On Optimal Secure Message Transmission by Public Discussion

Hongsong Shi, Shaoquan Jiang, Reihaneh Safavi-Naini, Mohammed Ashraful Tuhin

Abstract—In a secure message transmission (SMT) scenario a sender wants to send a message in a private and reliable way to a receiver. Sender and receiver are connected by $n$ vertex disjoint paths, referred to as wires, $t$ of which can be controlled by an adaptive adversary with unlimited computational resources. In Eurocrypt 2008, Garay and Ostrovsky considered an SMT scenario where sender and receiver have access to a public discussion channel and showed that secure and reliable communication is possible when $n \geq t + 1$. In this paper we will show that a secure protocol requires at least 3 rounds of communication and 2 rounds invocation of the public channel and hence give a complete answer to the open question raised by Garay and Ostrovsky. We also describe a round optimal protocol that has constant transmission rate over the public channel.

Index Terms—SMT, public discussion, round complexity, MPC.

I. INTRODUCTION

Dolev, Dwork, Waarts and Yung [5] introduced Secure Message Transmission (SMT) systems to address the problem of delivering a message from sender $S$ to receiver $R$ in a network guaranteeing reliability and privacy. $S$ is connected to $R$ by $n$ node disjoint paths, referred to as wires, $t$ controlled by the adversary with unlimited computational power.

A perfectly secure message transmission or PSMT for short, guarantees that $R$ always receive the sent message and the adversary does not learn anything about it. It was shown that PSMT is possible if and only if $n \geq 2t + 1$. See [5], [7], [13], [2], [3], [1] for more references. Franklin and Wright [9] relaxed the security requirement of SMT protocols and proposed probabilistic security in which two parameters $\varepsilon$ and $\delta$ upper bound the advantage of the adversary in breaking privacy, and the probability that $R$ fails to recover the sent message, respectively. In a PSMT protocol $\varepsilon = \delta = 0$. In this paper we refer to these protocols as almost SMT protocols. We refer interested readers to [7], [2], [1], [15].

Franklin and Wright [9] also considered a model where an additional reliable broadcast channel is available to $S$ and $R$. A broadcast channel guarantees that all nodes of the network receive the same message. We refer to this model as Broadcast Model (BM). They showed that PSMT in this model requires $n \geq 2t + 1$, but probabilistic security can be obtained with $n > t$ and gave a 3-round $(0, \delta)$ protocol in this model.

Garay and Ostrovsky [11] replaced the broadcast channel with an authentic and reliable public channel that connects $S$ and $R$. A public channel is totally susceptible to eavesdropping but is immune to tampering. We refer to this communication model as Public Discussion Model (PDM). Garay and Ostrovsky [11] gave a 4 round protocol with probabilistic security when $n > t$, which shows that the connectivity requirement for PDM is the same as the broadcast model.

Efficiency parameters of SMT protocols are, (i) the number of rounds where each round is one message flow between $S$ and $R$, or vice versa, and (ii) the communication efficiency measured in terms of transmission rate which is the total number of bits sent over all wires for a message divided by the length of the secret.

Round complexity in PDM is measured by a pair $(r, r')$ where $r$ is the total number of rounds and $r'$ is the number of rounds that the public channel is invoked $(r \geq r')$.

Related models: Public channel has been used in other contexts including unconditionally secure key agreement [14] where the public channel is used for the advantage distillation, information reconciliation and privacy amplification. The public channel in this case is a free resource and its communication cost is not considered. In PDM however, the cost of realizing a channel in a distributed system is taken into account.

A. Our Results

Garay et al. [11] proposed a $(4, 3)$-round protocol and subsequently improved its round complexity to $(3, 2)$-round [10]. However it was not known if this round complexity was optimal.

The main result of this paper is to prove that the minimum values of $r$ and $r'$ for which an $(r, r')$-round $(\varepsilon, \delta)$ protocol can exist are 3 and 2, respectively. This answers the question of round optimality of almost SMT protocols in PDM that was raised in [11].

Our results on round optimality are obtained in three steps. We first prove that there is no $(2, 2)$-round $(\varepsilon, \delta)$ protocol in PDM with $\varepsilon + \delta < 1 - 1/|M|$ when $n \leq 2t$, where $M$ denotes the message space. This means that message transmission protocols in PDM with $(2, 2)$-round complexity will be either unreliable, or insecure.

In the second step we will show that when the invocation of the public channel does not depend on the protocol execution
and is statically determined as part of protocol description, there is no \((r \geq 3, 1)\)-round \((\varepsilon, \delta)\) protocol with \(\varepsilon + \delta < 1 - 1/|M|\) and \(\delta < \frac{1}{2}(1 - 1/|M|)\) when \(n \leq 2t\).

Then we generalize this result to the case that the invoker of the public channel is not fixed at the start of the protocol and is adaptively determined in each execution, and show that there is no \((3, 1)\)-round \((\varepsilon, \delta)\) protocol with \(3\varepsilon + 2\delta < 1 - 3/|M|\).

We also construct a round optimal protocol that has constant transmission rate over the public channel when the length of message (i.e., \(\log |M|\)) is \(\Omega((n \log \delta)^2)\) bits long.

Table I summarizes our results and puts them in relation to others’ works.

B. Discussion

One of the main motivations for studying SMT is to reduce connectivity requirement in secure multiparty protocols \([3, 4, 16]\). Secure multiparty protocols require a secure and reliable channel between every two nodes and so require the network graph to be complete. Using an SMT protocol one can simulate secure connection between any two nodes using a network with sufficient connectivity, that is, \(n\) disjoint paths (and not direct link) between any two nodes where \(n > 2t\). Secure message transmission in PDM can further reduce connectivity \((n > t)\) as long as there is an authentic public channel. This is the lowest possible connectivity and shows that two nodes can securely communicate as long as there is one uncorrupted path between them (and a public channel). Realizing a public channel in a point-to-point sparse network however is costly. For example it is possible to simulate such a channel using almost-everywhere broadcast protocol \([11]\) that uses almost-everywhere Byzantine agreement protocol \([6]\). It is shown \([19]\) that in degree-bounded networks agreement on a single bit using almost-everywhere agreement protocol requires at least \(O(\log N)\) rounds communication, where \(N\) is the number of nodes in the network.

The high cost of simulating the public channel is the motivation for reducing the number of invocation and transmission rate of such a channel.

C. Organization

Section 2 describes the security model and relevant definitions. Lower bounds on round complexity of SMT protocol in PDM are proved in Section 3. Section 4 describes an round optimal \((0, \delta)\)-SMT by public discussion protocol. Finally we draw a conclusion in Section 5.

II. Preliminaries

A. Model and Notations

Network model. We assume a synchronous, connected point-to-point incomplete network. Players \(S\) and \(R\) are connected by \(n\) vertex-disjoint paths, called wires. In addition to the wires, we assume there is an authentic and reliable public channel between \(S\) and \(R\). Messages over this channel are publicly accessible and are correctly delivered to the recipient. All wires and the public channel are bidirectional. SMT protocols proceed in rounds. In each round, one player may send a message on each wire and the public channel, while the other player will only receive the sent messages. The sent messages will be delivered before the next round starts.

Adversary model. The adversary \(A\) is computationally unbounded. \(A\) can corrupt nodes on paths between \(S\) and \(R\). A wire is corrupted if at least one node on the path is corrupted. We assume up to \(t \leq n - 1\) wires can be corrupted by the adversary. \(A\) can eavesdrop, modify or block messages sent over the corrupted wires. \(A\) is assumed to be adaptive, meaning that she can corrupt wires during the protocol execution based on the communication traffic it has seen so far.

We also consider static adversary by which we mean that the adversary chooses the corrupted wires before the start of the protocol. A static adversary will however act adaptively during the protocol execution with regard to messages that are sent over the corrupted wires: in each round the adversary sees the traffic over all the corrupted wires and the public channel before tampering the traffic over the corrupted wires in that round.

Notations. Let \(M\) be the message space. Let \(M_S\) denote the secret message of \(S\), and \(M_R\) the message output by \(R\). We use \(\perp\) to denote null string and \(\emptyset\) to denote empty set. The notation \(u \sim \mathcal{U}\) denotes that a value \(u\) is sampled uniformly from a set \(\mathcal{U}\).
B. Definitions

The statistical distance of two random variables $X$, $Y$ over a set $U$ is given by,

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

Lemma 1: \cite{20} Let $X, Y$ be two random variables over a set $U$. The advantage of any computationally unbounded algorithm $D : U \rightarrow \{0, 1\}$ to distinguish $X$ from $Y$ is

$$|\Pr[D(X) = 1] - \Pr[D(Y) = 1]| \leq \Delta(X, Y).$$

In an execution of an SMT protocol $\Pi$, $S$ wants to send $M_S \in M$ to $R$ privately and reliably. We assume that at the end of the protocol, $R$ always outputs a message $M_R \in M$.

An execution is completely determined by the random coins of all the players including the adversary, and the message distribution of $M_S$. For $P \in \{S, R, A\}$, the view of $P$ includes the random coins of $P$ and the messages that $P$ receives. Denote by $V_A(m, c_A)$ the view of $A$ when the protocol is run with $M_S = m$ and $A$’s randomness $C_A = c_A$.

Definition 1: A protocol between $S$ and $R$ is an $(\epsilon, \delta)$-Secure Message Transmission by Public Discussion (SMT-PD) protocol if the following two conditions are satisfied:

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

$$\Delta(V_A(m_0, c_A), V_A(m_1, c_A)) \leq \epsilon,$$

where the probability is taken over the randomness of $S$ and $R$.

- **Reliability:** $R$ recovers the message $M_S$ with probability larger than $1 - \delta$, or formally

$$\Pr[M_R \neq M_S] \leq \delta,$$

where the probability is over the randomness of players $S$, $R$ and $A$, and the choice of $M_S$.

Observe that the above definition is oblivious of the message distribution, meaning that given an SMT-PD protocol, it will be secure with the same privacy and reliability parameters regardless of the concrete distribution over $M$.

III. Round Complexity of SMT-PD Protocol

By the similarity of broadcast model and public discussion model, we recall Franklin and Wright’s results \cite{20} in our language as follows.

Theorem 1: \cite{20} If $n \leq 2t$, then: (i) For any values $r \geq r'$, it is impossible to construct $(r, r')$-round (0, 0)-SMT-PD protocols; (ii) For any values $r > 0$ and $0 \leq \epsilon \leq 1$, it is impossible to construct $(r, 0)$-round $(\epsilon, \delta)$-SMT-PD protocols with $\delta < \frac{1}{2}(1 - \frac{1}{|M|})$.

In this section, we will prove when $n \leq 2t$ any $(\epsilon, \delta)$-SMT-PD protocol needs $(3, 2)$-round complexity. This is by proving that: (i) secure $(2, 2)$-round $(\epsilon, \delta)$-SMT-PD protocols do not exist, and (ii) for any $(3, 1)$-round protocol, either privacy or reliability can be compromised.

The following lemma plays a central role in proving the impossibility results in this paper. Loosely speaking, the lemma shows that for an $(\epsilon, \delta)$-SMT-PD protocol no algorithm that is given the adversary’s view as the input, can output $M_S$ with a probability much better than random guess.

Lemma 2: Let $\Pi$ be an $(\epsilon, \delta)$-SMT-PD protocol and assume $S$ selects $M_S \leftarrow M$. Then no adversary $A$ can correctly guess $M_S$ with probability larger than $\epsilon + 1/|M|$. That is,

$$\Pr[M_A = M_S] \leq \epsilon + 1/|M|,$$

where $M_A$ denotes the adversary’s output, and the probability is taken over the random coins of $S$, $R$ and $A$.

In proving Lemma 2 we need the Lemma 3 below (See Appendix for its proof).

Lemma 3: Consider an $(\epsilon, \delta)$-SMT-PD protocol $\Pi$ and an adversary $B$ that plays the following game: the challenger $C$ sets up the system; $B$ selects two messages $M_0, M_1$ from $M$ and gives them to a challenger $C$ who selects $b \leftarrow \{0, 1\}$ and runs the protocol (by simulating $S, R$) to transmit $M_b$. $B$ can corrupt up to $t$ wires and finally outputs a bit $b'$.

Let $\mathcal{B}^{\Pi(M_b)}()$ be the output of $B$ when $b$ is selected by $C$ in the simulation. Then

$$\Pr[\mathcal{B}^{\Pi(M_b)}() = 1] - \Pr[\mathcal{B}^{\Pi(M_0)}() = 1] \leq \epsilon,$$

where the probability is taken over the randomness of $C$ and $B$.

Proof: (of Lemma 2) The proof is by contradiction: assume that there is an adversary $A$ that can output $M_A$ with probability $\Pr[M_A = M_S] > \epsilon + 1/|M|$. We will construct an algorithm $B$ to invalidate Eq. (2).

The code of $B$ is as follows: $B$ randomly chooses two messages $(M_0, M_1) \in M$ and asks its challenger $C$ to transmit one of the two messages. $C$ chooses a bit $b \leftarrow \{0, 1\}$ and simulates $S, R$ to run protocol $\Pi$ in transmitting $M_b$. $B$ runs adversary $A$ as a subroutine to attack the protocol. B answers $A$’s queries by forwarding them to the challenger and returning the results back to $A$. At the end of the protocol $A$ outputs a message in $M$ (which can be different from $M_0$ and $M_0$). $B$ outputs 1 if $A$ outputs $M_1$, and outputs 0, otherwise. Note that $B$ will have the complete view of $A$. Then

$$\Pr[\mathcal{B}^{\Pi(M_1)}() = 1] = \Pr[M_A = M_1 | C \text{ has chosen } M_1] > \epsilon + 1/|M|,$$

and

$$\Pr[\mathcal{B}^{\Pi(M_0)}() = 1] = \Pr[M_A = M_1 | C \text{ has chosen } M_0] = 1/|M|.$$  \hspace{1cm} (3)

Note that Eq. (3) follows by that fact that $M_1$ is chosen independent of $M_0$ and the randomness of players $S$ and $R$ in the simulation of $C$ and so the probability of $A$’s output to be equal to $M_1$ (which is chosen randomly) is at most the probability of random guess which is $1/|M|$. Hence, we have $\Pr[\mathcal{B}^{\Pi(M_1)}() = 1] - \Pr[\mathcal{B}^{\Pi(M_0)}() = 1] > \epsilon$, contradicting Corollary 3.
A. Impossibility of (2, 2)-Round $(\varepsilon, \delta)$-SMT-PD Protocol when $n \leq 2t$

The impossibility proof needs to analyze the actions of the adversary in rounds, hence we start by decomposing an SMT-PD protocol into rounds as follows.

**Definition 2:** For a $(r, r')$-round SMT-PD protocol, the functionality of the protocol is described as a sequence of randomized functions $(f_1, \ldots, f_r, g)$.

The function $f_i$ denotes the round encoding function that is used to generate the traffic sent in the $i$-th round. The input of $f_i$ consists of the received messages of previous rounds and random coins of the caller. For a player $P \in \{S, R\}$, $C_p$ denotes the random coins of $P$, and $M_p$ denotes the set of all messages received by $P$ during the first $i$ rounds with $M_0^S = \{S\}$ and $M_0^R = \emptyset$. If the initiator of round $i \leq i \leq r$ is $P$, we write $P_{i-1}X_iY_i = f_i(M_{i-1}, C_p)$ to denote the random variable corresponding to traffic in round $i$; here $P_i$ denotes the traffic over the public channel, and $X_i$ and $Y_i$ denote the traffic over the corrupted wires and the uncorrupted wires, respectively, or vice versa.

The function $g$ denotes the decoding function. By the end of the protocol $R$ outputs $M_R = g(M_{r'}, C_R)$.

**Theorem 2:** Let $n \leq 2t$. Then there is no $(2, 2)$-round $(\varepsilon, \delta)$-SMT-PD protocol with $\varepsilon + \delta < 1 - 1/|M|$.

The proof is by contradiction: suppose there exists a $(2, 2)$-round $(\varepsilon, \delta)$-SMT-PD protocol $\Pi$ with $\varepsilon + \delta < 1 - 1/|M|$. We construct an adversary $A$ that breaks the privacy of $\Pi$ by impersonating $R$. We show that for each execution of $\Pi$ where $S$ sends a message $m$ to $R$, there exists a second execution called a swapped execution where $S$ sends the message $m$ but $A$ impersonates $R$ such that $S$ receives identical traffic in the two executions and so cannot distinguish the two. The views of $R$ and $A$ are however swapped in the two executions, and so if $R$ outputs $M_R = S$ in one of the executions, then $A$ outputs $M_A = S$ in the swapped execution and so $Pr[M_A = S] \geq Pr[M_R = S]$. Using Lemma 2 and that $\Pi$ is an $(\varepsilon, \delta)$-SMT-PD protocol, we have $\varepsilon + \delta \geq 1 - 1/|M|$ which is a contradiction.

**Proof:** Assume by contradiction that there is a $(2, 2)$-round $(\varepsilon, \delta)$-SMT-PD protocol $\Pi$ with $\varepsilon + \delta < 1 - 1/|M|$, and the message distribution over $M$ is uniform. Suppose wires are labeled by 1, 2, $\ldots$, $n$, and $n = 2t$. (Note if there exists an $(\varepsilon, \delta)$-SMT-PD protocol for $n' < 2t$, the same protocol can be run for $n = 2t$ by neglecting the last $n - n'$ wires. Thus an impossibility result for $n = 2t$ still holds for $n' < 2t$.)

The adversary is assumed to be static in the following. That is, the corrupted wires are selected at the start of the protocol. The impossibility results obtained for such adversary will hold for more powerful adversarial adversaries who will corrupt the wires during the running of the protocol.

We write $A$'s randomness as $C_A = (C_{A0}, C_{A1})$ where $C_{A0} \in \{0, 1\}$ is used to select one of the two sets of $t$ wires: $\{1, \ldots, t\}$ or $\{t+1, \ldots, 2t\}$ for corruption and $C_{A1} \in \{0, 1\}^*$ is used for encoding and decoding of the traffic. Let $C_{A0} = 0$ and $C_{A0} = 1$ denote the first and the last $t$ sets of wires will be corrupted, respectively.

Before going ahead, we remark that: (i) The last round message of a SMT-PD protocol can only be from $S$ to $R$ as otherwise it can be removed without affecting the output of $R$. (ii) For generality we don’t assume the interaction in a SMT-PD protocol should be back-and-forth, meaning that some consecutive rounds of the protocol may have the same sender and cannot be combined into one round. Under the effect of public channel, this provides a possible paradigm in designing SMT-PD protocols. E.g., both of the first two rounds of the protocol in [11] are from $S$ to $R$, and are from $R$ to $S$ in [10].

Therefore, depending on the order of the first round, a 2-round SMT-PD protocol has two kinds of interactions.

**CASE 1:** In this case, the first round traffic is from $R$ to $S$, while the second round is from $S$ to $R$. Assume $A_{C_{A0}} = 1$, i.e., the last $t$ wires are corrupted. We illustrate the strategy of $A$ in Fig. 8 and formalize it as follows.

- Round 1: When $R$ sends $P_1X_1Y_1 = f_1(C_R)$, $A$ computes $P_1X'_1Y'_1 = f_1(C'_R)$ where $C'_R$ is the value computed from $C_{A1}$, and results in $P_1$ over the public channel, hence $A$ can leave the transmission over the public channel unchanged. This is always possible because the function table of $f_1$ is public and $A$ is computationally unbounded. Thus $A$ can find the set of random strings such that $\Omega = \{r \mid f_1(r) = P_1X'_1\}$ and $C'_R \leftarrow \Omega$. $A$ will then replaces $Y_1$ by $Y'_1$.

- Round 2: When $S$ generates message $P_2X_2Y_2 = f_2(M_S, P_1X_1Y'_1, C_S), A$ blocks the transmission over the corrupted wires and outputs $M_A = g(P_2X_2, C'_R)$.

Let $E$ be the set of all executions of $\Pi$ in presence of $A$. We consider a binary relation $W$ over $E$ such that $(E, \hat{E}) \in W$ if, (i) $M_S, C_S$ are the same in the two executions; (ii) $C_{A0} \cap C_{A1} = 0$; and (iii) $C_R = C'_R, C'_R = C_R$, where '·' in the superscript denotes the random coins used and messages output by $A$ and $R$ in $\hat{E}$, respectively. Note that in the two executions, the $t$ corrupted wires are swapped with the uncorrupted ones such that the messages received by $A$ and $R$ are swapped as shown in Fig. 8 and 2.

For a pair of $(E, \hat{E}) \in W$, the first round messages received by $S$ in $E$ and $\hat{E}$ are identical and equal to $P_1X_1Y_1$. Thus in the second round, $S$ will generate the same traffic $P_2X_2Y_2$ in both $E$ and $\hat{E}$, and so if $R$ outputs $M_R$ in $E$, $A$ will output $M_A = M_R$ in $\hat{E}$ since $M_R = g(P_2X_2, C_R)$. Also, $\omega(P_2X_2, C'_R) = M_A$.

Let $p_E$ be the probability that execution $E$ is running. Similarly define $p_{\hat{E}}$. Denote by $S \subseteq E$ the set of executions with $M_R = S$ and so we have $Pr[M_R = S] = \sum_{E \in S} p_E$. Now $M_A = M_R$ holds in $\hat{E}$ if $M_R = M_S$ holds in $E$ and so we have $Pr[M_A = M_S] = \sum_{E \in S} p_E$.

Observe that $p_E$ is completely determined by the probability of selecting $M_S$ and other random coins of all the players. For any two executions $(E, \hat{E}) \in W$, we note that $(M_S, C_S) = (M_S', C_S')$, while $C_R$ and $C'_R$ are both selected with uniform probability. Moreover, when $C_R$ and $C'_R$ are fixed, both of the probability of selecting $C_A$ and $C'_A$ are $2^{-1 - \lceil \log |H| \rceil}$. We thus get $p_E = p_{\hat{E}}$. 
Then by Lemma 2 and above argument,
\[ 1 - \delta \leq \Pr[M_R = M_S] \leq \Pr[M_A = M_S] \leq 1/|M| + \epsilon. \quad (4) \]
Therefore, it has \( \epsilon + \delta \geq 1 - 1/|M| \), which contradicts the assumption on \( \Pi \).

**CASE 2.** In this case, both of the two rounds traffic are from \( S \) to \( R \). Intuitively, if \( n \leq 2t \) and \( S \) receives no feedback from \( R \), \( A \) can just block the traffic over the \( t \) corrupted wires such that \( R \) has no advantage over \( A \) in recovering \( M_S \).

More specifically, considering two executions \( E \) and \( \hat{E} \) in this case, where the random coins of \( A \) and \( R \) are swapped, and the corrupted and uncorrupted wires are also swapped. If \( A \) blocks the \( t \) corrupted wires, the view of \( R \) in \( E \) will equal the view of \( A \) in \( \hat{E} \). Then if \( R \) outputs \( M_S \) in one execution, \( A \) will output it in the swapped execution. By Lemma 2 and the assumption on \( \Pi \), Eq. (4) holds also in this case, thus it follows that \( \epsilon + \delta \geq 1 - 1/|M| \).

**B. Impossibility of \((r, 1)\)-Round \((\epsilon, \delta)\)-SMT-PD Protocol when \( n \leq 2t \)**

Theorem 2 shows that optimal \((\epsilon, \delta)\)-SMT-PD protocols need at least 3 rounds, while Theorem 1 shows that at least one round public channel invocation is necessary. A natural question thus is to find out if secure \((r, 3)\)-round SMT-PD protocols can exist. As a warm-up, the following theorem gives a negative answer to the case that the invoker of public channel is specified initially in the protocol.

**Theorem 3:** Let \( n \leq 2t \) and \( r \geq 3 \). Then a \((r, 1)\)-round \((\epsilon, \delta)\)-SMT-PD protocol with fixed invoker of public channel has either \( \epsilon + \delta \geq 1 - \frac{1}{2|M|} \) or \( \delta \geq \frac{1}{2} (1 - \frac{1}{|M|}) \).

The proof is by contradiction: assume there exists a \((r, 1)\)-round \((\epsilon, \delta)\)-SMT-PD protocol \( \Pi \) with fixed invoker of public channel, where values of \( \epsilon \) and \( \delta \) do not satisfy any of the above inequalities. We construct an adversary who can break either the privacy or the reliability of \( \Pi \).

\( \mathcal{A} \)'s strategy is to block the traffic (over the \( t \) corrupted channels) sent by the invoker of public channel, and to replace the traffic (over the \( t \) corrupted wires) sent to the invoker by forged traffic that is constructed according to the protocol description. Then,

1. If the public channel is invoked by \( S \), we will show that \( S \) cannot distinguish two swapped executions in which she has the same views. The two executions have the property that if \( R \) outputs \( M_R = M_S \) in one execution then \( A \) outputs \( M_A = M_S \) in the swapped execution. Using an argument similar to Theorem 2 we prove that the adversary can break the privacy of the protocol and thus obtain \( \epsilon + \delta \geq 1 - \frac{1}{2|M|} \).

2. If the public channel is invoked by \( R \), we will show that \( R \) cannot distinguish two swapped executions in which he has the same views. If in one execution \( R \) outputs \( M_S \), he will output \( M_A \) in the swapped execution with the same probability. The two executions have the same probability and so when \( M_S \neq M_A \), we prove the adversary can break the reliability of the protocol and so obtain \( \delta \geq \frac{1}{2} (1 - \frac{1}{|M|}) \).

**Proof:** We stress that in this proof the invoker of the public channel is already specified in the protocol, whereas the actual invocation round of the public channel can be adaptive to the protocol execution. The impossibility result will hold straightforwardly for the case that the invocation round of the public channel is a part of the protocol specification.

As noted in the proof of Theorem 2, the interaction order in the protocol is not necessarily back-and-forth, and the last round is from \( S \) to \( R \). Moreover, we also suppose the message distribution over \( M \) is uniform, and \( n = 2t \) and the adversary is static.

We separate the randomness \( C_A \) (of \( A \)) into four parts: \((C_{M_A}, C_{A0}, C_{A1}, C_{A2})\), where \( C_{A0} \in \{0, 1\} \) is used to choose one of the two subsets of \( t \) wires to corrupt \((C_{A0} = 0 \text{ and } C_{A0} = 1 \text{ are used for the first or the last } t \text{ wires, respectively})\), \( C_{A1} \) is used to generate traffic for substituting the message sent by \( S \), \( C_{A2} \) for generating traffic to substitute the message sent by \( R \), and \( C_{M_A} \) denotes the randomness of \( A \) uniformly selecting a message from \( M \) to impersonate \( S \)'s traffic.
CASE 1. [S invokes the public channel.] We show that in this case \( A \) will break the privacy of \( \Pi \). Without loss of generality, assume \( C_{A0} = 1 \). We describe the action of \( A \) as follows: in round \( 1 \leq j \leq r \),

- When \( S \) sends \( X_i Y_j \) or \( P_j X_i Y_j \), \( A \) blocks \( Y_j \).
- When \( R \) sends \( X_i Y_j \), \( A \) computes \( X'_i Y'_j = f_j(M_{A}^{i-1}, C_{A2}) \), then replaces \( Y_j \) by \( Y'_j \). (Here \( M_{A}^{i-1} \) denotes the messages eavesdropped by \( A \) during the first \( j - 1 \) rounds.)

Finally, \( A \) outputs \( M_A = g(M_A^{r}, C_{A2}) \).

The above strategy of \( A \) is also shown in Fig. 3. Note that \( A \) can block and forge messages as above since \( A \) can randomly select \( C_A \) to generate messages \( \{X_iY_j\} \), and make them consistent with the requirement of protocol \( \Pi \). Also note that \( C_{MA} = M_A \) and \( C_{A1} = \perp \) since \( A \) needs not to impersonate \( S \) in this case.

Let \( E \) be the set of executions of \( \Pi \). We define a binary relation \( W_1 \) over \( E \) to specify two executions \( E \) and \( E' \) as follows: \( (E, E') \in W_1 \) if: (i) \( (M_S, C_S) \) are the same for both executions; (ii) \( C_{A0} + C_{A0} = 1 \); and (iii) \( C_{A2} = C_R \) and \( C_R = C_{A2} \).

Claim 1: (i)the view of \( S \) in \( E \) is the same as her view in \( E' \); and (ii)the view of \( A \) in \( E \) is identical to the view of \( R \) in \( E \). Thus the output of \( R \) in \( E \) is the same as the output of \( A \) in \( E' \). That is, \( M_R = M_A \).

Proof: Without loss of generality assume in execution \( E \) we have \( C_{A0} = 1 \) and the public channel is used in round \( i \). Also assume during the first \( i - 1 \) rounds, \( R \) is the initiator of rounds \( \{r_1, \ldots, r_i\} \subseteq \{1, \ldots, i - 1\} \), ordered nondecreasingly.

We first prove statements (i) and (ii) hold during the first \( r_i \) rounds, then using the same technique we will prove the statements hold in the later rounds and thus prove \( M_R = M_A \).

The proof is by induction over \( \ell \). When \( \ell = 0 \), the statements (i) and (ii) hold trivially from the facts that \( S \) doesn’t receive messages in the first \( i - 1 \) rounds and \( C_{A0} + C_{A0} = 1 \).

For each \( j < r, \) suppose that the statements (i) and (ii) hold in the first \( r_j \) rounds for \( \ell = j \). The induction hypothesis states that \( M_{Rj} = \{X_k\}_{k < r_j} \) and \( M_{Aj} = \{Y_k\}_{k < r_j} \) are swapped, while \( M_{Sj} \) are the same in executions \( E \) and \( E' \). Our objective is to prove that the statements (i) and (ii) also hold during the first \( r_j \) rounds for \( \ell = j + 1 \). Note that in all those rounds \( k \) for \( k < r_j < k < r_{j+1} \), transmissions are only from \( S \) to \( R \). Formally the message of each round \( k \) is \( X_k Y_k = f_k(M_A^j, C_S) \), and \( R \) and \( A \) will receive \( \{X_k\}_{r_j < k < r_{j+1}} \) and \( \{Y_k\}_{r_j < k < r_{j+1}} \) respectively. Thus \( M_{Rj+1} = M_{Rj} \cup \{X_k\}_{r_j < k < r_{j+1}} \) and \( M_{Aj+1} = M_{Aj} \cup \{Y_k\}_{r_j < k < r_{j+1}} \). As \( C_{A0} + C_{A0} = 1 \), it follows that \( M_{Rj+1} \) and \( M_{Aj+1} \) are swapped in \( E \) and \( E' \).

Let \( X_{r_j+1} Y_{r_j+1} = f_{r_j+1}(M_{Rj}^{r_j+1}, C_R) \) and \( X_{r_j+1} Y_{r_j+1} = f_{r_j+1}(M_{Aj}^{r_j+1}, C_A) \) be the messages received by \( S \) in round \( r_{j+1} \) of \( E \). Then \( S \) will receive the same messages in round \( r_{j+1} \) of \( E \) because \( C_{A2} = C_R, C_R = C_{A2} \), and then \( M_{Rj+1}^{r_j+1} \) and \( M_{Aj+1}^{r_j+1} \) are exchanged in \( E \) and \( E' \). Thus the statements (i) and (ii) hold during the first \( r_{j+1} \) rounds.

Henceforth, \( S \) will send \( X_k Y_k = f_k(M_S^j, C_S) = f_k(M_A^j, C_S) \) in each later round \( k \) for \( r_j < k < i \). Observe that in these rounds \( S \) won’t receive messages from \( R \). Thus if \( S \) invokes the public channel in round \( i \) of \( E \), it will do the same in \( E' \). And it follows that the view of \( M_{Rj}^i \) and \( M_{Aj}^i \) in \( E \) and \( E' \) are swapped during the first \( i \) rounds. A similar argument shows that after the \( i \)-th round \( S \) will receive identical messages in the two swapped executions. Finally, the views of \( S \) in the two executions will be the same, but \( M_{Rj}^i \) and
$M'_A$ are swapped in $E$ and $\tilde{E}$. At the end of the protocol, we have $M_R = g(M'_R, C_R) = g(M'_A, C_{A_2}) = M_A$, where $M'_A$ denotes the messages that $A$ has eavesdropped in execution $E$.

Let $S_1 \in \mathcal{E}$ be the set of all successful executions in which $\mathcal{R}$ outputs $M_R = M_S$, and $p_E$ denotes the probability of execution $E$ determined by the random coins of all players. Define $p_{\tilde{E}}$ similarly. Then $\Pr[M_R = M_S] = \sum_{E \in S_1} p_E$. By Claim 1 if $E \in S_1$, $A$ will output $M_S$ in the swapped execution of $\tilde{E}$; therefore $\Pr[M_A = M_S] \geq \sum_{E \in S_1} p_E$.

Additionally, by the definition of $W_1$ and the observation of $C_{M_A} = C_{A_1} = \bot$ in this case, we have,

$$p_E = \frac{1}{|M|} 2^{-r_S - r_R - r_{A_2} - 1} = p_{\tilde{E}},$$

(5)

where $r_S, r_R, r_{A_2}$ denote the length of the random coins of $C_S, C_R, C_{A_2}$ used by $S, \mathcal{R}$ and $A$ respectively.

Now by Eq. (5), and Lemma 2 it follows that Eq. (4) also holds in this case, then it yields that $1 - \frac{1}{|M|} \leq \varepsilon + \delta$, contradicting the assumption on $\Pi$.

CASE 2. [\mathcal{R} invokes the public channel.] We will show that in this case the reliability of $\Pi$ will be broken. This is by showing that for every successful execution there exists an unsuccessful one and so probability of success is at most $1/2$.

Formally, the strategy of $A$ is similar to CASE 1, that is when $C_{A_0} = 1$, then in each round $1 \leq j \leq r$:

- When $S$ sends $X_j Y_j$ or $P_j X_j Y_j$, $A$ blocks $Y_j$.
- When $S$ sends $X_j Y_j$, $A$ computes $X_j Y'_j = f_j(M_j^{j-1}, C_{A_1})$ and replaces $Y_j$ by $Y'_j$. (Here $M_j^{j-1}$ denotes the messages selected and eavesdropped by $A$ during the first $j - 1$ rounds.)

Note that $C_{A_2} = \bot$ in this case. For simplicity, we abuse the notation $M_A$ here to denote the uniformly selected message of $A$ using coins $C_{M_A}$.

Let $E$ and $p_{\tilde{E}}$ be as defined in CASE 1 and consider a binary relation $W_2$ over $E$ where $(E, \tilde{E}) \in W_2$ if: (i) $C_R$ is the same in the two executions; (ii) $C_{A_0} \oplus C_{A_1} = 1$; and (iii) $C_{A_1} = C_S, C_S = C_{A_1}$; (iv) $M_S = M_A$ and $M_A = M_S$.

Denote by $S_2$ the set of successful executions in which $\mathcal{R}$ outputs $M_R = M_S$ under the condition that $M_A \neq M_S$.

Claim 2: For each swapped execution pair $(E, \tilde{E}) \in W_2$, the views of $\mathcal{R}$ in $E$ and $\tilde{E}$ are identical and so if $E \in S_2$ is a successful execution, then $\tilde{E} \notin S_2$ is a failed execution.

Proof: Without loss of generality, assume $\mathcal{R}$ invokes the public channel in round $i$ of $E$, and during the first $i$ rounds $S$ is the initiator of rounds $\{r_1, \ldots, r_i\} \subseteq \{1, \ldots, i-1\}$ (ordered in nondecreasing order) in execution $E$. By induction on $i$, we can prove that $\mathcal{R}$ will receive the same messages during the first $r_i$ rounds of the two swapped executions. This means that $\mathcal{R}$ will invoke the public channel in the same round $i$ of $E$ and $\tilde{E}$, both. Furthermore, we can prove $\mathcal{R}$ will receive the same messages during the later rounds of the two executions. Thus, we have $M'_R = M'_R$, where $M'_R$ denotes all messages that $\mathcal{R}$ received in $\tilde{E}$. The proof is similar to Claim 1.

Now because $M_S$ and $M_A$ are swapped in $E$ and $\tilde{E}$, if $\mathcal{R}$ outputs $M_R = g(M'_R, C_{R}) = M_S$ in $E$, he will output $M_R = g(M'_R, C_{R}) = M_A = M_S$ in $\tilde{E}$. Thus for any two swapped executions $(E, \tilde{E}) \in W_2$ when $M_A \neq M_S$, we have $\tilde{E} \notin S_2$.

Claim 3: (i) The probability of any two swapped executions $(E, \tilde{E}) \in W_2$ is the same; that is $p_E = p_{\tilde{E}}$; and (ii) When $M_S \neq M_A$, the failure probability of $\mathcal{R}$ in recovering the secret message is not less than the success probability of $\mathcal{R}$; formally

$$\Pr[M_R = M_S | M_S \neq M_A] \leq \Pr[M_R \neq M_S | M_S \neq M_A],$$

where the probability is taken over the random coins and messages selected by $S, \mathcal{R}$ and $A$.

Proof: (i) Note that an execution $E \in E$ is completely determined by the random coins and messages selected by all the players. Then for each $E \in E$, we have $p_E = \frac{1}{|M|} 2^{-r_S - r_R - r_{A_2}}$, where $r_S, r_R$ and $r_A$ denote the length of the random coins of $C_S, C_R$ and $C_A$, respectively. Similarly, we have $p_{\tilde{E}} = \frac{1}{|M|} 2^{-r_S - r_R - r_{A_2}}$.

As $C_{A_2} = \bot$ in this case, it has $r_A = r_{M_A} + r_{A_0} + r_{A_1}$, where $r_{M_A}, r_{A_0}, r_{A_1}$ denote respectively the length of $C_{M_A}, C_{A_0}, C_{A_1}$. Similarly, it has $r_{\tilde{A}} = r_{M_A} + r_{A_0} + r_{A_1}$.

Note that $r_{A_0} = r_{A_0} = 1$ and $r_{M_A} = |\log |M||$.

By the definition of $W_2$, we have that $r_R = r_{R'}, r_S = r_{A_1}$ and $r_{A_1} = r_{A_1}$. Hence it has $r_S + r_R + r_A = r_S + r_{R'} + r_{A_1}$, and then $p_E = p_{\tilde{E}}$ holds.

(ii) Let $S_2 = E \setminus S_2$ denote the set of failed executions. Since $E \in S_2$ holds for any $E \in S_2$, and the one-to-one correspondence of $E$ and $\tilde{E}$, we get that $|S_2| \leq |S_2|$. The probability that $\Pi$ fails when $M_A \neq M_S$ can be computed as,

$$\Pr[M_R \neq M_S | M_A \neq M_A] = \Pr[E \notin S_2]$$

$$\geq \sum_{E \in S_2} p_E$$

$$= \sum_{E \in S_2} p_{\tilde{E}}$$

$$= \Pr[M_R = M_S | M_S \neq M_A].$$

From Claim 3 we must have $\Pr[M_R \neq M_S | M_A \neq M_A] \geq \frac{1}{2}$; hence

$$\Pr[M_R \neq M_S]$$

$$\geq \Pr[M_R \neq M_S | M_S \neq M_A] \Pr[M_S \neq M_A]$$

$$\geq \frac{1}{2}(1 - \frac{1}{|M|}).$$

On the other hand, since $\Pi$ is a $\delta$ reliable protocol, we have $\Pr[M_R \neq M_S] \leq \delta$. It follows that $\delta \geq \frac{1}{2}(1 - \frac{1}{|M|})$, which contradicts the assumption on $\Pi$.

C. Impossibility of $(3,1)$-Round PD-adaptive $(\varepsilon, \delta)$-SMT-PD Protocol

Theorem 3 says when the invoker of public channel is known at the start of the protocol, then $(r,1)$-round SMT-PD protocol is impossible. In this section we consider protocols that allow the invoker of public channel depends on the executions; or more precisely depends on the random coins of players. We call this type of SMT-PD protocols PD-adaptive.

Definition 3: A $(r, r')$-round SMT-PD protocol $\Pi$ is called PD-adaptive if the invoker of the public channel and the
round of invocation of the public channel are not specified at the start but depend on $C_S, C_R, C_A$ and $M_S$.

More specifically, for each round $1 \leq i \leq r$, let player $P \in \{S, R\}$ be the initiator of the round. Let $M_{i-1}^P$ be the set of all messages received by $P$ during the first $i - 1$ rounds and that $M_0^S = \{M_S\}$ and $M_0^R = \emptyset$. We denote by $P_iX_iY_i \triangleq f_i(M_{i-1}^P, C_P)$ the traffic of round $i$, where $P_i$ denotes the traffic over the public channel, and $X_i$ and $Y_i$ are the traffic over the two sets of wires, one all corrupted and one all uncorrupted.

Traffic on the public channel, that is $P_i = \perp$ or $P_i \neq \perp$ is determined by $M_0^P$ and $C_P$. Moreover, it must have $P_1 = \perp$ if the public channel has been used $r'$ times before round $j$.

**Theorem 4:** Let $n \leq 2t$. Then a PD-adaptive $(3,1)$-round $(\varepsilon, \delta)$-SMT-PD protocol must have

$$3\varepsilon + 2\delta \geq 1 - \frac{3}{|M|}.$$  

**Proof:** Suppose $\Pi$ is an arbitrarily PD-adaptive $(3,1)$-round $(\varepsilon, \delta)$-SMT-PD protocol. We construct a static adversary $A$ that breaks privacy or reliability of $\Pi$ and so prove that $3\varepsilon + 2\delta \geq 1 - \frac{3}{|M|}$ should hold for any $\Pi$. The message distribution is assumed to be uniform in this proof.

$A$ selects the first or last $t$ wires to corrupt. In the rounds before invocation of the public channel, $A$ conducts man-in-the-middle attack between $S$ and $R$ by tampering with the corrupted wires. When player $P \in \{S, R\}$ uses public channel, $A$ simply blocks the corrupted wires and continues to cheat $P$ by tampering the later transmissions (from the other player $P \to P$) over the corrupted wires until the end of the protocol.

Observe that despite $P$ will learn the locations of corrupted channels, but since the public channel has been used, $P$ cannot notify $P$. Thus $A$ can continue to cheat $P$ in the later execution of the protocol. We will prove that $A$ can conduct the above attack and thus violate the privacy or reliability of the protocol.

We use $A - B - C$ to indicate the initiators of the first, second and third rounds are $A, B$ and $C$, respectively. The proof is divided into four steps stated as lemmas, each proving an impossibility result for an interaction order. The omitted proofs can be found in Appendix B.

**Lemma 4:** If the interaction order of protocol $\Pi$ is $[S\to\to S\to]$, then $\varepsilon + \delta \geq 1 - \frac{1}{|M|}$.

**Proof:** The invoker of public channel in this case must be $S$ and so $A$ only blocks the traffic over the corrupted wires. This is an special case of Theorem 2 and we have $\varepsilon + \delta \geq 1 - \frac{1}{|M|}$.

**Lemma 5:** If the interaction order of protocol $\Pi$ is $[S\to\to R\to S\to]$, then $\varepsilon + \delta \geq \frac{3}{2} - \frac{1}{|M|}$.

**Lemma 6:** If the interaction order of protocol $\Pi$ is $[R\to\to R\to S\to S\to]$, then $3\varepsilon + 2\delta \geq 1 - \frac{3}{|M|}$.

**Lemma 7:** If the interaction order of protocol $\Pi$ is $[R\to\to R\to S\to S\to]$, then $\varepsilon + \delta \geq \frac{3}{2} - \frac{1}{|M|}$.

The above argument shows that a protocol with order $[R\to\to R\to S\to]$ may have better security than protocols with other interaction orders. However, even in this case, the protocol cannot guarantee privacy and reliability at the same time. This completes the proof.

## IV. An Round Optimal SMT-PD Protocol

As noted earlier the modified version of the protocol in [10] has optimal round complexity but has linear (in $n$) transmission rates over the wires and the public channel, while the complexity of protocol in [9] is similar.

In this section we describe a $(3,2)$-round $(0,\delta)$-SMT-PD protocol with constant transmission rate over the public channel, and $O(n)$ transmission rate over the wires (when the message is long enough).

### A. Our Construction

The proposed protocol uses universal hash functions.

**Definition 4:** Let $m > \ell$. A function family $\mathcal{H} = \{h : \{0,1\}^m \to \{0,1\}^\ell\}$ is called *almost strongly universal* hash function family if given any $a_1, a_2 \in \{0,1\}^m$, $a_1 \neq a_2$, and any $b_1, b_2 \in \{0,1\}^\ell$, it holds that $\Pr_{h \in \mathcal{H}}(h(a_1) = b_1 \wedge h(a_2) = b_2) \leq \gamma$.

1) $(S \to \to R):$ For $i = 1, \ldots, n$, $S$ randomly selects $r_i \in \{0,1\}^\ell$ and $R_i \in \{0,1\}^m$ and sends the pair $(r_i, R_i)$ to $R$ along wire $i$.

2) $(S \to R):$ For $i = 1, \ldots, n$, if $R$ correctly receives a pair $(r'_i, R'_i)$ along wire $i$ (i.e., $r'_i \in \{0,1\}^m$, $R'_i \in \{0,1\}^m$), he selects $h_i \to \mathcal{F}$ and computes $T'_i = r'_i \oplus h_i(R'_i)$; otherwise, wire $i$ is assumed corrupted. He then constructs an indicator bit string $B = b_1b_2\ldots b_n$ where $b_i = 1$ if the wire $i$ is corrupted and $b_i = 0$ otherwise. Finally, he sends $(B, (H_1, \ldots, H_n))$ over the public channel, where $H_i = (h_i, T'_i)$ if $b_i = 0$; and $H_i$ is empty, otherwise.

3) $(S \to \to R):$ $S$ ignores the wires with $b_i = 1$. For $i = 1, \ldots, n$, if $b_i = 0$, $S$ computes $T_i = r_i \oplus h_i(R_i)$ and checks $T'_i = T_i$; if $T'_i = T_i$, wire $i$ is assumed consistent; otherwise, wire $i$ is corrupted.

$S$ constructs an indicator bit string $V = v_1v_2\ldots v_n$, where $v_i = 1$ if wire $i$ is considered consistent; otherwise $v_i = 0$. Finally, she publishes the pair $(V, C = M_S \oplus \{ \oplus_{i=1}^{n} R_i \})$ over the public channel.

**$R$** **reverses the message:** When gets $(V, C)$, $R$ recovers $M_R = C \oplus \{ \oplus_{i=1}^{n} R_i \}$ and outputs it.

**Fig. 4.** The $(3,2)$-round $(0,\delta)$-SMT-PD protocol $\Pi_1$.
From Definition 4, $\Pr_{h \in \mathcal{H}}[h(a_1) = c_1 \oplus b \land h(a_2) = c_2 \oplus b] \leq \gamma$ and so $\Pr_{h \in \mathcal{H}}[c_1 \oplus h(a_1) = c_2 \oplus h(a_2)] \leq 2^\ell \gamma$, and the result follows.

Wegman and Carter [21] constructed a $2^{1-2\ell}$-almost strongly universal2 hash family $\mathcal{F} = \{ h : \{0, 1\}^m \to \{0, 1\}^\ell \}$. Functions in $\mathcal{F}$ can be described by $O(\log m)$ bits and computed in polynomial time. The short description length of the family $\mathcal{F}$ allows us to authenticate messages with low communication complexity. The protocol $\Pi_1$ transmits $M_S \in \{0, 1\}^m$ to $R$ is described in Fig. 4.

**Theorem 5:** The protocol $\Pi_1$ is a $(3, 2)$-round $(0, (n-1) \cdot 2^{1-\ell})$-smt-PD protocol. Moreover, $\Pi_1$ is polynomial time computable, and its transmission rate is $O(n)$ over the wires and constant over the public channel when $m = \Omega(n^{\kappa^2})$, where $\kappa$ is the reliability parameter of the system with $\delta = (n-1) \cdot 2^{1-\ell} = 2^{-\kappa}$.

**Proof:** Let $\text{Cor} = \{ i \mid \text{wire} \ i \text{ is corrupted} \}$, and $\text{Con} = \{ i \mid \text{wire} \ i \text{ is consistent} \}$.

- **Reliability:** If $\mathcal{S}$ can detect all corrupted wires with $(r'_i, R'_i) \neq (r_i, R_i)$, the protocol is thus perfectly reliable; otherwise, one such a wire will break the reliability. Using Corollary 2, we show this probability is small. A more formal proof follows.

  In the second round the wires with $b_i = 1$ are detected as corrupted, and are ignored in the third round. Hence in the following we only consider wires with $b_i = 0$. For wire $i$, the wire is called bad if $(r_i, R_i) \neq (r'_i, R'_i)$ but $r_i \oplus h_i(R_i) = r'_i \oplus h_i(R'_i)$. Bad wires are always included in $\text{Con}$. Using Corollary 1 and noting that $r_i, R_i, r'_i, R'_i$ are fixed before the second round and then $h_i$ is selected with uniform distribution, we have

  \[
  \Pr[\text{wire} \ i \text{ is bad}] = \Pr[r_i \oplus h_i(R_i) = r'_i \oplus h_i(R'_i) \land (r_i, R_i) \neq (r'_i, R'_i)] \\
  \leq \Pr[r_i \oplus h_i(R_i) = r'_i \oplus h_i(R'_i) \mid (r_i, R_i) \neq (r'_i, R'_i)] \\
  \leq 2^{1-\ell},
  \]

  where the probability is over the random coins of all the players.

  Then, the probability of unreliable message transmission is

  \[
  \Pr[M_R \neq M_S] = \Pr[\exists j \in \text{Con} R_j \neq \exists j \in \text{Con} R'_j] \\
  \leq \Pr[\exists j \in \text{Con} \text{ s.t. } R_j \neq R'_j] \\
  \leq \Pr[\exists j \text{ at least one bad wire}] \\
  \leq \sum_{j \in \text{Cor}} \Pr[\text{wire} \ j \text{ is bad}] \\
  \leq (n-1) \cdot 2^{1-\ell},
  \]

  where the probability is over the random coins of all the players.

- **Perfect Privacy:** The intuition for proving perfect privacy is as follows: the adversary can obtain transmissions related to $M_S$ only from the public channel in round 3. However, $M_S$ is masked by $R_i$ (if wire $i$ is uncorrupted), and the adversary knows nothing about $R_i$ because the only transmission which depends on $R_i$ is in the second round invocation of public channel $(h(R_i))$ which is masked by $r_i$ and is not known by the adversary. This is true because $r_i$ was only transmitted on a secure wire $i$.

A more formal proof follows.

Let $M_S = m^*$ be the message chosen by $S$ and $C_A = c_A$ denotes the value of $A$’s coin. We first describe $A$’s view in the protocol. Observe that in protocol $\Pi_1$ Cor is formed completely in the first round since the last two rounds are only over the public channel. Then in the first round $A$ sees $\{(r_i, R_i)\} \in \text{Cor}$ over the corrupted wires and modifies them into $\{(r'_i, R'_i)\} \in \text{Cor}$. In the second and third round, $A$ sees respectively $(B, (H_1, \ldots, H_n))$ and $(V, M \oplus \{ \{R_i\} \in \text{Cor} \})$ over the public channel. Since $\{(r'_i, R'_i)\} \in \text{Cor}$ is computed by $A$ using $c_A$ and $\{(r_i, R_i)\} \in \text{Cor}$ (in adaptive way), and when $A$ knows $\{(r'_i, R'_i), \{R_i\} \in \text{Cor} \}$, she can compute $\{(r'_i + h_i(R'_i)) \in \text{Cor}, B\}$ and $(\{R_i\} \in \text{Cor} \cap \text{Cor}, V)$ by herself, we thus remove the computable part from her view and describe it as a 4-tuple of random variables as follows,

\[
V_A(m^*, c_A) = (c_A, V_1, V_2, V_3) = (c_A, \{(r_i, R_i)\} \in \text{Cor}, \{(h_i)_{i=1}^n, \{r_i \oplus h_i(R_i)\} \in \text{Cor}\}, m^* \oplus (\{\oplus \text{Cor} \}, R_i)),
\]

where $V_i$ is $A$’s view in round $i$.

For two messages $m_0, m_1$ and $C_A = c_A$, the statistical distance between $V_A(m_0, c_A)$ and $V_A(m_1, c_A)$ is given by,

\[
\Delta(V_A(m_0, c_A), V_A(m_1, c_A)) = \frac{1}{2} \sum_v | \Pr[V_A(m_0, c_A) = v] - \Pr[V_A(m_1, c_A) = v] |,
\]

where the probability is over the choices of $CS$ and $CR$.

Then the term $\Pr[V_A(m_0, c_A) = v]$ is given by,

\[
\Pr[V_A(m_0, c_A) = v] = \sum_{c_S, c_R: V_A(m_0, c_A) = v} \Pr[C_S = c_S \land C_R = c_R].
\]

Note that $C_S$ and $C_R$ are independent and have length $(m + \ell)$ and $\ell$ respectively, where $\ell$ is the Hamming weight of the string $B$ and $k$ is the description length of function in $\mathcal{F}$. Hence $\Pr[C_S = c_S \land C_R = c_R] = 1/(2^{(m + \ell) + wk})$; note this value is independent of the value of $m_0$.

Therefore we only need to count the number of executions in which the coin tosses of the sender and the receiver are such that random variable $V_A(m_0, c_A) = v$.

Suppose that $v = (c_A, V_1, V_2, V_3)$ is fixed, it implies that $\text{Cor}$ and $c_A = \{h_i\}_{i=1}^n$ are also determined; then the choices of $\{(r_i, R_i)\} \in \text{Cor}$ should be consistent with $V_2$ and $V_3$. Since $\{\oplus \text{Cor} \}, R_i = V_3 \oplus m_0$, when $m_0, V_3$ are fixed, at most $m - |\text{Cor}| - 1$ elements in $\{R_i\} \in \text{Cor}$ can be selected freely. Moreover, when $V_2$ and $\{R_i\} \in \text{Cor}$ are fixed, $\{r_i\} \in \text{Cor}$ are also determined. Therefore, the number of $C_S, C_R$ result in $V_A(m_0, c_A) = v$ is bounded by the number of $R_i$ for $i \notin \text{Cor}$. Totally, they have $2^{m-|\text{Cor}|^{n-1}}$ different choices. Hence we have,

\[
\Pr[V_A(m_0, c_A) = v] = \frac{2^{m-n(|\text{Cor}|-1)}}{2^{n(m+\ell)+wk}}.
\]

The proof is complete by noting that the above probability is independent of $m_0$. 

• **Complexity:** Since the hash function is polynomial time computable in \( m \), the computation complexity of \( S \) and \( R \) is polynomial in \( n \) and \( m \). For communication complexity, \( H_1 \) needs to communicate \( m + \ell \) bits over each wire, and at most \((4s \log m + \ell + 2)n + m \) bits over the public channel, where \( s = \ell + \log \log m \). If the reliability requirement is set to \( \delta = 2^{-n} = (n-1):2^{1-\ell} \), then \( \ell = \kappa + \log(n-1) + 1 \). The transmission rate over the public channel assuming \( m = \Omega(n^2\kappa^2) \), is \((4s \log m + \ell + 2)n + m)/m \) which is constant asymptotically.

### B. Comparisons with Schemes in \([9], [10]\)

As noted earlier communication over public channel is much more costly than communication over wires, and so minimizing the transmission rate over the public channel will have a large effect on overall efficiency of the protocol. This is particularly important for transmitting long messages. For example in most cases \( \kappa = 30 \) provide sufficient reliability. However messages can be as long as \( 2^{20} \) bits. When \( n = 30 \) wires are available, our proposed protocol transmits around \( 2^{20} \) bits over the public channel with reliability higher than \( 1 - 2^{-30} \) (since \( m > n^2\kappa^2 \)). The protocols in \([9], [10]\) both have transmission rate \( O(n) \) and so need to send almost 30 times data \((30 \times 2^{20} \approx 2^{25}) \) bits over the public channel. The reliability is \( 1 - 2^{-O(m)} = 1 - 2^{-2^{20}} \) in \([9], [10]\), which would be unnecessarily high.

### V. Conclusion and Further Research

In this work we considered round optimality protocols for secure message transmission (SMT) by public discussion. This is an important communication model in realizing almost-everywhere multiparty computation. Since the implementation cost of public channel is high, it is important to minimize transmission over the public channel. Our results show that secure protocol in this model need at least 3 rounds and in 2 of them the public channel must be invoked. We prove this result in a general setting where the invocation of public channel is not known at the start of the protocol and depends on the coin tosses of participants. We describe a round optimal protocol that has constant transmission rate over the public channel and linear transmission rate over other wires.

Existence of PD-adaptive SMT-PD protocols with \( r \geq 4 \) rounds and one round public discussion, and construction of round optimal protocols with optimal communication complexity over wires and public channel (if there exists) are interesting open problems.

### References

[1] T. Araki. “Almost Secure 1-Round Message Transmission Scheme with polynomial-time Message Decryption,” in *Proc. of International Conference on Information Theoretic Security*, ser. Lecture Notes in Computer Science, no.5155, New York: Springer-Verlag, 2008, pp.2-13.

[2] S. Agarwal, R. Cramer, and R. de Haan. “Asymptotically optimal two-round perfectly secure message transmission,” in *Advances in Cryptology - CRYPTO 2006*, ser. Lecture Notes in Computer Science, no.4117, New York: Springer-Verlag, pp.394-408.

[3] M. Ben-Or, S. Goldwasser, and A. Wigderson. “Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract),” *STOC*, pp.1-10, 1988.

[4] D. Chaum, C. Crepeau, and I. Damgård. “Multiparty unconditionally secure protocols (extended abstract),” *FOCS*, pp.11-19, 1988.

[5] D. Dolev, C. Dwork, O. Waarts, and M. Yung. “Perfectly secure message transmission,” *J. ACM*, vol.40, no.1, pp.17-47, 1993.

[6] D. Dwork, D. Peleg, N. Pippenger, and E. Upfal. “Fault tolerance in networks of bounded degree,” *SIAM J. Comput.*, vol.17, no.5, pp.975-988, 1988.

[7] Y. Desmedt and Y. Wang. “Perfectly secure message transmission revisited,” in *Advances in Cryptology-Eurocrypt 02*, ser. Lecture Notes in Computer Science, no.2332, New York: Springer-Verlag, 2002, pp.502-517.

[8] M. Fitzi, M. Franklin, J. Garay, and S. H. Vardhan. “Towards Optimal and Efficient Perfectly Secure Message Transmission,” in *Proc. of TCC 2007*, ser. Lecture Notes in Computer Science, no.4392, New York: Springer-Verlag, 2007, pp.311-322.

[9] M. Franklin, and R. N. Wright. “Secure Communication in Minimal Connectivity Models,” *J. Cryptol.*, vol.13, no.1, pp.9-30, 2000.

[10] J. Garay. “Partially Connected Networks: Information Theoretically Secure Protocols and Open Problems,” *An invited talk in ICITS 2008*, Aug 11, 2008.

[11] J. Garay, R. Ostrovsky. “Almost-everywhere Secure Computation,” in *Advances in Cryptology-Eurocrypt 2008*, ser. Lecture Notes in Computer Science, no.4945, New York: Springer-Verlag, 2008, pp.307-323.

[12] K. Kurosawa and K. Suzuki. “Almost secure (1-round, n-channel) message transmission scheme,” Cryptology ePrint Archive, Report 2007/076, 2007. Available: [http://eprint.iacr.org/](http://eprint.iacr.org/).

[13] K. Kurosawa, and K. Suzuki. “Truly Efficient 2-Round Perfectly Secure Message Transmission Scheme,” in *Advances in Cryptology-Eurocrypt 2008*, ser. Lecture Notes in Computer Science, no.4965, New York: Springer-Verlag, 2008, pp.324-340.

[14] U. Maurer. “Secret key agreement by public discussion from common information,” *IEEE Trans. Inform. Theory*, vol.39, no.3, pp.733-742, 1993.

[15] A. Patra, A. Choudhary, K. Srinathan, and C. Pandu Rangan. “Unconditionally Reliable and Secure Message Transmission in Undirected Synchronous Networks: Possibility, Feasibility and Optimality,” Cryptology ePrint Archive, Report 2008/141, 2007. Available: [http://eprint.iacr.org/2008/141.pdf](http://eprint.iacr.org/2008/141.pdf).

[16] T. Rabin and M. Ben-Or. “Verifiable secret sharing and multiparty protocols with honest majority (extended abstract),” *STOC*, pp.73-85, 1989.

[17] H. Sayeed and H. Abu-Amara. “Efficient perfectly secure message transmission in synchronous networks,” *Information and Communication*, vol.126, no.1, pp.53-61, 1996.

[18] K. Srinathan, A. Narayanan, and C. Pandu Rangan. “Optimal perfectly secure message transmission,” in *Advances in Cryptology-CRYPTO 2004*, ser. Lecture Notes in Computer Science, no.3152, New York: Springer-Verlag, 2004, pp.545-561.

[19] E. Upfal. “Tolerating Linear Number of Faults in Networks of Bounded Degree,” *PODC*, pp.83-89, 1992.

[20] J. Juels. “Oblivious Transfer Amplification,” *Ph.D. dissertation*, ETH, Zürich, 2006. Available: [http://arxiv.org/abs/cs/0608076](http://arxiv.org/abs/cs/0608076).

[21] M. Wegman, J. Carter. “New Hash Functions and Their Use in Authentication and Set Equality,” *J. Comput Syst Sci*, vol.22, no.2, pp.265-279, 1981.

### Appendix

#### A. Proof for Lemma 3

**Proof:** By Definition 1 and Lemma 1 we have: For any algorithm \( D \), any two messages \( m_0, m_1 \in M \), and any adversary \( B \) with randomness \( c_B \in \{0, 1\}^* \),

\[
| Pr[D(V_B(m_0, c_B)) = 1] - Pr[D(V_B(m_1, c_B)) = 1] | \leq \varepsilon,
\]

(7)

where the probability is over the random coins of \( S \) and \( R \). Note here \( V_B(m, c) \) is (the random variable of) the view of \( B \) when the (fixed) message \( m \in M \) is transmitted and \( B \) uses the (fixed) coins \( C_B = c_B \) in the protocol.
Then by taking average over the randomness of $C_B$, the following holds from Eq.\(\text{[4]}\)

\[
\Pr[D(V_B(m_0)) = 1] - \Pr[D(V_B(m_1)) = 1] \leq \varepsilon, \tag{8}
\]

where $V_B(m)$ denotes the view of $B$ when the fixed message $m \in \mathcal{M}$ is transmitted in the protocol, and it is a random variable over the random coins of $S, R$, and $B$.

The adversary’s strategy consists of: selecting messages $(M_0, M_1)$ followed by attacking the protocol and so we write $B = (B_1, B_2)$. We use $C_{B1}$ to denote the random coins used by $B_1$ to select $(M_0, M_1)$. Let $p_0 \overset{\text{def}}{=} \Pr[B_1^{\mathcal{H}(M_0)}(1)]$ and $p_1 \overset{\text{def}}{=} \Pr[B_1^{\mathcal{H}(M_1)}(1)]$. We have,

\[
\begin{align*}
&\Pr[B_1^{\mathcal{H}(M_0)}(1)] - \Pr[B_1^{\mathcal{H}(M_1)}(1)] \\
&= \sum_{C_{B1} = c} \Pr[C_{B1} = c] (p_0 - p_1) \\
&\leq \varepsilon.
\end{align*}
\]

The last step follows from the observation that $|p_0 - p_1| \leq \varepsilon$ due to Eq.\(\text{[3]}\).

B. Proofs Omitted From Theorem 4

As in the proof of Theorem 3, we separate $A$’s random coins into four parts: $(C_{M_A}, C_{A0}, C_{A1}, C_{A2})$. For the sake of clarity, the message selected by $A$ using randomness $C_{M_A}$ is denoted by $M_A$, while the message outputted by $A$ by the end of the protocol is denoted by $M^+_A$.

1) Proof of Lemma 5

The public channel can be used in any of the three rounds. For simplicity, we assume $C_{A0} = 1$, i.e., $A$ selects the last $t$ wires to corrupt. The actions of $A$ is illustrated as in Fig.\(\text{[4]}\) and \(\text{[7]}\) respectively. (We remark that when $C_{A0} = 0$, $A$’s action is similar.) The detail of $A$ selecting $(M_A, C_{A1}, C_{A2})$ when $S$ doesn’t use the public channel in the first round is supplied in Fig.\(\text{[5]}\).

We remark that: (i) When $S$ doesn’t use public channel in round 1 and $\Omega_2 \neq \emptyset$, the strategy as described in Fig.\(\text{[5]}\) ensures that $A$ can produce message $X'_1 Y'_2$ without public channel communication in the second round. (ii) Since $A$ is computationally unbounded, she knows $f_1$ and $f_2$’s function tables and so knows the sets $\Omega_1$ and $\Omega_2$. Thus $A$ can conduct the above attacks.

We analyze the success probability of $A$ in the following. Let $E_1$ and $E_2$ denote the events that $S$ invokes the public channel in round 1 and 3, respectively. Let $E_2$ be the event that $R$ invokes the public channel in round 2. Then $E_1$, $E_2$ and $E_3$ are disjoint events and $\Pr[E_1 \lor E_2 \lor E_3] = 1$ since II is a $(3,1)$-round protocol.

Assume in the first round $S$ sends $X_1 Y_1$ and let the sets $\Omega_1 \subseteq \mathcal{M} \times \{0,1\}^*$ and $\Omega_2 \subseteq \Omega_1 \times \{0,1\}^*$ be defined as

\[
\Omega_1 \overset{\text{def}}{=} \{(m, c_1) \mid f_1(m, c_1) \text{ doesn’t use public channel}\}.
\]

and

\[
\Omega_2 \overset{\text{def}}{=} \{(m, c_1, c_2) \mid (m, c_1) \in \Omega_1, c_2 \in \{0,1\}^* \text{ s.t. } f_2(X'_1 Y_1, c_2) \text{ doesn’t use public channel}\}
\]

We have $(M_S, C_S) \in \Omega_1$. If $\Omega_2 \neq \emptyset$, $A$ randomly chooses $(M_A, C_{A1}, C_{A2}) \leftarrow \Omega_2$; otherwise, $A$ randomly chooses $(M_A, C_{A1}, C_{A2}) \leftarrow \Omega_1 \times \{0,1\}^*$.

Fig. 5. The strategy that $A$ selects $(M_A, C_{A1}, C_{A2})$ when $S$ doesn’t use public channel in round 1.

Claim 4: Let $b \in \{1,3\}$. If $E_b$ occurs, we have

\[
\Pr[M^+_A = M_S \mid E_b] \geq \Pr[M_R = M_S \mid E_b].
\]

Proof: (i) We first prove the case of $b = 1$. Denote by $E_1$ the set of all executions where $E_1$ occurs, and by $S_1 \subseteq E_1$ the set of successful executions in which $R$ outputs $M_R = M_S$.

Define a relation $W_1 \subseteq E_1 \times E_1$, where $(E, E') \in W_1$ if: (i) $M_S, C_S$ remain unchanged in the two executions; (ii) $C_{A0} \oplus C_{A0} = 1$; (iii) $C_{A2} = C_{R'}, C_R = C_{A2}$.

Similar to CASE 1 in Theorem 2, we can prove that $S$ cannot distinguish two swapped executions $(E, E') \in W_1$ and so if $M_R = M_S$, we have $M^+_A = M_S$. Furthermore, we have $p_E = \frac{1}{|E|} 2^{-t - r - r_H} = p_E$, where $\emptyset \subseteq \mathcal{M} \times \{0,1\}^t$ is the set of all $(M_S, C_S)$ such that $E_1$ occurs, and $t, r, r_H, r_R$ denote the length of the randomness used by $S, A, R$, respectively.

We then obtain,

\[
\Pr[M^+_A = M_S \mid E_1] \geq \sum_{E \in E_0} p_E = \sum_{E \in E_0} p_E = \Pr[M_R = M_S \mid E_1].
\]

(ii) When $b = 3$, let $E_3$ be the set of all executions where $E_3$ occurs, and $S_3 \subseteq E_3$ be the set of all successful executions in which $R$ outputs $M_R = M_S$. Define a relation $W_3 \subseteq E_3 \times E_3$, where $(E, E') \in W_3$ if: (i) $M_S, C_S$ and $M_A, C_{A1}$ remain unchanged in the two executions; (ii) $C_{A0} \oplus C_{A0} = 1$; (iii) $C_{A2} = C_{R'}, C_R = C_{A2}$.

Then by a similar proof of CASE 1 in Theorem 2, we have $M^+_A = M_R$.

For any two executions $(E, E') \in W_3$, suppose $(M_S, C_S, C_R, C_A) = (m_S, c_S, c_R, c_A)$ and $(M_S, C_S, C_R, C_A) = (m_S, c_S, c_R, c_A)$. Then the probability that $E$ occurs is $p_E = \Pr[(M_S, C_S) = (m_S, c_S) \land C_R = c_R \land C_A = c_A \mid E_3] = \alpha \cdot \beta$, where $\alpha = \Pr[(M_S, C_S) = (m_S, c_S) \mid E_3]$ and $\beta = \Pr[C_A = c_A \land C_R = c_R \mid (M_S, C_S) = (m_S, c_S) \mid E_3]$. Similarly, it has $p_E = \Pr[(M_S, C_S) = (m_S, c_S) \land C_R = c_R \land C_A = c_A \mid E_3] = \alpha \cdot \beta$, then $\Pr[C_A = c_A \land C_R = c_R \mid (M_S, C_S) = (m_S, c_S) \mid E_3] = \frac{1}{ \Pr[(M_S, C_S) = (m_S, c_S) \mid E_3]}$.
Obviously, it has \( \alpha = \hat{\alpha} \) as \((M_S, C_S) = (M_S, C_S)\). The following is to prove \( \beta = \hat{\beta} \). Since \((M_A, C_A1) = (M_A, C_A1)\), this is equivalent to proving

\[
\Pr[C_{A2} = c_{A2} \land C_R = c_R \mid \mathcal{X}] = \Pr[C_{A2} = c_{A2} \land C_R = c_R \mid \hat{\mathcal{X}}],
\]

where \( \mathcal{X} \) denotes the event that \((M_S, C_S) = (m_S, c_S) \land (M_A, C_A0, C_A1) = (m_A, c_A0, c_A1) \land \mathcal{E}_3\), and \( \hat{\mathcal{X}} \) denotes the event that \((M_S, C_S) = (m_S, c_S) \land (M_A, C_A0, C_A1) = (m_A, c_A0, c_A1) \land \hat{\mathcal{E}}_3\).

Note that \( C_R \) is uniformly selected by \( \mathcal{R} \) and \( C_{A2} \) is selected by \( \mathcal{A} \) in the first round without seeing any information about \( C_R \). Hence \( C_{A2} \) and \( C_R \) are independent. Similarly, \( C_{A2} \) and \( \hat{C}_R \) are independent.

Then Eq.(9) can be expressed as

\[
\Pr[C_{A2} = c_{A2} \mid \mathcal{X}] \Pr[C_R = c_R \mid \mathcal{X}] = \Pr[C_{A2} = c_{A2} \mid \hat{\mathcal{X}}] \Pr[C_R = c_R \mid \hat{\mathcal{X}}].
\]

We thus prove the equality of Eq.(9), which implies that \( p_{E} = p_{\hat{E}} \), and then

\[
\Pr[M^+_A = M_S \mid \mathcal{E}_3] \geq \sum_{E \in S_3} p_E = \Pr[M_R = M_S \mid \mathcal{E}_3].
\]

Claim 5: \( \Pr[M_R \neq M_S \mid M_S \neq M_A \land \mathcal{E}_2] \geq \Pr[M_R = M_S \mid M_S \neq M_A \land \mathcal{E}_2]. \)

Proof: Denote by \( E_2 \) the set of all executions where \( \mathcal{E}_2 \) occurs. Let \( S_2 \subseteq E_2 \) denote the set of executions in which \( \mathcal{R} \) outputs \( M_R = M_S \) given that \( M_A \neq M_S \).

We define a relation \( W_2 \subseteq E_2 \times E_2 \) such that \((E, \hat{E}) \in W_2\) if: (i) \( C_R \) remains unchanged in the two executions; (ii)
\[ C_{A0} \oplus C_{A0} = 1; \] (iii) \( C_{A1} = C_S, CS = C_{A1} \); and (iv) \( MS = M_A, MA = M_S \).

Then \( R \) cannot distinguish two swapped executions \((E, E')\) in \( W_2 \) and if \( E \in S_2 \), we have \( E \notin S_2 \). Moreover, for any \( E \in E_2 \), a proof similar to case (ii) in Claim 4 can be used to prove that \( p_E = p_E \). We thus have,

\[
\Pr[M_R \neq M_S \mid M_S \neq M_A \land E_2] = \Pr[E \notin S_2] \\
\geq \sum_{E \in S_2} p_E \\
= \Pr[M_R = M_S \mid M_S \neq M_A \land E_2],
\]

From Claim 4 and 5, we have

\[
\Pr[M^*_A = M_S] = \Pr[M^*_A = M_S \mid E_1]\Pr[E_1] \\
+ \Pr[M^*_A = M_S \mid E_3]\Pr[E_3] \\
\geq \Pr[M_R = M_S \mid E_1] + \Pr[M_R = M_S \mid E_3]
\]

and

\[
\Pr[M_R \neq M_S] \\
\geq \Pr[M_R \neq M_S \mid E_2]\Pr[E_2] \\
\geq \Pr[M_R \neq M_S \mid M_S \neq M_A \land E_2] \cdot \Pr[M_S \neq M_A \land E_2] \\
\geq \Pr[M_R = M_S \mid M_S \neq M_A \land E_2] \cdot \Pr[M_S \neq M_A \land E_2] \\
= \Pr[M_R = M_S \mid E_2] \\
\geq (1 - \Pr[M_S = 0 \mid M_R = M_S \land E_2]) \\
\geq \Pr[M_R = M_S \mid E_2] - \Pr[M_A = M_S]
\]

Moreover, we also have \( \Pr[M_A = M_S] \leq \varepsilon + \frac{1}{|S|} \), as otherwise by choosing \( M^*_A \) to be \( M_A \), we have \( \Pr[M^*_A = M_S] > \varepsilon + \frac{1}{|S|} \), which contradicts Lemma 2.

Hence, it has

\[
\Pr[M^*_A = M_S] + \Pr[M_R \neq M_S] \\
\geq \Pr[M_R = M_S \land E_1] + \Pr[M_R = M_S \land E_3] \\
\geq \Pr[M_R = M_S \land E_1] + \Pr[M_R = M_S \land E_3] - \Pr[M_A = M_S] \\
= \Pr[M_R = M_S] - \Pr[M_A = M_S],
\]

Thus, by noting that \( \Pr[M^*_A = M_S] \leq \varepsilon + \frac{1}{|S|} \) and \( \Pr[M_S \neq M_R] \leq \delta \), we get \( \varepsilon + \delta \geq \frac{1}{2} - \frac{1}{|S|} \).

2) Proof of Lemma 6 Assume \( C_{A0} = 1 \), we illustrate \( A \)'s strategy as follows.

Round 1: (i) If \( R \) uses public channel, \( A \) just blocks the \( t \) corrupted wires. Then \( A \) selects \((M_A, C_{A1}) \leftarrow M \times \{0,1\}^*\), and sets \( C_{A2} = \perp \).

(ii) Otherwise, assume \( R \) sends out \( X_1 Y_1 \). Consider the following two sets

\[
\Omega_1 \overset{\text{def}}{=} \{c \mid c \in \{0,1\}^* \text{ s.t. } f_1(c) \text{ involves no public channel communication}\},
\]

\[
\Omega_2 \overset{\text{def}}{=} \{c \mid c \in \Omega_1 \text{ s.t. } f_2(c) \text{ involves no public channel communication}\}.
\]

Obviously, \( C_R \in \Omega_1 \). Then if \( |\Omega_2| > 0 \), \( A \) selects \( C_{A2} \leftarrow \Omega_2 \); otherwise, selects \( C_{A2} \leftarrow \Omega_1 \). \( A \) also chooses \((M_A, C_{A1}) \leftarrow M \times \{0,1\}^*\), then computes \( X'_1 Y'_1 = f_1(C_{A2}) \) and replaces \( Y_1 \) by \( Y'_1 \).

Round 2: (i) If \( R \) uses public channel in this round or public channel has been used in round 1, \( A \) just blocks the corrupted wires. (ii) Otherwise, suppose \( R \) responses \( X_2 Y_2 \), it has \( C_R \in \Omega_2 \), then the selection of \( C_{A2} \) ensures that \( A \) can produce message \( X'_2 Y'_2 \) without public channel communication. \( A \) thus replaces \( Y_2 \) by \( Y'_2 \).

Round 3: (i) If \( S \) sends out \( P_3 X_3 Y_3, A \) just blocks \( Y_3 \), and computes \( M^*_A = g(P_3 Y_3, C_{A2}) \). (ii) Otherwise, assume \( S \) sends out \( X_3 Y_3 \), it implies that public channel has been used in the first two rounds, \( A \) thus computes \( X'_3 Y'_3 \) and replaces \( Y_3 \) by \( Y'_3 \).

Then by a similar calculation of Eq. (10) and (11), we get

\[
\Pr[M_R \neq M_S] \\
\geq \Pr[M_R = M_S \land E_1] + \Pr[M_R = M_S \land E_2] - 2 \Pr[M_S = M_A]
\]

and

\[
\Pr[M^*_A = M_S] \geq \Pr[M^*_A = M_S \land E_3] \\
\geq \Pr[M_R = M_S \land E_3],
\]

where \( E_1, E_2 \) denote the events that \( R \) uses the public channel in round 1 and 2 respectively, and \( E_3 \) denotes the event that \( S \) uses the public channel in round 3. Finally we obtain \( 3\varepsilon + 2\delta \geq 1 - \frac{3}{|S|} \).

3) Proof of Lemma 7 \( A \)'s strategy with \( C_{A0} = 1 \) is described as follows.

Round 1: (i) If \( R \) does not use the public channel in round 1, it says \( S \) will be the invoker of public channel, thus \( A \) just blocks the corrupted wires. (ii) Otherwise, \( A \) chooses \((M_A, C_{A1}) \leftarrow M \times \{0,1\}^*\) and computes \( X'_1 Y'_1 \) and \( X'_2 Y'_2 \), then modifies the corrupted wires.

We note that the impossibility proof in this scenario is similar to Lemma 5 and thus omit it here.