An Efficient Test for the Possibility of Information-Theoretic Key Agreement Secure Against Active Adversaries

Stefan Wolf [1]

Abstract — **We describe a mechanical model for representing discrete distributions and show that it leads to an efficient test for the possibility of key agreement unconditionally secure against active adversaries.**

I. Motivation

Assume that two parties Alice and Bob have access to independent realizations of the random variables X and Y, respectively, and that an adversary Eve knows Z. Let P_{XYZ} be the joint distribution of the three random variables. Can Alice generate a string M such that Bob is convinced that M comes from Alice and not from Eve? Clearly, the answer to this question depends on P_{XYZ}, more precisely, on the following property of P_{XYZ}.

Definition 1. 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 $P_{\overline{X}Y} = \sum P_{YZ} \cdot P_{\overline{X}|Z}$.

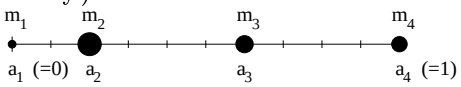
It is not surprising that Eve can impersonate Alice towards Bob if and only if $\mathrm{sim}_Y(Z \to X)$ holds. In case of non-simulatability, the string M can be a sufficiently long block of independent realizations of X.

Another, closely related, application of the simulatability condition is the following. The XYZ-scenario was considered with respect to the question whether Alice and Bob can, by communication over an insecure channel, generate a secret key S about which the adversary has virtually no information. As the important quantities in this context, the secret-key rate $S(X;Y||Z)$, with respect to *passive* adversaries, and the *robust* secret-key rate $S^*(X;Y||Z)$, secure against *active* adversaries with complete control over the communication channel, were defined [1]. It was shown that either $S^*(X;Y||Z) = S(X;Y||Z)$ or $S^*(X;Y||Z) = 0$ holds, and that the simulatability condition separates the two cases: If neither $\mathrm{sim}_Y(Z \to X)$ nor $\mathrm{sim}_X(Z \to Y)$ holds, then secret-key agreement secure against active adversaries is possible at the same rate as against passive wire-tappers, but completely impossible otherwise.

Unfortunately, the simulatability condition is a priori not very helpful since it is not clear how it can be verified in finite time, let alone efficiently. It is the goal of this note to present a new intuitive formalism based on a mechanical model, and to show that this leads to efficient criteria for simulatability.

II. A Mechanical Model for Discrete Distributions and Channels

Let us consider the following representation of joint distributions of discrete random variables U and V. For simplicity, we assume that V is binary, i.e., $\mathcal{V} = \{v_0, v_1\}$. Then the constellation $M_{U \leftarrow V}$ is defined by the list of pairs $M_{U \leftarrow V} := (P_U(u), P_{V|U=u}(v_0))_{U \in \mathcal{U}}$. The pairs of such a constellation $M = (m_i, a_i)_{i=1\ldots l}$ can be represented as mass points in the interval $[0, 1]$, where m_i determines the mass of a point, and a_i is its position. (This representation is one-dimensional because V is binary.)



Definition 2. Let $M = (m_i, a_i)_{i=1\ldots l}$ be a constellation with $\sum m_i = 1$. The center of gravity of M is defined as $\sum m_i a_i$. We say that a constellation $M' = (m'_i, a'_i)_{i=1,\ldots,l'}$ is derived from M by *mass splitting* if it arises from M by replacing a pair (m_i, a_i) by two pairs (pm_i, a_i) and $((1-p)m_i, a_i)$ for some $0 \leq p \leq 1$. Furthermore, M' is derived from M by *mass union* if two pairs (m_i, a_i) and (m_j, a_j) are replaced by the single pair $(m_i + m_j, (m_i a_i + m_j a_j)/(m_i + m_j))$, corresponding to the sum mass in the center of gravity of the two masses. 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'.

Note first that $\mathrm{sim}_Y(Z \to X)$ is equivalent to $M_{Z \leftarrow Y} \rightsquigarrow M_{X \leftarrow Y}$. The reason is that a channel $P_{\overline{X}|Z}$ can be translated into a sequence of basic mass operations in the mechanical model, and vice versa. However, this does not directly lead to an efficiently verifiable criterion for simulatability. It is only a reformulation of the condition. We now define a property of a pair of mass constellations which is efficiently checkable and equivalent to one constellation being stronger than the other.

Definition 3. For a mass constellation M and for $0 < t \leq 1$, we denote by $\ell_t(M)$ the leftmost masses of M of total amount t. 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.

Given two mass constellations M and M', this condition can be checked in linear time. Indeed, note that $M' \prec M$ is equivalent to the fact that for every $1 \leq k < l'$, 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 1. *Let P_{XYZ} be the joint distribution of random variables X, Y, and Z, where Y is binary. Then $\mathrm{sim}_Y(Z \to X)$ is equivalent to $M_{X \leftarrow Y} \prec M_{Z \leftarrow Y}$.*

If Y is N-ary, the distribution can be represented in an $(N-1)$-dimensional space. However, the straight-forward generalization of the above condition is not always sufficient. It is an open problem to find an efficient test for the general case.

References

[1] U. Maurer, "Information-theoretically secure secret-key agreement by NOT authenticated public discussion," *EUROCRYPT '97*, LNCS, vol. 1233, pp. 209–225, 1997.

[1] Department of Computer Science, ETH Zürich, CH–8092 Zürich, Switzerland. E-mail: wolf@inf.ethz.ch