同種条件を満たさない被覆攻撃の対象となる偶標数有限体上の楕円・超楕円曲線の分類に関する研究

A Classification of Elliptic and Hyperelliptic Curves Over Finite Fields of Even Characteristic Without the Isogeny Condition Subject to the Cover Attack

登丸尚哉・暗号認証分科会・中央大学

The cover attack to elliptic and hyperelliptic curve cryptosystems is known to solve the discrete logarithm on curves defined over an extension field by mapping it to the discrete logarithm of their covering curves over the base field. Recently, a classification of elliptic and hyperelliptic curves over finite fields of odd characteristic subject to the cover attack has been obtained. On elliptic and hyperelliptic curves over finite fields of even characteristic subject to the cover attack, a classification under the isogeny condition were reported by Momose and re-examined by Murai. In this paper, we show classification on several classes of elliptic and hyperelliptic curves over finite fields of even characteristic without the isogeny condition subject to the cover attack

研究目的・背景

被覆攻撃とは,有限体$k=\mathbb{F}_q$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楕円・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．また偶標数に関しては百瀬らにより，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($g(C)=dg(C_0)$)下で曲線の分類行われ，村井らによって再検討が行われた．本研究では，いまだ分類が行われていない，被覆攻撃の対象となる同種条件を満たさない偶標数有限体上の楕円・超楕円曲線の4つのクラスに対して分類を行った．

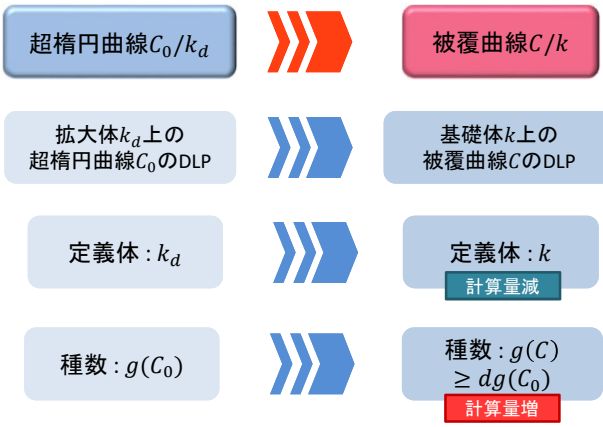
楕円・超楕円曲線

偶標数有限体 $k:=\mathbb{F}_q(q=2^r)$のd次拡大体 $k_d:=\mathbb{F}_{q^d}$ 上定義される種数$g=g(C_0)$の楕円・超楕円曲線C_0.

$$C_0/k_d\colon y^2+g(x)y=f(x)$$
$$(\deg f(x)=2g+1 \deg g(x)\le g \ or \ \deg f(x)=2g+2, \deg g(x)=g+1)$$

C_0は$g(C_0)=1$のとき楕円曲線，$g(C_0)\ge 2$のとき超楕円曲線という．楕円・超楕円曲線暗号は楕円・超楕円曲線C_0のヤコビ群上の離散対数問題(DLP)の求解が困難なことを安全性の根拠としている．

被覆攻撃の概要



被覆曲線CのDLPを解くことで，元の曲線C_0のDLPを解くことができる．定義体や種数の増減によってDLPの計算量が小さくなれば攻撃成功となる．実際，鍵長160bitの安全性を持つ曲線が，鍵長107bit程度の安全性に低下したという結果もある．
同種条件とは，$g(C)=dg(C_0)$のときをいう．
同種条件を満たさない場合は，$g(C)\ge dg(C_0)+e\ (e\in\mathbb{N})$となる．

同種条件を満たさない曲線の分類

本研究では以下の攻撃の対象となる同種条件を満たさない楕円・超楕円曲線のクラスに対して分類を行った．

$(a):g(C_0)=1,d=3,n=3$　$(b):g(C_0)=1,d=5,n=4$
$(c):g(C_0)=2,d=4,n=3$　$(d):\ d=2^n-1$
($n(\le d)$はC_0と共役な曲線$\sigma^i C_0$に対する$k_d(\sigma^i C_0)$が線形無関連となる最大の値)

$(a)(b)(c)$では楕円・超楕円曲線C_0とその共役な曲線$\sigma^i C_0$を組み合わせて構成される新たな曲線内，共役な曲線でない曲線の構造を調べることで，$dg(C_0)+e$のeの値と，C_0の係数条件などを示した．(d)では被覆攻撃の特徴から，攻撃の対象となる同種条件を満たさない楕円・超楕円曲線が存在しないことを示した．

以下に分類表より抜粋した$(a)(c)$の一部の結果を掲載する

No.	$g(C_0),d,n$	e	$g(C)$	C_0	係数条件
1	$g(C_0)=1$ $d=3$ $n=3$	1	4	$y^2+xy=ax^3+bx^2+cx$	$a\in k\backslash\{0\}, c\in k_3\backslash k, b\in k_3,\ \mathrm{Tr}(c)\neq 0$
2					$c\in k\backslash\{0\}, a\in k_3\backslash k, b\in k_3,\ \mathrm{Tr}(a)\neq 0$
3		3	6		$a,c,ac\in k_3\backslash k, b\in k_3, \mathrm{Tr}(a)=0, \mathrm{Tr}(c)\neq 0$
4					$a,c,ac\in k_3\backslash k, b\in k_3, \mathrm{Tr}(c)=0, \mathrm{Tr}(a)\neq 0$
5		4	7		$a,c,ac\in k_3\backslash k, b\in k_3, \mathrm{Tr}(a)\neq 0, \mathrm{Tr}(c)\neq 0$
6	$g(C_0)=2$ $d=4$ $n=3$	4	12	$y^2+g(x)y=f(x)$, $f(x)=ax^5+bx^4+cx^3+dx^2+ex+f$ (∗), $g(x)=(x+\alpha)(x+\alpha^q)$, $f(x)+\sigma^2 f(x)=g(x)^2 l$ (†)	$\alpha\in k_2\backslash k, b,d,f\in k_2, a,c,e\in k_4\backslash k_2,$ $l=sx,(s\in k\backslash\{0\})$
7					$\alpha\in k_2\backslash k, a,b,c,d,e,f\in k_4\backslash k_2,$ $l=sx+t,(s,t\in k\backslash\{0\})$
8		6	14	C_0は(†)と同じ $\sigma^i C_0+\sigma^j C_0:\mathbb{P}^1$ではない $i\neq j\ (i,j\in\{0,1,2\})$	$\alpha\in k_2\backslash k, a\in k_4\backslash k_2, b,c,d,e,f\in k_4$

$g(C)$は被覆曲線Cの種数の下限を表している
(∗) $\mathrm{Tr}(a)=0,\mathrm{Tr}(b)=0,\mathrm{Tr}(c)=0,\mathrm{Tr}(d)=0,\mathrm{Tr}(e)=0,\mathrm{Tr}(f)=0$

結論・今後の課題

いまだ分類の行われていない，被覆攻撃の対象となる同種条件を満たさない偶標数楕円・超楕円曲線の4つのクラスに対して分類を行い，係数条件などを明らかにした．今後の課題として，他の拡大次数に対する楕円・超楕円曲線の分類などが挙げられる．