

(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
2010年3月4日(04.03.2010)

(10) 国際公開番号
WO 2010/024401 A1

PCT

- (51) 国際特許分類:
G09C 1/00 (2006.01)
- (21) 国際出願番号: PCT/JP2009/065099
- (22) 国際出願日: 2009年8月28日(28.08.2009)
- (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 2008-222556 2008年8月29日(29.08.2008) 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). 赤根 正剛(AKANE, Masataka) [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). 酒見 由美(SAKEMI, Yumi) [JP/JP]; 〒7008530 岡山県岡山市北区津島中三

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).

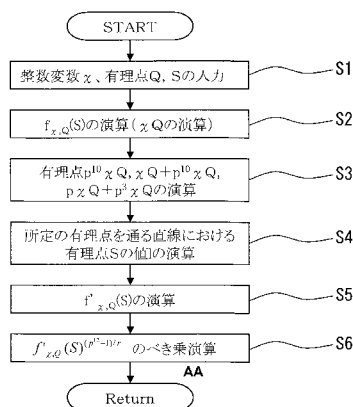
- (74) 代理人: 森 寿夫, 外(MORI, Hisao et al.); 〒7100047 岡山県倉敷市大島505-14 Okayama (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, 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, 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,

[続葉有]

(54) Title: PAIRING COMPUTATION DEVICE, PAIRING COMPUTATION METHOD, AND PAIRING COMPUTATION PROGRAM

(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

[図2]



$$e(Q, S) = f'_{x,Q}(S)^{(p^k-1)/r} \quad (1)$$

- S1 INPUT INTEGER VARIABLE x , RATIONAL POINTS Q , S
S2 COMPUTE $f_{x,Q}(S)$ (COMPUTE xQ)
S3 COMPUTE RATIONAL POINTS $p^{10} xQ$, $xQ+p^{10} xQ$, $pxQ+p^3 xQ$
S4 COMPUTE VALUE I OF RATIONAL POINT S ON LINE THROUGH PREDETERMINED RATIONAL POINT
S5 COMPUTE $f'_{x,Q}(S)$
AA RAISING OF

(57) Abstract: Disclosed are a pairing computation device, a pairing computation method, and a pairing computation program, all enabling fast pairing computation. The pairing computation device includes a computing means for computing a rational function $f_{x,Q}(S)$ letting the expression of a curve be given by $y^2=x^3+ax+b$ where $a \in F_p$ and $b \in F_p$, E be an additive group of rational points on a pairable elliptic curve the embedding order of which is k and the definition of which is F_p^k , $E[r]$ be a set of rational points having a prime order r , ϕ_p be a Frobenius endomorphism, and the order r and the trace t of the Frobenius endomorphism ϕ_p be functions of an integer variable x ; a computing means for computing the value of a line through a predetermined rational point at a rational point $S(x_s, y_s)$; a computing means for computing a rational function $f'_{x,Q}(S)$ by using the results of the computations by the former two computing means; and a computing means for performing pairing computation by using the rational function $f'_{x,Q}(S)$ where $e(Q, S)$ is given by mathematical formula (1).

(57) 要約: 高速なペアリング演算を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提供する。曲線の式が $y^2=x^3+ax+b$, $a \in F_p$, $b \in F_p$ で与えられ、埋込み次数が 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_p をフロベニウス自己準同型写像として、位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t を整数変数 x の関数とし、有理関数 $f_{x,Q}(S)$ を演算する演算手段と、所定の有理点を通る直線の有理点 $S(x_s, y_s)$ における値を演算する演算手段と、これらの演算手段の演算結果を用いて有理関数 $f'_{x,Q}(S)$ を演算する演算手段と、有理関数 $f'_{x,Q}(S)$ を用いて式(1)としてペアリング演算を行う演算手段と有するものとする。



GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, 添付公開書類:

NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ,

CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN,

TD, TG).

— 国際調査報告 (条約第 21 条(3))

明 細 書

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

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に関する。

背景技術

[0002] 従来、個人ユーザがインターネットなどのネットワーク上において提供されている各種のサービスを利用する場合に、その個人ユーザが正規のユーザであることを確認する認証処理が行われていることがある。このような認証処理では、一般的に、個人ユーザごとにあらかじめ設定されたID及びパスワード等を用いて認証している。そのために、ネットワークには、認証処理を実行するための認証サーバが設けられている。

[0003] 最近では、デジタル署名技術を用いることにより、個々のデータ自体に個人ユーザに固有のデジタル署名データを付加している。このデジタル署名データによって、個人ユーザが利用するデータ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きた。

[0004] 一方、デジタル署名では、認証サーバでの認証処理にともなって個人ユーザが特定されるため、認証処理のたびに認証サーバに個々の個人ユーザの履歴が情報として逐次蓄積されることとなっている。したがって、認証サーバには、個人ユーザが、どのようなサイトにアクセスしたかとか、どのようなサービスを利用したかなどの個人情報が蓄積されることとなるので、個人情報保護の点からこれらの情報の漏洩が生じないように、十分な注意が払われている。

[0005] このようなデジタル署名を用いることによって生じる個人ユーザの履歴情報の蓄積を解消するために、デジタル署名を拡張したデジタルグループ署名を用いることが提案されている。

[0006] デジタルグループ署名を用いた場合には、個人ユーザは、認証サーバに対して匿名で所定の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個人ユーザを特定することなく個人ユーザ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、認証サーバでは、グループに属さない個人ユーザによる不正利用を阻止する一方で、個人ユーザごとの履歴情報を蓄積することなく個人ユーザを認証している。

[0007] このようなデ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。

[0008] ペアリング演算は、2入力1出力の関数を用いた演算であって、たとえば、 S を素体 F_p 上の有理点、 Q を k 次拡大体 F_{p^k} 上の有理点として、2つの有理点 S と Q を入力することにより拡大体 $F_{p^k}^*$ の元 z が出力されるものである。しかも、ペアリング演算は、有理点 S の a 倍と、有理点 Q の b 倍を入力した場合に、 z の ab 乗が算出されるという双線形性を有している。この双線形性を利用して認証を行っている。ここで、「 k 」は埋込み次数であり、「 $F_{p^k}^*$ 」は、数学における表記上、正しくは、

[数1]

$$F_{p^k}^*$$

であるが、表示の制限上、「 $F_{p^k}^*$ 」と表示している。

[0009] 一般的に、有理点 S 、 Q にはそれぞれ楕円曲線上の点が用いられている。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とで構成されている。

[0010] 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、まず、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ている。次いで、デジタルグループ署名では、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。

[0011] したがって、たとえば、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に、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いる。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は約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秒を要することとなっている。したがって、現状では、デジタルグループ署名は実用的な技術とは考えられておらず、広く利用されるものとはなっていなかった。

[0012] 現状では、デジタルグループ署名を実用化するために、ペアリング演算の演算速度を向上させる研究が行われている。たとえば、ペアリング演算の高速化の技術として、楕円曲線上で定義される Tate ペアリング演算を用い、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の技術では未だに十分ではなく、さらなる高速化が求められていた。

[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 $y^2 = x^3 + ax + b$, $a \in F_p$, $b \in F_p$ で与えられ、埋込み次数が 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_p をフロベニウス自己準同型写像として、

$$G_1 = E[r] \cap \text{Ker}(\phi_p - [1]),$$

$$G_2 = E[r] \cap \text{Ker}(\phi_p - [p])$$

により、

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

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、 $S \in G_1$ 、 $Q \in G_2$ としてペアリング $e(Q, S)$ を演算して演算結果を出力するペアリング演算装置であって、フロベニウス自己準同型写像 ϕ_p のトレースを t として、ペアリング $e(Q, S)$ をミラーのアルゴリズムを用いて計算される有理関数 $f_{t-1, Q}(S)$ を用いて

[数2]

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

として演算する代わりに、位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t を整数変数 χ の関数として、有理関数 $f_{\chi, Q}(S)$ を演算する演算手段と、所定の有理点を通る直線の有理点 $S(x_s, y_s)$ における値を演算する演算手段と、これらの演算手段の演算結果を用いて有理関数 $f'_{\chi, Q}(S)$ を演算する演算手段と、有理関数 $f'_{\chi, Q}(S)$ を用いて

[数3]

$$e(Q, S) = f'_{\chi, Q}(S)^{(p^k - 1)/r}$$

としてペアリング演算を行う演算手段とによりペアリング演算を行うこととした。

[0016] さらに、本発明のペアリング演算装置では、有理関数 $f_{\chi, Q}(S)$ を演算する演算手段では、 χQ を演算して演算結果を所定のレジスタに記憶し、 χQ の演算結果を用いて所定の有理点を演算する演算手段を有することにも特徴を有する。

[0017] しかも、本発明のペアリング演算装置では、埋込み次数 $k=12$ の場合に、

位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t を、整数変数 χ を用いて

$$r(\chi) = 36\chi^4 - 36\chi^3 + 18\chi^2 - 6\chi + 1,$$

$$t(\chi) = 6\chi^2 + 1$$

とし、 $\chi Q = R$ として、この R のフロベニウス自己準同型写像 ϕ_p が $\phi_p(R) = pR$ である関係を用いて、有理点 $p^{10}\chi Q$ 、 $\chi Q + p^{10}\chi Q$ 、 $p\chi Q + p^3\chi Q$ をそれぞれ演算し、有理点 $(\chi Q, p^{10}\chi Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_1 と、有理点 $(\chi Q + p^{10}\chi Q, p\chi Q + p^3\chi Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_2 をそれぞれ演算し、有理点 $(p\chi Q, p^3\chi Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_3 を用いて

[数4]

$$f'_{\chi,Q}(S) = f_{\chi,Q}(S)^{1+p+p^3+p^{10}} \cdot l_1 \cdot l_2 \cdot l_3$$

として有理関数 $f'_{\chi,Q}(S)$ を演算することにも特徴を有する。

[0018] そのうえ、本発明のペアリング演算装置では、有理関数 $f_{\chi,Q}(S)$ のフロベニウス自己準同型写像 ϕ_p が $\phi_p(f_{\chi,Q}(S)) = f_{\chi,Q}(S)^p$ であることを用いて

[数5]

$$f_{\chi,Q}(S)^{1+p^{10}} \cdot l_1$$

を演算するとともに、 $Q_1, Q_2 \in G_2$ である有理点 (Q_1, Q_2) を通る直線における有理点 $S(x_s, y_s)$ の値 l のフロベニウス自己準同型写像 ϕ_p が有理点 (pQ_1, pQ_2) を通る直線における有理点 $S(x_s, y_s)$ の値であることを用いて

[数6]

$$f_{\chi,Q}(S)^{p+p^3} \cdot l_3 = \phi_p^3(f_{\chi,Q}(S)^{1+p^{10}} \cdot l_1)$$

となる

[数7]

$$f_{\chi,Q}(S)^{p+p^3} \cdot l_3$$

を演算して有理関数 $f'_{\chi,Q}(S)$ を演算することにも特徴を有する。

[0019] また、本発明のペアリング演算方法では、曲線の式が $y^2 = x^3 + ax + b$, $a \in F_p$, $b \in F_p$ で与えられ、埋込み次数が 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なす加法群を E 、素數位数 r の有理点の集合を $E[r]$ とし、 ϕ_p をフロベニウス自己準同型写像として、

$$G_1 = E[r] \cap \text{Ker}(\phi_p - [1]),$$

$$G_2 = E[r] \cap \text{Ker}(\phi_p - [p])$$

により、

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

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、 $S \in G_1$, $Q \in G_2$ としてCPUを備えた電子計算機でペアリング $e(Q, S)$ を演算するペアリング演算方法であって、フロベニウス自己準同型写像 ϕ_p のトレースを t として、ペアリング $e(Q, S)$ をミラーのアルゴリズムを用いて計算される有理関数 $f_{t-1,Q}(S)$ を用いて

[数2]

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

として演算する代わりに、位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t を整数変数 χ の関数として、電子計算機のCPUを演算手段として機能させて、有理関数 $f_{\chi,Q}(S)$ を演算するステップと、電子計算機のCPUを演算手段として機能させて、所定の有理点を通る直線の有理点 $S(x_s, y_s)$ における値を演算するステップと、電子計算機のCPUを演算手段として機能させて、前記の演算結果を用いて有理関数 $f'_{\chi,Q}(S)$ を演算するステップと、電子計算機のCPUを演算手段として機能させて、有理関数 $f'_{\chi,Q}(S)$ を用いて

[数3]

$$e(Q, S) = f'_{\chi, Q}(S)^{(p^k - 1)/r}$$

として演算するステップとを有するものである。

[0020] さらに、本発明のペアリング演算方法では、有理関数 $f_{\chi, Q}(S)$ を演算するステップの後、電子計算機のCPUを演算手段として機能させて、 χQ を演算し、この χQ の演算結果を用いて所定の有理点を演算するステップを有することにも特徴を有する。

[0021] また、本発明のペアリング演算プログラムでは、曲線の式が $y^2 = x^3 + ax + b$, $a \in F_p$, $b \in F_p$ で与えられ、埋込み次数が 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_p をフロベニウス自己準同型写像として、

$$G_1 = E[r] \cap \text{Ker}(\phi_p - [1]),$$

$$G_2 = E[r] \cap \text{Ker}(\phi_p - [p])$$

により、

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

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、 $S \in G_1$ 、 $Q \in G_2$ としてCPUを備えた電子計算機にペアリング $e(Q, S)$ を演算させるペアリング演算プログラムであって、フロベニウス自己準同型写像 ϕ_p のトレースを t として、ペアリング $e(Q, S)$ をミラーのアルゴリズムを用いて計算される有理関数 $f_{t-1, Q}(S)$ を用いて

[数2]

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

として演算させる代わりに、位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t を整数変数 χ の関数として、電子計算機を、有理関数 $f_{\chi, Q}(S)$ を演算する演算手段と、所定の有理点を通る直線の有理点 $S(x_s, y_s)$ における値を演算する演算手段と、これらの演算手段の演算結果を用いて有理関数 $f'_{\chi, Q}(S)$

S)を演算する演算手段と、この有理関数 $f'_{\chi,Q}(S)$ を用いて

[数3]

$$e(Q, S) = f'_{\chi, Q}(S)^{(p^k - 1)/r}$$

として演算する演算手段として機能させることとした。

- [0022] さらに、本発明のペアリング演算プログラムでは、電子計算機を、 χQ を演算する演算手段と、この χQ の演算結果を用いて所定の有理点を演算する演算手段として機能させることにも特徴を有する。

発明の効果

- [0023] 本発明によれば、ペアリング演算の際にミラーのアルゴリズムを用いて計算される有理関数を、整数変数 χ の関数とすることにより、有理関数の計算を高速に行うことができ、ペアリング演算を高速化することができる。したがって、実用性のあるデジタルグループ署名のサービスを提供できる。

図面の簡単な説明

- [0024] [図1]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模式図である。

[図2]図2は、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3]図3は、有理関数 $f_{\chi,Q}(S)$ を演算するためのフローチャートである。

[図4]図4は、本発明の他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。

符号の説明

- [0025] 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

[0026] 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、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、その演算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整数変数 χ を用いて有理関数を演算することにより、演算を高速化している。

[0027] 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、埋込み次数が 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_p をフロベニウス自己準同型写像として、

$$G_1 = E[r] \cap \text{Ker}(\phi_p - [1]),$$

$$G_2 = E[r] \cap \text{Ker}(\phi_p - [p])$$

により、

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

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、 $S \in G_1$ 、 $Q \in G_2$ 、フロベニウス自己準同型写像 ϕ_p のトレースを t として、ミラーのアルゴリズムで計算される有理関数 $f_{t-1,Q}(S)$ を用いて、ペアリング $e(Q, S)$ を、 Ate ペアリングとして知られている次式により演算していた。

[数2]

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

[0028] これに対して、本発明者らは、楕円曲線の整数変数 χ を用いることにより、より高速に演算が可能なペアリングを見出した。このペアリングを、「 $Xate$ ペアリング」と呼ぶこととする。

[0029] すなわち、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、 Ate ペアリングではなく $Xate$ ペアリング

を用いることにより、高速な演算を可能としているものである。

- [0030] 特に、ペアリング演算に用いられる楕円曲線は、組み込み次数に応じてそれぞれペアリングフレンドリ曲線として知られており、例えば組み込み次数 $k=12$ の場合には、位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t が、整数変数 χ を用いて次のように表せることが知られている。

$$r(\chi) = 36\chi^4 - 36\chi^3 + 18\chi^2 - 6\chi + 1,$$

$$t(\chi) = 6\chi^2 + 1.$$

- [0031] また、組み込み次数 $k=10$ の場合には、次のように表せることが知られている。

$$r(\chi) = 25\chi^4 + 25\chi^3 + 15\chi^2 + 5\chi + 1,$$

$$t(\chi) = 10\chi^2 + 5\chi + 3.$$

あるいは、次のようにも表せることが知られている。

$$r(\chi) = \chi^8 - 1,$$

$$t(\chi) = -\chi^6 + \chi^4 - \chi^2 + 2.$$

- [0032] また、組み込み次数 $k=8$ の場合には、次のように表せることが知られている。

$$r(\chi) = 9\chi^4 + 12\chi^3 + 8\chi^2 + 4\chi + 1,$$

$$t(\chi) = -9\chi^3 - 3\chi^2 - 2\chi.$$

あるいは、次のようにも表せることが知られている。

$$r(\chi) = \chi^4 - 8\chi^2 + 25,$$

$$t(\chi) = (2\chi^3 - 11\chi + 15) / 15.$$

あるいは、次のようにも表せることが知られている。

$$r(\chi) = \chi^8 - \chi^4 + 1,$$

$$t(\chi) = \chi^5 - \chi + 1.$$

- [0033] また、組み込み次数 $k=18$ の場合には、次のように表せることが知られている。

$$r(\chi) = (\chi^6 + 37\chi^3 + 343) / 343,$$

$$t(\chi) = (\chi^4 + 16\chi + 7) / 7.$$

[0034] 以下において、組み込み次数 $k=12$ の場合を一例として X a t e ペアリングを説明する。

[0035] なお、組み込み次数 $k=12$ の場合には、曲線の式が $y^2 = x^3 + b$, $b \in F_p$ で与えられ、 $F_{p^{12}}$ 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_p をフロベニウス自己準同型写像として、

$$G_1 = E[r] \cap \text{Ker}(\phi_p - [1]),$$

$$G_2 = E[r] \cap \text{Ker}(\phi_p - [p])$$

により、

$$e : G_2 \times G_1 \rightarrow F_p^{*12} / (F_p^{*12})^r$$

である非退化な双線形写像としてペアリング e を定義している。

[0036] この場合、位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t は、上述したように整数変数 χ を用いて次のように表せる。

$$r(\chi) = 36\chi^4 - 36\chi^3 + 18\chi^2 - 6\chi + 1 \quad \dots \quad (\text{式 } 1)$$

$$t(\chi) = 6\chi^2 + 1 \quad \dots \quad (\text{式 } 2)$$

[0037] (式 2) は次のように式変形できる。なお、特に必要でない場合には、便宜上、 (χ) の表記を省略する。

$$6\chi^2 \equiv t - 1 \equiv p \pmod{r} \quad \dots \quad (\text{式 } 3)$$

ここで、標数 p には次の関係式があることを用いている。

$$p = r + t - 1 \quad \dots \quad (\text{式 } 4)$$

[0038] したがって、標数 p は整数変数 χ を用いて次のように表せる。

$$p(\chi) = 36\chi^4 - 36\chi^3 + 24\chi^2 - 6\chi + 1 \quad \dots \quad (\text{式 } 5)$$

[0039] (式 3) を用いて、(式 5) は次のように式変形できる。

$$p \equiv p^2 - 6\chi(p+1) + 4p + 1 \pmod{r} \quad \dots \quad (\text{式 } 6)$$

[0040] この(式 6) は、次のように式変形できる。

$$6\chi(1+p) \equiv p^2 + 3p + 1 \pmod{r} \quad \dots \quad (\text{式 } 7)$$

[0041] ここで、既に知られている $p^4 - p^2 + 1 \equiv 0 \pmod{r}$ の関係式から、次の式が得られる。

$$p^2(1-p)(1+p) \equiv 1 \pmod{r} \quad \dots \text{(式 8)}$$

[0042] この(式 8)は、次のように式変形できる。

$$(1+p)^{-1} \equiv p^2(1-p) \pmod{r} \quad \dots \text{(式 9)}$$

[0043] (式 9)を用いるとともに、 $p^6 \equiv -1 \pmod{r}$ の関係式から、(式 7)は次のように式変形できる。

$$\begin{aligned} 6\chi &\equiv (1+p)^{-1}\{(1+p)^2+p\} \\ &\equiv 1+p+p^3+p^{10} \pmod{r} \quad \dots \text{(式 10)} \end{aligned}$$

[0044] 次に、A t e ペアリングの有理関数 $f_{t-1,Q}(\cdot)$ について考える。特に、(式 3)によって有理関数 $f_{t-1,Q}(\cdot)$ は次のように表すことができる。ここで、 $t-1 = T$ としている。

[数8]

$$f_{6\chi^2,Q} = f_{T,Q} \quad \dots \text{(式 1 1)}$$

[0045] ここで、 $Q \in G_2$ であり、 $\forall S \in G_1$ に対して、以下の式とする。

[数9]

$$f_{6\chi^2,Q}(S)^{(p^{12}-1)/r} = f_{T,Q}(S)^{(p^{12}-1)/r} = \alpha(Q,S) \quad \dots \text{(式 1 2)}$$

[0046] (式 1 0)を用いることにより次の式が得られる。

[数10]

$$f_{6\chi^2,Q} = f_{6\chi \cdot \chi,Q} = f_{(1+p+p^3+p^{10})\chi,Q} \quad \dots \text{(式 1 3)}$$

[0047] ここで、有理関数は、次の関係式を満たすこととなっている。

[数11]

$$f_{a+b,Q} = f_{a,Q} \cdot f_{b,Q} \cdot g_{aQ,bQ} \quad \dots \text{(式 1 4)}$$

[数12]

$$f_{ab,Q} = f_{b,Q}^a \cdot f_{a,bQ} = f_{a,Q}^b f_{b,aQ} \quad \dots \text{(式 1 5)}$$

[数13]

$$f_{p^i, Q} = f_{p, Q}^{ip^{i-1}} \quad \dots(\text{式 } 16)$$

[0048] したがって、(式13)は次のように式変形できる。

[数14]

$$f_{(1-p+p^3+p^{10}), Q} = f_{\chi, Q} \cdot f_{\chi, Q}^p \cdot g_{\chi Q, p\chi Q} \cdot f_{\chi, Q}^{p^3} \cdot f_{\chi, Q}^{p^{10}} \cdot g_{p^3\chi Q, p^{10}\chi Q} \\ g_{\chi Q + p\chi Q, p^3\chi Q + p^{10}\chi Q} \cdot f_{p, \chi Q}^{1+3p^2+10p^9} \quad \dots(\text{式 } 17)$$

[0049] なお、 $g_{aQ, bQ} = l_{aQ, bQ} / v_{aQ+bQ}$ であって、 $l_{aQ, bQ}$ は2つの有理点 aQ と bQ を通る直線の値、 v_{aQ+bQ} は有理点 $aQ + bQ$ の鉛直線の値である。組み込み次数が偶数の場合には、 v_{aQ+bQ} の計算は省略できる。

[0050] また、(式17)中の

[数15]

$$f_{p, \chi Q}^{1+3p^2+10p^9} \quad \dots(\text{式 } 18)$$

は、双線形性を有していることから、次のように式変形できる。

[数16]

$$f_{p, Q}^{\chi(1+3p^2+10p^9)} \quad \dots(\text{式 } 19)$$

[0051] したがって、(式3)と(式13)と(式19)を用いて(式17)を式変形することにより、次のようになる。

[数17]

$$f_{p, Q} \cdot \left\{ f_{p, Q}^{\chi(1+3p^2+10p^9)} \right\}^{-1} = f_{\chi, Q} \cdot f_{\chi, Q}^p \cdot g_{\chi Q, p\chi Q} \cdot f_{\chi, Q}^{p^3} \cdot f_{\chi, Q}^{p^{10}} \cdot g_{p^3\chi Q, p^{10}\chi Q} \cdot g_{\chi Q + p\chi Q, p^3\chi Q + p^{10}\chi Q} \quad \dots(\text{式 } 20)$$

[0052] ここで、本発明者らは、(式20)の左辺が双線形性を有していることから、(式20)の右辺も双線形性を有していることに思い至り、この(式20)の右辺を新たな有理関数を $f'_{\chi, Q}(\cdot)$ とすることとした。

[0053] すなわち、次の式によりペアリング $e(Q, S)$ の演算を行うこととするものである。

[数18]

$$e(Q, S) = f'_{\chi, Q}(S)^{(p^{12}-1)/r}$$

本発明者らは、このペアリング $e(Q, S)$ を X a t e ペアリングと呼んでいる。

[0054] さらに、(式20)の右辺は、次のように式変形できる。

[数19]

$$f_{\chi, Q}^{1+p+p^3+p^{10}} \cdot g_{\chi Q, p^{10}\chi Q} \cdot g_{p\chi Q, p^3\chi Q} \cdot g_{\chi Q+p^{10}\chi Q, p\chi Q+p^3\chi Q} \dots (\text{式21})$$

[0055] すなわち、組み込み次数 $k=12$ の場合には、有理点 $(\chi Q, p^{10}\chi Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_1 と、有理点 $(\chi Q + p^{10}\chi Q, p\chi Q + p^3\chi Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_2 と、有理点 $(p\chi Q, p^3\chi Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_3 をそれぞれ演算して特定しておくことにより、次の式に基づいてミラーのアルゴリズムを用いた演算を高速化できる。

[数4]

$$f'_{\chi, Q}(S) = f_{\chi, Q}(S)^{1+p+p^3+p^{10}} \cdot l_1 \cdot l_2 \cdot l_3$$

[0056] しかも、(式20)の右辺は、次のように式変形できるので、 $f'_{\chi, Q}(S)$ の演算をより高速化できる。

[数20]

$$\left\{ f_{\chi, Q}^{1+p^{10}} \cdot g_{\chi Q, p^{10}\chi Q} \right\}^{1+p^3} \cdot g_{\chi Q+p^{10}\chi Q, p\chi Q+p^3\chi Q} \dots (\text{式22})$$

[0057] 以上のように、X a t e ペアリングを用いることによって、ペアリング演算を行う場合には、有理関数 $f_{\chi, Q}(S)$ と、所定の有理点を通る直線の値を用いて得られた新たな有理関数 $f'_{\chi, Q}(S)$ を用いて演算でき、特に、特に有理関数 $f'_{\chi, Q}(S)$ が、 $t-1$ よりもサイズの小さい χ を用いて演算できることによって、ペアリング演算を高速化できる。

[0058] ここまでは、組み込み回数 $k=12$ の場合について説明してきたが、組み込み回数 $k=8, 10, 18$ の場合にも基本的に同様であるので詳細な説明は省略する。

[0059] 以下において、組み込み回数 $k=12$ の場合の実施形態について詳説する。なお、本実施形態では、デジタルグループ署名を想定しており、所要の電子計算機で構成された認証サーバをペアリング演算装置としている。ただし、ペアリング演算装置は、認証サーバで構成する場合に限定されるものではなく、少なくともCPUなどの演算手段を備えてペアリング演算が実行可能となった装置であれば、どのような装置であってもよい。

[0060] 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。

[0061] また、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1中、15は電子計算機10の入出力制御部である。

[0062] 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に一旦記憶する。次いで、電子計算機10では、ペアリング演算プログラムを実行することによりペアリング演算を行っている。

[0063] すなわち、電子計算機10では、ペアリング演算プログラムの実行にともなって、図2に示すフローチャートに基づいてペアリング演算を行い、デジタルグループ署名を実現している。なお、デジタルグループ署名における認証処理については詳説せず、認証処理におけるサブルーチン処理としての

ペアリング演算についてのみ詳説する。

- [0064] ペアリング演算プログラムによって、電子計算機10では、図2に示すようにステップS1として、CPU11を入力手段として機能させて、必要なデータの入力を行っている。すなわち、電子計算機10では、メモリ装置13にあらかじめ記憶している整数変数 χ のデータと有理点QのデータをCPU11の内部に設けている所定のレジスタに入力し、さらに、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SのデータをCPU11の内部に設けている所定のレジスタに入力している。
- [0065] 次に、ペアリング演算プログラムによって、電子計算機10では、ステップS2として、CPU11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る有理関数 $f_{\chi,Q}(S)$ の演算を行っている。
- [0066] この有理関数 $f_{\chi,Q}(S)$ の演算は、具体的には図3のフローチャート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 $f_{\chi,Q}(S)$ の演算とともに χQ の演算を行い、 χQ の演算結果をCPU11の内部に設けている所定のレジスタの記憶している。
- [0067] すなわち、図3のフローチャートに基づいて、電子計算機10は、ステップS21として、初期設定を行っている。すなわち、電子計算機10では、 $f \leftarrow 1$ 、 $T \leftarrow Q$ とする処理を行い、さらに $i \leftarrow \lceil \log_2(\chi) \rceil$ として、整数変数 χ を2進数表示とした場合のビット数を i としている。
- [0068] 次に、図3のフローチャートに基づいて、電子計算機10は、ステップS22として、有理関数 $f_{\chi,Q}(S)$ 部分の所定の演算を行っている。
- [0069] 次に、図3のフローチャートに基づいて、電子計算機10は、ステップS23として、 χQ 部分の所定の演算を行っている。
- [0070] 次に、図3のフローチャートに基づいて、電子計算機10は、ステップS24として、整数変数 χ の i 番目のビットの値 u_i が「1」であるか「0」であるかを判定している。
- [0071] $u_i = 1$ の場合には、図3のフローチャートに基づいて、電子計算機10は、ステップS25として、有理関数 $f_{\chi,Q}(S)$ 部分の所定の演算を行い、さらに、

ステップS 2 6として、 χQ 部分の所定の演算を行っている。

[0072] 次いで、図3のフローチャートに基づいて、電子計算機10は、ステップS 2 7として、終了判定を行っている。

[0073] ステップS 2 7において $i \neq 1$ の場合には、図3のフローチャートに基づいて、電子計算機10は、ステップS 2 8として、 i のデクリメントを行ってステップS 2 2に戻り、ステップS 2 7において $i = 1$ となるまで有理関数 $f_{\chi, Q}(S)$ 及び χQ の演算を繰り返し行っている。

[0074] ステップS 2 7において $i = 1$ の場合には、電子計算機10は、有理関数 $f_{\chi, Q}(S)$ の演算結果、及び χQ の演算結果をそれぞれ所定のレジスタに記憶して、図3のフローチャートに基づくサブルーチンを終了している。

[0075] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップS 3として、CPU11を第2演算手段として機能させて、有理点 $p^{10}\chi Q$ 、 $\chi Q + p^{10}\chi Q$ 、 $p\chi Q + p^3\chi Q$ をそれぞれ演算している。

[0076] 特に、第2演算手段では、ステップS 2において所定のレジスタに記憶された $\chi Q = R$ とし、この R のフロベニウス自己準同型写像 ϕ_p が $\phi_p(R) = pR$ である関係を用いて、各有理点 $p^{10}\chi Q = p^{10}R$ 、 $\chi Q + p^{10}\chi Q = R + p^{10}R$ 、 $p\chi Q + p^3\chi Q = pR + p^3R$ として演算を行っている。

[0077] 具体的には、 $T = \chi Q = R$ であって、 $X = p^{10}R$ 、 $Y = R + p^{10}R$ 、 $Z = pR + p^3R$ とし、電子計算機10では、次のように演算している。

$$X \leftarrow \phi_p^{10}(T),$$

$$Y \leftarrow T + X,$$

$$Z \leftarrow \phi_p^3(Y).$$

[0078] したがって、ステップS 3において、電子計算機10は、乗算処理をすることなく演算を実行できるので、演算を高速化することができる。

[0079] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップS 4として、CPU11を第3演算手段として機能させて、有理点 $(\chi Q, p^{10}\chi Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_1 と、有理点 $(\chi Q + p^{10}\chi Q, p\chi Q + p^3\chi Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_2 をそれぞれ演算

している。

[0080] 具体的には、電子計算機10では、 $l_1 = l_{T,X}(S)$ を次のように演算している。

$$\lambda_{T,X} \leftarrow (y_X - y_T) / (x_X - x_T),$$

$$l_{T,X}(S) \leftarrow (x_S - x_X) \lambda_{T,X} - (y_S - y_X).$$

[0081] また、電子計算機10では、 $l_2 = l_{Y,Z}(S)$ を次のように演算している。

$$\lambda_{Y,Z} \leftarrow (y_Z - y_Y) / (x_Z - x_Y),$$

$$l_{Y,Z}(S) \leftarrow (x_S - x_Z) \lambda_{Y,Z} - (y_S - y_Z).$$

[0082] 次に、ペアリング演算プログラムによって、電子計算機10では、ステップS5として、CPU11を第4演算手段として機能させて、第1演算手段での演算結果と、第3演算手段での演算結果と、有理点 $(p \cdot X, p^3 \cdot X)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_3 を用いて、次のように有理関数 $f'_{X,Q}(S)$ を演算している。

[数4]

$$f'_{X,Q}(S) = f_{X,Q}(S)^{1+p+p^3+p^{10}} \cdot l_1 \cdot l_2 \cdot l_3$$

[0083] 特に、この場合に、電子計算機10では、有理関数 $f_{X,Q}(S)$ のフロベニウス自己準同型写像 ϕ_p が、 $\phi_p(f_{X,Q}(S)) = f_{X,Q}(S)^p$ であって、 $\phi_{p^{10}}(f_{X,Q}(S)) = f_{X,Q}(S)^{p^{10}}$ （ここで、 p^{10} は p^{10} であることを表している）を用いて

[数5]

$$f_{X,Q}(S)^{1+p^{10}} \cdot l_1$$

を演算している。

[0084] さらに、電子計算機10では、 $Q_1, Q_2 \in G_2$ である有理点 (Q_1, Q_2) を通る直線における有理点 $S(x_s, y_s)$ の値 l のフロベニウス自己準同型写像 ϕ_p が、有理点 $(p \cdot Q_1, p \cdot Q_2)$ を通る直線における有理点 $S(x_s, y_s)$ の値であることを用いて

[数6]

$$f_{X,Q}(S)^{p+p^3} \cdot l_3 = \phi_p^3(f_{X,Q}(S)^{1+p^{10}} \cdot l_1)$$

となる

[数7]

$$f_{\chi, Q}(S)^{p+p^3} \cdot l_3$$

を演算して有理関数 $f'_{\chi, Q}(S)$ を演算している。

[0085] 具体的には、電子計算機10は、次のように演算を行っている。ここで、 $p^{\wedge}3$ は p^3 であることを表している。

1. $C \leftarrow f \cdot p^{\wedge}10$
2. $C \leftarrow C \cdot f$
3. $A \leftarrow C \cdot l_{T, X}(S)$
4. $B \leftarrow A \cdot p^{\wedge}3$
5. return A, B

[0086] したがって、

[数4]

$$f'_{\chi, Q}(S) = f_{\chi, Q}(S)^{1+p+p^3+p^{10}} \cdot l_1 \cdot l_2 \cdot l_3$$

は、

$$f' \leftarrow A \cdot B \cdot l_{Y, Z}(S)$$

として演算できる。

[0087] このように、X a t eペアリングを用いることによって演算量を大きく削減することができ、ペアリング演算を高速化できる。

[0088] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップS6として、CPU11を第5演算手段として機能させて、ペアリング $e(Q, S)$ における最終べきのべき乗算を行っている。

[0089] 具体的には、電子計算機10は、次のように演算を行っている。

1. $f' \leftarrow f' \cdot p^{\wedge}6 \cdot f'^{-1}$
2. $f' \leftarrow f' \cdot p^{\wedge}2 \cdot f'$
3. $a \leftarrow (f'^6)^X \cdot (f'^5)^{p^{\wedge}6}$

4. $b \leftarrow a^p$
5. $b \leftarrow a \cdot b$
6. compute $f'^p, f'^{p^2}, \text{ and } f'^{p^3}$
7. $c \leftarrow b \cdot (f'^p)^2 \cdot f'^{p^2}$
8. $f' \leftarrow f'^{p^3} \cdot (c^6)^{x^2} \cdot c \cdot b \cdot (f'^p \cdot f')^9 \cdot a \cdot f'^4$
9. Return f'

[0090] 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。

[0091] 本実施形態では、組み込み次数 $k=12$ の場合について説明したが、例えば組み込み次数 $k=10$ の場合でも、同様に演算できる。

[0092] なお、組み込み次数 $k=10$ の場合には、曲線の式が $y^2 = x^3 + ax + b$, $a \in F_p$, $b \in F_p$ で与えられ、埋込み次数が10で、 $F_{p^{10}}$ 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_p をフロベニウス自己準同型写像として、

$$G_1 = E[r] \cap \text{Ker}(\phi_p - [1]),$$

$$G_2 = E[r] \cap \text{Ker}(\phi_p - [p])$$

により、

$$e : G_2 \times G_1 \rightarrow F_p^{*10} / (F_p^{*10})^r$$

である非退化な双線形写像としてペアリング e を定義している。

[0093] この場合、位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t は、整数変数 χ を用いて次のように表せる。

$$r(\chi) = 25\chi^4 + 25\chi^3 + 15\chi^2 + 5\chi + 1,$$

$$t(\chi) = 10\chi^2 + 5\chi + 3.$$

[0094] また、整数変数 χ の標数 p による p 進数展開は次のように表される。

$$5\chi = p^4 + p^5 + p^7 + p^8 = p^4(1 + p + p^3 + p^4) \pmod{r(\chi)}.$$

[0095] そして、有理点 $(\chi \mathbb{Q}, p\chi \mathbb{Q})$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_4 と、有理点 $(\chi \mathbb{Q} + p\chi \mathbb{Q}, p^3\chi \mathbb{Q} + p^4\chi \mathbb{Q})$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_5 をそれぞれ演算し、さらに、有理点 $(p^3\chi \mathbb{Q}, p^4\chi \mathbb{Q})$ を通る直線

における有理点 $S(x_s, y_s)$ の値 l_6 を用いることにより、有理関数 $f'_{\chi, Q}(S)$ を次の式により演算している。

[数21]

$$f'_{\chi, Q}(S) = \phi_p^4(f_{\chi, Q}(S))^{1+p+p^3+p^4} \cdot l_4 \cdot l_5 \cdot l_6$$

[0096] 埋め込み次数 $k=12$ の場合と同様に、埋め込み次数 $k=10$ の場合でも、認証サーバでは、ペアリング演算プログラムを実行することにより、図4に示すフローチャートに基づいてペアリング演算を行っている。

[0097] ペアリング演算プログラムによって、電子計算機10では、図4に示すようにステップT1として、CPU11を入力手段として機能させて、必要なデータの入力を行っている。すなわち、電子計算機10では、メモリ装置13にあらかじめ記憶している整数変数 χ のデータと有理点 Q のデータをCPU11の内部に設けている所定のレジスタに入力し、さらに、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 S のデータをCPU11の内部に設けている所定のレジスタに入力している。

[0098] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップT2として、CPU11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る有理関数 $f_{\chi, Q}(S)$ の演算を行っている。

[0099] なお、このステップT2では、図3に示したフローチャートのステップS22における1番目の式を、次のようにしている。

$$1. \quad \lambda_{T,1} \leftarrow (3x_T^2 + a) / (2y_T)$$

[0100] ここで、「 a 」は、 $y^2 = x^3 + ax + b$, $a \in F_p$, $b \in F_p$ で与えられた楕円曲線における1次の係数であり、この1番目の式以外は、図3に示したフローチャートと同様に有理関数 $f_{\chi, Q}(S)$ の演算を行っている。

[0101] また、電子計算機10は、ステップT2でも、有理関数 $f_{\chi, Q}(S)$ とともに χQ を演算して、演算結果を所定のレジスタに記憶している。

[0102] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップT3として、CPU11を第2演算手段として機能させて、有理点 $p\chi Q$ 、

$\chi Q + p \chi Q$ 、 $p^3 \chi Q + p^4 \chi Q$ をそれぞれ演算している。

- [0103] 特に、第2演算手段では、ステップT2において所定のレジスタに記憶された $\chi Q = R$ とし、このRのフロベニウス自己準同型写像 ϕ_p が $\phi_p(R) = pR$ である関係を用いて、各有理点 $p \chi Q = pR$ 、 $\chi Q + p \chi Q = R + pR$ 、 $p^3 \chi Q + p^4 \chi Q = p^3R + p^4R$ として演算を行っている。

- [0104] 具体的には、 $T = \chi Q = R$ であって、 $X = pR$ 、 $Y = R + pR$ 、 $Z = p^3R + p^4R$ とし、電子計算機10では、次のように演算している。

$$X \leftarrow \phi_p(T),$$

$$Y \leftarrow T + X,$$

$$Z \leftarrow \phi_p^3(Y).$$

- [0105] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップT4として、CPU11を第3演算手段として機能させて、有理点 $(\chi Q, p \chi Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_4 と、有理点 $(\chi Q + p \chi Q, p^3 \chi Q + p^4 \chi Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_5 をそれぞれ演算している。

- [0106] 具体的には、電子計算機10では、 $l_4 = l_{T,X}(S)$ を次のように演算している。

$$\lambda_{T,X} \leftarrow (y_X - y_T) / (x_X - x_T),$$

$$l_{T,X}(S) \leftarrow (x_S - x_X) \lambda_{T,X} - (y_S - y_X).$$

- [0107] また、電子計算機10では、 $l_5 = l_{Y,Z}(S)$ を次のように演算している。

$$\lambda_{Y,Z} \leftarrow (y_Z - y_Y) / (x_Z - x_Y),$$

$$l_{Y,Z}(S) \leftarrow (x_S - x_Z) \lambda_{Y,Z} - (y_S - y_Z).$$

- [0108] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップT5として、CPU11を第4演算手段として機能させて、第1演算手段での演算結果と、第3演算手段での演算結果と、有理点 $(p^3 \chi Q, p^4 \chi Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_6 を用いて、次のように有理関数 $f'_{\chi,Q}(S)$ を演算している。

[数21]

$$f'_{\chi,Q}(S) = \phi_p^4(f_{\chi,Q}(S)^{1+p+p^3+p^4} \cdot l_4 \cdot l_5 \cdot l_6)$$

[0109] 特に、この場合に、電子計算機10では、有理関数 $f_{\chi,Q}(S)$ のフロベニウス自己準同型写像 ϕ_p が、 $\phi_p(f_{\chi,Q}(S)) = f_{\chi,Q}(S)^p$ であることを用いて

[数22]

$$f_{\chi,Q}(S)^{1+p} \cdot l_4$$

を演算している。

[0110] さらに、電子計算機10では、 $Q_1, Q_2 \in G_2$ である有理点 (Q_1, Q_2) を通る直線における有理点 $S(x_s, y_s)$ の値 l のフロベニウス自己準同型写像 ϕ_p が、有理点 (pQ_1, pQ_2) を通る直線における有理点 $S(x_s, y_s)$ の値であることを用いて

[数23]

$$f_{\chi,Q}(S)^{p^3+p^4} \cdot l_6 = \phi_p^3(f_{\chi,Q}(S)^{1+p} \cdot l_4)$$

となる

[数24]

$$f_{\chi,Q}(S)^{p^3+p^4} \cdot l_6$$

を演算して有理関数 $f'_{\chi,Q}(S)$ を演算している。

[0111] 具体的には、電子計算機10は、次のように演算を行っている。ここで、 $p^{\frown}3$ は p^3 であることを表している。

1. $C \leftarrow f^p$
2. $C \leftarrow C \cdot f$
3. $A \leftarrow C \cdot l_{T,\chi}(S)$
4. $B \leftarrow A^{p^{\frown}3}$
5. return A, B

[0112] さらに、電子計算機10は、

$$1. \quad f' \leftarrow A \cdot B \cdot l_{\chi, Z}(S)$$

$$2. \quad f' \leftarrow f'^{p^4}$$

として演算することにより、

[数21]

$$f'_{\chi, Q}(S) = \phi_p^4(f_{\chi, Q}(S)^{1+p+p^3+p^4} \cdot l_4 \cdot l_5 \cdot l_6)$$

を演算している。

[0113] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップ6として、CPU11を第5演算手段として機能させて、ペアリング $e(Q, S)$ における最終べきのべき乗算を行っている。

[0114] 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。

[0115] また、組み込み次数 $k=10$ の場合には、ミラーのアルゴリズムを用いて計算される有理関数を $f_{\chi^2, Q}(S)$ (χ^2 は χ^2 であることを示す)としてペアリング $e(Q, S)$ を演算することもできる。

[0116] この場合、位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t は、整数変数 χ を用いて次のように表せる。

$$r(\chi) = \chi^8 - 1,$$

$$t(\chi) = -\chi^6 + \chi^4 - \chi^2 + 2.$$

[0117] また、整数変数 χ の標数 p による p 進数展開は次のように表される。

$$p\chi^2 = -p \pmod{r(\chi)}.$$

[0118] そして、電子計算機10では、有理関数 $f'_{\chi, Q}(S)$ を次の式により演算している。

[数25]

$$f'_{\chi, Q}(S) = f_{\chi^2, Q}(S)^p$$

[0119] したがって、ペアリング演算プログラムによって、電子計算機10では、ペアリング $e(Q, S)$ を

[数26]

$$e(Q, S) = f'_{\chi, Q}(S)^{(p^{10}-1)/r}$$

として演算することができる。

- [0120] また、組み込み次数 $k=8$ の場合には、曲線の式が $y^2 = x^3 + ax$, $a \in F_p$ で与えられ、 F_{p^8} 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_p をフロベニウス自己準同型写像として、

$$G_1 = E[r] \cap \text{Ker}(\phi_p - [1]),$$

$$G_2 = E[r] \cap \text{Ker}(\phi_p - [p])$$

により、

$$e : G_2 \times G_1 \rightarrow F_{p^8}^* / (F_{p^8}^*)^r$$

である非退化な双線形写像としてペアリング e を定義している。

- [0121] この場合、位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t は、整数変数 χ を用いて次のように表せる。

$$r(\chi) = 9\chi^4 + 12\chi^3 + 8\chi^2 + 4\chi + 1,$$

$$t(\chi) = -9\chi^3 - 3\chi^2 - 2\chi.$$

- [0122] また、整数変数 χ の標数 p による p 進数展開は次のように表される。

$$3\chi = -1 - p^2 + p^3 \pmod{r(\chi)}.$$

- [0123] そして、有理点 $(\chi Q, \chi Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_7 と、有理点 $(2\chi Q, \chi Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_8 と、有理点 $(p^2 Q, (3\chi + 1)Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_9 と、有理点 $(3\chi Q, Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_{10} を用いることにより、電子計算機10では、有理関数 $f'_{\chi, Q}(S)$ を次の式により演算している。

[数27]

$$f'_{\chi, Q}(S) = f_{\chi, Q}(S)^3 \cdot l_7 \cdot l_8 \cdot l_9 \cdot l_{10}$$

- [0124] すなわち、ペアリング演算プログラムによって、電子計算機10では、上述

したようにミラーのアルゴリズムによる有理関数 $f_{\chi,Q}(S)$ の演算を行い、有理関数 $f_{\chi,Q}(S)$ とともに χQ を演算して、演算結果を所定のレジスタに記憶している。

- [0125] 次いで、電子計算機10では、所定のレジスタに記憶された $\chi Q = R$ とし、この R のフロベニウス自己準同型写像 ϕ_p が $\phi_p(R) = pR$ である関係を用いて、各有理点 $2\chi Q$ 、 $p^2\chi$ 、 $3\chi Q$ 、 $(3\chi + 1)Q$ を演算して、この演算結果を用いて各値 l_7 、 l_8 、 l_9 、 l_{10} を演算し、有理関数 $f'_{\chi,Q}(S)$ を演算している。

- [0126] そして、電子計算機10では、ペアリング $e(Q, S)$ を
[数28]

$$e(Q, S) = f'_{\chi,Q}(S)^{(p^8-1)/r}$$

として演算することができる。

- [0127] なお、組み込み次数 $k=8$ の場合には、位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t を、整数変数 χ を用いて次のように表すこともできる。

$$r(\chi) = \chi^4 - 8\chi^2 + 25,$$

$$t(\chi) = (2\chi^3 - 11\chi + 15) / 15.$$

- [0128] この場合、整数変数 χ の標数 p による p 進数展開は次のように表される。

$$\chi = -p + 2p^3 \pmod{r(\chi)}.$$

- [0129] この場合には、有理点 $(pQ, \chi Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_{11} を用いて有理関数 $f'_{\chi,Q}(S)$ を次の式により演算することもできる。

[数29]

$$f'_{\chi,Q}(S) = f_{\chi,Q}(S) \cdot l_{11}$$

- [0130] あるいは、組み込み次数 $k=8$ の場合において、ミラーのアルゴリズムを用いて計算される有理関数を $f_{\chi^2,Q}(S)$ (χ^2 は χ^2 であることを示す) 及び $f_{\chi,Q}(S)$ としてペアリング $e(Q, S)$ を演算することもできる。

- [0131] このとき、位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t は、整数変数 χ を用いて次のように表すことができる。

$$r(\chi) = \chi^8 - \chi^4 + 1,$$

$$t(\chi) = \chi^5 - \chi + 1.$$

[0132] この場合、整数変数 χ の標数 p による p 進数展開は次のように表される。

$$p\chi + \chi^2 = -p^2 \pmod{r(\chi)}$$

[0133] この場合には、有理点 $(\chi^2 Q, p\chi Q)$ を通る直線における有理点 $S(x_s, y_s)$ の値 l_{12} を用いて有理関数 $f'_{\chi, Q}(S)$ を次の式により演算することができる。

[数30]

$$f'_{\chi, Q}(S) = f_{\chi^2, Q}(S) \cdot f_{\chi, Q}(S)^p \cdot l_{12}$$

[0134] ここで、電子計算機10では、上述したようにミラーのアルゴリズムによる有理関数 $f_{\chi^2, Q}(S)$ 及び有理関数 $f_{\chi, Q}(S)$ の演算を行うとともに χQ を演算して、演算結果を所定のレジスタに記憶している。

[0135] そして、電子計算機10では、所定のレジスタに記憶された $\chi Q = R$ とし、この R のフロベニウス自己準同型写像 ϕ_p が $\phi_p(R) = pR$ である関係を用いて、有理点 $p\chi Q$ を演算して、この演算結果を用いて前記の値 l_{12} を演算し、有理関数 $f'_{\chi, Q}(S)$ を演算し、ペアリング $e(Q, S)$ を

[数28]

$$e(Q, S) = f'_{\chi, Q}(S)^{(p^8 - 1)/r}$$

として演算することができる。

[0136] また、組み込み次数 $k=18$ の場合には、曲線の式が $y^2 = x^3 + b$, $b \in F_p$ で与えられ、 $F_{p^{18}}$ 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_p をフロベニウス自己準同型写像として、

$$G_1 = E[r] \cap \text{Ker}(\phi_p - [1]),$$

$$G_2 = E[r] \cap \text{Ker}(\phi_p - [p])$$

により、

$$e : G_2 \times G_1 \rightarrow F_{p^{18}}^* / (F_{p^{18}}^*)^r$$

である非退化な双線形写像としてペアリング e を定義している。

[0137] この場合、位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t は、整数変数 χ を用いて次のように表せる。

$$r(\chi) = (\chi^6 + 37\chi^3 + 343) / 343,$$

$$t(\chi) = (\chi^4 + 16\chi + 7) / 7.$$

[0138] この場合、整数変数 χ の標数 p による p 進数展開は次のように表される。

$$\chi = -3p + p^4 \pmod{r(\chi)}.$$

[0139] そして、有理点 $(3pQ, \chi Q)$ を通る直線の有理点 $S(x_s, y_s)$ の値 l_{13} 、電子計算機10では、有理関数 $f'_{\chi,Q}(S)$ を次の式により演算している。

[数31]

$$f'_{\chi,Q}(S) = f_{\chi,Q}(S) \cdot l_{13}$$

[0140] すなわち、ペアリング演算プログラムによって、電子計算機10では、上述したようにミラーのアルゴリズムによる有理関数 $f_{\chi,Q}(S)$ の演算を行い、有理関数 $f_{\chi,Q}(S)$ とともに χQ を演算して、演算結果を所定のレジスタに記憶している。

[0141] 次に、電子計算機10では、有理関数 $f_{\chi,Q}(S)$ と χQ の演算結果を用いて前記の値 l_{13} を演算し、有理関数 $f'_{\chi,Q}(S)$ を演算して、ペアリング $e(Q, S)$ を

[数32]

$$e(Q, S) = f'_{\chi,Q}(S)^{(p^{18}-1)/r}$$

として演算することができる。

[0142] 以上のように、X a t e ペアリングによってペアリング演算を行うことにより、ペアリング演算を高速化でき、ペアリング演算を用いたグループ署名を実用化させることができる。

産業上の利用可能性

[0143] 本発明によれば、高速なペアリング演算装置を提供でき、実用性のあるデジタルグループ署名のサービスを提供できる。

請求の範囲

[請求項1]

曲線の式が $y^2 = x^3 + ax + b$, $a \in F_p$, $b \in F_p$ で与えられ、埋込み次数が 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_p をフロベニウス自己準同型写像として、

$$G_1 = E[r] \cap \text{Ker}(\phi_p - [1]),$$

$$G_2 = E[r] \cap \text{Ker}(\phi_p - [p])$$

により、

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

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、

$S \in G_1$ 、 $Q \in G_2$ としてペアリング $e(Q, S)$ を演算して演算結果を出力するペアリング演算装置であって、

フロベニウス自己準同型写像 ϕ_p のトレースを t として、ペアリング $e(Q, S)$ をミラーのアルゴリズムを用いて計算される有理関数 $f_{t-1, Q}(S)$ を用いて

[数2]

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

として演算する代わりに、

位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t を整数変数 χ の関数として、

有理関数 $f_{\chi, Q}(S)$ を演算する演算手段と、

所定の有理点を通る直線の有理点 $S(x_s, y_s)$ における値を演算する演算手段と、

これらの演算手段の演算結果を用いて有理関数 $f'_{\chi, Q}(S)$ を演算する演算手段と、

前記有理関数 $f'_{\chi, Q}(S)$ を用いて

[数3]

$$e(Q, S) = f'_{\chi, Q}(S)^{(p^k - 1)/r}$$

としてペアリング演算を行う演算手段と

によりペアリング演算を行うペアリング演算装置。

[請求項2]

前記有理関数 $f_{\chi, Q}(S)$ を演算する演算手段では、 χQ を演算して演算結果を所定のレジスタに記憶し、

前記 χQ の演算結果を用いて前記所定の有理点を演算する演算手段を有する請求項 1 に記載のペアリング演算装置。

[請求項3]

前記埋込み次数 $k = 12$ の場合に、

位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t を、前記整数変数 χ を用いて

$$r(\chi) = 36\chi^4 - 36\chi^3 + 18\chi^2 - 6\chi + 1,$$

$$t(\chi) = 6\chi^2 + 1$$

とし、 $\chi Q = R$ として、この R のフロベニウス自己準同型写像 ϕ_p が $\phi_p(R) = pR$ である関係を用いて、有理点 $p^{10}\chi Q$ 、 $\chi Q + p^{10}\chi Q$ 、 $p\chi Q + p^3\chi Q$ をそれぞれ演算し、

有理点 $(\chi Q, p^{10}\chi Q)$ を通る直線における前記有理点 $S(x_s, y_s)$ の値 l_1 と、有理点 $(\chi Q + p^{10}\chi Q, p\chi Q + p^3\chi Q)$ を通る直線における前記有理点 $S(x_s, y_s)$ の値 l_2 をそれぞれ演算し、

有理点 $(p\chi Q, p^3\chi Q)$ を通る直線における前記有理点 $S(x_s, y_s)$ の値 l_3 を用いて

[数4]

$$f'_{\chi, Q}(S) = f_{\chi, Q}(S)^{1+p+p^3+p^{10}} \cdot l_1 \cdot l_2 \cdot l_3$$

として前記有理関数 $f'_{\chi, Q}(S)$ を演算する請求項 2 に記載のペアリング演算装置。

[請求項4]

前記有理関数 $f_{\chi, Q}(S)$ のフロベニウス自己準同型写像 ϕ_p が $\phi_p(f_{\chi, Q}(S)) = p f_{\chi, Q}(S)$ である関係を用いて、

$S)) = f_{\chi, Q}(S)^p$ であることを用いて

[数5]

$$f_{\chi, Q}(S)^{1+p^{10}} \cdot l_1$$

を演算するとともに、

$Q_1, Q_2 \in G_2$ である有理点 (Q_1, Q_2) を通る直線における前記有理点 $S(x_s, y_s)$ の値 l のフロベニウス自己準同型写像 ϕ_p が有理点 (pQ_1, pQ_2) を通る直線における前記有理点 $S(x_s, y_s)$ の値であることを用いて

[数6]

$$f_{\chi, Q}(S)^{p+p^3} \cdot l_3 = \phi_p^3(f_{\chi, Q}(S)^{1+p^{10}} \cdot l_1)$$

となる

[数7]

$$f_{\chi, Q}(S)^{p+p^3} \cdot l_3$$

を演算して前記有理関数 $f'_{\chi, Q}(S)$ を演算する請求項3に記載のペアリング演算装置。

[請求項5]

曲線の式が $y^2 = x^3 + ax + b$, $a \in F_p$, $b \in F_p$ で与えられ、埋込み次数が 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_p をフロベニウス自己準同型写像として、

$$G_1 = E[r] \cap \text{Ker}(\phi_p - [1]),$$

$$G_2 = E[r] \cap \text{Ker}(\phi_p - [p])$$

により、

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

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、

$S \in G_1$ 、 $Q \in G_2$ としてCPUを備えた電子計算機でペアリング $e(Q, S)$ を演算するペアリング演算方法であって、

フロベニウス自己準同型写像 ϕ_p のトレースを t として、ペアリング $e(Q, S)$ をミラーのアルゴリズムを用いて計算される有理関数 $f_{t-1, Q}(S)$ を用いて

[数2]

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

として演算する代わりに、

位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t を整数変数 χ の関数として、

前記電子計算機のCPUを演算手段として機能させて、有理関数 $f_{\chi, Q}(S)$ を演算するステップと、

前記電子計算機のCPUを演算手段として機能させて、所定の有理点を通る直線の有理点 $S(x_s, y_s)$ における値を演算するステップと、

前記電子計算機のCPUを演算手段として機能させて、前記の演算結果を用いて有理関数 $f'_{\chi, Q}(S)$ を演算するステップと、

前記電子計算機のCPUを演算手段として機能させて、前記有理関数 $f'_{\chi, Q}(S)$ を用いて

[数3]

$$e(Q, S) = f'_{\chi, Q}(S)^{(p^k - 1)/r}$$

として演算するステップと

を有するペアリング演算方法。

[請求項6]

前記有理関数 $f_{\chi, Q}(S)$ を演算するステップの後、

前記電子計算機のCPUを演算手段として機能させて、 χQ を演算し、この χQ の演算結果を用いて前記所定の有理点を演算するステップを有する請求項5に記載のペアリング演算方法。

[請求項7]

曲線の式が $y^2 = x^3 + ax + b$, $a \in F_p$, $b \in F_p$ で与えられ、埋込み次数が 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_p をフロベニウス自己準同型写像として、

$$G_1 = E[r] \cap \text{Ker}(\phi_p - [1]),$$

$$G_2 = E[r] \cap \text{Ker}(\phi_p - [p])$$

により、

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

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、

$S \in G_1$ 、 $Q \in G_2$ として CPU を備えた電子計算機にペアリング $e(Q, S)$ を演算させるペアリング演算プログラムであって、

フロベニウス自己準同型写像 ϕ_p のトレースを t として、ペアリング $e(Q, S)$ をミラーのアルゴリズムを用いて計算される有理関数 $f_{t-1, Q}(S)$ を用いて

[数2]

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

として演算させる代わりに、

位数 r と、フロベニウス自己準同型写像 ϕ_p のトレース t を整数変数 χ の関数として、

前記電子計算機を、

有理関数 $f_{\chi, Q}(S)$ を演算する演算手段と、

所定の有理点を通る直線の有理点 $S(x_s, y_s)$ における値を演算する演算手段と、

前記の演算結果を用いて有理関数 $f'_{\chi, Q}(S)$ を演算する演算手段と

、

前記有理関数 $f'_{\chi, Q}(S)$ を用いて

[数3]

$$e(Q, S) = f'_{\chi, Q}(S)^{(p^k - 1)/r}$$

として演算する演算手段

として機能させるペアリング演算プログラム。

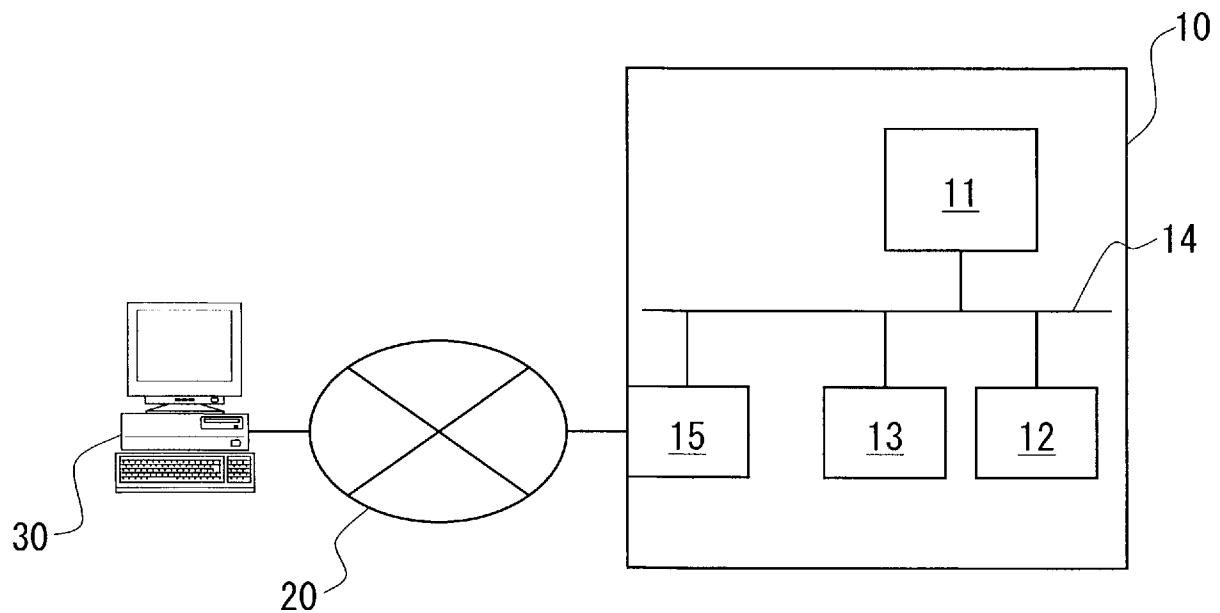
[請求項8]

前記電子計算機を、

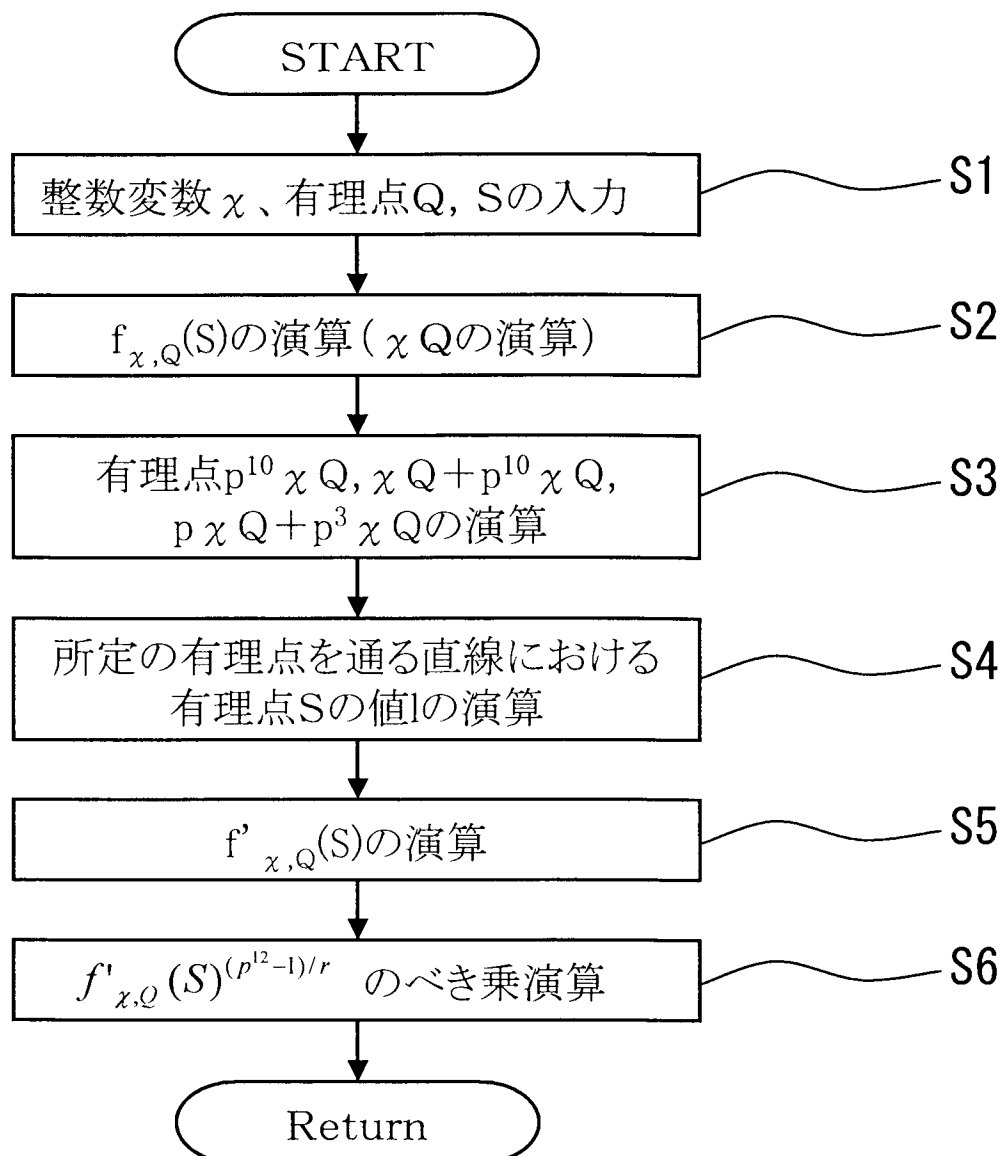
χ Qを演算する演算手段と、

この χ Qの演算結果を用いて前記所定の有理点を演算する演算手段
として機能させる請求項7に記載のペアリング演算プログラム。

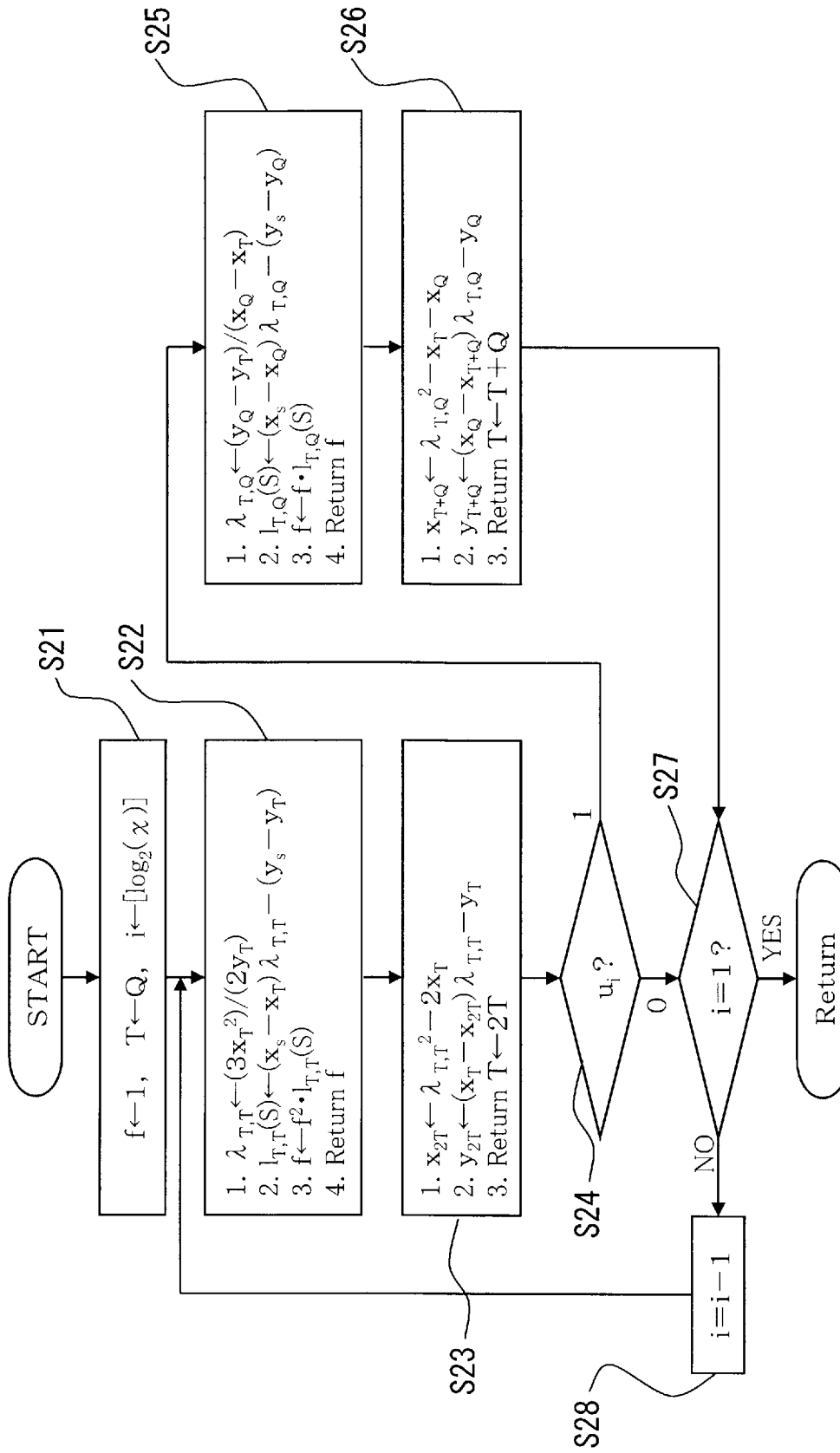
[図1]



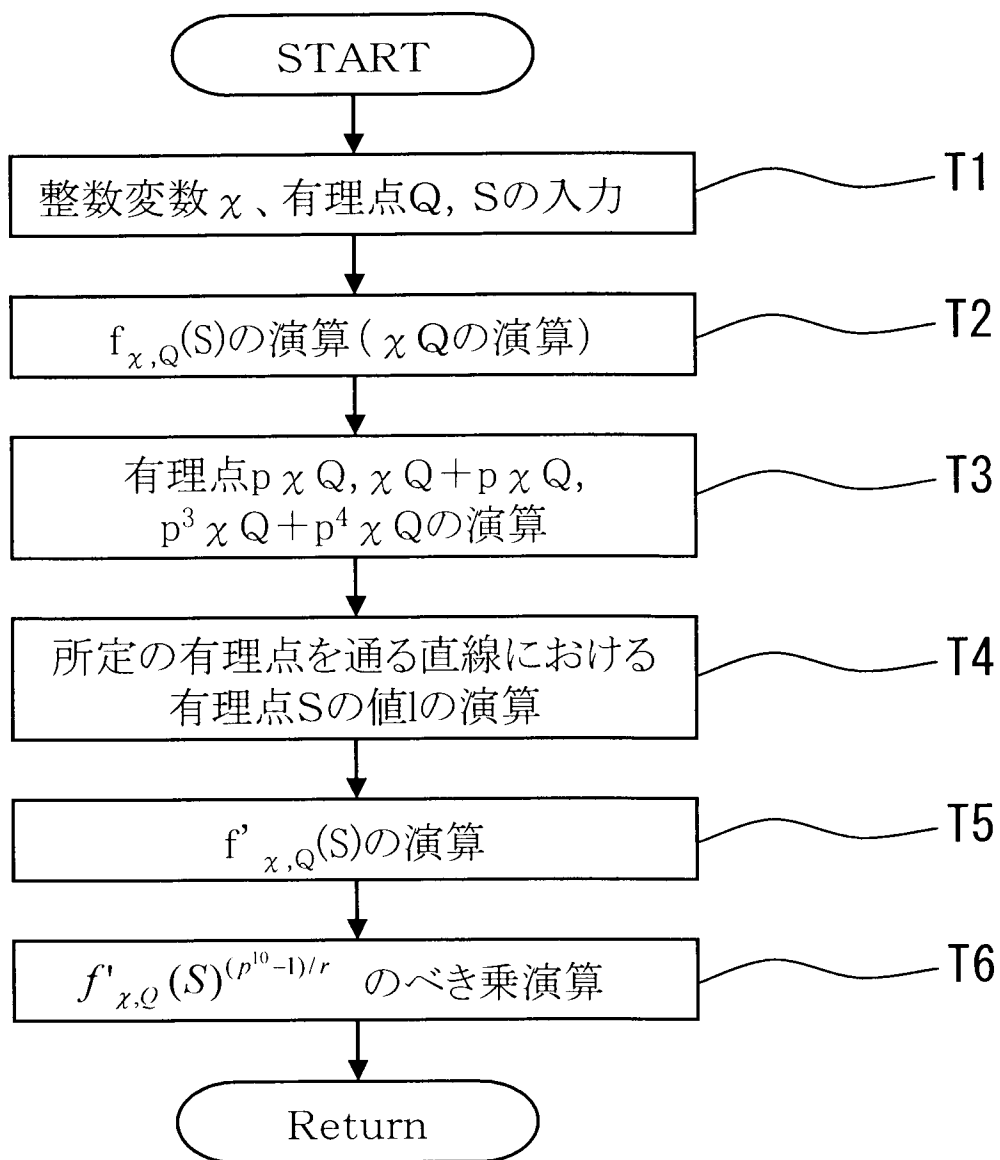
[図2]



[図3]



[図4]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/065099

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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Ezekiel Justin Kachisa et.al., Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field, Cryptology ePrint Archive, 2007, p.1-12	1-8
A	Paulo S. L. M. Barreto et.al., Pairing-Friendly Elliptic Curves of Prime Order, Proceedings of SAC 2005, 2005, p.1-13	1-8
A	SAKAMI et al., "Hamming Omomi no Chiisai Seisu Hensu o Parameter Settei ni Mochiita Twisted Ate Pairing no Kairyo", 2008 Nen Symposium on Cryptography and Information Security, 2008.01, pages 1 to 6	1-8

☐ 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
15 September, 2009 (15.09.09)

Date of mailing of the international search report
06 October, 2009 (06.10.09)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））

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（I P C））

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

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
A	Ezekiel Justin Kachisa et.al., Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field, Cryptology ePrint Archive, 2007, p.1-12	1-8
A	Paulo S. L. M. Barreto et.al., Pairing-Friendly Elliptic Curves of Prime Order, Proceedings of SAC 2005, 2005, p.1-13	1-8

☒ 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 5 . 0 9 . 2 0 0 9

国際調査報告の発送日

0 6 . 1 0 . 2 0 0 9

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）

鳥居 稔

5 S

3 8 5 7

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

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 請求項の番号
A	酒見他，ハミング重みの小さい整数変数をパラメータ設定に用いた Twisted Ate ペアリングの改良，2008年暗号と情報セキュリティシンポジウム予稿集，2008.01，p.1-6	1-8