Admin:

Today:


(Finish elliptic curves - Yael)

Pedersen commitments

PK encryption

EL Gamal PK enc.

Semantic security

DDH (Decision Diffie-Hellman)

IND-CCA2

Cramer-Shoup

if time

Readings:

Paar: Chapters 6, 7, 8

Katz: Chapters 10, 11
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 $x \in \mathbb{Z}_m = \{0, 1, \ldots, m-1\}$
   return $y = g^x$

3. If $y \in G$ & $z \in G$, 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: \( \text{Commit}(x) \rightarrow \text{"commitment to } x\)"

\( \text{Reveal}(c) \rightarrow \text{"opens commitment, reveals } x\)"

Properties:

- **Hiding:** Commitment 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 \( x \).

**Setup:**

\[ p, q \text{ large primes s.t. } q \mid p-1 \text{ (e.g., } p \text{ 'safe prime')} \]

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

\( e.g., \text{if } p \text{ safe then } \langle g \rangle = \mathbb{Z}_p^* \)

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

\( a \neq 0 \mod q \)

\( x \in \mathbb{Z}_q \) (i.e., \( 0 \leq x < q \))

Sender chooses random \( r \in \mathbb{Z}_q \)

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

**Reveal:**

Sender reveals \( x \) and \( r \)

Receiver verifies that \( c = g^x h^r \mod p \)
Pedersen commitment (cont.)

Hiding: Given \( c = g^x h^r \)

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

\[
\begin{align*}
  g^x h^r &= g^{x'} h^{r'} \\
  g^x g^{ar} &= g^{x'} g^{ar'} \\
  g^{x+ar} &= g^{x'+ar'} \\
  x + ar &= x' + ar' & (\text{mod } q) \\
  r' &= (x - x')/a + r \\
  &\text{if } q \text{ is prime so } a^{-1} \text{ exists and } r' \neq r \text{ since } x \neq x'
\end{align*}
\]

Binding: If sender can reveal two ways

\[
\begin{align*}
  c = g^x h^r &= g^{x'} h^{r'} & (\text{mod } p) \\
  x + ar &= x' + ar' & (\text{mod } q) \\
  a = (x - x')/(r - r) \\
  &\text{if } r \neq r' \text{ and } q \text{ is prime} \\
  &= \text{discrete log of } h, \text{ base } g, \text{ mod } p
\end{align*}
\]

Non-malleable: No.

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

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

(Some applications don't need non-malleability)
Public-key encryption:

Let $\lambda$ = "security parameter" (i.e. "key size")

Then $1^\lambda = 11 \ldots 1$ $\lambda$ 1's in a row. Length = $\lambda$

Need three algorithms:

1. **Keygen ($1^\lambda$) $\rightarrow$ (PK, SK)**

2. **E (PK, m) $\rightarrow$ 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 $\lambda$.)

Keygen:
Pick $x$ at random from $[0...|G| - 1]$

Let $SK = x$.
Let $PK = g^x$
Output $(PK, SK)$ (a description of $G$, if needed)

Encryption: (of message $m$)
Pick $k$ at random from $[0...|G| - 1]$
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 $a^x = g^{kx} = g^{xk} = y^k$.]
How to define security for PK encryption?

We'll see two definitions:

1. "semantic security" (Goldwasser & Micali)

2. "adaptive chosen ciphertext attack" (ACCA) secure
   (as 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, of same length,
  and "state information" s. [m_0 ≠ m, required]

Phase II ("Guess"):  
- Examiner picks b^R ← {0, 1}, computes c^R = E(PK, m_b)
- Examiner sends c, s to Adversary
- Adversary computes for polynomial (in λ) time,
  then outputs b̂ (his "guess" for b).

Adversary "wins" game if b̂ ≠ b.
**Def:** A PK encryption scheme is **semantically secure** if $\text{Prob}[\text{Adv wins}] \leq \frac{1}{3} + \text{negligible}$.

**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.)*

Is El Gamal PK encryption semantically secure?

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