One Way Functions (Part II)

601.642/442: Modern Cryptography

Fall 2019

Last Time

- Modeling adversaries as non-uniform PPT Turing machines
- Negligible functions
- Definitions of strong OWFs
- Multiplication function and Factoring assumption

Today's Agenda

- Weak OWFs and candidate $f_\times$
- Proving $f_\times$ is a weak OWF based on factoring assumption
- Yao's hardness amplification: from weak to strong OWFs

Recall: Multiplication Function

- Recall the function $f_\times : \mathbb{N}^2 \to \mathbb{N}$.
- Observation 1: If randomly chosen x and y happen to be primes, no PPT $\mathcal{A}$ can invert (except with negligible probability). Call it the **GOOD** case.
- If GOOD case occurs with probability $> \varepsilon$,

  $\Rightarrow$ every PPT $\mathcal{A}$ must fail to invert $f_\times$ with probability at least ε.
- Now suppose that ε is a non-negligible function (think of it as inverse polynomial, i.e., $\frac{1}{p(\cdot)}$ for some polynomial $p(\cdot)$.)

  $\Rightarrow$ every $\mathcal{A}$ must fail to invert $f_\times$ with non-negligible probability.
- This is already useful!
- Usually called a **weak** OWF.

Weak One Way Functions

Definition (Weak One Way Function)

A function $f : \{0,1\}^* \to \{0,1\}^*$ is a *weak one-way function* if it satisfies the following two conditions:

- **Easy to compute:** there is a polynomial-time algorithm $\mathcal{C}$ s.t. $\forall x \in \{0,1\}^*$,

$$\Pr\left[\mathcal{C}(x) = f(x)\right] = 1.$$

- **Somewhat hard to invert:** there is a non-negligible function $\varepsilon : \mathbb{N} \to \mathbb{R}$ s.t. for every non-uniform PPT $\mathcal{A}$ and $\forall n \in \mathbb{N}$:

$$\Pr\left[x \leftarrow \{0,1\}^n, x' \leftarrow \mathcal{A}(1^n, f(x)) : f(x') \neq f(x)\right] \geqslant \varepsilon(n).$$

Back to Multiplication

- Can we prove that $f_\times$ is a weak OWF?
- Remember the GOOD case? Both x and y are prime.
- If we can show that GOOD case occurs with non-negligible probability, we can prove that $f_\times$ is a weak OWF.

Theorem

Assuming the factoring assumption, function $f_\times$ is a weak OWF.

- Proof Idea: The fraction of prime numbers between 1 and 2^n is non-negligible!
- **Chebyshev's theorem**: An n bit number is a prime with probability $\frac{1}{2n}$

Proof Idea

- Let $\textsc{Good}$ be the set of inputs (x, y) to $f_\times$ s.t. both x and y are prime numbers
- When $(x, y) \in \textsc{Good}$, adversary cannot invert $f_\times(x, y)$ (due to hardness of factoring)
- Suppose adversary inverts with probability 1 when $(x, y) \notin \textsc{Good}$
- But if $\Pr[(x, y) \in \textsc{Good}]$ is non-negligible, then overall, adversary can only invert with a bounded non-negligible probability
- Formally: Let $q(n) = 8n^2$. Will show that no non-uniform PPT adversary can invert $f_\times$ with probability greater than $1 - \frac{1}{q(n)}$

Proof via Reduction

Goal: Given an adversary A that breaks weak one-wayness of $f_\times$ with probability *at least* $1 - \frac{1}{q(n)}$, we will construct an adversary B that breaks the factoring assumption with non-negligible probability

Adversary $B(z)$**:**

1. $x, y \xleftarrow{\$} \{0,1\}^n$
2. If x and y are primes, then $z' = z$
3. Else, $z' = x \cdot y$
4. $w \leftarrow A(1^n, z')$
5. Output w if x and y are primes

Analysis of B:

- Since A is non-uniform PPT, so is B (using polynomial-time primality testing)
- A fails to invert with probability at most $\frac{1}{q(n)} = \frac{1}{8n^2}$
- B fails to pass z to A with probability at most $1 - \frac{1}{4n^2}$ (by Chebyshev's Thm.)
- Union bound: B fails with probability at most $1 - \frac{1}{8n^2}$
- B succeeds with probability at least $\frac{1}{8n^2}$: Contradiction to factoring assumption!

Back to Strong OWFs

- How can we construct strong OWFs?
- Can we modify $f_\times$ to construct a strong OWF?
- Or better yet, can we convert a strong OWF from *any* weak OWF?
- **Yao's Hardness Amplification:** YES!

Weak to Strong OWFs

Theorem (Yao)

Strong OWFs exist if and only weak OWFs exist

- This is called hardness amplification: convert a somewhat hard problem into a really hard problem
- Intuition: Use the weak OWF *many* times
- Think: Is $f(f(...f(x)))$ a good idea?

Weak to Strong OWFs

Theorem

For any weak one-way function $f : \{0,1\}^n \rightarrow \{0,1\}^n$*, there exists a polynomial* $N(\cdot)$ *s.t. the function* $F : \{0,1\}^{n \cdot N(n)} \rightarrow \{0,1\}^{n \cdot N(n)}$ *defined as*

$$F(x_1, \ldots, x_N(n)) = (f(x_1), \ldots, f(x_N(n)))$$

is strongly one-way.

- Think: Show that when f is the $f_\times$ function, then F is a strong one-way function

Weak to Strong OWFs: Intuition

- Recall: OWFs only guarantee average-case hardness
- GOOD inputs: hard to invert, BAD inputs: easy to invert
- A OWF is weak when the fraction of BAD inputs is **non-negligible**
- In a strong OWF, the fraction of BAD inputs is **negligible**
- To convert weak OWF to strong, use the weak OWF on **many** (say N) inputs independently
- In order to successfully invert the new OWF, adversary must invert ALL the N outputs of the weak OWF
- If N is sufficiently large and the inputs are chosen independently at random, then the probability of inverting all of them should be small

Weak to Strong OWFs: Intuition

- The above intuition does not quite work as you expect because even though the instances are chosen independently, adversary gets to see them all together and does not have to invert them independently.
- Nevertheless, it can be shown via a non-trivial proof that hardness does amplify for one-way functions (albeit not all the way to exponentially small inversion probability – there are counterexamples to this!)
- In fact, hardness amplification is not a general phenomenon; for other cases such as interactive arguments (we will study later), hardness does not amplify in general

Weak to Strong OWFs: Example

- We will show that Yao's hardness amplification works for $f_\times$
- The general case requires a different and careful proof; see lecture notes for details

Hardness Amplification for $f_\times$

Theorem

Assume the factoring assumption and let $m = 4n^3$. *Then,* $\mathcal{F} : \left(\{0,1\}^{2n}\right)^m \to \left(\{0,1\}^{2n}\right)^m$ *is a strong OWF:*

$$\mathcal{F}\big((x_1, y_1), \ldots, (x_m, y_m)\big) = \big(f_\times(x_1, y_1), \ldots, f_\times(x_m, y_m)\big).$$

- **Intuition:** Recall that by Chebyshev's Thm, a pair of random n-bit numbers are both primes with prob $\frac{1}{4n^2}$
- When we choose $m = 4n^3$ pairs, then the prob that no pair consists of primes is at most e^{-n}, which is negligible

Hardness Amplification for $f_\times$: Proof Details

- Let $N = 2n \cdot 4n^3 = 8n^4$. Let $(\mathbf{x}, \mathbf{y}) = (x_1, y_1), \ldots, (x_m, y_m)$
- Suppose $\mathcal{F}$ is not a strong OWF. Then, $\exists$ a non-uniform PPT adversary A that inverts $\mathcal{F}$ with prob at least $\varepsilon(2n)$ for some non-negligible function $\varepsilon(\cdot)$
- We will use A to construct a non-uniform PPT adversary B that breaks the factoring assumption

Adversary $B(z^*)$**:**

```
1. $\mathbf{x}, \mathbf{y} \overset{\$}{\leftarrow} \{0,1\}^N$
2. Compute $\mathbf{z} \leftarrow \mathcal{F}(\mathbf{x}, \mathbf{y})$
3. If $\exists$ $i$ s.t. $(x_i, y_i)$ are both primes, then:
     • Replace $z_i$ with $z^*$ (only once)
     • Compute $(\mathbf{x}', \mathbf{y}') \leftarrow A(1^N, \mathbf{z})$
     • Output $(x'_i, y'_i)$
4. Else, fail
```

Analysis of B

- Easy to verify that B is PPT
- Also, easy to verify that A feeds the correct input distribution to B, except with prob e^{-n}
- Overall, B fails with prob at most $(1 - \varepsilon(2n) + e^{-n} < (1 - \frac{\varepsilon(2n)}{2})$
- Thus, B succeeds with prob at least $\frac{\varepsilon(2n)}{2}$, which is a contradiction