Composite residuosity and its application to cryptography

Tomoko Adachi
Department of Information Sciences, Toho University
2-2-1 Miyama, Funabashi, Chiba, 274-8510, Japan
E-mail: adachi@is.sci.toho-u.ac.jp

Abstract It is well-known that a quadratic residue is adopted to public key cryptosystem, for example, we show Rabin cryptosystem. In this paper, we describe a composite residue and its application to cryptography.

1. Introduction

At first, we review a quadratic residue and its application to cryptography. Suppose $p$ is an odd prime and $a$ is an integer. $a$ is defined to be a quadratic residue modulo $p$ if $a \not\equiv 0 \pmod{p}$ and the congruence $y^2 \equiv a \pmod{p}$ has a solution $y$ where nonnegative $y$ is less than $n$. It is well-known that a quadratic residue is adopted to public key cryptosystems. For example, we show Rabin Cryptosystem [5]. Let $n = pq$, where $p$ and $q$ are primes, and $p, q \equiv 3 \pmod{4}$. The value $n$ is the public key, while $p$ and $q$ are the private key. For a plaintext $m < n$, we define the ciphertext $c = m^2 \pmod{n}$. Quadratic residue is adopted in a trapdoor mechanism of this public key cryptosystem. As well, the public key cryptosystem by Kurosawa et. al. [2] also utilized a quadratic residue. Moreover, the public key cryptosystem by Naccache and Stern [3] utilized a higher residue. Further, the public key cryptosystem by Paillier [4] utilized a composite residue. In this paper, we describe a composite residue and its application to cryptography.

2. Composite residue

In this section, we describe a definition of a composite residue. A composite residue, that is, an $n$-th residue is introduced by Benaloh [1].

We set $n = pq$ where $p$ and $q$ are large primes. In this case, we denote by $\phi(n) = (p - 1)(q - 1)$ the Euler's function. And we denote by $\lambda(n) = \text{lcm}(p - 1, q - 1)$ the least common multiple of $p - 1$ and $q - 1$. We adopt $\lambda$ instead of $\lambda(n)$ for visual comfort.
We denote by $Z_{n^2}$ a residue class ring modulo $n^2$. And We denote by $Z^*_{n^2}$ its invertible element set. The set $Z^*_{n^2}$ is a multiplicative subgroup of $Z_{n^2}$ of order $\phi(n^2) = n\phi(n) = pq(p-1)(q-1)$.

For any $w \in Z^*_{n^2}$, the following equations hold,

$$w^\lambda = 1 \pmod{n},$$
$$w^{n\lambda} = 1 \pmod{n^2}.$$ 

**Definition 2.1.** A number $z$ is said to be an $n$-th residue modulo $n^2$ if there exists a number $y \in Z^*_{n^2}$, such that

$$z = y^n \pmod{n^2}.$$ 

For example, we suppose $p = 3$, $q = 5$, that is, $n = 15$. Then we obtain $\phi(n) = 8$, $\lambda = 4$, $\phi(n^2) = 120$, and that every element of the set $\{1, 26, 82, 107, 118, 143, 199, 224\}$ an $n$-th residue modulo $n^2$.

**3. Property of Composite residue**

In this section, we describe some properties of an $n$-th residue. We set $n = pq$ where $p$ and $q$ are large primes.

The set of $n$-th residues is a multiplicative subgroup of $Z^*_{n^2}$ of order $\phi(n)$. The problem of deciding $n$-th residuosity, that is, distinguishing $n$-th residues from non $n$-th residues will be denoted by CR[$n$]. As for prime residuosity, deciding $n$-th residuosity, is believed to be computationally hard.

Let $g$ be some element of $Z^*_{n^2}$ and denote by $\varepsilon_g$ the integer-valued function defined by

$$Z_n \times Z^*_n \rightarrow Z^*_{n^2}$$

$$(x, y) \mapsto g^x y^n \pmod{n^2}.$$ 

Here, depending on $g$, $\varepsilon_g$ may feature an interesting property such as the following lemma.

**Lemma 3.1.** If the order of $g$ is a nonzero multiple of $n$ then $\varepsilon_g$ is bijection.
We denote by $\mathcal{B}_\alpha \subset \mathbb{Z}_{n^2}^*$ the set of elements of order $n\alpha$ and by $\mathcal{B}$ their disjoint union for $\alpha = 1, \cdots, \lambda$.

In the case of $n = 15$, we obtain the following sets as $\mathcal{B}_\alpha$ and $\mathcal{B}$:

\[\mathcal{B}_1 = \{16, 31, 46, 61, 76, 91, 106, 121, 136, 151, 166, 181, 196, 211\},\]
\[\mathcal{B}_2 = \{14, 29, 44, 59, 74, 89, 104, 119, 134, 149, 164, 179, 194, 209\},\]
\[\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_4.\]

Here, we verify that $\mathcal{B}_i \cap \mathcal{B}_j = \emptyset$ for $i, j (i \neq j)$.

**Definition 3.2.** Assume that $g \in \mathcal{B}$. For $w \in \mathbb{Z}_{n^2}^*$, we call $n$-th residuosity class of $w$ with respect to $g$ the unique integer $x \in \mathbb{Z}_n$ for which there exists $y \in \mathbb{Z}_n^*$ such that $\epsilon_g(x, y) = w$.

Adopting Benaloh's notations [1], the class of $w$ is denoted $[w]_g$. It is worthwhile noticing the following property.

**Lemma 3.2.** $[w]_g = 0$ if and only if $w$ is an $n$-th residue modulo $n^2$. Furthermore,

$$\forall w_1, w_2 \in \mathbb{Z}_{n^2}^* \quad [w_1 w_2]_g = [w_1]_g + [w_2]_g \pmod{n}$$

that is, the class function $w \mapsto [w]_g$ is a homomorphism from $(\mathbb{Z}_{n^2}^*, \times)$ to $(\mathbb{Z}_n, +)$ for any $g \in \mathcal{B}$.

By Lemma 3.2, it can easily be shown that, for any $w \in \mathbb{Z}_{n^2}^*$ and $g_1, g_2 \in \mathcal{B}$, we have

$$[w]_{g_1} = [w]_{g_2} [g_2]_{g_1} \pmod{n},$$

which yields $[g_1]_{g_2} = [g_2]_{g_1}^{-1} \pmod{n}$ and thus $[g_2]_{g_1}$ is invertible modulo $n$.

The set

$$S_n = \{u < n^2 \mid u = 1 \pmod{n}\}$$

is a multiplicative subgroup of integers modulo $n^2$ over which the function $L$ such that

$$\forall u \in S_n \quad L(u) = \frac{u - 1}{n}$$
is clearly well-defined.

**Lemma 3.3.** For any $w \in Z_{n^{2}}^{*}$, there holds as follows,

\[ L(w^\lambda \mod n^2) = \lambda[[w]]_{1+n} \mod n. \]

By Lemma 3.3, for any $g \in B$ and $w \in Z_{n^2}^*$, we can compute

\[ \frac{L(w^\lambda \mod n^2)}{L(g^\lambda \mod n^2)} = \frac{\lambda[[w]]_{1+n}}{\lambda[[g]]_{1+n}} \mod n. \]

By virtue of Equation 3.1, for any $g \in B$ and $w \in Z_{n^2}^*$, we can compute

\[ \frac{[[w]]_{1+n}}{[[g]]_{1+n}} = [[w]]_g \mod n. \]

Therefore, for any $g \in B$ and $w \in Z_{n^2}^*$, we can compute

\[ \frac{L(w^\lambda \mod n^2)}{L(g^\lambda \mod n^2)} = [[w]]_g \mod n. \quad (3.2) \]

4. Application to cryptography

Now, we describe the public key cryptosystem based on the $n$-th residuosity class problem.

Set $n = pq$ and randomly select a base $g \in B$. We review that $\epsilon_g$ be the function defined by

\[ Z_n \times Z_n^* \rightarrow Z_{n^2}^* \]

\[ (x, y) \mapsto \epsilon_g(x, y) = g^xy^n \mod n^2. \quad (4.1) \]

For the plaintext $x$, we employ this function $\epsilon_g$ as an encryption function.

Moreover, we review that we define the function $L$ as follows:

\[ S_n = \{u < n^2 \mid u \equiv 1 \mod n\} \rightarrow Z_n \]

\[ u \mapsto L(u) = \frac{u-1}{n}. \quad (4.2) \]

For the ciphertext $c = \epsilon_g(x, y)$, we employ the rate of these two functions $L(c^\lambda)$ and $L(g^\lambda)$ as an decryption function.

**Theorem 4.1.** We set $n = pq$ and $\lambda = lcm(p-1,q-1)$. For any $g \in B$, we obtain public-key cryptosystem as public keys $(n, g)$ and private keys $(p, q)$. For a plaintext $m < n$, we select a random $r < n$, and compute
the ciphertext $c$ by Equation 4.3. For a ciphertext $c < n^2$, we compute the plaintext $m$ by Equation 4.4.

$$c = g^m r^n \pmod{n^2}, \quad \text{(4.3)}$$

$$m = \frac{L(c^\lambda \pmod{n^2})}{L(g^\lambda \pmod{n^2})} \pmod{n}. \quad \text{(4.4)}$$

For example, we suppose $n = 15$ and $g = 14$. Then, for a plaintext $m = 3$ and a random $r = 4$, we compute the ciphertext $c = 206$ by Equation 4.3. For a ciphertext $c = 206$, we compute the plaintext

$$m = \frac{L(206^4 \pmod{n^2})}{L(14^4 \pmod{n^2})} = \frac{L(46)}{L(166)} \pmod{n}$$

by Equation 4.4. Here, we compute

$$L(46) = \frac{46 - 1}{15} = 3 \pmod{n}$$

$$L(166) = \frac{166 - 1}{15} = 11 \pmod{n}$$

by Equation 4.2. Therefore, we can obtain

$$m = \frac{L(46)}{L(166)} = \frac{3}{11} = 3. \pmod{n}$$

For $n = pq$, we obtain the public key cryptosystem based on the $n$-th residuosity class problem.

References


