SCIS2000 The 2000 Symposium on Cryptography and Information Security
Okinawa, Japan, January 26-28, 2000

Superelliptic Curve を用いた暗号系の構成
Construction of Superelliptic Curve Cryptosystems (Extended Abstract)

久保山 拓* 神尾 一也* 松尾 和人† 趙 晋輝‡ 辻井 重男*
Hiraku Kuboyama Kazuya Kamio Kazuto Matsuo Jinhui Chao Shigeo Tsujii

あらまし 近年，様々な平面代数曲線上で安全な暗号系を構成する研究が盛んに行われている．
最近，Galbraith 達によって superelliptic curve 上の divisor の高速加算方法が提案され，また de Jong, Noot により CM Jacobi 多様体を無限に含む superelliptic curve の family が示されことで，超楕円曲線に比べ，より広い class である superelliptic curve を用いて暗号系を構成することが可能となった．そこで，本論文では superelliptic curve を用いて安全な暗号系を構成する方法を提案する．

キーワード superelliptic curve を用いた暗号系，superelliptic curves，complex multiplication，ordinary lifting

1 まえがき

楕円曲線に比べ，超楕円曲線或はより一般な曲線の Jacobi 多様体上の離散対数問題に基づく暗号系は，安全性の検証や曲線の構成法等がより複雑になっている．その為，必ずしも十分な研究が為されているとは言い難い．更に，近年の計算機演算能力の劇的な向上，楕円・超楕円曲線を用いた暗号系への攻撃法の研究の進展を考えれば，より一般な Jacobi 多様体を用いる暗号系を模索することは必然の流れであろう．

一般な Jacobi 多様体を用いた暗号系の構成を考えた際，2 つの課題がある．即ち，効率的な群演算の方法，そして安全な位数を持つ曲線の構成である．最近，Galbraith, Paulus, Smart [4] により superelliptic curve 上の divisor の高速加算法が示された．また，de Jong, Noot [3] により Jacobi 多様体が CM を持つ曲線（CM 曲線）を無限に含む family が示されている．これによって，超楕円曲線に比べより広い class である，superelliptic curve を用いた暗号系を現実に構築する可能性が示された．

Superellitic curve を用いた暗号系を構成するには安全な位数を持つ曲線が必要不可欠である．曲線の構成法には次の方法が考えられる．

1. Order Counting による構成
2. 数体上の CM 曲線を用いる構成

1. は，アルゴリズムが高次多項式オーダーになる上に安全な位数を持つ曲線が得られるまで繰り返し行わなければならない．

2. の方法は現在，唯一現実的である．この構成法は，素イデアル分解を用いた Weil number の計算による，数体上の CM (Complex Multiplication) を持つ曲線を有限体上に reduction したときの高速な位数設計法 [33] である．即ち，数体上の CM 曲線が与えられれば，この方法を用いて，安全な暗号系を多数，従来の方法よりも極めて高速に構成する事が可能である．

我々は 2. の構成法に着目し，この構成法に用いる為の数体上の CM superelliptic curve を構成する事を目標とする．

CM 超楕円曲線の構成法として Frey, Spallek により提案されている Siegel modular form を用いて invariant [9] を計算する方法（種数 $g = 2$ の場合）[29], [36], そして，小さな有限体から中国人剰余定理を用いて超楕円曲線を lift する構成法 [10], [11] が知られている．一般に $g \geq 3$ の場合，invariant が知られていない為，$g \geq 3$ となる superelliptic curve の構成では invariant を計算する方法は現在のところ不可能である．

そこで本論文では，構成する曲線に種数等の制限がつかないという点と代数演算のみの高速算法である利点

* 中央大学理工学部情報工学科，〒 112-8551 東京都文京区春日 1-13-27，Department of Information and System Engineering, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan
† 東洋通信機株式会社，〒 253-0192 神奈川県高座郡寒川町小谷 2-1-1，Toyo Communication Equipment Co., LTD., 2-1-1 Koyato, Samukawa-machi, Koza-gun, Kanagawa 253-0192, Japan
‡ 中央大学理工学部電気・電子工学科，〒 112-8551 東京都文京区春日 1-13-27，Department of Electrical and Electronic Enginnering, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8851, Japan

を生かし，model lifting による CM superelliptic curve の構成法を提案する．構成は大きく分けて，曲線の探索と lift 後の曲線に対する CM test との 2 つの部分に分けられる．

本構成法では，model として de Jong, Noot により示された family の内，1-parameter のものを用いる．この CM 曲線を豊富に含む family を用いることで CM superelliptic curve を多数構成出来ることが期待される．また，1-parameter の family を用いることで曲線の探索数を大幅に削減することが出来る．

2 Superelliptic Curve

この章では superellipctic curve とその Jacobi 多様体上の加算，そして Jacobi 多様体上に定義される離散対数問題を Galbraith 等 [4] に従って説明する．

2.1 Supereliptic Curve

まず，superelliptic curve を定義する．

定義 1 体 k 上の superelliptic curve を

$$C/k : y^n = c(x) := a_\delta x^\delta + \cdots + a_0$$

と定義する．但し，$n, \delta \geq 3$ とする．また，

$$\gcd(c(x),\, c'(x)) = 1,\ (n,\, \mathrm{char}\, k) = 1,\ (n,\, \delta) = 1$$

を満たすものとする．

このとき C の種数 $g = \frac{1}{2}(n-1)(\delta-1)$ となる．

k が有限体 $\mathbb{F}_q$ であると仮定すると，$(n,\, q-1) = 1$ のとき，$x \in \mathbb{F}_q$ に対して $y \in \mathbb{F}_q$ が必ず存在する．従って，$(n,\, q^j - 1) = 1\ (j = 1, \ldots, g)$ のとき $\#C(\mathbb{F}_{q^j}) = q^j + 1$ となる．このとき，Frobenius endomorphism 特性多項式は $X^{2g} + q^g$ となり superelliptic curve の Jacobi 多様体の位数は $q^g + 1$ になる．

体 k 上の曲線 C の関数体を $K = k(C)$ とする．このとき $(n,\, \mathrm{char}\, k) = 1$ より K は関数体 $k(x)$ の n 次分離拡大となっている．従って，関数体 K の元は

$$\sum_{i=0}^{n-1} a_i(x) y^i \quad (a_i(x) \in k(x))$$

によって表される．また $K/k(x)$ は Galois 拡大であり $\alpha \in K$ の norm は

$$N_{K/k(x)}(\alpha) := \prod_{\sigma \in \mathrm{Gal}(K/k(x))} \sigma(\alpha)$$

で与えられる．

2.2 Divisor の加算

$\mathcal{J}$ を C の Jacobi 多様体, $\mathcal{O}$ を多項式環 $k[x, y]$, $Cl(\mathcal{O})$ を $\mathcal{O}$ のイデアル類群とすると

$$Cl(\mathcal{O}) \cong \mathcal{J}$$

が成り立つ．従って，Jacobi 多様体の divisor の加算は $Cl(\mathcal{O})$ のイデアル類の乗算に置き換えることによって実現可能である．

$\mathcal{O}$ の integral ideal α は basis

$$[\alpha_0, \ldots, \alpha_{n-1}] \quad \left(\alpha_i = \sum_{j=0}^{n-1} a_{ij}(x) y^j,\ a_{ij} \in k[x] \right)$$

を持つ $k[x]$-module となり，行列 $(a_{ij})_{i,\, j=0,\ldots,n-1}$ の Hermite Normal Form (HNF) を計算することにより一意的に表現される．このとき ideal D の次数 $\deg(D)$ は行列の対角要素の積によって与えられる．

ideal α, β の乗算は，互いの basis 間の全ての積

$$[\alpha_0\beta_0, \alpha_0\beta_1, \ldots, \alpha_{n-1}\beta_{n-1}]$$

の行列表現に対して，HNF を計算する事で得られる．

D を $\mathcal{O}$ の ideal とする．このとき $\deg(E) \leq g$ となる D と同値な reduced ideal E が一意に存在する．

この reduced ideal を $Cl(\mathcal{O})$ の元の代表元として計算を進める．reduced ideal は Paulus の関数体上の lattice basis reduction algorithm [21] を用いて求めることができる．

この $Cl(\mathcal{O})$ 上の乗算，即ち $\mathcal{J}$ 上の加算の時間計算量は $O(n^6\delta^2 g^2)$ である．

2.3 離散対数問題

$\mathbb{F}_q$ 上の superelliptic curve C が与えられたとき，楕円・超楕円曲線の場合と同様に superelliptic curve の Jacobi 多様体上の離散対数問題が定義出来る．

Problem 1 (離散対数問題) $\mathbb{F}_q$ 上の superelliptic curve を C，C の Jacobi 多様体を $\mathcal{J}$ とする．与えられた $D_1, D_2 \in \mathcal{J}$ に対して，

$$D_2 = \lambda D_1$$

となる $\lambda \in \mathbb{Z}$ を求める問題を $\mathcal{J}$ 上の離散対数問題と言う．

3 de Jong-Noot Family

この章では，提案する CM superelliptic curve の構成法に用いる，superelliptic curve の family について述べる．

まず，Abel 多様体の CM 体を定義する．

定義 2 A を simple な Abel 多様体，K を数体とする．

$K \subset \mathrm{End}^0(A)$ であり，$[K:\mathbb{Q}] = 2\dim(A)$ となるような K が存在するとき，A は CM を持つと言い，K を A の CM 体と言う．

以下，Jacobi 多様体が CM を持つ曲線を CM 曲線と呼ぶ．

これまで，$\mathbb{C}$ 上の $g \geq 4$ の CM 曲線は有限個であると考えられていた．これに対し，de Jong と Noot は，CM 曲線を無限に含む $\mathbb{C}$ 上の $g = 4, 6$ の superelliptic curve の family を与えた．

定理 1 (de Jong, Noot) [3] 以下で $\mathbb{C}$ 上の曲線の family を定義する:

$$y^3 = x(x-1)(x-\lambda)(x-\mu)(x-\nu) \quad (1)$$
$$y^5 = x(x-1)(x-\lambda) \quad (2)$$
$$y^7 = x(x-1)(x-\lambda) \quad (3)$$

これらの family は各々 CM 曲線を無限に含む．ここで，(1), (2) は $g = 4$，(3) は $g = 6$ である．

ここで，(1), (2), (3) で与えられる family を de Jong-Noot family と呼ぶ事とする．

(1), (2), (3) は各々 superelliptic curve の family であり，これらに含まれる曲線の有限体上への reduction を暗号系に用いる事が可能である．しかしながら，$g \geq 5$ の曲線の Jacobi 多様体上の離散対数問題に対して，実際に baby-step-giant-step 攻撃より高速な攻撃法が，Gaudry[5] によって提案されている．従って，(3) を暗号系の構成に用いる場合には慎重な取り扱いが必用である．

4 Ordinary Lifting による Superelliptic Curve の構成

ここでは de Jong-Noot family を用いた CM superelliptic curve の model lifting による構成法を提案する．

本構成法は model の小さな有限体上への ordinary reduction の CM 体から有限体上で reduction された曲線を選択し，この選択された曲線から中国人剰余定理を用いて model を数体上に lift するものである．一般にこの ordinary lifting を用いた CM 曲線の構成では，幾つかの小さな有限体上で，定義される曲線全てに対してその Jacobi 多様体の CM 体を計算する必要がある [6]．この計算回数は固定した有限体 $\mathbb{F}_q$ に対して $O(q^{2g})$ であり，例え $g = 4$ 程度であっても実際の計算は困難である．

そこで我々は，曲線の model として de Jong-Noot family の (2) や (3) のような 1-parameter family に着目し，model lifting による CM 曲線の構成法を提案してきた [10], [11]．1-parameter family は $\mathbb{F}_q$ に reduction したときの曲線数が q 本であり，曲線構成時の探索曲線数を大幅に削減できる．即ち，計算回数が $O(q)$ となり，現実的に計算可能となる．

しかしながら，これまでに知られていた 1-parameter family は CM 曲線を豊富に含む事が保証されていなかった為，model lifting によって CM 曲線を構成する際に family の探索を必要とした．

本構成法は，CM 曲線を無限に含む de Jong-Noot family 用いる事で，これまでの構成法に比べより確実に CM 曲線を構成できるものである．

Algorithm1 に，de Jong-Noot family を用いた $\mathbb{Q}$ 上の CM superelliptic curve の構成法を示す．

Algorithm 1 (CM curve model の lifting)

step 1. 小さな素数 p_1 を選ぶ．

step 2. 任意の $\lambda \in \mathbb{F}_{p_1}$ を選ぶ．全ての λ を選択済みなら step 1. へ．

step 3. $C/\mathbb{F}_{p_1} : y^5 = x(x-1)(x-\lambda)$ の Jacobi 多様体 $\mathcal{J}$ の p_1-Frobenius endomorphism π_{p_1} の特性多項式 $Z(X)$ を計算する．

step 4. $\mathcal{J}$ が ordinary でなければ step 2. へ．

step 5. $K = \mathbb{Q}(\pi_{p_1})$.

step 6. $T = \{(p_1, \{\lambda\})\}$.

step 7. $\mathcal{J}$ の reflex CM 体 K' を計算する．

step 8. CM 体 K を持つ $\mathcal{J}$ が simple である事をチェックする．simple でないならば step 2. へ．

step 9. $i = 2$.

step 10. K' で完全分解する小さな素数 p_i を選ぶ．

step 11. $T' = \{\}$.

step 12. 任意の $\lambda \in \mathbb{F}_{p_i}$ を選ぶ．

step 13. $C/\mathbb{F}_{p_i} : y^5 = x(x-1)(x-\lambda)$ の Jacobi 多様体 $\mathcal{J}$ の CM 体 K_i を計算する．

step 14. $K_i \cong K$ ならば T' に λ を加える．

step 15. 可能なら新たな $\lambda \in \mathbb{F}_{p_i}$ を選び step 13. へ．

step 16. $T' = \{\}$ ならば step 2. へ．

step 17. T と T' から $\lambda \in \mathbb{Q}$ を中国人剰余定理によって lift する．

step 18. 得られた λ に対して，

$$C/\mathbb{Q} : y^5 = x(x-1)(x-\lambda)$$

として，C に対して CM test を行う．CM test を通る曲線があれば，その曲線を出力して終了．

step 19. T に (p_i, T') を加える．

step 20. $i = i + 1$ とし，step 10. へ．

Algorithm1. の step 3. の $Z(X)$，step 13. の K_i，step 7. の K'，及び step 8. の simplicity テストの詳細は [33] に譲る．

謝辞

本研究を行うにあたり，de Jong-Noot family を御教示賜わりました京都大学数理科学研究所伊原康隆教授に深謝致します．

参考文献

[1] L. M. Adleman and M. D. A. Huang. *Primality Testing and Abelian Varieties over Finite Fields*, Vol. 1512 of *Lecture Notes in Mathematics*. Springer-Verlag, 1992.

[2] Henri Cohen. *A Course in Computational Algebraic Number Theory*, Vol. 138 of *Graduate Texts in Mathematics*. Springer-Verlag, 1993.

[3] Johan de Jong and Rutger Noot. Jacobians with complex multiplication. In *Arithmetic Algebraic Geometry*, Vol. 89 of *Progress in Mathematics*, pp. 177 - 192. Birkhäuser, 1991.

[4] S. D. Galbraith, S. Paulus, and N. P. Smart. Arithmetic on Superelliptic Curves. preprint, 1998.

[5] P. Gaudry, A variant of the Adleman-DeMarais-Huang algorithm and its application to small genera, Technical report, LIX/RR/99/04, Ecole Polytech., 1999.

[6] T. Haga, K. Matsuo, J. Chao, and S. Tsujii. Construction of CM Hyperelliptic Curve using Ordinary Liftings. In *Proceedings of SCIS2000*. IEICE, Symposium on Cryptography and Information Security 2000, C51, 2000.

[7] K. Hashimoto and N. Murabayashi. Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two, In *Tohoku mathematical journal*, Vol. 47, pp. 271 - 296. Mathematical Institute of Tohoku University, second edition, 1995.

[8] Ki-ichiro Hashimoto. On Brumer's family of RM-curves of genus two. Technical Report No. 96-39, Advanced Research Center for Science and Engineering, Waseda University, 1996.

[9] Jun-ichi Igusa. Arithemetic Variety of Moduli for Genus Two. *Ann. of Mathematica*, Vol. 72, No. 3, November 1960. *Printed in Japan.*

[10] K. Kamio, H. Kawashiro, J. Chao, and S. Tsujii. A Fast Algorithm of Model Lifting for CM Hyperelliptic Curves. In *Proceedings of SCIS'99*, Vol. I, pp. 185 - 188. IEICE, Symposium on Cryptography and Information Security 1999, W3-1.6, 1999.

[11] H. Kawashiro, O. Nakamura, J. Chao, and S. Tsujii. Construction of CM hyperelliptic curves using RM families. SCIS'98, 4-1-A, Jan. IEICE Tech. Rep. ISEC97-72, pages 43 - 50, March, 1998.

[12] S. Lang *Abelian Varieties*. Springer-Verlag, reprint edition, 1983.

[13] S. Lang *Complex Multiplication*, Vol. 255 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, 1983.

[14] Jean-Francois Mestre. Courbes hyperelliptiques à multiplications réelles. C. R. Acad. Sci. Paris, t. 307, Série I, p. 721 - 724, 1988.

[15] Jean-Francois Mestre. Construction de courbes de genre 2 a partir de lenurs moddules. In *Effective Methods in Algebraic Geometry*, Vol. 94, Birkhäuser, 1991.

[16] Jean-Francois Mestre. Famillies de courbes hyperelliptiques à multiplications réells. In *Arithmetic Algebraic Geometry*, Vol. 89 of *Progress in Mathematics*, pp. 193 - 208. Birkhäuser, 1991.

[17] D. Mumford. *Tata Lectures on Theta I*, Vol. 28 of *Progress in Mathematics*. Birkhäuser, 1982.

[18] D. Mumford. *Tata Lectures on Theta II : Jacobian Theta Functions and Differential Equations*, Vol. 43 of *Progress in Mathematics*. Birkhäuser, 1982.

[19] D. Mumford. *Abelian Varieties*. No. 5 in Tata Institute of Fundamental Research Studies in Mathematic. Oxford University Press, 2nd edition, 1986.

[20] O. Nakamura, N. Matsuda, J. Chao, and S. Tsujii. Cryptosystems Based on CM Abelian Variety, Technical report, ISEC97-81, 1997.

[21] Sachar Paulus. Lattice basis reduction in function fields. In J. P. Buhler, editor, *Algorithmic Number Theory*, Vol. 1423 of *Lecture Notes in Computer Science*. Third International Symposium, ANTS-III, Springer-Verlag, 1998.

[22] J. Pila. Frobenius maps of Abelian varieties and finding roots of unity in finite fields. In *Mathematics of Computation*, Vol. 55, Number 192, pp. 745 - 763. American Mathematical Society, 1990.

[23] M. Pohst and H. Zassenhaus. *Algorithmic Algebraic Number Theory*. No. 30 in Encyclopedia of Mathematics and Its Applications. Cambridge University Press, first paperback edition, 1997.

[24] Michael E. Pohst. *Computational Algebraic Number Theory*, Vol. 21 of *DMV seminar Band*. Brikhäuser, 1994.

[25] Bjron Poonen. Computational Aspects of Curves of Genus at Least 2. In H. Cohen, editor, *Algorithmic Number Theory*, Vol. 1122 of *Lecture Notes in Computer Science*, pp. 283- 306. Second International Symposium, ANTS-II, Springer-Verlag, 1996.

[26] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Function*, Princeton University Press, 1994. Originally published : Iwanami Shoten, 1971.

[27] G. Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*, Vol. 46 of *Princeton Mathematical Series*. Princeton University Press, 1998.

[28] G. Shimura and Y. Taniyama. Complex multiplication of abelian varieties and its application to number theory. In *Publications of the Mathematical Society of Japan; 6*, pp. 152 - 154. Mathematical Society of Japan, 1961.

[29] A. -M. Spalleck. *Kurven vom Geschlecht 2 unt ihre Anwendung in Public Key Kryptosystemen.* PhD thesis, Institut für Experimentelle Mathematik, Universitā GH Essen, 1994.

[30] J. Tate. Endomorphisms of Abelian Varieties over Finite Fields. In *Inventiones mathematicae*, Vol. 2, pp. 134 - 144. Springer-Verlag, 1966.

[31] T. Umeki, M. Hosoya, K. Matsuo, J. Chao, and S.Tsujii. Computation of CM type of Jacobian Varieties. In *Proceedings of SCIS2000.* IEICE, Symposium on Cryptography and Information Security 2000, C49, 2000.

[32] Emil J. Volcheck. Computitng in the Jacobian of Plane Algebraic Curve. In *Proceedings of Algorithmic Number Theory Symposium I*, 1994.

[33] T. Wakabayashi, T. Nakamizo, K. Matsuo, J. Chao, and S. Tsujii. Computation of Weil Number of CM Varieties and Design of Jacobian Cryptosystems. In *Proceedings of SCIS2000.* IEICE, Symposium on Cryptography and Information Security 2000, C50, 2000.

[34] Paul Van Wamelen. Example of genus two CM curves defined over the rationals. In *Mathematics of Computation*, Vol. 68, Number 225, pp.307 - 320. American Mathematical Society, 1999.

[35] Paul Van Wamelen. Proving that a genus 2 curve has complex multiplication. In *Mathematics of Computation*, Vol. 68, Number 228, pp. 1663 - 1677. American Mathematical Society, 1999.

[36] Xiangdong Wang. 2-dimensional simple factors of $J_0(N)$. In *manuscripta mathematica*, Vol. 87, pp. 179 - 197. Springer-Verlag, 1995.

[37] William C. Waterhouse. Abelian varieties over finite fields. *Ann. scient. Ec. Norm. Sup.* 4^o *t. 2*, pp. 521 - 560, 1969.

[38] Hermann-Josef Weber. Hyperelliptic Simple Factors of $J_0(N)$ with Dimension at Least 3. In *Experimental Mathematics*, pp. 273 - 287. A K Peters, Ltd., 1997.