

# Price of Low Communication Followup

Authors

matan.shtepel@gmail.com, nakulkhambhati@ucla.edu

**Abstract.** Follow up on the Price of Low Communication

## 1 Model: Low communication and mobile adversaries

For the mobile setting, as in the adaptive one, we adopt the natural model in which each of the operations “send-message,” “receive-message,” and “erase-messages from state” are atomic. One modification from the original paper is that instead of dividing rounds into “mini-rounds”, where parties can exclusively send, receive or erase a message, we enforce that the parties operate in rounds that alternate between “receive and then send” and “erase”. When  $P_i$  sends a message  $m$  to  $P_j$ , a record of that message is stored in the internal states of both parties. We assume that this record cannot be falsified. The party set  $\mathcal{P} = \mathcal{S} \cup \mathcal{C}$  where  $\mathcal{S} = \{s_1, \dots, s_n\}$  is the set of servers and  $\mathcal{C} = \{c_0, c_1\}$  is the set of clients.

The execution is divided into rounds: in an odd round  $2\rho + 1$ , all parties  $P$  receive any messages sent to them by any party  $P'$  at round  $2\rho - 1$ , perform computation, then sends messages to any other parties. In any even round  $2\rho + 2$ , any party in  $P$  can erase messages from its internal state. The erasure is atomic and completes at the end of the round. The protocol can go on for  $\text{poly}(n)$  rounds.

Should we also consider an adversary that cannot corrupt during erasure rounds?

A  $(t, \lambda)$  mobile adversary  $\mathcal{A}$  can have at most  $t$  parties corrupted simultaneously. As a part of the model, we impose that, at the end of each round,  $\mathcal{A}$  can only decorrupt  $\lambda$  fraction of his servers to study how the corruption bound varies with  $\lambda$ . If at the beginning of round  $i$ ,  $\mathcal{A}$  controls  $\tau_{i-1} \leq t$  parties then we allow  $\mathcal{A}$  to instantaneously decorrupt up to  $\min\{\lambda t, \tau_{i-1}\}$  at the end of the round. At the end of every round  $\mathcal{A}$  can decorrupt up to  $\lambda t$  servers. In analogy to rushing adversaries in the standard model, if  $P_i$  is corrupted under  $\mathcal{A}$ 's control in round  $2\rho$  and in round  $2\rho - 1$   $P_j$  sent  $P_i$  a message, that message will be available to  $\mathcal{A}$  at the beginning of round  $2\rho$  (where it would only be available to  $P_j$  at the beginning of round  $2\rho + 1$ ). This way,  $\mathcal{A}$  sees messages sent to corrupted servers a round before the servers receive them.

We need to specify when/how  $\mathcal{A}$  computes its next corruptions. As described here,  $\mathcal{A}$  computes statically i.e. at the end of round  $\rho$  it computes  $\mathcal{C}_{\rho+1}$  as a function of the views of parties in  $\mathcal{C}_\rho$ . What we could also look at is a stronger adversary that computes dynamically in the sense that in round  $\rho$  it has corrupted  $s$  that has a reference to  $s'$  which has a reference to  $s''$ . The stronger

$\mathcal{A}$  here can corrupt both  $s'$  and  $s''$  in round  $\rho + 1$ . I think this doesn't make sense practically: to see the view of  $s'$  it needs to corrupt it which can only happen in  $\rho + 1$  which means that the earliest it can corrupt  $s''$  is in round  $\rho + 2$ . However, this much stronger adversary only delays the protocol by two rounds so it's worth stating this result as well.

## 2 Results

Here we should include a table of our results in the low communication setting: Upper and lower bounds for semihonest and malicious – static, adaptive, mobile. We should separate mobile into two types of adversary Type A and Type B and list values for  $\lambda = 1/4, 1/2, 3/4, 1$ . Also maybe include different erasure models (the uninteresting simultaneous erase and send as well).

## 3 Technical Overview

### 3.1 Semi-Honest Mobile upper bound

Much of the proof can be reused for both Type A and Type B adversaries. The protocol and calculations will be different. Currently, calculations have been done for Type B (our mistake). We should first present Type A's (133) protocol, explain why it wouldn't work for Type B and then present the (135) protocol WITH DIAGRAMS.

In this section, we give a short summary with main ideas which go into proving the semi-honest mobile upper bound, but first, we state it informally.

For some polynomial  $\mathfrak{P}_\lambda(x)$  (defined in Theorem 2) let  $\theta(\lambda)$  be the (unique, determined by  $\lambda = 0$ ) solution to

$$\mathfrak{P}_\lambda(x) = 0 \tag{1}$$

**Theorem 1 (Informal Theorem 2).** *Let  $\lambda \in [0, 1]$ . There exists protocol  $\Pi_{sh}^{mob}$  computing the OT functionality in the  $(2, n)$ -client/server model with erasures in the presence of a mobile  $(t, \lambda)$ -adversary  $A/B$  (where  $\lambda t$  is the number of parties that can be decorrputed at the end of every round) with  $t < (\theta(\lambda) - \epsilon)n$  for any  $\epsilon$  where  $0 < \epsilon < \theta(\lambda)$ . Moreover,  $\Pi_{sh}^{mob}$  communicates  $O(\log^\delta n)$  bits.*

Here  $\Pi_{sh}^{mob}$  is nearly the same semi-honest adaptive protocol given in [GIOZ17] (server wakes up with small probability, generate OT-pair, send half to an intermediary, they both erase, and then send to a different client).

I know this is a summary but there's no flow and needs to be fixed. We begin by defining some needed notation. Let  $c_\alpha$  denote the corrupted client where  $\alpha \in \{0, 1\}$ ,  $m_1^{(b)}, \dots, m_g^{(b)}$  be the messages recieved by  $c_b$  throughout the execution of the protocol,  $\mathcal{S}_1$  the set of parties that volunteer in round 1,  $g = |\mathcal{S}_1|$ ,

and  $\mathcal{S}_2$  be the set of servers that receive at least one message from a server in  $\mathcal{S}_1$ . Let  $\mathcal{O}^{\mathcal{A}}$  be the set indexing the OT pairs learned by  $\mathcal{A}$ , that is

$$\mathcal{O}^{\mathcal{A}} = \{j | \exists \rho \text{ s.t. } m_j^{2-\alpha} \text{ is in the view of } s_k \text{ in round } \rho \text{ where } k \in \mathcal{C}_\rho\} \subset [|\mathcal{S}_1|]$$

where  $\mathcal{C}_\rho$  is the set of parties corrupted at the start of round  $\rho$ . Observe that if  $m_i^{(2-\alpha)}$  is not in the adversary's view at any point in the protocol's execution, the adversary's view is information-theoretically independent of  $m_j^{(1-\alpha)}$ . Thus, by the security of the OT-combiner [HKN<sup>+</sup>05], to show the protocol is secure we must show that for all  $(t, \lambda)$  adversaries  $\mathcal{A}$

$$\Pr \left[ |\mathcal{O}^{\mathcal{A}}| \geq \frac{|\mathcal{S}_1|}{2} \right] \leq \text{negl}(n)$$

We divide the rest of the proof into 3 parts and overview the main ideas of each part below:

- (a) Describe  $(t, \lambda)$  adversary  $\mathcal{A}^\dagger$  (corrupt  $t$  random servers in round 1, decorrupt  $\lambda t$  random servers in every other round, if a corrupted server sends / receives a message from another server corrupt the other server) and prove (Lemma 1) that protocol  $\Pi_{\text{sh}}^{\text{mob}}$  tolerates  $\mathcal{A}^\dagger$ . That is,

$$\Pr \left[ |\mathcal{O}^{\mathcal{A}^\dagger}| \geq \frac{|\mathcal{S}_1|}{2} \right] \leq \text{negl}(n)$$

This part of the proof follows a similar outline to the first half of the semi-honest adaptive upper bound of [GIOZ17]: we isolate out an overconnected set of servers who receive multiple message, bound its size, and give it to the  $\mathcal{A}^\dagger$  for free. After removing the overconnected set, the communication graph is a bipartite matching and it is possible to compute the probability  $\mathcal{A}^\dagger$  corrupts a given OT-pair. We conduct these computations (which are more complex in the mobile than the adaptive setting and requires careful probabilistic and analytic justification) and find that when  $t < (\theta(\lambda) - \epsilon)n$  where  $\theta(\lambda)$  is the root of some not-so-simple polynomial

$$\Pr \left[ |\mathcal{O}^{\mathcal{A}^\dagger}| \geq \frac{|\mathcal{S}_1|}{2} \right] \leq \text{negl}(n)$$

is satisfied.

- (b) Prove (Lemma 2) that  $\mathcal{A}^\dagger$  is at least as strong as any other adversary with the same corruption budget. That is, for all  $(t, \lambda)$  adversaries  $\mathcal{A}$ ,

$$\Pr \left[ |\mathcal{O}^{\mathcal{A}^\dagger}| \geq \frac{|\mathcal{S}_1|}{2} \right] \geq \Pr \left[ |\mathcal{O}^{\mathcal{A}}| \geq \frac{|\mathcal{S}_1|}{2} \right]$$

A mobile adversary can corrupt according to many more different “strategies” than an adaptive adversary can, and thus to show that  $\mathcal{A}^\dagger$  is in “optimal” we must deviate significantly from the adaptive upper bound in

[GIOZ17]. We begin the proof by contradiction and assume there exists an adversary  $\mathcal{A}$  s.t.

$$\Pr \left[ |\mathcal{O}^{\mathcal{A}}| \geq \frac{|\mathcal{S}_1|}{2} \right] > \Pr \left[ |\mathcal{O}^{\mathcal{A}^\dagger}| \geq \frac{|\mathcal{S}_1|}{2} \right]$$

Through a series of 5 propositions, we show that wlog, we may assume  $\mathcal{A}$  “behaves like  $\mathcal{A}^\dagger$ ” in various ways (e.g. other than corrupting servers that send it messages,  $\mathcal{A}$ ’s corruptions are independent of its view). Each proposition proceeds somewhat differently, but in general they aim to show that when we modify  $\mathcal{A}$  in various ways (to be more like  $\mathcal{A}^\dagger$ )

$$\Pr \left[ |\mathcal{O}^{\mathcal{A}}| \geq \frac{|\mathcal{S}_1|}{2} \right]$$

only increases.

- (c) Show (Lemma 3) that except from with negligible probability and for some constant  $c$ ,  $\Pi_{\text{sh}}^{\text{mob}}$  communicates at most  $O(\log^c n)$  bits. This is obtained via a simple Chernoff bound on the probability each server wake up.

These lemmas trivially combine to prove our theorem.

## 4 Upper bound for Mobile adversaries

In this section, we give an upper bound for the semi-honest, mobile-adversary (A/B) sublinear-communication, information-theoretic, with erasures setting. We begin by describing our model, which offers slight but necessary modifications to the mobile setting from [GIOZ17].

### 4.1 The protocol

We present a protocol that allows clients  $c_0$  and  $c_1$  to compute a 1-out-of-2 OT functionalities  $f_{\text{OT}}((m_0, m_1), b) = (\perp, m_b)$  in the  $(2, n)$ -client/server model with sublinear communication complexity (Figure 1). The completeness of OT ensures that this allows  $c_0$  and  $c_1$  to compute any given function. The protocol is similar to the one presented in [GIOZ17] for the adaptive case with a minor modification: each server in the set that decides to volunteer *randomly* chooses which component of the OT pair to send to the intermediary server. In Theorem 2, we prove  $\Pi_{\text{sh}}^{\text{mob}}$  can tolerate  $(t, \lambda)$  adversary for  $t$  less than the root of a polynomial  $\mathfrak{P}_\lambda$  described in Figure 2. **This is (135), we also want to present (133).** For example for  $\lambda = 0, 1/7, 1/2, 1$ ,  $\Pi_{\text{sh}}^{\text{mob}}$  can tolerate a  $(t, \lambda)$  adversary with  $t$  less than  $0.293n, 0.214n, 0.125n, 0.079n$ , respectively.<sup>1</sup> Notice that for  $\lambda = 0$  we recover the semi-honest adaptive upper bound of [GIOZ17][Thm #], as desired.

<sup>1</sup> The bound of 0.293 for  $\lambda = 0$  is a numerical approximation of  $1 - \sqrt{0.5}$  presented in [GIOZ17]

**Protocol  $\Pi_{sh}^{mob}$** 

Recall that we enforce that rounds alternate between “receive & send” and “erase”.

1. Every server  $s_i \in \mathcal{S}$  locally decides to become active with probability  $p = \frac{\log^\delta n}{n}$  for a publicly known constant  $\delta > 1$ . Let  $\mathcal{S}_1$  denote the set of parties that become active in this round. Every  $s_i \in \mathcal{S}_1$  prepares an OT pair  $((m_i^{(0)}, m_i^{(1)}), \text{otid}_i)$ , where  $\text{otid}_i \in \{0, 1\}^{\log^\delta n}$  **shouldn't log log n suffice?** is a uniformly chosen identifier. Every  $s_i \in \mathcal{S}_1$  chooses an intermediary  $s_{ij} \in \mathcal{S}$  as well as  $\sigma_i \in \{0, 1\}$  uniformly at random and sends  $(\sigma_i, m_i^{\sigma_i}, \text{otid}_i)$  to  $s_{ij}$ . Denote by  $\mathcal{S}_2 = \{s_{ij} | s_i \in \mathcal{S}_1\}$  the set of all relayers.
2. Every  $s_i \in \mathcal{S}_1$  erases  $m_i^{\sigma_i}$ , the identity of  $s_{ij}$  and the randomness used to select  $s_{ij}$ .
3. Every  $s_{ij} \in \mathcal{S}_2$  receives  $(m_i^{\sigma_i}, \text{otid}_i)$ . Every  $s_i \in \mathcal{S}_1$  sends  $(m_i^{1-\sigma_i}, \text{otid}_i)$  to  $c_{1-\sigma_i}$ .
4. Every  $s_i \in \mathcal{S}_1$  erases its entire internal state. Every  $s_{ij} \in \mathcal{S}_2$  erases the identity of  $s_i$ .
5. Every  $s_{ij} \in \mathcal{S}_2$  sends  $(m_i^{\sigma_i}, \text{otid}_i)$  to  $c_{\sigma_i}$ .
6. Every  $s_{ij} \in \mathcal{S}_1$  erases its entire internal state.
7. The clients  $c_1$  and  $c_2$  use the OT pairs with matching **otid**'s within a (semi-honest)  $(n/2, n)$  OT-combiner to obtain a secure OT pair.

**Fig. 1.** A protocol to compute OT in the presence of mobile semi-honest adversaries.

**Theorem 2.** Fix  $0 \leq \lambda \leq 1$ . Protocol  $\Pi_{sh}^{mob}$  unconditionally securely computes the functionality  $f_{OT}((m_0, m_1), b) = (\perp, m_b)$  in the  $(2, n)$ -client/server model with erasures in the presence of a mobile  $(t, \lambda)$ -adversary (where  $\lambda t$  is the number of parties that can be decorruped at the end of every round) with  $t < (\theta(\lambda) - \epsilon)n$ .  $\theta(\lambda)$  is the solution to

$$\mathfrak{P}(x) = \sum_{i=0}^{10} a_i(\lambda) x^i = 0 \quad (2)$$

for  $a_i$  given in Figure 2 and for any  $\epsilon$  where  $0 < \epsilon < \theta(\lambda)$ . Moreover,  $\Pi_{mob}^{OT}$  communicates  $O(\log^\delta n)$  bits for some  $\delta > 1$ , except with negligible probability.

*Proof.* We begin by defining the notation that will carry us through the proof. Let  $c_\alpha$  denote the corrupted client where  $\alpha \in \{0, 1\}$ . For  $b \in \{0, 1\}$  let  $m_1^{(b)}, \dots, m_g^{(b)}$  be the messages recieved by  $c_b$  throughout the execution of the protocol. Let  $\mathcal{S}_1$  the set of parties that volunteer in round 1, and let  $\mathcal{S}_2$  be the set of servers that recieve at least one message from a server in  $\mathcal{S}_1$ . Let  $\mathcal{C}_\rho^{\mathcal{A}} \subset [n]$  denote the indices of servers corrupted by  $\mathcal{A}$  at the start of round  $\rho$ . Let  $\mathcal{C}_\rho^{\mathcal{A}} \subset [n]$  be the indices of corrupted servers after  $\mathcal{A}$  makes its round  $\rho$  corruptions and before it makes its round  $\rho$  decorrupations which, in turn, are denoted  $D_\rho^{\mathcal{A}} \subset \mathcal{C}_\rho^{\mathcal{A}} \subset [n]$ . As a sanity

Coefficient	Value
$a_0$	$-0.5$
$a_1$	$11.5\lambda + 6.0$
$a_2$	$-47.5\lambda^2 - 61.5\lambda - 15.0$
$a_3$	$110.3\lambda^3 + 251.5\lambda^2 + 152.5\lambda + 28.0$
$a_4$	$-140.9\lambda^4 - 535.0\lambda^3 - 568.8\lambda^2 - 232.5\lambda - 35.0$
$a_5$	$84.5\lambda^5 + 592.5\lambda^4 + 1016.8\lambda^3 + 708.0\lambda^2 + 227.5\lambda + 28.0$
$a_6$	$-0.9\lambda^6 - 308.0\lambda^5 - 907.5\lambda^4 - 968.3\lambda^3 - 510.8\lambda^2 - 136.5\lambda - 14.0$
$a_7$	$-24.5\lambda^7 + 24.9\lambda^6 + 366.0\lambda^5 + 612.3\lambda^4 + 468.3\lambda^3 + 201.0\lambda^2 + 45.5\lambda + 4.0$
$a_8$	$10.8\lambda^8 + 38.0\lambda^7 - 38.2\lambda^6 - 161.3\lambda^5 - 160.8\lambda^4 - 92.0\lambda^3 - 33.5\lambda^2 - 6.5\lambda - 0.5$
$a_9$	$-1.8\lambda^9 - 14.6\lambda^8 - 12.6\lambda^7 + 17.8\lambda^6 + 19.9\lambda^5 + 4.5\lambda^4$
$a_{10}$	$1.8\lambda^9 + 3.8\lambda^8 - 0.9\lambda^7 - 3.6\lambda^6 - 1.1\lambda^5$

**Fig. 2.** Table of coefficients for  $\mathfrak{P}(x)$  as referenced in Theorem 2 and derived in [ref](#)

check, note that for any round  $\rho$  we get that

$$\mathcal{C}_\rho = \mathcal{C}_{\rho-1} \cup (C_\rho \setminus D_{\rho-1})$$

where we set  $\mathcal{C}_0 = D_0 = \emptyset$  so that the formula holds for  $\mathcal{C}_1$  as well.

**Definition 1 (OT pairs learned by  $\mathcal{A}$ ).** Let  $\mathbb{V}_\rho(s)$  denote the view of server  $s$  at the end of round  $\rho \in \mathbb{N}$  and let  $\mathcal{O}^\mathcal{A}$  be the (random) variable indexing the OT pairs learned by  $\mathcal{A}$  during the execution of the protocol. Formally,

$$\mathcal{O}^\mathcal{A} = \left\{ j \in [n] \mid \exists \rho \in \mathbb{N}, \exists k \in \mathcal{C}_\rho : m_j^{(1-\alpha)} \in \mathbb{V}_\rho(s_k) \right\}$$

*Remark 1.* In the above definition, it is implicit that  $\mathcal{A}$  learns all of the OT pair components  $m_j^{(\alpha)}$  sent to the corrupted client  $c_\alpha$  so to learn the OT pair  $(m_j^{(0)}, m_j^{(1)})$ , it needs to learn  $m_j^{(1-\alpha)}$ .

We will omit the  $\mathcal{A}$  superscript when it is clear from context. Observe that if  $m_j^{(1-\alpha)}$  is not in the adversary's view at any point in the protocol's execution, the adversary's view is information-theoretically independent of  $m_j^{(1-\alpha)}$ . Thus, by the security of the OT-combiner [HKN<sup>+</sup>05], to show the protocol is secure we must show that for all  $(t, \lambda)$  adversaries  $\mathcal{A}$ <sup>2</sup>

$$\Pr \left[ |\mathcal{O}^\mathcal{A}| \geq \frac{|\mathcal{S}_1|}{2} \right] \leq \text{negl}(n)$$

We divide the rest of the proof into 3 parts:

- (a) Describe  $(t, \lambda)$  adversary  $\mathcal{A}^\dagger$  (Definition 2) and prove (Lemma 1) that protocol  $\Pi_{\text{sh}}^{\text{mob}}$  tolerates  $\mathcal{A}^\dagger$ . That is,

$$\Pr \left[ |\mathcal{O}^{\mathcal{A}^\dagger}| \geq \frac{|\mathcal{S}_1|}{2} \right] \leq \text{negl}(n)$$

<sup>2</sup> All probabilities in this proof are over the randomness of the servers, clients, and the adversary.

- (b) Prove (Lemma 2) that  $\mathcal{A}^\dagger$  is at least as strong as any other adversary with the same corruption budget. That is, for all  $(t, \lambda)$  adversaries  $\mathcal{A}$ ,

$$\Pr \left[ |\mathcal{O}^{\mathcal{A}^\dagger}| \geq \frac{|\mathcal{S}_1|}{2} \right] \geq \Pr \left[ |\mathcal{O}^{\mathcal{A}}| \geq \frac{|\mathcal{S}_1|}{2} \right]$$

- (c) Show (Lemma 3) that except from with negligible probability and for some constant  $c$ ,  $\Pi_{\text{sh}}^{\text{mob}}$  communicates at most  $O(\log^c n)$  bits .

These lemmas trivially combine to prove our theorem.

**Definition 2 (Description of  $\mathcal{A}^\dagger$ ).** *An adversary  $\mathcal{A}^\dagger$  operates as follows. If  $s_k$ , where  $k \in \mathcal{C}_\rho$ , receives a message from or sends a message to  $s_l$ , then  $\mathcal{A}^\dagger$  corrupts  $s_l$  at the beginning of round  $\rho + 1$  (unless it is already corrupted). We call this behavior acting on references and denote the set of servers corrupted by references in round  $\rho$  as  $R_\rho$  and the set of servers corrupted by reference up to and including round  $\rho$  as  $\mathcal{R}_\rho$ .*

*In addition to corrupting by reference, at the beginning of round 1,  $\mathcal{A}^\dagger$  corrupts  $t$  servers at random. At the beginning of round  $\rho = 2, \dots, 6$ ,  $\mathcal{A}^\dagger$  corrupts  $\lambda t$  random servers from  $\mathcal{S} \setminus \bigcup_{i=1}^{\rho-1} \mathcal{C}_i$ . At end of round  $\rho = 1, \dots, 6$ ,  $\mathcal{A}^\dagger$  decorrupts  $\lambda t$  parties at random from  $\mathcal{C}_\rho \setminus \mathcal{R}_\rho$ .*

Before proceeding to Lemma 1, we show that  $\mathcal{A}^\dagger$  is a legal  $(\lambda, t)$  adversary.

**Proposition 1.** *Except from with negligible probability in  $n$ ,  $\mathcal{A}^\dagger$  does not exceed the  $(\theta(\lambda) - \epsilon)n$  corruption bound.*

*Proof.* Let  $\epsilon = ((\theta(\lambda) - \epsilon)n - t)/2 > 0$ . By Lemma 3, for some constant  $\delta$ , except from with negligible probability, at most  $\log^\delta n$  messages are sent in the protocol. For sufficiently large  $n$ ,  $\epsilon > \log^\delta n$ . Thus we have that  $\mathcal{A}^\dagger$  makes at most  $\epsilon + t < t' < (\theta(\lambda) - \epsilon)n$  corruptions, not exceeding its budget for sufficiently large  $n$ .

**Lemma 1.**  *$\mathcal{A}^\dagger$  is tolerable by  $\Pi_{\text{sh}}^{\text{mob}}$*

*Proof.* As discussed above, by the security of OT-combiners, it is sufficient to show that

$$\Pr \left[ |\mathcal{O}^{\mathcal{A}}| \geq \frac{|\mathcal{S}_1|}{2} \right] \leq \text{negl}(n)$$

To show this, we begin by following [GIOZ17] and isolate an “over-connected” subset of servers  $\mathcal{S}^{\text{overconnected}} \subset \mathcal{S}$  for which we will not give strong corruption bounds.

**Definition 3 (over-connected servers).** *Let  $E = \{\{s, s'\} | s \in \mathcal{S}_1 \wedge s' \in \mathcal{S}_2\}$  and let  $G$  denote the graph with vertex-set  $\mathcal{S}$  and edge-set  $E$ . We say that server  $s$  is an over-connected server if  $\{s, s'\}, \{s, s''\} \in E$  for  $s' \neq s''$ .*

In [GIOZ17][Lemma 1], Garay et al show that for all  $\epsilon, \epsilon' > 0$  and for sufficiently large  $n$   $|\mathcal{S}^{\text{overconnected}}| < \epsilon |\mathcal{S}_1| \leq \epsilon' n$  except from with negligible probability. Thus, intuitively, the set is small enough that we can “give up” all the servers in  $\mathcal{S}^{\text{overconnected}}$  to the adversary, constructing a strictly stronger adversary  $\mathcal{A}^\dagger$ , which we will show  $\Pi_{\text{sh}}^{\text{mob}}$  can still tolerate. From now on, Let  $\mathcal{A}^\dagger$  denote the strictly stronger adversary that gets  $\mathcal{S}^{\text{overconnected}}$  as input, corrupts the servers in  $\mathcal{S}^{\text{overconnected}}$  at the beginning of round 1 and proceeds as  $\mathcal{A}^\dagger$  would otherwise (including all of  $\mathcal{A}^\dagger$ ’s round 1 corruptions).

Having taken all the the servers in  $\mathcal{S}^{\text{overconnected}}$  to be corrupted, we can now proceed with a much simpler analysis. In particular, observe that  $\mathcal{S}_1 \setminus \mathcal{S}^{\text{overconnected}}$  and  $\mathcal{S}_2 \setminus \mathcal{S}^{\text{overconnected}}$  form a perfect matching, with  $s_i$  sending a message to a unique  $s_{ij}$ . For  $s_i \in \mathcal{S}_1 \setminus \mathcal{S}^{\text{overconnected}}$  let  $X_i$  denote the random Boolean variable with  $X_i = 1$  if  $i \in \mathcal{O}^\mathcal{A}$ , (i.e. the event where  $\mathcal{A}^\dagger$  learns  $m_j^{(1-\alpha)}$ ) and  $X_i = 0$  otherwise. Since the corruption pattern is random and communication is random, we have that  $\Pr[X_i = 1] = \Pr[X_j = 1]$  for all  $i, j$ . So we will compute  $\Pr[X_i = 1]$  and use it to compute  $\Pr[|\mathcal{O}^\mathcal{A}| \geq \frac{|\mathcal{S}_1|}{2}]$  via a Chernoff bound. For this purpose, let  $X_i^{(\rho)} = 1$  if  $s_i$  or  $s_{ij}$  (whichever holds  $m_j^{(1-\alpha)}$  **we need to make this more rigorous**) is in  $C_\rho$  and  $X_i^{(r)} = 0$  for all  $r < \rho$ , else  $X_i^{(\rho)} = 0$ .

Then,

$$X_i = \sum_{\rho \in [6]} X_i^{(\rho)}.$$

Since  $X_i = 0$  if and only if  $X_i^{(\rho)} = 0$  for all  $\rho \in [6]$ ,

$$\Pr[X_i = 1] = 1 - \Pr \left[ \sum_{\rho \in [6]} X_i^{(\rho)} = 0 \right]. \quad (3)$$

We rewrite this in terms of probabilities that we can more easily calculate by conditioning

$$\Pr \left[ \sum_{\rho \in [6]} X_i^{(\rho)} = 0 \right] = \Pr \left[ X_i^{(6)} = 0 \mid \sum_{\rho \in [5]} X_i^{(\rho)} = 0 \right] \cdot \Pr \left[ \sum_{\rho \in [5]} X_i^{(\rho)} = 0 \right] \quad (4)$$

Recursively applying 4 and substituting the result in 3, we get

$$\begin{aligned} \Pr[X_i = 1] &= 1 - \prod_{\rho \in [6]} \Pr \left[ X_i^{(\rho)} = 0 \mid \sum_{k \in [\rho-1]} X_i^{(k)} = 0 \right] \\ &= 1 - \prod_{\rho \in [6]} (1 - p_\rho) \end{aligned}$$

where  $p_\rho$  denotes  $\Pr[X_i^{(\rho)} = 1 \mid \bigcap_{k \in [\rho-1]} X_i^{(k)} = 0]$ .

**All of this needs to be revised.** Notice  $p_i$  is a (rational) function. We calculate  $p_1$  through  $p_6$ , giving the details in Appendix A. Let  $\mathfrak{P}, r$  be the (unique)



relatively prime polynomials such that

$$1 - \prod_{\rho \in [6]} (1 - p_\rho) = \frac{\mathfrak{P}}{r} + \frac{1}{2}$$

We detail the computation of  $\mathfrak{P}$  in Appendix B and list the coefficients of  $\mathfrak{P}(x)$  in Table 2<sup>3</sup>. Recall  $\theta(\lambda)$  was chosen such that  $\mathfrak{P}(\theta(\lambda)) = 0$  ( $\lambda$  fixed in Theorem 2's statement). In Appendix B we show that  $r(\theta(\lambda)) - \epsilon$  is bounded away from 0 in the positive direction for all  $0 < \epsilon < \theta(\lambda)$ . By [GIOZ17][Theorem 3] we know that  $\theta(0) = 1 - \sqrt{1/2}$  and when  $\lambda = 0$ , we see that  $\mathfrak{P}(1 - \sqrt{1/2}) = 0$ . Since  $\theta(\cdot)$  is continuous justify later we know how to calculate it from  $\mathfrak{P}$ .

Since  $a_1(\lambda) > 0$  (Table 2) we have that  $\frac{d\mathfrak{P}(x)}{dx} \Big|_{x=\theta(\lambda)} > 0$  for all  $\lambda, \theta(\lambda) > 0$ . Thus,

$$\mathfrak{P}(\theta(\lambda) - \epsilon) \leq \mathfrak{P}(\theta(\lambda)) - q(\epsilon) \tag{5}$$

for some  $q(\cdot) > 0$  for  $\cdot > 0$ , for all  $\theta(\lambda) > \epsilon > 0$  which implies (Eq 2, Eq 5)

$$\begin{aligned} \Pr[X_i = 1] &\leq \frac{\mathfrak{P}(\theta(\lambda)) - q(\epsilon)}{r(\theta(\lambda) - \epsilon)} + \frac{1}{2} \\ &= \frac{1}{2} - \frac{q(\epsilon)}{r(\theta(\lambda) - \epsilon)} < \frac{1}{2} \end{aligned}$$

Because the  $X_i$ 's are independent, the assumptions in [GIOZ17][Theorem 8] are satisfied for  $\delta = \frac{1}{2} - f(\epsilon)$ , where  $f(\epsilon)$  denotes  $\frac{q(\epsilon)}{r(\theta(\lambda) - \epsilon)}$ . Hence,

$$\Pr \left[ \sum_{i \in \mathcal{S}_1 \setminus \mathcal{S}'} X_i \geq (1/2 - f(\epsilon))|\mathcal{S}_1 \setminus \mathcal{S}'| \right] \leq e^{-nf(\epsilon)/2}$$

Recall that we have given the overconnected set to  $\mathcal{A}^\dagger$  for free and, by [GIOZ17][Lemma 1], for large enough  $n$ , except for some negligible probability  $\mu$ ,  $|\mathcal{S}'| < \epsilon'|\mathcal{S}_1|$  so we can write

$$|\mathcal{O}^{\mathcal{A}^\dagger}| = \sum_{i \in \mathcal{S}_1 \setminus \mathcal{S}'} X_i + \epsilon' n$$

Finally, for sufficiently large  $n$ , for some  $f'(\epsilon) > 0$  we have

$$\Pr \left[ |\mathcal{O}^{\mathcal{A}^\dagger}| \geq (1/2 - f'(\epsilon))|\mathcal{S}_1| \right] \leq e^{-nf'(\epsilon)/2} + \mu$$

which is negligible. Thus, with overwhelming probability the total fraction of corrupted OT pairs is less than half.  $\square$

<sup>3</sup> Computer algebra calculation given at <https://github.com/GnarlyMshtep/price-of-low-com-followup-calculations>.

**Lemma 2.** *For all  $(t, \lambda)$  adversaries  $\mathcal{A}$ ,*

$$\Pr \left[ |\mathcal{O}^{\mathcal{A}^\dagger}| \geq \frac{|\mathcal{S}_1|}{2} \right] \geq \Pr \left[ |\mathcal{O}^{\mathcal{A}}| \geq \frac{|\mathcal{S}_1|}{2} \right]$$

*Proof.* Assume for a contradiction there exists an adversary  $\mathcal{A}$  s.t.  $\Pr[|\mathcal{O}^{\mathcal{A}}| \geq |\mathcal{S}_1|/2] > \Pr[|\mathcal{O}^{\mathcal{A}^\dagger}| \geq |\mathcal{S}_1|/2]$ . Notice that since  $\mathcal{A}$  is semi-honest,  $\mathcal{A}$  can be entirely described by a mapping from its view to the identities of the servers it corrupts and decorrupts. Through a series of propositions (Proposition 2, 3, 4, 5, and 6) we will show that  $\mathcal{A}$  “were to act more like  $\mathcal{A}^\dagger$ ” then  $\Pr[|\mathcal{O}^{\mathcal{A}}| \geq |\mathcal{S}_1|/2]$  would not decrease. Combining these propositions we will obtain that, without loss of generality  $\mathcal{A} = \mathcal{A}^\dagger$  reaching

$$\Pr \left[ |\mathcal{O}^{\mathcal{A}^\dagger}| \geq |\mathcal{S}_1|/2 \right] > \Pr \left[ |\mathcal{O}^{\mathcal{A}^\dagger}| \geq |\mathcal{S}_1|/2 \right]$$

a contradiction.

**Proposition 2.** *Without loss of generality,  $\mathcal{A}$  does not corrupt any servers after round 6.*

*Proof.* After round 6 the states of all the servers have been erased and no more messages will be sent. Indeed, for any such adversary  $\mathcal{A}$  there exists an adversary  $\mathcal{A}'$  who outputs a view with the same distribution as  $\mathcal{A}$  but does not corrupt any of the parties that  $\mathcal{A}$  corrupts after round 6. Thus  $\Pr[|\mathcal{O}^{\mathcal{A}'}| \geq |\mathcal{S}_1|/2] \geq \Pr[|\mathcal{O}^{\mathcal{A}}| \geq |\mathcal{S}_1|/2]$  and hence we can assume  $\mathcal{A} = \mathcal{A}'$ .  $\square$

**Proposition 3.** *Without loss of generality,  $\mathcal{A}$  acts on references. That is, if in the view of any corrupted server  $s_k \in \mathcal{C}_\rho^{\mathcal{A}}$  is a message from/to server  $s_l$ , then  $\mathcal{A}$  corrupts  $s_l$  at the beginning of round  $\rho + 1$  (unless it is already corrupted). We can also assume that  $\mathcal{A}$  never decorrupts  $s_l$ .*

*Proof.* Except with negligible probability, at most  $O(\log^\delta n)$  messages are sent in the execution of the protocol (Lemma 3). Thus, by a similar argument to Proposition 1, even if  $\mathcal{A}$  corrupts all  $O(\log^\delta n)$  servers that send/recieve a message in an execution of the protocol, for sufficiently large  $n$   $\mathcal{A}$  would not exceed its corruption bound, even without ever decorrupting them. Since the view of  $\mathcal{A}'$  emulating  $\mathcal{A}$  and acting on references and not decorrupting them strictly contains the view of  $\mathcal{A}$  it is clear  $\Pr[|\mathcal{O}^{\mathcal{A}'}| \geq |\mathcal{S}_1|/2] \geq \Pr[|\mathcal{O}^{\mathcal{A}}| \geq |\mathcal{S}_1|/2]$  and hence we can assume  $\mathcal{A} = \mathcal{A}'$ .  $\square$

**Proposition 4.** *Without loss of generality, at the beginning of round  $\rho$   $\mathcal{A}$  corrupts at random from the previously uncorrupted servers  $\mathcal{S} \setminus \cup_{k \in [\rho-1]} C_k$  and decorrupts at random from  $\mathcal{C}_\rho$ .*

*Proof.* Let  $R_\rho$  be the set of references  $\mathcal{A}$  will act on in round  $\rho$  (Definition 2), and  $C_\rho \setminus R_\rho = H = \{h_1, \dots, h_\kappa\} \subset \mathcal{S} \setminus \cup_{k \in [\rho-1]} C_k$  the parties  $\mathcal{A}$  chooses to corrupt at the beginning of round  $\rho$  (which may depend on its view  $V$  at the end of round  $\rho-1$ ). Let  $A = \{a_1, \dots, a_\kappa\}$  be a random subset of  $\mathcal{S} \setminus \cup_{k \in [\rho-1]} C_k$  of size  $|C_\rho \setminus R_\rho|$ .

Let  $\mathbb{V}(H), \mathbb{V}(A)$  be the distribution of views  $\mathcal{A}$  samples from if it would corrupt according to  $R_\rho \cup H, R_\rho \cup A$  respectively. We will show that  $\mathbb{V}(H) = \mathbb{V}(A)$ , concluding the proof.

Let  $V$  be an outcome of  $\mathbb{V}(H)$  which is assigned probability  $p$ . Let  $\mathbb{V}(s)$  be the distribution of views of server  $s$ . Then the distribution  $\mathbb{V}(a_i)$  is identical to  $\mathbb{V}(k_i)$  conditioned on  $V$  because, (a)  $\mathbb{V}(k_i) = \mathbb{V}(a_i)$  when not conditioned on anything and (b) as of round  $\rho$ , the servers in  $A \cup H$  did not communicate with the servers whose views are in  $V$ , and the view of each server  $s$  is identical information-theoretically independent from the view of all servers  $s'$  it has not messaged. Since

$$\mathbb{V}(H) = V \cup_{i \in [\kappa]} \mathbb{V}(h_i)$$

and

$$\cup_{i \in [\kappa]} \mathbb{V}(h_i)|_V = \cup_{i \in \kappa} \mathbb{V}(a_i)$$

then

$$\mathbb{V}(H) = \mathbb{V}(A)$$

as desired.

The argument for decorrutions is nearly identical and we leave it to the reader.  $\square$

**Proposition 5.** *Wlog,  $\mathcal{A}$  decorrups  $\lambda t$  servers at the end of every round and  $|C_\rho^{\mathcal{A}}| \geq \lambda t$*

*Proof.* Assume there exists a round in which  $\mathcal{A}$  corrupts  $|C_\rho| < \lambda t$  servers. Then there exists  $\mathcal{A}'$  which corrupts some  $\lambda t - |C_\rho|$  random servers from  $\mathcal{S} \setminus \mathcal{C}$  and decorrups them at the end of the round. At the begining of the next round  $\mathcal{A}'$  has the same corruption budget as  $\mathcal{A}$  and can do exactly as it does. Clearly the  $\mathcal{A}$ 's view is contained within the view of  $\mathcal{A}$ .  $\square$

Here (Prop 5), we should say something about “acts on references”. Minor: what happens if  $\mathcal{C}$  becomes  $\mathcal{S}$  and  $\mathcal{A}$  still has a corruption budget, i.e.,  $t + 5\lambda t > |\mathcal{S}|$ ?

We know  $\mathcal{A}$  does not corrupt after round 6, acts on references, decorrups at random from the set of currently corrupted servers, and other than corrupting references, randomly corrupts from the set of previously uncorrupted servers. Hence  $\mathcal{A}$  executes exactly like  $\mathcal{A}^\dagger$  except that  $\mathbf{C}^{\mathcal{A}} = (|C_k^{\mathcal{A}} \setminus R_k^{\mathcal{A}}|)_{k \in [6]}$ , the number of servers  $\mathcal{A}$  corrupts in round (which may depend on protocol execution) might not be equal to  $(t, \lambda t, \lambda t, \lambda t, \lambda t, \lambda t)$ , the number of servers  $\mathcal{A}^\dagger$  in each round (regardless of protocol execution).

**Proposition 6.** *Without loss of generality,  $\mathbf{C}^{\mathcal{A}} = (t, \lambda t, \lambda t, \lambda t, \lambda t, \lambda t) = \mathbf{C}^{\mathcal{A}^\dagger}$*

*Proof.* try to ensure consistent symbolic usage of  $\mathbb{V}$  in the following We construct adversary  $\mathcal{A}'$  which obeys Proposition 2, 3, 4, and 5, where  $\mathbf{C}^{\mathcal{A}'} = (t, \lambda t, \lambda t, \lambda t, \lambda t, \lambda t)$ . Let  $\mathbb{V}_{\mathcal{A}}, \mathbb{V}_{\mathcal{A}'}$  be the mappings from the randomness of the adversary and the parties of the protocol  $(r_{\mathcal{A}}, (r_p)_{p \in \mathcal{P}})$  to the of views of  $\mathcal{A}, \mathcal{A}'$ ,

respectively, representing the distribution of views of each adversary. We will show that for all  $\mathbf{r} = (r_{\mathcal{A}}, (r_p)_{p \in \mathcal{P}})$  we have that  $\mathbb{V}_{\mathcal{A}}(\mathbf{r}) \subset \mathbb{V}_{\mathcal{A}'}(\mathbf{r})$  implying that

$$\Pr \left[ |\mathcal{O}^{\mathcal{A}'}| \geq \frac{|\mathcal{S}_1|}{2} \right] \geq \Pr \left[ |\mathcal{O}^{\mathcal{A}}| \geq \frac{|\mathcal{S}_1|}{2} \right]$$

Fix  $\mathbf{r}$ . Since other than corrupting references,  $\mathcal{A}$  randomly corrupts from the set of previously uncorrupted servers,  $\mathcal{A}'$  can use  $\mathbf{r}$  to compute  $A = \{s_{i_1}, \dots, s_{i_{t(1+5\lambda)}}\} \subset \mathcal{S}$  where for some  $0 = j_0 \leq \dots \leq j_5 \leq j_6 \leq t(1+5\lambda)$  (potentially unknown to  $\mathcal{A}'$ ) we have that  $C_{\rho}^{\mathcal{A}} \setminus R_{\rho}^{\mathcal{A}} = \{s_{j_{\rho-1}}, \dots, s_{j_{\rho}}\}$ .

$\mathcal{A}'$  operates as follows. In addition to acting on references at the beginning of each round, it corrupts the first  $t$  parties from  $A$  in round 1, and in every subsequent round, the next  $\lambda t$  servers from  $A$ . Before decorrupting in round  $\rho$ ,  $\mathcal{A}'$  can simulate  $\mathcal{A}$  and learn  $D_{\rho}^{\mathcal{A}}$ . Since (by induction on  $\rho$ )  $\mathcal{C}_{\rho}^{\mathcal{A}} \subset \mathcal{C}_{\rho}^{\mathcal{A}'}$ , at the end of round  $\rho$ ,  $\mathcal{A}'$  decorrupts  $D_{\rho}^{\mathcal{A}}$ . Notice that if  $\mathcal{A}$  had corrupted some  $s$  by reference in round  $\rho$  due to a communication with  $s' \in \mathcal{C}_{\rho-1}^{\mathcal{A}}$ , then  $s' \in \mathcal{C}_{\rho-1}^{\mathcal{A}'}$  and hence  $\mathcal{A}'$  would have also corrupted him by reference. Thus, it is easy to verify that  $\mathbb{V}_{\mathcal{A}}(\mathbf{r}) \subset \mathbb{V}_{\mathcal{A}'}(\mathbf{r})$ , concluding the proof.  $\square$

This concludes the proof of Lemma 2.  $\square$

**Lemma 3.** *Except with negligible probability, the communication complexity of  $\Pi_{sh}^{mob}$  is  $O(\log^{\delta} n)$ .*

Since every message has  $O(1)$  bits, we will prove that the message complexity of  $\Pi_{sh}^{mob}$  is  $O(\log^{\delta} n)$  except with negligible probability. Every server  $s \in \mathcal{S}$  is included in  $\mathcal{S}_1$  with probability  $p = \frac{\log^{\delta} n}{n}$  independent of other servers. Thus, by application of the Chernoff bound, we get that for every  $0 < \gamma < 1/2$ :

$$\Pr[|\mathcal{S}| > (1 + \gamma) \log^{\delta} n] < e^{-\frac{\gamma \log^{\delta} n}{3}}$$

which is negligible. Moreover, each  $s_i \in \mathcal{S}_1$  chooses one additional relay-party  $s_{ij}$  for any constant  $1/2 < \gamma' < 1$ :

$$|\mathcal{S}_1 \cup \mathcal{S}_2| \leq (2 + \gamma') \log^{\delta} n$$

with overwhelming probability. Since each such party communicates at most two messages, the total message complexity is  $O(\log^{\delta} n)$  plus the messages exchanged in the OT combiner, which are polynomial in the number of OT pairs. Thus, with overwhelming probability, the total number of messages is  $O(\log^{\delta'} n)$  for some constant  $\delta'$ .  $\square$

This concludes the proof of Theorem 1.  $\square$

## 5 Lower Bound in the mobile semi-honest model

Removed everything and moved it to graveyard. The only thing we know for sure is that  $\mathcal{A}^\dagger$  can corrupt message paths with probability  $1/2$ . This is using the causal path + parallel intermediary argument.

In this section, we complement the upper bound of Section 4 with a (tight?) lower bound. That is, we show that in a  $(n, 2)$  low-communication setting with erasures, there does not exist a protocol for computing the OT functionality  $f_{\text{OT}}((m_0, m_1), b) = (\perp, m_b)$  that can tolerate every  $(t, \lambda)$  semi-honest mobile adversary for  $t > (\theta(\lambda) + \epsilon)n$  and  $\theta(\lambda)$  is defined in the statement of Theorem 2. Since protocol  $\Pi_{\text{sh}}^{\text{mob}}$  (Figure 1) can tolerate any  $(t, \lambda)$  semi-honest mobile adversary for  $t < (\theta(\lambda) - \epsilon)n$  (Theorem 2),  $\Pi_{\text{sh}}^{\text{mob}}$  is corruption-optimal. Our result strictly generalizes [GIOZ17][Theorem 4]; for  $\lambda = 0$ , a mobile adversary is adaptive. Indeed, fixing  $\lambda = 0$  retrieves the  $t > (1 - \sqrt{1/2} + \epsilon)n$  lower bound of [GIOZ17][Theorem 4].

Let  $\mathbf{P}$  be the set of the protocols (needs to be characterized by some adversarial strategy that it can tolerate) that compute the OT functionality with information-theoretic security and sublinear communication in the  $(n, 2)$  server-client model. To prove our lower bound, we need to show that for all  $\Pi \in \mathbf{P}$ , for all  $\epsilon > 0$ , there exists some (mobile-sh- $t > \theta(\lambda) + \epsilon$ ) adversary  $\mathcal{A}$  that cannot be tolerated by  $\Pi$ . In fact, we will show that  $\mathcal{A}^\dagger$  described earlier (with  $t = \theta(\lambda) + \epsilon$ ) is intolerable for all  $\Pi \in \mathbf{P}$ .

### 5.1 Discussion

Note that in [GIOZ17], a lower bound for a corruption budget of  $1 - \sqrt{0.5}$  is proved in the adaptive setting. Our adversary  $\mathcal{A}^\dagger$  in fact extends the adversary they consider (call it  $\hat{\mathcal{A}}$ ). This means that for  $\lambda = 0$  they behave the same way.<sup>4</sup> They then consider a slightly weaker adversary<sup>5</sup>  $\hat{\mathcal{A}}$  and show that it is intolerable.

To show that  $\hat{\mathcal{A}}$  is intolerable, they first assume by contradiction it is tolerable. This means there exists a protocol  $\Pi$  that can securely compute OT in the presence of  $\hat{\mathcal{A}}$ . They modify this to get  $\hat{\Pi}$  a protocol that can securely compute  $b_1 \vee b_2$  for the clients. In this protocol,  $\hat{\mathcal{A}}$  ends up corrupting either client with prob.  $1/2$ . This contradicts a 2PC impossibility result (what is the exact theorem?) so  $\hat{\mathcal{A}}$  is intolerable.

**Why is it not straightforward for us to extend this proof?** The proof in the adaptive setting exploits the fact that with a  $1 - \sqrt{0.5}$  corruption budget, each communication “edge” is initially corrupted with probability  $1/2$  so, by acting on references, we can corrupt  $1/2$  of the messages. The mobile adversary that we consider has a lower corruption budget and therefore it does

<sup>4</sup> For the lower bound, they actually consider a weaker adversary that doesn’t corrupt servers talking to  $c_\alpha$ .

<sup>5</sup> Technically, they reduce it to probabilistic edge adversary structures. See [GIOZ17][Lemma 6].

NOT corrupt each edge with probability  $1/2$ . As a result, even for  $\Pi_{\text{sh}}^{\text{mob}}$ ,  $\mathcal{A}^\dagger$  with  $t = \theta(\lambda) + \epsilon$  does NOT learn half of the messages exchanged (verified on iPad that  $\mathcal{A}^\dagger$  learns  $(s_i, s_{ij})$  with prob.  $\leq 0.45$ ) in the protocol but it DOES learn half of the OT pairs. Therefore, the proof of our lower bound will require a method where it is not necessary that  $\mathcal{A}^\dagger$  corrupts half of the messages. So, it may not be possible to transform a protocol  $\Pi \in \mathbf{P}$  tolerating  $\mathcal{A}^\dagger$  (or something weaker) into a protocol  $\hat{\Pi}$  that computes OR in the presence of an adversary that corrupts either party with prob.  $1/2$ .

## 5.2 Restricting the set of protocols

One way to proceed (as suggested by Vassilis) would be to consider a subset  $\mathbf{P} \subset \mathbf{P}$  of protocols characterized by some property and proving the lower bound for these protocols.

**Definition 4 (message path in  $\Pi$ ).** Let  $\Pi$  be an arbitrary protocol in the  $(2, n)$  client server model. Let  $u, v \in \mathcal{P} = \mathcal{S} \cup \{c_0, c_1\}$ . Let  $k \geq 0$ . Formally, a message path from  $u$  to  $v$ ,  $P_{u,v}$ , in  $\Pi$  is a list of  $k$  parties  $s_1, s_2, \dots, s_k$ ,  $k+1$  messages  $m_0, m_1, \dots, m_k$  and  $k+1$  integers  $\rho_0, \rho_1, \dots, \rho_k$  such that  $s_i$  sends  $m_i$  to  $s_{i+1}$  in round  $\rho_i$  and  $\rho_{i+1} \geq \rho_i + 2$  for all  $i \in \{0, 1, \dots, k\}$  where we set  $s_0 = u$  and  $s_{k+1} = v$ .

*Remark 2.* Informally, we define a message path  $P_{u,v}$  from  $u$  to  $v$  as a sequence of messages starting at  $u$  and ending at  $v$  through intermediate servers  $s_1, \dots, s_k$  such that each message is separated by at least two rounds.

$$u \xrightarrow[\rho_0]{m_0} s_1 \xrightarrow[\rho_1]{m_1} s_2 \longrightarrow \dots \longrightarrow s_k \xrightarrow[\rho_k]{m_k} v$$

We hope to show that if there does not exist any common server with message paths to  $c_1$  and  $c_2$  then they cannot have correlated messages (in a secure OT setting).

**Definition 5 (protocols where correlation implies root server).** Consider the subset  $\bar{\mathbf{P}} \subset \mathbf{P}$  of protocols  $\Pi$  where  $c_0, c_1$  sharing a correlated message pair  $(m_0, m_1)$  implies that there exists some  $s \in \mathcal{P} = \mathcal{S} \cup \{c_0, c_1\}$  such that in round  $\rho$  its view contains  $(m_0, m_1)$  and that there exist message paths  $P_{s,c_0}$  and  $P_{s,c_1}$  in  $\Pi$  where the first message is sent in round  $\rho$  and the last message in  $P_{s,c_b}$  is received by  $c_b$  before it outputs  $m_b$  for  $b \in \{0, 1\}$ .

**Proposition 7.** Let  $s \in \mathcal{P} = \mathcal{S} \cup \{c_0, c_1\}$  such that in round  $\rho$  its view contains  $(m_0, m_1)$ . Let  $\Pi$  be an arbitrary protocol with sublinear communication in the  $(2, n)$  client server model such that at the end of the protocol  $c_b$  outputs  $m_b$  for  $b \in \{0, 1\}$ . Further, assume there exist message paths  $P_{s,c_0}$  and  $P_{s,c_1}$  in  $\Pi$  where the first message is sent in round  $\rho$  and the last message in  $P_{s,c_b}$  is received by  $c_b$  before it outputs  $m_b$  for  $b \in \{0, 1\}$ . Then  $\mathcal{A}^\dagger$  can output (or its view contains)  $(m_0, m_1)$  with probability at least  $1/2$ .

*Proof.* We first prove some lemmas to isolate the structure of  $\Pi_{\text{sh}}^{\text{mob}}$  presented in the upper bound.

**Lemma 4.** *If both  $P_{s,c_0}$  and  $P_{s,c_1}$  have length  $k = 0$  (define) then  $\mathcal{A}^\dagger$  outputs  $(m_0, m_1)$  with prob.  $\geq 1/2$ .*

*Proof.* If both message paths have length  $k = 0$  then  $s$  sends a message to some client say  $c_b$  in round  $\rho$ . Recall that  $c_b = c_\alpha$  with probability  $1/2$  so  $\mathcal{A}$  learns the identity of  $s$  in round  $\rho + 1$  and corrupts it in the same round, viewing  $(m_0, m_1)$  before  $s$  can erase it.

So wlog we assume there exists at least one intermediary server  $l_1$ , say in  $P_{s,c_0}$ , that  $s$  sends a message to in round  $\rho$ .

**Lemma 5.** *Wlog, either  $s$  erases  $m_1$  after round  $\rho + 3$  or sends it to some  $r_1 \in \mathcal{S}$  in round  $\rho$ .*

*Proof.* Assume that it erases  $m_1$  in round  $\rho + 1$ . This means it either sends  $m_1$  in round  $\rho$  or not at all. The latter gives us a contradiction as  $c_1$  outputs  $m_1$ . In the first case, using our argument from the previous lemma, if it sends to a client then  $\mathcal{A}$  learns  $(m_0, m_1)$  with prob.  $1/2$  so it must send to a server  $r_1 \in \mathcal{S}$ .

We have now isolated the protocol to one of the two structures below insert tikz diags:

1. In the first case,  $s$  knows and  $l_1$  has a reference to  $(m_0, m_1)$  in rounds  $\rho$  and  $\rho + 1$  and  $l_1$  and  $s$  have references to  $m_1$  in rounds  $\rho + 2$  and  $\rho + 3$ . And  $l_1$  also has a ref to  $m_0$  in  $\rho + 2, \rho + 3$  by corrupting the entire path to  $c_0$  need to see if this is required. Comparing this with the corruptions in  $\Pi_{\text{sh}}^{\text{mob}}$  it is clear (i still need to write it all out. if  $\Pi$  doesn't send to a client randomly, i think i need a different adversary) that  $\mathcal{A}^\dagger$  with corruption budget  $\theta(\lambda) + \epsilon$  learns  $(m_0, m_1)$  with probability at least  $1/2$ .
2. In the second case,  $s, l_1$  and  $r_1$  know/have a reference to  $(m_0, m_1)$  in rounds  $\rho$  and  $\rho + 1$ . And  $l_1$  also has a ref to  $m_0$  in  $\rho + 2, \rho + 3$  by corrupting the entire path to  $c_0$  need to see if this is required. The following calculation shows that  $\mathcal{A}^\dagger$  with corruption budget  $\theta(\lambda) + \epsilon$  learns  $(m_0, m_1)$  with probability at least  $1/2$ .

**Proposition 8.** *Let  $\Pi \in \bar{\mathbf{P}}$ . Then  $\Pi$  cannot tolerate  $\mathcal{A}^\dagger$  with corruption budget  $t > \theta(\lambda) + \epsilon$  for any  $\epsilon > 0$ .*

*Proof.* Let  $\Pi \in \bar{\mathbf{P}}$ . By construction, our proposition applies here. Every OT pair that  $c_0$  and  $c_1$  share has more than  $1/2$  probability of being learned by  $\mathcal{A}^\dagger$  (because an OT pair is a correlated message pair) and each pair is learned independently of the others since  $\mathcal{A}^\dagger$  makes corruptions independently. Thus, (Is this really enough to show intolerable?)  $\Pi$  cannot tolerate  $\mathcal{A}^\dagger$ .

*Remark 3.* This gives us a lower bound. In particular, the bound from Section 4 is tight for protocols in  $\bar{\mathbf{P}}$ . It remains to show that  $\bar{\mathbf{P}} = \mathbf{P}$ .

### 5.3 Proving a less tight lower bound

If all else fails, we can try proving a less tight lower bound. Since a mobile adversary can do everything an adaptive adversary can, it is clear that a lower bound of  $1 - \sqrt{0.5} + \epsilon$  works here as well. We can try improving this a bit in the mobile setting and maybe using an argument similar to [GIOZ17].

## 6 (Tight) Upper Bound for adaptive malicious adversaries

In this section, we give an upper bound on the corruption threshold in the low-communication information-theoretic setting against adaptive malicious adversaries. By [GIOZ17][Theorem N], our upper bound is tight. We prove our upper bound by specifying Protocol

Protocol $\Pi_{\text{malicious}}^{\text{adaptive}}$
<ol style="list-style-type: none"> <li>1. Servers wake up with probability <math>\log^\delta n/n</math>.</li> <li>2. Each woken server <math>s_i</math> prepares an OT pair and sends a random half of it to random server <math>s_{ij}</math> <ol style="list-style-type: none"> <li>(a) okay, consider the “nueanced” model only for the mobile adversaries, so there is no <math>s_i</math> erases, etc, round.</li> </ol> </li> <li>3. <math>s_i</math> and <math>s_{ij}</math> erase their entire state, except from the half of the OT-pair they will each send <math>c_1, c_2</math> respectively.             <ol style="list-style-type: none"> <li>(a) An <math>s_{ij}</math> receiving any message not of the format above will simply ignore it.</li> </ol> </li> <li>4. <math>s_i, s_{ij}</math> send respective half of OT pairs to <math>c_1, c_2</math> respectively.</li> <li>5. If <math>c_b</math> receives more than <math>(1 - 324\epsilon^4 - 288\epsilon^5 - 64\epsilon^6) \log^\delta n</math> messages (similar to Page 19, step 5), it aborts and alerts the other player</li> <li>6. <math>c_1, c_2</math> use malicious OT-combiner to get one honest OT-pair.</li> </ol>

**Fig. 3.** A protocol tolerant of malicious adaptive adversaries

We will now show that Protocol  $\Pi_{\text{malicious}}^{\text{adaptive}}$  is secure. This proof combines techniques from [GIOZ17][Theorem adap-upper-sh, mal-static-upper].

**Theorem 3.** *For all  $\epsilon > 0$ , Protocol  $\Pi_{\text{malicious}}^{\text{adaptive}}$  computes the random OT functionality with communication  $O(\log^\delta n)$  can tolerate adaptive malicious adversaries with corruption threshold  $t < (1 - \sqrt{0.5} - \epsilon)n$  (with abort)*

*Proof.* A malicious adaptive adversary can send arbitrary messages from any server in the set of parties that it controls and corrupt parties according to its dynamic view.

Informally, we will show that if a malicious adaptive adversary  $\mathcal{A}$  corrupts according to a view of its semi-honest execution, which we call  $\mathcal{A}^\dagger$ , and is also



allowed to send arbitrary messages, then it is tolerable by our protocol. Then we will show that the  $\mathcal{A}$  cannot act any better than  $\mathcal{A}^\dagger$  because if it does then it contradicts [ref](#) stating that  $\mathcal{A}^\dagger$  is optimal.

Fix an adaptive semi-honest adversarial strategy  $\mathcal{A}^\dagger$  and let  $C^\dagger \subset \mathcal{S}$  be the set of corrupted servers.

**Proposition 9.**  $\Pi_{\text{malicious}}^{\text{adaptive}}$  can tolerate an adversary that follows  $\mathcal{A}^\dagger$  and can send an arbitrary number of messages.

*Proof.* Let  $W \subset \mathcal{S}$  be the servers that would have woken up on an honest execution of the protocol. By a Chernoff bound, we get that for any constant  $0 < \gamma < 1$ :

$$\Pr[|W| \leq (1 - \gamma) \log^\delta n] < e^{-\frac{\gamma^2 \log^\delta n}{3}}$$

so for  $\gamma = (18\epsilon^2 + 8\epsilon^3)$  the above implies that with overwhelming probability:

$$|W| > (1 - (18\epsilon^2 + 8\epsilon^3)) \log^\delta n$$

Wlog, we can assume that  $\mathcal{A}^\dagger$  corrupts  $T = \lfloor (1 - \sqrt{0.5} - \epsilon)n \rfloor$  parties. For each  $s_i \in W$ , we let  $X_i$  denote the random variable that is equal to 1 if  $s_i$  or  $s_{ij} \in C^\dagger$  and 0 otherwise. Since parties wake up independently  $X_1 \dots, X_{|W|}$  are i.i.d. random variables. Since  $\mathcal{A}^\dagger$  corrupts  $T$  parties [need to fill in some overconnected stuff](#),

$$\begin{aligned} \Pr[X_i = 1] &= \Pr[s_i \in C^\dagger] + \Pr[s_{ij} \in C^\dagger] - [\{s_i, s_{ij}\} \subset C^\dagger] \\ &= \frac{2T}{n} - \frac{T^2}{n^2} \end{aligned}$$

Let  $X = \sum_{i=1}^{|W|} X_i = |W \cap C^\dagger|$  denote the number of corrupted parties that send or receive an OT pair, which has mean  $\mu = |W|(\frac{2T}{n} - \frac{T^2}{n^2})$ . Another Chernoff bound gives us that for any  $0 < \epsilon_1 < 1$ :

$$\Pr[X \geq (1 + \epsilon_1)\mu] < e^{-\frac{\epsilon_1^2 \mu}{3}}.$$

Hence, with overwhelming probability and for  $\epsilon_1 = 4\epsilon$ :

$$\begin{aligned} X &< (1 + 4\epsilon)(2(1 - \sqrt{0.5} - \epsilon) - (1 - \sqrt{0.5} - \epsilon)^2)|W| \\ &< (1 + 4\epsilon)(\frac{1}{2} - 2\epsilon - \epsilon^2)|W| \\ &= (\frac{1}{2} - (9\epsilon^2 + 4\epsilon^3))|W| \end{aligned}$$

Therefore, again with overwhelming probability, the number  $h$  of honest parties that contact each of the parties as OT dealers is:

$$h = |W - C^\dagger| \geq (\frac{1}{2} + (9\epsilon^2 + 4\epsilon^3))|W| > (\frac{1}{2} + (9\epsilon^2 + 4\epsilon^3))(1 - (18\epsilon^2 + 8\epsilon^3)) \log^\delta n.$$

As specified in the protocol, unless the honest client aborts, he accepts at most  $\rho = (1 - 324\epsilon^4 - 288\epsilon^5 - 64\epsilon^6) \log^\delta n$  offers for dealers. Therefore, the fraction of honest OT dealers among these  $\rho$  dealers is

$$\frac{h}{\rho} > \frac{(\frac{1}{2} + (9\epsilon^2 + 4\epsilon^3)(1 - (18\epsilon^2 + 8\epsilon^3)))}{(1 - 324\epsilon^4 - 288\epsilon^5 - 64\epsilon^6)} = \frac{1}{2}.$$

Thus at least  $1/2$  of the OT components that an honest client receives are correct, in which case the security of the protocol follows from the security of the underlying OT-combiner.  $\square$

**Proposition 10.** *For any malicious adaptive adversary  $\mathcal{A}^{\text{mal}}$ , there exists a semihonest adaptive adversary  $\mathcal{A}^{\text{sh}}$  such that*

$$\Pr \left[ |\mathcal{O}^{\mathcal{A}^{\text{sh}}}| \geq \frac{|\mathcal{S}_1|}{2} \right] = \Pr \left[ |\mathcal{O}^{\mathcal{A}^{\text{mal}}}| \geq \frac{|\mathcal{S}_1|}{2} \right]$$

*Proof.* We want to prove that any *malicious* adversarial strategy  $\mathcal{A}^{\text{mal}}$  gives a *semi-honest* adversarial strategy  $\mathcal{A}^{\text{sh}}$  with equal success probability. Given  $\mathcal{A}^{\text{mal}}$ , we will describe  $\mathcal{A}^{\text{sh}}$  which works by internally simulating  $\mathcal{A}^{\text{mal}}$ , tweaking his view when necessary and reproducing the simulated steps of  $\mathcal{A}^{\text{mal}}$  in the real execution.

In each round  $\mathcal{A}^{\text{mal}}$  can send arbitrary messages and corrupt servers (within its budget) based on its dynamic view at that instant. For  $\mathcal{A}^{\text{sh}}$  to run  $\mathcal{A}^{\text{mal}}$ 's internal code, it needs to be able to simulate  $\mathcal{A}^{\text{mal}}$ 's view at every step. *Reorganize to put simulation and proof together?* Consider the following simulation: In every round,  $\mathcal{A}^{\text{sh}}$  follows  $\mathcal{A}^{\text{mal}}$ 's corruption pattern but lets the parties it controls behave semi-honestly. When  $s \in \mathcal{C}^{\text{mal}}$  sends any message,  $\mathcal{A}^{\text{sh}}$  appends this exchange to the simulated view of  $s$ . If  $s \in \mathcal{C}^{\text{mal}}$  sends a message to  $s' \in \mathcal{C}^{\text{mal}}$  or  $c_\alpha$ , then  $\mathcal{A}^{\text{sh}}$  also adds this message to its simulated view of  $s'$  or  $c_\alpha$ . If  $s \in \mathcal{C}^{\text{mal}}$  sends a message to a server  $s' \in \mathcal{S} \setminus \mathcal{C}^{\text{mal}}$  or  $c_{1-\alpha}$  and the message is not in the format of an OT pair, the message is ignored by the specification of  $\Pi_{\text{malicious}}^{\text{adaptive}}$ . If the message is a component of a corrupted OT pair, then  $\mathcal{A}^{\text{sh}}$  ignores this if the message is meant for  $c_{1-\alpha}$  otherwise adds this message to the view of  $c_\alpha$ .

Fix some round  $\rho$  and let  $\mathbb{V}_\rho(\mathcal{A}^{\text{mal}})$  be the real distribution of views  $\mathcal{A}^{\text{mal}}$  samples from for its round  $\rho$  corruptions. Let  $\mathbb{V}_\rho^{\text{sim}}(\mathcal{A}^{\text{mal}})$  be the simulated distribution of views of  $\mathcal{A}^{\text{mal}}$ , simulated by  $\mathcal{A}^{\text{sh}}$ .

**Definition 6 (containment of distributions).** *For all configurations of randomness, view is contained.*

Inductively, we will show that if  $\mathcal{C}_\rho^{\text{mal}} = \mathcal{C}_\rho^{\text{sh}}$  and  $\mathbb{V}_\rho^{\text{sim}}(\mathcal{A}^{\text{mal}}) \supset \mathbb{V}_\rho(\mathcal{A}^{\text{mal}})$  then  $\mathbb{V}_{\rho+1}^{\text{sim}}(\mathcal{A}^{\text{mal}}) \supset \mathbb{V}_{\rho+1}(\mathcal{A}^{\text{mal}})$ . Since  $\mathcal{A}^{\text{sh}}$  can simulate  $\mathcal{A}^{\text{mal}}$ 's view, it can internally run  $\mathcal{A}^{\text{mal}}$  and follow its corruption pattern so that  $\mathcal{C}_{\rho+1}^{\text{mal}} = \mathcal{C}_{\rho+1}^{\text{sh}}$ . Then by induction, their corruptions are the same in every round so

$$\Pr \left[ |\mathcal{O}^{\mathcal{A}^{\text{sh}}}| \geq \frac{|\mathcal{S}_1|}{2} \right] = \Pr \left[ |\mathcal{O}^{\mathcal{A}^{\text{mal}}}| \geq \frac{|\mathcal{S}_1|}{2} \right]$$

concluding the proof.

Assume that  $\mathcal{C}_\rho^{\text{mal}} = \mathcal{C}_\rho^{\text{sh}}$  and  $\mathbb{V}_\rho^{\text{sim}}(\mathcal{A}^{\text{mal}}) \supset \mathbb{V}_\rho(\mathcal{A}^{\text{mal}})$ . We will show that  $\mathbb{V}_{\rho+1}^{\text{sim}}(\mathcal{A}^{\text{mal}}) \supset \mathbb{V}_{\rho+1}(\mathcal{A}^{\text{mal}})$ . In words, given that  $\mathcal{A}^{\text{mal}}$  and  $\mathcal{A}^{\text{sh}}$  have the same corrupted set at the start of round  $\rho$  and  $\mathcal{A}^{\text{sh}}$  can simulate  $\mathcal{A}^{\text{mal}}$ 's view at the start of round  $\rho$ , we need to show it can also simulate its view at the end of round/start of next round. Let  $\mathbb{V}_\rho(s)$  be the distribution of views of server  $s$  at the start of round  $\rho$  (then  $\mathbb{V}_{\rho+1}(s)$  is the view at the end of round  $\rho$ ). For all  $s \in \mathcal{C}_\rho^{\text{mal}}$ ,  $\mathbb{V}_{\rho+1}(s) \subset \mathbb{V}_{\rho+1}^{\text{sim}}(\mathcal{A}^{\text{mal}})$ . It remains to show that  $\mathbb{V}_{\rho+1}^{\text{sim}}(\mathcal{A}^{\text{mal}})$  contains  $\mathbb{V}_{\rho+1}(\mathcal{A}^{\text{mal}}) \setminus \bigcup_{s \in \mathcal{C}_\rho^{\text{mal}}} \mathbb{V}_{\rho+1}(s)$  i.e. that  $\mathcal{A}^{\text{sh}}$  can simulate  $\mathbb{V}_{\rho+1}(\mathcal{A}^{\text{mal}}) \setminus \bigcup_{s \in \mathcal{C}_\rho^{\text{mal}}} \mathbb{V}_{\rho+1}(s)$ . Note that parties not in  $\mathcal{C}_\rho^{\text{mal}}$  must behave according to the protocol so wlog we only consider servers in  $\mathcal{C}_\rho^{\text{mal}}$  sending arbitrary messages.

1. Assume that  $p \in \mathcal{C}_\rho^{\text{mal}} \cup c_\alpha$  sends a message  $m$  to  $p' \in \mathcal{C}_\rho^{\text{mal}} \cup c_\alpha$ . Then  $\mathcal{A}^{\text{sh}}$  can simulate this exchange by appending it **how do I formalize this? it adds the message and the identity of whom it sends to/receives from** to  $\mathbb{V}_{\rho+1}^{\text{sim}}(p)$  and  $\mathbb{V}_{\rho+1}^{\text{sim}}(p')$ .
2. Assume that  $p \in \mathcal{C}_\rho^{\text{mal}} \cup c_\alpha$  sends a message  $m$  to  $p' \in \mathcal{P} \setminus (\mathcal{C}_\rho^{\text{mal}} \cup c_\alpha)$ .  $\mathcal{A}^{\text{sh}}$  appends this exchange to  $\mathbb{V}_{\rho+1}^{\text{sim}}(p)$ . Also:
  - (a) If the message is not in the format of an OT pair then by the specification of the protocol,  $p'$  ignores the message.
  - (b) If the message is a corrupted OT pair, then  $\mathcal{A}^{\text{sh}}$  appends this exchange to  $\mathbb{V}_{\rho+1}^{\text{sim}}(c_\alpha)$  if the message is meant for  $c_\alpha$  and ignores it otherwise. **Need to potentially add it to the view later. How do I fix this?**

We have covered all cases where  $\mathbb{V}_{\rho+1}(\mathcal{A}^{\text{mal}})$  may differ from  $\mathbb{V}_{\rho+1}(\mathcal{A}^{\text{sh}})$  assuming that  $\mathbb{V}_\rho^{\text{sim}}(\mathcal{A}^{\text{mal}}) \supset \mathbb{V}_\rho(\mathcal{A}^{\text{mal}})$  and  $\mathcal{C}_\rho^{\text{sh}} = \mathcal{C}_\rho^{\text{mal}}$ . In each case, we have shown that  $\mathcal{A}^{\text{sh}}$  can simulate the view of  $\mathcal{A}^{\text{mal}}$  if parties in  $\mathcal{C}_\rho^{\text{mal}} \cup c_\alpha$  send arbitrary messages. At this point, if there exists randomness  $\vec{r}$  (of  $\mathcal{S}, \mathcal{C}, \mathcal{A}^{\text{mal}}, \mathcal{A}^{\text{sh}}$ ) s.t.  $\mathbb{V}_{\rho+1}^{\text{sim}}(\mathcal{A}^{\text{mal}}) \not\supset \mathbb{V}_{\rho+1}(\mathcal{A}^{\text{mal}})$ . Since  $\mathcal{A}^{\text{sh}}$  is internally simulating  $\mathcal{A}^{\text{mal}}$ , it must be that at a certain point, as a result of  $\mathcal{A}^{\text{mal}}$  actually sending messages in the real protocol execution, and  $\mathcal{A}^{\text{sh}}$  not,  $\mathcal{A}^{\text{mal}}$  *recieved a message from a party outside of  $\mathcal{C}^{\text{mal}}$ , and  $\mathcal{A}^{\text{sh}}$  didn't*. But this is impossible.  $\square$

**Need more words now.** Thus, the existence  $\mathcal{A}^{\text{mal}}$  gives us a semi-honest adversary  $\mathcal{A}^{\text{sh}}$  with at least as much corruption probability, which is a contradiction to our semi-honest result.  $\square$

## References

- GIOZ17. Juan A. Garay, Yuval Ishai, Rafail Ostrovsky, and Vassilis Zikas. The price of low communication in secure multi-party computation. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, volume 10401 of *Lecture Notes in Computer Science*, pages 420–446. Springer, 2017.

HKN<sup>+</sup>05. Danny Harnik, Joe Kilian, Moni Naor, Omer Reingold, and Alon Rosen. On robust combiners for oblivious transfer and other primitives. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, pages 96–113, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

## A Lemma 1: Calculation of $p_1, \dots, p_6$

We compute  $p_1, \dots, p_6$ , as defined in the proof of Lemma 1. For brevity, we let  $\theta'$  denote  $\theta - \epsilon$ .<sup>6</sup>

1. In round 1,  $s_i$  creates the OT pair and therefore knows both  $m_i^{(0)}$  and  $m_i^{(1)}$ .  $X_i^{(1)} = 1$  if and only if  $s_i$  gets corrupted in round 1 or the (future) corresponding  $s_{ij}$  gets corrupted in round 1 and is not decorrputed at the end of it so  $\mathcal{A}$  receives  $m_i^{(\sigma_i)}$  at the start of round 2.<sup>7</sup>

$$\begin{aligned}
 p_1 &= \Pr[s_i \in C'_1] + \Pr[s_{ij} \notin D_1 | s_{ij} \in C'_1] \cdot \Pr[s_{ij} \in C'_1] \\
 &\quad - \Pr[s_{ij} \notin D_1 | s_{ij} \in C'_1] \cdot \Pr[\{s_i, s_{ij}\} \subset C'_1] \\
 &= \frac{|C'_1|}{n} + (1 - \lambda) \frac{|C'_1|}{n} - (1 - \lambda) \left( \frac{|C'_1|}{n} \right)^2 \\
 &= \frac{\theta' n}{n} + (1 - \lambda) \frac{\theta' n}{n} - (1 - \lambda) \left( \frac{\theta' n}{n} \right)^2 \\
 &= (2 - \lambda)\theta' - (1 - \lambda)\theta'^2
 \end{aligned}$$

2. In round 2,  $s_i$  still knows both  $m_i^{(0)}$  and  $m_i^{(1)}$ . Also, an adversary controlling  $s_{ij}$  receives  $m_i^{(1-\sigma_i)}$  and has a reference to  $s_i$  that holds  $m_i^{(\sigma_i)}$ .  $X_i^{(2)} = 1$  if and only if  $s_i$  or  $s_{ij}$  get corrupted in round 2. In round 2,  $\mathcal{A}$  randomly corrupts from the set of uncorrupted servers which is of size  $n - |C'_1|$ .

$$\begin{aligned}
 p_2 &= \Pr[s_i \in C'_2 | s_i \notin C'_1] + \Pr[s_{ij} \in C'_2 | s_{ij} \notin C'_1] \\
 &\quad - \Pr[\{s_i, s_{ij}\} \subset C'_2 | s_i \notin C'_1 \wedge s_{ij} \notin C'_1] \\
 &= \frac{|C'_2|}{n - |C'_1|} + \frac{|C'_2|}{n - |C'_1|} - \left( \frac{|C'_2|}{n - |C'_1|} \right)^2 \\
 &= 2 \frac{\lambda \theta' n}{n - \theta' n} - \left( \frac{\lambda \theta' n}{n - \theta' n} \right)^2 \\
 &= \frac{2\lambda\theta'}{1 - \theta'} - \frac{\lambda^2\theta'^2}{(1 - \theta')^2}
 \end{aligned}$$

<sup>6</sup> Computer algebra calculation given at <https://github.com/GnarlyMshtep/price-of-low-com-followup-calculations>.

<sup>7</sup>  $m_i^{\sigma_i}$  is the message sent by  $s_i$  to  $s_{ij}$  as defined in Protocol  $\Pi_{\text{sh}}^{\text{mob}}$  (Figure 1).

3. In round 3,  $s_i$  has forgotten the identity of  $s_{ij}$  but  $s_{ij}$  still remembers  $s_i$ . Therefore, if  $s_i$  is the one holding  $m_i^{(2-\alpha)}$ , it suffices to corrupt either  $s_i$  or  $s_{ij}$ .  
 Need to change all this to make it more clear which is left, which is right  
 $X_i^{(3)} = 1$  if and only if either  $\sigma_i = 2 - \alpha$  and  $\mathcal{A}$  corrupts  $s_{ij}$  or  $\sigma_i = \alpha - 1$  and  $\mathcal{A}$  corrupts  $s_{ij}$  or  $s_i$ . For brevity, let  $N_l^i$  denote the event  $\bigwedge_{k \in [l]} s_i \notin C'_k$  and  $N_l^{ij}$  denote the event  $\bigwedge_{k \in [l]} s_{ij} \notin C'_k$ .

$$\begin{aligned}
 p_3 &= \Pr[\sigma_i = 2 - \alpha] \cdot \Pr[s_{ij} \in C'_3 | N_2^{ij}] + \Pr[\sigma_i = \alpha - 1] \cdot (\Pr[s_i \in C'_3 | N_2^i] \\
 &\quad + \Pr[s_{ij} \in C'_3 | N_2^{ij}] - \Pr[\{s_i, s_{ij}\} \subset C'_3 | N_2^i \wedge N_2^{ij}]) \\
 &= \frac{1}{2} \frac{|C'_3|}{n - |C'_1| - |C'_2|} + \frac{1}{2} \left( 2 \frac{|C'_3|}{n - |C'_1| - |C'_2|} - \left( \frac{|C'_3|}{n - |C'_1| - |C'_2|} \right)^2 \right) \\
 &= \frac{1}{2} \frac{\lambda c' n}{n - c' n - \lambda \theta' n} + \frac{1}{2} \left( 2 \frac{\lambda \theta' n}{n - \theta' n - \lambda \theta' n} - \left( \frac{\lambda \theta' n}{n - \theta' n - \lambda \theta' n} \right)^2 \right) \\
 &= \frac{3}{2} \frac{\lambda \theta'}{1 - (1 + \lambda) \theta'} - \frac{1}{2} \left( \frac{\lambda \theta'}{1 - (1 + \lambda) \theta'} \right)^2
 \end{aligned}$$

4.  $p_4$  can be calculated in the same way as  $p_3$ . However, the adversary corrupts randomly from a smaller set.

$$\begin{aligned}
 p_4 &= \frac{1}{2} \frac{|C'_4|}{n - \sum_{k \in [3]} |C'_k|} + \frac{1}{2} \left( 2 \frac{|C'_4|}{n - \sum_{k \in [3]} |C'_k|} - \left( \frac{|C'_4|}{n - \sum_{k \in [3]} |C'_k|} \right)^2 \right) \\
 &= \frac{3}{2} \frac{\lambda \theta'}{1 - (1 + 2\lambda) \theta'} - \frac{1}{2} \left( \frac{\lambda \theta'}{1 - (1 + 2\lambda) \theta'} \right)^2
 \end{aligned}$$

5. In round 5,  $s_i$  has erased its entire internal state and  $s_{ij}$  has erased the identity of  $s_i$  so  $X_i^{(5)} = 1$  if and only if  $\sigma_i = 2 - \alpha$  and  $\mathcal{A}$  corrupts  $s_{ij}$ .

$$\begin{aligned}
 p_5 &= \Pr[\sigma_i = 2 - \alpha] \cdot \Pr[s_{ij} \in C'_5 | N_4^{ij}] \\
 &= \frac{1}{2} \frac{|C'_5|}{n - \sum_{k \in [4]} |C'_k|} \\
 &= \frac{1}{2} \frac{\lambda \theta'}{1 - (1 + 3\lambda) \theta'}
 \end{aligned}$$

6. Again,  $p_6$  is the same as  $p_5$  except for  $\mathcal{A}$  corrupting from a smaller set.

$$\begin{aligned}
 p_6 &= \frac{1}{2} \frac{|C'_6|}{n - \sum_{k \in [5]} |C'_k|} \\
 &= \frac{1}{2} \frac{\lambda \theta'}{1 - (1 + 4\lambda) \theta'}
 \end{aligned}$$

## B compute $\mathfrak{P}$

Do a new computer algebra calculation for the rational functions in reduced form directly. Also should these be functions of  $\lambda$  as well or can we do away without that since we have fixed  $\lambda$  at the start? I think we cannot because of the continuous root argument. Technically,  $\theta(\lambda)$  is not a single root but a contour/level plane/solution curve. Wait is it a polynomial? Maybe thinking about this a bit deeper (mathematically) might simplify some writing.

Consider the rational functions  $\mathfrak{p}_\rho(x)$  for  $\rho \in [6]$  defined by replacing  $\theta'$  with  $x$  in  $p_\rho$  (Appendix A) such that  $p_\rho = \mathfrak{p}_\rho(\theta')$ . We use computer algebra to rewrite

$$1 - \prod_{\rho \in [6]} (1 - \mathfrak{p}_\rho) = \frac{1}{2} + \frac{\mathfrak{P}(x)}{r(x)}$$

where  $\mathfrak{P}(x)$  and  $r(x)$  are (the unique) relatively prime polynomials such that the above holds and  $r(x)$  is a monic with positive leading coefficient. The computation of these polynomials was done with the help of a computer algebra software (ref) and the coefficients of  $\mathfrak{P}(x)$  have been listed in Figure 2. Recall that  $\theta$  was chosen to be a root of this polynomial such that  $\mathfrak{P}(\theta) = 0$ .<sup>8</sup> It suffices to show, since  $r(x) > 0$ , that for sufficiently small (justify)  $\epsilon > 0$ ,  $\mathfrak{P}(\theta - \epsilon) < 0$ . We show this by observing the coefficients of  $\mathfrak{P}(x)$  and deduce that a small nudge in the input changes the output in the same direction.

---

<sup>8</sup> Since  $\mathfrak{P}(x)$  has multiple roots, we need to specify which root we are talking about. Note that when  $\lambda = 0$ ,  $\mathfrak{P}(x)$  has only one root (justify) between 0 and 1. We pick  $\theta$  to be this root and since  $\mathfrak{P}$  is also a polynomial in  $\lambda$ , the root we pick is the (unique) one that changes continuously with  $\lambda$ .