Complete Characterization of Broadcast and Pseudo-Signatures from Correlations*

Varun Narayanan[1], Vinod M. Prabhakaran[2], Neha Sangwan[2], and Shun Watanabe[3]

[1] Technion, Israel ✉ varunnkv@gmail.com
[2] Tata Institute of Fundamental Research, Mumbai
✉ {vinodmp,neha_010}@tifr.res.in
[3] Tokyo University of Agriculture and Technology, Japan
✉ shunwata@cc.tuat.ac.jp

Abstract. Unconditionally secure broadcast is feasible among parties connected by pairwise secure links only if there is a strict two-thirds majority of honest parties when no additional resources are available. This limitation may be circumvented when the parties have recourse to additional resources such as correlated randomness. Fitzi, Wolf, and Wullschleger (CRYPTO 2004) attempted to characterize the conditions on correlated randomness shared among three parties which would enable them to realize broadcast. Due to a gap in their impossibility argument, it turns out that their characterization is incorrect. Using a novel construction we show that broadcast is feasible under a considerably larger class of correlations. In fact, we realize pseudo-signatures, which are information theoretic counterparts of digital signatures using which unconditionally secure broadcast may be obtained. We also obtain a matching impossibility result thereby characterizing the class of correlations on which three-party broadcast (and pseudo-signatures) can be based. Our impossibility proof, which extends the well-know argument of Fischer, Lynch and Merritt (Distr. Comp., 1986) to the case where parties observe correlated randomness, maybe of independent interest.

Keywords: Unconditional security, broadcast, pseudo-signatures, information theory.

1 Introduction

Broadcast is one of the more fundamental primitives in cryptography. For instance, to realize unconditionally secure multiparty secure computation, a strict majority of honest parties suffices if broadcast is available,

* VN was supported by ISF Grants 1709/14 & 2774/20 and ERC Project NTSC (742754). VP was supported by SERB through project MTR/2020/000308 and DAE under project no. RTI4001. NS was supported by the TCS Foundation through the TCS Research Scholar Program and by DAE under project no. RTI4001. SW is supported in part by the Japan Society for the Promotion of Science (JSPS) KAKENHI under Grant 20H02144.

while, in its absence, more than two-thirds (a supermajority) of the parties must be honest. In fact, in a landmark paper, Lamport, Shostak, and Pease [24] showed that unconditionally secure broadcast can be realized if and only if there is an honest supermajority. Furthermore, they showed that broadcast can be realized with any number of malicious parties if digital signature is available among the parties.

Digital signatures based on public-key cryptography is necessarily only computationally secure. Towards realizing unconditionally secure broadcast without an honest supermajority, Pfitzmann and Waidner [32] introduced the concept of pseudo-signatures. Unlike digital signatures, pseudo-signatures have a fixed *transferability* – the number of transfers that can be made among the parties before they stop being secure. Unconditionally secure broadcast protocols can be realized without an honest supermajority if pseudo-signatures with sufficiently large transferability is available.

In the absence of an honest supermajority, pseudo-signatures (and broadcast) may be realized if the parties have access to correlated random variables. Realizing cryptographic primitives based on such a model has received considerable attention. For instance, secret key generation [1, 20, 25, 35, 37], authentication [26–28, 36], and oblivious transfer [2, 8–10, 12, 23, 31, 33, 39] have all been studied in this model. For broadcast and pseudo-signatures, such a study was initiated by Fitzi, Wolf, and Wullschleger [19]; see also [14–17].

Pseudo-signature and broadcast protocols using correlated random variables available to the parties were presented in [19]. The necessary and sufficient condition for the correlations for pseudo-signature (and broadcast) to be feasible was also claimed. However, there was a gap in the proof of necessity. In fact, it turns out that the condition itself is not necessary and there are counterexamples. In order to resolve this, novel ideas for both the construction and impossibility are needed which we present here.

There has been a renewed interest in the problem of broadcast (byzantine agreement) because of its connections to blockchains; e.g., see [5] and references therein. In this context, establishing the theoretical foundations of broadcast and pseudo-signatures takes on added interest.

The focus of this paper is on three-party broadcast (and, hence, also on three-party pseudo-signatures). However, there are implications for more than three parties. For instance, it is known that for n parties, if broadcast among every triple of them is available, then broadcast among all n parties tolerating $t < n/2$ corrupted parties is feasible [18] (and hence n-party MPC with unconditional security with the same threshold for corruption is feasible [3, 34]). We leave the problem of establishing the necessary and sufficient conditions on the correlations to realize broadcast/pseudo-signature for more than three parties as a fascinating open question.

1.1 Problem Formulation

We consider a network consisting of three parties, P_1, P_2, and P_3. The parties are connected by pairwise secure channels; we assume that the

network is synchronous, i.e., each party can recognize who should communicate next based on a common clock. As we mentioned, it is impossible to realize broadcast or pseudo-signatures from scratch if one among the three parties may be malicious. We assume that P_1, P_2, and P_3 observe random variables $(X_i)_{i\in[n]}, (Y_i)_{i\in[n]}, (Z_i)_{i\in[n]}$, respectively, where $[n] = \{1, 2, \ldots, n\}$, such that the triples $(X_i, Y_i, Z_i)_{i\in[n]}$, are independent and identically distributed (i.i.d.) according to a known distribution P_{XYZ}.

Broadcast. In a broadcast protocol, the sender P_1 has a message $b \in \{0, 1\}$ it wants to convey to the other parties. The parties communicate interactively over the pairwise secure channels. In each round of communication, the communicating party computes the message it sends based on its observations (i.e., parts of the correlation it observes), its transcript so far, and its private randomness. At the end of the protocol, the receivers P_2 and P_3 output $b_2 \in \{0, 1\}$ and $b_3 \in \{0, 1\}$, respectively. We say that a protocol is an ε-secure implementation of broadcast if the following two conditions are satisfied:

- *Correctness*: When the sender P_1 is honest with input $b \in \{0, 1\}$, then all the honest receivers output b with probability at least $1 - \varepsilon$;
- *Agreement*: When both the receivers P_2 and P_3 are honest, they output the same value $b_2 = b_3$ with probability at least $1 - \varepsilon$.

We are interested in the necessary and sufficient condition on the distribution P_{XYZ} of the correlation such that an ε-secure implementation of broadcast exists for an arbitrary $\varepsilon > 0$ and sufficiently many copies n of the correlation.

Pseudo-signature. In a pseudo-signature (PS) protocol with transfer path $P_1 \to P_2 \to P_3$, the sender P_1 has an input message $b \in \{0, 1\}$, and the protocol consists of two phases, the signing phase and the transfer phase. In the signing phase, after some prescribed rounds of communication over the pairwise secure channels, the intermediate party P_2 outputs $b_2 \in \{0, 1, \perp\}$, where the symbol $\perp$ indicates that P_2 rejects the message sent by P_1; the protocol proceeds to the transfer phase only when P_2 does not reject in the signing phase. In the transfer phase, after some prescribed rounds of communication over the pairwise secure channels, the receiver P_3 outputs $b_3 \in \{0, 1, \perp\}$, where the symbol $\perp$ indicates that P_3 rejects the message transferred by P_2. We say that a protocol is an ε-secure implementation of pseudo-signature with transfer path $P_1 \to P_2 \to P_3$ if the following four conditions are satisfied:

- *Correctness*: If P_1 and P_2 are honest, then $b_2 = b$ with probability at least $1 - \varepsilon$;
- *Unforgeability*: If P_1 and P_3 are honest, then the probability of the event $b_3 \notin \{b, \perp\}$ is less than ε;
- *Transferability*: If P_2 and P_3 are honest, then the probability of the event $(b_2 \neq \perp) \wedge (b_3 \neq b_2)$ is less than ε;
- *Secrecy*: If P_1 and P_2 are honest, then the view of P_3 in the signing phase is almost independent of the message b, i.e., the conditional

distribution of P_3's view in the signing phase given $b = 0$ and $b = 1$ are close to each other in total variation distance[4].

We are interested in the necessary and sufficient condition on P_{XYZ} such that an ε-secure pseudo-signature protocol with transfer path $P_1 \to P_2 \to P_3$ exists for an arbitrary $\varepsilon > 0$ and sufficiently large n.

Relation between broadcast and pseudo-signature. Broadcast and pseudo-signature are closely related. If a pseudo-signature protocol with either transfer path $P_1 \to P_2 \to P_3$ or $P_1 \to P_3 \to P_2$ is available, we can construct a secure implementation of broadcast with sender P_1; e.g., see [16, 32][5]. Thanks to this result, a construction for pseudo-signature implies a construction for broadcast, and an impossibility result for broadcast implies an impossibility result for pseudo-signature. Thus, we focus on constructions of pseudo-signatures and impossibility results for broadcast in this paper. The conditions on correlations under which pseudo-signature with transfer path $P_1 \to P_2 \to P_3$ is feasible and broadcast with sender P_1 is feasible turn out to be same giving us a complete characterization.

1.2 Related Work

The problem of the broadcast was introduced in [24], where the necessary and sufficient condition for feasibility of broadcast was established. An alternative proof for the impossibility part was proposed in [13]. This argument has been widely used for proving impossibility results in distributed computing; e.g., see [6, 15]. Many impossibility results on distributed computing have been derived using variants of this argument.
The concept of the pseudo-signature was introduced in [32]; see also [4] for an earlier attempt at introducing an information theoretic version of digital signature. They proposed a pseudo-signature protocol for a one bit message. More efficient constructions based on bivariate polynomials were introduced in [21] (see also [22]).
The problem of implementing broadcast and pseudo-signature from correlated random variables was studied in [19]; this problem was motivated by an implementation of broadcast from measurement outcomes of quantum entanglement [14]. The minimum requirement for realizing broadcast was studied in [15]; for instance, the global broadcast among all the parties can be constructed from the three party broadcast as long as honest majority is satisfied [18].

1.3 Main Contributions and Results

The main technical contributions of this paper are three-fold:

[4] Our construction provides a protocol with perfect secrecy, while we prove our impossibility results without making use of the secrecy condition. Thus, the secrecy condition does not affect the characterization.

[5] On the other hand, if broadcast protocols with *each* party as sender is available, a pseudo-signature protocol, also known as an information checking protocol, can be constructed [7].

(i) We give a construction for pseudo-signature from correlations (Theorem 5) which considerably expands the class of correlations for which it was known to be feasible. As we show, this construction, when combined with (ii) below, fully characterizes the class of feasible correlations which was an open problem [38, Section 18.7].

(ii) Given a pseudo-signature protocol with transfer path $P_1 \to P_3 \to P_2$, we construct a pseudo-signature protocol with transfer path $P_1 \to P_2 \to P_3$ (Theorem 6); an observation which is new to the best of our knowledge.

(iii) We prove an impossibility for broadcast (which implies tight results for pseudo-signatures and broadcast) by generalizing the well-known technique of Fischer, Lynch, and Merritt [13] to our case which has a setup in the form of correlations at the parties (Theorem 7). We believe this may be of more general interest.

Using these we precisely characterize the class of correlations on which pseudo-signatures (Theorem 8) and broadcast (Theorem 9) can be based. As mentioned earlier, this class is the same for broadcast from sender P_1 and for pseudo-signatures with either of the transfer paths which start with P_1. We also provide characterizations of the correlations under which pseudo-signature can be obtained when there is limited connectivity/directionality of links between the parties (Theorems 10-12)[6].

1.4 Technical Overview

Pseudo-signature from correlations. Attempts at altering a random variable X may leave a statistical trace that a party who holds a correlated random variable Y may be able to detect – this observation forms the basis of building a pseudo-signature protocol from correlation. The party with Y can only hope to detect anomalies in those parts of X which non-trivially depend on Y. For instance, if two symbols x and x' satisfy $P_{Y|X}(\cdot|x) = P_{Y|X}(\cdot|x')$, then a party observing Y cannot detect the swapping of x and x'. To account for this, following [19], let us define $X \setminus Y$ as the maximal part of X which non-trivially depends on Y (in statistics, this is known as the minimal sufficient statistic for Y given X).

Definition 1 (Minimal sufficient statistics). *For a pair of random variables X, Y with joint distribution P_{XY}, consider the partition of the alphabet $\mathcal{X}$ of X induced by the following equivalence relation:*

$$x \sim x' \text{ if } P_{Y|X}(y|x) = P_{Y|X}(y|x'),\ \forall y.$$

We define $\psi_{X\setminus Y}$ to be the function which maps the elements in $\mathcal{X}$ to their cell (i.e., part) in the above partition, and we define $X \setminus Y \stackrel{\text{def}}{=} \psi_{X\setminus Y}(X)$.

Notice that $X \setminus Y$ is a random variable which is a function of X alone, where the function ($\psi_{X\setminus Y}$) is defined in terms of the distribution P_{XY}.

[6] A similar question for broadcast turns out to be trivial.

Fitzi, Wolf, and Wullschleger [19] constructed a pseudo-signature protocol for transfer path $P_1 \to P_2 \to P_3$ from n i.i.d. copies of a correlation X, Y, Z observed at parties P_1, P_2, P_3, respectively. The sender P_1 attaches copies of $X \setminus Y$ as the signature (the first $n/2$ copies for message bit 0 and the second $n/2$ for message bit 1). As foreshadowed, P_2, who holds the copies of Y, may detect any significant anomalies in the signature (with high confidence for sufficiently large n; see Lemma 1). They showed that their protocol is secure as long as the simulatability condition[7]

$$X \setminus Y \longleftrightarrow Y \longleftrightarrow Z \tag{1}$$

does *not* hold. Heuristically, (1) says that P_2 can forge P_1's signature $X \setminus Y$ using Y in a manner undetectable by P_3 relying on its observations Z.

Furthermore, it was claimed in [19] that when $X \setminus Y \longleftrightarrow Y \longleftrightarrow Z$ and $X \setminus Z \longleftrightarrow Z \longleftrightarrow Y$ hold, then pseudo-signature with either of the transfer paths in which P_1 is the sender (i.e., $P_1 \to P_2 \to P_3$ or $P_1 \to P_3 \to P_2$) is impossible to build based on (X, Y, Z). However, there is a gap in the proof of [19, Theorem 3][8], and a pseudo-signature can be implemented even if both these Markov chains hold. In essence, these simulatability conditions do not account for the fact that P_2 and P_3 may effectively "upgrade" their observations by communicating with the other parties even if they do not trust the other parties. We demonstrate different possible ways in which this can be accomplished using a few examples; these examples also serve as counterexamples to [19, Theorem 3] and build up intuition for our construction.

Example 1 (Upgrading P_3's observation by communication from P_1). Let us consider a correlation induced by Rabin's oblivious transfer. Suppose that X is uniformly distributed on $\{0, 1\}$, and $Y = Z$ such that it is X with probability $\frac{1}{2}$ and the erasure symbol e with probability $\frac{1}{2}$. Then, since $Y = Z$, this correlation satisfies both $X \setminus Y \longleftrightarrow Y \longleftrightarrow Z$ and $X \setminus Z \longleftrightarrow Z \longleftrightarrow Y$. However, we can implement a pseudo-signature protocol from this correlation as follows. Let $(X_i, Y_i, Z_i)_{i\in[n]}$ be i.i.d. observations distributed according to P_{XYZ}.

1. To send message $b \in \{0, 1\}$, P_1 sends b and $(\tilde{X}_i)_{i\in T_b} = (X_i)_{i\in T_b}$ to P_2, where $T_b = \{i : \frac{bn}{2} + 1 \le i \le \frac{(b+1)n}{2}\}$.
2. P_2 rejects if $Y_i \notin \{X_i, \mathsf{e}\}$ for some $i \in T_b$. Otherwise, P_2 accepts b.
3. P_1 sends $(\hat{X}_i)_{i\in[n]} = (X_i)_{i\in[n]}$ to P_3.
4. To transfer a message b it accepted, P_2 sends $\hat{b} = b$ and $(\breve{X}_i)_{i\in T_{\hat{b}}} = (\tilde{X}_i)_{i\in T_b}$ to P_3.

[7] We write "the Markov chain $U \longleftrightarrow V \longleftrightarrow W$ holds," or simply "$U \longleftrightarrow V \longleftrightarrow W$" to mean U and W are conditionally independent conditioned on V.

[8] It turns out that by considering restricted connectivity, specifically, when there is no link between P_1 and P_3 and the link from P_2 to P_3 is unidirectional, it can be shown that pseudo-signature from (X, Y, Z) is possible (if and) only if $X \setminus Y \longleftrightarrow Y \longleftrightarrow Z$ is not a Markov chain (see Theorem 12).

5. P_3 accepts $\hat{b}$ if any one of the following holds: (i) $Z_i \notin \{\hat{X}_i, \mathsf{e}\}$ for some $i \in [n]$; and (ii) $|\{i \in T_{\hat{b}} : \breve{X}_i \neq \hat{X}_i\}| \leq n\delta$ for a parameter $\delta > 0$. Otherwise, P_3 rejects.

Clearly, the above protocol is perfectly correct. To verify transferability (security against P_1), notice that, to be successful, a corrupt P_1 must convince P_3 to reject in step 5 while ensuring that P_2 accepts in step 2. In order for this, P_1's transmissions $(\breve{X}_i)_{i \in T_b}$ and $(\hat{X}_i)_{i \in T_b}$ to P_2 and P_3, respectively, must disagree in more than $n\delta$ locations. However, unless the observations of P_2 and P_3 (i.e., $Y_i = Z_i$) are not e in *all* such locations, the attack will not succeed (since either P_2 will reject in step 2 or P_3 will accept the bit P_2 transfers in step 5). Hence, the chance of success for P_1 is at most $2^{-\delta n}$. To see unforgeability (security against P_2), notice that a successful attack by P_2 requires it to guess X_i for all $i \in T_{1-b}$ where $Y_i = \mathsf{e}$ such that the number of incorrect guesses is no more than $n\delta$. Since for each $i \in T_{1-b}$, the probability of $Y_i = \mathsf{e}$ is $1/2$ and P_2 has even odds of guessing correctly, the probability of a successful attack is $2^{-\Omega(n)}$ for $\delta < 1/8$ (see, e.g., [29, Theorem 4.5]). ▷

In the above example, P_3's observation is effectively upgraded from Z to (X, Z) using communication from P_1 in step 3. Note that (in step 5) P_3 verifies this communication from P_1; if the verification fails, P_3 accepts any message P_2 transfers, and if the verification succeeds, with overwhelming probability P_1 has not lied on more than a small fraction of locations. In general, P_3 can only (statistically) verify the parts of X which non-trivially depend on Z, namely $X \setminus Z$ (which happens to be X in this example). Thus, following the intuition in the example, we may build[9] a pseudo-signature protocol from correlations (X, Y, Z) whenever the following condition (which is stronger compared to (1)) does not hold:

$$X \setminus Y \longleftrightarrow Y \longleftrightarrow (Z, X \setminus Z). \tag{2}$$

It turns out that we may further expand the class of feasible correlations by upgrading P_3's observation via communication from both P_1 and P_2 (also see [30, Example 3 in Appendix A]). Note that the communication from P_2 could be part of the transfer step (i.e., step 4 in the example), where now, in addition to what was received from P_1, party P_2 may also send its observation Y to P_3. Assume that, as in the example, P_1 sends its X observations and P_3 has verified the $X \setminus Z$ part of this (if the verification fails, P_3 accepts the message transferred by P_2). Now, P_3 may also verify the part $Y \setminus Z$ of the Y observations sent by P_3. If the verification fails, P_3 rejects the message P_2 transfers. Otherwise, it may now upgrade its observation to $Z_1 = (Z, (X \setminus Z), (Y \setminus Z))$. Using this P_3 is now able to verify more parts of the X observations received from P_1, specifically, $X \setminus Z_1$, and similarly $Y \setminus Z_1$ of the Y received from P_2. It is clear that this procedure can be repeated. In each step, the upgrade operation involves a verification step where, based on what is currently known, the maximal dependent part of the observation being

[9] This needs a slightly more elaborate test from the one in the protocol in the example which exploits the fact that Rabin OT has erasures and no "errors."

used to perform the upgrade is verified. If the verification fails, P_3 either accepts or rejects the transferred message depending on who provided the observation. It turns out that only a fixed number of such steps suffice to reach the best possible upgraded observation. The number of steps needed depends on the distribution of (X, Y, Z) and is at most $|\mathcal{X}||\mathcal{Y}|$, the product of the alphabet sizes of X and Y; see Definition 3, the discussion after that, and Definition 4. We denote by $X^{\ddagger}$ (see Definition 4) the additional information P_3 acquires about X through this repeated upgradation procedure. The above intuition allows building a pseudo-signature protocol whenever the following condition (which is stronger still compared to (2)) does not hold:

$$X \searrow Y \longleftrightarrow Y \longleftrightarrow (Z, X^{\ddagger}). \tag{3}$$

In some cases it is also useful to upgrade P_2's observation partially so that the party is able to verify P_1's signature, but is still unable to forge the signature. The following example illustrates the idea.

Example 2 (Partially upgrading P_2's observation using communication from P_3). Consider a function MAC that takes a message M and a key K and computes an information theoretic message authentication code (MAC) as $\mathsf{MAC}_K(M)$. MACs guarantee non-forgeability, i.e., a forger (who may have access to a (message, MAC) pair) can succeed in producing a valid MAC for a fresh message with negligible probability if the key is unknown. Let MAC and MAC' be two information theoretic MACs such that MAC takes a message from $\mathcal{U}$ and a key uniformly at random from $\mathcal{V}$, and MAC' takes a message from $\mathcal{V}$ and a key uniformly at random from $\mathcal{W}$. Consider the correlation (X, Y, Z) generated using the following process:

1. Sample U, V, W uniformly and independently from $\mathcal{U}, \mathcal{V}, \mathcal{W}$, respectively.
2. Define $X = (U, \mathsf{MAC}_V(U))$, $Y = W$ and $Z = (V, \mathsf{MAC}'_W(V))$.

For all $i \in [m], j \in \{0, 1\}$, suppose $(X_{i,j}, Y_{i,j}, Z_{i,j})$ are i.i.d. according to the distribution of (X, Y, Z) described above. When P_1, P_2 and P_3 have $(X_{i,j})$, $(Y_{i,j})$ and $(Z_{i,j})$, respectively, for $i \in [m], j \in \{0, 1\}$, the following protocol implements pseudo-signature with transfer path $P_1 \to P_2 \to P_3$.

Signing Phase

1. P_3 choose $S \subset [m]$ uniformly at random conditioned on $|S| = \frac{m}{2}$ and sends S and $(\widehat{Z}_{i,j})_{i \in S, j \in \{0,1\}} = (Z_{i,j})_{i \in S, j \in \{0,1\}}$ to P_2.
2. To send message $b \in \{0, 1\}$, P_1 sends b and $(\widetilde{X}_{i,b})_{i \in [m]} = (X_{i,b})_{i \in [m]}$ to P_2.
3. P_2 accepts b unless for some $i \in S$, $\widetilde{X}_{i,b} = (u, \bar{u}), Y_{i,b} = w, \widehat{Z}_{i,b} = (v, \bar{v})$ such that $\bar{u} \neq \mathsf{MAC}_v(u)$ and $\bar{v} = \mathsf{MAC}'_w(v)$.

Transfer Phase

4. To transfer a message b it accepted, P_2 sends $\hat{b} = b$ and $(\check{X}_{i,\hat{b}})_{i \in [m]} = (\widetilde{X}_{i,b})_{i \in [m]}$ to P_3.
5. P_3 rejects $\hat{b}$ if there are more that $m/4$ distinct $i \in [m] \setminus S$ such that $\bar{u}_i \neq \mathsf{MAC}_{v_i}(u_i)$, where $\check{X}_{i,\hat{b}} = (u_i, \bar{u}_i)$ and $Z_{i,\hat{b}} = (v_i, \bar{v}_i)$. Otherwise, P_3 accepts $\hat{b}$.

To see *security against* P_1 (transferability), notice that a corrupt P_1 must ensure that the $(\widetilde{X}_{i,b})_{i\in[m]} = (u_i, \bar{u}_i)_{i\in[m]}$ it sends to P_2 is such that for all $i \in S$, $\bar{u}_i = \mathsf{MAC}_{V_{i,b}}(u_i)$ so that P_2 accepts and for at least $m/4$ of the remaining $i \in [m] \setminus S$, $\bar{u}_i \neq \mathsf{MAC}_{V_{i,b}}(u_i)$ so that P_3 rejects. Since S is a set unknown to P_1 of size $m/2$ chosen uniformly at random from $[m]$, the probability of success is negligible in m (i.e., $2^{-\Omega(m)}$). *Security against* P_2 (unforgeability) follows from the security of MAC. To convince P_3 to accept $\hat{b} = 1 - b$, the corrupt P_2 needs to generate $m/2$ purported (message, MAC) pairs corresponding to keys $(V_{i,1-b})_{i\in[m]\setminus S}$ (which it does not know) such that at least $m/4$ of them are valid pairs. Using a MAC with security parameter ϵ/m, we may ensure that only with at most ϵ probability will even one of the pairs be valid. Unlike the previous examples, P_3 participates in the signing phase. Hence we also need to consider *security against* P_3 (correctness). This will follow from the security of MAC'. A corrupt P_3 (suppose it correctly guessed P_1's b), who observes $Z_{i,b} = (V_{i,b}, \mathsf{MAC}'_{W_{i,b}}(V_{i,b})), i \in [m]$, needs to generate a valid (message, MAC) pair $(v'_{i,b}, \bar{v}'_{i,b})$ corresponding to the (unknown) key $W_{i,b}$ such that $v'_{i,b} \neq V_{i,b}$ for at least one $i \in [m]$ so that (with $S \ni i$), P_2 may reject b if $\mathsf{MAC}_{V_{i,b}}(U_{i,b}) \neq \mathsf{MAC}_{v'_{i,b}}(U_{i,b})$. If MAC' has security parameter ϵ/m, the probability that P_3 succeeds is at most ϵ. Hence, the protocol is ϵ-secure if $m = O(\log(1/\epsilon))$ and the MACs are (ϵ/m)-secure. ▷

In the above example, by providing P_3's observation (i.e., Z) to P_2 on a random subset S of the instances, we achieved two things. Firstly, this enabled P_2 to verify the signature sent by P_1 with the same confidence as P_3 would on these instances. Since S is unknown to P_1, if P_2 does not detect an anomaly among these, with overwhelming probability, P_1 has not lied on more than a constant fraction of all the instances. Secondly, by the independence of these instances, P_2 is still as oblivious about P_3's observation outside of S as before the upgrade. P_3 checking the signature only on $[m] \setminus S$ denies P_2 the possibility of a forging attack.

Note that a corrupt P_3 could try to make P_2 distrust an honest P_1 by giving out incorrect values of its observation (on a potentially cherry-picked set S; in the above example there was no advantage in cherry picking S). Hence, it is important that P_2 uses only those parts of P_3's observation it can verify to be correct, i.e., $Z \setminus Y$ (in the example, this component turns out to be all of P_3's observation). If the verification fails, P_2 accepts P_1's message. In general, these verifications may require a statistical test which may be reliable only when run over a long vector of observations (in the example, MAC allowed this verification to be done element-wise); the same is true for (the upgraded) P_2 verifying P_1's signature (which was again possible element-wise in the example). Thus, in our construction, we consider two indices: $i \in [m]$ which serves the same purpose as in the above example and $j \in [n]$ such that in step 2, for each $i \in S$, statistical tests can be carried out by P_2 over a vector indexed by j; such tests also takes away any advantage P_3 can hope to gain by picking S carefully. Similarly, in step 5, for each $i \in [m] \setminus S$, P_3 conducts statistical tests over vectors indexed by j. With these we may obtain a pseudo-signature protocol construction in which (the upgraded)

P_2 can verify signatures $X \setminus Y'$, where $Y' := (Y, Z \setminus Y)$. This pseudo-signature protocol is secure as long as the following is not a Markov chain (a stronger condition than (1)):

$$X \setminus Y' \longleftrightarrow Y \longleftrightarrow Z.$$

Notice that only the first random variable has changed in the condition. The middle random variable continues to be Y (and not Y'). This is because the upgrade of P_2's observation to Y' is limited to a random subset S, and, as we saw in the example, P_3 verifies the signature transferred by P_2 in $[m] \setminus S$ where P_2 only holds Y.
Now suppose P_2 has verified $X \setminus Y'$ as above and hence holds $Y'' = (Y', X \setminus Y')$. Then, P_2 may further upgrade its observation by verifying more of the Z it received from P_3. In particular, P_2 may verify $Z \setminus Y''$ and, if the verification passes (in case of failure P_2 accepts P_1's message), P_2 may upgrade itself to $Y''' = (Y'', Z \setminus Y'')$. With this additional upgrade, P_2 is equipped to verify a heftier signature (specifically $X \setminus Y'''$). It is clear that this procedure may be repeated, similar to the repeated upgradation procedure we saw for P_3. In each alternate step, P_2 verifies Z and X until no further upgradation is possible (this is again attained in only a finite number of steps). We denote by $X^\dagger$ (see Definition 5) the part of X that the repeated upgradation procedure allows P_2 to verify and learn. We emphasize that P_2 learns $X^\dagger$ only on a subset of instances which prevents it from using this information to mount a successful forging attack. Thus, pseudo-signature is feasible if the following Markov chain does not hold:

$$X^\dagger \longleftrightarrow Y \longleftrightarrow Z. \tag{4}$$

Our construction for pseudo-signature in Section 3.1, which combines all the ideas above and upgrades the observations of P_3 and P_2 (in a subset), gives the following result (cf. (3)-(4)):

Theorem 1 (informal). *Pseudo-signature with transfer path $P_1 \to P_2 \to P_3$ from correlation (X, Y, Z) is feasible if the following is not a Markov chain*

$$X^\dagger \longleftrightarrow Y \longleftrightarrow (Z, X^\ddagger). \tag{5}$$

Characterization of correlations. We also observe that given a pseudo-signature protocol with transfer path $P_1 \to P_3 \to P_2$, we may construct a pseudo-signature protocol with transfer path $P_1 \to P_2 \to P_3$. Our construction in Section 3.2 effectively samples a correlation using the given pseudo-signature protocol and uses this correlation to implement the protocol with the requisite altered transfer path. This observation, when combined with Theorem 1, implies that pseudo-signature from a correlation (X, Y, Z) is feasible if either (5) or its analog when the roles of Y and Z are swapped does not hold. The latter Markov chain is in fact $X^\ddagger \longleftrightarrow Z \longleftrightarrow (Y, X^\dagger)$, i.e., exchanging the roles of Y and Z also exchanges the corresponding upgrades $X^\dagger$ and $X^\ddagger$ as is evident from the similarity of the repeated upgradation procedures at P_2 and P_3 (also see Definitions 3-5). This gives the construction for our characterization theorem for pseudo-signatures.

Theorem 2 (informal). *If parties P_1, P_2, P_3 observe independent copies of correlation (X, Y, Z), a pseudo-signature protocol with transfer path $P_1 \to P_2 \to P_3$ exists if and only if at least one of the following Markov chains does not hold:*

$$X^{\dagger} \longleftrightarrow Y \longleftrightarrow (Z, X^{\ddagger}) \tag{6}$$

$$X^{\ddagger} \longleftrightarrow Z \longleftrightarrow (Y, X^{\dagger}) \tag{7}$$

Impossibility. To show the impossibility part of the above theorem, we leverage the connection between pseudo-signatures and broadcast. As mentioned earlier, broadcast with sender P_1 may be realized using a pseudo-signature protocol with P_1 as the signing party. We show that broadcast from correlation (X, Y, Z) with sender P_1 is impossible if both Markov chains (6) and (7) hold. Our impossibility proof in Section 4 is along the lines of the proof of impossibility of three-party broadcast from scratch due to Fischer, Lynch, and Merritt (FLM) [13]. It may be thought of as an extension of their argument to the case when correlations are available to the parties. Similar to [13], we make two copies of the parties (in fact, only copying party P_1 suffices) and rewire the parties to create a fictitious network. The parties in this network are fed observations from a *carefully chosen correlation* so that we may give three different interpretations which lead to a contradiction. Under each interpretation, two of the parties are honest and the third dishonest party simulates the remaining parties in the rewired network. Moreover, the choice of correlation fed to the parties in the rewired network is such that in each interpretation the correlations of the two honest parties and the one dishonest party are (X, Y, Z), and the dishonest party is able to sample the correlations needed to perform the simulation. Like in [13], the interpretations lead to a contradiction proving the impossibility. We note here that the rewired network we use is identical to the one in the (flawed) proof of [19, Theorem 7], however the rest of the proof including our use of a carefully chosen distribution is different. To the best of our knowledge this is the first instance where FLM's argument has been extended to a problem with setup where a carefully chosen setup is provided to the parties in the fictitious network. In [6], the FLM argument was applied to a case where parties may invoke partial broadcast (e.g., three party broadcast); there, providing the parties in the fictitious network with (the more obvious choice of) partial broadcast sufficed. Given the extensive use of FLM argument in proving impossibility results in distributed computing, our extension might be of independent interest. From the above discussion it is clear that we also have a characterization theorem for broadcast from correlations:

Theorem 3 (informal). *If parties P_1, P_2, P_3 observe independent copies of correlation (X, Y, Z), broadcast with sender P_1 is feasible if and only if at least one of the following Markov chains does not hold:*

$$X^{\dagger} \longleftrightarrow Y \longleftrightarrow (Z, X^{\ddagger})$$

$$X^{\ddagger} \longleftrightarrow Z \longleftrightarrow (Y, X^{\dagger})$$

Pseudo-Signature under limited connectivity. Our construction only used the unidirectional links $P_1 \Rightarrow P_2$, $P_1 \Rightarrow P_3$, and the bidirectional link $P_2 \Leftrightarrow P_3$, while the impossibility applies for protocols which may use all pairwise links in either direction. We also study pseudo-signature with transfer path $P_1 \to P_2 \to P_3$, which necessarily requires the $P_1 \Rightarrow P_2$ and $P_2 \Rightarrow P_3$ links, when one or both of $P_1 \Rightarrow P_3$ and $P_3 \Rightarrow P_2$ links that our construction additionally used are absent and provide the characterizations.

2 Preliminaries

We use the method of types from information theory [11] to prove some of the technical lemmas; see [30, Appendix B.1] for a review. A sequence $(x_i)_{i\in[n]}$ is said to be *typical* with respect to a distribution P_X when its empirical probability is close to P_X as below:

Definition 2 (γ-typical sequences). *Let X be a random variable defined on alphabet $\mathcal{X}$ with distribution P_X. For a parameter $\gamma > 0$, a sequence $(x_i)_{i\in[n]}$, where $x_i \in \mathcal{X}, i \in [n]$, is said to be (strongly)* γ-typical *if for all $a \in \mathcal{X}$ and for $N\left(a, (x_i)_{i\in[n]}\right) \stackrel{\text{def}}{=} |\{i : x_i = a, i \in [n]\}|$,*

$$\left| \frac{N\left(a, (x_i)_{i\in[n]}\right)}{n} - P_X(a) \right| \leq \frac{\gamma}{|\mathcal{X}|}.$$

The set of all γ-typical *sequences is denoted by $\mathcal{T}_\gamma^n(P_X)$.*

The nomenclature is justified by the following theorem [11, Lemma 2.12] which states that when $(X_i)_{i\in[n]}$ is drawn i.i.d. according to P_X, with overwhelming probability it will fall in $\mathcal{T}_\gamma^n(P_X)$.

Theorem 4. *Let $(X_i)_{i\in[n]}$ be a sequence of i.i.d. P_X random variables, then for any $0 < \gamma \leq 1/2$,*

$$\Pr\left[(X_i)_{i\in[n]} \notin \mathcal{T}_\gamma^n(P_X)\right] = 2^{-\Omega(n)}. \tag{8}$$

We now formalize the intuition we gave for minimal sufficient statistics $X \setminus Y$ (see the discussion around Definition 1). The following lemma states that if $(X_i, Y_i)_{i\in[n]}$ is i.i.d. according to P_{XY} and a party who possesses $(X_i)_{i\in[n]}$, but crucially no additional side-information about $(Y_i)_{i\in[n]}$, attempts to tamper with $(X_i)_{i\in[n]}$ such that the $\psi_{X\setminus Y}$ parts are significantly altered, with overwhelming probability this attempt can be detected by a second party who possesses the correlated observations $(Y_i)_{i\in[n]}$. Proofs of the lemmas in this section are available in [30, Appendix B].

Lemma 1. *For any joint distribution P_{XY} and $\gamma > 0$, there exists $\delta > 0$ that approaches 0 as γ approaches 0 such that, when $(X_i, Y_i)_{j\in[n]}$ are i.i.d. according to P_{XY}, and $(\hat{X}_j)_{j\in[n]} \longleftrightarrow (X_j)_{j\in[n]} \longleftrightarrow (Y_j)_{j\in[n]}$ is a Markov chain, then*

$$\Pr\Big[\left(|\{j : \psi_{X\setminus Y}(\hat{X}_j) \neq \psi_{X\setminus Y}(X_j)\}| > n\delta\right) \\ \wedge \left((\hat{X}^n, Y^n) \in \mathcal{T}_\gamma^n(P_{XY})\right)\Big] \leq 2^{-\Omega(n)}. \tag{9}$$

The following lemma states two basic properties of minimal sufficient statistics (Definition 1).

Lemma 2. (i) $X \longleftrightarrow (X \setminus Y) \longleftrightarrow Y$

(ii) *Suppose Y_1 is a function of Y_2, then $X \setminus Y_1 = (X \setminus Y_2) \setminus Y_1$ and hence $X \setminus Y_1$ is a function of $X \setminus Y_2$. i.e., the partition of $\mathcal{X}$ corresponding to $X \setminus Y_2$ is a refinement of the one corresponding to $X \setminus Y_1$.*

The following random variables play a role in the upgrade of P_3's observation.

Definition 3 (Upgraded random variables). *For a triple of random variables (X, Y, Z) with joint distribution P_{XYZ}, we define:*

$$\begin{aligned} Z^{(1)} &= (Z, (X \setminus Z), (Y \setminus Z)) \\ Z^{(2)} &= (Z^{(1)}, (X \setminus Z^{(1)}), (Y \setminus Z^{(1)})) \\ &\vdots \\ Z^{(i+1)} &= (Z^{(i)}, (X \setminus Z^{(i)}), (Y \setminus Z^{(i)})) \\ &\vdots \end{aligned}$$

For $j > i$, note that $Z^{(i)}$ is a function of $Z^{(j)}$. Hence, by Lemma 2(ii), $(X \setminus Z^{(i)})$ (resp., $(Y \setminus Z^{(i)})$) is a function of $(X \setminus Z^{(j)})$ (resp., $(Y \setminus Z^{(j)})$). In other words, as i increases, $X \setminus Z^{(i)}$ and $Y \setminus Z^{(i)}$ correspond to finer and finer partitions of $\mathcal{X}$ and $\mathcal{Y}$, respectively. Here $\mathcal{X}$ and $\mathcal{Y}$ denote the alphabets of X and Y respectively. Clearly, if for some i, $((X \setminus Z^{(i+1)}), (Y \setminus Z^{(i+1)})) = ((X \setminus Z^{(i)}), (Y \setminus Z^{(i)}))$ a.s. (i.e., with probability 1), then, for all $j \geq i$, $Z^{(j)} = Z^{(i)}$ a.s. and $((X \setminus Z^{(j)}), (Y \setminus Z^{(j)})) = ((X \setminus Z^{(i)}), (Y \setminus Z^{(i)}))$ a.s. Hence, the finest partitions are attained (at least) by index $i = |\mathcal{X}||\mathcal{Y}|$ and we denote these using the following notation.

Definition 4 (Upgraded random variables cont.).

$$X^{\ddagger} = X \setminus Z^{(|\mathcal{X}||\mathcal{Y}|)}, \qquad Y^{*} = Y \setminus Z^{(|\mathcal{X}||\mathcal{Y}|)}.$$

Analogously, for the upgrade of P_2's observations, we define:

Definition 5 (Upgraded random variables cont.). *For a triple of random variables (X, Y, Z) with joint distribution P_{XYZ}, we recursively define the following random variables:*

$$\begin{aligned} Y^{(1)} &= (Y, (X \setminus Y), (Z \setminus Y)) \\ Y^{(2)} &= (Y^{(1)}, (X \setminus Y^{(1)}), (Z \setminus Y^{(1)})) \\ &\vdots \\ Y^{(i+1)} &= (Y^{(i)}, (X \setminus Y^{(i)}), (Z \setminus Y^{(i)})) \\ &\vdots \\ X^{\dagger} &= X \setminus Y^{(|\mathcal{X}||\mathcal{Z}|)}, \qquad Z^{*} = Z \setminus Y^{(|\mathcal{X}||\mathcal{Z}|)}. \end{aligned}$$

The following lemma follows from the definitions and Lemma 2(i):

Lemma 3.
(i) $X \longleftrightarrow X^\dagger \longleftrightarrow (Y, Z^*)$
(ii) $Z \longleftrightarrow Z^* \longleftrightarrow (Y, X^\dagger)$
(iii) $X \longleftrightarrow X^\ddagger \longleftrightarrow (Z, Y^*)$
(iv) $Y \longleftrightarrow Y^* \longleftrightarrow (Z, X^\ddagger)$

3 Constructions

In this section we present our main constructions. In Section 3.1 we show that pseudo-signature with transfer path $P_1 \to P_2 \to P_3$ is feasible if the parties P_1, P_2, P_3 observe correlations X, Y, Z, respectively, such that $X^\dagger \longleftrightarrow Y \longleftrightarrow (Z, X^\ddagger)$ is not a Markov chain. In Section 3.2 we argue that, given a pseudo-signature protocol with transfer path $P_1 \to P_3 \to P_2$, we can obtain a pseudo-signature protocol with transfer path $P_1 \to P_2 \to P_3$ (albeit with a weaker security parameter). These two constructions together give us the feasibility direction of the characterizations of correlations which allow pseudo-signatures (and broadcast); see Section 5.

3.1 A Pseudo-Signature Protocol From Correlations

Theorem 5. *Suppose P_{XYZ} is a joint distribution such that the Markov chain $X^\dagger \longleftrightarrow Y \longleftrightarrow (Z, X^\ddagger)$ does not hold. Then, for any $\epsilon > 0$, there is an ϵ-secure pseudo-signature scheme with transfer path $P_1 \to P_2 \to P_3$ which uses $N = O(\log^2(\frac{1}{\epsilon}))$ independent copies of the correlation (X, Y, Z).*

The construction we use to prove this theorem relies on a statistical test which we describe first: Consider a joint distribution P_{UVW}. Let $U^{(0)} = U$, and $U^{(r)}$ be recursively defined as (cf. Definitions 3 and 4)

$$U^{(r)} = (U^{(r-1)}, V \setminus U^{(r-1)}, W \setminus U^{(r-1)}), \quad 1 \le r \le |\mathcal{V}||\mathcal{W}|.$$

For parameters $\gamma_1, \ldots, \gamma_{|\mathcal{V}||\mathcal{W}|} > 0$ (to be decided; see Lemma 4), the statistical test Σ_{UVW} takes as input $(u_j, v_j, w_j)_{j\in[n]}$ and proceeds as follows:

1. Set $u_j^{(0)} = u_j$ for each $j \in [n]$ and set $r = 1$.
2. If $(u_j^{(r-1)}, v_j)_{j\in[n]} \notin \mathcal{T}^n_{\gamma_r}(P_{U^{(r-1)},V})$, report failure w.r.t. V and terminate.
3. If $(u_j^{(r-1)}, w_j)_{j\in[n]} \notin \mathcal{T}^n_{\gamma_r}(P_{U^{(r-1)},W})$, report failure w.r.t. W and terminate.
4. Set $u_j^{(r)} = (u_j^{(r-1)}, \psi_{V\setminus U^{(r-1)}}(v_j), \psi_{W\setminus U^{(r-1)}}(w_j))$ for each $j \in [n]$, and set $r = r+1$. If $r \le |\mathcal{V}||\mathcal{W}|$, go to step 2; else report success and terminate.

For $r = 1$ to $|\mathcal{V}||\mathcal{W}|$, the test attempts to recursively "upgrade" $(u_j^{(r-1)})_{j\in[n]}$ by attaching to it $(f^{(r)}(v_j), g^{(r)}(w_j))_{j\in[n]}$. Before doing so, the test must verify if these attachments are valid. The intuition here is that the function $\psi_{V\setminus U^{(r-1)}}$ of $(v_j)_{j\in[n]}$ (resp. $\psi_{W\setminus U^{(r-1)}}$ of $(w_j)_{j\in[n]}$) is indeed something a statistical test can be used to test the validity of based on $(u_j^{(r-1)})_{j\in[n]}$ (see Definition 1). Step 2 (resp., 3) performs this validity check by testing whether $(v_j)_{j\in[n]}$ (resp., $(w_j)_{j\in[n]}$) is "typical" with the current $u_j^{(r-1)}$ according to the joint distribution $P_{U^{(r-1)},V}$ (resp., $P_{U^{(r-1)},W}$). If not, the test terminates at this step with failure w.r.t. V (resp. W). The test terminates with success if none of the validity tests fail. When this happens, the test has verified the validity of $(\psi_{V\setminus U^{(|\mathcal{V}||\mathcal{W}|)}}(v_j), \psi_{W\setminus U^{(|\mathcal{V}||\mathcal{W}|)}}(w_j))_{j\in[n]}$.

The following lemma formalizes the intuition. It states that while the test will report failure with negligible property when run with inputs $(U_j, V_j, W_j)_{j\in[n]}$ generated P_{UVW} i.i.d., it is also robust to maliciously generated inputs. Specifically, if $(W_j)_{j\in[n]}$ is replaced with a $(\hat{W}_j)_{j\in[n]}$ generated conditionally independent of $(U_j, V_j)_{j\in[n]}$ conditioned on $(W_j)_{j\in[n]}$, then only with negligible probability will the test (a) report failure w.r.t. V, or (b) report success when for more than a small fraction of j's, $\hat{W}_j$ and W_j map to different values under $\psi_{W\setminus U^{(|\mathcal{V}||\mathcal{W}|)}}$ (or $\psi_{W\setminus U^{(r)}}$ for any r as $r = |\mathcal{V}||\mathcal{W}|$ corresponds to the finest partition). The lemma gives similar guarantees when $(V_j)_{j\in[n]}$ is replaced with a $(\hat{V}_j)_{j\in[n]}$.

Lemma 4. *Suppose (U_j, V_j, W_j) are i.i.d. according to P_{UVW} for all $j \in [n]$. For any $\delta > 0$, there exist parameters $\gamma_1, \ldots, \gamma_{|\mathcal{V}||\mathcal{W}|} > 0$ such that*

(i) *Σ_{UVW} succeeds with probability $1-2^{-\Omega(n)}$ on input $(U_j, V_j, W_j)_{j\in[n]}$.*

(ii) *Suppose $(\hat{W}_j)_{j\in[n]} \longleftrightarrow (W_j)_{j\in[n]} \longleftrightarrow (U_j, V_j)_{j\in[n]}$ is a Markov chain. On input $(U_j, V_j, \hat{W}_j)_{j\in[n]}$,*
   (a) Σ_{UVW} reports failure w.r.t. V with probability $2^{-\Omega(n)}$.
   (b) When $\ell = |\mathcal{V}||\mathcal{W}|$,

$$\Pr\Big[(|\{j : \psi_{W\setminus U^{(\ell)}}(\hat{W}_j) \neq \psi_{W\setminus U^{(\ell)}}(W_j)\}| > n\delta) \wedge (\Sigma_{UVW} \text{ reports success})\Big] \leq 2^{-\Omega(n)}.$$

(iii) *Suppose $(\hat{V}_j)_{j\in[n]} \longleftrightarrow (V_j)_{j\in[n]} \longleftrightarrow (U_j, W_j)_{j\in[n]}$ is a Markov chain. On input $(U_j, \hat{V}_j, W_j)_{j\in[n]}$,*
   (a) Σ_{UVW} reports failure w.r.t. W with probability $2^{-\Omega(n)}$.
   (b) When $\ell = |\mathcal{V}||\mathcal{W}|$,

$$\Pr\Big[(|\{j : \psi_{V\setminus U^{(\ell)}}(\hat{V}_j) \neq \psi_{V\setminus U^{(\ell)}}(V_j)\}| > n\delta) \wedge (\Sigma_{UVW} \text{ reports success})\Big] \leq 2^{-\Omega(n)}.$$

See [30, Appendix C.1] for a proof which makes repeated uses of Lemma 1.

We will show that the following protocol implements pseudo-signature with transfer path $P_1 \to P_2 \to P_3$ using the correlation (X, Y, Z).

Parties P_1, P_2 and P_3 receive inputs $(X_{i,j})_{i\in[m],j\in[n]}$, $(Y_{i,j})_{i\in[m],j\in[n]}$, and $(Z_{i,j})_{i\in[m],j\in[n]}$, respectively, such that, for all $i \in [m], j \in [n]$,

$(X_{i,j}, Y_{i,j}, Z_{i,j})$ are i.i.d. according to P_{XYZ}. The parameters m, n, and $\gamma > 0$ in the protocol will be specified during the security analysis.

Signing Phase

1. P_3 uniformly samples $S \subset [m]$ conditioned on $|S| = m/2$ and sends S, $(\hat{Z}_{i,j})_{i\in S, j\in[n]} = (Z_{i,j})_{i\in S, j\in[n]}$ to P_2.
2. To send message $b \in \{0,1\}$, P_1 sends b and $(\tilde{X}_{i,j})_{i\in[m], j\in T_b} = (X_{i,j})_{i\in[m], j\in T_b}$ to P_2, where $T_b = \{i : \frac{bn}{2} + 1 \le i \le \frac{(b+1)n}{2}\}$.
3. P_2 accepts b unless for some $i \in S$ (S of size $m/2$) the statistical test Σ_{YZX} with input $(Y_{i,j}, \widehat{Z}_{i,j}, \widetilde{X}_{i,j})_{j\in T_b}$ fails w.r.t. X. In the latter case P_2 rejects b.

Transfer Phase

4. To transfer a message b it accepted, P_2 sends $\hat{b} = b$ and $(\breve{X}_{i,j}, \breve{Y}_{i,j})_{i\in[m], j\in T_{\hat{b}}} = (\tilde{X}_{i,j}, Y_{i,j})_{i\in[m], j\in T_b}$ to P_3.
5. P_1 sends $(\hat{X}_{i,j})_{i\in[m], j\in[n]} = (X_{i,j})_{i\in[m], j\in[n]}$ to P_3.
6. For each $i \in [m] \setminus S$, P_3 runs Σ_{ZXY} with input $(Z_{i,j}, \hat{X}_{i,j}, \breve{Y}_{i,j})_{j\in T_{\hat{b}}}$. If for some $i \in [m] \setminus S$, Σ_{ZXY} fails w.r.t. X, P_3 accepts $\hat{b}$, else if Σ_{ZXY} fails w.r.t. Y for some $i \in [m] \setminus S$, P_3 rejects. If Σ_{ZXY} reports success for all $i \in [m] \setminus S$, go to the next step.
7. Denote $\psi_{X\searrow Y^{(|\mathcal{X}||\mathcal{Z}|)}}$ by $f^\dagger$ and $\psi_{X\searrow Z^{(|\mathcal{X}||\mathcal{Y}|)}}$ by $f^\ddagger$. P_3 rejects $\hat{b}$ if there are more than $m/4$ distinct $i \in [m] \setminus S$ such that

$$(f^\dagger(\breve{X}_{i,j}), Z_{i,j}, f^\ddagger(\hat{X}_{i,j}))_{j\in T_{\hat{b}}} \notin \mathcal{T}_\gamma^{n/2}(P_{X^\dagger Z X^\ddagger}).$$

   P_3 accepts $\hat{b}$ otherwise.

Proof (Theorem 5). Let $\delta, \gamma > 0$ (to be decided) and set the parameters for the statistical tests Σ_{YZX} and Σ_{ZXY} in the protocol from Lemma 4. We first argue the correctness of the protocol. Lemma 4(i) guarantees that when all parties behave honestly, each invocation of the tests Σ_{YZX} and Σ_{ZXY} in the protocol reports success with probability $1 - 2^{-\Omega(n)}$. Furthermore, since $\gamma > 0$, each typicality check made by P_3 in step 7 succeeds with probability $1 - 2^{-\Omega(n)}$ by Theorem 4. Thus, by a union bound, P_2 and P_3 together accept P_1's message with probability $1 - m2^{-\Omega(n)}$.

We will separately consider the cases where P_1, P_2, and P_3 are corrupt.

Security against P_3 (Correctness). Suppose P_3 sends $S \subset [m]$ and $(\hat{Z}_{i,j})_{i\in S, j\in[n]}$ to P_2 in step 1. To prove security against P_3, it suffices to show that, for all $i \in S$, when P_2 runs Σ_{YZX} with input $(Y_{i,j}, \hat{Z}_{i,j}, X_{i,j})_{j\in T_b}$ in step 3, it reports failure w.r.t. X with only a negligible probability. Notice that $(S, (\hat{Z}_{i,j})_{i\in S, j\in[n]})$ satisfies the Markov chain

$$S, (\hat{Z}_{i,j})_{i\in S, j\in[n]} \longleftrightarrow (Z_{i,j})_{i\in[m], j\in[n]} \longleftrightarrow (X_{i,j}, Y_{i,j})_{i\in[m], j\in[n]}. \quad (10)$$

Let us define

$$(\hat{Z}_{i,j})_{i\in[m]\setminus S, j\in T_b} = (Z_{i,j})_{i\in[m]\setminus S, j\in T_b}. \quad (11)$$

Then

$$\Pr\left[\exists i \in S \text{ s.t. } \Sigma_{YZX} \text{ fails w.r.t. } X \text{ on input } (Y_{i,j}, \hat{Z}_{i,j}, X_{i,j})_{j\in T_b}\right]$$

$$\leq \Pr\left[\exists i \in [m] \text{ s.t. } \Sigma_{YZX} \text{ fails w.r.t. } X \text{ on input } (Y_{i,j}, \hat{Z}_{i,j}, X_{i,j})_{j\in T_b}\right]$$
$$\leq \sum_{i=1}^{m} \Pr\left[\Sigma_{YZX} \text{ fails w.r.t. } X \text{ on input } (Y_{i,j}, \hat{Z}_{i,j}, X_{i,j})_{j\in T_b}\right],$$

where the last step is a union bound. To bound each of these probabilities, we notice that by (10)-(11) and the fact that $(X_{i,j}, Y_{i,j}, Z_{i,j})$ are i.i.d. over $i \in [m], j \in [n]$, the following Markov chain holds for each $i \in [m]$:

$$(\hat{Z}_{i,j})_{j\in[n]} \longleftrightarrow (Z_{i,j})_{j\in[n]} \longleftrightarrow (X_{i,j}, Y_{i,j})_{j\in[n]} \tag{12}$$

Hence, by Lemma 4(iii)(a), for $i \in [m]$,

$$\Pr\left[\Sigma_{YZX} \text{ fails w.r.t. } X \text{ on input } (Y_{i,j}, \hat{Z}_{i,j}, X_{i,j})_{j\in T_b}\right] = 2^{-\Omega(|T_b|)} = 2^{-\Omega(n)}.$$

Thus, P_2 accepts P_1's message with probability $1 - m2^{-\Omega(n)}$.

Security against P_1 (Transferability). To prove security against P_1, it is sufficient to show that, if P_2 accepts, then P_3 also accepts with overwhelming probability. Fix $b \in \{0, 1\}$. Suppose P_1 sends $(b, (\tilde{X}_{i,j})_{i\in[m],j\in T_b})$ to P_2 in step 2 and $(\hat{X}_{i,j})_{i\in[m],j\in[n]}$ to P_3 in step 5. Then,

$$\begin{aligned}\left((\hat{X}_{i,j})_{i\in[m],j\in[n]}, (\tilde{X}_{i,j})_{i\in[m],j\in T_b}\right) &\longleftrightarrow (X_{i,j})_{i\in[m],j\in[n]} \\ &\longleftrightarrow \left(S, (Y_{i,j}, Z_{i,j})_{i\in[m],j\in[n]}\right).\end{aligned} \tag{13}$$

Formally, we need to show that the event $E = (E_1 \vee E_2) \wedge (E_3 \vee (E_4 \wedge E_5))$ occurs with negligible probability, where

1. E_1 is the event "Σ_{YZX} succeeds on input $(Y_{i,j}, Z_{i,j}, \tilde{X}_{i,j})_{j\in T_b}$ in step 3 for each $i \in S$".
2. E_2 is the event "Σ_{YZX} fails w.r.t. Z on input $(Y_{i,j}, Z_{i,j}, \tilde{X}_{i,j})_{j\in T_b}$ in step 3 for some $i \in S$".
3. E_3 is the event "Σ_{ZXY} fails w.r.t. Y on input $(Z_{i,j}, \hat{X}_{i,j}, Y_{i,j})_{j\in T_b}$ in step 6 for some $i \in [m] \setminus S$".
4. E_4 is the event "Σ_{ZXY} succeeds on input $(Z_{i,j}, \hat{X}_{i,j}, Y_{i,j})_{j\in T_b}$ in step 6 for each $i \in [m] \setminus S$".
5. E_5 is the event "in step 7, $(f^\dagger(\tilde{X}_{i,j}), Z_{i,j}, f^\ddagger(\hat{X}_{i,j}))_{j\in T_b} \notin \mathcal{T}_\gamma^n(P_{X^\dagger ZX^\ddagger})$ for at least $\frac{m}{4}$ distinct values of $i \in [m] \setminus S$."

Note that, here $E_1 \vee E_2$ is the event in which P_2 accepts the signature, and $E_3 \vee (E_4 \wedge E_5)$ is the event in which P_3 rejects the signature. Since $(E_1 \vee E_2) \wedge (E_3 \vee (E_4 \wedge E_5)) \subset E_2 \vee E_3 \vee (E_1 \wedge E_4 \wedge E_5)$,

$$\begin{aligned}\Pr[E] &= \Pr[(E_1 \vee E_2) \wedge (E_3 \vee (E_4 \wedge E_5))] \\ &\leq \Pr[E_2] + \Pr[E_3] + \Pr[E_1 \wedge E_4 \wedge E_5].\end{aligned} \tag{14}$$

We now bound each of these probabilities. We have

$$\Pr[E_2] = \sum_{\hat{S}\subset[m]:|\hat{S}|=\frac{m}{2}} \Pr[S = \hat{S}] \cdot \Pr[E_2 | S = \hat{S}].$$

Since S is chosen independent of $(\tilde{X}_{i,j}, Y_{i,j}, Z_{i,j})_{i\in[m],j\in T_b}$,

$$\begin{aligned}\Pr[E_2|S=\hat{S}] &= \Pr\left[\exists i \in \hat{S} \text{ s.t. } \Sigma_{YZX} \text{ fails w.r.t. } Z \text{ for } (Y_{i,j}, Z_{i,j}, \tilde{X}_{i,j})_{j\in T_b}\right] \\ &\leq \sum_{i\in\hat{S}} \Pr\left[\Sigma_{YZX} \text{ fails w.r.t. } Z \text{ on } (Y_{i,j}, Z_{i,j}, \tilde{X}_{i,j})_{j\in T_b}\right] \\ &= |\hat{S}| 2^{-\Omega(|T_b|)} = m2^{-\Omega(n)},\end{aligned}$$

where the bound on the probabilities in the last step follows from Lemma 4(ii)(a) since, by (13) and the fact that $(X_{i,j}, Y_{i,j}, Z_{i,j})$ are i.i.d. over $i \in [m], j \in [n]$, the following Markov chain holds for each $i \in [m]$:

$$(\tilde{X}_{i,j})_{j\in T_b} \longleftrightarrow (X_{i,j})_{j\in T_b} \longleftrightarrow (Y_{i,j}, Z_{i,j})_{j\in T_b}. \tag{15}$$

Hence,

$$\Pr[E_2] \leq \sum_{\hat{S}\subset[m]:|\hat{S}|=\frac{m}{2}} \Pr[S=\hat{S}]\, m2^{-\Omega(n)} = m2^{-\Omega(n)}. \tag{16}$$

To bound $\Pr[E_3]$, using the fact that

$$(\hat{X}_{i,j})_{j\in T_b} \longleftrightarrow (X_{i,j})_{j\in T_b} \longleftrightarrow (Y_{i,j}, Z_{i,j})_{j\in T_b} \tag{17}$$

is a Markov chain for each $i \in [m]$ and that $(\hat{X}_{i,j}, Y_{i,j}, Z_{i,j})_{i\in[m],j\in T_b}$ is independent of S, following similar steps as above (invoking Lemma 4(iii)(a) along the way) we have

$$\begin{aligned}\Pr[E_3] &= \Pr\left[\exists i \in [m]\setminus S \text{ s.t. } \Sigma_{ZXY} \text{ fails w.r.t. } Y \text{ for } (Z_{i,j}, \hat{X}_{i,j}, Y_{i,j})_{j\in T_b}\right] \\ &= m2^{-\Omega(n)}.\end{aligned} \tag{18}$$

We now bound $\Pr[E_1 \wedge E_4 \wedge E_5]$. Recall that we denote $f^\dagger = \psi_{X\searrow Y^{(|\mathcal{X}||\mathcal{Z}|)}}$ and $f^\ddagger = \psi_{X\searrow Z^{(|\mathcal{X}||\mathcal{Y}|)}}$. Let us define the events

$$\begin{aligned}B &= \left(|\{i\in[m]\setminus S : |\{j\in T_b : f^\dagger(\tilde{X}_{i,j}) \neq f^\dagger(X_{i,j})\}| > n\delta)\}| \geq \frac{m}{8}\right), \\ C &= \left(\exists i \in [m]\setminus S \text{ such that } |\{j\in T_b : f^\ddagger(\hat{X}_{i,j}) \neq f^\ddagger(X_{i,j})\}| > n\delta\right).\end{aligned}$$

Since $E_1 \wedge E_4 \wedge E_5 \subset (E_1 \wedge B) \vee (E_4 \wedge C) \vee (E_5 \wedge B^c \wedge C^c)$,

$$\Pr[E_1 \wedge E_4 \wedge E_5] \leq \Pr[E_1 \wedge B] + \Pr[E_4 \wedge C] + \Pr[E_5 \wedge B^c \wedge C^c]. \tag{19}$$

We proceed to bound each of these probabilities.

$$\Pr[E_1 \wedge B] \leq \Pr[B \wedge D] + \Pr[E_1 \wedge D^c],$$

where $D = \bigwedge_{i\in S}(|\{j \in T_b : f^\dagger(\tilde{X}_{i,j}) \neq f^\dagger(X_{i,j})\}| \leq n\delta)$. For $i \in [m]$, if we define F_i as the indicator random variable of the event $(|\{j \in T_b : f^\dagger(\tilde{X}_{i,j}) \neq f^\dagger(X_{i,j})\}| > n\delta)$, then

$$B = \left(\sum_{i=1}^{m} F_i \geq \frac{m}{8}\right), \qquad D = \left(\sum_{i\in S} F_i = 0\right).$$

Since S is a random subset of size $m/2$ uniformly chosen from $[m]$ independent of $(\tilde{X}_{i,j}, X_{i,j})_{i\in[m],j\in T_b}$ (and therefore independent of $(F_i)_{i\in[m]}$),

$$\Pr[B \wedge D] = 2^{-\Omega(m)}.$$

Now, to bound $\Pr[E_1 \wedge D^c]$, for $i \in [m]$, let

$$E_{1,i} = \Big((\Sigma_{YZX} \text{ succeeds for } (Y_{i,j}, Z_{i,j}, \tilde{X}_{i,j})_{j\in T_b}) \\ \wedge \left(|\{j \in T_b : f^\dagger(\tilde{X}_{i,j}) \neq f^\dagger(X_{i,j})\}| > n\delta\right)\Big).$$

Then

$$E_1 \wedge D^c = \Big((\Sigma_{YZX} \text{ succeeds for } (Y_{i,j}, Z_{i,j}, \tilde{X}_{i,j})_{j\in T_b}, \forall i \in S) \\ \wedge \left(\exists i \in S \text{ s.t. } |\{j \in T_b : f^\dagger(\tilde{X}_{i,j}) \neq f^\dagger(X_{i,j})\}| > n\delta\right)\Big) \\ \subset \bigvee_{i\in S} E_{1,i}.$$

Hence,

$$\Pr[E_1 \wedge D^c] \leq \Pr\left[\bigvee_{i\in S} E_{1,i}\right] \\ \leq \sum_{\hat{S}\subset[m]:|\hat{S}|=\frac{m}{2}} \Pr[S = \hat{S}] \sum_{i\in\hat{S}} \Pr[E_{1,i}|S = \hat{S}],$$

where the last inequality is a union bound. By the independence of S and $(\tilde{X}_{i,j}, Y_{i,j}, Z_{i,j})_{i\in[m],j\in T_b}$,

$$\Pr[E_{1,i}|S = \hat{S}] \\ = \Pr\Big[(\Sigma_{YZX} \text{ succeeds for } (Y_{i,j}, Z_{i,j}, \tilde{X}_{i,j})_{j\in T_b}) \\ \wedge \left(|\{j \in T_b : f^\dagger(\tilde{X}_{i,j}) \neq f^\dagger(X_{i,j})\}| > n\delta\right)\Big] \\ = 2^{-\Omega(n)},$$

where the last step follows from Lemma 4(ii)(b) since the Markov chain (15) holds for each $i \in [m]$ and $f^\dagger = \psi_{X\setminus Y^{(|\mathcal{X}||\mathcal{Z}|)}}$. Thus, $\Pr[E_1 \wedge B] = 2^{-\Omega(m)} + m2^{-\Omega(n)}$.
To bound the term $\Pr[E_4 \wedge C]$ in (19), let us define, for $i \in [m]$,

$$E_{4,i} = \Big((\Sigma_{ZXY} \text{ succeeds for } (Z_{i,j}, \hat{X}_{i,j}, Y_{i,j})_{j\in T_b}) \\ \wedge \left(|\{j \in T_b : f^\ddagger(\hat{X}_{i,j}) \neq f^\ddagger(X_{i,j})\}| > n\delta\right)\Big).$$

Since $(E_4 \wedge C) \subset \bigvee_{i\in[m]\setminus S} E_{4,i}$,

$$\Pr\left[E_4 \wedge C\right] \leq \Pr\left[\bigvee_{i\in[m]\setminus S} E_{4,i}\right]$$

$$\leq \sum_{\hat{S}\subset[m]:|\hat{S}|=\frac{m}{2}} \Pr[S=\hat{S}] \sum_{i\in[m]\setminus\hat{S}} \Pr[E_{4,i}|S=\hat{S}].$$

We may bound $\Pr[E_{4,i}|S=\hat{S}]$ using the Markov chain (17) and the independence of $(\hat{X}_{i,j}, Y_{i,j}, Z_{i,j})_{i\in[m],j\in T_b}$ and S following similar steps as in the bound for $\Pr[E_{1,i}|S=\hat{S}]$ above (now invoking Lemma 4(iii)(b)) to obtain $\Pr[E_4 \wedge C] \leq m2^{-\Omega(n)}$.
To bound the term $\Pr[E_5 \wedge B^c \wedge C^c]$ in (19), we will make use of the following lemma:

Lemma 5. *For any distribution P_{UV} and $\delta > 0$, there exists $\gamma > 0$ that approaches 0 as δ approaches 0 such that, for random variables $(U_j, V_j, \hat{U}_j, \hat{V}_j)_{j\in[n]}$ with $(U_j, V_j)_{j\in[n]}$ i.i.d. according to P_{UV},*

$$\Pr\Big[(|\{j:\hat{U}_j \neq U_j\}| \leq n\delta) \wedge (|\{j:\hat{V}_j \neq V_j\}| \leq n\delta) \\ \wedge ((\hat{U}_j,\hat{V}_j)_{j\in[n]} \notin \mathcal{T}_\gamma^n(P_{UV}))\Big] \leq 2^{-\Omega(n)}. \quad (20)$$

For $i \in [m]$, define the events

$$E_{5,i} = \Big(((f^\dagger(\tilde{X}_{i,j}), Z_{i,j}, f^\ddagger(\hat{X}_{i,j}))_{j\in T_b} \notin \mathcal{T}_\gamma^{\frac{n}{2}}(P_{X^\dagger ZX^\ddagger})) \\ \wedge (|\{j\in T_b : f^\dagger(\tilde{X}_{i,j}) \neq f^\dagger(X_{i,j})\}| \leq n\delta) \\ \wedge (|\{j\in T_b : f^\ddagger(\hat{X}_{i,j}) \neq f^\ddagger(X_{i,j})\}| \leq n\delta)\Big).$$

Since $E_5 \wedge B^c \wedge C^c \subset \bigvee_{i\in[m]\setminus S} E_{5,i}$,

$$\Pr[E_5 \wedge B^c \wedge C^c] \leq \Pr\left[\bigvee_{i\in[m]\setminus S} E_{5,i}\right] \\ \leq \sum_{\hat{S}\subset[m]:|\hat{S}|=\frac{m}{2}} \Pr[S=\hat{S}] \sum_{i\in[m]\setminus\hat{S}} \Pr[E_{5,i}|S=\hat{S}].$$

Once again, since $(\tilde{X}_{i,j}, \hat{X}_{i,j}, Y_{i,j}, Z_{i,j})_{i\in[m],j\in T_b}$ is independent of S,

$$\Pr[E_{5,i}|S=\hat{S}] \\ \leq \Pr\Big[((f^\dagger(\tilde{X}_{i,j}), Z_{i,j}, f^\ddagger(\hat{X}_{i,j}))_{j\in T_b} \notin \mathcal{T}_\gamma^{\frac{n}{2}}(P_{X^\dagger ZX^\ddagger})) \\ \wedge (|\{j\in[n] : f^\ddagger(\hat{X}_{i,j}) \neq f^\ddagger(X_{i,j})\}| \leq n\delta) \\ \wedge \Big(|\{j\in T_b : f^\dagger(\tilde{X}_{i,j}) \neq f^\dagger(X_{i,j})\}| \leq n\delta)\Big)\Big] \\ = 2^{-\Omega(n)},$$

where the bound in the last step follows from Lemma 5 (take P_{UV} as $P_{X^\dagger(ZX^\ddagger)}$, i.e., $U = X^\dagger$ and $V = (Z, X^\ddagger)$) as long as $\delta > 0$ is sufficiently small for a given choice of $\gamma > 0$ (we ensure that this is the case at the end of this proof). Hence, $\Pr[E_5 \wedge B^c \wedge C^c] = m2^{-\Omega(n)}$. Gathering the bounds for all terms in (19), we have shown that $\Pr[E_1 \wedge E_4 \wedge E_5] = m2^{-\Omega(n)} + 2^{-\Omega(m)}$. Together with (14),(16),(18), this proves security against a corrupt P_1 if we choose $m = n$ (as we will do at the end of the proof).

Security against P_2 (Unforgeability). To prove security against P_2, it is sufficient to show that, when P_1's message is b and P_2 claims in step 4 that it received $1-b$ from P_1, party P_3 rejects with overwhelming probability. Suppose P_2 sends $(1-b, (\breve{X}_{i,j}, \breve{Y}_{i,j})_{i\in[m], j\in T_{1-b}})$ to P_3 in step 4. Then, these random variables satisfy the following Markov chain

$$\begin{aligned}&(\breve{X}_{i,j}, \breve{Y}_{i,j})_{i\in[m], j\in T_{1-b}}\\ &\quad\longleftrightarrow \left(S, (Y_{i,j})_{i\in[m],j\in[n]}, (X_{i,j})_{i\in[m],j\in T_b}, (Z_{i,j})_{i\in S, j\in[n]}\right)\\ &\quad\quad\longleftrightarrow \left((X_{i,j})_{i\in[m],j\in T_{1-b}}, (Z_{i,j})_{i\in[m]\setminus S, j\in[n]}\right). \end{aligned} \tag{21}$$

P_3 accepts $1-b$ from P_2 only if event $E' = E'_1 \vee E'_2$ occurs, where

1. E'_1 is the event "Σ_{ZXY} fails w.r.t. X on input $(Z_{i,j}, X_{i,j}, \breve{Y}_{i,j})_{j\in T_{1-b}}$ in step 6 for some $i \in [m] \setminus S$".
2. E'_2 is the event "$(f^{\dagger}(\breve{X}_{i,j}), Z_{i,j}, f^{\ddagger}(X_{i,j}))_{j\in T_{1-b}}$ is a γ-typical sequence w.r.t. $P_{X^{\dagger}ZX^{\ddagger}}$ for at least $\frac{m}{4}$ instances of $i \in [m] \setminus S$".

$$\Pr[E'] = \Pr[E'_1 \vee E'_2] \le \Pr[E'_1] + \Pr[E'_2]. \tag{22}$$

We will show that these events occur with negligible probability. For $i \in [m]$, let

$$E'_{1,i} = (\Sigma_{ZXY} \text{ fails w.r.t. } X \text{ for } (Z_{i,j}, X_{i,j}, \breve{Y}_{i,j})_{j\in T_{1-b}}).$$

Then

$$\begin{aligned}\Pr[E'_1] &= \Pr\left[\bigvee_{i\in[m]\setminus S} E'_{1,i}\right]\\ &\le \sum_{\hat{S}\subset[m]:|\hat{S}|=\frac{m}{2}} \Pr[S=\hat{S}] \sum_{i\in[m]\setminus\hat{S}} \Pr[E'_{1,i}|S=\hat{S}].\end{aligned}$$

And for each $\hat{S} \subset [m]$ of size $m/2$ and $i \in [m] \setminus \hat{S}$,

$$\begin{aligned}&\Pr[E'_{1,i}|S=\hat{S}]\\ &\quad= \Pr\left[\Sigma_{ZXY} \text{ fails w.r.t. } X \text{ for } (Z_{i,j}, X_{i,j}, \breve{Y}_{i,j})_{j\in T_{1-b}} \middle| S=\hat{S}\right]\\ &\quad= 2^{-\Omega(|T_b|)} = 2^{-\Omega(n)},\end{aligned}$$

where the last step follows from Lemma 4(ii)(a) since, conditioned on $S = \hat{S}$,

(i) $(X_{i,j}, Y_{i,j}, Z_{i,j})_{i\in[m],j\in[n]}$ is distributed P_{XYZ} i.i.d. (since S is independent of $(X_{i,j}, Y_{i,j}, Z_{i,j})_{i\in[m],j\in[n]}$), and

(ii) by (21) and (i) above, for $i \in [m] \setminus \hat{S}$,

$$(\breve{Y}_{i,j})_{j\in T_{1-b}} \longleftrightarrow (Y_{i,j})_{j\in T_{1-b}} \longleftrightarrow (X_{i,j}, Z_{i,j})_{j\in T_{1-b}} \tag{23}$$

is a Markov chain.

Hence,

$$\Pr[E'_1] = m2^{-\Omega(n)}. \tag{24}$$

Finally, to bound $\Pr[E'_2]$, we need the following lemma:

Lemma 6. *Suppose the Markov chain $X^\dagger \longleftrightarrow Y \longleftrightarrow (Z, X^\ddagger)$ does not hold for the joint distribution P_{XYZ}. Let $(X_j, Y_j, Z_j)_{j\in[n]}$ be i.i.d. according to P_{XYZ}. For any $(\hat{X}_j)_{j\in[n]}$ satisfying the Markov chain*

$$(\hat{X}_j)_{j\in[n]} \longleftrightarrow (Y_j)_{j\in[n]} \longleftrightarrow (Z_j, X_j)_{j\in[n]},$$

and all sufficiently small $\gamma > 0$,

$$\Pr\left[\left(f^\dagger(\hat{X}_j), Z_j, f^\ddagger(X_j)\right)_{j\in[n]} \in \mathcal{T}_\gamma^n\left(P_{X^\dagger Z X^\ddagger}\right)\right] \leq 2^{-\Omega(n)}, \tag{25}$$

where $f^\dagger = \psi_{X\searrow Y}(|\mathcal{X}||\mathcal{Z}|)$ and $f^\ddagger = \psi_{X\searrow Z}(|\mathcal{X}||\mathcal{Y}|)$.

For $i \in [m]$, let

$$E'_{2,i} = ((f^\dagger(\breve{X}_{i,j}), Z_{i,j}, f^\ddagger(X_{i,j}))_{j\in T_{1-b}} \in \mathcal{T}_\gamma^{n/2}(P_{X^\dagger Z X^\ddagger})).$$

Clearly, $E'_2 \subset \bigvee_{i\in[m]\setminus S} E'_{2,i}$ (in fact, E'_2 requires at least $m/4$ instances of $E'_{2,i}$'s to occur for $i \in [m] \setminus S$). Hence,

$$\begin{aligned}\Pr[E'_2] &= \Pr\left[\bigvee_{i\in[m]\setminus S} E'_{2,i}\right] \\ &\leq \sum_{\hat{S}\subset[m]:|\hat{S}|=\frac{m}{2}} \Pr[S=\hat{S}] \sum_{i\in[m]\setminus\hat{S}} \Pr[E'_{2,i}|S=\hat{S}].\end{aligned}$$

As seen in the analysis of $\Pr[E'_1]$ above, conditioned on $S = \hat{S}$, the random variables $(X_{i,j}, Y_{i,j}, Z_{i,j})_{i\in[m],j\in[n]}$ are distributed P_{XYZ} i.i.d. Together with (21), this implies that, conditioned on $S = \hat{S}$, for all $i \in [m] \setminus \hat{S}$,

$$(\breve{Y}_{i,j})_{j\in T_{1-b}} \longleftrightarrow (Y_{i,j})_{j\in T_{1-b}} \longleftrightarrow (X_{i,j}, Z_{i,j})_{j\in T_{1-b}} \tag{26}$$

is a Markov chain. Further, by the hypothesis of the theorem, P_{XYZ} is such that $X^\dagger \longleftrightarrow Y \longleftrightarrow (Z, X^\ddagger)$ is not a Markov chain. Hence, for sufficiently small $\gamma > 0$, by Lemma 6, $\Pr[E'_{2,i}|S = \hat{S}] \leq 2^{-\Omega(n)}$ for all $i \in [m] \setminus \hat{S}$. Thus, $\Pr[E'_2] = m2^{-\Omega(n)}$ which together with (22) and (24) gives $\Pr[E'] = m2^{-\Omega(n)}$. The proof of security against P_2 follows.

At different points in the proof we made the following assumptions about the parameters $\gamma > 0, \delta > 0$: the parameter $\gamma > 0$ should be sufficiently small as required by Lemma 6 in the proof of security against P_2, and, for a given $\gamma > 0$, the parameter $\delta > 0$ should be sufficiently small as required by Lemma 5 in the proof of security against P_1. Clearly, we may simultaneously choose these parameters to satisfy these assumptions. Further, we set $m = n$ so that the number of samples of the correlation used is $N = nm = n^2$ and the security parameter, as calculated above, is $\epsilon = 2^{-\Omega(n)} = 2^{-\Omega(\sqrt{N})}$, i.e., $N = O(\log^2(\frac{1}{\epsilon}))$ as desired.

3.2 Altering the Transfer Path of a Pseudo-Signature Protocol

Theorem 6. *A pseudo-signature protocol with transfer path $P_1 \to P_3 \to P_2$ implies the existence of a pseudo-signature protocol with transfer path $P_1 \to P_2 \to P_3$.*

Proof. Let Π be an ε-secure pseudo-signature protocol for the transfer path $P_1 \to P_3 \to P_2$. We build an η-secure pseudo-signature protocol with transfer path $P_1 \to P_2 \to P_3$, where $\eta = O\left(\varepsilon \log\left(\frac{1}{\varepsilon}\right)\right)$. Fix a number $n = \Theta\left(\log\left(\frac{1}{\varepsilon}\right)\right)$. This protocol makes n independent invocations Π_i, $i \in [n]$ of the given protocol.

Setup phase *(Establishing a new correlation).*

1. P_1 samples uniformly random bits $U_1, \ldots, U_n$. For $i \in [n]$, P_1 signs U_i and sends to P_3 using the *signing phase* of Π_i.
2. If P_3 rejects any of these n messages at the end of the respective signature phases, it aborts the *setup phase* after informing P_2.
3. P_2 picks $S_0 \subset [n/2]$, $S_1 \subset [n] \backslash [n/2]$ with $|S_0| = |S_1| = n/4$ uniformly at random and sends $S_0 \cup S_1$ to P_3.
4. If P_3 has not aborted the *setup phase* in step 2, for each $i \in S_0 \cup S_1$, P_3 sends $\tilde{U}_i = U_i$ to P_2 using the *transfer phase* of Π_i.
5. If for any $i \in S_0 \cup S_1$, P_2 rejects $\tilde{U}_i$ at the end of *transfer phase* of Π_i, then P_2 flags P_3 as corrupt.

Signing phase $P_1 \to P_2$.

6. To send message $b \in \{0, 1\}$, P_1 sends b and $(\hat{U}_i)_{i \in T_b} = (U_i)_{i \in T_b}$ to P_2 where $T_b = \{i : \frac{bn}{2} + 1 \leq i \leq \frac{(b+1)n}{2}\}$.
7. If P_2 flagged P_3 as corrupt in step 5, or P_2 was informed by P_3 in step 2 that it is aborting the *setup phase*, then P_2 accepts b. Else, P_2 accepts if $\hat{U}_i = \tilde{U}_i$ for each $i \in S_b$, and rejects otherwise.

Transfer phase $P_2 \to P_3$.

8. To transfer an accepted b, P_2 sends $\left(\hat{b}, (\breve{U}_i)_{i \in T_{\hat{b}}}\right) = \left(b, (\hat{U}_i)_{i \in T_b}\right)$ to P_3.
9. P_3 accepts $\hat{b}$ if it aborted the setup phase in step 2. Else, if $\breve{U}_i = U_i$ for at least $n/6$ distinct $i \in T_{\hat{b}} \setminus S_{\hat{b}}$, P_3 accepts $\hat{b}$, and rejects otherwise.

Security against P_1 (Transferability). We will show that if P_2 accepts b in the *signing phase*, then P_3 rejects b in the *transfer phase* with a negligible probability. Examining steps 7 and 9, this event happens only if (i) P_2 flagged honest P_3 as corrupt in step 5 (in this case P_2 accepts any signature that P_1 sends in the *signing phase*), or (ii) $(U_i)_{i \in T_{\hat{b}}}$ and $(\hat{U}_i)_{i \in T_b}$ sent by P_1 in steps 1 and 6, respectively, are such that $\breve{U}_i = U_i$ for all $i \in S_b$ and $\hat{U}_i \neq U_i$ for more than $n/4 - n/6 = n/12$ distinct $i \in T_b \setminus S_b$. By ε-security of Π, if P_3 accepts a message in the signing phase of Π, then P_2 rejects it in the transfer phase with probability ε. Hence, by a union bound, (i) occurs with at most $n\varepsilon/2$ probability. Since S_b is chosen uniformly at random independent of $(U_i, \hat{U}_i)_{i \in T_b}$ (as S_b is unknown to P_1), by Chernoff's bound, (ii) occurs with probability $2^{-\Omega(n)}$.

Security against P_2 (Unforgeability). Suppose P_1's message is b, but in the *transfer phase*, P_2 sends $(1-b, (\breve{U}_i)_{i\in T_{1-b}})$ to P_3. Examining step 9, P_3 accepts $1-b$ only if (i) P_3 aborted the *setup phase* in step 2, or (ii) $\breve{U}_i = U_i$ for at least $n/6$ distinct $i \in T_{1-b} \setminus S_{1-b}$. By ε-security of Π, if P_1 is honest, then P_3 rejects the message in the signing phase with probability ε. Hence, by a union bound, (i) occurs with at most $n\varepsilon/2$ probability. Each U_i, $i \in T_{1-b} \setminus S_{1-b}$ is chosen uniformly and independently from $\{0,1\}$ (unknown to P_2), hence $\Pr[\breve{U}_i = U_i] = 1/2$ for $i \in T_{1-b} \setminus S_{1-b}$. Hence, by Chernoff's bound, (ii) occurs with probability $2^{-\Omega(n)}$.

Security against P_3 (Correctness). This amounts to showing that P_2 rejects the message from P_1 in the signing phase with a negligible probability. Examining step 7, this occurs only if P_2 has not flagged P_3 as corrupt in step 5, P_3 did not report abort in step 2, and $\hat{U}_i \neq \tilde{U}_i$ for some $i \in S_b$. Noting that $\hat{U}_i = U_i$ for all $i \in [n]$, this occurs only if, for some $i \in S_b$, P_2 accepts $\tilde{U}_i = 1 - U_i$ at the end of the transfer phase of Π_i when P_1's input is U_i. By ε-security of Π, for any $i \in [n]$, this occurs with probability ε. Hence, we may bound the probability of this event (over any arbitrary choice of S_b) by $n\varepsilon/2$.
For $n = \Theta\left(\log \frac{1}{\varepsilon}\right)$, these error probabilities compound to $O\left(\varepsilon \log\left(\frac{1}{\varepsilon}\right)\right)$. Hence, the above protocol is η-secure.

4 Impossibility

Theorem 7. *Let (X_1, Y_1, Z_1), (X_2, Y_2, Z_2), ..., (X_n, Y_n, Z_n) be independent and identically distributed (i.i.d.) triples with distribution P_{XYZ}. Suppose parties P_1, P_2, P_3 have access to correlations $(X_i)_{i\in[n]}, (Y_i)_{i\in[n]}$, $(Z_i)_{i\in[n]}$, respectively, and are connected pairwise by secure channels.*
For any n, and $\epsilon < 1/3$, there is no ϵ-secure broadcast protocol for the three parties with sender P_1 if the following Markov chain holds:[10]

$$X^{\dagger} \longleftrightarrow Y \longleftrightarrow Z \longleftrightarrow X^{\ddagger}. \tag{27}$$

We prove Theorem 7 in two steps. We first generalize the technique of Fischer, Lynch, and Merritt [13] to our setting with correlations. As in [13], we consider a new system with copies of the parties (in fact, only making two copies of party P_1 suffices) and the connections rewired (see Figure 1). The key step is in identifying a judiciously chosen correlation ($Q_{\underline{X}YZ\bar{X}}$ in the lemma below) to feed the parties in the new network. Lemma 7 below gives the conditions on this correlation $Q_{\underline{X}YZ\bar{X}}$ under which an impossibility can be shown. We then establish Theorem 7 by showing that such a $Q_{\underline{X}YZ\bar{X}}$ exists when (27) holds.

Lemma 7. *Consider the setup of Theorem 7. For any n, $\epsilon < 1/3$, there is no ϵ-secure broadcast protocol for the three parties with sender P_1 if there is a distribution $Q_{\underline{X}YZ\bar{X}}$ such that $Q_{\underline{X}Y} = P_{XY}$, $Q_{YZ} = P_{YZ}$, $Q_{Z\bar{X}} = P_{ZX}$, and*
(i) *$\exists\, Q_{\widetilde{Z}|\underline{X}YZ\bar{X}}$ s.t. $Q_{\widetilde{Z}|\underline{X}Y} = P_{Z|XY}$ and $(\underline{X}, Y) \longleftrightarrow \widetilde{Z} \longleftrightarrow (Z, \bar{X})$,*

[10] We write "$\mathrm{T} \longleftrightarrow \mathrm{U} \longleftrightarrow \mathrm{V} \longleftrightarrow \mathrm{W}$" to mean $P_{TUVW} = P_T P_{U|T} P_{V|U} P_{W|V}$.

(ii) $\exists\, Q_{\widetilde{Y}|\underline{X}YZ\bar{X}}$ *s.t.* $Q_{\widetilde{Y}|Z\bar{X}} = P_{Y|ZX}$ *and* $(Z, \bar{X}) \longleftrightarrow \widetilde{Y} \longleftrightarrow (\underline{X}, Y)$,
(iii) $\exists\, Q_{\widetilde{X}|\underline{X}YZ\bar{X}}$ *s.t.* $Q_{\widetilde{X}|YZ} = P_{X|YZ}$ *and* $(Y, Z) \longleftrightarrow \widetilde{X} \longleftrightarrow (\underline{X}, \bar{X})$.

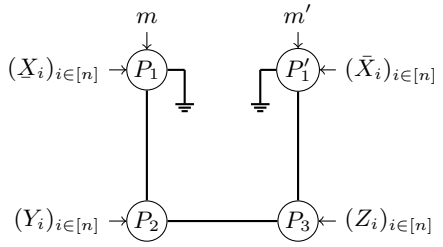

Fig. 1: A wiring diagram. Parties P_1, P_2, P_3 and P_1' observe correlations $(\underline{X}_i)_{i\in[n]}$, $(Y_i)_{i\in[n]}$, $(Z_i)_{i\in[n]}$, and $(\bar{X}_i)_{i\in[n]}$, respectively, i.i.d. according to $Q_{\underline{X}YZ\bar{X}}$. Party P_1 with input m, and P_1' with input $m' \neq m$ are identical copies of the sender. All parties run the protocol honestly.

Proof (Lemma 7). Suppose there is a (for now, a perfectly secure) broadcast protocol with sender P_1 . Consider the wiring diagram[11] in Figure 1 where the correlations $(\underline{X}_i)_{i\in[n]}, (Y_i)_{i\in[n]}, (Z_i)_{i\in[n]}, (\bar{X}_i)_{i\in[n]}$ of the parties P_1, P_2, P_3, P_1', respectively, are i.i.d. according to $Q_{\underline{X}YZ\bar{X}}$. Note that P_1 and P_1' are identical copies of the sender with the only difference being the correlated observations they use ($(\underline{X}_i)_{i\in[n]}$ for P_1 and $(\bar{X}_i)_{i\in[n]}$ for P_1') and their messages (m for P_1 and $m' \neq m$ for P_1').

- P_1 is connected to P_2, but it is disconnected from P_3. Its messages to P_3 are lost and it receives no messages from P_3.
- P_2 is connected to P_1 and P_3.
- P_3 is connected to P_2 and P_1' (instead of P_1).
- P_1' is connected to P_3 and disconnected from P_2.

Note that all parties here are honest. We will give three different interpretations of the new system in the diagram as instantiations of the original system (where the correlations are P_{XYZ} i.i.d.). In each interpretation, two of the parties are honest and the third party, who is dishonest, simulates the remaining two nodes in the new system. This will lead us to a contradiction establishing the impossibility of broadcast.

First interpretation: malicious P_3. Since $Q_{\underline{X}Y} = P_{XY}$, the joint distribution of the correlated observations $(\underline{X}_i)_{i\in[n]}$ and $(Y_i)_{i\in[n]}$ of P_1 and P_2 are as in the original system. We will argue that the joint view of P_1 and P_2 in the new system is identical to that in the original system where P_1 (with input m) and P_2 are honest and P_3 is corrupt as follows: corrupt P_3 in the original system simulates P_3 and P_1' of the new system, i.e., the corrupt P_3 ignores messages from P_1, does not send any messages to P_1, and simulates P_3 and P_1' by sending/receiving

[11] The wiring diagram is similar to the one described in [19, proof of Theorem 7], but the rest of the argument (including the identification of a correlation $Q_{\underline{X}YZ\bar{X}}$ to establish an impossibility) is different.

messages on the communication link with P_2. In order to simulate P_3 and P_1' of the new system, the corrupt P_3 must be able to generate the observations of these nodes (i.e., $(Z_i, \bar{X}_i)_{i\in[n]}$) in such a way that they are jointly distributed with $(\underline{X}_i, Y_i)_{i\in[n]}$ of P_1 and P_2 i.i.d. according to the distribution $Q_{\underline{X}YZ\bar{X}}$. For this, the corrupt P_3 may make use of the Z-observations it receives which are jointly distributed with the observations $(\underline{X}_i, Y_i)_{i\in[n]}$ of P_1 and P_2 i.i.d. according to P_{XYZ}. Since (by the lemma's hypothesis (i)) $Q_{\underline{X}Y}Q_{\widetilde{Z}|\underline{X}Y} = P_{XY}P_{Z|XY} = P_{XYZ}$, we may treat the observations received by P_3 as $(\widetilde{Z}_i)_{i\in[n]}$. Then, by virtue of the Markov chain $(\underline{X}, Y) \longleftrightarrow \widetilde{Z} \longleftrightarrow (Z, \bar{X})$ (of lemma's hypothesis (i)), the corrupt P_3 may sample $(Z_i, \bar{X}_i)_{i\in[n]}$ to simulate P_3 and P_1'. Specifically, the conditional independence of $(\bar{X}, Z)$ and $(\underline{X}, Y)$ conditioned on $\widetilde{Z}$ means that the corrupt P_3 may locally generate the samples of $\bar{X}$ and Z (which it needs to simulate P_1' and P_3) using only the samples of $\widetilde{Z}$ it observes (and without knowing the samples of $\underline{X}$ and Y of P_1 and P_2 which it does not have access to). Thus, the joint view of P_1 and P_2 in the new system is identical to that in the original system where P_1 (with input m) and P_2 are honest and P_3 is corrupt. Therefore, P_2 in the new system must output m.

Second interpretation: malicious P_2. Arguing similarly using $Q_{Z\bar{X}} = P_{ZX}$ and hypothesis (ii) of the lemma, we may conclude that P_3 in the new system must output m'.

Third interpretation: malicious P_1. Similarly, using $Q_{YZ} = P_{YZ}$ and hypothesis (iii), we may conclude that the joint view of P_2 and P_3 in the new system is identical to that in the original system where P_2 and P_3 are honest and P_1 is corrupt. Hence the outputs of P_2 and P_3 must agree, a contradiction.

The above discussion assumed a perfectly secure broadcast. For an ϵ-secure broadcast, the conclusions in each interpretation are guaranteed to hold with probability $1-\epsilon$. So, we arrive at contradiction if $\epsilon < 1/3$.

Theorem 7 now follows from the lemma below which is proved in [30].

Lemma 8. *If P_{XYZ} is such that the Markov chain of (27) holds, the distribution $Q_{\underline{X}YZ\bar{X}}$ defined below satisfies $Q_{\underline{X}Y} = P_{XY}$, $Q_{YZ} = P_{YZ}$, $Q_{Z\bar{X}} = P_{ZX}$, and conditions (i)-(iii) in the hypothesis of Lemma 7.*

$$Q_{\underline{X}YZ\bar{X}}(\underline{x}, y, z, \bar{x}) \stackrel{\text{def}}{=} P_{YZ}(y,z)P_{X|Y}(\underline{x}|y)P_{X|Z}(\bar{x}|z), \quad \forall\, \underline{x}, y, z, \bar{x}. \tag{28}$$

5 Characterizations

In Theorem 5, we have shown that pseudo-signature with transfer path $P_1 \to P_2 \to P_3$ is feasible from correlation (X, Y, Z) if the Markov chain $X^\dagger \longleftrightarrow Y \longleftrightarrow (Z, X^\ddagger)$ does not hold; by symmetry, we can show that pseudo-signature with transfer path $P_1 \to P_3 \to P_2$ is feasible from correlation (X, Y, Z) if the Markov chain $X^\ddagger \longleftrightarrow Z \longleftrightarrow (Y, X^\dagger)$ does not hold. Furthermore, in Theorem 6, we have shown that pseudo-signature with transfer path $P_1 \to P_2 \to P_3$ is feasible if pseudo-signature with transfer path $P_1 \to P_3 \to P_2$ is, and vice versa. Thus, we can conclude

that pseudo-signatures with both transfer paths $P_1 \to P_2 \to P_3$ and $P_1 \to P_3 \to P_2$ are feasible if at least one of the following Markov chains do not hold.

$$X^\dagger \longleftrightarrow Y \longleftrightarrow (Z, X^\ddagger) \tag{29}$$

$$X^\ddagger \longleftrightarrow Z \longleftrightarrow (Y, X^\dagger) \tag{30}$$

On the other hand, in Theorem 7, we have shown that broadcast with sender P_1 is infeasible if the following Markov chain holds.

$$X^\dagger \longleftrightarrow Y \longleftrightarrow Z \longleftrightarrow X^\ddagger. \tag{31}$$

In fact, the Markov chain condition (31) and the pair of Markov chain conditions (29) and (30) are equivalent: clearly (31) implies (29) and (30); to verify the opposite implication, note that (29) implies that

$$P_{X^\dagger Y Z X^\ddagger} = P_{X^\dagger} P_{Y|X^\dagger} P_{ZX^\ddagger|Y} = P_{X^\dagger} P_{Y|X^\dagger} P_{Z|Y} P_{X^\ddagger|ZY}.$$

Now, (30) implies that $X^\ddagger \longleftrightarrow Z \longleftrightarrow Y$, i.e., $P_{X^\ddagger|ZY} = P_{X^\ddagger|Z}$. Hence, (29) and (30) together imply that $P_{X^\dagger Y Z X^\ddagger} = P_{X^\dagger} P_{Y|X^\dagger} P_{Z|Y} P_{X^\ddagger|Z}$, which is (31). Using this observation, we can provide a complete characterization of feasibility of pseudo-signature and broadcast. Even though the conditions on the correlation are the same for pseudo-signature and broadcast, we state them separately to clarify the logical difference of the derivations.

Theorem 8 (Characterization of pseudo-signature). *Pseudo-signature with transfer path $P_1 \to P_2 \to P_3$ is feasible from correlation (X, Y, Z) if and only if the Markov chain (31) does not hold. The same statement holds for pseudo-signature with transfer path $P_1 \to P_3 \to P_2$.*

Proof. The "if" part follows from Theorem 5 and Theorem 6. On the other hand, the "only if" part follows from the fact that pseudo-signature with either transfer implies broadcast with sender P_1 and Theorem 7.

Theorem 9 (Characterization of broadcast). *Broadcast with sender P_1 is feasible from correlation (X, Y, Z) if and only if the Markov chain (31) does not hold.*

Proof. The "if" part follows from Theorem 5 (invoked for either transfer path with signer P_1) and the fact that the pseudo-signature with signer P_1 implies broadcast with sender P_1. On the other hand, the "only if" part follows from Theorem 7.

6 Characterizations for Pseudo-Signatures with Limited Connectivity

Notice that the construction in Section 3.1 only used the unidirectional links $P_1 \Rightarrow P_2$, $P_1 \Rightarrow P_3$, and the bidirectional link $P_2 \Leftrightarrow P_3$, while the impossibility in Section 4 (via the fact that pseudo-signature with transfer path $P_1 \to P_2 \to P_3$ implies broadcast with sender P_1) applies

for pseudo-signature protocols which may use all pairwise links in either direction. In this section we consider networks with more limited connectivity than what the construction in Section 3.1 demands and give characterizations. Note that a similar question is uninteresting for broadcast with sender P_1 as it is easy to argue that broadcast is impossible without all the links demanded by our construction present.
For pseudo-signature protocols with transfer path $P_1 \to P_2 \to P_3$, since the links $P_1 \Rightarrow P_2$ and $P_2 \Rightarrow P_3$ are needed, we consider cases where one or both of the links $P_1 \Rightarrow P_3$ and $P_3 \Rightarrow P_2$ that our construction additionally needs are absent.

Pseudo-signatures with connectivity $P_1 \Leftrightarrow P_2 \Leftrightarrow P_3$. This network does not have the $P_1 \Rightarrow P_3$ link our construction needs. This prevents P_3 from being upgraded. However, the partial upgrade of P_2 may still be implemented. Straightforward modifications of the construction (to only use $P_1 \Rightarrow P_2$ and $P_2 \Leftrightarrow P_3$ links) show that a pseudo-signature protocol with transfer path $P_1 \to P_2 \to P_3$ is feasible as long as $X^\dagger \longleftrightarrow Y \longleftrightarrow Z$ does not hold. As we show in [30, Appendix E.1], this turns out to be the characterizing condition.

Theorem 10. *Pseudo-signature with transfer path $P_1 \to P_2 \to P_3$ is feasible from correlation (X, Y, Z) when secure links $P_1 \Leftrightarrow P_2$ and $P_2 \Leftrightarrow P_3$ are available if and only if the following Markov chain does not hold*

$$X^\dagger \longleftrightarrow Y \longleftrightarrow Z. \tag{32}$$

Pseudo-signatures with no $P_3 \Rightarrow P_2$ link. Here the link between P_2 to P_3 is unidirectional. This prevents P_2 from being upgraded, but P_3 may still be upgraded. With straightforward changes to use only $P_1 \Rightarrow P_2$, $P_1 \Rightarrow P_3$, and $P_2 \Rightarrow P_3$ links, our construction gives a pseudo-signature protocol if $(X \setminus Y) \longleftrightarrow Y \longleftrightarrow (Z, X^\ddagger)$ does not hold. This turns out to be the characterizing condition (see [30, Appendix E.2]).

Theorem 11. *Pseudo-signature with transfer path $P_1 \to P_2 \to P_3$ is feasible from correlation (X, Y, Z) when secure links $P_1 \Leftrightarrow P_2$, $P_1 \Leftrightarrow P_3$, and $P_2 \Rightarrow P_3$ are available if and only if the following Markov chain does not hold*

$$(X \setminus Y) \longleftrightarrow Y \longleftrightarrow (Z, X^\ddagger). \tag{33}$$

Pseudo-signatures with connectivity $P_1 \Leftrightarrow P_2 \Rightarrow P_3$. In this third case both $P_1 \Rightarrow P_3$ and $P_3 \Rightarrow P_2$ links are absent. This prevents both P_2 and P_3 from being upgraded. The pseudo-signature protocol in [19] (or by altering our construction) which uses only the $P_1 \Rightarrow P_2$ and $P_2 \Rightarrow P_3$ links is secure as long as $X \setminus Y \longleftrightarrow Y \longleftrightarrow Z$ is not true. This is also the characterizing condition for this case (see [30, Appendix E.3]).

Theorem 12. *Pseudo-signature with transfer path $P_1 \to P_2 \to P_3$ is feasible from correlation (X, Y, Z) when secure links $P_1 \Leftrightarrow P_2$ and $P_2 \Rightarrow P_3$ are available if and only if the following Markov chain does not hold*

$$X \setminus Y \longleftrightarrow Y \longleftrightarrow Z. \tag{34}$$

References

1. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography–part I: Secret sharing. IEEE Trans. Inform. Theory **39**(4), 1121–1132 (July 1993). https://doi.org/10.1109/18.243431
2. Ahlswede, R., Csiszár, I.: On oblivious transfer capacity. Information Theory, Combinatorics, and Search Theory pp. 145–166 (2013). https://doi.org/10.1007/978-3-642-36899-8_6
3. Beaver, D.: Multiparty protocols tolerating half faulty processors. In: Brassard, G. (ed.) CRYPTO'89. LNCS, vol. 435, pp. 560–572. Springer, Heidelberg (Aug 1990). https://doi.org/10.1007/0-387-34805-0_49
4. Chaum, D., Roijakkers, S.: Unconditionally secure digital signatures. In: Menezes, A.J., Vanstone, S.A. (eds.) CRYPTO'90. LNCS, vol. 537, pp. 206–214. Springer, Heidelberg (Aug 1991). https://doi.org/10.1007/3-540-38424-3_15
5. Chen, J., Micali, S.: Algorand: A secure and efficient distributed ledger. Theoretical Computer Science **777**, 155–183 (2019). https://doi.org/10.1016/j.tcs.2019.02.001
6. Considine, J., Fitzi, M., Franklin, M., Levin, L.A., Maurer, U., Metcalf, D.: Byzantine agreement given partial broadcast. Journal of Cryptology **18**, 191–217 (2005). https://doi.org/10.1007/s00145-005-0308-x
7. Cramer, R., Damgård, I., Nielsen, J.: Secure Multiparty Computation and Secret Sharing. Cambridge University Press (2015). https://doi.org/10.1017/CBO9781107337756
8. Crépeau, C.: Equivalence between two flavours of oblivious transfers. In: Pomerance, C. (ed.) CRYPTO'87. LNCS, vol. 293, pp. 350–354. Springer, Heidelberg (Aug 1988). https://doi.org/10.1007/3-540-48184-2_30
9. Crépeau, C.: Efficient cryptographic protocols based on noisy channels. In: Fumy, W. (ed.) EUROCRYPT'97. LNCS, vol. 1233, pp. 306–317. Springer, Heidelberg (May 1997). https://doi.org/10.1007/3-540-69053-0_21
10. Crépeau, C., Kilian, J.: Weakening security assumptions and oblivious transfer (abstract). In: Goldwasser, S. (ed.) CRYPTO'88. LNCS, vol. 403, pp. 2–7. Springer, Heidelberg (Aug 1990). https://doi.org/10.1007/0-387-34799-2_1
11. Csiszár, I., Körner, J.: Information Theory: Coding Theorems for Discrete Memoryless Systems. Cambridge University Press, 2 edn. (2011). https://doi.org/10.1017/CBO9780511921889
12. Dowsley, R., Nascimento, A.C.: On the oblivious transfer capacity of generalized erasure channels against malicious adversaries: The case of low erasure probability. IEEE Trans. Inform. Theory **63**(10), 6819–6826 (October 2017). https://doi.org/10.1109/TIT.2017.2735423
13. Fischer, M.J., Lynch, N.A., Merritt, M.: Easy impossibility proofs for distributed consensus problems. Distributed Computing **1**(1), 26–39 (1986). https://doi.org/10.1007/BF01843568

14. Fitzi, M., Gisin, N., Maurer, U.: Quantum solution to Byzantine agreement problem. Physical Review Letter **87**(21), 217901 (November 2001). https://doi.org/10.1103/PhysRevLett.87.217901
15. Fitzi, M., Garay, J.A., Maurer, U.M., Ostrovsky, R.: Minimal complete primitives for secure multi-party computation. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 80–100. Springer, Heidelberg (Aug 2001). https://doi.org/10.1007/3-540-44647-8_5
16. Fitzi, M., Gisin, N., Maurer, U.M., von Rotz, O.: Unconditional byzantine agreement and multi-party computation secure against dishonest minorities from scratch. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 482–501. Springer, Heidelberg (Apr / May 2002). https://doi.org/10.1007/3-540-46035-7_32
17. Fitzi, M., Hirt, M., Holenstein, T., Wullschleger, J.: Two-threshold broadcast and detectable multi-party computation. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 51–67. Springer, Heidelberg (May 2003). https://doi.org/10.1007/3-540-39200-9_4
18. Fitzi, M., Maurer, U.M.: From partial consistency to global broadcast. In: 32nd ACM STOC. pp. 494–503. ACM Press (May 2000). https://doi.org/10.1145/335305.335363
19. Fitzi, M., Wolf, S., Wullschleger, J.: Pseudo-signatures, broadcast, and multi-party computation from correlated randomness. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 562–578. Springer, Heidelberg (Aug 2004). https://doi.org/10.1007/978-3-540-28628-8_34
20. Gohari, A.A., Anantharam, V.: Information-theoretic key agreement of multiple terminals: Part i. IEEE Trans. Inform. Theory **56**(8), 3973 – 3996 (August 2010). https://doi.org/10.1109/TIT.2010.2050832
21. Hanaoka, G., Shikata, J., Zheng, Y., Imai, H.: Unconditionally secure digital signature schemes admitting transferability. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 130–142. Springer, Heidelberg (Dec 2000). https://doi.org/10.1007/3-540-44448-3_11
22. Hanaoka, G., Shikata, J., Zheng, Y., Imai, H.: Efficient and unconditionally secure digital signatures and a security analysis of a multireceiver authentication code. In: Naccache, D., Paillier, P. (eds.) PKC 2002. LNCS, vol. 2274, pp. 64–79. Springer, Heidelberg (Feb 2002). https://doi.org/10.1007/3-540-45664-3_5
23. Khurana, D., Maji, H.K., Sahai, A.: Secure computation from elastic noisy channels. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part II. LNCS, vol. 9666, pp. 184–212. Springer, Heidelberg (May 2016). https://doi.org/10.1007/978-3-662-49896-5_7
24. Lamport, L., Shostak, R., Pease, M.: The Byzantine general problem. ACM Transactions on Programming Languages and Systems **4**(3), 382–401 (July 1982). https://doi.org/10.1145/357172.357176
25. Maurer, U.: Secret key agreement by public discussion from common information. IEEE Trans. Inform. Theory **39**(3), 733–742 (May 1993). https://doi.org/10.1109/18.256484

26. Maurer, U., Wolf, S.: Secret-key agreement over unauthenticated public channels—part I: Definitions and a completeness result. IEEE Trans. Inform. Theory **49**(4), 822–831 (April 2003). https://doi.org/10.1109/TIT.2003.809563
27. Maurer, U., Wolf, S.: Secret-key agreement over unauthenticated public channels—part II: Privacy amplification. IEEE Trans. Inform. Theory **49**(4), 839–851 (April 2003). https://doi.org/10.1109/TIT.2003.809559
28. Maurer, U., Wolf, S.: Secret-key agreement over unauthenticated public channels—part II: The simulatability condition. IEEE Trans. Inform. Theory **49**(4), 832–838 (April 2003). https://doi.org/10.1109/TIT.2003.809560
29. Mitzenmacher, M., Upfal, E.: Probability and Computing: Randomized Algorithms and Probabilistic Analysis. Cambridge University Press (2005). https://doi.org/10.1017/CBO9780511813603
30. Narayanan, V., Prabhakaran, V.M., Sangwan, N., Watanabe, S.: Complete characterization of broadcast and pseudo-signatures from correlations. Cryptology ePrint Archive, Paper 2023/233 (2023), https://eprint.iacr.org/2023/233
31. Nascimento, A.C.A., Winter, A.: On the oblivious-transfer capacity of noisy resources. IEEE Trans. Inform. Theory **54**(6), 2572–2581 (2008). https://doi.org/10.1109/TIT.2008.921856
32. Pfitzmann, B., Waidner, M.: Information-theoretic pseudosignatures and Byzantine agreement for $t \geq n/3$. IBM Research Technical Report **RZ 2882 (#90830)** (1996)
33. Prabhakaran, V., Prabhakaran, M.: Assisted common information with an application to secure two-party sampling. IEEE Trans. Inform. Theory **60**(6), 3413–3434 (June 2014). https://doi.org/10.1109/TIT.2014.2316011
34. Rabin, T., Ben-Or, M.: Verifiable secret sharing and multiparty protocols with honest majority (extended abstract). In: 21st ACM STOC. pp. 73–85. ACM Press (May 1989). https://doi.org/10.1145/73007.73014
35. Renner, R., Wolf, S.: New bounds in secret-key agreement: The gap between formation and secrecy extraction. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 562–577. Springer, Heidelberg (May 2003). https://doi.org/10.1007/3-540-39200-9_35
36. Renner, R., Wolf, S.: Unconditional authenticity and privacy from an arbitrarily weak secret. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 78–95. Springer, Heidelberg (Aug 2003). https://doi.org/10.1007/978-3-540-45146-4_5
37. Tyagi, H., Watanabe, S.: Converses for secret key agreement and secure computing. IEEE Trans. Inform. Theory **61**, 4809–4827 (2015). https://doi.org/10.1109/TIT.2015.2457926
38. Tyagi, H., Watanabe, S.: Information-theoretic Cryptography. Cambridge University Press (2023)
39. Wolf, S., Wullschleger, J.: New monotones and lower bounds in unconditional two-party computation. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 467–477. Springer, Heidelberg (Aug 2005). https://doi.org/10.1007/11535218_28