6.857 Recitation 6
Quadratic Residues, Pedersen Commitments, El Gamal

TA: Leo de Castro

March 18, 2019

Today

- DDH Assumption
  - Groups of prime order
- Pedersen Commitments
- El Gamal Encryption

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].

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

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 $(-1)^2 = 1$.

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.

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.

3 El Gamal Encryption

Let g be a generator of a group G where we believe DDH is hard. Our secret key is an element $x \leftarrow \{1, 2, \ldots, |G| - 1\}$. The public key is g^x.

To encrypt a message $m \in G$, sample a random $y \leftarrow \{1, 2, \ldots, |G| - 1\}$ and compute g^{xy}. Output $c = (g^y, m \cdot g^{xy})$.