An Identity Based Encryption Scheme based on Quadratic Residues

Pei-Chuan Tsai

Department of Computer Science, National Chiao Tung University

Sep. 04, 2007

Outline

Legendre symbol

- **Definition**
  If p is an odd prime and $a \in \mathbb{Z}$, then the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a \\ 1, & \text{if } \exists k \in \mathbb{Z} \text{ such that } k^2 \equiv a \pmod{p} \\ -1, & \text{if } a \text{ is not a square modulo } p \end{cases}$$

- **Example**:
  In $\mathbb{Z}_5$:

$x \pmod{5}$	0	1	2	3	4
$x^2 \pmod{5}$	0	1	4	4	1

Then

$$\left(\frac{0}{5}\right) = 0, \quad \left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1, \quad \left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1$$

Jacobi symbol

- Definition
  Let $n > 0$ be odd and let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the prime factorization of n.
  For any integer a, the Jacobi symbol

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}$$

  where the symbols on the right are all Legendre symbols.

- Example:

1. $$\left(\frac{8}{15}\right) = \left(\frac{8}{3}\right)\left(\frac{8}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{3}{5}\right) = (-1)(-1) = 1$$

2. $$\left(\frac{4}{15}\right) = \left(\frac{4}{3}\right)\left(\frac{4}{5}\right) = (1)(1) = 1$$

Compute Jacobi symbol

- We can compute Jacobi symbol without knowing the factorization of n by using the following properties:
  1. $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$, if $a = b$ mod n
  2. $\left(\frac{1}{n}\right) = 1$ and $\left(\frac{0}{n}\right) = 0$
  3. $\left(\frac{2m}{n}\right) = \left(\frac{m}{n}\right)$, if $n = \pm 1$ mod 8 . Otherwise, $\left(\frac{2m}{n}\right) = -\left(\frac{m}{n}\right)$
  4. If m, n are both odd, then $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$ unless both m and n are congruent to 3 mod 4, in which case $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$

- Example:
  1. $$\left(\frac{8}{15}\right) = \left(\frac{4}{15}\right) = \left(\frac{2}{15}\right) = \left(\frac{1}{15}\right) = 1$$
  2. $$\left(\frac{11}{15}\right) = -\left(\frac{15}{11}\right) = -\left(\frac{4}{11}\right) = \left(\frac{2}{11}\right) = -\left(\frac{1}{15}\right) = -1$$

Quadratic residues

- Definition
  A number q is called a quadratic residue modulo n if there exists an integer x such that

$$x^2 \equiv q \pmod{n}$$

  Otherwise, q is called a quadratic non-residue.

- Example:
  In $\mathbb{Z}_5$

$x \pmod{5}$	0	1	2	3	4
$x^2 \pmod{5}$	0	1	4	4	1

  Then $0, 1, 4$ are quadratic residues and $2, 3$ are quadratic non-residues.

Cocks's IBE Scheme

Pei-Chuan Tsai

Department of Computer Science, National Chiao Tung University

Sep. 04, 2007

Introduction

- Proposed by Clifford Cocks in 2001.
- Based on the hard problem of composite quadratic residues.
- It is currently the only IBE scheme which does not use bilinear pairing.
- Disadvantage:
  Encrypt each single bit

The hard problem - (1/2)

- Let $n = p \times q$ where p, q are odd primes and let

$$\mathbf{QR}(n) = \left\{ x \mid \left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = 1 \right\}$$

$$\widetilde{\mathbf{QR}}(n) = \left\{ x \mid \left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = -1 \right\}$$

Example:
Since

$$\left(\frac{8}{15}\right) = 1,\ \left(\frac{8}{3}\right) = \left(\frac{8}{5}\right) = -1; \quad \left(\frac{4}{15}\right) = 1,\ \left(\frac{4}{3}\right) = \left(\frac{4}{5}\right) = 1$$

Then $8 \in \widetilde{\mathbf{QR}}(n)$ and $4 \in \mathbf{QR}(n)$

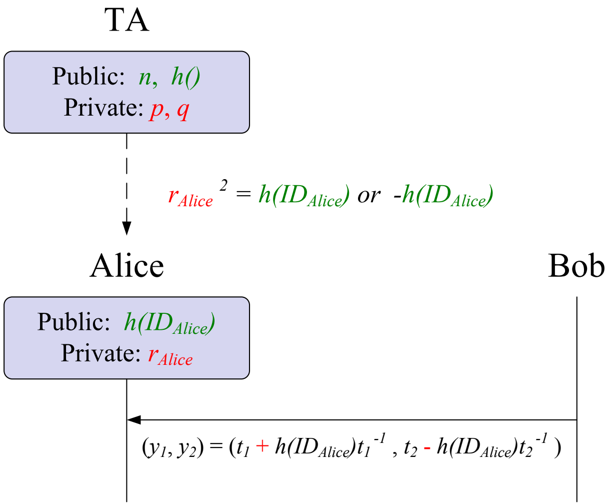
The hard problem - (2/2)

- Composite quadratic residue problem:

  Given $\left(\frac{x}{n}\right) = 1$ (p, q are unknown) , it is hard to decide whether

$$x \in \mathbf{QR}(n) \quad \text{or} \quad x \in \widetilde{\mathbf{QR}}(n)$$

Cocks's IBE scheme



System parameters

- Public parameters:
  1. number n (where $n = p \times q$)
  2. hash function $h : \{0, 1\}^* \rightarrow \mathbb{Z}_n$, such that

$$\left(\frac{h(ID)}{n}\right) = 1, \quad \text{for all ID}$$

- Private parameters:
  1. odd primes p , q

Extraction

- When an user identifies himself to TA, TA extracts the key of the user as following:

  Assume the ID of the user is ID_U

  - Public key:
    $K_U^{pub} = h(ID_U)$, where

$$\left(\frac{h(ID_U)}{n}\right) = 1$$

  - Private key:
    $K_U^{priv} = r_U$, where

$$r_U^2 = \begin{cases} h(ID_U) \text{ mod } n \ , & \text{if } h(ID_U) \in \mathbf{QR}(n) \\ -h(ID_U) \text{ mod } n \ , & \text{if } h(ID_U) \in \widetilde{\mathbf{QR}}(n) \end{cases}$$

Encryption

- Assume Bob wants to send message to Alice, he sends to Alice each bit as follows:

  0. For each single bit x of the message, code it as $+1$ or -1
  1. For $x \in \{+1, -1\}$, choose random number $t_1, t_2 \in \mathbb{Z}_n$ where

  $$\left(\frac{t_1}{n}\right) = \left(\frac{t_2}{n}\right) = x$$

  2. Compute

  $$\begin{aligned} y_1 &= t_1 + h(ID_{Alice}) \cdot t_1^{-1} \mod n \\ y_2 &= t_2 - h(ID_{Alice}) \cdot t_2^{-1} \mod n \end{aligned}$$

  3. Send (y_1, y_2) to Alice.

Decryption

- When Alice receives (y_1, y_2), she can recover x as follows:
  1. If ${r_{Alice}}^2 = h(ID_{Alice})$, set $y = y_1$.
     Otherwise, set $y = y_2$.
  2. Compute
$$x = \left(\frac{y + 2r_{Alice}}{n}\right)$$

- Verify: (assume ${r_{Alice}}^2 = h(ID_{Alice})$)

$$\begin{aligned}
\left(\frac{y+2r_{Alice}}{n}\right) &= \left(\frac{y_1+2r_{Alice}}{n}\right) = \left(\frac{t_1+h(ID_{Alice})\cdot t_1^{-1}+2r_{Alice}}{n}\right) \\
&= \left(\frac{t_1\left(1+{r_{Alice}}^2\cdot t_1^{-2}+2r_{Alice}\cdot t_1^{-1}\right)}{n}\right) = \left(\frac{t_1\left(1+r_{Alice}\cdot t_1^{-1}\right)^2}{n}\right) \\
&= \left(\frac{t_1}{n}\right)\cdot\left(\frac{\left(1+r_{Alice}\cdot t_1^{-1}\right)^2}{n}\right) = \left(\frac{t_1}{n}\right) = x
\end{aligned}$$

Security proof - (1/3)

- It can be proved that if $y = y_1$, then y_2 provides no information about x $(= \left(\frac{t_2}{n}\right)$) , vice versa.

  Proof:

  Suppose that ${r_{Alice}}^2 = h(ID_{Alice})$

$$
\begin{array}{lll}
 & y_2 = t_2 - h(ID_{Alice}) \cdot t_2^{-1} & \bmod n \\
\rightarrow & t_2^2 - y_2 t_2 - h(ID_{Alice}) = 0 & \bmod n \\
\rightarrow & t_2^2 - y_2 t_2 - h(ID_{Alice}) = 0 & \bmod p \text{ and } \quad (1) \\
 & t_2^2 - y_2 t_2 - h(ID_{Alice}) = 0 & \bmod q \qquad\quad (2)
\end{array}
$$

  Let t_{21}, t_{22} be the roots of equation (1), and t_{23}, t_{24} be the roots of equation (2).

  $\rightarrow$ There will be 4 possible values of t_2

Security proof - (2/3)

- Proof: (continue)

  Since

$$t_{21} \cdot t_{22} = -h(ID_{Alice}) \mod p$$
$$t_{23} \cdot t_{24} = -h(ID_{Alice}) \mod q$$

  Then

$$\left(\frac{t_{21} \cdot t_{22}}{p}\right) = \left(\frac{-h(ID_{Alice})}{p}\right) = -1 = \left(\frac{t_{21}}{p}\right)\left(\frac{t_{22}}{p}\right)$$

$$\left(\frac{t_{23} \cdot t_{24}}{q}\right) = \left(\frac{-h(ID_{Alice})}{q}\right) = -1 = \left(\frac{t_{23}}{q}\right)\left(\frac{t_{24}}{q}\right)$$

  So

$$x = \left(\frac{t_2}{n}\right) = \begin{cases} +1, & \text{possibility} = 1/2 \\ -1, & \text{possibility} = 1/2 \end{cases}$$

Security proof - (3/3)

- Assume someone can recover message x by using n, $h(ID)$, (y_1, y_2) , then we can solve the composite quadratic residue problem.
  1. Let the decrypt function be $F(n, h(ID), (y_1, y_2))$
  2. We can choose $x = +1$ (or -1), compute corresponding y_1 and give y_2 randomly.
  3. See if the output is correct or not, then we can decide whether $h(ID) \in \mathbf{QR}(n)$ or not.