

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2012年2月2日(02.02.2012)



(10) 国際公開番号
WO 2012/015047 A1

- (51) 国際特許分類:
G06F 17/10 (2006.01) H04L 9/30 (2006.01)
- (21) 国際出願番号: PCT/JP2011/067520
- (22) 国際出願日: 2011年7月29日(29.07.2011)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2010-173065 2010年7月30日(30.07.2010) JP
特願 2010-173064 2010年7月30日(30.07.2010) JP
- (71) 出願人(米国を除く全ての指定国について): 国立大学法人岡山大学(NATIONAL UNIVERSITY CORPORATION OKAYAMA UNIVERSITY) [JP/JP]; 〒7008530 岡山県岡山市北区津島中一丁目1番1号 Okayama (JP).
- (72) 発明者; および
- (75) 発明者/出願人(米国についてのみ): 野上保之(NOGAMI Yasuyuki) [JP/JP]; 〒7008530 岡山県岡山市北区津島中三丁目1番1号 国立大学法人岡山大学大学院自然科学研究科内 Okayama (JP). 森川良孝(MORIKAWA Yoshitaka) [JP/JP]; 〒7008530 岡山県岡山市北区津島中三丁目1番1号 国立大学法人岡山大学大学院自然科学研

究科内 Okayama (JP). 出田哲也(IZUTA Tetsuya) [JP/JP]; 〒7008530 岡山県岡山市北区津島中三丁目1番1号 国立大学法人岡山大学工学部内 Okayama (JP).

- (74) 代理人: 松尾憲一郎(MATSUO Kenichiro); 〒8100042 福岡県福岡市中央区赤坂1丁目10番17号 しんくみ赤坂ビル7階 Fukuoka (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI

[続葉有]

(54) Title: PAIRING COMPUTATION AND SCALAR MULTIPLICATION OF EMBEDDING DEGREE 1 AND COMPOSITE ORDER RATIONAL POINT ON ELLIPTIC CURVE

(54) 発明の名称: 埋め込み次数1かつ合成数位数の楕円曲線上の有理点のスカラー倍算およびペアリング演算

[図5]

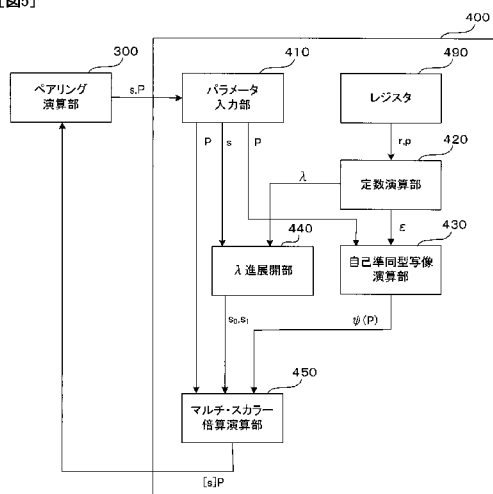


FIG. 5
300 PAIRING COMPUTATION UNIT
410 PARAMETER INPUT UNIT
420 CONSTANT COMPUTATION UNIT
430 ENDOMORPHISM MAP COMPUTATION UNIT
440 λ -ADIC DEVELOPMENT UNIT
450 MULTI-SCALAR MULTIPLICATION COMPUTATION UNIT
490 REGISTER

(57) Abstract: Pairing computation and scalar multiplication are efficiently performed on rational points that are embedding degree 1 and composite order and that are on an elliptic curve by means of using a subgroup defined by an endomorphism map.

(57) 要約: 埋め込み次数1かつ合成数位数の楕円曲線上の有理点について、自己準同型写像により定まる部分群を用いることにより、スカラー倍算およびペアリング演算を効率的に行う。

WO 2012/015047 A1



(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG). 添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：

埋め込み次数 1 かつ合成数位数の楕円曲線上の有理点のスカラー倍算およびペアリング演算

技術分野

[0001] 本発明は、有理点 P のスカラー倍算 $[s]P$ を行うスカラー倍算装置、スカラー倍算方法、及びスカラー倍算プログラム、並びにペアリング演算を高速に実行可能としたペアリング演算装置、ペアリング演算方法、及びペアリング演算プログラムに関する。特に、有理点群の埋め込み次数を 1 とした場合において、有理点 P のスカラー倍算 $[s]P$ を行うスカラー倍算装置、スカラー倍算方法、及びスカラー倍算プログラム、並びに有理点群の埋め込み次数を 1 とした場合において、ペアリング演算を高速に実行可能としたペアリング演算装置、ペアリング演算方法、及びペアリング演算プログラムに関する。

背景技術

[0002] 昨今、インターネットなどの電気通信回線を利用した情報ネットワーク技術が高度に発展し、インターネットによって様々な情報を取得するだけでなく、インターネットバンキングや行政機関への電子申請などのような各種のサービスが提供されてきている。

[0003] このようなサービスを利用する場合には、サービスの利用者が成りすましや架空の人間などではなく、適正な利用者であることを確認するための認証処理が必要であり、信頼性の高い認証方法として、公開鍵と秘密鍵を用いる公開鍵暗号をベースとした電子認証技術がよく利用されている。

[0004] しかしながら、公開鍵暗号方式の電子認証では、公開鍵あるいは秘密鍵が漏洩した場合には直ちに公開鍵と秘密鍵を変更する必要がある、公開鍵及び秘密鍵の管理を慎重に行わなければならないとともに、必要に応じて新たな公開鍵と秘密鍵の設定登録作業が生じるという煩雑さがあるため、最近では

、利用者の氏名やメールアドレスのように利用者特有のIDを用いて電子認証を行うIDベース暗号が用いられることが多くなっている。

[0005] また、電子認証を行う認証装置によって利用者の個人認証を行った場合には、認証装置に利用者ごとの履歴が蓄積されることとなり、この履歴情報自体が利用者の個人情報であって、最近では、この履歴情報が漏洩することによる個人情報の漏洩のおそれが指摘されている。

[0006] そこで、認証装置では利用者の個人情報を利用して認証を行うのではなく、複数の利用者をひとまとまりのグループとして、このグループに所属していることを示すグループ署名を用いることにより、利用者を特定することなく認証を行うことによって、認証装置に個人情報が蓄積されることなく認証を可能としたグループ署名技術が提案されている。

[0007] 国家UNS戦略プログラムにおいても、プライバシーを保護しつつユーザ認証を行うことのできる匿名認証技術の重要性、必要性が取り上げられている。

UNS:Universal Communications、New Generation Networks、Security and safety

[0008] このようなIDベース暗号やグループ署名等を簡便に実現するための数学的な土台としてペアリング暗号がある。ペアリングとは、楕円曲線上で定義される2入力1出力の関数であり、入力は楕円曲線上の2つの有理点、出力は有限体の元が用いられている。このペアリングは2入力に対して双線形性を持つ。すなわち、例えば、 P を素体 F_p 上で定義される楕円曲線上の有理点、 Q を k 次拡大体 F_{p^k} 上で定義される楕円曲線上の有理点として、 P と Q を入力して拡大体 $F_{p^k}^*$ の元 z が出力されるとき、 a 倍の P と b 倍の Q を入力すると z の ab 乗が出力される。ペアリング暗号ではこの双線形性を利用して暗号システムを構築する。なお、ここで「 k 」を埋め込み次数と呼び「 $F_{p^k}^*$ 」は、位数が p^k である有限体（拡大体）から単位元 0 を除いた乗法群を表わす。

[0009] 楕円曲線上の有理点とは、楕円曲線 $y^2 = x^3 + ax + b$ を満たす有限体 F_q の元の座標 (x, y) の組をいう。この集合に無限遠点 0 を加えたものは加法群を成し、 $E(F_q)$ と表わす。すなわち、楕円曲線上の2つの有理点 P 、 Q を通る直線が

楕円曲線と交わる点の x 軸を対称とした点を R とすれば、 $P+Q=R$ が成立する。

この演算を楕円加算と呼ぶ。PとQが同一点の場合はPを通る接線が楕円曲線と交わる点のx軸を対称とした点をRとすれば、 $P+P=2P=R$ が成立する。この演算を楕円2乗算と呼ぶ。ペアリング暗号及び楕円暗号の安全性の根拠は楕円曲線上の離散対数問題の求解困難性に基いている。素因数分解の困難性を安全性の根拠とするRSA暗号等と比べ、はるかに短い鍵長で同等の暗号強度（安全性強度）を実現できる。

[0010] このような楕円曲線上の有理点のペアリング演算は、ミラーのアルゴリズムを用いて演算するステップとその演算結果に対してべき乗算を行うステップで構成されている。

[0011] デジタルグループ署名では、グループに所属する個人ユーザのアクセス権の認証処理を行う際に、アクセス権が失効している個人ユーザを除外するためのペアリング演算を行った後に所定の個人ユーザのペアリング演算を行って認証処理を行うことにより、個人ユーザごとのアクセス権の発行または失効の属性変更に柔軟に対応可能としている。

[0012] したがって、例えば、10,000人の個人ユーザで構成されるグループのデジタルグループ署名の場合、アクセス権が失効している個人ユーザが100人いれば、100回のペアリング演算が必要となっており、現時点での一般的な電子計算機による1回のペアリング演算に約0.1秒を要していることから、100回のペアリング演算には約10秒を要することになってしまうため、実用上、個人ユーザの数が制限されることとなって、広く利用されるものとはなっていなかった。

[0013] そこで、ペアリング演算の演算速度を向上させることによりデジタルグループ署名の実用性を向上させるために、例えば、ペアリング演算として楕円曲線上で定義されるTateペアリング演算法を用い、演算負荷を低減させて高速化を図る技術が提案されている（例えば、特許文献1、非特許文献1参照）。

「0014」 また、IDベース暗号における暗号化あるいは復号の処理や、グループ署名

における認証処理では、できるだけ短時間に実行することが求められる。特にペアリングに基づく暗号方式などにおいてはスカラー倍算が数多く実行されているためスカラー倍算を高速に実行することも求められている。

[0015] スカラー倍算の高速化手法として、バイナリー法やWindow法が知られている。

また、自己準同型写像を利用することにより、演算回数を削減して高速化を図る手法も提案されている（例えば、非特許文献2、特許文献2参照。）。

[0016] このように、これまでペアリングを用いた暗号方式（IDベース暗号、グループ署名等）は数多く提案され、また、それを高速に実行するために大きな割合を占めるスカラー倍算の高速化手法も数多く提案されているが、その多くは、160ビット以上の素数位数を持つペアリング曲線（ペアリングに効率のよい楕円曲線）を用いるものである。本発明者らはこれまで、土台の数学的構造から、拡大体における計算、楕円曲線暗号の計算、ペアリング計算について出願を行ってきた。そのいずれもが、素数位数のペアリング暗号を効率化するものである。

[0017] 一方、近年、有理点群の埋め込み次数が1で2000ビットを超える合成数位数（ $r=2^{2000}$ ）を持つペアリング曲線を用いるものが提案されており、また新たなアプリケーションも提案されている（例えば、非特許文献3参照。）。

[0018] 素数位数のペアリング暗号を効率化するこれまでの手法は、本発明がターゲットとする大きな合成数位数のペアリングに対して即座に適用できるものではない。言い換えれば、合成数位数のペアリング曲線は埋め込み次数が1となるなど特殊な状況におかれるため、これを考慮した新たな高速化手法を提案する必要性がでてきた。埋め込み次数を1とする理由は、ペアリング暗号の暗号強度を必要十分に確保するための強度と効率のバランスを図るのに最も適しているのが埋め込み次数1だからである。埋め込み次数を大きくした場合は暗号強度が十分すぎ、また実現する上での効率が悪くなる。

[0019] しかしながら、有理点群の埋め込み次数を1とし合成数位数を用いるアプリケーションに用いるためのペアリング曲線の生成法や、ペアリング計算や

スカラー倍算の効率化手法等は未だ十分ではない。

先行技術文献

特許文献

[0020] 特許文献1：特開 2 0 0 5 - 3 1 6 2 6 7 号公報

特許文献2：特開 2 0 0 4 - 2 7 1 7 9 2 号公報

非特許文献

[0021] 非特許文献1：K.Takashima, “Scaling Security of Elliptic Curves with Fast Pairing Using Efficient Endomorphisms” , IEICE, vol.90-A, no.1, Jan 2007

非特許文献2：R. Gallant, R. Lambert, and S. Vanstone, “Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms”

非特許文献3：D. Boneh, K. Rubin and A. Silverberg, “Finding Composite Order Ordinary Elliptic Curves Using the Cock-Pinch method”

発明の開示

発明が解決しようとする課題

[0022] 従来、有理点群の埋め込み次数が1でない場合には、2つの有理点部分群 G_1 , G_2 を簡便に識別できたため、それらを用いてGLV (Gallant-Lambert-Vanstone) 法 (スカラー倍算の高速化手法) やXateペアリング (ペアリングの高速化手法) を適用することができた。

[0023] しかしながら、有理点群の埋め込み次数を1とした場合、従来のように効率的にスカラー倍算やペアリング計算を行うことができる有理点の部分群を特定する方法がこれまで知られていなかった。そこで、そのような特殊な条件、すなわち、素体上でスカラー倍算を効率的に行えるような有理点だけから成る部分群を識別、特定する必要があった。そして、現在提案されているスカラー倍算及びペアリング演算の高速化は未だに十分ではなく、さらなる高速化が求められている。

[0024] 本発明者らは、このような現状に鑑み、有理点群の埋め込み次数を1とし

大きな合成数位数を持つペアリング曲線におけるスカラー倍算及びペアリング演算を高速化することにより実用性を向上させるべく研究開発を行って、本発明を成すに至ったものである。

課題を解決するための手段

[0025] 本発明のスカラー倍算装置では、

標数 p の有限体 F_p 上で定義された楕円曲線上の有理点の成す加法群を $E(F_p)$ とし、合成数位数 r を持つ有理点の集合すなわち前記加法群の部分群を $G = E(F_p)[r]$ として、有理点 $P \in G$ の整数 $0 < s < r$ によるスカラー倍算 $[s]P$ を演算するCPU及び記憶手段を備えたスカラー倍算装置において、

前記加法群 $E(F_p)$ は、埋め込み次数を 1 とし、

前記CPUは、

有理点 $P' \in E(F_p)[r]$ 、前記整数 s 、をそれぞれ入力して前記記憶手段に記憶する入力手段と、

前記記憶手段から前記有理点 P' を読み出し、自己準同型写像 $\phi(P) = \lambda P$ (λ は整数) を満足する前記有理点 P の集合である前記部分群 G を特定し、前記有理点 P を前記記憶手段に記憶する有理点部分群特定手段と、

前記記憶手段から前記有理点 P を読み出し、前記自己準同型写像 $\phi(P)$ を演算し、その結果の有理点を前記記憶手段に記憶する自己準同型写像演算手段と、

、

前記記憶手段から前記整数 s を読み出し、次式に基づいて λ を展開し、

$$s = s_0 + s_1 \lambda$$

係数 s_0 及び s_1 を求めその結果を前記記憶手段に記憶する λ を展開手段と、

スカラー倍算を、

$$[s]P = [s_0 + s_1 \lambda]P = [s_0]P + [s_1] \phi(P)$$

として演算し、その結果を前記記憶手段に記憶するマルチ・スカラー倍算演算手段と、を有することとした。

[0026] さらに、本発明のスカラー倍算装置では、

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $3 \nmid (p-1)$ であり、

前記合成数位数 r は、 $r \nmid \#E(F_p)$, $3 \mid (r-1)$ を満たし、

前記整数 λ は、 $\lambda^2 + \lambda + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$(x, y) \rightarrow (\varepsilon x, y)$, $\varepsilon^3 = 1$, $\varepsilon (\neq 1) \in F_p$ であることにも特徴を有するものである。

[0027] さらに、本発明のスカラー倍算装置では、

前記楕円曲線は、 $E: y^2 = x^3 + ax$, $a \in F_p$, $4 \mid (p-1)$ であり、

前記合成数位数 r は、 $r \nmid \#E(F_p)$, $4 \mid (r-1)$ を満たし、

前記整数 λ は、 $\lambda^2 + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$(x, y) \rightarrow (-x, \zeta y)$, $\zeta^4 = 1$, $\zeta, \zeta^2 (\neq 1) \in F_p$ であることにも特徴を有するものである。

[0028] さらに、本発明のスカラー倍算装置では、

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $6 \mid (p-1)$ であり、

前記合成数位数 r は、 $r \nmid \#E(F_p)$, $3 \mid (r-1)$ を満たし、

前記整数 λ は、 $\lambda^2 - \lambda + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$(x, y) \rightarrow (\varepsilon x, -y)$, $\varepsilon^3 = 1$, $\varepsilon (\neq 1) \in F_p$ であることにも特徴を有するものである。

[0029] 本発明のスカラー倍算方法では、

標数 p の有限体 F_p 上で定義された楕円曲線上の有理点の成す加法群を $E(F_p)$ と

し、合成数位数 r を持つ有理点の集合すなわち前記加法群の部分群を $G = E(F_p)[r]$

として、有理点 $P \in G$ の整数 $0 < s < r$ によるスカラー倍算 $[s]P$ を、CPU 及び記憶手段を備えた電子計算機で演算するスカラー倍算方法において、

前記加法群 $E(F_p)$ は、埋め込み次数を 1 とし、

前記電子計算機の CPU を入力手段として機能させて、有理点 $P' \in E(F_p)[r]$ 、前

記整数 s 、をそれぞれ入力して前記記憶手段に記憶する入力ステップと、

前記電子計算機の CPU を有理点部分群特定手段として機能させて、前記記憶手

段から P' を読み出し、自己準同型写像 $\phi(P) = \lambda P$ (λ は整数)を満足する前記有理点 P の集合である前記部分群 G を特定し、前記有理点 P を前記記憶手段に記憶する有理点部分群特定ステップと、

前記電子計算機のCPUを自己準同型写像演算手段として機能させて、前記記憶手段から前記有理点 P を読み出し、前記自己準同型写像 $\phi(P)$ を演算しその結果の有理点を前記記憶手段に記憶する自己準同型写像演算ステップと、

前記電子計算機のCPUを λ 進展開手段として機能させて、前記記憶手段から前記整数 s を読み出し次式に基づいて λ 進展開し、

$$s = s_0 + s_1 \lambda$$

係数 s_0 及び s_1 を求めその結果を前記記憶手段に記憶する λ 進展開ステップと、

、

前記電子計算機のCPUをスカラー倍算演算手段として機能させて、スカラー倍算を、

$$[s]P = [s_0 + s_1 \lambda]P = [s_0]P + [s_1] \phi(P)$$

として演算しその結果を前記記憶手段に記憶するマルチ・スカラー倍算演算ステップと、を有することとした。

[0030] さらに、本発明のスカラー倍算方法では、

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $3 \nmid (p-1)$ であり、

前記合成数位数 r は、 $r \nmid \#E(F_p)$, $3 \mid (r-1)$ を満たし、

前記整数 λ は、 $\lambda^2 + \lambda + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$(x, y) \rightarrow (\varepsilon x, y)$, $\varepsilon^3 = 1$, $\varepsilon (\neq 1) \in F_p$ であることにも特徴を有するものである。

[0031] さらに、本発明のスカラー倍算方法では、

前記楕円曲線は、 $E: y^2 = x^3 + ax$, $a \in F_p$, $4 \nmid (p-1)$ であり、

前記合成数位数 r は、 $r \nmid \#E(F_p)$, $4 \mid (r-1)$ を満たし、

前記整数 λ は、 $\lambda^2 + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$(x, y) \rightarrow (-x, \zeta y), \zeta^4=1, \zeta, \zeta^2 (\neq 1) \in F_p$ であることにも特徴を有するものである。

[0032] さらに、本発明のスカラ倍算方法では、

前記楕円曲線は、 $E: y^2 = x^3 + b, b \in F_p, 6 \nmid (p-1)$ であり、

前記合成数位数 r は、 $r \nmid \#E(F_p), 3 \nmid (r-1)$ を満たし、

前記整数 λ は、 $\lambda^2 - \lambda + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$(x, y) \rightarrow (\varepsilon x, -y), \varepsilon^3=1, \varepsilon (\neq 1) \in F_p$ であることにも特徴を有するものである。

[0033] 本発明のスカラ倍算プログラムでは、

標数 p の有限体 F_p 上で定義された楕円曲線上の有理点の成す加法群を $E(F_p)$ とし、合成数位数 r を持つ有理点の集合すなわち前記加法群の部分群を $G=E(F_p)[r]$ として、

有理点 $P \in G$ の整数 $0 < s < r$ によるスカラ倍算 $[s]P$ を、CPU 及び記憶手段を備えた電子計算機に演算させるスカラ倍算プログラムにおいて、

前記加法群 $E(F_p)$ は、埋め込み次数を 1 とし、

前記電子計算機の CPU を、

有理点 $P' \in E(F_p)[r]$ 、前記整数 s をそれぞれ入力し、前記記憶手段に記憶する入力手段、前記記憶手段から P' を読み出し自己準同型写像 $\phi(P) = \lambda P$ を満足する前記有理点 P の集合である前記部分群 G を特定し、前記有理点 P を前記記憶手段に記憶する有理点部分群特定手段、

前記記憶手段から前記有理点 P を読み出し、自己準同型写像 $\phi(P)$ を演算しその結果の有理点を前記記憶手段に記憶する自己準同型写像演算手段、

前記記憶手段から前記整数 s を読み出し、次式に基づいて λ 進展開し、

$$s = s_0 + s_1 \lambda$$

係数 s_0 及び s_1 を求めその結果を前記記憶手段に記憶する λ 進展開手段、

スカラ倍算を、

$$[s]P = [s_0 + s_1 \lambda]P = [s_0]P + [s_1] \phi(P)$$

として演算し、その結果を前記記憶手段に記憶するマルチ・スカラ倍算演

算手段、

として機能させることとした。

[0034] さらに、本発明のスカラー倍算プログラムでは、
 前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $3 \mid (p-1)$ であり、
 前記合成数位数 r は、 $r \mid \#E(F_p)$, $3 \mid (r-1)$ を満たし、
 前記整数 λ は、 $\lambda^2 + \lambda + 1 \equiv 0 \pmod{r}$ を満たし、
 前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、
 $(x, y) \rightarrow (\varepsilon x, y)$, $\varepsilon^3 = 1$, $\varepsilon (\neq 1) \in F_p$ であることにも特徴を有するものである。

[0035] さらに、本発明のスカラー倍算プログラムでは、
 前記楕円曲線は、 $E: y^2 = x^3 + ax$, $a \in F_p$, $4 \mid (p-1)$ であり、
 前記合成数位数 r は、 $r \mid \#E(F_p)$, $4 \mid (r-1)$ を満たし、
 前記整数 λ は、 $\lambda^2 + 1 \equiv 0 \pmod{r}$ を満たし、
 前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、
 $(x, y) \rightarrow (-x, \zeta y)$, $\zeta^4 = 1$, $\zeta, \zeta^2 (\neq 1) \in F_p$ であることにも特徴を有するものである。

[0036] さらに、本発明のスカラー倍算プログラムでは、
 前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $6 \mid (p-1)$ であり、
 前記合成数位数 r は、 $r \mid \#E(F_p)$, $3 \mid (r-1)$ を満たし、
 前記整数 λ は、 $\lambda^2 - \lambda + 1 \equiv 0 \pmod{r}$ を満たし、
 前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、
 $(x, y) \rightarrow (\varepsilon x, -y)$, $\varepsilon^3 = 1$, $\varepsilon (\neq 1) \in F_p$ であることにも特徴を有するものである。

[0037] 本発明のペアリング演算装置では、
 標数 p の有限体 F_p 上で定義された楕円曲線上の有理点の成す加法群を $E(F_p)$ とし、合成数位数 r を持つ有理点の集合すなわち前記加法群の部分群を $G_1 = E(F_p)[r]$ 、 $G_2 = E(F_p)[r]$ として、次式により、

$$e: G_1 \times G_2 \rightarrow F_p^* / (F_p^*)^r$$

である非退化な双線形写像としてペアリング e を定義し、
有理点 $P(x_p, y_p) \in G_1$ 及び $Q(x_q, y_q) \in G_2$ 、ミラーのアルゴリズムを用いて計算される有理関数を f として、ペアリング $e(P, Q)$ を演算するCPU及び記憶手段を備えたペアリング演算装置において、

前記加法群 $E(F_p)$ は、埋め込み次数を1とし、

前記CPUは、

有理点 P' を前記記憶手段に入力する入力手段と、

前記記憶手段から前記有理点 P' を読み出し、自己準同型写像 ϕ により、

$\lambda_1 P = \phi(P)$ 、 $\lambda_2 Q = \phi(Q)$ ($\lambda_1 \neq \lambda_2$ は整数)を満足する前記有理点 P 及び Q の

集合である前記部分群 G_1 及び G_2 を特定する有理点部分群特定手段と、

前記記憶手段から前記有理点 P または Q を読み出し、前記自己準同型写像 $\phi(P)$

または $\phi(Q)$ を演算しその結果の有理点を前記記憶手段に記憶する自己準同型写像演算手段と、

前記 f を演算する第1演算手段と、

所定の有理点を通る直線及び垂線の前記有理点 Q における値を演算する第2演算手段と、

前記 f と前記値を用いて $f'_{r,p}(Q)$ を演算する第3演算手段と、

前記 $f'_{r,p}(Q)$ を用いて前記ペアリング $e(P, Q)$ を

[数13]

$$e(P, Q) = f'_{r,p}(Q)^{(p-1)/r}$$

として演算する第4演算手段と

を有することとした。

[0038] さらに、本発明のペアリング演算装置では、

前記楕円曲線は、 $E: y^2 = x^3 + ax$, $a \in F_p$, $4 \nmid (p-1)$ であり、

前記合成数位数 r は、 $r \mid \#E(F_p)$, $4 \nmid (r-1)$ を満たし、

前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$$(x, y) \rightarrow (-x, \zeta y), \zeta^4 = 1, \zeta, \zeta^2 (\neq 1) \in F_p \text{ であり、}$$

前記 $f'_{r,p}(Q)$ は、

[数14]

$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2+1,p}(Q) \\ &= f_{\lambda_1^2,p}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_1,p}(Q)^{\lambda_1} \cdot f_{\lambda_1,\psi(P)}(Q) \cdot (x_Q - x_P) \end{aligned}$$

であることにも特徴を有するものである。

[0039] さらに、本発明のペアリング演算装置では、

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $3 \mid (p-1)$ であり、

前記合成数位数 r は、 $r \mid \#E(F_p)$, $3 \mid (r-1)$ を満たし、

前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 + \lambda_1 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 + \lambda_2 + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$$(x, y) \rightarrow (\varepsilon x, y), \quad \varepsilon^3 = 1, \quad \varepsilon (\neq 1) \in F_p \quad \text{であり、}$$

前記 $f'_{r,p}(Q)$ は、

[数15]

$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2 + \lambda_1 + 1, p}(Q) \\ &= f_{\lambda_1, p}(Q)^{\lambda_1 + 1} \cdot f_{\lambda_1 + 1, \psi(P)}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_1, p}(Q) \cdot f_{\lambda_1, p}(Q)^{\lambda_1} \cdot f_{\lambda_1, \psi(P)}(Q) \cdot l_{[\lambda_1]\psi(P), \psi(P)}(Q) \end{aligned}$$

であることにも特徴を有するものである。

[0040] さらに、本発明のペアリング演算装置では、

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $6 \mid (p-1)$ であり、

前記合成数位数 r は、 $r \mid \#E(F_p)$, $3 \mid (r-1)$ を満たし、

前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 - \lambda_1 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 - \lambda_2 + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$$(x, y) \rightarrow (\varepsilon x, -y), \quad \varepsilon^3 = 1, \quad \varepsilon (\neq 1) \in F_p \quad \text{であり、}$$

前記 $f'_{r,p}(Q)$ は、

[数16]

$$\begin{aligned}
 f'_{r,P}(Q) &= f_{\lambda_1^2 - \lambda_1 + 1, P}(Q) \\
 &= f_{\lambda_1, P}(Q)^{\lambda_1 - 1} \cdot f_{\lambda_1 - 1, \psi(P)}(Q) \cdot (x_Q - x_P) \\
 &= \left\{ f_{\lambda_1 - 1, P}(Q) \cdot \frac{l_{[\lambda_1 - 1]P, P}(Q)}{v_{[\lambda_1 - 1]P + P}(Q)} \right\}^{\lambda_1 - 1} \\
 &\quad \cdot f_{\lambda_1 - 1, \psi(P)}(Q) \cdot (x_Q - x_P)
 \end{aligned}$$

であることにも特徴を有するものである。

[0041] 本発明のペアリング演算方法では、

標数 p の有限体 F_p 上で定義された楕円曲線上の有理点の成す加法群を $E(F_p)$ とし、合成数位数 r を持つ有理点の集合すなわち前記加法群の部分群を $G_1 = E(F_p)[r]$ 、 $G_2 = E(F_p)[r]$ として、次式により、

$$e: G_1 \times G_2 \rightarrow F_p^* / (F_p^*)^r$$

である非退化な双線形写像としてペアリング e を定義し、

有理点 $P(x_P, y_P) \in G_1$ 及び $Q(x_Q, y_Q) \in G_2$ 、ミラーのアルゴリズムを用いて計算される有理関数を f として、CPU 及び記憶手段を備えた電子計算機でペアリング $e(P, Q)$ を演算するペアリング演算方法において、

前記加法群 $E(F_p)$ は、埋め込み次数を 1 とし、

前記電子計算機の CPU を入力手段として機能させて、有理点 P' を入力し記憶手段に記憶するステップと、

前記電子計算機の CPU を有理点部分群特定手段として機能させて、前記記憶手段から前記有理点 P' を読み出し、自己準同型写像 ϕ により、

$\lambda_1 P = \phi(P)$ 、 $\lambda_2 Q = \phi(Q)$ ($\lambda_1 \neq \lambda_2$ は整数) を満足する前記有理点 P 及び Q の集合である前記部分群 G_1 及び G_2 を特定するステップと、

前記電子計算機の CPU を自己準同型写像演算手段として機能させて、前記記憶手段から前記有理点 P または Q を読み出し、前記自己準同型写像 $\phi(P)$ または $\phi(Q)$ を演算しその結果の有理点を前記記憶手段に記憶する自己準同型写像演算ステップと、

前記電子計算機の CPU を第 1 演算手段として機能させて、前記 f を演算する第 1 演算ステップと、

前記電子計算機のCPUを第2演算手段として機能させて、所定の有理点を通る直線及び垂線の前記有理点Qにおける値を演算する第2演算ステップと、
前記電子計算機のCPUを第3演算手段として機能させて、前記 f と前記値を用いて $f'_{r,p}(Q)$ を演算する第3演算ステップと、
前記電子計算機のCPUを第4演算手段として機能させて、前記 $f'_{r,p}(Q)$ を用いて前記ペアリング $e(P, Q)$ を

[数17]

$$e(P, Q) = f'_{r,p}(Q)^{(p-1)/r}$$

として演算する第4演算ステップと、
を有することとした。

[0042] さらに本発明のペアリング演算方法では、

前記楕円曲線は、 $E: y^2 = x^3 + ax$, $a \in F_p$, $4 \nmid (p-1)$ であり、
前記合成数位数 r は、 $r \nmid \#E(F_p)$, $4 \mid (r-1)$ を満たし、
前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 + 1 \equiv 0 \pmod{r}$ を満たし、
前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$$(x, y) \rightarrow (-x, \zeta y), \zeta^4 = 1, \zeta, \zeta^2 (\neq 1) \in F_p \text{ であり、}$$

前記 $f'_{r,p}(Q)$ は、

[数18]

$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2+1,p}(Q) \\ &= f_{\lambda_1^2,p}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_1,p}(Q)^{\lambda_1} \cdot f_{\lambda_1,\psi(P)}(Q) \cdot (x_Q - x_P) \end{aligned}$$

であることにも特徴を有するものである。

[0043] さらに本発明のペアリング演算方法では、

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $3 \mid (p-1)$ であり、
前記合成数位数 r は、 $r \nmid \#E(F_p)$, $3 \mid (r-1)$ を満たし、
前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 + \lambda_1 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 + \lambda_2 + 1 \equiv 0 \pmod{r}$ を満たし、
前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$$(x, y) \rightarrow (\varepsilon x, y), \varepsilon^3 = 1, \varepsilon (\neq 1) \in F_p \text{ であり、}$$

前記 $f'_{r,p}(Q)$ は、

[数19]

$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2 + \lambda_1 + 1, P}(Q) \\ &= f_{\lambda_1, P}(Q)^{\lambda_1 + 1} \cdot f_{\lambda_1 + 1, \psi(P)}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_1, P}(Q) \cdot f_{\lambda_1, P}(Q)^{\lambda_1} \cdot f_{\lambda_1, \psi(P)}(Q) \cdot l_{[\lambda_1]\psi(P), \psi(P)}(Q) \end{aligned}$$

であることにも特徴を有するものである。

[0044] さらに本発明のペアリング演算方法では、

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $6 \nmid (p-1)$ であり、

前記合成数位数 r は、 $r \nmid \#E(F_p)$, $3 \mid (r-1)$ を満たし、

前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 - \lambda_1 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 - \lambda_2 + 1 \equiv 0 \pmod{r}$ であり、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$$(x, y) \rightarrow (\varepsilon x, -y), \varepsilon^3 = 1, \varepsilon (\neq 1) \in F_p \text{ であり、}$$

前記 $f'_{r,p}(Q)$ は、

[数20]

$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2 - \lambda_1 + 1, P}(Q) \\ &= f_{\lambda_1, P}(Q)^{\lambda_1 - 1} \cdot f_{\lambda_1 - 1, \psi(P)}(Q) \cdot (x_Q - x_P) \\ &= \left\{ f_{\lambda_1 - 1, P}(Q) \cdot \frac{l_{[\lambda_1 - 1]P, P}(Q)}{v_{[\lambda_1 - 1]P, P}(Q)} \right\}^{\lambda_1 - 1} \\ &\quad \cdot f_{\lambda_1 - 1, \psi(P)}(Q) \cdot (x_Q - x_P) \end{aligned}$$

であることにも特徴を有するものである。

[0045] 本発明のペアリング演算プログラムでは、

標数 p の有限体 F_p 上で定義された楕円曲線上の有理点の成す加法群を $E(F_p)$ と

し、合成数位数 r を持つ有理点の集合すなわち前記加法群の部分群を $G_1 = E(F_p)$

$[r]$ 、 $G_2 = E(F_p)[r]$ として、次式により、

$$e: G_1 \times G_2 \rightarrow F_p^* / (F_p^*)^r$$

である非退化な双線形写像としてペアリング e を定義し、

有理点 $P(x_P, y_P) \in G_1$ 及び $Q(x_Q, y_Q) \in G_2$ 、ミラーのアルゴリズムを用いて計算され

る有理関数を f として、CPU 及び記憶手段を備えた電子計算機にペアリング $e(P, Q)$ を演算させるペアリング演算プログラムにおいて、

前記加法群 $E(F_p)$ は、埋め込み次数を 1 とし、

前記電子計算機のCPUを、有理点 P' を入力して記憶手段に記憶する入力手段、

前記記憶手段から前記有理点 P' を読み出し、自己準同型写像 ϕ により、

$\lambda_1 P = \phi(P)$ 、 $\lambda_2 Q = \phi(Q)$ ($\lambda_1 \neq \lambda_2$ は整数)を満足する前記有理点 P 及び Q の集合である前記部分群 G_1 及び G_2 を特定する有理点部分群特定手段、

前記記憶手段から前記有理点 P または Q を読み出し、前記自己準同型写像 $\phi(P)$

または $\phi(Q)$ を演算しその結果の有理点を前記記憶手段に記憶する自己準同型写像演算手段、

前記 f を演算する第1演算手段、

所定の有理点を通る直線及び垂線の前記有理点 Q における値を演算する第2演算手段、

前記 f と前記値を用いて $f'_{r,p}(Q)$ を演算する第3演算手段、

前記 $f'_{r,p}(Q)$ を用いて前記ペアリング $e(P, Q)$ を

[数21]

$$e(P, Q) = f'_{r,p}(Q)^{(p-1)/r}$$

として演算する第4演算手段、

として機能させることとした。

[0046] さらに本発明のペアリング演算プログラムでは、

前記楕円曲線は、 $E: y^2 = x^3 + ax$, $a \in F_p$, $4 \nmid (p-1)$ であり、

前記合成数位数 r は、 $r \nmid \#E(F_p)$, $4 \mid (r-1)$ を満たし、

前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 + 1 \equiv 0 \pmod{r}$ であり、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$$(x, y) \rightarrow (-x, \zeta y), \zeta^4 = 1, \zeta, \zeta^2 (\neq 1) \in F_p \text{ であり、}$$

前記 $f'_{r,p}(Q)$ は、

[数22]

$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2+1,P}(Q) \\ &= f_{\lambda_1^2,P}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_1,P}(Q)^{\lambda_1} \cdot f_{\lambda_1,\psi(P)}(Q) \cdot (x_Q - x_P) \end{aligned}$$

であることにも特徴を有するものである。

[0047] さらに本発明のペアリング演算プログラムでは、

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $3 \nmid (p-1)$ であり、

前記合成数位数 r は、 $r \nmid \#E(F_p)$, $3 \mid (r-1)$ を満たし、

前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 + \lambda_1 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 + \lambda_2 + 1 \equiv 0 \pmod{r}$ であり、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$(x, y) \rightarrow (\varepsilon x, y)$, $\varepsilon^3 = 1$, $\varepsilon (\neq 1) \in F_p$ であり、

前記 $f'_{r,p}(Q)$ は、

[数23]

$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2 + \lambda_1 + 1, P}(Q) \\ &= f_{\lambda_1, P}(Q)^{\lambda_1 + 1} \cdot f_{\lambda_1 + 1, \psi(P)}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_1, P}(Q) \cdot f_{\lambda_1, P}(Q)^{\lambda_1} \cdot f_{\lambda_1, \psi(P)}(Q) \cdot l_{[\lambda_1] \psi(P), \psi(P)}(Q) \end{aligned}$$

であることにも特徴を有するものである。

[0048] さらに本発明のペアリング演算プログラムでは、

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $6 \mid (p-1)$ であり、

前記合成数位数 r は、 $r \nmid \#E(F_p)$, $3 \mid (r-1)$ を満たし、

前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 - \lambda_1 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 - \lambda_2 + 1 \equiv 0 \pmod{r}$ であり、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$(x, y) \rightarrow (\varepsilon x, -y)$, $\varepsilon^3 = 1$, $\varepsilon (\neq 1) \in F_p$ であり、

前記 $f'_{r,p}(Q)$ は、

[数24]

$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2 - \lambda_1 + 1, P}(Q) \\ &= f_{\lambda_1, P}(Q)^{\lambda_1 - 1} \cdot f_{\lambda_1 - 1, \psi(P)}(Q) \cdot (x_Q - x_P) \\ &= \left\{ f_{\lambda_1 - 1, P}(Q) \cdot \frac{l_{[\lambda_1 - 1] P, P}(Q)}{v_{[\lambda_1 - 1] P + P}(Q)} \right\}^{\lambda_1 - 1} \\ &\quad \cdot f_{\lambda_1 - 1, \psi(P)}(Q) \cdot (x_Q - x_P) \end{aligned}$$

であることにも特徴を有するものである。

発明の効果

[0049] 本発明のスカラー倍算によれば、有理点群の埋め込み次数が 1 の場合にお

いて、有理点 P のスカラー s によるスカラー倍算 $[s]P$ を演算するにあたり、

$$\lambda P = \phi(P) \quad (\lambda \text{ は整数})$$

となる有理点の集合Gを特定して、s を λ 進展開して $s=s_0+s_1\lambda$ とし、スカラー倍算 $[s]P$ を、

$$[s]P = (s_0 + s_1\lambda)P = s_0P + s_1\phi(P)$$

として演算を行うことにより、バイナリー法に比べ、演算量をほぼ半減させることができ、スカラー倍算を高速化することができる。

[0050] また、本発明のペアリング演算によれば、ペアリング演算において、ミラーのアルゴリズムを用いて計算される有理関数の計算を2回行うこととなるが、前半で求めた値を記憶手段に保持しておき、それらを後半の計算に効率よく用いることにより、Tateペアリングと比べ約30%の効率化を図ることができる。

図面の簡単な説明

[0051] [図1]本発明の実施形態にかかるスカラー倍算装置またはペアリング演算装置の概略構成を示す模式図である。

[図2]本発明の実施形態にかかるスカラー倍算装置またはペアリング演算装置の全体構成を例示したブロック図である。

[図3]本発明の実施形態にかかる有理点部分群特定部の機能構成を例示した図である。

[図4]本発明の実施形態にかかる有理点部分群特定プログラムのフローチャートである。

[図5]本発明の実施形態にかかるスカラー倍算演算部の機能構成を例示した図である。

[図6]本発明の実施形態にかかるスカラー倍算演算プログラムのフローチャートである。

[図7]本発明の実施形態にかかるペアリング演算部の機能構成を例示した図である。

[図8]本発明の実施形態にかかるペアリング演算プログラムのフローチャートである。

[図9]本発明の実施形態にかかるペアリング演算プログラムのフローチャートである。

[図10]本発明の実施形態にかかるペアリング演算プログラムのフローチャートである。

[図11]本発明の実施形態にかかるペアリング演算プログラム（メモリ節約型）のフローチャートである。

発明を実施するための最良の形態

[0052] 本発明の成果を適用できるようなペアリング曲線は、以下のような条件を満たす必要がある。まず、標数 p の有限体 F_p 上で定義される楕円曲線を、

$E/F_p: y^2 = x^3 + ax + b, a \in F_p, b \in F_p$ とし、

$E(F_p)$: 標数 p の有限体 F_p 上で定義される楕円曲線の有理点が成す加法群、

$r: E(F_p)$ の位数 $\#E(F_p)$ を割り切る合成数、

$E[r]$: 位数が合成数 r である有理点の集合、

ϕ : 有理点に対する自己準同型写像、

t : フロベニウス写像のトレース、

$[j]$: 有理点を j 倍する写像、

$G: G = E[r] \cap \text{Ker}(\phi - \lambda)$ 、(λ は整数) を満たす有理点の集合、と定義する。

また、 $x \mid y$ は、 x が y を割り切ることを表わすものとする。

[0053] 楕円曲線の生成には CM (Complex Multiplication) 法が知られている。標数 p 、フロベニウス写像のトレース t 、判別式 D による次式のような CM 方程式において、判別式 $D=1, 3$ の場合を考える。

$$4p = t^2 - Ds^2 \quad (1)$$

この時、ペアリング曲線の式はそれぞれ以下のように与えられる。

$$E_a: y^2 = x^3 + ax, a \in F_p \quad (D=1) \quad (2a)$$

$$E_b: y^2 = x^3 + b, b \in F_p \quad (D=3) \quad (2b)$$

本発明者らは、大きな合成数位数に対してこのようなペアリング曲線を生成する簡便な生成法を提案済みである。上記のペアリング曲線上の有理点が簡単な自己準同型写像 ϕ (即ち有理点を P 、整数を λ として、 $\phi(P) = \lambda P$) を持

つためには、パラメータの条件がある。これには、以下に示すように、自己準同型写像の周期 3, 4, 6 に対応して 3 次、4 次、6 次の 3 つの場合がある。

この自己準同型写像をスカラー倍算に用いるのが GLV 法である。

また、この自己準同型写像をペアリング演算の高速化にも用いる。

以下に、パラメータの条件及びその写像を示す。

[0054] <3 次の場合>

楕円曲線のパラメータが、 $3 \mid (p-1)$, $E: y^2 = x^3 + b$, $b \in F_p$, $D=3$ の場合、 $r \mid \#E(F_p)$, $3 \mid (r-1)$ を満たす合成数 r に対して、次式を満足するある整数 λ_3 が存在する。

$$\lambda_3^2 + \lambda_3 + 1 \equiv 0 \pmod{r} \quad (3)$$

また、以下に示す周期 3 の自己準同型写像 ϕ_3 が与えられる。

$$\phi_3: E(F_p)[r] \rightarrow E(F_p)[r], \quad (4a)$$

[数25]

$$(x, y) \mapsto (\varepsilon x, y), \quad \varepsilon^3 = 1, \quad \varepsilon (\neq 1) \in F_p. \quad (4b)$$

このような合成数 r を位数として持つ有理点を $P \in E(F_p)[r]$ とすれば、3 次の場合、 $[\lambda_3]P = \phi_3(P)$ の関係を用いることでスカラー倍算の効率化を図っている。また、後述のペアリング演算の効率化も図っている。

[0055] 具体的には、スカラー倍算の場合、 r に較べて極めて小さい λ_3 であれば、これは $[\lambda_3]P$ というスカラー倍算が簡便な自己準同型写像 $\phi_3(P)$ で求められる（すなわち、有理点 P の x 座標値を ε 倍する演算だけでよい）ことから、スカラー s を λ_3 進展開することなどによりこの自己準同型写像を効率よく用いてこれを計算する。

[0056] しかしながら、有理点群の埋め込み次数が 1 の場合、一般の有理点 $P' \in E(F_p)[r]$ に対しては、 $[\lambda_3]P' = \phi_3(P')$ は成り立たない。そのため GLV 法は適用することができない。上述したように、これを満たすような有理点の割合は $1/r = 1/2^{2000}$ であり、簡便にそのような有理点及び有理点部分群を準備できる必要がある。

[0057] 本発明では、本発明者らが発見した以下の性質を用いる。

まず、任意の有理点 $P' \in E(F_p)[r]$ は次式を満たす。

$$[(\phi_3 - \lambda_3)(\phi_3 + \lambda_3 + 1)]P' = 0 \quad (5)$$

ここで、0 は無限遠点を表わしている。

すなわち、ランダムに生成した有理点 $P' \in E(F_p)[r]$ を $(\phi_3 + \lambda_3 + 1)$ 倍し、

$$P = [\phi_3 + \lambda_3 + 1]P' \quad (6)$$

とすることにより、その有理点 P は $[\lambda_3]P = \phi_3(P)$ を満たすこととなる。そして、そのような P が生成する有理点部分群を G_1 とする。また逆に、

$$Q = [\phi_3 - \lambda_3]P' \quad (7)$$

とすれば、 $[\lambda_3 + 1]Q = -\phi_3(Q)$ を満たす有理点 Q となる。そして、そのような Q が生成する有理点部分群を G_2 とする。これら G_1 、 G_2 を用いて後述のスカラー倍算及びペアリング演算の高速化を実現することができる。

[0058] <関係式の導出法の説明>

3次の場合の式(5)の導出について以下に説明する。

まず、任意の有理点 $P' \in E(F_p)[r]$ は、 $E(F_p)$ のフロベニウス写像のトレース t 及びフロベニウス写像 ϕ を用いて、次式を満たすことが知られている。

$$\begin{aligned} \phi : (x, y) &\rightarrow (x^p, y^p) \\ (\phi^2 - t\phi + [p])P' &= 0 \end{aligned} \quad (8)$$

同様に、 P' を $E(F_p)$ と同型な群を内包する拡大体上ツイスト曲線 $E'(F_{p^3})$ に写像した有理点 P^- を考えれば、 $E'(F_{p^3})$ のフロベニウス写像のトレースを t' として次式を満たす。

$$(\phi^2 - t'\phi + [p])P^- = 0 \quad (9)$$

ここで、ツイスト曲線は、 $E' : y^2 = x^3 + bv^{-2}$, $b \in F_p$ で与えられ、 v は F_p の 3 乗非剰余な元であり、 P^- は、 $P' = (x, y)$ として以下で与えられる。

$$P^- = (xv^{2/3}, yv) \quad (10)$$

ここで、上式を写像 $\phi : P' \in E(F_p) \rightarrow P^- \in E'(F_{p^3})$ とすれば、式(9)は次式のように変形できる。

$$\{(\phi^{-1}\phi^2\phi) - t'(\phi^{-1}\phi\phi) + [p]\}P' = 0 \quad (11)$$

そしてこの場合、 $\phi^{-1}\phi\phi = \phi_3$ が成り立つので次式を得る。

$$(\phi_3^2 - t' \phi_3 + [p])P' = 0 \quad (12)$$

上式に対して、有理点群の埋め込み次数が1であることから $p \equiv 1 \pmod{r}$ であり、加えてこれに用いる楕円曲線を $t' \equiv -1$ (3次)、 0 (4次)、 1 (6次) $\pmod{r}$ となるように生成していることから、 $P' \in E(F_p)[r]$ (位数 r の有理点) とすれば、3次のときには次式を得る。

$$(\phi_3^2 + \phi_3 + [1])P' = 0 \quad (13)$$

一方で3次の場合には、式(3)を満たすような整数 λ_3 も存在し、すなわち $\phi_3^2 + \phi_3 + 1 \equiv 0$

$\pmod{r}$ を、 ϕ_3 を変数とするような方程式と考えれば、その解の1つが ϕ_3 となる。したがって、式(5)のような因数分解された関係式が得られる。

[0059] <4次の場合>

同様に、楕円曲線のパラメータが、 $4 \mid (p-1)$, $E: y^2 = x^3 + ax$, $a \in F_p$, $D=1$ の場合、

$r \mid \#E(F_p)$, $4 \mid (r-1)$ を満たす合成数 r に対して、次式を満足するある整数 λ_4 が存在する。

$$\lambda_4^2 + 1 \equiv 0 \pmod{r} \quad (14)$$

また、以下に示す周期4の自己準同型写像 ϕ_4 が与えられる。

$$\phi_4: E(F_p)[r] \rightarrow E(F_p)[r], \quad (15a)$$

[数26]

$$(x, y) \mapsto (-x, \zeta y), \quad \zeta^4 = 1, \quad \zeta (\neq 1) \in F_p. \quad (15b)$$

このような合成数 r を位数として持つ有理点を $P \in E(F_p)[r]$ とすれば、4次の場合は、 $[\lambda_4]P = \phi_4(P)$ の関係を用いることでスカラー倍算の効率化を図っている。また、後述のペアリング演算の効率化も図っている。

[0060] 本発明では、本発明者らが発見した以下の性質を用いる。

まず、任意の有理点 $P' \in E(F_p)[r]$ は次式を満たす。

$$[(\phi_4 - \lambda_4)(\phi_4 + \lambda_4)]P' = 0 \quad (16)$$

すなわち、ランダムに生成した有理点 $P' \in E(F_p)[r]$ を $(\phi_4 + \lambda_4)$ 倍し、

$$P = [\phi_4 + \lambda_4]P' \quad (17)$$

とすることにより、その有理点 P は $[\lambda_4]P = \phi_4(P)$ を満たすこととなる。そし

て、そのようなPが生成する有理点部分群を G_1 とする。また逆に、

$$Q = [\phi_4 - \lambda_4]P' \quad (18)$$

とすれば、 $[\lambda_4]Q = -\phi_4(Q)$ を満たす有理点Qとなる。そして、そのようなQが生成する有理点部分群を G_2 とする。これら G_1, G_2 を用いて後述のスカラー倍算及びペアリング演算の高速化を実現することができる。

[0061] 4次の場合の式(16)の導出については、3次の場合と同様であるので説明は省略する。

[0062] <6 次の場合>

さらに同様に、楕円曲線のパラメータが、 $6 \mid (p-1)$, $E: y^2 = x^3 + b$, $b \in F_p$, $D=3$ の場合、

$r \mid \#E(F_p)$, $3 \mid (r-1)$ を満たす合成数 r に対して、次式を満足する λ_6 が存在する。

$$\lambda_6^2 - \lambda_6 + 1 \equiv 0 \pmod{r}. \quad (19)$$

また、以下に示す周期6の自己準同型写像 ϕ_6 が与えられる。

$$\phi_6: E(F_p)[r] \rightarrow E(F_p)[r], \quad (20a)$$

[数27]

$$(x, y) \mapsto (\varepsilon x, -y), \quad \varepsilon^3 = 1, \quad \varepsilon (\neq 1) \in F_p. \quad (20b)$$

このような位数 r を持つ有理点を $P \in E(F_p)[r]$ とし、6次の場合は、 $[\lambda_6]P = \phi_6(P)$ の関係を用いることでスカラー倍算の効率化を図っている。また、後述のペアリング演算の効率化も図っている。

[0063] 本発明では、本発明者らが発見した以下の性質を用いる。

まず、任意の有理点 $P' \in E(F_p)[r]$ は次式を満たす。

$$[(\phi_6 - \lambda_6)(\phi_6 + \lambda_6 - 1)]P' = 0 \quad (22)$$

すなわち、ランダムに生成した有理点 $P' \in E(F_p)[r]$ を $(\phi_6 + \lambda_6 - 1)$ 倍し、

$$P = [\phi_6 + \lambda_6 - 1]P' \quad (23)$$

とすることにより、その有理点Pは $[\lambda_6]P = \phi_6(P)$ を満たすこととなる。そして、そのようなPが生成する有理点部分群を G_1 とする。また逆に、

$$Q = [\phi_6 - \lambda_6]P' \quad (24)$$

とすれば、 $[\lambda_6 - 1]Q = -\phi_6(Q)$ を満たす有理点 Q となる。そして、そのような Q が生成する有理点部分群を G_2 とする。これら G_1 、 G_2 を用いて後述のスカラー倍算及びペアリング演算の高速化を実現することができる。

[0064] 6次の場合の式(22)の導出についても、3次の場合と同様であるので説明は省略する。

[0065] 以下に、本発明のGLV法によるスカラー倍算について説明する。

有理点 P のスカラー $0 < s < r$ によるスカラー倍算 $[s]P$ は、 s を λ 進展開して、

$$s = s_0 + s_1 \lambda \quad s_0, s_1 < \lambda \quad (25)$$

とすると、

$$[s]P = [s_0 + s_1 \lambda]P = [s_0]P + [s_1 \lambda]P = [s_0]P + [s_1] \phi(P) \quad (26)$$

となる。

s_0 、 s_1 は λ より小さく、 λ は r に較べてはるかに小さい。また $\phi(P)$ は上述したように簡単な計算（有限体上の乗算1回）で求めることができる。従って s よりはるかに小さいスカラー値を用いてスカラー倍算を求めることができ、高速化を実現できる。式(26)は複数の有理点のスカラー倍算を求める場合の既存の高速化手法である後述のマルチ・スカラー倍算法（[表1]参照。）により求めることができる。 $\lambda^2 \div r$ であり、 s_0 、 s_1 は、2進数展開したときのビット数が約半分となるので、バイナリー法に比べおおよそ半分の計算時間で求まることとなる。

[0066] 以下において、本発明のスカラー倍算の実施形態について、図を用いて説明する。図1は、本発明の実施形態にかかるスカラー倍算装置の概略模式図である。図2は、本発明の実施形態にかかるスカラー倍算装置の全体構成を例示したブロック図である。まず、図1及び図2を用いてこの形態の全体について説明し、次にその詳細について説明する。なお、本実施形態では、所要の電子計算機で構成された認証サーバによってデジタルグループ署名の認証処理を行う際に、与えられたペアリング曲線から上述した有理点部分群を特定するプログラム、及び一般的にサブルーチン処理として実行されているスカラー倍算演算プログラム部分についてのみ説明する。なお、有理点部分群

の特定及びスカラー倍算の演算は、認証サーバで実行される場合に限定されるものではなく、少なくともCPUなどの演算手段及び記憶手段を備えた装置であれば、どのような装置であってもよい。

[0067] 図1に示すように、認証サーバを構成する電子計算機10は、演算処理を実行するCPU 11と有理点部分群特定プログラム、スカラー倍算演算プログラム、ペアリング演算プログラムなどの各種プログラム、及びこれらのプログラムで使用するデータなどを記憶したハードディスクなどの記憶装置12と、これらのプログラムを展開して実行可能とするとともに、これらプログラムの実行にともなって生成されたデータを一時的に記憶するRAMなどで構成されたメモリ装置13を備えている。図1中、14はバスである。

[0068] また、認証サーバを構成する電子計算機10は、インターネットなどの電気通信回線20に接続して、この電気通信回線20に接続されたクライアント装置30から送信されたデジタルグループ署名の署名データを受信可能としている（図2、認証データ入力部100）。図1中、15は電子計算機10の入出力部である。

[0069] 認証サーバを構成する電子計算機10では、クライアント装置30からデジタルグループ署名の署名データが送信されると、送信された署名データをメモリ装置13に一旦記憶し（認証データ入力部100）、有理点部分群特定プログラムを起動して効率的な自己準同型写像を可能とする有理点部分群を特定（図2、有理点部分群特定部200）した後、ペアリング演算プログラムを起動して、ペアリング演算を実行している（図2、ペアリング演算部300）。

そして、認証サーバを構成する電子計算機10では、ペアリング演算の実行に際して、所要のスカラー倍算の演算が必要となった場合に、スカラー倍算演算プログラムを起動して、スカラー倍算を実行している（図2、スカラー倍算演算部400）。

その後、認証結果を出力している（図2、認証結果出力部500）。

[0070] 次に、本実施形態の詳細について図を用いて説明する。

<有理点部分群の特定>

[0071] 図3は図1で示した装置で所定のプログラムを実行させることにより実現される有理点部分群特定部の機能構成を例示した図である。

図4は有理点部分群特定部の処理を行う有理点部分群特定プログラムのフローチャートである。

電子計算機10では、起動した有理点部分群特定プログラムによって、図4に示すフローチャートに基づいて効率的な自己準同型写像を可能とする有理点部分群を特定している。すなわち、入力された、有理点群が埋め込み次数1の一般の有理点を特定の有理点部分群内の有理点に変換している。この場合電子計算機10は有理点部分群特定手段として機能する。以下では、3次GLV法の場合について説明する。

[0072] ステップ T1（有理点入力部210）では、外部から与えられ入力手段により記憶手段に記憶された一般の有理点 P' を読み出している。

ステップ T2（定数演算部220）では、あらかじめレジスタに記憶された有限体の標数 p 及び合成数位数 r とを用いて、式（3）で示した $\lambda^2 + \lambda + 1 \equiv 0 \pmod{r}$ となる λ 及び、式（4b）で示した $\varepsilon^3 \equiv 1 \pmod{p}$ となる $\varepsilon (\neq 1)$ を演算し設定している。

ステップ T3（自己準同型写像演算部230）では、式（4b）の $\phi(P') : (x, y) \rightarrow (\varepsilon x, y)$ として、 P' の x 座標値 x を ε 倍し、 $\phi(P')$ を求めている。

ステップ T4（有理点演算部240）では、式（6）の $P = \phi(P') + (\lambda + 1)P'$ を計算している。なお、この $\phi(P') + (\lambda + 1)P'$ は2個の有理点スカラー倍算を同時に求める後述の[表1]に基づくアルゴリズムにより求めている。

ステップ T5（判定部250）では、 $P=0$ （無限遠点）かどうかを判定している。

$P=0$ の場合は、2つの部分群を特定できないのでエラー・リターンしている。

ステップ T6（有理点演算部240）では、式（7）の $Q = \phi(P') + (-\lambda)P'$ を計算している。なお、この $\phi(P') + (-\lambda)P'$ も2個の有理点のスカラー倍算を同時に求める後述の[表1]に基づくアルゴリズムにより求めている。

ステップ T7(判定部250)では、 $Q=0$ (無限遠点)かどうかを判定している。

$Q=0$ の場合は2つの部分群を特定できないのでエラー・リターンしている)。

ステップ T8では、 P 、 Q を記憶手段に記憶している。 P の集合が有理点部分群 G_1 となり、 Q の集合が有理点部分群 G_2 となる。

[0073] 本実施形態では、3次GLV法の場合について説明したが、4次GLV法、及び6次GLV法の場合も、 λ 、 $\phi(P')$ 、 ε または ζ 、 P 、 Q がそれぞれ

4次GLV法では、式(14)： $\lambda^2+1 \equiv 0 \pmod{r}$ 、

式(15b)： $\phi(P') : (x, y) \rightarrow (-x, \zeta y)$ 、($\zeta^4=1$, $\zeta, \zeta^2(\neq 1) \in F_p$)、

式(17)： $P = \phi(P') + \lambda P'$ 、

式(18)： $Q = \phi(P') + (-\lambda)P'$

となり、

6次GLV法では、式(19)： $\lambda^2 - \lambda + 1 \equiv 0 \pmod{r}$ 、

式(20b)： $\phi(P') : (x, y) \rightarrow (\varepsilon x, -y)$ 、($\varepsilon^3=1$, $\varepsilon(\neq 1) \in F_p$)、

式(23)： $P = \phi(P') + (\lambda - 1)P'$ 、

式(24)： $Q = \phi(P') + (-\lambda)P'$

となるだけであり、同様に有理点部分群を特定することができる(説明は省略する。))。

[0074] <スカラー倍算演算プログラム>

図5は図1で示した装置で所定のプログラムを実行させることにより実現されるスカラー倍算演算部の機能構成を例示した図である。図6はスカラー倍算演算部の処理を行うスカラー倍算演算プログラムのフローチャートである。

電子計算機10では、起動したスカラー倍算演算プログラムによって、図6に示すフローチャートに基づいてスカラー倍算の演算を行い、演算結果を記憶手段に記憶すると共に、メインルーチンのプログラムに返している。以下では、3次GLV法の場合について説明する。

- [0075] 起動したスカラー倍算演算プログラムによって、電子計算機10では、ペアリング演算部300より、スカラー s のデータ及び、有理点 P のデータ、を入力して、CPU11の内部に設けている所定のレジスタ490にそれぞれ入力している（パラメータ入力部410）（ステップ S1）。
- [0076] 次いで、電子計算機10では、スカラー倍算演算プログラムによってCPU11を定数演算手段として機能させて、あらかじめレジスタ490に格納されている合成数位数 r 及び有限体の標数 p を用いて、式(3)で示した $\lambda^2 + \lambda + 1 \equiv 0 \pmod{r}$ となる λ 及び式(4b)で示した $\varepsilon^3 \equiv 1 \pmod{p}$ となる $\varepsilon (\neq 1)$ を演算しそれぞれ設定している（定数演算部420）（ステップ S2）。
- [0077] 次いで、電子計算機10では、スカラー倍算演算プログラムによってCPU11を自己準同型写像演算手段として機能させて、式(4b)で示した $P(x, y) \rightarrow \phi(P)(\varepsilon x, y)$ を演算している。すなわち、 P の x 座標値を ε 倍して新たな有理点を求めている（自己準同型写像演算部430）（ステップ S3）。
- [0078] 次いで、電子計算機10では、スカラー倍算演算プログラムによってCPU11を λ 進展開手段として機能させて、スカラー s を λ 進展開して、式(25)で示した
- $$s = s_0 + s_1 \lambda \pmod{r}$$
- となる係数 s_0 、 s_1 を演算している（ λ 進展開部440）（ステップ S4）。
- 具体的には、 $s_0 = s \% \lambda$ 、 $s_1 = (s - s_0) / \lambda$ としている。（ $\%$ は、剰余演算子、 $/$ は除算演算子。）
- [0079] 次いで、電子計算機10では、スカラー倍算演算プログラムによってCPU11をスカラー倍算演算手段として機能させて、式(26)で示した
- $$[s]P = (s_0 + s_1 \lambda)P = s_0 P + s_1 \lambda P = s_0 P + s_1 \phi(P)$$
- としてスカラー倍算 $[s]P$ の演算を行っている（マルチ・スカラー倍算演算部450）（ステップ S5）。
- この $s_0 P + s_1 \phi(P)$ の演算は、二つの有理点のスカラー倍算の演算を同時に求めるマルチ・スカラー倍算として以下の[表1]のアルゴリズムに基づいて行っている。

[0080] [表1] マルチ・スカラー倍算アルゴリズム

Input: $w, k=(k_{t-1}, \dots, k_1, k_0)_2, l=(l_{t-1}, \dots, l_1, l_0)_2, P, Q.$

Output: $kP + lQ.$

(1) Compute $iP+jQ$ for all $i, j \in [0, 2^w-1].$

(2) Write $k=(k^{d-1}, \dots, k^1, k^0)$ and $l=(l^{d-1}, \dots, l^1, l^0), d=\lceil t/w \rceil.$

(3) $R \leftarrow 0.$

(4) For i from $d-1$ down to 0 do

(4.1) $R \leftarrow 2^w R.$

(4.2) $R \leftarrow R + (k^i P + l^i Q).$

(5) Return(R).

この場合、このアルゴリズムにおける入力パラメータの k は s_0 、 l は s_1 、 P は入力した有理点 P 、 Q は有理点 $\phi(P)$ となる。 w はウィンドー巾である。 k_j 、 l_j は k 、 l を 2 進展開した時の各係数、 k^i 、 l^i は k 、 l を 2^w 進展開した時の各係数である。全体で d 個となる。

ステップ 1 では、ウィンドー巾までの有理点 P, Q の全てのスカラー倍算の組合せについて、事前に計算しておきテーブル化して記憶手段に記憶している。

ステップ 2 では、各 k^i 、 l^i を求めている。

ステップ 3 では、求めるべき有理点の変数 R を初期化している。

ステップ 4 では、以下の 4. 1 及び 4. 2 のステップを i が $d-1$ から 0 まで繰り返している。

ステップ 4. 1 では、 R をウィンドー巾倍すなわち楕円 2 乗算を w 回行っている。

ステップ 4. 2 では、ステップ 1 で作成したテーブルを参照して $k^i P + l^i Q$ の値を R に楕円加算している。

ステップ 5 では、 R を戻り値としてリターンしている。

[0081] このとき、スカラー s が 2000 ビットであった場合には s_0 及び s_1 は 1000 ビットとなるため、バイナリー法に比べ、演算量を半減させることができ、スカラー倍算を高速化することができる。

[0082] 演算後、電子計算機 10 では、演算結果をメモリ装置 13 に記憶するとともに

メインルーチンのプログラムに返している。

[0083] 本実施形態では、3次GLV法の場合について説明したが、4次GLV法、及び6次GLV法の場合も、 λ 及び $\phi(P)$ と、 ε または ζ がそれぞれ、

4次GLVでは、式(14) : $\lambda^2 + 1 \equiv 0 \pmod{r}$ 、

式(15b) : $\phi(P) : (x, y) \rightarrow (-x, \zeta y)$, ($\zeta^4 \equiv 1 \pmod{p}$)

となり、

6次GLVでは、式(19) : $\lambda^2 - \lambda + 1 \equiv 0 \pmod{r}$ 、

式(20b) : $\phi(P) : (x, y) \rightarrow (\varepsilon x, -y)$, ($\varepsilon^3 \equiv 1 \pmod{p}$)

となるだけであり、同様に演算することができる(説明は省略する。)。

[0084] 以上説明したように、本実施形態の有理点部分群特定手段である有理点部分群特定部200では、有理点入力部210において、有理点群の埋め込み次数が1である F_p 上の一般の有理点 $P' \in F_p[r]$ を入力し、定数演算部220において、あらかじめレジスタ290に格納された合成数位数 r 及び標数 p を用いて、式(3)に示す $\lambda^2 + \lambda + 1 \equiv 0 \pmod{r}$ 及び式(4b)に示す $\varepsilon^3 \equiv 1 \pmod{p}$ を演算し、自己準同型写像演算部230において自己準同型写像 $\phi(P')$ を演算し、有理点演算部240において有理点 P 及び Q を演算して、有理点部分群を特定している。このようにすることにより、これら有理点部分群の1つを用いてスカラー倍算の演算を高速に行うことができる。

[0085] また、本実施形態のスカラー倍算演算部400では、入力手段であるパラメータ入力部410において、スカラー値 s 及び有理点 P を入力し、定数演算部420において、あらかじめレジスタ490に格納された合成数位数 r 及び標数 p を用いて、式(3)に示す $\lambda^2 + \lambda + 1 \equiv 0 \pmod{r}$ 及び式(4b)に示す $\varepsilon^3 \equiv 1 \pmod{p}$ を演算し、自己準同型写像演算手段である自己準同型演算部430において自己準同型写像 $\phi(P)$ を演算し、 λ 進展開手段である λ 進展開部440においてスカラー s を λ 進展開し、マルチ・スカラー倍算演算手段であるマルチ・スカラー倍算演算部450において、スカラー倍算 $[s]P$ を演算している。このようにすることにより有理点群が埋め込み次数1である有理点のスカラー倍算を高速に実行することができる。

[0086] なお、本発明のスカラー倍算は、上述の実施形態に限定されるものではない。例えば、マルチ・スカラー倍算演算部では、既存の手法であるJSF (Joint Sparse Form)を用いて演算してもよい。

[0087] また、有理点群特定プログラム及びスカラー倍算演算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することができる。また、これらのプログラムをサーバのコンピュータの記憶装置に記憶しておき、ネットワークを介して電子計算機の記憶装置にダウンロードすることもできる。

[0088] 以下に本発明のペアリング演算について説明する。

本発明のペアリング演算では、ペアリング演算におけるミラーのアルゴリズムを用いて有理関数を演算する第1のステップと、その結果に対してべき乗算を行う第2のステップのうち、第1のステップにおいて、上記整数 λ 及び自己準同型写像 $\phi(P)$ を用いて有理関数を演算することにより、演算の高速化を図っているものである。

[0089] すなわち、従来のペアリング演算では、曲線の式が $y^2=x^3+ax+b$, $a \in F_p$, $b \in F_p$ で与えられ、 F_p 上の素数位数 r を持つ有理点の集合を $E[r]$ とし、埋め込み次数が k で F_{p^k} を定義体とするペアリング可能な楕円曲線上の有理点の成す加法群を $E(F_{p^k})$ 、 ϕ_p をフロベニウス自己準同型写像として、

$$G_1=E[r],$$

$$G_2=E(F_{p^k})$$

により、

$$e:G_1 \times G_2 \rightarrow F_{p^k}^*/(F_{p^k}^*)^r$$

である非退化な双線形写像としてペアリング e を定義し、有理点 $P(x_p, y_p) \in G_1$ 及び $Q(x_q, y_q) \in G_2$ 、ミラーのアルゴリズムを用いて計算される有理関数 $f_{r,p}(Q)$ を用いて、ペアリング $e(P, Q)$ を、

[数28]

$$e(P, Q) = f_{r,p}(Q)^{(p^k-1)/r}$$

として演算していた。これらは、Tateペアリングとして知られているものである。

[0090] これに対して、本発明者らは、有理点群の埋め込み次数が1の場合において、有理点部分群 G_1 、 G_2 を特定し、その特性により有理関数 $f_{r,P}(Q)$ の計算を例えば、4次の場合、以下のように行うこととした。

[数29]

$$\begin{aligned} f_{r,P}(Q) &= f_{\lambda_4^2+1,P}(Q) \\ &= f_{\lambda_4^2,P}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_4,P}(Q)^{\lambda_4} \cdot f_{\lambda_4, [\lambda_4]P}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_4,P}(Q)^{\lambda_4} \cdot f_{\lambda_4, \psi_4(P)}(Q) \cdot (x_Q - x_P) \end{aligned}$$

まず、 $f_{\lambda_4,P}(Q)$ を計算する。この計算の過程で得られる途中のデータを記憶手段に記憶する。続いて $f_{\lambda_4, \psi_4(P)}(Q)$ を計算する際に先の計算と $\psi_4(P)$ のみが異なること、加えてそれが簡単な写像 ψ_4 を仲介して与えられていることから、先に記憶しておいた計算結果を活用することができ、加えて、その計算の初期値として $f_{\lambda_4,P}(Q)$ の計算結果を使うことにより、残りの λ_4 乗算（べき乗算）も併せて済ませることができる。これにより、おおよそ30%の効率化が図れる。

[0091] 3次の場合も同様に、

[数30]

$$\begin{aligned} f_{r,P}(Q) &= f_{\lambda_3^2+\lambda_3+1,P}(Q) \\ &= f_{\lambda_3,P}(Q)^{\lambda_3+1} \cdot f_{\lambda_3+1, [\lambda_3]P}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_3,P}(Q)^{\lambda_3+1} \cdot f_{\lambda_3+1, \psi_3(P)}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_3,P}(Q)^{\lambda_3+1} \cdot f_{\lambda_3, \psi_3(P)}(Q) \cdot l_{[\lambda_3]\psi_3(P), \psi_3(P)}(Q) \end{aligned}$$

として計算する。

[0092] さらに、6次の場合も同様に、

[数31]

$$\begin{aligned} f_{r,P}(Q) &= f_{\lambda_6^2-\lambda_6+1,P}(Q) \\ &= f_{\lambda_6,P}(Q)^{\lambda_6-1} \cdot f_{\lambda_6-1, [\lambda_6]P}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_6,P}(Q)^{\lambda_6-1} \cdot f_{\lambda_6-1, \psi_6(P)}(Q) \cdot (x_Q - x_P) \\ &= \left\{ f_{\lambda_6-1,P}(Q) \cdot l_{[\lambda_6-1]P, P}(Q) / v_{[\lambda_6-1]P+P}(Q) \right\}^{\lambda_6-1} \\ &\quad \cdot f_{\lambda_6-1, \psi_6(P)}(Q) \cdot (x_Q - x_P) \end{aligned}$$

として計算する。

[0093] 以下において、本発明のペアリング演算の実施形態について、図を用いて説明する。

図1は、本発明の実施形態にかかるペアリング演算装置の概略構成を示す模式図である。

図2は、本発明の実施形態にかかるペアリング演算装置の全体構成を例示したブロック図である。

図1及び図2については、スカラー倍算の場合と同様であるので説明は省略する。

[0094] 次に、本実施形態の詳細について図を用いて説明する。

＜有理点部分群の特定＞

[0095] 図3は図1で示した装置で所定のプログラムを実行させることにより実現される有理点部分群特定部の機能構成を例示した図である。

図4は有理点部分群特定部の処理を行う有理点部分群特定プログラムのフローチャートである。

図3及び図4についてもスカラー倍算の場合と同様であるので説明は省略する。

＜ペアリング演算プログラム＞

[0096] 図7は、図1で示した装置で所定のプログラムを実行させることにより実現されるペアリング演算部の機能構成を例示した図である。

図8は、ペアリング演算部の処理を行うペアリング演算プログラムのフローチャートである。以下では4次の場合について説明する。

[0097] 起動したペアリング演算プログラムによって、電子計算機10では、CPU 11を入力手段として機能させて、メモリ装置13にあらかじめ記憶されている整数 $\lambda_1 = \lambda_4$ のデータと、有理点Pのデータ、及び署名データとしてメモリ装置13に一旦記憶された有理点QのデータをCPUの内部に設けている所定のレジスタにそれぞれ入力している（パラメータ入力部）（ステップS1）。

[0098] 次いで、有理関数 $f_{\lambda_4, P}(Q)$ の変数 f_1, h_1 を初期化すなわち $f_1 = 1$ 、 $h_1 = 1$ としている。（ステップS2）

- [0099] 次いで、電子計算機10では、ペアリング演算プログラムによってCPU 11を第1演算手段として機能させて、ミラーのアルゴリズムによって有理関数 $f_{\lambda_{4,P}}(Q)$ を演算しその演算結果をメモリ装置13に記憶している。(ステップS3)。
- [0100] この有理関数 $f_{\lambda_{4,P}}(Q)$ は、具体的には図9に示すように実行している。特にステップS2では、有理関数 $f_{\lambda_{4,P}}(Q)$ の演算とともに T_1 の中間結果を楕円2倍算、楕円加算に分けてメモリ装置13に記憶している。
- [0101] まず、初期設定として $T_1 \leftarrow P$ とするとともに整数 λ を2進数表示とした場合のビット数を i としている(ステップS31)。
- [0102] 次いで、ステップS32では、CPU 11を第2演算手段として機能させて直線及び垂線における値を求め、有理関数 $f_{\lambda_{4,P}}(Q)$ の楕円2倍算に伴う所定の演算を行っている。ここで、有理関数を求めるには f_1/h_1 が必要であるが、都度の除算を避けて f_1 、 h_1 のままとしている。
- [0103] 次いで、 T_1 の中間結果を配列 $C_{dbl}[i]$ に記憶するとともに有理点変数 T_1 の楕円2倍算を行い T_1 に代入している。(ステップS33)。
- [0104] 次いで、ステップS34では、整数 λ_4 の低次から数えて i 番目のビットの値 λ_{4i} が「1」かであるか「0」であるかを判定し、 $\lambda_{4i}=1$ の場合には、ステップS35で、有理関数 $f_{\lambda_{4,P}}(Q)$ の楕円加算に伴う所定の演算を行っている。ここでも都度の除算を避けて f_1 、 h_1 のままとしている。ステップS36で、 T_1 の中間結果を配列 $C_{add}[i]$ に記憶するとともに有理点変数 T_1 の有理点 P との楕円加算を行い T_1 に代入している。
- [0105] 次いで、 $\lambda_{4i} \neq 1$ の場合、 i のデクリメントを行って(ステップS38)、ステップS32に戻り、ステップS37で $i=1$ になるまで繰り返すことにより、有理関数 $f_{\lambda_{4,P}}(Q)$ を演算しその結果である f_1 、 h_1 をメモリ装置13にそれぞれ記憶している。
- [0106] 次いで、有理関数 $f_{\lambda_{4,P}}(Q)$ の変数 f_1 、 h_1 をメモリ装置13から読み出し初期化している。すなわち、ステップS3での結果をステップS5の初期値としている。(ステップS4)。
- [0107] 次いで、電子計算機10では、ペアリング演算プログラムによってCPU 11を

第1演算手段として機能させて、ミラーのアルゴリズムによって有理関数 $f_{\lambda_4, \phi_4(P)}(Q)$ を演算しその演算結果をメモリ装置13に記憶している。(ステップS5)。

[0108] この有理関数 $f_{\lambda_4, \phi_4(P)}(Q)$ は、具体的には図10に示すように実行している。

[0109] まず、初期設定として、整数 λ_4 を2進数表示とした場合のビット数を i としている(ステップS51)

[0110] ステップS52では、配列 $C_{dbl}[i]$ を記憶装置13から読み出し、CPU 11を自己準同型写像手段として機能させて、 $\phi_4(C_{dbl}[i])$ を求め、その結果を T_1 に代入している。

[0111] 次に、ステップS53では、CPU 11を第2演算手段として機能させて直線及び垂線における値を求め、有理関数 $f_{\lambda_4, P}(Q)$ の楕円2倍算に伴う所定の演算を行っている。ここで、有理関数を求めるには f_1/h_1 が必要であるが、都度の除算を避けて f_1, h_1 のままとしている。

[0112] 次に、ステップS54では、整数 λ_4 の低次から数えて i 番目のビットの値 λ_{4i} が「1」かであるか「0」であるかを判定し、 $\lambda_{4i}=1$ の場合には、ステップS55でメモリ装置13から配列 $C_{add}[i]$ を読み出し、CPU 11を自己準同型写像手段として機能させて、 $\phi_4(C_{add}[i])$ を求め、その結果を T_1 に代入している。ステップS56では、CPU 11を第2演算手段として機能させて直線及び垂線における値を求め、有理関数 $f_{\lambda_4, P}(Q)$ の楕円加算に伴う所定の演算を行っている。ここでも都度の除算を避けて f_1, h_1 のままとしている。

[0113] 次に、 $\lambda_{4i} \neq 1$ の場合、 i のデクリメントを行って(ステップS58)、ステップS52に戻り、ステップS57で $i=1$ になるまで繰り返すことにより、有理関数 $f_{\lambda_4, \phi_4(P)}(Q)$ を演算している。

[0114] 次に、ステップS59では、 f_1/h_1 を行い f_1 に代入している。ループの中で除算を実行することなく、1度の除算で済ませている。次に、 $f_1 \cdot (x_0 - x_P)$ を計算し $f'_{r, P}(Q)$ の値を求め、 f_1 に代入し、その結果をメモリ装置13に記憶している。

[0115] 具体的には、記号の意味を次の通りとして、

λ_{4i} : λ_4 を2進表記した際の低次から*i*番目のビット

$l_{T_1, T_1}(Q)$: 有理点 T_1 での接線における有理点 Q の値

(表示の制限上、下付き文字は正しくは T_1 であるが $T1$ としている。以下も同じ。)

$l_{T_1, P}(Q)$: 有理点 T_1 と有理点 P を通る直線における有理点 Q の値

$v_{2T_1}(Q)$: 有理点 $2T_1$ での垂線における有理点 Q の値

$v_{T_1+P}(Q)$: 有理点 T_1+P での垂線における有理点 Q の値

$C_{dbl}[i]$: 繰り返し回数が*i*番目の2倍算 $2T_1$ を格納するための配列(メモリ)

$C_{add}[i]$: 繰り返し回数が*i*番目の加算 T_1+P を格納するための配列(メモリ)

以下のアルゴリズムを実行している。

[表2] ミラーのアルゴリズム 1 (4次の場合 : スピード重視型)

入力: $\lambda_4, P \in G_1, Q \in G_2$

出力: $f'_{r, P}(Q)$

1. $f_1 \leftarrow 1, f_2 \leftarrow 1, h_1 \leftarrow 1, h_2 \leftarrow 1, T_1 \leftarrow P$

2. For $i = \lceil \log_2(\lambda_4) \rceil$ down to 1 do:

3. $f_1 \leftarrow f_1^2 \cdot l_{T_1, T_1}(Q).$

4. $h_1 \leftarrow h_1^2 \cdot v_{2T_1}(Q).$

5. $C_{dbl}[i] \leftarrow T_1.$

6. $T_1 \leftarrow 2T_1.$

7. if $\lambda_{4i} = 1$, then:

8. $f_1 \leftarrow f_1 \cdot l_{T_1, P}(Q).$

9. $h_1 \leftarrow h_1 \cdot v_{T_1+P}(Q).$

10. $C_{add}[i] \leftarrow T_1.$

11. $T_1 \leftarrow T_1 + P.$

12. $T_1 \leftarrow P.$

13. $f_2 \leftarrow f_1.$

14. $h_2 \leftarrow h_1.$

15. For $i = \lceil \log_2(\lambda_4) \rceil$ down to 1 do:

16. $T_1 \leftarrow \phi_4(C_{dbl}[i]).$

17. $f_1 \leftarrow f_1^2 \cdot l_{T_1, T_1}(Q).$

18. $h_1 \leftarrow h_1^2 \cdot v_{2T_1}(Q).$

19. if $\lambda_{4i} = 1$, then:

20. $T_1 \leftarrow \phi_4(C_{add}[i]).$

21. $f_1 \leftarrow f_1 \cdot f_2 \cdot l_{T_1, P}(Q).$

22. $h_1 \leftarrow h_1 \cdot h_2 \cdot v_{T_1+P}(Q).$

23. $f_1 \leftarrow f_1/h_1.$

24. $f_1 \leftarrow f_1 \cdot (x_Q - x_P).$

25. Return $f_1.$

すなわち、CPU 11は、メモリ装置13を用いて上記手順の各演算を行い $f_{1,P}(Q)$ を得てその値をメモリ装置13に記憶している。具体的には、手順1では、有理関数変数 f_1, f_2, h_1, h_2 を1に、有理点変数 T_1 を有理点 P に初期設定している。手順2では、変数 i を整数 λ_4 を2進数展開した時のビット数に初期設定し、手順3から手順11までを繰り返している。手順3及び4では有理関数の演算を直線及び垂線に分けて行っている。有理関数の値を求めるには f_1/h_1 が必要であるが除算の回数を減らすためループの中では除算を行わないようにしている。手順5では、中間結果の T_1 を配列 $C_{dbl}[i]$ に代入している。手順6では、有理点 T_1 の楕円2倍算を行い T_1 に代入している。手順7では、整数 λ_4 の低次から i 番目のビットが「1」か「0」かを判定し「1」の場合に手順8から11を実行している。手順8及び9では有理関数の演算を直線及び垂線に分けて行っている。有理関数の値を求めるには f_1/h_1 が必要であるが除算の回数を減らすためループの中では除算を行わないようにしている。手順10では、有理点変数 T_1 の中間結果を配列 $C_{add}[i]$ に代入している。手順11では、有理点変数 T_1 と有理点 P を楕円加算しその値を T_1 に代入している。

手順12では有理点変数 T_1 を有理点 P に初期設定している。手順13, 14では、前半の結果を f_2, h_2 に代入している。手順15では、変数 i を、整数 λ_4 を2進数展開し

た時のビット数に初期設定し、手順16から手順22までを繰り返している。手順16では、配列 $C_{dbl}[i]$ をメモリ装置13から読み出し自己準同型写像を行い、その値を有理点変数 T_1 に代入している。手順17, 18では、有理関数の演算を直線及び垂線に分けて行っている。有理関数の値を求めるには f_1/h_1 が必要であるが除算の回数を減らすためループの中では除算を行わないようにしている。手順19では、整数 λ_4 の低次から i 番目のビットが「1」か「0」かを判定し「1」の場合に手順20から22を実行している。手順20では、配列 $C_{add}[i]$ をメモリ装置13から読み出し自己準同型写像を行い、その値を有理点変数 T_1 に代入している。手順21及び22では、有理関数の演算を直線及び垂線に分けて行うと共にそれぞれ f_2 、 h_2 を掛け合わせるにより λ_4 乗を実現している。手順23, 24では最終的な有理関数の値 $f'_{r,p}(Q)$ を求め f_1 に代入している。

[0116] 次いで、電子計算機10では、ペアリング演算プログラムによってCPU 11を第4演算手段として機能させて、ステップS5で得られた $f'_{r,p}(Q)$ の値をメモリ装置13から読み出し、ペアリング $e(P, Q)$ における最終べきの、べき乗算を行いその結果をメモリ装置13に記憶している（ステップS6）。

[0117] 具体的には、

[表3] 最終べきのアルゴリズム

1. $a \leftarrow p-1$
2. $a \leftarrow a \cdot r^{-1}$
3. $f' \leftarrow f'^a$
4. Return f'

として演算し、 f' すなわち $e(P, Q)$ の値をメモリ装置13に記憶している。

[0118] 認証サーバを構成する電子計算機10では、上述したようにして得られたペアリングの演算結果を用いて認証処理を行っている。

[0119] 以上、4次の場合のペアリング演算について、図8及び表2では、前半のミラー・アルゴリズムの計算の結果を求める際に得られた中間結果をメモリ装置13に記憶しておき後半のミラー・アルゴリズムの計算に活用することによりペアリング演算を高速に実行することとしているが、メモリ容量を節約し

て実行することもできる。図 1 1 及び表 4 は、その場合のフローチャート及びアルゴリズムである。記号の意味は、表 2 の場合と同じなので説明は省略する。

[表 4] ミラーのアルゴリズム 2 (4 次: メモリ節約型)

入力: $\lambda_4, P \in G_1, Q \in G_2$

出力: $f'_{r,P}(Q)$

1. $f_1 \leftarrow 1, f_2 \leftarrow 1, h_1 \leftarrow 1, h_2 \leftarrow 1, T_1 \leftarrow P$

2. For $i = [\log_2(\lambda_4)]$ down to 1 do:

3. $f_1 \leftarrow f_1^2 \cdot l_{T_1, T_1}(Q).$

4. $h_1 \leftarrow h_1^2 \cdot v_{2T_1}(Q).$

5. $T_2 \leftarrow \phi_4(T_1).$

6. $f_2 \leftarrow f_2^2 \cdot l_{T_2, T_2}(Q).$

7. $h_2 \leftarrow h_2^2 \cdot v_{2T_2}(Q).$

8. $T_1 \leftarrow 2T_1.$

9. If $\lambda_{4i} = 1$, then :

10. $f_1 \leftarrow f_1 \cdot l_{T_1, P}(Q).$

11. $h_1 \leftarrow h_1 \cdot v_{T_1+P}(Q).$

12. $T_2 \leftarrow \phi_4(T_1).$

13. $f_2 \leftarrow f_2 \cdot l_{T_2, P}(Q).$

14. $h_2 \leftarrow h_2 \cdot v_{T_2+P}(Q).$

15. $T_1 \leftarrow T_1 + P.$

16. $f_1 \leftarrow f_1^{\lambda_4 - 4}.$

17. $h_1 \leftarrow h_1^{\lambda_4 - 4}.$

18. $f_1 \leftarrow (f_1 \cdot f_2) / (h_1 \cdot h_2).$

19. $f_1 \leftarrow f_1 \cdot (x_0 - x_P).$

20. Return $f_1.$

すなわち、手順 1 では、有理関数変数 f_1, f_2, h_1, h_2 を 1 に、有理点変数 T_1 を有理点 P に初期設定している。手順 2 では、変数 i を整数 λ_4 を 2 進数展開した時のビ

ット数に初期設定し、手順3から手順15までを繰り返している。手順3及び4では、第2演算手段を用いて、楕円2倍算にともなう有理関数の演算を直線及び垂線に分けて行っている。有理関数の値を求めるには f_1/h_1 が必要であるが除算の回数を減らすためループの中では除算を行わないようにしている。手順5では、自己準同型写像演算手段により、有理点 T_1 を変換し T_2 に代入している。手順6及び7では、第2演算手段を用いて、楕円加算にともなう有理関数の演算を直線及び垂線に分けて行っている。有理関数の値を求めるには f_2/h_2 が必要であるが除算の回数を減らすためループの中では除算を行わないようにしている。手順8では、有理点 T_1 の楕円2倍算を行い T_1 に代入している。手順9では、整数 λ_4 の低次から i 番目のビットが「1」か「0」かを判定し「1」の場合に手順10から15を実行している。手順10及び11では、 T_1 について有理関数の演算を直線及び垂線に分けて行っている。有理関数の値を求めるには f_1/h_1 が必要であるが除算の回数を減らすためループの中では除算を行わないようにしている。手順12では、自己準同型写像演算手段により、有理点 T_1 を変換し T_2 に代入している。手順13及び14では、第2演算手段を用いて、楕円加算にともなう有理関数の演算を直線及び垂線に分けて行っている。有理関数の値を求めるには f_2/h_2 が必要であるが除算の回数を減らすためループの中では除算を行わないようにしている。手順15では、有理点変数 T_1 と有理点 P を楕円加算しその値を T_1 に代入している。手順16及び17では、 f_1 及び h_1 の λ_4 乗算を行っている。

手順18及び19では最終的な有理関数の値 $f'_{r,p}(Q)$ を求め f_1 に代入している。除算は、手順18の1回だけで済ませている。

[0120] 以上、本実施形態では、4次の場合について説明したが、3次及び6次の場合でも同様のアルゴリズムでペアリング演算を高速に演算できる。

以下に、3次の場合のアルゴリズムを示す。記号の意味は、表2の場合と同様なので説明は省略する。

[表5] ミラーのアルゴリズム3(3次の場合：スピード重視型)

入力: λ_3 , $P \in G_1$, $Q \in G_2$

出力 : $f'_{r,P}(Q)$

1. $f_1 \leftarrow 1, f_2 \leftarrow 1, h_1 \leftarrow 1, h_2 \leftarrow 1, T_1 \leftarrow P.$

2. For $i = [\log_2(\lambda_3)]$ down to 1 do:

3. $f_1 \leftarrow f_1^2 \cdot l_{T_1, T_1}(Q).$

4. $h_1 \leftarrow h_1^2 \cdot v_{2T_1}(Q).$

5. $C_{dbl}[i] \leftarrow T_1.$

6. $T_1 \leftarrow 2T_1.$

7. if $\lambda_{3i} = 1$, then:

8. $f_1 \leftarrow f_1 \cdot l_{T_1, P}(Q).$

9. $h_1 \leftarrow h_1 \cdot v_{T_1+P}(Q).$

10. $C_{add}[i] \leftarrow T_1.$

11. $T_1 \leftarrow T_1 + P.$

12. $T_1 \leftarrow P.$

13. $f_2 \leftarrow f_1.$

14. $f_3 \leftarrow f_1 / h_1.$

15. $h_2 \leftarrow h_1.$

16. For $i = [\log_2(\lambda_3)]$ down to 1 do:

17. $T_1 \leftarrow \phi_3(C_{dbl}[i]).$

18. $f_1 \leftarrow f_1^2 \cdot l_{T_1, T_1}(Q).$

19. $h_1 \leftarrow h_1^2 \cdot v_{2T_1}(Q).$

20. if $\lambda_{3i} = 1$, then:

21. $T_1 \leftarrow \phi_3(C_{add}[i]).$

22. $f_1 \leftarrow f_1 \cdot f_2 \cdot l_{T_1, P}(Q).$

23. $h_1 \leftarrow h_1 \cdot h_2 \cdot v_{T_1+P}(Q).$

24. $f_1 \leftarrow f_1 \cdot l_{T_1, \phi_3(P)}(Q).$

25. $f_1 \leftarrow f_1 / h_1.$

26. $f_1 \leftarrow f_1 \cdot f_3.$

27. Return $f_1.$

3次の場合のアルゴリズムは、4次の場合と同様であるので、異なる部分のみ説明する。

手順14では、前半の結果を f_3 に代入し、手順26で $\lambda_3 + 1$ 乗を得ている。手順24では、補正項 $l_{T_1, \phi_3(P)}(Q)$ を掛け合わせている。

[0121] 以下に、6次の場合のアルゴリズムを示す。記号の意味は、表2の場合と同様なので説明は省略する。

[表6] ミラーのアルゴリズム4 (6次の場合：スピード重視型)

入力: $\lambda_6, P \in G_1, Q \in G_2$

出力: $f'_{r,P}(Q)$

1. $f_1 \leftarrow 1, f_2 \leftarrow 1, h_1 \leftarrow 1, h_2 \leftarrow 1, T_1 \leftarrow P.$
2. For $i = [\log_2(\lambda_6 - 1)]$ down to 1 do:
3. $f_1 \leftarrow f_1^2 \cdot l_{T_1, T_1}(Q).$
4. $h_1 \leftarrow h_1^2 \cdot v_{2T_1}(Q).$
5. $C_{dbl}[i] \leftarrow T_1.$
6. $T_1 \leftarrow 2T_1.$
7. if $\lambda_{6i} = 1$, then:
8. $f_1 \leftarrow f_1 \cdot l_{T_1, P}(Q).$
9. $h_1 \leftarrow h_1 \cdot v_{T_1+P}(Q).$
10. $C_{add}[i] \leftarrow T_1.$
11. $T_1 \leftarrow T_1 + P.$
12. $T_1 \leftarrow P.$
13. $f_1 \leftarrow f_1 \cdot l_{T_1, P}(Q).$
14. $h_1 \leftarrow h_1 \cdot v_{T_1+P}(Q).$
15. $f_2 \leftarrow f_1.$
16. $h_2 \leftarrow h_1.$
17. For $i = [\log_2(\lambda_6 - 1)]$ down to 1 do:
18. $T_1 \leftarrow \phi_6(C_{dbl}[i]).$
19. $f_1 \leftarrow f_1^2 \cdot l_{T_1, T_1}(Q).$

20. $h_1 \leftarrow h_1^2 \cdot v_{2T_1}(Q).$
21. if $\lambda_{6i}=1$, then:
22. $T_1 \leftarrow \phi_6(C_{add}[i]).$
23. $f_1 \leftarrow f_1 \cdot f_2 \cdot l_{T_1,p}(Q).$
24. $h_1 \leftarrow h_1 \cdot h_2 \cdot v_{T_1+p}(Q).$
25. $f_1 \leftarrow f_1 / h_1.$
26. $f_1 \leftarrow f_1 \cdot (x_Q - x_P).$
27. Return $f_1.$

6次の場合のアルゴリズムも4次の場合と同様であるので異なる部分のみ説明する。

手順2及び17の繰り返し回数は $\lambda_6 - 1$ 回としている。手順13、14では補正項を掛け合わせている。

[0122] なお、上述においては、各演算結果を記憶する記憶手段としてメモリ装置13を用いることとしたがCPU 11の内部に設けているレジスタを上記記憶手段として用いるようにしてもよい。

[0123] また、有理点群特定プログラム及びペアリング演算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することができる。また、これらのプログラムをサーバのコンピュータの記憶装置に記憶しておき、ネットワークを介して電子計算機の記憶装置にダウンロードすることもできる。

符号の説明

- [0124]
- 10 電子計算機
 - 11 CPU
 - 12 記憶装置
 - 13 メモリ装置
 - 14 バス
 - 15 入出力制御部
 - 20 電気通信回線
 - 30 クライアント装置

- 100 認証データ入力部
- 200 有理点部分群特定部
- 300 ペアリング演算部
- 400 スカラー倍算演算部
- 500 認証結果出力部
- 210 有理点入力部
- 220 定数演算部
- 230 自己準同型演算部
- 240 有理点演算部
- 250 判定部
- 290 レジスタ
- 310 パラメータ入力部
- 320 第3演算部
- 330 第1演算部
- 340 第2演算部
- 350 自己準同型写像演算部
- 360 第4演算部
- 380 記憶手段
- 390 レジスタ
- 410 パラメータ入力部
- 420 定数演算部
- 430 自己準同型写像演算部
- 440 マルチ・スカラー倍算演算部
- 490 レジスタ

請求の範囲

- [請求項1] 標数 p の有限体 F_p 上で定義された楕円曲線上の有理点の成す加法群を $E(F_p)$ とし、合成数位数 r を持つ有理点の集合すなわち前記加法群の部分群を $G=E(F_p)[r]$ として、有理点 $P \in G$ の整数 $0 < s < r$ によるスカラー倍算 $[s]P$ を演算するCPU及び記憶手段を備えたスカラー倍算装置において、
- 前記加法群 $E(F_p)$ は、埋め込み次数を 1 とし、
- 前記CPUは、
- 有理点 $P' \in E(F_p)[r]$ 、前記整数 s 、をそれぞれ入力して前記記憶手段に記憶する入力手段と、
- 前記記憶手段から前記有理点 P' を読み出し、自己準同型写像 $\phi(P) = \lambda P$ (λ は整数) を満足する前記有理点 P の集合である前記部分群 G を特定し、前記有理点 P を前記記憶手段に記憶する有理点部分群特定手段と、
- 前記記憶手段から前記有理点 P を読み出し、前記自己準同型写像 $\phi(P)$ を演算し、その結果の有理点を前記記憶手段に記憶する自己準同型写像演算手段と、
- 前記記憶手段から前記整数 s を読み出し、次式に基づいて λ を展開し、
- $$s = s_0 + s_1 \lambda$$
- 係数 s_0 及び s_1 を求めその結果を前記記憶手段に記憶する λ 進展開手段と、
- スカラー倍算を、
- $$[s]P = [s_0 + s_1 \lambda] P = [s_0] P + [s_1] \phi(P)$$
- として演算し、その結果を前記記憶手段に記憶するマルチ・スカラー倍算演算手段と、を有することを特徴とするスカラー倍算装置。
- [請求項2] 前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $3 \nmid (p-1)$ であり、
- 前記合成数位数 r は、 $r \nmid \#E(F_p)$, $3 \nmid (r-1)$ を満たし、

前記整数 λ は、 $\lambda^2 + \lambda + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$(x, y) \rightarrow (\varepsilon x, y)$, $\varepsilon^3 = 1$, $\varepsilon (\neq 1) \in F_p$ である請求項 1 に記載の
スカラー倍算装置。

[請求項3]

前記楕円曲線は、 $E: y^2 = x^3 + ax$, $a \in F_p$, $4 \nmid (p-1)$ であり、

前記合成数位数 r は、 $r \mid \#E(F_p)$, $4 \mid (r-1)$ を満たし、

前記整数 λ は、 $\lambda^2 + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$(x, y) \rightarrow (-x, \zeta y)$, $\zeta^4 = 1$, $\zeta (\neq 1) \in F_p$ である請求項 1 に記載
のスカラー倍算装置。

[請求項4]

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $6 \mid (p-1)$ であり、

前記合成数位数 r は、 $r \mid \#E(F_p)$, $3 \mid (r-1)$ を満たし、

前記整数 λ は、 $\lambda^2 - \lambda + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$(x, y) \rightarrow (\varepsilon x, -y)$, $\varepsilon^3 = 1$, $\varepsilon (\neq 1) \in F_p$ である請求項 1 に記載のスカ
ラー倍算装置。

[請求項5]

標数 p の有限体 F_p 上で定義された楕円曲線上の有理点の成す加法群
を $E(F_p)$ とし、合成数位数 r を持つ有理点の集合すなわち前記加法群
の部分群を $G = E(F_p)[r]$ として、有理点 $P \in G$ の整数 $0 < s < r$ によるスカ
ラー倍算 $[s]P$ を、CPU 及び記憶手段を備えた電子計算機で演算するスカ
ラー倍算方法において、

前記加法群 $E(F_p)$ は、埋め込み次数を 1 とし、

前記電子計算機の CPU を入力手段として機能させて、有理点 $P' \in E(F_p)$
 $[r]$ 、前記整数 s 、をそれぞれ入力して前記記憶手段に記憶する入力
ステップと、

前記電子計算機の CPU を有理点部分群特定手段として機能させて、前
記記憶手段から P' を読み出し、自己準同型写像 $\phi(P) = \lambda P$ (λ は整数
) を満足する前記有理点 P の集合である前記部分群 G を特定し、前記有

理点Pを前記記憶手段に記憶する有理点部分群特定ステップと、
 前記電子計算機のCPUを自己準同型写像演算手段として機能させて、
 前記記憶手段から前記有理点Pを読み出し、前記自己準同型写像 $\phi(P)$
 を演算しその結果の有理点を前記記憶手段に記憶する自己準同型写像
 演算ステップと、
 前記電子計算機のCPUを λ 進展開手段として機能させて、前記記憶手
 段から前記整数 s を読み出し次式に基づいて λ 進展開し、

$$s = s_0 + s_1 \lambda$$

係数 s_0 及び s_1 を求めその結果を前記記憶手段に記憶する λ 進展開ス
 テップと、
 前記電子計算機のCPUをマルチ・スカラー倍算演算手段として機能さ
 せて、スカラー倍算を、

$$[s]P = [s_0 + s_1 \lambda]P = [s_0]P + [s_1]\phi(P)$$

として演算しその結果を前記記憶手段に記憶するマルチ・スカラー倍
 算演算ステップと、を有することを特徴とするスカラー倍算方法。

[請求項6]

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $3 \mid (p-1)$ であり、
 前記合成数位数 r は、 $r \mid \#E(F_p)$, $3 \mid (r-1)$ を満たし、
 前記整数 λ は、 $\lambda^2 + \lambda + 1 \equiv 0 \pmod{r}$ を満たし、
 前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、
 $(x, y) \rightarrow (\varepsilon x, y)$, $\varepsilon^3 = 1$, $\varepsilon (\neq 1) \in F_p$ である請求項5に記載のスカ
 ラー倍算方法。

[請求項7]

前記楕円曲線は、 $E: y^2 = x^3 + ax$, $a \in F_p$, $4 \mid (p-1)$ であり、
 前記合成数位数 r は、 $r \mid \#E(F_p)$, $4 \mid (r-1)$ を満たし、
 前記整数 λ は、 $\lambda^2 + 1 \equiv 0 \pmod{r}$ を満たし、
 前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、
 $(x, y) \rightarrow (-x, \zeta y)$, $\zeta^4 = 1$, $\zeta (\neq 1) \in F_p$ である請求項5に記載のスカ
 ラー倍算方法。

[請求項8]

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $6 \mid (p-1)$ であり、

前記合成数位数 r は、 $r \mid \#E(F_p)$, $3 \mid (r-1)$ を満たし、
 前記整数 λ は、 $\lambda^2 - \lambda + 1 \equiv 0 \pmod{r}$ を満たし、
 前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、
 $(x, y) \rightarrow (\varepsilon x, -y)$, $\varepsilon^3 = 1$, $\varepsilon (\neq 1) \in F_p$ である請求項 5 に記載のスカ
 ラー倍算方法。

[請求項9] 標数 p の有限体 F_p 上で定義された楕円曲線上の有理点の成す加法群
 を $E(F_p)$ とし、合成数位数 r を持つ有理点の集合すなわち前記加法群
 の部分群を $G = E(F_p)[r]$ として、有理点 $P \in G$ の整数 $0 < s < r$ によるスカ
 ラー倍算 $[s]P$ を、CPU 及び記憶手段を備えた電子計算機に演算させるス
 カラー倍算プログラムにおいて、
 前記加法群 $E(F_p)$ は、埋め込み次数を 1 とし、
 前記電子計算機の CPU を、
 有理点 $P' \in E(F_p)[r]$ 、前記整数 s をそれぞれ入力し、前記記憶手段
 に記憶する入力手段、
 前記記憶手段から P' を読み出し自己準同型写像 $\phi(P) = \lambda P$ を満足す
 る前記有理点 P の集合である前記部分群 G を特定し、前記有理点 P を前
 記記憶手段に記憶する有理点部分群特定手段、前記記憶手段から前記
 有理点 P を読み出し、自己準同型写像 $\phi(P)$ を演算しその結果の有理点
 を前記記憶手段に記憶する自己準同型写像演算手段、
 前記記憶手段から前記整数 s を読み出し、次式に基づいて λ 進展開し
 、

$$s = s_0 + s_1 \lambda$$

係数 s_0 及び s_1 を求めその結果を前記記憶手段に記憶する λ 進展開手
 段、

スカラー倍算を、

$$[s]P = [s_0 + s_1 \lambda]P = [s_0]P + [s_1] \phi(P)$$

として演算し、その結果を前記記憶手段に記憶するマルチ・スカラー
 倍算演算手段、

として機能させることを特徴とするスカラー倍算プログラム。

[請求項10]

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $3 \mid (p-1)$ であり、

前記合成数位数 r は、 $r \mid \#E(F_p)$, $3 \mid (r-1)$ を満たし、

前記整数 λ は、 $\lambda^2 + \lambda + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$(x, y) \rightarrow (\varepsilon x, y)$, $\varepsilon^3 = 1$, $\varepsilon (\neq 1) \in F_p$ である請求項9に記載のスカラー倍算プログラム。

[請求項11]

前記楕円曲線は、 $E: y^2 = x^3 + ax$, $a \in F_p$, $4 \mid (p-1)$ であり、

前記合成数位数 r は、 $r \mid \#E(F_p)$, $4 \mid (r-1)$ を満たし、

前記整数 λ は、 $\lambda^2 + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$(x, y) \rightarrow (-x, \zeta y)$, $\zeta^4 = 1$, $\zeta (\neq 1) \in F_p$ である請求項9に記載のスカラー倍算プログラム。

[請求項12]

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $6 \mid (p-1)$ であり、

前記合成数位数 r は、 $r \mid \#E(F_p)$, $3 \mid (r-1)$ を満たし、

前記整数 λ は、 $\lambda^2 - \lambda + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$(x, y) \rightarrow (\varepsilon x, -y)$, $\varepsilon^3 = 1$, $\varepsilon (\neq 1) \in F_p$ である請求項9に記載のスカラー倍算プログラム。

[請求項13]

標数 p の有限体 F_p 上で定義された楕円曲線上の有理点の成す加法群

を $E(F_p)$ とし、合成数位数 r を持つ有理点の集合すなわち前記加法群

の部分群を $G_1 = E(F_p)[r]$ 、 $G_2 = E(F_p)[r]$ として、次式により、

$$e: G_1 \times G_2 \rightarrow F_p^* / (F_p^*)^r$$

である非退化な双線形写像としてペアリング e を定義し、

有理点 $P(x_p, y_p) \in G_1$ 及び $Q(x_0, y_0) \in G_2$ 、ミラーのアルゴリズムを用いて

計算される有理関数を f として、ペアリング $e(P, Q)$ を演算するCPU及

び記憶手段を備えたペアリング演算装置において、

前記加法群 $E(F_p)$ は、埋め込み次数を 1 とし、

前記CPUは、

有理点 P' を入力して前記記憶手段に記憶する入力手段と、

前記記憶手段から前記有理点 P' を読み出し、自己準同型写像 ϕ により、

$\lambda_1 P = \phi(P)$ 、 $\lambda_2 Q = \phi(Q)$ ($\lambda_1 \neq \lambda_2$ は整数)を満足する前記有理点 P 及び Q の集合である前記部分群 G_1 及び G_2 を特定する有理点部分群特定手段と、

前記記憶手段から前記有理点 P または Q を読み出し、前記自己準同型写像 $\phi(P)$ または $\phi(Q)$ を演算しその結果の有理点を前記記憶手段に記憶する自己準同型写像演算手段と、

前記 f を演算する第1演算手段と、

所定の有理点を通る直線及び垂線の前記有理点 Q における値を演算する第2演算手段と、

前記 f と前記値を用いて $f'_{r,p}(Q)$ を演算する第3演算手段と、

前記 $f'_{r,p}(Q)$ を用いて前記ペアリング $e(P, Q)$ を

[数1]

$$e(P, Q) = f'_{r,p}(Q)^{(p-1)/r}$$

として演算する第4演算手段と

を有するペアリング演算装置。

[請求項14]

前記楕円曲線は、 $E: y^2 = x^3 + ax$, $a \in F_p$, $4 \nmid (p-1)$ であり、

前記合成数位数 r は、 $r \nmid \#E(F_p)$, $4 \nmid (r-1)$ を満たし、

前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$$(x, y) \rightarrow (-x, \zeta y), \zeta^4 = 1, \zeta (\neq 1) \in F_p \text{ であり、}$$

前記 $f'_{r,p}(Q)$ は、

[数2]

$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2 + 1, p}(Q) \\ &= f_{\lambda_1^2, p}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_1, p}(Q)^{\lambda_1} \cdot f_{\lambda_1, \psi(P)}(Q) \cdot (x_Q - x_P) \end{aligned}$$

である請求項 1 3 に記載のペアリング演算装置。

[請求項15]

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $3 \mid (p-1)$ であり、

前記合成数位数 r は、 $r \mid \#E(F_p)$, $3 \mid (r-1)$ を満たし、

前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 + \lambda_1 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 + \lambda_2 + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$$(x, y) \rightarrow (\varepsilon x, y), \quad \varepsilon^3 = 1, \quad \varepsilon (\neq 1) \in F_p \quad \text{であり、}$$

前記 $f'_{r,p}(Q)$ は、

[数3]

$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2 + \lambda_1 + 1, p}(Q) \\ &= f_{\lambda_1, p}(Q)^{\lambda_1 + 1} \cdot f_{\lambda_1 + 1, \psi(p)}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_1, p}(Q) \cdot f_{\lambda_1, p}(Q)^{\lambda_1} \cdot f_{\lambda_1, \psi(p)}(Q) \cdot l_{[\lambda_1]\psi(p), \psi(p)}(Q) \end{aligned}$$

である請求項 1 3 に記載のペアリング演算装置。

[請求項16]

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $6 \mid (p-1)$ であり、

前記合成数位数 r は、 $r \mid \#E(F_p)$, $3 \mid (r-1)$ を満たし、

前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 - \lambda_1 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 - \lambda_2 + 1 \equiv 0 \pmod{r}$ を満たし、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$$(x, y) \rightarrow (\varepsilon x, -y), \quad \varepsilon^3 = 1, \quad \varepsilon (\neq 1) \in F_p \quad \text{であり、}$$

前記 $f'_{r,p}(Q)$ は、

[数4]

$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2 - \lambda_1 + 1, p}(Q) \\ &= f_{\lambda_1, p}(Q)^{\lambda_1 - 1} \cdot f_{\lambda_1 - 1, \psi(p)}(Q) \cdot (x_Q - x_P) \\ &= \left\{ f_{\lambda_1 - 1, p}(Q) \cdot \frac{l_{[\lambda_1 - 1]p, p}(Q)}{v_{[\lambda_1 - 1]p + p}(Q)} \right\}^{\lambda_1 - 1} \\ &\quad \cdot f_{\lambda_1 - 1, \psi(p)}(Q) \cdot (x_Q - x_P) \end{aligned}$$

である請求項 1 3 に記載のペアリング演算装置。

[請求項17]

標数 p の有限体 F_p 上で定義された楕円曲線上の有理点の成す加法群を $E(F_p)$ とし、合成数位数 r を持つ有理点の集合すなわち前記加法群の部分群を $G_1 = E(F_p)[r]$ 、 $G_2 = E(F_p)[r]$ として、次式により、

$$e: G_1 \times G_2 \rightarrow F_p^* / (F_p^*)^r$$

である非退化な双線形写像としてペアリング e を定義し、
 有理点 $P(x_p, y_p) \in G_1$ 及び $Q(x_q, y_q) \in G_2$ 、ミラーのアルゴリズムを用いて
 計算される有理関数を f として、CPU及び記憶手段を備えた電子計算
 機でペアリング $e(P, Q)$ を演算するペアリング演算方法において、
 前記加法群 $E(F_p)$ は、埋め込み次数を1とし、
 前記電子計算機のCPUを入力手段として機能させて、有理点 P' を入力
 して前記記憶手段に記憶する入力ステップと、
 前記電子計算機のCPUを有理点部分群特定手段として機能させて、前
 記記憶手段から前記有理点 P' を読み出し、自己準同型写像 ϕ により
 、

$\lambda_1 P = \phi(P)$ 、 $\lambda_2 Q = \phi(Q)$ ($\lambda_1 \neq \lambda_2$ は整数)を満足する前記有理点
 P 及び Q の集合である前記部分群 G_1 及び G_2 を特定するステップと、

前記電子計算機のCPUを自己準同型写像演算手段として機能させて、
 前記記憶手段から前記有理点 P または Q を読み出し、前記自己準同型写
 像 $\phi(P)$ または $\phi(Q)$ を演算しその結果の有理点を前記記憶手段に記
 憶する自己準同型写像演算ステップと、

前記電子計算機のCPUを第1演算手段として機能させて、前記 f を演算
 する第1演算ステップと、

前記電子計算機のCPUを第2演算手段として機能させて、所定の有理点
 を通る直線及び垂線の前記有理点 Q における値を演算する第2演算ステ
 ップと、

前記電子計算機のCPUを第3演算手段として機能させて、前記 f と前記
 値を用いて $f'_{r,p}(Q)$ を演算する第3演算ステップと、

前記電子計算機のCPUを第4演算手段として機能させて、前記 $f'_{r,p}(Q)$
 を用いて前記ペアリング $e(P, Q)$ を

[数5]

$$e(P, Q) = f'_{r,p}(Q)^{(p-1)/r}$$

として演算する第4演算ステップと、
を有するペアリング演算方法。

[請求項18] 前記楕円曲線は、 $E: y^2 = x^3 + ax$, $a \in \mathbb{F}_p$, $4 \mid (p-1)$ であり、
前記合成数位数 r は、 $r \mid \#E(\mathbb{F}_p)$, $4 \mid (r-1)$ を満たし、
前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 + 1 \equiv 0 \pmod{r}$ を満たし、
、
前記自己準同型写像は、 $\phi: E(\mathbb{F}_p)[r] \rightarrow E(\mathbb{F}_p)[r]$ 、
 $(x, y) \rightarrow (-x, \zeta y)$, $\zeta^4 = 1$, $\zeta (\neq 1) \in \mathbb{F}_p$ であり、
前記 $f'_{r,p}(Q)$ は、

[数6]

$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2+1,p}(Q) \\ &= f_{\lambda_1^2,p}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_1,p}(Q)^{\lambda_1} \cdot f_{\lambda_1,\psi(P)}(Q) \cdot (x_Q - x_P) \end{aligned}$$

である請求項17に記載のペアリング演算方法。

[請求項19] 前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in \mathbb{F}_p$, $3 \mid (p-1)$ であり、
前記合成数位数 r は、 $r \mid \#E(\mathbb{F}_p)$, $3 \mid (r-1)$ を満たし、
前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 + \lambda_1 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 + \lambda_2 + 1 \equiv 0 \pmod{r}$ を
満たし、
前記自己準同型写像は、 $\phi: E(\mathbb{F}_p)[r] \rightarrow E(\mathbb{F}_p)[r]$ 、
 $(x, y) \rightarrow (\varepsilon x, y)$, $\varepsilon^3 = 1$, $\varepsilon (\neq 1) \in \mathbb{F}_p$ であり、
前記 $f'_{r,p}(Q)$ は、

[数7]

$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2+\lambda_1+1,p}(Q) \\ &= f_{\lambda_1,p}(Q)^{\lambda_1+1} \cdot f_{\lambda_1+1,\psi(P)}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_1,p}(Q) \cdot f_{\lambda_1,p}(Q)^{\lambda_1} \cdot f_{\lambda_1,\psi(P)}(Q) \cdot l_{[\lambda_1]\psi(P),\psi(P)}(Q) \end{aligned}$$

である請求項17に記載のペアリング演算方法。

[請求項20] 前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in \mathbb{F}_p$, $6 \mid (p-1)$ であり、
前記合成数位数 r は、 $r \mid \#E(\mathbb{F}_p)$, $3 \mid (r-1)$ を満たし、

前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 - \lambda_1 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 - \lambda_2 + 1 \equiv 0 \pmod{r}$ であり、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$$(x, y) \rightarrow (\varepsilon x, -y), \varepsilon^3 = 1, \varepsilon (\neq 1) \in F_p \text{ であり、}$$

前記 $f'_{r,p}(Q)$ は、

[数8]

$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2 - \lambda_1 + 1, p}(Q) \\ &= f_{\lambda_1, p}(Q)^{\lambda_1 - 1} \cdot f_{\lambda_1 - 1, \psi(p)}(Q) \cdot (x_Q - x_P) \\ &= \left\{ f_{\lambda_1 - 1, p}(Q) \cdot \frac{l_{[\lambda_1 - 1]p, p}(Q)}{v_{[\lambda_1 - 1]p, p}(Q)} \right\}^{\lambda_1 - 1} \\ &\quad \cdot f_{\lambda_1 - 1, \psi(p)}(Q) \cdot (x_Q - x_P) \end{aligned}$$

である請求項 17 に記載のペアリング演算方法。

[請求項21]

標数 p の有限体 F_p 上で定義された楕円曲線上の有理点の成す加法群を $E(F_p)$ とし、合成数位数 r を持つ有理点の集合すなわち前記加法群の部分群を $G_1 = E(F_p)[r]$ 、 $G_2 = E(F_p)[r]$ として、次式により、

$$e: G_1 \times G_2 \rightarrow F_p^* / (F_p^*)^r$$

である非退化な双線形写像としてペアリング e を定義し、

有理点 $P(x_P, y_P) \in G_1$ 及び $Q(x_Q, y_Q) \in G_2$ 、ミラーのアルゴリズムを用いて計算される有理関数を f として、CPU 及び記憶手段を備えた電子計算機にペアリング $e(P, Q)$ を演算させるペアリング演算プログラムにおいて、

前記加法群 $E(F_p)$ は、埋め込み次数を 1 とし、

前記電子計算機の CPU を、有理点 P' を入力して前記記憶手段に記憶する入力手段、

前記記憶手段から前記有理点 P' を読み出し、自己準同型写像 ϕ により、

$\lambda_1 P = \phi(P)$ 、 $\lambda_2 Q = \phi(Q)$ ($\lambda_1 \neq \lambda_2$ は整数) を満足する前記有理点 P 及び Q の集合である前記部分群 G_1 及び G_2 を特定する有理点部分群特定手段、

前記記憶手段から前記有理点 P または Q を読み出し、前記自己準同型写

像 $\phi(P)$ または $\phi(Q)$ を演算しその結果の有理点を前記記憶手段に記憶する自己準同型写像演算手段、

前記 f を演算する第1演算手段、

所定の有理点を通る直線及び垂線の前記有理点 Q における値を演算する第2演算手段、

前記 f と前記値を用いて $f'_{r,p}(Q)$ を演算する第3演算手段、

前記 $f'_{r,p}(Q)$ を用いて前記ペアリング $e(P, Q)$ を

[数9]

$$e(P, Q) = f'_{r,p}(Q)^{(p-1)/r}$$

として演算する第4演算手段、

として機能させるペアリング演算プログラム。

[請求項22]

前記楕円曲線は、 $E: y^2 = x^3 + ax$, $a \in F_p$, $4 \nmid (p-1)$ であり、

前記合成数位数 r は、 $r \nmid \#E(F_p)$, $4 \mid (r-1)$ を満たし、

前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 + 1 \equiv 0 \pmod{r}$ であり、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$$(x, y) \rightarrow (-x, \zeta y), \zeta^4 = 1, \zeta (\neq 1) \in F_p \text{ であり、}$$

前記 $f'_{r,p}(Q)$ は、

[数10]

$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2+1,p}(Q) \\ &= f_{\lambda_1^2,p}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_1,p}(Q)^{\lambda_1} \cdot f_{\lambda_1,\phi(P)}(Q) \cdot (x_Q - x_P) \end{aligned}$$

である請求項 21 に記載のペアリング演算プログラム。

[請求項23]

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $3 \mid (p-1)$ であり、

前記合成数位数 r は、 $r \nmid \#E(F_p)$, $3 \mid (r-1)$ を満たし、

前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 + \lambda_1 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 + \lambda_2 + 1 \equiv 0 \pmod{r}$ であり、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$$(x, y) \rightarrow (\varepsilon x, y), \varepsilon^3 = 1, \varepsilon (\neq 1) \in F_p \text{ であり、}$$

前記 $f'_{r,p}(Q)$ は、

[数11]

$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2 + \lambda_1 + 1, p}(Q) \\ &= f_{\lambda_1, p}(Q)^{\lambda_1 + 1} \cdot f_{\lambda_1 + 1, \psi(p)}(Q) \cdot (x_Q - x_P) \\ &= f_{\lambda_1, p}(Q) \cdot f_{\lambda_1, p}(Q)^{\lambda_1} \cdot f_{\lambda_1, \psi(p)}(Q) \cdot l_{[\lambda_1]\psi(p), \psi(p)}(Q) \end{aligned}$$

である請求項21に記載のペアリング演算プログラム。

[請求項24]

前記楕円曲線は、 $E: y^2 = x^3 + b$, $b \in F_p$, $6 \nmid (p-1)$ であり、

前記合成数位数 r は、 $r \nmid \#E(F_p)$, $3 \mid (r-1)$ を満たし、

前記整数 λ_1 、 λ_2 は、 $\lambda_1^2 - \lambda_1 + 1 \equiv 0 \pmod{r}$ 、 $\lambda_2^2 - \lambda_2 + 1 \equiv 0 \pmod{r}$ であり、

前記自己準同型写像は、 $\phi: E(F_p)[r] \rightarrow E(F_p)[r]$ 、

$$(x, y) \rightarrow (\varepsilon x, -y), \varepsilon^3 = 1, \varepsilon (\neq 1) \in F_p \text{ であり、}$$

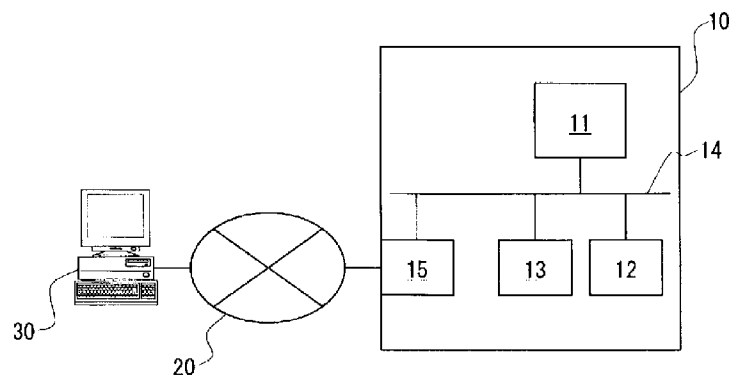
前記 $f'_{r,p}(Q)$ は、

[数12]

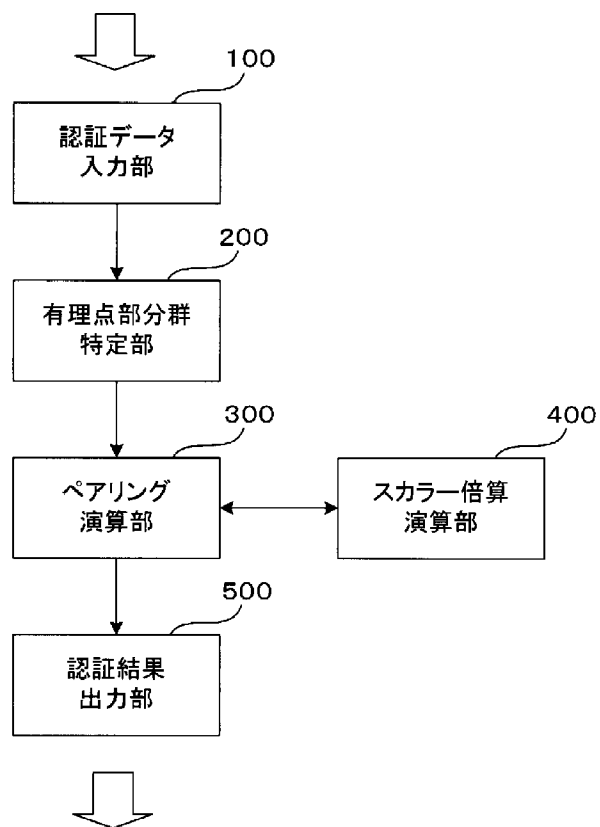
$$\begin{aligned} f'_{r,p}(Q) &= f_{\lambda_1^2 - \lambda_1 + 1, p}(Q) \\ &= f_{\lambda_1, p}(Q)^{\lambda_1 - 1} \cdot f_{\lambda_1 - 1, \psi(p)}(Q) \cdot (x_Q - x_P) \\ &= \left\{ f_{\lambda_1 - 1, p}(Q) \cdot \frac{l_{[\lambda_1 - 1]p, p}(Q)}{v_{[\lambda_1 - 1]p + p}(Q)} \right\}^{\lambda_1 - 1} \\ &\quad \cdot f_{\lambda_1 - 1, \psi(p)}(Q) \cdot (x_Q - x_P) \end{aligned}$$

である請求項21に記載のペアリング演算プログラム。

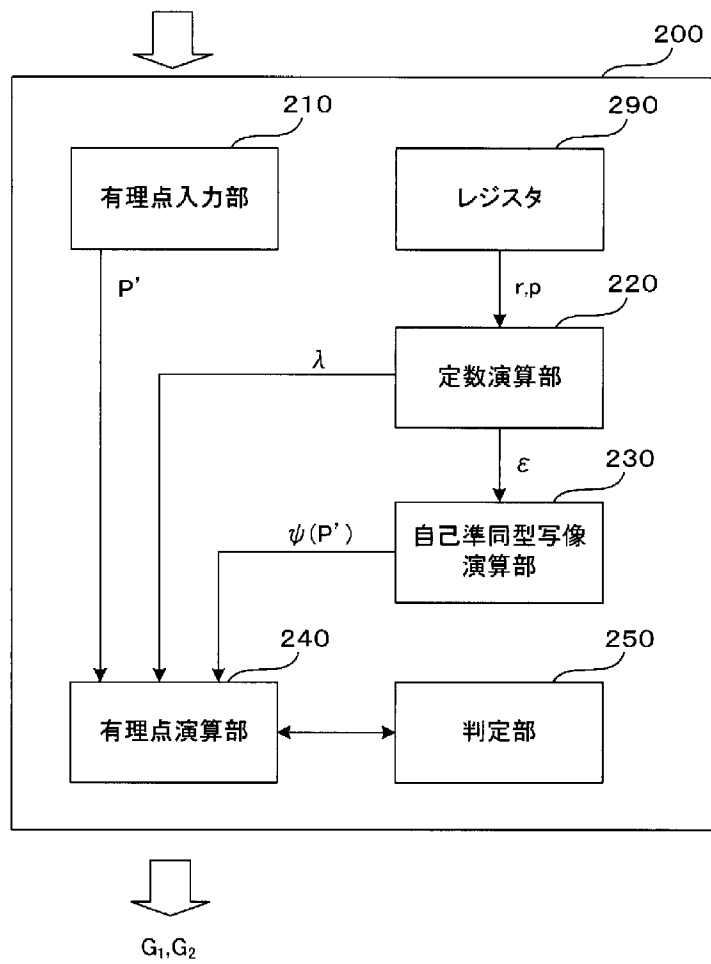
[図1]



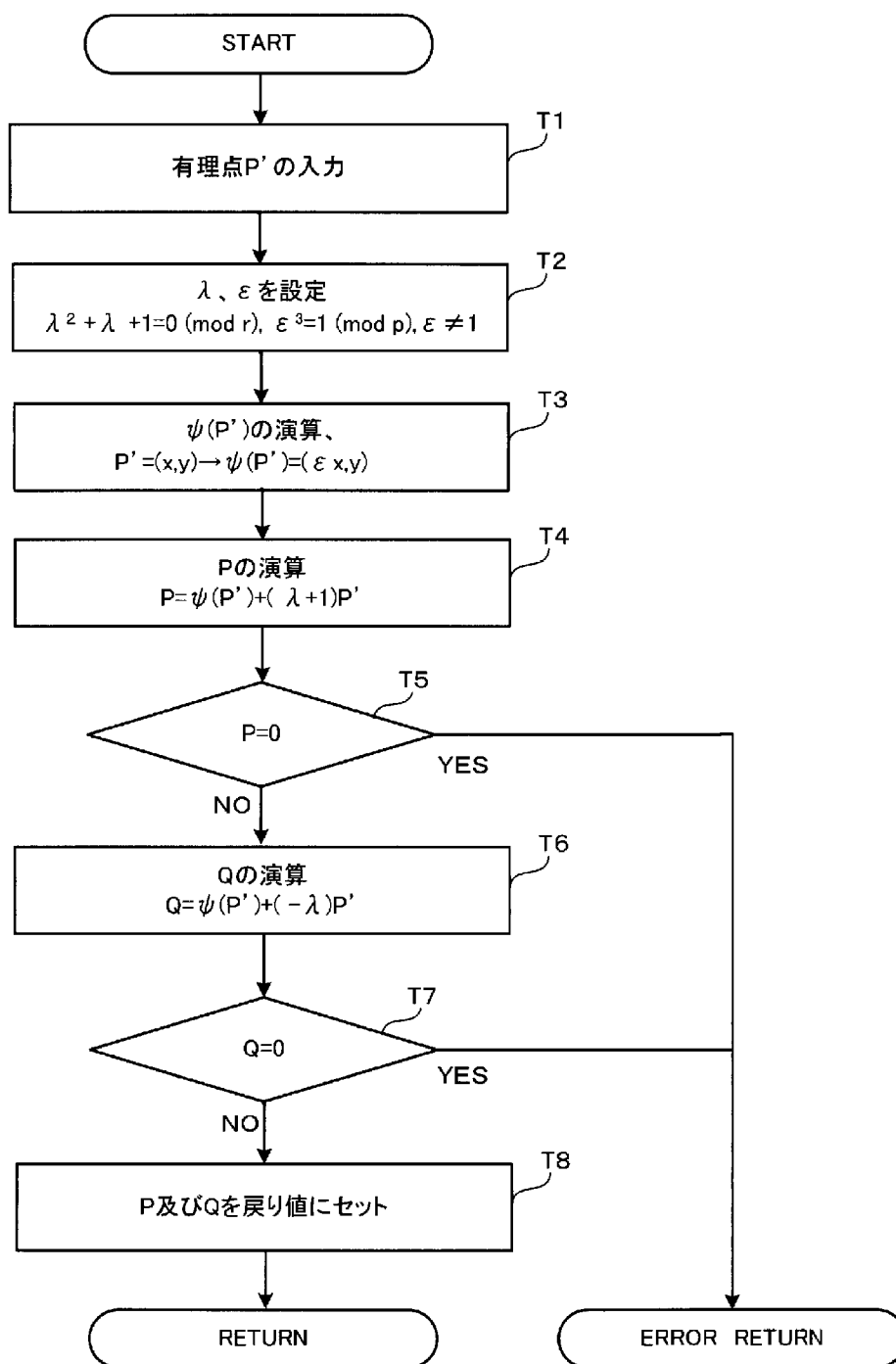
[図2]



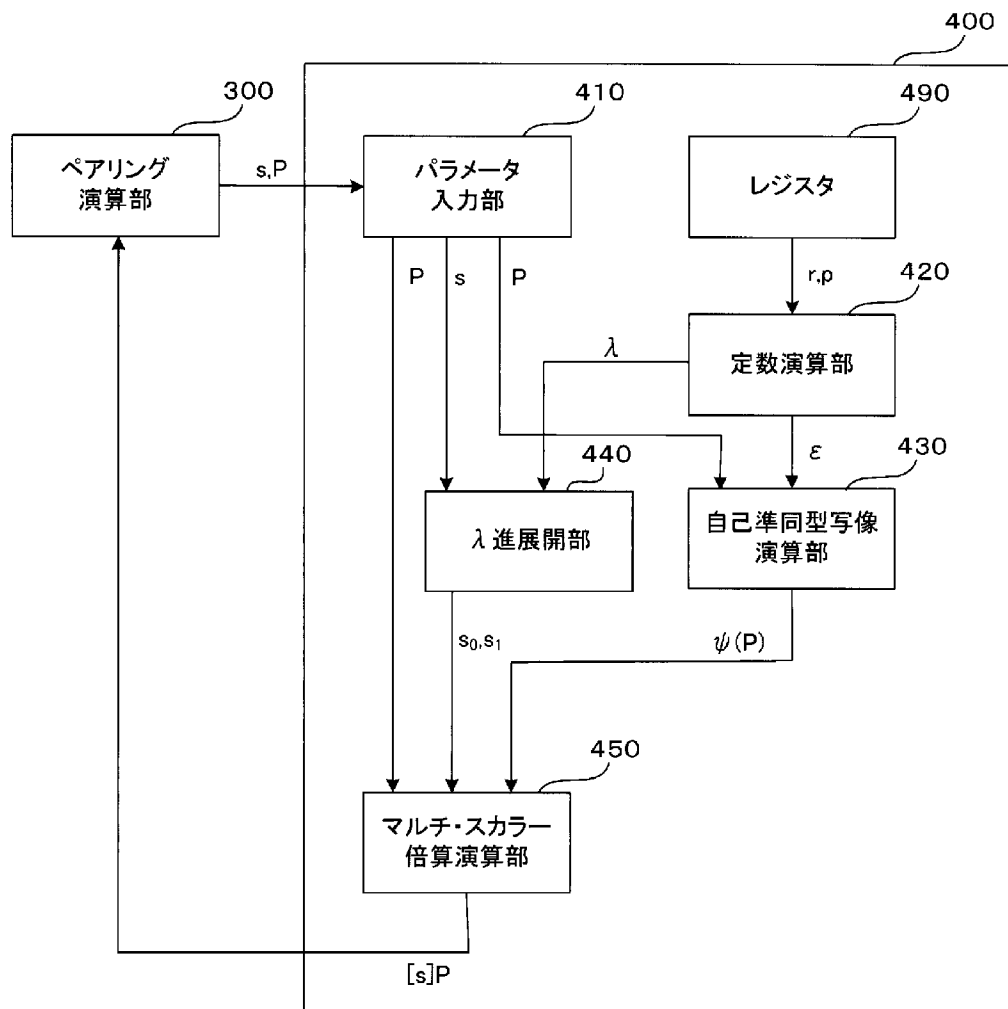
[図3]



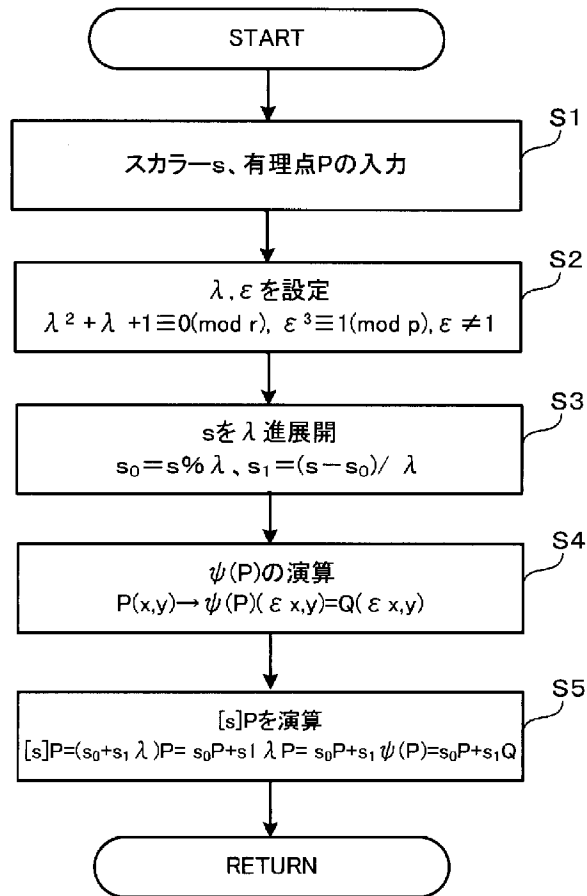
[図4]



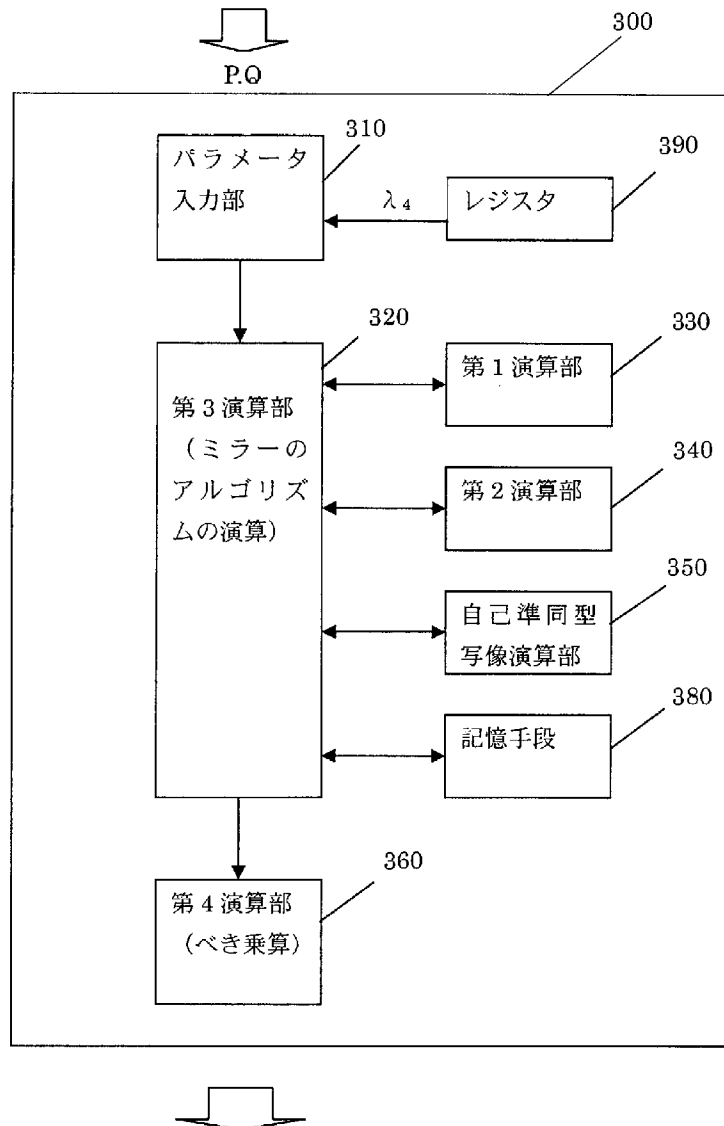
[図5]



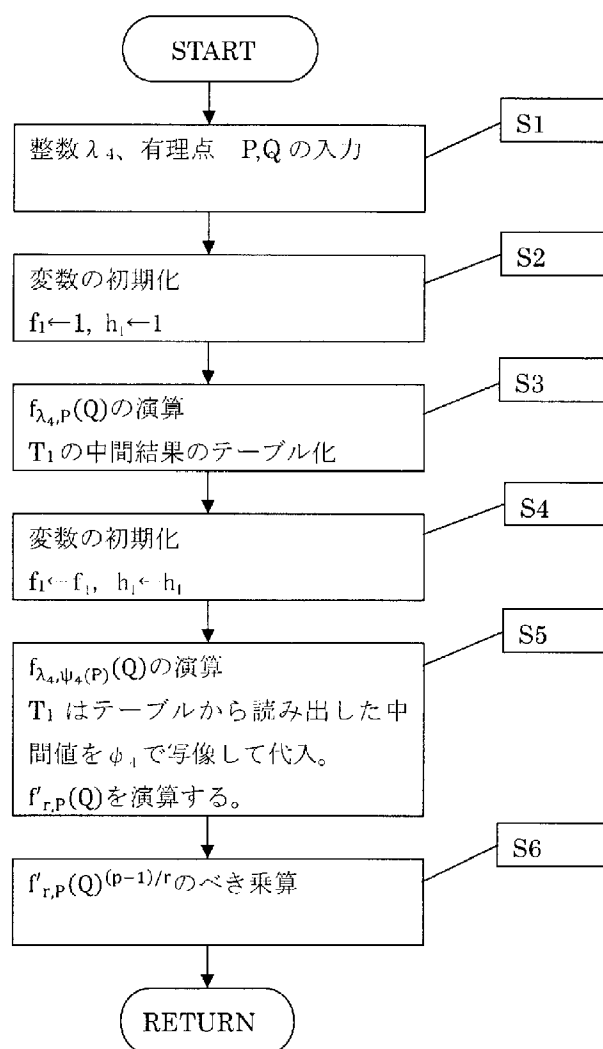
[図6]



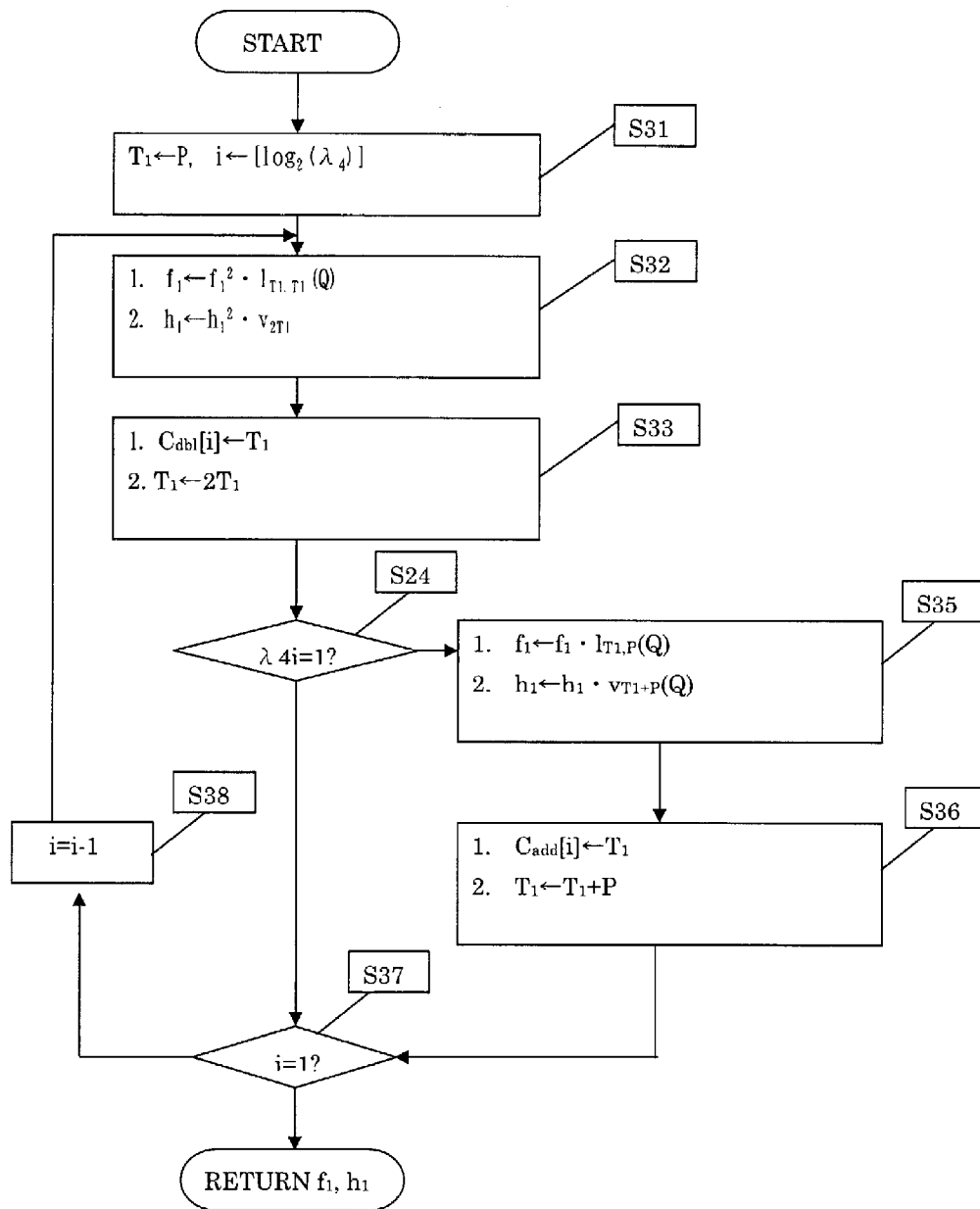
[図7]



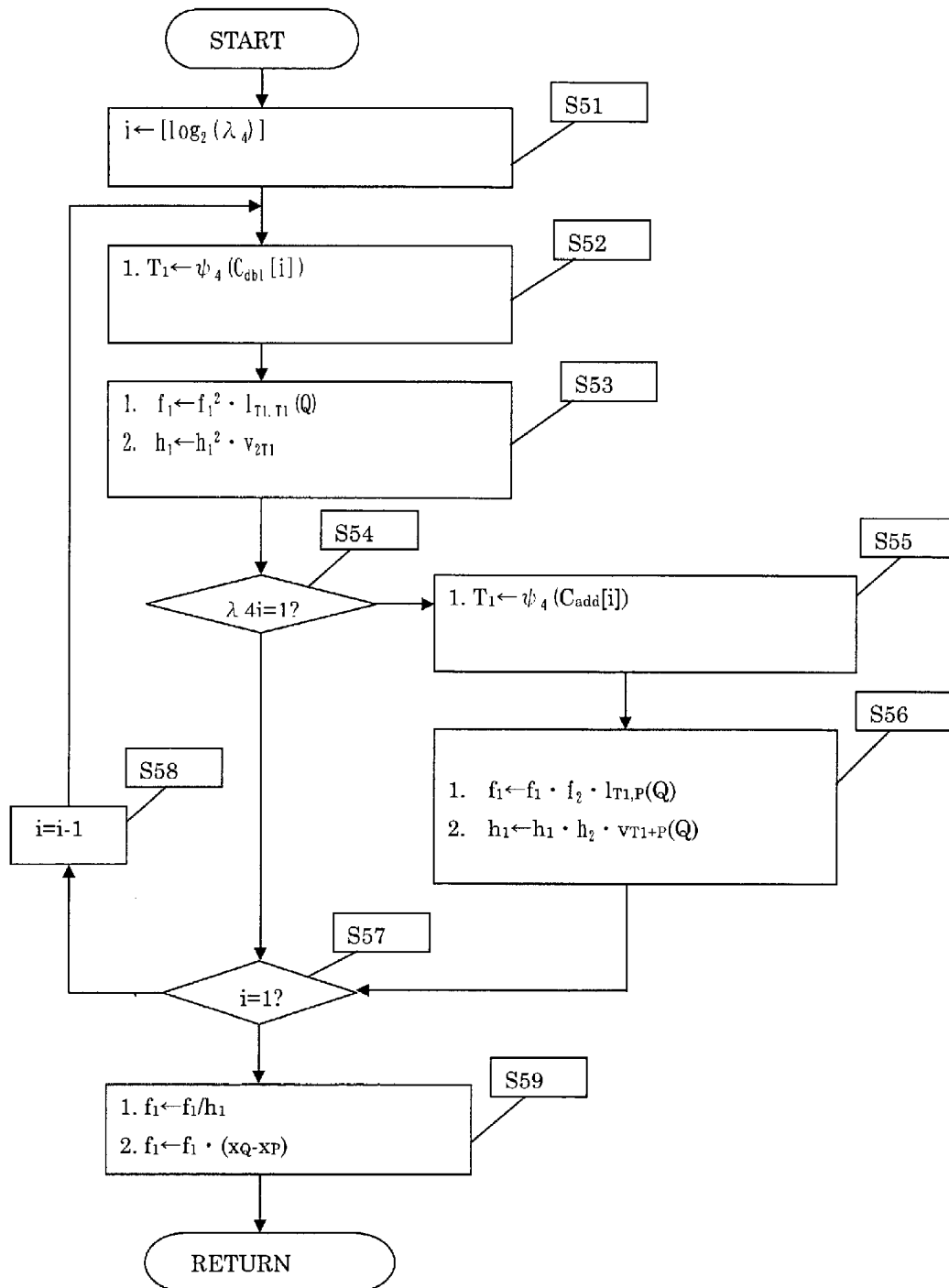
[図8]



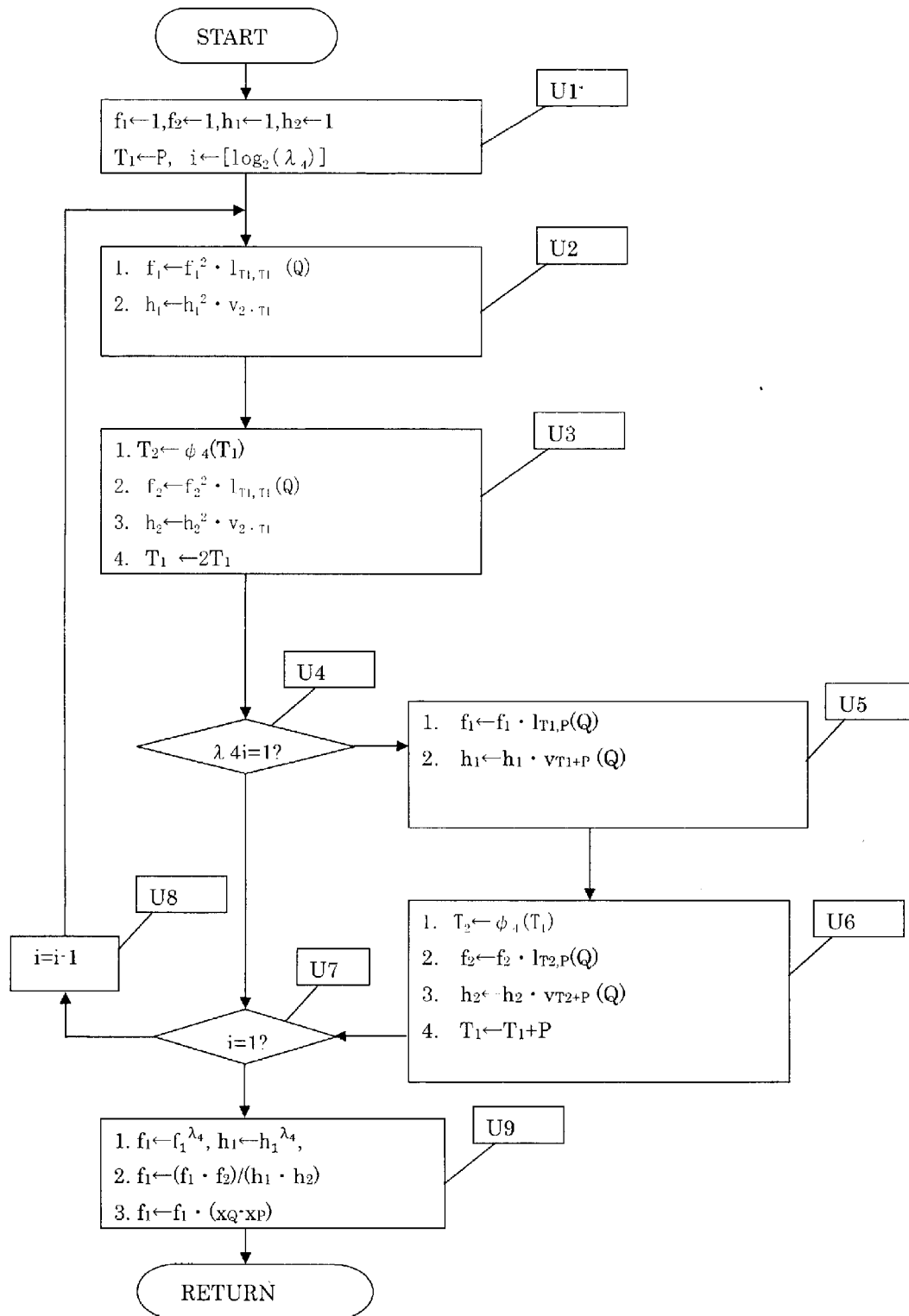
[図9]



[図10]



[図11]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2011/067520

A. CLASSIFICATION OF SUBJECT MATTER

G06F17/10 (2006.01) i, H04L9/30 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F17/10, H04L9/30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2011
Kokai Jitsuyo Shinan Koho	1971-2011	Toroku Jitsuyo Shinan Koho	1994-2011

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JSTPlus/JMEDPlus/JST7580 (JDreamII), pairng, elliptic curve

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Shoichi TAKEUCHI et al., "GLV Method for Non-Supersingular Paring-Friendly Curves of Embedding Degree 1", IEICE Technical Report, 09 December 2009 (09.12.2009), vol.109, no.337, pages 37 to 41, particularly, 2. Sugakuteki Junbi, 3. GLV-ho no Tekiyo	1-12
X	Ionica, S. et al., Pairing computation on curves with efficiently computable endomorphism and small embedding degree, Cryptology ePrint Archive, Report 2010/379, 2010.07.07, 3 Speeding up pairing computation using endomorphisms of small degree	13-24

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
12 September, 2011 (12.09.11)

Date of mailing of the international search report
20 September, 2011 (20.09.11)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2011/067520

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Claims of the present application are classified into the following two groups.

1. claims 1-12

The invention wherein scalar multiplication of a rational point on an elliptic curve line is calculated.

2. claims 13-24

The invention wherein pairing of a rational point on an elliptic curve line is calculated.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl. G06F17/10(2006.01)i, H04L9/30(2006.01)i

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (I P C))

Int.Cl. G06F17/10, H04L9/30

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 1 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 1 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 1 年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JSTPlus/JMEDPlus/JST7580(JDreamII) pairng, elliptic curve

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
X	竹内翔一他, 埋め込み次数 1 の非超特異ペアリングフレンドリ曲線上での G L V 法の適用, 電子情報通信学会技術研究報告, 2009.12.09, 第 109 巻 第 337 号, p.37-41, 特に 2. 数学的準備, 3. G L V 法の適用	1-12
X	Ionica, S. et al., Pairing computation on curves with efficiently computable endomorphism and small embedding degree, Cryptology ePrint Archive, Report 2010/379, 2010.07.07, 3 Speeding up pairing computation using endomorphisms of small degree	13-24

C 欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の 1 以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

1 2 . 0 9 . 2 0 1 1

国際調査報告の発送日

2 0 . 0 9 . 2 0 1 1

国際調査機関の名称及びあて先

日本国特許庁 (I S A / J P)

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区霞が関三丁目 4 番 3 号

特許庁審査官 (権限のある職員)

中里 裕正

5 S

9 3 6 4

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6

第Ⅱ欄 請求の範囲の一部の調査ができないときの意見（第1ページの2の続き）

法第8条第3項（PCT17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求項 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、
2. ☐ 請求項 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求項 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第Ⅲ欄 発明の単一性が欠如しているときの意見（第1ページの3の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。
本願の特許請求の範囲は、以下の2群に区分される。

1. 請求項 1-12
楕円曲線上の有理点のスカラー倍を計算するもの
2. 請求項 13-24
楕円曲線上の有理点のペアリングを計算するもの

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求項について作成した。
2. ☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求項について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求項のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求項について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。
- ☐ 追加調査手数料の納付はあったが、異議申立てはなかった。