Quiz Review
04/13/18
Akshay Degwekar

Agenda

- Def^{n}s: Public key Enc, Digital Signatures
- Discrete Log ~~based~~
  - Assumptions: DLog, CDH, DDH.
  - DH Key Exchange, El-gamal
  - El gamal Signatures.
  - Pederson Commitments

- Factoring & RSA.
  - Vanilla RSA & OAEP.
  - Signatures

- Gap Groups & Bilinear Maps
  - 3 party KE
  - Short signatures.

Def^n: Public Key Encryption

Syntax: Gen, Enc & Dec Algorithms.

$(pk, sk) \leftarrow \text{Gen}$.

$ct \leftarrow \text{Enc}(pk, m)$.

$\text{Dec}(sk, ct)$: returns m.

CPA
(Chosen Plaintext)

$$\begin{array}{ccc} Ch & \xrightarrow{\quad pk \quad} & A \\ & & \\ ct_b = \text{Enc}(m_b),\ b \leftarrow \{0,1\} & \xleftarrow{\ m_0, m_1\ } & \\ & \xrightarrow{\ ct_b\ } & \\ & \xleftarrow{\ b'\ } & \end{array}$$

win if $b = b'$

CCA
(Chosen Cipher text)

$$\begin{array}{ccc} Ch & \xrightarrow{\quad pk \quad} & A \\ & \xleftarrow{\ ct_i\ } & \\ & \xrightarrow{\ m_i\ } & \\ b \leftarrow \{0,1\} & \xleftarrow{\ m_0, m_1\ } & \\ ct_b = \text{Enc}_{pk}(b) & \xrightarrow{\ ct_b\ } & \\ & \xleftarrow{\ ct\ } & \\ & \xrightarrow{\ m\ } & \\ & \xleftarrow{\ b'\ } & \end{array}$$

wins if $b = b'$.

$$\Pr[A \text{ wins}] \leq \frac{1}{2} + \text{negl}(\lambda)$$

- **Note**: Don't need Enc_{pk} oracle as A can generate those by himself.

Def^n : Digital Signatures :

Syntax : Gen : o/p sk, vk (signing & verif)

Sign(sk, m) o/p signature σ.

Verify(vk, m, σ) : True or false.

Security : ~~Ada~~ Unforgeability under adaptive chosen message attacks

$$\begin{array}{ccc} Ch & \xrightarrow{\quad vk \quad} & A \\ & \xleftarrow{\quad m \quad} & \\ & \xrightarrow{\quad \sigma = Sign(sk, m) \quad} & \\ & \xleftarrow{\quad m^*, \sigma^* \quad} & \end{array}$$

Adv wins if m^* was not queried & Verify(m^*, σ^*, vk) = true.

Discrete Log.

Let g generate G st $|G| = q$ (prime order)

i) Discrete Log : given g^x, find x.

($x \leftarrow \{0, 1 \dots q-1\}$.

ii) Computational Diffie-Hellman (CDH)

Given g, g^a, g^b find g^{ab}.

iii) Decisional Diffie Hellman. (DDH).

Distinguish $\{g, g^a, g^b, g^{ab}\} \approx \{g, g^a, g^b, g^c\}$

Discrete log : hardest to DDH : easiest.

Pederson Commitments.

A, B pick gen g, h at random.

A $\xleftarrow{\quad h \quad}$ B

$\xrightarrow{\quad h^r \cdot g^m \quad}$

$\xrightarrow{\quad \text{Reveal } r, m \quad}$

- Perfectly hiding (Alice's message dist is same no matter which message.)

- Computationally ~~bidu~~ binding if DLog is hard.

[Two ~~comm~~ Reveals (m, r) & (m', r') find dlog ~~of~~ h. wrt g.]

Diffie Hellman & ElGamal

$$\begin{array}{ccc} A & \xrightarrow{g^x} & B \\ x & & y \\ & \xleftarrow{g^y} & \end{array}$$

o/p $(g^y)^x$ $\qquad$ $(g^x)^y$

pk : (g, g^x). $\quad$ sk : x

Enc (pk, m) : $(g^y, (g^x)^y \cdot g^m)$

- CPA secure not CCA.

Both secure under DDH assumption

El gamal Signatures

(Reminder. g gen ~~sub~~ G of ord q contained in $\mathbb{Z}_p^*$.)

KeyGen : $sk = x$ (in $\{0, \ldots, q-1\}$)
$pk = y = g^x$.

Sign (sk, m) : Pick $k \leftarrow \mathbb{Z}_q^*$

$$\sigma = (r, s) = \left(g^k \bmod p, \ \frac{h(m) + rx}{k} \bmod q \right)$$

Verify : check if $y^{r/s} \cdot g^{h(m)/s} = r$.

Factoring & RSA

$N = p \times q$.

'Vanilla RSA' : $\underline{pk}: (N, e)$

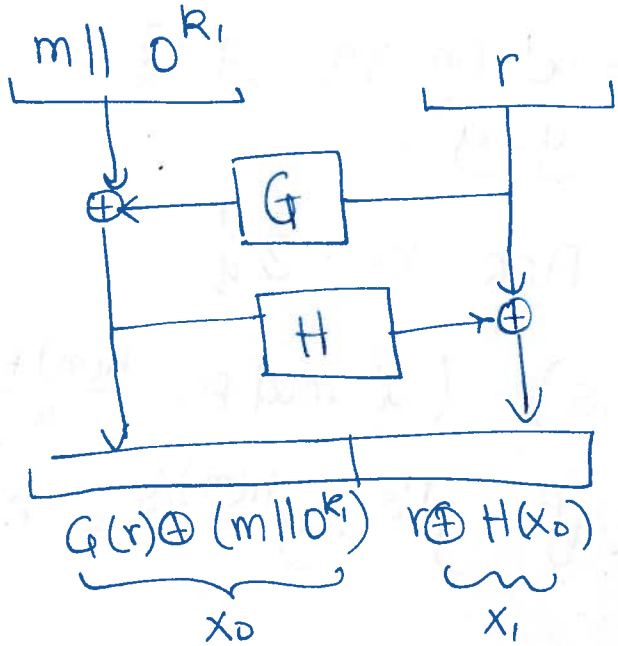
$\underline{sk}$: d st $ed \equiv 1 \pmod{\phi(N)}$.

$Enc(pk, m) = o/p \quad m^e \pmod N$

$Dec(sk, ct) = (ct)^d = (m^e)^d = m \pmod N$

- Deterministic, $f(x) = x^e$: Trapdoor function.

OAEP. (Optimal Asymmetric Enc. Padding)



& CCA-2 secure in Random Oracle Model.

GMR Signatures

~~Sign(~~ pk: (n, e)
sk: (n, d) st $de \equiv 1 \pmod{\phi(n)}$.

$\text{Sign}((sk, h), m) = h(m)^d$

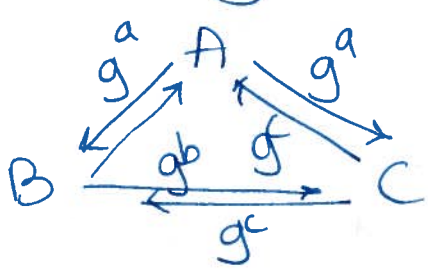
$\text{Verify}(pk, h, m, \sigma) = 1$ iff $\sigma^e \equiv h(m) \pmod{n}$

"Hash & Sign" paradigm.

Gap Groups & Bilinear maps.

- Groups where CDH is true, DDH not.
- $e: G_1 \times G_1 \to G_2$ such that.
  - i) $e(g^a, g^b) = e(g,g)^{ab}$.
  - ii) $e(g,g)$ generates G_2 (den. by h).

- 3 Party KE



All compute:
$e(g,g)^{abc}$.

eg: A: $(e(g^b, g^c))^a$

Secure under Bilinear Decisional DH.

$$(g, g^a, g^b, g^c, e(g,g)^{abc}) \approx (g, g^a, g^b, g^c, h^d)$$

Short Signatures (BLS).

$H: \{0,1\}^* \to G_1 \quad e: G_1 \times G_1 \to G_2$.

$sk: x \quad pk: g^x$ (in G_1)

$\text{Sign}(m) = \sigma = H(m)^x$. (in G_1).

$\text{Verify}(pk, m, \sigma) = \text{Check}$.

$$e(g, \sigma) \stackrel{?}{=} e(g^x, H(m)).$$

Identity based Encryp. (Boneh Franklin 01)

$mpk = y = g^s \quad msk \stackrel{\$}{=} s$ (master sk, held by Trusted P).

$\text{Enc}(mpk: y, \text{name}, m)$:

$r \leftarrow \mathbb{Z}_q$,

$(g^r, m \oplus H_2(g_A^r))$

where $g_A = e(H_1(\text{name}), y)$

$\text{Decrypt}(u, v)$:

$SK_{Alice} = H(Alice)^s$

$$m = v \oplus H_2[e(H_1(\text{name}), g^r)]$$

$$= v \oplus H_2(e(H_1(\text{name}), y)^r]$$