

(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10月28日(28.10.2010)

PCT

(10) 国際公開番号
WO 2010/123151 A3

- (51) 国際特許分類:
G06F 17/10 (2006.01) G09C 1/00 (2006.01)
- (21) 国際出願番号: PCT/JP2010/057534
- (22) 国際出願日: 2010年4月21日(21.04.2010)
- (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 2009-121398 2009年4月21日(21.04.2009) 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). 那須弘明(NASU Hiroaki) [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).

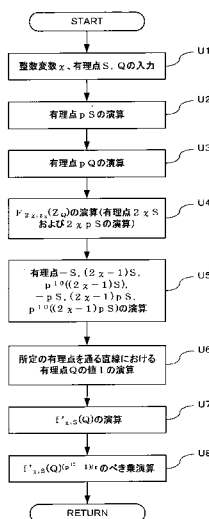
- (74) 代理人: 松尾憲一郎(MATSUO Kenichiro); 〒8100042 福岡県福岡市中央区赤坂1丁目10番17号 しんくみ赤坂ビル7階 Fukuoka (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH,

[続葉有]

(54) Title: PAIRING ARITHMETIC DEVICE, PAIRING ARITHMETIC METHOD AND RECORDING MEDIUM HAVING PAIRING ARITHMETIC PROGRAM RECORDED THEREON

(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5]



[83]
$$e(S, Q) = f'_{x,S}(Q)^{(p^k-1)/r}$$

- U1 Input variable integer x and rational points S, Q
U2 Calculate rational point pS
U3 Calculate rational point pQ
U4 Calculate $f_{2x, 2S}(Z_Q)$ (calculate rational points C and $2xS$)
U5 Calculate rational points $-S, (2x-1)S, p^{-1}((2x-1)S), -pS, (2x-1)pS, p^{-1}((2x-1)pS)$
U6 Calculate value 1 of the rational point Q on the straight line that passes through predetermined rational points
U7 Calculate $f_{x,S}(Q)$
U8 Exponential calculation of $f_{x,S}(Q)^{(p^{12}-1)/r}$

(57) Abstract: A pairing arithmetic device is provided with a CPU which calculates pairing $e(S, Q)$, with F as a rational function calculated using $S \in G_1$, $Q \in G_2$, a predetermined integer variable as x , and an algorithm (MMA) of a mirror with respect to multi-pairing as F . The order r , the trace t of the Frobenius endomorphism map/image Φ_p are specified using the integer variable x according to the degree of embedding k . The CPU carries out the arithmetic operation by means of: an inputting means which inputs the aforementioned integer variable x , the rational point S , and the rational point Q into their respective predetermined registers; a calculating means which calculates F ; a calculating means which calculates values at a rational point $Q(x_Q, y_Q)$ on a straight line which passes through predetermined rational points; a calculating means which calculates $f_{x,S}(Q)$ using F and the aforementioned value; and a calculating means which uses $f_{x,S}(Q)$ to calculate the pairing $e(S, Q)$ as a [83].

(57) 要約: $S \in G_1$, $Q \in G_2$ 、所定の整数変数を x 、マルチペアリングに対するミラーのアルゴリズム(MMA)を用いて計算される有理関数を F として、ペアリング $e(S, Q)$ を演算する CPU を備えたペアリング演算装置であって、位数 r と、フロベニウス自己準同形写像 Φ_p のトレース t を、前記埋め込み次数 k に応じて前記整数変数 x を用いて特定しておき、前記 CPU は、記整数変数 x と、前記有理点 S と、前記有理点 Q をそれぞれ所定のレジスタに入力する入力手段と、 F 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 $Q(x_Q, y_Q)$ における値を演算する演算手段と、前記 F と前記値を用いて $f_{x,S}(Q)$ を演算する演算手段と、前記 $f_{x,S}(Q)$ を用いて前記ペアリング $e(S, Q)$ を [数 83] として演算する演算手段とによって演算を行う。



PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (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,

- 国際調査報告 (条約第 21 条(3))
— 請求の範囲の補正の期限前の公開であり、補正を受理した際には再公開される。(規則 48.2(h))

(88) 国際調査報告書の公開日: 2010 年 12 月 23 日

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2010/057534

A. CLASSIFICATION OF SUBJECT MATTER

G06F17/10(2006.01)i, 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)

G06F17/10, 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/JMEDPlus/JST7580(JDreamII) pairing

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Lee, E. et al., Efficient and Generalized Pairing Computation on Abelian Varieties, IEEE Transactions on Information Theory, 2009.03.16, Volume 55, Issue 4, p.1793-1803, especially III. THE R-ATE PAIRING, IV. THE R-ATE PAIRING ON ELLIPTIC CURVES	1-24
A	Sakemi, Y. et al., An Improvement of Twisted Ate Pairing with Barreto-Naehrig Curve by using Frobenius Mapping, Third International Conference on Convergence and Hybrid Information Technology, 2008., 2008.11.18, p.406-410, especially 2.2 Twisted Ate Pairing with BN curve, 3.2 Proposed Method	1-24



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

“&” document member of the same patent family

Date of the actual completion of the international search

05 October, 2010 (05.10.10)

Date of mailing of the international search report

19 October, 2010 (19.10.10)

Name and mailing address of the ISA/

Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2010/057534

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Nogami, Y. et al., Integer Variable χ -Based Ate Pairing, Lecture Notes in Computer Science, Vol. 5209, 2008, p.178-191, especially 3 Main Proposal	1-24
A	Vercauteren, F., Optimal Pairings, Cryptology ePrint Archive, Report 2008/096, 2008.03.07, p.1-14, especially 3 Optimal Pairing, 4 Examples	1-24
P, X	Yumi SAKEMI et al., "Multi Pairing o Mochiita Twisted Ate Pairing no Kairyo", 2010 Nen Symposium on Cryptography and Information Security Koen Ronbunshu, 19 January 2010 (19. 01.2010), pages 1 to 6, particularly, 3 approach	1-24

A. 発明の属する分野の分類（国際特許分類（I P C）） Int.Cl. G06F17/10(2006.01)i, 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. G06F17/10, 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 1 0 年 日本国実用新案登録公報 1 9 9 6 - 2 0 1 0 年 日本国登録実用新案公報 1 9 9 4 - 2 0 1 0 年			
国際調査で使用した電子データベース（データベースの名称、調査に使用した用語） JSTPlus/JMEDPlus/JST7580(JDreamII) pairing			
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	Lee, E. et al., Efficient and Generalized Pairing Computation on Abelian Varieties, IEEE Transactions on Information Theory, 2009.03.16, Volume 55, Issue 4, p.1793-1803, especially III. THE R-ATE PAIRING, IV. THE R-ATE PAIRING ON ELLIPTIC CURVES	1-24	
☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。			
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す） 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願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 0 5 . 1 0 . 2 0 1 0		国際調査報告の発送日 1 9 . 1 0 . 2 0 1 0	
国際調査機関の名称及びあて先 日本国特許庁（I S A / J P） 郵便番号 1 0 0 - 8 9 1 5 東京都千代田区霞が関三丁目4番3号		特許庁審査官（権限のある職員） 中里 裕正 電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6	5 S 9 3 6 4