L-039

サイドチャネル攻撃に安全な Granger-Scott 法
Granger-Scott method against Side-Channel Attack

久木崎 聖矢† 松尾 和人‡ 趙 晋輝*
Seiya KUKISAKI Kazuto MATSUO Jinhui CHAO

1. 序論

楕円曲線暗号の暗号処理の計算量は, 楕円曲線上のスカラー倍算が多くを占めているため, スカラー倍算の高速化の研究が多く行われており, 最近 R.Granger, M.Scott による分割計算法が提案されている. しかし, 近年の脅威として電力解析攻撃という暗号処理から秘密鍵を特定する攻撃が知られている. 電力解析攻撃への対策は計算量が増加し易く, 安全で高速な暗号処理のためには, スカラー倍算の高速化と両立する必要がある. 本研究では, 鍵長が 521bit の楕円曲線暗号を対象として, Granger-Scott 法 を適用したスカラー倍算アルゴリズムに電力解析攻撃への対策を施し, 高速な暗号処理が行われることを検証する.

2. 楕円曲線

標数 $2,3$ でない体 $\mathbb{F}_p$ 上で定義される楕円曲線は, Weierstrass 標準形といわれる $y^2 = x^3 + ax + b\ (a, b \in \mathbb{F}_p)$ の形をしている. 521bit の楕円曲線暗号として NIST が推奨する楕円曲線 P-521 は, $y^2 = x^3 - 3x + b\ (b \in \mathbb{F}_{2^{521}-1})$ で, b は非常に大きな数である[1]. また, H. Edwards 曲線は, $\mathbb{F}_{2^{521}-1}$ 上で定義されている. E-521 と呼ばれる $x^2 + y^2 = 1 - 376014x^2y^2$ が示されている[2][3].

2.1 計算量の比較

射影座標上の P-521 と E-521 の計算量を比較する. OpenSSL では P-521 が使用されており, ヤコビ座標上に定義されている. 体上の乗算を M, 加算を S とすると, 楕円曲線上の点の加算と 2 倍算は表 1 の通りになる.

表 1 スカラー倍算の計算量

楕円曲線の形	座標系	楕円曲線上の点の加算	楕円曲線上の点の 2 倍算
P-521	射影	$12M + 2S$	$7M + 5S$
P-521 (OpenSSL)	ヤコビ	$12M + 4S$	$4M + 6S$
E-521	射影	$10M + 1S$	$3M + 4S$

表 1 より, 楕円曲線上の加算と 2 倍算は E-521 が高速であることがわかる.

3. Granger-Scott 法

$^\forall a, b \in \mathbb{F}_{2^{521}-1}$ の乗算 $a \cdot b$ を高速に行う分割計算法が R.Granger, M.Scott によって提案されている[4]. 521 bit 程度の大きな数を扱う場合多倍長演算を用いることがあるのに対し, Granger-Scott 法では 9 つに分割した 58 bit サイズの数として扱うことにより数値演算が可能になる. 多倍長演算のライブラリを参照できないときに有効な手段である.

521 bit 整数に Granger-Scott 法を適用するときは, $t = 2^{58}$ として $^\forall x, y \in \mathbb{F}_{2^{521}-1}$ を $x = \Sigma_{i=0}^{8} x_i t^i, y = \Sigma_{i=0}^{8} y_i t^i$ を満たす $x_i, y_i\ (i = 0, \cdots, 8)$ に分割する. x_i, y_i を用い $\bar{x} = [x_0, \cdots, x_8], \bar{y} = [y_0, \cdots, y_8]$ とし, 剰余算 $\bar{z} \equiv \bar{x}\bar{y} \pmod{t^9 - 2}$ を行う. このとき剰余算で得られる $\bar{z}$ は,

$$\bar{z} = [z_0, \cdots, z_8] =$$
$$[x_0y_0 + 2x_1y_8 + 2x_2y_7 + 2x_3y_6 + 2x_4y_5 + 2x_5y_4 + 2x_6y_3 + 2x_7y_2 + 2x_8y_1,$$
$$x_0y_1 + x_1y_0 + 2x_2y_8 + 2x_3y_7 + 2x_4y_6 + 2x_5y_5 + 2x_6y_4 + 2x_7y_3 + 2x_8y_2,$$
$$x_0y_2 + x_1y_1 + x_2y_0 + 2x_3y_8 + 2x_4y_7 + 2x_5y_6 + 2x_6y_5 + 2x_7y_4 + 2x_8y_3,$$
$$x_0y_3 + x_1y_2 + x_2y_1 + x_3y_0 + 2x_4y_8 + 2x_5y_7 + 2x_6y_6 + 2x_7y_5 + 2x_8y_4,$$
$$x_0y_4 + x_1y_3 + x_2y_2 + x_3y_1 + x_4y_0 + 2x_5y_8 + 2x_6y_7 + 2x_7y_6 + 2x_8y_5,$$
$$x_0y_5 + x_1y_4 + x_2y_3 + x_3y_2 + x_4y_1 + x_5y_0 + 2x_6y_8 + 2x_7y_7 + 2x_8y_6,$$
$$x_0y_6 + x_1y_5 + x_2y_4 + x_3y_3 + x_4y_2 + x_5y_1 + x_6y_0 + 2x_7y_8 + 2x_8y_7,$$
$$x_0y_7 + x_1y_6 + x_2y_5 + x_3y_4 + x_4y_3 + x_5y_2 + x_6y_1 + x_7y_0 + 2x_8y_8,$$
$$x_0y_8 + x_1y_7 + x_2y_6 + x_3y_5 + x_4y_4 + x_5y_3 + x_6y_2 + x_7y_1 + x_8y_0].$$

y を x に置き換えることで $\bar{z} \equiv \bar{x}^2 \pmod{t^9 - 2}$ を計算することができる.

$^\forall x \in \mathbb{F}_{2^{521}-1}$ の逆元 x^{-1} を考える. $2^{521} - 1$ は素数なので, フェルマーの小定理より $x^{2^{521}-2} \equiv 1 \pmod{2^{521} - 1}$ が成り立つ. よって逆元 x^{-1} は $x^{2^{521}-3}$ となる. 逆元を求める計算量は, 13M+520S となる.

4. Window 法

スカラー倍算を高速に行う方法として Window 法がある. 秘密鍵 d の m 進数展開を利用してスカラー倍算を求める方法である. $m = 4$ のとき, つまり幅を 2 としたときのアルゴリズムをアルゴリズム 1 window method-2 に示す.

アルゴリズム 1 window method-2

Input: $d = (d_{n-1}, \cdots, d_0)_2, P \in E(K)$ Output: dP
Pre-computation 1: $T[0,0] = 0, T[0,1] = P, T[1,0] = 2P, T[1,1] = 3P.$
2: $Q = T[d_i, d_{i-1}]$ 3: for $i = n - 1$ down to 1 do 3.1: $Q = 4Q$ 3.2: $Q = Q + T[d_i, d_{i-1}]$ 3.3: $i = i - 2$ 4: Return Q

5. 電力解析攻撃

5.1 概要

電力解析攻撃は, サイドチャネル攻撃の一種であり, 暗号デバイスが処理する演算や内部情報と, その消費電力に相関を利用した攻撃手法である. 電力解析攻撃は大きく SPA 方式と DPA 方式に分類することができる.

† 中央大学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 Univ.
‡ 神奈川大学理学部 Faculty of Science, Kanagawa Univ.
* 中央大学理工学部情報工学科 Department of Information and Systems Engineering, School of Science and Engineering, Chuo Univ

5.2 電力解析攻撃の分類

SPA 攻撃は, 1 回の暗号化処理の消費電力を観測し得られた消費電力波形を用いる攻撃である. この攻撃手法は, 暗号デバイスの処理する命令が変化することを利用する.

DPA 攻撃は, 暗号化処理の消費電力を多数観測し, 得られた複数の消費電力波形を統計的に解析することで秘密情報を復元する.

RPA 攻撃は DPA 攻撃を応用した攻撃手法であり, ZPA はそれをさらに一般化したものである.

RPA 攻撃は, $(x, 0)$ と $(0, y)$ という 2 つの点を利用し, DPA 対策として有効なランダムな射影座標, 同型写像を用いた防御法を破ることができる.

ZPA は, 基本的な構想は RPA 攻撃と変わりはないが, $(x, 0)$ や $(0, y)$だけでなく, 楕円曲線上の加算, 2 倍算の計算途中にも 0 の値を演算させることができるため, より多くの曲線において RPA 攻撃を適用できる.

5.3 対策法

SPA 攻撃は条件分岐を使用しないことで, 命令処理の差異をなくす. これにより消費電力波形を識別不可能になり, 対策できる. DPA 攻撃の対策法は, 乱数によって演算や, 秘密鍵, 平文や点 P をランダム化することである. しかし, SPA や DPA に対する有効な防御法の一部は RPA や ZPA を防ぐことができない. これらの手法に対しては, 平文やランダムな点 R と点 P の加算による点 P のランダム化が有効である.

これらの対策を用いたアルゴリズムが H. Mamiya らにより提案されている[4]. このアルゴリズムには分岐がないため SPA 攻撃に対して安全である. さらにランダムな点 R を用いることにより, 点 P をランダム化し DPA, RPA 攻撃, ZPA に対し安全である. このランダムな点 R と window 法を用いることからこの方式は WBRIP (Window-Based Algorithm with Basic SPA-resistant algorithm with Random Initial Point) と呼ばれる. 以下 WBRIP と呼ぶ. 幅 2 に設定した WBRIP をアルゴリズム 2 WBRIP-2 に示す.

アルゴリズム 2 WBRIP-2

Input: $d = (d_{n-1}, \cdots, d_0)_2, P \in E(K)$ Output: dP
Pre-computation 1: Choose a random point $R \in E(K) \setminus O$ 2: $T[2] = R, T[1] = -R,$ $T[0,0] = -3R, T[0,1] = P - 3R,$ $T[1,0] = 2P - 3R, T[1,1] = 3P - 3R.$
3: for $i = n - 1$ down to 1 do 3.1: $T[2] = 4T[2]$ 3.2: $T[2] = T[2] + T[d_i, d_{i-1}]$ 3.3: $i = i - 2$ 4: Return $T[2] + T[1]$

6. 検証

521bit 楕円曲線暗号を対象とした本研究では, 高速な剰余算の手法である Granger-Scott 法に, 電力解析攻撃の対策を施したスカラー倍算アルゴリズムを用いた速度を検証する. 検証に用いる楕円曲線は P-521 と E-521 とする. アルゴリズムには幅 6 に設定した WBRIP を用いる. 具体的なアルゴリズムは, アルゴリズム 3 WBRIP-6 となる.

アルゴリズム 3 WBRIP-6

Input: $d = (d_{521}, \cdots, d_0)_2, P \in E(K)$ Output: dP
Pre-computation 1: Choose a random point $R \in E(K) \setminus O$ 2: $T[2] = R, T[1] = -R,$ $T[0,0,0,0,0,0] = -63R,$ $T[0,0,0,0,0,1] = P - 63R,$ $T[0,0,0,0,1,0] = 2P - 63R,$ ⋮ $T[1,1,1,1,1,1] = 63P - 63R.$
3: for $i = 521$ down to 5 do 3.1: $T[2] = 64T[2]$ 3.2: $T[2] = T[2] + T[d_i, d_{i-1}, d_{i-2}, d_{i-3}, d_{i-4}, d_{i-5}]$ 3.3: $i = i - 6$ 4: Return $T[2] + T[1]$

6.1 実装結果

比較対象として OpenSSL ver.1.0.1j を用いた. コンパイラに Gcc 4.8.2 を用いた Ubuntu 14.04 LTS, i7-4650U 1.7GHz 上で実行した結果を表 2 楕円スカラー倍算の計算量比較に示す.

表 2 楕円スカラー倍算の計算量比較

No.	手法	Clock cycle	削減量
1	OpenSSL –speed command	1,420,000	-
2	Window-6 with Granger-Scott method on P-521	838,000	40.98%
3	Window-6 with Granger-Scott method on E-521	719,000	49.36%
4	WBRIP-6 with Granger-Scott method on P-521	893,000	37.11%
5	WBRIP-6 with Granger-Scott method on E-521	751,000	47.11%

7. 結論

表 2 の No.1 と No.2 ～ No.5 を比較すると Granger- Scott 法により約 40%の clock cycle を削減できており, 高速化の効果が確認できた. 本論には比較する表を載せていないが, Granger-Scott 法の乗算と 2 乗算は Gcc4.6 より Gcc4.8.2 の方が高速であった. これは Granger-Scott 法がコンパイラの影響を受けやすく, スカラー倍算全体の clock cycle にも影響を与えていることを示している. 一方で, No.2 と No.4, No.3 と No.5 を比較するとサイドチャネル攻撃への対策は約 5% の clock cycle が増加する程度で計算時間への影響は少なく, OpenSSL より高速である. 以上より, 提案手法によって, 電力解析攻撃に安全な Granger-Scott 法が高速な暗号化処理をする可能性を示した.

参考文献

[1] US Department of Commerce/N.I.S.T.2000, “digital signature standard”, Federal Information Processing Standards Publication 186-2. Fips 186-4. (2013).
[2] H. Edwards, “A Normal Form for Elliptic Curve”, Bulletin of the American Mathematical Society, Vol.44, No.3, P393-422 (2007).
[3] D. J. Bernstein, T. Lange, “Safe Curves”, http://safecurves.cr.yp.to/
[4] R. Granger, M. Scott, “Faster ECC over $F_{2^{521}-1}$”, Cryptology ePrint Archive (2014).
[5] H. Mamiya, A. Miyaji, H. Morimoto, “Efficient Countermeasures against RPA, DPA and SPA”, CHES 2004, P343-356 (2004).