TOPIC: 6.857

DATE: 3/20/17

FILE UNDER:

PAGE: L12.1

Admin:

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

Today:

(Finish elliptic curves – Yael)

Pedersen commitments

PK encryption

EL Gamal PK enc.

Semantic security

DDH (Decision Diffie-Hellman)

IND-CCA2 } if time

Cramer-Shoup

Readings:

Paar: Chapters 6, 7, 8

Katz: Chapters 10, 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 d^{th} 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)

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

$a \not\equiv 0 \bmod q$

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 $x' \in Z_q$, for some r'

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

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

$$r' = (x-x')/\underline{a} + r$$

↑ 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

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

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

$$a = (x-x')/\underline{(r'-r)}$$

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

(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 = λ

Need three algorithms:

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

2. $E(PK, m) \longrightarrow c$

   Encryption takes $m \in$ message space $\mathcal{M}$

   to $c \in$ ciphertext space $\mathcal{C}$

   (with given public key PK)

   Encryption may be randomized.

3. $D(SK, c) \rightarrow m$

   Decryption is deterministic

   s.t. (Correctness condition)

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

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 recipient

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 $a^x = g^{kx} = g^{xk} = y^k$.]

El Gamal encryption related to DH key exchange:

Alice $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ Bob

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

$$\xleftarrow{\quad a = g^k \quad}$$

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

$=$

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

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
   ($\approx$ 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 $\hat{b} = b$.

TOPIC

DATE

FILE UNDER

Def: A PK encryption scheme is semantically secure

if Prob[Adv wins] $\leq \frac{1}{2}$ + negligible

Fact: In order for a PK encryption scheme to be semantically secure, it must necessarily be randomized.* (Randomized encryption is

for stateless enc → necessary but not sufficient for semantic security.)

Is El Gamal PK encryption semantically secure?

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