One-Way Functions and Hardcore Predicates

Iftach Haitner, Tel Aviv University

Bar-Ilan Winter School

January 27, 2014

Today's Plan

1. One-way functions and hardcore predicates
2. Pseudorandom generators
3. Pseudorandom functions and permutations
4. Symmetric encryption and MACs.

Online Material

Books:

- Oded Goldreich. Foundations of Cryptography
  http://www.wisdom.weizmann.ac.il/~oded/foc-book.html

Online Material

Books:

- Oded Goldreich. Foundations of Cryptography
  http://www.wisdom.weizmann.ac.il/~oded/foc-book.html

Lecture notes:

- Ran Canetti http://www.cs.tau.ac.il/~canetti/f08.html
- Iftach Haitner http://www.cs.tau.ac.il/~iftachh/Courses/FOC/Spring13/index.html
- Yehuda Lindell http://u.cs.biu.ac.il/~lindell/89-856/main-89-856.html
- Luca Trevisan http://www.cs.berkeley.edu/~daw/cs276/
- Salil Vadhan
  http://people.seas.harvard.edu/~salil/cs120/

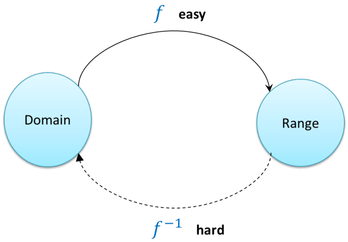
Before we Begin

- We assume basic knowledge of probability theory and computational models, yet please ask us if something is unclear
- We sometimes skip some details (left as exercises for you :-)) and sometimes slightly cheat (we'll clearly mark when)
- Slides are slightly different from your version.
- Please ask questions

Part I

One-Way Functions

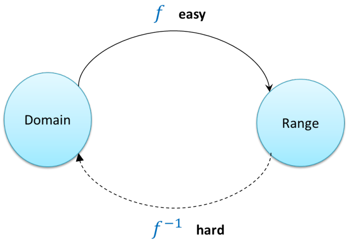
Informal Discussion



A one-way function (OWF) is:

- Easy to compute, everywhere
- Hard to invert, on the average

Informal Discussion

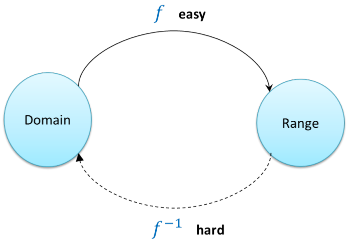


A one-way function (OWF) is:

- Easy to compute, everywhere
- Hard to invert, on the average

- Why should we care about OWFs?

Informal Discussion

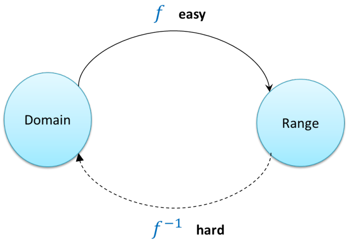


A one-way function (OWF) is:

- Easy to compute, everywhere
- Hard to invert, on the average

- Why should we care about OWFs?
- Hidden in (almost) any cryptographic primitive: necessary for "cryptography"

Informal Discussion



A one-way function (OWF) is:

- Easy to compute, everywhere
- Hard to invert, on the average

- Why should we care about OWFs?
- Hidden in (almost) any cryptographic primitive: necessary for "cryptography"
- Sufficient for many cryptographic primitives

Formal Definition

Definition 1 (one-way functions (OWFs))

A polynomial-time computable function $f\colon \{0,1\}^* \mapsto \{0,1\}^*$ is one-way, if

$$\Pr_{x \xleftarrow{R} \{0,1\}^n} \left[A(1^n, f(x)) \in f^{-1}(f(x)) \right] = \text{neg}(n)$$

for any PPT A.

polynomial-time computable: there exists polynomial-time algorithm F, such that $F(x) = f(x)$ for every $x \in \{0,1\}^*$

neg: a function $\mu \colon \mathbb{N} \mapsto [0,1]$ is a negligible function of n, denoted $\mu(n) = \text{neg}(n)$, if for any $p \in \text{poly}$ there exists $n' \in \mathbb{N}$ such that $\mu(n) < 1/p(n)$ for all $n > n'$

$x \xleftarrow{R} \{0,1\}^n$: x is uniformly drawn from $\{0,1\}^n$

PPT: probabilistic polynomial-time algorithm

We typically omit 1^n from the input list of A

Formal Definition

Definition 1 (one-way functions (OWFs))

A polynomial-time computable function $f\colon \{0,1\}^* \mapsto \{0,1\}^*$ is one-way, if

$$\Pr_{x \xleftarrow{R} \{0,1\}^n} \left[\mathsf{A}(1^n, f(x)) \in f^{-1}(f(x)) \right] = \operatorname{neg}(n)$$

for any PPT A.

- Efficiently computable function

Formal Definition

Definition 1 (one-way functions (OWFs))

A polynomial-time computable function $f\colon \{0,1\}^* \mapsto \{0,1\}^*$ is one-way, if

$$\Pr_{x \xleftarrow{R} \{0,1\}^n}\left[\mathsf{A}(1^n, f(x)) \in f^{-1}(f(x))\right] = \operatorname{neg}(n)$$

for any PPT A.

- Efficiently computable function
- Hard on the average

Formal Definition

Definition 1 (one-way functions (OWFs))

A polynomial-time computable function $f\colon \{0,1\}^* \mapsto \{0,1\}^*$ is one-way, if

$$\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n}\left[\mathsf{A}(1^n, f(x)) \in f^{-1}(f(x))\right] = \operatorname{neg}(n)$$

for any PPT A.

- Efficiently computable function
- Hard on the average
- Negligible inversion probability (i.e., $< 1/\operatorname{poly}(n)$)

Formal Definition

Definition 1 (one-way functions (OWFs))

A polynomial-time computable function $f\colon \{0,1\}^* \mapsto \{0,1\}^*$ is one-way, if

$$\Pr_{x \xleftarrow{R} \{0,1\}^n} \left[\mathsf{A}(1^n, f(x)) \in f^{-1}(f(x)) \right] = \operatorname{neg}(n)$$

for any PPT A.

- Efficiently computable function
- Hard on the average
- Negligible inversion probability (i.e., $< 1/\operatorname{poly}(n)$)
- PPT— probabilistic polynomial-time algorithm

Formal Definition

Definition 1 (one-way functions (OWFs))

A polynomial-time computable function $f\colon \{0,1\}^* \mapsto \{0,1\}^*$ is one-way, if

$$\Pr_{x \xleftarrow{R} \{0,1\}^n}\left[\mathsf{A}(1^n, f(x)) \in f^{-1}(f(x))\right] = \operatorname{neg}(n)$$

for any PPT A.

- Efficiently computable function
- Hard on the average
- Negligible inversion probability (i.e., $< 1/\operatorname{poly}(n)$)
- PPT— probabilistic polynomial-time algorithm
- Asymptotic

Non-Uniform OWFs

Definition 2 (non-uniform OWFs)

A polynomial-time computable function $f : \{0,1\}^* \mapsto \{0,1\}^*$ is non-uniformly one-way, if

$$\Pr_{x \xleftarrow{R} \{0,1\}^n} \left[C_n(f(x)) \in f^{-1}(f(x)) \right] = \operatorname{neg}(n)$$

for any polynomial-size family of circuits $\{C_n\}_{n \in \mathbb{N}}$.

Non-Uniform OWFs

Definition 2 (non-uniform OWFs)

A polynomial-time computable function $f : \{0,1\}^* \mapsto \{0,1\}^*$ is non-uniformly one-way, if

$$\Pr_{x \xleftarrow{R} \{0,1\}^n} \left[C_n(f(x)) \in f^{-1}(f(x))\right] = \text{neg}(n)$$

for any polynomial-size family of circuits $\{C_n\}_{n \in \mathbb{N}}$.

Implies the uniform version

Non-Uniform OWFs

Definition 2 (non-uniform OWFs)

A polynomial-time computable function $f : \{0,1\}^* \mapsto \{0,1\}^*$ is non-uniformly one-way, if

$$\Pr_{x \xleftarrow{R} \{0,1\}^n} \left[C_n(f(x)) \in f^{-1}(f(x)) \right] = \text{neg}(n)$$

for any polynomial-size family of circuits $\{C_n\}_{n \in \mathbb{N}}$.

Implies the uniform version

We will mainly focus on uniform security

Length Preserving OWF

Definition 3 (length preserving functions)

A function $f\colon \{0,1\}^* \mapsto f\colon \{0,1\}^*$ is length preserving, if $|f(x)| = |x|$ for every $x \in \{0,1\}^*$

Length Preserving OWF

Definition 3 (length preserving functions)

A function $f\colon \{0,1\}^* \mapsto f\colon \{0,1\}^*$ is length preserving, if $|f(x)| = |x|$ for every $x \in \{0,1\}^*$

Theorem 4

Assume that OWFs exit, then there exist length-preserving OWFs

Length Preserving OWF

Definition 3 (length preserving functions)

A function $f \colon \{0,1\}^* \mapsto f \colon \{0,1\}^*$ is length preserving, if $|f(x)| = |x|$ for every $x \in \{0,1\}^*$

Theorem 4

Assume that OWFs exit, then there exist length-preserving OWFs

Proof idea: “pad" the *non* length-preserving OWF to create a length-preserving one.

Length Preserving OWF

Definition 3 (length preserving functions)

A function $f\colon \{0,1\}^* \mapsto f\colon \{0,1\}^*$ is length preserving, if $|f(x)| = |x|$ for every $x \in \{0,1\}^*$

Theorem 4

Assume that OWFs exit, then there exist length-preserving OWFs

Proof idea: “pad" the *non* length-preserving OWF to create a length-preserving one.

Convention for rest of the talk

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

Weak One-Way Functions

Weak One-Way Functions

Definition 5 (weak one-way functions)

A poly-time computable function $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ is α-one-way, if

$$\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n} \left[\mathsf{A}(1^n, f(x)) \in f^{-1}(f(x)) \right] \leq \alpha(n)$$

for any PPT A and large enough $n \in \mathbb{N}$.

Weak One-Way Functions

Definition 5 (weak one-way functions)

A poly-time computable function $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ is α-one-way, if

$$\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n}\left[A(1^n, f(x)) \in f^{-1}(f(x))\right] \leq \alpha(n)$$

for any PPT A and large enough $n \in \mathbb{N}$.

- (strong) OWF according to Definition 1, is neg-one-way according to the above definition

Weak One-Way Functions

Definition 5 (weak one-way functions)

A poly-time computable function $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ is α-one-way, if

$$\Pr_{x \xleftarrow{R} \{0,1\}^n} \left[\mathsf{A}(1^n, f(x)) \in f^{-1}(f(x)) \right] \leq \alpha(n)$$

for any PPT A and large enough $n \in \mathbb{N}$.

- (strong) OWF according to Definition 1, is neg-one-way according to the above definition
- Can we convert (i.e., amplify) weak OWFs into strong ones?

Strong to Weak OWFs

Claim 6

Assume there exists OWFs, then there exist functions that are $\frac{2}{3}$-one-way, but not (strong) one-way

Strong to Weak OWFs

Claim 6

Assume there exists OWFs, then there exist functions that are $\frac{2}{3}$-one-way, but not (strong) one-way

Proof:

Strong to Weak OWFs

Claim 6

Assume there exists OWFs, then there exist functions that are $\frac{2}{3}$-one-way, but not (strong) one-way

Proof: For a OWF f, let

$$g(x) = \begin{cases} (1, f(x)), & x_1 = 1; \\ 0, & \text{otherwise } (x_1 = 1). \end{cases}$$

Weak to Strong OWFs

Theorem 7 (weak to strong OWFs (Yao))

Assume there exist $(1 - \delta)$*-weak OWFs with* $\delta(n) \geq 1/q(n)$ *for some* $q \in \mathrm{poly}$*, then there exist (strong) one-way functions.*

Weak to Strong OWFs

Theorem 7 (weak to strong OWFs (Yao))

Assume there exist $(1-\delta)$-weak OWFs with $\delta(n) \geq 1/q(n)$ for some $q \in \text{poly}$, then there exist (strong) one-way functions.

- Idea: parallel repetition (i.e., direct product): Consider $g(x_1, \ldots, x_t) = f(x_1), \ldots, f(x_t)$ for large enough t

Weak to Strong OWFs

Theorem 7 (weak to strong OWFs (Yao))

Assume there exist $(1-\delta)$-weak OWFs with $\delta(n) \geq 1/q(n)$ for some $q \in \text{poly}$, then there exist (strong) one-way functions.

- Idea: parallel repetition (i.e., direct product): Consider $g(x_1, \ldots, x_t) = f(x_1), \ldots, f(x_t)$ for large enough t
- Motivation: if something is somewhat hard, than doing it many times is (very) hard

Weak to Strong OWFs

Theorem 7 (weak to strong OWFs (Yao))

Assume there exist $(1-\delta)$-weak OWFs with $\delta(n) \geq 1/q(n)$ for some $q \in \text{poly}$, then there exist (strong) one-way functions.

- Idea: parallel repetition (i.e., direct product): Consider $g(x_1, \ldots, x_t) = f(x_1), \ldots, f(x_t)$ for large enough t
- Motivation: if something is somewhat hard, than doing it many times is (very) hard
- But, is it really so?

Weak to Strong OWFs

Theorem 7 (weak to strong OWFs (Yao))

Assume there exist $(1-\delta)$-weak OWFs with $\delta(n) \geq 1/q(n)$ for some $q \in \text{poly}$, then there exist (strong) one-way functions.

- Idea: parallel repetition (i.e., direct product): Consider $g(x_1, \ldots, x_t) = f(x_1), \ldots, f(x_t)$ for large enough t
- Motivation: if something is somewhat hard, than doing it many times is (very) hard
- But, is it really so?

  Consider matrix multiplication: Let $A \in \mathbb{R}^{n \times n}$ and $x \in \mathbb{R}^n$

  Computing Ax takes $\Theta(n^2)$ times, but computing $A(x_1, x_2, \ldots, x_n)$ takes ...

Weak to Strong OWFs

Theorem 7 (weak to strong OWFs (Yao))

Assume there exist $(1-\delta)$-weak OWFs with $\delta(n) \geq 1/q(n)$ for some $q \in \text{poly}$, then there exist (strong) one-way functions.

- Idea: parallel repetition (i.e., direct product): Consider $g(x_1, \ldots, x_t) = f(x_1), \ldots, f(x_t)$ for large enough t
- Motivation: if something is somewhat hard, than doing it many times is (very) hard
- But, is it really so?

  Consider matrix multiplication: Let $A \in \mathbb{R}^{n \times n}$ and $x \in \mathbb{R}^n$

  Computing Ax takes $\Theta(n^2)$ times, but computing $A(x_1, x_2, \ldots, x_n)$ takes …

Weak to Strong OWFs

Theorem 7 (weak to strong OWFs (Yao))

Assume there exist $(1-\delta)$-weak OWFs with $\delta(n) \geq 1/q(n)$ for some $q \in \text{poly}$, then there exist (strong) one-way functions.

- Idea: parallel repetition (i.e., direct product): Consider $g(x_1,\ldots,x_t) = f(x_1),\ldots,f(x_t)$ for large enough t
- Motivation: if something is somewhat hard, than doing it many times is (very) hard
- But, is it really so?

  Consider matrix multiplication: Let $A \in \mathbb{R}^{n\times n}$ and $x \in \mathbb{R}^n$

  Computing Ax takes $\Theta(n^2)$ times, but computing $A(x_1, x_2, \ldots, x_n)$ takes . . . only $O(n^{2.3\ldots}) < \Theta(n^3)$

Weak to Strong OWFs

Theorem 7 (weak to strong OWFs (Yao))

Assume there exist $(1-\delta)$-weak OWFs with $\delta(n) \geq 1/q(n)$ for some $q \in \text{poly}$, then there exist (strong) one-way functions.

- Idea: parallel repetition (i.e., direct product): Consider $g(x_1, \ldots, x_t) = f(x_1), \ldots, f(x_t)$ for large enough t
- Motivation: if something is somewhat hard, than doing it many times is (very) hard
- But, is it really so?

  Consider matrix multiplication: Let $A \in \mathbb{R}^{n\times n}$ and $x \in \mathbb{R}^n$

  Computing Ax takes $\Theta(n^2)$ times, but computing $A(x_1, x_2, \ldots, x_n)$ takes …only $O(n^{2.3\ldots}) < \Theta(n^3)$
- Fortunately, parallel repetition does amplify weak OWFs :-)

Amplification via Parallel Repetition

Theorem 8

Let $f\colon \{0,1\}^n \mapsto \{0,1\}^n$*, and for* $t(n) := \left\lceil \frac{\log^2 n}{\delta(n)} \right\rceil$ *define* $g\colon (\{0,1\}^n)^{t(n)} \mapsto (\{0,1\}^n)^{t(n)}$ *as*

$$g(x_1,\ldots,x_{t(n)}) = f(x_1),\ldots,f(x_{t(n)})$$

Assume f *is* $(1-\delta)$*-weak OWF and* $\delta(n) = 1/q(n)$ *for some (positive)* $q \in \mathrm{poly}$*, then* g *is a one-way function.*

Amplification via Parallel Repetition

Theorem 8

Let $f\colon \{0,1\}^n \mapsto \{0,1\}^n$*, and for* $t(n) := \left\lceil \frac{\log^2 n}{\delta(n)} \right\rceil$ *define* $g\colon (\{0,1\}^n)^{t(n)} \mapsto (\{0,1\}^n)^{t(n)}$ *as*

$$g(x_1,\ldots,x_{t(n)}) = f(x_1),\ldots,f(x_{t(n)})$$

Assume f *is* $(1-\delta)$*-weak OWF and* $\delta(n) = 1/q(n)$ *for some (positive)* $q \in \mathrm{poly}$*, then* g *is a one-way function.*

Clearly g is efficient.

Amplification via Parallel Repetition

Theorem 8

Let $f\colon \{0,1\}^n \mapsto \{0,1\}^n$*, and for* $t(n) := \left\lceil \frac{\log^2 n}{\delta(n)} \right\rceil$ *define* $g\colon (\{0,1\}^n)^{t(n)} \mapsto (\{0,1\}^n)^{t(n)}$ *as*

$$g(x_1,\ldots,x_{t(n)}) = f(x_1),\ldots,f(x_{t(n)})$$

Assume f *is* $(1-\delta)$*-weak OWF and* $\delta(n) = 1/q(n)$ *for some (positive)* $q \in \mathrm{poly}$*, then* g *is a one-way function.*

Clearly g is efficient. Is it one-way?

Amplification via Parallel Repetition

Theorem 8

Let $f\colon \{0,1\}^n \mapsto \{0,1\}^n$*, and for* $t(n) := \left\lceil \frac{\log^2 n}{\delta(n)} \right\rceil$ *define* $g\colon (\{0,1\}^n)^{t(n)} \mapsto (\{0,1\}^n)^{t(n)}$ *as*

$$g(x_1,\ldots,x_{t(n)}) = f(x_1),\ldots,f(x_{t(n)})$$

Assume f *is* $(1-\delta)$*-weak OWF and* $\delta(n) = 1/q(n)$ *for some (positive)* $q \in \mathrm{poly}$*, then* g *is a one-way function.*

Clearly g is efficient. Is it one-way? Proof via reduction:

Amplification via Parallel Repetition

Theorem 8

Let $f\colon \{0,1\}^n \mapsto \{0,1\}^n$*, and for* $t(n) := \left\lceil \frac{\log^2 n}{\delta(n)} \right\rceil$ *define* $g\colon (\{0,1\}^n)^{t(n)} \mapsto (\{0,1\}^n)^{t(n)}$ *as*

$$g(x_1,\ldots,x_{t(n)}) = f(x_1),\ldots,f(x_{t(n)})$$

Assume f *is* $(1-\delta)$*-weak OWF and* $\delta(n) = 1/q(n)$ *for some (positive)* $q \in \mathrm{poly}$*, then* g *is a one-way function.*

Clearly g is efficient. Is it one-way? Proof via reduction: Assume $\exists$ PPT A violating the one-wayness of g, we show there exists a PPT B violating the weak hardness of f.

Amplification via Parallel Repetition

Theorem 8

Let $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, *and for* $t(n) := \left\lceil \frac{\log^2 n}{\delta(n)} \right\rceil$ *define* $g\colon (\{0,1\}^n)^{t(n)} \mapsto (\{0,1\}^n)^{t(n)}$ *as*

$$g(x_1,\ldots,x_{t(n)}) = f(x_1),\ldots,f(x_{t(n)})$$

Assume f *is* $(1-\delta)$*-weak OWF and* $\delta(n) = 1/q(n)$ *for some (positive)* $q \in \text{poly}$, *then* g *is a one-way function.*

Clearly g is efficient. Is it one-way? Proof via reduction: Assume $\exists$ PPT A violating the one-wayness of g, we show there exists a PPT B violating the weak hardness of f.

Difficultly: We need to use an inverter for g with low success probability, e.g., $\frac{1}{n}$, to get an inverter for f with high success probability, e.g., $\frac{1}{2}$ or even $1-\frac{1}{n}$

Amplification via Parallel Repetition

Theorem 8

Let $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, *and for* $t(n) := \left\lceil \frac{\log^2 n}{\delta(n)} \right\rceil$ *define* $g\colon (\{0,1\}^n)^{t(n)} \mapsto (\{0,1\}^n)^{t(n)}$ *as*

$$g(x_1,\ldots,x_{t(n)}) = f(x_1),\ldots,f(x_{t(n)})$$

Assume f *is* $(1-\delta)$*-weak OWF and* $\delta(n) = 1/q(n)$ *for some (positive)* $q \in \mathrm{poly}$, *then* g *is a one-way function.*

Clearly g is efficient. Is it one-way? Proof via reduction: Assume $\exists$ PPT A violating the one-wayness of g, we show there exists a PPT B violating the weak hardness of f.

Difficultly: We need to use an inverter for g with low success probability, e.g., $\frac{1}{n}$, to get an inverter for f with high success probability, e.g., $\frac{1}{2}$ or even $1 - \frac{1}{n}$

In the following we fix (an assumed) PPT A, $p \in \mathrm{poly}$ and infinite set $\mathcal{I} \subseteq \mathbb{N}$ s.t.

$$\Pr_{w \xleftarrow{R} \{0,1\}^{t(n)\cdot n}} [\mathsf{A}(g(w)) \in g^{-1}(g(w))] \geq 1/p(n)$$

for every $n \in \mathcal{I}$.

Amplification via Parallel Repetition

Theorem 8

Let $f\colon \{0,1\}^n \mapsto \{0,1\}^n$*, and for* $t(n) := \left\lceil \frac{\log^2 n}{\delta(n)} \right\rceil$ *define* $g\colon (\{0,1\}^n)^{t(n)} \mapsto (\{0,1\}^n)^{t(n)}$ *as*

$$g(x_1,\ldots,x_{t(n)}) = f(x_1),\ldots,f(x_{t(n)})$$

Assume f *is* $(1-\delta)$*-weak OWF and* $\delta(n) = 1/q(n)$ *for some (positive)* $q \in \mathrm{poly}$*, then* g *is a one-way function.*

Clearly g is efficient. Is it one-way? Proof via reduction: Assume $\exists$ PPT A violating the one-wayness of g, we show there exists a PPT B violating the weak hardness of f.

Difficultly: We need to use an inverter for g with low success probability, e.g., $\frac{1}{n}$, to get an inverter for f with high success probability, e.g., $\frac{1}{2}$ or even $1-\frac{1}{n}$

In the following we fix (an assumed) PPT A, $p \in \mathrm{poly}$ and infinite set $\mathcal{I} \subseteq \mathbb{N}$ s.t.

$$\Pr_{w \xleftarrow{R} \{0,1\}^{t(n)\cdot n}}[\mathsf{A}(g(w)) \in g^{-1}(g(w))] \geq 1/p(n)$$

for every $n \in \mathcal{I}$. We also “fix" $n \in \mathcal{I}$ and omit it from the notation.

Proving that g is One-Way – the Naive Approach

Assume A attacks each of the t outputs of g independently: $\exists$ PPT A′ such that $A(z_1, \ldots, z_t) = A'(z_1) \ldots, A'(z_t)$

Proving that g is One-Way – the Naive Approach

Assume A attacks each of the t outputs of g independently: $\exists$ PPT A′ such that $\mathsf{A}(z_1, \ldots, z_t) = \mathsf{A}'(z_1) \ldots, \mathsf{A}'(z_t)$

It follows that A′ inverts f with probability greater than $(1 - \delta(n))$.

Proving that g is One-Way – the Naive Approach

Assume A attacks each of the t outputs of g independently: $\exists$ PPT A' such that $A(z_1, \ldots, z_t) = A'(z_1) \ldots, A'(z_t)$

It follows that A' inverts f with probability greater than $(1 - \delta(n))$.
Otherwise

$$\Pr_{w \xleftarrow{R} \{0,1\}^{t(n)\cdot n}} [A(g(w)) \in g^{-1}(g(w))] = \prod_{i=1}^{t} \Pr_{x \xleftarrow{R} \{0,1\}^n} \left[A'(f(x)) \in f^{-1}(f(x))\right]$$
$$\leq (1 - \delta(n))^{t(n)} \leq e^{-\log^2 n} \leq n^{-\log n}$$

Proving that g is One-Way – the Naive Approach

Assume A attacks each of the t outputs of g independently: $\exists$ PPT A' such that $A(z_1, \ldots, z_t) = A'(z_1) \ldots, A'(z_t)$

It follows that A' inverts f with probability greater than $(1 - \delta(n))$.
Otherwise

$$\Pr_{w \xleftarrow{R} \{0,1\}^{t(n) \cdot n}} [A(g(w)) \in g^{-1}(g(w))] = \prod_{i=1}^{t} \Pr_{x \xleftarrow{R} \{0,1\}^n} \left[A'(f(x)) \in f^{-1}(f(x))\right]$$
$$\leq (1 - \delta(n))^{t(n)} \leq e^{-\log^2 n} \leq n^{-\log n}$$

Hence A' violates the weak hardness of f

Proving that g is One-Way – the Naive Approach

Assume A attacks each of the t outputs of g independently: $\exists$ PPT A' such that $A(z_1, \ldots, z_t) = A'(z_1) \ldots, A'(z_t)$

It follows that A' inverts f with probability greater than $(1 - \delta(n))$. Otherwise

$$\Pr_{w \xleftarrow{R} \{0,1\}^{t(n)\cdot n}} [A(g(w)) \in g^{-1}(g(w))] = \prod_{i=1}^{t} \Pr_{x \xleftarrow{R} \{0,1\}^n} \left[A'(f(x)) \in f^{-1}(f(x))\right]$$
$$\leq (1 - \delta(n))^{t(n)} \leq e^{-\log^2 n} \leq n^{-\log n}$$

Hence A' violates the weak hardness of f

A less naive approach would be to assume that A goes over the inputs sequentially.

Proving that g is One-Way – the Naive Approach

Assume A attacks each of the t outputs of g independently: $\exists$ PPT A$'$ such that $\mathsf{A}(z_1,\ldots,z_t) = \mathsf{A}'(z_1)\ldots,\mathsf{A}'(z_t)$

It follows that A$'$ inverts f with probability greater than $(1-\delta(n))$. Otherwise

$$\Pr_{w \xleftarrow{R} \{0,1\}^{t(n)\cdot n}}[\mathsf{A}(g(w)) \in g^{-1}(g(w))] = \prod_{i=1}^{t} \Pr_{x \xleftarrow{R} \{0,1\}^n}\left[\mathsf{A}'(f(x)) \in f^{-1}(f(x))\right]$$
$$\leq (1-\delta(n))^{t(n)} \leq e^{-\log^2 n} \leq n^{-\log n}$$

Hence A$'$ violates the weak hardness of f

A less naive approach would be to assume that A goes over the inputs sequentially.

Unfortunately, we can assume none of the above.

Proving that g is One-Way – the Naive Approach

Assume A attacks each of the t outputs of g independently: $\exists$ PPT A′ such that $A(z_1, \ldots, z_t) = A'(z_1) \ldots, A'(z_t)$

It follows that A′ inverts f with probability greater than $(1 - \delta(n))$. Otherwise

$$\Pr_{w \stackrel{R}{\leftarrow} \{0,1\}^{t(n)\cdot n}} [A(g(w)) \in g^{-1}(g(w))] = \prod_{i=1}^{t} \Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n} \left[A'(f(x)) \in f^{-1}(f(x))\right]$$
$$\leq (1 - \delta(n))^{t(n)} \leq e^{-\log^2 n} \leq n^{-\log n}$$

Hence A′ violates the weak hardness of f

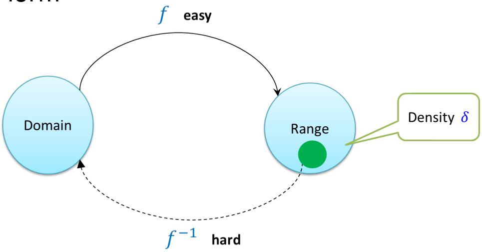
A less naive approach would be to assume that A goes over the inputs sequentially.

Unfortunately, we can assume none of the above.

Any idea?

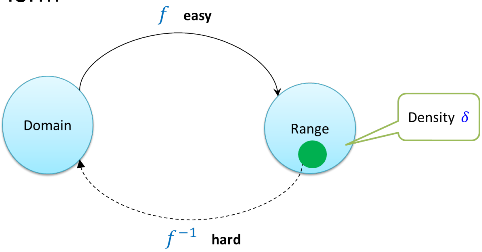
Hardcore Sets

Assume f is of the form



Hardcore Sets

Assume f is of the form



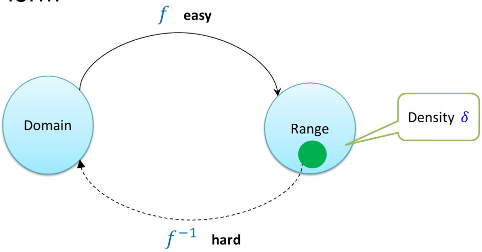
Definition 9 (hardcore sets)

$\mathcal{S} = \{\mathcal{S}_n \subseteq \{0,1\}^n\}$ is a δ-hardcore set for $f \colon \{0,1\}^n \mapsto \{0,1\}^n$, if:

1. $\Pr_{x \xleftarrow{R} \{0,1\}^n}[f(x) \in \mathcal{S}] \geq \delta(n)$ for large enough n, and
2. For any PPT A and $q \in \text{poly}$: for large enough n, it holds that $\Pr\left[\mathsf{A}(y) \in f^{-1}(y)\right] \leq \frac{1}{q(n)}$ for every $y \in \mathcal{S}_n$.

Hardcore Sets

Assume f is of the form



Definition 9 (hardcore sets)

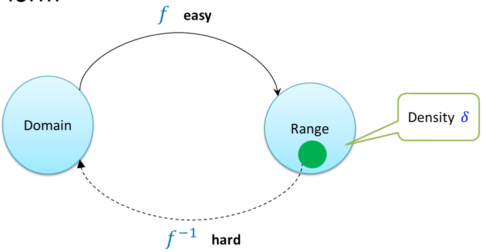
$\mathcal{S} = \{\mathcal{S}_n \subseteq \{0,1\}^n\}$ is a δ-hardcore set for $f \colon \{0,1\}^n \mapsto \{0,1\}^n$, if:

1. $\Pr_{x \xleftarrow{R} \{0,1\}^n} [f(x) \in \mathcal{S}] \geq \delta(n)$ for large enough n, and
2. For any PPT A and $q \in \text{poly}$: for large enough n, it holds that $\Pr\left[A(y) \in f^{-1}(y)\right] \leq \frac{1}{q(n)}$ for every $y \in \mathcal{S}_n$.

Assuming f has a δ seems like a good starting point :-)

Hardcore Sets

Assume f is of the form



Definition 9 (hardcore sets)

$\mathcal{S} = \{\mathcal{S}_n \subseteq \{0,1\}^n\}$ is a δ-hardcore set for $f \colon \{0,1\}^n \mapsto \{0,1\}^n$, if:

1. $\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n} [f(x) \in \mathcal{S}] \geq \delta(n)$ for large enough n, and
2. For any PPT A and $q \in \text{poly}$: for large enough n, it holds that $\Pr\left[\mathsf{A}(y) \in f^{-1}(y)\right] \leq \frac{1}{q(n)}$ for every $y \in \mathcal{S}_n$.

Assuming f has a δ seems like a good starting point :-)

Unfortunately, we do not know how to prove that f has hardcore set :-<

Failing Sets

Failing Sets

Definition 10 (failing sets)

A function $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ has a δ-failing set for a pair (A, q) of algorithm and polynomial, if exists $\mathcal{S} = \{\mathcal{S}_n \subseteq \{0,1\}^n\}$, such that the following holds for large enough n:

1. $\Pr_{x \overset{R}{\leftarrow} \{0,1\}^n}[f(x) \in \mathcal{S}_n] \geq \delta(n)$, and
2. $\Pr\left[\mathsf{A}(y) \in f^{-1}(y)\right] \leq 1/q(n)$, for every $y \in \mathcal{S}_n$

Failing Sets

Definition 10 (failing sets)

A function $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ has a δ-failing set for a pair (A, q) of algorithm and polynomial, if exists $\mathcal{S} = \{\mathcal{S}_n \subseteq \{0,1\}^n\}$, such that the following holds for large enough n:

1. $\Pr_{x \xleftarrow{R} \{0,1\}^n} [f(x) \in \mathcal{S}_n] \geq \delta(n)$, and
2. $\Pr\left[\mathsf{A}(y) \in f^{-1}(y)\right] \leq 1/q(n)$, for every $y \in \mathcal{S}_n$

Claim 11

Let f be a $(1-\delta)$-OWF, then f has a $\delta/2$-failing set, for any pair of PPT A and $q \in \text{poly}$.

Failing Sets

Definition 10 (failing sets)

A function $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ has a δ-failing set for a pair (A, q) of algorithm and polynomial, if exists $\mathcal{S} = \{\mathcal{S}_n \subseteq \{0,1\}^n\}$, such that the following holds for large enough n:

1. $\Pr_{x \xleftarrow{R} \{0,1\}^n}[f(x) \in \mathcal{S}_n] \geq \delta(n)$, and
2. $\Pr\left[\mathsf{A}(y) \in f^{-1}(y)\right] \leq 1/q(n)$, for every $y \in \mathcal{S}_n$

Claim 11

Let f be a $(1-\delta)$-OWF, then f has a $\delta/2$-failing set, for any pair of PPT A and $q \in \text{poly}$.

Proof:

Failing Sets

Definition 10 (failing sets)

A function $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ has a δ-failing set for a pair (A, q) of algorithm and polynomial, if exists $\mathcal{S} = \{\mathcal{S}_n \subseteq \{0,1\}^n\}$, such that the following holds for large enough n:

1. $\Pr_{x \xleftarrow{R} \{0,1\}^n} [f(x) \in \mathcal{S}_n] \geq \delta(n)$, and
2. $\Pr\left[\mathsf{A}(y) \in f^{-1}(y)\right] \leq 1/q(n)$, for every $y \in \mathcal{S}_n$

Claim 11

Let f be a $(1-\delta)$-OWF, then f has a $\delta/2$-failing set, for any pair of PPT A and $q \in \text{poly}$.

Proof: Assume $\exists$ PPT A and $q \in \text{poly}$, such that for any $\mathcal{S} = \{\mathcal{S}_n \subseteq \{0,1\}^n\}$ at least one of the following holds:

1. $\Pr_{x \xleftarrow{R} \{0,1\}^n} [f(x) \in \mathcal{S}_n] < \delta(n)/2$ for infinitely many n's, or
2. For infinitely many n's: $\exists y \in \mathcal{S}_n$ with $\Pr\left[\mathsf{A}(y) \in f^{-1}(y)]\right] \geq 1/q(n)$.

Failing Sets

Definition 10 (failing sets)

A function $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ has a δ-failing set for a pair (A, q) of algorithm and polynomial, if exists $\mathcal{S} = \{\mathcal{S}_n \subseteq \{0,1\}^n\}$, such that the following holds for large enough n:

1. $\Pr_{x \xleftarrow{R} \{0,1\}^n}[f(x) \in \mathcal{S}_n] \geq \delta(n)$, and
2. $\Pr\left[\mathsf{A}(y) \in f^{-1}(y)\right] \leq 1/q(n)$, for every $y \in \mathcal{S}_n$

Claim 11

Let f be a $(1-\delta)$-OWF, then f has a $\delta/2$-failing set, for any pair of PPT A and $q \in \mathrm{poly}$.

Proof: Assume $\exists$ PPT A and $q \in \mathrm{poly}$, such that for any $\mathcal{S} = \{\mathcal{S}_n \subseteq \{0,1\}^n\}$ at least one of the following holds:

1. $\Pr_{x \xleftarrow{R} \{0,1\}^n}[f(x) \in \mathcal{S}_n] < \delta(n)/2$ for infinitely many n's, or
2. For infinitely many n's: $\exists y \in \mathcal{S}_n$ with $\Pr\left[\mathsf{A}(y) \in f^{-1}(y)\right] \geq 1/q(n)$.

We'll use A to contradict the hardness of f.

Using A to Invert f

For $n \in \mathbb{N}$, let $\mathcal{S}_n := \{y \in \{0,1\}^n \colon \Pr\left[\mathsf{A}(y) \in f^{-1}(y)\right] < 1/q(n)\}$.

Using A to Invert f

For $n \in \mathbb{N}$, let $\mathcal{S}_n := \{y \in \{0,1\}^n \colon \Pr\left[\mathsf{A}(y) \in f^{-1}(y)\right] < 1/q(n)\}$.

Claim 12

$\exists$ infinite $\mathcal{I} \subseteq \mathbb{N}$ with $\Pr_{x \xleftarrow{R} \{0,1\}^n}[f(x) \in \mathcal{S}_n] < \delta(n)/2$ for every $n \in \mathcal{I}$.

Using A to Invert f

For $n \in \mathbb{N}$, let $\mathcal{S}_n := \{y \in \{0,1\}^n \colon \Pr\left[A(y) \in f^{-1}(y)\right] < 1/q(n)\}$.

Claim 12

$\exists$ infinite $\mathcal{I} \subseteq \mathbb{N}$ with $\Pr_{x \xleftarrow{R} \{0,1\}^n}[f(x) \in \mathcal{S}_n] < \delta(n)/2$ for every $n \in \mathcal{I}$.

Algorithm 13 (The inverter B on input $y \in \{0,1\}^n$)

Do (with fresh randomness) for $n \cdot q(n)$ times:
If $x = A(y) \in f^{-1}(y)$, return x

Using A to Invert f

For $n \in \mathbb{N}$, let $\mathcal{S}_n := \{y \in \{0,1\}^n \colon \Pr\left[\mathsf{A}(y) \in f^{-1}(y)\right] < 1/q(n)\}$.

Claim 12

$\exists$ infinite $\mathcal{I} \subseteq \mathbb{N}$ with $\Pr_{x \xleftarrow{R} \{0,1\}^n}[f(x) \in \mathcal{S}_n] < \delta(n)/2$ for every $n \in \mathcal{I}$.

Algorithm 13 (The inverter B on input $y \in \{0,1\}^n$)

Do (with fresh randomness) for $n \cdot q(n)$ times:
If $x = \mathsf{A}(y) \in f^{-1}(y)$, return x

Clearly, B is a PPT

Using A to Invert f

For $n \in \mathbb{N}$, let $\mathcal{S}_n := \{y \in \{0,1\}^n \colon \Pr\left[\mathsf{A}(y) \in f^{-1}(y)\right] < 1/q(n)\}$.

Claim 12

$\exists$ infinite $\mathcal{I} \subseteq \mathbb{N}$ with $\Pr_{x \xleftarrow{R} \{0,1\}^n}[f(x) \in \mathcal{S}_n] < \delta(n)/2$ for every $n \in \mathcal{I}$.

Algorithm 13 (The inverter B on input $y \in \{0,1\}^n$)

Do (with fresh randomness) for $n \cdot q(n)$ times:
If $x = \mathsf{A}(y) \in f^{-1}(y)$, return x

Clearly, B is a PPT

Claim 14

For $n \in \mathcal{I}$, it holds that $\Pr_{x \xleftarrow{R} \{0,1\}^n}\left[\mathsf{B}(f(x)) \in f^{-1}(f(x))\right] > 1 - \frac{\delta(n)}{2} - 2^{-n}$

Using A to Invert f

For $n \in \mathbb{N}$, let $\mathcal{S}_n := \{y \in \{0,1\}^n \colon \Pr\left[\mathsf{A}(y) \in f^{-1}(y)\right] < 1/q(n)\}$.

Claim 12

$\exists$ infinite $\mathcal{I} \subseteq \mathbb{N}$ with $\Pr_{x \xleftarrow{R} \{0,1\}^n}[f(x) \in \mathcal{S}_n] < \delta(n)/2$ for every $n \in \mathcal{I}$.

Algorithm 13 (The inverter B on input $y \in \{0,1\}^n$)

Do (with fresh randomness) for $n \cdot q(n)$ times:
If $x = \mathsf{A}(y) \in f^{-1}(y)$, return x

Clearly, B is a PPT

Claim 14

For $n \in \mathcal{I}$, it holds that $\Pr_{x \xleftarrow{R} \{0,1\}^n}\left[\mathsf{B}(f(x)) \in f^{-1}(f(x))\right] > 1 - \frac{\delta(n)}{2} - 2^{-n}$

Proof: ?

Using A to Invert f

For $n \in \mathbb{N}$, let $\mathcal{S}_n := \{y \in \{0,1\}^n \colon \Pr\left[A(y) \in f^{-1}(y)\right] < 1/q(n)\}$.

Claim 12

$\exists$ infinite $\mathcal{I} \subseteq \mathbb{N}$ with $\Pr_{x \xleftarrow{R} \{0,1\}^n}[f(x) \in \mathcal{S}_n] < \delta(n)/2$ for every $n \in \mathcal{I}$.

Algorithm 13 (The inverter B on input $y \in \{0,1\}^n$)

Do (with fresh randomness) for $n \cdot q(n)$ times:
If $x = A(y) \in f^{-1}(y)$, return x

Clearly, B is a PPT

Claim 14

For $n \in \mathcal{I}$, it holds that $\Pr_{x \xleftarrow{R} \{0,1\}^n}\left[B(f(x)) \in f^{-1}(f(x))\right] > 1 - \frac{\delta(n)}{2} - 2^{-n}$

Proof: ?

Hence, for large enough $n \in \mathcal{I}$: $\Pr_{x \xleftarrow{R} \{0,1\}^n}\left[B(f(x)) \in f^{-1}(f(x))\right] > 1 - \delta(n)$.

Using A to Invert f

For $n \in \mathbb{N}$, let $\mathcal{S}_n := \{y \in \{0,1\}^n \colon \Pr\left[\mathsf{A}(y) \in f^{-1}(y)\right] < 1/q(n)\}$.

Claim 12

$\exists$ infinite $\mathcal{I} \subseteq \mathbb{N}$ with $\Pr_{x \xleftarrow{R} \{0,1\}^n}[f(x) \in \mathcal{S}_n] < \delta(n)/2$ for every $n \in \mathcal{I}$.

Algorithm 13 (The inverter B on input $y \in \{0,1\}^n$)

Do (with fresh randomness) for $n \cdot q(n)$ times:
If $x = \mathsf{A}(y) \in f^{-1}(y)$, return x

Clearly, B is a PPT

Claim 14

For $n \in \mathcal{I}$, it holds that $\Pr_{x \xleftarrow{R} \{0,1\}^n}\left[\mathsf{B}(f(x)) \in f^{-1}(f(x))\right] > 1 - \frac{\delta(n)}{2} - 2^{-n}$

Proof: ?

Hence, for large enough $n \in \mathcal{I}$: $\Pr_{x \xleftarrow{R} \{0,1\}^n}\left[\mathsf{B}(f(x)) \in f^{-1}(f(x))\right] > 1 - \delta(n)$.

Namely, f is not $(1-\delta)$-one-way $\square$

Proving g is One-Way cont.

We show that is g is not one way, then f has no $\delta/2$ flailing-set for some PPT B and $q \in$ poly.

Proving g is One-Way cont.

We show that is g is not one way, then f has no $\delta/2$ flailing-set for some PPT B and $q \in$ poly.

Claim 15

Assume $\exists$ PPT A, $p \in$ poly and an infinite set $\mathcal{I} \subseteq \mathbb{N}$ such that

$$\Pr_{w \xleftarrow{R} \{0,1\}^{t(n) \cdot n}} \left[\mathsf{A}(g(x)) \in g^{-1}(g(w)) \right] \geq \frac{1}{p(n)}$$

for every $n \in \mathcal{I}$.

Proving g is One-Way cont.

We show that is g is not one way, then f has no $\delta/2$ flailing-set for some PPT B and $q \in \text{poly}$.

Claim 15

Assume $\exists$ PPT A, $p \in \text{poly}$ and an infinite set $\mathcal{I} \subseteq \mathbb{N}$ such that

$$\Pr_{w \xleftarrow{R} \{0,1\}^{t(n)\cdot n}} \left[\mathsf{A}(g(x)) \in g^{-1}(g(w)) \right] \geq \frac{1}{p(n)}$$

for every $n \in \mathcal{I}$. Then $\exists$ PPT B such that

$$\Pr_{x \xleftarrow{R} \{0,1\}^n | y=f(x) \in \mathcal{S}_n} \left[\mathsf{B}(y) \in f^{-1}(y) \right] \geq \frac{1}{t(n)p(n)} - n^{-\log n}$$

for every $n \in \mathcal{I}$ and every $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \xleftarrow{R} \{0,1\}^n} [f(x) \in \mathcal{S}_n] \geq \delta(n)/2$.

Proving g is One-Way cont.

We show that is g is not one way, then f has no $\delta/2$ flailing-set for some PPT B and $q \in \text{poly}$.

Claim 15

Assume $\exists$ PPT A, $p \in \text{poly}$ and an infinite set $\mathcal{I} \subseteq \mathbb{N}$ such that

$$\Pr_{w \stackrel{R}{\leftarrow} \{0,1\}^{t(n)\cdot n}} \left[A(g(x)) \in g^{-1}(g(w)) \right] \geq \frac{1}{p(n)}$$

for every $n \in \mathcal{I}$. Then $\exists$ PPT B such that

$$\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n | y = f(x) \in \mathcal{S}_n} \left[B(y) \in f^{-1}(y) \right] \geq \frac{1}{t(n)p(n)} - n^{-\log n}$$

for every $n \in \mathcal{I}$ and every $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n} [f(x) \in \mathcal{S}_n] \geq \delta(n)/2$.

Fix $\mathcal{S} = \{\mathcal{S}_n \subseteq \{0,1\}^n\}$.

Proving g is One-Way cont.

We show that is g is not one way, then f has no $\delta/2$ flailing-set for some PPT B and $q \in$ poly.

Claim 15

Assume $\exists$ PPT A, $p \in$ poly and an infinite set $\mathcal{I} \subseteq \mathbb{N}$ such that

$$\Pr_{w \xleftarrow{R} \{0,1\}^{t(n)\cdot n}} \left[\mathsf{A}(g(x)) \in g^{-1}(g(w)) \right] \geq \frac{1}{p(n)}$$

for every $n \in \mathcal{I}$. Then $\exists$ PPT B such that

$$\Pr_{x \xleftarrow{R} \{0,1\}^n | y=f(x) \in \mathcal{S}_n} \left[\mathsf{B}(y) \in f^{-1}(y) \right] \geq \frac{1}{t(n)p(n)} - n^{-\log n}$$

for every $n \in \mathcal{I}$ and every $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \xleftarrow{R} \{0,1\}^n} [f(x) \in \mathcal{S}_n] \geq \delta(n)/2$.

Fix $\mathcal{S} = \{\mathcal{S}_n \subseteq \{0,1\}^n\}$. By Claim 15, for every $n \in \mathcal{I}$, either

- $\Pr_{x \xleftarrow{R} \{0,1\}^n} [f(x) \in \mathcal{S}_n] < \delta(n)/2$, or
- $\Pr_{x \xleftarrow{R} \{0,1\}^n | y=f(x) \in \mathcal{S}_n} \left[\mathsf{B}(y) \in f^{-1}(y) \right] \geq \frac{1}{t(n)p(n)} - n^{-\log n}$

Proving g is One-Way cont.

We show that is g is not one way, then f has no $\delta/2$ flailing-set for some PPT B and $q \in \mathrm{poly}$.

Claim 15

Assume $\exists$ PPT A, $p \in \mathrm{poly}$ and an infinite set $\mathcal{I} \subseteq \mathbb{N}$ such that

$$\Pr_{w \xleftarrow{R} \{0,1\}^{t(n)\cdot n}} \left[\mathsf{A}(g(x)) \in g^{-1}(g(w)) \right] \geq \frac{1}{p(n)}$$

for every $n \in \mathcal{I}$. Then $\exists$ PPT B such that

$$\Pr_{x \xleftarrow{R} \{0,1\}^n | y=f(x) \in \mathcal{S}_n} \left[\mathsf{B}(y) \in f^{-1}(y) \right] \geq \frac{1}{t(n)p(n)} - n^{-\log n}$$

for every $n \in \mathcal{I}$ and every $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \xleftarrow{R} \{0,1\}^n} [f(x) \in \mathcal{S}_n] \geq \delta(n)/2$.

Fix $\mathcal{S} = \{\mathcal{S}_n \subseteq \{0,1\}^n\}$. By Claim 15, for every $n \in \mathcal{I}$, either

- $\Pr_{x \xleftarrow{R} \{0,1\}^n} [f(x) \in \mathcal{S}_n] < \delta(n)/2$, or
- $\Pr_{x \xleftarrow{R} \{0,1\}^n | y=f(x) \in \mathcal{S}_n} \left[\mathsf{B}(y) \in f^{-1}(y) \right] \geq \frac{1}{t(n)p(n)} - n^{-\log n} \overset{\text{(for large enough } n \in \mathcal{I})}{\geq} \frac{1}{2t(n)p(n)}$

Proving g is One-Way cont.

We show that is g is not one way, then f has no $\delta/2$ flailing-set for some PPT B and $q \in \text{poly}$.

Claim 15

Assume $\exists$ PPT A, $p \in \text{poly}$ and an infinite set $\mathcal{I} \subseteq \mathbb{N}$ such that

$$\Pr_{w \stackrel{R}{\leftarrow} \{0,1\}^{t(n)\cdot n}} \left[\mathsf{A}(g(x)) \in g^{-1}(g(w)) \right] \geq \frac{1}{p(n)}$$

for every $n \in \mathcal{I}$. Then $\exists$ PPT B such that

$$\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n | y = f(x) \in \mathcal{S}_n} \left[\mathsf{B}(y) \in f^{-1}(y) \right] \geq \frac{1}{t(n)p(n)} - n^{-\log n}$$

for every $n \in \mathcal{I}$ and every $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n} [f(x) \in \mathcal{S}_n] \geq \delta(n)/2$.

Fix $\mathcal{S} = \{\mathcal{S}_n \subseteq \{0,1\}^n\}$. By Claim 15, for every $n \in \mathcal{I}$, either

- $\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n} [f(x) \in \mathcal{S}_n] < \delta(n)/2$, or
- $\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n | y = f(x) \in \mathcal{S}_n} \left[\mathsf{B}(y) \in f^{-1}(y) \right] \geq \frac{1}{t(n)p(n)} - n^{-\log n} \overset{\text{(for large enough } n \in \mathcal{I})}{\geq} \frac{1}{2t(n)p(n)}$

  $\overset{\text{(for large enough } n \in \mathcal{I})}{\Longrightarrow} \exists y \in \mathcal{S}_n \colon \Pr \left[\mathsf{B}(y) \in f^{-1}(y) \right] \geq \frac{1}{2t(n)p(n)}$

Proving g is One-Way cont.

We show that is g is not one way, then f has no $\delta/2$ flailing-set for some PPT B and $q \in$ poly.

Claim 15

Assume $\exists$ PPT A, $p \in$ poly and an infinite set $\mathcal{I} \subseteq \mathbb{N}$ such that

$$\Pr_{w \xleftarrow{R} \{0,1\}^{t(n)\cdot n}}\left[\mathsf{A}(g(x)) \in g^{-1}(g(w))\right] \geq \frac{1}{p(n)}$$

for every $n \in \mathcal{I}$. Then $\exists$ PPT B such that

$$\Pr_{x \xleftarrow{R} \{0,1\}^n | y = f(x) \in \mathcal{S}_n}\left[\mathsf{B}(y) \in f^{-1}(y)\right] \geq \frac{1}{t(n)p(n)} - n^{-\log n}$$

for every $n \in \mathcal{I}$ and every $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \xleftarrow{R} \{0,1\}^n}[f(x) \in \mathcal{S}_n] \geq \delta(n)/2$.

Fix $\mathcal{S} = \{\mathcal{S}_n \subseteq \{0,1\}^n\}$. By Claim 15, for every $n \in \mathcal{I}$, either

- $\Pr_{x \xleftarrow{R} \{0,1\}^n}[f(x) \in \mathcal{S}_n] < \delta(n)/2$, or
- $\Pr_{x \xleftarrow{R} \{0,1\}^n | y = f(x) \in \mathcal{S}_n}\left[\mathsf{B}(y) \in f^{-1}(y)\right] \geq \frac{1}{t(n)p(n)} - n^{-\log n} \overset{\text{(for large enough } n \in \mathcal{I})}{\geq} \frac{1}{2t(n)p(n)}$

  $\overset{\text{(for large enough } n \in \mathcal{I})}{\Longrightarrow} \exists y \in \mathcal{S}_n$: $\Pr\left[\mathsf{B}(y) \in f^{-1}(y)\right] \geq \frac{1}{2t(n)p(n)}$

Namely, f has no $\delta/2$ failing set for $(\mathsf{B}, q = 2t(n)p(n))$

The No Failing-Set Algorithm

Algorithm 16 (Inverter B on input $y \in \{0,1\}^n$)

1. Choose $w \stackrel{R}{\leftarrow} (\{0,1\}^n)^{t(n)}$, $z = (z_1, \ldots, z_t) = g(w)$ and $i \stackrel{R}{\leftarrow} [t]$
2. Set $z' = (z_1, \ldots, z_{i-1}, y, z_{i+1}, \ldots, z_t)$
3. Return $\mathsf{A}(z')_i$

The No Failing-Set Algorithm

Algorithm 16 (Inverter B on input $y \in \{0,1\}^n$)

1. Choose $w \stackrel{R}{\leftarrow} (\{0,1\}^n)^{t(n)}$, $z = (z_1, \ldots, z_t) = g(w)$ and $i \stackrel{R}{\leftarrow} [t]$
2. Set $z' = (z_1, \ldots, z_{i-1}, y, z_{i+1}, \ldots, z_t)$
3. Return $\mathsf{A}(z')_i$

Fix $n \in \mathcal{I}$ and a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n}[f(x) \in \mathcal{S}] \geq \delta(n)/2$.

The No Failing-Set Algorithm

Algorithm 16 (Inverter B on input $y \in \{0,1\}^n$)

1. Choose $w \stackrel{R}{\leftarrow} (\{0,1\}^n)^{t(n)}$, $z = (z_1, \ldots, z_t) = g(w)$ and $i \stackrel{R}{\leftarrow} [t]$
2. Set $z' = (z_1, \ldots, z_{i-1}, y, z_{i+1}, \ldots, z_t)$
3. Return $\mathsf{A}(z')_i$

Fix $n \in \mathcal{I}$ and a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n}[f(x) \in \mathcal{S}] \geq \delta(n)/2$.

Claim 17

$\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n | y = f(x) \in \mathcal{S}_n} \left[\mathsf{B}(y) \in f^{-1}(y)\right] \geq \frac{1}{t(n) \cdot p(n)} - n^{-\log n}$.

The No Failing-Set Algorithm

Algorithm 16 (Inverter B on input $y \in \{0,1\}^n$)

1. Choose $w \overset{R}{\leftarrow} (\{0,1\}^n)^{t(n)}$, $z = (z_1, \ldots, z_t) = g(w)$ and $i \overset{R}{\leftarrow} [t]$
2. Set $z' = (z_1, \ldots, z_{i-1}, y, z_{i+1}, \ldots, z_t)$
3. Return $\mathsf{A}(z')_i$

Fix $n \in \mathcal{I}$ and a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \overset{R}{\leftarrow} \{0,1\}^n}[f(x) \in \mathcal{S}] \geq \delta(n)/2$.

Claim 17

$\Pr_{x \overset{R}{\leftarrow} \{0,1\}^n | y = f(x) \in \mathcal{S}_n}\left[\mathsf{B}(y) \in f^{-1}(y)\right] \geq \frac{1}{t(n) \cdot p(n)} - n^{-\log n}$.

Proof:

The No Failing-Set Algorithm

Algorithm 16 (Inverter B on input $y \in \{0,1\}^n$)

1. Choose $w \stackrel{R}{\leftarrow} (\{0,1\}^n)^{t(n)}$, $z = (z_1, \ldots, z_t) = g(w)$ and $i \stackrel{R}{\leftarrow} [t]$
2. Set $z' = (z_1, \ldots, z_{i-1}, y, z_{i+1}, \ldots, z_t)$
3. Return $\mathsf{A}(z')_i$

Fix $n \in \mathcal{I}$ and a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n}[f(x) \in \mathcal{S}] \geq \delta(n)/2$.

Claim 17

$\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n | y = f(x) \in \mathcal{S}_n}\left[\mathsf{B}(y) \in f^{-1}(y)\right] \geq \frac{1}{t(n) \cdot p(n)} - n^{-\log n}$.

Proof: Assume for simplicity that A is deterministic.

The No Failing-Set Algorithm

Algorithm 16 (Inverter B on input $y \in \{0,1\}^n$)

1. Choose $w \stackrel{R}{\leftarrow} (\{0,1\}^n)^{t(n)}$, $z = (z_1, \ldots, z_t) = g(w)$ and $i \stackrel{R}{\leftarrow} [t]$
2. Set $z' = (z_1, \ldots, z_{i-1}, y, z_{i+1}, \ldots, z_t)$
3. Return $\mathsf{A}(z')_i$

Fix $n \in \mathcal{I}$ and a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n}[f(x) \in \mathcal{S}] \geq \delta(n)/2$.

Claim 17

$\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n \mid y = f(x) \in \mathcal{S}_n}\left[\mathsf{B}(y) \in f^{-1}(y)\right] \geq \frac{1}{t(n) \cdot p(n)} - n^{-\log n}$.

Proof: Assume for simplicity that A is deterministic.

The No Failing-Set Algorithm

Algorithm 16 (Inverter B on input $y \in \{0,1\}^n$)

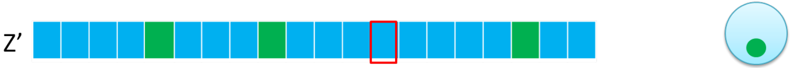
1. Choose $w \xleftarrow{R} (\{0,1\}^n)^{t(n)}$, $z = (z_1, \ldots, z_t) = g(w)$ and $i \xleftarrow{R} [t]$
2. Set $z' = (z_1, \ldots, z_{i-1}, y, z_{i+1}, \ldots, z_t)$
3. Return $\mathsf{A}(z')_i$

Fix $n \in \mathcal{I}$ and a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \xleftarrow{R} \{0,1\}^n} [f(x) \in \mathcal{S}] \geq \delta(n)/2$.

Claim 17

$$\Pr_{x \xleftarrow{R} \{0,1\}^n \mid y = f(x) \in \mathcal{S}_n} \left[\mathsf{B}(y) \in f^{-1}(y)\right] \geq \frac{1}{t(n) \cdot p(n)} - n^{-\log n}.$$

Proof: Assume for simplicity that A is deterministic.



The No Failing-Set Algorithm

Algorithm 16 (Inverter B on input $y \in \{0,1\}^n$)

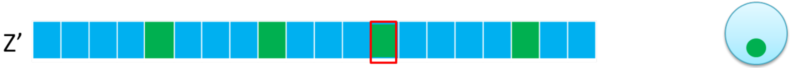
1. Choose $w \xleftarrow{R} (\{0,1\}^n)^{t(n)}$, $z = (z_1, \ldots, z_t) = g(w)$ and $i \xleftarrow{R} [t]$
2. Set $z' = (z_1, \ldots, z_{i-1}, y, z_{i+1}, \ldots, z_t)$
3. Return $A(z')_i$

Fix $n \in \mathcal{I}$ and a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \xleftarrow{R} \{0,1\}^n}[f(x) \in \mathcal{S}] \geq \delta(n)/2$.

Claim 17

$\Pr_{x \xleftarrow{R} \{0,1\}^n | y = f(x) \in \mathcal{S}_n}\left[B(y) \in f^{-1}(y)\right] \geq \frac{1}{t(n) \cdot p(n)} - n^{-\log n}$.

Proof: Assume for simplicity that A is deterministic.



The No Failing-Set Algorithm

Algorithm 16 (Inverter B on input $y \in \{0,1\}^n$)

1. Choose $w \xleftarrow{R} (\{0,1\}^n)^{t(n)}$, $z = (z_1, \ldots, z_t) = g(w)$ and $i \xleftarrow{R} [t]$
2. Set $z' = (z_1, \ldots, z_{i-1}, y, z_{i+1}, \ldots, z_t)$
3. Return $\mathsf{A}(z')_i$

Fix $n \in \mathcal{I}$ and a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \xleftarrow{R} \{0,1\}^n}[f(x) \in \mathcal{S}] \geq \delta(n)/2$.

Claim 17

$$\Pr_{x \xleftarrow{R} \{0,1\}^n | y = f(x) \in \mathcal{S}_n}\left[\mathsf{B}(y) \in f^{-1}(y)\right] \geq \frac{1}{t(n) \cdot p(n)} - n^{-\log n}.$$

Proof: Assume for simplicity that A is deterministic.

Let $Typ = \{v \in \{0,1\}^{t(n) \cdot n} \colon \exists i \in [t(n)] \colon v_i \in \mathcal{S}_n\}$.

The No Failing-Set Algorithm

Algorithm 16 (Inverter B on input $y \in \{0,1\}^n$)

1. Choose $w \stackrel{R}{\leftarrow} (\{0,1\}^n)^{t(n)}$, $z = (z_1, \ldots, z_t) = g(w)$ and $i \stackrel{R}{\leftarrow} [t]$
2. Set $z' = (z_1, \ldots, z_{i-1}, y, z_{i+1}, \ldots, z_t)$
3. Return $\mathsf{A}(z')_i$

Fix $n \in \mathcal{I}$ and a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n}[f(x) \in \mathcal{S}] \geq \delta(n)/2$.

Claim 17

$$\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n | y = f(x) \in \mathcal{S}_n}\left[\mathsf{B}(y) \in f^{-1}(y)\right] \geq \frac{1}{t(n) \cdot p(n)} - n^{-\log n}.$$

Proof: Assume for simplicity that A is deterministic.

Z'

Let $Typ = \{v \in \{0,1\}^{t(n) \cdot n} \colon \exists i \in [t(n)] \colon v_i \in \mathcal{S}_n\}$. $\Pr_z[Typ] \geq 1 - n^{-\log n}$.

The No Failing-Set Algorithm

Algorithm 16 (Inverter B on input $y \in \{0,1\}^n$)

1. Choose $w \stackrel{R}{\leftarrow} (\{0,1\}^n)^{t(n)}$, $z = (z_1, \ldots, z_t) = g(w)$ and $i \stackrel{R}{\leftarrow} [t]$
2. Set $z' = (z_1, \ldots, z_{i-1}, y, z_{i+1}, \ldots, z_t)$
3. Return $A(z')_i$

Fix $n \in \mathcal{I}$ and a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n}[f(x) \in \mathcal{S}] \geq \delta(n)/2$.

Claim 17

$$\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n | y = f(x) \in \mathcal{S}_n}\left[B(y) \in f^{-1}(y)\right] \geq \frac{1}{t(n) \cdot p(n)} - n^{-\log n}.$$

Proof: Assume for simplicity that A is deterministic.

Z'

Let $Typ = \{v \in \{0,1\}^{t(n) \cdot n} \colon \exists i \in [t(n)] \colon v_i \in \mathcal{S}_n\}$. $\Pr_z[Typ] \geq 1 - n^{-\log n}$.

For all $\mathcal{L} \subseteq \{0,1\}^{t(n) \cdot n}$: $\Pr_{z'}[\mathcal{L}] \geq \frac{\Pr_z[\mathcal{L} \cap Typ]}{t(n)}$

The No Failing-Set Algorithm

Algorithm 16 (Inverter B on input $y \in \{0,1\}^n$)

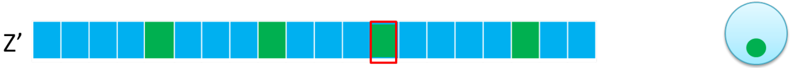
1. Choose $w \stackrel{R}{\leftarrow} (\{0,1\}^n)^{t(n)}$, $z = (z_1, \ldots, z_t) = g(w)$ and $i \stackrel{R}{\leftarrow} [t]$
2. Set $z' = (z_1, \ldots, z_{i-1}, y, z_{i+1}, \ldots, z_t)$
3. Return $\mathsf{A}(z')_i$

Fix $n \in \mathcal{I}$ and a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n}[f(x) \in \mathcal{S}] \geq \delta(n)/2$.

Claim 17

$\Pr_{x \stackrel{R}{\leftarrow} \{0,1\}^n | y = f(x) \in \mathcal{S}_n}\left[\mathsf{B}(y) \in f^{-1}(y)\right] \geq \frac{1}{t(n) \cdot p(n)} - n^{-\log n}$.

Proof: Assume for simplicity that A is deterministic.



Let $\mathit{Typ} = \{v \in \{0,1\}^{t(n) \cdot n} \colon \exists i \in [t(n)] \colon v_i \in \mathcal{S}_n\}$. $\Pr_z[\mathit{Typ}] \geq 1 - n^{-\log n}$.

For all $\mathcal{L} \subseteq \{0,1\}^{t(n) \cdot n}$: $\Pr_{z'}[\mathcal{L}] \geq \frac{\Pr_z[\mathcal{L} \cap \mathit{Typ}]}{t(n)} \geq \frac{\Pr_z[\mathcal{L}] - n^{-\log n}}{t(n)}$. $\square$

The No Failing-Set Algorithm

Algorithm 16 (Inverter B on input $y \in \{0,1\}^n$)

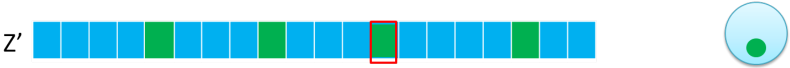
1. Choose $w \overset{R}{\leftarrow} (\{0,1\}^n)^{t(n)}$, $z = (z_1, \ldots, z_t) = g(w)$ and $i \overset{R}{\leftarrow} [t]$
2. Set $z' = (z_1, \ldots, z_{i-1}, y, z_{i+1}, \ldots, z_t)$
3. Return $\mathsf{A}(z')_i$

Fix $n \in \mathcal{I}$ and a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with $\Pr_{x \overset{R}{\leftarrow} \{0,1\}^n} [f(x) \in \mathcal{S}] \geq \delta(n)/2$.

Claim 17

$$\Pr_{x \overset{R}{\leftarrow} \{0,1\}^n \mid y = f(x) \in \mathcal{S}_n} \left[\mathsf{B}(y) \in f^{-1}(y)\right] \geq \frac{1}{t(n) \cdot p(n)} - n^{-\log n}.$$

Proof: Assume for simplicity that A is deterministic.



Let $Typ = \{v \in \{0,1\}^{t(n) \cdot n} \colon \exists i \in [t(n)] \colon v_i \in \mathcal{S}_n\}$. $\Pr_z[Typ] \geq 1 - n^{-\log n}$.

For all $\mathcal{L} \subseteq \{0,1\}^{t(n) \cdot n}$: $\Pr_{z'}[\mathcal{L}] \geq \frac{\Pr_z[\mathcal{L} \cap Typ]}{t(n)} \geq \frac{\Pr_z[\mathcal{L}] - n^{-\log n}}{t(n)}$. $\square$

To conclude the proof take $\mathcal{L} = \{v \in \{0,1\}^{t(n) \cdot n} \colon \mathsf{A}(v) \in g^{-1}(v)\}$

Closing remarks

- One-way functions (OWFs) are hidden in (almost) any cryptographic primitive

Closing remarks

- One-way functions (OWFs) are hidden in (almost) any cryptographic primitive
- Weak OWFs can be amplified into strong one

Closing remarks

- One-way functions (OWFs) are hidden in (almost) any cryptographic primitive
- Weak OWFs can be amplified into strong one
- Can we give a more efficient amplification?

Closing remarks

- One-way functions (OWFs) are hidden in (almost) any cryptographic primitive
- Weak OWFs can be amplified into strong one
- Can we give a more efficient amplification?
- Similar hardness amplification theorems for other cryptographic primitives (e.g., Captchas, general protocols)?

Closing remarks

- One-way functions (OWFs) are hidden in (almost) any cryptographic primitive
- Weak OWFs can be amplified into strong one

- Can we give a more efficient amplification?
- Similar hardness amplification theorems for other cryptographic primitives (e.g., Captchas, general protocols)?
- What properties of the weak OWFs have we used in the proof?

Part II

Hardcore Predicates

Informal Discussion

f is one-way $\implies$ predicting x from $f(x)$ is hard.

Informal Discussion

f is one-way $\implies$ predicting x from $f(x)$ is hard.

But predicting parts of x might be easy.

Informal Discussion

f is one-way $\implies$ predicting x from $f(x)$ is hard.

But predicting parts of x might be easy.

e.g., let f be a OWF then $g(x, w) = (f(x), w)$ is one-way

Informal Discussion

f is one-way $\implies$ predicting x from $f(x)$ is hard.

But predicting parts of x might be easy.

e.g., let f be a OWF then $g(x,w) = (f(x), w)$ is one-way

Can we find a function of x that is totally unpredictable — looks uniform — given $f(x)$?

Informal Discussion

f is one-way $\implies$ predicting x from $f(x)$ is hard.

But predicting parts of x might be easy.

e.g., let f be a OWF then $g(x, w) = (f(x), w)$ is one-way

Can we find a function of x that is totally unpredictable — looks uniform — given $f(x)$?

Such functions have many cryptographic applications

Formal Definition

Definition 18 (hardcore predicates)

A poly-time computable $b\colon \{0,1\}^n \mapsto \{0,1\}$ is an hardcore predicate of $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, if

$$\Pr_{x \xleftarrow{R} \{0,1\}^n}[\mathsf{P}(f(x)) = b(x)] \leq \frac{1}{2} + \operatorname{neg}(n)$$

for any PPT P.

Formal Definition

Definition 18 (hardcore predicates)

A poly-time computable $b\colon \{0,1\}^n \mapsto \{0,1\}$ is an hardcore predicate of $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, if

$$\Pr_{x \xleftarrow{R} \{0,1\}^n} [\mathsf{P}(f(x)) = b(x)] \leq \frac{1}{2} + \mathrm{neg}(n)$$

for any PPT P.

- Does any OWF has such a predicate?

Formal Definition

Definition 18 (hardcore predicates)

A poly-time computable $b\colon \{0,1\}^n \mapsto \{0,1\}$ is an hardcore predicate of $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, if

$$\Pr_{x \xleftarrow{R} \{0,1\}^n} [\mathsf{P}(f(x)) = b(x)] \leq \frac{1}{2} + \operatorname{neg}(n)$$

for any PPT P.

- Does any OWF has such a predicate?
- Is there a generic hardcore predicate for all one-way functions?

Formal Definition

Definition 18 (hardcore predicates)

A poly-time computable $b\colon \{0,1\}^n \mapsto \{0,1\}$ is an hardcore predicate of $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, if

$$\Pr_{x \xleftarrow{R} \{0,1\}^n} [\mathsf{P}(f(x)) = b(x)] \leq \frac{1}{2} + \mathrm{neg}(n)$$

for any PPT P.

- Does any OWF has such a predicate?
- Is there a generic hardcore predicate for all one-way functions?

  Let f be a OWF and let b be a predicate, then $g(x) = (f(x), b(x))$ is one-way.

Formal Definition

Definition 18 (hardcore predicates)

A poly-time computable $b\colon \{0,1\}^n \mapsto \{0,1\}$ is an hardcore predicate of $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, if

$$\Pr_{x \xleftarrow{R} \{0,1\}^n}[\mathsf{P}(f(x)) = b(x)] \leq \frac{1}{2} + \operatorname{neg}(n)$$

for any PPT P.

- Does any OWF has such a predicate?
- Is there a generic hardcore predicate for all one-way functions?

  Let f be a OWF and let b be a predicate, then $g(x) = (f(x), b(x))$ is one-way.
- Does the existence of hardcore predicate for f implies that f is one-way?

Formal Definition

Definition 18 (hardcore predicates)

A poly-time computable $b\colon \{0,1\}^n \mapsto \{0,1\}$ is an hardcore predicate of $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, if

$$\Pr_{x \xleftarrow{R} \{0,1\}^n}[\mathsf{P}(f(x)) = b(x)] \leq \frac{1}{2} + \operatorname{neg}(n)$$

for any PPT P.

- Does any OWF has such a predicate?
- Is there a generic hardcore predicate for all one-way functions?

  Let f be a OWF and let b be a predicate, then $g(x) = (f(x), b(x))$ is one-way.
- Does the existence of hardcore predicate for f implies that f is one-way?

  Consider $f(x,y) = x$, then $b(x,y) = y$ is a hardcore predicate for f

Formal Definition

Definition 18 (hardcore predicates)

A poly-time computable $b\colon \{0,1\}^n \mapsto \{0,1\}$ is an hardcore predicate of $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, if

$$\Pr_{x \xleftarrow{R} \{0,1\}^n}[\mathsf{P}(f(x)) = b(x)] \leq \frac{1}{2} + \mathsf{neg}(n)$$

for any PPT P.

- Does any OWF has such a predicate?
- Is there a generic hardcore predicate for all one-way functions?

  Let f be a OWF and let b be a predicate, then $g(x) = (f(x), b(x))$ is one-way.
- Does the existence of hardcore predicate for f implies that f is one-way?

  Consider $f(x,y) = x$, then $b(x,y) = y$ is a hardcore predicate for f

  Answer to above is positive, in case f is one-to-one

Weak Hardcore Predicates

Weak Hardcore Predicates

For $x \in \{0,1\}^n$ and $i \in [n]$, let x_i be the i'th bit of x.

Weak Hardcore Predicates

For $x \in \{0,1\}^n$ and $i \in [n]$, let x_i be the i'th bit of x.

Theorem 19

For $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, *define* $g\colon \{0,1\}^n \times [n] \mapsto \{0,1\}^n \times [n]$ *by*

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

Assuming f *is one way, then*

$$\Pr_{x \xleftarrow{R} \{0,1\}^n, i \xleftarrow{R} [n]} [\mathsf{A}(f(x), i) = x_i] \leq 1 - 1/2n$$

for any PPT A.

Weak Hardcore Predicates

For $x \in \{0,1\}^n$ and $i \in [n]$, let x_i be the i'th bit of x.

Theorem 19

For $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, *define* $g\colon \{0,1\}^n \times [n] \mapsto \{0,1\}^n \times [n]$ *by*

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

Assuming f *is one way, then*

$$\Pr_{x \xleftarrow{R} \{0,1\}^n, i \xleftarrow{R} [n]}[\mathsf{A}(f(x),i) = x_i] \le 1 - 1/2n$$

for any PPT A.

Proof: ?

Weak Hardcore Predicates

For $x \in \{0,1\}^n$ and $i \in [n]$, let x_i be the i'th bit of x.

Theorem 19

For $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, define $g\colon \{0,1\}^n \times [n] \mapsto \{0,1\}^n \times [n]$ by

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

Assuming f is one way, then

$$\Pr_{x \xleftarrow{R} \{0,1\}^n, i \xleftarrow{R} [n]} [\mathsf{A}(f(x), i) = x_i] \leq 1 - 1/2n$$

for any PPT A.

Proof: ?

We can now construct an hardcore predicate “for" f:

- Construct a weak hardcore predicate for g (i.e., $b(x,i) := x_i$).
- Amplify into a (strong) hardcore predicate for g^t via parallel repetition

Weak Hardcore Predicates

For $x \in \{0,1\}^n$ and $i \in [n]$, let x_i be the i'th bit of x.

Theorem 19

For $f \colon \{0,1\}^n \mapsto \{0,1\}^n$, define $g \colon \{0,1\}^n \times [n] \mapsto \{0,1\}^n \times [n]$ by

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

Assuming f is one way, then

$$\Pr_{x \xleftarrow{R} \{0,1\}^n, i \xleftarrow{R} [n]} [\mathsf{A}(f(x), i) = x_i] \leq 1 - 1/2n$$

for any PPT A.

Proof: ?

We can now construct an hardcore predicate "for" f:

- Construct a weak hardcore predicate for g (i.e., $b(x,i) := x_i$).
- Amplify into a (strong) hardcore predicate for g^t via parallel repetition

The resulting predicate is not for f but for (the one-way function) g^t ...

The Goldreich-Levin Hardcore predicate

For $x, r \in \{0,1\}^n$, let $\langle x, r \rangle_2 := (\sum_{i=1}^{n} x_i \cdot r_i) \bmod 2 = \bigoplus_{i=1}^{n} x_i \cdot r_i$.

The Goldreich-Levin Hardcore predicate

For $x, r \in \{0,1\}^n$, let $\langle x, r \rangle_2 := (\sum_{i=1}^{n} x_i \cdot r_i) \bmod 2 = \bigoplus_{i=1}^{n} x_i \cdot r_i$.

Theorem 20 (Goldreich-Levin)

For $f \colon \{0,1\}^n \mapsto \{0,1\}^n$, define $g \colon \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}^n \times \{0,1\}^n$ as $g(x,r) = (f(x), r)$.

If f is one-way, then $b(x,r) := \langle x, r \rangle_2$ is an hardcore predicate of g.

The Goldreich-Levin Hardcore predicate

For $x, r \in \{0,1\}^n$, let $\langle x, r \rangle_2 := (\sum_{i=1}^{n} x_i \cdot r_i) \bmod 2 = \bigoplus_{i=1}^{n} x_i \cdot r_i$.

Theorem 20 (Goldreich-Levin)

For $f \colon \{0,1\}^n \mapsto \{0,1\}^n$, define $g \colon \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}^n \times \{0,1\}^n$ as $g(x,r) = (f(x), r)$.

If f is one-way, then $b(x,r) := \langle x, r \rangle_2$ is an hardcore predicate of g.

- Note that if f is one-to-one, then so is g.

The Goldreich-Levin Hardcore predicate

For $x, r \in \{0,1\}^n$, let $\langle x, r\rangle_2 := (\sum_{i=1}^{n} x_i \cdot r_i) \bmod 2 = \bigoplus_{i=1}^{n} x_i \cdot r_i$.

Theorem 20 (Goldreich-Levin)

For $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, define $g\colon \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}^n \times \{0,1\}^n$ as $g(x, r) = (f(x), r)$.

If f is one-way, then $b(x, r) := \langle x, r\rangle_2$ is an hardcore predicate of g.

- Note that if f is one-to-one, then so is g.
- A slight cheat, b is defined for g and not for the original OWF f

The Goldreich-Levin Hardcore predicate

For $x, r \in \{0,1\}^n$, let $\langle x, r \rangle_2 := (\sum_{i=1}^n x_i \cdot r_i) \bmod 2 = \bigoplus_{i=1}^n x_i \cdot r_i$.

Theorem 20 (Goldreich-Levin)

For $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, define $g\colon \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}^n \times \{0,1\}^n$ as $g(x,r) = (f(x), r)$.

If f is one-way, then $b(x,r) := \langle x, r \rangle_2$ is an hardcore predicate of g.

- Note that if f is one-to-one, then so is g.
- A slight cheat, b is defined for g and not for the original OWF f

The Goldreich-Levin Hardcore predicate

For $x, r \in \{0,1\}^n$, let $\langle x, r\rangle_2 := (\sum_{i=1}^n x_i \cdot r_i) \bmod 2 = \bigoplus_{i=1}^n x_i \cdot r_i$.

Theorem 20 (Goldreich-Levin)

For $f \colon \{0,1\}^n \mapsto \{0,1\}^n$, define $g \colon \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}^n \times \{0,1\}^n$ as $g(x,r) = (f(x), r)$.

If f is one-way, then $b(x,r) := \langle x, r\rangle_2$ is an hardcore predicate of g.

- Note that if f is one-to-one, then so is g.
- A slight cheat, b is defined for g and not for the original OWF f

Proof by reduction: a PPT A for predicting $b(x,r)$ “too well" from $(f(x), r)$, implies an inverter for f

Proving Goldreich-Levin Theorem

Proving Goldreich-Levin Theorem

Assume $\exists$ PPT A, $p \in$ poly and infinite set $\mathcal{I} \subseteq \mathbb{N}$ with

$$\Pr[\mathsf{A}(g(U_n, R_n)) = b(U_n, R_n)] \geq \frac{1}{2} + \frac{1}{p(n)},$$

for any $n \in \mathcal{I}$, where U_n and R_n are uniformly (and independently) distributed over $\{0, 1\}^n$.

Proving Goldreich-Levin Theorem

Assume $\exists$ PPT A, $p \in$ poly and infinite set $\mathcal{I} \subseteq \mathbb{N}$ with

$$\Pr[\mathsf{A}(g(U_n, R_n)) = b(U_n, R_n)] \geq \frac{1}{2} + \frac{1}{p(n)},$$

for any $n \in \mathcal{I}$, where U_n and R_n are uniformly (and independently) distributed over $\{0,1\}^n$.

Claim 21

For $n \in \mathcal{I}$, there exists a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with

1. $\frac{|\mathcal{S}_n|}{2^n} \geq \frac{1}{2p(n)}$, and
2. $\Pr[\mathsf{A}(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{2p(n)}$, for every $x \in \mathcal{S}_n$.

Proving Goldreich-Levin Theorem

Assume $\exists$ PPT A, $p \in$ poly and infinite set $\mathcal{I} \subseteq \mathbb{N}$ with

$$\Pr[A(g(U_n, R_n)) = b(U_n, R_n)] \geq \frac{1}{2} + \frac{1}{p(n)},$$

for any $n \in \mathcal{I}$, where U_n and R_n are uniformly (and independently) distributed over $\{0,1\}^n$.

Claim 21

For $n \in \mathcal{I}$, there exists a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with

1. $\frac{|\mathcal{S}_n|}{2^n} \geq \frac{1}{2p(n)}$, and
2. $\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{2p(n)}$, for every $x \in \mathcal{S}_n$.

Proof: ?

Proving Goldreich-Levin Theorem

Assume $\exists$ PPT A, $p \in$ poly and infinite set $\mathcal{I} \subseteq \mathbb{N}$ with

$$\Pr[A(g(U_n, R_n)) = b(U_n, R_n)] \geq \frac{1}{2} + \frac{1}{p(n)},$$

for any $n \in \mathcal{I}$, where U_n and R_n are uniformly (and independently) distributed over $\{0,1\}^n$.

Claim 21

For $n \in \mathcal{I}$, there exists a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with

1. $\frac{|\mathcal{S}_n|}{2^n} \geq \frac{1}{2p(n)}$, and
2. $\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{2p(n)}$, for every $x \in \mathcal{S}_n$.

Proof: ?

We next show $\exists$ PPT B and $q \in$ poly with

$$\Pr\left[B(f(x)) \in f^{-1}(f(x))\right] \geq \frac{1}{q(n)},$$

for every $n \in \mathcal{I}$ and $x \in \mathcal{S}_n$.

Proving Goldreich-Levin Theorem

Assume $\exists$ PPT A, $p \in$ poly and infinite set $\mathcal{I} \subseteq \mathbb{N}$ with

$$\Pr[\mathsf{A}(g(U_n, R_n)) = b(U_n, R_n)] \geq \frac{1}{2} + \frac{1}{p(n)},$$

for any $n \in \mathcal{I}$, where U_n and R_n are uniformly (and independently) distributed over $\{0,1\}^n$.

Claim 21

For $n \in \mathcal{I}$, there exists a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with

1. $\frac{|\mathcal{S}_n|}{2^n} \geq \frac{1}{2p(n)}$, and
2. $\Pr[\mathsf{A}(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{2p(n)}$, for every $x \in \mathcal{S}_n$.

Proof: ?

We next show $\exists$ PPT B and $q \in$ poly with

$$\Pr\left[\mathsf{B}(f(x)) \in f^{-1}(f(x))\right] \geq \frac{1}{q(n)},$$

for every $n \in \mathcal{I}$ and $x \in \mathcal{S}_n$. $\implies$ B violates the one-wayness of f.

Proving Goldreich-Levin Theorem

Assume $\exists$ PPT A, $p \in$ poly and infinite set $\mathcal{I} \subseteq \mathbb{N}$ with

$$\Pr[\mathsf{A}(g(U_n, R_n)) = b(U_n, R_n)] \geq \frac{1}{2} + \frac{1}{p(n)},$$

for any $n \in \mathcal{I}$, where U_n and R_n are uniformly (and independently) distributed over $\{0,1\}^n$.

Claim 21

For $n \in \mathcal{I}$, there exists a set $\mathcal{S}_n \subseteq \{0,1\}^n$ with

1. $\frac{|\mathcal{S}_n|}{2^n} \geq \frac{1}{2p(n)}$, and
2. $\Pr\left[\mathsf{A}(f(x), R_n) = b(x, R_n)\right] \geq \frac{1}{2} + \frac{1}{2p(n)}$, for every $x \in \mathcal{S}_n$.

Proof: ?

We next show $\exists$ PPT B and $q \in$ poly with

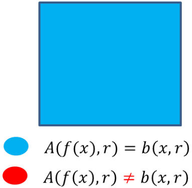
$$\Pr\left[\mathsf{B}(f(x)) \in f^{-1}(f(x))\right] \geq \frac{1}{q(n)},$$

for every $n \in \mathcal{I}$ and $x \in \mathcal{S}_n$. $\implies$ B violates the one-wayness of f.

In the following we fix $n \in \mathcal{I}$ and $x \in \mathcal{S}_n$.

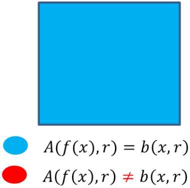
The Perfect Case

$$\Pr\left[\mathsf{A}(f(x), R_n) = b(x, R_n)\right] = 1$$



The Perfect Case

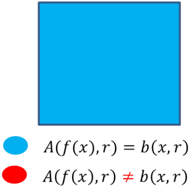
$$\Pr\left[A(f(x), R_n) = b(x, R_n)\right] = 1$$



In particular, $A(f(x), e^i) = b(x, e^i)$ for every $i \in [n]$, where $e^i = (\underbrace{0, \ldots, 0}_{i-1}, 1, \underbrace{0, \ldots, 0}_{n-i})$.

The Perfect Case

$$\Pr\left[A(f(x), R_n) = b(x, R_n)\right] = 1$$

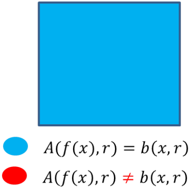


In particular, $A(f(x), e^i) = b(x, e^i)$ for every $i \in [n]$, where $e^i = (\underbrace{0, \ldots, 0}_{i-1}, 1, \underbrace{0, \ldots, 0}_{n-i})$.

Hence, $x_i = \langle x, e^i \rangle_2$

The Perfect Case

$\Pr[\mathsf{A}(f(x), R_n) = b(x, R_n)] = 1$

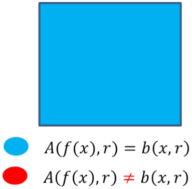


In particular, $\mathsf{A}(f(x), e^i) = b(x, e^i)$ for every $i \in [n]$, where $e^i = (\underbrace{0, \ldots, 0}_{i-1}, 1, \underbrace{0, \ldots, 0}_{n-i})$.

Hence, $x_i = \langle x, e^i \rangle_2 = b(x, e^i) = \mathsf{A}(f(x), e^i)$

The Perfect Case

$\Pr[A(f(x), R_n) = b(x, R_n)] = 1$



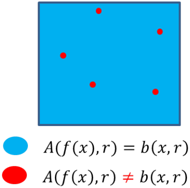
In particular, $A(f(x), e^i) = b(x, e^i)$ for every $i \in [n]$, where $e^i = (\underbrace{0, \ldots, 0}_{i-1}, 1, \underbrace{0, \ldots, 0}_{n-i})$.

Hence, $x_i = \langle x, e^i \rangle_2 = b(x, e^i) = A(f(x), e^i)$

Let $B(y) = (A(y, e^1), \ldots, A(y, e^n))$

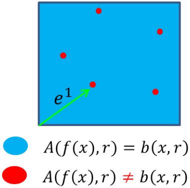
Easy case

$$\Pr\left[A(f(x), R_n) = b(x, R_n)\right] \geq 1 - \text{neg}(n)$$



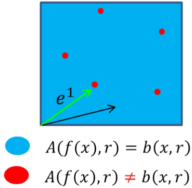
Easy case

$$\Pr\left[A(f(x), R_n) = b(x, R_n)\right] \geq 1 - \text{neg}(n)$$



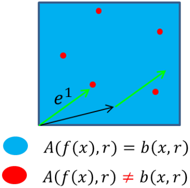
Easy case

$$\Pr\left[A(f(x), R_n) = b(x, R_n)\right] \geq 1 - \mathrm{neg}(n)$$



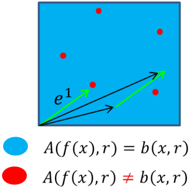
Easy case

$$\Pr\left[A(f(x), R_n) = b(x, R_n)\right] \geq 1 - \text{neg}(n)$$



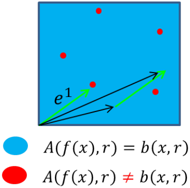
Easy case

$$\Pr\left[A(f(x), R_n) = b(x, R_n)\right] \geq 1 - \text{neg}(n)$$



Easy case

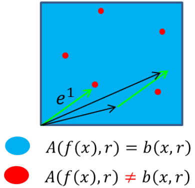
$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq 1 - \text{neg}(n)$$



1. $b(x, w) \oplus b(x, y) = b(x, w \oplus y)$ for every $w, y \in \{0, 1\}^n$.

Easy case

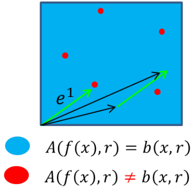
$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq 1 - \mathrm{neg}(n)$$



1. $b(x, w) \oplus b(x, y) = b(x, w \oplus y)$ for every $w, y \in \{0,1\}^n$.
2. $\forall r \in \{0,1\}^n$, the rv $(R_n \oplus r)$ is uniformly distributed over $\{0,1\}^n$.

Easy case

$\Pr[A(f(x), R_n) = b(x, R_n)] \geq 1 - \mathrm{neg}(n)$



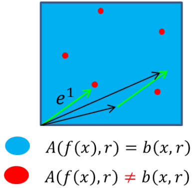
1. $b(x, w) \oplus b(x, y) = b(x, w \oplus y)$ for every $w, y \in \{0,1\}^n$.
2. $\forall r \in \{0,1\}^n$, the rv $(R_n \oplus r)$ is uniformly distributed over $\{0,1\}^n$.

Hence, $\forall i \in [n]$:

1. $x_i = b(x, e^i) = b(x, r) \oplus b(x, r \oplus e^i)$ for every $r \in \{0,1\}^n$

Easy case

$\Pr\left[A(f(x), R_n) = b(x, R_n)\right] \geq 1 - \text{neg}(n)$



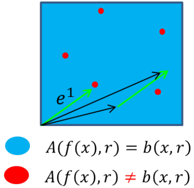
1. $b(x, w) \oplus b(x, y) = b(x, w \oplus y)$ for every $w, y \in \{0, 1\}^n$.
2. $\forall r \in \{0, 1\}^n$, the rv $(R_n \oplus r)$ is uniformly distributed over $\{0, 1\}^n$.

Hence, $\forall i \in [n]$:

1. $x_i = b(x, e^i) = b(x, r) \oplus b(x, r \oplus e^i)$ for every $r \in \{0, 1\}^n$
2. $\Pr[A(f(x), R_n) = b(x, R_n) \wedge A(f(x), R_n \oplus e^i) = b(x, R_n \oplus e^i)] \geq 1 - \text{neg}(n)$

Easy case

$\Pr[\mathsf{A}(f(x), R_n) = b(x, R_n)] \geq 1 - \operatorname{neg}(n)$



1. $b(x, w) \oplus b(x, y) = b(x, w \oplus y)$ for every $w, y \in \{0,1\}^n$.
2. $\forall r \in \{0,1\}^n$, the rv $(R_n \oplus r)$ is uniformly distributed over $\{0,1\}^n$.

Hence, $\forall i \in [n]$:

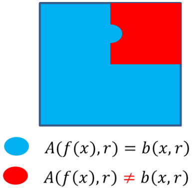
1. $x_i = b(x, e^i) = b(x, r) \oplus b(x, r \oplus e^i)$ for every $r \in \{0,1\}^n$
2. $\Pr[\mathsf{A}(f(x), R_n) = b(x, R_n) \wedge \mathsf{A}(f(x), R_n \oplus e^i) = b(x, R_n \oplus e^i)] \geq 1 - \operatorname{neg}(n)$

Algorithm 22 (Inverter B on input y)

Return $(\mathsf{A}(y, R_n) \oplus \mathsf{A}(y, R_n \oplus e^1)), \ldots, \mathsf{A}(y, R_n) \oplus \mathsf{A}(y, R_n \oplus e^n))$.

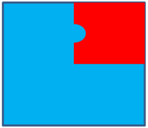
Intermediate Case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{3}{4} + \frac{1}{q(n)}$$



Intermediate Case

$$\Pr\left[\mathrm{A}(f(x), R_n) = b(x, R_n)\right] \geq \frac{3}{4} + \frac{1}{q(n)}$$

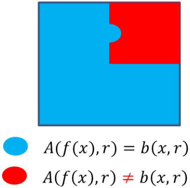


For any $i \in [n]$

$$\begin{aligned} &\Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \\ &\quad \geq \quad \Pr[A(f(x), R_n) = b(x, R_n) \wedge A(f(x), R_n \oplus e^i) = b(x, R_n \oplus e^i)] \end{aligned}$$

Intermediate Case

$$\Pr\left[\mathrm{A}(f(x), R_n) = b(x, R_n)\right] \geq \tfrac{3}{4} + \tfrac{1}{q(n)}$$

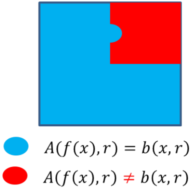


For any $i \in [n]$

$$\begin{aligned}
&\Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \\
&\quad \geq \Pr[A(f(x), R_n) = b(x, R_n) \wedge A(f(x), R_n \oplus e^i) = b(x, R_n \oplus e^i)] \\
&\quad \geq 1 - \left(1 - (\frac{3}{4} + \frac{1}{q(n)})\right) - \left(1 - (\frac{3}{4} + \frac{1}{q(n)})\right)
\end{aligned}$$

Intermediate Case

$$\Pr\left[\mathrm{A}(f(x), R_n) = b(x, R_n)\right] \geq \tfrac{3}{4} + \tfrac{1}{q(n)}$$

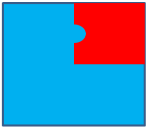


For any $i \in [n]$

$$\begin{aligned}
&\Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \\
&\quad \geq \quad \Pr[A(f(x), R_n) = b(x, R_n) \wedge A(f(x), R_n \oplus e^i) = b(x, R_n \oplus e^i)] \\
&\quad \geq \quad 1 - \left(1 - (\frac{3}{4} + \frac{1}{q(n)})\right) - \left(1 - (\frac{3}{4} + \frac{1}{q(n)})\right) = \frac{1}{2} + \frac{2}{q(n)}
\end{aligned}$$

Intermediate Case

$\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{3}{4} + \frac{1}{q(n)}$



For any $i \in [n]$

$$\begin{aligned}
&\Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \\
&\quad \geq \quad \Pr[A(f(x), R_n) = b(x, R_n) \wedge A(f(x), R_n \oplus e^i) = b(x, R_n \oplus e^i)] \\
&\quad \geq \quad 1 - \left(1 - (\frac{3}{4} + \frac{1}{q(n)})\right) - \left(1 - (\frac{3}{4} + \frac{1}{q(n)})\right) = \frac{1}{2} + \frac{2}{q(n)}
\end{aligned}$$

Algorithm 23 (Inverter B on input $y \in \{0,1\}^n$)

1. For every $i \in [n]$
   1. Sample $r^1, \ldots, r^v \in \{0,1\}^n$ uniformly at random
   2. Let $m_i = \text{maj}_{j \in [v]}\{(A(y, r^j) \oplus A(y, r^j \oplus e^i)\}$
2. Output $(m_1, \ldots, m_n)$

B's Success Provability

The following holds for "large enough" $v = v(n) \in \text{poly}(n)$.

Claim 24

For every $i \in [n]$, it holds that $\Pr[m_i = x_i] \geq 1 - \text{neg}(n)$.

B's Success Provability

The following holds for "large enough" $v = v(n) \in \text{poly}(n)$.

Claim 24

For every $i \in [n]$, it holds that $\Pr[m_i = x_i] \geq 1 - \text{neg}(n)$.

Proof: For $j \in [v]$, let the indicator rv W^j be 1, iff $A(f(x), r^j) \oplus A(f(x), r^j \oplus e^i) = x_i$.

B's Success Provability

The following holds for “large enough" $v = v(n) \in \text{poly}(n)$.

Claim 24

For every $i \in [n]$, it holds that $\Pr[m_i = x_i] \geq 1 - \text{neg}(n)$.

Proof: For $j \in [v]$, let the indicator rv W^j be 1, iff $A(f(x), r^j) \oplus A(f(x), r^j \oplus e^i) = x_i$.
We want to lowerbound $\Pr\left[\sum_{j=1}^{v} W^j > \frac{v}{2}\right]$.

B's Success Provability

The following holds for "large enough" $v = v(n) \in \text{poly}(n)$.

Claim 24

For every $i \in [n]$, it holds that $\Pr[m_i = x_i] \geq 1 - \text{neg}(n)$.

Proof: For $j \in [v]$, let the indicator rv W^j be 1, iff $A(f(x), r^j) \oplus A(f(x), r^j \oplus e^i) = x_i$.
We want to lowerbound $\Pr\left[\sum_{j=1}^{v} W^j > \frac{v}{2}\right]$.

- The W^j are iids and $\text{E}[W^j] \geq \frac{1}{2} + \frac{2}{q(n)}$ for every $j \in [v]$

B's Success Provability

The following holds for "large enough" $v = v(n) \in \text{poly}(n)$.

Claim 24

For every $i \in [n]$, it holds that $\Pr[m_i = x_i] \geq 1 - \text{neg}(n)$.

Proof: For $j \in [v]$, let the indicator rv W^j be 1, iff $A(f(x), r^j) \oplus A(f(x), r^j \oplus e^i) = x_i$.
We want to lowerbound $\Pr\left[\sum_{j=1}^{v} W^j > \frac{v}{2}\right]$.

- The W^j are iids and $\text{E}[W^j] \geq \frac{1}{2} + \frac{2}{q(n)}$ for every $j \in [v]$

Lemma 25 (Hoeffding's inequality)

Let $X^1, \ldots, X^v$ be iids over $[0,1]$ with expectation μ. Then,
$\Pr\left[\left|\frac{\sum_{j=i}^{v} X^j}{v} - \mu\right| \geq \varepsilon\right] \leq 2 \cdot \exp(-2\varepsilon^2 v)$ *for every* $\varepsilon > 0$.

B's Success Provability

The following holds for "large enough" $v = v(n) \in \text{poly}(n)$.

Claim 24

For every $i \in [n]$, it holds that $\Pr[m_i = x_i] \geq 1 - \text{neg}(n)$.

Proof: For $j \in [v]$, let the indicator rv W^j be 1, iff $A(f(x), r^j) \oplus A(f(x), r^j \oplus e^i) = x_i$.

We want to lowerbound $\Pr\left[\sum_{j=1}^{v} W^j > \frac{v}{2}\right]$.

- The W^j are iids and $\text{E}[W^j] \geq \frac{1}{2} + \frac{2}{q(n)}$ for every $j \in [v]$

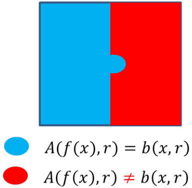
Lemma 25 (Hoeffding's inequality)

Let $X^1, \ldots, X^v$ be iids over $[0, 1]$ with expectation μ. Then, $\Pr\left[\left|\frac{\sum_{j=i}^{v} X^j}{v} - \mu\right| \geq \varepsilon\right] \leq 2 \cdot \exp(-2\varepsilon^2 v)$ *for every* $\varepsilon > 0$.

We complete the proof taking $X^j = W^j$, $\varepsilon = 1/4q(n)$ and $v \in \omega(\log(n) \cdot q(n)^2)$.

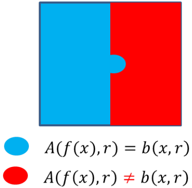
The actual (hard) case

$$\Pr\left[A(f(x), R_n) = b(x, R_n)\right] \geq \frac{1}{2} + \frac{1}{q(n)}$$



The actual (hard) case

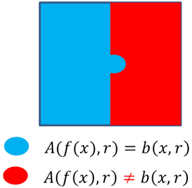
$$\Pr\left[A(f(x), R_n) = b(x, R_n)\right] \geq \frac{1}{2} + \frac{1}{q(n)}$$



- What goes wrong?

The actual (hard) case

$\Pr\left[\mathrm{A}(f(x), R_n) = b(x, R_n)\right] \geq \frac{1}{2} + \frac{1}{q(n)}$

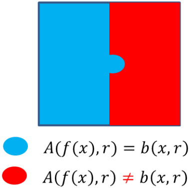


- What goes wrong?

  $\Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \geq \frac{2}{q(n)}$

The actual (hard) case

$$\Pr\left[A(f(x), R_n) = b(x, R_n)\right] \geq \frac{1}{2} + \frac{1}{q(n)}$$



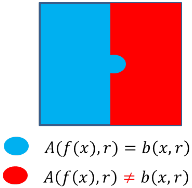
- What goes wrong?

  $\Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \geq \frac{2}{q(n)}$

- Hence, using a random guess does better than using A :-<

The actual (hard) case

$$\Pr\left[\mathsf{A}(f(x), R_n) = b(x, R_n)\right] \geq \frac{1}{2} + \frac{1}{q(n)}$$

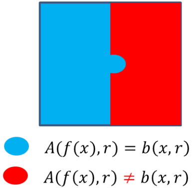


- What goes wrong?

  $\Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \geq \frac{2}{q(n)}$
- Hence, using a random guess does better than using A :-<
- Idea: guess the values of $\{b(x, r^1), \ldots, b(x, r^v)\}$ (instead of calling $\{\mathsf{A}(f(x), r^1), \ldots, \mathsf{A}(f(x), r^v)\}$)

The actual (hard) case

$$\Pr\left[\mathsf{A}(f(x), R_n) = b(x, R_n)\right] \geq \frac{1}{2} + \frac{1}{q(n)}$$



- What goes wrong?

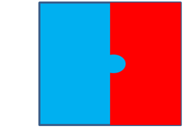
  $\Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \geq \frac{2}{q(n)}$

- Hence, using a random guess does better than using A :-<
- Idea: guess the values of $\{b(x, r^1), \ldots, b(x, r^v)\}$
  (instead of calling $\{\mathsf{A}(f(x), r^1), \ldots, \mathsf{A}(f(x), r^v)\}$)

  Problem: negligible success probability

The actual (hard) case

$\Pr\left[\mathrm{A}(f(x), R_n) = b(x, R_n)\right] \geq \frac{1}{2} + \frac{1}{q(n)}$



- What goes wrong?

  $\Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \geq \frac{2}{q(n)}$

- Hence, using a random guess does better than using A :-<

- Idea: guess the values of $\{b(x, r^1), \ldots, b(x, r^v)\}$
  (instead of calling $\{\mathrm{A}(f(x), r^1), \ldots, \mathrm{A}(f(x), r^v)\}$)

  Problem: negligible success probability

  Solution: choose the samples in a correlated manner

Conclusion

- A close relative of any one-way function has an hardcore predicate.

Conclusion

- A close relative of any one-way function has an hardcore predicate.

  Can we construct an hardcore predicate for any one-way function?

Conclusion

- A close relative of any one-way function has an hardcore predicate.

  Can we construct an hardcore predicate for any one-way function?

- Hardcore functions:

  Similar ideas allows to output $\log n$ “pseudorandom bits"

Conclusion

- A close relative of any one-way function has an hardcore predicate.

  Can we construct an hardcore predicate for any one-way function?

- Hardcore functions:

  Similar ideas allows to output $\log n$ “pseudorandom bits"

- LPN - learning parity with noise:

  Find x given polynomially many samples of $\langle x, R_n \rangle_2 \oplus y$, where $\Pr[y = 1] \leq \frac{1}{2} - \delta$.

Conclusion

- A close relative of any one-way function has an hardcore predicate.

  Can we construct an hardcore predicate for any one-way function?

- Hardcore functions:

  Similar ideas allows to output $\log n$ “pseudorandom bits"

- LPN - learning parity with noise:

  Find x given polynomially many samples of $\langle x, R_n \rangle_2 \oplus y$, where $\Pr[y = 1] \leq \frac{1}{2} - \delta$.

- LPN is believed to be hard

Conclusion

- A close relative of any one-way function has an hardcore predicate.

  Can we construct an hardcore predicate for any one-way function?

- Hardcore functions:

  Similar ideas allows to output $\log n$ “pseudorandom bits"

- LPN - learning parity with noise:

  Find x given polynomially many samples of $\langle x, R_n \rangle_2 \oplus y$, where $\Pr[y = 1] \leq \frac{1}{2} - \delta$.

- LPN is believed to be hard

  The difference comparing to Goldreich-Levin – no control over the R_n's.

Conclusion

- A close relative of any one-way function has an hardcore predicate.

  Can we construct an hardcore predicate for any one-way function?

- Hardcore functions:

  Similar ideas allows to output $\log n$ “pseudorandom bits"

- LPN - learning parity with noise:

  Find x given polynomially many samples of $\langle x, R_n \rangle_2 \oplus y$, where $\Pr[y = 1] \leq \frac{1}{2} - \delta$.

- LPN is believed to be hard

  The difference comparing to Goldreich-Levin – no control over the R_n's.

- Least decoding error correction codes