

偶標数素数次拡大体上の楕円曲線に基づく P^1 上の $(2, \dots, 2)$ 型被覆の構成法に関する研究

Construction of $(2, \dots, 2)$ coverings over P^1 from Elliptic curves

over prime degree extension fields of even characteristic.

森下 拓也・暗号認証分科会・中央大学大学院

The GHS attack is known to map the discrete logarithm problem(DLP) in the Jacobian of a curve C_0 defined over the extension field k_d to the DLP in the Jacobian of covering curve C of C_0 over k . An important issue in the GHS attack is to classify weak curves having a covering curve C/k and a covering $\pi/k_d: C \rightarrow C_0$. I show a classification procedure for even characteristic case, based on Elliptic involution and hyperelliptic involution, and then show a covering $\pi/k_d: C \rightarrow C_0$.

1. GHS攻撃

拡大体上定義される楕円曲線暗号に対する攻撃手法として、GHS攻撃及びGHS攻撃を一般化した被覆攻撃が知られている。これらの攻撃は、有限体 $k := F_q$ の拡大体 $k_d := F_{q^d}$ 上定義される曲線 C_0/k_d 上の離散対数問題(DLP)を、 k 上定義される曲線 C/k 上のDLPへと変換して解読しようとする手法である。奇標数3次拡大体上の曲線において、160bitの安全性を持つ暗号系が攻撃により107bit程度の安全性になってしまう場合が見つかる等、現存の暗号系に強力に作用することが判明した。

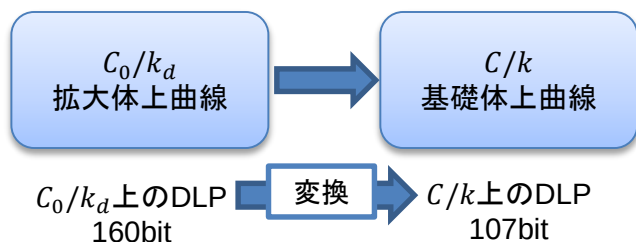


図1: GHS攻撃の概念

2. 曲線の分類

C_0/k_d が代数曲線 C/k と被覆写像 $\pi/k_d: C \rightarrow C_0$ を持つとき、攻撃の対象となることから、被覆曲線 C を持つ曲線を調べるのが重要な研究課題となっている。奇標数素数次拡大体上の楕円・超楕円曲線について、曲線の分岐点を利用した分類手法が提案されており、曲線の分類が進められてきた。一方で、偶標数体上の曲線については、分岐の様子複雑さから奇標数体上の曲線の分類手法を適用することは困難とされてきた。

本研究では、偶標数体上で次のような超楕円曲線 C/k を仮定することで、被覆 $\pi: C \rightarrow C_0$ を持つ k_2 上の楕円曲線 C_0/k_2 を分類した。さらに、具体的な被覆 π を導出した。

C/k の条件:

次数2の被覆 $\pi: C \rightarrow C_0$ が存在し、 $J(C) \sim C_0^{\times^2} C_0$

→ このとき、 $C_0 = C/\varphi$ となる自己同型写像 φ が存在する。

3. 提案手法(ordinaryの場合)

$$C_0/k_2: y^2 + a_1xy + a_3x = x^3 + a_2x^2 + a_4x + a_6, \\ a_i \in k_d$$

以下の手順に従って曲線の分類を行っていく。

- ① 有限体上の楕円曲線 C_0 の一般形を、同型変換を用いて導く。
- ② C/k_2 とする。 $\rho: C \rightarrow P^1$ について、 φ の固定点 $P_\infty = \varphi(P_\infty)$ として、自己同型写像 φ, ι (C_0 上の hyperelliptic involution) の作用から、 C_0, C の係数の関係式を導く。
- ③ C/k とする。このとき、 P^1 上の一次分数変換を用いて得られた②と同値な C_0 の方程式と②で得られた関係式との係数比較により、 C_0 の式を導く。
- ④ ③で得られた C_0 の式から、ordinaryな C_0 の標準形の式を導く。得られた2式の関係式から、 C/k の式を導く。

以下、本手法により得られた C_0, C 及び被覆 π を示す。

$$C_0: y^2 + xy = x^3 + bx^2 + cx \\ C: y^2 + (x^2 + x + l)y = \eta\bar{\eta}x^5 + (b + \eta\bar{\eta} + \eta^2l)x^4 \\ + \eta\bar{\eta}x^3 + (b + \eta\bar{\eta} + \eta^2l)x^2 + \eta\bar{\eta}l^2x \\ + (bl^2 + \text{Tr}(c) + l^2(\eta\bar{\eta} + \eta^2)) \\ \begin{cases} \eta^2 = \frac{c}{\text{Tr}(c)} \\ l = \text{Tr}(b) \end{cases}$$

$$\pi: C \rightarrow C_0$$

$$(x, y) \mapsto (\eta^2(x^2 + x + l), \eta^2(y + \eta x^3 + \eta(l+1)x + \text{Tr}(c) + l\eta))$$