6ZA-02

Atomic blockを利用した楕円曲線暗号に対するサイドチャネル攻撃対策

竹村　友佑[†]　　伯田　恵輔[†]　　篠原　直行[‡]
国立大学法人島根大学[†]　　国立研究開発法人情報通信研究機構[‡]

1　はじめに

暗号技術は情報の保護やコンピュータセキュリティに欠かせない技術であり，特に楕円曲線暗号 (ECC) は広く使用されている．暗号の安全性を脅かす攻撃手法の一つ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を処理する機器が暗復号時に発する消費電力，処理時間などの内部動作に関わる副次的情報 (サイドチャネル情報) を観測し解析することで，機器内で処理されている暗号を解読する手がかりを得ようとする攻撃手法の総称である．現在，ECC に対する様々なサイドチャネル攻撃が提案されており，ECC を安全に運用するためにサイドチャネル攻撃への対策は重要な課題である．本稿では有限体 $\mathbb{F}_{2^n}$ 上の楕円曲線を用いた ECC に対するサイドチャネル攻撃への対策アルゴリズムを提案する．

2　楕円曲線暗号とサイドチャネル攻撃

楕円曲線暗号 (ECC) は現在広く使用されている公開鍵暗号の一つである．ECC の暗号処理時にはスカラー倍算 (ECSM) と呼ばれる計算が実行される．ECSM とは楕円曲線上の点 P に対し P の d 倍点 $[d]P$ を求める計算であり，d は秘密鍵などの秘匿されるべき情報である．サイドチャネル攻撃では $[d]P$ を計算する際の消費電力や処理時間を観測する事で d のビット値 $(d_l, ..., d_0)$ を取得する．この節では $[d]P$ の計算を説明し，サイドチャネル攻撃によって d の情報が取得されることについて述べる．

2.1　有限体 $\mathbb{F}_{2^n}$ 上の楕円曲線

ECC で利用される楕円曲線の一種である標数 2 の楕円曲線 $E/\mathbb{F}_{2^n}$ は以下の式で与えられる:

$$E/\mathbb{F}_{2^n} : y^2 + xy = x^3 + ax^2 + b.$$

ここで，$a = 0, 1$ であり，本稿では $a = 1$ の楕円曲線を扱う．また，標数 2 の楕円曲線において係数は 0 と 1 しか取り得ないという特徴があり，体 $\mathbb{F}_{2^n}$ 上の四則演算において 0 と 2 は等しいものとしてあつかう．ECSM を計算するには楕円加算 (以後，ECADD と記述) と楕円 2 倍算 (以後，ECDBL と記述) の計算を必要とする．ECADD は $E/\mathbb{F}_{2^n}$ 上の 2 点 P, Q $(P \neq Q)$ に対し $P+Q$ を求める計算であり，ECDBL は $E/\mathbb{F}_{2^n}$ 上の点 P に対し $2P$ $(= P+P)$ を求める計算である．それぞれの計算は López-Dahab (LD) 射影座標を利用して Algorithm 1,2 [2] のように求められる．ここで，楕円曲線上の点 (x, y) と一致する LD 射影座表の点は $(X : Y : Z)$ で表現され，$Z \neq 0, x = X/Z, y = X/Z^2$ である．

Algorithm 1 楕円加算 (ECADD)

Input: $P = (X_1 : Y_1 : Z_1) \in E/\mathbb{F}_{2^n}$,
$Q = (x_2, y_2) \in E/\mathbb{F}_{2^n}$.
Output: $P + Q = (X_3 : Y_3 : Z_3) \in E/\mathbb{F}_{2^n}$.

$A \leftarrow y_2 \cdot Z_1^2 + Y_1$
$B \leftarrow x_2 \cdot Z_1 + X_1$
$C \leftarrow Z_1 \cdot B$
$D \leftarrow B^2 \cdot (C + Z_1^2)$
$Z_3 \leftarrow C^2$
$E \leftarrow A \cdot C$
$X_3 \leftarrow A^2 + D + E$
$F \leftarrow X_3 + x_2 \cdot Z_3$
$G \leftarrow (x_2 + y_2) \cdot Z_3^2$
$Y_3 \leftarrow (E + Z_3) \cdot F + G$
return $(X_3 : Y_3 : Z_3)$

Algorithm 2 楕円 2 倍算 (ECDBL)

Input: $P = (X_1 : Y_1 : Z_1) \in E/\mathbb{F}_{2^n}$.
Output: $2P = (X_3 : Y_3 : Z_3) \in E/\mathbb{F}_{2^n}$.

$Z_3 \leftarrow X_1^2 \cdot Z_1^2$
$X_3 \leftarrow X_1^4 + b \cdot Z_1^4$
$Y_3 \leftarrow bZ_1^4 \cdot Z_3 + X_3 \cdot (Z_3 + Y_1^2 + bZ_1^4)$
return $(X_3 : Y_3 : Z_3)$

ECSM を計算する手法の一つに Left-to-Right アルゴリズムがある．このアルゴリズムでは，秘密情報 d の最上位 bit (d_l) から最下位 bit (d_0) まで順に確認していき，$d_i = 0$ のときは ECDBL の計算のみを行い，$d_i = 1$ のときは ECDBL と ECADD の順に計算を行い ECSM を計算する．そのため，ECSM 計算時のサイドチャネル情報から ECADD と ECDBL のどちらを実行

A side-channel atomicity for elliptic curve cyptosystems
Yusuke Takemura[†], Keisuke Hakuta[†] and Naoyuki Shinohara[‡]
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[‡]

したかが特定されると d が復元され，秘密情報 d が取得されてしまう．

3 サイドチャネル攻撃と atomic block

下記の 3 つのサイドチャネル攻撃 (SPA，HCCA，IBMA) の対策となる提案 atomic block (表 1) について説明する．

3.1 SPA への対策

Simple Power Analysis (SPA) [2] は暗号処理時の消費電力から実施された体乗算と体加算の順序を特定することによって，ECADD と ECDBL のどちらが実施されたかを決定する．Algorithm 1, 2 から分かるように ECADD と ECDBL が単純に実装されている場合，体乗算と体加算の回数と順序が異なっているため SPA 攻撃者に ECADD と ECDBL を特定されてしまう．SPA の対策として atomic block が挙げられる．Atomic block とは，デバイス内で暗号化・復号を行う際の演算の種類や順序を統一し，その統一された規則に従って構成されたアルゴリズムである．ここで，提案 atomic block (表 1) では ECADD1，ECADD2 の順に計算する事で ECADD を計算している．また，提案 atomic block (表 1) 内における '$\star$' では，atomic block で演算処理を統一するためにランダムな変数を用いて同一 step の同じ演算処理を実施する．本稿では表 1 のように各 atomic block で実施する体乗算と体加算の順序を統一するために '$\star$' を利用し，atomic block を構成した．しかし，サイドチャネル攻撃には SPA 以外に HCCA や IBMA といった攻撃手法があるため，SPA 以外のサイドチャネル攻撃にも対抗できるように atomic block (表 1) を構成した．

3.2 HCCA への対策

Horizontal Collision Correlation Attack (HCCA) [1] では暗号機器内で処理された 2 つの体乗算 ($A \times B, C \times D$) の電力波形を比較する事で，その 2 つの体乗算内において使用している非演算子 (オペランド) が同一の値 ($A = C, A = D, B = C, B = D$) であるかを特定する．本稿では 2 つの体乗算内で同一の値を持つオペランドのことを共有オペランドと呼ぶ．HCCA 攻撃者は共有オペランドの情報を基に ECADD と ECDBL の各 atomic block 内の共有オペランドの回数やタイミングの違いから ECADD と ECDBL の特定を行う．そのため，提案 atomic block (表 1) の step 8, 10 のように各 atomic block で共有オペランドのタイミングが同じになるように構成した．

表 1: 提案 atomic block

step	ECDBL	ECADD1	ECADD2
1	$T_1 \leftarrow Z_1^2$	$\star$	$T_{10} \leftarrow T_8^2$
2	$T_2 \leftarrow X_1^2$	$\star$	$\star$
3	$\star$	$\star$	$T'_{12} \leftarrow T'_4 \times T'_8$
4	$D_1 \leftarrow T_1 \times x_2$	$T_1 \leftarrow Z_1 \times x_2$	$T_{13} \leftarrow Z_3 \times x_2$
5	$\star$	$\star$	$T_{11} \leftarrow T_9 + T_{10}$
6	$\star$	$T_3 \leftarrow X_1 + T_1$	$T_{12} \leftarrow T'_{12} + R''_1$
7	$T_4 \leftarrow {T_1}^2$	$T_2 \leftarrow {Z_1}^2$	$T_{14} \leftarrow {Z_3}^2$
8	$Z_3 \leftarrow T_1 \times T_2$	$T_4 \leftarrow Z_1 \times T_3$	$D_4 \leftarrow Z_3 \times D_5$
9	$\star$	$T'_4 \leftarrow R_1 + T_4$	$X_3 \leftarrow T_{11} + T_{12}$
10	$T_3 \leftarrow {T_2}^2$	$T_7 \leftarrow {T_3}^2$	$D_7 \leftarrow {D_5}^2$
11	$T_5 \leftarrow T_4 \times b$	$D_4 \leftarrow D_3 \times b$	$D_6 \leftarrow D_6 \times b$
12	$X_3 \leftarrow T_3 + T_5$	$T_6 \leftarrow T_4 + T_2$	$T_{15} \leftarrow T_{13} + X_3$
13	$T_6 \leftarrow Y_1^2$	$Z_3 \leftarrow T_4^2$	$\star$
14	$D_2 \leftarrow D_2 \times y_2$	$T_2 \leftarrow T_2 \times y_2$	$D_7 \leftarrow D_7 \times y_2$
15	$T_7 \leftarrow T_6 + Z_3$	$T_8 \leftarrow Y_1 + T_2$	$T_{16} \leftarrow T_{12} + Z_3$
16	$T_8 \leftarrow T_7 + T_5$	$R'_1 \leftarrow T'_4 + T_8$	$T_{17} \leftarrow x_2 + y_2$
17	$T_9 \leftarrow X_3 \times T_8$	$T_9 \leftarrow T_7 \times T_6$	$T_{18} \leftarrow T_{16} \times T_{15}$
18	$T_{10} \leftarrow T_5 \times Z_3$	$R''_1 \leftarrow R_1 \times R'_1$	$T_{19} \leftarrow T_{14} \times T_{17}$
19	$Y_3 \leftarrow T_9 + T_{10}$	$T'_8 \leftarrow R_1 + T_8$	$Y_3 \leftarrow T_{18} + T_{19}$

3.3 IBMA への対策

Improving HCCA using Big-Mac Attack (IBMA) [3] は HCCA と同様，暗号機器内で処理されている体乗算間において共有オペランドが存在するかどうかを特定する．しかし，HCCA とは異なり ECSM アルゴリズム全体で変化しない固定値の共有オペランド (b, x_2, y_2) の回数やタイミングの違いから ECADD と ECDBL のどちらの処理が行われているかを特定する．そのため，提案 atomic block (表 1) の step 11 のように ECSM 全体において固定値の共有オペランドを扱う体乗算は同 step で処理されるように構成した．

4 まとめ

本稿では，標数 2 の楕円曲線を利用した楕円曲線暗号において複数のサイドチャネル攻撃に対する対策 atomic block を提示した．

参考文献

[1] A. Bauer, E. Jaulmes, E. Prouff, and J. Wild, Horizontal Collision Correlation Attack on Elliptic Curves, SAC 2013, LNCS 8282, 2014, pp.553–570.

[2] D. Hankerson, A.J. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography, Springer-Verlag , 2003.

[3] J.-L. Danger, S. Guilley, P. Hoogvorst, C. Murdica, and D. Naccache, Improving the Big Mac Attack on Elliptic Curve Cryptography, The New Codebreakers, LNCS 9100, 2016, pp.374–386.