CS6846 – Quantum Algorithms and Cryptography

Building Cryptography

Instructor: Shweta Agrawal, IIT Madras
Email: shweta@cse.iitm.ac.in

Hardness Assumptions

We will study the following number theoretic assumptions:

1. Factoring
2. RSA
3. Discrete Log
4. Computational and Decisional Diffie Hellman

Cryptographic Constructions

From these we will construct:

1. One way functions
2. One way permutations
3. Trapdoor permutations
4. Key Exchange and Symmetric Key encryption
5. Public Key Encryption

Katz-Lindell

Factoring:

Let genModulus be a polytime algo which on input 1^n outputs (N, p, q) where $N = pq$, p & q are n bit primes (except with probability negligible in n).

Consider the Factoring experiment; $FACTOR_{A, \text{genModulus}}$

Adversary PPT Algorithm

1. Run genModulus(1^n) to get (N, p, q)
2. A is given N, & outputs $p', q' > 1$.
3. Define output to be 1 if $N = \underline{p'q'}$ else 0.

Definition: Factoring is hard relative to GenModulus if $\forall$ PPT algorithms $\mathcal{A}$, $\exists$ negligible function negl s.t.

$$\Pr\left[\text{Factor}_{\mathcal{A},\text{GenModulus}}(1^n) = 1\right] \leq \text{negl}(n).$$

The factoring assumption is the assumption that $\exists$ GenModulus relative to which factoring is hard.

Eg One way function.

$$f(x, y) = x \cdot y.$$

RSA Assumption:

genRSA : PPT, on i/p 1^n, outputs modulus $\underline{N} = pq$, as well as 2 integers $\underline{e}$, $\underline{d}$ s.t.

$\gcd(e, \phi(N)) = 1$ & $ed \equiv 1 \bmod \varphi(N)$.

↳ Euler's Totient function.
numbers < N which are relatively prime to N.

By Extended Euclid, $\exists$ d, f s.t.

$$de + \cancel{f\,\varphi(N)} = 1$$

$\therefore$ Taking mod $\varphi(N)$

$$e \cdot d \equiv 1 \bmod \varphi(N).$$

RSA experiment $RSA_{A, GenRSA}(1^n)$:

1. Run $GenRSA(1^n)$ to get (N, e, d).
2. Choose uniform $y \in \mathbb{Z}_N^*$
3. $A(N, e, y)$ & outputs $x \in \mathbb{Z}_N^*$
4. Output is 1 if $x^e \equiv y \bmod N$.

RSA is hard relative to GenRSA if $\forall$ PPT A,

$$\Pr\left[RSA_{A, GenRSA}(1^n) \to 1\right] \leq \text{negligible}$$

RSA Assumption is $\exists$ GenRSA for which RSA exp. is hard

$N, e, y, d.$ $\quad y^d = (x^e)^d = x^{ed} = x \bmod N.$

If I know p, q, is it hard to compute d.

$$\varphi(N) = (p-1)(q-1).$$

Given e, s.t. $\gcd(e, \varphi(N)) = 1$

Run Extended Euclid's algo to get

d, f s.t.

$$ed + f\varphi(N) = 1$$

$$\Rightarrow ed \equiv 1 \bmod \varphi(N).$$

RSA $\Rightarrow$ Trapdoor Permutations.

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

$$\mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$$

Discrete log:

Let $\mathcal{G}$ be a group generation algorithm which takes as input 1^n, outputs a description of a cyclic group G of order q, s.t $\|q\| = n$, & a generator $g \in G$.

Given $g, y \in G$. $\exists$ x s.t $\underline{\underline{g}}^{x} = y$

x is called the discrete logarithm of y w.r.t g.

Discrete log Exp:

- Run $\mathcal{G}(1^n) \to (G, q, g)$ order, generator
- Choose uniform $y \in G$.
- $\mathcal{A}$ is given G, g, q, y & outputs $x \in \mathbb{Z}_q$.
- o/p 1 if $g^x = y$, else o/p 0.

DL hard if $\forall$ PPT $\mathcal{A}$, $\Pr\left(\text{Dlog}_{\mathcal{A},G}(1^n) = 1\right) \leq \text{negl}(n)$.

DL assumption is that $\exists\ \mathcal{G}$ for which DL problem is hard.

$f(x) = g^x$

$f: G \to G$.

gives a one way permutation.

Diffie - Hellman Problems:

Computational

CDH

Decisional

DDH.

Define $\boxed{DH_g(h_1, h_2) = g^{\log h_1 \cdot \log h_2}}$.

If $h_1 = g^{x_1}$, $h_2 = g^{x_2}$ then

$$DH_g(h_1, h_2) = g^{x_1 x_2} = h_1^{x_2} = h_2^{x_1}.$$

- CDH Problem is compute $DH_g(h_1, h_2)$ for uniform h_1 & h_2.

- DDH is to distinguish $DH_g(h_1, h_2)$ from uniform.

Key Exchange

A		B
$x_1 \leftarrow \mathbb{Z}_q^*$		$x_2 \leftarrow \mathbb{Z}_q^*$.
	$\xrightarrow{\quad g^{x_1} \quad}$	
	$\xleftarrow{\quad g^{x_2} \quad}$	

$$\underbrace{(g^{x_2})^{x_1} \qquad\qquad (g^{x_1})^{x_2}}_{g^{x_1 x_2} \;\cong\; \text{uniform.}}$$