Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.3, Jun. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.3.567

Brezing-Weng 다항식족을 이용한 페어링 친화 아벨 곡면의 CM 파라미터 생성법*

윤 기 순,[1†] 박 영 호,[2‡] 장 남 수[2]
[1]엔에스에이치씨, [2]세종사이버대학교

A generating method of CM parameters of pairing-friendly abelian surfaces using Brezing-Weng family*

Kisoon Yoon,[1†] Young-Ho Park,[2‡] Nam Su Chang[2]
[1]NSHC, [2]Sejong Cyber University

요 약

Brezing과 Weng은 페어링 친화 타원곡선의 CM 파라미터들을 수체(number field)의 다항식 표현을 이용하여 생성하는 방법을 제안하였고, Freeman은 그 방법을 아벨 다양체(abelian variety)의 경우로 일반화 시켰다. 본 논문에서는 특히 단순 아벨 곡면(simple abelian surface)의 경우에 대해 Brezing-Weng 방법에서 사용되는 다항식족(polynomial family)을 구하는 새로운 공식들을 유도하고, 이를 이용하여 CM 파라미터들을 생성할 수 있음을 보인다.

ABSTRACT

Brezing and Weng proposed a method to generate CM parameters of pairing-friendly elliptic curves using polynomial representations of a number field, and Freeman generalized the method for the case of abelian varieties. In this paper we derive explicit formulae to find a family of polynomials used in Brezing-Weng method especially in the case of abelian surfaces, and present some examples generated by the proposed method.

Keywords: abelian variety, Brezing-Weng method, pairing-based cryptography, complex multiplication

I. 서 론

Brezing과 Weng은 수체의 다항식 표현을 이용하여 페어링 친화 타원곡선의 CM 파라미터를 생성하기 위한 다항식족(family of polynomials)을 찾는 방법을 제안했고, Freeman[3], Yoon[4] 등이 이 아이디어를 응용하여 효율적인 다항식족들을 찾아냈다. 페어링 암호의 가용성을 높이기 위해 종수(genus)가 1 이상인 아벨 다양체(abelian variety)를 이용하는 것이 가능하며, 특히 종수가 2인 아벨 곡면의 경우 그 암호학적인 가치가 커 많은 연구가 필요하다. Streng, Stevenhagen, Freeman[1]은 중국인의 나머지 정리와 타입노름을 이용하여 페어링 친화 아벨 다양체의 CM 파라미터를 구하는 방법을 제안했고, Freeman[2]은 유사한 아이디어를 이용하여 Brezing-Weng 방법을 아벨 다양체의 경우로 일반화 했다. 본 논문에서는 페어링 친화 아벨 곡면의 CM 파라미터를 생성하는 Brezing-Weng 다항식족을 찾아 내는 새로운 공식을 제안하고, 이를 이용하여 생성

접수일(2015년 3월 31일), 게재확정일(2015년 4월 27일)
* 이 논문은 2014년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2013R1A1A2013340)
† 주저자, kisoon.yoon@gmail.com
‡ 교신저자, youngho@sjcu.ac.kr(Corresponding author)

된 예제들을 보인다.

II. 아벨 다양체

차수 $2g$인 수체 M이 g차 전적 실확장체(totally real extension field)의 전적 복소이차확장체(totally imaginary quadratic extension field)일 때 M을 *CM 체(CM field)*라 한다. A가 p개의 원소를 가지는 유한체 F_p 상에서 정의되는 g차원 단순 아벨 다양체(simple ordinary abelian variety)라 하자. A의 프로베니우스 자기준동형사상의 특성다항식을 *p-Weil 다항식*이라 하며 그 근은 절대값이 p인 대수적 정수로서 *p-Weil 수*라 부른다. 이때 $M:=End(A)\otimes Q$은 기약인 p-Weil 다항식을 최소다항식으로 가지는 CM 체가 된다. Tate-Honda 이론에 의해 하나의 p-Weil 다항식, 즉 p-Weil 수의 켤레류(conjugacy class)는 하나의 아벨 다양체의 등원류(isogeny class)에 대응하며 p-Weil 수를 하나 찾아내면 그에 대응하는 아벨 다양체를 CM 방법으로 구할 수 있다[1, 2, 5].

L을 g차원 CM 체 M의 정규폐체(normal closure), $G:=Gal(L/Q)$, H는 $L^H=M$인 G의 부분군이라 하자. 이 때 G/H의 서로 켤레가 아닌 g개의 원소들의 집합 $\Phi=\{\phi_1,\cdots,\phi_g\}$에 대해 (M,Φ)를 *CM 타입*이라 한다. $S=\{\sigma\in G:\sigma|_M\in\Phi\}$, $\hat{S}=\{\sigma^{-1}\in G:\sigma\in S\}$, $\hat{M}$은 G의 부분군 $\hat{H}=\{\gamma\in G:\gamma S=S\}$에 의해 고정되는 L의 부분체, 그리고 $\Psi=\hat{S}/\hat{H}\subseteq G/\hat{H}$ 라 하자. 그러면 $(\hat{M},\Psi)$는 CM 타입이며, (M,Φ)의 *반사타입(reflex type)*이라고 부르고, $\hat{M}$을 M의 *반사체(reflex field)*라 부른다. 어떤 CM 타입이 진부분 CM 타입을 가지지 않는 경우 *원시적(primitive)*이라 하며 그것은 단순 아벨 다양체에 대응된다. *타입노름(type norm)* $N_\Phi:M\to L$ 은 $\xi\mapsto\prod_{i=1}^{g}\phi_i(\xi)$로서 정의된다. 특히 $N_\Phi(M)\subseteq\hat{M}$이고 $N_\Psi(\hat{M})\subseteq M$라는 사실이 성립한다.

r을 어떤 소수라 하자. A가 주양극화된(principally polarized) 아벨 다양체라면, A는 $A[r]\times A[r]$에서 $\mu_r=\{\alpha\in\overline{F_p}:\alpha^r=1\}$로 가는 비퇴화 쌍선형 페어링 사상(non-degenerate bilinear pairing map)을 가진다. r이 $|A(F_p)|$를 나누고 $p(p-1)$과 서로소라 할 때, 주어진 자연수 k가 F_r^*에서 p의 위수이면 $A[r]\subseteq A(F_{p^k})$가 된다[1,2]. A가 페어링 친화적이기 위해서는 큰 r과 작은 k에 대해 이 조건이 성립하면 된다. 이 조건은 A에 대응하는 p-Weil 수를 π라 할 때 (i) $r|N_{M/Q}(\pi-1)$, (ii) $r|\Phi_k(p)$와 같이 다시 쓸 수 있다. 여기에서 $\Phi_k(x)$는 k번째 원분다항식(cyclotomic polynomial)이다.

III. 아벨 곡면에 대응하는 CM 체들

아벨 곡면의 경우 $g=2$이므로 최대실이차체 $M_+=Q(\sqrt{D})$를 포함하는 4차의 CM 체 M을 고려한다. 여기서 D는 제곱 없는 양의 정수이다. $\varphi(\sqrt{D})=-\sqrt{D}$일 때 $Gal(M_+/Q)=\{1,\varphi\}$라 하자. 정수 a와 영이 아닌 정수 b에 대하여 M_+의 원소 $\delta:=a+b\sqrt{D}>0$가 $\delta^\varphi>0$를 만족한다고 하자. 또한 유리수 c와 제곱 없는 양의 정수 $E\neq1$에 대하여 $\delta\delta^\varphi=Ec^2$가 된다고 하고, $\eta=i\sqrt{\delta}$, $\eta_*=i\sqrt{\delta^\varphi}$라 하자. 그러면 $M=Q(\eta)$이다. M의 임의의 p-Weil 수는 $\pi=(t+\eta y)/2$ ($t\in O_{M_+}$, $y\in M_+$)와 같이 쓸 수 있고, $\pi\overline{\pi}=(t^2+\delta y^2)/4\in Z$이며 그 p-Weil 다항식은 $C=(x^2-tx+p)(x^2-t^\varphi+p)$이다. G의 원소들 τ, σ, ρ 를 다음과 같이 정의하자: $\eta^\sigma=\eta_*$, $\eta_*^\sigma=-\eta$, $\eta^\rho=\eta_*$, $\eta_*^\rho=\eta$. 상기 가정 하에 M은 다음 두 가지 유형으로 분류된다. 특별히 혼동이 없는 경우 G/H와 $G/\hat{H}$의 원소들을 G의 원소처럼 표기한다.

(A) M/Q는 갈루아, $D=E$, $L=M$, $G=\langle\sigma\rangle$, $H=\hat{H}=\{1\}$; $(M,\{1,\sigma\})$는 원시 CM 타입이고 그 반사타입은 $(M,\{1,\sigma^3\})$.

(B) M/Q는 비갈루아, $D\neq E$, $L=M(\eta_*)$, $G=\langle\sigma,\rho\rangle$, $H=\{1,\rho\sigma\}$, $\hat{H}=\{1,\rho\}$; $(M,\{1,\sigma\})$은 원시 CM 타입이고 반사타입은 $(Q(\eta+\eta_*),\{1,\sigma^3\})$.

참고로, 4차 CM 체 중 $G\cong Z/2Z\oplus Z/2Z$인 유형은 원시 CM 타입을 가지지 않으므로 논외로 한다.

IV. 다항식족 구하기

$(\hat{M},\Psi:=\{1,\psi\})$은 CM 타입, M을 그 반사체라 하자. π의 켤레 중 하나를 고려하므로 (A)형과 (B)형의 경우 모두 $\psi=\sigma^3$으로 고정한다. M과 $\hat{M}$의 최대실이차체는 각각 $M_+=Q(\sqrt{D})$와 $\hat{M}_+=Q(\sqrt{E})$

이다. k는 주어진 임베딩 차수, ζ_k는 1의 k번째 원시근이라 하자. K는 L과 ζ_k를 포함하는 최소체이고, K/Q은 갈루아 확장이라 하자. K/Q의 최소다항식 r이 R, $R^{\varphi} \in M_+[x]$에 대해 $r = RR^{\varphi}$과 같이 인수분해 된다고 하자. 그러면 $Q[x]/(r) \cong M_+[x]/(R) \cong M_+[x]/(R^{\varphi})$이므로 K의 원소들은 R (또는 R^{φ})을 법으로 하여 $M_+[x]$의 다항식으로 표현 가능하다. 지금부터 체 K의 원소 γ의 r, R, R^{φ}를 법으로 하는 다항식 표현을 각각 $[\gamma]_r$, $[\gamma]_R$, $[\gamma]_{R^{\varphi}}$로 표기하자. $\theta = \eta + \eta_*$라 놓자. 그러면 $\theta^{\psi} = \eta - \eta_*$이다. $\widehat{M}[x]$의 원소 $\xi = U + V\theta$ ($U, V \in \widehat{M_+}[x]$)에 대해 $\pi = N_{\Psi}(\xi)$라 놓자. 그러면 타입노름의 성질에 의해 $\pi \in M[x]$이다. 또 $M_+[x]$의 원소들 $T = 2(UU^{\psi} + VV^{\psi}\theta\theta^{\psi})$, $Y = 2(U^{\psi}V\theta + UV^{\psi}\theta^{\psi})/\eta$에 대해 $\pi = (T + Y\eta)/2$로 쓸 수 있고, $p = \pi\overline{\pi} = (T^2 + \delta Y^2)/4 = N_{\Psi}(\xi)\,\overline{N_{\Psi}(\xi)} = N_{M/Q}(\xi) \in Q[x]$이다. 이제 다음 방정식들

$$T \equiv [\zeta_k + 1]_R,\ Y \equiv [(\zeta_k - 1)/\eta]_R \pmod{R},$$

$$T \equiv [\zeta_k + 1]_{R^{\varphi}},\ Y \equiv [(\zeta_k - 1)/\eta]_{R^{\varphi}} \pmod{R^{\varphi}}$$

을 만족시키는 다항식들 U, $V \in M_+[x]$를 찾아내면 다항식 $p \in Q[x]$가 조건 $\Phi_k(p) = 0 \pmod{r}$을 만족시킨다. $U = u_1 + u_2\sqrt{E}$, $V = v_1 + v_2\sqrt{E}$ (u_1, u_2, v_1, $v_2 \in Q[x]$)라 놓자. 그리고 다항식 변수들 f_1, f_2, g_1, $g_2 \in Q[x]$들을 다음과 같이 놓을 때,

$$f_1 = u_1^2 - Eu_2^2,\ f_2 = v_1^2 - Ev_2^2,$$

$$g_1 = (u_1 - u_2\sqrt{E})(v_1 + v_2\sqrt{E}),$$

$$g_2 = (u_1 + u_2\sqrt{E})(v_1 - v_2\sqrt{E}),$$

다음을 만족시키는 u_1, u_2, v_1, $v_2 \in Q[x]$를 찾는다.

$$f_1 - 2bf_2\sqrt{D} = \left[\frac{\zeta_k + 1}{2}\right]_R \pmod{R},$$

$$f_1 - 2bf_2\sqrt{D} = \left[\frac{\zeta_k + 1}{2}\right]_{R^{\varphi}} \pmod{R^{\varphi}},$$

$$[g_1\theta + g_2\theta^{\psi}]_R = \left[\frac{\zeta_k - 1}{2}\right]_R \pmod{R},$$

$$[g_1\theta + g_2\theta^{\psi}]_{R^{\varphi}} = \left[\frac{\zeta_k - 1}{2}\right]_{R^{\varphi}} \pmod{R^{\varphi}}.$$

모든 변수들을 $Q[x]/(r)$에서 찾으면 충분하므로 방정식들의 계수들 $\sqrt{D}$, $[\sqrt{E}]_R$, $[\theta]_R$, $[\theta^{\psi}]_R$을 각각 $[\sqrt{D}]_r$, $[\sqrt{E}]_r$, $[\theta]_r$, $[\theta^{\psi}]_r$로 바꾸어 얻어진 방정식들을 r을 법으로 하여 풀면 된다. 방정식의 해는 다음 정리를 이용하여 구할 수 있다.

정리 1. 상기한 방정식의 일반해 $(\bmod r)$ 는 다음과 같다. (u_{10}, u_{20})가 $u_1^2 - Eu_2^2 = 0 \pmod{r}$의 한 해일 때,

(i) $u_{10} + u_{20}[\sqrt{E}]_r \neq 0$인 경우 $w_1^2 - Dw_2^2 \neq 0$이고 $\lambda \neq 0, -1$인 K의 원소들 w_1, w_2와 λ에 대해

$$f_1 = \left[(1/\lambda + 1 + (\lambda + 1)\zeta_k)/4\right]_r,$$

$$f_2 = \left[1/\lambda - 1 + (\lambda - 1)\zeta_k)/(8b\sqrt{D})\right]_r,$$

$$g_1 = \left[(-1/\lambda - 1 + (\lambda + 1)\zeta_k)/(4\theta)\right]_r,$$

$$g_2 = \left[(1/\lambda - 1 - (\lambda - 1)\zeta_k)/(4\theta^{\psi})\right]_r,$$

$$v_1 = \left[-\frac{2(w_1^2 v_{10} - Ew_1 w_2 v_{20})}{(w_1^2 - Ew_2^2)} + v_{10}\right]_r,$$

$$v_2 = \left[-\frac{2(w_1 w_2 v_{10} - Ew_2^2 v_{20})}{(w_1^2 - Ew_2^2)} + v_{20}\right]_r,$$

$$u_1 = \left[\frac{f_1(v_1 + v_2\sqrt{E})}{2g_1} + \frac{g_1}{2(v_1 + v_2\sqrt{E})}\right]_r,$$

$$u_2 = \left[\frac{f_1(v_1 + v_2\sqrt{E})}{2g_1\sqrt{E}} - \frac{g_1}{2(v_1 + v_2\sqrt{E})\sqrt{E}}\right]_r.$$

(ii) $u_{10} + u_{20}[\sqrt{E}]_r = 0$인 경우 0이 아닌 K의 원소 λ에 대해

$$u_1 = [u_{10} + \lambda]_r,\ u_2 = [u_{20} - \lambda/\sqrt{E}]_r,$$

$$v_1 = [\lambda f_2/g_1 + g_1/(4\lambda)]_r,$$

$$v_2 = -[\lambda f_2/(g_1\sqrt{E}) + g_1/(4\lambda\sqrt{E})]_r,$$

$$f_1 = [0]_r,\ f_2 = [-(\zeta_k + 1)/(4b\sqrt{D})]_r,$$

$$g_1 = [(\zeta_k - 1)/(2\eta)]_r,\ g_2 = [0]_r.$$

증명.[5]의 4장을 참조하라. □

V. 예 제

CM 체가 (A)형인 경우 IV절의 방정식과 해의 기호들을 $\theta \to \eta$, $b \to c/2$, $E \to D$로 바꾸어 적용시켜도 무방하다. 체가 (B)형인 경우에는 기호들을 그대로 적용시킨다. g차원 아벨 다양체의 경우 다항식족의 효율성 척도는 $\rho_x = g\dfrac{\deg p(x)}{\deg r(x)}$ 로 정의한다[1,2].

1. (A)형, $k=3$, $\eta=i\sqrt{2+\sqrt{2}}$, $\gamma=(1-\sqrt{2})\eta\zeta_3$일 때 K 원시원소 γ의 최소 다항식은 $r=x^8-4x^6+14x^4-8x^2+4$이다. 정리 1의 (i)에서 $\lambda=-1/\zeta_3$, $w_1/w_2=\frac{(1+4\eta)}{1-4\eta}\sqrt{2}$로 놓으면 다음을 얻는다.

$$\pi=\frac{1}{196}(2x^{12}-21x^8+164x^6-294x^4+168x^2-68)+\frac{1}{25088}(-356x^{14}+2044x^{12}-11529x^{10}+28236x^8-63294x^6+35000x^4-1028x^2)\sqrt{2}+\frac{1}{1568}(-22x^{13}+21x^{11}-42x^9-684x^7+224x^5+336x^3+216x)(\eta+\eta_*)+\frac{1}{3136}(16x^{13}+70x^{11}-497x^9+2544x^7-3794x^5+2800x^3-404x)\sqrt{2}(\eta-\eta_*)$$

이 때 $\rho_x=7$이다.

2.(A)형, $k=2$, $\eta=i\sqrt{5+\sqrt{5}}$, $\gamma=(-1-(1+\sqrt{5})\eta)\zeta_2$일 때 정리 1의 (i)에서 $\lambda=-1/\zeta_2$, $w_1/w_2=\frac{1+4\eta}{1-4\eta}\sqrt{5}$로 놓으면 $\rho_x=6$인 다항식족을 얻는다.

3.(B)형, $k=2$, $\eta=i\sqrt{3+\sqrt{3}}$, $\gamma=(1-\sqrt{3}+\eta+\eta^\sigma)\zeta_2$일 때 정리 1의 (i)에서 $\lambda=-1/\zeta_2$, $w_1/w_2=\frac{1+4\eta}{1-4\eta}\sqrt{6}$로 놓으면 $\rho_x=7$인 다항식족을 얻는다.

VI. 결 론

본 논문에서는 페어링 친화 아벨 곡면의 CM 파라미터를 생성하기 위한 Brezing-Weng 다항식족을 찾는 새로운 공식을 유도했다. 제안된 방법을 이용하면 체 K의 원시원소 γ와 자유변수들 λ, w_1, w_2을 변화시키며 다양한 다항식족을 생성할 수 있고, 이를 이용하여 생성된 ρ_x값이 6~7인 다항식족들을 생성해 보았다. 앞으로 이 결과를 이용하여 더 낮은 ρ_x값을 가지는 다항식족을 생성할 수 있을 것으로 기대된다.

References

[1] D. Freeman, "A generalized Brezing-Weng algorithm for constructing pairing-friendly ordinary abelian varieties," Algorithmic Number Theory, LNCS vol. 5029, pp. 60-73, Oct. 2008.

[2] D. Freeman, P. Stevenhagen and M. Streng, "Abelian varieties with prescribed embedding degree," Pairing-Based Cryptography - Pairing 2008, LNCS vol. 5011, pp. 60-73, May. 2008.

[3] D. Freeman, M. Scott and E. Teske, "A Taxonomy of Pairing-Friendly Elliptic Curves," J. Cryptology vol. 23, no. 2, pp. 224-280, Apr. 2010.

[4] K. Yoon, "A new method of choosing primitive elements for Brezing - Weng families of pairing-friendly elliptic curves," J. Mathmatical Cryptology vol 9, no. 1, pp. 1-9, Mar. 2015.

[5] K. Yoon, "Construction de courbes elliptiques et de surfaces abéliennes adaptées à la cryptographie à couplage," PhD thesis, Université de Caen Basse-Normandie Nov. 2013.

〈저자소개〉

윤 기 순 (Kisoon Yoon) 정회원
1998년 8월: 경희대학교 수학과 이학사
2007년 8월: 고려대학교 정보보호학과 공학석사
2013년 11월: Université de Caen 수학과 이학박사
2013년 11월~현재: 엔에스에이치씨 암호기술팀 팀장
〈관심분야〉 정수론, 암호학, 정보보호

박 영 호 (Young-Ho Park) 종신회원
1990년 2월: 고려대학교 수학과 이학사
1993년 2월: 고려대학교 수학과 이학석사
1997년 2월: 고려대학교 수학과 이학박사
2002년 3월~현재: 세종사이버대학교 정보보호학과 교수
〈관심분야〉 공개키 암호, 암호 프로토콜, 부채널 공격, 암호안전성평가

장 남 수 (Nam Su Chang) 정회원
2002년 2월: 서울 시립대학교 수학과 이학사
2004년 8월: 고려대학교 정보보호 대학원 공학석사
2010년 2월: 고려대학교 정보경영공학전문대학원 공학박사
2010년 7월~현재: 세종사이버대학교 정보보호학과 조교수
〈관심분야〉 암호칩 설계 기술, 부채널 공격, 공개키 암호 알고리즘, 공개키 암호 암호분석