# Oblivious Transfer in Incomplete Networks

Varun Narayanan and Vinod M. Prabahakaran

Tata Institute of Fundamental Research, Mumbai
varun.narayanan@tifr.res.in, vinodmp@tifr.res.in

**Abstract.** Secure message transmission and Byzantine agreement have been studied extensively in incomplete networks. However, information theoretically secure multiparty computation (MPC) in *incomplete* networks is less well understood. In this paper, we characterize the conditions under which a pair of parties can compute *oblivious transfer (OT)* information theoretically securely against a general adversary structure in an incomplete network of reliable, private channels. We provide characterizations for both semi-honest and malicious models. A consequence of our results is a complete characterization of networks in which a given subset of parties can compute any functionality securely with respect to an adversary structure in the semi-honest case and a partial characterization in the malicious case.

## 1 Introduction

Secure message transmission (SMT) [12, 33, 13, 34, 28, 36, 35] and Byzantine agreement [31, 12, 14, 15, 37] in incomplete networks have been studied extensively. However, information theoretically secure multiparty computation (MPC) in *incomplete* networks is less well studied with a few notable exceptions [26, 6, 3, 17]. In this paper we consider the problem of realizing *oblivious transfer (OT)* between a given pair of parties in an incomplete network of reliable, private links with unconditional security with respect to a general adversary structure. We characterize networks in which a given pair of parties may securely compute OT in both the semi-honest and malicious models. For the malicious case, our characterization is limited to statistical security.

For a pair of parties $A$ and $B$ to compute OT securely in an incomplete network, an approach which might suggest itself is the following. Try to complete the network (or a part of the network which includes $A$ and $B$) by using SMT to realize the missing private links. Then, use a protocol for complete networks [4, 9, 24] on the 'completed' (part of the) network to realize OT between $A$ and $B$. It turns out that such a direct approach is, in general, not adequate. In particular, Figure 1 shows a network where this approach fails, but it is still possible to realize OT securely.

In the graph $G$ (Figure 1), vertices represent parties and edges represent private authenticated communication links. Our characterization (Theorem 1) shows that $A$ and $B$ can realize 2-secure OT in $G$ in the semi-honest case. However, we cannot achieve this using the aforementioned direct approach. Observe

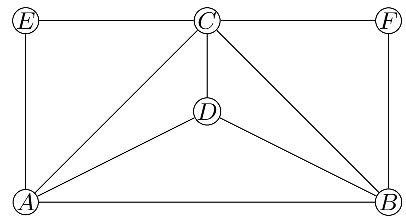


**Fig. 1.** Semi-honest 2-secure OT between $A$ and $B$ is possible in $G$ by Theorem 1. However, a 'direct' approach of completing (a part of) the network using semi-honest SMT with 2-security and applying a standard MPC protocol for complete networks does not work.

that the pairs of vertices that are not already connected by an edge are only 2-connected, hence no new semi-honest 2-secure links can be established in this network using SMT. Thus, the biggest complete network containing $A$ and $B$ that can be obtained by such a 'completion' is the subgraph induced by vertices $A, B, C, D$. Theorem 1 also shows that 2-secure OT between $A$ and $B$ is impossible in this induced subgraph. Alternatively, this impossibility can be seen as follows. If 2-secure OT can be realized between a pair of parties in a complete network with 4 parties, then, by symmetry, it is possible to set up 2-secure OT between every pair of parties in the network. This would imply semi-honest 2-secure MPC in a network with 4 parties [18, 19], which is impossible [4, 9].

Standard results [18, 19, 11, 20, 25] allow reduction of MPC to establishing pairwise OT between the parties wishing to compute securely. In the semi-honest case, a consequence of our result is a complete characterization of networks in which a given subset of parties can compute any functionality with perfect privacy with respect to a given adversary structure. When the adversary is malicious, our results imply a condition that is necessary for statistically secure computation of any functionality among a given subset of parties in an incomplete network. This condition is also sufficient for statistically secure computation of any functionality, but *with abort and no fairness*.

### 1.1 Our Model and Results

Consider a simple graph $G(\mathcal{V}, \mathcal{E})$ on a set $\mathcal{V}$ of $n$ parties (or vertices), where each undirected edge $\{u, v\} \in \mathcal{E}$ represents a private, authenticated, synchronous, bidirectional communication link between the distinct parties $u$ and $v$. Let $A, B \in \mathcal{V}$ be two distinct parties. Given an adversary structure $\mathbb{Z} \subseteq 2^{\mathcal{V}}$, we seek necessary and sufficient conditions on $G$ so that $A$ and $B$ may compute OT with unconditional security with respect to (w.r.t.) the adversary structure $\mathbb{Z}$. By security w.r.t. $\mathbb{Z}$, we mean security against the corruption of every set of parties in $\mathbb{Z}$. We restrict our attention to static adversaries, but consider both the semi-honest and malicious cases.

Given a vertex $u \in \mathcal{V}$ and a subset of vertices $\mathcal{Z} \subseteq \mathcal{V}$, we define *u-blocked vertices of* $\mathcal{Z}$, denoted by $\Gamma_u(\mathcal{Z})$, as the set of vertices whose every path to $u$ contains some vertex in $\mathcal{Z}$. Our main result for the semi-honest case is the following:

**Theorem 1.** *Given a graph $G(\mathcal{V}, \mathcal{E})$ and an adversary structure $\mathbb{Z}$, two distinct parties $A, B \in \mathcal{V}$ can compute OT with perfect unconditional security in the semi-honest, static adversary setting if and only if the following conditions are satisfied:*

1. *For every $\mathcal{Z} \in \mathbb{Z}$ such that $A, B \notin \mathcal{Z}$, there exists a path from $A$ to $B$ that does not have any vertex from $\mathcal{Z}$.*
2. *There do not exist sets of parties $\mathcal{Z}_A, \mathcal{Z}_B \in \mathbb{Z}$ such that $A \in \mathcal{Z}_A$, $B \notin \mathcal{Z}_A$, $B \in \mathcal{Z}_B$, $A \notin \mathcal{Z}_B$, and*

$$\Gamma_B(\mathcal{Z}_A) \cup \Gamma_A(\mathcal{Z}_B) = \mathcal{V}.$$

*Moreover, when these conditions are satisfied and $|\mathbb{Z}| = \mathsf{poly}(n)$, there is an efficient ($\mathsf{poly}(n)$ complexity) protocol to compute OT securely.*

Standard results [18, 19] imply that if every pair in a set of vertices can realize oblivious transfer with security w.r.t. $\mathbb{Z}$, then these vertices can compute any functionality with security w.r.t. $\mathbb{Z}$.

**Corollary 1.** *Given a graph $G(\mathcal{V}, \mathcal{E})$ and a subset of vertices $\mathcal{K} \subseteq \mathcal{V}$, any functionality can be computed among the vertices in $\mathcal{K}$ with perfect security with respect to a semi-honest adversary structure $\mathbb{Z}$ if and only if the conditions in Theorem 1 are satisfied by every pair of vertices in $\mathcal{K}$.*

The proof is provided in Appendix A. When $G$ is complete, $\Gamma_u(\mathcal{Z}) = \mathcal{Z}$ whenever $u \notin Z \subset \mathcal{V}$. Hence, when $\mathcal{K} = \mathcal{V}$, the condition in Corollary 1 is equivalent to non-existence of sets $\mathcal{Z}_1, \mathcal{Z}_2 \in \mathbb{Z}$ such that $\mathcal{Z}_1 \cup \mathcal{Z}_2 = \mathcal{V}$. Thus, for this case, we retrieve the $\mathcal{Q}^2$ condition of Hirt and Maurer [24].

While the focus of this paper is on deriving tight necessary and sufficient conditions on the network which permit information theoretically secure computation, we consider efficiency in two regimes for $t$-privacy (i.e., semi-honest adversary structures of the form $\mathbb{Z}^t := \{\mathcal{Z} \subset \mathcal{V} : |\mathcal{Z}| \leq t\}$). Theorem 1 already gives an efficient protocol for $t = O(1)$. We separately consider the case of $n = 2t + O(1)$ and give an efficient protocol in this setting as well (when the conditions of Theorem 1 are satisfied). The case of other regimes of $t$ remains open.

The following is our result for the malicious case:

**Theorem 2.** *Two vertices $A, B$ in $G(\mathcal{V}, \mathcal{E})$ can realize OT with statistical security (with guaranteed output delivery) against an adversary structure $\mathbb{Z}$ in the malicious static adversary setting if and only if the following conditions are satisfied:*

1. *For every $\mathcal{Z}_1, \mathcal{Z}_2 \in \mathbb{Z}$ such that $A, B \notin \mathcal{Z}_1 \cup \mathcal{Z}_2$, there exists a path from $A$ to $B$ that does not have any vertex from $\mathcal{Z}_1 \cup \mathcal{Z}_2$.*

*2. There do not exist* $\mathcal{Z}_A, \mathcal{Z}_B, \mathcal{Z} \in \mathbb{Z}$ *such that* $A \in \mathcal{Z}_A$*,* $B \notin \mathcal{Z}_A$*,* $B \in \mathcal{Z}_B$*,* $A \notin \mathcal{Z}_B$*,* $A, B \notin \mathcal{Z}$*, and*

$$\Gamma_B(\mathcal{Z}_A \cup \mathcal{Z}) \cup \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z}) = \mathcal{V}.$$

*Moreover, when these conditions are satisfied and* $|\mathbb{Z}| = \mathsf{poly}(n)$*, there is an efficient (*$\mathsf{poly}(n)$ *complexity) protocol to compute OT securely.*

This characterization can be easily extended to 2-party functionalities with output only at one party since standard results [27] allow reduction of such functionalities to establishing OT between the parties. Unlike in the semi-honest case, the availability of secure OT between every pair of parties does not directly imply that any functionality may be computed securely in the malicious case. Hence, we have a more modest implication in this case using standard results in [11, 20] and [25].

**Corollary 2.** *Consider a graph* $G(\mathcal{V}, \mathcal{E})$*, a subset of vertices* $\mathcal{K} \subseteq \mathcal{V}$ *and a malicious adversary structure* $\mathbb{Z}$*.*

1. *The vertices in* $\mathcal{K}$ *can statistically securely compute any functionality w.r.t.* $\mathbb{Z}$ *only if every pair of vertices in* $\mathcal{K}$ *satisfies the conditions in Theorem 2.*
2. *The vertices in* $\mathcal{K}$ *can statistically securely compute any functionality* with abort and no fairness *w.r.t.* $\mathbb{Z}$ *if every pair of vertices in* $\mathcal{K}$ *satisfies the conditions in Theorem 2.*

The proof is provided in Appendix B. When $G$ is complete and $\mathcal{K} = \mathcal{V}$, we indeed recover the $\mathcal{Q}^3$ condition of Hirt and Maurer [24]. Note that, for this case, [24] shows that $\mathcal{Q}^3$ condition is sufficient to achieve perfect security.

### 1.2 Technical Overview

We now give a quick overview of the technical details of our results.

**Necessity of Conditions: Semi-honest Case.** The first condition in Theorem 1 is simply the necessary (and sufficient) condition for SMT between $A$ and $B$ in the semi-honest setting. To show the necessity of the second condition, we observe that security w.r.t. the adversary structure $\{\mathcal{Z}_A, \mathcal{Z}_B\}$ implies security w.r.t. $\{\Gamma_B(\mathcal{Z}_A), \Gamma_A(\mathcal{Z}_B)\}$, i.e., we may throw into $\mathcal{Z}_A$ those vertices which it blocks from reaching $B$, and, similarly, for $\mathcal{Z}_B$ and $A$. Our condition simply says that this should not be a $\mathcal{Q}^2$ adversary structure [24].

**Sufficiency of Conditions: Semi-honest Case.** To show the sufficiency of these conditions, we first observe (Lemma 1) that if one could find a vertex $C$ which cannot be blocked from an honest $A$ or $B$, then $C$ can provide $A$ and $B$ with precomputed OT through SMT channels. But, in general, the conditions in Theorem 1 do not guarantee that such a $C$ exists. Our approach is to find a set of such $C$'s such that a majority of them will work against each member of the

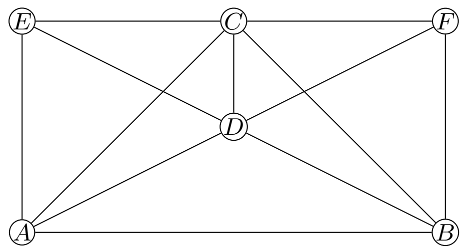


**Fig. 2.** $H_{\mathsf{OT}}$: OT between $A$ and $B$ is not possible with security against the malicious adversary structure $\{\{C\}, \{A, D\}$ and $\{B, D\}\}$.

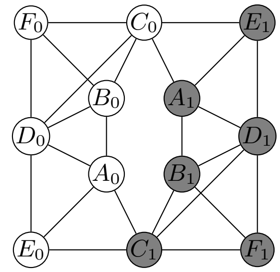


**Fig. 3.** $S_{\mathsf{OT}}$: constructed by interconnecting two copies of $H_{\mathsf{OT}}$.

adversary structure. This will allow us to employ the idea of *OT combiner* [22, 23, 32, 38] to obtain one protocol which is secure w.r.t. the adversary structure. The bulk of our proof is in showing that there is a set of such $C$'s. In fact, we do this for a special class of adversary structures (Lemma 3) – those with only one member which contains $A$ ($B$, respectively). We show that, in this case, the vertices $C$ of interest are precisely those that are not blocked from $B$ ($A$, respectively) the unique member of the adversary structure which contains $A$ ($B$, respectively). We then obtain a protocol for OT in the general case by employing the idea of OT combiner again, this time on the protocols constructed for the special class of adversary structures above.

**Efficiency of $t$-privacy.** Our protocol has complexity which is polynomial in the size of the graph and the size of the adversary structure. So, it is efficient for $t$-privacy when $t = O(1)$. We also give a $t$-private protocol which is efficient when $n = 2t+O(1)$. For this, we first consider adversary structures where all the members which contain $A$ ($B$, respectively) block the same set of vertices. We show that for such an adversary structure, using OT combiner, we may construct an efficient protocol for OT. We show that, similar to the construction in the general case, we may combine these protocols to get a $t$-private OT protocol. If $n = 2t + O(1)$, the number of such adversary structures is polynomial in $n$, thereby making the combiner efficient.

**Necessity of Conditions: Malicious Case.** The first condition of Theorem 2 is just the necessary (and sufficient) condition for SMT between $A$ and $B$ in the malicious setting. We show the necessity of the second condition by reducing the problem to the case of an OT in a specific graph and showing that such an OT cannot be computed securely in that graph using arguments similar to the proof of impossibility of Byzantine agreement by Fischer *et al.* in [15]. For ease of exposition, in Section 3, we consider a special case (the general case is proved in the appendix along similar lines), which we reduce to the case of the graph $H_{\mathsf{OT}}$ in Figure 2 (Lemma 5). To show that $A$ and $B$ cannot compute OT in

$H_{\mathsf{OT}}$ securely w.r.t. the malicious adversary structure $\{\{C\}, \{A, D\}, \{B, D\}\}$, we interconnect two copies of $H_{\mathsf{OT}}$ (see Figure 3) and consider (a pair of) executions of a purported OT protocol to argue that this would give a secure two-party OT protocol in the semi-honest setting (Lemma 4).

**Sufficiency of Conditions: Malicious Case.** To show the sufficiency of these conditions, we proceed along the lines of the semi-honest case. But here, we construct a separate OT protocol corresponding to each set in the adversary structure which does not contain either $A$ or $B$. The parties in this set do not participate in the protocol thereby ensuring that it is perfectly secure against their corruption. However, the corruption of any other set in the adversary structure may force this protocol to abort. But, if the protocol does not abort, it is guaranteed to compute OT with statistical security w.r.t $\mathbb{Z}$. Our final protocol iterates over every protocol of this kind. If the OT is computed in any iteration, it is guaranteed to be statistically secure. If every iteration is aborted, either $A$ or $B$ is corrupt, in which case, a honest $B$ may output a random bit.

### 1.3 Related Work

Secure multiparty computation in complete networks is addressed in a large body of literature. Ben-Or, Goldwasser, and Wigderson [4] and Chaum, Crépeau, and Damgård [9] showed that every function can be computed with perfect information theoretic security against a semi-honest adversary whenever there is an honest majority; and against a malicious adversary if more than two-third of the parties are honest. Hirt and Maurer [24] extended these results and characterized adversary structures, in both semi-honest and malicious settings, that allow perfectly secure computation. Keeping these results in view, our problem formulation is a natural one. However, to the best of our knowledge, there is no prior work on the characterization problem we address even in restricted settings of graph topologies other than the complete graph. We list below the works in the literature that come closest to our problem.

Franklin and Yung [16] studied private message exchange in incomplete networks of hypergraph communication channels with the goal of performing secure computation over such networks. Jakoby, Liśkiewicz, and Reischuk [26] studied the trade-off between connectivity and randomness required for private computation. Bläser *et al.* [6] characterized Boolean functions which can be computed with 1-privacy in non-2-connected networks. Beimel [3] studied the case of general functions in the same setting. Garay and Ostrovsky [17] introduced the notion of almost-everywhere secure computation where, in an incomplete network of potentially small degree, secure computation is accomplished by all but a small number of honest parties. Improvements on the results in [17] were reported by Chandran, Garay, and Ostrovsky in [8]. They also studied the case of edge corruptions in [7]. For non-2-connected networks, Bläser *et al.* [5] studied protocols that provide a relaxed notion of privacy for functions that cannot be privately computed in an incomplete network. Harnik, Ishai, and Kushilevitz [22] and

Kumaresan, Raghuraman, and Sealfon [29] characterized incomplete networks of OT channels which, when used along with a *complete* pairwise communication network, allow $t$-secure computation. Halevi *et al.* [21] studied notions of security in multiparty computation with restricted interaction patterns.

Privacy and reliability of communication over incomplete networks has been extensively studied. The problems of reliable and private message transmission have been studied for threshold adversary structures [12, 13, 33, 34, 36, 1, 30, 35] and for arbitrary adversary structures [28]. The problem of Byzantine agreement was studied in [31, 12, 14, 15, 37].

## 2 Semi-Honest Case

In this section we prove Theorem 1. We start with some notation and definitions which will be used throughout the sequel. We define the following subclasses of an adversary structure $\mathbb{Z}$.

$$\mathbb{Z}_A := \{\mathcal{Z} \in \mathbb{Z} \mid A \in \mathcal{Z}\},$$
$$\mathbb{Z}_B := \{\mathcal{Z} \in \mathbb{Z} \mid B \in \mathcal{Z}\},$$
$$\mathbb{Z}_{\neg A \neg B} := \{\mathcal{Z} \in \mathbb{Z} \mid A, B \notin \mathcal{Z}\}.$$

Clearly if $\mathcal{Z} \in \mathbb{Z}_A \cup \mathbb{Z}_B$, then it cannot be in $\mathbb{Z}_{\neg A \neg B}$ by definition. If $\mathcal{Z} \in \mathbb{Z}_A \cap \mathbb{Z}_B$, then $A, B \in \mathcal{Z}$, but any protocol is trivially secure against the corruption of such a set since only $A$ and $B$ have inputs and outputs. Hence, without loss of generality, we consider only adversary structures $\mathbb{Z}$ that do not contain such sets. Thus, $\mathbb{Z}_A, \mathbb{Z}_B$, and $\mathbb{Z}_{\neg A \neg B}$ form a partition of $\mathbb{Z}$.

**Definition 1.** *Given a pair of vertices $u, v \in \mathcal{V}$ in an undirected graph $G(\mathcal{V}, \mathcal{E})$, a* ***path*** *from $u$ to $v$ is a sequence of distinct vertices such that $u$ is the first vertex and $v$ is the last vertex and there is an edge between every pair of consecutive vertices. The length-one sequence $u$ is a path from $u$ to $u$.*

**Definition 2.** *Given a vertex $u \in \mathcal{V}$ and a subset of vertices $\mathcal{Z} \subseteq \mathcal{V}$, we define* ***$u$-blocked vertices of $\mathcal{Z}$*** *as the set of vertices whose every path to $u$ includes some vertex in $\mathcal{Z}$. We denote this set by $\Gamma_u(\mathcal{Z})$.*

$$\Gamma_u(\mathcal{Z}) := \{v \in \mathcal{V} \mid \textit{every path from } v \textit{ to } u \textit{ has a vertex from } \mathcal{Z}\}.$$

### 2.1 Necessity of Conditions

**Necessity of the first condition.** Secure OT can be used for secure communication, i.e., secure message transmission (SMT). So a necessary condition for SMT is also a necessary condition for OT. SMT between $A$ and $B$ is possible (if and) only if for every $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$ there is a path from $A$ to $B$ that has no vertex from $\mathcal{Z}$ [13]. Hence, OT between $A$ and $B$ with security w.r.t. $\mathbb{Z}$ is possible only if the first condition in Theorem 1 is satisfied.

**Necessity of the second condition.** We show that if the second condition in Theorem 1 is not satisfied, a protocol that can realize OT between $A$ and $B$ would imply a 2-party OT protocol. The necessity then follows from the impossibility of 2-party OT. Suppose the second condition is not satisfied, then there are $\mathcal{Z}_A \in \mathbb{Z}_A$ and $\mathcal{Z}_B \in \mathbb{Z}_B$ such that $\Gamma_B(\mathcal{Z}_A) \cup \Gamma_A(\mathcal{Z}_B) = \mathcal{V}$. Let $\Pi$ be an OT protocol that is secure against the corruption of $\mathcal{Z}_A$ and $\mathcal{Z}_B$.

*Claim 1.* $\Pi$ is secure against the corruption of $\Gamma_B(\mathcal{Z}_A)$ and of $\Gamma_A(\mathcal{Z}_B)$.

*Proof.* We prove that $\Pi$ is secure against the corruption of $\Gamma_B(\mathcal{Z}_A)$, the other case can be proved in a similar manner. Let $u$ be a vertex in $\Gamma_B(\mathcal{Z}_A) \setminus \mathcal{Z}_A$ and $v$ be any vertex outside $\Gamma_B(\mathcal{Z}_A)$. By the definition of $B$-blocked vertices of $\mathcal{Z}_A$ (*i.e.,* $\Gamma_B(\mathcal{Z}_A)$), every path from $u$ to $B$ has a vertex from $\mathcal{Z}_A$ and $v$ has a path to $B$ that has no vertex from $\mathcal{Z}_A$. Hence, every path from $u$ to $v$ must have a vertex from $\mathcal{Z}_A$. Also, no vertex in $\Gamma_B(\mathcal{Z}_A) \setminus \mathcal{Z}_A$ has inputs since $A \in \mathcal{Z}_A$ and $B \notin \Gamma_B(\mathcal{Z}_A)$. Hence we may conclude that the vertices in $\Gamma_B(\mathcal{Z}_A) \setminus \mathcal{Z}_A$ do not have inputs or outputs and are separated from $\mathcal{V} \setminus \Gamma_B(\mathcal{Z}_A)$ by $\mathcal{Z}_A$. Consequently, the *view* of $\Gamma_B(\mathcal{Z}_A) \setminus \mathcal{Z}_A$ may be simulated by $\mathcal{Z}_A$. Since $\Pi$ is secure against the corruption of $\mathcal{Z}_A$, it must also be secure against the corruption of $\Gamma_B(\mathcal{Z}_A)$. □

Now consider three parties $\mathcal{P}_1, \mathcal{P}_2$, and $\mathcal{P}_3$. Let $\mathcal{P}_3$ simulate vertices in the set $\mathcal{Z} := \Gamma_B(\mathcal{Z}_A) \cap \Gamma_A(\mathcal{Z}_B)$ and $\mathcal{P}_1$ and $\mathcal{P}_2$ simulate $\Gamma_B(\mathcal{Z}_A) \setminus \mathcal{Z}$ and $\Gamma_A(\mathcal{Z}_B) \setminus \mathcal{Z}$ respectively. By Claim 1, there is a 3-party protocol $\Pi_3$ that computes OT between $\mathcal{P}_1$ and $\mathcal{P}_2$ that is secure against the corruption of $\{\mathcal{P}_1, \mathcal{P}_3\}$ and that of $\{\mathcal{P}_2, \mathcal{P}_3\}$. Since $\mathcal{P}_3$ does not have any input, $\Pi_3$ is also secure against the corruption of $\{\mathcal{P}_1\}$ (and $\{\mathcal{P}_2\}$); see [22, Lemma 2]. From $\Pi_3$ we can get a 2-party OT protocol $\Pi_2$ by letting one party simulate $\mathcal{P}_1$ and the other party simulate $\{\mathcal{P}_2, \mathcal{P}_3\}$ (see [22, Section 3.2]), yielding a contradiction.

### 2.2 Sufficiency of Conditions

Next, we construct a protocol $\Pi_{\mathsf{sh}}$ for OT between $A$ and $B$ that is secure w.r.t. an adversary structure $\mathbb{Z}$ if the conditions in Theorem 1 are met. If the size of $\mathbb{Z}$ is polynomial in $n$, the $\Pi_{\mathsf{sh}}$ constructed is efficient. We first consider a few special cases that will lead us up to the general case.

For the complete graph on 3 vertices $A, B, C$, 1-secure OT between $A$ and $B$ can be realized as follows: Vertex $C$ samples a *precomputed OT* uniformly at random and sends it privately to $A$ and $B$, who use this to securely realize OT [2]. i.e., $C$ samples independent, uniform bits $r_0, r_1, c$ and then sends $(r_0, r_1)$ to $A$ and $(c, r_c)$ to $B$ privately. $B$ sends to $A$ the sum $u := b \oplus c$ of its input $b$ with $c$, where $\oplus$ denotes addition in the binary field. Let $(x_0, x_1)$ be the input to $A$, then $A$ replies with $(y_0, y_1) := (x_0 \oplus r_u, x_1 \oplus r_{1 \oplus u})$. $B$ reconstructs $x_b$ as $y_b \oplus r_c$.

We first generalize the above protocol to networks and adversary structures where we can find a node $C$ which can not be corrupted together with $A$ or $B$, and such that it can communicate to $A$ with privacy against $\mathbb{Z}_B$ and to $B$ with privacy against $\mathbb{Z}_A$.

**Lemma 1.** *Consider $G(\mathcal{V}, \mathcal{E})$ with vertices $A, B \in \mathcal{V}$ and a semi-honest adversary structure $\mathbb{Z}$ that satisfy the conditions in Theorem 1. Suppose there exists a vertex $C$ such that*

*(i)* $\forall \mathcal{Z}_A \in \mathbb{Z}_A, C \notin \Gamma_B(\mathcal{Z}_A)$, *and*
*(ii)* $\forall \mathcal{Z}_B \in \mathbb{Z}_B, C \notin \Gamma_A(\mathcal{Z}_B)$.

*Then, there is an efficient protocol $\Pi^C$ for securely computing OT between $A$ and $B$.*

The protocol involves $C$ sending precomputed OT to $A$ and $B$ using SMT. $A$ and $B$ use it to carry out OT by using the standard protocol from [2] mentioned above. In carrying out the OT, $A$ and $B$ communicate with each other using SMT; something which the first condition of Theorem 1 guarantees is possible. The conditions in the lemma ensure that if $C$ is corrupt, $A$ and $B$ must be honest and, since they carry out OT over SMT, they have privacy. If $A$ is corrupt, the conditions in the lemma guarantee that both $C$ and $B$ are honest, and have a path of honest vertices between them ensuring the privacy of SMT from $C$ to $B$ used to deliver the precomputed OT. The privacy of $B$'s input then follows. A similar argument can be made for the case when $B$ is corrupt. The full proof which includes a description of $\Pi^C$ is deferred to Appendix C. Note that $A$ is a valid candidate for the choice of $C$ in Lemma 1 if (and only if) $\mathbb{Z}_A$ is empty, i.e., $A$ is honest. Similarly, $B$ is a valid choice if and only if $\mathbb{Z}_B$ is empty, i.e., $B$ is honest. The protocols, $\Pi^A$ and $\Pi^B$, for these cases will play a role in the sequel.

In general, the conditions in Theorem 1 do not imply the existence of a vertex $C$ that satisfies the conditions in Lemma 1. Our approach is to next consider several protocols of the kind used in the proof of this lemma, each corresponding to a potentially different choice of $C$. In general, no such protocol on its own may be secure against the corruption of each set in $\mathbb{Z}$. We invoke the idea of *OT combiner* [22, 23, 32, 38] to obtain one protocol which is secure w.r.t. $\mathbb{Z}$. An OT combiner is a compiler of OT protocols which produces one OT protocol which is secure w.r.t. $\mathbb{Z}$ by 'combining' many OT protocols, none of which is secure against the corruption of every set in $\mathbb{Z}$.

**Lemma 2.** *[22, 23, 32, 38]*

*Let $\Pi_1, \ldots, \Pi_m$ be $m$ protocols for OT between $A$ and $B$, such that against the passive corruption of every $\mathcal{Z} \in \mathbb{Z}$, a majority of $\Pi_1, \ldots, \Pi_m$ is secure. Then, there exists a protocol* $\mathsf{Combiner}(\Pi_1, \ldots, \Pi_m)$ *for OT between $A$ and $B$ which is secure w.r.t. the semi-honest adversary structure $\mathbb{Z}$. Moreover, this protocol is efficient if $m$ is polynomial in $n$, and $\Pi_i$ is efficient for each $i \in [m]$.*

We proceed in two steps. We first consider adversary structures $\mathbb{Z}$ such that $\mathbb{Z}_A$ (or $\mathbb{Z}_B$) is a singleton set. Specifically, we first prove our result for adversary structure $\mathbb{Z} = \{\mathcal{Z}_A\} \cup \mathbb{Z}_B \cup \mathbb{Z}_{\neg A \neg B}$ where $\mathcal{Z}_A$ is such that $A \in \mathcal{Z}_A$; similarly, we consider $\mathbb{Z} = \{\mathcal{Z}_B\} \cup \mathbb{Z}_A \cup \mathbb{Z}_{\neg A \neg B}$, where $\mathcal{Z}_B$ is such that $B \in \mathcal{Z}_B$. We will later use this to prove our general result.

**Lemma 3.** *Consider $G(\mathcal{V},\mathcal{E})$ with vertices $A, B \in \mathcal{V}$ and a semi-honest adversary structure $\mathbb{Z} = \{\mathcal{Z}_A\} \cup \mathbb{Z}_B \cup \mathbb{Z}_{\neg A \neg B}$, where $A \in \mathcal{Z}_A$, ($\mathbb{Z} = \{\mathcal{Z}_B\} \cup \mathbb{Z}_A \cup \mathbb{Z}_{\neg A \neg B}$, $B \in \mathcal{Z}_B$, respectively) that satisfy the conditions in Theorem 1. There is an efficient protocol $\Pi^{\mathcal{Z}_A}$ ($\Pi^{\mathcal{Z}_B}$, respectively) that securely realizes OT between $A$ and $B$.*

Before we present the construction of the protocols, we make the following claims.

*Claim 2.* For every $C \notin \Gamma_B(\mathcal{Z}_A)$, the protocol $\Pi^C$ (Protocol 11) is secure w.r.t. $\{\mathcal{Z}_A\} \cup \mathbb{Z}_{\neg A \neg B}$.

*Proof.* If $C \notin \Gamma_B(\mathcal{Z}_A)$, then $C$ satisfies both the conditions in Lemma 1 for the adversary structure $\{\mathcal{Z}_A\} \cup \mathbb{Z}_{\neg A \neg B}$. This proves the claim. □

*Claim 3.* Let $\mathcal{Z}'_B \in \mathbb{Z}_B$, then there exists $C \notin \Gamma_B(\mathcal{Z}_A) \cup \Gamma_A(\mathcal{Z}'_B)$. The protocol $\Pi^C$ (Protocol 11) is secure w.r.t. $\{\mathcal{Z}_A\} \cup \mathbb{Z}_{\neg A \neg B} \cup \{\mathcal{Z}'_B\}$.

*Proof.* If there exists a $C \notin \Gamma_B(\mathcal{Z}_A) \cup \Gamma_A(\mathcal{Z}'_B)$, then $C$ satisfies both the conditions in Lemma 1 for the adversary structure $\{\mathcal{Z}_A\} \cup \mathbb{Z}_{\neg A \neg B} \cup \{\mathcal{Z}'_B\}$ and second part of the claim follows. Such a $C$ must exist, since $\Gamma_B(\mathcal{Z}_A) \cup \Gamma_A(\mathcal{Z}'_B) \neq \mathcal{V}$ by the second condition in Theorem 1. □

Similar claims can be made regarding the adversary structure $\{\mathcal{Z}_B\} \cup \mathbb{Z}_A \cup \mathbb{Z}_{\neg A \neg B}$, and the proof for these claims are similar.

Claims 2, 3 directly imply the following observations. For $\mathcal{Z}_A \in \mathbb{Z}_A$, let $\mathcal{V} \setminus \Gamma_B(\mathcal{Z}_A) = \{C^1, \ldots, C^{k_A}\}$. Note that $\mathcal{V} \setminus \Gamma_B(\mathcal{Z}_A)$ is non-empty since $B \notin \Gamma_B(\mathcal{Z}_A)$. Then, by Claim 2, $\Pi^{C^i}$ is secure w.r.t. $\{\mathcal{Z}_A\} \cup \mathbb{Z}_{\neg A \neg B}$ for all $i \in [k_A]$. By Claim 3, for each $\mathcal{Z}'_B \in \mathbb{Z}_B$, there exists $i \in [k_A]$ such that $\Pi^{C^i}$ is secure w.r.t. $\{\mathcal{Z}_A\} \cup \mathbb{Z}_{\neg A \neg B} \cup \{\mathcal{Z}'_B\}$. Similarly, for $\mathcal{Z}_B \in \mathbb{Z}_B$, let $\mathcal{V} \setminus \Gamma_A(\mathcal{Z}_B) = \{C^1, \ldots, C^{k_B}\}$. Then $\Pi^{C^i}$ is secure w.r.t. $\{\mathcal{Z}_B\} \cup \mathbb{Z}_{\neg A \neg B}$ for all $i \in [k_B]$. For each, $\mathcal{Z}'_A \in \mathbb{Z}_A$ there exists $i \in [k_B]$ such that $\Pi^{C^i}$ is secure w.r.t. $\{\mathcal{Z}'_A\} \cup \mathbb{Z}_{\neg A \neg B} \cup \{\mathcal{Z}_B\}$.

*Proof (Proof of Lemma 3).*

Consider a collection of protocols $\Pi_1, \ldots \Pi_{2k_A-1}$, where $\Pi_i := \Pi^{C^i}$ for $i \in [k_A]$ and $\Pi_i := \Pi^A$ for $i = k_A + 1, \ldots, 2k_A - 1$. We construct the protocol $\Pi^{\mathcal{Z}_A}$ as $\mathsf{Combiner}(\Pi_1, \ldots, \Pi_{2k_A-1})$. Since $\Pi_1, \ldots \Pi_{2k_A-1}$ are protocols for OT between $A$ and $B$, this is a valid combiner. As we argued above, $\Pi_1, \ldots, \Pi_{k_A}$ ($= \Pi^{C^1}, \ldots, \Pi^{C^{k_A}}$) are secure w.r.t. $\{\mathcal{Z}_A\} \cup \mathbb{Z}_{\neg A \neg B}$. Hence a majority of the protocols ($k_A$ out of $2k_A - 1$ protocols) used in the combiner is secure w.r.t. $\{\mathcal{Z}_A\} \cup \mathbb{Z}_{\neg A \neg B}$. The security of $\Pi^{\mathcal{Z}_A}$ w.r.t. $\{\mathcal{Z}_A\} \cup \mathbb{Z}_{\neg A \neg B}$ now follows from Lemma 2. Consider the corruption of any $\mathcal{Z}'_B \in \mathbb{Z}_B$. Since $A$ is honest (i.e., $A \notin \mathcal{Z}'_B$), the $k_A - 1$ copies of $\Pi^A$ used in the combiner are secure against the corruption of $\mathcal{Z}'_B$. As we previously observed, for each $\mathcal{Z}'_B \in \mathbb{Z}_B$, at least one of the protocols $\Pi_1, \ldots, \Pi_{k_A}$ is secure against the corruption of $\mathcal{Z}'_B$. Hence, at least $k_A$ protocols used in the combiner are secure against the corruption of each $\mathcal{Z}'_B \in \mathbb{Z}_B$. From Lemma 2, it follows that $\Pi^{\mathcal{Z}_A}$ is secure w.r.t. $\mathbb{Z}_B$ and hence against $\{\mathcal{Z}_A\} \cup \mathbb{Z}_{\neg A \neg B} \cup \mathbb{Z}_B$. Observe that $\Pi^{\mathcal{Z}_A}$ is a combiner of $2k_A - 1 < 2n$

protocols of the kind $\Pi^C$. Since, by Lemma 1, each of these protocols is efficient, $\Pi^{\mathcal{Z}_A}$ is efficient according to Lemma 2.

Similarly, the protocol $\Pi^{\mathcal{Z}_B} := \mathsf{Combiner}(\Pi_1, \dots \Pi_{2k_B-1})$, where $\Pi_i := \Pi^{C^i}$ for $i \in [k_B]$ and $\Pi_i := \Pi^B$ for $i = k_B + 1, \dots, 2k_B - 1$ will efficiently realize OT between $A$ and $B$ with security w.r.t. $\{\mathcal{Z}_B\} \cup \mathbb{Z}_{\neg A \neg B} \cup \mathbb{Z}_A$. □

We are finally ready to prove Theorem 1. The idea is to combine protocols of the kind $\Pi^{\mathcal{Z}_A}, \mathcal{Z}_A \in \mathbb{Z}_A$ and $\Pi^{\mathcal{Z}_B}, \mathcal{Z}_B \in \mathbb{Z}_B$ in a way such that a majority of these protocols is secure against the corruption of every set of vertices in $\mathbb{Z}$.

*Proof (Proof of Theorem 1).* If the adversary structure $\mathbb{Z}$ is such that $\mathbb{Z}_A$ ($\mathbb{Z}_B$), respectively) is empty then, we have already seen that $\Pi^A$ ($\Pi^B$, respectively) is secure w.r.t. $\mathbb{Z}$. So, let $\mathbb{Z}_A = \{\mathcal{Z}_A^1, \dots, \mathcal{Z}_A^{\ell_A}\}$ and $\mathbb{Z}_B = \{\mathcal{Z}_B^1, \dots, \mathcal{Z}_B^{\ell_B}\}$. We consider the following pairs of protocols.

$$(\Pi_{1,1}, \Pi_{1,2}), \dots, (\Pi_{\ell_A,1}, \Pi_{\ell_A,2}), (\Pi_{\ell_A+1,1}, \Pi_{\ell_A+1,2}), \dots, (\Pi_{\ell_A+\ell_B,1}, \Pi_{\ell_A+\ell_B,2}),$$

where

$$(\Pi_{i,1}, \Pi_{i,2}) := (\Pi^{\mathcal{Z}_A^i}, \Pi^B), \text{ for } 1 \le i \le \ell_A, \tag{1}$$

$$(\Pi_{\ell_A+i,1}, \Pi_{\ell_A+i,2}) := (\Pi^{\mathcal{Z}_B^i}, \Pi^A), \text{ for } 1 \le i \le \ell_B. \tag{2}$$

Let $\Pi_{\mathsf{sh}} := \mathsf{Combiner}((\Pi_{1,1}, \Pi_{1,2}) \dots, (\Pi_{\ell_A+\ell_B,1}, \Pi_{\ell_A+\ell_B,2}))$. All the protocols used in the combiner realize OT between $A$ and $B$, hence the combiner is valid. For all $\mathcal{Z}_A \in \mathbb{Z}_A$ and $\mathcal{Z}_B \in \mathbb{Z}_B$, $\Pi^{\mathcal{Z}_A}$ and $\Pi^{\mathcal{Z}_B}$ are secure w.r.t. $\mathbb{Z}_{\neg A \neg B}$ by Lemma 3. $\Pi^A$ and $\Pi^B$ are also secure w.r.t. $\mathbb{Z}_{\neg A \neg B}$. Therefore, by Lemma 2, $\Pi_{\mathsf{sh}}$ is secure w.r.t. $\mathbb{Z}_{\neg A \neg B}$. The essential idea for the proof of security of $\Pi_{\mathsf{sh}}$ w.r.t. $\mathbb{Z}_A \cup \mathbb{Z}_B$ is the fact that for each $\mathcal{Z} \in \mathbb{Z}_A \cup \mathbb{Z}_B$, both protocols in the pair corresponding to $\mathcal{Z}$ are secure against the corruption of $\mathcal{Z}$ and at least one protocol from every other pair is also secure against the corruption of $\mathcal{Z}$. Hence, a majority of protocols used in the combiner is secure against the corruption of $\mathcal{Z}$.

Formally, let $\mathcal{Z}_A^j$ be any set in $\mathbb{Z}_A$. Note that $(\Pi_{j,1}, \Pi_{j,2}) = (\Pi^{\mathcal{Z}_A^j}, \Pi^B)$. By Lemma 3, $\Pi^{\mathcal{Z}_A^j}$ is secure against the corruption of $\mathcal{Z}_A^j$. Also, $\Pi^B$ is secure against the corruption of $\mathcal{Z}_A^j$ since $B \notin \mathcal{Z}_A^j$. Hence, the pair of protocols $(\Pi_{j,1}, \Pi_{j,2})$ is secure against the corruption of $\mathcal{Z}_A^j$. Among the other pairs, for $1 \le i \le \ell_A$, the protocols $\Pi_{i,2}$ are copies of $\Pi^B$ and hence, secure against the corruption of $\mathcal{Z}_A^j$. For the remaining pairs, note that $\Pi_{\ell_A+i,1} = \Pi^{\mathcal{Z}_B^i}, 1 \le i \le \ell_B$ are also secure against the corruption of $\mathcal{Z}_A^j$ by Lemma 3. Thus, at least $\ell_A + \ell_B + 1$ protocols (among $2(\ell_A + \ell_B)$) protocols used in the combiner are secure against the corruption of $\mathcal{Z}_A^j$. Hence, by Lemma 2, $\Pi_{\mathsf{sh}}$ is secure against the corruption of this set. This proves that the protocol $\Pi_{\mathsf{sh}}$ is secure w.r.t. $\mathbb{Z}_A$. The proof of security against $\mathbb{Z}_B$ is similar.

If the size of $\mathbb{Z}_A \cup \mathbb{Z}_B$ is polynomial in $n$, $\Pi_{\mathsf{sh}}$ is a combiner of $\mathsf{poly}(n)$ protocols, each of which is efficient by Lemma 3. Hence, in this case $\Pi_{\mathsf{sh}}$ is efficient by Lemma 2. □

### 2.3 Efficiency of $t$-privacy

A protocol is said to be *t-private* if it is secure w.r.t. the semi-honest adversary structure $\mathbb{Z}^t := \{\mathcal{Z} \subseteq \mathcal{V} : |\mathcal{Z}| \leq t\}$. Without loss of generality, we restrict our attention to $t < n/2$ since OT cannot be computed with $\lceil n/2 \rceil$-privacy even in a complete graph [4, 9]. We have the following result:

**Theorem 3.** *Given a communication graph $G(\mathcal{V}, \mathcal{E})$, vertices $A, B \in \mathcal{V}$ can compute OT with perfect $t$-privacy if and only if the following conditions are satisfied:*

1. *There exists an edge or at least $t+1$ vertex disjoint paths between $A$ and $B$.*
2. *There do not exist $\mathcal{Z}_A, \mathcal{Z}_B \subset \mathcal{V}$ of size at most $t$ such that $A \in \mathcal{Z}_A, B \notin \mathcal{Z}_A, A \notin \mathcal{Z}_B, B \in \mathcal{Z}_B$, and $\Gamma_B(\mathcal{Z}_A) \cup \Gamma_A(\mathcal{Z}_B) = \mathcal{V}$.*

*Moreover, this can be performed using an efficient protocol if $t = O(1)$ or $n = 2t + O(1)$.*

The conditions 1 and 2 above are just restatements of the conditions in Theorem 1 for $\mathbb{Z}^t$. The efficiency when $t = O(1)$ follows from Theorem 1 as the size of the adversary structure in this case is $\mathsf{poly}(n)$. It only remains to construct an efficient $t$-private OT protocol for the case of $n = 2t + O(1)$. In Appendix D, we give such a protocol and prove the theorem.

## 3 Malicious Case

In this section, we characterize graphs in which a given pair of vertices may realize OT with statistical security w.r.t. an adversary structure $\mathbb{Z}$ in the static malicious setting.

### 3.1 Necessity of Conditions

**Necessity of the first condition.** If $A$ and $B$ can compute OT with statistical security, then they can communicate with non-trivial (greater than 1/2) probability of success. Necessity of the condition follows from the fact that in a graph, if $A$ and $B$ are disconnected by removing two vertices $C$ and $D$ from the graph, then $A$ and $B$ cannot communicate with non-trivial probability of success w.r.t the adversary structure $\{\{C\}, \{D\}\}$ in the malicious setting [15]. Note that although the proof in [15] is for communication with zero-error, it also works for communication with non-trivial probability of success. A full proof of the necessity of this condition is included in Appendix E.

**Necessity of the second condition.** We show that in a graph $G$, it is impossible to realize OT between two of its vertices $A$ and $B$ with statistical security w.r.t. the adversary structure $\mathbb{Z}$ if the second condition is not satisfied, *i.e.,* there exists $\mathcal{Z}_A \in \mathbb{Z}_A, \mathcal{Z}_B \in \mathbb{Z}_B$, and $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$ such that

$$\Gamma_B(\mathcal{Z}_A \cup \mathcal{Z}) \cup \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z}) = \mathcal{V}. \tag{3}$$

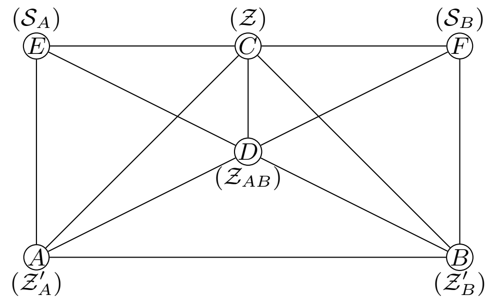


**Fig. 4.** $H_{\mathsf{OT}}(\mathcal{V}_{H_{\mathsf{OT}}}, \mathcal{E}_{H_{\mathsf{OT}}})$: OT between $A$ and $B$ with security w.r.t. malicious adversary structure $\{\{C\}, \{A, D\}, \{B, D\}\}$ is impossible (Lemma 4). The sets shown inside brackets correspond to the vertex identification used in the proof of Lemma 5.

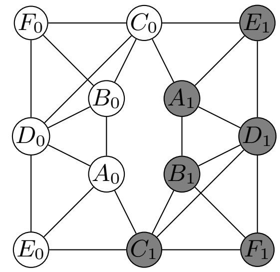


**Fig. 5.** $S_{\mathsf{OT}(\mathcal{V}_{S_{\mathsf{OT}}}, \mathcal{E}_{S_{\mathsf{OT}}})}$: Constructed by interconnecting two copies of $H_{\mathsf{OT}}$. We analyze the scenario where $v_i, i = 0, 1$ in $S_{\mathsf{OT}}$ execute the instructions for $v$ in $H_{\mathsf{OT}}$ for protocol $\Pi$ faithfully.

For the ease of exposition, we provide a proof for a special case where the following additional conditions hold for the sets $\mathcal{Z}_A, \mathcal{Z}_B$ and $\mathcal{Z}$ satisfying (3).[1]

$$(\Gamma_B(\mathcal{Z}_A \cup \mathcal{Z}) \setminus (\mathcal{Z}_A \cup \mathcal{Z})) \cap \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z}) = \emptyset, \qquad (4)$$

$$(\Gamma_A(\mathcal{Z}_B \cup \mathcal{Z}) \setminus (\mathcal{Z}_B \cup \mathcal{Z})) \cap \Gamma_B(\mathcal{Z}_A \cup \mathcal{Z}) = \emptyset. \qquad (5)$$

The proof for the general case is included in the appendix. The proof technique is identical, but uses a more elaborate construction (Figure 10).

The proof proceeds in two steps: First we show the impossibility of OT between $A$ and $B$ in the graph $H_{\mathsf{OT}}$ of Figure 4 with security w.r.t. a certain adversary structure (Lemma 4), then we use this observation to prove the necessity of the second condition in Theorem 2 for the special case through a reduction argument (Lemma 5).

**Lemma 4.** *In $H_{\mathsf{OT}}(\mathcal{V}_{H_{\mathsf{OT}}}, \mathcal{E}_{H_{\mathsf{OT}}})$ (Figure 4), it is impossible to realize OT between $A$ and $B$ with statistical security w.r.t. the malicious adversary structure $\{\{C\}, \{A, D\}, \{B, D\}\}$.*

*Proof.* The proof uses ideas from the proof for impossibility of Byzantine agreement by Fischer *et al.* in [15]. We first consider the case of perfect security for clarity and later argue the case of statistical security. We will show that a protocol for OT between $A$ and $B$ with perfect security w.r.t. the malicious adversary structure $\{\{C\}, \{A, D\}, \{B, D\}\}$ would imply a secure 2-party OT protocol for the semi-honest case. The impossibility will then follow from the impossibility of secure 2-party semi-honest OT. To prove a contradiction, let $\Pi$ be a protocol that realizes OT between $A$ and $B$ with *perfect* security w.r.t. $\{\{C\}, \{A, D\}, \{B, D\}\}$. Similar to the construction used in [15], we construct a

[1] $\Gamma_B(\mathcal{Z}_A \cup \mathcal{Z}) \setminus (\mathcal{Z}_A \cup \mathcal{Z})$ is the set of vertices outside $\mathcal{Z}_A \cup \mathcal{Z}$ that have no paths to $B$ except through vertices in $\mathcal{Z}_A \cup \mathcal{Z}$, similarly for $\Gamma_B(\mathcal{Z}_A \cup \mathcal{Z}) \setminus (\mathcal{Z}_A \cup \mathcal{Z})$.

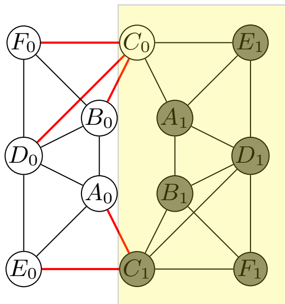


**Fig. 6.** We may visualize the execution of $\Pi'$ as vertices $A_0, B_0, D_0, E_0$, $F_0$ following $\Pi$ honestly and the corrupted set $\{C\}$ simulating all the vertices in the yellow region. Since $\Pi$ is secure against the corruption of $\{C\}$, $A_0$ and $B_0$ must have computed OT correctly.

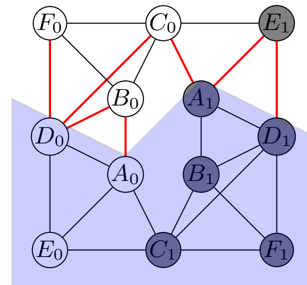


**Fig. 7.** We may also visualize the execution of $\Pi'$ as vertices $B_0, C_0, F_0, E_1$ following $\Pi$ honestly and the corrupted set $\{A, D\}$ simulating all the vertices in the blue region. Since $\Pi$ is secure against the corruption of $\{A, D\}$, view of all vertices in the blue region is independent of $B_0$'s input.

graph $S_{\mathsf{OT}}(\mathcal{V}_{S_{\mathsf{OT}}}, \mathcal{E}_{S_{\mathsf{OT}}})$ by interconnecting two copies of $H_{\mathsf{OT}}$ as shown in Figure 5. Consider the map $\phi : \mathcal{V}_{S_{\mathsf{OT}}} \to \mathcal{V}_{H_{\mathsf{OT}}}$ such that $\phi(v_i) = v, i = 0, 1$, *i.e.,* $\phi(A_0) = \phi(A_1) = A$, $\phi(B_0) = \phi(B_1) = B$ and so on. Then $S_{\mathsf{OT}}$ looks locally like $H_{\mathsf{OT}}$. For example, $A_0$ has edges to $B_0, D_0, E_0$ and $C_1$ in $S_{\mathsf{OT}}$, whereas in $H_{\mathsf{OT}}$, $\phi(A_0)$ has edges to $\phi(B_0), \phi(D_0), \phi(E_0)$, and $\phi(C_1)$. Let each vertex $v$ in $S_{\mathsf{OT}}$ run the instruction for $\phi(v)$ in the protocol $\Pi$. We *fix* the input to $A_1$ as $(0, 0)$ and input to $B_1$ as 0 and let the input to $A_0$ be $(X_0, X_1)$ and that to $B_0$ be $Q$, where $X_0, X_1, Q$ are independent uniformly random bits. We call this the execution of a protocol $\Pi'$ in $S_{\mathsf{OT}}$. Clearly $\Pi'$ is not the same as $\Pi$ ($\Pi$ is defined for 6 parties), but it is easy to see that this execution is well-defined.

*Claim 4.* The output at $B_0$ is $X_Q$.

*Proof.* In Figure 6, it can be verified none of the vertices in the yellow region has any inputs or outputs in the protocol (inputs of $A_1, B_1$ have been fixed) and that all the edges that enter the yellow region (edges in red) are incident on either $C_0$ or $C_1$. Hence, all the vertices in the yellow region may be thought of as being simulated by a malicious $C$. The execution of $\Pi'$ in $S_{\mathsf{OT}}$ can be interpreted as an execution of $\Pi$ among honest vertices $A_0, B_0, D_0, E_0, F_0$, and a corrupted set $\{C\}$ as shown in Figure 6. $\Pi$ is assumed to be secure against the corruption of $C$, therefore $A_0, B_0, D_0, E_0, F_0$ halt and realize OT between $A_0$ and $B_0$; hence $B_0$ outputs $X_Q$. This proves the claim. □

*Claim 5.* Let $\mathcal{A}_{\{A,D\}} := \{A_0, A_1, D_0, D_1, B_1, C_1, F_1, E_0\}$, the vertices in the blue region of Figure 7. Then $Q$ is independent of the view of $\mathcal{A}_{\{A,D\}}$.

*Proof.* In Figure 7, the only vertex in the blue region with input or output to the protocol $\Pi'$ is $A_0$. Also, $A_0, D_0, A_1, D_1$ are the only vertices to which there are edges (red edges in the figure) from the vertices outside the blue region. Hence, the execution of $\Pi'$ in $S_{\mathsf{OT}}$ can also be interpreted as an execution of $\Pi$ by honest $B_0, C_0, E_1, F_0$, and a corrupted set $\{A, D\}$ that simulates $\mathcal{A}_{\{A,D\}}$ (the vertices in the blue region) and communicates with the honest vertices accordingly. Since $\Pi$ is secure against the corruption of $\{A, D\}$, the input $Q$ of $B_0$ is independent of the view of $\{A, D\}$. Hence $Q$ is independent of the view of $\mathcal{A}_{\{A,D\}}$. □

*Claim 6.* Let $\mathcal{A}_{\{B,D\}} := \{B_0, B_1, D_0, D_1, A_1, C_0, E_1, F_0\}$, the vertices in the yellow region of Figure 8. $X_0, X_1$ is independent of the view of $\mathcal{A}_{\{B,D\}}$ conditioned on $Q, X_Q$.

*Proof.* Similar to the previous claims, as shown in Figure 8, the execution of $\Pi'$ in $S_{\mathsf{OT}}$ can also be interpreted as an execution of $\Pi$ by honest parties $A_0, E_0, C_1, F_1$ and a corrupted set $\{B, D\}$ simulates the vertices in the yellow region ($\mathcal{A}_{\{B,D\}}$) and communicates with the honest vertices accordingly. Notice that the view of this set contains the input $Q$ and output $X_Q$ of $B_0$. Since $\Pi$ is secure against the corruption of $\{B, D\}$, the input $(X_0, X_1)$ of $A_0$ is independent of the view of $\{B, D\}$ conditioned on its input and output. Hence $(X_0, X_1)$ is independent of the view of $\mathcal{A}_{\{B,D\}}$ conditioned on $Q, X_Q$. □

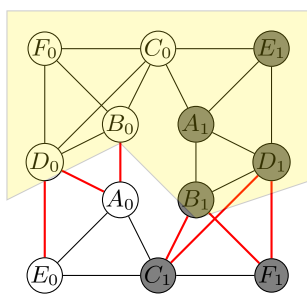


**Fig. 8.** We may visualize the execution of $\Pi'$ as vertices $A_0, C_1, E_0, F_1$ following $\Pi$ honestly and the corrupted set $\{B, D\}$ simulating all the vertices in the yellow region. Since $\Pi$ is secure against the corruption of $\{B, D\}$, the view of vertices in the yellow region must be conditionally independent of $A_0$'s input conditioned on $B_0$'s input and output.

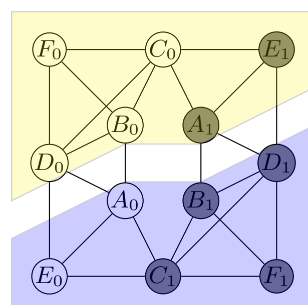


**Fig. 9.** $\mathcal{P}_1$ and $\mathcal{P}_2$ simulate the vertices in the blue and yellow regions respectively and run $\Pi'$ faithfully by setting their inputs as inputs to $A_0$ and $B_0$ respectively to securely realize a 2-party OT, a contradiction.

We show that Claims 4, 5, and 6 lead to a contradiction. To see this, let parties $\mathcal{P}_1$ and $\mathcal{P}_2$ simulate the vertices in the blue region ($\mathcal{A}_{\mathcal{P}_1}$) and yellow region ($\mathcal{A}_{\mathcal{P}_2}$) respectively in Figure 9. Let them execute $\Pi'$ faithfully with $\mathcal{P}_1$ setting the input to the simulated $A_0$ as $X_0, X_1$ and that to the simulated $B_1$ as 0, and $\mathcal{P}_2$ setting the input to the simulated $B_0$ as $Q$ and that to the simulated $A_1$ as $(0, 0)$. Then,

| Set | Definition | |
|---|---|---|
| $\mathcal{Z}$ | $\mathcal{Z}$ | $= \psi^{-1}(C)$ |
| $\mathcal{Z}_{AB}$ | $(\mathcal{Z}_A \cap \mathcal{Z}_B) \setminus \mathcal{Z}$ | $= \psi^{-1}(D)$ |
| $\mathcal{Z}'_A$ | $\mathcal{Z}_A \setminus (\mathcal{Z} \cup (\mathcal{Z}_A \cap \mathcal{Z}_B))$ | $= \psi^{-1}(A)$ |
| $\mathcal{Z}'_B$ | $\mathcal{Z}_B \setminus (\mathcal{Z} \cup (\mathcal{Z}_A \cap \mathcal{Z}_B))$ | $= \psi^{-1}(B)$ |
| $\mathcal{S}_A$ | $\Gamma_A \setminus (\mathcal{Z}_A \cup \mathcal{Z}_B \cup \mathcal{Z})$ | $= \psi^{-1}(E)$ |
| $\mathcal{S}_B$ | $\Gamma_B \setminus (\mathcal{Z}_A \cup \mathcal{Z}_B \cup \mathcal{Z})$ | $= \psi^{-1}(F)$ |

**Table 1.** Partition of $\mathcal{V}$. Here $\Gamma_A := \Gamma_B(\mathcal{Z}_A \cup \mathcal{Z})$ and $\Gamma_B := \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z})$.

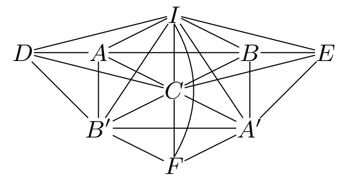


**Fig. 10.** In Appendix F, we show the necessity of the second condition for the general case by showing the impossibility of OT between $A$ and $B$ in this graph with statistical security w.r.t. the malicious adversary structure $\{\{C\}, \{A, A', I\}, \{B, B', I\}\}$.

(i) The output at $B_0$ is $X_Q$.
(ii) $Q$ is independent of the view of $\mathcal{A}_{\mathcal{P}_1}$.
(iii) $X_0, X_1$ is independent of the view of $\mathcal{A}_{\mathcal{P}_2}$ conditioned on $Q, X_Q$.

Here (i) follows from Claim 4. Claim 5 implies (ii) since the vertices $\mathcal{A}_{\mathcal{P}_1}$ (the blue region in Figure 9) is contained in $\mathcal{A}_{\{A,D\}}$ (the blue region in Figure 7) and the only vertex in $\mathcal{A}_{\{A,D\}}$ with input or output is $A_0$. Similarly, Claim 6 implies (iii) because $\mathcal{A}_{\mathcal{P}_2}$ (the blue region in Figure 9) is contained in $\mathcal{A}_{\{B,D\}}$ (the blue region in Figure 8) and the only vertex in $\mathcal{A}_{\{B,D\}}$ with input or output in $\mathcal{A}_{\{B,D\}}$ is $B_0$. But, (i), (ii), and (iii) together imply that parties $\mathcal{P}_1$ and $\mathcal{P}_2$ can securely realize a 2-party OT in the semi-honest setting. Hence a protocol for OT between $A$ and $B$ with perfect security w.r.t. the adversary structure $\{\{C\}, \{A, D\}, \{B, D\}\}$ in the graph $H_{\mathsf{OT}}$ in the malicious setting implies a perfectly secure 2-party OT protocol in the semi-honest setting. By the same line of reasoning, a protocol for statistically secure OT between $A$ and $B$ in the same setting would imply a statistically secure 2-party OT protocol in the semi-honest setting. The lemma now follows from the impossibility of statistically secure semi-honest 2-party OT. □

Lemma 5 below shows that if $\mathcal{Z}_A \in \mathbb{Z}_A, \mathcal{Z}_B \in \mathbb{Z}_B$, and $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$ satisfy conditions (3), (4), and (5), then any protocol for OT between $A$ and $B$ in $G$ with security w.r.t. $\mathbb{Z}$ may be simulated in $H_{\mathsf{OT}}$ to realize OT between $A$ and $B$ with security w.r.t. $\{\{C\}, \{A, D\}, \{B, D\}\}$. The necessity of the second condition in Theorem 2 for the special case when (4) and (5) is satisfied will then follow from Lemma 5.

**Lemma 5.** *Let $\mathcal{Z}_A \in \mathbb{Z}_A, \mathcal{Z}_B \in \mathbb{Z}_B$, and $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$ be such that conditions (3), (4), and (5) are satisfied. If OT between $A$ and $B$ in $G(\mathcal{V}, \mathcal{E})$ can be computed with statistical security w.r.t. the malicious adversary structure $\{\mathcal{Z}_A, \mathcal{Z}_B, \mathcal{Z}\}$ then $A$ and $B$ in $H_{\mathsf{OT}}(\mathcal{V}_{H_{\mathsf{OT}}}, \mathcal{E}_{H_{\mathsf{OT}}})$ (Figure 4) can realize OT with statistical security w.r.t. the malicious adversary structure $\{\{C\}, \{A, D\}, \{B, D\}\}$.*

*Proof.* Consider the subsets of $\mathcal{V}$ defined in Table 1. We show the following:

(i) $\mathcal{Z}'_A, \mathcal{Z}'_B, \mathcal{Z}, \mathcal{Z}_{AB}, \mathcal{S}_A$, and $\mathcal{S}_B$ form a partition of $\mathcal{V}$ and $A \in \mathcal{Z}'_A, B \in \mathcal{Z}'_B$.

(ii) Let the map $\psi : \mathcal{V} \to \mathcal{V}_{H_{\mathsf{OT}}}$ be as given in Figure 4, *i.e.,* for $v \in \mathcal{Z}'_A, \psi(v) = A$ and so on. (i) implies that $\psi$ is well-defined. For $u, v \in \mathcal{V}$, edge $\{u, v\}$ is in $G$ only if $\psi(u) = \psi(v)$ or edge $\{\psi(u), \psi(v)\}$ is present in $H_{\mathsf{OT}}$. In short, $H_{\mathsf{OT}}$ (or a subgraph of $H_{\mathsf{OT}}$) is obtained from $G$ on applying *vertex contraction* to every subset of $\mathcal{V}$ given in Table 1.

(iii) If $\Pi$ realizes OT between $A$ and $B$ in $G$ securely w.r.t. malicious adversary structure $\{\mathcal{Z}, \mathcal{Z}_A, \mathcal{Z}_B\}$, then it is also secure w.r.t. malicious adversary structure $\{\mathcal{Z}, \mathcal{Z}'_A \cup \mathcal{Z}_{AB}, \mathcal{Z}'_B \cup \mathcal{Z}_{AB}\} = \{\psi^{-1}(\{C\}), \psi^{-1}(\{A, D\}), \psi^{-1}(\{B, D\})\}$.

Assuming (i), (ii), and (iii), it is easy to see that the vertices in $H_{\mathsf{OT}}$ can simulate $\Pi$ and realize OT between $A$ and $B$ with statistical security w.r.t. the malicious adversary $\{\{C\}, \{A, D\}, \{B, D\}\}$. It remains to show (i), (ii), and (iii).

*Proof of (i)* – From their definitions, it can be easily verified that $\mathcal{Z}, \mathcal{Z}_{AB}, \mathcal{Z}'_A, \mathcal{Z}'_B$ are disjoint and that their union is $\mathcal{Z} \cup \mathcal{Z}_A \cup \mathcal{Z}_B$. By definition of $\mathcal{S}_A, \mathcal{S}_B$, their union is $\Gamma_B(\mathcal{Z}_A \cup \mathcal{Z}) \cup \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z}) \setminus (\mathcal{Z}_A \cup \mathcal{Z}_B \cup \mathcal{Z})$. By condition (3), this union is equal to $\mathcal{V} \setminus (\mathcal{Z} \cup \mathcal{Z}_A \cup \mathcal{Z}_B)$. Finally, the fact that $\mathcal{S}_A$ and $\mathcal{S}_B$ are disjoint follows from (4) since $\mathcal{S}_A \subseteq \Gamma_B(\mathcal{Z}_A \cup \mathcal{Z}) \setminus (\mathcal{Z}_A \cup \mathcal{Z})$ and $\mathcal{S}_B \subseteq \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z})$.

*Proof of (ii)* – Note that the only edges missing in $H_{\mathsf{OT}}$ are $\{F, A\}, \{F, E\}$ and $\{E, B\}$. We will now show that there is no edge between any vertex in $\psi^{-1}(F) = \mathcal{S}_B$ and any vertex in $\psi^{-1}(A) = \mathcal{Z}'_A$ or $\psi^{-1}(E) = \mathcal{S}_A$. The fact that there is no edge between any vertex in $\psi^{-1}(E) = \mathcal{S}_A$ and any vertex in $\psi^{-1}(B) = \mathcal{Z}'_B$ follows similarly. Suppose there exists $u \in \mathcal{S}_B$ and $v \in \mathcal{Z}'_A \cup \mathcal{S}_A$ such that $\{u, v\}$ is an edge in $G$. Since $\mathcal{Z}_B \cup \mathcal{Z} \subseteq \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z})$, we have

$$\begin{aligned}
\mathcal{Z}_A \cap \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z}) &= (\mathcal{Z}_A \cap (\mathcal{Z}_B \cup \mathcal{Z})) \cup (\mathcal{Z}_A \cap (\Gamma_A(\mathcal{Z}_B \cup \mathcal{Z}) \setminus (\mathcal{Z}_B \cup \mathcal{Z}))) \\
&= (\mathcal{Z}_A \cap (\mathcal{Z}_B \cup \mathcal{Z})) \cup \emptyset \text{ (by (5) since } \mathcal{Z}_A \subset \Gamma_B(\mathcal{Z}_A \cup \mathcal{Z})) \\
&\subseteq \mathcal{Z} \cup (\mathcal{Z}_A \cap \mathcal{Z}_B) \\
\implies \mathcal{Z}'_A &= \mathcal{Z}_A \setminus (\mathcal{Z} \cup (\mathcal{Z}_A \cap \mathcal{Z}_B)) \subseteq \mathcal{V} \setminus \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z}). \\
\mathcal{S}_A &= \Gamma_B(\mathcal{Z}_A \cup \mathcal{Z}) \setminus (\mathcal{Z} \cup \mathcal{Z}_A \cup \mathcal{Z}_B) \subseteq \Gamma_B(\mathcal{Z}_A \cup \mathcal{Z}) \setminus (\mathcal{Z}_A \cup \mathcal{Z}) \\
\implies \mathcal{S}_A &\subseteq \mathcal{V} \setminus \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z}), \text{ by (4).}
\end{aligned}$$

Hence we have $v \in \mathcal{Z}'_A \cup \mathcal{S}_A \subseteq \mathcal{V} \setminus \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z})$ and $u \in \mathcal{S}_B \subseteq \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z}) \setminus (\mathcal{Z}_B \cup \mathcal{Z})$. Since $v \in \mathcal{V} \setminus \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z})$, there is a path from $v$ to $A$ that does not have any vertex from $\mathcal{Z}_B \cup \mathcal{Z}$. Since edge $\{u, v\}$ is present in $G$, $u$ has a path via $v$ to $A$ that does not contain any vertex from $\mathcal{Z}_B \cup \mathcal{Z}$ (note that $u \notin \mathcal{Z}_B \cup \mathcal{Z}$). But $u \in \mathcal{S}_B$ and hence $u \in \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z})$, a contradiction.

*Proof of (iii)* – $A \in \mathcal{Z}'_A$ and $B \in \mathcal{Z}'_B$ are the only vertices with input or output in $\Pi$. Also, $\mathcal{Z}'_A \cup \mathcal{Z}_{AB} \subseteq \mathcal{Z}_A$ and $\mathcal{Z}'_B \cup \mathcal{Z}_{AB} \subseteq \mathcal{Z}_B$. Hence, if $\Pi$ is secure w.r.t. $\{\mathcal{Z}, \mathcal{Z}_A, \mathcal{Z}_B\}$, then it is also secure w.r.t. $\{\mathcal{Z}, \mathcal{Z}'_A \cup \mathcal{Z}_{AB}, \mathcal{Z}'_B \cup \mathcal{Z}_{AB}\}$. □

*General Case:* The necessity of the second condition for the general case is proved in a similar manner. We first show that it is impossible to realize OT between $A$ and $B$ in the graph shown in Figure 10 with statistical security w.r.t. the malicious adversary structure $\{\{C\}, \{A, A', I\}, \{B, B', I\}\}$. This is shown using an argument similar to the one used in Lemma 4 on a graph constructed by interconnecting *three copies* of this graph. Then we use this observation to prove the necessity of the second condition in Theorem 2 for the general case through a reduction argument. This proof is included in Appendix F.

### 3.2 Sufficiency of Conditions

In this section, we consider a graph $G(\mathcal{V}, \mathcal{E})$ with $A, B \in \mathcal{V}$ and a malicious adversary structure $\mathbb{Z}$ that satisfies the conditions in Theorem 2 and construct a protocol $\Pi_{\mathsf{mal}}$ that realizes OT between $A$ and $B$ with statistical security w.r.t. $\mathbb{Z}$. First we comment on two protocols we use extensively in this section: for realizing secure communication and for computing OT from sampled OT.

*Realizing Perfectly Secure Communication:* In the previous section, we saw that the first condition in Theorem 2 is necessary for statistically correct communication. In [28], Kumar *et al.* showed that this condition is sufficient for perfectly secure communication. We will use their protocol for realizing secure communication between $A$ and $B$ in all the protocols that follow. This protocol is guaranteed to be efficient if the size of $\mathbb{Z}$ is polynomial in $n$. We note here that their protocol can be shown to be composable.

*OT computation using sampled OT:* A *sampled OT* or a precomputed OT between $A$ and $B$ is a functionality that generates $r_0, r_1, c$ independently and uniformly at random and sends the ordered pair $(r_0, r_1)$ to $A$ and the ordered pair $(c, r_c)$ to $B$. The following protocol describes a well known technique for realizing OT between $A$ with input $(x_0, x_1)$ and $B$ with input $b$ using this sampled OT. The OT computed by this protocol is statistically secure as long as the sampled OT was computed with statistical security [2].

**Protocol 4** ($\mathsf{SampledOT} \rightarrow \mathsf{OT}\,(A : (x_0, x_1; r_0, r_1), B : (b; c, r_c))$). [2]

1. $B$: Sends $p := b \oplus c$ to $A$ securely.
2. $A$: Sends $(y_0, y_1) := (x_0 \oplus r_p, x_1 \oplus r_{1\oplus p})$ securely.
3. $B$: Stores the messages it received as $(y_0, y_1)$ and outputs $y_b \oplus r_c$.

*Overview of the Section:* The protocol $\Pi_{\mathsf{mal}}$ constructed in this section executes many sub-protocols which in turn execute other sub-protocols. Figure 11 shows the sub-protocols that are used in the construction of each of the protocols described in the section. All the protocols that follow, except $\Pi, \Pi^A$, and $\Pi^B$ have the property that they either compute OT with statistical security or *abort* depending on the malicious behavior of the adversary. A protocol is said to have

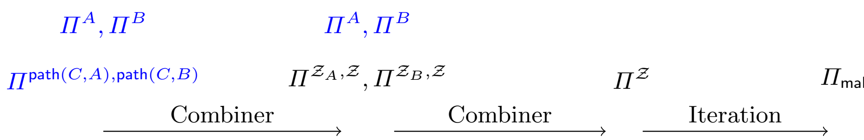


**Fig. 11.** Protocols in each column (except the ones in blue) make calls to the protocols in the previous column.

aborted if both $A$ and $B$ output $\perp$ while guaranteeing *perfect privacy* of the inputs of $A$ and $B$.

First we demonstrate the construction $\Pi_{\mathsf{mal}}$ assuming the following lemma which claims the existence of protocols $\Pi^{\mathcal{Z}}, \mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$ with certain properties. We prove this lemma later in the section by giving an explicit construction for $\Pi^{\mathcal{Z}}, \mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$. The construction and analysis of $\Pi^{\mathcal{Z}}, \mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$ is very similar to that of protocol $\Pi_{\mathsf{sh}}$ described in the semi-honest section.

**Lemma 6.** *Consider a pair of vertices $A, B$ in $G(\mathcal{V}, \mathcal{E})$, and a malicious adversary structure $\mathbb{Z}$ such that the conditions in Theorem 2 hold. For each $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$, there is a protocol $\Pi^{\mathcal{Z}}$ such that*

*(i) $\Pi^{\mathcal{Z}}$ computes OT between $A$ and $B$ with perfect security against the corruption of $\mathcal{Z}$.*
*(ii) $\Pi^{\mathcal{Z}}$ is either aborted or it computes OT between $A$ and $B$ with statistical security w.r.t. $\mathbb{Z} \setminus \{\mathcal{Z}\}$.*

*This protocol is efficient if the size of $\mathbb{Z}$ is polynomial in $n$.*

*Protocol $\Pi_{\mathsf{mal}}$.* This protocol computes OT between $A$ and $B$ with statistical security with guaranteed output delivery. For each $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$, $A$ and $B$ attempts to compute a sampled OT by executing $\Pi^{\mathcal{Z}}$ with independent uniform bits as input. If, for some $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}, \Pi^{\mathcal{Z}}$ succeeds in computing a sampled OT, $A$ and $B$ use this sampled OT to realize the OT. Since the sampled OT is statistically secure by Lemma 6 (ii), the OT computed using it is also statistically secure. By Lemma 6 (i), $\Pi^{\mathcal{Z}}$ aborts for all $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$ only if the corrupted set is not in $\mathbb{Z}_{\neg A \neg B}$, *i.e.,* either $A$ or $B$ is corrupt. In that case, $B$ (if honest) may output a random bit and the computation is still secure. Let $\mathbb{Z}_{\neg A \neg B} = \{\mathcal{Z}_1, \dots, \mathcal{Z}_\ell\}$, we formally describe $\Pi_{\mathsf{mal}}$ as follows:

**Protocol 5** **($\Pi_{\mathsf{mal}}(A : (x_0, x_1), B : (b))$).**

1. For $i = 1, \dots, \ell$:

   (a) $A$ generates bits $r_0^i, r_1^i$ uniformly and independently and $B$ generates a bit $c^i$ uniformly and executes $\Pi^{\mathcal{Z}^i}(A : (r_0^i, r_1^i), B : c^i)$.

[2] $A$ and $B$ treat missing and incorrect messages as 0.

(b) If for some $i \leq \ell, B$ receives $\bar{r}_c^i$ as output (*i.e.,* $\Pi^{\mathcal{Z}^i}$ does not abort) then $A$ and $B$ execute $\mathsf{SampledOT} \to \mathsf{OT}\left(A : (x_0, x_1; r_0^i, r_1^i), B : (b; c^i, \bar{r}_c^i)\right)$, output whatever the protocol outputs and terminate.

2. If for all $i \leq \ell$, $\Pi^{\mathcal{Z}^i}$ aborts, then $B$ outputs a bit uniformly at random.

*Proof (Proof of the sufficiency part of Theorem 2).* We show that $\Pi_{\mathsf{mal}}$ computes OT between $A$ and $B$ with statistical security w.r.t. $\mathbb{Z}$. For every $i = 1, \dots \ell$, the inputs of $A$ and $B$ to $\Pi^{\mathcal{Z}^i}$ are random bits independent of their real inputs. Hence their input remains perfectly private after the execution of $\Pi^{\mathcal{Z}^i}$ irrespective of whether it is aborted or not. We consider two cases.

*Case 1 – For some iteration $i \in \{1, \dots, \ell\}$, $\Pi^{\mathcal{Z}^i}$ does not abort:* By Lemma 6 (ii), the sampled OT computed by $\Pi^{\mathcal{Z}^i}$ is statistically secure, hence the OT computed using this sampled OT is also statistically secure.

*Case 2 – For $i = 1, \dots \ell$, $\Pi^{\mathcal{Z}^i}$ aborts:* By Lemma 6 (i), for any $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$, $\Pi^{\mathcal{Z}}$ realizes OT with perfect security against the corruption of $\mathcal{Z}$. Hence, $\Pi^{\mathcal{Z}^i}$ aborts for all $i$ only if the corrupted set is in $\mathbb{Z} \setminus \mathbb{Z}_{\neg A \neg B}$ *i.e.,* either $A$ or $B$ is corrupted. In this case, an honest $B$ may output a random bit and the protocol remains perfectly secure.

Hence $\Pi_{\mathsf{mal}}$ computes OT between $A$ and $B$ with statistical security w.r.t. $\mathbb{Z}$. The efficiency claim follows from the fact that $\Pi_{\mathsf{mal}}$ runs at most $|\mathbb{Z}_{\neg A \neg B}|$ protocols of the kind $\Pi^{\mathcal{Z}}$, each of which is efficient when $\mathbb{Z}$ is of size $\mathsf{poly}(n)$ according to Lemma 6. □

In the rest of this section, we prove Lemma 6 by explicitly constructing $\Pi^{\mathcal{Z}}, \mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$. As a first step, we construct a protocol $\Pi^{\mathsf{path}(C,A),\mathsf{path}(C,B)}$ that is defined for $C \in \mathcal{V} \setminus \{A, B\}$, and paths $\mathsf{path}(C, A)$ and $\mathsf{path}(C, B)$ from $C$ to $A$ and $B$, respectively.

*Protocol $\Pi^{\mathsf{path}(C,A),\mathsf{path}(C,B)}$ (analogous to $\Pi^C$ in Lemma 1).* In this protocol vertex $C$ facilitates an OT computation between $A$ and $B$ by providing them with a sampled OT similar to protocol $\Pi^C$ described in the semi-honest case. The protocol either computes OT with statistical security or aborts in a precomputation phase unless $A$ and a vertex in $\mathsf{path}(C, B)$ are corrupted simultaneously or $B$ and a vertex in $\mathsf{path}(C, A)$ are corrupted simultaneously.

The protocol has two phases; a precomputation phase and an OT computation phase. In the precomputation phase, vertex $C$ generates a sampled OT and distributes it to $A$ and $B$ by communicating with $A$ and $B$ along $\mathsf{path}(C, A)$ and $\mathsf{path}(C, B)$ respectively. Unlike in the semi-honest case, the correctness of the sampled OT has to be verified, lest $A$ and $B$ compute OT using an incorrect sampled OT. If the verification succeeds, $A$ and $B$ enter the OT computation phase in which they use the sampled OT to compute OT with their real inputs, else the protocol aborts. The verification step accepts an incorrect sampled OT with positive probability, but this probability can be made as small as needed.

**Protocol 6** **($\Pi^{\mathsf{path}(C,A),\mathsf{path}(C,B)}\,(A : (x_0, x_1), B : b)$).**

– **Precomputation Phase**[3]
  1. $C$: Generates uniformly random bits $r_0, r_1, c$, and chooses $a_0, a_1$ independently and uniformly at random from $\mathbb{F}$ of size at least 3. Define $p_0(x) := a_0x + r_0$, and $p_1(x) := a_1x + r_1$. $C$ sends $(p_0, p_1)$ to $A$ along $\mathsf{path}(C, A)$ and $(c, p_c)$ to $B$ along $\mathsf{path}(C, B)$.
  2. $A$: Stores the received polynomials as $\bar{p}_0^A, \bar{p}_1^A$. $B$: Stores the received bit as $\bar{c}$ and polynomial as $\bar{p}_{\bar{c}}^B$
  3. $B$: Generates $\alpha$ uniformly at random from $\mathbb{F} \setminus \{0\}$. $B$ sends $\alpha$ to $C$ along $\mathsf{path}(C, B)$ and sends $\alpha$ to $A$ securely.
  4. $C$: Sends $\alpha$ received from $B$ to $A$ along $\mathsf{path}(C, A)$. If $\alpha$ is non-zero, it sends $(p_0(\alpha), p_1(\alpha))$ to $B$ along $\mathsf{path}(C, B)$ else it sends $\perp$ to $B$.
  5. $A$: If $\alpha$ received from $B$ and $C$ are identical and non-zero, $A$ sends $(p_0^A(\alpha), p_1^A(\alpha))$ to $B$ securely, otherwise it sends $\perp$ to $B$ securely and aborts by outputting $\perp$.
  6. $B$: Stores evaluations received from $A$ as $y_0^A, y_1^A$ and evaluations from $C$ as $y_0^C, y_1^C$. If $y_i^A = y_i^C, i = 0, 1$ and $y_{\bar{c}}^A = \bar{p}_{\bar{c}}^B(\alpha)$:
     – Then: Sends ACCEPT to $A$ securely and stores the sampled OT $(\bar{c}, \bar{p}_{\bar{c}}^B(0))$.
     – Else: Sends REJECT to $A$ securely and aborts by outputting $\perp$.
  7. $A$: If REJECT is received from $B$, then it aborts by outputting $\perp$ else it stores the sampled OT $(\bar{p}_0^A(0), \bar{p}_1^A(0))$.

– **OT computation Phase**:
  Execute $\mathsf{SampledOT} \to \mathsf{OT}\left(A : (x_0, x_1; \bar{p}_0^A(0), \bar{p}_1^A(0), B : (b; \bar{c}, \bar{p}_{\bar{c}}^B(0))\right)$ and return the output.

**Lemma 7.** *Consider a network $G(\mathcal{V}, \mathcal{E})$, vertices $A, B \in \mathcal{V}$ and a malicious adversary structure $\mathbb{Z}$ such that the conditions in Theorem 2 hold. Suppose there exists a vertex $C \in \mathcal{V} \setminus \{A, B\}$, and paths $\mathsf{path}(C, A)$ and $\mathsf{path}(C, B)$ from $C$ to $A$ and $B$ respectively such that, for every set $\mathcal{Z} \in \mathbb{Z}$, at least one of the following conditions is satisfied.*

*(i)* $A, B \notin \mathcal{Z}$,
*(ii)* $A \in \mathcal{Z}$ *but* $\mathsf{path}(C, B) \cap \mathcal{Z} = \emptyset$,
*(iii)* $B \in \mathcal{Z}$ *but* $\mathsf{path}(C, A) \cap \mathcal{Z} = \emptyset$.

*Then, the protocol $\Pi^{\mathsf{path}(C,A),\mathsf{path}(C,B)}$ is either aborted in the precomputation phase while guaranteeing perfect privacy of inputs or computes OT between A and B with statistical security w.r.t. $\mathbb{Z}$ with error probability $\frac{1}{|\mathbb{F}|-1}$. Moreover, this protocol is efficient as long as the size of $\mathbb{Z}$ is polynomial in $n$.*

*Proof.* Refer to Appendix G for the proof. □

The probability of error in this protocol can be brought down to $\left(\frac{1}{|\mathbb{F}|-1}\right)^k$ if $C$ distributes $k$ pairs of independent and uniformly random polynomials with

[3] If $A$ or $B$ receives an invalid message at any stage, it sends an abort message to the other party and aborts by outputting $\perp$.

$r_0, r_1$ as constant terms and the verification steps are carried out independently for each pair of polynomials with a fresh sample of $\alpha$.

We define OT protocols $\Pi^A, \Pi^B$ as follows. In both these protocols, $A$ and $B$ interpret missing or invalid messages as 0.

**Protocol 7** **($\Pi^A(A : (x_0, x_1), B : b)$).**

1. $B$: Sends $b$ to $A$ securely.
2. $A$: Sends $x_b$ to $B$ securely.
3. $B$: Outputs $x_b$.

**Protocol 8** **($\Pi^B(A : (x_0, x_1), B : b)$).**

1. $A$: Sends $(x_0, x_1)$ to $B$ securely.
2. $B$: Outputs $x_b$.

It is easy to see that $\Pi^A$ is perfectly secure as long as $A$ is honest and communication between $A$ and $B$ is secure, similarly $\Pi^B$ is perfectly secure as long as $B$ is honest and communication between $A$ and $B$ is secure. Specifically, if $A, B$ satisfy the conditions in Theorem 2 for an adversary structure $\mathbb{Z}$, then $\Pi^A$ is secure w.r.t. $\mathbb{Z}_B \cup \mathbb{Z}_{\neg A \neg B}$ and $\Pi^B$ is secure w.r.t. $\mathbb{Z}_A \cup \mathbb{Z}_{\neg A \neg B}$. These protocols are also efficient as long as $\mid \mathbb{Z} \mid = \mathsf{poly}(n)$ since the secure communication between $A$ and $B$ can be carried out efficiently.

We construct the protocol $\Pi^{\mathcal{Z}}$ corresponding to each $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$ in two steps along the lines of the construction of OT protocol $\Pi_{\mathsf{sh}}$ in the semi-honest case. In the first step, the protocol will be secure w.r.t. some specific adversary structures. Then we use these protocols to construct a protocol for the general case. In both these protocols, similar to the semi-honest case, we invoke the idea of compiling many protocols that are not individually secure w.r.t. the adversary structure to create a protocol that is secure. For this, we use an OT combiner for malicious setting as described in [23].

**Lemma 8.** *[23, Corollary 7]*

*Given a malicious adversary structure $\mathbb{Z}$ and protocols $\Pi_1, \ldots, \Pi_m$ realizing OT between A and B such that against the corruption of every set $\mathcal{Z} \in \mathbb{Z}$, a majority of protocols $\Pi_1, \ldots, \Pi_m$ are statistically secure, there is a hybrid protocol $\mathsf{Combiner}_{\mathsf{mal}}(\Pi_1, \ldots, \Pi_m)$ that makes calls to $\Pi_1, \ldots, \Pi_m$ and computes OT between A and B with statistical security w.r.t. $\mathbb{Z}$. Moreover, if $m$ is polynomial in $n$ and each $\Pi_i$ is efficient for $i \in [m]$, then the combiner is efficient.*

In the first step, for $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$ and $\mathcal{Z}_A \in \mathbb{Z}_A$ ($\mathcal{Z}_B \in \mathbb{Z}_B$, respectively), we construct a protocol $\Pi^{\mathcal{Z}, \mathcal{Z}_A}$ ($\Pi^{\mathcal{Z}, \mathcal{Z}_B}$, respectively) that runs in two stages. It is either aborted in the first stage or computes OT between $A$ and $B$ with security w.r.t. the adversary structure $\{\mathcal{Z}_A\} \cup \mathbb{Z}_{\neg A \neg B} \cup \mathbb{Z}_B$ ($\{\mathcal{Z}_B\} \cup \mathbb{Z}_{\neg A \neg B} \cup \mathbb{Z}_A$, respectively). The protocol has the additional property that it computes OT with *perfect security* against the corruption of $\mathcal{Z}$.

*Protocol $\Pi^{\mathcal{Z}, \mathcal{Z}_A}$ (analogous to $\Pi^{\mathcal{Z}_A}$ in Lemma 3).* The protocol involves only the vertices in $\mathcal{V} \setminus \mathcal{Z}$, hence it is perfectly secure against the corruption of $\mathcal{Z}$. It is a combiner of a set of protocols of the kind defined in Protocol 6 and copies of $\Pi^A$. It runs in two phases. In the first phase, $A$ and $B$ compute and store sufficient number of sampled OTs for each protocol of the kind $\Pi^{\mathsf{path}(C,A), \mathsf{path}(C,B)}$ used in the combiner by running their precomputation phases. $\Pi^{\mathcal{Z}, \mathcal{Z}_B}$ is aborted if any of the precomputation phases abort. Otherwise, $A$ and $B$ proceed to compute the combiner with each call to $\Pi^{\mathsf{path}(C,A),\mathsf{path}(C,B)}$ being realized by executing the OT computation phase of Protocol 6. Analysis of this protocol is very similar to $\Pi^{\mathcal{Z}_A}$ described in Lemma 3. Since the protocol $\Pi^{\mathcal{Z},\mathcal{Z}_B}$ is similar, with the roles of $A$ and $B$ reversed, we omit its description.

Consider the adversary structure $\{\mathcal{Z}_A\} \cup \mathbb{Z}_{\neg A \neg B} \cup \mathbb{Z}_B$, such that $A \in \mathcal{Z}_A$ and a set $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$. For every $\mathcal{Z}_B \in \mathbb{Z}_B$, there exists a vertex $C_{\mathcal{Z}_B}$ and paths $\mathsf{path}_{\mathcal{Z}_B}(C_{\mathcal{Z}_B}, B)$ and $\mathsf{path}_{\mathcal{Z}_B}(C_{\mathcal{Z}_B}, A)$ such that $\mathsf{path}_{\mathcal{Z}_B}(C_{\mathcal{Z}_B}, A)$ does not have any vertex from set $\mathcal{Z}_B \cup \mathcal{Z}$ and $\mathsf{path}_{\mathcal{Z}_B}(C_{\mathcal{Z}_B}, B)$ does not have any vertex from set $\mathcal{Z}_A \cup \mathcal{Z}$. Otherwise, for each vertex $v \in \mathcal{V}$, we have $v \in \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z})$ or $v \in \Gamma_B(\mathcal{Z}_A \cup \mathcal{Z})$. This would lead to the contradiction that $\Gamma_A(\mathcal{Z}_B \cup \mathcal{Z}) \cup \Gamma_B(\mathcal{Z}_A \cup \mathcal{Z}) = \mathcal{V}$. Note that, since $C_{\mathcal{Z}_B} \notin \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z}) \cup \Gamma_B(\mathcal{Z}_A \cup \mathcal{Z})$, it can not be $A$ or $B$, hence $\Pi^{\mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, A), \mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, B)}$ are well-defined.

Let $\mathbb{Z}_B = \{\mathcal{Z}_B^1, \ldots, \mathcal{Z}_B^{\ell_B}\}$. Consider the protocols $\Pi_1, \ldots, \Pi_{2\ell_B - 1}$, where

$$\Pi_i := \Pi^{\mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, A), \mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, B)}, \text{ for } 1 \le i \le \ell_B,$$
$$\Pi_i := \Pi^A, \text{ for } \ell_B + 1 \le j \le 2\ell_B - 1.$$

Consider the combiner of these $2\ell_B - 1$ protocols for OT between $A$ and $B$. Let $\mathsf{Calls}(\Pi_i)$ represent the number of calls made to the protocol $\Pi_i$ during an execution of the combiner. Then we construct the protocol $\Pi^{\mathcal{Z},\mathcal{Z}_A}$ as follows.

**Protocol 9** **($\Pi^{\mathcal{Z},\mathcal{Z}_A}(A : (x_0, x_1), B : b)$).**

1. For $1 \le i \le \ell_B$, perform $\mathsf{Calls}(\Pi_i)$ number of independent executions of the precomputation phase of $\Pi^{\mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, A), \mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, B)}$.
2. If any of the executions is aborted: abort the protocol otherwise execute the protocol $\mathsf{Combiner}_{\mathsf{mal}}(\Pi_1, \ldots, \Pi_{2\ell_B - 1})$ with $(x_0, x_1)$ and $b$ as input from $A$ and $B$ respectively and output what the combiner outputs.
**Note:** Every call to $\Pi_i, 1 \le i \le \ell_B$ is realized by executing the OT computation phase of $\Pi^{\mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, A), \mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, B)}$ with the sampled OT from step 1. All other protocols in the combiner are copies of $\Pi^A$, which are executed online.

**Lemma 9.** *Consider a pair of vertices $A, B$ in a graph $G(\mathcal{V}, \mathcal{E})$, and a malicious adversary structure $\mathbb{Z} = \{\mathcal{Z}_A\} \cup \mathbb{Z}_{\neg A \neg B} \cup \mathbb{Z}_B$ where $A \in \mathcal{Z}_A$ ($\mathbb{Z} = \mathbb{Z}_A \cup \mathbb{Z}_{\neg A \neg B} \cup \{\mathcal{Z}_B\}$ where $B \in \mathcal{Z}_B$, respectively) such that the conditions in Theorem 2 hold. Let $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$, then the following hold:*

*(i) $\Pi^{\mathcal{Z},\mathcal{Z}_A}$ ($\Pi^{\mathcal{Z},\mathcal{Z}_B}$, respectively) computes OT between $A$ and $B$ with perfect security against the corruption of $\mathcal{Z}$.*
*(ii) $\Pi^{\mathcal{Z},\mathcal{Z}_A}$ ($\Pi^{\mathcal{Z},\mathcal{Z}_B}$, respectively) is either aborted in step 1 or computes OT between $A$ and $B$ with statistical security w.r.t. $\mathbb{Z} \setminus \{\mathcal{Z}\}$.*

*The protocol $\Pi^{\mathcal{Z},\mathcal{Z}_A}$ ($\Pi^{\mathcal{Z},\mathcal{Z}_B}$, respectively) is efficient if the size of $\mathbb{Z}$ is polynomial in $n$.*

*Proof.* Refer to Appendix G for the proof. □

*Protocol $\Pi^{\mathcal{Z}}$ (analogous to $\Pi_{\mathsf{sh}}$ in the proof of Theorem 1).* Now we are ready to prove Lemma 6 which will complete the proof of the sufficiency of Theorem 2. We do this by constructing $\Pi^{\mathcal{Z}}$ for each $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$ using protocols $\Pi^{\mathcal{Z},\mathcal{Z}_A}, \mathcal{Z}_A \in \mathbb{Z}_A$, $\Pi^{\mathcal{Z},\mathcal{Z}_B}, \mathcal{Z}_B \in \mathbb{Z}_B$ and copies of $\Pi^A$ and $\Pi^B$. This protocol realizes OT between $A$ and $B$ with perfect security against corruption of $\mathcal{Z}$ and guarantees statistical security w.r.t. $\mathbb{Z}\backslash\{\mathcal{Z}\}$ whenever it is not aborted. The construction of this protocol and its analysis is similar to the construction of $\Pi_{\mathsf{sh}}$ from $\Pi^{\mathcal{Z}_A}, \mathcal{Z}_A \in \mathbb{Z}_A, \Pi^{\mathcal{Z}_B}, \mathcal{Z}_A \in \mathbb{Z}_B$ and copies of $\Pi^A, \Pi^B$ in the semi-honest case (Proof of Theorem 1). Let $\mathbb{Z}_A = \{\mathcal{Z}_A^1, \ldots, \mathcal{Z}_A^{\ell_A}\}$ and $\mathbb{Z}_B = \{\mathcal{Z}_B^1, \ldots, \mathcal{Z}_B^{\ell_B}\}$. Consider the following set of protocols

$$(\Pi_{1,1}, \Pi_{1,2}), \ldots, (\Pi_{\ell_A,1}, \Pi_{\ell_A,2}),(\Pi_{\ell_A+1,1}, \Pi_{\ell_A+1,2}), \ldots, (\Pi_{\ell_A+\ell_B,1}, \Pi_{\ell_A+\ell_B,2}),$$
$$\text{where } (\Pi_{i,1}, \Pi_{i,2}) := (\Pi^{\mathcal{Z},\mathcal{Z}_A}, \Pi^B), \text{ for } 1 \le i \le \ell_A,$$
$$(\Pi_{\ell_A+i,1}, \Pi_{\ell_A+i,2}) := (\Pi^{\mathcal{Z},\mathcal{Z}_B}, \Pi^A), \text{ for } 1 \le i \le \ell_B.$$

Let $\mathsf{Calls}(\Pi_{i,j})$ represent the maximum number of calls made to the protocol $\Pi_{i,j}$ during any execution of $\mathsf{Combiner}_{\mathsf{mal}}(\Pi_{1,1}, \Pi_{1,2}, \ldots, \Pi_{\ell_A+\ell_B,1}, \Pi_{\ell_A+\ell_B,2})$.

**Protocol 10** **($\Pi^{\mathcal{Z}}(A : (x_0, x_1), B : b)$).**

- **Precomputation Phase**
  1. For $1 \le i \le \ell_A$: Execute $\mathsf{Calls}(\Pi_{i,1})$ instances of $\Pi^{\mathcal{Z},\mathcal{Z}_A}$ with uniformly random independent bits as inputs by $A$ and $B$.
     (a) If any of the executions abort: abort the protocol.
     (b) Else: Store the sampled OT from each execution.
  2. For $1 \le i \le \ell_B$: Execute $\mathsf{Calls}(\Pi_{\ell_A+i,1})$ instances of $\Pi^{\mathcal{Z},\mathcal{Z}_B}$ with uniformly random independent bits as inputs by $A$ and $B$.
     (a) If any of the executions abort: abort the protocol.
     (b) Else: Store the sampled OT from each execution.
- **OT Computation Phase**
  1. Run $\mathsf{Combiner}_{\mathsf{mal}}(\Pi_{1,1}, \Pi_{1,2}, \ldots, \Pi_{\ell_A+\ell_B,1}, \Pi_{\ell_A+\ell_B,2})$ and output what the combiner outputs. Calls to $\Pi_{i,1}, 1 \le i \le \ell_A + \ell_B$ are realized by computing OT using the sampled OT from the corresponding protocol.

*Proof (Proof of Lemma 6).* The protocol involves only vertices in $\mathcal{V}\backslash\mathcal{Z}$, hence it is perfectly secure against the corruption of $\mathcal{Z}$. Consider any set $\mathcal{Z}' \in \mathbb{Z}\backslash\{\mathcal{Z}\}$. If the protocol aborts during the precomputation phase, the inputs of honest vertices are private since the real inputs are not used in this phase. Suppose the protocol is not aborted in the precomputation phase. Using the same argument we used in the proof of security of $\Pi_{\mathsf{sh}}$ in the semi-honest case, one could verify that against the corruption of any $\mathcal{Z}' \in \mathbb{Z} \setminus \{\mathcal{Z}\}$, a majority of the protocols used in the combiner is secure. Hence, the combiner computes OT with statistical security by Lemma 8. Moreover, if the size of $\mathbb{Z}$ is polynomial in $n$, then the protocols that are combined are all efficient by Lemma 9 and properties of $\Pi^A, \Pi^B$. Since, $\Pi^{\mathcal{Z}}$ is a combiner of $2(|\mathbb{Z}_A|+|\mathbb{Z}_B|)$ protocols, Lemma 8 implies that it is efficient in this case. This proves the lemma. □

## 4 Discussion

In this section we address some of the limitations of our results and scope for further improvements.

- In the semi-honest case, Theorem 1 provides a complete characterization of incomplete networks that allow a given pair of parties to compute OT. Furthermore, this result implies the more general result (Corollary 1) regarding the characterization of networks in which a given subset may realize MPC. As we previously observed, this generalizes the result by Hirt and Maurer [24] on feasibility of MPC with respect to a general adversary structure in complete networks.
  However, in the malicious case, our characterization is limited to the notion of statistical security. Our results leave open the possibility that the necessary and sufficient condition for OT with perfect security between a given pair of parties in an incomplete network might be different from the one in Theorem 2. As previously observed, our characterization directly extends to statistically secure computation of 2-party functionalities with output only at one party. However, the problem of 2-party secure computation with output at both parties remains open. Although our current technique using OT combiners is unable to realize secure computation (with fairness), we conjecture that the conditions in Theorem 2 might be sufficient for statistically secure MPC of such functionalities too.
  Corollary 2 only partially solves the problem of the characterization of networks in which a given subset of parties may realize statistically secure MPC. The characterization of networks in which a given subset of parties may realize statistically secure MPC *without abort and with fairness* (guaranteed output delivery) still remains open. The example given in Figure 12 shows that the necessary and sufficient condition for this must be strictly stronger than the condition given in Corollary 2. We also leave open the problem of whether the conditions in Corollary 2 are sufficient for a given subset of parties to realize statistically secure MPC with fairness, but with abort.
- Section 2.3 addresses efficiency for threshold adversarial structures when the threshold is a constant or when $n = 2t + O(1)$. Except for these cases, the communication complexity of our protocols are polynomial in the size of adversary structure. Efficiency of the protocol in the case of large adversary structures is an important aspect which needs further study. Being the first work on this problem, our focus has been mostly on the characterization. We hope that future work will address the efficiency question more thoroughly; we believe this might require a different set of tools.
- Protocols for general adversary structures often have the following property: if they are secure against the corruption of a set of parties, then they would be secure against the corruption of a subset of these parties. This is not true, in general, for the protocols we construct, neither in the semi-honest nor in the malicious setting. Consider a graph $G(\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{A, B, 1\}$ and $\mathcal{E} = \{\{A, 1\}, \{1, B\}\}$. It can be verified that semi-honest OT is feasible between $A$ and $B$ with security against corruption of vertices $\{A, 1\}$. However,

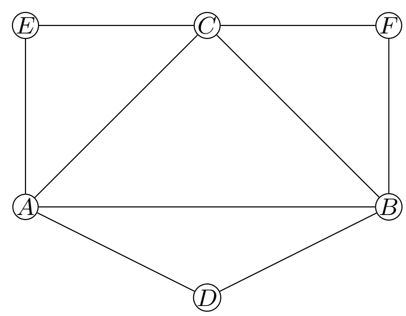


**Fig. 12.** Consider the problem of MPC among the parties $\{A, B, C\}$ with statistical security w.r.t. the malicious adversary structure $\mathbb{Z} = \{\{A\}, \{B\}, \{C\}\}$. Every pair of parties in $\{A, B, C\}$ satisfies the conditions in Theorem 2, hence the condition given in Corollary 2 is satisfied. However, an argument almost identical to the one presented by Fischer *et al.* in [15] can be used to show the impossibility of Byzantine agreement among $\{A, B, C\}$ in this network. This shows that the conditions given in Corollary 2 are not sufficient for a given subset of parties in an incomplete network to do MPC with statistical security w.r.t. a given adversary structure, with guaranteed output delivery.

OT between $A$ and $B$ is impossible with security against the corruption of vertex 1, as SMT between $A$ and $B$ with security against such a corruption itself is impossible. As a consequence, unlike most protocols constructed for general adversary structures, our protocols are not efficient in the number of maximal sets in the adversary structure. However, a more limited form of monotonicity does hold for our protocols. It is easy to see from the conditions in both Theorems 2 and 1 that if a set $\mathcal{Z}_A \subset \mathcal{V}$ such that $A \in \mathcal{Z}_A$ is present in the adversary structure, then we may as well throw in sets of the kind $\mathcal{Z}'_A \subset \mathcal{Z}_A$ such that $A \in \mathcal{Z}'_A$ and this larger adversary structure will satisfy the conditions stated in both these Theorems if and only if the adversary structure we started out with satisfied these conditions. Similarly, if $B \in C_B \subset \mathcal{V}$ is present in the adversary structure, we may as well throw in sets of the kind $\mathcal{Z}'_B \subset C_B$ such that $B \in \mathcal{Z}'_B$. Also, if $\mathcal{Z}$ such that $A, B \notin \mathcal{Z}$ is present in the adversary structure, then throwing in every subset of $\mathcal{Z}$ will not make any difference. Indeed, with some modifications, our protocols can be made efficient w.r.t. the size of 'maximal' adversary structure in the above sense.

Another consequence of this lack of monotonicity is that our protocols do not, in general, continue to be secure when the adversary is adaptive rather than static (see [10, Chapter 4.5]). To see this, we again consider the graph $G(\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{A, B, 1\}$ and $\mathcal{E} = \{\{A, 1\}, \{1, B\}\}$ along with the adversary structure $\{\{A, 1\}\}$. Semi-honest OT between $A$ and $B$ is feasible w.r.t this adversary structure when the adversary is static. However, there exists no protocol that is secure against an adaptive adversary who corrupts 1 at the beginning of the protocol and waits for B to output before corrupting $A$.

## 5 Acknowledgments

We acknowledge useful discussions with Manoj Prabhakaran, IIT Bombay.

## References

[1] S. Agarwal, R. Cramer, and R. de Haan. "Asymptotically Optimal Two-round Perfectly Secure Message Transmission". In: *CRYPTO*. 2006, pp. 394–408.
[2] D. Beaver. "Precomputing Oblivious Transfer". In: *CRYPTO*. 1995, pp. 97–109.
[3] A. Beimel. "On private computation in incomplete networks". In: *J. Distributed Computing* 19.3 (2007), pp. 237–252.
[4] M. Ben-Or, S. Goldwasser, and A. Wigderson. "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation". In: *STOC*. 1988, pp. 1–10.
[5] M. Bläser et al. "Privacy in Non-private Environments". In: *J. Theory Comput. Syst.* 48.1 (2011), pp. 211–245.
[6] M. Bläser et al. "Private Computation: k-Connected versus 1-Connected Networks". In: *J. Cryptology* 19.3 (2006), pp. 341–357.
[7] N. Chandran, J. Garay, and R. Ostrovsky. "Edge Fault Tolerance on Sparse Networks". In: *ICALP*. 2012, pp. 452–463.
[8] N. Chandran, J. Garay, and R. Ostrovsky. "Improved Fault Tolerance and Secure Computation on Sparse Networks". In: *ICALP*. 2010, pp. 249–260.
[9] D. Chaum, C. Crépeau, and I. Damgård. "Multiparty Unconditionally Secure Protocols". In: *STOC*. 1988, pp. 11–19.
[10] R. Cramer, I. Damgård, and J. Nielsen. *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press, 2015.
[11] C. Crépeau, J. van de Graaf, and A. Tapp. "Committed Oblivious Transfer and Private Multi-Party Computation". In: *CRYPTO*. 1995, pp. 110–123.
[12] D. Dolev. "The Byzantine Generals Strike Again". In: *J. Algorithms* 3.1 (1982), pp. 14–30.
[13] D. Dolev et al. "Perfectly Secure Message Transmission". In: *J. ACM* 40.1 (1993), pp. 17–47.
[14] C. Dwork et al. "Fault Tolerance in Networks of Bounded Degree". In: *SIAM J. Comput.* 17.5 (1988), pp. 975–988.
[15] M. J. Fischer, N. A. Lynch, and M. Merritt. "Easy Impossibility Proofs for Distributed Consensus Problems". In: *J. Distributed Computing* 1.1 (1986), pp. 26–39.
[16] M. K. Franklin and M. Yung. "Secure Hypergraphs: Privacy from Partial Broadcast". In: *SIAM J. Discrete Math.* 18.3 (2004), pp. 437–450.
[17] J. Garay and R. Ostrovsky. "Almost-everywhere Secure Computation". In: *EUROCRYPT*. 2008, pp. 307–323.

[18] O. Goldreich, S. Micali, and A. Wigderson. "How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority". In: *STOC*. 1987, pp. 218–229.

[19] O. Goldreich and R. Vainish. "How to Solve any Protocol Problem - An Efficiency Improvement". In: *CRYPTO*. 1987, pp. 73–86.

[20] S. Goldwasser and Y. Lindell. "Secure Computation without Agreement". In: *Distributed Computing*. 2002, pp. 17–32.

[21] S. Halevi et al. "Secure Multiparty Computation with General Interaction Patterns". In: *ITCS*. 2016, pp. 157–168.

[22] D. Harnik, Y. Ishai, and E. Kushilevitz. "How Many Oblivious Transfers Are Needed for Secure Multiparty Computation?" In: *CRYPTO*. 2007, pp. 284–302.

[23] D. Harnik et al. "OT-Combiners via Secure Computation". In: *TCC*. 2008, pp. 393–411.

[24] M. Hirt and U. M. Maurer. "Complete Characterization of Adversaries Tolerable in Secure Multi-Party Computation (Extended Abstract)". In: *PODC*. 1997, pp. 25–34.

[25] Y. Ishai, M. Prabhakaran, and A. Sahai. "Founding Cryptography on Oblivious Transfer - Efficiently". In: *CRYPTO*. 2008, pp. 572–591.

[26] A. Jakoby, M. Liśkiewicz, and R. Reischuk. "Private Computations in Networks: Topology versus Randomness". In: *STACS*. 2003, pp. 121–132.

[27] J. Kilian. "Founding Cryptography on Oblivious Transfer". In: *STOC*. 1988, pp. 20–31.

[28] M. V. N. A. Kumar et al. "On perfectly secure communication over arbitrary networks". In: *PODC*. 2002, pp. 193–202.

[29] R. Kumaresan, S. Raghuraman, and A. Sealfon. "Network Oblivious Transfer". In: *CRYPTO*. 2016, pp. 366–396.

[30] K. Kurosawa and K. Suzuki. "Truly Efficient 2-round Perfectly Secure Message Transmission Scheme". In: *IEEE Trans. Inf. Theor.* 55.11 (2009), pp. 5223–5232.

[31] L. Lamport, R. Shostak, and M. Pease. "The Byzantine Generals Problem". In: *ACM Trans. Program. Lang. Syst.* (1982), pp. 382–401.

[32] R. Meier, B. Przydatek, and J. Wullschleger. "Robuster Combiners for Oblivious Transfer". In: *TCC*. 2007, pp. 404–418.

[33] T. Rabin and M. Ben-Or. "Verifiable Secret Sharing and Multiparty Protocols with Honest Majority". In: *STOC*. 1989, pp. 73–85.

[34] H. Md. Sayeed and H. Abu-Amara. "Efficient Perfectly Secure Message Transmission in Synchronous Networks". In: *J. Inf. Comput.* 126.1 (1996), pp. 53–61.

[35] G. Spini and G. Zémor. "Perfectly Secure Message Transmission in Two Rounds". In: *TCC*. 2016, pp. 286–304.

[36] K. Srinathan, A. Narayanan, and C. P. Rangan. "Optimal Perfectly Secure Message Transmission". In: *CRYPTO*. 2004, pp. 545–561.

[37] E. Upfal. "Tolerating Linear Number of Faults in Networks of Bounded Degree". In: *PODC*. 1992, pp. 83–89.

[38] J. Wullschleger. “Oblivious-Transfer Amplification”. In: *EUROCRYPT*. 2007, pp. 555–572.

## A Proof of Corollary 1

Clearly, if the conditions in Theorem 1 are not satisfied by a pair of vertices $A, B \in \mathcal{K}$, then from Theorem 1 it follows that OT is not possible between these two parties with security w.r.t. the semi-honest adversary structure $\mathbb{Z}$, hence the condition is necessary. From [19, 18], it follows that if every pair of parties in $\mathcal{K}$ can realize OT with security w.r.t. $\mathbb{Z}$, then $\mathcal{K}$ can compute any functionality securely w.r.t. $\mathbb{Z}$. This proves the corollary. $\square$

## B Proof of Corollary 2

Theorem 2 gives a necessary and sufficient condition for a pair of parties to realize OT with statistical security. Hence, if a pair of parties $A, B \in \mathcal{K}$ do not satisfy the conditions given in Theorem 2 then $A$ and $B$ cannot realize OT with statistical security w.r.t. the malicious adversary $\mathbb{Z}$. This proves the first statement. In [11], Crépeau *et al.* showed that, provided that a set of parties have pairwise OT channels and a broadcast channel, any functionality can be computed with statistical security with abort as long as at least one of the parties is honest. In [20], Goldwasser and Lindell proposed a compiler that takes such a protocol in the broadcast model and constructs a protocol that does not use a broadcast channel and provides the same security guarantees, but with abort and without fairness. This result is also implied by [25]. If every pair of parties in $\mathcal{K}$ satisfy conditions in Theorem 2, then OT can be realized by all pairs of parties in $\mathcal{K}$ with statistical security w.r.t. $\mathbb{Z}$. Hence, the second statement follows from [11, 20, 25]. $\square$

## C Proof of Lemma 1

Before we describe the protocol $\Pi^C$, we note that there exists an *efficient protocol* $\mathsf{Send}$ for communication between vertices such that if for every $\mathcal{Z} \in \mathbb{Z}$, if there is at least one path from $S$ to $R$ that does not contain any vertex in $\mathcal{Z}$, then communication using between $S$ and $R$ using $\mathsf{Send}^{S \to R}$ is secure w.r.t. $\mathbb{Z}$. While we believe that an efficient protocol for this must be available in the literature, we were unable to find one. Hence, we provide it in Appendix H for completeness.

Let $(x_0, x_1)$ be the inputs of $A$ and $b$ be the input of $B$, we construct the protocol $\Pi^C$ as follows,

**Protocol 11** **($\Pi^C(A : (x_0, x_1); B : b)$).**

1. $C$: Generates uniform, independent bits $r_0, r_1, c$ and sends $(r_0, r_1)$ to $A$ using $\mathsf{Send}^{C\to A}$ and sends $(c, r_c)$ to $B$ using $\mathsf{Send}^{\mathsf{C}\to\mathsf{B}}$.
2. $B$: Sends $p := c \oplus b$ to $A$ using $\mathsf{Send}^{\mathsf{B}\to\mathsf{A}}$.
3. $A$: Sends $(y_0, y_1) := (x_0 \oplus r_{0\oplus p}, x_1 \oplus r_{1\oplus p})$ to $B$ using $\mathsf{Send}^{A\to B}$.
4. $B$: Outputs $y_b \oplus r_c$.

$\Pi^A$ ($\Pi^B$, respectively) can also be defined in this manner with $A$ ($B$, respectively), taking the role of $C$ in this protocol.

The protocol computes OT using a well known technique due to Beaver [2] that converts a precomputed OT to OT. It is secure against any corruption $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$ (even if the precomputed OT is not private) as the communication between $A$ and $B$ is perfectly secure. Against any $\mathcal{Z}_A \in \mathbb{Z}_A$ ($\mathcal{Z}_B \in \mathbb{Z}_B$, respectively), since $C$ is not corrupt and the communication between $C$ and $B$ ($A$, respectively) is secure, the precomputed OT is secure. This ensures that the OT computed using the this precomputed OT is also secure. The protocol is efficient as it uses only a constant rounds of efficient communication steps. □

In the cases of $\Pi^A$ and $\Pi^B$, Protocol 11 can be simplified as follows:

**Protocol 12** **($\Pi^A(A : (x_0, x_1) B : b)$).**

1. $B$: Sends $b$ to $A$ using $\mathsf{Send}^{B\to A}$.
2. $A$: Sends $x_b$ to $B$ using $\mathsf{Send}^{A\to B}$.
3. $B$: Outputs $x_b$.

**Protocol 13** **($\Pi^B(A : (x_0, x_1) B : b)$).**

1. $A$: Sends $(x_0, x_1)$ to $B$ using $\mathsf{Send}^{A\to B}$.
2. $B$: Outputs $x_b$.

## D Proof of Theorem 3

As in Section 2.2, we first consider certain specific adversary structures and construct efficient protocols for these. We will then use these protocols to construct protocols for the general case. For a set $\mathcal{S} \subseteq \mathcal{V}$, let

$$\mathbb{Z}^t_A(\mathcal{S}) := \{\mathcal{Z}_A \in \mathbb{Z}^t_A \mid \Gamma_B(\mathcal{Z}_A) \setminus \mathcal{Z}_A = \mathcal{S}\}, \text{ where } \mathbb{Z}^t_A := \{\mathcal{Z}_A \in \mathbb{Z}^t \mid A \in \mathcal{Z}_A\},$$
$$\mathbb{Z}^t_B(\mathcal{S}) := \{\mathcal{Z}_B \in \mathbb{Z}^t_B \mid \Gamma_A(\mathcal{Z}_B) \setminus \mathcal{Z}_B = \mathcal{S}\}, \text{ where } \mathbb{Z}^t_B := \{\mathcal{Z}_B \in \mathbb{Z}^t \mid B \in \mathcal{Z}_B\}.$$

To interpret this, $\mathbb{Z}^t_A(\mathcal{S})$ are sets containing $A$ and of size at most $t$ (i.e., they can be corrupted) such that the set of additional vertices they block off from reaching $B$ is precisely $\mathcal{S}$. Loosely, $\mathcal{S}$ is the "shadow" of sets in $\mathbb{Z}^t_A(\mathcal{S})$. Now we define the collections of such "shadow" sets.

$$\mathbb{S}^t_A := \{\mathcal{S} \subseteq \mathcal{V} \mid \mathbb{Z}^t_A(\mathcal{S}) \neq \emptyset\}, \qquad \text{and} \qquad \mathbb{S}^t_B := \{\mathcal{S} \subseteq \mathcal{V} \mid \mathbb{Z}^t_B(\mathcal{S}) \neq \emptyset\}.$$

It is clear that $\mathbb{Z}^t_A = \cup_{\mathcal{S}_A \in \mathbb{S}^t_A} \mathbb{Z}^t_A(\mathcal{S}_A)$ and $\mathbb{Z}^t_B = \cup_{\mathcal{S}_B \in \mathbb{S}^t_B} \mathbb{Z}^t_B(\mathcal{S}_B)$.

*Claim 7.* Let $k = n - 2t$. $|\mathcal{S}_A| < k$ for all $\mathcal{S}_A \in \mathbb{S}^t_A$, and $|\mathcal{S}_B| < k$ for all $\mathcal{S}_B \in \mathbb{S}^t_B$. Sizes of $\mathbb{S}^t_A$ and $\mathbb{S}^t_B$ are $O(n^k)$.

*Proof.* Let $\mathcal{S}_A \in \mathbb{S}^t_A$. Then, there exists $\mathcal{Z}_A \in \mathbb{Z}^t_A$ such that $\Gamma_B(\mathcal{Z}_A) \setminus \mathcal{Z}_A = \mathcal{S}_A$, so clearly $B \notin \mathcal{S}_A$. Suppose $|\mathcal{S}_A| \geq k$.

If $|\mathcal{V} \setminus (\mathcal{S}_A \cup \{B\})| < t$, the size of $\mathcal{V} \setminus \mathcal{S}_A$ is at most $t$. Since $\mathcal{S}_A \subseteq \Gamma_B(\mathcal{Z}_A)$, $\mathcal{V} \setminus \Gamma_B(\mathcal{Z}_A)$ is of size at most $t$ with $B$ as an element. Hence, $\mathcal{V} \setminus \Gamma_B(\mathcal{Z}_A) \in \mathbb{Z}^t_B$;

call this set $\mathcal{Z}_B$. Then $\Gamma_B(\mathcal{Z}_A) \cup \Gamma_A(\mathcal{Z}_B) = \mathcal{V}$ which violates the second condition in Theorem 1.

Therefore, $|\mathcal{V} \setminus (\mathcal{S}_A \cup \{B\})| \geq t$. This implies that there is $\mathcal{Z}'_A \subseteq \mathcal{V} \setminus \mathcal{S}_A \cup \{B\}$ of size $t$ such that $\mathcal{Z}_A \subsetneq \mathcal{Z}'_A$. Since, $\Gamma_B(\mathcal{Z}'_A) \supseteq \mathcal{S}_A \cup \mathcal{Z}'_A$, size of $\Gamma_B(\mathcal{Z}'_A)$ is at least $t + k$. But then, $|\mathcal{V} \setminus \Gamma_B(\mathcal{Z}'_A)| \leq n - (t + k) = t$ and $B$ is a member of this set. Hence $\mathcal{V} \setminus \Gamma_B(\mathcal{Z}'_A) \in \mathbb{Z}^t_B$; call this set $\mathcal{Z}_B$. Then $\Gamma_A(\mathcal{Z}_B) \cup \Gamma_B(\mathcal{Z}'_A) = \mathcal{V}$, a contradiction. Thus, $|\mathcal{S}_A| < k$ for all $\mathcal{S}_A \in \mathbb{S}^t_A$. Further, this implies that $|\mathbb{S}^t_A|$ is $O(n^k)$. The proof for sizes of $\mathcal{S}_B \in \mathbb{S}^t_B$ and $\mathbb{S}^t_B$ is similar. □

We next construct efficient protocols for OT between $A$ and $B$ that are secure w.r.t. adversary structures of the kind $\mathbb{Z}^t_A(\mathcal{S}_A) \cup \mathbb{Z}^t_B \cup \mathbb{Z}^t_{\neg A \neg B}$, where $\mathcal{S}_A \in \mathbb{S}^t_A$, and adversary structures of the kind $\mathbb{Z}^t_A \cup \mathbb{Z}^t_B(\mathcal{S}_B) \cup \mathbb{Z}^t_{\neg A \neg B}$, where $\mathcal{S}_B \in \mathbb{S}^t_B$. Then, we use a combiner of these protocols to construct an efficient protocol $\Pi'_{\mathsf{sh}}$ that is secure w.r.t. $\mathbb{Z}^t$. The efficiency of $\Pi'_{\mathsf{sh}}$ will follow from Claim 7 which shows that the sizes of the adversary structures $\mathbb{S}_A$ and $\mathbb{S}_B$ are of the order $n^k$.

**Lemma 10.** *For every $\mathcal{S}_A \in \mathbb{S}^t_A$ ($\mathcal{S}_B \in \mathbb{S}^t_B$, respectively) there is an efficient protocol $\Pi^{\mathcal{S}_A}$ ($\Pi^{\mathcal{S}_B}$, respectively) that realizes OT between A and B with security w.r.t. a semi-honest adversary structure $\mathbb{Z} = \mathbb{Z}^t_A(\mathcal{S}_A) \cup \mathbb{Z}_B \cup \mathbb{Z}_{\neg A \neg B}$, ($\mathbb{Z} = \mathbb{Z}^t_B(\mathcal{S}_B) \cup \mathbb{Z}_A \cup \mathbb{Z}_{\neg A \neg B}$, respectively) if the conditions in Theorem 3 are satisfied.*

*Proof.* For $\mathcal{S}_A \in \mathbb{S}^t_A$, we define $\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A) := \cap_{\mathcal{Z}_A \in \mathbb{Z}^t(\mathcal{S}_A)} \mathcal{Z}_A$. Similarly, $\mathcal{Z}^B_{\mathsf{min}}(\mathcal{S}_B) := \cap_{\mathcal{Z}_B \in \mathbb{Z}^t(\mathcal{S}_B)} \mathcal{Z}_B$, $\mathcal{S}_B \in \mathbb{S}^t_B$. The following claim shows that $\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A)$ ($\mathcal{Z}^B_{\mathsf{min}}(\mathcal{S}_B)$, respectively) is the smallest set in $\mathbb{Z}^t(\mathcal{S}_A)$ ($\mathbb{Z}^t(\mathcal{S}_B)$, respectively).

*Claim 8.* (i) For each $\mathcal{S}_A \in \mathbb{S}^t_A$, $\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A)$ is a member of $\mathbb{Z}^t_A(\mathcal{S}_A)$. (ii) For each $\mathcal{S}_B \in \mathbb{S}^t_B$, $\mathcal{Z}^B_{\mathsf{min}}(\mathcal{S}_B)$ is a member of $\mathbb{Z}^t_B(\mathcal{S}_B)$.

*Proof.* We prove (i) below, the proof of (ii) is similar. $\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A)$ is a member of $\mathbb{Z}^t_A$ since $A$ is a member and, being an intersection of sets of size at most $t$, it has size at most $t$. Let $\mathcal{S}'_A := \Gamma_B(\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A)) \setminus \mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A)$. To prove (i), it is enough to show that $\mathcal{S}_A = \mathcal{S}'_A$.
$\mathcal{S}'_A \subseteq \mathcal{S}_A$: $\forall \mathcal{Z}_A \in \mathbb{Z}^t(\mathcal{S}_A)$, $\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A) \subseteq \mathcal{Z}_A$, hence $\Gamma_B(\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A)) \subseteq \Gamma_B(\mathcal{Z}_A)$.

$$\begin{aligned}
\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A) \cup \mathcal{S}'_A = \Gamma_B(\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A)) &\subseteq \cap_{\mathcal{Z}_A \in \mathbb{Z}^t(\mathcal{S}_A)} (\mathcal{Z}_A \cup (\Gamma_B(\mathcal{Z}_A) \setminus \mathcal{Z}_A)) \\
&\subseteq \mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A) \cup \mathcal{S}_A \\
\implies \mathcal{S}'_A \subseteq \mathcal{S}_A &\text{ since } \mathcal{S}'_A \text{ and } \mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A) \text{ are disjoint.}
\end{aligned}$$

$\mathcal{S}_A \subseteq \mathcal{S}'_A$: Consider the set of neighbors of $\mathcal{S}_A$ defined as $\mathcal{N}(\mathcal{S}_A) := \{v \in \mathcal{V} \setminus \mathcal{S}_A \mid \exists u \in \mathcal{S}_A \text{ and } \{u, v\} \in \mathcal{E}\}$. Suppose $\mathcal{N}(\mathcal{S}_A)$ is a subset of $\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A)$, then clearly $\mathcal{S}_A \subseteq \Gamma_B(\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A))$ and since $\mathcal{S}_A \cap \mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A) = \emptyset$, $\mathcal{S}_A \subseteq \mathcal{S}'_A$. Now, suppose $\exists v \in \mathcal{N}(\mathcal{S}_A)$ such that $v \notin \mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A)$, then there exists $\mathcal{Z}_A \in \mathbb{S}^t_A$ such that $v \notin \mathcal{Z}_A$. Consider the set $\Gamma_B(\mathcal{Z}_A) \setminus \mathcal{Z}_A$. If $v \in \Gamma_B(\mathcal{Z}_A) \setminus \mathcal{Z}_A$, then $\Gamma_B(\mathcal{Z}_A) \setminus \mathcal{Z}_A \neq \mathcal{S}_A$, therefore $v$ must be in $\mathcal{V} \setminus \Gamma_B(\mathcal{Z}_A)$. This implies that there is a path from $v$ to $B$ without any vertex from $\mathcal{Z}_A$. Since $v \in \mathcal{N}(\mathcal{S}_A)$, there is a vertex $u$ in $\mathcal{S}_A$ such that $\{u, v\} \in \mathcal{E}$. But then there is a path from $u$ to $B$ via $v$ that has no vertex from $\mathcal{Z}_A$. Hence, $u \notin \Gamma_B(\mathcal{Z}_A)$, a contradiction. □

By Claim 8, for a set $\mathcal{S}_A \in \mathbb{S}_A^t$, $\Gamma_B(\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A)) = (\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A) \cup \mathcal{S}_A)$. Hence $\mathcal{V} \setminus \Gamma_B(\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A))$ is of size $n-(r+s)$ when $\mid \mathcal{S}_A \mid = s$ and $\mid (\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A) \mid = r$ ($\leq t$ as $\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A) \in \mathbb{Z}_A^t(\mathcal{S}_A)$). Let $\mathcal{V} \setminus \Gamma_B(\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A))$ be represented by $\{v_1, \dots, v_{n-(r+s)}\}$. Consider the protocols[4]

$$\Pi_1, \dots, \Pi_{n-(r+s)}, \Pi_{n-(r+s)+1}, \dots, \Pi_{2[n-(t+s)]-1},$$

where $\Pi_i := \Pi^{v_i}$ for $1 \leq i \leq n-(r+s)$ and $\Pi_i := \Pi^A$ for $n-(r+s)+1 \leq i \leq 2[n-(t+s)]-1$. Let $\Pi^{\mathcal{S}_A}$ be a combiner of these $2[n-(t+s)]-1$ OT protocols.

$$\Pi^{\mathcal{S}_A} := \mathsf{Combiner}(\Pi_1, \dots, \Pi_{2[n-(t+s)]-1}).$$

For a set $\mathcal{S}_B \in \mathbb{S}_B$, we similarly define $\Pi^{\mathcal{S}_B}$ (with $\mathcal{V} \setminus \Gamma_A(\mathcal{Z}^B_{\mathsf{min}}(\mathcal{S}_B))$ and $B$ playing the roles of the corresponding entities above).

*Claim 9.* For all $\mathcal{S}_A \in \mathbb{S}_A^t$: (i) $\Pi^{\mathcal{S}_A}$ is secure w.r.t. $\mathbb{Z}_A^t(\mathcal{S}_A)$, (ii) $\Pi^{\mathcal{S}_A}$ is secure w.r.t. $\mathbb{Z}^t_{\neg A \neg B}$, (iii) $\Pi^{\mathcal{S}_A}$ is secure w.r.t. $\mathbb{Z}_B^t$.

*Proof.* Consider $\mathcal{Z}_A \in \mathbb{Z}_A^t(\mathcal{S}_A)$.

*Proof of (i)*: By Claim 8, $\mathcal{V} \setminus \Gamma_B(\mathcal{Z}_A)$ is contained in $\mathcal{V} \setminus \Gamma_B(\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A))$. So $\Pi^v$ for each vertex $v \in \mathcal{V} \setminus \Gamma_B(\mathcal{Z}_A)$ is used in the combiner. By Lemma 1, each of these protocols is private against $\mathcal{Z}_A$. Since the size of $\Gamma_B(\mathcal{Z}_A)$ ($= \mathcal{Z}_A \cup \mathcal{S}_A$) is at most $t+s$ where $s$ is the size of $\mathcal{S}_A$, the size of $\mathcal{V} \setminus \Gamma_B(\mathcal{Z}_A)$ is at least $n-(t+s)$. Hence, at least $n-(t+s)$ out of $2[n-(t+s)]-1$ protocols in the combiner are secure against the corruption of $\mathcal{Z}_A$. It follows from Lemma 2 that $\Pi^{\mathcal{S}_A}$ is secure against the corruption of $\mathcal{Z}_A$.

*Proof of (ii)*: This is true because all the protocols used in the combiner are secure w.r.t. $\mathbb{Z}^t_{\neg A \neg B}$.

*Proof of (iii)*: For any $\mathcal{Z}_B \in \mathbb{Z}_B^t$, we prove that at most $n-(t+s)-1$ vertices from the set $\mathcal{V} \setminus \Gamma_B(\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A))$ are present in the set $\Gamma_A(\mathcal{Z}_B)$. Then at least $n-(t+s)$ protocols in the combiner are of the kind $\Pi^v$ such that $v \in \mathcal{V} \setminus \Gamma_A(\mathcal{Z}_B)$ which are secure against the corruption of $\mathcal{Z}_B$. This will guarantee that $\Pi^{\mathcal{S}_A}$ is secure against the corruption of $\mathcal{Z}_B$.

To prove a contradiction, suppose that there exists $\mathcal{Z}_B \in \mathbb{Z}_B$ such $\{\mathcal{V} \setminus \Gamma_B(\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A))\} \cap \Gamma_A(\mathcal{Z}_B)$ is of size at least $n-(t+s)$. For ease of notation we define $\mathcal{I}(\mathcal{Z}_B) := \{\mathcal{V} \setminus \Gamma_B(\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A))\} \cap \Gamma_A(\mathcal{Z}_B)$. Then size of $\mathcal{V} \setminus \mathcal{I}(\mathcal{Z}_B)$ is at most $t+s$. Since $\mathcal{S}_A \subseteq \mathcal{V} \setminus \mathcal{I}(\mathcal{Z}_B)$, $\mathcal{V} \setminus (\mathcal{I}(\mathcal{Z}_B) \cup \mathcal{S}_A)$ is of size at most $t$. Let $\mathcal{Z}_A = \mathcal{V} \setminus (\mathcal{I}(\mathcal{Z}_B) \cup \mathcal{S}_A)$, then $\mathcal{Z}_A$ is a set of size at most $t$ that contains $\mathcal{Z}^A_{\mathsf{min}}(\mathcal{S}_A)$. So $\mathcal{Z}_A \in \mathbb{Z}_A^t$ and $\Gamma_B(\mathcal{Z}_A) \supseteq \mathcal{S}_A \cup \mathcal{Z}_A = \mathcal{I}(\mathcal{Z}_B)$. By definition, $\mathcal{I}(\mathcal{Z}_B) \subseteq \Gamma_A(\mathcal{Z}_B)$. Therefore, $\Gamma_B(\mathcal{Z}_A) \cup \Gamma_A(\mathcal{Z}_B) = \mathcal{V}$. This contradicts the second condition in Lemma 3. □

The proof of all the corresponding claims for $\Pi^{\mathcal{S}_B}, \mathcal{S}_B \in \mathbb{S}_B^t$ are similar. $\Pi^{\mathcal{S}_A}$ and $\Pi^{\mathcal{S}_B}$ as defined above are efficient because they are both combiners of less than $2n$ efficient OT protocols[5]. □

[4] $2[n-(t+s)]-1 = 2(t+k-s)-1 > 2t+k-s-1 \geq 2t+k-r-s = n-(r+s)$, where equality is because $n = 2t+k$, first inequality is because $s < k$ (by Claim 7) and second inequality is because $r \geq 1$.

[5] We note that the protocols $\Pi^A, \Pi^B$ and $\Pi^{v_i}$ (see protocol 11 in Appendix) indeed remain efficient even when the size of adversary structure is exponential in $n$. This

*Proof (Proof of Theorem 3).* The construction of $\Pi'_{\mathsf{sh}}$ is similar to that of $\Pi_{\mathsf{sh}}$ in the proof of Theorem 1. Let $\mathbb{S}_A^t = \{\mathcal{S}_A^1, \ldots, \mathcal{S}_A^{\ell_A}\}$ and $\mathbb{S}_B^t = \{\mathcal{S}_B^1, \ldots, \mathcal{S}_B^{\ell_B}\}$. We construct $\Pi'_{\mathsf{sh}}$ as

$$\Pi'_{\mathsf{sh}} := \mathsf{Combiner}((\Pi_{1,1}, \Pi_{1,2}), \ldots, (\Pi_{\ell_A+\ell_B,1}, \Pi_{\ell_A+\ell_B,2})),$$
$$\text{where } (\Pi_{i,1}, \Pi_{i,2}) := (\Pi^{\mathcal{S}_A^i}, \Pi^B), \text{ for } 1 \leq i \leq \ell_A, \text{ and}$$
$$(\Pi_{i,1}, \Pi_{i,2}) := (\Pi^{\mathcal{S}_B^i}, \Pi^B), \text{ for } \ell_A + 1 \leq i \leq \ell_A + \ell_B.$$

From Lemma 10 and the properties of $\Pi^A, \Pi^B$, it is easy to see that against the corruption of every $\mathcal{Z} \in \mathbb{Z}^t$, a majority of the protocols in the combiner are secure. A pair of efficient protocols are contributed by every $\mathcal{S} \in \mathbb{S}_A^t \cup \mathbb{S}_B^t$ to the combiner, but as we previously observed, the size of $\mathbb{S}_A^t \cup \mathbb{S}_B^t$ is of the order $n^k$. Hence the combiner is efficient, this proves that $\Pi'_{\mathsf{sh}}$ is efficient. □

# E Proof of necessity of the first condition in Theorem 2 (Section 3.1)

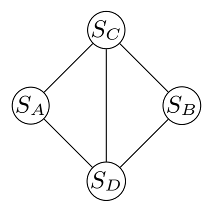


**Fig. 13.** $H_{\mathsf{MT}}$: Reliable message transmission is not possible between $S_A$ and $S_B$ if either $S_C$ or $S_D$ may be corrupted by a malicious adversary.

We show that, if the first condition of Theorem 2 is not satisfied, then $A$ and $B$ cannot communicate with non-trivial (greater that 1/2) probability of success. This leads to a contradiction as statistically secure OT implies communication with non-trivial probability of success. It is known that, if $A$ and $B$ are disconnected by removing two vertices, say, $C$ and $D$, then $A$ and $B$ cannot communicate with non-trivial probability of success if either $C$ or $D$ may be corrupted by a malicious adversary [15][6]. Suppose the first condition in Theorem 2 is not satisfied, then, there exist $\mathcal{Z}_1, \mathcal{Z}_2 \in \mathbb{Z}_{\neg A \neg B}$ such that $\mathcal{Z}_1 \cup \mathcal{Z}_2$ disconnects

is accomplished by using a secure message transmission protocol which is efficient irrespective of the size of the adversary structure.

[6] Note that although the proof in [15] is for communication without errors, it also works for our case since the contradiction is arrived at by showing that two distinct messages sent by the sender cannot be distinguished by the receiver for two different adversarial behaviors.

$A$ from $B$. Let $\mathsf{MT}$ be a protocol that realizes communication between $A$ and $B$ with probability of success more than $1/2$ with resilience against an adversary structure $\{\mathcal{Z}_1, \mathcal{Z}_2\}$. We define sets of vertices $\mathcal{V}_A := \Gamma_B(\mathcal{Z}_1 \cup \mathcal{Z}_2) \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2)$ and $\mathcal{V}_B := \mathcal{V} \setminus \Gamma_B(\mathcal{Z}_1 \cup \mathcal{Z}_2)$. Execute the protocol $\mathsf{MT}$ in $H_{\mathsf{MT}}$ (Figure 13) with $S_A, S_B, S_C$ and $S_D$ simulating $\mathcal{V}_A, \mathcal{V}_B, \mathcal{Z}_1$ and $\mathcal{Z}_2 \setminus \mathcal{Z}_1$ respectively and $S_A$ setting its input as the input to the simulated $A$ and $S_B$ returning the output at vertex $B$ it simulates. Note that vertices in $H_{\mathsf{MT}}$ are able to simulate this protocol because the vertices $\mathcal{V}_A$ (simulated by $S_A$) do not have edges to vertices in $\mathcal{V}_B$ (simulated by $S_B$). Since $\mathsf{MT}$ is resilient to the adversary structure $\{\mathcal{Z}_1, \mathcal{Z}_2 \setminus \mathcal{Z}_1\}$ (resilience against $\{\mathcal{Z}_1, \mathcal{Z}_2\}$ implies this), its execution in $H_{\mathsf{MT}}$ is resilient to the adversary structure $\{\{S_C\}, \{S_D\}\}$ The output at $B$ simulated by $S_B$ at the end of the execution is correct with probability more than $1/2$. This is a contradiction.

# F Proof of necessity of the second condition (general case) in Theorem 2 (Section 3.1)

We proceed the same way we did in the special case considered in the paper. We prove the necessity in two steps: First we show that in the graph $H'_{\mathsf{OT}}$ (Figure 14) OT cannot be realized between $A$ and $B$ with statistical security w.r.t. the malicious adversary structure $\{\{C\}, \{A, A', I\}, \{B, B', I\}\}$. Then we use this observation to prove the necessity of the second condition in Theorem 2 through a reduction argument (Lemma 12).

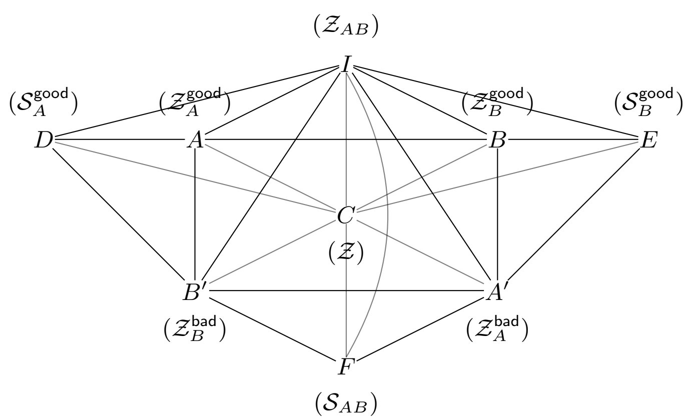


**Fig. 14.** $H'_{\mathsf{OT}}$: OT between $A$ and $B$ with security w.r.t. malicious adversary structure $\{\{C\}, \{A, A', I\}, \{B, B', I\}\}$ is impossible. This implies the necessity of condition 2 in Theorem 2. The sets shown inside brackets correspond to the vertex identification used in the proof of Lemma 12.

**Lemma 11.** *In $H'_{\mathsf{OT}}$, OT between $A$ and $B$ with statistical security w.r.t. the malicious adversary structure $\{\{C\}, \{A, A', I\}, \{B, B', I\}\}$ is impossible.*

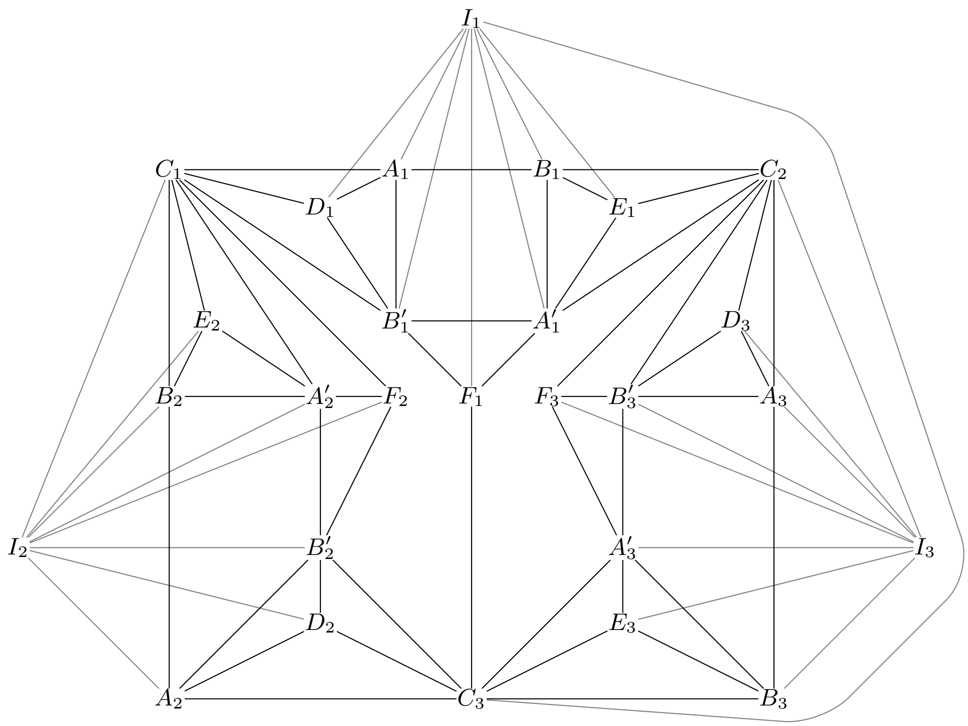


**Fig. 15.** $S'_{\mathsf{OT}}$: Constructed by interconnecting three copies of $H'_{\mathsf{OT}}$. We analyze the scenario where $v_i, i = 1, 2, 3$ in $S'_{\mathsf{OT}}$ execute the instructions for $v$ in $H'_{\mathsf{OT}}$ for protocol $\Pi$ faithfully.

*Proof.* We prove this the same way we proved Lemma 4. We first consider the case of perfect security for clarity and later argue the case of statistical security. We show that such an OT between $A$ and $B$ would imply secure 2-party OT in the semi-honest setting. To prove a contradiction let $\Pi$ be a protocol that realizes OT between $A$ and $B$ with perfect security w.r.t. the adversary structure $\{\{C\}, \{A, A', I\}, \{B, B', I\}\}$. Consider graph $S'_{\mathsf{OT}}$ in Figure 15 constructed by interconnecting three copies of $H'_{\mathsf{OT}}$. The mapping $\phi'$ from vertices in $S'_{\mathsf{OT}}$ to vertices in $H'_{\mathsf{OT}}$ is such that $\phi'(A_1) = \phi'(A_2) = \phi'(A_3) = A$, $\phi'(B_1) = \phi'(B_2) = \phi'(B_3) = B$ and so on. Then $S'_{\mathsf{OT}}$ looks locally like $H'_{\mathsf{OT}}$. For example, $B_1$ is connected to $A_1, A'_1, E_1, I_1$ and $C_2$ in $S'_{\mathsf{OT}}$, whereas in $H'_{\mathsf{OT}}$, $\phi'(B_1)$ is connected to $\phi'(A_1), \phi'(A'_1), \phi'(E_1), \phi'(I_1)$ and $\phi'(C_2)$. Let each vertex $v$ in $S'_{\mathsf{OT}}$ run the instruction for $\phi'(v)$ in the protocol $\Pi$ after fixing the input to $A_2$ and $A_3$ as

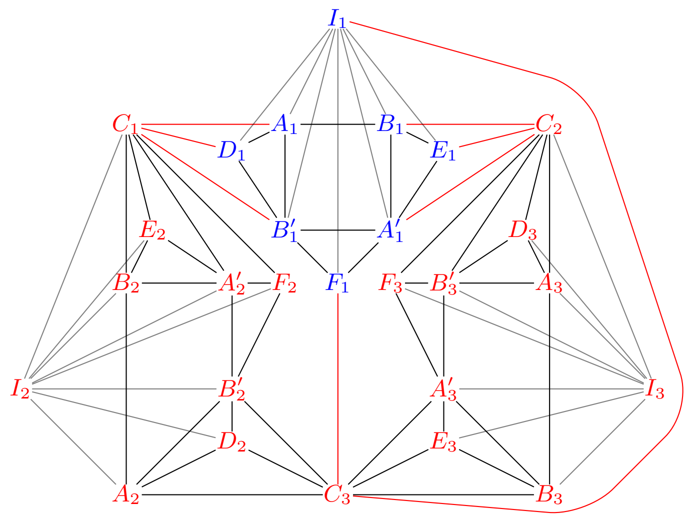


**Fig. 16.** We may visualize the execution of $\Pi'$ as vertices $A_1, B_1, D_1, E_1, F_1, I_1$ following $\Pi$ honestly and the corrupted set $\{C\}$ simulating all the vertices in red. Since $\Pi$ is secure against the corruption of $\{C\}$, $A_1$ and $B_1$ must have computed OT correctly.

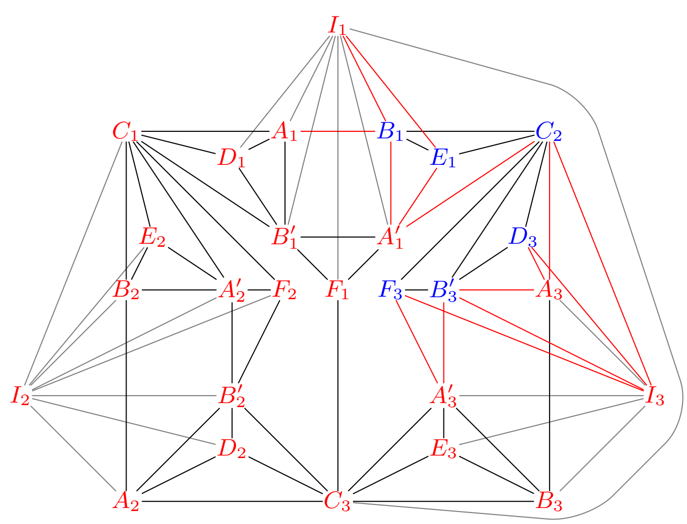


**Fig. 17.** We may visualize the execution of $\Pi'$ as vertices $B_1, E_1, C_2, B'_3, D_3, F_3$ following $\Pi$ honestly and the corrupted set $\{A, A', I\}$ simulating all the vertices in red. Since $\Pi$ is secure against the corruption of $\{A, A', I\}$, the view of all vertices in red is independent of $B_1$'s input.

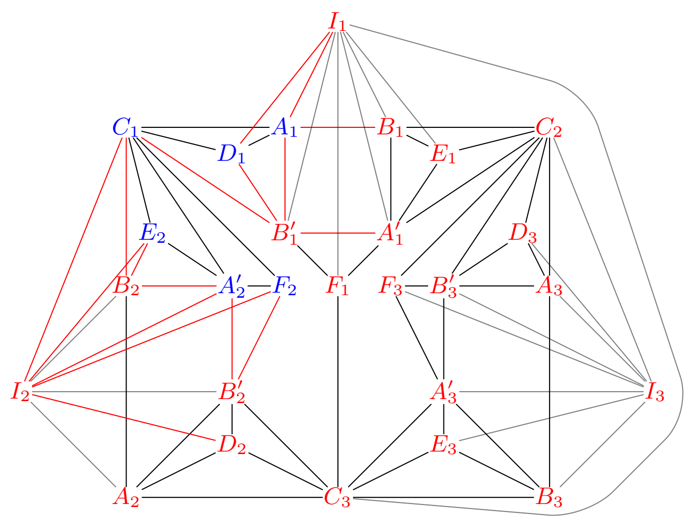


**Fig. 18.** We may visualize the execution of $\Pi'$ as vertices $A_1, D_1, C_1, A'_2, E_2, F_2$ following $\Pi$ honestly and the corrupted set $\{B, B', I\}$ simulating all the vertices in red. Since $\Pi$ is secure against the corruption of $\{B, B', I\}$, the view of vertices in red must be conditionally independent of $A_1$'s input conditioned on $B_1$'s input and output.

$(0, 0)$ and input to $B_2$ and $B_2$ as 0 and set the input to $A_1$ be $(X_0, X_1)$ and that to $B_1$ be $Q$, where $X_0, X_1, Q$ are independent uniformly random bits. We call this the execution of protocol $\Pi'$ in $S'_{\mathsf{OT}}$. Clearly $\Pi'$ is not the same as $\Pi$ ($\Pi$ is defined for 9 parties), but it is easy to see that this execution is well defined.

*Claim 10.* The output at $B_1$ is $X_Q$.

*Proof.* In Figure 16, none of the vertices in red have inputs or outputs in the protocol and $C_1, C_2$ and $C_3$ are the only vertices which have edges to any of the blue vertices (see edges in red). Hence, all the vertices in red may be thought of as being simulated by a malicious $C$. The execution of $\Pi'$ in $S'_{\mathsf{OT}}$ can be interpreted as an execution of $\Pi$ among honest parties $A_1, A'_1, B_1, B'_1, D_1, E_1, F_1, I_1$ (represented in blue) and a corrupt $C$ that simulates all the vertices in red. $\Pi$ is assumed to be secure against the corruption of $C$, therefore $A_1$ and $B_1$ must have realized OT with perfect security, hence $B_1$ outputs $X_Q$. This proves the claim. □

*Claim 11.* Let the set of vertices represented in red in Figure 17 be denoted by $\mathcal{A}_{\{A,A',I\}}$. The view of $\mathcal{A}_{\{A,A',I\}}$ is independent of $Q$.

*Proof.* In Figure 17, it can be verified that the only vertex in red that has input to output is $A_1$ and the only vertices in red to which vertices in blue have edges (edges represented in red) are $A_1, A'_1, I_1, A_3, A'_3$ and $I_3$. Hence, the execution of $\Pi'$ can also be interpreted as an execution of $\Pi$ among the honest parties (represented in blue) which include $B_1$ and a corrupt set $\{A, A', I\}$ that simulates all the parties in $\mathcal{A}_{\{A,A',I\}}$ (represented in red). $\Pi$ is assumed to be perfectly secure against the corruption of $\{A, A', I\}$. The claim follows from the fact that the view of $\mathcal{A}_{\{A,A',I\}}$ is the same as the view of $\{A, A', I\}$.

*Claim 12.* Let the set of vertices represented in red in Figure 18 be denoted by $\mathcal{A}_{\{B,B',I\}}$. The view of $\mathcal{A}_{\{B,B',I\}}$ is independent of $X_0, X_1$ conditioned on $Q, X_Q$.

*Proof.* The execution of $\Pi'$ can also be interpreted as an execution of $\Pi$ among the honest parties (represented in blue) which include $A_1$ and a corrupt set $\{B, B', I\}$ that simulates all the parties in $\mathcal{A}_{\{B,B',I\}}$ (represented in red). $\Pi$ is assumed to be perfectly secure against the corruption of $\{B, B', I\}$. Hence the view of $\mathcal{A}_{\{B,B',I\}}$ which is exactly the view of $\{B, B', I\}$ is independent of $A_1$'s input $(X_0, X_1)$ conditioned on $(Q, X_Q)$. □

Similar to the proof for the special case, we show that these claims lead to a contradiction. To see this, let parties $\mathcal{P}_1$ simulate the vertices represented in red and let $\mathcal{P}_2$ simulate vertices represented in blue in Figure 19. The vertices in the red region is the set $\mathcal{A}_{\{A,A',I\}}$ defined in the second claim and those in blue is a subset of $\mathcal{A}_{\{B,B',I\}}$ defined in the third claim and it contains the only vertex in $\mathcal{A}_{\{B,B',I\}}$ with input to the protocol. Let them execute $\Pi'$ faithfully with $\mathcal{P}_1$ setting its own input, $(X_0, X_1)$ as the input to the simulated $A_1$ and $\mathcal{P}_1$ setting its own input $Q$ as the input to the simulated $B_1$. Then,

(i) From the first claim, it follows that the output at $B_0$ is $X_Q$.
(ii) The view of $\mathcal{P}_1$ is independent of $\mathcal{P}_2$'s input $Q$ by the second claim.
(iii) The view of $\mathcal{P}_2$ is independent of $\mathcal{P}_2$'s inputs $(X_0, X_1)$ conditioned on $(Q, X_Q)$ by the third claim.

Hence $\mathcal{P}_1$ and $\mathcal{P}_2$ have realized a OT with privacy in the semi-honest setting. Hence a protocol for OT between $A$ and $B$ with perfect security w.r.t. the adversary structure $\{\{C\}, \{A, A', I\}, \{B, B', I\}\}$ in the graph $H_{\mathsf{OT}}$ in the malicious setting implies a perfectly secure 2-party OT protocol in the semi-honest setting. By the same line of reasoning, a protocol for statistically secure OT between $A$ and $B$ in the same setting would imply a statistically secure 2-party OT protocol in the semi-honest setting. The lemma now follows from the impossibility of statistically secure semi-honest 2-party OT. □

The following lemma shows that if $\mathcal{Z}_A \in \mathbb{Z}_A, \mathcal{Z}_B \in \mathbb{Z}_B$ and $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$ satisfy

$$\Gamma_B(\mathcal{Z}_A \cup \mathcal{Z}_B) \cup \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z}) = \mathcal{V}, \tag{6}$$

then any protocol for OT between $A$ and $B$ in $G$ with statistical security w.r.t. the malicious adversary structure $\mathbb{Z}$ can be simulated in $H'_{\mathsf{OT}}$ to realize OT between $A$ and $B$ in $H'_{\mathsf{OT}}$ with statistical security w.r.t. the malicious adversary $\{\{C\}, \{A, A', I\}, \{B, B', I\}\}$.

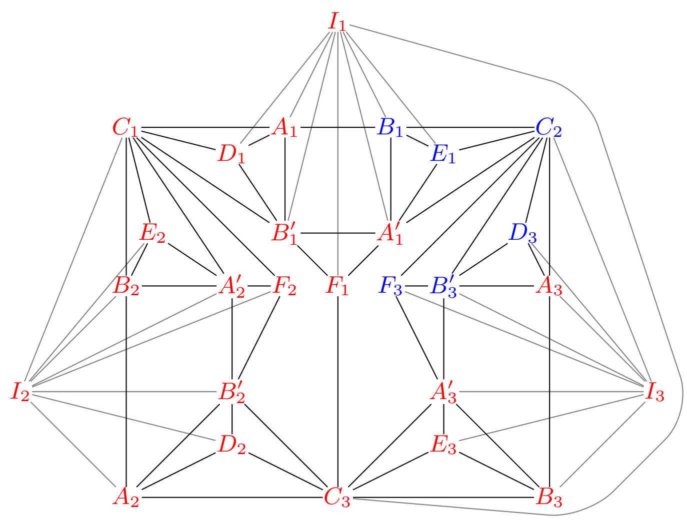


**Fig. 19.** $\mathcal{P}_1$ and $\mathcal{P}_2$ simulate the vertices represented in red and blue respectively and run $\Pi'$ faithfully after setting their inputs as inputs to $A_1$ and $B_1$ respectively to securely realize a 2-party OT, a contradiction.

**Lemma 12.** *Let $\mathcal{Z}_A \in \mathbb{Z}_A, \mathcal{Z}_B \in \mathbb{Z}_B$ and $\mathcal{Z} \in \mathbb{Z}_{\neg A \neg B}$ such that condition* (6) *is satisfied. If OT between A and B in $G(\mathcal{V}, \mathcal{E})$ can be computed with statistical security w.r.t. the malicious adversary structure $\{\mathcal{Z}_A, \mathcal{Z}_B, \mathcal{Z}\}$ then A and B in $H'_{\mathsf{OT}}(\mathcal{V}_{H'_{\mathsf{OT}}}, \mathcal{E}_{H'_{\mathsf{OT}}})$ can realize OT with statistical security w.r.t. the malicious adversary structure $\{\{C\}, \{A, A', I\}, \{B, B', I\}\}$.*

**Table 2.** Partition of $\mathcal{V}$. We represent $\Gamma_B(\mathcal{Z}_A \cup \mathcal{Z}), \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z})$ by $\Gamma_A, \Gamma_B$ respectively to reduce clutter.

| Set | Definition | Properties | |
|---|---|---|---|
| $\mathcal{Z}$ | $\mathcal{Z}$ | - | $= \xi^{-1}(C)$ |
| $\mathcal{Z}_{AB}$ | $(\mathcal{Z}_A \cap \mathcal{Z}_B) \setminus \mathcal{Z}$ | - | $= \xi^{-1}(G)$ |
| $\mathcal{Z}_A^{\mathsf{good}}$ | $(\mathcal{Z}_A \setminus (\mathcal{Z} \cup (\mathcal{Z}_A \cap \mathcal{Z}_B))) \setminus \Gamma_B$ | $\subseteq \mathcal{V} \setminus \Gamma_B$ | $= \xi^{-1}(A)$ |
| $\mathcal{Z}_A^{\mathsf{bad}}$ | $(\mathcal{Z}_A \setminus (\mathcal{Z} \cup (\mathcal{Z}_A \cap \mathcal{Z}_B))) \cap \Gamma_B$ | $\subseteq \Gamma_B \setminus (\mathcal{Z}_B \cup \mathcal{Z})$ | $= \xi^{-1}(A')$ |
| $\mathcal{Z}_B^{\mathsf{good}}$ | $(\mathcal{Z}_B \setminus (\mathcal{Z} \cup (\mathcal{Z}_A \cap \mathcal{Z}_B))) \setminus \Gamma_A$ | $\subseteq \mathcal{V} \setminus \Gamma_A$ | $= \xi^{-1}(B)$ |
| $\mathcal{Z}_B^{\mathsf{bad}}$ | $(\mathcal{Z}_B \setminus (\mathcal{Z} \cup (\mathcal{Z}_A \cap \mathcal{Z}_B))) \cap \Gamma_A$ | $\subseteq \Gamma_A \setminus (\mathcal{Z}_A \cup \mathcal{Z})$ | $= \xi^{-1}(B')$ |
| $\mathcal{S}_A^{\mathsf{good}}$ | $(\Gamma_A \setminus \Gamma_B) \setminus (\mathcal{Z}_A \cup \mathcal{Z}_B \cup \mathcal{Z})$ | $\subseteq (\mathcal{V} \setminus \Gamma_B) \cap (\Gamma_A \setminus (\mathcal{Z}_A \cup \mathcal{Z}))$ | $= \xi^{-1}(D)$ |
| $\mathcal{S}_B^{\mathsf{good}}$ | $(\Gamma_B \setminus \Gamma_A) \setminus (\mathcal{Z}_A \cup \mathcal{Z}_B \cup \mathcal{Z})$ | $\subseteq (\mathcal{V} \setminus \Gamma_A) \cap (\Gamma_B \setminus (\mathcal{Z}_B \cup \mathcal{Z}))$ | $= \xi^{-1}(E)$ |
| $\mathcal{S}_{AB}$ | $(\Gamma_B \cap \Gamma_A) \setminus (\mathcal{Z}_A \cup \mathcal{Z}_B \cup \mathcal{Z})$ | $\subseteq (\Gamma_A \setminus (\mathcal{Z}_A \cup \mathcal{Z})) \cap (\Gamma_B \setminus (\mathcal{Z}_B \cup \mathcal{Z}))$ | $= \xi^{-1}(F)$ |

*Proof.* We represent $\Gamma_B(\mathcal{Z}_A \cup \mathcal{Z}), \Gamma_A(\mathcal{Z}_B \cup \mathcal{Z})$ by $\Gamma_A, \Gamma_B$ respectively to reduce clutter. The proof proceeds the same way as the proof for Lemma 5. Consider the subsets of $\mathcal{V}$ defined in Table 2. We show the following:

(i) Sets given in Table 2 form a partition of $\mathcal{V}$ and $A \in \mathcal{Z}_A^{\mathsf{good}}, B \in \mathcal{Z}_B^{\mathsf{good}}$.

(ii) Let the map $\xi : \mathcal{V} \to \mathcal{V}_{H'_{\mathsf{OT}}}$ be as given in Figure 14, *i.e.*, for $v \in \mathcal{Z}_A^{\mathsf{good}}, \xi(v) = A$ and so on. (i) implies that $\xi$ is well defined. For $u, v \in \mathcal{V}$, edge $\{u, v\} \in \mathcal{E}$ only if $\xi(u) = \xi(v)$ or $\{\xi(u), \xi(v)\} \in \mathcal{E}_{H'_{\mathsf{OT}}}$. In short, $H'_{\mathsf{OT}}$ (or a subgraph of $H'_{\mathsf{OT}}$) is obtained from $G$ on applying *vertex contraction* to every subset of $\mathcal{V}$ given in Table 2.

(iii) If $\Pi$ realizes OT between $A$ and $B$ in $G$ securely w.r.t. the malicious adversary structure $\{\mathcal{Z}, \mathcal{Z}_A, \mathcal{Z}_B\}$, then it is also secure w.r.t. the malicious adversary structure $\{\mathcal{Z}, \mathcal{Z}_A^{\mathsf{good}} \cup \mathcal{Z}_A^{\mathsf{bad}} \cup \mathcal{Z}_{AB}, \mathcal{Z}_B^{\mathsf{good}} \cup \mathcal{Z}_B^{\mathsf{bad}} \cup \mathcal{Z}_{AB}\} = \{\xi^{-1}(C), \xi^{-1}(A) \cup \xi^{-1}(A') \cup \xi^{-1}(G), \xi^{-1}(B) \cup \xi^{-1}(B') \cup \xi^{-1}(G)\}$.

Assuming (i), (ii) and (iii), it is easy to see that the vertices in $H'_{\mathsf{OT}}$ can simulate $\Pi$ and realize OT between $A$ and $B$ with statistical security w.r.t. the malicious adversary $\{\{C\}, \{A, A', I\}, \{B, B', I\}\}$. It remains show (i), (ii) and (iii).

*Proof of (i)* – It can be easily verified from the definition of the sets that

$$\mathcal{Z} \cap \mathcal{Z}_{AB} = \emptyset \text{ and } \mathcal{Z} \cup \mathcal{Z}_{AB} = \mathcal{Z} \cup (\mathcal{Z}_A \cap \mathcal{Z}_B)$$

and that

$$\mathcal{Z}_A^{\mathsf{good}} \cap \mathcal{Z}_A^{\mathsf{bad}} = \emptyset \text{ and } \mathcal{Z}_A^{\mathsf{good}} \cup \mathcal{Z}_A^{\mathsf{bad}} = \mathcal{Z}_A \setminus (\mathcal{Z} \cup (\mathcal{Z}_A \cap \mathcal{Z}_B))$$
$$\mathcal{Z}_B^{\mathsf{good}} \cap \mathcal{Z}_B^{\mathsf{bad}} = \emptyset \text{ and } \mathcal{Z}_B^{\mathsf{good}} \cup \mathcal{Z}_B^{\mathsf{bad}} = \mathcal{Z}_B \setminus (\mathcal{Z} \cup (\mathcal{Z}_A \cap \mathcal{Z}_B))$$

Hence, $\mathcal{Z}_B^{\mathsf{good}} \cup \mathcal{Z}_B^{\mathsf{bad}}$ is disjoint from $\mathcal{Z}_A^{\mathsf{good}} \cup \mathcal{Z}_A^{\mathsf{bad}}$. Thus, $\mathcal{Z}, \mathcal{Z}_{AB}, \mathcal{Z}_A^{\mathsf{good}}, \mathcal{Z}_A^{\mathsf{bad}}, \mathcal{Z}_B^{\mathsf{good}}$ and $\mathcal{Z}_B^{\mathsf{bad}}$ are disjoint and their union is $\mathcal{Z} \cup \mathcal{Z}_A \cup \mathcal{Z}_B$. From their definitions, it is easy to verify that $\mathcal{S}_A^{\mathsf{good}}, \mathcal{S}_B^{\mathsf{good}}$ and $\mathcal{S}_{AB}$ are disjoint from from each other and from $\mathcal{Z}_A \cup \mathcal{Z}_B \cup \mathcal{Z}$. That the union of these sets give $(\Gamma_A \cup \Gamma_B) \setminus (\mathcal{Z}_A \cup \mathcal{Z}_B \cup \mathcal{Z})$ can also be verified easily. Then, from (6) it follows that these sets form a partition of $\mathcal{V}$.

Before we prove (ii), we make the following claim.

*Claim 13.* If $u \in \Gamma_A \setminus (\mathcal{Z}_A \cup \mathcal{Z})$ and $v \in \mathcal{V} \setminus \Gamma_A$, then there is no edge between $u$ and $v$.

*Proof.* $v \in \mathcal{V} \setminus \Gamma_A$ implies that there is a path from $v$ to $B$ that has no vertices from $\mathcal{Z}_A \cup \mathcal{Z}$. If there is an edge between $u$ and $v$, then $u$ has a path through $v$ that has no vertex from $\mathcal{Z}_A \cup \mathcal{Z}$. But this is a contradiction as $u \in \Gamma_A$. Similar claim may be made when $u \in \Gamma_B \setminus (\mathcal{Z}_A \cup \mathcal{Z})$ and $v \in \mathcal{V} \setminus \Gamma_B$. □

*Proof of (ii)* – This can be verified in the same way as in the proof of Lemma 5 using the properties of these sets as listed in the table and the above claim. For example, there are no edges from $\xi^{-1}(D) = \mathcal{S}_A^{\mathsf{good}}$ to $\xi^{-1}(E) = \mathcal{S}_B^{\mathsf{good}}$ since $\mathcal{S}_A^{\mathsf{good}} \subseteq \Gamma_A \setminus (\mathcal{Z}_A \cup \mathcal{Z})$ and $\mathcal{S}_B^{\mathsf{good}} \subseteq \mathcal{V} \setminus \Gamma_A$. Similarly, by the same claim, there is no edge from $\xi^{-1}(D) = \mathcal{S}_A^{\mathsf{good}}$ to $\xi^{-1}(F) = \mathcal{S}_{AB}$ as $\mathcal{S}_A^{\mathsf{good}} \subseteq \mathcal{V} \setminus \Gamma_B$ and $\mathcal{S}_{AB} \subseteq \Gamma_B \setminus (\mathcal{Z}_A \cup \mathcal{Z})$.

*Proof of (iii)* – Since $A \in \mathcal{Z}_A^{\mathsf{good}}$ and $B \in \mathcal{Z}_B^{\mathsf{good}}$ are the only vertices with input or output in $\Pi$ and $\mathcal{Z}_A^{\mathsf{good}} \cup \mathcal{Z}_A^{\mathsf{bad}} \cup \mathcal{Z}_{AB} \subseteq \mathcal{Z}_A$ and $\mathcal{Z}_B^{\mathsf{good}} \cup \mathcal{Z}_B^{\mathsf{bad}} \cup \mathcal{Z}_{AB} \subseteq \mathcal{Z}_B$, if $\Pi$ is secure w.r.t. $\{\mathcal{Z}, \mathcal{Z}_A, \mathcal{Z}_B\}$ then it is also secure w.r.t. $\{\mathcal{Z}, \mathcal{Z}_A^{\mathsf{good}} \cup \mathcal{Z}_A^{\mathsf{bad}} \cup \mathcal{Z}_{AB}, \mathcal{Z}_B^{\mathsf{good}} \cup \mathcal{Z}_B^{\mathsf{bad}} \cup \mathcal{Z}_{AB}\}$. □

The necessity of the conditions in Theorem 2 follows from Lemma 11 and Lemma 12.

## G Details Omitted from Section 3.2

*Proof (Proof of Lemma 7).* Since the inputs of $A$ and $B$ are not used in the precomputation phase, if the protocol is aborted in this phase, the input of honest parties remain private. Suppose the protocol is not aborted in the first phase. Consider $\mathcal{Z} \in \mathbb{Z}$. There are three possible cases.

Case 1 — $A, B \notin \mathcal{Z}$ : First we show that, if the protocol reaches OT computation phase, then the sampled OT is consistent, *i.e.,* $\bar{p}_{\bar{c}}^A(0) = \bar{p}_{\bar{c}}^B(0)$ with high probability. Suppose $\bar{p}_{\bar{c}}^A(0) \neq \bar{p}_{\bar{c}}^B(0)$, then the polynomials $\bar{p}_{\bar{c}}^A(x)$ and $\bar{p}_{\bar{c}}^B(x)$ are different. Hence,

$$Pr_{\alpha \in_R \mathbb{F} \setminus \{0\}} \left( \bar{p}_{\bar{c}}^A(\alpha) \neq \bar{p}_{\bar{c}}^B(\alpha) \right) \leq \frac{1}{|\mathbb{F}| - 1}.$$

This implies that the probability with which the protocol does not abort during the precomputation phase when $\bar{p}_{\bar{c}}^A(0) \neq \bar{p}_{\bar{c}}^B(0)$ is at most $\frac{1}{|\mathbb{F}|-1}$.

Since the first condition in Theorem 2 is satisfied, communication between $A$ and $B$ is perfectly secure. It is easy to see that, since $A$ and $B$ are not corrupt, the OT computation is perfectly secure provided that the sampled OT is consistent (even if the sampled OT is not private). Hence, in this case the computed OT is perfectly private and statistically correct whenever the protocol does not abort.

Case 2 — $A \in \mathcal{Z}$ but $\mathsf{path}(C, B) \cap \mathcal{Z} = \emptyset$: Since $C$ is honest, it supplies a secure sampled OT. $B$ receives her part of the sampled OT securely along $\mathsf{path}(C, B)$ as it contains no corrupted vertices. If the protocol is aborted in the precomputation phase, the privacy of $B$'s input is preserved as the real input is never used until the OT computation phase. $B$ agrees to proceed to OT computation phase if and only if the evaluations $p_0(\alpha), p_1(\alpha)$ sent by $A$ coincides with those sent by the honest $C$ (see step 6). This ensures that $A$ cannot infer anything about $B$'s input from the aborting or non-aborting of the protocol. Hence if the verification succeeds, the OT computation using the sampled OT is perfectly secure, *i.e.,* $B$'s input remains private from the adversary.

Case 3 — $B \in \mathcal{Z}$ and $\mathsf{path}(C, A) \cap \mathcal{Z} = \emptyset$: Similar to the previous case, $C$ provides a secure sampled OT and $A$ receives his part securely as $\mathsf{path}(C, A)$ contains no corrupted vertices. During the verification, $A$ sends the evaluations of the polynomials only if the $\alpha$ it received directly from $B$ and from $B$ via $C$ are identical and non-zero. Hence, $B$ obtains the evaluation of $p_0, p_1$ only on a single non-zero point from both $A$ and $C$. This ensures that $r_{1-c}$ is private from $B$ and hence if the verification succeeds, the OT computation using the sampled OT is perfectly secure.

The protocol uses a constant number of rounds of communication between vertices, of which communication between $C$ & $A$ and $C$ & $B$ use single paths of length at most $n$. The claim of efficiency then follows from the fact that the protocol used for secure communication between $A$ and $B$ is efficient as long as the size of $\mathbb{Z}$ is polynomial in $n$. □

*Proof (Proof of Lemma 9).* Paths used by $\Pi^{\mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, A), \mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, B)}$, $1 \leq i \leq \ell_B$ do not contain vertices from $\mathcal{Z}$ by construction. Hence, no vertex from $\mathcal{Z}$ is involved in the execution of the protocol, therefore (i) in Lemma 3 is true.

Consider a set $\mathcal{Z}' \in \mathbb{Z} \setminus \{\mathcal{Z}\}$. If the protocol aborts in step 1, then the inputs of honest $A$ or $B$ are private as they are not used in this step. Suppose the protocol reaches step 2 without getting aborted. If we show that against the corruption of each set in $\mathbb{Z} \setminus \{\mathcal{Z}\}$ the majority of protocols in the combiner are statistically secure, then by Lemma 8, the combiner computes OT with statistical security against $\mathbb{Z} \setminus \{\mathcal{Z}\}$. This would prove the lemma.

Consider the corruption of any set in $\mathbb{Z}_{\neg A \neg B}$. According to Lemma 7, if $\Pi^{\mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, A), \mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, B)}$ does not abort in the precomputation stage, then the OT computed in the OT computation phase is statistically secure. As previously observed, $\Pi^A$ is perfectly secure against the corruption of every set in $\mathbb{Z}_{\neg A \neg B}$. Hence all the protocols in the combiner are statistically secure against this corruption.

Against the corruption of $\mathcal{Z}_A$, protocols $\Pi^{\mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, A), \mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, B)}, 1 \leq i \leq \ell_B$ are perfectly secure. This is because $\mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, B)$ has no vertices from $\mathcal{Z}_A$ by definition, hence by Lemma 7, the OT computed by such a protocol is statistically secure against the corruption of $\mathcal{Z}_A$. Therefore, $\ell_B$ out of $2\ell_B - 1$ protocols are perfectly secure against the corruption of $\mathcal{Z}_A$, hence by Lemma 8, the claim is true for $\mathcal{Z}_A$.

Now consider any set $\mathcal{Z}_B^i \in \{\mathcal{Z}_B^1, \ldots, \mathcal{Z}_B^{\ell_B}\} = \mathbb{Z}_B$. Since $\mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, A)$ contains no vertex from $\mathcal{Z}_B^i$, the protocol $\Pi^{\mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, A), \mathsf{path}_{\mathcal{Z}_B^i}(C_{\mathcal{Z}_B^i}, B)}$ is secure against the corruption of $\mathcal{Z}_B^i$ by Lemma 7. Also, protocols $\Pi_{\ell_B+1}, \ldots, \Pi_{2\ell_B-1}$ are copies of $\Pi^A$ which are all perfectly secure against the corruption of $\mathcal{Z}_B^i$. Hence, at least $\ell_B$ among the $2\ell_B - 1$ protocols being combined are secure against the corruption of $\mathcal{Z}_B^i$.

If $\mathbb{Z}$ is of size $\mathsf{poly}(n)$, then each protocol used in the combiner is efficient by Lemma 7 and by the properties of $\Pi^A$. Hence, by Lemma 8, $\Pi^{\mathcal{Z}, \mathcal{Z}_A}$ is efficient, as it is a combiner of $2|\mathbb{Z}_B| - 1$ protocols of this kind. □

## H Protocol **Send** used in the proof of Lemma 1 (Appendix C)

Let $m$ be the message that $S$ wants to send to $R$. Let the set of all directed paths from $S$ to $R$ be represented by $\mathsf{Paths}^{S\to R} = \{p_1, \ldots, p_r\}$. In a path $p \in \mathsf{Paths}^{S\to R}$, let the $i^{th}$ vertex be represented by $p(i), i = 1, \ldots, \ell(p)$, where $\ell(p)$ is the length of the path $p$. Notice that $\ell(p) \leq n$, $p(1) = S$, and $p(\ell) = R$. We define the following:

$$\begin{aligned}
\mathsf{Out}^i(v) &:= \{w \in \mathcal{V} : \exists p \in \mathsf{Paths}^{S\to R},\ \text{where } p(i) = v, p(i+1) = w\}, 1 \leq i \leq n-1,\\
\mathsf{In}^i(v) &:= \{u \in \mathcal{V} : \exists p \in \mathsf{Paths}^{S\to R},\ \text{where } p(i-1) = u, p(i) = v\}, 2 \leq i \leq n,\\
m^1(S) &:= m,\\
r_v^i(u) &:= \text{Additive share of } m^i(v), \text{ if } u \in \mathsf{Out}^i(v), 1 \leq i \leq n-1,\\
m^i(v) &:= \sum_{u \in \mathsf{In}^i(v)} r_u^{i-1}(v), \text{ if } \mathsf{In}^i(v) \neq \emptyset, 2 \leq i \leq n.
\end{aligned}$$

**Protocol 14** (Send)**.**

1. For $1 \leq i \leq n, \forall v \in \mathcal{V}$:
   (a) Compute $m^i(v)$ (Note: $m^1(S) = m$, where $m$ is the message)
   (b) Send $r_v^i(u)$ to $u$ on edge $\{u, v\}, \forall u \in \mathsf{Out}^i(v)$
2. $R$ outputs $\sum_{i\in[n]:\mathsf{In}^i(R)\neq\emptyset} m^i(R)$

**Lemma 13.** $\mathsf{Send}^{(S\to R)}$ *efficiently realizes secure message transmission between $S$ and $R$ secure w.r.t. a semi-honest adversary structure $\mathbb{Z}$ if there exists a path between them that contains only honest vertices.*

*Proof.* It is easy to verify that at every step $i$, the sum of all the symbols received by any vertex and all the symbols received by $R$ in all the previous steps $(1, \ldots, i-1)$ is the message $m$. Since, during step $\ell(p^*)$, where $p^*$ is the longest path from $S$ to $R$, no vertex other than $R$ receives any symbol, $R$ can recover $m$ after this step by summing all the symbols it received.

Consider the corruption of a set of vertices such that there is a path $p$ from $S$ to $R$ whose vertices are all honest. The share of the message $m$ that $S$ sends to the second vertex in $p$ ($p(2)$) is hidden from the view of the corrupted vertices. This is because one of the additive shares sent forth by the second vertex in $p$ ($p(2)$) would go to the third vertex in the path ($p(3)$) and so on, and each vertex in $p$ is honest.

The protocol has $n$ rounds. In each round of the protocol, every vertex receives messages from its neighbors (at most $n-1$) and sends messages to its neighbors (at most $n-1$). Therefore, the total number of computations carried out by a vertex in the protocol is at most $n^2$ and total communication is at most $n^2$ for each vertex, this makes the protocol efficient. Note that this holds irrespective of the size of $\mathbb{Z}$. □