(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
2014 年 1 月 9 日(09.01.2014)

WIPO | PCT

(10) 国際公開番号
WO 2014/007310 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *G06F 21/62* (2013.01)

(21) 国際出願番号: PCT/JP2013/068328

(22) 国際出願日: 2013 年 7 月 4 日(04.07.2013)

(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 2012-151140 2012 年 7 月 5 日(05.07.2012) 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二丁目３番１号 Tokyo (JP).

(72) 発明者: 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). 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).

(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, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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.

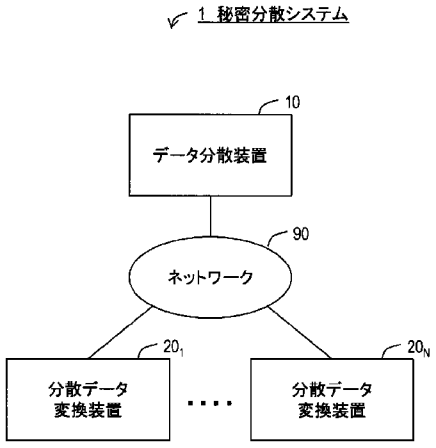
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI

[続葉有]

(54) **Title**: SECRET SHARING SYSTEM, DATA DISTRIBUTION DEVICE, DISTRIBUTED DATA CONVERSION DEVICE, SECRET SHARING METHOD, AND PROGRAM

(54) 発明の名称 : 秘密分散システム、データ分散装置、分散データ変換装置、秘密分散方法、およびプログラム

[図1]



1... SECRET SHARING SYSTEM
10... DATA DISTRIBUTION DEVICE
201, 20N... DISTRIBUTED DATA CONVERSION DEVICE
90... NETWORK

(57) **Abstract**: A secret sharing system converts a computational secret sharing distribution value to a homomorphic secret sharing distribution value. In a data distribution device, a key selection unit selects K'-1 number of keys (s_j). A pseudorandom number generation unit generates a pseudorandom number (r_j) from the keys (s_j). An encryption unit generates an encrypted text (c) from a set of information (a) by using the pseudorandom number (r_j). A key distribution unit distributes the keys (s_j) into N number of distribution values ($f_{sj}(n)$) by means of a given secret sharing method (S1). An encrypted text distribution unit distributes the encrypted text (c) into N number of distribution values ($f_c(n)$) by means of a given distribution method (S0). In a distributed data conversion device, when K number of distribution values ($f_{sj}(i)$) are inputted, a decompression unit extracts distribution values ($f_{sj}(i)$) by means of the secret sharing method (S1) and generates a decompression value (U_j), and when K number of distribution values ($f_c(i)$) are inputted, the decompression unit extracts distribution values ($f_c(i)$) by means of the given distribution method (S0) and generates a decompression value ($U_j(j=K')$). A redistribution unit distributes decompression value (U_j) into N number of distribution values ($f_{Uj}(n)$) by means of a homomorphic secret sharing method (S2). A conversion unit generates a distribution value ($g_a(i)$) of the information (a) from K' number of distribution values (f_{Uj}).

(57) 要約:

[続葉有]

WO 2014/007310 A1

(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)）

秘密分散システムは、計算量型秘密分散の分散値を、準同型性をもつ秘密分散の分散値に変換する。データ分散装置は、鍵選択部が、K'-1 個の鍵 s_j を選択する。擬似乱数生成部が鍵 s_j から擬似乱数 r_j を生成する。暗号化部が、情報 a から擬似乱数 r_j を用いて暗号文 c を生成する。鍵分散部が、鍵 s_j を任意の秘密分散方式 S1 によりそれぞれ N 個の分散値 $f_{sj}(n)$に分散する。暗号文分散部が、暗号文 c を任意の分散方式 S0 により N 個の分散値 $f_c(n)$に分散する。分散データ変換装置は、復元部が、K 個の分散値 $f_{sj}(i)$が入力されると、分散値 $f_{sj}(i)$を秘密分散方式 S1 により復元し、復元値 U_j を生成し、K 個の分散値 $f_c(i)$が入力されると、分散値 $f_c(i)$を分散方式 S0 により復元することで、復元値 $U_j(j=K')$を生成する。再分散部が、準同型性をもつ秘密分散方式 S2 により復元値 U_j を N 個の分散値 $f_{Uj}(n)$に分散する。変換部が、K'個の分散値 f_{Uj} から情報 a の分散値 $g_a(i)$を生成する。

明　細　書

発明の名称 ：

秘密分散システム、データ分散装置、分散データ変換装置、秘密分散方法、およびプログラム

技術分野

[0001] この発明は、計算量型秘密分散技術およびマルチパーティ計算技術に関する。

背景技術

[0002] 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。分散値の総数をN、復元に必要な分散値の最小数をK（≦N）としたとき、N,Kの値に制限がない方式と制限がある方式とがある。

[0003] 秘密分散の代表的な方式として、Shamir秘密分散方式がある（例えば、非特許文献１参照）。この方式の例では、pを素数、GF(p)を位数pの有限体として、a∈GF(p)に対してf(0)=aとなるような、xを変数とするK-1次式f(x)から、aの分散値$S_i(a)=f(i)$（i=1,…,N）を得る。$n_1,\cdots,n_K$を互いに異なる1以上N以下の整数として以下の関係が成り立つため、任意の異なるK個の分散値からaを復元できる。

[数1]

$$a=f(0)=\sum_{i=1}^{K} f(n_i)\cdot L_i(0)$$

$$L_i(x)=\prod_{j\neq i,j=1}^{K}\frac{x-n_j}{n_i-n_j}$$

[0004] また、秘密分散の一種として、計算量的安全性に基づ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、計算量型秘密分散方式がある（例えば、非特許文献２参照）。この方式の例では、情報$a=(a_0,a_1,\cdots,a_{K-1})$(

$a_0, a_1, \cdots, a_{K-1} \in GF(p)$)を共通鍵暗号を用いて暗号化し、当該暗号文$c=(c_0, c_1, \cdots, c_{K-1})$（ただし$c_0, c_1, \cdots, c_{K-1} \in GF(p)$）から決まる、xを変数とするK-1次式$f(x)=c_0+c_1x+\cdots+c_{K-1}x^{K-1}$から、cの分散値$T_i(c)=f(i)(i=1,\cdots,N)$を得る。また、共通鍵は別途Shamir秘密分散方式などにより分散する。すると、$n_1, \cdots, n_K$を互いに異なる1以上N以下の整数として、式f(x)のK個の点$(n_i, f(n_i))(i=1,\cdots,K)$から式f(x)の係数$c_0, c_1, \cdots, c_{K-1}$を一意に求めることができる。これは$c_0, c_1, \cdots, c_{K-1}$を変数とする以下の行列について$c_0, c_1, \cdots, c_{K-1}$の解を求めればよい。

[数2]

$$\begin{pmatrix} f(n_1) \\ \vdots \\ f(n_K) \end{pmatrix} = \begin{pmatrix} n_1^0 & \cdots & n_1^{K-1} \\ \vdots & \ddots & \vdots \\ n_K^0 & \cdots & n_K^{K-1} \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{K-1} \end{pmatrix}$$

そして共通鍵を復元して、cを復号すれば、aを得ることができる。

[0005] 一方、秘密分散を要素技術としたマルチパーティ計算方式が提案されている。マルチパーティ計算は、各計算主体$i(i=1,\cdots,N)$がそれぞれ情報a_iを入力として、他の計算主体に情報a_iを明かすことなく、特定の関数値$F_i(a_1, \cdots, a_N)$を得る技術である。上述のShamir秘密分散方式では、情報$a,b \in GF(p)$の分散値$S_i(a), S_i(b)$から、各計算主体の入力を明かさず、a+bの分散値$S_i(a+b)$およびabの分散値$S_i(ab)$を得ることができる（非特許文献３参照）。すなわち、Shamir秘密分散方式であれば、加算および乗算のマルチパーティ計算ができる。なお、$S_i(a)+S_i(b)=S_i(a+b)$の関係を満たす秘密分散を、加法準同型性をもつ秘密分散と呼ぶ。

[0006] また、秘密分散の一種として、線形秘密分散方式がある。線形秘密分散方式は、元のデータ$a \in GF(p)$についてすべての分散値が$a \in GF(p)$および$GF(p)$上の乱数の線形結合で表現できる秘密分散と定義される。任意の線形秘密分散方式をマルチパーティ計算に拡張できることが知られている（非特許文献４参照）。

先行技術文献

非特許文献

[0007] 非特許文献1：A.Shamir, “How to share a secret.”, Commun. ACM 22(11), pp. 612-613, 1979.

非特許文献2：H.Krawczyk, “Secret sharing made short.”, CRYPTO 1993, pp. 136-146, 1993.

非特許文献3：M. Ben-Or, S. Goldwasser, and A. Wigderson, “Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract),” STOC 1988, pp. 1-10, 1988.

非特許文献4：R. Cramer, I. Damgard, and U. Maurer, “General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme”, Eurocrypto 2000, pp. 316-334, 2000.

発明の概要

発明が解決しようとする課題

[0008] Shamir秘密分散方式では、情報aおよびその各分散値のデータ量を一定とすると、分散値の総データ量がそれぞれ情報aのデータ量のおよそN倍となる。復元に必要な分散値の総データ量はそれぞれ情報aのデータ量のおよそK倍となる。分散値のデータ量の増加は通信時間や保存データの増大につながるため、できるだけ分散値のデータ量を抑えることが望ましい。

[0009] 計算量型秘密分散方式は一般に$T_i(a)+T_i(b)\neq T_i(a+b)$となる。したがって、計算量型秘密分散方式では、Shamir秘密分散方式とは異なり、各入力の加算のマルチパーティ計算を行う方法は自明でない。しかし、計算量型秘密分散方式には、分散値の総データ量や復元に必要な分散値の総データ量をShamir秘密分散方式よりも少なくできるという利点がある。

[0010] この発明はこのような点に鑑みてなされたものであり、計算量型秘密分散方式による分散値を用いてマルチパーティ計算を行うことができる秘密分散技術を提供することを目的とする。

課題を解決するための手段

[0011] 上記の課題を解決するために、この発明の一態様の秘密分散システムは、データ分散装置とN台の分散データ変換装置を含む。この発明では、N,Kは2以上の整数であり、N≧Kであり、n=1,…,Nであり、λは互いに異なる1以上N以下のK個の整数であり、iはi∈λの整数であり、$f_x(n)$はxのN個の分散値であり、Rは環であり、Sは鍵空間であり、P(x)はx∈Sを環Rへ移す写像であるものとする。

[0012] この態様のデータ分散装置は、鍵選択部と擬似乱数生成部と暗号化部と鍵分散部と暗号文分散部とを備える。鍵選択部は、K-1個の鍵$s_1,\cdots,s_{K-1}\in S$を選択する。擬似乱数生成部は、鍵$s_1,\cdots,s_{K-1}$から$r_j=P(s_j)(j=1,\cdots,K-1)$を計算することにより擬似乱数$r_1,\cdots,r_{K-1}$を生成する。暗号化部は、情報a∈Rから擬似乱数$r_1,\cdots,r_{K-1}$を用いて暗号文cを生成する。鍵分散部は、鍵$s_{1,\cdots,}s_{K-1}$を任意の秘密分散方式S1によりそれぞれN個の分散値$f_{s1}(n),\cdots,f_{sK-1}(n)$に分散する。暗号文分散部は、暗号文cを任意の秘密分散方式S0によりN個の分散値$f_c(n)$に分散する。

[0013] この態様の分散データ変換装置は、復元部と再分散部と変換部とを備える。復元部は、K個の分散値$f_{sj}(i)$が入力されると、分散値$f_{sj}(i)$を所定の秘密分散方式S1により復元した値u_jから$U_j=P(u_j)$を計算し、K個の分散値$f_c(i)$が入力されると、分散値$f_c(i)$を所定の秘密分散方式S0により復元することで、復元値$U_j(j=K)$を生成する。再分散部は、復元値U_jを任意の準同型性をもつ秘密分散方式S2によりN個の分散値$f_{Uj}(n)$に分散する。変換部は、K個の分散値$f_{U1}(i),\cdots,f_{UK}(i)$から情報aの分散値$g_a(i)$を生成する。

[0014] この発明の他の一態様の秘密分散システムは、データ分散装置とN台の分散データ変換装置を含む。この発明では、N,K, K'は2以上の整数であり、N≧Kであり、n=1,…,Nであり、λは互いに異なる1以上N以下のK個の整数であり、iはi∈λの整数であり、$f_x(n)$はxのN個の分散値であり、Rは環であり、Sは鍵空間であり、P(x)はx∈Sを環Rへ移す写像であるものとする。

[0015] この態様のデータ分散装置は、鍵選択部と擬似乱数生成部と暗号化部と鍵分散部と暗号文分散部とを備える。鍵選択部は、K'-1個の鍵$s_1,\cdots,s_{K'-1}\in S$を

選択する。擬似乱数生成部は、鍵$s_1,\cdots,s_{K'-1}$から$r_j=P(s_j)(j=1,\cdots,K'-1)$を計算することにより擬似乱数$r_1,\cdots,r_{K'-1}$を生成する。暗号化部は、情報$a\in R$から擬似乱数$r_1,\cdots,r_{K'-1}$を用いて暗号文cを生成する。鍵分散部は、鍵$s_{1,\cdots,}s_{K'-1}$を任意の秘密分散方式S1によりそれぞれN個の分散値$f_{s1}(n),\cdots,f_{sK'-1}(n)$に分散する。暗号文分散部は、暗号文cを任意の分散方式S0によりN個の分散値$f_c(n)$に分散する。

[0016] この態様の分散データ変換装置は、復元部と再分散部と変換部とを備える。復元部は、K個の分散値$f_{sj}(i)$が入力されると、分散値$f_{sj}(i)$を所定の秘密分散方式S1により復元した値u_jから$U_j=P(u_j)$を計算し、K個の分散値$f_c(i)$が入力されると、分散値$f_c(i)$を所定の分散方式S0により復元することで、復元値$U_j(j=K')$を生成する。再分散部は、復元値U_jを任意の準同型性をもつ秘密分散方式S2によりN個の分散値$f_{Uj}(n)$に分散する。変換部は、K'個の分散値$f_{U1}(i),\cdots,f_{UK'}(i)$から情報aの分散値$g_a(i)$を生成する。

発明の効果

[0017] この発明の秘密分散技術によれば、計算量型秘密分散方式による分散値を、任意の準同型性をもつ秘密分散方式による分散値に変換することができる。例えば、Shamir秘密分散方式など既存の多くの線形秘密分散方式は準同型性をもつ秘密分散方式であり、Shamir秘密分散方式など既存の線形秘密分散方式による分散値を用いてマルチパーティ計算を行う方法は既知である。そのため、準同型性をもつ秘密分散方式としてShamir秘密分散方式など既存の線形秘密分散方式を選択することで、計算量型秘密分散方式による分散値を用いてマルチパーティ計算を行うことができるようになる。また、暗号文cを分散する秘密分散方式S0として符号化効率がよい計算量型秘密分散方式を適用すれば、分散値のサイズが小さくなるため、保存する分散値の総データ容量および復元に必要な分散値の総データ容量を減らすことができる。

図面の簡単な説明

[0018] [図1]図１は、第一実施形態の秘密分散システムの機能構成を例示する図である。

[図2]図２は、第一実施形態のデータ分散装置の機能構成を例示する図である。

[図3]図３は、第一実施形態の分散データ変換装置の機能構成を例示する図である。

[図4]図４は、第一実施形態のデータ分散装置の処理フローを例示する図である。

[図5]図５は、第一実施形態の分散データ変換装置の処理フローを例示する図である。

[図6]図６は、第二実施形態の秘密分散システムの機能構成を例示する図である。

[図7]図７は、第二実施形態のデータ分散装置の機能構成を例示する図である。

[図8]図８は、第二実施形態の分散データ変換装置の機能構成を例示する図である。

[図9]図９は、第二実施形態のデータ分散装置の処理フローを例示する図である。

[図10]図１０は、第二実施形態の分散データ変換装置の処理フローを例示する図である。

発明を実施するための形態

[0019] 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］

この発明の第一実施形態に係る秘密分散システムは、計算量型秘密分散方式による分散値を、準同型性をもつ任意の秘密分散方式による分散値に変換する。

[0020] ＜構成＞

図１を参照して、第一実施形態に係る秘密分散システム１の構成例を説明する。秘密分散システム１は、データ分散装置１０と少なくともN台の分散デ

ータ変換装置２０$_1$～２０$_N$とネットワーク９０を含む。データ分散装置１０と分散データ変換装置２０$_1$～２０$_N$は、ネットワーク９０に接続される。ネットワーク９０は、データ分散装置１０と分散データ変換装置２０$_1$～２０$_N$それぞれと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、データ分散装置１０と分散データ変換装置２０$_1$～２０$_N$それぞれとは必ずしもネットワーク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、データ分散装置１０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分散データ変換装置２０$_1$～２０$_N$へオフラインで入力するように構成してもよい。

[0021] 図２を参照して、秘密分散システム１に含まれるデータ分散装置１０の構成例を説明する。データ分散装置１０は、入力部１１０と鍵選択部１２０と擬似乱数生成部１３０と暗号化部１４０と鍵分散部１５０と暗号文分散部１６０と出力部１７０とを備える。

[0022] 図３を参照して、秘密分散システム１に含まれる分散データ変換装置２０の構成例を説明する。分散データ変換装置２０は、入力部２１０と復元部２２０と再分散部２３０と変換部２４０と出力部２５０と記憶部２９０とを備える。記憶部２９０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）などの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。

[0023] ＜データ分散処理＞

図４を参照して、データ分散装置１０の動作例を、実際に行われる手続きの順に従って説明する。以下の説明では、N,Kは2以上の整数であり、N≧Kであり、n=1,…,Nであり、λは互いに異なる1以上N以下のK個の整数であり、iはi∈λの整数であり、$f_x(n)$はxのN個の分散値であり、Rは環であり、Sは鍵空間であり、P(x)はx∈Sを環Rへ移す写像であるものとする。写像P(x)は、入力

されたx∈Sに対して環Rの要素を出力するものである。同一の入力xには同一のP(x)が対応する。すなわち、写像P(x)は入力が等しければ出力も等しくなる、確定的な写像である。入力xとP(x)とは一対一で対応してもよいし、しなくてもよい。例えば、写像P(x)はxをシードとして環Rの要素を返す擬似乱数生成関数である。また例えば、写像P(x)はxを暗号化鍵として固定の平文に対して環Rに属する暗号文を出力する共通鍵暗号関数である。写像P(x)は関数であってもよいし、アルゴリズムであってもよい。

[0024] ステップＳ１１０において、入力部１１０に、情報aが入力される。情報aは環Rに含まれる値である。したがって、a∈Rと表すことができる。情報aの例は、動画ファイル、音声ファイル、テキストファイル、表ファイルなどである。情報aのデータ量は、例えば1メガバイト以上である。

[0025] ステップＳ１２０において、鍵選択部１２０は、K-1個の鍵$s_1,\cdots,s_{K-1}\in S$を選択する。鍵選択部１２０は、逐一ランダムにK-1個の鍵$s_1,\cdots,s_{K-1}$を選択してもよいし、事前に生成されメモリに格納されている複数個の値から所定の規則に従ってK-1個の鍵$s_1,\cdots,s_{K-1}$を選択してもよい。鍵$s_1,\cdots,s_{K-1}$の鍵長は、必要な安全性と許容できる処理性能を確保できる長さに設定する。例えば、128～256ビットとするのが一般的であるが、この限りではない。

[0026] 鍵$s_1,\cdots,s_{K-1}$は擬似乱数生成部１３０に入力される。ステップＳ１３０において、擬似乱数生成部１３０は、鍵$s_1,\cdots,s_{K-1}$から$r_j=P(s_j)(j=1,\cdots,K-1)$を計算することにより擬似乱数$r_1,\cdots,r_{K-1}$を生成する。

[0027] 情報aと擬似乱数$r_1,\cdots,r_{K-1}$は暗号化部１４０に入力される。ステップＳ１４０において、暗号化部１４０は、情報aから擬似乱数$r_1,\cdots,r_{K-1}$を用いて暗号文cを生成する。より具体的には、以下の式に示す通り、情報aから擬似乱数$r_1,\cdots,r_{K-1}$の総和を減算した結果を暗号文cとする。

[数3]

$$c=a-\sum_{k=1}^{K-1}r_k$$

[0028] 鍵$s_1,\cdots,s_{K-1}$は鍵分散部１５０にも入力される。ステップＳ１５０において、鍵分散部１５０は、鍵$s_{1,\cdots,}s_{K-1}$をそれぞれ任意の秘密分散方式S1によりN個の

分散値$f_{s1}(n),\cdots,f_{sK-1}(n)(n=1,\cdots,N)$に分散する。秘密分散方式S1は、どのような秘密分散方式であってもよいが、情報aの復号に用いる鍵を分散するため、より安全性の高い秘密分散方式を適用することが望ましい。例えば、Shamir秘密分散方式を適用することができる。Shamir秘密分散方式は、N,Kが2以上の整数であり、N≧Kであるとして、元のデータをN個に分散した分散値のうちK個以上の分散値からは元のデータを復元することができるが、K個未満の分散値からは元のデータの情報を一切得ることができないため、安全性が高い秘密分散方式である。

[0029] 暗号文cは暗号文分散部１６０に入力される。ステップＳ１６０において、暗号文分散部１６０は、暗号文cを任意の秘密分散方式S0によりN個の分散値$f_c(n)(n=1,\cdots,N)$に分散する。秘密分散方式S0はどのような秘密分散方式であってもよいが、例えば非特許文献２に記載の方法を適用することができる。ただし非特許文献２に記載の方法を適用する場合には、環R上の値cをGF(p)上のK次ベクトルに変換する必要がある。これは例えば、素数pのビット長をL+1、環Rの要素のビット長をK×L以下とすれば、環Rの要素がK×Lビットになるように上位ビットを0でパディングし、値cをLビット毎に分割し、各Lビット分割値を0以上2^L未満の整数としてGF(p)の元とすればよい。

[0030] ステップＳ１７０において、出力部１７０は、分散値$f_{s1}(n),\cdots,f_{sK-1}(n),f_c(n)(n=1,\cdots,N)$を出力する。出力された各分散値$f_{s1}(n),\cdots,f_{sK-1}(n),f_c(n)(n=1,\cdots,N)$は、それぞれ分散データ変換装置$２０_1$～$２０_N$にネットワーク９０もしくはUSBメモリ等の可搬型記録媒体を経由して入力される。

[0031] ＜分散データ変換処理＞

図５を参照して、分散データ変換装置２０_iの動作例を、実際に行われる手続きの順に従って説明する。

ステップＳ２１１において、入力部２１０に、データ分散装置１０が出力したK個の分散値$f_{sj}(i)(i\in\lambda)$もしくはK個の分散値$f_c(i)$が入力される。分散値$f_{sj}(i)$もしくは$f_c(i)$は記憶部２９０に記憶しておき、任意のタイミングで後続の処理を実行するように構成してもよい。記憶部２９０には記憶せず、分

散値$f_{sj}(i)$もしくは$f_c(i)$が入力されると引き続き後続の処理を実行するように構成してもよい。

[0032] K個の分散値$f_{sj}(i)$もしくはK個の分散値$f_c(i)$は復元部２２０に入力される。ステップＳ２２０において、復元部２２０は、入力された分散値$f_{sj}(i)$もしくは分散値$f_c(i)$から復元値U_jを生成する。分散値$f_{sj}(i)$が入力されると、分散値$f_{sj}(i)$を任意の秘密分散方式S1により復元して値u_jを生成する。続いて、$U_j=P(u_j)$を計算することで、復元値U_jとする。写像$P(x)$はデータ分散装置１０の備える擬似乱数生成部１３０と同じ写像である。上述の通り、データ分散装置１０の備える鍵分散部１５０により、$f_{sj}(i)(j=1,\cdots,K-1)$には鍵$s_j$の分散値が設定されているため、同じ写像$P(x)$が鍵$s_j$を写した復元値$U_j$は擬似乱数$r_j$と等しくなる。秘密分散方式S1はどのような秘密分散方式であってもよいが、データ分散装置１０の備える鍵分散部１５０が用いる秘密分散方式S1と同じ方式でなければならない。

[0033] 分散値$f_c(i)$が入力されると、分散値$f_c(i)$を任意の秘密分散方式S0により復元することで、復元値$U_j(j=K)$を生成する。上述の通り、データ分散装置１０の備える暗号文分散部１６０により、$f_c(i)$には暗号文cの分散値が設定されているため、復元値U_jは暗号文cと等しくなる。秘密分散方式S0はどのような秘密分散方式であってもよいが、データ分散装置１０の備える暗号文分散部１６０が用いる秘密分散方式S0と同じ方式でなければならない。

[0034] 復元値U_jは再分散部２３０に入力される。ステップＳ２３０において、再分散部２３０は、復元値U_jを任意の準同型性をもつ秘密分散方式S2によりN個の分散値$f_{Uj}(n)(n=1,\cdots,N)$に分散する。準同型性とは2つの情報a,bの分散値$f_a(i)$,$f_b(i)$およびa+bの分散値$f_{a+b}(i)$について、$f_a(i)+f_b(i)=f_{a+b}(i)$が成り立つことをいう。秘密分散方式S2は準同型性をもつ秘密分散方式であればどのような秘密分散方式でもよい。例えば、Shamir秘密分散方式など既存の線形秘密分散方式を適用することができる。

[0035] なお、図５に示すステップＳ２１１からステップＳ２３０までの処理は、N台の分散データ変換装置２０_1～２０_Nのすべてが行う必要はなく、任意に選択

された少なくともK台が行えばよい。

[0036] ステップＳ２１２において、入力部２１０に、K台の分散データ変換装置２０$_i$($i\in\lambda$)の備える再分散部２３０が生成したK個の分散値$f_{U1}(i),\cdots,f_{UK}(i)$が入力される。分散値$f_{U1}(i),\cdots,f_{UK}(i)$は記憶部２９０に記憶しておき、任意のタイミングで後続の処理を実行するように構成してもよい。記憶部２９０には記憶せず、分散値$f_{U1}(i),\cdots,f_{UK}(i)$が入力されると引き続き後続の処理を実行するように構成してもよい。

[0037] 分散値$f_{U1}(i),\cdots,f_{UK}(i)$は変換部２４０に入力される。ステップＳ２４０において、変換部２４０は、K個の分散値$f_{U1}(i),\cdots,f_{UK}(i)$から情報aの分散値$g_a(i)$を生成する。より具体的には、以下の式に示す通り、分散値$f_{U1}(i),\cdots,f_{UK}(i)$の総和を分散値$g_a(i)$とすることができる。

[数4]

$$g_a(i)=\sum_{k=1}^{K} f_{U_k}(i)$$

[0038] 上述の通り、$f_{UK}(i)$は準同型性をもつ秘密分散方式S2により暗号文cを分散した分散値であり、$f_{U1}(i),\cdots,f_{UK-1}(i)$は準同型性をもつ秘密分散方式S2により擬似乱数$r_1,\cdots,r_{K-1}$をそれぞれ分散した分散値である。したがって、準同型性の性質により、$f_{U1}(i),\cdots,f_{UK}(i)$の総和は、暗号文cと擬似乱数$r_1,\cdots,r_{K-1}$の総和を加算した値を秘密分散方式S2により分散した分散値となる。暗号文cは情報aから擬似乱数$r_1,\cdots,r_{K-1}$の総和を減算した値であるため、この分散値$g_a(i)$は、情報aを秘密分散方式S2により分散した分散値と等しい。

[0039] ステップＳ２５０において、出力部２５０は、分散値$g_a(i)$を出力する。分散値$g_a(i)$を記憶部２９０へ記憶しておき、外部からの要求に応じて記憶部２９０から分散値$g_a(i)$を読みだして出力してもよい。

なお、図５に示すステップＳ２１２からステップＳ２５０までの処理は、N台の分散データ変換装置２０$_1$～２０$_N$のすべてで行う。

[0040] ＜機密性＞

分散データ変換装置２０$_1$～２０$_N$が得る情報aに関する情報は、準同型性をもつ秘密分散方式S2による分散値であり、各分散値の生成に用いる乱数が互

いに独立であれば、この実施形態の機密性は、利用する準同型性をもつ秘密分散方式S2の機密性に帰着される。また、K台の分散データ変換装置２０$_i$はそれぞれ情報aの分散値である復元値U_jの何れかを得るが、K個の復元値$U_1,\cdots,U_K$すべてを得られない限り情報aを得ることはできない。そのため、この実施形態の機密性は、結局、利用する秘密分散方式S2の機密性に帰着される。

[0041] ＜効果＞

この実施形態の秘密分散システムは、計算量型秘密分散方式による情報aの分散値$f_a(1),\cdots,f_a(N)$を、任意の準同型性をもつ秘密分散方式S2による分散値$g_a(1),\cdots,g_a(N)$に変換することができる。

[0042] 準同型性をもつ秘密分散方式としては、例えば、Shamir秘密分散方式など既存の線形秘密分散方式が挙げられる。Shamir秘密分散方式など既存の線形秘密分散方式を用いてマルチパーティ計算を行う方法は既知であるため、秘密分散方式S2としてShamir秘密分散方式など既存の任意の線形秘密分散方式を選択することで、計算量型秘密分散方式による分散値を用いてマルチパーティ計算を行うことができるようになる。

[0043] 例えば、非特許文献２に記載の計算量型秘密分散方式は分散値のサイズの下限が元のデータの1/Kとなるため、暗号文cを分散する秘密分散方式S0として非特許文献２に記載の計算量型秘密分散方式を適用すれば、分散値のサイズが元のデータと同程度となるShamir秘密分散方式と比較して、分散値を保存するために必要となる記憶容量を削減することができる。

[0044] ［第二実施形態］

この発明の第二実施形態に係る秘密分散システムは、計算量型秘密分散方式による分散値を、準同型性をもつ任意の秘密分散方式による分散値に変換する。第一実施形態では、生成する鍵の数と秘密分散方式の復元の閾値を同数であったが、必ずしも同数でなくとも構わない。第二実施形態では、鍵の数と復元の閾値を異なる値とした場合の例を示す。

[0045] ＜構成＞

図６を参照して、第二実施形態に係る秘密分散システム２の構成例を説明

する。秘密分散システム２は、データ分散装置１２と少なくともN台の分散データ変換装置22_1～22_Nとネットワーク９０を含む。データ分散装置１２と分散データ変換装置22_1～22_Nは、ネットワーク９０に接続される。ネットワーク９０は、データ分散装置１２と分散データ変換装置22_1～22_Nそれぞれと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、データ分散装置１２と分散データ変換装置22_1～22_Nそれぞれとは必ずしもネットワーク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、データ分散装置１２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分散データ変換装置22_1～22_Nへオフラインで入力するように構成してもよい。

[0046] 図７を参照して、秘密分散システム２に含まれるデータ分散装置１２の構成例を説明する。データ分散装置１２は、入力部１１０と鍵選択部１２２と擬似乱数生成部１３２と暗号化部１４２と鍵分散部１５２と暗号文分散部１６０と出力部１７２とを備える。

[0047] 図８を参照して、秘密分散システム２に含まれる分散データ変換装置２２の構成例を説明する。分散データ変換装置２２は、入力部２１２と復元部２２０と再分散部２３０と変換部２４２と出力部２５０と記憶部２９０とを備える。記憶部２９０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）などの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。

[0048] ＜データ分散処理＞

図９を参照して、データ分散装置１２の動作例を、実際に行われる手続きの順に従って説明する。以下の説明では、N,K,K’は2以上の整数であり、$N \geqq K$であり、$n=1,\cdots,N$であり、λは互いに異なる1以上N以下のK個の整数であり、iは$i \in \lambda$の整数であり、$f_x(n)$はxのN個の分散値であり、Rは環であり、Sは

鍵空間であり、P(x)はx∈Sを環Rへ移す写像であるものとする。写像P(x)は、入力されたx∈Sに対して環Rの要素を出力するものである。同一の入力xには同一のP(x)が対応する。すなわち、写像P(x)は入力が等しければ出力も等しくなる、確定的な写像である。入力xとP(x)とは一対一で対応してもよいし、しなくてもよい。例えば、写像P(x)はxをシードとして環Rの要素を返す擬似乱数生成関数である。また例えば、写像P(x)はxを暗号化鍵として固定の平文に対して環Rに属する暗号文を出力する共通鍵暗号関数である。写像P(x)は関数であってもよいし、アルゴリズムであってもよい。

[0049] ステップＳ１１０において、入力部１１０に、情報aが入力される。情報aは環Rに含まれる値である。したがって、a∈Rと表すことができる。情報aの例は、動画ファイル、音声ファイル、テキストファイル、表ファイルなどである。情報aのデータ量は、例えば1メガバイト以上である。

[0050] ステップＳ１２２において、鍵選択部１２２は、K’-1個の鍵$s_1,\cdots,s_{K'-1}\in S$を選択する。鍵選択部１２２は、逐一ランダムにK’-1個の鍵$s_1,\cdots,s_{K'-1}$を選択してもよいし、事前に生成されメモリに格納されている複数個の値から所定の規則に従ってK’-1個の鍵$s_1,\cdots,s_{K'-1}$を選択してもよい。鍵$s_1,\cdots,s_{K'-1}$の鍵長は、必要な安全性と許容できる処理性能を確保できる長さに設定する。例えば、128～256ビットとするのが一般的であるが、この限りではない。

[0051] 鍵$s_1,\cdots,s_{K'-1}$は擬似乱数生成部１３２に入力される。ステップＳ１３２において、擬似乱数生成部１３２は、鍵$s_1,\cdots,s_{K'-1}$から$r_j=P(s_j)(j=1,\cdots,K'-1)$を計算することにより擬似乱数$r_1,\cdots,r_{K'-1}$を生成する。

[0052] 情報aと擬似乱数$r_1,\cdots,r_{K'-1}$は暗号化部１４２に入力される。ステップＳ１４２において、暗号化部１４２は、情報aから擬似乱数$r_1,\cdots,r_{K'-1}$を用いて暗号文cを生成する。より具体的には、以下の式に示す通り、情報aから擬似乱数$r_1,\cdots,r_{K'-1}$の総和を減算した結果を暗号文cとする。

[数5]

$$c=a-\sum_{k=1}^{K'-1}r_k$$

[0053] 鍵$s_1,\cdots,s_{K'-1}$は鍵分散部１５２にも入力される。ステップＳ１５２において

、鍵分散部１５２は、鍵$s_{1,\cdots,}s_{K'-1}$をそれぞれ任意の秘密分散方式S1によりN個の分散値$f_{s1}(n),\cdots,f_{sK'-1}(n)(n=1,\cdots,N)$に分散する。秘密分散方式S1は、どのような秘密分散方式であってもよいが、情報aの復号に用いる鍵を分散するため、より安全性の高い秘密分散方式を適用することが望ましい。例えば、Shamir秘密分散方式を適用することができる。Shamir秘密分散方式は、N,Kが2以上の整数であり、N≧Kであるとして、元のデータをN個に分散した分散値のうちK個以上の分散値からは元のデータを復元することができるが、K個未満の分散値からは元のデータの情報を一切得ることができないため、安全性が高い秘密分散方式である。

[0054] 暗号文cは暗号文分散部１６０に入力される。ステップＳ１６０において、暗号文分散部１６０は、暗号文cを任意の分散方式S0によりN個の分散値$f_c(n)(n=1,\cdots,N)$に分散する。分散方式S0はどのような分散方式であってもよく、情報伝播アルゴリズム（Information Dispersal Algorithm、IDA）と呼ばれる、秘匿性を考慮しない分散方式であっても構わない。分散方式S0は、例えば非特許文献２に記載の方法を適用することができる。ただし非特許文献２に記載の方法を適用する場合には、環R上の値cをGF(p)上のK次ベクトルに変換する必要がある。これは例えば、素数pのビット長をL+1、環Rの要素のビット長をK×L以下とすれば、環Rの要素がK×Lビットになるように上位ビットを0でパディングし、値cをLビット毎に分割し、各Lビット分割値を0以上2^L未満の整数としてGF(p)の元とすればよい。

[0055] ステップＳ１７２において、出力部１７２は、分散値$f_{s1}(n),\cdots,f_{sK'-1}(n),f_c(n)(n=1,\cdots,N)$を出力する。出力された各分散値$f_{s1}(n),\cdots,f_{sK'-1}(n),f_c(n)(n=1,\cdots,N)$は、それぞれ分散データ変換装置$２２_1$～$２２_N$にネットワーク９０もしくはUSBメモリ等の可搬型記録媒体を経由して入力される。

[0056] ＜分散データ変換処理＞

図１０を参照して、分散データ変換装置２２_iの動作例を、実際に行われる手続きの順に従って説明する。

ステップＳ２１１において、入力部２１２に、データ分散装置１２が出力

したK個の分散値$f_{sj}(i)$($i\in\lambda$)もしくはK個の分散値$f_c(i)$が入力される。分散値$f_{sj}(i)$もしくは$f_c(i)$は記憶部２９０に記憶しておき、任意のタイミングで後続の処理を実行するように構成してもよい。記憶部２９０には記憶せず、分散値$f_{sj}(i)$もしくは$f_c(i)$が入力されると引き続き後続の処理を実行するように構成してもよい。

[0057] K個の分散値$f_{sj}(i)$もしくはK個の分散値$f_c(i)$は復元部２２０に入力される。ステップＳ２２０において、復元部２２０は、入力された分散値$f_{sj}(i)$もしくは分散値$f_c(i)$から復元値U_jを生成する。分散値$f_{sj}(i)$が入力されると、分散値$f_{sj}(i)$を任意の秘密分散方式S1により復元して値u_jを生成する。続いて、$U_j=P(u_j)$を計算することで、復元値U_jとする。写像P(x)はデータ分散装置１２の備える擬似乱数生成部１３０と同じ写像である。上述の通り、データ分散装置１２の備える鍵分散部１５０により、$f_{sj}(i)$($j=1,\cdots,K'-1$)には鍵s_jの分散値が設定されているため、同じ写像P(x)が鍵s_jを写した復元値U_jは擬似乱数r_jと等しくなる。秘密分散方式S1はどのような秘密分散方式であってもよいが、データ分散装置１２の備える鍵分散部１５０が用いる秘密分散方式S1と同じ方式でなければならない。

[0058] 分散値$f_c(i)$が入力されると、分散値$f_c(i)$を任意の分散方式S0により復元することで、復元値U_j($j=K'$)を生成する。上述の通り、データ分散装置１２の備える暗号文分散部１６０により、$f_c(i)$には暗号文cの分散値が設定されているため、復元値U_j($j=K'$)は暗号文cと等しくなる。分散方式S0はどのような分散方式であってもよいが、データ分散装置１２の備える暗号文分散部１６０が用いる分散方式S0と同じ方式でなければならない。

[0059] 復元値U_jは再分散部２３０に入力される。ステップＳ２３０において、再分散部２３０は、復元値U_jを任意の準同型性をもつ秘密分散方式S2によりN個の分散値$f_{Uj}(n)$($n=1,\cdots,N$)に分散する。準同型性とは2つの情報a,bの分散値$f_a(i)$,$f_b(i)$およびa+bの分散値$f_{a+b}(i)$について、$f_a(i)+f_b(i)=f_{a+b}(i)$が成り立つことをいう。秘密分散方式S2は準同型性をもつ秘密分散方式であればどのような秘密分散方式でもよい。例えば、Shamir秘密分散方式など既存の線形秘密分

散方式を適用することができる。

[0060] なお、図１０に示すステップＳ２１１からステップＳ２３０までの処理は、N台の分散データ変換装置２２_1～２２_Nのすべてが行う必要はなく、任意に選択された少なくともK台が行えばよい。

[0061] ステップＳ２１３において、入力部２１２に、K’台の分散データ変換装置２２_i($i \in \lambda$)の備える再分散部２３０が生成したK’個の分散値$f_{U1}(i),\cdots,f_{UK'}(i)$が入力される。分散値$f_{U1}(i),\cdots,f_{UK'}(i)$は記憶部２９０に記憶しておき、任意のタイミングで後続の処理を実行するように構成してもよい。記憶部２９０には記憶せず、分散値$f_{U1}(i),\cdots,f_{UK'}(i)$が入力されると引き続き後続の処理を実行するように構成してもよい。

[0062] 分散値$f_{U1}(i),\cdots,f_{UK'}(i)$は変換部２４２に入力される。ステップＳ２４２において、変換部２４２は、K’個の分散値$f_{U1}(i),\cdots,f_{UK'}(i)$から情報aの分散値$g_a(i)$を生成する。より具体的には、以下の式に示す通り、分散値$f_{U1}(i),\cdots,f_{UK'}(i)$の総和を分散値$g_a(i)$とすることができる。

[数6]

$$g_a(i)=\sum_{k=1}^{K'} f_{U_k}(i)$$

[0063] 上述の通り、$f_{UK'}(i)$は準同型性をもつ秘密分散方式S2により暗号文cを分散した分散値であり、$f_{U1}(i),\cdots,f_{UK'-1}(i)$は準同型性をもつ秘密分散方式S2により擬似乱数$r_1,\cdots,r_{K'-1}$をそれぞれ分散した分散値である。したがって、準同型性の性質により、$f_{U1}(i),\cdots,f_{UK'}(i)$の総和は、暗号文cと擬似乱数$r_1,\cdots,r_{K'-1}$の総和を加算した値を秘密分散方式S2により分散した分散値となる。暗号文cは情報aから擬似乱数$r_1,\cdots,r_{K'-1}$の総和を減算した値であるため、この分散値$g_a(i)$は、情報aを秘密分散方式S2により分散した分散値と等しい。

[0064] ステップＳ２５０において、出力部２５０は、分散値$g_a(i)$を出力する。分散値$g_a(i)$を記憶部２９０へ記憶しておき、外部からの要求に応じて記憶部２９０から分散値$g_a(i)$を読みだして出力してもよい。

なお、図１０に示すステップＳ２１３からステップＳ２５０までの処理は、N台の分散データ変換装置２２_1～２２_Nのすべてで行う。

[0065] ＜機密性＞

分散データ変換装置２２$_1$～２２$_N$が得る情報aに関する情報は、準同型性をもつ秘密分散方式S2による分散値であり、各分散値の生成に用いる乱数が互いに独立であれば、この実施形態の機密性は、利用する準同型性をもつ秘密分散方式S2の機密性に帰着される。また、K’台の分散データ変換装置２２$_i$はそれぞれ情報aの分散値である復元値U_jの何れかを得るが、K’個の復元値U_1,…,$U_{K'}$すべてを得られない限り情報aを得ることはできない。ただし$U_{K'}$については、任意の分散方式で分散していたため、秘匿性は保証できない。そのため、この実施形態の機密性は、結局、K’>Kとすれば、利用する秘密分散方式S2の機密性に帰着される。

[0066] ＜効果＞

この実施形態の秘密分散システムは、計算量型秘密分散方式による情報aの分散値$f_a(1),\cdots,f_a(N)$を、任意の準同型性をもつ秘密分散方式S2による分散値$g_a(1),\cdots,g_a(N)$に変換することができる。

準同型性をもつ秘密分散方式としては、例えば、Shamir秘密分散方式など既存の線形秘密分散方式が挙げられる。Shamir秘密分散方式など既存の線形秘密分散方式を用いてマルチパーティ計算を行う方法は既知であるため、秘密分散方式S2としてShamir秘密分散方式など既存の任意の線形秘密分散方式を選択することで、計算量型秘密分散方式による分散値を用いてマルチパーティ計算を行うことができるようになる。

[0067] 例えば、非特許文献２に記載の計算量型秘密分散方式は分散値のサイズの下限が元のデータの1/Kとなるため、暗号文cを分散する分散方式S0として非特許文献２に記載の計算量型秘密分散方式を適用すれば、分散値のサイズが元のデータと同程度となるShamir秘密分散方式と比較して、分散値を保存するために必要となる記憶容量を削減することができる。

[0068] ［プログラム、記録媒体］

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。上記実施例

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。

[0069] また、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。

[0070] 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。

[0071] 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。

[0072] 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。

[0073] 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] データ分散装置とN台の分散データ変換装置を含む秘密分散システムであって、

N,Kは2以上の整数であり、N≧Kであり、n=1,…,Nであり、λは互いに異なる1以上N以下のK個の整数であり、iはi∈λの整数であり、$f_x(n)$はxのN個の分散値であり、Rは環であり、Sは鍵空間であり、P(x)はx∈Sを環Rへ移す写像であり、

前記データ分散装置は、

K-1個の鍵$s_1,\cdots,s_{K-1}\in S$を選択する鍵選択部と、

前記鍵$s_1,\cdots,s_{K-1}$から$r_j=P(s_j)(j=1,\cdots,K-1)$を計算することにより擬似乱数$r_1,\cdots,r_{K-1}$を生成する擬似乱数生成部と、

情報a∈Rから前記擬似乱数$r_1,\cdots,r_{K-1}$を用いて暗号文cを生成する暗号化部と、

前記鍵$s_{1,\cdots,}s_{K-1}$を任意の秘密分散方式S1によりそれぞれN個の分散値$f_{s1}(n),\cdots,f_{sK-1}(n)$に分散する鍵分散部と、

前記暗号文cを任意の秘密分散方式S0によりN個の分散値$f_c(n)$に分散する暗号文分散部と、

を備え、

前記分散データ変換装置は、

K個の分散値$f_{sj}(i)$が入力されると、前記分散値$f_{sj}(i)$を前記秘密分散方式S1により復元した値u_jから$U_j=P(u_j)$を計算し、K個の分散値$f_c(i)$が入力されると、前記分散値$f_c(i)$を前記秘密分散方式S0により復元することで、復元値$U_j(j=K)$を生成する復元部と、

前記復元値U_jを任意の準同型性をもつ秘密分散方式S2によりN個の分散値$f_{Uj}(n)$に分散する再分散部と、

K個の分散値$f_{U1}(i),\cdots,f_{UK}(i)$から前記情報aの分散値$g_a(i)$を生成する変換部と、

を備える秘密分散システム。

[請求項2] データ分散装置とN台の分散データ変換装置を含む秘密分散システムであって、

N,K,K'は2以上の整数であり、N≧Kであり、n=1,…,Nであり、λは互いに異なる1以上N以下のK個の整数であり、iはi∈λの整数であり、$f_x(n)$はxのN個の分散値であり、Rは環であり、Sは鍵空間であり、P(x)はx∈Sを環Rへ移す写像であり、

前記データ分散装置は、

K'-1個の鍵$s_1,\cdots,s_{K'-1}\in S$を選択する鍵選択部と、

前記鍵$s_1,\cdots,s_{K'-1}$から$r_j=P(s_j)(j=1,\cdots,K'-1)$を計算することにより擬似乱数$r_1,\cdots,r_{K'-1}$を生成する擬似乱数生成部と、

情報a∈Rから前記擬似乱数$r_1,\cdots,r_{K'-1}$を用いて暗号文cを生成する暗号化部と、

前記鍵$s_{1,\cdots,}s_{K'-1}$を任意の秘密分散方式S1によりそれぞれN個の分散値$f_{s1}(n),\cdots,f_{sK'-1}(n)$に分散する鍵分散部と、

前記暗号文cを任意の分散方式S0によりN個の分散値$f_c(n)$に分散する暗号文分散部と、

を備え、

前記分散データ変換装置は、

K個の分散値$f_{sj}(i)$が入力されると、前記分散値$f_{sj}(i)$を前記秘密分散方式S1により復元した値u_jから$U_j=P(u_j)$を計算し、K個の分散値$f_c(i)$が入力されると、前記分散値$f_c(i)$を前記分散方式S0により復元することで、復元値$U_j(j=K')$を生成する復元部と、

前記復元値U_jを任意の準同型性をもつ秘密分散方式S2によりN個の分散値$f_{Uj}(n)$に分散する再分散部と、

K'個の分散値$f_{U1}(i),\cdots,f_{UK'}(i)$から前記情報aの分散値$g_a(i)$を生成する変換部と、

を備える秘密分散システム。

[請求項3] 請求項１に記載の秘密分散システムであって、

前記暗号化部は、前記情報aから前記擬似乱数$r_1,\cdots,r_{K-1}$の総和を減算して前記暗号文cを生成し、

前記変換部は、前記分散値$f_{U1}(i),\cdots,f_{UK}(i)$の総和を前記分散値$g_a(i)$とする

秘密分散システム。

[請求項4] 請求項２に記載の秘密分散システムであって、

前記暗号化部は、前記情報aから前記擬似乱数$r_1,\cdots,r_{K'-1}$の総和を減算して前記暗号文cを生成し、

前記変換部は、前記分散値$f_{U1}(i),\cdots,f_{UK'}(i)$の総和を前記分散値$g_a(i)$とする

秘密分散システム。

[請求項5] 請求項１から４のいずれかに記載の秘密分散システムであって、

前記秘密分散方式S2は、Shamir秘密分散方式である

秘密分散システム。

[請求項6] N,Kは2以上の整数であり、N≧Kであり、n=1,…,Nであり、$f_x(n)$はxのN個の分散値であり、Rは環であり、Sは鍵空間であり、P(x)はx∈Sを環Rへ移す写像であり、

K-1個の鍵$s_1,\cdots,s_{K-1}\in S$を選択する鍵選択部と、

前記鍵$s_1,\cdots,s_{K-1}$から$r_j=P(s_j)(j=1,\cdots,K-1)$を計算することにより擬似乱数$r_1,\cdots,r_{K-1}$を生成する擬似乱数生成部と、

情報a∈Rから前記擬似乱数$r_1,\cdots,r_{K-1}$を用いて暗号文cを生成する暗号化部と、

前記鍵$s_{1,\cdots,}s_{K-1}$を任意の秘密分散方式S1によりそれぞれN個の分散値$f_{s1}(n),\cdots,f_{sK-1}(n)$に分散する鍵分散部と、

前記暗号文cを任意の秘密分散方式S0によりN個の分散値$f_c(n)$に分散する暗号文分散部と、

を備えるデータ分散装置。

[請求項7] N,K,K’は2以上の整数であり、N≧Kであり、n=1,…,Nであり、$f_x(n$

)はxのN個の分散値であり、Rは環であり、Sは鍵空間であり、P(x)はx∈Sを環Rへ移す写像であり、

K'-1個の鍵$s_1,\cdots,s_{K'-1}\in S$を選択する鍵選択部と、

前記鍵$s_1,\cdots,s_{K'-1}$から$r_j=P(s_j)(j=1,\cdots,K'-1)$を計算することにより擬似乱数$r_1,\cdots,r_{K'-1}$を生成する擬似乱数生成部と、

情報a∈Rから前記擬似乱数$r_1,\cdots,r_{K'-1}$を用いて暗号文cを生成する暗号化部と、

前記鍵$s_{1,\cdots,}s_{K'-1}$を任意の秘密分散方式S1によりそれぞれN個の分散値$f_{s1}(n),\cdots,f_{sK'-1}(n)$に分散する鍵分散部と、

前記暗号文cを任意の分散方式S0によりN個の分散値$f_c(n)$に分散する暗号文分散部と、

を備えるデータ分散装置。

[請求項8] N,Kは2以上の整数であり、N≧Kであり、n=1,…,Nであり、λは互いに異なる1以上N以下のK個の整数であり、iはi∈λの整数であり、$f_x(n)$はxのN個の分散値であり、Rは環であり、Sは鍵空間であり、P(x)はx∈Sを環Rへ移す写像であり、

K個の分散値$f_{sj}(i)$が入力されると、前記分散値$f_{sj}(i)$を所定の秘密分散方式S1により復元した値u_jから$U_j=P(u_j)$を計算し、K個の分散値$f_c(i)$が入力されると、前記分散値$f_c(i)$を所定の秘密分散方式S0により復元することで、復元値U_jを生成する復元部と、

前記復元値U_jを任意の準同型性をもつ秘密分散方式S2によりN個の分散値$f_{Uj}(n)$に分散する再分散部と、

K個の分散値$f_{U1}(i),\cdots,f_{UK}(i)$から前記情報aの分散値$g_a(i)$を生成する変換部を備え、

前記分散値$f_{sj}(i)$は、K個の鍵$s_1,\cdots,s_{K-1}\in S$を前記秘密分散方式S1によりそれぞれN個に分散した分散値$f_{s1}(n),\cdots,f_{sK-1}(n)$に含まれ、

前記分散値$f_c(i)$は、前記鍵$s_1,\cdots,s_{K-1}$から$r_j=P(s_j)(j=1,\cdots,K-1)$を計算することにより生成された擬似乱数$r_1,\cdots,r_{K-1}$を用いて情報a∈Rか

ら生成した暗号文cを、前記秘密分散方式S0によりN個に分散した分散値$f_c(n)$に含まれる

分散データ変換装置。

[請求項9] N,K,K'は2以上の整数であり、N≧Kであり、n=1,…,Nであり、λは互いに異なる1以上N以下のK個の整数であり、iはi∈λの整数であり、$f_x(n)$はxのN個の分散値であり、Rは環であり、Sは鍵空間であり、P(x)はx∈Sを環Rへ移す写像であり、

K個の分散値$f_{sj}(i)$が入力されると、前記分散値$f_{sj}(i)$を所定の秘密分散方式S1により復元した値u_jから$U_j=P(u_j)$を計算し、K個の分散値$f_c(i)$が入力されると、前記分散値$f_c(i)$を所定の分散方式S0により復元することで、復元値$U_j(j=K')$を生成する復元部と、

前記復元値U_jを任意の準同型性をもつ秘密分散方式S2によりN個の分散値$f_{Uj}(n)$に分散する再分散部と、

K'個の分散値$f_{U1}(i),\cdots,f_{UK'}(i)$から前記情報aの分散値$g_a(i)$を生成する変換部を備え、

前記分散値$f_{sj}(i)$は、K'個の鍵$s_1,\cdots,s_{K'-1}\in S$を前記秘密分散方式S1によりそれぞれN個に分散した分散値$f_{s1}(n),\cdots,f_{sK'-1}(n)$に含まれ、

前記分散値$f_c(i)$は、前記鍵$s_1,\cdots,s_{K'-1}$から$r_j=P(s_j)(j=1,\cdots,K'-1)$を計算することにより生成された擬似乱数$r_1,\cdots,r_{K'-1}$を用いて情報a∈Rから生成した暗号文cを、前記分散方式S0によりN個に分散した分散値$f_c(n)$に含まれる

分散データ変換装置。

[請求項10] N,Kは2以上の整数であり、N≧Kであり、n=1,…,Nであり、λは互いに異なる1以上N以下のK個の整数であり、iはi∈λの整数であり、$f_x(n)$はxのN個の分散値であり、Rは環であり、Sは鍵空間であり、P(x)はx∈Sを環Rへ移す写像であり、

データ分散装置が、K-1個の鍵$s_1,\cdots,s_{K-1}\in S$を選択する鍵選択ステップと、

前記データ分散装置が、前記鍵$s_1,\cdots,s_{K-1}$から$r_j=P(s_j)(j=1,\cdots,K-1)$を計算することにより擬似乱数$r_1,\cdots,r_{K-1}$を生成する擬似乱数生成ステップと、

前記データ分散装置が、情報$a\in R$から前記擬似乱数$r_1,\cdots,r_{K-1}$を用いて暗号文cを生成する暗号化ステップと、

前記データ分散装置が、前記鍵$s_{1,\cdots,}s_{K-1}$を任意の秘密分散方式S1によりそれぞれN個の分散値$f_{s1}(n),\cdots,f_{sK-1}(n)$に分散する鍵分散ステップと、

前記データ分散装置が、前記暗号文cを任意の秘密分散方式S0によりN個の分散値$f_c(n)$に分散する暗号文分散ステップと、

分散データ変換装置が、K個の分散値$f_{sj}(i)$が入力されると、前記分散値$f_{sj}(i)$を前記秘密分散方式S1により復元した値u_jから$U_j=P(u_j)$を計算し、K個の分散値$f_c(i)$が入力されると、前記分散値$f_c(i)$を前記秘密分散方式S0により復元することで、復元値U_jを生成する復元ステップと、

前記分散データ変換装置が、前記復元値U_jを任意の準同型性をもつ秘密分散方式S2によりN個の分散値$f_{Uj}(n)$に分散する再分散ステップと、

前記分散データ変換装置が、K個の分散値$f_{U1}(i),\cdots,f_{UK}(i)$から前記情報aの分散値$g_a(i)$を生成する変換ステップと、

を含む秘密分散方法。

[請求項11] N,K,K'は2以上の整数であり、$N\geqq K$であり、$n=1,\cdots,N$であり、λは互いに異なる1以上N以下のK個の整数であり、iは$i\in\lambda$の整数であり、$f_x(n)$はxのN個の分散値であり、Rは環であり、Sは鍵空間であり、P(x)は$x\in S$を環Rへ移す写像であり、

データ分散装置が、K'-1個の鍵$s_1,\cdots,s_{K'-1}\in S$を選択する鍵選択ステップと、

前記データ分散装置が、前記鍵$s_1,\cdots,s_{K'-1}$から$r_j=P(s_j)(j=1,\cdots,K'$

-1)を計算することにより擬似乱数$r_1,\cdots,r_{K'-1}$を生成する擬似乱数生成ステップと、

前記データ分散装置が、情報a∈Rから前記擬似乱数$r_1,\cdots,r_{K'-1}$を用いて暗号文cを生成する暗号化ステップと、

前記データ分散装置が、前記鍵$s_{1,\cdots,}s_{K'-1}$を任意の秘密分散方式S1によりそれぞれN個の分散値$f_{s1}(n),\cdots,f_{sK'-1}(n)$に分散する鍵分散ステップと、

前記データ分散装置が、前記暗号文cを任意の分散方式S0によりN個の分散値$f_c(n)$に分散する暗号文分散ステップと、

分散データ変換装置が、K個の分散値$f_{sj}(i)$が入力されると、前記分散値$f_{sj}(i)$を前記秘密分散方式S1により復元した値u_jから$U_j=P(u_j)$を計算し、K個の分散値$f_c(i)$が入力されると、前記分散値$f_c(i)$を前記分散方式S0により復元することで、復元値$U_j(j=K')$を生成する復元ステップと、

前記分散データ変換装置が、前記復元値U_jを任意の準同型性をもつ秘密分散方式S2によりN個の分散値$f_{Uj}(n)$に分散する再分散ステップと、

前記分散データ変換装置が、K'個の分散値$f_{U1}(i),\cdots,f_{UK'}(i)$から前記情報aの分散値$g_a(i)$を生成する変換ステップと、

を含む秘密分散方法。

[請求項12] 請求項６または７に記載のデータ分散装置もしくは請求項８または９に記載の分散データ変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]

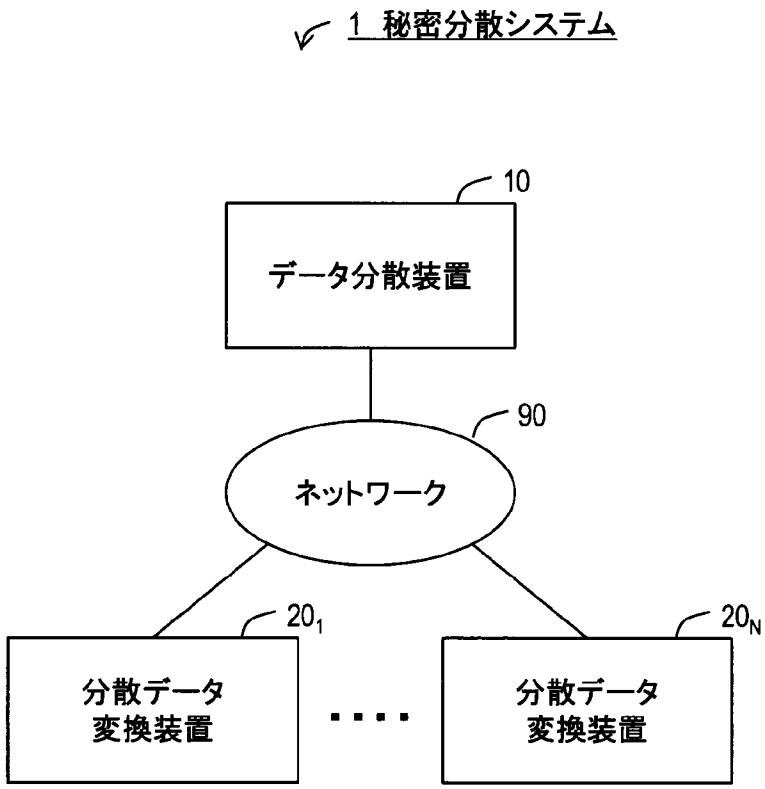

1 秘密分散システム
10
データ分散装置
90
ネットワーク
20_1
20_N
分散データ
変換装置
分散データ
変換装置

図1

[図2]

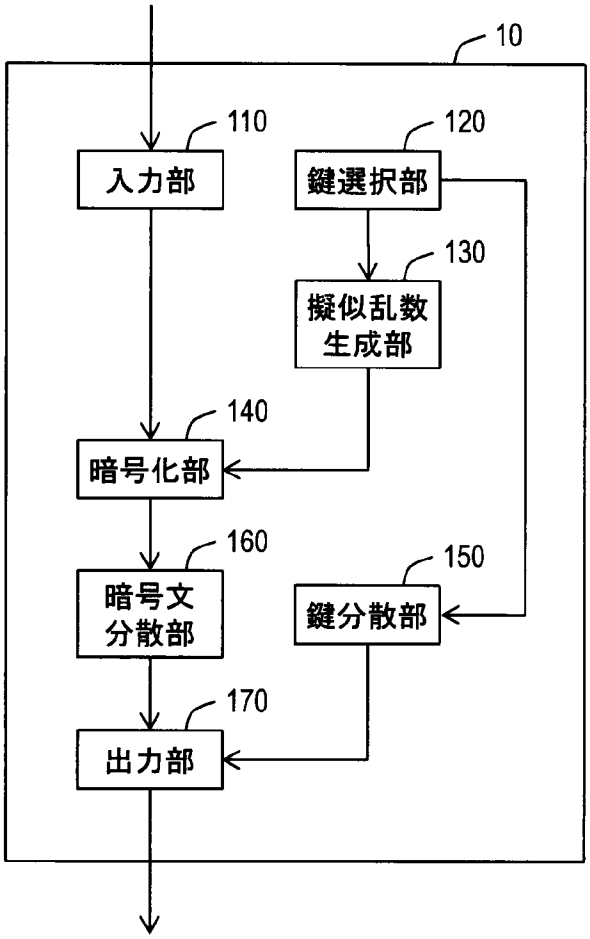

10
110
入力部
120
鍵選択部
130
擬似乱数
生成部
140
暗号化部
160
暗号文
分散部
150
鍵分散部
170
出力部

図2

[図3]

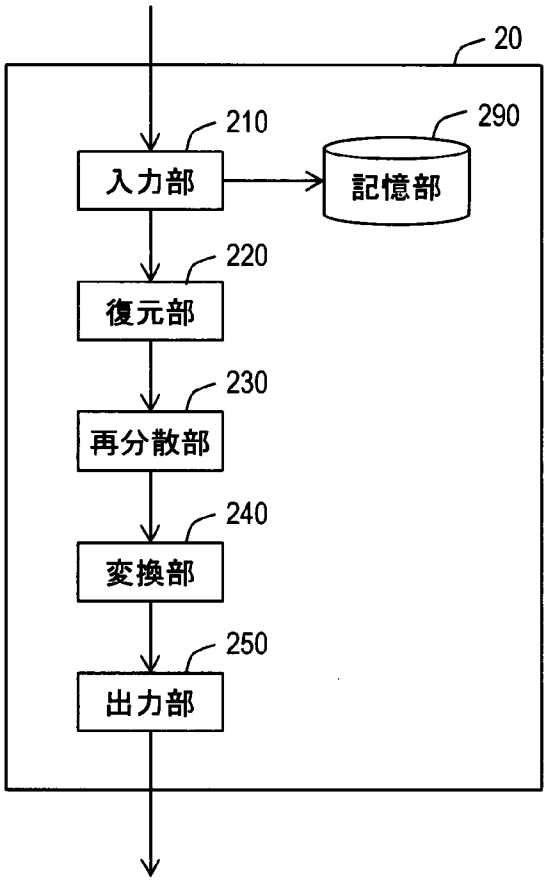


図3

[図4]

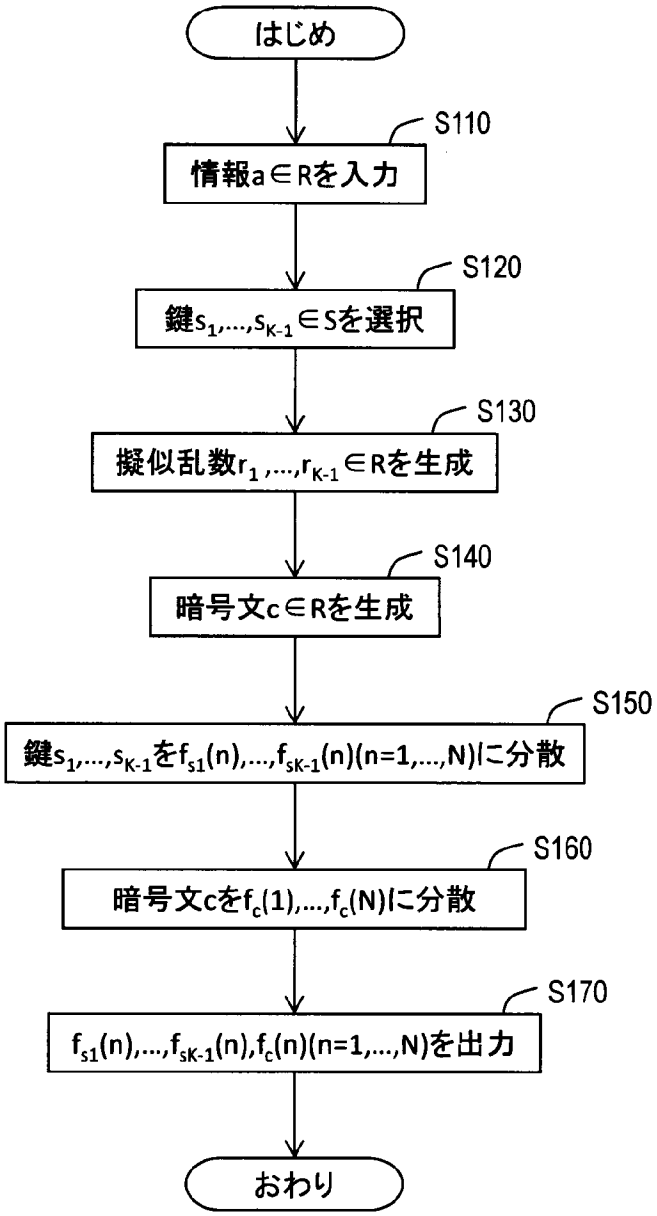

はじめ
S110
情報a∈Rを入力
S120
鍵$s_1,...,s_{K-1}$∈Sを選択
S130
擬似乱数$r_1,...,r_{K-1}$∈Rを生成
S140
暗号文c∈Rを生成
S150
鍵$s_1,...,s_{K-1}$を$f_{s1}(n),...,f_{sK-1}(n)$(n=1,...,N)に分散
S160
暗号文cを$f_c(1),...,f_c(N)$に分散
S170
$f_{s1}(n),...,f_{sK-1}(n),f_c(n)$(n=1,...,N)を出力
おわり

図4

[図5]

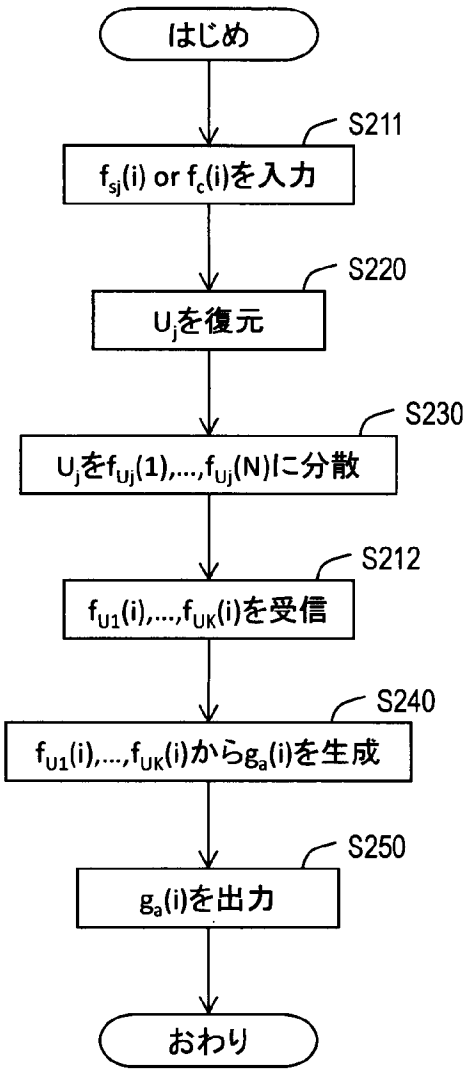

はじめ
S211
$f_{sj}(i)$ or $f_c(i)$を入力
S220
U_jを復元
S230
U_jを$f_{Uj}(1),\ldots,f_{Uj}(N)$に分散
S212
$f_{U1}(i),\ldots,f_{UK}(i)$を受信
S240
$f_{U1}(i),\ldots,f_{UK}(i)$から$g_a(i)$を生成
S250
$g_a(i)$を出力
おわり

図5

[図6]

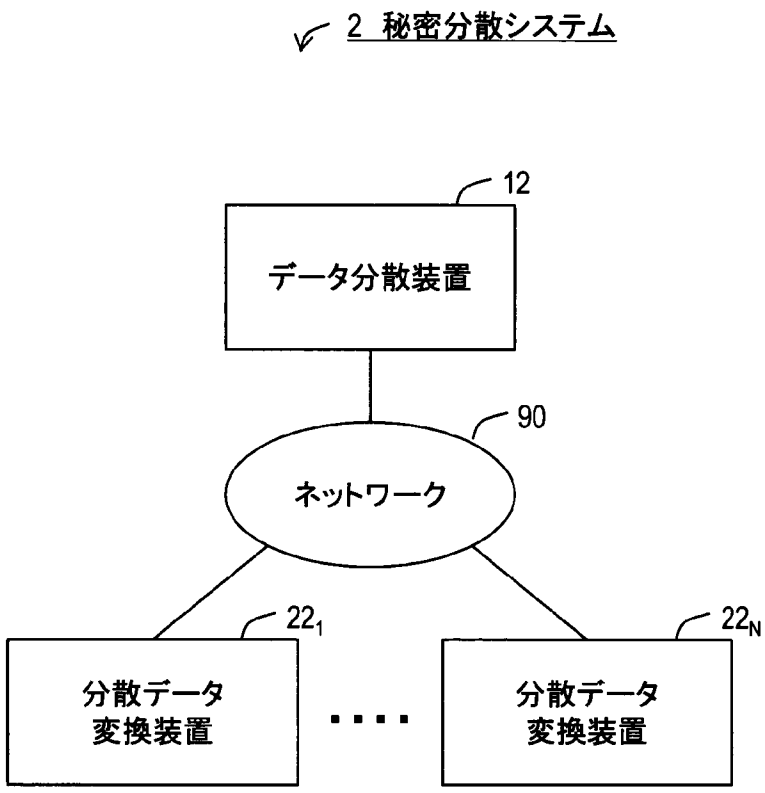

2 秘密分散システム
12
データ分散装置
90
ネットワーク
22_1
22_N
分散データ
変換装置
分散データ
変換装置

図6

[図7]

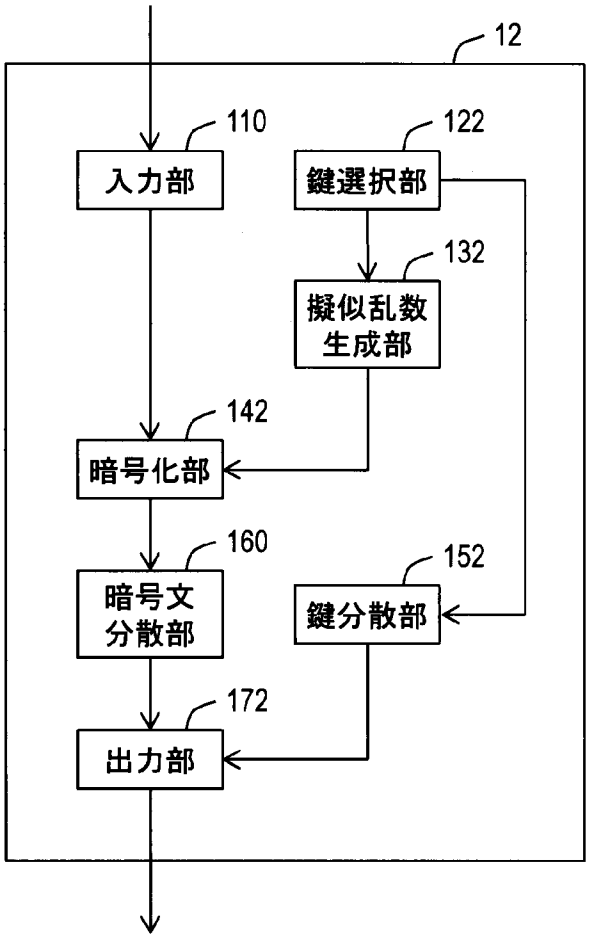

12
110
入力部
122
鍵選択部
132
擬似乱数
生成部
142
暗号化部
160
暗号文
分散部
152
鍵分散部
172
出力部

図7

[図8]

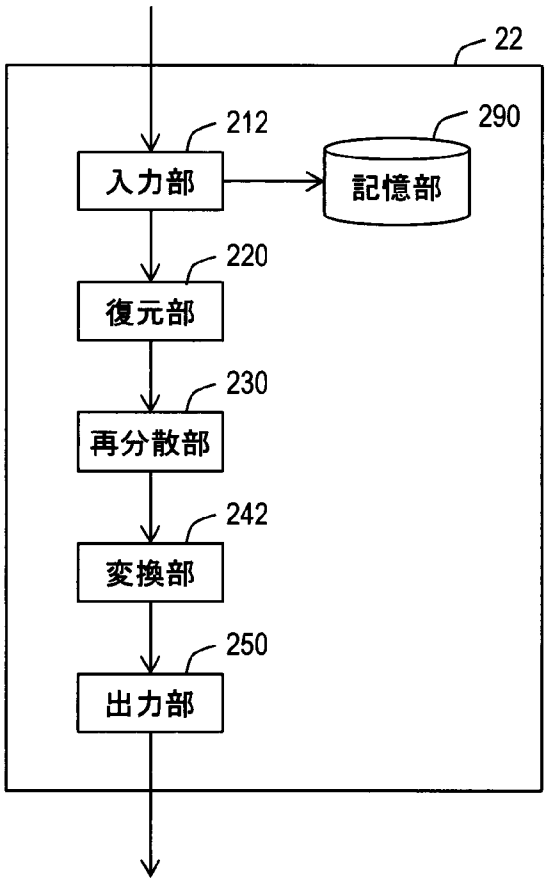


図8

[図9]

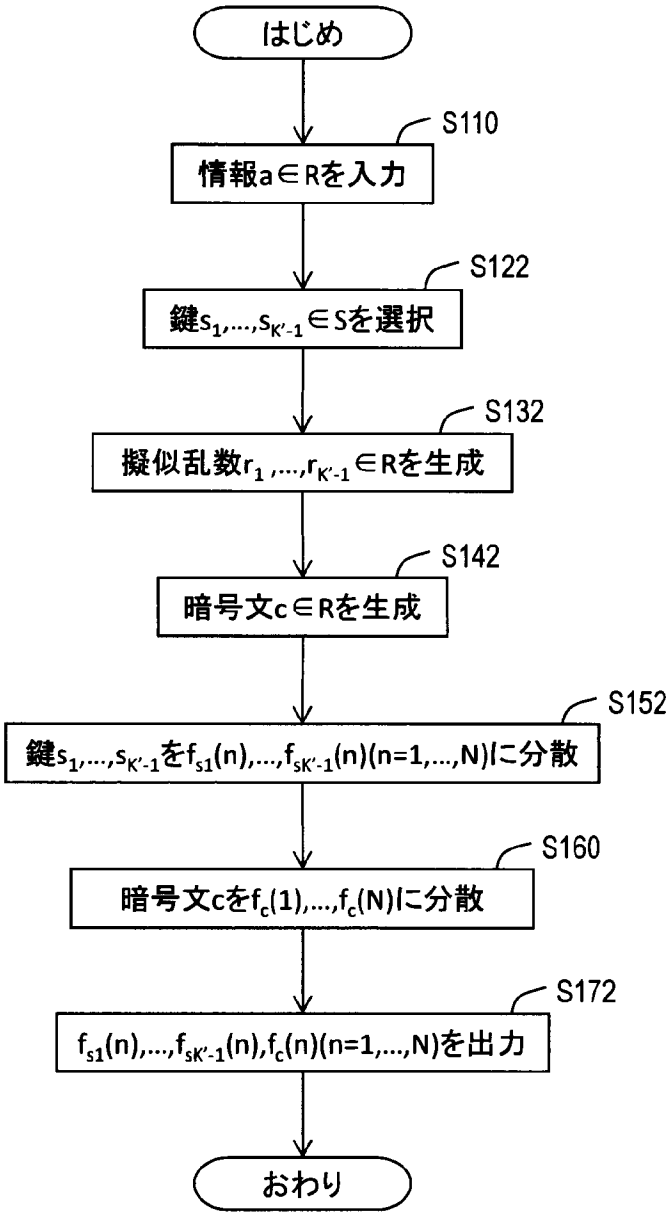

はじめ
S110
情報a∈Rを入力
S122
鍵$s_1,\ldots,s_{K'-1}$∈Sを選択
S132
擬似乱数$r_1,\ldots,r_{K'-1}$∈Rを生成
S142
暗号文c∈Rを生成
S152
鍵$s_1,\ldots,s_{K'-1}$を$f_{s1}(n),\ldots,f_{sK'-1}(n)(n=1,\ldots,N)$に分散
S160
暗号文cを$f_c(1),\ldots,f_c(N)$に分散
S172
$f_{s1}(n),\ldots,f_{sK'-1}(n),f_c(n)(n=1,\ldots,N)$を出力
おわり

図9

[図10]

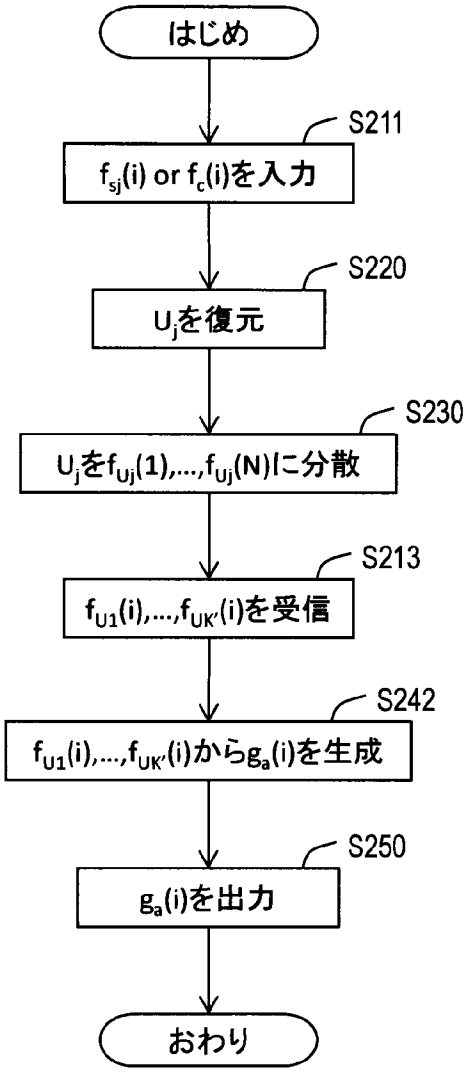

はじめ
S211
$f_{sj}(i)$ or $f_c(i)$を入力
S220
U_jを復元
S230
U_jを$f_{Uj}(1),\ldots,f_{Uj}(N)$に分散
S213
$f_{U1}(i),\ldots,f_{UK'}(i)$を受信
S242
$f_{U1}(i),\ldots,f_{UK'}(i)$から$g_a(i)$を生成
S250
$g_a(i)$を出力
おわり

図10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/068328

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i, *G06F21/62*(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)
H04L9/08, G06F21/62

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 1996-2013
Kokai Jitsuyo Shinan Koho 1971-2013 Toroku Jitsuyo Shinan Koho 1994-2013

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	Koji CHIDA et al., "Multiparty Keisan ni Tekiyo Kano na Keisanryoteki Short Himitsu Bunsan", Dai 29 Kai Symposium on Cryptography and Information Security (SCIS2012), 30 January 2012 (30.01.2012), 3B3-2	6,7,12 1-5,8-11
Y	JP 2004-279526 A (Oki Electric Industry Co., Ltd.), 07 October 2004 (07.10.2004), paragraphs [0003] to [0007], [0027] to [0030], [0046] to [0065], [0169] & US 2004/0179686 A1 & CN 1531241 A	1-5,8-11

☒ 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
26 July, 2013 (26.07.13)	06 August, 2013 (06.08.13)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/068328

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2007-124610 A (Nippon Telegraph and Telephone Corp.), 17 May 2007 (17.05.2007), paragraphs [0029] to [0051] (Family: none)	1-12
P,X	Koji CHIDA et al., "Efficient Conversions from Computational SSS And Ramp SSS to Multi-Party Computation", IEICE Technical Report, 12 July 2012 (12.07.2012), vol.112, no.126, pages 267 to 271	1-12

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１３／０６８３２８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(2006.01)i, G06F21/62(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.　H04L9/08, G06F21/62

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	１９７１－２０１３年
日本国実用新案登録公報	１９９６－２０１３年
日本国登録実用新案公報	１９９４－２０１３年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
X Y	千田浩司，他， "マルチパーティ計算に適用可能な計算量的ショート秘密分散"， 第29回 暗号と情報セキュリティシンポジウム（SCIS2012）， 2012.01.30，3B3-2	6,7,12 1-5,8-11
Y	JP 2004-279526 A（沖電気工業株式会社）2004.10.07， 段落 0003-0007，0027-0030，0046-0065，0169 & US 2004/0179686 A1 & CN 1531241 A	1-5,8-11

☑　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
２６．０７．２０１３	０６．０８．２０１３

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　４５３８
金沢　史明
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	JP 2007-124610 A (日本電信電話株式会社) 2007.05.17, 段落 0029-0051 (ファミリーなし)	1-12
P,X	千田浩司, 他, "計算量的秘密分散およびランプ型秘密分散のマルチパーティ計算拡張", 電子情報通信学会技術研究報告, 2012.07.12, Vol. 112, No. 126, pp. 267-271	1-12