(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10月31日(31.10.2019)

WIPO | PCT

(10) 国際公開番号
WO 2019/208484 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号： PCT/JP2019/016985

(22) 国際出願日： 2019年4月22日(22.04.2019)

(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 2018-084114 2018年4月25日(25.04.2018) 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).

(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, 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, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) **Title:** SECURE AGGREGATE SUM SYSTEM, SECURE COMPUTATION DEVICE, SECURE AGGREGATE SUM METHOD, AND PROGRAM

(54) 発明の名称： 秘密集約総和システム、秘密計算装置、秘密集約総和方法、およびプログラム

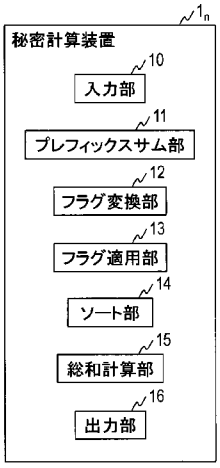


図2

1n Secure computation device
10 Input unit
11 Prefix sum unit
12 Flag conversion unit
13 Flag application unit
14 Sort unit
15 Sum computation unit
16 Output unit

(57) **Abstract:** The present invention efficiently finds an aggregate sum while maintaining confidentiality. According to the present invention, a prefix sum unit (11) computes prefix sums from shares for sorted value attributes. A flag conversion unit (12) performs a format conversion on shares for flags that represent the final elements of groups. A flag application unit (13) generates a share for a vector in which a prefix sum is set when the flag that represents the final element of a group is true and in which a sum is set when the flag is false. A sort unit (14) generates a share for a sorted vector that is the result of the vector being sorted by permutation that arranges the final elements of the groups in order from the top. A sum computation unit (15) generates a share for a vector in which the differences between the values of given elements of the sorted vector and the values of the previous elements are set and that represents the sum of each group.

(57) 要約：秘匿性を保ったまま集約総和を効率的に求める。プレフィックスサム部（１１）は、ソート済みのバリュー属性のシェアからプレフィックスサムを計算する。フラグ変換部（１２）は、グループの最後の要素を表すフラグのシェアを形式変換する。フラグ適用部（１３）は、グループの最後の要素を表すフラグが真のときプレフィックスサムを設定し、フラグが偽のとき全体の総和を設定したベクトルのシェアを生成する。ソート部（１４）は、ベクトルを各グループの最後の要素を先頭から順に並ぶように移動する置換でソートしたソート済みベクトルのシェアを生成する。総和計算部（１５）は、ソート済みベクトルのある要素の値と前の要素の値との差を設定してグループ毎の総和を表すベクトルのシェアを生成する。

WO 2019/208484 A1

[続葉有]

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:

一 国際調査報告(条約第21条(3))

明　細　書

発明の名称 ：

秘密集約総和システム、秘密計算装置、秘密集約総和方法、およびプログラム

技術分野

[0001] この発明は秘密計算技術に関し、特に、秘匿性を保ったまま集約関数を計算する技術に関する。

背景技術

[0002] 集約関数は、テーブルにキー属性とバリュー属性があるときに、キー属性の値に基づいてグループ分けした統計値を得る演算である。集約関数は、group-by演算とも呼ばれる。キー属性は、テーブルのレコードをグループ分けするために用いる属性であり、例えば、役職や性別などが挙げられる。バリュー属性は、統計値を計算するために用いる属性であり、例えば、給料や身長などが挙げられる。group-by演算は、例えば、キー属性が性別のときに、男女別の平均身長を求める演算などである。キー属性は複数の属性による複合キーであってもよく、例えば、キー属性が性別と年齢のときに、10代男性の平均身長、20代男性の平均身長、・・・を得るような演算であってもよい。非特許文献１には、group-by演算を秘密計算で行う方法が記載されている。

[0003] 集約総和は、集約関数の一つであり、テーブルをキー属性の値に基づいてグループ分けしたときに、グループごとに所望のバリュー属性の総和を集計する演算である。集約総和は、group-by総和とも呼ばれる。group-by総和は、例えば、キー属性が性別と年齢のときに、10代男性の給料総額、20代男性の給料総額、・・・を得るような演算である。

[0004] group-by総和を用いれば、グループごとに乗算の和を求めるgroup-by積和や、グループごとに二乗の和を求めるgroup-by二乗和も計算することができる。group-by積和であれば、各レコードのバリュー属性に乗算を施した結果に対してgroup-by総和を求めればよい。また、group-by二乗和であれば、同

様に、各レコードのバリュー属性に二乗を施した結果に対してgroup-by総和を求めればよい。

先行技術文献

非特許文献

[0005] 非特許文献1：五十嵐大，千田浩司，濱田浩気，高橋克巳，“軽量検証可能３パーティ秘匿関数計算の効率化及びこれを用いたセキュアなデータベース処理”，２０１１年暗号と情報セキュリティシンポジウム

発明の概要

発明が解決しようとする課題

[0006] 従来の秘密計算技術では、group-by総和を求めるために、nを計算主体の数としてlog(n)の通信回数が必要となり、効率が悪かった。

[0007] この発明の目的は、上記のような技術的課題に鑑みて、秘匿性を保ったままgroup-by総和を効率的に求めることができる技術を提供することである。

課題を解決するための手段

[0008] 上記の課題を解決するために、この発明の一態様の秘密集約総和システムは、複数の秘密計算装置を含む秘密集約総和システムであって、mは２以上の整数であり、$[v]:=[v_0]$，…，$[v_{m-1}]$はキー属性とバリュー属性とからなるテーブルをキー属性の値に基づいてソートしたときの所望のバリュー属性$v:=v_0$，…，v_{m-1}を秘密分散したシェアであり、$[e]:=[e_0]$，…，$[e_{m-1}]$はテーブルをキー属性の値に基づいてグループ分けしたときに各グループの最後の要素が真、その他の要素が偽であるフラグ$e:=e_0$，…，e_{m-1}を秘密分散したシェアであり、{{σ}}はテーブルをキー属性の値に基づいてグループ分けしたときに各グループの最後の要素が先頭から順に並ぶように移動する置換σを秘密分散したシェアであり、gはグループの最大数であり、秘密計算装置は、シェア[v]を用いて、0以上m-1以下の各整数iについてv'_iにv_0からv_iまでの総和を設定して、復元するとベクトル$v':=v'_0$，…，v'_{m-1}となるシェア[v']を生成するプレフィックスサム部と、シェア[v']とシェア[e]とを用いて、0以上m-1以下の各

整数iについて[e_i]が真ならば[t_i]に[v'_i]を設定し、[e_i]が偽ならば[t_i]に[v'_{m-1}]を設定して、復元するとベクトル$t:=t_0, \cdots, t_{m-1}$となるシェア[t]を生成するフラグ適用部と、シェア[t]とシェア{{σ}}とを用いて、復元するとベクトルtを置換σでソートしたソート済みベクトルσ(t)となるシェア[σ(t)]を生成するソート部と、シェア[σ(t)]を用いて、1以上min(g,m)-1以下の各整数iについて[s_i]:=[$\sigma(t)_i-\sigma(t)_{i-1}$]を設定し、かつ、[$s_0$]:=[$\sigma(t)_0$]を設定して、復元するとグループ毎のバリュー属性vの総和を表すベクトル$s:=s_0, \cdots, s_{min(g,m)-1}$となるシェア[s]を生成する総和計算部と、を含む。

発明の効果

[0009] この発明の秘密集約総和技術によれば、秘匿性を保ったままgroup-by総和をO(1)の通信回数で効率的に求めることができる。

図面の簡単な説明

[0010] [図1]図１は、秘密集約総和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、秘密集約総和方法の処理手続きを例示する図である。

[図4]図４は、変形例の秘密計算装置の機能構成を例示する図である。

発明を実施するための形態

[0011] 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。

[0012] [x]∈[F]は、ある値xが任意の環F上の秘密分散等により秘匿されていることを表す。{b}∈{B}は、１ビットのある値bが１ビットを表せる環B上の秘密分散等により秘匿されていることを表す。{{s}}∈{{S_m}}は、m個の要素の置換の集合S_mに属するある置換sが秘密分散等により秘匿されていることを表す。以下、秘密分散された値を「シェア」とも呼ぶ。

[0013] 実施形態中で用いる秘密計算におけるソート処理（安定ソートを含む）は、例えば、下記参考文献１に記載されたソートを用いることができる。置換sのシェア{{s}}については下記参考文献１に記載されたハイブリッド置換{{π}}を用いればよい。

[0014] 〔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”，ＣＳＳ２０１７

＜実施形態＞

図１を参照して、実施形態の秘密集約総和システム１００の構成例を説明する。秘密集約総和システム１００は、N（≧2）台の秘密計算装置1_1，…，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９へ接続される。通信網９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（Local Area Network）、WAN（Wide Area Network）などを用いることができる。なお、各装置は必ずしも通信網９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，…，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1_1，…，1_Nへオフラインで入力するように構成してもよい。

[0015] 図２を参照して、秘密集約総和システム１００に含まれる秘密計算装置1_n（n=1，…，N）の構成例を説明する。秘密計算装置1_nは、例えば、図２に示すように、入力部１０、プレフィックスサム部１１、フラグ変換部１２、フラグ適用部１３、ソート部１４、総和計算部１５、および出力部１６を含む。この秘密計算装置1_n（$1 \leqq n \leqq N$）が他の秘密計算装置$1_{n'}$（$n'=1, \cdots, N$、ただし$n \neq n'$）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集約総和方法が実現される。

[0016] 秘密計算装置1_nは、例えば、中央演算処理装置（CPU: Central Processing 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1_n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1_n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_nの各処理部は、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。

[0017] 図３を参照して、実施形態の秘密集約総和システム１００が実行する秘密集約総和方法の処理手続きを説明する。

[0018] ステップＳ１０において、各秘密計算装置1_nの入力部１０は、キー属性でソート済みのバリュー属性$v\in F^m$を秘密分散により秘匿したシェア$[v]\in[F]^m$と、フラグ$e\in B^m$を秘密分散により秘匿したシェア$\{e\}\in\{B\}^m$と、置換σを秘密分散により秘匿したシェア$\{\{\sigma\}\}\in\{\{S_m\}\}$と、最大グループ数gとを入力として受け取る。ただし、mは２以上の整数である。入力部１０は、バリュー属性vのシェア[v]をプレフィックスサム部１１へ、フラグeのシェア{e}をフラグ変換部１２へ、置換σのシェア$\{\{\sigma\}\}$をソート部１４へ出力する。

[0019] フラグeは、グループの境界を表すフラグである。例えば、フラグeは、テーブルをキー属性で安定ソートしたときに同じキー属性の値をもつレコードを同じグループとして、各グループの最後の要素（すなわち、グループの境界の直前の要素）に該当する値が真（例えば１）となり、その他の要素に該当する値が偽（例えば０）となるフラグである。なお、安定ソートとは、ソート演算のうち、同じ値の要素が存在した場合に、同じ値の要素同士の順序を保存する演算である。例えば、社員番号順でソートされたテーブルに対して性別で安定ソートすると、各性別の中で社員番号順が保たれているソート結果が得られる。以下、$\{e\}\in\{B\}^m$の各要素は、$\{e_i\}\in\{B\}$（$i=0, \cdots, m-1$）で参照することもある。

[0020] 置換σは、各グループのキー属性の値を先頭から１つずつ並べる置換である。例えば、置換σは、テーブルをキー属性で安定ソートしたときに同じキー属性の値をもつレコードを同じグループとして、各グループの最後の要素が先頭から順に並び、続いて他の要素が順に並ぶように移動する置換である。置換σのシェア$\{\{\sigma\}\}$は上記参考文献１に記載されたハイブリッド置換$\{\{\pi\}\}$を用いて構成すればよい。

[0021] 最大グループ数gは、キー属性が取り得る値の組み合わせの数、すなわち、キー属性が取り得る値の種類の数である。

[0022] ステップＳ１１において、各秘密計算装置1_nのプレフィックスサム部１１は、バリュー属性vのシェア[v]を用いて、[v']:=prefix-sum([v])を計算し、復元するとベクトルv':=v'_0, …, v'_{m-1}∈Fとなるシェア[v']∈[F]^{m}を生成する。prefix-sumは、mを入力ベクトルvの長さとして、0以上m-1以下の各整数iについて、出力ベクトルv'のi番目の要素v'_iには入力ベクトルvの0番目の要素v_0からi番目の要素v_iまでの値の総和を設定する演算である。プレフィックスサム部１１は、ベクトルv'のシェア[v']をフラグ適用部１３へ出力する。

[0023] ステップＳ１２において、各秘密計算装置1_nのフラグ変換部１２は、フラグeのシェア{e}∈{B}^{m}を任意の環F上の秘密分散によるシェア[e]∈[F]^{m}に変換する。フラグ変換部１２は、フラグeのシェア[e]をフラグ適用部１３へ出力する。

[0024] ステップＳ１３において、各秘密計算装置1_nのフラグ適用部１３は、ベクトルv'のシェア[v']とフラグeのシェア[e]とを用いて、0以上m-1以下の各整数iについて[t_i]:=[e_i?v'_i:v'_{m-1}]を設定し、復元するとベクトルt:=t_0, …, t_{m-1}∈Fとなるシェア[t]∈[F]^{m}を生成する。ここで、「?」は条件演算子（または三項演算子）である。すなわち、[e_i]が真（例えば、[e_i]=[1]）のときは[t_i]:=[v'_i]を設定し、[e_i]が偽（例えば、[e_i]=[0]）のときは[t_i]:=[v'_{m-1}]を設定する。ベクトルtは、テーブルをキー属性で安定ソートしたときに同じキー属性の値をもつレコードを同じグループとして、各グループの最後の要素にはその要素以前のバリュー属性の値の総和が設定され、その他の要素にはテーブル全体のバリュー属性の値の総和が設定されたベクトルとなる。フラグ適用部１３は、ベクトルtのシェア[t]をソート部１４へ出力する。

[0025] ステップＳ１４において、各秘密計算装置1_nのソート部１４は、ベクトルtのシェア[t]と置換σのシェア{{σ}}とを用いて、復元するとベクトルtを置換σでソートしたソート済みベクトルσ(t)となるシェア[σ(t)]∈[F]^{m}を生成する。以下、[σ(t)]∈[F]^{m}の各要素は、[σ(t)$_i$]∈[F]（i=0, …, m-1）で参

照することもある。ソート部１４は、ソート済みベクトルσ(t)のシェア[σ(t)]を総和計算部１５へ出力する。

[0026] ステップＳ１５において、各秘密計算装置1_nの総和計算部１５は、ソート済みベクトルσ(t)のシェア[σ(t)]を用いて、1以上min(g,m)-1以下の各整数iについて$[s_i]:=[\sigma(t)_i-\sigma(t)_{i-1}]$を設定し、かつ、$[s_0]:=[\sigma(t)_0]$を設定して、復元するとグループ毎のバリュー属性vの総和$s:=s_0, \cdots, s_{min(g,m)-1}\in F$となるシェア$[s]\in[F]^{min(g,m)}$を生成する。ソート済みベクトルσ(t)のi番目の要素$\sigma(t)_i$は、0番目からi番目までの各グループに属するバリュー属性vの値の総和が設定されているため、ベクトルsのi番目の要素s_iには、i番目のグループに属するバリュー属性vの値の総和が設定されることになる。総和計算部１５は、総和sのシェア[s]を出力部１６へ出力する。

[0027] ステップＳ１６において、各秘密計算装置1_nの出力部１６は、総和sのシェア[s]を出力する。

[0028] ＜変形例＞

上記の実施形態では、入力部１０へバリュー属性vのシェア[v]とフラグeのシェア{e}と置換σのシェア{{σ}}とが入力される構成を説明した。変形例では、入力部１０へテーブルを秘密分散等により秘匿したシェアが入力され、バリュー属性vのシェア[v]とフラグeのシェア{e}と置換σのシェア{{σ}}とを求めてから、上記の実施形態で説明した手順に従ってgroup-by総和を計算する構成を説明する。

[0029] 変形例の秘密計算装置2_n（n=1, …, N）は、例えば、図４に示すように、実施形態の秘密計算装置1_n（n=1, …, N）が備える各処理部に加えて、ビット分解部２１、グループソート生成部２２、ビット列ソート部２３、フラグ生成部２４、キー集約ソート生成部２５、およびバリューソート部２６を含む。以下、実施形態の秘密集約総和システム１００と異なる点についてのみ説明する。

[0030] 各秘密計算装置2_nの入力部１０は、n_k個のキー属性$k_0, \cdots, k_{nk-1}\in F^m$それぞれを秘密分散により秘匿したシェア$[k_0], \cdots, [k_{nk-1}]\in[F]^m$と、$n_a$個のバリュ

一属性v_0，…，v_{na-1}∈F^mそれぞれを秘密分散により秘匿したシェア[v_0]，…，[v_{na-1}]∈[F]^{m}とを入力として受け取る。ただし、n_k，n_aは１以上の整数である。以下、[k_j]∈[F]^m（j=0，…，n_k-1）の各要素は、[$k_{j,i}$]∈[F]（i=0，…，m-1）で参照することもある。入力部１０は、キー属性k_0，…，k_{nk-1}のシェア[k_0]，…，[k_{nk-1}]をビット分解部２１へ出力する。

[0031] 各秘密計算装置2_nのビット分解部２１は、キー属性k_0，…，k_{nk-1}のシェア[k_0]，…，[k_{nk-1}]をビット分解して結合し、復元するとキー属性k_0，…，k_{nk-1}のビット表現を結合したビット列b:=b_0，…，b_{m-1}∈B^λとなるシェア{b}∈{B}$^\lambda$を得る。ただし、λはビット列bのビット長であり、各b_i（i=0，…，m-1）のビット長の総和である。言い替えると、{b_i}は、キー属性k_0，…，k_{nk-1}のシェア[k_0]，…，[k_{nk-1}]それぞれのi番目の要素[$k_{0,i}$]，…，[$k_{nk-1,i}$]のビット表現を結合したビット列である。ビット分解部２１は、ビット列bのシェア{b}をグループソート生成部２２へ出力する。

[0032] 各秘密計算装置2_nのグループソート生成部２２は、ビット列bのシェア{b}を用いて、復元するとビット列bを昇順で安定ソートするための置換σ_0となるシェア{{σ_0}}∈{{S_m}}を生成する。ビット列bはキー属性k_0，…，k_{nk-1}のビット表現を結合したものであるため、置換σ_0はキー属性k_0，…，k_{nk-1}の値が等しいレコードを連続するように並び替えてグループ分けする操作であるとも言える。グループソート生成部２２は、ビット列bのシェア{b}と置換σ_0のシェア{{σ_0}}とをビット列ソート部２３へ出力する。また、グループソート生成部２２は、置換σ_0のシェア{{σ_0}}をバリューソート部２６へ出力する。

[0033] 各秘密計算装置2_nのビット列ソート部２３は、ビット列bのシェア{b}と置換σ_0のシェア{{σ_0}}とを用いて、復元するとビット列bを置換σ_0でソートしたソート済みビット列b':=b'$_0$，…，b'$_{m-1}$∈B^λとなるシェア{b'}∈{B}$^\lambda$を得る。ビット列ソート部２３は、ソート済みビット列b'のシェア{b'}をフラグ生成部２４へ出力する。

[0034] 各秘密計算装置2_nのフラグ生成部２４は、ソート済みビット列b'のシェア{b'}を用いて、0以上m-2以下の各整数iについて{e_i}:={b'$_i$≠b'$_{i+1}$}を設定し、か

つ、$\{e_{m-1}\}:=\{1\}$を設定して、復元するとフラグ$e:=e_0, \cdots, e_{m-1} \in B^m$となるシェア$\{e\} \in \{B\}^m$を生成する。フラグ$e_i$はソート済みビット列b'のi番目の要素$b'_i$がi+1番目の要素$b'_{i+1}$と異なる場合に真が設定されるため、各グループの最後の要素（すなわち、グループ間の境界の直前の要素）を示すフラグとなる。フラグ生成部２４は、フラグeのシェア{e}をキー集約ソート生成部２５へ出力する。また、フラグ生成部２４は、フラグeのシェア{e}をフラグ変換部１２へ出力する。

[0035] 各秘密計算装置2_nのキー集約ソート生成部２５は、まず、フラグeのシェア{e}を用いて、復元するとフラグeの否定¬eであるフラグe'となるシェア$\{e'\} \in \{B\}^m$を生成する。すなわち、0以上m-1以下の各整数iについて$\{e'_i\}:=\{\neg e_i\}$を設定する。次に、キー集約ソート生成部２５は、フラグe'のシェア{e'}を用いて、復元するとフラグe'を昇順に安定ソートするための置換σとなるシェア$\{\{\sigma\}\} \in \{\{S_m\}\}$を生成する。キー集約ソート生成部２５は、置換σのシェア$\{\{\sigma\}\}$をバリューソート部２６へ出力する。また、キー集約ソート生成部２５は、置換σのシェア$\{\{\sigma\}\}$をソート部１４へ出力する。

[0036] 各秘密計算装置2_nのバリューソート部２６は、バリュー属性$v_0, \cdots, v_{na-1}$のシェア$[v_0], \cdots, [v_{na-1}]$と置換$\sigma_0$のシェア$\{\{\sigma_0\}\}$とを用いて、復元するとバリュー属性$v_0, \cdots, v_{na-1}$を置換$\sigma_0$でソートしたソート済みバリュー属性$v''_0, \cdots, v''_{na-1}$となるシェア$[v''_0], \cdots, [v''_{na-1}]$を生成する。バリューソート部２６は、ソート済みバリュー属性$v''_0, \cdots, v''_{na-1}$のシェア$[v''_0], \cdots, [v''_{na-1}]$のうち、グループ毎の総和を計算したいものをバリュー属性vのシェア[v]としてプレフィックスサム部１１へ出力する。

[0037] 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。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。

[0038] ［プログラム、記録媒体］

上記実施形態で説明した各装置における各種の処理機能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。そして、このプログラムをコンピュータで実行することにより、上記各装置における各種の処理機能がコンピュータ上で実現される。

[0039] 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。

[0040] 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。

[0041] 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。

[0042] また、この形態では、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。

請求の範囲

[請求項1] 複数の秘密計算装置を含む秘密集約総和システムであって、

mは２以上の整数であり、$[v]:=[v_0], \cdots, [v_{m-1}]$はキー属性とバリュー属性とからなるテーブルを上記キー属性の値に基づいてソートしたときの所望のバリュー属性$v:=v_0, \cdots, v_{m-1}$を秘密分散したシェアであり、$[e]:=[e_0], \cdots, [e_{m-1}]$は上記テーブルを上記キー属性の値に基づいてグループ分けしたときに各グループの最後の要素が真、その他の要素が偽であるフラグ$e:=e_0, \cdots, e_{m-1}$を秘密分散したシェアであり、$\{\{\sigma\}\}$は上記テーブルを上記キー属性の値に基づいてグループ分けしたときに各グループの最後の要素が先頭から順に並ぶように移動する置換σを秘密分散したシェアであり、gは上記グループの最大数であり、

上記秘密計算装置は、

上記シェア[v]を用いて、0以上m-1以下の各整数iについてv'_iにv_0からv_iまでの総和を設定して、復元するとベクトル$v':=v'_0, \cdots, v'_{m-1}$となるシェア[v']を生成するプレフィックスサム部と、

上記シェア[v']と上記シェア[e]とを用いて、0以上m-1以下の各整数iについて$[e_i]$が真ならば$[t_i]$に$[v'_i]$を設定し、$[e_i]$が偽ならば$[t_i]$に$[v'_{m-1}]$を設定して、復元するとベクトル$t:=t_0, \cdots, t_{m-1}$となるシェア[t]を生成するフラグ適用部と、

上記シェア[t]と上記シェア$\{\{\sigma\}\}$とを用いて、復元すると上記ベクトルtを上記置換σでソートしたソート済みベクトルσ(t)となるシェア$[\sigma(t)]$を生成するソート部と、

上記シェア$[\sigma(t)]$を用いて、1以上min(g,m)-1以下の各整数iについて$[s_i]:=[\sigma(t)_i-\sigma(t)_{i-1}]$を設定し、かつ、$[s_0]:=[\sigma(t)_0]$を設定して、復元するとグループ毎のバリュー属性vの総和を表すベクトル$s:=s_0, \cdots, s_{\min(g,m)-1}$となるシェア[s]を生成する総和計算部と、

を含む秘密集約総和システム。

[請求項2] 請求項１に記載の秘密集約総和システムであって、

Fは任意の環であり、n_kは１以上の整数であり、$[k_0]$, …, $[k_{nk-1}]$はキー属性k_0, …, $k_{nk-1}\in F^m$を秘密分散したシェアであり、[v”]は上記テーブルを上記キー属性の値に基づいてソートする前の所望のバリュー属性$v”\in F^m$を秘密分散したシェアであり、

上記秘密計算装置は、

上記シェア$[k_0]$, …, $[k_{nk-1}]$を用いて、復元すると上記キー属性k_0, …, k_{nk-1}をビット分解して結合したビット列$b:=b_0$, …, b_{m-1}となるシェア{b}から、復元すると上記ビット列bを昇順に安定ソートする置換σ_0となるシェア$\{\{\sigma_0\}\}$を生成するグループソート生成部と、

上記シェア{b}と上記シェア$\{\{\sigma_0\}\}$とを用いて、復元すると上記ビット列bを上記置換σ_0でソートしたソート済みビット列$b':=b'_0$, …, b'_{m-1}となるシェア{b’}を生成するビット列ソート部と、

上記シェア{b’}を用いて、0以上m-2以下の各整数iについて$\{e_i\}:=\{b'_i\neq b'_{i+1}\}$を設定し、かつ、$\{e_{m-1}\}:=\{1\}$を設定して、復元すると上記フラグ$e:=e_0$, …, e_{m-1}となる上記シェア{e}を生成するフラグ生成部と、

上記シェア{e}を用いて、復元すると上記フラグeの否定¬eを昇順に安定ソートする上記置換σとなる上記シェア$\{\{\sigma\}\}$を生成するキー集約ソート生成部と、

上記シェア[v”]と上記シェア$\{\{\sigma_0\}\}$とを用いて、復元すると上記バリュー属性v”を上記置換σ_0でソートした上記バリュー属性vとなるシェア[v]を生成するバリューソート部と、

をさらに含む秘密集約総和システム。

[請求項3] mは２以上の整数であり、$[v]:=[v_0]$, …, $[v_{m-1}]$はキー属性とバリュー属性とからなるテーブルを上記キー属性の値に基づいてソートしたときの所望のバリュー属性$v:=v_0$, …, v_{m-1}を秘密分散したシェアであり、$[e]:=[e_0]$, …, $[e_{m-1}]$は上記テーブルを上記キー属性の値に基

づいてグループ分けしたときに各グループの最後の要素が真、その他の要素が偽であるフラグe:=e_0, …, e_{m-1}を秘密分散したシェアであり、{{σ}}は上記テーブルを上記キー属性の値に基づいてグループ分けしたときに各グループの最後の要素が先頭から順に並ぶように移動する置換σを秘密分散したシェアであり、gは上記グループの最大数であり、

上記シェア[v]を用いて、0以上m-1以下の各整数iについてv'$_i$にv_0からv_iまでの総和を設定して、復元するとベクトルv':=v'$_0$, …, v'$_{m-1}$となるシェア[v']を生成するプレフィックスサム部と、

上記シェア[v']と上記シェア[e]とを用いて、0以上m-1以下の各整数iについて[e_i]が真ならば[t_i]に[v'$_i$]を設定し、[e_i]が偽ならば[t_i]に[v'$_{m-1}$]を設定して、復元するとベクトルt:=t_0, …, t_{m-1}となるシェア[t]を生成するフラグ適用部と、

上記シェア[t]と上記シェア{{σ}}とを用いて、復元すると上記ベクトルtを上記置換σでソートしたソート済みベクトルσ(t)となるシェア[σ(t)]を生成するソート部と、

上記シェア[σ(t)]を用いて、1以上min(g,m)-1以下の各整数iについて[s_i]:=[σ(t)$_i$-σ(t)$_{i-1}$]を設定し、かつ、[s_0]:=[σ(t)$_0$]を設定して、復元するとグループ毎のバリュー属性vの総和を表すベクトルs:=s_0, …, $s_{min(g,m)-1}$となるシェア[s]を生成する総和計算部と、

を含む秘密計算装置。

[請求項4] 複数の秘密計算装置を含む秘密集約総和システムが実行する秘密集約総和方法であって、

mは２以上の整数であり、[v]:=[v_0], …, [v_{m-1}]はキー属性とバリュー属性とからなるテーブルを上記キー属性の値に基づいてソートしたときの所望のバリュー属性v:=v_0, …,v_{m-1}を秘密分散したシェアであり、[e]:=[e_0], …, [e_{m-1}]は上記テーブルを上記キー属性の値に基づいてグループ分けしたときに各グループの最後の要素が真、その他

の要素が偽であるフラグe:=e_0, …, e_{m-1}を秘密分散したシェアであり、{{σ}}は上記テーブルを上記キー属性の値に基づいてグループ分けしたときに各グループの最後の要素が先頭から順に並ぶように移動する置換σを秘密分散したシェアであり、gは上記グループの最大数であり、

上記秘密計算装置のプレフィックスサム部が、上記シェア[v]を用いて、0以上m-1以下の各整数iについてv'_iにv_0からv_iまでの総和を設定して、復元するとベクトルv':=v'_0, …, v'_{m-1}となるシェア[v']を生成し、

上記秘密計算装置のフラグ適用部が、上記シェア[v']と上記シェア[e]とを用いて、0以上m-1以下の各整数iについて[e_i]が真ならば[t_i]に[v'_i]を設定し、[e_i]が偽ならば[t_i]に[v'_{m-1}]を設定して、復元するとベクトルt:=t_0, …, t_{m-1}となるシェア[t]を生成し、

上記秘密計算装置のソート部が、上記シェア[t]と上記シェア{{σ}}とを用いて、復元すると上記ベクトルtを上記置換σでソートしたソート済みベクトルσ(t)となるシェア[σ(t)]を生成し、

上記秘密計算装置の総和計算部が、上記シェア[σ(t)]を用いて、1以上min(g,m)-1以下の各整数iについて[s_i]:=[$\sigma(t)_i - \sigma(t)_{i-1}$]を設定し、かつ、[$s_0$]:=[$\sigma(t)_0$]を設定して、復元するとグループ毎のバリュー属性vの総和を表すベクトルs:=s_0, …, $s_{\min(g,m)-1}$となるシェア[s]を生成する、

秘密集約総和方法。

[請求項5] 請求項３に記載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]

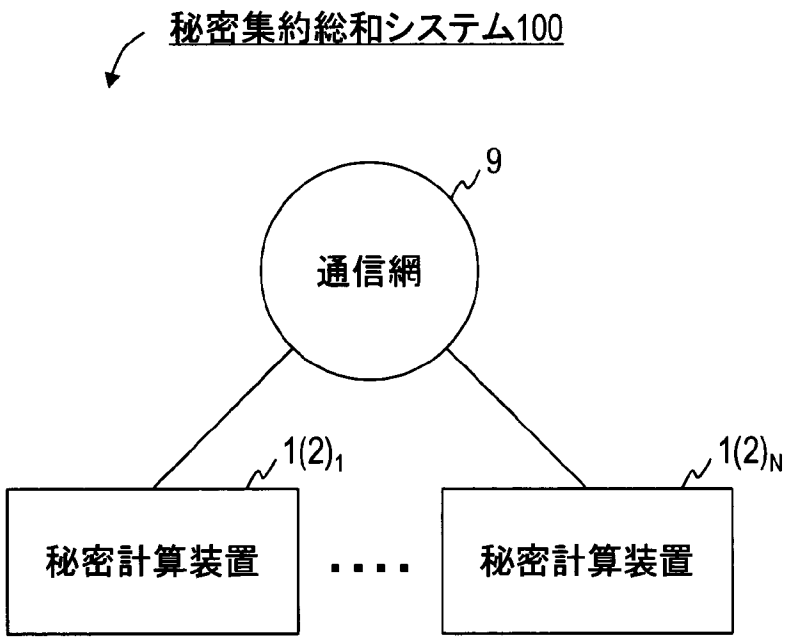


図1

[図2]

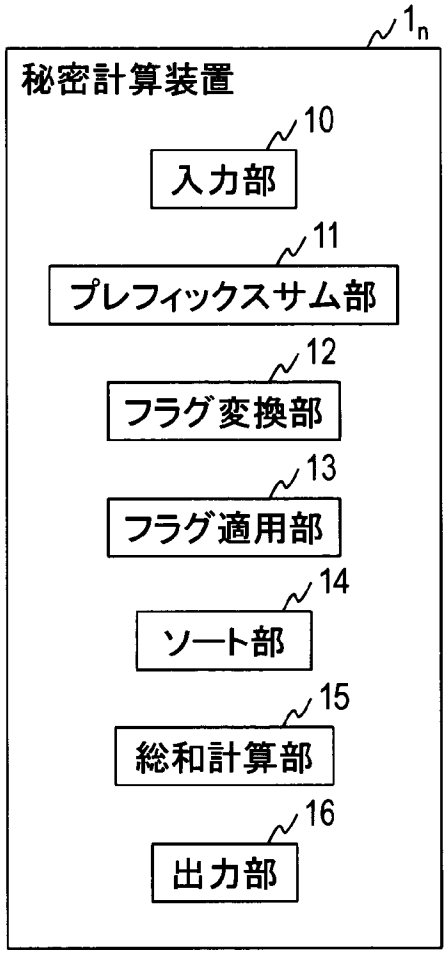

1n
秘密計算装置
10
入力部
11
プレフィックスサム部
12
フラグ変換部
13
フラグ適用部
14
ソート部
15
総和計算部
16
出力部

図2

[図3]

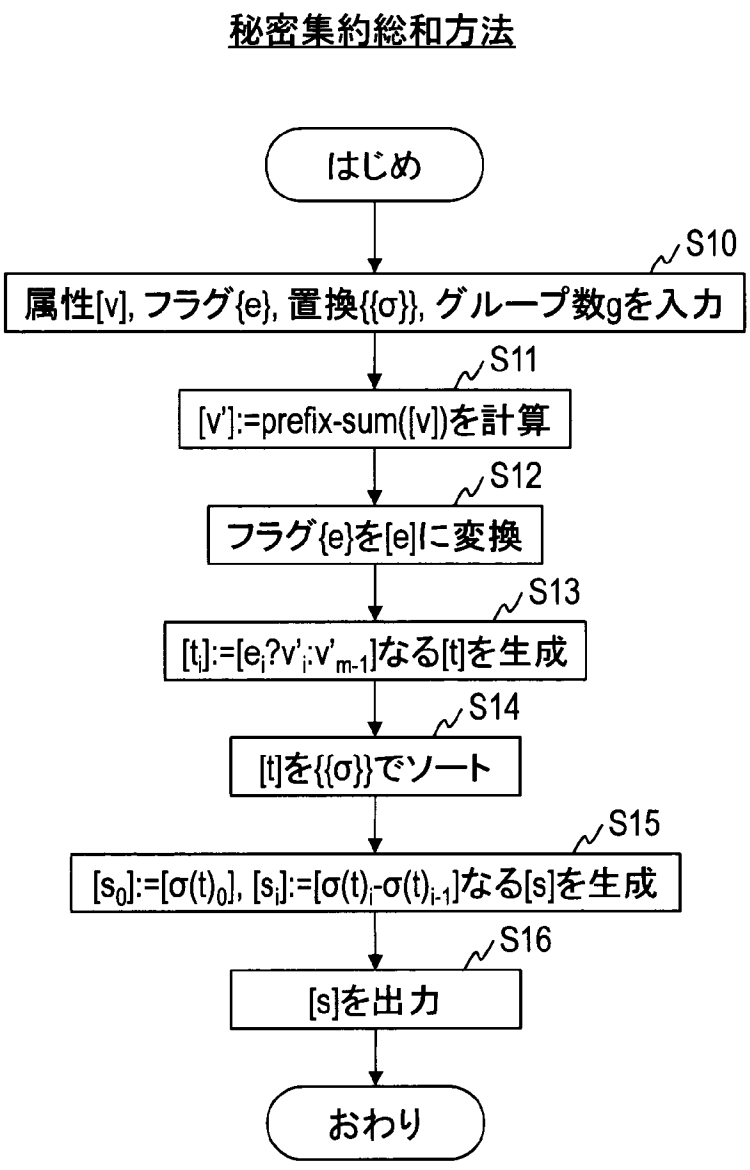

秘密集約総和方法
はじめ
S10
属性[v], フラグ{e}, 置換{{σ}}, グループ数gを入力
S11
[v']:=prefix-sum([v])を計算
S12
フラグ{e}を[e]に変換
S13
[t_i]:=[e_i?v'_i:v'_m-1]なる[t]を生成
S14
[t]を{{σ}}でソート
S15
[s_0]:=[σ(t)_0], [s_i]:=[σ(t)_i-σ(t)_i-1]なる[s]を生成
S16
[s]を出力
おわり

図3

[図4]

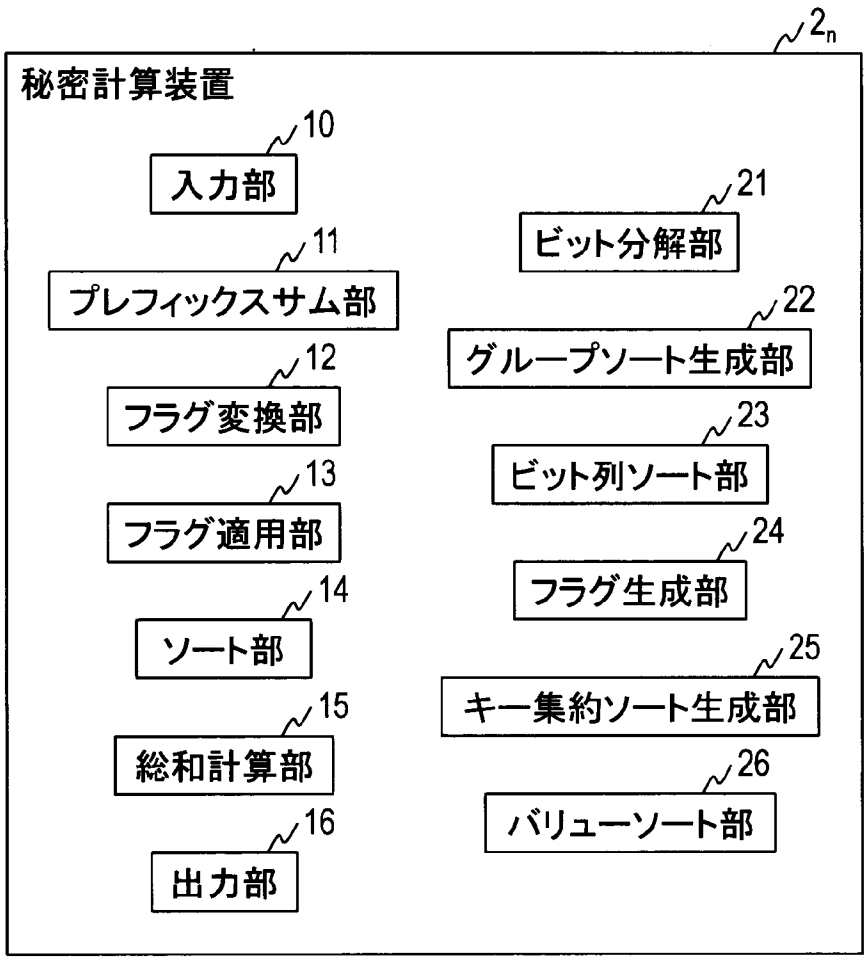

2n
秘密計算装置
10
入力部
11
プレフィックスサム部
12
フラグ変換部
13
フラグ適用部
14
ソート部
15
総和計算部
16
出力部
21
ビット分解部
22
グループソート生成部
23
ビット列ソート部
24
フラグ生成部
25
キー集約ソート生成部
26
バリューソート部

図4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/016985

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	JP 2012-154968 A (NIPPON TELEGRAPH AND TELEPHONE CORP.) 16 August 2012, paragraphs [0013]-[0020] (Family: none)	1-5
A	JP 2014-164144 A (NIPPON TELEGRAPH AND TELEPHONE CORP.) 08 September 2014, paragraphs [0034]-[0037] (Family: none)	1-5

☒ 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
04 July 2019 (04.07.2019)	16 July 2019 (16.07.2019)

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/JP2019/016985

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，秘密計算上の関係代数演算アルゴリズムの改良，電子情報通信学会技術研究報告，28 February 2013, vol. 112, no. 466, pp. 77-82, (HAMADA, Koki et al., "Improved Algorithms for Computing Relational Algebra Operators for Secure Function Evaluation", IEICE technical report)	1-5
A	濱田浩気ほか，実用的な速度で統計分析が可能な秘密計算システムMEVAL，コンピュータセキュリティシンポジウム2013論文集，14 October 2013, vol. 2013, no. 4, pp. 777-784, Symposium series of Information Processing Society of Japan, (HAMADA, Koki et al., "MEVAL: A Practically Efficient System for Secure Multi-Party Statistical Analysis", Proceedings of Computer Security Symposium 2013)	1-5

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／０１６９８５

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	JP 2012-154968 A（日本電信電話株式会社） 2012.08.16，段落 0013－0020 （ファミリーなし）	1-5
A	JP 2014-164144 A（日本電信電話株式会社） 2014.09.08，段落 0034－0037 （ファミリーなし）	1-5

☑　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
０４．０７．２０１９	１６．０７．２０１９

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　６３０４
行田　悦資
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，秘密計算上の関係代数演算アルゴリズムの改良，電子情報通信学会技術研究報告，2013.02.28，第112巻，第466号，p.77－82	1-5
A	濱田浩気ほか，実用的な速度で統計分析が可能な秘密計算システムＭＥＶＡＬ，コンピュータセキュリティシンポジウム２０１３論文集，2013.10.14，第2013巻，第4号，p.777－784，情報処理学会シンポジウムシリーズ	1-5