# One-Way Functions (II)

601.642/442: Modern Cryptography

Fall 2020

# Recap: One Way Functions

$$\begin{tikzcd} x \arrow[r, bend left, "\text{EASY}"] & f(x) \arrow[l, bend left, "\text{HARD}"] \end{tikzcd}$$

- A function is one-way if it "easy to compute," but "hard to invert"
- Necessary for the existence of most cryptographic primitives (e.g., multi-message encryption, digital signatures)
- Also sufficient for some cryptographic primitives (e.g., pseudorandom generators, secret-key encryption, digital signatures).

# Recap: One Way Functions (Definition)

**Definition (One Way Function)**

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

- **Easy to compute:** there is a polynomial-time algorithm $\mathcal{C}$ s.t. $\forall x \in \{0,1\}^*$,
$$\Pr\left[\mathcal{C}(x) = f(x)\right] = 1.$$
- **Hard to invert:** there exists a negligible function $\nu : \mathbb{N} \rightarrow \mathbb{R}$ s.t. for every non-uniform PPT adversary $\mathcal{A}$ and $\forall n \in \mathbb{N}$:
$$\Pr\left[x \xleftarrow{\$} \{0,1\}^n, x' \leftarrow \mathcal{A}(1^n, f(x)) : f(x') = f(x)\right] \leqslant \nu(n).$$

- The above definition is also called **strong** one-way functions.

# Recap: Factoring Assumption

**Definition (Factoring Assumption)**

For every non-uniform PPT adversary $\mathcal{A}$, there exists a negligible function $\nu$ such that

$$\Pr\left[p \xleftarrow{\$} \Pi_n; q \xleftarrow{\$} \Pi_n; N = pq : \mathcal{A}(N) \in \{p, q\}\right] \leqslant \nu(n).$$

# Multiplication Function

- Recall: multiplication function $f_\times : \mathbb{N}^2 \to \mathbb{N}$.

$$f_\times(x,y) = \begin{cases} \perp & \text{if } x = 1 \vee y = 1 \\ x \cdot y & \text{otherwise} \end{cases}$$

# Multiplication Function

- Recall: multiplication function $f_\times : \mathbb{N}^2 \to \mathbb{N}$.

$$f_\times(x,y) = \begin{cases} \perp & \text{if } x = 1 \vee y = 1 \\ x \cdot y & \text{otherwise} \end{cases}$$

- **Observation 1** (follows from factoring assumption): 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.

# Multiplication Function

- Recall: multiplication function $f_\times : \mathbb{N}^2 \to \mathbb{N}$.

$$f_\times(x, y) = \begin{cases} \perp & \text{if } x = 1 \lor y = 1 \\ x \cdot y & \text{otherwise} \end{cases}$$

- **Observation 1** (follows from factoring assumption): 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 $\varepsilon$.

# Multiplication Function

- Recall: multiplication function $f_\times : \mathbb{N}^2 \to \mathbb{N}$.

$$f_\times(x, y) = \begin{cases} \perp & \text{if } x = 1 \vee y = 1 \\ x \cdot y & \text{otherwise} \end{cases}$$

- **Observation 1** (follows from factoring assumption): 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 $\varepsilon$.

- Now suppose that $\varepsilon$ is a **noticeable function** (say e.g. an inverse polynomial, i.e., $\frac{1}{p(\cdot)}$)

  $\Rightarrow$ every $\mathcal{A}$ must fail to invert $f_\times$ with **noticeable** probability.

# Multiplication Function

- Recall: multiplication function $f_\times : \mathbb{N}^2 \to \mathbb{N}$.

$$f_\times(x, y) = \begin{cases} \perp & \text{if } x = 1 \vee y = 1 \\ x \cdot y & \text{otherwise} \end{cases}$$

- **Observation 1** (follows from factoring assumption): 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 $\varepsilon$.

- Now suppose that $\varepsilon$ is a **noticeable function** (say e.g. an inverse polynomial, i.e., $\frac{1}{p(\cdot)}$)

  $\Rightarrow$ every $\mathcal{A}$ must fail to invert $f_\times$ with **noticeable** probability.

- This is already useful!

# Multiplication Function

- Recall: multiplication function $f_\times : \mathbb{N}^2 \to \mathbb{N}$.

$$f_\times(x, y) = \begin{cases} \bot & \text{if } x = 1 \vee y = 1 \\ x \cdot y & \text{otherwise} \end{cases}$$

- **Observation 1** (follows from factoring assumption): 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 $\varepsilon$.

- Now suppose that $\varepsilon$ is a **noticeable function** (say e.g. an inverse polynomial, i.e., $\frac{1}{p(\cdot)}$)

  $\Rightarrow$ every $\mathcal{A}$ must fail to invert $f_\times$ with **noticeable** probability.

- This is already useful!

- Usually called a **weak** OWF.

# Noticeable Functions

These are functions that are **at most polynomially small**.

**Definition (Noticeable Function)**

A function $\nu(n)$ is noticeable if $\exists c, n_0$ such that $\forall n > n_0$, $\nu(n) \geqslant \frac{1}{n^c}$.

# 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 noticeable 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?

# Back to Multiplication

- Can we prove that $f_\times$ is a weak OWF?
- Remember the GOOD case? Both $x$ and $y$ are prime.

# 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 noticeable probability, we can prove that $f_\times$ is a weak OWF.

# 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 noticeable probability, we can prove that $f_\times$ is a weak OWF.

**Theorem**

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

# 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 noticeable 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 noticeable!

# 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 noticeable 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 noticeable!
- **Chebyshev's theorem**: An $n$ bit number is a prime with probability $\frac{1}{2n}$

# Proof Idea

- Let $\mathsf{GOOD}$ be the set of inputs $(x, y)$ to $f_\times$ s.t. both $x$ and $y$ are prime numbers

# Proof Idea

- Let $\mathsf{GOOD}$ be the set of inputs $(x, y)$ to $f_\times$ s.t. both $x$ and $y$ are prime numbers
- When $(x, y) \in \mathsf{GOOD}$, adversary cannot invert $f_\times(x, y)$ (due to hardness of factoring)

# Proof Idea

- Let $\mathsf{GOOD}$ be the set of inputs $(x, y)$ to $f_\times$ s.t. both $x$ and $y$ are prime numbers
- When $(x, y) \in \mathsf{GOOD}$, adversary cannot invert $f_\times(x, y)$ (due to hardness of factoring)
- Suppose adversary inverts with probability 1 when $(x, y) \notin \mathsf{GOOD}$

# Proof Idea

- Let $\mathsf{GOOD}$ be the set of inputs $(x, y)$ to $f_\times$ s.t. both $x$ and $y$ are prime numbers
- When $(x, y) \in \mathsf{GOOD}$, adversary cannot invert $f_\times(x, y)$ (due to hardness of factoring)
- Suppose adversary inverts with probability 1 when $(x, y) \notin \mathsf{GOOD}$
- But if $\Pr[(x, y) \in \mathsf{GOOD}]$ is noticeable, then overall, the adversary can only invert with some bounded noticeable probability.

# Proof Idea

- Let $\mathsf{GOOD}$ be the set of inputs $(x, y)$ to $f_\times$ s.t. both $x$ and $y$ are prime numbers
- When $(x, y) \in \mathsf{GOOD}$, adversary cannot invert $f_\times(x, y)$ (due to hardness of factoring)
- Suppose adversary inverts with probability 1 when $(x, y) \notin \mathsf{GOOD}$
- But if $\Pr[(x, y) \in \mathsf{GOOD}]$ is noticeable, then overall, the adversary can only invert with some bounded noticeable 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 $\mathcal{A}$ that breaks weak one-wayness of $f_\times$ with probability *at least* $1 - \frac{1}{q(n)}$, we will construct an adversary $\mathcal{B}$ that breaks the factoring assumption with noticeable probability

# Proof via Reduction

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

**factoring Challenger**

$p, q \leftarrow_\$ \Pi_n$

$z := p \cdot q$

$\xrightarrow{\quad z \quad}$

$\mathcal{B}$

$x, y \leftarrow_\$ \{0,1\}^n$

if $x$ and $y$ both primes

$\quad \tilde{z} := z$

else

$\quad \tilde{z} := x \cdot y$

$\xrightarrow{\quad \tilde{z} \quad}$ $\mathcal{A}$ $\xrightarrow{\quad \tilde{\omega} \quad}$

if $x$ and $y$ both primes

$\quad \omega := \tilde{\omega}$

else

$\quad$ output $\perp$

$\xleftarrow{\quad \omega \quad}$

if $\omega \in \{p, q\}$ output 1

# Proof via Reduction

Why did we randomly choose $(x, y)$ instead of passing the input $z$ directly to $\mathcal{A}$?

Why did we randomly choose $(x, y)$ instead of passing the input $z$ directly to $\mathcal{A}$?

The input of $\mathcal{B}$ is a product of two random $n$-bit **primes** while that of $\mathcal{A}$ is the product of two random $n$-bit **numbers**. Passing the input directly to $\mathcal{A}$ would not emulate the distribution of the inputs given to $\mathcal{A}$.

# Analysis of $\mathcal{B}$

- Since $\mathcal{A}$ is non-uniform PPT, so is $\mathcal{B}$ (using polynomial-time primality testing)

$$\begin{aligned}\Pr[\mathcal{B}\text{ fails}] &= \Pr[\mathcal{B}\text{ passes input to }\mathcal{A}]\cdot\Pr[\mathcal{A}\text{ fails to invert }f_\times] \\ &\quad + \Pr[\mathcal{B}\text{ fails to pass input to }\mathcal{A}] \\ &\leqslant \Pr[\mathcal{A}\text{ fails to invert }f_\times] + \Pr[\mathcal{B}\text{ fails to pass input to }\mathcal{A}] \\ &\leqslant \frac{1}{8n^2} + \left(1-\frac{1}{4n^2}\right) \leqslant \left(1-\frac{1}{8n^2}\right)\end{aligned}$$

- $\mathcal{B}$ succeeds with probability at least $\frac{1}{8n^2}$: Contradiction to factoring assumption!

# Back to Strong OWFs

- How can we construct strong OWFs?

# Back to Strong OWFs

- How can we construct strong OWFs?
- Can we modify $f_\times$ to construct a strong OWF?

# 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 construct a strong OWF from *any* weak OWF?

# 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 construct 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

# 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

# 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 $f(f(\ldots f(x)))$ a good idea?

# Weak to Strong OWFs

**Theorem**

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

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

*is strongly one-way.*

# Weak to Strong OWFs: Intuition

- Recall: OWFs only guarantee average-case hardness

# Weak to Strong OWFs: Intuition

- Recall: OWFs only guarantee average-case hardness
- GOOD inputs: hard to invert, BAD inputs: easy to invert

# 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 **noticeable**.

# 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 **noticeable**.
- In a strong OWF, the fraction of BAD inputs is **negligible**

# 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 **noticeable**.
- 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

# 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 **noticeable**.
- 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

# 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 **noticeable**.
- 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.

# 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!)

# 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, $\mathcal{F} : \left(\{0,1\}^{2n}\right)^m \rightarrow \left(\{0,1\}^{2n}\right)^m$ 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 $\frac{1}{4n^2}$

# 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:*

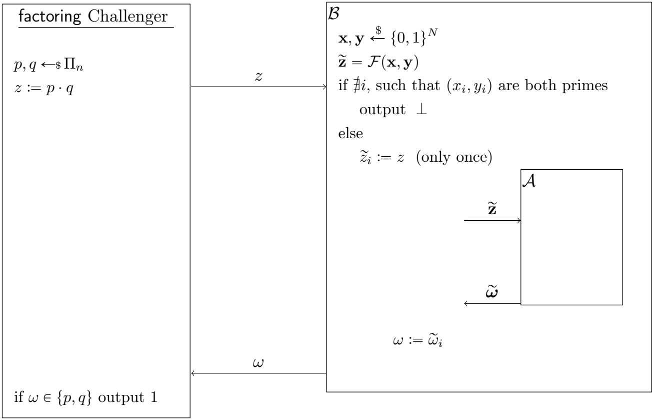
$$\mathcal{F}\big((x_1, y_1), \ldots, (x_m, y_m)\big) = \big(f_\times(x_1, y_1), \ldots, f_\times(x_m, y_m)\big).$$

- **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 $\mathcal{A}$ that inverts $\mathcal{F}$ with prob at least $\varepsilon(2n)$ for some non-negligible function $\varepsilon(\cdot)$
- We will use $\mathcal{A}$ to construct a non-uniform PPT adversary $\mathcal{B}$ that breaks the factoring assumption

# Hardness Amplification for $f_\times$: Reduction



# Analysis of $\mathcal{B}$

- Easy to verify that $\mathcal{B}$ is PPT

# Analysis of $\mathcal{B}$

- Easy to verify that $\mathcal{B}$ is PPT
- Also, easy to verify that $\mathcal{A}$ feeds the correct input distribution to $\mathcal{B}$, except with prob $e^{-n}$

# Analysis of $\mathcal{B}$

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

# Analysis of $\mathcal{B}$

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