(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
2015 年 7 月 23 日(23.07.2015)

WIPO | PCT

(10) 国際公開番号
WO 2015/107952 A1

(51) 国際特許分類:
G09C 1/00 (2006.01) *G06F 21/60* (2013.01)

(21) 国際出願番号: PCT/JP2015/050231

(22) 国際出願日: 2015 年 1 月 7 日(07.01.2015)

(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 2014-006694 2014 年 1 月 17 日(17.01.2014) 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). 濱田 浩気(HAMADA, Koki); 〒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). 菊池 亮(KIKUCHI, Ryo); 〒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). 千田 浩司(CHIDA, Koji); 〒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４階 Tokyo (JP).

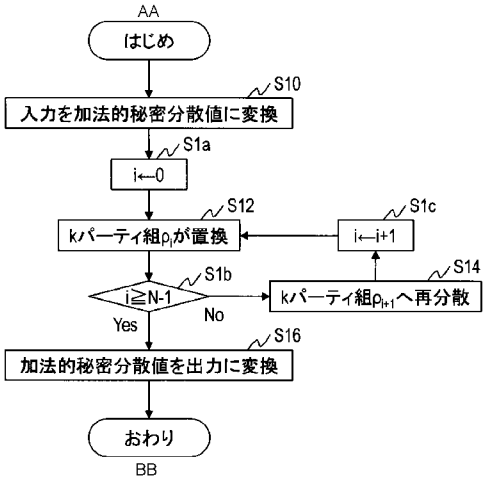
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[続葉有]

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

(54) 発明の名称 : 秘密計算方法、秘密計算システム、ランダム置換装置及びプログラム

[図3]



AA... START
S10... CONVERT INPUT TO ADDITIVE SECURE DISPERSION VALUE
S12... SUBSTITUTE BY k PARTY GROUP (ρ_i)
S14... REDISPERSION TO K PARTY GROUP (ρ_{i+1})
S16... CONVERT ADDITIVE SECURE DISPERSION VALUE TO OUTPUT
BB... END

(57) **Abstract**: The purpose of the present invention is to carry out secure computation that includes secure random substitution at high speed. In a unit substitution step (S12), random substitution devices (p_0, … , p_{k-1}) make substitution of an additive secure dispersion value ($<<a>>^{\rho i}$) for plain text (a) using substitution data (π) sub share ($\pi_{\rho i}$). In a redispersion step (S14) the random substitution device (p_0) generates an additive secure dispersion value ($<<a>>^{\rho i+1}{}_{pk}$) using random numbers (r_1, …, r_{k-1}) shared with each of random substitution devices (p_j) (j = 1, …, k-1) and sends the same to the random substitution device (p_k). Each of the random substitution devices (p_j) generates an additive secure dispersion value ($<<a>>^{\rho i+1}{}_{pj}$) using a random number (r_j).

(57) 要約: 秘密ランダム置換が含まれる秘密計算を高速に行う。単位置換ステップＳ１２は、ランダム置換装置 $p_0,\ldots,p_{k-1}$ が、平文 a の加法的秘密分散値 $\ll a\gg^{\rho i}$ を置換データ π のサブシェア $\pi_{\rho i}$ により置換する。再分散ステップＳ１４は、ランダム置換装置 p_0 が、ランダム置換装置 p_j (j=1,…,k-1) それぞれと共有する乱数 $r_1,\ldots,r_{k-1}$ を用いて加法的秘密分散値 $\ll a\gg^{\rho i+1}{}_{pk}$ を生成してランダム置換装置 p_k へ送信し、ランダム置換装置 p_j それぞれが乱数 r_j を用いて加法的秘密分散値 $\ll a\gg^{\rho i+1}{}_{pj}$ を生成する。

WO 2015/107952 A1

(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:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ：

秘密計算方法、秘密計算システム、ランダム置換装置及びプログラム

技術分野

[0001] この発明は、秘密計算技術に関し、特に、秘密ランダム置換を行う技術に関する。

背景技術

[0002] 秘密計算とは、秘密分散によりデータを秘匿しつつデータ処理を行う技術である。秘密分散は、データを複数の分散値に変換し、一定個数以上の分散値を用いれば元のデータを復元でき、一定個数未満の分散値からは元のデータを一切復元できなくする技術である。秘密分散はいくつかの種類に分類でき、例えば、(k,n)-秘密分散、加法的秘密分散、置換データ秘密分散などがある。

[0003] (k,n)-秘密分散とは、入力された平文をn個のシェアに分割し、n個のパーティ$P=(p_0,\cdots,p_{n-1})$に分散しておき、任意のk個のシェアが揃えば平文を復元でき、k個未満のシェアからは平文に関する一切の情報を得られないような秘密分散である。(k,n)-秘密分散の具体的な方式には、例えば、Shamir秘密分散、複製秘密分散などがある。

[0004] 加法的秘密分散とは、複製秘密分散による(k,k)-秘密分散である。(k,k)-秘密分散とは、(k,n)-秘密分散において、n=kとした場合である。(k,k)-秘密分散では、全パーティのシェアが集まらない限り平文を復元することはできない。加法的秘密分散は、k個のシェアを加算するだけで平文が復元される最もシンプルな秘密分散である。

[0005] 置換データ秘密分散は、置換データを秘匿して行う秘密分散である。置換データとは、データ列を並び替えるときの並び替え方を表すデータである。m個のデータ列を並び替えるとき、大きさmの置換データπは全単射写像$\pi:N_m\rightarrow N_m$を表すデータである。ただし、任意の整数mに対して、N_mはm未満の非負整数

の集合である。例えば、ベクトル$\vec{x}\in(N_m)^m$で各要素が互いに異なるデータは大きさmのランダム置換データと見なせる。

[0006] より具体的には、ベクトル$\vec{x}=(3,0,2,1)$を大きさ4のランダム置換データと見なすことができる。例えば、データ列$\vec{y}=(1,5,7,10)$をベクトル$\vec{x}$によって並び替えるとする。データ列$\vec{y}$の0番目の要素である1を、ベクトル$\vec{x}$の0番目の要素が示す3番目に移動する。データ列$\vec{y}$の1番目の要素である5を、ベクトル$\vec{x}$の1番目の要素が示す0番目に移動する。同様に、7を2番目に移動し、10を1番目に移動する。結果として、置換後のデータ列$\vec{z}=(5,10,7,1)$が得られる。

[0007] 置換データ秘密分散は、以下の手順により置換データを秘匿する。N個のkパーティ組の列$P=\rho_0,\cdots,\rho_{N-1}$があるとする。例えば、k=2のとき、各kパーティ組ρ_iは、パーティp_0とパーティp_1の組(p_0,p_1)や、パーティp_0とパーティp_2の組(p_0,p_2)などである。各kパーティ組ρ_i内の全パーティが互いに置換データ$\pi_{\rho i}$を共有し、補集合$\bar{\rho}_i$には知らさないものとする。そして、対応する平文を$\pi_0(\pi_1(\cdots(\pi_{N-1}(I))\cdots))$とする。ただし、Iは入力と同じ並びでそのまま出力する置換、つまり恒等置換である。このとき、kパーティ組の列$P=\rho_0,\cdots,\rho_{N-1}$を、「（条件１）任意のk-1パーティ組$\rho$に対して、いずれかの補集合$\bar{\rho}_i$が$\rho\subseteq\bar{\rho}_i$を満たす」ように設定すれば、どのようにk-1パーティが結託しても、いずれかの置換データ$\pi_{\rho i}$を知らないことになる。

[0008] 例えば、パーティ数nが$n\geqq 2k-1$を満たすとき、kパーティ組の列Ｐをすべてのkパーティ組を含む集合とすれば上記の条件１を満たす。また、パーティ数nが$n>2k-1$を満たすときは、すべてのkパーティ組を含まなくても上記の条件１が実現されることがある。例えば、k=2, n=4のとき、$\{(p_0,p_1),(p_2,p_3)\}$はすべてのkパーティ組を含みはしないが条件１を満たす。

[0009] 秘密ランダム置換とは、どのような順番に置換したのかを処理実行者にもわからないように、入力されたデータ列をランダムに置換する技術である。秘密ランダム置換を行う従来技術として非特許文献１に記載の技術がある。

[0010] 非特許文献１に記載の秘密ランダム置換の基本形は、(k,n)-秘密分散値の

列[a→]を入力とし、置換データ秘密分散値<π>を生成し、(k,n)-秘密分散値の列[b→]=([$a_{\pi(0)}$],…,[$a_{\pi(m-1)}$])を出力する。このとき、置換データ秘密分散値<π>の平文π、つまりデータ列をどのような順序で入れ替えたのかがいずれのパーティにもわからないことが特徴である。具体的な処理としては、置換データ秘密分散の各サブシェア$\pi_{\rho i}$に対して、kパーティ集合ρ_iに属するパーティp∈ρ_iが秘密計算ではない通常の置換処理により、入力[a→]=([a_0],…,[a_{m-1}])から([$a_{\pi\rho i(0)}$],…,[$a_{\pi\rho i(m-1)}$])を生成し、これを再分散と呼ばれる処理により秘密分散し直すことを繰り返す。

[0011] 秘密ランダム置換は入出力の型の違いから以下の三種類が考えられる。一つ目は、入力も出力も(k,n)-秘密分散値である場合である。二つ目は、入力が(k,n)-秘密分散値であり、出力は公開値の場合である。三つ目は、入力が公開値であり、出力は(k,n)-秘密分散値の場合である。入力が公開値の場合、公開値を秘密分散して秘密分散値としてから上記の基本形の処理を行う。また、出力が公開値の場合、上記の基本形の処理を行った後に公開処理を行う。公開値とは全パーティが知っている値である。公開処理とは、例えば、全パーティが自身のシェアを他の全パーティに送信し、全パーティが受信したシェアから秘密分散の復元を行うことである。

先行技術文献

非特許文献

[0012] 非特許文献1：濱田浩気、五十嵐大、千田浩司、高橋克巳、“3パーティ秘匿関数計算のランダム置換プロトコル”、コンピュータセキュリティシンポジウム2010、2010年

発明の概要

発明が解決しようとする課題

[0013] 非特許文献１に記載の秘密ランダム置換は、(k,n)-秘密分散値を用いて置換と再分散の処理を繰り返す。(k,n)-秘密分散値を再分散するためには、各パーティが全パーティと相互に通信を行わなければならず、通信量及び通信

段数が大きいという問題がある。

[0014] この発明の目的は、秘密ランダム置換に要する通信量及び通信段数を低減し、秘密ランダム置換が含まれる秘密計算を高速に行うことである。

課題を解決するための手段

[0015] 上記の課題を解決するために、この発明の秘密計算方法は、n,kを2以上の整数とし、n>kとし、$N={}_nC_k$とし、ρをn台のランダム置換装置から選択したk台のランダム置換装置の組とし、$\rho_0,\cdots,\rho_{N-1}$はi=0,…,N-2について$|\rho_i \setminus \rho_{i+1}|=1$となるように構成されており、$\ll a \gg^{\rho i}$をi番目のランダム置換装置の組$\rho_i$が保持する平文aの加法的秘密分散値とし、$\ll a \gg^{\rho i}_p$を加法的秘密分散値$\ll a \gg^{\rho i}$のうちランダム置換装置pが保持する加法的秘密分散値とし、$\pi_{\rho i}$をi番目のランダム置換装置の組ρ_iに対応する置換データπのサブシェアとし、ランダム置換装置p_0をi番目のランダム置換装置の組ρ_iに含まれi+1番目のランダム置換装置の組ρ_{i+1}に含まれないランダム置換装置とし、ランダム置換装置p_kをi番目のランダム置換装置の組ρ_iに含まれずi+1番目のランダム置換装置の組ρ_{i+1}に含まれるランダム置換装置とし、ランダム置換装置p_j（j=1,…,k-1）をi番目のランダム置換装置の組ρ_i及びi+1番目のランダム置換装置の組ρ_{i+1}のいずれにも含まれるk-1台のランダム置換装置として、ランダム置換装置$p_0,\cdots,p_{k-1}$が、加法的秘密分散値$\ll a \gg^{\rho i}$をサブシェア$\pi_{\rho i}$により置換する単位置換ステップと、ランダム置換装置p_0が、ランダム置換装置$p_1,\cdots,p_{k-1}$と共有する乱数$r_1,\cdots,r_{k-1}$を用いて加法的秘密分散値$\ll a \gg^{\rho i+1}_{pk}$を生成してランダム置換装置$p_k$へ送信し、ランダム置換装置$p_j$それぞれが乱数$r_j$を用いて加法的秘密分散値$\ll a \gg^{\rho i+1}_{pj}$を生成する再分散ステップと、を含む。

発明の効果

[0016] この発明の秘密計算技術によれば、秘密ランダム置換を行う際の通信量及び通信段数を低減することができる。したがって、秘密ランダム置換が含まれる秘密計算を高速に実行できる。

図面の簡単な説明

[0017] [図1]図１は、秘密計算システムの機能構成を例示する図である。

[図2]図２は、第一実施形態のランダム置換装置の機能構成を例示する図である。

[図3]図３は、第一実施形態の秘密計算方法の処理フローを例示する図である。

[図4]図４は、第二実施形態の秘密計算方法の処理フローを例示する図である。

[図5]図５は、第三実施形態の秘密計算方法の処理フローを例示する図である。

[図6]図６は、第四実施形態のランダム置換装置の機能構成を例示する図である。

[図7]図７は、第四実施形態の秘密計算方法の処理フローを例示する図である。

[図8]図８は、第一実施形態におけるk=2, n=3の具体例を示す図である。

[図9]図９は、第一実施形態におけるk=3, n=5の具体例を示す図である。

[図10]図１０は、第二実施形態におけるk=2, n=3の具体例を示す図である。

[図11]図１１は、第二実施形態におけるk=3, n=5の具体例を示す図である。

[図12]図１２は、第三実施形態におけるk=2, n=3の具体例を示す図である。

[図13]図１３は、第三実施形態におけるk=3, n=5の具体例を示す図である。

発明を実施するための形態

[0018] 実施形態の説明に先立ち、この明細書で用いる表記方法及び用語を定義する。

［表記方法］

pは、シェアを所持するパーティを表す。

$P=(p_0, \cdots, p_{n-1})$は、シェアを所持するnパーティ全体の集合を表す。

$\rho=(p_0, \cdots, p_{k-1})$は、置換処理を実行するkパーティ組の集合を表す。

$P=(\rho_0, \cdots, \rho_{N-1})$は、各置換処理を実行するkパーティ組の順番を表す。ただし、$N={}_nC_k$は、置換処理の実行回数であり、nパーティからkパーティを選択するすべての組み合わせの数である。

[x]は、平文x∈Gの(k,n)-秘密分散値を表す。ここで、Gは可換群である。(k,n)-秘密分散値とは、平文xを(k,n)-秘密分散で分散したシェアすべてを集めた組である。秘密分散値[x]は、普段はnパーティ集合Pに分散されて所持されているため、一か所ですべてを所持されることはなく、仮想的である。

$[x]_p$は、(k,n)-秘密分散値[x]のうち、パーティp∈Pが所持するシェアを表す。

$[x^{\rightarrow}]$は、平文の列が$x^{\rightarrow}$となる(k,n)-秘密分散値の列を表す。

[G]は、可換群G上の(k,n)-秘密分散値全体の集合を表す。

$\ll x \gg^{\rho}$は、平文x∈Gの加法的秘密分散値で、kパーティ組ρがシェアを所持するものを表す。加法的秘密分散値とは、平文xを加法的秘密分散で分散したシェアすべてを集めた組を表す。

$\ll x \gg^{\rho}_{p}$は、加法的秘密分散値$\ll x \gg^{\rho}$のうち、パーティp∈ρが所持するシェアを表す。

$\ll x^{\rightarrow} \gg^{\rho}$は、平文の列が$x^{\rightarrow}$となる加法的秘密分散値の列を表す。

$\ll G \gg^{\rho}$は、可換群G上の加法的秘密分散値全体の集合を表す。

$\langle \pi \rangle$は、置換データπの置換データ秘密分散値を表す。

Πは、大きさmの置換データ全体の集合を表す。

$\langle \Pi \rangle$は、大きさmの置換データ秘密分散値全体の集合を表す。

[0019] [発明のポイント]

この発明の秘密ランダム置換の概要は以下の通りである。

ステップ１．入力を(k,n)-秘密分散値または公開値から加法的秘密分散値に変換する。

ステップ２．加法的秘密分散値上で、シェアを持つkパーティ集合ρに属する各パーティが置換データ秘密分散値$\langle \pi \rangle$のサブシェアπ_{ρ}による通常の置換を行い、再分散することを繰り返す。ただし、最終回は再分散しない。以下、反復の一回を単位置換と呼び、繰り返す処理全体を反復置換と呼ぶ。

ステップ３．出力を加法的秘密分散値から(k,n)-秘密分散値または公開値に変換する。

[0020] ステップ１及びステップ３は、既存の手法を適用できる。以下では、ステップ２の処理におけるポイントについて説明する。

[0021] ＜単位置換＞

単位置換におけるポイントは、i回目の単位置換で、$|\rho_i \setminus \rho_{i+1}|=1$となるようにkパーティ集合$\rho_i$を選択することである。つまり、i回目の単位置換を行うkパーティ集合ρ_iと、i+1回目の単位置換を行うkパーティ集合ρ_{i+1}とでは、1パーティだけが異なり残りのk-1パーティは同じパーティということである。このような単位置換を、パーティが一つしか異ならない場合であることから、1-加法的再分散プロトコルと呼ぶ。

[0022] 非特許文献１に記載の秘密ランダム置換における再分散では、(n-1)(k-1)個のG要素の通信量を要する。一方、1-加法的再分散プロトコルでは、k-1個のG要素の通信量で済む。特に、シードを予め共有して疑似乱数を共有すれば、通信量は1個のG要素の通信量で済む。この場合は、通信量が定数となり、非常に効率的である。

[0023] 1-加法的再分散プロトコルは、入力をkパーティ組$\rho=p_0,\cdots,p_{k-1}$が所持する秘密分散値$\ll a \gg^{\rho} \in \ll G \gg^{\rho}$とし、以下の手順でデータ処理を行い、他のkパーティ組$\rho'=p_1,\cdots,p_k$が所持する秘密分散値$\ll a \gg^{\rho'} \in \ll G \gg^{\rho'}$を出力する。ただし、パーティの役割は適切に変更されるものとする。

[0024] まず、パーティp_0は、i=1,…,k-1について、パーティp_iと乱数$r_i \in G$を共有する。次に、パーティp_0は、次式により秘密分散値$\ll a \gg^{\rho'}{}_{p_k}$を計算して、パーティ$p_k$に送信する。パーティ$p_k$は、受信した$\ll a \gg^{\rho'}{}_{p_k}$を出力する。

[数1]

$$\langle\langle a \rangle\rangle_{p_k}^{\rho'} = \langle\langle a \rangle\rangle_{p_0}^{\rho} - \sum_{1 \le i < k} r_i$$

[0025] 続いて、パーティp_i（i=1,…,k-1）は、次式により秘密分散値$\ll a \gg^{\rho'}{}_{p_i}$を計算して出力する。

[数2]

$$\langle\langle a \rangle\rangle_{p_i}^{\rho'} = \langle\langle a \rangle\rangle_{p_i}^{\rho} + r_i$$

[0026] ＜反復置換の中の単位置換の並列化＞

反復置換は、置換→再分散→置換→再分散→…→置換という繰り返しであり、置換をN回、再分散をN-1回実行する。これを単純に行うと、通信の段数はそのまま再分散の回数であり、N-1段となる。しかし、1-加法的再分散プロトコルによる単位置換は、通信に関して並列化することができる。データ受信を待つパーティが1パーティ、すなわち前回の単位置換に参加していないパーティだけだからであり、他のパーティは何らのデータ受信を待つことなく、オフライン処理だけを実行して次の単位置換処理に移行できるからである。加法的秘密分散のシェアはk個であるから、kパーティ組の順番Ｐを適切に設定すれば、最大k回の単位置換を1段で実行することができる。これにより、通信段数を(N-1)/k段に低減することができる。

[0027] kパーティ組の順番Ｐは、任意のi<kについて、パーティp_iからの経路の通信段数が互いに等しいか、最大値と最小値の差が最も小さい順番にすることで、通信段数を効率化することができる。

[0028] パーティp_iからの経路とは、長さLのkパーティ組の列Ｐ=($\rho_0, \cdots, \rho_{L-1}$)に対して、パーティの列($p_{j0}, p_{j1}, \cdots, p_{jL-1}$)であって、次式により帰納的に定められる列である。

[数3]

$$p_{j_0} = p_i,$$

$$p_{j_{L+1}} = \begin{cases} p_{j_L} & \text{if } p_{j_L} \in P_{L+1} \\ P_{L+1} \setminus P_L \text{の唯一の元 } p & \text{otherwise} \end{cases}$$

[0029] 経路の通信段数とは、経路の中でパーティが変化することで通信が必要となるλの数、すなわち$|\{\lambda \in N_L | p_{j\lambda} \neq p_{j\lambda+1}\}|$である。1-加法的再分散プロトコルの通信では、パーティp_kがパーティp_0からの送信を待つ以外は乱数の通信であり、前段の再分散の結果に依存していない。経路の通信段数は、このパーティp_0からパーティp_kの通信のうち直列に並んでおり並列に実行できない段数を表している。反復置換全体の通信段数は、次式に示すとおりであるため、各経路の通信段数が均等になっていると効率的である。

[数4]

$$\max_{i<k}(p_i\text{からの経路の通信段数})$$
かつ
$$\sum_{i<k}(p_i\text{からの経路の通信段数}) = |\mathrm{P}|$$

[0030] 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。

［第一実施形態］

図１を参照して、第一実施形態に係る秘密計算システムの構成例を説明する。秘密計算システムは、n（≧2）台のランダム置換装置1_1,…,1_nとネットワーク９を含む。ランダム置換装置1_1,…,1_nはネットワーク９にそれぞれ接続される。ネットワーク９はランダム置換装置1_1,…,1_nそれぞれが相互に通信可能なように構成されていればよく、例えばインターネットやＬＡＮ、ＷＡＮなどで構成することができる。また、ランダム置換装置1_1,…,1_nそれぞれは必ずしもネットワーク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、あるランダム置換装置1_i（$1 \leqq i \leqq n$）が出力する情報を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異なるランダム置換装置1_j（$1 \leqq j \leqq n$、$i \neq j$）へオフラインで入力するように構成してもよい。

[0031] 図２を参照して、秘密計算システムに含まれるランダム置換装置１の構成例を説明する。ランダム置換装置１は、事前変換部１０、単位置換部１２、再分散部１４、事後変換部１６及び記憶部１８を含む。ランダム置換装置１は、例えば、中央演算処理装置（Central Processing Unit、ＣＰＵ）、主記憶装置（Random Access Memory、ＲＡＭ）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。ランダム置換装置１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。ランダム置換装置１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読み出されて他の処理に利用される。ランダム置換装置１が備え

る記憶部１８は、例えば、ＲＡＭ（Random Access Memory）などの主記憶装置、ハードディスクや光ディスクもしくはフラッシュメモリ（Flash Memory）のような半導体メモリ素子により構成される補助記憶装置、またはリレーショナルデータベースやキーバリューストアなどのミドルウェアにより構成することができる。

[0032] パーティpに対応するランダム置換装置1_{ρ}が備える記憶部１８には、平文aの(k,n)-秘密分散値$[a]_{\rho}$もしくは公開値a、パーティpが含まれるkパーティの組ρに対応する置換データπのサブシェアπ_{ρ}及びN×k個のシード$s_{0,1}, \cdots, s_{N-1,k}$が記憶されている。なお、シード$s_{0,1}, \cdots, s_{N-1,k}$は、後述する再分散部１４の処理において乱数を生成する際に通信無しで行うために予め記憶しておくものであるが、都度協調して乱数生成を行う場合には記憶していなくても構わない。

[0033] 図３を参照しながら、第一実施形態に係る秘密計算システムが実行する秘密計算方法の処理フローの一例を、実際に行われる手続きの順に従って説明する。

[0034] ステップＳ１０において、k台のランダム置換装置$1_{\rho 0}$が備える事前変換部１０は、記憶部１８に記憶されている(k,n)-秘密分散値$[a]_{p_i}$もしくは公開値aを加法的秘密分散値$\ll a \gg^{\rho 0}$へ変換する。ρ_0はkパーティ組の列$P=(\rho_0, \cdots, \rho_{N-1})$の0番目の要素であり、ランダム置換装置$1_{\rho 0}$は、$\rho_0=(p_0, \cdots, p_{k-1})$に対応するk台のランダム置換装置$1_{p0}, \cdots, 1_{pk-1}$である。

[0035] (k,n)-秘密分散値もしくは公開値から加法的秘密分散値へ変換する方法は、既知の方法により行えばよい。

[0036] 入力が公開値である場合、加法的秘密分散値への変換は、例えば以下のように行うことができる。ρをk台のランダム置換装置$1_{p0}, \cdots, 1_{pk-1}$の組とし、$a \in G$を入力された公開値とし、ランダム置換装置1_{p0}が公開値aを知っているとする。公開値aから加法的秘密分散値$\ll a \gg^{\rho}$への変換は、i=0,…,k-1について、次式により行えばよい。

[数5]

$$\langle\langle a \rangle\rangle_{p_i}^{P} := \begin{cases} a & \text{if } i = 0 \\ 0 & \text{otherwise} \end{cases}$$

[0037] 入力が(k,n)-秘密分散値である場合、加法的秘密分散値への変換は、例えば下記の参考文献１及び参考文献２に記載された方法により行うことができる。参考文献１には、Shamir秘密分散を含む線形秘密分散から加法的秘密分散へ通信無しで変換する方法が記述されている。参考文献２には、複製秘密分散から線形秘密分散へ通信無しで変換する方法が記述されているため、複製秘密分散から加法的秘密分散への変換は、参考文献２に記載の方法と参考文献１に記載の方法を組み合わせることで通信無しで実現される。

〔参考文献１〕五十嵐大、濱田浩気、菊池亮、千田浩司、“少パーティの秘密分散ベース秘密計算のための$O(l)$ビット通信ビット分解および$O(|p'|)$ビット通信Modulus変換法”、コンピュータセキュリティシンポジウム2013、2013年

〔参考文献２〕R. Cramer, I. Damgard, and Y. Ishai, “Share conversion, pseudorandom secret-sharing and applications to secure computation”, TCC 2005, Vol. 3378 of Lecture Notes in Computer Science, pp. 342-362, 2005.

[0038] ステップＳ１ａにおいて、k台のランダム置換装置$1_{\rho 0}$は、置換処理の実行回数を表すカウンタiを0に初期化する。

[0039] ステップＳ１２において、k台のランダム置換装置$1_{\rho i}$が備える単位置換部１２は、記憶部１８に記憶されている置換データのサブシェア$\pi_{\rho i}$を用いて加法的秘密分散値≪a≫$^{\rho i}$を置換する。ρ_iはkパーティ組の列$P=(\rho_0, \cdots, \rho_{N-1})$のi番目の要素であり、ランダム置換装置$1_{\rho i}$は、$\rho_i=(p_0, \cdots, p_{k-1})$に対応するk台のランダム置換装置$1_{p0}, \cdots, 1_{pk-1}$である。置換の方法は、従来の置換データ秘密分散の方法により行えばよい。

[0040] ステップＳ１ｂにおいて、k台のランダム置換装置$1_{\rho i}$は、所定回数の置換処理が実行されたか否かを判定する。具体的には、$N={}_nC_k$を単位置換の総実行

回数として、カウンタiの値がN-1に達したか否かを判定する。i<N-1であれば、ステップＳ１４へ処理を進める。i≧N-1であれば、ステップＳ１６へ処理を進める。

[0041] ステップＳ１４において、k台のランダム置換装置$1_{\rho i+1}$が備える再分散部１４は、1-加法的再分散プロトコルにより加法的秘密分散値≪a≫$_{\rho i}$の再分散を行う。以下、ランダム置換装置1_{p0}を、ランダム置換装置$1_{\rho i}$に含まれてランダム置換装置$1_{\rho i+1}$には含まれないランダム置換装置とし、ランダム置換装置1_{pk}を、ランダム置換装置$1_{\rho i}$に含まれずランダム置換装置$1_{\rho i+1}$に含まれるランダム置換装置とする。また、ランダム置換装置1_{pj}（j=1,…,k-1）を、ランダム置換装置1_{pk}を除くランダム置換装置$1_{\rho i+1}$に含まれるk-1台のランダム置換装置を表すものとする。

[0042] まず、ランダム置換装置$1_{\rho i+1}$が備える再分散部１４は、k個の乱数$r_1,\cdots,r_k$∈Gを生成する。乱数$r_1,\cdots,r_k$は、k台のランダム置換装置$1_{\rho i+1}$が協調して共有の乱数$r_1,\cdots,r_k$を生成してもよいし、記憶部１８に記憶されているシード$s_{i,1},\cdots,s_{i,k}$を用いて疑似乱数$r_1,\cdots,r_k$を生成してもよい。予め共有したシード$s_{i,1},\cdots,s_{i,k}$を用いて疑似乱数を生成すればランダム置換装置間の通信無く乱数生成ができるので非常に効率的である。

[0043] 次に、ランダム置換装置1_{p0}が備える再分散部１４は、ランダム置換装置1_{pk}のための加法的秘密分散値≪a≫$^{\rho i+1}{}_{pk}$を、加法的秘密分散値≪a≫$^{\rho i}{}_{p0}$及び乱数$r_0,\cdots,r_{k-1}$を用いて次式により生成し、ランダム置換装置1_{pk}へ送信する。

[数6]

$$\langle\langle a\rangle\rangle_{p_k}^{\rho_{i+1}} = \langle\langle a\rangle\rangle_{p_0}^{\rho_i} - \sum_{1\le i<k} r_i$$

[0044] そして、ランダム置換装置1_{pj}が備える再分散部１４は、加法的秘密分散値≪a≫$^{\rho i}{}_{pj}$及び乱数r_jを用いて、加法的秘密分散値≪a≫$^{\rho i+1}{}_{pj}$を、次式により生成する。

[数7]

$$\langle\langle a\rangle\rangle_{p_j}^{\rho_{i+1}} = \langle\langle a\rangle\rangle_{p_j}^{\rho_i} - r_j$$

[0045] ステップＳ１ｃにおいて、k台のランダム置換装置$1_{\rho i+1}$は、置換処理の実行回数を表すカウンタiへ1を加算する。以降、ステップＳ１ｂにおいてカウンタiがN-1に達したと判定されるまで、ステップＳ１２の単位置換とステップＳ１４の再分散を繰り返す。

[0046] ステップＳ１６において、k台のランダム置換装置$1_{\rho N-1}$が備える事後変換部１６は、加法的秘密分散値を(k,n)-秘密分散値もしくは公開値へ変換する。加法的秘密分散値から他の形式へ変換する方法は、比較的軽量に行うことができる。なお、下記の変換方法は一例であり、他の変換方法では適用できないということを意味するものではない。

[0047] 出力が公開値である場合、出力を得たいランダム置換装置1_p（$1 \leqq p \leqq n$）に対して、最後に置換処理を実行したk台のランダム置換装置$1_{\rho N-1}$が加法的秘密分散値$\ll a \gg^{\rho N-1}{}_{pj}$（j=0,…,k-1）を送信し、ランダム置換装置$1_p$が復元を行う方法がある。その他に、出力を得たい複数台のランダム置換装置1_ρ（$\rho \subseteq \{1,\cdots,n\}$）から選択した一台のランダム置換装置$1_p$（$p \in \rho$）に対して、最後に置換処理を実行したk台のランダム置換装置$1_{\rho N-1}$が加法的秘密分散値$\ll a \gg^{\rho N-1}{}_{\rho j}$(j=0,…,k-1）を送信し、ランダム置換装置$1_p$が復元を行い、他のランダム置換装置$1_\rho$へ復元結果を送信する方法もある。

[0048] 出力が(k,n)-秘密分散値である場合、線形秘密分散、複製秘密分散など加法準同型性を持つ、つまり秘密分散値上で通信無しで加法を行える秘密分散に対しては、例えば、以下の手順により変換することができる。まず、k台のランダム置換装置$1_{\rho N-1}$は変換先の(k,n)-秘密分散によって加法的秘密分散値$\ll a \gg^{\rho N-1}{}_{pj}$を秘密分散し、n台のランダム置換装置$1_P$へ(k,n)-秘密分散値$[\ll a \gg^{\rho N-1}{}_{pj}]_p$（p=1,…,n）を配信する。そして、n台のランダム置換装置1_Pは受信したk個の(k,n)-秘密分散値$[\ll a \gg^{\rho N-1}{}_{pj}]_p$をすべて加算する。

[0049] このように、第一実施形態の秘密計算システムは、入力を加法的秘密分散値に変換することで、再分散の処理における通信量を低減させることができ、従来のランダム置換よりも効率的に処理を行うことが可能である。

[0050] ［第二実施形態］

秘密ランダム置換の入力が公開値である場合には第一実施形態よりもさらに効率化することができる。非特許文献１や第一実施形態の方法でランダム置換の置換データを秘密にするためには、任意のk-1パーティ組ρに対して、いずれかの補集合$\rho\bar{}_i$が$\rho \subseteq \rho\bar{}_i$を満たすようなkパーティ組の列Ｐの要素数だけ、単位置換を行う必要がある。しかし、あるパーティpがもつ公開値が入力の場合、もっと少ない回数の単位置換でよい。入力が公開値であるため、最初はパーティpが1パーティで置換を行うことができ、パーティpが知っている分の置換をすべてまとめて行うことができるからである。

[0051] 少なくとも1台のランダム置換装置$1_{\rho 0}$が備える記憶部１８には、公開値aが記憶されている。公開値aは少なくとも1台が所持していればよく、何台のランダム置換装置が所持していても構わない。

[0052] ランダム置換装置$1_{\rho 0}$を除くn-1台のランダム置換装置$1_{\rho 1}, \cdots, 1_{\rho n-1}$が備える記憶部１８には、パーティ$p_i$が含まれるkパーティの組$\rho_i$に対応する置換データ$\pi$のサブシェア$\pi_{\rho i}$及びN×k個のシード$s_{0,1}, \cdots, s_{N-1,k}$が記憶されているものとする。ただし、Nは${}_{n-1}C_k$である。第一実施形態と同様に、シード$s_{0,1}, \cdots, s_{N-1,k}$は必ずしも記憶していなくても構わない。

[0053] 図４を参照しながら、第二実施形態に係る秘密計算システムが実行する秘密計算方法の処理フローの一例を、実際に行われる手続きの順に従って説明する。

[0054] ステップＳ１２$_{\rho 0}$において、ランダム置換装置$1_{\rho 0}$が備える単位置換部１２は、ランダムな置換データπを生成し、置換データπにより公開値aを置換する。置換の方法は、従来の置換方法と同様である。

[0055] ステップＳ１０$_{\rho 0}$において、ランダム置換装置$1_{\rho 0}$が備える事前変換部１０は、置換後の公開値aを加法的秘密分散値$\ll a \gg_{\rho^{-1}}$へ変換する。変換の方法は、第一実施形態のステップＳ１０と同様である。加法的秘密分散値$\ll a \gg_{\rho^{-1}}$は、ランダム置換装置$1_{\rho 0}$のうち、任意に選択したk-1台に配信される。ここでは、ランダム置換装置$1_{\rho 1}, \cdots, 1_{\rho k-1}$に配信されたものとする。

[0056] ステップＳ１４$_{\rho 0}$において、k台のランダム置換装置$1_{\rho 0}$が備える再分散部１

４は、1-加法的再分散プロトコルにより加法的秘密分散値≪a≫$_{\rho^{-1}}$の再分散を行う。再分散の方法は、第一実施形態のステップＳ１４と同様である。

[0057] 以降、ランダム置換装置１$_{\rho 0}$を除くn-1台のランダム置換装置１$_{\rho 1}$, …, １$_{\rho n-1}$により、ステップＳ１ａからＳ１６までの処理を実行する。

[0058] このように、第二実施形態の秘密計算システムでは、1台のランダム置換装置によりまとめて置換を行った後にn-1台のランダム置換装置によりランダム置換を行うため、置換処理の回数が$_{n-1}C_k$+1となり、第一実施形態の秘密計算システムよりも効率的に処理を行うことが可能である。

[0059] ［第三実施形態］

秘密ランダム置換の入力が公開値の場合と同様に、秘密ランダム置換の出力が公開値の場合にも、第一実施形態よりもさらに効率化ができる。出力が公開値であるため、n-1パーティがランダム置換を行った後に、残りの1パーティに秘密分散値を送信し、復元した公開値に対してまとめて置換を行うことができるからである。

[0060] ランダム置換装置１$_{\rho 0}$を除くn-1台のランダム置換装置１$_{\rho 1}$, …, １$_{\rho n-1}$が備える記憶部１８には、パーティp_iが含まれるkパーティの組ρ_iに対応する置換データπのサブシェアπ_{ρ_i}及びN×k個のシード$s_{0,1}$, …, $s_{N-1,k}$が記憶されているものとする。ただし、Nは$_{n-1}C_k$である。第一実施形態と同様に、シード$s_{0,1}$, …, $s_{N-1,k}$は必ずしも記憶していなくても構わない。

[0061] 図５を参照しながら、第三実施形態に係る秘密計算システムが実行する秘密計算方法の処理フローの一例を、実際に行われる手続きの順に従って説明する。

[0062] ステップＳ１０からＳ１ｂにおいてi≧N-1と判定されるまでの処理を、ランダム置換装置１$_{\rho 0}$を除くn-1台のランダム置換装置１$_{\rho 1}$, …, １$_{\rho n-1}$により実行する。

[0063] ステップＳ１６$_{\rho 0}$において、ランダム置換装置１$_{\rho 0}$が備える事後変換部１６は、加法的秘密分散値を公開値へ変換する。変換の方法は第一実施形態のステップＳ１６と同様である。具体的には、ランダム置換装置１$_{\rho 0}$に対して、最

後に置換処理を実行したk台のランダム置換装置$1_{\rho^{N-1}}$が加法的秘密分散値≪a≫$_{\rho^{N-1}_j}$（j=0,…,k-1）を送信し、ランダム置換装置$1_{\rho 0}$が備える事後変換部１６が加法的秘密分散値≪a≫$_{\rho^{N-1}}$を復元する。

[0064] ステップＳ１２$_{\rho 0}$において、ランダム置換装置$1_{\rho 0}$が備える単位置換部１２は、ランダムな置換データπを生成し、復元された公開値を置換する。置換の方法は、従来の置換方法と同様である。

[0065] このように、第三実施形態の秘密計算システムでは、n-1台のランダム置換装置によりランダム置換を行った後に1台のランダム置換装置によりまとめて置換を行うため、置換処理の回数が$_{n-1}C_k+1$となり、第一実施形態の秘密計算システムよりも効率的に処理を行うことが可能である。

[0066] ［第四実施形態］

第四実施形態は、この発明の秘密ランダム置換に対して秘密計算中の改ざんを検知することを可能とする実施形態である。秘密計算中の改ざんを検知する秘密改ざん検知方法として、下記参考文献３に記載の方法が提案されている。参考文献３では、３つのフェーズで秘密計算中の改ざん検知を行う。ランダム化フェーズでは、分散値を正当性検証可能なランダム化分散値へと変換する。計算フェーズでは、semi-honestの演算により構成されるランダム化分散値用の演算を用いて所望の秘密計算を実行する。このとき、後続の正当性証明フェーズでチェックサムを計算するために必要となるランダム化分散値を収集しながら計算が行われる。正当性証明フェーズでは、計算フェーズで収集されたランダム化分散値に対して、一括でチェックサムを計算し正当性証明を行う。チェックサムが正当であれば計算フェーズによる計算結果を出力し、正当でなければ計算結果は出力せずに正当でない旨のみを出力する。

〔参考文献３〕五十嵐大、千田浩司、濱田浩気、菊池亮、“非常に高効率なn≧2k-1 malicious モデル上秘密分散ベースマルチパーティ計算の構成法”、SCIS2013、2013年

しかしながら、参考文献３に記載の方法を適用するためには、秘密計算で

実行する各演算がtamper-simulatableである必要がある（参考文献４）。

〔参考文献４〕D. Ikarashi, R. Kikuchi, K. Hamada, and K. Chida, “Actively Private and Correct MPC Scheme in t<n/2 from Passively Secure Schemes with Small Overhead”, IACR Cryptology ePrint Archive, vol. 2014, p. 304, 2014

[0067] そこで、第四実施形態では、参考文献３に記載の秘密改ざん検知方法を上記の条件を満たすように第一実施形態の秘密ランダム置換に適用した構成例を示す。なお、以下では第一実施形態に適用した例を示すが、同様の考え方により、第二実施形態及び第三実施形態に適用することも可能である。

[0068] 図６を参照して、第四実施形態に係るランダム置換装置２の構成例を説明する。ランダム置換装置２は、上述の実施形態に係るランダム置換装置１と同様に、事前変換部１０、単位置換部１２、再分散部１４、事後変換部１６及び記憶部１８を含み、ランダム化部２０、単位変換部２２及び正当性証明部２４をさらに含む。

[0069] 図７を参照しながら、第四実施形態に係る秘密計算システムが実行する秘密計算方法の処理フローの一例を、実際に行われる手続きの順に従って説明する。

[0070] ステップＳ２０において、k台のランダム置換装置$1_{\rho 0}$が備えるランダム化部２０は、記憶されている(k,n)-秘密分散値$[a]_{pi}$をランダム化分散値へ変換する。記憶部１８に公開値aが記憶されている場合には、公開値aを(k,n)-秘密分散値$[a]_{pi}$へ変換した上で、ランダム化分散値へ変換する。ランダム化分散値とは、値a∈Rの分散値$[a]_{pi}$と、値a∈Rと乱数r∈Aとの積算値arの分散値$[ar]_{pi}$との組$([a]_{pi},[ar]_{pi})$である。ここで、Rは環であり、Aは環R上の結合多元環である。結合多元環とは、結合的な環であって、かつそれと両立するような、何らかの体上の線型空間の構造を備えたものである。結合多元環は、ベクトル空間で扱う値が体ではなく環でよくなったものと言える。ランダム化分散値の第０成分（$[a]_{pi}$）はR成分、第１成分（$[ar]_{pi}$）はA成分とも呼ぶ。

[0071] ランダム化分散値を生成する際に用いる乱数は、同一の環上の秘密分散を

複数利用する場合には、一方の秘密分散のための分散値を他方の秘密分散のための分散値に変換することで、乱数の値が同一となるように生成する。この形式変換においても、改ざん検知が可能もしくは改ざんが不可能でなければならない。例えば、複製型秘密分散（replicated secret sharing）から線形秘密分散（linear secret sharing）へ変換する改ざん不可能な方法は上記参考文献２に記載されている。

[0072] ステップＳ２２において、k台のランダム置換装置１$_{\rho_i}$が備える単位変換部２２は、単位置換部１２により置換された加法的秘密分散値≪a≫$_{\rho_i}$を(k,n)-秘密分散によるランダム化分散値に変換して記憶部１８に蓄積する。蓄積したランダム化分散値は後述の正当性証明部２４においてチェックサムを計算するために利用される。ランダム化分散値の蓄積は、すべての単位置換の後に必ず行わなくともよく、一部の単位置換の際にのみ行うようにしてもよい。

[0073] ステップＳ２４において、正当性証明部２４は、すべての秘密分散についてすべての秘密計算が終了するまで待機する同期処理（SYNC）を実行する。すべての秘密分散についてすべての秘密計算が終了したことを検知すると、ランダム化部２０で用いた乱数$r_0,\cdots,r_{J-1}$の分散値$[r_0],\cdots,[r_{J-1}]$を用いてチェックサム$C_0,\cdots,C_{J-1}$を検証し、秘密ランダム置換の結果として得られる(k,n)-秘密分散値もしくは公開値の正当性を検証する。チェックサム$C_0,\cdots,C_{J-1}$を検証した結果、改ざんがないと判定した場合はステップＳ１６へ処理を進める。改ざんがあったと判断した場合はその旨を示す情報（例えば、「⊥」など）を出力する。

[0074] チェックサムの検証は、j=0,…,J-1について、チェックサムC_jに含まれるランダム化分散値のR成分の総和に分散値$[r_j]$を乗じた分散値$[\phi_j]$と、チェックサムC_jに含まれるランダム化分散値のA成分の総和である分散値$[\phi_j]$とを計算し、分散値$[\phi_j]$と分散値$[\phi_j]$を減算した分散値$[\delta_j]=[\phi_j]-[\phi_j]$を復元して、値$\delta_0,\cdots,\delta_{J-1}$がすべて0であれば秘密ランダム置換全体を通して改ざんがなかったものと判定する。いずれかの値δ_jが0以外であれば、秘密ランダム置換

のいずれかの演算において改ざんがあったものと判定する。

[0075] J個の秘密分散のうち同一の環上の秘密分散が存在する場合には、可能な限りまとめて正当性証明を行うと、公開される値の数が少なくなるため、より秘匿性を向上することができる。例えば、α（α=0,…,J-1）番目の秘密分散とβ（β=0,…,J-1、$\alpha \neq \beta$）番目の秘密分散が同一の環上の秘密分散である場合には、以下のように正当性証明を行う。まず、チェックサムC_αから上述のように算出した分散値[ϕ_α]と、チェックサムC_αから上述のように算出した分散値[ϕ_α]とをそれぞれβ番目の秘密分散へ変換する。そして、変換後の分散値[ϕ_α]とチェックサムC_βから同様に算出した分散値[ϕ_β]とを合算した分散値[$\phi_\alpha+\phi_\beta$]と、変換後の分散値[ϕ_α]とβ番目のチェックサムC_βから同様に算出した分散値[ϕ_β]とを合算した分散値[$\phi_\alpha+\phi_\beta$]とを減算した分散値[δ]=([ϕ_α]+[ϕ_β])-([ϕ_α]+[ϕ_β])を復元し、復元値δが0であれば改ざんがなかったものと判定し、復元値δが0以外であれば改ざんがあったものと判定する。このようにして、すべての同一の環上の秘密分散の組み合わせについて検証し、秘密ランダム置換全体で改ざんがなかったことを検証する。本形態では２個の秘密分散が同一の環上の秘密分散である例を説明したが、３個以上の秘密分散が同一の環上の秘密分散である場合でも、同様の方法により正当性証明を行うことができる。

[0076] ステップＳ１６において、事後変換部１６は、加法的秘密分散値を(k,n)-秘密分散値もしくは公開値へ変換する。上述の実施形態では、出力が公開値の場合には、最後の置換処理を行った後の加法的秘密分散値$\ll a \gg_{\rho^{N-1}}$をランダム置換装置1_ρへ送信し、そのランダム置換装置1_ρが加法的秘密分散の復元方法により公開値aを得るように構成した。本形態では、公開時の改ざんを検知するために、加法的秘密分散値を(k,n)-秘密分散値に一旦変換した上で、(k,n)-秘密分散の復元方法により公開値aを得るように構成する。

[0077] (k,n)-秘密分散値から公開値を得る際には、改ざん検知が可能な公開方法による必要がある。改ざん検知が可能な公開方法としては、上記参考文献４のappendixに記載の方法がある。もしくは、以下のようにして公開を行うこ

とで改ざん検知が可能である。

[0078] ランダム置換装置1_pは、任意のk-1台のランダム置換装置から、加法的秘密分散値$\ll a \gg_{\rho^{N-1}}$を形式変換した(k,n)-秘密分散値を受信する。また、残りのn-k台のランダム置換装置からは、加法的秘密分散値$\ll a \gg_{\rho^{N-1}}$を形式変換した(k,n)-秘密分散値のハッシュ値などのチェックサムを受信する。チェックサムはハッシュ値でなくてもよく、より安全な情報理論的なチェックサムを用いることもできる。情報理論的なチェックサムは、例えば、チェックサムの計算対象をa_iとして、乱数rと$a_i r^{i+1}$の組である。ランダム置換装置1_pは、自らの持つ(k,n)-秘密分散値を加えたk個の(k,n)-秘密分散値からn-k個の(k,n)-秘密分散値を復旧し、復旧した(k,n)-秘密分散値それぞれからチェックサムを計算する。なお、復旧とは、一部の分散値が失われた際に、利用可能なk個の分散値から利用不能となったn-k個の分散値を秘匿性を失わずに再構築する方法である。

[0079] 続いて、ランダム置換装置1_pは、n-k台のランダム置換装置から受信した(k,n)-秘密分散値のチェックサムと、復旧した(k,n)-秘密分散値のチェックサムとが一致するか否かを確認する。すべてのチェックサムが一致した場合には改ざんがなかったものと判定し、(k,n)-秘密分散値もしくは公開値を出力する。いずれかのチェックサムが異なっていた場合には改ざんがあったものと判定し、その旨を示す情報（例えば、「⊥」など）を出力する。

[0080] 本形態のように構成すれば、この発明の秘密ランダム置換において、改ざん検知が可能となり、安全性が向上する。

[0081] ［構成例の組み合わせ］

この発明は、上述の実施形態の他にも、四つの独立した観点の組み合わせにより、様々な構成とすることが可能である。

[0082] 一つ目の観点は、入出力の型の観点である。この観点では、四つの構成方法が考えられる。一つ目の構成は、入力が線形秘密分散値であり出力が線形秘密分散値の場合である。二つ目の構成は、入力が線形秘密分散値であり出力が複製秘密分散値の場合、もしくはその逆に入力が複製秘密分散値であり

出力が線形秘密分散値の場合である。三つ目の構成は、入力が公開値であり出力が秘密分散値の場合である。四つ目の構成は、入力が線形秘密分散値であり出力が公開値の場合である。

[0083] 二つ目の観点は、乱数生成方法の観点である。この観点では、二つの構成方法が考えられる。一つ目の構成は、乱数があらかじめ共有されたシードから生成される疑似乱数の場合である。二つ目の構成は、乱数がプロトコル実行時に共有される場合である。

[0084] 三つ目の観点は、ランダム置換の種類の観点である。この観点では、二つの構成方法が考えられる。一つ目の構成は、置換データが任意の場合であり、完全にランダムにシャッフルしたい場合である。二つ目の構成は、置換データがローテーションに制限される場合、つまり置換データがある$r \in N_m$で表現され、$\pi(i)=i+r \bmod m$となっており、絶対的な位置は秘匿したいが相対的な並び順は秘匿しなくてよい場合である。

[0085] 四つ目の観点は、k,nを限定した反復置換の具体例の観点である。一つ目の構成は、k=2, n=3の構成である。二つ目の構成は、k=3, n=5の構成である。この観点では、各構成に対して、さらに入出力の観点を加えた計六つの具体例が考えられる。

[0086] 一つ目の具体例は、k=2, n=3の構成において、入出力とも秘密分散値の場合である。図６を参照しながら、この具体例の反復置換について説明する。図６において、縦軸はパーティを表し、横軸は単位置換の回数を表している。丸印は単位置換において処理を行うパーティを示している。実線の矢印は再分散において秘密分散値が送信されるパーティの方向を示している。点線の矢印は再分散において同一のパーティが引き続き秘密分散値を保持することを示している。図６の例では、kパーティ組の順番$P=(\rho_0, \rho_1, \rho_2)$は、$\rho_0=(p_0, p_1)$、$\rho_1=(p_1, p_2)$、$\rho_2=(p_0, p_2)$と設定される。一回目の単位置換ではパーティ$p_0, p_1$が処理を行い、一回目の再分散ではパーティ$p_0$からパーティ$p_2$へ秘密分散値が送信される。二回目の単位置換ではパーティp_1, p_2が処理を行い、二回目の再分散ではパーティp_1からパーティp_0へ秘密分散値が送信される。三回目

の単位置換でパーティp_0, p_2が処理を行い、反復置換が完了する。

[0087] 二つ目の具体例は、k=3, n=5の構成において、入出力とも秘密分散値の場合である。図７を参照しながら、この具体例の反復置換について説明する。図の記法は、図６と同様である。図７の例では、kパーティ組の順番Ｐ=(ρ_0, …, ρ_9)は、$\rho_0=(p_0, p_1, p_2)$、$\rho_1=(p_1, p_2, p_3)$、$\rho_2=(p_2, p_3, p_4)$、$\rho_3=(p_0, p_3, p_4)$、$\rho_4=(p_0, p_1, p_4)$、$\rho_5=(p_1, p_3, p_4)$、$\rho_6=(p_0, p_1, p_3)$、$\rho_7=(p_0, p_2, p_3)$、$\rho_8=(p_0, p_2, p_4)$、$\rho_9=(p_1, p_2, p_4)$と設定される。一回目の単位置換ではパーティp_0, p_1, p_2が処理を行い、一回目の再分散ではパーティp_0からパーティp_3へ秘密分散値が送信される。二回目の単位置換ではパーティp_1, p_2, p_3が処理を行い、二回目の再分散ではパーティp_1からパーティp_4へ秘密分散値が送信される。三回目の単位置換ではパーティp_2, p_3, p_4が処理を行い、三回目の再分散ではパーティp_2からパーティp_0へ秘密分散値が送信される。四回目の単位置換ではパーティp_0, p_3, p_4が処理を行い、四回目の再分散ではパーティp_3からパーティp_1へ秘密分散値が送信される。ここで、パーティp_3からパーティp_1へ送信される秘密分散値は、一回目の再分散でパーティp_0からパーティp_3へ送信された秘密分散値であるから、五回目の再分散の前にパーティp_1は受信待ちが発生する。したがって、四回目の再分散までは通信の一段目となる。以降、同様に置換と再分散を繰り返すことで、この具体例では三段の通信段数で反復置換が完了する。

[0088] 三つ目の具体例は、k=2, n=3の構成において、入力が公開値であり出力が秘密分散値の場合である。図８を参照しながら、この具体例の反復置換について説明する。図の記法は、図６と同様である。図８の例では、kパーティ組の順番Ｐ=(ρ_0, ρ_1, ρ_2)は、$\rho_0=\rho_1=(p_0)$、$\rho_2=(p_1, p_2)$と設定される。一回目と二回目の単位置換ではパーティp_0のみが処理を行う。この単位置換は単純に二回繰り返してもよいし、二回分の置換をまとめて行うこともできる。二回目の再分散ではパーティp_0からパーティp_1, p_2へ秘密分散値が送信される。三回目の単位置換でパーティp_1, p_2が処理を行い、反復置換が完了する。

[0089] 四つ目の具体例は、k=3, n=5の構成において、入力が公開値であり出力が秘密分散値の場合である。図９を参照しながら、この具体例の反復置換につ

いて説明する。図の記法は、図６と同様である。図９の例では、kパーティ組の順番Ｐ=($\rho_0, \cdots, \rho_9$)は、$\rho_0=\rho_1=\rho_2=\rho_3=\rho_4=\rho_5=(p_0)$、$\rho_6=(p_2, p_3, p_4)$、$\rho_7=(p_1, p_3, p_4)$、$\rho_8=(p_1, p_2, p_4)$、$\rho_9=(p_1, p_2, p_3)$と設定される。一回目から六回目の単位置換ではパーティp_0のみが処理を行う。この単位置換は単純に六回繰り返してもよいし、六回分の置換をまとめて行うこともできる。六回目の再分散ではパーティp_0からパーティp_2, p_3, p_4へ秘密分散値が送信される。七回目の単位置換ではパーティp_2, p_3, p_4が処理を行い、七回目の再分散ではパーティp_2からパーティp_1へ秘密分散値が送信される。八回目の単位置換ではパーティp_1, p_3, p_4が処理を行い、八回目の再分散ではパーティp_3からパーティp_2へ秘密分散値が送信される。九回目の単位置換ではパーティp_1, p_2, p_4が処理を行い、九回目の再分散ではパーティp_4からパーティp_3へ秘密分散値が送信される。十回目の単位置換ではパーティp_1, p_2, p_3が処理を行い、反復置換が完了する。図７に示すとおり、この具体例では二段の通信段数で反復置換が完了する。

[0090] 五つ目の具体例は、k=2, n=3の構成において、入力が秘密分散値であり出力が公開値の場合である。図１０を参照しながら、この具体例の反復置換について説明する。図の記法は、図６と同様である。図１０の例では、kパーティ組の順番Ｐ=(ρ_0, ρ_1, ρ_2)は、$\rho_0=(p_1, p_2)$、$\rho_1=\rho_2=(p_0)$と設定される。一回目の単位置換ではパーティp_1, p_2が処理を行い、パーティp_1, p_2からパーティp_0へ秘密分散値が送信される。パーティp_0は秘密分散値の復元を行い、二回目と三回目の単位置換を行う。この単位置換は単純に二回繰り返してもよいし、二回分の置換をまとめて行うこともできる。以上で反復置換が完了する。

[0091] 六つ目の具体例は、k=3, n=5の構成において、入力が秘密分散値であり出力が公開値の場合である。図１１を参照しながら、この具体例の反復置換について説明する。図の記法は、図６と同様である。図１１の例では、kパーティ組の順番Ｐ=($\rho_0, \cdots, \rho_9$)は、$\rho_0=(p_2, p_3, p_4)$、$\rho_1=(p_1, p_3, p_4)$、$\rho_2=(p_1, p_2, p_4)$、$\rho_3=(p_1, p_2, p_3)$、$\rho_4=\rho_5=\rho_6=\rho_7=\rho_8=\rho_9=(p_0)$と設定される。一回目の単位置換ではパーティ$p_2, p_3, p_4$が処理を行い、一回目の再分散ではパーティ$p_2$からパーティ$p_1$へ秘密分散値が送信される。以降、パーティ$p_1, p_2, p_3, p_4$により置換と

再分散を繰り返し、N（$=_4C_3=4$）回目の置換が完了した後、パーティp_1, p_2, p_3からパーティp_0へ秘密分散値が送信される。パーティp_0は秘密分散値の復元を行い、五回目から十回目の単位置換を行う。この単位置換は単純に六回繰り返してもよいし、六回分の置換をまとめて行うこともできる。以上で反復置換が完了する。

[0092] この発明は上述の実施形態に限定されるものではなく、この発明の趣旨を逸脱しない範囲で適宜変更が可能であることはいうまでもない。上記実施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。

[0093] ［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。

[0094] 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。

[0095] 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。

[0096] 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、自己の記録媒体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。

[0097] 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] n,kを2以上の整数とし、n>kとし、$N={}_nC_k$とし、ρをn台のランダム置換装置から選択したk台のランダム置換装置の組とし、$\rho_0,\cdots,\rho_{N-1}$はi=0,…,N-2について$|\rho_i \setminus \rho_{i+1}|=1$となるように構成されており、≪a≫$^{\rho i}$をi番目のランダム置換装置の組$\rho_i$が保持する平文aの加法的秘密分散値とし、≪a≫$^{\rho i}{}_p$を加法的秘密分散値≪a≫$^{\rho i}$のうちランダム置換装置pが保持する加法的秘密分散値とし、$\pi_{\rho i}$をi番目のランダム置換装置の組ρ_iに対応する置換データπのサブシェアとし、ランダム置換装置p_0をi番目のランダム置換装置の組ρ_iに含まれi+1番目のランダム置換装置の組ρ_{i+1}に含まれないランダム置換装置とし、ランダム置換装置p_kをi番目のランダム置換装置の組ρ_iに含まれずi+1番目のランダム置換装置の組ρ_{i+1}に含まれるランダム置換装置とし、ランダム置換装置p_j（j=1,…,k-1）をi番目のランダム置換装置の組ρ_i及びi+1番目のランダム置換装置の組ρ_{i+1}のいずれにも含まれるk-1台のランダム置換装置とし、

上記ランダム置換装置$p_0,\cdots,p_{k-1}$が、上記加法的秘密分散値≪a≫$^{\rho i}$を上記サブシェア$\pi_{\rho i}$により置換する単位置換ステップと、

上記ランダム置換装置p_0が、上記ランダム置換装置p_jそれぞれと共有する乱数$r_1,\cdots,r_{k-1}$を用いて加法的秘密分散値≪a≫$^{\rho i+1}{}_{pk}$を生成して上記ランダム置換装置p_kへ送信し、上記ランダム置換装置p_jそれぞれが上記乱数r_jを用いて加法的秘密分散値≪a≫$^{\rho i+1}{}_{pj}$を生成する再分散ステップと、

を含む秘密計算方法。

[請求項2] 請求項１に記載の秘密計算方法であって、

上記再分散ステップは、上記ランダム置換装置p_0が次式により上記加法的秘密分散値≪a≫$^{\rho i+1}{}_{pk}$を生成し、

[数8]

$$\langle\langle a\rangle\rangle_{p_k}^{\rho_{i+1}} = \langle\langle a\rangle\rangle_{p_0}^{\rho_i} - \sum_{1\le i<k} r_i$$

上記ランダム置換装置p_jそれぞれが次式により上記加法的秘密分散値≪a≫$^{\rho_{i+1}}_{p_j}$を生成する

[数9]

$$\langle\langle a\rangle\rangle_{p_j}^{\rho_{i+1}} = \langle\langle a\rangle\rangle_{p_j}^{\rho_i} - r_j$$

秘密計算方法。

[請求項3] 請求項２に記載の秘密計算方法であって、

$\rho_0, \cdots, \rho_{N-1}$は、0番目のランダム置換装置の組$\rho_0$に含まれるk台のランダム置換装置からN-1番目のランダム置換装置の組ρ_{N-1}に含まれるk台のランダム置換装置への経路の通信段数が、最大値と最小値の差が最も小さくなるように構成されている

秘密計算方法。

[請求項4] 請求項１から３のいずれかに記載の秘密計算方法であって、

上記平文aの(k,n)-秘密分散による秘密分散値[a]を上記加法的秘密分散値≪a≫$^{\rho_0}$に変換する事前変換ステップと、

上記加法的秘密分散値≪a≫$^{\rho_{N-1}}$を上記秘密分散値[a]に変換して出力する事後変換ステップと、

をさらに含む秘密計算方法。

[請求項5] 請求項１から３のいずれかに記載の秘密計算方法であって、

$N={}_{n-1}C_k$とし、 ρをn台のランダム置換装置から所定のランダム置換装置qを除いて選択したk台のランダム置換装置の組とし、

上記平文aを上記加法的秘密分散値≪a≫$^{\rho_0}$に変換する事前変換ステップと、

上記加法的秘密分散値≪a≫$^{\rho_{N-1}}$を(k,n)-秘密分散による秘密分散値[a]に変換して出力する事後変換ステップと、

をさらに含み、

上記単位置換ステップは、

$i \leqq {}_nC_k - {}_{n-1}C_k$であれば、上記ランダム置換装置qが、上記平文aを上記サブシェアπ_{ρ_i}により置換し、

$i>{}_nC_k-{}_{n-1}C_k$であれば、上記ランダム置換装置$p_1,\cdots,p_{k-1}$が、上記加法的秘密分散値≪a≫$^{\rho i}$を上記サブシェア$\pi_{\rho i}$により置換する

秘密計算方法。

[請求項6] 請求項１から３のいずれかに記載の秘密計算方法であって、

$N={}_{n-1}C_k$とし、ρをn台のランダム置換装置から所定のランダム置換装置qを除いて選択したk台のランダム置換装置の組とし、

上記平文aの(k,n)-秘密分散による秘密分散値[a]を上記加法的秘密分散値≪a≫$^{\rho 0}$に変換する事前変換ステップと、

上記加法的秘密分散値≪a≫$^{\rho N-1}$を復元して上記平文aを出力する事後変換ステップと、

をさらに含み、

上記単位置換ステップは、

$i\leqq{}_{n-1}C_k$であれば、上記ランダム置換装置$p_1,\cdots,p_{k-1}$が、上記加法的秘密分散値≪a≫$^{\rho i}$を上記サブシェア$\pi_{\rho i}$により置換し、

$i>{}_{n-1}C_k$であれば、上記ランダム置換装置qが、上記平文aを上記サブシェア$\pi_{\rho i}$により置換する

秘密計算方法。

[請求項7] 請求項１から６のいずれかに記載の秘密計算方法であって、

上記単位置換ステップにより置換された上記加法的秘密分散値≪a≫$^{\rho i}$を(k,n)-秘密分散による秘密分散値[a]に変換して記憶部に蓄積する単位変換ステップ

をさらに含む秘密計算方法。

[請求項8] nを2以上の整数とし、n台のランダム置換装置を含む秘密計算システムであって、

kを2以上の整数とし、n>kとし、$N={}_nC_k$とし、ρをn台のランダム置換装置から選択したk台のランダム置換装置の組とし、$\rho_0,\cdots,\rho_{N-1}$はi=0,…,N-2について$|\rho_i\setminus\rho_{i+1}|=1$となるように構成されており、≪a≫$^{\rho i}$をi番目のランダム置換装置の組$\rho_i$が保持する平文aの加法的秘密

分散値とし、$\ll a \gg^{\rho i}{}_{p}$を加法的秘密分散値$\ll a \gg^{\rho i}$のうちランダム置換装置pが保持する加法的秘密分散値とし、$\pi_{\rho i}$をi番目のランダム置換装置の組ρ_iに対応する置換データπのサブシェアとし、ランダム置換装置p_0をi番目のランダム置換装置の組ρ_iに含まれi+1番目のランダム置換装置の組ρ_{i+1}に含まれないランダム置換装置とし、ランダム置換装置p_kをi番目のランダム置換装置の組ρ_iに含まれずi+1番目のランダム置換装置の組ρ_{i+1}に含まれるランダム置換装置とし、ランダム置換装置p_j（j=1,…,k-1）をi番目のランダム置換装置の組ρ_i及びi+1番目のランダム置換装置の組ρ_{i+1}のいずれにも含まれるk-1台のランダム置換装置とし、

上記ランダム置換装置は、

上記加法的秘密分散値$\ll a \gg^{\rho i}$を上記サブシェア$\pi_{\rho i}$により置換する単位置換部と、

当該ランダム置換装置が上記ランダム置換装置p_0であれば、上記ランダム置換装置p_jそれぞれと共有する乱数$r_1,\cdots,r_{k-1}$を用いて加法的秘密分散値$\ll a \gg^{\rho i+1}{}_{pk}$を生成して上記ランダム置換装置$p_k$へ送信し、当該ランダム置換装置が上記ランダム置換装置p_jのいずれかであれば、上記乱数r_jを用いて加法的秘密分散値$\ll a \gg^{\rho i+1}{}_{pj}$を生成する再分散部と、

を含む秘密計算システム。

[請求項9] n,kを2以上の整数とし、n>kとし、$N={}_nC_k$とし、ρをn台のランダム置換装置から選択したk台のランダム置換装置の組とし、$\rho_0,\cdots,\rho_{N-1}$はi=0,…,N-2について$|\rho_i \setminus \rho_{i+1}|=1$となるように構成されており、$\ll a \gg^{\rho i}$をi番目のランダム置換装置の組$\rho_i$が保持する平文aの加法的秘密分散値とし、$\ll a \gg^{\rho i}{}_{p}$を加法的秘密分散値$\ll a \gg^{\rho i}$のうちランダム置換装置pが保持する加法的秘密分散値とし、$\pi_{\rho i}$をi番目のランダム置換装置の組ρ_iに対応する置換データπのサブシェアとし、ランダム置換装置p_0をi番目のランダム置換装置の組ρ_iに含まれi+1番目のラン

ダム置換装置の組ρ_{i+1}に含まれないランダム置換装置とし、ランダム置換装置p_kをi番目のランダム置換装置の組ρ_iに含まれずi+1番目のランダム置換装置の組ρ_{i+1}に含まれるランダム置換装置とし、ランダム置換装置p_j（j=1,…,k-1）をi番目のランダム置換装置の組ρ_i及びi+1番目のランダム置換装置の組ρ_{i+1}のいずれにも含まれるk-1台のランダム置換装置とし、

上記加法的秘密分散値≪a≫$^{\rho i}$を上記サブシェア$\pi_{\rho i}$により置換する単位置換部と、

当該ランダム置換装置が上記ランダム置換装置p_0であれば、上記ランダム置換装置p_jそれぞれと共有する乱数$r_1,\cdots,r_{k-1}$を用いて加法的秘密分散値≪a≫$^{\rho i+1}{}_{pk}$を生成して上記ランダム置換装置p_kへ送信し、当該ランダム置換装置が上記ランダム置換装置p_jのいずれかであれば、上記乱数r_jを用いて加法的秘密分散値≪a≫$^{\rho i+1}{}_{pj}$を生成する再分散部と、

を含むランダム置換装置。

[請求項10] 請求項９に記載のランダム置換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]

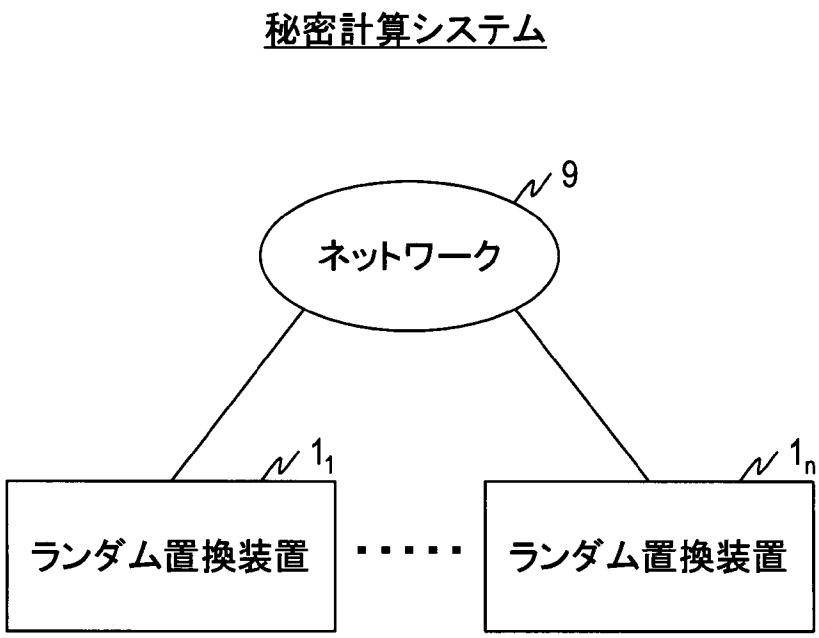


図1

[図2]

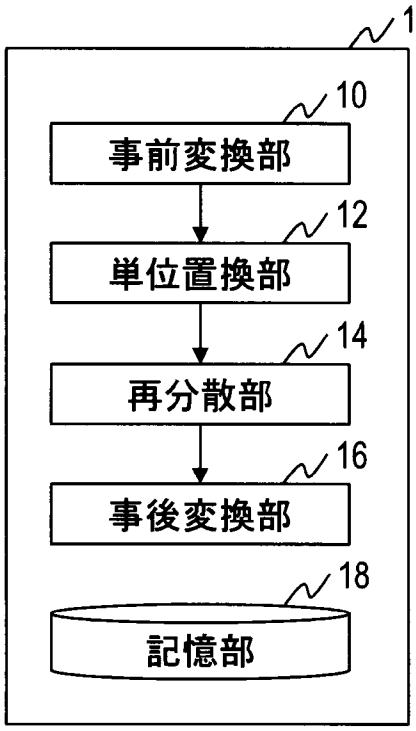


図2

[図3]

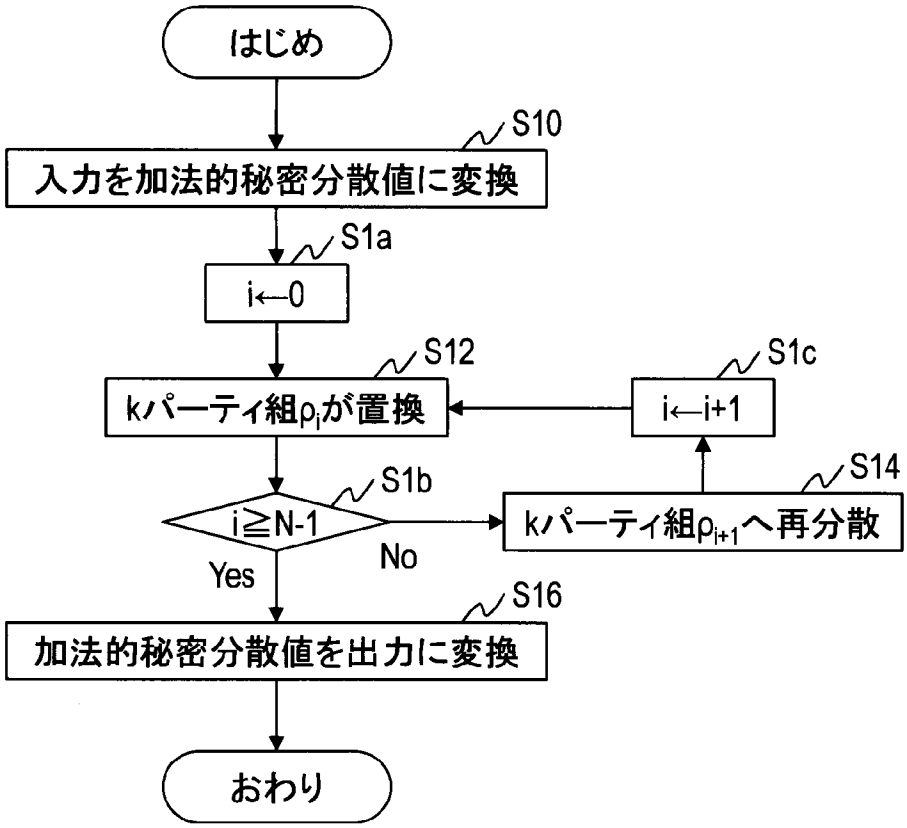

はじめ
S10
入力を加法的秘密分散値に変換
S1a
i←0
S12
kパーティ組ρiが置換
S1c
i←i+1
S1b
i≧N-1
Yes
No
S14
kパーティ組ρi+1へ再分散
S16
加法的秘密分散値を出力に変換
おわり

図3

[図4]

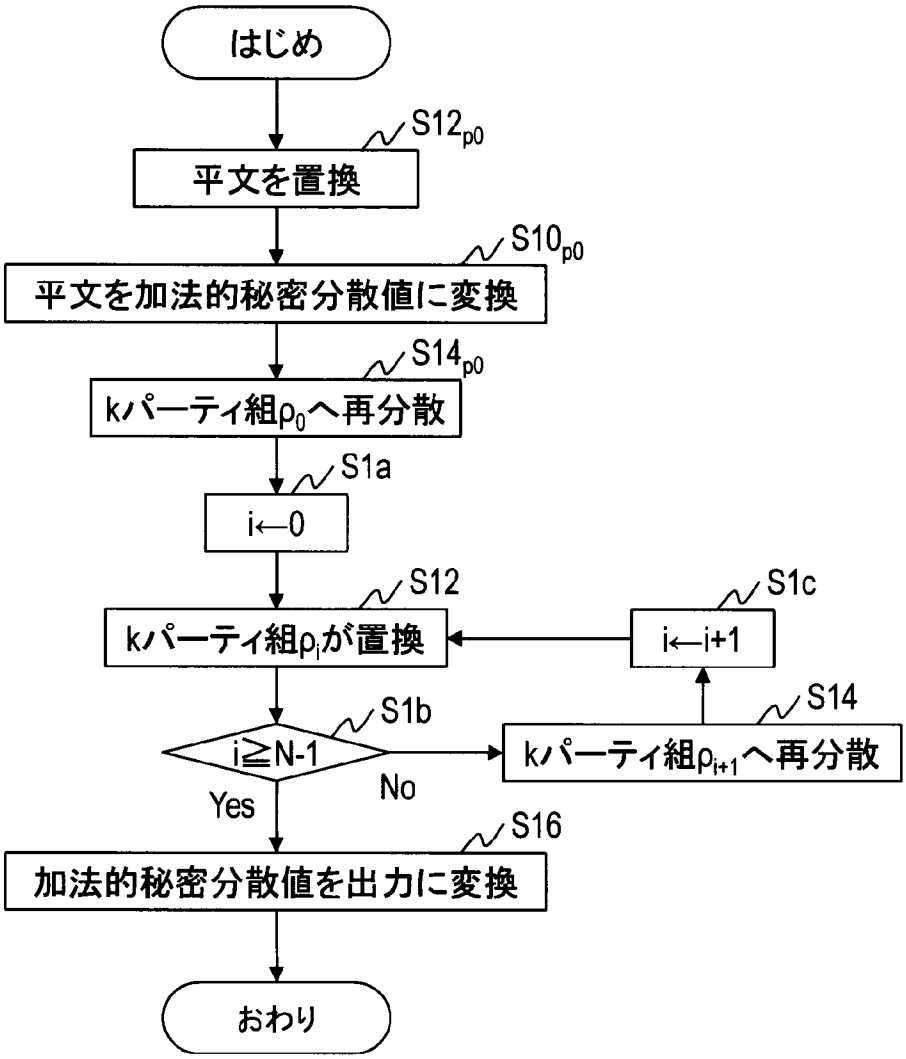

はじめ
S12p0
平文を置換
S10p0
平文を加法的秘密分散値に変換
S14p0
kパーティ組ρ0へ再分散
S1a
i←0
S12
kパーティ組ρiが置換
S1c
i←i+1
S1b
i≧N-1
No
S14
kパーティ組ρi+1へ再分散
Yes
S16
加法的秘密分散値を出力に変換
おわり

図4

[図5]

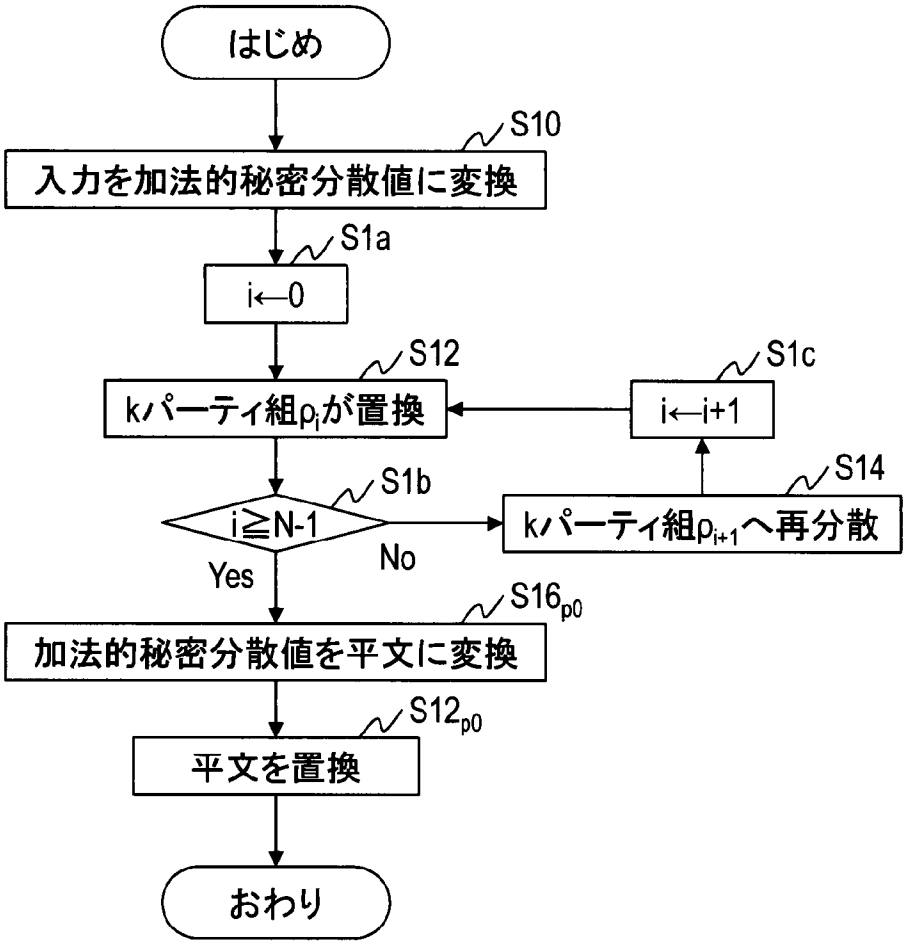

はじめ
S10
入力を加法的秘密分散値に変換
S1a
i←0
S12
kパーティ組ρiが置換
S1c
i←i+1
S1b
i≧N-1
No
S14
kパーティ組ρi+1へ再分散
Yes
S16p0
加法的秘密分散値を平文に変換
S12p0
平文を置換
おわり

図5

[図6]

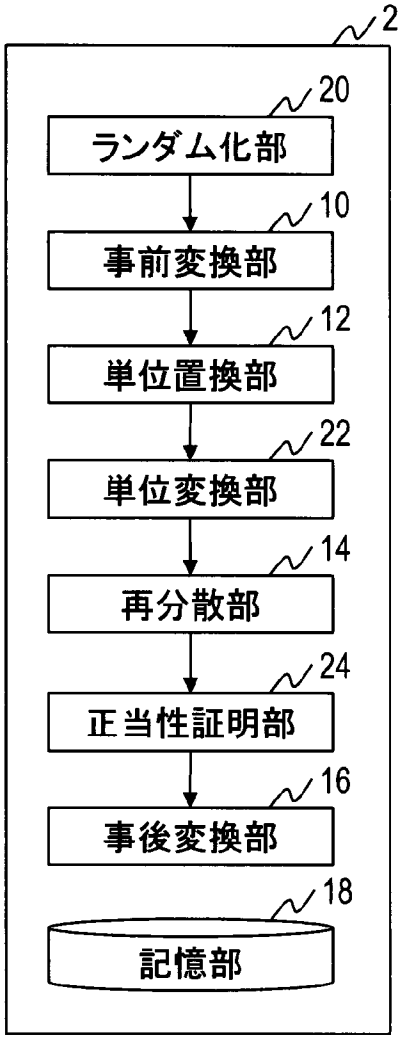

2
20
ランダム化部
10
事前変換部
12
単位置換部
22
単位変換部
14
再分散部
24
正当性証明部
16
事後変換部
18
記憶部

図6

[図7]

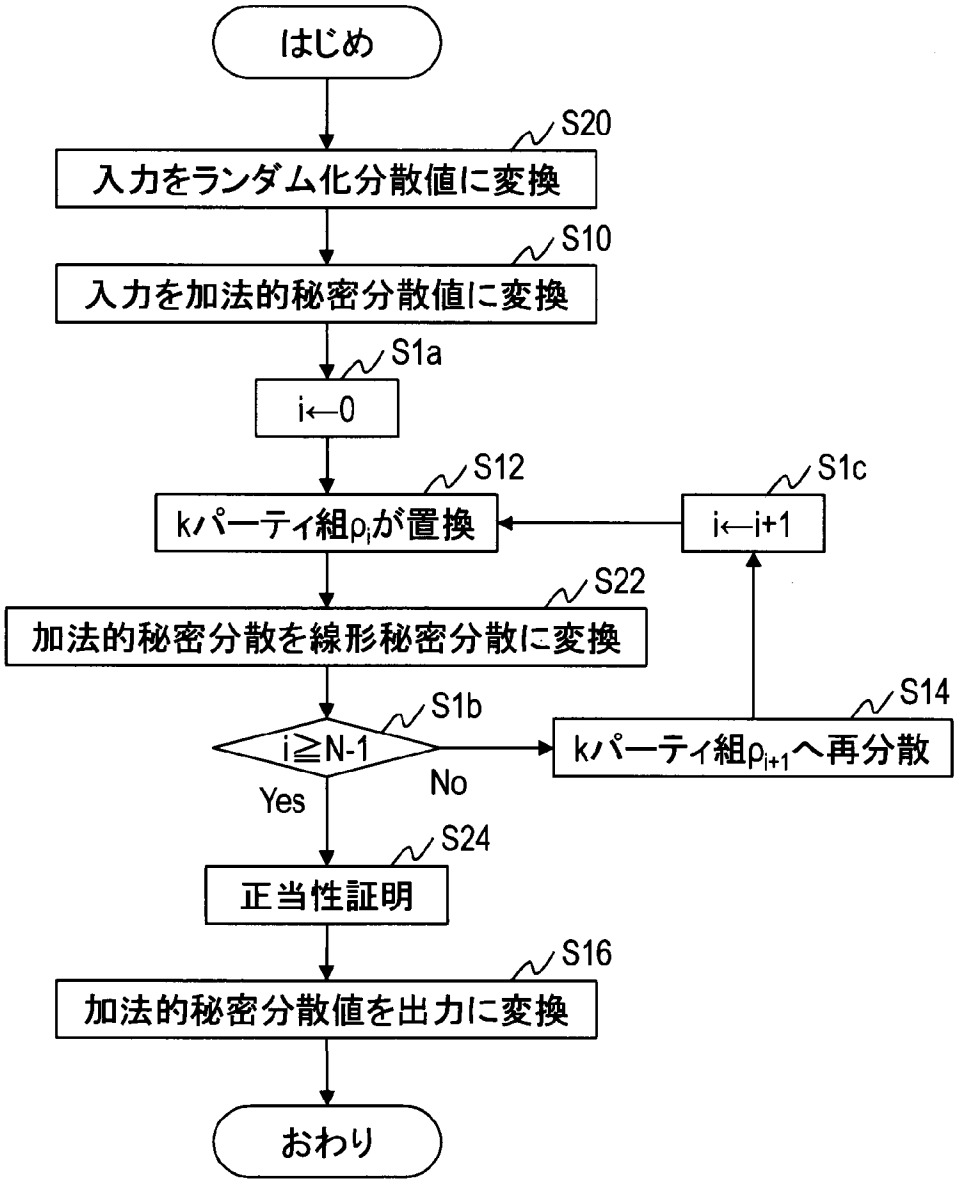

はじめ
S20
入力をランダム化分散値に変換
S10
入力を加法的秘密分散値に変換
S1a
i←0
S12
kパーティ組ρiが置換
S1c
i←i+1
S22
加法的秘密分散を線形秘密分散に変換
S1b
i≧N-1
No
S14
kパーティ組ρi+1へ再分散
Yes
S24
正当性証明
S16
加法的秘密分散値を出力に変換
おわり

図7

[図8]

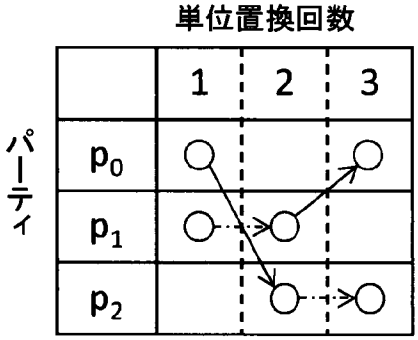

単位置換回数
1
2
3
パーティ
p_0
p_1
p_2

図8

[図9]

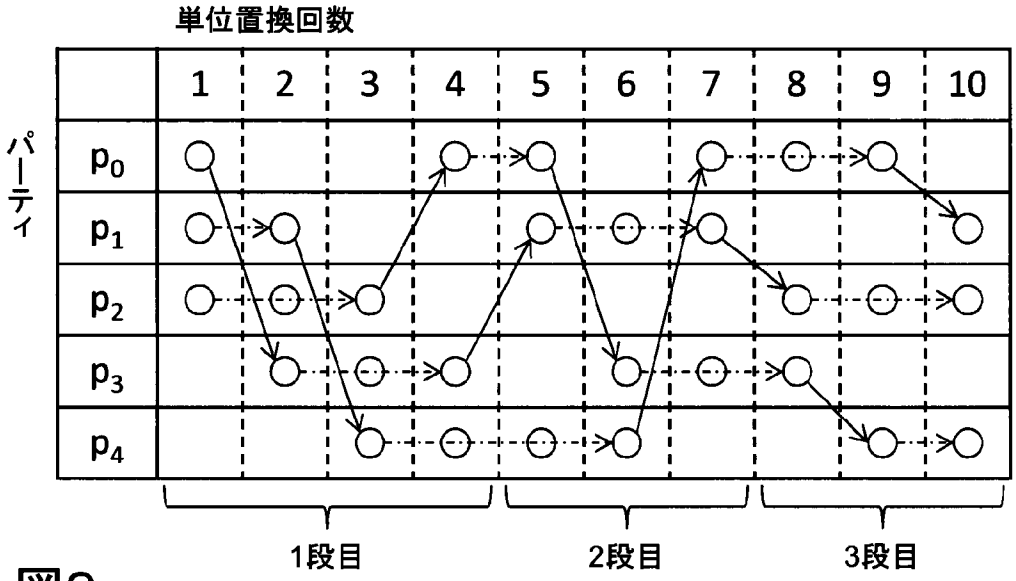

単位置換回数
1
2
3
4
5
6
7
8
9
10
パーティ
p_0
p_1
p_2
p_3
p_4
1段目
2段目
3段目

図9

[図10]

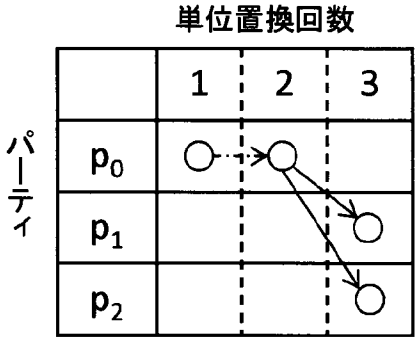


図10

[図11]

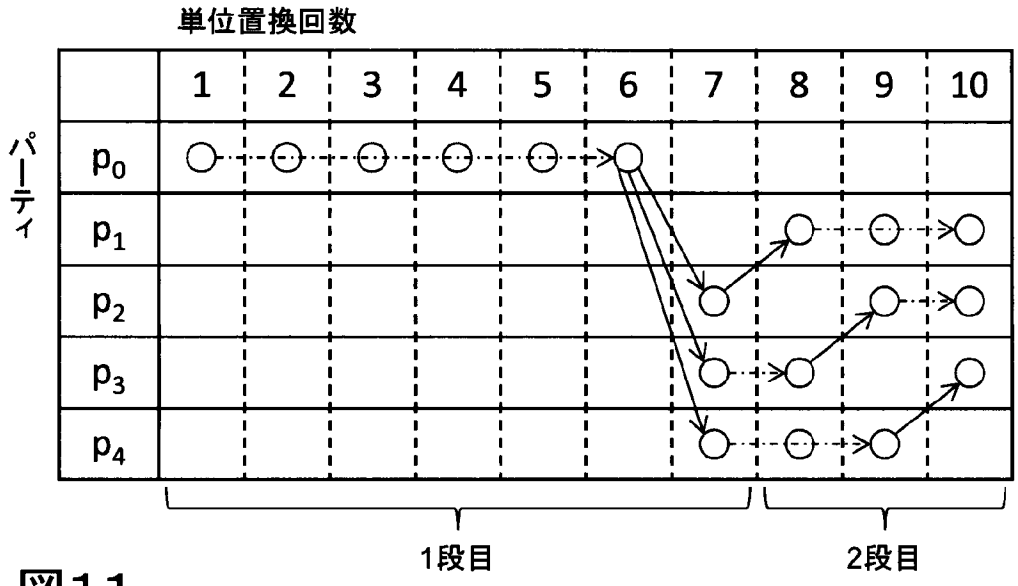


図11

[図12]

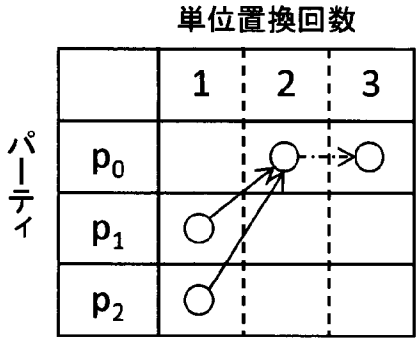


図12

[図13]

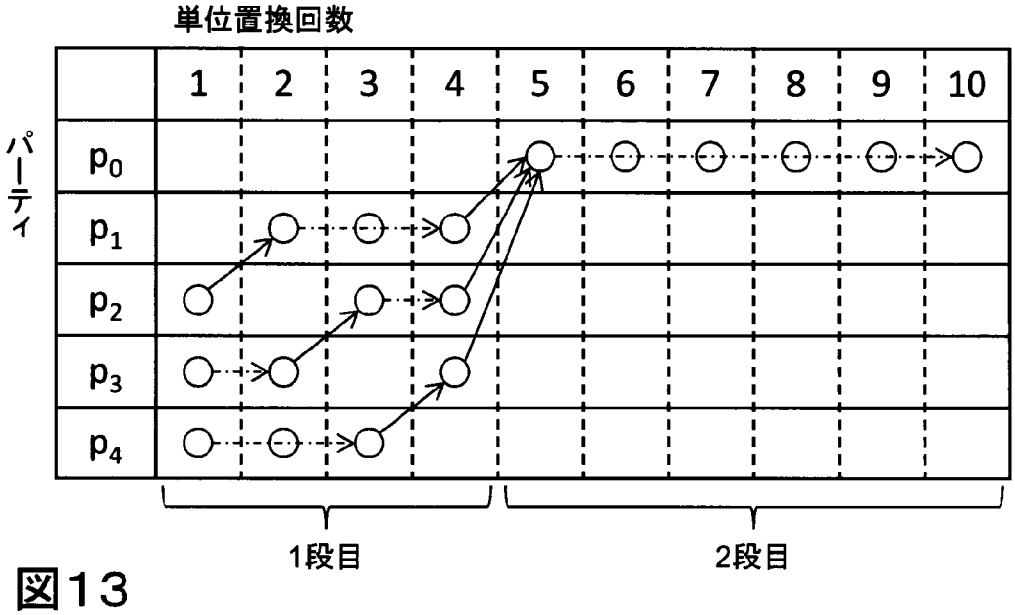


図13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/050231

A. CLASSIFICATION OF SUBJECT MATTER
G09C1/00(2006.01)i, *G06F21/60*(2013.01)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)
G09C1/00, G06F21/60

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2015
Kokai Jitsuyo Shinan Koho	1971-2015	Toroku Jitsuyo Shinan Koho	1994-2015

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamIII), multi-party computation, random permutation

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2003/0046547 A1 (Jakobsson, B. M. and Wetzel, S. G.), 06 March 2003 (06.03.2003), paragraphs [0025] to [0071]	1-10
A	US 6772339 B1 (Lucent Technologies Inc.), 03 August 2004 (03.08.2004), column 3, line 1 to column 8, line 48	1-10
A	JP 5411994 B2 (Nippon Telegraph and Telephone Corp.), 15 November 2013 (15.11.2013), paragraphs [0011] to [0022], [0043] to [0052]	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
28 January 2015 (28.01.15)	10 February 2015 (10.02.15)

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/JP2015/050231

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Laur, S. et al., Round-efficient Oblivious Database Manipulation, Cryptology ePrint Archive:Report 2011/429 [online], 2011.08.12, [retrived on 2015.01.27] Retrieved from the Internet:<URL: https://eprint.iacr.org/2011/429> especially 4 Protocols for Oblivious Shuffle	1-10
P,X	Dai IKARASHI et al., "Internet Kankyo Response 1 Byo no Tokei Shori o Mezashita, Himitsu Keisan Kisu Sort no Kairyo", 2014 Nen Symposium on Cryptography and Information Security Koen Ronbunshu, 21 January 2014 (21.01.2014), particularly, 5.3 Random Chikan Protocol no Kairyo	1-10

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2015/050231

US 2003/0046547 A1	2003.03.06	(Family: none)	
US 6772339 B1	2004.08.03	(Family: none)	
JP 5411994 B2	2013.11.15	US 2013/0182836 A1	2013.07.18
		EP 2608190 A1	2013.06.26
		WO 2012/046692 A1	2012.04.12
		CN 103141056 A	2013.06.05

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１５／０５０２３１

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, G06F21/60(2013.01)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, G06F21/60

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	１９７１－２０１５年
日本国実用新案登録公報	１９９６－２０１５年
日本国登録実用新案公報	１９９４－２０１５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）

JSTPlus/JMEDPlus/JST7580(JDreamⅢ)
multi-party computation, random permutation

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	US 2003/0046547 A1 (Jakobsson, B. M. and Wetzel, S. G.) 2003.03.06, 25-71 段落	1-10
A	US 6772339 B1 (Lucent Technologies Inc.) 2004.08.03, 3 欄 1 行-8 欄 48 行	1-10
A	JP 5411994 B2 (日本電信電話株式会社) 2013.11.15, 11-22, 43-52 段落	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
２８．０１．２０１５	１０．０２．２０１５

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　９３６４
中里　裕正
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	Laur, S. et al., Round-efficient Oblivious Database Manipulation, Cryptology ePrint Archive:Report 2011/429 [online], 2011.08.12, [retrived on 2015.01.27] Retrieved from the Internet:<URL: https://eprint.iacr.org/2011/429> especially 4 Protocols for Oblivious Shuffle	1-10
ＰＸ	五十嵐大 他，インターネット環境レスポンス１秒の統計処理を目指した，秘密計算基数ソートの改良，2014年暗号と情報セキュリティシンポジウム講演論文集，2014.01.21，特に5.3 ランダム置換プロトコルの改良	1-10

US 2003/0046547 A1	2003.03.06	ファミリーなし	
US 6772339 B1	2004.08.03	ファミリーなし	
JP 5411994 B2	2013.11.15	US 2013/0182836 A1	2013.07.18
		EP 2608190 A1	2013.06.26
		WO 2012/046692 A1	2012.04.12
		CN 103141056 A	2013.06.05