

(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
2022年1月13日(13.01.2022)



(10) 国際公開番号

WO 2022/009389 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2020/026860

(22) 国際出願日: 2020年7月9日(09.07.2020)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人: 三菱電機株式会社(MITSUBISHI ELECTRIC CORPORATION) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 Tokyo (JP).

(72) 発明者: 早坂 健一郎(HAYASAKA, Kenichiro); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP).

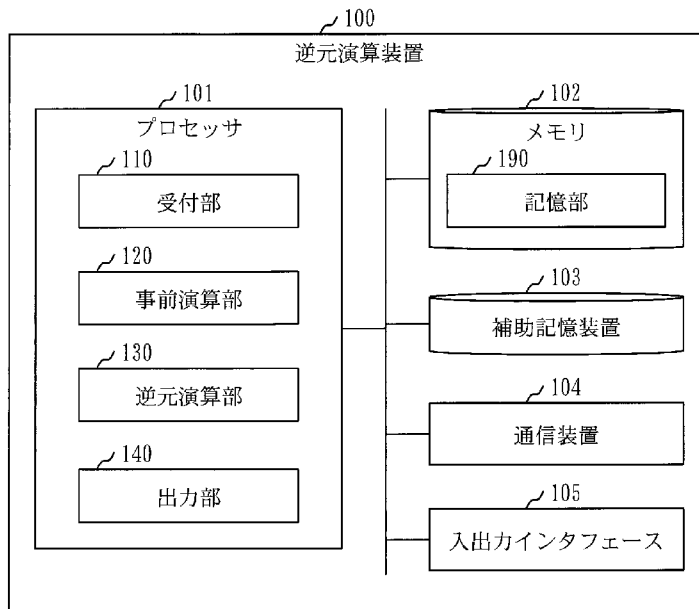
(74) 代理人: 溝井 国際特許業務法人(MIZOI INTERNATIONAL PATENT FIRM); 〒2470056 神奈川県鎌倉市大船二丁目17番10号3階 Kanagawa (JP).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,

(54) Title: INVERSE COMPUTING DEVICE, INVERSE COMPUTING METHOD, AND INVERSE COMPUTING PROGRAM

(54) 発明の名称: 逆元演算装置、逆元演算方法および逆元演算プログラム

図1



- 100 Inverse computing device
- 101 Processor
- 102 Memory
- 103 Auxiliary storage device
- 104 Communication device
- 105 Input/output interface
- 110 Acceptance unit
- 120 Preliminary computing unit
- 130 Inverse computing unit
- 140 Output unit
- 190 Storage unit

(57) Abstract: An acceptance unit (110) accepts an element a . A preliminary computation unit (120) uses a_0 , a_1 , and a_2 to compute t_1 that is a computational result of a_0^2 , t_2 that is a computational result of a_2^2 , t_3 that is a computational result of a_0a_1 , t_4 that is a computational result of a_1a_2 , and t_7 that is equal to a computational result of $(a_0+a_1)(a_1-a_2)$. An inverse computing unit (130) uses t_1 , t_2 , t_3 , t_4 , and t_7 to compute b_0 that is equal to a computational result of $a_0^2-a_1a_2v$, b_1 that is equal to a computational result of $a_2^2v-a_0a_1$, and b_2 that

MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,
NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,
QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

- 一 国際調査報告（条約第21条(3)）

is equal to a computational result of $a_1^2 - a_0 a_2$. An output unit (140) uses b_0 , b_1 , and b_2 to generate and output the inverse a^{-1} .

(57) 要約：受付部（1 1 0）は元 a を受け付ける。事前演算部（1 2 0）は、 a_0 と a_1 と a_2 を用いて、 a_0^2 の計算結果である t_1 と、 a_2^2 の計算結果である t_2 と、 $a_0 a_1$ の計算結果である t_3 と、 $a_1 a_2$ の計算結果である t_4 と、 $(a_0 + a_1)(a_1 - a_2)$ の計算結果に等しい t_7 と、を算出する。逆元演算部（1 3 0）は、 t_1 と t_2 と t_3 と t_4 と t_7 を用いて、 $a_0^2 - a_1 a_2 v$ の計算結果に等しい b_0 と、 $a_2^2 v - a_0 a_1$ の計算結果に等しい b_1 と、 $a_1^2 - a_0 a_2$ の計算結果に等しい b_2 と、を算出する。出力部（1 4 0）は、 b_0 と b_1 と b_2 を用いて前記逆元 a^{-1} を生成して出力する。

明 細 書

発明の名称：

逆元演算装置、逆元演算方法および逆元演算プログラム

技術分野

[0001] 本開示は、有限体の部分群における高速な乗法逆元算を可能とする技術に関するものである。

背景技術

[0002] 有限体上の演算を利用した暗号アルゴリズムは複数存在する。

有限体の部分群の性質を利用すると、演算の計算量を削減でき、結果として暗号アルゴリズムを効率化できる場合がある。

[0003] ペアリング暗号は、非退化かつ双線形というペアリング写像の特長を利用して利便性の高い様々な機能を実現している。

ペアリング写像の計算は有限体上の演算で構成される。そのため、有限体上の演算を高速化することは、ペアリング暗号を効率化するうえで重要である。

[0004] ペアリング写像の計算アルゴリズムである $At e$ ペアリングまたは $Optimal At e$ ペアリングなどでは、有限体の部分群の性質を利用することで逆元算および二乗算をより高速に計算でき、ペアリング暗号を効率化できる、ということが知られている。

[0005] ペアリング写像の計算は、以下のように逆元算を必要とする。

素体 F_p に対して、次のような拡大体 (F_{p^n}, F_{p^k}) を考える。拡大体 F_{p^n} と拡大体 F_{p^k} は、それぞれ素体 F_p の拡大体である。素体 F_p と拡大体 F_{p^n} と拡大体 F_{p^k} は、それぞれ有限体である。

$$F_{p^n} = F_p[v] / (v^n - \alpha),$$

$$F_{p^k} = F_{p^n}[w] / (w^3 - v).$$

「 k 」は、素数 r および素数 p に対して $r \mid (p^k - 1)$ を満たす最小の整数である。「 k 」は、整数 n に対して $k = 3n$ を満たす。

「 α 」は、素体 F_p の元である。

「 v 」は、素体 F_p 上既約な多項式 $f(X) = X^n - \alpha$ に対して $f(v) = 0$ を満たす拡大体 F_{p^n} の元である。

「 w 」は、拡大体 F_{p^n} 上既約な多項式 $g(X) = X^3 - v$ に対して $g(w) = 0$ を満たす拡大体 F_{p^k} の元である。

[0006] 位数が $\Phi 3(p^n)$ である拡大体 F_{p^k} の元の集合を `c y c l o t o m i c s u b g r o u p` とよぶ。この集合を $G\Phi 3(p^n)$ と記す。ただし、 $\Phi m(x)$ は第 m 円分多項式を意味する。

ここで、集合 $G\Phi 3(p^n)$ の元 a を以下の式で表す。「 a_0 」と「 a_1 」と「 a_2 」は、それぞれ拡大体 F_{p^n} の元である。

$$a = a_0 + a_1 w + a_2 w^2$$

[0007] この場合、集合 $G\Phi 3(p^n)$ の元 a の逆元 a^{-1} は、2回の `F r o b e n i u s` 演算と1回の拡大体 F_{p^k} 上の乗算で算出できる。

これは、集合 $G\Phi 3(p^n)$ 上の逆元算が、拡大体 F_{p^k} 上の逆元算よりも高速に計算可能であることを示している。

非特許文献1は、「 $k = 27$ 」の場合において集合 $G\Phi 3(p^n)$ 上の逆元算が可能なことを示している。

[0008] さらに、逆元 a^{-1} を以下の式で表す。

$$a^{-1} = (a_0^2 - a_1 a_2 v) + (a_2^2 v - a_0 a_1) w + (a_1^2 - a_0 a_2) w^2$$

この式には、拡大体 F_{p^n} 上の3回の乗算 ($a_1 a_2$, $a_0 a_1$, $a_0 a_2$) と3回の二乗算 (a_0^2 , a_2^2 , a_1^2) が含まれる。

非特許文献2は、「 $k = 9, 15, 27$ 」の場合においてこの式による逆元算が可能なことを示している。

先行技術文献

非特許文献

[0009] 非特許文献1: X. Zhang and D. Lin, "Analysis of Optimum Pairing Products at

High Security Levels,” INDOCRYPT 2012, LNCS 7668, pp. 412–430, 2012.

非特許文献2: E. Fouotsa, N. El Mrabet and A. Pecha “Optimal Ate Pairing on Elliptic Curves with Embedding Degree 9, 15 and 27,” IACR Cryptology ePrint Archive, 2016/1187, 2016.

発明の概要

発明が解決しようとする課題

[0010] ペアリング写像のための逆元算は有限体上の演算を必要とし、有限体上の演算はペアリング暗号を効率化する上でボトルネックとなる。

特に、有限体上の演算のうち、乗算および二乗算は、加算、減算および分数倍算（ $1/2$ 倍算または $1/4$ 倍算など）に比べて、計算量が多い。

[0011] 本開示は、ペアリング写像のための逆元算に要する計算量を削減できるようにすることを目的とする。

課題を解決するための手段

[0012] 本開示の逆元演算装置は、元 a の逆元 a^{-1} を算出する。

前記元 a は、 $a = a_0 + a_1 w + a_2 w^2$ で表される。

前記逆元 a^{-1} は、 $a^{-1} = (a_0^2 - a_1 a_2 v) + (a_2^2 v - a_0 a_1) w + (a_1^2 - a_0 a_2) w^2$ で表される。

前記逆元演算装置は、

前記元 a を受け付ける受付部と、

a_0 と a_1 と a_2 を用いて、 a_0^2 の計算結果である t_1 と、 a_2^2 の計算結果である t_2 と、 $a_0 a_1$ の計算結果である t_3 と、 $a_1 a_2$ の計算結果である t_4 と、 $(a_0 + a_1)(a_1 - a_2)$ の計算結果に等しい t_7 と、を算出する事前演算部と、

t_1 と t_2 と t_3 と t_4 と t_7 を用いて、 $a_0^2 - a_1 a_2 v$ の計算結果に等しい b_0 と、 $a_2^2 v - a_0 a_1$ の計算結果に等しい b_1 と、 $a_1^2 - a_0 a_2$ の計算結果

に等しい b_2 と、を算出する逆元演算部と、

b_0 と b_1 と b_2 を用いて前記逆元 a^{-1} を生成して出力する出力部と、を備える。

発明の効果

[0013] 本開示によれば、逆元 a^{-1} を算出するための有限体上の二乗算を3回から2回に減らすことができる。つまり、ペアリング写像のための逆元算に要する計算量を削減できる。その結果、ペアリング暗号を効率化することができる。

図面の簡単な説明

- [0014] [図1]実施の形態1における逆元演算装置100の構成図。
[図2]実施の形態1における事前演算部120の構成図。
[図3]実施の形態1における逆元演算部130の構成図。
[図4]実施の形態1における逆元演算方法のフローチャート。
[図5]実施の形態1における事前演算処理(S120)のフローチャート。
[図6]実施の形態1における逆元演算処理(S130)のフローチャート。
[図7]実施の形態1における逆元演算装置100のハードウェア構成図。
[図8]実施の形態2における逆元演算装置200の構成図。
[図9]実施の形態2における事前演算部220の構成図。
[図10]実施の形態2における逆元演算部230の構成図。
[図11]実施の形態2における逆元演算方法のフローチャート。
[図12]実施の形態2における事前演算処理(S220)のフローチャート。
[図13]実施の形態2における逆元演算処理(S230)のフローチャート。
[図14]実施の形態2における逆元演算装置200のハードウェア構成図。

発明を実施するための形態

[0015] 実施の形態および図面において、同じ要素または対応する要素には同じ符号を付している。説明した要素と同じ符号が付された要素の説明は適宜に省略または簡略化する。図中の矢印はデータの流れ又は処理の流れを主に示している。

[0016] 実施の形態 1.

cyclotomic subgroup の元 a の逆元 a^{-1} を算出する形態について、図 1 から図 7 に基づいて説明する。

[0017] ***構成の説明***

図 1 に基づいて、逆元演算装置 100 の構成を説明する。

逆元演算装置 100 は、プロセッサ 101 とメモリ 102 と補助記憶装置 103 と通信装置 104 と入出力インタフェース 105 といったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。

[0018] プロセッサ 101 は、演算処理を行う IC であり、他のハードウェアを制御する。例えば、プロセッサ 101 は CPU である。

IC は、Integrated Circuit の略称である。

CPU は、Central Processing Unit の略称である。

[0019] メモリ 102 は揮発性または不揮発性の記憶装置である。メモリ 102 は、主記憶装置またはメインメモリとも呼ばれる。例えば、メモリ 102 は RAM である。メモリ 102 に記憶されたデータは必要に応じて補助記憶装置 103 に保存される。

RAM は、Random Access Memory の略称である。

[0020] 補助記憶装置 103 は不揮発性の記憶装置である。例えば、補助記憶装置 103 は、ROM、HDD またはフラッシュメモリである。補助記憶装置 103 に記憶されたデータは必要に応じてメモリ 102 にロードされる。

ROM は、Read Only Memory の略称である。

HDD は、Hard Disk Drive の略称である。

[0021] 通信装置 104 はレシーバ及びトランスミッタである。例えば、通信装置 104 は通信チップまたは NIC である。

NIC は、Network Interface Card の略称である。

[0022] 入出力インタフェース105は、入力装置および出力装置が接続されるポートである。例えば、入出力インタフェース105はUSB端子であり、入力装置はキーボードおよびマウスであり、出力装置はディスプレイである。

USBは、Universal Serial Busの略称である。

[0023] 逆元演算装置100は、受付部110と事前演算部120と逆元演算部130と出力部140といった要素を備える。これらの要素はソフトウェアで実現される。

[0024] 補助記憶装置103には、受付部110と事前演算部120と逆元演算部130と出力部140としてコンピュータを機能させるための逆元演算プログラムが記憶されている。逆元演算プログラムは、メモリ102にロードされて、プロセッサ101によって実行される。

補助記憶装置103には、さらに、OSが記憶されている。OSの少なくとも一部は、メモリ102にロードされて、プロセッサ101によって実行される。

プロセッサ101は、OSを実行しながら、逆元演算プログラムを実行する。

OSは、Operating Systemの略称である。

[0025] 逆元演算プログラムの入出力データは記憶部190に記憶される。

メモリ102は記憶部190として機能する。但し、補助記憶装置103、プロセッサ101内のレジスタおよびプロセッサ101内のキャッシュメモリなどの記憶装置が、メモリ102の代わりに、又は、メモリ102と共に、記憶部190として機能してもよい。

[0026] 逆元演算装置100は、プロセッサ101を代替する複数のプロセッサを備えてもよい。

[0027] 逆元演算プログラムは、光ディスクまたはフラッシュメモリ等の不揮発性の記録媒体にコンピュータ読み取り可能に記録（格納）することができる。

[0028] 図2に基づいて、事前演算部120の構成を説明する。

事前演算部120は、二乗算部121と第1乗算部122と加算部123

と減算部 1 2 4 と第 2 乗算部 1 2 5 といった要素を備える。これらの要素の機能を後述する。

[0029] 図 3 に基づいて、逆元演算部 1 3 0 の構成を説明する。

逆元演算部 1 3 0 は、第 1 演算部 1 3 1 と第 2 演算部 1 3 2 と第 3 演算部 1 3 3 といった要素を備える。これらの要素の機能を後述する。

[0030] ***前提の説明***

逆元演算装置 1 0 0 による逆元算の前提を説明する。

「 p 」は、素数である。

「 F_p 」は、要素数が p である体である。

「 k 」および「 n 」は、 $k = 3n$ を満たす整数である。

「 F_{p^n} 」と「 F_{p^k} 」は、それぞれ体 F_p の拡大体である。

「 α 」は、体 F_p の元である。

[0031] 拡大体 F_{p^n} と拡大体 F_{p^k} は、以下の式で表される。

$$F_{p^n} = F_p[v] / (v^n - \alpha),$$

$$F_{p^k} = F_{p^n}[w] / (w^3 - v).$$

[0032] 「 $G\Phi 3(p^n)$ 」は、位数が $\Phi 3(p^n)$ である拡大体 F_{p^k} の元の集合であり、`cyclotomic subgroup` とよぶ。ただし、 $\Phi m(x)$ は第 m 円分多項式である。

「 a 」は、集合 $G\Phi 3(p^n)$ の元である。つまり、「 a 」は、`cyclotomic subgroup` の元である。

「 a^{-1} 」は、元 a の逆元である。

「 a_0 」と「 a_1 」と「 a_2 」は、それぞれ拡大体 F_{p^n} の元である。

[0033] 元 a は、以下の式で表される。

$$a = a_0 + a_1 w + a_2 w^2 \in G\Phi 3(p^n)$$

[0034] 逆元「 a^{-1} 」は、以下の式で表される。

$$a^{-1} = (a_0^2 - a_1 a_2 v) + (a_2^2 v - a_0 a_1) w + (a_1^2 - a_0 a_2) w^2$$

[0035] ***動作の説明***

逆元演算装置 100 の動作の手順は逆元演算方法に相当する。また、逆元演算装置 100 の動作の手順は逆元演算プログラムによる処理の手順に相当する。

[0036] 図 4 に基づいて、逆元演算方法を説明する。

ステップ S 110 において、受付部 110 は、元 a を受け付ける。

例えば、元 a は、ペアリング写像の演算を行うペアリング写像装置またはペアリング暗号の演算を行うペアリング暗号装置から逆元演算装置 100 へ送信される。そして、受付部 110 は、元 a を受信する。

例えば、元 a は、利用者によって逆元演算装置 100 に入力される。そして、受付部 110 は、入力された元 a を受け付ける。

[0037] 元 a は、 a_0 と a_1 と a_2 を含み、以下の式で表される。

$$a = a_0 + a_1 w + a_2 w^2$$

[0038] ステップ S 120 において、事前演算部 120 は、 a_0 と a_1 と a_2 を用いて、 t_1 と t_2 と t_3 と t_4 と t_7 を算出する。

t_1 は、 a_0^2 の計算結果である。

t_2 は、 a_2^2 の計算結果である。

t_3 は、 $a_0 a_1$ の計算結果である。

t_4 は、 $a_1 a_2$ の計算結果である。

t_7 は、 $(a_0 + a_1)(a_1 - a_2)$ の計算結果に等しい。

X の計算結果は、 X を計算して得られる値である。

X の計算結果に等しい Y は、 X を計算して得られる値と同じ値であり、 X を計算せずに得られる。

ステップ S 120 の詳細を後述する。

[0039] ステップ S 130 において、逆元演算部 130 は、 t_1 と t_2 と t_3 と t_4 と t_7 を用いて、 b_0 と b_1 と b_2 を算出する。

b_0 は、 $a_0^2 - a_1 a_2 v$ の計算結果に等しい。

b_1 は、 $a_2^2 v - a_0 a_1$ の計算結果に等しい。

b_2 は、 $a_1^2 - a_0 a_2$ の計算結果に等しい。

ステップS 1 3 0の詳細を後述する。

[0040] ステップS 1 4 0において、出力部 1 4 0は、逆元 a^{-1} を出力する。

例えば、出力部 1 4 0は、元 a の送信元へ逆元 a^{-1} を送信する。または、出力部 1 4 0は、利用者に指定された記録媒体に逆元 a^{-1} を書き込む。

逆元 a^{-1} は、元 a の逆元であり、以下の式で表される。

$$a^{-1} = (a_0^2 - a_1 a_2 v) + (a_2^2 v - a_0 a_1) w + (a_1^2 - a_0 a_2) w^2$$

[0041] 図5に基づいて、事前演算処理 (S 1 2 0) を説明する。

ステップS 1 2 1において、二乗算部 1 2 1は a_0 を用いて二乗算を行う。具体的には、二乗算部 1 2 1は a_0^2 を計算する。これにより、 t_1 が算出される。

[0042] t_1 は、 a_0^2 の計算結果であり、以下のように表される。

$$t_1 \leftarrow a_0^2$$

[0043] ステップS 1 2 2において、二乗算部 1 2 1は a_2 を用いて二乗算を行う。

具体的には、二乗算部 1 2 1は a_2^2 を計算する。これにより、 t_2 が算出される。

[0044] t_2 は、 a_2^2 の計算結果であり、以下のように表される。

$$t_2 \leftarrow a_2^2$$

[0045] ステップS 1 2 3において、第1乗算部 1 2 2は、 a_0 と a_1 を用いて乗算を行う。具体的には、第1乗算部 1 2 2は $a_0 a_1$ を計算する。これにより、 t_3 が算出される。

[0046] t_3 は、 $a_0 a_1$ の計算結果であり、以下のように表される。

$$t_3 \leftarrow a_0 a_1$$

[0047] ステップS 1 2 4において、第1乗算部 1 2 2は、 a_1 と a_2 を用いて乗算を行う。具体的には、第1乗算部 1 2 2は $a_1 a_2$ を計算する。これにより、 t_4 が算出される。

[0048] t_4 は、 $a_1 a_2$ の計算結果であり、以下のように表される。

$$t_4 \leftarrow a_1 a_2$$

[0049] ステップS 1 2 5において、加算部1 2 3は、 a_0 と a_1 を用いて加算を行う。具体的には、加算部1 2 3は $a_0 + a_1$ を計算する。これにより、 t_5 が算出される。

[0050] t_5 は、 $a_0 + a_1$ の計算結果であり、以下のように表される。

$$t_5 \leftarrow a_0 + a_1$$

[0051] ステップS 1 2 6において、減算部1 2 4は、 a_1 と a_2 を用いて減算を行う。具体的には、減算部1 2 4は $a_1 - a_2$ を計算する。これにより、 t_6 が算出される。

[0052] t_6 は、 $a_1 - a_2$ の計算結果であり、以下のように表される。

$$t_6 \leftarrow a_1 - a_2$$

[0053] ステップS 1 2 7において、第2乗算部1 2 5は、 t_5 と t_6 を用いて乗算を行う。具体的には、第2乗算部1 2 5は $t_5 t_6$ を計算する。これにより、 t_7 が算出される。

[0054] t_7 は、 $t_5 t_6$ の計算結果であり、以下のように表される。

$$t_7 \leftarrow t_5 t_6 = (a_0 + a_1) (a_1 - a_2)$$

[0055] 図6に基づいて、逆元演算処理(S 1 3 0)を説明する。

ステップS 1 3 1において、第1演算部1 3 1は、 t_1 と t_4 を用いて減算を行う。

具体的には、第1演算部1 3 1は、 t_4 に v を掛けて $t_4 v$ を算出する。そして、第1演算部1 3 1は $t_1 - t_4 v$ を計算する。「 v 」は、あらかじめ決められた値である。

これにより、 b_0 が算出される。

[0056] b_0 は、 $t_1 - t_4 v$ の計算結果であり、以下のように表される。

$$b_0 \leftarrow t_1 - t_4 v = a_0^2 - a_1 a_2 v$$

[0057] ステップS 1 3 2において、第2演算部1 3 2は、 t_2 と t_3 を用いて減算を行う。

具体的には、第2演算部1 3 2は、 t_2 に v を掛けて $t_2 v$ を算出する。そして、第2演算部1 3 2は $t_2 v - t_3$ を計算する。

これにより、 b_1 が算出される。

[0058] b_1 は、 $t_2 v - t_3$ の計算結果であり、以下のように表される。

$$b_1 \leftarrow t_2 v - t_3 = a_2^2 v - a_0 a_1$$

[0059] ステップS133において、第3演算部133は、 t_3 と t_4 と t_7 を用いて加算および減算を行う。具体的には、第3演算部133は $t_7 - t_3 + t_4$ を計算する。これにより、 b_2 が算出される。

[0060] b_2 は、 $t_7 - t_3 + t_4$ の計算結果であり、以下のように表される。

$$\begin{aligned} b_2 &\leftarrow t_7 - t_3 + t_4 \\ &= (a_0 + a_1)(a_1 - a_2) - a_0 a_1 + a_1 a_2 \\ &= a_0 a_1 - a_0 a_2 + a_1^2 - a_1 a_2 - a_0 a_1 + a_1 a_2 \\ &= a_1^2 - a_0 a_2 \end{aligned}$$

[0061] ***実施の形態1の効果***

実施の形態1により、逆元 a^{-1} を算出するための有限体上の二乗算を3回から2回に減らすことができる。つまり、逆元算の高速化が可能である。その結果、ペアリング暗号の効率化が可能となる。

[0062] ***実施の形態1の補足***

図7に基づいて、逆元演算装置100のハードウェア構成を説明する。

逆元演算装置100は処理回路109を備える。

処理回路109は、受付部110と事前演算部120と逆元演算部130と出力部140とを実現するハードウェアである。

処理回路109は、専用のハードウェアであってもよいし、メモリ102に格納されるプログラムを実行するプロセッサ101であってもよい。

[0063] 処理回路109が専用のハードウェアである場合、処理回路109は、例えば、単回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ASIC、FPGAまたはこれらの組み合わせである。

ASICは、Application Specific Integrated Circuitの略称である。

FPGAは、Field Programmable Gate Arr

a y の略称である。

[0064] 逆元演算装置 100 は、処理回路 109 を代替する複数の処理回路を備えてもよい。

[0065] 処理回路 109 において、一部の機能が専用のハードウェアで実現されて、残りの機能がソフトウェアまたはファームウェアで実現されてもよい。

[0066] このように、逆元演算装置 100 の機能はハードウェア、ソフトウェア、ファームウェアまたはこれらの組み合わせで実現することができる。

[0067] 実施の形態 2.

cyclotomic subgroup の元 a の逆元 a^{-1} を算出する形態について、主に実施の形態 1 と異なる点を図 8 から図 14 に基づいて説明する。

[0068] ***構成の説明***

図 8 に基づいて、逆元演算装置 200 の構成を説明する。

逆元演算装置 200 は、実施の形態 1 における逆元演算装置 100 に相当する。

逆元演算装置 200 は、プロセッサ 201 とメモリ 202 と補助記憶装置 203 と通信装置 204 と入出力インタフェース 205 といったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。

[0069] プロセッサ 201 は、演算処理を行う IC であり、他のハードウェアを制御する。例えば、プロセッサ 201 は CPU である。

[0070] メモリ 202 は揮発性または不揮発性の記憶装置である。メモリ 202 は、主記憶装置またはメインメモリとも呼ばれる。例えば、メモリ 202 は RAM である。メモリ 202 に記憶されたデータは必要に応じて補助記憶装置 203 に保存される。

[0071] 補助記憶装置 203 は不揮発性の記憶装置である。例えば、補助記憶装置 203 は、ROM、HDD またはフラッシュメモリである。補助記憶装置 203 に記憶されたデータは必要に応じてメモリ 202 にロードされる。

[0072] 通信装置204はレシーバ及びトランスミッタである。例えば、通信装置204は通信チップまたはNICである。

[0073] 入出力インタフェース205は、入力装置および出力装置が接続されるポートである。例えば、入出力インタフェース205はUSB端子であり、入力装置はキーボードおよびマウスであり、出力装置はディスプレイである。

[0074] 逆元演算装置200は、受付部210と事前演算部220と逆元演算部230と出力部240といった要素を備える。これらの要素はソフトウェアで実現される。

[0075] 補助記憶装置203には、受付部210と事前演算部220と逆元演算部230と出力部240としてコンピュータを機能させるための逆元演算プログラムが記憶されている。逆元演算プログラムは、メモリ202にロードされて、プロセッサ201によって実行される。

補助記憶装置203には、さらに、OSが記憶されている。OSの少なくとも一部は、メモリ202にロードされて、プロセッサ201によって実行される。

プロセッサ201は、OSを実行しながら、逆元演算プログラムを実行する。

[0076] 逆元演算プログラムの入出力データは記憶部290に記憶される。

メモリ202は記憶部290として機能する。但し、補助記憶装置203、プロセッサ201内のレジスタおよびプロセッサ201内のキャッシュメモリなどの記憶装置が、メモリ202の代わりに、又は、メモリ202と共に、記憶部290として機能してもよい。

[0077] 逆元演算装置200は、プロセッサ201を代替する複数のプロセッサを備えてもよい。

[0078] 逆元演算プログラムは、光ディスクまたはフラッシュメモリ等の不揮発性の記録媒体にコンピュータ読み取り可能に記録（格納）することができる。

[0079] 図9に基づいて、事前演算部220の構成を説明する。

事前演算部220は、第1乗算部221と乗算部222と第1分数倍算

部 2 2 3 と演算部 2 2 4 と第 2 乗算部 2 2 5 と第 2 分数倍算部 2 2 6 といった要素を備える。これらの要素の機能を後述する。

[0080] 図 1 0 に基づいて、逆元演算部 2 3 0 の構成を説明する。

逆元演算部 2 3 0 は、第 1 演算部 2 3 1 と第 2 演算部 2 3 2 と第 3 演算部 2 3 3 といった要素を備える。これらの要素の機能を後述する。

[0081] ***前提の説明***

逆元演算装置 2 0 0 による逆元算の前提は、実施の形態 1 における前提と同じである。

[0082] ***動作の説明***

逆元演算装置 2 0 0 の動作の手順は逆元演算方法に相当する。また、逆元演算装置 2 0 0 の動作の手順は逆元演算プログラムによる処理の手順に相当する。

[0083] 図 1 1 に基づいて、逆元演算方法を説明する。

ステップ S 2 1 0 において、受付部 2 1 0 は、元 a を受け付ける。

$$a = a_0 + a_1 w + a_2 w^2$$

ステップ S 2 1 0 は、実施の形態 1 におけるステップ S 1 1 0 と同じである。

[0084] ステップ S 2 2 0 において、事前演算部 2 2 0 は、 a_0 と a_1 と a_2 を用いて、 t_1 と t_2 と t_3 と t_4 と t_7 を算出する。

t_1 は、 a_0^2 の計算結果である。

t_2 は、 a_2^2 の計算結果である。

t_3 は、 $a_0 a_1$ の計算結果である。

t_4 は、 $a_1 a_2$ の計算結果である。

t_7 は、 $a_0^2 + a_1^2 + a_2^2 / 4 + 2 a_0 a_1 - a_0 a_2 - a_1 a_2$ の計算結果に等しい。

t_8 は、 $a_2^2 / 4$ の計算結果に等しい。

ステップ S 2 2 0 の詳細を後述する。

[0085] ステップ S 2 3 0 において、逆元演算部 2 3 0 は、 t_1 と t_2 と t_3 と t_4 と

t_7 と t_8 を用いて、 b_0 と b_1 と b_2 を算出する。

b_0 は、 $a_0^2 - a_1 a_2 v$ の計算結果に等しい。

b_1 は、 $a_2^2 v - a_0 a_1$ の計算結果に等しい。

b_2 は、 $a_1^2 - a_0 a_2$ の計算結果に等しい。

ステップS230の詳細を後述する。

[0086] ステップS240において、出力部140は、逆元 a^{-1} を出力する。

$$a^{-1} = (a_0^2 - a_1 a_2 v) + (a_2^2 v - a_0 a_1) w + (a_1^2 - a_0 a_2) w^2$$

ステップS240は、実施の形態1におけるステップS140と同じである。

[0087] 図12に基づいて、事前演算処理(S220)を説明する。

ステップS221において、第1二乗算部221は、 a_0 を用いて二乗算を行う。具体的には、第1二乗算部221は a_0^2 を計算する。これにより、 t_1 が算出される。

[0088] t_1 は、 a_0^2 の計算結果であり、以下のように表される。

$$t_1 \leftarrow a_0^2$$

[0089] ステップS222において、第1二乗算部221は、 a_2 を用いて二乗算を行う。具体的には、第1二乗算部221は a_2^2 を計算する。これにより、 t_2 が算出される。

[0090] t_2 は、 a_2^2 の計算結果であり、以下のように表される。

$$t_2 \leftarrow a_2^2$$

[0091] ステップS223において、乗算部222は、 a_0 と a_1 を用いて乗算を行う。具体的には、乗算部222は $a_0 a_1$ を計算する。これにより、 t_3 が算出される。

[0092] t_3 は、 $a_0 a_1$ の計算結果であり、以下のように表される。

$$t_3 \leftarrow a_0 a_1$$

[0093] ステップS224において、乗算部222は、 a_1 と a_2 を用いて乗算を行う。具体的には、乗算部222は $a_1 a_2$ を計算する。これにより、 t_4 が算出

される。

[0094] t_4 は、 $a_1 a_2$ の計算結果であり、以下のように表される。

$$t_4 \leftarrow a_1 a_2$$

[0095] ステップ S 2 2 5 において、第 1 分数倍算部 2 2 3 は、 a_2 を用いて $1/2$ 倍算を行う。具体的には、第 1 分数倍算部 2 2 3 は $a_2/2$ を計算する。これにより、 t_5 が算出される。

[0096] t_5 は、 $a_2/2$ の計算結果であり、以下のように表される。

$$t_5 \leftarrow a_2/2$$

[0097] ステップ S 2 2 6 において、演算部 2 2 4 は、 a_0 と a_1 と t_5 を用いて加算及び減算を行う。具体的には、演算部 2 2 4 は $a_0 + a_1 - t_5$ を計算する。これにより、 t_6 が算出される。

[0098] t_6 は、 $a_0 + a_1 - t_5$ の計算結果であり、以下のように表される。

$$t_6 \leftarrow a_0 + a_1 - t_5 = a_0 + a_1 - a_2/2$$

[0099] ステップ S 2 2 7 において、第 2 二乗算部 2 2 5 は、 t_6 を用いて二乗算を行う。具体的には、第 2 二乗算部 2 2 5 は t_6^2 を計算する。これにより、 t_7 が算出される。

[0100] t_7 は、 t_6^2 の計算結果であり、以下のように表される。

$$\begin{aligned} t_7 &\leftarrow t_6^2 = (a_0 + a_1 - a_2/2)^2 \\ &= a_0^2 + a_0 a_1 - a_0 a_2/2 + a_0 a_1 + a_1^2 - a_1 a_2/2 - a_0 a_2/2 \\ &\quad - a_1 a_2/2 + a_2^2/4 \\ &= a_0^2 + a_1^2 + a_2^2/4 + 2 a_0 a_1 - a_0 a_2 - a_1 a_2 \end{aligned}$$

[0101] ステップ S 2 2 8 において、第 2 分数倍算部 2 2 6 は、 t_2 を用いて $1/4$ 倍算を行う。具体的には、第 2 分数倍算部 2 2 6 は $t_2/4$ を計算する。これにより、 t_8 が算出される。

[0102] t_8 は、 $t_2/4$ の計算結果であり、以下のように表される。

$$t_8 \leftarrow t_2/4 = a_2^2/4$$

[0103] 図 1 3 に基づいて、逆元演算処理 (S 2 3 0) を説明する。

ステップ S 2 3 1 において、第 1 演算部 2 3 1 は、 t_1 と t_4 を用いて減算

を行う。

具体的には、第1演算部131は、 t_4 に v を掛けて $t_4 v$ を算出する。そして、第1演算部131は $t_1 - t_4 v$ を計算する。

これにより、 b_0 が算出される。

b_0 は、 $a_0^2 - a_1 a_2 v$ の計算結果であり、以下のように表される。

$$b_0 \leftarrow t_1 - t_4 v = a_0^2 - a_1 a_2 v$$

[0104] ステップS232において、第2演算部232は、 t_2 と t_3 を用いて減算を行う。

具体的には、第2演算部132は、 t_2 に v を掛けて $t_2 v$ を算出する。そして、第2演算部132は $t_2 v - t_3$ を計算する。

これにより、 b_1 が算出される。

[0105] b_1 は、 $t_2 v - t_3$ の計算結果であり、以下のように表される。

$$b_1 \leftarrow t_2 v - t_3 = a_2^2 v - a_0 a_1$$

[0106] ステップS233において、第3演算部233は、 t_1 と t_3 と t_4 と t_7 と t_8 を用いて加算および減算を行う。具体的には、第3演算部233は $t_7 - t_1 - t_8 - 2t_3 + t_4$ を計算する。これにより、 b_2 が算出される。

[0107] b_2 は、 $t_7 - t_1 - t_8 - 2t_3 + t_4$ の計算結果であり、以下のように表される。

$$\begin{aligned} b_2 &\leftarrow t_7 - t_1 - t_8 - 2t_3 + t_4 \\ &= a_0^2 + a_1^2 + a_2^2 / 4 + 2a_0 a_1 - a_0 a_2 - a_1 a_2 - a_0^2 - a_2^2 / 4 - 2a_0 a_1 + a_1 a_2 \\ &= a_1^2 - a_0 a_2 \end{aligned}$$

[0108] ***実施の形態2の効果***

実施の形態2により、逆元 a^{-1} を算出するための有限体上の乗算を3回から2回に減らすことができる。つまり、逆元算の高速化が可能である。その結果、ペアリング暗号の効率化が可能となる。

[0109] ***実施の形態2の補足***

図14に基づいて、逆元演算装置200のハードウェア構成を説明する。

逆元演算装置 200 は処理回路 209 を備える。

処理回路 209 は、受付部 210 と事前演算部 220 と逆元演算部 230 と出力部 240 とを実現するハードウェアである。

処理回路 209 は、専用のハードウェアであってもよいし、メモリ 202 に格納されるプログラムを実行するプロセッサ 201 であってもよい。

[0110] 処理回路 209 が専用のハードウェアである場合、処理回路 209 は、例えば、単回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ASIC、FPGA またはこれらの組み合わせである。

[0111] 逆元演算装置 200 は、処理回路 209 を代替する複数の処理回路を備えてもよい。

[0112] 処理回路 209 において、一部の機能が専用のハードウェアで実現されて、残りの機能がソフトウェアまたはファームウェアで実現されてもよい。

[0113] このように、逆元演算装置 200 の機能はハードウェア、ソフトウェア、ファームウェアまたはこれらの組み合わせで実現することができる。

[0114] ***実施の形態の補足***

各実施の形態は、好ましい形態の例示であり、本開示の技術的範囲を制限することを意図するものではない。各実施の形態は、部分的に実施してもよいし、他の形態と組み合わせて実施してもよい。フローチャート等を用いて説明した手順は、適宜に変更してもよい。

逆元演算装置（100、200）の要素である「部」は、「処理」または「工程」と読み替えてもよい。

符号の説明

[0115] 100 逆元演算装置、101 プロセッサ、102 メモリ、103 補助記憶装置、104 通信装置、105 入出力インタフェース、109 処理回路、110 受付部、120 事前演算部、121 二乗算部、122 第1乗算部、123 加算部、124 減算部、125 第2乗算部、130 逆元演算部、131 第1演算部、132 第2演算部、133 第3演算部、140 出力部、190 記憶部、200 逆元演算装置、

201 プロセッサ、202 メモリ、203 補助記憶装置、204 通信装置、205 入出力インタフェース、209 処理回路、210 受付部、220 事前演算部、221 第1二乗算部、222 乗算部、223 第1分数倍算部、224 演算部、225 第2二乗算部、226 第2分数倍算部、230 逆元演算部、231 第1演算部、232 第2演算部、233 第3演算部、240 出力部、290 記憶部。

請求の範囲

[請求項1] 元 a の逆元 a^{-1} を算出する逆元演算装置であり、
 前記元 a は、 $a = a_0 + a_1 w + a_2 w^2$ で表され、
 前記逆元 a^{-1} は、 $a^{-1} = (a_0^2 - a_1 a_2 v) + (a_2^2 v - a_0 a_1) w + (a_1^2 - a_0 a_2) w^2$ で表され、
 前記逆元演算装置は、
 前記元 a を受け付ける受付部と、
 a_0 と a_1 と a_2 を用いて、 a_0^2 の計算結果である t_1 と、 a_2^2 の計算結果である t_2 と、 $a_0 a_1$ の計算結果である t_3 と、 $a_1 a_2$ の計算結果である t_4 と、 $(a_0 + a_1)(a_1 - a_2)$ の計算結果に等しい t_7 と、を算出する事前演算部と、
 t_1 と t_2 と t_3 と t_4 と t_7 を用いて、 $a_0^2 - a_1 a_2 v$ の計算結果に等しい b_0 と、 $a_2^2 v - a_0 a_1$ の計算結果に等しい b_1 と、 $a_1^2 - a_0 a_2$ の計算結果に等しい b_2 と、を算出する逆元演算部と、
 b_0 と b_1 と b_2 を用いて前記逆元 a^{-1} を生成して出力する出力部と、
 、
 を備える逆元演算装置。

[請求項2] 前記事前演算部は、
 a_0 を用いて二乗算を行って a_0^2 の計算結果である t_1 を算出し、
 a_2 を用いて二乗算を行って a_2^2 の計算結果である t_2 を算出する二乗算部と、
 a_0 と a_1 を用いて乗算を行って $a_0 a_1$ の計算結果である t_3 を算出し、
 a_1 と a_2 を用いて乗算を行って $a_1 a_2$ の計算結果である t_4 を算出する第1乗算部と、
 a_0 と a_1 を用いて加算を行って $a_0 + a_1$ の計算結果である t_5 を算出する加算部と、
 a_1 と a_2 を用いて減算を行って $a_1 - a_2$ の計算結果である t_6 を算出する減算部と、

t_5 と t_6 を用いて乗算を行って $(a_0 + a_1)(a_1 - a_2)$ の計算結果に等しい t_7 を算出する第2乗算部と、を備える
請求項1に記載の逆元演算装置。

[請求項3] 前記第2乗算部は、 $t_5 t_6$ を計算することによって t_7 を算出する
請求項2に記載の逆元演算装置。

[請求項4] 前記逆元演算部は、
 t_1 と t_4 を用いて減算を行って $a_0^2 - a_1 a_2 v$ の計算結果に等しい b_0 を算出する第1演算部と、
 t_2 と t_3 を用いて減算を行って $a_2^2 v - a_0 a_1$ の計算結果に等しい b_1 を算出する第2演算部と、
 t_3 と t_4 と t_7 を用いて加算および減算を行って $a_1^2 - a_0 a_2$ の計算結果に等しい b_2 を算出する第3演算部と、を備える
請求項1から請求項3のいずれか1項に記載の逆元演算装置。

[請求項5] 前記第1演算部は、 $t_1 - t_4 v$ を計算することによって b_0 を算出し、
前記第2演算部は、 $t_2 v - t_3$ を計算することによって b_1 を算出し、
前記第3演算部は、 $t_7 - t_3 + t_4$ を計算することによって b_2 を算出する
請求項4に記載の逆元演算装置。

[請求項6] 元 a の逆元 a^{-1} を算出する逆元演算方法であり、
前記元 a は、 $a = a_0 + a_1 w + a_2 w^2$ で表され、
前記逆元 a^{-1} は、 $a^{-1} = (a_0^2 - a_1 a_2 v) + (a_2^2 v - a_0 a_1) w + (a_1^2 - a_0 a_2) w^2$ で表され、
受付部が、前記元 a を受け付け、
事前演算部が、 a_0 と a_1 と a_2 を用いて、 a_0^2 の計算結果である t_1 と、 a_2^2 の計算結果である t_2 と、 $a_0 a_1$ の計算結果である t_3 と、 $a_1 a_2$ の計算結果である t_4 と、 $(a_0 + a_1)(a_1 - a_2)$ の計算結

果に等しい t_7 と、を算出し、

逆元演算部が、 t_1 と t_2 と t_3 と t_4 と t_7 を用いて、 $a_0^2 - a_1 a_2 v$ の計算結果に等しい b_0 と、 $a_2^2 v - a_0 a_1$ の計算結果に等しい b_1 と、 $a_1^2 - a_0 a_2$ の計算結果に等しい b_2 と、を算出し、

出力部が、 b_0 と b_1 と b_2 を用いて前記逆元 a^{-1} を生成して出力する

逆元演算方法。

[請求項7]

元 a の逆元 a^{-1} を算出するための逆元演算プログラムであり、

前記元 a は、 $a = a_0 + a_1 w + a_2 w^2$ で表され、

前記逆元 a^{-1} は、 $a^{-1} = (a_0^2 - a_1 a_2 v) + (a_2^2 v - a_0 a_1) w + (a_1^2 - a_0 a_2) w^2$ で表され、

前記逆元演算プログラムは、

前記元 a を受け付ける受付処理と、

a_0 と a_1 と a_2 を用いて、 a_0^2 の計算結果である t_1 と、 a_2^2 の計算結果である t_2 と、 $a_0 a_1$ の計算結果である t_3 と、 $a_1 a_2$ の計算結果である t_4 と、 $(a_0 + a_1)(a_1 - a_2)$ の計算結果に等しい t_7 と、を算出する事前演算処理と、

t_1 と t_2 と t_3 と t_4 と t_7 を用いて、 $a_0^2 - a_1 a_2 v$ の計算結果に等しい b_0 と、 $a_2^2 v - a_0 a_1$ の計算結果に等しい b_1 と、 $a_1^2 - a_0 a_2$ の計算結果に等しい b_2 と、を算出する逆元演算処理と、

b_0 と b_1 と b_2 を用いて前記逆元 a^{-1} を生成して出力する出力処理と、

をコンピュータに実行させるための逆元演算プログラム。

[請求項8]

元 a の逆元 a^{-1} を算出する逆元演算装置であり、

前記元 a は、 $a = a_0 + a_1 w + a_2 w^2$ で表され、

前記逆元 a^{-1} は、 $a^{-1} = (a_0^2 - a_1 a_2 v) + (a_2^2 v - a_0 a_1) w + (a_1^2 - a_0 a_2) w^2$ で表され、

前記逆元演算装置は、

前記元 a を受け付ける受付部と、

a_0 と a_1 と a_2 を用いて、 a_0^2 の計算結果である t_1 と、 a_2^2 の計算結果である t_2 と、 $a_0 a_1$ の計算結果である t_3 と、 $a_1 a_2$ の計算結果である t_4 と、 $a_0^2 + a_1^2 + a_2^2 / 4 + 2 a_0 a_1 - a_0 a_2 - a_1 a_2$ の計算結果に等しい t_7 と、 $a_2^2 / 4$ の計算結果に等しい t_8 を算出する事前演算部と、

t_1 と t_2 と t_3 と t_4 と t_7 と t_8 を用いて、 $a_0^2 - a_1 a_2 v$ の計算結果に等しい b_0 と、 $a_2^2 v - a_0 a_1$ の計算結果に等しい b_1 と、 $a_1^2 - a_0 a_2$ の計算結果に等しい b_2 と、を算出する逆元演算部と、

b_0 と b_1 と b_2 を用いて前記逆元 a^{-1} を生成して出力する出力部と、
を備える逆元演算装置。

[請求項9]

前記事前演算部は、

a_0 を用いて二乗算を行って a_0^2 の計算結果である t_1 を算出し、
 a_2 を用いて二乗算を行って a_2^2 の計算結果である t_2 を算出する第1二乗算部と、

a_0 と a_1 を用いて乗算を行って $a_0 a_1$ の計算結果である t_3 を算出し、
 a_1 と a_2 を用いて乗算を行って $a_1 a_2$ の計算結果である t_4 を算出する乗算部と、

a_2 を用いて $1 / 2$ 倍算を行って $a_2 / 2$ の計算結果である t_5 を算出する第1分数倍算部と、

a_0 と a_1 と t_5 を用いて加算および減算を行って $a_0 + a_1 - a_2 / 2$ の計算結果に等しい t_6 を算出する演算部と、

t_6 を用いて二乗算を行って $a_0^2 + a_1^2 + a_2^2 / 4 + 2 a_0 a_1 - a_0 a_2 - a_1 a_2$ の計算結果に等しい t_7 を算出する第2二乗算部と、

t_2 を用いて $1 / 4$ 倍算を行って $a_2^2 / 4$ の計算結果に等しい t_8 を算出する第2分数倍算部と、を備える

請求項8に記載の逆元演算装置。

[請求項10] 前記演算部は、 $a_0 + a_1 - t_5$ を計算することによって t_6 を算出し、

前記第2乗算部は、 t_6^2 を計算することによって t_7 を算出し、

前記第2分数倍算部は、 $t_2 / 4$ を計算することによって t_8 を算出する

請求項9に記載の逆元演算装置。

[請求項11] 前記逆元演算部は、

t_1 と t_4 を用いて減算を行って $a_0^2 - a_1 a_2 v$ の計算結果に等しい b_0 を算出する第1演算部と、

t_2 と t_3 を用いて減算を行って $a_2^2 v - a_0 a_1$ の計算結果に等しい b_1 を算出する第2演算部と、

t_1 と t_3 と t_4 と t_7 と t_8 を用いて加算および減算を行って $a_1^2 - a_0 a_2$ の計算結果に等しい b_2 を算出する第3演算部と、を備える
請求項8から請求項10のいずれか1項に記載の逆元演算装置。

[請求項12] 前記第1演算部は、 $t_1 - t_4 v$ を計算することによって b_0 を算出し、

前記第2演算部は、 $t_2 v - t_3$ を計算することによって b_1 を算出し、

前記第3演算部は、 $t_7 - t_1 - t_8 - 2 t_3 - t_4$ を計算することによって b_2 を算出する

請求項11に記載の逆元演算装置。

[請求項13] 元 a の逆元 a^{-1} を算出する逆元演算方法であり、

前記元 a は、 $a = a_0 + a_1 w + a_2 w^2$ で表され、

前記逆元 a^{-1} は、 $a^{-1} = (a_0^2 - a_1 a_2 v) + (a_2^2 v - a_0 a_1) w + (a_1^2 - a_0 a_2) w^2$ で表され、

受付部が、前記元 a を受け付け、

事前演算部が、 a_0 と a_1 と a_2 を用いて、 a_0^2 の計算結果である t_1 と、 a_2^2 の計算結果である t_2 と、 $a_0 a_1$ の計算結果である t_3 と、

$a_1 a_2$ の計算結果である t_4 と、 $a_0^2 + a_1^2 + a_2^2 / 4 + 2 a_0 a_1 - a_0 a_2 - a_1 a_2$ の計算結果に等しい t_7 と、 $a_2^2 / 4$ の計算結果に等しい t_8 を算出し、

逆元演算部が、 t_1 と t_2 と t_3 と t_4 と t_7 と t_8 を用いて、 $a_0^2 - a_1 a_2 v$ の計算結果に等しい b_0 と、 $a_2^2 v - a_0 a_1$ の計算結果に等しい b_1 と、 $a_1^2 - a_0 a_2$ の計算結果に等しい b_2 と、を算出し、

出力部が、 b_0 と b_1 と b_2 を用いて前記逆元 a^{-1} を生成して出力する

逆元演算方法。

[請求項14]

元 a の逆元 a^{-1} を算出するための逆元演算プログラムであり、

前記元 a は、 $a = a_0 + a_1 w + a_2 w^2$ で表され、

前記逆元 a^{-1} は、 $a^{-1} = (a_0^2 - a_1 a_2 v) + (a_2^2 v - a_0 a_1) w + (a_1^2 - a_0 a_2) w^2$ で表され、

前記逆元演算プログラムは、

前記元 a を受け付ける受付処理と、

a_0 と a_1 と a_2 を用いて、 a_0^2 の計算結果である t_1 と、 a_2^2 の計算結果である t_2 と、 $a_0 a_1$ の計算結果である t_3 と、 $a_1 a_2$ の計算結果である t_4 と、 $a_0^2 + a_1^2 + a_2^2 / 4 + 2 a_0 a_1 - a_0 a_2 - a_1 a_2$ の計算結果に等しい t_7 と、 $a_2^2 / 4$ の計算結果に等しい t_8 を算出する事前演算処理と、

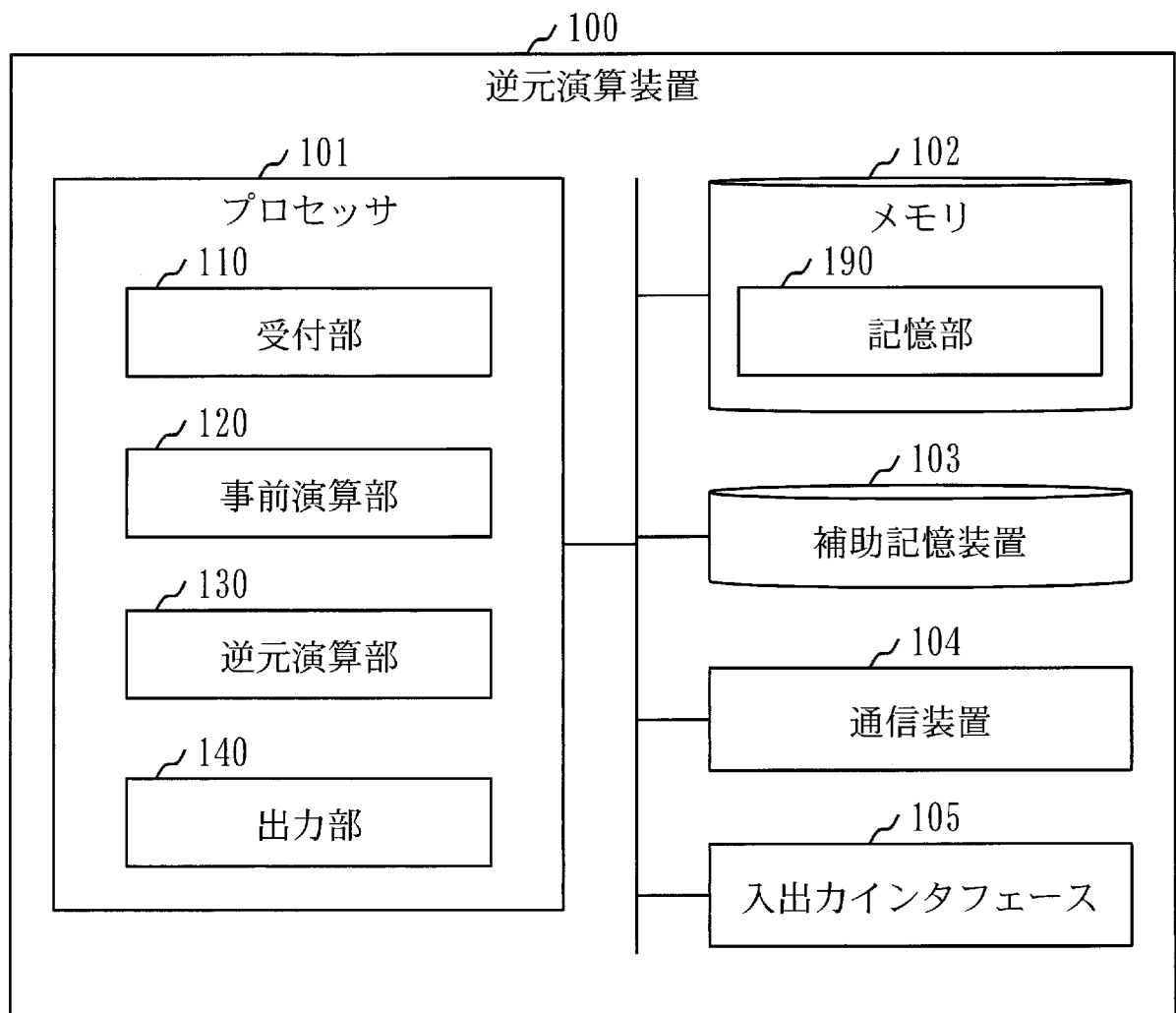
t_1 と t_2 と t_3 と t_4 と t_7 と t_8 を用いて、 $a_0^2 - a_1 a_2 v$ の計算結果に等しい b_0 と、 $a_2^2 v - a_0 a_1$ の計算結果に等しい b_1 と、 $a_1^2 - a_0 a_2$ の計算結果に等しい b_2 と、を算出する逆元演算処理と、

b_0 と b_1 と b_2 を用いて前記逆元 a^{-1} を生成して出力する出力処理と、

をコンピュータに実行させるための逆元演算プログラム。

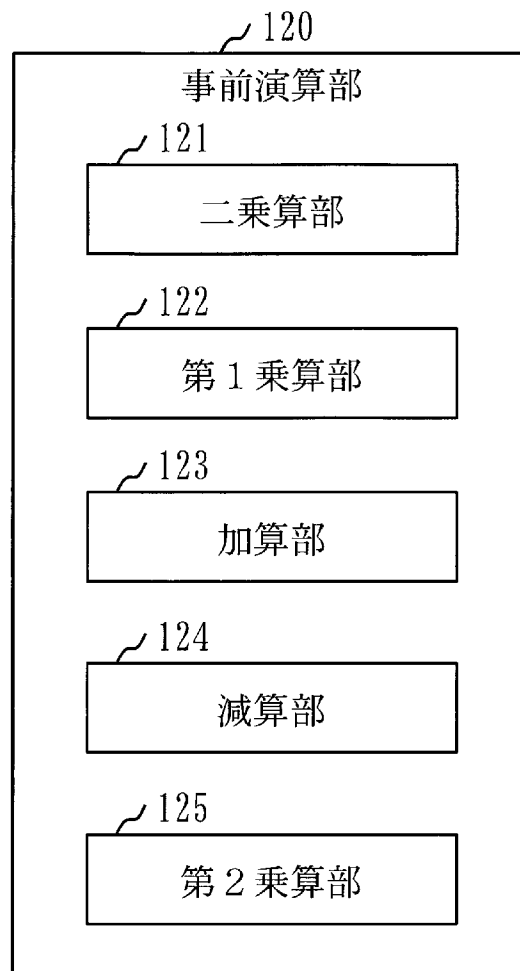
[図1]

図1



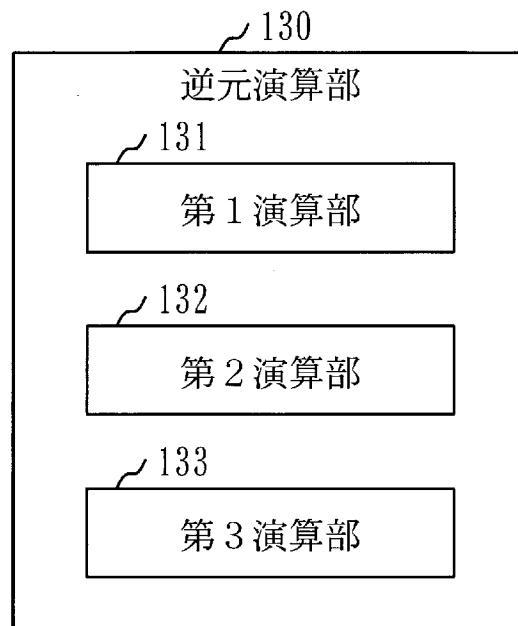
[図2]

図2



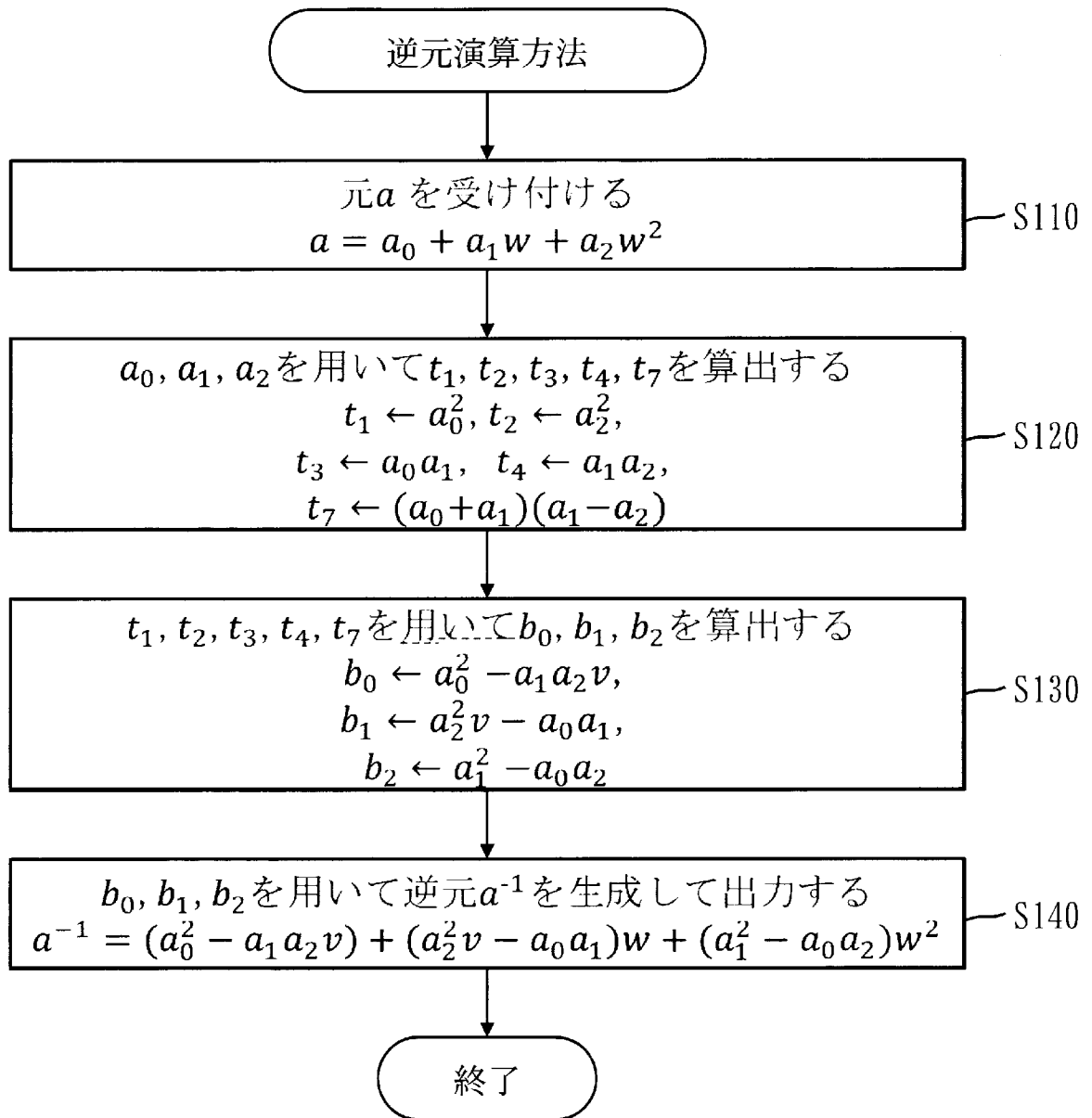
[図3]

図3



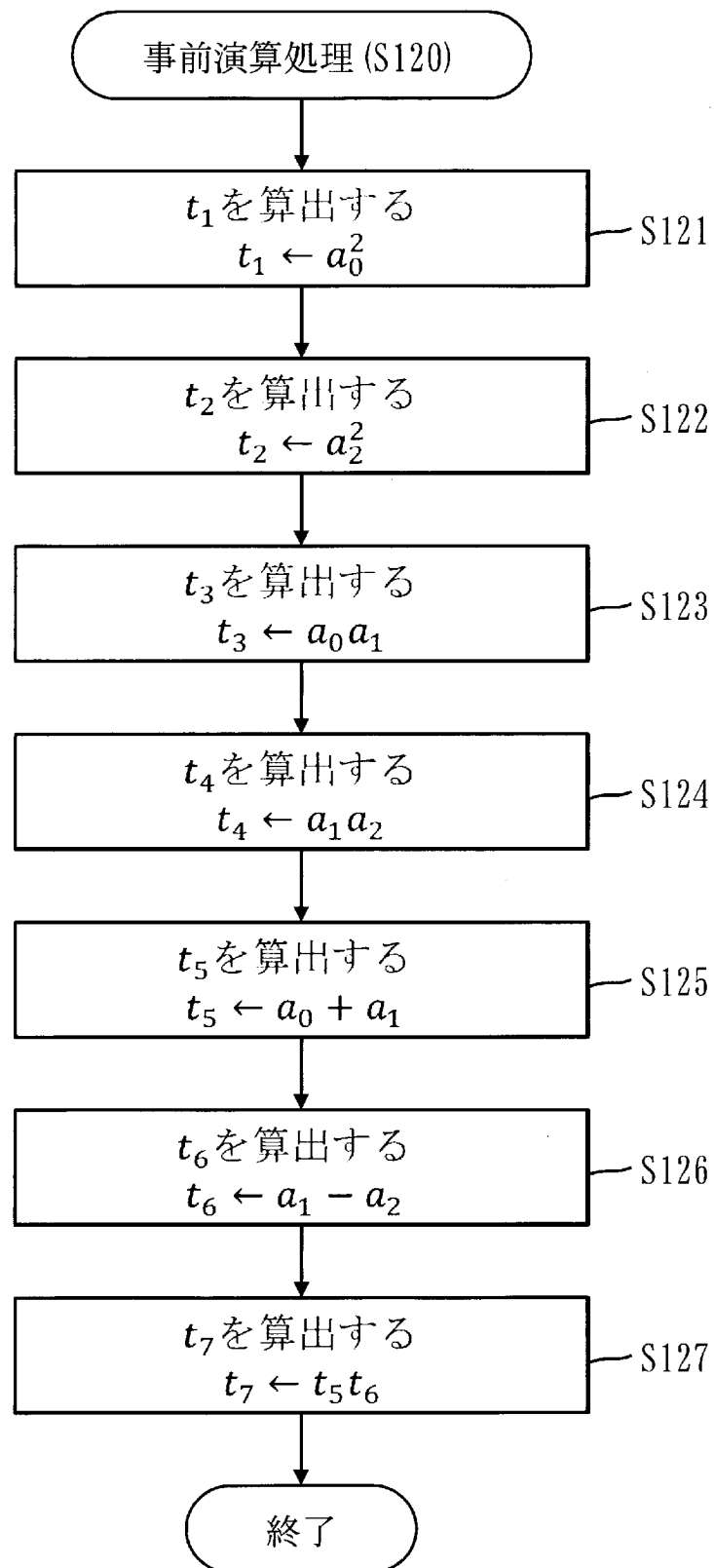
[図4]

図4



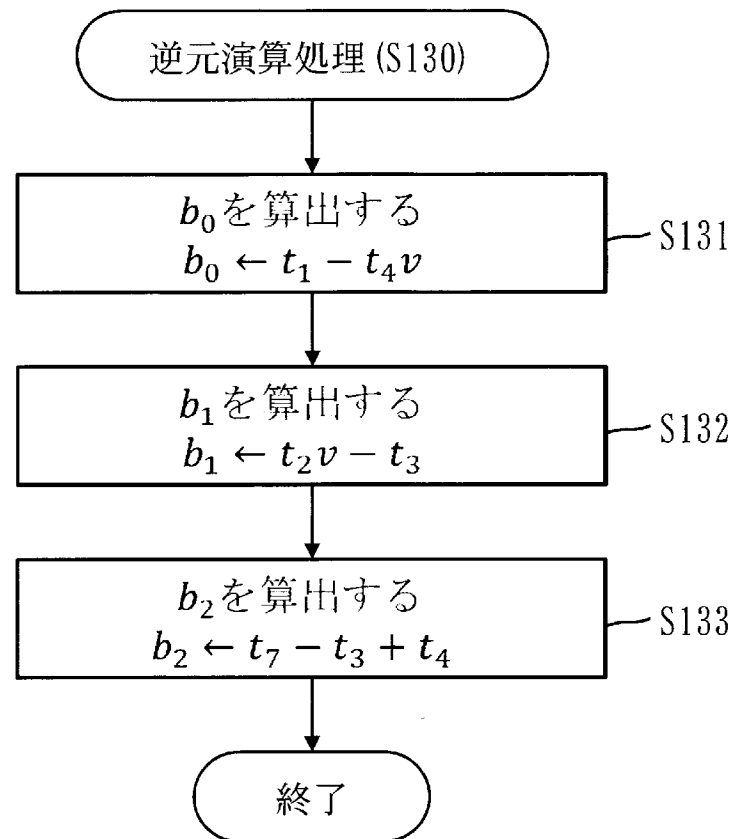
[図5]

図5



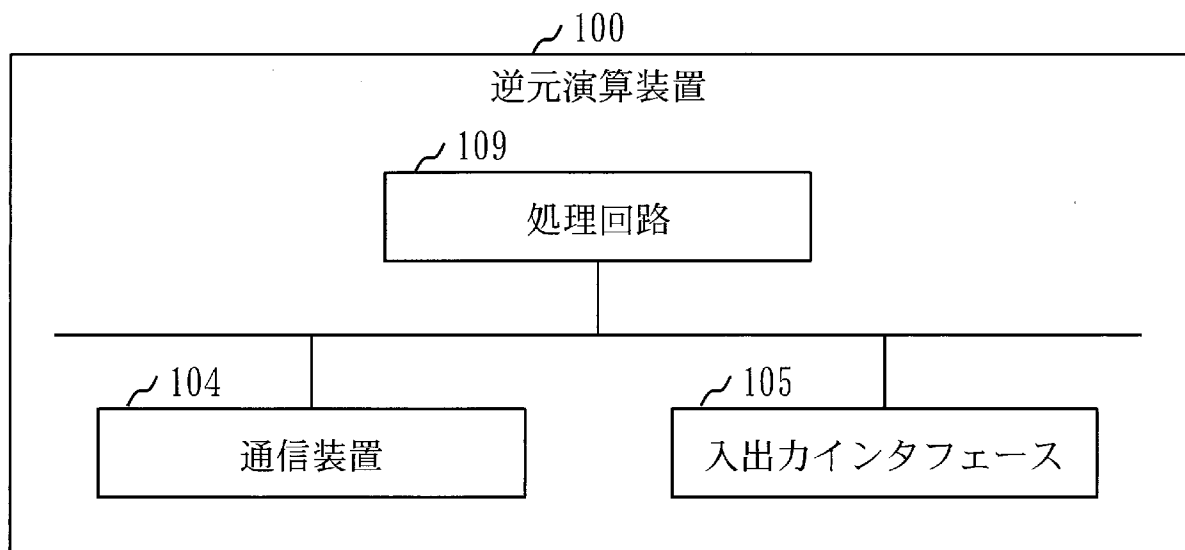
[図6]

図6



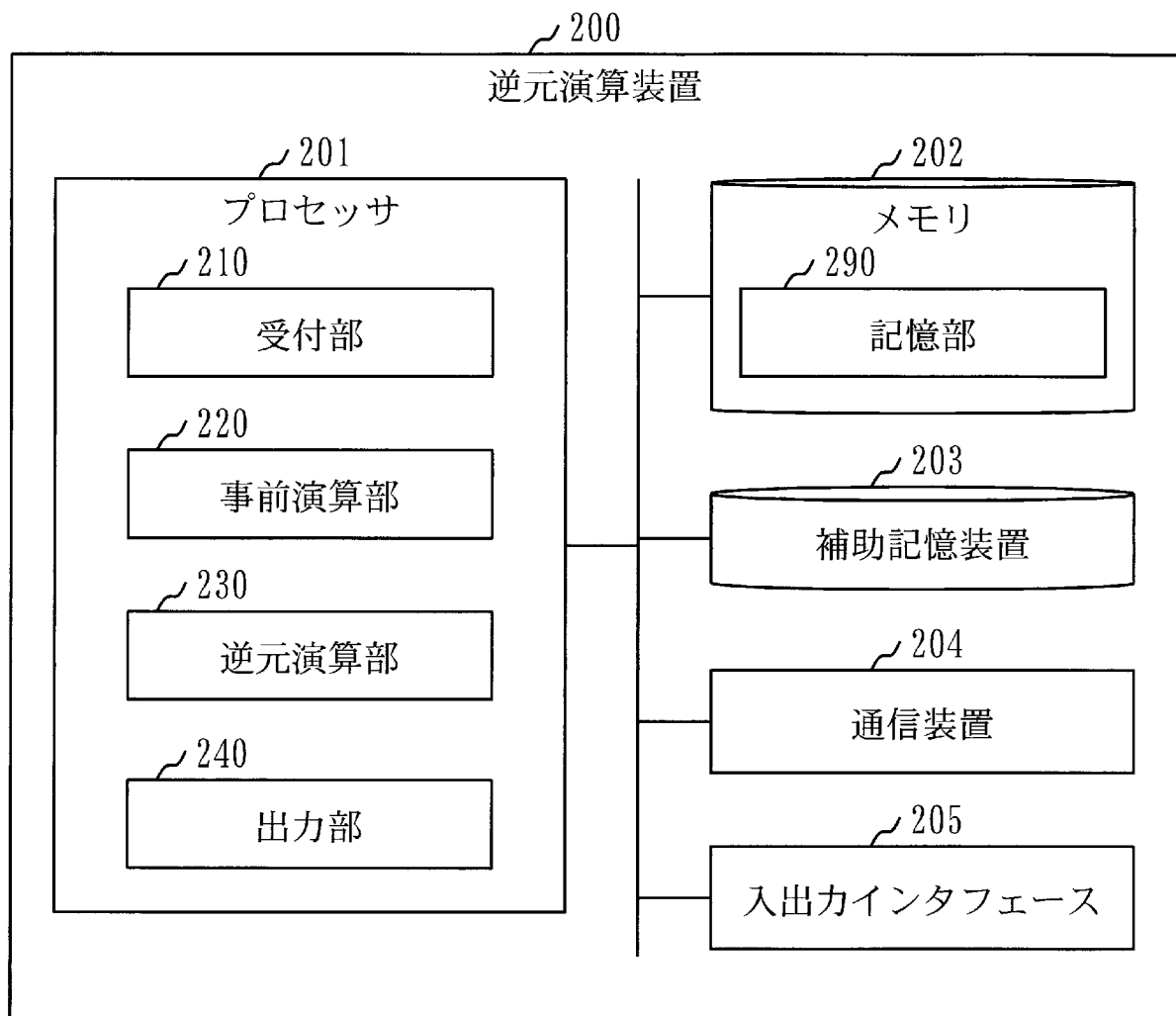
[図7]

図7



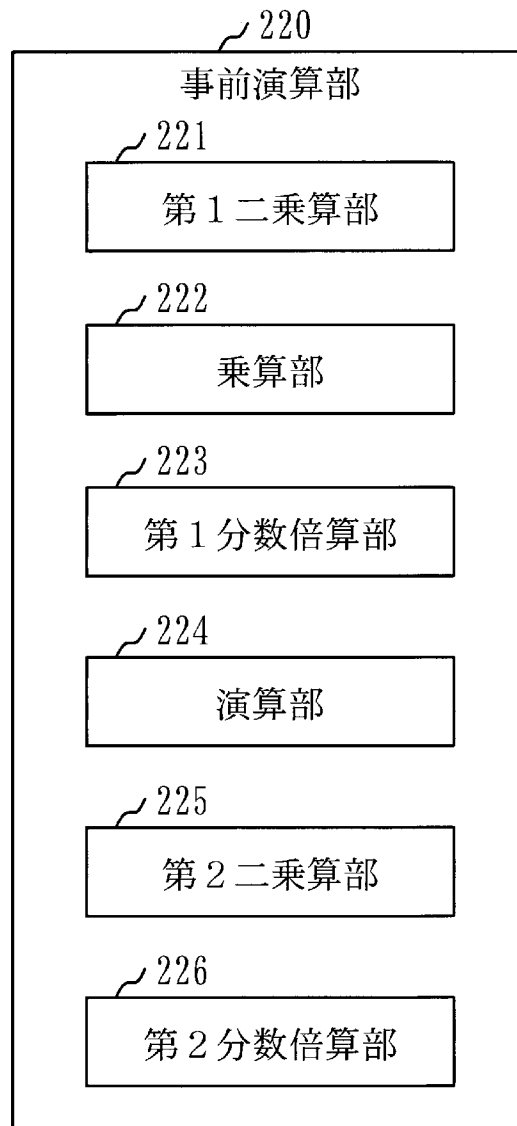
[図8]

図8



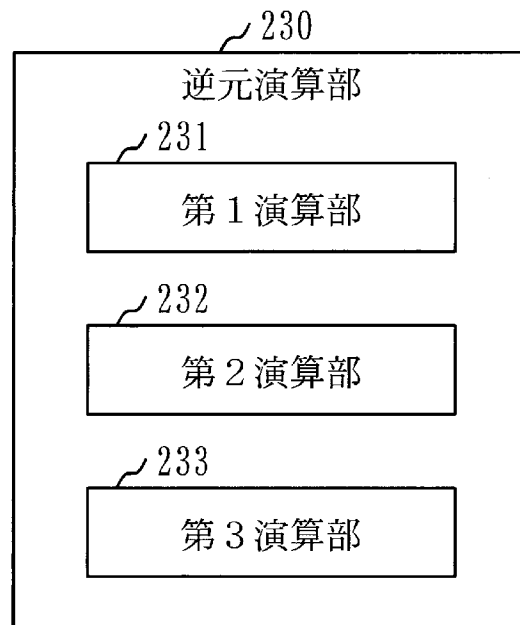
[図9]

図9



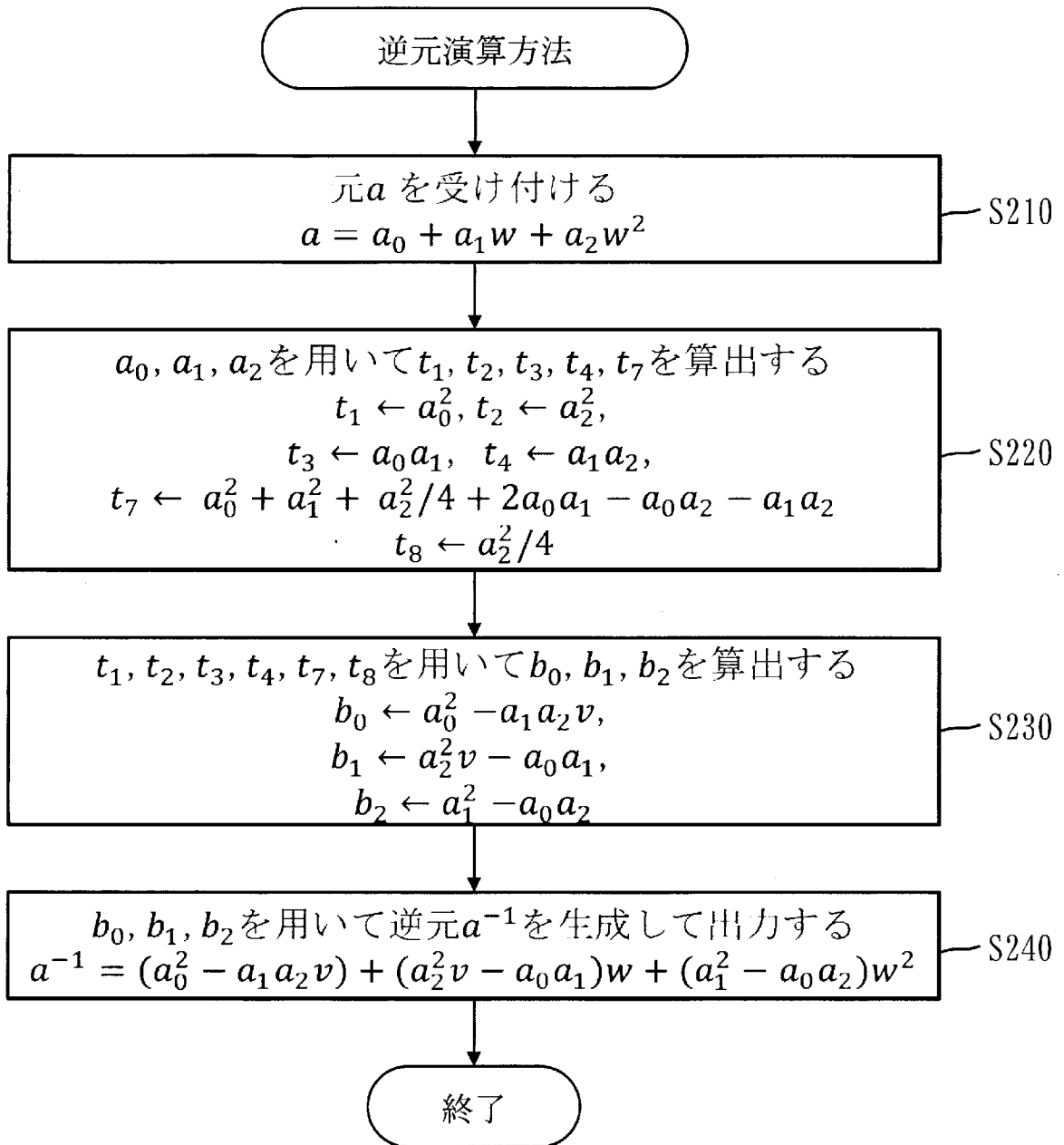
[図10]

図10



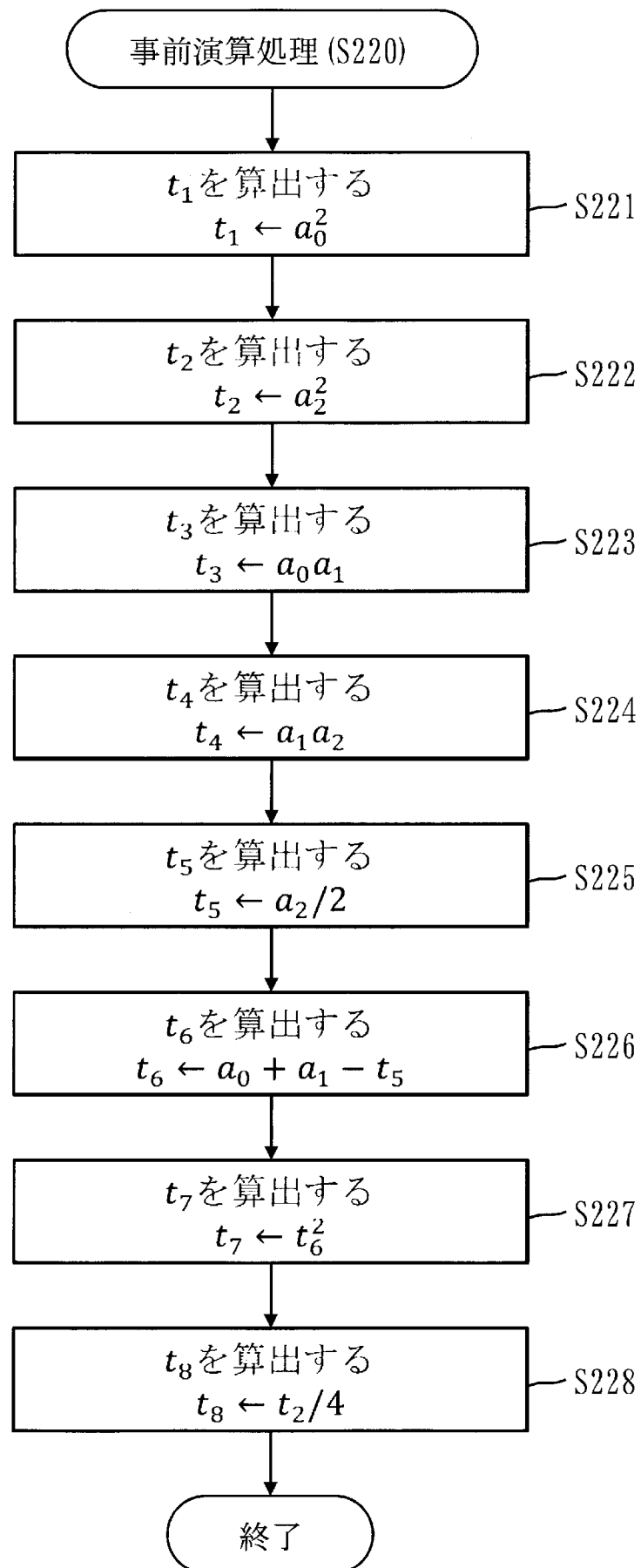
[図11]

図11



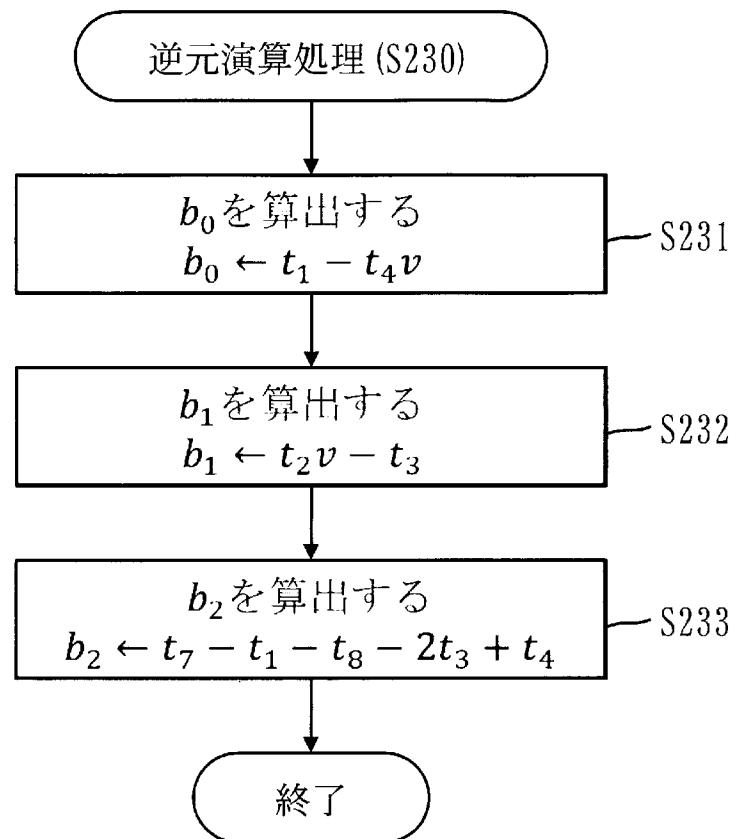
[図12]

図12



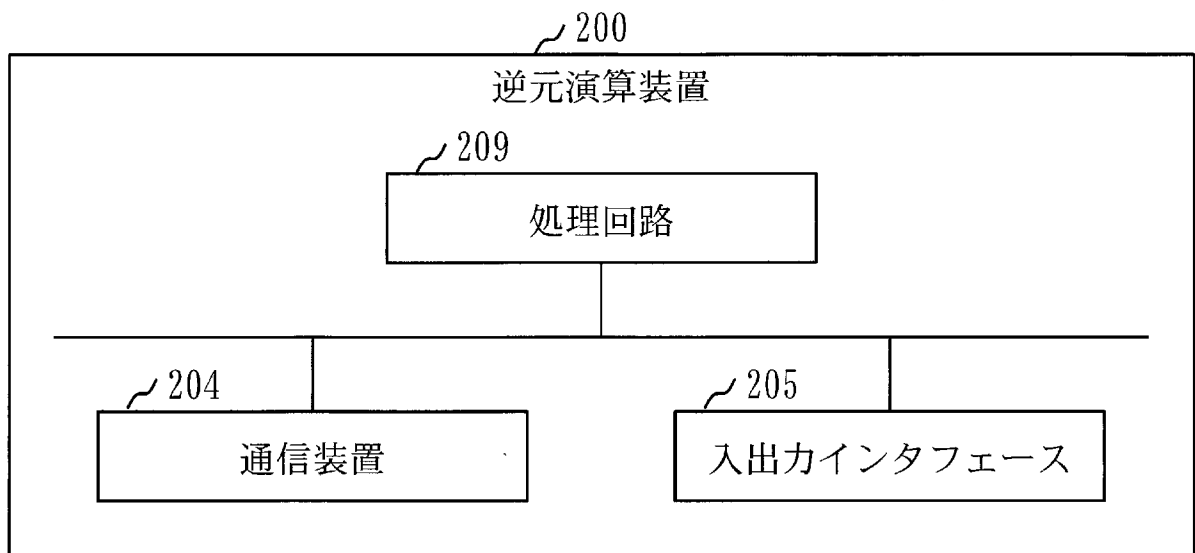
[図13]

図13



[図14]

図14



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/026860

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. G09C1/00 (2006.01) i

FI: C09C1/00 650A

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)

Int. Cl. G09C1/00

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

Published examined utility model applications of Japan 1922-1996

Published unexamined utility model applications of Japan 1971-2020

Registered utility model specifications of Japan 1996-2020

Published registered utility model applications of Japan 1994-2020

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	FOUOTSA, Emmanuel et al. Optimal Ate Pairing on Elliptic Curves with Embedding Degree 9, 15 and 27, arXiv [online], 16 April 2020, 2002.11920v2, pp. 1-25, [retrieved on 17 September 2020], Retrieved from the Internet: <URL: https://arxiv.org/abs/2002.11920v2 > in particular, pp. 20-25	1-14



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

17.09.2020

Date of mailing of the international search report

29.09.2020

Name and mailing address of the ISA/

Japan Patent Office

3-4-3, Kasumigaseki, Chiyoda-ku,

Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/026860

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	TOURE, Mahamadou Abdou et al. Optimal Ate Pairing on Elliptic Curves with Embedding Degree 21. International Journal of Science and Reserch (IJSR) [online], November 2019, vol. 8, issue 11, pp. 1659-1666, [retrieved on 17 September 2020], Retrieved from the Internet: <URL: https://ijsr.net/get_abstract.php?paper_id=ART20203004 > in particular, p. 1661	1-14

A. 発明の属する分野の分類（国際特許分類（IPC）） G09C 1/00(2006.01)i FI: G09C1/00 650A		
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）） 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 1971-2020年 日本国実用新案登録公報 1996-2020年 日本国登録実用新案公報 1994-2020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	FOUOTSA, Emmanuel et al., Optimal Ate Pairing on Elliptic Curves with Embedding Degree 9, 15 and 27, arXiv [online], 2020.04.16, 2002.11920v2, pp. 1-25, [retrieved on 2020.09.17], Retrieved from the Internet: <URL: https://arxiv.org/abs/2002.11920v2> 特にpp. 20-25	1-14
A	TOURE, Mahamadou Abdou et al., Optimal Ate Pairing on Elliptic Curves with Embedding Degree 21, International Journal of Science and Research (IJSR) [online], 2019.11, Vol. 8, Issue 11, pp. 1659-1666, [retrieved on 2020.09.17], Retrieved from the Internet: <URL: https://ijsr.net/get_abstract.php?paper_id=ART20203004> 特にp. 1661	1-14
☐ 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抵触するものではなく、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 17.09.2020	国際調査報告の発送日 29.09.2020	
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 金沢 史明 5S 4538 電話番号 03-3581-1101 内線 3546	