On the Communication Complexity of Reliable and Secure Message Transmission in Asynchronous Networks

Ashish Choudhury⋆[1] and Arpita Patra[2]

[1] Department of Computer Science
University of Bristol
Ashish.Choudhary@bristol.ac.uk, partho31@gmail.com
[2] Department of Computer Science
ETH Zuruch
arpitapatra10@gmail.com, arpita.patra@inf.ethhz.ch

Abstract. In this paper, we study the communication complexity of *Reliable Message Transmission* (RMT) and *Secure Message Transmission* (SMT) protocols in *asynchronous* settings. We consider two variants of the problem, namely *perfect* (where no error is allowed in the protocol outcome) and statistical (where the protocol may output a wrong outcome with negligible probability). RMT and SMT protocols have been investigated rigorously in synchronous settings. But not too much attention has been paid to the asynchronous version of the problem. In a significant work, Choudhury et al. (ICDCN 2009 and JPDC 2011) have studied the network connectivity requirement for asynchronous perfect and statistical SMT protocols. Their investigation reveals the following two important facts:

1. *perfect* SMT protocols require *more* network connectivity in asynchronous network than synchronous network.
2. Connectivity requirement of *statistical* SMT protocols is *same* for both synchronous and asynchronous network.

Unfortunately, nothing is known about the communication complexity of RMT and SMT protocols in asynchronous settings. In this paper, we derive tight bounds on the communication complexity of the above problems and compare our results with the existing bounds for synchronous protocols. The interesting conclusions derived from our results are:

1. **RMT:** Asynchrony *increases* the communication complexity of *perfect* RMT protocols. However, asynchrony has *no impact* on the communication complexity of *statistical* RMT protocols.
2. **SMT:** Communication complexity of SMT protocols is *more* in asynchronous network, for *both* perfect as well as statistical case.

⋆ Part of this work was done when the author was working at Center of Excellence in Cryptology, Indian Statistical Institute Kolkata India. The work in this paper was partially supported by EPSRC via grant EP/I03126X/1, and by the European Commission through the ICT Programme under Contract ICT2007216676 ECRYPT II.

1 Introduction

Reliable Message Transmission (RMT) and *Secure Message Transmission* (SMT) [4] are fundamental problems in secure distributed computing as well as in cryptography. In the problem of RMT, there are n disjoint channels (also called as *wires*) between a sender $\mathbf{S}$ and a receiver $\mathbf{R}$. $\mathbf{S}$ and $\mathbf{R}$ shares no information in advance. There is a *computationally unbounded active* adversary, denoted as $\mathcal{A}_t$, who can listen and forge the communication over t out of the n wires, where $t < n$. $\mathbf{S}$ has a message $m^{\mathbf{S}}$, which is a sequence of ℓ elements, chosen from a finite field $\mathbb{F}$, where $\ell \geq 1$ and $|\mathbb{F}| > n$. The challenge is to design a protocol, such that at the end of the protocol, $\mathbf{R}$ correctly outputs $m^{\mathbf{R}} = m^{\mathbf{S}}$. Now there are two flavors of RMT:

1. Perfect RMT (**PRMT**): Here $m^{\mathbf{R}} = m^{\mathbf{S}}$, without any error.
2. Statistical RMT (**SRMT**): Here $m^{\mathbf{R}} = m^{\mathbf{S}}$ with probability at least $1 - \delta$, where $0 < \delta < 1/2$ and is called the error probability.

Notice that there is no issue of privacy in RMT protocols; i.e., the adversary can also know $m^{\mathbf{S}}$ during the protocol execution. If we add the issue of privacy to RMT protocols, then we arrive at the notion of SMT protocols. In SMT protocols, we require that not only $\mathbf{R}$ outputs $m^{\mathbf{R}} = m^{\mathbf{S}}$, but also $\mathcal{A}_t$ should not learn any information about $m^{\mathbf{S}}$ in *information theoretic* sense. We can have two types of SMT protocols:

1. Perfect SMT (**PSMT**): Here $m^{\mathbf{R}} = m^{\mathbf{S}}$, without any error.
2. Statistical SMT (**SSMT**): Here $m^{\mathbf{R}} = m^{\mathbf{S}}$ with probability at least $1 - \delta$, where $0 < \delta < 1/2$ and is called error probability. However, there is no compromise in the privacy which should be error free and information theoretic.

RMT and SMT problem were first formulated by Dolev et al. [4]. Any RMT or SMT protocol has the following important parameters:

1. *Connectivity*: It is the total number of wires n (expressed as a function of t) required in the protocol. We consider following two types of wires:
   (a) *Uni-directional wires*: where all the n wires are uni-directional, directed from $\mathbf{S}$ to $\mathbf{R}$, allowing only one way communication (i.e., no interaction) from $\mathbf{S}$ to $\mathbf{R}$;
   (b) *Bi-directional wires*: where all the n wires are bi-directional, allowing bi-directional communication (i.e., interaction) between $\mathbf{S}$ and $\mathbf{R}$.
2. *Communication Complexity*: It is the number of field elements communicated by $\mathbf{S}$ and $\mathbf{R}$ (expressed as a function of n, ℓ) in the protocol.

RMT and SMT problem have been studied rigorously by several researchers (see for example [11, 13, 1, 5, 7, 9, 3]) and tight bounds have been established on connectivity and communication complexity of PRMT, SRMT, PSMT and SSMT protocols. These bounds are summarized in Table 1.

Table 1. Existing bounds for RMT and SMT protocols

Type of Protocol	Type of Channels	n	Bound on the Communication Complexity
PRMT	Uni-directional	$n \geq 2t+1$ [4]	$\Theta\left(\frac{n\ell}{n-2t}\right)$ [13, 15]
PRMT	Bi-directional	$n \geq 2t+1$ [4]	$\Theta(\ell)$ [15, 8]
SRMT	Uni-directional	$n \geq 2t+1$ [6]	$\Theta(\ell)$ [9]
SRMT	Bi-directional	$n \geq 2t+1$ [6]	$\Theta(\ell)$ [9]
PSMT	Uni-directional	$n \geq 3t+1$ [4]	$\Theta\left(\frac{n\ell}{n-3t}\right)$ [5]
PSMT	Bi-directional	$n \geq 2t+1$ [4]	$\Theta\left(\frac{n\ell}{n-2t}\right)$ [13, 15, 8, 7]
SSMT	Uni-directional	$n \geq 2t+1$ [6]	$\Theta\left(\frac{n\ell}{n-2t}\right)$ [9]
SSMT	Bi-directional	$n \geq 2t+1$ [6]	$\Theta(\ell)$ [9]

Remark 1. (**Note on the Communication Complexity of SRMT and SSMT Protocols**) In any SRMT/SSMT, the field size $|\mathbb{F}|$ is selected as a function of the error probability δ. So though δ is not figuring out explicitly in the communication complexity expressions of SRMT/SSMT protocols in Table 1, it is implicitly present. More specifically, each element of $\mathbb{F}$ can be represented by $\log|\mathbb{F}|$ bits, which will be a function of δ. So if we consider the total number of bits communicated during any SRMT/SSMT protocol, δ will be present in the communication complexity expression. This point will be made more clear, when we discuss our protocols. □

Motivation of Our Work. The results given in Table 1 assume that the underlying network is *synchronous*, where there is a global clock and the transmission delay over each wire is bounded by an upper bound. Though theoretically interesting, this does not model the real life scenario (like the Internet) appropriately, as the delay in the transmission of even a single message will affect the overall properties of the protocol. In a typical large network like the Internet, every message can have arbitrary delay and this can be modeled more appropriately by *asynchronous* networks, where no timing assumptions are made. Unfortunately, unlike synchronous networks, not much attention has been paid to RMT and SMT protocols in asynchronous settings. In this paper, we improve this situation by deriving tight bounds on the communication complexity of asynchronous RMT and SMT protocols.

Asynchronous Network Model. In an asynchronous network, every wire can have *arbitrary*, yet finite delay. That is, the messages are assumed to be delivered *eventually.* To model the worst case scenario, it is assumed that $\mathcal{A}_t$ can schedule the messages over each wire and hence can control the transmission delay over each wire. *However, note that $\mathcal{A}_t$ can only schedule the messages sent over an honest wire, without having any access to them.* The inherent difficulty that arises in designing a protocol in asynchronous settings is that we cannot distinguish between a *slow wire* and a *corrupted wire*. That is, if in the protocol, some information is supposed to arrive over a wire and if no information arrives, then it cannot be distinguished whether the wire is honest and the information is simply delayed (due to the malicious scheduling by $\mathcal{A}_t$) or whether $\mathcal{A}_t$ has simply blocked the transmission over the wire by taking its control. Due to this, neither **S** nor **R** can afford to wait for all the n wires to transmit their information, as waiting for all of them may turn out to be endless. So they have to start the computation, as soon as they receive information over at least $n - t$ wires and they may have to ignore the transmission over t (potentially honest) wires. Due to this limitation, the techniques from the synchronous world cannot be adapted straight forwardly to the asynchronous settings.

We call the asynchronous PRMT, SRMT, PSMT and SSMT protocols as APRMT, ASRMT, APSMT and ASSMT respectively. Now in addition to the reliability and secrecy condition (as in the synchronous protocols), these asynchronous protocols also have to explicitly satisfy **termination** condition, according to which both **S** and **R** should eventually terminate the protocol.

Existing Results for Asynchronous Protocols. The first asynchronous SMT protocol was proposed in [10], where the authors have designed an APSMT protocol with $n = 2t + 1$ uni-directional wires from **S** to **R**. However, in [2], Choudhury et al. have shown that the protocol of [10] is insecure. Moreover, they have also studied the connectivity requirement for APSMT and ASSMT protocols. More specifically, they have shown the following two *surprising* results:

1. Any APSMT protocol requires $n \geq 3t + 1$ wires, irrespective of whether the wires are uni-directional or bi-directional. This is quiet surprising, since we can design PSMT protocols in synchronous settings with $n \geq 2t + 1$ bi-directional wires (see sixth row of Table 1). This shows that *asynchrony affects the connectivity of PSMT protocols.*
2. Any ASSMT protocol requires $n \geq 2t + 1$ wires, irrespective of whether the wires are uni-directional or bi-directional. The same connectivity is required even for SSMT protocols (see the last two rows of Table 1). This implies *asynchrony has no affect on the connectivity of SSMT protocols.*

Our Results and their Significance. So far nothing is known about the communication complexity of APRMT, ASRMT, APSMT and ASSMT protocols. We derive tight bounds on the communication complexity of the above problems. These bounds are summarized in Table 2.

Comparing Table 1 and Table 2, we find the following surprising facts:

1. **PRMT:** *Asynchrony increases the communication complexity of PRMT protocols.* With $n = 2t + 1$ bi-directional wires, PRMT protocol can be designed with a communication complexity of $\Theta(\ell)$ (second row of Table 1), where as APRMT protocol must have a communication complexity of $\Theta(n\ell)$ (second row of Table 2).

Table 2. Our Bounds for Asynchronous RMT and SMT Protocols

Type of Protocol	Type of Channels	n	Bound on the Communication Complexity
APRMT	Uni-directional	$n \geq 2t+1$	$\Theta\left(\frac{n\ell}{n-2t}\right)$
APRMT	Bi-directional	$n \geq 2t+1$	$\Theta\left(\frac{n\ell}{n-2t}\right)$
ASRMT	Uni-directional	$n \geq 2t+1$	$\Theta(\ell)$
ASRMT	Bi-directional	$n \geq 2t+1$	$\Theta(\ell)$
APSMT	Uni-directional	$n \geq 3t+1$	$\Theta\left(\frac{n\ell}{n-3t}\right)$
APSMT	Bi-directional	$n \geq 3t+1$	$\Theta\left(\frac{n\ell}{n-3t}\right)$
ASSMT	Uni-directional	$n \geq 2t+1$	$\Theta\left(\frac{n\ell}{n-2t}\right)$
ASSMT	Bi-directional	$n \geq 2t+1$	$\Theta\left(\frac{n\ell}{n-2t}\right)$

2. **SRMT:** *Asynchrony does not affect the communication complexity of SRMT protocols.* In this case, the communication complexity is *same* for both synchronous as well as asynchronous protocols (third and fourth row of Table 1 and Table 2 respectively).
3. **PSMT:** *Asynchrony increases the communication complexity of PSMT protocols.* From [2], asynchrony increases the connectivity requirement of PSMT protocols. Our results show that the same holds even for the communication complexity (see the sixth row of Table 1 and Table 2).
4. **SSMT:** Interestingly, we find that *asynchrony even increases the communication complexity of SSMT protocols.* Specifically, for $n = 2t+1$ bi-directional wires, SSMT protocol can be designed with a communication complexity of $\Theta(\ell)$ (last row of Table 1), where as ASSMT scheme must have a communication complexity of $\Theta(n\ell)$ (last row of Table 2). However, [2] shows that asynchrony does not increase the connectivity of SSMT protocols.

The Road-map. We present our results on APRMT, ASRMT, APSMT and ASSMT in Section 2, 3, 4 and 5 respectively. We conclude the paper and discuss few open problems in Section 6.

2 Bound on the Communication Complexity of APRMT

Throughout Section 2, we assume $n \geq 2t+1$, as $n \geq 2t+1$ wires (uni-directional or bi-directional) are required for any PRMT protocol (Table 1), we require the same for APRMT protocols as well.

2.1 Bounds for Uni-Directional Wires

Theorem 1. *Any APRMT protocol, executed over n ($n \geq 2t+1$) uni-directional wires has a communication complexity of $\Omega\left(\frac{n\ell}{n-2t}\right)$.*

Proof: Easy, as the bound holds for PRMT protocols [13]. □

Theorem 2. *Let there n $(n = 2t+1)$ uni-directional wires from* $\mathbf{S}$ *to* $\mathbf{R}$*. Then there exists an APRMT protocol with communication complexity of* $\mathcal{O}(n\ell) = \mathcal{O}\left(\frac{n\ell}{n-2t}\right)$.

Proof: Consider the following protocol: To reliably send a message of size ℓ, $\mathbf{S}$ sends the message over all the n wires. $\mathbf{R}$ waits for a message received identically over $t+1$ wires and output the message. The output is correct, since at least one wire out of these $t+1$ wires is honest, which will deliver the original message. Moreover, termination is guaranteed since there are at least $t+1$ honest wires, which will eventually deliver correct message. It is easy to verify that the communication complexity is $\mathcal{O}(n\ell)$. □

2.2 Bounds for Bi-Directional Wires

Let $\mathbf{S}$ and $\mathbf{R}$ be connected by n bi-directional wires, denoted by $\mathcal{W} = \{w_1, \ldots, w_n\}$, where $n \geq 2t+1$. Then we show that any APRMT protocol has a communication complexity of $\Omega\left(\frac{n\ell}{n-2t}\right)$. For this, we prove the following:

1. We first show that the information exchanged over *any* $n-2t$ wires should completely determine the message in any APRMT protocol executed over n bi-directional wires (Lemma 1).
2. Next, we show that any APRMT protocol where the information exchanged over *any* $n-2t$ wires completely determine the message, must communicate $\Omega\left(\frac{n\ell}{n-2t}\right)$ (Lemma 2).

Lemma 1. *In any APRMT protocol executed over $n \geq 2t+1$ bi-directional wires, the information exchanged over any $n-2t$ wires completely determines the message.*

Proof: On contrary, let Π^{APRMT} be an APRMT protocol where the information exchanged over any $n-2t$ wires is independent of $m^{\mathbf{S}}$. We divide the set of n wires into *three* groups, namely G_1, G_2 and G_3. The group G_1 consists of the first $n-2t$ wires $w_1, \ldots, w_{n-2t}$, group G_2 consists of the next t wires $w_{n-2t+1}, \ldots, w_{n-t}$ and group G_3 consists of the last t wires $w_{n-t+1}, \ldots, w_n$. *Now according to our assumption, the information exchanged over the wires in group G_1 (consisting of $n-2t$ wires) in any execution of Π^{APRMT} will be independent of message.* That is, there exist a pair of messages, say $m_1^{\mathbf{S}}$ and $m_2^{\mathbf{S}}$ such that the information communicated over G_1 while sending $m_1^{\mathbf{S}}$ and respectively $m_2^{\mathbf{S}}$ are same. We define the following variables with respect to any execution E of Π^{APRMT}:

1. $time(E, \mathbf{R}, w_i)$: lists the arrival time-stamps of different messages (with respect to the local clock of $\mathbf{R}$) received by $\mathbf{R}$ along wire w_i, for $i = 1, \ldots, n$ in execution E.
2. $time(E, \mathbf{S}, w_i)$: lists the arrival time-stamps of the different messages (with respect to the local clock of $\mathbf{S}$) received by $\mathbf{S}$ along wire w_i, for $i = 1, \ldots, n$ in execution E.

3. E^{time}: denotes the total time taken (with respect to $\mathbf{R}$) by execution E; i.e., the time at which $\mathbf{R}$ terminates the protocol in execution E.

Since Π^{APRMT} is an APRMT protocol, any execution E of Π^{APRMT} must terminate. Now consider the following two possible executions of Π^{APRMT}, E_1 and E_2. Let $\mathbf{R}$ terminates E_1 (E_2) at time E_1^{time} (E_2^{time}), correctly outputting $m_1^{\mathbf{S}}$ ($m_2^{\mathbf{S}}$).

1. Execution E_1: The random coins of $\mathbf{S}$ and $\mathbf{R}$ are r_1 and r_2 respectively. $\mathbf{S}$ wants to reliably send the message $m_1^{\mathbf{S}}$. The adversary strategy is to passively listen (without modifying them) the communication over the wires in group G_2 and arbitrarily delaying the communication over the wires in group G_3, till the time $E_1^{time} + E_2^{time} + 1$. Let α and β_1 denote the messages that are exchanged between $\mathbf{S}$ and $\mathbf{R}$, along the wires in group G_1 and G_2 respectively.
2. Execution E_2: The random coins of $\mathbf{S}$ and $\mathbf{R}$ are r_3 and r_2 respectively. $\mathbf{S}$ wants to reliably send the message $m_2^{\mathbf{S}} \neq m_1^{\mathbf{S}}$. The adversary strategy is to passively listen (without modifying them) the communication over the wires in group G_2 and arbitrarily delaying the communication over the wires in group G_3, till the time $E_1^{time} + E_2^{time} + 1$. Let α and β_2 denote the messages that are exchanged between $\mathbf{S}$ and $\mathbf{R}$, along the wires in group G_1 and G_2 respectively. *Notice that α is same as in execution E_1 due to our assumption about the distribution of information over the wires in G_1 in Π^{APRMT}.*

We now show another possible execution of Π^{APRMT} and an adversary strategy, where $\mathbf{R}$ outputs an incorrect message.

3. Execution E^{Cor}: The random coins of $\mathbf{S}$ and $\mathbf{R}$ are r_1 and r_2 respectively. $\mathbf{S}$ wants to reliably send the message $m_1^{\mathbf{S}}$. Let α denote the messages exchanged over the wires in G_1. *Notice that α is same as in execution E_1 and E_2.* Now the adversary strategy in E^{Cor} is as follows: adversary delay any information along the wires in group G_3 for time $E_1^{time} + E_2^{time} + 1$. In addition, the adversary controls the wires in group G_2 in Byzantine fashion and change the communication over these wires, such that $\mathbf{R}$ gets messages corresponding to β_2 along G_2, while $\mathbf{S}$ receives messages corresponding to β_1 along G_2. Moreover, adversary schedules the messages along the wires in G_1 and G_2 in such a way that $time(E^{\text{Cor}}, \mathbf{S}, w_i) = time(E_1, \mathbf{S}, w_i)$, for every $w_i \in G_1 \cup G_2$ and $time(E^{\text{Cor}}, \mathbf{R}, w_i) = time(E_2, \mathbf{R}, w_i)$, for every $w_i \in G_1 \cup G_2$. Thus the view of $\mathbf{S}$ is $\alpha\ \beta_1$, while view of $\mathbf{R}$ is $\alpha\ \beta_2$.

Thus the view of $\mathbf{S}$ in E_1 and E^{Cor} are same, so $\mathbf{S}$ will assume that $m_1^{\mathbf{S}}$ has been communicated reliably. However, the view of $\mathbf{R}$ in E^{Cor} is same as in E_2 and hence $\mathbf{R}$ will output $m_2^{\mathbf{S}}$. But this violates the perfect reliability property of Π^{APRMT}, which is a contradiction. Hence Π^{APRMT} does not exist. □

Lemma 2. *Any APRMT protocol tolerating $\mathcal{A}_t$ executed over n ($n \geq 2t+1$) bi-directional wires, in which the information exchanged over any $n-2t$ wires completely determine the message, has a communication complexity of $\Omega\left(\frac{n\ell}{n-2t}\right)$.*

Proof: Let Π^{APRMT} be an APRMT protocol, executed over n bi-directional wires (where $n \geq 2t+1$), to reliably send a message of size ℓ, such that the information exchanged over *any* $n-2t$ wires completely determine the message. We now define the following notations:

1. $\mathcal{M}$ denotes the message space from where $\mathbf{S}$ selects the message to be sent. So $\mathcal{M} = \mathbb{F}^{\ell}$.
2. $\mathbf{T}_i^m$ denotes the set of all possible transmissions that can occur on wire $w_i \in \{w_1, \ldots, w_n\}$, when $\mathbf{S}$ transmits message $m \in \mathcal{M}$ using Π^{APRMT}.
3. For $j \geq i$, $\mathbf{M}_{i,j}^m \subseteq \mathbf{T}_i^m \times \mathbf{T}_{i+1}^m \times \ldots \times \mathbf{T}_j^m$ denotes the set of all possible transmissions that can occur over the wires $\{w_i, w_{i+1}, \ldots, w_j\}$, when $\mathbf{S}$ transmits message $m \in \mathcal{M}$ using protocol Π^{APRMT}.
4. $\mathbf{M}_{i,j} = \bigcup_{m \in \mathcal{M}} \mathbf{M}_{i,j}^m$ and $\mathbf{T}_i = \bigcup_{m \in \mathcal{M}} \mathbf{T}_i^m$. We call $\mathbf{T}_i$ as the *capacity* of wire w_i and $\mathbf{M}_{i,j}$ as the *capacity* of the set of wires $\{w_i, w_{i+1}, \ldots, w_j\}$.

In protocol Π^{APRMT}, one element from the set $\mathbf{T}_i$ is transmitted over each wire w_i, for $i = 1, \ldots, n$. Moreover, each element of the set $\mathbf{T}_i$ can be represented by $\log |\mathbf{T}_i|$ bits. Thus, the lower bound on the communication complexity of Π^{APRMT} is $\Sigma_{i=1}^n \log |\mathbf{T}_i|$ bits. In the sequel, we try to estimate $\mathbf{T}_i$.

Since the transmission over any set of $n-2t$ wires in Π^{APRMT} completely determines the message, it must hold that $|\mathbf{M}_{2t+1,n}| \geq |\mathcal{M}|$.
Though the above relation must hold for any set of $n-2t$ wires, for simplicity, we have focussed specifically on the last $n-2t$ wires. From the definition of $\mathbf{T}_i$ and $\mathbf{M}_{i,j}$, we get

$$\prod_{i=2t+1}^{n} |\mathbf{T}_i| \geq |\mathbf{M}_{2t+1,n}| \geq |\mathcal{M}|.$$

Let $g = n - 2t$. The above inequality holds for any selection of g wires $\mathcal{D} \subset \{w_1, \ldots, w_n\}$, where $|\mathcal{D}| = g$; i.e., $\prod_{w_i \in \mathcal{D}} |\mathbf{T}_i| \geq |\mathcal{M}|$. In particular, it holds for every selection $\mathcal{D}_k = \{w_{kg+1 \bmod n}, w_{kg+2 \bmod n}, \ldots, w_{kg+g \bmod n}\}$, with $k \in \{0, \ldots, n-1\}$. If we consider all the $\mathcal{D}_k$ sets collectively, then each wire is counted exactly g times in the collection. Thus, the product of the capacities of all $\mathcal{D}_k$ yields the capacity of the full wire set to the g^{th} power and also since each $\mathcal{D}_k$ has capacity at least $|\mathcal{M}|$, we get

$$\prod_{k=0}^{n-1} \prod_{w_j \in \mathcal{D}_k} |\mathbf{T}_j| = \left(\prod_{i=1}^{n} |\mathbf{T}_i| \right)^g, \text{ and } |\mathcal{M}|^n \leq \prod_{k=0}^{n-1} \prod_{w_j \in \mathcal{D}_k} |\mathbf{T}_j|$$

and therefore

$$n \log(|\mathcal{M}|) \leq g \sum_{i=1}^{n} \log(|\mathbf{T}_i|).$$

As $\log(|\mathcal{M}|) = \ell \log(|\mathbb{F}|)$, from the above inequality, we get

$$\sum_{i=1}^{n} \log(|\mathbf{T}_i|) \geq \left(\frac{n\ell \log(|\mathbb{F}|)}{g} \right) \geq \left(\frac{n\ell \log(|\mathbb{F}|)}{n-2t} \right).$$

As mentioned earlier, $\sum_{i=1}^{n} \log(|\mathbf{T}_i|)$ denotes the lower bound on the communication complexity in bits. From the above inequality, we find that the lower bound is $\left(\frac{n\ell \log(|\mathbb{F}|)}{n-2t}\right)$ bits. Now each field element can be represented by $\log(|\mathbb{F}|)$ bits. Thus the lower bound is $\left(\frac{n\ell}{n-2t}\right)$ field elements. □

From the previous two lemmas, we get the following theorem.

Theorem 3. *Any APRMT protocol executed over n ($n \geq 2t+1$) bi-directional wires has a communication complexity of $\Omega\left(\frac{n\ell}{n-2t}\right)$.*

Any protocol executed over n uni-directional wires can also be executed over n bi-directional wires. From Theorem 2, there exists an APRMT protocol which can be executed over $n = 2t+1$ wires and requires a communication complexity of $\mathcal{O}\left(\frac{n\ell}{n-2t}\right)$. Thus the bound in Theorem 3 is tight.

3 Bounds on the Communication Complexity of ASRMT

Throughout Section 3, we assume $n \geq 2t+1$. These many wires wires (uni-directional or bi-directional) are required for any SRMT protocol (Table 1). So it will also be required for ASRMT protocols.

3.1 Bounds for Uni-Directional Wires

Theorem 4. *Any ASRMT protocol executed over the n ($n \geq 2t+1$) uni-directional wires has a communication complexity of $\Omega(\ell)$.*

Proof: Easy, as any ASRMT protocol has to at least send the message. □

We now show that the bound in Theorem 4 is *asymptotically tight*. That is, suppose there exists $n = 2t+1$ uni-directional wires from $\mathbf{S}$ to $\mathbf{R}$ and consider a finite field $\mathbb{F}$, where $|\mathbb{F}| = \frac{t^2}{\delta}$. Then we design an ASRMT protocol tolerating $\mathcal{A}_t$ called ASRMT-Uni-Directional, which reliably sends a message $m^{\mathbf{S}}$ of size $(t+1)^2 = \Theta(n^2)$ field elements and has a total communication complexity of $\mathcal{O}(n^2)$. The protocol has an error probability of δ. The high level idea of the protocol is as follows: let the n wires be denoted by $\mathcal{W} = \{w_1, \ldots, w_n\}$ and let $m^{\mathbf{S}} = \{m^{\mathbf{S}}_{i,j} : i, j = 0, \ldots, t\}$, consisting of $(t+1)^2$ elements of $\mathbb{F}$. $\mathbf{S}$ selects a bi-variate polynomial $Q^{\mathbf{S}}(x,y)$ of degree-t in x and y, whose $(t+1)^2$ coefficients are elements of $m^{\mathbf{S}}$. Now $Q^{\mathbf{S}}(x,y)$ is evaluated at $y = 1, \ldots, n$ to obtain the uni-variate polynomials $f^{\mathbf{S}}_i(x) = Q^{\mathbf{S}}(x,i)$ and $f^{\mathbf{S}}_i(x)$ is sent over wire w_i (by sending its coefficients). To recover $m^{\mathbf{S}}$, $\mathbf{R}$ should correctly recover $Q^{\mathbf{S}}(x,y)$ which requires $\mathbf{R}$ to know $t+1$ correct $f^{\mathbf{S}}_i(x)$'s. In order to facilitate $\mathbf{R}$ to identify the correct $f^{\mathbf{S}}_i(x)$'s, $\mathbf{S}$ authenticates each $f^{\mathbf{S}}_i(x)$ using n different secret authentication keys and sends the authentication information and authentication key across the n wires. Now at the receiving end, $\mathbf{R}$ will consider an $f^{\mathbf{S}}_i(x)$ as *valid* only if it passes the authentication test with respect to the keys of $t+1$ wires. Since at least one of these $t+1$ wires is honest and the adversary will have no information about the authentication keys delivered over an honest wire, with very high probability a polynomial considered as valid by $\mathbf{R}$ will be indeed a correct polynomial. Moreover, there are at least $t+1$ honest wires, who will eventually deliver $t+1$ correct $f^{\mathbf{S}}_i(x)$'s. The complete details are in Fig. 1.

Fig. 1. Protocol ASRMT-Uni-Directional with $n = 2t + 1$ unidirectional wires

Computation and Communication by $\mathbf{S}$:

1. Corresponding to the message $m^{\mathbf{S}} = \{m^{\mathbf{S}}_{i,j} : i, j = 0, \ldots, t\}$, $\mathbf{S}$ forms the bivariate polynomial $Q^{\mathbf{S}}(x, y) = \sum_{i=0,j=0}^{\substack{i=t\\j=t}} m^{\mathbf{S}}_{i,j} x^i y^j$.
2. For $i = 1, \ldots, n$, $\mathbf{S}$ computes $f^{\mathbf{S}}_i(x) = Q^{\mathbf{S}}(x, i)$ and the *authentication values* $Auth^{\mathbf{S}}_{ij} = f^{\mathbf{S}}_i(Key^{\mathbf{S}}_{ij})$, corresponding to random *authentication keys* $Key^{\mathbf{S}}_{ij}$, for $j = 1, \ldots, n$.
3. For $i = 1, \ldots, n$, $\mathbf{S}$ sends the following to $\mathbf{R}$ over wire w_i and terminates:
   (a) The degree-t polynomial $f^{\mathbf{S}}_i(x)$;
   (b) n authentication keys $Key^{\mathbf{S}}_{ji}$, for $j = 1, \ldots, n$;
   (c) n authentication values $Auth^{\mathbf{S}}_{ji}$, for $j = 1, \ldots, n$.

Message Recovery by $\mathbf{R}$:

For $r = 0, \ldots, t$, $\mathbf{R}$ does the following in iteration r:

1. Let $\mathcal{W}^{\mathbf{R}}$ be the set of wires w_i over which $\mathbf{R}$ receives a complete set of values; i.e.,
   (a) A degree-t polynomial $f^{\mathbf{R}}_i(x)$;
   (b) n Authentication keys $Key^{\mathbf{R}}_{ji}$, for $j = 1, \ldots, n$;
   (c) n authentication values $Auth^{\mathbf{R}}_{ji}$, for $j = 1, \ldots, n$.
   Let $W^{\mathbf{R}}_r$ denote the contents of $\mathcal{W}^{\mathbf{R}}$, when $\mathcal{W}^{\mathbf{R}}$ contains exactly $t + 1 + r$ wires.
2. Wait until $|\mathcal{W}^{\mathbf{R}}| \geq t + 1 + r$. Now corresponding to every $w_i \in W^{\mathbf{R}}_r$, $\mathbf{R}$ computes
$$Support_i = \{w_j \in W^{\mathbf{R}}_r : Auth^{\mathbf{R}}_{ij} = f^{\mathbf{R}}_i(Key^{\mathbf{R}}_{ij})$$
3. If $Support_i \geq t + 1$, then $\mathbf{R}$ concludes that $f^{\mathbf{R}}_i(x)$ is a *valid* polynomial.
4. If $\mathbf{R}$ finds $t + 1$ valid polynomials, then using them $\mathbf{R}$ constructs the bi-variate polynomial $Q^{\mathbf{R}}(x, y) = \sum_{i=0,j=0}^{\substack{i=t\\j=t}} m^{\mathbf{R}}_{i,j} x^i y^j$, outputs $m^{\mathbf{R}} = \{m^{\mathbf{R}}_{i,j} : i, j = 0, \ldots, t\}$ and terminates the protocol. Otherwise $\mathbf{R}$ proceeds to the next iteration.

Lemma 3. *In protocol ASRMT-Uni-Directional, if $\mathbf{R}$ concludes that $f^{\mathbf{R}}_i(x)$ is a valid polynomial, then $f^{\mathbf{R}}_i(x) = f^{\mathbf{S}}_i(x)$ except with probability $\frac{t}{|\mathbb{F}|}$.*

Proof: The lemma trivially holds without any error if w_i is honest. So let w_i be a corrupted wire, which delivers $f^{\mathbf{R}}_i(x) \neq f^{\mathbf{S}}_i(x)$. In order that $f^{\mathbf{R}}_i(x)$ is considered as a valid polynomial by $\mathbf{R}$, it must hold that $Support_i \geq t + 1$. This further implies that there exists at least one honest wire, say w_j, such that $w_j \in Support_i$. This implies that $Auth^{\mathbf{R}}_{ij} = f^{\mathbf{R}}_i(Key^{\mathbf{R}}_{ij})$. Now notice that w_j is an honest wire and so $Auth^{\mathbf{R}}_{ij} = Auth^{\mathbf{S}}_{ij} = f^{\mathbf{S}}_i(Key^{\mathbf{S}}_{ij})$ and $Key^{\mathbf{R}}_{ij} = Key^{\mathbf{S}}_{ij}$. However $\mathcal{A}_t$ will have no information about $Auth^{\mathbf{R}}_{ij}$ and $Key^{\mathbf{R}}_{ij}$, as they are sent over w_j. So the probability that $f^{\mathbf{R}}_i(Key^{\mathbf{S}}_{ij}) = f^{\mathbf{S}}_i(Key^{\mathbf{S}}_{ij})$, even if $f^{\mathbf{R}}_i(x) \neq f^{\mathbf{S}}_i(x)$ is at most $\frac{t}{|\mathbb{F}|}$. This is because two different polynomials of degree-t can agree on at most t points and $Key^{\mathbf{S}}_{ij}$ is selected randomly by $\mathbf{S}$. So except with error probability $\frac{t}{|\mathbb{F}|}$, $f^{\mathbf{R}}_i(x) = f^{\mathbf{S}}_i(x)$ for every valid polynomial $f^{\mathbf{R}}_i(x)$. □

Lemma 4 (Termination). **R** *will eventually terminate* ASRMT-Uni-Directional.

PROOF: The proof follows from the fact that there always exists at least $t+1$ honest wires, who will eventually deliver valid polynomials. □

Lemma 5 (Communication Complexity). ASRMT-Uni-Directional *has a communication complexity of* $\mathcal{O}(n^2)$ *to send a message of size* $(t+1)^2 = \Theta(n^2)$.

PROOF: Easy and follows from the protocol description. □

Lemma 6 (Reliability). *In protocol* ASRMT-Uni-Directional, **R** *will output the correct message, except with error probability* δ.

PROOF: From Lemma 3, $f_i^{\mathbf{R}}(x) = f_i^{\mathbf{S}}(x)$ for every valid polynomial $f_i^{\mathbf{R}}(x)$, except with probability $\frac{t}{|\mathbb{F}|}$. In the worst case, out of the $t+1$ wires which have delivered valid polynomials, t could be corrupted. So the probability that **R** outputs an incorrect message is at most $\frac{t^2}{|\mathbb{F}|} = \delta$ (since $|\mathbb{F}| = \frac{t^2}{\delta}$). □

Theorem 5. *Assume that there are* n $(n = 2t+1)$ *uni-directional wires from* **S** *to* **R**. *Then there exists an ASRMT scheme which can reliably send a message containing* $\Theta(n^2)$ *elements from* $\mathbb{F}$ *by communicating* $\mathcal{O}(n^2)$ *elements from* $\mathbb{F}$, *where* $|\mathbb{F}| = \frac{t^2}{\delta}$ *and* δ *is the error probability.*

3.2 Bounds for Bi-Directional Wires

It is obvious that $\Theta(\ell)$ can be the most tight bound on the communication complexity of any ASRMT protocol, irrespective of whether the wires are uni-directional or bi-directional. Now in the previous section, we have already shown that this bound is achieved if we consider only uni-directional wires. The same bound will also hold even if we consider bi-directional wires.

Till now, we have focussed only on RMT protocols, without worrying about the privacy. We next begin our discussion on SMT protocols, where we have to ensure privacy, in addition to reliability.

4 Bounds on the Communication Complexity of APSMT

Throughout Section 4, we assume that $n \geq 3t+1$ since $n \geq 3t+1$ wires (uni-directional or bi-directional) are required for any APSMT protocol [2].

4.1 Bounds for Uni-Directional Wires

In [5], it is shown that any PSMT protocol has a communication complexity of $\Omega\left(\frac{n\ell}{n-3t}\right)$, when there exists $n \geq 3t+1$ uni-directional wires from **S** to **R**. The lower bound will also hold for APSMT protocols. Moreover, in [2], the authors have designed an APSMT protocol, which requires a communication complexity of $\mathcal{O}(n\ell) = \mathcal{O}\left(\frac{n\ell}{n-3t}\right)$ to send a message of size ℓ, provided there are $n = 3t+1$ uni-directional wires from **S** to **R**. From this discussion, we can state the following theorem.

Theorem 6. *Any APSMT scheme executed over n uni-directional wires from* $\mathbf{S}$ *to* $\mathbf{R}$*, where $n \geq 3t+1$ has a communication complexity of* $\Theta\left(\frac{n\ell}{n-3t}\right)$.

4.2 Bounds for Bi-Directional Wires

Let $\mathbf{S}$ and $\mathbf{R}$ be connected by n bi-directional wires, denoted by $\mathcal{W} = \{w_1, \ldots, w_n\}$, where $n \geq 3t+1$. Then we show that any APSMT protocol has a communication complexity of $\Omega\left(\frac{n\ell}{n-3t}\right)$. To derive the lower bound, we use an approach similar to the one used Theorem 3. Specifically, we show the following:

1. We first show that in any APSMT protocol executed over n bi-directional wires, where $n \geq 3t+1$, the information exchanged over *any* $n-2t$ wires completely determine the message (Lemma 7).
2. Next, we show that any APSMT protocol where the information exchanged over $n-2t$ wires completely determine the message has a communication complexity of $\Omega\left(\frac{n\ell}{n-3t}\right)$ (Lemma 8).

Lemma 7. *In any APSMT protocol executed over n bi-directional wires, where $n \geq 3t+1$, the information exchanged over any $n-2t$ wires should completely determine the secret message $m^{\mathbf{S}}$.*

Proof: The proof follows using same arguments as in Lemma 1. □

Lemma 8. *Any APSMT protocol executed over n ($n \geq 3t+1$) bi-directional wires, in which the information exchanged over any $n-2t$ wires completely determine the message, has a communication complexity of* $\Omega\left(\frac{n\ell}{n-3t}\right)$.

Proof: Here we will use same arguments as used in Lemma 2. But we will also use an additional fact about APSMT protocols. Let Π^{APSMT} be an APSMT protocol, executed over n bi-directional wires (where $n \geq 3t+1$), to securely send a message of size ℓ, such that the information exchanged over *any* $n-2t$ wires completely determine the message. We now define the notations $\mathcal{M}$, $\mathbf{T}_i^m$, $\mathbf{M}_{i,j}^m$ and $\mathbf{M}_{i,j}$, which are exactly the same as in Lemma 2.

Since Π^{APSMT} is an APSMT protocol, it implies that in Π^{APSMT}, the transmission on any set of t wires is *independent* of the secret message. If it is not the case, then adversary will also know the secret message by passively listening the t wires. Thus, for any two messages $m_1, m_2 \in \mathcal{M}$, it must hold that

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

Notice that the above relation must hold for any selection of t wires. We focussed on the set $\{w_{2t+1}, \ldots, w_{3t}\}$ just for simplicity. Now in Π^{APSMT}, the transmission over any set of $n-2t$ wires has *full* information about the secret message. Thus it must also hold that

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

We again stress that the above relation must hold for any selection of $n-2t$ wires. We focussed on the set $\{w_{2t+1},\ldots,w_n\}$ just for simplicity. As mentioned earlier, $\mathbf{M}^m_{2t+1,3t}$ will be same for all messages $m \in \mathcal{M}$. Thus, in order that the above relation holds, it must hold that $\mathbf{M}^m_{3t+1,n}$ is *unique* for every message $m \in \mathcal{M}$. This implies that

$$|\mathbf{M}_{3t+1,n}| = |\mathcal{M}|.$$

From the definition of $\mathbf{T}_i$ and $\mathbf{M}_{i,j}$, we get

$$\prod_{i=3t+1}^{n} |\mathbf{T}_i| \geq |\mathbf{M}_{3t+1,n}| \geq |\mathcal{M}|.$$

Let $g = n - 3t$. The above inequality holds for any selection of g wires $\mathcal{D} \subset \{w_1,\ldots,w_n\}$, where $|\mathcal{D}| = g$; i.e., $\prod_{w_i \in \mathcal{D}} |\mathbf{T}_i| \geq |\mathcal{M}|$. In particular, it holds for every selection $\mathcal{D}_k = \{w_{kg+1 \bmod n}, w_{kg+2 \bmod n}, \ldots, w_{kg+g \bmod n}\}$, with $k \in \{0,\ldots,n-1\}$. If we consider all the $\mathcal{D}_k$ sets collectively, then each wire is counted exactly g times in the collection. Thus, the product of the capacities of all $\mathcal{D}_k$ yields the capacity of the full wire set to the g-th power, and since each $\mathcal{D}_k$ has capacity at least $|\mathcal{M}|$, we get

$$|\mathcal{M}|^n \leq \prod_{k=0}^{n-1} \mathit{\Pi}_{w_j \in \mathcal{D}_k} |\mathbf{T}_j| = \left(\prod_{i=1}^{n} |\mathbf{T}_i|\right)^g,$$

and therefore

$$n \log(|\mathcal{M}|) \leq g \sum_{i=1}^{n} \log(|\mathbf{T}_i|).$$

As $\log(|\mathcal{M}|) = \ell \log(|\mathbb{F}|)$, from the above inequality, we get

$$\sum_{i=1}^{n} \log(|\mathbf{T}_i|) \geq \left(\frac{n\ell \log(|\mathbb{F}|)}{g}\right) \geq \left(\frac{n\ell \log(|\mathbb{F}|)}{n-3t}\right).$$

Now $\sum_{i=1}^{n} \log(|\mathbf{T}_i|)$ denotes the lower bound on the communication complexity of protocol $\mathit{\Pi}^{\text{APSMT}}$ in bits. From the above inequality, we find that the lower bound is $\left(\frac{n\ell \log(|\mathbb{F}|)}{n-3t}\right)$ bits. Now each field element can be represented by $\log(|\mathbb{F}|)$ bits. Thus the lower bound is $\left(\frac{n\ell}{n-3t}\right)$ field elements. □

Theorem 7. *Any APSMT protocol executed over n ($n \geq 3t+1$) bi-directional wires has a communication complexity of $\Omega\left(\frac{n\ell}{n-3t}\right)$.*

Now any protocol executed over n uni-directional wires can also be executed over n bi-directional wires. From Theorem 6, there exists an APSMT protocol which can be executed over $n = 3t+1$ uni-directional wires and requires a communication complexity of $\mathcal{O}\left(\frac{n\ell}{n-3t}\right)$. So the bound in Theorem 7 is tight.

5 Bounds on the Communication Complexity of ASSMT

Any ASSMT protocol requires $n \geq 2t+1$ wires, irrespective of whether the wires are uni-directional or bi-directional [2]. So we assume that $n \geq 2t+1$ throughout Section 5.

5.1 Bounds for Uni-Directional Wires

Theorem 8. *Any ASSMT protocol executed over n ($n \geq 2t+1$) uni-directional wires has a communication complexity of $\Omega\left(\frac{n\ell}{n-2t}\right)$.*

Proof: The theorem follows from the fact that any SSMT protocol with $n \geq 2t+1$ uni-directional wires [9] requires the same communication complexity. □

We now show that the bound in Theorem 8 is asymptotically tight. Let there exists $n = 2t+1$ uni-directional wires $\mathcal{W} = \{w_1, \ldots, w_n\}$ from $\mathbf{S}$ to $\mathbf{R}$. Then we design a protocol called ASSMT-Uni-Directional, which securely sends a message $m^{\mathbf{S}} = \{m^{\mathbf{S}}_k : k = 1, \ldots, n\}$ containing $\ell = n$ elements from the field $\mathbb{F}$ and has a communication complexity of $\mathcal{O}(n^2) = \mathcal{O}\left(\frac{n\ell}{n-2t}\right)$, where $|\mathbb{F}| = \frac{nt}{\delta}$.

The high level idea of the protocol is as follows: for each $m^{\mathbf{S}}_k$, sender generates n Shamir shares [12]. Now the i^{th} share of each $m^{\mathbf{S}}_k$ is sent over wire w_i. However, it is not enough to just send the shares, as the adversary can delay the communication over t honest wires and it can also change the shares over t corrupted wires. So $\mathbf{S}$ also sends some authentication information, which will enable $\mathbf{R}$ to identify the corrupted shares with very high probability. For performing the authentication, we use similar idea as used in our ASRMT protocol (see Fig. 1), with some *additional* steps. More specifically, we interpret the i^{th} shares of n secrets as the coefficients of a polynomial $f^{\mathbf{S}}_i(x)$ of degree-n. This polynomial will be sent over w_i (this is same as sending the i^{th} shares for the n messages). Now the polynomial $f^{\mathbf{S}}_i(x)$ can be authenticated by n random authentication keys $Key^{\mathbf{S}}_{ij}$ by computing $Auth^{\mathbf{S}}_{ij} = f^{\mathbf{S}}_i(Key^{\mathbf{S}}_{ij})$. However, the communication of $Key^{\mathbf{S}}_{ij}, Auth^{\mathbf{S}}_{ij}$ over wire w_j will breach the privacy of $f^{\mathbf{S}}_i(x)$, if w_i is honest and w_j is corrupted. To avoid this, we perform the authentication in the following way: corresponding to $Key^{\mathbf{S}}_{ij}$, we select a random masking key $Mask^{\mathbf{S}}_{ij}$ and define $Auth^{\mathbf{S}}_{ij} = f^{\mathbf{S}}_i(Key^{\mathbf{S}}_{ij}) + Mask^{\mathbf{S}}_{ij}$. Finally, $Key^{\mathbf{S}}_{ij}, Auth^{\mathbf{S}}_{ij}$ will be sent over w_j, while $Mask^{\mathbf{S}}_{ij}$ will be sent over w_i, along with $f^{\mathbf{S}}_i(x)$. As we will show later, this will help to maintain the perfect privacy and will also help to identify the corrupted shares with very high probability. Once $\mathbf{R}$ receives $t+1$ correct shares (which he will receive eventually), $\mathbf{R}$ will correctly recover each $m^{\mathbf{S}}_k$ with very high probability. The details are in Fig. 2.

We now prove the properties of protocol ASSMT-Uni-Directional.

Lemma 9. *In protocol ASSMT-Uni-Directional, if $\mathbf{R}$ concludes that $f^{\mathbf{R}}_i(x)$ is a valid polynomial, then $f^{\mathbf{R}}_i(x) = f^{\mathbf{S}}_i(x)$ except with probability $\frac{n}{|\mathbb{F}|}$.*

Proof (sketch): Follows using similar arguments as in Lemma 3 and the fact that two different polynomials of degree-(n) can agree on at most n points. □

Fig. 2. Protocol ASSMT-Uni-Directional. Let $m^{\mathbf{S}} = \{m_k^{\mathbf{S}} : k = 1, \ldots, n\}$.

Computation and Communication by S:

1. For $k = 1, \ldots, n$, corresponding to $m_k^{\mathbf{S}}$, **S** selects a random degree-t polynomial $p_k^{\mathbf{S}}(x)$, where $p_k^{\mathbf{S}}(0) = m_k^{\mathbf{S}}$ and computes $Sh_{ki}^{\mathbf{S}} = p_k^{\mathbf{S}}(i)$, for $i = 1, \ldots, n$.
2. For $i = 1, \ldots, n$, **S** forms a polynomial $f_i^{\mathbf{S}}(x) = Sh_{1i}^{\mathbf{S}} \cdot x + Sh_{2i}^{\mathbf{S}} \cdot x^2 + \ldots + Sh_{ni}^{\mathbf{S}} \cdot x^n$.
3. For $i = 1, \ldots, n$, corresponding to the polynomial $f_i^{\mathbf{S}}(x)$, **S** selects n random authentication keys $Key_{ij}^{\mathbf{S}}$ and n random masking keys $Mask_{ij}^{\mathbf{S}}$, for $j = 1, \ldots, n$. **S** then computes $Auth_{ij}^{\mathbf{S}} = f_i^{\mathbf{S}}(Key_{ij}^{\mathbf{S}}) + Mask_{ij}^{\mathbf{S}}$.
4. For $i = 1, \ldots, n$, **S** sends the following to **R** over wire w_i and terminates:
   (a) The polynomial $f_i^{\mathbf{S}}(x)$ of degree-n by sending its coefficients;
   (b) n Masking keys $Mask_{ij}^{\mathbf{S}}$, for $j = 1, \ldots, n$;
   (c) n authentication keys $Key_{ji}^{\mathbf{S}}$ and n authentication values $Auth_{ji}^{\mathbf{S}}$, for $j = 1, \ldots, n$.

Message Recovery by R:

For $r = 0, \ldots, t$, **R** does the following in iteration r:

1. Let $\mathcal{W}^{\mathbf{R}}$ be the set of wires w_i over which **R** receives a complete set of values; i.e.,
   (a) A polynomial $f_i^{\mathbf{R}}(x)$ of degree-n;
   (b) n Masking keys $Mask_{ij}^{\mathbf{R}}$, for $j = 1, \ldots, n$;
   (c) n authentication keys $Key_{ji}^{\mathbf{R}}$ and n authentication values $Auth_{ji}^{\mathbf{R}}$, for $j = 1, \ldots, n$.

   Let $W_r^{\mathbf{R}}$ denote the contents of $\mathcal{W}^{\mathbf{R}}$, when $\mathcal{W}^{\mathbf{R}}$ contains exactly $t + 1 + r$ wires.
2. Wait until $|\mathcal{W}^{\mathbf{R}}| \geq t + 1 + r$. Now corresponding to every $w_i \in W_r^{\mathbf{R}}$, **R** computes
$$Support_i = \{w_j \in W_r^{\mathbf{R}} : Auth_{ij}^{\mathbf{R}} = f_i^{\mathbf{R}}(Key_{ij}^{\mathbf{R}}) + Mask_{ij}^{\mathbf{R}}\}$$
3. If $Support_i \geq t + 1$, then **R** concludes that $f_i^{\mathbf{R}}(x)$ is a *valid* polynomial. Let $f_i^{\mathbf{R}}(x) = Sh_{1i}^{\mathbf{R}} \cdot x + Sh_{2i}^{\mathbf{R}} \cdot x^2 + \ldots + Sh_{ni}^{\mathbf{R}} \cdot x^n$. Then $Sh_{ki}^{\mathbf{R}}$ is considered as a valid share for $m_k^{\mathbf{S}}$, for $k = 1, \ldots, n$.
4. If **R** finds $t + 1$ valid polynomials, then from their coefficients, **R** finds $t + 1$ valid shares for each $m_k^{\mathbf{S}}$, for $k = 1, \ldots, n$. Now using these valid shares, **R** reconstructs the degree-t polynomials $p_k^{\mathbf{R}}(x)$, outputs $m^{\mathbf{R}} = \{p_k^{\mathbf{R}}(0) : k = 1, \ldots, n\}$ and terminates the protocol. Otherwise **R** proceeds to the next iteration.

Lemma 10 (Termination). **R** *will eventually terminate ASSMT-Uni-Directional.*

Proof: The proof follows from the fact that there always exists at least $t + 1$ honest wires, who will eventually deliver valid polynomials. □

Lemma 11 (Communication Complexity). *ASSMT-Uni-Directional has a communication complexity of $\mathcal{O}(n^2)$ to send a message of size n.*

Proof: Easy and follows from the protocol description. □

Lemma 12 (Reliability). *In protocol ASSMT-Uni-Directional,* **R** *will output the correct message, except with error probability δ.*

Proof(sketch): The proof follows using similar arguments as used in Lemma 6 and the fact that $|\mathbb{F}| = \frac{nt}{\delta}$. □

Lemma 13 (Perfect Secrecy). *In protocol ASSMT-Uni-Directional, the message $m^{\mathbf{S}}$ will be perfectly secure.*

Proof: Without loss of generality, let $w_1, \ldots, w_t$ be under the control of $\mathcal{A}_t$. So the adversary will know t shares for each $m_k^{\mathbf{S}}$, for $k = 1, \ldots, n$ through the polynomials $f_1^{\mathbf{S}}(x), \ldots, f_t^{\mathbf{S}}(x)$. The adversary will also know $Auth_{ji}$, for $j = t+1, \ldots, n$ and $i = 1, \ldots, t$. But this will not reveal any new information about $f_j^{\mathbf{S}}(x)$, for $j = t+1, \ldots, n$, as the adversary will not know the corresponding masking keys $Mask_{ji}$, for $j = t+1, \ldots, n$ and $i = 1, \ldots, t$ because they are sent over wires w_j, for $j = t+1, \ldots, n$, which are honest. Now the secrecy of each $m_k^{\mathbf{S}}$ follows from the properties of Shamir secret sharing [12]. □

Theorem 9. *Let there exists n $(n \geq 2t+1)$ uni-directional wires from $\mathbf{S}$ to $\mathbf{R}$. Then there exists an ASSMT protocol, which securely sends a message of size $\ell = n$ and requires a communication complexity of $\mathcal{O}(n^2) = \mathcal{O}\left(\frac{n\ell}{n-2t}\right)$.*

5.2 Bounds for Bi-Directional Wires

Theorem 10. *Any ASSMT protocol executed over n $(n \geq 2t+1)$ bi-directional wires has a communication complexity of $\Omega\left(\frac{n\ell}{n-2t}\right)$.*

Proof(sketch): We give the high level idea. We first claim that in any ASSMT protocol executed over n $(n \geq 2t+1)$ bi-directional wires, the communication over any set of $n-t$ wires should completely determine the secret message. This is obvious, since the adversary can arbitrarily delay the communication over t wires. So $\mathbf{R}$ should have the capacity to recover the message even from the communication done over $n-t$ wires. We next claim that in any ASSMT protocol, the communication over any set of t wires should be completely independent of the secret message. Now from these two facts, we can derive that the communication complexity will be $\Omega\left(\frac{n\ell}{n-2t}\right)$. □

From Theorem 9, there exists an ASSMT scheme, which can be executed over $n = 2t+1$ uni-directional wires and which has an asymptotic communication complexity of $\mathcal{O}\left(\frac{n\ell}{n-2t}\right)$. The same protocol can also be executed over $n = 2t+1$ bi-directional wires. Thus the bound in Theorem 10 is asymptotically tight.

6 Conclusion and Open Problems

In this paper, we have resolved the communication complexity of asynchronous RMT and SMT protocols. Our investigation reveals several insightful facts. We have considered settings where all the n wires are either uni-directional or bi-directional. It is interesting to consider a more general setting, where certain wires are directed from $\mathbf{S}$ to $\mathbf{R}$ and certain wires are directed from $\mathbf{R}$ to $\mathbf{S}$.

References

1. S. Agarwal, R. Cramer, and R. de Haan. Asymptotically optimal two round perfectly secure message transmission. In *CRYPTO*, LNCS 4117, pp 394–408, 2006.
2. A. Choudhary, A. Patra, Ashwinkumar B. V, K. Srinathan, and C. Pandu Rangan. On minimal connectivity requirement for secure message transmission in asynchronous networks. In *ICDCN*, LNCS 5408, pp 148–162, 2009. Full version to appear in *JPDC* 2011.
3. A. Choudhury. Protocols for reliable and secure message transmission. Cryptology ePrint Archive, Report 2010/281, 2010.
4. D. Dolev, C. Dwork, O. Waarts, and M. Yung. Perfectly secure message transmission. *JACM*, 40(1):17–47, 1993.
5. M. Fitzi, M. K. Franklin, J. A. Garay, and S. H. Vardhan. Towards optimal and efficient perfectly secure message transmission. In *TCC*, pp 311–322, 2007.
6. M. Franklin and R. Wright. Secure communication in minimal connectivity models. *Journal of Cryptology*, 13(1):9–30, 2000.
7. K. Kurosawa and K. Suzuki. Truly efficient 2 round perfectly secure message transmission scheme. In *EUROCRYPT*, LNCS 4965, pp 324–340, 2008.
8. A. Patra, A. Choudhary, K. Srinathan, and C. Pandu Rangan. Constant phase bit optimal protocols for perfectly reliable and secure message transmission. In *INDOCRYPT*, LNCS 4329, pp 221–235, 2006.
9. A. Patra, A. Choudhary, K. Srinathan, and C. Pandu Rangan. Unconditionally reliable and secure message transmission in undirected synchronous networks: Possibility, feasibility and optimality. *IJACT*, 2(2):1599–197, 2010.
10. H. Sayeed and H. Abu-Amara. Perfectly secure message transmission in asynchronous networks. In *IEEE Symposium on Parallel and Distributed Processing*, pp 100–105, 1995.
11. H. Sayeed and H. Abu-Amara. Efficient perfectly secure message transmission in synchronous networks. *Information and Computation*, 126(1):53–61, 1996.
12. A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.
13. K. Srinathan, A. Narayanan, and C. Pandu Rangan. Optimal perfectly secure message transmission. In *CRYPTO*, LNCS 3152, pp 545–561, 2004.
14. K. Srinathan, A. Patra, A. Choudhary, and C. Pandu Rangan. Probabilistic perfectly reliable and secure message transmission - possibility, feasibility and optimality. In *INDOCRYPT*, LNCS 4859, pp 101–122, 2007.
15. K. Srinathan, N. R. Prasad, and C. Pandu Rangan. On the optimal communication complexity of multiphase protocols for perfect communication. In *IEEE S&P*, pp 311–320, 2007.