Lecture Notes: 02/20/2002

1 Definitions

DEFINITION 1 *Let D, D' be probability distributions. D and D' are (t, ϵ) indistinguishable if for any adversary A running in time $\leq t$,*

$$|\Pr_{x \leftarrow D}[A(x) = 1] - \Pr_{x \leftarrow D'}[A(x) = 1]| \leq \epsilon$$

DEFINITION 2 *$G : X \to Y$ is a (t, ϵ) pseudo-random generator if $G(\mathcal{U}_X)$, $\mathcal{U}_Y$ are (t, ϵ) indistinguishable.*

DEFINITION 3 *If $f : X \to Y$ is one-way and $B : X \to \{0, 1\}$ is balanced, then B is a (t, ϵ)-hardcore bit for f if for all adversaries running in time $\leq t$*

$$|\Pr_{x \leftarrow \mathcal{U}_X}[A(f(x)) = B(x)] - \frac{1}{2}| \leq \epsilon$$

Equivalently,

$$(A \circ f) \oplus B \text{ and } \mathcal{U}_{\{0,1\}} \text{ are } \epsilon \text{ apart.}$$

Equivalently, for all simulators S,

$$\Pr_{x \leftarrow X}[S() = B(x)] = \frac{1}{2}$$

2 Blum-Micali-Yao Construction

THEOREM 1
Suppose $f : X \to X$ is a one-way permutation and $B : X \to \{0,1\}$ is a (t, ϵ)-hardcore bit for f. Define $G(x) = (f(x), B(x))$. Then G is a $(t - O(1), 2\epsilon)$-PRG. This is the Blue-Micali-Yao construction.
PROOF: Suppose A $(t - O(1), 2\epsilon)$-breaks PRG.
Define A', given y [goal: predict $B(f^{-1}(y))$]

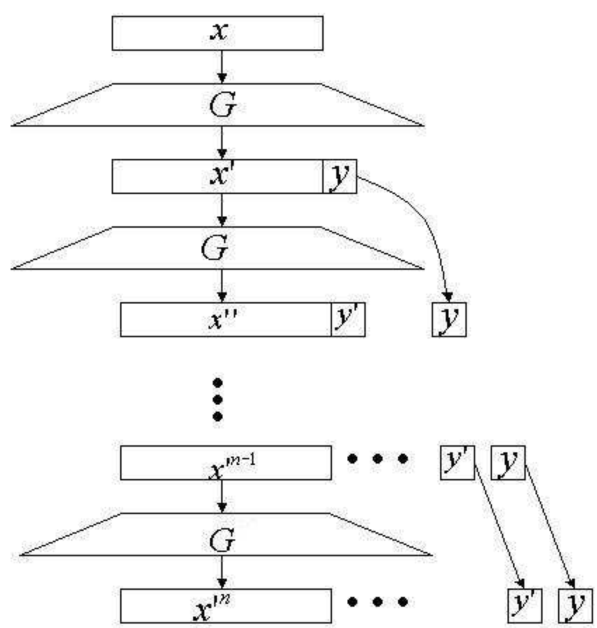
- Pick two bits uniformly at random, $b, b' \in_R \{0, 1\}$
- **if** $A(y, b) = 1$, **then** output b, **else** output b'.

$$\begin{aligned}
\Pr_{\substack{y \leftarrow X \\ b \leftarrow \{0,1\}}}[A'(y) = B(f^{-1}(y))] &= \frac{1}{2}\Pr[A(y,b) = 1 \mid b = B(f^{-1}(y))] + \frac{1}{2}\Pr[A(y,b) = 0] \\
&= \frac{1}{2}\Pr_{x \leftarrow X}[A(G(x)) = 1] + \frac{1}{2}(1 - \Pr_{u \leftarrow X \times \{0,1\}}[A(u) = 1]) \\
&= \frac{1}{2} + \frac{1}{2}\left(\Pr[A(G(x)) = 1] - \Pr[A(u) = 1]\right) \\
&> \frac{1}{2} + \epsilon
\end{aligned}$$

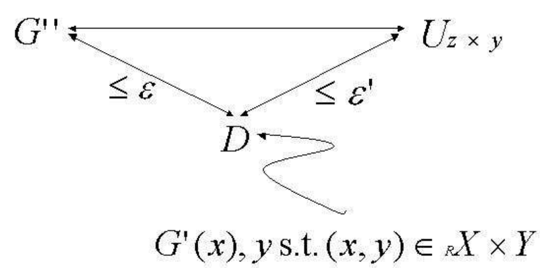
So A' guesses $B(x)$ significantly better than $\frac{1}{2}$, contradicting the assumption that B is a hardcore predicate for f. Then G is a PRG. □

3 Construction of a More Powerful Pseudo-Random Generator

We have proved that we can build a pseudo-random generator that expands the seed by one bit. How can we generalize this idea to build a more powerful pseudo-random generator? For an n-bit seed, we can iterate on G n times to get an output of length 2n. The following figure illustrates this process.



THEOREM 2
Let $G : X \to X \times Y$ be a (t, ϵ)-PRG and $G' : X \to Z$ be a (t, ϵ')-PRG. Define $H : X \to X, T : X \to Y$ s.t. $H(x) = x', T(x) = y$, where $G(x) = (x', y)$. Define $G'' : X \to Z \times Y$ s.t. $G''(x) = (G'(H(x)), T(x))$. Then G'' is a $(t - O(1), \epsilon + \epsilon')$-PRG.
PROOF: Define $\mathcal{D} = \{(G''(x), y) \mid (x, y) \in_R X \times Y\}$. We will proceed with the proof by using a triangle inequality argument. We will first show that $G''(\mathcal{U}_X)$ and $\mathcal{D}$ are ϵ apart. Then we will show $\mathcal{D}$ and $\mathcal{U}_{Z\times Y}$ are ϵ' apart. Finally, we will show that $G''(\mathcal{U}_X)$ and $\mathcal{U}_{Z\times Y}$ are $\epsilon + \epsilon'$ apart.



CLAIM 3
$G''(\mathcal{U}_X)$ and $\mathcal{D}$ are $(t - O(1), \epsilon)$ indistinguishable.

PROOF: Suppose $A(t, \epsilon)$-distinguishes $G''(\mathcal{U}_X)$ from $\mathcal{D}$.
Define A', given (x, y). [goal: distinguish $G(\mathcal{U}_X)$ from a random permutation]

- Output $A(G'(x), y)$.

Then A' distinguishes G from $\mathcal{U}_{X\times Y}$ $\square$

CLAIM 4
$\mathcal{D}$,$\mathcal{U}_{\mathcal{Z}\times\mathcal{Y}}$ are $(t - O(1), \epsilon')$ indistinguishable.

PROOF: Suppose $A(t, \epsilon')$-distinguishes $\mathcal{D}$,$\mathcal{U}_{\mathcal{Z}\times\mathcal{Y}}$.
Define A', given z [goal: was z from G', or from a uniformly random distribution?]

- Pick $y \in_R Y$
- Output $A(z, y)$

Then A' (t, ϵ')-breaks G'. $\square$

For any A

$$
\begin{aligned}
& |\Pr_{g \leftarrow G''(\mathcal{U}_X)}[A(g)=1] - \Pr_{u \leftarrow \mathcal{U}_{Z \times Y}}[A(u)=1]| \\
= \; & |\Pr_{g \leftarrow G''(\mathcal{U}_X)}[A(g)=1] - \Pr_{d \leftarrow \mathcal{D}}[A(d)=1] + \Pr_{d \leftarrow D}[A(d)=1] - \Pr_{u \leftarrow \mathcal{U}_{Z \times Y}}[A(u)=1]| \\
\leq \; & |\Pr_{g \leftarrow G''(\mathcal{U}_X)}[A(g)=1] - \Pr_{d \leftarrow \mathcal{D}}[A(d)=1]| + |\Pr_{d \leftarrow \mathcal{D}}[A(d)=1] - \Pr_{u \leftarrow \mathcal{U}_{Z \times Y}}[A(u)=1]| \\
\leq \; & \epsilon + \epsilon'
\end{aligned}
$$

□

COROLLARY 5
If $G : \{0,1\}^k \to \{0,1\}^{k+1}$ *is* (t, ϵ)*-PRG, then* $F_l : \{0,1\}^k \to \{0,1\}^{k+l}$ *(iterate l times) is* $(t - O(l), l\epsilon)$*-PRG.*

PROOF: The proof is by induction. □

4 Definition of a Pseudo-Random Function

DEFINITION 4 $F : K \times X \to Y$ *is a pseudo-random function if* F_k *and* R *are indistinguishable where* $k \leftarrow_R K$ *and* $R \leftarrow_R$ *Functions* $(X \leftarrow Y)$.