Foundations of Cryptography

Notes of lecture No. 6 (given on Apr. 9th)

Notes taken by Michal Seidmann and Nir Dvir

Summary

In this lecture we recall the definition of semantic security, and introduce the central notion of *indistinguishability.* We will use this concept in another definition of secure encryption scheme: *Security in the sense of indistinguishability of encryptions.* We claim that an encryption scheme which is secure according to the last definition, is also secure according to the first one.

1. Semantic Security

Semantic security was defined in the previous lecture using probability distributions. In the sequel, we state this definition in terms of random variables.

Polynomial Random Variable

Let X_n be a random variable ranging over $\{0,1\}^n$ (i.e. X_n maps elements of some sample space Ω to $\{0,1\}^n$). Actually, we shall speak of sequences of random variables $\{X_n\}_{n\in\mathbf{N}}$, such that for all n, the random variable X_n is distributed over $\{0,1\}^n$.

The sequence $\{X_n\}_{n\in\mathbf{N}}$ is said to be a *sequence of polynomial random variables,* iff there exists a probabilistic polynomial algorithm S, such that $X_n = S(1^n)$ (We would like S to be polynomial-time in n , and therefore it is given the input n in unary). We call S a *sampling* algorithm for $\{X_n\}_{n\in\mathbf{N}}$.

We will sometimes say: " X_n is a polynomial random variable" as a short way of saying: " $\{X_n\}_{n\in\mathbf{N}}$ is a sequence of polynomial random variables".

Examples:

I. Given the unary input 1^n , algorithm S_1 tosses n coins, and outputs the outcome. In this case: $X_n = S_1(1^n)$ is uniformly distributed over the sample space $\{0,1\}^n$. i.e.

$$\forall\, \alpha \in \{0,1\}^n \quad \text{Prob}\,(X_n = \alpha) = 2^{-n}$$

II. Given the unary input 1^n, algorithm S_2 always outputs 1^n. Here: $X_n = S_2(1^n)$ is identically 1^n . Thus, Prob ($X_n = 1^n$) = 1 , and: $\forall \alpha \in \{0,1\}^n$, $\alpha \neq 1^n \Rightarrow$ Prob ($X_n = \alpha$) = 0

III. Given 1^n , algorithm S_3 tosses $\frac{n}{2}$ coins. Let r be the outcome. The output of S_3 is $r \circ r$. One can

easily see that

$$a \neq b \;\Rightarrow\; \text{Prob}\,(X_n = a \circ b) = 0$$

$$a = b \;\Rightarrow\; \text{Prob}\,(X_n = a \circ b) = 2^{-\frac{n}{2}}$$

where $|a| = |b| = \frac{n}{2}$.

It is important to note that not all sequences of random variables can be efficiently sampled (i.e. by a polynomial algorithm). In order to see this, note that the cardinality of the set of all sequences of random variables is $\aleph$ (note that this is a set of infinite sequences), while the cardinality of the set of all polynomial-time sampling algorithms is $\aleph_0$. It follows that most of the sequences of random variables cannot be polynomially sampled.

Definition:

An encryption scheme (G,E,D) is said to be *Semantically Secure* iff for every sequence $\{X_n\}_{n \in N}$ of [polynomial] random variables, for every [polynomial] function h , for every function f and for every probabilistic polynomial algorithm A , there exists a probabilistic polynomial algorithm A' such that for every constant $c > 0$ and for every sufficiently large n , the following inequality holds:

$$\text{Prob}\left[A(E_{G(1^n)}(X_n),\, h(X_n),\, 1^n) = f(X_n)\right] \leq \text{Prob}\left[A'(h(X_n),\, 1^n) = f(X_n)\right] + \frac{1}{n^c}$$

while the probability is taken over X_n's distribution and the coin tosses of A or A', G and E .

Remarks:

(1) The intuition, as in the last lecture, is that the encryption does not add any further information to what was known a-priori about the message.

(2) This definition is actually two different definitions: The one including the brackets ([ ]) is the definition for *Uniform* Semantic Security, and the one excluding the brackets is for *Non-Uniform* Semantic Security. In the non-uniform case, wherever we mention the words *'polynomial algorithm'* we mean *'a non-uniform polynomial algorithm'* . Obviously, probabilism can be removed in these non-uniform algorithms.

Clearly, if an encryption scheme is semantically secure in the non-uniform sense, then it is also secure in the uniform sense. But, we still give both definitions, because it is "easier" to prove the existence of uniform semantically secure encryption schemes than the existence of non-uniform ones. By *'easier'* we mean that the required assumptions seem less strong in the uniform case. In this case we will assume existence of uniform one-way permutation, while in the second case we will have to assume that these

one-way permutations cannot be reversed by non-uniform polynomial algorithms.

We would like to introduce another definition for secure encryption schemes, perhaps less natural (more technical), but showing the existence of secure encryption schemes will be simpler using this new definition. Also, this definition will be more convenient to deal with, when the encryption scheme is used in a cryptographic protocol.
Before giving this definition we introduce and give examples of a notion central to this course: "Polynomial indistinguishability ".

2. Polynomial Indistinguishability.

We introduce and motivate the notion of polynomial indistinguishability in the context of secure encryption, but this notion is of general importance to complexity theory and will be used throughout the course in other context as well. In particular, many of the central cryptographic notions refer to the concept of indistinguishability . Intuitively, while dealing with encryption schemes, polynomial indistinguishability means the lack of the ability to decide efficiently, given two messages M_1, M_2 and an encryption $E(M_i)$ of one of them, to which message the encryption corresponds. In a general sense, one can look at indistinguishability this way: Given an object, which was chosen with equal probability from one of two baskets, it cannot be guessed successfully (with a probability significantly greater than ½), from which of the baskets it was taken.

If the sampling algorithms are deterministic, then it can be guessed successfully (with probability 1), which one of the two random variables was sampled, therefore the notion of indistinguishability is meaningless in this case.

Definition : Two sequences $\{X_n\}_{n\in\mathbf{N}}$, $\{Y_n\}_{n\in\mathbf{N}}$ of random variables (not necessarily polynomial), are *polynomially indistinguishable* iff for every polynomial algorithm A, for every $c>0$ and for every sufficiently large n:

$$\text{Prob}\left[A(X_n)=1\right]-\text{Prob}\left[A(Y_n)=1\right] < \frac{1}{n^c}$$

Intuitively, we can interpret this definition by considering that $A(\alpha)=1$ indicates that α *is from the* X_n *sample*, while $A(\alpha)=0$, indicates that α *is from the* Y_n *sample* . Thus, the meaning is that there is no efficient way to distinguish from which one of the spaces the sample was taken. In other words, the "indication" is oblivious of the truth, as it has essentially the same probability on both samples.

Remarks:

1) This definition is the uniform one. The non-uniform definition will be the same, but the word *'algorithm'* will stand for *'non-uniform algorithm'* .

2) If we replace the inequality at the end of the definition with:

$$|\text{Prob}\left[A(X_n)=1\right]-\text{Prob}\left[A(Y_n)=1\right]| \prec \frac{1}{n^c} \qquad (*)$$

the resultant definition is equivalent.

proof:

I. It is obvious that the condition (*) implies the condition in the original definition.

II. If the condition (*) fails, then there exist a polynomial algorithm A , a constant $c \succ 0$ and an infinite sequence $B \subseteq \mathbf{N}$, such that

$$\forall i \in B \quad |\text{Prob}\left[A(X_i)=1\right]-\text{Prob}\left[A(Y_i)=1\right]| \geq \frac{1}{i^c}$$

This sequence has an infinite subsequence $B' \subseteq B$, such that

$$\forall i \in B' \quad \text{Prob}\left[A(X_i)=1\right]-\text{Prob}\left[A(Y_i)=1\right] \geq \frac{1}{i^c}$$

or an infinite subsequence $B'' \subseteq B$, such that

$$\forall i \in B'' \quad -\left[\text{Prob}\left[A(X_i)=1\right]-\text{Prob}\left[A(Y_i)=1\right]\right] \geq \frac{1}{i^c}$$

In the first case the original definition's condition is immediately contradicted, while in the second case we can present an algorithm A' such that $A'(\alpha)=1-A(\alpha)$ and thus

$$\forall i \in B'' \quad -\text{Prob}\left[A(X_i)=1\right]+\text{Prob}\left[A(Y_i)=1\right] \geq \frac{1}{i^c}$$

$$\Leftrightarrow \forall i \in B'' \quad -\left[1-\text{Prob}\left[A'(X_i)=1\right]\right]+1-\text{Prob}\left[A'(Y_i)=1\right] \geq \frac{1}{i^c}$$

$$\Leftrightarrow \forall i \in B'' \quad \text{Prob}\left[A'(X_i)=1\right]-\text{Prob}\left[A'(Y_i)=1\right] \geq \frac{1}{i^c}$$

and again, the original definition's condition fails. ■

3) As was said before, the intuition of indistinguishability is that for every algorithm A, given α - taken at random from one of the two distributions, A cannot successfuly guess from which one of the two random variables α was sampled. i.e. The probability of having a successful guess is not significantly greater than ½ . The definition given here is consistent with this intuition. Namely:

Let $\{X_n\}$, $\{Y_n\}$ be two sequences of random variables. Let T_n be a random variable which is uniformly distibuted over $\{0,1\}$ and independent of X_n and Y_n. Let Z_n be the random variable:

$$Z_n = \begin{cases} Y_n & T_n = 0 \\ X_n & T_n = 1 \end{cases}$$

Let A be a probabilistic polynomial algorithm that given α as input, outputs 1 or 0 (which may be interpreted as α is a X_n or Y_n sampling, respectively).

Note that intuitively, Prob $(A(\alpha) = T_n)$ means that A decides successfully if α is from the X_n or Y_n samples.

Then, the two following conditions are equivalent :

$$\exists N,\ \forall n > N: \quad \left| \text{Prob}\left[A(X_n) = 1\right] - \text{Prob}\left[A(Y_n) = 1\right] \right| < \frac{1}{n^c} \tag{1}$$

$$\exists N,\ \forall n > N: \quad \text{Prob}\left[A(\alpha) = T_n\right] < \frac{1}{2} + \frac{1}{2 \cdot n^c} \tag{2}$$

i.e. it is equivalent to say : "The probability of A outputing a correct answer is not significantly greater than ½ " or " A cannot distinguish between $\{X_n\}$ and $\{Y_n\}$ ".

Proof:

$$\exists N,\ \forall n > N: \quad \left| \text{Prob}\left[A(X_n) = 1\right] - \text{Prob}\left[A(Y_n) = 1\right] \right| < \frac{1}{n^c}$$

$$\Leftrightarrow \exists N,\ \forall n > N: \quad \text{Prob}\left[A(X_n) = 1\right] - \text{Prob}\left[A(Y_n) = 1\right] < \frac{1}{n^c}$$

$$\Leftrightarrow \exists N,\ \forall n > N: \quad \text{Prob}\left[A(X_n) = 1\right] - \left[1 - \text{Prob}\left[A(Y_n) = 0\right]\right] < \frac{1}{n^c}$$

$$\Leftrightarrow \exists N,\ \forall n > N: \quad \text{Prob}\left[A(X_n) = 1\right] + \text{Prob}\left[A(Y_n) = 0\right] < 1 + \frac{1}{n^c}$$

$$\Leftrightarrow \exists N,\ \forall n > N:$$

$$\text{Prob}\left[A(Z_n) = 1 \mid T_n = 1\right] + \text{Prob}\left[A(Z_n) = 0 \mid T_n = 0\right] < 1 + \frac{1}{n^c}$$

$$\Leftrightarrow \exists N,\ \forall n > N:$$

$$\frac{1}{2} \cdot \left[\text{Prob}\left[A(Z_n) = 1 \mid T_n = 1\right] + \text{Prob}\left[A(Z_n) = 0 \mid T_n = 0\right]\right] < \frac{1}{2} + \frac{1}{2 \cdot n^c}$$

$\Leftrightarrow \exists N,\ \forall n > N$:

$$\text{Prob}\left[A(Z_n)=1 \,|\, T_n=1\right]\cdot\text{Prob}\,(T_n=1)+\text{Prob}\left[A(Z_n=0 \,|\, T_n=0\right]\cdot\text{Prob}\,(T_n=0) < \frac{1}{2}+\frac{1}{2\cdot n^c}$$

$$\Leftrightarrow \exists N,\ \forall n > N:\ \text{Prob}\left[A(Z_n)=T_n\right] < \frac{1}{2}+\frac{1}{2\cdot n^c} \qquad \blacksquare$$

Examples:

1) X_n is uniformly distributed over $\{0,1\}^n$, Y_n is uniformly distributed over $\{\sigma_1\cdots\sigma_n \,|\, \bigoplus_{i=1}^{n} \sigma_i = 0\}$.

$\{X_n\}$, $\{Y_n\}$ are polynomially distinguishable.

Proof: Let A be the following algorithm:

Given $\alpha=\alpha_1\circ\cdots\circ\alpha_n$, $A(\alpha)=\bigoplus_{i=1}^{n}\alpha_i$.

$\text{Prob}\left[A(X_n)=1\right]=½$, since exactly half of the strings $\alpha\in\{0,1\}^n$ satisfy $\bigoplus_{i=1}^{n}\alpha_i=1$.

$\text{Prob}\left[A(Y_n)=1\right]=0$, since Y_n ranges over strings α with $\bigoplus_{i=1}^{n}\alpha_i=0$.

$$\Rightarrow \quad \text{Prob}\left[A(X_n)=1\right]-\text{Prob}\left[A(Y_n)=1\right]=\frac{1}{2}$$

and this is significantly greater than zero. $\blacksquare$

2) X_n is uniformly distributed over $\{0,1\}^n$, Y_n is uniformly distributed over $\{0,1\}^n \setminus S_1$, $S_1=\{1\}^{\frac{n}{2}}\circ\{0,1\}^{\frac{n}{2}}$.

$\{X_n\}$, $\{Y_n\}$ are polynomially indistinguishable.

Proof: Intuitively, there are "few" α such that α is from the X_n sample and not from the Y_n sample (the fraction is $2^{-\frac{n}{2}}$) and thus, given a string α :

$$\text{Prob}\,(X_n=\alpha)\approx\text{Prob}\,(Y_n=\alpha)$$

More precisely, we will see that X_n and Y_n are statistically close (This notion will be defined later). namely : For **any** function f , we will prove that

$$\forall c > 0\ \exists N,\ \forall n > N:\ \text{Prob}\left[f(X_n)=1\right]-\text{Prob}\left[f(Y_n)=1\right] < \frac{1}{n^c}$$

Let $S \triangleq f^{-1}(1)$. Then

$$\text{Prob}\left[f(X_n)=1\right]=\sum_{\alpha\in S}\text{Prob}\,(X_n=\alpha) \qquad (*)$$

since the events are disjoint. and similarly for Y_n :

$$\text{Prob}\left[f(Y_n)=1\right] = \sum_{\alpha\in S} \text{Prob}\,(Y_n=\alpha)$$

Thus,

$$\left|\text{Prob}\left[f(X_n)=1\right] - \text{Prob}\left[f(Y_n)=1\right]\right| = \left|\sum_{\alpha\in S}\text{Prob}\,(X_n=\alpha) - \sum_{\alpha\in S}\text{Prob}\,(Y_n=\alpha)\right| \le$$

$$\le \sum_{\alpha\in S}\left|\text{Prob}\,(X_n=\alpha) - \text{Prob}\,(Y_n=\alpha)\right| \le$$

$$\le \sum_{\alpha\in\{0,1\}^n}\left|\text{Prob}\,(X_n=\alpha) - \text{Prob}\,(Y_n=\alpha)\right| =$$

$$= \sum_{\alpha\in S_1\cap\{0,1\}^n}\left|\text{Prob}\,(X_n=\alpha) - \text{Prob}\,(Y_n=\alpha)\right| + \sum_{\alpha\in\{0,1\}^n\setminus S_1}\left|\text{Prob}\,(X_n=\alpha) - \text{Prob}\,(Y_n=\alpha)\right|$$

Now,

$$\alpha\in S_1\cap\{0,1\}^n \;\Rightarrow\; \text{Prob}\,(X_n=\alpha)=\frac{1}{2^n} \quad\text{and}\quad \text{Prob}\,(Y_n=\alpha)=0$$

$$\alpha\in\{0,1\}^n\setminus S_1 \;\Rightarrow\; \text{Prob}\,(X_n=\alpha)=\frac{1}{2^n} \quad\text{and}\quad \text{Prob}\,(Y_n=\alpha)=\frac{1}{2^n-2^{\frac{n}{2}}}$$

In the first summation not more than $|S_1|=2^{\frac{n}{2}}$ elements are summed. In the second summation $|\{0,1\}^n\setminus S_1|=2^n-2^{\frac{n}{2}}$ elements are summed. Therefore, the total result is not greater than :

$$\frac{1}{2^n}\cdot 2^{\frac{n}{2}} + \left(\frac{1}{2^n-2^{\frac{n}{2}}} - \frac{1}{2^n}\right)\cdot(2^n-2^{\frac{n}{2}}) = \frac{2}{2^{\frac{n}{2}}}$$

which is a *negligible* fraction, i.e.

$$\forall c>0\ \exists N,\ \forall n>N:\ \frac{2}{2^{\frac{n}{2}}} < \frac{1}{n^c}\quad\blacksquare$$

As was mentioned before, the random variables in this example are statistically close.

In general, two sequences of random variables $\{X_n\}, \{Y_n\}$ ranging over $\{0,1\}^n$ are said to be *statistically close* iff for any constant $c>0$ and for any sufficiently large n :

$$\sum_{\alpha\in\{0,1\}^n}\left|\text{Prob}\,(X_n=\alpha) - \text{Prob}\,(Y_n=\alpha)\right| < \frac{1}{n^c}$$

The above proof shows that statistically close random variables are polynomially indistinguishable. In fact, statistically close random variables are indistinguishable by any algorithm (even non-uniform one

with no restriction on time bounds).

This case of indistinguishability is not so interesting since the sample spaces are almost identical.

In the next example the random variables range over disjoint sets, and are yet indistinguishable.

3) Let $b(\alpha)$ denote a hard core predicate for a one-way permutation f.

Let X_n be uniformly distributed over the set $\left\{ f(\alpha) \,|\, \alpha \in \{0,1\}^n \wedge b(\alpha) = 0 \right\}$ and let Y_n be uniformly distributed over the set $\left\{ f(\alpha) \,|\, \alpha \in \{0,1\}^n \wedge b(\alpha) = 1 \right\}$. Clearly, X_n and Y_n are not statistically close : In fact, $\sum_{\beta \in \{0,1\}^n} |\text{Prob}(X_n = \beta) - \text{Prob}(Y_n = \beta)| = 1$.

Claim: If b is a hard core predicate with regard to f, then $\{X_n\}$ and $\{Y_n\}$ are polynomially indistinguishable.

Proof: Assume by contradiction that $\{X_n\}$, $\{Y_n\}$ are polynomially distinguishable.

Therefore, there exists a probabilistic polynomial algorithm A, such that:

$$\exists\, c > 0,\ \forall N,\ \exists n > N:\ \ \text{Prob}\left[A(X_n) = 1\right] - \text{Prob}\left[A(Y_n) = 1\right] > \frac{1}{n^c} \qquad (*)$$

Let Z_n be a random variable uniformly distributed over $\{0,1\}^n$.

$$p \triangleq \text{Prob}\left[A(Y_n) = 1\right] = \text{Prob}\left[A(f(Z_n)) = b(Z_n) \,|\, b(Z_n) = 1\right]$$

$$1 - q \triangleq \text{Prob}\left[A(X_n) = 1\right] = \text{Prob}\left[A(f(Z_n)) \neq b(Z_n) \,|\, b(Z_n) = 0\right] =$$

$$= 1 - \text{Prob}\left[A(f(Z_n)) = b(Z_n) \,|\, b(Z_n) = 0\right]$$

Now, $\text{Prob}\left[b(Z_n) = 0\right] \approx \text{Prob}\left[b(Z_n) = 1\right] \approx ½$, since b is a hard core predicate (by $\approx$ we mean "equal up to a negligible additive fraction").

Thus,

$$\text{Prob}\left[A(f(Z_n)) = b(Z_n)\right] =$$

$$= \text{Prob}\left[A(f(Z_n)) = b(Z_n) \,|\, b(Z_n) = 1\right] \cdot \text{Prob}\left[b(Z_n) = 1\right] +$$

$$+ \text{Prob}\left[A(f(Z_n)) = b(Z_n) \,|\, b(Z_n) = 0\right] \cdot \text{Prob}\left[b(Z_n) = 0\right] \approx$$

$$\approx p \cdot ½ + q \cdot ½ = ½ \cdot (p + q)$$

By $(*)$, $p - (1 - q) > \frac{1}{n^c}$

$$\Rightarrow p+q > 1+\frac{1}{n^c}$$

$$\Rightarrow \text{Prob}\left[A(f(Z_n)) = b(Z_n)\right] > \frac{1}{2}+\frac{1}{2\cdot n^c}$$

That is, there exists a probabilistic polynomial algorithm A and a constant $c' > 0$, such that

$$\text{Prob}\left[A(f(Z_n)) = b(Z_n)\right] > \frac{1}{2}+\frac{1}{n^{c'}}$$

contradiction to b being a hard core predicate of function f.

We conclude that $\{X_n\}$ and $\{Y_n\}$ are polynomially indistinguishable. ■

One may consider a stronger notion of polynomial indistinguishability. Namely, consider pairs of polynomial random variables, which cannot be distinguished even by an algorithm that is given as input a polynomial number of samplings of one of the random variables, instead of just one sampling. More precisely: for every polynomial algorithm A, for every polynomial $q(n)$, for every constant $c > 0$ and for every sufficiently large n:

$$\text{Prob}\left[A(\bar{X}_n) = 1\right] - \text{Prob}\left[A(\bar{Y}_n) = 1\right] < \frac{1}{n^c}$$

where $\bar{X}_n$ denotes a vector of $q(n)$ independent X_n samplings, and similarly for Y_n

We will see in the future that both notions are equivalent.

3. Security in the sense of Indistinguishability

Now that the concept of indistinguishability is clarified, we shall use it for defining an encryption scheme which is secure in the sense of indistinguishability of encryptions.

Definition: An encryption scheme (G,E,D) is said to be *secure in the sense of indistinguishability* iff for every [polynomial] sequence of random variables $\{X_n = X_n^{(1)} \circ X_n^{(2)}\}$, for every polynomial algorithm A, for every constant $c > 0$ and for every sufficiently large n:

$$\sum_{\alpha,\beta\in\{0,1\}^n} \text{Prob}\,(X_n = \alpha\circ\beta)\cdot\left|\text{Prob}\left[A(\alpha\circ\beta\,,\,E_{G(1^n)}(\alpha)) = 1\right] - \text{Prob}\left[A(\alpha\circ\beta\,,\,E_{G(1^n)}(\beta)) = 1\right]\right| < \frac{1}{n^c}$$

while the probability is taken over $X_n^{(1)}$ and $X_n^{(2)}$'s distributions and the coin tosses of A, G and E.

This definition states that on the avarage, the encryption spaces of $X_n^{(1)}$ and $X_n^{(2)}$ are indistinguishable.

An alternative formalization: An encryption scheme (G,E,D) is said to be secure in the sense of indistinguishability iff for every probabilistic polynomial-time algorithm F (F for *Find*), for every probabilistic polynomial-time algorithm A , for every constant $c > 0$ and for every sufficiently large n :

$$\text{Prob}\left[F(1^n) = \alpha\circ\beta \ \ s.t. \left|\text{Prob}\left[A(\alpha\circ\beta\ ,\ E_{G(1^n)}(\alpha)) = 1\right] - \text{Prob}\left[A(\alpha\circ\beta\ ,\ E_{G(1^n)}(\beta)) = 1\right]\right| > \frac{1}{n^c}\right] < \frac{1}{n^c}$$

Again, the probability is taken over the coin tosses of F , A , E and G .
The intuition is much the same : The probability of efficiently finding a pair α,β such that their encryptions are polynomially distinguishable, is negligible.

As before , the formalizations including the brackets are uniform. In the non-uniform definition brackets are omitted, and *'algorithms'* means *'non−uniform algorithms'* . In the non-uniform case both formalizations are equivalent to the simple following one:
(G,E,D) is said to be secure in the sense of indistinguishability iff for every probabilistic polynomial-time algorithm A , for every constant $c > 0$, for every sufficiently large n and for **every** pair α , $\beta \in \{0,1\}^n$

$$\left|\text{Prob}\left[A(\alpha\circ\beta\ ,\ E_{G(1^n)}(\alpha)) = 1\right] - \text{Prob}\left[A(\alpha\circ\beta\ ,\ E_{G(1^n)}(\beta)) = 1\right]\right| < \frac{1}{n^c}$$

This stronger formulation is possible because the sampling algorithm in the first definition and the algorithm F in the second one , can now be non-uniform. Thus, if there exists a pair α,β that violates the condition, the algorithms (F and A) can incorporate it in them, and thus the probability of sampling / finding this pair is 1.
Of course, since the algorithm F is not used any more in the second definition, it can be omitted.

In the next lecture we shall prove the following Theorem:
If an encryption scheme (G,E,D) is secure in the sense of indistinguishability, then it is semantically secure.

Actually, the two definitions are equivalent, but the above implication is the interesting one, since the existence of encryption schemes secure in the sense of indistinguishability will be proved, and this fact, together with the theorem, implies the existence of semantically secure encryption schemes.