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 $\mathrm{poly}(n)$ rounds.

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

A (t, λ) mobile adversary $\mathcal{A}$ can have at most t parties corrupted simulatenously. As a part of the model, we impose that, at the end of each round, $\mathcal{A}$ can only decorrupt λ fraction of his servers to study how the corruption bound varies with λ. 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 λt servers. In analogy to rushing adversaries in the standard model, if P_i is corrupted under $\mathcal{A}$'s control in round 2ρ and in round $2\rho - 1$ P_j sent P_i a message, that message will be avalabile to $\mathcal{A}$ at the begining of tound 2ρ (where it would only be available to P_j at the begining 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 ρ 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 ρ 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 Π_{sh}^{mob} computing the OT functionality in the $(2, n)$-client/server model with erasures in the presence of a mobile (t, λ)-adversary A/B (where λt is the number of parties that can be decorrupted at the end of every round) with $t < (\theta(\lambda) - \epsilon)\, n$ for any ϵ where $0 < \epsilon < \theta(\lambda)$. Moreover, Π_{sh}^{mob} communicates $O(\log^{\delta} n)$ bits.*

Here $\Pi_{\mathrm{sh}}^{\mathrm{mob}}$ is nearly the same semi-honest adaptive protocol given in [GIOZ17] (server wakes up with small probability, generate OT-pair, send half to an intermidiary, 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_α 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 recieve 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 ρ. 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+05], to show the protocol is secure we must show that for all (t, λ) 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 ovrerview the main ideas of each part below:

(a) Describe (t, λ) adversary $\mathcal{A}^\dagger$ (corrupt t random servers in round 1, decorrupt λt random servers in every other round, if a corrupted server sends / recieves 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 simillar outline to the first half of the semi-honest adaptive upper bound of [GIOZ17]: we isolate out an overconnected set of servers who recieve 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, λ) 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 increrases.

(c) Show (Lemma 3) that except from with negligable 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 necessery 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 toloerate (t, λ) 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, λ) adversary with t less than $0.293n, 0.214n, 0.125n, 0.079n$, respectively.[1] Notice that for $\lambda = 0$ we recover the semi-honest adaptive upper bound of [GIOZ17][Thm #], as desired.

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

Protocol $\Pi^{\mathsf{mob}}_{\mathsf{sh}}$

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 S_1 denote the set of parties that become active in this round. Every $s_i \in \mathcal{S}_1$ prepares an OT pair $((m_i^{(0)}, m_i^{(1)}), \mathtt{otid}_i)$, where $\mathtt{otid}_i \in \{0,1\}^{\log^{\delta} n}$ shouldn't log log n suffice? is a uniformly chosen identifier. Every $s_i \in \mathcal{S}_1$ choses an intermediary $s_{ij} \in \mathcal{S}$ as well as $\sigma_i \in \{0,1\}$ uniformly at random and sends $(\sigma_i, m_i^{\sigma_i}, \mathtt{otid}_i)$ 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 $(m_i^{\sigma_i}, \mathtt{otid}_i)$. Every $s_i \in \mathcal{S}_1$ sends $(m_i^{1-\sigma_i}, \mathtt{otid}_i)$ 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 $(m_i^{\sigma_i}, \mathtt{otid}_i)$ to c_{σ_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 $\mathtt{otid}$'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 Π^{mob}_{sh} 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, λ)-adversary (where λt is the number of parties that can be decorrupted at the end of every round) with $t < (\theta(\lambda) - \epsilon)\, n$. $\theta(\lambda)$ is the solution to*

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

for a_i given in Figure 2 and for any ϵ where $0 < \epsilon < \theta(\lambda)$. Moreover, Π^{OT}_{mob} 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_α denote the corrupted client where $\alpha \in \{0,1\}$. For $b \in \{0,1\}$ let $m_1^{(b)}, \ldots, m_g^{(b)}$ 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 $C_\rho^{\mathcal{A}} \subset [n]$ denote the indices of servers corrupted by $\mathcal{A}$ at the start of round ρ. Let $\mathcal{C}_\rho^{\mathcal{A}} \subset [n]$ be the indices of corrupted servers after $\mathcal{A}$ makes its round ρ corruptions and before it makes its round ρ decorruptions 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 ρ we get that

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

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 $\mathbb{V}_p(s)$ 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,*

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

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_α 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+05], to show the protocol is secure we must show that for all (t, λ) adversaries $\mathcal{A}$ [2]

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

We divide the rest of the proof into 3 parts:

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

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

.

[2] All probabilities in this proof are over the randomenss 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, λ) 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 negligable 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 $k \in \mathcal{C}_\rho$, recieves 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 behaivor* acting on references *and denote the set of servers corrupted by refrences in round ρ as R_ρ and the set of servers corrupted by reference up to and including round ρ 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 λt random servers from $\mathcal{S} \setminus \cup_{i=1}^{\rho-1} C_i$. At end of round $\rho = 1, \dots, 6$, $\mathcal{A}^\dagger$ decorrupts λt 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 (λ, t) adversary.

Proposition 1. *Except from with negligable 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 δ, except from with negligable 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 Π_{sh}^{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 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 negligable 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 $\mathcal{S}_1 \backslash \mathcal{S}^{\text{overconnected}}$ and $\mathcal{S}_2 \backslash \mathcal{S}^{\text{overconnected}}$ form a perfect matching, with s_i sending a message to a unique s_{ij}. For $s_i \in \mathcal{S}_1 \backslash \mathcal{S}^{\text{overconnected}}$ 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 $\Pr\left[|\mathcal{O}^{\mathcal{A}}| \geq \frac{|\mathcal{S}_1|}{2}\right]$ 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_ρ 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 $\rho \in [6]$,

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

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

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

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

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

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

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 C and list the coefficients of $\mathfrak{P}(x)$ in Table 2 [3]. Recall $\theta(\lambda)$ was chosen such that $\mathfrak{P}(\theta(\lambda))=0$ (λ fixed in Theorem 2's statement). In Appendix C 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 μ, $|\mathcal{S}'|<\epsilon'|\mathcal{S}_1|$ 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. □

[3] Computer algebra calculation given at `https://github.com/GnarlyMshtep/price-of-low-com-followup-calculations`.

Lemma 2. *For all* (t, λ) *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. $\Pr[|\mathcal{O}^{\mathcal{A}}| \geq |\mathcal{S}_1|/2] > \Pr[|\mathcal{O}^{\mathcal{A}}| \geq |\mathcal{S}_1|/2]$. 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 $\mathcal{A} = \mathcal{A}'$. □

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 simillar 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 $\mathcal{A} = \mathcal{A}'$. □

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

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

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 becuase, (a) $\mathbb{V}(k_i) = \mathbb{V}(a_i)$ when not conditioned on anything and (b) as of round ρ, 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 decorruptions is nearly identical and we leave it to the reader. □

Proposition 5. *Wlog, $\mathcal{A}$ decorrupts λt 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 $\mathcal{S}\backslash\mathcal{C}$ and decorrupts 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 $\mathcal{A}$. □

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, decorrupts 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 $\mathbf{C}^{\mathcal{A}} = (|C_k^{\mathcal{A}} \backslash R_k^{\mathcal{A}}|)_{k\in[6]}$, 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 $\mathfrak{r} = (r_{\mathcal{A}}, (r_p)_{p \in \mathcal{P}})$ we have that $\mathbb{V}_{\mathcal{A}}(\mathfrak{r}) \subset \mathbb{V}_{\mathcal{A}'}(\mathfrak{r})$ 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 $\mathfrak{r}$. Since other than corrupting refrences, $\mathcal{A}$ randomly corrupts from the set of previously uncorrupted servers, $\mathcal{A}$' can use $\mathfrak{r}$ to compute $A = \{s_{i_1}, \ldots, s_{i_{t(1+5\lambda)}}\} \subset \mathcal{S}$ where for some $0 = j_0 \leq \cdots \leq j_5 \leq j_6 \leq t(1+5\lambda)$ (potentially unkown to $\mathcal{A}'$) we have that $C_\rho^{\mathcal{A}} \backslash R_\rho^{\mathcal{A}} = \{s_{j_{\rho-1}}, \ldots, s_{j_\rho}\}$.

$\mathcal{A}'$ 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 λt servers from A. Before decorrupting in round ρ, $\mathcal{A}'$ can simulate $\mathcal{A}$ and and learn $D_\rho^{\mathcal{A}}$. Since (by induction on ρ) $\mathcal{C}_\rho^{\mathcal{A}} \subset \mathcal{C}_\rho^{\mathcal{A}'}$, at the end of round ρ, $\mathcal{A}'$ decorrupts $D_\rho^{\mathcal{A}}$. Notice that if $\mathcal{A}$ had corrupted some s by reference in round ρ 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 $\mathbb{V}_{\mathcal{A}}(\mathfrak{r}) \subset \mathbb{V}_{\mathcal{A}'}(\mathfrak{r})$, concluding the proof.

□

This concludes the proof of Lemma 2. □

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

Since every message has $O(1)$ bits, we will prove that the message complexity of $\Pi_{\text{sh}}^{\text{mob}}$ 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 δ'. □

This concludes the proof of Theorem 1. □

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 $f_{\mathrm{OT}}((m_0, m_1), b) = (\perp, m_b)$ that can tolerate every (t, λ) semi-honest mobile adversary for $t > (\theta(\lambda) + \epsilon)n$ and $\theta(\lambda)$ is defined in the statement of Theorem 2. Since protocol $\Pi^{\mathrm{mob}}_{\mathrm{sh}}$ (Figure 1) can tolerate any (t, λ) semi-honest mobile adversary for $t < (\theta(\lambda) - \epsilon)n$ (Theorem 2), $\Pi^{\mathrm{mob}}_{\mathrm{sh}}$ 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 protcols Π that compute the OT functionality with sublinear communication (No statement made about security yet! Just needs to corretly compute OT) 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 Π. 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 $\bar{\mathcal{A}}$). This means that for $\lambda = 0$ they behave the same way.[4] They then consider a slightly weaker adversary [5] $\hat{\mathcal{A}}$ 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 Π 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

[4] For the lower bound, they actually consider a weaker adversary that doesn't corrupt servers talking to c_α.

[5] 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. ≤ 0.45 for $\lambda = 1/2$) 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 $\bar{\mathbf{P}} \subset \mathbf{P}$ of protocols characterized by some property and proving the lower bound for these protocols.

Definition 4 (message path in Π). *Let Π 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 $k >= 0$. Formally, a message path from u to v, $P_{u,v}$, in Π 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 ρ_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.

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

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 an OT setting).

Definition 5 (protocols where correlation implies root server). *Consider the subset $\bar{\boldsymbol{P}} \subset \boldsymbol{P}$ of protocols Π where c_0, c_1's views consist only of OT components and identities of parties that send them. Further assume that c_0, c_1 sharing an OT 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 ρ its view contains (m_0, m_1) and that there exist message paths P_{s,c_0} and P_{s,c_1} in Π where the first message is sent in round ρ and the last message in P_{s,c_b} is received by c_b before m_b enters its view for the first time for $b \in \{0, 1\}$.*

Proposition 7. *Let $s \in \mathcal{P} = \mathcal{S} \cup \{c_0, c_1\}$ such that in round ρ its view contains (m_0, m_1). Let Π 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 Π where the first message is sent in round ρ 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 ρ. 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 ρ.

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

Proof. Assume that it erases m_1 in round $\rho + 1$. This means it either sends m_1 in round ρ or not at all. The latter gives us a contradiction as c_1 eventually sees 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 ρ 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. Comparing this with the corruptions in $\Pi_{\text{sh}}^{\text{mob}}$ it is clear (if Π doesn't send to a client randomly, i think i need a slightly different adversary that works according to the protocol, so might need to introduce another parameter and show that $1/2$ is optimal) 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 ρ and $\rho + 1$. And l_1 (r_1) also has a ref to m_0 (m_1) in $\rho + 2, \rho + 3$ by corrupting the entire path to c_0 (c_1). The following calculation shows that $\mathcal{A}^\dagger$ with corruption budget $\theta(\lambda) + \epsilon$ learns (m_0, m_1) with probability at least $1/2$. We just show that factor being < 1 when required.

Proposition 8. *Let $\Pi \in \bar{\mathbf{P}}$. Then Π 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 $(m_0^{(i)}, m_1^{(i)})$ that c_0 and c_1 share has more than $1/2$ probability of being learned by $\mathcal{A}^\dagger$. Thus, if Π can tolerate $\mathcal{A}^\dagger$, there must exist a secure combiner for OT that tolerates an insecure majority, which I think is a contradiction.

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 $\Pi^{\text{adaptive}}_{\text{malicous}}$

1. Servers wake up with probability $log^{\delta} n/n$.
2. Each woken server s_i prepares an OT pair and sends a random half of it to random server s_{ij}
   (a) okay, consider the "nueanced" model only for the mobile adversaries, so there is no s_i erases, etc, round.
3. s_i and s_{ij} erase their entire state, except from the half of the OT-pair they will each send c_1, c_2 respectively.
   (a) An s_{ij} receiving any message not of the format above will simply ignore it.
4. s_i, s_{ij} send respective half of OT pairs to c_1, c_2 respectively.
5. If c_b receives more than $(1-324\epsilon^4-288\epsilon^5-64\epsilon^6)\log^{\delta} n$ messages (similar to Page 19, step 5), it aborts and alerts the other player
6. c_1, c_2 use malicious OT-combiner to get one honest OT-pair.

Fig. 3. A protocol tolerant of malicious adaptive adversaries

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

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

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

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

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

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

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

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

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

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

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 ρ and $\mathcal{A}^{\text{sh}}$ can simulate $\mathcal{A}^{\text{mal}}$'s view at the start of round ρ, 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 ρ (then $\mathbb{V}_{\rho+1}(s)$ is the view at the end of round ρ). 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 $\mathbb{V}_{\rho+1}^{sim}(c_\alpha)$ if the message is meant for c_α 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. $\mathbb{V}_{\rho+1}^{\text{sim}}(\mathcal{A}^{\text{mal}}) \not\supset \mathbb{V}(\mathcal{A}^{\text{mal}})_{\rho+1}$. 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 proocol 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. □

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. □

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+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 θ' denote $\theta - \epsilon$. [6]

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 decorrupted at the end of it so $\mathcal{A}$ receives $m_i^{(\sigma_i)}$ at the start of round 2. [7]

$$\begin{aligned}
p_1 &= \Pr[s_i \in C_1'] + \Pr[s_{ij} \notin D_1 | s_{ij} \in C_1'] \cdot \Pr[s_{ij} \in C_1'] \\
&\quad - \Pr[s_{ij} \notin D_1 | s_{ij} \in C_1'] \cdot \Pr[\{s_i, s_{ij}\} \subset C_1'] \\
&= \frac{|C_1'|}{n} + (1-\lambda)\frac{|C_1'|}{n} - (1-\lambda)\left(\frac{|C_1'|}{n}\right)^2 \\
&= \frac{\theta' n}{n} + (1-\lambda)\frac{\theta' n}{n} - (1-\lambda)\left(\frac{\theta' n}{n}\right)^2 \\
&= (2-\lambda)\theta' - (1-\lambda)\theta'^2
\end{aligned}$$

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 $n - |C_1'|$.

$$\begin{aligned}
p_2 &= \Pr[s_i \in C_2' | s_i \notin C_1'] + \Pr[s_{ij} \in C_2' | s_{ij} \notin C_1'] \\
&\quad - \Pr[\{s_i, s_{ij}\} \subset C_2' | s_i \notin C_1' \wedge s_{ij} \notin C_1'] \\
&= \frac{|C_2'|}{n-|C_1'|} + \frac{|C_2'|}{n-|C_1'|} - \left(\frac{|C_2'|}{n-|C_1'|}\right)^2 \\
&= 2\frac{\lambda\theta' n}{n-\theta' n} - \left(\frac{\lambda\theta' n}{n-\theta' n}\right)^2 \\
&= \frac{2\lambda\theta'}{1-\theta'} - \frac{\lambda^2\theta'^2}{(1-\theta')^2}
\end{aligned}$$

[6] Computer algebra calculation given at `https://github.com/GnarlyMshtep/price-of-low-com-followup-calculations`.

[7] $m_i^{\sigma_i}$ is the message sent by s_i to s_{ij} as defined in Protocol $\Pi_{\mathrm{sh}}^{\mathrm{mob}}$ (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 Calculations for (133)

B.1 Upper bound

Fix some OT pair (m_0, m_1) Once again, we calculate p_1 through p_4 where p_i is the probability is (an upper bound on) the probability that $\mathcal{A}^\dagger$ learns (m_0, m_1) in round i given it didn't learn it in the previous rounds. It learns m_α with prob. 1 so we bound the probability it learns $m_{1-\alpha}$.

In fact, for ease of computation we calculate $q_i = 1 - p_i$. Note that $\mathcal{A}^\dagger$ learns the pair with probability less than $1 - \prod q_i$. So we equate $\prod q_i = 1/2$ to find $\theta(\lambda)$.

1. q_1 is at least the probability that s_i is not corrupted in round 1 and s_{ij} is either not corrupted or corrupted and then decorrupted at the end of round 1. Since corruptions are made independently at random, this probability is
$$(1-\theta)(1-\theta(1-\lambda))$$
2. q_2 is at least the prob. that s_i and s_{ij} are not corrupted in the second round.
$$\left(1 - \frac{\lambda\theta}{1-\theta}\right)^2$$
3. By round 3, s_i erases the identity of s_{ij} so corrupting it only gives us the $m_{1-\alpha}$ with probability 1/2. However, corrupting s_{ij} still gives both. So q_3 is at least
$$\left(1 - \frac{\lambda\theta}{1-\theta-\lambda\theta}\right)\left(1 - \frac{1}{2}\frac{\lambda\theta}{1-\theta-\lambda\theta}\right)$$
4. Similarly q_4 is at least
$$\left(1 - \frac{\lambda\theta}{1-\theta-2\lambda\theta}\right)\left(1 - \frac{1}{2}\frac{\lambda\theta}{1-\theta-2\lambda\theta}\right)$$

   Therefore $\mathcal{A}$ learns the pair with probability at most $1 - \prod q_i$. This probability increases in θ so we solve it for $\prod q_i = 1/2$ and then $\theta - \epsilon$ gives us a probability strictly less than 1/2 as required.

B.2 Lower bound

In the proof, we isolated two cases:

1. In this case we have two servers that know the pair (i.e. $\mathcal{A}^\dagger$ corrupting them can learn the pair) in rounds ρ and $\rho + 1$ and one server that knows the pair while another that knows half of it in rounds $\rho + 2$ and $\rho + 3$. The exact same calculations with $\theta + \epsilon$ show that $\mathcal{A}^\dagger$ learns it with probability greater than 1/2.

2. Here, the situation is slightly different. In rounds $\rho+2, \rho+3$ we have two servers that have half of the message. So we miss out on a half given by the other server. But we gain on another server r_1 that has a reference to the pair in rounds $\rho, \rho+1$. It remains to show that this is an increase in probability. **NOT OPTIMAL FOR THIS ADV BUT OPTIMAL FOR STRONGER ONE**. By bounding the probability that $\mathcal{A}$ learns (m_0, m_1) in this case, we show that it is greater than the probability of winning in case 1. The calculation boils down to

$$(1-c_1)(1-c_2) \leq \left(1-\frac{c_3}{2}\right)\left(1-\frac{c_4}{2}\right)$$

C compute $\mathfrak{P}$

$\theta(\lambda)$ is not a single root but a contour/ level plane/solution curve. I think it's the inverse of some function that we can explicitly describe but I need to find which one. We can approximate the inverse using `https://randorithms.com/2021/08/31/Taylor-Series-Inverse.html#:~:text=For%20example%2C%20if%20we%20have,3y3%2B...`. The inverse makes sense for fixed λ we get an inverse of the polynomial that evaluates to the root at zero. But what does the inverse of a multivariate function even mean?

In the worst case, we discretize λ taking values separated at 0.01 between $[0,1]$, use root-finding algorithms to evaluate $\theta(\lambda)$ and then use polynomial interpolation or splinefitting.

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. In fact for any λ it has only one root justify between 0 and 0.3 which is the only one of interest. So we always pick that root.