# 고차잉여류 문제에 기반을 둔 공개키 암호알고리즘 류

박성준*O, 양형규**, 원동호*

* 성균관대학교 정보공학과

** 강남대학교 전자계산학과

# A Class of Public Key Residue Cryptosystems

Sung Jun Park*, Hyung Kyu Yang** and Dong Ho Won*

* Dept. of Information Engineering, Sung Kyun Kwan University

E-mail : sjpark@simsan.skku.ac.kr

** Dept. of Computer Science, Kangnam University

요 약

본 논문에서는 지금까지 $\gamma^{th}$-잉여류 문제를 이용하여 제안된 공개키 잉여류 암호알고리즘들을 살펴보고, $\gamma$의 크기에 따라 제안된 각 암호알고리즘들을 분류해 본다.

특히 이산대수 문제를 이용하여 현재까지 제안된 공개키 잉여류 암호알고리즘에서 사용하는 $\gamma$의 크기와 형태를 더욱더 일반화한 새로운 공개키 잉여류 암호알고리즘을 제안한다.

## 1. 서 론

$\gamma^{th}$-잉여류 문제에 기반을 둔 안전성이 증명되는 최초의 확률론적 암호알고리즘은 1984년 Goldwasser에 의해 제안되었다. 제안된 확률론적 암호알고리즘의 안전성은 이차잉여류 문제에 근거하였다.[4] 이후 Benaloh가 이차 잉여류 문제를 작은 홀수인 소수 $\gamma$로 확장한 $\gamma^{th}$-잉여류 문제에 안전성 기반을 둔 확률론적 암호알고리즘을 제안하였다.[2] 이를 Zheng, Matsumoto, Imai는 $\gamma$가 임의의 작은 홀수(소수에 상관없이)일 경우에 $\gamma^{th}$-잉여류 문제에 안전성 기반을 둔 확률론적 암호알고리즘으로 일반화하였다.[10][11] 또한 Kurosawa는 $\gamma$가 임의의 작은 정수일 경우에 $\gamma^{th}$-잉여류 문제에 안전성 기반을 둔 확률론적 암호알고리즘을 제안하였다.[6]

그러나 위에서 제안된 공개키 잉여류 암호알고리즘들은 모두 $\gamma$의 크기가 다항식 크기(polynomial size)인 경우이며, $\gamma$가 지수적 크기(exponential size)일 경우에는 확률론적 암호알고리즘을 구성할 수 없다고 생각하였다.

그러나 박성준, 원동호와 Sakai, M.Kasahara는 독립적으로 $\gamma$가 지수적 크기를 갖는다 하더라도 어떤 특별한 형태를 갖는 경우에는 확률론적 암호알고리즘을 구성할 수 있음을 증명하였다.[7][8][9]

본 논문에서는 위에서 제안된 공개키 잉여류 암호알고리즘들의 $\gamma$의 크기와 형태를 살펴보고, 특히 이산대수 문제와 결합하여 $\gamma$의 크기를 더욱더 일반화하였다.

## 2. 수학적 배경 및 기존의 공개키 잉여류 암호알고리즘

이 절에서는 $\gamma^{th}$-잉여류 문제에 대한 수학적 개념들을 정리하고 기존의 공개키 잉여류 암호알고리즘들을 특성에 따라 분류해 본다.

$\gamma^{th}$-잉여류 문제를 정의하기 전에 먼저 기본적인 이차 잉여류 문제(Quadratic Residuosity Problem)를 알아본다.

$gcd(z, n) = 1$인 정수 $z$에 대하여,법 n에 관한 이차 합동식 $z = w^2 \bmod n$ 가 해를 가질 때 z를 법 n에 관한 이차 잉여(quadratic residue mod n)라 하고 이 합동식이 해를 가지지 않을 때 z를 법 n에 관한 이차 비잉여(quadratic nonresidue mod n)라고 한다. z, n에 대하여 z가 법 n에 관한 이차 잉여인지 이차 비잉여인지를 결정하는 문제를 법 n상의 이차 잉여류 문제라 한다. 이차 잉여류 문제의 계산복잡도는 n의 소인수분해 문제와 동치임이 증명되고, Goldwasser에 의해 제안된 최초의 확률론적 암호알고리즘의 안전성 근거도 이차 잉여류 문제이다.[4]

이차 잉여류 문제의 확장으로 $gcd(z, n) = 1$인 정수 $z$에 대하여,고차 합동식 $z = w^{\gamma} \bmod n$ (단, $\gamma > 2$인 양의 정수)가 해를 가질 때 x를 법 n에 관한 $\gamma^{th}$-잉여류($\gamma^{th}$-residue)라 하고 이 합동식이 해를 가지지 않을 때 x를 법 n에 관한 $\gamma^{th}$-비잉여류($\gamma^{th}$-nonresidue)라고 한다.

**[정의 2.1]** 양의 정수 $\gamma$, n이 주어질 때 정수 $z$가 다음의 조건을 만족하면, z를 법 n에 관하여 $\gamma^{th}$-잉여류라 한다.

(조건) $gcd(z, n) = 1$이고, $z \equiv x^{\gamma} \bmod n$를 만족하는 x가 존재한다

위의 조건을 만족하지 않는 z는 법 n에 관하여 $\gamma^{th}$-비잉여류라 한다.

고차 잉여류 문제($\gamma^{th}$-Residuosity Problem: 약어로 $\gamma^{th}$-RP)란 주어진 $gcd(z, n) = 1$인 양의 정수 $z \in Z_n^*$ 가 $\gamma^{th}$-잉여류인지 $\gamma^{th}$-비잉여류인지를 결정하는 문제이다.

고차 잉여류 문제의 계산복잡도는 $\gamma$가 다항식 크기(polynomial size)일 때는 n의 소인수분해 문제와 동치이고 $\gamma$가 지수적 크기(expoenential size)일 때는 n의 소인수분해 문제보다 어렵다고 간주되고 있다.[10][11]

**[정의 2.2]** 양의 정수 $\gamma$, n와 임의의 $z \in Z_n^*$ 가 주어지고 $z = y^i u^{\gamma} \bmod n$를 만족하는 유일한 i가 존재할 때, i를 z의 잉여류 지수(class-index)로 정의한다

일반적으로 $z \in Z_n^*$ 에 대해서, 위의 수식을 만족하는 i는 존재 안할 수도 있고, 존재하더라도 유일하지 않을 수가 있다. 기존에 제안된 공개키 잉여류 암호알고리즘들은 모두 $z = y^i u^{\gamma} \bmod n$ 를 만족하는 유일한 i가 존재하는 세쌍 (n, $\gamma$, y)의 조건을 분석하고, 이러한 조건을 만족하는 (n, $\gamma$, y) 상에서 암호알고리즘을 구성하였다.

즉, Glodwasser, Micali는 y가 2차 비잉여류인 경우이며, Benaloh는 perfect consonant (n, $\gamma$, y) 개념을, Zheng은 acceptable triple (n, $\gamma$, y) 개념을, Kurosawa는 Basic element (n, $\gamma$, y) 개념을 사용하였다. 또한 Sakai는 최대생성원 y를 이용하였으며, 박성준, 원동호는 aceeptable triple (n, $\gamma$, y) 개념을 aceeptable triple (n, $\gamma^s$, y) 개념으로 일반화하였다.

또한 기존의 공개키 잉여류 암호알고리즘들은 암호알고리즘을 구성하기 위하여 $\gamma^{th}$-잉여류 문제와 밀접하게 관련된 문제로 잉여류-지수-비교(class-index-comparing) 문제와 잉여류-지수-계산(class-index-finding) 문제를 고려하였다.

**① $\gamma^{th}$-잉여류 문제 :**

(n, γ, y) 과 gcd(z, n) = 1인 양의 정수 $z \in Z_n^*$ 가 주어졌을때 $z \in Z_n^*$ 가 $\gamma^{th}$-잉여류인지 $\gamma^{th}$-비잉여류인지를 결정하는 문제이다.

**② 잉여류-지수-비교(Class-index-comparing) 문제 :**

(n, γ, y) 과 $z_1, z_2 \in Z_n^*$ 이 주어졌을때 $z_1 = y^i u^\gamma \bmod n$ 과 $z_2 = y^j v^\gamma \bmod n$ 의 잉여류 지수 i, j를 비교하는 문제

**③ 잉여류-지수-계산(Class-index-finding) 문제 :**

(n, γ, y) 과 $z \in Z_n^*$ 가 주어졌을때 $z = y^i u^\gamma \bmod n$ 의 잉여류 지수 i를 찾는 문제

특히 잉여류 지수를 계산하는 알고리즘은 $\gamma^{th}$-잉여류 지수를 비교하는 방법에 의해 구성되어 암호알고리즘의 복호알고리즘의 계산복잡도는 γ에 의해 결정되고 (즉, 비교 횟수), 이로 인해 각 공개키 잉여류 암호알고리즘에서 사용되는 γ의 크기는 실질적으로 적은 수로 제약받았다 즉, 박성준, 원동호 암호알고리즘에서의 복호가 가능한 (효율성을 무시하더라도) γ의 크기는 $10^7 \sim 10^7$ 범위내외이다. 실제적으로 박성준, 원동호 암호알고리즘에서 사용한 γ와 s의 크기는 각각 257과 16이고, Sakai 암호알고리즘에서 사용한 γ는 $10^2 \sim 10^3$ 정도의 인수들의 곱으로 구성되었다.

## 3. 제안하는 공개키 잉여류 암호알고리즘 (γ의 확장)

본 절에서는 이산대수 문제와 결합하여 γ가 매우 큰 경우에도 공개키 잉여류 암호알고리즘이 구성가능한 방법을 분석하였다.

k를 양의 정수인 안전성 계수라 한다. γ를 3보다 큰 고정된 홀수인 정수라 하자.

$n = pq$, $p = 2\gamma p' + 1$, $q = 2q' + 1$, $\gcd(\gamma^s, q') = 1$, 여기서 p, q, p′ 그리고 q′는 모두 소수, $|p'| = |q'| = k$.

y를 최대생성원이라 놓자.

**[ 송신자 A의 암호알고리즘 ]** E(n, γ, y, m)

m는 평문:

1. $Z_n^*$ 상의 임의의 x를 랜덤하게 선택한다.
2. 암호문 $c = y^m x^\gamma \bmod n$ 를 계산한다.

암호문 c의 복호알고리즘으로 기존의 알고리즘을 사용하면, γ의 크기에 제약을 받으므로 본 논문에서는 γ의 크기를 확장하기 위하여 잉여류 지수 계산 문제를 이산대수 문제로 환원하여 복호하고자 한다. 즉, 이산대수 문제로 환원한 복호알고리즘은 다음과 같다.

**[ 수신자 B의 복호알고리즘 ]** D(p, q, γ, y, c)

c에 대하여 다음의 계산을 수행한다:

1. $c^{\phi(n)/\gamma} \bmod n = (y^m x^\gamma)^{\phi(n)/\gamma} \bmod n = (y^{\phi(n)/\gamma})^m \bmod n$
2. $Y = y^{\phi(n)/\gamma} \bmod n$ 라 놓으면,
$$c^{\phi(n)/\gamma} \bmod n = Y^m \bmod n.$$
3. 평문 m은 mod n 상의 Y에 대한 이산대수이다.
(Y의 order는 γ이다. 즉, ord(Y) = γ.)

위의 복호알고리즘의 계산복잡도는 이산대수를 푸는 알고리즘에 의해 계산되어진다. 또한 이산대수를 푸는 알고리즘의 계산복잡도는 n의 크기가 아닌 밑수 Y의 지수 (즉, $\gamma$ = ord(Y))에 의해 결정된다.[ 11 ]

일반적으로 mod n 상의 밑수를 g라 하고, g의 지수를 q라 놓으면 이산대수 알고리즘의 계산복잡도는 $O(q^{1/2})$이다. 이 경우에 $\gamma$의 크기가 $10^{10}$ 이상이라 하더라도 암호문 c에서 평문 m을 계산할 수 있게 된다. 그러나 이는 기존의 복호알고리즘으로는 계산 불가능하다.

## 4. 결 론

본 논문에서는 $\gamma^{th}$-잉여류 문제를 이용하여 제안된 공개키 잉여류 암호알고리즘들을 알아보고, 제안된 각 암호알고리즘에서 복호알고리즘이 구성가능한 $\gamma$의 크기를 알아보았다. 그 결과, 기존의 공개키 잉여류 암호알고리즘에서의 $\gamma$의 크기는 매우 제한적이었다.

그러나 본 논문에서는 이산대수 문제를 이용하여 현재까지 제안된 공개키 잉여류 암호알고리즘에서 사용하는 $\gamma$의 크기를 더욱 확장한 새로운 공개키 잉여류 암호알고리즘을 제안한다. 제안된 새로운 공개키 잉여류 암호알고리즘에서 사용가능한 $\gamma$의 크기는 이산대수 문제의 계산복잡도에 의존하며, 현재로는 $10^{10}$ 이상도 가능한 것으로 판단된다.

향후에는 이러한 계산복잡도 문제를 이론적으로 정확히 계산하여, 각 공개키 잉여류 암호알고리즘들에서 복호알고리즘의 계산복잡도를 비교하고자 한다.

## [ 참고 문헌 ]


[1] L. Adleman,"subexponential algorithm for the discrete logarithm problems with applications to cryptography", Proc. IEEE 20th Annual Symposium on Foundations o Computer Science, 1979, pp.55-60.

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

[3] J. Cohen and M. Fisher, "A Robust and Verifiable Cryptographically Secure Election Scheme", Proc. 26th IEEE Symp. on Foundations of Computer Science, pp.372-382, 1985.

[4] S. Goldwasser and S. Micali, "Probabilistic encryption", Journal of Computer and Sysytem Sciences, 28, pp.270-299, 1984.

[5] N. Koblitz, A course in Number Theory and Cryptography, Springer-Verag,1987.

[6] K. Kurosawa,Y. Katayama, and W. Ogata, "General public key cryptosystems and mental poker protocols", Proc. of EUROCRYPT'90, pp.374-388, 1990.

[7] S. J. Park and D. H. Won, "A Generalization of Public Key Residue Cryptosystem", Proceeding of JW-ISC'93, pp.202-206, 1993.11.

[8] S. J. Park and D. H. Won, "A Generalized Public Key Residue Cryptosystem and Its Applications", IEEE GLOBECOM'95, Singapore, 1995.11.

[9] R. Sakai and M. Kasahara, "A note on probabilistic cryptosystems using $\gamma$-th residue problem", SCIS'93, 1993.

[10] Y. Zheng,T. Matsumoto, and H. Imai, "Residuosity Problem and its Applications to Cryptography", Trans. IEICE, vol.E71, No.8, pp.759-767, 1988.

[11] Y. Zheng, A Study on Probabilistic Cryptosystems and Zero-Knowledge Protocol, Master thesis, Yokohama National University, 1988.