(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
2021年9月30日(30.09.2021)

WIPO | PCT

(10) 国際公開番号
WO 2021/192006 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号： PCT/JP2020/012906

(22) 国際出願日： 2020年3月24日(24.03.2020)

(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 気 株 式 会 社 (**NEC CORPORATION**) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者: 土 田 光 (**TSUCHIDA, Hikaru**); 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

(74) 代理人: 加藤 朝道(**KATO, Asamichi**); 〒2220033 神奈川県横浜市港北区新横浜２丁目１７番１９号加藤内外特許事務所内 Kanagawa (JP).

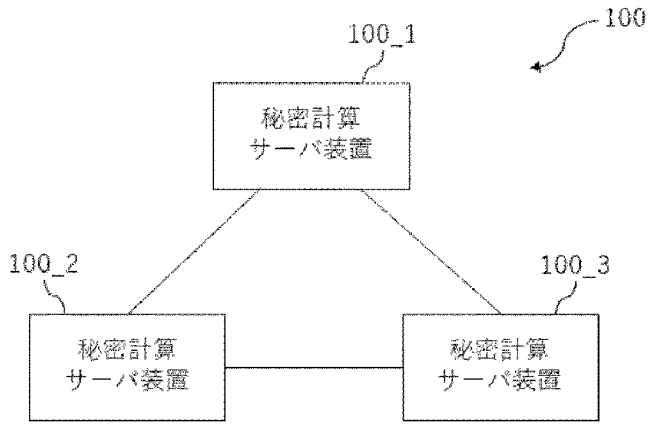
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, 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, 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,

WO 2021/192006 A1

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

(54) 発明の名称： 秘密計算システム、秘密計算サーバ装置、秘密計算方法および秘密計算プログラム



100_1, 100_2, 100_3... Secure computation server device

(57) **Abstract:** Each secure computation server device comprises: a bit decomposition operation unit that performs bit decomposition on a secret shared share value with a constant round number; a table operation unit that, using a table in which determination expressions determining whether or not equality holds in respective bits are arrayed in a row direction and combinations of determination expressions are arrayed in a column direction, determines whether or not equality holds in the respective bits of the bit decomposition; and an equality determination unit that determines an array reference corresponding to the share value by performing an equality determination on a value obtained by accumulating the results of whether or not equality holds in the respective bits of the bit decomposition with the constant round number.

［続葉有］

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)）

(57) 要約：秘密計算サーバ装置のそれぞれが、秘密分散されたシェア値を定数ラウンド数でビット分解を行うビット分解演算部と、各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、判定式の組み合わせを列方向に配列したテーブルを用いて、ビット分解の各ビットにおける等号の成否を判定するテーブル演算部と、ビット分解の各ビットにおける等号の成否を集積した値に対して定数ラウンド数で等号判定をすることで、シェア値に対応する配列参照を判定する等号判定部とを有する。

明　細　書

発明の名称 ：

秘密計算システム、秘密計算サーバ装置、秘密計算方法および秘密計算プログラム

技術分野

[0001] 本発明は、秘密計算システム、秘密計算サーバ装置、秘密計算方法および秘密計算プログラムに関するものである。

背景技術

[0002] 近年、秘密計算と呼ばれる技術の研究開発が盛んに行われている。秘密計算は、第三者に対して入力と計算過程の値を秘匿しつつ所定の処理を実行する技術の一つである。秘密計算における代表的な技術の一つとして、マルチパーティ計算技術が挙げられる。マルチパーティ計算技術では、秘匿するデータを複数のサーバ（秘密計算サーバ）に分散配置し、秘匿したまま当該データの任意の演算を実行する。以降、特に断りがない限り、本書で「秘密計算」という語を用いた場合は、マルチパーティ計算技術を意味するものとする。

[0003] 秘密計算の処理の一つとして、配列参照が存在する。配列参照とは、配列して格納された要素を参照するための処理であり、秘密計算における配列参照では、どこを参照するかのインデックスまでも秘匿することが要請されることがある。そして、このようなインデックスを秘匿する配列参照に用いるサブプロトコルとして、Ｄｅｍｕｘ（ｄｅｍｕｌｔｉｐｌｅｘｅｒ）プロトコルがある（例えば、非特許文献１参照）。秘密計算におけるＤｅｍｕｘプロトコルでは、秘匿されたインデックスを入力として、入力されたインデックスに対応した配列の要素のみが１であり、その他の要素は０であるような出力を秘匿したまま計算する処理である。

先行技術文献

非特許文献

[0004] 非特許文献1：J. Launchbury et al. Efficient Lookup-Table Protocol in Secure Multiparty Computation. In ICFP 2012.
非特許文献2：Catrina, Octavian. Round-efficient protocols for secure multiparty fixed-point arithmetic. 2018 International Conference on Communications (COMM). IEEE, 2018.

発明の概要

発明が解決しようとする課題

[0005] なお、上記先行技術文献の各開示を、本書に引用をもって繰り込むものとする。以下の分析は、本発明者らによってなされたものである。

[0006] ところで、マルチパーティ計算技術を用いる秘密計算では、秘匿するデータを複数のサーバに分散配置した状態で処理を行うので、処理の効率化という観点では、通信コストの低減が課題となる。そして、この通信コストは、通信の対象となるデータ量を表す通信量と、最大限の並列化を行った場合の通信の回数を表す通信ラウンド数に分解できる。

[0007] また、この通信量とラウンド数との間には、トレードオフの関係が成り立つことが多々ある一方、環境によっては通信量と通信ラウンド数のどちらを優先すべきかが異なることもある。例えば、ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）環境などの通信遅延が大きい環境では、通信回数が小さい方が有利であるので、通信ラウンド数が小さい秘密計算の方が好ましい。例えば、非特許文献１に開示されているＤｅｍｕｘプロトコルでは、通信ラウンド数が$O(\log_2 k)$であるので、通信ラウンド数が定数であるＤｅｍｕｘプロトコルを実現すると、通信遅延が大きい環境などでの通信コストを低減することができる。

[0008] 本発明の目的は、上述した課題を鑑み、通信ラウンド数を低減することに寄与する秘密計算システム、秘密計算サーバ装置、秘密計算方法および秘密計算プログラムを提供する。

課題を解決するための手段

[0009] 本発明の第１の視点では、相互にネットワークで接続した少なくとも３台

以上の秘密計算サーバ装置を備える秘密計算システムであって、前記秘密計算サーバ装置のそれぞれが、秘密分散されたシェア値を定数ラウンド数でビット分解を行うビット分解演算部と、各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、前記判定式の組み合わせを列方向に配列したテーブルを用いて、前記ビット分解の各ビットにおける等号の成否を判定するテーブル演算部と、前記ビット分解の各ビットにおける等号の成否を集積した値に対して定数ラウンド数で等号判定をすることで、前記シェア値に対応する配列参照を判定する等号判定部と、を有する、秘密計算システムが提供される。

[0010] 本発明の第２の視点では、相互にネットワークで接続した少なくとも３台以上の秘密計算サーバ装置の一つであって、秘密分散されたシェア値を定数ラウンド数でビット分解を行うビット分解演算部と、各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、前記判定式の組み合わせを列方向に配列したテーブルを用いて、前記ビット分解の各ビットにおける等号の成否を判定するテーブル演算部と、前記ビット分解の各ビットにおける等号の成否を集積した値に対して定数ラウンド数で等号判定をすることで、前記シェア値に対応する配列参照を判定する等号判定部と、を備える、秘密計算サーバ装置が提供される。

[0011] 本発明の第３の視点では、相互にネットワークで接続した少なくとも３台以上の秘密計算サーバ装置を用いる秘密計算方法であって、秘密分散されたシェア値を定数ラウンド数でビット分解を行い、各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、前記判定式の組み合わせを列方向に配列したテーブルを用いて、前記ビット分解の各ビットにおける等号の成否を判定し、前記ビット分解の各ビットにおける等号の成否を集積した値に対して定数ラウンド数で等号判定をすることで、前記シェア値に対応する配列参照を判定する、秘密計算方法が提供される。

[0012] 本発明の第４の視点では、相互にネットワークで接続した少なくとも３台以上の秘密計算サーバ装置に実行させる秘密計算プログラムであって、秘密

分散されたシェア値を定数ラウンド数でビット分解を行い、各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、前記判定式の組み合わせを列方向に配列したテーブルを用いて、前記ビット分解の各ビットにおける等号の成否を判定し、前記ビット分解の各ビットにおける等号の成否を集積した値に対して定数ラウンド数で等号判定をすることで、前記シェア値に対応する配列参照を判定する、秘密計算プログラムが提供される。

なお、このプログラムは、コンピュータが読み取り可能な記憶媒体に記録することができる。記憶媒体は、半導体メモリ、ハードディスク、磁気記録媒体、光記録媒体等の非トランジェント（non-transient）なものとすることができる。本発明は、コンピュータプログラム製品として具現することも可能である。

発明の効果

[0013] 本発明の各視点によれば、ラウンド数を低減することに寄与する秘密計算システム、秘密計算サーバ装置、秘密計算方法および秘密計算プログラムを提供することができる。

図面の簡単な説明

[0014] [図1]図１は、秘密計算システムの機能構成例を示すブロック図である。

[図2]図２は、秘密計算サーバ装置の機能構成例を示すブロック図である。

[図3]図３は、Ｄｅｍｕｘプロトコルに関する動作例を示すフローチャートである。

[図4]図４は、秘密計算サーバ装置のハードウェア構成例を示す図である。

[図5]図５は、決定木を例示する図である。

[図6]図６は、秘密計算システムの機能構成例を示すブロック図である。

[図7]図７は、秘密計算サーバ装置の機能構成例を示すブロック図である。

[図8]図８は、節点要素参照部の機能構成例を示すブロック図である。

[図9]図９は、節点要素の配列参照を例示する図である。

[図10]図１０は、経路計算部の機能構成例を示すブロック図である。

[図11]図１１は、決定木の経路計算とテーブルの関係を例示する図である。

発明を実施するための形態

[0015] 以下、図面を参照しながら、本発明の実施形態について説明する。ただし、以下に説明する実施形態により本発明が限定されるものではない。さらに、図面は模式的なものであり、各要素の寸法の関係、各要素の比率などは、現実のものとは異なる場合があることに留意する必要がある。図面の相互間においても、互いの寸法の関係や比率が異なる部分が含まれている場合がある。

[0016] ［準備］

以下、実施形態の説明にあたり、記法の定義および処理要素の説明を行う。以下で説明する記法および演算要素は、各実施形態の説明の中で共通して用いられる。

[0017] 体上で線形秘密分散されたxのシェアを[x]と表す。秘密分散されたシェア[x]とは、後述する秘密計算システムにおける各秘密計算サーバ装置が分散して保持する分散データ$[x]_i$のことであり、これら全ての分散データ$[x]_i$が揃って初めて秘匿された値xが復号できるものである。

[0018] 秘密計算とは、秘密分散されたシェアを入力として、秘匿された情報を秘匿されたまま処理を行う計算のことをいう。Ｄｅｍｕｘプロトコルでは、[x] s.t. $0 \leqq x < 2^k$という入力に対して、下式のように、xに対応した配列の要素のみが１であり、その他の要素は０であるような出力を秘匿したまま計算する処理である。

[0019] [数1]

$$\{[b_j]\}_{j=0}^{2^k-1} \ \text{s.t.} \ b_j = \begin{cases} 1 \ (j = x) \\ 0 \ (else) \end{cases} \quad \cdots (1)$$

[0020] また、以下で説明する実施形態では、ビルディングブロック（処理要素）として以下に示すプロトコルを用いる。

[0021] 〔等号判定〕

等号判定として、特に０との等号の成否を判定するプロトコルを用いる。容易に解るように、０ではない値との等号の成否も引き算と組み合わせるこ

とによって判定することが可能である。この等号判定を以下のように表す。

[0022] [数2]

$$[b] \leftarrow EQZ([x]) \quad \text{s.t.} \quad b = \begin{cases} 1 \ (x = 0) \\ 0 \ (else) \end{cases} \quad \cdots (2)$$

[0023] なお、等号判定の具体的処理は、例えば非特許文献２に記載の方法を用いることができる。非特許文献２に記載の等号判定は、通信ラウンド数が定数で抑えられる。しかしながら、通信ラウンド数が定数であれば、その他の適切な等号判定の処理を用いても本発明の効果に影響を及ぼすことはない。

[0024] 〔ビット分解〕

ビット分解とは、下式のように、[x] s.t. $0 \leqq x < 2^k$という入力に対して、これをビット表記した際の各桁を出力する処理である。

[0025] [数3]

$$\{[x_j]\}_{j=0}^{k-1} \leftarrow BD([x]) \quad \text{s.t.} \quad x = \sum_{j=0}^{k-1} 2^j \cdot x_j \quad \cdots (3)$$

[0026] なお、ビット分解の具体的処理は、例えば非特許文献２に記載の方法を用いることができる。非特許文献２に記載の等号判定は、通信ラウンド数が定数で抑えられる。しかしながら、通信ラウンド数が定数であれば、その他の適切なビット分解の処理を用いても本発明の効果に影響を及ぼすことはない。

[0027] ［第１の実施形態］

以下、図１、図２を参照して、本発明の第１の実施形態に係る秘密計算システムおよび秘密計算サーバ装置について説明する。

[0028] 図１は、第１の実施形態における秘密計算システムの機能構成例を示すブロック図である。図１に示すように、本発明の第１の実施形態による秘密計算システム１００は、第１の秘密計算サーバ装置１００_１と第２の秘密計算サーバ装置１００_２と第３の秘密計算サーバ装置１００_３とを備えている

。第１の秘密計算サーバ装置１００_１、第２の秘密計算サーバ装置１００_２、および第３の秘密計算サーバ装置１００_３は、それぞれが互いにネットワーク経由で通信可能に接続されている。

[0029] 図２は、秘密計算サーバ装置の機能構成例を示すブロック図である。図２に示される秘密計算サーバ装置１００_ｉ（ｉ＝１，２，３）は、第１の秘密計算サーバ装置１００_１、第２の秘密計算サーバ装置１００_２、および第３の秘密計算サーバ装置１００_３を代表して例示した機能構成例である。

[0030] 図２に示すように、秘密計算サーバ装置１００_ｉは、算術演算部１０１_ｉとシェア値記憶部１０２_ｉとを備えている。また、算術演算部１０１_ｉは、さらに、ビット分解演算部１０３_ｉとテーブル演算部１０４_ｉと等号判定部１０５_ｉとを含んでいる。これら算術演算部１０１_ｉ、シェア値記憶部１０２_ｉ、ビット分解演算部１０３_ｉ、テーブル演算部１０４_ｉ、および等号判定部１０５_ｉは、後に例示するハードウェア構成によって、メモリに記憶されたプログラムをプロセッサが実行することによって実現することが可能である。

[0031] 上記構成の第１～第３の秘密計算サーバ装置１００_ｉ（ｉ＝１，２，３）を備える秘密計算システム１００においては、第１～第３の秘密計算サーバ装置１００_ｉ（ｉ＝１、２、３）の内のいずれかの秘密計算サーバ装置１００_ｉが入力した値に対し、その入力や計算過程の値を知られることなく目的のシェアを計算し、これを第１～第３の秘密計算サーバ装置１００_ｉ（ｉ＝１，２，３）における各シェア値記憶部１０２_ｉに記憶することができる。

[0032] また、上記構成の第１～第３の秘密計算サーバ装置１００_ｉ（ｉ＝１，２，３）を備える秘密計算システム１００においては、第１～第３の秘密計算サーバ装置１００_ｉ（ｉ＝１，２，３）における各シェア値記憶部１０２_ｉに記憶されたシェアに対し、その計算過程の値を知られることなく目的のシェアを計算し、これを第１～第３の秘密計算サーバ装置１００_ｉ（ｉ＝１，２，３）における各シェア値記憶部１０２_ｉに記憶することができる。

[0033] なお、上記計算結果のシェアは、第１～第３の秘密計算サーバ装置１００_

１～１００_３とシェアを送受信することで、復元してもよい。あるいは、第１～第３の秘密計算サーバ装置１００_１～１００_３ではない外部にシェアを送信することで、復号してもよい。

[0034] ビット分解演算部１０３_ｉは、秘密分散されたシェア値を定数ラウンド数でビット分解を行う。テーブル演算部１０４_ｉは、各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、前記判定式の組み合わせを列方向に配列したテーブルを用いて、ビット分解演算部１０３_ｉの結果の各ビットにおける等号の成否を判定する。各ビットにおける等号の成否は、算術XORと算術NOTで行うことができるので、通信ラウンド数は定数で抑えられる。そして、等号判定部１０５_ｉは、ビット分解の各ビットにおける等号の成否を集積した値に対して定数ラウンド数で等号判定をすることで、入力したシェア値に対応する配列参照を判定する。

[0035] ここで算術XORとは、シェア[x],[y]に対し、[x xor y]を計算するという処理である。なお、x,yはでビットあることから、その値は0か1であり、$([x]-[y])^2 = [x \text{ xor } y]$が成り立つ。つまり、算術XORは、差の二乗を計算する処理に相当する。一方、算術NOTとは、シェア[x]に対し、[x xor 1]を計算するという処理であり、$([x]-1)^2 = [x \text{ xor } 1]$が成り立つ。つまり、算術NOTとは、入力から1を引いた値の二乗を計算する処理に相当する。

[0036] これらの性質を用いると、１ビットの等号判定は、次のように実行できる。シェア[x],[y]に対し、[x ?= y]を計算するという処理では、$(([x]-[y])^2 - 1)^2$を計算すればよい。つまり、[x]と[y]について，算術XORを行い，その結果に対し，算術NOTを行う。例えば、x=yの場合、算術XORの結果は[0]となり、その後の算術NOTによって[1]が出力される。一方、x≠yの場合、算術XORの結果は[1]となり、その後の算術NOTによって[0]が出力される。

[0037] 上記のように、ビット分解演算部１０３_ｉ、テーブル演算部１０４_ｉ、および等号判定部１０５_ｉは、通信ラウンド数が定数で抑えられる処理を行っているので、Ｄｅｍｕｘプロトコルの処理全体としても、通信ラウンド数が定数で抑えられる。すなわち、上記構成の秘密計算システム１００および

秘密計算サーバ装置１００_ｉ（ｉ＝１，２，３）は、Ｄｅｍｕｘプロトコルにおいて通信ラウンド数を低減することに寄与することができ、通信遅延が大きい環境などでの通信コストを低減することができる。

[0038] 次に、本発明の第１の実施形態における秘密計算方法について詳細に説明を行う。すなわち、上記説明した第１～第３の秘密計算サーバ装置１００_ｉ（ｉ＝１，２，３）を備える秘密計算システム１００の動作について説明する。図３は、Ｄｅｍｕｘプロトコルに関する動作例を示すフローチャートである。以下、各ステップを説明する。

[0039]（ステップＡ１）

秘密計算システム１００における第１～第３の秘密計算サーバ装置１００_ｉ（ｉ＝１，２，３）は、秘密分散されたシェア値を定数ラウンド数でビット分解を行う。ここで、秘密分散されたシェア値は、秘密計算システム１００の外部から入力された情報から計算されたシェア値であってもよく、また、第１～第３の秘密計算サーバ装置１００_ｉ（ｉ＝１，２，３）におけるシェア値記憶部１０２_ｉに既に秘密分散されて記憶しているシェア値であってもよい。

[0040] 具体的なビット分解の処理は、通信ラウンド数が定数で抑えられるものであれば適切に選択することが可能であるが、例えば先述したビルディングブロックのビット分解を用いることができる。

[0041]（ステップＡ２）

秘密計算システム１００における第１～第３の秘密計算サーバ装置１００_ｉ（ｉ＝１，２，３）は、各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、前記判定式の組み合わせを列方向に配列したテーブルを用意する。ここで用意するテーブルは、各第１～第３の秘密計算サーバ装置１００_ｉ（ｉ＝１，２，３）の記憶装置に既に記憶しておくことが可能な場合もあれば、ステップＡ１での入力に対応させて作成するとしてもよい。

[0042] 本ステップＡ２で用いるテーブルの具体的な形は以下のように例示するこ

とができる。なお、下記表の各要素における「?=」は等号が成立しているか否かを判定することを意味している。判定結果としては、等号が成立している場合に１を出力し、等号が成立していない場合に０を出力する。なお、既に指摘したように、各ビットにおける等号の成否は、算術XORと算術NOTで行うことができる。

[0043] [表1]

	k-1	k-2	k-3		2	1	0
0	$[x_{k-1}?=0]$	$[x_{k-1}?=0]$	$[x_{k-1}?=0]$	…	$[x_2?=0]$	$[x_1?=0]$	$[x_0?=0]$
1	$[x_{k-1}?=0]$	$[x_{k-1}?=0]$	$[x_{k-1}?=0]$	…	$[x_2?=0]$	$[x_1?=0]$	$[x_0?=1]$
2	$[x_{k-1}?=0]$	$[x_{k-1}?=0]$	$[x_{k-1}?=0]$	…	$[x_2?=0]$	$[x_1?=1]$	$[x_0?=0]$
3	$[x_{k-1}?=0]$	$[x_{k-1}?=0]$	$[x_{k-1}?=0]$	…	$[x_2?=0]$	$[x_1?=1]$	$[x_0?=1]$
	⋮	⋮	⋮		⋮	⋮	⋮
2^k-2	$[x_{k-1}?=1]$	$[x_{k-1}?=1]$	$[x_{k-1}?=1]$	…	$[x_2?=1]$	$[x_1?=1]$	$[x_0?=0]$
2^k-1	$[x_{k-1}?=1]$	$[x_{k-1}?=1]$	$[x_{k-1}?=1]$	…	$[x_2?=1]$	$[x_1?=1]$	$[x_0?=1]$

[0044] 上記テーブルは、先述の式（３）のビット分解の結果における各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列している。例えば、０番目の行は、式（３）のビット分解の結果におけるすべてのビットが０である場合にすべての判定式の出力が１となる。ビット分解の入力は、[x] s.t. $0 \leqq x < 2^k$であることから、判定式の組み合わせは2^k通りであり、入力が[x]である場合、x番目の行のみがすべての判定式の出力が１となる。

[0045] （ステップＡ３）

テーブル演算部１０４_ｉは、このようなテーブルを用いて、ビット分解演算部１０３_ｉの結果の各ビットにおける等号の成否を判定する。各ビットにおける等号の成否を判定は、行方向の配列（つまりベクトル）として出力される。このベクトルをrow_j $(0 \leqq j < 2^k)$と表記する。

[0046] （ステップＡ４）

秘密計算システム１００における第１～第３の秘密計算サーバ装置１００_ｉ（ｉ＝１，２，３）は、ビット分解の各ビットにおける等号の成否を集積する。具体的には、ステップＡ２の結果であるrow_j $(0 \leqq j < 2^k)$と(1,...,1)の内積を計算することで集積する。ベクトル(1,...,1)との内積を計算すること

で、row_jに含まれている１の数を集積することが可能である。これを$0 \leqq j < 2^k$となるjについて行い、結果を$[res_j]$とする。なお、この内積の計算も通信ラウンド数が定数で抑えられる。

[0047] [数4]

$$[res_j] \leftarrow InnerProduct(\vec{1} = (1, \ldots, 1),\ row_j) \text{ for } j = 0, \ldots, 2^k - 1 \quad \cdots (4)$$

[0048] （ステップＡ５）

秘密計算システム１００における第１～第３の秘密計算サーバ装置１００_ｉ（ｉ＝１，２，３）は、上記のように集積した値に対して定数ラウンド数で等号判定をすることで、入力されたシェア値に対応する配列参照を判定する。具体的な等号判定の処理は、通信ラウンド数が定数で抑えられるものであれば適切に選択することが可能であるが、例えば先述したビルディングブロックの等号判定を用いることができる。すなわち、下式のような等号判定を行えば、x番目のビットのみ１となり、それ以外が０となる配列b_jが得られる。

[0049] [数5]

$$\text{Return } \{[b_j] \leftarrow EQZ([res_j] - k)\}_{j=0}^{k-1}$$

[0050] 上記秘密計算方法では、すべてのステップで通信ラウンド数が定数で抑えられる処理を行っているので、Ｄｅｍｕｘプロトコルの処理全体としても、通信ラウンド数が定数で抑えられる。すなわち、上記秘密計算方法は、Ｄｅｍｕｘプロトコルにおいて通信ラウンド数を低減することに寄与することができ、通信遅延が大きい環境などでの通信コストを低減することができる。

[0051] ［ハードウェア構成例］

図４は、秘密計算サーバ装置のハードウェア構成例を示す図である。すなわち、図４に示すハードウェア構成例は、秘密計算サーバ装置１００_ｉ，２００_ｉ，３００_ｉ（ｉ＝１，２，３）のハードウェア構成例である。図４に示すハードウェア構成を採用した情報処理装置（コンピュータ）は、上記

説明した秘密計算方法をプログラムとして実行することで、秘密計算サーバ装置１００_ｉ，２００_ｉ，３００_ｉの各機能を実現することを可能にする。

[0052] ただし、図４に示すハードウェア構成例は、秘密計算サーバ装置１００_ｉ，２００_ｉ，３００_ｉ（ｉ＝１，２，３）の各機能を実現するハードウェア構成の一例であり、秘密計算サーバ装置１００_ｉ，２００_ｉ，３００_ｉ（ｉ＝１，２，３）のハードウェア構成を限定する趣旨ではない。秘密計算サーバ装置１００_ｉ，２００_ｉ，３００_ｉ（ｉ＝１，２，３）は、図４に示さないハードウェアを含むことができる。

[0053] 図４に示すように、秘密計算サーバ装置１００_ｉ，２００_ｉ，３００_ｉ（ｉ＝１，２，３）が採用し得るハードウェア構成１０は、例えば内部バスにより相互に接続される、ＣＰＵ（Central Processing Unit）１１、主記憶装置１２、補助記憶装置１３、およびＩＦ（Interface）部１４を備える。

[0054] ＣＰＵ１１は、秘密計算サーバ装置１００_ｉ，２００_ｉ，３００_ｉ（ｉ＝１，２，３）が実行する秘密計算プログラムに含まれる各指令を実行する。主記憶装置１２は、例えばＲＡＭ（Random Access Memory）であり、秘密計算サーバ装置１００_ｉ，２００_ｉ，３００_ｉ（ｉ＝１，２，３）が実行する秘密計算プログラムなどの各種プログラムなどをＣＰＵ１１が処理するために一時記憶する。

[0055] 補助記憶装置１３は、例えば、ＨＤＤ（Hard Disk Drive）であり、秘密計算サーバ装置１００_ｉ，２００_ｉ，３００_ｉ（ｉ＝１，２，３）が実行する秘密計算プログラムなどの各種プログラムなどを中長期的に記憶しておくことが可能である。秘密計算プログラムなどの各種プログラムは、非一時的なコンピュータ可読記録媒体（non-transitory computer-readable storage medium）に記録されたプログラム製品として提供することができる。補助記憶装置１３は、非一時的なコンピュータ可読記録媒体に記録された秘密計算プログラムなどの各種プログラムを中長期的に記憶することに利用することが可能である。

[0056] ＩＦ部１４は、秘密計算サーバ装置１００_ｉ，２００_ｉ，３００_ｉ（ｉ＝１，２，３）間の入出力に関するインターフェイスを提供する。ＩＦ部１４は、ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）などの通信遅延が大きいネットワークに接続されることもある。

[0057] 上記のようなハードウェア構成１０を採用した情報処理装置は、先述した秘密計算方法をプログラムとして実行することで、秘密計算サーバ装置１００_ｉ，２００_ｉ，３００_ｉ（ｉ＝１，２，３）の各機能を実現できる。

[0058] ［第２の実施形態］

以下、図５から図１１を参照して、本発明の第２の実施形態に係る秘密計算システムおよび秘密計算サーバ装置について説明する。本発明の第２の実施形態に係る秘密計算システムおよび秘密計算サーバ装置は、図５に例示するような決定木の計算に対して本発明の実施を適用した実施形態である。

[0059] 図５に例示するように、決定木は節点と枝から構成されている。決定木を用いた計算では、節点での判定に用いる要素を参照する処理と、各節点において分岐を判定する処理と、各分岐をどのように辿ったかの経路を計算する処理とを含む。秘密計算を用いた決定木の計算では、これらすべての計算を秘匿された状態で行う。

[0060] 図６は、第２の実施形態における秘密計算システムの機能構成例を示すブロック図である。図６に示すように、本発明の第２の実施形態による秘密計算システム２００は、第１の秘密計算サーバ装置２００_１と第２の秘密計算サーバ装置２００_２と第３の秘密計算サーバ装置２００_３とを備えている。第１の秘密計算サーバ装置２００_１、第２の秘密計算サーバ装置２００_２、および第３の秘密計算サーバ装置２００_３は、それぞれが互いにネットワーク経由で通信可能に接続されている。

[0061] 図７は、秘密計算サーバ装置の機能構成例を示すブロック図である。図７に示される秘密計算サーバ装置２００_ｉ（ｉ＝１，２，３）は、第１の秘密計算サーバ装置２００_１、第２の秘密計算サーバ装置２００_２、および第３の秘密計算サーバ装置２００_３を代表して例示した機能構成例である。

[0062] 図７に示すように、秘密計算サーバ装置２００_ｉは、算術演算部２０１_ｉとシェア値記憶部２０２_ｉとを備えている。また、算術演算部２０１_ｉは、さらに、節点要素参照部２１０_ｉと節点判定部２２０_ｉと経路計算部２３０_ｉとを含んでいる。これら算術演算部２０１_ｉ、シェア値記憶部２０２_ｉ、節点要素参照部２１０_ｉ、節点判定部２２０_ｉ、および経路計算部２３０_ｉは、先述のハードウェア構成によって、メモリに記憶されたプログラムをプロセッサが実行することによって実現することが可能である。

[0063] 図８は、節点要素参照部の機能構成例を示すブロック図である。図８に示すように、節点要素参照部２１０_ｉは、ビット分解演算部２０３_ｉとテーブル演算部２０４_ｉと等号判定部２０５_ｉとを含んでいる。これらビット分解演算部２０３_ｉ、テーブル演算部２０４_ｉ、および等号判定部２０５_ｉも、先述のハードウェア構成によって、メモリに記憶されたプログラムをプロセッサが実行することによって実現することが可能である。

[0064] 図５に示したように、決定木を用いた計算では、各節点における判定に要素$a1,...,a_2^{\{k-1\}}$を用いる。これら要素$a1,...,a_2^{\{k-1\}}$は、図９に示すように、シェア値記憶部２０２_ｉに配列されて記憶されている。そこで、決定木を用いた計算では、要素$a1,...,a_2^{\{k-1\}}$を配列参照する必要があるが、この配列参照に対して第１の実施形態で説明したＤｅｍｕｘプロトコルを用いることができる。

[0065] つまり、ビット分解演算部２０３_ｉは、要素a_xのインデックスxを定数ラウンド数でビット分解を行う。テーブル演算部２０４_ｉは、各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、前記判定式の組み合わせを列方向に配列したテーブルを用いて、ビット分解演算部２０３_ｉの結果の各ビットにおける等号の成否を判定する。そして、等号判定部２０５_ｉは、ビット分解の各ビットにおける等号の成否を集積した値に対して定数ラウンド数で等号判定をすることで、要素a_xのインデックスxに対応する配列参照を判定する。

[0066] なお、節点要素参照部２１０_ｉによって得られた要素a_xは、節点判定部２

２０_ｉによってどちらの分岐に進むかが判定されるが、この処理は、例えば非特許文献２に記載の処理など、公知の処理を用いることにより通信ラウンド数が定数で抑えられる処理で行うことができる。

[0067] 図１０は、経路計算部の機能構成例を示すブロック図である。図１０に示すように、経路計算部２３０_ｉは、テーブル演算部２０６_ｉと等号判定部２０７_ｉとを含んでいる。これらテーブル演算部２０６_ｉおよび等号判定部２０７_ｉも、先述のハードウェア構成によって、メモリに記憶されたプログラムをプロセッサが実行することによって実現することが可能である。

[0068] 経路計算部２３０_ｉは、図１１に示すようにテーブルを用いて経路計算を行う。図１１は、決定木の経路計算とテーブルの関係を例示する図である。図１１に示すように、決定木の各節点で分岐された経路は、分岐判定をビットで表記し、決定木の深さをビット分解の桁であると考えると、第１の実施形態で説明したテーブルと同じものが作成できる。すなわち、経路計算部２３０_ｉが経路計算を行うために用いるテーブルは、各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、前記判定式の組み合わせを列方向に配列したテーブルである。

[0069] したがって、テーブル演算部２０６_ｉおよび等号判定部２０７_ｉは、第１の実施形態と同様に当該テーブルを用いて経路計算を行うことができる。経路計算部２３０_ｉの出力は、決定木を用いた計算の結果であり、決定木を用いて行われた判断ないし分析の結果を指し示す配列参照になる。

[0070] 上記のように、節点要素参照部２１０_ｉ、節点判定部２２０_ｉ、および経路計算部２３０_ｉは、通信ラウンド数が定数で抑えられる処理を行っているので、決定木を用いた処理全体としても、通信ラウンド数が定数で抑えられる。すなわち、上記構成の秘密計算システム１００および秘密計算サーバ装置１００_ｉ（ｉ＝１，２，３）は、決定木を用いた処理全体において通信ラウンド数を低減することに寄与することができ、通信遅延が大きい環境などでの通信コストを低減することができる。

[0071] 上記の実施形態の一部又は全部は、以下の付記のようにも記載され得るが

、以下には限られない。

［付記１］

相互にネットワークで接続した少なくとも３台以上の秘密計算サーバ装置を備える秘密計算システムであって、

前記秘密計算サーバ装置のそれぞれが、

秘密分散されたシェア値を定数ラウンド数でビット分解を行うビット分解演算部と、

各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、前記判定式の組み合わせを列方向に配列したテーブルを用いて、前記ビット分解の各ビットにおける等号の成否を判定するテーブル演算部と、

前記ビット分解の各ビットにおける等号の成否を集積した値に対して定数ラウンド数で等号判定をすることで、前記シェア値に対応する配列参照を判定する等号判定部と、

を有する、秘密計算システム。

［付記２］

前記ビット分解の各ビットにおける等号の成否を集積した値は、前記ビット分解の各ビットにおける等号の成否の結果と(1,...,1)との内積を計算することで得られる、付記１に記載の秘密計算システム。

［付記３］

前記等号判定部は、前記配列参照の候補に関して前記等号判定を繰り返すことで前記配列参照を判定する、付記１または付記２に記載の秘密計算システム。

［付記４］

前記テーブルにおける前記判定式は、前記秘密分散されたシェア値が[x]である場合、x番目の行のみがすべての判定式の出力が１となる、付記１から付記３のいずれか１つに記載の秘密計算システム。

［付記５］

前記テーブルは、Ｄｅｍｕｘプロトコルにおける入力のビット分解に対す

る判定式に関するものである、付記１から付記４のいずれか１つに記載の秘密計算システム。

［付記６］

前記テーブルは、決定木の節点における判定に用いる要素のインデックスのビット分解に対する判定式に関するものである、付記１から付記４のいずれか１つに記載の秘密計算システム。

［付記７］

前記テーブルは、決定木の分岐に対する判定式に関するものである、付記１から付記４のいずれか１つに記載の秘密計算システム。

［付記８］

相互にネットワークで接続した少なくとも３台以上の秘密計算サーバ装置の一つであって、

秘密分散されたシェア値を定数ラウンド数でビット分解を行うビット分解演算部と、

各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、前記判定式の組み合わせを列方向に配列したテーブルを用いて、前記ビット分解の各ビットにおける等号の成否を判定するテーブル演算部と、

前記ビット分解の各ビットにおける等号の成否を集積した値に対して定数ラウンド数で等号判定をすることで、前記シェア値に対応する配列参照を判定する等号判定部と、

を備える、秘密計算サーバ装置。

［付記９］

相互にネットワークで接続した少なくとも３台以上の秘密計算サーバ装置を用いる秘密計算方法であって、

秘密分散されたシェア値を定数ラウンド数でビット分解を行い、

各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、前記判定式の組み合わせを列方向に配列したテーブルを用いて、前記ビット分解の各ビットにおける等号の成否を判定し、

前記ビット分解の各ビットにおける等号の成否を集積した値に対して定数ラウンド数で等号判定をすることで、前記シェア値に対応する配列参照を判定する、秘密計算方法。

［付記１０］

相互にネットワークで接続した少なくとも３台以上の秘密計算サーバ装置に実行させる秘密計算プログラムであって、

秘密分散されたシェア値を定数ラウンド数でビット分解を行い、

各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、前記判定式の組み合わせを列方向に配列したテーブルを用いて、前記ビット分解の各ビットにおける等号の成否を判定し、

前記ビット分解の各ビットにおける等号の成否を集積した値に対して定数ラウンド数で等号判定をすることで、前記シェア値に対応する配列参照を判定する、秘密計算プログラム。

[0072] なお、引用した上記の非特許文献等の各開示は、本書に引用をもって繰り込むものとする。本発明の全開示（請求の範囲を含む）の枠内において、さらにその基本的技術思想に基づいて、実施形態ないし実施例の変更・調整が可能である。また、本発明の全開示の枠内において種々の開示要素（各請求項の各要素、各実施形態ないし実施例の各要素、各図面の各要素等を含む）の多様な組み合わせ、ないし、選択（部分的削除を含む）が可能である。すなわち、本発明は、請求の範囲を含む全開示、技術的思想にしたがって当業者であればなし得るであろう各種変形、修正を含むことは勿論である。特に、本書に記載した数値範囲については、当該範囲内に含まれる任意の数値ないし小範囲が、別段の記載のない場合でも具体的に記載されているものと解釈されるべきである。さらに、上記引用した文献の各開示事項は、必要に応じ、本発明の趣旨に則り、本発明の開示の一部として、その一部又は全部を、本書の記載事項と組み合わせて用いることも、本願の開示事項に含まれるものと、みなされる。

符号の説明

[0073] １００，２００　秘密計算システム

１００_ｉ，２００_ｉ　秘密計算サーバ装置

１０１_ｉ，２０１_ｉ　算術演算部

１０２_ｉ，２０２_ｉ　シェア値記憶部

１０３_ｉ，２０３_ｉ　ビット分解演算部

１０４_ｉ，２０４_ｉ，２０６_ｉ　テーブル演算部

１０５_ｉ，２０５_ｉ，２０７_ｉ　等号判定部

請求の範囲

[請求項1] 相互にネットワークで接続した少なくとも３台以上の秘密計算サーバ装置を備える秘密計算システムであって、

前記秘密計算サーバ装置のそれぞれが、

秘密分散されたシェア値を定数ラウンド数でビット分解を行うビット分解演算部と、

各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、前記判定式の組み合わせを列方向に配列したテーブルを用いて、前記ビット分解の各ビットにおける等号の成否を判定するテーブル演算部と、

前記ビット分解の各ビットにおける等号の成否を集積した値に対して定数ラウンド数で等号判定をすることで、前記シェア値に対応する配列参照を判定する等号判定部と、

を有する、秘密計算システム。

[請求項2] 前記ビット分解の各ビットにおける等号の成否を集積した値は、前記ビット分解の各ビットにおける等号の成否の結果と(1,...,1)との内積を計算することで得られる、請求項１に記載の秘密計算システム。

[請求項3] 前記等号判定部は、前記配列参照の候補に関して前記等号判定を繰り返すことで前記配列参照を判定する、請求項１または請求項２に記載の秘密計算システム。

[請求項4] 前記テーブルにおける前記判定式は、前記秘密分散されたシェア値が[x]である場合、x番目の行のみがすべての判定式の出力が１となる、請求項１から請求項３のいずれか１つに記載の秘密計算システム。

[請求項5] 前記テーブルは、Ｄｅｍｕｘプロトコルにおける入力のビット分解に対する判定式に関するものである、請求項１から請求項４のいずれか１つに記載の秘密計算システム。

[請求項6] 前記テーブルは、決定木の節点における判定に用いる要素のインデ

ックスのビット分解に対する判定式に関するものである、請求項１から請求項４のいずれか１つに記載の秘密計算システム。

[請求項7] 前記テーブルは、決定木の分岐に対する判定式に関するものである、請求項１から請求項４のいずれか１つに記載の秘密計算システム。

[請求項8] 相互にネットワークで接続した少なくとも３台以上の秘密計算サーバ装置の一つであって、

秘密分散されたシェア値を定数ラウンド数でビット分解を行うビット分解演算部と、

各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、前記判定式の組み合わせを列方向に配列したテーブルを用いて、前記ビット分解の各ビットにおける等号の成否を判定するテーブル演算部と、

前記ビット分解の各ビットにおける等号の成否を集積した値に対して定数ラウンド数で等号判定をすることで、前記シェア値に対応する配列参照を判定する等号判定部と、

を備える、秘密計算サーバ装置。

[請求項9] 相互にネットワークで接続した少なくとも３台以上の秘密計算サーバ装置を用いる秘密計算方法であって、

秘密分散されたシェア値を定数ラウンド数でビット分解を行い、

各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、前記判定式の組み合わせを列方向に配列したテーブルを用いて、前記ビット分解の各ビットにおける等号の成否を判定し、

前記ビット分解の各ビットにおける等号の成否を集積した値に対して定数ラウンド数で等号判定をすることで、前記シェア値に対応する配列参照を判定する、秘密計算方法。

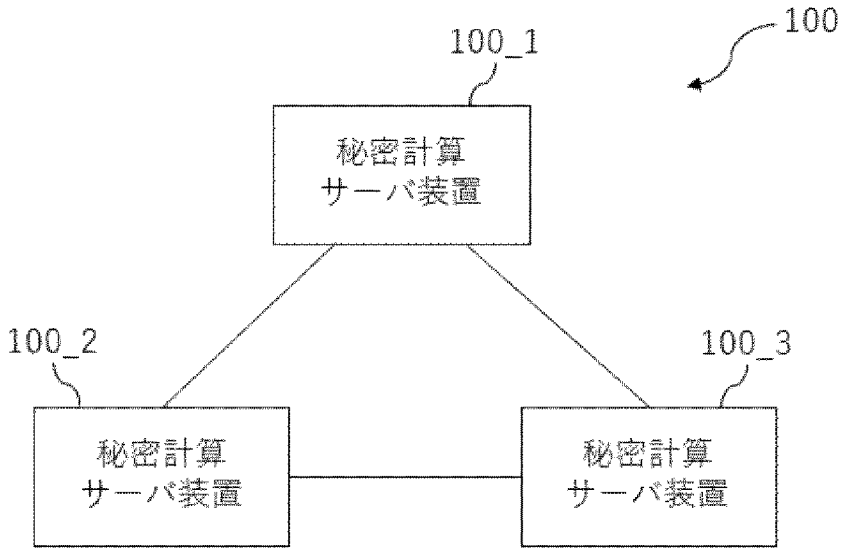
[請求項10] 相互にネットワークで接続した少なくとも３台以上の秘密計算サーバ装置に実行させる秘密計算プログラムであって、

秘密分散されたシェア値を定数ラウンド数でビット分解を行い、

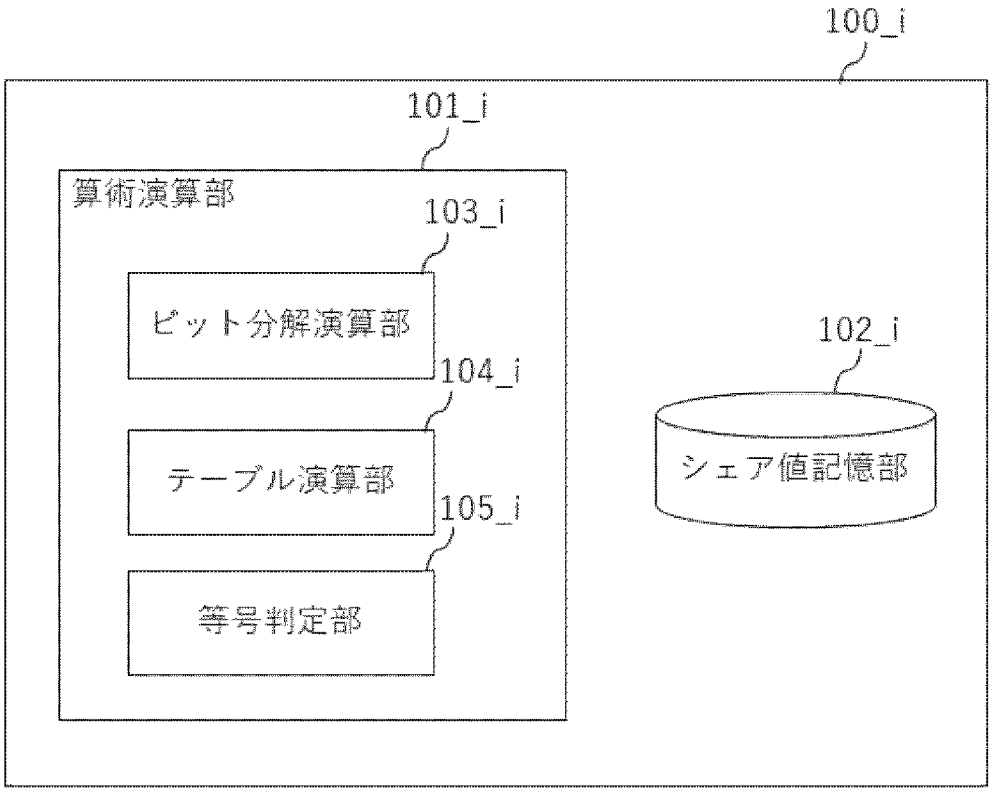
各ビットにおいて等号が成立するか否かを判定する判定式を行方向に配列し、前記判定式の組み合わせを列方向に配列したテーブルを用いて、前記ビット分解の各ビットにおける等号の成否を判定し、

前記ビット分解の各ビットにおける等号の成否を集積した値に対して定数ラウンド数で等号判定をすることで、前記シェア値に対応する配列参照を判定する、秘密計算プログラム。

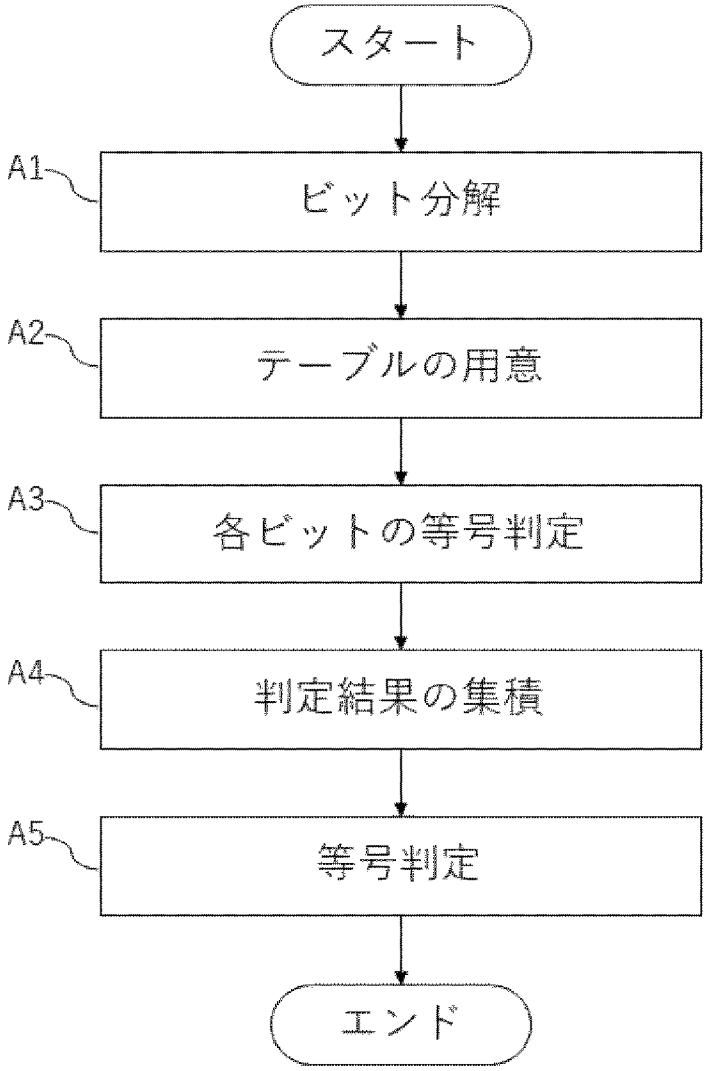
[図1]



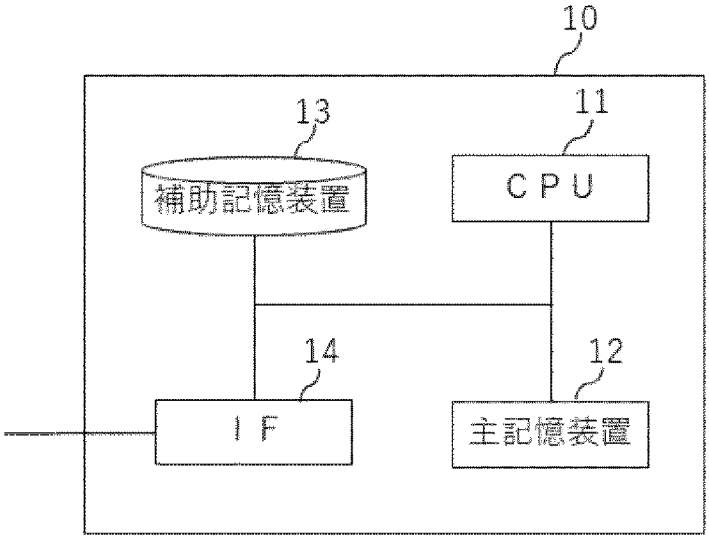
[図2]


100_i
101_i
算術演算部
103_i
ビット分解演算部
104_i
テーブル演算部
105_i
等号判定部
102_i
シェア値記憶部

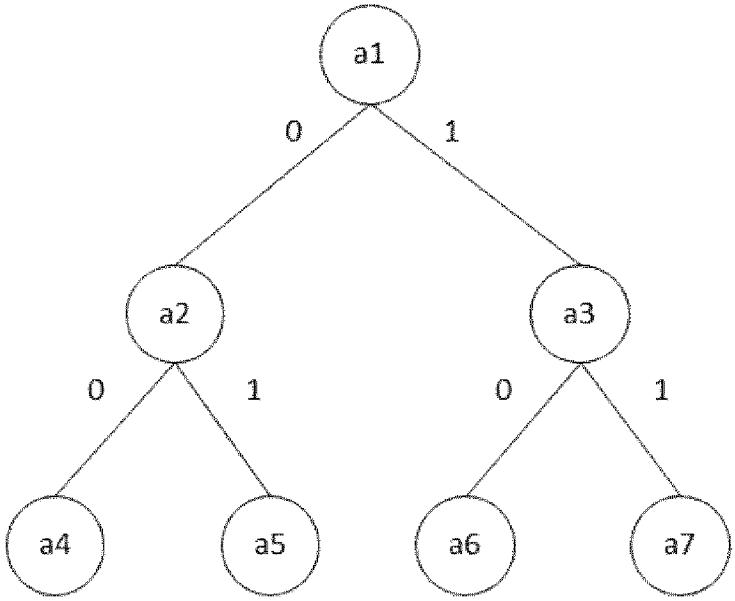
[図3]



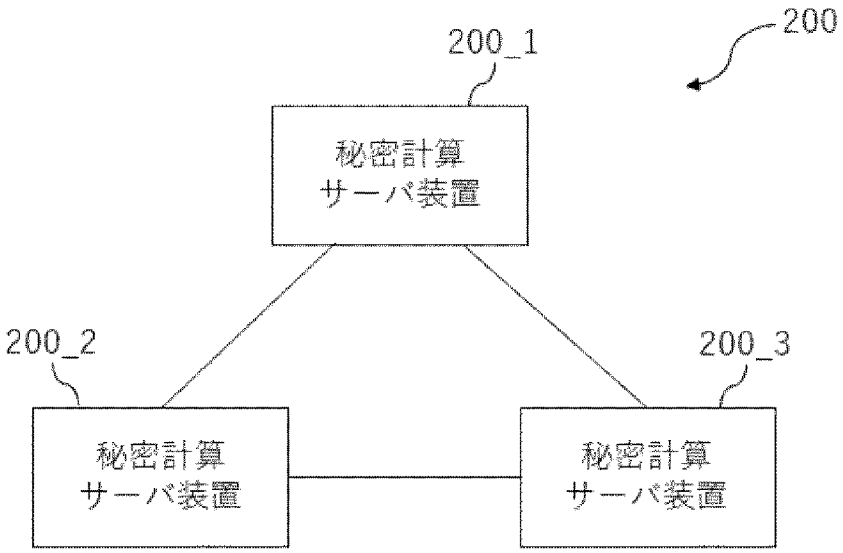
[図4]



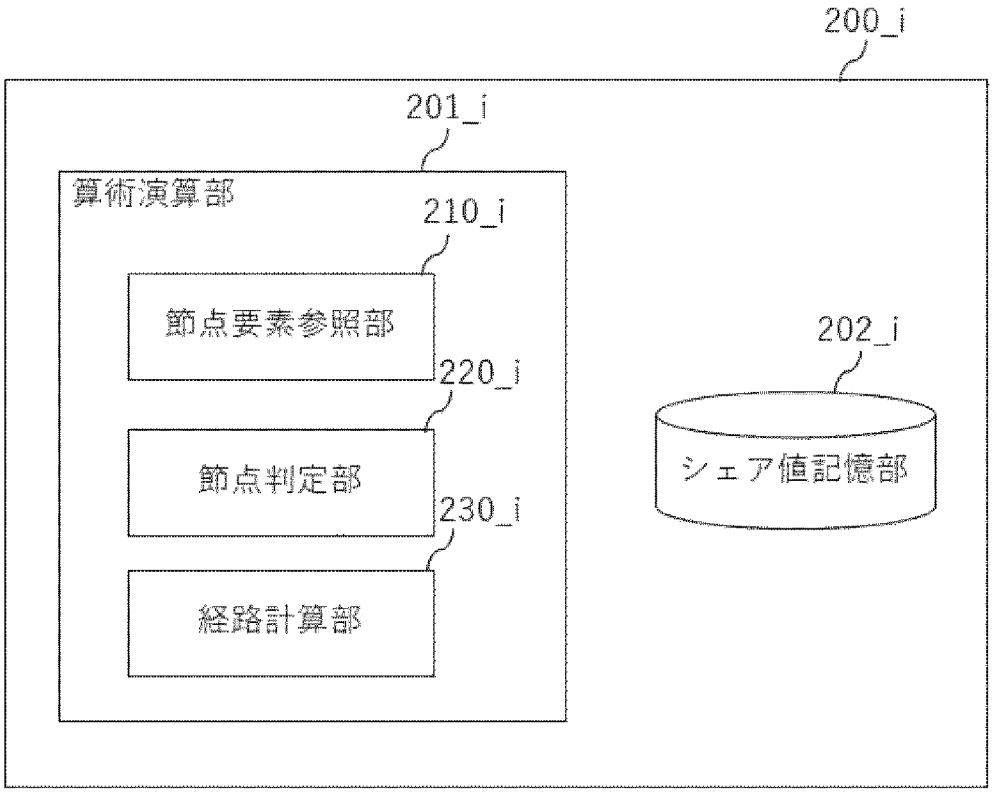
[図5]



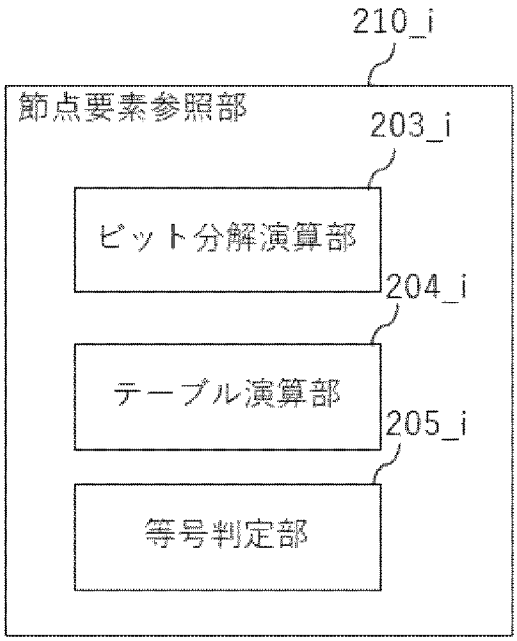
[図6]



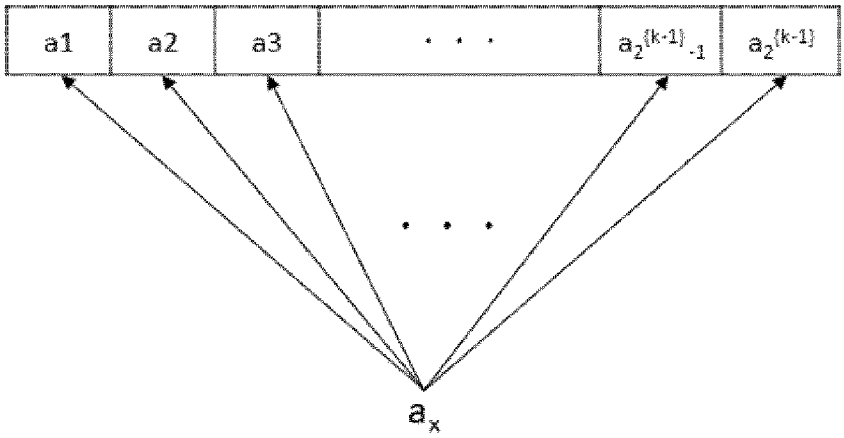
[図7]


200_i
201_i
算術演算部
210_i
節点要素参照部
220_i
節点判定部
230_i
経路計算部
202_i
シェア値記憶部

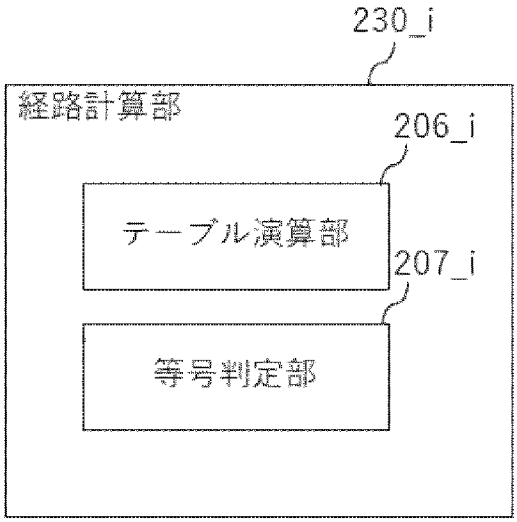
[図8]



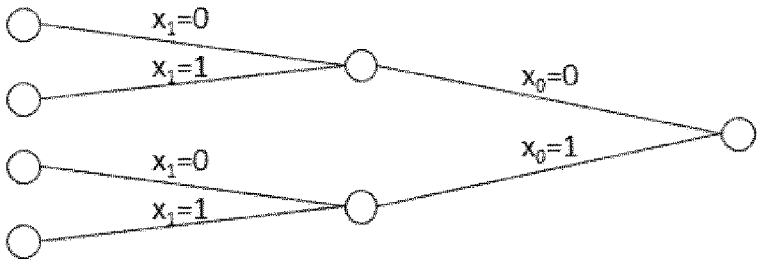
[図9]



[図10]



[図11]



Path1	[x_1?=0]	[x_0?=0]
Path2	[x_1?=0]	[x_0?=1]
Path3	[x_1?=1]	[x_0?=0]
Path4	[x_1?=1]	[x_0?=1]

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/012906

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	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

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	LAUNCHBURY, John et al., "Application-Scale Secure Multiparty Computation", Lecture Notes in Computer Science, 2014, vol. 8410, pp. 8-26, in particular 4.2(pp. 20-23)	1-10
A	KELLER, Marcel et al., "Faster Secure Multi-Party Computation of AES and DES Using Lookup Tables", Cryptology ePrint Archive [online], May 2017, Report 2017/378, Ver. 20170501:134527, pp. 1-26, [retrieved on 03 September 2020], Retrieved from the Internet:<URL:https://eprint.iacr.org/2017/378/20170501:134527>, in particular 4.3(pp. 12-14)	1-10
A	KELLER, Marcel et al., "Efficient, Oblivious Data Structures for MPG", Cryptology ePrint Archive [online], August 2014, Report 2014/137, Ver. 20140815:182750, pp. 1-31, [retrieved on 03 September 2020], Retrieved from the Internet:<URL:https://eprint.iacr.org/2014/137/20140815:182750>, in particular 2.1(page 4), 3.1(page 6), protocol 2(page 17), protocol 7(page 19)	1-10

☐ 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
03 September 2020 (03.09.2020)	15 September 2020 (15.09.2020)

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

国際調査報告

国際出願番号
PCT/JP2020/012906

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	１９７１－２０２０年
日本国実用新案登録公報	１９９６－２０２０年
日本国登録実用新案公報	１９９４－２０２０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	LAUNCHBURY, John et al., Application-Scale Secure Multiparty Computation, Lecture Notes in Computer Science, 2014, vol. 8410, pp. 8-26 特に4.2(pp.20-23)	1-10
A	KELLER, Marcel et al., Faster Secure Multi-Party Computation of AES and DES Using Lookup Tables, Cryptology ePrint Archive [online], 2017.05, Report 2017/378, Ver. 20170501:134527, pp. 1-26, [retrieved on 2020.09.03], Retrieved from the Internet: <URL: https://eprint.iacr.org/2017/378/20170501:134527> 特に4.3(pp.12-14)	1-10
A	KELLER, Marcel et al., Efficient, Oblivious Data Structures for MPC, Cryptology ePrint Archive [online], 2014.08, Report 2014/137, Ver. 20140815:182750, pp. 1-31, [retrieved on 2020.09.03], Retrieved from the Internet: <URL: https://eprint.iacr.org/2014/137/20140815:182750> 特に2.1(p.4), 3.1(p.6), Protocol 2(p.17)及びProtocol 7(p.19)	1-10

☐ 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
03.09.2020	15.09.2020

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）
金沢　史明 5S 4538

電話番号 03-3581-1101 内線 3546