MIT 6.875

Foundations of Cryptography
Lecture 6

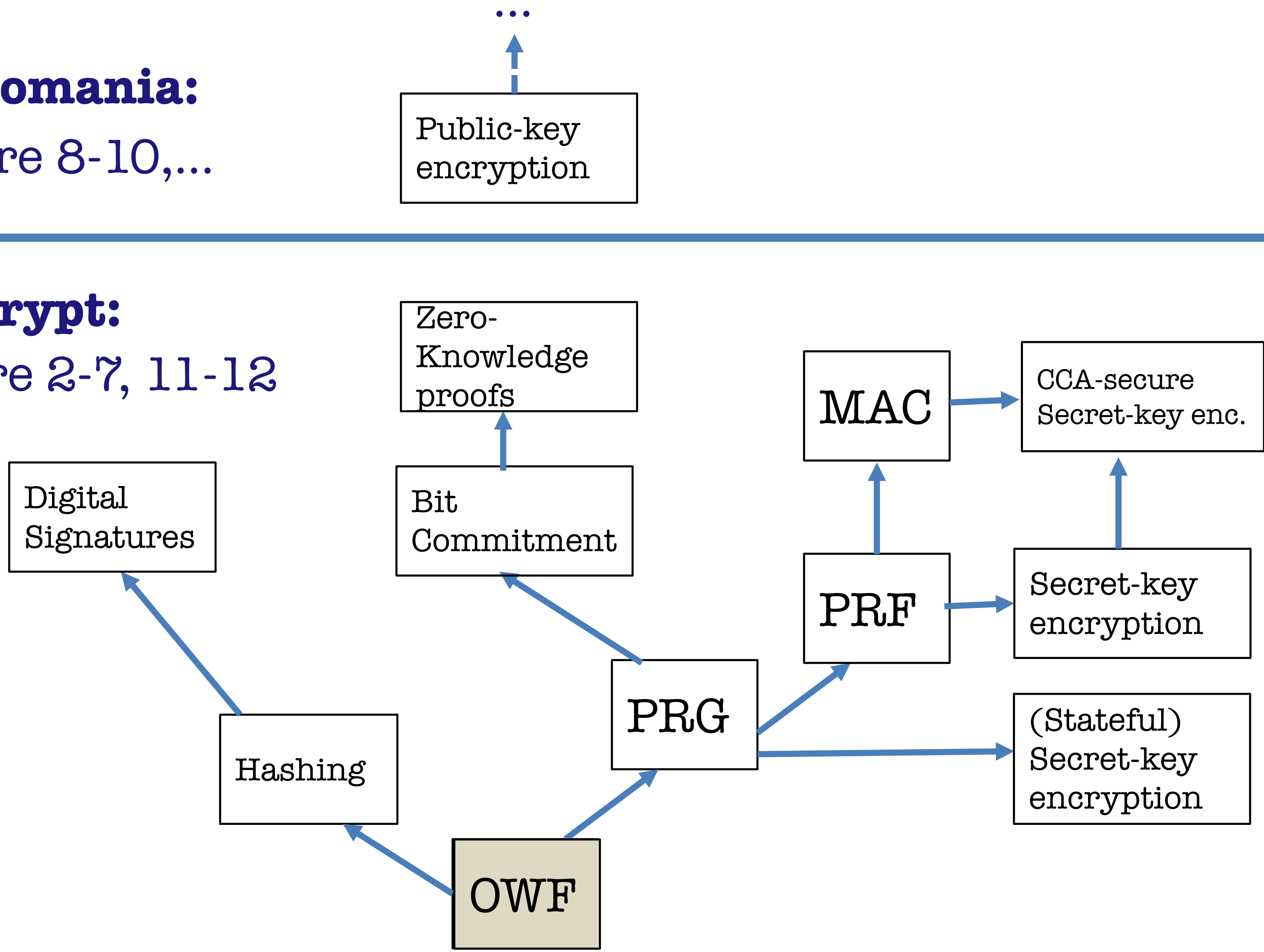
Roadmap of the Course:

Cryptomania:

Lecture 8-10,…

Minicrypt:

Lecture 2-7, 11-12



This Week

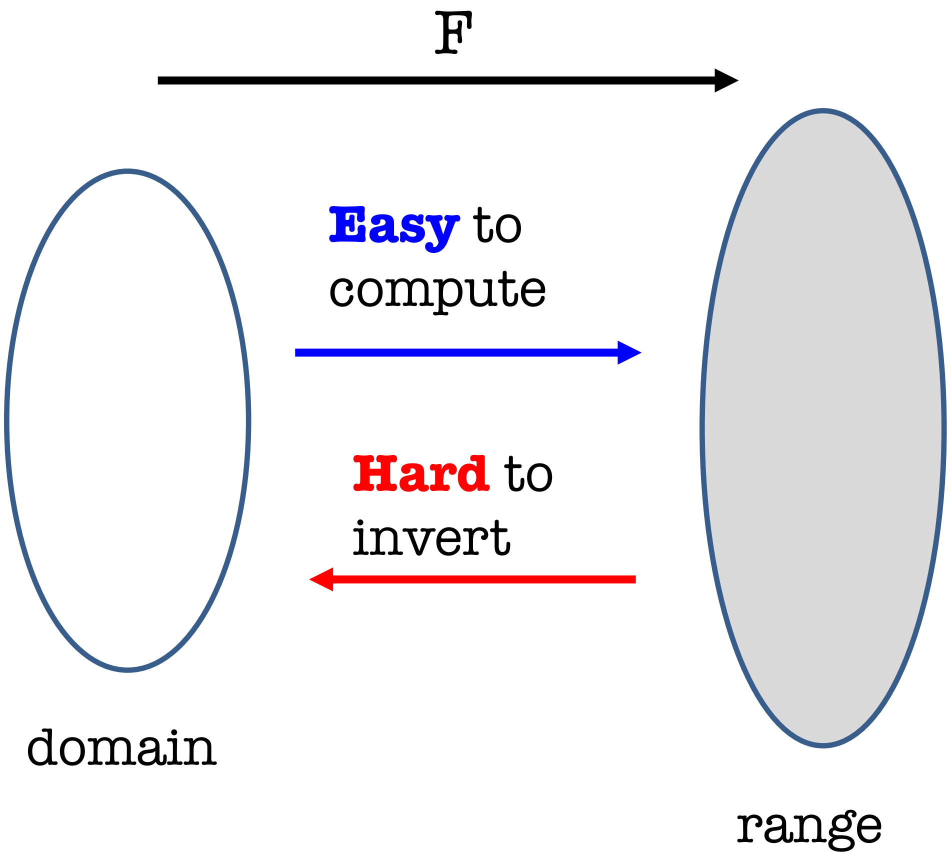
1. Define one-way functions (OWF).

2. Define Hardcore bits (HCB).

3. Show that one-way functions* + HCB $\Rightarrow$ PRG

4. **Goldreich-Levin Theorem**: every OWF has a HCB.

One-way Functions (Informally)



One-way Functions (Take 1)

A function (family) $\{F_n\}_{n\in\mathbb{N}}$ where $F_n\colon \{0,1\}^n \rightarrow \{0,1\}^{m(n)}$ is one-way if for every p.p.t. adversary A, there is a negligible function μ s.t.

$$\Pr[x \leftarrow \{0,1\}^n; y = F_n(x) \colon A(1^n, y) = x] \leq \mu(n)$$

Consider $\boldsymbol{F_n(x) = 0}$ for all x.

This is one-way according to the above definition.
In fact, impossible to find *the* inverse even if A has unbounded time.

Conclusion: not a useful/meaningful definition.

One-way Functions (Take 1)

A function (family) $\{F_n\}_{n\in\mathbb{N}}$ where $F_n: \{0,1\}^n \rightarrow \{0,1\}^{m(n)}$ is one-way if for every p.p.t. adversary A, there is a negligible function μ s.t.

$$\Pr[x \leftarrow \{0,1\}^n; y = F_n(x): A(1^n, y) = x] \leq \mu(n)$$

The Right Definition: Impossible to find ***an*** inverse in p.p.t.

One-way Functions: The Definition

A function (family) $\{F_n\}_{n \in \mathbb{N}}$ where $F_n: \{0,1\}^n \rightarrow \{0,1\}^{m(n)}$ is one-way if for every p.p.t. adversary A, there is a negligible function μ s.t.

$$\Pr[x \leftarrow \{0,1\}^n; y = F_n(x); A(1^n, y) = \boldsymbol{x'}\colon \boldsymbol{y = F_n(x')}] \leq \mu(n)$$

- Can always find *an* inverse with unbounded time
- ... but should be hard with probabilistic polynomial time

One-way Permutations:

One-to-one one-way functions with $m(n) = n$.

Today

1. Define one-way functions (OWF).

2. Define Hardcore bits (HCB).

3. Show that one-way *permutations* (OWP) $\Rightarrow$ PRG

4. Goldreich-Levin Theorem: every OWF has a HCB.

Hardcore Bits

If F is a one-way function, we know it's hard to compute a pre-image of $F(x)$ for a randomly chosen x.

How about computing partial information about an inverse?

Exercise: There are one-way functions for which it is easy to compute the first half of the bits of an inverse.

Hardcore Bits

If F is a one-way function, we know it's hard to compute a pre-image of $F(x)$ for a randomly chosen x.

HARDCORE BIT (Take 1)

Nevertheless, there has to be a hardcore set of hard to invert inputs. Concretely: Does there exist some bit of x that is hard to compute?

Does there necessarily exist some bit of x that is hard to guess with probability non-negligibly better than 1/2?

- Any bit can be guessed correctly w.p. 1/2
- So, "hard to compute" → "hard to guess with probability non-negligibly better than 1/2"

Hardcore Bits

If F is a one-way function, we know it's hard to compute a pre-image of $F(x)$ for a randomly chosen x.

HARDCORE BIT (Take 1)

For any function (family) $F: \{0,1\}^n \rightarrow \{0,1\}^m$, a bit $i = i(n)$ is hardcore if for every p.p.t. adversary A, there is a negligible function μ s.t.

$$\Pr[x \leftarrow \{0,1\}^n; y = F(x): A(y) = x_i] \leq \frac{1}{2} + \mu(n)$$

Does every one-way function have a hardcore bit?

PS2: There are functions that are one-way, yet *every* bit is somewhat easy to predict (say, with probability $\frac{1}{2} + 1/n$).

So, we will generalize the notion of a hardcore "bit".

Hardcore Bits

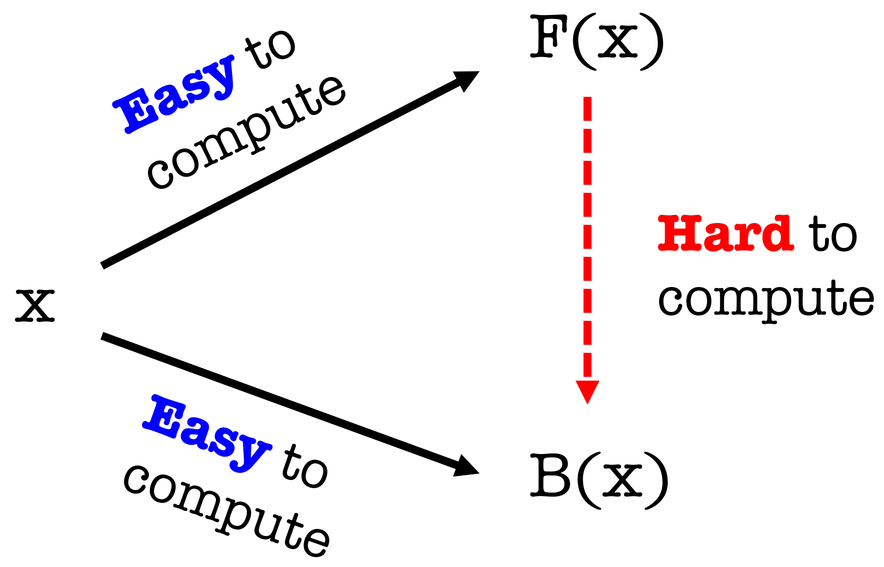
HARDCORE PREDICATE (Definition)

For any function (family) $F: \{0,1\}^n \to \{0,1\}^m$, a function $B: \{0,1\}^n \to \{0,1\}$ is a hardcore **predicate** if for every p.p.t. adversary A, there is a negligible function μ s.t.

$$\Pr[x \leftarrow \{0,1\}^n; y = F(x): A(y) = B(x)] \leq \frac{1}{2} + \mu(n)$$

For us, henceforth, a hardcore bit will mean a hardcore predicate.

Hardcore Predicate (in pictures)



Discussion on the Definition

HARDCORE PREDICATE (Definition)

For any function (family) $F: \{0,1\}^n \to \{0,1\}^m$, a bit $B: \{0,1\}^n \to \{0,1\}$ is a hardcore **predicate** (HCP) if for every p.p.t. adversary A, there is a negligible function μ s.t.

$$\Pr[x \leftarrow \{0,1\}^n; y = F(x): A(y) = B(x)] \leq \frac{1}{2} + \mu(n)$$

1. Definition of HCP makes sense for *any* function family, not just one-way functions.

2. Some functions can have information-theoretically hard to guess predicates (e.g., compressing functions)

3. We'll be interested in settings where x is uniquely determined given $\mathrm{F}(x)$, yet $\mathrm{B}(x)$ is hard to predict given $\mathrm{F}(x)$

Today

1. Define one-way functions (OWF).

2. Define Hardcore bits (HCB).

3. Show that one-way *permutations* (OWP) $\Rightarrow$ PRG

4. Goldreich-Levin Theorem: every OWF has a HCB.

OWP $\Rightarrow$ PRG

CONSTRUCTION

Let F be a one-way permutation, and B an associated hardcore predicate for F.

Then, define $G(x) = \mathrm{F}(x) \mid \mathrm{B}(x)$.

Theorem: G is a PRG assuming F is a one-way permutation.

(Note that G stretches by one bit. We already know how to turn this into a G' that stretches to any poly number of bits.)

OWP $\Rightarrow$ PRG

CONSTRUCTION

Let F be a one-way permutation, and B an associated hardcore predicate for F.

Then, define $G(x) = \mathrm{F}(x) \mid \mathrm{B}(x)$.

Theorem: G is a PRG assuming F is a one-way permutation.

Proof (next slide): Use next-bit unpredictability.

OWP $\Rightarrow$ PRG

Theorem: G is a PRG assuming F is a one-way permutation.

Proof: Assume for contradiction that G is not a PRG.
Therefore, there is a next-bit predictor D, and index i, and a polynomial function p such that

$$\Pr[x \leftarrow \{0,1\}^n; y = G(x): D(y_{1\ldots i-1}) = y_i] \geq \frac{1}{2} + 1/p(n)$$

Observation: The index i has to be $n + 1$. Do you see why?

Hint: $G(x) = \mathrm{F}(x) \mid \mathrm{B}(x)$ and F is a one-way permutation.

OWP $\Rightarrow$ PRG

Theorem: G is a PRG assuming F is a one-way permutation.

Proof: Assume for contradiction that G is not a PRG.
Therefore, there is a next-bit predictor D and a polynomial function p such that

$$\Pr[x \leftarrow \{0,1\}^n; y = G(x): D(y_{1\ldots n}) = y_{n+1}] \geq \frac{1}{2} + 1/p(n)$$

OWP ⇒ PRG

Theorem: G is a PRG assuming F is a one-way permutation.

Proof: Assume for contradiction that G is not a PRG.
Therefore, there is a next-bit predictor D and a polynomial function p such that

$$\Pr[x \leftarrow \{0,1\}^n : D(F(x)) = B(x)] \geq \frac{1}{2} + 1/p(n)$$

So, D is a hardcore bit predictor! QED.

Today

1. Define one-way functions (OWF).

2. Define Hardcore bits (HCB).

3. Show that one-way *permutations* (OWP) $\Rightarrow$ PRG

4. Goldreich-Levin Theorem: every OWF has a HCB.

A Hardcore Predicate for all OWF

Let's shoot for a *universal* hardcore predicate.

i.e., a single predicate B where it is hard to guess $B(x)$ given $\mathrm{F}(x)$

Is this possible?

Turns out the answer is "no".

You will tell me why in PS2.

So, what is one to do?

Goldreich-Levin (GL) Theorem

Let $\{B_r : \{0,1\}^n \rightarrow \{0,1\}\}$ where

$$B_r(x) = \langle r, x \rangle = \sum_{i=1}^{n} r_i x_i \bmod 2$$

be a collection of predicates (one for each r). Then, a ***random*** B_r is hardcore for ***every*** one-way function F. That is, for every one-way function F, every PPT A, there is a negligible function μ s.t.

$$\Pr[x \leftarrow \{0,1\}^n; r \leftarrow \{0,1\}^n : A(F(x), r) = B_r(x)] \leq \frac{1}{2} + \mu(n)$$

GL Theorem: Alternative Interpretation

For ***every*** one-way function F, there is a related one-way function

$$F'(x,r) = (F(x), r)$$

which has a *deterministic* hardcore predicate. In particular, the predicate $B(x,r) = \langle r, x\rangle \bmod 2$ is hardcore for F'.

$$\Pr\left[x \leftarrow \{0,1\}^n; r \leftarrow \{0,1\}^n : A\left(F'(x,r)\right) = \langle r, x\rangle\right] \le \frac{1}{2} + \mu(n)$$

<u>Key Point</u>:

This statement is *sufficient* to construct PRGs from any OWP.

Proof of GL Theorem

Let's make our lives easier: assume a perfect predictor P

~~Assume for contradiction there is a predictor P~~

$$\Pr[x \leftarrow \{0,1\}^n; r \leftarrow \{0,1\}^n : P(F(x), r) = \langle r, x\rangle] \geq \frac{1}{2} + 1/p(n)$$

$$\Pr[x \leftarrow \{0,1\}^n; r \leftarrow \{0,1\}^n : P(F(x), r) = \langle r, x\rangle] = 1$$

We will need to show an inverter A for F

$$\Pr\left[x \leftarrow \{0,1\}^n : A\big(F(x)\big) = x' : F(x') = F(x)\right] \geq 1/p'(n)$$

Proof of GL Theorem

Let's make our lives easier: assume a perfect predictor P

~~Assume for contradiction there is a predictor P~~

$$\Pr[x \leftarrow \{0,1\}^n; r \leftarrow \{0,1\}^n : P(F(x), r) = \langle r, x \rangle] = 1$$

The inverter A works as follows:

On input y $= F(x)$, A runs the predictor P n times, on inputs $(y, e_1), (y, e_2), \ldots,$ and (y, e_n) where $e_1 = 100..0, e_2 = 010 \ldots 0,$… are the unit vectors.

Since A is perfect, it returns $\langle e_i, x \rangle = x_i$, the i^{th} bit of x on the i^{th} invocation.

Proof of GL Theorem

OK, now let's assume less: assume a pretty good predictor P

~~Assume for contradiction there is a predictor P~~

$$\Pr[x \leftarrow \{0,1\}^n; r \leftarrow \{0,1\}^n : P(F(x), r) = \langle r, x \rangle] \geq \frac{3}{4} + 1/p(n)$$

First, we need an **averaging argument**.

Claim: For at least a $1/2p(n)$ fraction of the x,

$$\Pr[r \leftarrow \{0,1\}^n : P(F(x), r) = \langle r, x \rangle] \geq \frac{3}{4} + 1/2p(n)$$

Proof: Exercise in counting.

Call these the good x.

Proof of GL Theorem

For at least a $1/2p(n)$ fraction of the x,

$$\Pr[r \leftarrow \{0,1\}^n : P(F(x), r) = \langle r, x\rangle] \geq \frac{3}{4} + 1/2p(n)$$

Key Idea: Linearity

Pick a random r and ask P to tells us $\langle r, x\rangle$ and $\langle r + e_i, x\rangle$.
Subtract the two answers to get $\langle e_i, x\rangle = x_i$.

Proof: $\Pr[\text{we compute } x_i \text{ correctly}]$

$$\geq \Pr[\text{P predicts } \langle r, x\rangle \text{ and } \langle r + e_i, x\rangle \text{ correctly}]$$

$$= 1 - \Pr[\text{P predicts} \langle r, x\rangle \text{ or } \langle r + e_i, x\rangle \text{ wrong}]$$

$$\geq 1 - (\Pr[\text{P predicts} \langle r, x\rangle \text{ wrong}] + \Pr[\text{P predicts} \langle r + e_i, x\rangle \text{ wrong}])$$ *(by union bound)*

$$\geq 1 - 2 \cdot \left(\frac{1}{4} - \frac{1}{2p(n)}\right) = \frac{1}{2} + 1/p(n)$$

Proof of GL Theorem

For at least a $1/2p(n)$ fraction of the x,

$$\Pr[r \leftarrow \{0,1\}^n : P(F(x), r) = \langle r, x \rangle] \geq \frac{3}{4} + 1/2p(n)$$

Inverter A:

Repeat for each $i \in \{1,2, \dots, n\}$:

Repeat $\log n * p(n)$ times:

Pick a random r and ask P to tells us $\langle r, x \rangle$ and $\langle r + e_i, x \rangle$.
Subtract the two answers to get a guess for x_i.

Compute the majority of all such guesses and set the bit as x_i

Output the concatenation of all x_i as x.

Analysis: Chernoff + Union Bound

Now the real Proof…

Assume (after averaging) that for $\geq 1/2p(n)$ fraction of the x,

$$\Pr[r \leftarrow \{0,1\}^n : P(F(x), r) = \langle r, x \rangle] \geq \frac{\mathbf{1}}{\mathbf{2}} + 1/2p(n)$$

Who's the culprit here?

For at least a $1/2p(n)$ fraction of the x,

$$\Pr[r \leftarrow \{0,1\}^n : P(F(x), r) = \langle r, x \rangle] \geq \frac{3}{4} + 1/2p(n)$$

Pick a random r and ask P to tells us $\langle r, x \rangle$ and $\langle r + e_i, x \rangle$.
Subtract the two answers to get $\langle e_i, x \rangle = x_i$.

Proof: $\Pr[$we compute x_i correctly$]$

$\geq \Pr[\text{P predicts } \langle r, x \rangle \text{ and } \langle r + e_i, x \rangle \text{ correctly}]$

$= 1 - \Pr[\text{P predicts} \langle r, x \rangle \text{ or } \langle r + e_i, x \rangle \text{ wrong}]$

$\geq 1 - (\boldsymbol{Pr}[\text{P } \textbf{predicts} \langle \boldsymbol{r}, \boldsymbol{x} \rangle \textbf{ wrong}] +$
$\boldsymbol{Pr}[\text{P } \textbf{predicts} \langle \boldsymbol{r} + \boldsymbol{e_i}, \boldsymbol{x} \rangle \textbf{ wrong}])$ ***(by union bound)***

$\geq 1 - 2 \cdot \left(\frac{1}{4} - \frac{1}{2p(n)} \right) = \frac{1}{2} + 1/p(n)$

Now on to the Real Proof

Assume (after averaging) that for $\geq 1/2p(n)$ fraction of the x,

$$\Pr[r \leftarrow \{0,1\}^n : P(F(x), r) = \langle r, x \rangle] \geq \mathbf{\frac{1}{2}} + 1/2p(n)$$

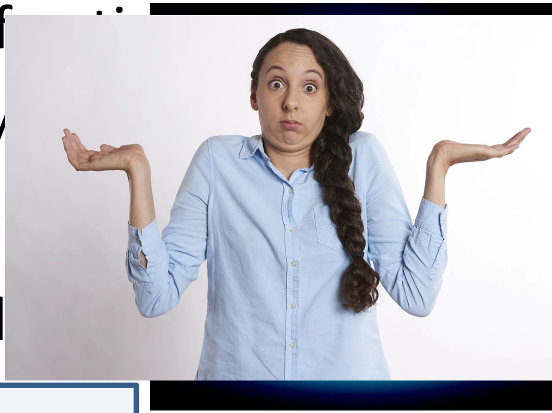
Key Idea: Pairwise independence

A Proof of the GL Theorem

(attributed to Charlie Rackoff)

Assume (after averaging) that for $\geq 1/2p(n)$ f

$$\Pr[r \leftarrow \{0,1\}^n : P(F(x), r) = \langle r, x \rangle] \geq \mathbf{\frac{1}{2}} + 1/$$



For a minute, assume we have a bit of help/ad

Pick a random r, ask the Oracle to tells us $\langle r, x \rangle$ and ask P to tell us $\langle r + e_i, x \rangle$. Subtract the two answers to get $\langle e_i, x \rangle = x_i$.

Proof: $\Pr[$we compute x_i correctly$]$

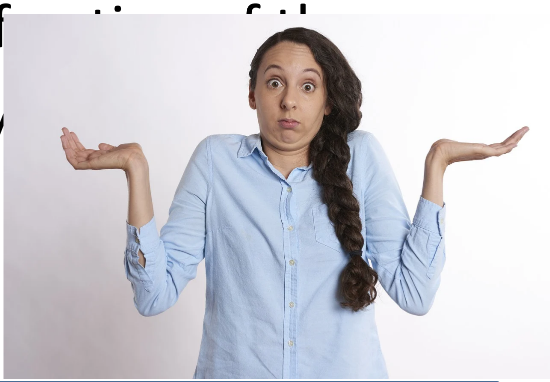
$\geq \boldsymbol{Pr}[$**P predicts**$\boldsymbol{\langle r + e_i, x \rangle}$ **correctly**$] \geq \frac{1}{2} + 1/2p(n)$

A Proof of the GL Theorem

(attributed to Charlie Rackoff)

Assume (after averaging) that for $\geq 1/2p(n)$ f

$\Pr[r \leftarrow \{0,1\}^n\colon P(F(x),r) = \langle r,x\rangle] \geq \mathbf{\frac{1}{2}} + 1/$



Pick a random r, **guess** $\langle r,x\rangle$ and ask P to tell us $\langle r+e_i,x\rangle$.
Subtract the two to get $\langle e_i,x\rangle = x_i$.

If our guesses are all correct, then the analysis works out just as before.

But what's the chance…?
The number of r's is $m = \mathrm{O}(n\log n\,(p(n))^2)$.

Parsimony in Guessing

Pick random "seed vectors" $s_1, \dots, s_{\log(m+1)}$, and **guess** $c_j = \langle s_j, x \rangle$ for all j.

The probability that all guesses are correct is $\frac{1}{2^{\log(m+1)}} = 1/(m+1)$ which is not bad.

From the seed vectors, generate many more $\boldsymbol{r_i}$.

Let $T_1, \dots, T_m$ denote all possible non-empty subsets of $\{1,2, \dots, \log(m+1)\}$. We will let

$$r_i = \bigoplus_{j \in T_i} s_j \qquad \text{and} \qquad b_i = \bigoplus_{j \in T_i} c_j$$

Key Observation: If the guesses $c_1, \dots, c_{\log(m+1)}$ are all correct, then so are the $b_1, \dots, b_m$.

The OWF Inverter

Generate random $s_1, \ldots, s_{\log(m+1)}$ and bits $c_1, \ldots, c_{\log(m+1)}$.

From them, derive $r_1, \ldots, r_{\log(m+1)}$ and bits $b_1, \ldots, b_m$ as in the previous slide.

Repeat for each $i \in \{1,2, \ldots, n\}$:

Repeat $\mathbf{100n(p(n))^2}$ times:

Ask P to tells us $\langle r_i + e_i, x\rangle$. XOR P's reply with b_i to get a guess for x_i.

Compute the majority of all such guesses and set the bit as x_i

Output the concatenation of all x_i as x.

Analysis of the Inverter

Let's condition on the guesses $c_1, \ldots, c_{\log(m+1)}$ being all correct.

The main issue: The r_i are not independent (can't do Chernoff)

Key Observation: The r_i **are** pairwise independent.

Therefore, can apply Chebyshev!

We have that

$p := \Pr[\text{Inverter succeeds} \mid \text{all guesses correct, good x}] \geq 0.99.$

(Pf. on the board, also in the next two slides)

Analysis of the Inverter

The probability that a single iteration of the inner loop gives the correct x_i is at least $\frac{1}{2} + 1/2p(n)$.

Let this be the good event E_i (for the i^{th} iteration of the inner loop).

The majority decision is correct if the number of events E_i that occur is at least $\frac{m}{2} = 50\, n(p(n))^2$.

The expected number of events that occur is

$$(\frac{1}{2} + \frac{1}{2p(n)}).\ 100\, n(p(n))^2 = 50\, n(p(n))^2 + 50np(n).$$

The variance is

$$\approx \frac{1}{4} \cdot 100\, n\left(p(n)\right)^2 = 25n\left(p(n)\right)^2$$

Analysis of the Inverter

The expected number of events that occur is

$$(\frac{1}{2}+\frac{1}{2p(n)}).\ 100\, n(p(n))^2 = 50\, n(p(n))^2 + 50np(n).$$

The variance is $\approx \frac{1}{4} \cdot 100\, n\big(p(n)\big)^2 = 25n\big(p(n)\big)^2$

By an application of Chebyshev, we have

$$\Pr[\mathit{majority\ decision\ w.r.t\ } x_i \mathit{\ incorrect}] \leq \frac{25n\big(p(n)\big)^2}{\big(50np(n)\big)^2} = \frac{1}{100n}$$

By an application of union bound, we have

$$\Pr[\mathit{one\ of\ the\ } x_i \mathit{\ is\ incorrect}] \leq n \cdot \frac{1}{100n} = 1/100$$

∴ The inverter outputs the correct inverse w.p. $\mathrm{p} \geq 0.99$.

Putting it all together

Pr[Inverter succeeds]
$\geq$ Pr[Inverter succeeds | all guesses correct, good x] $\cdot$
Pr[all guesses correct] $\cdot$ Pr[good x]
$= p \cdot \frac{1}{m+1} \cdot \frac{1}{2p(n)} = p \cdot \frac{1}{2n^2 p(n)^3}$

So, it suffices to show that p is large.

By our calculation (last two slides), $p \geq 0.99$, so we are done. ∎

Can also make the success probability $\approx 1/p(n)$ by enumerating over all the "guesses". Each guess results in a supposed inverse, but we can check which of them is the actual inverse!

The Coding-Theoretic View of GL

$x \to (\langle x, r \rangle)_{r \in \{0,1\}^n}$ can be viewed as a highly redundant, exponentially long encoding of x = **the Hadamard code**.

$P(F(x), r)$ can be thought of as providing access to a **noisy** codeword.

What we proved = **unique decoding** algorithm for Hadamard code with error rate $\frac{1}{4} - 1/p(n)$.

The real proof = **list-decoding algorithm** for Hadamard code with error rate $\frac{1}{2} - 1/p(n)$.

Hardcore Predicates from any List-Decodable Code

(due to Impagliazzo and Sudan)

$x \to C(x)$ is the encoding.

Given a $C(x)$ that is incorrect at $\frac{1}{2} - \varepsilon$ fraction of the locations, a list-decoder outputs a list $\{x_1, \ldots, x_m\}$ of possibilities for x.

The hardcore predicate is

$$\boldsymbol{B_i(x) = C(x)_i}.$$

A hardcore-bit predictor gives us access to a corrupted codeword. Running the list-decoder on it gives us the list of possible inverses. The fact that the OWF is easy to compute means that we can filter out the bogus (non-)inverses.

Recap

1. Defined one-way functions (OWF).

2. Defined Hardcore bits (HCB).

3. Goldreich-Levin Theorem: every OWF has a HCB.

   (showed proof for an important special case)

4. Show that one-way *permutations* (OWP) ⇒ PRG

   (in fact, one-way functions ⇒ PRG, but that's a much harder theorem)

Universal Hardcore Predicate Conjecture 1

For every one-way function F,
there exists a circuit B_F s.t.
for every PPT Circuit/Turing Machine A,
there is a negligible function μ s.t.

$$\Pr\left[x \leftarrow \{0,1\}^n : A\big(F(x)\big) = B_F(x)\right] \leq \frac{1}{2} + \mu(n)$$

<u>In fact</u>: I conjecture that for every one-way function F, there ***exists*** an r_F for which the predicate $B_{r_F}(x) = \langle r_F, x \rangle$ that is hardcore.

Universal Hardcore Predicate Conjecture 2

For every one-way function F,
there is **an efficiently generatable** circuit B_F s.t.
for every PPT Circuit/Turing Machine A,
there is a negligible function μ s.t.

$$\Pr\left[x \leftarrow \{0,1\}^n : A\big(F(x)\big) = B_F(x)\right] \leq \frac{1}{2} + \mu(n)$$