CSL 759 – Cryptography and Network Security Jan 15, 2014

Lecture 5

Instructor: Shweta Agrawal *Scribe: Karan Goel*

1 Computing One-Bit

Lemma 1 *Given* $g^x \bmod p \in \mathbb{Z}_p^\star$*, we can compute the LSB of* x *efficiently.*

Proposition 1 *Consider a quadratic equation,*

$$x^2 \equiv a \bmod p$$

in the group $\mathbb{Z}_p^\star$*.*

Claim: This equation has exactly 0 or 2 roots, and it cannot have 1 root. We prove this as follows.
Proof. For this equation to have a single root is impossible as $x \neq -x \bmod p$, and also

$$\begin{gathered} x^2 \equiv y^2 \bmod p \\ (x+y)(x-y) \equiv 0 \\ x = \pm y \\ \because \mathbb{Z}_p \text{ is in integral domain} \end{gathered}$$

Thus, the equation cannot have more than two roots as well. ■

Definition 1 (Quadratic Residues) $a \in \mathbb{Z}_p^\star$ *is called a quadratic residue if*

$$x^2 \equiv a \bmod p$$

has exactly two solutions.

We can use the Quadratic Residue (QR) to determine the $LSB(x)$. However, it can get hard to determine QRs in a composite order field.

Lemma 2 *Suppose* g *is a generator of* $\mathbb{Z}_p^\star$*,* $a \in \mathbb{Z}_p^\star$ *and* $a = g^z$*, then*

$$a \textit{ is a } QR \Leftrightarrow z \textit{ is even} \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \bmod p$$

Proof.

1.

$$\begin{gathered}\text{If } z = 2w, \\ \implies a = g^z = (g^w)^2 \text{ is a QR.}\end{gathered}$$

Conversely,

$$\begin{gathered}\text{if } a = (g^w)^2, \\ \text{then } z \equiv 2w \bmod (p-1), \\ \text{and since } (p-1) \text{ and } 2w \text{ are even} \\ \implies 2w \bmod (p-1) \text{ is even} \\ \implies z \text{ is even}\end{gathered}$$

2.

$$\begin{gathered}\text{If } z = 2w, \\ \implies a^{\frac{p-1}{2}} = g^{\frac{z(p-1)}{2}} = g^{w(p-1)} \equiv 1 \bmod p \text{ (By Fermat's Little Theorem)}\end{gathered}$$

Conversely,

$$\begin{gathered}\text{if } g \text{ is a generator and } g^{\frac{z(p-1)}{2}} \equiv 1 \\ \implies z \cdot \frac{p-1}{2} \equiv 0 \bmod (p-1) \\ \implies z \cdot \frac{p-1}{2} = w(p-1), \text{ , for some } w \\ \implies z = 2w \\ \therefore z \text{ is even}\end{gathered}$$

■

Corollary: Exactly half of the elements in $\mathbb{Z}_p^\star$ are QR.

Definition 2 (Legendre Symbol) *Suppose p is prime and $a \in \mathbb{Z}_p^\star$,*

$$\begin{gathered}(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \bmod p, \\ (\frac{a}{p})^2 \equiv 1 \bmod p, (\frac{a}{p}) \in \{+1, -1\},\end{gathered}$$

where $(\frac{a}{p})$ is called the Legendre symbol of a, and a is a QR if and only if its Legendre symbol is $+1$.

Note that the Legendre symbol can be computed efficiently. Thus, we can find the LSB easily (z will become even/odd), depending on the Legendre symbol.

There might be a possibility that a part of x is discovered which if it is being used as a secret key, can be dangerous.

A **trapdoor permutation** can be inverted using some secret information.
If we have a group $\mathbb{Z}_n^\star$, where $n = pq$ (p and q are arbitrary large primes), pick $e \in \mathbb{Z}_{\phi(n)}^\star$. $\exists$ some d such that $e.d = 1 \bmod \phi(n)$ ($\because$ inverses in a group).

The RSA Encryption Scheme

Let the Public Key be (n, e) and the Secret Key be d. Let there be a OWF, $f(x)$ such that

$$f(x) = x^e \bmod n$$

Using the SK d, one can quickly recover x, as shown below

$$(x^e)^d = x^{ed \bmod \phi(n)} = x^1 = x$$

1. Security is only proven for a uniformly random distribution of x (in which case $f(x)$ is hard to invert). However, messages are not guaranteed to be uniformly random. Therefore, RSA is secure only if messages are uniformly random.

2. The RSA scheme does not guarantee that every bit of x is kept secret. It is possible that a bit of x may be discovered, which can potentially leak some partial information.

If factoring is easy, then RSA is easy, and the encryption scheme will no longer be secure. However, the converse is not true and RSA is not as hard as factoring.

Chinese Remainder Theorem

Theorem 3 (Chinese Remainder Theorem) *Let m_1, m_2,..., m_k be pairwise relatively prime and let $m = \Pi m_i$. Then $\forall a_1 \in \mathbb{Z}_{m_1}$, $\forall a_2 \in \mathbb{Z}_{m_2}$, . . ., $\forall a_k \in \mathbb{Z}_{m_k}$, $\exists$ a unique $a \in \mathbb{Z}_m$ such that*

$$a \equiv a_i \bmod m_i, \forall i \in 1, .., k$$

Proof. The proof is left as an exercise for the reader.

■

Definition 3 (Jacobi's Symbol) *If $n = pq$, where p, q are 2 primes, then we define the Jacobi's symbol of $a \in {\mathbb{Z}_n}^*$, where $a = (a_1, a_2)$, to be*

$$\left(\frac{a}{n}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{q}\right)$$

where the RHS contains Legendre symbols (prime order components) that are multiplied together. There exists a PPT algorithm to compute $\left(\frac{a}{n}\right)$*, without factoring* n *into its primes* p *and* q*.*

Lemma 4 *If* a *is a QR, and* $\left(\frac{a}{n}\right)$ *is the Jacobi's symbol of* a*, then* $\left(\frac{a}{n}\right) = +1$*. The converse is not necessarily true.*

Given an element, determining the QR over composite order groups is a hard problem.