + \rho'_{i2})$ for all i such that w_i is not neglected by **R**.

Phase III: S to R

• **S** correctly receives the identities of $(n - n')$ wires neglected by **R** during **Phase II** (because irrespective of the value of t_b and t_p, n is at least $2t_b + t_o + t_f + 1$. So any information which is broadcast over n wires will be received correctly). **S** eliminates these wires. **S** also correctly receives K and the values, say $u_i = (K\rho'_{i1} + \rho'_{i2})$ for each i, such that wire w_i is not eliminated by **R**.

• **S** then computes the set H such that $H = \{w_i | u_i = (K\rho_{i1} + \rho_{i2})\}$. Furthermore, **S** calculates the secret key ρ where: $\rho = \sum_{w_i \in H} \rho_{i2}$. **S** then broadcasts the set H and the blinded message $\mathbf{M} \oplus \rho$ to **R**, where **M** is a single field element.

Message Recovery by R

• **R** correctly receives H and computes his version of ρ'. If z' is the blinded message received, **R** outputs $\mathbf{M} = z' \oplus \rho'$.

through $(t_b + t_o + t_f)$ vertex disjoint paths and thereby ensure that every value received by **R** is also listened by the adversary.

Sufficiency: Suppose that network is $(t_b + \max(t_b, t_p) + t_o + t_f + 1)$-(**S,R**)-connected. Then from Menger's theorem [6], there exist at least $n = (t_b + \max(t_b, t_p) + t_o + t_f + 1)$ vertex disjoint paths from **S** to **R**. We model these paths as wires $w_1, w_2, \ldots, w_n$. We design a three phase PPSMT protocol called **SECURE** to securely send a single field element.

It can be shown that with a probability of at least $\left(1 - \frac{1}{|\mathbb{F}|}\right)$, $\rho' = \rho$ and hence **R** almost always learns the correct message (Proof is similar to that of the correctness and security of the information-checking protocol of [10]). Since $n = t_b + \max(t_b, t_p) + t_o + t_f + 1$, there exists at least one wire say w_i, which is not controlled by the adversary. So, the corresponding ρ_{i2} is unknown to adversary implying information theoretic security for $\rho = \sum_{w_i \in H} \rho_{i2}$ and hence for **M**. It is easy to see that the communication complexity of **SECURE** is $O(n^2)$. □

MultiPhase PSMT vs MultiPhase PPSMT: *From [7], for any multiphase Perfectly Secure Message Transmission (PSMT) protocol, the network should be* $(2t_b + t_o + t_f + t_p + 1)$-*(***S, R***) connected. Thus, except when either* t_b *or* $t_p = 0$*, Theorem 5 shows that allowing a negligible error probability in the reliability of the protocol (without sacrificing the secrecy) significantly helps in the possibility of multiphase secure message transmission protocol.*

Note: *Theorem 5 characterizes multiphase PPSMT protocol. A single phase PPSMT protocol tolerating Byzantine adversary is given in [5]. The characterization, lower bound on the communication complexity and an optimal single phase PPSMT tolerating mixed adversary is given in [8]. The connectivity requirement for single phase PPSMT is more*[10] *than multiphase PPSMT [8].*

3.2 Lower Bound on Communication Complexity of Multiphase PPSMT Protocol

We now prove the lower bound on the communication complexity of any r-phase ($r \geq 2$) PPSMT protocol which sends ℓ field elements tolerating a mixed adversary (t_b, t_o, t_f, t_p). Let $n \geq t_b + \max(t_b, t_p) + t_o + t_f + 1$.

Theorem 6. *Any* r*-phase* ($r \geq 2$) *PPSMT protocol which securely sends* ℓ *field elements in the presence of a threshold adversary* (t_b, t_o, t_f, t_p) *needs to communicate at least* $\Omega\left(\frac{n\ell}{n-(t_b+t_o+t_f+t_p)}\right)$ *field elements.*

Proof: The proof follows from Lemma 8 and Lemma 9, which are proved below.

Lemma 8. *The communication complexity of any multi-phase PPSMT protocol to send a message against an adversary corrupting up to* $b(\leq t_b), F(\leq t_f)$ *and* $P(\leq t_b + t_o + t_p)$ *of the wires in Byzantine, Fail-stop and passive manner respectively is not less than the communication complexity of distributing* n *shares for*

[10] In [8], it is shown that for the existence of single phase PPSMT protocol the network should be $2t_b + 2t_o + t_f + t_p + 1$-(**S, R**)-connected.

the message such that any set of $n-F$ correct shares has full information about the message while any set of P shares has no information.

To prove the lemma, we begin with defining a weaker version of single-phase PPSMT called PPSMT with Error Detection (PPSMTED). We then prove the equivalence of communication complexity of PPSMTED protocol to send message $\mathbf{M}$ and the share complexity of distributing n shares for $\mathbf{M}$ such that any set of $n-F$ correct shares has full information about $\mathbf{M}$ while any set of P shares has no information about $\mathbf{M}$. To prove the aforementioned statement, we first show their equivalence (Claim 1). Finally, we will show the equivalence of single-phase protocol PPSMTED and multiphase PPSMT protocol in terms of communication complexity and also answer the question: why it is weaker than multiphase PPSMT protocol (Claim 3). These two equivalence will prove the desired equivalence as stated in this lemma. Note that b, F and P are bounded by t_b, t_f and $t_b + t_o + t_p$ respectively.

Definition 1. *A single phase PPSMT protocol is called PPSMTED if it satisfies the following:*

1. *If the adversary is passive on all the P ($P \leq t_b+t_o+t_p$ which is the maximum limit on the number of passive adversaries) corrupted wires then $\mathbf{R}$ securely receives the message sent by $\mathbf{S}$.*
2. *If the adversary corrupts information over some b wires ($b \leq t_b$), then $\mathbf{R}$ detects it, and aborts.*
3. *If adversary blocks some $F \leq t_f$ wires, without doing any other modification, then $\mathbf{R}$ recovers message correctly. Else if adversary blocks more than t_f wires or do some modification (or both), then $\mathbf{R}$ aborts.*
4. *The adversary obtains no information about the transmitted message.*

We next show that the properties of PPSMTED protocol for sending message $\mathbf{M}$ is equivalent to the problem of distributing n shares for $\mathbf{M}$ such that any set of $n-F$ correct shares has full information about $\mathbf{M}$ while any set of P shares has no information about the message.

Claim 1. *Let Π be a PPSMTED protocol tolerating an adversary that can corrupt up to any b, F and P of the n wires connecting $\mathbf{S}$ and $\mathbf{R}$ in Byzantine, fail-stop and passive manner respectively. In an execution of Π for sending a message $\mathbf{M}$, the data $s_i, 1 \leq i \leq n$ sent by the $\mathbf{S}$ along wires $w_i, 1 \leq i \leq n$ form n shares for $\mathbf{M}$ such that any set of $n-F$ correct shares has full information about $\mathbf{M}$ while any set of P shares has no information.*

Proof: The fact that any set of P shares have no information about $\mathbf{M}$ follows directly from property 1 and 4 of definition of PPSMTED. We now show that any set of $n-F$ correct shares has full information about $\mathbf{M}$. The proof is by contradiction. For a set of wires $A \subseteq W$, let $Message(\mathbf{M}, A)$, denotes the set of messages sent along the wires in A during the execution of PPSMTED to send $\mathbf{M}$. Now for any set C, $|C| \geq n-F$ of honest wires, $Message(\mathbf{M}, C)$ should uniquely determine the message $\mathbf{M}$. Suppose not, then there exists another message $\mathbf{M}'$ such that $Message(\mathbf{M}, C) = Message(\mathbf{M}', C)$. By definition

the fail-stop adversary can block all the messages sent along the F wires not in C. Thus for two different executions of PPSMTED to send two distinct message $\mathbf{M}$ and $\mathbf{M}'$, there exists an adversary strategy such that view of $\mathbf{R}$ at the end of two executions is exactly same. This is a contradiction to the property 3 of PPSMTED protocol Π which outputs the correct message if at most F fail-stop errors take place. □

The above claim also says that the communication complexity of PPSMTED protocol to send $\mathbf{M}$ is same as the share complexity (length of the sum of all shares) of distributing n shares for a message $\mathbf{M}$ such that any set of $n-F$ correct shares has full information about $\mathbf{M}$ while any set of P shares has no information about the message. Now we step forward to show the communication complexity of PPSMTED protocol is the lower bound on the communication complexity of any multiphase PPSMT protocol.

Before that we take a closer look at the execution of any multi-phase PPSMT protocol. $\mathbf{S}$ and $\mathbf{R}$ are modeled as polynomial time Turing machines with access to a random tape. The number of random bits used by the $\mathbf{S}$ and $\mathbf{R}$ are bounded by a polynomial $q(n)$. Let $r_1, r_2 \in \{0,1\}^{q(n)}$ denote the contents of the random tapes of $\mathbf{S}$ and $\mathbf{R}$ respectively. The message $\mathbf{M}$ is an element from the set $\{0,1\}^{p(n)}$, where $p(n)$ is a polynomial. A transcript for an execution of a multiphase PPSMT protocol Π is the concatenation of all the messages sent by $\mathbf{S}$ and $\mathbf{R}$ along all the wires.

Definition 2. *A passive transcript $\mathcal{T}(\Pi, \mathbf{M}, r_1, r_2)$ is a transcript for the execution of the multiphase protocol Π with $\mathbf{M}$ as the message to be sent, r_1, r_2 as the contents of the random tapes of sender $\mathbf{S}$ and the receiver $\mathbf{R}$ and the adversary remaining passive throughout the execution. Let $\mathcal{T}(\Pi, \mathbf{M}, r_1, r_2, w_i)$ denote the passive transcript restricted to messages exchanged along the wire w_i. When $\Pi, \mathbf{M}, r_1, r_2$ are obvious from the context, we drop them and denote the passive transcript restricted to a wire w_i by $\mathcal{T}_{w_i}$. Similarly, $\mathcal{T}_B$ denotes the set of passive transcripts over the set of wires in B.*

Given $(\mathbf{M}, r_1, r_2)$ it is possible for $\mathbf{S}$ to compute $\mathcal{T}(\Pi, \mathbf{M}, r_1, r_2)$ by simulating $\mathbf{R}$ with random tape r_2. Similarly given $(\mathbf{M}, r_1, r_2)$ $\mathbf{R}$ can compute $\mathcal{T}(\Pi, \mathbf{M}, r_1, r_2)$ by simulating $\mathbf{S}$. Note that although $\mathbf{S}$ and receiver require both r_1, r_2 to generate the transcript, $\mathbf{R}$ requires only r_2 in order to obtain the message $\mathbf{M}$ from the transcript. This is clear since $\mathbf{R}$ does not have access to r_1 during the execution of Π but still can retrieve the message $\mathbf{M}$ from the messages exchanged.

Definition 3. *A transcript $\mathcal{T}_B$, with $n - F \leq |B| \leq n$ is said to be a valid fault-free transcript with respect to $\mathbf{R}$ if there exists random string r_2 and message $\mathbf{M}$ such that protocol Π at $\mathbf{R}$ with r_2 as the contents of the random tape and $\mathcal{T}_B$ as the messages exchanged, terminates by outputting the message $\mathbf{M}$.*

Definition 4. *Two transcripts $\mathcal{T}_B$ and $\mathcal{T}'_B$, where $n - F \leq B \leq n$ are said to be* adversely close *if the two transcripts differ only on a set of wires A such that $|A| \leq b + (|B| - (n - F))$. Formally $|\{w_i \in W | \mathcal{T}_{w_i} \neq \mathcal{T}'_{w_i}\}| \leq b + (|B| - (n - F))$.*

Claim 2. *Two valid fault-free transcripts* $\mathcal{T}_B(\Pi, \mathbf{M}, r_1, r_2)$ *and* $\mathcal{T}_B(\Pi, \mathbf{M}', r_1', r_2')$ *with two different message inputs* $\mathbf{M}, \mathbf{M}'$*, cannot be adversely close to each other, where* $n - F \leq B \leq n$.

Proof: Suppose two valid fault-free transcripts $\mathcal{T}_B(\Pi, \mathbf{M}, r_1, r_2)$ and $\mathcal{T}_B(\Pi, \mathbf{M}', r_1', r_2')$ are adversely close, then there is a set of wires A, $|A| \leq b + (|B| - (n - F))$ such that the two transcripts differ only on messages sent along the wires in A. Without loss of generality, assume last $b + (|B| - (n - F))$ wires belong to A with $A = X \circ Y$ where $|X| = b$ and $|Y| = (|B| - (n - F))$. Consider the following two executions of Π where the contents of **S**'s and **R**'s random tapes are r_1, r_2 respectively.

• **S** wants to send **M**. **S** and **R** executes Π while the adversary stop the wires in Y to deliver any message. As $\mathcal{T}_{B-Y}(\Pi, \mathbf{M}, r_1, r_2)$ is a valid transcript with respect to **M**, **R** terminates with output **M**.

• **S** wants to send **M**. **S** and **R** executes Π. The adversary blocks messages over Y and changes the messages along wires in X such that the view of **S** is $\mathcal{T}_{B-Y}(\Pi, \mathbf{M}, r_1, r_2)$ but the view of **R** is $\mathcal{T}_{B-Y}(\Pi, \mathbf{M}', r_1', r_2')$. Since $\mathcal{T}_{B-Y}(\Pi, \mathbf{M}', r_1', r_2')$ is a valid transcript with respect to $\mathbf{M}'$, **R** will terminate with output $\mathbf{M}'$.

The two scenarios differ only in the adversarial behavior and in the contents of **R**'s random tape. In both the scenarios **S** wanted to send message **M**. But the message received by receiver **R** in the second case is an incorrect message $\mathbf{M}'$. Thus, with only probability 1/2, **R** will output the correct message **M**. This is a contradiction because Π is a PPSMT protocol. □

Till now, we have shown that a transcript over at least $n - F$ correct wires allows **R** to output **M** correctly. We now show how to reduce a multiphase PPSMT protocol into a single phase PPSMTED protocol.

Protocol PPSMTED

• **S** computes the passive transcript $\mathcal{T}(\Pi, \mathbf{M}, r_1, r_2)$ for some random r_1 and r_2 and sends $\mathcal{T}(\Pi, \mathbf{M}, r_1, r_2, w_i)$ to **R** along w_i.

• If **R** does not receives information through at least $n - F$ wires then **R** outputs ERROR and stop. Otherwise, let **R** receives information over the set of wires $B = \{w_{i_1}, w_{i_2}, \ldots, w_{i_\alpha}\}$ where $n - F \leq |B| \leq n$. **R** concatenates the values received along these wires to obtain a transcript $\mathcal{T}_B$ (which may be corrupted along t_b wires) and does the following:

– for each $\mathbf{M} \in \{0,1\}^{p(n)}$ and $r_2 \in \{0,1\}^{q(n)}$ do:
  If $\mathcal{T}_B$ is a valid transcript with random tape contents r_2 for message **M** then output **M** and stop.
  Output ERROR.

Claim 3. *The Communication complexity of any multiphase PPSMT protocol* Π *is at least the communication complexity of* **PPSMTED** *protocol. Also* Π *has stronger properties than* **PPSMTED**. *Finally,* **PPSMTED** *does not reveals* **M** *to the adversary.*

Proof: The communication complexity of any multiphase PPSMT protocol Π assuming the adversary to be passive during the complete execution is trivially a lower bound for any multiphase PPSMT protocol with corruption in any phases. In **PPSMTED**, **S** communicates the transcript generated by him assuming adversary to be passive throughout the execution of Π to **R**. The cost of communicating such a transcript by **PPSMTED** is same as of Π with the assumption that adversary remain passive throughout the execution of Π. **PPSMTED** is weaker than Π for the following reason: under the passive adversary assumption Π always outputs M but **PPSMTED** does not output M for certain adversarial behavior . But in that case it detects it and aborts.

The message sent along the wire w_i in **PPSMTED** is the concatenation of the messages sent along w_i in an execution of Π. Hence the adversary cannot obtain any information about the message **M**. From Claim 2, we know that valid transcripts of two different messages cannot be adversely close to each other. So irrespective of the actions of the adversary, the transcript received by **R** cannot be a valid transcript for any message other than **M** for any value of r_2. Hence if **R** outputs a message **M** then it is the same message sent by **S**. □

This completes the proof of Lemma 8. We now prove the share complexity of distributing n shares for a message such that any set of $n-F$ correct shares has full information while any set of P shares has no information about the message.

Lemma 9. *The share-complexity (that is the length of the sum of all shares) of distributing n shares for a message of size ℓ field elements from $\mathbb{F}$ such that any set of $n-F$ correct shares has full information about the message while any set of P shares has no information about the message is $\Omega(\frac{n\ell}{(n-F-P)})$.*

Proof: Let X_i denotes the i^{th} share. For any subset $A \subseteq \{1, 2 \ldots n\}$ let X_A denote the set of variables $\{X_i | i \in A\}$. Let **M** be a value drawn uniformly at random from $\mathbb{F}^l$. 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 [2]. Since **M** is a value drawn uniformly at random from $\mathbb{F}^\ell$, we have $H(\mathbf{M}) = \ell$. Since any set B consisting of $n-F$ correct shares has full information about **M**, we have $H(\mathbf{M}|X_B) = 0$. Consider any subset $A \subset B$ such that $|A| = P$. Since any set of P shares has no information about **M**, we have $H(\mathbf{M}|X_A) = H(\mathbf{M})$. It is clear that

$$H(\mathbf{M}|X_A) = H(\mathbf{M}|X_A|X_{B-A}) + H(X_{B-A}) \leq H(\mathbf{M}|X_A, X_{B-A})) + H(X_{B-A}) = H(X_{B-A})$$
$$\text{So } H(\mathbf{M}) \leq H(X_{B-A}) \quad \{ \text{ since } H(\mathbf{M}|X_A) = H(\mathbf{M}) \}$$

Since $|B| = n-F$ and $|A| = P$, $|B-A| = n-F-P$. So for any set C of size $|B-A| = n-F-P$,

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

Since there are $\binom{n}{n-F-P}$ possible subsets of cardinality $n-F-P$, summing the above equation over all possible subsets of cardinality $n-F-P$ we get

$$\sum_{C}\sum_{i\in C} H(X_i) \geq \binom{n}{n-F-P} H(\mathbf{M})$$

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

$$\binom{n-1}{n-F-P-1}\sum_{i=1}^{n} H(X_i) \geq \binom{n}{n-F-P} H(\mathbf{M}) \;\Rightarrow\; \sum_{i=1}^{n} H(X_i) \geq \frac{n}{n-F-P} H(\mathbf{M})$$

which is equal to $\frac{n\ell}{n-F-P}$. Thus the share-complexity for any $\mathbf{M} \in \mathbb{F}^{\ell}$ is $\Omega\left(\frac{n\ell}{n-F-P}\right)$. □

Since $P \leq t_b + t_o + t_b$ and $F \leq t_f$, $\Omega\left(\frac{n\ell}{n-F-P}\right) = \Omega\left(\frac{n\ell}{n-(t_b+t_o+t_f+t_p)}\right)$. Theorem 6 now follows from Lemma 8 and Lemma 9. □

Note. *In terms of bits, any multiphase PPSMT protocol must communicate* $\Omega\left(\frac{n\ell}{n-(t_b+t_o+t_f+t_p)} \log|\mathbb{F}|\right)$ *bits to send* $\ell \log|\mathbb{F}|$ *bits, where* $|\mathbb{F}|$ *is a function of* δ*. In the next section, we give a concrete PPSMT protocol satisfying this bound and show how to set* $|\mathbb{F}|$ *as a function of* δ*.*

Randomization Helps in Reducing the Communication Complexity of Multiphase Secure Protocols: *In [7], it is shown that any multiphase PSMT protocol has a communication complexity of* $\Omega\left(\frac{n\ell}{n-(2t_b+t_o+t_f+t_p)}\right)$ *to securely send* ℓ *field elements. Comparing this bound with Theorem 6, we find that allowing a negligible error probability in reliability (without sacrificing the privacy) significantly reduces the communication complexity of multiphase secure protocol. We support this claim by designing a four phase PPSMT protocol whose total communication complexity matches the bound proved in Theorem 6.*

3.3 Constant Phase Bit Optimal PPSMT Protocol

Here we design a *bit optimal* multiphase PPSMT protocol called **PPSMT_Mixed** tolerating mixed adversary. The protocol terminates in four phases and uses the three phase **SECURE** protocol (described in Theorem 5) as a black-box[11]. The four phase protocol **PPSMT_Mixed** securely sends ℓ field elements by communicating $O(\ell)$ field elements against only Byzantine adversary, thus achieving *secrecy* with *constant* overhead.

[11] Since $n = t_b + \max(t_b, t_p) + t_o + t_f + 1$, we can execute **SECURE** protocol as a black-box. We cannot use any single phase PPSMT protocol as a black-box because the connectivity requirement for single phase and multi phase PPSMT are different.

If $t_p \geq t_b$, then the protocol securely sends n^2 field elements by communicating $O(n^3)$ field elements and if $t_b > t_p$, then $(t_b - t_p)n^2$ field elements by communicating $O(n^3)$ field elements. Let, $n = t_b + \max(t_b, t_p) + t_o + t_f + 1$. In the protocol, depending upon whether $t_b \leq t_p$ or $t_p < t_b$, the field size $|\mathbb{F}|$ is set to at least $\frac{3n^2}{\delta}$ or $\frac{4n^4(t_b - t_p)}{\delta t_b}$ respectively, where δ is the error probability of the protocol. Before describing the protocol, we first recall an algorithm from [12].

Consider the following problem: Suppose **S** and **R** by some means agree on a sequence of n numbers $x = [x_1 x_2 \dots x_n] \in \mathbb{F}^n$ such that the adversary knows $n - f$ components of x, but the adversary has no information about the other f components of x, however, **S** and **R** do not necessarily know which values are known to the adversary. The goal is for **S** and **R** to agree on a sequence of f numbers $y_1 y_2 \dots y_f \in \mathbb{F}$ such that the adversary has no information about $y_1 y_2 \dots y_f$. This is achieved by the following algorithm [12]:

Algorithm EXTRAND$_{n,f}(x)$. Let V be a $n \times f$ Vandermonde matrix with members in $\mathbb{F}$. This matrix is published as a part of the protocol specification. **S** and **R** both locally compute the product $[y_1\ y_2\ \dots\ y_f] = [x_1\ x_2\ \dots\ x_n]V$.

Lemma 10 ([12]). *The adversary gets no information about* $[y_1\ y_2\ \dots\ y_f]$ *computed in EXTRAND.*

Theorem 7. *By setting* $|\mathbb{F}| \geq \frac{3n^2}{\delta}$ *(if* $t_p \geq t_b$*) or* $|\mathbb{F}| \geq \frac{4n^4(t_b - t_p)}{\delta t_b}$ *(if* $t_b > t_p$*) the protocol* **PPSMT_Mixed** *securely transmits the message* **M** *with an error probability bounded by* δ*.*

Proof: For better understanding, we first prove the theorem when $t_b > t_p$. So $|\mathbb{F}| \geq \frac{4n^4(t_b - t_p)}{\delta t_b}$. It is evident from the protocol construction that the theorem holds if the following are true:

1. For all $1 \leq i \leq n$, $\rho'_i = \rho_i$ with probability $\geq (1 - \frac{\delta}{4})$.
2. For all $1 \leq i \leq n$, $y'_i = y_i$ with probability $\geq (1 - \frac{\delta}{4})$.
3. If the wire w_i were indeed corrupt (i.e., the n^2 tuple sent over w_i is changed by the adversary), then $w_i \in L_{fault}$ with probability $\geq (1 - \frac{\delta}{4})$.
4. The protocol **PPRMT_Single_Phase** to send the vector d fails with probability of at most $\frac{\delta}{4}$.
5. The adversary learns no (additional) information about the transmitted message **M**.

The error probability of the protocol depends upon the error probability of the first four events. If each of the above are true, then the protocol's failure probability is bounded by δ. We prove now each of the above four claims separately.

Claim 4. *In* **PPSMT_Mixed**, *for all* $1 \leq i \leq n$, $\rho'_i = \rho_i$ *with probability* $\geq (1 - \frac{\delta}{4})$.

Protocol PPSMT_Mixed
A Bit Optimal 4-Phase PPSMT Protocol Tolerating Mixed Adversary

The message $\mathbf{M}$ is a sequence of n^2 field elements if $t_b \leq t_p$, otherwise it is a sequence of $(t_b - t_p)n^2$ field elements.

Phase I ($\mathbf{R}$ to $\mathbf{S}$)

• $\mathbf{R}$ selects at random n^3 elements, r_{ij}, $1 \leq i \leq n, 1 \leq j \leq n^2$ from field $\mathbb{F}$. $\mathbf{R}$ also randomly selects $\rho_1, \rho_2, \ldots \rho_n$ from $\mathbb{F}$.

• $\mathbf{R}$ computes $y_i = \sum_{j=1}^{n^2} \rho_i^j r_{ij}, 1 \leq i \leq n$. Note that ρ_i^j is j^{th} power of ρ_i.

• $\mathbf{R}$ sends to $\mathbf{S}$ over $w_i, 1 \leq i \leq n$, the n^2 field elements $r_{ij}, 1 \leq j \leq n^2$. $\mathbf{R}$ also sends $\rho_i, y_i, 1 \leq i \leq n$ to $\mathbf{S}$ using $2n$ **parallel invocations of the three phase SECURE protocol (described in Theorem 5)** as there are total $2n$ elements to send. Hence **Phase I, II** and **Phase III** are used to do $2n$ parallel executions of **SECURE** protocol.

Phase IV ($\mathbf{S}$ to $\mathbf{R}$)

• Let $\mathbf{S}$ receives $r'_{ij}, 1 \leq j \leq n^2$ along $w_i, 1 \leq i \leq n$. $\mathbf{S}$ adds w_i to a list $L_{erasure}$, if $\mathbf{S}$ does not receive any information over w_i.

• Let $\mathbf{S}$ receives ρ'_i and $y'_i, 1 \leq i \leq n$ after the $2n$ parallel executions of the three phase **SECURE** protocol initiated by $\mathbf{R}$. For each i, such that $w_i \notin L_{erasure}$, $\mathbf{S}$ verifies whether $y'_i \stackrel{?}{=} \sum_{j=1}^{n^2} \rho_i'^j r'_{ij}$. If false, then $\mathbf{S}$ adds the wire w_i to the set of faulty wires, denoted by L_{faulty}. $\mathbf{S}$ sets $L_{honest} = \mathcal{W} \setminus (L_{faulty} \cup L_{erasure})$. If $t_p \geq t_b$, then $\mathbf{S}$ computes a random pad $Z = (z_1, z_2, \ldots, z_{n^2})$ of size n^2 field elements as follows:

$$Z = EXTRAND_{n^2|L_{honest}|,n^2}(r'_{ij}|w_i \in L_{honest})$$

However, if $t_b > t_p$, $\mathbf{S}$ computes a random pad Z of length $(t_b - t_p)n^2$ from $n^2|L_{honest}|$ elements using the above method.

• $\mathbf{S}$ computes $d = \mathbf{M} \oplus Z$. If $t_p \geq t_b$ then d is of size n^2, so $\mathbf{S}$ broadcasts d to $\mathbf{R}$. On the other hand, if if $t_b > t_p$ then d consists of $(t_b - t_p)n^2$ field elements and $\mathbf{S}$ reliably sends d to $\mathbf{R}$ by invoking $\frac{(t_b - t_p)}{t_b} * n$ parallel executions of single phase **PPRMT_Single_Phase** protocol (This is possible because n is at least $2t_b + t_o + t_f + 1$, which is necessary and sufficient for single phase PPRMT. Since **PPRMT_Single_Phase** protocol reliably sends nt_b field elements, d consisting of $(t_b - t_p)n^2$ field elements can be communicated by $\mathbf{S}$ by invoking the single phase PPRMT protocol $\frac{(t_b - t_p)}{t_b} * n$ times). $\mathbf{S}$ also broadcasts the set L_{faulty} and $L_{erasure}$ to $\mathbf{R}$.

Message recovery by R.

• $\mathbf{R}$ correctly receives L_{faulty} and $L_{erasure}$ and sets $L_{honest} = \mathcal{W} \setminus (L_{faulty} \cup L_{erasure})$. $\mathbf{R}$ receives d with certainty (probability one) when $t_p \geq t_b$ and with high probability when $t_b > t_p$. If $t_b \leq t_p$, then $\mathbf{R}$ computes $Z^{\mathbf{R}} = (z_1, z_2, \ldots, z_{n^2})$ of size n^2 field elements as follows:

$$Z^{\mathbf{R}} = EXTRAND_{n^2|L_{honest}|,n^2}(r_{ij}|w_i \in L_{honest})$$

If $t_b > t_p$, then $\mathbf{R}$ computes $Z^{\mathbf{R}}$ of length $(t_b - t_p)n^2$ using the above method and recovers $\mathbf{M}$ by computing $\mathbf{M} = Z^{\mathbf{R}} \oplus d$.

Proof: In **PPSMT_Mixed**, ρ_i's are sent using n parallel execution of the three phase **SECURE** protocol. From Theorem 5, the error probability of a single execution of **SECURE** protocol is bounded by $\frac{1}{|\mathbb{F}|}$. Hence the total error probability of n parallel executions of **SECURE** to communicate ρ_i, $1 \leq i \leq n$, is bounded by $\frac{n}{|\mathbb{F}|}$. If $|\mathbb{F}| \geq \frac{4n}{\delta}$, then the total error probability of n parallel executions of **SECURE** is bounded by $\frac{\delta}{4}$. Since, $|\mathbb{F}| \geq \frac{4n^4(t_b - t_p)}{\delta t_b} > \frac{4n}{\delta}$, the claim holds. □

Claim 5. *In* **PPSMT_Mixed**, *for all* $1 \leq i \leq n$, $y'_i = y_i$ *with probability* $\geq (1 - \frac{\delta}{4})$.

Proof: Similar to the proof of the above claim. □

Claim 6. *In* **PPSMT_Mixed**, *if wire* w_i *is corrupted (i.e., at least one of the value* $r_{ij}, 1 \leq j \leq n^2$ *is changed by the adversary) and for all* i, $\rho'_i = \rho_i$ *then* $w_i \in L_{fault}$ *with probability* $\geq (1 - \frac{\delta}{4})$.

Proof: From the security argument of **SECURE** protocol, the adversary gains no information about ρ_i, y_i for all $1 \leq i \leq n$. Assume that adversary has changed the n^2 tuple over some wire w_i and it is not marked as faulty by **S**. This implies that $y_i = \sum_{j=1}^{n^2} \rho_i^j r_{ij} = \sum_{j=1}^{n^2} \rho_i^j r'_{ij} = y'_i$. As inferred by the expression, y_i and y'_i are the y-values (evaluated at $x = \rho_i$) of the polynomials of degree n^2 constructed using r_{ij}, $1 \leq j \leq n^2$ and r'_{ij}, $1 \leq j \leq n^2$ as coefficients. Since the polynomials are of degree n^2, there are at most n^2 points of intersection between the two. The point ρ_i is chosen uniformly by **R** in $\mathbb{F}$. Thus, with probability at most $\frac{n^2}{|\mathbb{F}|}$, the protocol fails to detect the faulty wire. In order to bound this error probability by $\frac{\delta}{4}$, we require $|\mathbb{F}|$ to be at least $\frac{4n^2}{\delta}$. Since, $|\mathbb{F}| \geq \frac{4n^4(t_b - t_p)}{\delta t_b} > \frac{4n^2}{\delta}$, the claim holds. □

Claim 7. *In* **PPSMT_Mixed**, *the single phase PPRMT protocol* **PPRMT_Single_Phase** *which is executed parallely* $\frac{n(t_b - t_p)}{t_b}$ *times to reliably send* d, *fails with probability of at most* $\frac{\delta}{4}$.

Proof: In **PPSMT_Mixed**, d is sent during **Phase IV** using $\frac{n(t_b - t_p)}{t_b}$ parallel executions of **PPRMT_Single_Phase** protocol. If δ' is the failure probability of a single execution of **PPRMT_Single_Phase**, the total failure probability to send d is bounded by $\frac{n(t_b - t_p)\delta'}{t_b}$. To obtain $\frac{n(t_b - t_p)\delta'}{t_b} \leq \frac{\delta}{4}$, we require $\delta' \leq \frac{\delta t_b}{4n(t_b - t_p)}$. Now from Theorem 4, if $|\mathbb{F}| = \frac{n^3}{\delta'}$ then the error probability of **PPRMT_Single_Phase** is bounded by δ'. So to bound the error probability of **PPRMT_Single_Phase** by $\delta' \leq \frac{\delta t_b}{4n(t_b - t_p)}$, we require $|\mathbb{F}| \geq \frac{4n^4(t_b - t_p)}{\delta t_b}$ which is true in this case. Hence the claim follows. □

Thus Theorem 7 is true if $t_b > t_p$ and $|\mathbb{F}| \geq \frac{4n^4(t_b - t_p)}{\delta t_b}$. If $t_p \geq t_b$, then **PPSMT_Mixed** will have an error probability of δ if the error probability of each of first three events mentioned in Theorem 7 is bounded by $\frac{\delta}{3}$. This is because 4^{th} event does not occur, as d is broadcast in this case during **Phase IV**, instead of sending by single phase PPRMT. It is easy to check that by setting $|\mathbb{F}| \geq \frac{3n^2}{\delta}$, the theorem holds for $t_b \leq t_p$. □

Note: *From Theorem 7, the field size should be either* $\frac{3n^2}{\delta}$ *or* $\frac{4n^4(t_b - t_p)}{\delta t_b}$. *However, in* **PPSMT_Mixed**, *during* **Phase I**, **R** *needs to select at least* n^3 *random field elements from* $\mathbb{F}$. *So depending upon* δ, *we will set the field size as* $max(n^3, \frac{3n^2}{\delta})$. *Setting field size like this will not affect the working of the protocol.*

Theorem 8. *In* **PPSMT_Mixed**, *the adversary learns no information about the transmitted message* **M**.

Proof: The proof is divided into the following two cases:

1. **Case I: If** $t_p \geq t_b$: In this case, $n = t_b + t_p + t_o + t_f + 1$. In the worst case, the adversary can passively listen the contents over $t_b + t_o + t_p$ wires and block t_f wires. So there will be only one honest wire w_i and hence the adversary will have no information about the n^2 random elements sent over w_i. In this case, **S** generates a random pad of length n^2 and sends **M** containing n^2 field elements, using this pad. The proof follows from the correctness of EXTRAND algorithm.
2. **Case II: If** $t_b > t_p$: In this case, $n = 2t_b + t_o + t_f + 1$. In the worst case, the adversary can passively listen the contents of at most $t_b + t_p + t_o$ wires and block t_f wires. So there are at least $(t_b - t_p)$ honest wires and hence the adversary will have no information about the n^2 random elements sent over these honest wires. In this case, **S** generates a random pad of length $(t_b - t_p)n^2$ and sends **M** containing $(t_b - t_p)n^2$ field elements, using this pad. The proof now follows from the correctness of EXTRAND algorithm. □

Theorem 9. *The communication complexity of* **PPSMT_Mixed** *is* $O(n^3)$.

Proof: During **Phase I**, **R** sends n^2 random field elements over each of the n wires causing a communication complexity of $O(n^3)$. **R** also invokes $2n$ parallel executions of **SECURE** protocol with communication complexity of $O(n^2)$. This incurs total communication overhead of $O(n^3)$. During **Phase IV**, **S** sends d to **R**. If $t_p \geq t_b$, then d will consist of n^2 field elements and hence broadcasting it to **R** incurs a communication complexity of $O(n^3)$. On the other hand, if $t_b > t_p$, d consist of $(t_b - t_p)n^2$ field elements. In this case, **S** will send d by invoking $\frac{(t_b - t_p)}{t_b} * n$ parallel executions of single phase PPRMT protocol. Since, each execution of the single phase PPRMT protocol has a communication complexity of $O(n^2)$, total communication complexity is $O\left(\frac{(t_b - t_p) * n^3}{t_b}\right)$, which is $O(n^3)$. Thus, overall communication complexity of **PPSMT_Mixed** is $O(n^3)$. □

Finally to comment on the communication complexity of **PPSMT_Mixed** in terms of bits, we state the following: **PPSMT_Mixed** sends $(t_b - t_p)n^2 \log |\mathbb{F}|$ (if $t_b > t_p$) or $n^2 \log |\mathbb{F}|$ bits (if $t_b \leq t_p$) by communicating $O(n^3 \log |\mathbb{F}|)$ bits, where $|\mathbb{F}|$ is either $\frac{4n^4(t_b - t_p)}{\delta t_b}$ or $\frac{3n^2}{\delta}$ respectively. From Theorem 6, if $t_b \geq t_p$ (n will $2t_b + t_o + t_f + 1$), then any four phase PPSMT protocol needs to communicate $\Omega(n^3 \log |\mathbb{F}|)$ bits to securely send $(t_b - t_p)n^2 \log |\mathbb{F}|$ bits. Similarly, if $t_p \geq t_b$ (n will be $t_b + t_p + t_o + t_f + 1$), then any four phase PPSMT protocol need to communicate $\Omega(n^3 \log |\mathbb{F}|)$ bits in order to securely send $n^2 \log |\mathbb{F}|$ bits. Since total communication complexity of **PPSMT_Mixed** in both cases is $O(n^3 \log |\mathbb{F}|)$ bits, our protocol is **bit optimal**.

Significance of the Protocol: *In [7], the authors have designed a PSMT protocol achieving optimum communication complexity in* $O(log(t_o + t_f))$ *phases. Our PPSMT protocol achieves optimum communication complexity in* **four phases**,

which shows the power of randomization. However, our protocol does not sacrifice security in any sense for gaining **optimality**.

Achieving Probabilistic Reliability and Perfect Security with Constant Overhead in Four Phases: In [13], the lower bound on the communication complexity of any multiphase PSMT protocol has been proved to be $\Omega\left(\frac{n\ell}{n-2t_b}\right)$ in the presence of Byzantine adversary. Hence, communicating any message *secretly* with *constant* overhead is *impossible* by *any* PSMT protocol. However protocol **PPSMT_Mixed** achieves this bound. In **PPSMT_Mixed**, if $t_o = t_p = t_f = 0$, then it sends $t_b n^2 = O(n^3)$ field elements in four phases by communicating $O(n^3)$ field elements (when $t_o = t_f = t_p = 0$, $n = 2t_b + 1$ and so $t_b = O(n)$). Thus we get *secrecy* with *constant* overhead in four phases when **PPSMT_Mixed** is executed considering *only* Byzantine adversary. Like **PPRMT_Single_Phase**, **PPSMT_Mixed** is also a *special* kind of a PPSMT protocol in that **R** actually *knows* if the protocol outputs the correct message or not.

4 Conclusion

We have studied the problem of PPRMT and PPSMT in the presence of mixed adversary. The paper shows considerably strong effect of randomization in the *possibility*, *feasibility* and *optimality* of reliable and secure message transmission protocols. We summarize our results in Table 1 and Table 2.

Table 1. Connectivity Requirement for the Existence of Protocol

Model	Single Phase	Multiple Phase
PRMT(Mixed Adversary)	$n \geq 2t_b + t_o + t_f + 1$ [7]	$n \geq 2t_b + t_o + t_f + 1$ [7]
PPRMT(Mixed Adversary)	$n \geq 2t_b + t_o + t_f + 1$, Theorem 2	$n \geq 2t_b + t_o + t_f + 1$, Theorem 2
PSMT(Mixed Adversary)	$n \geq 3t_b + 2t_o + 2t_f + t_p + 1$ [11]	$n \geq 2t_b + t_o + t_f + t_p + 1$ [7]
PPSMT(Mixed Adversary)	$n \geq 2t_b + 2t_o + t_f + t_p + 1$ [8]	$n \geq t_b + \max(t_b, t_p) + t_o + t_f + 1$, Theorem 5

Table 2. Protocols with Optimum Communication Complexity. ℓ is the message size.

Model	Communication Complexity	Number of Phases	Remarks
PRMT (Byzantine Adversary)	$O(\ell)$	3	$\ell = n^2$ [9].
PPRMT (Byzantine Adversary)	$O(\ell)$	1	$\ell = O(n^2)$ (Protocol **PPRMT_Single_Phase** given in this paper by substituting $t_o = t_f = 0$).
PSMT (Byzantine Adversary)	$O\left(\frac{n\ell}{n-3t_b}\right)$	1	$\ell = O(n)$ [11].
	$O\left(\frac{n\ell}{n-2t_b}\right)$	2	Exponential computation [1].
	$O\left(\frac{n\ell}{n-2t_b}\right)$	3	Polynomial computation [9].
PPSMT (Byzantine Adversary)	$O\left(\frac{n\ell}{n-t_b}\right)$	1	$\ell = O(n)$ [8].
	$O(\ell)$	4	$\ell = O(n^3)$ (by substituting $t_o = t_f = t_p = 0$ in **PPSMT_Mixed**)
PSMT (Mixed Adversary)	$O\left(\frac{n\ell}{n-(2t_b+t_o+t_f+t_p)}\right)$	$O(\log(t_o + t_f))$	$\ell = n \log(t_o + t_f)$ [7]
PPSMT (Mixed Adversary)	$O\left(\frac{n\ell}{n-(t_b+t_o+t_f+t_p)}\right)$	4	$\ell = n^2$ or $\ell = (t_b - t_p)n^2$ Protocol **PPSMT_Mixed** given in this paper

References

1. Agarwal, S., Cramer, R., de Haan, R.: Asymptotically optimal two-round perfectly secure message transmission. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 394–408. Springer, Heidelberg (2006)
2. Cover, T.H., Thomas, J.A.: Elements of Information Theory. John Wiley & Sons, Chichester (2004)
3. Dolev, D., Dwork, C., Waarts, O., Yung, M.: Perfectly secure message transmission. JACM 40(1), 17–47 (1993)
4. Franklin, M., Wright, R.N.: Secure communication in minimal connectivity models. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 346–360. Springer, Heidelberg (1998)
5. Kurosawa, K., Suzuki, K.: Almost secure (1-round, n-channel) message transmission scheme. Cryptology ePrint Archive, Report 2007/076 (2007), `http://eprint.iacr.org/`
6. Menger, K.: Zur allgemeinen kurventheorie. Fundamenta Mathematicae 10, 96–115 (1927)
7. Patra, A., Choudhary, A., Srinathan, K., Rangan, P.C.: Bit optimal protocols for perfectly reliable and secure message transmission in the presence of mixed adversary. Manuscript
8. Patra, A., Choudhary, A., Srinathan, K., Rangan, P.C.: Does randomization helps in reliable and secure communication. Manuscript
9. Patra, A., Choudhary, A., Srinathan, K., Rangan, C.P.: Constant phase bit optimal protocols for perfectly reliable and secure message transmission. In: Barua, R., Lange, T. (eds.) INDOCRYPT 2006. LNCS, vol. 4329, pp. 221–235. Springer, Heidelberg (2006)
10. Rabin, T., Ben-Or, M.: Verifiable secret sharing and multiparty protocols with honest majority. In: Proc. of twenty-first annual ACM symposium on Theory of computing, pp. 73–85. ACM Press, New York (1989)
11. Srinathan, K.: Secure Distributed Communication. PhD thesis, Indian Institute of Technology Madras (2006)
12. Srinathan, K., Narayanan, A., Rangan, C.P.: Optimal perfectly secure message transmission. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 545–561. Springer, Heidelberg (2004)
13. Srinathan, K., Prasad, N.R., Rangan, C.P.: On the optimal communication complexity of multiphase protocols for perfect communication. In: IEEE Symposium on Security and Privacy, pp. 311–320 (2007)
14. Wang, Y., Desmedt, Y.: Secure communication in multicast channels: The answer to Franklin and Wright's question. Journal of Cryptology 14(2), 121–135 (2001)