

位数4の有理点を用いたCurve25519に対する サイドチャネル攻撃に関する考察

谷田 翔吾^{1,a)} 上竹 嘉紀¹ 小椋 央都¹ 日下 卓也¹ 籠谷 裕人¹ 野上 保之^{1,b)}

概要：IoT時代の到来に伴い、インターネットに接続する端末数が爆発的に増加することが予想されている。IoT機器のような限られた計算資源下においても、暗号技術を用いた高信頼な情報通信を実現することが要求される。楕円曲線暗号は安全かつ効率的な公開鍵暗号であり、Curve25519は利便性の高い楕円曲線として注目を集める。一方で、サイドチャネル攻撃への耐性評価も重要となる。本稿では、FPGAに実装したCurve25519に対し、位数4の有理点を利用した単純電力解析による攻撃を行った。その結果、位数4の有理点を選択暗号文として用いることで、秘密鍵の特定が可能であることがわかった。

A Consideration of Side-Channel Attacks on Curve25519 using Order 4 Rational Points

TANIDA SHOGO^{1,a)} UETAKE YOSHINORI¹ OGURA HIROTO¹ KUSAKA TAKUYA¹ KAGOTANI HIROTO¹
NOGAMI YASUYUKI^{1,b)}

Abstract: With the matter of secure communication between devices, and especially for IoT devices, more and more applications need trustful protocols to communicate using public key cryptography. Elliptic curve cryptography is nowadays a secure and efficient public key cryptography. One of the most recent and secure curves is Curve25519 and one of its failures is an attack on low-order elements during a Diffie-Hellman key exchange. This document shows that an attack using order 4 rational points is possible on an FPGA with simple power analysis, points out every IoT device using Curve25519 as a cryptographic method has a potential target to side-channel attacks.

1. はじめに

IoT時代と呼ばれ久しく、様々な「もの」がインターネットに接続され、巨大な情報網の一部を構成している。我々がそうしたサービスや製品の利便性を享受する反面、インターネットを介した通信は常に攻撃の危険に曝されている。そうした中で、通信内容の保護や認証などの機能に暗号技術が用いられており、暗号技術の重要性は益々高まりをみせている。

楕円曲線暗号は1985年にNeal Koblitz [1] と Victor S. Miller [2] によって提案された公開鍵暗号である。楕円曲

線暗号はRSA暗号 [3] に比べ、短い鍵長で同程度のセキュリティ強度を確保することができ、その計算効率の観点からも注目を集めている。2006年にDaniel J. Bernsteinによって提案されたCurve25519 [4] は、鍵共有プロトコルとしてTLS [5] によって推奨されている。この楕円曲線はその数学的構造の特徴から、安全かつ効率的な実装が可能であり [6]、計算資源の限られたIoT機器への実装にも向いている。その一方で、暗号処理中に発生する副次的な情報を利用するサイドチャネル攻撃 [7] への耐性評価が重要となる。

本研究では、組込み機器として広く使用されるFPGAにCurve25519を実装し、サイドチャネル攻撃に対する脆弱性を調査する。攻撃には選択暗号文になりうる位数4の有理点を用いられることを想定し、単純電力解析による秘密鍵の解析を行う。また、機械学習による消費電力波形の解

¹ 岡山大学自然科学研究科
Graduate School of Natural Science and Technology,
Okayama University, Japan

a) shogo.tanida@s.okayama-u.ac.jp

b) yasuyuki.nogami@okayama-u.ac.jp

析を行い、その脅威を報告する。

本稿では、まず楕円曲線暗号の数学的基礎事項とサイドチャネル攻撃について紹介する。そして評価実験の結果とそこから導かれる考察について述べる。

2. 数学的準備

本章では、楕円曲線暗号を構成する楕円曲線を主に、攻撃実験に必要な基礎事項について述べる。

2.1 楕円曲線

素体 $\mathbb{F}_p$ 上の楕円曲線 E は以下のように定義される。

$$E: y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_p$$

無限遠点と呼ばれる単位元の役割をする点を $\mathcal{O}$ とし、 $E(\mathbb{F}_p)$ を次のように定義する。

$$E(\mathbb{F}_p) \triangleq \{(x, y) | y^2 = x^3 + ax + b, x, y, a, b \in \mathbb{F}_p\} \cup \{\mathcal{O}\}$$

このとき $E(\mathbb{F}_p)$ は有理点集合と呼ばれる。さらに有理点 $P \in E(\mathbb{F}_p)$ に対し、 $[s]P$ を次のように定義する。

$$[s]P \triangleq \underbrace{P + P + P \cdots + P + P}_{s \text{ 個の } P \text{ の楕円加算}}$$

$[s]P$ を求める計算を楕円スカラー倍算と呼び、 $[r]P = \mathcal{O}$ を満たす最小の正整数 r を点 P の位数と呼ぶ。

2.2 Montgomery 曲線

$B(A^2 - 4) \not\equiv 0 \pmod{p}$ を満たす $A, B \in \mathbb{F}_p$ を用いて、以下の式を満たすものを Montgomery 曲線と呼ぶ。

$$M_{A,B}: By^2 = x^3 + Ax^2 + x$$

また、Montgomery 曲線の有理点の総数は必ず 4 の倍数とすることが知られている [8]。

2.2.1 Montgomery 曲線の特殊な加算公式

曲線上の任意の有理点 $P = (x, y)$ について、射影座標系 $(x, y) = (X/Z : Y/Z)$ を用いた場合の加算公式について考える。 $P = (X_m : Z_m)$, $Q = (X_n : Z_n)$, $R = (X_{m+n} : Z_{m+n})$ に対して、楕円加算 (Elliptic Curve Addition: ECA) $R = P + Q$ が次のように定義される [9]。

$$\begin{aligned} X_{m+n} &= Z_{m-n}[(X_m - Z_m)(X_n + Z_n) \\ &\quad + (X_m + Z_m)(X_n - Z_n)]^2 \\ Z_{m+n} &= X_{m-n}[(X_m - Z_m)(X_n + Z_n) \\ &\quad - (X_m + Z_m)(X_n - Z_n)]^2 \end{aligned} \quad (1)$$

特に $m = n$ の場合は楕円二倍算 (Elliptic Curve Doubling: ECD) と呼ばれ、次の式が得られる。

$$\begin{aligned} X_{2n} &= (X_n + Z_n)^2(X_n - Z_n)^2 \\ T &= (X_n + Z_n)^2 - (X_n - Z_n)^2 \\ Z_{2n} &= T[(X_n - Z_n)^2 + \frac{A+2}{4} \cdot T] \end{aligned} \quad (2)$$

Montgomery 曲線のスカラー倍算は、後述する Montgomery Ladder を用いる場合には Y 座標を必要としないため、他の曲線のスカラー倍算と比べて計算効率が良いとされる。

2.3 Montgomery Ladder

Montgomery Ladder [6] は、効率的にスカラー倍算の結果を求めるアルゴリズムである。Montgomery Ladder は常に ECA と ECD を繰り返すアルゴリズムであり、後述するサイドチャネル攻撃への対策として有効であるとされている [10]。以下にアルゴリズムの詳細を示す。なお、アルゴリズム中の T_1, T_2 は中間変数を表し、全演算終了後の戻り値 T_1 が最終出力となる。

Algorithm 1 Montgomery Ladder

Input: $P, s = \{s_{n-1}, s_{n-2}, \dots, s_1, s_0\}$

Output: $T_1 (= [s]P)$

```

1:  $T_1 \leftarrow \mathcal{O}$ 
2:  $T_2 \leftarrow P$ 
3: for  $i = n - 1$  to 0 do
4:   if  $s_i = 1$  then
5:      $T_1 \leftarrow \text{ECA}(T_1, T_2)$ 
6:      $T_2 \leftarrow \text{ECD}(T_2)$ 
7:   else
8:      $T_2 \leftarrow \text{ECA}(T_1, T_2)$ 
9:      $T_1 \leftarrow \text{ECD}(T_1)$ 
10:  end if
11: end for
12: return  $T_1$ 

```

本稿は、サイドチャネル攻撃への耐性を選択暗号文攻撃を用いて改めて見直すものである。

2.4 Curve25519

Curve25519 は Daniel J. Bernstein によって提案された Montgomery 曲線である [4]。この曲線は素数 $q = 2^{255} - 19$ で構成される素体 $\mathbb{F}_q$ 上に定義され、その効率性と安全性の観点から多くの注目を集めている。

$$E_{25519}: y^2 = x^3 + 486662x^2 + x$$

Curve25519 は特徴的な位数の有理点を有しており、アフィン座標系で示された $(1, \pm\sqrt{486664})$ は位数 4 の有理点であることが知られている [8]。

2.5 サイドチャネル攻撃

解読法として、従来の数学的解法の他に、暗号ハードウェアの物理的な挙動を解析することで解読する方法がある。このような攻撃はサイドチャネル攻撃 [7] と呼ばれる。一般に暗号ハードウェアとして半導体集積回路であるデジタル IC が利用される。デジタル IC で広く使用される CMOS ゲートは、p-MOS と n-MOS の 2 種類のトランジ

スタの on/off を切り替えることでデジタル値の 0 と 1 を制御する．暗号処理に伴い CMOS ゲートの状態が遷移すると，MOS トランジスタのスイッチングに伴う電流が発生し，電源電圧の変動や電磁放射を引き起こす．暗号回路では状態遷移するゲート数は平文や暗号文，秘密鍵などに依存する．つまり，暗号処理時に副次的に発生する物理現象を観測することで，秘密鍵を解析できる可能性がある．サイドチャネル攻撃は電力解析攻撃と電磁波解析攻撃に大別される．電力解析攻撃では，IC から漏洩するサイドチャネル信号として IC の電源系回路内での電圧変動を観測する．一方，電磁波解析攻撃では IC 近傍に放射される電磁界を観測する．

3. 実装

本章では，実際に安全性評価を行う際に用いた評価対象の実装方法について示す．

3.1 実装対象の性能

Curve25519 を用いた楕円曲線暗号を実装した FPGA である Altera 社製 Cyclone V Soc SX シリーズの詳細を表 1 に示す．

表 1 FPGA の仕様

Manufacturer	Intel Corporation
Device name	5CSXFC6C6U23C6N
Family	Cyclone V
Logic elements	110K logic elements
Transceiver	6(3.125 Gbps)
Package	UBGA(672 pins)
Temperature	Commercial(0..85)
Speed Grade	6(fastest)

3.2 特殊な加算公式の実装

Curve25519 の特殊な加算公式では， 256×256 bit の乗算回路や素数 $2^{255} - 19$ での剰余演算回路が必要となる．本実装では乗算回路は Karatsuba 法を用いることで， 256×256 bit の乗算を 64×64 bit の乗算に分割する．また，Karatsuba 法を適用するにあたり乗算処理を 5 clocks のパイプライン実装することで，効率的な計算を実現している．剰余演算回路では，素数 $2^{255} - 19$ が $2^{255} - 2^4 - 2^1 - 2^0$ で表現できることを用いることで，ビット連結と加算処理のみで剰余演算を実現している．実装に用いた乗算回路，剰余演算回路，加減算回路は回路面積を極力小さくするために各一つずつモジュールとして実装し，パイプライン処理のステージ数に合わせて演算スケジュールを調整することで効率的な動作を実現している．

表 2 回路規模と性能の比較

256 × 256 bit	Used	Available	Utilization
Logic utilization (in ALMs)	13,328	41,910	32 %
Total registers	12,889	83,820	15 %
Total RAM Blocks	12	553	2 %
Total DSP Blocks	100	112	89 %
Clcok Speed	20 MHz		
Calculation time	410.3 μ s		
Karatsuba	Used	Available	Utilization
Logic utilization (in ALMs)	10,431	41,910	25 %
Total registers	17,074	83,820	20 %
Total RAM Blocks	12	553	2 %
Total DSP Blocks	90	112	80 %
Clcok Speed	60 MHz		
Calculation time	167.2 μ s		

実際に乗算回路を 256×256 bit で実装したものと Karatsuba 法を用いたものとの回路規模と処理性能を比較した結果を表 2 に示す． 256×256 bit の乗算回路は 1 clock で乗算結果を出力するため，Clock Speed が Karatsuba 法と比較した際に小さくなっている．また，パイプライン処理で動作する各種演算回路を効率的に利用し，高速なスカラ倍算を実現するために，ECA や ECD の式 (1), (2) を展開した形で計算する．実際に展開した式を式 (3), (4) に示す．ただし式中における X_m, Z_m, X_n, Z_n は以下の式の a, b, c, d に対応する．

- ECA

$$\begin{aligned} X_{m+n} &= 4Z_{m-n}(a^2c^2 - 2abcd + b^2d^2) \\ Z_{m+n} &= 4X_{m-n}(a^2d^2 - 2abcd + b^2c^2) \end{aligned} \quad (3)$$

- ECD

$$\begin{aligned} X_{2m} &= a^4 - 2a^2b^2 + b^4 \\ Z_{2m} &= 4(a^3b + ha^2b^2 + ab^3) \quad (h = 486662) \end{aligned} \quad (4)$$

以上のような積和形式に変更することにより，ECA や ECD を計算する際の乗算回路や剰余演算回路の並列性を向上させることができ，結果的に高速な演算が実現できる．

3.3 Montgomery Ladder の実装

Alg. 1 で示されているように，Montgomery Ladder はスカラ値 s の 2 進数表現 s_i の値によらず，ECA と ECD を実行することにより秘密情報を抜き出す行為の対策に繋がっている．しかし， s_i の値によって ECD を計算する有理点は T_1, T_2 のいずれか一方に定まり，その時の計算量の違いから秘密鍵の情報が解析されることが懸念される．そこで本実装の Montgomery Ladder では， s_i の値に関わらず T_1, T_2 のどちらの有理点に関しても ECD を計算することで， s_i の違いによる計算量の違いをなくす工夫を施している．

4. 攻撃手法

本章では、位数 4 の有理点を用いたサイドチャネル攻撃の流れを示した後、機械学習を用いた攻撃とテンプレートマッチングを適用した攻撃の 2 種類の攻撃手法について説明する。

4.1 サイドチャネル攻撃：位数 4 の有理点

攻撃者が意図的に楕円スカラー倍算の初期点を位数 4 の有理点に置き換えて入力した場合（選択暗号文攻撃）を考える。2.4 節で示されているように、今回の実装対象である Curve25519 は位数 4 の有理点を有していることが分かっている。そこで、まず位数 4 となる有理点 P を射影座標系を用いて表現した $\bar{P}$ を定義する。

$$\bar{P} = (X = \beta : Z = \beta) \quad \beta \neq 0$$

また、 $\bar{P}$ の ECD を計算した結果は、位数 2 の有理点である $2\bar{P}$ となる。

$$2\bar{P} = (X = 0 : Z \neq 0)$$

さらに、 $3\bar{P}$ に関しては $\bar{P}$ の Y 軸反転したものになっている。しかし、Montgomery Ladder を併用した加算公式に射影座標系の Y 座標の情報を含んでいないことから、 $\bar{P}$ と同様の有理点として扱うことができる。

$$3\bar{P} = (X = \beta : Z = \beta) = \bar{P}$$

最後に、単位元の役割をする無限遠点 O を以下のように定義する。

$$O = (X \neq 0 : Z = 0)$$

これらの有理点集合の加法演算については以下の関係が成り立つ。

$$O + \bar{P} = \bar{P}, O + 2\bar{P} = 2\bar{P}$$

$$\bar{P} + \bar{P} = 2\bar{P}, \bar{P} + 2\bar{P} = \bar{P}, 2\bar{P} + 2\bar{P} = O$$

以上の関係性より、位数 4 の有理点もしくはその有理点のスカラー倍算で得られる有理点同士の加算演算の結果はすべて $\bar{P}, 2\bar{P}, O$ のいずれかになる。位数 4 の有理点 $\bar{P}$ を Montgomery Ladder の初期点 P とした際に得られる T_1, T_2 の状態遷移を図 1 に示す。Alg. 1 における T_1, T_2 は、図 1 における状態 $[T_1, T_2]$ に対応しており、矢印とそれに付随した数字は遷移の方向と s_i の値を示している。位数 4 の有理点を用いたサイドチャネル攻撃では、以上の状態遷移図の遷移時に生じる物理情報を解析することで鍵情報を解析することを目的とする。本実装の場合は s_i による計算量の違いをなくすような Montgomery Ladder を採用しているため、各状態 $[T_1, T_2]$ の遷移に焦点を当てる。図 1 中の状態 $[O, \bar{P}], [\bar{P}, 2\bar{P}], [2\bar{P}, \bar{P}], [\bar{P}, O]$ をそれぞ

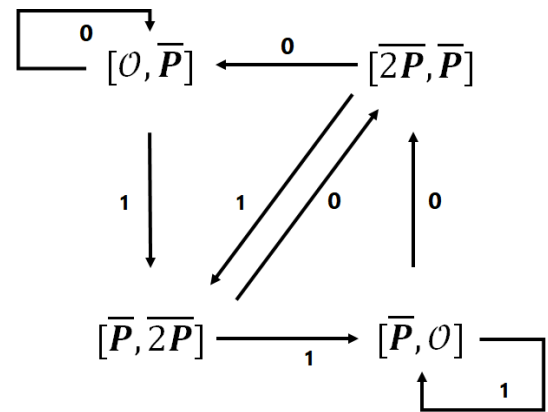


図 1 位数 4 の有理点の Montgomery Ladder 内での状態遷移図

れ State1 ~ State4 として、物理情報からこの状態遷移の変化を Montgomery Ladder の初期状態 $[O, \bar{P}]$ から追っていくことができれば、すべての s_i を状態遷移図から推定することが可能である。単純電力解析では、0 を乗ずる乗算を実行した場合の電力消費量がそれ以外の乗算を実行した場合と比較して小さくなることを用いて解析する。そこで、State1 ~ State4 の ECA と ECD の計算式中における、0 を乗ずる乗算の部分を示す。また、以下の式における a, b, c, d は式 (3), (4) の各値と対応している。

- State1
ECA や有理点 O の ECD に必要な b を含む項を計算する際に、0 を乗ずる乗算を行う。
- State2
ECA や有理点 $2\bar{P}$ の ECD に必要な c を含む項を計算する際に、0 を乗ずる乗算を行う。
- State3
ECA や有理点 $2\bar{P}$ の ECD に必要な a を含む項を計算する際に、0 を乗ずる乗算を行う。
- State4
ECA や有理点 O の ECD に必要な d を含む項を計算する際に、0 を乗ずる乗算を行う。

以上のように、 $[T_1, T_2]$ のどちらかに $O, 2\bar{P}$ を含んでいた際には、0 を乗ずる乗算を行う必要があり、それらを乗算回路で計算するタイミングに違いがあることから電力消費量が異なると考えて攻撃を行った。

4.2 機械学習を用いた攻撃

近年、サイドチャネル攻撃に対して機械学習を適用した報告が数多くされている [11]。その中で機械学習の教師あり学習における分類問題を適用させることで、秘密鍵などの秘密情報を特定する方法が研究されている。今回は様々な学習方法の中から畳み込みニューラルネットワーク (CNN) とサポートベクターマシン (SVM) を用いて解析を行った。それぞれの教師あり学習の際に用いる教師データを作成するために、既知の鍵を用いて位数 4 の有理点 $\bar{P}$

を初期点とした際に得られるスカラー倍算の電圧波形のデータを40回測定し取得した。そして、それぞれの実データをスカラー倍算のループ回数で分割し、0を乗ずる乗算を行っている箇所を抜き出し教師データとした。教師データには State1 ~ State4 のラベル付けを行い、学習させる。

4.3 テンプレートマッチングを適用した攻撃

分類問題を扱うための単純な方法の一つとしてテンプレートマッチング手法がある。今回の解析では、テンプレートデータと分類対象となるデータとの相互相関 (Cross Correlation) を計算して最も高い値をとったものを分類結果とする。テンプレートデータは、機械学習で用いた教師データと同じものを用いて作成した。

5. 評価実験

本章では、評価方法と評価に用いたパラメータを示した後、評価対象にそれぞれの攻撃を適用した際の実験結果を示す。

5.1 評価方法とパラメータ

評価対象であるFPGAの電源電圧をオシロスコープを用いて測定し、教師データを取得した後、それぞれの解析を行う。評価の際には教師データとは異なる鍵を用いて、スカラー倍算したときの電圧波形のデータを各 State に分類できるか、また、その分類結果から推測できる鍵の各ビット毎の正答率を評価する。つまり、鍵長に対してどれくらいの割合で State の分類や鍵の推定が一致しているかが分かる。教師用と評価用に用いた鍵と攻撃に用いた位数4の有理点 $\bar{P}$ は付録に示す。

5.2 実験結果

まず最初にテンプレートマッチングを適用した攻撃に用いた State1 ~ State4 のテンプレートデータを図2に示す。図2の x 軸は時間 $[\mu s]$ 、 y 軸は電圧 $[V]$ を示している。それぞれのテンプレートデータの特徴の一部として、0.35 ~ 0.40 μs 付近では、State2 と State4 の電圧が高くなっている。また、0.25 ~ 0.30 μs 付近では、State3 の電圧が高くなっている。これらの時間では、0を乗ずる乗算を行っていることが実装した際の乗算器の演算スケジュールと照らし合わせることで確認できた。図2の各 State のテンプレートデータを用いて、まず評価用の鍵でスカラー倍算を行った際の電圧波形の各ビット毎との相互相関を計算して波形データの分類を行う。そして、図1を用いて各ビット毎に鍵を推定する。その結果を表3に示す。

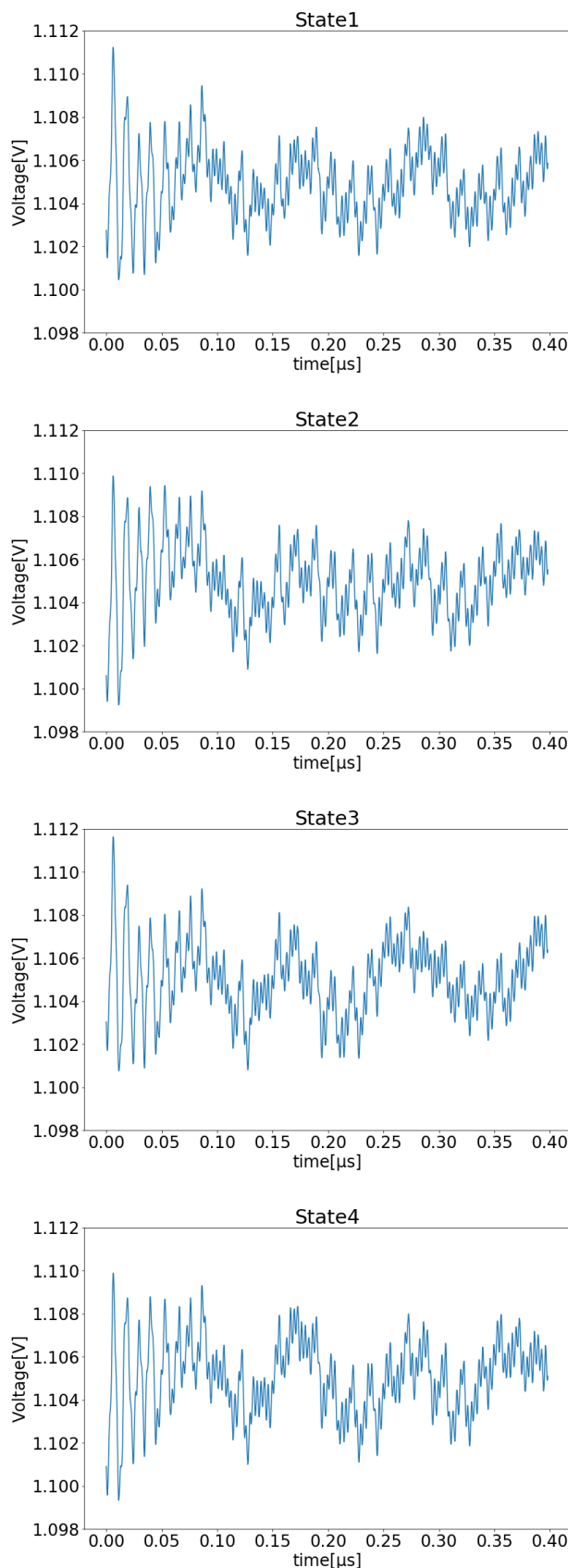


図2 テンプレートデータの電圧波形

表 3 テンプレートマッチングの結果

鍵	状態分類の正答率	鍵の正答率
key1	240/256	247/256
key2	214/256	227/256
key3	234/256	241/256
key4	200/256	222/256

また、機械学習を用いた攻撃では CNN は Keras ,SVM は scikit-learn を用いた . SVM は scikit-learn の SVC の rbf カーネルを用いて解析を行った . また , rbf のパラメータは同ライブラリ内のグリッドサーチを用いてパラメータのチューニングを行い , CNN では畳み込み層の後に全結合層をつなげた単純なネットワークで構築した . テンプレートデータを適用した攻撃と同様に正答率を表 4 に示す .

表 4 機械学習の結果

鍵	状態分類の正答率		鍵の正答率	
	CNN	SVM	CNN	SVM
key1	248/256	254/256	249/256	255/256
key2	253/256	252/256	254/256	253/256
key3	256/256	250/256	256/256	251/256
key4	246/256	244/256	250/256	248/256

6. 考察

それぞれの攻撃手法の評価結果より , 位数 4 の有理点を
用いた攻撃では電圧波形情報からスカラー倍算時の特異な状態遷移を高確率で追うことができ , その遷移パターンから鍵を推定できることを確認した . また , テンプレートマッチングを適用したものと比較して , 機械学習を用いた 2 つの手法はどちらも正答率が高いことから , サイドチャネル攻撃に機械学習を適用することの有用性と機械学習を踏まえた上での安全性評価を行うことが必要になると考えられる . また , 今回の攻撃では位数 4 という特異な有理点を対象となる暗号モジュールに暗号化させることが条件となっていることから , 鍵共有プロトコルなどの実装においては , ブラックリスト方式などを用いて対策を施す必要があると考えられる .

7. まとめ

本研究では ,FPGA に実装された Curve25519 に対して , 位数 4 の有理点を利用したサイドチャネル攻撃への安全性評価を行った . その結果 , 位数 4 の有理点が選択暗号文として利用されることで , 単純電力解析によって秘密鍵が特定される危険性があることがわかった . さらに , 秘密鍵の解読における機械学習の適用について実験を行い , その脅威を報告した . 今後の課題として , 脆弱な実装へのより詳細な理論づけを行うことやアルゴリズムレベルでの対策を導入することが挙げられる .

参考文献

- [1] Koblitz, N.: Elliptic curve cryptosystems, *Mathematics of computation*, Vol. 48, No. 177, pp. 203–209 (1987).
- [2] Miller, V. S.: Use of elliptic curves in cryptography, *Conference on the theory and application of cryptographic techniques*, Springer, pp. 417–426 (1985).
- [3] Rivest, R. L., Shamir, A. and Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, Vol. 21, No. 2, pp. 120–126 (1978).
- [4] Bernstein, D. J.: Curve25519: new Diffie-Hellman speed records, *International Workshop on Public Key Cryptography*, Springer, pp. 207–228 (2006).
- [5] P., K.: Formal request from TLS WG to CFRG for new elliptic curves (2014).
- [6] Montgomery, P. L.: Speeding the Pollard and elliptic curve methods of factorization, *Mathematics of computation*, Vol. 48, No. 177, pp. 243–264 (1987).
- [7] Peeters, E.: Advanced DPA theory and practice (2013).
- [8] Costello, C. and Smith, B.: Montgomery curves and their arithmetic: The case of large characteristic fields., *IACR Cryptology ePrint Archive*, Vol. 2017, p. 212 (2017).
- [9] Bernstein, D. J. and Lange, T.: Montgomery curves and the Montgomery ladder., *IACR Cryptology ePrint Archive*, Vol. 2017, p. 293 (2017).
- [10] : Elliptic curve point multiplication, https://en.wikipedia.org/wiki/Elliptic_curve_point_multiplication.
- [11] Hospodar, G., Gierlichs, B., De Mulder, E., Verbauwhede, I. and Vandewalle, J.: Machine learning in side-channel analysis: a first study, *Journal of Cryptographic Engineering*, Vol. 1, No. 4, p. 293 (2011).

付 録

評価実験に用いた各種パラメータを表 A.1 に示す .

表 A.1 各種パラメータ

教師用 (key0)	0x0e9e0e2aca4625731aebbb69ea37e0fa859e499b8a186ca64292c816fdeb885
評価用 (key1)	0x06f09e26afc57244bc6d7850662f668f8e4fa034037c72204612bd7b74bef738
評価用 (key2)	0x08c413fb203d5c4ebc4f2310c96093218d45ad278c02ea5a44c1a569c6854246
評価用 (key3)	0x0bba39a0cd282f2aaf509544af407ed4e22b9ef14565a37ae405082f4c52773b
評価用 (key4)	0x0d75897ac164dc421188d238e117b1ccc3b80c0ab9e374f81fab09d2a42c7f66
有理点 $\bar{P}$	($X = 1 : Z = 1$)