1988 Symp. on Cryptography & Information Security, Japan, Feb. 22-24 1988

Cryptographic Applications of γ^{th}-Residuosity Problem with γ an Odd Integer

Yuliang Zheng

Tsutomu Matsumoto

Hideki Imai

Division of Electrical and Computer Engineering

Yokohama National University

156 Tokiwadai, Hodogaya, Yokohama, 240 Japan

Abstract Let γ and n be positive integers. An integer z with $\gcd(z,n)=1$ is called a γ^{th}-residue $\bmod n$ if there exists an integer x such that $z \equiv x^{\gamma} \pmod{n}$, or a γ^{th}-nonresidue $\bmod n$ if there doesn't exist such an x. Denote by Z_n^* the set of integers relatively prime to n between 0 and n. The problem of determining whether or not a randomly selected element $z \in Z_n^*$ is a γ^{th}-residue $\bmod n$ is called the γ^{th}-*Residuosity Problem* (γ^{th}-RP), and appears to be intractable when n is a composite integer whose factorization is unknown. In this paper, we explore some important properties of γ^{th}-RP for the case where γ is an odd integer greater than 2, and discuss its applications to cryptography. Based on the difficulty of γ^{th}-RP, we generalize the Goldwasser-Micali bit-by-bit probabilistic encryption to a block-by-block probabilistic one, and propose a direct protocol for the dice casting problem over a network. This problem is a general one which includes the well-studied coin flipping problem.

1. Introduction

Let γ and n be positive integers. An integer z with $\gcd(z,n) = 1$ is called a γ^{th}-residue mod$n$ if there exists an integer x such that $z \equiv x^\gamma \pmod n$, or a γ^{th}-nonresidue mod$n$ if there doesn't exist such an x. Denote by Z_n^* the set of integers relatively prime to n between 0 and n. The *γ^{th}-Residuosity Problem* (γ^{th}-RP) is characterized as: Given a randomly selected element $z \in Z_n^*$, determine whether or not z is a γ^{th}-residue mod$n$.

When n is a prime, the problem is readily solvable [9]. However, when n is a composite integer and the factorization of n is unknown, the problem seems to be very difficult [1].

If γ is fixed to 2, the problem is called *Quadratic Residuosity Problem*, which plays central roles in many cryptographic protocols [5,6].

In this paper, we focus our attention on the case when n is the product of large primes and γ is an odd integer greater than 2. We explore some important properties of γ^{th}-RP, and discuss its applications to cryptography. The main results are summarized as follows:

⟨1⟩ Some properties of γ^{th}-RP are discussed (Sections 2, 3). Of particular interest is Theorem 3 (Section 2), since a corollary of it states that if γ and n satisfy the conditions of $n = pq = (2\gamma p' + 1)(2q' + 1)$ and $\gcd(\gamma, q') = 1$, where γ is an odd integer greater than 2 and p, q, p', q' are all primes, then Z_n^* is divided into γ subsets of equal size according to the *class-indices* of elements in Z_n^*.

⟨2⟩ When γ is small, the Goldwasser-Micali bit-by-bit probabilistic encryption (the GM encryption, for short) [6] is generalized to a block-by-block probabilistic one (Section 4). Our generalized encryption achieves Shannon's *perfect secrecy* when the power of an adversary is limited to polynomial time, and is more efficient than the GM encryption. The generalized encryption is especially preferable to the GM encryption in environments (such as the transmission of secret English files) where encrypting a file *letter by letter* is more natural than doing it *bit by bit*.

⟨3⟩ A *direct* dice casting protocol is proposed (Section 5). The well-studied problem — coin flipping is a special case of the dice casting problem. A dice casting protocol can be constructed from a coin flipping protocol by repeating the latter several times. However, such a protocol is too inefficient, and hence of little practical use. To the knowledge of the authors, no *direct* dice casting protocol has yet been published.

2. Some Number-Theoretic Results

In this section, after introducing some basic concepts in Number Theory, we will investigate the structure of Z_n^* for a special kind of composite integers n.

Let n be the product of odd prime powers, i.e., $n = n_1 n_2 \cdots n_t$, where for each $1 \le i \le t$, $n_i = p_i^{\alpha_i}$, p_i is an odd prime, and $p_i \ne p_j$ when $i \ne j$. Denote by Z_n^* the set of integers relatively prime to n between 0 and n, and by $\phi(n)$ the number of elements in Z_n^*. From elementary Group Theory [3] we know that Z_n^* forms an *abelian* group under the mod$n$ multiplication, and that Z_n^* can be represented by $Z_n^* = Z_{n_1}^* \times Z_{n_2}^* \times \cdots \times Z_{n_t}^*$ when we take each $Z_{n_i}^*$ as a subgroup of Z_n^*, where $\times$ denotes the *direct product* operation on groups.

For each $1 \le i \le t$, $Z_{n_i}^*$ constitutes a *cyclic* group, since n_i is a prime power. Thus there is an integer g_i, called *primitive root* modn_i, such that every element $x_{ij} \in Z_{n_i}^*$ can be written as $x_{ij} \equiv g_i^{a_{ij}} \pmod{n_i}$ for some $1 \le a_{ij} \le \phi(n_i)$. (In fact there are as many as $\phi(\phi(n_i))$ such g_i's.) Lemma 2 of [11, p.100] tells us a very useful result:

From the Chinese Remainder Theorem, we can construct $h_1, h_2, \ldots, h_t$ *from the above* $g_1, g_2, \ldots, g_t$ *such that* $h_i \equiv g_i \pmod{n_i}$, *and* $h_i \equiv 1 \pmod{n_j}$ *for* $j \neq i$. *Utilizing these particular elements* $h_1, h_2, \ldots, h_t$, *every element* $x \in Z_n^*$ *can be written uniquely as* $x \equiv \prod_{i=1}^{t} h_i^{a_i} \pmod{n}$, *where* $1 \leq a_i \leq \phi(n_i)$.

Apparently, each h_i defined above is also a primitive root $\bmod n_i$. Let $\langle h_1, h_2, \ldots, h_t \rangle$ denote the ordered tuple of such special primitive roots. $\langle h_1, h_2, \ldots, h_t \rangle$ is called a *generator-vector (for* Z_n^* *)*, for simplicity. Notice that there are a lot of generator-vectors for Z_n^* .

The following two lemmas are obviously true (see for example [7, Chapter 4]).

[Lemma 1] *Let* n *be a composite integer factorized as* $n = n_1 n_2 \cdots n_t$, *where each* n_i *is an odd prime power. Also let* γ *be an odd integer greater than 2, and* x *be an element of* Z_n^* . *Then* x *is a* γ^{th}*-residue* $\bmod n$ *iff* x *is a* γ^{th}*-residue* $\bmod n_i$ *for all* $1 \leq i \leq t$.

[Lemma 2] *Let* m *be an odd prime power, and* γ *be an odd integer greater than 2. Let* g *be any primitive root* $\bmod m$, *and let* x, *written as* $x \equiv g^a \pmod{m}$ *for some* $1 \leq a \leq \phi(m)$, *be a positive integer with* $\gcd(x, m) = 1$. *Then when* $\gcd(\gamma, \phi(m)) = 1$, x *is necessarily a* γ^{th}*-residue* $\bmod m$; *and when* $\gcd(\gamma, \phi(m)) = \gamma$, x *is a* γ^{th}*-residue* $\bmod m$ *iff* $a = b\gamma$ *for some integer* b.

From Lemma 1 and Lemma 2, we can get Theorem 1 stated below.

[Theorem 1] *Let* n *be a composite integer factorized as* $n = n_1 n_2 \cdots n_t$, *where each* n_i *is an odd prime power, and let* γ *be an odd integer greater than 2 such that for each* $1 \leq i \leq t$, $\gcd(\gamma, \phi(n_i)) =$ *either* 1 *or* γ. *Also let* $\langle h_1, h_2, \ldots, h_t \rangle$ *be any generator-vector for* Z_n^* *defined above, and* x *be an element of* Z_n^* . *Suppose that* x *is expressed as* $x \equiv \prod_{i=1}^{t} h_i^{a_i} \pmod{n}$. *Then (a) when* $\gcd(\gamma, \phi(n_i)) = 1$ *for each* $1 \leq i \leq t$, x *is necessarily a* γ^{th}*-residue* $\bmod n$; *and (b) when* $\gcd(\gamma, \phi(n_i)) = \gamma$ *for at least one* $1 \leq i \leq t$, x *is a* γ^{th}*-residue* $\bmod n$ *iff for all those i's satisfying* $\gcd(\gamma, \phi(n_i)) = \gamma$, a_i *can be written as* $a_i = a_i'\gamma$ *where* a_i' *is some integer.*

Proof: The truth of (a) follows trivially from Lemma 1 and Lemma 2. Now we show the truth of (b). For simplicity, we assume that there is an integer $1 \leq s \leq t$ such that $\gcd(\gamma, \phi(n_i)) = \gamma$ for each $1 \leq i \leq s$, and that $\gcd(\gamma, \phi(n_i)) = 1$ for each $s < i \leq t$ if $s < t$.

(1) The proof of "if " part: For each $1 \leq i \leq s$, $x \equiv h_1^{a_1} h_2^{a_2} \cdots h_t^{a_t} \equiv h_i^{a_i} \pmod{n_i}$. Now from Lemma 2, we know that x is a γ^{th}-residue $\bmod n_i$ for each $1 \leq i \leq s$, since $a_i = a_i'\gamma$; and if $s < t$, x is also a γ^{th}-residue $\bmod n_i$ for each $s < i \leq t$, since $\gcd(\gamma, \phi(n_i)) = 1$. By Lemma 1, we conclude that x is a γ^{th}-residue $\bmod n$.

(2) The proof of "only if " part: Now by Lemma 1, $x \equiv h_1^{a_1} h_2^{a_2} \cdots h_t^{a_t} \equiv h_i^{a_i} \pmod{n_i}$ is a γ^{th}-residue $\bmod n_i$ for each $1 \leq i \leq t$. In particular, when $1 \leq i \leq s$, we know from Lemma 2 that a_i must take the form of $a_i = a_i'\gamma$ where a_i' is some integer. ∎

We call a triple (n, γ, y) *acceptable* if n, γ and y satisfy the following three conditions:

- n is the product of powers of different odd primes, i.e., $n = n_1 n_2 \cdots n_t$, where each n_i is an odd prime power.
- γ is an odd integer greater than 2 with $\gcd(\gamma, \phi(n_\ell)) = \gamma$ for just one $1 \leq \ell \leq t$, and $\gcd(\gamma, \phi(n_i)) = 1$ for all $i \neq \ell, 1 \leq i \leq t$. For simplicity, we will assume that $\ell = 1$.

- y is an element of Z_n^* written as $y \equiv h_1^{b_1\gamma+e} \prod_{j=2}^t h_j^{b_j} \pmod n$, where $0 < e < \gamma$, $\gcd(e, \gamma) = 1$, $1 \le b_j \le \phi(n_j)$ for each $1 \le j \le t$, and $\langle h_1, h_2, \ldots, h_t \rangle$ is a generator-vector for Z_n^*.

We claim that if (n, γ, y) is an acceptable triple, then y is a γ^{th}-nonresidue $\bmod n$. In fact, it follows immediately from the following corollary of Theorem 1.

[Corollary 1] *Let (n, γ, y) be an acceptable triple. Then an element x of Z_n^*, expressed as $x \equiv h_1^{a_1} \prod_{j=2}^t h_j^{a_j} \pmod n$, is a γ^{th}-residue* $\bmod n$ *iff $a_1 = a_1'\gamma$ for some integer a_1'.*

We are ready to prove a theorem, which is of fundamental importance to this paper.

[Theorem 2] *Let (n, γ, y) be an acceptable triple. Then every element $x \in Z_n^*$ can be represented as $x \equiv y^i w^\gamma \pmod n$ for a* unique $0 \le i < \gamma$ *and some (not necessarily unique) $w \in Z_n^*$.*

Proof: Notice that $y \equiv h_1^{b_1\gamma+e} \prod_{j=2}^t h_j^{b_j} \pmod n$, where $0 < e < \gamma$, $\gcd(e, \gamma) = 1$ and $\langle h_1, h_2, \ldots, h_t \rangle$ is a generator-vector for Z_n^*. As mentioned above, using $\langle h_1, h_2, \ldots, h_t \rangle$, the element x can be written as $x \equiv h_1^{a_1\gamma+f} \prod_{j=2}^t h_j^{a_j} \pmod n$ where $0 \le f < \gamma$.

Now we prove in two steps that there is a unique $0 \le i < \gamma$ such that $x/y^i \bmod n$ is a γ^{th}-residue $\bmod n$. In the first step, we prove that there is such a unique $0 \le i < \gamma$ for the specified generator-vector $\langle h_1, h_2, \ldots, h_t \rangle$. And in the second step, we prove that the above i does not change its value even when $\langle h_1, h_2, \ldots, h_t \rangle$ is replaced with another generator-vector $\langle \hat{h}_1, \hat{h}_2, \ldots, \hat{h}_t \rangle$, i.e., i depends only on x and y themselves, but not on generator-vectors.

(1) Let the generator-vector under consideration be the specified one: $\langle h_1, h_2, \ldots, h_t \rangle$. Since $\gcd(e, \gamma) = 1$, the equation of $i \cdot e \equiv f \pmod \gamma$ has a unique solution $i = f \cdot e^{-1} \bmod \gamma$. Now let $f - i \cdot e = d \cdot \gamma$, we can get the following:

$$\begin{aligned}\frac{x}{y^i} &\equiv \frac{h_1^{a_1\gamma+f} \prod_{j=2}^t h_j^{a_j}}{h_1^{i(b_1\gamma+e)} \prod_{j=2}^t h_j^{ib_j}} \equiv h_1^{(a_1\gamma+f)-i(b_1\gamma+e)} \prod_{j=2}^t h_j^{a_j-ib_j} \\ &\equiv h_1^{(a_1-ib_1)\gamma+(f-ie)} \prod_{j=2}^t h_j^{a_j-ib_j} \equiv h_1^{(a_1-ib_1+d)\gamma} \prod_{j=2}^t h_j^{a_j-ib_j} \pmod n.\end{aligned}$$

By Corollary 1, $x/y^i \bmod n$ is indeed a γ^{th}-residue $\bmod n$.

(2) Let $\langle \hat{h}_1, \hat{h}_2, \ldots, \hat{h}_t \rangle$ be another generator-vector for Z_n^*. It is well-known that each $\hat{h}_i$ can be represented as $\hat{h}_i \equiv h_i^{c_i} \pmod{n_i}$ for some c_i, where h_i is the corresponding constituent of the generator-vector $\langle h_1, h_2, \ldots, h_t \rangle$, and c_i satisfies $\gcd(c_i, \phi(n_i)) = 1$. Notice that $\gcd(c_1, \phi(n_1)) = 1$ implies $\gcd(c_1, \gamma) = 1$, since $\gcd(\gamma, \phi(n_1)) = \gamma$. Using $\langle \hat{h}_1, \hat{h}_2, \ldots, \hat{h}_t \rangle$, the elements y and x can be written as

$$y \equiv (\hat{h}_1)^{\hat{b}_1\gamma+\hat{e}} \prod_{j=2}^t (\hat{h}_j)^{\hat{b}_j} \pmod n \quad \text{and} \quad x \equiv (\hat{h}_1)^{\hat{a}_1\gamma+\hat{f}} \prod_{j=2}^t (\hat{h}_j)^{\hat{a}_j} \pmod n$$

where $1 \le \hat{e} < \gamma$ and $0 \le \hat{f} < \gamma$. ($\hat{e}$ can not be 0, since y is a γ^{th}-nonresidue $\bmod n$.)

We now show that the equation of $\hat{i} \cdot \hat{e} \equiv \hat{f} \pmod \gamma$ has a unique solution $\hat{i} = i = f \cdot e^{-1} \bmod \gamma$. Notice that

$$y \equiv h_1^{b_1\gamma+e} \pmod{n_1} \quad \text{and that} \quad x \equiv h_1^{a_1\gamma+f} \pmod{n_1}.$$

On the other hand,

$$y \equiv (\hat{h}_1)^{\hat{b}_1\gamma+\hat{e}} \equiv (h_1^{c_1})^{\hat{b}_1\gamma+\hat{e}} \equiv h_1^{c_1\hat{b}_1\gamma+c_1\hat{e}} \pmod{n_1}$$

and

$$x \equiv (\hat{h}_1)^{\hat{a}_1\gamma+\hat{f}} \equiv (h_1^{c_1})^{\hat{a}_1\gamma+\hat{f}} \equiv h_1^{c_1\hat{a}_1\gamma+c_1\hat{f}} \pmod{n_1}.$$

Since $\gamma|\phi(n_1)$, from the above four equations we have $c_1 \cdot \hat{e} \equiv e \pmod{\gamma}$ and $c_1 \cdot \hat{f} \equiv f \pmod{\gamma}$. Also since $\gcd(c_1, \gamma) = 1$, we have further $\hat{e} = e \cdot c_1^{-1} \bmod \gamma$ and $\hat{f} = f \cdot c_1^{-1} \bmod \gamma$. Thus the equation $\hat{i} \cdot \hat{e} \equiv \hat{f} \pmod{\gamma}$ is solvable for $\hat{i}$ iff $\hat{i} \cdot e \cdot c_1^{-1} \equiv f \cdot c_1^{-1} \pmod{\gamma}$ is solvable for $\hat{i}$. The latter equation has a unique solution $\hat{i} = i = f \cdot e^{-1} \bmod \gamma$. The remaining work is simple: We need only to check that, for the generator-vector $\langle \hat{h}_1, \hat{h}_2, \ldots, \hat{h}_t \rangle$, $x/y^{\hat{i}} \bmod n$ is a γ^{th}-residue $\bmod n$, which is indeed true. ∎

For an acceptable triple (n, γ, y) and an element $z \in Z_n^*$, we call i the *class-index* of z with respect to (n, γ, y) if $z \equiv y^i u^\gamma \pmod{n}$ for some $u \in Z_n^*$. For $0 \le i < \gamma$, let $R_{n,\gamma,y}^i = \{w \mid w \equiv y^i x^\gamma \pmod{n}, w \in Z_n^*, x \in Z_n^*\}$. $R_{n,\gamma,y}^i$ is the set of elements in Z_n^* which have the same class-index i with respect to (n, γ, y). We denote by $\#X$ the number of elements in a set X.

Let $Z_\gamma = \{0, 1, \ldots, \gamma - 1\}$. Z_γ constitutes a group under the $\bmod \gamma$ addition. By the uniqueness of class-index proved in Theorem 2, we can define a function $f : Z_n^* \to Z_\gamma$ as follows: $f(x) = i$ iff $x = y^i u^\gamma \bmod n$ for some $u \in Z_n^*$. Now we probe more deeply into the structure of Z_n^*.

[Lemma 3] *Let (n, γ, y) be an acceptable triple. Then the function f defined above is an epimorphism (a homomorphism which is also a surjection) from Z_n^* to Z_γ.*

Proof: Again, we prove the theorem in two steps: First, we prove that f is a homomorphism from Z_n^* to Z_γ. Next we prove that f is also a surjection from Z_n^* to Z_γ.

(1) Let $x_i = y^i u^\gamma \bmod n \in R_{n,\gamma,y}^i$ and $x_j = y^j v^\gamma \bmod n \in R_{n,\gamma,y}^j$. Also let $a = (i + j) \bmod \gamma$. Thus $i + j = b\gamma + a$ for some b. Now we have

$$\begin{aligned} f(x_i \cdot x_j) &= f(y^i u^\gamma \bmod n \cdot y^j v^\gamma \bmod n) = f(y^{i+j}(uv)^\gamma \bmod n) \\ &= f(y^{b\gamma+a}(uv)^\gamma \bmod n) = f(y^a(y^b uv)^\gamma \bmod n) \end{aligned}$$

From the uniqueness of index-class (Theorem 2), we conclude that $f(x_i \cdot x_j) = a = (i + j) \bmod \gamma$, i.e., that f is a homomorphism from Z_n^* to Z_γ.

(2) For any $i \in Z_\gamma$, we can choose a $u \in Z_n^*$, and form $x_i = y^i u^\gamma \bmod n$. Clearly, x_i is in Z_n^*, and it satisfies $f(x_i) = i$. So f is also a surjection from Z_n^* to Z_γ. ∎

The following theorem is a straightforward consequence of Lemma 3 just proved above and the *Fundamental Theorem on Group Homomorphisms* [3, Chapter 16].

[Theorem 3] *Let (n, γ, y) be an acceptable triple. Then for any $0 \le i < \gamma$, the number $\#R_{n,\gamma,y}^i$ of elements in Z_n^* which have the same class-index i with respect to (n, γ, y) is $\#R_{n,\gamma,y}^i = \#Z_n^* / \gamma = \phi(n)/\gamma$.*

Proof: See [12]. ∎

γ^{th}-RP should be compared with Quadratic Residuosity Problem. We refer the reader to [6] for a comprehensive exposition of the latter one. In practice, we will always choose an n that is the product of two large primes p_1 and p_2. Since 2 divides both p_1 and p_2, only $\phi(n)/2^2 = \phi(n)/4$ elements of Z_n^* are quadratic residue $\bmod n$. Half elements of Z_n^* have the *Jacobi Symbol* [7, p.65] of -1, and hence can be easily identified without knowing the factorization of n. These elements are "wasted " in the sense that they can never be used as encryptions of messages. However, for γ^{th}-RP with γ being an odd integer, we can elaborately select two primes p_1 and p_2 such that $\gcd(\gamma, p_1 - 1) = \gamma$ and $\gcd(\gamma, p_2 - 1) = 1$, and an element $y \in Z_n^*$ which is a γ^{th}-nonresidue mod$n$ such that (n, γ, y) is an acceptable triple. Now Z_n^* is prettily divided into γ subsets $R_{n,\gamma,y}^0, R_{n,\gamma,y}^1, \ldots, R_{n,\gamma,y}^{\gamma-1}$, each of which has exactly $\phi(n)/\gamma$ elements. In other words, no elements of Z_n^* are "wasted ".

3. Residuosity and Related Problems

In this section we discuss several problems related to γ^{th}-RP, and reveal some relations among them. Also we compare the difficulty of γ^{th}-RP with that of the *factorization problem*. And finally, we state an assumption about the intractability of γ^{th}-RP.

3.1 Three Problems

Suppose k is a positive integer. k will play the role of the *security parameter*. Let $\gamma \geq 3$ be a fixed odd integer. The *hard number set* H_k^γ is defined as:

$$H_k^\gamma = \{n \mid n = pq, p = 2\gamma p' + 1, q = 2q' + 1, \gcd(\gamma, q') = 1, p, q, p' \text{ and } q' \text{ are all primes}, |p'| = |q'| = k\},$$

where $|x|$ denotes the number of bits in the binary expansion of the integer x.

Let $n \in H_k^\gamma$, and let $y \in Z_n^*$ be a γ^{th}-nonresidue mod$n$ such that (n, γ, y) is an acceptable triple. From Theorem 3, Z_n^* is divided into γ subsets according to the class-indices with respect to (n, γ, y) of elements in it, and all subsets have the same size of $\phi(n)/\gamma$.

We referred briefly to γ^{th}-RP at the beginning of the paper. Besides γ^{th}-RP, there are two other problems related intimately to the former. For completeness, the three problems are formally defined below.

(1) *γ^{th}-RP*: Given n, γ and an element $z \in Z_n^*$, decide whether or not z is a γ^{th}-residue mod$n$.

(2) *class-index-comparing problem*: Given an acceptable triple (n, γ, y) and two elements $z_1, z_2 \in Z_n^*$, judge whether or not z_1 and z_2 have the same class-index with respect to (n, γ, y) .

(3) *class-index-finding problem*: Given an acceptable triple (n, γ, y) and an element $z \in Z_n^*$, find the class-index of z with respect to (n, γ, y) .

Theorem 4 shows some relations among the three problems. Before proving it, we first introduce a few conventions. These conventions can be found in recent papers or books on the theory of *circuit complexity*. See for example [10] as well as the references cited there.

By a *circuit* we mean a logic network composed of ordinary AND, OR and NOT gates, and by the size of a circuit we mean the number of logic gates in the circuit.

Let P_1 and P_2 be any two problems among the above three ones. By "P_1 is reducible to P_2" we mean that, given a circuit $T^2[\cdots]$ which solves P_2 for some integer $n \in H_k^\gamma$, we can construct another *polynomial size* circuit $T^1[\cdots]$ which, by using $T^2[\cdots]$ as an *oracle gate*, solves P_1 for the same integer n *with overwhelming probability*. If P_1 and P_2 are reducible to each other, then we say they are (polynomially) equivalent.

Notice that in proving the claim of "P_1 is reducible to P_2", we need only to show explicitly a (probabilistic) polynomial time *algorithm* which is constructed from the circuit $T^2[\cdots]$, and solves P_1 with overwhelming probability. Such an algorithm can be easily converted into a polynomial size circuit completing exactly the same tasks done by the algorithm.

[Theorem 4] *(a) γ^{th}-RP and the class-index-comparing problem are equivalent; (b) γ^{th}-RP and the class-index-comparing problem are reducible to the class-index-finding problem; (c) γ^{th}-RP and the class-index-comparing problem are equivalent to the class-index-finding problem when $\gamma = O(\mathrm{poly}(k))$, where $\mathrm{poly}(\cdot)$ denotes a polynomial.*

Proof:

(1) The Proof of (a)

• the class-index-comparing problem is reducible to γ^{th}-RP: Suppose there is a circuit $T^1[\cdot,\cdot]$ which, for an integer $n \in H_k^\gamma$ and for any element $z \in Z_n^*$, outputs a bit 1 when z is a γ^{th}-residue $\bmod n$ or a bit 0 when z is a γ^{th}-nonresidue $\bmod n$. Using $T^1[\cdot,\cdot]$, we can judge whether or not two elements $z_1, z_2 \in Z_n^*$ have the same class-index with respect to (n,γ,y) : We form $z = (z_1/z_2) \bmod n$, and consult $T^1[n,z]$. $T^1[n,z]$ will outputs 1 iff z_1 and z_2 have the same class-index with respect to (n,γ,y).

• γ^{th}-RP is reducible to the class-index-comparing problem: Suppose there is a circuit $T^2[\cdot,\cdot,\cdot,\cdot]$ which, for an integer $n \in H_k^\gamma$, for any y which is a γ^{th}-nonresidue $\bmod n$ such that (n,γ,y) is an acceptable triple, and for any elements $z_1, z_2 \in Z_n^*$, tells us whether or not z_1 and z_2 have the same class-index with respect to (n,γ,y).

We take $T^2[\cdot,\cdot,\cdot,\cdot]$ as an oracle, and construct an algorithm solving γ^{th}-RP. To consult the oracle successfully, we have to input to it an element $y \in Z_n^*$ which is a γ^{th}-nonresidue $\bmod n$ such that (n,γ,y) is an acceptable triple. We are not given directly such a y. This problem can be resolved by the *randomization* argument: We select *randomly* $y \in Z_n^*$, $x \in Z_n^*$, form $z' = x^\gamma \bmod n$, and consult $T^2[n,y,z',z]$. With probability $\phi(\gamma)/\gamma$, y is a desired γ^{th}-nonresidue $\bmod n$. And with the same probability, $T^2[n,y,z',z]$ outputs the correct answer. Repeating the above steps when needed, we can get the correct answer with arbitrarily high probability.

(2) The Proof of (b)

Suppose there is a circuit $T^3[\cdot,\cdot,\cdot]$ which, for an integer $n \in H_k^\gamma$, for any y which is a γ^{th}-nonresidue $\bmod n$ such that (n,γ,y) is an acceptable triple, and for any element $z \in Z_n^*$, finds the class-index of z with respect to (n,γ,y). Using $T^3[\cdot,\cdot,\cdot]$, we can quickly judge whether or not two elements $z_1, z_2 \in Z_n^*$ have the same class-index with respect to (n,γ,y). Thus the class-index-comparing problem, and hence γ^{th}-RP are both reducible to the class-index-finding problem.

(3) The Proof of (c)

By (1), γ^{th}-RP and the class-index-comparing problem are equivalent, and by (2), γ^{th}-RP and the the class-index-comparing problem are reducible to the class-index-finding problem, thus it suffices to prove that the class-index-finding problem is reducible to γ^{th}-RP when $\gamma = O(\mathrm{poly}(k))$. Suppose that we are given a circuit $T^1[\cdot,\cdot]$ which answers the residuosity of z for an integer $n \in H_k^\gamma$ and any element $z \in Z_n^*$. By using $T^1[\cdot,\cdot]$ as an oracle and consulting it as follows, we can determine the class-index of z with respect to (n,γ,y) :

> $i := 0; w := z;$
> **while** $T^1[n,w] = 0$ **do**
> $\{i := i + 1;$
>   *Select at random an* $x \in Z_n^*$;
> $w := (w/y)x^\gamma \bmod n$ };
> **output**(i).

This algorithm halts after consulting $T^1[\cdot,\cdot]$ for $O(\gamma) = O(\text{poly}(k))$ expected times, hence the class-index-finding problem is reducible to γ^{th}-RP when $\gamma = O(\text{poly}(k))$. ∎

3.2 How Difficult are the Problems

From Theorem 4, we know that the class-index-finding problem is in general harder than both γ^{th}-RP and the class-index-comparing problem. Also we know that the latter two ones are equivalent in any cases, so from now on, we will not refer to the class-index-comparing problem.

Now we informally compare the difficulties of γ^{th}-RP and the class-index-finding problem with that of the factorization problem. We do it in two cases: (1) γ is small, i.e., γ grows polynomially in (the security parameter) k. Such a γ is denoted by $\gamma = O(\text{poly}(k))$. (2) γ is large, i.e., γ grows faster than any polynomial in k.

(1) When γ is Small

In this case, the class-index-finding problem is equivalent to γ^{th}-RP.

When the factorization (p,q) of $n \in H_k^\gamma$ is known, deciding the residuosity of $z \in Z_n^*$ is easy: By Lemma 2 and Corollary 1, z is a γ^{th}-residue mod$n$ iff $z^{(p-1)/\gamma} \equiv 1 \pmod{p}$. This equation can be checked in $O(\text{poly}(k))$ time. Hence γ^{th}-RP can not be more difficult than the factorization problem.

On the other hand, when the factorization is unknown, γ^{th}-RP seems to be intractable. Adleman and McDonnell showed that [1]: *If there is an oracle which solves γ^{th}-RP for any randomly selected $\gamma = O(\text{ poly }(k))$, then we can use the oracle to construct an efficient (although not polynomial) algorithm for factoring (large integer) n.*

Thus for a *randomly selected* $\gamma = O(\text{poly}(k))$, γ^{th}-RP and the class-index-finding problem are both *approximately* equivalent to the factorization problem. In cryptographic uses, γ is usually fixed to some small odd integer. However, even in such situations, γ^{th}-RP seems to be equally difficult.

(2) When γ is Large

The equation $z^{(p-1)/\gamma} \equiv 1 \pmod{p}$ can be checked in $O(\text{poly}(k))$ time even when γ is exponentially large in k. Thus γ^{th}-RP for a large γ is also solvable provided that we know the factorization of n. If γ^{th}-RP with a large γ is solvable, the factorization problem seems to be also solvable, though we can not prove it now. The class-index-finding problem, however, appears to be still intractable even when the factorization of n is known. We can consider that, when γ is large, the class-index-finding problem is harder than both γ^{th}-RP and the factorization problem, and the latter two problems are equivalent.

3.3 γ^{th}-Residuosity Assumption

Having known that γ^{th}-RP is intractable, now we can formally describe our intractability assumption for γ^{th}-RP:

[**γ^{th}-Residuosity Assumption**] Let Ω denote the set of circuits which, for a fraction $1/\text{ poly }(k)$ of $n \in H_k^\gamma$, and for all $z \in Z_n^*$, take as inputs n and z, output a bit 1 iff z is a γ^{th}-residue mod$n$. Denote by S_k the minimum size among all sizes of circuits in Ω. Then $S_k > \text{poly}(k)$ for all sufficiently large k.

4. Generalizing the GM Encryption

This section is concerned with generalizing the GM bit-by-bit probabilistic encryption to a block-by-block probabilistic one, based on the difficulty of solving γ^{th}-RP. In [2] Benaloh and Yung discussed briefly a generalization for the most restricted case where γ is a small odd *prime*. For our generalization presented below, γ can be any small odd *integer* greater than 2. So Benaloh and Yung's generalization is, as a special case, included in ours.

Moreover, our generalized encryption is more efficient than the GM encryption, and shares with the latter an appealing property — it hides all *partial information* [6] from a polynomial time bounded adversary, or it achieves Shannon's *perfect secrecy* when the power of an adversary is limited to polynomial time.

4.1 The Generalized Encryption

Consider the situation in which B wants to send some secret information to A. Let γ be an odd integer of poly (k) size agreed upon between A and B, and let the *message space* be $M_\gamma^\ell = \{m \mid m = m_1\|m_2\|\cdots\|m_\ell, m_i \in Z_\gamma, 1 \le i \le \ell\}$, where ℓ is a positive integer of size $O(\text{poly}(k))$, $Z_\gamma = \{0, 1, \ldots, \gamma - 1\}$, and $a\|b$ denotes the concatenation of a and b.

A selects an $n(= pq) \in H_k^\gamma$, and uses the factorization (p, q) of n to choose at random an element $y \in Z_n^*$ such that y is a γ^{th}-nonresidue mod$n$ $y \in Z_n^*$ and (n, γ, y) is an acceptable triple. Then A makes n and y public, but keeps p and q secret.

The encryption algorithm for B and the decryption algorithm for A are as follows:

Encryption Algorithm $E(n, \gamma, y, m)$

Let $m = m_1\|m_2\|\cdots\|m_\ell$. From $i = 1$ to ℓ, do as follows:

1. Randomly choose an $x_i \in Z_n^*$;

2. Compute $c_i := y^{m_i} x_i^\gamma \bmod n$.

$c = c_1\|c_2\|\cdots\|c_\ell$ is an encryption of the message $m = m_1\|m_2\|\cdots\|m_\ell$.

Decryption Algorithm $D(p, q, \gamma, y, c)$

Recall that by Lemma 2 and Corollary 1, an element $z \in Z_n^*$ is a γ^{th}-residue mod$n$ iff $z^{(p-1)/\gamma} \equiv 1 \pmod p$. Let $c = c_1\|c_2\|\cdots\|c_\ell$. Now for each $c_i, 1 \le i \le \ell$, do as follows:

1'. Randomly select an $f \in Z_\gamma$ *and an* $x \in Z_n^*$;

2'. Compute $z := y^f x^\gamma c_i \bmod n$;

3'. **if** $z^{(p-1)/\gamma} \not\equiv 1 \pmod p$ **then goto** *1'*;

4'. $m_i := \gamma - f \bmod \gamma$.

$m = m_1\|m_2\|\cdots\|m_\ell$ is the message concealed in the encryption $c = c_1\|c_2\|\cdots\|c_\ell$.

The foregoing decryption algorithm runs in $O(\gamma\,\text{poly}\,(k))$ expected time. Rabin's fast probabilistic algorithm [9], which finds a root of a polynomial of degree γ over the finite field $GF(p)$ by $O(\gamma(\log\gamma)^2(\log\log\gamma)(\log p))$ expected number of arithmetic operations over $GF(p)$, can also be used for our decryption purpose.

Clearly, the running time of either of the two algorithms grows polynomially in the size of γ. This puts limitations upon our degree of freedom of selecting γ. To be sure that the decryption algorithm runs in $O(\text{poly}\,(k))$ time, we have to choose γ such that $\gamma = O(\text{poly}\,(k))$.

It seems to the authors that γ^{th}-RP with a large γ is unlikely to be applicable to constructing GM-like probabilistic encryptions. Nevertheless, the problem may have application to other cryptographic problems such as the digital signature and the key distribution problems.

4.2 Security of the Generalized Encryption

Under *Quadratic Residuosity Assumption*, the GM encryption has been proved to be *polynomially secure*. Notions introduced in [6], where the basic message unit for encryption is a bit 0/1, can be obviously generalized to those for the case where the basic message unit for encryption is an integer from $\{0, 1, \ldots, \gamma-1\}$. In particular, the definition of *unapproximable trapdoor predicates* of [6] can be generalized to that of *unapproximable trapdoor functions*. Then under γ^{th}-Residuosity Assumption, we can prove that our generalized probabilistic encryption is also polynomially secure. For detail descriptions see [12], where we also give first proofs for certain theorems about probabilistic encryptions.

5. How to Cast Dice over a Network

A (two-party) coin flipping protocol is a communication protocol between two *mutually distrusted* parties A and B in a network, by which the two parties can jointly generate a sequence of unbiased random *bits*, i.e., a sequence where each *bit* is equally likely to be 0 or 1 independent of preceding bits.

Coin flipping is a special case of *β-face dice casting* (throwing a die with β faces, each of which has a score differing from all other faces) with $\beta = 2$. By a β-face dice casting protocol, two mutually distrusted parties can jointly generate a sequence of unbiased random *letters* from a β-letter alphabet, i.e., a sequence where each *letter* is equally likely to be any letter from the β-letter alphabet independent of preceding letters.

In the sequel, we will simply assume that a β-letter alphabet Σ is a set of integers defined by $\Sigma = \{0, 1, \ldots, \beta - 1\}$.

Many fair coin flipping protocols have been proposed in the literature. In contrast to this, few *direct* and *efficient* dice casting protocols are known.

A coin flipping protocol can be easily translated into a β-face dice casting protocol in the following way:

> *Repeat the coin flipping protocol $|\beta|$ times, where $|\beta|$ denotes the number of bits in the binary expansion of β. Take the resultant $|\beta|$-bit sequence as an integer, and check whether or not the integer is in Σ. If not in, throw away the sequence and return to the beginning; otherwise output the integer as an agreed die score.*

However, such a *naïve* β-face dice casting protocol would be very inefficient in practice.

Along another line, researchers (see for example [4]) have constructed various protocols which solve all mental games (including dice casting, key sharing, etc.). Unfortunately, all those protocols seem to be only of theoretical value.

In the following, we propose two direct β-face dice casting protocols: the first is a general one based on any one-way one-to-one function; the second is a practical and efficient one based on γ^{th}-RP. See [12] for a unified treatment.

Below, just as in Section 3.2, "small" means growing polynomially in (the security parameter) k, and "large" growing faster than any polynomial in k. To simplify our discussions, we will assume that the communication channel between A and B provides *data integrity* in the following sense: (1) data transmitted through the channel is not affected by natural noise, and (2) no adversary can alter or insert something into data transmitted through the channel.

5.1 A General Protocol

In this subsection, we show that a one-way one-to-one function, such as Discrete Exponentiation (over a large finite field) whose inverse (called Discrete Logarithm) is widely considered to be intractable [8], can be used to construct a general β-face dice casting protocol.

Let $S_m = \{0,1\}^m$ denote the set of binary strings of length m over the alphabet $\{0,1\}$, where m is a positive integer. Also let I_m denote the set of m-bit integers $0, 1, \ldots, 2^m - 1$. If $m \leq 0$, S_m as well as I_m is defined as an empty set. For any integer $x \in I_m$, $\bar{x}$ denotes the m-bit binary representation of x.

Suppose that $\beta = |\Sigma| = 2^\ell$ for some integer $1 \leq \ell \leq k$, where k is the security parameter.

First, A and B jointly select a one-way one-to-one function $f(\cdot) : S_k \rightarrow I_k$, then they do as follows:

Dice_Casting_Protocol_1:

1. A selects at random an $x \in I_\ell = \{0, 1, \ldots, 2^\ell - 1\}$ and an $r \in S_{k-\ell} = \{0,1\}^{k-\ell}$, then he sends $z = f(r\|\bar{x})$ to B;

2. B returns a random $y \in I_\ell$ to A;

3. A reveals x and r to B;

4. B checks whether x, r and z satisfy $z = f(r\|\bar{x})$. If so, then A and B agree upon the letter $d = x + y \bmod 2^\ell$; otherwise B detects A's cheating.

Replacing the step *4* with the following step *4'*, we obtain a protocol for the case where β is any positive integer less than or equal to 2^ℓ.

4'. B checks whether x, r and z satisfy $z = f(r\|\bar{x})$. If the check is not passed, then B detects A's cheating. Otherwise, A and B agree upon the letter $d = x + y \bmod 2^\ell$ whenever $d \in \Sigma = \{0, 1, \ldots, \beta - 1\}$, and they return to the step *1* whenever $d \notin \Sigma$.

Remark: We combined r and x by $r\|\bar{x}$, since for many one-to-one functions $f(\cdot)$ which are seemingly one-way and have received extensive examination, such as Discrete Exponentiation and the RSA encryption function, the least or nearly least significant bits of v appear to be extremely hard to extract from $u = f(v)$ [8]. Of course, which method for combining r and x should actually be taken depends on the function $f(\cdot)$ selected.

For the above protocol, neither A nor B can control the result d: Since $f(\cdot)$ is one-way, B, whose power is tacitly assumed to be polynomially bounded, can not compute $r\|\bar{x} = f^{-1}(z)$ from z, and hence can not bias the result. On the other hand, since $f(\cdot)$ is also one-to-one, A can not change his mind after sending z to B.

For most functions $f(\cdot)$ which seem to be one-way one-to-one, evaluating $z = f(r\|\bar{x})$ is time-consuming, so the above protocol may be inefficient in applications. In Section 5.2, we describe a practical protocol based on γ^{th}-RP. This protocol is especially efficient when β is not so large.

5.2 A Practical Protocol

Here, γ^{th}-RP once again finds its application to cryptography: Under γ^{th}-Residuosity Assumption, we can construct a direct β-face dice casting protocol which can be executed very fast when β is small.

Suppose A and B has agreed upon an odd integer γ such that $\gamma \geq \beta$. Also suppose A has published a large integer $n \in H_k^\gamma$, and a γ^{th}-nonresidue mod$n$ $y \in Z_n^*$ such that (n, γ, y) is an acceptable triple. Thus, every element $z \in Z_n^*$ has a unique class-index with respect to (n, γ, y) .

Now we give a protocol for the special case when $\beta = \gamma$, i.e., β is an *odd integer*.

Dice_Casting_Protocol_2:

1) A chooses randomly an $i \in Z_\gamma = \{0, 1, \ldots, \gamma - 1\}$ and an $x \in Z_n^*$, then sends $z = y^i x^\gamma \bmod n$ to B;

2) B gives back a random $j \in Z_\gamma$ to A;

3) A reveals i, x to B;

4) B checks whether i and x satisfy $z \equiv y^i x^\gamma \pmod{n}$. If so, then A and B agree upon the letter $d = i+j \bmod \gamma$; otherwise B detects A's cheating.

Modifying the step *4)* in the same way as in Section 5.1, a protocol for the case when $0 < \beta \leq \gamma$ can be obtained. Details are omitted here.

Dice_Casting_Protocol_2 has several desirable features:

⟨1⟩ B can not be cheated by A — By our assumption, z has a unique class-index with respect to (n, γ, y) . Thus, A can not change his mind after sending z to B;

⟨2⟩ A can not be cheated by B — If γ^{th}-RP is intractable, (and hence class-index-finding problem is also intractable,) then B, when given z, n, y and γ, can not get any information about the class-index of z with respect to (n, γ, y) . This is the very basis of our block-by-block *probabilistic* encryption presented in Section 4. Thus, under γ^{th}-Residuosity Assumption, B has no way of biasing the result.

⟨3⟩ If A follows the protocol, then he gives B no information which may have help to B in trying to cheat A or more directly to factorize the integer n — The reason is very obvious: Both i and x are selected by A randomly and independently of B. Hence $z = y^i \cdot x^\gamma \bmod n$ is also a random element in Z_n^* . Thus when B tries to cheat A or to factorize the integer n, he can not hope to do them better with these random i, x and z than without. (A formal proof is given in [12].)

Now it becomes clear that the resultant letter d is a random letter from $\Sigma = Z_\gamma$ if at least one of the two parties follows the protocol. Repeating the protocol if needed, A and B can jointly generate a sequence of unbiased random letters from Σ.

One may argue that B may be cheated by A from the beginning, since (n, γ, y) is published by A and hence it may *not* be an acceptable triple. B's concern about this kind of cheating is removed if A can convince B in some way that (n, γ, y) *is indeed an acceptable triple.*

General, though extremely inefficient, interactive protocols for the above convincing problem exist. See for instance [4]. But if β is small, there is a simple solution to the problem: We force A and B to cast dice using the same triple (n, γ, y) as those, which are published by A and are used for constructing probabilistic encryptions for protecting information transmitted to A. To decrypt uniquely and efficiently an encryption transmitted to him, A has to choose a triple (n, γ, y) such that it is an acceptable one. Thus, if such (n, γ, y) is used in casting dice, B is ensured that he will not be cheated by A.

If there is a trusted authority in the network, we can take another approach to the above problem: (1) Let A open the factorization of his n to the authority; (2) The authority checks whether or not A's triple (n, γ, y) is acceptable, and tells B "YES" if is, or "NO" if not. Or more simply, we can let the authority choose and publish an acceptable triple (n, γ, y) . Now it is not necessary for the users in the network to concern about whether or not the triple is acceptable, since the authority is trusted. Moreover, any two parties in the network can cast dice by using the same acceptable triple (n, γ, y) and following **Dice_Casting_Protocol_2**.

6. Conclusion

We have revealed several useful properties of γ^{th}-RP with γ an odd integer greater than 2. Under the assumption that γ^{th}-RP is intractable, we have generalized the Goldwasser-Micali bit-by-bit probabilistic encryption to a block-by-block probabilistic one, and have proposed a direct protocol for the β-face dice casting problem. Applications of γ^{th}-RP to other cryptographic problems such as the key distribution and digital signature problems are worth investigating.

References

[1] Adleman,L. and McDonnell,R. "An Application of Higher Reciprocity to Computational Number Theory." *Proc. of* 23^{rd} *IEEE Symp. on Foundations of Computer Science*, 1982, pp.100-106.

[2] Benaloh,J. and Yung,M. "Distributing the Power of a Government to Enhance the Privacy of Voters." *Proc. of* 5^{th} *ACM Symp. on Principles of Distributed Computing*, 1986, pp.52-62.

[3] Burn,R.P. *Groups: A Path to Geometry*, Cambridge University Press, 1985.

[4] Chaum,D., Crépeau,C. and Damgård,I. "Multiparty Unconditionally Secure Protocols." *Proc. of CRYPTO'87*, 1987.

[5] Galil,Z., Haber,S. and Yung,M. "A Private Interactive Test of a Boolean Predicate and Minimum-Knowledge Public-Key Cryptosystems." *Proc. of* 26^{th} *IEEE Symp. on Foundations of Computer Science*, 1985, pp.360-371.

[6] Goldwasser,S. and Micali,S. "Probabilistic Encryption." *Journal of Computer and System Sciences*, Vol.28, 1984, pp.270-299.

[7] Ireland,K. and Rosen,M. *A Classical Introduction to Modern Number Theory* , Springer-Verlag, 1982.

[8] Peralta,R. "Simutaneously Security of Bits in the Discrete Log." *Proc. of EUROCRYPTO'85*, 1985, pp.62-72.

[9] Rabin,M. "Probabilistic Algorithms in Finite Fields." *SIAM Journal on Computing*, Vol.9, No.2, 1980, pp.273-280.

[10] Schöning,U. *Complexity and Structure*, Lecture Notes in Computer Science, Vol.211, Springer-Verlag, 1986.

[11] Shanks,D. *Solved and Unsolved Problems in Number Theory*, Chelsea Publishing Company, 1985.

[12] Zheng,Y. "A Study on Probabilistic Cryptosystems and Zero-Knowledge Protocols." *Master Thesis Submitted to the Division of Electrical and Computer Engineering, Yokohama National University*, February 1988.