(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
2023年1月5日(05.01.2023)

WIPO | PCT

(10) 国際公開番号
WO 2023/276142 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号： PCT/JP2021/025131

(22) 国際出願日： 2021年7月2日(02.07.2021)

(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: 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).

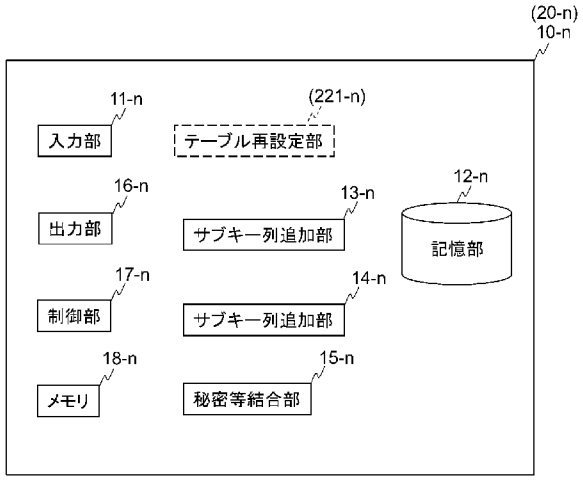
(72) 発明者: 橋本 順子 (**HASHIMOTO, Junko**); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 五十嵐 大(**IKARASHI, Dai**); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP).

(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, 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, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,

(54) **Title:** SECRET EQUIJOIN DEVICE, SECRET EQUIJOIN METHOD, AND PROGRAM

(54) 発明の名称： 秘密等結合装置、秘密等結合方法、およびプログラム



11-n Input unit
12-n Storage unit
13-n, 14-n Sub-key sequence addition unit
15-n Secret equijoin unit
16-n Output unit
17-n Control unit
18-n Memory
221-n Table resetting unit

図2

(57) **Abstract:** A secret equijoin device according to the present invention uses, as input, a first concealed table that is concealed information of a first table including a plurality of keys and a second concealed table that is concealed information of a second table including a plurality of keys, obtains a first concealed addition table that is concealed information of a first addition table in which a sub-key sequence has been added to the first table by secure computation, obtains a second concealed addition table that is concealed information of a second addition table in which a sub-key sequence has been further added to a third table prepared by duplicating and adding records in the second table multiple times, and obtains a concealed junction table that is concealed information of a junction table in which the first addition

WO 2023/276142 A1

［続葉有］

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)）

table and the second addition table are equi-joined, using pairs of keys and sub-keys as key attributes.

(57) 要約：秘密等結合装置は、複数個のキーを持つ第１テーブルの秘匿情報である第１秘匿化テーブルと複数個のキーを持つ第２テーブルの秘匿情報である第２秘匿化テーブルを入力とし、秘密計算によって、第１テーブルにサブキー列を追加した第１追加テーブルの秘匿情報である第１秘匿化追加テーブルを得、第２テーブルの各レコードを複数回複製して追加した第３テーブルにさらにサブキー列を追加した第２追加テーブルの秘匿情報である第２秘匿化追加テーブルを得、キーとサブキーとの組をキー属性とし、第１追加テーブルと第２追加テーブルとを等結合した結合テーブルの秘匿情報である秘匿化結合テーブルを得る。

明　細　書

発明の名称 ：

秘密等結合装置、秘密等結合方法、およびプログラム

技術分野

[0001]　本発明は、秘密計算技術において、特に、テーブルの情報を秘匿したまま、２つのテーブルを等結合する秘密等結合技術に関する。

背景技術

[0002]　一般的な暗号方式では、秘匿したいデータを秘匿化（暗号化）し、サーバに格納しても、その値を用いて計算を行う際には、復元（復号）を行ってから計算を行う。しかし、データを秘匿化したまま計算を行うことができる技術として、秘密計算技術がある。秘密計算技術では、数値を秘匿化された複数のシェアに変換し、複数個の秘密計算装置が各々シェアを持ち、各自自身のシェアの情報は漏らさずに、加算、乗算、論理演算などを行う（マルチパーティプロトコル）。

[0003]　また、データベースに格納されたテーブルを用いて計算を行う場合、１つのテーブルでは計算に必要な情報が揃っておらず、複数のテーブルから情報を集めて計算することがある。このような、複数のテーブルを結合する前処理が必要となる。特許文献１には、テーブルの情報を秘匿したまま、選択されたキー列の要素（キー）をキー属性として、２つのテーブルを等結合する技術が開示されている。

先行技術文献

特許文献

[0004] 特許文献1：国際公開第２０１８／０６１８００号

発明の概要

発明が解決しようとする課題

[0005]　特許文献１の技術は、等結合対象の２つのテーブルのうち、一方のテーブルのキー列が互いに同値の複数のキー（キー属性）を含む場合にも適用でき

る。

[0006] しかしながら、一方のテーブルのキー列が互いに同値の複数のキーを含み、かつ、他方のテーブルのキー列も同値の複数のキーを含む場合には、特許文献１の技術を直接適用することはできない。

[0007] ここで、一方のテーブルのキー列が含む同値のキーの最大数（最大重複数）をKLとした場合に、当該一方のテーブルをキー列が互いに同値のキーを含まないKL個のテーブルに分割し、特許文献１の技術を用い、KL回の秘密等結合を行い、結果として出力されたKL個のテーブルを結合することで、出力を得ることもできる。

[0008] しかし、値を秘匿したままテーブルを分割することは難しく、テーブルを分割する過程で、分割した各テーブルに関する情報（例えば、分割前のテーブルに含まれる互いに同値のキーの個数に関する情報）が漏洩してしまう。また、この方法では、秘密等結合以外に、秘密等結合前のテーブルの分割、秘密等結合後のテーブルの結合の処理時間がかかる。特にテーブルの結合処理は並列化できないため、処理性能のボトルネックとなる。

[0009] 本発明では、等結合対象の２つのテーブルのうち、一方のテーブルのキー列が互いに同値の複数のキーを含み、かつ、他方のテーブルのキー列も同値の複数のキーを含む場合であっても、テーブルの情報を秘匿したまま、高速に２つのテーブルを等結合できる技術を提供する。

課題を解決するための手段

[0010] 複数個の第１キーを持つ第１キー列と複数個の第１任意要素を持つ第１任意要素列とを含む第１テーブルの秘匿情報である第１秘匿化テーブルと、複数個の第２キーを持つ第２キー列と複数個の第２任意要素を持つ第２任意要素列とを含む第２テーブルの秘匿情報である第２秘匿化テーブルとに対し、以下の処理を行う。

[0011] 第１サブキー列追加部が、第１秘匿化テーブルを用いた秘密計算によって、第１サブキー列を第１テーブルに追加した第１追加テーブルの秘匿情報である第１秘匿化追加テーブルを得る。ただし、第１サブキー列は複数個の第

１サブキーを持ち、第１キーのそれぞれには、第１サブキーの何れかが対応付けられている。前記第１キー列に含まれる互いに同値の前記第１キーの個数の最大値がKLであり、KLは２以上の整数である。互いに同値の第１キーには、互いに異なる値の第１サブキーが対応付けられている。

[0012] 第２サブキー列追加部が、第２秘匿化テーブルを用いた秘密計算によって、第２サブキー列を第３テーブルに追加した第２追加テーブルの秘匿情報である第２秘匿化追加テーブルを得る。ただし、第３テーブルは、第２テーブルの各レコードをＫ回（ただし、K≧KL）ずつ複製して得られる複数の複製レコードを第２テーブルに追加したテーブルである。第２テーブルの各レコードは、各第２キーと各第２任意要素とを含む。第３テーブルは、第２キー及び第２キーの複製を含む複数の第３キーを持つ第３キー列と、第２任意要素及び第２任意要素の複製を含む複数の第３任意要素を持つ第３任意要素列とを含む。第２サブキー列は複数個の第２サブキーを持つ。第３キーのそれぞれには、第２サブキーの何れかが対応付けられている。第３キー列が何れかの第１キーと同じ共通値を表す第３キーを含む場合、共通値を表す第３キーの少なくとも一部には、共通値を表す第１キーに対応付けられる第１サブキーと同値の第２サブキーが対応付けられている。

[0013] 秘密等結合部は、第１秘匿化追加テーブルと第２秘匿化追加テーブルとを用いた秘密計算によって、第１キーと第１サブキーとの組を第１追加テーブルのキー属性とし、第３キーと第２サブキーとの組を第２追加テーブルのキー属性として、第１追加テーブルと第２追加テーブルとを等結合した結合テーブルの秘匿情報である秘匿化結合テーブルを得る。

発明の効果

[0014] これにより、等結合対象の２つのテーブルのうち、一方のテーブルのキー列が互いに同値の複数のキーを含み、かつ、他方のテーブルのキー列も同値の複数のキーを含む場合であっても、テーブルの情報を秘匿したまま、高速に２つのテーブルを等結合できる。

図面の簡単な説明

[0015] [図1]図１は、実施形態の秘密等結合システムの構成を例示するためのブロック図である。

[図2]図２は、実施形態の秘密等結合装置の構成を例示するためのブロック図である。

[図3]図３は、実施形態の秘密等結合方法を例示するためのフロー図である。

[図4]図４Ａは等結合対象のテーブル１１０（第１テーブル）を例示するための図である。図４Ｂは等結合対象のテーブル１２０（第２テーブル）を例示するための図である。

[図5]図５Ａは、テーブル１１０（第１テーブル）にサブキー列（第１サブキー列）を追加した追加テーブル１３０（第１追加テーブル）を例示するための図である。図５Ｂは、テーブル１２０（第２テーブル）の各レコードを複製して得られる複数の複製レコードをテーブル１２０に追加したテーブル１４０（第３テーブル）を例示するための図である。

[図6]図６は、サブキー列１５１（第２サブキー列）をテーブル１４０（第３テーブル）に追加した追加テーブル１５０（第２追加テーブル）を例示するための図である。

[図7]図７Ａから図７Ｃは等結合対象のテーブルを例示するための図である。図７Ｄは、図７Ａから図７Ｃのテーブルを等結合したテーブルを例示するための図である。

[図8]図８は、等結合を例示するための図である。

[図9]図９Ａは、図７Ｂのテーブル（第１テーブル）にシーケンス番号（SeqNo）列（第１サブキー列）を追加したテーブル（第１追加テーブル）を例示するための図である。図９Ｂは、図７Ｃのテーブル（第２テーブル）の各レコードを複製して得られる複数の複製レコードを当該テーブルに追加し、さらにシーケンス番号列（第２サブキー列）を追加したテーブル（第２追加テーブル）を例示するための図である。

[図10]図１０は、識別子（ID）とシーケンス番号（SeqNo）との組をキー属性として、図９Ａのテーブル（第１追加テーブル）と図９Ｂのテーブル（第２

追加テーブル）とを等結合したテーブルを例示するための図である。

[図11]図１１は、実施形態の秘密等結合装置のハードウェア構成を例示したブロック図である。

発明を実施するための形態

[0016] 以下、図面を参照して本発明の実施形態を説明する。

［用語および記号の定義］

以下、本実施形態で使用する用語および記号を定義する。

テーブル(表)の表記に以下の記号を用いる。

T.X：テーブルTのある列XをT.Xと表記する。

テーブルTのj番目のレコードをT_jと表記する。jは0以上の整数である。

テーブルTのj番目のレコードの列（カラム）Xの値を$T.X_j$と表記する。

[0017] 交差結合：交差結合は、クロスジョインとも呼ばれ、入力された２つのテーブルTLおよびテーブルTRのすべてのレコードの組み合わせについて、テーブルTLのレコードTL_jとテーブルTRのレコードTL_pとを対応付けたテーブルTLRを得るテーブル結合方法である。ただし、jは0以上の整数であり、ｐは0以上の整数であり、j=0,...,LRN-1であり、p=0,...,RRN-1であり、LRNはテーブルTLのレコード数を表す正整数であり、RRNはテーブルTRのレコード数を表す正整数である。すなわち、交差結合結果のテーブルTLRは、テーブルTLとテーブルTRとのレコード（TL_0,...,TL_{LRN-1}およびTR_0,...,TR_{RRN-1}）についての直積である。テーブルTLとテーブルTRとの交差結合結果のテーブルTLRのレコード数はLRN*RRNとなる。ただし、「*」は積を表す演算子である。実際の利用シーンでは、このテーブルTRLから、ある条件を満たすレコードだけを抜き出して利用することが多い。

[0018] 等結合：等結合は、等化結合や内部結合とも呼ばれ、入力された２つのテーブルTLおよびテーブルTRの交差結合結果のテーブルTRLから、テーブルTLから選択された属性（キー属性$TL.Key_j$）とテーブルTRから選択された属性（キー属性$TR.Key_p$）とについて等号（$TL.Key_j=TR.Key_p$）が成り立つレコードだけを抜き出したテーブルETRLを得るテーブル結合方法である。なお、キー属性

は選択された列（カラム）の要素である。すなわち、等結合は、入力された２つのテーブルTLおよびテーブルTRのレコードのうち、$TL.Key_j=TR.Key_p$を満たす全レコードの組み合わせについて、テーブルTLのレコードTL_jとテーブルTRのレコードTL_pとを対応付けたテーブルETLRを得るテーブル結合方法である。

[0019] 秘匿情報の表記には以下の記法を用いる。

[a]：aの秘匿情報を[a]と表記する。例えば、$a\in Z_n$である。aを秘密計算が可能なように秘密分散して得られるシェアが[a]であってもよいし（例えば、参考文献１等参照）、aを秘密計算が可能なように暗号化して得られる暗号文（準同型暗号の暗号文）が[a]であってもよい。aをN個（Nは1以上の整数）のパーティに秘密分散した場合、aに対してN種類のシェア$[a]_0,...[a]_{N-1}$が得られ、シェア$[a]_0,...[a]_{N-1}$のそれぞれについて秘密計算が行われる。しかしながら、これらの秘密計算のアルゴリズムは全シェアについて共通であるため、$[a]_0,...[a]_{N-1}$の添え字を省略して[a]と表記することにする。

参考文献１：千田浩司，濱田浩気，五十嵐大，高橋克巳，“軽量検証可能３パーティ秘匿関数計算の再考(A Three-Party Secure Function Evaluation with Lightweight Verifiability Revisited)”，In CSS, 2010.

Z_n：Z_nは0からn-1までの整数の集合（nは1以上の整数）からなる有限環を表す。

[T]：あるテーブルTの秘匿情報を[T]と表記する。

[T.X]：列T.Xの秘匿情報を[T.X]と表記する。[T.X]の各レコード（すなわち、各フィールド）には秘匿化された値が格納されている。

$[T_j]$：レコードT_jの秘匿情報を$[T_j]$と表記する。$[T_j]$の各列（すなわち、各フィールド）には秘匿化された値が格納されている。

$[T.X_j]$：テーブルTのj番目のレコードの列（カラム）Xの値$T.X_j$の秘匿情報を$[T.X_j]$と表記する。すなわち、[T]の各フィールドにはテーブルTの各フィールドの値の秘匿情報が格納されている。

[0020] ［第１実施形態］

本発明の第１実施形態を説明する。

＜構成＞

図１に例示するように、本実施形態の秘密等結合システム１は、Ｎ個の秘密等結合装置１０－０，…，１０－（Ｎ－１）を含む。本実施形態の秘密等結合装置１０－０，…，１０－（Ｎ－１）は、ネットワークを通じて通信可能に接続されている。ここで、秘密分散に基づく秘密計算が行われる場合にはＮは２以上の整数であり（例えば、Ｎ＝３）、準同型暗号に基づく秘密計算が行われる場合にはＮは１以上の整数である（例えば、Ｎ＝１）。

[0021] 図２に例示するように、各秘密等結合装置１０－ｎ（ただし、ｎ＝０，…，Ｎ－１）は、入力部１１－ｎ、記憶部１２－ｎ、サブキー列追加部１３－ｎ（第１サブキー列追加部）、サブキー列追加部１４－ｎ（第２サブキー列追加部）、秘密等結合部１５－ｎ、出力部１６－ｎ、制御部１７－ｎ、およびメモリ１８－ｎを有する。以下では説明を省略するが、各秘密等結合装置１０－ｎは、制御部１７－ｎに基づいて各処理を実行し、入力されたデータおよび各処理で得られたデータをメモリ１８－ｎに格納し、必要に応じて読み出して使用する。

[0022] ＜事前処理＞

事前処理として、秘密等結合対象の秘匿化テーブル（第１秘匿化テーブル）[TL]および秘匿化テーブル（第２秘匿化テーブル）[TR]が、各秘密等結合装置１０－ｎ（図２）の入力部１１－ｎに入力され、記憶部１２－ｎに格納される。

[0023] 図４Ａに秘匿化テーブル[TL]を例示する。秘匿化テーブル[TL]は、テーブルTL（第１テーブル，左テーブル）の秘匿情報である。テーブルTLは、複数個(LRN個)のキー$TL.Key_0,...,TL.Key_{LRN-1}$（第１キー）を持つキー列TL.Key（第１キー列）と、複数個(LRN個)の任意要素$TL.V(v)_0,...,TL.V(v)_{LRN-1}$（第１任意要素）を持つ任意要素列TL.V(v)とを含む。ただし、v=0,...,LVN-1であり、LVNは任意要素列の数を表す正整数である。テーブルTLのj番目のレコードTL_jは、キー$TL.Key_j$とLVN個の任意要素$TL.V(0)_j,...,TL.V(LVN-1)_j$とを含む。テーブルTLのレコード数はLRNであり、本実施形態ではLRNは２以上の整数である

。

[0024] 具体的には、本実施形態で例示する秘匿化テーブル[TL]は、複数個(LRN個)の秘匿化キー[TL.Key_0],...,[TL.Key_{LRN-1}]を持つ秘匿化キー列[TL.Key]と、複数個(LRN個)の秘匿化任意要素[TL.$V(v)_0$],...,[TL.$V(v)_{LRN-1}$]を持つ任意要素列[TL.V(v)]とを含む。秘匿化レコード[TL_j]は、秘匿化キー[TL.Key_j]と、LVN個の秘匿化任意要素[TL.$V(0)_j$],...,[TL.$V(LVN-1)_j$]とを含む（図４Ａ）。

[0025] 本実施形態の秘匿化テーブル[TL]は、秘匿化キー列[TL.Key]のキー列TL.Keyを基準としてソートされたものである。このソートは秘匿化前に行われていてもよいし、秘匿化後に秘密計算によって行われていてもよい。秘密計算によるソート方法は公知であり、例えば、参考文献２等に開示されている。

参考文献２：五十嵐大，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，” CSS，2017.

[0026] また、テーブルTLのキー列TL.Key（第１キー列）は、２個以上KL個以下の互いに同値のキー（第１キー）を含む。すなわち、キー列TL.Keyは値が重複する複数のキーを含み、その重複数の最大値（第１キー列に含まれる互いに同値の第１キーの個数の最大値）はKLである。KLは２以上の整数である。このKLの値も秘匿化テーブル[TL]に対応付けて記憶部１２－ｎに格納される。

[0027] 図４Ｂに秘匿化テーブル[TR]を例示する。秘匿化テーブル[TR]は、テーブルTR（第２テーブル，右テーブル）の秘匿情報である。テーブルTRは、複数個(RRN個)のキーTR.Key_0,...,TR.Key_{RRN-1}（第２キー）を持つキー列TR.Key（第２キー列）と、複数個(RRN個)の任意要素TR.$V(w)_0$,...,TR.$V(w)_{RRN-1}$（第２任意要素）を持つ任意要素列TR.V(w)とを含む。ただし、w=0,...,RVN-1であり、RVNは任意要素列の数を表す正整数である。テーブルTRのp番目のレコードTR_pは、キーTR.Key_pとRVN個の任意要素TR.$V(0)_p$,...,TR.$V(RVN-1)_p$とを含む。テーブルTRのレコード数はRRNであり、本実施形態ではRRNは２以上の整数である。

[0028] 具体的には、本実施形態で例示する秘匿化テーブル[TR]は、複数個(RRN個)の秘匿化キー[TR.Key_0],...,[TR.Key_{RRN-1}]を持つ秘匿化キー列[TR.Key]と、複数個(RRN個)の秘匿化任意要素[TR.$V(w)_0$],...,[TR.$V(w)_{RRN-1}$]を持つ任意要素列

[TR.V(w)]とを含む。秘匿化レコード[TR_p]は、秘匿化キー[$TR.Key_p$]とRVN個の秘匿化任意要素[$TR.V(0)_p$],...,[$TR.V(RVN-1)_p$]とを含む（図４Ｂ）。

[0029] 本実施形態の秘匿化テーブル[TR]は、秘匿化キー列[TR.Key]のキー列TR.Keyを基準としてソートされたものである。このソートは秘匿化前に行われていてもよいし、秘匿化後に秘密計算によって行われていてもよい。

[0030] また、テーブルTRのキー列TR.Key（第２キー列）は、２個以上KR個以下の互いに同値のキー（第２キー）を含む。すなわち、キー列TR.Keyは値が重複する複数のキーを含み、その重複数の最大値（第２キー列に含まれる互いに同値の第２キーの個数の最大値）はKRである。KRは２以上の整数である。このKRの値も秘匿化テーブル[TR]に対応付けて記憶部１２－ｎに格納される。

[0031] ＜処理＞

図３を用いて本実施形態の秘密等結合方法を説明する。

≪サブキー列追加部１３－ｎの処理（ステップＳ１３－ｎ）≫

各秘密等結合装置１０－ｎ（図２）のサブキー列追加部１３－ｎ（第１サブキー列追加部）は、記憶部１２－ｎから読み出した秘匿化テーブル（第１秘匿化テーブル）[TL]を用いた秘密計算によって、サブキー列TLs.S（第１サブキー列）をテーブルTL（第１テーブル）に追加した追加テーブルTLs（第１追加テーブル）の秘匿情報である秘匿化追加テーブル[TLs]（第１秘匿化追加テーブル）を得て出力する（図５Ａ）。

[0032] 図５Ａに例示するように、追加テーブルTLsのキー列TLs.KeyはテーブルTL（図４Ａ）のキー列TL.Key（第１キー列）であり、キー列TLs.KeyのキーTLs.Key_0,...,TLs.Key_{LRN-1}はTLs.Key_0=TL.Key_0,...,TLs.Key_{LRN-1}=TL.Key_{LRN-1}（第１キー）である。追加テーブルTLsの任意要素列TLs.V(v)はテーブルTL（図４Ａ）の任意要素列TL.V(v)であり、任意要素列TLs.V(v)の任意要素TLs.$V(v)_0$,...,TLs.$V(v)_{LRN-1}$はTLs.$V(v)_0$=TL.$V(v)_0$,...,TLs.$V(v)_{LRN-1}$=TL.$V(v)_{LRN-11}$（第１任意要素）である。

[0033] 図５Ａに例示するように、サブキー列TLs.S（第１サブキー列）は複数個（LRN個）のサブキーTLs.S_0,...,TLs.S_{LRN-1}（第１サブキー）を持つ。キーTL.Key

$_0$,...,TL.Key$_{LRN-1}$（第１キー）のそれぞれには、サブキーTLs.S$_0$,...,TLs.S$_{LRN-1}$（第１サブキー）の何れかが対応付けられている。図５Ａの例では、キーTL.Key$_j$にサブキーTLs.S$_j$がそれぞれ対応付けられており、具体的には、秘匿化キー[TL.Key$_j$]に秘匿化サブキー[TLs.S$_j$]がそれぞれ対応付けられている。

[0034] 前述のように、キー列TL.Key（第１キー列）は、２個以上KL個以下の互いに同値のキー（第１キー）を含む。キーTL.Key$_0$,...,TL.Key$_{LRN-1}$のうち互いに同値のキー（第１キー）には、互いに異なる値のサブキーTLs.S$_j$（第１サブキー）が対応付けられる。図５Ａの例では、秘匿化キー[TL.Key$_0$],...,[TL.Key$_{LRN-1}$]のうち復元値（復号値）が互いに同値の秘匿化キーには、互いに異なる値のサブキーTLs.S$_j$の秘匿情報である秘匿化サブキー[TLs.S$_j$]が対応付けられている。

[0035] j=0,…,LRN-1について、キーTL.Key$_j$およびサブキーTLs.S$_j$の関係を例示すると以下のようになる。

(b-1)j=0のときTLs.S$_j$=0

(b-2)j>0かつTL.Key$_j$≠TL.Key$_{j-1}$であればTLs.S$_j$=0

(b-3)j>0かつTL.Key$_j$=TL.Key$_{j-1}$であればTLs.S$_j$=TLs.S$_{j-1}$+1

ここで(b-1)は最初のキーTL.Key$_0$にはサブキーTLs.S$_j$=0が対応付けられることを意味する。(b-2)は２番目以降のキーTL.Key$_j$が直前のキーTL.Key$_{j-1}$と異なる値である場合、当該キーTL.Key$_j$にはサブキーTLs.S$_j$=0が対応付けられることを意味する。(b-3)は２番目以降のキーTL.Key$_j$が直前のキーTL.Key$_{j-1}$と同値である場合、当該キーTL.Key$_j$にはサブキーTLs.S$_j$=TLs.S$_{j-1}$+1が対応付けられることを意味する。秘匿化テーブル[TL]は秘匿化キー列[TL.Key]のキー列TL.Keyを基準としてソートされたものであるため、(b-1)(b-2)(b-3)により、キーTL.Key$_0$,...,TL.Key$_{LRN-1}$のうち互いに同値のキーに互いに異なる値（0,1,2,3...と１ずつ増加する値）のサブキーTLs.S$_j$が対応付けられる。ただし、これは一例であって本発明を限定するものではない。サブキー列追加部１３－ｎが、秘匿化テーブル[TL]を用いた秘密計算によって、各値を秘匿化したまま、(b-1)(b-2)(b-3)を実行するためには、秘匿化された[TL.Key]より秘匿化された[

TLs.S]を計算する必要がある。この計算には、例えば、参考文献３の秘密グループ化計算で用いられている方法を用いることができる。

参考文献３：濱田浩気，五十嵐大，千田浩司，“秘匿計算上の集約関数中央値計算アルゴリズム”，In CSS, 2012.

秘密グループ化演算は、表[T]を秘匿したまま、列[Key]の値でグループ化を行い、グループごとの中央値などを求める方法である。参考文献３では、Key列を基準として秘密ソートした表[T]が有する同一値のKey_jの秘匿値[Key_j]に対し、0から始まるインクリメント値の秘匿値を付与する方法が説明されている（階段＋の計算）。この演算を行う関数をgroupbyと表現すると、サブキー列追加部１３－ｎは以下のように、[TL.Key]から[TLs.S]を求めることができる。

関数groupby：

[TLs.S]=groupby([TL.Key])

入力：[TL.Key]

出力：[TLs.S]

[0036] ≪サブキー列追加部１４－ｎの処理（ステップＳ１４－ｎ）≫

各秘密等結合装置１０－ｎのサブキー列追加部１４－ｎ（第２サブキー列追加部）は、記憶部１２－ｎから読み出した秘匿化テーブル（第２秘匿化テーブル）[TR]を用いた秘密計算によって、サブキー列TRs.S（第２サブキー列）をテーブルTRc（第３テーブル）に追加した追加テーブルTRs（第２追加テーブル）の秘匿情報である秘匿化追加テーブル[TRs]（第２秘匿化追加テーブル）を得て出力する（図５Ｂおよび図６）。

[0037] テーブルTRc（第３テーブル）は、テーブルTR（第２テーブル）（図４Ｂ）の各レコードTR_p（ただし、p=0,...,RRN-1）をK回ずつ複製して得られる複数の複製レコードをテーブルTR（第２テーブル）に追加したテーブルである（図５Ｂ）。ただし、K≧KLであり、好ましくはK=KLである。本実施形態では、KLの値は記憶部１２－ｎから読みだされて使用される。前述のようにテーブルTR（第２テーブル）の各レコードTR_pはキー$TR.Key_p$（第２キー）と任意要素

TR.V(0)$_p$,...,TR.V(RVN-1)$_p$（第２任意要素）とを含む。例えば、図５Ｂに例示する[TRc]は、[TR]の各[TR$_p$]（ただし、p=0,...,RRN-1）をK回ずつ複製して得られる複数の秘匿化複製レコードを[TR]に追加したテーブルである。例えば、[TR]の各[TR$_p$]は[TR.Key$_p$]と[TR.V(0)$_p$],...,[TR.V(RVN-1)$_p$]とを含む。

[0038] 図５Ｂに例示するように、テーブルTRc（第３テーブル）のキー列TRc.Key（第３キー列）は、RRN*K個のキーTRc.Key$_0$=TR.Key$_0$,...,TRc.Key$_{K-1}$=TR.Key$_0$,TRc.Key$_K$=TR.Key$_1$,...,TRc.Key$_{2K-1}$=TR.Key$_1$,...,TRc.Key$_{RRN*K-1}$=TR.Key$_{RRN-1}$（第２キー及び第２キーの複製を含む複数の第３キー）を含む。テーブルTRcの任意要素列TRc.V(v)（第３任意要素列）は、TRc.V(v)$_0$=TR.V(v)$_0$,...,TRc.V(v)$_{K-1}$=TR.V(v)$_0$,TRc.V(v)$_K$=TR.V(v)$_1$,...,TRc.V(v)$_{2K-1}$=TR.V(v)$_1$,...,TRc.V(v)$_{RRN*K-1}$=TR.V(v)$_{RRN-1}$（第２任意要素及び第２任意要素の複製を含む複数の第３任意要素）を含む。

[0039] 図６に例示するように、追加テーブルTRsのキー列TRs.Keyはテーブル TRc（図５Ｂ）のキー列TRc.Key（第３キー列）であり、RRN*K個のキーTRs.Key$_0$=TR.Key$_0$,...,TRs.Key$_{K-1}$=TR.Key$_0$,TRs.Key$_K$=TR.Key$_1$,...,TRs.Key$_{2K-1}$=TR.Key$_1$,...,TRs.Key$_{RRN*K-1}$=TR.Key$_{RRN-1}$（第２キー及び第２キーの複製を含む複数の第３キー）を含む。追加テーブルTRsの任意要素列TRs.V(v)はテーブルTRc（図５Ｂ）の任意要素列TRc.V(v)（第３任意要素列）であり、TRs.V(v)$_0$=TR.V(v)$_0$,...,TRs.V(v)$_{K-1}$=TR.V(v)$_0$,TRs.V(v)$_K$=TR.V(v)$_1$,...,TRs.V(v)$_{2K-1}$=TR.V(v)$_1$,...,TRs.V(v)$_{RRN*K-1}$=TR.V(v)$_{RRN-1}$（第２任意要素及び第２任意要素の複製を含む複数の第３任意要素）を含む。

[0040] 追加テーブルTRs（第２追加テーブル）のサブキー列TRs.S（第２サブキー列）は複数個（RRN*K個）のサブキーTRs.S$_0$,...,TRs.S$_{RRN*K-1}$（第２サブキー）を持つ。追加テーブルTRsのキーTRs.Key$_0$=TR.Key$_0$,...,TRs.Key$_{K-1}$=TR.Key$_0$,TRs.Key$_K$=TR.Key$_1$,...,TRs.Key$_{2K-1}$=TR.Key$_1$,...,TRs.Key$_{RRN*K-1}$=TR.Key$_{RRN-1}$（第３キー）のそれぞれには、サブキーTRs.S$_0$,...,TRs.S$_{RRN*K-1}$（第２サブキー）の何れかが対応付けられている。本実施形態では、キーTRs.Key$_i$にサブキーTRs.S$_i$（ただし、i=0,...,RRN*K-1）が対応付けられている。例えば、キーTRs.Key$_0$,..

.,TRs.$Key_{RRN*K-1}$のうち互いに同値のキーには、互いに異なる値のサブキーTRs.S_iが対応付けられている。図６の例では、秘匿化キー[TRs.Key_0],...,[TRs.$Key_{RRN*K-1}$]のうち、それらの復元値（復号値）が互いに同値の秘匿化キーには、互いに異なる値のサブキーTRs.S_iの秘匿情報である秘匿化サブキー[TRs.S_i]が対応付けられている。

[0041] また、例えば、追加テーブルTRs（第２追加テーブル）のキー列TRs.Key（第３キー列，TRc.Key）（図６）が、追加テーブルTLs（図５Ａ）の何れかのキーTLs.Key_j（第１キー，TL.Key_j）と同じ値（共通値）を表すTRs.Key_i（第３キー，TR.Key_i）を含む場合、当該共通値を表すTRs.Key_i（第３キー，TR.Key_i）の少なくとも一部には、当該共通値を表すキーTLs.Key_j（第１キー，TL.Key_j）に対応付けられるサブキーTLs.S_j（第１サブキー）と同値のサブキーTRs.S_i（第２サブキー）が対応付けられる。例えば、当該共通値を表すTRs.Key_i（第３キー，TR.Key_i）の秘匿情報である[TRs.Key_i]の少なくとも一部には、当該共通値を表すキーTLs.Key_j（第１キー，TL.Key_j）に対応付けられるサブキーTLs.S_j（第１サブキー）と同値のサブキーTRs.S_i（第２サブキー）の秘匿情報である[TRs.S_i]が対応付けられる。好ましくは、追加テーブルTRs（第２追加テーブル）（図６）のキー列TRs.Key（第３キー列，TRc.Key）が当該共通値を表すTRs.Key_i（第３キー，TR.Key_i）を含む場合、当該共通値を表すキーTLs.Key_j（第１キー，TL.Key_j）（図５Ａ）に対応付けられている何れのサブキーTLs.S_j（第１サブキー）の値も、当該共通値を表すTRs.Key_i（第３キー，TR.Key_i）に対応付けられているサブキーTRs.S_0,...,TRs.$S_{RRN*K-1}$（第２サブキー）の何れかと同値である。例えば、当該共通値を表すキーTLs.Key_j（第１キー，TL.Key_j）の秘匿情報である[TLs.Key_j]（図５Ａ）に対応付けられている何れの秘匿化サブキー[TLs.S_j]の復元値（復号値）であるサブキーTLs.S_j（第１サブキー）の値も、当該共通値を表すTRs.Key_i（第３キー，TR.Key_i）の秘匿情報である[TRs.Key_i]に対応付けられている秘匿化サブキー[TRs.S_0],...,[TRs.$S_{RRN*K-1}$]の復元値（復号値）であるサブキーTRs.S_0,...,TRs.$S_{RRN*K-1}$（第２サブキー）の何れかと同値である。

[0042] 以下に[TR]と[TRc]と[TRs]との関係を例示する。

i=0,…,RRN・K-1について、iをKで割った商がidk（すなわち、idk=i div K）であり、imk=i-idk*Kであるとする。テーブルTR（第２テーブル）（図４Ｂ）のidk番目のレコードがTR_{idk}であり、テーブルTRc（第３テーブル）（図５Ｂ）のi番目のレコードがTRc_iであり、追加テーブルTRs（第２追加テーブル）（図６）のサブキー列TRs.S（第２サブキー列）のｉ番目のサブキー（第２サブキー）が$TRs.S_i$である。この場合、$TRs_i=TRc_i=TR_{idk}$であり、$TRs.S_i=imk$である。

[0043] したがって、サブキー列追加部１４－ｎは、以下のように、秘匿化テーブル[TR]から秘匿化追加テーブル[TRs]を得ることができる。

i=0,…,RRN・K-1について、iをKで割った商をidkとし、imk=i-idk*Kとし、以下の処理を行う。

(c-1) $[TRs_i]=[TRc_i]=[TR_{idk}]$

(c-2) $[TRs.S_i]=[imk]$

ここで(c-1)は、秘匿化テーブル[TR]の秘匿化レコード$[TR_{idk}]$を$[TRs_i]$として複製することで実現できる。(c-2)は、imkを秘匿化（例えば、秘密分散）して$[TRs.S_i]=[imk]$とすることで実現できる。

[0044] なお、ここでは説明のためにテーブルTRcおよび秘匿化テーブル[TRc]を示したが、サブキー列追加部１４－ｎは、秘匿化テーブル[TR]（図４Ｂ）を用いた秘密計算によって、秘匿化追加テーブル[TRs]（図６）を得ればよく、必ずしもテーブルTRcを秘匿化した秘匿化テーブル[TRc]（図５Ｂ）を得る必要はない。すなわち、サブキー列追加部１４－ｎは、[TR]から[TRs]を直接得てもよいし、[TR]から[TRc]を得、さらに[TRc]から[TRs]を得てもよい。

[0045] ≪秘密等結合部１５－ｎの処理（ステップＳ１５－ｎ）≫

各秘密等結合装置１０－ｎの秘密等結合部１５－ｎは、上述のように得られた秘匿化追加テーブル[TLs]（第１秘匿化追加テーブル）（図５Ａ）と秘匿化追加テーブル[TRs]（第２秘匿化追加テーブル）（図６）とを用いた秘密計算によって、テーブルTLsのTLs.Key_j（第１キー）とサブキーTLs.S_j（第１サ

ブキー）との組(TLs.Key$_j$, TLs.S$_j$)（j=0,...,LRN-1）を追加テーブルTLs（第１追加テーブル）のキー属性とし、追加テーブルTRsのキーTRs.Key$_i$（第３キー）とサブキーTRs.S$_i$（第２サブキー）との組(TRs.Key$_i$, TRs.S$_i$)（i=0,…,RRN*K-1）を追加テーブルTRs（第２追加テーブル）のキー属性として、追加テーブルTLs（第１追加テーブル）と追加テーブルTRs（第２追加テーブル）とを等結合した結合テーブルETRLの秘匿情報である秘匿化結合テーブル[ETRL]を得て出力する。前述したように、結合テーブルTLRは、追加テーブルTLsと追加テーブルTRsとの交差結合結果のテーブルTRLから、等号(TLs.Key$_j$, TLs.S$_j$)=(TRs.Key$_i$, TRs.S$_i$)が成り立つレコードだけを抜き出したテーブルである。

[0046] ここで、追加テーブルTLs（第１追加テーブル）のキーTLs.Key$_0$=TL.Key$_0$,...,TLs.Key$_{LRN-1}$=TL.Key$_{LRN-1}$のうち互いに同値のキーには、互いに異なる値のサブキーTLs.S$_j$が対応付けられている。そのため、追加テーブルTLsのキー属性である組(TLs.Key$_j$,TLs.S$_j$)の値は各レコードTLs$_j$を一義的に特定する。言い換えると、追加テーブルTLsの組(TLs.Key$_0$,TLs.S$_0$),...,(TLs.Key$_{LRN-1}$,TLs.S$_{LRN-1}$)には、互いに同値の組（両要素が重複する組）は存在しない。一方、追加テーブルTRs（第２追加テーブル）のキー属性である組(TRs.Key$_i$,TRs.S$_i$)の値は各レコードTRs$_j$を一義的に特定しない。言い換えると、追加テーブルTRsの組(TRs.Key$_0$,TRs.S$_0$),…,(TRs.Key$_{RRN*K-1}$,TRs.S$_{RRN*K-1}$)には、互いに同値の組（両要素が重複する組）が存在する。このように、等結合対象の２つのテーブルのうち、一方のテーブルのキー属性に重複がなく、他方のテーブルのキー属性のみに重複がある場合に、秘密計算によって等結合を行う方法は特許文献１に開示されている。したがって、秘密等結合部１５－ｎは、例えば、特許文献１に開示された方法に従い、秘匿化追加テーブル[TLs]と秘匿化追加テーブル[TRs]とを用いた秘密計算によって、秘匿化結合テーブル[ETRL]を得て出力する。この処理は以下のように記述される。

関数join：

[ETRL]=join(([TLs.Key],[TLs.S],[TLs.V(0)],...,[TLs.V(LVN-1)]),

([TRs.Key],[TRs.S],[TRs.V(0)],...,[TRs.V(RVN-1)]),

([TLs.Key],[TLs.S]),

([TRs.Key],[TRs.S]))

入力：([TLs.Key],[TLs.S],[TLs.V(0)],...,[TLs.V(LVN-1)]),([TRs.Key],[TRs.S],[TRs.V(0)],...,[TRs.V(RVN-1)])

出力：[ETRL]=([TLs.Key],[TLs.S],[TLs.V(0)],...,[TLs.V(LVN-1)],[TRs.Key],[TRs.S],[TRs.V(0)],...,[TRs.V(RVN-1)])

ただし、joinは以下のような秘密等結合を関数である。

[テーブル１と２を等結合したテーブル]=join([テーブル１],[テーブル２],[テーブル１のキー属性],[テーブル２のキー属性])

[0047] 得られた秘匿化結合テーブル[ETRL]は、秘密等号装置１０－ｎにおいて他の処理（例えば、秘密等号処理や復元処理）に用いられてもよいし、出力部１６－ｎから出力されて他の装置での処理に用いられてもよい。

[0048] ＜実施例＞

次に、本実施形態を具体例を用いて説明する。

この具体例では、図７Ａから図７Ｃに例示する秘匿化テーブルを秘密等結合し、図７Ｄに例示する秘匿化結合テーブルを得る例を示す。図７Ａの秘匿化テーブルは、”ID”をキー列とし、”飲料商品名”を任意要素列とする飲料商品名テーブルの秘匿情報である（以下、「秘匿化飲料商品名テーブル」）。飲料商品名テーブルのキー列はID=”1000”,”4050”,”3210”を要素に持ち、任意要素列は飲料商品名=”ミネラル水A”,”ブラックコーヒーB”,”オレンジジュースC”を要素に持つ。図７Ｂの秘匿化テーブルは、”ID”をキー列とし、”容量”を任意要素列とする容量テーブルの秘匿情報である（以下、「秘匿化容量テーブル」）。容量テーブルのキー列はID=”1000”,”1000”,”1000”,”4050”,”3210”を要素に持ち、任意要素列は容量=”200”,”500”,”1000”,”200”,”500”を要素に持つ。図７Ｃの秘匿化テーブルは、IDをキー列とし、”容器”を任意要素列とする容器種類テーブルの秘匿情報である（以下、「秘匿化容器種類テーブル」）。容器種類テーブルのキー列はID=”1000”,”1000”,”4050”,”4050”,”3210”を要素に持ち、任意要素列は容器=”ペットボトル”,”アルミ缶”,”ペットボ

トル”,”アルミ缶”,”アルミ缶”を要素に持つ。

[0049] ここで、図７Ａの秘匿化飲料商品名テーブルに対応するキー列は互いに同値の要素（キー）を持たない。一方、図７Ｂの秘匿化容量テーブルに対応するキー列は互いに同値の要素”1000”を持ち、図７Ｃの秘匿化容器種類テーブルに対応するキー列は互いに同値の要素”1000”及び”4050”を持つ。そこで、図８に例示するように、(1)まず本実施形態の方法を用い、図７Ｂの秘匿化容量テーブルと図７Ｃの秘匿化容器種類テーブルとの秘密等結合を行って秘匿化結合テーブル得、次に(2)当該秘匿化結合テーブルと図７Ａの秘匿化飲料商品名テーブルとの秘密等結合を行って、図７Ｄに例示する最終的な秘匿化結合テーブルを得る。ここでは、秘匿化容量テーブルを[TL]とし、LRN=5,LVN=1,[TL.Key]=[ID],[TL.Key_0]=[1000],[TL.Key_1]=[1000],[TL.Key_2]=[1000],[TL.Key_3]=[4050],[TL.Key_4]=[3210],[TL.$V(0)_0$]=[200],[TL.$V(0)_1$]=[500],[TL.$V(0)_2$]=[1000],[TL.$V(0)_3$]=[200],[TL.$V(0)_4$]=[500]とする。また、秘匿化容器種類テーブルを[TR]とし、RRN=5,RVN=1,[TR.Key]=[ID],[TR.Key_0]=[1000],[TR.Key_1]=[1000],[TR.Key_2]=[4050],[TR.Key_3]=[4050],[TR.Key_4]=[3210],[TR.$V(0)_0$]=[ペットボトル],[TR.$V(0)_1$]=[アルミ缶],[TR.$V(0)_2$]=[ペットボトル],[TR.$V(0)_3$]=[アルミ缶],[TR.$V(0)_4$]=[アルミ缶]とする。

[0050] 秘匿化容量テーブル[TL]に対してステップＳ１３－ｎの処理が実行されると、例えば、図９Ａに例示する秘匿化追加テーブル（秘匿化された「容量＋シーケンス番号」テーブル）[TLs]が得られる。この秘匿化追加テーブル[TLs]では、LRN=5,LVN=1,[TLs.Key]=[ID],[TLs.Key_0]=[1000],[TLs.Key_1]=[1000],[TLs.Key_2]=[1000],[TLs.Key_3]=[4050],[TLs.Key_4]=[3210],[TLs.S]=[SeqNo],[TLs.S_0]=[0],[TLs.S_1]=[1],[TLs.S_2]=[2],[TLs.S_3]=[0],[TLs.S_4]=[0],[TLs.$V(0)_0$]=[200],[TLs.$V(0)_1$]=[500],[TLs.$V(0)_2$]=[1000],[TLs.$V(0)_3$]=[200],[TLs.$V(0)_4$]=[500]となる。

[0051] 秘匿化容器種類テーブル[TR]に対してステップＳ１４－ｎの処理が実行されると、例えば、図９Ｂに例示する秘匿化追加テーブル（秘匿化された「容量種類＋シーケンス番号」テーブル）[TRs]が得られる。この秘匿化追加テー

ブル[TRs]では、K=5,RRN=5,RVN=1,[TRs.Key]=[ID],[TRs.Key_0]=[1000],[TRs.Key_1]=[1000],[TRs.Key_2]=[1000],[TRs.Key_3]=[1000],[TRs.Key_4]=[1000],[TRs.Key_5]=[1000],[TRs.Key_6]=[4050],[TRs.Key_7]=[4050],[TRs.Key_8]=[4050],[TRs.Key_9]=[4050],[TRs.Key_{10}]=[4050],[TRs.Key_{11}]=[4050],[TRs.Key_{12}]=[3210],[TRs.Key_{13}]=[3210],[TRs.Key_{14}]=[3210],[TRs.S]=[SeqNo],[TRs.S_0]=[0],[TRs.S_1]=[1],[TRs.S_2]=[2],[TRs.S_3]=[0],[TRs.S_4]=[1],[TRs.S_5]=[2],[TRs.S_6]=[0],[TRs.S_7]=[1],[TRs.S_8]=[2],[TRs.S_9]=[0],[TRs.S_{10}]=[1],[TRs.S_{11}]=[2],[TRs.S_{12}]=[0],[TRs.S_{13}]=[1],[TRs.S_{14}]=[2],[TRs.V(0)$_0$]=[ペットボトル],[TRs.V(0)$_1$]=[ペットボトル],[TRs.V(0)$_2$]=[ペットボトル],[TRs.V(0)$_3$]=[アルミ缶],[TRs.V(0)$_4$]=[アルミ缶],[TRs.V(0)$_5$]=[アルミ缶],[TRs.V(0)$_6$]=[ペットボトル],[TRs.V(0)$_7$]=[ペットボトル],[TRs.V(0)$_8$]=[ペットボトル],[TRs.V(0)$_8$]=[アルミ缶],[TRs.V(0)$_9$]=[アルミ缶],[TRs.V(0)$_{10}$]=[アルミ缶],[TRs.V(0)$_{11}$]=[アルミ缶],[TRs.V(0)$_{12}$]=[アルミ缶],[TRs.V(0)$_{13}$]=[アルミ缶],[TRs.V(0)$_{14}$]=[アルミ缶]となる。

[0052] このような秘匿化追加テーブル[TLs]と秘匿化追加テーブル[TRs]とに対してステップＳ１５－ｎの処理が実行されると、例えば、図１０に例示する秘匿化結合テーブル[ETRL]=([TLs.Key],[TLs.S],[TLs.V(0)],...,[TLs.V(LVN-1)],[TRs.Key],[TRs.S],[TRs.V(0)],...,[TRs.V(RVN-1)])=([ID],[SeqNo],[容量],[ID],[SeqNo],[容器])が得られる。

[0053] ＜本実施形態の特徴＞

以上のように、本実施形態では、サブキー列追加部１３－ｎが、秘匿化テーブル（第１秘匿化テーブル）[TL]を用いた秘密計算によって、サブキー列TLs.S（第１サブキー列）をテーブルTL（第１テーブル）に追加した追加テーブルTLs（第１追加テーブル）の秘匿情報である秘匿化追加テーブル[TLs]（第１秘匿化追加テーブル）を得る（ステップＳ１３－ｎ）。また、サブキー列追加部１４－ｎが、秘匿化テーブル（第２秘匿化テーブル）[TR]を用いた秘密計算によって、サブキー列TRs.S（第２サブキー列）をTRのレコードを複製して得られるテーブルTRc（第３テーブル）に追加した追加テーブルTRs（

第２追加テーブル）の秘匿情報である秘匿化追加テーブル[TRs]（第２秘匿化追加テーブル）を得る（ステップＳ１４－ｎ）。そして、秘密等結合部１５－ｎが、秘匿化追加テーブル[TLs]（第１秘匿化追加テーブル）と秘匿化追加テーブル[TRs]（第２秘匿化追加テーブル）とを用いた秘密計算によって、テーブルTLsのTLs.Key$_j$（第１キー）とサブキーTLs.S$_j$（第１サブキー）との組(TLs.Key$_j$, TLs.S$_j$)（j=0,...,LRN-1）を追加テーブルTLs（第１追加テーブル）のキー属性とし、追加テーブルTRsのキーTRs.Key$_i$（第３キー）とサブキーTRs.S$_i$（第２サブキー）との組(TRs.Key$_i$, TRs.S$_i$)（i=0,…,RRN*K-1）を追加テーブルTRs（第２追加テーブル）のキー属性として、追加テーブルTLs（第１追加テーブル）と追加テーブルTRs（第２追加テーブル）とを等結合した結合テーブルETRLの秘匿情報である秘匿化結合テーブル[ETRL]を得て出力する（ステップＳ１５－ｎ）。ここで、追加テーブルTLs（第１追加テーブル）のキーTLs.Key$_0$=TL.Key$_0$,...,TLs.Key$_{LRN-1}$=TL.Key$_{LRN-1}$のうち互いに同値のキーには、互いに異なる値のサブキーTLs.S$_j$が対応付けられている。そのため、追加テーブルTLsのキー属性である組(TLs.Key$_0$,TLs.S$_0$),...,(TLs.Key$_{LRN-1}$,TLs.S$_{LRN-1}$)には、互いに同値の組（両要素が重複する組）は存在しない。秘密等結合部１５－ｎは、例えば、特許文献１に開示された方法に従い、秘匿化追加テーブル[TLs]と秘匿化追加テーブル[TRs]とを用いた秘密計算によって、秘匿化結合テーブル[ETRL]を得ることができる。この場合、秘密等結合前のテーブルの分割、秘密等結合後のテーブルの結合といった処理が不要となるため、テーブルの情報を秘匿したまま、高速に２つのテーブルを等結合できる。

[0054] 特に、テーブルTRc（第３テーブル）（図５Ｂ）は、テーブルTR（第２テーブル）（図４Ｂ）の各レコードTR$_p$（ただし、p=0,...,RRN-1）をK回ずつ複製して得られる複数の複製レコードをテーブルTR（第２テーブル）に追加したテーブルであるが、K=KLの場合に最も高速に処理を行うことができる。

[0055] さらに、テーブルTR（第２テーブル，右テーブル）のキー列TR.Key（第２キー列）に含まれる互いに同値のキー（第２キー）の個数の最大値KRが、テーブルTL（第１テーブル，左テーブル）のキー列TL.Key（第１キー列）に含

まれる互いに同値のキーの個数の最大値KL以下である場合（KR≦KL）、より高速に処理を行うことができる。そのため、KR≦KLとなるように、秘匿化テーブル（第１秘匿化テーブル）[TL]および秘匿化テーブル（第２秘匿化テーブル）[TR]が記憶部１２－ｎに格納されていることが好ましい。

[0056] なお、本実施形態では、KLおよびKRの値が記憶部１２－ｎに格納されていたが、これらの少なくとも一方が既知であるならば、その既知の値が記憶部１２－ｎに格納されなくてもよい。

[0057] ［第２実施形態］

上述のように、KR≦KLとなるように、秘匿化テーブル（第１秘匿化テーブル）[TL]および秘匿化テーブル（第２秘匿化テーブル）[TR]が記憶部１２－ｎに格納されていることでより高速に処理を行うことができる。このようなことが保証されない環境の場合、KR≦KLとなるように秘匿化テーブルを入れ替える処理が行われてもよい。以下では、第１実施形態との相違点を中心に説明を行い、説明済みの事項については同じ参照番号を流用して説明を簡略化する。

[0058] ＜構成＞

図１に例示するように、本実施形態の秘密等結合システム２は、Ｎ個の秘密等結合装置２０－０，…，２０－（Ｎ－１）を含む。本実施形態の秘密等結合装置２０－０，…，２０－（Ｎ－１）は、ネットワークを通じて通信可能に接続されている。

[0059] 図２に例示するように、各秘密等結合装置２０－ｎ（ただし、ｎ＝０，…，Ｎ－１）は、テーブル再設定部２２１－ｎ、入力部１１－ｎ、記憶部１２－ｎ、サブキー列追加部１３－ｎ（第１サブキー列追加部）、サブキー列追加部１４－ｎ（第２サブキー列追加部）、秘密等結合部１５－ｎ、出力部１６－ｎ、制御部１７－ｎ、およびメモリ１８－ｎを有する。以下では説明を省略するが、各秘密等結合装置２０－ｎは、制御部１７－ｎに基づいて各処理を実行し、入力されたデータおよび各処理で得られたデータをメモリ１８－ｎに格納し、必要に応じて読み出して使用する。

[0060] ＜事前処理＞

第１実施形態と同じである。

[0061] ＜処理＞

図３を用いて本実施形態の秘密等結合方法を説明する。

《テーブル再設定部２２１－ｎの処理（ステップＳ２２１－ｎ）》

テーブル再設定部２２１－ｎは、記憶部１２－ｎからKR（第２キー列に含まれる互いに同値の第２キーの個数の最大値）およびKL（第１キー列に含まれる互いに同値の第１キーの個数の最大値）の値を読み出し、KRがKLよりも大きい場合、記憶部１２－ｎに格納された秘匿化テーブル[TL]（第１秘匿化テーブル）と秘匿化テーブル[TR]（第２秘匿化テーブル）とを入れ替えて記憶部１２－ｎに格納する。これにより、複数個(LRN個)のキー$TL.Key_0,...,TL.Key_{LRN-1}$（第１キー）を持つキー列TL.Key（第１キー列）と、複数個(LRN個)の任意要素$TL.V(v)_0,...,TL.V(v)_{LRN-1}$（第１任意要素）を持つ任意要素列TL.V(v)とを含むテーブルTL（第１テーブル，左テーブル）、および、複数個(RRN個)のキー$TR.Key_0,...,TR.Key_{RRN-1}$（第２キー）を持つキー列TR.Key（第２キー列）と、複数個(RRN個)の任意要素$TR.V(w)_0,...,TR.V(w)_{RRN-1}$（第２任意要素）を持つ任意要素列TR.V(w)とを含むテーブルTR（第２テーブル，右テーブル）を、それぞれ、複数個(RRN個)のキー$TR.Key_0,...,TR.Key_{RRN-1}$（第２キー）を持つキー列TR.Key（第２キー列）と、複数個(RRN個)の任意要素$TR.V(w)_0,...,TR.V(w)_{RRN-1}$（第２任意要素）を持つ任意要素列TR.V(w)とを含むテーブルTR（第２テーブル，右テーブル）、および、複数個(LRN個)のキー$TL.Key_0,...,TL.Key_{LRN-1}$（第１キー）を持つキー列TL.Key（第１キー列）と、複数個(LRN個)の任意要素$TL.V(v)_0,...,TL.V(v)_{LRN-1}$（第１任意要素）を持つ任意要素列TL.V(v)とを含むテーブルTL（第１テーブル，左テーブル）として再設定する。このように再設定された秘匿化テーブル[TL]（第１秘匿化テーブル）と秘匿化テーブル[TR]（第２秘匿化テーブル）は、KR≦KLの関係を満たす。一方、KRおよびKLがKR≦KLの関係を満たしている場合、テーブル再設定部２２１－ｎは秘匿化テーブル[TL]および[TR]の入れ替えを行わない。

[0062] ステップＳ２２１－ｎの後、第１実施形態で説明したステップＳ１３－ｎ，Ｓ１４－ｎ，およびＳ１５－ｎの処理が実行される。

[0063] ＜本実施形態の特徴＞

本実施形態でも第１実施形態と同様な効果を得ることができる。さらに、記憶部１２－ｎにKR≦KLの関係を満たす[TL]および[TR]が格納されていなかったとしても、それらを入れ替えることでKR≦KLの関係を満たす[TL]および[TR]に再設定できる。これにより、より高速に秘密等結合を行うことができる。

[0064] ［ハードウェア構成］

各実施形態における秘密等結合装置１０－ｎ，２０－ｎは、例えば、ＣＰＵ（central processing unit）等のプロセッサ（ハードウェア・プロセッサ）や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装置である。すなわち、各実施形態における秘密等結合装置１０－ｎ，２０－ｎは、例えば、それぞれが有する各部を実装するように構成された処理回路（processing circuitry）を有する。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、単独で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。また、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。

[0065] 図１１は、各実施形態における秘密等結合装置１０－ｎ，２０－ｎのハードウェア構成を例示したブロック図である。図１１に例示するように、この例の秘密等結合装置１０－ｎ，２０－ｎは、ＣＰＵ（Central Processing Unit）１０ａ、入力部１０ｂ、出力部１０ｃ、ＲＡＭ（Random Access Memory）１０ｄ、ＲＯＭ（Read Only Memory）１０ｅ、補助記憶装置１０ｆ及びバ

ス１０ｇを有している。この例のＣＰＵ１０ａは、制御部１０ａａ、演算部１０ａｂ及びレジスタ１０ａｃを有し、レジスタ１０ａｃに読み込まれた各種プログラムに従って様々な演算処理を実行する。また、入力部１０ｂは、データが入力される入力端子、キーボード、マウス、タッチパネル等である。また、出力部１０ｃは、データが出力される出力端子、ディスプレイ、所定のプログラムを読み込んだＣＰＵ１０ａによって制御されるＬＡＮカード等である。また、ＲＡＭ１０ｄは、ＳＲＡＭ（Static Random Access Memory）、ＤＲＡＭ（Dynamic Random Access Memory)等であり、所定のプログラムが格納されるプログラム領域１０ｄａ及び各種データが格納されるデータ領域１０ｄｂを有している。また、補助記憶装置１０ｆは、例えば、ハードディスク、ＭＯ（Magneto-Optical disc）、半導体メモリ等であり、所定のプログラムが格納されるプログラム領域１０ｆａ及び各種データが格納されるデータ領域１０ｆｂを有している。また、バス１０ｇは、ＣＰＵ１０ａ、入力部１０ｂ、出力部１０ｃ、ＲＡＭ１０ｄ、ＲＯＭ１０ｅ及び補助記憶装置１０ｆを、情報のやり取りが可能なように接続する。ＣＰＵ１０ａは、読み込まれたＯＳ（Operating System）プログラムに従い、補助記憶装置１０ｆのプログラム領域１０ｆａに格納されているプログラムをＲＡＭ１０ｄのプログラム領域１０ｄａに書き込む。同様にＣＰＵ１０ａは、補助記憶装置１０ｆのデータ領域１０ｆｂに格納されている各種データを、ＲＡＭ１０ｄのデータ領域１０ｄｂに書き込む。そして、このプログラムやデータが書き込まれたＲＡＭ１０ｄ上のアドレスがＣＰＵ１０ａのレジスタ１０ａｃに格納される。ＣＰＵ１０ａの制御部１０ａａは、レジスタ１０ａｃに格納されたこれらのアドレスを順次読み出し、読み出したアドレスが示すＲＡＭ１０ｄ上の領域からプログラムやデータを読み出し、そのプログラムが示す演算を演算部１０ａｂに順次実行させ、その演算結果をレジスタ１０ａｃに格納していく。このような構成により、秘密等結合装置１０－ｎ，２０－ｎの機能構成が実現される。

[0066] 上述のプログラムは、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。

[0067] 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。上述のように、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。そして、処理の実行時、このコンピュータは、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。また、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。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（コンピュータに対する直接の指令ではないがコンピ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。

[0068] 各実施形態では、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ェア的に実現することとしてもよい。

[0069] なお、本発明は上述の実施形態に限定されるものではない。例えば、秘密

等結合装置１０－０，…，１０－（Ｎ－１）（または２０－０，…，２０－（Ｎ－１））がネットワークではなく、可搬型記録媒体を介してデータの受け渡しを行ってもよい。また、上述の実施形態では、サブキーとして0,1,2,3...と１ずつ増加する値のようなシーケンス番号を例示したが、その他の番号や記号をサブキーとしてもよい。

[0070] また、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。

符号の説明

[0071] １，２　秘密等結合システム

１０－ｎ，２０－ｎ　秘密等結合装置

１３－ｎ，１４－ｎ　サブキー追加部

１５－ｎ　秘密等結合部

２２１－ｎ　テーブル再設定部

請求の範囲

[請求項1] (a)記憶部と、(b)第１サブキー列追加部と、(c)第２サブキー列追加部と、(d)秘密等結合部と、を有し、

(a)前記記憶部は、複数個の第１キーを持つ第１キー列と複数個の第１任意要素を持つ第１任意要素列とを含む第１テーブルの秘匿情報である第１秘匿化テーブルと、

複数個の第２キーを持つ第２キー列と複数個の第２任意要素を持つ第２任意要素列とを含む第２テーブルの秘匿情報である第２秘匿化テーブルと

を格納し、

(b)前記第１サブキー列追加部は、前記第１秘匿化テーブルを用いた秘密計算によって、第１サブキー列を前記第１テーブルに追加した第１追加テーブルの秘匿情報である第１秘匿化追加テーブルを得、

前記第１サブキー列は複数個の第１サブキーを持ち、

前記第１キーのそれぞれには、前記第１サブキーの何れかが対応付けられており、

前記第１キー列に含まれる互いに同値の前記第１キーの個数の最大値がＫＬであり、ＫＬは２以上の整数であり、

互いに同値の前記第１キーには、互いに異なる値の前記第１サブキーが対応付けられており、

(c)前記第２サブキー列追加部は、前記第２秘匿化テーブルを用いた秘密計算によって、第２サブキー列を第３テーブルに追加した第２追加テーブルの秘匿情報である第２秘匿化追加テーブルを得、

前記第２テーブルの各レコードは、各前記第２キーと各前記第２任意要素とを含み、

前記第３テーブルは、前記第２テーブルの各前記レコードをＫ回ずつ複製して得られる複数の複製レコードを前記第２テーブルに追加したテーブルであり、K≧KLであり、

前記第３テーブルは、前記第２キー及び前記第２キーの複製を含む複数の第３キーを持つ第３キー列と、前記第２任意要素及び前記第２任意要素の複製を含む複数の第３任意要素を持つ第３任意要素列とを含み、

前記第２サブキー列は複数個の第２サブキーを持ち、

前記第３キーのそれぞれには、前記第２サブキーの何れかが対応付けられており、

前記第３キー列が何れかの前記第１キーと同じ共通値を表す前記第３キーを含む場合、前記共通値を表す前記第３キーの少なくとも一部には、前記共通値を表す前記第１キーに対応付けられる前記第１サブキーと同値の前記第２サブキーが対応付けられ、

(d)前記秘密等結合部は、前記第１秘匿化追加テーブルと前記第２秘匿化追加テーブルとを用いた秘密計算によって、前記第１キーと前記第１サブキーとの組を前記第１追加テーブルのキー属性とし、前記第３キーと前記第２サブキーとの組を前記第２追加テーブルのキー属性として、前記第１追加テーブルと前記第２追加テーブルとを等結合した結合テーブルの秘匿情報である秘匿化結合テーブルを得る、

秘密等結合装置。

[請求項2] 請求項１の秘密等結合装置であって、

前記第３キー列が前記共通値を表す前記第３キーを含む場合、前記共通値を表す前記第１キーに対応付けられている何れの前記第１サブキーの値も、前記共通値を表す前記第３キーに対応付けられている前記第２サブキーの何れかと同値である、秘密等結合装置。

[請求項3] 請求項１または２の秘密等結合装置であって、

K=KLである、秘密等結合装置。

[請求項4] 請求項１から３の何れかの秘密等結合装置であって、

前記第２キー列に含まれる互いに同値の前記第２キーの個数の最大値は、前記第１キー列に含まれる互いに同値の前記第１キーの個数の

最大値以下である、秘密等結合装置。

[請求項5] 請求項１から３の何れかの秘密等結合装置であって、

(e)前記第２キー列に含まれる互いに同値の前記第２キーの個数の最大値が、前記第１キー列に含まれる互いに同値の前記第１キーの個数の最大値よりも大きい場合、前記第１秘匿化テーブルと前記第２秘匿化テーブルとを入れ替え、

前記第１キーを持つ前記第１キー列と前記第１任意要素を持つ前記第１任意要素列とを含む前記第１テーブル、および、前記第２キーを持つ前記第２キー列と前記第２任意要素を持つ前記第２任意要素列とを含む前記第２テーブルを、それぞれ、前記第２キーを持つ前記第２キー列と前記第２任意要素を持つ前記第２任意要素列とを含む前記第２テーブル、および、前記第１キーを持つ前記第１キー列と前記第１任意要素を持つ前記第１任意要素列とを含む前記第１テーブルとして再設定するテーブル再設定部をさらに有する、秘密等結合装置。

[請求項6] 請求項１から５の何れかの秘密等結合装置であって、

前記第１テーブルのレコード数がLRNであり、前記第２テーブルのレコード数がRRNであり、LRNおよびRRNは２以上の整数であり、

(b)j=0,…,LRN-1であり、

前記第１キー列のｊ番目の前記第１キーが$TL.Key_j$であり、

前記第１サブキー列のｊ番目の前記第１サブキーが$TLs.S_j$であり、

j=0のとき$TLs.S_j=0$であり、

j>0かつ$TL.Key_j \neq TL.Key_{j-1}$であれば$TLs.S_j=0$であり、

j>0かつ$TL.Key_j=TL.Key_{j-1}$であれば$TLs.S_j=TLs.S_{j-1}+1$であり、

(c)i=0,…,RRN*K-1であり、

iをKで割った商がidkであり、

imk=i-idk*Kであり、

前記第２テーブルのidk番目のレコードがTR_{idk}であり、

前記第３テーブルのi番目のレコードがTRc_iであり、

$TRc_i=TR_{idk}$であり、

前記第２サブキー列のｉ番目の前記第２サブキーが$TRs.S_i$であり、

$TRs.S_i=imk$である、秘密等結合装置。

[請求項7] 秘密等結合装置の秘密等結合方法であって、

(a)記憶ステップと、(b)第１サブキー列追加ステップと、(c)第２サブキー列追加ステップと、(d)秘密等結合ステップと、を有し、

(a)記憶ステップは、複数個の第１キーを持つ第１キー列と複数個の第１任意要素を持つ第１任意要素列とを含む第１テーブルの秘匿情報である第１秘匿化テーブルと、

複数個の第２キーを持つ第２キー列と複数個の第２任意要素を持つ第２任意要素列とを含む第２テーブルの秘匿情報である第２秘匿化テーブルと

を記憶部に格納するステップであり、

(b)前記第１サブキー列追加ステップは、第１サブキー列追加部が、前記第１秘匿化テーブルを用いた秘密計算によって、第１サブキー列を前記第１テーブルに追加した第１追加テーブルの秘匿情報である第１秘匿化追加テーブルを得るステップであり、

前記第１サブキー列は複数個の第１サブキーを持ち、

前記第１キーのそれぞれには、前記第１サブキーの何れかが対応付けられており、

前記第１キー列に含まれる互いに同値の前記第１キーの個数の最大値がＫＬであり、ＫＬは２以上の整数であり、

互いに同値の前記第１キーには、互いに異なる値の前記第１サブキーが対応付けられており、

(c)前記第２サブキー列追加ステップは、第２サブキー列追加部が、前記第２秘匿化テーブルを用いた秘密計算によって、第２サブキー列を第３テーブルに追加した第２追加テーブルの秘匿情報である第２秘匿化追加テーブルを得るステップであり、

前記第２テーブルの各レコードは、各前記第２キーと各前記第２任意要素とを含み、

前記第３テーブルは、前記第２テーブルの各前記レコードをＫ回ずつ複製して得られる複数の複製レコードを前記第２テーブルに追加したテーブルであり、Ｋ≧ＫＬであり、

前記第３テーブルは、前記第２キー及び前記第２キーの複製を含む複数の第３キーを持つ第３キー列と、前記第２任意要素及び前記第２任意要素の複製を含む複数の第３任意要素を持つ第３任意要素列とを含み、

前記第２サブキー列は複数個の第２サブキーを持ち、

前記第３キーのそれぞれには、前記第２サブキーの何れかが対応付けられており、

前記第３キー列が何れかの前記第１キーと同じ共通値を表す前記第３キーを含む場合、前記共通値を表す前記第３キーの少なくとも一部には、前記共通値を表す前記第１キーに対応付けられる前記第１サブキーと同値の前記第２サブキーが対応付けられ、

(d)前記秘密等結合ステップは、前記秘密等結合部が、前記第１秘匿化追加テーブルと前記第２秘匿化追加テーブルとを用いた秘密計算によって、前記第１キーと前記第１サブキーとの組を前記第１追加テーブルのキー属性とし、前記第３キーと前記第２サブキーとの組を前記第２追加テーブルのキー属性として、前記第１追加テーブルと前記第２追加テーブルとを等結合した結合テーブルの秘匿情報である秘匿化結合テーブルを得るステップである、

秘密等結合方法。

[請求項8] 請求項１から６の何れかの秘密等結合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]

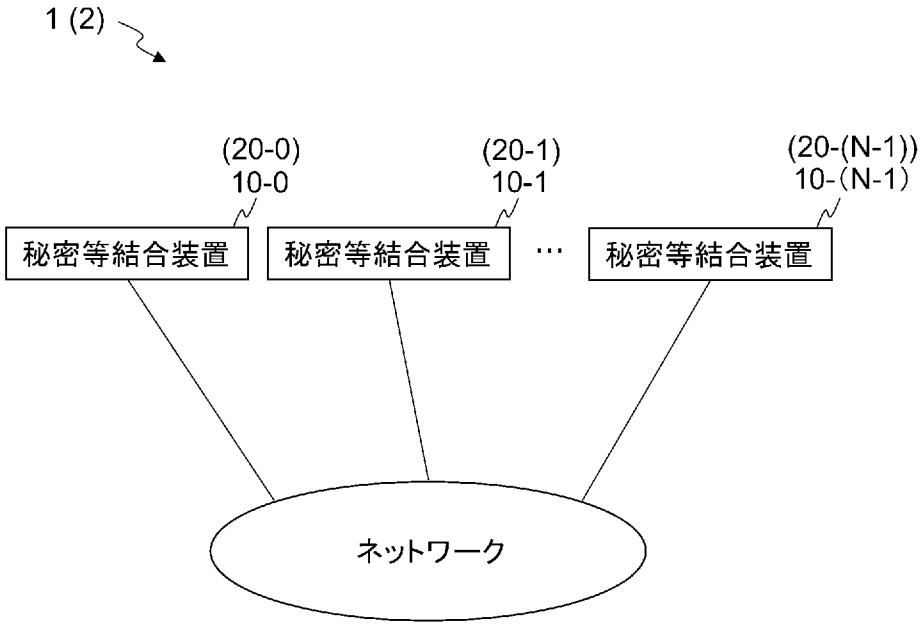


図1

[図2]

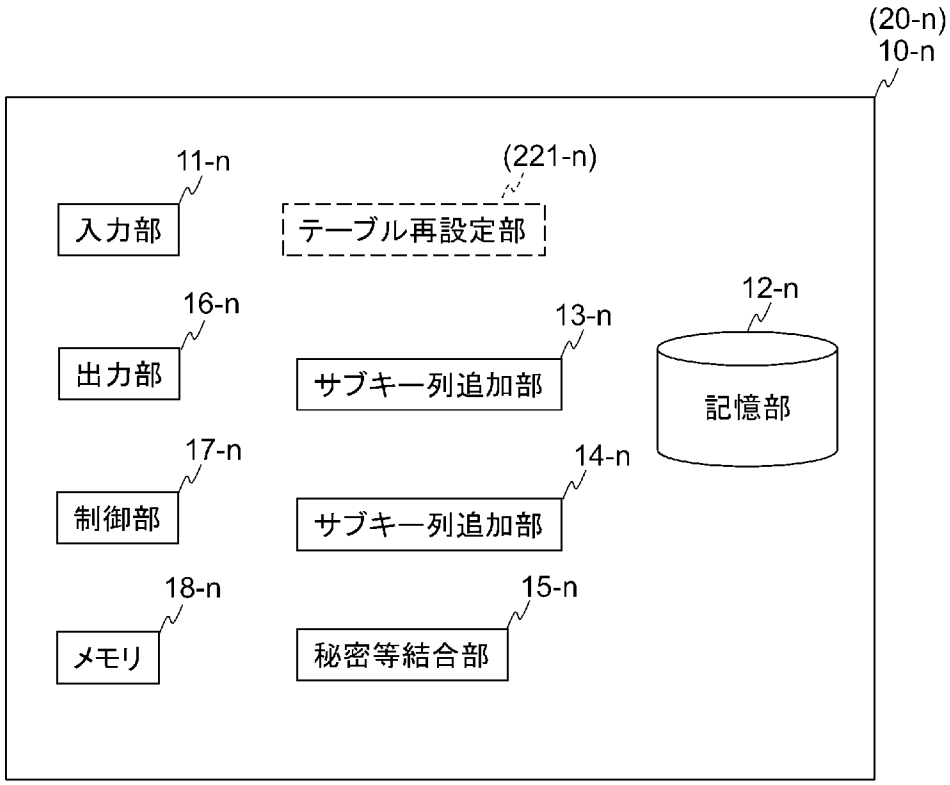

(20-n)
10-n
11-n
入力部
(221-n)
テーブル再設定部
12-n
記憶部
16-n
出力部
13-n
サブキー列追加部
17-n
制御部
14-n
サブキー列追加部
18-n
メモリ
15-n
秘密等結合部

図2

[図3]

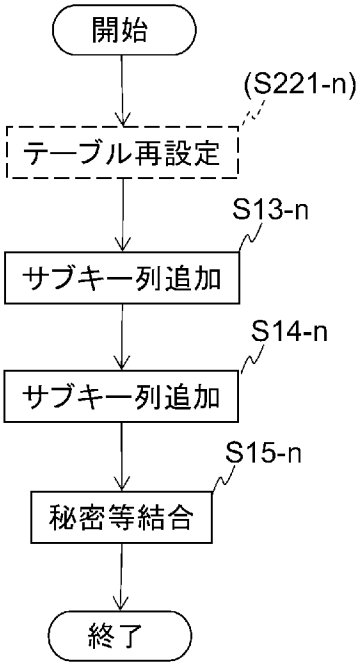


図3

[図4]

図4A

[TL]

[TL.Key]	[TL.V(0)]	...	[TL.V(LVN-1)]
[TL.Key$_0$]	[TL.V(0)$_0$]	...	[TL.V(LVN-1)$_0$]
[TL.Key$_1$]	[TL.V(0)$_1$]	...	[TL.V(LVN-1)$_1$]
...	...	...	...
[TL.Key$_j$]	[TL.V(0)$_j$]	...	[TL.V(LVN-1)$_j$]
...	...	...	...
[TL.Key$_{LRN-1}$]	[TL.V(0)$_{LRN-1}$]	...	[TL.V(LVN-1)$_{LRN-1}$]

[TL$_j$]

図4B

[TR]

[TR.Key]	[TR.V(0)]	...	[TR.V(RVN-1)]
[TR.Key$_0$]	[TR.V(0)$_0$]	...	[TR.V(RVN-1)$_0$]
[TR.Key$_1$]	[TR.V(0)$_1$]	...	[TR.V(RVN-1)$_1$]
...	...	...	...
[TR.Key$_p$]	[TR.V(0)$_p$]	...	[TR.V(RVN-1)$_p$]
...	...	...	...
[TR.Key$_{RRN-1}$]	[TR.V(0)$_{RRN-1}$]	...	[TR.V(RVN-1)$_{RRN-1}$]

[TR$_p$]

[図5]

図5A

[TLs]

[TLs.Key]	[TLs.S]	[TLs.V(0)]	...	[TLs.V(LVN-1)]
[TL.Key$_0$]	[TLs.S$_0$]	[TL.V(0)$_0$]	...	[TL.V(LVN-1)$_0$]
[TL.Key$_1$]	[TLs.S$_1$]	[TL.V(0)$_1$]	...	[TL.V(LVN-1)$_1$]
...	...	...	...	...
[TL.Key$_j$]	[TLs.S$_j$]	[TL.V(0)$_j$]	...	[TL.V(LVN-1)$_j$]
...	...	...	...	...
[TL.Key$_{LRN-1}$]	[TLs.S$_{LRN-1}$]	[TL.V(0)$_{LRN-1}$]	...	[TL.V(LVN-1)$_{LRN-1}$]

図5B

[TRc]

[TRc.Key]	[TRc.V(0)]	...	[TRc.V(RVN-1)]
[TR.Key$_0$]	[TR.V(0)$_0$]	...	[TR.V(RVN-1)$_0$]
...	...	...	...
[TR.Key$_0$]	[TR.V(0)$_0$]	...	[TR.V(RVN-1)$_0$]
...	...	...	...
[TR.Key$_p$]	[TR.V(0)$_p$]	...	[TR.V(RVN-1)$_p$]
...	...	...	...
[TR.Key$_p$]	[TR.V(0)$_p$]	...	[TR.V(RVN-1)$_p$]
...	...	...	...
[TR.Key$_{RRN-1}$]	[TR.V(0)$_{RRN-1}$]	...	[TR.V(RVN-1)$_{RRN-1}$]
...	...	...	...
[TR.Key$_{RRN-1}$]	[TR.V(0)$_{RRN-1}$]	...	[TR.V(RVN-1)$_{RRN-1}$]

K

[図6]

[TRs]

[TRs.Key]	[TRs.S]	[TRs.V(0)]	...	[TRs.V(RVN-1)]
[TR.Key$_0$]	[TRs.S$_0$]	[TR.V(0)$_0$]	...	[TR.V(RVN-1)$_0$]
...	...	...	...	...
[TR.Key$_0$]	[TRs.S$_{K-1}$]	[TR.V(0)$_0$]	...	[TR.V(RVN-1)$_0$]
...	...	...	...	...
[TR.Key$_p$]	[TRs.S$_{p*K}$]	[TR.V(0)$_p$]	...	[TR.V(RVN-1)$_p$]
...	...	...	...	...
[TR.Key$_p$]	[TRs.S$_{(p+1)*K-1}$]	[TR.V(0)$_p$]	...	[TR.V(RVN-1)$_p$]
...	...	...	...	...
[TR.Key$_{RRN-1}$]	[TRs.S$_{(RRN-1)*K}$]	[TR.V(0)$_{RRN-1}$]	...	[TR.V(RVN-1)$_{RRN-1}$]
...	...	...	...	...
[TR.Key$_{RRN-1}$]	[TRs.S$_{RRN*K-1}$]	[TR.V(0)$_{RRN-1}$]	...	[TR.V(RVN-1)$_{RRN-1}$]

図6

[図7]

図7A

■飲料商品名

ID	飲料商品名
[1000]	[ミネラル水A]
[4050]	[ブラックコーヒーB]
[3210]	[オレンジジュースC]

図7B

■容量

ID	容量
[1000]	[200]
[1000]	[500]
[1000]	[1000]
[4050]	[200]
[3210]	[500]

図7C

■容器種類

ID	容器
[1000]	[ペットボトル]
[1000]	[アルミ缶]
[4050]	[ペットボトル]
[4050]	[アルミ缶]
[3210]	[アルミ缶]

図7D

■飲料商品リスト

ID	飲料商品名	容量	容器
[1000]	[ミネラル水A]	[200]	[ペットボトル]
[1000]	[ミネラル水A]	[200]	[アルミ缶]
[1000]	[ミネラル水A]	[500]	[ペットボトル]
[1000]	[ミネラル水A]	[500]	[アルミ缶]
[1000]	[ミネラル水A]	[1000]	[ペットボトル]
[1000]	[ミネラル水A]	[1000]	[アルミ缶]
[4050]	[ブラックコーヒーB]	[200]	[ペットボトル]
[4050]	[ブラックコーヒーB]	[200]	[アルミ缶]
[3210]	[オレンジジュースC]	[500]	[アルミ缶]

[図8]

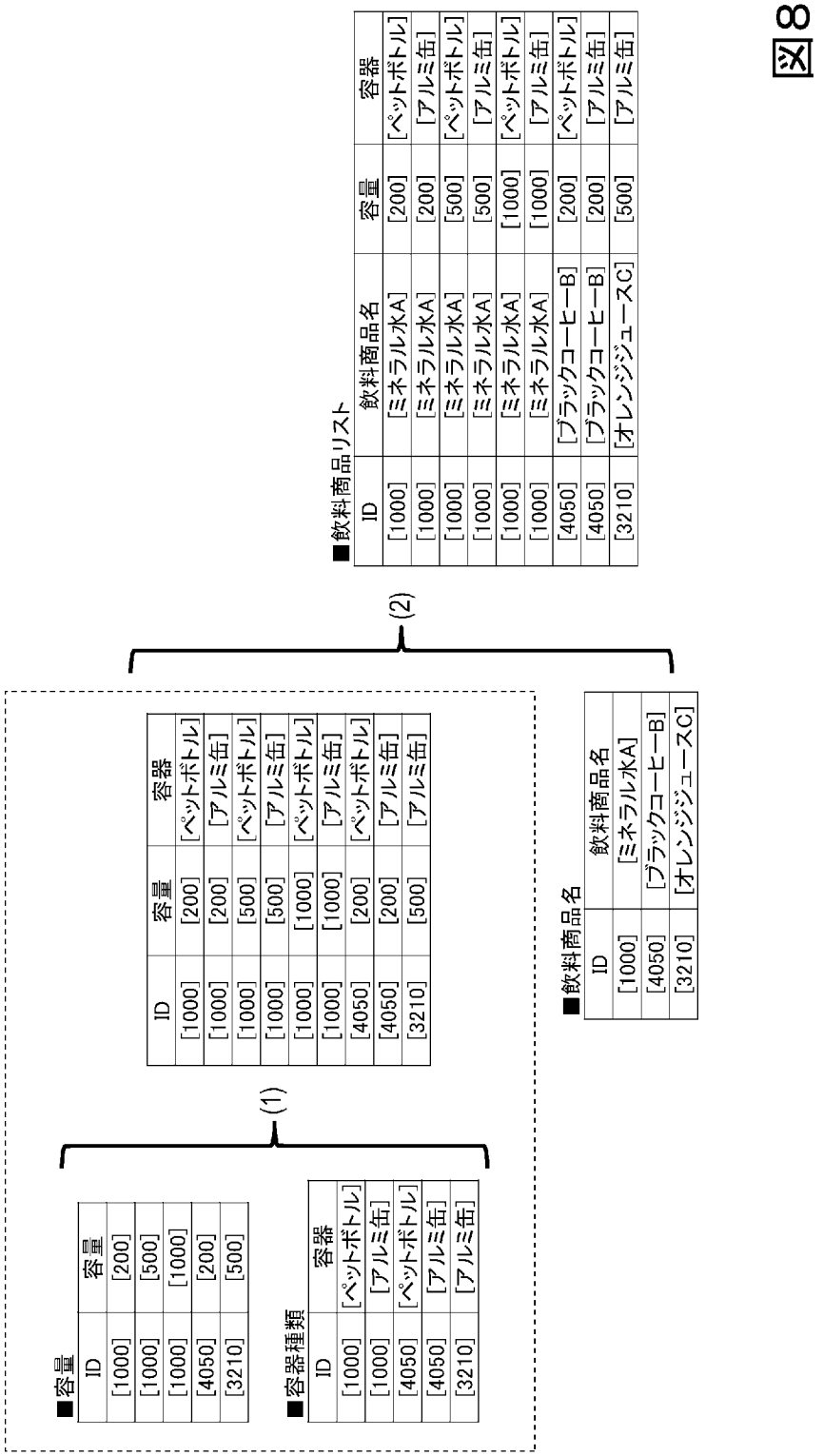

■容量
ID 容量
[1000] [200]
[1000] [500]
[1000] [1000]
[4050] [200]
[3210] [500]
■容器種類
ID 容器
[1000] [ペットボトル]
[1000] [アルミ缶]
[4050] [ペットボトル]
[4050] [アルミ缶]
[3210] [アルミ缶]
(1)
ID 容量 容器
[1000] [200] [ペットボトル]
[1000] [200] [アルミ缶]
[1000] [500] [ペットボトル]
[1000] [500] [アルミ缶]
[1000] [1000] [ペットボトル]
[1000] [1000] [アルミ缶]
[4050] [200] [ペットボトル]
[4050] [200] [アルミ缶]
[3210] [500] [アルミ缶]
■飲料商品名
ID 飲料商品名
[1000] [ミネラル水A]
[4050] [ブラックコーヒーB]
[3210] [オレンジジュースC]
(2)
■飲料商品リスト
ID 飲料商品名 容量 容器
[1000] [ミネラル水A] [200] [ペットボトル]
[1000] [ミネラル水A] [200] [アルミ缶]
[1000] [ミネラル水A] [500] [ペットボトル]
[1000] [ミネラル水A] [500] [アルミ缶]
[1000] [ミネラル水A] [1000] [ペットボトル]
[1000] [ミネラル水A] [1000] [アルミ缶]
[4050] [ブラックコーヒーB] [200] [ペットボトル]
[4050] [ブラックコーヒーB] [200] [アルミ缶]
[3210] [オレンジジュースC] [500] [アルミ缶]

図8

[図9]

図9A

■容量＋シーケンス番号

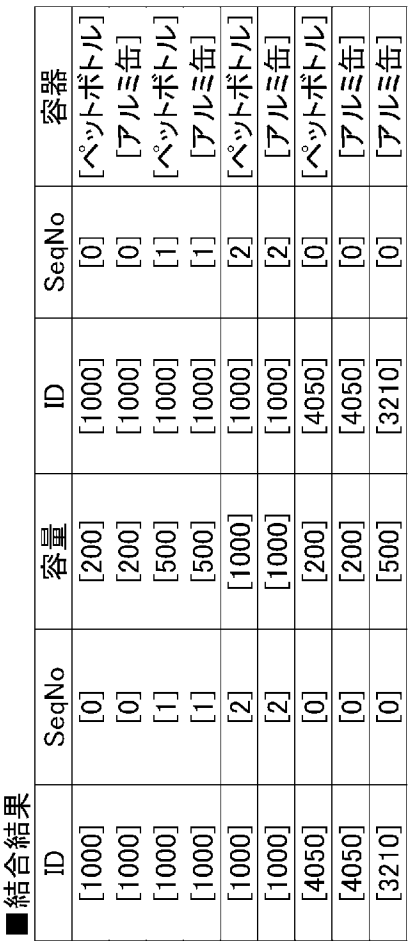
ID	SeqNo	容量
[1000]	[0]	[200]
[1000]	[1]	[500]
[1000]	[2]	[1000]
[4050]	[0]	[200]
[3210]	[0]	[500]

図9B

■容器種類×ｋ＋シーケンス番号

ID	SeqNo	容器
[1000]	[0]	[ペットボトル]
[1000]	[1]	[ペットボトル]
[1000]	[2]	[ペットボトル]
[1000]	[0]	[アルミ缶]
[1000]	[1]	[アルミ缶]
[1000]	[2]	[アルミ缶]
[4050]	[0]	[ペットボトル]
[4050]	[1]	[ペットボトル]
[4050]	[2]	[ペットボトル]
[4050]	[0]	[アルミ缶]
[4050]	[1]	[アルミ缶]
[4050]	[2]	[アルミ缶]
[3210]	[0]	[アルミ缶]
[3210]	[1]	[アルミ缶]
[3210]	[2]	[アルミ缶]

[図10]



■結合結果

ID	SeqNo	容量	ID	SeqNo	容器
[1000]	[0]	[200]	[1000]	[0]	[ペットボトル]
[1000]	[0]	[200]	[1000]	[0]	[アルミ缶]
[1000]	[1]	[500]	[1000]	[1]	[ペットボトル]
[1000]	[1]	[500]	[1000]	[1]	[アルミ缶]
[1000]	[2]	[1000]	[1000]	[2]	[ペットボトル]
[1000]	[2]	[1000]	[1000]	[2]	[アルミ缶]
[4050]	[0]	[200]	[4050]	[0]	[ペットボトル]
[4050]	[0]	[200]	[4050]	[0]	[アルミ缶]
[3210]	[0]	[500]	[3210]	[0]	[アルミ缶]

図10

[図11]

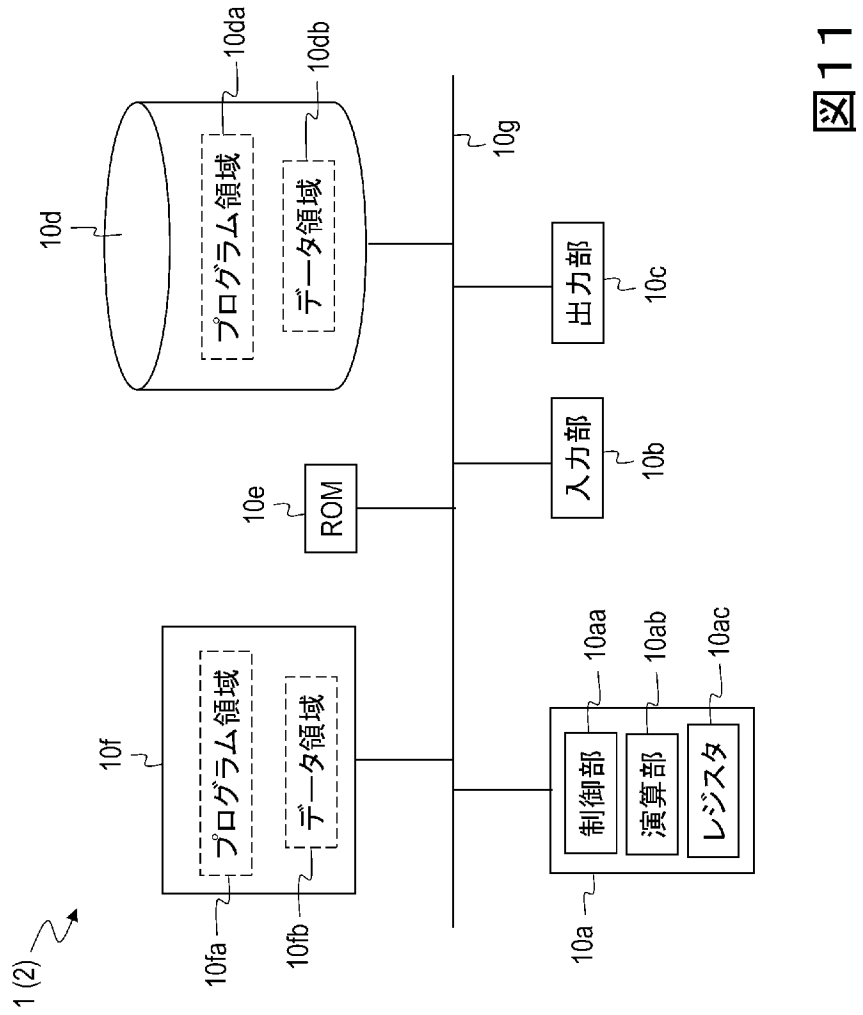

1 (2)
10f
プログラム領域
データ領域
10fa
10fb
10d
プログラム領域
データ領域
10da
10db
10e
ROM
10a
制御部
演算部
レジスタ
10aa
10ab
10ac
10g
入力部
10b
出力部
10c

図11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2021/025131

A. CLASSIFICATION OF SUBJECT MATTER
G09C 1/00(2006.01)i
FI: G09C1/00 650Z

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G09C1/00

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

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2021
Registered utility model specifications of Japan	1996-2021
Published registered utility model applications of Japan	1994-2021

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	JP 2014-139640 A (NIPPON TELEGR & TELEPH CORP <NTT>) 31 July 2014 (2014-07-31) entire text, all drawings	1-8
A	WO 2018/061800 A1 (NIPPON TELEGRAPH & TELEPHONE) 05 April 2018 (2018-04-05) entire text, all drawings	1-8
A	「秘匿計算システム データを暗号化したまま処理可能にして、RDB からの情報漏洩を防止する」，BUSINESS COMMUNICATION, 01 March 2014, vol. 51, no. 3, pp. 82-83, [ISSN] 0385-695X, in particular, description in “development of a system that can process RDB data without decoding”, non-official translation (Concealment calculation system: Preventing information leakage from RDB by making it possible to process data while it is encrypted)	1-8

☐ 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
20 August 2021 (20.08.2021)	31 August 2021 (31.08.2021)

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
Information on patent family members

International application No.
PCT/JP2021/025131

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2014-139640 A	31 Jul. 2014	(Family: none)	
WO 2018/061800 A1	05 Apr. 2018	US 2019/0228010 A1 entire text, all drawings EP 3522137 A1 CN 109791741 A	

国際調査報告

国際出願番号
PCT/JP2021/025131

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 650Z

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	１９７１－２０２１年
日本国実用新案登録公報	１９９６－２０２１年
日本国登録実用新案公報	１９９４－２０２１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	JP 2014-139640 A (日本電信電話株式会社) 31.07.2014 (2014-07-31) 全文、全図	1-8
A	WO 2018/061800 A1 (日本電信電話株式会社) 05.04.2018 (2018-04-05) 全文、全図	1-8
A	「秘匿計算システム　データを暗号化したまま処理可能にして、ＲＤＢからの情報漏洩を防止する」, ＢＵＳＩＮＥＳＳ ＣＯＭＭＵＮＩＣＡＴＩＯＮ, 2014.03.01, 第５１巻　第３号, pp. 82-83, [ＩＳＳＮ] 0385-695X 特に、「ＲＤＢのデータを復号せずに処理できるシステムを開発」における記載	1-8

☐ 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	国際調査報告の発送日
20.08.2021	31.08.2021

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）
松平　英 5S 3146

電話番号 03-3581-1101 内線 3546

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/JP2021/025131

引用文献	公表日	パテントファミリー文献	公表日
JP 2014-139640 A	31.07.2014	（ファミリーなし）	
WO 2018/061800 A1	05.04.2018	US 2019/0228010 A1 全文、全図 EP 3522137 A1 CN 109791741 A	