(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
2019 年 12 月 26 日 (26.12.2019)

WIPO IPCT

(10) 国際公開番号
\¥0 2019/244756 入1

(51) 国際特許分類：
0090 1/00 (2006.01)

(21) 国際出願番号： P(：171?2019/023390

(22) 国際出願日： 2019 年 6 月 13 日 (13.06.2019)

(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 2018-1 16576 2018 年 6 月 20 日 (20.06.2018) JP

(71) 出願人：日本電信電話株式会社 **(NIPPON TELEGRAPH AND TELEPHONE CORPORATION)** [JP/JP]；〒10081 16 東京都千代田区大手町一丁目 5 番 1 号 Tokyo (JP).

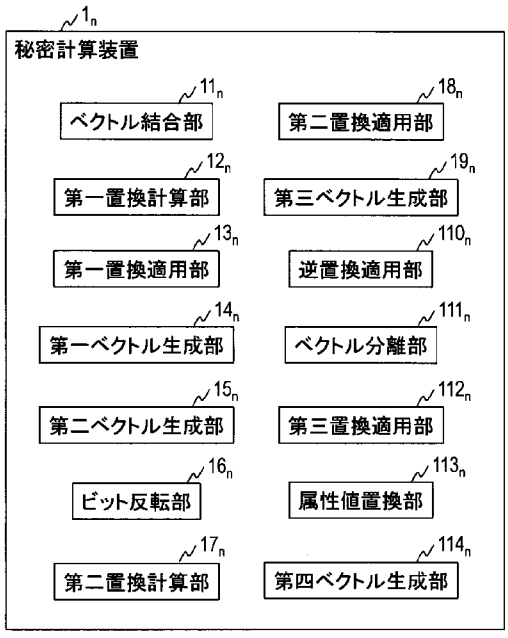
(72) 発明者：五十嵐 大 **(IKARASHI ,Dai)**；〒 1808585 東京都武蔵野市緑町三丁目 **9** 番 **1 1** 号 **NTT** 知的財産センタ内 Tokyo (JP). 濱田 浩気 **(HAMADA ,Koki)**；〒 1808585 東京都武蔵野市緑町三丁目 **9** 番 **1 1** 号 **NTT** 知的財産センタ内 Tokyo (JP).

(74) 代理人：中尾 直樹，外 (、八1ζA0，**Naoki** et 纪.)；〒 1600022 東京都新宿区新宿三丁目 1 番 2 2 号 新宿 问已0 ビル 6 階 丁Ο砂 ○ (圯)·

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能)：处 ，人ら 人レ AM, 人○, 人丁，人11, 心 ，6 ん 66, 60, 611, BN, BR, 6 W, BY, 似 ，○ん ○ I, ○,，。凡 00, CI1, 01, CZ, 0 ¾ ○1. ○反, 0¾/[, ○○, DZ, EC, EE, EG, ES, ?**1, 0 6 ,** GD, **0** ¾ 011 **, 0** ¾/[, 0 T；

(54) **Title:** SECRET COMBINATION SYSTEM, METHOD, SECRET CALCULATION DEVICE, AND PROGRAM

(54) 発明の名称：秘密結合システム、方法、秘密計算装置及びプログラム



1_n Secret calculation device
11_n Vector combination unit
12_n First permutation calculation unit
13_R First permutation application unit
14_p First vector generation unit
15_p Second vector generation unit
16_n Bit inversion unit
17_p Second permutation calculation unit
18_n Second permutation application unit
19_n Third vector generation unit
110_n Inverse permutation application unit
111_n Vector separation unit
112_n Third permutation application unit
113_n Attribute value permutation unit
114_n Fourth vector generation unit

図 **2**

(57) Abstract: This secret combination system includes a plurality of secret calculation devices, and the plurality of secret calculation devices are each provided with a vector combination unit 11_n, a first permutation calculation unit 12_n, a first permutation application unit 13_n, a first vector generation unit 14_n, a second vector generation unit 15_n, a bit inversion unit 16_n, a second permutation calculation unit 17_n, a second permutation application unit 18_n, a third vector generation unit 19_n, an inverse permutation application unit 110_n, a vector

W○ 2019/244756 A1

[続葉有]

11凡 1111, 1111, 10, 1レ 1凡 III, IS, X), 疋 现 , 反〇, 101, 1〈N, 1¾ 101, 反界, KZ, し八, し〇, 1^, 1.11, 1.S, 风 1.Y,]Mん MD, 嫌 , MG, MK, 丽 ,]^, MX, MY, MZ, 贼 如 , N1, N0, 似 , 〇]^, 卩ん PE, 戸。, 卩11, 卩し, 卩丁, (5人 110, 118, 1111, 尺界 ,8人 8 (: ,80, SE, 80, 81^ ,SL, 81^, 81; SV, 8乂 111, 17, TM, 1^, 711, 丁丁, 丁¾ 11八, 110, 1JS ,11¾ 见 , VN, Σん 兀M, Σ界.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): AR1卩0 田界, 011, 01^, 反¾ 1^1, 1^,]M界, MZ, NA, 尺界 ,80, SL, 81; SZ, 丁Σ, 110, 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, 0 K, £¾ £8^1, 戸艮 03, 011, 1111, 1111, 1¾ IS, II; 1.T ,し11, 1^/, MC, MK, M丁, 见 , N0, 卩レ 卩丁, 110, 118, 8¾ 81, 8K, 81^ ,见),0处 1田ろ3Ⅰ,〇尸,00, 〇,〇M, 。ん 。凡 GQ, GW, 疆 ,他 , 1^11, 呢 SN, TD, 丁。).

添付公開書類:

- 国際調査報告 (条約第21条(3))

separation unit lli $_n$, a third permutation application unit 112_n, an atribute value permutation unit 113_n, and a fourth vector generation unit 114_n.

(57) 要約: 秘密結合システムは、複数の秘密計算装置を含む秘密結合システムであって、複数の秘密計算装置は、ベクトル結合部11„、第一置換計算部12„、第一置換適用部13„、第一ベクトル生成部14„、第二ベクトル生成部15„、ビット反転部16„、第二置換計算部17„、第二置換適用部18„、第三ベクトル生成部19„、逆置換適用部110„、ベクトル分離部111„、第三置換適用部112„、属性値置換部113„及び第四ベクトル生成部114„を備えている。

明 細 書

発明の名称 :

秘密結合システム、方法、秘密計算装置及びプログラム

技術分野

[0001] この発明は、秘密計算技術に関する。この発明は、特に、秘匿性を保ったまま2つのテーブルを結合する技術に関する。

背景技術

[0002] 秘密計算技術の分野において、秘匿性を保ったまま2つのテーブルを結合する技術が求められている。

[0003] 秘匿性を保ったまま2つのテーブルを結合する技術として、例えば非特許文献1に記載された技術が知られている。非特許文献1では、キー重複ありの場合の等結合が実現されている。

先行技術文献

非特許文献

[0004] 非特許文献1:桐淵直人、五十嵐大、諸橋玄武、濱田浩気、 属性情報と履歴情報の秘匿統合分析に向けた秘密計算による高速な等結合アルゴリズムとその実装」、055201 6, 201 6

発明の概要

発明が解決しようとする課題

[0005] この発明は、キー重複がない場合に非特許文献1の技術よりも高速に秘匿性を保ったまま2つのテーブルを結合する秘密結合システム、方法、秘密計算装置及びプログラムを提供することである。

課題を解決するための手段

[0006] この発明の一態様による秘密結合システムは、複数の秘密計算装置を含む秘密結合システムであって、Ꮷは任意の環であり、《を任意のベクトルとして[«]は《が秘密分散されたシェアであり、ß を任意の置換として{{β}}はß

が秘密分散されたシェアであり、m_0, m_1, L_0, L_1は１以上の整数であり、$k_0 \in F^{m0}$は第一テーブルのキーのベクトルであり、$k_1 \in F^{m1}$は第二テーブルのキーのベクトルであり、ロ＝０，…，1_0－１として$v_{0,}$已ドｒ０は第一テーブルの属性ロの属性値のベクトルであり、ロ＝０，…，L_1−1として$v_{1,q} \in F^{m1}$は第二テーブルの属性ロの属性値のベクトルであり、７１：$_0$，７１：，はそれぞれ長さ111_0，111，の所定の置換であり、複数の秘密計算装置は、ベクトルk_0のシェア|＞$_0$］及びベクトルk_1のシェア|＞，］を用いて、ベクトルk_0及びベクトルk_1を結合したベクトル$k' \in [F]^{m0+m1}$のシェア|＞＇］を生成する複数のベクトル結合部と、シェア｜＞＇］を用いて、ベクトルビを昇順に安定ソートする置換£7のシェア｛｛び｝｝を生成する複数の第一置換計算部と、シェア1＞＇］及びシェア｛｛£7｝｝を用いて、ベクトルk'に置換〆を適用したベクトル£7（ビ）のシェア［£7び＇）］を生成する複数の第一置換適用部と、シェア［£7び＇）］を用いて、ベクトルび＇）のある要素とそのある要素の次の要素とが、同じ場合には１を、違う場合には〇をそのある要素に対応する要素として持つベクトル６のシェア|＞］を生成する複数の第一ベクトル生成部と、シェア|＞］を用いて、ベクトル㊀のある要素とそのある要素の前の要素の一方が１の場合には１を、そうでない場合には〇をそのある要素に対応する要素として持つベクトル６＇のシェア|＞＇］を生成する複数の第二ベクトル生成部と、シェア|＞＇］を用いて、ベクトル６＇の各要素をビット反転させたベクトルe＇＇のシェア[e＇＇］を生成する複数のビット反転部と、シェア1＞＇］を用いて、ベクトル６＇＇を昇順に安定ソートする置換ゲのシェア｛｛ゲ｝｝を生成する複数の第二置換計算部と、シェア|＞＇＇］及びシェア｛｛〆＇｝｝を用いて、ベクトル６＇＇に置換〆＇を適用したベクトルゲレ＇＇）のシェア［ゲレ＇＇）］を生成する複数の第二置換適用部と、シェア［〆＇（㊀＇＇）］を用いて、ベクトル〆＇（６＇＇）のある要素」が、０である場合には し_|/2 」を、０でない場合には０をそのある要素」に対応する要素として持つベクトルXのシェア｜＞］を生成する複数の第三ベクトル生成部と、シェア［X］、シェア｛｛び｝｝及びシェア｛｛〆＇｝｝を用いて、ベクトルXに置換〆＇の逆置換〆$'^{-1}$及び置換〆の逆置換〆$^{-1}$を適用したベクトル〆$^{-1}$（〆＇$^{-1}$（X））のシェアア[σ^{-1}(σ'$^{-1}$(x))]を生成する複数の逆置換適用部と、シェア[σ^{-1}(σ'$^{-1}$(x))]

を用いて、ベクトル び$^{-1}$ィび’$^{-1}$ひ))の先頭から叫個の要素からなるベクトルS_{0}のシェア[3_{0}]と、ベクトル ィ$^{-1}$(ィ’$^{-1}$(乂))の残りの$_{111}$個の要素からなるベクトルS_{1}のシェア[3,]とを生成する複数のベクトル分離部と、シェア[3_{0}]、シェア[3,]及び置換冗$_{0}$, $_{71}$:,を用いて、ベクトル3_{0}に置換$_{71}$;$_{0}$を適用したベクトル て$_{0}$:=$_{71}$;$_{0}$(3_{0})のシェア[$_{71}$;$_{0}$(3_{0})]と、ベクトルS_{1}に置換 π_{1}を適用したベクトル$\tau_{1}:=\pi_{1}(s_{1})$のシェア[π_{1}(3,)]とを生成して、 て$_{0}$:=7$\sum_{0}$(3_{0})及び て,:=$_{71}$:,(3,) を公開する複数の第三置換適用部と、置換?$\sum_{0}$のシエア{{$_{71}$;$_{0}$}}、置換$_{71}$:,のシエア{{$_{71}$:,}}、ベクトル ソ$_{0,p}$のシェア[> ø』]及びベクトル$_{V,q}$のシェア[V,コを用いて、第一テーブルの各属性口の属性値のベクトル ソ$_{0,p}$を置換 π_{0}で置換したベクトル ソ’$_{0,p}$のシェアレ’$_{0,p}$]と、第二テーブルの各属性口の属性値のベクトル$_{V,q}$を置換 π_{1}で置換したベクトル$_{V}$’$_{;q}$のシェア[ゲひ]とを生成する複数の属性値置換部と、ベクトル て$_{0}$、ベクトル ·$\sum$,、シェア[v’$_{0,p}$]及びシェア[v’$_{1,}$。を用いて、ベクトル ·$\sum_{0}$のi’番目の要素が$_{0}$でない場合にはベクトル ソ’りの$_{1}$’番目の要素を$_{1}$’-! 番目の要素として持つベクトル$_{V}$’’$_{0,p}$のシェア[v’’む]と、ベクトル て,の¡’番目の要素が$_{0}$でない場合にはベクトル$_{V}$’$_{,q}$の$_{1}$’番目の要素を$_{1}$’-! 番目の要素として持つベクトル$_{V}$’’いのシェアレ’’い]とを生成する複数の第四ベクトル生成部と、を備えている。

発明の効果

[0007] 逆置換を用いることで、キー重複がない場合に非特許文献1の技術よりも高速に秘匿性を保ったまま2つのテーブルを結合することができる。

図面の簡単な説明

[0008] [図1]図1は、秘密結合システムの機能構成を例示する図である。

[図2]図2は、秘密計算装置の機能構成を例示する図である。

[図3]図3は、秘密結合方法の処理手続きを例示する図である。

[図4]図4は、コンピュータの機能構成例を示す図である。

発明を実施するための形態

[0009] 以下、この発明の実施の形態について詳細に説明する。なお、図面中において同じ機能を有する構成部には同じ番号を付し、重複説明を省略する。

[001 0] 図１を参照して、実施形態の秘密結合システムの構成例を説明する。秘密結合システムは、Ｎ（≧2）台の秘密計算装置１い…，1_Nを含む。本形態では、秘密計算装置1_1，…，1_Nはそれぞれ通信網２へ接続されている。通信網２は、接続される各装置が相互に通信可能なように構成された回線交換方式もしくはパケット交換方式の通信網であり、例えばインターネットやLAN (Loca l Area Network) 、WAN (Wi de Area Network) などである。なお、各装置は必ずしも通信網２を介してオンラインで通信可能である必要はない。例えば、秘密計算装置１,，…，1_Nへ入力する情報を磁気テープやUSBメモリなどの可搬型記録媒体に記憶し、その可搬型記録媒体から秘密計算装置１u …，しへオフラインで入力するように構成してもよい。

[001 1] 図２を参照して、秘密結合システムに含まれる秘密計算装置１„ (n=1，…，N) の構成例を説明する。秘密結合システムの秘密計算装置1_nは、例えば、図２に示すように、ベクトル結合部１１„、第一置換計算部１２„、第一置換適用部１３„、第一ベクトル生成部１４„、第二ベクトル生成部１５„、ビット反転部１６„、第二置換計算部１７„、第二置換適用部１８„、第三ベクトル生成部１９$_n$、逆置換適用部１１○$_n$、ベクトル分離部１１１$_n$、第三置換適用部１１２„、属性値置換部１１３„及び第四ベクトル生成部１１４„を備えている。

[001 2] 秘密計算装置１„（1≦n≦N）の各構成部が他の秘密計算装置$1_{n'}$ (n'＝1，…，N、ただしn≠n'）の各構成部と協調しながら後述する各ステップの処理を行うことにより実施形態の秘密結合方法が実現される。

[001 3] なお、各ステップの処理は、秘密計算により行われる。すなわち、秘密計算装置しは、シェアを復元することなく、言い換えればシェアの中身を知ることなく、各ステップの処理を行う。

[0014] 秘密計算装置１„は、例えば、中央演算処理装置 (CPU：Cent ra l Process ing Unit）、主記憶装置 (RAM：Random Access Memory) などを有する公知又は専用のコンピュータに特別なプログラムが読み込まれて構成された特別な装置である。秘密計算装置しは、例えば、中央演算処理装置の制御のもとで各処理を実行する。秘密計算装置しに入力されたデータや各処理で得られたデ

ータは、例えば、主記憶装置に格納され、主記憶装置に格納されたデータは必要に応じて中央演算処理装置へ読み出されて他の処理に利用される。秘密計算装置1。の各構成部は、少なくとも一部が集積回路等のハードウェアによって構成されていてもよい。

[0015] 以下の説明において、《を任意のベクトルとして[«]は《が秘密分散されたシェアであり、/3を任意の置換として{{β}}は/3が秘密分散されたシェアであるとする。

[0016] 図3を参照して、実施形態の秘密結合システムが実行する秘密結合方法の処理手続きを説明する。

[0017] 以下に説明する秘密結合システムは、第一テーブルと第二テーブルを秘密垂直結合する。言い換えれば、以下に説明する秘密結合システムは、秘匿性を保ちつつ、第_テーブル及び第二テーブルの共通するキーについての、第_テーブルの属性値及び第二テーブルの属性値を得る。

[0018] m_0, m_1, L_0,しは、1以上の整数であるとする。m_0, m_1, L_0,しは、同じ値であってもよいし、異なる値であってもよい。

[0019] 第_テーブルは、111_0個のレコードを有している。111_0個のレコードのそれぞれは、1個のキーと、L_0個の属性の属性値とを有している。¼巳ト⁰は第一テーブルのキーのベクトルであるとする。ᴾ=0,…,L_0-1として、ソ以⊖ドᶦʳ⁰は第一テーブルの属性ロの属性値のベクトルであるとする。第_テーブルの中は、重複するキーはないとする。

[0020] $[F]^{m0}$の上付き文字の中の1110は、「111_0」を意味する。このように、上付き文字の中では、更なる上付き文字及び下付き文字の表現を省略することがある。同様に、下付き文字の中では、更なる上付き文字及び下付き文字の表現を省略することがある。

[0021] 第二テーブルは、111.個のレコードを有している。111.個のレコードのそれぞれは、1個のキーと、し個の属性の属性値とを有している。$k_1 \in F^{m1}$は第二テーブルのキーのベクトルであるとする。$q=0,\cdots,L_1-1$として$v_{1,q} \in F^{m1}$は上記第二テーブルの属性ロの属性値のベクトルであるとする。第二テーブルの中では、重複

するキーはないとする。

[0022] 例えば、第一テーブルは、レコード数が3であり、キーのベクトル1^=(1，2，3)てと、1個の属性z1の属性値のベクトルソ$_{0,}$=(5，10，1)てとから構成されているとする。

[0023] また、第二テーブルは、レコード数が4であり、キーのベクトル1^=(1，3，4，5)てと、1個の属性z1'の属性値のベクトルソ$_{1.1}$=(2，4，9，8)てとから構成されているとする。

[0024] <ステップ3 1>

ベクトル結合部1 1,,…，1しに、ベクトルk$_{0}$のシェア!; ¾]及びベクトルk$_{1}$のシェア!; ϰ$_{1}$]が入力される。

[0025] ベクトル結合部1 1,,…，1しは、¾]と:k$_{1}$]を結合して[k']∈[F]$^{m0+m1}$を得る。

[0026] より詳細には、ベクトル結合部1 1,,…，1しは、ベクトルk$_{0}$のシェア!; ¾]及びベクトル、のシェア!; ϰ$_{1}$]を用いて、ベクトルk$_{0}$及びベクトルk$_{1}$を結合したベクトルk'∈[F]$^{m0+m1}$のシェア⊳']を生成する（ステップ3 1）。

[0027] 生成されたシェア⊳']は、第一置換計算部1 2,,-，1 2$_{N}$及び第一置換適用部1 3,,…，1 3$_{N}$に出力される。

[0028] 例えば、ベクトル1¾=(1，2，3)でであり、ベクトル1^=(1，3，4，5)でであるとする。この場合、ベクトルピ=(1，2，3，1，3，4，5)てとなる。

[0029] <ステップ3 2>

第一置換計算部1 2,,-，1 2„に、シェア⊳']が入力される。

[0030] 第一置換計算部1 2,,-，1 2„は、⊳']のソート{{び}}を得る。

[0031] より詳細には、第一置換計算部1 2$_{1}$,…，1 2$_{N}$は、シェア⊳']を用いて、ベクトルピを昇順に安定ソートする置換びのシェア{{び}}を生成する（ステップ3 2）$_{0}$

[0032] 安定ソートとは、同等なデータのソート前の順序が、ソート後も保存されるものをいう。安定ソートを行う置換ℊのシェア{{ℊ}}の生成は、例えば参考文献1の手法により実現することができる。

[0033] 参考文献1〕五十嵐大、濱田浩気、菊池亮、千田浩司、 「超高速秘密計算ソートの設計と実装 :秘密計算がスクリプト言語に並ぶ日」、055201 7, 2017

[0034] 生成されたシェア{{び}}は、第一置換適用部13,,-,13$_N$及び逆置換適用部1110],…,1 10$_N$に出力される。

[0035] 例えば、ベクトルピ=(1,2,3,1,3,4,5)であるとする。この場合、置換σは以下の式(1)のようになる。例えば、番号が1スタートで表記されるとして、置換びの各列(し』)では、置換が適用されるベクトルのI番目の要素を』番目に移動することを意味する。

[0036] [数1]

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\1&3&4&2&5&6&7\end{pmatrix} \quad (1)$$

[0037] なお、ベクトルピの各要素は、ビット分解されたものであってもよい。すなわち、ベクトルピの各要素は、その各要素が0,1のビットで表現されたものであつてもよい。

[0038] <ステップ33>

第一置換適用部13,,-,13„に、シエアト’]及びシエア{{び}}が入力される。

[0039] 第一置換適用部13,,-,13„は、ト’]に{{び}}を適用してネ(|○]を得る。

[0040] より詳細には、第一置換適用部13,,-,13„は、シエアト’]及びシエア{{ヂ}}を用いて、ベクトルk’に置換ヂを適用したベクトル〃ひ’)のシエア[〃ひ’)]を生成する(ステップ33)。

[0041] 生成されたシエア[σ(ピ)]は、第一ベクトル生成部14,,…,14$_N$に出力される。

[0042] 例えば、ベクトルピ=(1,2,3,1,3,4,5)であり、置換σが上記の式(1)で表される置換であるとする。この場合、ベクトルσ(1^)=(1,1,2,3,3,4,5)丁となる。

[0043] <ステップ34>

第一ベクトル生成部１４,,-,１４„に、シェア[£7(10]が入力される。

[0044] 第一ベクトル生成部１４,,-,１４„は、|>]:=[£7ひ’)尸びひ’)|+1]ただし[e_m0+ „,-,]:=[0]なる1>]を得る。，を０以上の整数として、６;はベクトル６の，番目の要素を意味し、ヂひ’)|はベクトルヴひ’)の‘I番目の要素を意味する。このように、，を０以上の整数として、ベクトルの下付きの，は、そのベクトルの，番目の要素を意味する。”:=”は、”:=”の左の変数に”:=”の右の値を代入することを意味する。例えば、a:=bは、変数３に1)の値を代入することを意味する。

[0045] なお、ベクトルの要素数を11/1とすると、ベクトルの最初の要素を○番目の要素と呼び、ベクトルの次の要素を１番目の要素と呼び、ベクトルの最後の要素を11/1-1番目の要素と呼ぶことにする。

[0046] より詳細には、第一ベクトル生成部１４,,-,１４„は、シェア[びひ’)]を用いて、ベクトルびひ’)のある要素とそのある要素の次の要素とが、同じ場合には１を、違う場合には○をそのある要素に対応する要素として持つベクトル６のシェア|>]を生成する（ステップ３４）。ただし、ベクトル６の最後の要素は０であるとする。

[0047] 生成されたシェア|>]は、第二ベクトル生成部１５1,▪--,１5Nに出力される。

[0048] 例えば、ベクトル£7ひ’)=(１，１，２，３，３，４，５)てであるとする。この場合、ベクトル６=(１，０，０，１，０，０，０)丁となる。

[0049] <ステップ３５>

第二ベクトル生成部１５,,-,１５„に、シェア|>]が入力される。

[0050] 第二ベクトル生成部１５1,…,１５Nは、[e’i]=[ei(+)ei-1]ただし[e’0]=[e0]なる1> ’]を得る。(+)は、排他的論理和又は加算である。

[0051] より詳細には、第二ベクトル生成部１５1,…,１５Nは、シェア|>]を用いて、ベクトル㊀のある要素とそのある要素の前の要素の一方が１の場合には１を、そうでない場合には○をそのある要素に対応する要素として持つベクトル６’のシェア|> ’]を生成する（ステップ３５）。ただし、ベクトル６’の最初の要素は、ベクトル㊀の最初の要素と同じであるとする。

[0052] 生成されたシェア|>’]は、ビット反転部１６1,'--, １６Nに出力される。

[0053] 例えば、ベクトル6=(1 ，0，0，1，0，0，0)でであるとする。この場合、ベクトル6’=(1 ，1，0，1，1，0，0)丁となる。

[0054] ＜ステップ３６＞

ビット反転部１６,,-，１６„に、シェア|>’]が入力される。

[0055] ビット反転部１６,,-，１６„は、|>’]のビット反転[e’’]を得る。

[0056] より詳細には、ビット反転部１６,,-，１６„は、シェア|>’]を用いて、ベクトル6’の各要素をビット反転させたベクトルe’’のシエア[e’’]を生成する（ステップ３６）。

[0057] 生成されたシェア|>’ ’]は、第二置換計算部１７,,-，１７Nび第二置換適用部１８,,-'-, １８ｎに出力される。

[0058] 例えば、6’=(1 ，1，0，1，1，0，0)でであるとする。この場合、ベクトル6’’=(0, 0, 1，0，0，1，1)Tとなる。

[0059] なお、ベクトルピの各要素がビット分解されたものであった場合には、例えば1110(^ 卩変換により、6’’の環が変更されてもよい。卩は、３以上の素数である。111(^ 「変換は、例えば参考文献１の3(^61116 5に記載された手法により実現することができる。

[0060] ＜ステップ３７＞

第二置換計算部１７,,-，１７„に、シェア[e’’]が入力される。

[0061] 第二置換計算部１７,,-，１７„は、[e’’]のソート{{ゲ }}を得る。

[0062] より詳細には、第二置換計算部１７,,-，１７„は、シェア[e’’]を用いて、ベクトル㊀’’を昇順に安定ソートする置換ゲのシェア{{ゲ }}を生成する（ステップ３７）。

[0063] 生成されたシェア{{ゲ }}は、第二置換適用部１８,,-，１８Nび逆置換適用部１１０】,…，１１０Nに出力される。

[0064] 例えば、ベクトル6’’=(0, 0, 1，0，0，1，1)でであるとする。この場合、置換ゲは以下の式（２）のようになる。

[0065]

[数 2]

$$\text{び}' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \text{い} & 2 & 5 & 3 & 4 & 6 & 7 \end{pmatrix} \quad (2)$$

[0066] ＜ステップ３８＞

第二置換適用部１８,,-,１８„に、シェア[e'']及びシェア{{ゲ }}が入力される。

[0067] 第二置換適用部１８,,-,１８„は、[e'']に{{σ'}}を適用して[σ'(e'')]を得る。

[0068] より詳細には、第二置換適用部１８,,-,１８„は、シェア[e'']及びシェア{{ｷ' }}を用いて、ベクトルe'に置換Ｅ7'を適用したベクトル〃'(6'')のシェア[ゲ レ'')]を生成する (ステップ３８)。

[0069] 生成されたシェア[ゲ レ'')]は、第三ベクトル生成部１９,,-,１９„に出力される。

[0070] 例えば、ベクトル6''=(0,0,1,0,0,1,1)であり、置換ゲが上記の式 (2) により表される置換であるとする。この場合、ベクトルゲ レ'')=(0,0,0,0,1,1,1)^{T}となる。

[0071] ＜ステップ３９＞

第三ベクトル生成部$19_1,\cdots,19_N$に、シェア[ゲ レ'')]が入力される。

[0072] 第三ベクトル生成部１９,,-,１もは、|>]:=[ゲ (Ø,,)¡?0：4/2 」+1]を得る。

[0073] より詳細には、第三ベクトル生成部$19_1,\cdots,19_N$は、シェア[ゲ レ'')]を用いて、ベクトルゲ レ'')のある要素 |が、0である場合には し_|/2」を、0でない場合には0をそのある要素 |に対応する要素として持つベクトルXのシェア Þ]を生成する (ステップ３９)。

[0074] ここで、$i=0,\cdots,m_0+m_1-1$であり、し_|/2」は、_|/2以下の最大の整数を意味する。

[0075] 生成されたシェア Þ]は、逆置換適用部１$10_1,\cdots,1$１○„に出力される。

[0076] 例えば、ベクトルゲ (6')=(0,0,0,0,1,1,1)であるとする。この場合、ベクトル 乂=(1,1,2,2,0,0,0)丁となる。

[0077] < ステップ３ １０ >

逆置換適用部 １１０$_1$,…, １１０$_N$に、シェア[X]、シェア{{び}}及びシェア{{ゲ }}が入力される。

[0078] 逆置換適用部 １１０$_1$,…, １１０„は、[X]に{{ゲ }}と{{び}}を逆適用して[$\sigma^{-1}(\sigma'^{-1}(x))$]を得る。

[0079] より詳細には、逆置換適用部 １１０$_1$,…, １１０„は、シェアﾈ]、シェア{{び}}及びシェア{{ﾀ'}}を用いて、ベクトルXに置換ﾀ'の逆置換ﾀ'-1及び置換○の逆置換ﾀ-1を適用したベクトル〃-1(ﾀ'-1(X))のシェア[ﾀ-1(ﾀ'-1(乂))]を生成する (ステップ３１０)。

[0080] 生成されたシェア[σ-,(ゲ -1。))]は、ベクトル分離部 １１１,,…, １１しに出力される。

[0081] 例えば、ベクトル父=(1, 1, 2, 2, 0, 0, 0)であり、置換びが上記の式 (１) により表される置換であり、置換ゲが上記の式 (２) により表される置換であるとする。この場合、ベクトルσ-,(ゲ -1。))：(1, 0, 2, 1, 2, 0, 0)となる。

[0082] < ステップ３ １１１ >

ベクトル分離部 １１１],…, １１しに、シェア!:び$^{-1}$(ゲ -1。))]が入力される。

[0083] ベクトル分離部 １１１],…, １１しは、[£$^{-1}$(〃'$^{-1}$(父))]を先頭から叫個の要素!: 3$_0$]と残りの,,,個の要素:3,]とに分離する。

[0084] より詳細には、ベクトル分離部 １１１],…, １１しは、シェア[$\sigma^{-1}(\sigma'^{-1}(x))$]を用いて、ベクトルﾀ$^{-1}$(〃'$^{-1}$(X))の先頭から,,,$_0$個の要素からなるベクトル3$_0$のシェア[3$_0$]と、ベクトルび、ﾀ'パレ))の残りの,,,個の要素からなるベクトル呂,のシェア:3,]とを生成する (ステップ３１１)。

[0085] 生成されたシェア:¾]及びシェア:3,]は、第三置換適用部 １１２,,-, １１$2_N$に出力される。

[0086] 例えば、ベクトルσ-1(ゲ -1。))=(],0, 2, 1, 2, 0, 0)丁であるとする。この場合、ベクトル3$_0$=(1, 0, 2)\ ベクトル3]=(1, 2, 0, 0)丁となる。

[0087] ベクトル3$_0$, 3,は、第－テーブルと第二テーブルで重複するキーの位置を示

している。例えば、第一テーブルのキーのベクトルが1^=(1，2，3)であり、第二テーブルのキーのベクトルが1^=(1，3，4，5)であるとする。この場合、ベクトル3_0=(1，0，2)\ ベクトル3,=(1，2，0，0)となる。第一テーブルと第二テーブルで重複するキーは、「1」「3」である。ベクトル3_0=(1，0，2)及びベクトル呂,=(1，2，0，0)では、それぞれベクトル1^=(1，2，3)及び1^=(1，3，4，5)での中の「1」「3」の位置を示している。

[0088] <ステップ3 1 2>

第三置換適用部1 1 2,,-，1 1 2„に、シェア¡¾]及びシェア!;3,]が入力される。

[0089] 第三置換適用部1 1 2⟧,…，1 1 2$_N$は、[冗$_0$(3_0)]，[冗办，)]を得て、て$_0$:=$7\sum_0$(8_0)，て，::冗イ呂,)を公開する。

[0090] より詳細には、第三置換適用部1 1 2,,-，1 1 2„は、シェア[¾]、シェア1^,]及び置換$71:_0$，71:,を用いて、ベクトル$S_\emptyset$に置換$71:_0$を適用したベクトルてø:=$71:_0$(3_0)のシェア[$71:_0$(3_0)]と、ベクトル呂,に置換71:,を適用したベクトルて，:=71:,(3,)のシェア[71^(3,)]とを生成して、ベクトルて$_0$及びベクトル·∑,を公開する（ステップ3 1 2）。ベクトル$7:_0$及びベクトル7:,は、秘密計算装置1$_n$（1≤冂≤$_1$○に公開される。

[0091] 置換冗$_0$，冗,は、所定の置換であり、例えばランダム置換である。置換$7\sum_0$，冗,は、予め定められた置換であってもよいし、ステップ3 1 2の処理をする際に生成されてもよい。置換冗$_0$，心及びこれらのシェア{{一}}，{{心}}は、例えば参考文献1の4.1節に記載された手法により生成することができる。秘密計算装置1„（1≤冂≤1\1)は、置換ろ，71:及びこれらのシェア{{ろ}}，{{一}}についての情報を有しており、置換冗$_0$，心及びこれらのシェア{{冗$_0$}}，{{π,}}を用いて計算が可能であるとする。

[0092] 生成されたシヱア[ろ($S_\emptyset$)]及びシヱア[冗办，)]は、属性値置換部1 1 3,,…，1 1 3$_N$に出力される。

[0093] 例えば、ベクトル3_0=(1，0，2)\ ベクトル3⟧=(1，2，0，0)であり、心が以下の式（3）により表される置換であり、71:,が以下の式（4）により表される置

換であるとする。

[0094] [数 3]

$$\pi_0 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad (3)$$

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \quad (4)$$

[0095] この場合、ベクトル て$_0$=(0, 2, 1)了 ベクトル !:,=(0, 1, 0, 2)了となる。

[0096] <ステップ３１３>

属性値置換部１１３,,-, １１３„に、シェアレ$_{0}$』]及びシェア[、$_{q}$]が入力される。

[0097] 属性値置換部１１３,,…, １１３$_N$は、第一テーブルの各属性値を{{ろ }}、第二テーブルの各属性値 {{冗,}}により置換する。

[0098] より詳細には、属性値置換部１１３,,…, １１３$_N$は、置換 冗$_0$のシェア{{冗$_0$}}、置換心のシェア{{心 }}、ベクトル$V_{0,p}$のシェア|> ø』]及びベクトル$_{v',q}$のシェア[V,$_{q}$]を用いて、第一テーブルの各属性。(。=0, … ,11½-1)の属性値のベクトルv$_{0,p}$を置換 71;$_0$で置換したベクトルゾ$_{0,p}$のシェア|> ’$_{0,p}$]と、第二テーブルの各属性9 (9=0, … ,111,-1)の属性値のベクトル$_{v',q}$を置換 7τ$_1$で置換したベクトルゾ’ぃのシェア!; $_{v}$’,$_{q}$]とを生成する（ステップ３１３）。

[0099] 生成されたシェア!; $_{v}$、$_{,}$口及びシェア!; $_{v}$’,$_{,}$」は、第四ベクトル生成部１１４,,…, １１4･$_N$に出力される。

[0100] 例えば、第一テーブルの属性z1のベクトル$V_{0,}$,=(5, 10, 1)ててあり、第二テーブルの属性z1’のベクトルゾ$_{1,1}$=(2, 4, 9, 8)^{T}であり、冗$_0$が上記の式（３）により表される置換であり、心が上記の式（４）により表される置換であるとする。この場合、ベクトルゾ’$_{0.1}$=(1 0, 1, 5)てベクトルゾ’$_{1.1}$=(9, 2, 8, 4)てとなる。

[0101] <ステップ３１４>

第四ベクトル生成部１１４$_1$,…, １１４$_N$に、ベクトル 77$_0$、ベクトル 7:トシェア[v’$_{0,p}$]及びシェア[v’$_{1,q}$]が入力される。

[0102] 第四ベクトル生成部１１４,,-, １１、は、1=1, 2として、置換した各属性値 ¦v’ぃ]について（て上 ,≠0のときに[(V’’し山 わ$_{)i'-1}$]:=[(ゾ’ぃ）ド]とする[(V’’し

]を得る。

[0103] より詳細には、第四ベクトル生成部１１４,,-,１１４$_N$は、ベクトルて$_0$、ベクトルて$_1$、シェア[v'$_{0,p}$]及びシェア[v'$_{1,}$。を用いて、ベクトルて$_0$の,'番目の要素が○でない場合にはベクトルゲ$_{0,p}$のI'番目の要素を1'-!番目の要素として持つベクトルV''$_0$』のシェア[v'、口と、ベクトルて,の,'番目の要素が0でない場合にはベクトルV'$_{1,q}$の,'番目の要素を,'-1番目の要素として持つベクトルv''ぃのシェア[ゲ'ぃ]とを生成する（ステップ３１４）。第四ベクトル生成部１１４,,…,１１4･$_N$は、この処理を各P(P=0,…,$_{1\_0}$-1)及び各口(口=0,…,$_1$「1)に対して行う。

[0104] 例えば、ベクトルて$_0$=(0, 2, 1)了ベクトルゲ$_{0,}$』=(1 0, 1, 5)了ベクトル!:』=(0, 1, 0, 2)\ ベクトルゲ..尸(9,之8メパであるとする。この場合、ベクトルゲ'$_{0,1}$=(5, 1)\ ベクトルv''$_{1,1}$=(2,4)Tとなる。

[0105] ベクトル3$_0$, 3,は第－テーブルと第二テーブルで重複するキーの位置を示しているため、ベクトル3$_0$, s$_1$をそれぞれ置換$_{71}$;$_0$, $_{71}$:,により置換したベクトルて$_{ø,}$て]]は、置換て$_{\Sigma;0,\ 71}$;による置換後の第一テーブルと第二テーブルで重複するキ—の位置を示している。

[0106] 上記の例では、ベクトルて$_0$=(0, 2, 1)での２番目の要素「$_1$」は置換冗$_0$による置換後の第一テーブルのキー「$_1$」の位置を示し、ベクトルて$_0$=(0, 2, 1)での１番目の要素「$_2$」は置換冗Qによる置換後の第一テーブルのキー「$_3$」の位置を示している。

[0107] 同様に、上記の例では、ベクトルて,=(0, 1, 0, 2)での１番目の要素「$_1$」は置換心による置換後の第二テーブルのキー「$_1$」の位置を示し、ベクトルて,=(0, 1, 0, 2)での３番目の要素「$_2$」は置換心による置換後の第二テーブルのキー「3」の位置を示している。

[0108] このため、(τ$_i$)$_{i'}$≠0のときに[(V''$_{i,j}$)$_{(7i)i}$]:= [(ソ'ぃ)「]とすることにより、第一テーブルのキー「$_1$」のレコードの属性z1の属性値「$_5$」をベクトルV'、,=(5, 1)での○番目の要素とし、第一テーブルのキー「$_3$」のレコードの属性z1の属性値「$_1$」をベクトルV''$_{0.}$,=(5, 1)での１番目の要素とすることができる。

[01 09] また、第二テーブルのキー 「1」のレコードの属性z1’の属性値 「2」をベクトルV’’,.,=(2, 4)70 〇番目の要素とし、第二テーブルのキー 「3」のレコードの属性z1’の属性値 「4」をベクトルV’’,.,=(2, 4)での1番目の要素とすることができる。

[01 10] 言い換えれば、ベクトルV’’0.,=(5, 1)での〇番目の要素 「5」は第一テーブルのキー 「1」のレコードの属性z1の属性値であり、ベクトルV’’0.,=(5, 1)での1番目の要素 「1」は、第一テーブルのキー 「3」のレコードの属性z1の属性値である。

[01 11] また、ベクトルV’’,.,=(2, 4)T0 〇番目の要素 「2」は第二テーブルのキー 「」のレコードの属性z1’の属性値であり、ベクトルV’’,,=(2, 4)Tの1番目の要素 「4」は第二テーブルのキー 「3」のレコードの属性z1’の属性値である。

[01 12] このように、ベクトルV’’0,]]=(5, 1)了 ベクトルV’’,.,=(2, 4)^は、第一テーブル及び第二テーブルの共通するキー 「1」 「3」についての、第- テーブルの属性値及び第二テーブルの属性値を表していると言える。

[01 13] この実施形態によれば、秘匿性を保ったまま、第一テーブル及び第二テーブルの共通するキーについての、第一テーブルの属性値及び第二テーブルの属性値を得ることができる。

[01 14] [変形例]

なお、Xを2以上の正の整数として、キーの属性が、X個の属性の複合キーであってもよい。この場合には、例えば以下のようにしてステップ3 1の処理を行ってもよい。

[01 15] 第- テーブルのキーは、k0,0,…,k0,x-1であるとする。第二テーブルのキーは、、0,…,、,であるとする。

[01 16] この場合、ステップ3 1の処理で、各,(ただし,=0,…,X-1)でk0,,と、,を結合して1’,を得る。そして、各1’,をビット分解してビット表現にし、横に結合する。例えばピ0=(1, 2, 3, 1, 3, 0, 1)\ 1^=(0, 0, 0, 0, 0, 1, 1)Tのとき、ピ0をビット分解すると、(ピ0)0=(1, 0, 1, 1, 1, 0, 1)\ ひ,ふ=(0, 1, 1, 0, 1, 0, 0)Tとなる。

[01 17] ここで、ピ0は1から3の値を取るため、ピ0の各要素は2ビットで表現するこ

とができる。ひ'$_0$)$_0$はピ$_0$をビット分解したときの下位ビットであり、ひ、),はk'$_0$をビット分解したときの上位ビットである。ピ,はこの例ではもともと1ビット数であるので分解する必要はなく、ピ,=(。,)$_{ø}$とする。(ピ$_0$)$_0$,ひ、$_{ø}$),(,)$_{ø}$を横に結合すると、

[01 18] [数4]

$$\begin{pmatrix} 1. & 0. & 1. & 1. & 1. & 0. \\ 0. & 1. & 1. & 0. & 1. & 0. & 0 \\ 0. & 0. & 0. & 0. & 1. & 1 \end{pmatrix}^{T}$$

[01 19] となる。このようにして並べたものを行列とみなし、この行列の各行を1レコードのキーのビット表現とみなすと、(1,2, 3, 1 ,3, 4, 5)というキーのビット表現のベクトルが得られる。このベクトルをステップ3 2以降で使うピとして用いてもよい。このようにして、複合キーの場合も処理できる。

[01 20] 複合キーでは、キーの重複とは、全てのキー属性の値の組み合わせの観点で重複するかどうかであり、個々の属性の値が重複しただけでは重複とはみなさないとする。例えば、組み合わせ(1,0)と(1,1)は重複ではない。

[01 21] 以上、この発明の実施の形態について説明したが、具体的な構成は、これらの実施の形態に限られるものではなく、この発明の趣旨を逸脱しない範囲で適宜設計の変更等があっても、この発明に含まれることはいうまでもない。

[01 22] 実施の形態において説明した各種の処理は、記載の順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。

[01 23] [プログラム、記録媒体]

上述の各種の処理は、図4に示すコンピュータの記録部２０２０に、上記方法の各ステップを実行させるプログラムを読み込ませ、制御部２０１０、入力部２０３０、出力部２０４０などに動作させることで実施できる。

[01 24] 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

体としては、例えば、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等どのようなものでもよい。

[01 25] また、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〇〆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ビ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。

[01 26] このようなプログラムを実行するコンビュータは、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。そして、処理の実行時、このコンビュータは、自己の記憶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。また、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、このコンビ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。また、サーバコンピュータから、このコンビ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。なお、本形態におけるプログラムには、電子計算機による処理の用に供する情報であってプログラムに準ずるもの (コンビュータに対する直接の指令ではないがコンビュータの処理を規定する性質を有するデータ等) を含むものとする。

[01 27] また、この形態では、コンビュータ上で所定のプログラムを実行させることにより、本装置を構成することとしたが、これらの処理内容の少なくとも一部をハードウエア的に実現することとしてもよい。

請求の範囲

[請求項1] 複数の秘密計算装置を含む秘密結合システムであって、

ドは任意の環であり、《を任意のベクトルとして[«]は《が秘密分散されたシェアであり、/3を任意の置換として{{/3}}は/3が秘密分散されたシェアであり、m_0, m_1, L_0, L_1は1以上の整数であり、$k_0 \in F^{m0}$は第一テーブルのキーのベクトルであり、、⊖ト1は第二テーブルのキーのベクトルであり、ロ=0，…，1_0-1として¥0左ドが0は上記第一テーブルの属性Ｉの属性値のベクトルであり、$q=0,\cdots,L_1-1$として$v_{1,q} \in F^{m1}$は上記第二テーブルの属性Ｉの属性値のベクトルであり、冗0，7τ_1はそれぞれ長さ叫，111,の所定の置換であり、

上記複数の秘密計算装置は、

上記ベクトルk_0のシェア[>0]及び上記ベクトルk_1のシェア[>,]を用いて、上記ベクトルk_0及び上記ベクトルk_1を結合したベクトルビ○[F]$^{m0+m1}$のシェア[>']を生成する複数のベクトル結合部と、

上記シェアヤ']を用いて、上記ベクトルk'を昇順に安定ソートする置換£7のシェア{{£7}}を生成する複数の第一置換計算部と、

上記シェア1>'']及び上記シェア{{£7}}を用いて、上記ベクトルk'に上記置換々を適用したベクトル[ひ'）のシェア[[ひ'）]を生成する複数の第一置換適用部と、

上記シェア[[ひ'）]を用いて、上記ベクトル[ひ'）のある要素とそのある要素の次の要素とが、同じ場合には1を、違う場合には○をそのある要素に対応する要素として持つベクトル⊖のシェア[>]を生成する複数の第一ベクトル生成部と、

上記シェア[>]を用いて、上記ベクトル6のある要素とそのある要素の前の要素の一方が1の場合には1を、そうでない場合には0をそのある要素に対応する要素として持つベクトルe'のシェア[e']を生成する複数の第二ベクトル生成部と、

上記シェア[>']を用いて、上記ベクトル6'の各要素をビット反転さ

せたベクトル6''のシェア[e'']を生成する複数のビット反転部と、

上記シェアᵽ'']を用いて、上記ベクトル6''を昇順に安定ソートする置換ゲのシェア{{ゲ}}を生成する複数の第二置換計算部と、

上記シェアᵽ'']及び上記シェア{{ᵞ'}}を用いて、上記ベクトル6''に上記置換ᵹ'を適用したベクトルᵞ'(6'')のシェア[ᵞ'(6'')]を生成する複数の第二置換適用部と、

上記シェア[ᵹ'(6'')]を用いて、上記ベクトルᵞ'(6'')のある要素1が、〇である場合には し_|/2」を、0でない場合には0をそのある要素に対応する要素として持つベクトルXのシェア[X]を生成する複数の第三ベクトル生成部と、

上記シェア[X]、上記シェア{{び}}及び上記シェア{{ᵞ'}}を用いて、上記ベクトルXに上記置換ᵹ'の逆置換ᵹ'⁻¹及び上記置換ᵹの逆置換σ⁻¹を適用したベクトル(7-〗(ᵞ'-〗(乂))のシェア[(7-〗(£7'⁻¹(乂))]を生成する複数の逆置換適用部と、

上記シェア[ᵹ⁻¹(ᵹ'⁻¹(父))]を用いて、上記ベクトル<7-〗(ᵞ'-〗(乂))の先頭からm₀個の要素からなるベクトルs₀のシェア[3₀]と、上記ベクトルᵞ⁻¹(ᵹ'⁻¹(X))の残りの個の要素からなるベクトル呂,のシェア[呂,]とを生成する複数のベクトル分離部と、

上記シェアᵻ₀]、上記シェア,3,]及び上記置換71;0,71;を用いて、上記ベクトルs₀に上記置換71;0を適用したベクトルて0:=71;0(30)のシェア[冗0(30)]と、上記ベクトルs₁に上記置換71:,を適用したベクトル𝜏1=71:,(呂,)のシェア[𝜏1(3,)]とを生成して、て0:=冗0(30)及びて,==71;(3,)を公開する複数の第三置換適用部と、

上記置換冗0のシェア{{71;0}}、上記置換71:,のシェア{{71;}}、上記ベクトルソ0,ρのシェア[>øᵢ]及び上記ベクトルV,,qのシェア[V,,コを用いて、上記第－テーブルの各属性りの属性値のベクトルv0,ρを上記置換71:0で置換したベクトルV、,ρのシェア!;ソ'0,ρ]と、上記第二テーブルの各属性9の属性値のベクトルV,,qを上記置換𝜏1で置換したベクトルV',,qのシ

エア！v ’ 1,q]と を 生 成 する 複 数 の 属 性 値 置 換 部 と 、

上 記 ベ ク トル て 0、 上 記 ベ ク トル ・∑ 、、 上 記 シ エア !> ’ 0,p]及 び 上 記 シ エア!! v ’ ・q]を 用 いて 、 上 記 ベ ク トル て 0の ¡ ’ 番 目の 要 素 が 0 でな い 場 合 には 上 記 ベ ク トル ソ ’ 0,pの ¡ ’ 番 目の 要 素 を 1 -! ’ 番 目の 要 素 と して 持 つ ベ ク トル v’’0,pのシェア[v’’0,p]と、上記ベクトル て ,の ¡ ’ 番目の要素が 0 でない場合には上記ベクトル v ’ 1,qの ¡ ’ 番目の要素を 1 - 1番目の要素として持つベクトル v ’ ’’ ’ ’’ いのシェアレ い]とを生成する複数の第四ベクトル生成部と、

を含む秘密結合システム。

[請求項2] 請求項1の秘密結合システムの秘密計算装置。

[請求項3] ドは任意の環であり、《を任意のベクトルとして[«]は《が秘密分散されたシェアであり、/3を任意の置換として{{ /3 }}は/3が秘密分散されたシェアであり、m_0, m_1, L_0, L_1は 1 以上の整数であり、$k_0 \in F^{m0}$は第一テーブルのキーのベクトルであり、、⊖ トは第二テーブルのキーのベクトルであり、ロ= 0 , ▪▪▪ , t_0 - 1 として ¥0 左 ドで0は上記第一テーブルの属性 ∏の属性値のベクトルであり、$q=0,\cdots,L_1-1$として$v_{1,q} \in F^{m1}$は上記第二テーブルの属性 ∏の属性値のベクトルであり、冗0 , 7τ1はそれぞれ長さ叫 , 111, の所定の置換であり、

複数のベクトル結合部が、上記ベクトル k_0のシェア |> 0]及び上記ベクトル k_1のシェア !>,]を用いて、上記ベクトル k_0及び上記ベクトル k_1を結合したベクトル ビ $\in [F]^{m0+m1}$のシェア |> ’]を生成する複数のベクトル結合ステップと、

複数の第一置換計算部が、上記シェア ヤ ’]を用いて、上記ベクトルビを昇順に安定ソートする置換 £7 のシェア{{ £7 }}を生成する複数の第一置換計算ステップと、

複数の第一置換適用部が、上記シェア 1>’]及び上記シェア{{ £7 }}を用いて、上記ベクトル k’に上記置換 々を適用したベクトル 〃ひ ’)のシェア [£7 ひ ’)]を生成する複数の第一置換適用ステップと、

複数の第一ベクトル生成部が、上記シェア[びひ’)]を用いて、上記ベクトル£7ひ’)のある要素とそのある要素の次の要素とが、同じ場合には１を、違う場合には○をそのある要素に対応する要素として持つベクトル6のシェア[>]を生成する複数の第一ベクトル生成ステップと、

複数の第二ベクトル生成部が、上記シェア[>]を用いて、上記ベクトル6のある要素とそのある要素の前の要素の一方が１の場合には１を、そうでない場合には０をそのある要素に対応する要素として持つベクトル6’のシェア[>’]を生成する複数の第二ベクトル生成ステップと、

複数のビット反転部が、上記シェア[1>’]を用いて、上記ベクトル6’の各要素をビット反転させたベクトル6’’のシェア[e’’]を生成する複数のビット反転ステップと、

複数の第二置換計算部が、上記シェア[1>’’]を用いて、上記ベクトル6’’を昇順に安定ソートする置換<7’のシェア{{’}}を生成する複数の第二置換計算ステップと、

複数の第二置換適用部が、上記シェア[1>’’]及び上記シェア{{£7’}}を用いて、上記ベクトルe’’に上記置換£7’を適用したベクトル’(6’’)のシェア[ゲレ’’)]を生成する複数の第二置換適用ステップと、

複数の第三ベクトル生成部が、上記シェア[ゲレ’’)]を用いて、上記ベクトルゲレ’’)のある要素が、０である場合には「し_|/2」を、０でない場合には０をそのある要素に対応する要素として持つベクトルXのシェア[>]を生成する複数の第三ベクトル生成ステップと、

複数の逆置換適用部が、上記シェア[X]、上記シェア{{び}}及び上記シェア{{’}}を用いて、上記ベクトルXに上記置換’の逆置換’-1及び上記置換の逆置換σ-1を適用したベクトル「び、’-1(乂))のシェア[;σ-1(£7’-1(X))]を生成する複数の逆置換適用ステップと、

複数のベクトル分離部が、上記シェア[£7-1(£7’-1ひ))]を用いて、

上記ベクトルマ・ｒ（(7 '・ｒ（乂））の先頭から111$_0$個の要素からなるベクトルS_0のシェア［3$_0$］と、上記ベクトルマ・ｒ（マ'$^{-1}$(X)）の残りの111,個の要素からなるベクトルS_1のシェア｝3，］とを生成する複数のベクトル分離ステップと、

複数の第三置換適用部が、上記シェアゃ$_0$］、上記シェア｝3，］及び上記置換71:$_0$，71:，を用いて、上記ベクトルS_0に上記置換71:$_0$を適用したベクトルて$_0$:＝71:$_0$（3$_0$）のシェア［71:$_0$（3$_0$）］と、上記ベクトルS_1に上記置換心を適用したベクトルτ_1＝＝71:，(3,)　のシェア［71:，(3,)　］とを生成して、て$_0$:＝71:$_0$（3$_0$）及びて$_1$:＝71:$_1$（3$_1$）を公開する複数の第三置換適用ステップと、

複数の属性値置換部が、上記置換?$\sum_{\varphi}$のシエア｛｛71:$_0$｝｝、上記置換71:，のシェア｛｛も｝｝、上記ベクトルソ$_{0,p}$のシェア｜ゃøﾛ］及び上記ベクトルv・，qのシェア［V，。を用いて、上記第一テーブルの各属性Ｉの属性値のベクトルv$_{0,p}$を上記置換71:$_0$で置換したベクトルソ'$_{0,p}$のシェア｜ゃ'$_{0,p}$］と、上記第二テーブルの各属性口の属性値のベクトルv・，qを上記置換$_7\tau_1$で置換したベクトルv'$_{\cup}$のシェア［ゲ$_{1,q}$］とを生成する複数の属性値置換ステップと、

複数の第四ベクトル生成部が、上記ベクトルて$_0$、上記ベクトルて，、上記シェア!>'$_{0,}$口及び上記シェア［v'い］を用いて、上記ベクトルて$_0$のｉ'番目の要素が0でない場合には上記ベクトルソ'$_{0,p}$の，'番目の要素を，'－1番目の要素として持つベクトルv''$_{0,p}$のシェア［V'$_{0,p}$］と、上記ベクトルて，のi'番目の要素が0でない場合には上記ベクトルv'$_{1,q}$のi'番目の要素を」－1番目の要素として持つベクトルン$_{1,q}$のシェア［ゲ$_{1,q}$］とを生成する複数の第四ベクトル生成ステップと、

を含む秘密結合方法。

［請求項4］　請求項2の秘密計算装置の各部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]

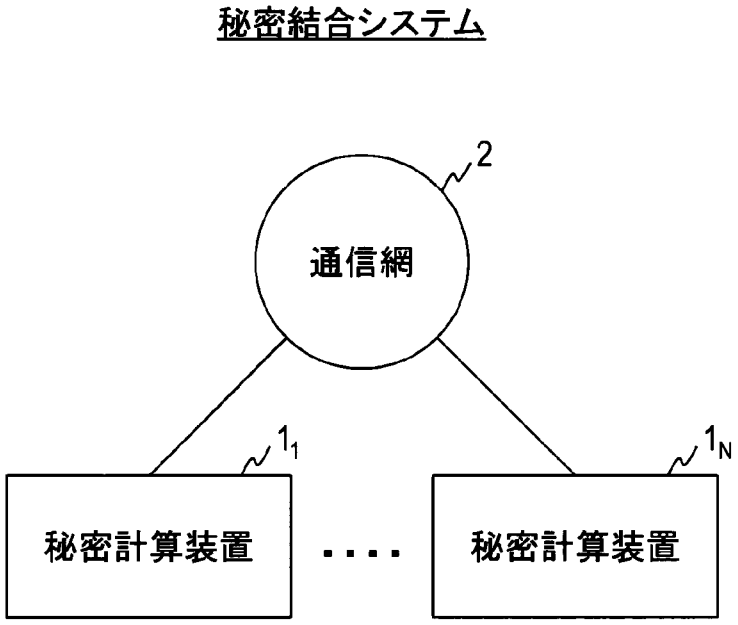


図1

[図2]

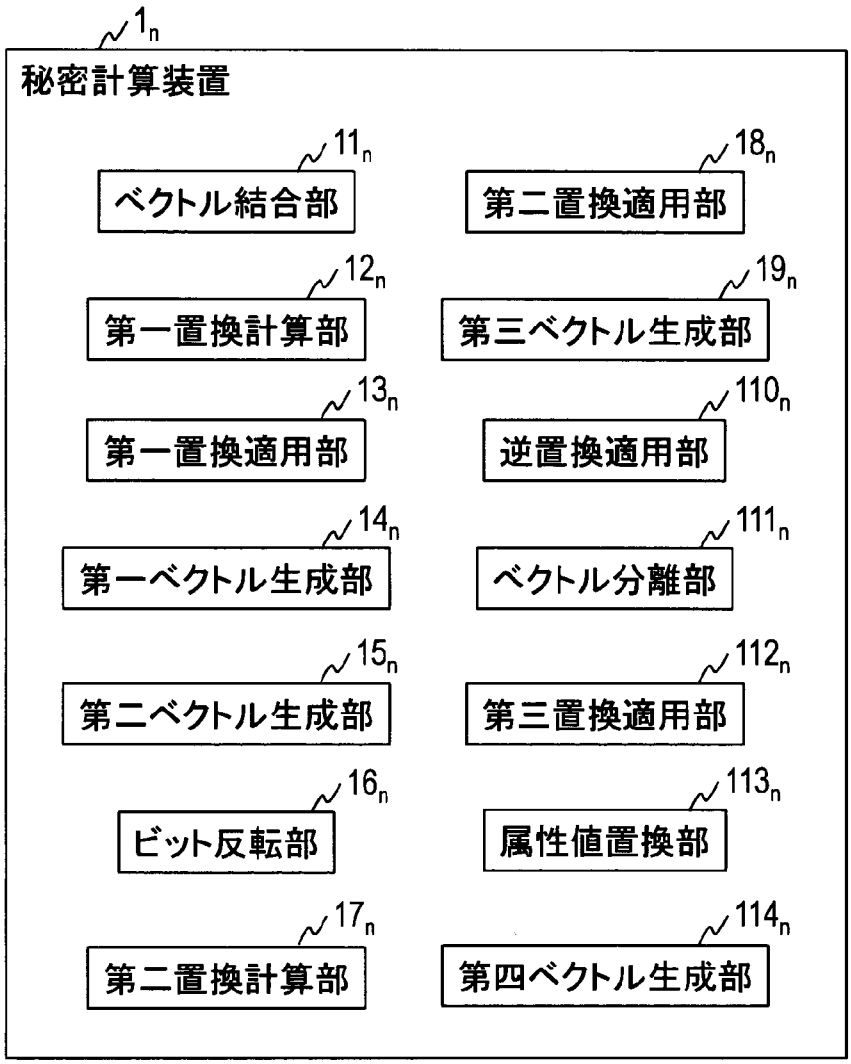

1n
秘密計算装置
11n
ベクトル結合部
12n
第一置換計算部
13n
第一置換適用部
14n
第一ベクトル生成部
15n
第二ベクトル生成部
16n
ビット反転部
17n
第二置換計算部
18n
第二置換適用部
19n
第三ベクトル生成部
110n
逆置換適用部
111n
ベクトル分離部
112n
第三置換適用部
113n
属性値置換部
114n
第四ベクトル生成部

図2

[図3]

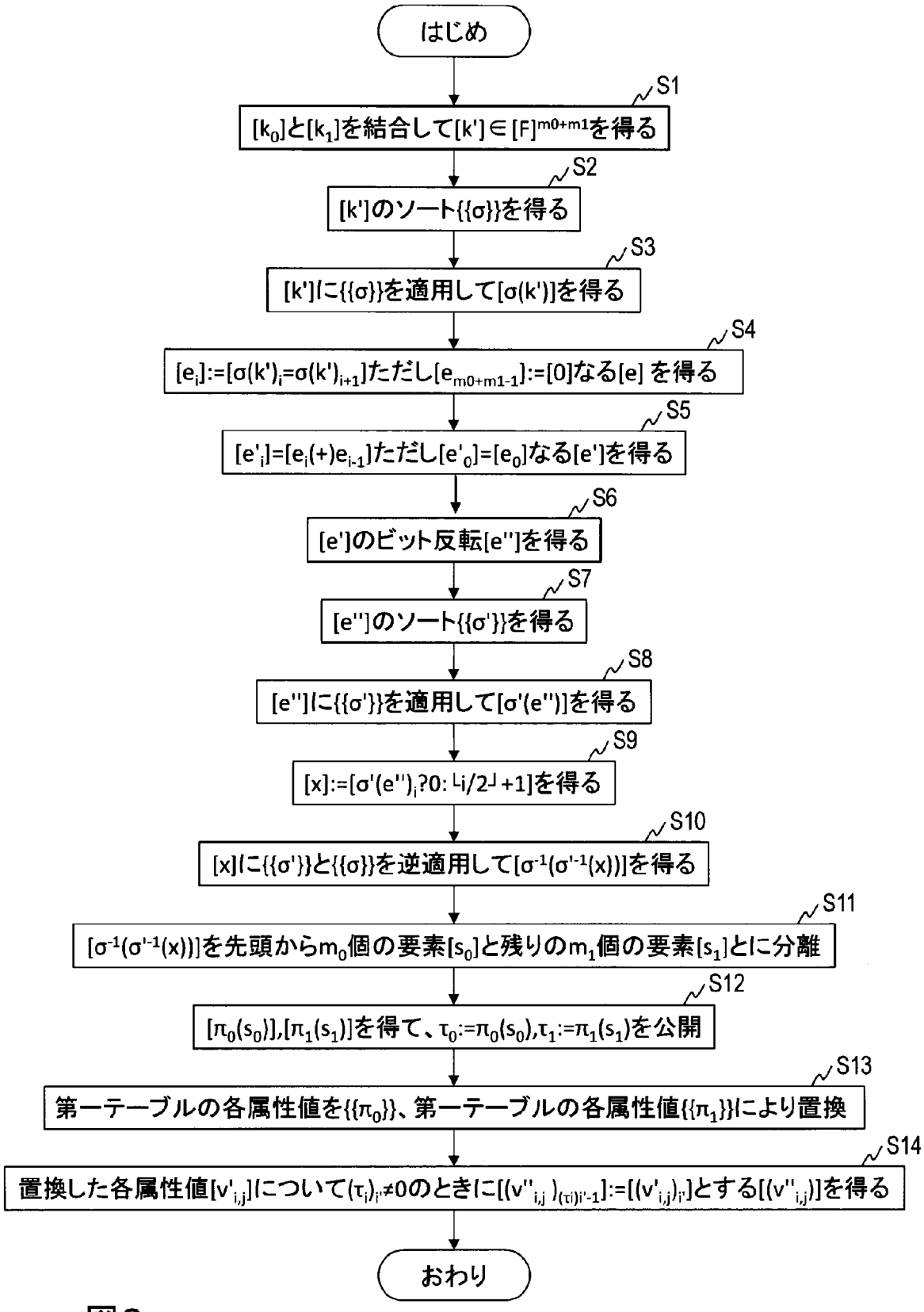

はじめ
S1
[k0]と[k1]を結合して[k']∈[F]m0+m1を得る
S2
[k']のソート{{σ}}を得る
S3
[k']に{{σ}}を適用して[σ(k')]を得る
S4
[ei]:=[σ(k')i=σ(k')i+1]ただし[em0+m1-1]:=[0]なる[e] を得る
S5
[e'i]=[ei(+)ei-1]ただし[e'0]=[e0]なる[e']を得る
S6
[e']のビット反転[e'']を得る
S7
[e'']のソート{{σ'}}を得る
S8
[e'']に{{σ'}}を適用して[σ'(e'')]を得る
S9
[x]:=[σ'(e'')i?0: ⌊i/2⌋+1]を得る
S10
[x]に{{σ'}}と{{σ}}を逆適用して[σ-1(σ'-1(x))]を得る
S11
[σ-1(σ'-1(x))]を先頭からm0個の要素[s0]と残りのm1個の要素[s1]とに分離
S12
[π0(s0)],[π1(s1)]を得て、τ0:=π0(s0),τ1:=π1(s1)を公開
S13
第一テーブルの各属性値を{{π0}}、第一テーブルの各属性値{{π1}}により置換
S14
置換した各属性値[v'i,j]について(τi)i'≠0のときに[(v''i,j)(τi)i'-1]:=[(v'i,j)i']とする[(v''i,j)]を得る
おわり

図3

[図4]

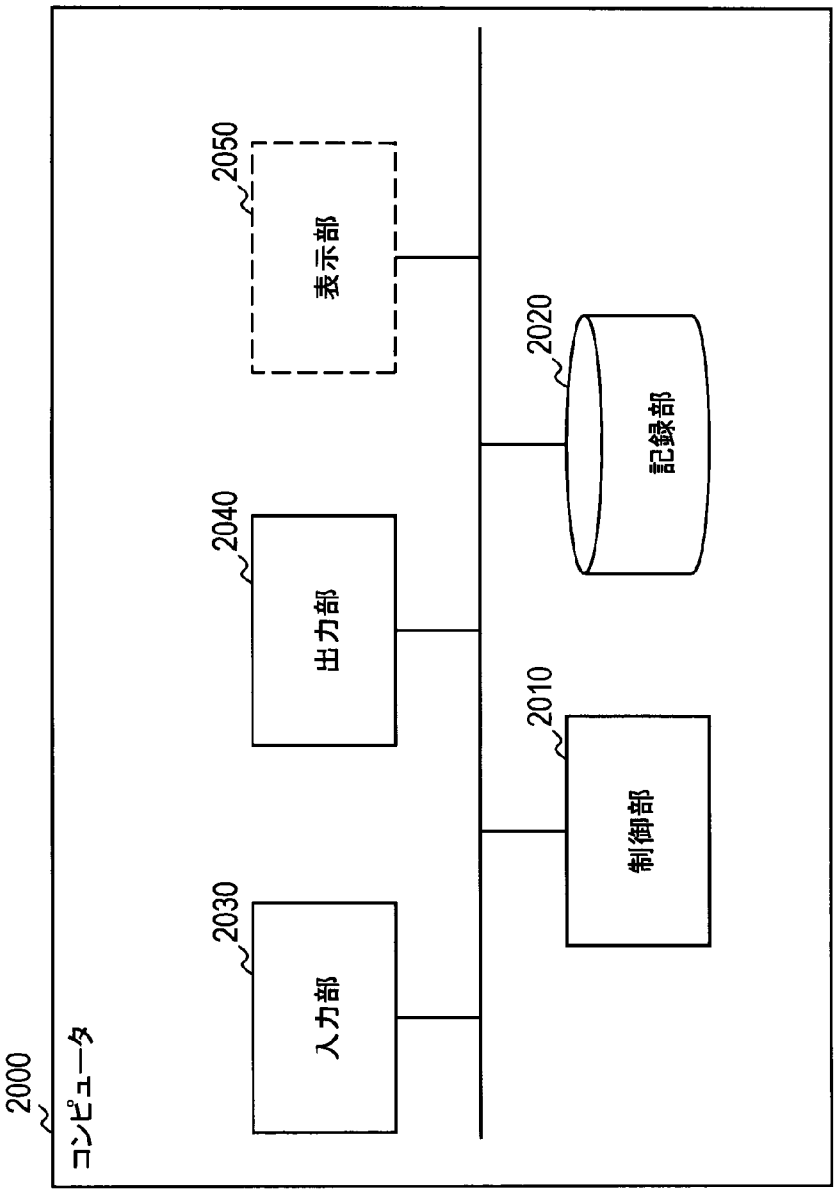


図4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/023390

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. 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)
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	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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	LAUR, Sven et al., "From Oblivious AES to Efficient and Secure Database Join in the Multiparty Setting", Applied Cryptography and Network Security, SpringerLink [online], 2013 [retrieved on 28 August 2019], Internet: <URL:https://link.springer.com/content/pdf/10.1007%2F978-3-642-38980-1_6.pdf> <DOI: 10.1007/978-3-642-38980-1_6>, pp. 84-101	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
27 August 2019 (27.08.2019)	10 September 2019 (10.09.2019)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/023390

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	濱田 浩気，ほか２名，キーに重複がある場合の秘密計算向け結合アルゴリズム，2015年暗号と情報セキュリティシンポジウム概要集，20 January 2015, non-official translation (HAMADA, Koki et al., "Combination algorithm for secure calculation in case of a duplicate key", Summaries of the 2015 Symposium on Cryptography and Information Security)	1-4
A	JP 2014-139640 A (NIPPON TELEGRAPH AND TELEPHONE CORP.) 31 July 2014, (Family: none)	1-4
A	WO 2018/061800 A1 (NIPPON TELEGRAPH AND TELEPHONE CORP.) 05 April 2018 & CN 109791741 A	1-4

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／０２３３９０

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	１９７１－２０１９年
日本国実用新案登録公報	１９９６－２０１９年
日本国登録実用新案公報	１９９４－２０１９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	LAUR,Sven ほか2名, From Oblivious AES to Efficient and Secure Database Join in the Multiparty Setting, Applied Cryptography and Network Security, SpringerLink [online], 2013 [retrieved on 2019.08.28], Internet:<URL: https://link.springer.com/content/pdf/10.1007%2F978-3-642-38980-1_6.pdf> <DOI: 10.1007/978-3-642-38980-1_6>, p.84-101	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	国際調査報告の発送日
２７．０８．２０１９	１０．０９．２０１９

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　１２０６
吉田　歩
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	濱田　浩気，ほか２名，キーに重複がある場合の秘密計算向け結合アルゴリズム，2015年 暗号と情報セキュリティシンポジウム概要集，2015.01.20	1-4
A	JP 2014-139640 A（日本電信電話株式会社）2014.07.31，（ファミリーなし）	1-4
A	WO 2018/061800 A1（日本電信電話株式会社）2018.04.05，& CN 109791741 A	1-4