Cryptography Notes - September 13

David Goff
dhg57

September 2011

1 Collection of OWF

A Collection of OWF is a family of functions

$$F = \{f_i : \mathscr{D}_i \to \mathscr{R}_i\}_{i \in I}$$

if

- $$\exists PPT\, Gen(1^n) \to i \in I$$
- $$\exists PPT\, Sample \to \mathscr{D}_i, given i$$
- $$\exists PPT\, Compute \to f_i(x), given i, x$$
- $$\forall \text{ nuPPT A } \exists \text{ neg } \varepsilon \text{ st } \Pr[i \leftarrow Gen(1^n), x \leftarrow \mathscr{D}_i : A(1^n, i, f_i(x)) \in f_i^{-1}(f_i(x))] \leq \varepsilon(n)$$

2

$$F_{mult}$$

f_{mult} family:

$$let I = N, \mathscr{D} = \{p,q\} st |p| = |q| = i, and q prime$$

$$f_i p, q = pq$$

$$Gen(1^n) \to n$$

3 Fact

Fact:

$\exists$ a collection of OWF iff $\exists$ OWF

(IF):

$$Gen(1^n) = n$$
$$\mathscr{D}_i = \{0,1\}^i$$
$$f_i(x) = f(x)$$

(only if):

$$f(r_1, r_2) = f_i(x), \text{ where,}$$
$$Gen_{r_1}(1^n) \to i$$
$$Sample_{r_2}(i) \to x$$

4 EXP

$$Gen(1^n) \to p, g \text{ where}$$
p is a random n-bit prime

g is a generator for Z_p^*

$$I = \{p, g : \text{ p is prime, g is a generator for } Z_p^*\}$$
$$f_{p,g}(x) = g^x \bmod p$$
$$\mathscr{D}_{p,g} = Z_p^*$$

Discrete log assumption:

$\{f_{p,q}\}_{\{p,q\} \in I}$ is a collection of OWF

g^x can be calculated quickly by repeated squaring

5 RSA collection

$$I = \{N = (pq), \text{ p and q are prime, } |p| = |q|\}$$
$$Gen(1^n) \to \text{(N, e), where}$$
$$N = pq, \text{ p and q are random n-bit primes}$$
e is a random element in $Z_{\varphi(N)}^*$

$$f_{N,e}(x) = x^e \bmod N$$

RSA assumption: this is a collection of OWFs

6 Hard-core bits

a predicate b : $\{0,1\}^* \rightarrow 0,1^*$ is a hard-core bit for $f()$ if

b is PPT computable, and

$\forall$ nuPPT A $\exists$ neg ε st $\forall n \in N, Pr[x \leftarrow \{0,1\}^n : A(1^n, f(x)) = b(x)] < \frac{1}{2} + \varepsilon(n)$

In other words, it is easy to calculate b(x) from x, but hard to calculate b(x) from f(x).

7 Examples of hard-core bits

let

$$hal f_m(x) = 0 \text{ if } 0 \leq x \leq \frac{m}{2},\ 1 \text{ otherwize}$$

For RSA,

$hal f_m(x)$ is hard-core for $f_{N,e}$

For EXP,

$hal f_{p-1}(x)$ is hard-core for $f_{p,q}$

8 To prove something is hard-core

Prove that, given some A that guesses

$$b(x)$$

with probability greather than

$$\frac{1}{2} + \frac{1}{poly},\ \text{given } f(x),$$

It is possible to write a B that recovers x given f(x)