Semaev's summation polynomial と Stange's elliptic nets のある関係式

齋藤 恆和 (九州大学), 横山 俊一 (九州大学),
小林 鉄太郎 (日本電信電話), 山本 剛 (日本電信電話)

概 要

楕円曲線上の点の分解の判定法は Semaev による summation polynomials を用いたものと Stange による elliptic net を用いたものがある. 本講演ではこの二つの Semaev's summation polynomials と Stange's elliptic nets のある関係式を導き, elliptic net を用いた指数計算法による攻撃は summation polynomial のものと同等であることを示す.

1 動機

1.1 Decomposition of Points on an Elliptic curve

体 k の Affine 平面 $\mathbf{A}^2(\overline{k})$ 上の楕円曲線上の点 $P = (x(P), y(P)) \in E$ に対して

$$mP = 0$$

の判定は m 等分多項式 ψ_m を用い $\psi_m(x(P), y(P)) = \mathcal{O}$ と同値であることは周知のことである. この拡張として, 複数の点の和が $\mathcal{O}$ となるかどうかを判定する手段が楕円曲線暗号において必要となる場合がある. この報告では, 以下の具体的なもんだいへの分解判定の必要のもと, その判定方法について述べ, それらの関係を求める.

楕円曲線暗号は楕円曲線離散対数問題の計算の複雑さをもとに構築されている. 有限素体 $\mathbf{F}_q$ と楕円曲線 $E/\mathbf{F}_q$ において楕円曲線離散対数問題とは $P \in E(\mathbf{F}_q), A \in \langle P \rangle$ に対して, $mA = P$ を満足する最少の $m \in \mathbf{Z}_{\geq 0}$ (これを $\log_P A$ と記す) を求める問題である. ここで中国の剰余定理から P の位数は素数としてよい. 一方, ある種の拡大有限体において四則演算の計算高速化が 1998 年に Bailey と Paar によって OEF と呼ばれる手法が提唱された [2]. 同じ程度の位数をもつ有限素体 $\mathbf{F}_q$ と拡大有限体 $\mathbf{F}_{q'^n}$ にたいして, 拡大有限体のほうが四則演算の計算が高速になる. これは q' と n によっては modular reduction が高速におこなわれるからである. この OEF の手法によって, 暗号プロトコルの高速化のために, それまで素体上の楕円曲線によって構築された暗号プロトコルではなく拡大体上の楕円曲線を用いた暗号プロトコルが提唱された [1]. しかしこの拡大体上の楕円曲線暗号に対して, 以下のような指数計算法を用いた攻撃方法が Gaudry と Diem によって提唱された [5], [4].

Step 1. 因子基底 $\mathfrak{F} = \{P \in E(\mathbf{F}_{q^n}) \,|\, x(P) \in \mathbf{F}_q\} = \{F_1, \ldots, F_s\}$ を定める.

Step 2. 適当な $\beta_i \in \mathbf{Z}/\mathrm{ord}(P)\mathbf{Z}$ を取り, s 個の関係式

$$\beta_i P = \sum_{j=1}^{s} f_{ij} F_j, (i = 1, \ldots, s)$$

を与える.

Step 3. 与えられた行列の関係式によって $\log_P F_j$ を求める.

Step 4. 再び $\alpha, \beta \in \mathbf{Z}/\mathrm{ord}(P)\mathbf{Z}$ を適当に与え, 関係式を与える.

$$\alpha A + \beta P = \sum_{j=1}^{s} f_j F_j.$$

Step 5. $F_j = (\log_P F_j)P$ より, $A = mP$ の形にできる.

この手法において, 関係式を与えるために, 任意の $P, P_1, \ldots, P_r \in E(\mathbf{F}_{q^n})$ に対して, 分解

$$P = \sum_{i=1}^{r} P_i$$

を満足するのかを判定する手法が必要である. また, Step 2, Step 3 において関係式の個数 s や与えた関係式によっては $\log_P F_j$ が求まらない場合があるが, その際は再度関係式を与え連立方程式を求める. 関係式の個数を連立方程式を解かせられるまでに増やしたとしても, 上のアルゴリズムの計算時間の評価が左右されることは無いことに注意する.

1.2 Semaev's Summation Polynomials

上の分解の判定方法に対して, Gaudry と Diem は以下の Semaev による summation polynomial を利用した方法を用いている [6]. この節では, k を任意の体とする.

Theorem 1.1 (Semaev [6]). (1) 任意の楕円曲線 E/k と整数 $n \in \mathbf{Z}_{\geq 2}$ に対して, n 変数多項式 $S_n(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ が存在し, 任意の点 $P_1, \ldots, P_n \in E$ に対して, $\epsilon_i \in \{\pm 1\}$ が存在し, $\epsilon_1 P_1 + \cdots + \epsilon_n P_n = 0$ であることと $S_n(x(P_1), \ldots, x(P_n)) = 0$ であることは同値である.
(2) 標数 $\mathrm{ch}(k)$ が 2, 3 以外 (ただし, この条件は本質的ではない) の場合, 楕円曲線の式を $E : y^2 = 4x^3 + ax + b$ としたときに S_n は次のように漸化的に与えられる.

$$\begin{aligned} S_2(X_1, X_2) &= X_1 - X_2, \\ S_3(X_1, X_2, X_3) &= (X_1 - X_2)^2 X_3^2 - 2\left((X_1 + X_2)\left(\frac{a}{4} + X_1 X_2\right) + \frac{b}{2}\right) X_3 \\ &\quad + \left(X_1 X_2 - \frac{a}{4}\right)^2 - b(X_1 + X_2), \\ S_n(X_1, \ldots, X_n) &= Res_X(S_j(X_1, \ldots, X_{j-1}, X), S_{n-j+2}(X_j, \ldots, X_n, X)), \end{aligned}$$

ここで j は $3 \leq j \leq n-1$ を満たす任意の整数である.
(3) $S_n(X_1, \ldots, X_n)$ の各変数 X_i の多項式としての次数は 2^{n-2} 次である.
(4) 既約多項式である.

この分解の判定方法を用いて Gaudry と Diem が提案した攻撃方法の関係式を求めることに対して次のような同値がわかる.

Theorem 1.2 (Gaudry [5]). 任意の点 $P \in E(\mathbf{F}_{q^n})$ と元 $Q_1, \ldots, Q_n \in \mathbf{F}_q$ に対し, 次の条件 (i), (ii), (iii) は同値である:

(i) 因子基底の点 $F_1, \ldots, F_n \in \mathfrak{F}$ が存在し, $x(F_1) = Q_1, \ldots, x(F_n) = Q_n$ かつ $P = F_1 + \cdots + F_n$ を満足する.

(ii) Semaev 多項式 S_{n+1} に対して, $S_{n+1}(Q_1, \ldots, Q_n, x(P)) = 0$.

(iii) 拡大体 $\mathbf{F}_{q^n}/\mathbf{F}_q$ の基底を $\{t_i \,|\, i = 1, \ldots, n\}$ として, Semaev 多項式を基礎体の係数に分解する, すなわち

$$S_{n+1}(X_1, \ldots, X_n, x(P)) = \sum_{i=1}^{n} s^i_{n+1,P}(X_1, \ldots, X_n) t_i (s^i_{n+1,P} \in \mathbf{F}_q[X_1, \ldots, X_n]).$$

このとき, $(Q_1, \ldots, Q_n)$ は多様体 $V(s^1_{n+1,P}, \ldots, s^n_{n+1,P})$ の $\mathbf{F}_q$ 有理点である.

故に Guadry と Diem が示したアルゴリズムの中で関係式を与える際には, 分解された Semaev 多項式 $s^1_{n+1,P}, \ldots, s^n_{n+1,P}$ の連立代数方程式をグレブナー基底や多重終結式等の適当な方法で解けば良い [3].

1.3 Stange's Elliptic Nets

上にあげた Semaev 多項式以外に関係式を求める方法を述べる. Stange は多変数楕円関数を用いて楕円曲線上の点の分解の判定法を以下の様に与えている [7].

任意の代数体 k に対して E を k 上の楕円曲線とする. また Weierstrass σ 関数を

$$\sigma(z) = z \prod_{\omega \in L_E} \left(1 - \frac{z}{\omega}\right) \exp\left(\frac{z}{\omega} + \frac{z^2}{2\omega^2}\right)$$

とする. ここで, L_E は E に付随する $\mathbf{C}$ 上の格子である. 整数値ベクトル $v = (v_1, \ldots, v_n) \in \mathbf{Z}^n$ と変数 $z = (z_1, \ldots, z_n) \in \mathbf{C}^n$ に対して

$$\Psi_v(z) = \frac{\sigma(v_1 z_1 + \cdots + v_n z_n)}{\prod_{i=1}^n \sigma(z_i)^{\sum_{j=1}^n 2v_i^2 - v_i v_j} \prod_{1 \le i < j \le n} \sigma(z_i + z_j)^{v_i v_j}}$$

とする. この $\Psi_v(z)$ は各変数 z_i に関して楕円関数である. この関数は等分多項式による楕円関数 $\psi_m(\wp(z), \wp'(z)) = \sigma(mz)/\sigma(z)^{m^2}$ の多変数化としてとらえることができる.

楕円曲線上の点を引き戻し $\pi^{-1} : E \cong \mathbf{C}/L_E \longrightarrow \mathbf{C}$ によって $\mathbf{C}$ 上の点とみなせる. 以下では, $\pi^{-1}(P)$ を混乱が無い限り P と省略して書く場合がある.

Theorem 1.3 (Stange [7]). 代数体 k と楕円曲線上の点 $P_1, \ldots, P_n \in E(k)$ に対して,

$$v_1 P_1 + \cdots + v_n P_n = 0 \Longleftrightarrow \Psi_v(P_1, \ldots, P_n) = 0$$

が成立する.

なお, 楕円曲線上の点 $P_1, \ldots, P_n \in E(k)$ に対して写像

$$W : \mathbf{Z}^n \longrightarrow k, \quad v \longmapsto \Psi_v(P_1, \ldots, P_n)$$

を $P_1, \ldots, P_n$ による elliptic net という. また, 任意の整数値ベクトル $p, q, r, s \in \mathbf{Z}^n$ に対して

$$W(p+q+s)W(p-q)W(r+s)W(r) + W(q+r+s)W(q-r)W(p+s)W(p) + W(r+p+s)W(r-p)W(q+s)W(q) = 0$$

を満足し, この elliptic net は elliptic divisibility sequence の一般化であるとみなせる. ここで, elliptic divisibility sequence とは以下の性質を満足する体の列である;

$$h_{m-n}h_{m+n}h_1^2 = h_{m+1}h_{n-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \quad (\text{for all } m > n > 0).$$

尚, ペアリング暗号においてさまざまなペアリングの計算高速化が急務であるが, この elliptic net を用いて Tate ペアリングを高速化を図ることが提唱されている [8].

2 関係式

任意の代数体 k 上の有理関数体 $K = k(\wp(z_1), \ldots, \wp(z_n))$ に対して, Gaolis 拡大 L を $L = K(\wp'(z_1), \ldots, \wp'(z_n))$ で定める. Semaev's summation polynomial は楕円曲線の点の x 座標のみによって点の分解の判定を与えている, すなわち有理関数体 $S_n(\wp(z_1), \ldots, \wp(z_n)) \in K$ として, 分解の判定を行う. 一方で Stange's elliptic net のもととなるべく関数 $\Psi_v(z)$ は楕円関数であるが L の元である. Galois 群 $\mathrm{Gal}(L/K) = \{\pm 1\}^n$ に対して, $(\epsilon_1, \ldots, \epsilon_n) \in \mathrm{Gal}(L/K)$ の $(z_1, \ldots, z_n) \in (\mathbf{C}/L_E)^n$ への作用は $(\epsilon_1, \ldots, \epsilon_n).(z_1, \ldots, z_n) = (\epsilon_1 z_1, \ldots, \epsilon_n z_n)$ で与えられる.

Theorem 2.1. 任意の整数 $n \in \mathbf{Z}_{\geq 2}$ と代数体上の楕円曲線 E に対して

$$N_{L/K}(\Psi_v(z)) = S_n(\wp(v_1 z_1), \ldots, \wp(v_n z_n))^2 \frac{\prod_{i=1}^n \Psi_{v_i}(z_i)^{2^n}}{\prod_{1 \leq s < t \leq n} (\wp(z_s) - \wp(z_t))^{2^{n-1} v_s v_t}}$$

が成立する.

この定理の右辺に現れる $\prod_{i=1}^n \Psi_{v_i}(z_i)^{2^{n-1}}$ の項は各点 P_i について $v_i P_i = 0$ の判定であり, $\prod_{1 \leq s < t \leq n} (\wp(z_s) - \wp(z_t))^{2^{n-1} v_s v_t}$ の項は $P_s = \pm P_t$ の判定である. もし, いずれかの場合には, n を $n-1$ にし, 再度判定を行えば良い. 故に, いずれも本質的な判定には無関係である. すなわち $\epsilon_1 v_1 P_1 + \epsilon_2 v_2 P_2 + \cdots + \epsilon_n v_n P_n = 0$ を判定するものとして, Semaev's summation polynomial と elliptic net のノルムは同等のものとして捉えられる.

Lemma 2.2. Semaev's summation polynomial S_n に対して次の漸化式が成立する:

$$\begin{aligned}
&S_n(\wp(z_1), \ldots, \wp(z_n)) \\
&\quad = S_{n-1}(\wp(z_1), \ldots, \wp(z_{n-1}))^2 \prod_{\epsilon_2, \ldots, \epsilon_{n-1} \in \{\pm 1\}} (\wp(z_1 + \epsilon_2 z_2 + \cdots + \epsilon_{n-1} z_{n-1}) - \wp(z_n)) \\
&\quad = (\wp(z_1) - \wp(z_2))^{2^{n-2}} \prod_{i=1}^{n-2} \prod_{\epsilon_2, \ldots, \epsilon_{n-i} \in \{\pm 1\}} (\wp(z_1 + \epsilon_2 z_2 + \cdots + \epsilon_{n-i} z_{n-i}) - \wp(z_{n-i+1}))^{2^{i-1}}
\end{aligned}$$

Proof. 数学的帰納法による. $n = 3$ のとき, $S_3(\wp(z_1), \wp(z_2), \wp(z_3)) = S_2(\wp(z_1), \wp(z_2))^2 (\wp(z_1 + z_2) - \wp(z_3))(\wp(z_1 - z_2) - \wp(z_3))$ が成立することは $\wp$ 関数の加法公式から直ちに導かれる. $n-1$ 以下の場合に主張すべき式が成立すると仮定する.

$$\begin{aligned}
&S_n(\wp(z_1), \ldots, \wp(z_n)) = Res_X(S_3(\wp(z_1), \wp(z_2), X), \\
&S_{n-1}(\wp(z_3), \ldots, \wp(z_n), X)) = Res_X(S_2(\wp(z_1), \wp(z_2))^2 \prod_{\epsilon_2 = \pm 1} (\wp(z_1 + \epsilon_2 z_2) - X), \\
&S_{n-2}(\wp(z_3), \ldots, \wp(z_n))^2 \prod_{\epsilon_4, \ldots, e_n \in \{\pm 1\}} (\wp(z_3 + \epsilon_4 z_4 + \cdots + \epsilon_n z_n) - X))
\end{aligned}$$

$$
\begin{aligned}
&= S_2(\wp(z_1),\wp(z_2))^{2^{n-2}} S_{n-2}(\wp(z_3),\dots,\wp(z_n))^{2^2} \\
&\quad\times \prod_{\epsilon_2,\epsilon_4,\dots,\epsilon_n\in\{\pm1\}} (\wp(z_1+\epsilon_2 z_2)-\wp(z_3+\epsilon_4 z_4+\cdots+\epsilon_n z_n)) \\
&= (\wp(z_1)-\wp(z_2))^{2^{n-2}} \left(\prod_{i=1}^{n-4} \prod_{\epsilon_4,\dots,\epsilon_{n-1}} (\wp(z_3+\epsilon_4 z_4+\cdots+\epsilon_{n-i}z_{n-i})-\wp(z_{n-i+1}))^{2^{i+1}} \right) \\
&\quad\times (\wp(z_3)-\wp(z_4))^{2^{n-2}} \prod_{\epsilon_2,\epsilon_4,\dots,\epsilon_n\in\{\pm1\}} (\wp(z_1+\epsilon_2 z_2)-\wp(z_3+\epsilon_4 z_4+\cdots+\epsilon_n z_n)).
\end{aligned}
$$

上の変形によって $S_n(\wp(z_1),\dots,\wp(z_n))$ の零点と極が補題の主張の式の左辺のものと一致することが分かる. また, 両辺の $z_1+z_2=0$ での級数展開を与えると一致している. Liouville の定理から主張は正しい. □

この補題をもとに定理の証明を与える.

Proof of Theorem 2.1. 数学的帰納法による. $n=2$ の場合,

$$
\begin{aligned}
N_{L/K}(\Psi_{(v_1,v_2)}(z_1,z_2)) &= \prod_{\epsilon_1,\epsilon_2\in\{\pm1\}} \frac{\sigma(\epsilon_1 v_1 z_1+\epsilon_2 v_2 z_2)}{\sigma(\epsilon_1 z_1)^{v_1^2-v_1v_2}\sigma(\epsilon_1 z_1+\epsilon_2 z_2)^{v_1v_2}\sigma(\epsilon_2 z_2)^{v_2^2-v_1v_2}} \\
&= \frac{\sigma(v_1z_1+v_2z_2)^2\sigma(v_1z_1-v_1z_2)^2}{\sigma(z_1)^{4v_1-4v_1v_2}\sigma(z_1+z_2)^{2v_1v_2}\sigma(z_1-z_2)^{2v_1v_2}\sigma(z_2)^{4v_2^2-4v_1v_2}} \\
&= \frac{\sigma(v_1z_1)^4\sigma(v_2z_2)^4(\wp(v_1z_1)-\wp(v_2z_2))^2}{\sigma(z_1)^{4v_1^2}\sigma(z_2)^{4v_2^2}(\wp(z_1)-\wp(z_2))^{2v_1v_2}}
\end{aligned}
$$

より, 定理の主張は成立する.

$n-1$ 以下のときに成立していると仮定する, すなわち

$$
\prod_{\epsilon_2,\dots,\epsilon_{n-1}\in\{\pm1\}} \Psi_{(v_1,\epsilon_2v_2,\dots,\epsilon_{n-1}v_{n-1})}(z) = S_{n-1}(\wp(v_1z_1),\dots,\wp(v_{n-1}z_{n-1})) \prod_{i=1}^{n-1} \Psi_{v_i}(z_i)^{2^{n-2}}.
$$

このもとで,

$$
\begin{aligned}
&\prod_{\epsilon_2,\dots,\epsilon_n\in\{\pm1\}} \Psi_{(v_1,\epsilon_2v_2\dots,\epsilon_nv_n)}(z_1,\dots,z_n) \\
&\quad= \prod_{\epsilon_2,\dots,\epsilon_n\in\{\pm1\}} \frac{\sigma(v_1z_1+\epsilon_2v_2z_2+\cdots+\epsilon_nv_nz_n)}{\prod_{j=1}^n \sigma(z_i)^{2-\epsilon_i\epsilon_jv_iv_j} \prod_{1\le i<j\le n}\sigma(z_i+z_j)^{\epsilon_i\epsilon_jv_iv_j}} \\
&\quad= \prod_{\epsilon_2,\dots,\epsilon_{n-1}\in\{\pm1\}} \Big((\wp(v_1z_1+\epsilon_2v_2z_2+\cdots+\epsilon_{n-1}v_{n-1}z_{n-1})-\wp(v_nz_n)) \\
&\qquad\times \frac{\sigma(z_1+\epsilon_2z_2+\cdots+\epsilon_{n-1}z_{n-1})^2\sigma(z_n)^2}{\prod_{i=1}^n \sigma(z_i)^{2^{n-1}v_i^2}} \Big) \\
&\quad= \Psi_{v_n}(z_n)^{2^{n-1}} \prod_{\epsilon_2,\dots,\epsilon_{n-1}\in\{\pm1\}} \Psi_{(v_1,\epsilon_2v_2,\dots,\epsilon_{n-1}v_{n-1})}(z_1,\dots,z_{n-1})^2 \\
&\qquad\times \prod_{\epsilon_2,\dots,\epsilon_{n-1}\in\{\pm1\}} (\wp(v_1z_1+\epsilon_2v_2z_2+\cdots+\epsilon_{n-1}v_{n-1}z_{n-1})-\wp(v_nz_n)) \\
&\quad= S_{n-1}(\wp(v_1z_1),\dots,\wp(v_{n-1}z_{n-1}))^2 \prod_{i=1}^n \Psi_{v_i}(z_i)^{2^{n-1}}
\end{aligned}
$$

$$\times \prod_{\epsilon_2,\ldots,\epsilon_{n-1}\in\{\pm 1\}} (\wp(v_1z_1+\epsilon_2v_2z_2+\cdots+\epsilon_{n-1}v_{n-1}z_{n-1})-\wp(v_nz_n))$$
$$= S_n(\wp(v_1z_1),\ldots,\wp(v_nz_n))\prod_{i=1}^{n}\Psi_{v_i}(z_i)^{2^{n-1}}.$$

□

3 いくつかの問題

この報告集では定義体を代数体としたが, 任意の体でも reduction theory により定理は成立する. この定理によって Gaudry と Diem によって与えられたアルゴリズムの中で elliptic net を y を消去して用いる手法と Semaev 多項式を用いることは同等であることが示された. しかし, elliptic net にたいしてグレブナー基底を用いて, 関係式を求めることができるのではないか. 具体的に, 関係式を求めるには楕円曲線上の点の分解を判定するの多項式から得られる連立代数方程式を解くのだが, 任意の点 $P\in E(\mathbf{F}_{q^n})$ に対して $\Psi_{(1,\ldots,1)}(X_1,Y_1,\ldots,X_n,Y_n,x(P),y(P))\in \mathbf{F}_{q^n}(X_1,Y_1,\ldots,X_n,Y_n)$ を計算する. それを基礎体 $\mathbf{F}_q$ において分解する;

$$\Psi_{(1,\ldots,1)}(X_1,Y_1,\ldots,X_n,Y_n,x(P),y(P))=\sum_{i=1}^{n}\Phi_P^{(i)}(X_1,Y_1,\ldots,X_n,Y_n)t^i.$$

ここで $\{t^i\,|\,i=1,\ldots,n\}$ は拡大体 $\mathbf{F}_{q^n}/\mathbf{F}_q$ の基底であり, $\Psi_P^{(i)}$ は $\mathbf{F}_q(X_1,Y_1,\ldots,X_n,Y_n)$ の元である. このとき, 多様体 $V(\Psi_P^{(1)},\ldots,\Psi_P^{(n)})$ の $\mathbf{F}_q$ 有理点を与えればよい. しかし, 一方で因子基底等の定義の仕方, どのくらいの計算量で方程式が解けるのかが問題になる.

参考文献

[1] K. Aoki, T, Kobayashi and A. Nagai, Supplemental Document for Odd Characteristic Extension Fields, Standards for Efficient Cryptography, 2009.

[2] D, Bailey and C. Paar, Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithm, CRYPTO98, LNCS 1462, 1998.

[3] D. Cox, J. Little, and D. O′Shea, Using Algebraic Geometry, Springer, 2005.

[4] C. Diem, On the discrete logrithm problem in elliptic curves, preprint, Aug. 2009.

[5] P. Gaudry, Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem, J. Symbolic Computation, 2009.

[6] I. Semaev, Summation polynomials and the discrete logarithm problem on elliptic curves, Available under http://eprint.iacr.org/2004/031, Feb. 2004.

[7] K. Stange, The Tate pairing via elliptic nets, Pairing 2007.

[8] N. Ogura, N, Kanayama, S, Uchiyama and E, Okamoto, Cryptographic Pairings Based on Elliptic Nets, preprint.