楕円曲線 Elgamal 暗号の紹介

滋賀職能短大：長尾孝一

Abstract

この報告では 最近その応用が期待されている楕円曲線 Elgamal 暗号についてその要約をすることを目標としています。報告では まず最初にこれらの基本となる Elgamal 暗号の概論、署名、離散対数問題について述べ、次に、 $_p$ 上定義された楕円曲線を使った暗号について、それに適した曲線を選ぶ Morain, 宮地 等の方法について述べます。最後にそのまとめとして、類数か 1,2 の虚 2 次体の Maximal Order に対応する楕円曲線の j-invarient の表を与えます。この表によって、Morain の方法が簡単に適応できる楕円曲線についての数表が得られたことになります。Abstract の最後に、
当研究集会を主催なさいました中村先生、小関先生、三宅先生に感謝の意を表したいと思います。

§1. Elgamal 暗号概論

ここでは G をアーベル群とする。(演算は加法 + で書く) (主に有限体の乗法群 $^{\times}_{p}$, 楕円曲線の $_p$有理点 $E(\ _p)$ が使われる)

$$\text{また } P_1, P_2 \in G \ \text{ s.t. } \ P_2 = n \cdot P_1 \text{とする}$$

注：$G = \ ^{\times}_{p}$ の時、演算は乗法で書けるので、

$$x_1, x_2 \in \ ^{\times}_{p} \ \text{ s.t. } \ x_2 = x_1^n \quad)$$

このような、P_1, P_2 (x_1, x_2) から、n を求める問題を離散対数問題と言う。($n = \log_{x_1} x_2$ と書けているから)

Ａ氏にたいして、

$G_A = G$, $P_{A,1} = P_1$, $P_{A,2} = P_2$ を公開鍵、$n_A = n$ を秘密鍵

とする暗号を Elgamal 暗号と言う。

§2. 文の暗号化と暗号の解読

A 氏, B 氏 の二人が暗号通信を行う時次の手順で、通信を行う。

Ｂ氏が先のＡ氏に暗号文を送る手順

1. $P \in G_A$ を送る DATA, r:乱数とする。
2. $Q_1 = r \cdot P_{A,1}$, $Q_2 = P + r \cdot P_{A,2}$ を Ａ氏に送る。

Ａ氏が暗号文を解読する手順

$Q_2 - n_A \cdot Q_1 (= P)$ を計算する。

$G = \ ^{\times}_{p}$ の時、

1. $x \in \ _{p_A}$ Data, r:乱数
2. $y_1 \equiv x^r_{A,1}$, $y_2 \equiv x \cdot x^r_{A,2} \bmod p_A$ をＡ氏に送る。

$x \equiv y_2 \cdot y_1^{-n_A} \bmod p_A$ で文を解読する。

§3. ＤＳＡ署名

　また、このような暗号通信を行う時、次のような署名を付けることができます。
Ａ氏: G_A,$P_{A,1}$,$P_{A,2}$:公開鍵、n_A:秘密鍵。
次の２つを公開鍵に付け加える。
$q_A := \#G_A,$
$\phi_A : G_A \to \quad / \quad _{q_A}$ (map を決めて置く)
Ａ氏がＢ氏に文を送る時、次のm, r, tを付け加えるとＡ氏からの文であることが分かる。
1. m, k:乱数 s.t. $gcd(k, q_A) = 1$
2. $r = \phi_A(k \cdot P_{A,1})$
3. $t \equiv (m + n_A \cdot r) \cdot k^{-1} \bmod q_A$ 4. m, r, tをＢ氏に送る。
Ｂ氏の解読
1. $Q = m \cdot t^{-1} \cdot P_{A,1} + r \cdot t^{-1} \cdot P_{A,2}$
注：$Q = t^{-1}(m + n_A \cdot r) \cdot P_{A,1} = k \cdot p_{A,1}$
2. $\phi_A(Q) = r \bmod q_A$ であれば、署名は正しい。

§4. 離散対数問題

　Elgamal 暗号で通信を行う時、、その安全性の基礎となるのが離散対数問題の難しさである。ここでは離散対数問題の解法アルゴリズムの計算量について知られている結果をまとめておく。
計算量を表す記号：

$$L_N[a, b] = exp\{b \cdot (\log N)^a \cdot (\log\log N)^{1-a}\}$$

注：$O(N^b \cdot (\log N$の多項式$) \leq L_N[1, b]$
$O((\log N)^b) = L_N[0, b]$
1. 一般のアーベル群の離散対数問題
$P_1, P_2 \in G$ s.t. $P_2 = n \cdot P_1$から、n を求める。
★ $G = G_1 \oplus G_2$ の時、G_1,G_2 の離散対数問題に帰着。
★ (Baby step giant step method due to Shanks)
$N = \#G$ とする。$O(\sqrt{N} \cdot \log N) = L_N[1, 1/2 + epsilon]$ で n は計算できる。

2. $G = \ _p^\times$ の時
$x, y \in \ _p^\times$ s.t. $x^n \equiv y \bmod p$ の時、n を求める。
★ (Adleman's index calculas) $L_p[1/2, c]$　　$c \approx 1$ で n は確率的に計算できる。
★ Gordon による改良によって、$L[1/3, 3^{2/3}]$ に改良される。

3. $E/ \ _p$:楕円曲線 $G = E(\ _p)$, の時
★ (MOV Reduction due to Menezes, 岡本, Vanstone)
$E/ \ _p$:super singular$(\#E(\ _p) = p + 1) \to$

F_{p^n} (n は小さい) の離散対数問題に帰着

◇ ∃ Weil pairing: $E(\mathbb{F}_p) \to \mathbb{F}_{p^n}^{\times}$ when $\#E(\mathbb{F}_p) | p^n - 1$

★ (佐藤、荒木、Smart)

$E/\mathbb{F}_p$:anomalous ($\#E(\mathbb{F}_p) = p$) → $O((\log p)^3)$

§5. $E/\mathbb{F}_p$ (p:素数) を使った Elgamal 暗号

§4 で述べたことより $E/\mathbb{F}_p$ に次の条件が必要となる。

1. $\#E(\mathbb{F}_p) =$ 小さな数 $\times$ 素数 (near prime と呼ぶ)
2. MOV, anomalous で無い。i.e. $\#E(\mathbb{F}_p) \neq p, \#E(\mathbb{F}_p) \not| p^n - 1$ for small n.

このために $\#E(\mathbb{F}_p)$ を control した、$E/\mathbb{F}_p$ を構成することが大切である。

Theorem

$$E : y^2 = x^3 + x \qquad (D = -4 : \text{で } C.M.) \text{ とする。}$$

1. $p \equiv 3 \bmod 4$ → $\#E(\mathbb{F}_p) = p + 1$
2. $p \equiv 1 \bmod 4$ の時、a, b, wを次と置く。

$p = a^2 + b^2$, w : $\mathbb{F}_p$の原始根

$E_i : y^2 = x^3 + w^i x, \qquad (i = 0, 1, 2, 3)$ と置く。

$\#E_i(\mathbb{F}_p) = p + 1 \pm 2a, p + 1 \pm 2b$

上の Theorem は古典的である (例えば Ireland & Rosen を見よ) これを使って次のようなアルゴリズムで $\#E(\mathbb{F}_p)$ をうまく control することができる。

アルゴリズム

1. $a, b \in \mathbb{Z}$ (偶奇は異なる) を選ぶ。
2. $p = a^2 + b^2$ が素数なら 3 へ違えば 1 へ。
3. $p + 1 \pm 2a, p + 1 \pm 2b$ のいずれかが near prime なら 4 へ、違えば 1 へ。
4. ($p + 1 + 2a$ が near prime として) $E_i(\mathbb{F}_p) = p + 1 + 2a$ なる E_iを決める。
5. $E_i/\mathbb{F}_p$ が MOV, anomalous でなければこれを暗号に使う。そうでなければ 1 へ。

Point. 虚数乗法論で $\#E(\mathbb{F}_p)$ を control している。これを次の章で一般化 (due to Morain) する。

§6. Morain による一般化

Morain の定理を述べる為にまず、幾つかの記号を用意する。

★ 数 jに対して、楕円曲線 E_j を

$$E_j : \begin{cases} Y^2 = X^3 + 1 & j = 0 \text{ の時} \\ Y^2 = X^3 + X & j = 1728 \text{ の時} \\ Y^2 = X^3 + 3\frac{j}{1728-j}X + 2\frac{j}{1728-j} & j \neq 0, 1728 \text{ の時} \end{cases}$$

と置く。
★ 記号 D : $D < 0$, $D \equiv 1\, or\, 0 \bmod 4$ とする。
3-ple (a, b, c) を 式 $at^2 + bt + c$ が 判別式が D である、reduced form とする。

$$\begin{cases} \tau = \frac{-b+\sqrt{D}}{2a} \in \\ q = e^{2\pi\sqrt{-1}\tau} \\ E_4(\tau) = 1 + 240 \sum_{n\geq 1} \sigma_3(n) q^n \\ E_6(\tau) = 1 - 504 \sum_{n\geq 1} \sigma_5(n) q^n \\ J(a,b,c) = 1728 \frac{E_4(\tau)^3}{E_4(\tau)^3 - E_6(\tau)^2} \end{cases}$$

と置く。ただし$\sigma_k(n) = \sum_{d|n} d^k$ 。

$$H_D(X) = \prod_{(a,b,c)} (X - J(a,b,c))$$

と置く。ただし (a,b,c) は 判別式 D の reduced form を動く。
注：類数 $h(D)$:=判別式 D の reduced form の個数。

★ 意味：E_j s.t. $H_D(j) = 0$ は 判別式 Dの虚 2 次体の order を CM にもつ楕円曲線。

★ THEOREM (Morain)
p:奇素数が $4p = x^2 - 4Dy^2$ と書け、$H_D(\tilde{j}) \equiv 0 \bmod p$ とする。
$E'_{\tilde{j}}$を $E_{\tilde{j}}$から $(\frac{c}{p}) = -1$ な元 c によって twist で得た曲線とする。

$$\#E'_{\tilde{j}}(\quad_p) \quad \#E_{\tilde{j}}(\quad_p) = p + 1 \pm x$$

注：$D = -3, -4$ の時は単数の関係で他にもとる値の可能性がある。

case 1. $h(D) = 1$ の時 (主に 宮地 によって研究された)
$H_D(X) = X - J(a,b,c)$ とかけ、その係数が整数であることより、$J(a,b,c) \in$ 　が分かる。よって、

$$E_{\mathcal{J}(D)}, \qquad \mathcal{J}(D) = J(a,b,c)$$

となる 判別式 D の虚 2 次体の order を CM に持つ　上定義された楕円曲線が作れる。
case 2. $h(D) = 2$ の時
$h(D) = 2$ とします。類数の定義より、判別式 D の reduced form は 2 つだけある。これを $(a_i, b_i, c_i)_{i=1,2}$ とします。また、
$H_D(X) = (X - J(a_1, b_1, c_1))(X - J(a_2, b_2, c_2))$ とかけ、その係数が整数であることより、$J(a_i, b_i, c_i) = \frac{\alpha \pm \sqrt{\beta}}{2}$, $(\alpha, \beta \in \quad, i = 1, 2)$ と書ける。よって、

$$E_{\mathcal{J}(D)}, \qquad \mathcal{J}(D) = \frac{\alpha + \sqrt{\beta}}{2}$$

となる Dを CM に持つ　上定義された楕円曲線が作れる。

参考文献

[1] 黒澤馨、藤岡淳、宮地充子; 暗号理論への応用, 暗号、ゼロ知識証明、数論, ed. 岡本龍明、太田和夫, 共立出版, p.216-238, (1995)

[2] F. Morain; Building Cyclic Elliptic curves modulo Large Primes, Proc. of Euro-Crypto'91, Lecture note in Computer Science 547, p.328-336 , (1991)

[3] J.H. Silvermann; The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag, (1986)

[4] K. Lreland, M. Rosen; A Classical Introduction to Modern Number Theory, (2nd ed.), GTM 84, Springer-Verlag, (1990)

Tables

最後に類数 1,2 の場合についてその $\mathcal{J}(D)$ の値を表にしてまとめておく。
類数 1 の虚 2 次体の maximam order と それを CM に持つ楕円曲線の j-invariant

$$D = D_0 \cdot f^2$$

D_0	f	$\mathcal{J}(D)$
-3	1	0
-4	1	$2^6 3^3$
-7	1	$-3^3 5^3$
-8	1	$2^6 5^3$
-11	1	-2^{15}
-19	1	$-2^{15} 3^3$
-43	1	$-2^{18} 3^3 5^3$
-67	1	$-2^{15} 3^3 5^3 11^3$
-163	1	$-2^{18} 3^3 5^3 23^3 29^3$
-3	2	$2^4 3^3 5^3$
-3	3	$-2^{15} 3 5^3$
-4	2	$2^3 3^3 11^3$
-7	2	$3^3 5^3 17^3$

類数 2 の虚 2 次体の maximam order と それを CM に持つ楕円曲線の j-invariant

$$D = D_0 \cdot f^2, \qquad \mathcal{J}(D) = (\alpha + \sqrt{\beta})/2$$

D_0	f	α	β
-15	1	-191025	36975700125
-20	1	1264000	1600421888000
-24	1	4834944	23318002925568
-35	1	-117964800	13916230909952000
-40	1	425692800	181177947389952000
-51	1	-5541101568	30703781538642788352
-52	1	6896880000	47569224388608000000
-88	1	6294842640000	39624980669819854848000000
-91	1	-10359073013760	107310393719793445232443392
-115	1	-427864611225600	183068125538712908225052672000
-123	1	-1354146840576000	1833713665246724383309824000000
-148	1	39660183801072000	1572930210727783937814220800000000
-187	1	-4545336381788160000	20660082823607097188475199291392000000
-232	1	604729957849891344000	365698321861647078693271164024078336000000
-235	1	-823177419449425920000	677621063891416051130099935716952768512000
-267	1	-19683091854079488000000	387424104936128170807937131856636411904000000
-403	1	-2452811389229331391979520000	6016283711133122621257773144230637860148322762752000000
-427	1	-15611455512523783919812608000	243717543219509240868384739765019962091695648014336000000
-3	4	2835810000	8041792158027000000
-3	5	-654403829760	428244351567542699950080
-3	7	-34848505552896000	1214418339224796145096065024000000
-4	3	153542016	23582314507272192
-4	4	82226316240	6761167111868754217248
-4	5	44031499226496	1938774092707953394078187520
-15	2	37018076625	1370337384321120340125
-7	4	274917323970000	75579535013475393572336437500
-11	3	-37616060956672	1414968042120748924076556288
-8	3	377674768000	142637300857798656000000
-8	2	52250000	2730013832000000