TOPIC: 6.857 - Computer & Network Security

DATE: 3/19/14

FILE UNDER:

PAGE: L13.1

Admin:

Project proposals due Friday!
(come to office hours if you need a team or help)

Gethys talk today 32G-882 "Insecurity in Home Embedded Devices"
4pm

Project idea:

See Gethys' talk

Today:

Pedersen Commitment

PK encryption

El Gamal PK encryption

Semantic security

↓

DDH (Decision Diffie-Hellman)

if time

IND-CCA2

Cramer-Shoup PK encryption

Readings:

Paar & Pelzl, Chapters 6, 7, 8

Katz & Lindell, Chapter 10

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

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.)

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

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

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

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

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

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

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

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

Binding: If sender can reveal two ways

$$c = g^x h^r = g^{x'} h^{r'}$$

$$x + ar = x' + ar'$$

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

$r' \neq r$ & q is prime

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

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 M

to $c \in$ ciphertext space 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:

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

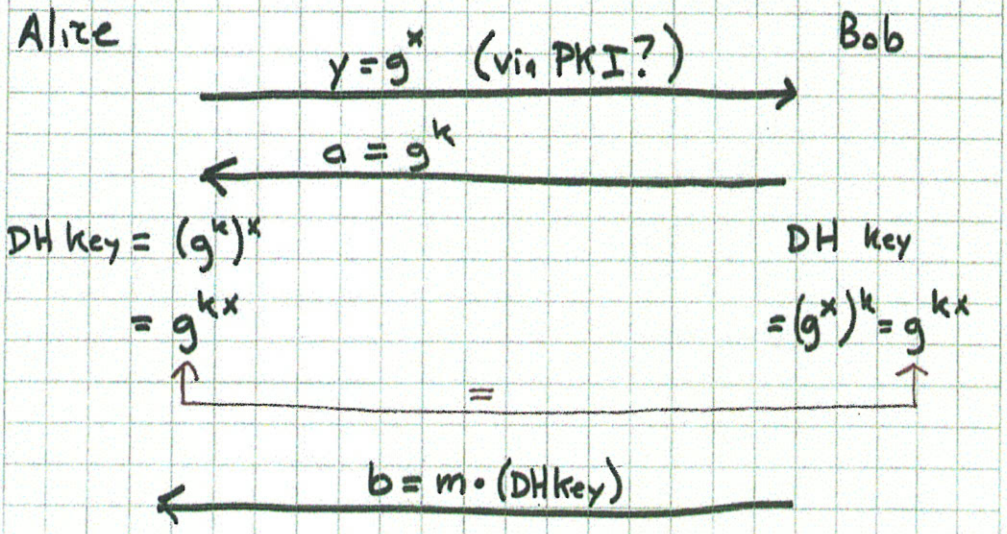
Decryption:

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

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

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

E) Gamal encryption related to DH key exchange:



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 $Keygen(1^\lambda)$
- 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 semantically secure 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 randomized.* (Randomized encryption is necessary but not sufficient for semantic security.)

for stateless encryption →

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

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

or as

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

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.)

<u>Theorem:</u> DDH ⇒ CDH

<u>Proof:</u> 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

$\iff$

DDH holds in G

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

  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 homomorphic:

  Given $c_1 \in E(m_1) = (g^r, m_1 \cdot y^r)$

  & given $c_2 \in E(m_2) = (g^s, m_2 \cdot y^s)$

  can produce $c_1 \cdot c_2 = (g^{r+s}, (m_1 \cdot m_2) \cdot y^{r+s})$

  $\in E(m_1 \cdot m_2)$
- Product of ciphertexts yields an encryption of product of plaintexts.
- Special case: multiplying by $E(1) = (g^s, y^s)$ re-randomizes 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.)

IND-CCA2 (ACCA) security game:

Phase I ("Find"):

- Examiner generates (PK, SK) using $Keygen(1^\lambda)$
- Examiner sends PK to Adversary
- Adversary computes for polynomial (in λ) time,

new ⇒ having access to a decryption oracle $D(SK, \cdot)$

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,

new ⇒ having access to a decryption oracle $D(SK, \cdot)$ except on input c_*

then outputs $\hat{b}$ (his "guess" for b).

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

Def: PK encryption method is IND-CCA2 secure (ACCA-secure) if

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

How to make El Gamal IND-CCA2 secure?

- Cramer–Shoup method is such an extension of El Gamal.
- Let G_q be a group of prime order q
  (e.g. $G_q = Q_p$, where $p = 2q+1$, p & q prime).
- **Keygen:**

$$g_1, g_2 \xleftarrow{R} G_q$$

$$x_1, x_2, y_1, y_2, z \xleftarrow{R} Z_q$$

$$c = g_1^{x_1} g_2^{x_2}$$

$$d = g_1^{y_1} g_2^{y_2}$$

$$\boxed{h = g_1^{z}}$$

EG

$$PK = (g_1, g_2, c, d, h)$$

H = hash fn mapping G_q^3 to Z_q

$$SK = (x_1, x_2, y_1, y_2, z)$$

- **Enc(m) [where $m \in G_q$]:**

  $r \xleftarrow{R} Z_q$ EG

  $u_1 = g_1^r$ EG

  $u_2 = g_2^r$

  $e = h^r \cdot m$ EG

  $\alpha = H(u_1, u_2, e)$

  $v = c^r d^{r\alpha}$

  ciphertext $= (u_1, u_2, e, v)$ EG

- **Decrypt (u_1, u_2, e, v):**

  $\alpha = H(u_1, u_2, e)$

  Check: $u_1^{x_1 + y_1 \alpha} u_2^{x_2 + y_2 \alpha} \stackrel{?}{=} v$

  If not equal, reject

  else output $m = e / u_1^z$ EG

Note: $u_1^{x_1} u_2^{x_2} = g_1^{r x_1} g_2^{r x_2} = c^r$

$u_1^{y_1} u_2^{y_2} = d^r$

$u_1^z = g_1^{rz} = h^r$ EG

Theorem: Cramer-Shoup is IND-CCA2 secure (i.e. secure against adaptive chosen ciphertexts) if

① DDH holds in G_q

② H satisfies a certain condition

(≈ "target collision resistance")

Thus, our strongest notion of security for PK encryption is in fact achievable, albeit at some cost in terms of speed & complexity.