Pseudo-Signatures, Broadcast, and Multi-Party Computation from Correlated Randomness

Matthias Fitzi[1] Stefan Wolf[2] Jürg Wullschleger[2]

[1] Department of Computer Science
University of California, Davis, U.S.A.
fitzi@cs.ucdavis.edu
[2] Département d'Informatique et R.O.
Université de Montréal, Canada.
{wolf,wullschj}@iro.umontreal.ca

Abstract. Unconditionally secure multi-party computations in general, and broadcast in particular, are impossible if any third of the players can be actively corrupted and if no additional information-theoretic primitive is given. In this paper, we relativize this pessimistic result by showing that such a primitive can be as simple as noisy communication channels between the players or weakly correlated pieces of information. We consider the scenario where three players have access to random variables X, Y, and Z, respectively, and give the exact condition on the joint distribution P_{XYZ} under which unconditional broadcast is possible. More precisely, we show that this condition characterizes the possibility of realizing so-called pseudo-signatures between the players. As a consequence of our results, we can give conditions for the possibility of achieving unconditional broadcast between n players and any minority of cheaters and, hence, general multi-party computation under the same condition.

Key words. Unconditional security, pseudo-signatures, broadcast, multi-party computation, information theory.

1 Motivation and Preliminaries

1.1 Introduction

Digital signatures [11, 19] are a powerful tool not only in the context of digital contract signing, but also as a basic primitive for cryptographic protocols such as electronic voting or secure multi-party computation. Much less known are so-called *pseudo-signature schemes*, which guarantee *unconditional* security—in contrast to classical digital-signature schemes. The inherent price for their higher security, however, is the signatures' limited transferability: Whereas classical signatures can be arbitrarily transfered without losing conclusiveness, pseudo-signatures only remain secure for a fixed number λ—the *transferability*—of transfers among different parties. Since the necessary number of signature transfers in a protocol is typically bounded by the number of involved parties, pseudo-signatures are, nevertheless, useful and offer a provably higher security level than traditional signature schemes. For example, the authenticated broadcast protocol in [13] can be based on pseudo-signatures and then guarantees unconditional (instead of computational) security against any number of corrupted players [25].

A pseudo-signature scheme among a number of players can either be set up by a mutually trusted party, by a protocol among the players when given global broadcast channels, or—as we will show—by exploiting an information source that provides the players with certain correlated pieces of information—a similar model has been considered in [21] in the context of secret-key agreement.

In this paper, we consider the general case of an information source that provides a set of n players with pieces of information distributed according to some given joint probability distribution. For the case of three players, we completely characterize when such an information source allows for setting up a pseudo-signature scheme. This result can be used for deriving a complete characterization of when unconditionally secure three-party computation—or broadcast, in particular—is achievable in the presence of an actively corrupted player. Furthermore, we give, in the same model, a sufficient condition for the achievability of unconditionally secure multi-party computation for any number n of players secure against $t < n/2$ actively corrupted players.

1.2 Context and Previous Work

Pseudo-signature schemes (PSS). The first pseudo-signature-like scheme was given in form of an information-checking protocol among three players [26]. In contrast to real pseudo-signatures, however, the signer is required to commit to her input value already during the setup of the scheme.

The first PSS was introduced in [7] with the restriction to be secure only with respect to a correct signer. In [25], finally, a complete PSS was proposed for any transferability λ and any number of corrupted players.

Setting up a PSS. It was shown in [25] how to set up a PSS using global broadcast channels, where the *dining-cryptographers protocol* [5, 4] was used. Obtaining a PSS from a common random source was considered in [15, 16], but only with respect to three players and *one particular* probability distribution.

Broadcast. The *broadcast problem* was introduced in [20]. It was proven that, in the standard model with secure channels between all pairs of players, but without the use of a signature scheme, broadcast is achievable if and only if the number t of cheaters satisfies $t < n/3$. Furthermore, it was shown that when additionally a signature scheme is given among the n players, then computationally secure broadcast is achievable for any number of corrupted players. The first efficient such protocol was given in [12]. In [25], an efficient protocol was given with unconditional security based on a pseudo-signature scheme with transferability $t + 1$.

Multi-party computation (MPC). Broadcast—or the availability of signatures with sufficiently high transferability—is a limiting factor for general *multi-party computation* introduced in [27]. A complete solution with respect to computational security was given in [18]. In [2, 6], it was shown that in a model with only pairwise secure channels, MPC unconditionally secure against an active adversary is achievable if and only if $t < n/3$ players are corrupted. As shown in [1, 26], $t < n/2$ is achievable when global broadcast channels are additionally given—and this bound was shown tight. A protocol more efficient than those in [1, 26] was given in [10].

1.3 Our Results

We first consider a set of three players, connected in pairs by secure channels, where an additional information source provides the players with correlated pieces of information. We give a necessary and sufficient condition on the joint probability distribution of this side information for when a pseudo-signature scheme can be set up among the three players with a *designated* signer. Furthermore, we show that the tight condition for the achievability of broadcast or multi-party computation among three players unconditionally secure against one actively corrupted player is exactly the same as the one for a pseudo-signature scheme with respect to an *arbitrary.* The derived condition shows that pseudo-signature schemes and broadcast among three players are possible under much weaker conditions than previously known.

We further consider the general case of n players, connected in pairs by secure channels, where, again, an additional information source provides the players with side information. For this model, and under the assumption that an active adversary can corrupt up to $t < n/2$ players, we show that MPC is possible under much weaker conditions than previously known.

1.4 Model and Definitions

We consider a set $P = \{P_1, \ldots, P_n\}$ of n players that are connected by a complete, synchronous network of pairwise secure channels—in the presence of an active adversary who can select up to t players and corrupt them in an arbitrary way. Furthermore, we assume this adversary to be computationally unbounded. A player which does not get corrupted by the adversary is called *correct.*

Pseudo-Signatures. We follow the definition of pseudo-signature schemes as given in [25].

Definition 1. A *pseudo-signature scheme (PSS) with transferability* λ among the players $P_1, \ldots, P_n$, where P_1 is the signer, satisfies the following properties.

Correctness. If player P_1 is correct and signs a message, then a correct player P_i accepts this message from P_1 except with small probability.

Unforgeability. A correct player P_i rejects any message that has not been signed by P_1 except with small probability.

Transferability. A message signed by the correct player P_1 can be transfered λ times, e.g., via

$$P_1 \rightarrow P_{i_1} \rightarrow \cdots \rightarrow P_{i_{\lambda+1}} \ ,$$

such that we have for each $j \leq \lambda$ and correct players P_{i_j} and $P_{i_{j+1}}$ that if P_{i_j} accepts a message m, then $P_{i_{j+1}}$ accepts the same message except with small probability.

If the path $i_1, \ldots, i_{\lambda+1}$ can be arbitrary, we call the scheme a *PSS with arbitrary transfer paths*, if the transfer is restricted to a specific path $i_1, \ldots, i_{\lambda+1}$, we call it a *PSS with transfer path* $i_1, \ldots, i_{\lambda+1}$.

The choice $\lambda = 1$ will be sufficient in our case since any such PSS allows for broadcast for $t < n/2$ corrupted players [17].

Broadcast and Multi-Party Computation. *Broadcast* is the problem of having a (possibly corrupted) sender distribute a value to every player such that all correct players are guaranteed to receive the same value.

Definition 2. A protocol among players $P_1, \ldots, P_n$, where P_1 is the sender and holds input x_s, and where every player P_i computes an output y_i, achieves *broadcast* if it satisfies the following conditions.

Validity. If the sender P_1 is correct, then every correct player P_i computes the output $y_i = x_s$.

Consistency. All correct players P_i and P_j compute the same output value, i.e., $y_i = y_j$ holds.

Broadcast is a special case of the more general problem of *multi-party computation (MPC)*, where the players want to evaluate in a distributed way some given function of their inputs and hereby guarantee privacy of these inputs as well as correctness of the computed result. From a qualitative point of view, the security of multi-party computation is often broken down to the conditions *privacy*, *correctness*, *robustness*, and *fairness*. In [8], it was shown that all these conditions can only be satisfied simultaneously if $t < n/2$ holds—the case to which we restrict our considerations in this paper.

2 Dependent Parts and Simulation of Random Variables

In this section we introduce the notion of the dependent part of a random variable with respect to another, and a certain simulatability condition, defined for a triple of random variables. The *dependent part of X from Y* isolates the part of X that is dependent on Y. Note that we always assume that the joint distribution is known to all the players.

Definition 3. Let X and Y be two random variables, and let $f(x) = P_{Y|X=x}$. The *dependent part of* X *from* Y is defined as $X \searrow Y := f(X)$.

The random variable $X \searrow Y$ is a function of X and takes on the value of the conditional probability distribution $P_{Y|X=x}$.

Lemma 1. *For all* X *and* Y*, we have* $X \longleftrightarrow (X \searrow Y) \longleftrightarrow Y$*, i.e., the sequence* $X, X \searrow Y, Y$ *is a Markov chain*[3].

Proof. Let $K = f(X) = X \searrow Y$. For all $x \in \mathcal{X}$—the range of X—and $k = f(x)$, we have $P_{Y|X=x,K=k} = P_{Y|K=k}$, and, hence, $P_{Y|XK} = P_{Y|K}$.

We will now show that $K = X \searrow Y$ is the part of X that a player who knows Y can verify to be correct. Lemma 2 shows that every $\overline{K}$ a player knowing X can construct that has the same joint distribution with Y as the actual K must indeed be *identical* with K. Lemma 3 shows that from K, a random variable $\overline{X}$ can be constructed which has the same joint distribution with Y as X. Hence, K is the largest part of X that someone knowing Y can verify to be correct.

Lemma 2. *Let* X*,* K*,* $\overline{K}$*, and* Y *be random variables such that* $K = X \searrow Y$*,* $Y \longleftrightarrow X \longleftrightarrow \overline{K}$*, and* $P_{KY} = P_{\overline{K}Y}$ *hold. Then we have* $\overline{K} = K$*.*

Proof. We have $K = f(X)$, $P_{\overline{K}|XY} = P_{\overline{K}|X}$, $P_K = P_{\overline{K}}$, and $P_{Y|K} = P_{Y|\overline{K}}$. Let us have a look at a value k for which $P_{Y|K=k}$ cannot be expressed as a linear combination of $P_{Y|X=x_i}$ for $x_i \in \mathcal{X}$ with $f(x_i) \neq k$. (It is easy to see that such a k must exist.) Let S be the set of all x with $f(x) = k$. In order to achieve $P_{Y|\overline{K}=k} = P_{Y|K=k}$, no x' not in S can be mapped to k by $P_{\overline{K}|X}$. Since $P_{\overline{K}}(k) = P_K(k)$ holds, $P_{\overline{K}|X}$ must map all values from S to k.

We remove the elements of S from $\mathcal{X}$, repeat the same argument for the next k, and continue this process until $\mathcal{X}$ is empty. Hence, $P_{\overline{K}|X}$ maps all x to $f(x)$, and $\overline{K} = K$ holds. □

Lemma 3. *Let* X *and* Y *be random variables, and let* $K = X \searrow Y$*. There exists a channel* $P_{\overline{X}|K}$*—which is equal to* $P_{X|K}$*—such that* $P_{XY} = P_{\overline{X}Y}$ *holds, where* $P_{\overline{X}Y} = \sum_k P_{KY} P_{\overline{X}|K}$*.*

Proof. Using Lemma 1, we get $P_{\overline{X}Y} = \sum_k P_{KY} P_{\overline{X}|K} = \sum_k P_{KY} P_{X|K} = P_{XY}$. □

The *simulatability condition*, which allows for determining the possibility of secret-key agreement over unauthenticated channels, was defined in [22] and further analyzed in [24]. It defines whether given Z, it is possible to simulate X in such a way that someone who only knows Y cannot distinguish the simulation of X from the true X.

[3] A sequence of three random variables A, B, C forms a *Markov chain*, denoted by $A \longleftrightarrow B \longleftrightarrow C$, if $I(A; C|B) = 0$ holds or, equivalently, if we have $P_{C|AB}(c, a, b) = P_{C|B}(c, b)$ for all $(a, b, c) \in \mathcal{A} \times \mathcal{B} \times \mathcal{C}$.

Definition 4. Let X, Y, and Z be random variables. Then X is *simulatable by Z with respect to Y*, denoted by

$$\mathrm{sim}_Y(Z \to X),$$

if there exists a conditional distribution $P_{\overline{X}|Z}$ such that $P_{\overline{X}Y} = P_{XY}$ holds, where $P_{\overline{X}Y} = \sum_z P_{YZ} P_{\overline{X}|Z}$.

Lemma 4. *For all P_{XYZ}, we have $\mathrm{sim}_Y(Z \to X)$ if and only if*

$$\mathrm{sim}_Y(Z \to (X \searrow Y)) \ .$$

Proof. Let $K := X \searrow Y$. K is a function of X and can be simulated whenever the same holds for X. On the other hand, let $P_{\overline{K}|Z}$ be a channel that simulates K. It follows from Lemma 3 that there exists a channel $P_{\overline{X}|\overline{K}}$—which is equal to $P_{X|K}$— such that the channel $P_{\overline{X}|Z} := \sum P_{\overline{X}|\overline{K}} P_{\overline{K}|Z}$ simulates X. □

Lemma 5. *For all P_{XYZ}, we have $\mathrm{sim}_Z(Y \to [X,Y])$ if and only if $X \longleftrightarrow Y \longleftrightarrow Z$.*

Proof. Suppose first that we have $\mathrm{sim}_Z(Y \to [X,Y])$. There must exist a channel $P_{\hat{X}\hat{Y}|Y}$ such that $P_{\hat{X}\hat{Y}Z} = P_{XYZ}$ holds, where $P_{\hat{X}\hat{Y}Z} = \sum P_{YZ} P_{\hat{X}\hat{Y}|Y}$. Let $K := Y \searrow Z$ and $\hat{K} := \hat{Y} \searrow Z$. Because of $Z \longleftrightarrow Y \longleftrightarrow \hat{Y}$ and $P_{\hat{Y}Z} = P_{YZ}$, we have $Z \longleftrightarrow Y \longleftrightarrow \hat{K}$ and $P_{\hat{K}Z} = P_{KZ}$. It follows from Lemma 2 that $\hat{K} = K$ holds. From Lemma 1 follows that $P_{Y|KZ} = P_{Y|K}$. We also have $P_{\hat{X}|\hat{K}\hat{Y}} = P_{\hat{X}|\hat{Y}}$. Now,

$$\begin{aligned} P_{\hat{X}\hat{Y}Z} &= \sum_y P_{YZ} P_{\hat{X}\hat{Y}|Y} = \sum_y \sum_k P_{KZ} P_{Y|KZ} P_{\hat{X}\hat{Y}|Y} \\ &= \sum_k P_{KZ} \sum_y P_{Y|K} P_{\hat{X}\hat{Y}|Y} = \sum_k P_{KZ} P_{\hat{X}\hat{Y}|K} \\ &= \sum_k P_{\hat{K}Z} P_{\hat{X}\hat{Y}|\hat{K}} = \sum_k P_{\hat{K}Z} P_{\hat{Y}|\hat{K}} P_{\hat{X}|\hat{K}\hat{Y}} = P_{\hat{Y}Z} P_{\hat{X}|\hat{Y}} \ . \end{aligned}$$

It follows that $P_{X|YZ} = P_{\hat{X}|\hat{Y}Z} = P_{\hat{X}|\hat{Y}} = P_{X|Y}$ holds and, hence, $X \longleftrightarrow Y \longleftrightarrow Z$.

Suppose now that we have $X \longleftrightarrow Y \longleftrightarrow Z$. It follows $P_{X|YZ} = P_{X|Y}$. Let $P_{\hat{X}\hat{Y}|Y} := P_{XY|Y}$. We get

$$P_{\hat{X}\hat{Y}Z} = \sum_y P_{YZ} P_{\hat{X}\hat{Y}|Y} = P_{YZ} P_{X|Y} = P_{YZ} P_{X|YZ} = P_{XYZ}.$$

□

3 Pseudo-Signature Schemes

3.1 The Case of Three Players

We will state the exact condition under which a PSS can be set up from correlated pieces of information. We need the following lemma.

Lemma 6. *Let P_{XYZ} be the probability distribution of three random variables X, Y, and Z. Then the following three conditions are equivalent:*

1. *There exist two channels $P_{\overline{X}|X}$ and $P_{\hat{X}\hat{Y}|Y}$ such that $P_{\overline{X}Y} = P_{XY}$ and $P_{\overline{X}YZ} = P_{\hat{X}\hat{Y}Z}$ hold, where $P_{\overline{X}Y} = \sum_x P_{XY}P_{\overline{X}|X}$, $P_{\overline{X}YZ} = \sum_x P_{XYZ}P_{\overline{X}|X}$, and $P_{\hat{X}\hat{Y}Z} = \sum_y P_{YZ}P_{\hat{X}\hat{Y}|Y}$,*
2. $\mathrm{sim}_Z(Y \to [X \searrow Y, Y])$ *,*
3. $(X \searrow Y) \longleftrightarrow Y \longleftrightarrow Z$ *.*

Proof. Lemma 5 implies that 2. and 3. are equivalent. In the following we will prove that 1. and 2. are equivalent.

Assume that 1. is true. We have $\mathrm{sim}_Z(Y \to [\overline{X}, Y])$ for some $\overline{X}$ with $P_{XY} = P_{\overline{X}Y}$ and $Y \longleftrightarrow X \longleftrightarrow \overline{X}$. Let $K = X \searrow Y$ and $\overline{K} = \overline{X} \searrow Y$. We have $P_{KY} = P_{\overline{K}Y}$ and $Y \longleftrightarrow X \longleftrightarrow \overline{K}$. From Lemma 2, it follows $K = \overline{K}$. Since $\overline{K}$ is a function of $\overline{X}$, we get $\mathrm{sim}_Z(Y \to [X \searrow Y, Y])$.

Assume now that 2. is true. Hence, there exists a channel $P_{\overline{KY}|Y}$ such that $P_{\overline{KY}Z} = P_{KYZ}$ holds for $K := X \searrow Y$. Lemma 3 implies that there exists a channel $P_{\overline{X}|K}$—which is equal to $P_{X|K}$—such that $P_{\overline{X}Y} = P_{XY}$ holds. We set $P_{\hat{X}\hat{Y}|Y} := \sum_k P_{X|K}P_{\overline{KY}|Y}$ and $P_{\overline{X}|X} := \sum_k P_{X|K}P_{K|X}$ to get

$$\begin{aligned}
P_{\overline{X}Y} &= \sum_x P_{XY}P_{\overline{X}|X} = \sum_x P_{XY}\sum_k P_{\overline{X}|K}P_{K|X} = \sum_k P_{\overline{X}|K}\sum_x P_{XY}P_{K|X} \\
&= \sum_k P_{\overline{X}|K}P_{KY} = \sum_k P_{X|K}P_{KY} = P_{XY} \ ,
\end{aligned}$$

$$\begin{aligned}
P_{\hat{X}\hat{Y}Z} &= \sum_y P_{YZ}P_{\hat{X}\hat{Y}|Y} = \sum_y P_{YZ}\sum_k P_{\hat{X}|K}P_{\overline{KY}|Y} = \sum_k P_{\hat{X}|K}\sum_y P_{YZ}P_{\overline{KY}|Y} \\
&= \sum_k P_{\hat{X}|K}P_{\overline{KY}Z} = \sum_k P_{\hat{X}|K}P_{KYZ} = \sum_k P_{\hat{X}|K}\sum_x P_{XYZ}P_{K|X} \\
&= \sum_x P_{XYZ}\sum_k P_{\hat{X}|K}P_{K|X} = \sum_x P_{XYZ}P_{\overline{X}|X} = P_{\overline{X}YZ} \ .
\end{aligned}$$

□

Our pseudo-signature protocol makes use of typical sequences. Intuitively, a sequence of independent realizations of a random variable is *typical* if the actual rate of occurrences of every specific outcome symbol in the sequence is close to the probability of this symbol.

Definition 5. **[3, 9]** Let X be a random variable with distribution P_X and range $\mathcal{X}$, let $n > 0$ be an integer, and let $\gamma > 0$. A sequence $x^n = (x_1, \ldots, x_n) \in \mathcal{X}^n$ is called *(strongly) γ-typical* if, for all $a \in \mathcal{X}$, the actual number $N(a, x^n)$ of appearances of a in x^n satisfies

$$\left| \frac{N(a, x^n)}{n} - P_X(a) \right| \leq \frac{\gamma}{|\mathcal{X}|} \ .$$

It is a consequence of the law of large numbers that for every $\gamma > 0$, sufficiently long sequences of independent realizations of a random variable are γ-typical with overwhelming probability.

Theorem 1. **[3, 9]** *Let $X^n = X_1 \cdots X_n$ be a sequence of n independent realizations of the random variable X with distribution P_X and range $\mathcal{X}$, and let $0 < \gamma \leq 1/2$. Then*

$$\text{Prob}\,[X^n \textit{ is strongly } \gamma\textit{-typical}\,] = 1 - 2^{-\Omega(n\gamma^2)} \ .$$

The following protocol allows P_1 for signing a bit along the transfer path $P_1 \to P_2 \to P_3$.

Protocol 1 Let P_{XYZ} be such that $\text{sim}_Z(Y \to [X \searrow Y, Y])$ does not hold. Let $K := X \searrow Y$ and $L := [K, Y] \searrow Z$. Lemma 4 implies that there must exist $\delta > 0$ such that for all channels $P_{\overline{L}|Y}$, the statistical distance between the distributions P_{LZ} and $P_{\overline{L}Z}$ is at least δ.

Let n be an even integer, and let $(X_1, Y_1, Z_1), \ldots, (X_n, Y_n, Z_n)$ be n triples distributed independently according to P_{XYZ}. Let $\gamma > 0$ be a security parameter and n be large enough. Let P_1, P_2, and P_3 know $(X_1, \ldots, X_n)$, $(Y_1, \ldots, Y_n)$, and $(Z_1, \ldots, Z_n)$, respectively. Let, finally, $m \in \{0, 1\}$ be the value P_1 wants to sign.

– P_1 calculates $K_i := X_i \searrow Y_i$ and sends $(m, K_{1+(n/2)m}, \ldots, K_{n/2+(n/2)m})$ to P_2.
– P_2 checks whether the received K_i and the corresponding Y_i are a γ-typical sequence with respect to P_{KY}. If so, he accepts, calculates $L_i := [K_i, Y_i] \searrow Z_i$, and sends $(m, L_{1+(n/2)m}, \ldots, L_{n/2+(n/2)m})$ to P_3.
– P_3 checks whether the received L_i and the corresponding Z_i are a $\delta/2$-typical sequence with respect to P_{LZ}. If so, he accepts.

Theorem 2. *Let $(X_1, Y_1, Z_1), \ldots, (X_n, Y_n, Z_n)$ be n triples distributed independently according to P_{XYZ}. Let P_1, P_2, and P_3 know the values X_i, Y_i, and Z_i, respectively. Let P_1 be able to send messages to P_2, and P_2 to P_3.*

If $\text{sim}_Z(Y \to [X \searrow Y, Y])$ does not hold and n is large enough, then Protocol 1 achieves PSS for the three players with the transfer path $P_1 \to P_2 \to P_3$.

Proof. We prove that Protocol 1 implements a PSS. First of all, it follows from Theorem 1 that the value from a correct sender P_1 is accepted by P_2 except with exponentially small probability. If P_2 is correct and accepts a value and if γ is small enough, Lemma 2 implies that P_1 must indeed have sent an arbitrarily large fraction (for sufficiently large N) of correct values $K_i = X_i \searrow Y_i$ to P_2. (Note that the knowledge of the values X_j for $j \neq i$ do not help P_1 to cheat since they are independent of X_i and Y_i.)

Therefore, also an arbitrarily large fraction of the values $L_i = [K_i, Y_i] \searrow Z_i$ are correct and—if P_3 is correct—P_3 will accept the values L_i sent to him by P_2 (except with exponentially small probability).

P_2, however, cannot (except with exponentially small probability) send any other value than the one sent by P_1. Indeed, his ability to do so would imply the existence of a channel $P_{\overline{L}|Y}$ such that $P_{\overline{L}Z}$ and P_{LZ} are identical (see the proof of Lemma 6 in [23]); such a channel, however, does not exist because of the assumption stated at the beginning of the protocol. □

We now show that the condition of Theorem 2 for the achievability of a PSS among three players is tight, in other words, that $\mathrm{sim}_Z(Y \to [X \searrow Y, Y])$ and $\mathrm{sim}_Y(Z \to [X \searrow Z, Z])$ imply that no PSS with signer P_1 is possible. In order to demonstrate impossibility, we use a similar technique as in [14]. There, the impossibility of broadcast among three players secure against one corrupted player was shown by analyzing a related system obtained by copying some of the players and rearranging the original players together with their copies in a specific way.

Theorem 3. *Let $(X_1, Y_1, Z_1), \ldots, (X_n, Y_n, Z_n)$ be n triples distributed independently according to P_{XYZ}. Let P_1, P_2, and P_3 know the values X_i, Y_i, and Z_i, respectively. Let the players be connected by pairwise secure channels.*

If $\mathrm{sim}_Z(Y \to [X \searrow Y, Y])$ and $\mathrm{sim}_Y(Z \to [X \searrow Z, Z])$ hold, then there does not exist—for any n—a PSS for the three players with any *transfer path and with P_1 as the signer.*

Proof. Let us assume that there exists a protocol among the players P_1, P_2, and P_3 that achieves a PSS for the three players with transfer path $P_1 \to P_2 \to P_3$. From Lemma 6, it follows that there exist channels $P_{\overline{X}|X}$ and $P_{\hat{X}\hat{Y}|Y}$ such that $P_{XY} = P_{\overline{X}Y}$ and $P_{\overline{X}YZ} = P_{\hat{X}\hat{Y}Z}$ hold, and $P_{\overline{X}'|X}$ and $P_{\hat{X}'\hat{Z}'|Z}$ such that $P_{XZ} = P_{\overline{X}'Z}$ and $P_{\overline{X}'YZ} = P_{\hat{X}'Y\hat{Z}'}$ hold.

Let P_1' be an identical copy of P_1. We now rearrange the four players P_1, P_2, P_3, and P_1' in the following way to form a new system. The analysis of that system then reveals that no PSS among the three *original* players is possible. Note that, in the new system, no player is corrupted: It is rather the *arrangement* of this new system that simulates corruption in the original system towards the players in the new system.

- P_1 is still connected to P_2 as originally, but disconnected from P_3, i.e., all messages P_1 would send to P_3 are discarded and no message P_3 would send to P_1 is ever received by P_1.
- P_2 is still connected to P_1 and P_3 as in the original system.
- P_3 is still connected to P_2 as originally, but disconnected from P_1. Instead, P_3 is connected to P_1': All messages that P_3 would send to P_1 are delivered

to P_1' instead, and all messages P_1' would send to P_3 are indeed delivered to P_3.
- P_1' is connected to P_3 as originally, but disconnected from P_2.

Furthermore, instead of X_i, let P_1 have input $\overline{X}_i$ and P_1' have input $\overline{X}_i'$. Let them execute their local programs defined by the PSS protocol, where P_1 signs the message m and P_1' signs the message m'.

- Since $P_{XY} = P_{\overline{X}Y}$ holds, the joint view among P_1 and P_2 is indistinguishable from their view in the original system where P_1 holds input m and P_3 is corrupted in the following way: P_3 cuts off communication to P_1, simulates P_1' using the channel $P_{\hat{X}'\hat{Z}'|Z}$ to produce the values $\hat{X}'$ and $\hat{Z}'$, and acts towards P_2 as if communicating with P_1' instead of P_1 (indistinguishability follows from $P_{\overline{X}'YZ} = P_{\hat{X}'Y\hat{Z}'}$). Hence, by the *correctness property*, P_2 must accept m as signed by P_1.
- The joint view of P_2 and P_3 is indistinguishable from their view in the original system where P_1 is corrupted in the following way: P_1 simulates player P_1', uses the channel $P_{\overline{X}|X}$ for his own and the channel $P_{\overline{X}'|X}$ for P_1''s input, and acts towards P_3 as P_1'. Thus, by the *transferability property*, P_3 must accept the transfered message m from P_2.
- Since $P_{XZ} = P_{\overline{X}'Z}$ holds, the joint view of P_1' and P_3 is indistinguishable from their view in the original system[4] where P_1' holds input m' and P_2 is corrupted in the following way: P_2 cuts off communication to P_1', simulates P_1 using the channel $P_{\hat{X}\hat{Y}|Y}$ to produce the values $\hat{X}$ and $\hat{Y}$, and acts towards P_3 as if communicating with P_1 instead of P_1' (indistinguishability follows from $P_{\overline{X}YZ} = P_{\hat{X}\hat{Y}Z}$). Hence, by the *unforgeability property*, P_3 must reject the signature transferred to him by P_2.

However, this is impossible since P_3 cannot accept and reject m at the same time. The proof for the transfer path $P_1 \to P_3 \to P_2$ is analogous. Hence, there does not exist a PSS for *any* transfer path. □

If the condition of Theorem 3 does not hold, then there exists a transfer path—namely either $P_1 \to P_2 \to P_3$ or $P_1 \to P_3 \to P_2$—for which Theorem 2 can be applied. Therefore, the bound of Theorem 3 is tight, and we can state the *exact* condition under which a PSS for three players and a designated signer exists.

Theorem 4. *Let $(X_1, Y_1, Z_1), \ldots, (X_n, Y_n, Z_n)$ be n triples distributed independently according to P_{XYZ}. Let P_1, P_2, and P_3 know the values X_i, Y_i, and Z_i, respectively. Let the players pairwisely be connected by secure channels.*

There exists a PSS for the three players with transfer path $P_1 \to P_j \to P_k$ $(j \neq k)$ for large enough n if and only if either $\mathrm{sim}_Z(Y \to [X \searrow Y, Y])$ *or* $\mathrm{sim}_Y(Z \to [X \searrow Z, Z])$ *does not hold.*

[4] For simplicity, we assume the original system to consist of the players $\{P_1', P_2, P_3\}$ for this case.

Application of Lemma 5 leads to the following corollary.

Corollary 1. *Let $(X_1, Y_1, Z_1), \ldots, (X_n, Y_n, Z_n)$ be n triples distributed independently according to P_{XYZ}. Let P_1, P_2, and P_3 know the values X_i, Y_i, and Z_i, respectively. Let the players pairwisely be connected by secure channels.*

There exists a PSS for the three players with transfer path $P_1 \rightarrow P_j \rightarrow P_k$ $(j \neq k)$ for large enough n if and only if either $(X \searrow Y) \longleftrightarrow Y \longleftrightarrow Z$ or $(X \searrow Z) \longleftrightarrow Z \longleftrightarrow Y$ does not hold.

We will now present a special case of noisy channels among three players for which our PSS works. This special case is related to the "satellite scenario" of [21] for secret-key agreement.

Corollary 2. *Let R be a binary random variable and let X, Y, and Z be random variables resulting from the transmission of R over three binary symmetric channels with error probabilities ε_X, ε_Y, and ε_Z, respectively, such that $0 \leq \varepsilon_X < 1/2$, $0 < \varepsilon_Y < 1/2$ and $0 < \varepsilon_Z < 1/2$ hold. Let $(X_1, Y_1, Z_1), \ldots, (X_n, Y_n, Z_n)$ be n triples generated independently this way. Let P_1, P_2, and P_3 be three players and assume that they know X_i, Y_i, and Z_i, respectively. Let, finally, the players pairwisely be connected by secure channels. Then, for large enough n, there exists a PSS for the three players with arbitrary transfer path.*

Proof. We have that $X \searrow Y$, $X \searrow Z$ and X are—up to renaming—equal, and neither $X \longleftrightarrow Y \longleftrightarrow Z$ nor $X \longleftrightarrow Z \longleftrightarrow Y$ holds. □

Corollary 3. *Let the players P_1, P_2, and P_3 be connected by a noisy broadcast channel. This is a channel for which P_1 has an input bit X, and P_2 and P_3 get output bits Y and Z, respectively, which result from sending X over two independent noisy channels with error probabilities $0 < \varepsilon_Y < 1/2$ and $0 < \varepsilon_Z < 1/2$. Then a PSS for the three players with arbitrary transfer path can be realized.*

Proof. Let the transfer path be $P_1 \rightarrow P_2 \rightarrow P_3$. P_1 sends n random bits over the channel. Both P_2 and P_3 check whether the received values are indeed random, that is, whether they are γ_2- and γ_3-typical. The values γ_2 and γ_3 are chosen such that even if P_1 cheats, P_2 does not accept if P_3 does not either—except with small probability. The resulting joint distribution satisfies the condition of Corollary 2. □

3.2 The Case of More than Three Players

Theorem 2 can be generalized to $p > 3$ players in a natural way. Assume that p players $P_1, \ldots, P_p$ want to implement a PSS along the transfer path $P_1 \rightarrow \cdots \rightarrow P_p$. Let $(X_1^1, \ldots, X_1^p), \ldots, (X_n^1, \ldots, X_n^p)$ be n lists distributed independently according to $P_{X^1 \cdots X^p}$. Let player P_j know the values X_i^j.

As in the protocol for three players, player P_1 sends m together with his signature $(m, K^1_{1+(n/2)m}, \ldots, K^1_{n/2+(n/2)m})$, where $K_i^1 := X_i^1 \searrow X_i^2$, to P_2. P_2 is able to check whether P_1 sent the correct values K_i^1 or not, and he only accepts the signature if almost all values K_i^1 were correct.

Now we let P_2 sign the value m himself, using the random variable $[X_i^2, K_i^1]$. (Since he only received half of the values K_i^1, he is able to sign m, *but not* $1-m$.) He sends $(m, K_{1+(n/2)m}^2, \ldots, K_{n/2+(n/2)m}^2)$, where $K_i^2 := [X_i^2, K_i^1] \searrow X_i^3$, to P_3. Now P_3 can check the signature and, if he accepts, sign the value m himself, and so forth. Note that the security parameter for every signature must be less restrictive than the previous one, because some of the received K_i^j may have been faulty. Nevertheless, the error probability remains exponentially small in n. Player P_j is not able to forge a signature if

$$\mathrm{sim}_{X^{j+1}}(X^j \to [K^{j-1}, X^j])$$

does not hold. Hence, we get the following theorem.

Theorem 5. *Let $(X_1^1, \ldots, X_1^p), \ldots, (X_n^1, \ldots, X_n^p)$ be n lists distributed independently according to $P_{X^1 \cdots X^p}$. Let $P_1, \ldots, P_p$ be p players, and let P_j know all the X_i^j. Assume that for all i, player P_i can send messages to P_{i+1} in a secure way (where $P_{p+1} = P_1$). Let $K^1 := X^1 \searrow X^2$ and $K^j := [X^j, K^{j-1}] \searrow X^{j+1}$ for $j \in \{2, \ldots, n-1\}$.*

Then, for large enough n, there exists a PSS for p players with the transfer path $P_1 \to \cdots \to P_p$ and tolerating one corrupted player if there does not exist $j \geq 2$ with

$$\mathrm{sim}_{X^{j+1}}(X^j \to [K^{j-1}, X^j]) \ .$$

4 Broadcast and Multi-Party Computation

4.1 The Case of Three Players

We will now apply the results of Section 3 and state the exact condition under which broadcast is possible for three players.

Theorem 6. *Let $(X_1, Y_1, Z_1), \ldots, (X_n, Y_n, Z_n)$ be n triples distributed independently according to P_{XYZ}. Assume that P_1, P_2, and P_3 know the values X_i, Y_i, and Z_i, respectively. Let all players pairwisely be connected by secure channels.*

If n is large enough and $\mathrm{sim}_Z(Y \to [X \searrow Y, Y])$ or $\mathrm{sim}_Y(Z \to [X \searrow Z, Z])$ does not hold, then there exists a broadcast protocol for three players with sender P_1.

Proof. If either $\mathrm{sim}_Z(Y \to [X \searrow Y, Y])$ or $\mathrm{sim}_Y(Z \to [X \searrow Z, Z])$ does not hold, it is possible to set up a PSS with either the transfer path $P_1 \to P_2 \to P_3$ or $P_1 \to P_3 \to P_2$. It was shown in [16] that this is sufficient to construct a broadcast protocol for three players. □

Theorem 7. *Let $(X_1, Y_1, Z_1), \ldots, (X_n, Y_n, Z_n)$ be n triples distributed independently according to P_{XYZ}. Assume that P_1, P_2, and P_3 know the values X_i, Y_i, and Z_i, respectively. Let all players pairwisely be connected by secure channels.*

If both $\mathrm{sim}_Z(Y \to [X \searrow Y, Y])$ and $\mathrm{sim}_Y(Z \to [X \searrow Z, Z])$ hold, then there exists no broadcast protocol (for any n) for three players with sender P_1.

Proof. From Lemma 6, it follows that there exist channels $P_{\overline{X}|X}$ and $P_{\hat{X}\hat{Y}|Y}$ such that $P_{XY} = P_{\overline{X}Y}$ and $P_{\overline{X}YZ} = P_{\hat{X}\hat{Y}Z}$ hold, as well as $P_{\overline{X}'|X}$ and $P_{\hat{X}'\hat{Z}'|Z}$ such that $P_{XZ} = P_{\overline{X}'Z}$ and $P_{\overline{X}'YZ} = P_{\hat{X}'Y\hat{Z}'}$ hold.

As in the proof of Theorem 3, we duplicate the sender P_1 and rearrange the four resulting players in the following way: We disconnect P_1 and P_3 but connect P_3 to P_1' instead, whereas P_2 stays connected as originally.

P_1 gets input $\overline{X}_i$, constructed by applying the channel $P_{\overline{X}|X}$ on X_i. P_1' gets input $\overline{X}'$, constructed by applying the channel $P_{\overline{X}'|X}$ on X_i. P_2 gets input Y_i, and P_3 gets input Z_i.

We give P_1 and P_1' two different inputs m and m' and let them all execute the protocol; they all output a value. We now consider three scenarios of an original system involving some of the players P_1, P_1', P_2, and P_3 of the new system obtained by interconnecting all four players as described above.

- Let P_1 and P_2 be correct and P_3 be corrupted. Using his variables Z_i, P_3 can produce $\hat{X}_i'$ and $\hat{Z}_i'$ such that P_2 cannot distinguish them from $\overline{X}_i'$ and Z_i. Furthermore, P_2 cannot distinguish $\overline{X}_i$, which he receives from P_1, from X_i. P_3 simulates P_1', giving him the values $\hat{X}_i'$ as input, and using the values $\hat{Z}_i'$ himself.
- Let P_1' and P_3 be correct and P_2 be corrupted. Using his variables Y_i, P_2 can produce $\hat{X}_i$ and $\hat{Y}_i$ such that P_3 cannot distinguish them from $\overline{X}_i$ and Y_i. Furthermore, P_3 cannot distinguish $\overline{X}_i'$, which he receives from P_1, from X_i. P_2 simulates P_1, giving him the values $\hat{X}_i$ as input, and using the values $\hat{Y}_i$ himself.
- Let P_2 and P_3 be correct and P_1 be corrupted. Using his variables X_i, P_1 can produce $\overline{X}_i$ and $\overline{X}_i'$. He can simulate player P_1' with $\overline{X}_i'$ as input and use $\overline{X}_i$ for himself.

The joint view of the players P_1 and P_2 in the new system is indistinguishable from their view in the first scenario, and they must thus output m. The joint view of the players P_1' and P_3 in the new system is indistinguishable from their joint view in the second scenario, and they, therefore, output m'. But also the joint view of players P_2 and P_3 in the new system is indistinguishable from their view in the third scenario, and thus they must agree on their output value, which contradicts what we derived above. Therefore, no broadcast protocol can exist. □

Using Theorems 6 and 7 we can now state the exact condition under which broadcast and MPC among three players are possible.

Theorem 8. *Let $(X_1, Y_1, Z_1), \ldots, (X_n, Y_n, Z_n)$ be n triples distributed independently according to P_{XYZ}. Let P_1, P_2, and P_3 know the values X_i, Y_i, and Z_i, respectively. Let all players pairwisely be connected by secure channels. Broadcast with sender P_1 is possible if and only if*

$$\neg \Big(\mathrm{sim}_Z(Y \to [X \searrow Y, Y]) \;\wedge\; \mathrm{sim}_Y(Z \to [X \searrow Z, Z])\Big)$$

holds.

Corollary 4. *Let $(X_1, Y_1, Z_1), \ldots, (X_n, Y_n, Z_n)$ be n triples distributed independently according to P_{XYZ}. Let P_1, P_2, and P_3 know the values X_i, Y_i, and Z_i, respectively. Let all players pairwisely be connected by secure channels.*

Broadcast with sender P_1 is possible if and only if

$$\neg \Big((X \searrow Y) \longleftrightarrow Y \longleftrightarrow Z \quad\wedge\quad (X \searrow Z) \longleftrightarrow Z \longleftrightarrow Y\Big)$$

holds.

Lemma 7. *Given three players P_1, P_2, and P_3, connected pairwisely by secure channels and additionally by broadcast channels from P_1 to $\{P_2, P_3\}$ and from P_2 to $\{P_1, P_3\}$ (but no other primitive such as a PSS among the players). Then broadcast from P_3 to $\{P_1, P_2\}$ is impossible.*

Proof. This follows from a generalization of the proof in [14], where only pairwise channels are assumed. □

Theorem 9. *Let $(X_1, Y_1, Z_1), \ldots, (X_n, Y_n, Z_n)$ be n triples distributed independently according to P_{XYZ}. Let P_1, P_2, and P_3 know the values X_i, Y_i, and Z_i, respectively. Let all players pairwisely be connected by secure channels.*

Broadcast with arbitrary sender as well as general multi-party computation secure against one corrupted player are possible if and only if

$$\begin{aligned}
&\neg \Big(\mathrm{sim}_Z(Y \to [X \searrow Y, Y]) \;\wedge\; \mathrm{sim}_Y(Z \to [X \searrow Z, Z])\Big) \;\wedge \\
&\neg \Big(\mathrm{sim}_X(Z \to [Y \searrow Z, Z]) \;\wedge\; \mathrm{sim}_Z(X \to [Y \searrow X, X])\Big) \;\wedge \\
&\neg \Big(\mathrm{sim}_X(Y \to [Z \searrow Y, Y]) \;\wedge\; \mathrm{sim}_Y(X \to [Z \searrow X, X])\Big)
\end{aligned}$$

holds.

Proof. The condition is sufficient for the possibility of broadcast because of Theorem 8 and Lemma 7. The achievability of multi-party computation then follows from [1, 26, 10]. Furthermore, since broadcast is a special case of multi-party computation, the impossibility of broadcast immediately implies the impossibility of MPC. □

Corollary 5. *Let $(X_1, Y_1, Z_1), \ldots, (X_n, Y_n, Z_n)$ be n triples distributed independently according to P_{XYZ}. Let P_1, P_2, and P_3 know the values X_i, Y_i, and Z_i respectively. Let all players pairwisely be connected by secure channels.*

Broadcast with arbitrary sender as well as general multi-party computation secure against one corrupted player are possible if and only if

$$\begin{array}{l}
\neg \Big((X \searrow Y) \longleftrightarrow Y \longleftrightarrow Z \quad \wedge \quad (X \searrow Z) \longleftrightarrow Z \longleftrightarrow Y \Big) \ \wedge \\
\neg \Big((Y \searrow Z) \longleftrightarrow Z \longleftrightarrow X \quad \wedge \quad (Y \searrow X) \longleftrightarrow X \longleftrightarrow Z \Big) \ \wedge \\
\neg \Big((Z \searrow Y) \longleftrightarrow Y \longleftrightarrow X \quad \wedge \quad (Z \searrow X) \longleftrightarrow X \longleftrightarrow Y \Big)
\end{array}$$

holds.

4.2 The Case of More than Three Players

Corollary 6. *Let $P_1, \ldots, P_n$ be n players. Let all players pairwisely be connected by secure channels. Furthermore, let every triple of players (P_i, P_j, P_k) have enough independent realizations of X^i, X^j, and X^k, respectively, such that either $\mathrm{sim}_{X^k}(X^j \to [X^i \searrow X^j, X^j])$ or $\mathrm{sim}_{X^j}(X^k \to [X^i \searrow X^k, X^k])$ does not hold. Then broadcast and multi-party computation unconditionally secure against $t < n/2$ corrupted players are achievable.*

Proof. From Theorem 9, it follows that any triple of players can execute a broadcast protocol. Using the protocol from [17], broadcast for n players tolerating $t < n/2$ corrupted players can be achieved. Using [1, 26, 10], a protocol for unconditional MPC can be constructed that can tolerate $t < n/2$ corrupted players. □

5 Concluding Remarks

In the model of unconditional security, we have completely characterized the possibility of pseudo-signatures, broadcast, and secure multi-party computation among three players having access to certain correlated pieces of information. Interestingly, this condition is closely related to a property called (non-) simulatability previously studied in an entirely different context, namely information-theoretic secret-key agreement.

As a consequence of this result, we gave a new, weaker condition for the possibility of achieving unconditional broadcast between n players and any minority of cheaters and, hence, general multi-party computation under the same conditions.

Acknowledgments

The first author was supported by the Packard Foundation and the second and the third author by Canada's NSERC.

References

1. Donald Beaver. Multiparty protocols tolerating half faulty processors. In *Advances in Cryptology: CRYPTO '89*, volume 435 of *Lecture Notes in Computer Science*, pages 560–572. Springer-Verlag, 1989.
2. Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC '88)*, pages 1–10. Springer-Verlag, 1988.
3. Richard E. Blahut. *Principles and practice of information theory.* Addison-Wesley, Reading, MA, 1988.
4. Jurjen Bos and Bert den Boer. Detection of disrupters in the DC protocol. In *Advances in Cryptology: EUROCRYPT '89*, volume 434 of *Lecture Notes in Computer Science*, pages 320–327. Springer-Verlag, 1990.
5. David Chaum. The Dining Cryptographers Problem: Unconditional sender and recipient untraceability. *Journal of Cryptology,* 1(1):65–75, 1988.
6. David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols (extended abstract). In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC '88)*, pages 11–19. ACM Press, 1988.
7. David Chaum and Sandra Roijakkers. Unconditionally-secure digital signatures. In *Advances in Cryptology: CRYPTO '90*, volume 537 of *Lecture Notes in Computer Science*, pages 206–214. Springer-Verlag, 1990.
8. Richard Cleve. Limits on the security of coin flips when half the processors are faulty. In *ACM Symposium on Theory of Computing (STOC '86)*, pages 364–369, ACM Press, 1986.
9. Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory.* Wiley-Interscience, New York, USA, 1991.
10. Ronald Cramer, Ivan Damgård, Stefan Dziembowski, Martin Hirt, and Tal Rabin. Efficient multiparty computations secure against an adaptive adversary. In *Advances in Cryptology: EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 311–326. Springer-Verlag, 1999.
11. Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.
12. Danny Dolev and H. Raymond Strong. Polynomial algorithms for multiple processor agreement. In *Proceedings of the 14th Annual ACM Symposium on Theory of Computing (STOC '82)*, pages 401–407, 1982.
13. Danny Dolev and H. Raymond Strong. Authenticated algorithms for Byzantine agreement. *SIAM Journal on Computing*, 12(4):656–666, 1983.
14. Michael J. Fischer, Nancy A. Lynch, and Michael Merritt. Easy impossibility proofs for distributed consensus problems. *Distributed Computing*, 1:26–39, 1986.
15. Matthias Fitzi, Nicolas Gisin, and Ueli Maurer. Quantum solution to the Byzantine agreement problem. *Physical Review Letters*, 87(21):7901–1–7901–4, 2001.
16. Matthias Fitzi, Nicolas Gisin, Ueli Maurer, and Oliver von Rotz. Unconditional Byzantine agreement and multi-party computation secure against dishonest minorities from scratch. In *Advances in Cryptology: EUROCRYPT '02*, volume 2332 of *Lecture Notes in Computer Science*, pages 482–501. Springer-Verlag, 2002.
17. Matthias Fitzi and Ueli Maurer. From partial consistency to global broadcast. In *32nd Annual Symposium on Theory of Computing, STOC '00*, pages 494–503. ACM, 2000.

18. Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC '87)*, pages 218–229. ACM Press, 1987.
19. Leslie Lamport. Constructing digital signatures from a one-way function. Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, 1979.
20. Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, 1982.
21. Ueli Maurer. Secret key agreement by public discussion. *IEEE Transaction on Information Theory*, 39(3):733–742, 1993.
22. Ueli Maurer. Information-theoretically secure secret-key agreement by NOT authenticated public discussion. In *Advances in Cryptology: EUROCRYPT '97*, volume 49 of *Lecture Notes in Computer Science*, pages 209–225. Springer-Verlag, 1997.
23. Ueli M. Maurer and Stefan Wolf. Secret-key agreement over unauthenticated public channels—Part I: Definitions and a completeness result. *IEEE Transactions on Information Theory*, 49:822–831, 2003.
24. Ueli M. Maurer and Stefan Wolf. Secret-key agreement over unauthenticated public channels—Part II: The simulatability condition. *IEEE Transactions on Information Theory*, 49:832–838, 2003.
25. Birgit Pfitzmann and Michael Waidner. Information-theoretic pseudosignatures and Byzantine agreement for $t >= n/3$. Technical Report RZ 2882 (#90830), IBM Research, 1996.
26. Tal Rabin and Michael Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC '89)*, pages 73–85, 1989.
27. Andrew C. Yao. Protocols for secure computations. In *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science (FOCS '82)*, pages 160–164, 1982.