V. Theoretical constructions of pseudorandom objects

Goal pseudorandom generators and pseudorandom functions from general assumptions.

Assumption one-way functions/permutations exist.

one-way fcts/perm ➔ hardcore predicates

➔ PRG with expansion n+1

➔ PRG with polynomial expansion factor

➔ PRF

Inverting game

$f:\{0,1\}^* \to \{0,1\}^*$, A probabilistic polynomial time algorithm

Inverting game $\text{Invert}_{A,f}(n)$

1. $x \leftarrow \{0,1\}^n, y := f(x)$.
2. A given input 1^n and y, outputs x'.
3. Output of game is 1, if $f(x') = y$, otherwise output is 0.

Write $\text{Invert}_{A,f}(n) = 1$, if output is 1. Say A has succeded or A has won.

Definition of one-way function

Definition 5.1 $f:\{0,1\}^* \to \{0,1\}^*$ called one-way, if

1. there is a ppt M_f with $M_f(x) = f(x)$ for all $x \in \{0,1\}^*$
2. for every probabilistic polynomial time algorithm A there is a negligible function $\mu:\mathbb{N} \to \mathbb{R}^+$ such that $\Pr\left[\text{Invert}_{A,f}(n) = 1\right] \le \mu(n)$.

Notation $\Pr_{x \leftarrow \{0,1\}^n}\left[A(f(x)) \in f^{-1}(f(x))\right] \le \mu(n)$

Definition of one-way permutation

$f:\{0,1\}^* \rightarrow \{0,1\}^*$ length preserving, if for all x $|f(x)| = |x|$.

$f_n := f_{|\{0,1\}^n}$, restriction of f to $\{0,1\}^n$.

Definition 5.2 A one-way function $f:\{0,1\}^* \rightarrow \{0,1\}^*$ is called one-way permutation, if

1. f is length-preserving,
2. for every $n \in \mathbb{N}$ the function f_n is a bijection.

Function families

Definition 5.3 A triple $\Pi = (\mathrm{Gen}, \mathrm{Samp}, f)$ of ppts is called a family of functions, if

1. $\mathrm{Gen}(1^n)$ outputs parameters I with $|I| \geq n$, where each I defines finite sets D_I and R_I for a function $f_I : D_I \to R_I$ defined below.

2. $\mathrm{Samp}(I)$ outputs $x \leftarrow D_I$.

3. f is deterministic and on input I, $x \in D_I$ outputs $y \in R_I$, $y := f_I(x)$.

Π is a family of permutations, if in addition for all I $D_I = R_I$ and f_I is a bijection

The inverting games

Inverting game $\text{Invert}_{A,\Pi}(n)$

1. $I \leftarrow \text{Gen}(1^n), x \leftarrow \text{Samp}(I), y := f_I(x)$.
2. A given input $1^n, I$ and y, outputs x'.
3. Output of game is 1, if $f_I(x') = y$, otherwise output is 0.

Definition 5.4 A family of functions $\Pi = (\text{gen}, \text{Samp}, f)$ is called one-way, if for every probabilistic polynomial time algorithm A there is a negligible function $\mu : \mathbb{N} \rightarrow \mathbb{R}^+$ such that $\Pr[\text{Invert}_{A,\Pi}(n) = 1] \leq \mu(n)$.

Candidates

1. $$f_{mult}: \{0,1\}^* \rightarrow \{0,1\}^*$$
$$x \mapsto (x_1 \cdot x_2, |x_1|, |x_2|),$$

where $|x_1| = \lfloor |x|/2 \rfloor, |x_2| = \lceil |x|/2 \rceil$, and identify bit strings and integers via binary representations.

Idea Multiplication easy, factoring hard

Candidates

2. $\text{Gen}(1^n)$ generates n n-bit integers uniformly at random,

$I = (a_1, \ldots, a_n)$

$\text{Samp}(I)$ $x \leftarrow \{0,1\}^n, x = (x_1, \ldots, x_n)$

$f_I(x)$ outputs $\sum_{i=1}^{n} x_i a_i$

Idea Addition is easy, SubsetSum is difficult.

Candidates

3. $\text{Gen}(1^n)$ generates prime number $p \geq 2^n$ and generator g for the multiplicative group $\mathbb{Z}_p^*, I = (p, g), D_I = \mathbb{Z}_{p-1}$, $R_I = \mathbb{Z}_p^*$

   $\text{Samp}(I)$ $x \leftarrow \mathbb{Z}_{p-1}$

   $f_I(x)$ outputs $g^x \bmod p$

Idea Exponentiation is easy, discrete logarithm is difficult.

Hardcore predicates

Definition 5.5 $hc:\{0,1\}^* \rightarrow \{0,1\}$ is a hardcore predicate for a function $f:\{0,1\}^* \rightarrow \{0,1\}^*$, if

1. hc can be computed in polynomial time,
2. for every probabilistic polynomial time algorithm A there is a negligible function $\mu:\mathbb{N} \rightarrow \mathbb{R}^+$ such that $\Pr_{x \leftarrow \{0,1\}^n}\left[A(f(x)) = hc(x)\right] \le 1/2 + \mu(n)$.

The Goldreich-Levin predicate

$f:\{0,1\}^* \to \{0,1\}^*$ one-way, then

$$\begin{aligned} g: \quad \{0,1\}^* &\to \{0,1\}^* \\ w &\mapsto f(x) \| r, \text{ where } w = x \| r, |x| = |r|, \end{aligned}$$

is also one-way.
Formally, g is only definied for arguments of even length, by padding w we can define it for all bit strings.

Theorem 5.6 Let f be a one-way function and g be defined as above. Then

$$\begin{aligned} gl: \quad \{0,1\}^* &\to \{0,1\} \\ (x,r) &\mapsto x \odot r = \sum x_i r_i \bmod 2 \end{aligned}$$

is a hardcore predicate for g.

The Goldreich-Levin predicate

Theorem 5.6 (reformulated) Let f be a one-way function. Let g and the predicate gl be defined as above. If there exists a ppt A and a polynomial $p(\cdot)$ such that

$$\Pr_{x,r \leftarrow \{0,1\}^n}\left[A(f(x),r) = gl(x,r)\right] \geq \frac{1}{2} + \frac{1}{p(n)}$$

for infinitely many values of n, then there exists a ppt A' and a polynomial $q(\cdot)$ such that

$$\Pr_{x \leftarrow \{0,1\}^n}\left[Invert_{A,f}(n) = 1\right] \geq \frac{1}{q(n)}$$

for infinitely many values of n.

An extremely simplified variant

Theorem 5.7 Let f be a one-way function and let gl be the Goldreich-Levin predicate. If there exists a ppt A and a polynomial p such that

$$\Pr_{x,r\leftarrow U_n}\left(A\left(f\left(x\right),r\right)=gl\left(x,r\right)\right)=1$$

for infinitely many values of n, then there exists a ppt A' such that

$$\Pr\left(\mathrm{Invert}_{A,f}\left(n\right)=1\right)=1$$

for infinitely many values of n.

A simplified variant

Theorem 5.8 Let f be a one-way function and let gl be the Goldreich-Levin predicate. If there exists a ppt A and a polynomial p such that

$$\Pr_{x,r \leftarrow U_n}\left(A\left(f\left(x\right),r\right) = gl\left(x,r\right)\right) \geq \frac{3}{4} + \frac{1}{p\left(n\right)}$$

for infinitely many values of n, then there exists a ppt A' such that

$$\Pr\left(\mathrm{Invert}_{A,f}\left(n\right) = 1\right) \geq \frac{1}{4p\left(n\right)}$$

for infinitely many values of n.

One-way functions and hard-core predicates

Claim 5.9 Let f,gl, A, p be as before. Then there exists a set $S_n \subseteq \{0,1\}^n$ of size at least $\frac{2^n}{2p(n)}$ such that for every $x \in S_n$

$$\Pr_{r \leftarrow U_n}\left(A\left(f\left(x\right),r\right) = gl\left(x,r\right)\right) \geq \frac{3}{4} + \frac{1}{2p(n)}.$$

One-way functions and hard-core predicates

Claim 5.10 Let f,gl, A, p be as before. Then there exists a set $S_n \subseteq \{0,1\}^n$ of size at least $\frac{2^n}{2p(n)}$ such that for every $x \in S_n$ and every $i \in \{1,\ldots,n\}$

$$\Pr_{r \leftarrow U_n}\left(A(f(x),r) = gl(x,r) \wedge A(f(x),r \oplus e^i) = gl(x,r \oplus e^i)\right) \geq \frac{1}{2} + \frac{1}{p(n)}.$$

Chebyshev's inequality

Theorem 5.11 (Chebyshev) Let X be a random variable and $\delta > 0$. Then

$$\Pr\left[\left|X - E[X]\right| \geq \delta\right] \leq \frac{\mathrm{Var}[X]}{\delta^2}.$$

Corollary 5.12 Let $X_1,\ldots,X_m$ be pairwise independent random variables with the same expectation μ and the same variance σ^2. Then, for every $\epsilon > 0$,

$$\Pr\left[\left|\frac{\sum_{i=1}^{m} X_i}{m} - \mu\right| \geq \epsilon\right] \leq \frac{\sigma^2}{\epsilon^2 m}.$$

From prediction to inversion

1. For $i=1$ to n do
2. For $j=2$ to $np(n)^2/2$ do
3. $r \leftarrow U_n$
4. $\bar{x}_{i,j} \leftarrow A(f(x), r) \oplus A(f(x), r \oplus e^i)$
5. $x_i := \text{majority}\left(\bar{x}_{i,1}, \ldots, \bar{x}_{i,np(n)^2/2}\right)$
6. Output $x := x_1 \ldots x_n$

Hardcore predicates and PRGs

Theorem 5.13 Let f be a one-way permutation and hc a hardcore predicate for f. Then

$$\begin{aligned} G: \quad \{0,1\}^* &\to \{0,1\}^* \\ s &\mapsto f(s) \,\|\, hc(s) \end{aligned}$$

is a PRG with expansion factor $n+1$.

Pseudorandom generators

Definition 2.5 (old) Let $l : \mathbb{N} \rightarrow \mathbb{N}$ be a polynomial with $l(n) > n$ for all $n \in \mathbb{N}$. A deterministic polynomial time algorithm G is a pseudorandom generator if

1. $\forall s \in \{0,1\}^* \quad |G(s)| = l(|s|)$,
2. For every ppt D there is a negligible function $\mu : \mathbb{N} \rightarrow \mathbb{R}^+$ such that $\forall n \in \mathbb{N} \; \left|\Pr[D(r) = 1] - \Pr[D(G(s)) = 1]\right| \leq \mu(n)$, where $r \leftarrow \{0,1\}^{l(n)}$ and $s \leftarrow \{0,1\}^n$.

l is called the expansion factor of G.

From distinguishers to predictors

A on input $f(s)$

1. $r' \leftarrow \{0,1\}$
2. Invoke D with input $f(s) \| r'$
3. If D returns 1, then output r', otherwise output complement of r'.

PRGs with arbitrary expansion

Theorem 5.14 If there is a PRG $\bar{G}$ with expansion factor n+1, then there is a PRG G with expansion factor $p(n)$ for every polynomial $p:\mathbb{N} \to \mathbb{N}$ with $p(n) \geq n$ for all $n \in \mathbb{N}$.

The construction

$\bar{G}$ PRG with expansion $n+1$

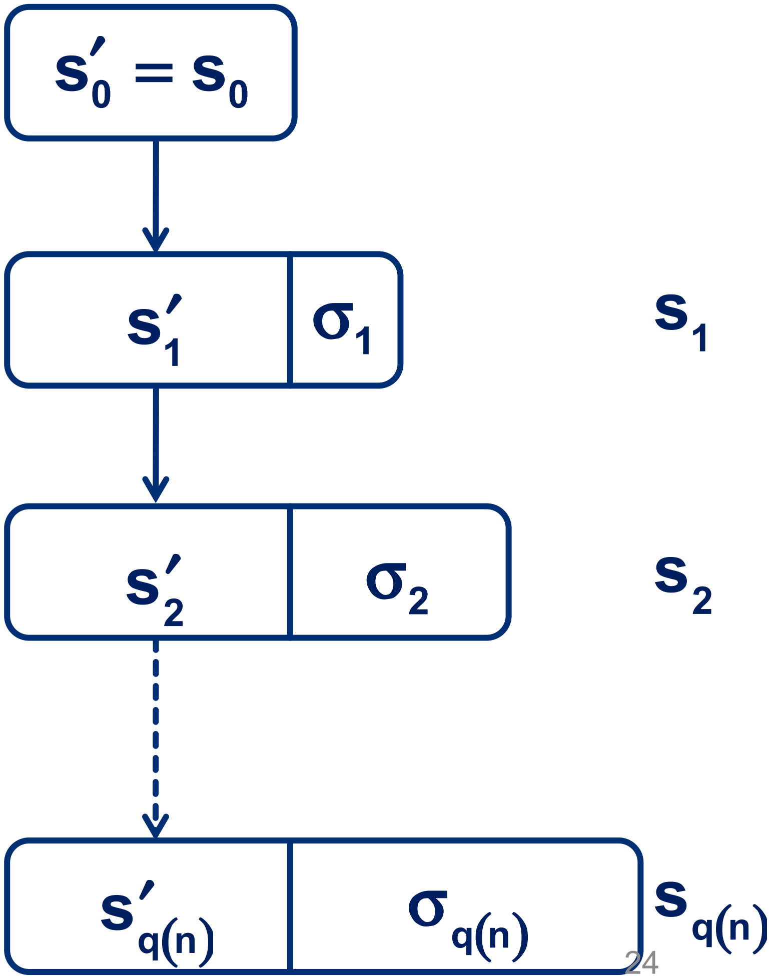
G on input $s \in \{0,1\}^n$

1. $q(n) := p(n) - n$.
2. Set $s_0 := s, \sigma_0 := \varepsilon$ (empty string)
3. For $i = 1, \ldots, q(n)$ do:
   a) Define s'_{i-1} to be the first n bits of s_{i-1}
   and σ_{i-1} to be the last $i-1$ bits of s_{i-1}.
   b) Set $s_i := \bar{G}(s'_{i-1}) \| \sigma_{i-1}$.
4. Output $s_{q(n)}$.

The construction

G on input $s \in \{0,1\}^n$

1. $q(n) := p(n) - n.$
2. Set $s_0 := s, \sigma_0 := \varepsilon$ (empty string)
3. For $i = 1,\dots,q(n)$ do:
   a) Define s'_{i-1} to be the first n bits of s_{i-1} and σ_{i-1} to be the last $i-1$ bits of s_{i-1}.
   b) Set $s_i := \bar{G}(s'_{i-1}) \parallel \sigma_{i-1}$.
4. Output $s_{q(n)}$.



The construction –a special case

- $f:\{0,1\}^* \rightarrow \{0,1\}^*$ a one-way function
- $hc:\{0,1\}^* \rightarrow \{0,1\}$ a hardcore predicate for f.
- $\bar{G}(s) = f(s) \| hc(s)$

G with expansion factor $p(n)$:

$$G(s) = f^{(p(n)-n)}(s) \| hc\left(f^{(p(n)-n-1)}(s)\right) \| \cdots \| hc\left(f^{(1)}(s)\right) \| hc\left(f^{(0)}(s)\right)$$

The case p(n)=n+2

Claim 5.15 If there is a PRG $\bar{G}$ with expansion factor $n+1$, then there is a PRG G with expansion factor $n+2$.

Hybrid distributions

$\bar{G}$ PRG with expansion $n+1$, G corresponding PRG with expansion factor $n+2$

3 distributions on $\{0,1\}^{n+2}$:

$$H_n^0: \quad s_0 \leftarrow \{0,1\}^n, s = G(s_0)$$

$$H_n^1: \quad s_1' \leftarrow \{0,1\}^n, \sigma_1 \leftarrow \{0,1\}, s = \bar{G}(s_1') \,\|\, \sigma_1$$

$$H_n^2: \quad s \leftarrow \{0,1\}^{n+2}$$

The case p(n)=n+2

Claim 5.15 If there is a PRG $\bar{G}$ with expansion factor $n+1$, then there is a PRG G with expansion factor $n+2$.

For every ppt D there is a negligible function $\mu(n)$ such that

$$\left|\Pr_{s_2 \leftarrow H_n^0}\left[D(s_2)=1\right]-\Pr_{s_2 \leftarrow H_n^1}\left[D(s_2)=1\right]\right| \leq \mu(n).$$

For every ppt D there is a negligible function $\mu(n)$ such that

$$\left|\Pr_{s_2 \leftarrow H_n^1}\left[D(s_2)=1\right]-\Pr_{s_2 \leftarrow H_n^2}\left[D(s_2)=1\right]\right| \leq \mu(n).$$

The case p(n)=n+2

D distinguisher against G, construct distinguisher D' against $\overline{G}$ as follows:

D' on input $w \in \{0,1\}^{n+1}$

1. $j \leftarrow \{1,2\}$
2. $\sigma_j \leftarrow \{0,1\}^{j-1}$
3. $s_j := w \| \sigma_j$. Run G, with input s_j and starting with iteration $i = j+1$, and output $D\left(s_{q(n)}\right)$.

The case p(n)=n+2

D' on input $w \in \{0,1\}^{n+1}$

1. $j \leftarrow \{1,2\}$
2. $\sigma_j \leftarrow \{0,1\}^{j-1}$
3. $s_j := w \| \sigma_j$. Run G, with input s_j and starting with iteration $i = j+1$, and output $D\left(s_{q(n)}\right)$.

Crucial equality

$$\left|\Pr_{w \leftarrow \{0,1\}^{n+1}}\left[D'(w)=1\right] - \Pr_{s \leftarrow \{0,1\}^{n}}\left[D'\left(\bar{G}(s)\right)=1\right]\right|$$

$$= \left|\frac{1}{2}\left(\Pr_{s_2 \leftarrow H_n^2}\left[D(s_2)=1\right] - \Pr_{s_2 \leftarrow H_n^1}\left[D(s_2)=1\right]\right)\right.$$

$$+ \left.\frac{1}{2}\left(\Pr_{s_2 \leftarrow H_n^1}\left[D(s_2)=1\right] - \Pr_{s_2 \leftarrow H_n^0}\left[D(s_2)=1\right]\right)\right|$$

$$= \frac{1}{2}\left|\Pr\left[D(s_2)=1\right] - \Pr\left[D(G(s))=1\right]\right|$$

Hybrid distributions for the general case

$\overline{G}$ PRG with expansion $n+1$, G corresponding PRG with expansion factor $p(n)$, set $q(n)=p(n)-n$.

Hybrid distribution $H_n^j, 0 \leq j \leq q(n)$

1. $s_j \leftarrow \{0,1\}^{n+j}$
2. Run G, starting with iteration $j+1$ and with s_j as input.
3. Output $s_{q(n)}$.

PRFs from PRGs

Theorem 5.16 **If there is a PRG G, then pseudorandom functions exist.**

Truly random functions

$$\text{Func}_n := \left\{ f : \{0,1\}^n \rightarrow \{0,1\}^n \right\}$$

$$\left|\text{Func}_n\right| = 2^{n2^n}$$

random function: $f \leftarrow \text{Func}_n$

Pseudorandom function (PRF)

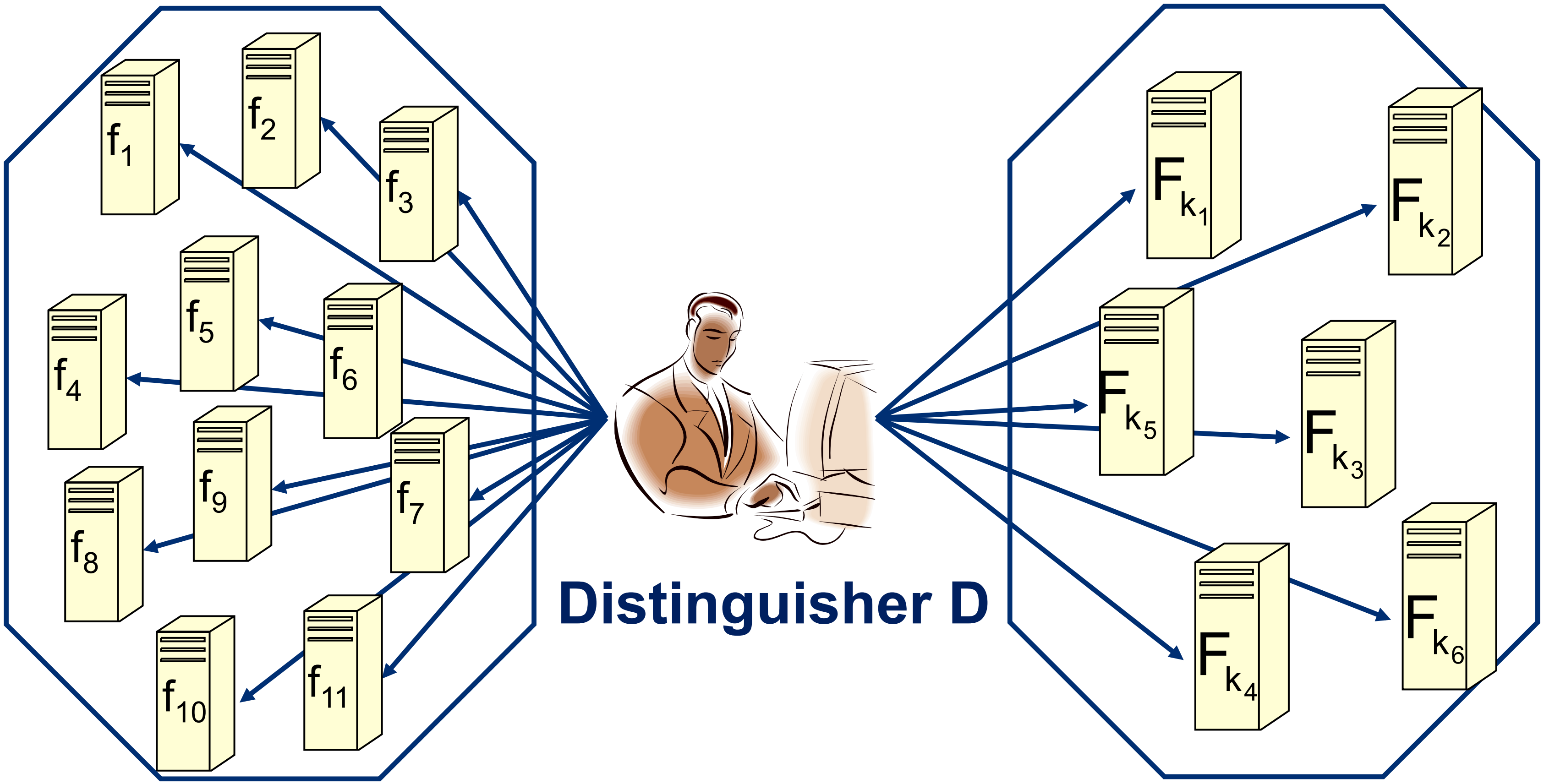
Definition 3.4 (old) Let $F:\{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ be a keyed, efficient and length-preserving function. F is called a pseudorandom function, if for all ppt distinguishers D there is a negligible function μ such that for all $n \in \mathbb{N}$

$$\left| \Pr\left[D^{F_k(\cdot)}\left(1^n\right) = 1 \right] - \Pr\left[D^{f(\cdot)}\left(1^n\right) = 1 \right] \right| \leq \mu(n),$$

where $k \leftarrow \{0,1\}^n, f \leftarrow \mathrm{Func}_n$.

$$\mathrm{Func}_n := \left\{ f : \{0,1\}^n \rightarrow \{0,1\}^n \right\}$$

Pseudorandom functions



$Func_n$
with uniform distribution

$$\mathcal{F}_n = \{F_k(\cdot)\}_{k \in \{0,1\}^n}$$

with distribution $k \leftarrow \{0,1\}^n$

From PRF to cpa-security

Construction 3.6 (old) Let $F:\{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ be a keyed, efficient, and length-preserving function. Define $\Pi_F = (Gen_F, Enc_F, Dec_F)$ as follows:

Gen_F : on input 1^n : $k \leftarrow \{0,1\}^n$.

Enc_F : on input $k, m \in \{0,1\}^n$, choose $r \leftarrow \{0,1\}^n$ and output $c := (r, m \oplus F_k(r))$.

Dec_F : on input $c = (r,s) \in \{0,1\}^n \times \{0,1\}^n$ and $k \in \{0,1\}^n$ output $m := s \oplus F_k(r)$.

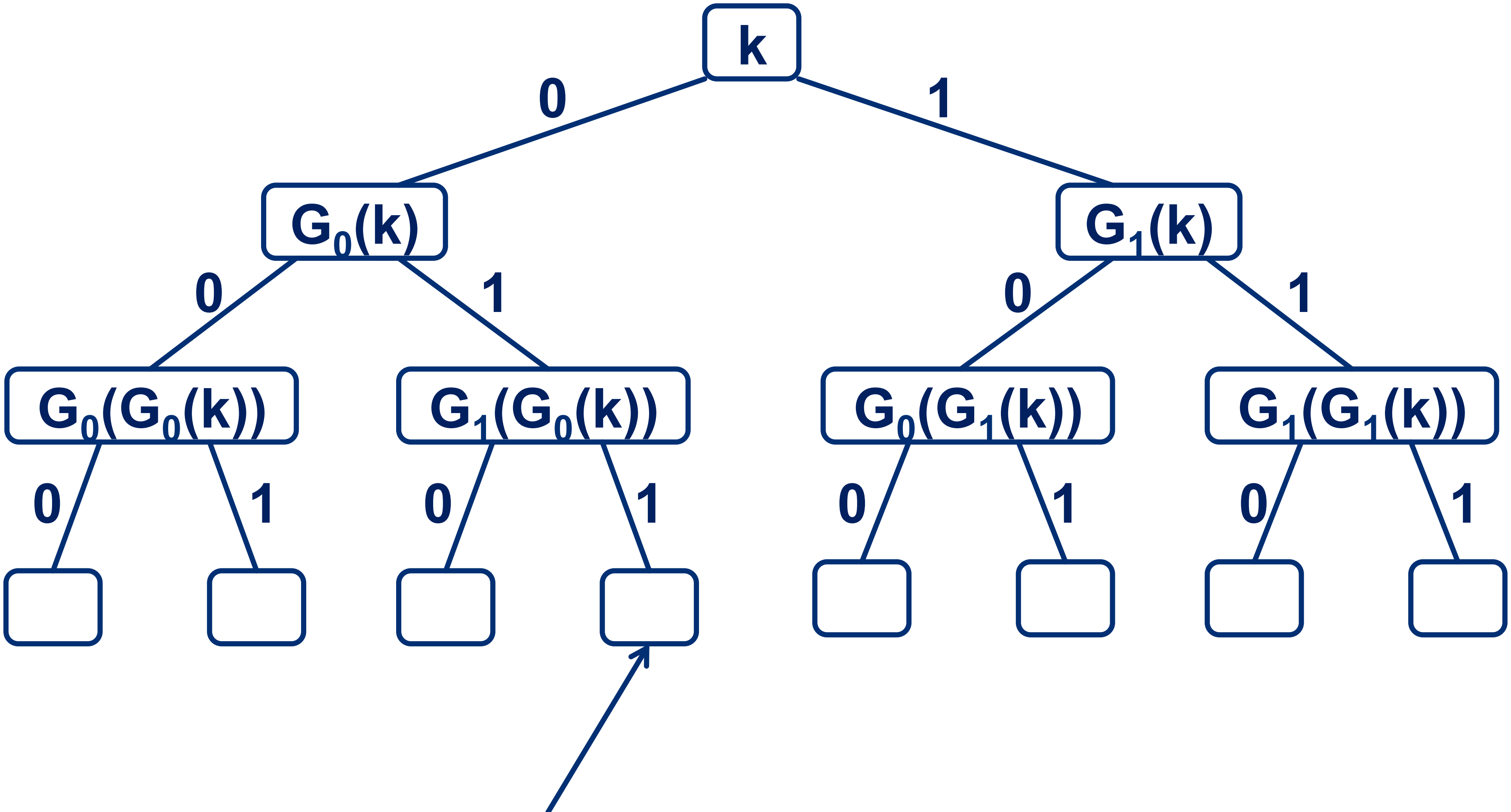
PRFs from PRGs

Theorem 5.16 If there is a PRG G, then pseudorandom functions exist.

Construction 5.17 Let G be a PRG G with expansion factor $p(n) = 2n$. By $G_0(k), G_1(k)$ denote the first and second half of G's output. For every k define the function F_k as follows.

$$\begin{aligned} F_k : \quad \{0,1\}^n &\rightarrow \{0,1\}^n \\ x = x_1 \ldots x_n &\mapsto G_{x_n}\left(\cdots\left(G_{x_2}\left(G_{x_1}(k)\right)\right)\cdots\right) \end{aligned}$$

PRFs from PRGs



$$F_k(011) = G_1(G_1(G_0(k)))$$

Hybrid distributions

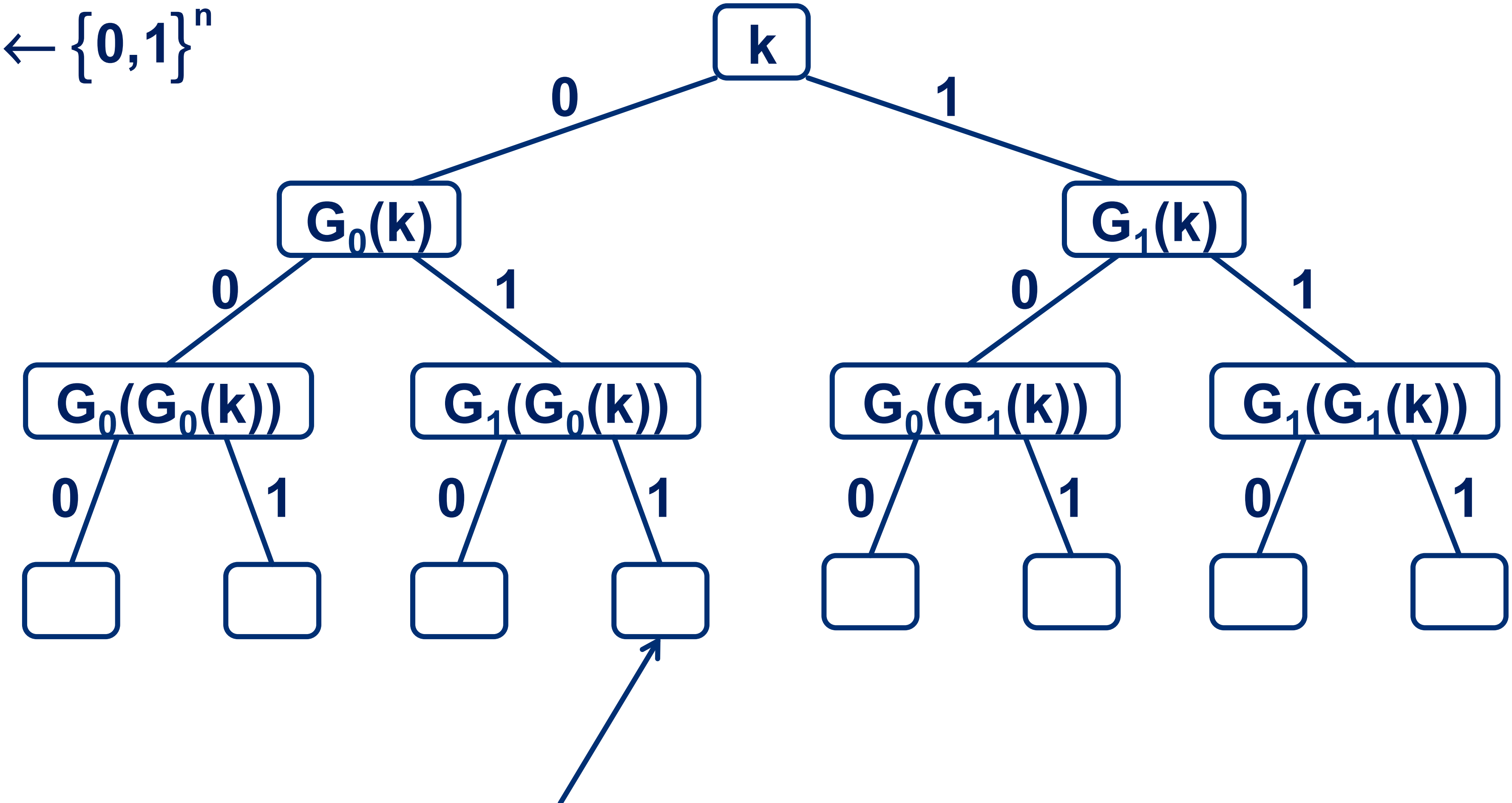
H_n^i distribution on a family of functions $\mathcal{F}_n^i := \{f_s\}_{s \in \{0,1\}^{n2^i}}$

distribution given by $s \leftarrow \{0,1\}^{n2^i}$

Hybrid distributions

Hybrid H_n^0

$k \leftarrow \{0,1\}^n$

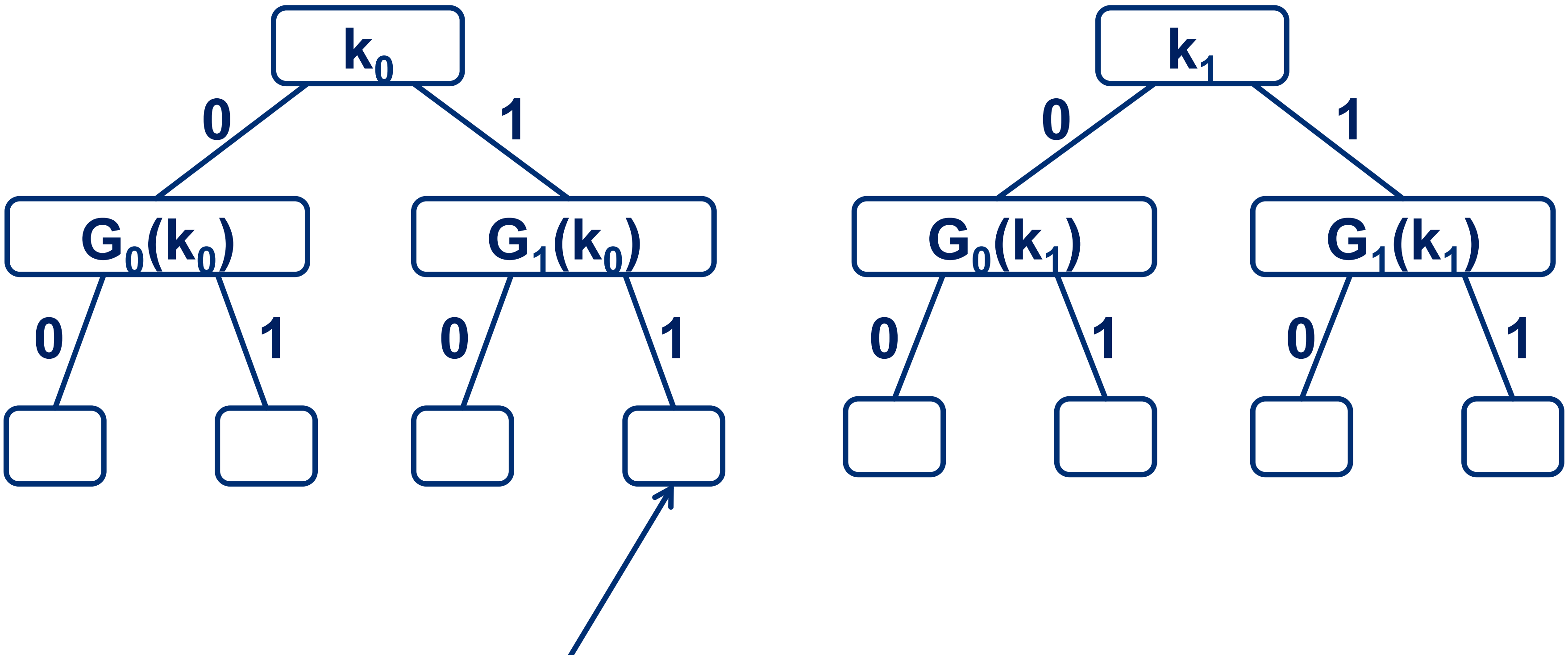


$F_k(011) = G_1(G_1(G_0(k)))$

Hybrid distributions

Hybrid H_n^1

$$k_0 \leftarrow \{0,1\}^n, k_1 \leftarrow \{0,1\}^n$$

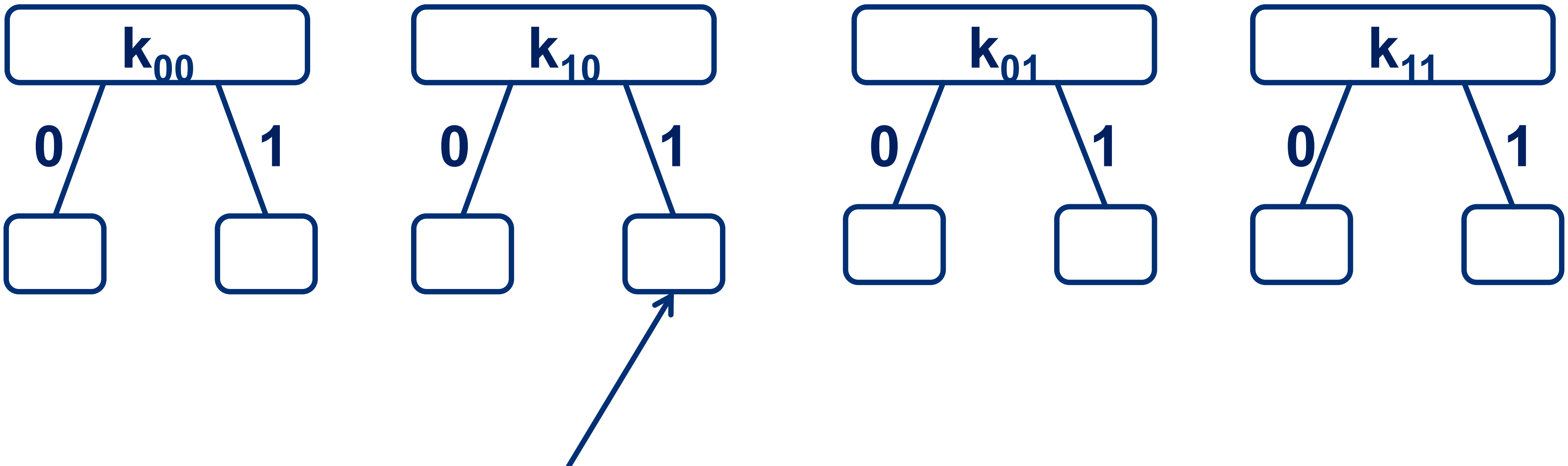


$$F_{k_0k_1}(011) = G_1(G_1(k_0))$$

Hybrid distributions

Hybrid H_n^2

$$k_{00} \leftarrow \{0,1\}^n, k_{10} \leftarrow \{0,1\}^n, k_{01} \leftarrow \{0,1\}^n, k_{11} \leftarrow \{0,1\}^n$$

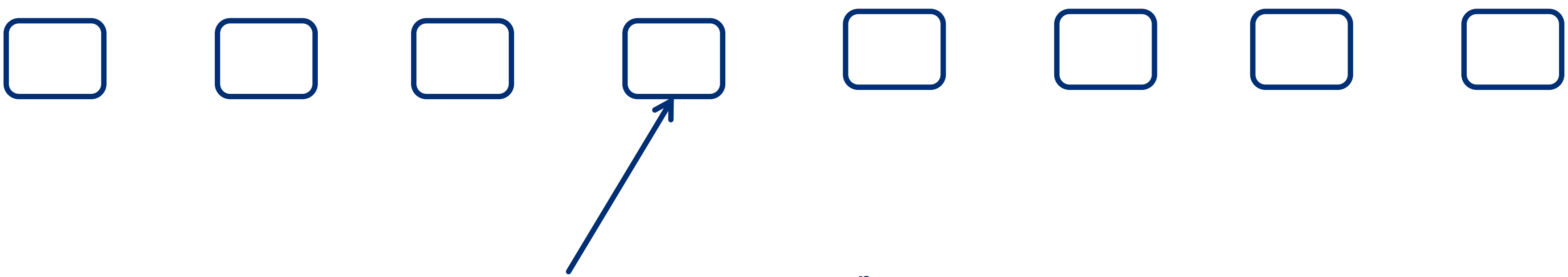


$$F_{k_{00}k_{10}k_{01}k_{11}}(011) = G_1(k_{10})$$

Hybrid distributions

Hybrid H_n^n

$$k_b \leftarrow \{0,1\}^n, b \in \{0,1\}^n$$



$$F_s(011) = k_{110}, s \in \{0,1\}^{n2^n}$$

Hybrid distributions

H_n^i distribution on a family of functions $\mathcal{F}_n^i := \{f_s\}_{s \in \{0,1\}^{n2^i}}$

distribution given by $s \leftarrow \{0,1\}^{n2^i}$

- H_n^0 pseudorandom function
- H_n^n random function
- H_n^i and H_n^{i+1} differ in one application of G
- Distinguisher for H_n^0 and H_n^n leads to distinguisher for H_n^i and H_n^{i+1} for some i.
- Distinguisher for H_n^i and H_n^{i+1} leads to distinguisher for G and uniform distribution.

Neccessary conditions

Theorem 5.18 If pseudorandom generators exist, then one-way functions exist.

Theorem 5.19 If encryption schemes with indistinguishable encryptions against eavesdropping adversaries exist, then one-way functions exist.