COMP 3704 Computer Security

Christian Grothoff
christian@grothoff.org

http://grothoff.org/christian/

Quadratic Residues

If p is prime and $0 < a < p$ then a is a **quadratic residue** $\mod p$ if there exists an x such that

$$x^2 \equiv a \mod p. \tag{1}$$

Legendre Symbol

For odd primes p and $a \in \mathbb{Z}$, define:

$$L(a,p) := a^{\frac{p-1}{2}} \mod p \tag{2}$$

$L(a,p) = 1$ if and only if a is a quadratic residue $\mod p$.

Computing $\sqrt{a} \mod pq$: Summary

If $n = pq$ for primes p and q, computing x such that $x^2 \equiv a \mod n$ for arbitrary $a \in \mathbb{Z}_n$ is as hard as factoring n.

Computing $\sqrt{a} \mod pq$: Reduction

Consider solving $x^2 - a \equiv 0 \mod pq$.

x can be found by instead solving first

$$x_1^2 - a \equiv 0 \mod p \quad (3)$$
$$x_2^2 - a \equiv 0 \mod q \quad (4)$$

and then solve

$$x \equiv x_1 \mod p \qquad \wedge \qquad x \equiv x_2 \mod q \quad (5)$$

for x using the Chinese remainder theorem.

Computing $\sqrt{u} \mod p$: Simple Case

If $p \in 3 + 4\mathbb{Z}$, suppose $x^2 \equiv u \mod p$. Then

$$
\begin{aligned}
u &\equiv x^2 \mod p && (6)\\
&\equiv x^2 x^{p-1} \mod p && (7)\\
&\equiv x^{p+1} \mod p && (8)\\
&\equiv u^{(p+1)/2} \mod p && (9)\\
&\equiv \left(u^{(p+1)/4}\right)^2 \mod p && (10)
\end{aligned}
$$

Thus $x \equiv u^{(p+1)/4} \mod p$.

Feige-Fiat-Shamir Identification Scheme

- Based quadratic residues $\mod n$
- Cut-and-choose protocol
- Requires multiple rounds of communication
- More computationally efficient than RSA

Feige-Fiat-Shamir Protocol

Peggy's public key is a quadratic residue $v \mod n$. Peggy's private key is $s \equiv \sqrt{v^{-1}} \mod n$

1. Peggy picks a random number r and sends $x \equiv r^2 \mod n$ to Victor.
2. Victor sends Peggy a random bit b.
3. If $b = 0$, Peggy sends Victor r. If $b = 1$, the Peggy sends Victor $y = r \cdot s \mod n$.
4. If $b = 0$, Victor verifies that $x \equiv r^2 \mod n$. If $b = 1$, Victor verifies that $x = y^2 \cdot v \mod n$.

Embedding Peggy's Identity

- Peggy does not need to have p, q so that $pq = n$.
- Trend may have p and q and just give Peggy s.
- v maybe constructed as $H(I, j)$ where I is Peggy's identity, s is then computed using p and q by Trend and given to Peggy.
- I and j becomes Peggy's public key. j is needed since $H(I)$ may not be a quadratic residue $\mod n$.

Schnorr Identification Scheme

- Based on difficulty of calculating discrete logarithms
- Not more efficient than RSA, but possibly more secure
- Uses two primes p and q and a number $a \neq 1$ where $q | p - 1$ and $a^q \equiv 1 \mod p$

Schnorr Protocol

Peggy's private key is $s < q$. $v \equiv a^{-s} \mod p$ is the public key.

1. Peggy picks random number $r < q$ and sends $x \equiv a^r \mod p$ to Victor.
2. Victor sends Peggy $e \in [0 : 2^t - 1]$.
3. Peggy responds with $y \equiv r + se \mod q$.
4. Victor verifies that $x \equiv a^y v^e \mod p$.

Questions

?

Problem

Show that $L(a, p) = 1$ if and only if a is a quadratic residue $\mod p$!

Reminder: For odd primes p and $a \in \mathbb{Z}$, we defined:

$$L(a, p) := a^{\frac{p-1}{2}} \mod p \tag{11}$$

UNIVERSITY OF DENVER

Proof (Part 1)

If a is a quadratic residue $\mod p$, then there exists x with $x^2 \equiv a \mod p$. Then:

$$
\begin{aligned}
1 &\equiv x^{p-1} \mod p && (12)\\
&\equiv a^{\frac{p-1}{2}} \mod p && (13)\\
&\equiv L(a,p) && (14)
\end{aligned}
$$

UNIVERSITY OF DENVER

Proof (Part 2)

For any $x \in \mathbb{Z}_p$ and $x \not\equiv 0 \mod p$ consider $y \equiv x - p \mod p$. Then $x \not\equiv y$ and

$$y^2 \equiv x^2 - 2xp + p^2 \mod p \tag{15}$$

$$\equiv x^2 \mod p \tag{16}$$

Suppose $z^2 \equiv x^2 \mod p$. Then $p | y^2 - z^2 = (y - z)(y + z)$ and thus either $p | y - z$ or $p | y + z$. Thus $z \equiv y$ or $z \equiv -y \equiv x \mod p$.

Proof (Part 3)

Part 2 implies that there are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ positive quadratic non-residues.

Also, $f(a) = a^{\frac{p-1}{2}} - 0$ has at most $\frac{p-1}{2}$ roots.

Since there are exactly $\frac{p-1}{2}$ quadratic residues $\mod p$, thus $f(a) \equiv 1 \mod p$ for all quadratic residues.