サイドチャネル攻撃を防ぐモンゴメリ型楕円曲線上の高速なスカラー倍計算方法——理論的アプローチ

桶 屋 勝 幸[†] 宮 崎 邦 彦[†] 櫻 井 幸 一[††]

我々は，モンゴメリ型楕円曲線におけるスカラー倍計算において，計算量が増大しないランダム化射影座標を提案する．ランダム化射影座標は楕円曲線暗号に対するサイドチャネル攻撃を防ぐための一手法である．これは，座標表現をランダム化することにより，特定の数値の出現を攻撃者に対して予測不能とする防御方法である．しかしながら従来法では，座標表現のランダム化により射影座標の1つである Z 座標の値を1とすることができず，そのため Z 座標との乗算が発生し計算量が増大していた．また，モンゴメリ型楕円曲線における元々のスカラー倍計算法では，Z 座標が1であるため高速計算可能であるが，サイドチャネル攻撃に対して脆弱である．提案法では，楕円曲線上の1つの点に対し，座標表現をランダム化した点とランダム化していない点という2つの表し方を用いることにより，サイドチャネル攻撃への耐性と高速性を達成している．また，提案法に対する厳密な耐性解析を行い，耐性を有することを示す．提案法のスカラー倍計算方法により，サイドチャネル攻撃の脅威にさらされるスマートカード等への実装に関する，モンゴメリ型楕円曲線の優位性を明らかにする．

An Efficient Countermeasure to Side Channel Attacks on ECC Using Randomized Projective Coordinates —— A Theoretical Approach

Katsuyuki Okeya,[†] Kunihiko Miyazaki[†] and Kouichi Sakurai[††]

In this paper, we propose a scalar multiplication method that does not incur a higher computational cost for randomized projective coordinates of the Montgomery form of elliptic curve. A randomized projective coordinates method is a countermeasure against side channel attacks on an elliptic curve cryptosystem in which an attacker cannot predict the appearence of a specific value because the coordinates have been randomized. However, because of this randomization, we cannot assume a projective coordinate, namely the Z-coordinate, to be 1. Thus, the computational cost increases by multiplications of Z-coordinates, 10%. On the other hand, the original scalar multiplication method on the Montgomery form is computable quickly, because of the Z-coordinate to be 1. However, it is vulnerable to side channel attacks. In the proposed method, for a point on the elliptic curve, we use its expression of coordinates in two ways, that is, the point with/without a randomized expression. As it turned out, the proposed method is immune to side channel attacks and computable quickly. Our results clarify the advantage of cryptographic usage of the Montgomery-form elliptic curves in constrained environments such as mobile devices and smart cards.

1. はじめに

ランダム化射影座標（*randomized projective coordinates*）は，**サイドチャネル攻撃**（*side channel attacks*）に対する防御法として有効な方法の1つであるが，計算量の増大という問題を引き起こす．本論文では，計算量の増大をともなわないランダム化射影座標を提案し，サイドチャネル攻撃を防ぎかつ高速なスカラー倍計算方法を構成する．

1.1 サイドチャネル攻撃とランダム化射影座標

Kocher らは，暗号処理を行う際に漏洩するデータから秘密情報を推定するサイドチャネル攻撃[10)~13)]を提案した．そして Coron は，楕円曲線暗号にサイドチャネル攻撃[5)]を拡張し，その防御法としてランダム化射影座標を提案した．一方で桶屋–櫻井は，ランダム化射影座標はサイドチャネル攻撃を防ぐために有効[19)]であることを示している．

1.2 モンゴメリ型楕円曲線

楕円曲線暗号（*an elliptic curve cryptosys-*

† 株式会社日立製作所システム開発研究所
Systems Development Laboratory, Hitachi, Ltd.
†† 九州大学システム情報科学研究院
Graduate School of Information Science and Electrical Engineering, Kyushu University

tem）[9),16)] に通常用いられているワイエルシュトラス型楕円曲線と呼ばれる楕円曲線は，$E : y^2 = x^3+ax+b$ により与えられる．Montgomery は，別の標準形の楕円曲線[17)] $E^M : By^2 = x^3 + Ax^2 + x$ を導入した．桶屋–櫻井は，この**モンゴメリ型楕円曲線**（***a Montgomery-form elliptic curve***）と呼ばれる楕円曲線において，ランダム化射影座標を用いて，サイドチャネル攻撃を防ぐ高速なスカラー倍計算方法[19)] を提案した．これは，楕円曲線上の入力される点 P の射影座標の値をランダム化することにより，サイドチャネル攻撃を防いでいる．しかしながら，点 P をランダム化した結果，その Z 座標は 1 ではなくなり，そのためモンゴメリ型楕円曲線における元々のスカラー倍計算方法と比べて計算量が増大している．他方，モンゴメリ型楕円曲線における元々のスカラー倍計算方法は，点 P の Z 座標を 1 ととっているため，高速演算が可能である．しかしながら，点 P をランダム化をしていないため，サイドチャネル攻撃に対して脆弱である．

1.3　本研究の成果

本論文では，サイドチャネル攻撃への耐性と高速性を有するスカラー倍計算方法を提案する．そのために，点 P という 1 つのものに対して，ランダム化した点 P と，ランダム化していない点 P という 2 通りの表し方を用いる．また，提案アルゴリズムの，サイドチャネル攻撃への耐性に対する厳密な解析を行い，その耐性を証明する．

モンゴメリ型楕円曲線におけるランダム化射影座標を用いたスカラー倍計算法は，ワイエルシュトラス型楕円曲線といった他の型の楕円曲線や，Jacobian 座標といった他の座標系に対しても適応できる．モンゴメリ型楕円曲線におけるスカラー倍計算法は，SPA（Simple Power Analysis）攻撃を防ぎ，そのうえ，他の耐 SPA スカラー倍計算法と比べてかなり高速である．

我々の試算によれば，160 ビットでの提案法のスカラー倍計算法の計算量は乗算 1468.4 回であり，モンゴメリ型楕円曲線におけるランダム化射影座標を用いた従来のスカラー倍計算法の計算量は乗算 1627.4 回であるので，約 10%高速である．また，ランダム化射影座標を用いないスカラー倍計算法の計算量は乗算 1467.4 回であるので，同程度の計算量である．ワイエルシュトラス型楕円曲線でウィンドウ法を用いたスカラー倍計算法の計算量は乗算 1565.74 回であるので，提案法が 6%以上高速である．また，ウィンドウ法はサイドチャネル攻撃に対して脆弱である．

以下，2 章でサイドチャネル攻撃とランダム化射影座標に関するサーベイを与える．3 章でモンゴメリ型楕円曲線における既存のランダム化射影座標を用いたスカラー倍計算方法を復習する．4 章で提案法のランダム化射影座標を説明し，サイドチャネル攻撃に関する安全性および計算量に関して検討する．

2.　サイドチャネル攻撃とランダム化射影座標

2.1　サイドチャネル攻撃

実際の環境下での暗号装置においては，暗号処理を実行する際に，入力データおよび出力データ以外にも漏洩するデータが存在する．たとえば，暗号処理にかかる計算時間であったり，スマートカードであれば電力は外部より供給されるので，電力消費量もその類のデータである．Kocher らは，それらの漏洩データより，暗号装置内部に格納されている秘密情報を推定する攻撃法，いわゆるサイドチャネル攻撃[10)~13)] を開発した．サイドチャネル攻撃には，タイミング攻撃[10),11)] や SPA 攻撃[10),11)]，DPA（Differential Power Analysis）攻撃[12),13)] がある．スマートカードは，サイドチャネル攻撃の影響を特に受けやすい暗号装置である．

タイミング攻撃[10),11)] はサイドチャネル攻撃の一種であり，漏洩情報として計算時間を用いて秘密情報を推定する攻撃である．秘密情報を推定する際に，統計的手法を用いるものもあるし，一度の計算により推定する方法もある．SPA 攻撃[10),11)] はサイドチャネル攻撃の一種であり，漏洩情報として電力消費量を用いる．その際，電力消費量の波形を直接観測することにより秘密情報を推定する．DPA 攻撃[12),13)] はサイドチャネル攻撃の一種であり，漏洩情報として電力消費量を用いる．その際，統計的処理を行うことにより秘密情報を推定する．DPA 攻撃はサイドチャネル攻撃の中でも最も強力な攻撃法である．

Kocher らが提案した攻撃は，その攻撃対象は主として DES[6)] や RSA[21)] であり，楕円曲線暗号に対する攻撃は知られていなかった．Coron は，DPA 攻撃を楕円曲線暗号[5)] へと拡張した．

Coron は次の耐 SPA スカラー倍計算法に対して，DPA 攻撃を構成している．

アルゴリズム：Coron の耐 SPA スカラー倍計算法
入力　スカラー値 d，点 P
出力　スカラー倍 dP
(1)　$Q[0] \leftarrow P$
(2)　For i from $|d| - 2$ to 0 do the following:
　(2.1)　$Q[0] \leftarrow 2Q[0]$
　(2.2)　$Q[1] \leftarrow Q[0] + P$
　(2.3)　$Q[0] \leftarrow Q[d_i]$

(3)　$Q[0]$ を dP として出力する．

ここで，$|d|$ は d のビット長を表し，d_i は d の i 番目のビットを表す．すなわち，$d = \sum_{i=0}^{|d|-1} d_i 2^i, d_i \in \{0,1\}$ である．

攻撃者は，まずビット $d_{|d|-2}$ を暴こうとする．攻撃者はとりあえず $d_{|d|-2} = 0$ と仮定する．攻撃者は与えられた P に対し，$4P$ を計算できるので，$4P$ の特定のビットの値を予測できる．そして，n 個の点 P_j $(j = 1, 2, \cdots, n)$ を，$4P_j$ の特定のビットの値により，2 つのクラスに分類する．次に，点 P_j を入力した際の電力消費量を測定し，各々のクラスの平均電力消費量を計算し，それら平均電力消費量の差分の値を計算する．もし，その差分の波形にスパイクが出現したとすると，攻撃者の仮定は正しかったことになり，$d_{|d|-2} = 0$ である．もし，その差分の波形が平坦であれば，攻撃者の仮定は間違っていたことになり，$d_{|d|-2} = 1$ である．なぜならば，もし $d_{|d|-2} = 0$ であれば，2 回目の繰返しのステップ 2.1 で $4P$ が計算され，電力消費量は特定のビットの値と相関関係☆がある．もし，$d_{|d|-2} = 1$ であれば，$4P$ が計算されないので，そのような相関関係はない．同様にして，攻撃者はスカラー値 d の残りのビットを特定する．

2.2　ランダム化射影座標

Coron は，DPA 攻撃を楕円曲線暗号に拡張するとともに，その防御法[5] についても提案している．そのうちの 1 つにランダム化射影座標がある．ランダム化射影座標は，楕円曲線上の点を射影座標で表現する際に，乱数により各座標を乗じた座標である．すなわち，楕円曲線上のスカラー倍演算等を行う際に，乱数 r を生成し，楕円曲線上の点 $P = (x, y)$ を射影座標において (rx, ry, r) と表現する．射影座標においては，任意の $r \neq 0$ に対して $(X, Y, Z) = (rX, rY, rZ)$ が成り立つため，(rx, ry, r) は点 P と同じ点を表している．

桶屋–櫻井は，サイドチャネル攻撃を防ぐための要件[19] を提案している．それによると要件は 2 つあり，1 つは秘密情報と計算実行手順とが独立であること，もう 1 つは計算対象の値をランダム化することである．1 つ目の要件は SPA 攻撃を防ぐことと同等である．そしてランダム化射影座標により，2 つ目の要件である計算対象の値のランダム化を達成することができる．

☆ 一般的に，コンデンサに電気を蓄えた状態が 1 を表し，放電した状態が 0 を表す．$4P$ を計算するときの処理で，片方のクラスは特定ビットを 1 にセットし，もう片方は 0 にセットする．したがって，1 をセットするクラスは電力を蓄え，0 をセットするクラスは電力を放電するので，各クラスの電力消費量の平均を比較すると違いが生じる．

2.3　DPA 攻撃の特徴に関する考察

Coron の DPA 攻撃[5] を考慮に入れると，DPA 攻撃が成立するための仮定は 3 つあると考えられる．

(i) 楕円曲線上のある点が計算途中で（タイミングも含めて）出現するか否かにより，スカラー値の（部分）情報を攻撃者が引き出すことができる．また，そのような点が存在する（そのような点のことを判別点と呼ぶことにする）．

(ii) 判別点の座標の値が，攻撃者にとって計算可能である，もしくは有為な確率により，推定可能である．

(iii) サイドチャネル情報を用いて，判別点が出現したかどうかを，攻撃者が判定できる．

この 3 つすべてがみたされているとすると，攻撃者は DPA 攻撃を成功させることができる．

(1) 攻撃者は，入力する点の集合を，判別点☆☆の座標の値により，2 つのクラスに分類☆☆☆する（(i) よりそのような点が存在し，(ii) より攻撃者が実行可能）．

(2) 攻撃者は，サイドチャネル情報を収集し，判別点が出現したか否かを判定する（(iii) より攻撃者が実行可能）．

(3) 攻撃者は判別点が出現したか否かが分かるので，スカラー値の部分情報を特定できる（(i) より攻撃者が実行可能）．

したがって DPA 攻撃を防ぐには，(i)〜(iii) のいずれかの仮定の成立を阻止する必要がある．(i) を回避するには，秘密情報（スカラー値）にまったく依存しないアルゴリズムが必要となるため，そのようなアルゴリズムの構成は困難と考えられる．(iii) は暗号アルゴリズムの実装環境に依存すると考えられるが，実際に電力消費量が，格納されているデータのハミングウェイトに依存するとの報告例[2] もあり，成立すると考えられる．ランダム化射影座標[5),19] は，(ii) を回避する方法と考えられる．すなわち，攻撃者は入力点の分類ができない，ということである．本論文では，サイドチャネル攻撃（DPA 攻撃）を防ぐために，ランダム化射影座標を用いて (ii) の成立の阻止を目指す．

3.　モンゴメリ型楕円曲線

3.1　モンゴメリ型楕円曲線の定義

$p (\geq 3)$ を素数とし，$\mathbf{F}_{p^n}$ を標数 p の有限体とする．

☆☆ 判別点は入力する点に依存して決まる．

☆☆☆ Coron の DPA 攻撃では，$4P$ が判別点となっている．

$\mathbf{F}_{p^n}$ 上のモンゴメリ型楕円曲線は次のように定義される．

$$E^M : By^2 = x^3 + Ax^2 + x$$

ここで $A, B \in \mathbf{F}_{p^n}$ および $B(A^2-4) \neq 0$ である．

次にモンゴメリ型楕円曲線における演算公式について説明する．E^M 上の点 P に対し，k 倍した点を kP とし，$mP = (X_m, Y_m, Z_m)$，$nP = (X_n, Y_n, Z_n)$，$(m-n)P = (X_{m-n}, Y_{m-n}, Z_{m-n})$ と射影座標で表す．そのとき Y 座標なしの $(m+n)P = mP + nP$ は，差分点 $(m-n)P$ を用いて次のように計算される[17)]．

加算公式 $(m \neq n)$

$$X_{m+n} = Z_{m-n}[(X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n)]^2$$

$$Z_{m+n} = X_{m-n}[(X_m - Z_m)(X_n + Z_n) - (X_m + Z_m)(X_n - Z_n)]^2$$

2 倍公式 $(m = n)$

$$4X_nZ_n = (X_n + Z_n)^2 - (X_n - Z_n)^2$$

$$X_{2n} = (X_n + Z_n)^2(X_n - Z_n)^2$$

$$Z_{2n} = (4X_nZ_n)((X_n - Z_n)^2 + ((A+2)/4)(4X_nZ_n))$$

すなわち，X_{m+n}/Z_{m+n} および X_{2n}/Z_{2n} は，それぞれ $(m+n)P$ および $2nP$ のアフィン座標における x 座標となる．M および S を，それぞれ $\mathbf{F}_{p^n}$ 上の乗算および 2 乗算の計算量を表すとする．そうすると，上記加算公式は $4M + 2S$，2 倍公式は $3M + 2S$ の計算量が必要となる．加算公式において，差分点の Z 座標 $Z_{m-n} = 1$ を仮定することができれば，その計算量は $3M + 2S$ となる．

3.2 スカラー倍計算方法

まず，モンゴメリ型楕円曲線におけるスカラー倍計算アルゴリズム[17)]について説明する．この計算方法は高速計算可能であるが，サイドチャネル攻撃に対して脆弱である．

アルゴリズム 1

入力 スカラー値 d☆，点 $P = (x, y)$ の x 座標

出力 スカラー倍 dP の X 座標および Z 座標

(1) $i \leftarrow |d| - 1$

(2) 2 倍公式を用いて，点 P より点 $2P$ を計算する．このとき点 P を射影座標で $P = (x, y, 1)$ と表して用いる．

(3) $m \leftarrow 1$

(4) $i = 0$ のときステップ (13) へ，そうでなければステップ (5) へ．

(5) $i \leftarrow i - 1$

(6) $d_i = 0$ のときステップ (7) へ，そうでなければステップ (10) へ．

(7) 加算公式を用いて，点 mP，点 $(m+1)P$ および点 P より，点 $(2m+1)P$ を計算する．

(8) 2 倍公式を用いて，点 mP より点 $2mP$ を計算する．

(9) $m \leftarrow 2m$ として，ステップ (4) へ．

(10) 加算公式を用いて，点 mP，点 $(m+1)P$ および点 P より，点 $(2m+1)P$ を計算する．

(11) 2 倍公式を用いて，点 $(m+1)P$ より点 $(2m+2)P$ を計算する．

(12) $m \leftarrow 2m+1$ として，ステップ (4) へ．

(13) 点 mP の X 座標および Z 座標をスカラー倍 dP の X 座標および Z 座標として出力する．

このアルゴリズムは，ステップ (7) およびステップ (10) の加算演算において，差分点 P の Z 座標が 1 であるので，この加算の計算量は $3M + 2S$ である．したがって全体の計算量は $(6|d| - 3)M + (4|d| - 2)S$ となる．

このアルゴリズムはスカラー倍点 dP の Y 座標を計算しない．しかしながら，モンゴメリ型楕円曲線における y 座標復元方法[20)]を用いることにより，Y 座標を容易に計算することができることを注意しておく．この y 座標復元方法は，dP の Y 座標を，dP，$(d+1)P$ の X，Z 座標および点 P から計算する☆☆．y 座標復元の計算量は $12M + S$ である．

3.3 ランダム化射影座標を用いたスカラー倍計算方法

次に，モンゴメリ型楕円曲線における，ランダム化射影座標を用いたスカラー倍計算アルゴリズム[19)]について説明する☆☆☆．この計算方法はサイドチャネル攻撃に対して耐性を有するが，高速計算ができない，という問題点がある．

アルゴリズム 2

入力 スカラー値 d，点 $P = (x, y)$ の x 座標

☆ 点 P の位数を k とすると，$d \leq k-2$ を仮定する．無限遠点を $\mathcal{O}$ とすると，$kP = \mathcal{O}$ となるので，$d \geq k$ のときは，$d \pmod k$ をあらためて d とすればよい．$d = k-1$ のときは，$(d+1)P (= \mathcal{O})$ を計算できないため，この場合を除く．またこの場合，P と dP の x 座標が一致するため，暗号利用の観点からは，$d = k-1$ とするのは好ましくない．

☆☆ ステップ (13) では点 dP の X 座標，Z 座標とともに，点 $(d+1)P$ の X 座標，Z 座標も求まっているため，y 座標復元方法を適用することができる．

☆☆☆ このアルゴリズムも，スカラー倍点 dP の Y 座標を計算しない．しかしながら，モンゴメリ型楕円曲線における y 座標復元方法[20)]を用いることにより，Y 座標を容易に計算することができることを注意しておく．

出力 スカラー倍 dP の X 座標および Z 座標
(1) 乱数 $r \in \mathbf{F}_{p^n} - \{0\}$ を生成する．
(2) 射影座標において，点 P を $P = (rx, ry, r)$ と表現する．ただし ry は計算しなくてよい．
(3) $i \leftarrow |d| - 1$
(4) 2 倍公式を用いて，点 P より点 $2P$ を計算する．
(5) $m \leftarrow 1$
(6) $i = 0$ のときステップ (15) へ，そうでなければステップ (7) へ．
(7) $i \leftarrow i - 1$
(8) $d_i = 0$ のときステップ (9) へ，そうでなければステップ (12) へ．
(9) 加算公式を用いて，点 mP，点 $(m+1)P$ および点 P より，点 $(2m+1)P$ を計算する．
(10) 2 倍公式を用いて，点 mP より点 $2mP$ を計算する．
(11) $m \leftarrow 2m$ として，ステップ (6) へ．
(12) 加算公式を用いて，点 mP，点 $(m+1)P$ および点 P より，点 $(2m+1)P$ を計算する．
(13) 2 倍公式を用いて，点 $(m+1)P$ より点 $(2m+2)P$ を計算する．
(14) $m \leftarrow 2m+1$ として，ステップ (6) へ．
(15) 点 mP の X 座標および Z 座標をスカラー倍 dP の X 座標および Z 座標として出力する．

このアルゴリズムは，ステップ (9) およびステップ (12) の加算演算において，差分点 P の Z 座標が r であり，一般的に $r \neq 1$ であるので，差分点 P の Z 座標が 1 ではない．そのため，この加算の計算量は $4M + 2S$ となる．したがって全体の計算量は $(7|d| - 3)M + (4|d| - 2)S$ となる．元々のスカラー倍計算の計算量と比べると，$|d|M$ だけ計算量が増大している．

3.4 従来法における問題点の考察

アルゴリズム 1 は点 P の Z 座標を 1 ととっているため，加算公式の計算量が $3M + 2S$ となり，高速演算が可能である．しかしながら，攻撃者にとって判別点の値は計算可能である．たとえば $d_{|d|-2}$ を求めるための判別点として $4P$ をとる☆と，点 P の Z 座標が 1 であるので攻撃者は $4P$ の，アルゴリズム 1 に用いられる射影座標の値を計算することができる．そして，$d_{|d|-2} = 1$ の場合，1 回目の繰返しのステップ (11) で $4P$ が計算される．$d_{|d|-2} = 0$ であったとすると，1 回目の繰返しのステップ (8) で $2P$ を計算することになり，したがって $d_{|d|-2}$ の値を判定することができる．そのため，アルゴリズム 1 はサイドチャネル攻撃に対して脆弱となる．

アルゴリズム 2 は点 P の値をランダム化したため，乱数の情報を知らない攻撃者は判別点である $4P$ の，アルゴリズム 2 に用いられる射影座標の値を計算できない．そのため，サイドチャネル攻撃に対して耐性を有する．しかしながら，点 P をランダム化した結果，その Z 座標は 1 ではなくなり，加算の計算量が $4M+2S$ となる．そのため，高速計算ができなくなる．

したがって，サイドチャネル攻撃を防ぎかつ高速なスカラー倍計算アルゴリズムを構成するためには，二律背反する次の 2 つの条件をみたさなくてはならない．(1) 高速性を達成するため点 P の Z 座標は 1 とする必要がある．(2) 攻撃者が判別点を計算できないようにするため点 P をランダム化する必要がある（すなわち Z 座標を 1 とすることができない）．

4. 提 案 法

サイドチャネル攻撃への耐性と高速性という 2 つの性質を有するスカラー倍計算アルゴリズムの構成のためには，点 P の Z 座標は 1 とする必要があり，また点 P はランダム化（すなわち Z 座標は 1 とはできない）する必要がある．提案法のスカラー倍計算アルゴリズム☆☆では，点 P という 1 つのものに対し，ランダム化した点 P と，ランダム化していない点 P という 2 通りの表し方を用いる．これにより，サイドチャネル攻撃への耐性と高速性を達成することができる．

アルゴリズム 3
入力 スカラー値 d，点 $P = (x, y)$ の x 座標
出力 スカラー倍 dP の X 座標および Z 座標
(1) 乱数 $r \in \mathbf{F}_{p^n} - \{0\}$ を生成する．
(2) 射影座標において，点 P を $P = (rx, ry, r)$ と表現する．ただし ry は計算しなくてよい．
(3) $i \leftarrow |d| - 1$
(4) 2 倍公式を用いて，点 P より点 $2P$ を計算する．
(5) $m \leftarrow 1$
(6) $i = 0$ のときステップ (15) へ，そうでなければステップ (7) へ．
(7) $i \leftarrow i - 1$
(8) $d_i = 0$ のときステップ (9) へ，そうでなければステップ (12) へ．

☆ $4P$ のほかには，$2P$，$5P$，$7P$ を判別点としてとることができる．

☆☆ このアルゴリズムも，スカラー倍点 dP の Y 座標を計算しない．しかしながら，モンゴメリ型楕円曲線における y 座標復元方法[20] を用いることにより，Y 座標を容易に計算することができることを注意しておく．

(9) 加算公式を用いて，点 mP，点 $(m+1)P$ および点 P より，点 $(2m+1)P$ を計算する．ここでの点 P はランダム化されていない点 $(x,y,1)$ を用いる．
(10) 2 倍公式を用いて，点 mP より点 $2mP$ を計算する．
(11) $m \leftarrow 2m$ として，ステップ (6) へ．
(12) 加算公式を用いて，点 mP，点 $(m+1)P$ および点 P より，点 $(2m+1)P$ を計算する．ここでの点 P はランダム化されていない点 $(x,y,1)$ を用いる．
(13) 2 倍公式を用いて，点 $(m+1)P$ より点 $(2m+2)P$ を計算する．
(14) $m \leftarrow 2m+1$ として，ステップ (6) へ．
(15) 点 mP の X 座標および Z 座標をスカラー倍 dP の X 座標および Z 座標として出力する．

4.1 正 当 性

まず，このアルゴリズムによりスカラー倍が計算できていることの正当性☆を示す．このためには，ステップ (9) およびステップ (12) の加算が，点 P として (rx, ry, r) を用いた場合と一致することを示せばよい．点 P の位数を k とすると，スカラー値 d は $d \le k-2$ が仮定されており，また計算途中の点 mP，$(m+1)P$ の m，$m+1$ は，d より小さい．そのため，点 mP，$(m+1)P$ が無限遠点 $\mathcal{O}$ となることはない．そのため，それらの点の射影座標系における Z 座標の値は 0 ではない．ステップ (9) の点 mP および $(m+1)P$ の射影座標における X 座標，Z 座標の値を，それぞれ X''_m，Z''_m および X''_{m+1}，Z''_{m+1} とし，ステップ (9) により計算された点の射影座標における X 座標を X''_{2m+1}，Z 座標を Z''_{2m+1} とする．アルゴリズム 2 のステップ (9) の点 mP および $(m+1)P$ の射影座標における X 座標，Z 座標の値を，それぞれ X'_m，Z'_m および X'_{m+1}，Z'_{m+1} とし，アルゴリズム 2 のステップ (9) により計算された点の射影座標における X 座標を X'_{2m+1}，Z 座標を Z'_{2m+1} とする．このとき $X''_m/Z''_m = x_m$，$X''_{m+1}/Z''_{m+1} = x_{m+1}$，$X'_m/Z'_m = x_m$ および $X'_{m+1}/Z'_{m+1} = x_{m+1}$ を仮定し，$X''_{2m+1}/Z''_{2m+1} = X'_{2m+1}/Z'_{2m+1}$ を示せばよい．なぜなら，$X'_{2m+1}/Z'_{2m+1} = x_{2m+1}$ であるからである．ここで，x_m，x_{m+1} および x_{2m+1} は，それぞれ mP，$(m+1)P$ および $(2m+1)P$ のアフィン座標における x 座標を表す．

☆ 提案アルゴリズムの正当性を示すことは，加法公式が射影座標のとり方によらず，うまく定義されていることを示すことと同値である．

命題 1 $X''_{2m+1}/Z''_{2m+1} = X'_{2m+1}/Z'_{2m+1}$

証明

$$
\begin{aligned}
&X''_{2m+1}/Z''_{2m+1} \\
&= 1 \cdot [(X''_{m+1} - Z''_{m+1})(X''_m + Z''_m) \\
&\qquad +(X''_{m+1} + Z''_{m+1})X''_m - Z''_m)]^2 \\
&\quad /x[(X''_{m+1} - Z''_{m+1})(X''_m + Z''_m) \\
&\qquad -(X''_{m+1} + Z''_{m+1})(X''_m - Z''_m)]^2 \\
&= \frac{[(x_{m+1}-1)(x_m+1) + (x_{m+1}+1)(x_m-1)]^2}{x[(x_{m+1}-1)(x_m+1) - (x_{m+1}+1)(x_m-1)]^2} \\
&= r[(X'_{m+1} - Z'_{m+1})(X'_m + Z'_m) \\
&\qquad +(X'_{m+1} + Z'_{m+1})(X'_m - Z'_m)]^2 \\
&\quad /rx[(X'_{m+1} - Z'_{m+1})(X'_m + Z'_m) \\
&\qquad -(X'_{m+1} + Z'_{m+1})(X'_m - Z'_m)]^2 \\
&= X'_{2m+1}/Z'_{2m+1}
\end{aligned}
$$

□

ステップ (12) もまったく同様であり，したがってスカラー倍計算の正当性が示せた．

4.2 高 速 性

次に，このアルゴリズムの計算量について試算する．このアルゴリズムはステップ (9) およびステップ (12) の加算演算において，差分点 P の Z 座標が 1 であるので，加算の計算量は $3M+2S$ となる．全体の計算量は $(6|d|-2)M + (4|d|-2)S$ となる．したがって，元々のスカラー倍計算の計算量と同等の計算量で達成できる．

今度は，ワイエルシュトラス型楕円曲線上における高速化のみを主眼においたスカラー倍計算方法と，高速性の観点から比較する．混合座標系を用いたウィンドウ法は，ワイエルシュトラス型楕円曲線上の最も高速なスカラー倍計算方法の 1 つである[4)]．この方法の計算量は，ビット長を l，ウィンドウサイズを w とした場合，次の式で見積もられる[4),14)]．

$$
\begin{aligned}
T^{Wei}(w,l) &= wI \\
&\quad + \left(\frac{8l}{w+2} + 4l + 5\cdot 2^{w-1} - 2w - 14\right) M \\
&\quad + \left(\frac{3l}{w+2} + 4l + 2^{w-1} - 2w - 2\right) S
\end{aligned}
$$

ここで，I は $\mathbf{F}_{p^n}$ 上の逆元演算の計算量である．素体上の逆元演算の計算量は $I = 30M$ 程度，2 乗算の計算量は $S = 0.8M$ 程度と見積もられる[14)] ので，それらを仮定し，ビット長 $l = 160$，ウィンドウサイズ $w = 4$ とした場合の計算量は，$T^{Wei}(w,l) = 1565.7M$ となる．一方，160 ビットでの提案法の計算量は $1468.4M$ であり，提案法が高速である．

4.3 安 全 性

最後に，このアルゴリズムの，サイドチャネル攻撃

に対する安全性を示す．桶屋–櫻井によれば，次の 2 つの要件をみたすことを調べればよい[19]．

（1）　秘密情報と計算実行手順とが独立である．

（2）　計算対象の値がランダム化されている．

まず (1) について調べる．ここでの秘密情報は，スカラー値 d とステップ 1 で生成した乱数 r である．また，計算実行手順は，アルゴリズム中において計算される楕円加算および 2 倍算の実行順序である．秘密情報と計算実行手順とが独立であることを示すには，秘密情報の値によらず，実行される楕円加算・2 倍算の順序が固定されていることを示せば十分である．また乱数 r は，射影座標の値をランダム化するための冗長な情報であり，楕円加算・2 倍算の実行順序とは関係がない．したがって，スカラー値 d に対して考察する．

ビット長を固定した任意のスカラー値に対して，ステップ (8) で $d_i = 0$ であればステップ (9)〜(11) を，$d_i = 1$ であればステップ (12)〜(14) を実行し，ステップ (6) へ戻るが，ともに，楕円曲線上の加算を行ってから楕円曲線上の 2 倍算を行うので，実行している計算は同一のものである．したがって計算実行手順は，ビット長を固定したすべてのスカラー値に対して同一である．ゆえに，提案法は (1) をみたす．

次に (2) について調べる．ここで，計算対象の値は判別点 mP の X 座標および Z 座標である．また，ランダム化されているとは，攻撃者が判別点として mP を選んだ場合に，mP の X 座標および Z 座標の値としてとりうる値の数が，定義体のビット長の指数オーダであることをいう．

命題 1 より，$X''_m = r_m X_m$，$Z''_m = r_m Z_m$ と，ある整数 $r_m \neq 0$ を用いて表すことができる．ただし，X''_m，Z''_m，X_m, Z_m は，それぞれアルゴリズム 3 の点 mP の X 座標，Z 座標，アルゴリズム 1 の点 mP の X 座標，Z 座標である．X''_m および Z''_m のとりうる値の数は，r_m のとりうる値の数に等しいので，(2) を示すためには，この r_m のとりうる値の数が定義体のビット長の指数オーダであることを示せばよい．

まず最初に，r_m と乱数 r との関係を調べるために次の関数 $e(s,t)$ を定義する．

$$e(s,t) := 2^{2s} + t(2^{s+2} - 2^s) \qquad \begin{cases} s = 0, 1, \cdots \\ t = 0, 1, \cdots \end{cases}$$

このとき次の等式が成立する．これらの等式は直接計算により確かめることができる．

補題 1

$$e(s+1, 0) = e(s, 2^s)$$
$$e(s+1, 2t) = 4e(s,t)$$
$$e(s+1, 2t+1) = 2(e(s,t) + e(s,t+1))$$

次に，$m = 1, 2, \cdots$ に対して関数 $e(m)$ を $e(m) := e(|m|-1, m - 2^{|m|-1})$ と定義する．そのとき上記 r_m は，ステップ (1) で生成した乱数 r と関数 $e(m)$ を用いて次のように表すことができる☆．

命題 2　$r_m = r^{e(m)}$

今，攻撃者が何らかの手段により，スカラー値 d の上位ビット列 m_0 ($m_0 = \sum_{i=0}^{j-1} d_{|d|+i-j} 2^i$, $|m_0| = j$) を特定できたとする．その次のビット $d_{|d|-j-1}$ を特定するための判別点となる点は，$2m_0P$，$(2m_0+2)P$，$(4m_0+1)P$，$(4m_0+3)P$ のいずれか☆☆である．そのため，判別点は攻撃者が選択可能ではあるが，4 点のみに制限されている．またそれらの判別点はスカラー値 d に依存して決まる．そのため，スカラー値 d を一様に選べば，対応する 4 点の判別点もスカラー値に応じて変わる．したがってここでは，判別点 mP はビット長 h 以下の集合から一様に選ばれていると仮定する．すなわち，$m \in_U \{m \big| |m| \leq h\}$ である．

$m \in_U \{m \big| |m| \leq h\}$ と一様に選んだとき，$r^{e(m)}$ のとりうる値の数の期待値に関する次の命題を示すことができる．

命題 3　定義体の乗法群の位数を $p^n - 1 = 2^{l_2} 3^{l_3} p_1^{l_{p_1}} \cdots p_k^{l_{p_k}}$ と表す．ただし，$p_1, \cdots, p_k$ は相異なる素数で，$l_{p_1}, \cdots, l_{p_k}$ は正整数であり，l_2，l_3 は非負整数である．そのとき，$h \in \{h \big| h \leq |p^n - 1|\}$ とし，$m \in_U \{m \big| |m| \leq h\}$ を一様に選んだとき，$\#\{r^{e(m)} | r \in \mathbf{F}_{p^n} - \{0\}\}$ の期待値 $E(h)$ は，

$$p^n - 1 \geq E(h) \geq (p^n - 1) \Bigg/ \left(2^{\min\{l_2, 2(h-1)\}} \prod_{j=1}^{k} p_j^{\frac{1}{p_j - 1}} \right)$$

をみたす．

$\prod_{j=1}^{k} p_j^{\frac{1}{p_j-1}}$ の評価に関して次の命題が成立する．

命題 4　ある定数 $c > 0$ が存在し，$|p^n - 1| \to \infty$ とするとき，

$$\prod_{j=1}^{k} p_j^{\frac{1}{p_j-1}} \leq c |p^n - 1|^2$$

☆ この節の命題の証明は付録において与えてある．

☆☆ $d_{|d|-j-1} = 0$ のとき，j 回目のステップ（10）の 2 倍算で $2m_0P$ が，$j+1$ 回目のステップ（9）もしくはステップ（12）の加算で $(4m_0+1)P$ が計算される．$d_{|d|-j-1} = 1$ のときは，j 回目のステップ（10）の 2 倍算で $(2m_0+2)P$ が，$j+1$ 回目のステップ（9）もしくはステップ（12）の加算で $(4m_0+3)P$ が計算される．$d_{|d|-j-1}$ の値のみに依存して計算される点は，上記以外には存在しない．

表 1 サイドチャネル攻撃に対する耐性と計算量
Table 1 Immunities to side channel attacks and computational costs.

計算法	DPA 攻撃に対する耐性	SPA 攻撃に対する耐性	160 ビットでの計算量	192 ビットでの計算量	256 ビットでの計算量
M 型スカラー倍	脆弱	安全	$1467.4M$	$1761.8M$	$2350.6M$
M 型 + RPC	安全	安全	$1627.4M$	$1955.4M$	$2606.6M$
提案法	安全	安全	$1468.4M$	$1762.8M$	$2351.6M$
W 型スカラー倍	脆弱	脆弱	$1565.7M$	$1851.6M$	$2423.3M$
M 型スカラー倍	脆弱	安全	$1467.4M$	$1761.8M$	$2350.6M$
W 型耐 SPA	脆弱	安全	$3072.0M$	$3686.4M$	$4915.2M$
J 型	脆弱	安全	$3075.2M$	$3689.6M$	$4918.4M$
H 型	脆弱	安全	$2306.4M$	$2767.2M$	$3688.8M$

M 型スカラー倍は，モンゴメリ型楕円曲線上のスカラー倍計算法（アルゴリズム 1），M 型 + RPC は，モンゴメリ型楕円曲線上のランダム化射影座標を用いたスカラー倍計算法（アルゴリズム 2），提案法は，提案法のモンゴメリ型楕円曲線上のランダム化射影座標を用いたスカラー倍計算法（アルゴリズム 3），W 型スカラー倍は，ワイエルシュトラス型楕円曲線上の混合座標系を用いたウィンドウ法，W 型耐 SPA は，ワイエルシュトラス型楕円曲線上の，Coron の耐 SPA スカラー倍計算法[5)]，J 型は，ヤコビ型楕円曲線におけるスカラー倍計算法[15)]，H 型は，ヘジアン型楕円曲線におけるスカラー倍計算法[7)] を，それぞれ指す．M は，各々対応する有限体における乗算を表す．

となる．

命題 4 を用いると次の命題を示すことができる．

命題 5 ある多項式関数 $f(x)$ に対して，$2^{\min\{l_2, 2(h-1)\}} \leq f(|p^n-1|)$ であれば，$E(h)$ は $|p^n-1|$ の指数オーダとなる．

アルゴリズム 3 は，スカラー値 d の上位ビットから順に用いて計算するため，攻撃者はスカラー値の上位ビットから順に特定しなければならない．そのため攻撃者はまず $d_{|d|-2}$ を特定する必要がある．$d_{|d|-2}$ を特定するための判別点は，$2P$，$4P$，$5P$，$7P$ のみである．そのためビット長の最大値 $h=3$ であり，これは $|p^n-1|$ に依存しない．したがって命題 5 より，$E(h)$ は $|p^n-1|$ の指数オーダである．ゆえに，提案法は要件 (2) をみたし，サイドチャネル攻撃に対する耐性を有することが示せた．

注意 1 定義体として，標数がフェルマー素数の素体を選ぶと，$p-1=2^{l_2}$ となる．そのため，h が $l_2 \leq 2(h-1)$ であれば，命題 3 より $E(h) \geq 1$ となる．また，実際に $|p-1|$ の指数オーダではない場合が生じる．しかしながら，定義体を暗号の設計者が選ぶ場合には，そのようなパラメータを避けることができる．また，$E(h)$ が $|p-1|$ の指数オーダとなるように定義体素数に関する 2 冪指数 l_2 は小さくとる方が望ましい．

4.4 サイドチャネル攻撃を防ぐ他の方法との比較

Coron はワイエルシュトラス型楕円曲線における，ダミー演算を用いた耐 SPA スカラー倍計算方法を提案した[5)]．これは，スカラー値 1 ビットにつき，必ず加算を計算し，もしそのビットが 0 である場合は計算結果を捨てる方法である．J，A，J^m はそれぞれ Jacobian 座標，アフィン座標，modified Jacobian 座標を表すとする．この方法の加算 $J+A \rightarrow J^m$ の計算量は $9M+5S$ であり，2 倍算 $J^m \rightarrow J$ の計算量は $3M+4S$ である．160 ビットに対する全体の計算量は，$S=0.8M$ を仮定して $3072.0M$ である．

Liardet らはヤコビ型楕円曲線における，耐 SPA スカラー倍計算方法を提案した[15)]．ヤコビ型楕円曲線における加算および 2 倍算は，同じ公式を用いて計算される．この性質により SPA 攻撃を防いでいる．ヤコビ型楕円曲線の加算の計算量は $16M$ である．この方法は，sliding window 法[3)] を用いることができるので，160 ビットにおける加算回数はおよそ 192.2 回である．全体の計算量は，$S=0.8M$ を仮定して $3075.2M$ である．

Joye らはヘジアン型楕円曲線における，耐 SPA スカラー倍計算方法を提案した[7)]．ヘジアン型楕円曲線における加算および 2 倍算は，同じ公式を用いて計算される．この性質により SPA 攻撃を防いでいる．ヘジアン型楕円曲線の加算の計算量は $12M$ である．この方法は，sliding window 法[3)] を用いることができるので，160 ビットにおける加算回数はおよそ 192.2 回である．全体の計算量は，$S=0.8M$ を仮定して $2306.4M$ である．

ランダム化（射影）座標のテクニックは，他の型の楕円曲線におけるスカラー倍計算にも適応できる．しかしながら，モンゴメリ型楕円曲線におけるスカラー倍計算法と比べ，それらのスカラー倍計算はかなり遅い．したがって，ワイエルシュトラス型，ヤコビ型，ヘジアン型楕円曲線において，ランダム化（射影）座標を用いたサイドチャネル攻撃（DPA 攻撃）の防御法は，速度面で効率的ではない．

同様に 192，256 ビットに対しても計算量の見積りを行い，以上議論したことをまとめると，**表 1** となる．

表 2 平均実行時間の比較
Table 2 Implementational results.

	160 ビット	192 ビット	256 ビット
アルゴリズム 1	3.735 [ms]	5.937 [ms]	11.946 [ms]
アルゴリズム 2	4.031 [ms]	6.448 [ms]	13.045 [ms]
アルゴリズム 3	3.751 [ms]	5.981 [ms]	12.017 [ms]

5. 実装結果

アルゴリズム 1，2，3 の実装を行い，その実行時間の計測を行った．以下の環境で実装実験を行った．

CPU：Pentium® III 650 MHz

開発言語：ANSI 準拠 C 言語

実行時間算出方法：スカラー倍演算を 10,000 回実行しその平均実行時間を求める．

実験結果をまとめたものが**表 2** である．

アルゴリズム 3 はアルゴリズム 2 よりも約 8%，高速であり，アルゴリズム 1 と比べて約 0.5%，低速である．速度向上割合の理論値との違いは，理論値では有限体上の加減算，乱数生成の時間を無視して見積もっていることと，実装では初期化処理や関数呼び出しのオーバヘッドが生じていること，有限体上の乗算と 2 乗算の比が理論値 0.8 と異なることが原因と考えられる．

実際，この実装環境では，有限体上の乗算と 2 乗算の比は約 1 であり，有限体上の加減算の計算時間は有限体上の乗算の計算時間の約 1/4 倍であり，乱数生成の時間は有限体上の乗算約 6 回分であった．これを加味した速度向上割合は，アルゴリズム 3 のアルゴリズム 2 に対する速度向上が約 8%であり，アルゴリズム 3 のアルゴリズム 1 に対する速度低下の割合が約 0.5%となり，実験結果に符合する．

6. まとめ

本論文では，サイドチャネル攻撃に対する防御法として，モンゴメリ型楕円曲線におけるスカラー倍計算において，ランダム化射影座標を用いた防御法を提案した．その防御法に入力される楕円曲線上の点はランダム化したものとランダム化していないものの 2 通りに表される．そして，計算の最初ではランダム化した点を用い，その後の加算に対する補助入力である差分点としては，ランダム化をしていない点を用いる．そのことにより，サイドチャネル攻撃を防ぎつつ計算量を削減することができた．差分点もランダム化する従来法と比べ，約 10%の高速化を図ることができる．提案法は他の型の楕円曲線にも適応可能であるが，その場合，速度面で効率的ではない．今後の課題としては，ランダム化射影座標を用いる場合と用いない場合とにおいて，その有効性の違いを示す DPA 攻撃実証実験がある．

参考文献

1) Apostol, T.M.: Introduction to Analytic Number Theory, *Undergraduate Texts in Mathematics*, Springer-Verlag (1995).
2) Akker, M.L., Bevan, R., Dischamp, P. and Moyart, D.: Power Analysis, What Is Now Possible..., *Advances in Cryptology — ASIACRYPT 2000*, LNCS1976, pp.489–502 (2000).
3) Blake, I.F., Seroussi, G. and Smart, N.P.: *Elliptic Curves in Cryptography*, Cambridge University Press (1999).
4) Cohen, H., Miyaji, A. and Ono, T.: Efficient Elliptic Curve Exponentiation Using Mixed Coordinates, *Advances in Cryptology — ASIACRYPT '98*, LNCS1514, pp.51–65 (1998).
5) Coron, J.S.: Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems, *Cryptographic Hardware and Embedded Systems* (*CHES'99*), LNCS1717, pp.292–302 (1999).
6) National Bureau of Standards: Data Encryption Standard, *Federal Information Processing Standards Publication 46* (*FIPS PUB 46*) (1977).
7) Joye, M. and Quisquater, J.J.: Hessian elliptic curves and side-channel attacks, *Cryptographic Hardware and Embedded Systems* (*CHES'01*), LNCS2162, pp.402–410 (2001).
8) Joye, M. and Tymen, C.: Protections against differential analysis for elliptic curve cryptography: An algebraic approach, *Cryptographic Hardware and Embedded Systems* (*CHES'01*), LNCS2162, pp.377–390 (2001).
9) Koblitz, N.: Elliptic curve cryptosystems, *Math. Comp.* 48, pp.203–209 (1987).
10) Kocher, C.: Cryptanalysis of Diffie-Hellman, RSA, DSS, and Other Systems Using Timing Attacks.
Available at http://www.cryptography.com/
11) Kocher, C.: Timing Attacks on Implementations of Diffie-Hellman, RSA,DSS, and Other Systems, *Advances in Cryptology — CRYPTO '96*, LNCS1109, pp.104–113 (1996).
12) Kocher, C., Jaffe, J. and Jun, B.: Introduction to Differential Power Analysis and Related Attacks. Available at http://www.cryptography.com/dpa/technical/index.html
13) Kocher, C., Jaffe, J. and Jun, B.: Differen-

tial Power Analysis, *Advances in Cryptology — CRYPTO '99*, LNCS1666, pp.388–397 (1999).

14) Lim, C.H. and Hwang, H.S.: Fast implementation of Elliptic Curve Arithmetic in $GF(p^m)$, *Proc. PKC'00*, LNCS1751, pp.405–421 (2000).

15) Liardet, P.Y. and Smart, N.P.: Preventing SPA/DPA in ECC systems using the Jacobi form, *Cryptographic Hardware and Embedded System* (*CHES'01*), LNCS2162, pp.391–401 (2001).

16) Miller, V.S.: *Use of elliptic curves in cryptography, Advances in Cryptology — CRYPTO '85*, LNCS218, pp.417–426 (1986).

17) Montgomery, P.L.: Speeding the Pollard and Elliptic Curve Methods of Factorizations, *Math. Comp.*, 48, pp.243–264 (1987).

18) Okeya, K., Kurumatani, H. and Sakurai, K.: Elliptic Curves with the Montgomery — Form and Their Cryptographic Applications, *Public Key Cryptography* (*PKC2000*), LNCS1751, pp.238–257 (2000).

19) Okeya, K. and Sakurai, K.: Power Analysis Breaks Elliptic Curve Cryptosystems even Secure against the Timing Attack, *Progress in Cryptology — INDOCRYPT 2000*, LNCS1977, pp.178–190 (2000).

20) Okeya, K. and Sakurai, K.: Efficient Elliptic Curve Cryptosystems from a Scalar Multiplication Algorithm with Recovery of the y-Coordinate on a Montgomery-Form Elliptic Curve, *Cryptographic Hardware and Embedded System* (*CHES'01*), LNCS2162, pp.126–141 (2001).

21) Rivest, R.L., Shamir, A. and Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Comm. ACM*, Vol.21, No.2, pp.120–126 (1978).

付　　録

A.1 命題の証明

命題 2 の証明　m に関する帰納法により証明する．$r_1 = r$，$r_2 = r^4$，$e(1) = 1$，$e(2) = 4$ は直接計算により確かめることができる．次に，$r_m = r^{e(m)}$，$r_{m+1} = r^{e(m+1)}$ を仮定し，$d_i = 0$ であれば $r_{2m} = r^{e(2m)}$，$r_{2m+1} = r^{e(2m+1)}$ を，$d_i = 1$ であれば $r_{2m+1} = r^{e(2m+1)}$，$r_{2m+2} = r^{e(2m+2)}$ を，示す．

まず $d_i = 0$ のときを示す．

$$\begin{aligned}X''_{2m} &= (X''_m + Z''_m)^2 (X''_m - Z''_m)^2 \\ &= (r_m X_m + r_m Z_m)^2 (r_m X_m - r_m Z_m)^2 \\ &= r_m^4 (X_m + Z_m)^2 (X_m - Z_m)^2 \\ &= r^{4e(m)} X_{2m}\end{aligned}$$

補題 1 より $4e(m) = e(2m)$ であり，したがって $r_{2m} = r^{e(2m)}$ である．

$$\begin{aligned}&X''_{2m+1} \\ &= [(X''_{m+1} - Z''_{m+1})(X''_m + Z''_m) \\ &\quad + (X''_{m+1} + Z''_{m+1})(X''_m - Z''_m)]^2 \\ &= [(r_{m+1}X_{m+1} - r_{m+1}Z_{m+1})(r_m X_m + r_m Z_m) \\ &\quad + (r_{m+1}X_{m+1} + r_{m+1}Z_{m+1})(r_m X_m - r_m Z_m)]^2 \\ &= r_{m+1}^2 r_m^2 [(X_{m+1} - Z_{m+1})(X_m + Z_m) \\ &\quad + (X_{m+1} + Z_{m+1})(X_m - Z_m)]^2 \\ &= r^{2(e(m+1)+e(m))} X_{2m+1}\end{aligned}$$

$|m+1| = |m|$ であれば，補題 1 より $2(e(m+1) + e(m)) = e(2m+1)$ であり，$r_{2m+1} = r^{e(2m+1)}$ を得る．$|m+1| = |m| + 1$ であれば，補題 1 より $e(m+1) = e(|m|, 0) = e(|m| - 1, 2^{|m|-1})$ となり，補題 1 より $r_{2m+1} = r^{e(2m+1)}$ を得る．

$d_i = 1$ の場合も，$d_i = 0$ の場合と同様に示すことができる．したがって，帰納法により，すべての m に対して $r_m = r^{e(m)}$ が成立する． □

命題 3 を示すために，いくつかの命題と補題を与え，それらを用いて証明する．まず，$e(m)$ は次の命題により明確に与えることができる．

命題 6　$e(m) = 2^{|m|-1}\left(2^{|m|-1} + 3\left(m - 2^{|m|-1}\right)\right)$

命題 6 の証明　m に関する帰納法により証明する．$m = 1$ に関しては直接計算により確かめることができる．

まず m に対して命題の式が成立すると仮定し，$2m$ に対しても成立することを示す．$|2m| = |m| + 1$ であり，また補題 1 より

$$\begin{aligned}e(2m) &= 4e(m) \\ &= 4\left(2^{|m|-1}\left(2^{|m|-1} + 3\left(m - 2^{|m|-1}\right)\right)\right) \\ &= 2^{|2m|-1}\left(2^{|2m|-1} + 3\left(2m - 2^{|2m|-1}\right)\right)\end{aligned}$$

が成り立つ．

次に m，$m+1$ に対して命題の式が成立すると仮定し，$2m+1$ に対しても成立することを示す．補題 1 より

$$\begin{aligned}&e(2m+1) \\ &= 2(e(m+1) + e(m)) \\ &= 2\left[2^{|m+1|-1}\left(2^{|m+1|-1} + 3\left(m+1-2^{|m+1|-1}\right)\right)\right. \\ &\quad \left. + 2^{|m|-1}\left(2^{|m|-1} + 3\left(m - 2^{|m|-1}\right)\right)\right]\end{aligned}$$

ここで，$|m+1| = |m|$ とすると，$|2m+1| = |m| + 1$ であるので，

$$\begin{aligned}&e(2m+1) \\ &= 2^{|2m+1|-1}\left(2^{|2m+1|-1} + 3\left(2m+1-2^{|2m+1|-1}\right)\right)\end{aligned}$$

が成り立つ．$|m+1| = |m|+1$ とすると，$m = 2^{|m|} - 1$，

$|2m+1| = |m|+1$ であるので，

$$
\begin{aligned}
&e(2m+1)\\
&= 2\left[2^{|m|}\left(2^{|m|}+3\left(2^{|m|}-2^{|m|}\right)\right)\right.\\
&\quad\left.+\,2^{|m|-1}\left(2^{|m|-1}+3\left(2^{|m|}-1-2^{|m|-1}\right)\right)\right]\\
&= 2\left[2^{|m|-1}\left(2^{|m|-1}+3\left(2^{|m|}-2^{|m|-1}\right)\right)\right.\\
&\quad\left.+\,2^{|m|-1}\left(2^{|m|-1}+3\left(2^{|m|}-1-2^{|m|-1}\right)\right)\right]\\
&= 2^{|2m+1|-1}\left(2^{|2m+1|-1}+3\left(2m+1-2^{|2m+1|-1}\right)\right)
\end{aligned}
$$

が成り立つ．したがって，帰納法によりすべての m に対して命題の式が成立する． □

次に，$e(m)$ の整除性について調べる．命題 6 より次のことがただちに分かる．

系 1 $2^{|m|-1}|e(m),\ 3\not|e(m)$

今度は，2，3 以外の数に対する整除性について調べる．m に対して，$q(m) := e(m)/2^{|m|-1}$ とおくと，系 1 より $q(m)$ は整数となり，また 3 の倍数ではない．$\mathbf{N}$ を 1 以上の整数の集合，

$\mathbf{3N} := \{n \in \mathbf{N} | n = 3\alpha \text{ for some } \alpha \in \mathbf{N}\}$,

$\mathbf{3N{+}1} := \{n \in \mathbf{N} | n = 3\alpha{+}1 \text{ for some } \alpha \in \mathbf{N}\cup\{0\}\}$,

$\mathbf{3N{+}2} := \{n \in \mathbf{N} | n = 3\alpha{+}2 \text{ for some } \alpha \in \mathbf{N}\cup\{0\}\}$

とする．そのとき以下の補題が成り立つ．

補題 2 $\mathbf{N} - \mathbf{3N} = (\mathbf{3N+1}) \cup (\mathbf{3N+2})$,
$(\mathbf{3N+1}) \cap (\mathbf{3N+2}) = \phi$

補題 2 の証明 定義より明らか． □

補題 3 $q : \mathbf{N} \ni m \mapsto q(m) \in \mathbf{N} - \mathbf{3N}$ は全単射である．

補題 3 の証明 まず単射性を示す．$m_1 < m_2$ とすると，次のいずれかが成り立つ．(i) $|m_1| = |m_2|$，$m_1 < m_2$，(ii) $|m_1| < |m_2|$，$|m_2| - |m_1|$: 奇数，(iii) $|m_1| < |m_2|$，$|m_2| - |m_1|$: 偶数.

(i) $|m_1| = |m_2|$，$m_1 < m_2$ とすると，$q(m_2) - q(m_1) = 3(m_2 - m_1) > 0$ となる．

(ii) $|m_1| < |m_2|$，$|m_2| - |m_1|$: 奇数とすると，$q(m_2) - q(m_1) \equiv 2^{|m_1|-1}(2^{|m_2|-|m_1|} - 1) \not\equiv 0 \pmod 3$ となるので，$q(m_2) \neq q(m_1)$ となる．

(iii) $|m_1| < |m_2|$，$|m_2| - |m_1|$: 偶数とする．$|m| = |m'|$ のとき，$m < m' \Rightarrow q(m) < q(m')$ である．$|m_2| = |m_1| + 2$ とすると，$q(m_2) - q(m_1) \geq (2^{|m_1|+1}) - (2^{|m_1|+1} - 3) > 0$ となる．次に $|m_2| = |m_1| + 2u$ と $u \in \mathbf{N}$ により表し，$m^{(v)}$ $(v = 1, 2, \cdots, u-1)$ を，$|m^{(v)}| = |m_1| + 2v$ をみたすように選ぶと，$q(m_2) > q(m^{(u-1)}) > \cdots > q(m_1)$ となる．したがって単射性が示せた．

次に全射性を示す．まず，$\forall 3\alpha + 1 \in \mathbf{3N+1}$ に対し，$\exists m \in \mathbf{N} : q(m) = 3\alpha + 1$ となることを示す．$w \in \mathbf{N} \cup \{0\}$ に対して，$S_1(w) := \sum_{j=0}^{w} 2^{2j}$ とおく．$w_{1,\alpha} := \min\{w \in \mathbf{N} \cup \{0\} | \alpha < S_1(w)\}$ とする．そのとき，$m := 2^{2w_{1,\alpha}+1} + \alpha - S_1(w_{1,\alpha})$ とすると，$|m| = 2w_{1,\alpha} + 1$ であり，直接計算により，$q(m) = 3\alpha + 1$ となることが分かる．

次に，$\forall 3\alpha + 2 \in \mathbf{3N} + 2$ に対し，$\exists m \in \mathbf{N} : q(m) = 3\alpha + 2$ となることを示す．$w \in \mathbf{N} \cup \{0\}$ に対して，$S_2(w) := \sum_{j=0}^{w} 2^{2j+1}$ とおく．$w_{2,\alpha} := \min\{w \in \mathbf{N} \cup \{0\} | \alpha < S_2(w)\}$ とする．そのとき，$m := 2^{2w_{2,\alpha}+2} + \alpha - S_2(w_{2,\alpha})$ とすると，$|m| = 2w_{2,\alpha} + 2$ であり，直接計算により，$q(m) = 3\alpha + 2$ となることが分かる． □

補題 4 $m_1 < m_2$ となる $m_1, m_2 \in \mathbf{N}$ に対して，$q(m_1), q(m_2) \in \mathbf{3N+1} \Rightarrow q(m_1) < q(m_2)$ および $q(m_1), q(m_2) \in \mathbf{3N+2} \Rightarrow q(m_1) < q(m_2)$ が成り立つ．

補題 4 の証明 補題 3 の単射性の証明より明らか． □

補題 5 $a \in \mathbf{N} - \mathbf{3N}$ とする．そのとき

$$\lim_{M\to\infty} \frac{\#\{m \leq M \,|\, q(m) \in \mathbf{3N{+}1}, a|q(m)\}}{\#\{m \leq M \,|\, q(m) \in \mathbf{3N{+}1}\}} = \frac{1}{a}$$

および

$$\lim_{M\to\infty} \frac{\#\{m \leq M \,|\, q(m) \in \mathbf{3N{+}2}, a|q(m)\}}{\#\{m \leq M \,|\, q(m) \in \mathbf{3N{+}2}\}} = \frac{1}{a}$$

が成り立つ．

補題 5 の証明 補題 3 より，$\forall 3\alpha + 1 \in \mathbf{3N+1}$，$\exists m : q(m) = 3\alpha{+}1$ となる．また補題 4 より，$q(\cdot)$ は値域を $\mathbf{3N+1}$ に制限すれば，大小関係を保ち，そのうえ補題 3 より単射である．したがって，$\mathbf{3N+1}$ の元が a で割れる確率を考えればよい．他方 $gcd(3, a) = 1$ なので，$\mathbf{3N+1}$ の元が a で割れる確率は $1/a$ である．後半についても同様である． □

これらの補題を用いると，$q(m)$ の整除性に関する次の命題を示すことができる．

命題 7 $a \in \mathbf{N} - \mathbf{3N}$ とする．そのとき

$$\lim_{M\to\infty} \frac{\#\{m \leq M \,|\, a|q(m)\}}{\#\{m \leq M\}} = \frac{1}{a}$$

が成り立つ．

命題 7 の証明 補題 5 より，$\forall a \in \mathbf{N}{-}\mathbf{3N}$ に対して，$\forall \epsilon > 0, \exists \delta : \forall M \geq \delta$,

$$\left|\frac{\#\{m \leq M | q(m) \in \mathbf{3N{+}1}, a|q(m)\}}{\#\{m \leq M | q(m) \in \mathbf{3N+1}\}} - \frac{1}{a}\right| < \epsilon,$$

$$\left|\frac{\#\{m \leq M | q(m) \in \mathbf{3N{+}2}, a|q(m)\}}{\#\{m \leq M | q(m) \in \mathbf{3N+2}\}} - \frac{1}{a}\right| < \epsilon$$

となる．したがって，補題 2 を考慮に入れると，$\forall \epsilon > 0$

に対して，$M \geq \delta$ であれば，

$$
\begin{aligned}
&\left|\frac{\#\{m \leq M|\, a|q(m)\}}{\#\{m \leq M\}} - \frac{1}{a}\right| \\
&\leq \left|\frac{\#\{m \leq M|\, q(m) \in \mathbf{3N+1}\}}{\#\{m \leq M\}}\right| \\
&\quad \cdot\left|\frac{\#\{m \leq M|\, q(m)\in\mathbf{3N+1},\, a|q(m)\}}{\#\{m \leq M|\, q(m)\in\mathbf{3N+1}\}} - \frac{1}{a}\right| \\
&+ \left|\frac{\#\{m \leq M|\, q(m) \in \mathbf{3N+2}\}}{\#\{m \leq M\}}\right| \\
&\quad \cdot\left|\frac{\#\{m \leq M|\, q(m)\in\mathbf{3N+2},\, a|q(m)\}}{\#\{m \leq M|\, q(m)\in\mathbf{3N+2}\}} - \frac{1}{a}\right| \\
&< \left|\frac{\#\{m \leq M|\, q(m) \in \mathbf{3N+1}\}}{\#\{m \leq M\}}\right|\epsilon \\
&+ \left|\frac{\#\{m \leq M|\, q(m) \in \mathbf{3N+2}\}}{\#\{m \leq M\}}\right|\epsilon \\
&= \epsilon
\end{aligned}
$$

となる．したがって，命題が成り立つ． □

今まで示した命題および補題を用いると，命題 3 を証明できる．

命題 3 の証明 $e(m)$ と p^n-1 の最大公約数を g とすると，$\#\{r-e(m)|\, r \in \mathbf{F}_{p^n}-\{0\}\} = (p^n-1)/g$ である．したがって，$E(h)$ を見積もるためには，g の期待値について見積もればよい．また $g \geq 1$ より，$p^n-1 \geq E(h)$ はただちに分かる．

まず，$e(m)$ の 2 冪に対する整除性について考察する．命題 6 より，$2^{|m|} \not| q(m)$ および $2^l|q(m) \Leftrightarrow 2^l|m$ が分かる．したがって系 1 より，$2^l||m$ とすると，$2^{|m|-1+l}||e(m)$ である．l の定義より $l \leq |m|-1$ なので，$e(m)$ が 2 で割れる回数の期待値は $2(h-1)$ 以下である．また，$2^{l_2+1} \not| g$ である．

次に，系 1 より $3 \not| e(m)$ であるので，3 冪については考慮しなくてよい．2，3 以外の素冪について考察する．命題 7 より，$e(m)$ が $p_j^l\ (j=1,\cdots,k;\, l=1,\cdots)$ で割れる確率は $1/p_j^l$ である．したがって，$m \leq h$ であることを考慮すれば，$e(m)$ が p_j で割れる回数の期待値は

$$\frac{1}{p_j}+\frac{1}{p_j^2}+\cdots = \frac{1}{p_j-1}$$

以下である．

したがって，

$$g \geq 2^{\min\{l_2, 2(h-1)\}} \prod_{j=1}^{k} p_j^{\frac{1}{p_j-1}}$$

であり，証明できた． □

命題 4 の証明 素数定理に関連した次の式[1)] が成立する．ある定数 $C_1 > 0$ が存在し，$x \to \infty$ とするとき，

$$\sum_{p:prime \leq x} \frac{\log p}{p} = \log x + C_1$$

となる．各項は非負の値であるので，項をずらして比較することにより，ある定数 $C_2 > 0$ が存在し，

$$\sum_{5 \leq p:prime \leq x} \frac{\log p}{p-1} = \log x + C_2$$

となることが分かる．したがって，ある定数 $C_3 > 0$ が存在し，

$$\prod_{5 \leq p:prime \leq x} p^{\frac{1}{p-1}} = C_3 x$$

となる．

一方，素数定理[1)] により，x を超えない素数の数 $\pi(x)$ は，$x \to \infty$ とするとき，$\pi(x) \to x/(\log x)$ であるので，

$$\prod_{p:prime \leq x} p \geq \exp\left(\frac{x}{\log x}\right)$$

が成り立つ．そのため，

$$\prod_{p:prime \leq (\log x)^2} p \geq \exp\left(\frac{(\log x)^2}{\log(\log x)^2}\right) \geq x$$

となる．したがって，$x = p^n-1 = 2^{l_2}3^{l_3}\prod_{j=1}^{k} p_j^{l_{p_j}}$ とすると，$k \leq (\log x)^2$ となる．ゆえに，$p < p'$ のとき，

$$p^{\frac{1}{p-1}} > p'^{\frac{1}{p'-1}}$$

を考慮すると，ある定数 $C_4 > 0$ が存在し，

$$
\begin{aligned}
\prod_{j=1}^{k} p_j^{\frac{1}{p_j-1}} &\leq C_4 \prod_{5 \leq p:prime \leq (\log x)^2} p^{\frac{1}{p-1}} \\
&= C_4 C_3 (\log x)^2
\end{aligned}
$$

となり，命題が成り立つ． □

命題 5 の証明 命題 3 より，

$$p^n-1 \geq E(h) \geq (p^n-1)\Big/\left(2^{\min\{l_2, 2(h-1)\}}\prod_{j=1}^{k} p_j^{\frac{1}{p_j-1}}\right)$$

である．命題 4 より，

$$\prod_{j=1}^{k} p_j^{\frac{1}{p_j-1}} \leq c|p^n-1|^2$$

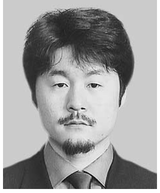
であるので，

$$E(h) \geq \frac{(p^n-1)}{\left(f(|p^n-1|)\cdot c|p^n-1|^2\right)}$$

となる．右辺の分母の値は $|p^n - 1|$ の多項式であるので，命題が成り立つ．□

Pentium は，Intel Corporation のアメリカ合衆国およびその他の国における登録商標です．

(平成 13 年 12 月 7 日受付)
(平成 14 年 6 月 4 日採録)



桶屋　勝幸（正会員）

1994 年富山大学理学部数学科卒業．1996 年九州大学大学院数理学研究科博士前期課程修了．1998 年（株）日立製作所入社．現在，システム開発研究所第 7 部（セキュリティシステム研究部）研究員．暗号，情報セキュリティ技術の研究に従事．電子情報通信学会，日本数学会，応用数理学会各会員

宮崎　邦彦

1996 年東京大学理学部数学科卒業．1998 年同大学大学院数理科学研究科修士課程修了．同年（株）日立製作所入社．現在，システム開発研究所第 7 部（セキュリティシステム研究部）に勤務．暗号，情報セキュリティ技術の研究に従事．電子情報通信学会会員．

櫻井　幸一（正会員）

1988 年九州大学工学研究科応用物理専攻修士課程修了．同年三菱電機（株）入社．現在，九州大学大学院システム情報科学研究院情報工学部門教授．1997 年 9 月より 1 年間コロンビア大学計算機科学科客員研究員．2001 年 4 月より九州大学システム LSI 研究センター併任．暗号理論・情報セキュリティ・社会情報工学の研究に従事．博士（工学）．2000 年情報処理学会酒井特別記念賞受賞．2000 年情報処理学会論文賞受賞．電子情報通信学会，日本数学会，ACM 各会員．