(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6777569号
(P6777569)
(45)発行日　令和2年10月28日(2020.10.28)　(24)登録日　令和2年10月12日(2020.10.12)

(51)Int.Cl.　F I
G09C 1/00 (2006.01)　G09C 1/00 650A

請求項の数 3　(全 12 頁)

(21)出願番号　特願2017-44529(P2017-44529)
(22)出願日　平成29年3月9日(2017.3.9)
(65)公開番号　特開2018-146903(P2018-146903A)
(43)公開日　平成30年9月20日(2018.9.20)
審査請求日　平成31年3月4日(2019.3.4)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町一丁目５番１号
(74)代理人　100121706
弁理士　中尾　直樹
(74)代理人　100128705
弁理士　中村　幸雄
(74)代理人　100147773
弁理士　義村　宗洋
(72)発明者　清村　優太郎
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内
(72)発明者　小林　鉄太郎
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】ペアリング演算装置、ペアリング演算方法、およびプログラム

(57)【特許請求の範囲】
【請求項１】
p，rを素数とし、kを埋め込み次数とし、dを正の整数とし、Eを楕円曲線とし、F_pを位数pの有限体とし、$F_{p^{(k/d)}}$を位数$p^{k/d}$の有限体とし、F_{p^k}を位数p^kの有限体とし、G_1を楕円曲線$E(F_p)$上の位数rの部分群とし、G_2を楕円曲線$E(F_{p^{(k/d)}})$上の位数rの部分群とし、G_3を有限体F_{p^k}上の位数rの部分群とし、eを$G_1 \times G_2 \rightarrow G_3$のペアリングとし、nを位数rを二進表現とした際の桁数とし、r_0，…，r_{n-1}を位数rを二進表現にしたときの各桁の値とし、
ECDBLを楕円曲線上の一点を入力とし、当該点を楕円曲線上で二倍算した点、および、値$\Lambda_n \in F_{p^{(k/d)}}$，$\lambda_d \in F_p$を出力とする、Compressed Jacobian座標系を用いて楕円曲線上の二倍算を演算するアルゴリズムとし、
ECADDを楕円曲線上の二点を入力とし、当該二点を楕円曲線上で加算した点、および、値$\Lambda_n \in F_{p^{(k/d)}}$，$\lambda_d \in F_p$を出力とする、Compressed Jacobian座標系を用いて楕円曲線上の加算を演算するアルゴリズムとし、
楕円曲線$E(F_p)$上の点$P=(x_P, y_P)$と楕円曲線$E(F_{p^{(k/d)}})$上の点$Q=(X_Q, Y_Q)$とのペアリングe(P，Q)を演算するペアリング演算装置であって、
値fに1を、点(X_1, Y_1, Z_1)に点$(X_Q, Y_Q, 1)$を代入する初期化部と、
点(X_1, Y_1, Z_1)を入力として上記アルゴリズムECDBLを演算し、点(X_1, Y_1, Z_1)を楕円曲線E上で二倍算した点(X_3, Y_3, Z_3)および上記値Λ_n，λ_dを得る楕円二倍算部と、
上記値f，Λ_n，λ_d，Z_3，点(x_P, y_P)，(X_1, Y_1, Z_1)を用いて、$L_{DBL} \leftarrow y_P Z_1^2 Z_3 + (-x_P \Lambda_n$

$Z_1^2+(\Lambda_n X_1-Y_1\lambda_d)$)，f←$f^2$・$L_{DBL}$を演算し、点($X_3$，$Y_3$，$Z_3$)を点($X_1$，$Y_1$，$Z_1$)に代入する二倍算部と、

点(X_1，Y_1，Z_1)，(X_Q，Y_Q，1)を入力として上記アルゴリズムECADDを演算し、点(X_1，Y_1，Z_1)と点(X_Q，Y_Q，1)とを楕円曲線E上で加算した点(X_3，Y_3，Z_3)および上記値Λ_n，λ_dを得る楕円加算部と、

上記値f，Λ_n，Z_3，点(x_P，y_P)，(X_Q，Y_Q，1)を用いて、L_{ADD}←$y_P Z_3+(-x_P\Lambda_n+(\Lambda_n X_Q-Y_Q Z_3))$，f←f・$L_{ADD}$を演算し、点($X_3$，$Y_3$，$Z_3$)を点($X_1$，$Y_1$，$Z_1$)に代入する加算部と、

$f^{(p\wedge k-1)/r}$を演算する最終冪演算部と、

を含み、

n-2から0までの各整数jについて、r_j=1のときは、上記楕円二倍算部と上記二倍算部と上記楕円加算部と上記加算部とを実行し、それ以外のときは、上記楕円二倍算部と上記二倍算部とを実行する、

ペアリング演算装置。

【請求項２】

p，rを素数とし、kを埋め込み次数とし、dを正の整数とし、Eを楕円曲線とし、F_pを位数pの有限体とし、$F_{p\wedge(k/d)}$を位数$p^{k/d}$の有限体とし、$F_{p\wedge k}$を位数p^kの有限体とし、G_1を楕円曲線E(F_p)上の位数rの部分群とし、G_2を楕円曲線E($F_{p\wedge(k/d)}$)上の位数rの部分群とし、G_3を有限体$F_{p\wedge k}$上の位数rの部分群とし、eを$G_1\times G_2\rightarrow G_3$のペアリングとし、nを位数rを二進表現とした際の桁数とし、r_0，…，r_{n-1}を位数rを二進表現にしたときの各桁の値とし、

ECDBLを楕円曲線上の一点を入力とし、当該点を楕円曲線上で二倍算した点、および、楕円曲線上の二倍算を演算する過程で計算される値$\Lambda_n\in F_{p\wedge(k/d)}$，$\lambda_d\in F_p$を出力とする、Compressed Jacobian座標系を用いて楕円曲線上の二倍算を演算するアルゴリズムとし、

ECADDを楕円曲線上の二点を入力とし、当該二点を楕円曲線上で加算した点、および、楕円曲線上の加算を演算する過程で計算される値$\Lambda_n\in F_{p\wedge(k/d)}$，$\lambda_d\in F_p$を出力とする、Compressed Jacobian座標系を用いて楕円曲線上の加算を演算するアルゴリズムとし、

初期化部と楕円二倍算部と二倍算部と楕円加算部と加算部と最終冪演算部とを含むペアリング演算装置が、楕円曲線E(F_p)上の点P=(x_P，y_P)と楕円曲線E($F_{p\wedge(k/d)}$)上の点Q=(X_Q，Y_Q)とのペアリングe(P，Q)を演算するペアリング演算方法であって、

初期化部が、値fに1を、点(X_1，Y_1，Z_1)に点(X_Q，Y_Q，1)を代入し、

楕円二倍算部が、点(X_1，Y_1，Z_1)を入力として上記アルゴリズムECDBLを演算し、点(X_1，Y_1，Z_1)を楕円曲線E上で二倍算した点(X_3，Y_3，Z_3)および上記値Λ_n，λ_dを得、

二倍算部が、上記値f，Λ_n，λ_d，Z_3，点(x_P，y_P)，(X_1，Y_1，Z_1)を用いて、L_{DBL}←$y_P Z_1^2 Z_3+(-x_P\Lambda_n Z_1^2+(\Lambda_n X_1-Y_1\lambda_d))$，f←$f^2$・$L_{DBL}$を演算し、点($X_3$，$Y_3$，$Z_3$)を点($X_1$，$Y_1$，$Z_1$)に代入し、

楕円加算部が、点(X_1，Y_1，Z_1)，(X_Q，Y_Q，1)を入力として上記アルゴリズムECADDを演算し、点(X_1，Y_1，Z_1)と点(X_Q，Y_Q，1)とを楕円曲線E上で加算した点(X_3，Y_3，Z_3)および上記値Λ_n，λ_dを得、

加算部が、上記値f，Λ_n，Z_3，点(x_P，y_P)，(X_Q，Y_Q，1)を用いて、L_{ADD}←$y_P Z_3+(-x_P\Lambda_n+(\Lambda_n X_Q-Y_Q Z_3))$，f←f・$L_{ADD}$を演算し、点($X_3$，$Y_3$，$Z_3$)を点($X_1$，$Y_1$，$Z_1$)に代入し、

最終冪演算部が、$f^{(p\wedge k-1)/r}$を演算し、

n-2から0までの各整数jについて、r_j=1のときは、上記楕円二倍算部と上記二倍算部と上記楕円加算部と上記加算部とを実行し、それ以外のときは、上記楕円二倍算部と上記二倍算部とを実行する、

ペアリング演算方法。

【請求項３】

請求項１に記載のペアリング演算装置としてコンピュータを機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】
【０００１】
この発明は、情報通信分野におけるペアリングを用いた暗号技術に関し、特に、ペアリングを効率的に演算する技術に関する。
【背景技術】
【０００２】
近年、楕円曲線上のペアリングが持つ双線形性によって、IDベース暗号（非特許文献１参照）や属性ベース暗号（非特許文献２参照）、関数型暗号（非特許文献３参照）などの高機能な暗号方式が提案されている。このようなペアリングを用いた暗号方式は、ペアリング暗号とも呼ばれる。近年では、Apache Milagro (incubating)（非特許文献４参照）でのオープンソースソフトウェア（OSS: Open Source Software）による開発や、インターネット技術タスクフォース（IETF: Internet Engineering Task Force）による標準化（非特許文献５、６参照）など、ペアリング暗号を実社会で利用するための活動が行われている。
【０００３】
楕円曲線上のペアリングは、Millerによって提案されたミラーアルゴリズム（Miller's Algorithm、非特許文献７参照）を用いて演算することができる。ミラーアルゴリズムでは、楕円曲線上の二点を通る直線または一点を通る接線であるＬ関数を構成する必要がある。Ｌ関数を構成する方法としては、Affine座標系／Jacobian座標系を用いた楕円曲線上の二倍算／加算において、演算途中で計算される傾きを用いて構成する方法が知られている（非特許文献８参照）。Affine座標系では逆元算を用い、Jacobian座標系では逆元算を用いないことが特徴であるため、計算機の乗算と逆元算の演算時間の比に応じて、これらの座標系を使い分ける。Affine座標系／Jacobian座標系以外の座標系には、Compressed Jacobian座標系（非特許文献９参照）があるが、この座標系を用いてＬ関数を構成する方法は知られていない。
【先行技術文献】
【非特許文献】
【０００４】
【非特許文献１】D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing", CRYPTO 2001, LNCS 2139, pp. 213-229, 2001.
【非特許文献２】A. Sahai and B. Waters, "Identity-Based Encryption", EUROCRYPT 2005, LNCS 3494, pp. 457-473, 2005.
【非特許文献３】T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption", CRYPTO 2010, LNCS 6223, pp. 191-208, 2010.
【非特許文献４】Apache Software Foundation、"MILAGRO"、［online］、［平成29年2月22日検索］、インターネット<URL: https://milagro.apache.org/>
【非特許文献５】RFC5091, "Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems", 2007.
【非特許文献６】RFC6508, "Sakai-Kasahara Key Encryption (SAKKE)", 2012.
【非特許文献７】V. S. Miller, "The Weil Pairing, and Its Efficient Calculation", Journal of Cryptology, vol. 17, pp. 235-261, 2004.
【非特許文献８】S. Chatterjee, P. Sarkar and R. Barua, "Efficient Computation of Tate Pairing in Projective Coordinate over General Characteristic Fields", ICISC 2004, LNCS 3506, pp. 168-181, 2005.
【非特許文献９】F. Hoshino, T. Kobayashi and K. Aoki, "Compressed Jacobian Coordinates for OEF", VIETCRYPT 2006, LNCS 4341, pp. 147-156, 2006.
【発明の概要】
【発明が解決しようとする課題】
【０００５】

ペアリング暗号を実際のシステムとして実現するためには、ペアリング演算を効率的に行うことが重要である。計算機の性能によっては、Compressed Jacobian座標系を用いた楕円曲線上の二倍算／加算が他の座標系よりも高速に演算できる場合がある。しかしながら、Compressed Jacobian座標系を用いてペアリング演算に必要なＬ関数を構成する方法は知られていなかった。

【０００６】

この発明の目的は、上記のような点に鑑みて、Compressed Jacobian座標系を用いてペアリング演算に必要なＬ関数を構成し、効率的にペアリングを演算することができる技術を実現することである。

【課題を解決するための手段】

【０００７】

上記の課題を解決するために、この発明のペアリング演算装置は、p，rを素数とし、kを埋め込み次数とし、dを正の整数とし、Eを楕円曲線とし、F_pを位数pの有限体とし、$F_{p^{(k/d)}}$を位数$p^{k/d}$の有限体とし、F_{p^k}を位数p^kの有限体とし、G_1を楕円曲線$E(F_p)$上の位数rの部分群とし、G_2を楕円曲線$E(F_{p^{(k/d)}})$上の位数rの部分群とし、G_3を有限体F_{p^k}上の位数rの部分群とし、eを$G_1 \times G_2 \rightarrow G_3$のペアリングとし、ECDBLを楕円曲線上の一点を入力とし、当該点を楕円曲線上で二倍算した点、および、楕円曲線上の二倍算を演算する過程で計算される値$\Lambda_n \in F_{p^{(k/d)}}$，$\lambda_d \in F_p$を出力とする、Compressed Jacobian座標系を用いて楕円曲線上の二倍算を演算するアルゴリズムとし、ECADDを楕円曲線上の二点を入力とし、当該二点を楕円曲線上で加算した点、および、楕円曲線上の加算を演算する過程で計算される値$\Lambda_n \in F_{p^{(k/d)}}$，$\lambda_d \in F_p$を出力とする、Compressed Jacobian座標系を用いて楕円曲線上の加算を演算するアルゴリズムとし、楕円曲線$E(F_p)$上の点$P=(x_P, y_P)$と楕円曲線$E(F_{p^{(k/d)}})$上の点$Q=(X_Q, Y_Q)$とのペアリング$e(P, Q)$を演算するペアリング演算装置であって、値fに1を、点(X_1, Y_1, Z_1)に点$(X_Q, Y_Q, 1)$を代入する初期化部と、点(X_1, Y_1, Z_1)を入力としてアルゴリズムECDBLを演算し、点(X_1, Y_1, Z_1)を楕円曲線E上で二倍算した点(X_3, Y_3, Z_3)および値Λ_n，λ_dを得る楕円二倍算部と、値f，Λ_n，λ_d，Z_3，点(x_P, y_P)，(X_1, Y_1, Z_1)を用いて、$L \leftarrow y_P Z_1^2 Z_3 + (-x_P \Lambda_n Z_1^2 + (\Lambda_n X_1 - Y_1 \lambda_d))$，$f \leftarrow f^2 \cdot L$を演算し、点$(X_3, Y_3, Z_3)$を点$(X_1, Y_1, Z_1)$に代入する二倍算部と、点$(X_1, Y_1, Z_1)$，$(X_Q, Y_Q, 1)$を入力としてアルゴリズムECADDを演算し、点$(X_1, Y_1, Z_1)$と点$(X_Q, Y_Q, 1)$とを楕円曲線E上で加算した点$(X_3, Y_3, Z_3)$および上記値$\Lambda_n$，$\lambda_d$を得る楕円加算部と、値f，$\Lambda_n$，$Z_3$，点$(x_P, y_P)$，$(X_Q, Y_Q, 1)$を用いて、$L \leftarrow y_P Z_3 + (-x_P \Lambda_n + (\Lambda_n X_Q - Y_Q Z_3))$，$f \leftarrow f \cdot L$を演算し、点$(X_3, Y_3, Z_3)$を点$(X_1, Y_1, Z_1)$に代入する加算部と、$f^{(p^k-1)/r}$を演算する最終冪演算部と、を含む。

【発明の効果】

【０００８】

この発明によれば、Compressed Jacobian座標系を用いてペアリング演算に必要なＬ関数を構成し、効率的にペアリングを演算することができる。

【図面の簡単な説明】

【０００９】

【図１】図１は、ペアリング演算装置の機能構成を例示する図である。

【図２】図２は、ペアリング演算方法の処理手続きを例示する図である。

【発明を実施するための形態】

【００１０】

以下、この発明の実施の形態について詳細に説明する。なお、図面中において同じ機能を有する構成部には同じ番号を付し、重複説明を省略する。

【００１１】

本明細書中で使用する、上付き添え字または下付き添え字の中で使用する記号「^」は、直後の文字を上付き添え字とすることを表す。例えば、$f^{(p^k-1)/r}$は、fを$(p^k-1)/r$乗することを表している。数式中においてはこれらの記号は本来の記法、すなわち上付き添え字の中での上付き添え字で記述する。例えば、$f^{(p^k-1)/r}$は、次式のように記述する。

【００１２】
【数１】
$$f^{(p^k-1)/r}$$

【００１３】
［準備］
実施形態の説明の前に、本明細書で用いる用語の概要を説明する。
【００１４】
＜ペアリング＞
p，rを素数とする。kを埋め込み次数とする。dを正の整数とする。Eを楕円曲線とする。F_pを位数pの有限体とする。$F_{p^{(k/d)}}$を位数$p^{k/d}$の有限体とする。F_{p^k}を位数p^kの有限体とする。G_1を楕円曲線$E(F_p)$上の位数rの部分群とする。G_2を楕円曲線$E(F_{p^{(k/d)}})$上の位数rの部分群とする。G_3を有限体F_{p^k}上の位数rの部分群とする。$f_{r,Q}$を有理関数とする。
【００１５】
群G_1，G_2，G_3に対して、ペアリングeを次のように定義する。
【００１６】
【数２】
$$e: G_1 \times G_2 \to G_3$$
$$(P,Q) \mapsto f_{r,Q}(P)^{\frac{p^k-1}{r}}$$

【００１７】
＜ミラーアルゴリズム＞
上記の有理関数$f_{r,Q}$は、上記非特許文献７に記載されているミラーアルゴリズムを用いて演算することができる。ミラーアルゴリズムをAlgorithm 1に示す。
【００１８】
【数３】
Algorithm 1: Miller's Algorithm

Input $P \in G_1, Q \in G_2, r = \sum_{i=0}^{n-1} r_i 2^i (n = \lfloor \log_2 r \rfloor, r_i \in \{0,1\})$

Output $f_{r,Q}(P) \in F_{p^k}$

1: $f \leftarrow 1, T \leftarrow Q$
2: **for** $i \leftarrow n-2$ **to** 0 **do**
3: $T' \leftarrow 2T$
4: $f \leftarrow f^2 \cdot L_{T,T}(P)$
5: $T \leftarrow T'$
6: **if** $r_i = \pm 1$ **then**
7: $T' \leftarrow T + Q$
8: $f \leftarrow f \cdot L_{T,Q}(P)$
9: $T \leftarrow T'$
10: **end if**
11: **end for**
12: **return** f

【００１９】
ミラーアルゴリズムのステップ３では、楕円曲線上の二倍算を演算する。ミラーアルゴリズムのステップ７では、楕円曲線上の加算を演算する。上述のとおり、楕円曲線上の演算を行う座標系には、Affine座標系、Jacobian座標系、Compressed Jacobian座標系の３つが知られている。以下、各座標系について説明する。なお、mはある正の整数である。

【００２０】
＜Affine座標系＞
Affine座標系は、下記参考文献１の79-82ページに詳しく記載されている。有限体F_{p^m}上で定義されるAffine座標系における楕円曲線E_Aは、$4a^3+27b^2 \neq 0$を満たすa，b$\in F_{p^m}$に対して、式（１）のとおり表現できる。
【００２１】
【数４】
$$E_A : y^2 = x^3 + ax + b \quad \cdots(1)$$
【００２２】
楕円曲線E_A上の点は、(x，y)$\in F_{p^m} \times F_{p^m}$と表現できる。Affine座標系では、この表現を用いて楕円曲線E_A上の二倍算／加算を行う。
【００２３】
〔参考文献１〕D. R. Hankerson, A. J. Menezes and S. A. Vanstone, "Guide to Elliptic Curve Cryptography", Springer, 2004.
【００２４】
＜Jacobian座標系＞
Jacobian座標系は、上記参考文献１の86-89ページに詳しく記載されている。有限体F_{p^m}上で定義されるJacobian座標系における楕円曲線E_Jは、X$\in F_{p^m}$，Y$\in F_{p^m}$，Z$\in F_{p^m}$に対して、上記式（１）を(x，y)=$(X/Z^2, Y/Z^3)$と置き換えることで、式（２）のとおり表現できる。
【００２５】
【数５】
$$E_J : Y^2 = X^3 + aXZ^4 + bZ^6 \quad \cdots(2)$$
【００２６】
楕円曲線E_J上の点は、(X，Y，Z)$\in F_{p^m} \times F_{p^m} \times F_{p^m}$と表現できる。Jacobian座標系では、この表現を用いて楕円曲線E_J上の二倍算／加算を行う。
【００２７】
＜Compressed Jacobian座標系＞
Compressed Jacobian座標系は、上記非特許文献９に詳しく記載されている。有限体F_{p^m}上で定義されるCompressed Jacobian座標系における楕円曲線E_{comJ}は、X$\in F_{p^m}$，Y$\in F_{p^m}$，z$\in F_p$に対して、上記式（１）を(x，y)=$(X/z^2, Y/z^3)$と置き換えることで、式（３）のとおり表現できる。
【００２８】
【数６】
$$E_{comJ} : Y^2 = X^3 + aXz^4 + bz^6 \quad \cdots(3)$$
【００２９】
楕円曲線E_{comJ}上の点は、(X，Y，z)$\in F_{p^m} \times F_{p^m} \times F_p$と表現できる。Compressed Jacobian座標系では、この表現を用いて楕円曲線E_{comJ}上の二倍算／加算を行う。
【００３０】
＜Ｌ関数＞
ミラーアルゴリズムのステップ４およびステップ８で用いられるＬ関数（$L_{T,T}(P)$，$L_{T,Q}(P)$）は、P=$(x_P, y_P)\in G_1$，T=$(x_T, y_T)\in G_2$，T'=$(x_{T'}, y_{T'})\in G_2$を通る直線の傾きλ$\in F_{p^m}$に対して、式（４）のとおり表現できる。
【００３１】
【数７】
$$L_{T,T'}(P) = (y_P - y_T) - \lambda(x_P - x_T) \quad \cdots(4)$$
【００３２】
Ｌ関数を演算するためには、ミラーアルゴリズムのステップ３およびステップ７で楕円曲線上の二倍算／加算を演算する中で計算される値λを用いる。Affine座標系、Jacobian座標系を用いた効率的なＬ関数の構成方法は知られているが、Compressed Jacobian座標

系を用いた効率的なＬ関数の構成方法は知られていない。

【００３３】

＜本発明によるミラーアルゴリズム＞

本発明によるCompressed Jacobian座標系を用いる楕円曲線上の二倍算／加算を用いたミラーアルゴリズムをAlgorithm 2に示す。

【００３４】

【数８】

Algorithm 2 : 本発明によるMiller's Algorithm

Input $P=(x_P,y_P)\in G_1, Q=(X_Q,Y_Q)\in G_2, r=\sum_{i=0}^{n-1} r_i 2^i (n=\lfloor \log_2 r \rfloor, r_i\in\{0,1\})$

Output $f_{r,Q}(P)\in G_3$

1: $f\leftarrow 1,(X_1,Y_1,Z_1)\leftarrow(X_Q,Y_Q,1)$
2: **for** $j\leftarrow n-2$ **to** 0 **do**
3: $((X_3,Y_3,Z_3),\Lambda_n,\lambda_d)\leftarrow ECDBL(X_1,Y_1,Z_1)$
4: $f\leftarrow DBL(f,\Lambda_n,\lambda_d,(x_P,y_P),(X_1,Y_1,Z_1),Z_3)$
5: $(X_1,Y_1,Z_1)\leftarrow(X_3,Y_3,Z_3)$
6: **if** $r_j=1$ **then**
7: $((X_3,Y_3,Z_3),\Lambda_n,\lambda_d)\leftarrow ECADD((X_1,Y_1,Z_1),(X_Q,Y_Q,1))$
8: $f\leftarrow ADD(f,\Lambda_n,(x_P,y_P),(X_Q,Y_Q,1),Z_3)$
9: $(X_1,Y_1,Z_1)\leftarrow(X_3,Y_3,Z_3)$
10: **end if**
11: **end for**
12: **return** f

【００３５】

ステップ３で実行するECDBLは、非特許文献９において提案されている、Compressed Jacobian座標系を用いて楕円曲線上の二倍算を演算するアルゴリズムである。アルゴリズムECDBLは、楕円曲線E上の一点を入力とし、当該点を楕円曲線E上で二倍した点、および、楕円曲線E上の二倍算を演算する過程で計算される値$\Lambda_n\in F_{p^{(k/d)}}$，$\lambda_d\in F_p$を出力する。

【００３６】

ステップ７で実行するECADDは、非特許文献９において提案されている、Compressed Jacobian座標系を用いて楕円曲線上の加算を演算するアルゴリズムである。アルゴリズムECADDは、楕円曲線E上の二点を入力とし、当該二点を楕円曲線E上で加算した点、および、楕円曲線E上の加算を演算する過程で計算される値$\Lambda_n\in F_{p^{(k/d)}}$，$\lambda_d\in F_p$を出力する。

【００３７】

ステップ４で実行するDBLは、値fと、ECDBLの出力する値Λ_n，λ_dと、点$P(x_P, y_P)$，点(X_1, Y_1, Z_1)と、点(X_3, Y_3, Z_3)のZ座標である値Z_3とを入力とし、更新された値fを出力する。アルゴリズムDBLをAlgorithm 3に示す。

【００３８】

【数９】

Algorithm 3: DBL

Input $f,(x_P,y_P)\in G_1,(X_1,Y_1,Z_1)\in G_2,\Lambda_n\in F_{p^{k/d}},\lambda_d\in F_p,Z_3\in F_p$

Output $f\in G_3$

1: $L_{DBL}\leftarrow y_P Z_1^2 Z_3+(-x_P\Lambda_n Z_1^2+(\Lambda_n X_1-Y_1\lambda_d))$

2: $f\leftarrow f^2\cdot L_{DBL}$

【００３９】

ステップ８で実行するADDは、値fと、ECADDの出力する値Λ_nと、点$P(x_P, y_P)$，点$(X_Q, Y_Q, 1)$と、点(X_3, Y_3, Z_3)のZ座標である値Z_3とを入力とし、更新された値fを出力する。

アルゴリズムADDをAlgorithm 4に示す。

【００４０】

【数１０】

Algorithm 4: ADD
Input $f, (x_P, y_P) \in G_1, (X_Q, Y_Q, 1) \in G_2, \Lambda_n \in F_{p^{k/d}}, Z_3 \in F_p$
Output $f \in G_3$
1: $L_{ADD} \leftarrow y_P Z_3 + (-x_P \Lambda_n + (\Lambda_n X_Q - Y_Q Z_3))$
2: $f \leftarrow f \cdot L_{ADD}$

【００４１】

［実施形態］

実施形態のペアリング演算装置１０は、図１に示すように、入力部１、初期化部２、ECDBL演算部３（楕円二倍算部とも呼ぶ）、DBL演算部４（二倍算部とも呼ぶ）、ECADD演算部５（楕円加算部とも呼ぶ）、ADD演算部６（加算部とも呼ぶ）、最終冪演算部７、および出力部８を備える。このペアリング演算装置１０が後述する各ステップの処理を行うことにより実施形態のペアリング演算方法が実現される。

【００４２】

ペアリング演算装置１０は、例えば、中央演算処理装置（CPU: Central Processing Unit）、主記憶装置（RAM: Random Access Memory）などを有する公知又は専用のコンピュータに特別なプログラムが読み込まれて構成された特別な装置である。ペアリング演算装置１０は、例えば、中央演算処理装置の制御のもとで各処理を実行する。ペアリング演算装置１０に入力されたデータや各処理で得られたデータは、例えば、主記憶装置に格納され、主記憶装置に格納されたデータは必要に応じて読み出されて他の処理に利用される。また、ペアリング演算装置１０の各処理部の少なくとも一部が集積回路等のハードウェアによって構成されていてもよい。

【００４３】

図２を参照して、実施形態のペアリング演算方法の処理手続きを説明する。

【００４４】

ステップＳ１において、入力部１へ楕円曲線E上の二点$P=(x_P, y_P)\in G_1$, $Q=(X_Q, Y_Q)\in G_2$、および群G_1, G_2の位数である素数rが入力される。なお、位数rは、式（５）に示すように、二進表現で入力されるものとする。

【００４５】

【数１１】

$$r=\sum_{i=0}^{n-1} r_i 2^i (n=\lfloor \log_2 r \rfloor, r_i \in \{0,1\}) \quad \cdots(5)$$

【００４６】

ステップＳ２において、初期化部２は、値fに1を代入し、Compressed Jacobian座標系の点(X_1, Y_1, Z_1)に点$(X_Q, Y_Q, 1)$を代入する。また、インデックスjをn-2に初期化する。nは、式（５）に示すとおり、位数rを二進表現とした際の桁数である。

【００４７】

ステップＳ３において、ECDBL演算部３は、点(X_1, Y_1, Z_1)を入力としてアルゴリズムECDBLを演算し、点(X_1, Y_1, Z_1)を楕円曲線E上で二倍算した点(X_3, Y_3, Z_3)、および、楕円曲線上の二倍算を演算する過程で計算される値Λ_n, λ_dを得る。

【００４８】

ステップＳ４において、DBL演算部４は、値f, Λ_n, λ_d, 点$P(x_P, y_P)$, (X_1, Y_1, Z_1), および点(X_3, Y_3, Z_3)のZ座標である値Z_3を入力としてアルゴリズムDBLを演算し、値fを更新する。また、DBL演算部４は、点(X_3, Y_3, Z_3)を点(X_1, Y_1, Z_1)に代入する。

【００４９】

ステップＳ５において、r_jが1と等しいか否かを判定する。$r_j=1$の場合（YES）、ステップＳ６、Ｓ７を実行する。$r_j\neq 1$の場合（NO）、ステップＳ６、Ｓ７を実行せず、ステップＳ８へ処理を進める。

【００５０】

ステップＳ６において、ECADD演算部５は、点(X_1, Y_1, Z_1), (X_Q, Y_Q, 1)を入力としてアルゴリズムECADDを演算し、点(X_1, Y_1, Z_1)と点(X_Q, Y_Q, 1)とを楕円曲線E上で加算した点(X_3, Y_3, Z_3)、および、楕円曲線上の加算を演算する過程で計算される値Λ_n, λ_dを得る。

【００５１】

ステップＳ７において、ADD演算部６は、値f, Λ_n, 点P(x_P, y_P), (X_Q, Y_Q, 1), および点(X_3, Y_3, Z_3)のZ座標である値Z_3を入力としてアルゴリズムADDを演算し、値fを更新する。また、ADD演算部６は、点(X_3, Y_3, Z_3)を点(X_1, Y_1, Z_1)に代入する。

【００５２】

ステップＳ８において、インデックスjが0を超えているか否かを判定する。j>0の場合（YES）、ステップＳ９においてj←j-1を計算し、すなわち、インデックスjをデクリメントし、ステップＳ３～Ｓ８の処理を再度実行する。j≦0の場合（NO）、ステップＳ１０へ処理を進める。

【００５３】

ステップＳ１０において、最終冪演算部７は、式（６）を計算し、ペアリング演算結果e(P, Q)を得る。

【００５４】

【数１２】

$$e(P,Q) \leftarrow f^{(p^k-1)/r} \quad \cdots(6)$$

【００５５】

ステップＳ１１において、出力部８は、ペアリング演算結果e(P, Q)を出力する。

【００５６】

［実験結果］

本発明の効果を実証するために、従来のミラーアルゴリズム（Algorithm 1）を用いたときの演算コストと、本発明によるミラーアルゴリズム（Algorithm 2）を用いたときの演算コストを比較した。以下では、Mを乗算の演算時間、Sを二倍算の演算時間、Iを逆元算の演算時間として、S=M, I=8Mとなる計算機を用いて、下記参考文献２に記載されたパラメータを用いてペアリングを演算する場合の高速化率を説明する。

【００５７】

〔参考文献２〕D. Aranha, K. Karabina, P. Longa, C. Gebotys and J. Lopez, "Faster Explicit Formulas for Computing Pairings over Ordinary Curves," EUROCRYPT 2011, LNCS 6632, pp. 48-68, 2011.

【００５８】

参考文献２に記載されたパラメータは、以下のとおりである。

【００５９】

【数１３】

$$E: y^2 = x^3 + 2$$

$$\chi = -(2^{62} + 2^{55} + 1)$$

$$p = 36z^4 + 36z^3 + 24z^2 + 6z + 1 \quad \cdots(7)$$

$$r = 36z^4 + 36z^3 + 18z^2 + 6z + 1$$

【００６０】

このとき、ω=|6z+2|とし、ある関数gに対するペアリングは、以下のように表される。

【００６１】

【数１４】

$$e(P,Q) = (f_{\omega,Q}(P) \cdot g)^{(p^{12}-1)/r} \quad \cdots(8)$$

【００６２】

なお、上述のミラーアルゴリズムではrを入力としてrを二進表現とした際の桁数だけル

ープしていたが、この実験ではループ回数をωに削減する一般的なテクニックを用いた。このテクニックは従来のミラーアルゴリズムでも本発明のミラーアルゴリズムでも同様に適用できるため、実験結果へは影響しない。

【００６３】

Jacobian座標系で従来のミラーアルゴリズム（Algorithm 1）を用いて$f_{\omega,Q}(P)$を演算すると、7164Mの演算時間が必要であった（Mは乗算一回の演算時間）。本発明によるミラーアルゴリズム（Algorithm 2）を用いて$f_{\omega,Q}(P)$を演算すると、6940Mの演算時間が必要であった。したがって、本発明によるミラーアルゴリズムを用いると、演算時間を3.2%削減できることがわかった。

【００６４】

以上、この発明の実施の形態について説明したが、具体的な構成は、これらの実施の形態に限られるものではなく、この発明の趣旨を逸脱しない範囲で適宜設計の変更等があっても、この発明に含まれることはいうまでもない。実施の形態において説明した各種の処理は、記載の順に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。

【００６５】

［プログラム、記録媒体］

上記実施形態で説明した各装置における各種の処理機能をコンピュータによって実現する場合、各装置が有すべき機能の処理内容はプログラムによって記述される。そして、このプログラムをコンピュータで実行することにより、上記各装置における各種の処理機能がコンピュータ上で実現される。

【００６６】

この処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、例えば、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等どのようなものでもよい。

【００６７】

また、このプログラムの流通は、例えば、そのプログラムを記録したDVD、CD-ROM等の可搬型記録媒体を販売、譲渡、貸与等することによって行う。さらに、このプログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することにより、このプログラムを流通させる構成としてもよい。

【００６８】

このようなプログラムを実行するコンピュータは、例えば、まず、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、一旦、自己の記憶装置に格納する。そして、処理の実行時、このコンピュータは、自己の記録媒体に格納されたプログラムを読み取り、読み取ったプログラムに従った処理を実行する。また、このプログラムの別の実行形態として、コンピュータが可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することとしてもよく、さらに、このコンピュータにサーバコンピュータからプログラムが転送されるたびに、逐次、受け取ったプログラムに従った処理を実行することとしてもよい。また、サーバコンピュータから、このコンピュータへのプログラムの転送は行わず、その実行指示と結果取得のみによって処理機能を実現する、いわゆるASP（Application Service Provider）型のサービスによって、上述の処理を実行する構成としてもよい。なお、本形態におけるプログラムには、電子計算機による処理の用に供する情報であってプログラムに準ずるもの（コンピュータに対する直接の指令ではないがコンピュータの処理を規定する性質を有するデータ等）を含むものとする。

【００６９】

また、この形態では、コンピュータ上で所定のプログラムを実行させることにより、本装置を構成することとしたが、これらの処理内容の少なくとも一部をハードウェア的に実現することとしてもよい。

【符号の説明】

【００７０】

１０　ペアリング演算装置
１　入力部
２　初期化部
３　ECDBL演算部
４　DBL演算部
５　ECADD演算部
６　ADD演算部
７　最終冪演算部
８　出力部

【図１】

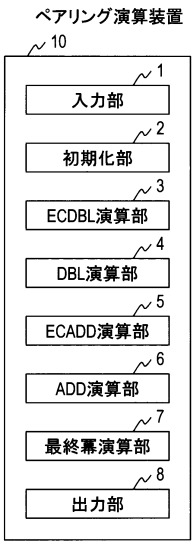

図1

【図２】

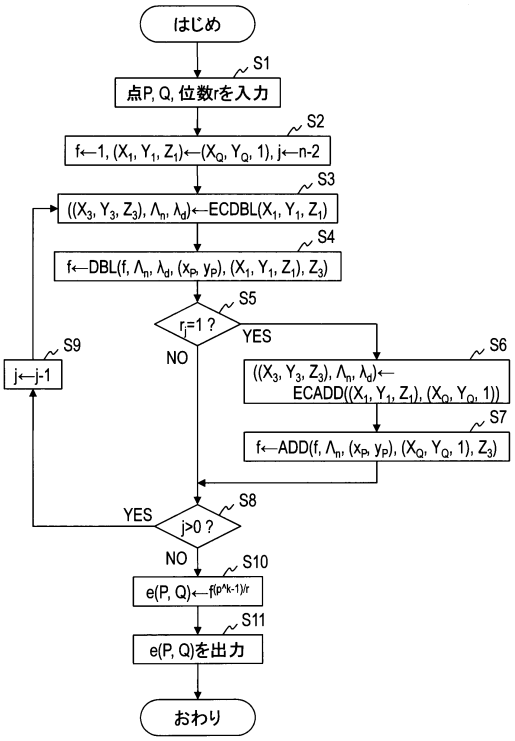

図2

フロントページの続き

(72)発明者　川原　祐人
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内

審査官　寺谷　大亮

(56)参考文献　特開２００６－３２３１６０（ＪＰ，Ａ）
Fumitaka Hoshino, Tetsutaro Kobayashi, and Kazumaro Aoki, “Compressed Jacobian Coordinates for OEF”, LNCS, ２００６年　9月, Vol.4341, p.147-156, Progress in Cryptology - VIETCRYPT 2006
小林鉄太郎, 青木和麻呂, 今井秀樹, “ペアリング高速実装”, ２００５年暗号と情報セキュリティシンポジウム　ＳＣＩＳ２００５　予稿集付録ＣＤ－ＲＯＭ, 日本, ２００５年　1月２５日, ３Ｆ４　ソフトウェア実装, ３Ｆ４－５

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０９Ｃ　　１／００