7X-01

楕円曲線間の擬距離を用いた fixed table attack への対策

石川　司[†]　　篠原　直行[‡]　　伯田　恵輔[†]

島根大学大学院総合理工学研究科[†]　　国立研究開発法人情報通信研究機構[‡]

1　はじめに

楕円曲線暗号 (以下, ECC) は現在利用されている代表的な公開鍵暗号方式であり, その安全性は楕円曲線上の離散対数問題 (以下, ECDLP) を解くことの困難性に依存している. ECDLP を解く代表的な手法として ρ 法や Pohling-Hellman の攻撃などがあるため, ECC で利用する巡回群はその位数が, 例えば 256 bit 長の素数となるように設定する必要がある. また, 上記の理論的な攻撃手法以外に, ECC の安全性を脅かす攻撃手法としてサイドチャネル攻撃が知られている. サイドチャネル攻撃とは, 暗号化等の暗号処理の計算時に生じる電磁波や消費電力などを観測することで秘密情報を不正に取得する暗号モジュールへの攻撃手法の総称である. したがって, ρ 法や Pohling-Hellman の攻撃などの理論的な攻撃に対して安全な暗号パラメータを用いたとしても, 秘密情報が漏洩する恐れがある. そこで, サイドチャネル攻撃に対する様々な対策が提案されており, ECC の研究において重要な研究課題となっている. 本稿ではサイドチャネル攻撃のうち, fixed table attack [3] に注目し, 有限体上の楕円曲線間の (擬) 距離関数を用いた対策について述べる.

2　fixed table attack とその対策

ECC では, 暗号化・復号処理時にスカラー倍算と呼ばれる計算が行われており, 暗号化・復号処理全体の大部分を占める. スカラー倍算とは, 正整数 m と楕円曲線上の点 P を入力とし, m 個の P の和である点 $[m]P$ を計算することである. スカラー倍算を高速に計算する手法として, 事前に計算した複数の点 $[n]P$ $(n \ll m)$ を用いる手法が一般的である. このとき, 事前に計算した結果 $[n]P$ をまとめたものを事前計算テーブルという. サイドチャネル攻撃の一つとして fixed table attack と呼ばれる攻撃手法がある. この攻撃は, 事前計算テーブルを利用したスカラー倍算を行う際, テーブル上に格納された点がアフィン座標で表されている場合, その点の値が一意に定まることを利用して秘密情報を不正に入手する手法である. 詳細は [3] を参照されたい. この対策として, システムパラメータとして公開されている楕円曲線上でスカラー倍算を計算せずに, それと同型な楕円曲線上でスカラー倍算を行い, 最後に元の楕円曲線に引き戻すという手法が知られている [3, Section 3.2]. ただし, この対策手法は同型な楕円曲線の情報を格納する必要がある.

3　距離関数と fixed table attack 対策

3 節では, 有限体上の楕円曲線の集合における距離関数に関する既存研究と距離関数を用いた fixed table attack 対策について述べる.

3.1　距離関数に関する既存研究

Mishra と Gupta は, 標数 5 以上の有限体上の short Weierstrass 型楕円曲線全体の集合に対して距離関数が構成できることを示した [4]. その後, Hakuta は, 標数が 2, 3 の有限体上の short Weierstrass 型非超特異楕円曲線全体の集合に対する距離関数の構成方法を提案している ([2] など).

3.2　距離関数を用いた fixed table attack 対策

Mishra と Gupta は, 3.1 節で述べた距離関数の暗号への応用例として ECC における fixed table attack への対策を挙げている [4]. その対策とは, 2 節で挙げた [3, Section 3.2] における対策において, 同型な楕円曲線の情報を格納する代わりに, 複数の距離の値をあらかじめ格納しておき, その距離関数の値を用いて, システムパラメータの楕円曲線と事前計算テーブルの各点を一定の頻度で同型な楕円曲線とその上の点に変換しつつスカラー倍算を行い, 最後的に元の楕円曲線に引き戻すという手法である.

4　距離関数の拡張

ECC で注目されている曲線として, short Weierstrass 型楕円曲線の他に, Edwards 型楕円曲線や Jacobi intersection 型楕円曲線などがある. これらの曲線は short Weierstrass 型楕円曲線ではないため, 3.2 節の対策手法を直接適用することはできない. 著者らは距離関数の一般的概念である擬距離関数でも 3.2 節と同様の対策が取れることを発見した. そこで一般の楕円曲線の

Pseudometrics between elliptic curves for a countermeasure against fixed table attack

Tsukasa Ishikawa[†], Naoyuki Shinohara[‡] and Keisuke Hakuta[†]

Interdisciplinary Graduate School of Science and Engineering, Shimane University, 1060 Nishikawatsu-cho, Matsue, Shimane 690-8504, Japan[†]

National Institute of Information and Communications Technology, 4-2-1, Nukui-kitamachi, Koganei, Tokyo 184-8795, Japan[‡]

集合に対して擬距離関数を構成する方法を本稿で提案する (4.2 節).

4.1 数学的準備

4.1 節では, 本稿で用いる数学的記号を準備する. 代数学の基本的な内容については例えば [1] を参照されたい. $\mathbb{R}$ を実数全体の集合とする. 標数 $p \geq 5$ の素体を $\mathbb{F}_p$ で表す. 以下, 本稿では

$$E_i/\mathbb{F}_p : y^2 + a_1^{(i)}xy + a_3^{(i)}y = x^3 + a_2^{(i)}x^2 + a_4^{(i)}x + a_6^{(i)} \ (i = 1, 2)$$

で $\mathbb{F}_p$ 上定義された楕円曲線とする (詳細は [5, Chapter 3]). また, $\widetilde{\mathcal{EC}}^{(p)} := \{E/\mathbb{F}_p : \text{楕円曲線}\}$ とおく.

$E_1/\mathbb{F}_p$ から $E_2/\mathbb{F}_p$, 及び $E_1/\mathbb{F}_p$ から $E_2/\mathbb{F}_p$ への射がそれぞれ存在し, これらの射の合成が恒等射になるとき, 2 つの楕円曲線 $E_1/\mathbb{F}_p$, $E_2/\mathbb{F}_p$ は $\mathbb{F}_p$-同型といい, $E_1/\mathbb{F}_p \cong E_2/\mathbb{F}_p$ で表す. 定理 1 は $\mathbb{F}_p$ 上定義された 2 つの同型な楕円曲線の間の変数変換方法を表している.

定理 1. ([5, Chapter 3]) 楕円曲線 $E_1, E_2 \in \widetilde{\mathcal{EC}}^{(p)}$ に対し, ある $u \in \mathbb{F}_p^*, r, s, t \in \mathbb{F}_p$ が存在し, 変数変換 $(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t)$ が E_1 から E_2 への変換である, かつそのときに限り, $\mathbb{F}_p$-同型である. $\mathbb{F}_p$-同型は同値関係である.

$E_i \in \widetilde{\mathcal{EC}}^{(p)} (i = 1, 2)$ は, 変数変換を行うことで,

$$E_i'/\mathbb{F}_p : y^2 = x^3 + a_i x + b_i \in \widetilde{\mathcal{EC}}^{(p)} \ (i = 1, 2) \quad (4.1)$$

と変換できる ([5, Chapter 3]). ここで, $E_i/\mathbb{F}_p \cong E_i'/\mathbb{F}_p$ である. 式 (4.1) で定義された楕円曲線は short Weierstrass 型楕円曲線と呼ばれる. $\mathbb{F}_p$ 上定義された short Weierstrass 型楕円曲線全体の集合を $\mathcal{EC}^{(p)}$ とおく:

$$\mathcal{EC}^{(p)} := \{E/\mathbb{F}_p : \text{short Weierstrass 型楕円曲線}\}.$$

$\mathcal{EC}^{(p)} \subsetneq \widetilde{\mathcal{EC}}^{(p)}$ であることに注意されたい. short Weierstrass 型楕円曲線は $\mathcal{EC}^{(p)}$ の元であり, Edwards 型楕円曲線や Jacobi intersection 型楕円曲線などの short Weierstrass 型でない楕円曲線は $\widetilde{\mathcal{EC}}^{(p)} \setminus \mathcal{EC}^{(p)}$ の元である. また, $E_i \in \widetilde{\mathcal{EC}}^{(p)}$ から $E_i' \in \mathcal{EC}^{(p)}$ へ変数変換する写像が知られている ([5, Chapter 3]). この変数変換の写像を $\rho_p : \widetilde{\mathcal{EC}}^{(p)} \to \mathcal{EC}^{(p)}$ で表す.

4.2 擬距離関数の構成

4.2 節では, 一般の楕円曲線の集合に対して擬距離関数の構成を行う. 写像 $\widetilde{d}_p$ を以下で定義する:

$$\begin{aligned} \widetilde{d}_p : \ \widetilde{\mathcal{EC}}^{(p)} \times \widetilde{\mathcal{EC}}^{(p)} &\to \mathbb{R} \cup \{\infty\}, \\ (E_1, E_2) &\mapsto d_p(\rho_p(E_1), \rho_p(E_2)). \end{aligned}$$

ここで, 写像 $d_p : \mathcal{EC}^{(p)} \times \mathcal{EC}^{(p)} \to \mathbb{R} \cup \{\infty\}$ は [4] で提案された $\mathcal{EC}^{(p)}$ 上の距離関数である. 写像 $\widetilde{d}_p$ が well-defined であることは, 写像 ρ_p と距離関数 d_p の定義より明らかである. $E_1 \in \widetilde{\mathcal{EC}}^{(p)} \setminus \mathcal{EC}^{(p)}$ かつ $E_2 \in \mathcal{EC}^{(p)}$ であり, $E_1/\mathbb{F}_p \cong E_2/\mathbb{F}_p$ とする. このとき, $E_1 \neq E_2$ かつ $\widetilde{d}_p(E_1, E_2) = 0$ を満たすので, 写像 $\widetilde{d}_p$ は距離関数ではないことに注意されたい. 次の定理 (主定理) は本稿の主結果であり, 写像 $\widetilde{d}_p$ が $\widetilde{\mathcal{EC}}^{(p)}$ 上の擬距離関数であることを示している.

主定理 . $(\widetilde{\mathcal{EC}}^{(p)}, \widetilde{d}_p)$ は擬距離空間である.

Proof. 紙数の都合により省略する. □

また, 標数 2,3 の有限体上の非超特異楕円曲線全体の集合に対して, 同様の擬距離関数を構成することができる. よって, 一般の楕円曲線の（部分）集合に対して擬距離関数の構成方法を示すことができた. 3.2 節の対策は short Weierstrass 型楕円曲線特有の手法であり, short Weierstrass 型でない楕円曲線には適用できなかった. しかし, 本稿の結果により, short Weierstrass 型でない楕円曲線に対して同様の fixed table attack 対策が適用可能となる.

5 まとめ

本稿では, short Weierstrass 型とは限らない一般の楕円曲線の集合に対し, 擬距離関数が構成できることを示した. 従って, 本稿の結果は, Mishra と Gupta の成果を一般の楕円曲線の集合に拡張したサイドチャネル攻撃対策に位置付けられる.

参考文献

[1] M. Artin, Algebra, Prentice-Hall, Englewood Cliffs, 1991.

[2] K. Hakuta, Metrics on the sets of nonsupersingular elliptic curves in simplified Weierstrass form over finite fields of characteristic two, Internat. J. Math. Math. Sci., vol. 2015, Article ID 597849, 5 pages, 2015.

[3] T. Izu, B. Möller, and T. Takagi, Improved elliptic curve multiplication methods resistant against side channel attacks, INDOCRYPT 2002, LNCS 2551, 2002, pp.296–313.

[4] P.K. Mishra and K.C. Gupta, A metric on the set of elliptic curves over $\mathbb{F}_p$, Appl. Math. Lett. **21** (2008), no. 12, 1330–1332.

[5] J.H. Silverman, The Arithmetic of Elliptic Curves, second edition, GTM 106, Springer-Verlag, 2009.