Lecture 2: One-way Functions
Concepts:
  - Negligible Functions

Proof Techniques:
Concepts:

- Negligible Functions
- PPT Constructions

Proof Techniques:
Concepts:

- Negligible Functions
- PPT Constructions
- n.u. PPT Adversaries

Proof Techniques:
Concepts:
- Negligible Functions
- PPT Constructions
- n.u. PPT Adversaries
- Function Evaluation (w.h.p.)

Proof Techniques:
Lecture 2: One-way Functions

Concepts:

- Negligible Functions
- PPT Constructions
- n.u. PPT Adversaries
- Function Evaluation (w.h.p.)
- Strong OWF Definition

Proof Techniques:
Concepts:
- Negligible Functions
- PPT Constructions
- n.u. PPT Adversaries
- Function Evaluation (w.h.p.)
- Strong OWF Definition

Proof Techniques:
- Reduction: Functions with string output to Functions with one-bit output
Concepts:
- Negligible Functions
- PPT Constructions
- n.u. PPT Adversaries
- Function Evaluation (w.h.p.)
- Strong OWF Definition

Proof Techniques:
- Reduction: Functions with string output to Functions with one-bit output
- Amplification: Slight advantage in predicting output to computing output w.h.p.
A function \( f : \{0, 1\}^* \rightarrow \{0, 1\}^* \) is a strong one-way function if it satisfies the following two conditions:

1. **Easy to compute.** There is a PPT \( C \) that computes \( f(x) \) on all inputs \( x \in \{0, 1\}^* \), and

2. **Hard to invert.** For any n.u. PPT adversary \( A \), there exists a negligible function \( \nu(\cdot) \) such that for any input length \( n \in \mathbb{N} \),

\[
\Pr \left[ \forall x \in \{0, 1\}^n ; \forall y \in \{0, 1\}^* : f(A(1^n, y), y) = y \right] \leq \nu(n)
\]
Definition (Weak One-way Function)

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

1. **Easy to compute.** There is a PPT $C$ that computes $f(x)$ on all inputs $x \in \{0, 1\}^*$, and
Weak One-way Functions

Definition (Weak One-way Function)

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

1. **Easy to compute.** There is a PPT $C$ that computes $f(x)$ on all inputs $x \in \{0, 1\}^*$, and

2. **Slightly hard to invert.** There exists a polynomial function $q : \mathbb{N} \rightarrow \mathbb{N}$ such that for any adversary $A$, for sufficiently large $n \in \mathbb{N}$, we have:

$$\Pr \left[ x \leftarrow \{0, 1\}^n; y \leftarrow f(x) : f(A(1^n, y)) = y \right] \leq 1 - \frac{1}{q(n)}$$
Theorem (Weak to Strong Amplification)

For any weak one-way function \( f : \{0,1\}^* \to \{0,1\}^* \), there exists a polynomial \( m(\cdot) \) such that the function \( f' : (\{0,1\}^n)^m(n) \to (\{0,1\}^*)^m(n) \) defined as follows:

\[
f'(x_1, x_2, \ldots, x_m(n)) := (f(x_1), f(x_2), \ldots, f(x_m(n))).
\]

is strongly one-way.

Think: Proof
Amplification

Theorem (Weak to Strong Amplification)

For any weak one-way function \( f : \{0, 1\}^* \rightarrow \{0, 1\}^* \), there exists a polynomial \( m(\cdot) \) such that the function

\[
f' : (\{0, 1\}^n)^{m(n)} \rightarrow (\{0, 1\}^*)^{m(n)}
\]

defined as follows:

\[
f'(x_1, x_2, \ldots, x_{m(n)}) := (f(x_1), f(x_2), \ldots, f(x_{m(n)})).
\]

is strongly one-way.
Amplification

Theorem (Weak to Strong Amplification)

For any weak one-way function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$, there exists a polynomial $m(\cdot)$ such that the function $f' : (\{0, 1\}^n)^{m(n)} \rightarrow (\{0, 1\}^*)^{m(n)}$ defined as follows:

$$f'(x_1, x_2, \ldots, x_{m(n)}) := (f(x_1), f(x_2), \ldots, f(x_{m(n)})).$$

is strongly one-way.

Think: Proof
Do they exist?

1. Do they exist?

2. Necessary for most cryptography [Impaglizzo-Luby-89]

3. Insufficient for a lot of useful cryptography [Impagliazzo-Rudich-89]

Technique: Black-box Separation

Interesting Open Problems exist!

Lecture 2: One-way Functions
Discussion

1. Do they exist? NOT Unconditionally
Discussion

1. Do they exist? NOT Unconditionally
2. Necessary for most cryptography [Impaglizzo-Luby-89]
Discussion

1. Do they exist? NOT Unconditionally
2. Necessary for most cryptography [Impaglizzo-Luby-89]
   - Variant of OWF: Distributionally One-way Functions [Impagliazzo-Ph.D.-Thesis]
Discussion

1. Do they exist? NOT Unconditionally
2. Necessary for most cryptography [Impaglizzo-Luby-89]
   - Variant of OWF: Distributionally One-way Functions [Impagliazzo-Ph.D.-Thesis]
   - Interesting Open Problems exist!

Lecture 2: One-way Functions
Discussion

1. Do they exist? NOT Unconditionally
2. Necessary for most cryptography [Impaglizzo-Luby-89]
   - Variant of OWF: Distributionally One-way Functions [Impagliazzo-Ph.D.-Thesis]
   - Interesting Open Problems exist!
3. Insufficient for a lot of useful cryptography [Impagliazzo-Rudich-89]
Discussion

1. Do they exist? NOT Unconditionally
2. Necessary for most cryptography [Impaglizzo-Luby-89]
   - Variant of OWF: Distributionally One-way Functions [Impagliazzo-Ph.D.-Thesis]
   - Interesting Open Problems exist!
3. Insufficient for a lot of useful cryptography [Impagliazzo-Rudich-89]
   - Technique: Black-box Separation
Discussion

1. Do they exist? NOT Unconditionally

2. Necessary for most cryptography [Impaglizzo-Luby-89]
   - Variant of OWF: Distributionally One-way Functions [Impagliazzo-Ph.D.-Thesis]
   - Interesting Open Problems exist!

3. Insufficient for a lot of useful cryptography [Impagliazzo-Rudich-89]
   - Technique: Black-box Separation
   - Interesting Open Problems exist!
Let $\Pi_n$ be the set of all prime numbers $< 2^n$. 

Think: What is $|\Pi_n|$?
Let $\Pi_n$ be the set of all prime numbers $< 2^n$

Think: What is $|\Pi_n|$?
Let $\Pi_n$ be the set of all prime number $< 2^n$

Think: What is $|\Pi_n|$?

Function: $f(x, y) = x \cdot y$
Factorization Problem

1. Let $\Pi_n$ be the set of all prime numbers $< 2^n$
   - Think: What is $|\Pi_n|$?

2. Function: $f(x, y) = x \cdot y$

3. Hardness: For $x, y \leftarrow \Pi_n$, “No adversary can factorize $f(x, y)$ with non-negligible probability”
Candidate Construction

1. Construct a OWF assuming Factorization is Hard

Candidate construction: $f(x, y) = x \cdot y$

Is it a one-way function? No, but it is a weak one-way function and we can amplify it.

Argument: Reduce weak one-way function guarantee of $f$ to hardness of Factorization.

Think: Proof

Lecture 2: One-way Functions
Candidate Construction

1. Construct a OWF assuming Factorization is Hard
2. Candidate construction

\[ f(x, y) = x \cdot y \]

Is it a one-way function? No, but it is a weak one-way function and we can amplify it.

Argument: Reduce weak one-way function guarantee of \( f \) to hardness of Factorization.
Construct a OWF assuming Factorization is Hard
Candidate construction: $f(x, y) = x \cdot y$
Candidate Construction

1. Construct a OWF assuming Factorization is Hard
2. Candidate construction: \( f(x, y) = x \cdot y \)
3. Is it a one-way function?
Candidate Construction

1. Construct a OWF assuming Factorization is Hard
2. Candidate construction: \( f(x, y) = x \cdot y \)
3. Is it a one-way function? No, but it is a weak one-way function and we can amplify it
1. Construct a OWF assuming Factorization is Hard
2. Candidate construction: \( f(x, y) = x \cdot y \)
3. Is it a one-way function? No, but it is a weak one-way function and we can amplify it
4. Argument: Reduce weak one-way function guarantee of \( f \) to hardness of Factorization
Construct a OWF assuming Factorization is Hard

Candidate construction: $f(x, y) = x \cdot y$

Is it a one-way function? No, but it is a weak one-way function and we can amplify it

Argument: Reduce weak one-way function guarantee of $f$ to hardness of Factorization
  - Think: Proof