(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6973632号
(P6973632)
(45)発行日　令和3年12月1日(2021.12.1)　(24)登録日　令和3年11月8日(2021.11.8)

(51)Int.Cl.　F I
G09C 1/00 (2006.01)　G09C 1/00 650Z
G09C 1/00 660D

請求項の数 5　(全 11 頁)

(21)出願番号　特願2020-516336(P2020-516336)
(86)(22)出願日　平成31年4月22日(2019.4.22)
(86)国際出願番号　PCT/JP2019/016985
(87)国際公開番号　WO2019/208484
(87)国際公開日　令和1年10月31日(2019.10.31)
審査請求日　令和2年10月14日(2020.10.14)
(31)優先権主張番号　特願2018-84114(P2018-84114)
(32)優先日　平成30年4月25日(2018.4.25)
(33)優先権主張国・地域又は機関
日本国(JP)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町一丁目５番１号
(74)代理人　100121706
弁理士　中尾　直樹
(74)代理人　100128705
弁理士　中村　幸雄
(74)代理人　100147773
弁理士　義村　宗洋
(72)発明者　五十嵐　大
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内

審査官　行田　悦資

最終頁に続く

(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

(57)【特許請求の範囲】
【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、$[v]:=[v_0]$，…，$[v_{m-1}]$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$v':=v'_0$，…，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]:=[$\sigma(t)_i$-$\sigma(t)_{i-1}$]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{{σ_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{{σ_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{{σ}}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{{σ_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]:=[$\sigma(t)_i$-$\sigma(t)_{i-1}$]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、$\{\{\sigma\}\}$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$\{\{\sigma\}\}$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$\sigma(t)$となるシェア$[\sigma(t)]$を生成し、

上記秘密計算装置の総和計算部が、上記シェア$[\sigma(t)]$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$s:=s_0$，…，$s_{\min(g,m)-1}$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。

【発明の詳細な説明】

【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、$\{\{\sigma\}\}$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$t:=t_0$，…，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$\{\{\sigma\}\}$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$\sigma(t)$となるシェア$[\sigma(t)]$を生成するソート部と、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$s:=s_0$，…，$s_{\min(g,m)-1}$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0(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≦n≦N）が他の秘密計算装置$1_{n'}$（n'=1，…，N、ただしn≠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∈F^mを秘密分散により秘匿したシェア[v]∈$[F]^m$と、フラグe∈B^mを秘密分散により秘匿したシェア{e}∈$\{B\}^m$と、置換σを秘密分散により秘匿したシェア{{σ}}∈{{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{{σ}}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，…，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$\{e\}\in\{B\}^m$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$\{\{\sigma\}\}$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$_i$]:=[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s:=s_0，…，$s_{min(g,m)-1}$∈Fとなるシェア[s]∈[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σ(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，…，k_{nk-1}∈F^mそれぞれを秘密分散により秘匿したシェア[k_0]，…，[k_{nk-1}]∈[F]^{m}と、n_a個のバリュー属性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}:={$b'_i \neq b'_{i+1}$}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，…，$e_{m-1} \in B^m$となるシェア{e}∈{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'}∈{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{{σ}}∈{{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{{σ}}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{{σ}}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，…，v_{na-1}のシェア[v_0]，…，[v_{na-1}]と置換σ_0のシェア{{σ_0}}とを用いて、復元するとバリュー属性v_0，…，v_{na-1}を置換σ_0でソートしたソート済みバリュー属性v''_0，…，v''_{na-1}となるシェア[v''_0]，…，[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，…，v''_{na-1}のシェア[v''_0]，…，[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。

【図１】

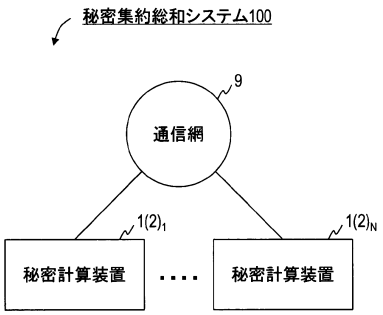

図1

【図２】

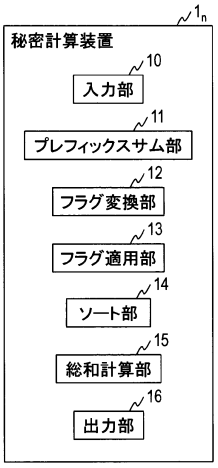

図2

【図３】

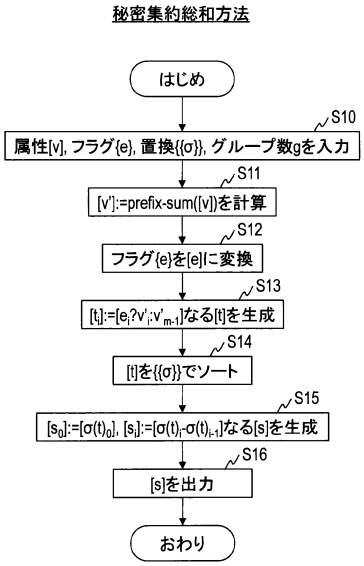
秘密集約総和方法
はじめ
S10
属性[v], フラグ{e}, 置換{{σ}}, グループ数gを入力
S11
[v']:=prefix-sum([v])を計算
S12
フラグ{e}を[e]に変換
S13
[t_i]:=[e_i?v'_i:v'_{m-1}]なる[t]を生成
S14
[t]を{{σ}}でソート
S15
[s_0]:=[σ(t)_0], [s_i]:=[σ(t)_i-σ(t)_{i-1}]なる[s]を生成
S16
[s]を出力
おわり

図3

【図４】

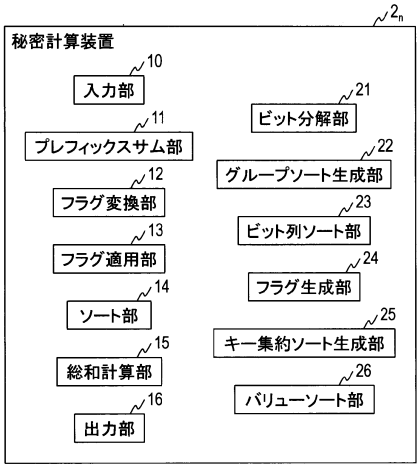
2n
秘密計算装置
10
入力部
11
プレフィックスサム部
12
フラグ変換部
13
フラグ適用部
14
ソート部
15
総和計算部
16
出力部
21
ビット分解部
22
グループソート生成部
23
ビット列ソート部
24
フラグ生成部
25
キー集約ソート生成部
26
バリューソート部

図4

フロントページの続き

(56)参考文献 特開２０１４－１６４１４４（ＪＰ，Ａ）
特開２０１２－１５４９６８（ＪＰ，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，日本，一般社団法人電子情報通信学会，2013年02月28日，第112巻，第466号，p.77－82
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，日本，一般社団法人情報処理学会，2013年10月14日，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

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　　１／００