(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 6 月 3 日(03.06.2010)

PCT

(10) 国際公開番号
WO 2010/061951 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2009/070127

(22) 国際出願日: 2009 年 11 月 30 日(30.11.2009)

(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 2008-305121 2008 年 11 月 28 日(28.11.2008) 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). 酒見 由美 (SAKEMI, Yumi) [JP/JP]; 〒7008530 岡山県岡山市北区津島中三丁目１番１号 国立大学法人岡山大学大学院自然科学研究科内 Okayama (JP). 森川 良孝 (MORIKAWA, Yoshitaka) [JP/JP]; 〒7008530 岡山県岡山市北区津島中三丁目１番１号 国立大学法人岡山大学大学院自然科学研究科内 Okayama (JP).

(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).

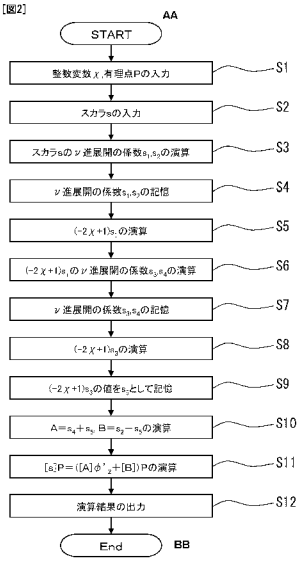
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, 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,

[続葉有]

(54) **Title**: SCALAR MULTIPLIER AND SCALAR MULTIPLICATION PROGRAM

(54) 発明の名称 : スカラ倍算器及びスカラ倍算プログラム

[図2]



AA START
S1 INPUT INTEGER VARIABLE χ AND RATIONAL POINT P
S2 INPUT SCALAR s
S3 CALCULATE ν-ADIC EXPANSION COEFFICIENTS s_1,s_2 OF SCALAR s
S4 STORE ν-ADIC EXPANSION COEFFICIENTS s_1,s_2
S5 CALCULATE $(-2\chi+1)s_1$
S6 CALCULATE ν-ADIC EXPANSION COEFFICIENTS s_3,s_4 OF $(-2\chi+1)s_1$
S7 STORE ν-ADIC EXPANSION COEFFICIENTS s_3,s_4
S8 CALCULATE $(-2\chi+1)s_3$
S9 STORE VALUE $(-2\chi+1)s_3$ AS s_5
S10 CALCULATE $A=s_4+s_5$, $B=s_2-s_5$
S11 CALCULATE $[s]P=([A]\varphi'_2+[B])P$
S12 OUTPUT CALCULATION RESULT
BB END

(57) **Abstract**: Provided are a scalar multiplier which makes it possible to execute scalar multiplication at high speed, and a scalar multiplication program. When calculating a scalar multiplication [s]P of a rational point P of an additive group E (Fp) comprising rational points on an elliptical curve wherein a characteristic p, an order r, and a trace t of a Frobenius endomorphism map at an embedded degree k = 12 using an integer variable χ are provided as $p(\chi)=36\chi^4-36\chi^3+24\chi^2-6\chi+1$, $r(\chi)=36\chi^4-36\chi^3+18\chi^2-6\chi+1=p(\chi)+1-t(\chi)$, $t(\chi)=6\chi^2+1$, assuming that the twist degree d is 6 and a positive integer e is 2 where k=d×e, $[s]P=([A]\varphi'_2+[B])P$ is calculated using the Frobenius map φ'_2 where $[p^2]P=\varphi'_2(P)$.

(57) 要約: スカラ倍算を高速で実行できるスカラ倍算器、及びスカラ倍算プログラムを提供する。 整数変数χを用いて、埋め込み次数ｋ＝12における標数ｐ、位数ｒ、フロベニウス自己準同型写像のトレースｔが、 $p(\chi)=36\chi^4-36\chi^3+24\chi^2-6\chi+1$, $r(\chi)=36\chi^4-36\chi^3+18\chi^2-6\chi+1=p(\chi)+1-t(\chi)$, $t(\chi)=6\chi^2+1$, として与えられる楕円曲線の有理点が成す加法群Ｅ(F_p)の有理点Ｐのスカラ倍算[s]Ｐを演算する際に、ツイスト次数ｄを６とし、ｋ＝ｄ×ｅとなる正整数ｅを２として、 $[p^2]P=\varphi'_2(P)$ となるフロベニウス写像φ'_2を用いて、 $[s]P=([A]\varphi'_2+[B])P$ として演算する。

WO 2010/061951 A1

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, MK, MT, NL, 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).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ： スカラ倍算器及びスカラ倍算プログラム

技術分野

[0001] 本発明は、有理点Ｐのスカラ倍算[s]Ｐを行うスカラ倍算器及びスカラ倍算プログラムに関する。

背景技術

[0002] 従来、インターネットなどの電気通信回線を利用して、インターネットバンキングや行政機関への電子申請などのような各種のサービスが提供されてきている。

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

[0004] 昨今では、より多くの利用者を効率よく管理しやすくするために、ＩＤベース暗号やグループ署名を用いた認証システムが提案されている。

[0005] ＩＤベース暗号やグループ署名では、ペアリング演算とともに、所要のべき乗算やスカラ倍算が行われており、認証処理に要する時間をできるだけ短縮させるには、これらの演算を高速に実行することが求められていた。

[0006] そのため、べき乗算やスカラ倍算をバイナリ法やWindow法などを用いて高速化することが提案されていた。

[0007] さらに、スカラ倍算においては、写像を利用することにより演算回数を削減して高速化する手法が提案されていた(例えば、特許文献１、特許文献２参照。)。

特許文献1：特開２００４－２７１７９２号公報

特許文献2：特開２００７－４１４６１号公報

発明の開示

発明が解決しようとする課題

[0008] しかしながら、単に写像を利用して演算回数を削減するだけでは高速化が十分ではなく、特に、１万人を超えるような利用者を対象とした認証処理を数秒以内で完了させることが困難であったため、実用に耐えないおそれがあった。

[0009] 本発明者らはこのような現状に鑑み、スカラ倍算を高速化することにより実用性を向上させるべく研究開発を行って、本発明を成すに至ったものである。

課題を解決するための手段

[0010] 本発明のスカラ倍算器では、整数変数χを用いて、埋め込み次数ｋ＝12における標数ｐ、位数ｒ、フロベニウス自己準同型写像のトレースｔが、

$$p(\chi)=36\chi^4-36\chi^3+24\chi^2-6\chi+1,$$

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

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

として与えられる楕円曲線の有理点が成す加法群Ｅ(F_p)の有理点Ｐのスカラ倍算[s]Ｐを演算するスカラ倍算器であって、ツイスト次数ｄを６とし、ｋ＝ｄ×ｅとなる正整数ｅを２として、

$$[p^2]P=\phi'_2(P),$$

となるフロベニウス写像ϕ'_2を用い、

$$[6\chi^2-4\chi+1]P=[(-2\chi+1)p^2]P=[-2\chi+1]\phi'_2(P)$$

であることから、$6\chi^2-4\chi+1=\nu$として前記スカラｓをν進数展開することにより

$$s=s_1\nu+s_2,\ s_2<\nu,$$

とし、

$$s\equiv(-2\chi+1)s_1p^2+s_2 \mod r,$$

であることから、$(-2\chi+1)s_1$部分をν進数展開して、

$$s\equiv(s_3\nu+s_4)p^2+s_2\equiv s_5p^4+s_4p^2+s_2 \mod r,$$

とし、$p^4\equiv p^2-1 \mod r$であることから、

$$s\equiv(s_4+s_5)p^2+(s_2-s_5) \mod r,$$

であることを利用して、スカラ倍算[s]Ｐを、

$$[s]P=([s_4+s_5]\phi'_2+[s_2-s_5])P,$$

として演算すべく、前記スカラｓの値を記憶する記憶手段と、前記係数s_1, s_2, s_3, s_4, s_5をそれぞれ記憶する第１～５補助記憶手段とを設け、前記スカラｓをν進数展開して得られた値を前記第１補助記憶手段と前記第２補助記憶手段に記憶させ、$(-2\chi+1)s_1$をν進数展開して得られた値を前記第３補助記憶手段と前記第４補助記憶手段に記憶させ、$(-2\chi+1)s_3$の値を前記第５補助記憶手段に記憶させることとした。

[0011] また、本発明のスカラ倍算プログラムでは、整数変数χを用いて、埋め込み次数ｋ＝12における標数ｐ、位数ｒ、フロベニウス自己準同型写像のトレースｔが、

$$p(\chi)=36\chi^4-36\chi^3+24\chi^2-6\chi+1,$$

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

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

として与えられる楕円曲線の有理点が成す加法群Ｅ(F_p)の有理点Ｐのスカラ倍算[s]Ｐを、ＣＰＵを備えた電子計算機に演算させるスカラ倍算プログラムであって、ツイスト次数ｄを６とし、ｋ＝ｄ×ｅとなる正整数ｅを２として、

$$[p^2]P=\phi'_2(P),$$

となるフロベニウス写像ϕ'_2を用い、

$$[6\chi^2-4\chi+1]P=[(-2\chi+1)p^2]P=[-2\chi+1]\phi'_2(P)$$

であることから、$6\chi^2-4\chi+1=\nu$として前記スカラｓをν進数展開することにより

$$s=s_1\nu+s_2,\ s_2<\nu,$$

とし、

$$s\equiv(-2\chi+1)s_1p^2+s_2 \mod r,$$

であることから、$(-2\chi+1)s_1$部分をν進数展開して、

$$s\equiv(s_3\nu+s_4)p^2+s_2\equiv s_5p^4+s_4p^2+s_2 \mod r,$$

とし、$p^4 \equiv p^2 - 1 \mod r$であることから、

$$s \equiv (s_4 + s_5)p^2 + (s_2 - s_5) \mod r,$$

であることを利用して、スカラ倍算[s]Ｐを、

$$[s]P = ([s_4 + s_5]\phi'_2 + [s_2 - s_5])P,$$

として前記電子計算機に演算させるべく、前記スカラｓをν進数展開して得られる前記s_1を第１のレジスタに格納させるとともに前記s_2を第２のレジスタに格納させるステップと、$(-2\chi + 1)s_1$をν進数展開して得られる前記s_3を第３のレジスタに格納させるとともに前記s_4を第４のレジスタに格納させるステップと、$(-2\chi + 1)s_3$の値を前記s_5の値として第５のレジスタに格納させるステップとを有することとした。

[0012] また、本発明のスカラ倍算器では、整数変数χを用いて、埋め込み次数ｋ＝8における標数ｐ、位数ｒ、フロベニウス自己準同型写像のトレースｔが、

$$p(\chi) = (81\chi^6 + 54\chi^5 + 45\chi^4 + 12\chi^3 + 13\chi^2 + 6\chi + 1)/4,$$

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

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

として与えられる楕円曲線の有理点が成す加法群Ｅ(F_p)の有理点Ｐのスカラ倍算[s]Ｐを演算するスカラ倍算器であって、

ツイスト次数ｄを４とし、ｋ＝ｄ×ｅとなる正整数ｅを２として、

$$[p^2]P = \phi'_2(P),$$

となるフロベニウス写像ϕ'_2を用い、

$$[3\chi^2 + 2\chi]P = [(-2\chi - 1)p^2]P = [-2\chi - 1]\phi'_2(P)$$

であることから、$3\chi^2 + 2\chi = \nu$として前記スカラｓをν進数展開することにより

$$s = s_1\nu + s_2,\ s_2 < \nu,$$

とし、

$$s \equiv (-2\chi - 1)s_1p^2 + s_2 \mod r,$$

であることから、$(-2\chi - 1)s_1$部分をν進数展開して、

$$s \equiv (s_3\nu + s_4)p^2 + s_2 \equiv s_5p^4 + s_4p^2 + s_2 \mod r,$$

とし、$p^4 \equiv -1 \mod r$であることから、

$$s \equiv s_4 p^2 + (s_2 - s_5) \mod r,$$

であることを利用して、スカラ倍算[s]Ｐを、

$$[s]P = ([s_4]\phi'_2 + [s_2 - s_5])P,$$

として演算すべく、前記スカラｓの値を記憶する記憶手段と、前記係数s_1, s_2, s_3, s_4, s_5をそれぞれ記憶する第１～５補助記憶手段とを設け、前記スカラｓをν進数展開して得られた値を前記第１補助記憶手段と前記第２補助記憶手段に記憶させ、$(-2\chi - 1)s_1$をν進数展開して得られた値を前記第３補助記憶手段と前記第４補助記憶手段に記憶させ、$(-2\chi - 1)s_3$の値を前記第５補助記憶手段に記憶させることとした。

[0013] また、本発明のスカラ倍算プログラムでは、整数変数χを用いて、埋め込み次数ｋ＝8における標数ｐ、位数ｒ、フロベニウス自己準同型写像のトレースｔが、

$$p(\chi) = (81\chi^6 + 54\chi^5 + 45\chi^4 + 12\chi^3 + 13\chi^2 + 6\chi + 1)/4,$$

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

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

として与えられる楕円曲線の有理点が成す加法群$E(F_p)$の有理点Ｐのスカラ倍算[s]Ｐを、ＣＰＵを備えた電子計算機に演算させるスカラ倍算プログラムであって、ツイスト次数ｄを４とし、ｋ＝ｄ×ｅとなる正整数ｅを２として、

$$[p^2]P = \phi'_2(P),$$

となるフロベニウス写像ϕ'_2を用い、

$$[3\chi^2 + 2\chi]P = [(-2\chi - 1)p^2]P = [-2\chi - 1]\phi'_2(P)$$

であることから、$3\chi^2 + 2\chi = \nu$として前記スカラｓをν進数展開することにより

$$s = s_1\nu + s_2,\ s_2 < \nu,$$

とし、

$$s \equiv (-2\chi - 1)s_1 p^2 + s_2 \mod r,$$

であることから、$(-2\chi-1)s_1$部分をν進数展開して、

$$s \equiv (s_3\nu + s_4)p^2 + s_2 \equiv s_5p^4 + s_4p^2 + s_2 \mod r,$$

とし、$p^4 \equiv -1 \mod r$であることから、

$$s \equiv s_4p^2 + (s_2 - s_5) \mod r,$$

であることを利用して、スカラ倍算[s]Ｐを、

$$[s]P = ([s_4]\phi'_2 + [s_2 - s_5])P,$$

として前記電子計算機に演算させるべく、前記スカラｓをν進数展開して得られる前記s_1を第１のレジスタに格納させるとともに前記s_2を第２のレジスタに格納させるステップと、$(-2\chi-1)s_1$をν進数展開して得られる前記s_3を第３のレジスタに格納させるとともに前記s_4を第４のレジスタに格納させるステップと、$(-2\chi-1)s_3$の値を前記s_5の値として第５のレジスタに格納させるステップとを有することとした。

発明の効果

[0014] 本発明によれば、スカラ倍算[s]Ｐを演算するに当たり、スカラｓをν進展開してスカラｓの大きさを小さくするとともに、

$$[p^2]P = \phi'_2(P)$$

を満たすフロベニウス写像$\phi'_2(P)$を用いることにより、スカラ倍算[s]Ｐの演算量をほぼ半減させることができ、スカラ倍算を高速化できる。

図面の簡単な説明

[0015] [図1]本発明の実施形態にかかるスカラ倍算器を備えた電子計算機の概略模式図である。

[図2]本発明の実施形態にかかるスカラ倍算プログラムのフローチャートである。

符号の説明

[0016] 10 電子計算機

11 ＣＰＵ

12 記憶装置

13 メモリ装置

14 バス

110 スカラ値用レジスタ

111 第１のレジスタ

112 第２のレジスタ

113 第３のレジスタ

114 第４のレジスタ

115 第５のレジスタ5

発明を実施するための最良の形態

[0017] 本発明の実施形態を説明するにあたり、最初に埋め込み次数ｋ＝12の場合について説明し、その後、埋め込み次数ｋ＝8の場合について説明する。

[0018] 本実施形態のスカラ倍算器及びスカラ倍算プログラムで実行されるスカラ倍算は、埋め込み次数ｋ＝12の場合、標数ｐ、位数ｒ、フロベニウス自己準同型写像のトレースｔが、

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

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

$$t(\chi)=6\chi^2+1, \quad \cdots \text{（式３）}$$

として与えられる楕円曲線の有理点が成す加法群$E(F_p)$の有理点Ｐのスカラ倍算[s]Ｐである。この楕円曲線は、ペアリングフレンドリ曲線の１種としてBarreto-Naehrig曲線（以下、「ＢＮ曲線」という。）が知られているものである。

[0019] このＢＮ曲線で表される楕円曲線に対しては、部分体ツイスト曲線が存在することが知られている。特に、埋め込み次数ｋ＝12の場合には、６次のツイスト曲線が知られており、

$$[p^2]P=\phi'_2(P),$$

となるフロベニウス写像ϕ'_2が知られている。

[0020] このフロベニウス写像ϕ'_2を用いることにより、スカラ演算を高速化することができることを利用するとともに、本発明では、以下に説明する関係式を

利用してスカラ演算を高速化している。

[0021] まず、式２より下式が得られる。

$$36\chi^4-36\chi^3+18\chi^2-6\chi+1\equiv 0 \bmod r. \quad \cdots \text{（式４）}$$

[0022] また、$p\equiv t-1 \bmod r$であるので、下式が得られる。

$$p^2-6\chi p+3p-6\chi+1\equiv 0 \bmod r. \quad \cdots \text{（式５）}$$

[0023] ここで、式５を変形することにより下式が得られる。

$$(-6\chi+3)p\equiv -p^2+6\chi-1 \bmod r. \quad \cdots \text{（式６）}$$

[0024] ここで、式６の両辺を平方することにより下式が得られる。

$$(-6\chi+3)^2p^2\equiv(p^2-6\chi+1)^2 \bmod r,$$

$$36\chi^2p^2-36\chi p^2+9p^2\equiv p^4-12\chi p^2+2p^2+36\chi^2-12\chi+1 \bmod r. \quad \cdots \text{（式７）}$$

[0025] さらに、$p^4+1\equiv p^2 \bmod r$であることを利用して式７を変形することにより、下式が得られる。

$$36\chi^2p^2-36\chi p^2+9p^2\equiv -12\chi p^2+3p^2+36\chi^2-12\chi \bmod r,$$

$$36\chi^2(p^2-1)\equiv(24\chi-6)p^2-12\chi \bmod r,$$

$$6\chi^2(p^2-1)\equiv(4\chi-1)p^2-2\chi \bmod r. \quad \cdots \text{（式８）}$$

[0026] そして、式８の両辺に$(p^2-1)^{-1}$を掛ける際に、

$$p^4-p^2+1\equiv 0 \bmod r, \quad \cdots \text{（式９）}$$

であることから、

$$-p^2(p^2-1)\equiv 1 \bmod r, \quad \cdots \text{（式１０）}$$

であるので、

$$(p^2-1)^{-1}\equiv -p^2 \bmod r, \quad \cdots \text{（式１１）}$$

であることを利用して、式８を下式にように変形できる。

$$6\chi^2\equiv-(4\chi-1)p^4+2\chi p^2$$

$$\equiv-(4\chi-1)(p^2-1)+2\chi p^2 \bmod r. \quad \cdots \text{（式１２）}$$

[0027] したがって、式１２を変形することにより下式が得られる。

$$6\chi^2-4\chi+1\equiv(-2\chi-1)p^2 \bmod r, \quad \cdots \text{（式１３）}$$

[0028] これにより、下式のフロベニウス写像ϕ'_2の関係式が得られる。

$[6\chi^2-4\chi+1]P=[(-2\chi+1)p^2]P=[-2\chi+1]\phi'_2(P)$, ・・・（式１４）

[0029] 次いで、フロベニウス写像ϕ'_2を用いたスカラ倍算[s]Ｐを考える。ここで、便宜上、

$\nu=6\chi^2-4\chi+1$, ・・・（式１５）

とする。

[0030] この場合、スカラｓのν進展開は下式のように表すことができる。

$s=s_1\nu+s_2, s_2<\nu$. ・・・（式１６）

[0031] ここで、式１６は、式１５と式１４より、下式のように表すことができる。

$s\equiv(-2\chi+1)s_1p^2+s_2 \bmod r$. ・・・（式１７）

[0032] なお、$(-2\chi+1)s_1$はνより大きくなることがある。そこで、$(-2\chi+1)s_1$をさらにν進展開して下式のように表すこととする。

$s\equiv(s_3\nu+s_4)p^2+s_2 \bmod r$. ・・・（式１８）

[0033] ここで式１４により$s_3\nu p^2\equiv(-2\chi+1)s_3p^4$であるので、$(-2\chi+1)s_3=s_5$とすることにより、式１８は下式のように表すことができる。

$s\equiv s_5p^4+s_4p^2+s_2 \bmod r$. ・・・（式１９）

[0034] この場合、s_4とs_2はνよりも小さい一方で、s_5はνより小さくないかもしれないが、そのような場合でもそれほど大きくなることはなく、問題となることはない。

[0035] 式９より$p^4\equiv p^2-1 \bmod r$であることから、式１９は下式のように変形できる。

$s\equiv s_5(p^2-1)+s_4p^2+s_2\equiv(s_4+s_5)p^2+(s_2-s_5) \bmod r$. ・・・（式２０）

[0036] ここで、

$A=s_4+s_5$, ・・・（式２１）

$B=s_2-s_5$, ・・・（式２２）

とすると、スカラ倍算[s]Ｐは

$[s]P=([A]\phi'_2+[B])P$, ・・・（式２３）

として演算できる。

[0037] したがって、たとえば、256ビットサイズのスカラｓに対するスカラ倍算を演算する際には、Ａ及びＢは128ビットサイズとなるので、演算量をほぼ半減させてスカラ倍算を高速化することができる。

[0038] 上述したスカラ倍算を行うスカラ倍算器は、図１に示すように電子計算機10で構成されるものであり、演算処理を実行するＣＰＵ11と、スカラ倍算プログラム及びスカラ倍算プログラムで使用する有理点の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、スカラ倍算プログラムを展開して実行可能とするとともに、スカラ倍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１中、14はバスである。

[0039] 本実施形態では、ＣＰＵ11内にスカラｓの値を記憶するスカラ値用レジスタ110を記憶手段として設けることとしている。さらに、ＣＰＵ11内には、上述したようにスカラｓのν進数展開にともなって生じる係数s_1, s_2, s_3, s_4, s_5の値をそれぞれ記憶する第１～５のレジスタ111, 112, 113, 114, 115を第１～５補助記憶手段として設けている。なお、スカラ値用レジスタ110で構成した記憶手段、及び第１～５のレジスタ111, 112, 113, 114, 115で構成した第１～５補助記憶手段は、ＣＰＵ11内にではなく、メモリ装置13などのＣＰＵ11以外の記憶手段に設けてもよい。

[0040] スカラ倍算器として機能する電子計算機10では、スカラ倍算の実行が必要となった場合にスカラ倍算プログラムを起動して、スカラ倍算を実行している。

[0041] すなわち、電子計算機10では、起動したスカラ倍算プログラムによって、図２に示すフローチャートに基づいてスカラ倍算を行い、演算結果を出力している。

[0042] 起動したスカラ倍算プログラムによって、電子計算機10では、ＣＰＵ11を入力手段として機能させて、記憶装置12またはメモリ装置13に記憶されている整数変数χのデータと、有理点Ｐのデータを読み出して、ＣＰＵ11の内部

に設けている所定のレジスタにそれぞれ入力している(ステップＳ１)。

[0043] さらに、電子計算機10では、スカラ倍算プログラムによってＣＰＵ11を入力手段として機能させて、スカラ倍算におけるスカラｓの値を入力させている。そして、ＣＰＵ11を記憶手段として機能させて、入力されたスカラｓの値をスカラ値用レジスタ110に記憶している(ステップＳ２)。

[0044] 次いで、電子計算機10では、スカラ倍算プログラムによってＣＰＵ11を演算手段として機能させて、上述したようにスカラｓをν進数展開して、ν進数展開の係数であるs_1とs_2を算出している(ステップＳ３)。すなわち、係数s_1は、スカラｓをνで除した際の商であり、係数s_2は、スカラｓをνで除した際の剰余である。

[0045] 算出されたν進数展開の係数であるs_1とs_2の値は、ＣＰＵ11を記憶手段として機能させて、第１のレジスタ111及び第２のレジスタ112にそれぞれ格納して、記憶させている(ステップＳ４)。

[0046] 次いで、電子計算機10では、ＣＰＵ11を演算手段として機能させて$(-2\chi+1)s_1$の値を演算し(ステップＳ５)、上述したように$(-2\chi+1)s_1$をν進数展開して、ν進数展開の係数であるs_3とs_4を算出している(ステップＳ６)。すなわち、係数s_3は、$(-2\chi+1)s_1$をνで除した際の商であり、係数s_4は、$(-2\chi+1)s_1$をνで除した際の剰余である。

[0047] 算出された$(-2\chi+1)s_1$のν進数展開の係数であるs_3とs_4の値は、ＣＰＵ11を記憶手段として機能させて、第３のレジスタ113及び第４のレジスタ114にそれぞれ格納して、記憶させている(ステップＳ７)。

[0048] 次いで、電子計算機10では、ＣＰＵ11を演算手段として機能させて$(-2\chi+1)s_3$の値を演算し(ステップＳ８)、この値を第５のレジスタ115にそれぞれ格納して、記憶させている(ステップＳ９)。

[0049] 次いで、電子計算機10では、ＣＰＵ11を演算手段として機能させて、第１～５のレジスタ11, 112, 113, 114, 115に記憶された値を用いて、s_4+s_5の値及びs_2-s_5の値を演算している(ステップＳ１０)。

[0050] 演算されたs_4+s_5の値及びs_2-s_5の値は、それぞれ所定のレジスタに格納し

て、記憶させている。説明の便宜上、$s_4+s_5=A$、$s_2-s_5=B$とする。

[0051] 次いで、電子計算機10では、ＣＰＵ11を演算手段として機能させて、スカラ倍算[s]Ｐを、[s]Ｐ＝([Ａ]ϕ'_2+[Ｂ])Ｐとして演算している(ステップＳ１１)。ここで、Ａ及びＢの値の大きさが、スカラｓの大きさの半分程度となることにより、演算時間を大きく削減できる。コンピュータシミュレーションでは、一般的なバイナリ法でのスカラ倍算と比較して、40%程度の高速化が可能であった。

[0052] なお、ステップＳ１１で行っている[s]Ｐ＝([Ａ]ϕ'_2+[Ｂ])Ｐの演算は、具体的には、以下のように行っている。

[0053] ここで、電子計算機10には、スカラ演算[s]Ｐの演算結果を記憶する演算結果用レジスタＲと、演算に必要となる値を一時的に記憶しておく第１補助レジスタＣと第２補助レジスタＤとを設けている。

[0054] まず、電子計算機10は、初期化処理として、演算結果用レジスタＲを零元とし、第１補助レジスタＣにϕ'_2(Ｐ)を代入し、第２補助レジスタＤに有理点Ｐを代入している。

[0055] また、上記のＡとＢをそれぞれ２進数表示した際のｉ番目の桁の値をA_iとB_iと表示するものとして、電子計算機10では、ＡとＢの全桁にわたって以下の演算ループを実行することとしている。

[0056] ｉ番目の桁において、A_i＝１かつB_i＝１の場合には、演算結果用レジスタＲに、演算結果用レジスタＲと第２補助レジスタＤの和を代入する。すなわち、Ｒ←Ｒ＋Ｄである。

[0057] ｉ番目の桁において、A_i＝１かつB_i＝０の場合には、演算結果用レジスタＲに、演算結果用レジスタＲと第１補助レジスタＣの和を代入する。すなわち、Ｒ←Ｒ＋Ｃである。

[0058] ｉ番目の桁において、A_i＝０かつB_i＝１の場合には、演算結果用レジスタＲに、演算結果用レジスタＲと有理点Ｐの和を代入する。すなわち、Ｒ←Ｒ＋Ｐである。

[0059] そして、演算結果用レジスタＲに、演算結果用レジスタＲと演算結果用レ

ジスタＲの和を代入する。すなわち、Ｒ←Ｒ＋Ｒである。

[0060] その後、電子計算機10は、デクリメントまたはインクリメントを行って、A_iとB_iの桁をずらしながらＡとＢの全桁にわたって演算を行うことによりスカラ演算[s]Ｐの演算を行って、演算結果を出力可能としている。

[0061] 本実施形態の演算では、ＡとＢとを同時進行で演算していることにより、ＡとＢの値の大きさが、スカラｓの大きさの半分程度となることのメリットを最大限利用することができる。

[0062] 次に、埋め込み次数ｋ＝8の場合について説明する。

[0063] 埋め込み次数ｋ＝8の場合、標数ｐ、位数ｒ、フロベニウス自己準同型写像のトレースｔが、

$$p(\chi)=(81\chi^6+54\chi^5+45\chi^4+12\chi^3+13\chi^2+6\chi+1)/4,$$

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

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

として与えられるＢＮ曲線の有理点が成す加法群$E(F_p)$の有理点Ｐでのスカラ倍算[s]Ｐとする。

[0064] この場合でも、部分体ツイスト曲線が存在することが知られている。特に、埋め込み次数ｋ＝8の場合には、４次のツイスト曲線が知られており、

$$[p^2]P=\phi'_2(P),$$

となるフロベニウス写像ϕ'_2が知られている。

[0065] また、埋め込み次数ｋ＝8の場合には、上述した式１４の代わりに、

$$[3\chi^2+2\chi]P=[(-2\chi-1)p^2]P=[-2\chi-1]\phi'_2(P), \quad \cdots \text{（式２４）}$$

の関係式があることを利用している。

[0066] そして、埋め込み次数ｋ＝12の場合と同様に、$3\chi^2+2\chi=\nu$として前記スカラｓをν進数展開すると、下式のように表すことができる。

$$s=s_1\nu+s_2, s_2<\nu. \quad \cdots \text{（式２５）}$$

[0067] ここで、式２４より、式２５は下式のように表すことができる。

$$s\equiv(-2\chi-1)s_1p^2+s_2 \bmod r. \quad \cdots \text{（式２６）}$$

[0068] なお、$(-2\chi-1)s_1$はνより大きくなることがある。そこで、$(-2\chi-1)s_1$をさらにν進展開して下式のように表すこととする。

$$s \equiv (s_3\nu + s_4)p^2 + s_2 \bmod r. \quad \cdots \text{（式２７）}$$

[0069] ここで式２４により$s_3\nu p^2 \equiv (-2\chi-1)s_3p^4$であるので、$(-2\chi-1)s_3=s_5$とすることにより、式２７は下式のように表すことができる。

$$s \equiv s_5p^4 + s_4p^2 + s_2 \bmod r. \quad \cdots \text{（式２８）}$$

[0070] この場合、s_4とs_2はνよりも小さい一方で、s_5はνより小さくないかもしれないが、そのような場合でもそれほど大きくなることはなく、問題となることはない。

[0071] 埋め込み次数ｋ＝8の場合、$p^4 \equiv -1 \bmod r$であることから、式２８は下式のように変形できる。

$$s \equiv -s_5 + s_4p^2 + s_2 \equiv s_4p^2 + (s_2 - s_5) \bmod r. \quad \cdots \text{（式２９）}$$

[0072] ここで、

$$A = s_4, \quad \cdots \text{（式３０）}$$

$$B = s_2 - s_5, \quad \cdots \text{（式３１）}$$

とすると、スカラ倍算[s]Ｐは、埋め込み次数ｋ＝12の場合と同様に

$$[s]P = ([A]\phi'_2 + [B])P,$$

として演算できる。

[0073] したがって、埋め込み次数ｋ＝8の場合には、埋め込み次数ｋ＝12の場合と比較して、第５のレジスタ115に格納される値の計算式、及び式３０のＡの値が異なるだけであり、埋め込み次数ｋ＝12の場合と同様に演算できる。

[0074] そこで、埋め込み次数ｋ＝8の場合におけるスカラ演算器は、埋め込み次数ｋ＝12の場合におけるスカラ演算器と同じとし、図２に示したフローチャートのステップＳ８での計算式を$(-2\chi-1)s_3$とし、ステップＳ９でs_5の値を$(-2\chi-1)s_3$とし、ステップＳ１０でＡ＝s_4としている。

[0075] これにより、埋め込み次数ｋ＝8の場合でも、Ａ及びＢの値の大きさが、スカラｓの大きさの半分程度となることにより、スカラ倍算[s]Ｐの演算時間を大きく削減できる。

産業上の利用可能性

[0076] 本発明によれば、グループ署名の演算中に必要となるスカラ演算の速度を向上させて、グループ署名の処理の高速化をはかることができる。

請求の範囲

[請求項1] 整数変数χを用いて、埋め込み次数ｋ＝12における標数ｐ、位数ｒ、フロベニウス自己準同型写像のトレースｔが、

$p(\chi)=36\chi^4-36\chi^3+24\chi^2-6\chi+1$,

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

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

として与えられる楕円曲線の有理点が成す加法群Ｅ(F_p)の有理点Ｐのスカラ倍算[s]Ｐを演算するスカラ倍算器であって、

ツイスト次数ｄを６とし、ｋ＝ｄ×ｅとなる正整数ｅを２として、

$[p^2]P=\phi'_2(P)$,

となるフロベニウス写像ϕ'_2を用い、

$[6\chi^2-4\chi+1]P=[(-2\chi+1)p^2]P=[-2\chi+1]\phi'_2(P)$

であることから、$6\chi^2-4\chi+1=\nu$として前記スカラｓをν進数展開することにより

$s=s_1\nu+s_2,\ s_2<\nu$,

とし、

$s\equiv(-2\chi+1)s_1p^2+s_2 \mod r$,

であることから、$(-2\chi+1)s_1$部分をν進数展開して、

$s\equiv(s_3\nu+s_4)p^2+s_2\equiv s_5p^4+s_4p^2+s_2 \mod r$,

とし、$p^4\equiv p^2-1 \mod r$であることから、

$s\equiv(s_4+s_5)p^2+(s_2-s_5) \mod r$,

であることを利用して、スカラ倍算[s]Ｐを、

$[s]P=([s_4+s_5]\phi'_2+[s_2-s_5])P$,

として演算すべく、

前記スカラｓの値を記憶する記憶手段と、

前記係数s_1, s_2, s_3, s_4, s_5をそれぞれ記憶する第１～５補助記憶手段とを設け、

前記スカラｓをν進数展開して得られた値を前記第１補助記憶手段

と前記第２補助記憶手段に記憶させ、$(-2\chi+1)s_1$をν進数展開して得られた値を前記第３補助記憶手段と前記第４補助記憶手段に記憶させ、$(-2\chi+1)s_3$の値を前記第５補助記憶手段に記憶させているスカラ倍算器。

[請求項2] 整数変数χを用いて、埋め込み次数ｋ＝12における標数ｐ、位数ｒ、フロベニウス自己準同型写像のトレースｔが、

$$p(\chi)=36\chi^4-36\chi^3+24\chi^2-6\chi+1,$$

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

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

として与えられる楕円曲線の有理点が成す加法群Ｅ(F_p)の有理点Ｐのスカラ倍算[s]Ｐを、ＣＰＵを備えた電子計算機に演算させるスカラ倍算プログラムであって、

ツイスト次数ｄを６とし、ｋ＝ｄ×ｅとなる正整数ｅを２として、

$$[p^2]P=\phi'_2(P),$$

となるフロベニウス写像ϕ'_2を用い、

$$[6\chi^2-4\chi+1]P=[(-2\chi+1)p^2]P=[-2\chi+1]\phi'_2(P)$$

であることから、$6\chi^2-4\chi+1=\nu$として前記スカラｓをν進数展開することにより

$$s=s_1\nu+s_2,\ s_2<\nu,$$

とし、

$$s\equiv(-2\chi+1)s_1p^2+s_2 \mod r,$$

であることから、$(-2\chi+1)s_1$部分をν進数展開して、

$$s\equiv(s_3\nu+s_4)p^2+s_2\equiv s_5p^4+s_4p^2+s_2 \mod r,$$

とし、$p^4\equiv p^2-1 \mod r$であることから、

$$s\equiv(s_4+s_5)p^2+(s_2-s_5) \mod r,$$

であることを利用して、スカラ倍算[s]Ｐを、

$$[s]P=([s_4+s_5]\phi'_2+[s_2-s_5])P,$$

として前記電子計算機に演算させるべく、

前記スカラｓをν進数展開して得られる前記s_1を第１のレジスタに格納させるとともに前記s_2を第２のレジスタに格納させるステップと、

$(-2\chi+1)s_1$をν進数展開して得られる前記s_3を第３のレジスタに格納させるとともに前記s_4を第４のレジスタに格納させるステップと、

$(-2\chi+1)s_3$の値を前記s_5の値として第５のレジスタに格納させるステップと、

を有するスカラ倍算プログラム。

[請求項3] 整数変数χを用いて、埋め込み次数ｋ＝8における標数ｐ、位数ｒ、フロベニウス自己準同型写像のトレースｔが、

$$p(\chi)=(81\chi^6+54\chi^5+45\chi^4+12\chi^3+13\chi^2+6\chi+1)/4,$$

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

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

として与えられる楕円曲線の有理点が成す加法群$E(F_p)$の有理点Ｐのスカラ倍算[s]Ｐを演算するスカラ倍算器であって、

ツイスト次数ｄを４とし、ｋ＝ｄ×ｅとなる正整数ｅを２として、

$$[p^2]P=\phi'_2(P),$$

となるフロベニウス写像ϕ'_2を用い、

$$[3\chi^2+2\chi]P=[(-2\chi-1)p^2]P=[-2\chi-1]\phi'_2(P)$$

であることから、$3\chi^2+2\chi=\nu$として前記スカラｓをν進数展開することにより

$$s=s_1\nu+s_2,\ s_2<\nu,$$

とし、

$$s\equiv(-2\chi-1)s_1p^2+s_2 \mod r,$$

であることから、$(-2\chi-1)s_1$部分をν進数展開して、

$$s\equiv(s_3\nu+s_4)p^2+s_2\equiv s_5p^4+s_4p^2+s_2 \mod r,$$

とし、$p^4\equiv-1 \mod r$であることから、

$$s\equiv s_4p^2+(s_2-s_5) \mod r,$$

であることを利用して、スカラ倍算[s]Ｐを、

$$[s]P=([s_4]\phi'_2+[s_2-s_5])P,$$

として演算すべく、

前記スカラｓの値を記憶する記憶手段と、

前記係数s_1, s_2, s_3, s_4, s_5をそれぞれ記憶する第１～５補助記憶手段とを設け、

前記スカラｓをν進数展開して得られた値を前記第１補助記憶手段と前記第２補助記憶手段に記憶させ、$(-2\chi-1)s_1$をν進数展開して得られた値を前記第３補助記憶手段と前記第４補助記憶手段に記憶させ、$(-2\chi-1)s_3$の値を前記第５補助記憶手段に記憶させているスカラ倍算器。

[請求項4] 整数変数χを用いて、埋め込み次数ｋ＝8における標数ｐ、位数ｒ、フロベニウス自己準同型写像のトレースｔが、

$$p(\chi)=(81\chi^6+54\chi^5+45\chi^4+12\chi^3+13\chi^2+6\chi+1)/4,$$

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

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

として与えられる楕円曲線の有理点が成す加法群Ｅ(F_p)の有理点Ｐのスカラ倍算[s]Ｐを、ＣＰＵを備えた電子計算機に演算させるスカラ倍算プログラムであって、

ツイスト次数ｄを４とし、ｋ＝ｄ×ｅとなる正整数ｅを２として、

$$[p^2]P=\phi'_2(P),$$

となるフロベニウス写像ϕ'_2を用い、

$$[3\chi^2+2\chi]P=[(-2\chi-1)p^2]P=[-2\chi-1]\phi'_2(P)$$

であることから、$3\chi^2+2\chi=\nu$として前記スカラｓをν進数展開することにより

$$s=s_1\nu+s_2,\ s_2<\nu,$$

とし、

$$s\equiv(-2\chi-1)s_1p^2+s_2 \mod r,$$

であることから、$(-2\chi-1)s_1$部分をν進数展開して、

$$s \equiv (s_3\nu + s_4)p^2 + s_2 \equiv s_5p^4 + s_4p^2 + s_2 \mod r,$$

とし、$p^4 \equiv -1 \mod r$であることから、

$$s \equiv s_4p^2 + (s_2 - s_5) \mod r,$$

であることを利用して、スカラ倍算[s]Pを、

$$[s]P = ([s_4]\phi'_2 + [s_2 - s_5])P,$$

として前記電子計算機に演算させるべく、

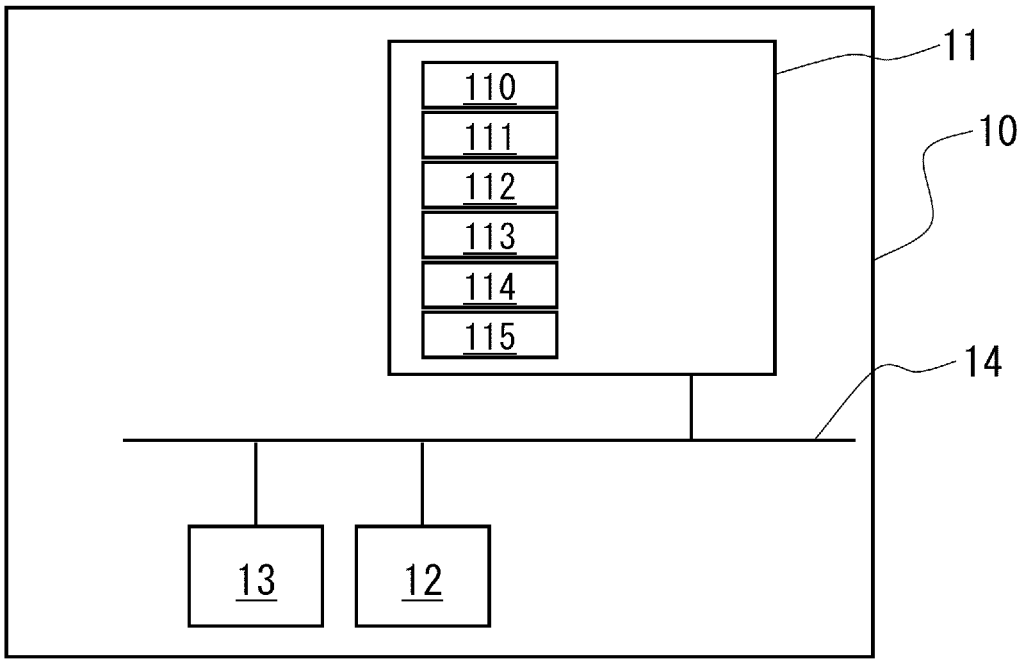
前記スカラsをν進数展開して得られる前記s_1を第１のレジスタに格納させるとともに前記s_2を第２のレジスタに格納させるステップと、

$(-2\chi-1)s_1$をν進数展開して得られる前記s_3を第３のレジスタに格納させるとともに前記s_4を第４のレジスタに格納させるステップと、

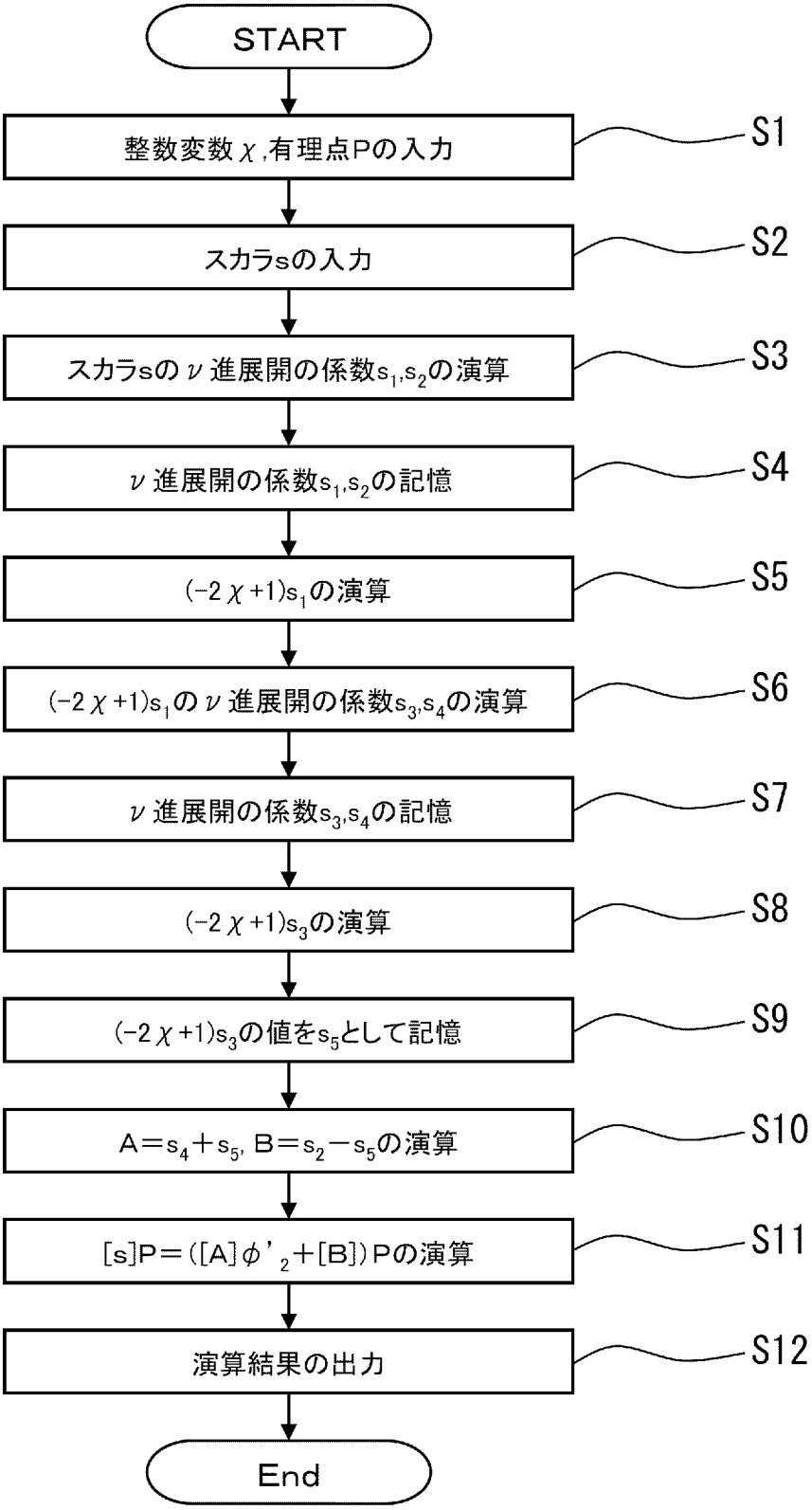
$(-2\chi-1)s_3$の値を前記s_5の値として第５のレジスタに格納させるステップと、

を有するスカラ倍算プログラム。

[図1]



[図2]


START
整数変数χ,有理点Pの入力
S1
スカラsの入力
S2
スカラsのν進展開の係数s_1,s_2の演算
S3
ν進展開の係数s_1,s_2の記憶
S4
$(-2\chi+1)s_1$の演算
S5
$(-2\chi+1)s_1$のν進展開の係数s_3,s_4の演算
S6
ν進展開の係数s_3,s_4の記憶
S7
$(-2\chi+1)s_3$の演算
S8
$(-2\chi+1)s_3$の値をs_5として記憶
S9
A＝s_4＋s_5, B＝s_2－s_5の演算
S10
[s]P＝([A]ϕ'_2＋[B])Pの演算
S11
演算結果の出力
S12
End

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/070127

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	1996-2010
Kokai Jitsuyo Shinan Koho	1971-2010	Toroku Jitsuyo Shinan Koho	1994-2010

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	Yasuyuki Nogami, Masataka Akane, Yumi Sakemi, Yoshitaka Morikawa, "Efficient Pairings on Twisted Elliptic Curve", 2008 Third International Conference on Convergence and Hybrid Information Technology, 2008.11.18, p.430-439	1-4
A	Masataka AKANE, Hidehiro KATO, Takuya OKIMOTO, Yasuyuki NOGAMI, Yoshitaka MORIKAWA, "Ate Pairing ni Tekishita Barreto-Naehrig Kyokusen no Parameter Settei", Computer Security Symposium 2007 Ronbunshu, 31 October 2007 (31.10.2007), vol.2007, no.10, pages 495 to 500, IPSJ Symposium Series	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
17 February, 2010 (17.02.10)	02 March, 2010 (02.03.10)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/070127

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Roberto Maria Avanzi, Mathieu Ciet, and Francesco Sica, "Faster Scalar Multiplication on Koblitz Curves Combining Point Halving with the Frobenius Endomorphism", LNCS, 2004.03, Vol.2947, p.28-40, Public Key Cryptography - PKC 2004	1-4
A	JP 2007-41461 A (Hitachi, Ltd.), 15 February 2007 (15.02.2007), entire text; all drawings (Family: none)	1-4
A	JP 2006-184831 A (Nippon Telegraph And Telephone Corp.), 13 July 2006 (13.07.2006), paragraphs [0027] to [0068] (Family: none)	1-4
T,A	Masataka AKANE, Yasuyuki NOGAMI, and Yoshitaka MORIKAWA, "Fast Ate Pairing Computation of Embedding Degree 12 Using Subfield - Twisted Elliptic Curve", IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 2009.02.01, VOL.E92-A, NO.2, p.508-516	1-4

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００９／０７０１２７

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	１９７１－２０１０年
日本国実用新案登録公報	１９９６－２０１０年
日本国登録実用新案公報	１９９４－２０１０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	関連する請求項の番号
A	Yasuyuki Nogami, Masataka Akane, Yumi Sakemi, Yoshitaka Morikawa, “Efficient Pairings on Twisted Elliptic Curve”, 2008 Third International Conference on Convergence and Hybrid Information Technology, 2008.11.18, p.430-439	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 １７．０２．２０１０	国際調査報告の発送日 ０２．０３．２０１０
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	関連する請求項の番号
Ａ	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，情報処理学会シンポジウムシリーズ	１－４
Ａ	Roberto Maria Avanzi, Mathieu Ciet, and Francesco Sica, “Faster Scalar Multiplication on Koblitz Curves Combining Point Halving with the Frobenius Endomorphism”, LNCS, 2004.03, Vol.2947, p.28-40, Public Key Cryptography - PKC 2004	１－４
Ａ	JP 2007-41461 A (株式会社日立製作所) 2007.02.15, 全文, 全図（ファミリーなし）	１－４
Ａ	JP 2006-184831 A（日本電信電話株式会社）2006.07.13，段落【００２７】－【００６８】（ファミリーなし）	１－４
Ｔ，Ａ	Masataka AKANE, Yasuyuki NOGAMI, and Yoshitaka MORIKAWA, “Fast Ate Pairing Computation of Embedding Degree 12 Using Subfield - Twisted Elliptic Curve”, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 2009.02.01, VOL.E92-A, NO.2, p.508-516	１－４