卒業研究論文

反復回数を利用した楕円曲線暗号に対するフォールト攻撃

Fault attacks to elliptic curve cryptosystems with number of iteration

学籍番号　12D8101003C
渡邊　千尋
Chihiro Watanabe

中央大学理工学部情報工学科
趙研究室

2016年3月

概論

現在, あらゆる情報機器に暗号が実装されており, 暗号の安全性がセキュリティの根拠となっている. 暗号装置への実装における安全性解析において注目を集めている手法に Fault 攻撃がある. Fault 攻撃とは, 暗号装置への物理的干渉により意図的に機器にエラーを起こさせ, 秘密情報を推測・特定する攻撃手法である.

本研究では, 楕円曲線暗号におけるスカラー倍算中のループ部分の反復回数をフォールトの導入対象とした, 新しい攻撃手法を提案する. さらに, NIST 推奨パラメータを用いた楕円曲線暗号への攻撃を行い, 攻撃の有効性を示した.

キーワード

- 楕円曲線暗号
- Fault 攻撃

目次

第 1 章

序論

近年, スマートフォンやデジタル家電に代表されるスマートデバイスが急速に普及している. モノのインターネットと盛んに言われるように, それらのスマートデバイスはインターネットに接続するのみならず, さまざまな機種間でデータのやりとりをすることができる. そのような低機能な情報機器の運用には, 機種に適した情報セキュリティ技術が必要不可欠であり, 世界中で盛んに研究されている.

低機能, 低コストな情報機器の情報セキュリティを実現するための核となる技術が暗号技術である. 暗号化手法には共通鍵暗号方式と公開鍵暗号方式の 2 つの方式がある. 共通鍵暗号方式は, 暗号化と複合化に同様の鍵を用いる暗号方式である. 共通鍵暗号方式は解読に必要な計算量をその安全性の根拠としている. 一方, 公開鍵暗号方式は暗号化の処理を行う鍵と複合化を行う鍵とを別のものを用いる. 公開鍵暗号方式は有限体上の素因数分解と離散対数問題などの求解の困難性に基づいている. 共通鍵暗号方式は主に情報の秘匿, 公開鍵暗号方式は主に認証の場面に用いられる.

本研究の対象となる, 公開鍵暗号方式の一種である楕円曲線暗号は, 有限体上に定義された楕円曲線の有理点に対する離散対数問題の求解の困難性を利用したもので, 従来の公開鍵暗号にくらべ格段に鍵長を短くできる. そのため, 楕円曲線暗号が次世代暗号として注目されているとともに, 物理メモリが制限されている状況での運用が容易であるため, 暗号機能付き IC カードなどの低機能な装置への実装が期待されている.

IC カードや RFID などの低機能な情報機器は, コストのかかるセキュリティ対策を取ることが難しい上に, 暗号モジュールが攻撃者自身に所持されることが多い. また, 暗号装置に対して物理的なアクセスに要する設備が比較的安価なことから, 暗号処理を実行中の装置から生じる漏洩情報 (消費電力, 電磁波放射, 処理時間など) を計測するサイドチャネル攻撃や, 暗号処理に誤りを導入し秘密情報の漏えいを誘発する Fault 攻撃などの危険性が指摘されている. とりわけ, Fault 攻撃は直接的に誤りを導入するためアルゴリズムレベルでの誤りの検出が必要となる.

楕円曲線暗号を対象とした Fault 攻撃は, 2000 年に Biehl らによって RSA 暗号を対象とした攻撃手法が拡張され, 初めて示された [**?**]. その後いくつかの攻撃手法が, RSA 暗号を対象とした攻撃手法の拡張として, あるいは独自に提案されてきた.

第 2 章

準備

2.1 群

集合 G の直積集合 $G \times G$ から集合 G への写像が 1 つ与えられているとき, この写像を G の 2 項演算と呼ぶ. 集合 G $(= \emptyset)$ に対して 2 項演算が成り立ち, 以下の 3 つの条件を全てを満たすとき, G はこの演算に関して**群**であるという.

1. 結合法則
   $^\forall a, b, c \in G$ に対して, $(a \circ b) \circ c = a \circ (b \circ c)$ が成り立つ.
2. 単位元の存在
   $^\forall a \in G0$ に対して, $a \circ e = e \circ a = a$ となる $e \in G$ が存在する.
3. 逆元の存在
   $^\forall a \in G$ に対して, $a \circ b = b \circ a = e$ となる $b \in G$ が存在する.

また, 2 項演算が 1. のみを満たす G と $\circ$ の組 $(G, \circ)$ をこの 2 項演算に関して半群といい, 2 項演算が 1. と 2. のみを満たす G と $\circ$ の組 $(G, \circ)$ をこの 2 項演算に関するモノイドという.
そして, 群 G が下記の 4. も同時に満たすとき, **可換群** (またはアーベル群) であるという.

4. 交換法則
   $^\forall a, b \in G$ に対して, $a \circ b = b \circ a$ が成立する.

ちなみに, 群 $(G, \circ)$ において 2 項演算が明らかな場合は, 単に群 G ということもある.
また, 群 G に属する元の個数が有限であるとき G を**有限群**, そうでないとき無限群という.

集合 G が 2 項演算 $\circ$ に対して可換群であり, $\circ$ が $+$ で表される場合その群を**加法群**と呼ぶ. そのとき $x + y$ を x と y の和といい, 単位元を 0, x の逆元を $-x$ で表す.

可換群 G の任意の元が 1 つの元 a のべき乗で表せるとき, G を a で生成された**巡回群**といい, $G = \langle a \rangle$ で表す. a を**生成元**, あるいは原始元という.

2.2 環

2.2.1 環の定義

2 種類の 2 項演算 (加法 $+$ と乗法 $\cdot$) の定義された集合 R が以下 3 つの条件を満たすとき, $(R, +, \cdot)$ は**環**であるという.

1. 加法に関して可換群をなす.
   即ち, $^\forall a, b, c \in R$ に対して以下 4 つの等式が成立する.
   (a) $(a + b) + c = a + (b + c)$
   (b) $a + 0_R = 0_R + a = a$
   (c) $a + (-a) = (-a) + a = 0_R$
   (d) $a + b = b + a$

2. 乗法に関してモノイドをなす.
   即ち, $^\forall a, b, c \in R$ に対して以下 2 つの等式が成立する.
   (a) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
   (b) $a \cdot 1_R = 1_R \cdot a = a$

3. 分配法則を満たす.
   即ち, $^\forall a, b, c \in R$ に対して以下 2 つの等式が成立する.
   $a \cdot (b + c) = a \cdot b + a \cdot c$
   $(a + b) \cdot c = a \cdot c + b \cdot c$

そして, 環 R が下記の 4. も同時に満たすとき, **可換環**であるという (満たさないときは, 非可換環という).

4. 交換法則を満たす.
   即ち, $^\forall a, b \in R$ に対して $a \cdot b = b \cdot a$ が成立する.

環における単位元は**加法単位元** 0_R と, **乗法単位元** 1_R がある. また, 環の乗法の記号 $\cdot$ は省略されることが多い. すなわち, $x \cdot y$ は xy と書かれる. 以下この記法で書くことにする.

2.2.2 部分環, イデアル, 商環

環 R の部分集合で, それ自身が R の演算において環になるものを R の部分環という.
環 R の部分集合 I において,

1. $^\forall a, b \in I$ ならば $a + b \in I$
2. $^\forall a \in I$ と $^\forall r \in R$ に対して $ra \in I$
3. $^\forall a \in I$ と $^\forall r \in R$ に対して $ar \in I$

条件 1. と 2. を満たすとき, I は R の左イデアル, 条件 1. と 3. を満たすとき, I は R の右イデアル, そして条件 1. から 3. まで全てを満たすとき, I は R の両側イデアルもしくは単に**イデアル**という. R が可換環の場合, 左イデアル, 右イデアル, 両側イデアルは一致する.
環 R の元 x, y がイデアル I を法として合同であるとは, $x + i = y$ となる元 $i \in I$ が存在することであり, こ

のとき $x \equiv y \pmod{I}$ と書く．この関係は同値関係である．環 R のイデアル I による同値類を $[x]$ と書けば, $[x] = x + I = \{x + i | i \in I\}$ となり, 同値類の集合 R/I に加法と乗法, つまり,

$$[x] + [y] = [x + y]\ ,\ \ [x] \cdot [y] = [xy]$$

が定義できる．これらの演算に関して同値類の集合 R/I は環になり, I を法とする R の商環または剰余環という．

2.2.3 多項式環

つぎに, 可換環, 体を係数とする多項式環を定義する．

X を変数とし, 可換環 R を係数とする 1 変数多項式環を $R[X]$ と書く．また, $X_1, \ldots, X_n$ を係数とする R 係数 n 変数多項式環を $R[X_1, \ldots, X_n]$ とかく．$X_1, \ldots, X_n$ を変数とし, 体 K を係数とする分数式全体を, $K[X_1, \ldots, X_n]$ の商体といい, $K(X_1, \ldots, X_n)$ と書く．

0 でない多項式 $F = a_0 + a_1 X + \cdots + a_d x^d \in R[X] (a_i \in R; a_d \neq 0)$ の次数 $\deg F$ を, $\deg F{:=}d$ と定義する．多項式 $F \in R[X_1, \ldots, X_n]$ が変数 $X_1, \ldots, X_n$ を含まない時, F を**定数**という．定数でない多項式 $F \in R[X_1, \ldots, X_n]$ の最高次数項 $X^{\deg F}$ の係数が 1 に等しいとき, F をモニック多項式という．また, 0 でない多項式 F, G に対して

$$\deg(FG) = \deg F + \deg G$$

が成立する．

$R[X_1, \ldots, X_n]$ において, $aX_1^{d_1} \ldots X_n^{d_n} (d_i \geq 0; a \in R \setminus \{0\})$ の形の多項式を**単項式**という．ここで, $R \setminus \{0\}$ は R から元 0 を除いたものを表す．単項式 $aX_1^{d_1} \cdots X_n^{d_n}$ の次数を $d_1 + \cdots + d_n$ と定義する．定義より多項式は単項式の和として一意に表せる．次数 d の単項式のみの和で表される多項式を次数 d の**斉次多項式**という．また F を $F = \sum_i F_i(X_1, \ldots, X_n)$(各 F_i は i 次斉次多項式) の形に書いたとき, F_i を F の i **次斉次成分**という．

体 k を係数とする, 定数でない n 変数多項式 $F \in k[X_1, \ldots, X_n]$ が, 定数でない多項式の 2 つの積で表せないとき, F を**既約多項式**, または F は**既約**であるという．つまり, $F = GH$ ならば G または H は 定数である．任意の定数でない多項式は既約多項式の積へと分解される．この分解は, 0 でない定数倍と, 既約多項式の積の順序を除いて一意的である．

2.2.4 準同型

2 つの環の間に, 和や積, 単位元を保つ写像を考える．このような写像を環の準同型写像, または単に準同型と呼ぶ．準同型が全単射のとき, つまり準同型により, 2 つの環の元が 1 対 1 に対応し, 和や積も対応するとき, 2 つの環を同じ環と考える．これを環の同型とよぶ．

1. 環 R から環 R' への写像 $\varphi : R \to R'$ が,

   $$\varphi(a + b) = \varphi(a) + \varphi(b); \varphi(ab) = \varphi(a)\varphi(b); \varphi(1) = 1$$

   を満たすとき, φ を **(環) 準同型**という．
2. 全単射な環準同型を **(環) 同型写像**, あるいは単に**同型**という．
3. 環 R と R' との間に 同型写像が存在するとき, R と R' は**同型**であるといい, $R \simeq R'$ と書く．
4. 環準同型 $\varphi : R \to R'$ に対し, $a \in R; \varphi(a) = 0$ 全体は R のイデアルである．これを φ の**核**といい, $\mathrm{Ker}\varphi$ と書く．

   $$\mathrm{Ker}\varphi := \{a \in R; \varphi(a) = 0\}$$

可換環の準同型 $\varphi : R \to R'$ に対して次が成り立つ

1. R のイデアル I に対し, $I = \mathrm{Ker}\varphi$ とすると, 写像

   $$\bar{\varphi} : R/I \to R'; [a] \to \varphi(a)$$

   は $\bar{\varphi}p = \varphi$ を満たす準同型である. ここで $[a]$ は a を含む同値類, p は自然な準同型を表す. さらに準同型 $\psi : R/I \to R'$が$\psi p = \varphi$ を満たせば, $\psi = \bar{\varphi}$である.
2. 1 において, $\bar{\varphi} : R/\mathrm{Ker}\varphi \to R'$は$\varphi(R)$ への同型写像である（**準同型定理**）. とくに φ が全射なら, $\bar{\varphi}$は R/I から R' への同型写像である.

可換環 k から可換環 R への環準同型 $\sigma : k \to R$ が与えられた環 R を k **代数**という. しばしば, $\sigma(a)1 \in R(a \in k)$ を単に $a \in R$ のように書く. また, k 代数の間の環準同型 $\varphi : R \to R'$ が任意の $a \in k$ と $r \in R$ に対し, $\varphi(ar) = a\varphi(r)$ をみたすとき, φ を k **代数の準同型**, または k **準同型**という.

2.3 体

可換環の 0 でない元の全てに, 乗法に関する逆元が存在するとき, **体**と呼ぶ. また, 元の個数が有限な体を**有限体**といい, その元の個数を体の**位数**という.

体 $\mathbb{K}$ の部分集合 l が $\mathbb{K}$ の**部分体**であるとは, l が空集合ではなく, 加法と乗法 (それぞれの逆元計算も含む) に関して閉じていることをいう. 体 l が体 $\mathbb{K}$ の部分体であるなら, $\mathbb{K}$ は l の**拡大体**または単に拡大であるという.

体 $\mathbb{L}$ が体 $\mathbb{K}$ の拡大体であり, α は $\mathbb{L}$ の元とする. α が $\mathbb{K}$ の元を係数とするゼロではない多項式の根になっているとき, α は $\mathbb{K}$ 上**代数的**であるという. 一般に拡大体 $\mathbb{K} \subset \mathbb{L}$ において, $\mathbb{L}$ のすべての元が $\mathbb{K}$ 上代数的であるとき, $\mathbb{L}$ は $\mathbb{K}$ 上**代数的**であるという.

$\mathbb{K} \subset \mathbb{L}$ であり $\alpha \in \mathbb{L}$ であるとき, $\mathbb{L}$ の部分体であって $\mathbb{K}$ と α を含むものすべての共通部分を記号 $\mathbb{K}(\alpha)$ で表し, $\mathbb{K}$ に α を**添加した体**という. これは $\mathbb{K}$ と α を含む $\mathbb{L}$ の部分体のうちで最小のものである. ただ 1 個の元を添加して得られる $\mathbb{K}$ の拡大体を $\mathbb{K}$ の**単純拡大**という.

$\mathbb{K}$ に係数を持つ全ての多項式を 1 次因子に完全に分解するという性質を体 $\mathbb{K}$ が持つなら, $\mathbb{K}$ は代数的に閉じているという. これは, $\mathbb{K}$ に係数を持つ全ての多項式が, $\mathbb{K}$ に根を持つことと同値である. 代数的に閉じている最小の $\mathbb{K}$ の拡大体は, $\mathbb{K}$ の**代数的閉包**と呼ばれ, $\overline{\mathbb{K}}$ で表される.

整数環 $\mathbb{Z}$, 素数 p に対して, p の倍数の集合を $p\mathbb{Z}$ とすると, $p\mathbb{Z}$ は $\mathbb{Z}$ のイデアルである. また, 商環 $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ は p 個の元からなる体になる. これと同型な体を $\mathbb{F}_p$ で表す.

もし $\mathbb{K}$ において, 乗法の単位元 1 をそれ自身に加えていっても決して 0 にならないなら, 体の標数は 0 であるという. そうでない場合, $1 + 1 + \cdots + 1(p \text{ 回})$ が 0 に等しくなるような素数 p が存在し, p は体 $\mathbb{K}$ の**標数**と呼ばれる. その場合, $\mathbb{K}$ は体 $\mathbb{Z}/p\mathbb{Z}$ と同形な体を含み, これを $\mathbb{K}$ の**素体**と呼ぶ.

2.4 離散対数問題

群 G における $g \in G$ に対する離散対数問題とは, $y \in G$ が与えられるとき, $g^x = y$ (演算を加法的に書くと $xg = y$) である整数 x が存在するとしたとき, それを求めるという問題のことである. この x を y の離散対数という.

第 3 章

楕円曲線と楕円曲線暗号

3.1　楕円曲線の定義

体 $\mathbb{K}$ 上で定義される楕円曲線とは，一般的に

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q) \tag{3.1}$$

で与えられる (x, y) に関する方程式のことである．$\mathbb{K}$ 上の楕円曲線とは, 無限遠点と呼ばれる要素 $\mathcal{O}$ を加えた $x, y \in K$ である点 (x, y) の集合を表す.
もし, K の標数が 2 であるとき, 方程式によって定義される平面曲線は

$$y^2 + xy = x^3 + ax^2 + b \quad (a, b \in \mathbb{K}) \tag{3.2}$$

と変形され, 上式を満たす点の集合となる.
また, K の標数が 3 であるとき, 方程式によって定義される平面曲線は

$$y^2 = x^3 + ax^2 + bx + c \quad (a, b, c \in \mathbb{K}) \tag{3.3}$$

と変形され, 標数が 3 より大きい場合は

$$E : y^2 = x^3 + ax + b \quad (a, b \in \mathbb{K}) \tag{3.4}$$

と変形される.

3.2　有限体上の楕円曲線の位数

p を素数, n を自然数とし, $q = p^n$ とする. 有限体 $\mathbb{F}_q$ 上の楕円曲線は有限個の有理点を持つ. それを $\#E(\mathbb{F}_q)$ で表す.

$$\#E(\mathbb{F}_q) = q + 1 - t$$

により定義された t を, q におけるフロベニウスのトレースとよぶ. $\mathbb{F}_q$ 上の楕円曲線 E の q 上フロベニウス写像 φ は

$$\begin{array}{rcl} E(\overline{\mathbb{F}}_q) & \to & E(\overline{\mathbb{F}}_q) \\ (x, y) & \to & (x^q, y^q) \\ \infty & \to & \infty \end{array}$$

で定義される. この写像は $E(\overline{\mathbb{F}}_q)$ の群自己同型であり, フロベニウス自己同型写像と呼ばれる. また, ハッセの定理よりフロベニウスのトレース t は

$$|t| \leq 2\sqrt{q}$$

をみたす. ハッセの定理とは, 有限体 k_d上の楕円曲線 E に対し

$$1 + p^d - 2\sqrt{q^d} \leq \#E(k_d) \leq 1 + p^d + 2\sqrt{q^d}$$

である.

楕円曲線 E には, supersingular 曲線, anomalous 曲線と呼ばれる 2 つの特別なクラスがある.

それぞれ, 標数 p が曲線 $E(\mathbb{F}_q)$ のフロベニウスのトレース t を割る場合, 曲線 $E(\mathbb{F}_q)$ のトレースが 1 となる場合である.

3.3 楕円曲線上の点の加算

楕円曲線上の有理点において, 通常の座標で行われる点の加算とは異なる加算の定義をする. 楕円曲線上の点 P, Q を取ってきたとき, まず点 P, Q を通る直線を引き, 第三の交点 $P * Q$ を見つける. 次に, $P * Q$ と無限遠点 $\mathcal{O}$ を通る直線 (x 軸との垂線) を引き, 楕円曲線と交わるもう 1 つの交点を, 楕円曲線における点 P と Q が加算された点とし $P \oplus Q$ と表す. 一方, $P = Q$ である場合は点 P における楕円曲線との接線を引き, その交点を $P * Q$ とする.

この加算により楕円曲線は群構造をなす. 例えば, 点 $P = (x, y)$ と $Q = (x, -y)$ の場合, 第三の交点は無限遠点となる. よって, $P \oplus Q = \mathcal{O}$ となり点 Q が点 P の逆元, $-P$ となる. すなわち単位元が無限遠点, 逆元は x 軸と対称な点になる. 結合法則は, 加算の定義により自明である.

この定義を実数上で描かれた楕円曲線のグラフを用いて示す. ただし, $P, Q \in E(\mathbb{F}_q)$ について $P = (x_1, y_1)$, $Q = (x_2, y_2)$ とする.

[Case 1] $P \neq Q, \quad x_1 \neq x_2 \longrightarrow$ 図 3.1
[Case 2] $P = Q \longrightarrow$ 図 3.2
[Case 3] $P \neq Q, \quad x_1 = x_2 \longrightarrow$ 図 3.3

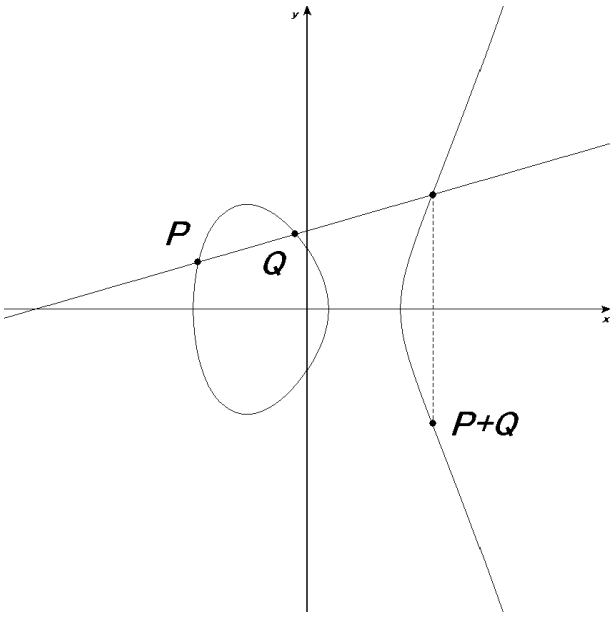

図 3.1 $P \oplus Q$

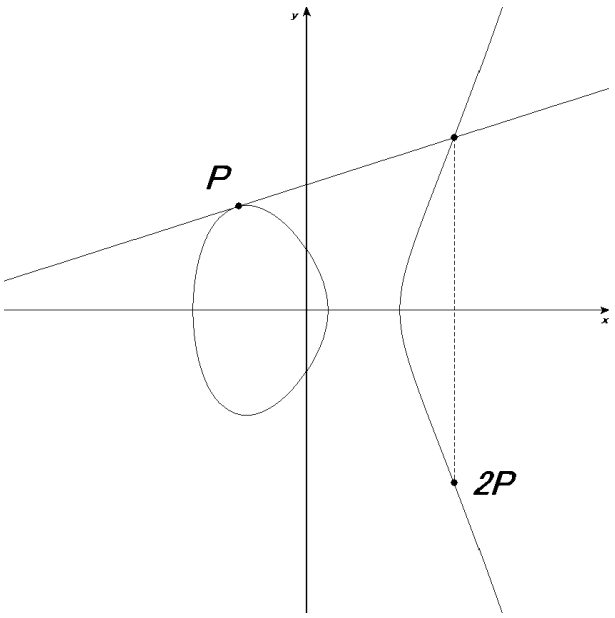

図 3.2 $2P$

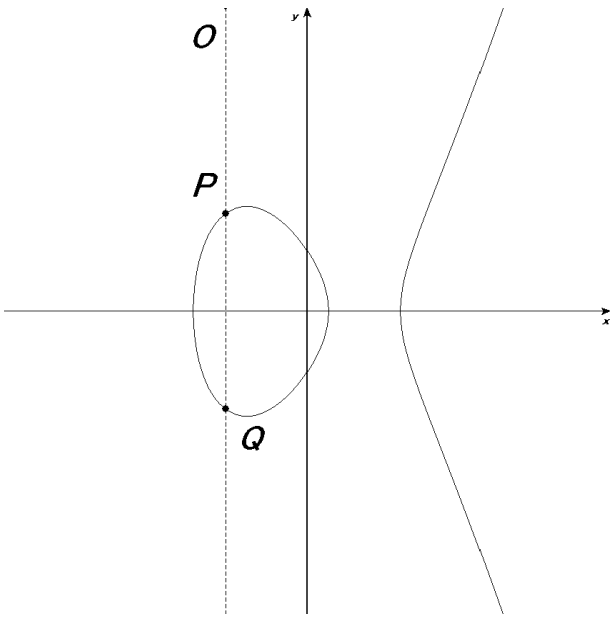

図 3.3　$P \oplus Q = \mathcal{O}$

ここで, $P \oplus Q$ を効率的に計算する為公式を与える. また, 計算を簡略化する為に, 楕円曲線は標数が 3 より大きいものを扱う. 楕円曲線 $E : y^2 = x^3 + ax + b$ の各点 $P,\ Q,\ P * Q,\ P \oplus Q$ を

$$P = (x_1, y_1),\ Q = (x_2, y_2),\ P * Q = (x_3, y_3),\ P \oplus Q = (x_3, -y_3)$$

と設定する.

$P \neq Q$ のとき, P と Q を結ぶ直線の方程式は

$$y = \lambda x + \upsilon \quad \left(\lambda = \frac{y_2 - y_1}{x_2 - x_1},\ \upsilon = y_1 - \lambda x_1\right)$$

となり, これを楕円曲線の式に代入し, 解と係数の関係から x_3 が得られ, y_3 は x_3 を P と Q を結ぶ直線の方程式に代入して得られる. すなわち,

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda x_3 + \upsilon$$

となる.

一方, $P = Q$ のとき, P と $-2P$ を結ぶ直線の傾き λ は, $\lambda = \frac{\partial y}{\partial x} = \frac{\partial y}{\partial E} * \frac{\partial E}{\partial x}$ を用いて

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

となり, 後は先ほどと同様に x_3 と y_3 を求めて,

$$x_3 = \lambda^2 - 2x_1$$

$$y_3 = \lambda x_3 + \upsilon$$

となる.

3.4 楕円曲線上の点のスカラー倍算

楕円曲線上の点のスカラー倍算とは, 楕円曲線上の任意の点 $P \in E(\mathbb{F}_q)$ と, 任意の整数 $n \in \mathbb{Z}$ に対して

$$nP = \begin{cases} P \oplus P \oplus \cdots \oplus P \ (n \text{ 回}) & (n > 0) \\ -P \ominus P \ominus \cdots \ominus P \ (-n \text{ 回}) & (n < 0) \end{cases}$$

と定義される. この演算は楕円曲線暗号の根幹を成す部分であり, 暗号演算の大半の時間を占めている.

3.4.1 Double and add

以下は秘密鍵 k を 2 進展開 $k = (k_{n-1}, ..., k_0)_2$ として表し, スカラー倍算 kP を計算するアルゴリズムである.

表 3.1 Algorithm 1:Double and add

input: $k = (k_{n-1}, ..., k_0)_2, P \in E(K)$
output: kP
$1: Q \leftarrow \mathcal{O}$
$2:$ **for** $i = n-1$ **down to 0 do**
$2.1: Q \leftarrow 2Q$
$2.2:$ **if** $k_i = 1$
$2.2.1: Q \leftarrow Q \oplus P$
$3:$ **end for**
$4:$ **return** Q

Algorithm 1 の計算時間は, k_i の値に依存するため, 暗号装置の電力消費を観測するサイドチャネル攻撃に対して脆弱性を持つ.

3.4.2 Double and add always

Double and add always は, Algorithm 1 を改良した, 各演算ステップの計算量が等しいスカラー倍算アルゴリズムである.

表 3.2 Algorithm 2:Double and add always

input: $k = (k_{n-1}, ..., k_0)_2, P \in E(K)$
output: kP
$1: Q[0] \leftarrow \mathcal{O}$
$2:$ **for** $i = n-1$ **down to 0 do**
$2.1: Q[0] \leftarrow 2Q$
$2.2: Q[1] \leftarrow Q[0] + P$
$2.3: Q[0] \leftarrow Q[k_i]$
$3:$ **end for**
$4:$ **return** $Q[0]$

3.4.3 Montgomery ladder

Montgomery ladder[**?**] はさらに Algorithm 1, Algorithm 2 を改良した, スカラー倍算アルゴリズムである. Montgomery ladder は, 点の加算や倍算において y 座標を使用せずに x 座標を計算可能だということが示されている.

具体的には, $P=(x_1,y_1), Q=(x_2,y_2), Q-P=(x_3,y_3)$ を, 楕円曲線 $E: y^2=x^3+ax+b$ 上の点に移し, $P+Q=(x_4,y_4), 2P=(x_5,y_5)$ の x 座標を以下の方程式で計算できる.

$$x_4 = \frac{2(x_1+x_2)(x_1x_2+a)+4b}{(x_1+x_2)^2} - x_3 \tag{3.5}$$

$$x_5 = \frac{(x_1^2-a)^2-8bx_1}{4(x_1^3+ax_1+b)} \tag{3.6}$$

このことを利用した高速なスカラー倍算アルゴリズムである Montgomery ladder を以下に記す.

表 3.3　Algorithm 3: Montgomery ladder

input: $k=(k_{n-1},....,k_0)_2, P\in E(K)$
output: The x-coordinate of kP
$1:\ Q[0]\leftarrow\mathcal{O}, Q[1]\leftarrow P$
$2:$ **for** $i=n-1$ **down to 0 do**
$2.1:\ Q[1-k_i]\leftarrow Q[0]\oplus Q[1]$
$2.2:\ Q[k_i]\leftarrow 2Q[k_i]$
$3:$ **end for**
$4:$ **return** $Q[0]$

3.5 楕円曲線暗号

楕円曲線暗号の安全性は**楕円曲線上離散対数問題 (ECDLP)** の求解の困難性に基づいている. ECDLP を解くには, 一般に完全指数時間かかる. しかしながら, 特別な曲線に限って準指数関数時間で解けることも示されている. そのため, 楕円曲線暗号を実装する際には暗号的に脆弱な曲線を避けた, 強固な曲線を選ぶ必要がある.

3.5.1 楕円曲線上の離散対数問題

有限体 $K=\mathbb{F}_q$ 上の楕円曲線を E とし, その曲線上の位数 n の点を $P\in E(\mathbb{K})$ とする. さらに, 点 $Q\in\langle P\rangle$ に対して整数値 $l\in[0,n-1]$ が $Q=lP$ を満たすとする. このとき, 整数値 l を P を底とした Q の**離散対数**と呼び, $l=\log_P Q$ と表す. このような l を点 P,Q から求めることを ECDLP を解くという.

3.5.2 強固な楕円曲線

暗号的に強固な楕円曲線とは, その曲線上の ECDLP を解くことが困難な曲線を指す.

ECDLP の解法で最も素朴なものは全探索である. 全探索とは $P, 2P, 3P\ldots$ が Q と一致するまで順番に調べる探索法である. この方法の計算量は最悪の場合 $n=ord(P)$, 平均で $n/2$ である. このことから n の十分な大きさが決められている (例 : $n\geq 2^{160}$[**?**]).

ECDLP に対する最も一般的な攻撃法は, Pohlig-Hellman 法 [**?**] と Pollard-ρ 法 [**?**] を組み合わせた手法である. こ

れは $O(\sqrt{p})$ の完全指数関数時間の計算量となる．ここで p は n の最大素因数とする．この攻撃法に対抗するためには, 点 P の位数が十分に大きな素数で割り切れるようにする．こうすることで攻撃者は ECDLP を解くことが現実的に不可能となる．

3.5.3 Pohlig-Hellman 法

Pohlig-Hellman 法 [**?**] は E 上の $l = \log_P Q$ の計算を, 中国の剰余定理を用いて $\langle P \rangle$ の素位数の部分群上の離散対数問題に移す．このとき, $\langle P \rangle$ 上の ECDLP は本来の素位数の部分群上の ECDLP よりも簡単である．このことから, 暗号を実装する際には位数が大きな素数で割り切られるような P を選択する．

表 3.4　Algorithm 3: Pohlig-Hellman 法

input: $P \in E(K), Q \in \langle P \rangle, n = ord(P) = \prod_{i=0}^{j-1} p_i^{e^i}, where\ p_i < p_{i+1}$
output: $l \bmod n$
1 : **for** $i = 0$ **to** $j - 1$ **do**
1.1 : $Q' = \mathcal{O}, l_i = 0$
1.2 : $P_i = (n/p_i)P$
1.3 : **for** $t = 0$ **to** $e_i - 1$ **do**
1.3.1 : $Q_{t,i} = (n/p_i^{t+1})(Q \oplus Q')$
1.3.2 : $W_{t,i} = \log_{P_i} Q_{t,i}$ { 位数が $ord(P_i)$ の部分群における ECDLP を解く.}
1.3.3 : $Q' = Q' \ominus W_{t,i} P^t P$
1.3.4 : $l_i = l_i + p^t W_{t,i}$
1.4 : **end for**
2 : **end for**
3 : 中国の剰余定理を用いてすべての i に対する合同式 $l \equiv l_i \pmod{p_i^{e_i}}$ を解くことで $l \bmod n$ が求まる.
4 : **return** l

3.5.4 Pollard-ρ 法

Pollard-ρ 法は, ECDLP に限らず, 一般の有限アベール群上の離散対数問題に対して適用できるアルゴリズムである．G を位数 l の有限巡回群とし, 問題を $g, h \in G$

Pollard-ρ 法 [**?**] の主要な考え方は

$$c'P \oplus d'P = c''P \oplus d''Q \tag{3.7}$$

を満たすような異なる (c', d') と (c'', d'') の組みを見つけることである．このとき,

$$(c' - c'')P = (d'' - d')Q = (d'' - d')lP \tag{3.8}$$

かつ, $\langle P \rangle$ において

$$c' - c'' \equiv d'' - d' \tag{3.9}$$

となる．ゆえに, $l = \log_P Q$ が

$$l = (d' - d'')^{-1}(c' - c'') \pmod{n} \tag{3.10}$$

の計算から求まる．

3.6　ペアリング暗号

第 4 章

Fault 攻撃

Fault 攻撃は一般的に, 暗号装置が秘密鍵を用いた演算中に起こる一時的, もしくは永続的な誤りを利用する. 誤りは攻撃者がハードウェア上の誤動作, またはソフトウェア上のバグを狙った物理的な干渉をすることにより導入される. 攻撃者は誤りによって得られる不正な出力値をもとに秘密鍵の情報を盗みだす. このように意図的に導入される誤りを Fault と呼ぶ. 以下に Fault 攻撃の既存手法を紹介する.

4.1 Invalid-Curve Attack

Invalid-Curve Attack は Biehl らによって提案された [**?**]. 前提として, 攻撃対象となる暗号装置が入力点 P とその演算結果である点 $Q = kP$ の 2 点に対して, 暗号的に強固な楕円曲線 E 上にのるかどうかのチェックをしないとする. 標数が 2 以上の有限体 K 上に定義された暗号的に強固な楕円曲線を E とする.

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{4.1}$$

ANSI X9.63 や IEEE 1363 で標準化される, 楕円曲線 E のパラメータ a_6 を使用しない点の加算公式を想定している. 暗号装置が入力として点 $\hat{P} = (\hat{x}, \hat{y}) \in K \times K$ かつ $\hat{P} \notin E$ を受け取る, このときスカラー倍算 $d\hat{P}$ は楕円曲線 $\hat{E}(a_1, a_2, a_3, a_4, \hat{a}_6,)$ 上に移される.

$$\hat{a}_6 = \hat{y}^2 + a_1\hat{x}\hat{y} + a_3\hat{y} - a_2\hat{x}^2 - a_4\hat{x} \tag{4.2}$$

楕円曲線 $\hat{E}$ は 式 (4.2) で定義された, 本来の楕円曲線 E とは異なる曲線である. 点 $\hat{P}$ の選び方としては, $\hat{P}$ によって移される曲線 $\hat{E}$ の位数が小さい約数 r を持ち, かつ点 $\hat{P}$ の位数が r と等しくなるように注意深く設定する. このように入力点を選ぶことで, 位数 r の点 $\hat{P}$ を生成元とする巡回部分群における ECDLP を考えることができ, これを解くことによって $k \pmod r$ の値を得る. 上記の過程を入力点 $\hat{P}_i$ をさまざまに入れ替えて, 十分多くの回数試行することにより, それぞれの演算結果 $k\hat{P}_i$ をもとに $r_i = ord_{E_i}\hat{P}_i$ として,

$$k_i \equiv k \pmod{r_i} \tag{4.3}$$

の値を集める. 最終的には, 十分な数の集めた値 k_i をもとに, 中国の剰余定理を用いて k を得る.

また, 得られる $\hat{Q}$ の y 座標が一意に定まらない場合, 点は $(x_0, \hat{y}_1), (x_0, \hat{y}_2) \in \hat{E}$ の 2 点のどちらかになる. この 2 点について, ECDLP を解くことで, 得られる値を c_1, c_2 とする. ここで, c_1, c_2 は $c_1 \equiv -c_2 \bmod ord(\hat{P})$ と, $k \equiv c_1 \bmod ord(\hat{P})$ もしくは, $k \equiv c_2 \bmod ord(\hat{P})$ を満たす. このことから, $k^2 \equiv c_0^2 \bmod ord(\hat{P})$ を得る. このような値 $k^2 \equiv c_i^2$ を複数集めて中国の剰余定理を用いることで k^2 を計算し, 最終的に k を得る.

4.1.1 防御策

この攻撃を防ぐためには, 出力前に入力点 P とそのスカラー倍算 kP の両方が楕円曲線 E に載るかどうかを曲線パラメータの a_6 を用いてチェックを行う. このように, 点が曲線に載るかどうかを演算に用いられていないパラメータを使用してチェックすることを, **ポイントチェック**と呼ぶ.

4.2 skipping attack

4.3 ペアリングに対するフォールト攻撃

$B = \{1, \xi, \sqrt{v}, \xi\sqrt{v}\}$ を $\mathbb{F}_q^k$ の基底とする.
$r_{\tau-1} = 0$ の場合,

$$F_{\tau+1,P}(Q) = (F_{\tau,P}(Q))^2 \times \ h_1(Q) \tag{4.4}$$

$$[j]P = (X_j, Y_j, Z_j) \tag{4.5}$$

$$T = [2j]P = (X_2 j, Y 2j, Z_2 j) \tag{4.6}$$

が分かり, h_1 の方程式を用いて以下の方程式を得る.

$$F_{\tau+1,P}(Q) = (F_{\tau,P}(Q))^2 \times \ (Z_{2j} Z_j^2 y\sqrt{v} - 3(X_j - Z_j^2)(X_j + (Z_j^2)(xZ_j^2 - X_j)) \tag{4.7}$$

点 P を秘密点とすると, j, τ, Q の座標が分かる. さらに, Miller algorithm により $F_{\tau+1,P}(Q)$ と $F_{\tau,P}(Q)$ が与えられる.
比 $R = \frac{F_{\tau+1,P}(Q)}{(F_{\tau,P}(Q))^2}$ を計算する. R の理論上の形と, 基底 B の分解を用いると, 恒等式によって以下の集合が得られる.

$$\begin{cases} Y_j Z j^2 = \lambda_2, \\ Z_j^2(X_j^2 - Z_j^4) = \lambda_1, \\ 3X_j(X_j^2 - Z_j^4) + 2Y_j^2 = \lambda_0, \end{cases} \tag{4.8}$$

非線形システムの分解により, 以下の式が与えられる.

$$(\lambda_0^2 - 9\ \lambda_1^2) Z^1 2 - (4\ \lambda_0 \lambda_2^2 + 9\ \lambda\ 1^3) Z^6 + 4\ \lambda_1^4 = 0 \tag{4.9}$$

Z_j の方程式を解くと, せいぜい $24 = 12 \times\ 2 \times\ 1$ で, 点 $[j]P$ の座標 (X_j, Y_j, Z_j) を見つけられる. $[j]P$ の値が分かると, $j \pmod r$ のインバース j' を見つけることで, $[j'][j]P = [j'j]P = P$ を見つけることが可能となる.

4.3.1 Second Attack

この項では, 攻撃者は入力点 P を選択することができず, かつ攻撃対象となる暗号装置が出力前に点の実装上のチェックを行うという前提での攻撃モデルである.

攻撃者は基準点を自由に選択できないため, 基準点の x 座標 x_0 に対して Fault を導入することで異なる値 $\hat{x}_0$ に変化させる. このとき, $\hat{x}_0$ はおよそ $1/2$ の確率で $\mathbb{K}$ 上で平方非剰余となる.

$\hat{x}_0$ が $\mathbb{K}$ 上平方非剰余となり, x 座標として $\hat{x}_0$ を持つ点のスカラー倍算 $(\hat{x}_1, \hat{y}_1) = k\hat{P}$ が計算されたとする. スカラー倍算結果が曲線に載るかどうかのチェック前に, $\hat{x}_1$ に Fault を導入する. これはさらに, $1/2$ の確率で $\hat{x}_1$ が $\mathbb{K}$ 上平方非剰余となりチェックが通る.

したがって, 狙ったデータを格納するランダムなビットに対して, スカラー倍算前と出力のチェック前の合わせて 2 回 Fault を導入することができれば, およそ 1/4 の確率で Fault を与えた値が得られることになる.

4.3.2 防御策

出力前に入力点 P とそのスカラー倍算 kP の両方が楕円曲線 E に載るかどうかを点の y 座標を用いてチェックを行うことにより防げる. また, 暗号装置に採用する楕円曲線 E の 2 次 twist 曲線 E_d が暗号的に脆弱な曲線にならないように, 曲線を選択する. このことにより, 万が一攻撃者が導入する Fault によって実装上のチェックが通り, 2 次 twist 曲線上の点の情報が出力されてしまっても, ECDLP を解くために必要な計算量が縮小することがなくなる. すなわち, この攻撃によって秘密情報が盗み出されることがなくなる. このように, ある楕円曲線が暗号的に強固な 2 次 twist 曲線を持つとき, その曲線を **twist secure** な曲線と呼ぶ. このような曲線は極めて極めて少ないことが知られている。

4.4 曲線パラメータに対する Fault 攻撃

以下の攻撃手法は Ciet と Joye によって提案された手法 [**?**] である. [**?**] では入力点に対する Fault 攻撃と, 定義体の標数に対する Fault 攻撃, 曲線パラメータに対する Fault 攻撃の 3 つの攻撃モデルが示されている. 本研究で参考とするのは曲線パラメータに対する Fault 攻撃である.

有限体 K 上に定義された暗号的に強固な楕円曲線を E とする.

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{4.10}$$

点の加算において曲線のパラメータ a_6 がスカラー倍算結果 dP に影響を及ぼさないとする. パラメータ a_4 に Fault を導入することを想定する（他のパラメータの場合も同様である）. Fault が導入された値を $\hat{a}_4$ と表す. また, パラメータ a_6 は点の加算式において使用しないため, 演算を本来の曲線 E から曲線 $\hat{E}(a_1, a_2, a_3, \hat{a}_4, \hat{a}_6)$ に移す. さらに, 入力点 $P = (x, y)$ と $\hat{Q} = dP = (\hat{x}_d, \hat{y}_d)$ の両方が曲線 $\hat{E}$ にのることから

$$\begin{cases} \hat{a}_4x + \hat{a}_6 = y^2 + a_1xy + a_3y - x^3 - a_2x^2 \\ \hat{a}_4\hat{x}_d + \hat{a}_6 = \hat{y}_d^2 + a_1\hat{x}_d\hat{y}_d + a_3\hat{y}_d - \hat{x}_d^3 - a_2\hat{x}_d^2 \end{cases} \tag{4.11}$$

という方程式の組を得る. この式の組を解くことによって $\hat{a}_4$ と $\hat{a}_6$ の値が与えられる. そして, 点 $\hat{Q}$ と巡回群 $\langle P \rangle \subseteq \hat{E}(a_1, a_2, a_3, \hat{a}_4, \hat{a}_6)$ に属す点 P について離散対数を解くことで $d \pmod r$ の値が求まる. ここで, $r = ord_{\hat{E}}(P)$ である. このようにして求まる $d \pmod r$ を集めて, 中国の剰余定理を用いることで, 秘密情報の d を盗み出す.

4.4.1 防御策

曲線パラメータや定義体の標数などのシステムパラメータに対する Fault 攻撃の防御策としては, スカラー倍算後, 点を出力する直前にパラメータに対するチェックを行うことが挙げられる. 具体的には, 点が入力される前の段階で各パラメータのチェックサムを計算しておき, スカラー倍算の直前とスカラー倍演算の終了後に計算されるそれぞれのチェックサムを比較して, 変化があった場合はエラーとして出力をしないようにする.

4.5 既存研究の問題点

既存の Fault 攻撃手法の多くは入力点 P の値に対して Fault を起こすものである. システムパラメータに対する攻撃, 特に曲線のパラメータに対する Fault 攻撃は十分な研究がされておらず, Montgomery ladder アルゴリズムを対

象とした攻撃手法もまだ示されていない。

第 5 章

ペアリング暗号

ペアリング暗号とは, 楕円曲線上で定義される双線形写像である「ペアリング」を用いた暗号方式である.

5.1 ペアリング

ペアリングとは, 楕円曲線上の点の直積から有限体の乗法群への写像である. G_1, G_2 を単位元 0 の加法に関するアーベル群とし, G_3 を単位元 1 の乗法に関する位数 n の巡回群とする. このとき,

$$e : G_1 \times\ G_2 \rightarrow G_3 \tag{5.1}$$

が, 以下の 2 つの性質を満たす時, e をペアリング写像よ呼ぶ.

1. 双線形性
   $^{\forall}P, P' \in G_1$ と $^{\forall}Q, Q' \in G_2$ に対して, 以下の 2 つが成り立つ.

$$e(P + P', Q) = e(P, Q) + e(P', Q), e(P, Q + Q') = e(P, Q) + e(P, Q') \tag{5.2}$$

2. 非退化

5.1.1 防御策

この攻撃を防ぐためには, 出力前に入力点 P とそのスカラー倍算 kP の両方が楕円曲線 E に載るかどうかを曲線パラメータの a_6 を用いてチェックを行う. このように, 点が曲線に載るかどうかを演算に用いられていないパラメータを使用してチェックすることを, **ポイントチェック**と呼ぶ.

5.2 ペアリング暗号

5.2.1 Miller algorithm

5.3 ペアリング暗号に対するフォールト攻撃

$B = \{1, \xi, \sqrt{v}, \xi\sqrt{v}\}$ を $\mathbb{F}_q^k$ の基底とする.
$r_{\tau-1} = 0$ の場合,

$$F_{\tau\ +1,P}(Q) = (F_{\tau,P}(Q))^2 \times\ h_1(Q) \tag{5.3}$$

$$[j]P = (X_j, Y_j, Z_j) \tag{5.4}$$

$$T = [2j]P = (X_2j, Y2j, Z_2j) \tag{5.5}$$

が分かり, h_1 の方程式を用いて以下の方程式を得る.

$$F_{\tau\ +1,P}(Q) = (F_{\tau\ ,P}(Q))^2 \times\ (Z_{2j} Z_j^2 y\sqrt{v} - 3(X_j - Z_j^2)(X_j + (Z_j^2)(xZ_j^2 - X_j)) \tag{5.6}$$

点 P を秘密点とすると, j, τ , Q の座標が分かる. さらに, Miller algorithm により $F_{\tau\ +1,P}(Q)$ と $F_{\tau\ ,P}(Q)$ が与えられる.

比 $R = \frac{F_{\tau\ +1,P}(Q)}{(F_{\tau\ ,P}(Q))^2}$ を計算する. R の理論上の形と, 基底 B の分解を用いると, 恒等式によって以下の集合が得られる.

$$\begin{cases} Y_j Z j^2 = \lambda_{\ 2}, \\ Z_j^2(X_j^2 - Z_j^4) = \lambda_{\ 1}, \\ 3X_j(X_j^2 - Z_j^4) + 2Y_j^2 = \lambda_{\ 0}, \end{cases} \tag{5.7}$$

非線形システムの分解により, 以下の式が与えられる.

$$(\lambda_{\ 0}^{\ 2} - 9\ \lambda_{\ 1}^{\ 2}) Z^1 2 - (4\ \lambda_{\ 0}\lambda_{\ 2}^{\ 2} + 9\ \lambda\ 1^3) Z^6 + 4\ \lambda_{\ 1}^{\ 4} = 0 \tag{5.8}$$

Z_j の方程式を解くと, せいぜい $24 = 12 \times\ 2 \times\ 1$ で, 点 $[j]P$ の座標 (X_j, Y_j, Z_j) を見つけられる. $[j]P$ の値が分かると, $j \pmod r$ のインバース j' を見つけることで, $[j'][j]P = [j'j]P = P$ を見つけることが可能となる.

5.3.1 防御策

曲線パラメータや定義体の標数などのシステムパラメータに対する Fault 攻撃の防御策としては, スカラー倍算後, 点を出力する直前にパラメータに対するチェックを行うことが挙げられる. 具体的には, 点が入力される前の段階で各パラメータのチェックサムを計算しておき, スカラー倍算の直前とスカラー倍演算の終了後に計算されるそれぞれのチェックサムを比較して, 変化があった場合はエラーとして出力をしないようにする.

5.4 既存研究の問題点

既存の Fault 攻撃手法の多くは入力点 P の値に対して Fault を起こすものである. システムパラメータに対する攻撃, 特に曲線のパラメータに対する Fault 攻撃は十分な研究がされておらず, Montgomery ladder アルゴリズムを対象とした攻撃手法もまだ示されていない。

第 6 章

提案手法

本研究では, Fault 導入の対象を曲線のパラメータとし, twist 曲線の手法を加えた新しい Fault 攻撃を提案する.

6.1 提案手法

楕円曲線暗号の実装環境によっては, 曲線のパラメータ a を固定した上でスカラー倍算をするものがある. そのため, 攻撃のモデルは a, もしくは b に限定した上で 1bit のビットフリップをする場合と, a, b 両方が変更可能なときに, どちらかの 1bit に Fault を導入する場合の, 合わせて 3 パターンを提案する.

6.1.1 前提

定義体を素体 $\mathbb{K} = \mathbb{F}_q$ とし, その体 $\mathbb{K}$ 上に定義された楕円曲線を $E : y^2 = x^3 + ax + b$ とする. 点のスカラー倍算には Montgomery ladder を用いる. また, 出力の直前に入力点 $P = (x_0, y_0)$ とそのスカラー倍算 $Q = kP$ に対するポイントチェックを行わないとする.

6.1.2 パラメータ b に対する攻撃

一つ目の提案手法として, 楕円曲線 E のパラメータ b に Fault を導入する場合の攻撃モデルを示す. このことにより変化したパラメータ値を $\hat{b}$ とする. ここで, 点のスカラー倍算を行う楕円曲線は $1/2$ の確率で

$$\hat{E} : y^2 = x^3 + ax + \hat{b} \tag{6.1}$$

もしくは, $y \notin \mathbb{K}$ のときには $\hat{E}$ の 2 次 twist 曲線 $\hat{E}_d$

$$\hat{E}_d : dy^2 = x^3 + ax + \hat{b} \tag{6.2}$$

のどちらかの曲線に移る.

楕円曲線が $\hat{E}$ に移るとする. このとき, 入力点 P のスカラー倍算には y_0 を用いないため, 入力点は $\hat{E}$ 上の点 $\hat{P} = (x_0, \hat{y}_0)$ となる. ここで, $\hat{y}_0^2 = x_0^3 + ax_0 + \hat{b}$ である.

$\hat{y}_0 \in \mathbb{K}$ のとき, 点 $\hat{P}$ が属す楕円曲線は $\hat{E}$ に移り, $\hat{y}_0 \notin \mathbb{K}$ のとき, 曲線が $\hat{E}_d$ に移る.

このことにより, スカラー倍算結果として $\hat{Q}$ の x 座標が出力される. ここで, $\hat{Q}$ の y 座標は一意に定まらないため, 4.1 で述べたように点を $(x_0, \hat{y}_1), (x_0, -\hat{y}_1)$ とおき, k^2 を用いてスカラー値 k の復元を行う.

また, 曲線 $\hat{E}$ 上の点 $\hat{P}$ の位数 $ord(\hat{P})$ は素数ではなく, 本来の曲線と比べて位数の最大素因数が小さい値となる. すなわち, ECDLP の求解に必要な計算量が減少する.

位数の最大素因数が十分に小さくなるとき, 2 点 $\hat{P}, \hat{Q}$ に関して ECDLP を解くことで $k \bmod ord(\hat{P})$ が求まる.

$ord(\hat{P})$ の値が $ord(P)$ よりも大きいときは $k \bmod ord(\hat{P})$ をスカラー値 k として得る.

$ord(\hat{P})$ の値が $ord(P)$ よりも小さいときは, 上記の処理を繰り返し行い, いくつかの $k_i \bmod ord(\hat{P}_i)$ を集め, 中国の剰余定理を用いることにより, スカラー値 k を復元する. 復元する際は, それぞれの点の位数 $r_i = ord(\hat{P}_i)$ がスムースなほど, 復元に必要な Fault の導入回数と, ECDLP 計算の計算量が少なくなる.

6.1.3 パラメータ a に対する攻撃

同じ前提**??**のもと, 楕円曲線 E のパラメータ a に対して 1bit の Fault を導入する場合を考える.

このことにより変化したパラメータ値を $\hat{a}$ とすると, 曲線は

$$\hat{E} : y^2 = x^3 + \hat{a}x + b \tag{6.3}$$

もしくは, この曲線 $\hat{E}$ の twist 曲線

$$\hat{E}_d : dy^2 = x^3 + \hat{a}x + b \tag{6.4}$$

に移る.

よって, 点 P は $\hat{P} = (x_0, \hat{y}_0)$ に移る. ここで, $\hat{y}_0^2 = x_0^3 + \hat{a}x_0 + b$ である.

以降の処理は, 前項 **??** と同様にスカラー値 k を盗み出す.

6.1.4 a もしくは b に対する攻撃

パラメータ a, b のデータを格納するレジスタの両方に対して Fault を導入することができる場合を考える. この手法では, 攻撃者が Fault の導入対象を a, b のどちらかに一方に, 選択的に限定できないと想定する. この想定では, Fault の導入時に攻撃者はパラメータ a, b のどちらに Fault が起きたか判断できないため, 復元段階において, **??**と**??**の方法を実行し判断をする. そのため, 復元に必要な探索範囲はおよそ倍になる.

パラメータ a, もしくは b のどちらか一方に Fault を導入するような攻撃アルゴリズムを表**??**に示す.

6.2 防御策

この攻撃手法への防御策としては, 4.4 と同様にパラメータに対してチェックをすることが挙げられる. チェックを実施するにあたって, 実行時間の冗長性が必要となる. 実装環境の制約から確実性が高くなくとも, 許容できる計算時間で実行できるチェックが採用される.

パラメータに対するチェックサムとして, CRC が挙げられる. CRC はチェック対象のデータにおける, 任意の多項式による剰余の値をチェックに用いる. このような性質から, チェックに用いる剰余の値が変化しないように元のデータを改ざんできる. 例えば, 最も単純なチェックサムであるパリティチェックであれば, 二進数データにおける 0(もしくは 1) の遇奇性が保たれるよう Fault を導入すると, 同一のチェック結果が出力されるため, パラメータの変化を検出できない. このように, 実装されているチェックの数学的な特性を用いて, 誤りを検出されないような Fault の導入方法も検討することができる.

注意すべき点として, 暗号装置に実装する曲線に twist secure な曲線を選択しても, 提案する攻撃手法への防御策としては有効ではない. 安全な曲線の選択には, twist secure であることに加えて, 曲線のパラメータが数 bit 変化したとしても一定の安全性を備えるよう, 注意深く検査する必要がある.

表 6.1　Algorithm 4: パラメータ a, もしくは b に対する攻撃

input: $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_q, P = (x_0, y_0) \in E(\mathbb{F}_q)$, ECDLP が計算可能な位数の上限 t
output: スカラー値 k

Phase 1: Fault 値を集める
1 : **for** $i = 1$ **to** n **do**
1.1 : E のパラメータ a または b に対して 1bit の Fault を導入する.
1.1.1 : Fault をパラメータ a に導入する場合, $\hat{E}_i : y^2 = x^3 + \hat{a}_i x + b$ となる. 点が $P = (x_0, y_0)$ から $\hat{P}_i = (x_0, \hat{y}_i)$ に移る. このとき, $\hat{y}_i^2 = x_0^3 + \hat{a}_i x_0 + b$ を満たす.
1.1.2 : Fault をパラメータ b に導入する場合, $\hat{E} : y^2 = x^3 + ax + \hat{b}_i$ となる. 点が $P = (x_0, y_0)$ から $\hat{P}_i = (x_0, \hat{y}_i)$ に移る. このとき, $\hat{y}_i^2 = x_0^3 + ax_0 + \hat{b}_i$ を満たす.
1.2 : $\hat{Q}_i = k\hat{P}_i$ を Algorithm 1 を用いて計算する.
2 : **end for**
Phase 2: スカラー値 k の復元
3 : $prod = 1$.
4 : **for** $i = 1$ **to** n **do**
4.1 : $R_i = ord(\hat{P})$ を計算する.
4.2 : $R_i = \prod r_{i,j} = r_{i,1} r_{i,2} \cdots r_{i,m}$ $(j = 1, 2, \ldots, m)$ として素因数分解する.
4.3 : **for** $j = 1$ **to** m **do**
4.3.1 : $\hat{P} \equiv \hat{P}_{i,j} \pmod{r_{i,j}}$, $\hat{Q} \equiv \hat{Q}_{i,j} \pmod{r_{i,j}}$ とおく.
4.3.2 : ECDLP : $k_{i,j} = \log_{P_{i,j}} Q_{i,j}$ を解き, $k \equiv k_{i,j} \pmod{r_{i,j}}$ を得る.
4.3.3 : **if** $((r_{i,j} < t)$ **and** $(gcd(prod, r_{i,j}) = 1))$ **then**
4.3.3.1 : $prod = prod \times r_{i,j}$.
4.3.4 : **end if**
4.3.5 : **if** $(prod \geq r_i i, j)$ **then**
4.3.5.1 : ステップ 4.3.3 を満たすすべての $k \equiv k_{i,j} \pmod{r_{i,j}}$ について中国の剰余定理を用いて, k を復元する.
4.3.5.2 : **return** k.
4.4 : **end for**
5 : **end for**
6 : **return** "failure".

第 7 章

実験

表**??**の攻撃アルゴリズムの数値実験を行った. 実験プログラムには Magma を用いた.

7.1 実験条件

以下の条件において, 試行回数に対して攻撃成功となる確率を測定する.

- パラメータ a, もしくは b のデータのランダムな 1bit を変化させる.
- 点 $\hat{P}$ を n 個集め, 2^{100} 以下となる位数の素因数の, 総乗値が $ord(P)$ 以上になるときに攻撃成功とする.
- 試行回数 m は 10000 回とする.
- 使用するパラメータは, NIST(米国国立標準技術研究所) が推奨する楕円曲線のシステムパラメータ P-192 と P-256[**?**] を用いる.
- 比較対象は, パラメータ a, もしくは b に対する [**?**] の攻撃手法とする. すなわち, 点が twist 曲線に属す場合は攻撃失敗となる.

7.2 実験結果

表 7.1 結果:P-196

攻撃手法 ＼ 使用する点の個数		1	2	3	4	5	6	7	8	9	10
NIST P-192	twist なし [**?**]	7.1%	18.4%	30.7%	42.1%	52.4%	61.6%	69.3%	75.6%	81.0%	85.2%
	提案手法	7.2%	27.5%	46.5%	62.4%	74.6%	83.7%	90.3%	94.1%	96.7%	98.3%

表 7.2 結果:P-256

攻撃手法 ＼ 使用する点の個数		1	2	3	4	5	6	7	8	9	10
NIST P-256	twist なし [**?**]	2.7%	6.9%	12.7%	20.1%	28.3%	37.0%	44.8%	52.9%	60.1%	66.5%
	提案手法	3.4%	10.5%	22.3%	36.6%	51.8%	65.3%	75.6%	83.7%	89.2%	93.4%

第 8 章

結論

8.1 結論

本研究では, Montgomery ladder を用いた楕円曲線暗号における曲線のパラメータを Fault 導入の対象とした, 新しい攻撃手法を提案した. この手法では Twist Attack で示された twist 曲線上の攻撃手法を組み合わせることによって, 曲線パラメータに対する単純な攻撃方法よりも攻撃成功率を高めた. さらに, プログラミング言語 Magma 上で, NIST 標準パラメータ [**?**] を用いた楕円曲線暗号に対する攻撃の実験を行い, 提案手法の有効性を実際に確かめた.

これは, 楕円曲線暗号の実装における, Fault 攻撃への対策の必要性を強調するものである.

8.2 今後の課題

今後の課題としては以下のものがあげられる.

- 定義体の標数が 2 の場合の攻撃.
- パラメータチェックへの対抗策を付加する.
- 特定の物理的干渉手段の特性を考慮した上での攻撃.

謝辞

本研究を進めるにあたり，適切な御指導, 御助言, 御検討を頂いた中央大学 理工学部 趙 晋輝 教授に，深く感謝いたします. また, デバイスの知識に関してご助言を頂いた中央大学 理工学部 古屋 清 教授に, 深く感謝いたします. 最後に, 日ごろの学生生活においてお世話になった中央大学趙研究室の皆様に深く感謝いたします.

参考文献

[1] I. Biehl, B. Meyer, and V. Müller. *Differential Fault Attacks on Elliptic Curve Cryptosystems*, Springer-Verlag, CRYPTO, pp.131-146, LNCS, 2000.

[2] Montgomery, P.L.: *Speeding the Pollard and Elliptic Curve Methods of Factorization.* Mathematics of Computation, Volume 48, pp.243-264, 1987.

[3] Tetsuya Izu, Bodo Möller, Tsuyoshi Takagi:*Improved Elliptic Curve Multiplication Methods Resistant against Side Channel Attacks*, Progress in Cryptology - INDOCRYPT 2002, pp. 296-313, Springer-Verlag, A. Menezes, P. Sarkar, 2002.

[4] Stephen C. Pohlig and Martin E. Hellman. *An improved algorithm for computing logarithms over GF(p) and its cryptographic significance*, IEEE Trans. on Inf. Theory, 24:106-110, 1978.

[5] J.M. Pollard. *Monte Carlo methods for index computation (modp)*,Mathematics of Computation, 32:918-924, 1978.

[6] Sergei P. Skorobogatov: *Semi-invasive attacks: A new approach to hardware security analysis*, Technical Report UCAM-CL-TR-630, Computer Laboratory, University of Cambridge, 2005.

[7] Barenghi, A., Bertoni, G., Parrinello, E. & Pelosi, G. *Low Voltage Fault Attacks on the RSA Cryptosystem*, 2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), 2009, pp.23-31.

[8] Alessandro Barenghi, Guido Bertoni, Luca Breveglieri, and others, *Low Voltage Fault Attacks to AES and RSA on General Purpose Processors*, IEEE International Workshop on Hardware-Oriented Security and Trust, 2010, pp.7-12.

[9] Schmid, J.M., Herbst, C.: *A Practical Fault Attack on Square and Multiply*,Fault Diagnosis and Tolerance in Cryptography (FDTC) 2008, pp.53-58, IEEE Computer Society, 2008.

[10] Nidhal Selmane, Sylvain Guilley, Jean-Luc Danger: *Practical Setup Time Violation Attacks on AES*,Seventh European Dependable Computing Conference, pp.91-96, IEEE Computer Society, 2002.

[11] P. A. Fouque, R. Lercier, D. Réal, F. Valette: *Fault Attack on Elliptic Curve Montgomery Ladder Implementation*, 2008 5th Workshop on Fault Diagnosis and Tolerance in Cryptography, 2008.

[12] M. Ciet and M. Joye: *Elliptic Curve Cryptosystems in the Presence of Permanent and Transient Faults*, Designs, Codes and Cryptography 36 (2005), pp.33-43, 2005.

[13] Federal Information Processing Standards Publication FIPS 186-2. Digital Signature Standard (DSS), appendix 6: *Recommended Elliptic Curves for Federal Government Use*, Technical report, NIST, January 27, 2000.

[14] ANSI X9.63.: *Public Key Cryptography For The Financial Services Industry:Key Agreement and Key Transport Using Elliptic Curve Cryptography*, 1999.

[15] Jörn-Marc Schmidt, Michael Hutter, Thomas Plos: *Optical Fault Attacks on AES: A Threat in Violet*, Fault Diagnosis and Tolerance in Cryptography (FDTC) 2009, pp.13-22, IEEE Computer Society, 2009.

[16] Sudhakar Govindavajhala, Andrew W. Appel: *Using Memory Errors to Attack a Virtual Machine*, 2003 IEEE Symposium on Security and Privacy, pp.154-165, IEEE Computer Society, 2003.

[17] Jörn-Marc Schmidt, Michael Hutter: *Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results*, 15th Austrian Workshop on Microelectronics (Austrochip 2007), pp.61-67, Verlag der Technischen Universität Graz, 2007

[18] 新妻弘, 木村哲三：**群・環・体　入門**, 共立出版, 1999.

[19] Christophe Doche, Tanja Lange : *Arithmetic of Elliptic Curves*, Handbook of elliptic and hyperelliptic curve cryptography, pp.267–302, Chapman & Hall/CRC, 2006.