(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
2009 年5 月7 日 (07.05.2009)

PCT

(10) 国際公開番号
WO 2009/057656 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2008/069683

(22) 国際出願日: 2008 年10 月29 日 (29.10.2008)

(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 2007-282487
2007 年10 月30 日 (30.10.2007) 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): 赤根正剛 (AKANE, Masataka) [JP/JP]; 〒7008530 岡山県岡山市津島中三丁目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). 野上保之 (NOGAMI, Yasuyuki) [JP/JP]; 〒7008530 岡山県岡山市津島中三丁目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).

(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).

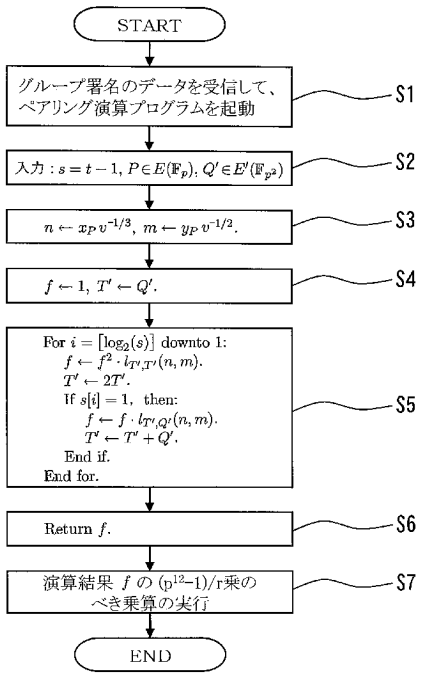
[続葉有]

WO 2009/057656 A1

(54) Title: PAIRING COMPUTATION DEVICE, PAIRING COMPUTATION METHOD, AND RECORDING MEDIUM WHERE PAIRING COMPUTATION PROGRAM IS RECORDED

(54) 発明の名称: 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を記録した記録媒体

[図3]



S1 RECEIVE DATA ON GROUP SIGNATURE AND BOOT UP PAIRING COMPUTATION PROGRAM

S2 INPUT : $s=t-1$, $P\in E(\mathbb{F}_p)$, $Q'\in E'(\mathbb{F}_{p^2})$

S7 CARRY OUT EXPONENTIATION OF COMPUTATION RESULT f TO $(p^{12}-1)/r$

$$e(Q,P)=f_{s,Q}(P)^{(q^k-1)/r} \qquad (1)$$

(57) Abstract: A paring computation device, a pairing computation method, and a recording medium where a pairing computation program is recorded all enabling a pairing computation at high speed. An Ate pairing e(Q, P) is defined as formula (I). If k is an integral multiple of 3, 4, or 6, the computation of a rational function necessary to derive a Miller function $f_{s,Q}(P)$ is conducted in a true subfield specified by a twist curve using a quadratic or third-power non-residue v which takes on one when exponentiation of $f_{s,Q}(P)$ to $(q^k-1)/r$-th power is carried out.

(57) 要約: 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を記録した記録媒体を提供する。 Ａｔｅペアリング$e(Q,P)$を 式（Ｉ） とし、ｋが偶数、３の倍数、４の倍数、６の倍数のいずれかである場合に、ミラー関数$f_{s,Q}(P)$の導出に必要となる有理関数の演算を、この$f_{s,Q}(P)$の（q^k-1）／ｒ乗のべき乗算の演算によって１となる平方非剰余あるいは３乗非剰余なｖを用いたツイスト曲線により特定される真部分体上の演算として行う。

(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, 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, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, 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 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

明 細 書

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を記録した記録媒体

技術分野

[0001] 本発明は、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を記録した記録媒体に関する。

背景技術

[0002] 昨今、高速な電気通信回線が低価格で利用可能となったことにより、インターネットなどのネットワーク上において、音楽や映像の配信、インターネットバンキング、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可能となっている。

[0003] また、企業による業務形態も変化しており、ノートパソコンや携帯電話などのいわゆるモバイル端末装置を用いて外出先などから会社のサーバ装置にアクセスして、各種の情報の入力あるいは取得が可能となっている。

[0004] 特に、日本では、携帯電話をネットワークへの接続装置として利用するサービスが充実しており、いかなる所からでも所要のネットワークにアクセスして各種の情報を入手したり、サービスを利用したりすることができるいわゆるユビキタス社会の到来がいよいよ現実味を帯びてきた。

[0005] このように各種の情報を取得したり、サービスを利用したりするためにネットワークにアクセスする際には、所要の認証手段を備えた認証サーバによって認証処理が行われ、ネットワークにアクセスした利用者が、あらかじめ登録されている特定の利用者であることが認証されて、情報の取得あるいはサービスの利用が可能となっている。

[0006] 特に、最近では、ディジタル署名技術を用いることにより、取り扱っている情報が第三者によって改ざんされていないこと、あるいは第三者に漏洩していないことを保証可能として、秘匿性の高い情報もネットワーク上で安全に取り扱い可能となっていることにより、さらに積極的にネットワークが利用されることとなっている。

[0007] ただし、このディジタル署名では、利用者個人が特定されるため、認証サーバにおける認証処理に基づいて認証サーバに利用者の履歴が情報として蓄積されることと

なっており、この履歴情報は一種の個人情報であって、個人情報保護の問題があった。

[0008] そこで、ディジタル署名を拡張したディジタルグループ署名を用いることが提案されている。ディジタルグループ署名を用いた場合には、利用者は、認証サーバに対して匿名でグループに属していることのみを証明する署名データを送信し、認証サーバでは、受信した署名データから利用者を特定することなく利用者が所定のグループに属していることを認証している。したがって、認証サーバに各利用者の使用の履歴情報が蓄積されることを防止できる一方で、グループに属さない利用者による不正利用を阻止可能としている。

[0009] ここで、ディジタルグループ署名における匿名認証には、ペアリング演算が用いられている。ペアリング演算では、2入力1出力の関数を用いた演算を行っており、たとえば、Pを素体F_q上の有理点、Qをk次拡大体F_q^k上の有理点として、ペアリングでPとQとを入力して拡大体F_q^{*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乗が算出されることを利用しているものであり、このような性質のことを双線形性と呼ぶ。なお、ここで、「k」を埋込み次数と呼び、「F_q^{*k}」は、正しくは、以下の表示であるが、表示の制限上、「F_q^{*k}」と表示している。

[数13]

$$F^*_{q^k}$$

[0010] 一般的に、有理点P，Qはそれぞれ楕円曲線上の点が用いられ、このような楕円曲線のペアリングの演算は、ミラーのアルゴリズムを用いて演算するステップと、最終べきのべき乗演算を行うステップとで構成されている。

[0011] たとえば、10,000人のメンバーで構成されるグループのディジタルグループ署名であって、各メンバーのアクセス権の発行と失効とを柔軟に対応可能とするために、ディジタルグループ署名の検証時に失効者分のペアリング演算を行う方式が知られている。この場合、失効者が100人であれば100回のペアリング演算が必要であり、現時点での一般的な電子計算機による1回のペアリングの演算に約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10秒を要することとなって、大規模なディジタルグループ署名での利用は実用的とは言えなかった。

[0012] そこで、ペアリングの演算速度を向上させるために様々な開発が行われており、たとえば有限体上の楕円曲線上で定義されるTateペアリング演算における高速化の技術が提案されている(例えば、特許文献1参照。)。

特許文献1:特開2005－316267号公報

発明の開示

発明が解決しようとする課題

[0013] しかしながら、現在提案されているペアリング演算の高速化技術では、未だに大規模なディジタルグループ署名での利用に適う速度とはなっておらず、ディジタルグループ署名のメンバー数を制限しなければならないという問題があった。

[0014] 本発明者らは、このような現状に鑑み、ペアリング演算を高速化す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

[0015] 本発明のペアリング演算装置では、曲線の式が$y^2=x^3+ax+b$, $a\in F_q$, $b\in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が2h次(h:自然数)で、F_q^{2h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r]\cap \mathrm{Ker}(\phi_q-[1])$

$G_2=E[r]\cap \mathrm{Ker}(\phi_q-[q])$

により、

$e:G_2\times G_1\rightarrow F_q^{*2h}/(F_q^{*2h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P\in G_1$、$Q\in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs=t－1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数14]

$$e(Q,P)=f_{s,Q}(P)^{(q^{2h}-1)/r}$$

としてAteペアリングe(Q,P)を演算するペアリング演算装置において、$f_{s,Q}(P)$の導出に必要となる有理関数の演算を、この$f_{s,Q}(P)$の$(q^{2h}-1)$／r乗のべき乗算の演算によっ

て1となる平方非剰余な$v \in F_q^h$を用いて、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2 = x^3 + av^{-2}x + bv^{-3}$による真部分体上で行うこととした。

[0016] 特に、

・$s = t - 1$、$P \in E(F_q)$であるP、$Q' \in E'(F_q^h)$であるQ'の入力を受け付ける入力手段、

・有理点Pの座標(x_P, y_P)に対して、$n \leftarrow x_P v^{-1}$、$m \leftarrow y_P v^{-3/2}$の代入演算を行うとともに、$f \leftarrow 1$、$T' \leftarrow Q'$の代入演算を行う代入手段、

・有理点Tを通る接線$l_{T,T}(x, y) = 0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-3/2}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行う第1演算手段、

・$T' \leftarrow 2T'$の代入演算を行う第2演算手段、

・sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y) = 0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-3/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行う第3演算手段、

・sを2進数表示とした場合の所定のビットの値が1である場合に、$T' \leftarrow T' + Q'$の代入演算を行う第4演算手段、

・$(q^{2h} - 1)/r$乗のべき乗算を演算する第5演算手段

を備えたことに特徴を有するものである。

[0017] また、本発明のペアリング演算装置では、曲線の式が$y^2 = x^3 + a$, $a \in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が$3h$次(h:自然数)で、F_q^{3h}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なす加法群をE、素数位数rの有理点の集合を$E[r]$とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1 = E[r] \cap \mathrm{Ker}(\phi_q - [1])$

$G_2 = E[r] \cap \mathrm{Ker}(\phi_q - [q])$

により、

$e: G_2 \times G_1 \rightarrow F_q^{*3h}/(F_q^{*3h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P \in G_1$、$Q \in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いて$s = t - 1$とし、ミラー関

数$f_{s,Q}(\cdot)$を用いて、

[数15]

$$e(Q,P) = f_{s,Q}(P)^{(q^{3h}-1)/r}$$

としてAteペアリングe(Q,P)を演算するペアリング演算装置において、

$f_{s,Q}(P)$の導出に必要となる有理関数の演算を、この$f_{s,Q}(P)$の$(q^{3h}-1)$／r乗のべき乗算の演算によって1となる平方剰余かつ3乗非剰余な$v \in F_q^h$を用いて、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2 = x^3 + av^{-1}$による真部分体上で行うこととした。

[0018] 特に、

・$s = t-1$、$P \in E(F_q)$であるP、$Q' \in E'(F_q^h)$であるQ'の入力を受け付ける入力手段、

・有理点Pの座標(x_P, y_P)に対して、$n \leftarrow x_P v^{-1/3}$、$m \leftarrow y_P v^{-1/2}$の代入演算を行うとともに、$f \leftarrow 1$、$T' \leftarrow Q'$の代入演算を行う代入手段、

・有理点Tを通る接線$l_{T,T}(x, y) = 0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-1/2}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行う第1演算手段、

・$T' \leftarrow 2T'$の代入演算を行う第2演算手段、

・sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y) = 0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-1/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行う第3演算手段、

・sを2進数表示とした場合の所定のビットの値が1である場合に、$T' \leftarrow T' + Q'$の代入演算を行う第4演算手段、

・$(q^{3h}-1)/r$乗のべき乗算を演算する第5演算手段

を備えたことに特徴を有するものである。

[0019] また、本発明のペアリング演算装置では、曲線の式が$y^2 = x^3 + ax$, $a \in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が4h次(h:自然数)で、4が$q^h - 1$を割り切るものとし、F_q^{4h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1 = E[r] \cap \mathrm{Ker}(\phi_q - [1])$

$G_2 = E[r] \cap \mathrm{Ker}(\phi_q - [q])$

により、

$e: G_2 \times G_1 \rightarrow F_q^{*4h}/(F_q^{*4h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P \in G_1$、$Q \in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs＝t－1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数16]

$$e(Q,P) = f_{s,Q}(P)^{(q^{4h}-1)/r}$$

としてAteペアリングe(Q,P)を演算するペアリング演算装置において、$f_{s,Q}(P)$の導出に必要となる有理関数の演算を、この$f_{s,Q}(P)$の$(q^{4h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余な$v \in F_q^h$を用いて、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2 = x^3 + av^{-1}x$による真部分体上で行うこととした。

[0020] 特に、

・s＝t－1、$P \in E(F_q)$であるP、$Q' \in E'(F_q^h)$であるQ'の入力を受け付ける入力手段、

・有理点Pの座標(x_P, y_P)に対して、$n \leftarrow x_P v^{-1/2}$、$m \leftarrow y_P v^{-3/4}$の代入演算を行うとともに、f←1、T'←Q'の代入演算を行う代入手段、

・有理点Tを通る接線$l_{T,T}(x, y)$＝0の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-3/4}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行う第1演算手段、

・T'←2T'の代入演算を行う第2演算手段、

・sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)$＝0の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-3/4}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行う第3演算手段、

・sを2進数表示とした場合の所定のビットの値が1である場合に、T'←T'＋Q'の代入演算を行う第4演算手段、

・$(q^{4h}-1)$/r乗のべき乗算を演算する第5演算手段と

を備えたことに特徴を有するものである。

[0021] また、本発明のペアリング演算装置では、曲線の式が$y^2=x^3+a$, $a\in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が6h次(h:自然数)で、F_q^{6h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r]\cap \mathrm{Ker}(\phi_q-[1])$

$G_2=E[r]\cap \mathrm{Ker}(\phi_q-[q])$

により、

$e:G_2\times G_1\rightarrow F_q^{*6h}/(F_q^{*6h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P\in G_1$、$Q\in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs=t−1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数17]

$$e(Q,P)=f_{s,Q}(P)^{(q^{6h}-1)/r}$$

としてAteペアリングe(Q,P)を演算するペアリング演算装置において、$f_{s,Q}(P)$の導出に必要となる有理関数の演算を、この$f_{s,Q}(P)$の$(q^{6h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余かつ3乗非剰余な$v\in F_q^h$を用いて、$E(F_q^h)$のツイスト曲線$E'(F_q^h):y^2=x^3+av^{-1}$による真部分体上で行うこととした。

[0022] 特に、

・s=t−1、$P\in E(F_q)$であるP、$Q'\in E'(F_q^h)$であるQ'の入力を受け付ける入力手段、

・有理点Pの座標(x_P, y_P)に対して、$n\leftarrow x_P v^{-1/3}$、$m\leftarrow y_P v^{-1/2}$の代入演算を行うとともに、f←1、T'←Q'の代入演算を行う代入手段、

・有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-1/2}$を$l_{T',T'}(n, m)$で演算して、$f\leftarrow f^2\cdot l_{T',T'}(n, m)$の代入演算を行う第1演算手段、

・T'←2T'の代入演算を行う第2演算手段、

・sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る

直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-1/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行う第3演算手段、

・sを2進数表示とした場合の所定のビットの値が1である場合に、$T' \leftarrow T' + Q'$の代入演算を行う第4演算手段、

・$(q^{6h}-1)/r$乗のべき乗算を演算する第5演算手段と

を備えたことに特徴を有するものである。

[0023] また、本発明のペアリング演算方法では、曲線の式が$y^2=x^3+ax+b$, $a \in F_q$, $b \in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が2h次(h:自然数)で、F_q^{2h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r] \cap \mathrm{Ker}(\phi_q-[1])$

$G_2=E[r] \cap \mathrm{Ker}(\phi_q-[q])$

により、

$e: G_2 \times G_1 \rightarrow F_q^{*2h}/(F_q^{*2h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P \in G_1$、$Q \in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs=t−1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数18]

$$e(Q,P)=f_{s,Q}(P)^{(q^{2h}-1)/r}$$

としてAteペアリングe(Q,P)を電子計算機で演算するペアリング演算方法において、$f_{s,Q}(P)$の$(q^{2h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余な$v \in F_q^h$、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2=x^3+av^{-2}x+bv^{-3}$を用い、

・電子計算機を入力手段として機能させて、s=t−1、$P \in E(F_p)$であるP、$Q' \in E'(F_p^2)$であるQ'の入力を受け付けるステップ、

・電子計算機を代入手段として機能させて、有理点Pの座標(x_P, y_P)に対して、$n \leftarrow x_P v^{-1}$、$m \leftarrow y_P v^{-3/2}$の代入演算を行うステップ、

・電子計算機を代入手段として機能させて、$f \leftarrow 1$、$T' \leftarrow Q'$の代入演算を行うステップ

、

・電子計算機を第1演算手段として機能させて、有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-3/2}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行うステップ、

・電子計算機を第2演算手段として機能させて、T'←2T'の代入演算を行うステップ、

・電子計算機を第3演算手段として機能させて、sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-3/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行うステップ、

・電子計算機を第4演算手段として機能させて、sを2進数表示とした場合の所定のビットの値が1である場合に、T'←T'＋Q'の代入演算を行うステップ

・電子計算機を第5演算手段として機能させて、$(q^{2h}-1)/r$乗のべき乗算の演算を行うステップと

を有することとした。

[0024] また、本発明のペアリング演算方法では、曲線の式が$y^2=x^3+a$, $a \in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が3h次(h:自然数)で、F_q^{3h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r] \cap \mathrm{Ker}(\phi_q-[1])$

$G_2=E[r] \cap \mathrm{Ker}(\phi_q-[q])$

により、

$e: G_2 \times G_1 \rightarrow F_q^{*3h}/(F_q^{*3h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P \in G_1$、$Q \in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs=t−1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数19]

$$e(Q,P)=f_{s,Q}(P)^{(q^{3h}-1)/r}$$

としてAteペアリングe(Q,P)を電子計算機で演算するペアリング演算方法において、f

$l_{s,Q}(P)$の$(q^{3h}-1)$／r乗のべき乗算の演算によって1となる平方剰余かつ3乗非剰余な$v \in F_q^h$、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2 = x^3 + av^{-1}$を用い、

・電子計算機を入力手段として機能させて、$s = t-1$、$P \in E(F_q)$であるP、$Q' \in E'(F_q^h)$であるQ'の入力を受け付けるステップ、

・電子計算機を代入手段として機能させて、有理点Pの座標(x_P, y_P)に対して、$n \leftarrow x_P v^{-1/3}$、$m \leftarrow y_P v^{-1/2}$の代入演算を行うステップ、

・電子計算機を代入手段として機能させて、$f \leftarrow 1$、$T' \leftarrow Q'$の代入演算を行うステップ、

・電子計算機を第1演算手段として機能させて、有理点Tを通る接線$l_{T,T}(x, y) = 0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-1/2}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行うステップ、

・電子計算機を第2演算手段として機能させて、$T' \leftarrow 2T'$の代入演算を行うステップ、

・電子計算機を第3演算手段として機能させて、sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y) = 0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-1/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行うステップ、

・電子計算機を第4演算手段として機能させて、sを2進数表示とした場合の所定のビットの値が1である場合に、$T' \leftarrow T' + Q'$の代入演算を行うステップ、

・電子計算機を第5演算手段として機能させて、$(q^{3h}-1)/r$乗のべき乗算の演算を行うステップと

を有することとした。

[0025] また、本発明のペアリング演算方法では、曲線の式が$y^2 = x^3 + ax$, $a \in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が4h次(h:自然数)で、4がq^h-1を割り切るものとし、F_q^{4h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1 = E[r] \cap \mathrm{Ker}(\phi_q - [1])$

$G_2 = E[r] \cap \mathrm{Ker}(\phi_q - [q])$

により、

$e: G_2 \times G_1 \rightarrow F^{*4h}_q/(F^{*4h}_q)^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P \in G_1$、$Q \in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs＝t－1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数20]

$$e(Q,P) = f_{s,Q}(P)^{(q^{4h}-1)/r}$$

としてAteペアリングe(Q,P)を電子計算機で演算するペアリング演算方法において、$f_{s,Q}(P)$の$(q^{4h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余な$v \in F^h_q$、$E(F^h_q)$のツイスト曲線$E'(F^h_q): y^2 = x^3 + av^{-1}x$を用い、

・電子計算機を入力手段として機能させて、s＝t－1、$P \in E(F_q)$であるP、$Q' \in E'(F^h_q)$であるQ'の入力を受け付けるステップ、

・電子計算機を代入手段として機能させて、有理点Pの座標(x_P, y_P)に対して、$n \leftarrow x_P v^{-1/2}$、$m \leftarrow y_P v^{-3/4}$の代入演算を行うステップ、

・電子計算機を代入手段として機能させて、f←1、T'←Q'の代入演算を行うステップ、

・電子計算機を第1演算手段として機能させて、有理点Tを通る接線$l_{T,T}(x, y)$＝0の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v_P^{-3/4}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行うステップ、

・電子計算機を第2演算手段として機能させて、T'←2T'の代入演算を行うステップ、

・電子計算機を第3演算手段として機能させて、sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)$＝0の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-3/4}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行うステップ、

・電子計算機を第4演算手段として機能させて、sを2進数表示とした場合の所定のビットの値が1である場合に、T'←T'＋Q'の代入演算を行うステップ、

・電子計算機を第5演算手段として機能させて、$(q^{4h}-1)/r$乗のべき乗算の演算を行うステップと

を有することとした。

[0026] また、本発明のペアリング演算方法では、曲線の式が$y^2=x^3+a$, $a\in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が6h次(h:自然数)で、F_q^{6h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r]\cap \mathrm{Ker}(\phi_q-[1])$

$G_2=E[r]\cap \mathrm{Ker}(\phi_q-[q])$

により、

$e:G_2\times G_1\rightarrow F_q^{*6h}/(F_q^{*6h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P\in G_1$、$Q\in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs=t−1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数21]

$$e(Q,P)=f_{s,Q}(P)^{(q^{6h}-1)/r}$$

としてAteペアリングe(Q,P)を電子計算機で演算するペアリング演算方法において、$f_{s,Q}(P)$の$(q^{6h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余かつ3乗非剰余なv$\in F_q^h$、$E(F_q^h)$のツイスト曲線$E'(F_q^h):y^2=x^3+av^{-1}$を用い、

・電子計算機を入力手段として機能させて、s=t−1、$P\in E(F_q)$であるP、$Q'\in E'(F_q^h)$であるQ'の入力を受け付けるステップ、

・電子計算機を代入手段として機能させて、有理点Pの座標(x_P, y_P)に対して、$n\leftarrow x_P v^{-1/3}$、$m\leftarrow y_P v^{-1/2}$の代入演算を行うステップ、

・電子計算機を代入手段として機能させて、f←1、T'←Q'の代入演算を行うステップ、

・電子計算機を第1演算手段として機能させて、有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-1/2}$を$l_{T',T'}(n, m)$で演算して、$f\leftarrow f^2\cdot l_{T',T'}(n, m)$の代入演算を行うステップ、

・電子計算機を第2演算手段として機能させて、T'←2T'の代入演算を行うステップ、

・電子計算機を第3演算手段として機能させて、sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-1/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行うステップ、

・電子計算機を第4演算手段として機能させて、sを2進数表示とした場合の所定のビットの値が1である場合に、T'←T'＋Q'の代入演算を行うステップ、

・電子計算機を第5演算手段として機能させて、$(q^{6h}-1)/r$乗のべき乗算の演算を行うステップと

を有することとした。

[0027] また、本発明のペアリング演算プログラムを記録した記録媒体では、曲線の式が$y^2=x^3+ax+b$, $a \in F_q$, $b \in F_q$ (q：3より大きい素数のべき乗)で与えられ、埋込み次数が2h次(h：自然数)で、F_q^{2h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r] \cap \mathrm{Ker}(\phi_q-[1])$

$G_2=E[r] \cap \mathrm{Ker}(\phi_q-[q])$

により、

$e: G_2 \times G_1 \rightarrow F_q^{*2h}/(F_q^{*2h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P \in G_1$、$Q \in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs＝t－1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数22]

$$e(Q,P)=f_{s,Q}(P)^{(q^{2h}-1)/r}$$

としてAteペアリングe(Q,P)を電子計算機に演算させるペアリング演算プログラムにおいて、$f_{s,Q}(P)$の$(q^{2h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余な$v \in F_q^h$、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2=x^3+av^{-2}x+bv^{-3}$を用い、

・電子計算機を入力手段として機能させて、s＝t－1、$P \in E(F_q)$であるP、$Q' \in E'(F_q^h)$であるQ'の入力を受け付けさせるステップ、

・電子計算機を代入手段として機能させて、有理点Pの座標(x_P, y_P)に対して、$n \leftarrow x_P v^{-1}$、$m \leftarrow y_P v^{-3/2}$の代入演算を行わせるステップ、

・電子計算機を代入手段として機能させて、$f \leftarrow 1$、$T' \leftarrow Q'$の代入演算を行わせるステップ、

・電子計算機を第1演算手段として機能させて、有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-3/2}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行わせるステップ、

・電子計算機を第2演算手段として機能させて、$T' \leftarrow 2T'$の代入演算を行わせるステップ、

・電子計算機を第3演算手段として機能させて、sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-3/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行わせるステップ、

・電子計算機を第4演算手段として機能させて、sを2進数表示とした場合の所定のビットの値が1である場合に、$T' \leftarrow T' + Q'$の代入演算を行わせるステップ、

・電子計算機を第5演算手段として機能させて、$(q^{2h}-1)/r$乗のべき乗算の演算を行わせるステップと

を電子計算機に実行させるペアリング演算プログラムを記録した記録媒体とした。

[0028] また、本発明のペアリング演算プログラムを記録した記録媒体では、曲線の式が$y^2 = x^3 + a$, $a \in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が3h次(h:自然数)で、F_q^{3h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1 = E[r] \cap \mathrm{Ker}(\phi_q - [1])$

$G_2 = E[r] \cap \mathrm{Ker}(\phi_q - [q])$

により、

$e: G_2 \times G_1 \rightarrow F_q^{*3h}/(F_q^{*3h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P \in G_1$、$Q \in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs=t−1とし、ミラー関

数$f_{s,Q}(\cdot)$を用いて、

[数23]

$$e(Q,P) = f_{s,Q}(P)^{(q^{3h}-1)/r}$$

としてAteペアリングe(Q,P)を電子計算機に演算させるペアリング演算プログラムにおいて、$f_{s,Q}(P)$の$(q^{3h}-1)$／r乗のべき乗算の演算によって1となる平方剰余かつ3乗非剰余な$v \in F_q^h$、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2 = x^3 + av^{-1}$を用い、

・電子計算機を入力手段として機能させて、$s = t-1$、$P \in E(F_q)$であるP、$Q' \in E'(F_q^h)$であるQ'の入力を受け付けさせるステップ、

・電子計算機を代入手段として機能させて、有理点Pの座標(x_P, y_P)に対して、$n \leftarrow x_P v^{-1/3}$、$m \leftarrow y_P v^{-1/2}$の代入演算を行わせるステップ、

・電子計算機を代入手段として機能させて、$f \leftarrow 1$、$T' \leftarrow Q'$の代入演算を行わせるステップ、

・電子計算機を第1演算手段として機能させて、有理点Tを通る接線$l_{T,T}(x, y) = 0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-1/2}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行わせるステップ、

・電子計算機を第2演算手段として機能させて、$T' \leftarrow 2T'$の代入演算を行わせるステップ、

・電子計算機を第3演算手段として機能させて、sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y) = 0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-1/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行わせるステップ、

・電子計算機を第4演算手段として機能させて、sを2進数表示とした場合の所定のビットの値が1である場合に、$T' \leftarrow T' + Q'$の代入演算を行わせるステップ、

・電子計算機を第5演算手段として機能させて、$(q^{3h}-1)/r$乗のべき乗算の演算を行わせるステップと

を電子計算機に実行させるペアリング演算プログラムを記録した記録媒体とした。

[0029] また、本発明のペアリング演算プログラムを記録した記録媒体では、曲線の式が$y^2 = x^3 + ax$, $a \in F_q$ (q：3より大きい素数のべき乗)で与えられ、埋込み次数が4h次(h：

自然数)で、4がq^h-1を割り切るものとし、F_q^{4h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r]\cap Ker(\phi_q-[1])$

$G_2=E[r]\cap Ker(\phi_q-[q])$

により、

$e:G_2\times G_1\rightarrow F_q^{*4h}/(F_q^{*4h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P\in G_1$、$Q\in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs=t−1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数24]

$$e(Q,P)=f_{s,Q}(P)^{(q^{4h}-1)/r}$$

としてAteペアリングe(Q,P)を電子計算機に演算させるペアリング演算プログラムにおいて、$f_{s,Q}(P)$の$(q^{4h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余な$v\in F_q^h$、$E(F_q^h)$のツイスト曲線$E'(F_q^h):y^2=x^3+av^{-1}x$を用い、

・電子計算機を入力手段として機能させて、s=t−1、$P\in E(F_q)$であるP、$Q'\in E'(F_q^h)$であるQ'の入力を受け付けさせるステップ、

・電子計算機を代入手段として機能させて、有理点Pの座標(x_P, y_P)に対して、$n\leftarrow x_P v^{-1/2}$、$m\leftarrow y_P v^{-3/4}$の代入演算を行わせるステップ、

・電子計算機を代入手段として機能させて、f←1、T'←Q'の代入演算を行わせるステップ、

・電子計算機を第1演算手段として機能させて、有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-3/4}$を$l_{T',T'}(n, m)$で演算して、$f\leftarrow f^2\cdot l_{T',T'}(n, m)$の代入演算を行わせるステップ、

・電子計算機を第2演算手段として機能させて、T'←2T'の代入演算を行わせるステップ、

・電子計算機を第3演算手段として機能させて、sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの

座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-3/4}$を$l_{T',Q'}(n, m)$で演算して、f←f・$l_{T',Q'}(n, m)$の代入演算を行わせるステップ、

・電子計算機を第4演算手段として機能させて、sを2進数表示とした場合の所定のビットの値が1である場合に、T'←T'＋Q'の代入演算を行わせるステップ、

・電子計算機を第5演算手段として機能させて、$(q^{4h}-1)/r$乗のべき乗算の演算を行わせるステップと

を電子計算機に実行させるペアリング演算プログラムを記録した記録媒体とした。

[0030] また、本発明のペアリング演算プログラムを記録した記録媒体では、曲線の式が$y^2=x^3+a$, $a\in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が6h次(h:自然数)で、F_q^{6h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r]\cap Ker(\phi_q-[1])$

$G_2=E[r]\cap Ker(\phi_q-[q])$

により、

$e:G_2\times G_1\rightarrow F_q^{*6h}/(F_q^{*6h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P\in G_1$、$Q\in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs＝t－1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数25]

$$e(Q,P)=f_{s,Q}(P)^{(q^{6h}-1)/r}$$

としてAteペアリングe(Q,P)を電子計算機に演算させるペアリング演算プログラムにおいて、$f_{s,Q}(P)$の$(q^{6h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余かつ3乗非剰余な$v\in F_q^h$、$E(F_q^h)$のツイスト曲線$E'(F_q^h):y^2=x^3+av^{-1}$を用い、

・電子計算機を入力手段として機能させて、s＝t－1、$P\in E(F_q)$であるP、$Q'\in E'(F_q^h)$であるQ'の入力を受け付けさせるステップ、

・電子計算機を代入手段として機能させて、有理点Pの座標(x_P, y_P)に対して、n←$x_P v^{-1/3}$、m←$y_P v^{-1/2}$の代入演算を行わせるステップ、

・電子計算機を代入手段として機能させて、f←1、T'←Q'の代入演算を行わせるステップ、

・電子計算機を第1演算手段として機能させて、有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-1/2}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行わせるステップ、

・電子計算機を第2演算手段として機能させて、T'←2T'の代入演算を行わせるステップ、

・電子計算機を第3演算手段として機能させて、sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-1/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行わせるステップ、

・電子計算機を第4演算手段として機能させて、sを2進数表示とした場合の所定のビットの値が1である場合に、T'←T'＋Q'の代入演算を行わせるステップ、

・電子計算機を第5演算手段として機能させて、$(q^{6h}-1)/r$乗のべき乗算の演算を行わせるステップと

を電子計算機に実行させるペアリング演算プログラムを記録した記録媒体とした。

発明の効果

[0031] 本発明では、ペアリング演算に際して、$f_{s,Q}(P)$の導出に必要となる有理関数の演算を、ツイスト曲線を用いて低次の真部分体上で行うことにより演算負荷を低減して、ペアリング演算の高速化を図ることができる。

図面の簡単な説明

[0032] [図1]従来のミラーのアルゴリズムの説明図である。

[図2]本発明に係るミラーのアルゴリズムの説明図である。

[図3]本発明に係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4]本発明の実施形態に係るペアリング演算装置の概略説明図である。

符号の説明

[0033] 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

発明を実施するための最良の形態

[0034] 本発明の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では、ミラーのアルゴリズムを用いて演算するステップと、最終べきのべき乗演算を行うステップとで構成されるペアリング演算において、ミラーのアルゴリズムを用いた演算を高速化することにより、高速演算を可能としているものである。

[0035] ミラーのアルゴリズムは、図1に示すアルゴリズムとして知られているものである。曲線の式が$y^2=x^3+ax+b$, $a\in F_q$, $b\in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が2h次(h:自然数)で、F_q^{2h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、ミラーのアルゴリズムでは、フロベニウス自己準同型写像ϕ_qのトレースtを用いたs=t−1と、$P\in E(F_q)$であるPと、$Q\in E(F_q^{2h})$であるQとが入力されることにより、$f_{s,Q}(P)$を出力している。

[0036] なお、埋込み次数は偶数次に限定されるものではなく、埋込み次数を3の倍数次とする場合には、曲線の式が$y^2=x^3+a$, $a\in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が3h次(h:自然数)で、F_q^{3h}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なす加法群を用いることが望ましい。

[0037] また、特に、埋込み次数が4の倍数次の場合には、曲線の式が$y^2=x^3+ax$, $a\in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が4h次(h:自然数)で、4がq^h-1を割り切るものとし、F_q^{4h}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なす加法群を用いることが望ましい。

[0038] さらに、特に、埋込み次数が6の倍数次の場合には、曲線の式が$y^2=x^3+a$, $a\in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が6h次(h:自然数)で、F_q^{6h}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なす加法群を用いることが望ましい。

[0039] 図1に示すミラーのアルゴリズムの第1ステップでは、f←1、T←Qの代入演算を行い、第2ステップの繰り返し条件に基づいて以下の演算を繰り返し行っている。第2ステップでは、具体的には、2進数表示したsによって得られるビット数をiの初期値とし、演算の繰り返しのたびにiを1ずつ減算しながら繰り返し回数を管理している。第5ステップのs[i]は、2進数表示したsの最小ビットから数えてi番目のビットの値を示すものであって、s[i]は「0」と「1」のいずれか一方である。

[0040] 図1に示すミラーのアルゴリズムの第3ステップでは、有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$の演算を行っており、第4ステップでは、T←2Tとして楕円二倍算を行っている。

[0041] 図1に示すミラーのアルゴリズムの第5ステップでは、sを2進数表示とした場合の所定のビットの値s[i]が1であるか否かを判定し、1である場合に、第6ステップで有理点TとQを通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$の演算を行い、第7ステップで、T←T＋Qとして楕円加算を行っている。

[0042] そして、第2ステップの繰り返し条件に基づいて演算を繰り返し行って、図1に示すミラーのアルゴリズムの第10ステップでは、演算結果を出力している。ペアリング演算では、最後に、ミラーのアルゴリズムによって演算されて出力された演算結果の$f_{s,Q}(P)$に対して$(q^{2h}-1)/r$乗のべき乗算を行っている。

[0043] なお、埋込み次数が3の倍数次の場合には、最終べきのべき乗算は$(q^{3h}-1)/r$乗のべき乗算であり、埋込み次数が4の倍数次の場合には、最終べきのべき乗算は$(q^{4h}-1)/r$乗のべき乗算であり、埋込み次数が6の倍数次の場合には、最終べきのべき乗算は$(q^{6h}-1)/r$乗のべき乗算である。

[0044] 以下において、第3ステップでの$l_{T,T}(x_P, y_P)$の演算、及び第5ステップでの$l_{T,Q}(x_P, y_P)$の演算方法を説明する。ここで、埋込み次数を偶数次、すなわち2h(h:自然数)次として、楕円曲線を$y^2=x^3+ax+b$, $a\in F_q$, $b\in F_q$(q:3より大きい素数のべき乗)とする。

[0045] $T=(x_T, y_T)$,$Q=(x_Q, y_Q)$とすると、$l_{T,Q}(x, y)$の傾き$\lambda_{T,Q}$は次式で与えられる。

[数26]

$$\lambda_{T,T}=\frac{3x_T^{\ 2}+a}{2y_T}$$

[数27]

$$\lambda_{T,Q}=\frac{y_Q-y_T}{x_Q-x_T}\qquad (T\neq Q\text{とする})$$

[0046] この傾き$\lambda_{T,Q}$を用いて$l_{T,Q}(x_P, y_P)$の値を以下のように計算する。

[数28]

$$l_{T,Q}(x_P,y_P)=(x_P-x_T)\lambda_{T,Q}-(y_P-y_T)$$

[0047] 通常では、この[数26]及び[数27]によって$E(F_q^{2h})$上で演算を行っているのであるが、埋込み次数を偶数次、すなわち2h(h:自然数)次として、楕円曲線を$y^2=x^3+ax+b$, $a\in F_q$, $b\in F_q$ (q:3より大きい素数のべき乗)とした場合には、$E(F_q^{h})$のツイスト曲線$E'(F_q^{h}): y^2=x^3+av^{-2}x+bv^{-3}$, $v\in F_q^{h}$が存在して、$E'(F_q^{h})$から$E(F_q^{2h})$への準同型写像$(x, y)\rightarrow(xv, yv^{3/2})$が存在する。ここで、新たなパラメータvは、$(q^{2h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余な元である。

[0048] したがって、$E(F_q^{2h})[r]$上の楕円加算を1／2の拡大次数の$E'(F_q^{h})[r]$上の楕円加算に置き換えて演算することが可能であり、演算負荷を低減して高速な演算を可能とすることができる。

[0049] 特に、有理点$T, Q\in E(F_q^{2h})$に対して、$T=(x_T, y_T)=(x_{T'}v, y_{T'}v^{3/2})$、$Q=(x_Q, y_Q)=(x_{Q'}v, y_{Q'}v^{3/2})$の関係が成り立つ有理点T'、Q'が$E'(F_q^{h})$に存在するので、まず、$l_{T,T}(x, y)$の傾き$\lambda_{T,T}$、及び$l_{T,Q}(x, y)$の傾き$\lambda_{T,Q}$を以下のように変形する。

[数29]

$$\lambda_{T,T}=\frac{3x_T^{\ 2}+a}{2y_T}=\frac{(3x_{T'}^{\ 2}+av^{-2})v^2}{2y_{T'}v^{3/2}}=\lambda_{T',T'}v^{1/2}$$

[数30]

$$\lambda_{T,Q}=\frac{y_Q-y_T}{x_Q-x_T}=\frac{(y_{Q'}-y_{T'})v^{3/2}}{(x_{Q'}-x_{T'})v}=\lambda_{T',Q'}v^{1/2}\qquad (T\neq Q\text{とする})$$

[0050] [数29]と[数30]から、T＝Q、T≠Qにかかわらず傾き$\lambda_{T,Q}$は、以下のようになる。

[数31]

$$\lambda_{T,Q} = \lambda_{T',Q'} v^{1/2}$$

[0051] したがって、[数31]の式から、[数28]の式は以下のようになる。

[数32]

$$\begin{aligned} l_{T,Q}(x_P, y_P) &= (x_P - x_T)\lambda_{T,Q} - (y_P - y_T) \\ &= (x_P - x_{T'} v)\lambda_{T',Q'} v^{1/2} - (y_P - y_{T'} v^{3/2}) \\ &= ((x_P v^{-1} - x_{T'})\lambda_{T',Q'} - (y_P v^{-3/2} - y_{T'}))v^{3/2} \\ &= l_{T',Q'}(x_P v^{-1}, y_P v^{-3/2}) v^{3/2} \end{aligned}$$

[0052] この[数32]の式の最後の$v^{3/2}$の部分は、ペアリング演算における$(q^{2h}-1)/r$乗の最終べきの演算によって1となるので、ミラーのアルゴリズムにおける$l_{T,Q}(x_P, y_P)$を演算する際には、$l_{T,Q}(x_P, y_P)$の演算を行うのではなく、$l_{T',Q'}(x_P v^{-1}, y_P v^{-3/2})$を真部分体上において演算すればよく、演算負荷を大きく低減することができる。

[0053] すなわち、曲線の式が$y^2 = x^3 + ax + b$, $a \in F_q$, $b \in F_q$ (q：3より大きい素数のべき乗)で与えられ、埋込み次数が2h次(h：自然数)で、F_q^{2h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1 = E[r] \cap \mathrm{Ker}(\phi_q - [1])$

$G_2 = E[r] \cap \mathrm{Ker}(\phi_q - [q])$

により、

$e: G_2 \times G_1 \rightarrow F_q^{*2h}/(F_q^{*2h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P \in G_1$、$Q \in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs＝t－1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数33]

$$e(Q,P) = f_{s,Q}(P)^{(q^{2h}-1)/r}$$

としてAteペアリングe(Q,P)を演算する場合に、$f_{s,Q}(P)$の導出に必要となる有理関数$l_{T,T}(x_P, y_P)$及び$l_{T,Q}(x_P, y_P)$の演算を、この$f_{s,Q}(P)$の$(q^{2h}-1)/r$乗のべき乗算の演算によって1となる平方非剰余な$v \in F_q^h$を用いて、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2 = x^3 + av^{-2}x + bv^{-3}$による真部分体上で$l_{T',T'}(x_P v^{-1}, y_P v^{-3/2})$及び$l_{T',Q'}(x_P v^{-1}, y_P v^{-3/2})$の演算として行うことにより、演算負荷を低減して高速な演算を可能とすることができる。

[0054] 埋込み次数を3の倍数次、すなわち3h(h:自然数)次として、曲線の式を$y^2 = x^3 + a$, $a \in F_q$ (q:3より大きい素数のべき乗)とした場合には、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2 = x^3 + av^{-1}$, $v \in F_q^h$が存在して、$E'(F_q^h)$から$E(F_q^{3h})$への準同型写像$(x, y) \to (xv^{1/3}, yv^{1/2})$が存在する。ここで、新たなパラメータvは、$(q^{3h}-1)/r$乗のべき乗算の演算によって1となる平方剰余かつ3乗非剰余な元である。

[0055] したがって、$E(F_q^{3h})$[r]上の楕円加算を1/3の拡大次数の$E'(F_q^h)$[r]上の楕円加算に置き換えて演算することが可能であり、演算負荷を低減して高速な演算を可能とすることができる。

[0056] 特に、有理点T、$Q \in E(F_q^{3h})$に対して、$T = (x_T, y_T) = (x_{T'}v^{1/3}, y_{T'}v^{1/2})$、$Q = (x_Q, y_Q) = (x_{Q'}v^{1/3}, y_{Q'}v^{1/2})$の関係が成り立つ有理点T'、Q'が$E'(F_q^h)$に存在するので、まず、$l_{T,T}(x, y)$の傾き$\lambda_{T,T}$、及び$l_{T,Q}(x, y)$の傾き$\lambda_{T,Q}$を以下のように変形する。

[数34]

$$\lambda_{T,T} = \frac{3x_T^2}{2y_T} = \frac{3x_{T'}^2 v^{2/3}}{2y_{T'}v^{1/2}} = \lambda_{T',T'}v^{1/6}$$

[数35]

$$\lambda_{T,Q} = \frac{y_Q - y_T}{x_Q - x_T} = \frac{(y_{Q'} - y_{T'})v^{1/2}}{(x_{Q'} - x_{T'})v^{1/3}} = \lambda_{T',Q'}v^{1/6} \qquad (T \neq Q\text{とする})$$

[0057] [数34]と[数35]から、T=Q、T≠Qにかかわらず傾き$\lambda_{T,Q}$は、以下のようになる。

[数36]

$$\lambda_{T,Q} = \lambda_{T',Q'}v^{1/6}$$

[0058] したがって、[数36]の式から、[数28]の式は以下のようになる。

[数37]

$$l_{T,Q}(x_P,y_P)=(x_P-x_T)\lambda_{T,Q}-(y_P-y_T)$$
$$=(x_P-x_{T'}v^{1/3})\lambda_{T',Q'}v^{1/6}-(y_P-y_{T'}v^{1/2})$$
$$=((x_Pv^{-1/3}-x_{T'})\lambda_{T',Q'}-(y_Pv^{-1/2}-y_{T'}))v^{1/2}$$
$$=l_{T',Q'}(x_Pv^{-1/3},y_Pv^{-1/2})v^{1/2}$$

この[数37]の式の最後の$v^{1/2}$の部分は、ペアリング演算における$(q^{3h}-1)/r$乗の最終べきの演算によって1となるので、ミラーのアルゴリズムにおける$l_{T,Q}(x_P, y_P)$を演算する際には、$l_{T,Q}(x_P, y_P)$の演算を行うのではなく、$l_{T',Q'}(x_Pv^{-1/3}, y_Pv^{-1/2})$を真部分体上において演算すればよく、演算負荷を大きく低減することができる。

[0059] すなわち、曲線の式が$y^2=x^3+a$, $a\in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が3h次(h:自然数)で、F_q^{3h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r]\cap Ker(\phi_q-[1])$

$G_2=E[r]\cap Ker(\phi_q-[q])$

により、

$e:G_2\times G_1\rightarrow F_q^{*3h}/(F_q^{*3h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P\in G_1$、$Q\in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs=t−1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数38]

$$e(Q,P)=f_{s,Q}(P)^{(q^{3h}-1)/r}$$

としてAteペアリングe(Q,P)を演算する場合に、$f_{s,Q}(P)$の導出に必要となる有理関数$l_{T,T}(x_P, y_P)$及び$l_{T,Q}(x_P, y_P)$の演算を、この$f_{s,Q}(P)$の$(q^{3h}-1)/r$乗のべき乗算の演算によって1となる平方剰余かつ3乗非剰余な$v\in F_q^h$を用いて、$E(F_q^h)$のツイスト曲線$E'(F_q^h)$:$y^2=x^3+av^{-1}$による真部分体上で$l_{T',T'}(x_Pv^{-1/3}, y_Pv^{-1/2})$及び$l_{T',Q'}(x_Pv^{-1/3}, y_Pv^{-1/2})$の演算として行うことによって、演算負荷を低減して高速な演算を可能とすることができる。

[0060] 埋込み次数を4の倍数次、すなわち4h(h:自然数)次として、曲線の式を$y^2=x^3+ax$, $a\in F_q$ (q:3より大きい素数のべき乗)で、4がq^h-1を割り切るとした場合には、$E(F_{q^h})$のツイスト曲線$E'(F_{q^h}): y^2=x^3+av^{-1}x$, $v\in F_{q^h}$が存在して、$E'(F_{q^h})$から$E(F_{q^{4h}})$への準同型写像$(x, y)\rightarrow(xv^{1/2}, yv^{3/4})$が存在する。ここで、新たなパラメータvは、$(q^{4h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余な元である。

[0061] したがって、$E(F_{q^{4h}})[r]$上の楕円加算を1／4の拡大次数の$E'(F_{q^h})[r]$上の楕円加算に置き換えて演算することが可能であり、演算負荷を低減して高速な演算を可能とすることができる。

[0062] 特に、有理点T、$Q\in E(F_{q^{4h}})$に対して、$T=(x_T, y_T)=(x_{T'}v^{1/2}, y_{T'}v^{3/4})$、$Q=(x_Q, y_Q)=(x_{Q'}v^{1/2}, y_{Q'}v^{3/4})$の関係が成り立つ有理点T'、Q'が$E'(F_{q^h})$に存在するので、まず、$l_{T,T}(x, y)$の傾き$\lambda_{T,T}$、及び$l_{T,Q}(x, y)$の傾き$\lambda_{T,Q}$を以下のように変形する。

[数39]

$$\lambda_{T,T}=\frac{3x_T^{\,2}+a}{2y_T}=\frac{(3x_{T'}^{\,2}+av^{-1})v}{2y_{T'}v^{3/4}}=\lambda_{T',T'}v^{1/4}$$

[数40]

$$\lambda_{T,Q}=\frac{y_Q-y_T}{x_Q-x_T}=\frac{(y_{Q'}-y_{T'})v^{3/4}}{(x_{Q'}-x_{T'})v^{1/2}}=\lambda_{T',Q'}v^{1/4}\qquad(T\neq Q\text{とする})$$

[0063] [数39]と[数40]から、T=Q、T≠Qにかかわらず傾き$\lambda_{T,Q}$は、以下のようになる。

[数41]

$$\lambda_{T,Q}=\lambda_{T',Q'}v^{1/4}$$

[0064] したがって、[数41]の式から、[数28]の式は以下のようになる。

[数42]

$$\begin{aligned}l_{T,Q}(x_P,y_P)&=(x_P-x_T)\lambda_{T,Q}-(y_P-y_T)\\&=(x_P-x_{T'}v^{1/2})\lambda_{T',Q'}v^{1/4}-(y_P-y_{T'}v^{3/4})\\&=((x_Pv^{-1/2}-x_{T'})\lambda_{T',Q'}-(y_Pv^{-3/4}-y_{T'}))v^{3/4}\\&=l_{T',Q'}(x_Pv^{-1/2},y_Pv^{-3/4})v^{3/4}\end{aligned}$$

[0065] この[数42]の式の最後の$v^{3/4}$の部分は、ペアリング演算における$(q^{4h}-1)$/r乗の最

終べきの演算によって1となるので、ミラーのアルゴリズムにおける$l_{T,Q}(x_P, y_P)$を演算する際には、$l_{T,Q}(x_P, y_P)$の演算を行うのではなく、$l_{T',Q'}(x_P v^{-1/2}, y_P v^{-3/4})$を真部分体上において演算すればよく、演算負荷を大きく低減することができる。

[0066] すなわち、曲線の式が$y^2=x^3+ax$, $a\in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が4h次(h:自然数)で、4がq^h-1を割り切るものとし、F_q^{4h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r]\cap Ker(\phi_q-[1])$

$G_2=E[r]\cap Ker(\phi_q-[q])$

により、

$e:G_2\times G_1\rightarrow F_q^{*4h}/(F_q^{*4h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P\in G_1$、$Q\in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs=t−1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数43]

$$e(Q,P)=f_{s,Q}(P)^{(q^{4h}-1)/r}$$

としてAteペアリングe(Q,P)を演算する場合に、$f_{s,Q}(P)$の導出に必要となる有理関数$l_{T,T}(x_P, y_P)$及び$l_{T,Q}(x_P, y_P)$の演算を、この$f_{s,Q}(P)$の$(q^{4h}-1)/r$乗のべき乗算の演算によって1となる平方非剰余な$v\in F_q^h$を用いて、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2=x^3+av^{-1}x$による真部分体上で$l_{T',T'}(x_P v^{-1/2}, y_P v^{-3/4})$及び$l_{T',Q'}(x_P v^{-1/2}, y_P v^{-3/4})$の演算として行うことによって、演算負荷を低減して高速な演算を可能とすることができる。

[0067] 埋込み次数を6の倍数次、すなわち6h(h:自然数)次として、曲線の式が$y^2=x^3+a$, $a\in F_q$ (q:3より大きい素数のべき乗)とした場合には、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2=x^3+av^{-1}$, $v\in F_q^h$が存在して、$E'(F_q^h)$から$E(F_q^{6h})$への準同型写像$(x, y)\rightarrow(xv^{1/3}, yv^{1/2})$が存在する。ここで、新たなパラメータvは、$(q^{6h}-1)/r$乗のべき乗算の演算によって1となる平方非剰余かつ3乗非剰余な元である。

[0068] したがって、$E(F_q^{6h})[r]$上の楕円加算を1／6の拡大次数の$E'(F_q^h)[r]$上の楕円加算に置き換えて演算することが可能であり、演算負荷を低減して高速な演算を可能とす

ることができる。

[0069] 特に、有理点T、Q∈E(F_q^{6h})に対して、T=(x_T, y_T)=($x_{T'}v^{1/3}$、$y_{T'}v^{1/2}$)、Q=(x_Q, y_Q)=($x_{Q'}v^{1/3}$、$y_{Q'}v^{1/2}$)の関係が成り立つ有理点T'、Q'がE'(F_p^h)に存在するので、まず、$l_{T,T}(x, y)$の傾き$\lambda_{T,T}$、及び$l_{T,Q}(x, y)$の傾き$\lambda_{T,Q}$を以下のように変形する。

[数44]

$$\lambda_{T,T}=\frac{3x_T^{\ 2}}{2y_T}=\frac{3x_{T'}^{\ 2}v^{2/3}}{2y_{T'}v^{1/2}}=\lambda_{T',T'}v^{1/6}$$

[数45]

$$\lambda_{T,Q}=\frac{y_Q-y_T}{x_Q-x_T}=\frac{(y_{Q'}-y_{T'})v^{1/2}}{(x_{Q'}-x_{T'})v^{1/3}}=\lambda_{T',Q'}v^{1/6} \qquad (T\neq Q\text{とする})$$

[0070] [数44]と[数45]から、T=Q、T≠Qにかかわらず傾き$\lambda_{T,Q}$は、以下のようになる。

[数46]

$$\lambda_{T,Q}=\lambda_{T',Q'}v^{1/6}$$

[0071] したがって、[数46]の式から、[数28]の式は以下のようになる。

[数47]

$$\begin{aligned}l_{T,Q}(x_P,y_P)&=(x_P-x_T)\lambda_{T,Q}-(y_P-y_T)\\&=(x_P-x_{T'}v^{1/3})\lambda_{T',Q'}v^{1/6}-(y_P-y_{T'}v^{1/2})\\&=((x_Pv^{-1/3}-x_{T'})\lambda_{T',Q'}-(y_Pv^{-1/2}-y_{T'}))v^{1/2}\\&=l_{T',Q'}(x_Pv^{-1/3},y_Pv^{-1/2})v^{1/2}\end{aligned}$$

[0072] この[数47]の式の最後の$v^{1/2}$の部分は、ペアリング演算における$(q^{6h}-1)/r$乗の最終べきの演算によって1となるので、ミラーのアルゴリズムにおける$l_{T,Q}(x_P, y_P)$を演算する際には、$l_{T,Q}(x_P, y_P)$の演算を行うのではなく、$l_{T',Q'}(x_Pv^{-1/3}, y_Pv^{-1/2})$を真部分体上において演算すればよく、演算負荷を大きく低減することができる。

[0073] すなわち、曲線の式が$y^2=x^3+a$, a∈F_q (q:3より大きい素数のべき乗)で与えられ、埋込み次数が6h次(h:自然数)で、F_q^{6h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1 = E[r] \cap \mathrm{Ker}(\phi_q - [1])$

$G_2 = E[r] \cap \mathrm{Ker}(\phi_q - [q])$

により、

$e: G_2 \times G_1 \rightarrow F_q^{*6h}/(F_q^{*6h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P \in G_1$、$Q \in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs＝t－1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数48]

$$e(Q,P) = f_{s,Q}(P)^{(q^{6h}-1)/r}$$

としてAteペアリングe(Q,P)を演算する場合に、$f_{s,Q}(P)$の導出に必要となる有理関数$l_{T,T}(x_P, y_P)$及び$l_{T,Q}(x_P, y_P)$の演算を、この$f_{s,Q}(P)$の$(q^{6h}-1)/r$乗のべき乗算の演算によって1となる平方非剰余かつ3乗非剰余な$v \in F_q^h$を用いて、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2 = x^3 + av^{-1}$による真部分体上で$l_{T',T'}(x_P v^{-1/3}, y_P v^{-1/2})$及び$l_{T',Q'}(x_P v^{-1/3}, y_P v^{-1/2})$の演算として行うことによって、演算負荷を低減して高速な演算を可能とすることができる。

[0074] 以下において、埋込み次数が、偶数次、3の倍数次、4の倍数次、及び6の倍数次の最小公倍数である12次の場合におけるペアリング演算のプログラムについて説明する。図2は、図1に対応させた埋込み次数が12次の場合のミラーのアルゴリズムである。ここで、これまで3より大きい素数のべき乗としていたqを、素数pとする。

[0075] 認証サーバなどのように電子計算機で構成されるペアリング演算装置では、図3に示すフローチャートに基づくプログラムによりペアリング演算を行って、大規模なディジタルグループ署名を実現している。

[0076] ここで、ペアリング演算を行う電子計算機は、図2に示したミラーのアルゴリズムに基づくプログラムを内蔵したペアリング演算プログラムを実行可能とした電子計算機であって、図4に示すように、電子計算機10は、演算処理を実行するCPU11と、ペアリング演算プログラムなどの各種プログラム、及びペアリング演算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、ペアリング演算プログラム

を展開して実行可能とするとともに、ペアリング演算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4中、14はバスである。なお、図示しないが電子計算機10には記録媒体ドライブを備えており、ペアリング演算プログラムを記録した記録媒体をこの記録媒体ドライブを介して記憶装置12に記憶させるようにすることも可能である。

[0077] 本発明のペアリング演算プログラムを利用するディジタルグループ署名技術においては、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から送信されたディ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4中、15は電子計算機10の入出力制御部である。電子計算機10では、クライアント装置30から送信されたディジタルグループ署名の署名データはメモリ装置13に一次的に記憶している。

[0078] 電子計算機10のCPU11は、クライアント装置30からディ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、ペアリング演算プログラムを起動させる(ステップS1)。

[0079] 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のCPU11は、入力手段として機能して、フロベニウス自己準同型写像ϕ_pのトレースtに基づくs＝t－1、P∈E(F_p)であるP、Q'∈E'(F_p^2)であるQ'の入力を受け付ける(ステップS2)。メモリ装置13に一旦記憶した署名データはPとQ'のいずれか一方であり、一般的にはPである。Q'及びフロベニウス自己準同型写像ϕ_pのトレースtまたはs＝t－1は、記憶装置12またはメモリ装置13の所定アドレスに記憶しており、所定アドレスから読み出して入力している。

[0080] 次いで、電子計算機10のCPU11は、代入手段として機能して、有理点Pの座標(x_P, y_P)に対して、n←$x_P v^{-1/3}$、m←$y_P v^{-1/2}$の代入演算を行う(ステップS3)。ここで、$v^{-1/3}$の値、及び$v^{-1/2}$の値は既知であって、記憶装置12またはメモリ装置13の所定アドレスに記憶しており、所定アドレスから読み出して入力して$x_P v^{-1/3}$の演算、及び$y_P v^{-1/2}$の演算を行っている。

[0081] なお、この代入演算は、埋込み次数が12次で、6の倍数次となっているのでn←$x_P v^{-1/3}$、m←$y_P v^{-1/2}$の代入演算であるが、埋込み次数が偶数次の場合にはn←$x_P v^{-1}$、

$m \leftarrow y_P v^{-3/2}$の代入演算、埋込み次数が3の倍数次の場合には$n \leftarrow x_P v^{-1/3}$、$m \leftarrow y_P v^{-1/2}$の代入演算、埋込み次数が4の倍数次の場合には$n \leftarrow x_P v^{-1/2}$、$m \leftarrow y_P v^{-3/4}$の代入演算となる。

[0082] 次いで、電子計算機10のCPU11は、代入手段として機能して、$f \leftarrow 1$、$T' \leftarrow Q'$の代入演算を行う(ステップS4)。これは、いわゆる初期値設定である。

[0083] 次いで、電子計算機10のCPU11は、2進数表示したsのビット数をいの初期値として、以下の演算の繰り返しのたびにiを1ずつ減算しながらfの値を演算している(ステップS5)。ここで、上記したのと同様に、s[i]は、2進数表示したsの最小ビットから数えてi番目のビットの値を示すものとする。

[0084] ステップS5では、具体的には、電子計算機10のCPU11は、第1演算手段として機能して、有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-1/2}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行い、次いで、電子計算機10のCPU11は、第2演算手段として機能して、$T' \leftarrow 2T'$の代入演算を行っている。

[0085] さらに、2進数表示したsのi番目のビットの値s[i]が1である場合には、電子計算機10のCPU11は、第3演算手段として機能して、有理点TとQを通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-1/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行い、次いで、電子計算機10のCPU11は、第4演算手段として機能して、$T' \leftarrow T' + Q'$の代入演算を行っている。

[0086] ステップS5での演算後、電子計算機10のCPU11は、演算結果のfをメモリ装置13に一次的に記憶して、ミラー関数の演算を終了している(ステップS6)。

[0087] 次いで、電子計算機10のCPU11は、演算結果のfの値を用いて$(p^{12}-1)/r$乗のべき乗算を行って、演算結果をペアリング演算の結果としてメモリ装置13に一次的に記憶している(ステップS7)。

[0088] 電子計算機10のCPU11では、上記のペアリング演算を失効者の数に応じた回数だけ繰り返し行って、ペアリング演算プログラムを終了している。

[0089] 電子計算機10が認証サーバである場合には、その後、電子計算機10のCPU11は

、ペアリング演算の結果を用いて認証を行っている。

[0090] このように、ペアリング演算を行う電子計算機で構成されたペアリング演算装置では、埋込み次数が12次の場合、$E(F_p^{12})[r]$上の楕円加算ではなく、$E'(F_p^{2})[r]$上の楕円加算として演算を行うことにより、ミラーのアルゴリズムに基づく演算に要する時間を30%程度削減可能であり、より高速にペアリング演算を可能とすることができる。

[0091] したがって、より多くのメンバーを対象としたディジタルグループ署名に利用でき、ディジタルグループ署名をより広範囲で利用することができる。

[0092] 本実施形態では、ディジタルグループ署名に用いるペアリング演算について説明したが、本発明に係るペアリング演算の装置、方法、プログラムを記録した記録媒体は、ディジタルグループ署名に用いる場合に限定するものではなく、必要に応じて適宜のペアリング演算に適用することができる。

請求の範囲

[1] 曲線の式が$y^2=x^3+ax+b$, $a\in F_q$, $b\in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が2h次(h:自然数)で、F_q^{2h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r]\cap Ker(\phi_q-[1])$

$G_2=E[r]\cap Ker(\phi_q-[q])$

により、

$e:G_2\times G_1\rightarrow F_q^{*2h}/(F_q^{*2h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P\in G_1$、$Q\in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs=t−1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数1]

$$e(Q,P)=f_{s,Q}(P)^{(q^{2h}-1)/r}$$

としてAteペアリングe(Q,P)を演算するペアリング演算装置において、

$f_{s,Q}(P)$の導出に必要となる有理関数の演算を、この$f_{s,Q}(P)$の$(q^{2h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余な$v\in F_q^h$を用いて、$E(F_q^h)$のツイスト曲線$E'(F_q^h):y^2=x^3+av^{-2}x+bv^{-3}$による真部分体上で行うべく、

前記s=t−1、$P\in E(F_q)$であるP、$Q'\in E'(F_q^h)$であるQ'の入力を受け付ける入力手段と、

有理点Pの座標(x_P, y_P)に対して、$n\leftarrow x_P v^{-1}$、$m\leftarrow y_P v^{-3/2}$の代入演算を行うとともに、f←1、T'←Q'の代入演算を行う代入手段と、

有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-3/2}$を$l_{T',T'}(n, m)$で演算して、$f\leftarrow f^2\cdot l_{T',T'}(n, m)$の代入演算を行う第1演算手段と、

T'←2T'の代入演算を行う第2演算手段と、

前記sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを

通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-3/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行う第3演算手段と、

前記sを2進数表示とした場合の所定のビットの値が1である場合に、$T' \leftarrow T' + Q'$の代入演算を行う第4演算手段と、

$(q^{2h}-1)/r$乗のべき乗算を演算する第5演算手段と

を備えたことを特徴とするペアリング演算装置。

[2] 曲線の式が$y^2=x^3+a$, $a \in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が3h次(h:自然数)で、F_q^{3h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r] \cap \mathrm{Ker}(\phi_q-[1])$

$G_2=E[r] \cap \mathrm{Ker}(\phi_q-[q])$

により、

$e: G_2 \times G_1 \rightarrow F_q^{*3h}/(F_q^{*3h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P \in G_1$、$Q \in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs=t−1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数2]

$$e(Q,P) = f_{s,Q}(P)^{(q^{3h}-1)/r}$$

としてAteペアリングe(Q,P)を演算するペアリング演算装置において、

$f_{s,Q}(P)$の導出に必要となる有理関数の演算を、この$f_{s,Q}(P)$の$(q^{3h}-1)$／r乗のべき乗算の演算によって1となる平方剰余かつ3乗非剰余な$v \in F_q^h$を用いて、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2=x^3+av^{-1}$による真部分体上で行うべく、

前記s=t−1、$P \in E(F_q)$であるP、$Q' \in E'(F_q^h)$であるQ'の入力を受け付ける入力手段と、

有理点Pの座標(x_P, y_P)に対して、$n \leftarrow x_P v^{-1/3}$、$m \leftarrow y_P v^{-1/2}$の代入演算を行うとともに、$f \leftarrow 1$、$T' \leftarrow Q'$の代入演算を行う代入手段と、

有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-1/2}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行う第1演算手段と、

T'←2T'の代入演算を行う第2演算手段と、

前記sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-1/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行う第3演算手段と、

前記sを2進数表示とした場合の所定のビットの値が1である場合に、T'←T'+Q'の代入演算を行う第4演算手段と、

$(q^{3h}-1)/r$乗のべき乗算を演算する第5演算手段と

を備えたことを特徴とするペアリング演算装置。

[3] 曲線の式が$y^2=x^3+ax$, $a \in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が4h次(h:自然数)で、4がq^h-1を割り切るものとし、F_q^{4h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r] \cap \mathrm{Ker}(\phi_q-[1])$

$G_2=E[r] \cap \mathrm{Ker}(\phi_q-[q])$

により、

$e: G_2 \times G_1 \rightarrow F_q^{*4h}/(F_q^{*4h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P \in G_1$、$Q \in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs=t-1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数3]

$$e(Q,P) = f_{s,Q}(P)^{(q^{4h}-1)/r}$$

としてAteペアリングe(Q,P)を演算するペアリング演算装置において、

$f_{s,Q}(P)$の導出に必要となる有理関数の演算を、この$f_{s,Q}(P)$の$(q^{4h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余な$v \in F_q^h$を用いて、$E(F_q^h)$のツイスト曲線$E'(F_q^h$

):$y^2=x^3+av^{-1}x$による真部分体上で行うべく、

前記s＝t－1、P∈E(F_q)であるP、Q'∈E'(F_q^h)であるQ'の入力を受け付ける入力手段と、

有理点Pの座標(x_P, y_P)に対して、n←$x_P v^{-1/2}$、m←$y_P v^{-3/4}$の代入演算を行うとともに、f←1、T'←Q'の代入演算を行う代入手段と、

有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-3/4}$を$l_{T',T'}(n, m)$で演算して、f←$f^2 \cdot l_{T',T'}(n, m)$の代入演算を行う第1演算手段と、

T'←2T'の代入演算を行う第2演算手段と、

前記sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-3/4}$を$l_{T',Q'}(n, m)$で演算して、f←$f \cdot l_{T',Q'}(n, m)$の代入演算を行う第3演算手段と、

前記sを2進数表示とした場合の所定のビットの値が1である場合に、T'←T'＋Q'の代入演算を行う第4演算手段と、

(q^{4h}－1)/r乗のべき乗算を演算する第5演算手段と

を備えたことを特徴とするペアリング演算装置。

[4] 曲線の式が$y^2=x^3+a$, a∈F_q(q:3より大きい素数のべき乗)で与えられ、埋込み次数が6h次(h:自然数)で、F_q^{6h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r]\cap \mathrm{Ker}(\phi_q-[1])$

$G_2=E[r]\cap \mathrm{Ker}(\phi_q-[q])$

により、

$e:G_2\times G_1\rightarrow F_q^{*6h}/(F_q^{*6h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、P∈G_1、Q∈G_2とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs＝t－1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数4]

$$e(Q,P) = f_{s,Q}(P)^{(q^{6h}-1)/r}$$

としてAteペアリングe(Q,P)を演算するペアリング演算装置において、

$f_{s,Q}(P)$の導出に必要となる有理関数の演算を、この$f_{s,Q}(P)$の$(q^{6h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余かつ3乗非剰余な$v \in F_q^h$を用いて、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2 = x^3 + av^{-1}$による真部分体上で行うべく、

前記s＝t－1、$P \in E(F_q)$であるP、$Q' \in E'(F_q^h)$であるQ'の入力を受け付ける入力手段と、

有理点Pの座標(x_P, y_P)に対して、$n \leftarrow x_P v^{-1/3}$、$m \leftarrow y_P v^{-1/2}$の代入演算を行うとともに、f←1、T'←Q'の代入演算を行う代入手段と、

有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-1/2}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行う第1演算手段と、

T'←2T'の代入演算を行う第2演算手段と、

前記sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-1/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行う第3演算手段と、

前記sを2進数表示とした場合の所定のビットの値が1である場合に、T'←T'＋Q'の代入演算を行う第4演算手段と、

$(q^{6h}-1)/r$乗のべき乗算を演算する第5演算手段と

を備えたことを特徴とするペアリング演算装置。

[5] 曲線の式が$y^2 = x^3 + ax + b$, $a \in F_q$, $b \in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が2h次(h:自然数)で、F_q^{2h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1 = E[r] \cap \mathrm{Ker}(\phi_q - [1])$

$G_2 = E[r] \cap \mathrm{Ker}(\phi_q - [q])$

により、

$e : G_2 \times G_1 \to F_q^{*2h}/(F_q^{*2h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P \in G_1$、$Q \in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs＝t－1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数5]

$$e(Q,P) = f_{s,Q}(P)^{(q^{2h}-1)/r}$$

としてAteペアリングe(Q,P)を電子計算機で演算するペアリング演算方法において、

$f_{s,Q}(P)$の$(q^{2h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余な$v \in F_q^h$、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2 = x^3 + av^{-2}x + bv^{-3}$を用いて、

前記電子計算機を入力手段として機能させて、前記s＝t－1、$P \in E(F_q)$であるP、$Q' \in E'(F_q^h)$であるQ'の入力を受け付けるステップと、

前記電子計算機を代入手段として機能させて、有理点Pの座標(x_P, y_P)に対して、$n \leftarrow x_P v^{-1}$、$m \leftarrow y_P v^{-3/2}$の代入演算を行うステップと、

前記電子計算機を代入手段として機能させて、f←1、T'←Q'の代入演算を行うステップと、

前記電子計算機を第1演算手段として機能させて、有理点Tを通る接線$l_{T,T}(x, y)$＝0の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-3/2}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行うステップと、

前記電子計算機を第2演算手段として機能させて、T'←2T'の代入演算を行うステップと、

前記電子計算機を第3演算手段として機能させて、前記sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)$＝0の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-3/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行うステップと、

前記電子計算機を第4演算手段として機能させて、前記sを2進数表示とした場合の所定のビットの値が1である場合に、T'←T'＋Q'の代入演算を行うステップと、

前記電子計算機を第5演算手段として機能させて、$(q^{2h}-1)/r$乗のべき乗算の演算を行うステップと

を有することを特徴とするペアリング演算方法。

[6] 曲線の式が$y^2=x^3+a$, $a\in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が3h次(h:自然数)で、F_q^{3h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r]\cap \mathrm{Ker}(\phi_q-[1])$

$G_2=E[r]\cap \mathrm{Ker}(\phi_q-[q])$

により、

$e:G_2\times G_1\rightarrow F_q^{*3h}/(F_q^{*3h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P\in G_1$、$Q\in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs=t−1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数6]

$$e(Q,P)=f_{s,Q}(P)^{(q^{3h}-1)/r}$$

としてAteペアリングe(Q,P)を電子計算機で演算するペアリング演算方法において、

$f_{s,Q}(P)$の$(q^{3h}-1)$／r乗のべき乗算の演算によって1となる平方剰余かつ3乗非剰余な$v\in F_q^h$、$E(F_q^h)$のツイスト曲線$E'(F_q^h):y^2=x^3+av^{-1}$を用いて、

前記電子計算機を入力手段として機能させて、前記s=t−1、$P\in E(F_q)$であるP、$Q'\in E'(F_q^h)$であるQ'の入力を受け付けるステップと、

前記電子計算機を代入手段として機能させて、有理点Pの座標(x_P, y_P)に対して、$n\leftarrow x_P v^{-1/3}$、$m\leftarrow y_P v^{-1/2}$の代入演算を行うステップと、

前記電子計算機を代入手段として機能させて、f←1、T'←Q'の代入演算を行うステップと、

前記電子計算機を第1演算手段として機能させて、有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-1/2}$を$l_{T',T'}(n, m)$で演算して、$f\leftarrow f^2\cdot l_{T',T'}(n, m)$の代入演算を行うステップと、

前記電子計算機を第2演算手段として機能させて、T'←2T'の代入演算を行うステップと、

前記電子計算機を第3演算手段として機能させて、前記sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-1/2}$を$l_{T',Q'}(n, m)$で演算して、f←f•$l_{T',Q'}(n, m)$の代入演算を行うステップと、

前記電子計算機を第4演算手段として機能させて、前記sを2進数表示とした場合の所定のビットの値が1である場合に、T'←T'＋Q'の代入演算を行うステップと、

前記電子計算機を第5演算手段として機能させて、$(q^{3h}-1)/r$乗のべき乗算の演算を行うステップと

を有することを特徴とするペアリング演算方法。

[7] 曲線の式が$y^2=x^3+ax$, $a\in F_q$（q：3より大きい素数のべき乗）で与えられ、埋込み次数が4h次（h：自然数）で、4がq^h-1を割り切るものとし、F_q^{4h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r]\cap Ker(\phi_q-[1])$

$G_2=E[r]\cap Ker(\phi_q-[q])$

により、

$e:G_2\times G_1\rightarrow F_q^{*4h}/(F_q^{*4h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P\in G_1$、$Q\in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs＝t－1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数7]

$$e(Q,P)=f_{s,Q}(P)^{(q^{4h}-1)/r}$$

としてAteペアリングe(Q,P)を電子計算機で演算するペアリング演算方法において、

$f_{s,Q}(P)$の$(q^{4h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余な$v\in F_q^h$、$E(F_q^h)$のツイスト曲線$E'(F_q^h):y^2=x^3+av^{-1}x$を用いて、

前記電子計算機を入力手段として機能させて、前記s＝t－1、$P\in E(F_q)$であるP、

$Q' \in E'(F_q^h)$であるQ'の入力を受け付けるステップと、

前記電子計算機を代入手段として機能させて、有理点Pの座標(x_P, y_P)に対して、$n \leftarrow x_P v^{-1/2}$、$m \leftarrow y_P v^{-3/4}$の代入演算を行うステップと、

前記電子計算機を代入手段として機能させて、$f \leftarrow 1$、$T' \leftarrow Q'$の代入演算を行うステップと、

前記電子計算機を第1演算手段として機能させて、有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-3/4}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行うステップと、

前記電子計算機を第2演算手段として機能させて、$T' \leftarrow 2T'$の代入演算を行うステップと、

前記電子計算機を第3演算手段として機能させて、前記sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-3/4}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行うステップと、

前記電子計算機を第4演算手段として機能させて、前記sを2進数表示とした場合の所定のビットの値が1である場合に、$T' \leftarrow T' + Q'$の代入演算を行うステップと、

前記電子計算機を第5演算手段として機能させて、$(q^{4h}-1)/r$乗のべき乗算の演算を行うステップと

を有することを特徴とするペアリング演算方法。

[8] 曲線の式が$y^2 = x^3 + a$, $a \in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が6h次(h:自然数)で、F_q^{6h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$$G_1 = E[r] \cap \mathrm{Ker}(\phi_q - [1])$$

$$G_2 = E[r] \cap \mathrm{Ker}(\phi_q - [q])$$

により、

$$e: G_2 \times G_1 \rightarrow F_q^{*6h}/(F_q^{*6h})^r$$

である非退化な双線形写像として定義されるAteペアリングeによって、$P \in G_1$、$Q \in$

G_2とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs＝t－1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数8]

$$e(Q,P)=f_{s,Q}(P)^{(q^{6h}-1)/r}$$

としてAteペアリングe(Q,P)を電子計算機で演算するペアリング演算方法において、

$f_{s,Q}(P)$の$(q^{6h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余かつ3乗非剰余な$v\in F_q^h$、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2=x^3+av^{-1}$を用いて、

前記電子計算機を入力手段として機能させて、前記s＝t－1、$P\in E(F_q)$であるP、$Q'\in E'(F_q^h)$であるQ'の入力を受け付けるステップと、

前記電子計算機を代入手段として機能させて、有理点Pの座標(x_P, y_P)に対して、$n\leftarrow x_P v^{-1/3}$、$m\leftarrow y_P v^{-1/2}$の代入演算を行うステップと、

前記電子計算機を代入手段として機能させて、f←1、T'←Q'の代入演算を行うステップと、

前記電子計算機を第1演算手段として機能させて、有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-1/2}$を$l_{T',T'}(n, m)$で演算して、$f\leftarrow f^2\cdot l_{T',T'}(n, m)$の代入演算を行うステップと、

前記電子計算機を第2演算手段として機能させて、T'←2T'の代入演算を行うステップと、

前記電子計算機を第3演算手段として機能させて、前記sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-1/2}$を$l_{T',Q'}(n, m)$で演算して、$f\leftarrow f\cdot l_{T',Q'}(n, m)$の代入演算を行うステップと、

前記電子計算機を第4演算手段として機能させて、前記sを2進数表示とした場合の所定のビットの値が1である場合に、T'←T'＋Q'の代入演算を行うステップと、

前記電子計算機を第5演算手段として機能させて、$(q^{6h}-1)/r$乗のべき乗算の演算を行うステップと

を有することを特徴とするペアリング演算方法。

[9] 曲線の式が$y^2=x^3+ax+b$, $a\in F_q$, $b\in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が2h次(h:自然数)で、F_q^{2h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r]\cap Ker(\phi_q-[1])$

$G_2=E[r]\cap Ker(\phi_q-[q])$

により、

$e:G_2\times G_1\rightarrow F_q^{*2h}/(F_q^{*2h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P\in G_1$、$Q\in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs=t−1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数9]

$$e(Q,P)=f_{s,Q}(P)^{(q^{2h}-1)/r}$$

としてAteペアリングe(Q,P)を電子計算機に演算させるペアリング演算プログラムにおいて、

$f_{s,Q}(P)$の$(q^{2h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余な$v\in F_q^h$、$E(F_q^h)$のツイスト曲線$E'(F_q^h):y^2=x^3+av^{-2}x+bv^{-3}$を用いて、

前記電子計算機を入力手段として機能させて、前記s=t−1、$P\in E(F_q)$であるP、$Q'\in E'(F_q^h)$であるQ'の入力を受け付けさせるステップと、

前記電子計算機を代入手段として機能させて、有理点Pの座標(x_P, y_P)に対して、$n\leftarrow x_P v^{-1}$、$m\leftarrow y_P v^{-3/2}$の代入演算を行わせるステップと、

前記電子計算機を代入手段として機能させて、f←1、T'←Q'の代入演算を行わせるステップと、

前記電子計算機を第1演算手段として機能させて、有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-3/2}$を$l_{T',T'}(n, m)$で演算して、$f\leftarrow f^2\cdot l_{T',T'}(n, m)$の代入演算を行わせるステップと、

前記電子計算機を第2演算手段として機能させて、T'←2T'の代入演算を行わせ

るステップと、

前記電子計算機を第3演算手段として機能させて、前記sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-3/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行わせるステップと、

前記電子計算機を第4演算手段として機能させて、前記sを2進数表示とした場合の所定のビットの値が1である場合に、T'←T'＋Q'の代入演算を行わせるステップと、

前記電子計算機を第5演算手段として機能させて、$(q^{2h}-1)/r$乗のべき乗算の演算を行わせるステップと

を前記電子計算機に実行させることを特徴とするペアリング演算プログラムを記録した記録媒体。

[10] 曲線の式が$y^2=x^3+a$, $a \in F_q$（q：3より大きい素数のべき乗）で与えられ、埋込み次数が3h次（h：自然数）で、F_q^{3h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r] \cap \mathrm{Ker}(\phi_q-[1])$

$G_2=E[r] \cap \mathrm{Ker}(\phi_q-[q])$

により、

$e: G_2 \times G_1 \rightarrow F^{*}_{q^{3h}}/(F^{*}_{q^{3h}})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P \in G_1$、$Q \in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs＝t－1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数10]

$$e(Q,P) = f_{s,Q}(P)^{(q^{3h}-1)/r}$$

としてAteペアリングe(Q,P)を電子計算機に演算させるペアリング演算プログラムにおいて、

$f_{s,Q}(P)$の$(q^{3h}-1)$／r乗のべき乗算の演算によって1となる平方剰余かつ3乗非剰

余な$v \in F_q^h$、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2 = x^3 + av^{-1}$を用いて、

前記電子計算機を入力手段として機能させて、前記$s = t - 1$、$P \in E(F_q)$であるP、$Q' \in E'(F_q^h)$であるQ'の入力を受け付けさせるステップと、

前記電子計算機を代入手段として機能させて、有理点Pの座標(x_P, y_P)に対して、$n \leftarrow x_P v^{-1/3}$、$m \leftarrow y_P v^{-1/2}$の代入演算を行わせるステップと、

前記電子計算機を代入手段として機能させて、$f \leftarrow 1$、$T' \leftarrow Q'$の代入演算を行わせるステップと、

前記電子計算機を第1演算手段として機能させて、有理点Tを通る接線$l_{T,T}(x, y) = 0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-1/2}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行わせるステップと、

前記電子計算機を第2演算手段として機能させて、$T' \leftarrow 2T'$の代入演算を行わせるステップと、

前記電子計算機を第3演算手段として機能させて、前記sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y) = 0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-1/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行わせるステップと、

前記電子計算機を第4演算手段として機能させて、前記sを2進数表示とした場合の所定のビットの値が1である場合に、$T' \leftarrow T' + Q'$の代入演算を行わせるステップと、

前記電子計算機を第5演算手段として機能させて、$(q^{3h} - 1)/r$乗のべき乗算の演算を行わせるステップと

を前記電子計算機に実行させることを特徴とするペアリング演算プログラムを記録した記録媒体。

[11] 曲線の式が$y^2 = x^3 + ax$, $a \in F_q$ (q:3より大きい素数のべき乗)で与えられ、埋込み次数が4h次(h:自然数)で、4が$q^h - 1$を割り切るものとし、F_q^{4h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1 = E[r] \cap \mathrm{Ker}(\phi_q - [1])$

$G_2 = E[r] \cap \mathrm{Ker}(\phi_q - [q])$

により、

$e: G_2 \times G_1 \rightarrow F_q^{*4h}/(F_q^{*4h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P \in G_1$、$Q \in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs＝t－1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数11]

$$e(Q,P) = f_{s,Q}(P)^{(q^{4h}-1)/r}$$

としてAteペアリングe(Q,P)を電子計算機に演算させるペアリング演算プログラムにおいて、

$f_{s,Q}(P)$の$(q^{4h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余な$v \in F_q^h$、$E(F_q^h)$のツイスト曲線$E'(F_q^h): y^2 = x^3 + av^{-1}x$を用いて、

前記電子計算機を入力手段として機能させて、前記s＝t－1、$P \in E(F_q)$であるP、$Q' \in E'(F_q^h)$であるQ'の入力を受け付けさせるステップと、

前記電子計算機を代入手段として機能させて、有理点Pの座標(x_P, y_P)に対して、$n \leftarrow x_P v^{-1/2}$、$m \leftarrow y_P v^{-3/4}$の代入演算を行わせるステップと、

前記電子計算機を代入手段として機能させて、f←1、T'←Q'の代入演算を行わせるステップと、

前記電子計算機を第1演算手段として機能させて、有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-3/4}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行わせるステップと、

前記電子計算機を第2演算手段として機能させて、T'←2T'の代入演算を行わせるステップと、

前記電子計算機を第3演算手段として機能させて、前記sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-3/4}$

を$l_{T',Q'}(n, m)$で演算して、f←f•$l_{T',Q'}(n, m)$の代入演算を行わせるステップと、

前記電子計算機を第4演算手段として機能させて、前記sを2進数表示とした場合の所定のビットの値が1である場合に、T'←T'＋Q'の代入演算を行わせるステップと、

前記電子計算機を第5演算手段として機能させて、$(q^{4h}-1)/r$乗のべき乗算の演算を行わせるステップと

を前記電子計算機に実行させることを特徴とするペアリング演算プログラムを記録した記録媒体。

[12] 曲線の式が$y^2=x^3+a$, $a\in F_q$（q：3より大きい素数のべき乗）で与えられ、埋込み次数が6h次（h：自然数）で、F_q^{6h}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なす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_qをフロベニウス自己準同型写像として、

$G_1=E[r]\cap Ker(\phi_q-[1])$

$G_2=E[r]\cap Ker(\phi_q-[q])$

により、

$e:G_2\times G_1\rightarrow F_q^{*6h}/(F_q^{*6h})^r$

である非退化な双線形写像として定義されるAteペアリングeによって、$P\in G_1$、$Q\in G_2$とし、フロベニウス自己準同型写像ϕ_qのトレースtを用いてs＝t－1とし、ミラー関数$f_{s,Q}(\cdot)$を用いて、

[数12]

$$e(Q,P)=f_{s,Q}(P)^{(q^{6h}-1)/r}$$

としてAteペアリングe(Q,P)を電子計算機に演算させるペアリング演算プログラムにおいて、

$f_{s,Q}(P)$の$(q^{6h}-1)$／r乗のべき乗算の演算によって1となる平方非剰余かつ3乗非剰余な$v\in F_q^h$、$E(F_q^h)$のツイスト曲線$E'(F_q^h):y^2=x^3+av^{-1}$を用いて、

前記電子計算機を入力手段として機能させて、前記s＝t－1、$P\in E(F_q)$であるP、$Q'\in E'(F_q^h)$であるQ'の入力を受け付けさせるステップと、

前記電子計算機を代入手段として機能させて、有理点Pの座標(x_P, y_P)に対して、$n \leftarrow x_P v^{-1/3}$、$m \leftarrow y_P v^{-1/2}$の代入演算を行わせるステップと、

前記電子計算機を代入手段として機能させて、f←1、T'←Q'の代入演算を行わせるステップと、

前記電子計算機を第1演算手段として機能させて、有理点Tを通る接線$l_{T,T}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,T}(x_P, y_P)$を演算する代わりに、$l_{T,T}(x_P, y_P)v^{-1/2}$を$l_{T',T'}(n, m)$で演算して、$f \leftarrow f^2 \cdot l_{T',T'}(n, m)$の代入演算を行わせるステップと、

前記電子計算機を第2演算手段として機能させて、T'←2T'の代入演算を行わせるステップと、

前記電子計算機を第3演算手段として機能させて、前記sを2進数表示とした場合の所定のビットの値が1である場合に、有理点TとQを通る直線$l_{T,Q}(x, y)=0$の左辺に有理点Pの座標(x_P, y_P)を代入した値$l_{T,Q}(x_P, y_P)$を演算する代わりに、$l_{T,Q}(x_P, y_P)v^{-1/2}$を$l_{T',Q'}(n, m)$で演算して、$f \leftarrow f \cdot l_{T',Q'}(n, m)$の代入演算を行わせるステップと、

前記電子計算機を第4演算手段として機能させて、前記sを2進数表示とした場合の所定のビットの値が1である場合に、T'←T'＋Q'の代入演算を行わせるステップと、

前記電子計算機を第5演算手段として機能させて、$(q^{6h}-1)/r$乗のべき乗算の演算を行わせるステップと

を前記電子計算機に実行させることを特徴とするペアリング演算プログラムを記録した記録媒体。

[図1]

入力：$s=t-1$, $P\in E(\mathbb{F}_p)$, $Q\in E(\mathbb{F}_{p^{12}})$
出力：$f_{s,Q}(P)$

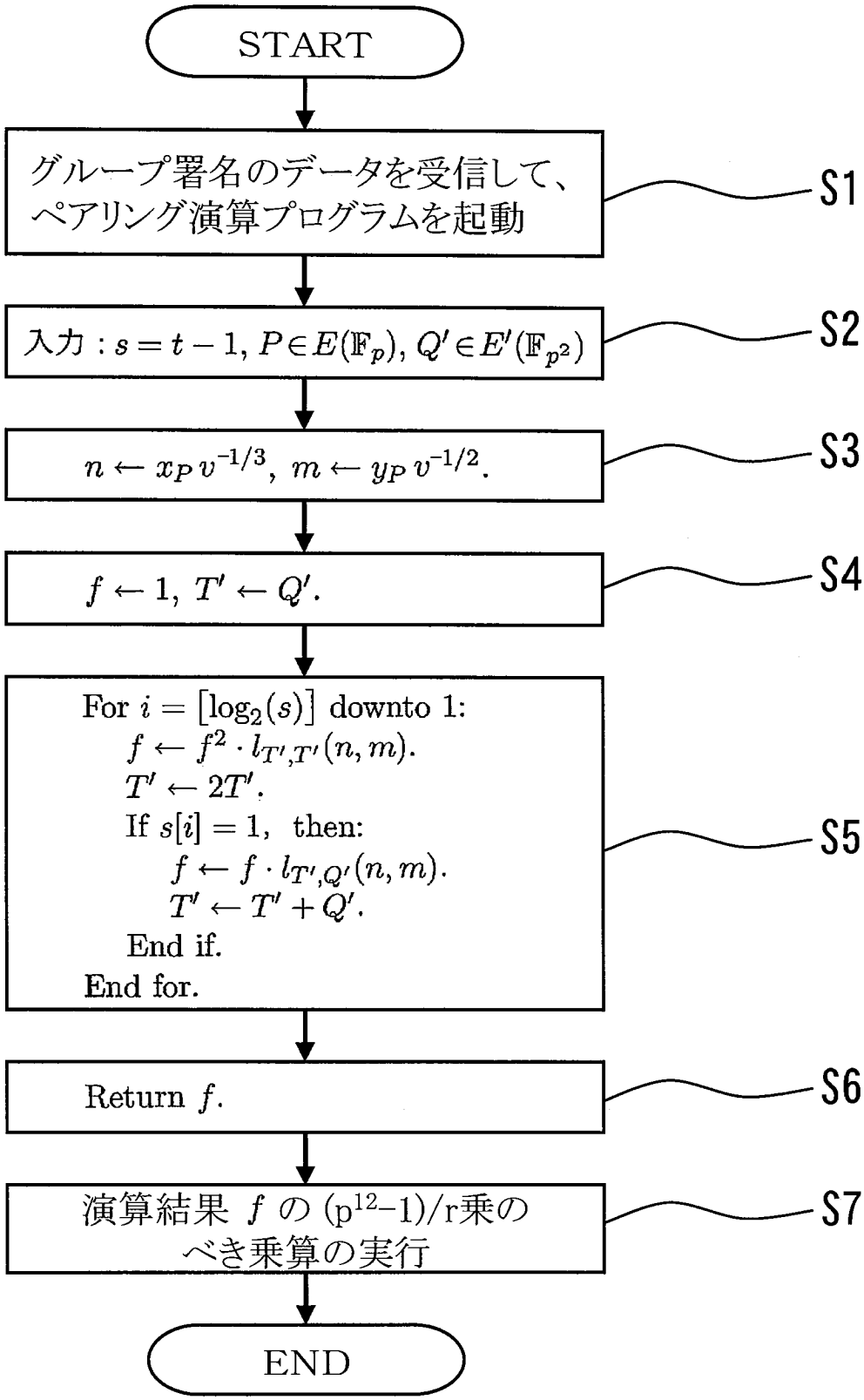
1. $f\leftarrow 1$, $T\leftarrow Q$.
2. For $i=[\log_2(s)]$ downto 1:
3. $\quad f\leftarrow f^2\cdot l_{T,T}(x_P,y_P)$.
4. $\quad T\leftarrow 2T$.
5. $\quad$ If $s[i]=1$, then:
6. $\quad\quad f\leftarrow f\cdot l_{T,Q}(x_P,y_P)$.
7. $\quad\quad T\leftarrow T+Q$.
8. $\quad$ End if.
9. End for.
10. Return f.

[図2]

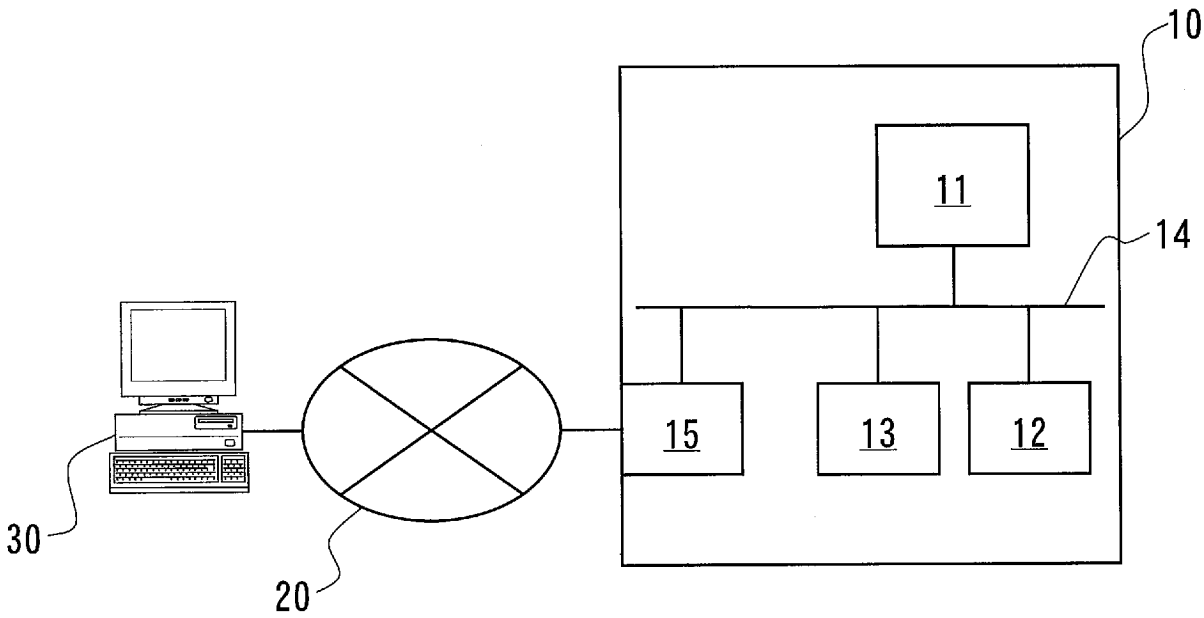
入力：$s=t-1$, $P\in E(\mathbb{F}_p)$, $Q'\in E'(\mathbb{F}_{p^2})$
出力：$f_{s,Q}(P)$

1. $n\leftarrow x_P v^{-1/3}$, $m\leftarrow y_P v^{-1/2}$.
2. $f\leftarrow 1$, $T'\leftarrow Q'$.
3. For $i=[\log_2(s)]$ downto 1:
4. $\quad f\leftarrow f^2\cdot l_{T',T'}(n,m)$.
5. $\quad T'\leftarrow 2T'$.
6. $\quad$ If $s[i]=1$, then:
7. $\quad\quad f\leftarrow f\cdot l_{T',Q'}(n,m)$.
8. $\quad\quad T'\leftarrow T'+Q'$.
9. $\quad$ End if.
10. End for.
11. Return f.

[図3]


START
グループ署名のデータを受信して、
ペアリング演算プログラムを起動
S1
入力：$s=t-1$, $P\in E(\mathbb{F}_p)$, $Q'\in E'(\mathbb{F}_{p^2})$
S2
$n \leftarrow x_P v^{-1/3}$, $m \leftarrow y_P v^{-1/2}$.
S3
$f \leftarrow 1$, $T' \leftarrow Q'$.
S4
For $i = [\log_2(s)]$ downto 1:
$f \leftarrow f^2 \cdot l_{T',T'}(n,m)$.
$T' \leftarrow 2T'$.
If $s[i] = 1$, then:
$f \leftarrow f \cdot l_{T',Q'}(n,m)$.
$T' \leftarrow T' + Q'$.
End if.
End for.
S5
Return f.
S6
演算結果 f の $(p^{12}-1)/r$乗の
べき乗算の実行
S7
END

[図4]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/069683

A. CLASSIFICATION OF SUBJECT MATTER
G09C1/00(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)
G09C1/00

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 1996-2009
Kokai Jitsuyo Shinan Koho 1971-2009 Toroku Jitsuyo Shinan Koho 1994-2009

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus(JDreamII), JMEDPlus(JDreamII), JST7580(JDreamII)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Seiichi MATSUDA, Naoki KANEYAMA, Ken OKAMOTO, Eiji OKAMOTO, "Twisted Ate Pairing no Kosokuka Shuho no Teian", IEICE Technical Report (ISEC 2006-101~114), 06 December, 2006 (06.12.06), Vol.106, No.411, pages 29 to 34	1-4
A	Masaaki SHIRASE, Go TAKAGI, Eiji OKAMOTO, "Tate Pairing no Koritsuteki na Algorithm", Information Processing Society of Japan Kenkyu Hokoku (2006-CSEC-34), 20 July, 2006 (20.07.06), Vol.2006, No.81, pages 19 to 26	1-4

☒ 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	Date of mailing of the international search report
06 January, 2009 (06.01.09)	20 January, 2009 (20.01.09)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/069683

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Takumi OKIMOTO, Masataka AKANE, Mayumi OBARA, Yasuyuki NOGAMI, Yoshitaka MORIKAWA, "Twist o Mochiita Kokateki na Pairing no Jissoho", Computer Security Symposium 2006 Ronbunshu, 25 October, 2006 (25.10.06), Vol.2006, No.11, pages 37 to 42	1-4
A	Yasuyuki NOGAMI, Yoshitaka MORIKAWA, "Twist o Mochiita Pairing Keisan no Kosokuka shuho", Dai 4 Kai Shanon Riron Workshop, 2006, pages 7 to 12	1-4
P,Y	Masataka AKANE, Hidehiro KATO, Takumi OKIMOTO, Yasuyuki NOGAMI, Yoshitaka MORIKAWA, "Barreto-Naehrig Kyokusen o Mochiita Ate Pairing ni Okeru Miller Algorithm no Kairyo", Computer Security Symposium 2007 Ronbunshu, 31 October, 2007 (31.10.07), Vol.2007, No.10, pages 489 to 494	1-4
P,Y	Masataka AKANE, Hidehiro KATO, Takumi OKIMOTO, Yasuyuki NOGAMI, Yoshitaka MORIKAWA, "Ate Pairing ni Tekishita Barreto-Naehrig Kyokusen no Parameter Settei", Computer Security Symposium 2007 Ronbunshu, 31 October, 2007 (31.10.07), Vol.2007, No.10, pages 495 to 500	1-4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/069683

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.: 5-12
because they relate to subject matter not required to be searched by this Authority, namely:
See the "extra sheet".

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:

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

[ ] The additional search fees were accompanied by the applicant's protest and, where applicable, 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.

Continuation of Box No.II-1 of continuation of first sheet(2)

Claim 5-8 relate to a scheme for computing an Ate pairing e(Q, P), and a mathematical computation procedure (algorithm) itself such as this scheme for computing an Ate pairing e(Q, P) is a scientific and mathematical theory. The "electronic computer" in the matter stated in claims 5-8 merely realizes the functions such as "input means", "substituting means", and "computing means" that existing electronic computers have on the basis of "the pairing computing scheme" i.e., a scientific and mathematic theory. Therefore, the matter stated in claims 5-8 relates to a scientific and mathematic theory, and the subject matter is not required to be searched by this International Searching Authority under PCT Article 17(2)(a)(i) and PCT Rule 39.1(i).

Claims 9-12 relate to a recording medium where a program for executing a scheme for computing an Ate pairing e(Q, P) is recorded, and a mathematical computation procedures (algorithm) itself such as this scheme for computing an Ate pairing e(Q, P) is a scientific and mathematical theory. The "electronic computer" in the matter stated in claims 9-12 merely realizes the functions such as "input means", "substituting means", and "computing means" that existing electronic computers have on the basis of "the pairing computing scheme" i.e., a scientific and mathematic theory. Further, the function of the "recording medium" stated in claims 9-12 is to mere present program information which is a scientific and mathematical theory and is mere presentation of information. Consequently, claims 9-12 relate to a scientific and mathematical theory and mere presentation of information, and the subject matter is not required to be searched by this International Searching Authority under PCT Article 17(2)(a)(i), PCT Rule 39.1(i), and PCT Rule 39.1(v).

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００８／０６９６８３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G09C1/00(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（ＩＰＣ））

Int.Cl.　G09C1/00

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	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００９年
日本国実用新案登録公報	１９９６－２００９年
日本国登録実用新案公報	１９９４－２００９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(JDreamII), JMEDPlus(JDreamII), JST7580(JDreamII)

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	関連する請求の範囲の番号
Ａ	松田誠一，金山直樹，岡本健，岡本栄司，“Ｔｗｉｓｔｅｄ　Ａｔｅペアリングの高速化手法の提案”，電子情報通信学会技術研究報告（ＩＳＥＣ２００６－１０１～１１４），2006.12.06，Ｖｏｌ．１０６，Ｎｏ．４１１，ｐ．２９－３４	１－４
Ａ	白勢政明，高木剛，岡本栄司，“Ｔａｔｅペアリングの効率的なアルゴリズム”，情報処理学会研究報告（２００６－ＣＳＥＣ－３４），2006.07.20，Ｖｏｌ．２００６，Ｎｏ．８１，ｐ．１９－２６	１－４

☑　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	国際調査報告の発送日
０６．０１．２００９	２０．０１．２００９

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
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）　５Ｓ　４２２９
青木　重徳
電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　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	関連する請求の範囲の番号
Ａ	沖本卓求弥，赤根正剛，小原真由美，野上保之，森川良孝，“ツイストを用いた効果的なペアリングの実装法”，コンピュータセキュリティシンポジウム２００６論文集，2006.10.25，Ｖｏｌ．２００６，Ｎｏ．１１，ｐ．３７－４２	１－４
Ａ	野上保之，森川良孝，“ツイストを用いたペアリング計算の高速化手法”，第４回シャノン理論ワークショップ，2006，ｐ．７－１２	１－４
Ｐ，Ｙ	赤根正剛，加藤英洋，沖本卓求弥，野上保之，森川良孝，“Ｂａｒｒｅｔｏ－Ｎａｅｈｒｉｇ曲線を用いたＡｔｅペアリングにおけるＭｉｌｌｅｒアルゴリズムの改良”，コンピュータセキュリティシンポジウム２００７　論文集，2007.10.31，Ｖｏｌ．２００７，Ｎｏ．１０，ｐ．４８９－４９４	１－４
Ｐ，Ｙ	赤根正剛，加藤英洋，沖本卓求弥，野上保之，森川良孝，“Ａｔｅペアリングに適したＢａｒｒｅｔｏ－Ｎａｅｈｒｉｇ曲線のパラメータ設定”，コンピュータセキュリティシンポジウム２００７　論文集，2007.10.31，Ｖｏｌ．２００７，Ｎｏ．１０，ｐ．４９５－５００	１－４

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００８／０６９６８３

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．☑ 請求の範囲 ５－１２ 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、
「特別ページ」を参照。

２．☐ 請求の範囲＿＿＿＿＿＿＿＿ 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．☐ 請求の範囲＿＿＿＿＿＿＿＿ 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。

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の範囲について作成した。

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の範囲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ので、この国際調査報告は、手数料の納付のあった次の請求の範囲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ので、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の範囲について作成した。

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。

請求の範囲５－８は、Ａｔｅペアリングｅ（Ｑ，Ｐ）を演算する手法について記載したものであって、Ａｔｅペアリングｅ（Ｑ，Ｐ）を演算する手法のような数学的な計算手順（アルゴリズム）そのものは科学及び数学の理論に該当し、また、請求の範囲５－８に係る事項における「電子計算機」は、「入力手段」や「代入手段」、「演算手段」という既存の電子計算機が有する機能を「ペアリング演算方法」という科学及び数学の理論に基いて実現しているに過ぎないから、よって、請求の範囲５－８は科学及び数学の理論に該当し、ＰＣＴ第１７条（２）（ａ）（ｉ）及びＰＣＴ規則３９．１（ｉ）の規定により、この国際調査機関が調査することを必要としない対象に係るものである。

請求の範囲９－１２は、Ａｔｅペアリングｅ（Ｑ，Ｐ）を演算する手法を実行するプログラムを記録した記録媒体について記載したものであって、Ａｔｅペアリングｅ（Ｑ，Ｐ）を演算する手法のような数学的な計算手順(アルゴリズム)そのものは科学及び数学の理論に該当し、請求の範囲９－１２に係る事項における「電子計算機」は、「入力手段」や「代入手段」、「演算手段」という既存の電子計算機が有する機能を「ペアリング演算方法」という科学及び数学の理論に基いて実現しているに過ぎず、さらに、請求の範囲９－１２に係る「記録媒体」の機能は、科学及び数学の理論に該当するプログラム情報を単に提示するだけのものであるから、情報の単なる提示に該当することから、よって、請求の範囲９－１２は科学及び数学の理論及び情報の単なる提示に該当し、ＰＣＴ第１７条（２）（ａ）（ｉ）及びＰＣＴ規則３９．１（ｉ），（ｖ）の規定により、この国際調査機関が調査することを必要としない対象に係るものである。