Secret-Key Agreement over Unauthenticated Public Channels – Part II: The Simulatability Condition

Ueli Maurer, *Fellow, IEEE* Stefan Wolf

Abstract— **This is the second part of a three-part paper on secret-key agreement secure against active adversaries. In the first part, we showed that when two parties, willing to generate a secret key, but connected only by a completely insecure communication channel, have access to independent repetitions of some random experiment, then the possibility of secret-key agreement depends on a certain property, called *simulatability*, of the probability distribution modeling the parties' initial knowledge. More generally, the simulatability condition is important in the context of identification and authentication among parties sharing some correlated but not necessarily identical partially secret keys. Unfortunately, this condition is a priori not very useful since it is not clear how to decide efficiently whether it is satisfied or not for a given distribution P_{XYZ}. We introduce a new formalism, based on a mechanical model for representing the involved quantities, that allows for dealing with discrete joint distributions of random variables and their manipulations by noisy channels. We show that this representation leads to a simple and efficient characterization of the possibility of secret-key agreement secure against active adversaries.**

Keywords. Cryptography, unconditional security, secret-key agreement, authentication.

I. Introduction

In many situations, two parties Alice and Bob, who have access to (correlated) information modeled by random variables X and Y, respectively, can, by communication over an insecure channel, generate a secret key S about which an adversary Eve, initially knowing a third random variable Z, has virtually no information (e.g., in terms of Shannon entropy). In particular, Eve cannot obtain substantial information about the secret key even with infinite computational resources.

In [9] it was shown that such key agreement can be possible in principle even if Alice and Bob's communication channel does not offer authenticity (let alone confidentiality). In this case however, the random variables X, Y, and Z must satisfy a certain condition, called *non-simulatability*. Unfortunately, this condition is a priori not easy to check for a given distribution P_{XYZ}. It is the goal of this paper to develop a calculus for discrete distributions which yields efficient criteria for the possibility of key agreement secure against active adversaries. Further applications of this calculus are also discussed.

The outline of this paper is as follows. In Section II, we repeat the definition of simulatability of a distribution P_{XYZ} and briefly recall the results of [9], stating that this is the key condition in the context of unconditional security of key agreement in the presence of active adversaries. In Section III we develop a new calculus, based on representing distributions in a mechanical model, for joint distributions of three random variables and noisy channels acting on them. Finally, we use this calculus in Section IV to derive efficiently verifiable criteria for (non-)simulatability.

II. The Simulatability Condition

It is not surprising that secret-key agreement secure against active adversaries as defined in [9] can only be possible if Alice and Bob have some initial advantage over Eve in terms of the distribution P_{XYZ}. More precisely, it was shown that this advantage must be such that Eve cannot generate from Z a random variable $\overline{X}$ which Bob, knowing Y, is unable to distinguish from X (and vice versa). The following property of a distribution P_{XYZ} was defined in [6] (see also [9]).

Definition 1: **[6]** 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 $P_{\overline{X}Y} = P_{XY}$, where $P_{\overline{X}Y} = \sum P_{YZ} \cdot P_{\overline{X}|Z}$.

Another way of stating that $\mathrm{sim}_Y(Z \to X)$ holds is that there exists a random variable $\overline{X}$ such that $I(\overline{X}; XY|Z) = 0$, i.e., $XY \to Z \to \overline{X}$ is a Markov chain, with $P_{\overline{X}Y} = P_{XY}$.

In [9] the following facts were shown. The pessimistic result is that whenever either $\mathrm{sim}_Y(Z \to X)$ or $\mathrm{sim}_X(Z \to Y)$ holds, then no secret-key agreement is possible at all in the active-adversary scenario. The reason is that Bob has no advantage over Eve from Alice's viewpoint, or vice versa. Thus Eve can impersonate one of the legitimate partners without facing the risk of being detected, and the protocol being aborted.

On the other hand, however, if neither X nor Y is simulatable by Eve, then an active adversary is not much more powerful than a passive one. More precisely, in the scenario where the parties have access to repeated realizations of their random variables, the achievable secret-key generation rates do not depend on whether Eve is only a passive wire-tapper or even an active attacker. (Clearly, an active Eve can always block the communication channel completely and prevent any communication between Alice and Bob.)

These facts show that the simulatability condition defined above is of paramount importance in the context of key agreement secure against active adversaries. Let us

This paper appeared in *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 832–838, 2003.

begin the analysis of this condition with two properties of distributions P_{XYZ} satisfying it.

Consider the special scenario where all the parties obtain noisy versions of a binary signal (e.g., a satellite signal) over some independent channels, i.e., where

$$P_{XYZ|R} = P_{X|R} \cdot P_{Y|R} \cdot P_{Z|R}$$

holds for some binary R (see for instance [5] or [7]). In this setting, the condition $\mathrm{sim}_Y(Z \to X)$ is *equivalent* to $I(Y;Z) \geq I(Y;X)$. One implication of this equivalence is always true, as Lemma 1 shows.

Lemma 1: Let P_{XYZ} be a distribution such that $\mathrm{sim}_Y(Z \to X)$ holds. Then

$$I(Y;Z) \geq I(Y;X) \ .$$

Proof. There exists a conditional distribution $P_{\overline{X}|Z}$ such that $P_{\overline{X}Y} = P_{XY}$. Hence we have

$$\begin{aligned} I(Y;Z) &= H(Y) - H(Y|Z) \\ &= H(Y) - H(Y|Z\overline{X}) \\ &\geq H(Y) - H(Y|\overline{X}) \\ &= I(Y;\overline{X}) \\ &= I(Y;X) \ , \end{aligned}$$

where the second equality holds since $I(Y;\overline{X}|Z) = 0$. □

However, the inverse implication is not true in general. To see this, consider the following distribution P_{XYZ} [8]. Let the random variables X and Y be binary and distributed according to

$$P_{XY}(0,0) = P_{XY}(1,1) = \frac{1-\alpha}{2} \ ,$$

$$P_{XY}(0,1) = P_{XY}(1,0) = \frac{\alpha}{2}$$

for some $\alpha < 1/2$. The random variable Z is generated by sending $[X,Y]$ over an erasure channel with positive erasure probability $1-r$. Clearly, both $\mathrm{sim}_Y(Z \to X)$ and $\mathrm{sim}_X(Z \to Y)$ hold for this distribution P_{XYZ} if and only if

$$r + \frac{1-r}{2} \geq 1 - \alpha \ ,$$

i.e., $r \geq 1 - 2\alpha$. On the other hand, $I(Y;Z) \geq I(Y;X)$ holds exactly if

$$r \geq 1 - h(\alpha) \ .$$

It may be somewhat surprising that for $r \in [1-h(\alpha), 1-2\alpha[$, Eve cannot simulate X with respect to Y although she has more information about Y than X provides.

As the example of the noisy versions of a binary signal shows, the fact that X and Y are simulatable does *not* imply that secret-key agreement against *passive* adversaries is not possible. However, the following statement, closely related to the inverse direction of this implication, is true. Note here that the so-called *intrinsic information* $I(X;Y{\downarrow}Z)$ was introduced in [8] as a general upper bound on the secret key rate $S(X;Y||Z)$. The definition of this quantity is $I(X;Y{\downarrow}Z) := \min_{XY \to Z \to \overline{Z}} I(X;Y|\overline{Z})$.

Lemma 2: Let P_{XYZ} be such that $I(X;Y{\downarrow}Z) = 0$. Then both $\mathrm{sim}_Y(Z \to X)$ and $\mathrm{sim}_X(Z \to Y)$ hold.

Proof. Let $P_{\overline{Z}|Z}$ be a conditional distribution with

$$I(X;Y|\overline{Z}) = 0 \ . \qquad (1)$$

(Such a distribution exists according to [2].) Equivalently, $XY \to Z \to \overline{Z}$ is a Markov chain such that (1) holds, i.e., $X \to \overline{Z} \to Y$ is also a Markov chain. We show $\mathrm{sim}_Y(Z \to X)$. The proof that $\mathrm{sim}_X(Z \to Y)$ holds is analogous. Let $\overline{X}$ be generated from $\overline{Z}$ by the channel $P_{\overline{X}|\overline{Z}} := P_{X|\overline{Z}}$. (This extends the Markov chain to $XY \to Z \to \overline{Z} \to \overline{X}$, hence $XY \to Z \to \overline{X}$ is also a Markov chain.) We show that $P_{\overline{X}Y} = P_{XY}$ holds. To see this, note that

$$P_{\overline{X}Y\overline{Z}} = P_{\overline{XZ}} \cdot P_{Y|\overline{XZ}} = P_{\overline{XZ}} \cdot P_{Y|\overline{Z}}$$

and

$$P_{XY\overline{Z}} = P_{X\overline{Z}} \cdot P_{Y|X\overline{Z}} = P_{X\overline{Z}} \cdot P_{Y|\overline{Z}}$$

because $I(\overline{X};Y|\overline{Z}) = I(X;Y|\overline{Z}) = 0$. From $P_{\overline{XZ}} = P_{X\overline{Z}}$ (which is true by construction of $\overline{X}$) we conclude $P_{\overline{X}Y\overline{Z}} = P_{XY\overline{Z}}$, hence $P_{\overline{X}Y} = P_{XY}$. □

III. A Calculus for Discrete Distributions and Channels

According to Section II, the simulatability condition allows for separating the cases where secret-key agreement is possible and impossible in the presence of active adversaries. However, the characterization is a priori not practical because it depends on the existence of a particular channel (with certain properties) among the (uncountably infinite) set of all discrete channels with given input and output alphabets. In the sequel, we address the following questions:

- Is it, for a given distribution P_{XYZ}, possible to decide efficiently whether $\mathrm{sim}_Y(Z \to X)$ holds?
- If $\mathrm{sim}_Y(Z \to X)$ holds, is it possible to efficiently find a channel $P_{\overline{X}|Z}$ for which we have $P_{\overline{X}Y} = P_{XY}$?

We start by analyzing an example.

Example 1: Let the distribution P_{XYZ} of the random variables X, Y, and Z with ranges $\mathcal{X} = \{x_1, x_2\}$, $\mathcal{Y} = \{y_1, y_2\}$, and $\mathcal{Z} = \{z_1, z_2, z_3\}$ be as follows:

$$\begin{aligned} &P_{XYZ}(x_1,y_1,z_1) = 6/100 \ , \\ &P_{XYZ}(x_2,y_1,z_1) = 4/100 \ , \\ &P_{XYZ}(x_1,y_1,z_2) = 9/100 \ , \\ &P_{XYZ}(x_2,y_1,z_2) = 6/100 \ , \\ &P_{XYZ}(x_1,y_1,z_3) = 15/100 \ , \\ &P_{XYZ}(x_2,y_1,z_3) = 10/100 \ , \\ &P_{XYZ}(x_1,y_2,z_1) = 36/100 \ , \\ &P_{XYZ}(x_2,y_2,z_1) = 4/100 \ , \\ &P_{XYZ}(x_1,y_2,z_2) = 9/100 \ , \\ &P_{XYZ}(x_2,y_2,z_2) = 1/100 \ , \\ &P_{XYZ}(x_1,y_2,z_3) = 0 \ , \\ &P_{XYZ}(x_2,y_2,z_3) = 0 \ . \end{aligned}$$

In order to decide whether $\mathrm{sim}_Y(Z \to X)$ holds, let us first consider the marginal distributions P_{XY} and P_{YZ}.

P_{XY}	y_1	y_2	$P_X(x_i)$	$P_{Y\|X=x_i}(y_1)$
x_1	0.3	0.45	0.75	0.4
x_2	0.2	0.05	0.25	0.8

P_{YZ}	y_1	y_2	$P_Z(z_j)$	$P_{Y\|Z=z_j}(y_1)$
z_1	0.1	0.4	0.5	0.2
z_2	0.15	0.1	0.25	0.6
z_3	0.25	0	0.25	1

We jointly represent these distributions as follows. We mark every symbol $x_i \in \mathcal{X}$ and every $z_j \in \mathcal{Z}$ with an empty or filled circle, respectively, where the size (or mass) of the circle corresponds to the probability $P_X(x_i)$ or $P_Z(z_j)$, and the position in the interval $[0,1]$ is given by the probability $P_{Y|X=x_i}(y_1)$ or $P_{Y|Z=z_j}(y_1)$, respectively (see Figure 1).

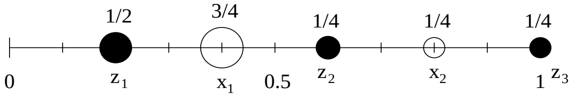

Fig. 1. Representation of P_{XYZ}

Note that not the entire information about P_{XYZ} is contained in this representation: only the distributions P_{XY} and P_{YZ}, but not P_{XYZ}, can be reconstructed from the quantities represented in the picture. We will see, however, that whether or not X is simulatable by Z with respect to Y depends, not surprisingly, only on P_{XY} and P_{YZ}, as Theorem 1 shows. On the other hand, not every such representation corresponds to a distribution P_{XYZ}. This is only true if the total mass of each point set is 1, and if the marginal distribution P_Y is equal for both distributions P_{XY} and P_{YZ}. The last condition is equivalent to the fact that the sets of full and empty circles have the same center of gravity when interpreted as point masses.

Let now $Z^{(2)}$ with $\mathcal{Z}^{(2)} = \{z_1^{(2)}, z_2^{(2)}\}$ be generated by sending Z over the channel

$$
\begin{aligned}
P_{Z^{(2)}|Z}(z_1^{(2)}, z_1) &= 1 , \\
P_{Z^{(2)}|Z}(z_2^{(2)}, z_2) &= 1 , \\
P_{Z^{(2)}|Z}(z_2^{(2)}, z_3) &= 1 .
\end{aligned}
$$

For the new distribution $P_{XYZ^{(2)}}$, the above representation is as shown in Figure 2: Two masses have been united in their center of gravity.

Let then $Z^{(2)}$ be sent over the additional channel $P_{Z^{(3)}|Z^{(2)}}$, where $\mathcal{Z}^{(3)} = \{z_1^{(3)}, z_2^{(3)}, z_3^{(3)}\}$, with

$$
\begin{aligned}
P_{Z^{(3)}|Z^{(2)}}(z_1^{(3)}, z_1^{(2)}) &= 1 , \\
P_{Z^{(3)}|Z^{(2)}}(z_2^{(3)}, z_2^{(2)}) &= 1/2 , \\
P_{Z^{(3)}|Z^{(2)}}(z_3^{(3)}, z_2^{(2)}) &= 1/2 .
\end{aligned}
$$

This corresponds to splitting one of the masses into two (equal) parts (see Figure 3).

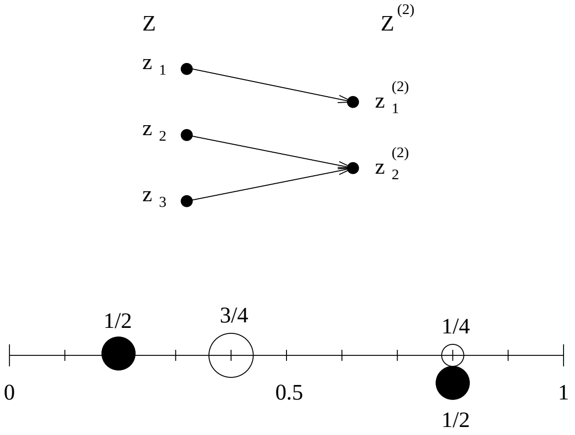

Fig. 2. The Channel $P_{Z^{(2)}|Z}$, and $P_{XYZ^{(2)}}$

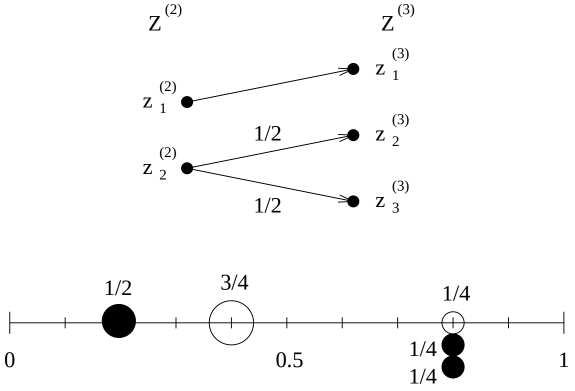

Fig. 3. The Channel $P_{Z^{(3)}|Z^{(2)}}$, and $P_{XYZ^{(3)}}$

Finally, let $P_{\overline{X}|Z^{(3)}}$, with $\overline{\mathcal{X}} = \{\overline{x}_1, \overline{x}_2\}$, be given by

$$
\begin{aligned}
P_{\overline{X}|Z^{(3)}}(\overline{x}_1, z_1^{(3)}) &= 1 , \\
P_{\overline{X}|Z^{(3)}}(\overline{x}_1, z_2^{(3)}) &= 1 , \\
P_{\overline{X}|Z^{(3)}}(\overline{x}_2, z_3^{(3)}) &= 1 .
\end{aligned}
$$

The use of this channel again corresponds to uniting two masses in their center of gravity. The constellation of the masses with respect to X and $\overline{X}$ are now equal (see Figure 4), which means that $P_{\overline{X}Y} = P_{XY}$ holds. Hence $\mathrm{sim}_Y(Z \to X)$ is true, and the corresponding channel $P_{\overline{X}|Z}$ is the cascade of the three channels above:

$$
\begin{aligned}
P_{\overline{X}|Z}(\overline{x}_1, z_1) &= 1 , \\
P_{\overline{X}|Z}(\overline{x}_1, z_2) &= P_{\overline{X}|Z}(\overline{x}_2, z_2) = 1/2 , \\
P_{\overline{X}|Z}(\overline{x}_1, z_3) &= P_{\overline{X}|Z}(\overline{x}_2, z_3) = 1/2
\end{aligned}
$$

(see Figure 5).

We will now make this representation in the mechanical model more precise and exploit the direct connection between distributions and channels on one side and mass constellations as well as mass operations on the other for giving a simple characterization of non-simulatability. The

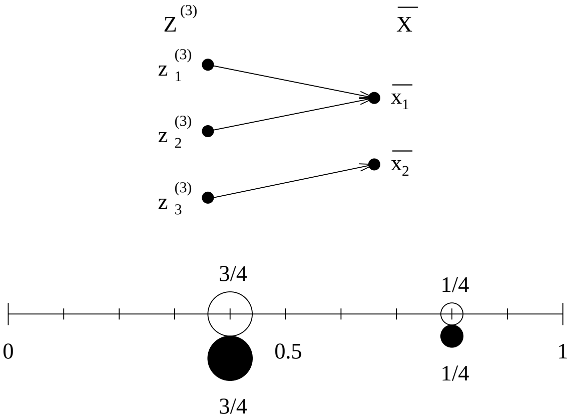

Fig. 4. The Channel $P_{\overline{X}|Z^{(3)}}$, and $P_{XY\overline{X}}$

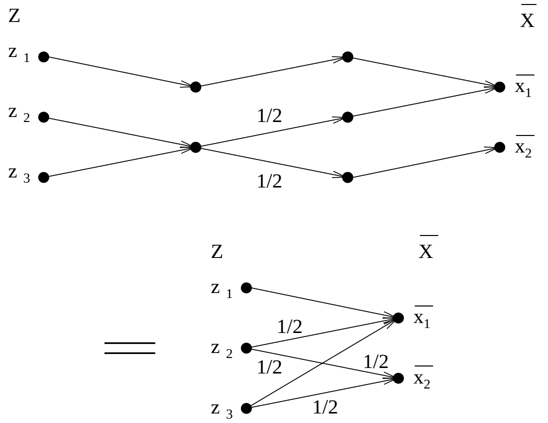

Fig. 5. The Cascaded Channel $P_{\overline{X}|Z}$

purpose of the physical model is to give more intuitive deductions and formulations of results that could as well be stated and proved purely in terms of distributions and channels. Theorem 1 below makes a direct link between the two formalisms and justifies the point of view we take. In the following, particular emphasis is given to an intuitive presentation.

Definition 2: For an integer $N \geq 1$, an *N-dimensional (normed) mass constellation* $M := (m_i, a_i)_{i=1,\ldots,\ell}$ is a family of pairs with $m_i \in (0,1]$ and $a_i \in [0,1]^N$ for all i such that $\sum_i m_i = 1$. We additionally assume that the pairs are ordered with respect to the lexicographic ordering of the vectors a_i. The *center of gravity* (*center* for short) $c(M)$ of such a constellation is given by

$$c(M) := \sum_{i=1}^{\ell} m_i a_i \ .$$

Two constellations are *equicentered* if they have the same center of gravity. A constellation $M' = (m'_i, a'_i)_{i=1,\ldots,\ell'}$ is *derived* from $M = (m_i, a_i)_{i=1,\ldots,\ell}$ by *mass splitting* if $\ell' = \ell + 1$, and if there exist $0 < p < 1$, $1 \leq i_0 \leq \ell$, such that

$$(m'_i, a'_i) = \begin{cases} (m_i, a_i) & 1 \leq i < i_0 \\ (p m_{i_0}, a_{i_0}) & i = i_0 \\ ((1-p) m_{i_0}, a_{i_0}) & i = i_0 + 1 \\ (m_{i-1}, a_{i-1}) & i_0 + 1 < i \leq \ell + 1 \ . \end{cases}$$

Furthermore, M' is *derived* from M by *mass union* if $\ell' = \ell - 1$, and if there exist $i_1 < i_2$, $i_1 \leq i_u \leq i_2$, such that

$$(m'_i, a'_i) = \begin{cases} (m_i, a_i) & 1 \leq i < i_1 \\ (m_{i+1}, a_{i+1}) & i_1 \leq i < i_u \\ (m_{i_1} + m_{i_2}, \\ \quad \frac{m_{i_1} a_{i_1} + m_{i_2} a_{i_2}}{m_{i_1} + m_{i_2}}) & i = i_u \\ (m_i, a_i) & i_u < i < i_2 \\ (m_{i+1}, a_{i+1}) & i_2 \leq i \leq \ell - 1 \ . \end{cases}$$

We call mass splitting and mass union *basic mass operations.* Neither of them changes the center of gravity. A constellation M is called *stronger* than M', denoted by $M \rightsquigarrow M'$, if there exists a finite sequence of basic operations that transforms M into M'.

It is clear that if $M \rightsquigarrow M'$, then the two constellations M and M' are equicentered. On the other hand, there exist equicentered constellations such that none is stronger than the other (see Figure 6).

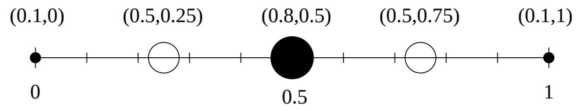

Fig. 6. Incomparable Constellations: None is Stronger

Let P_{UV} be the joint distribution of two random variables U and V with ranges $\mathcal{U}$ and $\mathcal{V} = \{v_1, \ldots, v_{N+1}\}$. Then the N-dimensional constellation $M_{U \leftarrow V}$ is defined by

$$M_{U \leftarrow V} =$$

$$(P_U(u), (P_{V|U=u}(v_1), \ldots, P_{V|U=u}(v_N)))_{u \in \mathcal{U}} \ .$$

Note that the definition of $M_{U \leftarrow V}$ leads to a one-to-one correspondence between distributions P_{UV}, where $|\mathcal{V}| = N + 1$, and N-dimensional normed mass constellations $(m_i, a_i)_{i=1,\ldots,\ell}$ contained in the simplex characterized by $(a)_j \geq 0$ and $\sum_{j=1}^{N} (a)_j \leq 1$.

Theorem 1 links simulatability and mass constellations. In this context, note first that for every distribution P_{XYZ}, $M_{X \leftarrow Y}$ and $M_{Z \leftarrow Y}$ are equicentered.

Theorem 1: Let P_{XYZ} be the joint distribution of X, Y, and Z. Then X is simulatable by Z with respect to Y if and only if $M_{X \leftarrow Y}$ is stronger than $M_{Z \leftarrow Y}$:

$$\mathrm{sim}_Y(Z \to X) \iff M_{Z \leftarrow Y} \rightsquigarrow M_{X \leftarrow Y} \ .$$

Proof. Let $P_{U_1 V}$ and $P_{U_2 V}$ be the joint distributions of random variables U_1 and V, and U_2 and V, respectively. Clearly, $M_{U_2 \leftarrow V}$ can be obtained from $M_{U_1 \leftarrow V}$ by a mass splitting or mass union operation if and only if there exists a "splitting channel" (as in Figure 2) or a "union channel" (see Figure 3) $P_{\overline{U}_2|U_1}$, respectively, such that

$$\begin{aligned} P_{\overline{U}_2 V}(u_2, v) &= \sum_{u_1 \in \mathcal{U}_1} P_{U_1 V}(u_1, v) \cdot P_{\overline{U}_2|U_1}(u_2, u_1) \\ &= P_{U_2 V}(u_2, v) \ . \end{aligned}$$

The statement now follows from the facts that every discrete channel (with m output symbols) can be represented as a cascade of splitting and union channels, and that a cascade of channels is equivalent to the sequence of the corresponding mass operations. The first of these two facts can be shown as follows. First, all the letters of the input alphabet can be split, one after the other, to m symbols each (by $m-1$ splitting channels with certain probabilities for each symbol), and they can be united by union channels to the output symbols of the discrete channel. The second fact is obvious. □

Unfortunately, the condition given in Theorem 1 is a priori not more than a new formulation of simulatability, and is not obviously verifiable more efficiently. However, it leads to an efficiently checkable criterion as Corollary 3 and Theorem 5 below show.

As a preparation for these results, we describe a special mass operation, called *mass approach*, that can be composed by four basic operations (see Figure 7).

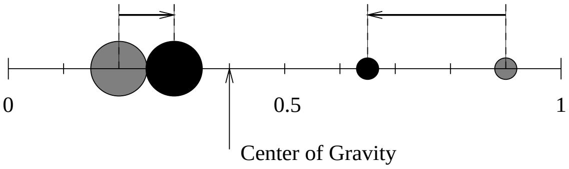

Fig. 7. A Mass Approach

Lemma 3: Let a constellation $M = (m_i, a_i)_{i=1,\ldots,\ell}$ be given, and let $i \neq i'$, $1 \leq i, i' \leq \ell$. We denote by

$$c_{i,i'} := (m_i a_i + m_{i'} a_{i'})/(m_i + m_{i'})$$

the center of gravity of the ith and i'th masses. Then for every $\lambda \in [0,1]$ there exists a sequence of four basic mass operations transforming M into the constellation that one obtains when the ith and i'th pairs are replaced by the pairs

$$(m_i, a_i + \lambda(c_{i,i'} - a_i))$$

and

$$(m_{i'}, a_{i'} + \lambda(c_{i,i'} - a_{i'}))$$

(which must be correctly put into the ordering).

Proof. The idea is that the masses m_i and $m_{i'}$ "exchange" a suitable mass $0 \leq m_e \leq \min\{m_i, m_{i'}\}$, i.e., that both masses are split into two parts, one of which is equal to m_e in both cases, and the union operation is applied twice to the remaining mass with the m_e-part of the other mass. Hence four basic operations are required. Because the choice $m_e = 0$ leaves m_i and $m_{i'}$ unchanged, whereas $m_e = \min\{m_i, m_{i'}\}$ corresponds to mass union, and since the result depends linearly on m_e, every position of m_i and $m_{i'}$ on their connecting line such that the masses are closer to each other, and such that the center of gravity remains unchanged, can be achieved this way. More explicitly, the mass m_e must be chosen as $\lambda \cdot \min\{m_i, m_{i'}\}$. □

IV. Efficiently Checking for Simulatability

A. The Binary Case

We have now established the mechanical model and the necessary techniques for our characterizations of simulatability. In Corollary 3 we give a simple and efficiently verifiable, both necessary and sufficient condition for simulatability with respect to a *binary* random variable Y. Furthermore, the proof of Theorem 2 additionally shows that the corresponding channel $P_{\overline{X}|Z}$ can even be computed efficiently.

We first define what it means that a one-dimensional mass constellation is "more centered" than another. This relation leads to the characterization we are looking for. Note that this relation is not a total ordering of the set of constellations: When considering two random mass constellations, typically no one will be more centered than the other (see Figure 6).

Definition 3: For a one-dimensional mass constellation M and for $0 < t \leq 1$, we denote by $\ell_t(M)$ the leftmost masses of M of total amount t. (Typically, of one of the masses in M, only a part will be in $\ell_t(M)$.) A constellation M' is called *more centered* than M, denoted by

$$M' \prec M \ ,$$

if for all t,

$$c(\ell_t(M')) \geq c(\ell_t(M))$$

holds, where $c(S)$ stands for the center of gravity of a set S of masses.

Note first that this is a symmetric notion, i.e., that "left" and "$\geq$" could be replaced by "right" and "$\leq$" without changing the definition. Given two (finite) mass constellations, this quantity can be efficiently checked (i.e., in time linear in the total number of masses—there cannot exist a more efficient algorithm since all the masses have to be taken into account). To see this, note that $M' = (m'_j, a'_j)_{j=1,\ldots,\ell'} \prec M$ is equivalent to the fact that for every $1 \leq k < \ell'$, the center of the set of masses $m'_1, \ldots, m'_k$ is not left of (i.e., smaller than) the center of $\ell_{m'_1+\cdots+m'_k}(M)$.

Theorem 2: Let two equicentered one-dimensional mass constellations M and M' be given. Then M is stronger than M' if and only if M' is more centered than M:

$$M \rightsquigarrow M' \iff M' \prec M \ .$$

Clearly, Corollary 3 follows immediately from Theorems 1 and 2.

Corollary 3: Let P_{XYZ} be the joint distribution of random variables X, Y, and Z, where Y is binary. Then X is simulatable by Z with respect to Y if and only if $M_{X \leftarrow Y}$ is more centered than $M_{Z \leftarrow Y}$, i.e.,

$$\mathrm{sim}_Y(Z \to X) \iff M_{X \leftarrow Y} \prec M_{Z \leftarrow Y} \ .$$

Proof of Theorem 2. We assume first that

$$M' = (m'_j, a'_j)_{j=1,\ldots,\ell'} \prec M = (m_i, a_i)_{i=1,\ldots,\ell}$$

holds. We show by induction that for every $0 \leq j_0 \leq \ell'$, there exists a sequence of basic mass operations that transforms M into a constellation $M_{j_0} = (\overline{m}_k, \overline{a}_k)_{k=1,\ldots,\overline{\ell}}$ such that for every $j \leq j_0$, there exists $k(j)$ (where $k(j) \neq k(j')$ if $j \neq j'$) with $\overline{m}_{k(j)} = m'_j$ and $\overline{a}_{k(j)} \leq a'_j$, and such that the center of the masses $\overline{m}_1, \ldots, \overline{m}_{j_0}$ of M_{j_0} is equal to $c(\ell_{\overline{m}_1+\cdots+\overline{m}_{j_0}}(M))$.

Clearly, this holds for $j_0 = 0$. We assume that the statement is true for $0 \leq j_0 < \ell'$ and show its validity also for $j_0 + 1$. Let $M_{j_0} = (\overline{m}_k, \overline{a}_k)_{k=1,\ldots,\overline{\ell}}$ be defined as above.

We transform M_{j_0} into M_{j_0+1} as follows. First, the leftmost among the masses $\overline{m}_{j_0+1}$,$\overline{m}_{j_0+2}, \ldots$, of total amount m'_{j_0+1}, are united into their center of gravity. Let $(\overline{m}_{j_0+1}, \overline{a}_{j_0+1}) = (m'_{j_0+1}, \overline{a}_{j_0+1})$ be the resulting mass. Then, because of $M' \prec M$ and by the induction assumption, the center of the masses $(\overline{m}_1, \overline{a}_1), \ldots, (\overline{m}_{j_0+1}, \overline{a}_{j_0+1})$ is not on the right-hand side of the center of gravity of $\ell_{m'_1+\ldots+m'_{j_0+1}}(M')$. Hence there exists a sequence of mass approaches, applied only to masses among $\overline{m}_1, \ldots, \overline{m}_{j_0+1}$, such that each of the resulting masses (still of the same sizes) is on the left-hand side of (or at the same position as) the corresponding mass of M' (see Figure 8). Hence this new constellation satisfies the induction assumption for $j_0 + 1$, and this concludes the induction argument.

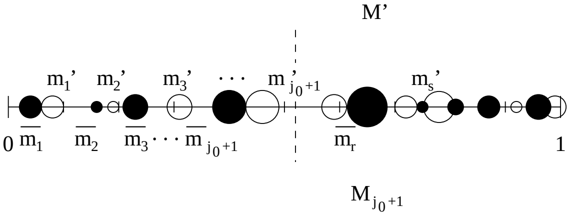

Fig. 8. M' and M_{j_0+1}

Therefore M is stronger than some $\overline{M}$ satisfying the above property, with respect to M', for $j_0 = \ell'$. However, because $\overline{M}$ and M' are both equicentered to M, and because all masses of $\overline{M}$ lie, roughly speaking, on the left of (or at the same place as) the corresponding masses of M', we must have that $\overline{M} = M'$, hence $M \rightsquigarrow M'$.

We show the necessity of the condition $M' \prec M$ for $M \rightsquigarrow M'$ to hold. Assume for M and M' and for some t that

$$c(\ell_t(M')) < c(\ell_t(M)).$$

Then $M \not\rightsquigarrow M'$ holds because the basic mass operations, i.e., mass union (mass splitting leaves all the centers unchanged), can only move the center of the set $\ell_t(M)$ to the right (union of two masses, one in the set $\ell_t(M)$, and one in the complement) or leave it at the same place (union within $\ell_t(M)$ or within its complement). □

The criterion for simulatability of Corollary 3 is simple and verifiable in linear time. Moreover, the proof of Theorem 2 also shows how a channel $P_{\overline{X}|Z}$ for simulating X with respect to Y can be constructed efficiently.

B. The General Case

Let us now, after the complete analysis of the case of a binary random variable Y, consider the general case again. In Definition 4, we give a straight-forward, and also efficiently checkable, generalization of the notion that a constellation is more centered than another. This leads to a *necessary* criterion for simulatability (Theorem 5). However, although it appears to be sufficient as well in many cases, we give an example for which non-simulatability is not detected by the criterion.

Definition 4: Let M and M' be two N-dimensional mass constellations. Let furthermore a line L, passing through the origin, be given. We now consider the orthogonal projections of all the masses in the N-dimensional space onto L. This yields two one-dimensional equicentered mass constellations M_L and M'_L. We say that M' is *more centered* than M, $M' \prec M$, if $M'_L \prec M_L$ for every line L.
It is not difficult to see that also in N dimensions $M \rightsquigarrow M'$ can only hold if $M' \prec M$ holds. The reason is that $M_L \rightsquigarrow M'_L$ follows from $M \rightsquigarrow M'$: Projections of mass operations are mass operations again.

Theorem 4: Let M and M' be N-dimensional equicentered mass constellations. If M is stronger than M', then M' must be more centered than M:

$$M \rightsquigarrow M' \implies M' \prec M\ .$$

Corollary 5: Let P_{XYZ} be the joint distribution of X, Y, and Z. If $M_{X \leftarrow Y}$ is *not* more centered than $M_{Z \leftarrow Y}$, then X is *not* simulatable by Z with respect to Y, i.e.,

$$M_{X \leftarrow Y} \not\prec M_{Z \leftarrow Y} \implies$$
$$\text{sim}_Y(Z \rightarrow X) \ \text{ does } \textit{not} \text{ hold}\ .$$

Note that this condition is, despite the fact that the number of lines through the origin is infinite, efficiently verifiable since the number of points is finite. First, not every direction, i.e., every line, has to be checked separately. There are only at most $\binom{\ell+\ell'}{2}$ directions for which the mass constellations are different (with respect to the order of the masses), where ℓ and ℓ' are the numbers of masses in M and M', respectively. Equal orders means that, in the N-dimensional space, the same masses are "leftmost." Hence, all these directions can be treated simultaneously by looking at extremal directions. Furthermore, only the values t corresponding to a subset of the masses in M' have to be considered (as in the one-dimensional case).

Unfortunately, the given condition is not sufficient for simulatability (i.e., for a mass constellation being stronger than another) in the $N(\geq 2)$-dimensional case (although it appears to be a "good" condition failing to detect non-simulatability only with small probability for "random" distributions.) The following is a counterexample.

Example 2: Consider the following two-dimensional mass constellations M and M'.

$$\begin{aligned} M &= (0.2, (0,0))\,, (0.2, (0, 0.5)) \\ &\quad\ (0.2, (0.5, 0))\,, (0.2, (0.5, 0.5)) \\ &\quad\ (0.2, (0.25, 0.25))\,, \end{aligned}$$

$$\begin{aligned} M' &= (0.2, (0.1, 0))\,, (0.2, (0.1, 0.5)) \\ &\quad\ (0.2, (0.4, 0))\,, (0.2, (0.4, 0.5)) \\ &\quad\ (0.1, (0.15, 0.25))\,, (0.1, (0.35, 0.25)) \end{aligned}$$

(see Figure 9).

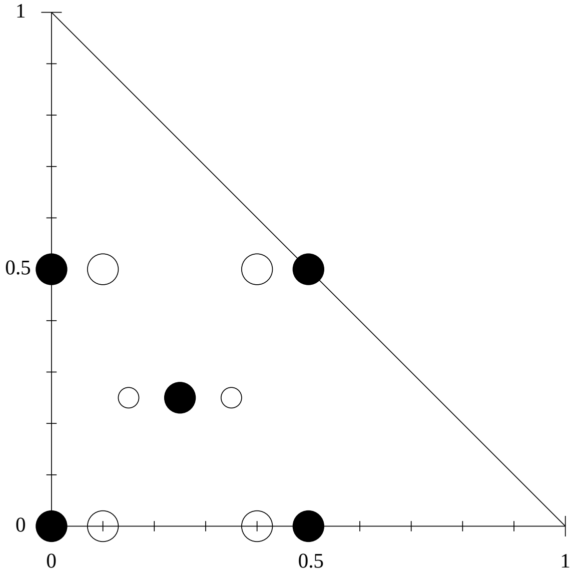

Fig. 9. A 2-Dimensional Counterexample

It is not difficult to see that $M' \prec M$ holds. First, it clearly holds for the horizontal line and, because the (horizontal) distances between neighboring masses change in the same ratios, for all lines except the vertical line, for which the projected constellations are identical however.

On the other hand, M cannot be transformed into M' by basic operations. This is true because when considering the projection to the vertical line, it is clear that no union operation can be made except between masses with the same y-coordinate. However, with such operations only, M can clearly not be transformed to M' because of the masses with y-coordinate $1/2$. Hence $M \not\to M'$ holds.

V. Concluding Remarks

We have analyzed the so-called simulatability condition which is of central importance in the context of unconditionally secure identification and authentication between parties sharing correlated information. For instance, this condition characterizes the possibility of secret-key agreement based on joint randomness in the presence of an active adversary [9]. However, the criterion was not shown to be efficiently verifiable previously; it was not even clear whether it can be checked in finite time.

We have introduced a new mechanical model for representing joint distributions of discrete random variables and their manipulations by noisy channels. This representation in one dimension (i.e., if one of the random variables is binary) leads to a simple necessary and sufficient criterion for simulatability which is verifiable in deterministic time linear in $|\mathcal{X}|+|\mathcal{Y}|+|\mathcal{Z}|$. Moreover, the given algorithm yields the corresponding channel if simulatability does hold. In the general $n\,(\geq 2)$-dimensional case, an apparently close-to-tight (yet not sufficient in all cases) *necessary* criterion, which is checkable in time polynomial in $|\mathcal{X}|+|\mathcal{Y}|+|\mathcal{Z}|$, has been described. It is an open question, however, to find a simple necessary and sufficient criterion for the general case.

The introduced formalism can be helpful also with respect to other problems dealing with discrete distributions and noisy channels. An example is to determine the *intrinsic conditional information* $I(X;Y{\downarrow}Z)$, a quantity that is closely related to the possibility of secret-key agreement against *passive* adversaries [8], [11], [4], [3].

References

[1] R. Ahlswede and I. Csiszár, Common randomness in information theory and cryptography – Part I: secret sharing, *IEEE Transactions on Information Theory*, Vol. 39, No. 4, pp. 1121–1132, 1993.

[2] M. Christandl, R. Renner, and S. Wolf, A property of the intrinsic mutual information, manuscript, 2002.

[3] N. Gisin, R. Renner, and S. Wolf, Linking classical and quantum key agreement: is there a classical analog to bound entanglement?, *Algorithmica*, Vol. 34, pp. 389–412, 2002.

[4] N. Gisin and S. Wolf, Linking classical and quantum key agreement: is there “bound information”?, *Proceedings of CRYPTO 2000*, Lecture Notes in Computer Science, Vol. 1880, pp. 482–500, Springer-Verlag, 2000.

[5] U. M. Maurer, Secret key agreement by public discussion from common information, *IEEE Transactions on Information Theory*, Vol. 39, No. 3, pp. 733–742, 1993.

[6] U. M. Maurer, Information-theoretically secure secret-key agreement by NOT authenticated public discussion, *Advances in Cryptology - EUROCRYPT '97*, Lecture Notes in Computer Science, Vol. 1233, pp. 209–225, Springer-Verlag, 1997.

[7] U. M. Maurer and S. Wolf, Towards characterizing when information-theoretic secret key agreement is possible, *Advances in Cryptology - ASIACRYPT '96*, Lecture Notes in Computer Science, Vol. 1163, pp. 196–209, Springer-Verlag, 1996.

[8] U. M. Maurer and S. Wolf, Unconditionally secure key agreement and the intrinsic conditional information, *IEEE Transactions on Information Theory*, Vol. 45, No. 2, pp. 499–514, 1999.

[9] U. M. Maurer and S. Wolf, Secret-key agreement over unauthenticated public channels – Part I: Definitions and a completeness result, *IEEE Transactions on Information Theory*, 2003.

[10] U. M. Maurer and S. Wolf, Secret-key agreement over unauthenticated public channels – Part III: Privacy amplification, *IEEE Transactions on Information Theory*, 2003.

[11] S. Wolf, *Information-theoretically and computationally secure key agreement in cryptography*, ETH dissertation No. 13138, Swiss Federal Institute of Technology (ETH Zurich), 1999.

[12] A. D. Wyner, The wire-tap channel, *Bell System Technical Journal*, Vol. 54, No. 8, pp. 1355–1387, 1975.