(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5411994号
(P5411994)
(45)発行日　平成26年2月12日(2014.2.12)　(24)登録日　平成25年11月15日(2013.11.15)

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

請求項の数 14 (全 25 頁)

(21)出願番号　特願2012-537700 (P2012-537700)
(86)(22)出願日　平成23年10月3日 (2011.10.3)
(86)国際出願番号　PCT/JP2011/072770
(87)国際公開番号　WO2012/046692
(87)国際公開日　平成24年4月12日 (2012.4.12)
審査請求日　平成25年3月19日 (2013.3.19)
(31)優先権主張番号　特願2011-192844 (P2011-192844)
(32)優先日　平成23年9月5日 (2011.9.5)
(33)優先権主張国　日本国 (JP)
(31)優先権主張番号　特願2010-226553 (P2010-226553)
(32)優先日　平成22年10月6日 (2010.10.6)
(33)優先権主張国　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二丁目３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　濱田　浩気
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　五十嵐　大
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
最終頁に続く

(54)【発明の名称】秘密分散システム、秘密分散装置、秘密分散方法、秘密ソート方法、秘密分散プログラム

(57)【特許請求の範囲】
【請求項１】
Ｎ個の秘密分散装置で構成された秘密分散システムであって、
Ｎを３以上の整数、ｎを１以上Ｎ以下の整数、Ｍを１以上の整数、ｍを1以上Ｍ以下の整数、Ｋを２以上の整数、ｋを１以上Ｋ以下の整数、数値$A_1^{(1)}$，…，$A_K^{(1)}$，…，$A_1^{(M)}$，…，$A_K^{(M)}$を各秘密分散装置が断片を分散して記録するＫ×Ｍ個の数値、数値$A_k^{(1)}$，…，$A_k^{(M)}$を対応付けられたｋ番目の数値群、$a_{kn}^{(m)}$をｎ番目の秘密分散装置が記録する数値$A_k^{(m)}$の断片、ｉをＮ個の秘密分散装置の中から選択された秘密分散装置を示すための１以上Ｎ以下の中の一部の整数とし、
２以上Ｎ未満の数の秘密分散装置を選択する選択手段と、
前記選択手段で選択された秘密分散装置の間で｛１，…，Ｋ｝→｛１，…，Ｋ｝の全単射πを作成し、選択されたｉ番目の秘密分散装置が記録する対応付けられたπ（ｋ）番目の数値群の断片$a_{\pi(k)i}^{(1)}$，…，$a_{\pi(k)i}^{(M)}$をそれぞれ対応付けられたｋ番目の数値群の断片にする断片置換手段と、
前記断片置換手段によって置換された数値$A_{\pi(k)}^{(1)}$，…，$A_{\pi(k)}^{(M)}$に対応する断片$a_{\pi(k)i}^{(1)}$，…，$a_{\pi(k)i}^{(M)}$を用いて再分散化して新しい断片$b_{k1}^{(1)}$，…，$b_{kN}^{(1)}$，…，$b_{k1}^{(M)}$，…，$b_{kN}^{(M)}$を求め、数値$B_k^{(1)}$，…，$B_k^{(M)}$の断片とする再分散手段と、
を備える秘密分散システム。
【請求項２】

請求項１記載の秘密分散システムであって、
Ｍ＝１である秘密分散システム。
【請求項３】
請求項２記載の秘密分散システムであって、
Ｎ個の秘密分散装置のどれも知らないＫ個の数値P_1，…，P_Kそれぞれの断片を秘密計算によって求め、ｎ番目の秘密分散装置に断片p_{1n}，…，p_{Kn}を記録する初期情報分散手段と、
Ｎ個の秘密分散装置で、$S_k = P_k \times A_k^{(1)}$である数値$S_k$の断片$s_{k1}$，…，$s_{kN}$を秘密計算によって求め、Ｎ個の秘密分散装置に分散して記録する初期乗算手段と、
ｋ＝１～Ｋについて、$Q_k = P_{\pi(k)}$である数値Q_kの断片q_{k1}，…，q_{kN}を秘密計算によって生成し、Ｎ個の秘密分散装置に分散して記録する確認分散手段と、
Ｎ個の秘密分散装置で、$T_k = Q_k \times B_k^{(1)}$である数値$T_k$の断片$t_{k1}$，…，$t_{kN}$を秘密計算によって求め、Ｎ個の秘密分散装置に分散して記録する確認乗算手段と、
ｋ＝１～Ｋについて、$T_k = S_{\pi(k)}$であることを確認する改ざん検出手段、
も備える秘密分散システム。
【請求項４】
請求項１記載の秘密分散システムであって、
Ｎ＝３、（α，β，γ）を（１，２，３）と（２，３，１）と（３，１，２）のいずれかの組み合わせ、数値$A_k^{(m)} = a_{k\alpha\beta}^{(m)} + a_{k\beta\gamma}^{(m)} + a_{k\gamma\alpha}^{(m)}$の３つの断片を（$a_{k\gamma\alpha}^{(m)}$，$a_{k\alpha\beta}^{(m)}$）と（$a_{k\alpha\beta}^{(m)}$，$a_{k\beta\gamma}^{(m)}$）と（$a_{k\beta\gamma}^{(m)}$，$a_{k\gamma\alpha}^{(m)}$）、前記の３つの断片は３つの秘密分散装置に分散して記録されているとし、
前記選択手段は、２つの秘密分散装置を選択し、選択された秘密分散装置の一方を第１の秘密分散装置、他方を第２の秘密分散装置、選択されなかった秘密分散装置を第３の秘密分散装置とし、
前記断片置換手段は、第１の秘密分散装置が記録する数値$A_k^{(m)}$の断片を$a_{k1}^{(m)} = (a_{k31}^{(m)}, a_{k12}^{(m)})$、第２の秘密分散装置が記録する数値$A_k^{(m)}$の断片を$a_{k2}^{(m)} = (a_{k12}^{(m)}, a_{k23}^{(m)})$、第３の秘密分散装置が記録する数値$A_k^{(m)}$の断片を$a_{k3}^{(m)} = (a_{k23}^{(m)}, a_{k31}^{(m)})$とし、第１の秘密分散装置または第２の秘密分散装置で｛１，…，Ｋ｝→｛１，…，Ｋ｝の全単射πを作成し、第１の秘密分散装置が記録する対応付けられたπ（ｋ）番目の数値群の断片$a_{\pi(k)1}^{(1)}$，…，$a_{\pi(k)1}^{(M)}$を対応付けられたｋ番目の数値群の断片にし、第２の秘密分散装置が記録する対応付けられたπ（ｋ）番目の数値群の断片$a_{\pi(k)2}^{(1)}$，…，$a_{\pi(k)2}^{(M)}$を対応付けられたｋ番目の数値群の断片にし、
前記再分散手段として、各秘密分散装置が、
第１の秘密分散装置のときには、対応付けられたｋ番目の数値群の断片の再分散化のために、ランダムな値である$b_{k31}^{(1)}$，…，$b_{k31}^{(M)}$を生成し、第３の秘密分散装置に送信する第１乱数生成部と、
第２の秘密分散装置のときには、対応付けられたｋ番目の数値群の断片の再分散化のために、ランダムな値である$b_{k23}^{(1)}$，…，$b_{k23}^{(M)}$を生成し、第３の秘密分散装置に送信する第２乱数生成部と、
第１の秘密分散装置のときには、対応付けられたｋ番目の数値群の断片の再分散化のために、ｍ＝１～Ｍについて$x_k^{(m)} = b_{k31}^{(m)} - a_{\pi(k)31}^{(m)}$を計算し、$x_k^{(1)}$，…，$x_k^{(M)}$を第２の秘密分散装置に送信する第１計算部と、
第２の秘密分散装置のときには、対応付けられたｋ番目の数値群の断片の再分散化のために、ｍ＝１～Ｍについて$y_k^{(m)} = b_{k23}^{(m)} - a_{\pi(k)23}^{(m)}$を計算し、$y_k^{(1)}$，…，$y_k^{(M)}$を第１の秘密分散装置に送信する第２計算部と、
第１の秘密分散装置または第２の秘密分散装置のときには、対応付けられたｋ番目の数値群の断片の再分散化のために、ｍ＝１～Ｍについて$b_{k12}^{(m)} = a_{\pi(k)12}^{(}$

$^{(m)}-x_k^{(m)}-y_k^{(m)}$を計算する第３計算部と、
第１の秘密分散装置のときには（$b_{k31}^{(m)}$，$b_{k12}^{(m)}$）を断片$b_{k1}^{(m)}$とし、第２の秘密分散装置のときには（$b_{k12}^{(m)}$，$b_{k23}^{(m)}$）を断片$b_{k2}^{(m)}$とし、第３の秘密分散装置のときには（$b_{k23}^{(m)}$，$b_{k31}^{(m)}$）を断片$b_{k3}^{(m)}$とする断片更新部と、
を備え、断片$b_{k1}^{(m)}$、$b_{k2}^{(m)}$、$b_{k3}^{(m)}$を数値$B_k^{(m)}$の断片として記録する
秘密分散システム。
【請求項５】
請求項４記載の秘密分散システムであって、
Ｍ＝１である秘密分散システム。
【請求項６】
請求項５記載の秘密分散システムであって、
第１の秘密分散装置でＫ個のランダムな値$R^{(1)}{}_1$，…，$R^{(1)}{}_K$を生成し、第２の秘密分散装置でＫ個のランダムな値$R^{(2)}{}_1$，…，$R^{(2)}{}_K$を生成し、前記３つの秘密分散装置で、$R^{(1)}{}_k$の断片（$r^{(1)}{}_{k31}$，$r^{(1)}{}_{k12}$）、（$r^{(1)}{}_{k12}$，$r^{(1)}{}_{k23}$）、（$r^{(1)}{}_{k23}$，$r^{(1)}{}_{k31}$）と、$R^{(2)}{}_k$の断片（$r^{(2)}{}_{k31}$，$r^{(2)}{}_{k12}$）、（$r^{(2)}{}_{k12}$，$r^{(2)}{}_{k23}$）、（$r^{(2)}{}_{k23}$，$r^{(2)}{}_{k31}$）とを秘密分散して記録し、前記３つの秘密分散装置で、$P_k=R^{(1)}{}_k+R^{(2)}{}_k$である数値$P_k$の断片（$p_{k31}$，$p_{k12}$）、（$p_{k12}$，$p_{k23}$）、（$p_{k23}$，$p_{k31}$）を秘密計算によって求め、前記３つの秘密分散装置に分散して記録する初期情報分散手段と、
前記３つの秘密分散装置で、$S_k=P_k\times A_k^{(1)}$である数値S_kの断片（s_{k31}，s_{k12}）、（s_{k12}，s_{k23}）、（s_{k23}，s_{k31}）を秘密計算によって求め、前記３つの秘密分散装置に分散して記録する初期乗算手段と、
前記の数値$R^{(1)}{}_{\pi(k)}$の別の断片（$r'^{(1)}{}_{\pi(k)31}$，$r'^{(1)}{}_{\pi(k)12}$）、（$r'^{(1)}{}_{\pi(k)12}$，$r'^{(1)}{}_{\pi(k)23}$）、（$r'^{(1)}{}_{\pi(k)23}$，$r'^{(1)}{}_{\pi(k)31}$）と、前記の数値$R^{(2)}{}_{\pi(k)}$の別の断片（$r'^{(2)}{}_{\pi(k)31}$，$r'^{(2)}{}_{\pi(k)12}$）、（$r'^{(2)}{}_{\pi(k)12}$，$r'^{(2)}{}_{\pi(k)23}$）、（$r'^{(2)}{}_{\pi(k)23}$，$r'^{(2)}{}_{\pi(k)31}$）とを前記３つの秘密分散装置に分散して記録し、前記３つの秘密分散装置で、$Q_k=R^{(1)}{}_{\pi(k)}+R^{(2)}{}_{\pi(k)}$である数値$Q_k$の断片（$q_{k31}$，$q_{k12}$）、（$q_{k12}$，$q_{k23}$）、（$q_{k23}$，$q_{k31}$）を当該別の断片を用いて秘密計算によって求め、前記３つの秘密分散装置に分散して記録する確認分散手段と、
前記３つの秘密分散装置で、$T_k=Q_k\times B_k^{(1)}$である数値T_kの断片（t_{k31}，t_{k12}）、（t_{k12}，t_{k23}）、（t_{k23}，t_{k31}）を秘密計算によって求め、前記３つの秘密分散装置に分散して記録する確認乗算手段と、
第１の秘密分散装置が記録する断片を$s_{k1}=(s_{k31},s_{k12})$、$t_{k1}=(t_{k31},t_{k12})$とし、第２の秘密分散装置が記録する断片を$s_{k2}=(s_{k12},s_{k23})$、$t_{k2}=(t_{k12},t_{k23})$とし、第３の秘密分散装置が記録する断片を$s_{k3}=(s_{k23},s_{k31})$、$t_{k3}=(t_{k23},t_{k31})$とし、
各秘密分散装置が、
第１の秘密分散装置のときに、ランダムな値であるu_kを生成し、第２の秘密分散装置に送信する第３乱数生成部と、
第２の秘密分散装置のときに、ランダムな値であるv_kを生成し、第１の秘密分散装置に送信する第４乱数生成部と、
第１の秘密分散装置のときに、$d_k=s_{\pi(k)12}-t_{k12}-u_k-v_k$を計算し、第３の秘密分散装置に送信する第４計算部と、
第２の秘密分散装置のときに、$e_k=s_{\pi(k)12}-t_{k12}-u_k-v_k$を計算し、第３の秘密分散装置に送信する第５計算部と、

第３の秘密分散装置のときに、$d_k = e_k$であることを確認し、異なっていれば処理を中止する第１確認部と、
第１の秘密分散装置のときに、$f_k = s_{\pi(k)31} - t_{k31} + u_k$を計算し、第３の秘密分散装置に送信する第６計算部と、
第２の秘密分散装置のときに、$g_k = s_{\pi(k)23} - t_{k23} + v_k$を計算し、第３の秘密分散装置に送信する第７計算部と、
第３の秘密分散装置のときに、$f_k + g_k + d_k = 0$であることを確認し、異なっていれば処理を中止する第２確認部と、
を備える
秘密分散システム。

【請求項７】
請求項４記載の秘密分散システムの中の秘密分散装置であって、
第１の秘密分散装置として選ばれたときには記録する数値$A_k^{(m)}$の断片を$a_{k1}^{(m)} = (a_{k31}^{(m)}, a_{k12}^{(m)})$、第２の秘密分散装置として選ばれたときには記録する数値$A_k^{(m)}$の断片を$a_{k2}^{(m)} = (a_{k12}^{(m)}, a_{k23}^{(m)})$、第３の秘密分散装置として選ばれたときには記録する数値$A_k^{(m)}$の断片を$a_{k3}^{(m)} = (a_{k23}^{(m)}, a_{k31}^{(m)})$とし、
第１の秘密分散装置または第２の秘密分散装置として選ばれたときは、$\{1, \cdots, K\} \rightarrow \{1, \cdots, K\}$の全単射πを作成し、対応付けられたπ（ｋ）番目の数値群の断片を対応付けられたｋ番目の数値群の断片にする断片置換部と、
第１の秘密分散装置のときには、対応付けられたｋ番目の数値群の断片の再分散化のために、ランダムな値である$b_{k31}^{(1)}, \cdots, b_{k31}^{(M)}$を生成し、第３の秘密分散装置に送信する第１乱数生成部と、
第２の秘密分散装置のときには、対応付けられたｋ番目の数値群の断片の再分散化のために、ランダムな値である$b_{k23}^{(1)}, \cdots, b_{k23}^{(M)}$を生成し、第３の秘密分散装置に送信する第２乱数生成部と、
第１の秘密分散装置のときには、対応付けられたｋ番目の数値群の断片の再分散化のために、ｍ＝１～Ｍについて$x_k^{(m)} = b_{k31}^{(m)} - a_{\pi(k)31}^{(m)}$を計算し、$x_k^{(1)}, \cdots, x_k^{(M)}$を第２の秘密分散装置に送信する第１計算部と、
第２の秘密分散装置のときには、対応付けられたｋ番目の数値群の断片の再分散化のために、ｍ＝１～Ｍについて$y_k^{(m)} = b_{k23}^{(m)} - a_{\pi(k)23}^{(m)}$を計算し、$y_k^{(1)}, \cdots, y_k^{(M)}$を第１の秘密分散装置に送信する第２計算部と、
第１の秘密分散装置または第２の秘密分散装置のときには、対応付けられたｋ番目の数値群の断片の再分散化のために、ｍ＝１～Ｍについて$b_{k12}^{(m)} = a_{\pi(k)12}^{(m)} - x_k^{(m)} - y_k^{(m)}$を計算する第３計算部と、
第１の秘密分散装置のときには$(b_{k31}^{(m)}, b_{k12}^{(m)})$を断片$b_{k1}^{(m)}$とし、第２の秘密分散装置のときには$(b_{k12}^{(m)}, b_{k23}^{(m)})$を断片$b_{k2}^{(m)}$とし、第３の秘密分散装置のときには$(b_{k23}^{(m)}, b_{k31}^{(m)})$を断片$b_{k3}^{(m)}$とする断片更新部と、
を備える秘密分散装置。

【請求項８】
請求項７記載の秘密分散装置であって、
Ｍ＝１である秘密分散装置。

【請求項９】
Ｋを２以上の整数、ｋを１以上Ｋ以下の整数、Ｍを１以上Ｍ以下の整数、ｍを１以上Ｍ以下の整数、$A_1^{(1)}, \cdots, A_K^{(1)}, \cdots, A_1^{(M)}, \cdots, A_K^{(M)}$をＫ×Ｍ個の数値、（α，β，γ）を（１，２，３）と（２，３，１）と（３，１，２）のいずれかの組み合わせ、数値$A_k^{(m)} = a_{k\alpha\beta}^{(m)} + a_{k\beta\gamma}^{(m)} + a_{k\gamma\alpha}^{(m)}$の３つの断片を$(a_{k\gamma\alpha}^{(m)}, a_{k\alpha\beta}^{(m)})$と$(a_{k\alpha\beta}^{(m)}, a_{k\beta\gamma}^{(m)})$と$(a_{k\beta\gamma}^{(m)}, a_{k\gamma\alpha}^{(m)})$、対応付けられたｋ番目の数値群を$A_k^{(1)}, \cdots, A$

$_k{}^{(M)}$とし、前記断片を分散して記録する３つの秘密分散装置を用いた秘密分散方法であって、

２つの秘密分散装置を選択し、選択された秘密分散装置の一方を第１の秘密分散装置、他方を第２の秘密分散装置、選択されなかった秘密分散装置を第３の秘密分散装置する選択ステップと、

第１の秘密分散装置が記録する数値$A_k{}^{(m)}$の断片を$a_{k1}{}^{(m)}=(a_{k31}{}^{(m)}, a_{k12}{}^{(m)})$、第２の秘密分散装置が記録する数値$A_k{}^{(m)}$の断片を$a_{k2}{}^{(m)}=(a_{k12}{}^{(m)}, a_{k23}{}^{(m)})$、第３の秘密分散装置が記録する数値$A_k{}^{(m)}$の断片を$a_{k3}{}^{(m)}=(a_{k23}{}^{(m)}, a_{k31}{}^{(m)})$とし、第１の秘密分散装置または第２の秘密分散装置で$\{1, \cdots, K\} \rightarrow \{1, \cdots, K\}$の全単射πを作成し、第１の秘密分散装置が記録する対応付けられたπ（ｋ）番目の数値群の断片$a_{\pi(k)1}{}^{(1)}, \cdots, a_{\pi(k)1}{}^{(M)}$を対応付けられたｋ番目の数値群の断片にし、第２の秘密分散装置が記録する対応付けられたπ（ｋ）番目の数値群の断片$a_{\pi(k)2}{}^{(1)}, \cdots, a_{\pi(k)2}{}^{(M)}$を対応付けられたｋ番目の数値群の断片にする断片置換ステップと、

第１の秘密分散装置が、対応付けられたｋ番目の数値群の断片の再分散化のために、ランダムな値である$b_{k31}{}^{(1)}, \cdots, b_{k31}{}^{(M)}$を生成し、第３の秘密分散装置に送信する第１乱数生成ステップと、

第２の秘密分散装置が、対応付けられたｋ番目の数値群の断片の再分散化のために、ランダムな値である$b_{k23}{}^{(1)}, \cdots, b_{k23}{}^{(M)}$を生成し、第３の秘密分散装置に送信する第２乱数生成ステップと、

第１の秘密分散装置が、対応付けられたｋ番目の数値群の断片の再分散化のために、ｍ＝１～Ｍについて$x_k{}^{(m)}=b_{k31}{}^{(m)}-a_{\pi(k)31}{}^{(m)}$を計算し、$x_k{}^{(1)}, \cdots, x_k{}^{(M)}$を第２の秘密分散装置に送信する第１計算ステップと、

第２の秘密分散装置が、対応付けられたｋ番目の数値群の断片の再分散化のために、ｍ＝１～Ｍについて$y_k{}^{(m)}=b_{k23}{}^{(m)}-a_{\pi(k)23}{}^{(m)}$を計算し、$y_k{}^{(1)}, \cdots, y_k{}^{(M)}$を第１の秘密分散装置に送信する第２計算ステップと、

第１の秘密分散装置と第２の秘密分散装置が、対応付けられたｋ番目の数値群の断片の再分散化のために、ｍ＝１～Ｍについて$b_{k12}{}^{(m)}=a_{\pi(k)12}{}^{(m)}-x_k{}^{(m)}-y_k{}^{(m)}$を計算する第３計算ステップと、

第１の秘密分散装置が$(b_{k31}{}^{(m)}, b_{k12}{}^{(m)})$を断片$b_{k1}{}^{(m)}$とし、第２の秘密分散装置が$(b_{k12}{}^{(m)}, b_{k23}{}^{(m)})$を断片$b_{k2}{}^{(m)}$とし、第３の秘密分散装置が$(b_{k23}{}^{(m)}, b_{k31}{}^{(m)})$を断片$b_{k3}{}^{(m)}$とする断片更新ステップと、

を有する秘密分散方法。

【請求項１０】

請求項９記載の秘密分散方法であって、

Ｍ＝１である秘密分散方法。

【請求項１１】

請求項１０記載の秘密分散方法であって、

第１の秘密分散装置がＫ個のランダムな値$R^{(1)}{}_1, \cdots, R^{(1)}{}_K$を生成し、第２の秘密分散装置がＫ個のランダムな値$R^{(2)}{}_1, \cdots, R^{(2)}{}_K$を生成し、前記３つの秘密分散装置が$R^{(1)}{}_k$の断片$(r^{(1)}{}_{k31}, r^{(1)}{}_{k12})$、$(r^{(1)}{}_{k12}, r^{(1)}{}_{k23})$、$(r^{(1)}{}_{k23}, r^{(1)}{}_{k31})$と$R^{(2)}{}_k$の断片$(r^{(2)}{}_{k31}, r^{(2)}{}_{k12})$、$(r^{(2)}{}_{k12}, r^{(2)}{}_{k23})$、$(r^{(2)}{}_{k23}, r^{(2)}{}_{k31})$とを秘密分散して記録し、前記３つの秘密分散装置が$P_k=R^{(1)}{}_k+R^{(2)}{}_k$である数値$P_k$の断片$(p_{k31}, p_{k12})$、$(p_{k12}, p_{k23})$、$(p_{k23}, p_{k31})$を秘密計算によって求め、前記３つの秘密分散装置に分散して記録する初期情報分散ステップと、

前記３つの秘密分散装置が、$S_k=P_k \times A_k{}^{(1)}$である数値$S_k$の断片（$s_{k31}$

，s_{k12}）、（s_{k12}，s_{k23}）、（s_{k23}，s_{k31}）を秘密計算によって求め、前記３つの秘密分散装置に分散して記録する初期乗算ステップと、

前記３つの秘密分散装置が、請求項１０記載の秘密分散システムによって得られた断片b_{k1}、b_{k2}、b_{k3}を数値$B_k^{(1)}$の断片として記録する秘密分散更新ステップと、

前記の数値$R^{(1)}_{\pi(k)}$の別の断片（$r'^{(1)}_{\pi(k)31}$，$r'^{(1)}_{\pi(k)12}$）、（$r'^{(1)}_{\pi(k)12}$，$r'^{(1)}_{\pi(k)23}$）、（$r'^{(1)}_{\pi(k)23}$，$r'^{(1)}_{\pi(k)31}$）と、前記の数値$R^{(2)}_{\pi(k)}$の別の断片（$r'^{(2)}_{\pi(k)31}$，$r'^{(2)}_{\pi(k)12}$）、（$r'^{(2)}_{\pi(k)12}$，$r'^{(2)}_{\pi(k)23}$）、（$r'^{(2)}_{\pi(k)23}$，$r'^{(2)}_{\pi(k)31}$）とを前記３つの秘密分散装置に分散して記録し、前記３つの秘密分散装置で、$Q_k = R^{(1)}_{\pi(k)} + R^{(2)}_{\pi(k)}$である数値$Q_k$の断片（$q_{k31}$，$q_{k12}$）、（$q_{k12}$，$q_{k23}$）、（$q_{k23}$，$q_{k31}$）を当該別の断片を用いて秘密計算によって求め、前記３つの秘密分散装置に分散して記録する確認分散ステップと、

前記３つの秘密分散装置が、$T_k = Q_k \times B_k^{(1)}$である数値$T_k$の断片（$t_{k31}$，$t_{k12}$）、（$t_{k12}$，$t_{k23}$）、（$t_{k23}$，$t_{k31}$）を秘密計算によって求め、前記３つの秘密分散装置に分散して記録する確認乗算ステップと、

第１の秘密分散装置が記録する断片をs_{k1}＝（s_{k31}，s_{k12}）、t_{k1}＝（t_{k31}，t_{k12}）とし、第２の秘密分散装置が記録する断片をs_{k2}＝（s_{k12}，s_{k23}）、t_{k2}＝（t_{k12}，t_{k23}）とし、第３の秘密分散装置が記録する断片をs_{k3}＝（s_{k23}，s_{k31}）、t_{k3}＝（t_{k23}，t_{k31}）とし、

第１の秘密分散装置が、ランダムな値であるu_kを生成し、第２の秘密分散装置に送信する第３乱数生成ステップと、

第２の秘密分散装置が、ランダムな値であるv_kを生成し、第１の秘密分散装置に送信する第４乱数生成ステップと、

第１の秘密分散装置が、$d_k = s_{\pi(k)12} - t_{k12} - u_k - v_k$を計算し、第３の秘密分散装置に送信する第４計算ステップと、

第２の秘密分散装置が、$e_k = s_{\pi(k)12} - t_{k12} - u_k - v_k$を計算し、第３の秘密分散装置に送信する第５計算ステップと、

第３の秘密分散装置が、$d_k = e_k$であることを確認し、異なっていれば処理を中止する第１確認ステップと、

第１の秘密分散装置が、$f_k = s_{\pi(k)31} - t_{k31} + u_k$を計算し、第３の秘密分散装置に送信する第６計算ステップと、

第２の秘密分散装置が、$g_k = s_{\pi(k)23} - t_{k23} + v_k$を計算し、第３の秘密分散装置に送信する第７計算ステップと、

第３の秘密分散装置が、$f_k + g_k + d_k = 0$であることを確認し、異なっていれば処理を中止する第２確認ステップと、

を有する秘密分散方法。

【請求項１２】

請求項９から１１のいずれかに記載の秘密分散方法であって、

前記断片更新ステップで得られた断片$b_{k1}^{(m)}$、$b_{k2}^{(m)}$、$b_{k3}^{(m)}$を新しい断片$a_{k1}^{(m)}$、$a_{k2}^{(m)}$、$a_{k3}^{(m)}$とし、

前記断片置換ステップで、あらかじめ定めた全ての組合せで前記秘密分散装置を選択するまで、前記の秘密分散方法を繰り返す

ことを特徴とする秘密分散方法。

【請求項１３】

請求項１２記載の秘密分散方法を用いた秘密ソート方法であって、

請求項１２記載の秘密分散方法によって断片を分散して記録した複数の数値に対して、

３つの秘密分散装置が、２つの数値を選択し、当該２つの数値の大小を秘密計算によって比較する比較ステップと、

秘密分散装置のそれぞれが、前記比較ステップの結果に基づいて数値の断片を入れ替える交換ステップと、
を有する秘密ソート方法。
【請求項１４】
請求項１から６のいずれかに記載の秘密分散システムの各秘密分散装置としてコンピュータを機能させる秘密分散プログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号応用技術に関するものであり、特に入力データを明かすことなく関数計算を行う秘密分散システム、秘密分散装置、秘密分散方法、秘密ソート方法、秘密分散プログラムに関する。
【背景技術】
【０００２】
暗号化された数値を復元すること無く特定の演算結果を得る方法として、秘密計算と呼ばれる方法がある(例えば、非特許文献１に記載された方法)。非特許文献１の方法では、３つの秘密計算装置に数値の断片を分散させ、数値を復元すること無く、加減算、定数和、乗算、定数倍、論理演算(否定，論理積，論理和，排他的論理和)、データ形式変換(整数,二進数)の結果を３つの秘密計算装置に分散保持させることができる。
【先行技術文献】
【非特許文献】
【０００３】
【非特許文献１】千田浩司，五十嵐大，高橋克巳，“効率的な３パーティ秘匿関数計算の提案とその運用モデルの考察”，第48回情報処理学会研究報告，CSEC，pp.1-7，2010，3月.
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、従来技術はデータの対応を隠したまま複数のデータをランダムに置換できないという課題がある。本発明の目的は、入力された複数のデータと対応つけることができないデータを出力する秘密計算技術を提供することである。
【課題を解決するための手段】
【０００５】
本発明は秘密分散に関する。一般に、（ｋ，ｎ）－秘密分散では、秘密分散システムが２つのパラメータｋ，ｎを持っており、秘密にしたい値をｎ個に分割し、そのうちｋ個未満を集めても元の値に関する情報は漏れないが、ｋ個以上を集めると元の値を復元できる。本発明の秘密分散システムは、Ｎ個の秘密分散装置R_1，…，R_Nで構成される。ここで、Ｎを３以上の整数、ｎを１以上Ｎ以下の整数、Ｍを１以上の整数、ｍを1以上Ｍ以下の整数、Ｋを２以上の整数、ｋを１以上Ｋ以下の整数、数値$A_1^{(1)}$，…，$A_K^{(1)}$，…，$A_1^{(M)}$，…，$A_K^{(M)}$を各秘密分散装置が断片を分散して記録するＫ×Ｍ個の数値、数値$A_k^{(1)}$，…，$A_k^{(M)}$を対応付けられたｋ番目の数値群、$a_{kn}^{(m)}$をｎ番目の秘密分散装置が記録する数値$A_k^{(m)}$の断片とする。本発明の秘密分散システムは、選択手段と断片置換手段と再分散手段を備える。選択手段は、２以上Ｎ未満の数の秘密分散装置を選択する。断片置換手段は、選択された秘密分散装置の間で｛１，…，Ｋ｝→｛１，…，Ｋ｝の全単射πを作成し、選択された秘密分散装置R_i（ただし、ｉは選択された秘密分散装置を示す番号）が記録する対応付けられたπ（ｋ）番目の数値群の断片$a_{\pi(k)i}^{(1)}$，…，$a_{\pi(k)i}^{(M)}$をそれぞれ対応付けられたｋ番目の数値群の断片にする。再分散手段は、断片置換手段によって置換された数値$A_{\pi(k)}^{(1)}$，…，$A_{\pi(k)}^{(M)}$に対応する断片$a_{\pi(k)i}^{(1)}$，…，$a_{\pi(k)i}^{(M}$

）を用いて再分散化して新しい断片$b_{k1}^{(1)}$，…，$b_{kN}^{(1)}$，…，$b_{k1}^{(M)}$，…，$b_{kN}^{(M)}$を求める（以下、これを「再分散化」と呼ぶ）。なお、対応つけられた数値群の対応を維持したまま数値群を再分散化する場合は、同一の全単射πを用いて、対応つけられた数値群の各数値の断片を置換すればよい。

【０００６】

また、本発明の秘密分散システムは、初期情報分散手段、初期乗算手段、確認分散手段、確認乗算手段、改ざん検出手段も備えてもよい。初期情報分散手段は、秘密分散装置R_1，…，R_Nのどれも知らないＫ個の数値P_1，…，P_Kそれぞれの断片p_{1n}，…，p_{Kn}を秘密計算によって求め、秘密分散装置R_nに記録させる。初期乗算手段は、秘密分散装置R_1，…，R_Nで、$S_k=P_k\times A_k^{(1)}$である数値S_kの断片s_{k1}，…，s_{kN}を秘密計算によって求め、秘密分散装置R_1，…，R_Nに分散して記録する。確認分散手段は、ｋ＝１～Ｋについて、$Q_k=P_{\pi(k)}$である数値Q_kの断片q_{k1}，…，q_{kN}を秘密計算によって生成し、秘密分散装置R_1，…，R_Nに分散して記録させる。確認乗算手段は、秘密分散装置R_1，…，R_Nで、$T_k=Q_k\times B_k^{(1)}$である数値T_kの断片t_{k1}，…，t_{kN}を秘密計算によって求め、秘密分散装置R_1，…，R_Nに分散して記録する。改ざん検出手段は、ｋ＝１～Ｋについて、$T_k=S_{\pi(k)}$であることを確認する。

【０００７】

例えば、３つの秘密分散装置で構成する場合であれば、ｋ番目の対応つけられた数値群のｍ番目の数値$A_k^{(m)}=a_{k\alpha\beta}^{(m)}+a_{k\beta\gamma}^{(m)}+a_{k\gamma\alpha}^{(m)}$（ただし、（α，β，γ）は、（１，２，３）、（２，３，１）、（３，１，２）のいずれか）の３つの断片を（$a_{k\gamma\alpha}^{(m)}$，$a_{k\alpha\beta}^{(m)}$）、（$a_{k\alpha\beta}^{(m)}$，$a_{k\beta\gamma}^{(m)}$）、（$a_{k\beta\gamma}^{(m)}$，$a_{k\gamma\alpha}^{(m)}$）とする。秘密分散装置が、第１の秘密分散装置として選ばれたときには記録する断片を$a_{k1}^{(m)}=(a_{k31}^{(m)},a_{k12}^{(m)})$、第２の秘密分散装置として選ばれたときには記録する断片を$a_{k2}^{(m)}=(a_{k12}^{(m)},a_{k23}^{(m)})$、第３の秘密分散装置として選ばれたときには記録する断片を$a_{k3}^{(m)}=(a_{k23}^{(m)},a_{k31}^{(m)})$とする。そして、各秘密分散装置は、断片置換部、第１乱数生成部、第２乱数生成部、第１計算部、第２計算部、第３計算部、断片更新部を備えればよい。断片置換部は、第１の秘密分散装置または第２の秘密分散装置として選ばれたときは、｛１，…，Ｋ｝→｛１，…，Ｋ｝の全単射πを作成し、π（ｋ）番目の対応つけられた数値群の各数値の断片をｋ番目の対応つけられた数値群の各数値の断片にする。第１乱数生成部は、第１の秘密分散装置のときには、移動後のｋ番目の対応つけられた数値群の各数値の断片の再分散化のために、ランダムな値である$b_{k31}^{(1)}$，…，$b_{k31}^{(M)}$を生成し、第３の秘密分散装置に送信する。第２乱数生成部は、第２の秘密分散装置のときには、ｋ番目の対応つけられた数値群の各数値の断片の再分散化のために、ランダムな値である$b_{k23}^{(1)}$，…，$b_{k23}^{(M)}$を生成し、第３の秘密分散装置に送信する。第１計算部は、第１の秘密分散装置のときには、ｋ番目の対応つけられた数値群の各数値の断片の再分散化のために、ｍ＝１～Ｍについて$x_k^{(m)}=b_{k31}^{(m)}-a_{\pi(k)31}^{(m)}$を計算し、第２の秘密分散装置に送信する。第２計算部は、第２の秘密分散装置のときには、ｋ番目の対応つけられた数値群の各数値の断片の再分散化のために、ｍ＝１～Ｍについて$y_k^{(m)}=b_{k23}^{(m)}-a_{\pi(k)23}^{(m)}$を計算し、第１の秘密分散装置に送信する。第３計算部は、第１の秘密分散装置または第２の秘密分散装置のときには、ｋ番目の対応つけられた数値群の各数値の断片の再分散化のために、ｍ＝１～Ｍについて$b_{k12}^{(m)}=a_{\pi(k)12}^{(m)}-x_k^{(m)}-y_k^{(m)}$を計算する。断片更新部は、第１の秘密分散装置のときには（$b_{k31}^{(m)}$，$b_{k12}^{(m)}$）を断片$b_{k1}^{(m)}$とし、第２の秘密分散装置のときには（$b_{k12}^{(m)}$，$b_{k23}^{(m)}$）を断片$b_{k2}^{(m)}$とし、第３の秘密分散装置のときには（$b_{k23}^{(m)}$，$b_{k31}^{(m)}$）を断片$b_{k3}^{(m)}$とする。なお、全ての秘密分散装置の断片置換部で、秘密分散システムの断片置換手段が構成される。また、第１乱数生成部、第２乱数生成部、第１計算部、第２計算部、第３計算部、断片更新部で

、秘密分散システムの再分散手段が構成される。

【発明の効果】

【０００８】

本発明の秘密分散システムによれば、断片置換部に選ばれなかった秘密分散装置は、全単射πを知らないので、数値$A_1^{(1)}$，…，$A_K^{(1)}$，…，$A_1^{(M)}$，…，$A_K^{(M)}$と数値$B_1^{(1)}$，…，$B_K^{(1)}$，…，$B_1^{(M)}$，…，$B_K^{(M)}$との対応が分からない。本発明を用いることにより、クイックソートなどの比較に基づくソーティングアルゴリズムを、比較回数を増やすことなく秘密計算上で実現できる。

【図面の簡単な説明】

【０００９】

【図１】実施例１，２の秘密分散システムの機能構成例を示す図。

【図２】実施例１の秘密分散システムでの秘密分散の処理フローを示す図。

【図３】本発明の秘密分散システムでの数値のソートの処理フローを示す図。

【図４】クイックソートのアルゴリズムを示す図。

【図５】実施例２の秘密分散システムでの秘密分散の処理フローを示す図。

【図６】実施例３，４の秘密分散システムの機能構成例を示す図。

【図７】実施例３，４の再分散部の詳細な構成の例を示す図。

【図８】実施例３の秘密分散システムでの秘密分散の処理フローを示す図。

【図９】実施例４の改ざん検出部の詳細な構造を示す図。

【図１０】実施例４の秘密分散システムでの秘密分散の処理フローを示す図。

【発明を実施するための形態】

【００１０】

以下、本発明の実施の形態について、詳細に説明する。なお、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。

【実施例１】

【００１１】

課題を解決するための手段では、数値$A_1^{(1)}$，…，$A_K^{(1)}$，…，$A_1^{(M)}$，…，$A_K^{(M)}$を各秘密分散装置が断片を分散して記録するK×M個の数値、数値$A_k^{(1)}$，…，$A_k^{(M)}$を対応付けられたｋ番目の数値群、$a_{kn}^{(m)}$をｎ番目の秘密分散装置が記録する数値$A_k^{(m)}$の断片として説明した。本実施例では、まず本発明の理解を助けるために、Ｍ＝１の場合について説明し、その後Ｍを１に限定しない場合について説明する。また、Ｍ＝１の場合の説明では、$A_k^{(1)}$をA_kと、$a_{kn}^{(1)}$をa_{kn}と表現する。

【００１２】

［限定シャッフル］

図１に実施例１の秘密分散システムの機能構成例を示す。図２に実施例１の秘密分散システムでの秘密分散の処理フローを示す。本実施例の秘密分散システムは、ネットワーク１０００に接続されたＮ個（Ｎは３以上の整数、ｎは１以上Ｎ以下の整数）の秘密分散装置100_1，…，100_Nと選択手段１０５で構成される。ここで、A_1，…，A_Kを各秘密分散装置100_nが断片を分散して記録するＫ個の数値（Ｋは２以上の整数）、数値A_kをｋ番目の数値（ｋは１以上Ｋ以下の整数）、a_{kn}を秘密分散装置100_nが記録するｋ番目の断片とする。なお、数値A_1，…，A_Kが、秘匿化したい数値群であって、例えば、ソートの対象となる数値群である。ソートの対象となる数値群としては、例えば、数値A_kが各々の人の年収を示すような数値群が考えられる。選択手段１０５は、いずれかの秘密分散装置の内部に配置されてもよいし、単独の装置であってもよい。

【００１３】

本実施例の秘密分散システムは、選択手段と断片置換手段と再分散手段を備える。また、秘密分散装置100_nは、少なくとも断片置換部110_nと再分散部120_nと記録部190_nを備える。記録部190_nは断片a_{1n}，…，a_{Kn}などを記録する。また、記録部190_nは、自身が記録している断片a_{kn}が数値A_kの何番目の断片なのかに関す

る情報も記録する。

【００１４】

選択手段１０５は、Ｎ未満の数の秘密分散装置を選択する（Ｓ１０５）。例えば、Ｎ個の断片のうちＮ’個を集めれば数値を復元できる秘密分散であれば、断片置換手段がＮ’個以上Ｎ未満の秘密分散装置を選べばよい。

【００１５】

断片置換手段は、少なくとも断片置換部１１０_{1}，…，１１０_{N}を含んで構成される。そして、選択手段１０５に選択された秘密分散装置１００_{i}（ただし、ｉは選択された秘密分散装置を示す番号）の断片置換部１１０_{i}間で｛１，…，Ｋ｝→｛１，…，Ｋ｝の全単射πを作成し、選択された秘密分散装置１００_{i}の記録部１９０_{i}が記録する断片$a_{\pi(k)i}$をｋ番目の断片にする（Ｓ１１０）。全単射πは、１～Ｋを単にランダムに並べ替えたものであってもよい。なお、全単射πは、望ましくは一様にランダムに並び替えられたものであり、例えばFisher-Yates shuffle（参考文献１：Richard Durstenfeld, “Algorithm 235: Random permutation”, Communications of the ACM archive, Volume 7, Issue 7, 1964.）などを用いて作成すればよい。また、全単射πは選択された秘密分散装置１００_{i}間で生成してもよいし、選択された秘密分散装置１００_{i}のうちの１つの秘密分散装置が生成して、選択された秘密分散装置１００_{i}間で共有してもよい。

【００１６】

再分散手段は、少なくとも再分散部１２０_{1}，…，１２０_{N}を含んで構成される。再分散手段は、断片置換手段によって置換された数値$A_{\pi(k)}$に対応する断片$a_{\pi(k)i}$（ｋ番目に置換されている）を用いて再分散化して新しい断片b_{k1}，…，b_{kN}を求め、数値B_{k}の断片とする（Ｓ１２０）。つまり、$A_{\pi(k)}=B_{k}$の関係が成り立つが、選ばれなかった秘密分散装置は全単射πを知らないので、$A_{\pi(k)}=B_{k}$であることを知らない。なお、各秘密分散装置１００_{n}の記録部１９０_{n}は、断片b_{kn}を記録するだけでなく、自身が記録しているｋ番目の断片である断片b_{kn}が数値B_{k}の断片であるという情報も記録する。また、数値B_{1}，…，B_{K}を新しい数値A_{1}，…，A_{K}とし、断片置換手段で選択する秘密分散装置の組み合わせを変更すれば、この処理を繰り返すことができる（Ｓ１１１，Ｓ１１２）。

【００１７】

本発明の秘密分散システムによれば、限定された秘密分散装置間で断片をシャッフルする。したがって、断片置換部に選ばれなかった秘密分散装置は、全単射πを知らないので、数値A_{1}，…，A_{K}と数値B_{1}，…，B_{K}との対応が分からない。つまり、特定の秘密分散装置からは数値A_{1}，…，A_{K}と数値B_{1}，…，B_{K}との対応が分からない状態にしたいのであれば、その秘密分散装置を断片置換部で選ばないように、選択する秘密分散装置をあらかじめ定めればよい。また、断片置換部が選ぶ秘密分散装置を変更しながらこの処理を繰り返し、全ての秘密分散装置が選ばれなかったことがある状態にすれば、全ての秘密分散装置が数値A_{1}，…，A_{K}と対応つけることができない数値B_{1}，…，B_{K}を得ることができる。

【００１８】

［再分散］

上述の限定シャッフルの説明では、再分散については詳しく説明しなかった。ここでは、再分散の方法について説明する。再分散の方法としては、参考文献２（Amir Herzberg, Stanislaw Jarecki, Hugo Krawczyk, and Moti Yung, “Proactive secret sharing or: How to cope with perpetual leakage”, In Don Coppersmith, editor, CRYPTO 1995, volume 963 of LNCS, pages 339-352. Springer, 1995.）の3.3節に示された更新方法と、参考文献３（Haiyun Luo and Songwu Lu, “Ubiquitous and robust authentication services for ad hoc wireless networks”, In UCLA-CSD-TR-200030, 2000.）の6.1節に示された再作成方法を用いる。選択手段１０５が選択した秘密計算装置間で参考文献２の更新方法を用いて新しい断片を生成し、その後、参考文献３の再作成方法を用いて選択手段１０５が選択しなかった秘密計算装置の新しい断片を生成する。

【００１９】
参考文献２の更新方法を、本件に適用したアルゴリズムを以下に示す。選択手段１０５がＮ’個の秘密分散装置を選択したとする。そして、ｉとｊは選択された秘密分散装置を示す番号（１～Ｎの中から選ばれたＮ’個の数の中のいずれか）であって、ｊ≠ｉとする。また、値z_1，…，z_Nはあらかじめ決められた値であり、すべての秘密分散装置間で共有されているとする。
（１）すべての秘密分散装置100_iは、Ｎ’－１個の乱数$u_{i,1}$，$u_{i,2}$，…，$u_{i,N'-1}$を作成する。
（２）すべての秘密分散装置100_iは、$Z_i(z) := 0 + u_{i,1}z + u_{i,2}z^2 + \cdots + u_{i,N'-1}z^{N'-1}$を定める。
（３）すべての秘密分散装置100_iは、選択された他の秘密分散装置100_j（Ｎ’－１個存在する）のすべてに対して、それぞれ$Z_i(z_j)$の値を送信する。
（４）すべての秘密分散装置100_iは、選択された他の秘密分散装置100_j（Ｎ’－１個存在する）から受け取ったすべての$Z_j(z_i)$の和を$Z(z_i)$とし、新しい断片b_{ki}を置換された断片$a_{\pi(k)i}$を用いて、
$b_{ki} = a_{\pi(k)i} + Z(z_i)$
のように求める。
【００２０】
次に、参考文献３の再作成方法を、本件に適用したアルゴリズムを以下に示す。ｈは選択されなかった秘密分散装置を示す番号（１～Ｎの中から選ばれなかったＮ－Ｎ’個の数のなかのいずれか）とする。また、$L_{ij}(z) = (z - z_j)/(z_i - z_j)$とし、$L_i(z)$は、すべてのｊについての$L_{ij}(z)$の積とする。
（５）すべての秘密分散装置100_iは、ｉ＜ｊであるｊと、選択されなかった秘密分散装置100_hのすべての組み合わせに対して、乱数$v_{i,j}^{(h)}$を生成する。
（６）すべての秘密分散装置100_iは、$v_{i,j}^{(h)}$を秘密分散装置100_jに送信する。
（７）すべての秘密分散装置100_iは、すべての選択されなかった秘密分散装置100_hについて、ｊ＜ｉのすべての乱数$v_{i,j}^{(h)}$の和を$V^{(h+)}$とし、ｉ＜ｊのすべての乱数$v_{i,j}^{(h)}$の和を$V^{(h-)}$とし、値w_{hi}を、
$w_{hi} = b_{ki}L_i(z_h) + V^{(h+)} - V^{(h-)}$
のように求め、秘密分散装置100_hに値w_{hi}を送信する。
（８）すべての秘密分散装置100_hは、受信したすべての値w_{hi}の和を新しい断片b_{kh}とする。
【００２１】
上述のように、（１）～（４）の処理で、すべての選択された秘密分散装置が、新しい断片を記録する。（５）～（８）の処理で、すべての選択されなかった秘密分散装置が、新しい断片を記録する。
【００２２】
なお、（３）と（６）の処理を同時に行えば、処理の高速化を図ることができる。具体的には、（１）、（２）、（５）の処理をまず行い、（３）と（６）を同時に行い、（４）、（７）、（８）の処理を行えばよい。
【００２３】
［ソート］
図３に実施例１の秘密分散システムでの数値のソートの処理フローを示す。上述の方法によって初期の数値A_1，…，A_Kと対応つけることができない新しい数値A_1，…，A_Kを得ている（Ｓ１０１）。ソートも行う場合は、秘密分散装置100_nは、比較部210_nと交換部220_nも備える。比較部210_1，…，210_Nは、２つの数値を選択し、当該２つの数値の大小を秘密計算によって比較する（Ｓ２１０）。
【００２４】
交換部220_1，…，220_Nは、それぞれ比較部210_1，…，210_Nでの比較結

果に基づいて、０組または１組または複数組の数値の断片を入れ替える（Ｓ２２０）。そして、全ての数値に対するソート処理が終わるまで、ステップＳ２１０とＳ２２０（比較、交換、組合せの変更などの必要な処理）を繰り返せばよい（Ｓ２１１，Ｓ２１２）。

【００２５】

ステップＳ２１０の比較結果は、全ての秘密分散装置の次の処理に必要な情報なので全ての秘密分散装置が知る情報である。しかし、ステップＳ１０１によって全ての秘密分散装置が初期の数値A_1，…，A_Kと対応できなくなった新しい数値A_1，…，A_Kに対して処理しているので、初期の数値A_1，…，A_Kに関する情報は漏れない。さらに、比較結果は、ソートの出力という公開情報から計算可能な情報でもある。そのため、本実施例のプロトコル全体で見ても、比較結果が開示されることは必要以上の情報を漏らしたことにはならない。

【００２６】

なお、より具体的には、ソートの部分（ステップＳ２１０，Ｓ２２０，Ｓ２１１，Ｓ２１２）には図４に示すクイックソートのアルゴリズムを適用すればよい。この場合もＡ［ｉ］とＡ［ｊ］とを比較する処理はＡ［ｉ］とＡ［ｊ］の値を秘匿したままで行い、比較結果は公開される。この方法の場合、比較回数は元のクイックソートと同じであり、平均Ｏ（Ｎ・ｌｏｇＮ）回である。また、この他にも、数値の大小比較の処理と配列の２つの要素を入れ替える処理で構成できるソーティングアルゴリズムにも本実施例は適用できる。

【００２７】

このように、本実施例の秘密分散システムを用いれば、比較と要素の入れ替えからなるソーティングアルゴリズムを比較回数を増やすことなく秘密計算で実現できる。

【００２８】

［限定シャッフルの変形例］

次に、Ｍを１に限定しない場合について説明する。Ｍは１以上の整数、ｍは１以上Ｍ以下の整数とする。$A^{(1)}$，…，$A^{(M)}$はそれぞれＫ個の要素を持つベクトルであり、$A^{(m)}=(A_1^{(m)},\cdots,A_K^{(m)})$とする。また、ベクトル$A^{(1)}$，…，$A^{(M)}$の各要素は対応付けられているとする。言い換えると、$A_k^{(1)}$，…，$A_k^{(M)}$は対応付けられたｋ番目の数値群とする。本変形例では、対応つけられた数値群の対応を維持したまま数値群を限定シャッフルする。また、$a_{kn}^{(m)}$を秘密分散装置100_nが記録する数値$A_k^{(m)}$の断片とする。なお、上述の限定シャッフルはＭ＝１の場合に相当するので、以下の説明はより一般的な限定シャッフルである。

【００２９】

秘密分散システムの構成は図１と同じであり、秘密分散の処理フローは図２と同じである。秘密分散装置100_nは、少なくとも断片置換部110_nと再分散部120_nと記録部190_nを備える。ただし、各構成部とその処理は以下のようになる。

【００３０】

記録部190_nは断片$a_{1n}^{(1)}$，…，$a_{Kn}^{(1)}$，…，$a_{1n}^{(M)}$，…，$a_{Kn}^{(M)}$などを記録する。また、記録部190_nは、自身が記録している断片a_{kn}が数値A_kの何番目の断片なのかに関する情報も記録する。

【００３１】

選択手段１０５は、Ｎ未満の数の秘密分散装置を選択する（Ｓ１０５）。例えば、Ｎ個の断片のうちＮ’個を集めれば数値を復元できる秘密分散であれば、断片置換手段がＮ’個以上Ｎ未満の秘密分散装置を選べばよい。この処理は同じである。

【００３２】

断片置換手段は、少なくとも断片置換部110_1，…，110_Nを含んで構成される。そして、選択手段１０５に選択された秘密分散装置100_i（ただし、ｉは選択された秘密分散装置を示す番号）の断片置換部110_i間で｛１，…，Ｋ｝→｛１，…，Ｋ｝の全単射πを作成し、選択された秘密分散装置100_iの記録部190_iが記録する断片$a_{\pi(k)i}^{(1)}$，…，$a_{\pi(k)i}^{(M)}$を対応付けられたｋ番目の数値群の断片にする

（Ｓ１１０）。

【００３３】

再分散手段は、少なくとも再分散部１２０_{1}，…，１２０_{N}を含んで構成される。再分散手段は、断片置換手段によって置換された数値群$A_{\pi(k)}^{(1)}$，…，$A_{\pi(k)}^{(M)}$に対応する断片$a_{\pi(k)i}^{(1)}$，…，$a_{\pi(k)i}^{(M)}$（ｋ番目に置換されている）を用いて再分散化して新しい断片$b_{k1}^{(1)}$，…，$b_{kN}^{(1)}$，…，$b_{k1}^{(M)}$，…，$b_{kN}^{(M)}$を求め、数値$B_{k}^{(1)}$，…，$B_{k}^{(M)}$の断片とする（Ｓ１２０）。つまり、$A_{\pi(k)}^{(m)}=B_{k}^{(m)}$の関係が成り立つが、選ばれなかった秘密分散装置は全単射πを知らないので、$A_{\pi(k)}^{(m)}=B_{k}^{(m)}$であることを知らない。なお、各秘密分散装置$１００_{n}$の記録部$１９０_{n}$は、断片$b_{kn}^{(m)}$を記録するだけでなく、自身が記録しているｋ番目の断片である断片$b_{kn}^{(m)}$が数値$B_{k}^{(m)}$の断片であるという情報も記録する。また、数値$B_{1}^{(1)}$，…，$B_{K}^{(1)}$，…，$B_{1}^{(M)}$，…，$B_{K}^{(M)}$を新しい数値$A_{1}^{(1)}$，…，$A_{K}^{(1)}$，…，$A_{1}^{(M)}$，…，$A_{K}^{(M)}$とし、断片置換手段で選択する秘密分散装置の組み合わせを変更すれば、この処理を繰り返すことができる（Ｓ１１１，Ｓ１１２）。

【００３４】

このように、ベクトルの各要素の対応を維持した限定シャッフルを利用すれば、例えば、表形式をしたデータの秘密分散から、各行を１つの要素（対応付けられた数値群）として列方向のランダム置換を行うことができる。

【実施例２】

【００３５】

［限定シャッフル］

実施例２の秘密分散システムの構成も図１に示す。なお、本実施例の秘密分散装置１００_{n}は、点線で示された構成部も備えている。図５に実施例２の秘密分散システムでの秘密分散の処理フローを示す。本実施例の秘密分散システムは、ネットワーク１０００に接続されたＮ個（Ｎは３以上の整数、ｎは１以上Ｎ以下の整数）の秘密分散装置１００_{1}，…，１００_{N}と選択手段１０５で構成される。ここで、A_{1}，…，A_{K}を各秘密分散装置１００_{n}が断片を分散して記録するＫ個の数値（Ｋは２以上の整数）、数値A_{k}をｋ番目の数値（ｋは１以上Ｋ以下の整数）、a_{kn}を秘密分散装置１００_{n}が記録する数値A_{k}の断片とする。

【００３６】

本実施例の秘密分散システムは、選択手段１０５、初期情報分散手段、初期乗算手段、断片置換手段、再分散手段、確認分散手段、確認乗算手段、改ざん検出手段を備える。また、秘密分散装置１００_{n}は、初期情報分散部１３０_{n}、初期乗算部１４０_{n}、断片置換部１１０_{n}、再分散部１２０_{n}、確認分散部１５０_{n}、確認乗算部１６０_{n}、改ざん検出部１７０_{n}、記録部１９０_{n}を備える。記録部１９０_{n}は断片a_{1n}，…，a_{Kn}などを記録する。また、記録部１９０_{n}は、自身が記録している断片a_{kn}が数値A_{k}の何番目の断片なのかに関する情報も記録する。

【００３７】

選択手段１０５は実施例１と同じである。初期情報分散手段は、初期情報分散部１３０_{1}，…，１３０_{N}で構成される。そして、選択手段１０５に選択された秘密計算装置１００_{i}の初期情報分散部１３０_{i}は、秘密分散装置１００_{1}，…，１００_{N}のどれも知らないＫ個の数値P_{1}，…，P_{K}それぞれの断片p_{11}，…，p_{K1}，…，p_{1n}，…，p_{Kn}，…，p_{1N}，…，p_{KN}を秘密計算によって求め、秘密分散装置１００_{n}に断片p_{1n}，…，p_{Kn}を記録する（Ｓ１３０）。具体的には、選択手段１０５に選択された秘密分散装置から、２つ以上の秘密分散装置を選定する。そして、選定された秘密分散装置が作った値に基づいて、どの装置も知らない値の断片を作ればよい。例えば、２つの秘密分散装置１００_{i}，１００_{j}を選定し（ただし、$i\neq j$）、秘密分散装置１００_{i}が生成した数値の断片と、秘密分散装置１００_{j}が生成した数値の断片を分散して記録する。そして、その２つの数値の和を秘密計算によって求め、結果が分からないように断片を分散し

て記録すれば、全ての秘密分散装置が知らない数値の断片を分散して記録できる。この例では、選定した秘密計算装置を２つとしたが、２つ以上でもかまわない。

【００３８】

初期乗算手段は、初期乗算部140_1，…，140_Nで構成される。初期乗算部140_1，…，140_Nは、$S_k=P_k\times A_k$である数値S_kの断片s_{k1}，…，s_{kN}を秘密計算によって求め、秘密分散装置100_1，…，100_Nに分散して記録する（Ｓ１４０）。

【００３９】

断片置換手段と再分散手段は、実施例１と同じである。確認分散手段は、確認分散部150_1，…，150_Nで構成される。確認分散部150_1，…，150_Nは、$k=1\sim K$について、$Q_k=P_{\pi(k)}$である数値Q_kの断片q_{k1}，…，q_{kN}を秘密計算によって生成し、秘密分散装置100_1，…，100_Nに分散して記録する（Ｓ１５０）。具体的には、ステップＳ１３０で選定された秘密分散装置が作った値に基づいて、どの装置も知らない値の別の断片を作ればよい。例えば、ステップＳ１３０で選定された秘密分散装置100_iが数値$P_{\pi(k)}$用に生成した数値の別の断片（新しい断片）と、ステップＳ１３０で選定された秘密分散装置100_jが数値$P_{\pi(k)}$用に生成した数値の別の断片（新しい断片）を分散して記録する。そして、その２つの数値の和を秘密計算によって求め、結果が分からないように断片を分散して記録すれば、$Q_k=P_{\pi(k)}$であり、かつ、全ての秘密分散装置が知らない数値の断片を分散して記録できる。この例では、選定した秘密計算装置を２つとしたが、ステップＳ１３０と同じように２つ以上でもかまわない。

【００４０】

確認乗算手段は、確認乗算部160_1，…，160_Nで構成される。確認乗算部160_1，…，160_Nは、$T_k=Q_k\times B_k$である数値T_kの断片t_{k1}，…，t_{kN}を秘密計算によって求め、秘密分散装置100_1，…，100_Nに分散して記録する（Ｓ１６０）。

【００４１】

改ざん検出手段は、改ざん検出部170_1，…，170_Nで構成される。改ざん検出部170_1，…，170_Nは、$k=1\sim K$について、$T_k=S_{\pi(k)}$であることを確認する（Ｓ１７０）。$t_{kn}\neq s_{\pi(k)n}$の場合には、改ざんがあったとして異常終了する。また、数値B_1，…，B_Kを新しい数値A_1，…，A_Kとし、断片置換手段で選択する秘密分散装置の組み合わせを変更すれば、この処理を繰り返すことができる（Ｓ１１１，Ｓ１１２）。

【００４２】

実施例２の秘密分散システムによれば、実施例１の秘密分散装置と同じ効果が得られると共に、数値A_1，…，A_Kと数値B_1，…，B_Kとの対応を分からなくする処理の途中に、他の秘密分散装置に改ざんした値を送信する不正がないことも確認できる。なお、ソートも行う場合は、秘密分散装置100_nは、比較部210_nと交換部220_nも備える。具体的なソートの処理については実施例１と同じである。

【実施例３】

【００４３】

実施例１、２では、秘密分散装置の数をＮ（Ｎは３以上の整数）としていた。実施例３では、秘密分散システムを構成する秘密分散装置の数を３に限定し、より具体的に説明する。

【００４４】

［限定シャッフル］

図６に実施例３の秘密分散システムの機能構成例を示す。図７に実施例３の再分散部の詳細な構成の例を示す。図８に実施例３の秘密分散システムでの秘密分散の処理フローを示す。本実施例の秘密分散システムは、ネットワーク１０００に接続された３つの秘密分散装置100_α，100_β，100_γと選択手段１０５で構成される。ここで、Ｋ個の数

値のｋ番目を数値$A_k = a_{k\alpha\beta} + a_{k\beta\gamma} + a_{k\gamma\alpha}$（ただし、Ｋは２以上の整数、ｋは１以上Ｋ以下の整数、（α，β，γ）は、（１，２，３）、（２，３，１）、（３，１，２）のいずれか）とし、その３つの断片を（$a_{k\gamma\alpha}$，$a_{k\alpha\beta}$）、（$a_{k\alpha\beta}$，$a_{k\beta\gamma}$）、（$a_{k\beta\gamma}$，$a_{k\gamma\alpha}$）とする。なお、選択手段１０５は、いずれかの秘密分散装置の内部に配置されてもよいし、単独の装置であってもよい。

【００４５】

本実施例の秘密分散システムは、選択手段１０５と断片置換手段と再分散手段を備える。各秘密分散装置100_nは、断片置換部110_n、再分散部120_n、記録部190_nを備えている（ただし、ｎはα、β、γのいずれか）。記録部190_nは、数値A_1，…，A_Kの断片などを記録する。

【００４６】

選択手段１０５は、２つの秘密分散装置を選択する。そして、選択手段１０５に選択された秘密分散装置の一方を第１の秘密分散装置100_1、他方を第２の秘密分散装置100_2、選択されなかった秘密分散装置を第３の秘密分散装置100_3とする（Ｓ１０５）。ここで、第１の秘密分散装置100_1が記録するｋ番目の断片を$a_{k1} = (a_{k31}, a_{k12})$、第２の秘密分散装置$100_2$が記録するｋ番目の断片を$a_{k2} = (a_{k12}, a_{k23})$、第３の秘密分散装置$100_3$が記録するｋ番目の断片を$a_{k3} = (a_{k23}, a_{k31})$とする。

【００４７】

断片置換手段は、少なくとも断片置換部110_α，110_β，110_γを含んで構成される。断片置換手段は、第１の秘密分散装置100_1または第２の秘密分散装置100_2で{１，…，Ｋ}→{１，…，Ｋ}の全単射πを作成し、第１の秘密分散装置100_1が記録する断片$a_{\pi(k)1}$をｋ番目の断片にし、第２の秘密分散装置100_2が記録する断片$a_{\pi(k)2}$をｋ番目の断片にする（Ｓ１１０）。実施例１で説明した通り、全単射πは、１～Ｋを単にランダムに並べ替えたものであってもよい。なお、全単射πは、望ましくは一様にランダムに並び替えられたものであり、例えばFisher-Yates shuffleなどを用いて作成すればよい。

【００４８】

再分散手段は、少なくとも再分散部120_α，120_β，120_γを含んで構成される。図７に示すように再分散部120_nは、第１乱数生成部121_n、第２乱数生成部122_n、第１計算部123_n、第２計算部124_n、第３計算部125_n、断片更新部126_nを備えている。

【００４９】

第１の秘密分散装置100_1の第１乱数生成部121_1は、ｋ番目の断片の再分散化のために、ランダムな値であるb_{k31}を生成し、第３の秘密分散装置100_3に送信する（Ｓ１２１）。第２の秘密分散装置100_2の第２乱数生成部122_2は、ｋ番目の断片の再分散化のために、ランダムな値であるb_{k23}を生成し、第３の秘密分散装置100_3に送信する（Ｓ１２２）。第１の秘密分散装置100_1の第１計算部123_1は、ｋ番目の断片の再分散化のために、$x_k = b_{k31} - a_{\pi(k)31}$を計算し、第２の秘密分散装置$100_2$に送信する（Ｓ１２３）。

【００５０】

第２の秘密分散装置100_2の第２計算部124_2は、ｋ番目の断片の再分散化のために、$y_k = b_{k23} - a_{\pi(k)23}$を計算し、第１の秘密分散装置$100_1$に送信する（Ｓ１２４）。第１の秘密分散装置$100_1$の第３計算部$125_1$と第２の秘密分散装置$100_2$の第３計算部$125_2$は、ｋ番目の断片の再分散化のために、それぞれ$b_{k12} = a_{\pi(k)12} - x_k - y_k$を計算する（Ｓ１２５）。第１の秘密分散装置$100_1$の断片更新部$126_1$は（$b_{k31}$，$b_{k12}$）を断片$b_{k1}$とし、第２の秘密分散装置$100_2$の断片更新部$126_2$は（$b_{k12}$，$b_{k23}$）を断片$b_{k2}$とし、第３の秘密分散装置$100_3$の断片更新部$126_3$は（$b_{k23}$，$b_{k31}$）を断片$b_{k3}$とする（Ｓ１２６）。なお、各秘密分散装置$100_n$の記録部$190_n$は、断片$b_{kn}$を記録するだ

けでなく、自身が記録しているｋ番目の断片である断片b_{kn}が数値B_kの断片であるという情報も記録する。実施例１と同じように、断片b_{k1}，b_{k2}，b_{k3}は、数値B_kの断片である。つまり、ステップＳ１２１～Ｓ１２６が、ステップＳ１２０に相当する。

【００５１】

また、数値B_1，…，B_Kを新しい数値A_1，…，A_Kとし、断片置換手段で選択する秘密分散装置の組み合わせを変更すれば、この処理を繰り返すことができる（Ｓ１１１，Ｓ１１２）。そして、断片置換部が選ぶ秘密分散装置を変更しながらこの処理を繰り返し、全ての秘密分散装置が選ばれなかったことがある状態にすれば、全ての秘密分散装置が数値A_1，…，A_Kと対応つけることができない数値B_1，…，B_Kを得ることができる。本実施例では、断片置換手段が選択する秘密分散装置を、{100_α，100_β}，{100_β，100_γ}，{100_γ，100_α}のように選択すれば、全ての秘密分散装置が選ばれなかったことがある状態にできる。

【００５２】

したがって、実施例３の秘密分散システムは、実施例１と同様の効果が得られる。なお、ソートも行う場合は、秘密分散装置100_nは、比較部210_nと交換部220_nも備える。具体的なソートの処理については実施例１と同じである。

【００５３】

［限定シャッフルの変形例］

Ｍは１以上の整数、ｍは１以上Ｍ以下の整数とする。$A^{(1)}$，…，$A^{(M)}$はそれぞれＫ個の要素を持つベクトルであり、$A^{(m)}=(A_1^{(m)},\cdots,A_K^{(m)})$とする。また、ベクトル$A^{(1)}$，…，$A^{(M)}$の各要素は対応付けられているとする。言い換えると、$A_k^{(1)}$，…，$A_k^{(M)}$は対応付けられたｋ番目の数値群である。本変形例では、対応つけられた数値群の対応を維持したまま数値群を限定シャッフルする。また、数値$A_k^{(m)}=a_{k\alpha\beta}^{(m)}+a_{k\beta\gamma}^{(m)}+a_{k\gamma\alpha}^{(m)}$（ただし、ｋは１以上Ｋ以下の整数、ｍは１以上Ｍ以下の整数、（α，β，γ）は、（１，２，３）、（２，３，１）、（３，１，２）のいずれか）とし、の３つの断片を（$a_{k\gamma\alpha}^{(m)}$，$a_{k\alpha\beta}^{(m)}$）、（$a_{k\alpha\beta}^{(m)}$，$a_{k\beta\gamma}^{(m)}$）、（$a_{k\beta\gamma}^{(m)}$，$a_{k\gamma\alpha}^{(m)}$）とする。なお、上述の限定シャッフルはＭ＝１の場合に相当するので、以下の説明はより一般的な限定シャッフルである。

【００５４】

秘密分散システムの機能構成例は図６と同じであり、再分散部の詳細な構成例は図７と同じであり、秘密分散の処理フローは図８と同じである。秘密分散システムは、選択手段１０５と断片置換手段と再分散手段を備える。秘密分散装置100_nは、少なくとも断片置換部110_nと再分散部120_nと記録部190_nを備える（ただし、ｎはα、β、γのいずれか）。ただし、各構成部とその処理は以下のようになる。

【００５５】

記録部190_nは断片$a_{1n}^{(1)}$，…，$a_{Kn}^{(1)}$，…，$a_{1n}^{(M)}$，…，$a_{Kn}^{(M)}$などを記録する。また、記録部190_nは、自身が記録している断片a_{kn}が数値A_kの何番目の断片なのかに関する情報も記録する。

【００５６】

選択手段１０５は、２つの秘密分散装置を選択する。そして、選択手段１０５に選択された秘密分散装置の一方を第１の秘密分散装置100_1、他方を第２の秘密分散装置100_2、選択されなかった秘密分散装置を第３の秘密分散装置100_3とする（Ｓ１０５）。ここで、第１の秘密分散装置100_1が記録する数値$A_k^{(m)}$の断片を$a_{k1}^{(m)}=(a_{k31}^{(m)},a_{k12}^{(m)})$、第２の秘密分散装置$100_2$が記録する数値$A_k^{(m)}$の断片を$a_{k2}^{(m)}=(a_{k12}^{(m)},a_{k23}^{(m)})$、第３の秘密分散装置$100_3$が記録する数値$A_k^{(m)}$の断片を$a_{k3}^{(m)}=(a_{k23}^{(m)},a_{k31}^{(m)})$とする。

【００５７】

断片置換手段は、少なくとも断片置換部110_α，110_β，110_γを含んで構成さ

れる。断片置換手段は、第１の秘密分散装置１００$_1$または第２の秘密分散装置１００$_2$で{１，…，Ｋ}→{１，…，Ｋ}の全単射πを作成し、第１の秘密分散装置１００$_1$が記録する断片$a_{\pi(k)1}^{(1)}$，…，$a_{\pi(k)1}^{(M)}$を対応付けられたｋ番目の数値群の断片にし、第２の秘密分散装置１００$_2$が記録する断片$a_{\pi(k)2}^{(1)}$，…，$a_{\pi(k)2}^{(M)}$を対応付けられたｋ番目の数値群の断片にする（Ｓ１１０）。

【００５８】

再分散手段は、少なくとも再分散部１２０$_\alpha$，１２０$_\beta$，１２０$_\gamma$を含んで構成される。図７に示すように再分散部１２０$_n$は、第１乱数生成部１２１$_n$、第２乱数生成部１２２$_n$、第１計算部１２３$_n$、第２計算部１２４$_n$、第３計算部１２５$_n$、断片更新部１２６$_n$を備えている。

【００５９】

第１の秘密分散装置１００$_1$の第１乱数生成部１２１$_1$は、対応付けられたｋ番目の数値群の断片の再分散化のために、ランダムな値である$b_{k31}^{(1)}$，…，$b_{k31}^{(M)}$を生成し、第３の秘密分散装置１００$_3$に送信する（Ｓ１２１）。第２の秘密分散装置１００$_2$の第２乱数生成部１２２$_2$は、対応付けられたｋ番目の数値群の断片の再分散化のために、ランダムな値である$b_{k23}^{(1)}$，…，$b_{k23}^{(M)}$を生成し、第３の秘密分散装置１００$_3$に送信する（Ｓ１２２）。第１の秘密分散装置１００$_1$の第１計算部１２３$_1$は、対応付けられたｋ番目の数値群の断片の再分散化のために、ｍ＝１～Ｍについて$x_k^{(m)}=b_{k31}^{(m)}-a_{\pi(k)31}^{(m)}$を計算し、$x_k^{(1)}$，…，$x_k^{(M)}$を第２の秘密分散装置１００$_2$に送信する（Ｓ１２３）。

【００６０】

第２の秘密分散装置１００$_2$の第２計算部１２４$_2$は、対応付けられたｋ番目の数値群の断片の再分散化のために、ｍ＝１～Ｍについて$y_k^{(m)}=b_{k23}^{(m)}-a_{\pi(k)23}^{(m)}$を計算し、$y_k^{(1)}$，…，$y_k^{(M)}$を第１の秘密分散装置１００$_1$に送信する（Ｓ１２４）。第１の秘密分散装置１００$_1$の第３計算部１２５$_1$と第２の秘密分散装置１００$_2$の第３計算部１２５$_2$は、対応付けられたｋ番目の数値群の断片の再分散化のために、それぞれｍ＝１～Ｍについて$b_{k12}^{(m)}=a_{\pi(k)12}^{(m)}-x_k^{(m)}-y_k^{(m)}$を計算する（Ｓ１２５）。第１の秘密分散装置１００$_1$の断片更新部１２６$_1$は（$b_{k31}^{(m)}$，$b_{k12}^{(m)}$）を断片$b_{k1}^{(m)}$とし、第２の秘密分散装置１００$_2$の断片更新部１２６$_2$は（$b_{k12}^{(m)}$，$b_{k23}^{(m)}$）を断片$b_{k2}^{(m)}$とし、第３の秘密分散装置１００$_3$の断片更新部１２６$_3$は（$b_{k23}^{(m)}$，$b_{k31}^{(m)}$）を断片$b_{k3}^{(m)}$とする（Ｓ１２６）。なお、各秘密分散装置１００$_n$の記録部１９０$_n$は、断片$b_{kn}^{(m)}$を記録するだけでなく、自身が記録しているｋ番目の断片である断片$b_{kn}^{(m)}$が数値$B_k^{(m)}$の断片であるという情報も記録する。実施例１と同じように、断片$b_{k1}^{(m)}$，$b_{k2}^{(m)}$，$b_{k3}^{(m)}$は、数値$B_k^{(m)}$の断片である。つまり、ステップＳ１２１～Ｓ１２６が、ステップＳ１２０に相当する。

【００６１】

また、数値$B_1^{(1)}$，…，$B_K^{(1)}$，…，$B_1^{(M)}$，…，$B_K^{(M)}$を新しい数値$A_1^{(1)}$，…，$A_K^{(1)}$，…，$A_1^{(M)}$，…，$A_K^{(M)}$とし、断片置換手段で選択する秘密分散装置の組み合わせを変更すれば、この処理を繰り返すことができる（Ｓ１１１，Ｓ１１２）。

【００６２】

このように、ベクトルの各要素の対応を維持した限定シャッフルを利用すれば、例えば、表形式をしたデータの秘密分散から、各行を１つの要素（対応付けられた数値群）として列方向のランダム置換を行うことができる。

【実施例４】

【００６３】

実施例４でも、秘密分散システムを構成する秘密分散装置の数を３に限定し、より具体的に説明する。また、実施例４では、実施例２と同じように不正検出機能を具備した例を

説明する。

【００６４】

［限定シャッフル］

実施例４の秘密分散システムの構成も図６に示す。なお、本実施例の秘密分散装置１００$_n$は、点線で示された構成部も備えている。図９に改ざん検出部の詳細な構造を示す。図１０に実施例４の秘密分散システムでの秘密分散の処理フローを示す。本実施例の秘密分散システムは、ネットワーク１０００に接続された３つの秘密分散装置１００$_\alpha$，１００$_\beta$，１００$_\gamma$と選択手段１０５で構成される。ここで、Ｋ個の数値のｋ番目を数値$A_k = a_{k\alpha\beta} + a_{k\beta\gamma} + a_{k\gamma\alpha}$（ただし、Ｋは２以上の整数、ｋは１以上Ｋ以下の整数、（α，β，γ）は、（１，２，３）、（２，３，１）、（３，１，２）のいずれか）とし、その３つの断片を（$a_{k\gamma\alpha}$，$a_{k\alpha\beta}$）、（$a_{k\alpha\beta}$，$a_{k\beta\gamma}$）、（$a_{k\beta\gamma}$，$a_{k\gamma\alpha}$）とする。

【００６５】

本実施例の秘密分散システムは、選択手段１０５、初期情報分散手段、初期乗算手段、断片置換手段、再分散手段、確認分散手段、確認乗算手段、改ざん検出手段を備える。秘密分散装置１００$_n$は、初期情報分散部１３０$_n$、初期乗算部１４０$_n$、断片置換部１１０$_n$、再分散部１２０$_n$、確認分散部１５０$_n$、確認乗算部１６０$_n$、改ざん検出部１７０$_n$、記録部１９０$_n$を備える（ただし、ｎはα、β、γのいずれか）。記録部１９０$_n$は、数値A_1，…，A_Kの断片などを記録する。

【００６６】

選択手段１０５は、２つの秘密分散装置を選択する。そして、選択手段１０５に選択された秘密分散装置の一方を第１の秘密分散装置１００$_1$、他方を第２の秘密分散装置１００$_2$、選択されなかった秘密分散装置を第３の秘密分散装置１００$_3$とする（Ｓ１０５）。ここで、第１の秘密分散装置１００$_1$が記録するｋ番目の断片をa_{k1}＝（a_{k31}，a_{k12}）、第２の秘密分散装置１００$_2$が記録するｋ番目の断片をa_{k2}＝（a_{k12}，a_{k23}）、第３の秘密分散装置１００$_3$が記録するｋ番目の断片をa_{k3}＝（a_{k23}，a_{k31}）とする。

【００６７】

初期情報分散手段は、初期情報分散部１３０$_\alpha$，１３０$_\beta$，１３０$_\gamma$で構成される。初期情報分散部１３０$_\alpha$，１３０$_\beta$，１３０$_\gamma$は、秘密分散装置１００$_\alpha$，１００$_\beta$，１００$_\gamma$のどれも知らないＫ個の数値P_1，…，P_Kそれぞれの断片p_{kn}を秘密計算によって求め、秘密分散装置１００$_n$に記録する（Ｓ１３０）。例えば、第１の秘密分散装置１００$_1$でＫ個のランダムな値$R^{(1)}{}_1$，…，$R^{(1)}{}_K$を生成し、第２の秘密分散装置１００$_2$でＫ個のランダムな値$R^{(2)}{}_1$，…，$R^{(2)}{}_K$を生成する。そして、秘密分散装置１００$_1$，１００$_2$，１００$_3$で、$R^{(1)}{}_k$の断片（$r^{(1)}{}_{k31}$，$r^{(1)}{}_{k12}$）、（$r^{(1)}{}_{k12}$，$r^{(1)}{}_{k23}$）、（$r^{(1)}{}_{k23}$，$r^{(1)}{}_{k31}$）と、$R^{(2)}{}_k$の断片（$r^{(2)}{}_{k31}$，$r^{(2)}{}_{k12}$）、（$r^{(2)}{}_{k12}$，$r^{(2)}{}_{k23}$）、（$r^{(2)}{}_{k23}$，$r^{(2)}{}_{k31}$）とを秘密分散して記録する。その後、秘密分散装置１００$_1$，１００$_2$，１００$_3$で、$P_k = R^{(1)}{}_k + R^{(2)}{}_k$である数値$P_k$の断片（$p_{k31}$，$p_{k12}$）、（$p_{k12}$，$p_{k23}$）、（$p_{k23}$，$p_{k31}$）を秘密計算によって求め、秘密分散装置１００$_1$，１００$_2$，１００$_3$に分散して記録する。このような処理によって、全ての秘密分散装置１００$_\alpha$，１００$_\beta$，１００$_\gamma$が知らない数値の断片を分散して記録できる。

【００６８】

初期乗算手段は、初期乗算部１４０$_\alpha$，１４０$_\beta$，１４０$_\gamma$で構成される。初期乗算部１４０$_\alpha$，１４０$_\beta$，１４０$_\gamma$は、$S_k = P_k \times A_k$である数値S_kの断片（$s_{k\gamma\alpha}$，$s_{k\alpha\beta}$）、（$s_{k\alpha\beta}$，$s_{k\beta\gamma}$）、（$s_{k\beta\gamma}$，$s_{k\gamma\alpha}$）を秘密計算によって求め、秘密分散装置１００$_\alpha$，１００$_\beta$，１００$_\gamma$に分散して記録する（Ｓ１４０）。

【００６９】

断片置換手段と再分散手段は、実施例３と同じである。断片置換手段と再分散手段によ

って、秘密分散装置１００$_{\alpha}$，１００$_{\beta}$，１００$_{\gamma}$に数値Ｂ$_{k}$の断片として断片ｂ$_{k1}$、ｂ$_{k2}$、ｂ$_{k3}$が記録される。確認分散手段は、確認分散部１５０$_{\alpha}$，１５０$_{\beta}$，１５０$_{\gamma}$で構成される。確認分散部１５０$_{\alpha}$，１５０$_{\beta}$，１５０$_{\gamma}$は、ｋ＝１～Ｋについて、Ｑ$_{k}$＝Ｐ$_{\pi(k)}$である数値Ｑ$_{k}$の断片（ｑ$_{k\gamma\alpha}$，ｑ$_{k\alpha\beta}$）、（ｑ$_{k\alpha\beta}$，ｑ$_{k\beta\gamma}$）、（ｑ$_{k\beta\gamma}$，ｑ$_{k\gamma\alpha}$）を秘密計算によって生成し、秘密分散装置１００$_{\alpha}$，１００$_{\beta}$，１００$_{\gamma}$に分散して記録する（Ｓ１５０）。例えば、ステップＳ１３０で第１の秘密分散装置１００$_{1}$が生成した数値Ｒ$^{(1)}_{\pi(k)}$の別の断片（ｒ’$^{(1)}_{\pi(k)31}$，ｒ’$^{(1)}_{\pi(k)12}$）、（ｒ’$^{(1)}_{\pi(k)12}$，ｒ’$^{(1)}_{\pi(k)23}$）、（ｒ’$^{(1)}_{\pi(k)23}$，ｒ’$^{(1)}_{\pi(k)31}$）と、第２の秘密分散装置１００$_{2}$が生成した数値Ｒ$^{(2)}_{\pi(k)}$の別の断片（ｒ’$^{(2)}_{\pi(k)31}$，ｒ’$^{(2)}_{\pi(k)12}$）、（ｒ’$^{(2)}_{\pi(k)12}$，ｒ’$^{(2)}_{\pi(k)23}$）、（ｒ’$^{(2)}_{\pi(k)23}$，ｒ’$^{(2)}_{\pi(k)31}$）とを秘密分散して記録する。その後、秘密分散装置１００$_{1}$，１００$_{2}$，１００$_{3}$で、Ｑ$_{k}$＝Ｒ$^{(1)}_{\pi(k)}$＋Ｒ$^{(2)}_{\pi(k)}$である数値Ｑ$_{k}$の断片（ｑ$_{k31}$，ｑ$_{k12}$）、（ｑ$_{k12}$，ｑ$_{k23}$）、（ｑ$_{k23}$，ｑ$_{k31}$）を別の断片を用いて秘密計算によって求め、秘密分散装置１００$_{1}$，１００$_{2}$，１００$_{3}$に分散して記録する。このような処理によって、Ｑ$_{k}$＝Ｐ$_{\pi(k)}$であり、かつ、全ての秘密分散装置１００$_{\alpha}$，１００$_{\beta}$，１００$_{\gamma}$が知らない数値の断片を分散して記録できる。

【００７０】

確認乗算手段は、確認乗算部１６０$_{\alpha}$，１６０$_{\beta}$，１６０$_{\gamma}$で構成される。確認乗算部１６０$_{\alpha}$，１６０$_{\beta}$，１６０$_{\gamma}$は、Ｔ$_{k}$＝Ｑ$_{k}$×Ｂ$_{k}$である数値Ｔ$_{k}$の断片（ｔ$_{k\gamma\alpha}$，ｔ$_{k\alpha\beta}$）、（ｔ$_{k\alpha\beta}$，ｔ$_{k\beta\gamma}$）、（ｔ$_{k\beta\gamma}$，ｔ$_{k\gamma\alpha}$）を秘密計算によって求め、秘密分散装置１００$_{\alpha}$，１００$_{\beta}$，１００$_{\gamma}$に分散して記録する（Ｓ１６０）。

【００７１】

改ざん検出手段は、改ざん検出部１７０$_{\alpha}$，１７０$_{\beta}$，１７０$_{\gamma}$で構成される。また、図９に示すように、改ざん検出部１７０$_{n}$は、第３乱数生成部１７１$_{n}$、第４乱数生成部１７２$_{n}$、第４計算部１７３$_{n}$、第５計算部１７４$_{n}$、第１確認部１７５$_{n}$、第６計算部１７６$_{n}$、第７計算部１７７$_{n}$、第２確認部１７８$_{n}$を備える。改ざん検出手段は、秘密分散装置１００$_{\alpha}$，１００$_{\beta}$，１００$_{\gamma}$が第１の秘密分散装置１００$_{1}$、第２の秘密分散装置１００$_{2}$、第３の秘密分散装置１００$_{3}$のいずれの装置として動作するかにしたがって、以下のように処理を行う。

【００７２】

第１の秘密分散装置１００$_{1}$の第３乱数生成部１７１$_{1}$は、ランダムな値であるｕ$_{k}$を生成し、第２の秘密分散装置１００$_{2}$に送信する（Ｓ１７１）。第２の秘密分散装置１００$_{2}$の第４乱数生成部１７２$_{2}$は、ランダムな値であるｖ$_{k}$を生成し、第１の秘密分散装置１００$_{1}$に送信する（Ｓ１７２）。第１の秘密分散装置１００$_{1}$の第４計算部１７３$_{1}$は、ｄ$_{k}$＝ｓ$_{\pi(k)12}$－ｔ$_{k12}$－ｕ$_{k}$－ｖ$_{k}$を計算し、第３の秘密分散装置１００$_{3}$に送信する（Ｓ１７３）。

【００７３】

第２の秘密分散装置１００$_{2}$の第５計算部１７４$_{2}$は、ｅ$_{k}$＝ｓ$_{\pi(k)12}$－ｔ$_{k12}$－ｕ$_{k}$－ｖ$_{k}$を計算し、第３の秘密分散装置１００$_{3}$に送信する（Ｓ１７４）。第３の秘密分散装置１００$_{3}$の第１確認部１７５$_{3}$は、ｄ$_{k}$＝ｅ$_{k}$であることを確認し、異なっていれば処理を中止する（Ｓ１７５）。

【００７４】

第１の秘密分散装置１００$_{1}$の第６計算部１７６$_{1}$は、ｆ$_{k}$＝ｓ$_{\pi(k)31}$－ｔ$_{k31}$＋ｕ$_{k}$を計算し、第３の秘密分散装置１００$_{3}$に送信する（Ｓ１７６）。第２の秘密分散装置１００$_{2}$の第７計算部１７７$_{2}$は、ｇ$_{k}$＝ｓ$_{\pi(k)23}$－ｔ$_{k23}$＋ｖ$_{k}$を計算し、第３の秘密分散装置１００$_{3}$に送信する（Ｓ１７７）。第３の秘密分散装置１００$_{3}$の第２確認部１７８$_{3}$は、ｆ$_{k}$＋ｇ$_{k}$＋ｄ$_{k}$＝０であることを確認し、異なっていれば処理を中止する（Ｓ１７８）。また、数値Ｂ$_{1}$，…，Ｂ$_{K}$を新しい数値Ａ$_{1}$，…，Ａ$_{K}$とし

、断片置換手段で選択する秘密分散装置の組み合わせを変更すれば、この処理を繰り返すことができる（Ｓ１１１，Ｓ１１２）。

【００７５】

実施例４の秘密分散システムによれば、実施例３の秘密分散装置と同じ効果が得られると共に、数値A_1，…，A_Kと数値B_1，…，B_Kとの対応を分からなくする処理の途中に、他の秘密分散装置に改ざんした値を送信する不正がないことも確認できる。なお、ソートも行う場合は、秘密分散装置100_nは、比較部210_nと交換部220_nも備える。具体的なソートの処理については実施例１と同じである。

【００７６】

［秘密計算］

上述の説明では、秘密計算については１つの方法に限定しないことを前提としており、具体例は示さなかった。以下では、実施例３、４の秘密分散システムの各構成部が利用できる基本的な秘密計算の具体例を示す。なお、以下の説明では、秘密分散装置100_α，100_β，100_γが分散して記録する数値Ａの断片を（$a_{\gamma\alpha}$，$a_{\alpha\beta}$）、（$a_{\alpha\beta}$，$a_{\beta\gamma}$）、（$a_{\beta\gamma}$，$a_{\gamma\alpha}$）、数値Ｂの断片を（$b_{\gamma\alpha}$，$b_{\alpha\beta}$）、（$b_{\alpha\beta}$，$b_{\beta\gamma}$）、（$b_{\beta\gamma}$，$b_{\gamma\alpha}$）、数値Ｃの断片を（$c_{\gamma\alpha}$，$c_{\alpha\beta}$）、（$c_{\alpha\beta}$，$c_{\beta\gamma}$）、（$c_{\beta\gamma}$，$c_{\gamma\alpha}$）とする。

【００７７】

数値Ａの秘密分散

（１）乱数$a_{\alpha\beta}$，$a_{\beta\gamma}$を生成する。

（２）$a_{\gamma\alpha}=A-a_{\alpha\beta}-a_{\beta\gamma}$を計算し、断片を（$a_{\gamma\alpha}$，$a_{\alpha\beta}$）、（$a_{\alpha\beta}$，$a_{\beta\gamma}$）、（$a_{\beta\gamma}$，$a_{\gamma\alpha}$）とし、秘密分散装置$100_\alpha$，$100_\beta$，$100_\gamma$に分散して記録する。

【００７８】

数値Ａの復元

（１）秘密分散装置100_αは秘密分散装置100_βに$a_{\gamma\alpha}$を送信し、秘密分散装置100_γに$a_{\alpha\beta}$を送信する。秘密分散装置100_βは秘密分散装置100_γに$a_{\alpha\beta}$を送信し、秘密分散装置100_αに$a_{\beta\gamma}$を送信する。秘密分散装置100_γは秘密分散装置100_αに$a_{\beta\gamma}$を送信し、秘密分散装置100_βに$a_{\gamma\alpha}$を送信する。

（２）秘密分散装置100_αは秘密分散装置100_βから受信した$a_{\beta\gamma}$と秘密分散装置100_γから受信した$a_{\beta\gamma}$とが一致していれば、$a_{\alpha\beta}+a_{\beta\gamma}+a_{\gamma\alpha}$を計算して数値Ａを復元する。秘密分散装置$100_\beta$は秘密分散装置$100_\gamma$から受信した$a_{\gamma\alpha}$と秘密分散装置$100_\alpha$から受信した$a_{\gamma\alpha}$とが一致していれば、$a_{\alpha\beta}+a_{\beta\gamma}+a_{\gamma\alpha}$を計算して数値Ａを復元する。秘密分散装置$100_\gamma$は秘密分散装置$100_\alpha$から受信した$a_{\alpha\beta}$と秘密分散装置$100_\beta$から受信した$a_{\alpha\beta}$とが一致していれば、$a_{\alpha\beta}+a_{\beta\gamma}+a_{\gamma\alpha}$を計算して数値Ａを復元する。

【００７９】

Ｃ＝Ａ＋Ｂの秘密計算

（１）秘密分散装置100_αは（$c_{\gamma\alpha}$，$c_{\alpha\beta}$）＝（$a_{\gamma\alpha}+b_{\gamma\alpha}$，$a_{\alpha\beta}+b_{\alpha\beta}$）を計算して記録し、秘密分散装置$100_\beta$は（$c_{\alpha\beta}$，$c_{\beta\gamma}$）＝（$a_{\alpha\beta}+b_{\alpha\beta}$，$a_{\beta\gamma}+b_{\beta\gamma}$）を計算して記録し、秘密分散装置$100_\gamma$は（$c_{\beta\gamma}$，$c_{\gamma\alpha}$）＝（$a_{\beta\gamma}+b_{\beta\gamma}$，$a_{\gamma\alpha}+b_{\gamma\alpha}$）を計算して記録する。

【００８０】

Ｃ＝Ａ－Ｂの秘密計算

（１）秘密分散装置100_αは（$c_{\gamma\alpha}$，$c_{\alpha\beta}$）＝（$a_{\gamma\alpha}-b_{\gamma\alpha}$，$a_{\alpha\beta}-b_{\alpha\beta}$）を計算して記録し、秘密分散装置$100_\beta$は（$c_{\alpha\beta}$，$c_{\beta\gamma}$）＝（$a_{\alpha\beta}-b_{\alpha\beta}$，$a_{\beta\gamma}-b_{\beta\gamma}$）を計算して記録し、秘密分散装置$100_\gamma$は（$c_{\beta\gamma}$，$c_{\gamma\alpha}$）＝（$a_{\beta\gamma}-b_{\beta\gamma}$，$a_{\gamma\alpha}-b_{\gamma\alpha}$）を計算して記録する。

【００８１】

Ｃ＝Ａ＋Ｓの秘密計算（ただし、Ｓは既知の定数）

（１）秘密分散装置１００$_{\alpha}$は（$c_{\gamma\alpha}$，$c_{\alpha\beta}$）＝（$a_{\gamma\alpha}$＋Ｓ，$a_{\alpha\beta}$）を計算して記録し、秘密分散装置１００$_{\gamma}$は（$c_{\beta\gamma}$，$c_{\gamma\alpha}$）＝（$a_{\beta\gamma}$，$a_{\gamma\alpha}$＋Ｓ）を計算して記録する。秘密分散装置１００$_{\beta}$の処理はない。

【００８２】

Ｃ＝ＡＳの秘密計算（ただし、Ｓは既知の定数）

（１）秘密分散装置１００$_{\alpha}$は（$c_{\gamma\alpha}$，$c_{\alpha\beta}$）＝（$a_{\gamma\alpha}$Ｓ，$a_{\alpha\beta}$Ｓ）を計算して記録し、秘密分散装置１００$_{\beta}$は（$c_{\alpha\beta}$，$c_{\beta\gamma}$）＝（$a_{\alpha\beta}$Ｓ，$a_{\beta\gamma}$Ｓ）を計算して記録し、秘密分散装置１００$_{\gamma}$は（$c_{\beta\gamma}$，$c_{\gamma\alpha}$）＝（$a_{\beta\gamma}$Ｓ，$a_{\gamma\alpha}$Ｓ）を計算して記録する。

【００８３】

Ｃ＝ＡＢの秘密計算

（１）秘密分散装置１００$_{\alpha}$は、乱数r_1，r_2，$c_{\gamma\alpha}$を生成し、$c_{\alpha\beta}$＝（$a_{\gamma\alpha}$＋$a_{\alpha\beta}$）（$b_{\gamma\alpha}$＋$b_{\alpha\beta}$）－r_1－r_2－$c_{\gamma\alpha}$を計算する。そして、秘密分散装置１００$_{\alpha}$は、秘密分散装置１００$_{\beta}$に（r_1，$c_{\alpha\beta}$）を、秘密分散装置１００$_{\gamma}$に（r_2，$c_{\gamma\alpha}$）を送信する。

（２）秘密分散装置１００$_{\beta}$は、$y=a_{\alpha\beta}b_{\beta\gamma}+a_{\beta\gamma}b_{\alpha\beta}+r_1$を計算し、秘密分散装置１００$_{\gamma}$に送信する。

（３）秘密分散装置１００$_{\gamma}$は、$z=a_{\beta\gamma}b_{\gamma\alpha}+a_{\gamma\alpha}b_{\beta\gamma}+r_2$を計算し、秘密分散装置１００$_{\alpha}$に送信する。

（４）秘密分散装置１００$_{\beta}$と秘密分散装置１００$_{\gamma}$は、それぞれ$c_{\beta\gamma}=y+z+a_{\beta\gamma}b_{\beta\gamma}$を計算する。

（５）秘密分散装置１００$_{\alpha}$は（$c_{\gamma\alpha}$，$c_{\alpha\beta}$）を記録し、秘密分散装置１００$_{\beta}$は（$c_{\alpha\beta}$，$c_{\beta\gamma}$）を記録し、秘密分散装置１００$_{\gamma}$は（$c_{\beta\gamma}$，$c_{\gamma\alpha}$）を記録する。

【００８４】

［プログラム、記録媒体］

上述の各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。その他、本発明の趣旨を逸脱しない範囲で適宜変更が可能であることはいうまでもない。

【００８５】

また、上述の構成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、上記処理機能がコンピュータ上で実現される。

【００８６】

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。

【００８７】

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。

【００８８】

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。

【００８９】

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】

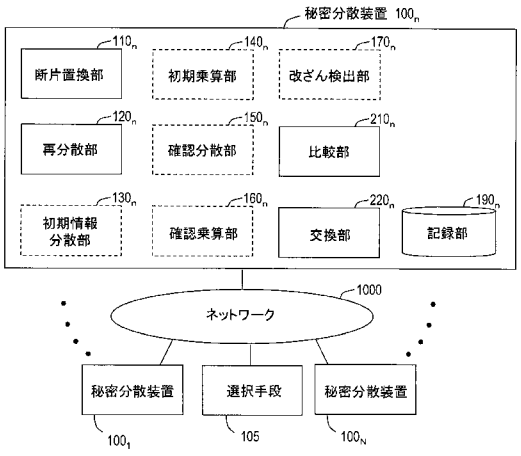

図1

【図２】

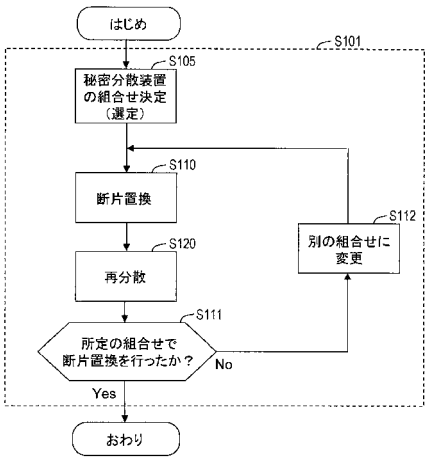

図2

【図３】

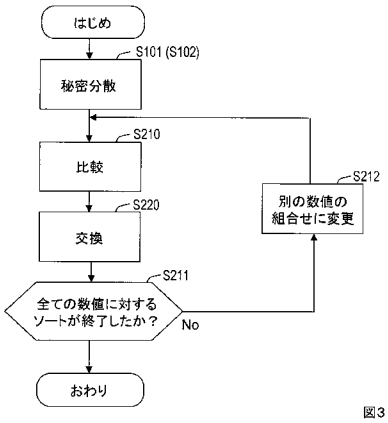

図3

【図４】

Algorithm 1 Quicksort(*A*, *p*, *r*)
1: **return unless** *p* < *r*
2: *q* ← Partition(*A*, *p*, *r*) // Algorithm 2
3: Quicksort(*A*, *p*, *q* -1)
4: Quicksort(*A*, *q* + 1, *r*)

Algorithm 2 Partition(*A*, *p*, *r*)
1: *i* ← *p* -1
2: **for** *j* ← *p* **to** *r* -1 **do**
3: **if** *A*[*j*] ≦*A*[*r*] **then**
4: *i* ← *i* + 1
5: swap(*A*[*i*] , *A*[*j*]) // *A*[*i*] , *A*[*j*] を交換
6: **end if**
7: **end for**
8: swap(*A*[*i* + 1], *A*[*r*])
9: **return** *i* + 1

図4

【図５】

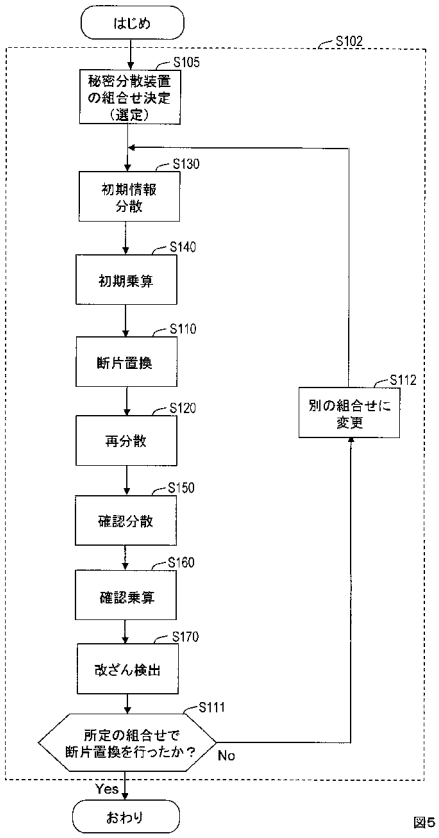

図5

【図６】

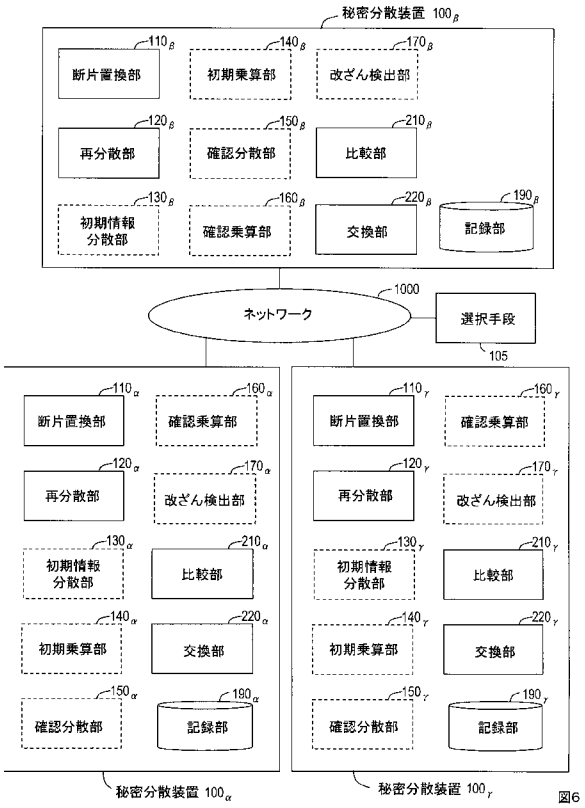

図6

【図７】

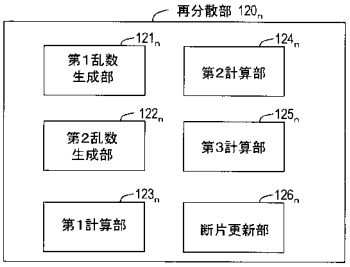

図7

【図８】

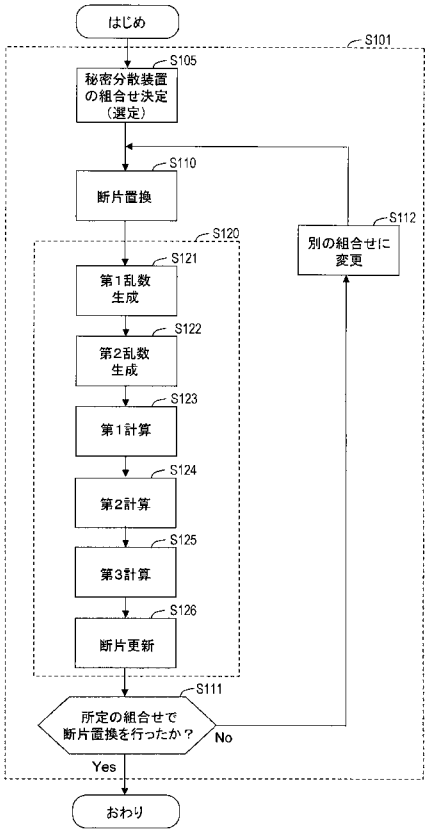

図8

【図９】

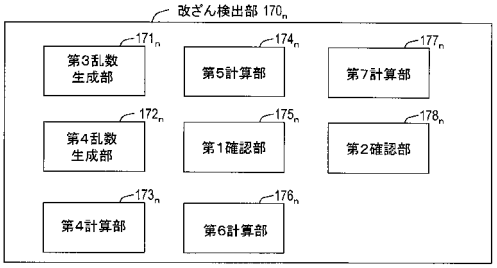

図9

【図１０】

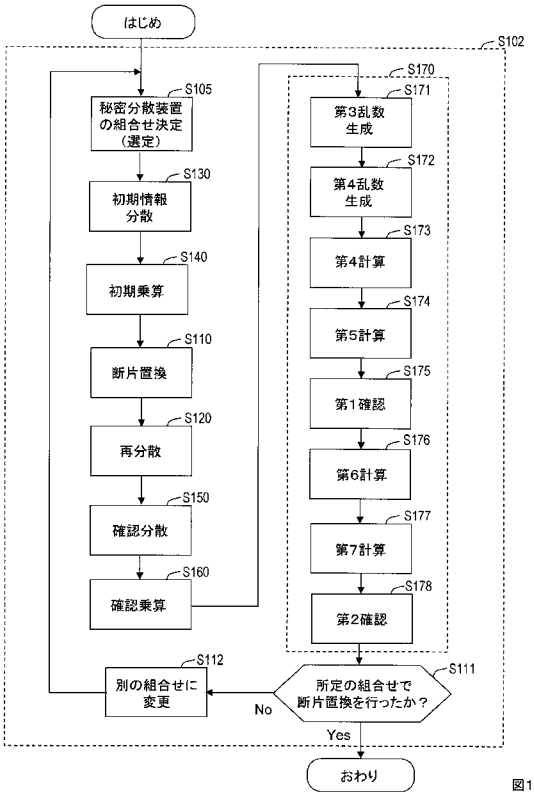

図10

フロントページの続き

(72)発明者　千田　浩司
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　高橋　克巳
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

審査官　松平　英

(56)参考文献　特開２００５－２２７３３１（ＪＰ，Ａ）
特開２００７－３００１５７（ＪＰ，Ａ）
千田　浩司　他，効率的な３パーティ秘匿関数計算の提案とその運用モデルの考察，情報処理学会研究報告　コンピュータセキュリティ（ＣＳＥＣ），日本，社団法人情報処理学会，２０１０年　4月１５日，Ｎｏ．４８，p.1-7
千田　浩司　他，軽量検証可能３パーティ秘匿関数計算の再考，コンピュータセキュリティシンポジウム２０１０　論文集　［第二分冊］，日本，一般社団法人情報処理学会　Information Processing Society of Japan，２０１０年１０月１２日，p.555-560
濱田　浩気　他，３パーティ秘匿関数計算上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　論文集　［第二分冊］，日本，一般社団法人情報処理学会，２０１２年１０月１２日，p.561-566

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　　１／００
Ｈ０４Ｌ　　９／００
Ｇ０６Ｆ　２１／２４