Cocks' IBE Algorithm

W.K. Chiu, C. Ding, C.L. Yu

May 16, 2010

Outline

Problems with Traditional Public Key Encryption

Traditional public key encryption is based on digital certificate, and is called **certificate-based encryption** (CBE).

- The generation of key pairs, the issuing of digital certificates, the publication of the digital certificates, and the management of all these requires a dedicated secure infrastructure.
- Such an infrastructure is expensive and complex, and does not scale well to large sizes, and does not easily extend to manage parties' attributes, e.g., their roles and rights.
- IBE offers an option with certain advantages in some applications.

What is Identity-Based Encryption?

- It is a public key encryption scheme.
- Public key: any valid string, which uniquely identifies a user and is chosen by the encrypting party
- Private key: it can be computed only by a trusted third party, called the **key server** or **private key generator**.
  – This need not be done at the same time when the public key is chosen.
- The trusted third party will release the private key, only to those parties who provide evidence of their right to have it.
- Parties who are issued with the private key can use it to decrypt the content encrypted with the public key.

Advantages of IBE over Certificate-Based Encryption (CBE)

- Eliminate the need for digital certificate and thus certification authorities
- Simplify the key management in some aspects

IBE Procedure

1. Alice encrypts the email using Bob's e-mail address, e.g. bob@bob.com, as the public key. Then she sends the ciphertext and the public key to Bob.
2. When Bob receives the message, he contacts the key server, asking the server to distribute the private key to him.
3. The key server contacts a directory or other external authentication source to authenticate Bob's identity and establish any other policy elements.
   After authenticating the Bob, the key server then returns his private key, through a secure channel.
4. After receiving the private key, Bob can decrypt the message. This private key can be used to decrypt future messages encrypted with the same public key.

The IBE Framework

- **Setup**:
  - Run by the Private Key Generator (PKG) one time for creating the whole IBE environment.
  - Output: Public system parameters P & a master-key K_m which is know only to the PKG.
- **Extraction**:
  - The process which the PKG generates the private key for user.
  - Input: system parameters P, master-key K_m and any arbitrary ID (i.e., the public key)
  - Output: private key d
- **Encryption**:
  - Input: system parameters P, ID of receiver and a plaintext message M
  - Output: ciphertext C
- **Decryption**:
  - Input: system parameters P, private key d issued by the PKG, and the ciphertext C
  - Output: plaintext message M

Comparisons of traditional CBE and IBE

Features	Certificate Based PKI	ID based PKI
Private key generation	By user or Certificate Authorities	By Private Key Generator (PKG)
Key certification	Yes	No
Key distribution	Requires an integrity protected channel for distributing a new public key from a user to his CA	Requires an integrity and privacy protected channel for distributing a new private key from the PKG to its owner
Public key retrieval	From public directory or key owner	On-the-fly based on owner's identifier

Notation

Notation

- m, n — Natural number
- p, q — Primes
- $\mathbb{Z}_p$ — Finite ring of integer modulo p, where p is prime
- $\mathbb{Z}_n$ — Finite ring of integer modulo n
- $\mathbb{Z}_p^*$ — Cyclic group of $p - 1$ elements
- $\mathbb{Z}_n^*$ — Group of units of $\mathbb{Z}_n$

Unless otherwise specified:

- Only integers are considered.
- All variables are assumed to be natural number.

Congruence modulo n

Let a, b be two integers (possibly negative):

Definition

The *congruence modulo n* relation, $a \equiv b \pmod{n}$ means $n \mid (a - b)$.

Note

The relation $\equiv$ is an equivalence relation.

Example

- $8 \equiv 18 \equiv 28 \equiv -2 \pmod{10}$
- $0 \equiv n \pmod{n}$

Basic Properties

Properties

If $x \equiv a \pmod{n}$ and $y \equiv b \pmod{n}$,

- $x \pm y \equiv a \pm b \pmod{n}$
- $xy \equiv ab \pmod{n}$
- $x^k \equiv a^k \pmod{n}$

Note

By division algorithm, for all $m \in \mathbb{N}$, there is a unique integer r s.t.

1. $m \equiv r \pmod{n}$
2. $0 \leq r < n$

We denoted such r, namely the *remainder*, by $m \bmod n$.

Finite ring of integers modulo n

Definition

$\mathbb{Z}_n$ is defined such that the following are all satisfied:

1. $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ with two operations $+_n$ and $\cdot_n$.
2. Addition of $x, y \in \mathbb{Z}_n$, denoted by $x +_n y$, is the unique element $z \in \mathbb{Z}_n$ s.t. $x + y \equiv z \pmod{n}$.
3. Multiplication of $x, y \in \mathbb{Z}_n$, denoted by $x \cdot_n y$, is the unique element $z \in \mathbb{Z}_n$ s.t. $x \cdot y \equiv z \pmod{n}$.
4. Additive identity 0 and multiplicative identity 1 exist.
5. For each element, its additive inverse exists.
6. Associative, commutative and distributive law holds.

In case of no ambiguity, the subscript n of operators under $\mathbb{Z}_n$ is omitted.

Finite ring of integers modulo n

Definition

$\mathbb{Z}_n$ is defined such that the following are all satisfied:

1. $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ with two operations $+_n$ and $\cdot_n$.
2. Addition of $x, y \in \mathbb{Z}_n$, denoted by $x +_n y$, is the unique element $z \in \mathbb{Z}_n$ s.t. $x + y \equiv z \pmod{n}$.
3. Multiplication of $x, y \in \mathbb{Z}_n$, denoted by $x \cdot_n y$, is the unique element $z \in \mathbb{Z}_n$ s.t. $x \cdot y \equiv z \pmod{n}$.
4. Additive identity 0 and multiplicative identity 1 exist.
5. For each element, its additive inverse exists.
6. Associative, commutative and distributive law holds.

In case of no ambiguity, the subscript n of operators under $\mathbb{Z}_n$ is omitted.

Finite ring of integers modulo n

Definition

$\mathbb{Z}_n$ is defined such that the following are all satisfied:

1. $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ with two operations $+_n$ and $\cdot_n$.
2. Addition of $x, y \in \mathbb{Z}_n$, denoted by $x +_n y$, is the unique element $z \in \mathbb{Z}_n$ s.t. $x + y \equiv z \pmod{n}$.
3. Multiplication of $x, y \in \mathbb{Z}_n$, denoted by $x \cdot_n y$, is the unique element $z \in \mathbb{Z}_n$ s.t. $x \cdot y \equiv z \pmod{n}$.
4. Additive identity 0 and multiplicative identity 1 exist.
5. For each element, its additive inverse exists.
6. Associative, commutative and distributive law holds.

In case of no ambiguity, the subscript n of operators under $\mathbb{Z}_n$ is omitted.

Finite ring of integers modulo n

Definition

$\mathbb{Z}_n$ is defined such that the following are all satisfied:

1. $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ with two operations $+_n$ and $\cdot_n$.
2. Addition of $x, y \in \mathbb{Z}_n$, denoted by $x +_n y$, is the unique element $z \in \mathbb{Z}_n$ s.t. $x + y \equiv z \pmod{n}$.
3. Multiplication of $x, y \in \mathbb{Z}_n$, denoted by $x \cdot_n y$, is the unique element $z \in \mathbb{Z}_n$ s.t. $x \cdot y \equiv z \pmod{n}$.
4. Additive identity 0 and multiplicative identity 1 exist.
5. For each element, its additive inverse exists.
6. Associative, commutative and distributive law holds.

In case of no ambiguity, the subscript n of operators under $\mathbb{Z}_n$ is omitted.

Finite ring of integers modulo n

Let $x \in \mathbb{Z}_n$ and the operations under $\mathbb{Z}_n$.

Definition

The *additive inverse* of x, denoted by $-x$, is the unique element $y \in \mathbb{Z}_p$ s.t. $x + y = 0$.

Let $k \in \mathbb{N}$,

Definition

The k-th power of $x \in \mathbb{Z}_n$ is defined as $x^k := \underbrace{x \cdot x \cdots x}_{k\text{-times}}$.

The zero-th power is defined as $x^0 := 1$.

Example

- Under $\mathbb{Z}_{10}$, $-2 = 8$ and $7^3 = 7 \cdot 7 \cdot 7 = 9 \cdot 7 = 3$.

Finite ring of integers modulo n

Let $x \in \mathbb{Z}_n$ be a non-zero element.

Definition

x is said to be a *unit* iff $\exists y \in \mathbb{Z}_n, xy = 1$.
y is called the *multiplicative inverse* of x and is denoted by x^{-1}.
$\mathbb{Z}_n^*$ is the *group of units of* $\mathbb{Z}_n$, *namely the set of units under* $\cdot$.

Example

Under $\mathbb{Z}_{11}$, $2^{-1} = 6$, since $2 \cdot 6 \equiv 12 \equiv 1 \pmod{11}$.

Fact

$\mathbb{Z}_p^*$ *is the cyclic group of the first* $p-1$ *integers.*
$\mathbb{Z}_n^*$ *has* $\phi(n)$ *elements, where* ϕ *is the Euler's phi function.*

Finite ring of integers modulo n

Let $x \in \mathbb{Z}_n$ be a non-zero element.

Definition

x is said to be a *unit* iff $\exists y \in \mathbb{Z}_n, xy = 1$.
y is called the *multiplicative inverse* of x and is denoted by x^{-1}.
$\mathbb{Z}_n^*$ is the *group of units of* $\mathbb{Z}_n$, *namely the set of units under* $\cdot$.

Example

Under $\mathbb{Z}_{11}$, $2^{-1} = 6$, since $2 \cdot 6 \equiv 12 \equiv 1 \pmod{11}$.

Fact

$\mathbb{Z}_p^*$ *is the cyclic group of the first* $p-1$ *integers.*
$\mathbb{Z}_n^*$ *has* $\phi(n)$ *elements, where* ϕ *is the Euler's phi function.*

Finite ring of integers modulo n

Let $x \in \mathbb{Z}_n$ be a non-zero element.

Definition

x is said to be a *unit* iff $\exists y \in \mathbb{Z}_n, xy = 1$.
y is called the *multiplicative inverse* of x and is denoted by x^{-1}.
$\mathbb{Z}_n^*$ is the *group of units of* $\mathbb{Z}_n$, *namely the set of units under* $\cdot$.

Example

Under $\mathbb{Z}_{11}$, $2^{-1} = 6$, since $2 \cdot 6 \equiv 12 \equiv 1 \pmod{11}$.

Fact

$\mathbb{Z}_p^*$ *is the cyclic group of the first* $p-1$ *integers.*
$\mathbb{Z}_n^*$ *has* $\phi(n)$ *elements, where* ϕ *is the Euler's phi function.*

Introduction – Solving linear equation in $\mathbb{Z}_n$

Warning

Unlike additive inverse, multiplicative inverse may not always exist. For example, $2 \in \mathbb{Z}_4$ has no multiplicative inverse.

- When does an element $x \in \mathbb{Z}_n$ have an multiplicative inverse?
- If it exists, how do we find it?

Consequence of Euclidean algorithm

For any given $k, m \in \mathbb{Z}_n$,

1. The equation $kx = m$ has solution(s) iff $\gcd(k, n) \mid m$.
2. The number of solutions is equal to $\gcd(k, n)$.

Therefore, $m \in \mathbb{Z}_n^* \iff \gcd(m, n) = 1$.

Introduction – Solving linear equation in $\mathbb{Z}_n$

Warning

Unlike additive inverse, multiplicative inverse may not always exist. For example, $2 \in \mathbb{Z}_4$ has no multiplicative inverse.

- When does an element $x \in \mathbb{Z}_n$ have an multiplicative inverse?
- If it exists, how do we find it?

Consequence of Euclidean algorithm

For any given $k, m \in \mathbb{Z}_n$,

1. The equation $kx = m$ has solution(s) iff $\gcd(k, n) \mid m$.
2. The number of solutions is equal to $\gcd(k, n)$.

Therefore, $m \in \mathbb{Z}_n^* \iff \gcd(m, n) = 1$.

Introduction – Solving linear equation in $\mathbb{Z}_n$

Warning

Unlike additive inverse, multiplicative inverse may not always exist. For example, $2 \in \mathbb{Z}_4$ has no multiplicative inverse.

- When does an element $x \in \mathbb{Z}_n$ have an multiplicative inverse?
- If it exists, how do we find it?

Consequence of Euclidean algorithm

For any given $k, m \in \mathbb{Z}_n$,

1. The equation $kx = m$ has solution(s) iff $\gcd(k, n) \mid m$.
2. The number of solutions is equal to $\gcd(k, n)$.

Therefore, $m \in \mathbb{Z}_n^* \iff \gcd(m, n) = 1$.

Introduction – Solving linear equation in $\mathbb{Z}_n$

Warning

Unlike additive inverse, multiplicative inverse may not always exist. For example, $2 \in \mathbb{Z}_4$ has no multiplicative inverse.

- When does an element $x \in \mathbb{Z}_n$ have an multiplicative inverse?
- If it exists, how do we find it?

Consequence of Euclidean algorithm

For any given $k, m \in \mathbb{Z}_n$,

1. The equation $kx = m$ has solution(s) iff $\gcd(k, n) \mid m$.
2. The number of solutions is equal to $\gcd(k, n)$.

Therefore, $m \in \mathbb{Z}_n^* \iff \gcd(m, n) = 1$.

Introduction – Solving linear equation in $\mathbb{Z}_n$

Warning

Unlike additive inverse, multiplicative inverse may not always exist. For example, $2 \in \mathbb{Z}_4$ has no multiplicative inverse.

- When does an element $x \in \mathbb{Z}_n$ have an multiplicative inverse?
- If it exists, how do we find it?

Consequence of Euclidean algorithm

For any given $k, m \in \mathbb{Z}_n$,

1. The equation $kx = m$ has solution(s) iff $\gcd(k, n) \mid m$.
2. The number of solutions is equal to $\gcd(k, n)$.

Therefore, $m \in \mathbb{Z}_n^* \iff \gcd(m, n) = 1$.

Finding square root or solving quadratic equation?

Problem

Given $m \in \mathbb{Z}_n$, can you solve the equation $x^2 = m$?

- Clearly, the equation $x^2 \equiv -1 \pmod 3$ has no solution.
- Is there an easy way to determine whether it has a solution? (This problem is important for our application in the sequel.)
- If a solution exists, anyway to solve it other than exhaustion? (This problem will not be discussed in the sequel.)

Finding square root or solving quadratic equation?

Problem

Given $m \in \mathbb{Z}_n$, can you solve the equation $x^2 = m$?

- Clearly, the equation $x^2 \equiv -1 \pmod{3}$ has no solution.
- Is there an easy way to determine whether it has a solution? (This problem is important for our application in the sequel.)
- If a solution exists, anyway to solve it other than exhaustion? (This problem will not be discussed in the sequel.)

Finding square root or solving quadratic equation?

Problem

Given $m \in \mathbb{Z}_n$, can you solve the equation $x^2 = m$?

- Clearly, the equation $x^2 \equiv -1 \pmod 3$ has no solution.
- Is there an easy way to determine whether it has a solution? (This problem is important for our application in the sequel.)
- If a solution exists, anyway to solve it other than exhaustion? (This problem will not be discussed in the sequel.)

Quadratic Residues

Let p be a prime,

Definition

The set of *quadratic residues modulo p*, $Q_p := \{x^2 : x \in \mathbb{Z}_p^*\}$.
The set of *quadratic nonresidues modulo p*, $\overline{Q_p} := \mathbb{Z}_p^* \setminus Q_p$.

Let $a \in \mathbb{Z}_p^*$,

Definition

a is said to be a *quadratic residue modulo p* iff $a \in Q_p$.
a is a *quadratic nonresidue modulo p* iff $a \in \overline{Q_p}$.

Quadratic Residues

Let p be a prime,

Definition

The set of *quadratic residues modulo p*, $Q_p := \left\{x^2 : x \in \mathbb{Z}_p^*\right\}$.
The set of *quadratic nonresidues modulo p*, $\overline{Q_p} := \mathbb{Z}_p^* \setminus Q_p$.

Let $a \in \mathbb{Z}_p^*$,

Definition

a is said to be a *quadratic residue modulo p* iff $a \in Q_p$.
a is a *quadratic nonresidue modulo p* iff $a \in \overline{Q_p}$.

Example

In $\mathbb{Z}_5$, -1 is a quadratic residue, since $3^2 = 4$.
$-1 \in \mathbb{Z}_7$ is a quadratic nonresidue, by exhaustion.
$2 \in \mathbb{Z}_7$ is a quadratic residue, since $3^2 = 2$.

Note

Since $\gcd(n, p) \neq 1 \implies \gcd(n, p) = p$.
The set $\mathbb{Z}_p$ is partitioned into three disjoint sets, $Q_p, \overline{Q_p}, \{0\}$.

Example

In $\mathbb{Z}_5$, -1 is a quadratic residue, since $3^2 = 4$.
$-1 \in \mathbb{Z}_7$ is a quadratic nonresidue, by exhaustion.
$2 \in \mathbb{Z}_7$ is a quadratic residue, since $3^2 = 2$.

Note

Since $\gcd(n, p) \neq 1 \implies \gcd(n, p) = p$.
The set $\mathbb{Z}_p$ is partitioned into three disjoint sets, $Q_p, \overline{Q_p}, \{0\}$.

Legendre Symbol

If $a \in \mathbb{Z}_p^*$, we define $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \in Q_p \\ -1 & \text{if } a \in \overline{Q_p} \end{cases}$

Define $\left(\frac{0}{p}\right) = 0$

If $a \geq p$, we define $\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$

Jacobi Symbol

Let $n = p_1^{d_1} \cdots p_m^{d_m}$ where all p_i's are pairwise distinct primes

If $a \in \mathbb{Z}_n^*$, we define $\left(\dfrac{a}{n}\right) = \displaystyle\prod_{k=1}^{m} \left(\dfrac{a}{p_k}\right)^{d_k}$

If $\gcd(a, n) \neq 1$, define $\left(\dfrac{a}{n}\right) = 0$.

If $a \geq n$, we define $\left(\dfrac{a}{n}\right) = \left(\dfrac{a \bmod n}{n}\right)$

Properties of Legendre Symbol

Let p and q be an odd prime, $p \neq q$ and $a, b \in \mathbb{Z}_p^*$.

1. $\left(\frac{a}{p}\right) = 1 \iff a \in Q_p$ and $\left(\frac{a}{p}\right) = -1 \iff a \in \overline{Q_p}$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. (*Euler's criterion*) $a^{(p-1)/2} \equiv 1 \pmod{p} \iff \left(\frac{a}{p}\right) = 1$
4. $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod{4}$
5. (Quadratic Reciprocity Law) $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$ and

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

Properties of Legendre Symbol

Let p and q be an odd prime, $p \neq q$ and $a, b \in \mathbb{Z}_p^*$.

1. $\left(\frac{a}{p}\right) = 1 \iff a \in Q_p$ and $\left(\frac{a}{p}\right) = -1 \iff a \in \overline{Q_p}$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. (*Euler's criterion*) $a^{(p-1)/2} \equiv 1 \pmod{p} \iff \left(\frac{a}{p}\right) = 1$
4. $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod{4}$
5. (Quadratic Reciprocity Law) $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$ and
$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

Properties of Legendre Symbol

Let p and q be an odd prime, $p \neq q$ and $a, b \in \mathbb{Z}_p^*$.

1. $\left(\dfrac{a}{p}\right) = 1 \iff a \in Q_p$ and $\left(\dfrac{a}{p}\right) = -1 \iff a \in \overline{Q_p}$
2. $\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$
3. (*Euler's criterion*) $a^{(p-1)/2} \equiv 1 \pmod{p} \iff \left(\dfrac{a}{p}\right) = 1$
4. $\left(\dfrac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod{4}$
5. (Quadratic Reciprocity Law) $\left(\dfrac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\dfrac{q}{p}\right)$ and
$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

Properties of Legendre Symbol

Let p and q be an odd prime, $p \neq q$ and $a, b \in \mathbb{Z}_p^*$.

1. $\left(\frac{a}{p}\right) = 1 \iff a \in Q_p$ and $\left(\frac{a}{p}\right) = -1 \iff a \in \overline{Q_p}$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. (*Euler's criterion*) $a^{(p-1)/2} \equiv 1 \pmod{p} \iff \left(\frac{a}{p}\right) = 1$
4. $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod{4}$
5. (Quadratic Reciprocity Law) $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$ and

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

Properties of Legendre Symbol

Let p and q be an odd prime, $p \neq q$ and $a, b \in \mathbb{Z}_p^*$.

1. $\left(\frac{a}{p}\right) = 1 \iff a \in Q_p$ and $\left(\frac{a}{p}\right) = -1 \iff a \in \overline{Q_p}$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. (*Euler's criterion*) $a^{(p-1)/2} \equiv 1 \pmod{p} \iff \left(\frac{a}{p}\right) = 1$
4. $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod{4}$
5. (Quadratic Reciprocity Law) $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$ and $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$

Properties of Legendre Symbol

Let p and q be an odd prime, $p \neq q$ and $a, b \in \mathbb{Z}_p^*$.

1. $\left(\frac{a}{p}\right) = 1 \iff a \in Q_p$ and $\left(\frac{a}{p}\right) = -1 \iff a \in \overline{Q_p}$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. (*Euler's criterion*) $a^{(p-1)/2} \equiv 1 \pmod{p} \iff \left(\frac{a}{p}\right) = 1$
4. $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod{4}$
5. (Quadratic Reciprocity Law) $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$ and

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

Properties of Jacobi Symbol

Let $a, b, m, n \in \mathbb{N}$

1. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$
2. $\left(\frac{1}{n}\right) = 1$
3. $\left(\frac{ab}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
4. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$
5. Quadratic Reciprocity Law still holds.

Properties of Jacobi Symbol

Let $a, b, m, n \in \mathbb{N}$

1. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$
2. $\left(\frac{1}{n}\right) = 1$
3. $\left(\frac{ab}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
4. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$
5. Quadratic Reciprocity Law still holds.

Properties of Jacobi Symbol

Let $a, b, m, n \in \mathbb{N}$

1. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$
2. $\left(\frac{1}{n}\right) = 1$
3. $\left(\frac{ab}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
4. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$
5. Quadratic Reciprocity Law still holds.

Properties of Jacobi Symbol

Let $a, b, m, n \in \mathbb{N}$

1. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$
2. $\left(\frac{1}{n}\right) = 1$
3. $\left(\frac{ab}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
4. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$
5. Quadratic Reciprocity Law still holds.

Properties of Jacobi Symbol

Let $a, b, m, n \in \mathbb{N}$

1. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$
2. $\left(\frac{1}{n}\right) = 1$
3. $\left(\frac{ab}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
4. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$
5. Quadratic Reciprocity Law still holds.

Example

Example

Is 69 a quadratic residue modulo 389 (prime)?

$$\left(\frac{69}{389}\right) = \left(\frac{3}{389}\right)\left(\frac{23}{389}\right) = \left(\frac{389}{3}\right)\left(\frac{389}{23}\right) = \left(\frac{2}{3}\right)\left(\frac{21}{23}\right)$$

$$= (-1)\left(\frac{-2}{23}\right) = (-1)(-1)\left(\frac{2}{23}\right) = 1$$

Be careful

The Jacobi symbol cannot give information whether a number is quadratic residue or not.

By definition $\left(\frac{8}{9}\right) = \left(\frac{8}{3}\right)^2 = \left(\frac{2}{3}\right)^2 = 1$.

However, there is no $x \in \mathbb{Z}_9$ such that $x^2 = 8$.

The Quadratic Residuosity Problem

Definition: Given an odd integer n and $a \in J_n$ (J_n is the set of all $a \in \mathbb{Z}_n^*$ having Jacobi symbol $+1$), decide whether or not a is quadratic residue modulo n.

Comments: If n is a prime, the quadratic residuosity problem is easy, as there is a polynomial time algorithm for the computation of $\left(\frac{a}{n}\right)$, which can determine whether a is a quadratic residue modulo n.

It is suspected to be a hard problem when n is an odd composite integer unless the factorization of n is known. Hence, the difficulty of this problem depends that of the factorization problem.

Setup

Private parameters:

- Two prime numbers p, q
  - $p \equiv q \equiv 3 \pmod 4$
  - Only known to the Private Key Generator (PKG)

Public parameters:

- $n = p \cdot q$
- $H : \{0,1\}^* \to J_n$, where $J_n = \left\{ x \in \mathbb{Z}_n^* : \left(\frac{x}{n}\right) = 1 \right\}$.

Example

- Let $p = 7$ and $q = 11$ such that $p, q \equiv 3 \pmod 4$
- $n = p \cdot q = 77$ and $|\mathbb{Z}_n^*| = 60$
- $\mathbb{Z}_n^* = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 20, 23, 24, 25, 26, 27, 29, 30, 31, 32, 34, 36, 37, 38, 39, 40, 41, 43, 45, 46, 47, 48, 50, 51, 52, 53, 54, 57, 58, 59, 60, 61, 62, 64, 65, 67, 68, 69, 71, 72, 73, 74, 75, 76\}$
- $J_n = \{i \in \mathbb{Z}_n^* : \left(\frac{i}{n}\right) = +1\} = \{1, 4, 6, 9, 10, 13, 15, 16, 17, 19, 23, 24, 25, 36, 37, 40, 41, 52, 53, 54, 58, 60, 61, 62, 64, 67, 68, 71, 73, 76\}$

Extraction of the Private Key

User contacts PKG through secure channel for his/her private key $\rightarrow$ PKG extracts this key from knowledge of the user's identity and its privately-known parameters p and q.

1. Compute $H(ID) = a$, such that $\left(\frac{a}{n}\right) = 1$
2. Compute $r = a^{\frac{(n+5)-(p+q)}{8}} \pmod{n}$, where r is the private key of the user.
   r must satisfy $r^2 \equiv \pm a \pmod{n}$ depending on which of a or $-a$ is a square modulo n. (See the proof in the next page.)
3. Transmit r, the private key, to the user.

Proof: a or $-a$ is a quadratic residue modulo n

$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$, since $\left(\frac{a}{n}\right) = 1$, there are two cases possible.

- Case 1: $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$
  Thus a is a quadratic residue modulo both p and q. This means that a is also a quadratic residue modulo n.
- Case 2: $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$
  Now $\left(\frac{-a}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{-1}{p}\right) = (-1)(-1) = 1.$
  Hence, $-a \in Q_p$ Similarly, $-a \in Q_q$.
  This means that $-a$ is also a quadratic residue modulo n.

Example

- $p = 7, q = 11, n = 77$
- Consider an arbitrary ID such that $H(ID) = 4$
- The PKG computes

$$r = a^{\frac{(n+5)-(p+q)}{8}} \bmod n \equiv 4^{\frac{(77+5)-(7+11)}{8}} \equiv 4^8 = 9 \pmod{77}$$

- Here, $r^2 = 9^2 \equiv 4 \pmod{77}$

Encryption

Given an m-bit plaintext message string $M = (x_1 \cdots x_m)$, and a secure public Hash function $H()$

1. Encode each bit x_i of the m-bit plaintext message string $M = (x_1 \cdots x_m)$ as either $+1$ or -1
2. Compute $H(ID) = a$, such that $\left(\frac{a}{n}\right) = 1$
3. Choose values t_1, t_2 at random modulo n, such that $t_1 \neq t_2$ and $\left(\frac{t_1}{n}\right) = \left(\frac{t_2}{n}\right) = x_i$.
4. Compute $s_{i,1} = (t_1 + at_1^{-1}) \bmod n$ and $s_{i,2} = (t_2 - at_2^{-1}) \bmod n$
5. Use $\langle s_{i,1}, s_{i,2} \rangle$ to represent the plaintext bit x_i

Example

- Consider plaintext message string $M = (1, 0)$ encoded as $(+1, -1)$
- First bit, $x_1 = +1$

  (To simplified this example, only $s_{1,1}$ is computed)

  - Choose $t = 10$ since $\left(\frac{10}{77}\right) = 1$
  - Compute $s_{1,1} = (t + at^{-1}) \bmod n \equiv 10 + 4 \cdot 10^{-1} \equiv 10 + 4 \cdot 54 \equiv 72 \pmod{77}$
- Second bit, $x_2 = -1$

  (To simplified this example, only $s_{2,1}$ is computed)

  - Choose $t = 20$ since $\left(\frac{20}{77}\right) = -1$
  - Compute $s_{2,1} \equiv (t + at^{-1}) \bmod n = 20 + 4 \cdot 20^{-1} \equiv 20 + 4 \cdot 27 \equiv 51 \pmod{77}$

Decryption

Given the private key r, and the encrypted message.
If $r^2 \equiv a \pmod{n}$, set $y = s_{i,1}$. Otherwise $y = s_{i,2}$.

- The plaintext bit x_i can be recovers from $(y + 2r) \bmod n$.
- $x_i = \left(\frac{y+2r}{n}\right)$
- Decryption will fail iff
$$\left(\frac{1+rt^{-1}}{n}\right) = 0 \iff \gcd\left(1+rt^{-1}, n\right) \neq 1,$$
where $t = t_1$ if $r^2 \equiv a \pmod{n}$ and $t = t_2$ otherwise. Since p and q are fairly large primes, the probability of such an event happening is quite low.

Remark: See the next slide for details.

Proof of the Correctness of Decryption

We assume that $r^2 \equiv a \pmod{n}$, and have then

$$\begin{aligned}
\left(\frac{y+2r}{n}\right) &= \left(\frac{s_{i,1}+2r}{n}\right) = \left(\frac{t_1 + at_1^{-1} + 2r}{n}\right) \\
&= \left(\frac{t_1(1 + r^2 t_1^{-2} + 2rt_1^{-1})}{n}\right) = \left(\frac{t_1}{n}\right)\left(\frac{(1+rt_1^{-1})^2}{n}\right) \\
&= \left(\frac{t_1}{n}\right) = x_i \qquad \text{if } \left(\frac{(1+rt_1^{-1})^2}{n}\right) \neq 0.
\end{aligned}$$

The proof for the other case is similar and omitted here. That is the case that $r^2 \equiv -a \pmod{n}$.

Example of Successful Decryption

- Given $s_{1,1} = 72$
  - Compute $s_{1,1} + 2r \equiv 72 + 2 \cdot 9 \equiv 13 \pmod{77}$
  - Calculate Jacobi symbol $\left(\dfrac{s+2r}{n}\right) = \left(\dfrac{13}{77}\right) = 1 = x_1$
- Given $s_{2,1} = 51$
  - Compute $s_{2,1} + 2r \equiv 51 + 2 \cdot 9 \equiv 69 \pmod{77}$
  - Calculate Jacobi symbol $\left(\dfrac{s+2r}{n}\right) = \left(\dfrac{69}{77}\right) = -1 = x_1$

Example of Unsuccessful Decryption

- At encryption,
  - For second bit, if choose $t = 12$ since $\left(\frac{12}{77}\right) = -1$
  - Compute $s_{2,1} \equiv t + at^{-1} \equiv 12 + 4 \cdot 12^{-1} \equiv 12 + 4 \cdot 45 \equiv 38 \pmod{77}$
- At decryption,
  - Compute $s_{2,1} + 2r \equiv 38 + 2 \cdot 9 = 56 \pmod{77}$
  - Calculate Jacobi symbol $\left(\frac{s+2r}{n}\right) = \left(\frac{56}{77}\right) = 0 \neq x_1$

Security of Cock's IBE

It can be shown that breaking the scheme is equivalent to solving the quadratic residuosity problem, which is suspected to be hard when the factorization of n is unknown.

A proof of this can be found in the second reference listed in the last slide.

Practical Aspects

- Message Inflation
  - $\langle x_i \rangle \longrightarrow \langle s_{i,1}, s_{i,2} \rangle$
  - Single bit of the message $\longrightarrow$ two elements of the group $\mathbb{Z}_n^*$
  - Message inflation by a factor of $2 \log_2 n$
  - Much more bandwidth needed which may not be acceptable.
  - Thus, it is only suitable for small data packets like a session key.
- Sending the private key from the PKG to the decrypting party requires a secure channel.
- Authenticating the decrypting party may be a bottleneck in the system.

References

- I. Niven, H. S. Zuckerman, H. L. Montgomery, In Introduction to the Theory of Numbers, the Fifth Edition, John Wiley, New York, 1991.
- L. Martin, Introduction to Identity Based Encryption, Artech House Publishers; 1 edition (January 2008).
- J. Baek, J. Newmarch, R. Safavi-Naini and W. Susilo, A Survey of Identity-Based Cryptography, Proc. of the 10th Annual Conference for Australian Unix User's Group (AUUG 2004), pp. 95-102, 2004.