

Advanced Cryptography

1st Semester 2007-2008

Indistinguishability

Pascal Lafourcade

Université Joseph Fourier, Verimag

Master: September 27th 2007

Last Time (I)

Introduction

- Presentation
- Organization
- Motivation
- Mathematics Recalls
- Birthday Paradox
- Perfect Encryption

Remarks, questions, comments ?

Last Time (II)

Exercises done

- 1) Give the security properties for an international airport
- 2) Drug Test
- 3) Expectation properties
- 9) Perfect Security

Others Exercises

- Proofs of different probabilistic theorems.
- Generalization of Birthday Paradox.
- Negligible and Noticeable Functions.

First Draft of Instructors Schedule

Monday		Thursday	
17/09/07	JLR 1	20/09/07	PL 1
24/09/07	JLR 2	27/09/07	PL 2
01/10/07	PL 3	04/10/07	JLR 3
08/10/07	FA 1	11/10/07	FA 2
15/10/07	FA 3 (TP1)	18/10/07	JLR 4
22/10/07	PL 4	25/10/07	FA 4 (TP2)

W44 HOLIDAYS

Monday		Thursday	
05/11/07	PL 5	08/11/07	JLR 5
12/11/07	PL 6	11/11/07	JLR 6
19/11/07	PL 7	22/11/07	JLR 7
26/11/07	PL 8	29/11/07	JLR 8

Negligible functions

We call a function $\mu : \mathbb{N} \rightarrow \mathbb{R}^+$ negligible if for every positive polynomial p there exists an N such that for all $n > N$

$$\mu(n) < \frac{1}{p(n)}$$

Properties

Let f and g be two negligible functions, then

- 1 $f.g$ is negligible.
- 2 For any $k > 0$, f^k is negligible.
- 3 For any λ, μ in \mathbb{R} , $\lambda.f + \mu.g$ is negligible.

Exercise: Proofs

Example Negligible functions (I)

Prove that $f(n) := (\frac{1}{2})^n$ is negligible.

Example Negligible functions (II)

$f(n) := (\frac{1}{2})^n$ is negligible? Show that for any positive polynomial p we have $f(n) \leq p(n)$ for sufficiently large n . Let d be the degree of p .

$$\lim \frac{f(n)}{1/p(n)} = \lim \frac{p(n)}{2^n} = \lim \frac{\delta^d p(n)}{\delta^d 2^n} = \lim \frac{0}{(\ln 2)^d \cdot 2^n} = 0$$

Using L'Hôpital's rule:

$$\lim_{x \rightarrow c} f(x) = \lim_{x \rightarrow c} g(x) = \pm\infty,$$

then:

$$\lim_{x \rightarrow c} \frac{f(x)}{g(x)} = \lim_{x \rightarrow c} \frac{f'(x)}{g'(x)}$$

Since $\frac{f(n)}{1/p(n)}$ converges to 0, and since p is positive, for sufficiently large n we have $f(n) \leq \frac{1}{p(n)}$. So f is negligible.

Independent Random Variables

Definition

Two random variables X , Y are **independent** if for all x in the image of X and all y in the image of Y , the events $X = x$ and $Y = y$ are independent:

$$P[X = x \wedge Y = y] = P[X = x]P[Y = y]$$

Equivalently, X and Y are independent if and only if their joint distribution is equal to the product of their individual distributions.

Exercise: Prove that X and Y are independent if and only if for all values x taken by X with non-zero probability, the conditional distribution of Y given the event $X = x$ is the same as the distribution of Y .

Pairwise Independent Random Variables

Let X_1, \dots, X_n be a collection of random variables, and let X_i be the image of X_i for $i = 1, \dots, n$. We say X_1, \dots, X_n are **pairwise independent** if for all $i, j = 1, \dots, n$ with $i \neq j$, the variables X_i and X_j are independent.

Mutually Independent Random Variables

We say that X_1, \dots, X_n are **mutually independent** if for all $x_1 = X_1, \dots, x_n = X_n$, we have

$$P[X_1 = x_1 \wedge \dots \wedge X_n = x_n] = \prod_{i=1}^n P[X_i = x_i]$$

More generally, for $k = 2, \dots, n$, we say that X_1, \dots, X_n are k -wise independent if any k of them are mutually independent.

Example

We toss three coins, and set $X_i := 0$ if the i th coin is "tails," and $X_i := 1$ otherwise.

Show that the variables X_1, X_2, X_3 are mutually independent.

Let us set $Y_{12} := X_1 \oplus X_2$, $Y_{13} := X_1 \oplus X_3$, and $Y_{23} := X_2 \oplus X_3$, where " \oplus " denotes "exclusive or," that is, addition modulo 2.

Show that the variables Y_{12}, Y_{13}, Y_{23} are pairwise independent, but not mutually independent.

Probability Notation

$$\Pr[A(X_n) = 1] = \sum_x \Pr[X_n = x] \cdot \Pr[A(x) = 1]$$

Outline of Today: **Indistinguishability**

- 1 Introduction
- 2 Definitions
- 3 Hybrid Technique
- 4 Conclusion

Outline

- 1 Introduction
- 2 Definitions
- 3 Hybrid Technique
- 4 Conclusion

Notion of Indistinguishability

Objects are considered to be computationally equivalent if they cannot be differentiated by any efficient procedure.

Hence, two distributions are said to be computationally indistinguishable if no efficient procedure can tell them apart.

Example with Distributions

Given an efficient algorithm D , we consider the probability that D accepts a string taken from the first distribution, and the probability for the second distribution. If these two probabilities are close, we say that D does not distinguish the two distributions.

Concrete Example (I)

Consider that in Box 1 there are 9 blue numerated balls and in Box 2 there are 9 red numerated balls, with uniform distributions.

Alice picks one ball into one of the two boxes and says the number of the ball.

Where did Alice pick the ball?

$$|Pr[A(\text{Box1}|\text{Number}) = 1] - Pr[A(\text{Box2}|\text{Number}) = 1]|$$

is negligible.

Concrete Example (II)

Consider now that Alice has $1/2$ probability to pick ball number 1 between the red balls and $1/16$ for the others $(2, \dots, 9)$.

Hence an adversary has a non negligible advantage to know which Box the ball comes from.

Medical Issue

Consider two sets of patients following two indistinguishable distributions of probability. We give in similar conditions to the first set a new medicine and only water to the second set.

If the results are significant then the treatment is efficient, i.e., the probability of distribution for the results with medicine is distinguishable from the fictive one.

Cryptographic Issue

For a perfect encryption scheme we wish:

$$|Pr[Enc(1) = 1] - Pr[Enc(0) = 1]|$$

is negligible.

Outline

- 1 Introduction
- 2 Definitions**
- 3 Hybrid Technique
- 4 Conclusion

Probability Ensemble

Let I be a countable index set. An ensemble indexed by I is a sequence of random variable indexed by I . Namely, any $X = \{X_i\}_{i \in I}$, where each X_i is a random variable, is an ensemble indexed by I .

Notations

- $X = \{X_n\}_{n \in \mathbb{N}}$ has each X_n ranging over strings of length $\text{poly}(n)$.
- $X = \{X_w\}_{w \in \{0,1\}^*}$ has each X_w ranging over string of length $\text{poly}(|w|)$.

Example

Sequences $\{x_n\}_{n \in \mathbb{N}}$ and $\{y_n\}_{n \in \mathbb{N}}$ are said to be computationally indistinguishable if no efficient procedure can tell them apart.

Polynomial-Time Indistinguishability

- Two ensembles, $X := \{X_n\}_{n \in \mathbb{N}}$ and $Y := \{Y_n\}_{n \in \mathbb{N}}$, are indistinguishable in polynomial time if for every probabilistic polynomial-time algorithm D , every positive polynomial $p(\cdot)$, and all sufficiently large n 's,

$$|\Pr[D(X_n, 1^n) = 1] - \Pr[D(Y_n, 1^n) = 1]| < \frac{1}{p(n)}$$

- Two ensembles, $X := \{X_w\}_{w \in S}$ and $Y := \{Y_w\}_{w \in S}$, are indistinguishable in polynomial time if for every probabilistic polynomial-time algorithm D , every positive polynomial $p(\cdot)$, and all sufficiently long $w \in S$,

$$|\Pr[D(X_w, w) = 1] - \Pr[D(Y_w, w) = 1]| < \frac{1}{p(|w|)}$$

Example (I)

Let b be a string generated by flipping a “fair” coin until head appears (head = 1). Let X be random variable which represents the size of b . Define random variables B_1, B_2, \dots , where B_i represents the value of the bit assigned to b in the i th flip, if $X \geq i$, and \star otherwise.

Note: exactly one B_i will take the value 1, in which case X takes the value i . Evidently, for each $i \geq 1$, then B_i is uniformly distributed over $\{0, 1\}$, and otherwise, $B_i = \star$.

$$P[B_i = 0 | X \geq i] = \frac{1}{2}$$

$$P[B_i = 1 | X \geq i] = \frac{1}{2}$$

$$P[B_i = \star | X < i] = 1$$

Example (II)

$$P[X \geq 1] = 1$$

$$P[X \geq 2] = P[B_1 = 0 | X \geq 1]P[X \geq 1] = \frac{1}{2}$$

$$P[X \geq 3] = P[B_2 = 0 | X \geq 2]P[X \geq 2] = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$$

By induction on i

$$P[X \geq i] = P[B_{i-1} = 0 | X \geq i-1]P[X \geq i-1] = \frac{1}{2} \cdot \frac{1}{2^{i-2}} = \frac{1}{2^{i-1}}$$

X has a geometric distribution with success $1/2$.

Example (III)

The following simple probabilistic algorithm corresponds to flipping a coin until head appears

repeat

$$b \leftarrow_R \{0, 1\}$$

until $b = 1$

Example (I)

Consider the algorithm D_1 which flips a coin and outputs its outcome (0 – 1), with probability $1/2$. Prove that

$$|\Pr[D_1(X) = 1] - \Pr[D_1(Y) = 1]|$$

is negligible.

Exercises (I)

Consider the algorithm D_2 that outputs 1 iff the input string contains more zeros than ones. If D_2 can be implemented in polynomial time, then prove that X and Y are polynomial-time-indistinguishable.

Exercises (II)

Transitivity

Let $X := \{X_n\}_{n \in \mathbb{N}}$, $Y := \{Y_n\}_{n \in \mathbb{N}}$ and $Z := \{Z_n\}_{n \in \mathbb{N}}$ three ensembles. If X and Y are indistinguishable in polynomial time, Y and Z are indistinguishable in polynomial time then X and Z are indistinguishable in polynomial time.

Indistinguishability by Repeated Sampling

Two ensembles, $X := \{X_n\}_{n \in \mathbb{N}}$ and $Y := \{Y_n\}_{n \in \mathbb{N}}$ are indistinguishable by polynomial-time sampling if for every probabilistic polynomial-time algorithm D , every positive polynomials $m(\cdot)$ and $p(\cdot)$, and all sufficiently large n 's:

$$|\Pr[D(X_n^1, \dots, X_n^{m(n)}) = 1] - \Pr[D(Y_n^1, \dots, Y_n^{m(n)}) = 1]| < \frac{1}{p(n)}$$

where X_n^1 through $X_n^{m(n)}$ and Y_n^1 through $Y_n^{m(n)}$ are independent random variables, with each X_n^i identical to X_n and Y_n^i identical to Y_n .

Efficiently Constructible Ensembles

An ensemble $X := \{X_n\}_{n \in \mathbb{N}}$ is said to be polynomial-time-constructible if there exists a probabilistic polynomial-time algorithm S such that for every n , the random variables $S(1^n)$ and X_n are identically distributed.

Outline

- 1 Introduction
- 2 Definitions
- 3 Hybrid Technique**
- 4 Conclusion

Theorem

Let $X := \{X_n\}_{n \in \mathbb{N}}$ and $Y := \{Y_n\}_{n \in \mathbb{N}}$ be two polynomial-time-constructible ensemble, and suppose that X and Y are indistinguishable in polynomial time. Then X and Y are indistinguishable by polynomial-time sampling.

Proof by contradiction

We prove that the existence of an efficient algorithm that distinguishes X and Y using several samples implies the existence of an efficient algorithm which distinguishes the ensembles X and Y .

Proof (I)

We assume that there is D a polynomial-time algorithm such that for many n 's holds:

$$\Delta(n) := |\Pr[D(X_n^{(1)}, \dots, X_n^{(m)}) = 1] - \Pr[D(Y_n^{(1)}, \dots, Y_n^{(m)}) = 1]| > \frac{1}{p(n)}$$

where $m := m(n)$ and the $X_n^{(i)}$ and $Y_n^{(i)}$ are defined by repeated sampling.

GOAL: Finding a probabilistic polynomial-time algorithm D' that distinguishes X and Y .

Introducing H_n^k

For every $0 \leq k \leq m$, we define the hybrid random variable

$$H_n^k := (X_n^{(1)}, \dots, X_n^{(k)}, Y_n^{(k+1)}, \dots, Y_n^{(m)})$$

where $X_n^{(1)}$ through $X_n^{(m)}$ and $Y_n^{(1)}$ through $Y_n^{(m)}$ are independent random variables, with each $X_n^{(i)}$ identical to X_n and $Y_n^{(i)}$ identical to Y_n .

Clearly we have

$$H_n^m := (X_n^{(1)}, \dots, X_n^{(m)})$$

and

$$H_n^0 := (Y_n^{(1)}, \dots, Y_n^{(m)})$$

Idea of the Proof

By hypothesis, D distinguishes H_n^0 and H_n^m .

We use D to build D' which distinguishes X and Y :

- 1 selects k uniformly in the set $\{0, 1, \dots, m-1\}$.
- 2 generates k independent samples of X_n denoted x^1, \dots, x^k
- 3 generates $m-k-1$ independent samples of Y_n denoted y^{k+2}, \dots, y^m .
- 4 invokes D with the input α and halts with the output

$$D'(\alpha) = D(x^1, \dots, x^k, \alpha, y^{k+2}, \dots, y^m)$$

Claim 1

$$\Pr[D'(X_n) = 1] = \frac{1}{m} \sum_{k=0}^{m-1} \Pr[D(H_n^{k+1}) = 1]$$

and

$$\Pr[D'(Y_n) = 1] = \frac{1}{m} \sum_{k=0}^{m-1} \Pr[D(H_n^k) = 1]$$

Claim 1

$$\Pr[D'(X_n) = 1] = \frac{1}{m} \sum_{k=0}^{m-1} \Pr[D(H_n^{k+1}) = 1]$$

and

$$\Pr[D'(Y_n) = 1] = \frac{1}{m} \sum_{k=0}^{m-1} \Pr[D(H_n^k) = 1]$$

Remark

- $\sum_{k=0}^{m-1} \Pr[D(H_n^{k+1}) = 1]$ corresponds to all H_n^i except H_n^0
- $\sum_{k=0}^{m-1} \Pr[D(H_n^k) = 1]$ corresponds to all H_n^i except H_n^m

Proof of Claim 1

By construction of the algorithm D' , we have

$$D'(\alpha) = D(X_n^{(1)}, \dots, X_n^{(k)}, \alpha, Y_n^{(k+2)}, \dots, Y_n^{(m)})$$

where k is uniformly distributed in $\{0, 1, \dots, m-1\}$.

$$\begin{aligned} \Pr[D'(X_n) = 1] &= \\ \sum_{l=0}^{m-1} \Pr[k = l] \Pr[D(X_n^{(1)}, \dots, X_n^{(k)}, X_n^{(l)}, Y_n^{(k+2)}, \dots, Y_n^{(m)}) = 1] \end{aligned}$$

Using the definition of the hybrids H_n^k , the claim follows.

$$\Pr[D'(X_n) = 1] = \frac{1}{m} \sum_{l=0}^{m-1} \Pr[D(H_n^{k+1}) = 1]$$

Claim 2

For $\Delta(n)$ we have:

$$|\Pr[D'(X_n) = 1] - \Pr[D'(Y_n) = 1]| = \frac{\Delta(n)}{m(n)}$$

where

$$\Delta(n) := |\Pr[D(X_n^{(1)}, \dots, X_n^{(m)}) = 1] - \Pr[D(Y_n^{(1)}, \dots, Y_n^{(m)}) = 1]|$$

where $m := m(n)$ and the X_n^i and Y_n^i are defined by repeated sampling.

Proof of Claim 2

Using Claim 1 we get,

$$\begin{aligned} & |Pr[D'(X_n) = 1] - Pr[D'(Y_n) = 1]| \\ &= \frac{1}{m} \left| \sum_{k=0}^{m-1} Pr[D(H_n^{k+1}) = 1] - \sum_{k=0}^{m-1} Pr[D(H_n^k) = 1] \right| \\ &= \frac{1}{m} |Pr[D(H_n^m) = 1] - Pr[D(H_n^0) = 1]| = \frac{\Delta(n)}{m} \end{aligned}$$

where the last equality follows by recalling that:

$$H_n^m := (X_n^{(1)}, \dots, X_n^{(m)})$$

$$H_n^0 := (Y_n^{(1)}, \dots, Y_n^{(m)})$$

Using the definition of $\Delta(n)$

End of the Proof

Our hypotheses said that $\Delta(n) > \frac{1}{p(n)}$ for infinitely many n 's, hence D' distinguishes X and Y , which contradicts the hypothesis of the theorem.

Outline

- 1 Introduction
- 2 Definitions
- 3 Hybrid Technique
- 4 Conclusion**

Summary

Today

- Indistinguishability
- Not to rush to conclusions regarding complex notions
- Hybrid technique

Thank you for your attention.

Questions ?