# 15-859I: Black-Box Theoretical Cryptography

Spring 2003

## Admin

- Instructor: Nick Hopper (hopper@cs)
- Course web page:
  http://www.cs.cmu.edu/~hopper/crypto_course/
- Web page has schedule, links to papers, hw
- Meetings: MW 1:30-3pm, WeH 4601
- Office Hours: Monday 3-4, WeH 8303
- If you want to get emails about the course, send mail to hopper@cs by Wednesday.

## Grading

- 7 HWs, due every other week (#1 due 1/27)
  - Graded on 0,✓-, ✓, ✓+ basis
- 1 Midterm, take-home.
  - Hand out on Monday 3/10
  - Due beginning of class Wed. 3/12
- 1 Presentation (Maybe)
  - Depends on how many people stick around…
- Pass if average a ✓.

## Content

- I will teach about the "black-box" theory of cryptography:
  - Results of the form: Given an (generic) object which satisfies property A, construct an object which satisfies property B.
  - Results about other connections between properties.
  - Results about limitations of black-box techniques.

## Content

I will not cover:

- Zero-Knowledge, except in bits where it is useful for crypto: ZK is a course on its own
- Number-theoretic results: If there are presentations, this will be your job.
- Any standards, implementations, etc.
- Anything that is covered already in 15-855, complexity theory.

## Lecture 1: Strengthening one-way functions

- Recall: A function f is one-way if:
  - It is easy to compute f.
  - It is hard to invert f.
- How "hard" is hard?

## Weak one-way functions:

- Definition: A function f : {0,1}* → {0,1}* is said to be a *Weak One-Way Function (weak OWF)* if:
  - f(x) is computable in time polynomial in |x|, and
  - There exists a polynomial p(n) > 1 such that for any probabilistic polynomial-time turing machine (PPTM) A:

$$\Pr_{x \leftarrow U_n}[f(A(1^n, f(x))) \neq f(x)] > \frac{1}{p(n)}$$

i.e., any PPTM fails to invert f on inputs of size n with probability at least 1/p(n).

## Strong OWFs

- Definition: A function f : {0,1}* → {0,1}* is said to be a *Strong One-Way Function (strong OWF)* if:
  - f(x) is computable in time polynomial in |x|
  - For any probabilistic polynomial-time turing machine (PPTM) A:

$$\Pr_{x \leftarrow U_n}[f(A(1^n, f(x))) = f(x)]$$

is negligible in *n*.

- Recall: $\mu(n)$ is negligible if for every c > 0, there exists an N such that $\mu(n) < n^{-c}$ when n > N.

## Today's theorem

- Weak OWFs exist iff strong OWFs exist
- (⇐) is easy: A strong OWF is a weak OWF already.
- To prove: if there exists a weak OWF, there exists a a strong OWF.

## Weak OWF → Strong OWF

- Let f be a weak OWF, and let p(n) be the polynomial such that every PPTM fails to invert f with probability at least 1/p(n). Let q(n) = 2np(n).
- Define $g(x_1,x_2,\ldots,x_{q(n)}) = f(x_1),f(x_2),\ldots,f(x_{q(n)})$
- Theorem: if f is a weak OWF, then g is a strong OWF.

## Naïve Proof

- Any PPTM A must fail to invert f with probability at least p(n)
- A PPTM can only invert g by inverting f on all of $x_1 \ldots x_{q(n)}$.
- So for any A,

$$\begin{aligned} \Pr[A \text{ inverts } g] &= \Pi_i \Pr[A \text{ inverts } f(x_i)] \\ &< (1 - 1/p(n))^{np(n)} \\ &< e^{-n} \end{aligned}$$

- Problem: Efforts to invert different $f(x_i)$'s might not be independent!

## Tools: Forward and Reverse Expansion

- Let H = (F,G,E) be a (M,N)-regular bipartite graph.
- H has (ε,δ)-forward expansion if:
  - For all $F \subseteq F$, if $\Pr_X[X \in F] \geq \varepsilon$ then $\Pr_Y[\exists x \in F : (x,Y) \in E] \geq 1-\delta$
- H has (ε,δ,γ)-reverse expansion if:
  - For all $G \subseteq G$, if $\Pr_Y[Y \in G] \geq \delta+\gamma$, then there exists $F \subseteq F$ such that:
    - $\Pr_X[X \in F] \geq 1-\varepsilon$
    - For all $x \in F$, $\Pr_{(x,Y) \in E}[Y \in G] \geq \gamma/N$

## Forward to Reverse Theorem

- If H has $(\varepsilon,\delta)$-forward expansion then for all $\gamma > 0$, H has $(\varepsilon,\delta,\gamma)$-reverse expansion
- Proof: Fix arbitrary $G \subseteq G$ such that $Pr_Y[Y \in G] \geq \delta + \gamma$. Define
  - $F' = \{x \in F : Pr_{(x,Y) \in E}[Y \in G] < \gamma/N\}$ (RH nodes that can't be in F)
  - $G' = \{ y \in G: \exists x \in F' : (x,Y) \in E\}$ (LH nodes in G adjacent to F')

## Forward-to-reverse, cont'd

- Suppose $Pr_X[X \in F'] > \varepsilon$ (In contradiction of theorem)
- Then: $Pr_Y[Y \in G'] \geq 1- \delta$ (forward expansion)
- Let $G'' = G' \cap G$. Then by union bound, $Pr_Y[Y \in G''] > \gamma$. So:

$$|G''| \geq \gamma |G| \geq \gamma |G'|.$$

- Notice: # edges out of $F' \leq N \cdot |G'|$
- And, # edges from F' to G'' $\geq \gamma |G'|$
- So, for $X \in_U F'$, $\Pr_{X,(X,Y)\in E}[Y \in G''] \geq \gamma / N$

## Weak OWF → Strong OWF

- Naïve proof fails because we only considered one type of adversary – he tries to invert g by inverting the q(n) copies of f independently.
- Instead, we will show how ANY adversary A that inverts g with probability 1/s(n) can be used to invert f with probability > 1 – 1/p(n):
  - On input f(x), repeat 2nq(n)s(n) times:
    - Choose $i \in_U \{1,\ldots,q(n)\}$. Choose $y_1 \ldots y_{i-1}, y_{i+1},\ldots y_{q(n)} \in_U \{0,1\}^n$.
    - Run $A(f(y_1),\ldots f(y_{i-1}),f(x),f(y_{i+1}),\ldots f(y_{q(n)}))$ to get $z_1 \ldots z_{q(n)}$
    - If $f(z_i) = f(x)$ return $z_i$.

## Proof that this works

- Let $F = \{0,1\}^n$, $G = \{0,1\}^{nq(n)}$, and $E = \{(x,y) : \exists i: x = y_i\}$.
  - H = (F,G,E) is $(2^{n(q(n)-1)},q(n))$ regular.
  - H has $(\varepsilon, (1- \varepsilon)^{q(n)})$-forward expansion:
  - In particular, H has (1/2p(n), 1/2s(n))-forward expansion when s(n) = poly(n)
  - Thus H has (1/2p(n),1/2s(n),1/2s(n))-reverse expansion as well..

## Proof, cont'd.

- We "win" when, on input x, we pick a y with $(x,y) \in E$ and A successfully inverts y.
- If A successfully inverts on 1/s(n) fraction of y's, reverse expansion guarantees that for a 1- ½(1/p(n)) fraction of x's, there is a 1/(2s(n)q(n)) chance that a random neighbor of x is in the "good" set of y's.
- So, for these "good" x, every independent y has probability > 1/2q(n)s(n) of success – so Pr[failure in 2nq(n)s(n) y's] < $e^{-n}$
- Thus the probability we fail to invert f is at most (1/2)(1/p(n)) + $e^{-n}$, contradicting the weak one-wayness of f.

## Problems

- The hardness of inverting g on inputs of size q(n) is related to the hardness of inverting f on inputs of size n.
- This is not good: suppose it is $2^n$ hard to invert f on more than ½ its inputs, then it is only $2^{\sqrt{n}}$ hard to invert g on inputs of size n.
- [GILVZ 90] show how to solve this problem for a one-way permutation, with a complicated construction involving expanders.

## Strengthening with public randomness

- Suppose we have a 1/p(n)-weak OWP f. We want to strengthen it without losing hardness. Let N = 2np(n).
- We also have a publicly available source of randomness, which outputs strings $\pi \in \{0,1\}^{n \times N}$.
- Define $g(x; \pi) = (y_{N+1}, \pi)$ where:

  $y_1 = x$; $y_i = \pi_{i-1} \oplus f(y_{i-1})$
- g is a strong OWP, with hardness related to f.

## Proof…

- Suppose we have adversary A which inverts g with probability 1/q(n). Here's how to use A to invert f with probability 1 – ½ (1/p(n)):
- On input f(x), repeat 2nNq(n) times:
  - Choose $i \in_U \{2,\ldots,N+1\}$. Choose $\pi \in \{0,1\}^{n \times N}$.
  - Let $y_i = \pi_{i-1} \oplus f(x)$, $y_{i+1} = \pi_i \oplus f(y_i)$, etc…
  - Compute $v_0 = A(y_{N+1}, \pi)$
  - Set $v_j = \pi_{j-1} \oplus f(v_{j-1})$, $j = 1 \ldots N+1$
  - If $f(v_{i-1}) = f(x)$, return $v_{i-1}$.

## …

- Define $F = \{0,1\}^n$, $G = \{0,1\}^{n \times (N+1)}$, and

  $E = \{ (y_i,(x,\pi)) : y_0 = x, y_j = \pi_{j-1} \oplus f(y_{j-1}) \}$
- $H = (F,G,E)$ is $(N2^{nN},N)$-regular and has forward expansion $(\varepsilon, (1-\varepsilon)^N)$
- The rest of the proof goes the same!
- Note: we need f to be a permutation, otherwise the graph isn't regular; The forward-to-reverse theorem requires regularity.
- Challenge: find a "linear-preserving" reduction which works for a general weak OWF.