Random Systems: Theory and Applications

Ueli Maurer

Department of Computer Science, ETH Zurich
maurer@inf.ethz.ch

Abstract. This short note accompanies the author's keynote lecture delivered at ICITS' 07. The concept of a random system is explained and a few results in the theory of random systems are mentioned.

1 Random Systems

Many cryptographic systems (e.g. a block cipher, the CBC-MAC construction, or more complex games) can be modeled as discrete systems. A discrete system interacts with its environment by taking a (generally unbounded) sequence of inputs $X_1, X_2, \ldots$ (from some alphabet $\mathcal{X}$) and generating, for each new input X_i, an output Y_i (from some alphabet $\mathcal{Y}$). The abstraction of the input-output behavior of such a discrete system, say $\mathbf{F}$, is captured by the following definition of [Mau02]. We also refer to [MPR07] for an introduction to random systems.

Definition 1. An $(\mathcal{X}, \mathcal{Y})$-*random system* $\mathbf{F}$ is a (generally infinite) sequence of conditional probability distributions $\mathsf{p}^{\mathbf{F}}_{Y_i|X^iY^{i-1}}$ for $i \geq 1$.[1]

This description of a system is exact and minimal in the sense that two systems, say $\mathbf{F}$ and $\mathbf{G}$, with different input-output behavior correspond to two different random systems, and two different random systems have different input-output behavior. Two systems $\mathbf{F}$ and $\mathbf{G}$ are *equivalent*, denoted $\mathbf{F} \equiv \mathbf{G}$, if they correspond to the same random system.

2 Indistinguishability and Game-Winning

Two major paradigms for cryptographic security definitions are:

- **Indistinguishability:** An ideal-world system is indistinguishable from a real-world system. For example, a secure encryption scheme can be seen as realizing a secure channel (ideal world) from an authenticated channel (real world).
- **Game-winning:** Breaking a system means that the adversary must achieve a certain goal, i.e., win a certain game. For example, a MAC is secure if the adversary cannot generate a fresh message together with the correct MAC, even if he can query the system arbitrarily.

[1] For arguments x^{i-1} and y^{i-1} such that $\mathsf{p}^{\mathbf{F}}_{Y^{i-1}|X^{i-1}}(y^{i-1}, x^{i-1}) = 0$, $\mathsf{p}^{\mathbf{F}}_{Y_i|X^iY^{i-1}}$ need not be defined.

Y. Desmedt (Ed.): ICITS 2007, LNCS 4883, pp. 44–45, 2009.

A game can be modeled as a random system with a special monotone binary output (MBO) which indicates whether or not the game has been won. Indeed, an important paradigm in indistinguishability proofs, made formal in [Mau02], is the definition of such an internal monotone condition in a system such that for any distinguisher $\mathbf{D}$ the distinguishing advantage can be shown to be upper bounded by the probability that $\mathbf{D}$ provokes this condition.

In [MPR07], the converse was proved, which we state informally: For two systems $\mathbf{F}$ and $\mathbf{G}$ one can always define new systems $\hat{\mathbf{F}}$ and $\hat{\mathbf{G}}$, which are equivalent to $\mathbf{F}$ and $\mathbf{G}$, respectively, but have an additional MBO, such that

(i) for any distinguisher $\mathbf{D}$ the distinguishing advantage for $\mathbf{F}$ and $\mathbf{G}$ is equal to the probability that $\mathbf{D}$ sets the MBO to 1 in $\hat{\mathbf{F}}$ (or $\hat{\mathbf{G}}$), and
(ii) the systems $\hat{\mathbf{F}}$ and $\hat{\mathbf{G}}$ are equivalent as long as the respective MBOs are 0.

3 An Application: Indistinguishability Amplification

Since analyzing game-winning for a combined game consisting of sub-games appears to be considerably simpler than analyzing the indistinguishability of combined systems, the above mentioned correspondence is very useful for proving amplification results of the following types (see [MPR07]).

Let $\mathbf{F}$ and $\mathbf{G}$ be systems for which the best distinguisher's advantage in distinguishing it from a uniform random function $\mathbf{R}$ within k queries is bounded by ϵ and ϵ', respectively. Then $\mathbf{F} \star \mathbf{G}$, the system consisting of $\mathbf{F}$ and $\mathbf{G}$ in parallel with their outputs combined by the group operation $\star$, can be distinguished with advantage at most $2\epsilon\epsilon'$ from $\mathbf{R}$ (for k queries). This bound is optimal. Another amplification result states that the optimal (adaptive) distinguishing advantage for $\mathbf{F} \star \mathbf{G}$ and $\mathbf{R}$ is bounded by the sum of the *non-adaptive* distinguishing advantages for $\mathbf{F}$ and $\mathbf{G}$.

The combination operation $\mathbf{F} \star \mathbf{G}$ can be generalized as follows, and the above results, appropriately generalized, hold for the general setting. Let $\mathbf{F}$ and $\mathbf{I}$ (and similarly $\mathbf{G}$ and $\mathbf{J}$) be systems for which the distinguishing advantage (of some type) is known to be bounded. A construction $\mathbf{C}(\cdot, \cdot)$ invoking two subsystems is called *neutralizing* for the pairs $(\mathbf{F}, \mathbf{I})$ and $(\mathbf{G}, \mathbf{J})$ of systems if

$$\mathbf{C}(\mathbf{F}, \mathbf{J}) \equiv \mathbf{C}(\mathbf{I}, \mathbf{G}) \equiv \mathbf{C}(\mathbf{I}, \mathbf{J}) \equiv \mathbf{Q}$$

(for some $\mathbf{Q}$). To obtain the above results one sets $\mathbf{C}(\mathbf{F}, \mathbf{G}) := \mathbf{F} \star \mathbf{G}$, $\mathbf{I} := \mathbf{R}$, $\mathbf{J} := \mathbf{R}$, and $\mathbf{Q} := \mathbf{R}$.

References

[Mau02] Maurer, U.: Indistinguishability of random systems. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 110–132. Springer, Heidelberg (2002)

[MPR07] Maurer, U., Pietrzak, K., Renner, R.: Indistinguishability amplification. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 130–149. Springer, Heidelberg (2007)