Optimal One Round Almost Perfectly Secure Message Transmission

Mohammed Ashraful Alam Tuhin and Reihaneh Safavi-Naini

Department of Computer Science, University of Calgary,
maatuhin@ucalgary.ca, rei@ucalgary.ca

Abstract. In this paper we consider 1-round almost perfect secure message transmission protocols with optimal transmission rate and provide two constructions for connectivities $n \geq 2t+1$ and $n \geq (2+c)t, c \geq \frac{1}{t}$, respectively. Here n and t are the total number of wires and the number of corrupted wires, respectively. The first protocol has a modular construction that with appropriate instantiations of each module results in optimal protocols for $n \geq 2t+1$. The second protocol is the first construction for optimal protocol when $n \geq (2+c)t, c \geq \frac{1}{t}$.

1 Introduction

The **S**ecure **M**essage **T**ransmission (**SMT**) problem was introduced in [5] to address the problem of secure communication between two nodes in an incomplete network. In the SMT problem, the sender $\mathcal{S}$ and the receiver $\mathcal{R}$ do not share a key but are connected by n 'wires' where *at most* t of which are controlled by an adversary $\mathcal{A}$. Wires are abstractions of node-disjoint paths between $\mathcal{S}$ and $\mathcal{R}$. Security means $\mathcal{R}$ will receive the message sent by $\mathcal{S}$ in a *private* and *reliable* way. The initial motivation of this model is to reduce connectivity requirements in secure multi-party protocols [3]. In recent years SMT protocols have found applications in key distribution in sensor networks [4].

1.1 Motivation of our work

It was shown [5] that one round protocols with perfect privacy and perfect reliability requires $n \geq 3t+1$. Franklin and Wright defined (ε, δ)-SMT $(0 \leq \varepsilon, \delta \leq 1)$ [8] where the loss of privacy and reliability is bounded by ϵ and δ, respectively. (ε, δ)-SMT protocols exist for $n \geq 2t+1$. A perfectly private $(\varepsilon = 0)$ and δ-reliable secure message transmission, denoted by $(0, \delta)$-SMT, is called an **A**lmost **P**erfect **S**ecure **M**essage **T**ransmission (**APSMT**, for short).

In this paper we consider the 1-round APSMT problem for different levels of network connectivity, starting from the minimum requirement of $n = 2t+1$ up to higher level of connectivity $n = (2+c)t$. These protocols are most suitable for key establishment in wireless ad hoc and sensor networks [12].

1.2 Our Results

We consider two types of connectivity. In the first case, $n = 2t+k$, where $k \geq 1$ is a constant. In the second case, $n = (2+c)t$, where c is a constant satisfying $c \geq \frac{1}{t}$ and so, a *constant fraction* of wires can be corrupted.

1. We first present a modular construction for 1-round APSMT protocol for $n = 2t + k$ which consists of two modules. The first module (n, t, δ)-$Send$ is a protocol that is used to deliver with δ-reliability, an information matrix of size $(n - 2t) \times n$ (random elements chosen from an alphabet, *e.g.* a finite field) to the receiver such that the adversary can learn *at most* a sub-matrix of size $(n-2t) \times t$. At the end of the module, sender and receiver share a sub-matrix of size $(n - 2t) \times (n - t)$ which is completely unknown to the adversary. However, the sender and the receiver do not know the sub-matrix.

The second module is a privacy amplification (PA) protocol that extracts $(n - t)$ elements that are completely unknown to the adversary, from a shared vector of size n which has at most t elements known by the adversary. We propose a new construction for the first module. For the second module, we adapt an existing PA technique which is computationally more efficient than the one used by [10]. We show that a construction that uses these two modules has linear (in n) transmission rate which is optimal and matches the lower bound on the transmission rate for 1-round APSMT protocol for this connectivity.

2. Next, we present a 1-round APSMT protocol for $n = (2 + c)t$, where c is a constant and $c \geq \frac{1}{t}$. This protocol has *constant* transmission rate and is *optimal*. The protocol uses the two modules (n, t, δ)-$Send$ and $PA(n, n - t)$ used in designing our first protocol above. We also adapt an existing protocol as the third module, to send the ciphertexts with *constant* transmission rate. The ciphertexts are obtained by encrypting messages using the one-time pads produced by using $PA(n, n - t)$.
The modular construction of SMT protocols introduced in this work is the first in the SMT literature and could result in construction of more efficient protocols.

Related Work. The lower bound on transmission rate for 1-round APSMT is $\Omega(\frac{n}{n-2t})$ [10]. Protocols whose transmission rate asymptotically matches this bound are called *rate-optimal* (or *optimal*, for short). This means that for $n = 2t + 1$ and $n = (2 + c)t$, optimal protocols have transmission rates $O(n)$ and $O(1)$, respectively.

An optimal and efficient 1-round APSMT protocol for $n = 2t + 1$ is given in [10]. All the other known 1-round APSMT protocols are either *not optimal* [7, 6] or *computationally inefficient* [9]. There are also efficient APSMT protocols for $n = 3t + 1$ [1, 10], but the one in [1] is *not optimal*. Prior to this work, there is *no* known general construction for connectivity $n = (2 + c)t$, where $c \geq \frac{1}{t}$.

Organization. Section 2 gives definitions and notations. In Section 3 we present the 1-round APSMT protocol for $n = 2t+k$ together with security and efficiency analysis and comparison with related work. In Section 4, we give our 1-round APSMT protocol for $n = (2 + c)t$ and analyze its security and efficiency. In Section 5 we conclude our work.

2 Background

Communication Model. We consider a *synchronous*, *incomplete* network. The sender $\mathcal{S}$ and the receiver $\mathcal{R}$ are connected by n vertex-disjoint paths, also known as wires or channels. Both $\mathcal{S}$ and $\mathcal{R}$ are honest. The goal is for $\mathcal{S}$ to send a message

m to $\mathcal{R}$ such that $\mathcal{R}$ receives it correctly and privately. The wires are undirected and two-way. The protocol can have one or more rounds. In a round, a message is sent by either $\mathcal{S}$ or $\mathcal{R}$ to the other party over the wires. Messages are delivered to the recipient of the round before the next round starts.

Adversary Model. The adversary $\mathcal{A}$ has *unlimited* computational power and corrupts a subset of nodes in the network. A path (wire) that includes a corrupted node is controlled by $\mathcal{A}$. Corrupted nodes can arbitrarily *eavesdrop, modify or block* messages sent over the corrupted wires. $\mathcal{A}$ uses all the information obtained from the corrupted wires to choose and corrupt a new wire up to the threshold t. $\mathcal{S}$ and $\mathcal{R}$ *do not know which wires are corrupted.*

Notation. $\mathcal{M}$ is the message space from which messages are chosen according to a probability distribution π. Let $M_{\mathcal{S}}$ be the message randomly selected by $\mathcal{S}$. We assume $\mathcal{M}$ and π are known in advance to all parties including the adversary. Let $R_{\mathcal{A}}$ be the random coins used by $\mathcal{A}$ to choose t out of total n wires to corrupt.

In an execution of an SMT protocol Π, $\mathcal{S}$ draws $M_{\mathcal{S}}$ from $\mathcal{M}$ using the distribution π, and aims to send it to $\mathcal{R}$ privately and reliably. We assume that at the end of the protocol, $\mathcal{R}$ outputs a message $M_{\mathcal{R}} \in \mathcal{M}$ or 'NULL'.

Let $V_{\mathcal{A}}(M_{\mathcal{S}}$ and $r_{\mathcal{A}})$ denotes the view of the adversary $\mathcal{A}$ when $\mathcal{S}$ has chosen $M_{\mathcal{S}}$ and $R_{\mathcal{A}} = r_{\mathcal{A}}$. $V_{\mathcal{A}}(M_{\mathcal{S}}, R_{\mathcal{A}})$ is a random variable that depends on the random coins of $\mathcal{S}$ and $\mathcal{R}$ and the choice of $M_{\mathcal{S}}$. When $R_{\mathcal{A}} = r$ and $M_{\mathcal{S}} = m$, we write $V_{\mathcal{A}}(M_{\mathcal{S}} = m, r_{\mathcal{A}} = r)$ or $V_{\mathcal{A}}(m, r)$, for short.

The *statistical distance* of two random variables X, Y over a set $\mathcal{U}$ is defined as

$$\Delta(X, Y) = \frac{1}{2} \sum_{u \in \mathcal{U}} |\Pr[X = u] - \Pr[Y = u]|$$

Definition 1. *[8] An SMT protocol is called an (ε, δ)-Secure Message Transmission ((ε, δ)-SMT) protocol if the following two conditions are satisfied:*

- ***Privacy:*** *For every two messages $m_0, m_1 \in \mathcal{M}$ and every $r \in \{0,1\}^*$,*

$$\Delta(V_{\mathcal{A}}(m_0, r), V_{\mathcal{A}}(m_1, r)) \leq \varepsilon,$$

  where the probability is over the randomness of $\mathcal{S}$ and $\mathcal{R}$.
- ***Reliability:*** *$\mathcal{R}$ receives the message M_S with probability $\geq 1 - \delta$. That is,*

$$\Pr[M_{\mathcal{R}} \neq M_{\mathcal{S}}] \leq \delta,$$

  where the probability is over the randomness of all the players and the choice of $M_{\mathcal{S}}$.

When $\varepsilon = 0$, the protocol is said to achieve *perfect privacy* and when $\delta = 0$, the protocol is said to achieve *perfect reliability.*

The number of ***rounds*** of a protocol is the number of interactions between $\mathcal{S}$ and $\mathcal{R}$. We consider synchronous network where time is divided into clock ticks and in each clock tick the sender or the receiver sends a message and the message is received by the other party before the next clock tick.

Communication complexity is the total number of bits transmitted between $\mathcal{S}$ and $\mathcal{R}$ for communicating the message. Communication efficiency is often

measured in terms of *transmission rate*, which is the ratio of the communication complexity to the length of the message m. That is,

$$\textit{Transmission Rate} = \frac{\text{total number of bits transmitted}(\ell)}{\text{size of the secrets}(|m|)}$$

The message is either one element or a sequence of elements from an alphabet. ***Computation complexity*** is the amount of computation performed by $\mathcal{S}$ and $\mathcal{R}$ throughout the protocol. A protocol which needs *exponential* in n computation is called *inefficient*. Efficient protocols need *polynomial* in n computation.
The relationship between n and t required for the existence of an SMT protocol is referred to as the ***connectivity requirements*** of the SMT protocol.

Bounds. It was shown in [8] that APSMT is possible if and only if $n \geq 2t+1$. Dolev *et al.* showed (1, 0)-SMT (PRMT) protocols are possible if $n \geq 2t+1$ [5].

Patra *et al.* showed that the lower bound on the transmission rate of 1-round APSMT protocol is given by $\Omega(\frac{n}{n-2t})$ [10]. When $n = 2t+k, k \geq 1$, the lower bound on transmission rate becomes $\Omega(n)$ and when $n = (2+c)t$, where $c \geq \frac{1}{t}$ is a constant, it becomes *constant*. SMT protocols that asymptotically achieve the above bounds, for respective connectivities, are called *optimal* with respect to the corresponding bound.

1-round PRMT Protocol for $n = (2+c)t$. We now present a 1-round PRMT protocol Π_1 for $n = (2+c)t, c \geq \frac{1}{t}$. The main idea of this protocol is to use codewords of Reed-Solomon codes to send ct messages (each consisting of one field element) with perfect reliability by sending n field elements. The sender constructs a polynomial $f(x)$ of degree at most $(ct-1)$ such that the ct coefficients of $f(x)$ are the messages to be sent perfectly reliably. The sender then sends evaluations of $f(x)$ on distinct points, each associated with a wire, through the corresponding wire. The receiver can correct the t possible errors, reconstruct the polynomial, and recover the ct sent messages. This protocol can be seen as an adaptation of the protocol REL-SEND of [11].

3 1-round Optimal APSMT Protocol for $n = 2t + k$

Our construction consists of two sub-protocols that will be used as black-boxes in the final protocol. The first subprotocol is called (n, t, δ)-*Send*. The second one is a non-interactive *privacy amplification (PA)* protocol, $PA(n, n-t)$.

3.1 (n, t, δ)-*Send*

This protocol constructs an input matrix R of size $n \times n$, $R = (r_{11}, ..., r_{1n}, ..., r_{n,1}, ..., r_{n,n})$ consisting of $(n-2t)n$ randomly chosen elements that the adversary has no knowledge about, and delivers it to the receiver as R' such that (i) $Pr(R = R') \geq 1-\delta, \delta < \frac{1}{2}$, and (ii) at most a sub-matrix of size $(n-2t) \times t$ of R will become known to the adversary $\mathcal{A}$. Therefore, a sub-matrix of size $(n-2t) \times (n-t)$ will be unknown to $\mathcal{A}$.
Our proposed (n, t, δ)-*Send* subprotocol is shown in Fig. 1.

Theorem 1. *Protocol (n, t, δ)-Send sends $(n-2t) \times n$ random elements so that all the $(n-2t) \times n$ will be received with probability $1-\delta$, and the adversary can*

Transmission: Consider a sequence of $(n-2t)n$ random elements $R = (r_{11}, ..., r_{1n}, ..., r_{n-2t,1}, ..., r_{n-2t,n})$ as a matrix of size $(n-2t) \times n$. The sender performs two steps as follows:

Step1 For each $i, 1 \leq i \leq n-t$:

Constructs a random polynomial $p_i(x)$ of degree $\leq (n-1)$ such that $p_i(x) = \sum_{j=0}^{n-1} a_{i,j}x^j$. Here a_{ij}'s are random elements from $\mathbb{F}$.

- For each $i, 1 \leq i \leq n$:
  Forms a poly. $q_i(x)$ of degree $\leq (n-t-1)$ such that the j^{th} coefficients of $q_i(x)$ is $a_{j,i-1}, 1 \leq j \leq n-t$.
- Suppose $r_{ij} = q_j(i), 1 \leq i \leq n-2t, 1 \leq j \leq n$.
- For each $i, n-t+1 \leq i \leq n$:
  Constructs a poly. $p_i(x)$ of degree $\leq (n-1)$ such that $p_i(x) = \sum_{j=0}^{n-1} q_j(i)x^j$.

Step 2 Randomly selects n^2 field elements $s_{ij}, 1 \leq i, j \leq n$ and constructs pairs $(s_{ij}, p_i(s_{ij})), 1 \leq i, j \leq n$.

- Sends $p_i(x)$ through wire i and $(s_{ij}, p_i(s_{ij}))$ through wire j, for $1 \leq i, j \leq n$.

Recovery: The receiver does the following. For each $i, 1 \leq i \leq n$:

Step 1 Receive $p'_i(x)$ over wire i, and $(s'_{ij}, v_{i,s_{ij}})$ through wire j, for $1 \leq j \leq n$. Suppose a'_{ij} are the coefficients of the received polynomials.

- Compute $k = |\{j : p'_i(s'_{ij}) \neq v_{i,s_{ij}}|$.
- If $k \geq t+1$, then decide wire i as corrupted and adds i to a list $FAULTY$.

Step 2 Suppose $i_1, i_2, ..., i_{n'}, n' \geq n-t$ are the indices of the wires $\notin FAULTY$. For each $j, 1 \leq j \leq n$, do the following:

  * Form a poly. $q'_j(x)$ of degree $\leq n-t-1$ using $a'_{i_1 j}, ..., a'_{i_{n-t} j}$ and verify whether $q'_j(i_l) \neq p'_{i_\ell}(i_\ell), \ell > n-t$. If there exists one such ℓ, then output 'NULL' and terminate the protocol.

- Reconstruct the first $(n-t)$ polynomials by considering any $(n-t)$ polynomials carried by wires not in the list $FAULTY$.
- Recover the $(n-2t) \times n$ random elements in the same way as the sender.

Fig. 1. (n, t, δ)-*Send.*

learn at most $(n-2t) \times t$ *elements, while* $(n-2t) \times (n-t)$ *elements are completely unknown to the adversary. The total required communication is* $O(n^2 \log |\mathbb{F}|)$.

Proof. **Perfect Privacy.** There are $(n\text{-}t)$ independently generated random polynomials. The adversary sees *at most* any t polynomials and t points of any other polynomials. Since polynomials are of degree n-1 then all n coefficients are independent and so in total $(n\text{-}2t) \times (n\text{-}t)$ elements remain unknown to the adversary.
δ-reliability. Omitted due to lack of space.

Efficiency. The sender sends n polynomials, each of degree at most $(n-1)$ through the n wires. This incurs a communication of $n^2 \log |\mathbb{F}|$. He also sends each of the n pair of values (evaluation points) through each wire, for all the polynomials. This needs a communication of $2n^2 \log |\mathbb{F}|$. Therefore, the total communication of this protocol is $n^2 \log |\mathbb{F}| + 2n^2 \log |\mathbb{F}| = O(n^2 \log |\mathbb{F}|)$. ■

3.2 Non-interactive Privacy Amplification for SMT

Privacy amplification allows the sender and the receiver to non-interactively generate a random elements which will be completely unknown to the adversary,

from $b > a$ random elements, where the adversary knows *at most* $(b-a)$ elements. We will employ the privacy amplification of [2] in this work given in Figure 2.

$PA(b, b-a)$; $a < b$: input $(x_1, ..., x_b) \in \mathbb{F}^b$; output: $(X_1, X_2, ..., X_a) \in \mathbb{F}^a$

1. Forms a polynomial $f(x)$ of degree $\leq (b-1)$ such that $f(i) = x_i, 1 \leq i \leq b$.
2. Outputs $(f(b+1), ..., f(b+a))$.

Fig. 2. The non-interactive Privacy Amplification Technique $PA(b, b-a)$.

3.3 Description of the protocol

Our 1-round APSMT protocol Π_2 for $n = 2t+1$ is given in Fig. 3. The receiver in this protocol will never output incorrect message(s). He will either output the correct message(s) or output 'NULL'.

The sender $\mathcal{S}$ wishes to send $n-t = (t+1)$ secrets $m_0, m_1, ..., m_t \in \mathbb{F}^{t+1}$ to the receiver $\mathcal{R}$. Since $n = 2t+1$, here $(n-2t)n = n$.

Step 1. The sender $\mathcal{S}$ does the following:
1. Call (n, t, δ)-*Send* to communicate n random elements $r_i, 1 \leq i \leq n$.
2. Call $PA(n, n-t)$ with $(r_1, r_2, ..., r_n)$ as input and get $(R_1, R_2, ..., R_{t+1})$.
3. Form $t+1$ ciphertexts as $c_i = m_i \oplus R_i$, and broadcast $c_i, 1 \leq i \leq t+1$.

Step 2. The receiver does the following.
1. Receive the n random elements $r_1, r_2, ..., r_n$.
2. Call $PA(n, n-t)$ with $(r_1, r_2, ..., r_n)$ as input and get $(R_1, R_2, ..., R_{t+1})$
3. Recover the $t+1$ messages as $m_i = c_i \oplus R_i, 1 \leq i \leq t+1$.

Fig. 3. The 1-round APSMT protocol Π_2 for $n = 2t+1$

Security and Efficiency Analysis. Besides using (n, t, δ)-*Send* and $PA(n, n-t)$, the protocol broadcasts the $(t+1)$ ciphertexts. Since, broadcasting ensures the reliable transmission of the ciphertexts and the one-time pads generated by PA are secure, the secrets transmitted will be perfectly private and δ-reliable. In other words, the privacy of the protocol Π_2 follows from the privacy of $PA(n, n-t)$ and Theorem 1. The reliability of Π_2 also follows from Theorem 1.
The transmission rate of Π_2 is $O(n)$. This is true because (n, t, δ)-*Send* has communication cost of $O(n^2 \log |\mathbb{F}|)$. The protocol Π_2 also broadcasts $(t+1)$ ciphertexts with a communication cost of $n(t+1)\log|\mathbb{F}|$. Therefore, the total communication of this protocol is $O(n^2 \log |\mathbb{F}|)$.The protocol sends $(t+1)$ messages of total size $(t+1)\log|\mathbb{F}| = O(n \log |\mathbb{F}|)$ and so the transmission rate is $O(n)$ which is optimal for a 1-round $(0, \delta)$-SMT protocol for $n = 2t+1$.

Comparison. The comparison with related work is outlined in Table 1.

[1] Here λ is the probability that the cheater win in a secret sharing scheme with a cheater.

Table 1. Comparison with 1-round APSMT protocols for $n = 2t + 1$ (here Comp. refers to computation complexity and q is the field size)

Author	**Comp.**	δ	**Optimality**
Kurosawa and Suzuki [9]	*Exp.*	$\leq (\binom{n}{t+1} - \binom{n-t}{t+1})\lambda$[1]	Yes
Desmedt and Wang [7]	*Poly.*	$\leq \frac{n}{q}$	No
Patra *et al.*[10]	*Poly.*	$\leq \frac{n^3}{q}$	Yes
Desmedt *et al.* [6]	*Poly.*	$\leq \frac{t(t+1)}{q}$	No
This work	*Poly.*	$\leq \frac{n^2}{q}$	Yes

4 1-round Optimal APSMT protocol for $n = (2 + c)t$

We present a 1-round APSMT protocol for $n = (2 + c)t$, where c is a constant satisfying $c \geq \frac{1}{t}$. The protocol has *optimal* transmission rate. The protocol is designed by extending the protocol Π_2 and using the 1-round PRMT protocol Π_1 for $n = (2 + c)t, c \geq \frac{1}{t}$ showed in Section 2.

Description of the protocol. The protocol is given in Fig. 4. The receiver will either output the correct message(s) or output 'NULL'.

The sender wishes to send $(n-t)(n-2t)$ secrets $m_{11}, ..., m_{1,n-t}, m_{21}, ..., m_{2,n-t}, ..., m_{n-2t,1}, ..., m_{n-2t,n-t} \in \mathbb{F}^{(n-2t)(n-t)}$ to the receiver $\mathcal{R}$.

Step 1. The sender $\mathcal{S}$ does the following:
1. Call (n, t, δ)-*Send* (communicate $(n - 2t)n$ random elements $r_{ij}, 1 \leq i \leq n - 2t, 1 \leq j \leq n$).
2. Call $PA(n, n - t)$, $(n - 2t)$ times, for $1 \leq i \leq n - 2t$ (use $(r_{ij}, 1 \leq j \leq n)$) as input to obtain $(n - t)$ random-elements $(R_{i1}, ..., R_{i,n-t})$).
3. Generate $(n-2t)(n-t)$ ciphertexts, $c_{ij} = m_{ij} \oplus R_{ij}, 1 \leq i \leq n-2t, 1 \leq j \leq n-t$ and send them by calling Π_1, in parallel, $(n - t)$ times.

Step 2. The receiver does the following.
1. Receive the $(n - 2t)n$ random elements $r_{ij}, 1 \leq i \leq n - 2t, 1 \leq j \leq n$..
2. Call $PA(n, n - t)$, $(n - 2t)$ times with $(r_{ij}, 1 \leq j \leq n))$ as input to get $(n - t)$ random-elements $(R_{i1}, ..., R_{i,n-t})$, for $1 \leq i \leq n - 2t$.
3. Receive the $(n - 2t)(n - t)$ ciphertexts perfectly reliably and recover the $(n - 2t)(n - t)$ secrets using $(R_{11}, ..., R_{1,n-t}, ..., R_{n-2t,1}, ..., R_{n-2t,n-t})$ as $m_{ij} = c_{ij} \oplus R_{ij}, 1 \leq i \leq n - 2t, 1 \leq j \leq n - t$.

Fig. 4. The 1-round APSMT protocol Π_3 for $n = (2 + c)t$

Perfect Privacy and δ-Reliability. Perfect privacy of Π_3 follows from the perfect privacy of all the three sub-protocols used in the main protocol. The reliability of Π_3 follows directly from the reliability of (n, t, δ)-*Send* and that of Π_1. Therefore, Π_3 is unreliable with probability *at most* $\frac{n^2}{|\mathbb{F}|}$.

Efficiency. (n, t, δ)-*Send* needs a communication of $O(n^2 \log |\mathbb{F}|)$. The communication for using Π_1 is $n(n-2t)\log|\mathbb{F}| = O(n^2 \log |\mathbb{F}|)$ bits. Therefore, the total communication of the protocol Π_3 is $O(n^2 \log |\mathbb{F}|)$. The protocol sends $(n-2t)(n-t) = ct(t+ct)$ messages of total size $ct(t+ct)\log|\mathbb{F}| = O(n^2 \log |\mathbb{F}|)$, resulting in $O(1)$ transmission rate and is thus *optimal*.

5 Conclusion and Open Problems

We gave two 1-round *optimal* APSMT protocols for connectivities $n = 2t + k$, where $k \geq 1$ is a constant, and $n \geq (2+c)t, c \geq \frac{1}{t}$, respectively. The first protocol has the highest reliability compared to all existing optimal 1-round APSMT protocol. The second protocol is the first for this kind of connectivity. It remains an interesting open problem to construct optimal 1-round APSMT protocols with more reliability than the protocols presented in this paper. We proposed modular construction for designing optimal SMT protocols. It is interesting to extend this approach to protocols with more than one round.

Acknowledgments. Financial support for this research was provided in part by Alberta Innovates Technology Future in the Province of Alberta, as well as NSERC (Natural Sciences and Engineering Research Council) in Canada.

References

1. T. Araki. Almost Secure 1-Round Message Transmission Scheme with Polynomial-time Message Decryption. In Proc. of ICITS 2008.
2. S. Agarwal, R. Cramer, and R. de Haan. Asymptotically Optimal Two-round Perfectly Secure Message Transmission. In CRYPTO, volume 4117 of LNCS, pages 394–408. Springer, 2006.
3. M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness Theorems for Non-cryptographic Fault-tolerant Distributed Computation (extended abstract). In Proc. of STOC, pp. 1–10, 1988.
4. H. Chan, A. Perrig, and D. Song. Random Key Predistribution for Sensor Networks. In Proc. of IEEE Conference on Security and Privacy, 2003.
5. D. Dolev, C. Dwork, O. Waarts, and M. Yung. Perfectly Secure Message Transmission. In Journal of the ACM, 40(1):17–47, 1993.
6. Y. Desmedt, S. Erotokritou, and R. Safavi-Naini. Simple and Communication Complexity Efficient Almost Secure and Perfectly Secure Message Transmission Schemes. In Proc. of AFRICACRYPT, pp. 166–183, 2010.
7. Y. Desmedt and Y. Wang Perfectly Secure Message Transmission Revisited. In Proc. of EUROCRYPT, pp. 502–517, LNCS 2332, 2002.
8. M. K. Franklin and R. N. Wright. Secure Communication in Minimal Connectivity Models. In Journal of Cryptology, 13(1):9–30, 2000.
9. K. Kurosawa and K. Suzuki. Almost Secure (1-round, n-channel) Message Transmission Scheme. In Proc. of ICITS, volume 4883 of LNCS, pages 99–112, 2009.
10. A. Patra, A. Choudhary, K. Srinathan, and C. Rangan. Unconditionally Reliable and Secure Message Transmission in Undirected Synchronous Networks: Possibility, Feasibility and Optimality. Available at http://eprint.iacr.org/2008/141.pdf.
11. K. Srinathan, A. Narayanan, and C. P. Rangan. Optimal Perfectly Secure Message Transmission. In Proc. of CRYPTO, volume 3152 of LNCS, Springer, 2004.
12. Y. Wang Robust Key Establishment in Sensor Networks. In SIGMOD Record 33(1): 14–19, 2004.