楕円曲線上の離散対数問題
Elliptic Curve Discrete Logarithm Problem

計算アルゴリズムの実装と比較
Implementation and Comparison of Algorithms for Computing the ECDLP

潮谷　真奈

早稲田大学大学院　基幹理工学研究科
数学応用数理専攻２年　楯研究室

2020 年 2 月 7 日

アウトライン

- 概要
- 楕円曲線
- 楕円曲線の群構造
- 楕円曲線離散対数問題（ECDLP）
- ECDLP に対する攻撃アルゴリズム
- 実験
- 結論と考察
- 参考文献

概要

楕円曲線暗号

- 1985 年頃, N.Koblitz と V.S.Miller が提案 ([7]p376).
- 従来の RSA 暗号や ELGamal 暗号より安全性に優れたものとして, インターネットの暗号通信などに広く使われている ([2]p11, [1]p53).
- 根拠：楕円曲線上の離散対数問題 (ECDLP)の困難性

計算アルゴリズム

- 総当たり法
- Shanks' Babystep-Giantstep Algorithm
- Pollard's ρ algorithm

研究の目的

- 各アルゴリズムのステップ数と計算時間の測定
- 最も効率的なアルゴリズムはどれか調べる
- 仮想通貨ビットコインに使用されている楕円曲線暗号の安全性について考察 (解読に要する時間の予測)

楕円曲線

定義 (楕円曲線)

K を体, $\bar{K}$ を K の代数閉体とする.

種数 1 の非特異な代数曲線を, 楕円曲線という. 射影平面曲線としては, 以下のように書ける.

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$
$$(a_1, a_2, a_3, a_4, a_6 \in \bar{K})$$

この楕円曲線は必ず, 無限遠点 $[0 : 1 : 0]$ を通る. これを O と表記する.

楕円曲線

- 簡単のため, $x = \frac{X}{Z}, y = \frac{Y}{Z}$ とおいてアフィン座標に変換した
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
を定義式として用いる.

- $a_1, a_2, a_3, a_4, a_6 \in K$ のとき, E は K 上の楕円曲線であるといい, E/K と表記する.

- E の K 有理点の集合を
$E(K) = \{(x, y) \in K^2 \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$
と表記する.

楕円曲線

$\mathrm{char}(K) \neq 2, 3$ のとき, より簡単な形の式で表される曲線に変換できる ([5]p16).

Weierstrass の標準形

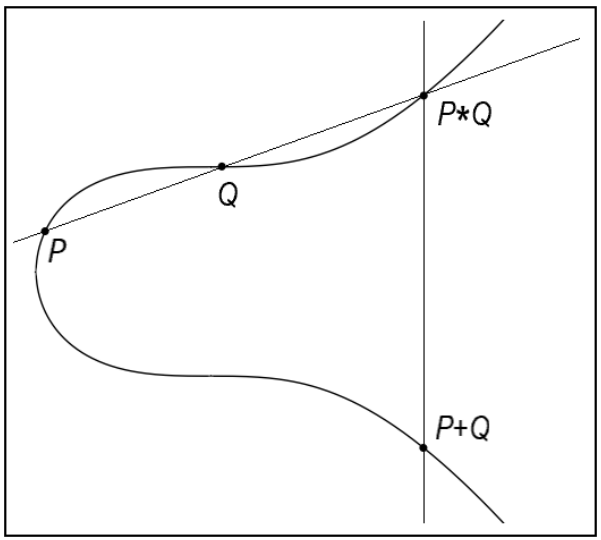
方程式 $y^2 = x^3 + ax + b$ を, Weierstrass の標準形という.

今後は $\mathrm{char}(K) \neq 2, 3$ の場合についてのみ考え, Weierstrass の標準形によって定義される楕円曲線 E/K を扱う.

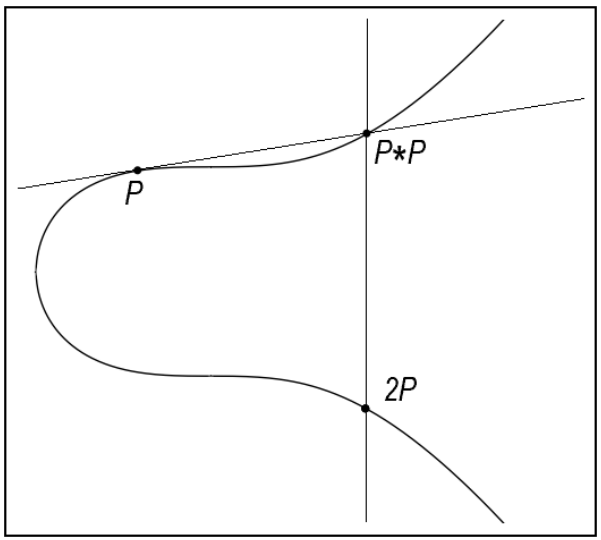
楕円曲線の群構造

Bézout の定理より, 射影空間において楕円曲線と直線は (重複度を含めて) ちょうど 3 点で交わる.

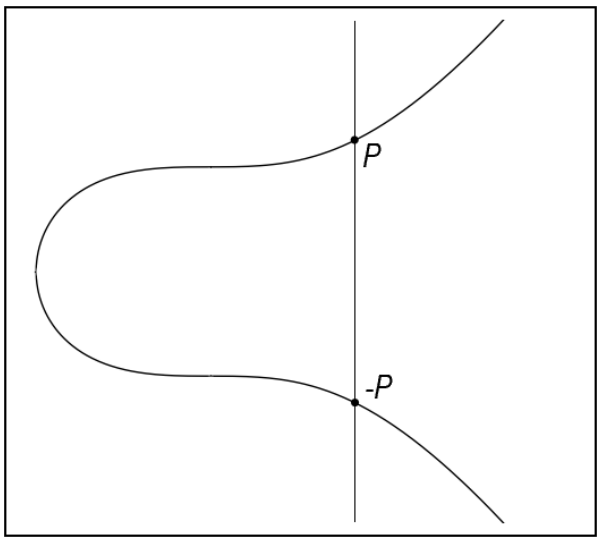
$\rightarrow$ $E(K)$ は, 以下で定義される $+$ を二項演算, O を単位元とする可換群とみなせる ([6]p187).



$P+Q$



$2P$



$-P$

楕円曲線離散対数問題 (ECDLP)

定義 (楕円曲線上の離散対数)

$P \in E(\mathbb{F}_q)$ について, $\langle P \rangle \subset E(\mathbb{F}_q)$ を点 P によって生成される巡回部分群とおく. このとき, 任意の $Q \in \langle P \rangle$ に対して,

$$\log_P Q = \min\{j \in \mathbb{Z}_{\geq 0} \mid Q = jP\}$$

を, P を底とする Q の離散対数という.

また, P をベースポイントという.

楕円曲線離散対数問題 (ECDLP)

定義 (楕円曲線上の離散対数問題 (ECDLP))

P と Q が与えられたとき, 離散対数 $\log_P Q$ を求める問題を, 楕円曲線上の離散対数問題 (ECDLP) という.

P の位数に大きな素数が含まれる場合, ECDLP は
(一部の特殊な楕円曲線を除き) 解読が困難な問題とされてる ([1]p75).

→ これを利用した楕円曲線暗号は,
RSA 暗号や ElGamal 暗号より安全性に優れ,
現在はインターネットの暗号通信プロトコルやビットコインにおける
ディジタル署名などに利用されている ([2]p11,[4]).

ECDLP に対する攻撃アルゴリズム
-総当たり法-

総当たり法

$P, 2P, 3P, \cdots$ と順に計算して $\log_P Q$ を求める解法.

本章では, ECDLP を解読するためのより効率的な方法について述べる.

以下, P の位数を n とおく.

ECDLP に対する攻撃アルゴリズム
-Shanks' Babystep-Giantstep Algorithm-

定理 ([7]p382)

$N = \lceil \sqrt{n} \rceil = \min\{m \in \mathbb{Z}_{\geq 0} \mid m \geq \sqrt{n}\}$, $R = -NP$ とおく.
$Q \in \langle P \rangle$ であれば, ある $0 \leq i, j < N$ が存在し, $\underline{iP = Q + jR}$が成立.

Shanks' Babystep-Giantstep Algorithm ([7]p382)

1. $N = \lceil \sqrt{n} \rceil = \min\{m \in \mathbb{Z}_{\geq 0} \mid m \geq \sqrt{n}\}$, $R = -NP$ を求める.
2. Babysteps : Baby リスト $\{iP \mid 0 \leq i < N\}$ を作成する.
3. Giantsteps : $Q, Q + R, Q + 2R, \cdots$ を順に計算し,
   Baby リスト上の点と一致する $Q + jR$ $(0 \leq j < N)$ を
   見つける.
4. $\underline{iP = Q + jR}$であれば, $Q = (i + jN)P$ となり,
   $\log_P Q \equiv i + jN \pmod{n}$ が成立.

$iP = Q + jR$ が見つかるまでのステップ数の期待値 : $\frac{3}{2}\sqrt{n}$ ([8]p3)

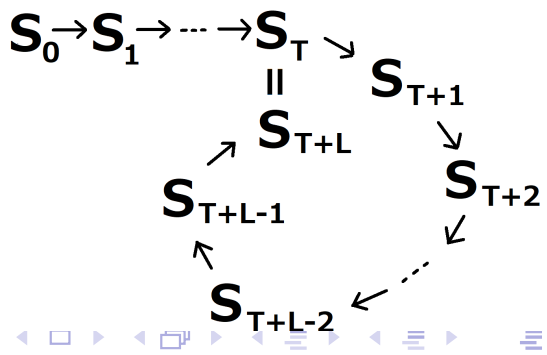
定義

$S_0 \in E(\mathbb{F}_q)$ を起点とし，点列 $S_1, S_2, \cdots$ を

$$\begin{aligned} f &: E(\mathbb{F}_q) \to E(\mathbb{F}_q), \\ S_i &= f(S_{i-1}) = \underbrace{f \circ \cdots \circ f}_{i}(S_0) \end{aligned}$$

によって定義する．ただし，f は $E(\mathbb{F}_q)$ 上の点を十分ランダムかつ効率的に定めることができる関数とする．

$E(\mathbb{F}_q)$ は有限群であるから，ある $t \in \mathbb{Z}_{\geq 0}, l \in \mathbb{N}$ が存在し，$S_t = S_{t+l}$ が成り立つ．このような t, l のうち最小のものをそれぞれ T, L と定義する．



$T + L$ の値の期待値：$\sqrt{\frac{\pi n}{2}}$ ([7]p383)

ECDLP に対する攻撃アルゴリズム -Pollard's ρ algorithm-

関数 f は, 例として以下のように定める.

定義 (random mapping f ([9]p206))

1. 任意の $m \in \mathbb{N}$ を選び, $E(\mathbb{F}_q)$ を元の数がおおよそ等しい m 個の集合 $G_1, \cdots, G_m$ に直和分割する.
2. $a_1, \cdots, a_m, b_1, \cdots, b_m \in \{0, \cdots, n-1\}$ をランダムに選ぶ. $M_l := a_l P + b_l Q$ $(l \in \{1, \cdots, m\})$
3. $f : E(\mathbb{F}_q) \to E(\mathbb{F}_q)$, $\underline{f(S) = S + M_l}$ $(S \in G_l)$

ECDLP に対する攻撃アルゴリズム -Pollard's ρ algorithm-

Pollard's ρ algorithm I ([9]p205)

1. $a_0, b_0 \in \{0, \cdots, n-1\}$ をランダムに選ぶ.
   点列 $(S_i) : S_0 = a_0P + b_0Q,\ S_i = f(S_{i-1})\ (i \in \mathbb{N})$
2. $S_1, S_2, S_3, \cdots$ と順に求め, $\underline{S_i = S_j}\ \ (j \in \{0, 1, \cdots, i-1\})$ となる i を見つける.
3. $a_iP + b_iQ = a_jP + b_jQ$ であるから,
   $\gcd((b_j - b_i), n) = 1$ であれば $\log_P Q \equiv (a_i - a_j)(b_j - b_i)^{-1} \pmod{n}$.

Shanks' Babystep-Giantstep Algorithm と Pollard's ρ algorithm I は, 一致する点を見つけるためにいくつかの点を保存し続け, 新たに求めた点といちいち比較する必要がある.

そこで最後に, 保存すべき点の個数をより少なく抑えたアルゴリズムについて述べる.

ECDLP に対する攻撃アルゴリズム -Pollard's ρ algorithm-

定理 ([7]p382)

ある $T \leq i' \leq T + L - 1$ が存在し, $S_{i'} = S_{2i'}$ が成り立つ.

Pollard's ρ algorithm II ([9]p206)

1. $a_0, b_0 \in \{0, \cdots, n-1\}$ をランダムに選ぶ.
   $(S_i) : S_0 = a_0P + b_0Q,\ S_i = f(S_{i-1})$
   $(T_i) : T_0 = a_0P + b_0Q,\ T_i = f \circ f(T_{i-1})\ (i \in \mathbb{N})$
2. $S_1, T_1, S_2, T_2, \cdots$ と順に求め, $S_i = T_i\ \ (= S_{2i})$ となる i を見つける.
3. $a_iP + b_iQ = a_{2i}P + b_{2i}Q$ であるから,
   $\gcd((b_{2i} - b_i), n) = 1$ であれば
   $\log_P Q \equiv (a_i - a_{2i})(b_{2i} - b_i)^{-1} \pmod{n}$.

ECDLP に対する攻撃アルゴリズム

- Shanks' Babystep-Giantstep Algorithm, Pollard's ρ algorithm I,II
  $\cdots$ 計算量は全て $O(\sqrt{n})$
  (保存すべき点が少ない $\rightarrow$Pollard's ρ algorithm II が優れている？)

  $\rightarrow$ 計算機を使用して ECDLP の作成・解読を行い,
  ステップ数 s と計算時間 t $[ms]$ を比較した.
  (Pollard's ρ algorithm については, 最適な m についても考察)

- n が大きい場合, 理論的にはステップ数 s が $\sqrt{n}$ に比例.
  さらに, 計算時間 t はステップ数 s に比例？
  $\rightarrow$ 計算時間 t も $\sqrt{n}$ に比例？ $t/\sqrt{n}$ が定数に収束する？

  $\rightarrow$ $t/\sqrt{n}$ (計算量対時間比と呼ぶ) を求め,
  計算が困難なほど位数の大きな楕円曲線における ECDLP について
  解読に要する時間の予測を試みた.

実験

アルゴリズム名の表記

- 総当たり法 → 総当たり
- Shanks' Babystep-Giantstep Algorithm → BSGS
- Pollard's ρ algorithm I $(m = 3)$ → Rho-I(3)
- Pollard's ρ algorithm II $(m = 3)$ → Rho-II(3)

実験に用いた計算環境

- OS:Windows 10 Pro
- プロセッサ:Intel(R)Core(TM)i7-8650U CPU @1.90GHz 2.11GHz
- 実装 RAM:16.0GB
- システムの種類:64 ビットオペレーティングシステム, x64 ベースプロセッサ
- 数式処理プログラム:Sagemath 8.8

実験

以下に従って楕円曲線を選び, $\log_P Q$ を求める ECDLP を作成した.

1. 楕円曲線の定義式 :
   - $y^2 = x^3 + 7$ (ビットコインに使用されている楕円曲線の定義式)
   - $y^2 = x^3 + 2$
   - $y^2 = x^3 - 3x + C_N$
     ($C_N := 1895828628556660800040866854449392641550468096867932107578723467256 4$)
2. 係数体は, 以下の条件を満たす $\mathbb{F}_p$ とした.
   - p のビット数は $10, 12, 14, \cdots, 30$
   - 曲線が non-singular
   - 群 $E(\mathbb{F}_p)$ が素数位数の巡回群
3. 点 P, Q をランダムに選ぶ. これを任意の回数行うことで, ECDLP を複数作成した.

実験

楕円曲線の定義式の選択は, SafeCurves[10] を参考にした.

Evaluation targets

The SafeCurves web site reports security assessments of various specific curves. Some of the curves listed on this site are deployed or have been proposed for deployment. Some of the curves are merely toy examples meant to illustrate how curves can fail to meet various security criteria.

"Safe" in the following table means that a curve meets all SafeCurves requirements. The curves are sorted in increasing order of the prime ℓ.

Curve	Safe?	Details
Anomalous	False	y^2 = x^3+153478980553715805908905767213143188232075319630356375030962 92x+744438644993450597036786520456912472835066187095959340427961 5 modulo p = 176763184868488930309615830187786706104890165129833517396771 43 Created as an illustration of additive transfer and small discriminant.
M-221	True	y^2 = x^3+117050x^2+x modulo p = 2^221 - 3 2013 Aranha–Barreto–Pereira–Ricardini (formerly named Curve2213)
E-222	True	x^2+y^2 = 1+160102x^2y^2 modulo p = 2^222 - 117 2013 Aranha–Barreto–Pereira–Ricardini
NIST P-224	False	y^2 = x^3-3x+18958286285566608000408668544493926415504680968679321075787234672564 modulo p = 2^224 - 2^96 + 1 2000 NIST; also in SEC 2
Curve1174	True	x^2+y^2 = 1-1174x^2y^2 modulo p = 2^251 - 9 2013 Bernstein–Hamburg–Krasnova–Lange
Curve25519	True	y^2 = x^3+486662x^2+x modulo p = 2^255 - 19 2006 Bernstein
BN(2,254)	False	y^2 = x^3+0x+2 modulo p = 16798108731015832284940804142231733909889187121439069848933715426072753864723 2011 Pereira–Simplicio–Naehrig–Barreto pairing-friendly curve. Included as an illustration of multiplicative transfer and small discriminant.
brainpoolP256t1	False	y^2 = x^3-3x+46214326585032579593829631435610129746736367449296220983687490401182983727876 modulo p = 76884956397045344220809746629001649093037950200943055203735601445031516197751 2005 Brainpool
ANSSI FRP256v1	False	y^2 = x^3-3x+10774454112204268879215520724278245515038276404308911414109663449756730154783 9 modulo p = 10945457133169727861767072503073512814596934964786873815720132355619602239385 9 2011 ANSSI
NIST P-256	False	y^2 = x^3-3x+41058363725152142129326129780047268409114441015993725554835256314039467401291 modulo p = 2^256 - 2^224 + 2^192 + 2^96 - 1 2000 NIST; also in SEC 2 and NSA Suite B
secp256k1	False	y^2 = x^3+0x+7 modulo p = 2^256 - 2^32 - 977 SEC2
E-382	True	x^2+y^2 = 1-67254x^2y^2 modulo p = 2^382 - 105

実験 -実験 1-

実験内容

総当たり, BSGS, Rho-I, Rho-II で ECDLP の解読を行い, それぞれのステップ数 sを求めた. ただし, 1 つの $E/\mathbb{F}_p$ について ECDLP を 1000 問作成して解読し, そのステップ数の平均を, 各アルゴリズムが要したステップ数 s として定めた.

- 定義式 : $y^2 = x^3 + 7$, $y^2 = x^3 + 2$, $y^2 = x^3 - 3x + C_N$
- Rho-I, Rho-II における直和分割の個数 : $m = 3, 4, \cdots, 50$

実験 -実験 1-

$y^2 = x^3 + 7$ におけるステップ数

総当たり,BSGS,Rho-I(期待値との比較)

標数	p	547	3511	11839	47017	194119	881539	2744713
	bit	10	12	14	16	18	20	22
n		547	3433	12049	47353	194917	880981	2746417
sの期待値	BSGS	35.082	87.888	164.652	326.411	662.241	1407.909	2485.848
	Rho-I	30.313	74.434	138.574	273.730	554.331	1177.368	2078.032
s	総当たり	273.488	1686.259	6287.919	23409.155	95410.809	430588.574	1334742.700
	BSGS	35.920	88.071	167.671	325.885	658.364	1398.057	2463.541
	Rho-I(3)	47.045	123.323	240.938	503.749	1096.188	2400.395	4537.627
	Rho-I(4)	38.838	96.634	183.229	365.701	759.749	1580.652	2857.279
	Rho-I(5)	36.404	88.595	164.888	328.418	654.931	1398.207	2491.537
	Rho-I(6)	34.472	85.673	160.360	305.563	631.797	1331.963	2374.995
	Rho-I(7)	32.912	83.971	148.607	296.930	616.520	1289.028	2357.589
	Rho-I(8)	32.865	81.428	149.799	300.260	587.900	1284.035	2252.272
	Rho-I(9)	33.356	82.486	148.688	292.405	577.755	1251.140	2258.565
	Rho-I(10)	32.664	80.762	151.439	289.784	609.567	1249.031	2209.169
	Rho-I(11)	32.434	79.250	148.489	291.293	597.774	1241.638	2222.169
	Rho-I(12)	32.322	78.051	146.949	281.465	599.103	1235.939	2104.026
	Rho-I(13)	32.042	79.215	143.234	283.498	569.152	1210.706	2106.247
	Rho-I(14)	32.282	77.214	146.387	284.327	581.773	1211.617	2160.343
	Rho-I(15)	31.774	77.314	143.443	286.829	572.197	1235.438	2122.745
	Rho-I(16)	31.792	78.600	141.103	285.901	574.317	1193.242	2188.094
	Rho-I(17)	31.468	75.397	145.101	284.538	572.965	1211.300	2096.734
	Rho-I(18)	31.002	76.061	144.361	282.251	587.282	1245.227	2158.488
	Rho-I(19)	30.657	77.178	145.758	280.654	597.035	1211.766	2187.496
	Rho-I(20)	31.376	75.331	144.431	287.889	577.523	1205.988	2143.799
	Rho-I(21)	32.011	79.287	142.979	283.639	568.427	1201.866	2149.878
	Rho-I(22)	31.248	74.361	140.473	278.349	568.434	1229.791	2168.768
	Rho-I(23)	30.891	78.010	142.156	280.452	568.827	1226.291	2180.467
	Rho-I(24)	30.786	77.754	139.872	280.485	577.171	1176.654	2175.949
	Rho-I(25)	30.683	76.372	143.372	276.264	570.766	1202.800	2088.978
	Rho-I(26)	30.431	76.264	143.216	273.736	564.792	1168.765	2069.492
	Rho-I(27)	31.565	76.225	143.182	281.464	581.500	1206.772	2086.471
	Rho-I(28)	30.156	77.263	140.269	279.540	577.939	1193.366	2043.145
	Rho-I(29)	30.485	77.928	142.928	271.781	558.278	1187.583	2118.069
	Rho-I(30)	31.073	75.277	145.646	281.322	572.544	1218.928	2147.381
	Rho-I(31)	31.048	75.179	142.552	284.724	565.167	1207.605	2100.650
	Rho-I(32)	30.312	75.214	138.733	279.176	561.306	1234.199	2172.899
	Rho-I(33)	30.898	74.129	137.201	278.384	564.324	1183.022	2116.767
	Rho-I(34)	29.972	74.660	144.447	281.426	560.600	1189.205	2127.349
	Rho-I(35)	30.841	77.577	139.864	278.723	567.305	1187.285	2069.279
	Rho-I(36)	31.427	76.723	138.705	278.689	573.307	1196.072	2123.811
	Rho-I(37)	29.755	74.887	140.457	289.426	567.559	1190.085	2146.196
	Rho-I(38)	30.141	76.378	143.159	273.748	559.848	1203.061	2112.161
	Rho-I(39)	29.810	75.921	140.332	281.122	574.754	1167.207	2124.322
	Rho-I(40)	30.451	74.646	142.400	274.213	572.518	1186.992	2123.668
	Rho-I(41)	29.880	74.606	136.437	274.015	550.474	1165.311	2187.536
	Rho-I(42)	30.644	74.087	140.591	276.476	559.104	1184.640	2043.446
	Rho-I(43)	31.077	76.055	137.873	282.601	575.343	1183.772	2150.929
	Rho-I(44)	30.062	78.395	140.050	273.786	561.108	1205.835	2035.671
	Rho-I(45)	30.383	75.281	138.912	282.872	563.097	1180.467	2126.154
	Rho-I(46)	30.869	73.136	141.358	279.089	579.024	1178.257	2150.056
	Rho-I(47)	30.402	75.086	139.484	278.555	565.882	1213.603	2106.513
	Rho-I(48)	30.340	75.554	139.266	285.036	570.035	1209.485	2082.557
	Rho-I(49)	30.033	74.703	136.796	286.856	557.713	1185.253	2112.565
	Rho-I(50)	30.431	76.996	140.614	277.811	571.844	1196.336	2077.680

総当たり,BSGS,Rho-I(最多・最少)

標数	p	547	3511	11839	47017	194119	881539	2744713
	bit	10	12	14	16	18	20	22
n		547	3433	12049	47353	194917	880981	2746417
sの期待値	BSGS	35.082	87.888	164.652	326.411	662.241	1407.909	2485.848
	Rho-I	30.313	74.434	138.574	273.730	554.331	1177.368	2078.032
s	総当たり	273.488	1686.259	6287.919	23409.155	95410.809	430588.574	1334742.700
	BSGS	35.920	88.071	167.671	325.885	658.364	1398.057	2463.541
	Rho-I(3)	47.045	123.323	240.938	503.749	1096.188	2400.395	4537.627
	Rho-I(4)	38.838	96.634	183.229	365.701	759.749	1580.652	2857.279
	Rho-I(5)	36.404	88.595	164.888	328.418	654.931	1398.207	2491.537
	Rho-I(6)	34.472	85.673	160.360	305.563	631.797	1331.963	2374.995
	Rho-I(7)	32.912	83.971	148.607	296.930	616.520	1289.028	2357.589
	Rho-I(8)	32.865	81.428	149.799	300.260	587.900	1284.035	2252.272
	Rho-I(9)	33.356	82.486	148.688	292.405	577.755	1251.140	2258.565
	Rho-I(10)	32.664	80.762	151.439	289.784	609.567	1249.031	2209.169
	Rho-I(11)	32.434	79.250	148.489	291.293	597.774	1241.638	2222.169
	Rho-I(12)	32.322	78.051	146.949	281.465	599.103	1235.939	2104.026
	Rho-I(13)	32.042	79.215	143.234	283.498	569.152	1210.706	2106.247
	Rho-I(14)	32.282	77.214	146.387	284.327	581.773	1211.617	2160.343
	Rho-I(15)	31.774	77.314	143.443	286.829	572.197	1235.438	2122.745
	Rho-I(16)	31.792	78.600	141.103	285.901	574.317	1193.242	2188.094
	Rho-I(17)	31.468	75.397	145.101	284.538	572.965	1211.300	2096.734
	Rho-I(18)	31.002	76.061	144.361	282.251	587.282	1245.227	2158.488
	Rho-I(19)	30.657	77.178	145.758	280.654	597.035	1211.766	2187.496
	Rho-I(20)	31.376	75.331	144.431	287.889	577.523	1205.988	2143.799
	Rho-I(21)	32.011	79.287	142.979	283.639	568.427	1201.866	2149.878
	Rho-I(22)	31.248	74.361	140.473	278.349	568.434	1229.791	2168.768
	Rho-I(23)	30.891	78.010	142.156	280.452	568.827	1226.291	2180.467
	Rho-I(24)	30.786	77.754	139.872	280.485	577.171	1176.654	2175.949
	Rho-I(25)	30.683	76.372	143.372	276.264	570.766	1202.800	2088.978
	Rho-I(26)	30.431	76.264	143.216	273.736	564.792	1168.765	2069.492
	Rho-I(27)	31.565	76.225	143.182	281.464	581.500	1206.772	2086.471
	Rho-I(28)	30.156	77.263	140.269	279.540	577.939	1193.366	2043.145
	Rho-I(29)	30.485	77.928	142.928	271.781	558.278	1187.583	2118.069
	Rho-I(30)	31.073	75.277	145.646	281.322	572.544	1218.928	2147.381
	Rho-I(31)	31.048	75.179	142.552	284.724	565.167	1207.605	2100.650
	Rho-I(32)	30.312	75.214	138.733	279.176	561.306	1234.199	2172.899
	Rho-I(33)	30.898	74.129	137.201	278.384	564.324	1183.022	2116.767
	Rho-I(34)	29.972	74.660	144.447	281.426	560.600	1189.205	2127.349
	Rho-I(35)	30.841	77.577	139.864	278.723	567.305	1187.285	2069.279
	Rho-I(36)	31.427	76.723	138.705	278.689	573.307	1196.072	2123.811
	Rho-I(37)	29.755	74.887	140.457	289.426	567.559	1190.085	2146.196
	Rho-I(38)	30.141	76.378	143.159	273.748	559.848	1203.061	2112.161
	Rho-I(39)	29.810	75.921	140.332	281.122	574.754	1167.207	2124.322
	Rho-I(40)	30.451	74.646	142.400	274.213	572.518	1186.992	2123.668
	Rho-I(41)	29.880	74.606	136.437	274.015	550.474	1165.311	2187.536
	Rho-I(42)	30.644	74.087	140.591	276.476	559.104	1184.640	2043.446
	Rho-I(43)	31.077	76.055	137.873	282.601	575.343	1183.772	2150.929
	Rho-I(44)	30.062	78.395	140.050	273.786	561.108	1205.835	2035.671
	Rho-I(45)	30.383	75.281	138.912	282.872	563.097	1180.467	2126.154
	Rho-I(46)	30.869	73.136	141.358	279.089	579.024	1178.257	2150.056
	Rho-I(47)	30.402	75.086	139.484	278.555	565.882	1213.603	2106.513
	Rho-I(48)	30.340	75.554	139.266	285.036	570.035	1209.485	2082.557
	Rho-I(49)	30.033	74.703	136.796	286.856	557.713	1185.253	2112.565
	Rho-I(50)	30.431	76.996	140.614	277.811	571.844	1196.336	2077.680

Rho-II(最多・最少)

標数	p	547	3511	11839	47017	194119	881539	2744713
	bit	10	12	14	16	18	20	22
n		547	3433	12049	47353	194917	880981	2746417
s	Rho-II(3)	38.543	101.720	202.827	419.245	862.866	1944.628	3633.208
	Rho-II(4)	31.422	80.885	152.934	288.814	619.227	1314.354	2284.849
	Rho-II(5)	28.768	72.280	137.001	273.093	552.934	1135.385	2063.606
	Rho-II(6)	28.013	71.076	131.661	259.110	510.049	1100.332	1943.237
	Rho-II(7)	27.279	67.025	126.213	245.395	507.166	1079.850	1915.664
	Rho-II(8)	26.671	67.607	123.147	242.095	493.634	1052.115	1874.270
	Rho-II(9)	25.964	65.435	126.227	238.289	489.704	1040.131	1786.262
	Rho-II(10)	26.066	64.680	119.062	242.265	498.202	1057.490	1805.020
	Rho-II(11)	25.765	62.422	119.075	239.343	476.075	1014.097	1797.229
	Rho-II(12)	25.532	63.179	121.866	233.224	479.494	1006.540	1813.831
	Rho-II(13)	25.709	62.848	117.872	233.890	488.115	1020.623	1711.149
	Rho-II(14)	25.514	62.227	115.259	228.938	476.430	1026.264	1763.085
	Rho-II(15)	25.474	63.484	118.402	228.952	481.980	1015.250	1819.964
	Rho-II(16)	25.628	63.541	118.199	234.543	474.490	997.690	1764.495
	Rho-II(17)	25.309	61.686	120.251	227.845	462.379	997.693	1740.113
	Rho-II(18)	25.335	64.250	118.473	232.706	459.200	1002.993	1793.827
	Rho-II(19)	24.579	60.789	118.357	229.095	469.669	959.915	1703.603
	Rho-II(20)	25.786	64.471	118.096	236.160	478.878	1034.599	1798.025
	Rho-II(21)	24.802	61.971	114.844	234.588	455.216	1007.128	1734.122
	Rho-II(22)	24.885	63.447	118.482	229.381	466.510	1005.399	1726.162
	Rho-II(23)	25.272	60.793	116.699	233.195	462.452	981.816	1761.026
	Rho-II(24)	25.013	64.166	116.607	235.029	468.256	1004.890	1771.809
	Rho-II(25)	24.995	62.431	114.597	228.457	475.993	972.390	1798.504
	Rho-II(26)	25.504	61.814	116.521	231.583	479.444	992.457	1758.936
	Rho-II(27)	24.647	62.212	116.753	223.745	460.284	986.541	1734.951
	Rho-II(28)	24.506	64.987	116.941	228.250	465.614	962.495	1761.806
	Rho-II(29)	24.841	61.276	116.340	225.956	472.212	988.065	1680.871
	Rho-II(30)	25.387	63.551	114.519	243.796	461.715	1002.624	1736.379
	Rho-II(31)	25.254	62.397	116.708	228.276	476.216	962.339	1700.236
	Rho-II(32)	24.373	62.009	117.924	225.221	477.589	984.062	1736.772
	Rho-II(33)	25.964	63.975	115.775	230.646	463.536	942.920	1774.100
	Rho-II(34)	25.348	62.630	115.100	231.178	464.809	991.535	1723.691
	Rho-II(35)	25.245	62.277	116.555	228.275	471.504	979.302	1707.627
	Rho-II(36)	25.256	63.058	115.008	230.363	458.904	970.873	1754.686
	Rho-II(37)	25.415	59.878	116.319	217.852	479.563	962.338	1681.031
	Rho-II(38)	25.410	62.462	115.035	230.946	448.164	1000.384	1766.243
	Rho-II(39)	24.544	60.714	112.589	234.781	458.761	981.923	1749.607
	Rho-II(40)	24.579	61.597	114.323	227.888	453.608	1001.853	1700.406
	Rho-II(41)	24.953	60.256	114.417	229.711	466.313	918.297	1736.455
	Rho-II(42)	24.964	61.229	115.951	233.232	457.266	976.425	1714.383
	Rho-II(43)	25.642	60.152	115.016	223.957	460.035	964.876	1733.855
	Rho-II(44)	25.360	63.836	116.808	225.090	458.364	973.530	1776.841
	Rho-II(45)	25.333	62.003	115.704	230.258	455.657	1004.581	1676.743
	Rho-II(46)	24.549	62.229	118.890	227.277	467.338	982.590	1699.967
	Rho-II(47)	24.744	61.891	117.084	226.497	470.954	994.089	1700.001
	Rho-II(48)	25.471	62.427	115.801	228.336	455.998	941.596	1702.607
	Rho-II(49)	24.338	60.621	113.799	225.601	456.488	975.594	1705.841
	Rho-II(50)	24.811	59.573	116.956	232.146	464.016	976.814	1732.133

実験 -実験 1-

ステップ数 s について

- ステップ数が最少：Rho-II （m の値は十分大きくとる必要がある. ）
- 総当たりは, 他のアルゴリズムに比べてステップ数が著しく多い.

f における直和分割の個数 m について

- Rho-I,II 共に, m が小さいほどステップ数が多くなる傾向があった.
- 「期待値との差が大きい 5 つ」と「ステップ数が多い 5 つ」が一致.
  「期待値との差が小さい 5 つ」と「ステップ数が少ない 5 つ」は, 分布の様子が似ていた.
- 期待値との差が大きい 5 つは $m \leq 10$,
  期待値との差が小さい 5 つは $m \geq 16$ の範囲に分布.

実験 -実験 2-

実験内容

総当たり, BSGS, Rho-I, Rho-II で ECDLP の解読を行い, それぞれの計算時間 tを求めた. ただし, 1 つの $E/\mathbb{F}_p$ について ECDLP を 30 問作成・解読して計算時間の平均を求め, それを各アルゴリズムが要した計算時間 t (ms) として定めた.

さらに, BSGS, Rho-I, Rho-II については計算量対時間比 $t/\sqrt{n}$を求め, 比較した.

- 定義式 : $y^2 = x^3 + 7$
- Rho-I と Rho-II における直和分割の個数 : $m = 3, 8, 20$

(m の値は, Pollard[11]p918,Sattler and Schnorr[12]p66,Teske[13]p1644 を参考に選択)

実験 -実験 2-

$y^2 = x^3 + 7$ における計算時間

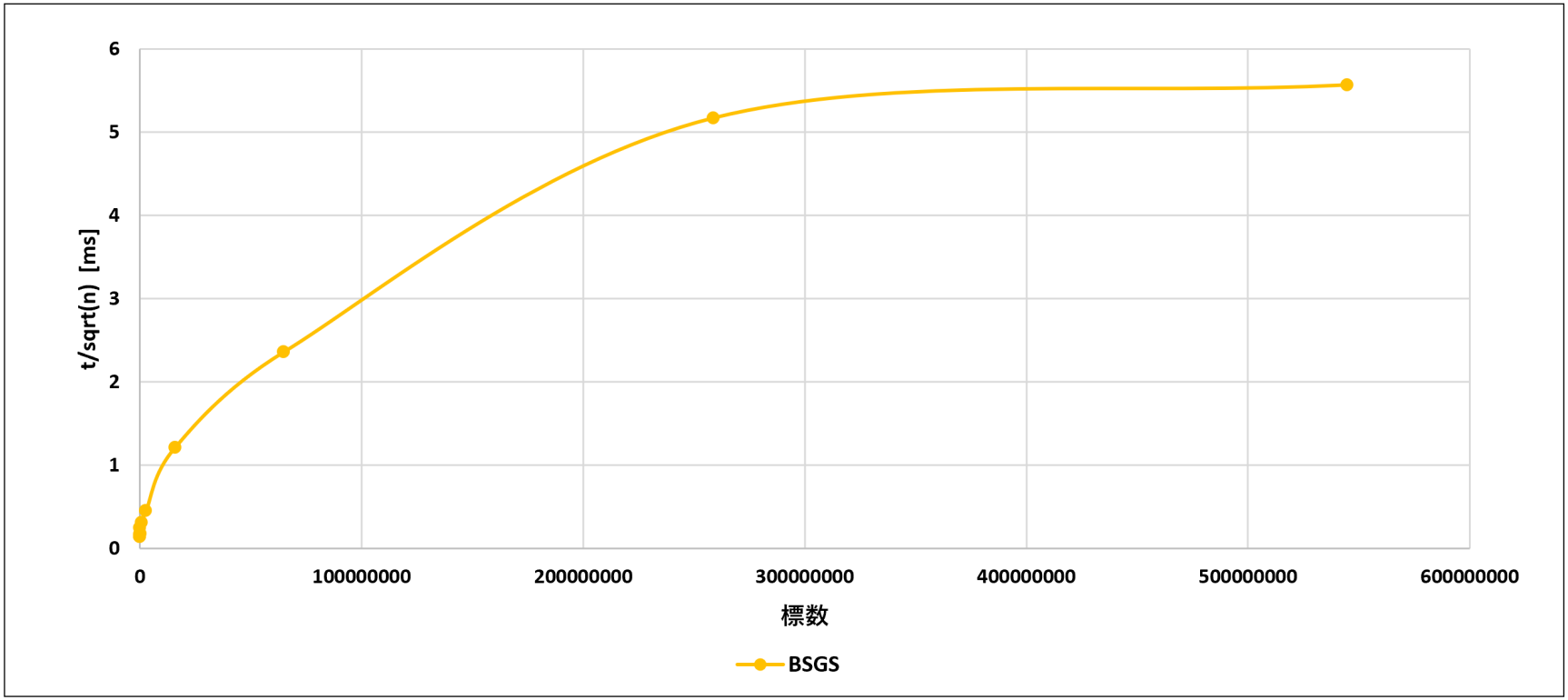
標数	p	547	3511	11839	47017	194119	881539	2744713	15801199	64971103	258652951	544707991
	bit	10	12	14	16	18	20	22	24	26	28	30
n		547	3433	12049	47353	194917	880981	2746417	15798577	64976101	258684961	544722709
t [ms]	総当たり	9.27	56.2	196	780	2380	11500	32300				
	BSGS	5.80	8.25	15.3	37.4	78.4	296	754	4810	19000	83100	130000
	Rho-I(3)	6.16	15.1	40.8	136	371	1720	6540	46900	158000		
	Rho-I(8)	8.76	14.0	23.7	52.2	205	407	2530	11400	37100		
	Rho-I(20)	17.9	24.6	42.2	69.2	160	552	1430	9770	38400		
	Rho-II(3)	7.88	15.2	25.1	43.4	76.3	178	286	714	1330	3270	4410
	Rho-II(8)	9.54	16.7	23.0	35.0	63.1	119	184	380	708	1660	2600
	Rho-II(20)	18.0	27.1	35.7	52.6	73.0	126	215	430	825	1620	2140

$y^2 = x^3 + 7$ における計算量対時間比

標数	p	547	3511	11839	47017	194119	881539	2744713	15801199	64971103	258652951	544707991
	bit	10	12	14	16	18	20	22	24	26	28	30
n		547	3433	12049	47353	194917	880981	2746417	15798577	64976101	258684961	544722709
t/sqrt(n) [ms]	BSGS	0.248	0.141	0.139	0.172	0.178	0.315	0.455	1.21	2.36	5.17	5.57
	Rho-I(3)	0.263	0.257	0.372	0.623	0.840	1.83	3.94	11.8	19.7		
	Rho-I(8)	0.375	0.239	0.216	0.240	0.465	0.434	1.53	2.86	4.60		
	Rho-I(20)	0.767	0.420	0.385	0.318	0.362	0.588	0.867	2.46	4.77		
	Rho-II(3)	0.337	0.259	0.229	0.199	0.173	0.189	0.173	0.180	0.165	0.203	0.189
	Rho-II(8)	0.408	0.285	0.210	0.161	0.143	0.127	0.111	0.0956	0.0878	0.103	0.111
	Rho-II(20)	0.768	0.462	0.325	0.242	0.165	0.134	0.130	0.108	0.102	0.100	0.0918

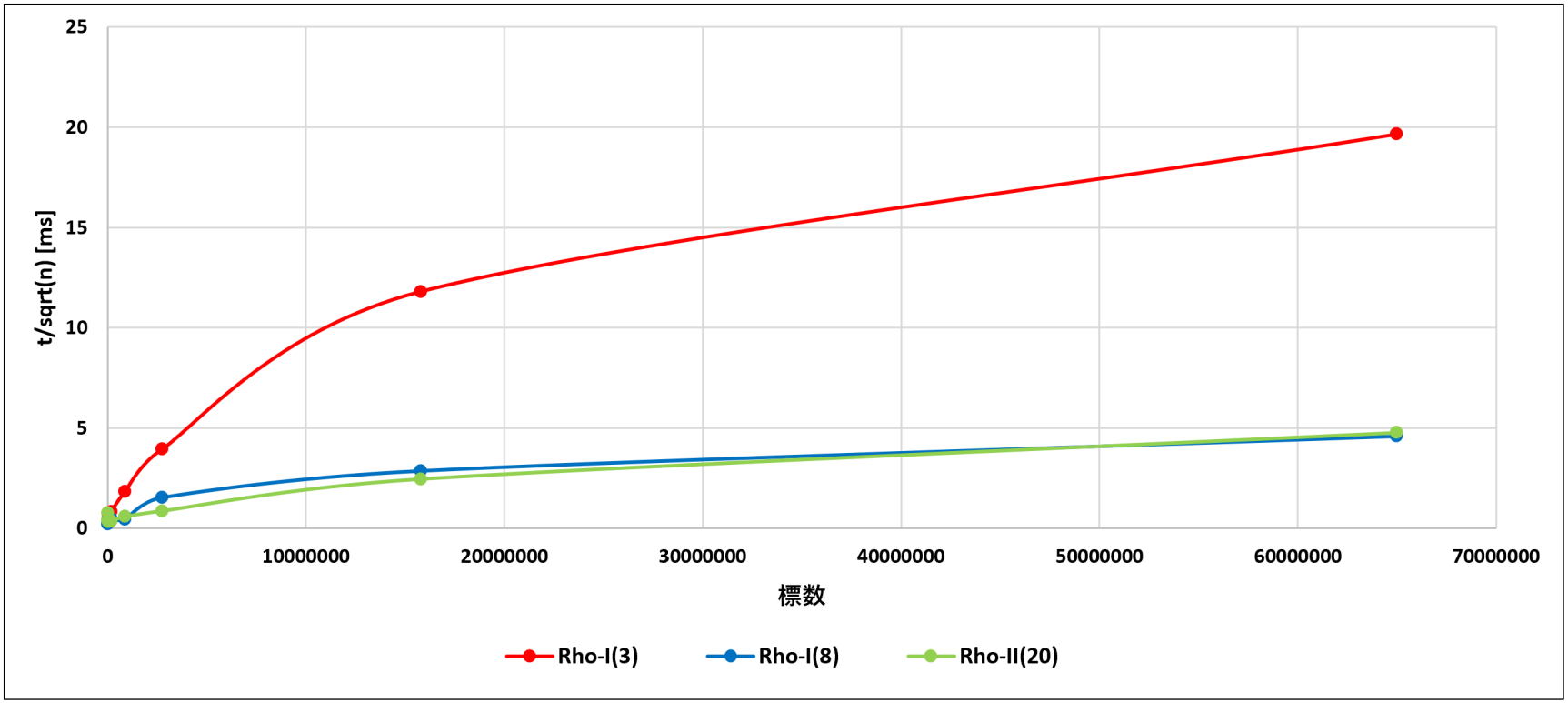
実験 -実験 2-

$y^2 = x^3 + 7$ における計算量対時間比 (BSGS)



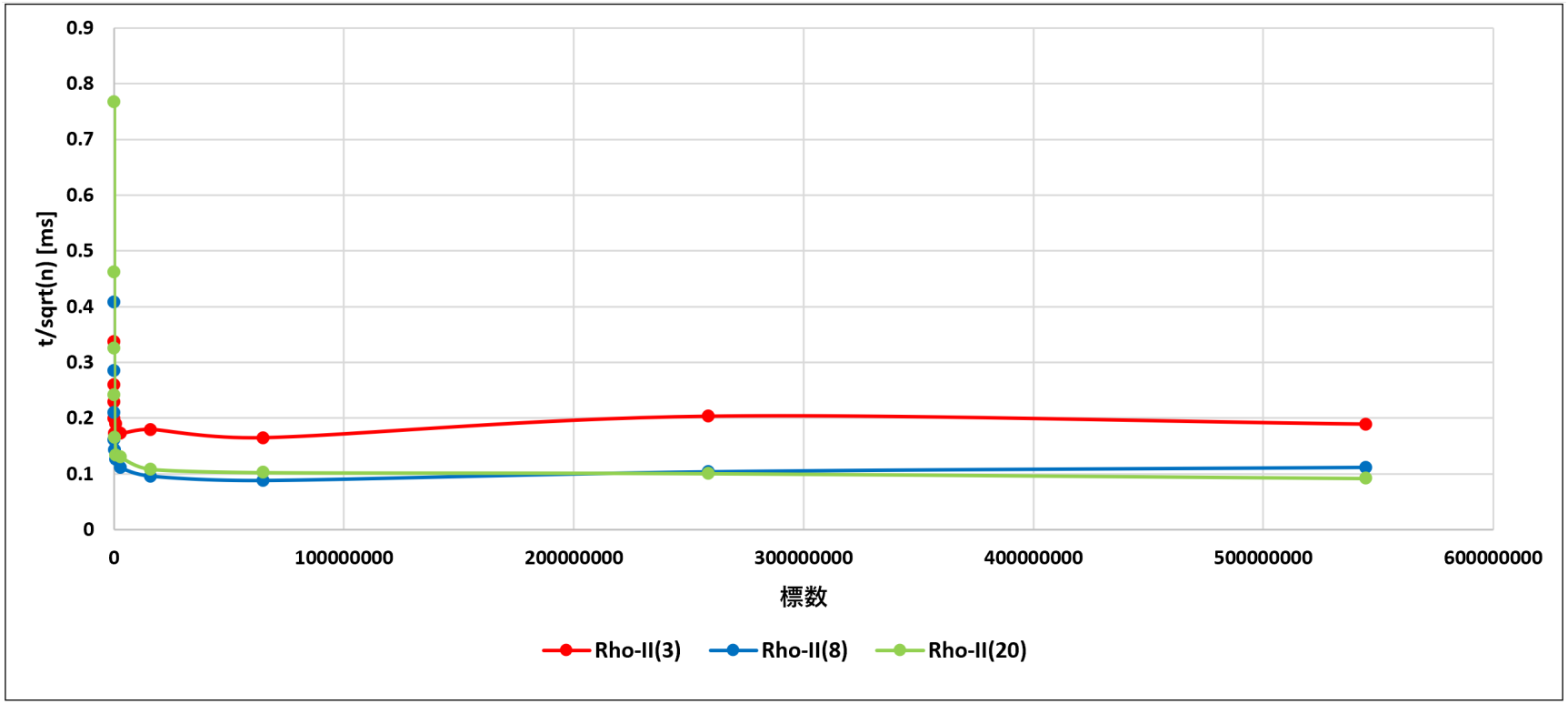
実験 -実験 2-

$y^2 = x^3 + 7$ における計算量対時間比 (Rho-I)



実験 -実験 2-

$y^2 = x^3 + 7$ における計算量対時間比 (Rho-II)



実験 -実験 2-

計算時間 t について

- 計算時間が最短のアルゴリズムは
  14 ビット以下：BSGS
  16〜26 ビット：Rho-Ⅱ(8)
  28 ビット以上：Rho-Ⅱ(20)
- 総当たりは, 12 ビット以上においては常に最長.

f における直和分割の個数 m について

- Rho-Ⅰ において,
  14 ビット以下：$m = 20$ の計算時間が最長.
  16 ビット以上：$m = 3$ が最長.
- Rho-Ⅱ についても, 16・18 ビットを境目として同様の逆転現象.

計算量対時間比 $t/\sqrt{n}$ について

- BSGS,Rho-Ⅱ：標数を大きくすると計算量対時間比が収束する傾向.

結論と考察

- 標数が大きい場合, ステップ数・計算時間共に
  Rho-Ⅱ が最も効率的であった.
  (ただし, 直和分割の個数 m は十分大きくとる必要がある.)

- Rho-Ⅰ と Rho-Ⅱ について, $m = 3, 8, 20$ を比べると
  ステップ数 : 常に $m = 20$ が最も少ない
  計算時間　 : 標数が小さい場合においては $m = 20$ が最も長い
  $\rightarrow$ 関数 f の定義にかかる時間などが影響
  (m が大きいほど, f の定義のために多くのランダムな点
  $M_1, M_2, \cdots, M_m$ を求める必要がある.)

- 「十分にランダムで効率的な関数 f」の実現には,
  $m \geq 11$ であることが必要であり, 特に $m \geq 16$ が望ましい.

結論と考察

- Rho-Ⅱ(20) : 標数を大きくすると計算量対時間比が定数に近づく傾向.
  (30 ビットで $t/\sqrt{n} = 0.0918$, 挙動が既に安定.)

- ビットコインに使用されている楕円曲線「secp256k1」
  (定義式 : $y^2 = x^3 + 7$, 標数 256 ビット ([4],[10])) について考えた.

  今回と同様の実験環境で, Rho-Ⅱ(20) を用いて解読を行った場合,
  計算量対時間比は約 0.0918 になると考えられる.

  $t/\sqrt{n} = 0.0918$ と仮定し, secp256k1 の位数 n をもとに計算した結果,
  ECDLP の解読に約 9.91×10^{26} 年かかると予測できた.
  (ちなみに, 宇宙の誕生が約 1.38×10^{10} 年前 ([14]).)

- 実用的な楕円曲線暗号についてより正確な情報を得るためには, さらに多くの試行と標数の拡大を行うことが必要.

参考文献

[1] 辻井重男, 笠原正雄編著: 暗号理論と楕円曲線. 森北出版, 2008.

[2] 清藤武暢: 次世代公開鍵暗号「楕円曲線暗号」とその適切な活用に向けて. 第 14 回情報セキュリティ・シンポジウム,2012.

[3] EdLyn Teske: *Speeding Up Pollard's Rho Method for Computing Discrete Logarithms.* Algorithmic number theory, 1998.

[4] *Bitcoin* 日本語情報サイト. https://jpbitcoin.com/

[5] Afred J. Menezes and Neal Koblitz: *Elliptic Curve Public Key Cryptosystems.* Springer Science+Business Media, 1993.

[6] 川又雄二郎: 射影空間の幾何学. 朝倉書店, 2001.

[7] J. H. Silverman: *The Arithmetic of Elliptic Curves.* 2nd Edition, GTM106, Springer, 2016.

[8] Steven D. Galbraith, Ping Wang and Fangguo Zhang: *Computing Elliptic Curve Discrete Logarithms with Improved Baby-step Giant-step Algorithm.* Adv. Math. Commun. 11(2017), no. 3.

[9] 宮地充子: 代数学から学ぶ暗号理論. 日本評論社, 2012.

[10] *SafeCurves:choosing safe curves for elliptic-curve cryptography.* http://safecurves.cr.yp.to/

[11] J. M. Pollard: *Monte Carlo Methods for Index Computation (mod p).* Mathematics of Computation, volume 32, no.143, 1978, 918–924.

[12] J.Sattler and C. P. Schnorr: *Generating Random Walks in Groups.* Ann. Univ. Sci. Budapest. Sect. Comput. 6, 1985.

[13] EdLyn Teske: *A Space Efficient Algorithm for Group Structure Computation.* Mathematics of Computation, volume 67, no.224, 1998, 1637–1663.

[14] European Space Agency: *Cosmic Detectives.* 2013. https://www.esa.int/Science_Exploration/Space_Science/Cosmic_detectives

[15] J. H. シルバーマン, J. テイト著: 楕円曲線論入門. 足立恒雄, 木田雅成, 小松啓一, 田谷久雄 訳, 丸善出版, 2001.

[16] *sonickun.log.* http://sonickun.hatenablog.com/

[17] 小暮昭仁: 有限体上での楕円曲線の有理点群位数計算. 早稲田大学大学院修士論文, 2019.