Conditional Equivalence of Random Systems and Indistinguishability Proofs

Ueli Maurer
Department of Computer Science
ETH Zurich
Switzerland
Email: maurer@inf.ethz.ch

***Abstract*—A random system is the mathematical object capturing the notion of a (probabilistic) interactive system that replies to every input X_i ($i = 1, 2, \ldots$) with an output Y_i. A distinguisher $\mathbf{D}$ for two systems $\mathbf{S}$ and $\mathbf{T}$ can adaptively generate inputs, receives the corresponding outputs, and after some number q of inputs guesses which system it is talking to, $\mathbf{S}$ or $\mathbf{T}$. Two systems are indistinguishable if for all distinguishers (in a certain class) the distinguishing advantage is very small.**

Indistinguishability proofs are of great importance because many security proofs in cryptography amount to the proof that two appropriately defined systems (sometimes called a real and an ideal system) are indistinguishable. In this paper we provide a general technique for proving the indistinguishability of two systems making use of the concept of conditional equivalence of systems.

I. Introduction

Discrete systems are of crucial importance in cryptography. Many cryptographic concepts (e.g. an encryption scheme, a message authentication scheme, etc.) can be described as a discrete system that takes a sequence of inputs (e.g. messages) and for each input generates an output (e.g. a ciphertext).

The security of a cryptographic system is often defined via the indistinguishability of two discrete systems. For example, a so-called block cipher is an encryption scheme that encrypts a plaintext block (of a certain bit-length), using a secret key, to a ciphertext block of the same length. The strongest security definition for a block cipher is that, without knowledge of the secret key, it is indistinguishable from a uniform bijective random function, a so-called uniform random permutation (URP). By indistinguishable one means that any feasible (often formalized as polynomial-time) algorithm can achieve at most a negligible distinguishing advantage, where negligible is also appropriately defined.

Indistinguishability proofs are of crucial importance in cryptography; they are at the core of many cryptographic security proofs. In this paper we propose a very general technique for proving indistinguishability. Many known (and new) results on indistinguishability can be obtained as simple applications of Theorem 3. Due to space limitations we only give one short application, the proof of the well-known so-called PRP-PRF switching lemma, whose previous proofs were substantially more involved.

The paper makes use of the random systems framework of [2] (see also [3]). Theorem 3 was already mentioned without proof in [2].

II. Discrete Interactive Systems

Definition 1. An $(\mathcal{X}, \mathcal{Y})$-*system* takes inputs $X_1, X_2, \ldots$ (from some alphabet $\mathcal{X}$) and generates, for each new input X_i, an output Y_i (from some alphabet $\mathcal{Y}$).[1] The output Y_i depends (possibly probabilistically) on the current input X_i and on the internal state.

***Example* 1.** A *(uniform) random function (URF)* from some domain $\mathcal{X}$ to some finite range $\mathcal{Y}$ (typically $\mathcal{X} = \{0,1\}^m$ for some m or $\mathcal{X} = \{0,1\}^*$, and $\mathcal{Y} = \{0,1\}^n$ for some n) is an $(\mathcal{X}, \mathcal{Y})$-system that replies to every query X_i with a uniformly random value $Y_i \in \mathcal{Y}$, but it replies consistently when a previous input is repeated, i.e., $X_i = X_j \Longrightarrow Y_i = Y_j$. A URF can either be thought of as being generated on the fly, as just described, or if $|\mathcal{X}|$ is finite it can be thought of as consisting of a randomly selected function table $\mathcal{X} \to \mathcal{Y}$ embedded in the system.

A *(uniform) random permutation (URP)* for domain $\mathcal{X}$ is a uniform random bijective function $\mathcal{X} \to \mathcal{X}$.

Definition 2. Consider two $(\mathcal{X}, \mathcal{Y})$-systems $\mathbf{S}$ and $\mathbf{T}$. For an operation $\star$ on $\mathcal{Y}$ (typically the operation $\oplus$ on $\{0,1\}^n$) the system $\mathbf{S} \star \mathbf{T}$ is the $(\mathcal{X}, \mathcal{Y})$-systems where the input is given to both $\mathbf{S}$ and $\mathbf{T}$ and their outputs are combined using $\star$ to obtain the output of $\mathbf{S} \star \mathbf{T}$.

III. The Input-Output Behavior of Discrete Systems

A. Describing the Behavior

The *input-output behavior*[2] of an $(\mathcal{X}, \mathcal{Y})$-system $\mathbf{S}$ is characterized completely by the sequence

$$\mathsf{p}^{\mathbf{S}}_{Y^i|X^i} \quad \text{for } i \geq 1$$

[1] It is not a relevant restriction to consider fixed input and output alphabets. This allows to model also systems where inputs and outputs come from different alphabets for different i.

[2] All statements about systems we are interested in, like the maximal distinguishing advantage of two systems, depend only on the observable *input-output behavior* of the system. The internals of a system (e.g. the state) are irrelevant if they can never be observed. Two systems with the same input-output behavior are equivalent in the sense that, if plugged into any environment (e.g. any application), they will behave identically. Hence replacing a system by an equivalent system has no effect in the environment. Therefore the particular language for describing systems (e.g. by pseudo-code) is irrelevant, as long as the behavior is fully specified by the description.

978-1-4799-0446-4/13/$31.00 ©2013 IEEE

of conditional probability distributions.[3]

Note that the conditional distribution $\mathsf{p}^{\mathbf{S}}_{Y^i|X^i}$ implies the conditional distributions $\mathsf{p}^{\mathbf{S}}_{Y^j|X^j}$ for all $j < i$, and hence the above description of the behavior of a system is redundant. The conditional distributions $\mathsf{p}^{\mathbf{S}}_{Y^i|X^i}$ must satisfy a consistency condition which ensures that Y_i does not depend on $X_{i+1}, X_{i+2}, \ldots$. We discuss this condition below in Section III-C. But if we describe a system $\mathbf{S}$ by its distributions $\mathsf{p}^{\mathbf{S}}_{Y^i|X^i}$, the consistency condition is of course automatically satisfied. A system answering only a certain number (say n) of queries is completely characterized by $\mathsf{p}^{\mathbf{S}}_{Y^n|X^n}$.

***Example* 2.** A $\mathcal{Y}$*-beacon*, often denoted as $\mathbf{B}$, is a system which outputs a new independent and uniformly distributed (over $\mathcal{Y}$) output Y_i for every new input X_i. The input alphabet $\mathcal{X}$ and the choice of an input are not relevant. In other words,

$$\mathsf{p}^{\mathbf{B}}_{Y^i|X^i}(y^i, x^i) = 1/|\mathcal{Y}|^i$$

for all y^i and for all x^i. A beacon for $\mathcal{X} = \{0,1\}^m$ and $\mathcal{Y} - \{0,1\}^n$ is denoted as $\mathbf{B}_{m,n}$.

B. Equivalence of Systems

Definition 3. Two systems $\mathbf{S}$ and $\mathbf{T}$ are *equivalent*, denoted

$$\mathbf{S} \equiv \mathbf{T},$$

if they have the same behavior, i.e., if for all $i \geq 1$

$$\mathsf{p}^{\mathbf{S}}_{Y^i|X^i} = \mathsf{p}^{\mathbf{T}}_{Y^i|X^i}.$$

***Example* 3.** If $\mathbf{B}'$ is a $\mathcal{Y}$-beacon (i.e., $\mathbf{B}' \equiv \mathbf{B}$) and $\mathbf{S}$ is any system for the same $\mathcal{Y} = \{0,1\}^n$, then the system $\mathbf{B}' \oplus \mathbf{S}$ resulting by feeding an input to both $\mathbf{B}$ and $\mathbf{S}$ and XORing the outputs (see Definition 2) satisfies

$$\mathbf{B}' \oplus \mathbf{S} \;\equiv\; \mathbf{B}.$$

Similarly, If $\mathbf{R}'$ is a URF (i.e., $\mathbf{R}' \equiv \mathbf{R}$) and $\mathbf{S}$ is any random function, then $\mathbf{R}' \oplus \mathbf{S} \;\equiv\; \mathbf{R}$.

C. Definition of the Behavior of a System, Random Systems

We can define the following conditional distributions:

$$\mathsf{p}^{\mathbf{S}}_{Y_i|X^iY^{i-1}}(y_i, x^i, y^{i-1}) \;=\; \frac{\mathsf{p}^{\mathbf{S}}_{Y^i|X^i}(y^i, x^i)}{\mathsf{p}^{\mathbf{S}}_{Y^{i-1}|X^{i-1}}(y^{i-1}, x^{i-1})}.$$

This sequence of conditional distributions is the minimal, redundancy-free description of the behavior of an $(\mathcal{X}, \mathcal{Y})$-system $\mathbf{S}$.[4] In other words, every such sequence corresponds to the behavior of a system, and two different such sequences correspond to different systems.

[3]As usual, we denote probabilities and conditional probabilities in a random experiment by P, but in contrast, conditional probability distributions defined in isolation (without a random experiment being defined) are denoted by the small letter p. Note that $\mathsf{p}^{\mathbf{S}}_{Y^i|X^i}$ is *not* a conditional distribution in a random experiment because the distribution of X^i is not defined.

[4]The consistency condition for the conditional distributions $\mathsf{p}^{\mathbf{S}}_{Y^i|X^i}$ is that $\mathsf{p}^{\mathbf{S}}_{Y_i|X^iY^{i-1}}$ defined above is indeed a conditional probability distribution, for all i.

For a system $\mathbf{S}$ we define the mathematical type of the input-output behavior of a discrete system and call it a *random system*. As already mentioned, for an $(\mathcal{X}, \mathcal{Y})$-system, every output Y_i depends (at most) on $X_1, \ldots, X_i$ and $Y_1, \ldots, Y_{i-1}$.

Definition 4. The *behavior* of an $(\mathcal{X}, \mathcal{Y})$-system $\mathbf{S}$ is a (possibly infinite) sequence of conditional probability distributions $\mathsf{p}^{\mathbf{S}}_{Y_i|X^iY^{i-1}}$ for $i \geq 1$.[5]

Note that two systems are equivalent if and only if they have the same behavior. The behavior of a system defines an equivalence class of systems (with the same behavior). The behavior is a valid (canonical) description of a system.

Definition 5. The system $\mathbf{S}$ defined by a behavior $\mathsf{p}^{\mathbf{S}}_{Y_i|X^iY^{i-1}}$ for $i \geq 1$ is called the corresponding $(\mathcal{X}, \mathcal{Y})$*-random system*.

For a system $\mathbf{S}$, the behavior description of the redundant form $\mathsf{p}^{\mathbf{S}}_{Y^i|X^i}$ is usually easier to work with than the form $\mathsf{p}^{\mathbf{S}}_{Y_j|X^jY^{j-1}}$. We discuss two examples of system behavior.

***Example* 4.** For a $\mathcal{Y}$*-beacon* we have $\mathsf{p}^{\mathbf{B}}_{Y_i|X^iY^{i-1}} = 1/|\mathcal{Y}|$ for all choices of the arguments.

***Example* 5.** For a URF $\mathbf{R}$ we have

$$\mathsf{p}^{\mathbf{R}}_{Y_i|X^iY^{i-1}}(y_i, x^i, y^{i-1}) = \begin{cases} 1 & \text{if } x_i = x_j \text{ for some } j < i \text{ and } y_i = y_j \\ 0 & \text{if } x_i = x_j \text{ for some } j < i \text{ and } y_i \neq y_j \\ 1/|\mathcal{Y}| & \text{else.} \end{cases}$$

$\mathsf{p}^{\mathbf{R}}_{Y_i|X^iY^{i-1}}(y_i, x^i, y^{i-1})$ is undefined if $x_j = x_k$ and $y_j \neq y_k$ for some $j < k < i$.

IV. Distinguishers for $(\mathcal{X}, \mathcal{Y})$-Systems

Consider the problem of distinguishing two $(\mathcal{X}, \mathcal{Y})$-systems $\mathbf{S}$ and $\mathbf{T}$ by means of a (possibly probabilistic) adaptive distinguisher $\mathbf{D}$ asking at most q queries, for some q. Such a $\mathbf{D}$ generates X_1 as an input to $\mathbf{S}$ (or $\mathbf{T}$), receives the output Y_1, then generates X_2, receives Y_2, etc. Finally, after receiving Y_q, it outputs a binary decision bit.

Definition 6. A *distinguisher* $\mathbf{D}$ *for* $(\mathcal{X}, \mathcal{Y})$*-systems* is a system that behaves like a $(\mathcal{Y}, \mathcal{X})$-system that generates its first output X_1 before receiving the first input Y_1, and which outputs a bit Z (at a separate interface) after a certain number q of queries. More precisely, the behavior of a distinguisher is described by the conditional distributions $\mathsf{p}^{\mathbf{D}}_{X_i|Y^{i-1}X^{i-1}}$ for all i, as well as the conditional distribution $\mathsf{p}^{\mathbf{D}}_{Z|X^qY^q}$.

Definition 7. A distinguisher $\mathbf{D}$ is *non-adaptive* if it ignores the outputs of the system it is connected to, i.e., if $\mathsf{p}^{\mathbf{D}}_{X_i|Y^{i-1}X^{i-1}} = \mathsf{p}^{\mathbf{D}}_{X_i|X^{i-1}}$ for $i \geq 1$. By NA we denote the

[5]Recall that such a conditional probability distribution is a function $\mathcal{Y} \times \mathcal{X}^i \times \mathcal{Y}^{i-1} \to R^+$ such that for all choices of the arguments x^i and y^{i-1}, the sum of the function values over the choices y_i equals 1. Note also that for arguments x^i and y^{i-1} such that $\mathsf{p}^{\mathbf{S}}_{Y^{i-1}|X^i}(y^{i-1}, x^i) = 0$, $\mathsf{p}^{\mathbf{S}}_{Y_i|X^iY^{i-1}}$ need not be defined.

class of computationally unbounded *non-adaptive* distinguishers. For a distinguisher $\mathbf{D}$ (for $(\mathcal{X},\mathcal{Y})$-systems) and an $(\mathcal{X},\mathcal{Y})$-system $\mathbf{T}$ we denote by $[\![\mathbf{DT}]\!]$ the *non-adaptive* distinguisher for $(\mathcal{X},\mathcal{Y})$-systems that generates X^q by interacting with $\mathbf{T}$ to generate a transcript (X^q,Y^q), ignoring Y^q (see Figure 1).

When a distinguisher $\mathbf{D}$ is connected to a system $\mathbf{S}$, resulting in the system $\mathbf{DS}$, this defines a random experiment. The probabilities of an event $\mathcal{E}$ in this experiment will be denoted as $\mathsf{P}^{\mathbf{DS}}(\mathcal{E})$. The probability distribution $\mathsf{P}^{\mathbf{DS}}_{X^qY^q}$ of the transcript (X^q,Y^q) can be expressed as

$$\begin{aligned}&\mathsf{P}^{\mathbf{DS}}_{X^qY^q}(x^q,y^q)\\ &=\prod_{i=1}^{q}\mathsf{p}^{\mathbf{D}}_{X_i|X^{i-1}Y^{i-1}}(x_i,x^{i-1},y^{i-1})\cdot\mathsf{p}^{\mathbf{S}}_{Y_i|X^iY^{i-1}}(y_i,x^i,y^{i-1})\\ &=\ \mathsf{p}^{\mathbf{D}}_{X^q|Y^{q-1}}(x^q,y^{q-1})\cdot\mathsf{p}^{\mathbf{S}}_{Y^q|X^q}(y^q,x^q)\ ,\end{aligned}\tag{1}$$

where we have made use of

$$\mathsf{p}^{\mathbf{S}}_{Y^q|X^q}(y^q,x^q)\ =\ \prod_{i=1}^{q}\mathsf{p}^{\mathbf{S}}_{Y_i|X^iY^{i-1}}(y_i,x^i,y^{i-1})$$

(and similarly for $\mathbf{D}$).[6]

Definition 8. The *advantage* of distinguisher $\mathbf{D}$ for random systems $\mathbf{S}$ and $\mathbf{T}$, for q queries, denoted $\Delta^{\mathbf{D}}_q(\mathbf{S},\mathbf{T})$, is defined as

$$\Delta^{\mathbf{D}}_q(\mathbf{S},\mathbf{T})\ :=\ \left|\mathsf{P}^{\mathbf{DS}}(Z=1)-\mathsf{P}^{\mathbf{DT}}(Z=1)\right|.$$

For a class $\mathcal{D}$ of distinguishers, the advantage of the best $\mathbf{D}$ in $\mathcal{D}$, asking at most q queries, is denoted as

$$\Delta^{\mathcal{D}}_q(\mathbf{S},\mathbf{T})\ :=\ \sup_{\mathbf{D}\in\mathcal{D}}\Delta^{\mathbf{D}}_q(\mathbf{S},\mathbf{T}).$$

For the class of *all* distinguishers asking at most q queries we simply write $\Delta_q(\mathbf{S},\mathbf{T})\ :=\ \sup_{\mathbf{D}}\Delta^{\mathbf{D}}_q(\mathbf{S},\mathbf{T})$.

V. Games and Game-winning

A. The Game Concept

An important paradigm in certain security definitions is the notion of winning a game (see [3]). A game is an interactive process where the goal is to reach a particular final state which one could call the *win state*. Here we consider games played by a *single* entity[7], namely the (hypothetical) adversary or the attacker. The security of certain cryptographic schemes is defined as a game, and the definition states that it is infeasible or otherwise impossible to win the game, except with negligible probability.

***Example* 6.** The security of a message authentication code (MAC) can be phrased as a game. A MAC for key space $\mathcal{K}$ and with n-bit output is a function

$$m:\ \{0,1\}^*\times\mathcal{K}\to\{0,1\}^n.$$

[6]Note that the conditional distribution $\mathsf{p}^{\mathbf{S}}_{Y^q|X^q}(y^q,x^q)$ describes the behavior of $\mathbf{S}$ for any input sequence x^q, but the actual conditional probability distribution $\mathsf{P}^{\mathbf{DS}}_{Y^q|X^q}$ in the random experiment with $\mathbf{D}$ and $\mathbf{S}$ is *not* equal to $\mathsf{p}^{\mathbf{S}}_{Y^q|X^q}$, as the reader can easily verify. This is one of the reasons for distinguishing between p and P.

[7]In the context of games this is sometimes called a solitary game.

Let $K\in\mathcal{K}$ be a uniformly chosen secret key. In the attack game an adversary can choose arbitrary messages $x\in\{0,1\}^*$ and obtain $m(x,K)$. He can also ask verification queries: For $x\in\{0,1\}^*$ and $y\in\{0,1\}^n$, is $m(x,K)=y$? The adversary wins the game if he produces a fresh message $\overline{x}\in\{0,1\}^*$ and a value $\overline{y}\in\{0,1\}^n$ such that $m(\overline{x},K)=\overline{y}$. A MAC function m is secure if no efficient adversary can win this game with non-negligible probability.

B. Games as Systems

Without loss of generality, a game with one player (e.g. the adversary) can be described as an $(\mathcal{X},\mathcal{Y})$-system which interacts with its environment by taking inputs $X_1,X_2,\ldots$ (considered as moves) and answering with outputs $Y_1,Y_2,\ldots$. In addition, after every input it also outputs a bit indicating whether the game has been won. This bit is monotone in the sense that it is initially set to 0 and that, once it has turned to 1 (the game is won), it can not turn back to 0 (even if playing the game were continued). This motivates the following definition.

Definition 9. For a $(\mathcal{X},\mathcal{Y}\times\{0,1\})$-system $\mathbf{S}$ the binary component A_i of the output (Y_i,A_i) is called a *monotone binary output (MBO)* if $A_i=1$ implies $A_j=1$ for $j\geq i$. Such a system $\mathbf{S}$ with MBO is also called a *game*.

A system $\mathbf{W}$ (which could be called "game winner") interacting with $\mathbf{S}$, trying to win the game defined by $\mathbf{S}$, is like a distinguisher, except that it need not have a binary output. Whether $\mathbf{W}$ "sees" the MBO or not is irrelevant if its only goal is to win the game. The MBO of $\mathbf{S}$ can be thought of as being output at a second interface not accessible to $\mathbf{W}$.

Definition 10. For a $(\mathcal{X},\mathcal{Y}\times\{0,1\})$-random system $\mathbf{S}$ with an MBO (called A_i) and for a system $\mathbf{W}$, we denote with $\Gamma^{\mathbf{W}}_q(\mathbf{S})$ the probability that $\mathbf{W}$ wins the game within q queries:[8]

$$\Gamma^{\mathbf{W}}_q(\mathbf{S})\ :=\ \mathsf{P}^{\mathbf{WS}}(A_q=1).$$

For a class $\mathcal{W}$ of distinguishers, the winning probability of the best $\mathbf{W}$ in $\mathcal{W}$ is denoted as

$$\Gamma^{\mathcal{W}}(\mathbf{S})\ :=\ \sup_{\mathbf{W}\in\mathcal{W}}\Gamma^{\mathbf{W}}(\mathbf{S}).$$

For the class of *all* distinguishers asking at most q queries we simply write $\Gamma_q(\mathbf{S})$.

C. Characterizing the Behavior of Games

Since we are only interested in how the game can be won (but not what happens afterwards), a game $\mathbf{S}$ is characterized completely by the sequence

$$\mathsf{p}^{\mathbf{S}}_{Y_i,A_i=0|X^iY^{i-1},A_{i-1}=0}\qquad\text{for } i\geq 1\tag{2}$$

of conditional probability distributions, where $A_0,A_1,A_2\ldots$ is the sequence of MBOs. This also defines the conditional distributions

$$\mathsf{p}^{\mathbf{S}}_{A_i=1|X^iY^{i-1},A_{i-1}=0}\qquad\text{for } i\geq 1.$$

[8]The notation $\mathsf{P}^{\mathbf{WS}}$ stands for the random experiment consisting of choosing $\mathbf{W}$ and $\mathbf{S}$ independently and letting them interact.

Note that $\mathsf{p}^{\mathbf{S}}_{Y_iA_i|X^iY^{i-1},A_{i-1}=1}$ is not relevant (and in some contexts may not even be defined). Equivalently to (2), the behavior of a game is also characterized by

$$\mathsf{p}^{\mathbf{S}}_{Y^i,A_i=0|X^i} \quad \text{for } i \geq 1.$$

D. Distinguisher Connected to a Game

If a distinguisher (or game winner) $\mathbf{D}$ for $(\mathcal{X},\mathcal{Y})$-systems is connected to a game $\mathbf{S}$, resulting in the system $\mathbf{DS}$, then the joint probability distribution of the transcript (X^q,Y^q) and the event "game not won" is given by

$$\begin{aligned}\mathsf{P}^{\mathbf{DS}}_{X^qY^q,A_q=0}(x^q,y^q) \;&=\\ &= \prod_{i=1}^{q}\Big(\mathsf{p}^{\mathbf{D}}_{X_i|X^{i-1}Y^{i-1}}(x_i,x^{i-1},y^{i-1})\\ &\qquad\cdot \mathsf{p}^{\mathbf{S}}_{Y_i,A_i=0|X^iY^{i-1},A_{i-1}=0}(y_i,x^i,y^{i-1})\Big)\\ &= \mathsf{p}^{\mathbf{D}}_{X^q|Y^{q-1}}(x^q,y^{q-1})\cdot\mathsf{p}^{\mathbf{S}}_{Y^q,A_q=0|X^q}(y^q,x^q), \qquad (3)\end{aligned}$$

and the probability that the game is won within q queries is

$$\begin{aligned}\Gamma^{\mathbf{D}}_q(\mathbf{S}) &= \mathsf{P}^{\mathbf{DS}}(A_q=1)\\ &= 1-\mathsf{P}^{\mathbf{DS}}(A_q=0)\\ &= 1-\sum_{x^q\in\mathcal{X}^q}\sum_{y^q\in\mathcal{Y}^q}\mathsf{P}^{\mathbf{DS}}_{X^qY^q,A_q=0}(x^q,y^q). \qquad (4)\end{aligned}$$

E. Game Equivalence

The following definition captures a restricted type of equivalence of games, capturing only that they behave equivalently *as long as the game is not won*. One could capture this by defining a restricted system which blinds its $\mathcal{Y}$-output as soon as the MBO is 1. Two systems are equivalent as games if their restricted versions are equivalent (as systems). The following definition is an alternative (and more directly useful) formulation of this concept.

Definition 11. Two $(\mathcal{X},\mathcal{Y}\times\{0,1\})$-systems with MBO, $\mathbf{S}$ and $\mathbf{T}$, are *equivalent as games*, denoted $\mathbf{S}\overset{g}{\equiv}\mathbf{T}$, if, for $i\geq 1$,

$$\mathsf{p}^{\mathbf{S}}_{Y^i,A_i=0|X^i} \;=\; \mathsf{p}^{\mathbf{T}}_{Y^i,A_i=0|X^i}.$$

If $\mathbf{S}$ and $\mathbf{T}$ are equivalent as games, it follows from (3) that the probability of any event defined on the transcript (X^q,Y^q) of $\mathbf{D}$ with $\mathbf{S}$ (or with $\mathbf{T}$), which includes the event $A_q=0$, is the same for $\mathbf{S}$ and $\mathbf{T}$. In particular, we have

$$\mathsf{P}^{\mathbf{DS}}(A_q=0) \;=\; \mathsf{P}^{\mathbf{DT}}(A_q=0)$$

and hence, using (4):

Lemma 1. *If $\mathbf{S}\overset{g}{\equiv}\mathbf{T}$, then, for any distinguisher $\mathbf{D}$ for $(\mathcal{X},\mathcal{Y})$-systems and any q,*

$$\Gamma^{\mathbf{D}}_q(\mathbf{S})=\Gamma^{\mathbf{D}}_q(\mathbf{T}).$$

Proof. According to (4), the term $\Gamma^{\mathbf{D}}_q(\mathbf{S})$ is computed as 1 minus the sum of $|\mathcal{X}|^q|\mathcal{Y}|^q$ terms, each of which, according to (3), is identical in the two random experiments (since $\mathsf{p}^{\mathbf{S}}_{Y^q,A_q=0|X^q}=\mathsf{p}^{\mathbf{T}}_{Y^q,A_q=0|X^q}$, see Definition 11). □

VI. Indistinguishability Proofs

A. Relating Game Winning and Distinguishing

For a game it is useful to define the system when the MBO is ignored:

Definition 12. *For an $(\mathcal{X},\mathcal{Y}\times\{0,1\})$-system $\mathbf{S}$ with MBO we define $\mathbf{S}^-$ as the $(\mathcal{X},\mathcal{Y})$-system resulting from $\mathbf{S}$ by ignoring the MBO, i.e.,*

$$\mathsf{p}^{\mathbf{S}^-}_{Y^i|X^i}=\mathsf{p}^{\mathbf{S}}_{Y^i|X^i}.$$

The following lemma was stated in [3] and in an equivalent but slightly different form in [2]. It implies the so-called "fundamental lemma of game playing" of [1] which is stated (and proved) only for a specific type of system description.

Lemma 2. *If $\mathbf{S}\overset{g}{\equiv}\mathbf{T}$, then, for any distinguisher $\mathbf{D}$ and any q,*

$$\Delta^{\mathbf{D}}_q(\mathbf{S}^-,\mathbf{T}^-) \;\leq\; \Gamma^{\mathbf{D}}_q(\mathbf{S}).$$

B. Conditional Equivalence

The following notion will lead to a very powerful tool for proving the indistinguishability of systems.

Definition 13. For an $(\mathcal{X},\mathcal{Y})\times\{0,1\}$-system $\mathbf{S}$ with MBO $A_0,A_1,A_2\ldots$, let $\mathcal{A}$ denote the sequence of events that the game is not won (i.e., $A_i=0$ for $i\geq 0$). For an $(\mathcal{X},\mathcal{Y})$-system $\mathbf{T}$ we say that $\mathbf{S}$ *conditioned on $\mathcal{A}$ is equivalent to* $\mathbf{T}$ (or $\mathbf{S}$ *while not won is equivalent to* $\mathbf{T}$), denoted

$$\mathbf{S}|\mathcal{A} \;\equiv\; \mathbf{T},$$

if, for $i\geq 1$,[9]

$$\mathsf{p}^{\mathbf{S}}_{Y^i|X^i,A_i=0} \;=\; \mathsf{p}^{\mathbf{T}}_{Y^i|X^i}.$$

Since $\mathsf{p}^{\mathbf{S}}_{Y^i,A_i=0|X^i} \;=\; \mathsf{p}^{\mathbf{S}}_{A_i=0|X^i}\cdot\mathsf{p}^{\mathbf{S}}_{Y^i|X^i,A_i=0}$, the above condition is equivalent to

$$\mathsf{p}^{\mathbf{S}}_{Y^i,A_i=0|X^i} \;=\; \mathsf{p}^{\mathbf{S}}_{A_i=0|X^i}\cdot\mathsf{p}^{\mathbf{T}}_{Y^i|X^i}.$$

***Example* 7.** Let $A_0,A_1,A_2\ldots$ be the MBO (defined for any system) defined by $A_i=0$ if and only if the first i inputs are distinct. Then for all m and n we have

$$\mathbf{R}_{m,n}|\mathcal{A} \;\equiv\; \mathbf{B}_{m,n}.$$

Stated informally, a URF $\mathbf{R}_{m,n}$ behaves like a beacon $\mathbf{B}_{m,n}$ as long as the inputs are distinct.

***Example* 8.** Consider a URF $\mathbf{R}_{n,n}$ and a URP $\mathbf{P}_n$, and let $A_0,A_1,A_2\ldots$ be the MBO defined as follows: $A_i=0$ if and only if for any two distinct inputs the corresponding two outputs are distinct. (In particular, if all inputs are distinct, then all outputs are distinct.) We have

$$\mathbf{R}_{n,n}|\mathcal{A} \;\equiv\; \mathbf{P}_n$$

as the reader can easily verify. Stated informally, a URF $\mathbf{R}_{n,n}$ behaves like a URP $\mathbf{P}_n$ as long as the outputs are distinct (whenever the inputs are distinct).

[9] Two conditional probability distributions are considered to be equal if they are equal for all arguments for which they are both defined. (Here one considers only x^i for which A_i has non-zero probability.)

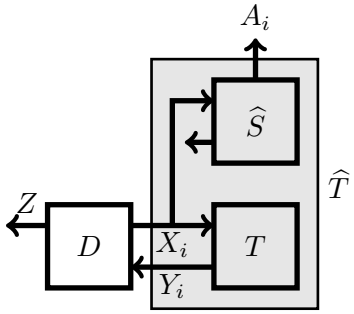

Fig. 1. The system $\hat{\mathbf{T}}$ and the distinguisher $\mathbf{D}$ connected to it.

C. From Conditional Equivalence to Indistinguishability

Often one considers an $(\mathcal{X}, \mathcal{Y})$-system $\mathbf{S}$ for which one can define an MBO $A_0, A_1, A_2 \ldots$. This results in a game $\hat{\mathbf{S}}$, characterized by $\mathsf{p}^{\hat{\mathbf{S}}}_{Y^i A_i | X^i}$, where, by definition,

$$\hat{\mathbf{S}}^- \equiv \mathbf{S},$$

i.e., $\mathsf{p}^{\hat{\mathbf{S}}^-}_{Y^i|X^i} = \mathsf{p}^{\mathbf{S}}_{Y^i|X^i}$.

The following theorem is very useful for indistinguishability proofs. It states that if $\hat{\mathbf{S}}|\mathcal{A} \equiv \mathbf{T}$, then the optimal distinguishing advantage for $\mathbf{S}$ and $\mathbf{T}$ (within q queries) can be bounded by the optimal probability of winning the game $\mathbf{S}$ *non-adaptively* (within q queries). Recall the definition of the non-adaptive distinguisher $[\![\mathbf{DT}]\!]$ (see Definition 7).

Theorem 3. *If for an $(\mathcal{X}, \mathcal{Y})$-system $\mathbf{S}$ one can define an MBO $A_0, A_1, A_2 \ldots$, such that $\hat{\mathbf{S}}|\mathcal{A} \equiv \mathbf{T}$, then, for every $\mathbf{D}$,*

$$\Delta^{\mathbf{D}}_q(\mathbf{S}, \mathbf{T}) \;\leq\; \Gamma^{[\![\mathbf{DT}]\!]}_q(\hat{\mathbf{S}}).$$

In particular,

$$\Delta_q(\mathbf{S}, \mathbf{T}) \;\leq\; \Gamma^{\mathsf{NA}}_q(\hat{\mathbf{S}}).$$

Proof. One can enhance $\mathbf{T}$ with an MBO $A_0, A_1, A_2 \ldots$ to a game $\hat{\mathbf{T}}$, as follows (see Figure 1):

$$\mathsf{p}^{\hat{\mathbf{T}}}_{Y^i A_i | X^i} = \mathsf{p}^{\mathbf{T}}_{Y^i|X^i} \cdot \mathsf{p}^{\hat{\mathbf{S}}}_{A_i|X^i}$$

(i.e., $\mathsf{p}^{\hat{\mathbf{T}}}_{A_i|X^i Y^i} = \mathsf{p}^{\hat{\mathbf{S}}}_{A_i|X^i}$). Then

$$\hat{\mathbf{S}} \;\stackrel{g}{\equiv}\; \hat{\mathbf{T}}$$

since

$$\mathsf{p}^{\hat{\mathbf{S}}}_{Y^i, A_i=0|X^i} \;=\; \underbrace{\mathsf{p}^{\hat{\mathbf{S}}}_{A_i=0|X^i}}_{=\mathsf{p}^{\hat{\mathbf{T}}}_{A_i=0|X^i}} \cdot \underbrace{\mathsf{p}^{\hat{\mathbf{S}}}_{Y^i|X^i, A_i=0}}_{=\mathsf{p}^{\mathbf{T}}_{Y^i|X^i}=\mathsf{p}^{\hat{\mathbf{T}}}_{Y^i|X^i}} \;=\; \mathsf{p}^{\hat{\mathbf{T}}}_{Y^i, A_i=0|X^i}.$$

(Note also that $\mathsf{p}^{\hat{\mathbf{T}}}_{Y^i|X^i} = \mathsf{p}^{\hat{\mathbf{T}}}_{Y^i|X^i, A_i=0}$.) Consider a distinguisher $\mathbf{D}$. According to Lemma 2, and using $\hat{\mathbf{S}}^- \equiv \mathbf{S}$ and $\hat{\mathbf{T}}^- \equiv \mathbf{T}$, we have

$$\Delta^{\mathbf{D}}_q(\mathbf{S}, \mathbf{T}) \;=\; \Delta^{\mathbf{D}}_q(\hat{\mathbf{S}}^-, \hat{\mathbf{T}}^-) \;\leq\; \Gamma^{\mathbf{D}}_q(\hat{\mathbf{S}}).$$

Since, according to Lemma 1, $\Gamma^{\mathbf{D}}_q(\hat{\mathbf{S}}) = \Gamma^{\mathbf{D}}_q(\hat{\mathbf{T}})$, it suffices to analyze $\Gamma^{\mathbf{D}}_q(\hat{\mathbf{T}})$. The way $\hat{\mathbf{T}}$ is defined (namely, as $\mathbf{T}$ enhanced with an independent system $\hat{\mathbf{S}}$ generating an MBO from the inputs $X_1, X_2, \ldots$), the distinguisher $\mathbf{D}$ together with $\mathbf{T}$ can be seen as a non-adaptive distinguisher or game winner $[\![\mathbf{DT}]\!]$ (see Definition 7) driving the system $\mathsf{p}^{\hat{\mathbf{S}}}_{A_i|X^i}$, ignoring the outputs of the system $\hat{\mathbf{S}}$. More precisely, we have $[\![\mathbf{DT}]\!]\hat{\mathbf{S}} \equiv \mathbf{D}\hat{\mathbf{T}}$ (see Figure 1) and hence $\Gamma^{\mathbf{D}}_q(\hat{\mathbf{T}}) = \Gamma^{[\![\mathbf{DT}]\!]}_q(\hat{\mathbf{S}})$.

The claim $\Delta_q(\mathbf{S}, \mathbf{T}) \leq \Gamma^{\mathsf{NA}}_q(\hat{\mathbf{S}})$ follows since $[\![\mathbf{DT}]\!] \in \mathsf{NA}$ for any $\mathbf{D}$. □

D. Example: The URP-URF "Switching Lemma"

We discuss a simple result which is usually called the PRP-PRF "switching lemma", where PRF (PRP) stands for pseudo-random function (permutation). But it is independent of complexity-theoretic arguments and is simply the statement that a URP $\mathbf{P}_n$ is indistinguishable from a URF $\mathbf{R}_{n,n}$ unless the number of queries is close to $2^{n/2}$, which is exponential and generally infeasible. This means that whenever one needs a pseudo-random function (PRF) one can also use a pseudo-random permutation (PRP) without losing much security. Since a block cipher (like AES) is often assumed to be a PRP, it can also be used as a PRF, as is for instance the case in the CBC-MAC.

The probability that a set of q independent and uniformly chosen values from an alphabet of size t contains a value twice (a collision) is denoted as $p_{\text{coll}}(t, q)$. It is well-known that

$$p_{\text{coll}}(t, q) \;\leq\; \tfrac{1}{2} q^2 / t.$$

Theorem 4. $\Delta_q(\mathbf{R}_{n,n}, \mathbf{P}_n) \;\leq\; \frac{1}{2} q^2 2^{-n}$.

Proof. As shown in Example 8, we can define an MBO $A_0, A_1, A_2, \ldots$ for the system $\mathbf{R}_{n,n}$, resulting in the game $\hat{\mathbf{R}}_{n,n}$, where the MBO is 1 if and only if for some distinct inputs the outputs are equal (a collision). We have $\mathbf{R}_{n,n}|\mathcal{A} \equiv \mathbf{P}_n$ (see Example 8) and hence, according to Theorem 3, we obtain

$$\Delta_q(\mathbf{R}_{n,n}, \mathbf{P}_n) \;\leq\; \Gamma^{\mathsf{NA}}_q(\hat{\mathbf{R}}_{n,n}).$$

It remains to analyze $\Gamma^{\mathsf{NA}}_q(\hat{\mathbf{R}}_{n,n})$. An optimal non-adaptive strategy chooses q distinct inputs. The probability of causing a collision is $p_{\text{coll}}(2^n, q)$, hence Lemma 2 can be applied. □

ACKNOWLEDGMENT

This research is supported by the Swiss National Science Foundation.

REFERENCES

[1] M. Bellare and P. Rogaway, The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs, In *Advances in Cryptology — EUROCRYPT '06*, volume 4004 of Lecture Notes in Computer Science, pp. 409–426, Springer Verlag, 2006.

[2] U. Maurer. Indistinguishability of random systems, In L. R. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pp. 110–132. Springer Verlag, 2002.

[3] U. Maurer, K. Pietrzak and R. Renner., Indistinguishability amplification. In *Advances in Cryptology — CRYPTO '07*, volume 4622 of Lecture Notes in Computer Science, pp. 130–149, Springer Verlag, 2007.