(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
2017 年 2 月 2 日(02.02.2017)

WIPO | PCT

(10) 国際公開番号
WO 2017/018285 A1

(51) 国際特許分類:
*G06F 21/60* (2013.01) *G09C 1/00* (2006.01)
*G06F 21/64* (2013.01)

(21) 国際出願番号: PCT/JP2016/071221

(22) 国際出願日: 2016 年 7 月 20 日(20.07.2016)

(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 2015-147774 2015 年 7 月 27 日(27.07.2015) JP

(71) 出願人: 日本電信電話株式会社(NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 五十嵐 大(IKARASHI, Dai); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 千田 浩司(CHIDA, Koji); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 濱田 浩気(HAMADA, Koki); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 菊池 亮(KIKUCHI, Ryo); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP).

(74) 代理人: 中尾 直樹, 外(NAKAO, Naoki et al.); 〒1600022 東京都新宿区新宿三丁目１番２２号 新宿ＮＳＯビル６階 Tokyo (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,

[続葉有]

(54) **Title**: SECURE COMPUTATION SYSTEM, SECURE COMPUTATION APPARATUS, SECURE COMPUTATION METHOD, AND PROGRAM

(54) 発明の名称 : 秘密計算システム、秘密計算装置、秘密計算方法、およびプログラム

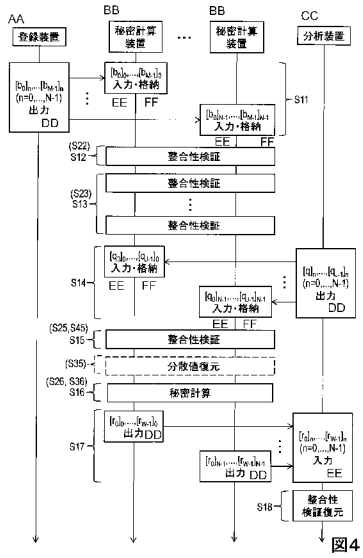



図4

S12, S13, S15 Consistency verification
S16 Secure computation
S18 Consistency verification restoration
S35 Sharing value restoration
AA Registration apparatus
BB Secure computation apparatus
CC Analysis apparatus
DD Output
EE Input
FF Store

(57) **Abstract**: In a secure computation apparatus according to the present invention, a secret sharing value of target data that is subject to secure computation is stored, and a query that requests the secure computation or a secret sharing value of the query is input. The secure computation apparatus performs consistency verification of the secret sharing value of the target data, performs consistency verification of the query or the secret sharing value of the query, performs, by using the secret sharing value of the target data that passed the consistency verification, secure computation according to the query or the secret sharing value of the query that passed the consistency verification so as to obtain a secret sharing value as a calculation result, and outputs the calculated secret sharing value.

(57) 要約: 秘密計算装置には、秘密計算の対象となる対象データの秘密分散値が格納され、秘密計算を要求するクエリまたはクエリの秘密分散値が入力される。秘密計算装置は、対象データの秘密分散値の整合性検証およびクエリまたはクエリの秘密分散値の整合性検証を行い、整合性検証に合格した対象データの秘密分散値を用い、整合性検証に合格したクエリまたはクエリの秘密分散値に応じた秘密計算を行って演算結果の秘密分散値を得、演算結果の秘密分散値を出力する。

WO 2017/018285 A1

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, IR, IS, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, 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, SM, ST, SV, SY, TH, 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, 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:

— 国際調査報告（条約第 21 条(3)）

# 明　細　書

## 発明の名称 ：

# 秘密計算システム、秘密計算装置、秘密計算方法、およびプログラム

## 技術分野

[0001]　本発明は、暗号技術を応用した情報セキュリティ技術に関し、特に、秘密計算技術に関する。

## 背景技術

[0002]　秘密分散値の改ざんを検知する技術として、検証可能秘密分散法（VSS: Verifiable secret sharing）がある（例えば、非特許文献１）。

## 先行技術文献

## 非特許文献

[0003] 非特許文献1：岡本龍明，山本博資，「現代暗号－シリーズ／情報科学の数学」，産業図書株式会社，１９９８年６月３０日，第２刷，ｐｐ．２１７－２１９．

## 発明の概要

## 発明が解決しようとする課題

[0004]　しかし、秘密計算装置に秘密計算の対象となる対象データの秘密分散値が格納され、秘密計算装置がこれらの対象データの秘密分散値を用い、入力されたクエリまたはクエリの秘密分散値に応じた秘密計算を行う場合に、改ざんによる不正を防止する方法は知られていない。

[0005]　本発明の課題は、秘密計算装置に秘密計算の対象となる対象データの秘密分散値が格納され、秘密計算装置がこれらの対象データの秘密分散値を用い、入力されたクエリまたはクエリの秘密分散値に応じた秘密計算を行う場合に、改ざんによる不正を防止することである。

## 課題を解決するための手段

[0006]　秘密計算装置には、秘密計算の対象となる対象データの秘密分散値が格納

され、秘密計算を要求するクエリまたはクエリの秘密分散値が入力される。秘密計算装置は、対象データの秘密分散値の整合性検証およびクエリまたはクエリの秘密分散値の整合性検証を行い、整合性検証に合格した対象データの秘密分散値を用い、整合性検証に合格したクエリまたはクエリの秘密分散値に応じた秘密計算を行って演算結果の秘密分散値を得、演算結果の秘密分散値を出力する。

## 発明の効果

[0007] これにより、秘密計算装置に秘密計算の対象となる対象データの秘密分散値が格納され、秘密計算装置がこれらの対象データの秘密分散値を用い、入力されたクエリまたはクエリの秘密分散値に応じた秘密計算を行う場合に、改ざんによる不正を防止できる。

## 図面の簡単な説明

[0008] [図1]図１は、実施形態の秘密計算システムの機能構成を例示したブロック図である。

[図2]図２Ａは、実施形態の秘密計算装置の機能構成を例示したブロック図である。図２Ｂは、実施形態の整合性検証部の機能構成を例示したブロック図である。

[図3]図３は、実施形態の分析装置の機能構成を例示したブロック図である。

[図4]図４は、実施形態の処理を例示したシーケンス図である。

[図5]図５は、実施形態の整合性検証処理を例示したフロー図である。

[図6]図６Ａおよび図６Ｂは、実施形態の処理を例示したフロー図である。

[図7]図７Ａおよび図７Ｂは、実施形態の処理を例示するための概念図である。

[図8]図８Ａおよび図８Ｂは、実施形態の処理を例示するための概念図である。

[図9]図９Ａおよび図９Ｂは、実施形態の処理を例示するための概念図である。

[図10]図１０Ａおよび図１０Ｂは、実施形態の処理を例示するための概念図

である。

## 発明を実施するための形態

[0009] 以下、本発明の実施形態を説明する。

［概要］

まず、実施形態の概要を説明する。

実施形態の秘密計算システムは、秘密計算の対象となる対象データの秘密分散値を出力する登録装置、複数個の秘密計算装置、およびクエリまたはクエリの秘密分散値を用いて秘密計算を要求する分析装置を有する。秘密計算装置のそれぞれには、登録装置から送られた対象データの秘密分散値が格納され、さらに分析装置から送られたクエリまたはクエリの秘密分散値が入力される。秘密計算装置は、対象データの秘密分散値の整合性検証およびクエリまたはクエリの秘密分散値の整合性検証を行い、整合性検証に合格した対象データの秘密分散値を用い、整合性検証に合格したクエリまたはクエリの秘密分散値に応じた秘密計算を行って演算結果の秘密分散値を得、演算結果の秘密分散値を出力する。これにより、登録装置、登録装置から秘密計算装置までの間、または秘密計算装置で対象データの秘密分散値が改ざんされたり、分析装置、または分析装置から秘密計算装置までの間でクエリまたはクエリの秘密分散値が改ざんされたりしても、その改ざんによって秘密計算装置から不正な結果が出力されることを防止できる。

[0010] 何れかの整合性検証が不合格であった場合、すべての対象データの秘密分散値の秘密計算装置への格納、および／または、すべてのクエリまたはクエリの秘密分散値の秘密計算装置への入力をやり直してもよい。あるいは、対象データの秘密分散値およびクエリまたはクエリの秘密分散値の両方の整合性検証が合格であった一部の秘密計算装置のみが演算結果の秘密分散値を出力してもよい。後者の場合、複数個の秘密計算装置のうち整合性検証に合格した対象データの秘密分散値を格納するものを要素とする「第１集合」と、複数個の秘密計算装置のうち整合性検証に合格したクエリまたはクエリの秘密分散値が入力されたものを要素とする「第２集合」と、の「共通部分」に

属する秘密計算装置が演算結果の秘密分散値を出力する。「第１集合」および「第２集合」の少なくとも一方は、複数個の秘密計算装置を要素とする「全体集合」の真部分集合であってもよい。これにより、整合性検証が不合格であった場合の処理量を削減できる。

[0011] 「第１集合」および「第２集合」の少なくとも一方が「全体集合」の真部分集合である場合、「共通部分」も「全体集合」の真部分集合である。秘密計算の内容によっては「全体集合」の真部分集合の秘密計算装置のみで秘密計算を実行できる場合（ケース１）もあれば、「全体集合」の秘密計算装置が協力しなければ秘密計算を実行できない場合（ケース２）もある。「ケース１」の場合には「共通部分」のみで秘密計算を行うことができるが、「ケース２」の場合には「共通部分」のみで秘密計算を行うことができず、整合性検証が不合格であった秘密計算装置と協力して秘密計算を行ったのでは、不正な結果が得られる可能性がある。そのため、「共通部分」に属する秘密計算装置が、「共通部分」の「補集合」（「全体集合」から「共通部分」を取り除いた集合）に属する秘密計算装置の対象データの秘密分散値およびクエリまたはクエリの秘密分散値の少なくとも一方を復元してもよい。秘密計算の内容に応じ、対象データの秘密分散値およびクエリまたはクエリの秘密分散値が復元されてもよいし、対象データの秘密分散値およびクエリまたはクエリの秘密分散値の何れかのみが復元されてもよい。これにより、「ケース２」の場合であっても「共通部分」のみで秘密計算を行うことができる。

[0012] 「共通部分」の要素数が演算結果を復元するために必要な秘密分散値の個数以上である場合に、「共通部分」に属する秘密計算装置が演算結果の秘密分散値を出力してもよい。これにより、演算結果を復元するために必要な個数の「演算結果の秘密分散値」が得られないにもかかわらず、演算結果の秘密分散値の計算および通信が行われることと防止できる。「共通部分」に属する秘密計算装置が「共通部分」の要素数が演算結果を復元するために必要な秘密分散値の個数未満である場合には、対象データの秘密分散値の格納、および／または、クエリまたはクエリの秘密分散値の入力をやり直すか、エ

ラー終了してもよい。

[0013] 複数の秘密計算装置で行った整合性検証が不合格であった場合、それらの何れかの秘密計算装置の「データ」（対象データの秘密分散値、または、クエリもしくはクエリの秘密分散値）に改ざんがあったことは分かるが、どの「データ」が改ざんされたかは分からない。そのため、「全体集合」の「第１部分集合」での対象データの秘密分散値の整合性検証が不合格であった場合、「第１部分集合」の真部分集合を新たな「第１部分集合」として対象データの秘密分散値の整合性検証を行う再帰処理を行ってもよい。例えば、「第１部分集合」を複数の真部分集合に分割し、各真部分集合をそれぞれ新たな「第１部分集合」としてもよいし、「第１部分集合」の何れかの真部分集合のみを新たな「第１部分集合」としてもよい。同様に、「全体集合」の「第２部分集合」でのクエリまたはクエリの秘密分散値の整合性検証が不合格であった場合、「第２部分集合」の真部分集合を新たな「第２部分集合」としてクエリまたはクエリの秘密分散値の整合性検証を行う再帰処理を行ってもよい。例えば、「第２部分集合」を複数の真部分集合に分割し、各真部分集合をそれぞれ新たな「第２部分集合」としてもよいし、「第２部分集合」の何れかの真部分集合のみを新たな「第２部分集合」としてもよい。これにより、上述の「第１集合」および／または「第２集合」を効率的に特定できる。

[0014] 「全体集合」の「第３部分集合」での対象データの秘密分散値の整合性検証が不合格であった場合、「第３部分集合」の真部分集合と「第３部分集合」の補集合（「全体集合」から「第３部分集合」を取り除いた集合）の部分集合との和集合を新たな「第３部分集合」として対象データの秘密分散値の整合性検証を行う再帰処理を行ってもよい。同様に、「全体集合」の「第４部分集合」でのクエリまたはクエリの秘密分散値の整合性検証が不合格であった場合、「第４部分集合」の真部分集合と「第４部分集合」の補集合（「全体集合」から「第４部分集合」を取り除いた集合）の部分集合との和集合を新たな「第４部分集合」としてクエリまたはクエリの秘密分散値の整合性

検証を行う再帰処理を行ってもよい。これによっても、上述の「第１集合」および／または「第２集合」を効率的に特定できる。特に、「第３部分集合」で整合性検証が不合格であるが、新たな「第３部分集合」で整合性検証が合格であった場合、更新前の「第３部分集合」には含まれるが新たな「第３部分集合」には含まれない秘密計算装置の「データ」に改ざんがあることが分かる。そのため、この秘密計算装置を除いた集合で新たに整合性検証を行い、それが合格であれば、その集合を「第１集合」および／または「第２集合」としてもよい。これにより、「第１集合」および／または「第２集合」の要素数を増加させ、「共通部分」に属する秘密計算装置の数を増加させることができる。

[0015] 秘密計算装置が、対象データの秘密分散値およびクエリまたはクエリの秘密分散値の整合性検証をまとめて行ってもよい。例えば、対象データの秘密分散値およびクエリまたはクエリの秘密分散値を含む情報を対象として整合性検証が行われてもよい。これにより、整合性検証の処理を効率化できる。この場合、対象データの秘密分散値およびクエリまたはクエリの秘密分散値を含む情報を撹乱させた情報の整合性検証を行ってもよい。これにより、整合性検証の過程で、対象データおよびクエリの少なくとも一方が漏洩することを防止できる。

[0016] 整合性検証方式に限定はない。例えば、非特許文献１に開示された方式が用いられてもよいし、その他の方式が用いられてもよい。例えば、秘密計算装置が「全体集合」の部分集合（全体集合またはその真部分集合）で得られた複数個の任意値の合成値ｓを得、合成値ｓの関数値を係数とし、対象データの秘密分散値およびクエリまたはクエリの秘密分散値の少なくとも一方を含む値の線形結合値［ｃ］$_i$を得、線形結合値［ｃ］$_i$に応じた秘密分散値［ｄ］$_i$を他の秘密計算装置に配送して整合性検証を行ってもよい。これにより、複数のデータの整合性検証をまとめて実行できるため、処理を効率化できる。この際、秘密計算装置が乱数秘密分散値［Ｒ］$_i$を得、乱数秘密分散値［Ｒ］$_i$で線形結合値［ｃ］$_i$を撹乱させた秘密分散値［ｄ］$_i$を得てもよい。こ

れにより、整合性検証の過程で、対象データおよびクエリの少なくとも一方が漏洩することを防止できる。

[0017] 以降、図面を参照しつつ、各実施形態を説明する。

［第１実施形態］

第１実施形態を説明する。

[0018] ＜構成＞

図１に例示するように、本形態の秘密計算システム１は、登録装置１１、Ｎ個の秘密計算装置１２－１，…，１２－（Ｎ－１）、および分析装置１３を有する。ただし、Ｎは２以上の整数であり、例えば３以上の整数である。登録装置１１と秘密計算装置１２－１，…，１２－（Ｎ－１）とは、インターネット等の安全ではないネットワークを通じて通信可能に構成されている。同様に、秘密計算装置１２－１，…，１２－（Ｎ－１）と分析装置１３とは、安全ではないネットワークを通じて通信可能に構成されている。なお、説明の便宜上、登録装置１１および分析装置１３がそれぞれ１個存在する例を示すが、これらの少なくとも一方が複数個存在していてもよい。

[0019] 図２Ａに例示するように、本形態の秘密計算装置１２－ｎ（ただし、ｎ＝０，…，（Ｎ－１））は、例えば、制御部１２０－ｎ、入力部１２１－ｎ、記憶部１２２－ｎ、整合性検証部１２３－ｎ、秘密計算部１２４－ｎ、および出力部１２５－ｎを有する。図２Ｂに例示するように、整合性検証部１２３－ｎは、例えば、任意値設定部１２３１－ｎ、合成部１２３２－ｎ、線形結合部１２３３－ｎ、および検証部１２３６－ｎを有する。整合性検証部１２３－ｎは、さらに撹乱値設定部１２３４－ｎおよび撹乱部１２３５－ｎを有していてもよい。秘密計算装置１２－ｎは、制御部１２０－ｎの制御のもとで各処理を実行する。秘密計算装置１２－ｎの各部で得られたデータは、図示していない一時メモリに格納され、必要に応じて読み出されて各処理に利用される。図３に例示するように、分析装置１３は、制御部１３０、分析依頼部１３１、出力部１３２、入力部１３３、記憶部１３４、および改ざん検知復元部１３５を有する。各装置は、例えば、ＣＰＵ（central processin

g unit）等のプロセッサ（ハードウェア・プロセッサ）およびＲＡＭ（random-access memory）・ＲＯＭ（read-only memory）等のメモリ等を備える汎用または専用のコンピュータが所定のプログラムを実行することで構成される。このコンピュータは１個のプロセッサやメモリを備えていてもよいし、複数個のプロセッサやメモリを備えていてもよい。このプログラムはコンピュータにインストールされてもよいし、予めＲＯＭ等に記録されていてもよい。また、ＣＰＵのようにプログラムが読み込まれることで機能構成を実現する電子回路（circuitry）ではなく、プログラムを用いることなく処理機能を実現する電子回路を用いて一部またはすべての処理部が構成されてもよい。１個の装置を構成する電子回路が複数のＣＰＵを含んでいてもよい。

[0020] ＜処理＞

本形態の処理は「登録処理」「保管処理」「分析処理」からなる。以下、図４を用いて本形態の処理を説明する。

[0021] 「登録処理」

登録処理では、登録装置１１が、秘密計算の対象となる対象データ$b_0$，…，$b_{M-1}$のそれぞれを秘密分散し、Ｎ個ずつの秘密分散値$[b_0]_0$，…，$[b_0]_{N-1}$，…，$[b_{M-1}]_0$，…，$[b_{M-1}]_{N-1}$を生成する。ただし、Ｍは１以上の整数であり（例えば、Ｍは２以上の整数）、対象データ$b_m$（ただし、$m=0$，…，$M-1$）のＮ個の秘密分散値を$[b_m]_0$，…，$[b_m]_{N-1}$と表記する。本形態の秘密分散は（Ｋ，Ｎ）しきい値秘密分散方式に則って行われる。（Ｋ，Ｎ）しきい値秘密分散方式では、Ｋ個以上の秘密分散値を集めれば元データ（平文）を完全に復元できるが、Ｋ－１以下の秘密分散値からは元データの情報が全く得られない。（Ｋ，Ｎ）しきい値秘密分散方式の具体例は、Shamirの秘密分散方式（例えば、参考文献１「A. Shamir, ”How to Share a Secret”, Communications of the ACM, November 1979, Volume 22, Number 11, pp.612-613.」等参照）、またはその変形方式である。対象データの秘密分散値$[b_0]_n$，…，$[b_{M-1}]_n$（ただし、$n=0$，…，$N-1$）は、それぞれ秘密計算装置１２－ｎに送られる。対象データの秘密分散値［

$b_0]_n$，…，$[b_{M-1}]_n$は、秘密計算装置１２－ｎ（図２Ａ）の入力部１２１－ｎに入力され、記憶部１２２－ｎに格納される（ステップＳ１１）。

[0022] 対象データの秘密分散値$[b_0]_n$，…，$[b_{M-1}]_n$が記憶部１２２－ｎに格納されると、Ｎ個の秘密計算装置１２－ｎ（ただし、ｎ＝０，…，Ｎ－１）の整合性検証部１２３－ｎが互いに通信し、対象データの秘密分散値$[b_0]_n$，…，$[b_{M-1}]_n$の整合性検証を行う。整合性検証は非特許文献１その他の公知方式によって行われてもよいし、後述する方式によって行われてもよい。これにより、登録装置１１、または登録装置１１から秘密計算装置１２－ｎまでの間で行われた対象データの秘密分散値$[b_0]_n$，…，$[b_{M-1}]_n$の改ざんが検知される。この整合性検証が合格であった場合、$[b_0]_n$，…，$[b_{M-1}]_n$が記憶部１２２－ｎに保持される。一方、この整合性検証が不合格であった場合、$[b_0]_n$，…，$[b_{M-1}]_n$が記憶部１２２－ｎから削除され、処理をステップＳ１１に戻すか、エラー終了させる（ステップＳ１２）。

[0023] 「保管処理」

保管処理では、各秘密計算装置１２－ｎが対象データの秘密分散値$[b_0]_n$，…，$[b_{M-1}]_n$を記憶部１２２－ｎに保持する。この間、定期的または所定の契機で、Ｎ個の秘密計算装置１２－ｎ（ただし、ｎ＝０，…，Ｎ－１）の整合性検証部１２３－ｎが互いに通信し、対象データの秘密分散値$[b_0]_n$，…，$[b_{M-1}]_n$の整合性検証を行ってもよい。これにより、秘密計算装置１２－ｎで行われた対象データの秘密分散値$[b_0]_n$，…，$[b_{M-1}]_n$の改ざんが検知される。この整合性検証が合格であった場合、$[b_0]_n$，…，$[b_{M-1}]_n$が記憶部１２２－ｎに保持される。一方、この整合性検証が不合格であった場合、$[b_0]_n$，…，$[b_{M-1}]_n$が記憶部１２２－ｎから削除され、処理をステップＳ１１に戻すか、エラー終了させる（ステップＳ１３）。

[0024] 「分析処理」

分析処理では、まず分析装置１３の分析依頼部１３１が、秘密計算を要求するクエリまたはクエリの秘密分散値を生成して出力する。クエリは秘密計

算を要求する演算内容を表してもよいし、演算対象のデータを表してもよい。本形態では、分析依頼部１３１が出力するクエリまたはクエリの秘密分散値を［$q_0$］$_n$，…，［$q_{J-1}$］$_n$（ただし、ｎ＝０，…，Ｎ－１）と表現する。ただし、Ｊは１以上の整数である。［$q_j$］$_n$（ただし、ｊ＝０，…，Ｊ－１）がクエリそのもの（元データ）である場合、［$q_j$］$_0$＝…＝［$q_j$］$_{N-1}$である。［$q_j$］$_n$（ただし、ｊ＝０，…，Ｊ－１）がクエリの秘密分散値である場合、［$q_j$］$_0$，…，［$q_j$］$_{N-1}$は、クエリ$q_j$のＮ個の秘密分散値である。出力部１３２は、クエリまたはクエリの秘密分散値［$q_0$］$_n$，…，［$q_{J-1}$］$_n$（ただし、ｎ＝０，…，Ｎ－１）を出力し、これらはそれぞれ秘密計算装置１２－ｎに送られる。［$q_0$］$_n$，…，［$q_{J-1}$］$_n$は、秘密計算装置１２－ｎ（図２Ａ）の入力部１２１－ｎに入力され、記憶部１２２－ｎに格納される（ステップＳ１４）。

[0025] クエリまたはクエリの秘密分散値［$q_0$］$_n$，…，［$q_{J-1}$］$_n$が記憶部１２２－ｎに格納されると、Ｎ個の秘密計算装置１２－ｎ（ただし、ｎ＝０，…，Ｎ－１）の整合性検証部１２３－ｎが互いに通信し、クエリまたはクエリの秘密分散値［$q_0$］$_n$，…，［$q_{J-1}$］$_n$の整合性検証を行う。ここで、［$q_j$］$_n$がクエリそのものであったとしても、［$q_j$］$_n$を秘密分散値とみなして整合性検証を行うことができる。これにより、分析装置１３、または分析装置１３から秘密計算装置１２－ｎまでの間で行われた［$q_0$］$_n$，…，［$q_{J-1}$］$_n$の改ざんが検知される。この整合性検証が合格である場合、［$q_0$］$_n$，…，［$q_{J-1}$］$_n$が記憶部１２２－ｎに保持される。一方、この整合性検証が不合格である場合、［$q_0$］$_n$，…，［$q_{J-1}$］$_n$が記憶部１２２－ｎから削除され、処理をステップＳ１４に戻すか、エラー終了させる（ステップＳ１５）。

[0026] ［$q_0$］$_n$，…，［$q_{J-1}$］$_n$の整合性検証が合格の場合、秘密計算装置１２－ｎの秘密計算部１２４－ｎは、記憶部１２２－ｎから、整合性検証に合格した［$b_0$］$_n$，…，［$b_{M-1}$］$_n$および［$q_0$］$_n$，…，［$q_{J-1}$］$_n$を読み込む。秘密計算部１２４－ｎは、整合性検証に合格した［$b_0$］$_n$，…，［$b_{M-1}$

$]_n$を用い、整合性検証に合格した$[q_0]_n$，…，$[q_{J-1}]_n$に応じた秘密計算を行って演算結果の秘密分散値$[r_0]_n$，…，$[r_{W-1}]_n$を得る。ただし、Wは１以上の整数である（例えば、Wは２以上の整数）。本形態では、改ざん検知付秘密計算（例えば、参考文献２「五十嵐大，千田浩司，濱田浩気，菊池亮，“非常に高効率なn≧2k-1 malicious モデル上秘密分散ベースマルチパーティ計算の構成法”， In SCIS2013, 2013.」等参照）によって秘密計算を行って演算結果の秘密分散値$[r_0]_n$，…，$[r_{W-1}]_n$を得る。この計算過程でのＫ－１個以下の秘密計算装置１２－ｎによる改ざんは、ここで検知できる。改ざんが検知された場合、この秘密計算を再び実行させるか、処理をエラー終了させる。改ざんが検知されなかった場合、演算結果の秘密分散値$[r_0]_n$，…，$[r_{W-1}]_n$が出力部１２５－ｎに送られる（ステップＳ１６）。出力部１２５－ｎ（ただし、ｎ＝０，…，Ｎ－１）は、演算結果の秘密分散値$[r_0]_n$，…，$[r_{W-1}]_n$を出力し、これらは分析装置１３に送られる（ステップＳ１７）。

[0027] 演算結果の秘密分散値$[r_0]_n$，…，$[r_{W-1}]_n$は、分析装置１３（図３）の入力部１３３に入力され、記憶部１３４に格納される。演算結果の秘密分散値$[r_0]_n$，…，$[r_{W-1}]_n$（ただし、ｎ＝０，…，Ｎ－１）は改ざん検知復元部１３５に送られる。改ざん検知復元部１３５はこれらの改ざん検知復元を行い（例えば、参考文献２参照）、演算結果$r_0$，…，$r_{W-1}$を復元して出力する。秘密計算装置１２－ｎまたは秘密計算装置１２－ｎから分析装置１３までの間での改ざんはここで検知される。改ざんが検知された場合、このステップＳ１６以降の処理を再び実行させるか、処理をエラー終了させる。改ざんが検知されなかった場合、演算結果$r_0$，…，$r_{W-1}$が出力される（ステップＳ１８）。

[0028] ＜整合性検証の具体例＞

図５を用いて整合性検証の具体例を示す。以下では、Ｉ個の秘密計算装置１２－０～１２－（Ｉ－１）が協力し、$[a_0]_i$，…，$[a_{Y-1}]_i$（ただし、ｉ＝０，…，Ｉ－１）の整合性検証を行う場合に一般化して説明する。た

だし、Ｙは１以上の整数であり、ＩはＫよりも大きく、Ｎ以下の整数であり（Ｎ≧Ｉ＞Ｋ。例えば、Ｎ≧Ｉ≧２）、｛０，…，Ｉ－１｝⊆｛０，…，Ｎ－１｝を満たす。$[a_0]_i$，…，$[a_{Y-1}]_i$の例は、対象データの秘密分散値$[b_0]_i$，…，$[b_{M-1}]_i$（この場合にはＹ＝Ｍ）、クエリまたはクエリの秘密分散値$[q_0]_i$，…，$[q_{J-1}]_i$（この場合にはＹ＝Ｊ）である。

[0029] まず、秘密計算装置１２－ｉ（図２Ｂ）の整合性検証部１２３－ｉの任意値設定部１２３１－ｉが、任意値$s_i$を選択する。任意値$s_i$の例は、擬似乱数、乱数、または定数である。任意値$s_i$は記憶部１２２－ｉに格納されるとともに、出力部１２５－ｉに送られる（ステップＳ１２０１）。任意値$s_i$は出力部１２５－ｉから出力され、他の秘密計算装置１２－ｉ’（ただし、ｉ’∈｛０，…，Ｉ－１｝かつｉ’≠ｉ）に配送される（ステップＳ１２０２）。他の秘密計算装置１２－ｉ’から配送された任意値$s_{i'}$は入力部１２１－ｉに入力され、記憶部１２２－ｉに格納される（ステップＳ１２０３）。合成部１２３２－ｉは、記憶部１２２－ｉから任意値$s_0$，…，$s_{I-1}$を読み込み、任意値$s_0$，…，$s_{I-1}$の合成値$s := g(s_0, \dots, s_{I-1})$を得る。ただし、「$\alpha := \beta$」は、$\alpha$を$\beta$と定義することを意味する。ｇ（・）は（・）の関数値を表す。任意値$s_0$，…，$s_{I-1}$に対して合成値ｓが一義的に定まるのであれば、どのようなｇ（・）が用いられてもよい。例えば、$s := s_0 + \dots + s_{I-1}$などの任意値$s_0$，…，$s_{I-1}$の線形結合を合成値ｓとしてもよいし、$s := s_0 \times \dots \times s_{I-1}$などの任意値$s_0$，…，$s_{I-1}$の積を合成値ｓとしてもよい。合成値ｓは記憶部１２２－ｉに格納される（ステップＳ１２０４）。

[0030] 線形結合部１２３３－ｉは、記憶部１２２－ｉから合成値ｓおよび$[a_0]_i$，…，$[a_{Y-1}]_i$を読み込み、合成値ｓの関数値を係数$z_y$（ただし、ｙ＝０，…，Ｙ－１）とし、$[a_0]_i$，…，$[a_{Y-1}]_i$（ただし、ｉ＝０，…，Ｉ－１）の線形結合値$[c]_i := z_0 [a_0]_i + \dots + z_{Y-1} [a_{Y-1}]_i$を得る。係数$z_y$は合成値ｓとｙとによって定まる値$z_y := h(s, y)$であってもよいし、合成値ｓのみに対して定まる値$z_y := h(s)$であってもよい

。ただし、ｈ（・）は（・）の関数値を表す。例えば、$z_y := s^{y+1}$であってもよいし、$z_y := s^{2y+1}$であってもよいし、$z_y := s$であってもよい。線形結合値$[c]_i$は記憶部１２２－ｉに格納される（ステップＳ１２０５）。

[0031] 検証部１２３６－ｉは、記憶部１２２－ｉから読み込んだ線形結合値$[c]_i$に応じた秘密分散値$[d]_i$を出力する。例えば、線形結合値$[c]_i$をそのまま秘密分散値$[d]_i$としてもよいし、$[c]_i$の関数値を秘密分散値$[d]_i$としてもよい。整合性検証部１２３－ｉが撹乱値設定部１２３４－ｉおよび撹乱部１２３５－ｉを含む場合、撹乱値設定部１２３４－ｉが乱数秘密分散値$[R]_i$を得、撹乱部１２３５－ｉが乱数秘密分散値$[R]_i$および線形結合値$[c]_i$を入力とし、乱数秘密分散値$[R]_i$で線形結合値$[c]_i$を撹乱させた秘密分散値$[d]_i$を得てもよい。例えば、撹乱値設定部１２３４－ｉが、生成した擬似乱数または乱数を乱数秘密分散値$[R]_i$とし、秘密計算によって$[d]_i := [c-R]_i$を得てもよい。ただし、$[c-R]_i$は（Ｋ，Ｎ）しきい値秘密分散方式に則ったｃ－Ｒの秘密分散値である。秘密分散値$[d]_i$は記憶部１２２－ｉに格納されるとともに、出力部１２５－ｉに送られる（ステップＳ１２０６）。

[0032] 秘密分散値$[d]_i$は出力部１２５－ｉから出力され、他の秘密計算装置１２－ｉ’（ただし、$i' \in \{0, \cdots, l-1\}$かつ$i' \neq i$）に配送される（ステップＳ１２０７）。他の秘密計算装置１２－ｉ’から配送された秘密分散値$[d]_{i'}$は入力部１２１－ｉに入力され、記憶部１２２－ｉに格納される（ステップＳ１２０８）。

[0033] 検証部１２３６－ｎは、記憶部１２２－ｉからＫ個の秘密分散値$[d]_{f(0)}, \cdots, [d]_{f(K-1)}$を読み込み、ラグランジュ（Lagrange）補間によって他のＬ－Ｋ個の秘密分散値$D_{f(K)} := [d]_{f(K)}, \cdots, D_{f(l-1)} := [d]_{f(l-1)}$を復元し、記憶部１２２－ｉに格納する。なお、$\{f(0), \cdots, f(l-1)\} = \{0, \cdots, l-1\}$を満たし、例えば、$f(i) = i$である（ステップＳ１２０９）。

[0034] 検証部１２３６－ｎは、記憶部１２２－ｉから、ステップＳ１２０８で入力された［ｄ］$_{f(K)}$，…，［ｄ］$_{f(N-1)}$と、ステップＳ１２０９で復元されたＤ$_{f(K)}$，…，Ｄ$_{f(N-1)}$とを読み込み、これらを比較する。ここで、すべてのｐ＝Ｋ，…，Ｉ－１についてＤ$_{f(p)}$＝［ｄ］$_{f(p)}$であるならば、検証部１２３６－ｎは、［ａ$_0$］$_i$，…，［ａ$_{Y-1}$］$_i$の整合性検証が合格である旨の結果を出力する（ステップＳ１２１１）。一方、何れかのｐについてＤ$_{f(p)}$≠［ｄ］$_{f(p)}$であるならば、検証部１２３６－ｎは、［ａ$_0$］$_i$，…，［ａ$_{Y-1}$］$_i$の整合性検証が不合格である旨の結果を出力する（ステップＳ１２１２）。

[0035] この整合性検証の具体例では、［ａ$_0$］$_i$，…，［ａ$_{Y-1}$］$_i$の整合性検証をまとめて実行できるため効率がよい。また、乱数秘密分散値［Ｒ］$_i$で線形結合値［ｃ］$_i$を撹乱させた秘密分散値［ｄ］$_i$を用いる場合には、ステップＳ１２０９で［ａ$_0$］$_i$，…，［ａ$_{Y-1}$］$_i$の復元値の情報が漏洩することを防止できる。

[0036] ［第２実施形態］

第２実施形態では、前述の「第１集合」と「第２集合」との「共通部分」に属する秘密計算装置が演算結果の秘密分散値を出力する。「第１集合」および「第２集合」の少なくとも一方は、複数個の秘密計算装置を要素とする「全体集合」の真部分集合であってもよい。以下では、既に説明した事項との相違点を中心に説明し、説明済みの事項についてはそれと同じ参照番号を流用して説明を簡略化する。

[0037] ＜構成＞

図１に例示するように、本形態の秘密計算システム２は、登録装置１１、Ｎ個の秘密計算装置２２－１，…，２２－（Ｎ－１）、および分析装置１３を有する。図２Ａに例示するように、本形態の秘密計算装置２２－ｎ（ただし、ｎ＝０，…，（Ｎ－１））は、例えば、制御部１２０－ｎ、入力部１２１－ｎ、記憶部１２２－ｎ、整合性検証部２２３－ｎ、秘密計算部２２４－ｎ、および出力部１２５－ｎを有する。

[0038] ＜処理＞

本形態の処理も「登録処理」「保管処理」「分析処理」からなる。以下、図４を用いて本形態の処理を説明する。

[0039] 「登録処理」

まず、登録装置１１と秘密計算装置２２－ｎとが、第１実施形態で説明したステップＳ１１の処理を実行する。次に、第１実施形態のステップＳ１２で説明したように、Ｎ個の秘密計算装置２２－ｎ（ただし、ｎ＝０，…，Ｎ－１）の整合性検証部２２３－ｎが互いに通信し、対象データの秘密分散値$[b_0]_n$，…，$[b_{M-1}]_n$の整合性検証を行う。ただし、本形態では、この整合性検証が不合格であっても、記憶部１２２－ｎから$[b_0]_n$，…，$[b_{M-1}]_n$が削除されない。代わりに、Ｎ個の秘密計算装置２２－ｎ（ただし、ｎ＝０，…，Ｎ－１）からなる集合の真部分集合$S_1$が選択され、真部分集合$S_1$に属する$N_{S1}$個（ただし、$N_{S1}>K$）の秘密計算装置２２－ｖ（$\eta$）（ただし、$\eta=0,\cdots,N_{S1}-1$）の整合性検証部２２３－ｖ（$\eta$）が互いに通信し、対象データの秘密分散値$[b_0]_{v(\eta)}$，…，$[b_{M-1}]_{v(\eta)}$の整合性検証を行う。なお、$\{v(0),\cdots,v(N_{S1}-1)\}=\{0,\cdots,N_{S1}-1\}$を満たし、例えば、$v(\eta)=\eta$である。この真部分集合$S_1$での整合性検証方法にも限定はない。例えば、非特許文献１の方法で整合性検証が行われてもよいし、$l:=N_{S1}$とし、$i:=v(\eta)$とし、$([a_0]_i,\cdots,[a_{Y-1}]_i):=([b_0]_{v(\eta)},\cdots,[b_{M-1}]_{v(\eta)})$とし、前述のステップＳ１２０１～Ｓ１２１２の方法で整合性検証が行われてもよい。真部分集合$S_1$に属する$N_{S1}$個の秘密計算装置２２－ｖ（$\eta$）（ただし、$\eta=0,\cdots,N_{S1}-1$）での整合性検証が不合格である場合、別の真部分集合$S_1$が選択され、選択された真部分集合$S_1$での整合性検証が実行される。真部分集合$S_1$は、予め定められた基準に従って選択される。真部分集合$S_1$の真部分集合が新たな真部分集合$S_1$とされてもよいし、真部分集合$S_1$の補集合が新たな真部分集合$S_1$とされてもよいし、真部分集合$S_1$の真部分集合と補集合との和集合が新たな真部分集合$S_1$とされてもよい。この具体例は後述する。Ｎ個の秘密

計算装置２２－ｎ（ただし、ｎ＝０，…，Ｎ－１）からなる全体集合Ｕでの整合性検証が合格であった場合、その旨の情報が記憶部１２２－ｎ（ただし、ｎ＝０，…，Ｎ－１）に格納される。真部分集合$S_1$での整合性検証が合格であった場合、その旨の情報が記憶部１２２－ｎ（ただし、ｎ＝０，…，Ｎ－１）に格納される。全体集合Ｕまたは真部分集合$S_1$での整合性検証が合格であった場合、対象データの秘密分散値$[b_0]_n$，…，$[b_{M-1}]_n$が記憶部１２２－ｎに保持される。一方、真部分集合$S_1$を所定回数更新しても整合性検証が合格にならなかった場合、所定の真部分集合$S_1$について整合性検証を行ってすべて不合格であった場合、または合格となった真部分集合$S_1$の要素数がＫ未満であった場合、$[b_0]_n$，…，$[b_{M-1}]_n$が記憶部１２２－ｎから削除され、処理をステップＳ１１に戻すか、エラー終了させる（ステップＳ２２）。

[0040] 「保管処理」

保管処理でも、定期的または所定の契機で、ステップＳ２２と同じ整合性検証が行われてもよい。Ｎ個の秘密計算装置２２－ｎ（ただし、ｎ＝０，…，Ｎ－１）からなる全体集合Ｕでの整合性検証が合格であった場合、その旨の情報が記憶部１２２－ｎ（ただし、ｎ＝０，…，Ｎ－１）に格納される。真部分集合$S_1$での整合性検証が合格であった場合、その旨の情報が記憶部１２２－ｎ（ただし、ｎ＝０，…，Ｎ－１）に格納される。全体集合Ｕまたは真部分集合$S_1$での整合性検証が合格であった場合、対象データの秘密分散値$[b_0]_n$，…，$[b_{M-1}]_n$が記憶部１２２－ｎに保持される。一方、真部分集合$S_1$を所定回数更新しても整合性検証が合格にならなかった場合、所定の真部分集合$S_1$について整合性検証を行ってすべて不合格であった場合、または合格となった真部分集合$S_1$の要素数がＫ未満であった場合、$[b_0]_n$，…，$[b_{M-1}]_n$が記憶部１２２－ｎから削除され、処理をステップＳ１１に戻すか、エラー終了させる（ステップＳ２３）。

[0041] 「分析処理」

まず、分析装置１３と秘密計算装置２２－ｎとが、第１実施形態で説明し

たステップＳ１４の処理を実行する。次に、第１実施形態のステップＳ１５で説明したように、Ｎ個の秘密計算装置２２－ｎ（ただし、ｎ＝０，…，Ｎ－１）の整合性検証部２２３－ｎが互いに通信し、クエリまたはクエリの秘密分散値を［$q_0$］$_n$，…，［$q_{J-1}$］$_n$の整合性検証を行う。ただし、本形態では、この整合性検証が不合格であっても、記憶部１２２－ｎから［$q_0$］$_n$，…，［$q_{J-1}$］$_n$が削除されない。代わりに、Ｎ個の秘密計算装置２２－ｎ（ただし、ｎ＝０，…，Ｎ－１）からなる集合の真部分集合$S_2$が選択され、真部分集合$S_2$に属する$N_{S2}$個（ただし、$N_{S2}$＞Ｋ）の秘密計算装置２２－ｕ（$\iota$）（ただし、$\iota$＝０，…，$N_{S2}$－１）が互いに通信し、［$q_0$］$_{u(\iota)}$，…，［$q_{J-1}$］$_{u(\iota)}$の整合性検証を行う。なお、｛ｕ（０），…，ｕ（$N_{S2}$－１）｝＝｛０，…，$N_{S2}$－１｝を満たし、例えば、ｕ（$\iota$）＝$\iota$である。この真部分集合$S_1$での整合性検証方法にも限定はない。例えば、非特許文献１の方法で整合性検証が行われてもよいし、Ｉ＝$N_{S2}$とし、ｉ＝ｕ（$\iota$）とし、（［$a_0$］$_i$，…，［$a_{Y-1}$］$_i$）＝（［$q_0$］$_{u(\iota)}$，…，［$q_{J-1}$］$_{u(\iota)}$）とし、前述のステップＳ１２０１～Ｓ１２１２の方法で整合性検証が行われてもよい。真部分集合$S_2$に属する$N_{S2}$個の秘密計算装置２２－ｕ（$\iota$）（ただし、$\iota$＝０，…，$N_{S2}$－１）での整合性検証が不合格である場合、別の真部分集合$S_2$が選択され、選択された真部分集合$S_2$での整合性検証が実行される。真部分集合$S_2$は、予め定められた基準に従って選択される。真部分集合$S_2$の真部分集合が新たな真部分集合$S_2$とされてもよいし、真部分集合$S_2$の補集合が新たな真部分集合$S_2$とされてもよいし、真部分集合$S_2$の真部分集合と補集合との和集合が新たな真部分集合$S_2$とされてもよい。Ｎ個の秘密計算装置２２－ｎ（ただし、ｎ＝０，…，Ｎ－１）からなる全体集合Ｕでの整合性検証が合格であった場合、その旨の情報が記憶部１２２－ｎ（ただし、ｎ＝０，…，Ｎ－１）に格納される。真部分集合$S_2$での整合性検証が合格であった場合、その旨の情報が記憶部１２２－ｎ（ただし、ｎ＝０，…，Ｎ－１）に格納される。全体集合Ｕまたは真部分集合$S_2$での整合性検証が合格であった場合、クエリまたはクエリの秘密分散値を［$q_0$］$_n$，…，［$q_{J-1}$

］$_n$が記憶部１２２－ｎに保持される。一方、真部分集合Ｓ$_2$を所定回数更新しても整合性検証が合格にならなかった場合、所定の真部分集合Ｓ$_2$について整合性検証を行ってすべて不合格であった場合、または、合格となった真部分集合Ｓ$_2$の要素数がＫ未満であった場合、［ｑ$_0$］$_n$，…，［ｑ$_{J-1}$］$_n$が記憶部１２２－ｎから削除され、処理をステップＳ１４に戻すか、エラー終了させる（ステップＳ２５）。

[0042] 全体集合Ｕまたは真部分集合Ｓ$_2$での整合性検証が合格であった場合、Ｎ個の秘密計算装置２２－０，…，２２－（Ｎ－１）のうち、ステップＳ２２，２３での整合性検証に合格した対象データの秘密分散値［ｂ$_0$］$_n$，…，［ｂ$_{M-1}$］$_n$を格納する秘密計算装置を要素とする「第１集合（ＵまたはＳ$_1$）」と、ステップＳ２５での整合性検証に合格したクエリまたはクエリの秘密分散値［ｑ$_0$］$_n$，…，［ｑ$_{J-1}$］$_n$が入力された秘密計算装置を要素とする「第２集合（ＵまたはＳ$_2$）」と、の「共通部分（Ｓ$_{12}$）」に属する秘密計算装置２２－κ（ただし、κ∈｛０，…，Ｎ－１｝）が秘密計算を行う。例えば、ステップＳ２２，２３，２５で全体集合Ｕでの整合性検証が合格であった場合、Ｕ＝Ｓ$_{12}$となり、Ｎ個の秘密計算装置２２－０，…，２２－（Ｎ－１）が第１実施形態で説明したステップＳ１６と同一の処理を行う（図７Ａおよび７Ｂ）。例えば、ステップＳ２２，２３で真部分集合Ｓ$_1$での整合性検証が合格であり、ステップＳ２５で真部分集合Ｓ$_2$での整合性検証が合格であったのであれば、真部分集合Ｓ$_1$と真部分集合Ｓ$_2$との「共通部分（Ｓ$_{12}$）」に属する秘密計算装置２２－κ（ただし、κ∈｛０，…，Ｎ－１｝）の秘密計算部２２４－κが、整合性検証に合格した［ｂ$_0$］$_\kappa$，…，［ｂ$_{M-1}$］$_\kappa$を用い、整合性検証に合格した［ｑ$_0$］$_\kappa$，…，［ｑ$_{J-1}$］$_\kappa$に応じた秘密計算を行って演算結果の秘密分散値［ｒ$_0$］$_\kappa$，…，［ｒ$_{W-1}$］$_\kappa$を得る。本形態でも、改ざん検知付秘密計算（例えば、参考文献２）が用いられる（ステップＳ２６）。その後、分析装置１３と秘密計算装置２２－ｎとが、第１実施形態で説明したステップＳ１７およびＳ１８と同じ処理を実行する。ただし、「共通部分（Ｓ$_{12}$）」の要素数が演算結果を復元するために必要な秘密分散値の個数Ｋ

以上である場合のみにステップＳ２６，Ｓ１７，Ｓ１８の処理が実行され、そうでない場合に処理をエラー終了させてもよい。

[0043] ＜整合性検証対象となる真部分集合の更新例＞

ステップＳ２２，Ｓ２３，Ｓ２５で説明した整合性検証対象となる真部分集合の更新例を説明する。更新例１では、「全体集合（Ｕ）」の「第１部分集合（ＵまたはＳ$_1$）」での対象データの秘密分散値［ｂ$_0$］$_{v(\eta)}$，…，［ｂ$_{M-1}$］$_{v(\eta)}$の整合性検証が不合格であった場合、「第１部分集合（ＵまたはＳ$_1$）」の真部分集合を新たな「第１部分集合（Ｓ$_1$）」として対象データの秘密分散値［ｂ$_0$］$_{v(\eta)}$，…，［ｂ$_{M-1}$］$_{v(\eta)}$の整合性検証を行う再帰処理を行う。また、「全体集合（Ｕ）」の「第２部分集合（ＵまたはＳ$_2$）」でのクエリまたはクエリの秘密分散値［ｑ$_0$］$_{u(\iota)}$，…，［ｑ$_{J-1}$］$_{u(\iota)}$の整合性検証が不合格であった場合、「第２部分集合（ＵまたはＳ$_2$）」の真部分集合を新たな「第２部分集合（Ｓ$_2$）」としてクエリまたはクエリの秘密分散値の整合性検証を行う再帰処理を行う。更新例２では、「全体集合（Ｕ）」の「第３部分集合（ＵまたはＳ$_1$）」での対象データの秘密分散値［ｂ$_0$］$_{v(\eta)}$，…，［ｂ$_{M-1}$］$_{v(\eta)}$の整合性検証が不合格であった場合、「第３部分集合（ＵまたはＳ$_1$）」の真部分集合と「第３部分集合（ＵまたはＳ$_1$）」の補集合の部分集合との和集合を新たな「第３部分集合Ｓ$_1$」として対象データの秘密分散値［ｂ$_0$］$_{v(\eta)}$，…，［ｂ$_{M-1}$］$_{v(\eta)}$の整合性検証を行う再帰処理を行う。「全体集合（Ｕ）」の「第４部分集合（ＵまたはＳ$_2$）」でのクエリまたはクエリの秘密分散値［ｑ$_0$］$_{u(\iota)}$，…，［ｑ$_{J-1}$］$_{u(\iota)}$の整合性検証が不合格であった場合、「第４部分集合（ＵまたはＳ$_2$）」の真部分集合と「第４部分集合（ＵまたはＳ$_2$）」の補集合の部分集合との和集合を新たな「第４部分集合Ｓ$_2$」としてクエリまたはクエリの秘密分散値［ｑ$_0$］$_{u(\iota)}$，…，［ｑ$_{J-1}$］$_{u(\iota)}$の整合性検証を行う再帰処理を行う。以下では、Ｓ$_1$およびＳ$_2$を部分集合Ｓに一般化して説明する。

[0044] ≪更新例１≫

図６Ａに例示するように、更新例１では、まずＮ個の秘密計算装置２２－

ｎ（ただし、ｎ＝０，…，Ｎ－１）の整合性検証部２２３－ｎが、Ｎ個の秘密計算装置２２－ｎの全体集合Ｕを集合系ＳＥＴの元として設定する（ＳＥＴ：＝｛Ｕ｝）（ステップＳ２２０１）。集合系ＳＥＴの元である部分集合Ｓ∈ＳＥＴ（初期値は全体集合Ｕ）に属する$N_S$個（ただし、$N_S$＞Ｋ）個の秘密計算装置２２－ｅ（ν）（ただし、ν＝０，…，$N_S$－１）の整合性検証部２２３－ｅ（ν）が互いに通信し、データ（対象データの秘密分散値、またはクエリもしくはクエリの秘密分散値）の整合性検証を行う。なお、｛ｅ（０），…，ｅ（$N_S$－１）｝＝｛０，…，$N_S$－１｝を満たし、例えば、ｅ（ν）＝νである（ステップＳ２２０２）。ここで、整合性検証に合格する部分集合Ｓが存在しないならば（ステップＳ２２０３）、整合性検証部２２３－ｅ（ν）は整合性検証の継続条件を満たすかを判定する（ステップＳ２２０４）。継続条件の例は、「部分集合Ｓの更新回数が所定数以下である」「所定の部分集合の整合性検証が終了していない」などである。ここで、整合性検証の継続条件を満たさない場合、整合性検証部２２３－ｅ（ν）は処理をエラー終了させる（ステップＳ２２０８）。一方、整合性検証の継続条件を満たす場合、整合性検証部２２３－ｅ（ν）は、部分集合Ｓをその真部分集合に置換して集合系ＳＥＴを更新する。例えば、図８Ａの例では、ＳＥＴ：＝｛$SS_{1-1}$｝のときに、部分集合Ｓ＝$SS_{1-1}$がその真部分集合$SS_{1-2}$および$SS_{1-3}$に置換され、ＳＥＴ：＝｛$SS_{1-2}$，$SS_{1-3}$｝に更新される。図８Ｂの例では、ＳＥＴ：＝｛$SS_{1-2}$，$SS_{1-3}$｝のときに、$SS_{1-2}$がその真部分集合$SS_{1-4}$および$SS_{1-5}$に置換され、$SS_{1-3}$がその真部分集合$SS_{1-6}$および$SS_{1-7}$に置換される。集合系ＳＥＴの更新後、ステップＳ２２０２に戻る（ステップＳ２２０５）。一方、ステップＳ２２０２で整合性検証に合格した部分集合Ｓが存在したならば（ステップＳ２２０３）、整合性検証部２２３－ｅ（ν）は整合性検証に合格した部分集合Ｓの要素数｜Ｓ｜＝$N_S$がＫ以上かを判定する（ステップＳ２２０６）。整合性検証に合格した何れかの部分集合Ｓの要素数｜Ｓ｜がＫ以上であれば、整合性検証部２２３－ｅ（ν）はその部分集合Ｓを表す情報を出力する（ステップＳ２２０

７）。そうでなければ、整合性検証部２２３－ｅ（ν）は処理をエラー終了させる（ステップＳ２２０８）。

[0045] ≪更新例２≫

図６Ｂに例示するように、更新例２では、図６Ａの処理のステップＳ２２０１がＳ２２１１に置換され、ステップＳ２２０５がステップＳ２２１５に置換される。ステップＳ２２１１では、Ｎ個の秘密計算装置２２－ｎ（ただし、ｎ＝０，…，Ｎ－１）の整合性検証部２２３－ｎが、全体集合Ｕの真部分集合を集合系ＳＥＴの元として設定する（ＳＥＴ：＝｛Ｓ｝（ただし、Ｓ⊂Ｕ））（ステップＳ２２１１）。ステップＳ２２１５では、整合性検証部２２３－ｅ（ν）が、部分集合ＳをＳの真部分集合Ａ⊂Ｓと、Ｓの補集合$C_S$の真部分集合Ｂ⊂$C_S$と、の和集合Ａ＋Ｂに置換する。例えば、和集合Ａ＋Ｂは部分集合Ｓをシフトさせた集合である。例えば、図９Ａおよび図９Ｂの例では、ＳＥＴ：＝｛$SS_{1-2}$，$SS_{1-3}$｝のときに、$SS_{1-2}$が和集合$SS_{1-4}$に置換され、$SS_{1-3}$が和集合$SS_{1-5}$に置換される。図９Ａおよび図９Ｂの例では、ＳＥＴ：＝｛$SS_{1-4}$，$SS_{1-5}$，$SS_{1-6}$，$SS_{1-7}$｝のときに、$SS_{1-4}$が和集合$SS_{1-8}$に置換され、$SS_{1-5}$が和集合$SS_{1-9}$に置換され、$SS_{1-6}$が和集合$SS_{1-10}$に置換され、$SS_{1-7}$が和集合$SS_{1-11}$に置換される。

[0046] ［第３実施形態］

第２実施形態では、「第１集合」と「第２集合」との「共通部分」に属する秘密計算装置が、「共通部分」の補集合に属する秘密計算装置の対象データの秘密分散値およびクエリまたはクエリの秘密分散値の少なくとも一方を復元し、秘密計算を行う。

[0047] ＜構成＞

図１に例示するように、本形態の秘密計算システム３は、登録装置１１、Ｎ個の秘密計算装置３２－１，…，３２－（Ｎ－１）、および分析装置１３を有する。図２Ａに例示するように、本形態の秘密計算装置３２－ｎ（ただし、ｎ＝０，…，（Ｎ－１））は、例えば、制御部１２０－ｎ、入力部１２

１－ｎ、記憶部１２２－ｎ、整合性検証部２２３－ｎ、秘密計算部３２４－ｎ、出力部１２５－ｎ、および分散値復元部３２６－ｎ、を有する。

[0048] ＜処理＞

本形態の処理も「登録処理」「保管処理」「分析処理」からなる。以下、図４を用いて本形態の処理を説明する。

[0049] 「登録処理」

登録装置１１と秘密計算装置３２－ｎとが、第１実施形態で説明したステップＳ１１の処理を実行する。次に、秘密計算装置３２－ｎが、第２実施形態で説明したステップＳ２２の処理を実行する。

[0050] 「保管処理」

秘密計算装置３２－ｎが、第２実施形態で説明したステップＳ２３の処理を実行する。

[0051] 「分析処理」

まず、分析装置１３と秘密計算装置２２－ｎとが、第１実施形態で説明したステップＳ１４の処理を実行する。次に、秘密計算装置３２－ｎが、第２実施形態で説明したステップＳ２５の処理を実行する。

[0052] 全体集合Ｕまたは真部分集合$S_2$での整合性検証が合格であった場合、前述の「第１集合（ＵまたはＳ$_1$）」と「第２集合（ＵまたはＳ$_2$）」との「共通部分（Ｓ$_{12}$）」に属する秘密計算装置３２－$\kappa$（ただし、$\kappa \in \{0, \cdots, N-1\}$）の分散値復元部３２６－$\kappa$が互いに通信を行い、「共通部分（Ｓ$_{12}$）」の補集合に属する秘密計算装置３２－$\theta$（ただし、$\theta \in \{0, \cdots, N-1\}$かつ$\theta \neq \kappa$）の対象データの秘密分散値$[b_0]_\theta, \cdots, [b_{M-1}]_\theta$およびクエリまたはクエリの秘密分散値$[q_0]_\theta, \cdots, [q_{J-1}]_\theta$を復元する。この復元は、例えばラグランジュ補間によって行われる。例えば、「共通部分（Ｓ$_{12}$）」に属する信頼できる特定の秘密計算装置３２－$\kappa$’の分散値復元部３２６－$\kappa$’に対し、「共通部分（Ｓ$_{12}$）」に属するその他の秘密計算装置３２－$\kappa$の分散値復元部３２６－$\kappa$が$[b_0]_\kappa, \cdots, [b_{M-1}]_\kappa$および$[q_0]_\kappa, \cdots, [q_{J-1}]_\kappa$を送る。秘密計算装置３２－$\kappa$’は、これらを用

い、ラグランジュ補間によって、$[b_0]_\theta$，…，$[b_{M-1}]_\theta$および$[q_0]_\theta$，…，$[q_{J-1}]_\theta$を復元し、記憶部１２２－$\kappa$’に格納する（ステップＳ３５）。

[0053] 「共通部分（$S_{12}$）」に属する秘密計算装置３２－$\kappa$（ただし、$\kappa \in \{0, \cdots, N-1\}$）は、整合性検証に合格した$[b_0]_\kappa$，…，$[b_{M-1}]_\kappa$を用い、整合性検証に合格した$[q_0]_\kappa$，…，$[q_{J-1}]_\kappa$に応じた秘密計算を行って演算結果の秘密分散値$[r_0]_\kappa$，…，$[r_{W-1}]_\kappa$を得る。復元された$[b_0]_\theta$，…，$[b_{M-1}]_\theta$および$[q_0]_\theta$，…，$[q_{J-1}]_\theta$を保持する秘密計算装置３２－$\kappa$は、さらに、復元された$[b_0]_\theta$，…，$[b_{M-1}]_\theta$を用い、復元された$[q_0]_\kappa$，…，$[q_{J-1}]_\kappa$に応じた秘密計算を行って演算結果の秘密分散値$[r_0]_\theta$，…，$[r_{W-1}]_\theta$を得る。本形態でも、改ざん検知付秘密計算（例えば、参考文献２）が用いられる（ステップＳ３６）。その後、分析装置１３と秘密計算装置３２－ｎとが、第１実施形態で説明したステップＳ１７およびＳ１８と同じ処理を実行する。ただし、$[r_0]_\theta$，…，$[r_{W-1}]_\theta$は、分析装置１３に送られてもよいし、送られなくてもよい。「共通部分（$S_{12}$）」の要素数が演算結果を復元するために必要な秘密分散値の個数Ｋ以上である場合のみにステップＳ３５，Ｓ３６，Ｓ１７，Ｓ１８の処理が実行され、そうでない場合に処理をエラー終了させてもよい。

[0054] ［第４実施形態］

第４実施形態では、対象データの秘密分散値およびクエリまたはクエリの秘密分散値の整合性検証をまとめて行う。

[0055] ＜構成＞

図１に例示するように、本形態の秘密計算システム４は、登録装置１１、Ｎ個の秘密計算装置４２－１，…，４２－（Ｎ－１）、および分析装置１３を有する。図２Ａに例示するように、本形態の秘密計算装置４２－ｎ（ただし、ｎ＝０，…，（Ｎ－１））は、例えば、制御部１２０－ｎ、入力部１２１－ｎ、記憶部１２２－ｎ、整合性検証部４２３－ｎ、秘密計算部１２４－ｎ、および出力部１２５－ｎを有する。

[0056] ＜処理＞

本形態の処理も「登録処理」「保管処理」「分析処理」からなる。以下、図４を用いて本形態の処理を説明する。

[0057] 「登録処理」

登録装置１１と秘密計算装置４２－ｎとが、第１実施形態で説明したステップＳ１１およびＳ１２の処理を実行する。ただし、本形態ではステップＳ１２の処理が省略されてもよい。

[0058] 「保管処理」

秘密計算装置４２－ｎが、第１実施形態で説明したステップＳ１３の処理を実行する。ただし、本形態ではステップＳ１３での整合性検証の処理が省略されてもよい。

[0059] 「分析処理」

まず、分析装置１３と秘密計算装置４２－ｎとが、第１実施形態で説明したステップＳ１４の処理を実行する。次に、Ｎ個の秘密計算装置４２－ｎ（ただし、ｎ＝０，…，Ｎ－１）の整合性検証部４２３－ｎが互いに通信し、対象データの秘密分散値$[b_0]_n$，…，$[b_{M-1}]_n$およびクエリまたはクエリの秘密分散値を$[q_0]_n$，…，$[q_{J-1}]_n$の整合性検証をまとめて行う。すなわち、整合性検証部４２３－ｎは、$[b_0]_n$，…，$[b_{M-1}]_n$，$[q_0]_n$，…，$[q_{J-1}]_n$を対象として整合性検証をまとめて行う。例えば、整合性検証部４２３－ｎは、Ｌ：＝Ｎとし、ｉ：＝ｎとし、Ｙ：＝Ｍ＋Ｊとし、$([a_0]_i, \cdots, [a_{Y-1}]_i) := ([b_0]_n, \cdots, [b_{M-1}]_n, [q_0]_n, \cdots, [q_{J-1}]_n)$とし、前述のステップＳ１２０１～Ｓ１２１２の方法で整合性検証を行う。この場合も、対象データの秘密分散値およびクエリまたはクエリの秘密分散値を含む情報（$[b_0]_n$，…，$[b_{M-1}]_n$，$[q_0]_n$，…，$[q_{J-1}]_n$）を撹乱させた情報の整合性検証が行われてもよい。この整合性検証が合格である場合、$[b_0]_n$，…，$[b_{M-1}]_n$，$[q_0]_n$，…，$[q_{J-1}]_n$が記憶部１２２－ｎに保持される。一方、この整合性検証が不合格である場合、$[b_0]_n$，…，$[b_{M-1}]_n$，$[q_0]_n$，…，$[q_{J-1}]_n$が記

憶部１２２－ｎから削除され、ステップＳ１１の処理に戻すか、処理をエラー終了させる（ステップＳ４５）。その後、第１実施形態のステップＳ１６～Ｓ１８の処理が実行される。

[0060] なお、第２実施形態または第３実施形態のステップＳ２５の整合性検証に代え、対象データの秘密分散値およびクエリまたはクエリの秘密分散値の整合性検証がまとめて行われてもよい。すなわち、Ｎ個の秘密計算装置４２－ｎの整合性検証部４２３－ｎでの整合性検証が不合格であった場合、Ｎ個の秘密計算装置４２－ｎ（ただし、ｎ＝０，…，Ｎ－１）からなる集合の真部分集合Ｓに属する秘密計算装置４２－ｕ（$\iota$）の整合性検証部４２３－ｕ（$\iota$）が、$[b_0]_{u(\iota)}$，…，$[b_{M-1}]_{u(\iota)}$，$[q_0]_{u(\iota)}$，…，$[q_{J-1}]_{u(\iota)}$を対象として整合性検証を行ってもよい。

[0061] ［その他の変形例等］

なお、本発明は上述の実施の形態に限定されるものではない。例えば、各装置がネットワークを通じて情報をやり取りするのではなく、少なくとも一部の組の装置が可搬型記録媒体を介して情報をやり取りしてもよい。或いは、少なくとも一部の組の装置が非可搬型の記録媒体を介して情報をやり取りしてもよい。すなわち、これらの装置の一部からなる組み合わせが、同一の装置であってもよい。また、上述した各演算は有限体上の演算であってもよいし、拡大体上の演算であってもよいし、環上の演算であってもよいし、その他の代数系上での演算であってもよい。また、改ざん検知付秘密計算に代えて、改ざん検知機能を持たない秘密計算が行われてもよい。

[0062] 上述の各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。その他、本発明の趣旨を逸脱しない範囲で適宜変更が可能であることはいうまでもない。

[0063] 上述の構成をコンピュータによって実現する場合、各装置が有すべき機能の処理内容はプログラムによって記述される。このプログラムをコンピュータで実行することにより、上記処理機能がコンピュータ上で実現される。こ

の処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体の例は、非一時的な（non-transitory）記録媒体である。このような記録媒体の例は、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等である。

[0064] このプログラムの流通は、例えば、そのプログラムを記録したＤＶＤ、ＣＤ－ＲＯＭ等の可搬型記録媒体を販売、譲渡、貸与等することによって行う。さらに、このプログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することにより、このプログラムを流通させる構成としてもよい。

[0065] このようなプログラムを実行するコンピュータは、例えば、まず、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、一旦、自己の記憶装置に格納する。処理の実行時、このコンピュータは、自己の記録装置に格納されたプログラムを読み取り、読み取ったプログラムに従った処理を実行する。このプログラムの別の実行形態として、コンピュータが可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することとしてもよく、さらに、このコンピュータにサーバコンピュータからプログラムが転送されるたびに、逐次、受け取ったプログラムに従った処理を実行することとしてもよい。サーバコンピュータから、このコンピュータへのプログラムの転送は行わず、その実行指示と結果取得のみによって処理機能を実現する、いわゆるＡＳＰ（Application Service Provider）型のサービスによって、上述の処理を実行する構成としてもよい。

[0066] 上記実施形態では、コンピュータ上で所定のプログラムを実行させて本装置の処理機能が実現されたが、これらの処理機能の少なくとも一部がハードウェアで実現されてもよい。

## 符号の説明

[0067] １～４　秘密計算システム

１１　登録装置

１２－ｎ～４２－ｎ　秘密計算装置

１３　分析装置

# 請求の範囲

[請求項1] 複数個の秘密計算装置を有し、

前記秘密計算装置のそれぞれは、

秘密計算の対象となる対象データの秘密分散値を格納する記憶部と、

前記秘密計算を要求するクエリまたは前記クエリの秘密分散値が入力される入力部と、

前記対象データの秘密分散値の整合性検証および前記クエリまたは前記クエリの秘密分散値の整合性検証を行う整合性検証部と、

整合性検証に合格した前記対象データの秘密分散値を用い、整合性検証に合格した前記クエリまたは前記クエリの秘密分散値に応じた秘密計算を行って演算結果の秘密分散値を得る秘密計算部と、

前記演算結果の秘密分散値を出力する出力部と、

を有する秘密計算システム。

[請求項2] 請求項１の秘密計算システムであって、

前記複数個の秘密計算装置のうち整合性検証に合格した前記対象データの秘密分散値を格納するものを要素とする第１集合と、前記複数個の秘密計算装置のうち整合性検証に合格した前記クエリまたは前記クエリの秘密分散値が入力されたものを要素とする第２集合と、の共通部分に属する前記秘密計算装置の前記出力部が前記演算結果の秘密分散値を出力し、

前記第１集合および前記第２集合の少なくとも一方が、前記複数個の秘密計算装置を要素とする全体集合の真部分集合である、秘密計算システム。

[請求項3] 請求項２の秘密計算システムであって、

前記共通部分に属する前記秘密計算装置は、前記共通部分の補集合に属する秘密計算装置の前記対象データの秘密分散値および前記クエリまたは前記クエリの秘密分散値の少なくとも一方を復元する復元部

を有する、秘密計算システム。

[請求項4] 請求項２または３の秘密計算システムであって、

前記共通部分に属する前記秘密計算装置の前記出力部は、前記共通部分の要素数が前記演算結果を復元するために必要な秘密分散値の個数以上である場合に、前記演算結果の秘密分散値を出力する、秘密計算システム。

[請求項5] 請求項２から４の何れかの秘密計算システムであって、

前記整合性検証部が、前記全体集合の第１部分集合での前記対象データの秘密分散値の整合性検証が不合格であった場合、前記第１部分集合の真部分集合を前記第１部分集合として前記対象データの秘密分散値の整合性検証を行う第１再帰処理を行う、および／または、前記全体集合の第２部分集合での前記クエリまたは前記クエリの秘密分散値の整合性検証が不合格であった場合、前記第２部分集合の真部分集合を前記第２部分集合として前記クエリまたは前記クエリの秘密分散値の整合性検証を行う第２再帰処理を行う、秘密計算システム。

[請求項6] 請求項２から５の何れかの秘密計算システムであって、

前記整合性検証部が、前記全体集合の第３部分集合での前記対象データの秘密分散値の整合性検証が不合格であった場合、前記第３部分集合の真部分集合と前記第３部分集合の補集合の部分集合との和集合を前記第３部分集合として前記対象データの秘密分散値の整合性検証を行う第３再帰処理を行う、および／または、前記全体集合の第４部分集合での前記クエリまたは前記クエリの秘密分散値の整合性検証が不合格であった場合、前記第４部分集合の真部分集合と前記第４部分集合の補集合の部分集合との和集合を前記第４部分集合として前記クエリまたは前記クエリの秘密分散値の整合性検証を行う第４再帰処理を行う、秘密計算システム。

[請求項7] 請求項１から６の何れかの秘密計算システムであって、

前記整合性検証部は、前記対象データの秘密分散値および前記クエ

リまたは前記クエリの秘密分散値の整合性検証をまとめて行う、秘密計算システム。

[請求項8] 請求項７の秘密計算システムであって、

前記整合性検証部は、前記対象データの秘密分散値および前記クエリまたは前記クエリの秘密分散値を含む情報を撹乱させた情報の整合性検証を行う、秘密計算システム。

[請求項9] 請求項１から８の何れかの秘密計算システムであって、

前記整合性検証部は、

前記複数個の秘密計算装置を要素とする全体集合の部分集合で得られた複数個の任意値の合成値ｓを得る合成部と、

前記合成値ｓの関数値を係数とし、前記対象データの秘密分散値および前記クエリまたは前記クエリの秘密分散値の少なくとも一方を含む値の線形結合値［ｃ］$_i$を得る線形結合部と、

前記線形結合値［ｃ］$_i$に応じた秘密分散値［ｄ］$_i$を他の秘密計算装置に配送して整合性検証を行う検証部と、を含む、秘密計算システム。

[請求項10] 請求項９の秘密計算システムであって、

前記整合性検証部は、

乱数秘密分散値［Ｒ］$_i$を得る撹乱値設定部と、

前記乱数秘密分散値［Ｒ］$_i$で前記線形結合値［ｃ］$_i$を撹乱させた前記秘密分散値［ｄ］$_i$を得る撹乱部と、を含む、秘密計算システム。

[請求項11] 秘密計算の対象となる対象データの秘密分散値を格納する記憶部と、

前記秘密計算を要求するクエリまたは前記クエリの秘密分散値が入力される入力部と、

前記対象データの秘密分散値の整合性検証および前記クエリまたは前記クエリの秘密分散値の整合性検証を行う整合性検証部と、

整合性検証に合格した前記対象データの秘密分散値を用い、整合性検証に合格した前記クエリまたは前記クエリの秘密分散値に応じた秘密計算を行って演算結果の秘密分散値を得る秘密計算部と、

前記演算結果の秘密分散値を出力する出力部と、

を有する秘密計算装置。

[請求項12] 請求項１１の秘密計算装置であって、

前記整合性検証部は、前記対象データの秘密分散値および前記クエリまたは前記クエリの秘密分散値の整合性検証をまとめて行う、秘密計算装置。

[請求項13] 請求項１２の秘密計算装置であって、

前記整合性検証部は、前記対象データの秘密分散値および前記クエリまたは前記クエリの秘密分散値を含む情報を撹乱させた情報の整合性検証を行う、秘密計算装置。

[請求項14] 請求項１１から１３の何れかの秘密計算装置であって、

前記整合性検証部は、

複数個の任意値の合成値ｓを得る合成部と、

前記合成値ｓの関数値を係数とし、前記対象データの秘密分散値および前記クエリまたは前記クエリの秘密分散値の少なくとも一方を含む値の線形結合値［ｃ］$_i$を得る線形結合部と、

前記線形結合値［ｃ］$_i$に応じた秘密分散値［ｄ］$_i$を他の秘密計算装置に配送して整合性検証を行う検証部と、を含む、秘密計算装置。

[請求項15] 請求項１４の秘密計算装置であって、

前記整合性検証部は、

乱数秘密分散値［Ｒ］$_i$を得る撹乱値設定部と、

前記乱数秘密分散値［Ｒ］$_i$で前記線形結合値［ｃ］$_i$を撹乱させた前記秘密分散値［ｄ］$_i$を得る撹乱部と、を含む、秘密計算装置。

[請求項16] 秘密計算の対象となる対象データの秘密分散値を記憶部に格納し、

前記秘密計算を要求するクエリまたは前記クエリの秘密分散値を受け付け、

前記対象データの秘密分散値の整合性検証および前記クエリまたは前記クエリの秘密分散値の整合性検証を行い、

整合性検証に合格した前記対象データの秘密分散値を用い、整合性検証に合格した前記クエリまたは前記クエリの秘密分散値に応じた秘密計算を行って演算結果の秘密分散値を得、

前記演算結果の秘密分散値を出力する、

を有する秘密計算方法。

［請求項17］ 請求項１１から１５のいずれかの秘密計算装置としてコンピュータを機能させるためのプログラム。

[図1]

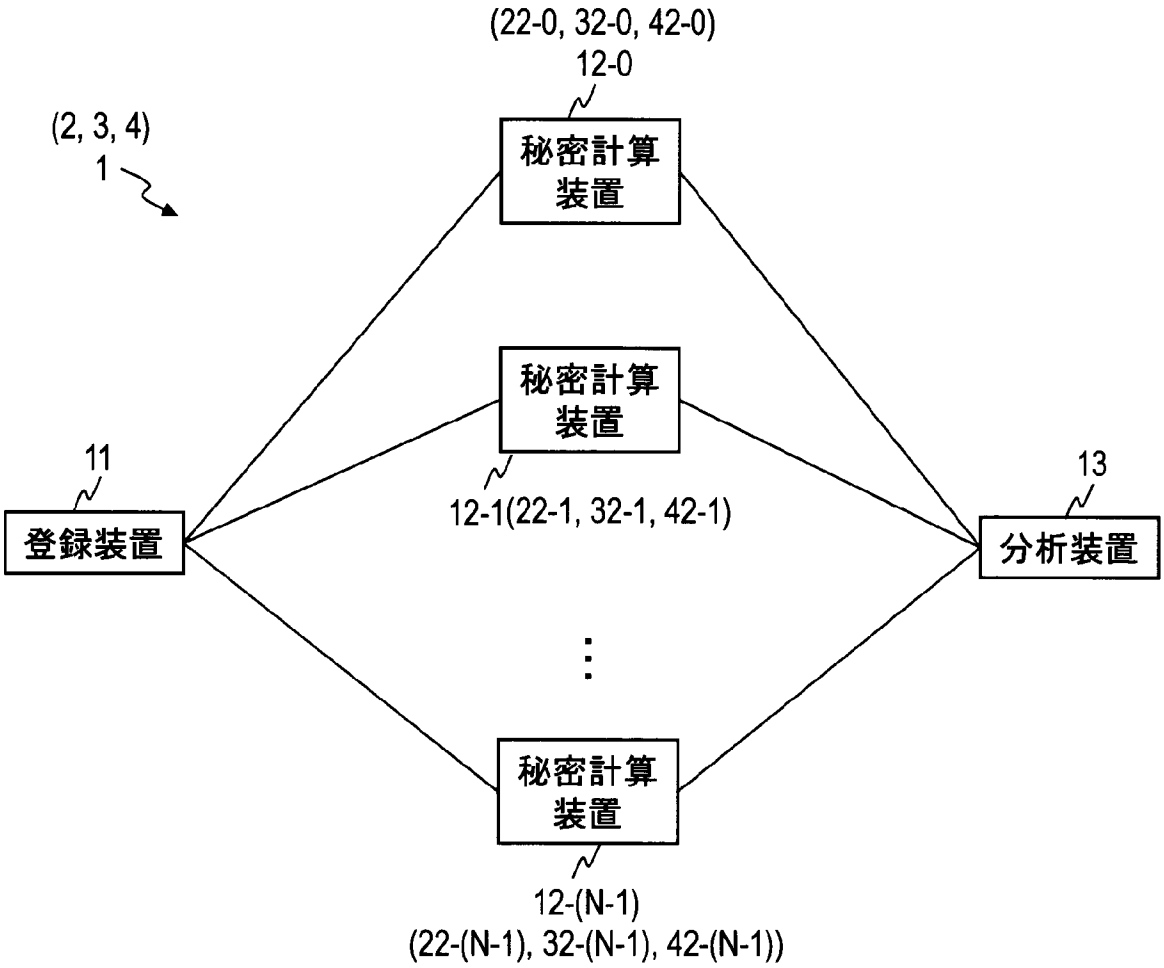

(22-0, 32-0, 42-0)
12-0
(2, 3, 4)
1
秘密計算装置
秘密計算装置
11
登録装置
12-1(22-1, 32-1, 42-1)
13
分析装置
秘密計算装置
12-(N-1)
(22-(N-1), 32-(N-1), 42-(N-1))

図1

[図2]

図2A

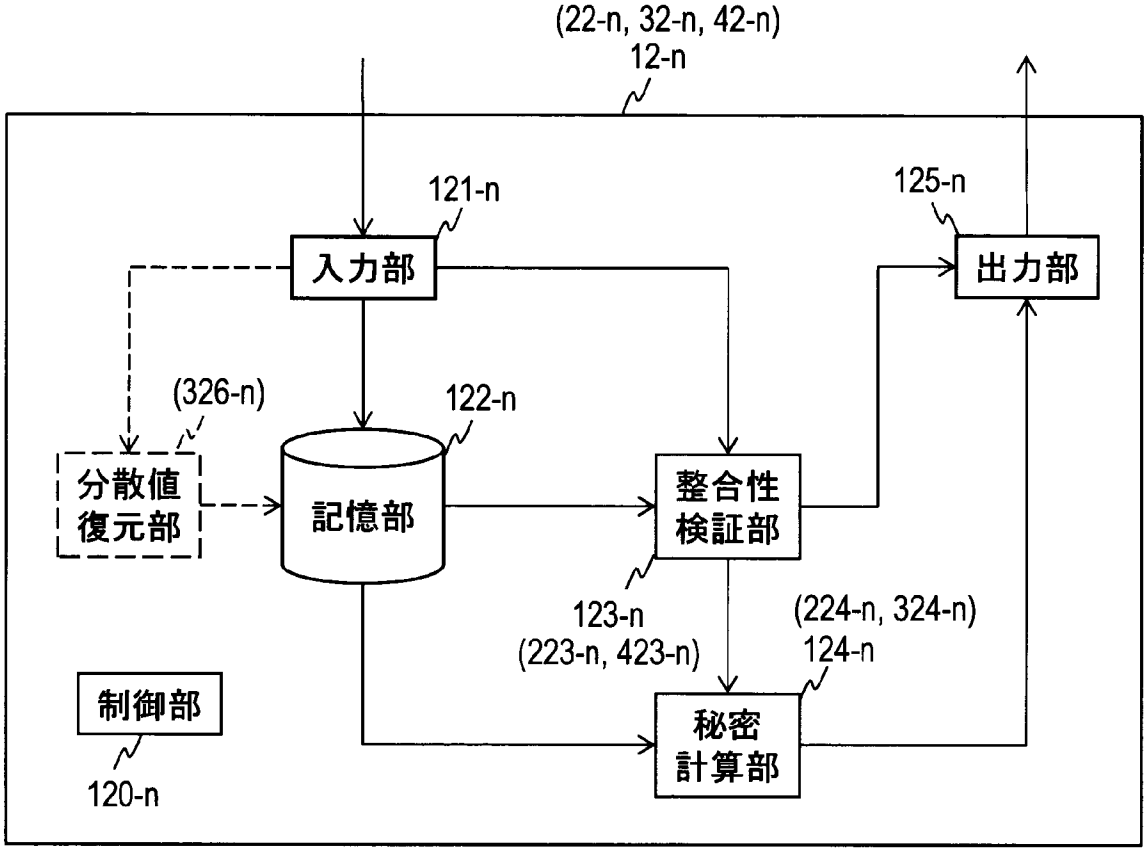
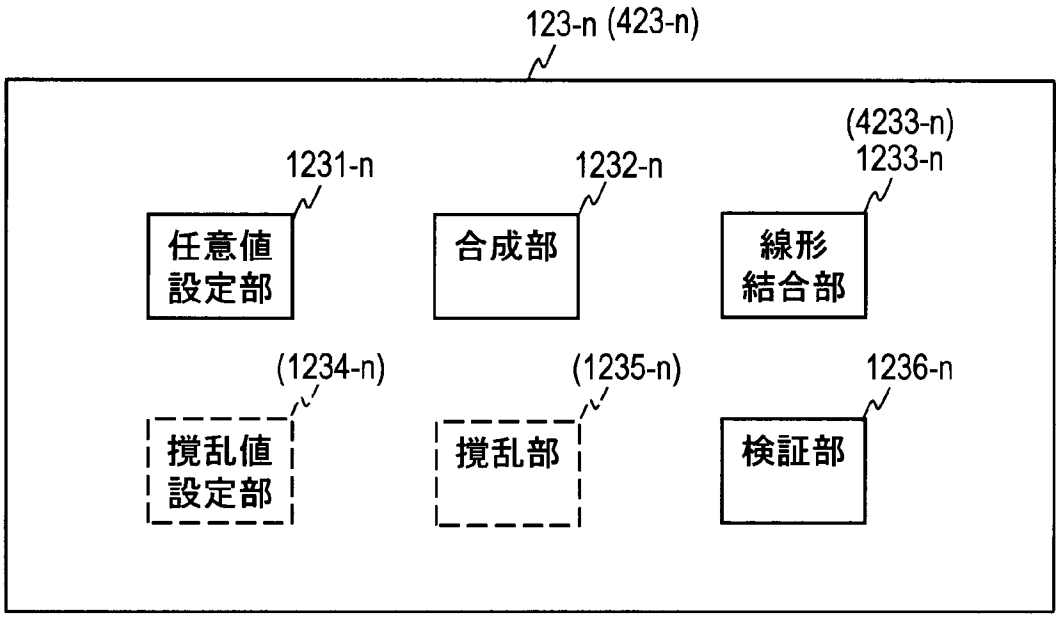

(22-n, 32-n, 42-n)
12-n
121-n
入力部
125-n
出力部
(326-n)
122-n
分散値
復元部
記憶部
整合性
検証部
123-n
(223-n, 423-n)
(224-n, 324-n)
124-n
制御部
120-n
秘密
計算部

図2B


123-n (423-n)
1231-n
任意値
設定部
1232-n
合成部
(4233-n)
1233-n
線形
結合部
(1234-n)
撹乱値
設定部
(1235-n)
撹乱部
1236-n
検証部

[図3]

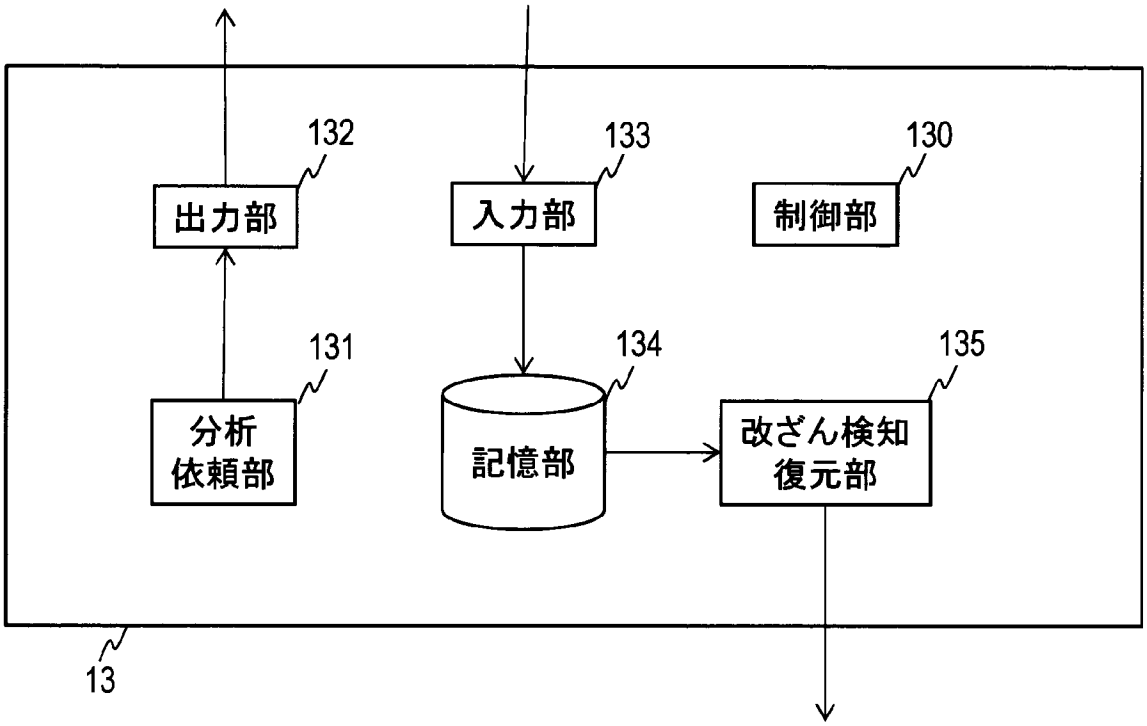



図3

[図4]

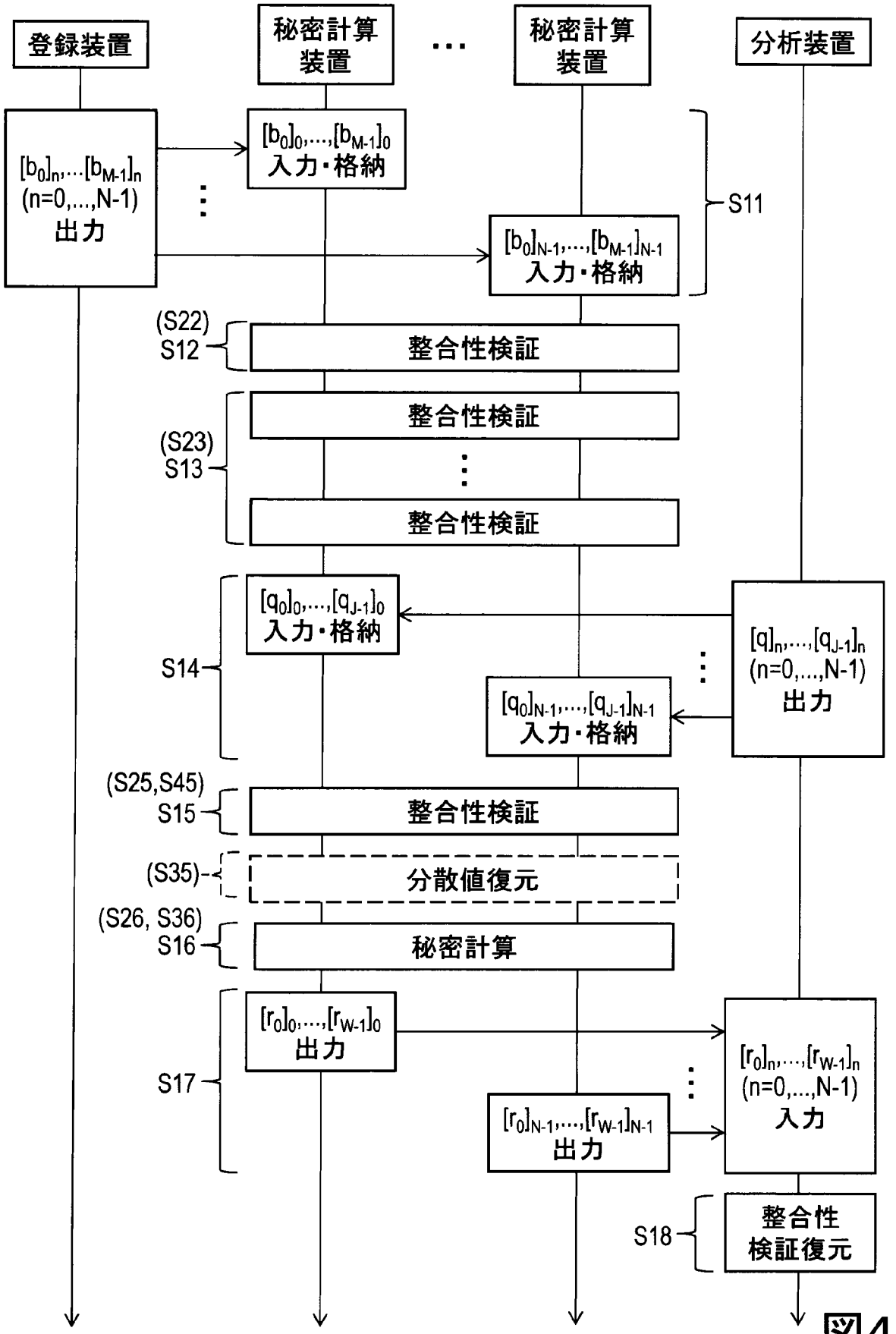

登録装置
秘密計算装置
秘密計算装置
分析装置
$[b_0]_n,\ldots,[b_{M-1}]_n$ (n=0,...,N-1) 出力
$[b_0]_0,\ldots,[b_{M-1}]_0$ 入力・格納
$[b_0]_{N-1},\ldots,[b_{M-1}]_{N-1}$ 入力・格納
S11
(S22) S12
整合性検証
(S23) S13
整合性検証
整合性検証
S14
$[q_0]_0,\ldots,[q_{J-1}]_0$ 入力・格納
$[q_0]_{N-1},\ldots,[q_{J-1}]_{N-1}$ 入力・格納
$[q]_n,\ldots,[q_{J-1}]_n$ (n=0,...,N-1) 出力
(S25,S45) S15
整合性検証
(S35)
分散値復元
(S26, S36) S16
秘密計算
S17
$[r_0]_0,\ldots,[r_{W-1}]_0$ 出力
$[r_0]_{N-1},\ldots,[r_{W-1}]_{N-1}$ 出力
$[r_0]_n,\ldots,[r_{W-1}]_n$ (n=0,...,N-1) 入力
S18
整合性検証復元

図4

[図5]

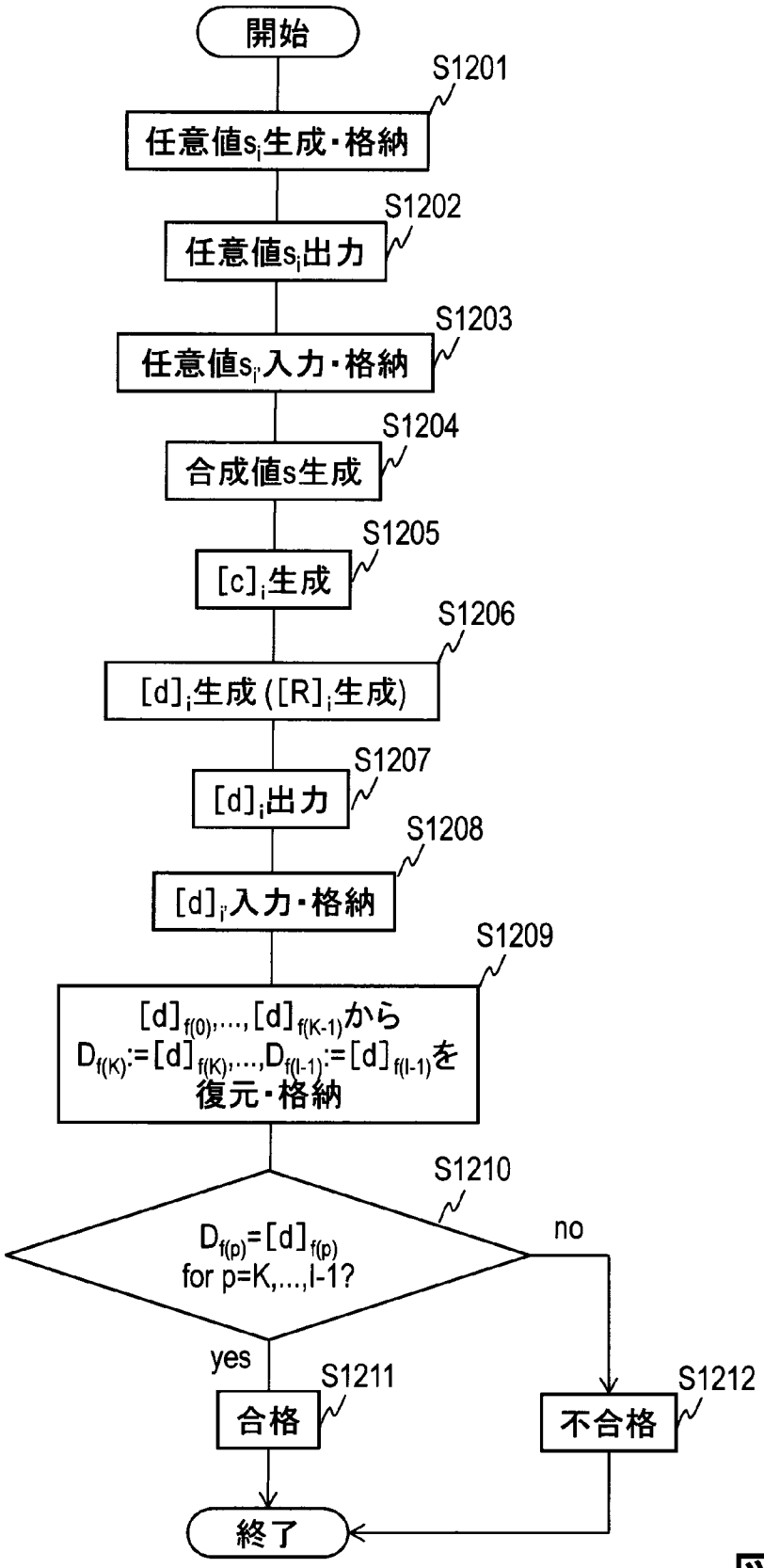

開始
S1201
任意値$s_i$生成・格納
S1202
任意値$s_i$出力
S1203
任意値$s_{i'}$入力・格納
S1204
合成値s生成
S1205
$[c]_i$生成
S1206
$[d]_i$生成($[R]_i$生成)
S1207
$[d]_i$出力
S1208
$[d]_{i'}$入力・格納
S1209
$[d]_{f(0)},\ldots,[d]_{f(K-1)}$から
$D_{f(K)}:=[d]_{f(K)},\ldots,D_{f(l-1)}:=[d]_{f(l-1)}$を
復元・格納
S1210
$D_{f(p)}=[d]_{f(p)}$
for p=K,...,l-1?
no
yes
S1211
合格
S1212
不合格
終了

図5

[図6]

図6A

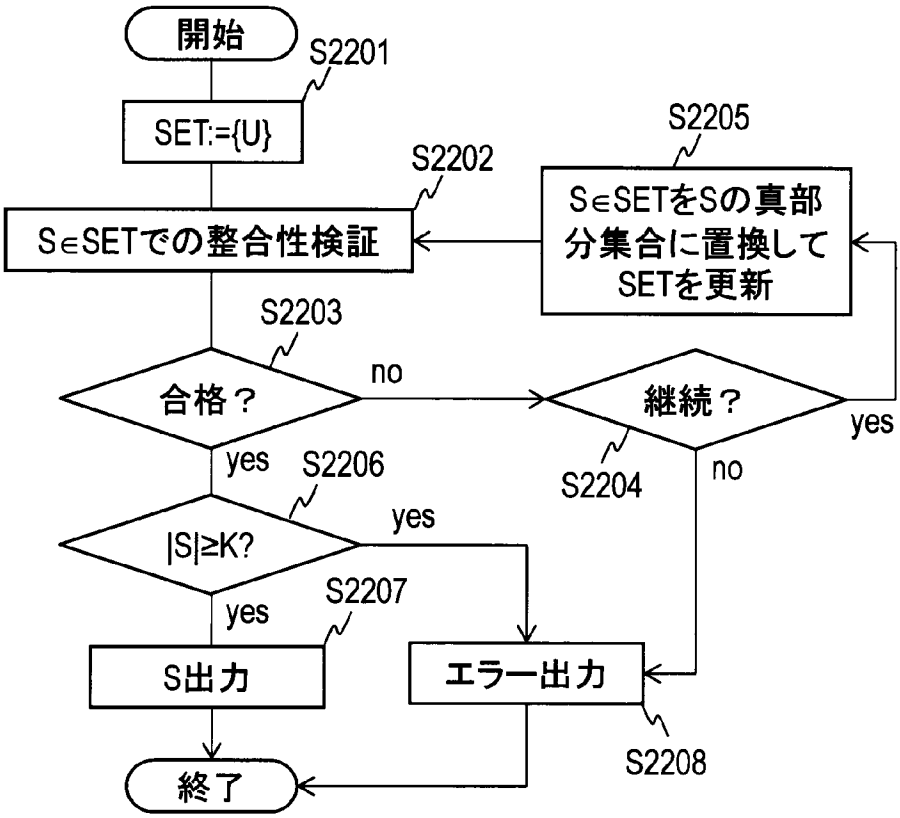
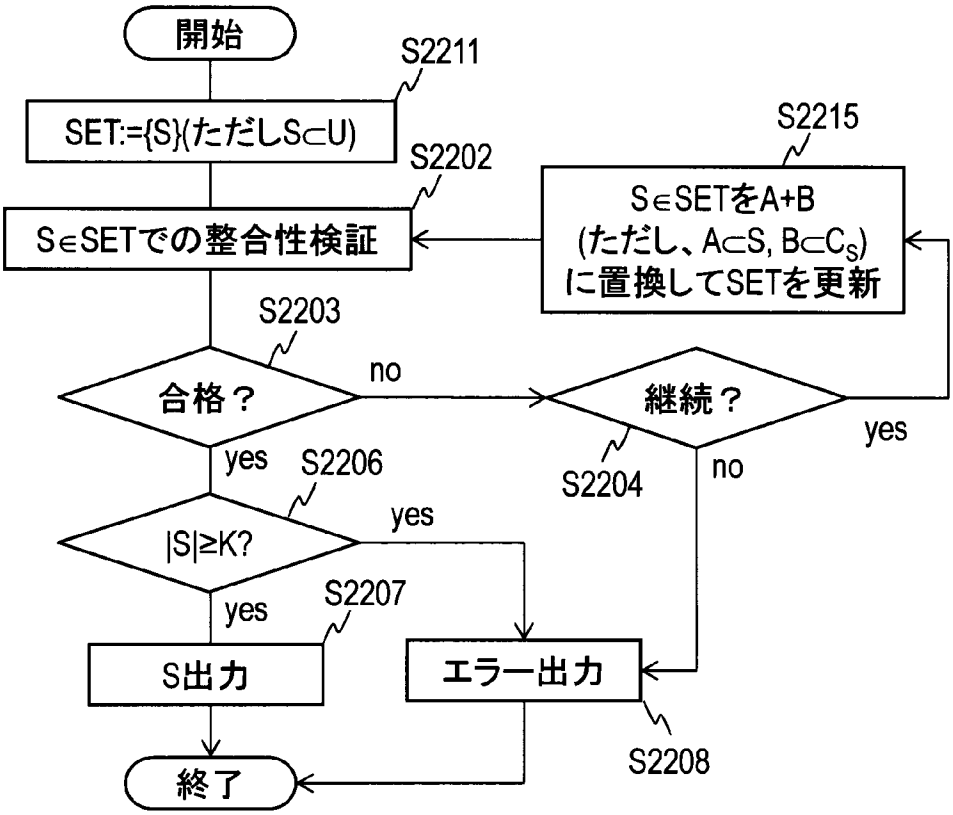

開始
S2201
SET:={U}
S2202
S∈SETでの整合性検証
S2205
S∈SETをSの真部分集合に置換してSETを更新
S2203
合格？
no
継続？
yes
S2204
no
yes
S2206
|S|≥K?
yes
yes
S2207
S出力
エラー出力
S2208
終了

図6B


開始
S2211
SET:={S}(ただしS⊂U)
S2202
S∈SETでの整合性検証
S2215
S∈SETをA+B
(ただし、A⊂S, B⊂C_S)
に置換してSETを更新
S2203
合格？
no
継続？
yes
S2204
no
yes
S2206
|S|≥K?
yes
yes
S2207
S出力
エラー出力
S2208
終了

[図7]

図7A

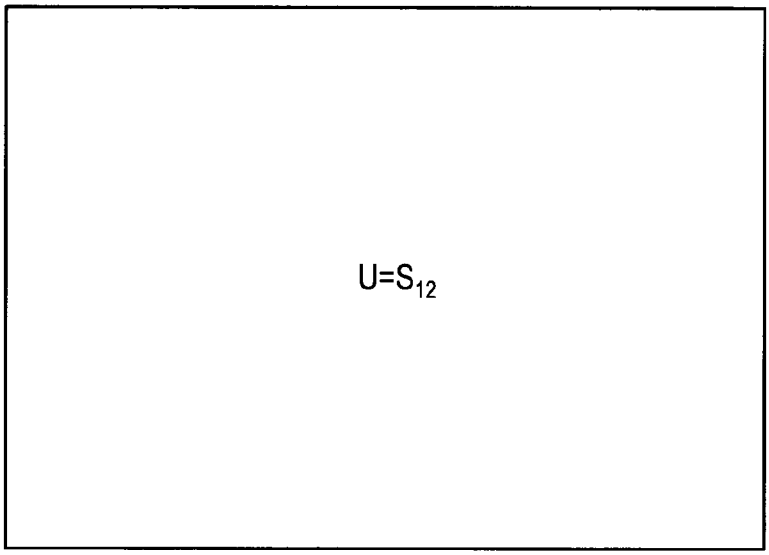
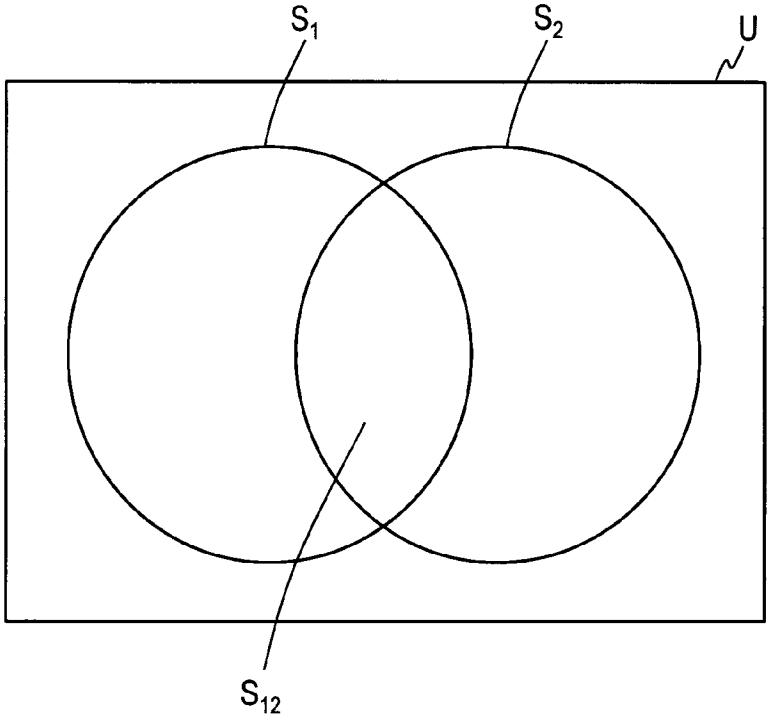



図7B



[図8]

図8A

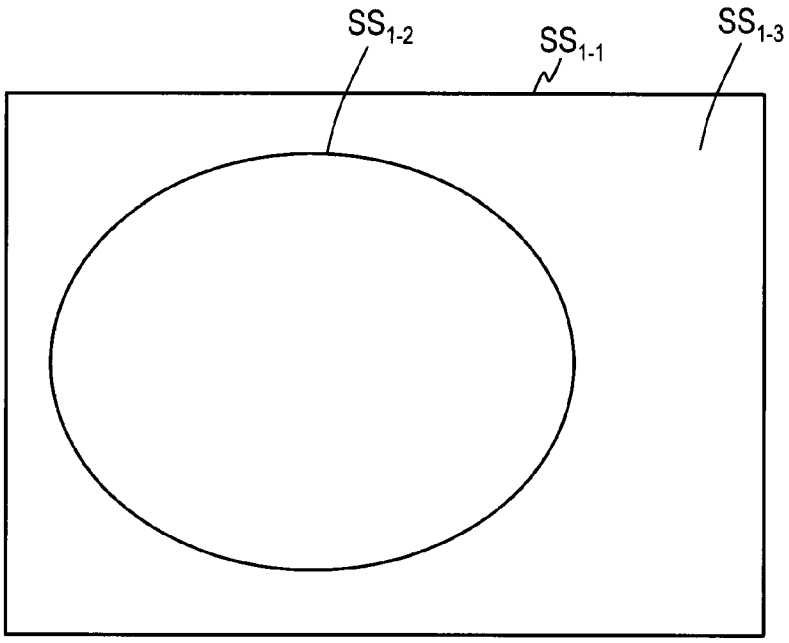
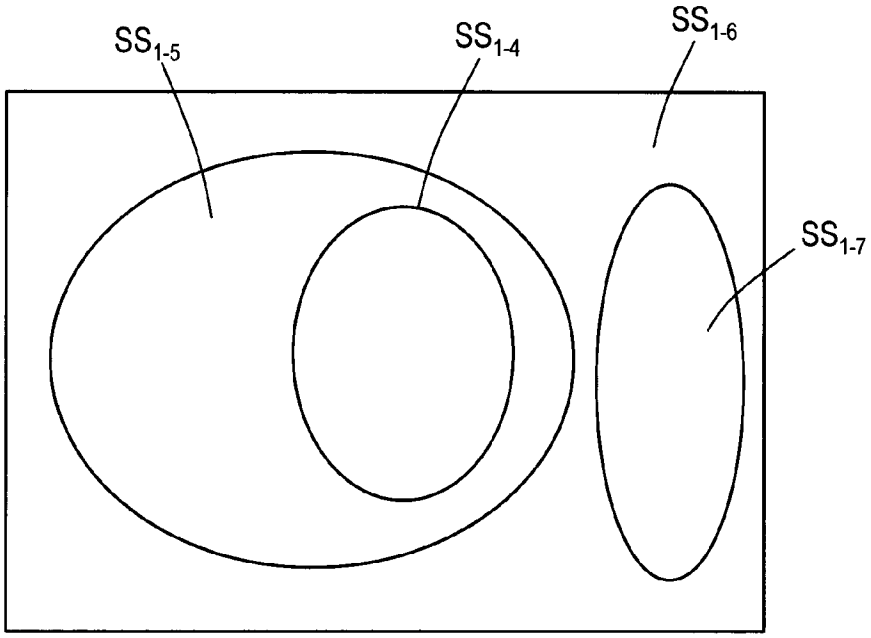



図8B



[図9]

図9A

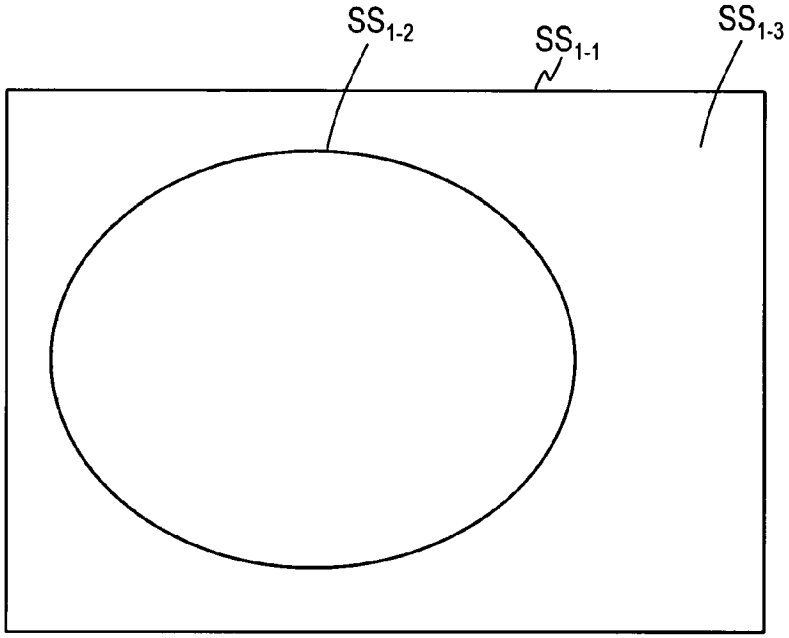
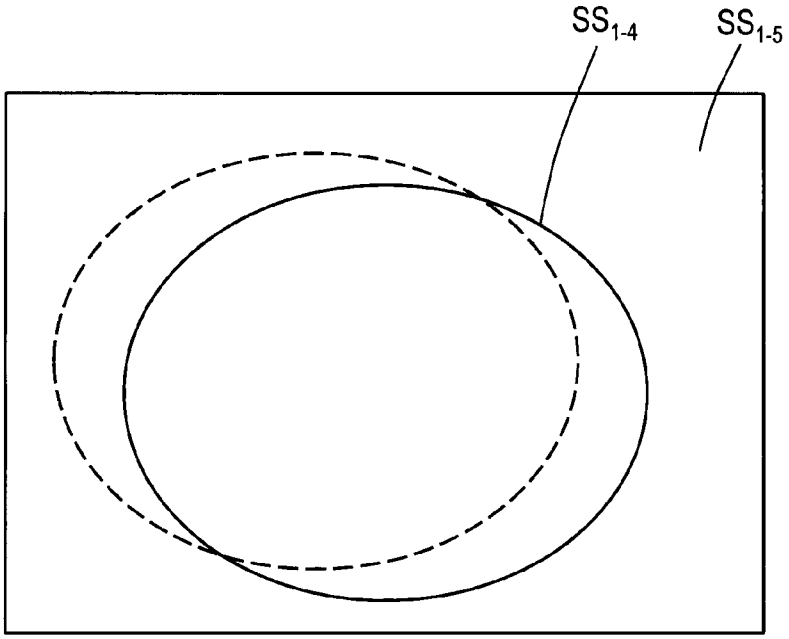



図9B



[図10]

図10A

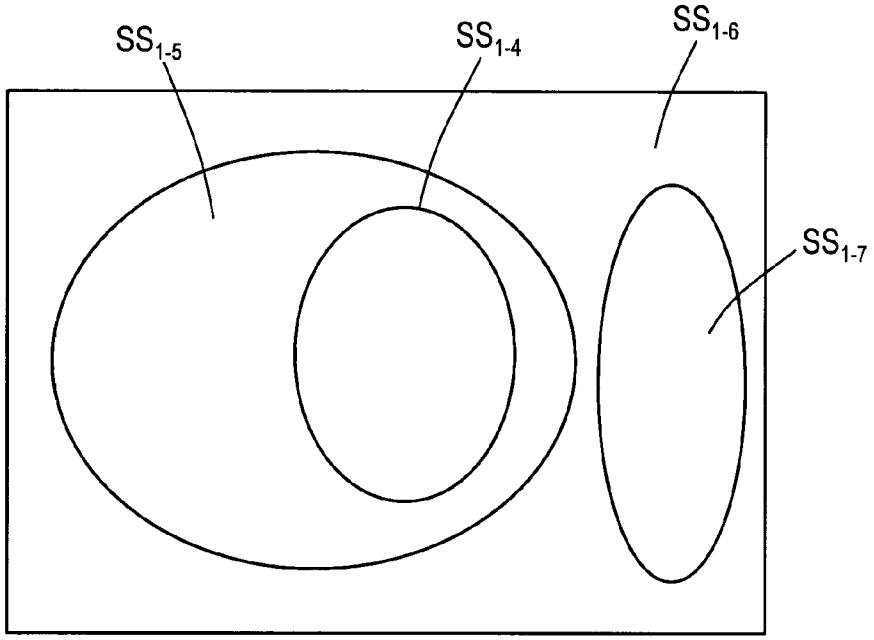
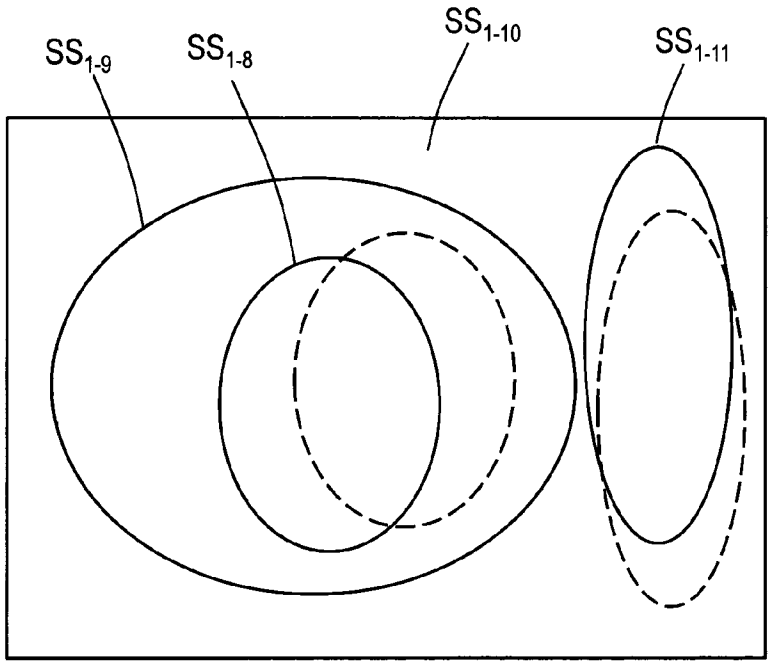



図10B



# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/071221

A. CLASSIFICATION OF SUBJECT MATTER
*G06F21/60*(2013.01)i, *G06F21/64*(2013.01)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)
G06F21/60, G06F21/64, 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 | 1996-2016 |
| Kokai Jitsuyo Shinan Koho | 1971-2016 | Toroku Jitsuyo Shinan Koho | 1994-2016 |

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamIII), IEEE Xplore,
multi-party computation

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y<br>A | Masanori SHIMURA et al., "Relational Algebra in Multi-party Protocol to Enable Structual Operation in Secret Shared Databases", Transactions of Information Processing Society of Japan, 15 September 2010 (15.09.2010), vol. 51, no.9, pages 1563 to 1578 | 1,2,4,7,8, 11-13,16,17<br>3,5,6,9,10, 14,15 |
| Y<br>A | JP 2014-137474 A (Nippon Telegraph and Telephone Corp.), 28 July 2014 (28.07.2014), paragraphs [0015] to [0034] | 1,2,4,7,8, 11-13,16,17<br>3,5,6,9,10, 14,15 |
| Y<br>A | Ryo KIKUCHI et al., "Kaizan Kenchi Kinotsuki no Jitsuyoteki na Himitsu Keisan System MEVAL 2", 2015 Nen Symposium on Cryptography and Information Security Koen Ronbunshu, 20 January 2015 (20.01.2015), pages 1 to 8 | 1,2,4,7,8, 11-13,16,17<br>3,5,6,9,10, 14,15 |

☒ 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<br>08 August 2016 (08.08.16) | Date of mailing of the international search report<br>16 August 2016 (16.08.16) |
| Name and mailing address of the ISA/<br>Japan Patent Office<br>3-4-3,Kasumigaseki,Chiyoda-ku,<br>Tokyo 100-8915,Japan | Authorized officer<br><br>Telephone No. |

**INTERNATIONAL SEARCH REPORT**

International application No.
PCT/JP2016/071221

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | US 2012/0002811 A1 (THE UNIVERSITY OF BRISTOL), 05 January 2012 (05.01.2012), all pages | 1-17 |
| A | US 2012/0070000 A1 (ALCATEL-LUCENT USA INC.), 22 March 2012 (22.03.2012), all pages | 1-17 |
| A | US 2012/0233460 A1 (Microsft Corp.), 13 September 2012 (13.09.2012), all pages | 1-17 |
| A | WO 2014/052113 A1 (ALCATEL LUCENT), 03 April 2014 (03.04.2014), all pages | 1-17 |
| A | Koji CHIDA et al., "Cloud Bussiness o Sasaeru Security Kiban Gijutsu", NTT Gijutsu Journal, 01 March 2014 (01.03.2014), vol.26, no.3, pages 67 to 70 | 1-17 |
| A | Naoto KIRIBUCHI et al., "Teisu Round Kanzen Icchi Kensaku no tameno Himitsu Keisan Protocol", 2014 Nen Symposium on Cryptography and Information Security Koen Ronbunshu, 21 January 2014 (21.01.2014), pages 1 to 7 | 1-17 |

**INTERNATIONAL SEARCH REPORT**
Information on patent family members

International application No.
PCT/JP2016/071221

| | | |
|---|---|---|
| JP 2014-137474 A | 2014.07.28 | (Family: none) |
| US 2012/0002811 A1 | 2012.01.05 | (Family: none) |
| US 2012/0070000 A1 | 2012.03.22 | (Family: none) |
| US 2012/0233460 A1 | 2012.09.13 | (Family: none) |
| WO 2014/052113 A1 | 2014.04.03 | JP 2015-530623 A 2015.10.15<br>US 2014/0105393 A1 2014.04.17<br>EP 2901613 A1 2015.08.05<br>CN 104685826 A 2015.06.03<br>KR 10-2015-0048827 A 2015.05.07 |

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１６／０７１２２１

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/60(2013.01)i, G06F21/64(2013.01)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（ＩＰＣ））

Int.Cl.　G06F21/60, G06F21/64, 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 | １９７１－２０１６年 |
| 日本国実用新案登録公報 | １９９６－２０１６年 |
| 日本国登録実用新案公報 | １９９４－２０１６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 (JDreamIII), IEEE Xplore
multi-party computation

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 |
|---|---|---|
| Y<br>A | 志村正法 他，秘密分散データベースの構造演算を可能にするマルチパーティプロトコルを用いた関係代数演算，情報処理学会論文誌，2010.09.15，第51巻 第9号，p.1563-1578 | 1,2,4,7,8,11-13,16,17<br>3,5,6,9,10,14,15 |
| Y<br>A | JP 2014-137474 A（日本電信電話株式会社）2014.07.28，段落[0015]-[0034] | 1,2,4,7,8,11-13,16,17<br>3,5,6,9,10,14,15 |

☑　Ｃ欄の続きにも文献が列挙されている。

☑　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

| 国際調査を完了した日 | 国際調査報告の発送日 |
|---|---|
| ０８．０８．２０１６ | １６．０８．２０１６ |

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　９３６４
中里　裕正
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 |
|---|---|---|
| Ｙ<br>Ａ | 菊池亮 他，改ざん検知機能付きの実用的な秘密計算システム　ＭＥＶＡＬ２，２０１５年暗号と情報セキュリティシンポジウム講演論文集，2015.01.20，p.1-8 | 1,2,4,7,8,11-13,16,17<br>3,5,6,9,10,14,15 |
| Ａ | US 2012/0002811 A1 (THE UNIVERSITY OF BRISTOL) 2012.01.05，全頁を参照 | 1-17 |
| Ａ | US 2012/0070000 A1 (ALCATEL-LUCENT USA INC.) 2012.03.22，全頁を参照 | 1-17 |
| Ａ | US 2012/0233460 A1 (Microsft Corporation) 2012.09.13，全頁を参照 | 1-17 |
| Ａ | WO 2014/052113 A1 (ALCATEL LUCENT) 2014.04.03，全頁を参照 | 1-17 |
| Ａ | 千田浩司 他，クラウドビジネスを支えるセキュリティ基盤技術，ＮＴＴ技術ジャーナル，2014.03.01，第26巻 第3号，p.67-70 | 1-17 |
| Ａ | 桐淵直人 他，定数ラウンド完全一致検索のための秘密計算プロトコル，２０１４年暗号と情報セキュリティシンポジウム講演論文集，2014.01.21，p.1-7 | 1-17 |

国際調査報告
パテントファミリーに関する情報

国際出願番号 ＰＣＴ／ＪＰ２０１６／０７１２２１

| | | | |
|---|---|---|---|
| JP 2014-137474 A | 2014.07.28 | ファミリーなし | |
| US 2012/0002811 A1 | 2012.01.05 | ファミリーなし | |
| US 2012/0070000 A1 | 2012.03.22 | ファミリーなし | |
| US 2012/0233460 A1 | 2012.09.13 | ファミリーなし | |
| WO 2014/052113 A1 | 2014.04.03 | JP 2015-530623 A | 2015.10.15 |
| | | US 2014/0105393 A1 | 2014.04.17 |
| | | EP 2901613 A1 | 2015.08.05 |
| | | CN 104685826 A | 2015.06.03 |
| | | KR 10-2015-0048827 A | 2015.05.07 |