Pseudorandomness

TFC
11/9/2017

PseudoRandom Generators [BM82, Yao82]

$\mathsf{G} : \{0,1\}^n \to \{0,1\}^m, \quad m > n$

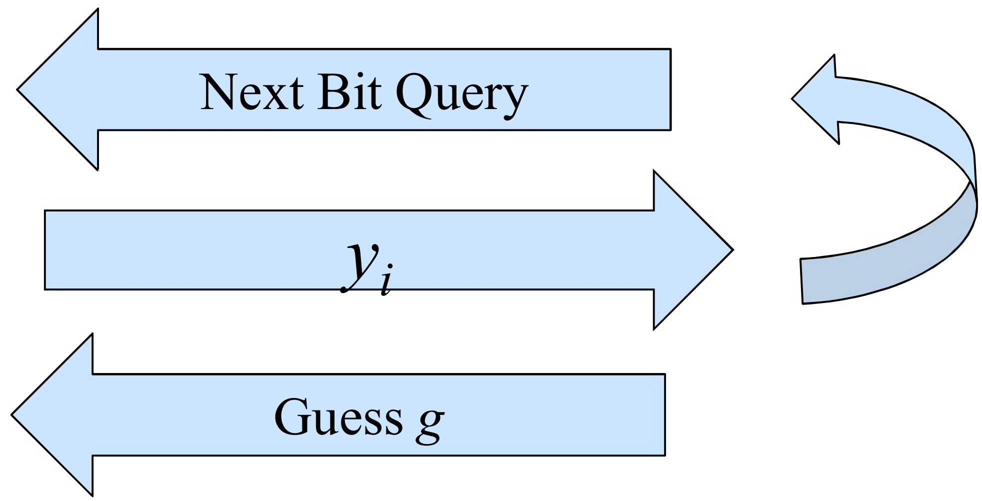
↑ Seed s

Informally: "stretches" random bits from n bits to $\mathsf{poly}(n)$ bits (which are "**unpredictable**".)

Next-bit Unpredictability

Experiment NBP:

1. Pick $s \in \{0,1\}^n$.
2. Let $y = G(s)$ and $i = 1$



- Send y_i
- $i = i + 1$

Output SUCCESS if:

- $i \leq m$
- $y_i = g$

We say that $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is a pseudo-random generator, if for every PPT bit-predictor A,

$$\Pr[\mathsf{Experiment - NBP(n)}\ \text{SUCCEEDS}] \leq \frac{1}{2} + \mathsf{negl(n)}$$

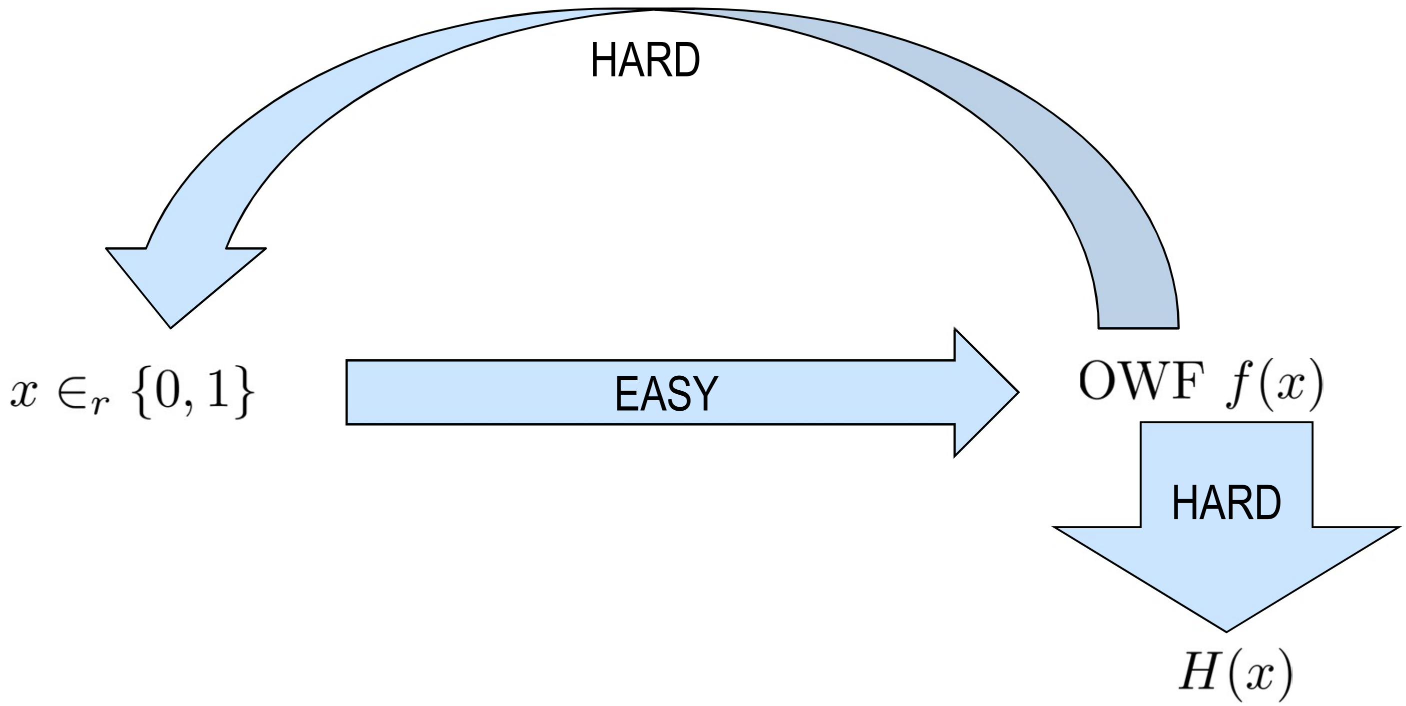
Discrete Logarithm Assumption

- Let $\mathbb{Z}_p$ is the field modulo p for a odd prime p. Let $\mathbb{Z}_p^*$ be the multiplicative group.
- Let g be a generator of the group.

Recall the statement of the Discrete Logarithm Assumption:
For any PPT A, there exists a negligble function $\eta()$, such that:

$$\Pr[p, g \leftarrow \mathsf{Gen_n}; \mathsf{x} \leftarrow \mathbb{Z}_\mathsf{p}^* : \mathsf{A}(\mathsf{p}, \mathsf{g}, \mathsf{g}^\mathsf{x} \bmod \mathsf{p}) = \mathsf{x}] \leq \eta(\mathsf{n})$$

Hard-core Predicate



A predicate $H()$ is hard-core for a function f, if for any PPT adversary A, there exists a negligble function $\eta()$ such that:

$$\Pr[x \xleftarrow{\$} \{0,1\}^n : A(1^n, f(x)) = H(x)] \leq \frac{1}{2} + \eta(n)$$

Hard-core Predicate For DLog

Let $H(x) = \{0, \text{ if } x < p/2 \text{ and } 1 \text{ otherwise}\}$.

Lemma 1. *$H()$ is hard-core for the OWP $f()$ defined by $f(x) = g^x$. Informally, given g^x (chosen appropriately), $H(x)$ is unpredictable.*

Some facts about squares in $\mathbb{Z}_p^*$:

1. x is even iff $a = g^x$ is a square.

2. a is a square iff $a^{\frac{(p-1)}{2}} = 1$

3. If a is a square, it has two distint square roots: $r_1 = g^{x/2}; r_2 = g^{x/2 + \frac{(p-1)}{2}}$.

Observe that $H(x/2) = 0$ and $H(x/2 + (p-1)/2) = 1$.

Hard-core Predicate For DLog

Let $H(x) = \{0,\ \text{if } x < p/2 \text{ and } \ 1 \text{ otherwise}\}$.

Lemma 1. *$H()$ is hard-core for the OWP $f()$ defined by $f(x) = g^x$. Informally, given g^x (chosen appropriately), $H(x)$ is unpredictable.*

Suppose $\exists$ a predictor D for the hard-core bit, then we will it to break DLog.

1. D can be used to distinguish r_1 from r_2.
2. Given $y = g^x$, find the last bit of x. (Simply raise it to $\frac{(p-1)}{2}$ to check whether it is a square. If it is, then last bit is 0.) If last bit is 1, then divide by g to make the bit 0.
3. Now, y is a square. Take its' square root (easy to do) and get r_1 using D.
4. This is the same as y except that the corresponding x value is right-shifted by one (the bit that came out).
5. Repeat to recover all the bits one-by-one.

Blum Micali PRG

Let $H(x) = \{0, \text{ if } x < p/2 \text{ and } 1 \text{ otherwise}\}$.

Let $x_1 = x$, $x_2 = g^{x_1}$, $\ldots$, $x_n = g^{x_{n-1}}$.
$G(x) = H(x_n), H(x_{n-1}), \ldots, H(x_2), H(x_1)$.

Theorem 1. *Under DLOG, G() is a PRG.*

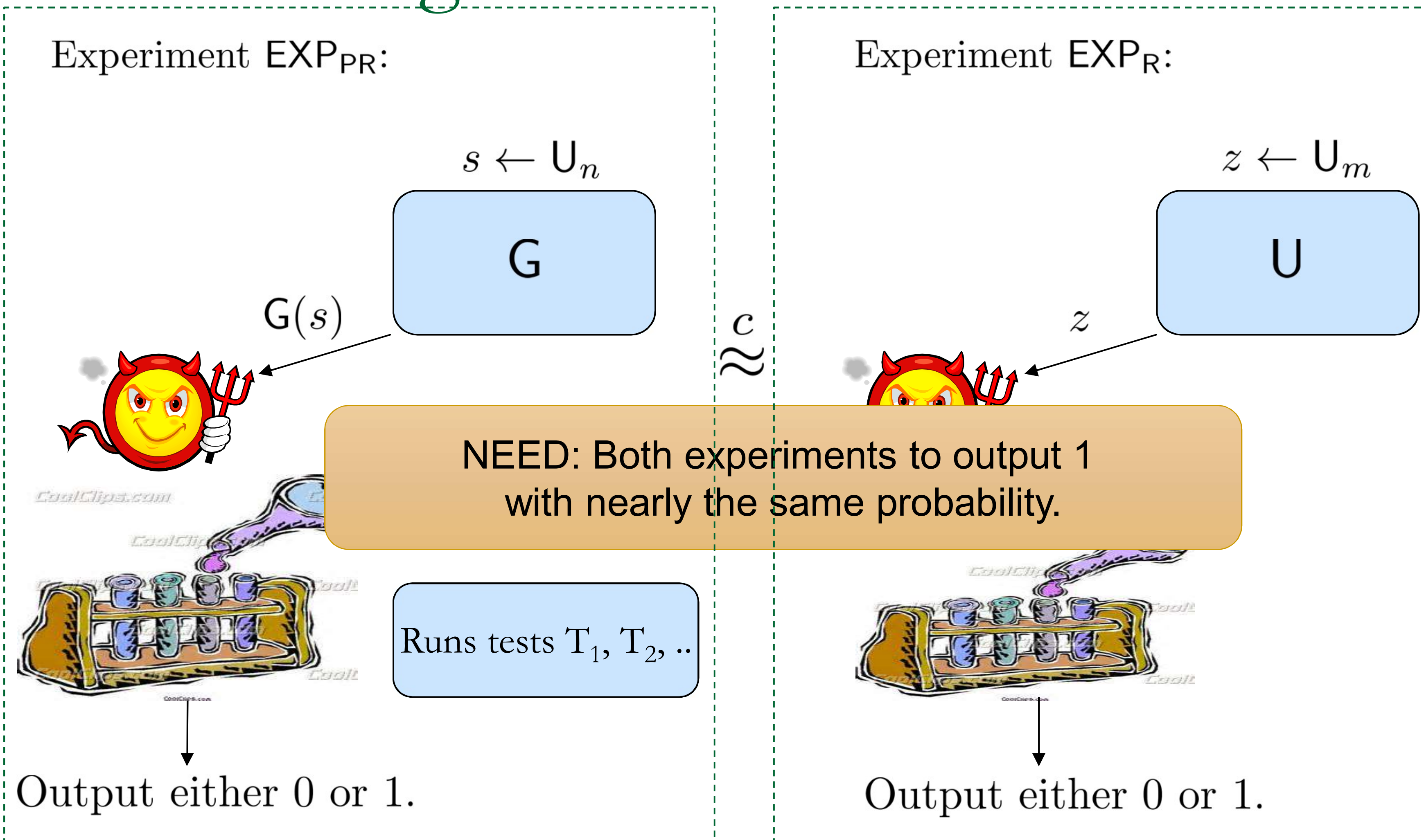
Proof. Suppose there is a next-bit predictor A. Then we will use it to predict a hard-core bit. (Which one? Pick any at random.) □

Computational Indistinguishability

TFC

11/9/2017

Formalizing via Statistical Tests



Main Theorem

- Recall: We say G is a pseudo-random generator if it satisfies the definition of next-bit unpredictability.
- Today: G is a PRG iff it fools all statistical tests.

Proof (Easy Part):

G fools all Statistical Tests => NB Unpredictable

- Assume for the sake of contradiction, that G is not a PRG. In particular, it doesn't satisfy next bit unpredictability.
- Let NBP be a next bit predictor for G.
- We will use NBP to build a statistical test T which G will not fool.

Proof: Indistinguishability implies PRG

Statistical Test T:

On input y, does as follows:

- Runs NBP feeding it bits of y in order.
- If NBP halts and outputs the correct "next bit", then output 1. Else output 0.

$$\Pr[\mathsf{Exp}_{\mathsf{PR}} \rightarrow 1] = \frac{1}{2} + \mu(n)$$

$$\Pr[\mathsf{Exp}_{\mathsf{R}} \rightarrow 1] = \frac{1}{2}$$

$$\Pr[\mathsf{Exp}_{\mathsf{PR}} \rightarrow 1] - \Pr[\mathsf{Exp}_{\mathsf{R}} \rightarrow 1] = \mu(n)$$

Proof: PRG implies Indistinguishability

- For the sake of contradiction, suppose that G is next-bit unpredictable.
- Also, suppose that there exists a statistical test T which G doesn't fool.
- Then we will use T to obtain a contradition by building a next-bit predictor.

$$\mathsf{Exp}_{\mathsf{PR}} : y_1, \ldots, y_{i-1}, y_i, y_{i+1} \cdots y_m$$

$$\not\approx \quad \text{(Via T)}$$

$$\mathsf{Exp}_{\mathsf{R}} : r_1, \ldots, r_{i-1}, r_i, r_{i+1}, \ldots, r_m$$

Proof: PRG implies Indistinguishability

A Hybrid Argument:

$$(\mathsf{Exp_R})\ \mathsf{Exp_0} : r_1, r_2, \ldots, r_{i-1}, r_i, r_{i+1}, \ldots, r_m$$

$$\mathsf{Exp_1} : y_1, r_2, \ldots, r_{i-1}, r_i, r_{i+1}, \ldots, r_m$$

$$\vdots$$

$$\mathsf{Exp_i} : y_1, \ldots, y_{i-1}, y_i, r_{i+1}, r_{i+2}, \ldots, r_m$$

$$\not\approx \quad \text{(Via T)}$$

$$\mathsf{Exp_{i+1}} : y_1, \ldots, y_{i-1}, y_i, y_{i+1}, r_{i+2}, \ldots, r_m$$

$$\vdots$$

$$(\mathsf{Exp_{PR}})\ \mathsf{Exp_m} : y_1, \ldots, y_{i-1}, y_i, y_{i+1}, y_{i+2}, \ldots, y_m$$

Proof: PRG implies Indistinguishability

$\mathsf{Exp_i}$: $y_1, \ldots, y_{i-1}, y_i, r_{i+1}, r_{i+2}, \ldots, r_m$

$\mathsf{Exp_{i+1}}$: $y_1, \ldots, y_{i-1}, y_i, y_{i+1}, r_{i+2}, \ldots, r_m$

$\not\approx$ (Via T)

Hope: Use T to build predictor for y_{i+1}.

NBP :

1. Select a random $g \leftarrow \{0, 1\}$.
2. Select a random $r \leftarrow \{0, 1\}^m$.
3. Set $z = [y]_1^i g [r]_{i+2}^m$
   (where it gets $[y]_1^i$ by requesting the first i bits of PRG output.)
4. Run $T(z)$. If $T(z) = 1$, then output $b = g$, else output $b = 1 - g$.

Proof: Indistinguishability implies PRG

$$\Pr[b = y_{i+1}] = \Pr[T(z) = 1 \wedge y_{i+1} = g] + \Pr[T(z) = 0 \wedge y_{i+1} = 1 - g].$$

Let z_1 be $[y]_1^i \; y_{i+1} \; [r]_{i+2}^m$.

Let z_2 be $[y]_1^i \; \overline{y_{i+1}} \; [r]_{i+2}^m$.

$$\Pr[b = y_{i+1}] = \Pr[T(z_1) = 1 \wedge g = y_{i+1}] + \Pr[T(z_2) = 0 \wedge g = 1 - y_{i+1}]$$

$$= \frac{1}{2}\Big(\Pr[T(z_1) = 1] + \Pr[T(z_2) = 0]\Big)$$

$$= \frac{1}{2} + \frac{1}{2}\Big(\Pr[T(z_1) = 1] - \Pr[T(z_2) = 1]\Big)$$

Proof: Indistinguishability implies PRG

$$\Pr[\mathsf{Exp_i} \to 1] = \frac{1}{2}\Big(\Pr[T(z_1) = 1] + \Pr[T(z_2) = 1]\Big)$$

$$\Pr[\mathsf{Exp_{i+1}} \to 1] = \Pr[T(z_1) = 1]$$

Subtracting,

$$\frac{1}{2}\Big(\Pr[T(z_1) = 1] - \Pr[T(z_2) = 1]\Big) = \Pr[\mathsf{Exp_{i+1}} \to 1] - \Pr[\mathsf{Exp_i} \to 1]$$

$$= \frac{\mu(n)}{m}$$

(Non-negligible, by assumption + poly stretch)

$$\Pr[b = y_{i+1}] = \frac{1}{2} + \frac{1}{2}\Big(\Pr[T(z_1) = 1] - \Pr[T(z_2) = 1]\Big)$$

(From previous slide)

$$= \frac{1}{2} + \frac{\mu(n)}{m}$$

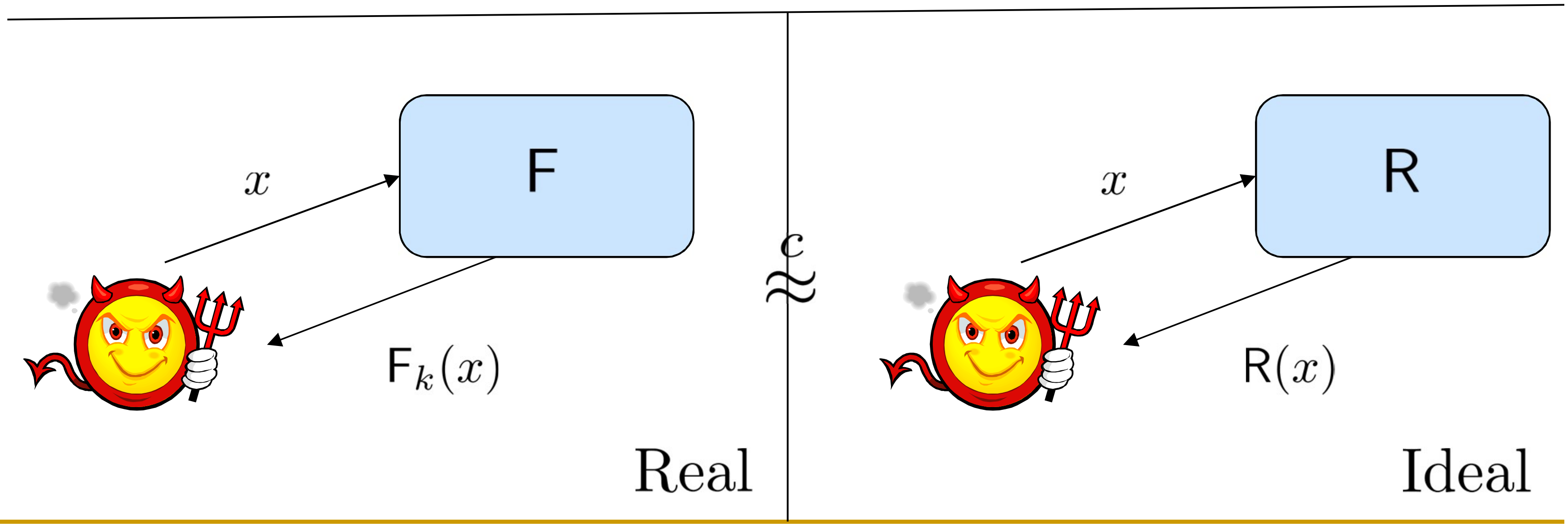
PseudoRandom Functions [GGM86]

$$\mathsf{F} : \{0,1\}^n \times \{0,1\}^u \to \{0,1\}^n$$

Key k — Input x — Output y

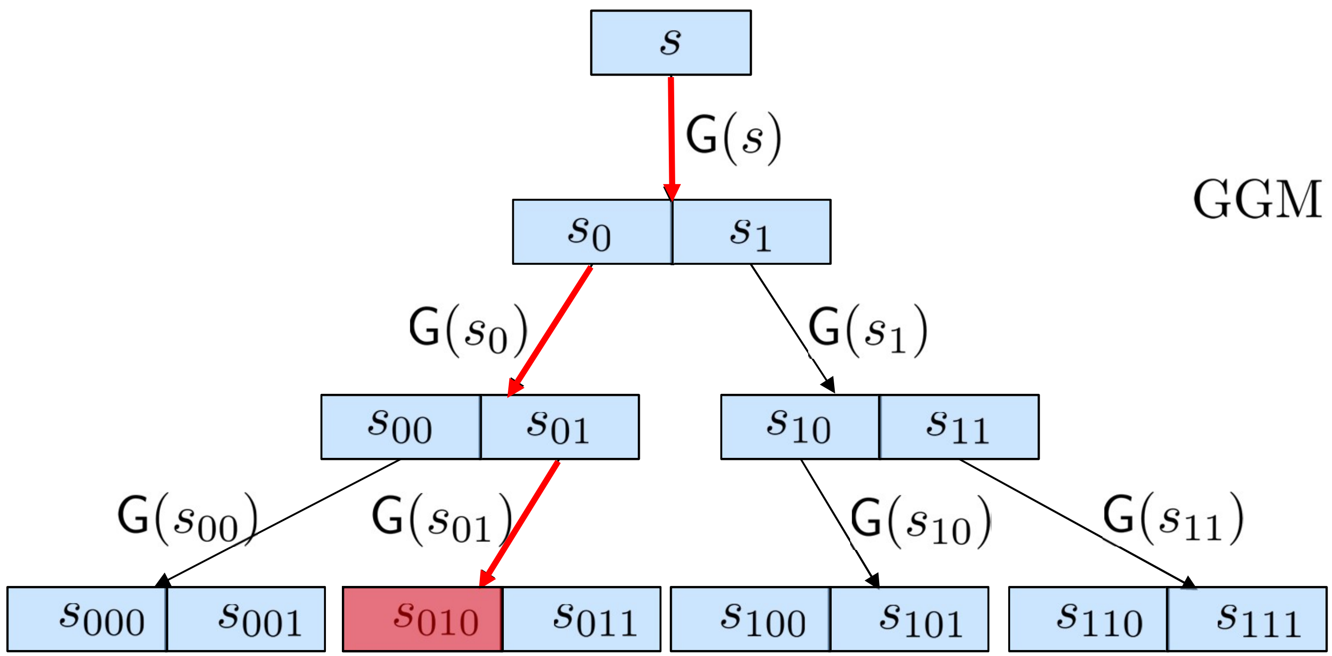
$|k| = n$
$|x| = u$
$|y| = n$

Informally: "stretches" random bits from n bits to $\mathsf{exp}(n)$ bits



PRFs from PRGs [GGM86]

$\mathsf{F} : \{0,1\}^n \times \{0,1\}^u \rightarrow \{0,1\}^n$ from $\mathsf{G} : \{0,1\}^n \rightarrow \{0,1\}^{2n}$



GGM Transform

$$\mathsf{F}(x = x_1 x_2 \ldots x_u) = s_{x_1 x_2 \ldots x_u}$$

$$\text{E.g. : } \mathsf{F}(010) = s_{010}$$