L-018

SIDH 鍵交換方式に対する Fault 攻撃
Fault attack to SIDH key exchange protocol

山岸純一 Junichi Yamagishi *
相賀陸 Riku Aiga *
趙晋輝 Jinhui Chao †

1 まえがき

高性能な量子計算機が実用化された場合, 素因数分解や有限体上と楕円曲線上の離散対数問題を安全性の根拠とする暗号方式が解読される可能性が示唆されている. そのため量子計算機の開発後の安全な通信を担保するため, 量子計算機でも計算量的に解読不可能な暗号方式である耐量子暗号の選定や研究が進んでいる. SIDH 鍵交換方式は耐量子暗号の 1 つで同種写像問題を安全性の根拠としている. この問題は, 拡大体上に定義されている超特異楕円曲線を利用している場合, 量子計算機を用いても高速で解くことが出来ないが、素体上であった場合, 準指数時間で解く事ができる. 本論文では公開パラメーターである定義体の定義多項式に対しフォルト攻撃を行い, 定義体が素体になることを利用して SIDH 鍵交換方式の安全性を低減させる手法を示す.

2 楕円曲線と同種写像

p を奇素数，$q = p^n$, E, E' を $\mathbb{F}_q$ 上の楕円曲線とする. 恒等写像でない有理点群の準同型写像 $f : E(\mathbb{F}_q) \to E'(\mathbb{F}_q)$ を同種写像といい, 同種写像が存在する曲線同士を同種であるという.

3 超特異曲線と自己準同型環

有限体 $\mathbb{F}_q$ 上の楕円曲線 E に対して不変量 t を $t = q + 1 - \#E(\mathbb{F}_q)$ と定義する. この t に対して $t \mid p$ が成り立つとき E は超特異 (supersingular) であるといい, それ以外のとき ordinary であるという. $\overline{\mathbb{F}_q}$ 上の超特異楕円曲線は全て $\mathbb{F}_{p^2}$ 上で定義されることが知られている.

$\mathbb{F}_q$ 上で定義された楕円曲線 E の自己準同型写像全体は環を成す. これを自己準同型環と呼び $End(E)$ と表す. 楕円曲線 E が ordinary あるいは $\mathbb{F}_p$ 上で定義される超特異な曲線の場合は $K = \mathbb{Q}(\sqrt{D})$ $(D = t^2 - 4q)$ の整数環の部分環となる [7]. 一方で, $\mathbb{F}_{p^2}$ 上で定義される超特異な曲線の場合 $End(E)$ は p, ∞ で分岐する四元数環の部分環となる. したがって $\mathbb{F}_{p^2}$ 上の超特異曲線の自己準同型環は非可換である.

* 中央大学大学院理工学研究科情報工学専攻 Department of Information and Systems Engineering, Graduate School of Science and Engineering, Chuo University.
† 中央大学理工学部情報工学科 Department of Information and Systems Engineering, Faculty of Science and Engineering, Chuo University.

4 SIDH 鍵交換方式

SIDH 鍵交換方式は Jao D et al. によって提案された暗号方式である [1]. この暗号方式は有限体上の Diffie-Hellman 鍵交換方式を元に, 安全性の根拠とする問題を離散対数問題から同種写像問題へと書き換えたものである.

公開パラメーターを次で与える.

- $p = {l_A}^{e_A} \cdot {l_B}^{e_B} \cdot f \pm 1$: 素数
- E : $\mathbb{F}_{p^2}$ 上の超特異楕円曲線
- P_A, Q_A : $E[{l_A}^{e_A}]$ の生成元
- P_B, Q_B : $E[{l_B}^{e_B}]$ の生成元

公開パラメーター決定後のアルゴリズムは以下のとおり

1. Alice はランダムに $0 \leq m_A,\ n_A < {l_A}^{e_A}$ を選ぶ
2. Alice は秘密鍵 $R_A = m_A P_A + n_A Q_A$ を計算する.
3. Alice は同種写像 $\phi_A : E \to E_A (Ker\ \phi_A = \langle R_A \rangle)$ と楕円曲線 E_A を計算する.
4. Alice は $\phi_A(P_B),\ \phi_A(Q_B)$ を計算し,Bob に $(E_A,\ \phi_A(P_B),\ \phi_A(Q_B))$ を送信する.
5. Bob は 1-4 の手順を A と B を入れ替えて行う.
6. Alice は Bob から送信された $(E_B,\ \phi_B(P_A),\ \phi_B(Q_A))$ と m_A, n_A を使い, $T_A = m_A \phi_B(P_A) + n_A \phi_B(Q_A)$ を計算する.
7. Alice は $\phi_{BA} : E_B \to E_{BA} (Ker\ g_A = \langle T_A \rangle)$,$j$-不変量 $K_A = j(E_{BA})$ を計算する.
8. Bob は 6-7 の手順を A と B を入れ替えて行う.

5 SIDH の安全性

SIDH は同種写像問題の求解困難性を安全性の根拠にする暗号方式である. 同種写像問題の解法は曲線の種類, 定義体の条件によって異なる.

5.1 Ordinary な曲線の場合

$\mathbb{F}_q$ 上の ordinary な楕円曲線 E_1, E_2 が与えられたとき, 同種写像 $\phi : E_1 \to E_2$ を与える現在最も速いアルゴリズムが Childs, Jao, Soukharev により提案された. その計算量は量子計算機で $L_q(\frac{1}{2}, \frac{\sqrt{3}}{2})$ である [5].

5.2 超特異曲線の場合

5.2.1 定義体が素体 $\mathbb{F}_p$ $\mathbb{F}_p$ 上で定義されている場合, 虚二次体の整数環の部分環となることが判明している. また Biasse, Jao, Sankar により定義体が $\mathbb{F}_p$ の場合は非特異曲線のときと同様に解読にかかる計算量は量子計算機で $L_p(\frac{1}{2})$ であることが知られている [4].

5.2.2 定義体が拡大体 $\mathbb{F}_{p^2}$　定義体が $\mathbb{F}_{p^2}$ の場合

(1) 超特異曲線 E_1, E_2 をそれぞれ $\mathbb{F}_p$ 上で定義された超特異楕円曲線 E_1', E_2' に移す同種写像を見つける.
(2) 同種写像 $\phi : E_1' \to E_2'$ を求める.

という手法が現在知られているアルゴリズムの中で最も速い. その計算量はステップ (1) が Grover のアルゴリズムを利用して $\tilde{O}(p^{\frac{1}{4}})$, ステップ (2) が $L_p(\frac{1}{2})$ であるため全体の計算量は $\tilde{O}(p^{\frac{1}{4}})$ である [4].

6 フォルト攻撃

フォルト攻撃とは暗号の実装部分に物理的に干渉することで公開パラメーターの数値を変化させ, 不正な値を集めて, その値から秘密情報を計算する攻撃手法である. 既存研究として楕円曲線暗号のベースポイント, 体の標数, 楕円曲線の係数への攻撃が知られている [6].

7 提案手法

本稿では, 2 次体の定義多項式へのフォルト攻撃を提案する. 2 次体 $\mathbb{F}_{p^2}$ の定義多項式を体 $\mathbb{F}_p$ 上 の既約多項式 $f(x) = x^2 + Ax + B, (A, B \in \mathbb{F}_p)$ とする. フォルト挿入によって A を A', 或いは B を B' に変化させた多項式が $\mathbb{F}_p$ 上で因数分解できるとき楕円曲線が素体上定義される. すると SIDH の計算は形式的に 2 次体上のまま, 自己準同型環が可換になり, 準指数時間の攻撃法が適用される. $\mathbb{F}_p$ 上の多項式の既約性は判別式 $A^2 - 4B$ が $mod\ p$ で平方剰余かどうかによって決まるため, ランダムなフォルトに対しては, ほぼ半分の確率で定義多項式が既約でなくなり攻撃が成立する.

8 実験

暗号装置への 1bit のフォルト挿入によりビット反転が起こる確率はいずれのビットも同じと仮定して, 二次拡大体の定義多項式 $f(x) = x^3 + Ax + B$ の係数 $A, B \in \mathbb{F}_p$ にランダムに 1bit の Fault を挿入し, どの程度の確率で定義多項式が可約になるのか調べる実験を行った.
実験に利用した素数は $p = 2^{372} * 3^{239} - 1$ とした [8].

1. $f(x) = x^2 + 1$
2. $f(x) = x^2 + x + 1$
3. $f(x) = x^2 + Ax + B$

$A = 10349294439841333552731315636081942643031428748$
$796477595826258962174496091483625936413224363828214$
$386263623721237957567286890373795733135506588588113$
$756324604906726530006430654797684206557602676475935$
$084517186972862019840130832522950870874360476010124$
$094645144168239511112286371196033497837579121233911$
27978524009400

$B = 433837756688833157230897540431705878893990792457$
$564187989846419654399156098084333702677721774579371 3$
$494454770602980010757876696572502872410069766778477 4$
$819678374705615985963425027419093719381566926023676 9$
$091263326965582607809354038029168343030586211200664 3$
$170953403453641528084948755393619457231065030847219 7$
4329578

9 実験結果

各多項式にフォルト攻撃を行った結果を以下の表に示す.

表 1　定義多項式

多項式	A への攻撃	B への攻撃	合計
1.	49.00%	49.66%	49.33%
2.	49.80%	50.46%	50.13%
3.	49.66%	48.73%	49.20%

9.1 実験評価

いずれの定義多項式についても攻撃する係数に関わらず約 50% 程度の確率で可約となった.

10 まとめと考察

本稿では SIDH 鍵交換方式に利用する曲線の二次体の定義多項式に対する Fault 攻撃を提案し, その有効性を示した. 今後の研究課題としては他の公開パラメーターへの攻撃手法の提案が挙げられる.

謝辞

本研究の一部は、総務省・SCOPE(181603006) の支援に基づいている。

参考文献

[1] Jao D., De Feo L.: *Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies*, ePrints, 2011, `https://eprint.iacr.org/2011/506.pdf`

[2] Steven D. Garbraith, Frederik Vercauteren: *Computational problems in supersingular elliptic curve isogenies*, ePrints, 2017, `https://eprint.iacr.org/2017/774.pdf`

[3] Silverman, Joseph H : *The Arithmetic of Elliptic Curves 2nd Edition*, Springer ,1994

[4] Biasse JF., Jao D., Sankar A. : *A Quantum Algorithm for Computing Isogenies between Supersingular Elliptic Curves.*, INDOCRYPT 2014. INDOCRYPT 2014. Lecture Notes in Computer Science, vol 8885. Springer, Cham, 2014

[5] Andrew M. Childs, David Jao,Vladimir Soukharev : *Constructing elliptic curve isogenies in quantum subexponential time*, Journal of Mathematical Cryptology, Volume 8, Issue 1, Pages 1-29, ISSN (Online) 1862-2984, ISSN (Print) 1862-2976, 2013

[6] Marc Joye and Michael Tunstall. :*Fault Analysis in Cryptography,, Springer-Verlag Berlin Heidelberg*, 2012

[7] Christina Delfs and Steven D. Galbraith.: *Computing isogenies between supersingular elliptic curves over* $\mathbb{F}_p$. Des. Codes Cryptography,78(2) p425-p440. 2016

[8] Costello C., Longa P., Naehrig M. (2016) Efficient Algorithms for Supersingular Isogeny Diffie-Hellman. In: Robshaw M., Katz J. (eds) Advances in Cryptology - CRYPTO 2016. CRYPTO 2016. Lecture Notes in Computer Science, vol 9814. Springer, Berlin, Heidelberg