One-way functions based on average-case assumption

Dmitry Itsykson
joint with Edward A. Hirsch

Steklov Institute of Mathematics at St. Petersburg

August 31, 2007

Plan of the talk

- One-way functions
- Average-case complexity
- Average-case hardness implies cryptographic hardness

One-way functions

Intuition:
Function f is one-way if

- it is easy to compute f;
- it is hard to invert f.

Example (RSA function)
$f(x) = x^d \bmod pq$, p, q are big prime numbers, d is integer.

Cryptographic motivation

User authentication by password (private key cryptosystems)

Server saves only $f(password)$

Other

- Public key cryptosystem (one-way functions with trapdoors)
- Digital signature (one-way permutations).

Formal definition

Worst case one-way function

f is worst case one-way if

- f is computable in polynomial time;
- f is honest i.e. $\forall y = f(x), |x| < poly(|y|)$;
- f^{-1} is not computable in polynomial time.

Defect of definition

Only one hard output!

$\mathbf{P} \neq \mathbf{NP} \implies \exists$ worst case one-way

$f : (\varphi, \sigma) \mapsto \varphi$ if σ is satisfying assignment of formula ϕ.

Cryptographic strong one-way function

f is strong one-way if

- f is computable in polynomial time;
- f is honest i.e. $\forall y = f(x), |x| < poly(|y|)$;
- $\forall$ randomized poly-time algorithm B $\forall$ polynomial $p(n)$ $\Pr_{x \leftarrow U(\{0,1\}^n)} \{B(f(x)) \in f^{-1}(f(x))\} \leq \frac{1}{p(n)}$.

Strong vs weak one-way

Weak one-way function

f is weak one-way if

- f is computable in polynomial time;
- f is honest i.e. $\forall y = f(x), |x| < poly(y)$;
- $\exists$ polynomial $p(n)$ $\forall$ randomized poly-time algorithm B $\Pr_{x \leftarrow U(\{0,1\}^n)} \{B(f(x)) \notin f^{-1}(f(x))\} \geq \frac{1}{p(n)}$.

Theorem

If there exists weak one-way function then there exists strong one-way function.

Strong vs weak one-way

Weak one-way function

f is weak one-way if

- f is computable in polynomial time;
- f is honest i.e. $\forall y = f(x), |x| < poly(y)$;
- $\exists$ polynomial $p(n)$ $\forall$ randomized poly-time algorithm B $\Pr\limits_{x \leftarrow U(\{0,1\}^n)} \{B(f(x)) \notin f^{-1}(f(x))\} \geq \frac{1}{p(n)}$.

Theorem

If there exists weak one-way function then there exists strong one-way function.

Average-case complexity

Ensemble of distributions

$D = \{D_n\}_{n=1}^{\infty}$ where $D_n : \{0,1\}^n \to \mathbb{R}_+$ such that

$$\sum_{a \in \{0,1\}^n} D_n(a) = 1.$$

Distributed problem

(f, D) where $f : \{0,1\}^* \to 2^{\{0,1\}^*}$ and an ensemble of distributions $D = \{D_n\}_{n=1}^{\infty}$.

Average-case complexity

Average polynomial time

A distributed problem (f, D) can be solved in polynomial average time if there exists an algorithm $A(x)$ which is $T(n)$ time

- $A(x) \in f(x)$;
- $\exists \epsilon > 0 : \mathbf{E}_{x \leftarrow D_n}\{T(n)^\epsilon\} = O(n)$.

Average polynomial time (equivalent definition)

$(f, D) \in$ **FAvgP** if there exists an algorithm $A(x, \delta)$ which is polynomial in $|x|$ and in $\frac{1}{\delta}$, such that

- $A(x, \delta) \in f(x) \cup \{\perp\}$;
- $\Pr_{x \leftarrow D_n}\{A(x, \delta) = \perp\} < \delta$.

Randomized average polynomial time

$(f, D) \in \mathbf{FAvgBPP}$ if there exists $0 < \epsilon < \frac{1}{2}$ and a randomized algorithm $A(x, \delta)$ which is polynomial in $|x|$ and in $\frac{1}{\delta}$ such that

- $\Pr\{A(x, \delta) \notin f(x) \cup \{\perp\}\} \leq \epsilon$ where the probability is taken over random bits of the algorithm A;
- $\Pr_{x \leftarrow D_n}\{\Pr\{A(x, \delta) = \perp\} \geq \epsilon\} \leq \delta$ where the inner probability is taken over random bits of the algorithm A;

$\mathbf{DistNP} = (\mathbf{NP}, \mathbf{PSamplable})$

Average-case reduction

$(f, D) \leq (f', D')$

- $\exists g, h$ are polynomial time computable
- $y \in f'(h(x)) \implies g(y) \in f(x)$ for any y and x with $D_{|x|}(x) > 0$;
- $\exists$ polynomial $p(n)$, such that $\sum_{x:h(x)=y,|x|=n} D_n(x) \leq p(n)D'_{|y|}(y)$ for any y.

Lemma 1

$(f, D) \leq (f', D'), (f', D') \in \mathbf{FAvgP} \implies (f, g) \in \mathbf{FAvgP}$

Lemma 2

$(f, D) \leq (f', D'), (f', D') \in \mathbf{FAvgBPP} \implies (f, g) \in \mathbf{FAvgBPP}$

Dreams

1st dream

$\mathbf{P} \neq \mathbf{NP} \implies \exists$ cryptographic one-way functions.

2d dream

$\mathbf{DistNP} \not\subset \mathbf{FAvgBPP} \implies \exists$ cryprographic one-way functions.

Dreams

1st dream

$\mathbf{P} \neq \mathbf{NP} \implies \exists$ cryptographic one-way functions.

2d dream

$\mathbf{DistNP} \not\subset \mathbf{FAvgBPP} \implies \exists$ cryprographic one-way functions.

Problem statement

Question

Suppose we have function f:

- f is polynomial time computable;
- $(f^{-1}, f(U(\{0,1\}^n)))$ is not from **FAvgBPP**.

Is it possible to use f to construct one-way function?

Answer

Yes, it is possible.

Fact. Inverse statement

If all languages from **NP** with uniform distribution are in **AvgBPP**, then there is no one-way functions.

Problem statement

Question

Suppose we have function f:

- f is polynomial time computable;
- $(f^{-1}, f(U(\{0,1\}^n)))$ is not from **FAvgBPP**.

Is it possible to use f to construct one-way function?

Answer

Yes, it is possible.

Fact. Inverse statement

If all languages from **NP** with uniform distribution are in **AvgBPP**, then there is no one-way functions.

The proof

Theorem

If there exists a length preserving polynomial time function f that can not be inverted in randomized average polynomial time then there exists strong one-way function.

Plan of the proof

- Padding version $f_p : (x, z) \mapsto (f(x), 1^{|z|})$;
- Distributions $U^f = f(U), U^{f_p} = f_p(U)$;
- $(f^{-1}, U^f) \leq (f_p^{-1}, U^{f_p})$;
- We will prove that f_p is weak one-way function.

Proof

- Suppose $\exists$ algorithm B; $\Pr\{B(f_p(x)) \in f_p^{-1}(f_p(x))\} \geq \frac{1}{n}$;
- We will show that $(f_p, f_p(U)) \in$ **FAvgBPP**;
- $x \mapsto x1^{\lceil \frac{1}{\delta} \rceil}$;
- $A(x, \delta)$ is defined by $B(x, 1^{\lceil \frac{1}{\delta} \rceil})$;
- Key observation $U^{f_p}(f(y), 1^t) = U^{f_p}(f(y)) = 2^{-|f(y)|}$;
- $\Pr\{B \text{ makes mistake}\} \leq \frac{1}{n + \frac{1}{\delta}} \leq \delta$.
- Since $(f^{-1}, U^f) \leq (f_p^{-1}, U^{f_p})$ we conclude $(f^{-1}, U^f) \in$ **FAvgBPP**. Contradiction.

Technical problem

Padding should be economic! Symbol "," is too expensive.

Open question

Question

Is it possible to use **DistNP**-complete problem to construct one-way function under assumption **DistNP** $\not\subset$ **FAvgBPP**?