TOPIC: 6.857

DATE: 3/19/18

FILE UNDER:

PAGE: L12.1

Admin:

Pset #3 due 3/27.
Proj. proposals due 3/24.

Today:

Pedersen commitments

PK encryption

El Gamal PK encryption

Semantic security

DDH (Decision Diffie-Hellman)

DDH ⇒ El Gamal is semantically secure

Readings:

Paar: Ch. 6, 7, 8

Katz: 10, 11

Ammasson: Ch. 11

TOPIC:

DATE:

FILE UNDER:

Group theory facts: (review)

Let G be a cyclic group with generator g.

Let $m = |G|$ (order of G)

Then:

1. $G = \{g^0, g^1, \ldots, g^{m-1}\}$

2. To pick a random element of G:

   Let $x \overset{R}{\in} \mathbb{Z}_m = \{0, 1, \ldots, m-1\}$

   return $y = g^x$

3. If $y \overset{R}{\in} G$ & $z \overset{R}{\in} G$, then yz uniformly random in G.

4. Suppose $d \mid m$

   Then set of dth powers

   $$\{g^0, g^d, g^{2d}, \ldots, g^{m-d}\}$$

   is a subgroup of order m/d

   Ex: quadratic residues in $\mathbb{Z}_p^*$ has order $\frac{p-1}{2}$.

   Subgroup is cyclic with generator g^d.

Pedersen Commitment Scheme

Recall: Commit(x) → "commitment to x"

Reveal(c) → "opens commitment, reveals x"

Properties: **Hiding**: Commit(x) reveals nothing about x

Binding: Can only open in one way (can't change x)

Nonmalleability (?): Can't produce commitment to e.g. x+1 from commitment to x.

values can be chosen by receiver

Setup: p, q large primes s.t. $q \mid p-1$ (e.g. p "safe prime")

g generator of order-q subgroup of $\mathbb{Z}_p^*$

(e.g. if p safe then $\langle g \rangle = Q_p$ = squares mod p)

$a \neq 0 \bmod q$

$h = g^a$ a secret h generates $\langle g \rangle$ as well

Commit(x): $x \in \mathbb{Z}_q$ (i.e. $0 \le x < q$)

Sender chooses random $r \in \mathbb{Z}_q$

$\text{Commit}(x) = c = g^x h^r \bmod p$

Reveal: Sender reveals x and r

Receiver verifies that $c = g^x h^r \pmod p$

Pedersen commitment (cont.)

"Perfectly Hiding"
(Adversary could have ∞ computational power...)

Hiding: Given $c = g^x h^r$

Can in principle be opened to any $x' \in \mathbb{Z}_q$, for some r'

$$\left.\begin{aligned} g^x h^r &= g^{x'} h^{r'} \\ g^x g^{ar} &= g^{x'} g^{ar'} \\ g^{x+ar} &= g^{x'+ar'} \end{aligned}\right\} \pmod p$$

$$x + ar = x' + ar' \pmod q$$

$$r' = (x - x')/a + r$$

$\uparrow$ q is prime so a^{-1} exists
$r' \neq r$ since $x \neq x'$

"Computationally Binding"
(Sender can't compute a)

Binding: If sender can reveal two ways

$$c = g^x h^r = g^{x'} h^{r'} \pmod p$$

$$x + ar = x' + ar' \pmod q$$

$$a = (x - x')/(r' - r)$$

$\uparrow$ $r' \neq r$ & q is prime

$$= \text{discrete log of } h, \text{ base } g, \text{ mod } p \quad \blacksquare$$

Non-malleable: Nope.

If $c = \text{Commit}(x) = g^x h^r$

then $c' = \text{Commit}(x+1) = g \cdot (g^x h^r) = g^{x+1} h^r$

(Some applications don't need non-malleability)

Public-key encryption:

Let λ = "security parameter" (i.e. "key size")

Then $1^\lambda = \underbrace{11\cdots1}_{\lambda}$ λ 1's in a row. Length $= \lambda$

Need three algorithms:

① $\text{Keygen}(1^\lambda) \longrightarrow (PK, SK)$

② $E(PK, m) \longrightarrow c$

Encryption takes $m \in$ message space M

to $c \in$ ciphertext space C

(with given public key PK)

Encryption may be <u>randomized</u>.

③ $D(SK, c) \rightarrow m$

Decryption is <u>deterministic</u>

s.t. (<u>Correctness condition</u>)

$$(\forall (PK, SK))(\forall m)\ D(SK, E(PK, m)) = m$$

El-Gamal PK encryption (Taher El Gamal, 1984)

Let $G = \langle g \rangle$ be a cyclic group with generator g.

(Keygen may output description of g & G, given λ.)

Keygen:

Pick x at random from $[0 \ldots |G|-1]$

Let $SK = x$.

Let $PK = g^x$

Output (PK, SK) (& description of G, if needed)

Encryption: (of message m)

randomized!

Pick k at random from $[0 \ldots |G|-1]$

Assume message m represented as element of G.

Let $y = g^x$ be PK of reciprent

Output $c = (g^k, m \cdot y^k)$ as ciphertext

Decryption:

Let $c = (a, b)$ be received ciphertext

Let $m = b / a^x$. Output m.

[Correctness follows since $a^x = g^{kx} = g^{xk} = y^k$.]

E) Gamal encryption related to DH key exchange:

Alice $\xrightarrow{y = g^x \text{ (via PKI?)}}$ Bob

Alice $\xleftarrow{a = g^k}$ Bob

DH key $= (g^k)^x$
$= g^{kx}$

DH key
$= (g^x)^k = g^{kx}$

$=$

Alice $\xleftarrow{b = m \cdot (\text{DH key})}$ Bob

Encrypt by multiplying by DH key.

Decrypt by dividing by DH key.

How to define security for PK encryption?

We'll see two definitions:

① "semantic security" (Goldwasser & Micali)

② "adaptive chosen ciphertext attack" (ACCA) secure

(≈ to IND-CCA we saw for symmetric encryption)

"Game" definition of semantic security:

Phase I ("Find"):

- Examiner generates (PK, SK) using Keygen(1^λ)
- Examiner sends PK to Adversary
- Adversary computes for polynomial (in λ) time, then outputs two messages m_0, m_1 of same length, and "state information" s. [$m_0 \neq m_1$ required]

Phase II ("Guess"):

- Examiner picks $b \xleftarrow{R} \{0,1\}$, computes $c_* = E(PK, m_b)$
- Examiner sends c_*, s to Adversary
- Adversary computes for polynomial (in λ) time, then outputs $\hat{b}$ (his "guess" for b).

Adversary "wins" game if $\hat{b} = b$.

Def: A PK encryption scheme is <u>semantically secure</u> if $\text{Prob}[\text{Adv wins}] \leq \frac{1}{2} + \text{negligible}$

Fact: In order for a PK encryption scheme to be semantically secure, it must necessarily be <u>randomized</u>.* (Randomized encryption is necessary but not sufficient for semantic security.)

for stateless enc

Is El Gamal PK encryption semantically secure?

* More precisely: it can't be stateless & deterministic. It may be randomized, or stateful, or both.

DDH (Decision Diffie-Hellman Assumption):

Given a group G with generator g:

It is hard/infeasible to decide whether a given triple of elements was generated as

$$(g^a, g^b, g^c) \qquad [a, b, c \text{ random}]$$

or as

$$(g^a, g^b, g^{ab}) \qquad [a, b \text{ random}]$$

Recall:
CDH ≡
Computing g^{ab} from g^a & g^b is hard

That is, if DDH holds in a group, you can't even <u>recognize</u> the DH key g^{ab} when it is given to you! (You can't distinguish it from a random element.)

Theorem: DDH ⇒ CDH

Proof: If ¬CDH, then ¬DDH (contrapositive).

If you can compute g^{ab} from g^a and g^b (i.e. ¬CDH) then you can decide if given third element <u>is</u> g^{ab} (i.e. ¬DDH). ∎

Theorem (Tsiounis & Yung):

El Gamal is semantically secure in G

$\Longleftrightarrow$

DDH holds in G

- Semantic security may not be enough for some applications.
- El Gamal is <u>malleable</u>:

  Given $E(m) = (g^k, m \cdot y^k)$

  it is easy to produce $E(2m) = (g^k, (2 \cdot m) \cdot y^k)$

  without knowing m!
- More generally, El Gamal is <u>homomorphic</u>:

$$\begin{array}{lll} \text{Given} & c_1 \in E(m_1) & = (g^r, m_1 \cdot y^r) \\ \text{\& given} & c_2 \in E(m_2) & = (g^s, m_2 \cdot y^s) \\ \hline \text{can produce} & c_1 \cdot c_2 & = (g^{r+s}, (m_1 \cdot m_2) \cdot y^{r+s}) \\ & & \in E(m_1 \cdot m_2) \end{array}$$

- Product of ciphertexts yields an encryption of <u>product of plaintexts</u>.
- Special case: multiplying by $E(1) = (g^s, y^s)$ <u>re-randomizes</u> encryption.

- What is stronger notion of security for PK encryption? (e.g. one that excludes malleability...)

- "IND-CCA2 secure" (ACCA secure = secure under adaptive chosen ciphertext attack)
  ≈ IND-CCA secure defn we saw for symmetric enc.

- Similar to semantic security defn, except that Adv allowed access to decryption oracle, too.
  (He has PK so access to encryption oracle already there.)
  (As before, may not use oracle to decrypt challenge ciphertext during "guess" phase.)