GHS攻撃の対象となる奇標数拡大体上の楕円曲線と種数2超楕円曲線の分類

Elliptic Curves and Genus 2 Hyperelliptic Curves Subject to the GHS Attack on Extension Fields of Odd Characteristic

小林龍平・暗号・認証分科会・中央大学大学院

GHS attack is a cryptic attack to solve discrete logarithm problems (DLP) in an elliptic curve C_0 defined over the d degree extension field k_d of $k := \mathbb{F}_q$ by mapping it to the DLP in a covering curve C of C_0 over k. Recently, classifications for all elliptic curves which possess (2,…,2)-covering C/k of $\mathbb{P}^1$ over prime degree extension fields of odd characteristic were shown. However, classification for hyperelliptic curves and elliptic curves over composite degree extension field of odd characteristic have not been found yet.

The principal aim of this study is to show a complete list of all genus 2 hyperelliptic curves over prime degree extension field and elliptic curves over composite degree (d = 4, 6, 8, 9) extension fields of odd characteristic which subject to the GHS attack.

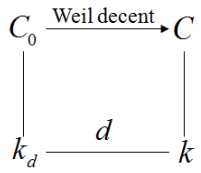
$k := \mathbf{F}_q$ (q は素数のべき乗), $k_d := \mathbf{F}_{q^d}$.

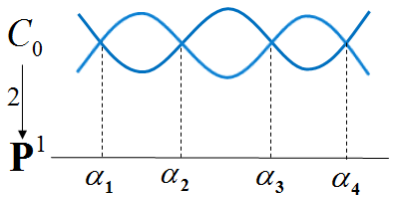
$C_0 / k_d : y^2 = f(x)$, deg f = 3 or 4.

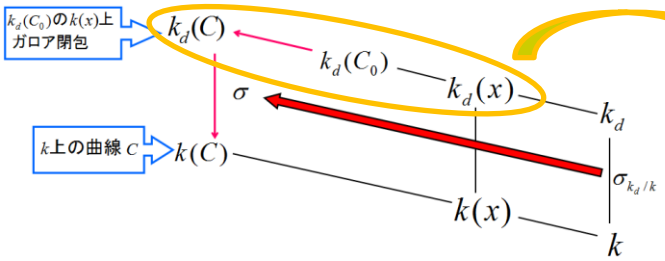
拡大体 k_d 上定義された曲線 C_0 上のDLP

↓ Weil decent

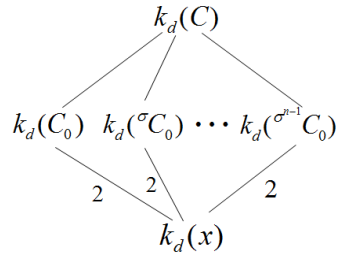
k 上定義された C_0 の被覆曲線 C 上のDLP



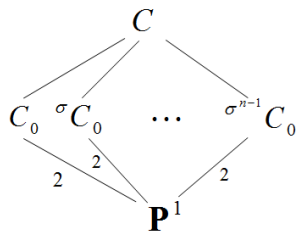




関数体の構造



被覆の構造



・GHS攻撃は k_d 上定義された曲線 C_0 上のDLPを, C_0 の被覆曲線 C 上のDLPへと変換する攻撃手法.
・この時, 定義体が k_d から k へ落ちるため, 計算量が減る場合がある.
・GHS攻撃は予想より多くの曲線が攻撃の対象となる事が明らかになった. 例えば, k_3 上ルジャンデル標準形楕円曲線の半分以上が対象になり, 160bit の安全性が107bit の安全性まで落ちる場合がある.
・GHS攻撃の対象となる曲線を一般的に求めるのは困難であり, 未だ完全に明らかになっていない.

結果

GHS攻撃の対象となるような (2,…2)型被覆を持つ奇標数素数次拡大体上種数2超楕円曲線, 及び, 奇標数合成数 (d = 4, 6, 8, 9)次拡大体上楕円曲線の分類を明らかにした.