被覆攻撃の対象となる奇標数有限体上楕円・超楕円曲線に対する被覆曲線の構成法に関する研究

On Construction of Covering Curves for Elliptic and Hyperelliptic Curves Over Finite Fields of Odd Characteristic Subject to Cover Attack

奥村祐太・暗号分科会・中央大学大学院

The covering attack is an attack method that transfers the discrete logarithm problem of an elliptic or hyperelliptic curve C_0 defined on an d-degree extension k_d of a finite field k to the discrete logarithm problem of a covering curve C defined on k. Diem's method, a method of constructing covering curves, has been applicable to only a small fraction of elliptic and hyperelliptic curves subject to the covering attack. In this study, we confirm that Diem's method is applicable to all types of elliptic and hyperelliptic curves over finite fields of odd characteristic, and show specific examples of the construction of covering curves for the types of elliptic and hyperelliptic curves for which the construction of covering curves has remained an issue. Furthermore, we discuss attack scenarios that make the covering attack more powerful, and confirm that the feasibility of such attacks does not exist.

研究目的・背景

被覆攻撃は，有限体kのd次拡大体k_d上に定義される楕円・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の離散対数問題に移す攻撃手法である．被覆攻撃に関する研究として被覆曲線の構成が挙げられる．Diemの手法と呼ばれる被覆曲線の構成手法は被覆攻撃の対象となる楕円・超楕円曲線のごく一部にのみ適用可能であった．本研究では，Diemの手法がすべての種類の奇標数有限体上楕円・超楕円曲線に対して適用可能であることを確認し，被覆曲線の構成が課題として残されていた種類の楕円・超楕円曲線についてその具体的な構成例を示す．さらに，被覆攻撃をより強力にする攻撃シナリオについて考察し，その実現可能性が存在しないことを確認する．

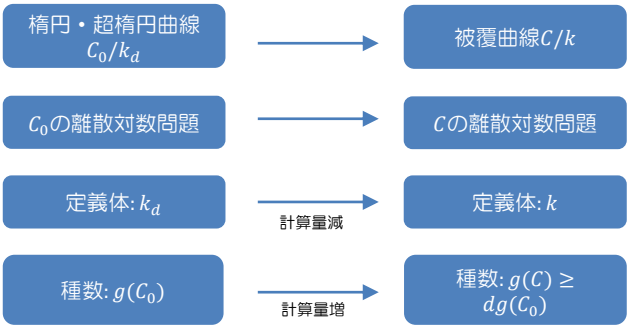
楕円・超楕円曲線

qを奇素数のべきとし，$k := \mathbb{F}_q$，k_dをkのd次拡大体とする．
このとき，k_d上定義される種数$g(C_0)$の楕円・超楕円曲線C_0は

$$C_0 : y^2 = c \cdot f(x), c \in k_d^{\times}, f(x) \in k_d[x]$$

で定義される．ただし，$f(x)$は$deg f(x) = 2g(C_0) + 1$または$2g(C_0) + 2$となる重根を持たないモニック多項式である．特に$g(C_0) = 1$のときを楕円曲線という．
楕円・超楕円曲線暗号の安全性は，楕円・超楕円曲線C_0のヤコビ群$J(C_0)$上の離散対数問題の求解困難性に基づいている．

被覆攻撃の概要



被覆攻撃を行うことでC_0の離散対数問題をCの離散対数問題に移すことができる．総合的に計算量が減少すれば攻撃成功となる．

一般の楕円・超楕円曲線に対する被覆曲線の構成

従来のDiemの手法では以下の適用条件を満たしている必要があった．

Diemの手法の適用条件

(1). dを法とした2の乗法的位数がnと一致する．
(2). $y^2 = c \cdot f(x)$のcがk_d上平方剰余である．

本研究では，上記の適用条件を満たしていない楕円曲線C_0に対する被覆曲線Cの構成を行った．以下は実験に用いたcaseである．

case	d	n	$g(C)$	$h_d(x)$	$\deg h_1(x)$
7	3	3	5	$(x-\alpha)$	3,2
10	3	3	11	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_3^q)$	0
25	7	4	17	$(x-\alpha)(x-\alpha^{q^2})(x-\alpha^{q^3})$	1,0

上記のcaseに対して，

$$(d,n) = (3,3) \to 2^n \pmod d \equiv 2^3 \pmod 3 \equiv 2$$
$$(d,n) = (7,4) \to 2^n \pmod d \equiv 2^4 \pmod 7 \equiv 2$$

となっており，Diemの手法の適用条件(1)を満たしていないことがわかる．
このときDiemの手法は問題なく適用でき，この結果をもとにDiemの手法が一般の奇標数有限体上楕円・超楕円曲線に対して適用可能であることが示された．
また，Diemの手法の適用条件を満たしていない場合に危惧される$k(C)/k(x)$の真の中間体を用いた攻撃シナリオが実現不可能であることを確認し，のちに一般にその事実が成り立つことが示された．

結論・今後の課題

Diemの手法の適用条件を満たさない曲線C_0に対する被覆曲線Cの例を具体的に構成し，それを手がかりとして一般の奇標数有限体上楕円・超楕円曲線に適用可能であることが示された．また，そのようなC_0, Cに関する$k(C)/k(x)$の真の中間体$k(C')/k(x)$を構成し，ヤコビ群の位数からC'がC_0の被覆にならないことを確認した．今後の課題として，実際に被覆攻撃を行うことや被覆曲線が hyper となる楕円・超楕円曲線の条件や曲線の具体例を調べることが挙げられる．