Hard Core Predicates

601.642/442: Modern Cryptography

Fall 2020

Last Time

- Proof via Reduction: $f_\times$ is a weak OWF
- Amplification: From weak to strong OWFs

Today

- Hard Core Predicate
- 1-bit stretch PRGs from hard core predicate.

What OWFs Hide

- OWFs guarantee that $f(x)$ hides x but nothing more!

What OWFs Hide

- OWFs guarantee that $f(x)$ hides x but nothing more!
  - E.g., it may not hide first bit of x,

What OWFs Hide

- OWFs guarantee that $f(x)$ hides x but nothing more!
  - E.g., it may not hide first bit of x,
  - Or even first half bits of x

What OWFs Hide

- OWFs guarantee that $f(x)$ hides x but nothing more!
  - E.g., it may not hide first bit of x,
  - Or even first half bits of x
- In fact: if $\mathbf{a}(x)$ is any non-trivial information about x, we don't know if $f(x)$ will hide it (except when $\mathbf{a}(x) = x$)

What OWFs Hide

- OWFs guarantee that $f(x)$ hides x but nothing more!
  - E.g., it may not hide first bit of x,
  - Or even first half bits of x
- In fact: if $\mathbf{a}(x)$ is any non-trivial information about x, we don't know if $f(x)$ will hide it (except when $\mathbf{a}(x) = x$)

Is there any non-trivial (non-identity) function of x, even 1 bit, that OWFs hide?

Hard Core Predicate

- A **hard core predicate** for a OWF f

Hard Core Predicate

- A **hard core predicate** for a OWF f
  - is a function over its inputs $\{x\}$

Hard Core Predicate

- A **hard core predicate** for a OWF f
  - is a function over its inputs $\{x\}$
  - its output is a single bit (called "hard core bit")

Hard Core Predicate

- A **hard core predicate** for a OWF f
  - is a function over its inputs $\{x\}$
  - its output is a single bit (called "hard core bit")
  - it can be easily computed given x

Hard Core Predicate

- A **hard core predicate** for a OWF f
  - is a function over its inputs $\{x\}$
  - its output is a single bit (called "hard core bit")
  - it can be easily computed given x
  - but "hard to compute" given only $f(x)$

Hard Core Predicate

- A **hard core predicate** for a OWF f
  - is a function over its inputs $\{x\}$
  - its output is a single bit (called "hard core bit")
  - it can be easily computed given x
  - but "hard to compute" given only $f(x)$
- Intuition: f may leak many bits of x but it does not leak the hard-core bit.
- In other words, learning the hardcore bit of x, even given $f(x)$, is "as hard as" inverting f itself.

Hard Core Predicate

- A **hard core predicate** for a OWF f
  - is a function over its inputs $\{x\}$
  - its output is a single bit (called "hard core bit")
  - it can be easily computed given x
  - but "hard to compute" given only $f(x)$
- Intuition: f may leak many bits of x but it does not leak the hard-core bit.
- In other words, learning the hardcore bit of x, even given $f(x)$, is "as hard as" inverting f itself.
- Think: What does "hard to compute" mean for a single bit?

Hard Core Predicate

- A **hard core predicate** for a OWF f
  - is a function over its inputs $\{x\}$
  - its output is a single bit (called "hard core bit")
  - it can be easily computed given x
  - but "hard to compute" given only $f(x)$
- Intuition: f may leak many bits of x but it does not leak the hard-core bit.
- In other words, learning the hardcore bit of x, even given $f(x)$, is "as hard as" inverting f itself.
- Think: What does "hard to compute" mean for a single bit?
  - you can always guess the bit with probability 1/2.

Hard Core Predicate: Definition

- Hard-core bit cannot be learned or "predicted" or "computed" with probability $> \frac{1}{2} + \nu(|x|)$ even given $f(x)$ (where ν is a negligible function)

Hard Core Predicate: Definition

- Hard-core bit cannot be learned or "predicted" or "computed" with probability $> \frac{1}{2} + \nu(|x|)$ even given $f(x)$ (where ν is a negligible function)

Definition (Hard Core Predicate)

A predicate $h : \{0,1\}^* \to \{0,1\}$ is a hard-core predicate for $f(\cdot)$ if h is efficiently computable given x and there exists a negligible function ν s.t. for every non-uniform PPT adversary $\mathcal{A}$ and $\forall n \in \mathbb{N}$:

$$\Pr\left[x \leftarrow \{0,1\}^n : \mathcal{A}(1^n, f(x)) = h(x)\right] \leqslant \frac{1}{2} + \nu(n).$$

Hard Core Predicate: Definition

- Hard-core bit cannot be learned or "predicted" or "computed" with probability $> \frac{1}{2} + \nu(|x|)$ even given $f(x)$ (where ν is a negligible function)

Definition (Hard Core Predicate)

A predicate $h : \{0,1\}^* \to \{0,1\}$ is a hard-core predicate for $f(\cdot)$ if h is efficiently computable given x and there exists a negligible function ν s.t. for every non-uniform PPT adversary $\mathcal{A}$ and $\forall n \in \mathbb{N}$:

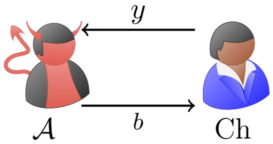
$$\Pr\left[x \leftarrow \{0,1\}^n : \mathcal{A}(1^n, f(x)) = h(x)\right] \leqslant \frac{1}{2} + \nu(n).$$

Hard Core Predicate: Game Based Definition

It is also instructive to think of that definition in this game-based form.

Hard Core Predicate: Game Based Definition

It is also instructive to think of that definition in this game-based form.

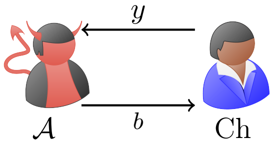


$$x \xleftarrow{\$} \{0,1\}^n$$
$$y = f(x)$$

$$\boxed{\mathcal{A} \text{ wins if } h(x) = b}$$

Hard Core Predicate: Game Based Definition

It is also instructive to think of that definition in this game-based form.



$$x \xleftarrow{\$} \{0,1\}^n$$
$$y = f(x)$$

$$\boxed{\mathcal{A} \text{ wins if } h(x) = b}$$

We want that for all n.u. PPT adversary $\mathcal{A}$, the adversary wins with probability only at most negligible more than 1/2.

$$\Pr[\mathcal{A} \text{ wins}] \leqslant \frac{1}{2} + \nu(n).$$

Hard Core Predicate: Construction

- Can we construct hard-core predicates for general OWFs f?

Hard Core Predicate: Construction

- Can we construct hard-core predicates for general OWFs f?
- Define $\langle x, r\rangle$ to be the **inner product** function mod 2. I.e:,

$$\langle x, r\rangle = \Big(\sum_i x_i r_i\Big) \mod 2$$

Hard Core Predicate: Construction

- Can we construct hard-core predicates for general OWFs f?
- Define $\langle x, r\rangle$ to be the **inner product** function mod 2. I.e:,

$$\langle x, r\rangle = \Big(\sum_i x_i r_i\Big) \mod 2$$

Theorem (Goldreich-Levin)

Let f be a OWF. Define function

$$g(x, r) = (f(x), r)$$

where $|x| = |r|$. Then g is a OWF and

$$h(x, r) = \langle x, r\rangle$$

is a hard-core predicate for f

Proof?

- Proof via Reduction?

Proof?

- Proof via Reduction?
- **Main challenge**: Adversary $\mathcal{A}$ for h only outputs 1 bit. Need to build an inverter $\mathcal{B}$ for f that outputs n bits.

Warmup Proof (1)

- Assumption: Given $g(x, r) = (f(x), r)$, adversary $\mathcal{A}$ **always** (i.e., with probability 1) outputs $h(x, r)$ correctly

Warmup Proof (1)

- Assumption: Given $g(x, r) = (f(x), r)$, adversary $\mathcal{A}$ **always** (i.e., with probability 1) outputs $h(x, r)$ correctly
- Inverter $\mathcal{B}$:

Warmup Proof (1)

- Assumption: Given $g(x,r) = (f(x), r)$, adversary $\mathcal{A}$ **always** (i.e., with probability 1) outputs $h(x,r)$ correctly
- Inverter $\mathcal{B}$:
  - Compute $x_i^* \leftarrow \mathcal{A}(f(x), e_i)$ for every $i \in [n]$ where:

$$e_i = (\underbrace{0, \ldots, 0}_{(i-1)\text{-times}}, 1, \ldots, 0)$$

Warmup Proof (1)

- Assumption: Given $g(x, r) = (f(x), r)$, adversary $\mathcal{A}$ **always** (i.e., with probability 1) outputs $h(x, r)$ correctly
- Inverter $\mathcal{B}$:
  - Compute $x_i^* \leftarrow \mathcal{A}(f(x), e_i)$ for every $i \in [n]$ where:

$$e_i = (\underbrace{0, \ldots, 0}_{(i-1)\text{-times}}, 1, \ldots, 0)$$

  - Output $x^* = x_1^* \ldots x_n^*$

Warmup Proof (2)

- Assumption: Given $g(x, r) = (f(x), r)$, adversary $\mathcal{A}$ outputs $h(x, r)$ with probability $3/4 + \varepsilon(n)$ (over choices of (x, r))

Warmup Proof (2)

- Assumption: Given $g(x, r) = (f(x), r)$, adversary $\mathcal{A}$ outputs $h(x, r)$ with probability $3/4 + \varepsilon(n)$ (over choices of (x, r))
- **Main Problem:** Adversary may not work on "improper" inputs (e.g., $r = e_i$ as in previous case)

Warmup Proof (2)

- Assumption: Given $g(x,r) = (f(x), r)$, adversary $\mathcal{A}$ outputs $h(x,r)$ with probability $3/4 + \varepsilon(n)$ (over choices of (x,r))
- **Main Problem:** Adversary may not work on "improper" inputs (e.g., $r = e_i$ as in previous case)
- **Main Idea:** Split each query into two queries s.t. each query individually looks random

Warmup Proof (2)

- Assumption: Given $g(x, r) = (f(x), r)$, adversary $\mathcal{A}$ outputs $h(x, r)$ with probability $3/4 + \varepsilon(n)$ (over choices of (x, r))
- **Main Problem:** Adversary may not work on "improper" inputs (e.g., $r = e_i$ as in previous case)
- **Main Idea:** Split each query into two queries s.t. each query individually looks random
- Inverter $\mathcal{B}$:

Warmup Proof (2)

- Assumption: Given $g(x,r) = (f(x), r)$, adversary $\mathcal{A}$ outputs $h(x,r)$ with probability $3/4 + \varepsilon(n)$ (over choices of (x,r))
- **Main Problem:** Adversary may not work on "improper" inputs (e.g., $r = e_i$ as in previous case)
- **Main Idea:** Split each query into two queries s.t. each query individually looks random
- Inverter $\mathcal{B}$:
  - Let $a := \mathcal{A}(f(x), e_i + r)$ and $b := \mathcal{A}(f(x), r)$, for $r \xleftarrow{\$} \{0,1\}^n$

Warmup Proof (2)

- Assumption: Given $g(x,r) = (f(x), r)$, adversary $\mathcal{A}$ outputs $h(x,r)$ with probability $3/4 + \varepsilon(n)$ (over choices of (x,r))
- **Main Problem:** Adversary may not work on "improper" inputs (e.g., $r = e_i$ as in previous case)
- **Main Idea:** Split each query into two queries s.t. each query individually looks random
- Inverter $\mathcal{B}$:
    - Let $a := \mathcal{A}(f(x), e_i + r)$ and $b := \mathcal{A}(f(x), r)$, for $r \xleftarrow{\$} \{0,1\}^n$
    - Compute $c := a \oplus b$

Warmup Proof (2)

- Assumption: Given $g(x,r) = (f(x), r)$, adversary $\mathcal{A}$ outputs $h(x,r)$ with probability $3/4 + \varepsilon(n)$ (over choices of (x,r))
- **Main Problem:** Adversary may not work on "improper" inputs (e.g., $r = e_i$ as in previous case)
- **Main Idea:** Split each query into two queries s.t. each query individually looks random
- Inverter $\mathcal{B}$:
  - Let $a := \mathcal{A}(f(x), e_i + r)$ and $b := \mathcal{A}(f(x), r)$, for $r \xleftarrow{\$} \{0,1\}^n$
  - Compute $c := a \oplus b$
  - $c = x_i$ with probability at least $\frac{1}{2} + \varepsilon$ (Union Bound)

Warmup Proof (2)

- Assumption: Given $g(x,r) = (f(x), r)$, adversary $\mathcal{A}$ outputs $h(x,r)$ with probability $3/4 + \varepsilon(n)$ (over choices of (x,r))
- **Main Problem:** Adversary may not work on "improper" inputs (e.g., $r = e_i$ as in previous case)
- **Main Idea:** Split each query into two queries s.t. each query individually looks random
- Inverter $\mathcal{B}$:
  - Let $a := \mathcal{A}(f(x), e_i + r)$ and $b := \mathcal{A}(f(x), r)$, for $r \xleftarrow{\$} \{0,1\}^n$
  - Compute $c := a \oplus b$
  - $c = x_i$ with probability at least $\frac{1}{2} + \varepsilon$ (Union Bound)
  - Repeat and take majority to obtain x_i^* s.t. $x_i^* = x_i$ with prob. $1 - \mathsf{negl}(n)(n)$

Warmup Proof (2)

- Assumption: Given $g(x,r) = (f(x), r)$, adversary $\mathcal{A}$ outputs $h(x,r)$ with probability $3/4 + \varepsilon(n)$ (over choices of (x,r))
- **Main Problem:** Adversary may not work on "improper" inputs (e.g., $r = e_i$ as in previous case)
- **Main Idea:** Split each query into two queries s.t. each query individually looks random
- Inverter $\mathcal{B}$:
  - Let $a := \mathcal{A}(f(x), e_i + r)$ and $b := \mathcal{A}(f(x), r)$, for $r \xleftarrow{\$} \{0,1\}^n$
  - Compute $c := a \oplus b$
  - $c = x_i$ with probability at least $\frac{1}{2} + \varepsilon$ (Union Bound)
  - Repeat and take majority to obtain x_i^* s.t. $x_i^* = x_i$ with prob. $1 - \mathsf{negl}(n)(n)$
  - Output $x^* = x_1^* \ldots x_n^*$

Full Proof

Try on your own

Full Proof

Try on your own (or read from lecture notes)

Full Proof

Try on your own (or read from lecture notes)

- Goldreich-Levin Theorem extremely influential even outside cryptography

Full Proof

Try on your own (or read from lecture notes)

- Goldreich-Levin Theorem extremely influential even outside cryptography
- Applications to learning, list-decoding codes, extractors,...

Full Proof

Try on your own (or read from lecture notes)

- Goldreich-Levin Theorem extremely influential even outside cryptography
- Applications to learning, list-decoding codes, extractors,...
- Extremely useful tool to add to your toolkit

One-Way Functions: Remarks

- One-way functions are necessary for most of cryptography

One-Way Functions: Remarks

- One-way functions are necessary for most of cryptography
- But often not sufficient. Black-box separations known [Impagliazzo-Rudich'89]; full separations not known

One-Way Functions: Remarks

- One-way functions are necessary for most of cryptography
- But often not sufficient. Black-box separations known [Impagliazzo-Rudich'89]; full separations not known
- Additional Reading: Universal One-way Functions

One-Way Functions: Remarks

- One-way functions are necessary for most of cryptography
- But often not sufficient. Black-box separations known [Impagliazzo-Rudich'89]; full separations not known
- Additional Reading: Universal One-way Functions
  - Suppose somebody tells you that OWFs exist! E.g., they might discover a proof for it!

One-Way Functions: Remarks

- One-way functions are necessary for most of cryptography
- But often not sufficient. Black-box separations known [Impagliazzo-Rudich'89]; full separations not known
- Additional Reading: Universal One-way Functions
  - Suppose somebody tells you that OWFs exist! E.g., they might discover a proof for it!
  - But they don't tell you what this function is. E.g., even they might not know the function! They just have a proof of its existence...

One-Way Functions: Remarks

- One-way functions are necessary for most of cryptography
- But often not sufficient. Black-box separations known [Impagliazzo-Rudich'89]; full separations not known
- Additional Reading: Universal One-way Functions
  - Suppose somebody tells you that OWFs exist! E.g., they might discover a proof for it!
  - But they don't tell you what this function is. E.g., even they might not know the function! They just have a proof of its existence...
  - Can you use this fact to build an **explicit** OWF?

One-Way Functions: Remarks

- One-way functions are necessary for most of cryptography
- But often not sufficient. Black-box separations known [Impagliazzo-Rudich'89]; full separations not known
- Additional Reading: Universal One-way Functions
  - Suppose somebody tells you that OWFs exist! E.g., they might discover a proof for it!
  - But they don't tell you what this function is. E.g., even they might not know the function! They just have a proof of its existence...
  - Can you use this fact to build an **explicit** OWF?
  - Yes! Levin gives us a method!

Back to PRGs

(How to construct PRGs with 1-bit stretch)

Pseudorandomness: Next-Bit Test

- Here is another interesting way to talk about pseudorandomness

Pseudorandomness: Next-Bit Test

- Here is another interesting way to talk about pseudorandomness
- A pseudorandom string should pass all efficient tests that a (truly) random string would pass

Pseudorandomness: Next-Bit Test

- Here is another interesting way to talk about pseudorandomness
- A pseudorandom string should pass all efficient tests that a (truly) random string would pass
- **Next Bit Test**: for a truly random sequence of bits, it is not possible to predict the "next bit" in the sequence with probability better than 1/2 even given all previous bits of the sequence so far

Pseudorandomness: Next-Bit Test

- Here is another interesting way to talk about pseudorandomness
- A pseudorandom string should pass all efficient tests that a (truly) random string would pass
- **Next Bit Test**: for a truly random sequence of bits, it is not possible to predict the "next bit" in the sequence with probability better than 1/2 even given all previous bits of the sequence so far
- A sequence of bits *passes the next bit test* if no efficient adversary can predict "the next bit" in the sequence with probability better than 1/2 even given all previous bits of the sequence so far

Next-bit Unpredictability

Definition (Next-bit Unpredictability)

An ensemble of distributions $\{X_n\}$ over $\{0,1\}^{\ell(n)}$ is next-bit unpredictable if, for all $0 \leqslant i < \ell(n)$ and n.u. PPT $\mathcal{A}$, $\exists$ negligible function $\nu(\cdot)$ s.t.:

$$\Pr[t = t_1 \dots t_{\ell(n)} \leftarrow X_n \colon \mathcal{A}(t_1 \dots t_i) = t_{i+1}] \leqslant \frac{1}{2} + \nu(n)$$

Next-bit Unpredictability

Definition (Next-bit Unpredictability)

An ensemble of distributions $\{X_n\}$ over $\{0,1\}^{\ell(n)}$ is next-bit unpredictable if, for all $0 \leqslant i < \ell(n)$ and n.u. PPT $\mathcal{A}$, $\exists$ negligible function $\nu(\cdot)$ s.t.:

$$\Pr[t = t_1 \dots t_{\ell(n)} \leftarrow X_n \colon \mathcal{A}(t_1 \dots t_i) = t_{i+1}] \leqslant \frac{1}{2} + \nu(n)$$

Theorem (Completeness of Next-bit Test)

If $\{X_n\}$ is next-bit unpredictable then $\{X_n\}$ is pseudorandom.

Next-bit Unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{x \leftarrow X_n, u \leftarrow U_n : x_1 \ldots x_i u_{i+1} \ldots u_{\ell(n)}\right\}$$

Next-bit Unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{x \leftarrow X_n, u \leftarrow U_n : x_1 \ldots x_i u_{i+1} \ldots u_{\ell(n)}\right\}$$

- First Hybrid: H_n^0 is the uniform distribution $U_{\ell(n)}$

Next-bit Unpredictability $\Longrightarrow$ Pseudorandomness

$$H_n^{(i)} := \left\{x \leftarrow X_n, u \leftarrow U_n : x_1 \ldots x_i u_{i+1} \ldots u_{\ell(n)}\right\}$$

- First Hybrid: H_n^0 is the uniform distribution $U_{\ell(n)}$
- Last Hybrid: $H_n^{\ell(n)}$ is the distribution X_n

Next-bit Unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{x \leftarrow X_n, u \leftarrow U_n : x_1 \ldots x_i u_{i+1} \ldots u_{\ell(n)}\right\}$$

- First Hybrid: H_n^0 is the uniform distribution $U_{\ell(n)}$
- Last Hybrid: $H_n^{\ell(n)}$ is the distribution X_n
- Suppose $H_n^{(\ell(n))}$ is next-bit unpredictable but not pseudorandom

Next-bit Unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{x \leftarrow X_n, u \leftarrow U_n : x_1 \dots x_i u_{i+1} \dots u_{\ell(n)}\right\}$$

- First Hybrid: H_n^0 is the uniform distribution $U_{\ell(n)}$
- Last Hybrid: $H_n^{\ell(n)}$ is the distribution X_n
- Suppose $H_n^{(\ell(n))}$ is next-bit unpredictable but not pseudorandom
- $H_n^{(0)} \not\approx H_n^{(\ell(n))} \implies \exists\ i \in [\ell(n)-1]$ s.t. $H_n^{(i)} \not\approx H_n^{(i+1)}$

Next-bit Unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{x \leftarrow X_n, u \leftarrow U_n : x_1 \dots x_i u_{i+1} \dots u_{\ell(n)}\right\}$$

- First Hybrid: H_n^0 is the uniform distribution $U_{\ell(n)}$
- Last Hybrid: $H_n^{\ell(n)}$ is the distribution X_n
- Suppose $H_n^{(\ell(n))}$ is next-bit unpredictable but not pseudorandom
- $H_n^{(0)} \not\approx H_n^{(\ell(n))} \implies \exists\ i \in [\ell(n)-1]$ s.t. $H_n^{(i)} \not\approx H_n^{(i+1)}$
- Now, next bit unpredictability is violated

Next-bit Unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{x \leftarrow X_n, u \leftarrow U_n : x_1 \ldots x_i u_{i+1} \ldots u_{\ell(n)}\right\}$$

- First Hybrid: H_n^0 is the uniform distribution $U_{\ell(n)}$
- Last Hybrid: $H_n^{\ell(n)}$ is the distribution X_n
- Suppose $H_n^{(\ell(n))}$ is next-bit unpredictable but not pseudorandom
- $H_n^{(0)} \not\approx H_n^{(\ell(n))} \implies \exists\ i \in [\ell(n) - 1]$ s.t. $H_n^{(i)} \not\approx H_n^{(i+1)}$
- Now, next bit unpredictability is violated
- <u>Exercise</u>: Do the full formal proof

PRG with 1-bit stretch

- Hardcore predicate: It is hard to guess $h(s)$ even given $f(s)$

PRG with 1-bit stretch

- Hardcore predicate: It is hard to guess $h(s)$ even given $f(s)$
- Let $G(s) = f(s) \| h(s)$ where f is a OWF

PRG with 1-bit stretch

- Hardcore predicate: It is hard to guess $h(s)$ even given $f(s)$
- Let $G(s) = f(s) \| h(s)$ where f is a OWF
- Some small issues:

PRG with 1-bit stretch

- Hardcore predicate: It is hard to guess $h(s)$ even given $f(s)$
- Let $G(s) = f(s) \| h(s)$ where f is a OWF
- Some small issues:
  - $|f(s)|$ might be less than $|s|$

PRG with 1-bit stretch

- Hardcore predicate: It is hard to guess $h(s)$ even given $f(s)$
- Let $G(s) = f(s) \| h(s)$ where f is a OWF
- Some small issues:
  - $|f(s)|$ might be less than $|s|$
  - $f(s)$ may always start with prefix 101 (not random)

PRG with 1-bit stretch

- Hardcore predicate: It is hard to guess $h(s)$ even given $f(s)$
- Let $G(s) = f(s)\|h(s)$ where f is a OWF
- Some small issues:
  - $|f(s)|$ might be less than $|s|$
  - $f(s)$ may always start with prefix 101 (not random)
- **Solution:** let f be a one-way permutation (OWP) over $\{0,1\}^n$

PRG with 1-bit stretch

- Hardcore predicate: It is hard to guess $h(s)$ even given $f(s)$
- Let $G(s) = f(s) \| h(s)$ where f is a OWF
- Some small issues:
  - $|f(s)|$ might be less than $|s|$
  - $f(s)$ may always start with prefix 101 (not random)
- **Solution:** let f be a one-way permutation (OWP) over $\{0,1\}^n$
  - Domain and Range are of same size, i.e., $|f(s)| = |s| = n$

PRG with 1-bit stretch

- Hardcore predicate: It is hard to guess $h(s)$ even given $f(s)$
- Let $G(s) = f(s) \| h(s)$ where f is a OWF
- Some small issues:
  - $|f(s)|$ might be less than $|s|$
  - $f(s)$ may always start with prefix 101 (not random)
- **Solution:** let f be a one-way permutation (OWP) over $\{0,1\}^n$
  - Domain and Range are of same size, i.e., $|f(s)| = |s| = n$
  - $f(s)$ is uniformly distributed over $\{0,1\}^n$ if s is

PRG with 1-bit stretch

- Hardcore predicate: It is hard to guess $h(s)$ even given $f(s)$
- Let $G(s) = f(s)\|h(s)$ where f is a OWF
- Some small issues:
  - $|f(s)|$ might be less than $|s|$
  - $f(s)$ may always start with prefix 101 (not random)
- **Solution:** let f be a one-way permutation (OWP) over $\{0,1\}^n$
  - Domain and Range are of same size, i.e., $|f(s)| = |s| = n$
  - $f(s)$ is uniformly distributed over $\{0,1\}^n$ if s is

    $\forall y : \Pr[f(s) = y] = \Pr[s = f^{-1}(y)] = 2^{-n}$

PRG with 1-bit stretch

- Hardcore predicate: It is hard to guess $h(s)$ even given $f(s)$
- Let $G(s) = f(s)\|h(s)$ where f is a OWF
- Some small issues:
  - $|f(s)|$ might be less than $|s|$
  - $f(s)$ may always start with prefix 101 (not random)
- **Solution:** let f be a one-way permutation (OWP) over $\{0,1\}^n$
  - Domain and Range are of same size, i.e., $|f(s)| = |s| = n$
  - $f(s)$ is uniformly distributed over $\{0,1\}^n$ if s is

    $\forall y : \Pr[f(s) = y] = \Pr[s = f^{-1}(y)] = 2^{-n}$

    $\Rightarrow f(s)$ is uniformly distributed

PRG with 1-bit stretch

- Let $f : \{0,1\}^* \rightarrow \{0,1\}^*$ be a **OWP**
- Let $h : \{0,1\}^* \rightarrow \{0,1\}$ be a hardcore predicate for f
- **Construction:** $G(s) = f(s) \parallel h(s)$

PRG with 1-bit stretch

- Let $f : \{0,1\}^* \to \{0,1\}^*$ be a **OWP**
- Let $h : \{0,1\}^* \to \{0,1\}$ be a hardcore predicate for f
- **Construction:** $G(s) = f(s) \parallel h(s)$

Theorem (PRG based on OWP)

G is a pseudorandom generator with 1-bit stretch.

- Think: Proof?

PRG with 1-bit stretch

- Let $f : \{0,1\}^* \to \{0,1\}^*$ be a **OWP**
- Let $h : \{0,1\}^* \to \{0,1\}$ be a hardcore predicate for f
- **Construction:** $G(s) = f(s) \parallel h(s)$

Theorem (PRG based on OWP)

G is a pseudorandom generator with 1-bit stretch.

- Think: Proof?
- Proof Idea: Use next-bit unpredictability. Since first n bits of the output are uniformly distributed (since f is a permutation), any adversary for next-bit unpredictability with non-negligible advantage $\frac{1}{p(n)}$ must be predicting the $(n+1)$th bit with advantage $\frac{1}{p(n)}$. Build an adversary for hard-core predicate to get a contradiction.