L-038

楕円曲線暗号における曲線パラメータに対する Fault 攻撃
Fault attacks to elliptic curve cryptosystems with definition equation errors

林 弘悦† 趙 晋輝‡
Hiroyoshi Hayashi Jinhui Chao

1. まえがき

Fault 攻撃はサイドチャネル攻撃の一種として, 暗号演算中の装置に対して物理的な干渉手段を用いて誤り(fault)を導入し秘密情報を盗みだす強力な攻撃である. 近年, 攻撃に使用する機器が手に入りやすくなっていることや物理的な干渉技術が発達していることから脅威となっている. 攻撃対象として共通鍵暗号, 公開鍵暗号ともに提案されている.

楕円曲線暗号は RSA 等の既存の公開鍵暗号よりも短い鍵を用いることが出来, スマートカードのような低機能なデバイスでの活用が見込まれている. 楕円曲線暗号の安全性は楕円曲線離散対数問題(ECDLP)の困難性に基づいている. ベースポイント $P \in E(K)$ に対してスカラー値 k を用いて $Q = kP$ を行うスカラー倍算が楕円曲線暗号の中心となる計算である. ECDLP の最も効率的な解法として Pohlig-Hellman 法と Pollard の rho 法が知られている. また, 奇標数体上の楕円曲線でのスカラー倍算のアルゴリズムでは Montgomery Ladder が効率的な手法として知られている.

楕円暗号に対する Fault 攻撃として、今までベースポイントと曲線パラメータに関する方式が提案されている[1,2,3]. 本論文では, 標数が 3 よりも大きい奇数である体 K 上の楕円曲線に対して Montgomery Ladder アルゴリズムを用いて点のスカラー倍算を行う楕円曲線暗号システムを標的とする新しい fault 攻撃手法を提案する. 具体的に楕円曲線の係数パラメータに対して fault を与えることでスカラー倍算を 2 次の twist 曲線を含める異なる曲線へ移し、ECDLP を Pohlig-Hellman 法と Pollard の rho 法により秘密情報を盗み出す手法である. また, NIST 推奨楕円曲線に対して攻撃を適用し, 提案手法の有効性評価を行った.

2. 既存研究

2.1 曲線パラメータに対する Fault 攻撃

楕円曲線の定義式の係数パラメータを変化させる攻撃手法を Ciet と Joye が提案している[2].

スカラー倍算に用いる曲線の方程式における係数一つに fault を起こす. これにより曲線が本来の曲線よりも十分に低い位数の曲線に移ったときには ECDLP に必要な計算量が減少し, Pohlig-Hellman 法と Pollard の rho 法を用いることで現実的な時間で鍵の復元が可能となる.

2.2 ベースポイントに対する攻撃手法

Invalid-Curve Attack はベースポイントに fault を与えることにより他の曲線にスカラー倍算を移す攻撃手法であり, Biehl らによって提案された[1].

この Invalid-Curve Attack を Montgomery Ladder を対象とし, 改良した攻撃手法が Fouque らが提案した手法である[3]. ベースポイントに fault を与えた際に Montgomery Ladder 上ではおよそ 1/2 の確率で本来の曲線から twist 曲線に移る. twist 曲線では本来の曲線よりも位数がスムーズになり ECDLP の弱体化が期待できる. この攻撃への対抗策として twist 曲線が脆弱でない Twist Secure な楕円曲線を設定することがあげられる.

3. 提案手法

以下では、標数が 3 よりも大きい奇数である体 K 上の楕円曲線に対して Montgomery Ladder アルゴリズムを用いた暗号系に対して、楕円曲線の定義式の係数 a, b に対してランダムな 1bit の fault を与えることでスカラー倍算を異なる曲線に移して攻撃し、とくにその際に twist 曲線も使用することにより攻撃成功率を高める手法を示す.

ここで与えるランダムな位置におけるランダムな 1bit の fault の想定は 1bit の fault の導入手法が多く報告されている[5]ことと, fault 位置の復元の容易さのためである.

3.1 Twist 曲線

標数が 3 より大きい体 K 上の楕円曲線 $E: y^2 = x^3 + ax + b \quad (a,b \in K)$ に対して, 2 次拡大体上の twist 曲線 E_d は $\sqrt{d} \notin K$ として次式で定義される.

$$E_d : dy^2 = x^3 + ax + b$$

3.2 パラメータ b に対する攻撃

fault の導入によってパラメータが b に変化したとする.

これによりベースポイント $P = (x_0, y_0)$ は $\overline{P} = (x_0, \overline{y_0})$ に移ると同時に, $x^3 + ax + \bar{b} \notin K$ として, 点のスカラー倍算を行う楕円曲線は 1/2 の確率で

$\overline{E} : y^2 = x^3 + ax + \bar{b}$ もしくは

$\overline{E_d} : dy^2 = x^3 + ax + \bar{b}, \quad d \notin K^2$ に移る.

Montgomery Ladder はベースポイントの y 座標を用いないためそれらの曲線上で $\overline{Q} = k\overline{P}$ が計算され, 出力される.

$\overline{E}(K)$ と $\overline{E_d}(K)$ の位数は計算により得られるため $<\overline{P}>$ 上の ECDLP を解くことにより $k \bmod ord(\overline{P})$ が求まる. この計算には Pohlig-Hellman 法と Pollard's rho 法を用いる.

3.3 パラメータ a に対する攻撃

パラメータ b の攻撃の想定と同様にパラメータ a に 1bit の fault が加わったとする. このときベースポイント $P = (x_0, y_0)$ は以下の式を満たす点 $\overline{P} = (x_0, \overline{y_0})$ に移る.

$\overline{E} : y^2 = x^3 + \bar{a}x + b$

もしくはその twist 曲線

$\overline{E_d} : dy^2 = x^3 + \bar{a}x + b, \quad d \notin K^2$

† 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.

の上に載る.

3.4 パラメータ a もしくは b に対する攻撃

攻撃者が a もしくは b のどちらに Fault が起きたか知ることができない場合を想定する. このとき攻撃者は a に対する攻撃と b に対する攻撃両方を試す必要がある. そのため試行する範囲はおよそ 2 倍になる.

4. 評価実験

提案する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. 実験条件は以下である.

- パラメータ a もしくは b のデータに,ランダムな 1bit を変化させる.
- 点 $\overline{P}$ 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 が推奨するパラメータ P-192 と P-256 を用いる.
- 比較対象は, Ciet Joye の攻撃手法とする. すなわち, Twist 曲線上の点を利用しない.

表 1 と表 2 はそれぞれ P-192, P-256 に対する Ciet Joye と提案手法の攻撃成功率を示している. 攻撃に使用する点の数がより少なくても高い攻撃成功率であることがわかる.

Fouque's Attack についても同様に NIST P-192 と P-256 においてベースポイントの x 座標に 1-bit の fault を与えたときの位数サイズを比較すると, 192 パターンの位置に対して, その 31.58%にあたる 60 パターンが twist 曲線に移った.

P-192 の twist 曲線の位数の最大素因数は 95bit であり, 脆弱と言えるレベルのサイズまで減少しているのに対して, P-256 では 241bit とほとんどサイズが減少しなかった.

提案手法を P-192 に対して適用した場合には 192 パターンの位置中 22.513%にあたる 43 パターンの位置に fault が導入された場合に, 移った先の曲線の位数の最大素因数が 100bit を下回る. P-256 では 256 パターン中 7.059%にあたる 18 パターンが 100bit を下回る結果となった.

表 1 P-192 での成功率

		成功確率	
		Ciet Joye	**提案手法**
攻撃に用いる点の個数	1	7.10%	7.20%
	2	18.40%	27.50%
	3	30.70%	46.50%
	4	42.10%	62.40%
	5	52.40%	74.60%
	6	61.60%	83.70%
	7	69.30%	90.30%
	8	75.60%	94.10%
	9	81.00%	96.70%
	10	85.20%	98.30%

表 2 P-256 での成功率

		成功確率	
		Ciet Joye	**提案手法**
攻撃に用いる点の個数	1	2.70%	3.40%
	2	6.90%	10.50%
	3	12.70%	22.30%
	4	20.10%	36.60%
	5	28.30%	51.80%
	6	37.00%	65.30%
	7	44.80%	75.60%
	8	52.90%	83.70%
	9	60.10%	89.20%
	10	66.50%	93.40%

図 1 と図 2 は fault を与えたそれぞれの bit 位置での最大素因数のサイズを示している.

Fouque's Attack では fault によって移る曲線が Twist 曲線ときまっているため, Twist Secure な実装においては効果があげられない. 提案手法では Twist Secure な曲線に対しても攻撃に必要な計算量が極めて小さくなる場合があるという点でも, より汎用性が高く強力な攻撃であると言える.

5. まとめと考察

本論文では Montgomery Ladder を用いる奇標数の楕円曲線暗号に対する新しい fault 攻撃手法を提案した. ECDLP を解き秘密鍵を奪う際に fault 曲線に加え, twist 曲線を使用することによって成功確率を高めたため、評価実験から提案手法が既存手法よりも優れていること、またパラメータ fault 攻撃はベースポイント fault 攻撃よりも強力であることを示した.

この攻撃の防御策としては点や曲線の係数などの種々の値に対して CRC などのチェックを行うことが考えられる. 標数が 2 の体上の楕円曲線暗号への攻撃手法ならびに防御策の検討は今後の課題である.

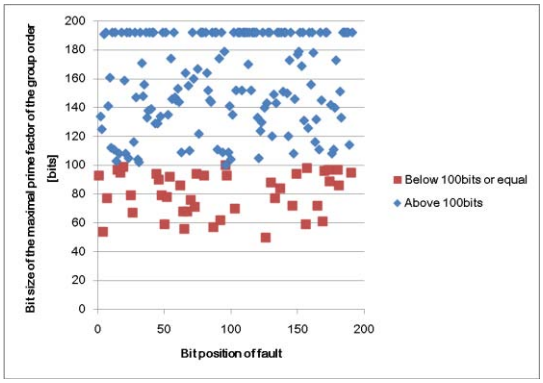

図 1　P-192 ビットサイズ分布

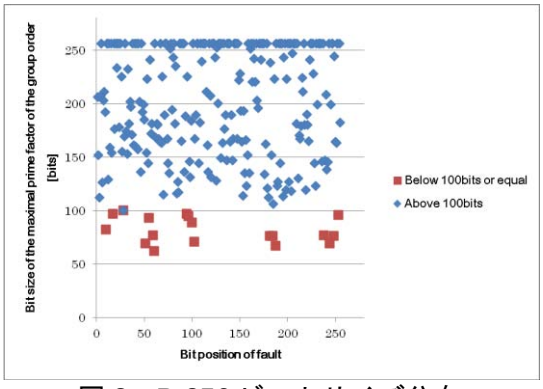

図 2　P-256 ビットサイズ分布

謝辞

本研究を進めるにあたり, デバイス技術に関する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致します.

参考文献

[1] Biehl, I., Meyer, B. and Müller, V., "Differential Fault Attacks on Elliptic Curve Cryptosystems", Advances in Cryptology-CRYPTO 2000, 131-146(2000).
[2] Ciet, M., Joye, M. "Elliptic Curve Cryptosystems in the Presence of Permanent and Transient Faults." Designs. Codes and Cryptography 36, 33-43 (2005).
[3] P. A. Fouque, R. Lercier, D.Réal, Frédéric Valette, "Fault Attack on Elliptic Curve Montgomery Ladder Implementation", 5th Workshop on Fault Diagnosis and Tolerance in Cryptography., 92-98 (2008).
[4] 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.
[5] M. Joye and M. Tunstall, "Fault Analysis in Cryptography". Springer LNCS, March 2011 http://joye.site88.net/FAbook.html. DOI: 10.1007/978-3-642-29656-7 ; ISBN 978-3-642-29655-0.