Distinguishing probability ensembles

Andreia Teixeira

(joint work with Armando Matos and André Souto)

1^{st} **July 2011**

Motivation

- The **computational indistinguishability** of two probabilistic ensembles is a fundamental concept in Cryptography;
- It is sometimes implicitly assumed that the most general method for **efficiently distinguishing** two probability ensembles P and Q is to use an efficient (probabilistic polynomial-time) algorithm A, which measures a property of the ensembles, outputting either 0 or 1;

Motivation

- The **computational indistinguishability** of two probabilistic ensembles is a fundamental concept in Cryptography;
- It is sometimes implicitly assumed that the most general method for **efficiently distinguishing** two probability ensembles P and Q is to use an efficient (probabilistic polynomial-time) algorithm A, which measures a property of the ensembles, outputting either 0 or 1;

Computational indistinguishability

"Classical" computational indistinguishability

The ensembles P_n and Q_n are **computationally indistinguishable** if, for any efficient randomized algorithm $A(x)$ with output 0 or 1, the function $|E(A(P_n)) - E(A(Q_n))|$ is negligible in n.

Negligible

The function $f : \mathbb{N}^+ \to \mathbb{R}$ is **negligible** in n if, for every polynomial $p(n)$, we have $f(n) \leq \frac{1}{p(n)}$ for sufficiently large n.

Computational indistinguishability

"Two from the same" indistinguishability

The ensembles P_n and Q_n are **"two from the same" indistinguishable** if, for any efficient randomized algorithm $A(x, y)$ with output 0 or 1, the function $|E(A(P_n, P_n)) - E(A(Q_n, Q_n))|$ is negligible in n.

Computational indistinguishability

"Integer output" indistinguishability

The ensembles P_n and Q_n are **"integer output" indistinguishable** if, for any efficient randomized algorithm $A(x)$ that outputs an integer, the function $|E(A(P_n)) - E(A(Q_n))|$ is negligible in n.

"One from each" indistinguishability

The ensembles P_n and Q_n are **"one from each" indistinguishable** if, for any efficient randomized algorithm $A(x, y)$ with output 0 or 1, the function $|E(A(P, Q)) - E(A(P, P))| + |E(A(P, P)) - E(A(Q, Q))|$ is negligible in n.

"Integer output" distinguishers

Theorem 1

"integer output" distinguishability in which the output of the algorithm is bounded by a constant $\Leftrightarrow$ **"classical" distinguishability**.

Theorem 2

"Integer output" distinguishability in which the output of the algorithm is bounded by a polynomial in $n \Leftrightarrow$ "classical" distinguishability in which the probabilistic polynomial-time algorithm has an $O(\log n)$ advice.

“One from each” distinguishers

Theorem 3

- “Classical” distinguishability $\Rightarrow$ “Two from the same” distinguishability;
- “Classical” distinguishability $\not\Leftarrow$ “Two from the same” distinguishability;
- **“Classical” distinguishability $\Rightarrow$ “One from each” distinguishability**;
- **“Two from the same” distinguishability $\Rightarrow$ “One from each” distinguishability**;

Conjecture (now it is a new result)

“One from each” distinguishability $\not\Rightarrow$ “Two from the same” distinguishability;

"One from each" distinguishers

Proof of Theorem 3

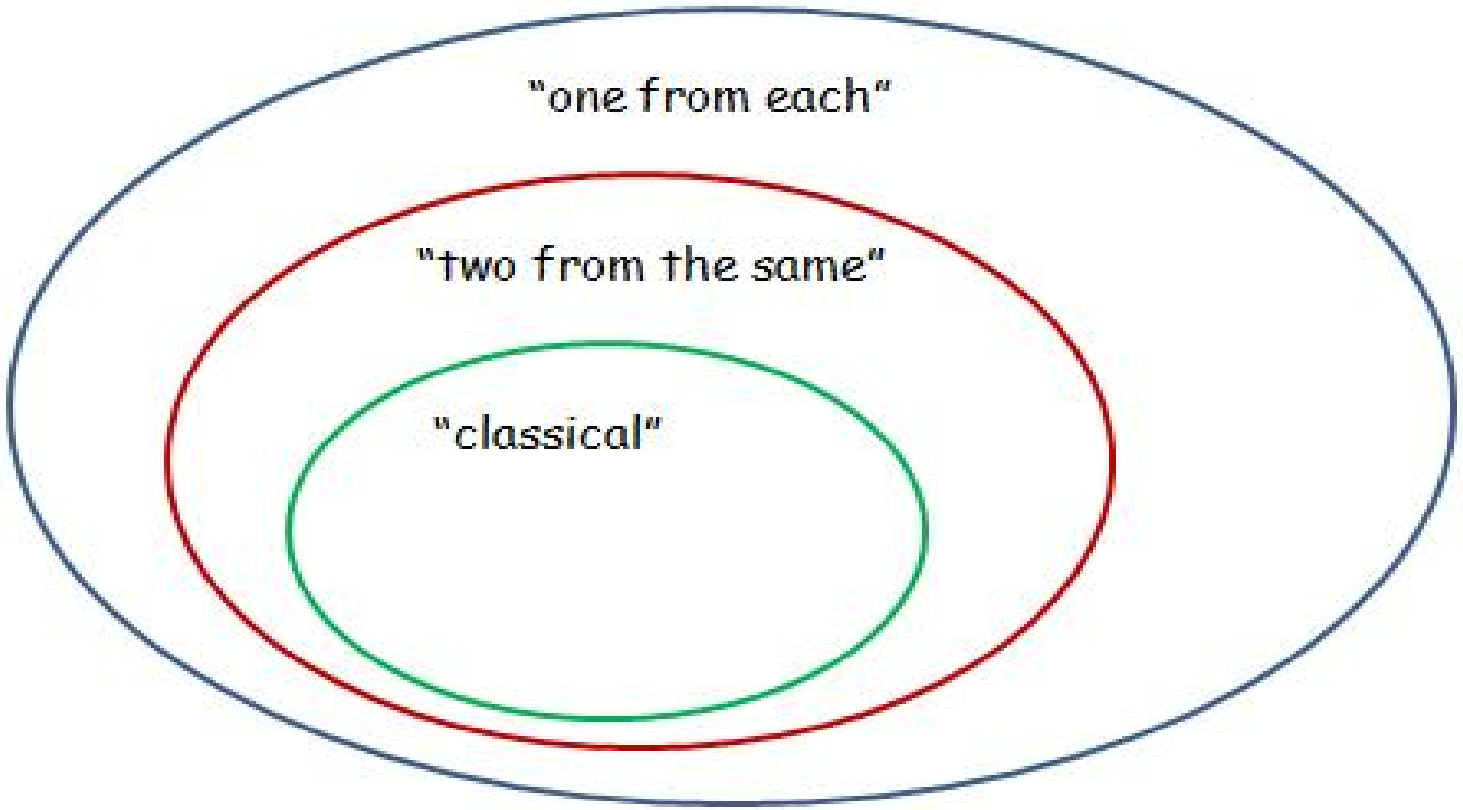
- **"Classical" distinguishability $\Rightarrow$ "One from each" distinguishability**:
  Define the algorithm B by $B(x,y) = A(x)$. We have
  $|E(B(P,Q)) - E(B(P,P))| + |E(B(P,P)) - E(B(Q,Q))| =$
  $|E(A(P)) - E(A(P))| + |E(A(P)) - E(A(Q))| = 0 + |E(A(P)) - E(A(Q))|$
- **"Two from the same" distinguishability $\Rightarrow$ "One from each" distinguishability**:
  Let Δ' be the criterion corresponding to the "one from each" definition.
  $\Delta' = |E(A(P,Q)) - E(A(P,P))| + |E(A(P,P)) - E(A(Q,Q))|$
  The result follows from the last term in Δ'.

"One from each" distinguishers

Proof of Theorem 3

- **"Classical" distinguishability $\Rightarrow$ "One from each" distinguishability**:
  Define the algorithm B by $B(x,y) = A(x)$. We have
  $|E(B(P,Q)) - E(B(P,P))| + |E(B(P,P)) - E(B(Q,Q))| =$
  $|E(A(P)) - E(A(P))| + |E(A(P)) - E(A(Q))| = 0 + |E(A(P)) - E(A(Q))|$
- **"Two from the same" distinguishability $\Rightarrow$ "One from each" distinguishability**:
  Let Δ' be the criterion corresponding to the "one from each" definition.
  $\Delta' = |E(A(P,Q)) - E(A(P,P))| + |E(A(P,P)) - E(A(Q,Q))|$
  The result follows from the last term in Δ'.

Summarizing...



Indistinguishability and Compressors

Definition

A **compressor** is a randomized algorithm $c(x)$ satisfying:

1. There is a randomized polynomial-time algorithm that computes $c(x, r)$;
2. $\forall x, r \;\; d(c(x, r)) = x$, for some algorithm d; c must be injective;

"Compressor" indistinguishability

The ensembles P and Q are **"compressor indistinguishable"** if, for any compressor $c(x, r)$, the function $|E(|c(P, R)|) - E(|c(Q, R)|)|$ is negligible in n.

Indistinguishability and Compressors

Theorem 4

"Classical" distinguishability $\Rightarrow$ "Compressor" distinguishability.

Indistinguishability and Compressors

Proof of Theorem 4

Assume that ensembles P and Q are classically distinguishable.
Then, there is a randomized polynomial algorithm A that distinguishes P from Q.
Consider the randomized compressor $c(x,r)$ defined as:

$$c(x,r) = \begin{cases} 0w & \text{if } A(x,r) = 0, \text{ where } w = \mathtt{LZ}(x) \\ 1^{m(n)+1-n}0x & \text{if } A(x,r) = 1 \end{cases}$$

where $n = |x|$ and $m(n) \geq n$ is an efficiently computable upper bound of $\mathtt{LZ}(x)$.

Indistinguishability and Compressors

Proof of Theorem 4 (Cont.)

Notice that:

$$\begin{cases} A(x,r) = 0 & \Rightarrow \quad |c(x,r)| \leq m+1 \\ A(x,r) = 1 & \Rightarrow \quad |c(x,r)| = m+2 \end{cases}$$

A decompressor $d(y)$ corresponding to c is

$$\begin{cases} \text{if } y \text{ has the form } 0z, \text{ then return } \mathtt{DLZ}(z) \\ \text{if } y \text{ has the form } 11\ldots10z, \text{ then return } z \end{cases}$$

Indistinguishability and Compressors

Proof of Theorem 4 (Cont.)

Consider the difference $\Delta = E(A(P,R)) - E(A(Q,R))$ and, w.l.g., assume that it is positive.
Then, we have that $A(x,r) = 1$ "more frequently" in the ensemble P than in Q. But, if for some $x_1 \in P$, $x_2 \in Q$ and random r, we have $A(x_1,r) = 1$ and $A(x_2,r) = 0$, then, by construction of the compressor c, we have $|c(x_1,r)| - |c(x_2,r)| \geq 1$ so that

$$|E(|c(P,R)|) - E(|c(Q,R)|)| \geq |E(A(P,R)) - E(A(Q,R))| \geq \frac{1}{p(n)}$$

for infinitely many values of n.

Thank you!