COM S 6830 – Cryptography Jan 20, 2009

Lecture 5: Levin's OWF and Multiplication

Instructor: Rafael Pass *Scribe: Shyam Lenna*

1 Definition and Theorem

Definition 1 *If $f \cdot \{0,1\}^* \to \{0,1\}^*$ is a One Way Function*

- f is PPT computable
- $\forall$nuPPT $A, \exists$neg. ε s.t. $\forall n \in N$, $\Pr[x \leftarrow \{0,1\}^n A(1^n, f(x)) \in f^{-1}(f(x))] \leq \varepsilon(n)$

We already know that a weak one way function can be used to get a strong one way function.
Aside: Existence of a OWF $\Rightarrow \mathsf{P} \neq \mathsf{NP}$

1.1 Levin's One Way Function

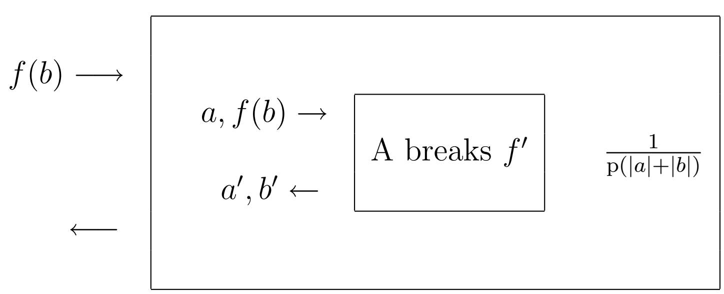
Theorem 1 *There $\exists$ (constructively) an explicit polytime computable function f that is One Way iff $\exists$ a OWF.*

CLAIM: If $\exists$ a OWF (Even if, say, n^{1000} steps), then $\exists$ a OWF that can be computed in time n^2. (We could even have one in linear time if desired, though it is unnecessary).

Proof. Assume f is a OWF that is computable in time n^c.
f$'(a,b) = a, f(b)$ Let $|a| = n^c, |b| = n$
note: the , here represents concatenation.
also note: $f(b)$ takes n^c steps, which is linear in terms of the input (a,b).
$f'(x)$ is computable in time $|x|^2$. So is f' OW?

Assume, for contradiction, $\exists$ someone who breaks f'. Show that he can also be used to break A'.

A': $a \leftarrow \{0,1\}^{n^c}$



A' succeeds with probability $\frac{1}{\mathrm{P}(|a|+|b|)} = \frac{1}{\mathrm{P}()n^2+n} = \frac{1}{\mathrm{P}(g(n))}$ where g is polynomial.
(This only works because a is polynomial, not exponential, in terms of n) While f' is more efficient, it is also a weaker OWF than f. ∎

1.2 Proof of Theorem 1

Proof.

$$f(M, x) = M, y$$

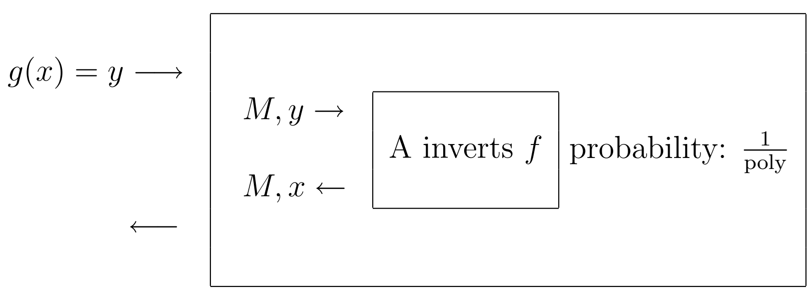
$$y = \begin{cases} M(x) & \text{if } M(x) \text{ takes } \leq |x|^2 \text{ steps.} \\ 0 & \text{otherwise} \end{cases}$$

$$|M| = \log(n), |x| = n - |M|$$

(can interpret M as code of program and x as the input)
Then run for $|x|^2$ steps.

CLAIM: If OW exists, then this is OW
Put the OWF as M - specifically one that can be computed in time n^2, which we know exists by the previous claim.
M is $\log(n)$ bits, so in probability $\frac{1}{\log(n)}$ we will pick this OWF: M.
Say, 10^5 bits $\leq \log(n)$ for sufficiently big n. This function can only become OW when n is very large, like 2^{10^5}.

To prove this, use contradiction/reduction.
Assume someone can do this in Pr. $\frac{2}{n}$, then someone can invert g as well. (g is a function computable in time n^2. The actual proof is in the lecture notes.



We still need to show that it works even though the input is biased. So it works, but we don't know how big n has to be. ∎

2 Primes

Theorem 2 *There exists a method to efficiently check if p is a prime number.*
(There is a simple one with probability $\frac{1}{2}$ that can be repeated.)

2.1 Chebyshev's Theorem

of primes between $1, N$ is at least $\left(\frac{N}{\log(N)}\right)$
Prime number theorem: # primes $\rightarrow \frac{N}{\log(N)}$
Pick $x \leftarrow \{0,1\}^2$
It will be prime with roughly probability $\frac{2^n}{\log(2^n)} = \frac{2^n}{n}$
So Prob[x prime] $\approx \frac{2^n}{\frac{n}{2^n}} = \frac{1}{n}$
In expectation, one needs n trials. This is a very fast way to find a random prime.

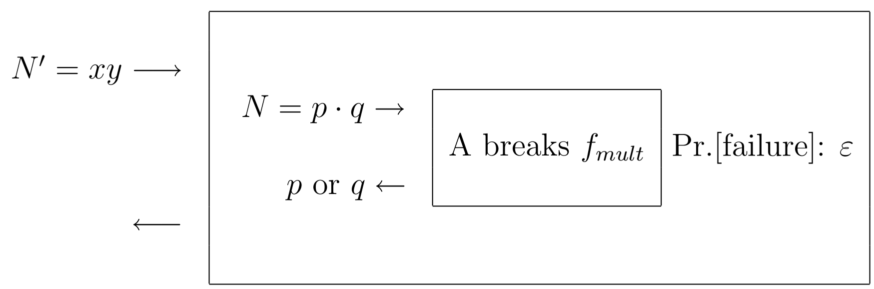
2.2 Multiplication

$$f_{mult}(x,y) = xy \qquad\qquad |x| = |y|$$

Factoring Assumption: $\forall$ nuPPT, $\exists$ neg. ε s.t. $\forall m \in n$:
Pr[$p, q \leftarrow$ random n-bit primes; $N = p \cdot q : A(N) \in \{P, Q\}] \leq \varepsilon(n)$
The best known algorithm is $2^{O(n^{1/3}(\log^{2/3}(n)))}$

Theorem 3 *If Factoring Assumption holds, then f_{mult} is a weak OWF.*

The way to prove this is a reduction, which can be seen in the lecture notes.
Also, can do a prime check at the $N = p \cdot q$ stage and only give the result to A if prime.



3 Collection of OWF

Definition 2 *A family of functions $F = \{f_i : D_i \rightarrow R_i\}_{i \in I}$ is a collection of OWF.*

1. *Easy to Sample function: $\exists$ PPT gen s.t. gen(1^n) outputs i$\in$I*
2. *Easy to Sample domain: $\exists$ PPT on input: sample uniform from D_i*
3. *Easy to evaluate: $\exists$ PPT $i, x \in D_i$; comp. $f_i(x)$*
4. *Hard to invert: $\forall$ nuPPT $A, \exists$ neg. ε s.t. $\forall n \in N$ $Pr[i \in gen(1^n); x \leftarrow D_i : A(1^n, i, f_i(x)) \in f_i^{-1}(f_i(x)))] \leq \varepsilon(n)$*

note: (n is not input length here).
also note: The $A(1^n, i, f_i(x))$ part should be hard to do.
A collection of OWF existing $\Leftrightarrow$ OWF exists.