6.857 Recitation 9: Quiz Review

TAs: Andrew He, Leo de Castro, Sean Fraser

Friday April 12, 2019

Agenda

- One Time Pad
- Hash Functions and Applications (e.g. Merkle Trees)
- Block Ciphers & Modes of Operation
- Security Scheme Definitions

  CPA-security, CCA-security, (symmetric / public key crypto)
- Message Authentication Codes (MACs)
- Quadratic Residues, Discrete Log, CDH, DDH
- Diffie Helman Key Exchange
- Shamir Secret Sharing (on quiz but not covered today, see lecture notes / paper)
- Commitment Schemes (Definition, Pedersen Commitments)
- Public Key Cryptosystems

  El Gamal

  RSA
- Digital Signatures

  Hash & Sign Paradigm

  El Gamal + DSA
- Miscellaneous (on quiz but not covered today, read lecture notes):

  Security of ML, PKI + TLS, Bitcoin, Differential Privacy, Voting Security

The last two thirds of the notes from the recitation are given below (starting at Quadratic Residues, Discrete Log, CDH, DDH).

1 DDH and QR

Recall the DDH assumption, where we assume that $(g^x, g^y, g^{xy}) \approx_c (g^x, g^y, g^z)$. In the pset, you will show that this assumption is false for general groups.

At a high level, the attack involves testing the order of an element in the group. But, what if all the elements in the group had the same order?

Theorem 1 (Lagrange's Theorem)**.** *For every finite group G and every element $x \in G$, $|x|$ divides $|G|$.*

If the order of G is prime, then every element $x \in G$ where $x \neq 1$ will have order $|x| = |G|$. We will construct such a group.

1.1 Quadratic Residues

Definition (Quadratic Residue)**.** An element $y \in G$ is a quadratic residue if there exists an $x \in G$ such that $x^2 = y$ (multiplication over G).

Consider a prime of the form $p = 2q + 1$, where q is also prime[1].

Lemma. *For all $y = x^2$, where $x \in G$, $2|y| \geq |x|$.*

Proof. Since the order of x is the smallest exponent t such that $x^t = 1$, we know that t cannot exceed $2s$, where $y^s = 1$, since $y^s = x^{2s} = 1$. □

Theorem 2. *For every safe prime $p = 2q + 1 > 7$, every quadratic residue in $\mathbb{Z}_p^*$ that is not 1 has order q.*

Proof. The order of $\mathbb{Z}_p^*$ is $p - 1 = 2q$. By theorem 1, the only possible orders of elements in $\mathbb{Z}_p^*$ are $1, 2, q$, and $2q$, since these are the only numbers that divide $2q$.

Consider a quadratic residue $y = x^2 \neq 1$ in $\mathbb{Z}_p^*$.

$|y| \neq 1$, since $y \neq 1$.

$|y| \neq 2$, since if it did then $|x|$ would have to either be 3 or 4 by the lemma above (if x had order 1 or 2 then we would have $y = 1$). Since $p > 7$, $q > 3$, we have that $3 \neq q$ and 4 is not prime, so by Lagrange's Theorem these orders are not possible.

$|y| \neq 2q$, since the order of y cannot be greater than q. This is because $y^q = x^{2q} = x^{p-1} = 1$, by Fermat's little theorem.

Therefore, $|y| = q$. □

Theorem 3. *The set of quadratic residues of $\mathbb{Z}_p^*$ for a safe prime p is a subgroup.*

Proof. Call QR the set of quadratic residues in $\mathbb{Z}_p^*$. Let's enumerate the properties of an abelian group.

1. Identity. $1 \in QR$, since $(-1)^2 = 1$.

[1] p is called a *safe prime* and q is called a *Sophie Germain* prime.

2. Closure. If $y_1 = (x_1)^2$ and $y_2 = (x_2)^2$, then $y_1 \cdot y_2 = (x_1 \cdot x_2)^2$, so $y_1 \cdot y_2 \in QR$.

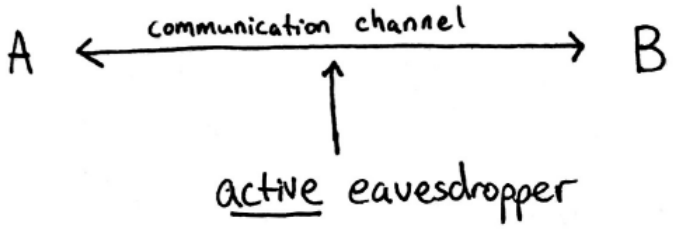
3. Associativity and Commutativity. Inherited from $\mathbb{Z}_p^*$.

4. Unique inverses. For all $y = x^2$, we know there exists a unique $y^{-1} \in \mathbb{Z}_p^*$ such that $y \cdot y^{-1} = 1$. All we need to show is that y^{-1} is a quadratic residue. Consider x^{-1}. We know that $y \cdot (x^{-1})^2 = x^2 \cdot (x^{-1})^2 = 1$, so $(x^{-1})^2 = y^{-1} \in QR$.

□

We now have a group of prime order. Finding a generator (an element g such that $|g| = |QR|$) is easy, since by theorem 2 any quadratic residue that's not 1 has order $q = |QR|$. In many of the constructions in class, we'll need to work over a group of prime order, so these results are very useful.

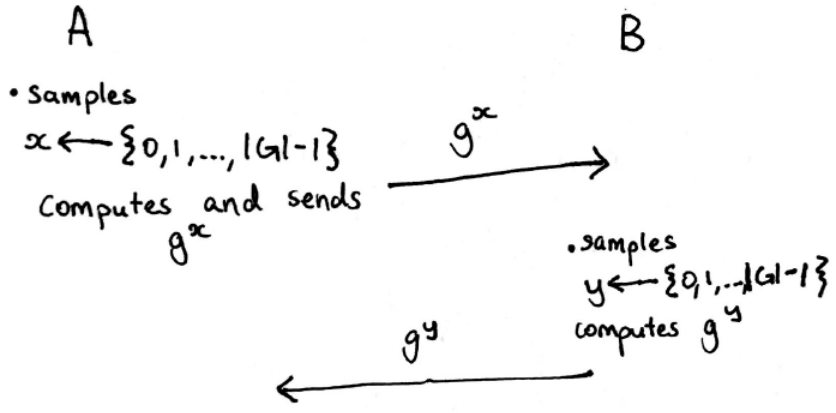
1 Man-In-The-Middle Attacks



We will illustrate an example of a Man-In-The-Middle attack using the textbook Diffie-Hellman (DH) Key Exchange. Suppose we have a communication channel between Alice (A) and Bob (B) with an active eavesdropper (Eve, or E) as shown. In class we showed this setup with a passive eavesdropper, and we will show why an active eavesdropper is problematic.

Recall: DH Key Exchange

- G is a finite cyclic group, with generator g.
  - $G = \{g^0, g^1, ..., g^{|G|-1}\}$
  - G and g are fixed and <u>public</u>



- A and B compute $K = g^{xy} = (g^x)^y = (g^y)^x$
- Relies on DDH - <u>Decisional</u> Diffie Hellman Assumption: $(g^x, g^y, g^{xy}) \approx_c (g^x, g^y, g^z)$

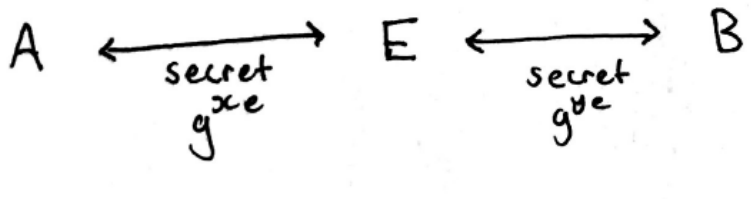
  Given g^x and g^y, cannot distinguish between g^{xy} and g^z with probability $> \frac{1}{2} + \lambda$, where $u \leftarrow \{0, 1, ..., |G| - 1\}$ (randomly drawn).

Note: confer with CDH, Computational Diffie Hellman assumption, in Lecture 9, which is less strong.

Assuming DDH, Diffie Hellman is secure under a *passive* adversary.

Problem: Totally insecure to an *active* eavesdropper.

Man-in-the-Middle Attack (MITM): active eavesdropper can intercept and relay messages in between Alice and Bob. In the DH key exchange for example, this means the adversary can establish a different key with each of A and B separately, using the DH key exchange, tricking Alice and Bob that Eve is the other person respectively when she is really not. This might work as shown below, with Eve intercepting each of g^x from Alice and g^y from Bob and sending g^e to both. This gives Eve full power to encrypt and decrypt messages between Alice and Bob, and change them how she likes.



Problem: Authenticity. A and B have no way of verifying the "identity" of the other.

Potential solution: Digital Signatures.

2 Pedersen Commitments

For generators g and h of a prime order group, a Pedersen commitment to a value x with randomness r is $c = g^x h^r$. To open the commitment, reveal x and r.

These commitments are perfectly hiding, since there exists an r' for any x' we may want to open. This is because $h = g^a$ for some a, so $c = g^z = g^{x+ra}$. Solving for r, we get that $r = a^{-1}(z - x)$.

Remark. For a general multiplicative group G, the exponents can be represented as elements in $\mathbb{Z}_q$, where $q = |G|$. Since $|G|$ is prime in the case above, $\mathbb{Z}_q$ is a field, so a^{-1} is always well defined (for $a \neq 0$).

For a given commitment, there exists an r' for every x', so these commitments can only be computationally binding. However, we can reduce the hardness of opening the commitments in two different ways to the difficulty of computing discrete logs by showing how to compute the discrete log of $h = g^a$ given two different openings for $c = g^x h^r = g^z$.

Given two openings (x, r) and (x', r'), we know that $c = g^x h^r = g^{x'} h^{r'}$. Therefore, $z = x + ra = x' + r'a$, so solving for a gives us the following equation:

$$a = \frac{x - x'}{r' - r}$$

Opening a Pedersen commitment in two different ways is at least as hard as computing the exponent a. If the discrete log assumption holds, then the exponent a is hard to compute, so Pedersen commitments are computationally binding.

Public Key Cryptosystems

- El Gamal
- RSA

Digital Signatures

- Hash & Sign Paradigm
- El Gamal
- DSA

Public Key Encryption

- Keygen, Enc, Dec algorithms

① Keygen: $\lambda \approx$ keysize / security parameter in unary 1^λ
only the length λ matters for poly. time measurement.

$(PK, SK) \leftarrow$ Keygen (1^λ)

② Enc: $c \leftarrow Enc(PK, m)$

③ Dec: $Dec(SK, c)$: returns m

Correctness:

$Dec(SK, Enc(PK, m)) = m$

for all m, $\forall (PK, SK)$

"Semantic Security" - Equivalent to IND-CPA Security

$(PK, Enc(PK, m)) \cong (PK, Enc(PK, m'))$ $\forall m, m' \in \mathcal{M}$ ← message space

ie. if any probabilistic polynomial time algorithm that is given c and λ cannot determine any other info w/ non-negligible prob.

- infeasible for computationally bounded adversary to gain any info about m given $(PK, Enc(PK, m))$

⇒ For semantic security (and CPA security)

Enc. must be randomized. in addition to keygen

(Dec usually deterministic).

El Gamal Encryption Scheme (relies on DDH assumption)

$G = \langle g \rangle$ cyclic group w/ generator g

Want DDH to hold in this group

re. $(g^x, g^y, g^{xy}) \approx (g^x, g^y, g^r)$ x, y, r random in $\{0, 1, \ldots, |G|-1\}$

eg. set of all quadratic residues in $\mathbb{Z}_p^*$, $p = 2q + 1$

ie. Q_p^*, prime order subgroup (order q), $q \mid p-1$

any $QR \neq 1$ is a generator of this group. $g \in \mathbb{Z}_p^*$

① Keygen: $x \xleftarrow{\text{random}} \{0, 1, \ldots, |G| - 1\}$

Let $SK = x$

$PK = g^x$ (relies on DLog assumption, fine since we assume DDH)

② Enc: Given $PK = g^x$, $m \in G$

$y \xleftarrow{\text{random}} \{0, 1, \ldots, |G| - 1\}$

compute $K = g^{xy}$

return $(g^y, K \cdot m)$ ← note similarity to key in DH key exchange.

3.

Dec: Given $SK = x$, and C

$$(a, b) = (g^y, g^{xy} \cdot m)$$

return $m = \frac{b}{a^x}$

$$= \frac{g^{xy} \cdot m}{(g^y)^x}$$

$$= m$$

divide by $a^x = g^{xy} = K$

Security: (semantic / CPA)

show given $PK = g^x$, g^y, and m

$K = g^{xy}$ uniformly distributed in G_1.

⇒ relies on DH key Exchange, which is known to be secure under DDH assumption

⇒ enc by multiplying by key g^{xy}
dec by dividing

Semantically secure (CPA-secure)

Not CCA2 (CCA) secure

why? **malleable** $Enc(g^x, m) = g^y, g^{xy} \cdot m$

→ easy to get $Enc(2m) = g^y, g^{xy} \cdot 2m$
⇒ breakable $m' = 2m$

Solution for CCA Security: **Cramer-Shoup extension**

→ Adds a "test" to ciphertext decrypt only if "test" passes, requires some knowledge of message. Dec oracle useless. exclude malleability

RSA Encryption Scheme - Public key

↳ "trapdoor" one-way permutation

deterministic => not semantically secure.

① Keygen(1^λ):

- pick large p, q set $n = p \cdot q$ e.g. (λ = 1024 bits)
- sample $e \leftarrow \mathbb{Z}^*_{\varphi(n)}$, compute $d = e^{-1} \bmod \varphi(n)$

$\varphi(n) = |\mathbb{Z}_n^*| = (p-1)(q-1)$

how to compute e^{-1}? Extended euclid algorithm, given $\varphi(n)$.

$PK = (n, e)$

$SK = (n, d)$

② $Enc(PK, m)$: $Enc((n, e), m) = m^e \bmod n$

③ $Dec((n, d), C) = C^d \bmod n$

$Dec(SK, C)$

$= (m^e)^d$

$= m \bmod n$

Deterministic, $f(x) = x^e$ ← trapdoor function

Relies on inability to factor p, q from $n = pq$.

$\varphi(n) = |\mathbb{Z}_n^*|$ = need to know p & q.

Not even CPA secure. How to make CCA secure?

RSA-OAEP (Optimal Asymmetric Enc Padding).

Apply RSA encryption on an encoding of the message

uses unbalanced feistel encryption structure.

Digital Signatures

use users (PK, SK) keys

want: 1 person to be able to sign
everyone able to verify.

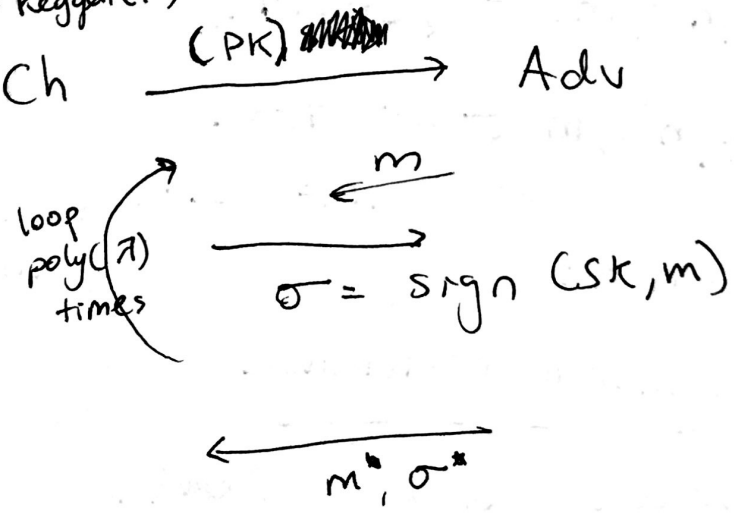
PK to sign, SK to verify.

Defn: Digital Signature Schemes

- keygen $(1^\lambda) \rightarrow (PK, SK)$
- Sign $(SK, m) \rightarrow \sigma_{SK}(m)$ ↙ (can be randomized)
- Verify $(PK, m, \sigma) \rightarrow$ True or False

Security "against adaptive chosen message attacks"
or "existential unforgeability".

$(PK, SK) \leftarrow$ keygen(1^λ)



Adv wins if m^* was not queried, and
verify (m^*, σ^*, PK) = True
i.e. valid signature forged.

Secure if Pr[Adv wins] = negl(λ).

Try:

$$\text{Sign}(SK, m) = \text{Dec}(SK, m)$$

$$\text{Verify}(PK, m, \sigma) = 1 \iff \text{Enc}(PK, \sigma) = m$$

with eg. deterministic PK encryption scheme,

eg. RSA.

$$\text{sign}(SK, m) = m^d \bmod n$$

easily can sign $m^2 \bmod n$

$$= (m^d)^2 \bmod n$$

insecure

Hash & Sign Paradigm

eg. GMR signatures (from RSA)

$$\text{Sign}((sk, h), m) = (h(m))^d \bmod n$$

$$\text{Verify}((PK, h), m, \sigma) = \text{true}$$

IFF $\sigma^e = h(m) \bmod n$.

- Security depends on h:

  needs collision resistance

- proven to be secure under ROM.
- enhances security & more efficient

7...

El Gamal Signatures

public parameters

(Reminder: g generates prime order subgroup (order q), contained in $\mathbb{Z}_p^*$)

Keygen: $SK = x$

$(x \leftarrow \mathbb{Z}_q)$ $\{0, \ldots, q-1\}$

$y = g^x \bmod p$

$PK = y$

Sign (SK, m):

$k \xleftarrow{\text{random}} \mathbb{Z}_q^*$

output $\sigma = (r, s) = \left(g^k \bmod p, \frac{h(m) + rx}{k} \bmod q\right)$

Verify: $(PK, m, (r,s))$

check if $\underbrace{y^{r/s} \cdot g^{h(m)/s}} = r$

$= g^{\frac{xr}{s}} \cdot g^{h(m)/s}$

$= g^{\frac{xr + h(m)}{s}}$

$= g^k$

$= r \bmod p.$

- Use $h(m||r)$ instead of $h(m)$
  - ⇒ now secure under adaptive chosen msg attacks, in ROM.

DSA (Digital Signature Algorithm)

- close variant of El gamal signatures
- much faster ⇒ works in subgroup of smaller order q instead of larger prime p
- same provable level of security if used with $h(m||r)$ instead of $h(m)$

  $|p| = 1024$ bits $|q| = 160$ bits
- ops done mod q e.g. $r = (g^k \bmod p) \bmod q$