Random Systems : Indistinguishability and Amplification

Kaushik Sarkar
Roll No: CS0804
M Tech (CS), 1st year
Year: 2009

under the supervision of
Palash Sarkar

Applied Statistics Unit
Indian Statistical Institute
203, B.T. Road, Kolkata
India 700108.

Contents

1 Introduction

Many cryptographic systems may be viewed as a discrete system that interacts with its environment through a sequence of inputs and outputs. Most of the time we are interested in the input-output behaviour (possibly probabilistic) of such discrete systems. Random systems which may be thought as a generalization of random variables can be helpful as a mathematical model for input-output abstraction of discrete systems.

Indistinguishability is another important and recurring theme of cryptographic security definition. For practical purposes one is mostly concerned with computational indistinguishability. But most of the theoretic proofs try to show information theoretic indistingushability between two systems. Though the idea of information theoretic indistingushability may appear only of theoretic interest, they have been successfully applied in the design of real crypto-systems.

Amplification of security is achieved via certain kind of combination of compatible cryptosystems. It can be achieved either in the form of lower distinguishing advantage for the combined system than the component systems or as strengthening the class of attack for the combined system.

1.1 Security Definition Paradigms in Cryptography

There are two main paradigms of cryptographic security definition - indistinguishability and game winning. This two notions are related and the relation will be discussed in detail in the following sections.

1.1.1 Indistinguishability

A distinguisher is an algorithm (possibly adaptive) whose job is to distinguish between two systems. The simplest problem is of distinguishing betweeen two random variables. It can be shown that the success probability or the advantage of the optimal distinguisher is the statistical distance between the two probability distribution.

The security of a cryptosystem is proved by showing that the adavantage of any distinguisher algorithm in distinguishing between the system in discussion and a 'perfect' system (which is unbreakable by definition) is negligibly small. For example let us consider a cryptosystem that uses PRF. First the PRF is replaced by a truely random function to get an 'idealized' system. Then by probability calculations the 'idealized' system and the defined 'perfect' system is shown information-theoretically indistinguishable. Now, if any algorithm for breaking the original cryptosystem exists then it must distinguish between this system and the 'perfect' system and the only way it can do so is by distinguishing between the original system and the 'idealized' system (since, the 'idealized system and the 'perfect' system has been shown to be indistinguishable) i.e. by distinguishing between PRF and truely random function.

1.1.2 Game Winning

The ineraction between an attacker and a cryptosystem can viewed as a one-player game where breaking the system will be considered as winning the game. In such situations security is proved by showing that the probability of the player winning the game is negligibly small.

2 Random Sytems

A discrete system $\mathbf{F}$ takes input $X_i \in \mathcal{X}$ and produces outputs $Y_i \in \mathcal{Y},\ i = 1, 2, 3, \ldots$ The output may depend (possibly probabilistically) on previous inputs and outputs.

Our problem is to capture the input-output behaviour of such systems. Similar kind of problems arise in communication theory also. Suppose we want to abstract out the input-output behaviour of a memory less channel $\mathbf{C}$. This can be achieved by the conditional probability distribution $\mathrm{P}^{\mathbf{C}}_{Y|X}$, where X and Y are the random variables representing respectively the input and output to the channel. This distribution gives a mathematical model of the channel irrespective of its physical description. We do the similar thing here. We model the input-output behaviour of any discrete system by the sequence of conditional probability distributions of Y_i given the values of the inputs $X_1, X_2, \ldots, X_i$ and outputs $Y_1, Y_2, \ldots, Y_{i-1}$ seen so far, for all values of i. This representation of a discrete system is called a random system. More precisely,

Definition 1 (Random System)**.** *An* $(\mathcal{X}, \mathcal{Y})$ **random system** $\mathbf{F}$ *is defined by a sequence of conditional probability distribution* $\mathrm{P}^{\mathbf{F}}_{Y_i|X^iY^{i-1}}$ *for* $i \geq 1$.

This definition of random systems is exact and minimal. Two discrete systems with different input-output behaviour corresponds to two different random systems and two different random systems corresponds to two differently behaving systems. for two systems $\mathbf{F}$ and $\mathbf{G}$ if their input-output behaviour is same, irrespective of their internal working they should correspond to same random system. This idea is formalized in the following definition of equivalent systems

Definition 2. *Two systems* $\mathbf{F}$ *and* $\mathbf{G}$ *are said to be* **equivalent**, *denoted* $\mathbf{F} \equiv \mathbf{G}$ *if they correspond to the same random system, i.e.,* $\forall i \geq 1$

$$\mathrm{P}^{\mathbf{F}}_{Y_i|X^iY^{i-1}} = \mathrm{P}^{\mathbf{G}}_{Y_i|X^iY^{i-1}} \tag{1}$$

A random system $\mathbf{F}$ can be alternatively represented by the sequence of probability distributions $\mathrm{P}^{\mathbf{F}}_{Y^i|X^i} \forall i \geq 1$. But the description is not minimal. The relation between the two definitions are as follows

$$\mathrm{P}^{\mathbf{F}}_{Y^i|X^i} = \prod_{j=1}^{i} \mathrm{P}^{\mathbf{F}}_{Y_j|X^jY^{j-1}} \tag{2}$$

2.1 Special Random Systems

Definition 3 (Random Function/Permutation)**.** *A* stateless *random system* $\mathcal{X} \to \mathcal{Y}$ *(a random permutation on* $\mathcal{X}$*) is a random variable which takes on values from the set of all functions* $\mathcal{X} \to \mathcal{Y}$ *(from the set of all permutations of* $\mathcal{X}$*).*

We denote the set of all random functions and all random permutations by $\mathcal{R}$ and $\mathcal{P}$ respectively.

A *stateful* random function, in addition of being a random function, is consistent; i.e. $X_i = X_j \Rightarrow Y_i = Y_j$. A stateful random permutation is defined in the similar way. We denote the set of all stateful random functions and permutations by $\mathcal{R}_S$ and $\mathcal{P}_S$ respectively. Clearly, $\mathcal{R} \subset \mathcal{R}_S$ and $\mathcal{P} \subset \mathcal{P}_S$.

Example: A *uniform random funciton (URF),* denoted by $\mathbf{R}$, is defined in the following way if both $\mathcal{X}$ and $\mathcal{Y}$ are finite

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

$\mathrm{P}^{\mathbf{R}}_{Y_i|X^iY^{i-1}}(y_i, x^i, y^{i-1})$ is undefined if $x_j = x_k$ for some $j < k < i$ and $y_j \neq y_k$. A *uniform random permutation* $\mathbf{P}$ is also defined in the similar way.

2.2 Composition

Two or more random systems can be composed to obtain a new random system (provided the component systems are input-output compatible). Two kinds of composition are possible.

Definition 4. *The sequential composition for two random systems* $\mathbf{F}$ *and* $\mathbf{G}$*, denoted by* $\mathbf{F} \rhd \mathbf{G}$*, is a random system where the input to the system is fed to* $\mathbf{F}$ *and the output of* $\mathbf{F}$ *is fed to* $\mathbf{G}$*. The output of* $\mathbf{G}$ *is the output of the combined system.*

Similarly the parallel composition of two random systems $\mathbf{F}$ *and* $\mathbf{G}$ *for some quasi-group operation* $\star$ *on the output alphabet, denoted by* $\mathbf{F} \star \mathbf{G}$*, is the random system obtained by feeding the input to both the systems and then combining their outputs by the* $\star$ *operation.*

Cascade of two random systems is another name for sequential composition. Bit-wise ex-OR $\oplus$ is an important example of parallel composition.

2.3 Distinguishing Random Systems

We want to distinguish between two random systems. As discussed earlier, a distinguisher is an algorithm for distinguishing between two random systems and the probability of its success is called its advantage. For two random systems X and X' defined over $\mathcal{X}$ their statistical distance is defined by

$$\delta(X, X') = ||\mathrm{P}_X - \mathrm{P}_{X'}|| \triangleq \frac{1}{2} \sum_{\forall x \in \mathcal{X}} |\mathrm{P}_X(x) - \mathrm{P}_{X'}(x)|. \tag{3}$$

It can be shown that the maximum advantage of any optimal distinguisher for distinguishing between X and X' is exactly $\delta(X, X')$. It is obvious that the job of distinguishing between two random systems will be more difficult.

A distinguisher $\mathbf{D}$ for distinguishing two $(\mathcal{X}, \mathcal{Y})$ random systems $\mathbf{F}$ and $\mathbf{G}$ is a random system which queries both the system with input X_i and observes the outputs Y_i and adaptively determines the next query X_{i+1}. After a specified number k of queries it outputs a decision bit W. More formally

Definition 5 (Distinguisher)**.** *A* $(\mathcal{X}, \mathcal{Y})$*-distinguisher* $\mathbf{D}$ *is a* $(\mathcal{Y}, \mathcal{X})$ *random system which stays one query ahead, i.e. it is defined by a sequence of probability distributions* $\mathrm{P}^{\mathbf{D}}_{X_i|Y^{i-1}X^{i-1}}$ *for all i. In particular* $\mathrm{P}^{\mathbf{D}}_{X_1}$ *is defined even before* $\mathbf{D}$ *is fed any input.* $\mathbf{D}$ *outputs a decision bit* W *after* k *queries.*

$\mathbf{D}\Diamond\mathbf{F}$ denotes the random experiment $\mathbf{D}$ quering $\mathbf{F}$. A $(\mathcal{Y}, \mathcal{X})$*-double-distinguishers* is a system which have access to two $(\mathcal{X}, \mathcal{Y})$-random systems, and which can arbitrary schedule their queries between the two systems. For a $(\mathcal{Y}, \mathcal{X})$-double-distinguisher $\mathbf{D}$ we denote with $\mathbf{D}\Diamond[\mathbf{F}, \mathbf{G}]$ the random experiment where $\mathbf{D}$ queries the two $(\mathcal{X}, \mathcal{Y})$-random systems $\mathbf{F}$ and $\mathbf{G}$. Note that if we instantiate just one of the two systems, we get a standard distinguisher, i.e. $\mathbf{D}\Diamond[\cdot, \mathbf{F}]$ and $\mathbf{D}\Diamond[\mathbf{F}, \cdot]$ is a $(\mathcal{Y}, \mathcal{X})$-distinguisher for any compatible $\mathbf{F}$.

2.3.1 Classes of Distinguisher

One can distinguish different classes of distinguishers by posing restrictions on how the distinguisher can access the system. In particular the following attacks will be of interest to us:

- CPA (Adaptively Chosen Plaintext Attack): This is the most general attack. Here the distinguisher can make any first query X_1 and receives the output Y_1, then it chooses a query X_2 depending on X_1 and Y_1 and receives Y_2, and so on. In general, he can choose the ith query X_i depending on X_{i-1} and Y_{i-1}.

- nCPA (Non-Adaptively Chosen Plaintext Attack): The distinguisher must choose all queries in advance.
- KPA (Known Plaintext Attack): The distinguisher obtains only distinct random inputs (i.e., the choice of input is beyond its control) to the system and the corresponding outputs.

If $\mathbf{F}$ is a permutation, then also its inverse $\mathbf{F}^{-1}$ is well defined. So in the case where the system queried is guaranteed to be a permutation, we can consider an even more powerful attack where the distinguisher can query the system at hand from both directions.

- CCA (Adaptively Chosen Ciphertext Attack): Is defined as CPA but the distinguisher can query from both sides.
- nCCA (Non-Adaptively Chosen Ciphertext Attack): Non adaptive version of CCA.

Definition 6 (ATK_2)**.** *Let* ATK *be one of the classes of distinguishers considered above, then a double distinguisher* $\mathbf{D}$ *(see Definition 5) is in the class* ATK_2 *if for any* $\mathbf{F}$ *the systems* $\mathbf{D}\Diamond[\cdot,\mathbf{F}]$ *and* $\mathbf{D}\Diamond[\mathbf{F},\cdot]$ *are* ATK *distinguishers.*

2.3.2 Distinguishing Advantage

For given $k \geq 1$, the two random experiments $\mathbf{D}\Diamond\mathbf{F}$ and $\mathbf{D}\Diamond\mathbf{G}$ each define a transcript X^kY^k, a random variable with alphabet $\mathcal{X}^k \times \mathcal{Y}^k$.

$$\mathrm{P}^{\mathbf{D}\Diamond\mathbf{F}}_{X^kY^k}(x^k,y^k) = \prod_{i=1}^{k} \mathrm{P}^{\mathbf{D}}_{X_i|Y^{i-1}X^{i-1}}(x_i,y^{i-1},x^{i-1})\mathrm{P}^{\mathbf{F}}_{Y_i|X^iY^{i-1}}(y_i,x^i,y^{i-1}) \tag{4}$$

The distinguisher takes its decision by checking this transcript. The distinguishing advantage of a distingusher can be defined in three different ways, two of them are equivalent and the other one can be related with them.

Definition 7. *The* advantage of distinguisher $\mathbf{D}$ *for random systems* $\mathbf{F}$ *and* $\mathbf{G}$*, for* k *queries, denoted* $\delta^{\mathbf{D}}_k(\mathbf{F},\mathbf{G})$*, is defined as*

$$\delta^{\mathbf{D}}_k(\mathbf{F},\mathbf{G}) \triangleq |\mathrm{P}^{\mathbf{D}\Diamond\mathbf{F}}(W=1) - \mathrm{P}^{\mathbf{D}\Diamond\mathbf{G}}(W=1)|$$

For a class ATK *of distinguishers, the advantage of the best* $\mathbf{D}$ *in* ATK*, asking atmost k queries, is denoted as*

$$\delta^{\mathbf{ATK}}_k(\mathbf{F},\mathbf{G}) \triangleq \max_{\mathbf{D}\in\mathrm{ATK}} \delta^{\mathbf{D}}_k(\mathbf{F},\mathbf{G})$$

To state an equivalent definition of the advantage we need the following definition.

Definition 8. *For two compatible systems* $\mathbf{F}$ *and* $\mathbf{G}$*,* $\langle\mathbf{F},\mathbf{G}\rangle$ *denotes the random system which is equal to system* $\mathbf{F}$ *or* $\mathbf{G}$ *with probability* $\frac{1}{2}$ *each. To make the independent unbiased binary random variable, say* Z*, selecting between* $\mathbf{F}$ *(for* $Z=0$*) and* $\mathbf{G}$ *(for* $Z=1$*) explicit, we write* $\langle\mathbf{F},\mathbf{G}\rangle_Z$

The advantage $\delta^{\mathbf{D}}_k(\mathbf{F},\mathbf{G})$ can be defined equivalently in terms of the probability that $\mathbf{D}$, interacting with the mixed system $\langle\mathbf{F},\mathbf{G}\rangle_Z$, guesses Z correctly:

Lemma 1. *For every distinguisher* $\mathbf{D}$*,*

$$\delta^{\mathbf{D}}_k(\mathbf{F},\mathbf{G}) = 2|\mathrm{P}^{\mathbf{D}\Diamond\langle\mathbf{F},\mathbf{G}\rangle_Z}(W=Z) - \frac{1}{2}|.$$

Another useful lemma which says that $\langle \mathbf{F}, \mathbf{G} \rangle_Z$ is kind of half way between $\mathbf{F}$ and $\mathbf{G}$ is the following:

Lemma 2. *For every* $\mathbf{D}$, $\delta_k^{\mathbf{D}}(\mathbf{F}, \langle \mathbf{F}, \mathbf{G} \rangle_Z) = \frac{1}{2}\delta_k^{\mathbf{D}}(\mathbf{F}, \mathbf{G})$.

The other alternative definition of advantage is based on the concept of statistical distance:

Definition 9. *For* $k \geq 1$*, the advantage of* $\mathbf{D}$ *after* k *queries in distinguishing* $\mathbf{F}$ *from* $\mathbf{G}$*, denoted* $\Delta_k^{\mathbf{D}}(\mathbf{F}, \mathbf{G})$*, is the statistical difference between the transcripts.*

$$\Delta_k^{\mathbf{D}}(\mathbf{F}, \mathbf{G}) \stackrel{\Delta}{=} ||\mathrm{P}_{X^k Y^k}^{\mathbf{D} \diamondsuit \mathbf{F}} - \mathrm{P}_{X^k Y^k}^{\mathbf{D} \diamondsuit \mathbf{G}}|| \tag{5}$$

For the best ATK *of distinguishers* $\mathbf{D}$*, asking atmost k queries,*

$$\Delta_k^{\mathbf{ATK}}(\mathbf{F}, \mathbf{G}) \stackrel{\Delta}{=} \max_{\mathbf{D} \in \mathrm{ATK}} \Delta_k^{\mathbf{D}}(\mathbf{F}, \mathbf{G})$$

It can be shown that for all $\mathbf{D}$, $\delta_k^{\mathbf{D}}(\mathbf{F}, \mathbf{G}) \leq \Delta_k^{\mathbf{D}}(\mathbf{F}, \mathbf{G})$ and for the distinguisher $\mathbf{D}$ which determines W optimally after checking the transcript the equality holds. We will use this definition of advantage throughout the rest of the report.

2.4 Monotone Binary Output and Game-Winning

For many kinds of cryptographic systems it is convenient to consider a condition imposed on some internal state (may be an internal random variable) of the system. The condition is binary in the sense that it can either hold or fail, i.e. can be modeled by an indicator random varible, and the conditions are monotonic because once they fail to satisfy they remain so for the rest of the time, for example "the input to some internal system is distinct (no collosion)" is a monotone binary condition.

Such systems with a monotone binary condition can be modeled by a random system with an additional 0/1 output. The monotonicity is achieved by setting it 0 at the beginning and once the system fails to meet the condition turning it to 1 and then keeping it unchanged. More formally:

Definition 10 (MBO)**.** *A random-system with a* monotone binary output (MBO) $\mathbf{S}$ *is a* $(\mathcal{X}, \mathcal{Y} \times \mathcal{A})$*-random system where* $\mathcal{A} = \{0, 1\}$ *and the* MBO *satisfies* $A_i = 1 \Rightarrow A_{i+1} = 1$

For such a random system $\mathbf{S}$ *with* MBO *we get two derived systems:*

- $\mathbf{S}^{\rightarrow}$ *is a* $(\mathcal{X}, \mathcal{Y})$ *obtained from* $\mathbf{S}$ *by ignoring its* A *output, i.e. applying the following function to its output:* $(y, b) \mapsto y$
- $\mathbf{S}^{\dashv}$ *is a* $(\mathcal{X}, \{\mathcal{Y} \cup \perp\} \times \mathcal{A})$ *random system which is identical to* $\mathbf{S}$ *as long as binary output is 0, but its* Y *output is masked by* $\perp$ *when the binary output turns 1, i.e. the following function is applied to the output of* $\mathbf{S}$*:*

$$(y, b) \mapsto (y', b), \text{where } y' = \begin{cases} y & \text{if } b = 0 \\ \perp & \text{if } b = 1 \end{cases}$$

We will use $\mathbf{S}$ and $\mathbf{T}$ to denote random systems with MBO and $\mathbf{F}$ and $\mathbf{G}$ for systems without one. We will often add an MBO to a system which previously had none. We will use '$\hat{}$' to denote addition of an MBO. Clearly, $\hat{\mathbf{F}}^{\rightarrow} \equiv \mathbf{F}$.

2.4.1 Game-Winning

A one-player game can be modeled by a $(\mathcal{X}, \mathcal{Y}\times\mathcal{A})$ random system $\mathbf{S}$ with an MBO and the player(provoker) can be modeled by a $(\mathcal{Y}, \mathcal{X})$-distinguisher $\mathbf{D}$ whose sole objective is to win the game, i.e. turn the MBO of $\mathbf{S}$ to 1 in k interactions. Clearly the winning probability of $\mathbf{D}$ is the probablity of turning the MBO of $\mathbf{S}$ to 1. More precisely,

Definition 11 (Winning advantage)**.** *For a $(\mathcal{X}, \mathcal{Y} \times \{0,1\})$-random system $\mathbf{S}$ with an MBO (called A_i) and for a distinguisher $\mathbf{D}$, we denote with $\nu_k^{\mathbf{D}}(\mathbf{S})$ the probability that $\mathbf{D}$ wins the game within k queries* (i.e. winning advantage)*:*

$$\nu_k^{\mathbf{D}}(\mathbf{S}) \stackrel{\Delta}{=} \mathrm{P}^{\mathrm{D}\Diamond\mathrm{S}}(A_k = 1) \tag{6}$$

For a class ATK *of distinguishers, the winning probability of the best $\mathbf{D}$ in* ATK *within k queries is denoted as*

$$\nu_k^{\mathbf{ATK}}(\mathbf{S}) \stackrel{\Delta}{=} \max_{\mathbf{D}\in\mathbf{ATK}} \nu_k^{\mathbf{D}}(\mathbf{S}) \tag{7}$$

For the class of all distinguishers we simply write $\nu_k(\mathbf{S})$.
For a double-distinguisher $\mathbf{D}$, we denote with $\nu_k^{\mathbf{D}}(\mathbf{S}, \mathbf{T})$ the advantage of $\mathbf{D}$ in setting both MBO*s to 1 making k queries to each system respectively.*

$$\nu_k^{\mathbf{D}}(\mathbf{S}, \mathbf{T}) \stackrel{\Delta}{=} \mathrm{P}^{\mathbf{D}\Diamond[\mathbf{S},\mathbf{T}]}(A_k = 1 \wedge B_k = 1) \quad \textit{and} \quad \nu_k^{\mathbf{ATK_2}}(\mathbf{S}, \mathbf{T}) \stackrel{\Delta}{=} \max_{\mathbf{D}\in\mathbf{ATK_2}} \nu_k^{\mathbf{D}}(\mathbf{S}, \mathbf{T}). \tag{8}$$

If two random systems $\mathbf{S}$ and $\mathbf{T}$ with MBOs are equivalent while the MBOs are 0, then clearly setting the MBO to 1 is equally difficult in both, i.e.

$$\mathbf{S}^{\dashv} = \mathbf{T}^{\dashv} \Rightarrow \forall \mathbf{D}, k : \nu_k^{\mathbf{D}}(\mathbf{S}) = \nu_k^{\mathbf{D}}(\mathbf{T}) \tag{9}$$

2.5 Relating Indistinguishability and Game-winning

2.5.1 From Game-winning to Indistinguishability

From the following lemma we get an upper bound of the distinguishing advantage of a distinguisher $\mathbf{D}$ from its winning advantage.

Lemma 3. *If $\mathbf{S}^{\dashv} \equiv \mathbf{T}^{\dashv}$, then for any distinguisher $\mathbf{D}$ and any $k \in \mathbb{N}$*

$$\Delta_k^{\mathbf{D}}(\mathbf{S}^{\dashv}, \mathbf{T}^{\dashv}) \leq \nu_k^{\mathbf{D}}(\mathbf{S}) = \nu_k^{\mathbf{D}}(\mathbf{T}) \tag{10}$$

The proof is easy and obtained from expanding the left-hand side by the Equation (5) and then applying an elementary inequality.

From the above inequality, if we add MBOs to $\mathbf{F}$ and $\mathbf{G}$ to get $\hat{\mathbf{F}}$ and $\hat{\mathbf{G}}$ such that $\hat{\mathbf{F}}^{\dashv} \equiv \hat{\mathbf{G}}^{\dashv}$ then we have,

$$\Delta_k^{\mathbf{D}}(\mathbf{F}, \mathbf{G}) \leq \nu_k^{\mathbf{D}}(\hat{\mathbf{F}}) = \nu_k^{\mathbf{D}}(\hat{\mathbf{G}}) \tag{11}$$

2.5.2 From Indistinguishability to Game-Winning

The following lemma is a converse of the previous one in some sense and it is a very useful tool in proving the subsequent results. The proof of the lemma is somewhat technical.

Lemma 4. *Let* $\mathbf{F}$ *and* $\mathbf{G}$ *be* $(\mathcal{X}, \mathcal{Y})$*-random systems. Then there exists systems* $\hat{\mathbf{F}}$ *and* $\hat{\mathbf{G}}$ *such that* $\hat{\mathbf{F}}^{\rightarrow} \equiv \mathbf{F}$*,* $\hat{\mathbf{G}}^{\rightarrow} \equiv \mathbf{G}$*,* $\hat{\mathbf{F}}^{\dashv} \equiv \hat{\mathbf{G}}^{\dashv}$ *and*
for any distinguisher $\mathbf{D}$ *and any* $k \in \mathbb{N}$

$$\Delta_k^{\mathbf{D}}(\mathbf{F}, \mathbf{G}) = \nu_k^{\mathbf{D}}(\hat{\mathbf{F}}) = \nu_k^{\mathbf{D}}(\hat{\mathbf{G}}) \tag{12}$$

3 Amplification

The term "amplification" is used in two different meaning:

- **Reduction of Distinguishing Advantage**. By suitable combination of two component systems we can get a system whose distinguishing advantage is less than the product of the advantage of the component systems. In fact, it can be shown that if $\mathbf{F}$ and $\mathbf{G}$ are systems, for each of which the best distinguishers advantage in distinguishing it from a uniform random function is bounded by ϵ and ϵ', respectively, then the system $\mathbf{F} \star \mathbf{G}$ obtained by using $\mathbf{F}$ and $\mathbf{G}$ in parallel and combining their outputs with $\star$, can be distinguished with advantage at most $2\epsilon\epsilon'$ from a uniform random function (for the same number of queries issued by the distinguisher).

- **Strengthening Attack**. Under certain conditions, for certain type of combinations it can be shown that the combined system can resist stronger class of attacks than the component systems. In the subsequent sections we will prove that the adaptive distinguishing advantage of a "neutralizing" combination of two systems is bounded by the sum of the individual distinguishing advantages for a weaker distinguisher class (e.g. non-adaptive, or for permutations, one-sided instead of two-sided queries).

Now as a motivating example we will consider the case of random variables for the first type of amplification. First we define the distance of a random variable X from uniform by $d(X) \stackrel{\Delta}{=} \delta(X, U)$, (see equation 3) where U is a uniform random variable on $\mathcal{X}$. The advantage of the best distinguisher for X and X' is $\delta(X, X')$.

Lemma 5. *For any two independent random variables* X *and* Y *over a finite domain* $\mathcal{X}$ *and any quasi-group operation* $\star$ *on* X*,*

$$d(X, Y) \leq 2d(X)d(Y). \tag{13}$$

This bound is tight, as the following example illustrates.
Example 1. Consider two independent biased bits, X with a 40/60-bias and Y with a 30/70-bias. Then $d(X) = 0.1,\ d(Y) = 0.2$, and $d(X \oplus Y) = 0.04\ (= 2 \cdot 0.1 \cdot 0.2)$, since $X \oplus Y$ is 54/46-biased.

Next, we generalize the concept of combination operators and define a class of operators called "neutralizing" operator which will be very useful in the ensuing discussion.

3.1 Neutralizing Combination

Definition 12 (Composition Operator)**.** *A composition operator* $\bowtie$ *for a class of random systems* $\mathcal{I}$ *is a random system which expects oracle access to two systems from* $\mathcal{I}$*. With* $\mathbf{F} \bowtie \mathbf{G}$ *we denote* $\bowtie$ *where the first and second oracle are instantiated with* $\mathbf{F}$ *and* $\mathbf{G}$*, respectively.*

We will only consider $\bowtie$ *where (i) for any* $\mathbf{F}, \mathbf{G} \in \mathcal{I}$*, also* $\mathbf{F} \bowtie \mathbf{G} \in \mathcal{I}$*, and that (ii) on every invocation of* $\mathbf{F} \bowtie \mathbf{G}$ *the system* $\mathbf{F}$ *and* $\mathbf{G}$ *is invoked exactly once.*

Definition 13 (Neutralizing Composition Operator)**.** *A composition operator* $\bowtie$ *is called neutralizing for the pairs* $(\mathbf{F}, \mathbf{H})$ *and* $(\mathbf{G}, \mathbf{J})$ *of (independent) systems if*

$$\mathbf{F} \bowtie \mathbf{J} \equiv \mathbf{H} \bowtie \mathbf{G} \equiv \mathbf{H} \bowtie \mathbf{J} \equiv \mathbf{Q} \tag{14}$$

for some $\mathbf{Q}$*.*

3.2 Winning Independent Games

The next lemma says that the best combined strategy for winning two independent games is actually as good as, and no better than applying the best individual strategies for the two games separately. To motivate the lemma we can think of a card player who is playing black-jack at two different tables and let us assume that he can schedule his moves in the two tables completely arbitrarily and with full knowledge of the situation at the other table. Certainly, if the games are not related in any way then this strategy as good as scheduling the moves in the two tabels depending on the information available at that table only. In other words, in case of independentt games, having information about what is happening at the other table doesn't help at all.

Lemma 6. *For any random systems* $\mathbf{S}$ *and* $\mathbf{T}$ *with* MBOs*, and any attack* ATK $\in \{$nCPA, CPA$\}$*, or if* $\mathbf{S}^{\rightarrow}$*,*$\mathbf{T}^{\rightarrow}$ *are permutations,* ATK $\in \{$nCCA, CCA$\}$*,*

$$\nu_k^{\mathbf{ATK_2}}(\mathbf{S}, \mathbf{T}) = \nu_k^{\mathbf{ATK}}(\mathbf{S}) \cdot \nu_k^{\mathbf{ATK}}(\mathbf{T}) \tag{15}$$

Though the statement appears to be obvious the proof is somewhat tricky and requires induction. The basic technique involves replacing the arbitrary interaction between the two systems by a sequence of messages passed between the two systems and then dispensing with the messages altogether in a systematic manner.

$\mathbf{S} \overset{\wedge}{\bowtie} \mathbf{T}$ denotes the system $\mathbf{S} \bowtie \mathbf{T}$, whose MBO is set to 1 when MBOs of both $\mathbf{S}$ and $\mathbf{T}$ are 1 and to 0 otherwise. Now, let us consider an attacker whose aim is to break both the systems. The following lemma says that the task is no easier when we have access to the combined system than when we have access to the individual systems separately.

Lemma 7. *For any composition operator* $\bowtie$ *and any class* ATK *of distinguishers, we have for any* $k \in \mathbb{N}$ *and* $\mathbf{S}, \mathbf{T}$

$$\nu_k^{\mathbf{ATK}}(\mathbf{S} \overset{\wedge}{\bowtie} \mathbf{T}) \leq \nu_k^{\mathbf{ATK_2}}(\mathbf{S}, \mathbf{T}) \tag{16}$$

3.3 Direct Product Theorem

We now state a very important theorem

Theorem 1. *If* $\bowtie$ *is neutralizing for the pairs* $(\mathbf{F}, \mathbf{I})$ *and* $(\mathbf{G}, \mathbf{I})$ *and* $\mathbf{I} \bowtie \mathbf{I} \equiv \mathbf{I}$*, then* $\forall k \in \mathbb{N}$ *and all class* ATK

$$\Delta_k^{\mathbf{ATK}}(\mathbf{F} \bowtie \mathbf{G}, \mathbf{I}) \leq 2 \cdot \Delta_k^{\mathbf{ATK}}(\mathbf{F}, \mathbf{I}) \cdot \Delta_k^{\mathbf{ATK}}(\mathbf{G}, \mathbf{I}) \tag{17}$$

The theorem is very general and abstract in nature. Actually the following corollary is much more concrete:

Corollary 1. *For* ATK $\in \{$nCPA, CPA, nCCA, CCA$\}$ *and any stateless random permutations* $\mathbf{F}, \mathbf{G}$

$$\Delta_k^{\mathbf{ATK}}(\mathbf{F} \rhd \mathbf{G}, \mathbf{P}) \leq 2 \cdot \Delta_k^{\mathbf{ATK}}(\mathbf{F}, \mathbf{P}) \cdot \Delta_k^{\mathbf{ATK}}(\mathbf{G}, \mathbf{P}) \tag{18}$$

For ATK $\in \{$nCPA, CPA$\}$ *and any (possibly stateful) random functions* $\mathbf{F}, \mathbf{G}$

$$\Delta_k^{\mathbf{ATK}}(\mathbf{F} \star \mathbf{G}, \mathbf{R}) \leq 2 \cdot \Delta_k^{\mathbf{ATK}}(\mathbf{F}, \mathbf{R}) \cdot \Delta_k^{\mathbf{ATK}}(\mathbf{G}, \mathbf{R}) \tag{19}$$

3.4 When Two Weak Make One Strong

The next theorem is also a very important one. It states that if two components which are safe only against some weak class of distinguishers are combined then their combination is safe against some stronger class of distinguishers, provided some conditions are satisfied.

Theorem 2. *Consider three classes of attacks, a strong one* ATK *and two weak ones denoted* wATK *and* wATK′. *Let* $\bowtie$ *be a neutralizing composition operator for the pairs* $(\mathbf{F}, \mathbf{I})$ *and* $(\mathbf{G}, \mathbf{I})$. *If* $\exists \alpha, \alpha' \in \mathbb{R}$ *such that for all random systems* $\mathbf{S}$ *with an* MBO *and* $\forall k \in \mathbb{N}$

$$\nu_k^{\mathbf{ATK}}(\mathbf{S} \bowtie \mathbf{I}) \leq \nu_k^{\mathbf{wATK}}(\mathbf{S} \bowtie \mathbf{I}) + \alpha \quad \textit{and} \quad \nu_k^{\mathbf{ATK}}(\mathbf{I} \bowtie \mathbf{S}) \leq \nu_k^{\mathbf{wATK'}}(\mathbf{I} \bowtie \mathbf{S}) + \alpha' \tag{20}$$

Then for all $\mathbf{F}, \mathbf{G}$ *and* $\forall k \in \mathbb{N}$

$$\Delta_k^{\mathbf{ATK}}(\mathbf{F} \bowtie \mathbf{G}, \mathbf{I} \bowtie \mathbf{I}) \leq \Delta_k^{\mathbf{wATK}}(\mathbf{F}, \mathbf{I}) + \Delta_k^{\mathbf{wATK'}}(\mathbf{G}, \mathbf{I}) + \alpha + \alpha'. \tag{21}$$

Similarly more concrete corollary is:

Corollary 2. *For any stateless random permutations* $\mathbf{F}$ *and* $\mathbf{G}$

$$\Delta_k^{\mathbf{CPA}}(\mathbf{F} \rhd \mathbf{G}, \mathbf{P}) \leq \Delta_k^{\mathbf{nCPA}}(\mathbf{F}, \mathbf{P}) + \Delta_k^{\mathbf{KPA}}(\mathbf{G}, \mathbf{P}) \tag{22}$$

$$\Delta_k^{\mathbf{CCA}}(\mathbf{F} \rhd \mathbf{G}^{-1}, \mathbf{P}) \leq \Delta_k^{\mathbf{nCPA}}(\mathbf{F}, \mathbf{P}) + \Delta_k^{\mathbf{nCPA}}(\mathbf{G}, \mathbf{P}) \tag{23}$$

For any (possibly stateful) random functions $\mathbf{F}, \mathbf{G}$

$$\Delta_k^{\mathbf{CPA}}(\mathbf{F} \star \mathbf{G}, \mathbf{R}) \leq \Delta_k^{\mathbf{nCPA}}(\mathbf{F}, \mathbf{R}) + \Delta_k^{\mathbf{nCPA}}(\mathbf{G}, \mathbf{R}) \tag{24}$$

References

[1] Ueli Maurer – *Indistinguishability of Random Systems*, Advances in Cryptology – EUROCRYPT'02, pages 110-132, (2002)

[2] Ueli Maurer, Krzysztof Pietrzak, Renato Renner – *Indistinguishabiltiy Amplification*, Advances in Cryptology – CRYPTO 2007, pages 130-149, (2007)