Admin:

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

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

Project idea:

See Gettys’ 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+ from commitment to x.

Setup: p, q large primes s.t. q | p-1 (e.g., p "safe prime")
g generator of order-q subgroup of $\mathbb{Z}_p^*$
(e.g., if p safe then $<g> = \mathbb{Z}_p^*$ = squares mod p)
h = g^a \text{ a secret}

Commit(x): $x \in \mathbb{Z}_q$ (i.e. $0 \leq x < q$)
Sender chooses random $r \in \mathbb{Z}_q$
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 \( r' \)

\[
\begin{align*}
    g^{x^r} &= g^{x'} h^{r'} \\
    g^{xg^r} &= g^{x'} g^{ar'} \\
    g^{x^r + ar'} &= g^{x' + ar'} \\
    x + ar &= x' + ar' \pmod{q}
\end{align*}
\]

\[ r' = (x-x')/a + r \]

\( q \) is prime so \( a \) exists

\( r' \neq r \) since \( x \neq x' \)

**Binding:** If sender can reveal two ways

\[ c = g^{x^r} = g^{x'} h^{r'} \]

\[ x + ar = x' + ar' \]

\[ a = (x-x)/(r-r') \]

\( r' \neq r \) and \( q \) is prime

\[ = \text{discrete log of} \ h, \ \text{base} \ g, \ \text{mod} \ p \]

**Non-malleable:** No.

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

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

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

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

Then \( 1^\lambda = 11\ldots1 \) \( \lambda \) 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 \( m \in \text{message space } M \)
   to \( c \in \text{ciphertext space } C \)
   (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 $(PK, SK)$ (8 description of $G$, if needed)

**Encryption:**

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

Assume message $m$ represented as element of $G$.

Let $y = g^k$ be $PK$ of recipient.

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

**Decryption:**

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

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

[Correctness follows since $a^k = g^{kx} = g^{xk} = y^k$.]
El Gamal encryption related to DH key exchange:

**Alice**
\[ y = g^x \quad \text{(via PKI?)} \]

**Bob**
\[ a = g^k \]

**DH Key**
\[ (g^k)^k = g^{kk} \]

**b = m \cdot (DH\ Key)\**

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
   (as 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 m₀, m, of same length,
  and "state information" s. [m₀ ≠ m, required]

Phase II ("Guess"):  
- Examiner picks b ∈ {0, 1}^R, computes c = E(PK, mₐ)
- Examiner sends c, s to Adversary
- Adversary computes for polynomial (in λ) time,
  then outputs ²b (his "guess" for b).

Adversary "wins" game if ²b = 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.)*

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

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

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

Theorem: $\text{DDH} \Rightarrow \text{CDH}$

Proof: If $\neg \text{CDH}$, then $\neg \text{DDH}$ (contrapositive).

If you can compute $g^{ab}$ from $g^a$ and $g^b$ ($i.e. \neg \text{CDH}$)
then you can decide if given third element is $g^{ab}$
($i.e. \neg \text{DDH}$). $\blacksquare$
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 $E(\alpha m) = (g^k, (\alpha m) \cdot y^k)$  
  without knowing $m$!
- More generally, El Gamal is homomorphic:  
  Given $c_1 \in E(m_1) = (g^r, m_1 \cdot y^r)$  
  and $c_2 \in E(m_2) = (g^s, m_2 \cdot y^s)$  
  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 games

Phase I ("Find"): 
- Examiner generates $(PK, SK)$ using Keygen($\lambda$)
- Examiner sends $PK$ to Adversary 
- Adversary computes for polynomial (in $\lambda$) time, having access to a decryption oracle $D(SK, \cdot)$ then outputs two messages $m_0, m_1$ of same length, and "state information" $s$. $[m_0 \neq m_1, \text{ required}]$

Phase II ("Guess"): 
- Examiner picks $b \leftarrow \{0, 1\}$ computes $c_\ast = E(PK, m_b)$
- Examiner sends $c_\ast, s$ to Adversary
- Adversary computes for polynomial (in $\lambda$) time, having access to a decryption oracle $D(SK, \cdot)$ except on input $c_\ast$
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 
$\Pr [\text{Adv wins}] \leq \frac{1}{2} + \text{negligible}$
How to make El Gamal IND-CCA2 secure?

- Cramer-Shoup method is such an extension of El Gamal.
- Let $G_g$ be a group of prime order $g$  
  (e.g., $G_g = \mathbb{Z}_p^*$, where $p = 2g+1$, $p$ & $g$ prime).
- **Keygen**:
  
  $g_1, g_2 \leftarrow \mathbb{G}_1$  
  $x_1, x_2, y_1, y_2, z \leftarrow \mathbb{Z}_g$  
  $c = g_1^{x_1} g_2^{x_2}$  
  $d = g_1^{y_1} g_2^{y_2}$  
  $h = g_1^z$  

PK = $(g_1, g_2, c, d, h)$  
H = hash fn mapping $G_2^3$ to $\mathbb{Z}_g$  
SK = $(x_1, x_2, y_1, y_2, z)$
\[ \text{Enc}(m) \] [where \( m \in \mathbb{G}_q \)]:

- \( r \leftarrow \mathbb{Z}_p^* \)
- \( u_1 = g_1^r \)
- \( u_2 = g_2^r \)
- \( e = h^{r \cdot m} \)
- \( \alpha = H(u_1, u_2, e) \)
- \( v = c^r d^{r \cdot \alpha} \)

\[ \text{ciphertext} = (u_1, u_2, e, v) \]

\[ \text{Decrypt}(u_1, u_2, e, v) : \]
- \( \alpha = H(u_1, u_2, e) \)
- Check: \( u_1^{x_1 + y_1 \cdot \alpha} u_2^{x_2 + y_2 \cdot \alpha} = v \)

If not equal, reject
else output \( m = e / u_2^2 \)

Note:
- \( u_1^{x_1} u_2^{x_2} = g_1^{r \cdot x_1} g_2^{r \cdot x_2} = c^r \)
- \( u_1^{x_1} u_2^{x_2} = d^r \)
- \( u_1^{x_2} = g_1^{r \cdot x_2} = h^r \)
Theorem: Cramer-Shoup is IND-CCA2
secure (i.e. secure against adaptive chosen
plaintexts) if
1. DDH holds in Gq
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.