Optimality of Non-Adaptive Strategies: The Case of Parallel Games

Grégory Demay[1], Peter Gaži[2], Ueli Maurer[1], and Björn Tackmann[1]

[1]Department of Computer Science, ETH Zürich, Switzerland,
`{gregory.demay,maurer,bjoern.tackmann}@inf.ethz.ch`
[2]Institute of Science and Technology, Austria, `peter.gazi@ist.ac.at`

April 28, 2014

Abstract

Most cryptographic security proofs require showing that two systems are indistinguishable. A central tool in such proofs is that of a game, where winning the game means provoking a certain condition, and it is shown that the two systems considered cannot be distinguished unless this condition is provoked. Upper bounding the probability of winning such a game, i.e., provoking this condition, for an arbitrary strategy is usually hard, except in the special case where the best strategy for winning such a game is known to be non-adaptive.

A sufficient criterion for ensuring the optimality of non-adaptive strategies is that of conditional equivalence to a system, a notion introduced in [Mau02]. In this paper, we show that this criterion is *not necessary* to ensure the optimality of non-adaptive strategies by giving two results of independent interest: 1) the optimality of non-adaptive strategies is not preserved under parallel composition; 2) in contrast, conditional equivalence is preserved under parallel composition.

Contents

1 Introduction

1.1 Conditional Equivalence

Most security definitions in cryptography [Can01, MR11, Mau11] are phrased as indistinguishability statements between two discrete systems, where one involves the protocol whose security is to be proven, while the other corresponds to a specification of the desired goal. A central tool in deriving such indistinguishability proofs between two systems is to characterize both systems as being equivalent until a certain condition arises [Mau02, BR06]. Thus, being able to distinguish both systems requires to provoke this condition, and one is then interested in upper bounding the probability of this event.

Interacting with a discrete system in order to provoke a certain condition is naturally modeled by the notion of a game [Mau02]. A game[1] is a system which replies to every input X_k by an output Y_k and a bit A_k indicating whether or not the game has been won. A strategy for a game consists of providing a sequence of inputs $X_1, X_2, \ldots$ to the game, where X_k depends a priori probabilistically on the past responses Y^{k-1} of the game as well as on the past queries X^{k-1}. Due to this non-trivial dependency, analyzing the maximal probability of winning a game, i.e., provoking the event $A_k = 1$, is in general challenging and sometimes infeasible.

This difficulty can be greatly reduced if the best strategy for winning a game is known to be *non-adaptive*, i.e., the optimal distribution of the inputs does not depend on the game's previous outputs. Thus, characterizing for which games non-adaptive strategies are optimal is essential in deriving security proofs. An important tool towards this characterization was given by the notion of *conditional equivalence* to a system, introduced in [Mau02] and also studied in [JÖS12], which can be seen as a sufficient criterion guaranteeing that non-adaptive strategies are optimal for winning a game. A typical example of this situation is the so-called PRP-PRF switching lemma [BR06] that we detail informally below.

Example 1 (URF vs. URP)**.** A uniform random function (URF) over some finite set $\mathcal{X}$ is a system that replies to every query $X_k \in \mathcal{X}$ with a uniformly random value $Y_k \in \mathcal{X}$, but replies consistently when a previous input is repeated. In contrast, a uniform random permutation (URP) over $\mathcal{X}$ is a URF which is bijective. The reason for comparing a URP to a URF arises for example when a block-cipher like AES, which is assumed to be (computationally) indistinguishable from a URP, is used for authentication, e.g., via CBC-MAC, whose security proof requires instead a URF [BR06].

Intuitively, a URF and a URP are indistinguishable unless a collision occurs in the URF's outputs, i.e., two distinct inputs to the URF are answered by the same value. It suffices thus to upper bound the probability of a collision in the URF's outputs in order to derive an indistinguishability statement between a URF and a URP. This upper bound is easily derived since the best strategy for provoking a collision in a URF's outputs is non-adaptive, a consequence of the fact that a URF and a URP can be shown to be conditionally equivalent (in the sense of [Mau13]). A more formal analysis of this example is given in [Mau13]. □

Since conditional equivalence is a sufficient criterion to ensure that the best strategy for winning a game is non-adaptive, a natural question is then whether the opposite direction holds, i.e., is conditional equivalence necessary for the optimal strategy of winning a game to be non-adaptive?

1.2 Parallel Composition

We show that conditional equivalence is *not* necessary for the optimal strategy of winning a game to be non-adaptive, by giving two results of independent interest in the context of composition. Two games can naturally be combined into a single game by considering the *disjunction* of those

[1] The term "game" is used in this paper in the sense of Definition 2, and not in the sense of game theory.

two games. Each game in the disjunction of two games can be accessed individually, and the resulting game is won if at least one of the two original games is won. Such a combination of two games appears when the security of an application depends on the security of two internal components (modeled each by an individual game), whose breach in security breaks the security of the whole application. One concrete example of such an application is the hash-then-sign paradigm given in the example below.

Example 2 (Hash-then-Sign)**.** A digital signature scheme (DSS) allows a signer who has established a public key to sign a message in such a way that any other party who knows this public key can verify that the received message indeed originated from the signer and was not modified in any way. The security of a DSS can be defined as a game, where the game is won if an adversary successfully forges a signature, i.e., the adversary finds a valid signature of a message which was not previously signed by the legitimate signer.

In order to extend a DSS restricted to messages of ℓ-bits, a collision-resistant hash function $h: \{0,1\}^* \to \{0,1\}^\ell$ is used first, i.e., the hash of the message $h(m)$ is signed instead of the message m itself. Forging a signature for this new scheme requires to win one of the following two games: finding a collision for the function h, i.e., two distinct messages m and m' such that $h(m) = h(m')$; or finding a forgery for the original length-restricted signature scheme. A more detailed analysis of the hash-then-sign paradigm can be found in [KL07, Sec. 12.4]. □

We separate the optimality of non-adaptive strategies from conditional equivalence by the following two results about parallel games:

1. the optimality of non-adaptive strategies is not preserved under parallel composition, i.e., adaptivity can help for winning the disjunction of two games, even if the optimal strategies for winning each game were non-adaptive;
2. in contrast, conditional equivalence is preserved under parallel composition, i.e., if two games are each conditionally equivalent to some system, then the disjunction of both games is conditionally equivalent to the parallel composition of the two other systems.

2 Preliminaries

2.1 Basic Notation

We denote sets by calligraphic letters (e.g., $\mathcal{X}$, $\mathcal{Y}$). Throughout this paper, we consider only discrete random variables. A discrete random variable will be denoted by an upper-case letter X, its range by the corresponding calligraphic letter $\mathcal{X}$, and a realization of the random variable X will be denoted by the corresponding lower-case letter x. A tuple of n random variables $(X_1, \ldots, X_n)$ will be denoted by X^n. Similarly, x^n will denote a tuple of n values $(x_1, \ldots, x_n)$. The probability distribution of a random variable X will be denoted as P_X.

2.2 Discrete Random Systems

Many cryptographic primitives like block ciphers, MAC schemes, random functions, etc., can be described as $(\mathcal{X}, \mathcal{Y})$-discrete random systems taking inputs $X_1, X_2, \cdots \in \mathcal{X}$ and generating for each input X_k an output $Y_k \in \mathcal{Y}$. In full generality, such an output Y_k depends probabilistically on all the previous inputs X^k as well as all the previous outputs Y^{k-1}. For an $(\mathcal{X}, \mathcal{Y})$-system $\mathbf{S}$, such a dependency for the k^{th} output is captured by a conditional probability distribution, which will be denoted by $\mathsf{p}^{\mathbf{S}}_{Y_k|X^kY^{k-1}}$ and where the superscript indicates the system considered. This motivates the definition from [Mau02] of a random system.

Definition 1 ([Mau02])**.** *An* $(\mathcal{X}, \mathcal{Y})$-system $\mathbf{S}$ *is a (possibly infinite) sequence of conditional probability distributions* $\left\{\mathsf{p}^{\mathbf{S}}_{Y_k|X^kY^{k-1}}\right\}_{k \geq 1}$, *where* $X_k \in \mathcal{X}$ *and* $Y_k \in \mathcal{Y}$ *for all* $k \geq 1$.

Note that an $(\mathcal{X},\mathcal{Y})$-system $\mathbf{S}$ considered in isolation does not define a random experiment since the distribution of the inputs to the system $\mathbf{S}$ is not defined. Hence, each conditional probability distribution $\mathsf{p}^{\mathbf{S}}_{Y_k|X^kY^{k-1}}$ involved in the definition of the system $\mathbf{S}$ is actually a function from $\mathcal{Y}\times\mathcal{X}^k\times\mathcal{Y}^{k-1}$ to $[0,1]$, where for all choices of the arguments x^k and y^{k-1} the sum of the function values over the choices of y_k equals 1, and not a probability distribution (which in contrast would have been denoted by the upper-case letter P).

It is sometimes convenient to use an alternative description of a random system $\mathbf{S}$, namely the sequence of conditional distributions $\mathsf{p}^{\mathbf{S}}_{Y^k|X^k}$, where

$$\mathsf{p}^{\mathbf{S}}_{Y^k|X^k} := \prod_{j=1}^{k} \mathsf{p}^{\mathbf{S}}_{Y_j|X^jY^{j-1}}.$$

Note that the conditional distribution $\mathsf{p}^{\mathbf{S}}_{Y^k|X^k}$ implies the conditional distribution $\mathsf{p}^{\mathbf{S}}_{Y^j|X^j}$ for all $j<k$ and hence the above description of a system is redundant. The conditional distribution $\mathsf{p}^{\mathbf{S}}_{Y^k|X^k}$ must satisfy a consistency condition which ensures that Y_k does not depend on $X_{k+1},X_{k+2},\ldots$.

2.3 Parallel Composition of Systems

In the spirit of [MR11], we define the notion of parallel composition between discrete random systems in order to model that several systems can be combined into a single one. Intuitively, the system resulting from the parallel composition of an $(\mathcal{X}_1,\mathcal{Y}_1)$-system $\mathbf{S}_1$ and an $(\mathcal{X}_2,\mathcal{Y}_2)$-system $\mathbf{S}_2$, denoted $\mathbf{S}_1\|\mathbf{S}_2$, allows access to the independent systems $\mathbf{S}_1$ and $\mathbf{S}_2$. This requires that part of the input to the system $\mathbf{S}_1\|\mathbf{S}_2$ specifies which system ($\mathbf{S}_1$ or $\mathbf{S}_2$) is queried. More formally, $\mathbf{S}_1\|\mathbf{S}_2$ is an $(\mathcal{X},\mathcal{Y})$-system, where $\mathcal{X}:=(\{1\}\times\mathcal{X}_1)\cup(\{2\}\times\mathcal{X}_2)$ and $\mathcal{Y}:=\mathcal{Y}_1\cup\mathcal{Y}_2$. The combined system $\mathbf{S}_1\|\mathbf{S}_2$ is depicted in Figure 1.

Let us now describe the conditional probability distribution $\mathsf{p}^{\mathbf{S}_1\|\mathbf{S}_2}_{Y_k|X^kY^{k-1}}$ for the system $\mathbf{S}_1\|\mathbf{S}_2$. For each round k, the system $\mathbf{S}_1\|\mathbf{S}_2$ takes as input an $x_k:=(s_k,\tilde{x}_k)\in\mathcal{X}$, where the first part of the input $s_k\in\{1,2\}$ is a selector indicating which of the two systems $\mathbf{S}_1$ or $\mathbf{S}_2$ is to be queried on the second part of the input $\tilde{x}_k$. The output of the system $\mathbf{S}_1\|\mathbf{S}_2$ is then given by the response y_k of the selected system. A transcript of k queries and responses for the system $\mathbf{S}_1\|\mathbf{S}_2$ corresponds thus to a sequence $\left(\left(s^k,\tilde{x}^k\right),y^k\right)$ which can be split into two parts: $\left(\left(1^{k_1},\tilde{x}^{k_1}_{(1)}\right),y^{k_1}_{(1)}\right)$ and $\left(\left(2^{k_2},\tilde{x}^{k_2}_{(2)}\right),y^{k_2}_{(2)}\right)$, where $\tilde{x}^{k_j}_{(j)}$ denotes the tuple of k_j queries made to the system $\mathbf{S}_j$ and $y^{k_j}_{(j)}$ the tuple of corresponding responses in the same order as they appeared in the global transcript $\left(\left(s^k,\tilde{x}^k\right),y^k\right)$, for all $j\in\{1,2\}$ and some integers k_1 and k_2 such that $k_1+k_2=k$. Then,

$$\mathsf{p}^{\mathbf{S}_1\|\mathbf{S}_2}_{Y_k|X^kY^{k-1}}\left(y_k,\left(s^k,\tilde{x}^k\right),y^{k-1}\right) := \begin{cases} \mathsf{p}^{\mathbf{S}_1}_{Y_{k_1}|X^{k_1}Y^{k_1-1}}\left(y_k,\tilde{x}^{k_1}_{(1)},y^{k_1-1}_{(1)}\right) & \text{if } s_k=1,\\ \mathsf{p}^{\mathbf{S}_2}_{Y_{k_2}|X^{k_2}Y^{k_2-1}}\left(y_k,\tilde{x}^{k_2}_{(2)},y^{k_2-1}_{(2)}\right) & \text{if } s_k=2.\end{cases} \tag{1}$$

2.4 Games and Conditional Equivalence

Following the definition of [MPR07], we model a game as an $(\mathcal{X},\mathcal{Y}\times\{0,1\})$-system, where the binary part of the output indicates whether or not 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, indicating that the game is won, it can not turn back to 0.

Definition 2 ([Mau02])**.** *An* $(\mathcal{X},\mathcal{Y})$-game $\mathbf{G}$ *is an* $(\mathcal{X},\mathcal{Y}\times\{0,1\})$*-system, where the binary component* A_j *of the output* $Y_j=(Y'_j,A_j)$ *satisfies the following monotonicity property*

$$A_j=1 \quad\Longrightarrow\quad A_k=1, \textit{ for all } k\geq j.$$

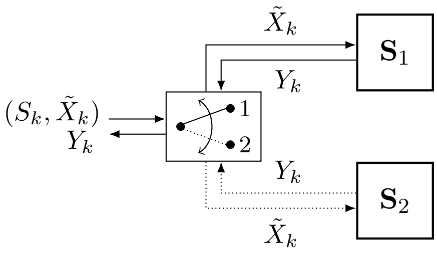

Figure 1: System $\mathbf{S}_1 \| \mathbf{S}_2$: output Y_k upon input $(S_k, \tilde{X}_k)$, where Y_k is the output of the system $\mathbf{S}_1$ (resp., $\mathbf{S}_2$) when queried on $\tilde{X}_k$ if $S_k = 1$ (resp., $S_k = 2$).

Unless stated otherwise, the monotone binary output of a game will be denoted by the symbol A. We formalize the notion of winning a game by the concept of a *game-winner*. Intuitively, a game-winner $\mathbf{W}$ for an $(\mathcal{X}, \mathcal{Y})$-game $\mathbf{G}$ corresponds to a $(\mathcal{Y}, \mathcal{X})$-system which is one query ahead: the output X_k of $\mathbf{W}$ corresponds to a query made to the game $\mathbf{G}$, where X_k depends on the given responses Y^{k-1} of the game $\mathbf{G}$ and on the previous queries X^{k-1} made to it.

Definition 3 ([Mau13])**.** *An* $(\mathcal{X}, \mathcal{Y})$-game-winner $\mathbf{W}$ *is a (possibly infinite) sequence of conditional probability distributions* $\left\{ \mathsf{p}^{\mathbf{W}}_{X_k|Y^{k-1}X^{k-1}} \right\}_{k \geq 1}$*, where* $Y_k \in \mathcal{Y}$ *and* $X_k \in \mathcal{X}$ *for all* $k \geq 1$*.*

An $(\mathcal{X}, \mathcal{Y})$-game-winner $\mathbf{W}$ is said to be *non-adaptive* if its queries can be fixed in advance without interacting with an $(\mathcal{X}, \mathcal{Y})$-game, i.e.,

$$\mathsf{p}^{\mathbf{W}}_{X_k|Y^{k-1}X^{k-1}} = \mathsf{p}^{\mathbf{W}}_{X_k|X^{k-1}},$$

for all $k \geq 1$. We denote by $\mathcal{W}$ and $\mathcal{W}_{\mathsf{na}}$ the set of all game-winners and non-adaptive game-winners, respectively. Consider the random experiment defined by a game winner $\mathbf{W}$ interacting with an $(\mathcal{X}, \mathcal{Y})$-game $\mathbf{G}$ depicted in Figure 2. Let $\Gamma^{\mathbf{W}}_k(\mathbf{G})$ denote the probability of $\mathbf{W}$ winning the game $\mathbf{G}$ within k queries, i.e.,

$$\Gamma^{\mathbf{W}}_k(\mathbf{G}) := \mathsf{P}_{A_k}(1),$$

where the probability is taken in the random experiment defined by the game-winner $\mathbf{W}$ interacting with the $(\mathcal{X}, \mathcal{Y})$-game $\mathbf{G}$. For a class $\mathcal{W}$ of game-winners, we define $\Gamma^{\mathcal{W}}_k(\mathbf{G})$ as

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

Note that whether or not a game-winner $\mathbf{W}$ sees the monotone binary output of an $(\mathcal{X}, \mathcal{Y})$-game $\mathbf{G}$ is irrelevant since the sole purpose of $\mathbf{W}$ is to win the game $\mathbf{G}$. For convenience, we will model the monotone binary output of a game $\mathbf{G}$ as not being accessible to a game winner $\mathbf{W}$ (as shown in Figure 2).

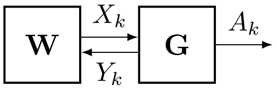

Figure 2: A game winner $\mathbf{W}$ interacting with an $(\mathcal{X}, \mathcal{Y})$-game $\mathbf{G}$.

The notion of *conditional equivalence* introduced in [Mau02] is a binary relation between a game $\mathbf{G}$ and a system $\mathbf{S}$. Conditional equivalence is a central tool for proving indistinguishability between the system formed by the game $\mathbf{G}$ (without its monotone binary output) and the system $\mathbf{S}$.

Definition 4 ([Mau13]). *An $(\mathcal{X}, \mathcal{Y})$-game* $\mathbf{G}$ *is said to be* conditionally equivalent *to an* $(\mathcal{X}, \mathcal{Y})$-*system* $\mathbf{S}$, *denoted*[2] $\mathbf{G} \models\equiv \mathbf{S}$, *if*

$$\mathsf{p}^{\mathbf{G}}_{Y^j|X^j A_j=0} = \mathsf{p}^{\mathbf{S}}_{Y^j|X^j},$$

for all $j \geq 1$ *and for all arguments for which* $\mathsf{p}^{\mathbf{G}}_{Y^j|X^j A_j=0}$ *is defined.*

We now define two predicates $\mathrm{NA}(\mathbf{G})$ and $\mathrm{CE}(\mathbf{G})$ for a game $\mathbf{G}$, where $\mathrm{NA}(\mathbf{G})$ indicates that the best strategy for winning the game $\mathbf{G}$ is non-adaptive, while $\mathrm{CE}(\mathbf{G})$ indicates that $\mathbf{G}$ is conditionally equivalent to some other system $\mathbf{S}$.

Definition 5. *For any game* $\mathbf{G}$, *let* $\mathrm{NA}(\mathbf{G})$ *and* $\mathrm{CE}(\mathbf{G})$ *be the following predicates,*

$$\begin{aligned} \mathrm{NA}(\mathbf{G}) = 1 \quad &:\Longleftrightarrow \quad \forall k \in \mathbb{N}: \ \Gamma^{\mathcal{W}}_k(\mathbf{G}) = \Gamma^{\mathcal{W}_{\mathsf{na}}}_k(\mathbf{G}), \\ \mathrm{CE}(\mathbf{G}) = 1 \quad &:\Longleftrightarrow \quad \exists \mathbf{S}: \ \mathbf{G} \models\equiv \mathbf{S}. \end{aligned}$$

The next theorem, which is only a part of the results in [Mau02, Th. 2], guarantees that if a game is conditionally equivalent to some system, then non-adaptive strategies are optimal for winning this game.

Theorem 1 ([Mau02]). *For any* $(\mathcal{X}, \mathcal{Y})$-*game* $\mathbf{G}$,

$$\mathrm{CE}(\mathbf{G}) \quad \Longrightarrow \quad \mathrm{NA}(\mathbf{G}).$$

2.5 Disjunctions of Games

Since games as defined in Definition 2 are systems, they can of course be composed by the parallel operation $\|$ defined in Section 2.3. However, note that if $\mathbf{G}_1$ is an $(\mathcal{X}_1, \mathcal{Y}_1)$-game and $\mathbf{G}_2$ is an $(\mathcal{X}_2, \mathcal{Y}_2)$-game, then the combined system $\mathbf{G}_1 \| \mathbf{G}_2$ is *not* necessarily an $(\mathcal{X}, \mathcal{Y})$-game, where $\mathcal{X} := (\{1\} \times \mathcal{X}_1) \cup (\{2\} \times \mathcal{X}_2)$ and $\mathcal{Y} := \mathcal{Y}_1 \cup \mathcal{Y}_2$. Indeed, the binary output of $\mathbf{G}_1 \| \mathbf{G}_2$ comes either from $\mathbf{G}_1$ or from $\mathbf{G}_2$, depending on which sub-game was queried, and thus is in general not monotone. In order to obtain an $(\mathcal{X}, \mathcal{Y})$ game, we add a logical OR operation between the monotone binary outputs of both games $\mathbf{G}_1$ and $\mathbf{G}_2$ to obtain the game denoted by $(\mathbf{G}_1 \| \mathbf{G}_2)^{\vee}$ and depicted in Figure 3.

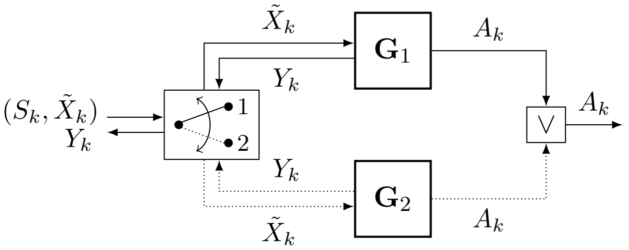

Figure 3: Game $(\mathbf{G}_1 \| \mathbf{G}_2)^{\vee}$: output (Y_k, A_k) upon input $(S_k, \tilde{X}_k)$, where (Y_k, A_k) is the output of the game $\mathbf{G}_1$ (resp., $\mathbf{G}_2$) when queried on $\tilde{X}_k$ if $S_k = 1$ (resp., $S_k = 2$).

Intuitively, a game-winner wins the game $(\mathbf{G}_1 \| \mathbf{G}_2)^{\vee}$ within k queries only if it wins the game $\mathbf{G}_1$ within k_1 queries or wins the game $\mathbf{G}_2$ within k_2 queries, for any integer k_1, k_2 such that $k_1 + k_2 \leq k$. Following the formalism developed in Section 2.3, if we denote by $\left(\left(j^{k_j}, \tilde{x}^{k_j}_{(j)}\right), y^{k_j}_{(j)}\right)$ the queries and responses done to the game $\mathbf{G}_j$ in a transcript of k inputs and outputs $\left(\left(s^k, \tilde{x}^k\right), y^k\right)$ done to the game $(\mathbf{G}_1 \| \mathbf{G}_2)^{\vee}$ such that it is not yet won ($A_k = 0$), we have

$$\mathsf{p}^{(\mathbf{G}_1 \| \mathbf{G}_2)^{\vee}}_{Y^k A_k=0|X^k}\left(y^k, (s^k, \tilde{x}^k)\right) := \mathsf{p}^{\mathbf{G}_1}_{Y^{k_1} A_{k_1}=0|X^{k_1}}\left(y^{k_1}_{(1)}, \tilde{x}^{k_1}_{(1)}\right) \cdot \mathsf{p}^{\mathbf{G}_2}_{Y^{k_2} A_{k_2}=0|X^{k_2}}\left(y^{k_2}_{(2)}, \tilde{x}^{k_2}_{(2)}\right). \tag{2}$$

[2] The expression $\mathbf{G} \models\equiv \mathbf{S}$ corresponds to $(\mathbf{G}^{-})|\mathcal{A} \equiv \mathbf{S}$ in [Mau13], where $\mathcal{A}$ denotes the sequence of monotone binary outputs $A_0, A_1, A_2, \ldots$. The notation we use here emphasizes that the monotone binary output is part of the game as a formal object.

3 Non-Adaptivity and Parallel Composition

If the best strategies in winning the games $\mathbf{G}_1$ and $\mathbf{G}_2$ are both non-adaptive, does it necessarily imply that the best strategy in winning the combined game $(\mathbf{G}_1 \| \mathbf{G}_2)^\vee$ is non-adaptive? The next theorem shows that this is not true in general.

Theorem 2. *If the best strategies for winning the $(\mathcal{X}_1, \mathcal{Y}_1)$-game $\mathbf{G}_1$ and the $(\mathcal{X}_2, \mathcal{Y}_2)$-game $\mathbf{G}_2$ are both non-adaptive, then the best strategy for winning the game $(\mathbf{G}_1 \| \mathbf{G}_2)^\vee$ is not necessarily non-adaptive, i.e.,*

$$\mathrm{NA}\left(\mathbf{G}_1\right) \text{ and } \mathrm{NA}\left(\mathbf{G}_2\right) \quad \not\Longrightarrow \quad \mathrm{NA}\left((\mathbf{G}_1 \| \mathbf{G}_2)^\vee\right).$$

Proof. We will define a sequence of games $\{\mathbf{G}_j\}_{j\geq 2}$ such that the implication $\mathrm{NA}\left(\mathbf{G}_j\right) \longrightarrow \mathrm{NA}\left((\mathbf{G}_j \| \mathbf{G}_j)^\vee\right)$ does not hold *for any* integer $j \geq 2$. As a side result, we will have proved the stronger statement that adaptivity can help in *any* round when trying to win the game $(\mathbf{G}_j \| \mathbf{G}_j)^\vee$.

Let j be an integer such that $j \geq 2$ and let $\mathbf{G}_j$ be the following $(\{0,1\}, \{0,1\})$-game. Any query $x_i \in \{0,1\}$ made to $\mathbf{G}_j$ is responded by a bit $y_i \in \{0,1\}$ chosen independently and uniformly at random. The monotone binary output of $\mathbf{G}_j$ is defined as $A_1 := 0, \ldots, A_{j-1} := 0$, and for all $i \geq j$, we have $A_i := Y_1$, where Y_1 is the response of $\mathbf{G}_j$ to the first query. We now show that the game $\mathbf{G}_j$ is such that

1. $\Gamma_k^{\mathcal{W}}\left(\mathbf{G}_j\right) = \Gamma_k^{\mathcal{W}_{\mathsf{na}}}\left(\mathbf{G}_j\right)$, for all $k \in \mathbb{N}$;
2. $\Gamma_{j+1}^{\mathcal{W}}\left((\mathbf{G}_j \| \mathbf{G}_j)^\vee\right) > \Gamma_{j+1}^{\mathcal{W}_{\mathsf{na}}}\left((\mathbf{G}_j \| \mathbf{G}_j)^\vee\right)$.

Condition 1). In order to win the game $\mathbf{G}_j$, a game-winner simply needs to make at least j queries resulting in the event $Y_1 = 1$. Since Y_1, the answer of $\mathbf{G}_j$ to the first query, is an independent uniform random variable, the best strategy for winning the game $\mathbf{G}_j$ is clearly non-adaptive. Thus,

$$\Gamma_k^{\mathcal{W}}\left(\mathbf{G}_j\right) = \Gamma_k^{\mathcal{W}_{\mathsf{na}}}\left(\mathbf{G}_j\right) = \begin{cases} 0 & \text{if } k < j, \\ \frac{1}{2} & \text{otherwise.} \end{cases} \tag{3}$$

Condition 2). Consider now a non-adaptive game-winner $\mathbf{W}$ trying to win the game $(\mathbf{G}_j \| \mathbf{G}_j)^\vee$ with $j+1$ queries. Since the game-winner $\mathbf{W}$ is non-adaptive, it has to fix all its queries in advance and in particular to which sub-game in $(\mathbf{G}_j \| \mathbf{G}_j)^\vee$ each query is addressed to. Note that (3) implies that the game $\mathbf{G}_j$ cannot be won by any game-winner making strictly less than j queries, so that $\mathbf{W}$ will not have a better chance of winning the game $(\mathbf{G}_j \| \mathbf{G}_j)^\vee$ with $j+1$ queries than if it had only j queries, i.e.,

$$\Gamma_{j+1}^{\mathcal{W}_{\mathsf{na}}}\left((\mathbf{G}_j \| \mathbf{G}_j)^\vee\right) = \frac{1}{2}.$$

On the other hand, consider the following adaptive game-winner $\mathbf{W}$ making $j+1$ queries $(s_1, \tilde{x}_1), \ldots, (s_{j+1}, \tilde{x}_{j+1})$ to the game $(\mathbf{G}_j \| \mathbf{G}_j)^\vee$, where $s_k \in \{1,2\}$ and $\tilde{x}_k \in \{0,1\}$. The game-winner $\mathbf{W}$ makes a first query $(1, \tilde{x}_1)$ to the game $(\mathbf{G}_j \| \mathbf{G}_j)^\vee$, corresponding to a query $\tilde{x}_1$ made to the first sub-game $\mathbf{G}_j$ in $(\mathbf{G}_j \| \mathbf{G}_j)^\vee$, which is replied by $Y_1 \in \{0,1\}$. If $Y_1 = 1$, then $\mathbf{W}$ makes its remaining j queries to the same sub-game it queried the first time by querying the game $(\mathbf{G}_j \| \mathbf{G}_j)^\vee$ on $(1, \tilde{x}_2), \ldots, (1, \tilde{x}_{j+1})$. Otherwise, if $Y_1 = 0$, then $\mathbf{W}$ makes its remaining j queries to the other sub-game by querying the game $(\mathbf{G}_j \| \mathbf{G}_j)^\vee$ on $(2, \tilde{x}_2), \ldots, (2, \tilde{x}_{j+1})$. Note that in the case where $Y_1 = 1$, which happens with probability $\frac{1}{2}$, $\mathbf{W}$ wins the game $(\mathbf{G}_j \| \mathbf{G}_j)^\vee$ with probability 1, while when $Y_1 = 0$ the game-winner $\mathbf{W}$ wins the game $(\mathbf{G}_j \| \mathbf{G}_j)^\vee$ with probability $\frac{1}{2}$, i.e.,

$$\Gamma_{j+1}^{\mathbf{W}}\left((\mathbf{G}_j \| \mathbf{G}_j)^\vee\right) = \frac{3}{4} > \Gamma_{j+1}^{\mathcal{W}_{\mathsf{na}}}\left((\mathbf{G}_j \| \mathbf{G}_j)^\vee\right).$$

The previous equation together with (3) imply that $\mathrm{NA}\left(\mathbf{G}_j\right) = 1$ and $\mathrm{NA}\left((\mathbf{G}_j \| \mathbf{G}_j)^\vee\right) = 0$, for all $j \geq 2$. □

4 Conditional Equivalence and Parallel Composition

If a game $\mathbf{G}_1$ (respectively, $\mathbf{G}_2$) is conditionally equivalent to a system $\mathbf{S}_1$ (respectively, $\mathbf{S}_2$), then the combined game $(\mathbf{G}_1 \| \mathbf{G}_2)^{\vee}$ is conditionally equivalent to the combined system $\mathbf{S}_1 \| \mathbf{S}_2$, a statement formalized in Lemma 1. In other words, parallel composition preserves conditional equivalence statements.

Lemma 1. *For any* $(\mathcal{X}_1, \mathcal{Y}_1)$*-game* $\mathbf{G}_1$ *(respectively,* $(\mathcal{X}_2, \mathcal{Y}_2)$*-game* $\mathbf{G}_2$*) and any* $(\mathcal{X}_1, \mathcal{Y}_1)$*-system* $\mathbf{S}_1$ *(respectively,* $(\mathcal{X}_2, \mathcal{Y}_2)$*-system* $\mathbf{S}_2$*),*

$$\mathbf{G}_1 \mathrel{|\!\!\equiv} \mathbf{S}_1 \text{ and } \mathbf{G}_2 \mathrel{|\!\!\equiv} \mathbf{S}_2 \quad \Longrightarrow \quad (\mathbf{G}_1 \| \mathbf{G}_2)^{\vee} \mathrel{|\!\!\equiv} \mathbf{S}_1 \| \mathbf{S}_2.$$

Proof. We shall denote by $\mathbf{G}$ and $\mathbf{S}$ the game $(\mathbf{G}_1 \| \mathbf{G}_2)^{\vee}$ and the system $\mathbf{S}_1 \| \mathbf{S}_2$, respectively, within the remainder of the proof. Following the notations of Sections 2.3 and 2.5, $\mathbf{G}$ is an $(\mathcal{X}, \mathcal{Y})$-game and $\mathbf{S}$ is an $(\mathcal{X}, \mathcal{Y})$-system, where $\mathcal{X} := (\{1\} \times \mathcal{X}_1) \cup (\{2\} \times \mathcal{X}_2)$ and $\mathcal{Y} := \mathcal{Y}_1 \cup \mathcal{Y}_2$. Consider a transcript $\left((s^k, \tilde{x}^k), y^k\right) \in \mathcal{X}^k \times \mathcal{Y}^k$ of k queries such that $\mathsf{p}^{\mathbf{G}}_{Y^k | X^k A_k = 0}\left(y^k, (s^k, \tilde{x}^k)\right)$ is defined. Such a transcript $\left((s^k, \tilde{x}^k), y^k\right)$ can be partitioned into 2 sub-transcripts $\left(\tilde{x}^{k_j}_{(j)}, y^{k_j}_{(j)}\right)$ corresponding to queries made to the game $\mathbf{G}_j$ or to the system $\mathbf{S}_j$, for all $j \in \{1, 2\}$. Note that $\mathsf{p}^{\mathbf{G}}_{Y^k | X^k A_k = 0}\left(y^k, (s^k, \tilde{x}^k)\right)$ being defined implies that $\mathsf{p}^{\mathbf{G}_j}_{Y^{k_j} | X^{k_j} A_{k_j} = 0}\left(y^{k_j}_{(j)}, \tilde{x}^{k_j}_{(j)}\right)$ is defined as well. Then,

$$\begin{aligned}
\mathsf{p}^{\mathbf{G}}_{Y^k | X^k A_k = 0}\left(y^k, (s^k, \tilde{x}^k)\right) &= \prod_{j=1}^{2} \mathsf{p}^{\mathbf{G}_j}_{Y^{k_j} | X^{k_j} A_{k_j} = 0}\left(y^{k_j}_{(j)}, \tilde{x}^{k_j}_{(j)}\right) \\
&= \prod_{j=1}^{2} \mathsf{p}^{\mathbf{S}_j}_{Y^{k_j} | X^{k_j}}\left(y^{k_j}_{(j)}, \tilde{x}^{k_j}_{(j)}\right) \\
&= \mathsf{p}^{\mathbf{S}}_{Y^k | X^k}\left(y^k, (s^k, \tilde{x}^k)\right),
\end{aligned}$$

where the first equality comes from (2), the second equality comes from the fact that $\mathbf{G}_j \mathrel{|\!\!\equiv} \mathbf{S}_j$ for all $j \in \{1, 2\}$, and the last equality follows from (1). Thus, the game $\mathbf{G}$ is conditionally equivalent to the system $\mathbf{S}$. □

The next theorem trivially follows from Lemma 1 and shows that conditional equivalence is preserved under the parallel operation $\|$.

Theorem 3. *For any* $(\mathcal{X}_1, \mathcal{Y}_1)$*-game* $\mathbf{G}_1$ *and any* $(\mathcal{X}_2, \mathcal{Y}_2)$*-game* $\mathbf{G}_2$*,*

$$\mathrm{CE}(\mathbf{G}_1) \text{ and } \mathrm{CE}(\mathbf{G}_2) \quad \Longrightarrow \quad \mathrm{CE}\left((\mathbf{G}_1 \| \mathbf{G}_2)^{\vee}\right).$$

5 Non-Adaptivity and Conditional Equivalence

It is not hard to see from the previous results that conditional equivalence is strictly stronger a requirement than non-adaptive strategies being optimal for winning a game, a statement formalized below in Theorem 4. Assume for the sake of contradiction that for any game $\mathbf{G}$,

$$\mathrm{NA}(\mathbf{G}) \quad \Longrightarrow \quad \mathrm{CE}(\mathbf{G}). \tag{4}$$

Consider two games $\mathbf{G}_1$ and $\mathbf{G}_2$ such that $\mathrm{NA}(\mathbf{G}_1)$ and $\mathrm{NA}(\mathbf{G}_2)$, but *not* $\mathrm{NA}\left((\mathbf{G}_1 \| \mathbf{G}_2)^{\vee}\right)$. Such games $\mathbf{G}_1$ and $\mathbf{G}_2$ must exist according to Theorem 2. Then, (4) implies $\mathrm{CE}(\mathbf{G}_1)$ and $\mathrm{CE}(\mathbf{G}_2)$, which in turn implies by Theorem 3 $\mathrm{CE}\left((\mathbf{G}_1 \| \mathbf{G}_2)^{\vee}\right)$. The contradiction then follows from Theorem 1 which implies $\mathrm{NA}\left((\mathbf{G}_1 \| \mathbf{G}_2)^{\vee}\right)$.

Theorem 4. *There exists a game* $\mathbf{G}$ *such that the best strategy in winning* $\mathbf{G}$ *is non-adaptive but there exists no system* $\mathbf{S}$ *such that* $\mathbf{G}$ *and* $\mathbf{S}$ *are conditionally equivalent, i.e.,*

$$\mathrm{NA}(\mathbf{G}) \quad \not\Longrightarrow \quad \mathrm{CE}(\mathbf{G}).$$

Acknowledgment

Our research was supported by the Zurich Information Security and Privacy Center (ZISC), the Swiss National Science Foundation (SNF) - project no. 200020-132794, and by the European Research Council under an ERC Starting Grant (259668-PSPC).

References

[BR06] Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 409–426. Springer Berlin Heidelberg, 2006.

[Can01] R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Foundations of Computer Science, 2001. Proceedings. 42nd IEEE Symposium on*, pages 136–145, 2001.

[JÖS12] Dimitar Jetchev, Onur Özen, and Martijn Stam. Understanding adaptivity: Random systems revisited. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology – ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 313–330. Springer Berlin Heidelberg, 2012.

[KL07] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography.* Chapman & Hall/CRC, 2007.

[Mau02] Ueli Maurer. Indistinguishability of random systems. In Lars Knudsen, editor, *Advances in Cryptology — EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 110–132. Springer-Verlag, May 2002.

[Mau11] Ueli Maurer. Constructive cryptography - a new paradigm for security definitions and proofs. In S. Moedersheim and C. Palamidessi, editors, *Theory of Security and Applications (TOSCA 2011)*, volume 6993, pages 33–56. Springer-Verlag, apr 2011.

[Mau13] Ueli Maurer. Conditional equivalence of random systems and indistinguishability proofs. In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 3150–3154, 2013.

[MPR07] Ueli Maurer, Krzysztof Pietrzak, and Renato Renner. Indistinguishability amplification. In Alfred Menezes, editor, *Advances in Cryptology — CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 130–149. Springer-Verlag, August 2007.

[MR11] Ueli Maurer and Renato Renner. Abstract cryptography. In Bernard Chazelle, editor, *The Second Symposium in Innovations in Computer Science, ICS 2011*, pages 1–21. Tsinghua University Press, January 2011.