One-Way Functions

CS 276: Introduction to Cryptography

Sanjam Garg

January 26, 2026

Overview

1. Hardness Amplification
2. Levin's One-Way Function

Weak vs Strong One-Way Functions

Strong One-Way Function

Inversion succeeds with **negligible** probability.

$$\Pr[\mathcal{A}(1^n, f(x)) \in f^{-1}(f(x))] \leq \mathsf{negl}(n)$$

Weak vs Strong One-Way Functions

Strong One-Way Function

Inversion succeeds with **negligible** probability.

$$\Pr[\mathcal{A}(1^n, f(x)) \in f^{-1}(f(x))] \leq \mathsf{negl}(n)$$

Weak One-Way Function

Inversion succeeds with probability **bounded away from 1**.

$$\Pr[\mathcal{A}(1^n, f(x)) \in f^{-1}(f(x))] \leq 1 - \alpha_f(n)$$

where $\alpha_f(n)$ is **noticeable**.

Weak vs Strong One-Way Functions

Strong One-Way Function

Inversion succeeds with **negligible** probability.

$$\Pr[\mathcal{A}(1^n, f(x)) \in f^{-1}(f(x))] \leq \mathrm{negl}(n)$$

Weak One-Way Function

Inversion succeeds with probability **bounded away from 1**.

$$\Pr[\mathcal{A}(1^n, f(x)) \in f^{-1}(f(x))] \leq 1 - \alpha_f(n)$$

where $\alpha_f(n)$ is **noticeable**.

Question

Can we amplify weak OWFs to strong OWFs?

Hardness Amplification: Motivation

Powerful Result

This shows that even if a function is only 'weakly' one-way (i.e., invertible with noticeable probability), we can amplify it to get a 'strong' one-way function (invertible with only negligible probability).

Hardness Amplification: Motivation

Powerful Result

This shows that even if a function is only 'weakly' one-way (i.e., invertible with noticeable probability), we can amplify it to get a 'strong' one-way function (invertible with only negligible probability).

Why This Matters

- Weak OWFs might be easier to construct
- Strong OWFs are what we need for cryptography
- Amplification bridges the gap

Hardness Amplification Theorem

Theorem 1

If there exists a weak one-way function, then there exists a (strong) one-way function.

Hardness Amplification Theorem

Theorem 1

If there exists a weak one-way function, then there exists a (strong) one-way function.

Construction

Given weak OWF $f : \{0,1\}^n \to \{0,1\}^m$ with noticeable function $\alpha_f(n)$, define:

$$g(x_1, \ldots, x_q) = f(x_1) \| f(x_2) \| \cdots \| f(x_q)$$

where $q = \lceil \frac{2n}{\alpha_f(n)} \rceil$.

Intuition for the Construction

Key Idea

A weak one-way function is "strong" in a small part of its domain. For this construction to result in a strong one-way function, we need just one of the q instantiations to be in the "hard" part.

Intuition for the Construction

Key Idea

A weak one-way function is "strong" in a small part of its domain. For this construction to result in a strong one-way function, we need just one of the q instantiations to be in the "hard" part.

More Concrete

If the weak OWF is hard to invert on at least an $\alpha_f(n)$ fraction of inputs, then with q independent copies, the probability that **ALL** are easy to invert is at most $(1 - \alpha_f(n))^q$, which becomes negligible for large enough q.

Proof: Setup

Goal

Show that if $\mathcal{B}$ breaks g with non-negligible probability, then we can construct $\mathcal{A}$ that breaks f with probability $> 1 - \alpha_f(n)$.

Proof: Setup

Goal

Show that if $\mathcal{B}$ breaks g with non-negligible probability, then we can construct $\mathcal{A}$ that breaks f with probability $> 1 - \alpha_f(n)$.

Construction of $\mathcal{A}$

$\mathcal{A}$ on input $(1^n, y)$ where $y = f(x)$ for random x:

1. Repeat $T = \frac{4n^2}{\alpha_f(n)\mu_{\mathcal{B},g}(nq)}$ times:
   - Sample $i \leftarrow [q]$ uniformly
   - Sample $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_q \leftarrow \{0,1\}^n$
   - Set $y_j = f(x_j)$ for $j \neq i$ and $y_i = y$
   - $(x'_1, \ldots, x'_q) \leftarrow \mathcal{B}(1^{nq}, y_1 \| \cdots \| y_q)$
   - If $f(x'_i) = y$, output x'_i and halt
2. Output $\perp$

Why the Analysis is Tricky

Naive Intuition

One might think: "If $\mathcal{B}$ succeeds with non-negligible probability, then at least one of the T iterations should succeed, so $\mathcal{A}$ should invert $f(x)$ with high probability."

Why the Analysis is Tricky

Naive Intuition

One might think: "If $\mathcal{B}$ succeeds with non-negligible probability, then at least one of the T iterations should succeed, so $\mathcal{A}$ should invert $f(x)$ with high probability."

Why This Doesn't Work

This intuition assumes the T iterations are **independent**, but they're **not**!

Why the Analysis is Tricky

Naive Intuition

One might think: "If $\mathcal{B}$ succeeds with non-negligible probability, then at least one of the T iterations should succeed, so $\mathcal{A}$ should invert $f(x)$ with high probability."

Why This Doesn't Work

This intuition assumes the T iterations are **independent**, but they're **not**!

The Problem

All T iterations share the **same** challenge x (through $y = f(x)$). The success or failure of different iterations is **correlated**.

Why Executions Are Correlated

What Makes Them Correlated?

- All iterations use the **same** $y = f(x)$ (the challenge we're trying to invert)
- Each iteration samples different $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_q$
- But the i-th position always uses the **same** $y = f(x)$
- $\mathcal{B}$'s behavior may depend on the entire input $(y_1, \ldots, y_q)$

Why Executions Are Correlated

What Makes Them Correlated?

- All iterations use the **same** $y = f(x)$ (the challenge we're trying to invert)
- Each iteration samples different $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_q$
- But the i-th position always uses the **same** $y = f(x)$
- $\mathcal{B}$'s behavior may depend on the entire input $(y_1, \ldots, y_q)$

Consequence

- If $\mathcal{B}$ fails on one iteration, it might be more likely to fail on others
- We cannot use simple union bound: $\Pr[\text{all fail}] \neq \prod_{t=1}^{T} \Pr[\text{iteration } t \text{ fails}]$
- Need a more sophisticated analysis

The Correlation Problem

Example of Why Correlation Matters

Suppose:

- For some "bad" x, $\mathcal{B}$ always fails (probability 0)
- For "good" x, $\mathcal{B}$ succeeds with probability $p > 0$
- If iterations were independent: $\Pr[\text{all } T \text{ fail}] = (1-p)^T$
- But they're correlated! If x is bad, **all** iterations fail

The Correlation Problem

Example of Why Correlation Matters

Suppose:

- For some "bad" x, $\mathcal{B}$ always fails (probability 0)
- For "good" x, $\mathcal{B}$ succeeds with probability $p > 0$
- If iterations were independent: $\Pr[\text{all } T \text{ fail}] = (1-p)^T$
- But they're correlated! If x is bad, **all** iterations fail

Our Solution

1. Define set S of "bad" x's (where $\mathcal{A}$ has low success probability)
2. Show that S is small: $\Pr[x \in S] \leq \alpha_f(n)/2$
3. For $x \notin S$, show that $\mathcal{A}$ succeeds with high probability

Proof: Running Time

Key Observations

1. Each iteration of $\mathcal{A}$ runs in polynomial time
2. $\mu_{\mathcal{B},g}(nq)$ is non-negligible
3. For infinitely many n, $\mu_{\mathcal{B},g}(nq) \geq$ some noticeable function
4. Therefore, T is polynomial in n for infinitely many n

Proof: Running Time

Key Observations

1. Each iteration of $\mathcal{A}$ runs in polynomial time
2. $\mu_{\mathcal{B},g}(nq)$ is non-negligible
3. For infinitely many n, $\mu_{\mathcal{B},g}(nq) \geq$ some noticeable function
4. Therefore, T is polynomial in n for infinitely many n

Conclusion

$\mathcal{A}$ runs in polynomial time (for infinitely many n).

Proof: Define Bad Set S

Definition

$$S := \left\{ x \mid \Pr_{\mathcal{B}}[\mathcal{A} \text{ inverts } f(x) \text{ in a single iteration}] \leq \frac{\alpha_f(n)\mu_{\mathcal{B},g}(nq)}{4n} \right\}$$

Proof: Define Bad Set S

Definition

$$S := \left\{ x \mid \Pr_{\mathcal{B}} [\mathcal{A} \text{ inverts } f(x) \text{ in a single iteration}] \leq \frac{\alpha_f(n)\mu_{\mathcal{B},g}(nq)}{4n} \right\}$$

Intuition

S contains the "bad" x's where $\mathcal{A}$ has low probability of success in a single iteration.

Proof: Define Bad Set S

Definition

$$S := \left\{ x \mid \Pr_{\mathcal{B}}[\mathcal{A} \text{ inverts } f(x) \text{ in a single iteration}] \leq \frac{\alpha_f(n)\mu_{\mathcal{B},g}(nq)}{4n} \right\}$$

Intuition

S contains the "bad" x's where $\mathcal{A}$ has low probability of success in a single iteration.

Goal

Show that $\Pr_{x \leftarrow \{0,1\}^n}[x \in S] \leq \frac{\alpha_f(n)}{2}$.

Proof: S is Small (Part 1)

Claim

$$\Pr_{x \leftarrow \{0,1\}^n}[x \in S] \leq \frac{\alpha_f(n)}{2}$$

Proof: S is Small (Part 1)

Claim

$$\Pr_{x \leftarrow \{0,1\}^n}[x \in S] \leq \frac{\alpha_f(n)}{2}$$

Proof by Contradiction

Assume $\Pr[x \in S] > \frac{\alpha_f(n)}{2}$. Then:

$$\begin{aligned}\mu_{\mathcal{B},g}(nq) &= \Pr_{(x_1,\ldots,x_q)}[\mathcal{B} \text{ succeeds}] \\ &\leq \Pr[\forall i : x_i \notin S] + \sum_{i=1}^{q} \Pr[\mathcal{B} \text{ succeeds} \wedge x_i \in S]\end{aligned}$$

Proof: S is Small (Part 2)

Continuing the Calculation

$$\leq \left(1 - \frac{\alpha_f(n)}{2}\right)^q + q \cdot \Pr[\mathcal{A} \text{ inverts } f(x) \text{ in one iteration} \wedge x \in S]$$

$$= \left(1 - \frac{\alpha_f(n)}{2}\right)^{\frac{2n}{\alpha_f(n)}} + q \cdot \Pr[x \in S] \cdot \Pr[\text{success} \mid x \in S]$$

$$\leq e^{-n} + \frac{2n}{\alpha_f(n)} \cdot 1 \cdot \frac{\mu_{\mathcal{B},g}(nq) \cdot \alpha_f(n)}{4n}$$

$$= e^{-n} + \frac{\mu_{\mathcal{B},g}(nq)}{2}$$

Proof: S is Small (Part 2)

Continuing the Calculation

$$
\begin{aligned}
&\leq \left(1 - \frac{\alpha_f(n)}{2}\right)^q + q \cdot \Pr[\mathcal{A} \text{ inverts } f(x) \text{ in one iteration} \wedge x \in S] \\
&= \left(1 - \frac{\alpha_f(n)}{2}\right)^{\frac{2n}{\alpha_f(n)}} + q \cdot \Pr[x \in S] \cdot \Pr[\text{success} \mid x \in S] \\
&\leq e^{-n} + \frac{2n}{\alpha_f(n)} \cdot 1 \cdot \frac{\mu_{\mathcal{B},g}(nq) \cdot \alpha_f(n)}{4n} \\
&= e^{-n} + \frac{\mu_{\mathcal{B},g}(nq)}{2}
\end{aligned}
$$

Contradiction

This implies $\mu_{\mathcal{B},g}(nq) \leq 2e^{-n}$, contradicting that $\mu_{\mathcal{B},g}$ is non-negligible!

Proof: Final Success Probability

Calculation

$$
\begin{aligned}
&\Pr_{x \leftarrow \{0,1\}^n}[\mathcal{A}(1^n, f(x)) = \perp] \\
&= \Pr_x[x \in S] + \Pr_x[x \notin S] \cdot \Pr[\mathcal{B} \text{ fails all } T \text{ iterations} \mid x \notin S] \\
&\leq \frac{\alpha_f(n)}{2} + (\Pr[\mathcal{B} \text{ fails in one iteration} \mid x \notin S])^T \\
&\leq \frac{\alpha_f(n)}{2} + \left(1 - \frac{\alpha_f(n)\mu_{\mathcal{B},g}(nq)}{4n}\right)^T \\
&\leq \frac{\alpha_f(n)}{2} + e^{-n} \leq \alpha_f(n)
\end{aligned}
$$

Proof: Final Success Probability

Calculation

$$
\begin{aligned}
&\Pr_{x \leftarrow \{0,1\}^n}[\mathcal{A}(1^n, f(x)) = \perp] \\
&= \Pr_x[x \in S] + \Pr_x[x \notin S] \cdot \Pr[\mathcal{B} \text{ fails all } T \text{ iterations} \mid x \notin S] \\
&\leq \frac{\alpha_f(n)}{2} + (\Pr[\mathcal{B} \text{ fails in one iteration} \mid x \notin S])^T \\
&\leq \frac{\alpha_f(n)}{2} + \left(1 - \frac{\alpha_f(n)\mu_{\mathcal{B},g}(nq)}{4n}\right)^T \\
&\leq \frac{\alpha_f(n)}{2} + e^{-n} \leq \alpha_f(n)
\end{aligned}
$$

Conclusion

$$\Pr[\mathcal{A}(1^n, f(x)) \in f^{-1}(f(x))] = 1 - \Pr[\mathcal{A}(1^n, f(x)) = \perp] > 1 - \alpha_f(n)$$

Levin's Construction: Future-Proof OWF

Goal

Construct an **explicit** one-way function that is secure as long as **any** one-way function exists.

Levin's Construction: Future-Proof OWF

Goal

Construct an **explicit** one-way function that is secure as long as **any** one-way function exists.

Why This Matters

- Typical primitives rely on **specific** hardness assumptions
- Those assumptions might be broken in the future
- Levin's OWF is **future-proof**: secure as long as **some** OWF exists

Levin's Construction: Future-Proof OWF

Goal

Construct an **explicit** one-way function that is secure as long as **any** one-way function exists.

Why This Matters

- Typical primitives rely on **specific** hardness assumptions
- Those assumptions might be broken in the future
- Levin's OWF is **future-proof**: secure as long as **some** OWF exists

Remarkable Result

This shows that if OWFs exist at all, we can construct one explicitly without knowing which specific assumption to rely on.

High-Level Idea

Intuition

- Parse input as (machine code M, input x)
- Output $(M, M(x))$ if $M(x)$ halts in time $|x|^2$
- For large enough n, we'll hit a one-way function with noticeable probability

High-Level Idea

Intuition

- Parse input as (machine code M, input x)
- Output $(M, M(x))$ if $M(x)$ halts in time $|x|^2$
- For large enough n, we'll hit a one-way function with noticeable probability

Key Insight

Since we assume one-way functions exist, there exists a uniform machine $\tilde{M}$ such that $|\tilde{M}|$ is constant and $\tilde{M}(x)$ is hard to invert for a random input x.

Levin's Function: Formal Definition

Construction

$$h(M, x) = \begin{cases} M \| M(x) & \text{if } M(x) \text{ halts in } \leq |x|^2 \text{ steps} \\ M \| 0 & \text{otherwise} \end{cases}$$

where $|M| = \log n$ and $|x| = n - \log n$.

Levin's Function: Formal Definition

Construction

$$h(M, x) = \begin{cases} M \| M(x) & \text{if } M(x) \text{ halts in } \leq |x|^2 \text{ steps} \\ M \| 0 & \text{otherwise} \end{cases}$$

where $|M| = \log n$ and $|x| = n - \log n$.

Key Properties

1. **Explicit**: Can be computed efficiently
2. **Weak OWF**: If any OWF exists, h is weak one-way
3. **Amplifiable**: Can use hardness amplification to get strong OWF

Why n^2 Time Bound?

Lemma

If there exists a one-way function computable in time n^c for a constant c, then there exists a one-way function computable in time n^2.

Why n^2 Time Bound?

Lemma

If there exists a one-way function computable in time n^c for a constant c, then there exists a one-way function computable in time n^2.

Construction

Given $f : \{0,1\}^n \to \{0,1\}^n$ computable in time n^c, define:

$$g(x, y) = f(x) \| y$$

where $x \in \{0,1\}^n, y \in \{0,1\}^{n^c}$.
Then $g(x, y)$ takes time linear in input length.

Proof Strategy for Levin's OWF

Goal

Show that if one-way functions exist, then h is a weak one-way function with $\alpha_h(n) = \frac{1}{n^2}$.

Proof Strategy for Levin's OWF

Goal

Show that if one-way functions exist, then h is a weak one-way function with $\alpha_h(n) = \frac{1}{n^2}$.

Proof by Contradiction

Assume adversary $\mathcal{A}$ breaks h with probability $\geq 1 - \frac{1}{n^2}$ for all sufficiently large n:

$$\mu_{\mathcal{A},h}(n) = \Pr_{(M,x)\leftarrow\{0,1\}^n}[\mathcal{A}(1^n, h(M,x)) \in h^{-1}(h(M,x))] \geq 1 - \frac{1}{n^2}$$

Proof Strategy for Levin's OWF

Goal

Show that if one-way functions exist, then h is a weak one-way function with $\alpha_h(n) = \frac{1}{n^2}$.

Proof by Contradiction

Assume adversary $\mathcal{A}$ breaks h with probability $\geq 1 - \frac{1}{n^2}$ for all sufficiently large n:

$$\mu_{\mathcal{A},h}(n) = \Pr_{(M,x)\leftarrow\{0,1\}^n}[\mathcal{A}(1^n, h(M,x)) \in h^{-1}(h(M,x))] \geq 1 - \frac{1}{n^2}$$

Key Setup

- By existence of OWFs and Lemma, there exists OWF $\tilde{M}$ computable in time n^2
- Consider $n > 2^{|\tilde{M}|}$ so $\tilde{M}$ can be described with $\log n$ bits
- $\tilde{M}$ appears with probability $\frac{1}{n}$ when sampling random M

Proof: Constructing Adversary $\mathcal{B}$

Construction

$\mathcal{B}$ on input y (where $y = \tilde{M}(x)$ for random x):

1. Output the $(n - \log n)$ lower-order bits of $\mathcal{A}(1^n, \tilde{M} \| y)$

Proof: Constructing Adversary $\mathcal{B}$

Construction

$\mathcal{B}$ on input y (where $y = \tilde{M}(x)$ for random x):

1. Output the $(n - \log n)$ lower-order bits of $\mathcal{A}(1^n, \tilde{M} \| y)$

Intuition

- If $\mathcal{A}$ successfully inverts $h(\tilde{M}, x) = \tilde{M} \| \tilde{M}(x)$
- Then $\mathcal{A}$ outputs something of form $\tilde{M} \| x'$ where $h(\tilde{M}, x') = h(\tilde{M}, x)$
- This means $\tilde{M}(x') = \tilde{M}(x)$, so x' is a valid preimage
- $\mathcal{B}$ extracts x' from $\mathcal{A}$'s output

Proof: Success Probability (Part 1)

Success Probability of $\mathcal{B}$

$$\mu_{\mathcal{B},\tilde{M}}(n - \log n) = \Pr_{x \leftarrow \{0,1\}^{n-\log n}}\left[\mathcal{B}(y) \in \tilde{M}^{-1}(\tilde{M}(x))\right]$$
$$\geq \Pr_{x}\left[\mathcal{A}(1^n, \tilde{M}\|\tilde{M}(x)) \in \tilde{M}\|\tilde{M}^{-1}(\tilde{M}(x))\right]$$

Proof: Success Probability (Part 1)

Success Probability of $\mathcal{B}$

$$\mu_{\mathcal{B},\tilde{M}}(n - \log n) = \Pr_{x \leftarrow \{0,1\}^{n-\log n}}\left[\mathcal{B}(y) \in \tilde{M}^{-1}(\tilde{M}(x))\right]$$
$$\geq \Pr_{x}\left[\mathcal{A}(1^n, \tilde{M}\|\tilde{M}(x)) \in \tilde{M}\|\tilde{M}^{-1}(\tilde{M}(x))\right]$$

Key Observation

If $\mathcal{A}$ outputs something of the form $\tilde{M}\|x'$ where $h(\tilde{M}, x') = h(\tilde{M}, x)$, then x' is a valid preimage of $\tilde{M}(x)$.

Proof: Success Probability (Part 2)

Relating to $\mathcal{A}$'s Success

We know:

$$1 - \frac{1}{n^2} \leq \mu_{\mathcal{A},h}(n) = \Pr_{(M,x)}[\mathcal{A}(1^n, h(M,x)) \in h^{-1}(h(M,x))]$$

Proof: Success Probability (Part 2)

Relating to $\mathcal{A}$'s Success

We know:

$$1 - \frac{1}{n^2} \leq \mu_{\mathcal{A},h}(n) = \Pr_{(M,x)}[\mathcal{A}(1^n, h(M,x)) \in h^{-1}(h(M,x))]$$

Splitting by Machine

$$\begin{aligned}
\mu_{\mathcal{A},h}(n) &\leq \Pr_M[M = \tilde{M}] \cdot \Pr_x\left[\mathcal{A}(1^n, \tilde{M}\|\tilde{M}(x)) \in \tilde{M}\|\tilde{M}^{-1}(\tilde{M}(x))\right] \\
&\quad + \Pr_M[M \neq \tilde{M}] \cdot 1 \\
&\leq \frac{1}{n} \cdot \mu_{\mathcal{B},\tilde{M}}(n - \log n) + \frac{n-1}{n} \\
&= \frac{1}{n} \cdot \mu_{\mathcal{B},\tilde{M}}(n - \log n) + 1 - \frac{1}{n}
\end{aligned}$$

Proof: Contradiction

Rearranging

From the previous slide:

$$1 - \frac{1}{n^2} \leq \frac{1}{n} \cdot \mu_{\mathcal{B},\tilde{M}}(n - \log n) + 1 - \frac{1}{n}$$

Proof: Contradiction

Rearranging

From the previous slide:

$$1 - \frac{1}{n^2} \leq \frac{1}{n} \cdot \mu_{\mathcal{B},\tilde{M}}(n - \log n) + 1 - \frac{1}{n}$$

Solving for $\mu_{\mathcal{B},\tilde{M}}$

$$\begin{aligned}
1 - \frac{1}{n^2} &\leq \frac{1}{n} \cdot \mu_{\mathcal{B},\tilde{M}}(n - \log n) + 1 - \frac{1}{n} \\
-\frac{1}{n^2} &\leq \frac{1}{n} \cdot \mu_{\mathcal{B},\tilde{M}}(n - \log n) - \frac{1}{n} \\
\frac{1}{n} - \frac{1}{n^2} &\leq \frac{1}{n} \cdot \mu_{\mathcal{B},\tilde{M}}(n - \log n) \\
1 - \frac{1}{n} &\leq \mu_{\mathcal{B},\tilde{M}}(n - \log n)
\end{aligned}$$

Proof: Contradiction

Rearranging

From the previous slide:

$$1 - \frac{1}{n^2} \leq \frac{1}{n} \cdot \mu_{\mathcal{B},\tilde{M}}(n - \log n) + 1 - \frac{1}{n}$$

Solving for $\mu_{\mathcal{B},\tilde{M}}$

$$\begin{aligned}
1 - \frac{1}{n^2} &\leq \frac{1}{n} \cdot \mu_{\mathcal{B},\tilde{M}}(n - \log n) + 1 - \frac{1}{n} \\
-\frac{1}{n^2} &\leq \frac{1}{n} \cdot \mu_{\mathcal{B},\tilde{M}}(n - \log n) - \frac{1}{n} \\
\frac{1}{n} - \frac{1}{n^2} &\leq \frac{1}{n} \cdot \mu_{\mathcal{B},\tilde{M}}(n - \log n) \\
1 - \frac{1}{n} &\leq \mu_{\mathcal{B},\tilde{M}}(n - \log n)
\end{aligned}$$

Proof: Conclusion

What We Proved

- If $\mathcal{A}$ breaks h with probability $\geq 1 - \frac{1}{n^2}$
- Then $\mathcal{B}$ breaks $\tilde{M}$ with probability $\geq \frac{n-1}{n}$
- This contradicts that $\tilde{M}$ is a one-way function
- Therefore, no such $\mathcal{A}$ can exist

Proof: Conclusion

What We Proved

- If $\mathcal{A}$ breaks h with probability $\geq 1 - \frac{1}{n^2}$
- Then $\mathcal{B}$ breaks $\tilde{M}$ with probability $\geq \frac{n-1}{n}$
- This contradicts that $\tilde{M}$ is a one-way function
- Therefore, no such $\mathcal{A}$ can exist

Final Result

- h is a **weak one-way function** with $\alpha_h(n) = \frac{1}{n^2}$
- Can use hardness amplification to get a **strong one-way function**
- This gives us an explicit OWF as long as any OWF exists!