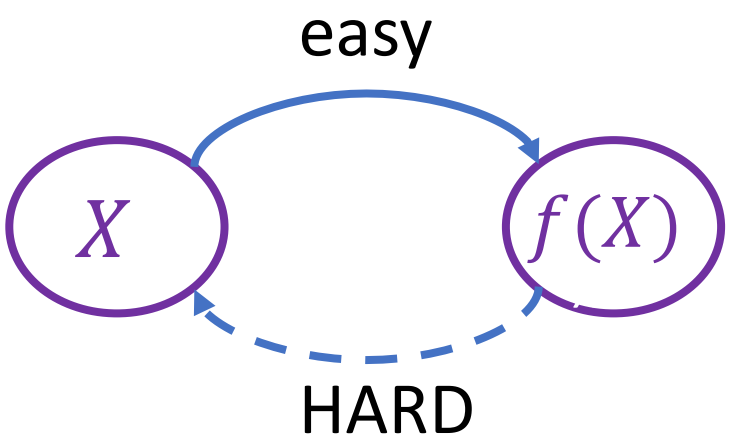
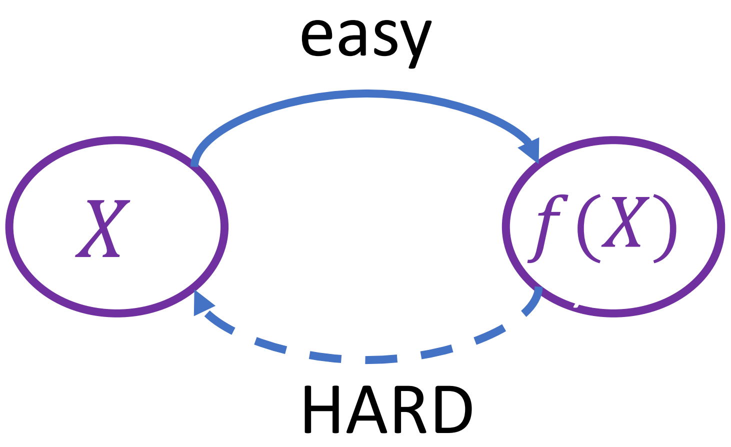
Counting Unpredictable Bits: Simple PRG from OWFs

Noam Mazor (Cornell Tech)
Rafael Pass (Tel Aviv University & Cornell Tech)

One-Way Functions

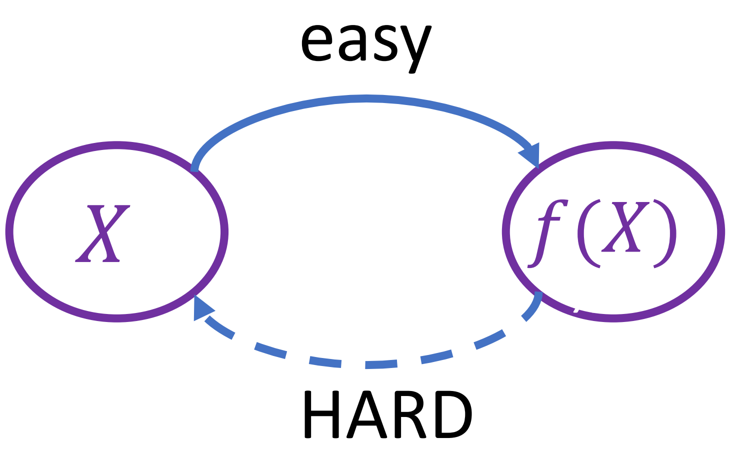


One-Way Functions



- The minimal assumption for cryptography

One-Way Functions



- The minimal assumption for cryptography
- Can be used to construct many useful primitives

OWF $\Rightarrow$ PRG

OWF $\Rightarrow$ PRG

Basic result in crypto [Hastad-Impagliazzo-Levin-Luby]

OWF $\Rightarrow$ PRG

Basic result in crypto [Hastad-Impagliazzo-Levin-Luby]

[Holenstein], [Haitner-Harnik-Reingold], [Haitner-Reingold-Vadhan], [Vadhan-Zheng], [Haitner-Vadhan]

OWF $\Rightarrow$ PRG

Basic result in crypto [Hastad-Impagliazzo-Levin-Luby]

[Holenstein], [Haitner-Harnik-Reingold], [Haitner-Reingold-Vadhan], [Vadhan-Zheng], [Haitner-Vadhan]

- Much simpler, better efficiency

OWF $\Rightarrow$ PRG

Basic result in crypto [Hastad-Impagliazzo-Levin-Luby]

[Holenstein], [Haitner-Harnik-Reingold], [Haitner-Reingold-Vadhan], [Vadhan-Zheng], [Haitner-Vadhan]

- Much simpler, better efficiency

- Still too complicated to teach in graduate course

OWF $\Rightarrow$ PRG

Basic result in crypto [Hastad-Impagliazzo-Levin-Luby]

[Holenstein], [Haitner-Harnik-Reingold], [Haitner-Reingold-Vadhan], [Vadhan-Zheng], [Haitner-Vadhan]

- Much simpler, better efficiency

- Still too complicated to teach in graduate course

This work: Simple proof for the non-uniform setting

OWF $\Rightarrow$ PRG

Basic result in crypto [Hastad-Impagliazzo-Levin-Luby]

[Holenstein], [Haitner-Harnik-Reingold], [Haitner-Reingold-Vadhan], [Vadhan-Zheng], [Haitner-Vadhan]

- Much simpler, better efficiency

- Still too complicated to teach in graduate course

This work: Simple proof for the non-uniform setting
with better parameters

Proving OWF $\Rightarrow$ PRG

Proving OWF ⇒ PRG

General approach:

Proving OWF ⇒ PRG

General approach:

1. Start with a weaker notion of pseudorandomness

Proving OWF $\Rightarrow$ PRG

General approach:

1. Start with a weaker notion of pseudorandomness
2. Amplify it

Proving OWF $\Rightarrow$ PRG

General approach:

1. Start with a weaker notion of pseudorandomness
2. Amplify it

[HILL]: Pseudoentropy

Proving OWF $\Rightarrow$ PRG

General approach:

1. Start with a weaker notion of pseudorandomness
2. Amplify it

[HILL]: Pseudoentropy

[HRV]: Next-Block Pseudoentropy

Proving OWF ⇒ PRG

General approach:

1. Start with a weaker notion of pseudorandomness
2. Amplify it

[HILL]: Pseudoentropy

[HRV]: Next-Block Pseudoentropy

<u>Key insight</u>: A simple weak notion of pseudorandomness

Proving OWF $\Rightarrow$ PRG

General approach:

1. Start with a weaker notion of pseudorandomness
2. Amplify it

[HILL]: Pseudoentropy

[HRV]: Next-Block Pseudoentropy

<u>Key insight</u>: A simple weak notion of pseudorandomness

Bits Unpredictability - Counting unpredictable bits

Next-Bit Unpredictability

Next-Bit Unpredictability

Let $X = (X_1, \dots, X_n)$

Next-Bit Unpredictability

Let $X = (X_1, \ldots, X_n)$

Next-Bit Unpredictability [Blum-Micali]:

Next-Bit Unpredictability

Let $X = (X_1, \dots, X_n)$

Next-Bit Unpredictability [Blum-Micali]:

- For every $i \in [n]$, X_i is hard to predict given $X_1, \dots, X_{i-1}$ by poly-time TM

Next-Bit Unpredictability

Let $X = (X_1, \dots, X_n)$

Next-Bit Unpredictability [Blum-Micali]:

- For every $i \in [n]$, X_i is hard to predict given $X_1, \dots, X_{i-1}$ by poly-time TM
- [Yao '82]: Next-bit unpredictability ⇔ Pseudorandomness

Next-Bit Unpredictability

Let $X = (X_1, \dots, X_n)$

Next-Bit Unpredictability [Blum-Micali]:

- For every $i \in [n]$, X_i is hard to predict given $X_1, \dots, X_{i-1}$ by poly-time TM
- [Yao '82]: Next-bit unpredictability $\Leftrightarrow$ Pseudorandomness

Bits Unpredictability: Some of the bits are unpredictable

Next-Bit Unpredictability

Let $X = (X_1, \dots, X_n)$

Next-Bit Unpredictability [Blum-Micali]:

- For every $i \in [n]$, X_i is hard to predict given $X_1, \dots, X_{i-1}$ by poly-time TM
- [Yao '82]: Next-bit unpredictability ⇔ Pseudorandomness

Bits Unpredictability: Some of the bits are unpredictable

- For every $i \in S \subseteq [n]$, X_i is hard to predict given $X_1, \dots, X_{i-1}$

Next-Bit Unpredictability

Let $X = (X_1, \dots, X_n)$

Next-Bit Unpredictability [Blum-Micali]:

- For every $i \in [n]$, X_i is hard to predict given $X_1, \dots, X_{i-1}$ by poly-time TM
- [Yao '82]: Next-bit unpredictability ⇔ Pseudorandomness

Bits Unpredictability: Some of the bits are unpredictable

- For every $i \in S \subseteq [n]$, X_i is hard to predict given $X_1, \dots, X_{i-1}$
- S is a random variable, can be dependent on X

Next-Bit Unpredictability

Let $X = (X_1, \dots, X_n)$

Next-Bit Unpredictability [Blum-Micali]:

- For every $i \in [n]$, X_i is hard to predict given $X_1, \dots, X_{i-1}$ by poly-time TM
- [Yao '82]: Next-bit unpredictability ⇔ Pseudorandomness

Bits Unpredictability: Some of the bits are unpredictable

- For every $i \in S \subseteq [n]$, X_i is hard to predict given $X_1, \dots, X_{i-1}$
- S is a random variable, can be dependent on X
- Want $|S|$ to be large

Proof Overview

Proof Overview

1. Constructing Bits Unpredictability from one-way function

Proof Overview

1. Constructing Bits Unpredictability from one-way function

2. Converting Bits Unpredictability to pseudorandomness

   ([HRV], but easier to analyize)

Proof Overview

1. Constructing Bits Unpredictability from one-way function

2. Converting Bits Unpredictability to pseudorandomness

   ([HRV], but easier to analyize)

Relying on simple tools (Goldriech-Levin, Chernoff, ...)

Part I:
OWF $\Rightarrow$ Bits Unpredictability

OWF $\Rightarrow$ Bits Unpredictability

OWF $\Rightarrow$ Bits Unpredictability

- Let $f: \{0,1\}^n \to \{0,1\}^n$ be a one-way function

OWF $\Rightarrow$ Bits Unpredictability

- Let $f: \{0,1\}^n \to \{0,1\}^n$ be a one-way function
- Let M be a random $n \times n$ binary matrix, and $X \leftarrow \{0,1\}^n$

OWF ⇒ Bits Unpredictability

- Let $f: \{0,1\}^n \to \{0,1\}^n$ be a one-way function
- Let M be a random $n \times n$ binary matrix, and $X \leftarrow \{0,1\}^n$

$$\boxed{\begin{array}{c} M(x) = M \cdot x = \langle M_1, x\rangle, \dots, \langle M_n, x\rangle \\ \text{For } M = (M_1, \dots, M_n) \end{array}}$$

OWF ⇒ Bits Unpredictability

- Let $f: \{0,1\}^n \to \{0,1\}^n$ be a one-way function
- Let M be a random $n \times n$ binary matrix, and $X \leftarrow \{0,1\}^n$

The construction:

$$M(x) = M \cdot x = \langle M_1, x\rangle, \dots, \langle M_n, x\rangle$$

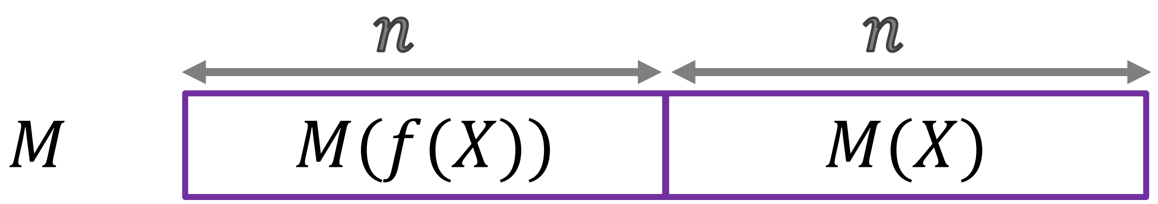
For $M = (M_1, \dots, M_n)$

OWF ⇒ Bits Unpredictability

- Let $f: \{0,1\}^n \to \{0,1\}^n$ be a one-way function
- Let M be a random $n \times n$ binary matrix, and $X \leftarrow \{0,1\}^n$

The construction:

$$g_M(X) = M\big(f(X)\big), M(X)$$



$$M(x) = M \cdot x = \langle M_1, x \rangle, \dots, \langle M_n, x \rangle$$

For $M = (M_1, \dots, M_n)$

OWF ⇒ Bits Unpredictability

- Let $f: \{0,1\}^n \to \{0,1\}^n$ be a one-way function
- Let M be a random $n \times n$ binary matrix, and $X \leftarrow \{0,1\}^n$

The construction:

	$\overleftrightarrow{\quad n \quad}$	$\overleftrightarrow{\quad n \quad}$
M	$M(f(X))$	$M(X)$

$$g_M(X) = M\big(f(X)\big), M(X)$$

$g_M(X)$ is not pseudorandom (given M)

$$M(x) = M \cdot x = \langle M_1, x\rangle, \dots, \langle M_n, x\rangle$$

For $M = (M_1, \dots, M_n)$

OWF $\Rightarrow$ Bits Unpredictability

- Let $f\colon \{0,1\}^n \to \{0,1\}^n$ be a one-way function
- Let M be a random $n \times n$ binary matrix, and $X \leftarrow \{0,1\}^n$

The construction:

$$g_M(X) = M\big(f(X)\big), M(X)$$

$$M \quad \overbrace{\boxed{M(f(X))}}^{n}\overbrace{\boxed{M(X)}}^{n}$$

$g_M(X)$ is not pseudorandom (given M)

- Can find X from $M, M(X)$

$$M(x) = M \cdot x = \langle M_1, x\rangle, \ldots, \langle M_n, x\rangle$$

For $M = (M_1, \ldots, M_n)$

OWF $\Rightarrow$ Bits Unpredictability

- Let $f:\{0,1\}^n \to \{0,1\}^n$ be a one-way function
- Let M be a random $n{\times}n$ binary matrix, and $X \leftarrow \{0,1\}^n$

The construction:

	$\overset{n}{\longleftrightarrow}$	$\overset{n}{\longleftrightarrow}$
M	$M(f(X))$	$M(X)$

$$g_M(X) = M\big(f(X)\big), M(X)$$

$g_M(X)$ is not pseudorandom (given M)

- Can find X from $M, M(X)$

What happens if we read it bit-by-bit?

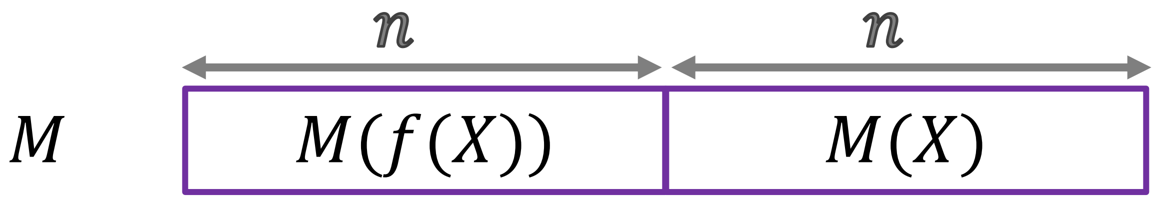
$$M(x) = M \cdot x = \langle M_1, x\rangle, \dots, \langle M_n, x\rangle$$

For $M = (M_1, \dots, M_n)$

OWF ⇒ Bits Unpredictability

- Let $f: \{0,1\}^n \to \{0,1\}^n$ be a one-way function
- Let M be a random $n \times n$ binary matrix, and $X \leftarrow \{0,1\}^n$

The construction:



$$g_M(X) = M\big(f(X)\big), M(X)$$

$g_M(X)$ is not pseudorandom (given M)

- Can find X from $M, M(X)$

What happens if we read it bit-by-bit?

<u>Thm</u>:

$g_M(X)$ has $(n + \log n)$ Bits Unpredictability (given M).

Proof: Bits Unpredictability from Regular OWF

	n	n
M	$M(f(X))$	$M(X)$

Proof: Bits Unpredictability from Regular OWF

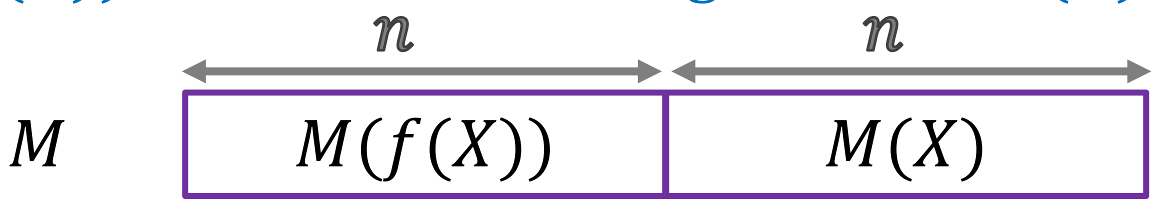
Assume $f:\{0,1\}^n \to \{0,1\}^n$ is r-regular ($\left|f^{-1}\left(f(x)\right)\right| = 2^r$) [Goldreich-Krawczyk-Luby]

	$\overbrace{\hspace{6em}}^{n}$	$\overbrace{\hspace{6em}}^{n}$
M	$M(f(X))$	$M(X)$

Proof: Bits Unpredictability from Regular OWF

Assume $f: \{0,1\}^n \to \{0,1\}^n$ is r-regular ($\left|f^{-1}\big(f(x)\big)\right| = 2^r$) [Goldreich-Krawczyk-Luby]

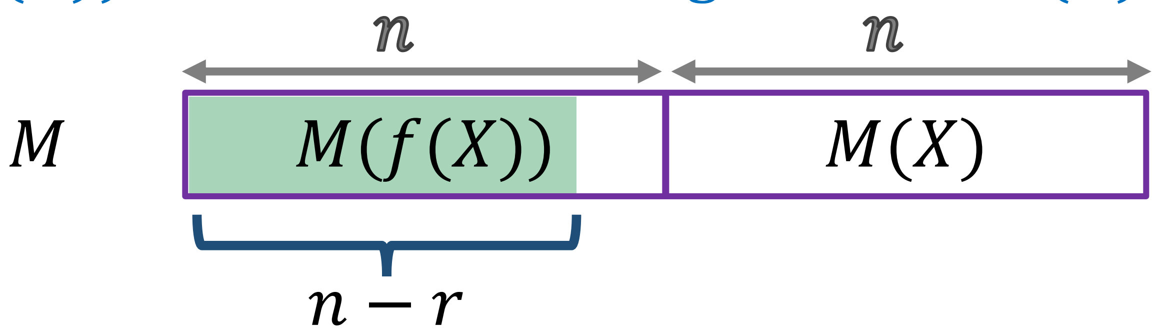
<u>Claim</u>: The first $\approx n - r$ bits of $M(f(X))$, and the first $r + \log n$ bits of $M(X)$ are unpredictable.



Proof: Bits Unpredictability from Regular OWF

Assume $f:\{0,1\}^n \to \{0,1\}^n$ is r-regular ($\left|f^{-1}\left(f(x)\right)\right| = 2^r$) [Goldreich-Krawczyk-Luby]

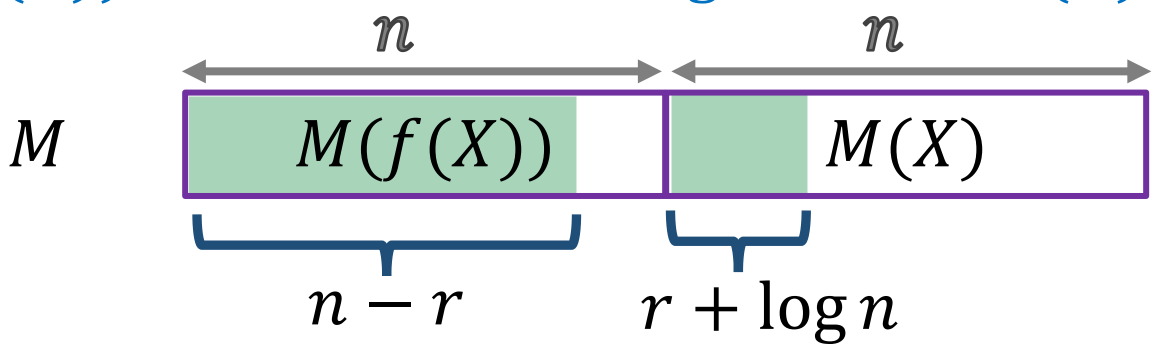
<u>Claim</u>: The first $\approx n - r$ bits of $M(f(X))$, and the first $r + \log n$ bits of $M(X)$ are unpredictable.



Proof: Bits Unpredictability from Regular OWF

Assume $f:\{0,1\}^n \to \{0,1\}^n$ is r-regular $\left(\left|f^{-1}\left(f(x)\right)\right| = 2^r\right)$ [Goldreich-Krawczyk-Luby]

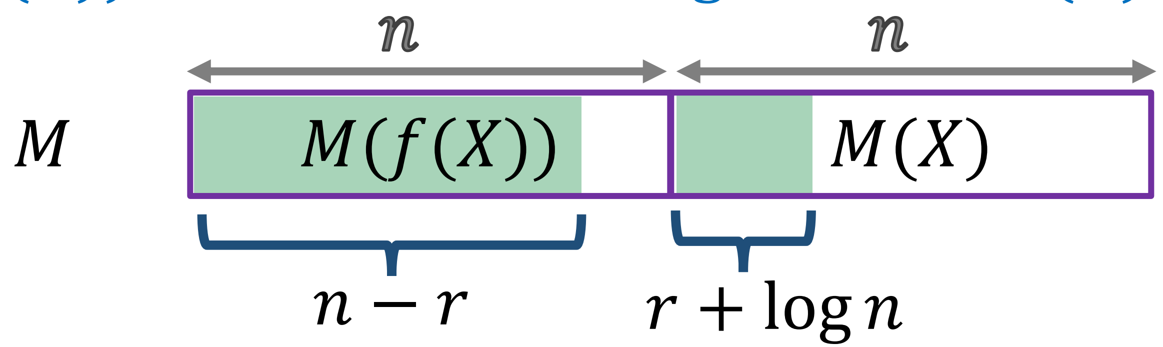
<u>Claim</u>: The first $\approx n - r$ bits of $M(f(X))$, and the first $r + \log n$ bits of $M(X)$ are unpredictable.



Proof: Bits Unpredictability from Regular OWF

Assume $f : \{0,1\}^n \to \{0,1\}^n$ is r-regular ($\left|f^{-1}\big(f(x)\big)\right| = 2^r$) [Goldreich-Krawczyk-Luby]

Claim: The first $\approx n - r$ bits of $M(f(X))$, and the first $r + \log n$ bits of $M(X)$ are unpredictable.

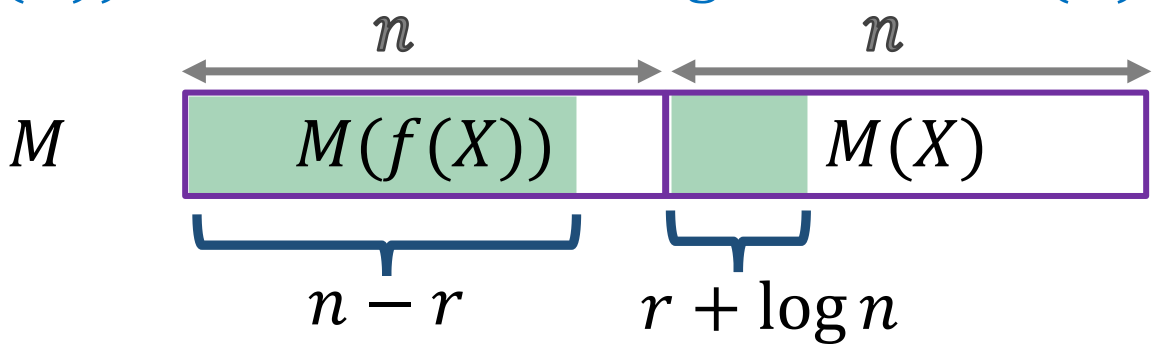


Pf: Similar to construction of PRG from regular one-way functions.

Proof: Bits Unpredictability from Regular OWF

Assume $f\colon \{0,1\}^n \to \{0,1\}^n$ is r-regular ($\left|f^{-1}\left(f(x)\right)\right| = 2^r$) [Goldreich-Krawczyk-Luby]

<u>Claim</u>: The first $\approx n - r$ bits of $M(f(X))$, and the first $r + \log n$ bits of $M(X)$ are unpredictable.



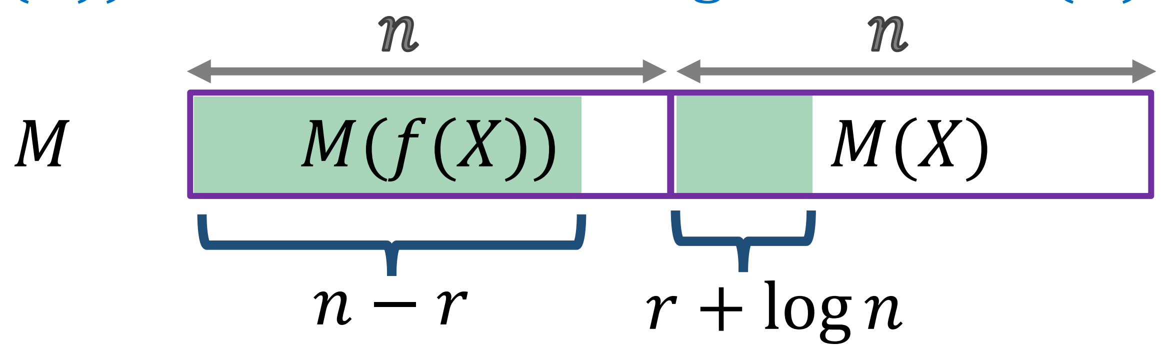
<u>Pf</u>: Similar to construction of PRG from regular one-way functions.

- $f(X)$ is a flat distribution over $2^n/2^r$ images. ($H_\infty\left(f(X)\right) = n - r$)

Proof: Bits Unpredictability from Regular OWF

Assume $f: \{0,1\}^n \to \{0,1\}^n$ is r-regular ($\left|f^{-1}\big(f(x)\big)\right| = 2^r$) [Goldreich-Krawczyk-Luby]

Claim: The first $\approx n - r$ bits of $M(f(X))$, and the first $r + \log n$ bits of $M(X)$ are unpredictable.



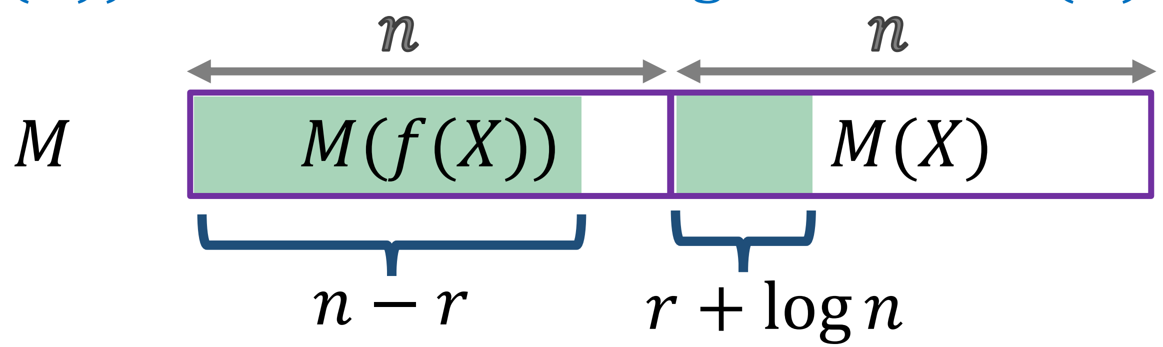
Pf: Similar to construction of PRG from regular one-way functions.

- $f(X)$ is a flat distribution over $2^n/2^r$ images. ($H_\infty\big(f(X)\big) = n - r$)
    - Can extract $\approx n - r$ random bits (Leftover hash lemma)

Proof: Bits Unpredictability from Regular OWF

Assume $f: \{0,1\}^n \to \{0,1\}^n$ is r-regular ($\left|f^{-1}\big(f(x)\big)\right| = 2^r$) [Goldreich-Krawczyk-Luby]

Claim: The first $\approx n - r$ bits of $M(f(X))$, and the first $r + \log n$ bits of $M(X)$ are unpredictable.



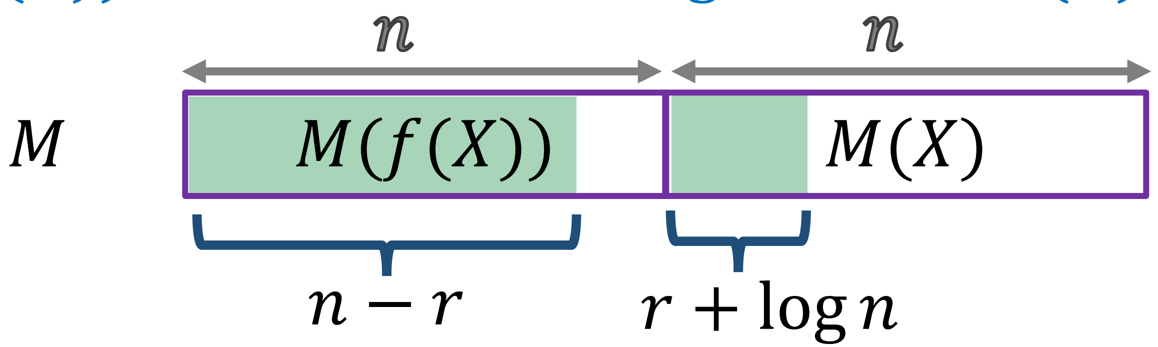
Pf: Similar to construction of PRG from regular one-way functions.

- $f(X)$ is a flat distribution over $2^n/2^r$ images. ($H_\infty\big(f(X)\big) = n - r$)
  - Can extract $\approx n - r$ random bits (Leftover hash lemma)
- $X|_{f(X)}$ is a flat distribution over 2^r pre-images. ($H_\infty\big(X|_{f(X)}\big) = r$)

Proof: Bits Unpredictability from Regular OWF

Assume $f : \{0,1\}^n \to \{0,1\}^n$ is r-regular ($\left|f^{-1}\big(f(x)\big)\right| = 2^r$) [Goldreich-Krawczyk-Luby]

<u>Claim</u>: The first $\approx n - r$ bits of $M(f(X))$, and the first $r + \log n$ bits of $M(X)$ are unpredictable.



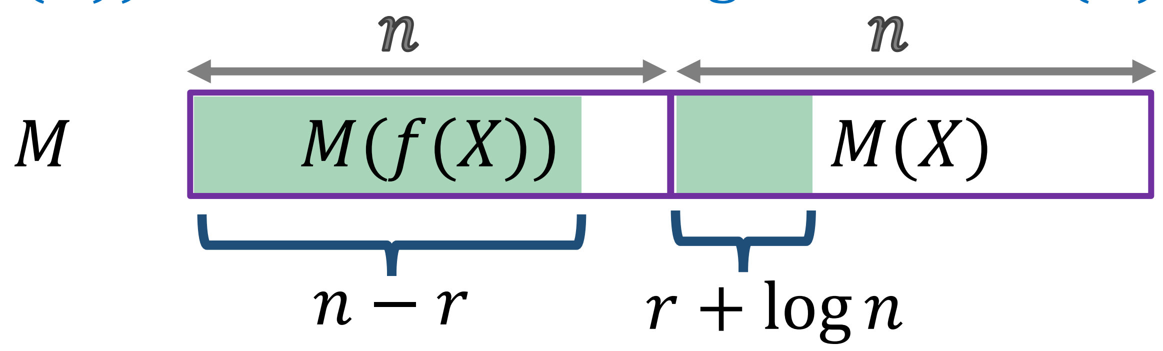
<u>Pf</u>: Similar to construction of PRG from regular one-way functions.

- $f(X)$ is a flat distribution over $2^n/2^r$ images. ($H_\infty\big(f(X)\big) = n - r$)
  - Can extract $\approx n - r$ random bits (Leftover hash lemma)
- $X|_{f(X)}$ is a flat distribution over 2^r pre-images. ($H_\infty\big(X|_{f(X)}\big) = r$)
  - Can extract r random bits $+ \log n$ pseudorandom bits (GL)

Proof: Bits Unpredictability from Regular OWF

Assume $f: \{0,1\}^n \to \{0,1\}^n$ is r-regular ($\left|f^{-1}\big(f(x)\big)\right| = 2^r$) [Goldreich-Krawczyk-Luby]

Claim: The first $\approx\ n - r$ bits of $M(f(X))$, and the first $r + \log n$ bits of $M(X)$ are unpredictable.



When reading $g_M(X)$ bit-by-bit, there are $n + \log n$ unpredictable bits!

Proof: Bits Unpredictability from Any OWF

What about arbitrary OWFs?

M	$M(f(X))$	$M(X)$

Proof: Bits Unpredictability from Any OWF

What about arbitrary OWFs?

Same construction works

M | $M(f(X))$ | $M(X)$

Proof: Bits Unpredictability from Any OWF

What about arbitrary OWFs?

Same construction works

M | $M(f(X))$ | $M(X)$

<u>Main observation</u>: Every function is a combination of regular functions.

Proof: Bits Unpredictability from Any OWF

What about arbitrary OWFs?

Same construction works

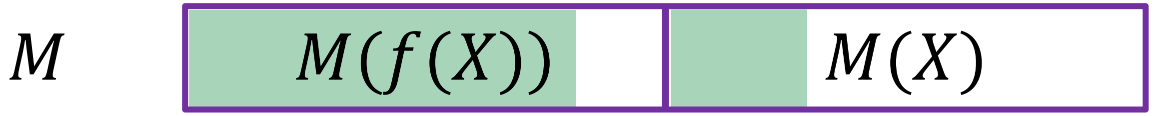
M | $M(f(X))$ | $M(X)$

Main observation: Every function is a combination of regular functions.

Proof: Bits Unpredictability from Any OWF

What about arbitrary OWFs?

Same construction works



<u>Main observation</u>: Every function is a combination of regular functions.

- For every x let $r(x) = \log|f^{-1}(f(x))|$

Proof: Bits Unpredictability from Any OWF

What about arbitrary OWFs?

Same construction works

M	$M(f(X))$	$M(X)$

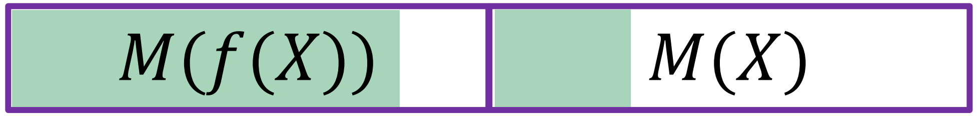
Main observation: Every function is a combination of regular functions.

- For every x let $r(x) = \log|f^{-1}(f(x))|$
- Let $D_j = \{x : r(x) = j\}$ for $j = 1, \dots, n$

Proof: Bits Unpredictability from Any OWF

What about arbitrary OWFs?

Same construction works

M 

Main observation: Every function is a combination of regular functions.

- For every x let $r(x) = \log|f^{-1}(f(x))|$
- Let $D_j = \{x: r(x) = j\}$ for $j = 1, \ldots, n$
- $f_j = f|_{D_j}: D_j \to \{0,1\}^n$ is j-regular

Proof: Bits Unpredictability from Any OWF

What about arbitrary OWFs?

Same construction works

M $\quad$ $M(f(X))$ $\quad$ $M(X)$

<u>Main observation</u>: Every function is a combination of regular functions.

- For every x let $r(x) = \log|f^{-1}(f(x))|$
- Let $D_j = \{x : r(x) = j\}$ for $j = 1, \ldots, n$
- $f_j = f|_{D_j} : D_j \to \{0,1\}^n$ is j-regular

$g_M(X)$ is a convex combination of distributions with $(n + \log n)$ Bits Unpredictability.

Part II:
Bits Unpredictability $\Rightarrow$ PRG

Bits Unpredictability ⇒ Pseudorandomness

M $\quad$ $M(f(X))$ $\quad$ $M(X)$

Bits Unpredictability ⇒ Pseudorandomness

For any OWF f, $g_M(X)$ has $(n + \log n)$-bits unpredictability

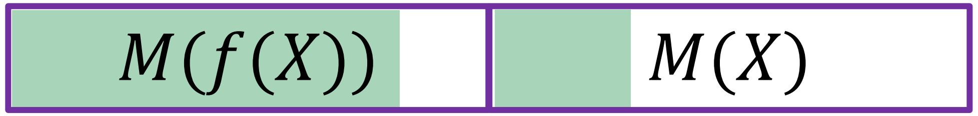
M $\quad$ $M(f(X))$ | $M(X)$

Bits Unpredictability ⇒ Pseudorandomness

For any OWF f, $g_M(X)$ has $(n + \log n)$-bits unpredictability

$g_M(X)$ is not pseudorandom

M



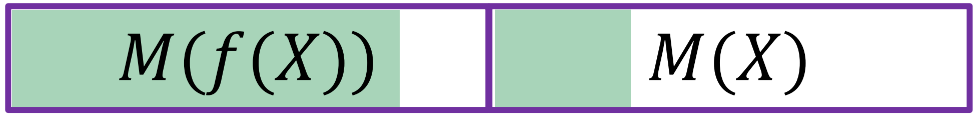
Bits Unpredictability ⇒ Pseudorandomness

For any OWF f, $g_M(X)$ has $(n + \log n)$-bits unpredictability

$g_M(X)$ is not pseudorandom

- Must use the next-bit property

M

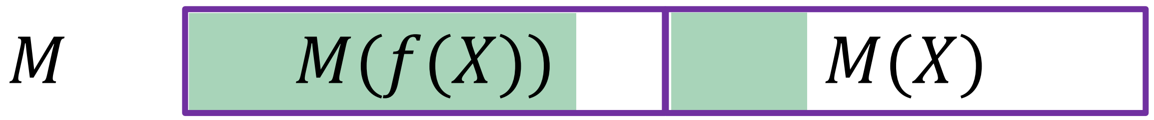


Bits Unpredictability ⇒ Pseudorandomness

For any OWF f, $g_M(X)$ has $(n + \log n)$-bits unpredictability

$g_M(X)$ is not pseudorandom

- Must use the next-bit property



Simple construction ([HRV])

Step 1: Bits Unpred. → Random Bits Unpred.

Step 1: Bits Unpred. → Random Bits Unpred.

Problem: We don’t know which bits are unpredictable

Step 1: Bits Unpred. → Random Bits Unpred.

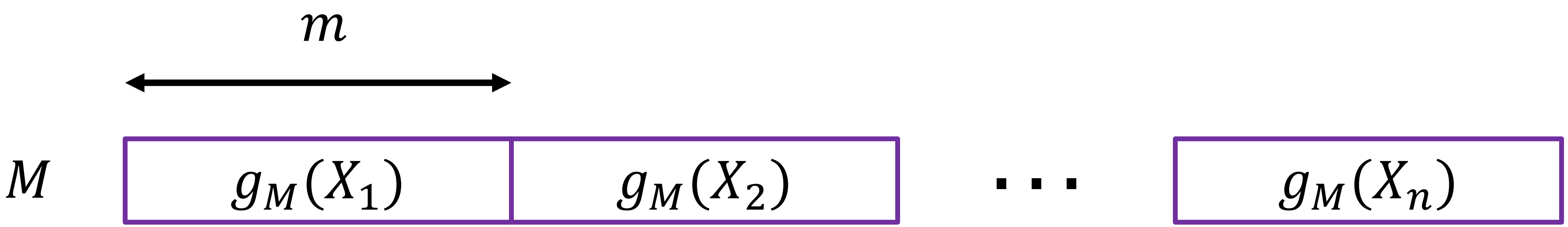
Problem: We don’t know which bits are unpredictable

- Maybe the i-th bit is always predictable

Step 1: Bits Unpred. → Random Bits Unpred.

Problem: We don't know which bits are unpredictable

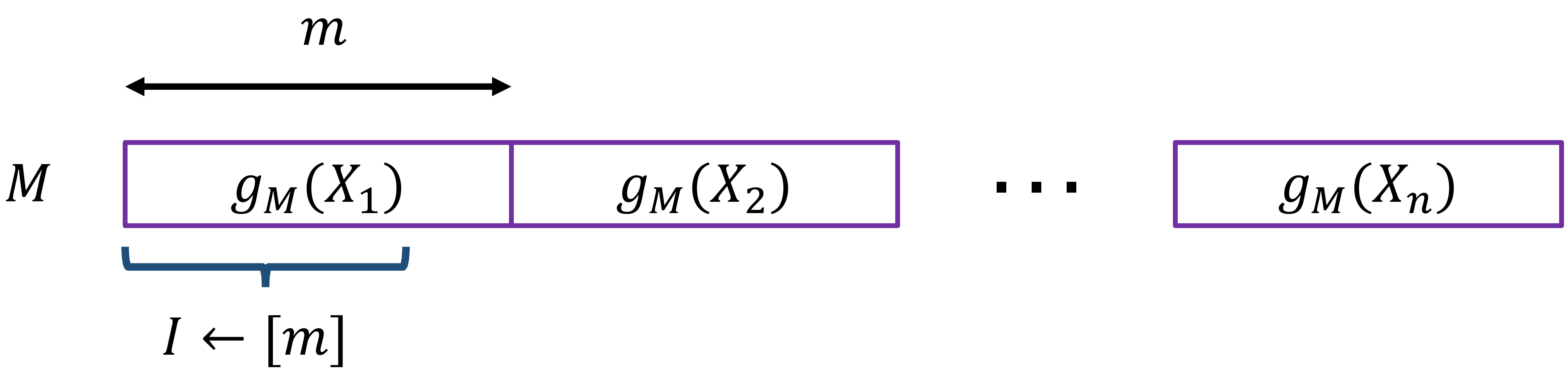
- Maybe the i-th bit is always predictable



Step 1: Bits Unpred. → Random Bits Unpred.

Problem: We don’t know which bits are unpredictable

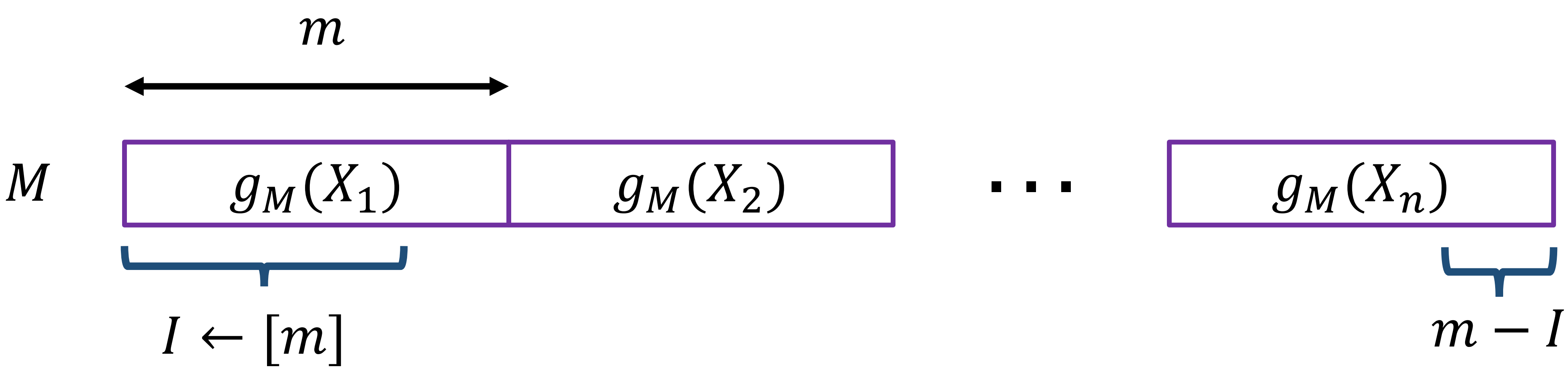
- Maybe the i-th bit is always predictable



Step 1: Bits Unpred. → Random Bits Unpred.

Problem: We don't know which bits are unpredictable

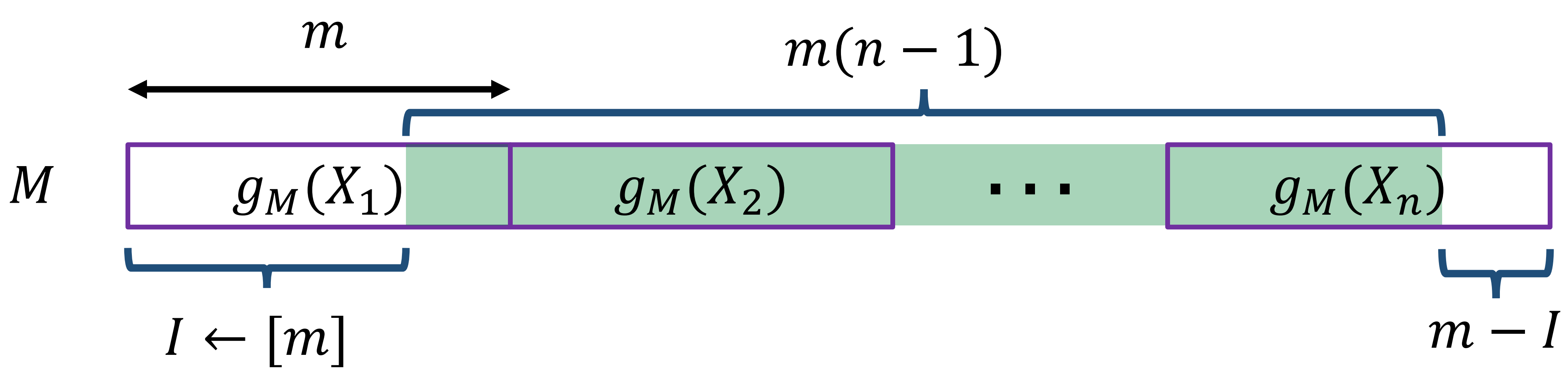
- Maybe the i-th bit is always predictable



Step 1: Bits Unpred. → Random Bits Unpred.

Problem: We don't know which bits are unpredictable

- Maybe the i-th bit is always predictable



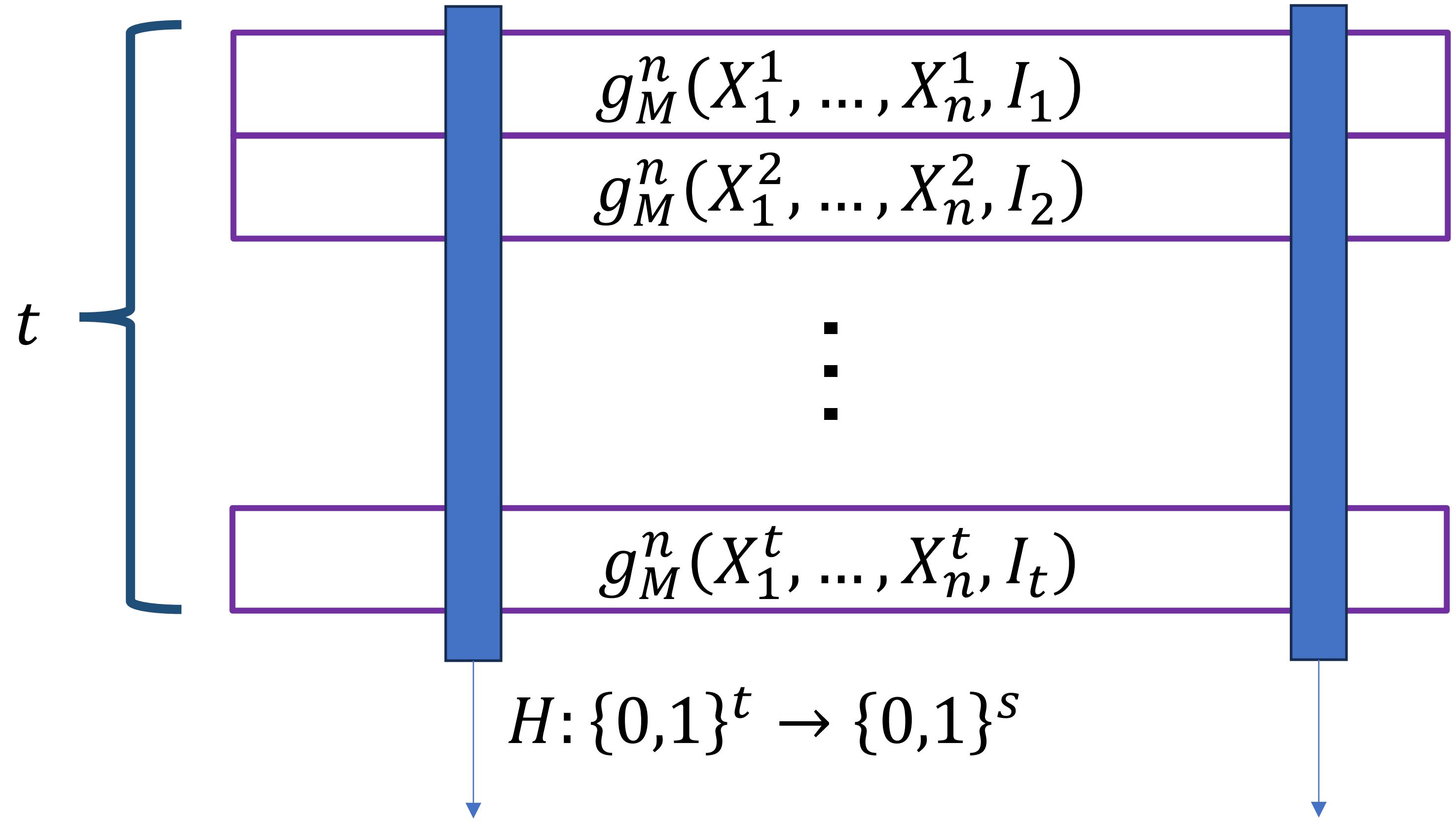
$$g_M^n(X_1, \ldots, X_n, I) = g_M(X_1)_{\geq I}, g_M(X_2), \ldots, g_M(X_n)_{<I}$$

Step 2: Extraction

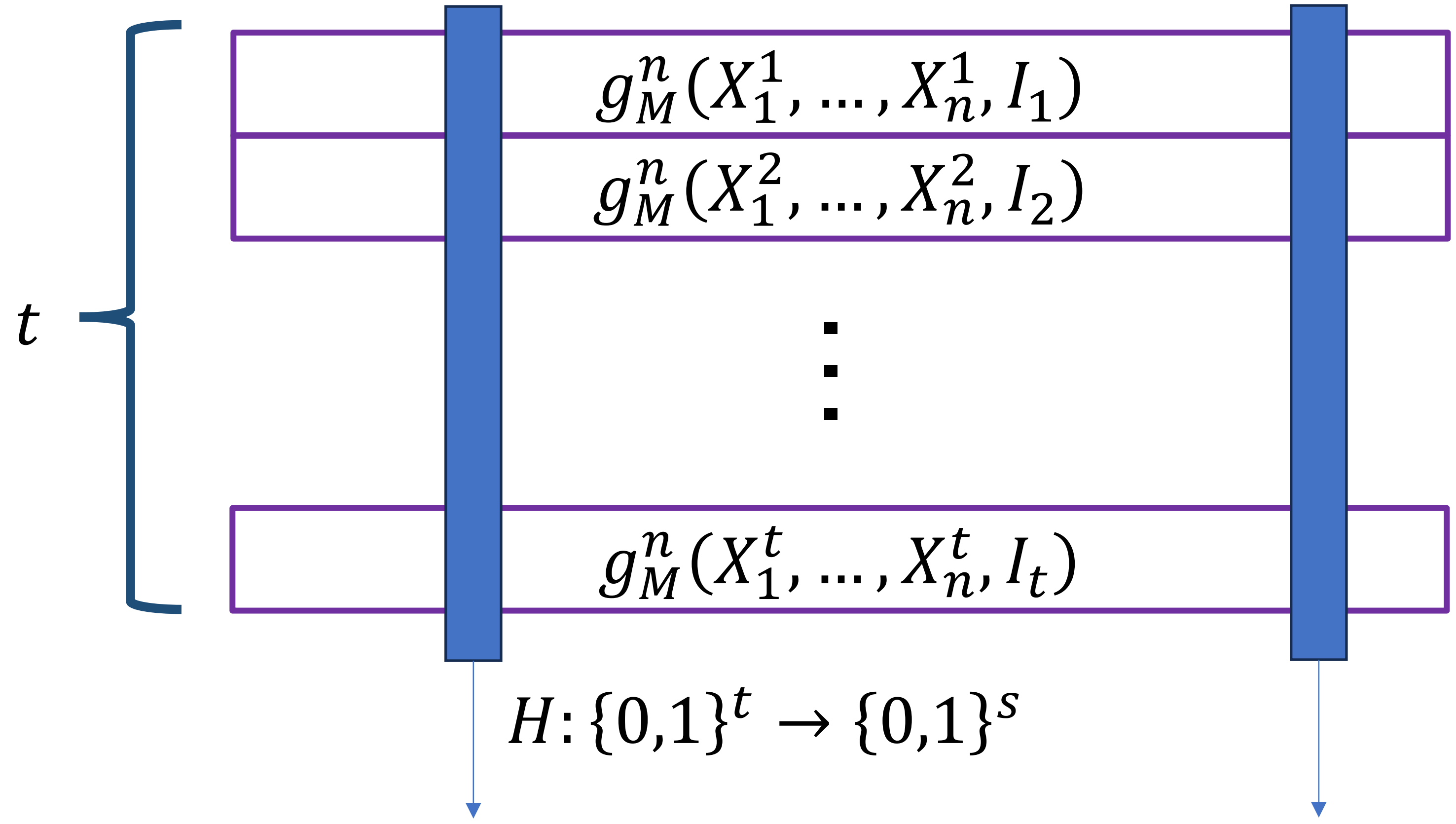
Step 2: Extraction

$$
t\left\{
\begin{array}{c}
\boxed{g_M^n(X_1^1, \dots, X_n^1, I_1)} \\
\boxed{g_M^n(X_1^2, \dots, X_n^2, I_2)} \\
\vdots \\
\boxed{g_M^n(X_1^t, \dots, X_n^t, I_t)}
\end{array}
\right.
$$

Step 2: Extraction



Step 2: Extraction



Here we improve parameters over [HRV]

Summary

Summary

Bits Unpredictabilty

Summary

Bits Unpredictabilty

- Simpler Proof

Summary

Bits Unpredictabilty

- Simpler Proof
- Better Parameters

Summary

Bits Unpredictabilty

- Simpler Proof
- Better Parameters

OWF → Bits Unpredictability

Summary

Bits Unpredictabilty

- Simpler Proof
- Better Parameters

OWF → Bits Unpredictability

- $g_M(\mathrm{X}) = \mathrm{M}\big(\mathrm{f}(\mathrm{X})\big), \mathrm{M}(\mathrm{X})$

Summary

Bits Unpredictabilty

- Simpler Proof
- Better Parameters

OWF → Bits Unpredictability

- $g_M(\mathrm{X}) = \mathrm{M}\big(\mathrm{f}(\mathrm{X})\big), \mathrm{M}(\mathrm{X})$

Bits Unpredictabity → PRG

Summary

Bits Unpredictabilty

- Simpler Proof
- Better Parameters

OWF $\rightarrow$ Bits Unpredictability

- $g_M(\mathrm{X}) = \mathrm{M}\big(\mathrm{f}(\mathrm{X})\big), \mathrm{M}(\mathrm{X})$

Bits Unpredictabity $\rightarrow$ PRG

<u>Question</u>: Simplifying other proofs/constructions

Summary

Bits Unpredictabilty

- Simpler Proof
- Better Parameters

OWF → Bits Unpredictability

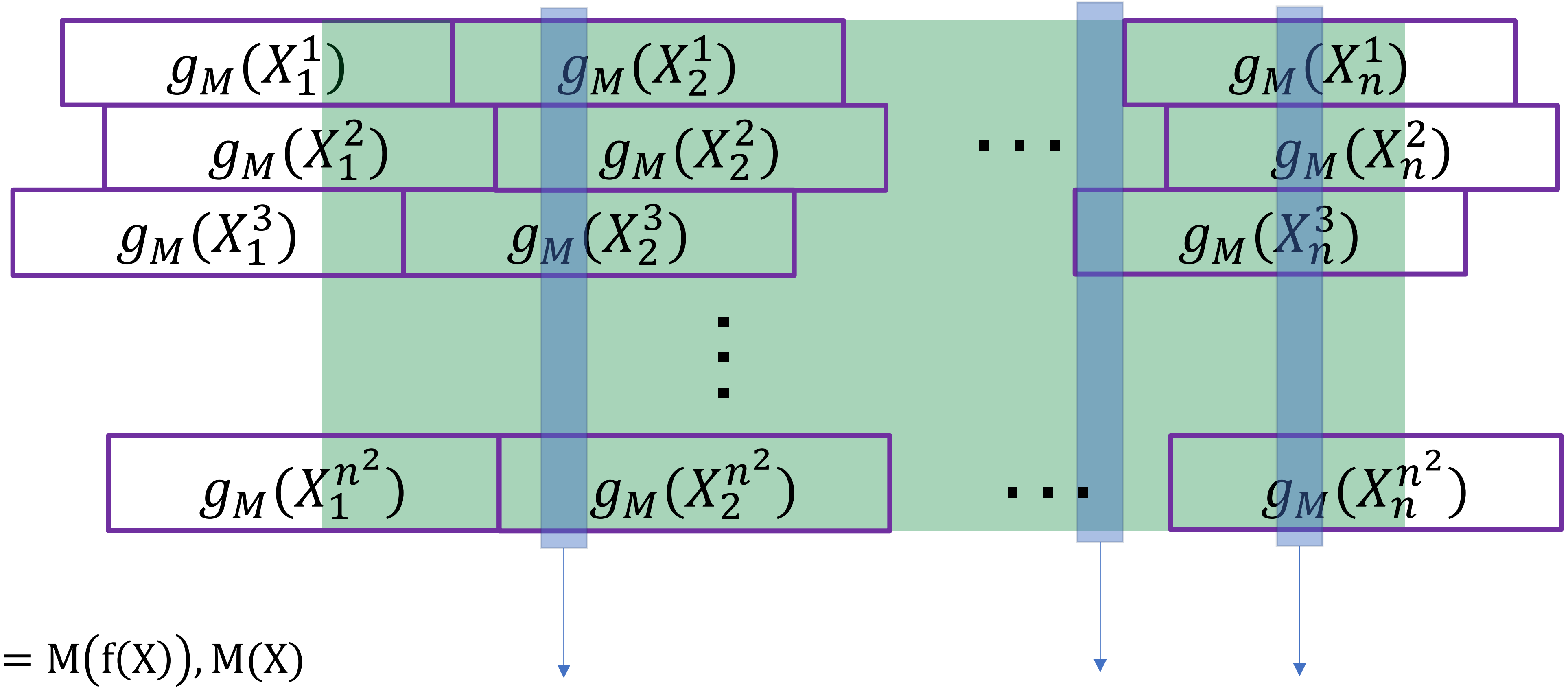
- $g_M(\mathrm{X}) = \mathrm{M}\big(\mathrm{f}(\mathrm{X})\big), \mathrm{M}(\mathrm{X})$

Bits Unpredictabity → PRG

<u>Question</u>: Simplifying other proofs/constructions

Thanks!

The Final Construction



$g_M(\mathrm{X}) = \mathrm{M}\big(\mathrm{f}(\mathrm{X})\big), \mathrm{M}(\mathrm{X})$

Bits Unpredictability – Formal Definition

Def:

$g_M: \{0,1\}^n \to \{0,1\}^m$ has k bit unpredictability if the following holds for every $\epsilon \in 1/poly$.

For every $x \in \{0,1\}^n$ there exists a set $S_x \subseteq [m]$, such that $|S_x| \geq k$, and,

$$\Pr_{\mathrm{M,X}}[P(M, g_M(X)_{<i}) = g_M(X)_i \mid i \in S_X] \leq \frac{1}{2} + \epsilon$$

For *any* PPT P.