Foundations II

601.442/642 Modern Cryptography

5th March 2026

Logistics

- Homework 5 is due **today**.
- Homework 6 will be out today and due next Thursday (12th March).

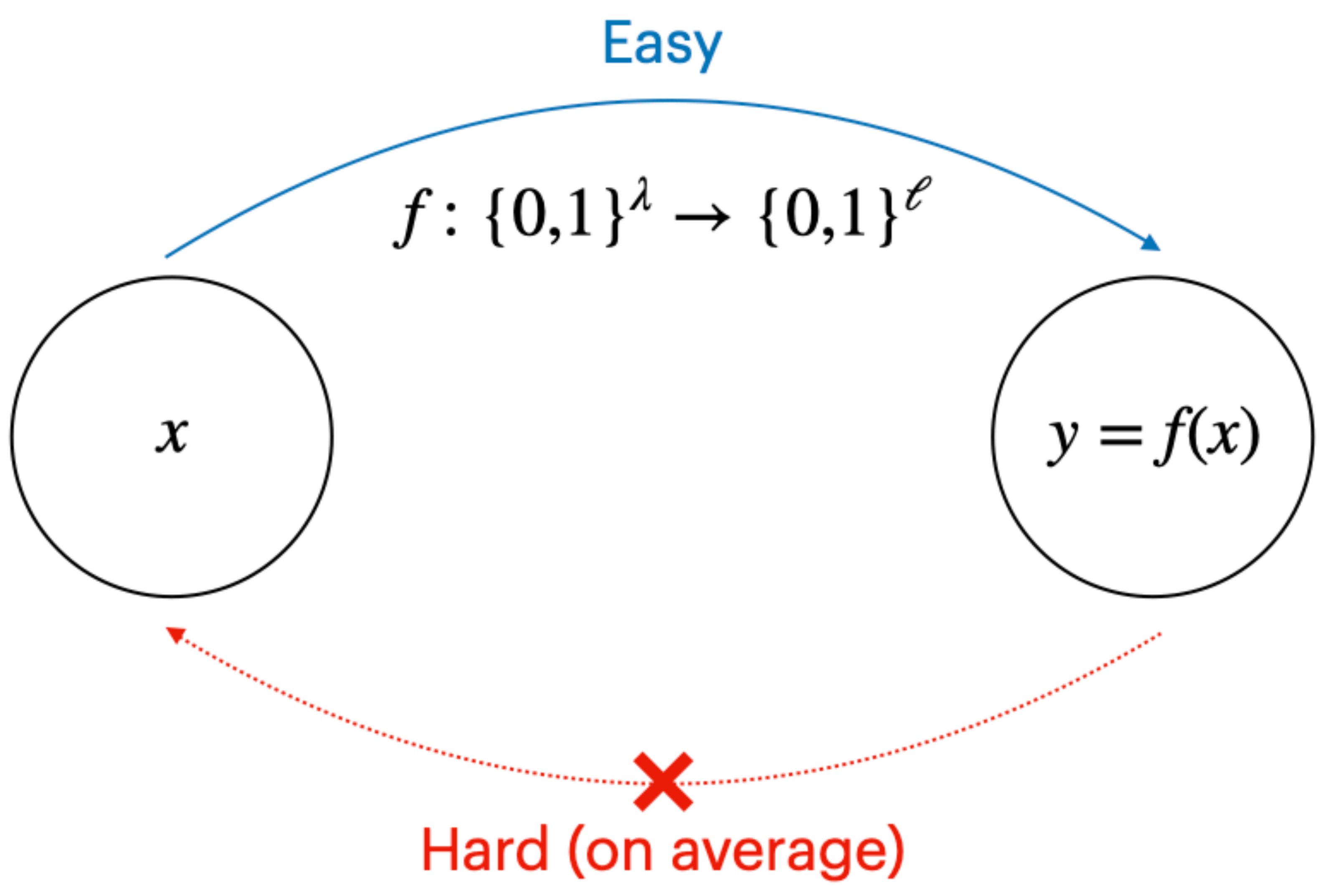
Recap: One-Way Functions

One-Way Function

A family of functions $\{f_\lambda : \{0,1\}^\lambda \to \{0,1\}^\ell\}_\lambda$ is a **one-way function** if it satisfies the following properties.

- **Easy to compute:** For all $\lambda \in \mathbb{N}$, f_λ can be computed in polynomial time.
- **Hard to invert:** For all NUPPT adversaries A, there exists a negligible function **negl**, such that for all $\lambda \in \mathbb{N}$

$$\Pr\left[f(x') = y : \begin{array}{r} x \xleftarrow{\$} \{0,1\}^\lambda \\ y := f(x) \\ x' \leftarrow A(1^\lambda, y) \end{array} \right] \leq \mathsf{negl}(\lambda).$$



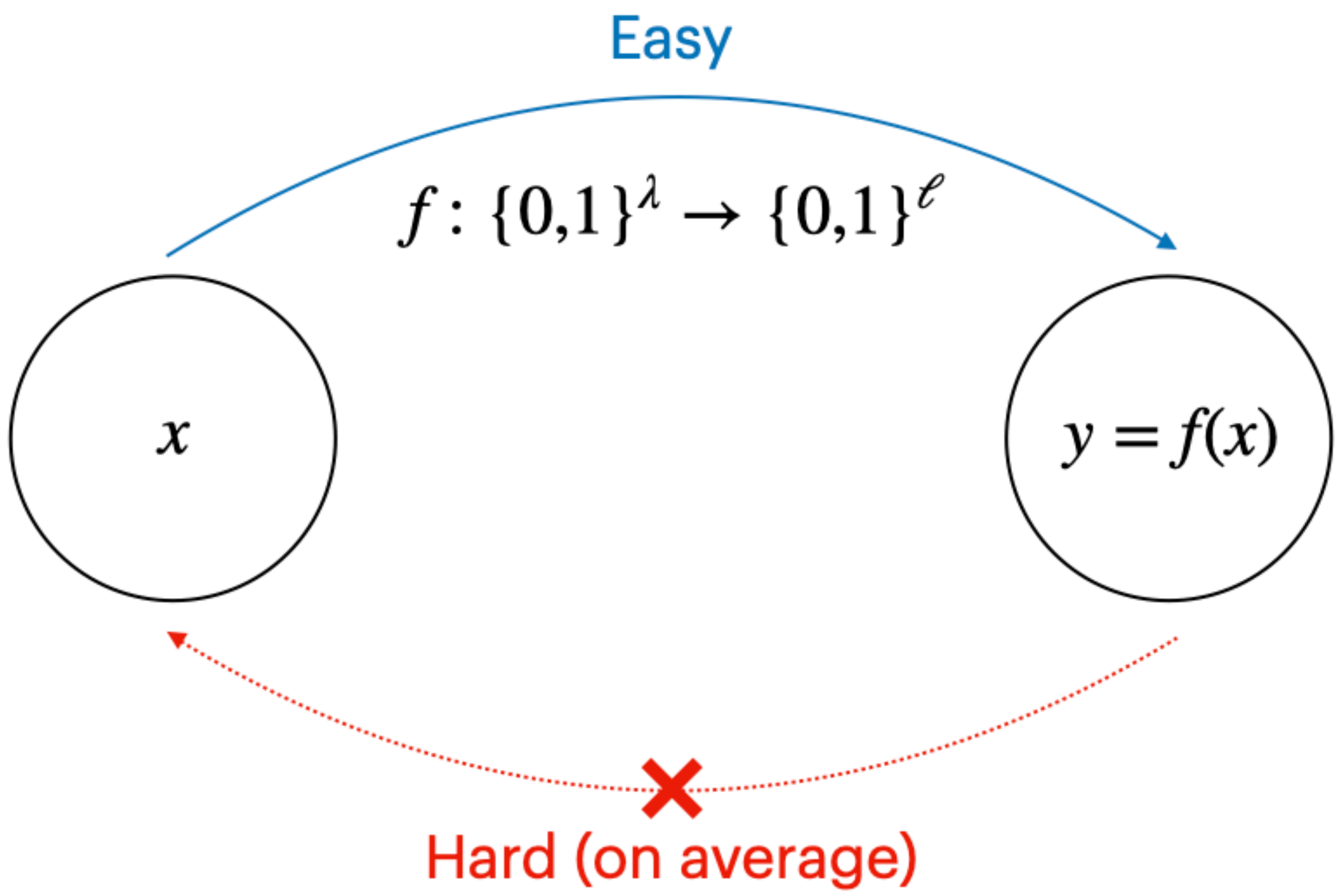
Recap: One-Way Functions

One-Way Function

A family of functions $\{f_\lambda : \{0,1\}^\lambda \to \{0,1\}^\ell\}_\lambda$ is a **one-way function** if it satisfies the following properties.

- **Easy to compute:** For all $\lambda \in \mathbb{N}$, f_λ can be computed in polynomial time.
- **Hard to invert:** For all NUPPT adversaries A, there exists a negligible function **negl**, such that for all $\lambda \in \mathbb{N}$

$$\Pr\left[f(x') = y : \begin{array}{c} x \xleftarrow{\$} \{0,1\}^\lambda \\ y := f(x) \\ x' \leftarrow A(1^\lambda, y) \end{array} \right] \leq \mathsf{negl}(\lambda).$$



One-way Permutation: One-one OWF with $\ell = \lambda$.

Recap: Hard-Core Predicate

Hard-Core Predicate

Given a one-way function f, a family of functions $\{\mathsf{hc}_\lambda : \{0,1\}^\lambda \to \{0,1\}\}_\lambda$ is a hard-core predicate for f if it satisfies the following properties.

- **Easy to compute:** For all $\lambda \in \mathbb{N}$, hc_λ can be computed in polynomial time.
- **Hard to predict:** For all NUPPT adversaries A, there exists a negligible function **negl**, such that for all $\lambda \in \mathbb{N}$

$$\Pr_{x \overset{\$}{\leftarrow} \{0,1\}^\lambda}\left[A(f(x)) = \mathsf{hc}(x)\right] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$

Recap: PRGs from OWF

Theorem [Håstad-Impagliazzo-Levin-Luby’90]**:**

$$\text{OWF} \Longrightarrow \text{PRG}.$$

Recap: PRGs from OWP

Theorem [Goldreich-Levin'89]**:**

$$\text{OWP} \implies \text{PRG}.$$

Recap: PRGs from OWP

Theorem [Goldreich-Levin'89]**:**

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \parallel \mathsf{hc}(x)\,.$$

PRG with single-bit stretch.

Recap: PRGs from OWP

Theorem [Goldreich-Levin'89]**:**

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \mathbin\Vert \mathsf{hc}(x)\,.$$

PRG with single-bit stretch.

Intuition:

Recap: PRGs from OWP

Theorem [Goldreich-Levin'89]**:**

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \parallel \mathsf{hc}(x)\,.$$

PRG with single-bit stretch.

Intuition:

Since f is a one-one, when x is sampled uniformly at random, $f(x)$ is uniformly random over $\{0,1\}^\lambda$.

Recap: PRGs from OWP

Theorem [Goldreich-Levin'89]:

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \parallel \mathsf{hc}(x) .$$

PRG with single-bit stretch.

Intuition:

Since f is a one-one, when x is sampled uniformly at random, $f(x)$ is uniformly random over $\{0,1\}^\lambda$.

Thus, if $G(x)$ is distinguishable from a uniformly random string, then it must be because of appending hc(x). But hc(x) is hard to predict even given $f(x)$.

PRGs from OWP

Theorem [Goldreich-Levin'89]**:**

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \parallel \mathsf{hc}(x) .$$

PRGs from OWP

Theorem [Goldreich-Levin'89]**:**

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \parallel \mathsf{hc}(x)\,.$$

Proof:

We want to show

$$\{f(x) \parallel \mathsf{hc}(x) : x \xleftarrow{\$} \{0,1\}^{\lambda}\}$$

$$\overset{c}{\approx}$$

$$\{r : r \xleftarrow{\$} \{0,1\}^{\lambda+1}\}$$

PRGs from OWP

Theorem [Goldreich-Levin'89]:

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \parallel \mathsf{hc}(x)\,.$$

Proof:

We want to show

$$\{f(x) \parallel \mathsf{hc}(x) : x \overset{\$}{\leftarrow} \{0,1\}^{\lambda}\}$$

$$\overset{c}{\approx}$$

$$\{r : r \overset{\$}{\leftarrow} \{0,1\}^{\lambda+1}\}$$

$$\equiv$$

$$\{f(x) \parallel b : x \overset{\$}{\leftarrow} \{0,1\}^{\lambda}, b \overset{\$}{\leftarrow} \{0,1\}\}$$

PRGs from OWP

Theorem [Goldreich-Levin'89]**:**

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \parallel \mathsf{hc}(x)\,.$$

Proof:

We want to show

$$\{f(x) \parallel \mathsf{hc}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$

$$\overset{c}{\approx}$$

$$\{f(x) \parallel b : x \xleftarrow{\$} \{0,1\}^\lambda, b \xleftarrow{\$} \{0,1\}\}$$

PRGs from OWP

Theorem [Goldreich-Levin'89]:

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \,\|\, \mathsf{hc}(x)\,.$$

Proof:

We want to show

$$\begin{array}{ccc} \{f(x) \,\|\, \mathsf{hc}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\} & & \{f(x) \,\|\, \mathsf{hc}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\} \\ \overset{c}{\approx} & \Longleftrightarrow & \overset{c}{\approx} \\ \{f(x) \,\|\, b : x \xleftarrow{\$} \{0,1\}^\lambda, b \xleftarrow{\$} \{0,1\}\} & & \{f(x) \,\|\, \overline{\mathsf{hc}}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\} \end{array}$$

$$\overline{\mathsf{hc}}(x) := \mathsf{hc}(x) \oplus 1$$

PRGs from OWP

Theorem [Goldreich-Levin'89]:

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \,\|\, \mathsf{hc}(x)\,.$$

Proof:

We want to show

$$\{f(x) \,\|\, \mathsf{hc}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\} \overset{c}{\approx} \{f(x) \,\|\, b : x \xleftarrow{\$} \{0,1\}^\lambda, b \xleftarrow{\$} \{0,1\}\} \iff \{f(x) \,\|\, \mathsf{hc}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\} \overset{c}{\approx} \{f(x) \,\|\, \overline{\mathsf{hc}}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$

$b = \mathsf{hc}(x)$ with probability 1/2; any distinguishing advantage must stem from when $b \neq \mathsf{hc}(x)$.

$\overline{\mathsf{hc}}(x) := \mathsf{hc}(x) \oplus 1$

PRGs from OWP

Theorem [Goldreich-Levin'89]:

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \,\|\, \mathsf{hc}(x)\,.$$

Proof:

We want to show

$$\{f(x) \,\|\, \mathsf{hc}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\} \overset{c}{\approx} \{f(x) \,\|\, b : x \xleftarrow{\$} \{0,1\}^\lambda, b \xleftarrow{\$} \{0,1\}\}$$

$\iff$

We will show

$$\{f(x) \,\|\, \mathsf{hc}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\} \overset{c}{\approx} \{f(x) \,\|\, \overline{\mathsf{hc}}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$

$\overline{\mathsf{hc}}(x) := \mathsf{hc}(x) \oplus 1$

$b = \mathsf{hc}(x)$ with probability 1/2; any distinguishing advantage must stem from when $b \neq \mathsf{hc}(x)$.

PRGs from OWP

Theorem [Goldreich-Levin'89]**:**

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \parallel \mathsf{hc}(x)\,.$$

Proof:

We want to show

$$H_0 := \{f(x) \parallel \mathsf{hc}(x) : x \overset{\$}{\leftarrow} \{0,1\}^\lambda\}$$

$$\overset{c}{\approx}$$

$$H_1 := \{f(x) \parallel \overline{\mathsf{hc}}(x) : x \overset{\$}{\leftarrow} \{0,1\}^\lambda\}$$

PRGs from OWP

Theorem [Goldreich-Levin'89]**:**

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \parallel \mathsf{hc}(x)\,.$$

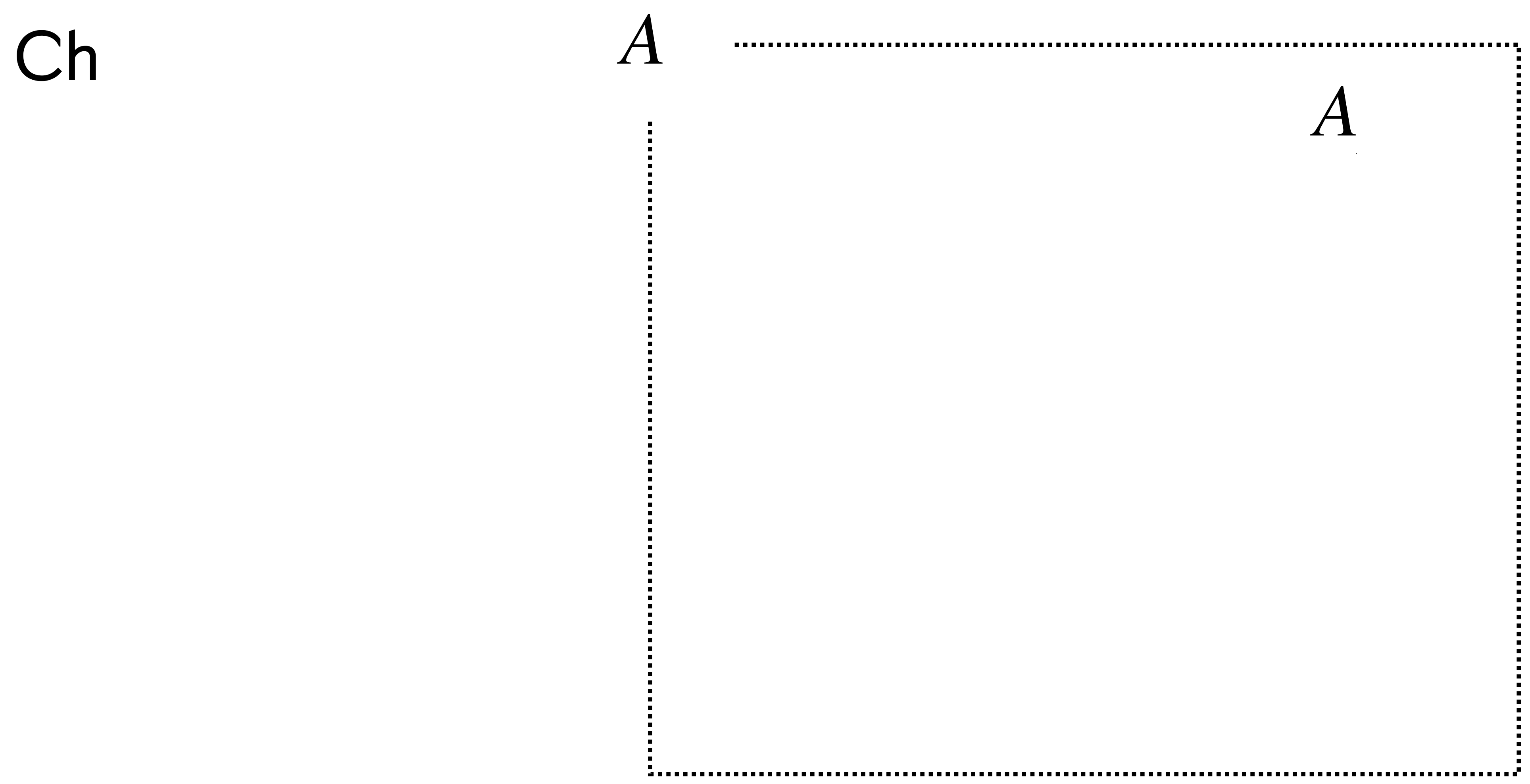
Proof:

We want to show

$$H_0 := \{f(x) \parallel \mathsf{hc}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$

$$\overset{c}{\approx}$$

$$H_1 := \{f(x) \parallel \overline{\mathsf{hc}}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$



PRGs from OWP

Theorem [Goldreich-Levin’89]**:**

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \parallel \mathsf{hc}(x)\,.$$

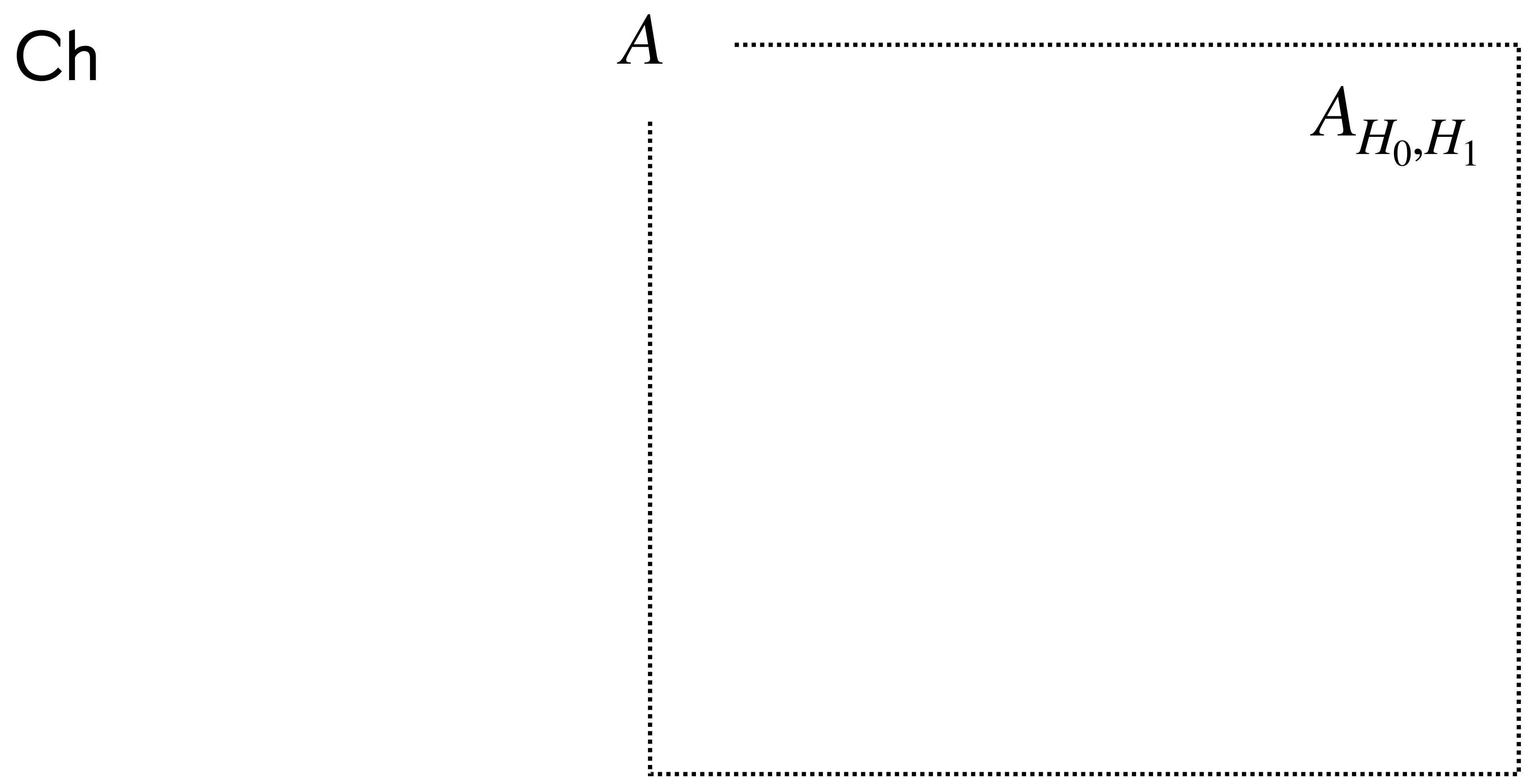
Proof:

We want to show

$$H_0 := \{f(x) \parallel \mathsf{hc}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$

$$\overset{c}{\approx}$$

$$H_1 := \{f(x) \parallel \overline{\mathsf{hc}}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$



PRGs from OWP

Theorem [Goldreich-Levin'89]**:**

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \parallel \mathsf{hc}(x)\,.$$

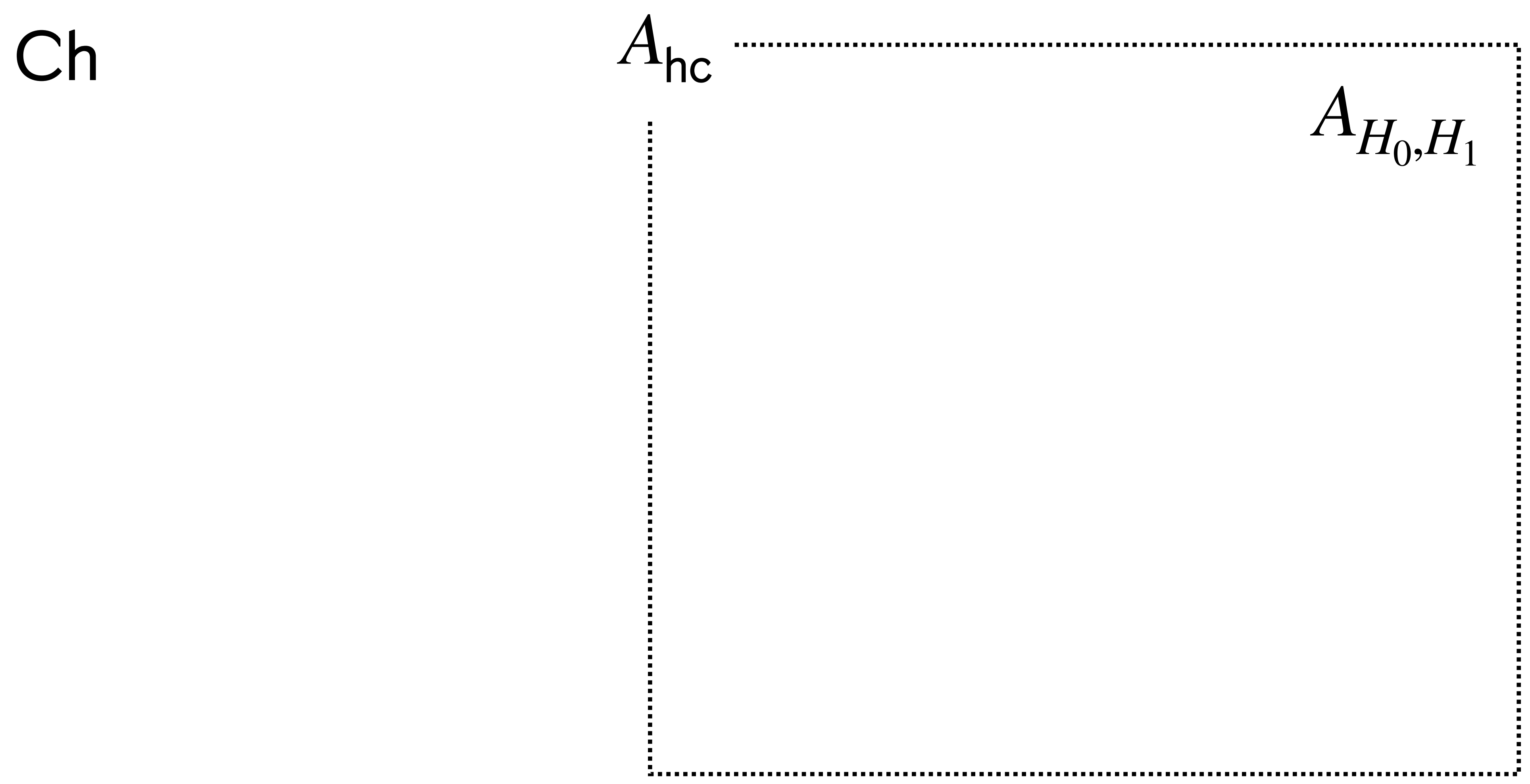
Proof:

We want to show

$$H_0 := \{f(x) \parallel \mathsf{hc}(x) : x \overset{\$}{\leftarrow} \{0,1\}^\lambda\}$$

$$\overset{c}{\approx}$$

$$H_1 := \{f(x) \parallel \overline{\mathsf{hc}}(x) : x \overset{\$}{\leftarrow} \{0,1\}^\lambda\}$$



PRGs from OWP

Theorem [Goldreich-Levin'89]**:**

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \parallel \mathsf{hc}(x)\,.$$

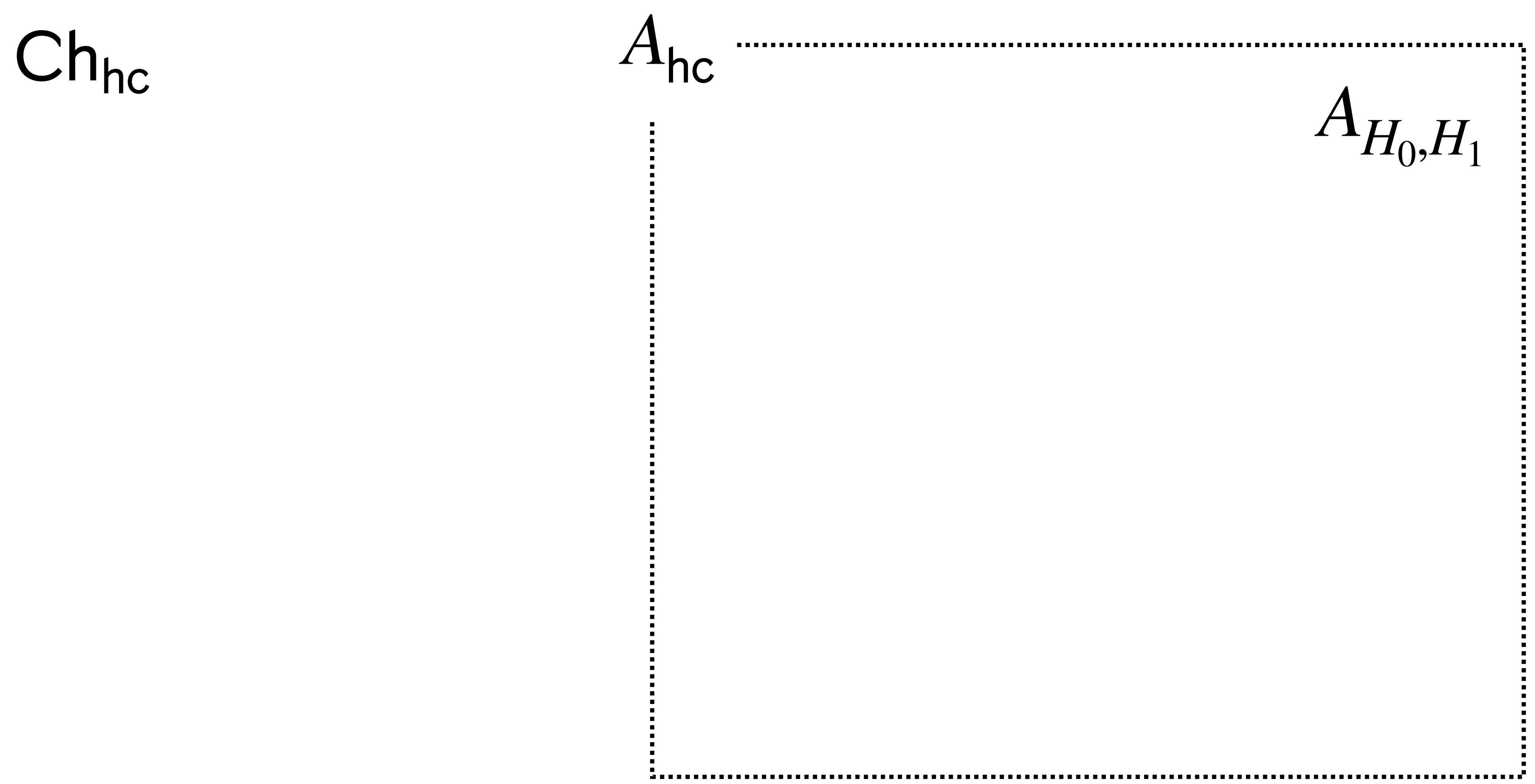
Proof:

We want to show

$$H_0 := \{f(x) \parallel \mathsf{hc}(x) : x \overset{\$}{\leftarrow} \{0,1\}^\lambda\}$$

$$\overset{c}{\approx}$$

$$H_1 := \{f(x) \parallel \overline{\mathsf{hc}}(x) : x \overset{\$}{\leftarrow} \{0,1\}^\lambda\}$$



$\mathsf{Ch}_{\mathsf{hc}}$

A_{hc}

A_{H_0,H_1}

PRGs from OWP

Theorem [Goldreich-Levin'89]:

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \parallel \mathsf{hc}(x)\,.$$

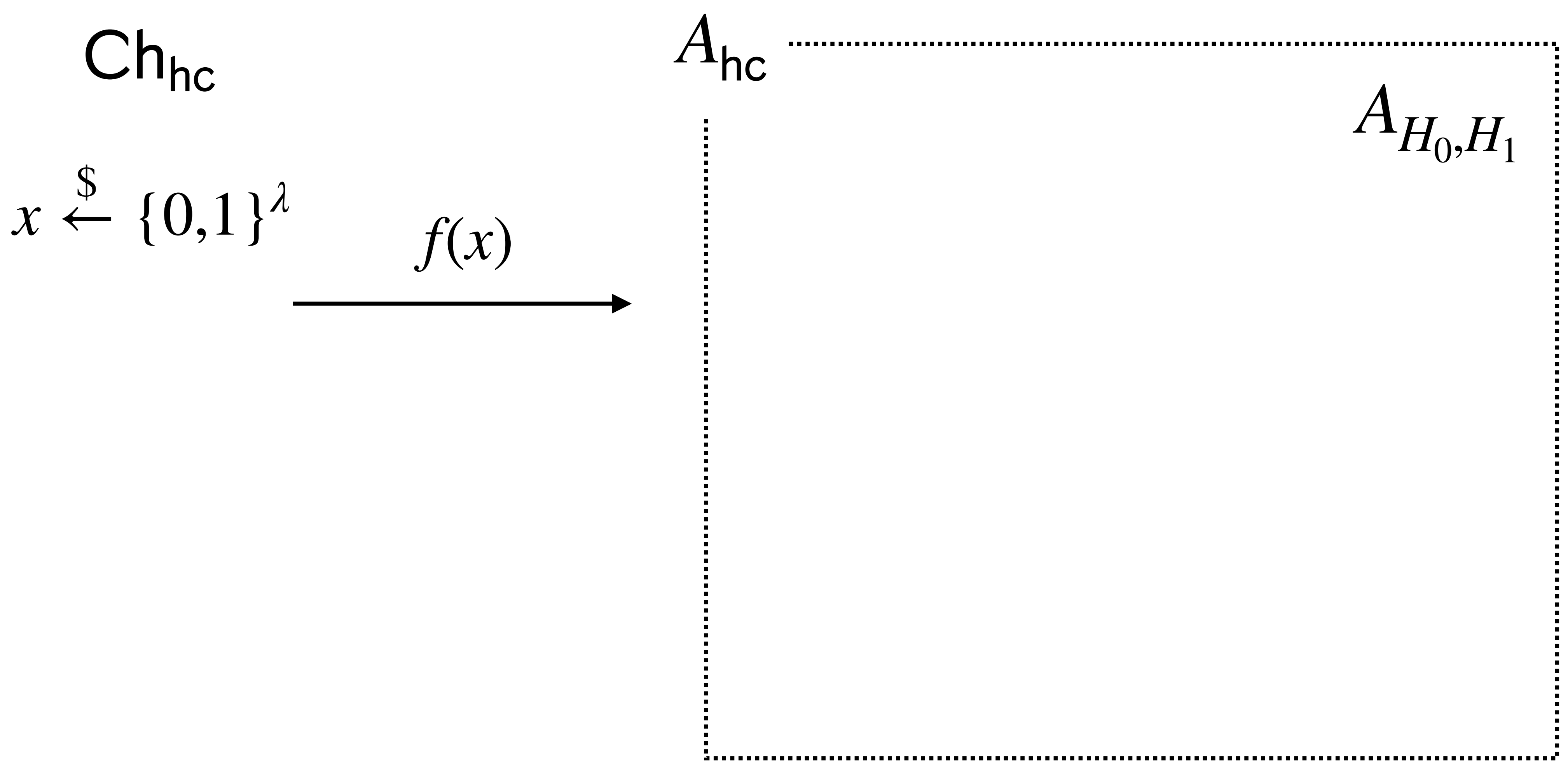
Proof:

We want to show

$$H_0 := \{f(x) \parallel \mathsf{hc}(x) : x \overset{\$}{\leftarrow} \{0,1\}^\lambda\}$$

$$\overset{c}{\approx}$$

$$H_1 := \{f(x) \parallel \overline{\mathsf{hc}}(x) : x \overset{\$}{\leftarrow} \{0,1\}^\lambda\}$$



$\mathsf{Ch}_{\mathsf{hc}}$

$x \overset{\$}{\leftarrow} \{0,1\}^\lambda$

PRGs from OWP

Theorem [Goldreich-Levin'89]**:**

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \,\|\, \mathsf{hc}(x)\,.$$

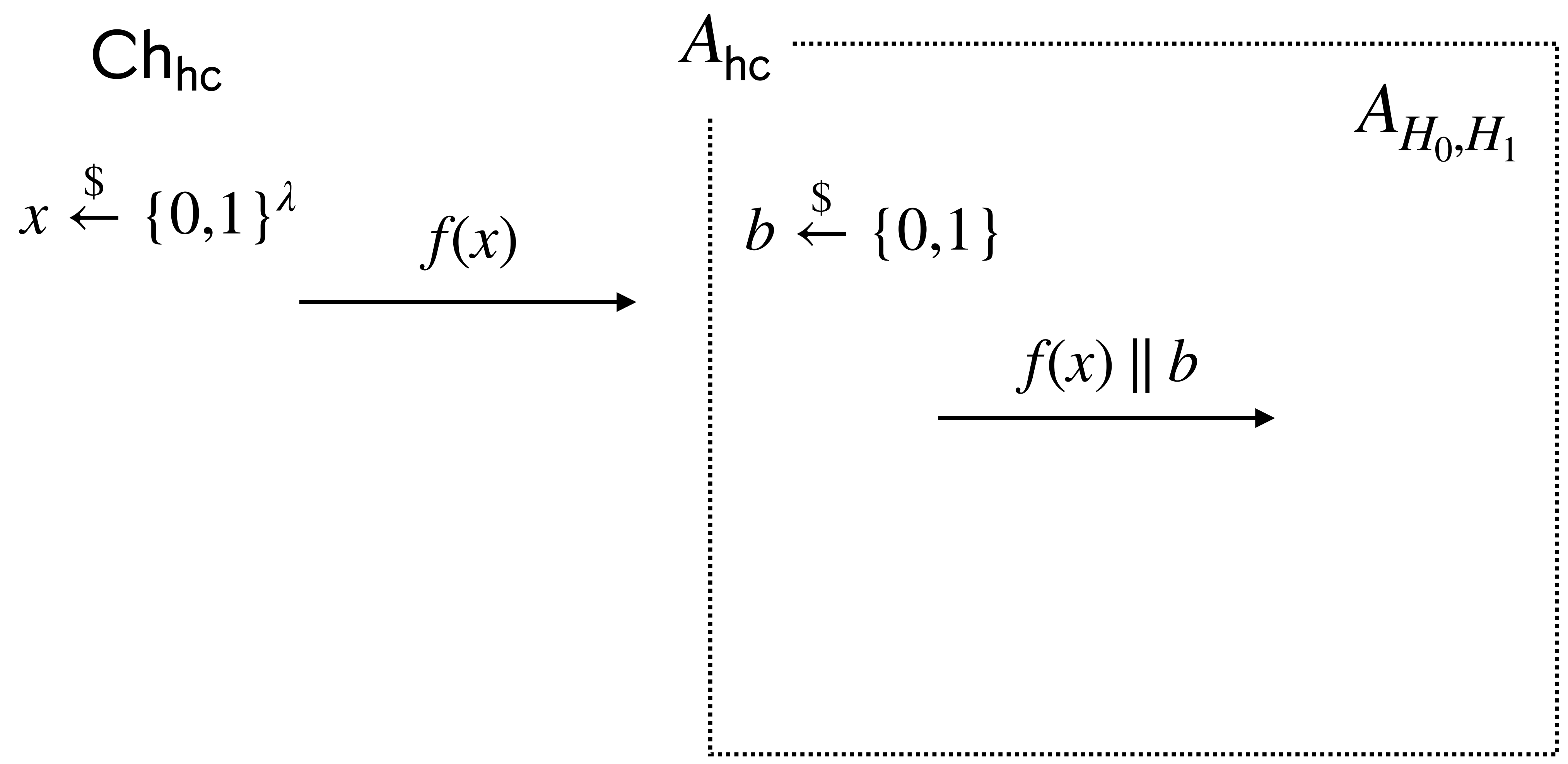
Proof:

We want to show

$$H_0 := \{f(x) \,\|\, \mathsf{hc}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$

$$\overset{c}{\approx}$$

$$H_1 := \{f(x) \,\|\, \overline{\mathsf{hc}}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$



$\mathsf{Ch}_{\mathsf{hc}}$

A_{hc}

A_{H_0,H_1}

$x \xleftarrow{\$} \{0,1\}^\lambda$

$f(x)$

$b \xleftarrow{\$} \{0,1\}$

$f(x) \,\|\, b$

PRGs from OWP

Theorem [Goldreich-Levin'89]:

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \,\|\, \mathsf{hc}(x)\,.$$

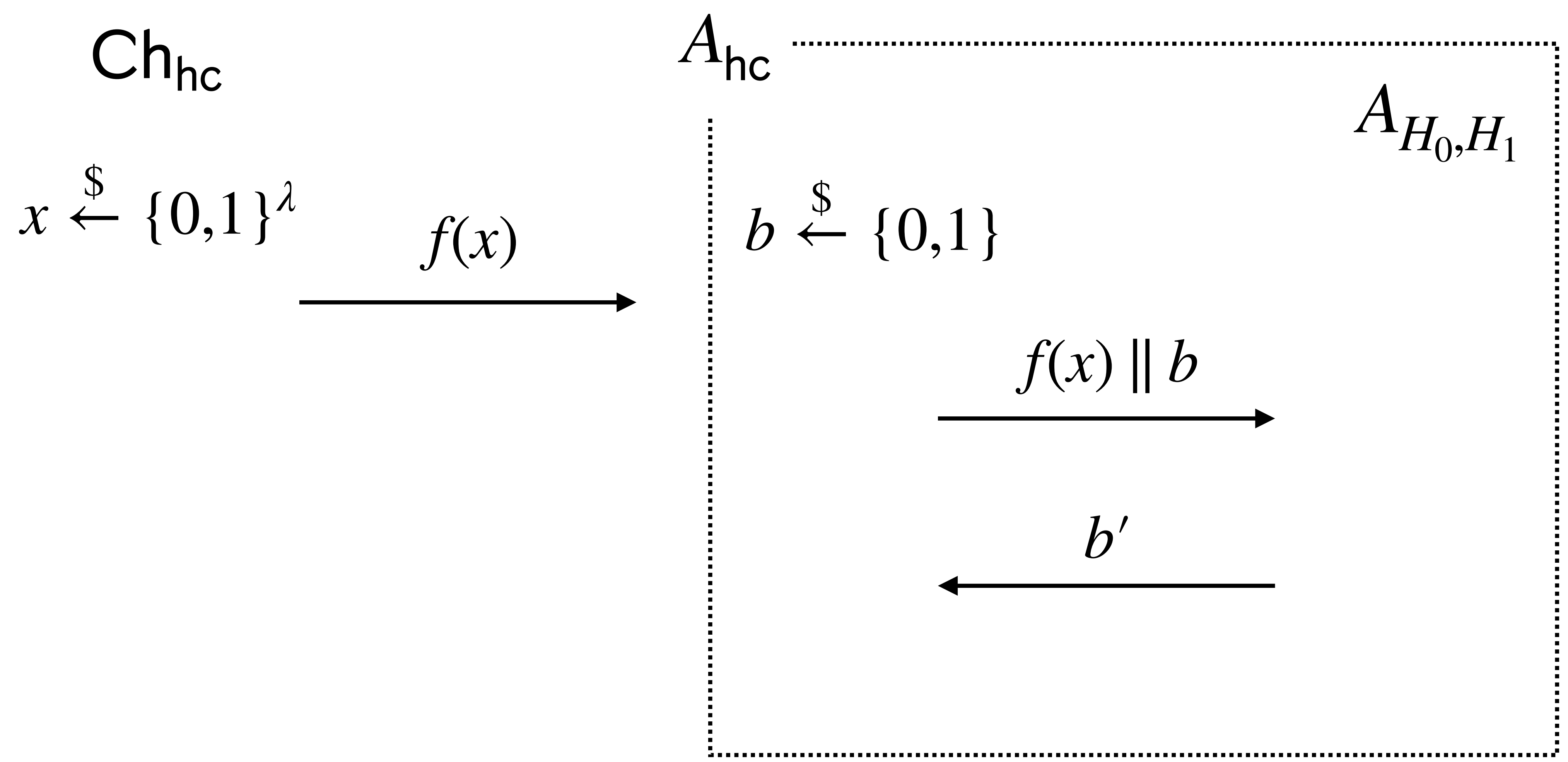
Proof:

We want to show

$$H_0 := \{f(x) \,\|\, \mathsf{hc}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$

$$\overset{c}{\approx}$$

$$H_1 := \{f(x) \,\|\, \overline{\mathsf{hc}}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$



$\mathsf{Ch}_{\mathsf{hc}}$
A_{hc}
A_{H_0,H_1}
$x \xleftarrow{\$} \{0,1\}^\lambda$
$f(x)$
$b \xleftarrow{\$} \{0,1\}$
$f(x) \,\|\, b$
b'

PRGs from OWP

Theorem [Goldreich-Levin’89]:

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \;\|\; \mathsf{hc}(x)\,.$$

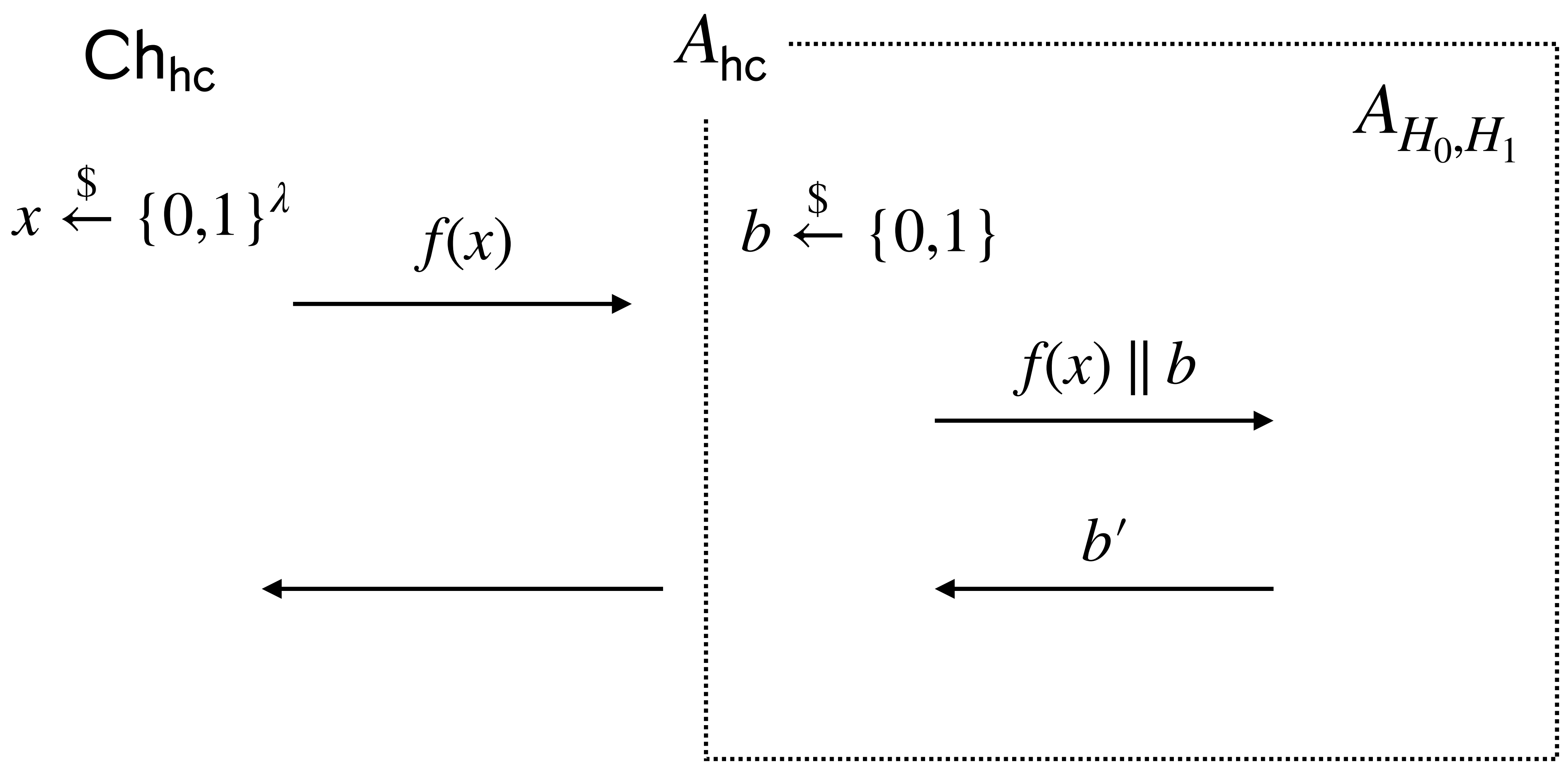
Proof:

We want to show

$$H_0 := \{f(x) \,\|\, \mathsf{hc}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$

$$\overset{c}{\approx}$$

$$H_1 := \{f(x) \,\|\, \overline{\mathsf{hc}}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$


$\mathsf{Ch}_{\mathsf{hc}}$
A_{hc}
A_{H_0,H_1}
$x \xleftarrow{\$} \{0,1\}^\lambda$
$f(x)$
$b \xleftarrow{\$} \{0,1\}$
$f(x) \,\|\, b$
b'

PRGs from OWP

Theorem [Goldreich-Levin’89]:

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \mathbin{\|} \mathsf{hc}(x)\,.$$

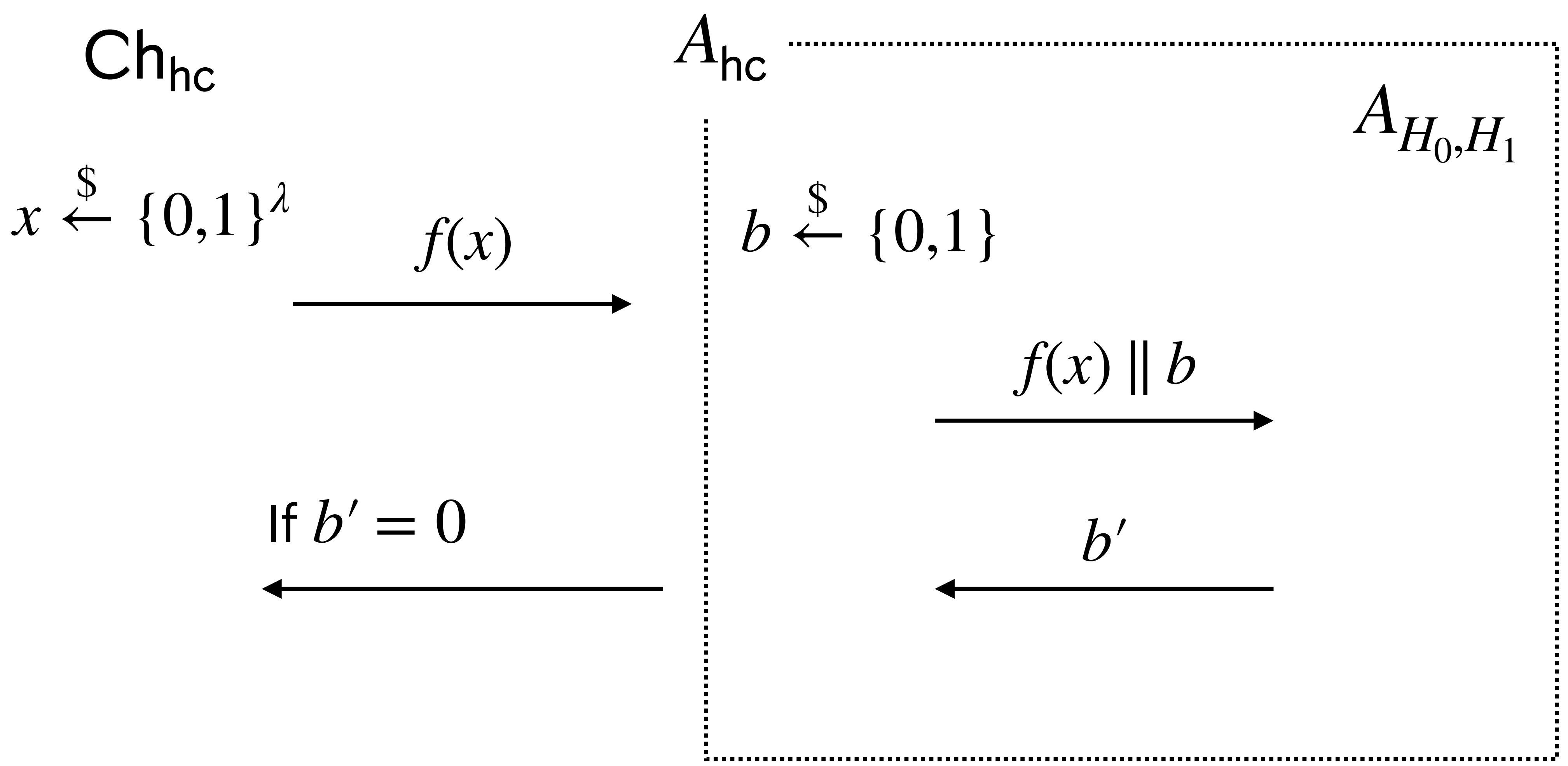
Proof:

We want to show

$$H_0 := \{f(x) \mathbin{\|} \mathsf{hc}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$

$$\overset{c}{\approx}$$

$$H_1 := \{f(x) \mathbin{\|} \overline{\mathsf{hc}}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$



$\mathsf{Ch}_{\mathsf{hc}}$

A_{hc}

A_{H_0,H_1}

$x \xleftarrow{\$} \{0,1\}^\lambda$

$f(x)$

$b \xleftarrow{\$} \{0,1\}$

$f(x) \mathbin{\|} b$

b'

If $b' = 0$

PRGs from OWP

Theorem [Goldreich-Levin'89]:

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \,\|\, \mathsf{hc}(x)\,.$$

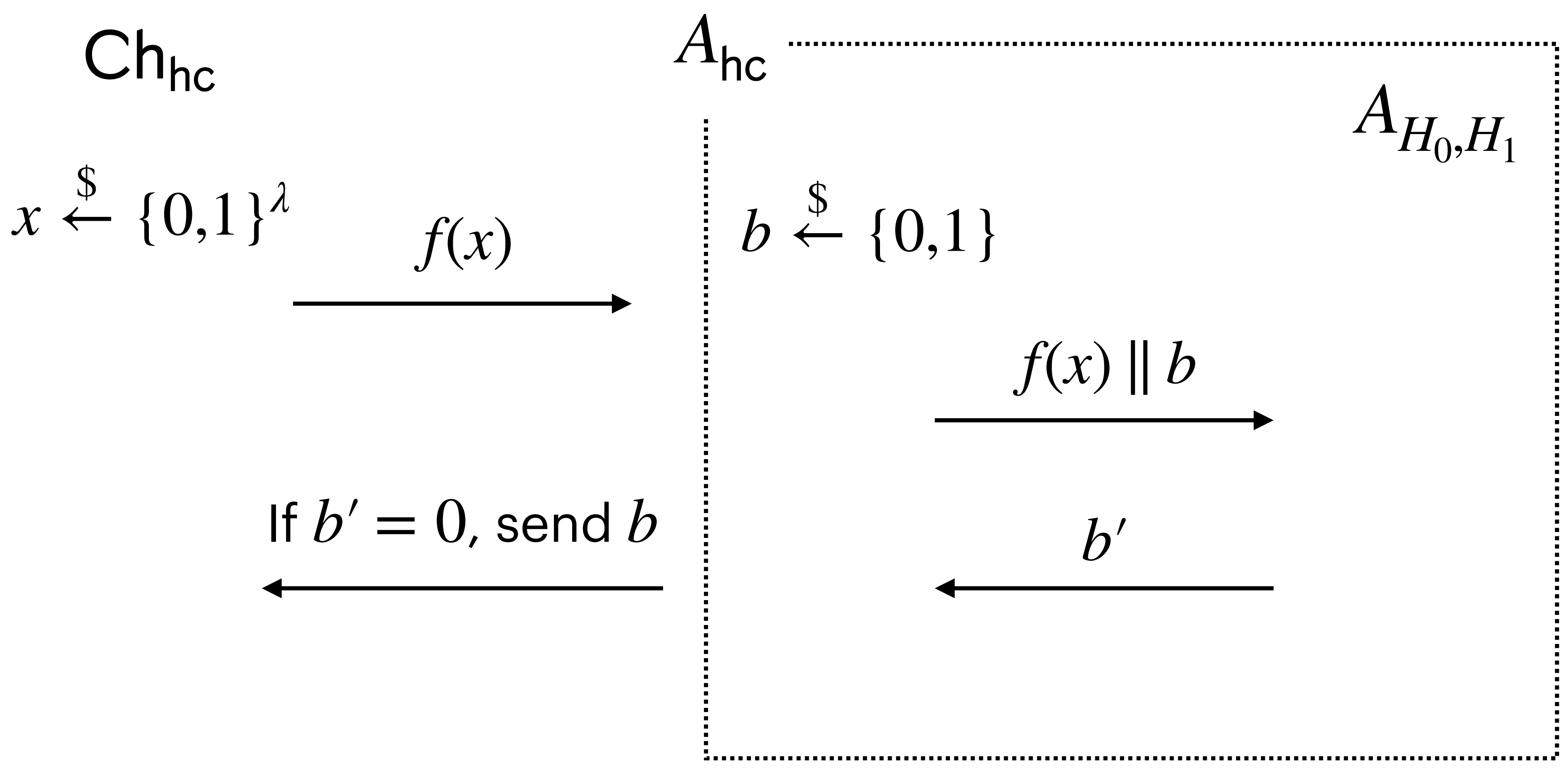
Proof:

We want to show

$$H_0 := \{f(x) \,\|\, \mathsf{hc}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$

$$\overset{c}{\approx}$$

$$H_1 := \{f(x) \,\|\, \overline{\mathsf{hc}}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$



$\mathsf{Ch}_{\mathsf{hc}}$

A_{hc}

A_{H_0,H_1}

$x \xleftarrow{\$} \{0,1\}^\lambda$

$f(x)$

$b \xleftarrow{\$} \{0,1\}$

$f(x) \,\|\, b$

b'

If $b' = 0$, send b

PRGs from OWP

Theorem [Goldreich-Levin'89]:

Given a OWP f and a hard-core predicate hc for f, the following construction G is a PRG

$$G(x) = f(x) \,\|\, \mathsf{hc}(x)\,.$$

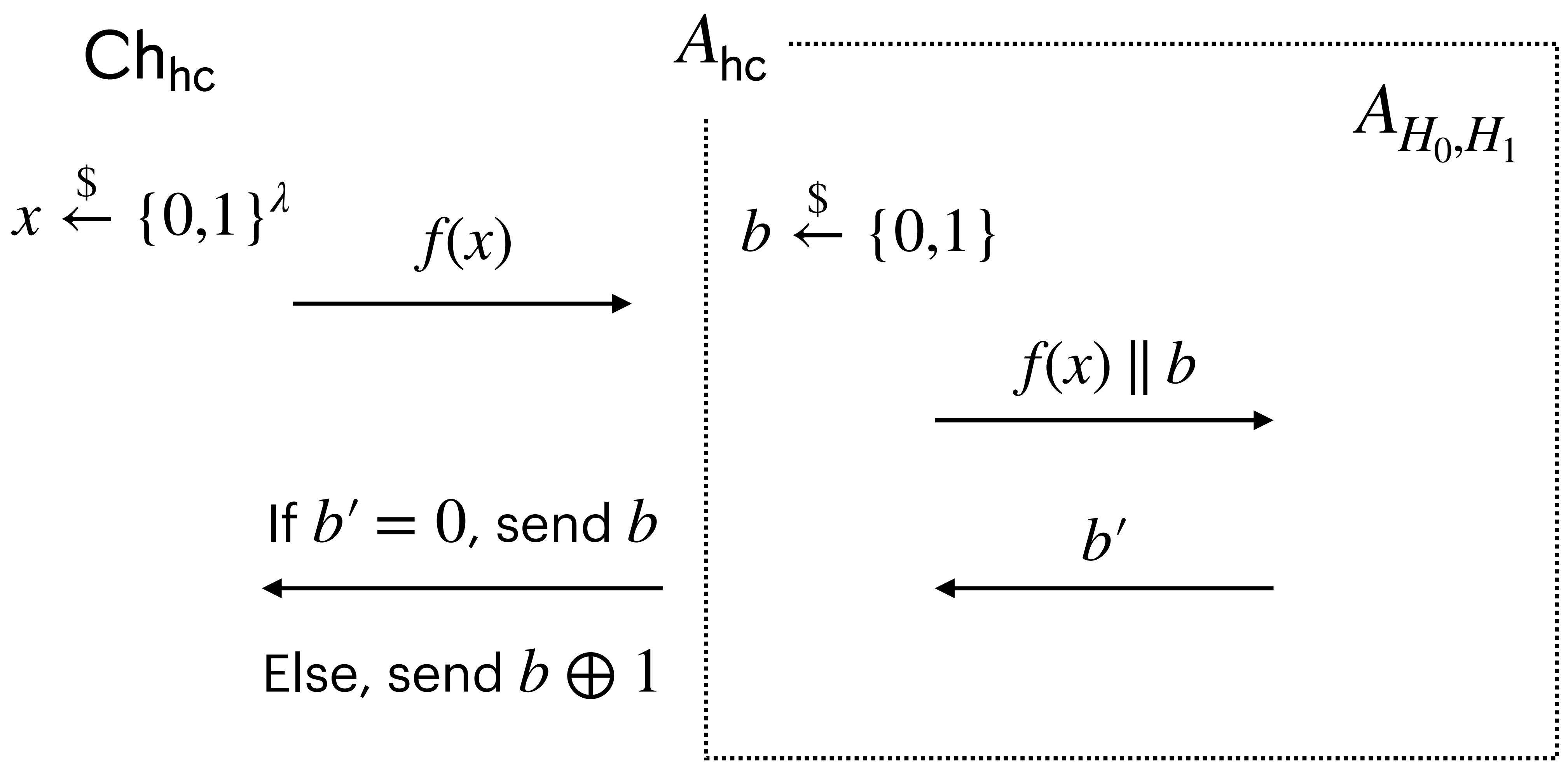
Proof:

We want to show

$$H_0 := \{f(x) \,\|\, \mathsf{hc}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$

$$\overset{c}{\approx}$$

$$H_1 := \{f(x) \,\|\, \overline{\mathsf{hc}}(x) : x \xleftarrow{\$} \{0,1\}^\lambda\}$$



$\mathsf{Ch}_{\mathsf{hc}}$

A_{hc}

A_{H_0,H_1}

$x \xleftarrow{\$} \{0,1\}^\lambda$

$f(x)$

$b \xleftarrow{\$} \{0,1\}$

$f(x) \,\|\, b$

b'

If $b' = 0$, send b

Else, send $b \oplus 1$

Constructing Hard-Core Predicates

- We have shown OWP + Hard-core predicate $\Longrightarrow$ PRG.

Constructing Hard-Core Predicates

- We have shown OWP + Hard-core predicate $\implies$ PRG.

- Our goal was to show that OWP $\implies$ PRG.

Constructing Hard-Core Predicates

- We have shown OWP + Hard-core predicate $\implies$ PRG.
- Our goal was to show that OWP $\implies$ PRG.
  - We need to show that OWP $\implies$ Hard-core predicate for the OWP.

Constructing Hard-Core Predicates

- We have shown OWP + Hard-core predicate $\implies$ PRG.
- Our goal was to show that OWP $\implies$ PRG.
  - We need to show that OWP $\implies$ Hard-core predicate for the OWP.

Theorem [Chor-Goldreich'84]: Under the RSA assumption,

hc(x) := Least-Significant-Bit(x) is a hard-core predicate for the OWP $f_{e,N}(x) := x^e \bmod N$.

Constructing Hard-Core Predicates

- We have shown OWP + Hard-core predicate $\Longrightarrow$ PRG.
- Our goal was to show that OWP $\Longrightarrow$ PRG.
  - We need to show that OWP $\Longrightarrow$ Hard-core predicate for the OWP.

Theorem [Chor-Goldreich'84]: Under the RSA assumption,

hc(x) := Least-Significant-Bit(x) is a hard-core predicate for the OWP $f_{e,N}(x) := x^e \bmod N$.

Theorem [Blum-Micali'84]: Under the Discrete logarithm assumption,

hc$(x) := x < p/2$ is a hard-core predicate for the OWP $f_{G,p,g}(x) := g^x$.

Constructing Hard-Core Predicates

What makes this challenging?

- We have shown OWP + Hard-core predicate $\Longrightarrow$ PRG.
- Our goal was to show that OWP $\Longrightarrow$ PRG.
  - We need to show that OWP $\Longrightarrow$ Hard-core predicate for the OWP.

Theorem [Chor-Goldreich'84]: Under the RSA assumption,

hc(x) := Least-Significant-Bit(x) is a hard-core predicate for the OWP $f_{e,N}(x) := x^e \bmod N$.

Theorem [Blum-Micali'84]: Under the Discrete logarithm assumption,

hc$(x) := x < p/2$ is a hard-core predicate for the OWP $f_{G,p,g}(x) := g^x$.

Constructing Hard-Core Predicates

What makes this challenging?

The reduction adversary must **compute the inverse** $x \in \{0,1\}^{\lambda}$, using an adversary that **guesses the hard-core bit** hc$(x) \in \{0,1\}$.

- We have shown OWP + Hard-core predicate $\Longrightarrow$ PRG.
- Our goal was to show that OWP $\Longrightarrow$ PRG.
  - We need to show that OWP $\Longrightarrow$ Hard-core predicate for the OWP.

Theorem [Chor-Goldreich'84]: Under the RSA assumption,

hc(x) := Least-Significant-Bit(x) is a hard-core predicate for the OWP $f_{e,N}(x) := x^e \bmod N$.

Theorem [Blum-Micali'84]: Under the Discrete logarithm assumption,

hc$(x) := x < p/2$ is a hard-core predicate for the OWP $f_{G,p,g}(x) := g^x$.

Constructing Hard-Core Predicates

- We have shown OWP + Hard-core predicate $\Longrightarrow$ PRG.
- Our goal was to show that OWP $\Longrightarrow$ PRG.
  - We need to show that OWP $\Longrightarrow$ Hard-core predicate for the OWP.

What makes this challenging?

The reduction adversary must **compute the inverse** $x \in \{0,1\}^{\lambda}$, using an adversary that **guesses the hard-core bit** $\mathsf{hc}(x) \in \{0,1\}$.

Can we construct a hard-core bit for any OWF?

Theorem [Chor-Goldreich'84]: Under the RSA assumption,

hc(x) := Least-Significant-Bit(x) is a hard-core predicate for the OWP $f_{e,N}(x) := x^e \bmod N$.

Theorem [Blum-Micali'84]: Under the Discrete logarithm assumption,

hc$(x) := x < p/2$ is a hard-core predicate for the OWP $f_{G,p,g}(x) := g^x$.

Constructing Hard-Core Predicates

Goal: For all OWFs $f,$ there exists a hard-core predicate **hc** for f.

Constructing Hard-Core Predicates

Goal: For all OWFs f, there exists a hard-core predicate hc for f.

Open problem!

Constructing Hard-Core Predicates

Goal: For all OWFs f, there exists a hard-core predicate **hc** for f.

Open problem!

Theorem [Goldreich-Levin'89]:

If f is a OWF, then there exists a OWF g and a hard-core predicate **hc** for g.

Constructing Hard-Core Predicates

Goal: For all OWFs f, there exists a hard-core predicate **hc** for f.

Open problem!

Theorem [Goldreich-Levin'89]**:**

If f is a OWF, then there exists a OWF g and a hard-core predicate **hc** for g.

One of the most influential results in computer science, with applications to cryptography, learning theory, coding theory, and more.

Goldreich-Levin Theorem

Theorem [Goldreich-Levin'89]**:** If f is a OWF, then there exists a OWF g and a hard-core predicate hc for g.

$$g(x \,\|\, r) := f(x) \,\|\, r \qquad \mathsf{hc}(x \,\|\, r) := \langle x, r \rangle = \sum_i x_i \cdot r_i$$

Goldreich-Levin Theorem

Theorem [Goldreich-Levin'89]**:** If f is a OWF, then there exists a OWF g and a hard-core predicate **hc** for g.

$$g(x \,\|\, r) := f(x) \,\|\, r \qquad\qquad \mathsf{hc}(x \,\|\, r) := \langle x, r \rangle = \sum_i x_i \cdot r_i$$

Intuition:

Goldreich-Levin Theorem

Theorem [Goldreich-Levin'89]**:** If f is a OWF, then there exists a OWF g and a hard-core predicate **hc** for g.

$$g(x \parallel r) := f(x) \parallel r$$

$$\mathsf{hc}(x \parallel r) := \langle x, r \rangle = \sum_i x_i \cdot r_i$$

Intuition: g is a OWF.

Goldreich-Levin Theorem

Theorem [Goldreich-Levin'89]**:** If f is a OWF, then there exists a OWF g and a hard-core predicate **hc** for g.

$$g(x \parallel r) := f(x) \parallel r \qquad \mathsf{hc}(x \parallel r) := \langle x, r \rangle = \sum_i x_i \cdot r_i$$

Intuition: g is a OWF. We will use proof by contradiction to show that hc is a hard-core predicate.

Goldreich-Levin Theorem

Theorem [Goldreich-Levin'89]**:** If f is a OWF, then there exists a OWF g and a hard-core predicate **hc** for g.

$$g(x \,\|\, r) := f(x) \,\|\, r \qquad\qquad \mathsf{hc}(x \,\|\, r) := \langle x, r \rangle = \sum_i x_i \cdot r_i$$

Intuition: g is a OWF. We will use proof by contradiction to show that **hc** is a hard-core predicate.

Assume we have a perfect predictor A for the hardcore bit.

$$\Pr_{x,r \xleftarrow{\$} \{0,1\}} \left[A\left(f(x) \,\|\, r \right) = \mathsf{hc}(x \,\|\, r) \right] = 1$$

Goldreich-Levin Theorem

Theorem [Goldreich-Levin'89]: If f is a OWF, then there exists a OWF g and a hard-core predicate **hc** for g.

$$g(x \,\|\, r) := f(x) \,\|\, r \qquad \mathsf{hc}(x \,\|\, r) := \langle x, r \rangle = \sum_i x_i \cdot r_i$$

Intuition: g is a OWF. We will use proof by contradiction to show that hc is a hard-core predicate.

Assume we have a perfect predictor A for the hardcore bit.

$$\Pr_{x,r \xleftarrow{\$} \{0,1\}} \left[A\left(f(x) \,\|\, r\right) = \mathsf{hc}(x \,\|\, r) \right] = 1$$

$\forall x, r \in \{0,1\}^\lambda, A\left(f(x) \,\|\, r\right) = \mathsf{hc}(x \,\|\, r)$

Goldreich-Levin Theorem

Theorem [Goldreich-Levin'89]**:** If f is a OWF, then there exists a OWF g and a hard-core predicate **hc** for g.

$$g(x \,\|\, r) := f(x) \,\|\, r \qquad\qquad \mathsf{hc}(x \,\|\, r) := \langle x, r \rangle = \sum_i x_i \cdot r_i$$

Intuition: g is a OWF. We will use proof by contradiction to show that **hc** is a hard-core predicate.

Assume we have a perfect predictor A for the hardcore bit.

$$\Pr_{x,r \overset{\$}{\leftarrow} \{0,1\}} \left[A\left(f(x) \,\|\, r\right) = \mathsf{hc}(x \,\|\, r) \right] = 1$$

$\forall x, r \in \{0,1\}^\lambda, A\left(f(x) \,\|\, r\right) = \mathsf{hc}(x \,\|\, r)$

Invert $f(x)$:

Goldreich-Levin Theorem

Theorem [Goldreich-Levin'89]: If f is a OWF, then there exists a OWF g and a hard-core predicate **hc** for g.

$$g(x \| r) := f(x) \| r \qquad\qquad \text{hc}(x \| r) := \langle x, r \rangle = \sum_i x_i \cdot r_i$$

Intuition: g is a OWF. We will use proof by contradiction to show that **hc** is a hard-core predicate.

Assume we have a perfect predictor A for the hardcore bit.

$$\Pr_{x,r \xleftarrow{\$} \{0,1\}} \left[A \left(f(x) \| r \right) = \text{hc}(x \| r) \right] = 1$$

$\forall x, r \in \{0,1\}^\lambda, A \left(f(x) \| r \right) = \text{hc}(x \| r)$

Invert $f(x)$**:**

$e_i := 0^{i-1} \| 1 \| 0^{\lambda - i}$

Given $y = f(x)$, compute

$$A(y \| e_1) = x_1 \qquad A(y \| e_2) = x_2 \qquad \cdots \qquad A(y \| e_\lambda) = x_\lambda$$

Goldreich-Levin Theorem

Theorem [Goldreich-Levin'89]**:** If f is a OWF, then there exists a OWF g and a hard-core predicate **hc** for g.

$$g(x \parallel r) := f(x) \parallel r \qquad \mathsf{hc}(x \parallel r) := \langle x, r \rangle = \sum_i x_i \cdot r_i$$

Intuition: g is a OWF. We will use proof by contradiction to show that **hc** is a hard-core predicate.

Goldreich-Levin Theorem

Theorem [Goldreich-Levin'89]: If f is a OWF, then there exists a OWF g and a hard-core predicate **hc** for g.

$$g(x \,\|\, r) := f(x) \,\|\, r \qquad \mathsf{hc}(x \,\|\, r) := \langle x, r \rangle = \sum_i x_i \cdot r_i$$

Intuition: g is a OWF. We will use proof by contradiction to show that **hc** is a hard-core predicate.

$$\Pr_{x,r \xleftarrow{\$} \{0,1\}} \left[A\left(f(x) \,\|\, r \right) = \mathsf{hc}(x \,\|\, r) \right] = \frac{3}{4} + \epsilon$$

Goldreich-Levin Theorem

Theorem [Goldreich-Levin'89]: If f is a OWF, then there exists a OWF g and a hard-core predicate **hc** for g.

$$g(x \| r) := f(x) \| r \qquad \mathsf{hc}(x \| r) := \langle x, r \rangle = \sum_i x_i \cdot r_i$$

Intuition: g is a OWF. We will use proof by contradiction to show that **hc** is a hard-core predicate.

$$\Pr_{x,r \xleftarrow{\$} \{0,1\}} \left[A\left(f(x) \| r\right) = \mathsf{hc}(x \| r) \right] = \frac{3}{4} + \epsilon$$

A might be completely useless for certain x.

Goldreich-Levin Theorem

Theorem [Goldreich-Levin'89]: If f is a OWF, then there exists a OWF g and a hard-core predicate **hc** for g.

$$g(x \,\|\, r) := f(x) \,\|\, r \qquad \mathsf{hc}(x \,\|\, r) := \langle x, r \rangle = \sum_i x_i \cdot r_i$$

Intuition: g is a OWF. We will use proof by contradiction to show that **hc** is a hard-core predicate.

$$\Pr_{x,r \xleftarrow{\$} \{0,1\}}\left[A\left(f(x) \,\|\, r\right) = \mathsf{hc}(x \,\|\, r)\right] = \frac{3}{4} + \epsilon$$

A might be completely useless for certain x.

But we can show that A must succeed with probability at least $3/4 + \epsilon/2$ for at least $\epsilon/2$ fraction of inputs x.

Goldreich-Levin Theorem

Theorem [Goldreich-Levin'89]: If f is a OWF, then there exists a OWF g and a hard-core predicate **hc** for g.

$$g(x \,\|\, r) := f(x) \,\|\, r \qquad\qquad \mathsf{hc}(x \,\|\, r) := \langle x, r \rangle = \sum_i x_i \cdot r_i$$

Intuition: g is a OWF. We will use proof by contradiction to show that **hc** is a hard-core predicate.

$$\Pr_{x,r \overset{\$}{\leftarrow} \{0,1\}} \left[A\left(f(x) \,\|\, r\right) = \mathsf{hc}(x \,\|\, r) \right] = \frac{3}{4} + \epsilon$$

A might be completely useless for certain x.

But we can show that A must succeed with probability at least $3/4 + \epsilon/2$ for at least $\epsilon/2$ fraction of inputs x.

Invert $f(x)$**:**

Goldreich-Levin Theorem

Theorem [Goldreich-Levin'89]: If f is a OWF, then there exists a OWF g and a hard-core predicate **hc** for g.

$$g(x \| r) := f(x) \| r \qquad \mathsf{hc}(x \| r) := \langle x, r \rangle = \sum_i x_i \cdot r_i$$

Intuition: g is a OWF. We will use proof by contradiction to show that **hc** is a hard-core predicate.

$$\Pr_{x,r \xleftarrow{\$} \{0,1\}} \left[A\left(f(x) \| r\right) = \mathsf{hc}(x \| r) \right] = \frac{3}{4} + \epsilon$$

A might be completely useless for certain x.

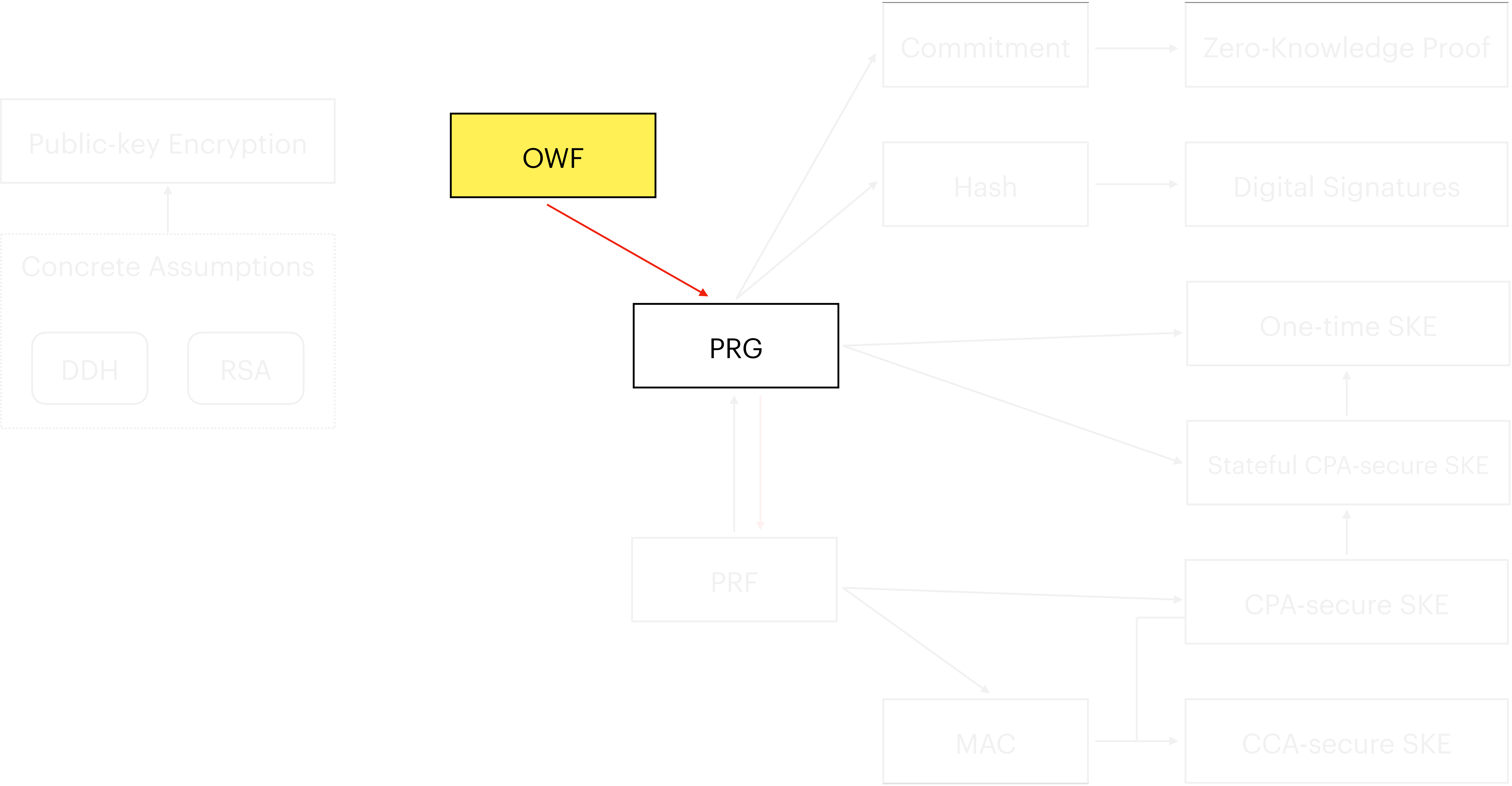
But we can show that A must succeed with probability at least $3/4 + \epsilon/2$ for at least $\epsilon/2$ fraction of inputs x.

Invert $f(x)$:

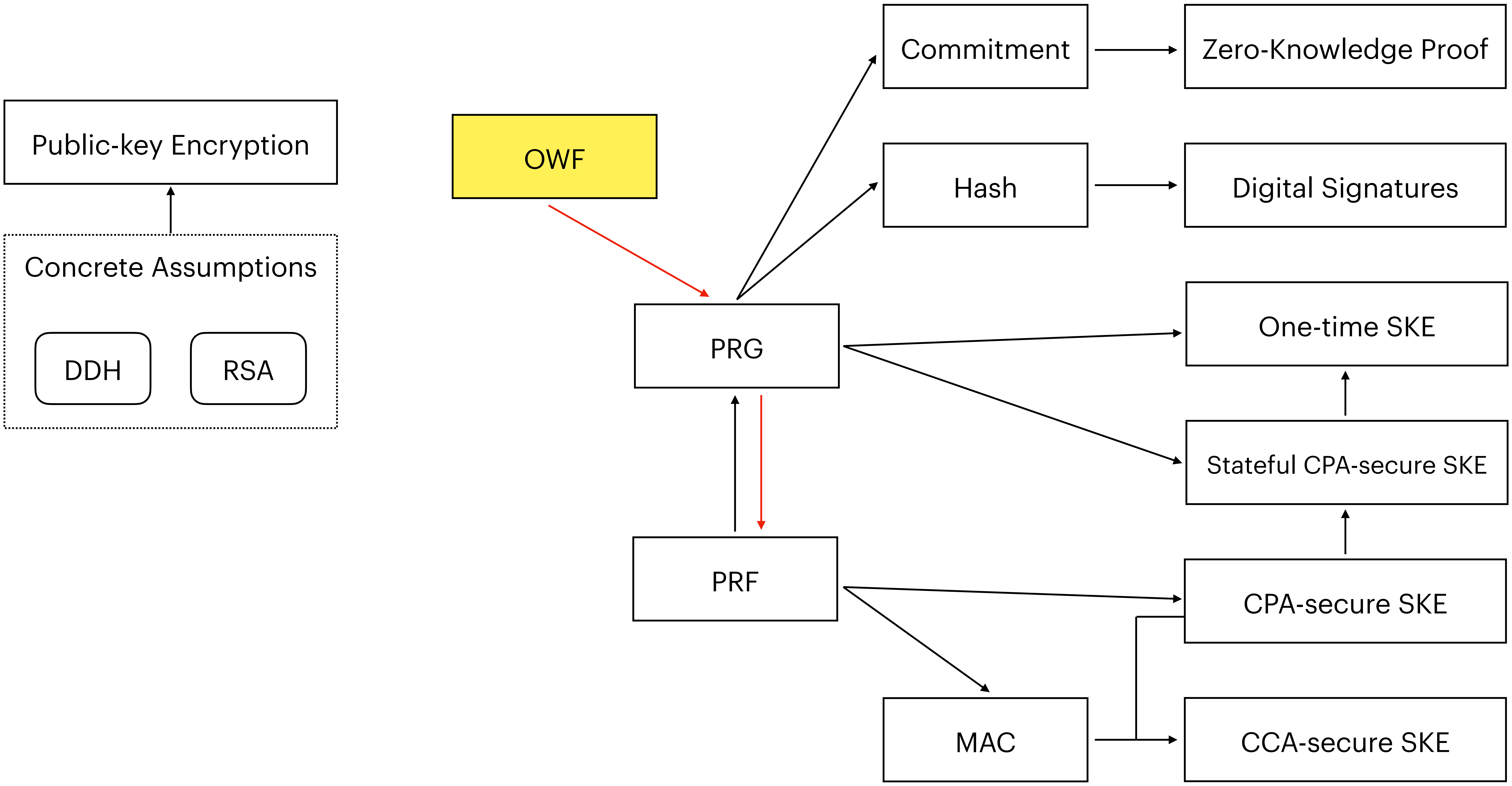
Given $y = f(x)$, sample $r \leftarrow \{0,1\}^\lambda$ and compute

$$A(y \| r) := b_1 \qquad A(y \| r \oplus e_i) := b_2 \qquad x_i := b_1 \oplus b_2$$

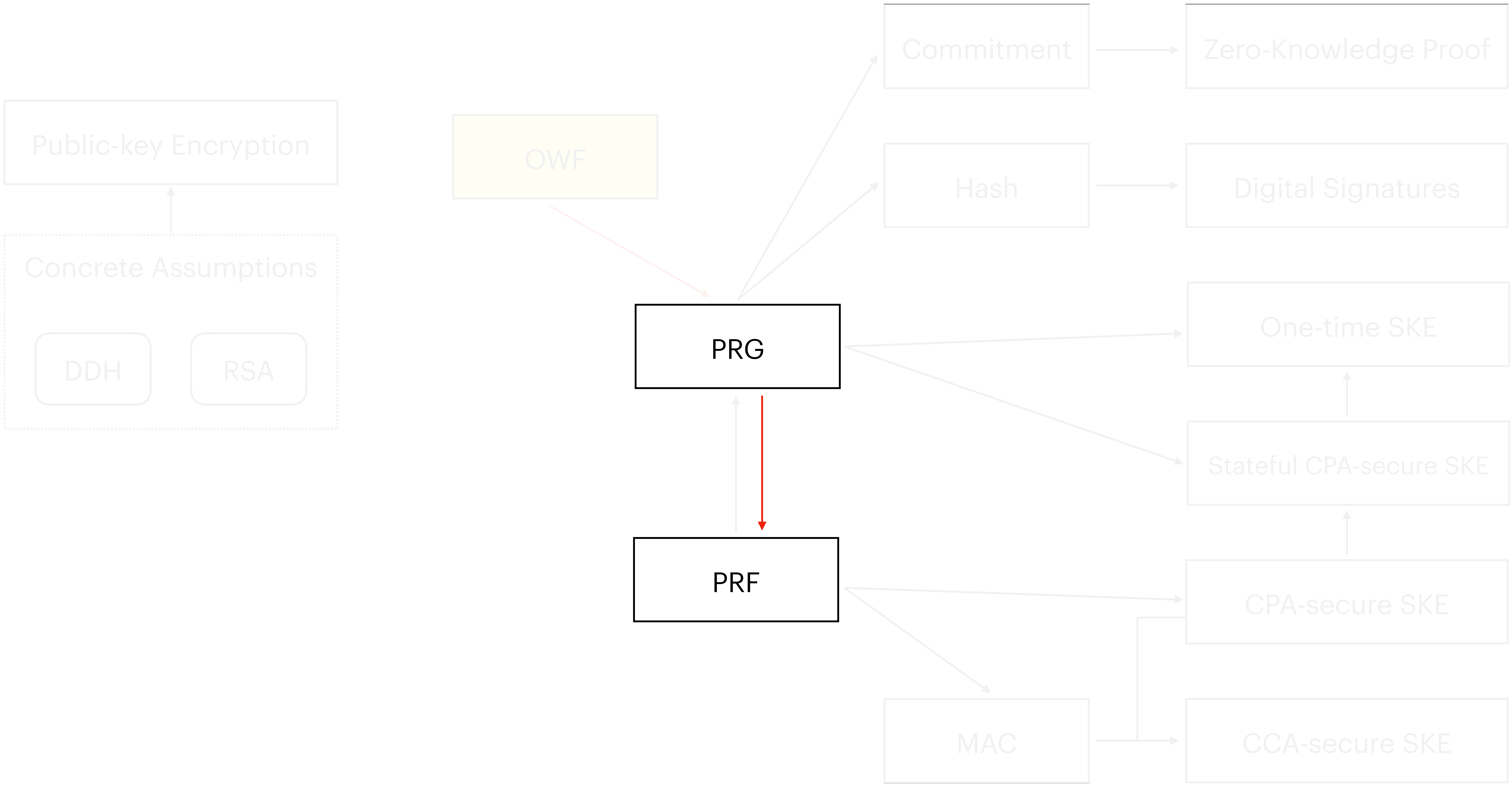
The Cryptography Landscape



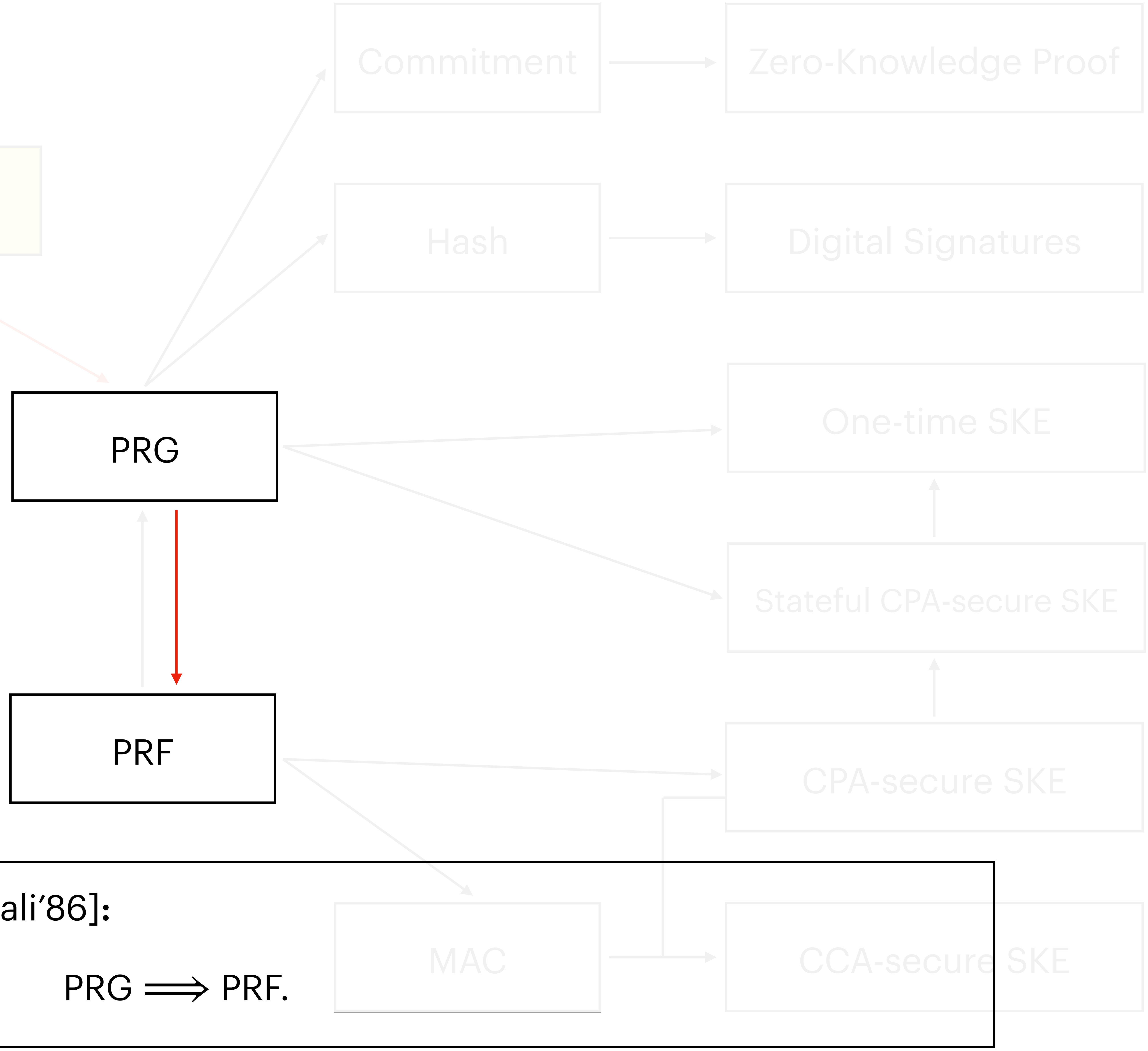
The Cryptography Landscape



The Cryptography Landscape



The Cryptography Landscape



Theorem [Goldreich-Goldwasser-Micali'86]**:**

$$\text{PRG} \Longrightarrow \text{PRF}.$$

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ be a length-doubling PRG.

- How to construct $F_k : \{0,1\} \to \{0,1\}^\lambda$?

Constructing PRFs from PRGs: Warmup

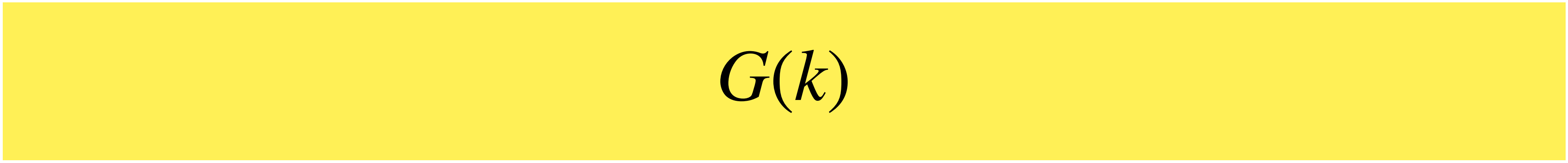
- Let $G : \{0,1\}^{\lambda} \to \{0,1\}^{2\lambda}$ be a length-doubling PRG.
- How to construct $F_k : \{0,1\} \to \{0,1\}^{\lambda}$?

$$G(k)$$

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ be a length-doubling PRG.

- How to construct $F_k : \{0,1\} \to \{0,1\}^\lambda$?

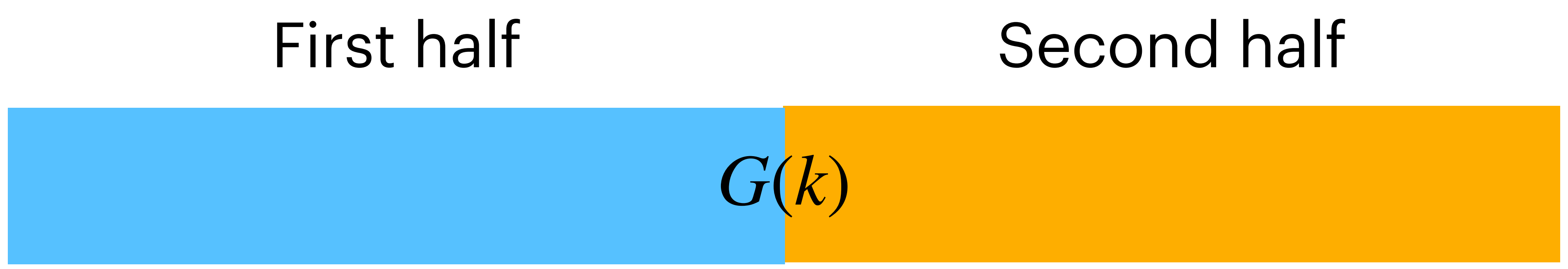


$G(k)$

Given $x \in \{0,1\}$,
how to evaluate F_k?

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^{\lambda} \to \{0,1\}^{2\lambda}$ be a length-doubling PRG.
- How to construct $F_k : \{0,1\} \to \{0,1\}^{\lambda}$?



First half

Second half

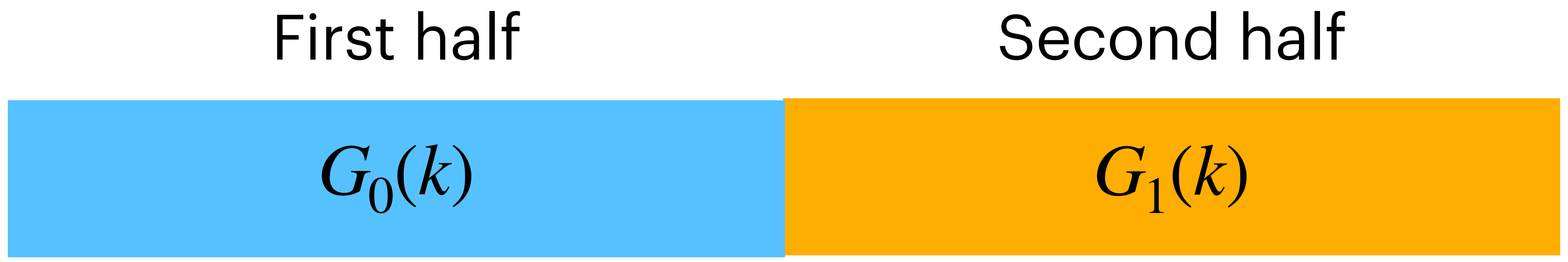
$G(k)$

Given $x \in \{0,1\}$,
how to evaluate F_k?

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^{\lambda} \to \{0,1\}^{2\lambda}$ be a length-doubling PRG.
- How to construct $F_k : \{0,1\} \to \{0,1\}^{\lambda}$?

$G(k) = G_0(k) \,\|\, G_1(k)$



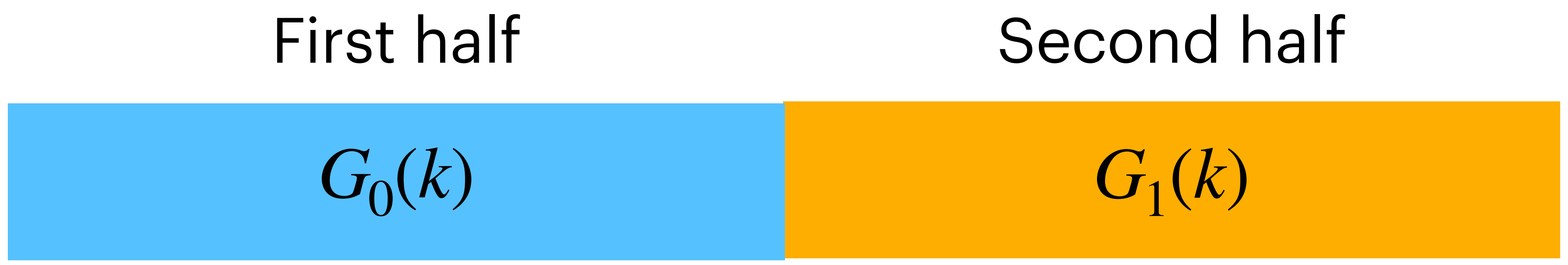
Given $x \in \{0,1\}$,
how to evaluate F_k?

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ be a length-doubling PRG.

- How to construct $F_k : \{0,1\} \to \{0,1\}^\lambda$?

$G(k) = G_0(k) \,\|\, G_1(k)$



Given $x \in \{0,1\}$,
how to evaluate F_k?

Output $G_x(k)$!

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^{\lambda} \to \{0,1\}^{2\lambda}$ be a length-doubling PRG.
- How to construct $F_k : \{0,1\} \to \{0,1\}^{\lambda}$?

$$G(k) = G_0(k) \,\|\, G_1(k)$$

x	$F_k(x)$
0	$G_0(k)$
1	$G_1(k)$

Given $x \in \{0,1\}$,
how to evaluate F_k?

Output $G_x(k)$!

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^{\lambda} \to \{0,1\}^{2\lambda}$ be a length-doubling PRG.
- How to construct $F_k : \{0,1\} \to \{0,1\}^{\lambda}$?

$$G(k) = G_0(k) \,\|\, G_1(k)$$

x	$F_k(x)$
0	$G_0(k)$
1	$G_1(k)$

How to extend this idea to $F_k : \{0,1\}^{\lambda} \to \{0,1\}^{\lambda}$?

Given $x \in \{0,1\}$,
how to evaluate F_k?

Output $G_x(k)$!

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^\lambda \rightarrow \{0,1\}^{2\lambda}$ be a length-doubling PRG.
- How to construct $F_k : \{0,1\} \rightarrow \{0,1\}^\lambda$?

$G(k) = G_0(k) \parallel G_1(k)$

x	$F_k(x)$
0	$G_0(k)$
1	$G_1(k)$

How to extend this idea to $F_k : \{0,1\}^\lambda \rightarrow \{0,1\}^\lambda$?

F_k's truth table has 2^λ rows while $G(k)$ outputs a 2λ-bit string!

Given $x \in \{0,1\}$, how to evaluate F_k?

Output $G_x(k)$!

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^{\lambda} \to \{0,1\}^{2\lambda}$ be a length-doubling PRG.
- How to construct $F_k : \{0,1\} \to \{0,1\}^{\lambda}$?

$$G(k) = G_0(k) \,\|\, G_1(k)$$

x	$F_k(x)$
0	$G_0(k)$
1	$G_1(k)$

How to extend this idea to $F_k : \{0,1\}^{\lambda} \to \{0,1\}^{\lambda}$?

F_k's truth table has 2^{λ} rows while $G(k)$ outputs a 2λ-bit string!

Given $x \in \{0,1\}$, how to evaluate F_k?

Output $G_x(k)$!

Can we extend $F'_k : \{0,1\}^{i} \to \{0,1\}^{\lambda}$ to $F_k : \{0,1\}^{i+1} \to \{0,1\}^{\lambda}$?

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^{\lambda} \rightarrow \{0,1\}^{2\lambda}$ be a PRG and $F'_k : \{0,1\}^{i} \rightarrow \{0,1\}^{\lambda}$ be a PRF.
- How to construct $F_k : \{0,1\}^{i+1} \rightarrow \{0,1\}^{\lambda}$?

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^{\lambda} \rightarrow \{0,1\}^{2\lambda}$ be a PRG and $F'_k : \{0,1\}^{i} \rightarrow \{0,1\}^{\lambda}$ be a PRF.
- How to construct $F_k : \{0,1\}^{i+1} \rightarrow \{0,1\}^{\lambda}$?

Given $x \in \{0,1\}^{i+1}$, let $x = x' \,||\, b$ where $x' \in \{0,1\}^{i}$.

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^{\lambda} \to \{0,1\}^{2\lambda}$ be a PRG and $F'_k : \{0,1\}^{i} \to \{0,1\}^{\lambda}$ be a PRF.
- How to construct $F_k : \{0,1\}^{i+1} \to \{0,1\}^{\lambda}$?

Given $x \in \{0,1\}^{i+1}$, let $x = x' \,||\, b$ where $x' \in \{0,1\}^{i}$.

$F'_k(x')$

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^{\lambda} \to \{0,1\}^{2\lambda}$ be a PRG and $F'_k : \{0,1\}^{i} \to \{0,1\}^{\lambda}$ be a PRF.
- How to construct $F_k : \{0,1\}^{i+1} \to \{0,1\}^{\lambda}$?

Given $x \in \{0,1\}^{i+1}$, let $x = x' \,\|\, b$ where $x' \in \{0,1\}^{i}$.

$$G\left(\boxed{F'_k(x')} \right)$$

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ be a PRG and $F'_k : \{0,1\}^i \to \{0,1\}^\lambda$ be a PRF.
- How to construct $F_k : \{0,1\}^{i+1} \to \{0,1\}^\lambda$?

Given $x \in \{0,1\}^{i+1}$, let $x = x' \,||\, b$ where $x' \in \{0,1\}^i$.

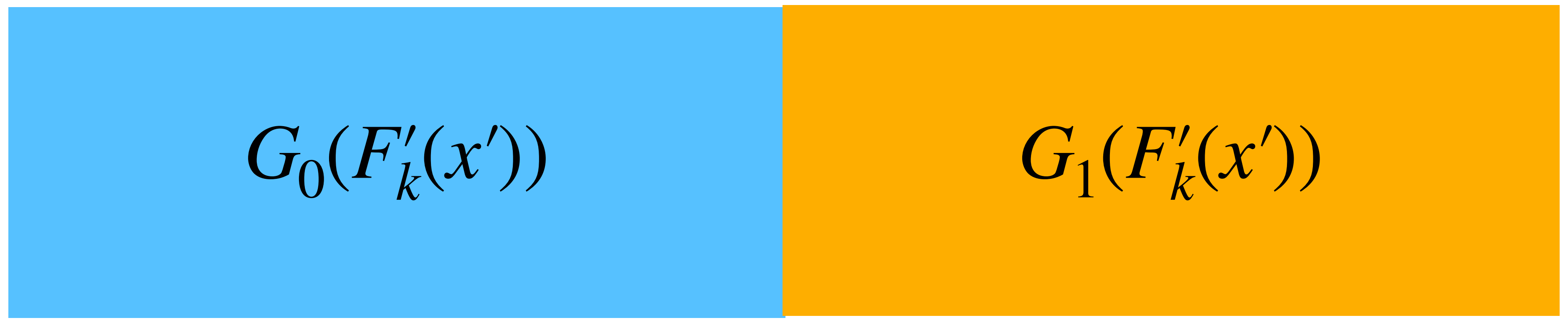
$$G\left(\quad F'_k(x') \quad \right)$$

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^{\lambda} \rightarrow \{0,1\}^{2\lambda}$ be a PRG and $F'_k : \{0,1\}^{i} \rightarrow \{0,1\}^{\lambda}$ be a PRF.
- How to construct $F_k : \{0,1\}^{i+1} \rightarrow \{0,1\}^{\lambda}$?

Given $x \in \{0,1\}^{i+1}$, let $x = x' \,||\, b$ where $x' \in \{0,1\}^{i}$.

$G(k) = G_0(k) \,||\, G_1(k)$



$G_0(F'_k(x'))$

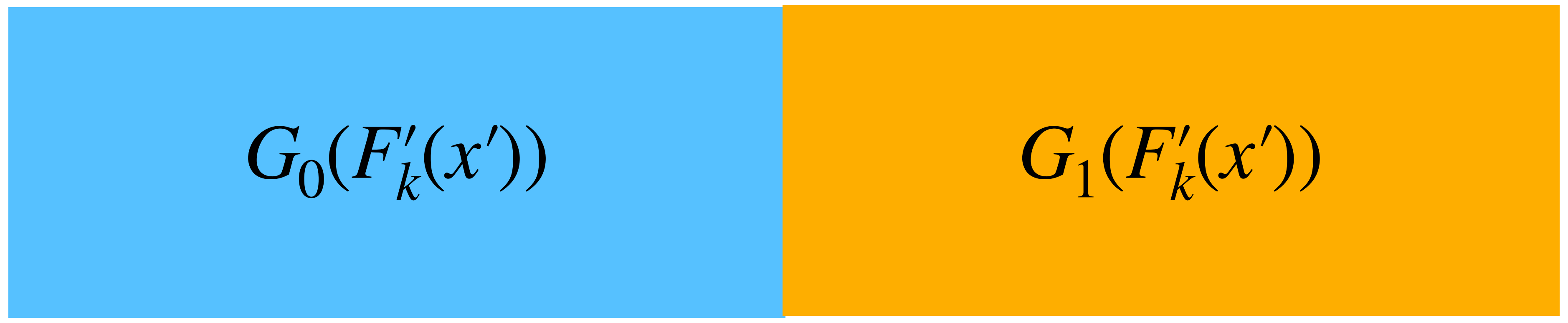
$G_1(F'_k(x'))$

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^{\lambda} \to \{0,1\}^{2\lambda}$ be a PRG and $F'_k : \{0,1\}^{i} \to \{0,1\}^{\lambda}$ be a PRF.
- How to construct $F_k : \{0,1\}^{i+1} \to \{0,1\}^{\lambda}$?

Given $x \in \{0,1\}^{i+1}$, let $x = x' \,||\, b$ where $x' \in \{0,1\}^{i}$.

$G(k) = G_0(k) \,||\, G_1(k)$



Output $F_k(x) := G_b(F'_k(x'))$!

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ be a PRG and $F'_k : \{0,1\}^i \to \{0,1\}^\lambda$ be a PRF.
- How to construct $F_k : \{0,1\}^{i+1} \to \{0,1\}^\lambda$?

Given $x \in \{0,1\}^{i+1}$, let $x = x' \,\|\, b$ where $x' \in \{0,1\}^i$.

$G(k) = G_0(k) \,\|\, G_1(k)$

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ be a PRG and $F'_k : \{0,1\}^i \to \{0,1\}^\lambda$ be a PRF.
- How to construct $F_k : \{0,1\}^{i+1} \to \{0,1\}^\lambda$?

Given $x \in \{0,1\}^{i+1}$, let $x = x' \,||\, b$ where $x' \in \{0,1\}^i$.

$G(k) = G_0(k) \,||\, G_1(k)$

$$x' = 0^i$$

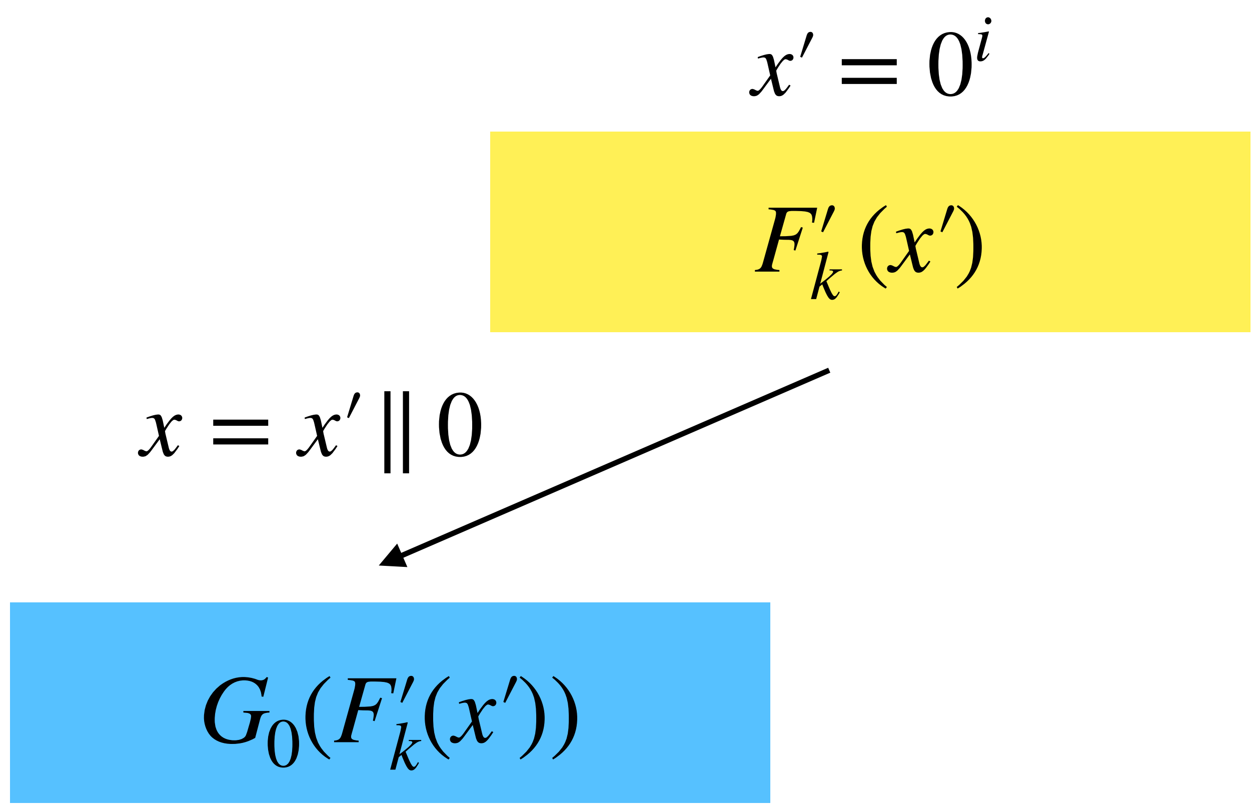
$$\boxed{F'_k(x')}$$

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^{\lambda} \rightarrow \{0,1\}^{2\lambda}$ be a PRG and $F'_k : \{0,1\}^{i} \rightarrow \{0,1\}^{\lambda}$ be a PRF.
- How to construct $F_k : \{0,1\}^{i+1} \rightarrow \{0,1\}^{\lambda}$?

Given $x \in \{0,1\}^{i+1}$, let $x = x' \,\|\, b$ where $x' \in \{0,1\}^{i}$.

$G(k) = G_0(k) \,\|\, G_1(k)$



$x' = 0^i$

$F'_k(x')$

$x = x' \,\|\, 0$

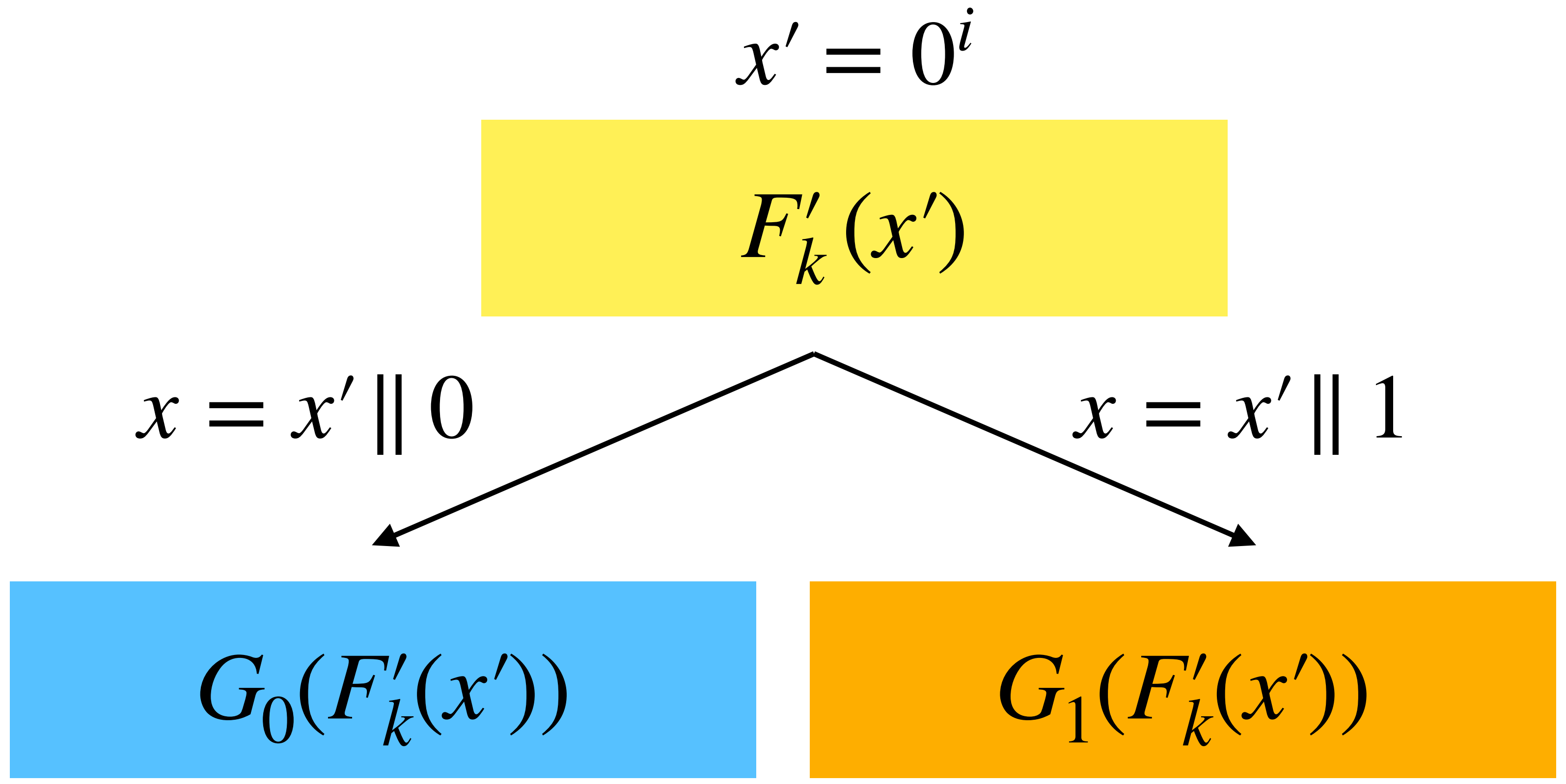
$G_0(F'_k(x'))$

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ be a PRG and $F'_k : \{0,1\}^i \to \{0,1\}^\lambda$ be a PRF.
- How to construct $F_k : \{0,1\}^{i+1} \to \{0,1\}^\lambda$?

Given $x \in \{0,1\}^{i+1}$, let $x = x' \| b$ where $x' \in \{0,1\}^i$.

$G(k) = G_0(k) \| G_1(k)$



$x' = 0^i$

$F'_k(x')$

$x = x' \| 0$

$x = x' \| 1$

$G_0(F'_k(x'))$

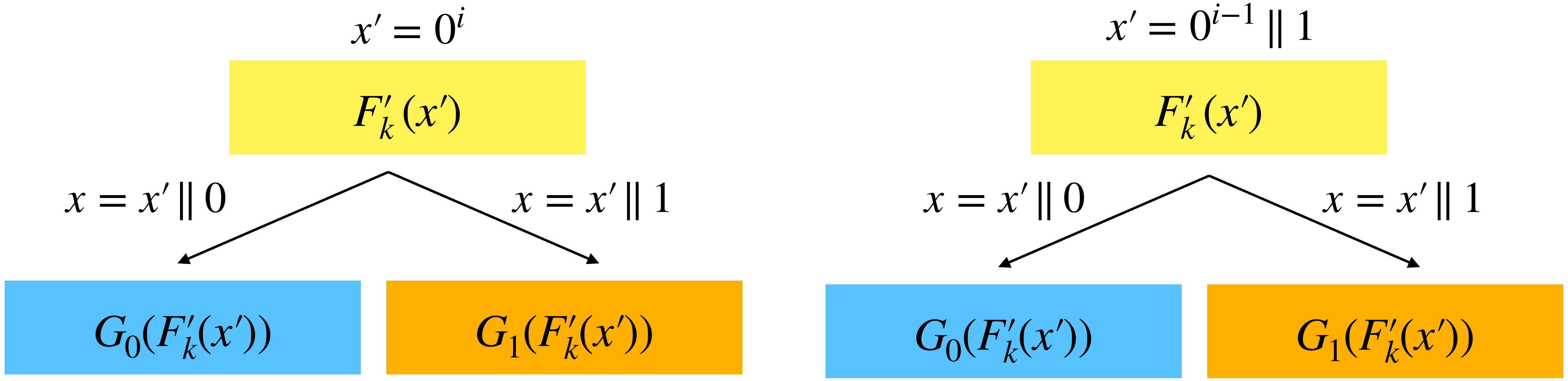
$G_1(F'_k(x'))$

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^{\lambda} \to \{0,1\}^{2\lambda}$ be a PRG and $F'_k : \{0,1\}^{i} \to \{0,1\}^{\lambda}$ be a PRF.
- How to construct $F_k : \{0,1\}^{i+1} \to \{0,1\}^{\lambda}$?

Given $x \in \{0,1\}^{i+1}$, let $x = x' \,\|\, b$ where $x' \in \{0,1\}^{i}$.

$G(k) = G_0(k) \,\|\, G_1(k)$



$x' = 0^i$

$F'_k(x')$

$x = x' \,\|\, 0$

$x = x' \,\|\, 1$

$G_0(F'_k(x'))$

$G_1(F'_k(x'))$

$x' = 0^{i-1} \,\|\, 1$

$F'_k(x')$

$x = x' \,\|\, 0$

$x = x' \,\|\, 1$

$G_0(F'_k(x'))$

$G_1(F'_k(x'))$

Constructing PRFs from PRGs: Warmup

- Let $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ be a PRG and $F'_k : \{0,1\}^i \to \{0,1\}^\lambda$ be a PRF.
- How to construct $F_k : \{0,1\}^{i+1} \to \{0,1\}^\lambda$?

Given $x \in \{0,1\}^{i+1}$, let $x = x' \,\|\, b$ where $x' \in \{0,1\}^i$.

$G(k) = G_0(k) \,\|\, G_1(k)$

$x' = 0^i$
$F'_k(x')$
$x = x' \,\|\, 0$
$x = x' \,\|\, 1$
$G_0(F'_k(x'))$
$G_1(F'_k(x'))$
$x' = 0^{i-1} \,\|\, 1$
$F'_k(x')$
$x = x' \,\|\, 0$
$x = x' \,\|\, 1$
$G_0(F'_k(x'))$
$G_1(F'_k(x'))$
$\cdots$
$x' = 1^i$
$F'_k(x')$
$x = x' \,\|\, 0$
$x = x' \,\|\, 1$
$G_0(F'_k(x'))$
$G_1(F'_k(x'))$

GGM Construction

Theorem [Goldreich-Goldwasser-Micali’86]**:**

$$\text{PRG} \implies \text{PRF}.$$

Proof.

GGM Construction

Theorem [Goldreich-Goldwasser-Micali'86]**:**

$$\text{PRG} \implies \text{PRF}.$$

Proof.

Let $G : \{0,1\} \to \{0,1\}^{2\lambda}$ and $G(k) = G_0(k) \parallel G_1(k)$.

GGM Construction

Theorem [Goldreich-Goldwasser-Micali'86]**:**

$$\text{PRG} \implies \text{PRF}.$$

Proof.

Let $G : \{0,1\} \to \{0,1\}^{2\lambda}$ and $G(k) = G_0(k) \| G_1(k)$. Output $F_k(x) := G_{x_\lambda}\left(\ldots G_{x_2}\left(G_{x_1}(k)\right)\right)$

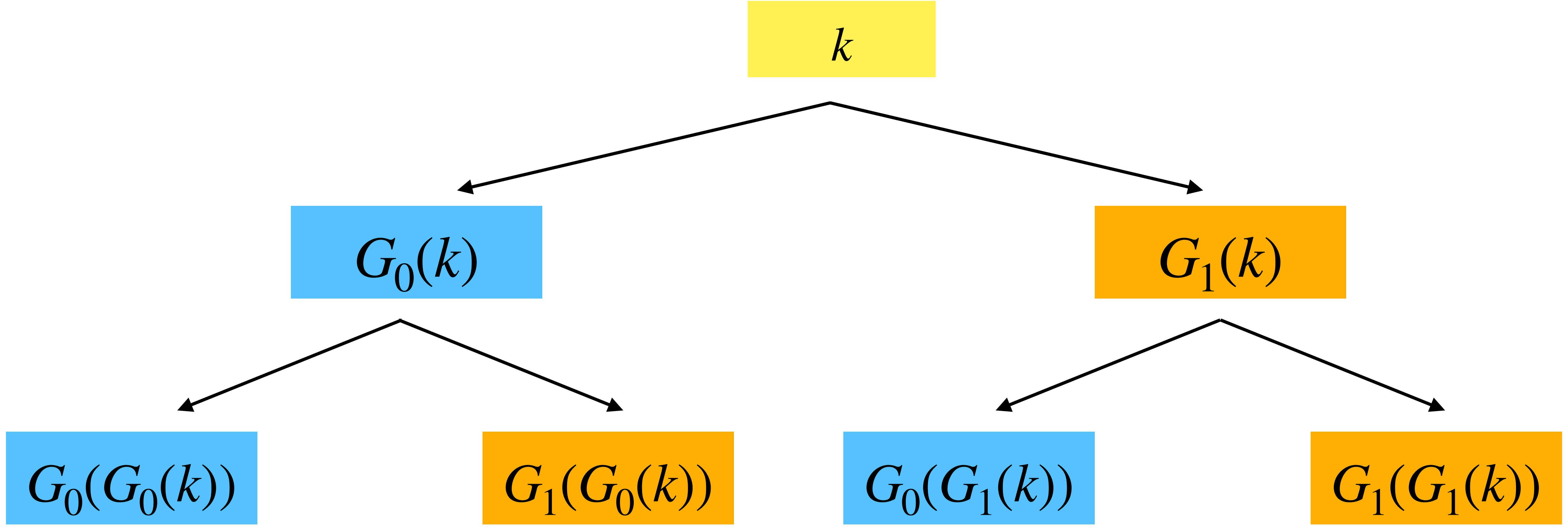
GGM Construction

Theorem [Goldreich-Goldwasser-Micali'86]:

PRG $\Longrightarrow$ PRF.

Proof.

Let $G : \{0,1\} \to \{0,1\}^{2\lambda}$ and $G(k) = G_0(k) \| G_1(k)$. Output $F_k(x) := G_{x_\lambda}\left(\ldots G_{x_2}\left(G_{x_1}(k)\right)\right)$



GGM Construction

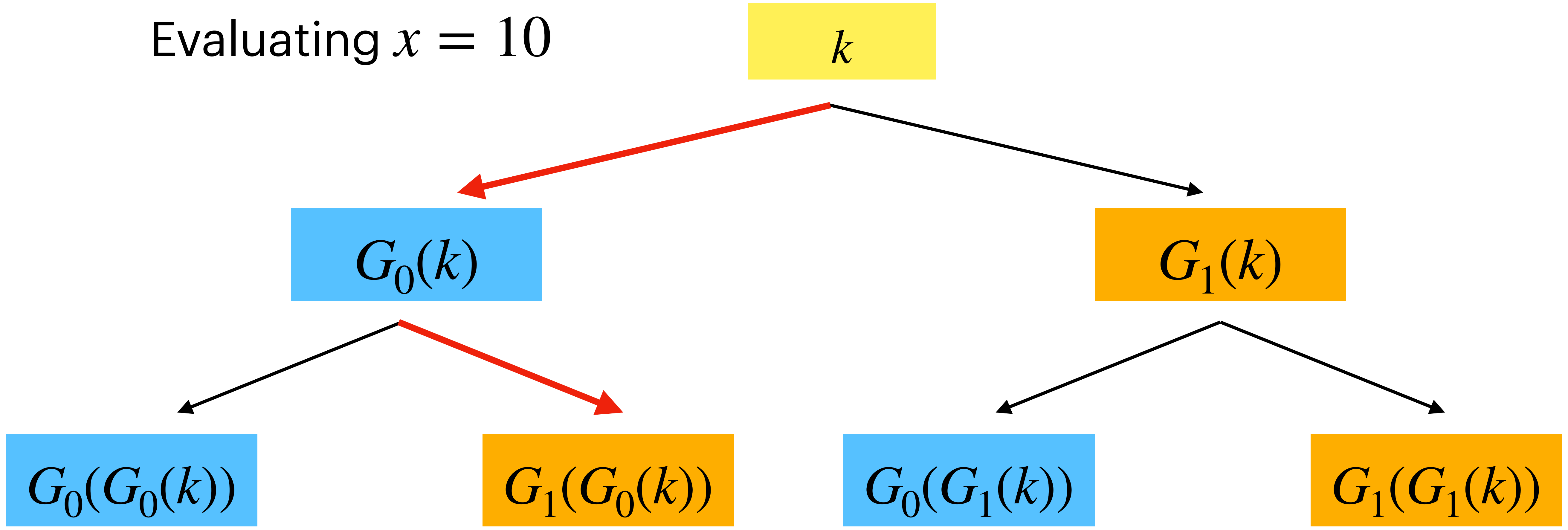
Theorem [Goldreich-Goldwasser-Micali'86]:

$$\text{PRG} \implies \text{PRF}.$$

Proof.

Let $G : \{0,1\} \to \{0,1\}^{2\lambda}$ and $G(k) = G_0(k) \,\|\, G_1(k)$. Output $F_k(x) := G_{x_\lambda}\left(\ldots G_{x_2}\left(G_{x_1}(k)\right)\right)$

Evaluating $x = 10$



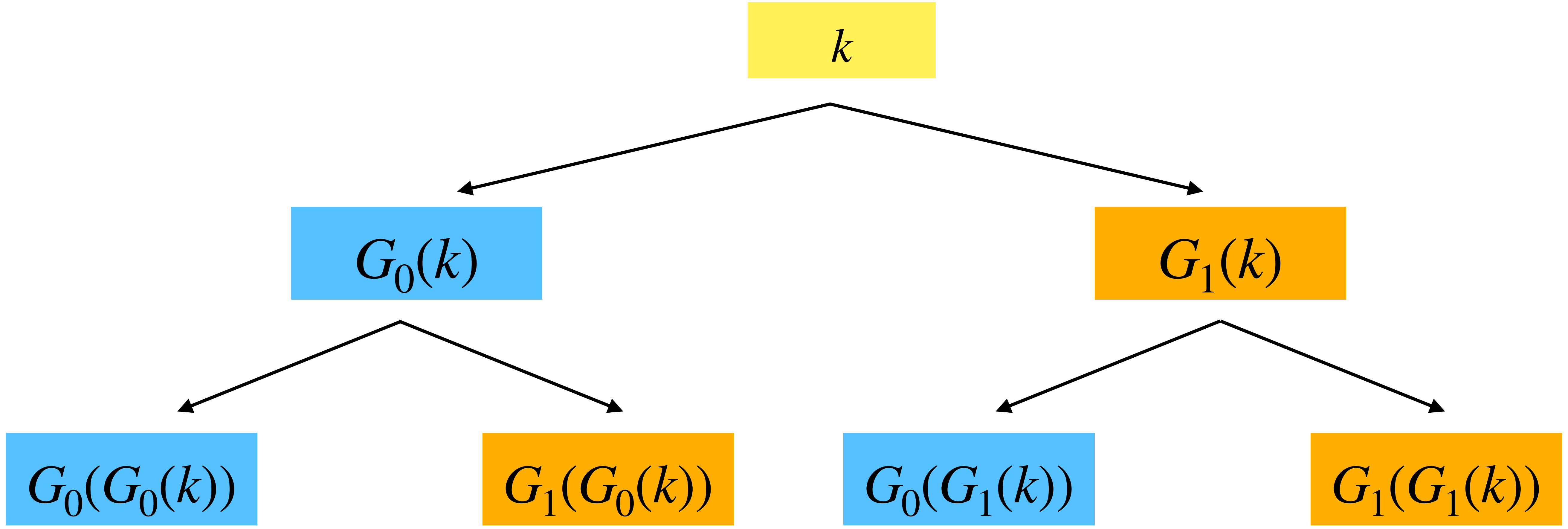
GGM Construction

Theorem [Goldreich-Goldwasser-Micali'86]:

$$\text{PRG} \Longrightarrow \text{PRF}.$$

Proof.

Let $G : \{0,1\} \to \{0,1\}^{2\lambda}$ and $G(k) = G_0(k) \,\|\, G_1(k)$. Output $F_k(x) := G_{x_\lambda}\left(\ldots G_{x_2}\left(G_{x_1}(k)\right)\right)$



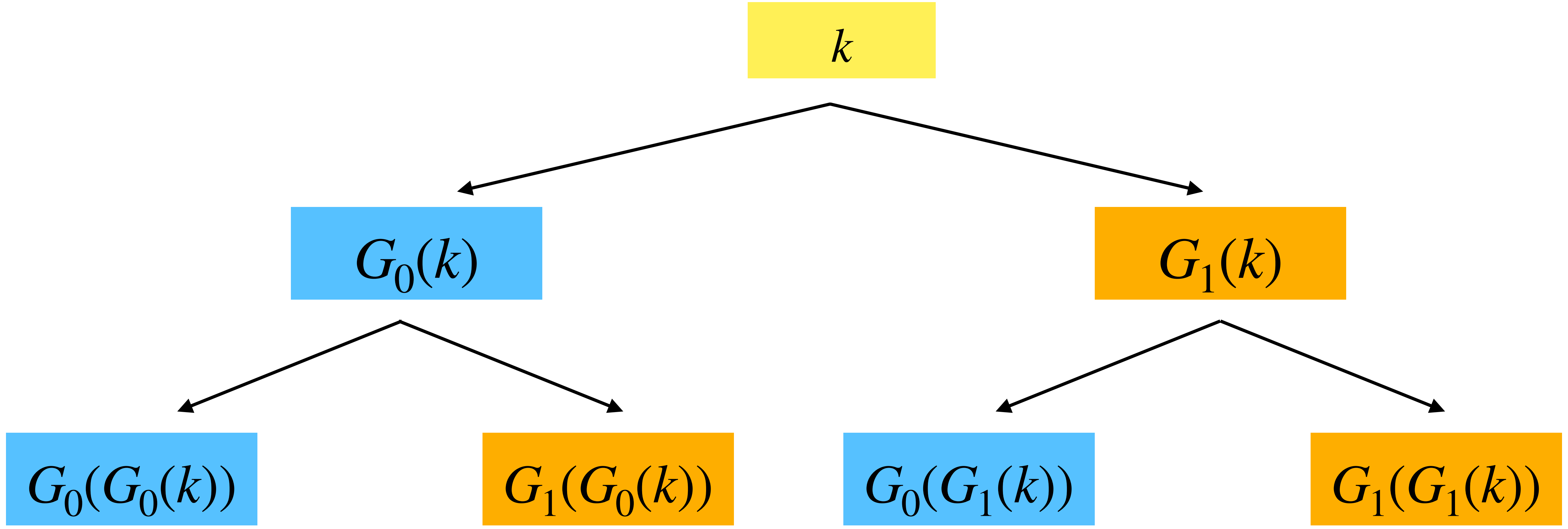
GGM Construction

Theorem [Goldreich-Goldwasser-Micali'86]:

$$\text{PRG} \implies \text{PRF.}$$

Proof.

Let $G : \{0,1\} \to \{0,1\}^{2\lambda}$ and $G(k) = G_0(k) \,\|\, G_1(k)$. Output $F_k(x) := G_{x_\lambda}\left(\ldots G_{x_2}\left(G_{x_1}(k)\right)\right)$



k

$G_0(k)$ $G_1(k)$

$G_0(G_0(k))$ $G_1(G_0(k))$ $G_0(G_1(k))$ $G_1(G_1(k))$

Height of the tree?

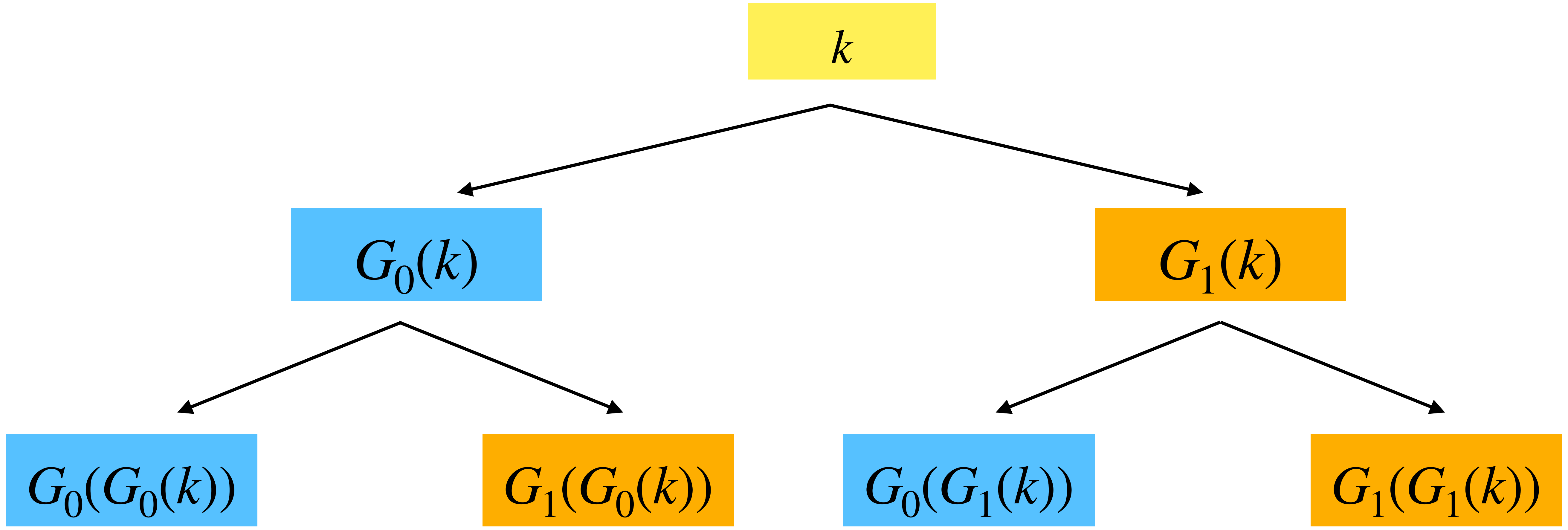
GGM Construction

Theorem [Goldreich-Goldwasser-Micali'86]:

$$\text{PRG} \implies \text{PRF}.$$

Proof.

Let $G : \{0,1\} \to \{0,1\}^{2\lambda}$ and $G(k) = G_0(k) \,\|\, G_1(k)$. Output $F_k(x) := G_{x_\lambda}\left(\ldots G_{x_2}\left(G_{x_1}(k)\right)\right)$



Height of the tree? $\log\left(\#\text{inputs}\right) = \lambda.$

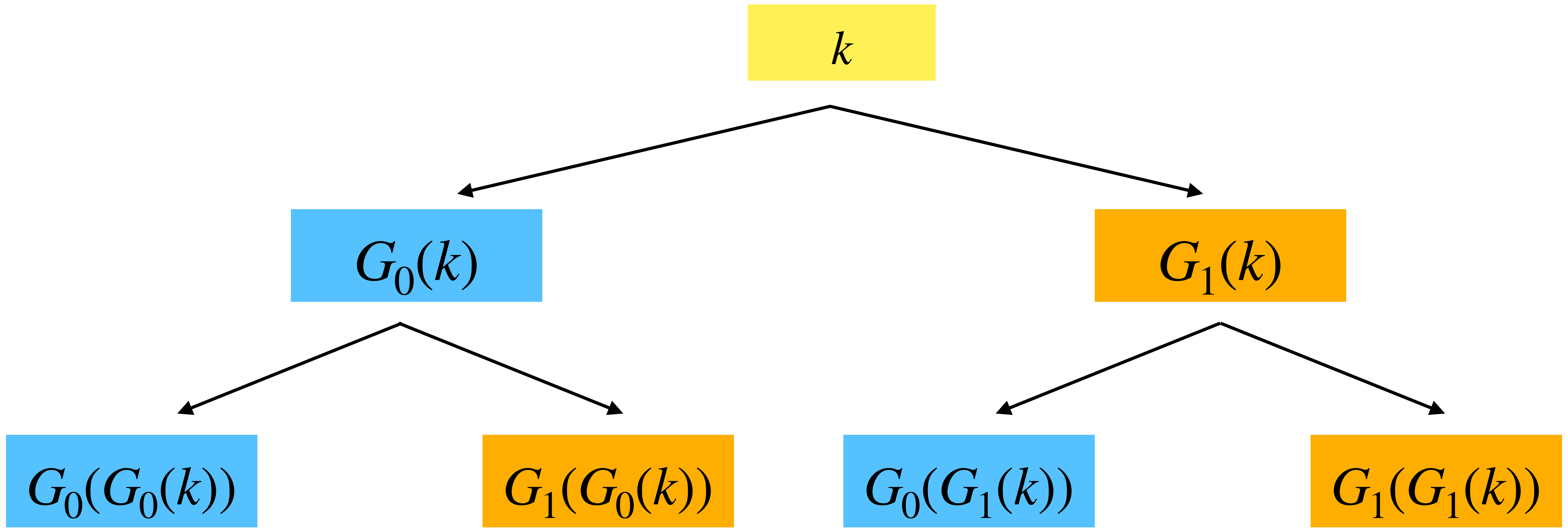
GGM Construction

Theorem [Goldreich-Goldwasser-Micali'86]:

PRG $\implies$ PRF.

Proof.

Let $G : \{0,1\} \to \{0,1\}^{2\lambda}$ and $G(k) = G_0(k) \,\|\, G_1(k)$. Output $F_k(x) := G_{x_\lambda}\left(\ldots G_{x_2}\left(G_{x_1}(k)\right)\right)$



Height of the tree? $\log(\text{\#inputs}) = \lambda.$

Security?

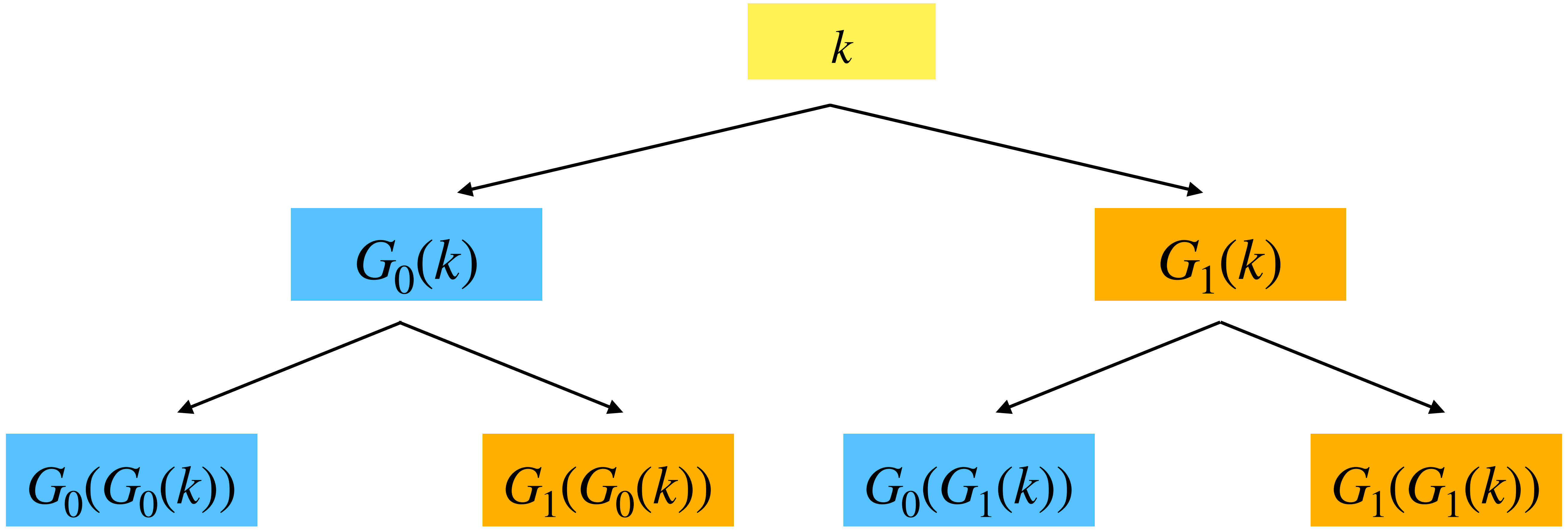
GGM Construction

Theorem [Goldreich-Goldwasser-Micali'86]:

$$\text{PRG} \Longrightarrow \text{PRF}.$$

Proof.

Let $G : \{0,1\} \to \{0,1\}^{2\lambda}$ and $G(k) = G_0(k) \,\|\, G_1(k)$. Output $F_k(x) := G_{x_\lambda}\left(\ldots G_{x_2}\left(G_{x_1}(k)\right)\right)$



Height of the tree? $\log(\#\text{inputs}) = \lambda$.

Security?

Hybrid Argument!

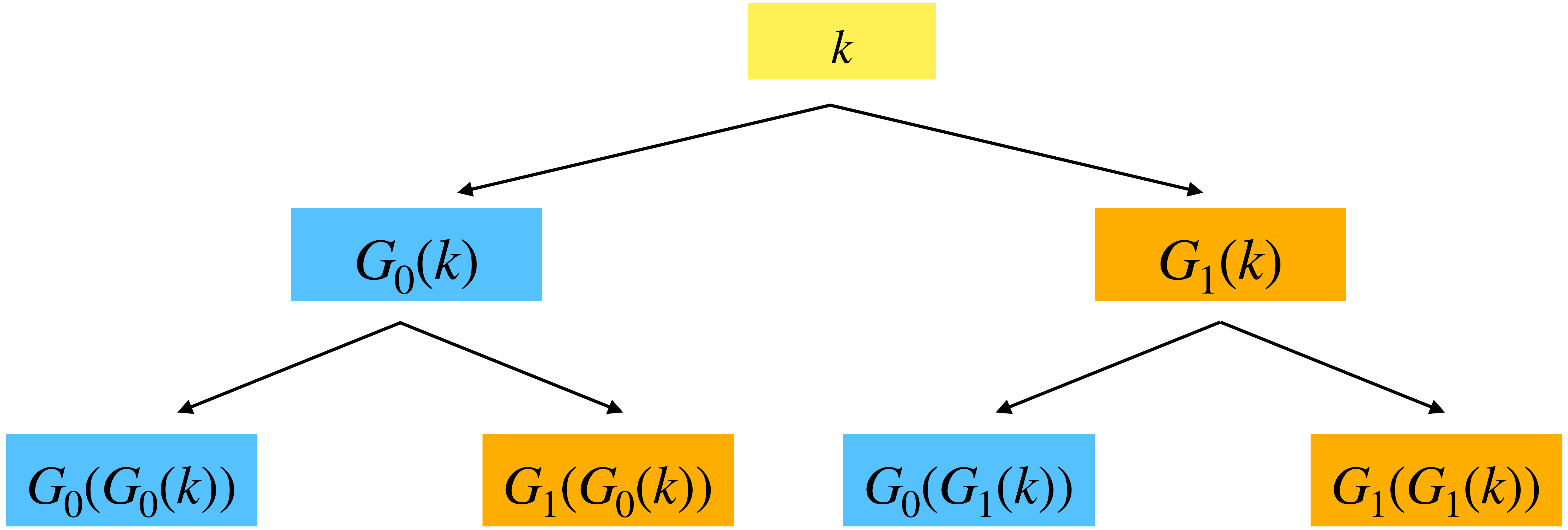
GGM Construction

Theorem [Goldreich-Goldwasser-Micali'86]:

$$\text{PRG} \implies \text{PRF}.$$

Proof.

Let $G : \{0,1\} \to \{0,1\}^{2\lambda}$ and $G(k) = G_0(k) \,\|\, G_1(k)$. Output $F_k(x) := G_{x_\lambda}\left(\ldots G_{x_2}\left(G_{x_1}(k)\right)\right)$



Height of the tree? $\log\left(\#\text{inputs}\right) = \lambda.$

Security?

Hybrid Argument!

One hybrid for each node?

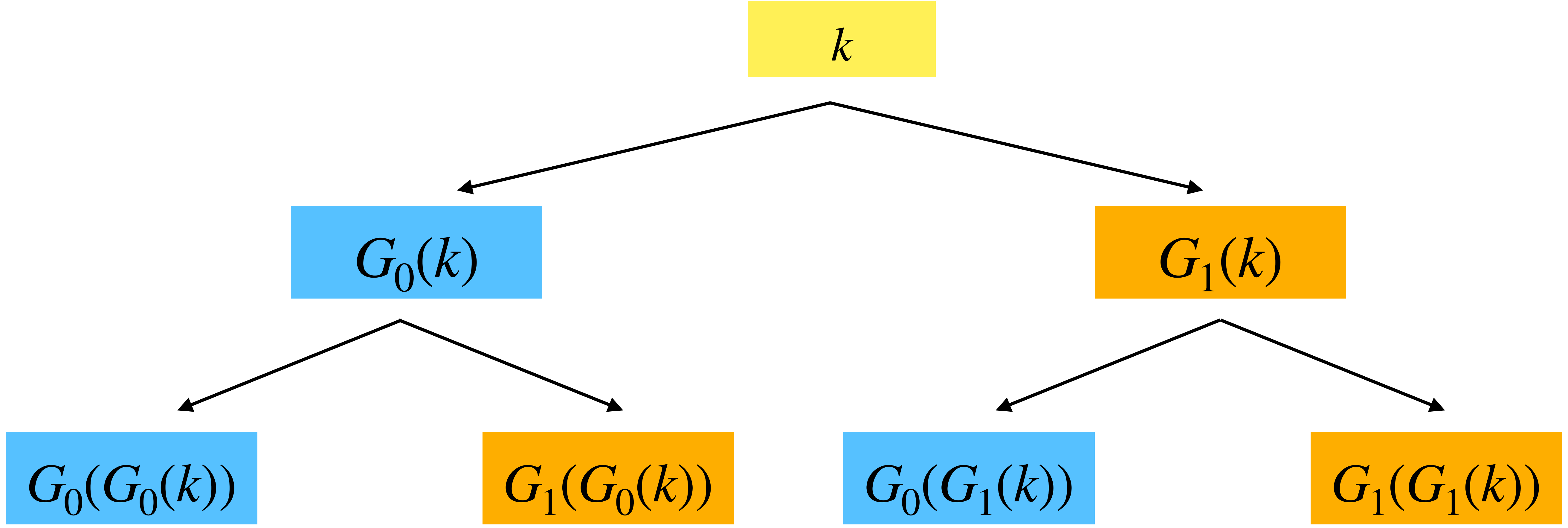
GGM Construction

Theorem [Goldreich-Goldwasser-Micali'86]:

PRG $\Longrightarrow$ PRF.

Proof.

Let $G : \{0,1\} \to \{0,1\}^{2\lambda}$ and $G(k) = G_0(k) \| G_1(k)$. Output $F_k(x) := G_{x_\lambda}\left(\ldots G_{x_2}\left(G_{x_1}(k)\right)\right)$



Height of the tree? $\log\left(\#\text{inputs}\right) = \lambda.$

Security?

Hybrid Argument!

One hybrid for each node? No! 2^λ nodes.

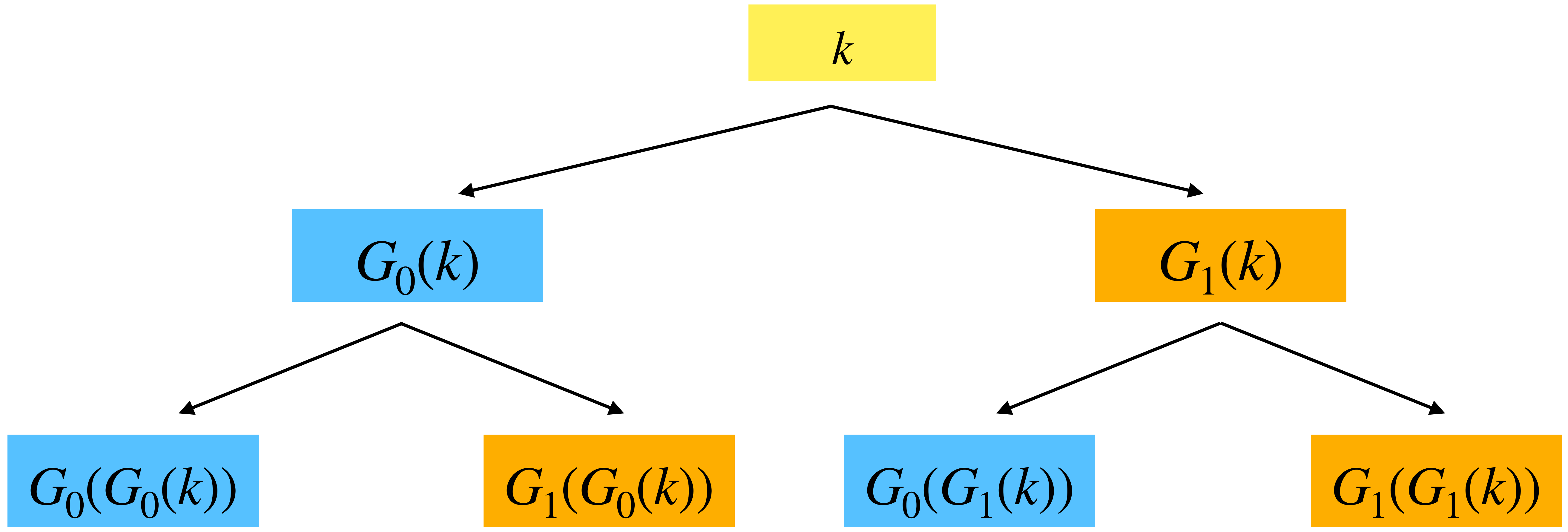
GGM Construction

Theorem [Goldreich-Goldwasser-Micali'86]:

PRG $\Longrightarrow$ PRF.

Proof.

Let $G : \{0,1\} \to \{0,1\}^{2\lambda}$ and $G(k) = G_0(k) \,\|\, G_1(k)$. Output $F_k(x) := G_{x_\lambda}\left(\ldots G_{x_2}\left(G_{x_1}(k)\right)\right)$



Height of the tree? $\log\left(\text{\#inputs}\right) = \lambda.$

Security?

Hybrid Argument!

One hybrid for each node? No! 2^λ nodes.

In hybrid H_i, view i-th layer as a random function $f : \{0,1\}^{2^i} \to \{0,1\}^\lambda$

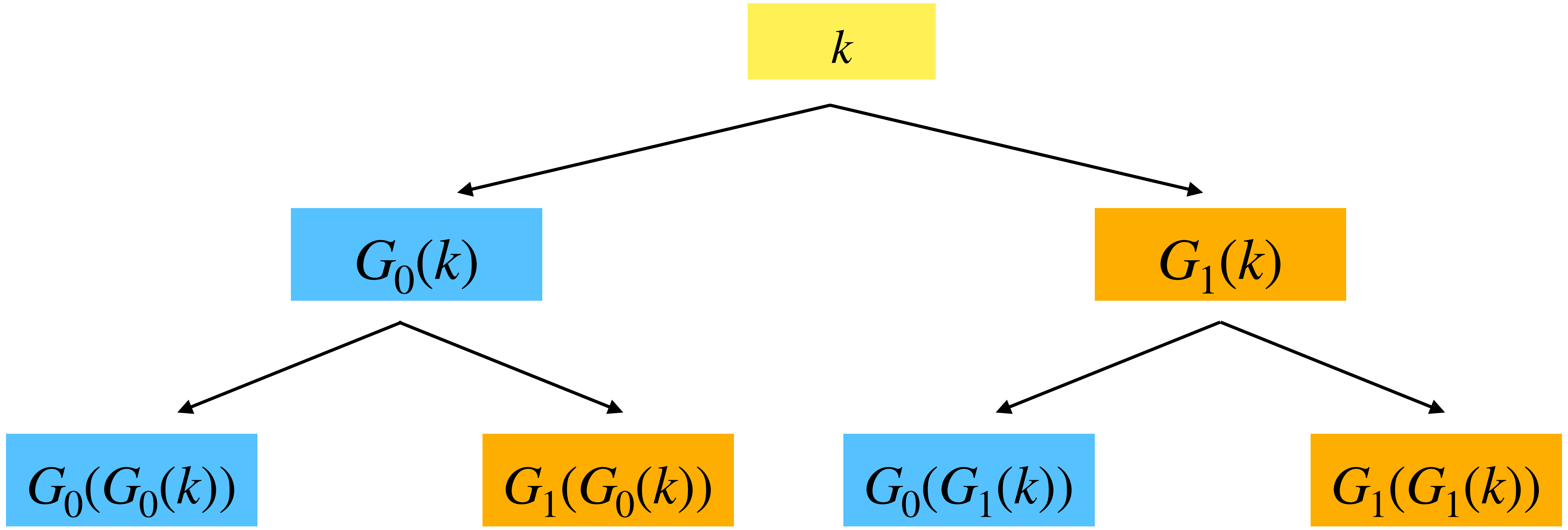
GGM Construction

Theorem [Goldreich-Goldwasser-Micali'86]:

PRG $\Longrightarrow$ PRF.

Proof.

Let $G : \{0,1\} \to \{0,1\}^{2\lambda}$ and $G(k) = G_0(k) \| G_1(k)$. Output $F_k(x) := G_{x_\lambda}\left(\ldots G_{x_2}\left(G_{x_1}(k)\right)\right)$



Height of the tree? $\log(\text{\#inputs}) = \lambda$.

Security?

Hybrid Argument!

One hybrid for each node? No! 2^λ nodes.

In hybrid H_i, view i-th layer as a random function $f : \{0,1\}^{2^i} \to \{0,1\}^\lambda$

f is evaluated at most poly(λ) points.