推薦論文

モンゴメリ型楕円曲線を用いたサイドチャネル攻撃対策法に対するAddress-bit Differential Power Analysisを用いた解析

伊藤孝一† 伊豆哲也† 武仲正彦†

本稿ではスマートカード上に実装された楕円曲線暗号に対する新しい攻撃法として，Address-bit DPAを提案する．この解析法はレジスタのアドレスの変化に着目した解析法で，もともと共通鍵暗号に対する解析法としてMesserges らによって提案されたが，データ値がランダム化されていれば防御できると考えられてきた．我々はこの攻撃法を拡張し，楕円曲線暗号においてデータがランダム化されていたとしても，スカラー倍算への適用が可能であることを示す．本稿では，モンゴメリ型楕円曲線を用いた防御法への攻撃について考察するが，我々の攻撃法は，Coron によって提案されたAdd-and-double-always 法など，他の楕円曲線暗号向けの防御法にも適用が可能である．また提案法の効果を示すため，モンゴメリ型楕円曲線を用いた防御法の1つであるOK-ECDH と OK-ECDSA に対して，提案法に基づく2種類の攻撃（SE-attack，ZE-attack）を行った解析結果を報告する．結果としてOK-ECDH と OK-ECDSA のスカラー値の判定に成功した．

Address-bit Differential Power Analysis against Side-channel Attack Countermeasure Based on the Montgomery-type Elliptic Curve

Kouichi Itoh,† Tetsuya Izu† and Masahiko Takenaka†

This paper proposes the Address-bit DPA for elliptic curve based crypto systems (ECC). This attack was orginaly proposed by Messerges et al. for common key cryptosystems, which analyzes differences of addresses of registers. However, it is thought to be of no effect if the intermediate data are randomized. We extend the attack so that it works against scalar exponentiations in ECC even if data are randomized, i.e., the implementation is resistant against the data-bit DPA. Our attack works against the side-channel attack countermeasure based on the Montgomery-type elliptic curve, but it will also work against other countermeasures, such as Add-and-double-always method proposed by Coron. We have experimented the analysis of cryptographic schemes OK-ECDH and OK-ECDSA, by two approaches (SE-attack, ZE-attack). We succeeded to reveal (a part of) secret keys by our analysis.

1. はじめに

DPA（Differential Power Analysis）は，暗号装置内を流れるデータ値と装置の消費電力との相関関係を利用する解析法で，暗号実装に対する強力な攻撃法である[15]．DPA は着目するデータの種類に応じてData-bit DPA と Address-bit DPA の2つに分類される．Data-bit DPA では，攻撃者はデータ値の差分と消費電力の差分の相関関係を利用するのに対し[4),16)]，Address-bit DPA ではレジスタのアドレス値の差分と消費電力の差分の間の相関関係を利用する[17]．従来の Address-bit DPA は Messerges らにより DES 実装に対して提案されたものであり[17]，Data-bit DPA と同程度に注意が必要である．しかしデータ値のランダム化を用いることで対策可能であったため，有効性は低いと考えられていた．本稿では Address-bit DPA を拡張し，楕円曲線暗号のスカラー倍算に対する適用法について述べる

本稿では，スカラー倍算のアルゴリズムが既知で，使用されるレジスタの個数が少ないという2つの仮定のもとで，データがランダム化されていても，Address-bit DPA が楕円曲線スカラー倍算に適用可能である

† 株式会社富士通研究所
FUJITSU LABORATORIES Ltd.

本稿の内容は 2002 年 10 月のコンピュータセキュリティシンポジウム 2002 にて報告され，CSEC 研究会前主査により情報処理学会論文誌への掲載が推薦された論文である．

ことを示す．提案する攻撃法の原理は，アドレス値の消費電力と秘密鍵の相関関係を利用したものであり，この相関関係がある暗号実装に対して有効である．サイドチャネル攻撃対策法におけるこのような実装法としては，モンゴメリ鎖[18]を用いた方法や Add-and-double-always[4]などが知られる．これらの方法は，秘密鍵の値に関係なく一定の処理を実行することで処理内容と消費電力の相関関係を利用したサイドチャネル攻撃法である SPA（Simple Power Analysis）[15]に対する防御を実現することができる．しかし，これらの方法においては，アクセスされるレジスタのアドレス値が秘密鍵のビット値に応じて決定されるため，データのランダム化のみでは十分な安全性を確保できない可能性がある．これを検証するために，本稿は，モンゴメリ鎖を用いたサイドチャネル攻撃対策法である OK-ECDH，OK-ECDSA を例にとり，Address-bit DPA を用いた攻撃法の原理と実験結果を報告する．

鍵共有スキーム OK-ECDH[20]とディジタル署名スキーム OK-ECDSA[21]は，2001 年度 CRYPTREC プロジェクト[6]に日立製作所から応募された暗号スキームである．OK-ECDH（OK-ECDSA）はモンゴメリ型楕円曲線[18]上での楕円曲線離散対数問題に基づいており，標準的な ECDH（ECDSA）[8),26)]との類似点が多い．以下では OK-ECDH と OK-ECDSA で共通に使用されるスカラー倍算部分を考察するので，これらスキームを総称して OKS（OK-Schemes）と呼ぶ．OKS の自己評価書ではサイドチャネル攻撃に対する耐性が主張されている[20),21)]が，2001 年度末に発行された暗号技術評価報告書[7]では「サイドチャネル攻撃に対する耐性は自己評価書に記載されている内容だけでは十分に確認できない」とされており，耐性評価は定まっていない☆．本稿では提案法の実効性を示すために，OKS に対する Address-bit DPA による解析結果を報告する．結果として OK-ECDH と OK-ECDSA のスカラー値の判定に成功した．なお我々の提案法は，実装アルゴリズムが既知であること，使用しているレジスタの数が少ないことが必要条件である．本稿では，OKS の一実装法として，3 変数を用いたモンゴメリ鎖を用い，かつ攻撃者はそれを知っている場合を仮定しており，提案法の必要条件を満たしているものとする．

なお，OKS の推奨アルゴリズムは 5 変数を用いているが，スマートカード等ハードウェアリソースの制約が大きい環境においては，5 変数を用いた実装法は必ずしも現実的な方法ではない．本稿では，メモリ領域を最適化した実装法の 1 つとして 3 変数の Montgomery-Ladder に基づいた OKS に対する攻撃法を考察するものであり，主張する攻撃法は，OKS の仕様書のアルゴリズムに完全に従った実装法に対するものではなく，あくまでメモリ領域を最適化した一実装法に対するものである．ただし，OKS が秘密鍵の 1 ビット値に応じてレジスタのアドレスを選択する以上，3 変数と 5 変数の実装法の間に本質的な安全性の差はなく，5 変数を用いた実装法に対しても同様の攻撃を構成可能と予想される．

本稿の構成は以下のとおりである．2 章で DPA について説明した後，3 章で Address-bit DPA を導入し，4 章で OKS に対する適用法と実験結果を報告する．なお本稿の提案法の詳細は文献 9) を参照されたい．

2. 準　　備

2.1 楕円曲線

本稿では有限体（素体）$K = GF(p)$ 上の楕円曲線を扱う．E を K 上の楕円曲線，$E(K)$ を曲線上の K-有理点集合（無限遠点 $\mathcal{O}$ を含む）とすると，点集合 $E(K)$ は加法群の構造を持つ．点の座標が与えられた場合の具体的な加法公式は教科書など（たとえば文献 3)）を参照されたい．$E(K)$ の 2 点 P_1，P_2 が与えられたとき，演算 $P_1 + P_2$ を ECADD（ただし $P_1 \neq P_2$），演算 $2 * P_1$ を ECDBL と表す．与えられた楕円曲線 $E(K)$，曲線上の点 $P \in E(K)$，整数 d に対し，演算 $d * P = P + P + \cdots + P$（$d$ 回）を P のスカラー倍算と呼び，P をベースポイント，d をスカラーと呼ぶ．スカラー倍算は ECADD と ECDBL の組合せによって計算される．d を n-bit の整数，その 2 進展開を $d = d[n-1] * 2^{n-1} + d[n-2] * 2^{n-2} + \ldots + d[1] * 2^1 + d[0]$ ($d[n-1] = 1$) とするとき，Algorithm 1 はスカラー倍算を計算するための ECADD と ECDBL の標準的な組合せ方法を示している（2 進展開法）．

```
INPUT: d, P
OUTPUT: d * P
 1: Q[0] = P
 2: for i=n-2 down to 0 {
 3:    Q[0] = ECDBL(Q[0])
 4:    if d[i]==1  Q[0] = ECADD(Q[0],P)
 5: }
 6: return Q[0]
```

Algorithm 1. 2 進展開法

☆ この背景のもと，同報告書では「電子政府での使用は薦められない」と結論づけられた（文献 7) の 2.2.1.(7) 節参照）．

2.2 サイドチャネル攻撃

Kocher らによって提案されたさサイドチャネル攻撃[14),15)]では，攻撃者は暗号装置（スマートカード）のサイドチャネル情報（消費電力）を観測し，その情報を元に装置内の秘密情報（秘密鍵）を暴こうとする．サイドチャネル情報と秘密情報の間に密接な関係が存在する場合，攻撃は有効となる．現在のところ，SPA（Simple Power Analysis）と DPA（Differential Power Analysis）がサイドチャネル攻撃の典型例として知られている．暗号を実装する場合，これらの攻撃法に対する対策を施す必要がある．

SPA は単一の処理の観測情報を利用する．Algorithm 1 で，ECADD は $d[i] = 1$ のときにだけ計算されるので，消費電力のパターンを調べることで，攻撃者は $d[i]$ の値が推測可能である．これに対し Coron は add-and-double-always method と呼ばれる防御法を提案した[4)]．この防御法では ECDBL と ECADD は $d[i]$ の値に依存せずつねに交互に計算され，サイドチャネル情報は決まったパターンを持つため，攻撃者は秘密鍵の情報を得ることが不可能となる．

デバイスの消費電力はデータ値と相関関係があるため，消費電力によるサイドチャネル情報を用いることで秘密鍵の解析が可能となる．これが DPA の基本原理である．Coron の DPA[4)] は Messerges-Dabbish-Sloan の DPA[16)] の 1 種であるので，我々は後者のみ扱う．Messerges らは攻撃者が満たす仮定に従って RSA 暗号に対する 3 種類の DPA を提案した．以下では楕円曲線暗号に適用した場合について説明する．

2.2.1 SEMD

SEMD（Single-Exponent, Multiple-Data）では，攻撃者は 1 つのスカラー d_k の値を知っており，任意のスカラーに対する消費電力のトレース（電力トレース）の測定は可能であるが，アルゴリズムは知らないことを仮定する．秘密鍵 d_u を暴こうとする攻撃者は，まず d_u を用いてランダム化された入力値の電力トレースを測定し，その平均をとる．次に d_k を用いて同じ入力値の電力トレースを測定し，その平均をとる．これらのトレースの差が 0 のとき 2 つの鍵で同じ演算が，0 でないと異なる演算が計算されていることが分かるので，デバイス内の ECADD と ECDBL の計算順序の特定が可能となる．

2.2.2 MESD

MESD（Multiple-Exponent, Single-Data）では，攻撃者は任意のスカラーの電力トレースを測定可能であるが，アルゴリズムは知らないことを仮定する．攻撃者は秘密鍵 d_u を用いてある入力値の電力トレースを測定する．もしも d_u の部分情報 $d_u[n-1], \cdots, d_u[i+1]$ を知っていれば，同じ値を入力したときの電力トレースとの差分を調べることで，$d_u[i]$ の値を推測することができる．もしも推測が正しければ，対応する差分は 0 となり，推測が正しいことが確信できる．同様の手順を繰り返すことで秘密鍵 d_u の特定が可能となる．

2.2.3 ZEMD

ZEMD（Zero-Exponent, Multiple-Data）では，攻撃者はスカラー倍算のアルゴリズム，モジュールを知っており，デバイス内の計算をシミュレート可能であることを仮定する．攻撃者はランダム化された入力値の消費電力の測定を繰り返し，各入力値に対する電力トレースをとる．次に最初のモジュールにおいて秘密鍵 d_u の部分情報 $d_u[i]$ の値を推測し，シミュレーションによって各入力値に対するモジュールの計算結果を得る．攻撃者は結果の Hamming Weight によって結果を 2 つに分類し，それぞれの平均電力トレースをとり，その差分を調べる．もしも推測が正しければ差分にスパイクが出現し，そうでなければスパイクは出現しない．同様の手順を繰り返すことで秘密鍵 d_u の特定が可能となる．

2.2.4 対　　策

スカラー倍算に Algorithm 1 を用いた場合，SEMD，MESD，ZEMD のいずれによっても解析可能である．Coron による add-and-double-always method では，ECDBL と ECADD は交互に計算されるため，電力トレースのパターンは任意の入力値に対して一定である．よって SEMD と MESD による解析は不可能である．しかしシミュレートは容易なので，ZEMD による解析は可能である．ZEMD に対する防御法として，中間値をランダム化することでシミュレーションを不可能にする方法が考えられる．たとえば Coron によるランダム化座標（Randomized Projective Coordinate, RPC）[4)] や Joye らによるランダム化曲線[13)] が提案されている．またスカラー値を乱数化させることでも防御可能である[4),5),10),16)]．

2.3 OK-ECDH および OK-ECDSA

鍵共有スキーム OK-ECDH[20)] とディジタル署名スキーム OK-ECDSA[21)] は，日立製作所によって開発された暗号スキームで，2001 年度 CRYPTREC プロジェクトに提案された．以下では OK-ECDH と OK-ECDSA で共通に使用されるスカラー倍算部分を考察するので，これらスキームを総称して OKS（OK-Schemes）と呼ぶ．OKS は楕円曲線上の離散対数問題を利用しており，標準スキーム ECDH，ECDSA[8),26)] との類似点も多い．OKS の特徴の 1 つに，モンゴメ

リ型楕円曲線 $By^2 = x^3 + Ax^2 + x \quad A, B \in GF(p)$, $B(A^2 - 4) \neq 0$ [18] を使用する点があげられる．この曲線上で y 座標を使用しない特殊な加法公式を用いた場合，高速なスカラー倍算が可能となることが知られている．OKS はこの性質を利用しており，高速な暗号演算が可能である [23),25)]．

OKS は特殊な加法公式を使用しているため，2 進展開法（Algorithm 1）の代わりにモンゴメリ鎖（Algorithm 2）を使用する．モンゴメリ鎖は ECDBL と ECADD を交互に計算するため，SPA，SEMD，MESD に対する耐性を有している [22)]．また OKS はランダム化座標を採用していることから，ZEMD に対する耐性も有している．さらに OKS の自己評価書では，秘密情報と演算の計算順序が独立であり，かつ中間値がランダム化されていれば，暗号スキームはサイドチャネル攻撃への耐性を有していることが主張されている [20),21)]．

INPUT: d, P
OUTPUT: $d * P$

```
1: Q[0] = P, Q[1] = ECDBL(P)
2: for i=n-2 to downto 0 {
3:   Q[2] = ECDBL(Q[d[i]])
4:   Q[1] = ECADD(Q[0],Q[1])
5:   Q[0] = Q[2-d[i]], Q[1] = Q[1+d[i]]
6: }
7: return Q[0]
```

Algorithm 2. モンゴメリ鎖

3. Address-bit DPA

2.2 節で紹介した Messerges らによる DPA [16)] はデータ値と電力トレースの差分との相関関係に着目していた（Data-bit DPA）．他方で彼らはレジスタのアドレス値と電力トレースの差分との相関関係に着目した別の DPA を提案した（Address-bit DPA）[17)]．この攻撃は，同じ値のデータを異なるアドレスのレジスタからロードした場合，電力消費はアドレス値に応じて変化するという事実に基づいた方法である．しかし彼らはアドレス値と電力トレースの相関関係を示す基礎実験結果と DES 実装への攻撃のアイデアを示したものの，具体的な攻撃実験結果は示していなかった．また，データのランダム化による Data-bit DPA 対策を行うことで Address-bit DPA も同時に防ぐことができることから，従来の Address-bit DPA は有効な攻撃法とは考えられていなかった．

本章では，我々は Address-bit DPA の概念を拡張し，楕円曲線暗号への適用法について述べる．提案法を用いた場合，中間値がランダム化され，Data-bit DPA に対する耐性を有していたとしても解析可能となる．

3.1 提案法の概要

従来の Address-bit DPA は同じ値のデータを異なるアドレスのレジスタからロードした場合の差分に注目した．異なる値のデータを異なるレジスタのアドレスからロードしても消費電力は変化するが，データの変化による影響を除去できれば，元の Address-bit DPA と同様な解析が可能となる．

実際，データの変化による影響は電力トレースの平均をとることで除去可能であり，平均電力トレースはレジスタのアドレス値の違いにしか影響を受けない．これが我々の提案する Address-bit DPA の原理である．提案法が攻撃に成功するのは，秘密情報とアクセスされるアドレスのレジスタの間に密接な関係が存在する場合である．一般的には使用されるレジスタは大量であるので，このアプローチは困難であるが，楕円曲線暗号の場合，使用されるレジスタは少量であり，一般的な場合よりも攻撃が容易である．

3.2 基礎実験

提案法の実効性を示すため，以下の基礎実験を行った．いま値の分からない変数 d (0 or 1) が与えられているとする．8-bit のデータが格納されている 2 つのレジスタ $Q[0]$, $Q[1]$ に対し，レジスタ $Q[d]$ からデータを $L = 500$ 回ロードすることで d の値を判定することを目的とする．ここで $Q[d]$ に格納されているデータはロードされた後にランダムな値に変化するものとする．この命令はアルゴリズムでは `A = Q[d]` と記述されるが，スマートカードのようなデバイスでは，この命令は (1) $Q[d]$ のアドレスの決定，(2) データのロード，という 2 つのステップに分割される．

我々は以下のようにして判定実験を行った．まず $d_a = 0$ の場合に L 個の電力トレースを取得する (a)．次に $d_b = d$ (b) と $d_c = 1 - d$ (c) に対して L 個のトレースを取得する．それぞれの i 番目の電力トレースを $S_{a,i}$，$S_{b,i}$，$S_{c,i}$，平均を S_a，S_b，S_c とする．このとき電力トレースの差分 D_{ab}，D_{ac} は以下で与えられる：

$$D_{ab} = \frac{1}{L}\sum_{i=1}^{L} S_{a,i} - \frac{1}{L}\sum_{i=1}^{L} S_{b,i} = S_a - S_b,$$

$$D_{ac} = \frac{1}{L}\sum_{i=1}^{L} S_{a,i} - \frac{1}{L}\sum_{i=1}^{L} S_{c,i} = S_a - S_c.$$

したがって D_{aj} にスパイクが出現すれば $d_a \neq d_j$，スパイクが出現しなければ $d_a = d_j$ となるはずであ

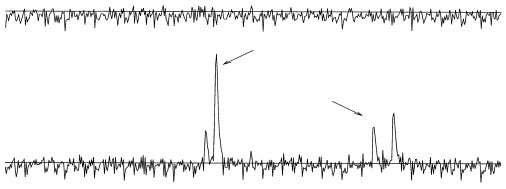

図 1 平均電力トレースの差分 D_{ab}（上段）および D_{ac}（下段）
Fig. 1 Differentials of power traces, D_{ab}(top) and D_{ac}(bottom).

る ($j \in \{b, c\}$)．このようなアプローチで実験を行った結果，得られた平均電力トレースの差分を**図 1** に示す．図 1 の上段，下段がそれぞれ D_{ab}，D_{ac} により算出した電力トレースの差分であり，D_{ac} に 2 つのスパイクが出現した（図の矢印）☆．よって $d = 0$ と解析され，実際の値と一致した．

実験では $Q[d]$ のアドレスは秘密情報 d によって決定され，アドレス値が電力トレースに影響を及ぼしている．この相関関係を利用して d の値の判定が可能となっている．以上のことから，データ値がランダム化されていても，秘密情報 d が Address-bit DPA によって特定可能であることが結論づけられる．

補足 1 (1) のスパイクはデータのロード時のものなので，Data-bit DPA からも観測可能である．この意味で Messerges らの Address-bit DPA の真のターゲットは (2) のスパイクである．

4. OKS に対する Address-bit DPA

本章では SEMD，ZEMD に基づく Address-bit DPA による OK-ECDH，OK-ECDSA の解析法について述べる．Data-bit DPA に対する耐性を目的として，OKS はランダム化座標を採用しており，入力値が同じであっても中間値はランダム化される．よって ‘Single Data’ を利用した解析は不可能であり，MESD を適用することができない．また SEMD と ZEMD を区別するうえで ‘MD’ は不要であるから，以下では単に SE，ZE と呼ぶことにする．SE-attack では，アルゴリズムが既知であることを仮定しており，元の SEMD よりも強い条件を課している．しかし OKS のアルゴリズムは既知であるから，OKS の解析のうえでは問題ない．

実装法については，OKS は次のアルゴリズムによって実装されていることを仮定する．ここで d は n-bit の秘密鍵，$d[i]$ は d の i-th bit，$Q[0]$，$Q[1]$，$Q[2]$ は中間値を格納するレジスタを表す．

```
Q[0]=P, Q[1]=ECDBL(P)
for i=n-2 to downto 0 {
  Q[2]=ECDBL(Q[d[i]]) (*11)
  Q[1]=ECADD(Q[0],Q[1])
  Q[0]=Q[2-d[i]], Q[1]=Q[1+d[i]] (*12)
}
return Q[0]
```

Algorithm 3. 実装例

実装例は (*11)，(*12) で $d[i]$ を使用するが，演算内容を変化させるためではなく，異なるレジスタからデータをロードするためである．OKS の推奨スカラー倍算アルゴリズム[20),21)] や関連論文[24)] のアルゴリズムは実装例と同等である．

我々の Address-bit DPA は中間レジスタのアドレスの変化を利用する．OKS のスカラー倍算（Algorithm 3）では，ECDBL と ECADD は交互に計算され，パターンはスカラーに依存しないが，入力値はランダム化射影座標によってランダム化されている．3 章で述べたとおり，消費電力に対するランダム化の影響は平均をとることで除去できるので，実装例の (*) 部分の平均電力トレースの差分を調べることで秘密鍵の特定が可能となる．

4.1 SE-Attack

SE-attack では，攻撃者は 1 個のスカラー d_k を知っていて，任意の入力に対する電力トレースの測定が可能であることを仮定する．さらに実装例が使用されているとする．攻撃者は d_k を用いてさまざまな値に対する電力トレースを測定し，d_k に対応する平均電力トレースを得る．$d_k[i]$ に対応する j 番目の観測の電力トレースを $S_{k,j}[i]$，平均電力トレースを $S_k[i]$ と書く．次に攻撃者は未知のスカラー d_u を用いて同じ値に対する電力トレースを測定する．$d_u[i]$ に対応する j 番目の観測の電力トレースを $S_{u,j}[i]$，平均電力トレースを $S_u[i]$ と書く．このとき差分電力トレース $D[i]$ は以下のようになる：

$$\begin{aligned} D[i] &= \frac{1}{L}\sum_{j=1}^{L} S_{k,j}[i] - \frac{1}{L}\sum_{j=1}^{L} S_{u,j}[i] \\ &= S_k[i] - S_u[i], \end{aligned}$$

ここで L は観測回数を表す．一方 OKS の実装例では，ECDBL と ECADD は d_k，d_u の値とは独立に一定のパターンで計算されるので，$S_{k,j}[i]$ と $S_{u,j}[i]$ はまったく同じ演算から生成されるシグナルとなることが期待できる．実際，$S_k[i]$，$S_u[i]$ はさまざまな値

☆ D_{ac} のはじめのスパイクは (1) のアドレス決定に，2 つ目のスパイクは (2) のロードに対応する．

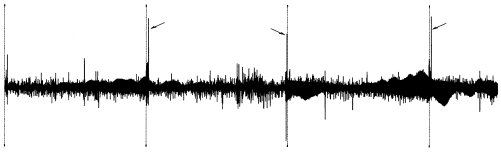

図 2 SE-attack による電力トレースの差分，左から順に $i = n-1,\ n-2,\ n-3,\ n-4$
Fig. 2 Differential of power traces in SE-attack, where leftmost section corresponds to $i = n-1$, then followed by sections corresponding to $i = n-2,\ n-3$ and $n-4$.

に対する平均電力トレースであるから，3 章で述べたとおり，データによる影響は除去できる．よって

$$D[i] \simeq \begin{cases} 0 & \text{if } d_k[i] = d_u[i] \\ \text{nonzero} & \text{if } d_k[i] \neq d_u[i] \end{cases}$$

となる．つまり差分が 0 ならば $d_k[i] = d_u[i]$ が，0 でなければ $d_k[i] \neq d_u[i]$ が判定できる．

以下に OKS に対する SE-attack の解析結果を示す．使用した曲線パラメータは次のとおりである：

$$\begin{array}{lllllll} p & = & \texttt{0x200011}, & A & = & \texttt{0x14c82a}, \\ B & = & \texttt{0x11133f}, & h & = & \texttt{0x8019d}, \\ x & = & \texttt{0x1b144d}, & y & = & \texttt{0x1aa97d}, \end{array}$$

ここで $GF(p)$ 上のモンゴメリ型楕円曲線の定義方程式は $By^2 = x^3 + Ax^2 + x$，曲線の位数は $4h$，☆ベースポイントは $P = (x, y)$ で与えられる．我々は $d_k = 1111\cdots$ を用いて実装法例によるスカラー倍算を $L = 500$ 回計算し，各計算の上位 4 ビットに対応する電力トレースを測定した．得られた電力トレースの差分を**図 2** に示す．図 2 は 4 つのセクションに分かれており，左から順に $i = n-1$，$n-2$，$n-3$，$n-4$ に対応している．$i = n-1$，$n-3$ にはスパイクが出現せず，$i = n-2$，$n-4$ にはスパイクが出現しているので，秘密鍵は $d_u = 1010\cdots$ であると解析され，実際の値と一致した．

補足 2 図 2 の $i = n-2$ では 2 つのスパイクが出現し，1 つ目は (*11) に，2 つ目は (*12) に対応している．図では $i = n-4$ の 2 つ目のスパイクは省略されている．

4.2 ZE-Attack

ZE-attack では，攻撃者はスカラー倍算のアルゴリズムが既知で，モジュールを知っており，デバイス内の計算をシミュレート可能で，任意の入力に対する電力トレースを測定可能であると仮定する．

☆ モンゴメリ型楕円曲線の位数はつねに 4 の倍数となる．

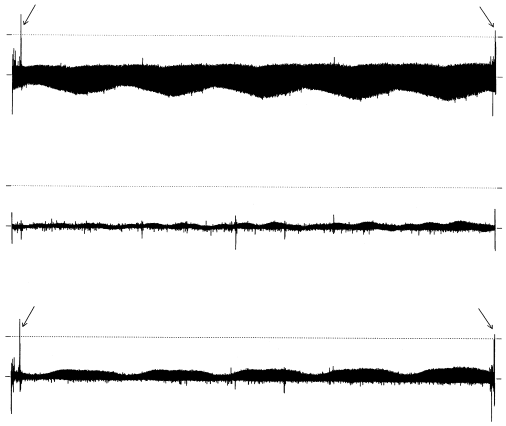

図 3 ZE-attack による電力トレースの差分，$D[0,1]$（上段），$D[0,2]$（中段）および $D[0,3]$（下段）
Fig. 3 Differentials of power traces in ZE-attack, $D[0,1]$(top), $D[0,2]$ (middle) and $D[0,3]$ (bottom).

攻撃者は未知の秘密鍵 d_u を用いてさまざまな値に対する電力トレースを測定し，その平均電力トレースをとる．次に平均電力トレースを各ビット $d_u[i]$ に対応するモジュール（ここでは ECDBL と ECADD を 1 組に考える）に分割する．OKS のスカラー倍算は ECDBL と ECADD の計算を繰り返すので，このような分割はきわめて容易である．攻撃者は平均電力トレースの差分を計算する．$d_u[i]$ に対応する j 番目の観測の電力トレースを $S_{u,j}[i]$，平均電力トレースを $S_u[i]$ と書く．このとき $d_u[a]$ と $d_u[b]$ の電力トレースの差分は以下のようになる：

$$\begin{aligned} D[a,b] &= \frac{1}{L}\sum_{j=1}^{L} S_{u,j}[a] - \frac{1}{L}\sum_{j=1}^{L} S_{u,j}[b] \\ &= S_u[a] - S_u[b], \end{aligned}$$

ここで L は観測回数を表す．一方 OKS の実装例では ECDBL と ECADD は d_u とは独立に一定のパターンで計算されるので，$S_u[a]$ と $S_u[b]$ はまったく同じ演算から生成されるシグナルとなることが期待できる．実際，$S_u[a]$, $S_u[b]$ はさまざまな値に対する平均電力トレースであるから，データによる影響は除去できる．よって

$$D[a,b] \simeq \begin{cases} 0 & \text{if } d_u[a] = d_u[b] \\ \text{nonzero} & \text{if } d_k[a] \neq d_u[b] \end{cases}$$

となる．つまり差分が 0 ならば $d_u[a] = d_u[b]$ が，0 でなければ $d_u[a] \neq d_u[b]$ が判定できる．

以下では実装例を使用した OKS に対する ZE-attack の解析結果を示す．前節の実験と同じパラメータを使用した．我々は未知の秘密鍵 d_u を用いて実装例によるス

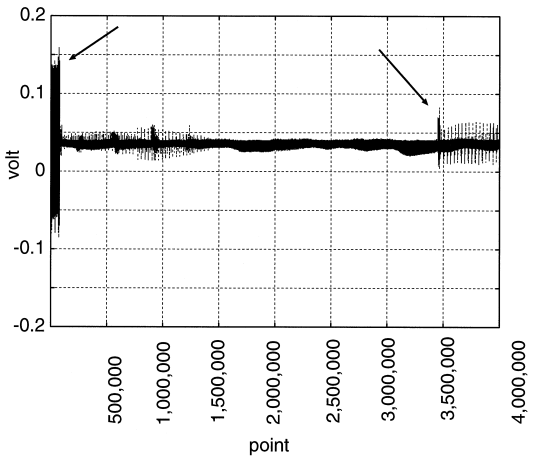

図 4 162-bit パラメータを用いた場合の電力トレースの差分 ($d_a \neq d_b$)
Fig. 4 Differentials of power traces in 162-bit parameter ($d_a \neq d_b$).

カラー倍算を $L = 500$ 回計算し，各計算の上位 3 ビットに対応する電力トレース $S_{u,j}[i]$ を測定した．そして平均電力トレース $S_u[i]$ を計算し，$S_u[0], \cdots, S_u[2]$ に分割した☆．得られた平均電力トレースの差分を**図 3** に示す．図 3 の上段，中段，下段がそれぞれ $D[0,1]$, $D[0,2]$, $D[0,3]$ を表す．$D[0,2]$ にはスパイクが出現していないのに対し，$D[0,1]$ および $D[0,3]$ にはスパイクが 2 つ出現している．これらの結果から，秘密鍵は $d_u = 1010\cdots$ であると解析され，実際の値と一致した．

補足 3 $D[0,1]$ および $D[0,3]$ にはスパイクが 2 つ出現している．SE-attack のときと同様に，1 つ目は (*11) に，2 つ目は (*12) に対応している．

4.3 現実的なパラメータを用いた実験

さらに OKS が推奨している 162-bit パラメータを用いた場合について実験を行った．使用したパラメータを以下に示す．

$$p = \texttt{0x3}, \texttt{6f378393}, \texttt{5bff79cf}, \texttt{9bccf7c9}, \texttt{483aadb8}, \texttt{73ece237}$$
$$A = \texttt{0x1}, \texttt{12cb60f5}, \texttt{b712ef06}, \texttt{f77f5e2f}, \texttt{5311e0f0}, \texttt{adad5f54}$$
$$B = \texttt{0x0}, \texttt{dbcde0e4}, \texttt{d6ffde73}, \texttt{e6f33df2}, \texttt{520eab6e}, \texttt{1cfb388e}$$

実験は SE/ZE-attack 両方の基本である，1 ビット秘密鍵 d_a, d_b を用いたスカラー倍算の電力トレースの差分をとることで行った．$d_a \neq d_b$，$L = 512$ 回について電力トレースの差分をとった結果を**図 4** に示す．

本グラフは 4,000,000 ポイントのサンプルから構成され，これらのうち 0 から 3,700,000 ポイントの範囲において，d_a, d_b を用いたスカラー倍算が実行されている．この範囲のほぼ両側（矢印が指す 0 ポイントと 3,500,000 ポイント近辺）にスパイクが出現し，実際の関係式である $d_a \neq d_b$ の手がかりを得ることに成功した．

また，スパイクが出現するタイミングの差分から得られる，d のビットあたりにかかる時間情報をもとに，測定時に収集する電力トレースの時間の範囲を変化させることで，SE/ZE-attack も同様に実現できるものと考えられる．

以上より，OKS の推奨している 162-bit 以上のパラメータについても提案する攻撃法が有効であることを実験により確認した．

4.4 実装法に関する考察

上記で述べた攻撃実験は，暗号デバイスにおけるレジスタ $Q[j]$ の実装法によって，攻撃の容易さ（スパイクの出現のしやすさ）が変化するものと考えられる．すなわち，レジスタ $Q[j]$ をソフトウェアからアクセスされるメモリとして実装するか，専用ハードウェアからアクセスされるメモリとして実装するか，専用ハードウェアからアクセスされるフリップフロップとして実装するかによって，結果は異なってくるものと考えられる．

本稿のすべての Address-bit 実験は，DPA の基本的な方法として知られるソフトウェアによるメモリアクセスを用いた環境に対する攻撃実験結果を示した．その他の環境における提案手法の有効性については，今後さらなる実験により確認する必要があると考えられるが，レジスタのアドレスにより消費電力が変化する環境においては，今回同様に実験が成功するものと考えられる．

5. 防 御 法

本章では Address-bit DPA の防御法を考察する．Address-bit DPA はアルゴリズムが使用する変数のレジスタと秘密鍵の間の相関関係を利用した攻撃法である．したがって Address-bit DPA を防ぐには，データのランダム化[4),13)] だけでは不十分であり，アドレス値をランダム化する必要がある．このような防御法として，スカラー d を $d' = d + r\phi$（r は乱数，ϕ は曲線の位数）に置き換える方法[4),16)]，d を r と $d - r$ に分割する方法[5)] などが知られているが，計算速度への影響は大きい．スカラー倍算にウィンドウ法が適用

☆ 簡単のため $0, \cdots, 3$ の場合で考えているが，これらの添え字は正確には $n-1, \cdots, n-3$ である．

できる場合には，ウィンドウをランダムに適用する方法[10] も提案されている．

以上の方法は，対策に速度劣化をともなうという欠点があるが，アドレスを直接ランダム化する方法[11] により，速度劣化をともなうことなく効率的な防御を実現する方法も提案されている．

Address-bit DPA に対する他の防御法として，レジスタのアドレスがつねに同じ Hamming Weight を持つように制御する方式が考えられる．この防御法はデバイスの消費電力が Hamming Weight Model に従うならば効果が期待できるが，Linear model や Quadratic model[1] では，Hamming Weight が同じであったとしても位置情報が特定できるため，この防御法では不十分である．

6. おわりに

本稿では楕円曲線暗号に対する Address-bit DPA による攻撃法を提案した．本攻撃法は，モンゴメリ型楕円曲線を用いたサイドチャネル攻撃対策法に対し有効であるが，そのほか Coron によって提案された Add-and-double-always 法などほかのサイドチャネル攻撃対策法[4] に対しても同様に有効であると考えられる．

また，モンゴメリ型楕円曲線を用いるサイドチャネル攻撃対策法への攻撃例として，OKS への Address-bit DPA 実験結果を報告した．結論として，スマートカード向けにメモリサイズを最適化した場合の一実装法である 3 変数を用いた OKS 実装に対して，Address-bit DPA による解析が可能であることが判明した．本稿の内容は，OKS の推奨仕様書に記載されている 5 変数アルゴリズムではなく，あくまで 3 変数を用いた実装法に対する攻撃である．ただし，5 変数のアルゴリズムも，秘密鍵の 1 ビット値に応じてアドレスを選択することに変わりはないため，5 変数と 3 変数の実装法の間に安全性に関する本質的な差はなく，提案する攻撃法は 5 変数の実装法に対しても拡張可能と考えられる．

OK-ECDH，OK-ECDSA では，モンゴメリ型楕円曲線のサイドチャネル攻撃耐性の主たる根拠としてモンゴメリ鎖（Algorithm 2）と点の表現のランダム化があげられている．しかしモンゴメリ鎖は標準的なワイヤシュトラス型楕円曲線にも適用可能であること[2),12)]，ワイヤシュトラス型楕円曲線でも点のランダム化が可能なこと，さらにはスキーム自体が ECDH，ECDSA との類似点を多く持つことから，仕様書が主張するような従来法に対するサイドチャネル攻撃耐性の優位性は低いと考えられる．

（提案法を含め）サイドチャネル攻撃は暗号実装に対する攻撃である．したがって，OK-ECDH，OK-ECDSA 以外についても，暗号スキームがサイドチャネル攻撃への耐性を保証したり，異なるスキーム間の安全性の差異を議論したりするのは，非常に困難がともなうと考えられる．これは，暗号学的な強度（理論による安全性検証）と実装攻撃の強度（理論を具体的にどのように実装するかによって，安全性が変化する場合がある）は異なることによるものである．たとえば文献 5) ではサイドチャネル攻撃に対する安全性の議論を試みているが，その議論は非常に抽象的なものであり，現実の暗号デバイスの安全性を保証するにはまた改良の余地を残しているものと思われれる．

参 考 文 献

1) Akkar, M., Dischamp, P. and Moyart, D.: Power Analysis, What is Now Possible..., *Asiacrypt 2000*, LNCS 1976, pp.489–502, Springer-Verlag (2000).
2) Brier, E. and Joye, M.: Weierstraß Elliptic Curves and Side-Channel Attacks, *PKC 2002*, LNCS 2274, pp.335–345, Springer-Verlag (2002).
3) Blake, I., Seroussi, G. and Smart, N.: *Elliptic Curves in Cryptography*, Cambridge University Press (1999).
4) Coron, J.: Resistance against differential power analysis for elliptic curve cryptosystem, *CHES'99*, LNCS 1717, pp.292–302, Springer-Verlag (1999).
5) Clavier, C. and Joye, M.: Universal exponentiation algorithm, *CHES 2001*, LNCS 2162, pp.300–308, Springer-Verlag (2001).
6) 暗号技術評価プロジェクト（CRYPTREC）. http://www.ipa.go.jp/security/enc/CRYPTREC/index.html
7) 暗号技術評価報告書（2001 年度版），情報処理振興事業協会，通信・放送機構 (Mar. 2001).
8) IEEE P1363, Standard Specifications for Public-Key Cryptography (2000).
9) Itoh, K., Izu, T. and Takenaka, M.: Address-bit Differential Power Analysis of Cryptographic Schemes OK-ECDH and OK-ECDSA, *CHES 2002*, LNCS 2523, pp.129–143, Springer-Verlag (2002).
10) Itoh, K., Yajima, J., Takenaka, M. and Torii, N.: DPA countermeasure by improving the window method, *CHES 2002*, LNCS 2523, pp.303–317, Springer-Verlag (2002).
11) Itoh, K., Izu, T. and Takenaka, M.: A Prac-

tical Countermeasure against Address-bit Differential Power Analysis, *CHES 2003*, LNCS 2779, pp.382–396, Springer-Verlag (2003).
12) Izu, T. and Takagi, T.: A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks, *PKC'02*, LNCS 2274, pp.280–296, Springer-Verlag (2002).
13) Joye, M. and Tymen, C.: Protections against differential analysis for elliptic curve cryptography, *CHES 2001*, LNCS 2162, pp.377–390, Springer-Verlag (2001).
14) Kocher, C.: Timing attacks on Implementations of Diffie-Hellman, RSA, DSS and other systems, *Crypto'96*, LNCS 1109, pp.104–113, Springer-Verlag (1996).
15) Kocher, C., Jaffe, J. and Jun, B.: Differential power analysis, *Crypto'99*, LNCS 1666, pp.388–397, Springer-Verlag (1999).
16) Messerges, T.S., Dabbish, E.A. and Sloan, R.H.: Power Analysis Attacks of Modular Exponentiation in Smartcards, *CHES'99*, LNCS 1717, pp.144–157, Springer (1999).
17) Messerges, T.S., Dabbish, E.A. and Sloan, R.H.: Investigations of Power Analysis Attacks on Smartcards, *USENIX Workshop on Smartcard Technology* (1999).
18) Montgomery, P.: Speeding the Pollard and elliptic curve methods for factorizations, *Math. of Comp.*, Vol.48, pp.243–264 (1987).
19) National Institute of Standards and Technology: Recommended Elliptic Curves for Federal Government Use, in the appendix of FIPS 186-2.
20) 鍵交換スキーム OK-ECDH，日立製作所 (2001). http://www.sdl.hitachi.co.jp/crypto/ok-ecdh/
21) ディジタル署名スキーム OK-ECDSA，日立製作所 (2001). http://www.sdl.hitachi.co.jp/crypto/ok-ecdsa/
22) Okeya, K., Kurumatani, H. and Sakurai, K.: Elliptic curves with the Montgomery form and their cryptographic applications, *PKC 2000*, LNCS 1751, pp.446–465, Springer-Verlag (2000).
23) Okeya, K., Miyazaki, K. and Sakurai, K.: A fast scalar multiplication method with randomized projective coordinates on a Montgomery-form elliptic curve secure against side channel attacks, *ICISC 2001*, LNCS 2288, pp.428–439, Springer-Verlag (2001).
24) Okeya, K. and Sakurai, K.: Power analysis breaks elliptic curve cryptosystem even secure against the timing attack, *Indocrypt 2000*, LNCS 1977, pp.178–190, Springer-Verlag (2000).
25) Okeya, K. and Sakurai, K.: Efficient elliptic curve cryptosystem from a scalar multiplication algorithm with recovery of the y-coordinate on a Montgomery-form elliptic curve, *CHES 2001*, LNCS 2162, pp.126–141, Springer-Verlag (2001).
26) Standards for Efficient Cryptography Group (SECG), Specification of Standards for Efficient Cryptography. http://www.secg.org/

(平成 15 年 5 月 9 日受付)
(平成 16 年 5 月 11 日採録)

推 薦 文

スマートカードに実装された楕円曲線暗号に対し，新しい実装攻撃を提案している．実際に実験結果を示し，そのような実装状況では，提案した攻撃に対する配慮が必要なことを示している．攻撃方法に新規性と有効性があり．注目度も高い．以上のように工学的に有意な結果が示されておりしかも情報セキュリティの分野に貢献するところ少なくないと考え，論文に推薦したい．

（CSEC 研究会前主査 岡本栄司）

伊藤 孝一

昭和 46 年生．平成 7 年東京工業大学工学部情報工学科卒業．平成 9 年北陸先端科学技術大学院大学情報科学研究科博士前期課程修了．同年（株）富士通研究所入社．公開鍵，共通鍵の実装技術，サイドチャネル攻撃の研究に従事．平成 14 年暗号と情報セキュリティシンポジウム（SCIS 2002）論文賞，平成 14 年コンピュータセキュリティシンポジウム（CSS 2002）優秀論文賞．電子情報通信学会会員．

伊豆　哲也（正会員）

昭和 42 年生．平成 4 年東京大学理学部数学科卒業．平成 6 年立教大学大学院理学研究科博士前期課程修了．平成 9 年立教大学大学院理学研究科博士後期課程退学．同年（株）富士通研究所入社．平成 13 年 Waterloo 大学（カナダ）客員研究員．公開鍵暗号に関する実装・安全性評価等の研究に従事．平成 11 年暗号と情報セキュリティシンポジウム（SCIS 1999）論文賞，平成 14 年コンピュータセキュリティシンポジウム（CSS 2002）優秀論文賞．応用数理学会，国際暗号研究学会（IACR）各会員．

武仲　正彦

昭和 42 年生．平成 2 年大阪大学工学部電気工学科卒業．平成 4 年大阪大学大学院工学研究科電気公害専攻博士前期課程修了．同年（株）富士通研究所入社．公開鍵，共通鍵の実装技術，共通鍵暗号攻撃，サイドチャネル攻撃，ネットワークセキュリティの研究に従事．平成 14 年コンピュータセキュリティシンポジウム（CSS 2002）優秀論文賞．