one way functions.

Wednesday, 7 October 2020 3:58 PM

Non-invertability: ?

Adv - Randomised Poly. Algo: ?

neg. small quantity:

$\epsilon(n)$ is neg. small

if $\epsilon(n) < \frac{1}{P(n)}$ $\forall n \geq n_0$

for every P, $\exists n_0$,

$2^n > P(n)$, $\frac{1}{2^n} < \frac{1}{P(n)}$

$\frac{1}{10^6} \sim 0$

$n^{\log n}$

$\{0,1\}^*$,

$f : \{0,1\}^* \to \{0,1\}^*$.

$f : \{0,1\}^n \to \{0,1\}^n$.

$: \{0,1\}^n \to \{0,1\}^m$?

one-way.

" easy to compute
Diff. to invert "

$D(x) = f(x)$
Algo.
D is a poly. algo:

x, y → f(x)

given $f(x)$

find $y \in f^{-1}(f(x))$ is a set.

$f(A(f(x))) = f(x)$?

$A(f(x)) \in f^{-1}(f(x))$

$Pr(A(f(x)) \in f^{-1}(f(x)))$

neg. small

Def^n: $f : \{0,1\}^* \to \{0,1\}^*$ is

one way:

for any eff. A → $n_0, n \geq 0$

$Pr(x \leftarrow \{0,1\}^n;\ y \leftarrow f(x);$
$x' \leftarrow A(1^n, y) : f(x') = y)$

$\leq \epsilon(n)$

$A(x \to y)$.

No poly time A can invert y ?

$Pr(A(y) \to x'$

$f(x) = f(x')) \leq \epsilon(n)$.

$f(x) = |x|$ expressed in binary.

$f(0 \cdots 0)$ (1024)

$f(101 \cdots 1)$ (1024).

$= 10000000000$ — 11 bits

$\{0,1\}^* \to \{0,1\}^*$

$f(101101) = (1100)$

$f^{-1}(101)$

$11 \cdots 1$
$00 \cdots 0$ } 2
1024

$f^{-1}(b_1 b_2 \cdots b_k)$

$b_1 b_2 \cdots b_k = B$

output $i_1 i_2 \cdots i_B$

$100 \cdots 0$ → $|x|$
y — exp.

$A(y) \to |A(y)|$ poly in y

but any $|x|$ is exp in y

$f(x) \to y$ ✗

$|x| \to |y|$
expo. small

input size of x.

$A(1^n, y)$

$= 111 \cdots 1$ (1024)

✗ (poly)

$A(y)$
$A(100 \cdots 0) \to 111 \cdots 1$ (1024)
This is an exponential algo ? in input.

$A(1^{1024}, y) \to 11 \cdots 1$
$00 \cdots 0$

is poly in input

$f : \{0,1\}^n \to \{0,1\}^m$

m is a poly in n

$A(1^n, y)$ (struck out)

$A(y)$

$f : \{0,1\}^n \to \{0,1\}^m$

where n & m are poly. related.

$m \leq X(n)$, $n \leq Y(m)$

Poly.

f is a one way fun if.

f is easy to com
f(x) is easy to com

C that takes x, outputs
f(x) in time Poly in |x|.

$A(f(x))$ — $|x|$, $|f(x)|$ Poly. related,

poly in $f(x)$.

Poly in $|x|$

---

f : length preserving.
length regular.
$|f(x)|$, $|x|$ are poly. related:

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

$p, q. \to p \cdot q = n$

easy.

given $n \to p$ & q.
is hard.

---

page 32 - 42.

42 - 47. weak OWF
$\Rightarrow$ S OWF.