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:

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.

Definition (Strong One-Way Function)

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

1. **Easy to compute.** There is a PPT $\mathcal{C}$ that computes $f(x)$ on all inputs $x \in \{0,1\}^*$, and
2. **Hard to invert.** For any n.u. PPT adversary $\mathcal{A}$, there exists a negligible function $\nu(\cdot)$ such that for any input length $n \in \mathbb{N}$,

$$\Pr\left[x \xleftarrow{\$} \{0,1\}^n; y \leftarrow f(x) \colon f(\mathcal{A}(1^n, y), y) = y\right] \leqslant \nu(n)$$

Weak One-way Functions

Definition (Weak One-way Function)

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

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

Weak One-way Functions

Definition (Weak One-way Function)

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

1. **Easy to compute.** There is a PPT $\mathcal{C}$ that computes $f(x)$ on all inputs $x \in \{0,1\}^*$, and
2. **Slightly hard to invert.** There exists a polynomial function $q\colon \mathbb{N} \to \mathbb{N}$ such that for any adversary $\mathcal{A}$, for sufficiently large $n \in \mathbb{N}$, we have:

$$\Pr\left[x \xleftarrow{\$} \{0,1\}^n; y \leftarrow f(x)\colon f(\mathcal{A}(1^n, y)) = y\right] \leqslant 1 - \frac{1}{q(n)}$$

Amplification

Amplification

Theorem (Weak to Strong Amplification)

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

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

is strongly one-way.

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 $f' : \left(\{0,1\}^n\right)^{m(n)} \to \left(\{0,1\}^*\right)^{m(n)}$ defined as follows:

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

is strongly one-way.

- Think: Proof

Discussion

1. Do they exist?

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!

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!

Factorization Problem

1. Let Π_n be the set of all prime number $< 2^n$

Factorization Problem

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

Factorization Problem

1. Let Π_n be the set of all prime number $< 2^n$
   - Think: What is $|\Pi_n|$?
2. Function: $f(x, y) = x \cdot y$

Factorization Problem

1. Let Π_n be the set of all prime number $< 2^n$
   - Think: What is $|\Pi_n|$?
2. Function: $f(x, y) = x \cdot y$
3. Hardness: For $x, y \xleftarrow{\$} \Pi_n$, "No adversary can factorize f(x,y) with non-negligible probability"

Candidate Construction

1. Construct a OWF assuming Factorization is Hard

Candidate Construction

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

Candidate Construction

1. Construct a OWF assuming Factorization is Hard
2. 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

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

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