Genus 2인 초타원 암호시스템

김진욱[1°], 전성태[2], 박근수[1]
[1]서울대학교 컴퓨터공학과
e-mail:{cwkim,kpark}@theory.snu.ac.kr
[2]건국대학교 응용수학과
e-mail.sungtae jun@kcucc.cj.konkuk.ac.kr

Hyperelliptic Cryptosystems of Genus 2

Jin Wook Kim[1], Sungtae Jun[2], Kunsoo Park[1]
[1]Department of Computer Engineering, Seoul National University
[2]Department of Applied Mathematics, Konkuk University

요약

타원곡선에 이어 초타원곡선을 공개키 암호시스템에 적용하는 방법이 Koblitz에 의해 제안되었다. 이를 위해 우선 곡선을 선택해야 하는데, 선택될 곡선은 현재까지 알려진 공격에 대해 안전하여야 한다. 본 논문에서는 초타원 암호시스템(hyperelliptic cryptosystem)을 구성하기 위해 genus 2인 초타원곡선 $v^2+v=u^5+u^3+u$와 특성계수(characteristic) 3인 기본 체(field)를 선택하고, 이로써 만들어질 암호시스템이 안전함을 보인다.

1 서론

타원곡선(elliptic curve)을 공개키 암호시스템에 이용하는 방법이 Koblitz[5]와 Miller[10]에 의해 각각 처음 제안되었다. 이 타원곡선 암호시스템은 기존의 시스템에 비해 훨씬 작은 체(field) 상에서 정의가 되어도 기존의 것과 동등한 안전성을 갖는다. 이는 타원곡선 상의 연산이 일반적인 연산보다 복잡하기 때문이다. 이런 이유로 키의 길이가 기존 시스템의 키 길이에 비해 짧아서, 스마트 카드와 같이 작은 메모리로 한정된 곳에서의 사용이 용이하다.

그 후 Koblitz[6]에 의해 타원곡선 대신 초타원곡선(hyperelliptic curve)을 암호시스템에 적용하는 방법이 제안되었다. 초타원곡선(또는 초타원군)은 타원곡선의 일반형으로, 타원곡선보다 더 작은 체 상에서 정의가 가능하다. 즉, 초타원 암호시스템에서는 타원곡선 암호시스템보다 키 길이가 더 짧아질 수 있다.

[13]에서는 몇 가지 초타원곡선에 대해 초타원곡선의 jacobian 군의 위수(order)를 계산하고 안전성을 검사하였다. [13]은 특성계수(characteristic)가 2인 경우만을 다루었는데, genus가 2인 경우에는 안전한 곡선을 찾을 수 없었다. 특성계수 2만을 다룬 이유는 Weil's conjecture에 기반한 위수 계산 방법을 이용하였기 때문인데, 다른 방법을 사용하면 특성계수가 더 큰 경우에 genus 2인 안전한 곡선을 찾을 수 있다고 하였다.

본 논문에서는 특성계수 3에서 genus 2인 곡선 $v^2+v=u^5+u^3+u$의 jacobian 군의 위수를 Weil's conjecture에 기반한 위수 계산 방법을 이용해서 계산하고, 이 곡선이 현재까지 알려진 공격에 대해 안전함을 보인다. 2장에서는 몇 가지 기본적인 정의와 Weil의 정리, 안전성에 대한 관련 연구를 알아보고, 3장에서는 위수 계산 방법과 선택한 곡선에서의 계산 결과를 알아본다. 4장에서는 3장에서 구한 결과의 안전성을 확인하고, 5장에서 결론과 앞으로의 할 일을 제시한다.

2 관련 연구

타원곡선 암호시스템은 주어진 유한체에서 유리점들이 일정한 법칙에 의하여 가환군이 되는 사실을 이용하여 구성된다. 이에 비하여 초타원곡선은 단순한 유리점들의 집합으로 가환군이 되지않고 유리점들에서 jacobian 군을 생각하면 가환군을 얻을 수 있다. 이러한 초타원곡선의 jacobian 군에서 이산로그 문제를 생각하는것이 초타원곡선을 이용한 암호시스템의 핵심이다. 자세한 정의는 [7]를 참조하고, 여기에서는 간단한 정의만 소개하기로 한다.

2.1 정의

정의 1 임의의 체 $\mathbf{F}$상의 *genus* g인 초타원곡선 C는 $v^2+h(u)v=f(u)$로 정의된다. 단, $h(u)\in\mathbf{F}[u]$는 차수가 g를 넘지 않는 다항식이고, $f(u)\in\mathbf{F}[u]$는 차수가 $2g+1$이며 최고차항의 계수가 1인 다항식이다. 또한, C상에 있는 (x,y)는 $2y+h(x)=0, h'(x)y-f'(x)=0$을 동시에 만족하지 않는다.

정의 2 *Divisor* D는 $D=\sum m_iP_i$로 정의된다. 단, P_i는 곡선 C상의 점이고, $m_i\in\mathbf{Z}$이다. *Divisor* D의 차수*(degree)*는 $\sum m_i$로 정의되고, 차수 *0*인 *divisor*들의 집합은 군이 되며 $\mathbf{D}^0$로 쓴다.

정의 3 곡선 C의 *jacobian* $\mathbf{J}$는 $\mathbf{J}=\mathbf{D}^0/\mathbf{P}$로 정의되며 군이다. 단, $\mathbf{P}$는 *principal divisor*로 $\mathbf{D}^0$의 부분군이다.

유한체 $\mathbf{F}_{q^n}$에서 정의된 곡선 C의 jacobian 군에서 두 개의 divisor D_1, D_2가 주어져 있을 때, $D_2=mD_1$인 정수 m을 찾는 것이 초타원 곡선의 jacobian 군에서의 이산로그문제이다.

2.2 Weil의 정리[7]

정의 4 C를 $\mathbf{F}_q$상에서 정의된 초타원곡선이라고 하고, M_r을 $\mathbf{F}_{q^r}$ 상에서 정의된 C의 점의 개수라고 하자. C의 *zeta*-함수는 다음과 같이 정의된다.

$$Z(C/\mathbf{F}_q;T) = e^{\sum_{r\geq 1} M_r T^r/r}$$

정리 1 (Weil) C를 $\mathbf{F}_q$상에서 정의된 초타원곡선이라고 하고, $Z(C/\mathbf{F}_q,T)$를 C의 *zeta*-함수라고 하자. 그리고, N_r은 체 $\mathbf{F}_{q^r}$ 상에서 정의된 *jacobian* 군의 위수를 나타낸다고 하자.

1) $Z(C/\mathbf{F}_q;T)$는 다음과 같이 표현된다.

$$Z(C/\mathbf{F}_q,T) = \frac{P(T)}{(1-T)(1-qT)}.$$

단, $P(T)$는 정수계수를 갖는 다음 $2g$차 다항식이다.

$$\begin{aligned} P(T) &= 1 + a_1 T + \quad + a_{g-1}T^{g-1} + a_g T^g \\ &\quad + qa_{g-1}T^{g+1} + \quad + q^{g-1}a_1 T^{2g-1} + q^g T^{2g} \end{aligned}$$

2) $P(T)$는 다음과 같이 인수분해된다.

$$P(T) = \prod_{i=1}^{g}(1-\alpha_i T)(1-\overline{\alpha}_i T)$$

단, α_i는 $|\alpha_i| = \sqrt{q}$인 복소수이고, $\overline{\alpha}_i$는 α_i의 켤레복소수이다

3) N_r은 다음과 같다

$$N_r = \prod_{i=1}^{g}|1-\alpha_i^r|^2 \qquad (1)$$

2.3 안전성

초타원군에서의 이산로그문제를 풀기 위한 방법으로는 baby-step giant-step 방법[11], Pohlig-Hellman 방법[12], Frey의 MOV-공격[1] 일반화 방법[2], Adleman-DeMarrais-Huang 방법[8] 등이 있다

Baby-step giant-step 방법은 군의 위수가 n일 때 $O(\sqrt{n})$의 공간과 최악의 경우 $O(\sqrt{n}\log\sqrt{n})$의 시간이 필요한 방법이다[9]. 큰 소인수를 가질수록 시간이 최악에 가까워진다.

Pohlig-Hellman 방법은 군의 위수를 소인수분해 했을 때, 각각의 부분군에서 이산로그를 구한 뒤 중국인의 나머지 정리를 적용하는 방법이다[9]. 이 때 큰 소인수를 가진다면 큰 이점이 없다

Frey의 MOV-공격 일반화 방법은 초타원군을 체 $\mathbf{F}_{q^n}$으로 imbed시키는 방법을 이용한다.[13] 하지만 큰 소인수가 $(q^n)^k-1$을 나누지 못한다면 적용할 수 없다.

Adleman-DeMarrais-Huang 방법은 큰 genus의 곡선에 적용되는 준지수시간(subexponential-time) 알고리즘이다.

3 jacobian 군의 위수 계산

Weil의 정리에서 임의의 r에 대해 N_r을 구하려면 우선 a_r들을 구해서 $P(T)$를 구하고, 이를 인수분해해서 $\alpha_i, \overline{\alpha}_i$를 구한뒤 식 (1)을 이용하면 된다.

Genus 2인 경우에 다음의 과정을 통해서 N_r을 구할 수 있다[7].

1. 전체 탐색(exhaustive search)으로 M_1, M_2를 구한다.
2. $a_1 = M_1 - 1 - q$, $a_2 = (M_2 - 1 - q^2 + a_1^2)/2$
3. $X^2 + a_1 X + (a_2 - 2q) = 0$의 두 근 γ_1, γ_2를 구한다
4. $X^2 - \gamma_1 X + q = 0, X^2 - \gamma_2 X + q = 0$의 각각의 근 α_1, α_2를 구한다
5. $N_r = |1-\alpha_1^r|^2 \cdot |1-\alpha_2^r|^2$

여기서 마지막의 N_r을 다음과 같이 바꿀 수 있다

$$\begin{aligned} N_r &= |1-\alpha_1^r|^2 \cdot |1-\alpha_2^r|^2 \\ &= (1-\alpha_1^r)(1-\overline{\alpha}_1^r)(1-\alpha_2^r)(1-\overline{\alpha}_2^r) \\ &= (1-A_r+q^r)(1-B_r+q^r) \end{aligned}$$

단, $A_r = \alpha_1^r + \overline{\alpha}_1^r$, $B_r = \alpha_2^r + \overline{\alpha}_2^r$이다. A_r, B_r은 다시 점화식으로 나타낼 수 있다.(B_r은 A_r과 같은 모양이다.)

$$A_r = \begin{cases} A_1^r - \sum_{i=1}^{\frac{r}{2}} q^i \binom{r}{i} A_{r-2i}, & r\text{은 짝수} \\ A_1^r - \sum_{i=1}^{\frac{r-1}{2}} q^i \binom{r}{i} A_{r-2i}, & r\text{은 홀수} \end{cases}$$

단, $A_0 = 1, A_1 = \alpha_1 + \overline{\alpha}_1 = \gamma_1$이다.

이로써 모든 α를 q와 γ로 바꿀 수 있었다 즉, 4번 단계를 생략할 수 있고, 따라서 복소수 계산 없이 실수 계산만으로 N_r을 구할 수 있다.

이 방법으로 C를 $v^2 + v = u^5 + u^3 + u$로, q는 3으로 정한 뒤 $2 \leq r \leq 500$인 r에 대해 N_r을 계산하였다. Ultra SPARC-1, 128MB RAM에 Solaris 2.6 운영체제에서 C 언어를 이용하여 구현하였고, 큰 수의 계산을 위해서 SIMATH[3]라는 수학 라이브러리를 이용하였다

r	길이†	N_r
13	41	2546017644580
19	60	1350962757723448580
41	129	1330279464106516066870600865836318965620
73	231	456775907450774037382416240137522401508913781641165797624588922380976
500	1584	1322078194808066368904552597521443659654220327521481676649203682268285973467048995407783138506080619639097776968725823288833499027844133949073916233579719810804745967498242126449039026059144517378680906152209403550892169233337420560373105790494595975551734662515996402024809038964331250382788136008044260513542995952537343750574085239075865577689713697011668069616371942771173934307383361733485366479653012240594053647161341650077996329641582274534788453050978001562500000000

† N_r을 2진수로 나타냈을 때 bit 수.

표 1. N_r 계산 결과

4 안전성

앞에서 구한 N_r들은 현재까지 알려진 공격방법들에 대한 안전성이 보장된 후 사용되어야한다. 안전성은 아래 조건을 통해 확인할 수 있다

다음 세 가지 조건을 모두 만족하는 r은 안전하다.[13]

1 N_r이 큰 소수로 나누어 진다.

2 N_r의 가장 큰 소인수가 $k < (\log q^r)^2$인 모든 k에 대해 $(q^r)^k - 1$을 나누지 않는다

3 $2g + 1 \leq \log q^r$

먼저 **3**을 보면, $2g + 1 = 2 \ \ 2 + 1 = 5 = \log 2^5 \leq \log 3^r$, $r \geq \log_3 32 \approx 3\ 1546$이다 즉, $r \geq 4$인 r은 조건을 만족한다

다음 **1**을 확인하기위해 N_r들을 소인수분해 해보았다. 그 결과 상당수의 N_r이 작은 소수들의 곱으로 이루어져 있었지만, 충분히 큰 소수를 갖는 것들도 있었다. 소인수분해는 SIMATH[3]와 GAP[4]의 루틴을 이용하였는데, 이 루틴에는 타원곡선 방법과 Pollard-ρ 방법이 포함되어 있다.

r	N_r 길이†	가장 큰 소인수 길이†
41	129	116
61	193	140
73	231	165
79	250	220
81	256	172
113	358	329
241	763	718
439	1391	1336
457	1448	1423
463	1467	1463

†2진수로 나타냈을 때 bit 수

표 2. N_r 소인수분해 결과

r이 $82 \leq r \leq 500$의 범위에서는 단지 10개에 대해서만 소인수분해를 할 수 있었다.[1]

마지막으로 **2**를 표 2의 r들에 대해서 확인해 보았다 확인 결과, 모든 r이 조건을 만족하였다. 실험은 SIMATH를 이용한 C 언어를 이용하였다

이상으로, 선택된 곡선은 세 가지 조건을 모두 만족하고, 따라서 안전하다.

5 결론

본 논문에서는 특성계수가 3인 경우 genus 2인 초타원곡선 $v^2 + v = u^5 + u^3 + u$의 위수를 Weil의 정리를 이용한 위수 계산 방법을 통해 구하고, 그 결과들이 안전함을 확인하였다 향후 본 연구의 결과들을 토대로 안전한 암호시스템을 구현할 예정이다.

참고문헌

[1] A. J. Menezes, T. Okamoto and S. A. Vanstone. Reducing elliptic curve logarithm to logarithm in a finite field *IEEE Transactions on Information Theory*, 39.1639–1646, 1993.

[2] G. Frey and H G Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 62:865–874, 1994

[3] SIMATH group and Siemens AG *SIMATH — SInix-MATHematik*, 1998. Universität des Saarlandes in Saarbrücken, Germany (ftp://ftp.math.uni-sb.de/pub/simath).

[4] The GAP Group. *GAP — Groups, Algorithms, and Programming* Version 4b5 School of Mathematical and Computational Sciences, University of St Andrews, North Haugh, St Andrews, Fife KY16 9SS, Scotland. and Lehrstuhl D fur Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany., 1998

[5] N Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48·203–209, 1987.

[6] N Koblitz. Hyperellitic cryptosystems. *Journal of Cryptology*, 1:139–150, 1989.

[7] N. Koblitz. *Algebraic Aspects of Cryptography* Springer, 1998.

[8] L. M Adleman, J. DeMarrais and M. Huang A subexponential algorithm for discrete logarithm over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields. In *Proc. of ANTS1*, volume 877 of *LNCS*, pages 28–40 Springer-Verlag, 1994.

[9] A Menezes. *Elliptic Curve Public Key Cryptosystems* Kluwer Academic Publishers, 1993.

[10] V. Miller Uses of elliptic curves in cryptography. In *CRYPTO '85*, LNCS, pages 417–426. Springer-Verlag, 1986

[11] A Odlyzko. Discrete logarithm and their cryptographic significance. In *EUROGRYPTO '84*, LNCS, pages 224–314 Springer-Verlag, 1985.

[12] S C Pohlig and M. E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance *IEEE Transactions on Information Theory*, 24:106–110, 1978.

[13] Y. Sakai, K Sakurai and H. Ishizuka. Secure hyperelliptic cryptosystems and their performance In *Public Key Cryptosystem*, volume 1 of *LNCS*, pages 164–181 Springer-Verlag, 1998.

[1] 84, 112, 113, 120, 128, 144, 241, 439, 457, 463