SCIS 2022 2022 Symposium on Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics, Information and Communication Engineers

被覆攻撃の対象となる偶標数有限体上の楕円・超楕円曲線に対する同種条件下の完全分類

A classification of elliptic and hyperelliptic curves over finite fields of even characteristic subjected to the cover attack under the isogeny condition

村井 公輔 * Kousuke Murai　志村 真帆呂 † Mahoro Shimura　飯島 努 ‡ Tsutomu Iijima　趙 晋輝 * Jinhui Chao

キーワード 楕円・超楕円曲線, 被覆攻撃, GHS 攻撃

1 あらまし

GHS攻撃の一般化である被覆攻撃とは, 有限体 $k := \mathbb{F}_q$ (q : 素数のベキ乗) の d 次拡大体 $k_d := \mathbb{F}_{q^d}$上定義される楕円・超楕円曲線 C_0の離散対数問題を, k 上定義される被覆曲線 C の離散対数問題に変換する攻撃手法である. 近年, 攻撃の対象となる奇標数拡大体上の種数 $1, 2, 3$ 超楕円曲線暗号に用いられる曲線の完全分類が行われた. 百瀬らにより, 偶標数拡大体 k_d上の種数 $1, 2, 3$ 楕円・超楕円曲線 C_0に対して, 同種条件 $(g(C) = d \cdot g(C_0))$ 下で曲線の分類結果が発表されている [1]. 本論文では, 百瀬らの結果を再検討し, 分類表の検証と修正を行い, 詳細な証明を与えた.

2 被覆攻撃

k_d/k 上のフロベニウス自己同型写像を$\sigma_{k_d/k}$とし, $\sigma_{k_d/k}$の位数 d の拡張σを考える. そのとき, $k_d(C_0)/k_d(x)$ のガロア閉包 K は, $K := k_d(C_0) \cdot k_d({}^{\sigma}C_0) \cdots k_d({}^{\sigma^{d-1}}C_0)$ であり, σの固定体 K'は, $K' := \{\zeta \in K \mid \sigma(\zeta) = \zeta\} \simeq k(C)$ となる. GHS 攻撃とは, 偶標数拡大体上の楕円曲線に対し, k_d上 $J(C_0)$ の 離散対数問題 を k 上 $J(C)$ の 離散対数問題に変換して解く手法である. 現在この手法は, より一般的な曲線にも適用されており, 被覆攻撃として一般化されている.

3 分類表抜粋

以下に被覆攻撃の対象となる偶標数拡大体 k_d上の超楕円曲線 C_0に対する同種条件下での分類の一部を記す.

$C_0/k_d : y^2 + g(x)y = f(x)$, $\mathrm{char}(k_d) = 2$

$\deg\, g(x) = g(C_0) + 1, \quad \deg\, f(x) = 2g(C_0) + 2$

(I) ${}^{\sigma}g(x) = g(x)$, (II) ${}^{\sigma}g(x) \neq g(x)$

	ex) $g(C_0) = 3,\ d = 3,\ n = 2$
(I)	$L(f(x)) = f(x) + {}^{\sigma}f(x) + {}^{\sigma^2}f(x) = 0$
(II)	$g(x) = g_1(x)(x + \alpha^q)(x + \alpha^{q^2}),\ \alpha \in k_3\backslash k$ $g_1(x) \in k[x]$, $\deg\, g_1(x) \leq 2$ $L((x + \alpha)^2 f(x)) = 0$ (*1)
(II)	$g(x) = (x + \alpha^q)^2(x + \alpha^{q^2})^2$ $\alpha \in k_3\backslash k$, $L((x + \alpha)^4 f(x)) = 0$ (*2)

(*1) $L((x+\alpha)^2 f(x)) = (x+\alpha)^2\, f(x) + (x+\alpha^q)^2\, {}^{\sigma}f(x) + (x + \alpha^{q^2})^2\, {}^{\sigma^2}f(x) = 0$

(*2) $L((x+\alpha)^4 f(x)) = (x+\alpha)^4\, f(x) + (x+\alpha^q)^4\, {}^{\sigma}f(x) + (x + \alpha^{q^2})^4\, {}^{\sigma^2}f(x) = 0$

参考文献

[1] F. Momose and J. Chao, "Classification of Weil restrictions obtained by $(2, \ldots, 2)$ coverings of $\mathbb{P}^1$", preprint, 2006. Available from http://eprint.iacr.org/2006/347

* 中央大学理工学研究科情報工学専攻, 〒 112-8551 東京都文京区春日 1-13-27, Information and System Engineering Course, Graduate School of Science and Engineering Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo
† 東海大学理学部情報数理学科, 〒 259-1292 神奈川県平塚市北金目 4-1-1, Department of Mathematical Sciences, Tokai University, 4-1-1 Kitakaname, Hiratsuka-shi, Kanagawa
‡ 株式会社 光電製作所, 〒 146-0095 東京都大田区多摩川 2-13-24, Koden Electronics Co., Ltd, 2-13-24, Tamagawa, Ota-ku, Tokyo