Pseudo-random:

You'll need bit test:

$x \in \{0,1\}^n$ $\quad f(x) \in \{0,1\}^n$ one-way permutation:

$r \in \{0,1\}^{n+1}$

$f : \{0,1\}^n \to \{0,1\}^n$, $\quad l > n$.

$z_1 z_2 \cdots z_{l-1}$, z_l

NBP $f(z_1 \cdots z_{l-1}) \to z_l$.

NIST.

$f : \{0,1\}^n \to \{0,1\}^{n+1}$

$f(x_1) \quad f(x_2) \cdots f(x_n) \quad f \cdots$

$\frac{1}{2^n} \quad \frac{1}{2^n} \quad \cdots \frac{1}{2^n} \quad 0 \cdots 0$

Distribution induced by f on $\{0,1\}^{n+1}$

$\to \frac{1}{2^{n+1}} \quad \frac{1}{2^{n+1}} \cdots \frac{1}{2^{n+1}}$

$\Pr(D(x) = 1)$ $\quad D : \{0,1\}^n \to \{0,1\}$

$x \in \{0,1\}^n$.

$x \in D^{-1}(1)$.

p_0, p_1 } distributions on $\{z_l\}^l$, $\{0,1\}^l$

$p_0(z^l)$ $\quad z^l$ – bit vector of length l

$z \in z_l = \{0,1\}$

$z^l = (z_1, z_2, z_3, \ldots, z_l)$

$p_1(z^l)$ – probability associated with z^l by p_1.

$p_0(z^l) = \frac{1}{2^l}$ (uniform distribution)

$\Pr(D(z^l) = 1)$?

$z^l \in \{0,1\}^l$

$D(z^l) = 1$ iff $z^l \in D^{-1}(1)$ and the sampling with probability

$E_D(1) = \sum_{z^l \in D^{-1}(1)} p_1(z^l)$ under p_0.

$E_D(1) = \sum_{z^l \in D^{-1}(1)} p_1(z^l)$ under p_1.

$\Pr(D(z^l) = 1) = E_D(p_1)$

$z^l \xleftarrow[p_1]{} \{0,1\}^l$

$\Pr(D(z^l) = 1) = E_D(p_1)$

$z^l \xleftarrow[p_1]{} \{0,1\}^l$

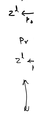
$E_D(p_0) = .7$ $\quad .3$

$E_D(p_1) = .5$ $\quad .5$ ✓

$D(z) = 1$ $\quad D(z) = 0$.

	H	T
C_1 —	1	0
C_2 —	0	1.

	H	T
C_1 —	$\frac{3}{4}$	$\frac{1}{4}$
C_2 —	$\frac{1}{4}$	$\frac{3}{4}$



$D(z) = 1$ $\quad$ test for Distinguisher.

$z \in \{ \vec{D}^{-1}(1) \}$

ϵ - Dist. for p_0 & p_1.

$| E_D(p_0) - E_D(p_1) | \geq \epsilon$.

$E_D(p_0) = \sum_{z^l \in \{z_l\}^l} p_0(z^l) \cdot \Pr(D(z^l) = 1)$

$f : A \to B$.

DOS $\quad$ DOS B

Dist

Next bit predictor:

f : ($b_1 b_2$) – bit generator.

$\{0,1\}^k \to \{0,1\}^k$, $\quad l > k$.

$1 \leq i \leq l-1$. $\quad i^{th}$ bit predictor.

nbp : $(z_1)^{i-1} \to z_i$

$z_1^{i-1} \to z_i$

$\{0,1\}^{i-1} \to \{0,1\}$

$(z_1 z_2 \cdots z_{i-1}) \to \{0,1\}$.

i^{th} bit

Let p_i ($z_1 \cdots z_{i-1}$) is the probability distribution induced by f on (z_i^{i-1}) ↑

$f : \{0,1\}^k \to \{0,1\}^k$

---

z_i is the distribution designed by f on i^{th} bit.

$\sum_{z_i^{i-1} \in \{z_i\}^{i-1}} p_i(z_i^{i-1}) \cdot \Pr(z_i = NBP(z^{i-1}))(z^{i-1})$

$\geq \frac{1}{2} + \epsilon$.

NBT for i^{th} bit generated by f has ϵ advantage w.r.

Suppose there is an ith bit NBT for f with ϵ advantage:

Then, there is a Dist. $\{(z_i)^l\}$ $(z_1, z_2 \cdots z_l)$

$\to p_0$ on $\{(z_i)^l\}$ $\quad p_1$ on $\{(z_i)^l\}$ $\quad p_i(z_i^l)$

$\left| E_{Dist}(p_1(z_i^l)) - E_{Dist}(p_i(z_i^l)) \right| \geq \epsilon$.

Dist $(z_1, \ldots z_l) = 1$ iff $NBP(z_1, \ldots z_{i-1}) = z_i$.

Dist $(z_1 \ldots z_{i-1}, 0) = 0$ $\quad$ Dist $(z_1 \ldots z_{i-1}, 1) = 1$

Dist unknown $(z_1 \cdots z_{i-1}, z_i)$ is you by p.

Douglas R. Stinson

Third Ed: Ch 9

321 – 344.

Sharan Kumar:

cs19m060@smail...

Straight Path.