楕円曲線上の離散対数問題

計算アルゴリズムの実装と比較

早稲田大学大学院　基幹理工学研究科
数学応用数理専攻　楫研究室
潮谷真奈 (5118A037-1)

2020/2/7

1　概要

楕円曲線暗号は, 1985 年頃に N.Koblitz と V.S.Miller によって提案され, 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 ([1]p53,[2]p11,[7]p376). その根拠となるのが, 楕円曲線上の離散対数問題 (ECDLP)の困難性である. 本論文では, 計算機を使用して ECDLP の作成・解読を行い, 複数のアルゴリズムについて, 要したステップ数 s と計算時間 t を比較した. 特に, Pollard's ρ algorithm については, 最適な直和分割の個数 m についても調べた. また, P の位数 n が大きければ $t/\sqrt{n}$ (本論文では計算量対時間比と呼ぶ) の値が定数に収束するという仮定の下, 計算量対時間比の挙動を調べた. さらに, ビットコインの安全性を保証するために使われている楕円曲線暗号の解読に要する時間を予測した.

2　定義

- 楕円曲線 $E/K : y^2 = x^3 + ax + b$ $(a, b \in K, \mathrm{char}(K) \neq 2, 3)$
- 楕円曲線 E/K は必ず, 無限遠点 $[0 : 1 : 0]$ を通る. これを O と表記する.
- $E(K) := \{(x, y) \in K^2 \mid y^2 = x^3 + ax + b\} \cup \{O\}$
- 二項演算 $+$ (単位元は O) :
  任意の点 $P, Q \in E(K)$ について,
  - $P \neq Q$ のとき, $P * Q$ は P, Q を通る直線と E とのもう 1 つの交点.
  - $P = Q$ のとき, $P * P$ は P における E の接線と E とのもう 1 つの交点. (P が変曲点のときは $P * P = P$)
  - $P + Q := O * (P * Q)$
- 楕円曲線上の離散対数問題 :
  $P \in E(\mathbb{F}_q)$ と $Q \in \langle P \rangle$ が与えられたとき, 離散対数 $\log_P Q = \min\{j \in \mathbb{Z}_{\geq 0} \mid Q = jP\}$ を求める問題.

3　ECDLP の計算アルゴリズム

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 : 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,
   2. のリスト上の点と一致する $Q + jR$ $(0 \leq j < N)$ を見つける.
4. $iP = Q + jR$ であれば, $Q = (i + jN)P$ となり, $\log_P Q \equiv i + jN \pmod{n}$ が成立.

Pollard's ρ algorithm I ([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. $f : E(\mathbb{F}_q) \to E(\mathbb{F}_q)$, $f(S) = S + M_l$ $(S \in G_l)$
4. $a_0, b_0 \in \{0, \cdots, n-1\}$ をランダムに選ぶ.
   点列 $(S_i) : S_0 = a_0 P + b_0 Q$, $S_i = f(S_{i-1})$ $(i \in \mathbb{N})$
5. $S_1, S_2, S_3, \cdots$ と順に求め, $S_i = S_j$ $(j \in \{0, 1, \cdots, i-1\})$ となる i を見つける.
6. $a_i P + b_i Q = a_j P + b_j Q$ であるから, $\gcd((b_j - b_i), n) = 1$ であれば
   $\log_P Q \equiv (a_i - a_j)(b_j - b_i)^{-1} \pmod{n}$.

Pollard's ρ algorithm Ⅱ ([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. $f : E(\mathbb{F}_q) \to E(\mathbb{F}_q),\ f(S) = S + M_l \ (S \in G_l)$
4. $a_0, b_0 \in \{0, \cdots, n-1\}$ をランダムに選ぶ.
   $(S_i) : S_0 = a_0 P + b_0 Q,\ S_i = f(S_{i-1})$
   $(T_i) : T_0 = a_0 P + b_0 Q,\ T_i = f \circ f(T_{i-1}) \ (i \in \mathbb{N})$
5. $S_1, T_1, S_2, T_2, \cdots$ と順に求め, $S_i = T_i \ \ (= S_{2i})$となる i を見つける.
6. $a_i P + b_i Q = a_{2i} P + b_{2i} Q$ であるから,
   $\gcd((b_{2i} - b_i), n) = 1$ であれば $\log_P Q \equiv (a_i - a_{2i})(b_{2i} - b_i)^{-1} \pmod{n}$.

4 実験

実験 1 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.

実験 2 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 $t/\sqrt{n}$を求めた.

5 結果・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 m は十分大きくとる必要がある.)
- Rho-I(3),(8),(20) を比べると, ステップ数は常に Rho-I(20) が最も少ない一方, 標数が小さい場合における計算時間は Rho-I(20) が最も長かった. 関数 f の定義にかかる時間などが影響していると考えられる.
- Rho-I,Ⅱ において, 「十分にランダムで効率的な関数」の実現には, $m \geq 11$ であることが必要であり, 特に $m \geq 16$ が望ましいという結論が得られた.
- Rho-Ⅱ(20) について, 標数を大きくしていくと計算量対時間比が定数に近づく傾向がみられた. (30 ビットで $t/\sqrt{n} = 0.0918$, 挙動が既に安定.)
- 実験結果をもとに, 現在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])) について考えると, 今回と同様の実験環境で Rho-Ⅱ(20) を用いて計算した場合, ECDLP の解読に約 9.91×10^{26} 年かかるという予測が得られた. (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である.

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.