공개키 잉여류 알고리즘의 효율적인 복호알고리즘

박성준O, 김승주, 원동호
성균관대학교 정보공학과

An Efficient Decryption Algorithm for Public Key Residue Cryptosystem

Sung Jun Park, Seung Joo Kim and Dong Ho Won
The Department of Information Engineering
Sung Kyun Kwan University
E-mail : sjpark@dosan.skku.ac.kr

요 약

본 논문에서는 γ^{th}-잉여류 문제에 안전성 기반을 둔 공개키 잉여류 암호 알고리즘의 효율적인 복호알고리즘을 제안한다.

제안한 복호알고리즘은 기존의 복호알고리즘 중 가장 많은 시간이 소요되는 γ^{th} 잉여류 판정 루틴을 소거하는 방법을 강구하였으며, 특히 복호알고리즘의 효율성을 위한 precomputation 방법을 분석하였다.

1. 서 론

γ^{th}-잉여류 문제에 안전성 기반을 둔 안전성이 증명되는 최초의 확률론적 암호알고리즘은 1983년 Goldwasser에 의해 제안되었다. 제안된 확률론적 암호알고리즘의 안전성은 이차잉여류 문제에 근거하였다.[4] 이후 Benaloh가 이차 잉여류 문제를 작은 홀수인 소수 γ로 확장한 γ^{th}-잉여류 문제에 안전성 기반을 둔 확률론적 암호알고리즘을 제안하였다.[1] 또한 Zheng, Matsumoto, Imai는 γ가 임의의 작은 홀수(소수에 상관없이)일 경우에 γ^{th}-잉여류 문제에 안전성 기반을 둔 확률론적 암호알고리즘을 제안하였다.[14][15] 그리고 γ가 다항식 크기를 넘는 지수적 크기(exponential size)일 경우에는 확률론적 암호알고리즘을 구성할 수 없다고 생각하였다.

그러나 박성준, 원동호는 γ가 지수적 크기를 갖는다 하더라도 어떤 특별한 형태를 갖는 경우에는 확률론적 암호알고리즘을 구성할 수 있음을 보였다.[7][12] 즉, γ의 크기가 지수적 크기라 하더라도 $O(poly_1(k))^{O(poly_2(k))}$의 형태를 가질 때는 확률론적 암호알고리즘을 구성할 수 있다. 특히 제안된 확률론적 암호알고리즘의 특성(안전성의 이론적인 증명, 평문의 크기가 지수적 크기 등)상 많은 응용분야를 갖게 되어, 암호화 프로토콜에서의 기본 함수(cryptographic primitive function)로 사용할 수 가 있는 장점이 있다.[8][9][10][11][16][17]

그러나 기존에 제안된 공개키 잉여류 암호알고리즘들은 복호알고리즘의 계산복잡도가 매우 크

다는 단점이 있다. 본 논문에서는 박성준, 원동호가 제안한 일반화한 공개키 잉여류 암호알고리즘을 바탕으로 이러한 단점을 해결할 수 있는 매우 효율적인 복호알고리즘을 제안한다.

2. 기존의 공개키 잉여류 알고리즘

본 절에서는 1993년 JW-ISC'93에서 박성준, 원동호가 제안한 공개키 잉여류 암호알고리즘을 간략히 설명한다.[7]

$n = pq$, $p = 2\gamma^s p'+1$, $q = 2q'+1$, $\gcd(\gamma^s, q')=1$, p, q, p' 그리고 q'는 모두 소수로 놓는다. 또한 y는 법 n상에서의 $(\gamma^s)^{th}$-비잉여류이고, (n, γ^s, y)는 acceptable triple이다.

이때 암호알고리즘과 복호알고리즘은 다음과 같다.

[암호알고리즘] $E(n, \gamma, y, s, m)$

m를 평문이라 놓자. $m = m_0+m_1\gamma+\ldots+m_{s-1}\gamma^{s-1}$.

1) Z_n^* 상의 임의의 랜덤한 수 x를 선택한다.

2) $c = y^m x^{\gamma^s} \bmod n$ 를 계산한다.

c가 평문 m의 암호문이다.

[복호알고리즘] $D(p, q, \gamma, y, s, c)$

$c = y^m x^{\gamma^s} \bmod n$

1) Z_n^* 상의 랜덤한 수 x에 대하여,

$$c = y^m x^{\gamma^s} \bmod n = y^{m_0+m_1\gamma+m_2\gamma^2+\ldots+m_{s-1}\gamma^{s-1}} x^{\gamma^s} \bmod n$$

2) 먼저 j=1에서 s-1까지 $c^{\gamma^j} \bmod n$ 를 계산한다.

$$c^{\gamma} = y^{m_0\gamma+m_1\gamma^2+m_2\gamma^3+\ldots+m_{s-2}\gamma^{s-1}+m_{s-1}\gamma^s} x^{\gamma^s\gamma} \pmod n$$

$$= y^{m_0\gamma+m_1\gamma^2+m_2\gamma^3+\ldots+m_{s-2}\gamma^{s-1}} y^{m_{s-1}\gamma^s} x^{\gamma^s\gamma} \pmod n$$

$$= y^{m_0\gamma+m_1\gamma^2+m_2\gamma^3+\ldots+m_{s-2}\gamma^{s-1}} (y^{m_{s-1}} x^{\gamma})^{\gamma^s} \pmod n$$

$$c^{\gamma^2} = y^{m_0\gamma^2+m_1\gamma^3+\ldots+m_{s-3}\gamma^{s-1}+m_{s-2}\gamma^s} (y^{m_{s-1}\gamma} x^{\gamma^2})^{\gamma^s} \pmod n$$

$$= y^{m_0\gamma^2+m_1\gamma^3+\ldots+m_{s-3}\gamma^{s-1}} (y^{m_{s-2}} y^{m_{s-1}\gamma} x^{\gamma^2})^{\gamma^s} \pmod n$$

$$\vdots$$

$$c^{\gamma^{s-1}} = y^{m_0\gamma^{s-1}} (y^{m_1} y^{m_2\gamma} \ldots y^{m_{s-1}\gamma^{s-2}} x^{\gamma^{s-1}})^{\gamma^s} \pmod n$$

3) j=s-1에서 1까지 c^{γ^j} 의 잉여류 지수를 구한다.

(1) $c^{\gamma^{s-1}}$의 잉여류 지수는 m_0

(2) $c^{\gamma^{s-2}}$와 m_0 에 의해 m_1 를 구한다.

.

(s-1) c^{γ}, m_0, ... , 그리고 m_{s-3} 에 의해 m_{s-2} 를 구한다.

마지막으로 c, m_{i0}, ... , 그리고 m_{s-2} 에 의해 m_{s-1} 를 구한다.

4) 평문 m : 암호문 c의 잉여류 지수

3. 제안하는 효율적인 복호알고리즘

본 절에서는 2장에서 살펴본 공개키 잉여류 암호알고리즘의 효율적인 복호알고리즘을 제안한다.

효율성을 개선하기 위하여 기존의 복호알고리즘 중 가장 많은 시간이 소요되는 γ^{th}-잉여류 판정 루틴을 소거하는 방법을 강구하였으며, 특히 복호알고리즘의 효율성을 위한 precomputation 방법을 분석하였다.

먼저 γ^{th}-잉여류 판정 루틴을 소거한 복호알고리즘은 다음과 같다.

[제안하는 복호알고리즘] D(p, q, γ, y, s, c)

1) For a random x in Z_n^*,

$$c = y^m x^{\gamma^s} \bmod n = y^{m_0+m_1\gamma+m_2\gamma^2+\ldots+m_{(s-1)}\gamma^{s-1}} x^{\gamma^s} \bmod n$$

2) First compute $c^{\phi(n)/\gamma^s}$

$$c^{\phi(n)/\gamma^s} = (y^{\phi(n)/\gamma^s})^{m_0+m_1\gamma+m_2\gamma^2+\ldots+m_{(s-2)}\gamma^{s-1}+m_{(s-1)}\gamma^{s-1}} \pmod n$$

Let $C = c^{\phi(n)/\gamma^s} \pmod n$, $Y = y^{\phi(n)/\gamma^s} \pmod n$

3) Compute $C^{\gamma^j} = (c^{\phi(n)/\gamma^s})^{\gamma^j}$ for j=1 to s-1

$$C^{\gamma} = Y^{m_0\gamma+m_1\gamma^2+m_2\gamma^3+\ldots+m_{(s-2)}\gamma^{s-1}+m_{(s-1)}\gamma^s} \pmod n$$

$$= Y^{m_0\gamma+m_1\gamma^2+m_2\gamma^3+\ldots+m_{(s-2)}\gamma^{s-1}} Y^{m_{(s-1)}\gamma^s} \pmod n$$

$$= Y^{m_0\gamma+m_1\gamma^2+m_2\gamma^3+\ldots+m_{(s-2)}\gamma^{s-1}} \pmod n$$

$$C^{\gamma^2} = Y^{m_0\gamma^2+m_1\gamma^3+\ldots+m_{(s-3)}\gamma^{s-1}+m_{(s-2)}\gamma^s} \pmod n$$

$$= Y^{m_0\gamma^2+m_1\gamma^3+\ldots+m_{(s-3)}\gamma^{s-1}} Y^{m_{(s-2)}\gamma^s} \pmod n$$

$$= Y^{m_0\gamma^2+m_1\gamma^3+\ldots+m_{(s-3)}\gamma^{s-1}} \pmod n$$

.

.

.

$$C^{\gamma^{s-1}} = Y^{m_0\gamma^{s-1}} \pmod n$$

4) Compute the index of C^{γ^j} for j=1 to s-1 by reverse order

(1) The index of $C^{\gamma^{s-1}}$ implies m_0

$$C^{\gamma^{s-1}} = (Y^{\gamma^{s-1}})^{m_0} \pmod{n}$$

(2) $C^{\gamma^{s-2}}$ and m_0 implies m_1

$$C^{\gamma^{s-2}} / Y^{m_0\gamma^{s-2}} = C^{\gamma^{s-2}} \cdot Y^{-(m_0\gamma^{s-2})} \pmod{n}$$
$$= (Y^{\gamma^{s-1}})^{m_1} \pmod{n}$$

(3) $C^{\gamma^{s-3}}$,m_0 ,and m_1 implies m_2

$$C^{\gamma^{s-3}} / Y^{m_0\gamma^{s-3}+m_1\gamma^{s-2}} = C^{\gamma^{s-3}} \cdot Y^{-(m_0\gamma^{s-3}+m_1\gamma^{s-2})} \pmod{n}$$
$$= (Y^{\gamma^{s-1}})^{m_2} \pmod{n}$$

.

.

.

(s-1) C^{γ}, m_0, ... , and $m_{(s-3)}$ implies $m_{(s-2)}$

Finally, C, m_0, ... , and $m_{(s-2)}$ implies $m_{(s-1)}$

5) Result : m = the index of c

또한 위의 개선된 복호알고리즘에서 항상 계산값이 요구되는 $\{\gamma^1, \gamma^2, \cdots, \gamma^{s-1}\}$, $Y = y^{\phi(n)/\gamma^s}$, Y^{-1}, $Y^{\gamma^{s-1}}$를 미리 계산(precomputation)하여 저장함으로서 복호알고리즘의 효율성을 개선할 수 있다. 이 경우, ($\frac{s(s-1)}{2}$ × |γ|) + (3 × |n|) 비트의 메모리를 추가로 요구하게 된다. (방법 1)

특히, 복호알고리즘 단계 4)의 모든 s개의 C^{γ^j} (j = 0, 1, ..., s-1)의 잉여류 지수를 계산하는 루틴의 수행시간을 줄이기 위하여 |n|비트의 γ개의 $(Y^{\gamma^{s-1}})^i \pmod{n}$ (i = 0, 1, 2, ..., γ-1) 값을 미리 계산하여 저장함으로서 전체 복호알고리즘의 수행시간을 크게 줄일 수 있다. 이 경우에는 γ × |n| 비트의 메모리를 추가로 요구하게 된다. (방법 2)

아래의 표는 기존의 복호알고리즘과 새로이 제안하는 복호알고리즘을 PC에서 구현하여, 그 수행속도를 비교한 것이다.

γ = 257 s = 16 |n| = 688 비트	기존의 복호알고리즘	제안하는 복호알고리즘
사전 계산 (방법 1)	0	2.69
복 호	3925.27	25.71

(단위 : sec)

표 1. 복호알고리즘의 속도 비교 (Pentium/90MHZ)

4. 결 론

본 논문에서는 박성준, 원동호가 JW-ISC'93에서 제안한 공개키 잉여류 암호알고리즘의 효율적

인 복호알고리즘을 제안하였다. 제안된 복호알고리즘은 γ^{th}-잉여류 문제에 기반을 둔 모든 공개키 잉여류 암호알고리즘에 적용할 수 있다.

제안한 복호알고리즘은 기존의 복호알고리즘 중 가장 많은 시간이 소요되는 γ^{th} 잉여류 판정 루틴을 소거하는 방법을 강구하였으며, 특히 복호알고리즘의 효율성을 위한 precomputation 방법을 소개하였다.

향후에는 제안한 개선된 복호알고리즘과 기존의 복호알고리즘의 계산복잡도를 이론적으로 분석하고자 한다.

[참고문헌]

[1] 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.

[2] G. Brassard,D. Chaum, and C. Crepeau, Minimum disclosure proofs of knowledge, Report PM-R8710,CWI,1987.

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

[6] M. Naor, Bit Commitment Using Pseudorandomness, J. Cryptology, Vol. 4, pp.151-158, 1991.

[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, Chung Ryong Jang, Kyung Sin Kim, and D. H. Won, "A "Paradoxical" identity-based scheme based on the γ^{th}-residuosity problem and discrete logarithm problem", An International Conference on Numbers and Forms, cryptography and codes, August 21-28,1994, Khabarovsk, Russia.

[9] S. J. Park, In sook Lee, and D. H. Won, "A Practical Group Signature", Proceeding of JW-ISC'95, Japan, 1995.1.

[10] S. J. Park, Bo Young Lee, and D. H. Won, "A Secure Multiway Election Scheme", ICCC'95, Korea, 1995.8.

[11] S. J. Park, and D. H. Won, "A Practical Identity-based Group Signature", ICEIC'95, China, 1995.8.

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

[13] R. Sakai and M. Kasahara, A note on probabilistic cryptosystems using γ-th residue problem, SCIS'93, 1993.

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

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

[16] 박성준, 원동호, "고차잉여류 문제와 이산대수 문제에 기반을 둔 역설적인 id-based 암호시스

템", 한국통신정보보호학회 논문지, 1994. 12.

[17] 박성준, 원동호, "Cryptographic k-capsule를 이용한 다후보 전자선거 프로토콜", 성균관대학교 논문지, 1994.12.