情報保護學會論文誌
第15卷 第6號, 2005. 12

대수기하 부호를 이용한 공개키 암호

이 정 근,† 박 상 우,‡ 김 재 헌
국가보안기술연구소

A Public Key Encryption Scheme Using Algebraic-Geometry Codes

Jung-Keun Lee,† Sangwoo Park,‡ Jaeheon Kim
National Security Research Institute

요 약

본 논문에서는 새로운 부호 기반 공개키 암호 스킴을 제안한다. 제안된 스킴은 Eurocrypt 2003에서 제안된 Augot-Finiasz 스킴을 수정한 것이다. Reed-Solomon 부호를 일반적인 대수기하 부호로 교체하고 복호화에서는 Guruswami-Sudan 복호 알고리즘을 사용한다. 본 암호 스킴은 Augot-Finiasz 스킴의 약점인 Coron의 공격이나 Kiayias-Yung의 공격에 대한 취약성을 가지지 않는다. Augot-Finiasz 스킴에서와 같은 기본적인 분석을 통해 Augot-Finiasz 스킴의 제안 논문에서 제시하였던 수준의 키 크기 대비 안전성을 가짐을 주장한다.

ABSTRACT

We propose a new code-based publick key encryption scheme. It is obtained by modifying the Augot and Finiasz scheme proposed at Eurocrypt 2003. We replace the Reed-Solomon codes with general algebraic-geometry codes and employ Guruswami-Sudan decoding algorithm for decryption. The scheme is secure against Coron's attack or Kiayias and Yung's attack to which the Augot and Finiasz scheme is vulnerable. Considering basic attacks applied to the Augot and Finiasz scheme, we claim that the proposed scheme provides similar security levels as the Augot and Finiasz scheme was claimed to provide for given key lengths.

Keywords : *대수기하 부호, Augot-Finiasz 공개키 암호, Guruswami-Sudan 복호 알고리즘*

Ⅰ. 서 론

현재 많이 사용되고 있는 공개키 암호들은 소인수 분해 문제나 이산대수 문제에 기반하고 있으나 양자 계산 분야의 기술이 발전함에 따라 가까운 미래에 효과적인 공격이 가능할 수 있다는 우려가 있다. 이러한 점을 고려하여 다른 수학적 난제에 기반한 공개키 암호를 개발하는 것은 의미 있는 일이다. 일반적인 선형 부호에서 복호의 어려움은 공개키 암호 설계에 이용될 수 있다. 현재까지 선형 부호를 이용하는 몇 가지 공개키 암호 스킴이 소개되었다. 초기의 것들로 McEliece 공개키 암호[1]와 Niederreiter 공개키 암호[2] 등이 있는데, 이들은 모두 적절한 안전성을 위해서는 키의 길이가 매우 커야 하는 단점을 가지고 있다. Eurocrypt 2003에서 발표된 Augot-Finiasz 공개키 암호(이하에서 AF 스킴이라 함)[3]는 이전의 부호 기반 공개키 암호에 비해서는 훨씬 작은 크기의 키를 필요로 하며 Reed-Solomon 부호와 관련된 특정 복호 문제의 어려움

접수일 : 2005년 10월 3일 ; 채택일 : 2005년 11월 30일
† 주저자 : jklee@etri.re.kr
‡ 교신저자 : psw@etri.re.kr

을 가정할 경우 키 길이에 관해 지수적 안전성을 가질 수 있음을 주장하였다. 그러나 곧바로 Coron에 의해 매우 효과적인 공격이 가능함이 보여졌으며,[4] Asiacrypt 2004에서는 Kiayias와 Yung에 의해, AF 스킴의 매개변수 변경 시에도 효과적인 공격이 성립함이 보여졌다.[5] 이러한 AF 스킴의 취약성을 제거하기 위해서 본 논문에서는 Reed-Solomon 부호 대신 일반적인 대수기하 부호를 도입한다. 결과적으로 Coron의 공격이나 Kiayias-Yung의 공격이 성립하지 않으며, 또한 AF스킴이 의도했던 키 길이 대비 안전성을 제공하는 것을 주장할 수 있다. 본 논문의 구성은 다음과 같다. Ⅱ절에서는 대수기하 부호의 정의를 제시하고 AF 스킴에 관해 간략히 설명한다. Ⅲ절에서는 본 논문에서 제안하는 공개키 암호 스킴을 설명하고 구체적인 예로서, 타원곡선으로부터 정의된 대수기하 부호를 이용한 공개키 암호 스킴을 제시한다. Ⅳ절에서는 제안된 암호 스킴의 안전성 분석 결과를 제시한다. 논문 [3]에서와 같이 기본적인 공격에 대한 안전성을 고려하고, Coron의 공격이나 Kiayias- Yung의 공격이 적용되지 않음을 설명한다. Ⅴ절에서는 제안된 공개키 암호 스킴의 효율성을 살펴본다.

Ⅱ. 기반 지식

본 절에서는 대수기하 부호에 관한 정의 및 사용될 기호에 대해 설명하고 AF 스킴에 대해 살펴본다.

1. 대수기하 부호

대수적 함수체에 관한 정의는 다음과 같다. (좀 더 자세한 정의는 [6],[7]에서 참조할 수 있다.)

정의 1. $\mathbb{F}_q$를 위수 q인 유한체라 하고, $\overline{\mathbb{F}}_q$를 그의 대수적 폐포(algebraic closure)라고 하자. F_q 상에서 종수(genus)가 g인 대수적 함수체는 다음 조건을 만족하는 순서쌍 $(\chi, \overline{\chi}, K)$이다.

- $\overline{\chi}$는 $\overline{\mathbb{F}}_q^l$의 부분집합이다.
- χ는 $\overline{\chi}$의 부분집합이다.
- K는 $\overline{\chi}$에서 $\overline{\mathbb{F}}_q \cup \{\infty\}$로 가는 함수들의 한 집합이다.

단,

1. K는, 각 점에서의 덧셈 및 곱셈 연산에 대해서, $\mathbb{F}_q$의 확장체이다. 즉, K는 그 자체로 체를 이루며 $\mathbb{F}_q$에서 값을 가지는 모든 상수함수를 포함하고 있다.
2. 임의의 $f \in K$와 임의의 $x \in K$에 대해서 $f(x) \in \mathbb{F}_q \cup \{\infty\}$이다.
3. $f \in K$가 $\sum_{x \in \overline{\chi}} \mathrm{ord}(f,x) < 0$을 만족할 경우 f는 항등적으로 0이다.
4. 각각의 $i \in \mathbb{Z}, x \in \overline{\chi}$에 대해서, $f \in K$:ord(f,x) $\{\leq i, \mathrm{ord}(f,y) \leq 0 \ \forall y \neq x\}$는 $\mathbb{F}_q$상의 차원이 $i-g+1$ 이상인 벡터공간이다. ($L_{i,x}$로 표기한다.)

위의 정의에서 사용된 $\mathrm{ord}(f,x)$는 다음과 같이 x에서 f의 극차수를 나타낸다.

- $f(x) \neq 0, \infty$일 경우 $\mathrm{ord}(f,x) = 0$
- x가 f의 단순 영점일 경우 $\mathrm{ord}(f,x) = -1$
- $f(x) = 0$이고 x에서 단순원점을 가지는 f_0와 양의 정수 k에 대해서 $f(x)/f_0^k(x) \neq 0, \infty$일 경우 $\mathrm{ord}(f,x) = -k$
- $f(x) = \infty$$x$이고 x에서 단순원점을 가지는 f_0와 양의 정수 k에 대해서 $f(x)f_0^k(x) \neq 0, \infty$일 경우 $\mathrm{ord}(f,x) = k$

Reed-Solomon 부호는 종수 0인 대수적 함수체 위에 정의된 대수기하 부호로 볼 수 있다. 본 논문에서 암호적 용도로 고려하는 대수적 함수체의 예는 다음과 같다.

- $\overline{\chi}$를 $\mathbb{F}_q[X_1, X_2]$의 기약다항식을 만족하는 $\overline{\mathbb{F}}_q^2$위의 점들의 집합이라고 하자. χ를 $\overline{\chi}$의 F_q-유리점들이라고 하고 K를 χ의 각 점에서는 $\mathbb{F}_q \cup \{\infty\}$에서 값을 가지는 유리함수체라고 한다.

다음 보조정리에 의해 대수적 함수체로부터 선형 부호들을 얻는다.

보조정리 1. $(\chi, \overline{\chi}, K)$를 유한체 F_q 상의 종수가 g인 대수적 함수체라고 하자. $x_0; x_1, \cdots, x_n$을 χ상의 점들이라고 할 때 선형사상 $L_{\{k \pm g-1, x_0\}} \rightarrow \mathbb{F}_q^n$, $f \mapsto (f(x_1), \cdots, f(x_n))$은 일대일이고 그 상은 $k' \geq k$, $d' \geq n-k-g+1$인 어떤 k', d'에 대해서 $[n, k', d']_q$-선형 부호이다.

보조정리 1에서와 같이 얻어진 선형 부호를 종수 g이고 설계거리 $d=n-k-g+1$인 $[n,k',d']_q$-대수기하 부호라고 부른다. 대수기하 부호에 대해서는 Guruswami-Sudan 리스트 복호 알고리즘이라는 효율적인 복호 알고리즘이 존재한다.[7]

정리 1. 종수 g, 설계거리 $d=n-k-g+1$인 $[n,k',d']_q$-대수기하 부호가 있을 때, 적절한 가정하에 $n-\sqrt{n(n-d)}$개 이하의 오류를 정정할 수 있는 다항식 복잡도의 리스트 복호 알고리즘이 존재한다.

정리 1에서의 가정들은 대수적 함수체 위에서 정의된 다항식들의 근을 계산하는 효율적인 알고리즘의 존재에 관한 것이다.[7,9]

2. Augot-Finiasz 공개키 암호

본 절에서는 Eurocrypt 2003에서 제안된 Augot-Finiasz 공개키 암호를 간단히 살펴본다.

- 매개변수
- q: 소수의 멱승인 자연수
- $n-W>k$, $w\le(n-W-k+1)/2$, $W\ge n-\sqrt{nk}$인 자연수 n, k, W, w
- $x_1,\cdots,x_n\in\mathbb{F}_q$와 이로부터 정의된 $[n,k,n-k+1]_q$ Reed-Solomon 부호
- 비밀키: 최고차항의 계수가 1인 $k-1$차 다항식에 대응하는 코드워드 c와 해밍 무게 W인 오류 E
- 공개키: $c+E$
- 암호화: 평문 m은 $k-2$차 이하의 다항식이다. m을 암호화하면 다음과 같다.

$$y=c_m+\alpha(c+E)+e$$

단, c_m은 m에 대응하는 코드워드이고, α는 랜덤하게 선택된 $\mathbb{F}_q$의 원소이며, e는 해밍 무게 w인 랜덤한 오류이다.

- 복호화: 암호문 $y\in\mathbb{F}_q^n$의 복호화 과정은 다음과 같다.
- 1단계: E에서 0이 아닌 위치를 제외하여 얻어진, 길이가 $n-W$인 단축된 부호에서 다음의 관계식을 얻는다.

$$\bar{y}=\overline{c_m}+\alpha\bar{c}+\bar{e}$$

- 2단계: $w\le(n-W-k+1)/2$이므로, 단축된 부호에 Reed-Solomon 복호 알고리즘을 적용할 수 있으며 그 결과 $\bar{y}$로부터 $\overline{c_m}+\alpha\bar{c}$에 대응하는, 차수가 k보다 작은 다항식 f를 얻을 수 있다. 그러한 f는 w가 단축된 부호의 절반보다 작기 때문에 유일하게 결정된다. 이렇게 구한 f는 원래의 부호에서 $c_m+\alpha c$에 대응된다.
- 3단계: α는 f의 $k-1$차 항의 계수로 구한다. α와 위에서 구한 $c_m+\alpha c$로부터 c_m과 평문 m을 구한다.

논문 [3]에서, Augot와 Finiasz는 기본적인 Reed-Solomon 부호의 복호기법들로부터 유도된 키 복구 공격 및 평문 복구 공격에 대한 정량적인 분석 결과를 제시하였다.

- 랜덤 계수에 대한 전수 조사: 암호화에 사용된 랜덤 계수 α가 올바르게 추측되면, 평문 복구가 바로 이루어진다.
- 정보집합복호(Information Set Decoding): 공개키나 암호문에서 오류가 없는 충분히 많은 위치를 추측하여 비밀키나 평문을 복구하는 방법이다.
- 오류집합복호(Error Set Decoding): 공개키나 암호문으로부터 적당한 숫자의 오류가 있는 위치를 찾은 후, 오류가 없는 위치를 이용해서 단축된 부호에서 복호알고리즘을 적용함으로써 비밀키 또는 평문을 복구하는 방법이다.

논문 [3]에서는 위의 공격방법들 이외에 정보집합복호보다 효율적인 Canteaut-Chabaud 알고리즘도 고려되었다.

Ⅲ. 제안 스킴

1. 명세

본 논문에서 제안하는 공개키 암호 스킴은 다음과 같다.

- 매개변수
- q: 소수의 멱승인 자연수, g: 양의 정수
- $W>n-\sqrt{nk}$, $w<(n-W-k+1)/2$, $w<n-W-\sqrt{(n-W)(k+g-1)}$, $k>2g-1$를

만족하는 자연수 n, k, W, w

- 정리 1에서와 같이 효율적인 리스트 복호 알고리즘을 가지는, 대수적 함수체 $(\chi, \bar{\chi}, K)$와 $x_1, \cdots, x_n \in \chi$로부터 정의된, 종수 g이고 설계거리 $n-k+1$인 $[n,k',d]_q$-대수기하 부호 $(d \geq n-k+1)$
- 비밀키: $\mathrm{ord}(p, x_0) = k-1, (hp)(x_0) = 1$을 만족하는 $p \in L_{k-1, x_0}$에 대응하는 코드워드 c와 해밍 무게 W인 오류 E
- 공개키: $c+E$
- 암호화: 평문 m은 $\mathrm{ord}(m, x_0) \leq k-2$인 L_{k-1, x_0}의 원소이다. m을 암호화하면 다음과 같다.

$$y = c_m + \alpha(c+E) + e$$

단, c_m은 m에 대응하는 코드워드이고, α는 랜덤하게 선택된 $\mathbb{F}_q$의 원소이며, e는 해밍 무게 w인 랜덤한 오류이다.

- 복호화: 암호문 $y \in \mathbb{F}_q^n$의 복호화 과정은 다음과 같다.
- 1단계: E에서 0이 아닌 위치를 제외하여 얻어진, 길이가 $n-W$인 단축된 부호에서 다음의 관계식을 얻는다.

$$\bar{y} = \overline{c_m} + \alpha\bar{c} + \bar{e}$$

- 2단계: $w < (n - W - \sqrt{(n-W)(k+g-1)})$이므로, 단축된 부호에 Guruswami-Sudan 리스트 복호 알고리즘을 적용할 수 있으며 그 결과 $\bar{y}$로부터 $\overline{c_m} + \alpha\bar{c}$과 $f \in L_{q-1, x_0}$를 얻을 수 있다. 그러한 f는 w가 단축된 부호의 절반보다 작기 때문에 유일하게 결정된다. 이렇게 구한 f는 원래의 부호에서 $c_m + \alpha c$에 대응된다.
- 3단계: $(fh)(x_0) = \alpha$로부터 α를 구하고, 위에서 구한 $c_m + \alpha c$로부터 c_m과 평문 m을 구한다.

제시된 암호 스킴에 대해서 좀 더 설명하면 다음과 같다..

- $W > n - \sqrt{nk}$라는 조건은 비밀키 중의 한 성분인 c가 복호 알고리즘을 이용해서 $c+E$로부터 복구되지 않도록 하기 위해서 필요하다.
- 평문 m의 집합은 $\mathbb{F}_q$ 상의 벡터공간 L_{k-1, x_0}의 부분공간인 L_{k-2, x_0}이다. 그러므로 평문 전체의 집합은 적당한 자연수 l에 대해서 $\mathbb{F}_q^l \mathbb{F}_q^l$과 일대일 대응을 시킬 수 있다.
- 제시된 암호 스킴은 AF 스킴의 확장으로 볼 수 있는데, Reed-Solomon 부호는 아핀 직선에서 정의된 종수 0인 대수기하 부호이며 차수 k인 다항식은 아핀 직선의 무한점(point at infinity)에서 차수가 k인 극점을 가지고 다른 점에서는 극점을 가지지 않는 유리함수이기 때문이다. 다만 종수 $g > 0$라는 조건을 추가함으로써 AF 스킴은 제외하였다.

2. 구체적 예

본 소절에서는 제안된 암호 스킴의 구체적인 예를 제시한다.

- $F = \mathbb{F}_q$를 위수 q인 유한체라고 하고 χ는 $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$으로 정의된 타원곡선이라고 하며 O는 χ의 무한점이라고 하자.
- 각각의 $i > 0$에 대해서 $L_i = L_{i \cdot O}$를 O에서 극차수 i 이하인 극점을 가지고 다른 극점은 가지지 않는 유리함수들의 집합이라고 하자. (영함수도 L_i의 원소로 포함시킨다.)

L_i는 $\mathbb{F}_q$ 상의 차원이 i 또는 $i+1$인 벡터공간으로 $\{1, x, x^2, \cdots, x^\delta, y, xy, \cdots, x^\delta y\}$를 기저로 가짐이 알려져 있다. (단, δ는 $i/2$ 또는 $(i-1)/2$이고 $\delta' = \delta - 1$) [6] 이 기저를 사용하면, L_i의 각 원소는 $\mathbb{F}_q$의 원소들의 순서쌍으로 표현할 수 있다.

이러한 사실들로부터 실제로 구현 가능한 종수 1인 대수기하 부호들을 얻을 수 있으며 이들에 대해서는 Guruswami-Sudan 리스트 복호 알고리즘이 효율적으로 적용됨이 알려져 있다. [7][9] 이제 이러한 대수기하 부호들을 이용해서 제시된 암호 스킴을 구성하는 데는 O에서 영점을 가지는 유리함수들이 필요하다. $x^{-l}y^{-m}(l, m > 0)$이 그러한 함수들의 예이다.

Ⅳ. 안전성 분석

이 절에서는 제안된 암호 스킴의 안전성을 살펴본

다. 구체적으로는 AF 스킴에 적용된 분석 기법들을 적용한다.

1. 기본 공격

본 소절에서는 Augot와 Finiasz가 고려한 일련의 안전성 분석 기법을 본 암호 스킴에 적용한 결과를 제시한다.

· 랜덤 계수에 대한 전수 조사

AF 스킴에서와 마찬가지로 랜덤 계수 α가 올바르게 추측되면, 평문은 오류 e를 복구함으로써 쉽게 계산할 수 있다: 올바른 α로부터 $y-\alpha(c+E)$에 Guruswami-Sudan 복호 알고리즘을 적용하여 c_m과 m을 구할 수 있다.

· 정보집합복호

앞에서 언급한 바와 같이 공개키나 암호문에서 오류가 없는 충분히 많은 위치를 추측함으로써 비밀키나 평문을 복구하는 방법이다.

· 키 복구 공격: 공개키 $c+E$에서 k개의 오류가 없는 위치를 찾는다면 AF 스킴에서와 마찬가지로 c를 구할 수 있다. 그러므로 공격량은 $\binom{n}{k}/\binom{n-W}{k}$이다.

· 평문 복구 공격: AF 스킴의 경우 길이 $k+1$인 임의의 벡터는 $[n,k]$-Reed-Solomon 부호에서 코드워드임을 이용하여 암호문에서 $k+1$개의 오류가 없는 위치를 찾음으로써 평문에 대한 복구가 성립한다. 그러나 제안된 암호 스킴에서 사용된 공개키 $c+E$는 임의의 $k+1$개의 위치로 단축시켰을 때 L_{k,x_0}에서의 코드워드가 되지 못한다. 그러므로 AF 스킴에 적용가능한 정보집합복호 방법을 이용한 평문 복구 공격은 성립하지 않는다.

· 오류집합복호

· 키 복구 공격: 공개키 $c+E$에서 적당한 수의 오류 위치를 찾고 이들 위치를 제외한 단축 부호에서 복호 알고리즘을 적용하여 비밀키 c를 구하는 공격이다. 구체적으로, $c+E$에서 β개의 오류 위치를 찾는다면 $W-\beta< n-\beta-\sqrt{(n-\beta)(k-1)}$ 일 경우 오류가 없는 위치로 한정한 단축 부호에서 $c+E$를 복호할 수 있다. 그러므로 공격량은 $\binom{n}{\beta}/\binom{W}{\beta}$이다. (단, $\beta=n-(n-W)^2/(k-1)$)

· 평문 복구 공격: 본 공격은 AF 스킴에서와 마찬가지 이유로 효율적이지 못하다.

Canteaut-Chabaud 알고리즘은 정보집합복호보다 효율적인 공격 방법이지만 일반적인 매개변수에 대해서 공격량을 제시하는 것이 어렵다. 그러나 AF 스킴에 대해서와 마찬가지로 적절히 매개변수를 설정할 경우 정보집합복호 방법과 거의 비슷한 공격량을 가질 것으로 보인다. 여기서 제시된 기본 공격들에 대한 공격량을 모두 고려했을 때, 이러한 기본 공격 이외에 효과적인 공격이 존재하지 않는다고 가정하면 AF 스킴이 제안된 논문에서 주장했던 키 크기 대비 안전성 수준을 본 논문에서 제안된 암호 스킴이 가진다고 볼 수 있다. 실제로는 평문 복구를 위한 정보집합복호 방법이 본 암호 스킴에 직접적으로 적용이 되지 않으므로 AF 스킴에서 주장했던 것보다 더 좋은 안전성을 가질 수 있을 것으로 보인다.

2. Coron의 공격과 Kiayias-Yung의 공격

PKC 2004에서 Coron은 AF 스킴에 대한 매우 효과적인 공격방법을 제시하였다.[4] Coron의 공격의 핵심은 일변수 다항식의 계수들에 관한 선형방정식을 고려하는 것이다. 좀 더 자세히 설명하면 다음과 같다.

Coron의 AF 스킴에 대한 공격은 Welch-Berlekampf 알고리즘의 변형으로 볼 수 있으며, 평문 m, 공개키 $z=c+E$로부터 얻어지는 암호문과 평문의 관계식

$$y_i = m(x_i) + \alpha z_i + e_i, (i=1, \cdots, n)$$

(단, m, α, e_i 등은 미지수)을 다음과 같은 방정식으로 변환한다.

$$V(x_i)(y_i - \alpha z_i) = V(x_i)m(x_i)$$

단, V는 x_i들 중에서 w개 이하의 점에서만 0이고 그 이외에서는 0의 값을 가지지 않는 다항식이다. (따라서 V는 차수 w 이하의 다항식이다.) 위의 방정식은 다시 다음과 같은 방정식으로 변환된다.

$$V(x_i)(y_i - \alpha z_i) = N(x_i)$$

단, N은 차수가 $w+k-2$이하인 다항식이다.

위의 방정식을 V의 계수들 및 N의 계수들에 관한 선형방정식으로 보고 그러한 선형방정식이 non-trivial한 해를 가지도록 하는 미지수 α를 구한다.

그러나 이러한 논리는 제안된 암호 스킴에는 적용될 수 없다. $x_i \in \chi$ 중 w개 이하의 점에서만 0이고 그 이외에서는 0의 값을 가지지 않는 모든 유리함수를 $w+1$개 이하의 고정된 유리함수의 선형결합으로 표현할 수 있는 방법이 없기 때문이다. 따라서 Coron의 공격은 제안된 암호 스킴에는 직접적으로 적용되지 않는다.

Asiacrypt 2004에서는 Kiayias와 Yung이 AF 스킴에서 사용된 매개변수들을 변경한 좀 더 일반적인 암호 스킴 및 이에 대한 공격을 제시하였다. AF 스킴에서 매개변수 w에 대한 조건을 완화하면 Coron의 공격이 적용되지 않는 경우가 존재함을 보이고 이러한 경우의 공격 알고리즘을 제시하였다. 그 공격에서는 다음과 같은 방정식을 고려하였다.

$$\sum_{j_1, j_2 \geq 0,\, j_1 + (k-1) j_2 < l} q_{j_1, j_2} x_i^{j_1} (y_i - \alpha z_i)^{j_2} = 0$$
$$(i = 1, \cdots, n)$$

단, q_{j_1, j_2}들과 α는 미지수이고 $l = n - w - 1$.

그러나 제안된 암호 스킴의 경우 $x_i^{j_1}$에 대응하는 항을 고려하기 힘들다. 본 스킴에서 x_i들은 $\mathbb{F}_q$상의 원소가 아니라 χ상에 있는, 여러 개의 좌표로 이루어진 점이기 때문이다. 따라서 Kiayias-Yung의 공격은 제안된 암호 스킴에 직접적으로 적용되지 않는다.

V. 효율성 분석

제안된 암호 스킴의 효율성은 대수적 함수체 및 대수기하 부호의 선택, 그리고 암호 스킴에 사용된 매개변수 등 많은 요인에 의해 결정된다. 일반적으로 효율성을 논하는 것은 상당히 어려운 일로 보이며 여기에서는 Ⅲ.2절에서 예로 든, 종수 1의 대수기하 부호를 이용한 암호 스킴에 대한 간단한 효율성 분석 결과를 제시한다.

- 암복호화 효율성: 암호화 효율성에 지배적으로 영향을 미치는 연산은 이변수 다항식에 대한 n개의 점에서의 값을 계산하는 것이다. 그러므로 전체적으로 암호화에 필요한 연산은 $O(nk\log_2^2(q))$ 번의 비트연산이다. 반면에 복호화에는 Guruswami-Sudan 리스트 복호 알고리즘이 사용되며 연산의 복잡도는 적당한 작은 자연수 a,b에 대해서 $O(n^3\log^a n\log_2^b(q))$ 비트 연산이다.
- 키 크기: 공개키의 길이는 약 $n\log_2 q$ 비트로 AF 스킴의 경우와 거의 같다. 비밀키의 길이는 AF 스킴의 경우와 마찬가지로 공개키의 길이의 두배이다. 80비트 수준의 안전성을 위해서는 약 80000비트 정도의 공개키가 필요하며 공개키의 크기는 안전성 수준에 거의 비례한다.

Ⅵ. 결 론

본 논문에서는 Augot-Finiasz 공개키 암호 스킴을 수정하고 확장함으로써 알려진 취약성을 제거한 새로운 공개키 암호 스킴을 제안하였다. 제안된 암호 스킴에는 Coron의 공격이나 Kiayias-Yung의 공격이 적용되지 못하며, 키 길이별로 Augot-Finiasz 스킴이 제안된 논문에서 주장했던 안전성을 제공하는 것으로 보인다. 암복호화 효율성의 경우 많은 매개변수가 암호 스킴에 적용된 관계로 일반적인 분석이 어려우며 어떠한 매개변수를 사용하는 것이 최적의 효율성을 제공하는가에 대한 연구가 필요하다

참 고 문 헌

[1] R. McEliece, "A Public-Key Encryption Scheme based on Algebraic Coding Theory," DSN Progress Report, Caltech, pp. 114-116, 1978.

[2] H. Niederreiter, "Knapsack-type encryption scheme and algebraic coding theory", Problems of Control and Information Theory 15(2), pp. 159-166, 1986

[3] D. Augot, M. Finiasz "A Public Key Encryption Scheme Based on the Polynomial Reconstruction Problem", *Eurocrypt 2003*, LNCS 2656, pp. 229-240, 2003

[4] J.-S. Coron, "Cryptanalysis of a public-key encryption scheme based on

the polynomial reconstruction problem", *PKC 2004*, LNCS 2947, pp. 14-27, 2004

[5] A. Kiayias, M. Yung, "Cryptanalyzing the Polynomial-Reconstruction Based Public-Key System Under Optimal Parameter Choice", *Asiacrypt 2004*, LNCS 3329, pp. 401-416, 2003

[6] I. Blake, C. Heegard, T. Hoholdt, V. Wei, "Algebraic Codes", IEEE Trans. Info. Theory 44(6), pp. 2596-2618, 1998

[7] V. Guruswami, M. Sudan, "Improved Decoding of Reed-Solomon and Algebraic-Geometry Codes", IEEE Trans. Info. Theory 45(6), pp. 1757-1767, 1999

[8] R. McEliece, "The Guruswami-Sudan Decoding Algorithm for Reed-Solomon Codes," IPN Progress Report, Caltech, pp. 42-153

[9] S. Gao, M. Shokrollahi, "Computing Roots of Polynomials over Function Fields of Curves", Proceedings of the Annapolis Conference on Number Theory, Coding Theory, and Cryptography, Springer, pp. 214-228, 1999.

〈著者紹介〉

이 정 근 (Jung-Keun Lee) 정회원
1994년 2월: 서울대학교 수학과 졸업
1996년 2월: 서울대학교 수학과 석사
2003년 2월: 서울대학교 수학과 박사
2004년 2월~현재: 국가보안기술연구소 연구원
〈관심분야〉 암호 이론

박 상 우 (Sangwoo Park) 정회원
1989년 2월: 고려대학교 수학교육과 졸업
1991년 8월: 고려대학교 수학과 석사
2003년 2월: 고려대학교 수학과 박사
1991년 8월~1999년 12월: 한국전자통신연구원 선임연구원
2000년 1월~현재: 국가보안기술연구소 선임연구원
〈관심분야〉 암호 이론, 정보보호

김 재 헌 (Jaeheon Kim) 정회원
1991년 2월: 한국과학기술원 수학과 학사
1993년 2월: 서울대 수학과 석사
2000년 8월: 서울대 수학과 박사
2000년 4월~현재: 국가보안기술연구소 선임연구원
〈관심분야〉 정보보호, 대수학