(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105900165 A
(43)申请公布日 2016.08.24

(21)申请号 201580004210.0
(22)申请日 2015.01.07
(30)优先权数据
2014-006694 2014.01.17 JP
(85)PCT国际申请进入国家阶段日
2016.07.11
(86)PCT国际申请的申请数据
PCT/JP2015/050231 2015.01.07
(87)PCT国际申请的公布数据
WO2015/107952 JA 2015.07.23
(71)申请人 日本电信电话株式会社
地址 日本东京都
(72)发明人 五十岚大 滨田浩气 菊池亮 千田浩司
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 胡金珑
(51)Int.Cl.
G09C 1/00(2006.01)
G06F 21/60(2006.01)

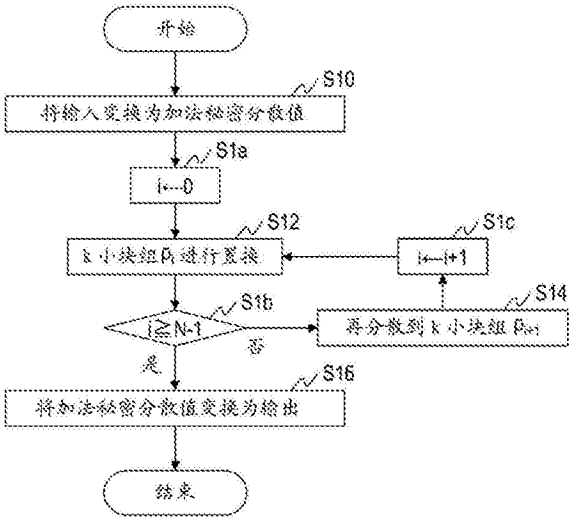
权利要求书3页 说明书14页 附图9页

(54)发明名称

秘密计算方法、秘密计算系统、随机置换装置以及程序

(57)摘要

高速进行包含秘密随机置换的秘密计算。单位置换步骤(S12)中，随机置换装置p_0，……，p_{k-1}通过置换数据π的子份额π_{pi}对明文a的加法秘密分散值《a》^{pi}进行置换。再分散步骤(S14)中，随机置换装置p_0使用与各个随机置换装置p_j(j＝1，……，k-1)共享的随机数r_1，……，r_{k-1}而生成加法秘密分散值《a》$^{pi+1}{}_{pk}$并发送给随机置换装置p_k，各个随机置换装置p_j使用随机数r_j而生成加法秘密分散值《a》$^{pi+1}{}_{pj}$。



CN 105900165 A

1.一种秘密计算方法,其中,

将n,k设为2以上的整数,设为n>k,设为$N={}_nC_k$,将ρ设为从n台随机置换装置选择的k台随机置换装置的组,$\rho_0,\cdots\cdots,\rho_{N-1}$构成为关于i=0,……,N-2成为$|\rho_i \backslash \rho_{i+1}|=1$,将《a》$^{\rho i}$设为第i个随机置换装置的组$\rho_i$所保持的明文a的加法秘密分散值,将《a》$^{\rho i}{}_p$设为加法秘密分散值《a》$^{\rho i}$之中随机置换装置p所保持的加法秘密分散值,将$\pi_{\rho i}$设为与第i个随机置换装置的组$\rho_i$对应的置换数据π的子份额,将随机置换装置$p_0$设为被包含于第i个随机置换装置的组$\rho_i$且不被包含于第i+1个随机置换装置的组$\rho_{i+1}$的随机置换装置,将随机置换装置$p_k$设为不被包含于第i个随机置换装置的组$\rho_i$且被包含于第i+1个随机置换装置的组$\rho_{i+1}$的随机置换装置,将随机置换装置$p_j$(j=1,……,k-1)设为在第i个随机置换装置的组ρ_i以及第i+1个随机置换装置的组ρ_{i+1}的任一个中都包含的k-1台随机置换装置,

所述秘密计算方法包含:

单位置换步骤,上述随机置换装置$p_0,\cdots\cdots,p_{k-1}$通过上述子份额$\pi_{\rho i}$对上述加法秘密分散值《a》$^{\rho i}$进行置换;以及

再分散步骤,上述随机置换装置p_0使用与各个上述随机置换装置p_j共享的随机数$r_1,\cdots\cdots,r_{k-1}$而生成加法秘密分散值《a》$^{\rho i+1}{}_{pk}$并发送给上述随机置换装置p_k,各个上述随机置换装置p_j使用上述随机数r_j而生成加法秘密分散值《a》$^{\rho i+1}{}_{pj}$。

2.如权利要求1所述的秘密计算方法,其中,

上述再分散步骤中,上述随机置换装置p_0通过下式而生成上述加法秘密分散值《a》$^{\rho i+1}{}_{pk}$,

【数8】

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

各个上述随机置换装置p_j通过下式而生成上述加法秘密分散值《a》$^{\rho i+1}{}_{pj}$

【数9】

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

3.如权利要求2所述的秘密计算方法,其中,

$\rho_0,\cdots\cdots,\rho_{N-1}$构成为,从第0个随机置换装置的组$\rho_0$中包含的k台随机置换装置至第N-1个随机置换装置的组ρ_{N-1}中包含的k台随机置换装置的路径的通信级数的最大值和最小值的差最小。

4.如权利要求1至3的任一项所述的秘密计算方法,其中,还包含:

事先变换步骤,将上述明文a的基于(k,n)-秘密分散的秘密分散值[a]变换为上述加法秘密分散值《a》$^{\rho 0}$;以及

事后变换步骤,将上述加法秘密分散值《a》$^{\rho N-1}$变换为上述秘密分散值[a]并进行输出。

5.如权利要求1至3的任一项所述的秘密计算方法,其中,

设为$N={}_{n-1}C_k$,将ρ设为从n台随机置换装置除去了规定的随机置换装置q而选择的k台随机置换装置的组,

所述秘密计算方法还包含:

事先变换步骤,将上述明文a变换为上述加法秘密分散值《a》$^{\rho 0}$;以及事后变换步骤,将

上述加法秘密分散值《a》$^{\rho N-1}$变换为基于(k,n)-秘密分散的秘密分散值[a]并进行输出，

上述单位置换步骤中，

若i≤$_{n}C_{k-n-1}C_{k}$，则上述随机置换装置q通过上述子份额$\pi_{\rho i}$对上述明文a进行置换，

若i>$_{n}C_{k-n-1}C_{k}$，则上述随机置换装置p_1，……，p_{k-1}通过上述子份额$\pi_{\rho i}$对上述加法秘密分散值《a》$^{\rho i}$进行置换。

6.如权利要求1至3的任一项所述的秘密计算方法，其中，

设为N=$_{n-1}C_{k}$，将ρ设为从n台随机置换装置除去了规定的随机置换装置q而选择的k台随机置换装置的组，

所述秘密计算方法还包含：

事先变换步骤，将上述明文a的基于(k,n)-秘密分散的秘密分散值[a]变换为上述加法秘密分散值《a》$^{\rho 0}$；以及

事后变换步骤，对上述加法秘密分散值《a》$^{\rho N-1}$进行复原并输出上述明文a，

上述单位置换步骤中，

若i≤$_{n-1}C_{k}$，则上述随机置换装置p_1，……，p_{k-1}通过上述子份额$\pi_{\rho i}$对上述加法秘密分散值《a》$^{\rho i}$进行置换，

若i>$_{n-1}C_{k}$，则上述随机置换装置q通过上述子份额$\pi_{\rho i}$对上述明文a进行置换。

7.如权利要求1至6的任一项所述的秘密计算方法，其中，还包含：

单位变换步骤，将通过上述单位置换步骤而置换的上述加法秘密分散值《a》$^{\rho i}$变换为基于(k,n)-秘密分散的秘密分散值[a]并积蓄在存储部中。

8.一种秘密计算系统，将n设为2以上的整数，包含n台随机置换装置，其中，

将k设为2以上的整数，设为n>k，设为N=$_{n}C_{k}$，将ρ设为从n台随机置换装置选择的k台随机置换装置的组，ρ_0，……，ρ_{N-1}构成为关于i=0，……，N-2成为$|\rho_i \backslash \rho_{i+1}|=1$，将《a》$^{\rho i}$设为第i个随机置换装置的组$\rho_i$所保持的明文a的加法秘密分散值，将《a》$^{\rho i}{}_{p}$设为加法秘密分散值《a》$^{\rho i}$之中随机置换装置p所保持的加法秘密分散值，将$\pi_{\rho i}$设为与第i个随机置换装置的组$\rho_i$对应的置换数据π的子份额，将随机置换装置$p_0$设为被包含于第i个随机置换装置的组$\rho_i$且不被包含于第i+1个随机置换装置的组$\rho_{i+1}$的随机置换装置，将随机置换装置$p_k$设为不被包含于第i个随机置换装置的组$\rho_i$且被包含于第i+1个随机置换装置的组$\rho_{i+1}$的随机置换装置，将随机置换装置$p_j$(j=1，……，k-1)设为在第i个随机置换装置的组ρ_i以及第i+1个随机置换装置的组ρ_{i+1}的任一个中都包含的k-1台随机置换装置，

上述随机置换装置包含：

单位置换部，通过上述子份额$\pi_{\rho i}$对上述加法秘密分散值《a》$^{\rho i}$进行置换；以及

再分散部，若该随机置换装置为上述随机置换装置p_0，则使用与各个上述随机置换装置p_j共享的随机数r_1，……，r_{k-1}而生成加法秘密分散值《a》$^{\rho i+1}{}_{pk}$并发送给上述随机置换装置p_k，若该随机置换装置为上述随机置换装置p_j的其中一个，则使用上述随机数r_j而生成加法秘密分散值《a》$^{\rho i+1}{}_{pj}$。

9.一种随机置换装置，其中，

将n,k设为2以上的整数，设为n>k，设为N=$_{n}C_{k}$，将ρ设为从n台随机置换装置选择的k台随机置换装置的组，ρ_0，……，ρ_{N-1}构成为关于i=0，……，N-2成为$|\rho_i \backslash \rho_{i+1}|=1$，将《a》$^{\rho i}$设为第i个随机置换装置的组$\rho_i$所保持的明文a的加法秘密分散值，将《a》$^{\rho i}{}_{p}$设为加法秘密分散

值《a》$^{\rho i}$之中随机置换装置p所保持的加法秘密分散值，将$\pi_{\rho i}$设为与第i个随机置换装置的组ρ_i对应的置换数据π的子份额，将随机置换装置p_0设为被包含于第i个随机置换装置的组ρ_i且不被包含于第i+1个随机置换装置的组ρ_{i+1}的随机置换装置，将随机置换装置p_k设为不被包含于第i个随机置换装置的组ρ_i且被包含于第i+1个随机置换装置的组ρ_{i+1}的随机置换装置，将随机置换装置p_j(j＝1,……,k-1)设为在第i个随机置换装置的组ρ_i以及第i+1个随机置换装置的组ρ_{i+1}的任一个中都包含的k-1台随机置换装置，

所述随机置换装置包含：

单位置换部，通过上述子份额$\pi_{\rho i}$对上述加法秘密分散值《a》$^{\rho i}$进行置换；以及

再分散部，若该随机置换装置为上述随机置换装置p_0，则使用与各个上述随机置换装置p_j共享的随机数r_1,……,r_{k-1}而生成加法秘密分散值《a》$^{\rho i+1}{}_{pk}$并发送给上述随机置换装置p_k，若该随机置换装置为上述随机置换装置p_j的其中一个，则使用上述随机数r_j而生成加法秘密分散值《a》$^{\rho i+1}{}_{pj}$。

10.一种程序，用于使计算机作为权利要求9所述的随机置换装置而发挥作用。

秘密计算方法、秘密计算系统、随机置换装置以及程序

技术领域

[0001] 本发明涉及秘密计算技术，特别是涉及进行秘密随机置换的技术。

背景技术

[0002] 秘密计算是通过秘密分散对数据进行保密且进行数据处理的技术。秘密分散是将数据变换为多个分散值，若使用一定个数以上的分散值则能够对原数据进行复原，根据小于一定个数的分散值则完全不能对原数据进行复原的技术。秘密分散能够分类为几个种类，例如，存在(k,n)-秘密分散、加法秘密分散、置换数据秘密分散等。

[0003] (k,n)-秘密分散是，将所输入的明文分割为n个份额(share)，分散到n个小块(party)$P=(p_0,\cdots\cdots,p_{n-1})$，若集齐任意k个份额则能够对明文进行复原，根据小于k个份额则不能得到与明文相关的所有信息的秘密分散。在(k,n)-秘密分散的具体方式中，例如存在Shamir秘密分散、复制秘密分散等。

[0004] 加法秘密分散是基于复制秘密分散的(k,k)-秘密分散。(k,k)-秘密分散是在(k,n)-秘密分散中设为n＝k的情况。在(k,k)-秘密分散中，只要不集齐全部小块的份额就不能对明文进行复原。加法秘密分散是仅通过将k个份额进行相加，明文就被复原的最简单的秘密分散。

[0005] 置换数据秘密分散是对置换数据进行保密而进行的秘密分散。置换数据是表示在对数据串进行重排时的重排方式的数据。在对m个数据串进行重排时，大小为m的置换数据π是表示双射(bijective)映射$\pi:N_m\rightarrow N_m$的数据。其中，对于任意整数m，N_m是小于m的非负整数的集合。例如，将矢量$\vec{x}\in(N_m)^m$中各要素相互不同的数据看作大小为m的随机置换数据。

[0006] 更具体而言，能够将矢量$\vec{x}=(3,0,2,1)$看作大小为4的随机置换数据。例如，设为将数据串$\vec{y}=(1,5,7,10)$通过矢量$\vec{x}$进行重排。将作为数据串$\vec{y}$的第0个要素的1移动到矢量$\vec{x}$的第0个要素所示的第3个。将作为数据串$\vec{y}$的第1个要素的5移动到矢量$\vec{x}$的第1个要素所示的第0个。同样，将7移动到第2个，将10移动到第1个。作为结果，得到置换后的数据串$\vec{z}=(5,10,7,1)$。

[0007] 置换数据秘密分散通过以下的过程对置换数据进行保密。设为存在N个k小块组的串$P=\rho_0,\cdots\cdots,\rho_{N-1}$。例如，在k＝2时，各k小块组$\rho_i$是小块$p_0$和小块$p_1$的组$(p_0,p_1)$、小块$p_0$和小块$p_2$的组$(p_0,p_2)$等。设为各k小块组$\rho_i$内的全部小块相互共享置换数据$\pi_{\rho i}$，而在补集$\bar{\rho}_i$中不知道。并且，将对应的明文设为$\pi_0(\pi_1(\cdots\cdots(\pi_{N-1}(I))\cdots\cdots))$。其中，I是以与输入相同的排列原样输出的置换、也就是说恒等置换。此时，若将k小块组的串$P=\rho_0,\cdots\cdots,\rho_{N-1}$设定为“(条件1)对于任意k-1小块组ρ，其中一个补集$\bar{\rho}_i$满足$\rho\subseteq\bar{\rho}_i$”，则无论k-1小块怎样结合，也不知道其中一个置换数据$\pi_{\rho i}$。

[0008] 例如，在小块数n满足$n\geq 2k-1$时，若将k小块组的串P设为包含全部k小块组的集合，则满足上述的条件1。此外，在小块数n满足$n>2k-1$时，即使不包含全部k小块组有时也实现上述的条件1。例如，在k＝2，n＝4时，$\{(p_0,p_1),(p_2,p_3)\}$不包含全部k小块组但满足条件

1。

[0009] 秘密随机置换是随机对所输入的数据串进行置换以使处理执行者也不知道以怎样的顺序进行了置换的技术。作为进行秘密随机置换的现有技术，存在非专利文献1中记载的技术。

[0010] 非专利文献1中记载的秘密随机置换的基本形式是，将(k,n)-秘密分散值的串[$a^{\rightarrow}$]作为输入，生成置换数据秘密分散值〈π〉，输出(k,n)-秘密分散值的串[$b^{\rightarrow}$]=([$a_{\pi(0)}$],……,[$a_{\pi(m-1)}$])。此时，其特征在于，哪个小块都不知道将置换数据秘密分散值〈π〉的明文π、也就是说数据串以怎样的顺序进行了调换。作为具体的处理，对置换数据秘密分散的各子份额$\pi_{\rho i}$，属于k小块集合ρ_i的小块$p \in \rho_i$通过不是秘密计算的通常的置换处理，根据输入[$a^{\rightarrow}$]=([a_0],……,[a_{m-1}])而生成([$a_{\pi\rho i(0)}$],……,[$a_{\pi\rho i(m-1)}$])，通过被称为再分散的处理反复对其进行重新秘密分散。

[0011] 秘密随机置换根据输入输出的类型的差异考虑以下的三种。第一种是输入和输出都为(k,n)-秘密分散值的情况。第二种是输入为(k,n)-秘密分散值，输出为公开值的情况。第三种是输入为公开值，输出为(k,n)-秘密分散值的情况。在输入为公开值的情况下，对公开值进行秘密分散而作为秘密分散值，而后进行上述的基本形式的处理。此外，在输出为公开值的情况下，在进行了上述的基本形式的处理后进行公开处理。公开值是全部小块知道的值。公开处理例如是全部小块将自身的份额发送给其他全部小块，全部小块根据所接收到的份额进行秘密分散的复原。

[0012] 现有技术文献

[0013] 非专利文献

[0014] 非专利文献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

发明内容

[0015] 发明要解决的课题

[0016] 非专利文献1中记载的秘密随机置换使用(k,n)-秘密分散值来反复进行置换和再分散的处理。为了对(k,n)-秘密分散值进行再分散，各小块必须与全部小块相互进行通信，存在通信量以及通信级数大的问题。

[0017] 本发明的目的在于，降低秘密随机置换所需的通信量以及通信级数，高速进行包含秘密随机置换的秘密计算。

[0018] 用于解决课题的手段

[0019] 为了解决上述的课题，本发明的秘密计算方法中，将n,k设为2以上的整数，设为n>k，设为$N={}_nC_k$，将ρ设为从n台随机置换装置选择的k台随机置换装置的组，ρ_0,……,ρ_{N-1}构成为关于i=0,……,N-2成为$|\rho_i \backslash \rho_{i+1}|=1$，将《a》$^{\rho i}$设为第i个随机置换装置的组$\rho_i$所保持的明文a的加法秘密分散值，将《a》$^{\rho i}{}_p$设为加法秘密分散值《a》$^{\rho i}$之中随机置换装置p所保持的加法秘密分散值，将$\pi_{\rho i}$设为与第i个随机置换装置的组$\rho_i$对应的置换数据π的子份额，将随机置换装置$p_0$设为被包含于第i个随机置换装置的组$\rho_i$且不被包含于第i+1个随机置换装置的组$\rho_{i+1}$的随机置换装置，将随机置换装置$p_k$设为不被包含于第i个随机置换装置的组$\rho_i$且被包含于第i+1个随机置换装置的组$\rho_{i+1}$的随机置换装置，将随机置换装置$p_j$(j=1,……,

k-1)设为在第i个随机置换装置的组ρ_i以及第i+1个随机置换装置的组ρ_{i+1}的任一个中都包含的k-1台随机置换装置，所述秘密计算方法包含：单位置换步骤，随机置换装置p_0，……，p_{k-1}通过子份额$\pi_{\rho i}$对加法秘密分散值《a》$^{\rho i}$进行置换；以及再分散步骤，随机置换装置p_0使用与随机置换装置p_1，……，p_{k-1}共享的随机数r_1，……，r_{k-1}而生成加法秘密分散值《a》$^{\rho i+1}{}_{pk}$并发送给随机置换装置p_k，各个随机置换装置p_j使用随机数r_j而生成加法秘密分散值《a》$^{\rho i+1}{}_{pj}$。

[0020] 发明效果

[0021] 根据本发明的秘密计算技术，能够降低在进行秘密随机置换时的通信量以及通信级数。从而，能够高速执行包含秘密随机置换的秘密计算。

附图说明

[0022] 图1是例示秘密计算系统的功能结构的图。

[0023] 图2是例示第一实施方式的随机置换装置的功能结构的图。

[0024] 图3是例示第一实施方式的秘密计算方法的处理流程的图。

[0025] 图4是例示第二实施方式的秘密计算方法的处理流程的图。

[0026] 图5是例示第三实施方式的秘密计算方法的处理流程的图。

[0027] 图6是例示第四实施方式的随机置换装置的功能结构的图。

[0028] 图7是例示第四实施方式的秘密计算方法的处理流程的图。

[0029] 图8是表示第一实施方式中的k＝2，n＝3的具体例的图。

[0030] 图9是表示第一实施方式中的k＝3，n＝5的具体例的图。

[0031] 图10是表示第二实施方式中的k＝2，n＝3的具体例的图。

[0032] 图11是表示第二实施方式中的k＝3，n＝5的具体例的图。

[0033] 图12是表示第三实施方式中的k＝2，n＝3的具体例的图。

[0034] 图13是表示第三实施方式中的k＝3，n＝5的具体例的图。

具体实施方式

[0035] 在实施方式的说明之前，定义在本说明书中使用的记载方法以及用语。

[0036] [记载方法]

[0037] p表示持有份额的小块。

[0038] P＝(p_0，……，p_{n-1})表示持有份额的n小块整体的集合。

[0039] ρ＝(p_0，……，p_{k-1})表示执行置换处理的k小块组的集合。

[0040] P＝(ρ_0，……，ρ_{N-1})表示执行各置换处理的k小块组的顺序。其中，$N={}_nC_k$为置换处理的执行次数，是从n小块选择k小块的全部组合的数目。

[0041] [x]表示明文x∈G的(k,n)-秘密分散值。在此，G为交换群。(k,n)-秘密分散值是汇集了通过(k,n)-秘密分散对明文x进行了分散的全部份额的组。秘密分散值[x]一般被分散到n小块集合P而持有，所以不会在一个地方持有全部，是虚拟的。

[0042] $[x]_p$表示(k,n)-秘密分散值[x]之中小块p∈P所持有的份额。

[0043] [x⁻]表示明文的串成为x⁻的(k,n)-秘密分散值的串。

[0044] [G]表示交换群G上的(k,n)-秘密分散值整体的集合。

[0045] 《x》$^{\rho}$表示明文x∈G的加法秘密分散值中k小块组ρ持有份额的加法秘密分散值。加法秘密分散值表示汇集了通过加法秘密分散对明文x进行了分散的全部份额的组。

[0046] 《x》$^{\rho}_{p}$表示加法秘密分散值《x》$^{\rho}$之中小块p∈ρ所持有的份额。

[0047] 《$\bar{x}$》$^{\rho}$表示明文的串成为$\bar{x}$的加法秘密分散值的串。

[0048] 《G》$^{\rho}$表示交换群G上的加法秘密分散值整体的集合。

[0049] 〈π〉表示置换数据π的置换数据秘密分散值。

[0050] Π表示大小为m的置换数据整体的集合。

[0051] 〈Π〉表示大小为m的置换数据秘密分散值整体的集合。

[0052] [发明点]

[0053] 本发明的秘密随机置换的概要如以下那样。

[0054] 步骤1.将输入从(k,n)-秘密分散值或公开值变换为加法秘密分散值。

[0055] 步骤2.反复进行以下处理:在加法秘密分散值上,属于具有份额的k小块集合ρ的各小块进行基于置换数据秘密分散值〈π〉的子份额π_{ρ}的通常的置换并进行再分散。其中,最后一次不进行再分散。以下,将反复的一次称为单位置换,将反复的处理整体称为反复置换。

[0056] 步骤3.将输出从加法秘密分散值变换为(k,n)-秘密分散值或公开值。

[0057] 步骤1以及步骤3能够应用已有的方法。以下,说明步骤2的处理中的要点。

[0058] ＜单位置换＞

[0059] 单位置换中的要点在于,在第i次单位置换中,选择k小块集合ρ_i以使成为$|\rho_i \backslash \rho_{i+1}|=1$。也就是说,在进行第i次单位置换的k小块集合$\rho_i$、和进行第i+1次单位置换的k小块集合$\rho_{i+1}$中,仅1小块不同而剩余的k-1小块为相同的小块。由于是只有一个小块不同的情况,因此将这样的单位置换称为1-加法再分散协议。

[0060] 在非专利文献1中记载的秘密随机置换中的再分散中,需要(n-1)(k-1)个G要素的通信量。另一方面,在1-加法再分散协议中,k-1个G要素的通信量就可以。特别是,若预先共享种子(seed)而共享伪随机数,则通信量为一个G要素的通信量即可。在该情况下,通信量成为常数,非常高效。

[0061] 1-加法再分散协议中,将输入设为k小块组$\rho=p_0,\cdots\cdots,p_{k-1}$所持有的秘密分散值《a》$^{\rho}$∈《G》$^{\rho}$,通过以下的过程进行数据处理,输出其他k小块组$\rho'=p_1,\cdots\cdots,p_k$所持有的秘密分散值《a》$^{\rho'}$∈《G》$^{\rho'}$。其中,设为小块的作用被适当变更。

[0062] 首先,小块p_0关于i＝1,……,k-1,共享小块p_i和随机数r_i∈G。接着,小块p_0通过下式来计算秘密分散值《a》$^{\rho'}_{p_k}$,并发送给小块p_k。小块p_k输出所接收到的《a》$^{\rho'}_{p_k}$。

[0063] 【数1】

[0064] $$\langle\langle a\rangle\rangle^{\rho'}_{p_k}=\langle\langle a\rangle\rangle^{\rho}_{p_0}-\sum_{1\le i<k} r_i$$

[0065] 接下来,小块p_i(i＝1,……,k-1)通过下式来计算秘密分散值《a》$^{\rho'}_{p_i}$并进行输出。

[0066] 【数2】

[0067] $$\langle\langle a\rangle\rangle^{\rho'}_{p_i}=\langle\langle a\rangle\rangle^{\rho}_{p_i}+r_i$$

[0068] ＜反复置换之中的单位置换的并行化＞

[0069] 反复置换是置换→再分散→置换→再分散→……→置换这样的反复，执行N次置换，执行N-1次再分散。若单纯地进行该反复置换，则通信的级数还是再分散的次数，成为N-1级。但是，基于1-加法再分散协议的单位置换能够关于通信而并行化。这是因为等待数据接收的小块仅为1小块、即没有参加上次的单位置换的小块，且因为其他小块不会等待任何数据接收，能够仅执行离线处理而转移到下一单位置换处理。由于加法秘密分散的份额为k个，若适当地设定k小块组的顺序P，则能够将最大k次单位置换以1级来执行。由此，能够将通信级数降低为(N-1)/k级。

[0070] k小块组的顺序P关于任意$i<k$，设为从小块p_i的路径的通信级数相互相等或最大值和最小值的差最小的顺序，从而能够将通信级数高效化。

[0071] 从小块p_i的路径针对长度为L的k小块组的串$P=(\rho_0,\cdots\cdots,\rho_{L-1})$，是指小块的串$(p_{j0},p_{j1},\cdots\cdots,p_{jL-1})$，并且是通过下式归纳地决定的串。

[0072] 【数3】

[0073] $p_{j0}=p_i$，

[0074] $$p_{j_{L+1}}=\begin{cases}p_{j_L} & \text{if } p_{j_L}\in P_{L+1}\\ P_{L+1}\setminus P_L\text{的唯一的元}\,p & \text{otherwise}\end{cases}$$

[0075] 路径的通信级数是，在路径之中因小块变化而需要通信的λ的数目、即$|\{\lambda\in N_L\,|\,p_{j\lambda}\neq p_{j\lambda+1}\}|$。在1-加法再分散协议的通信中，除了小块$p_k$等待从小块$p_0$的发送以外是随机数的通信，不依赖于前级的再分散的结果。路径的通信级数表示该小块p_0至小块p_k的通信之中串行排列而不能并行执行的级数。反复置换整体的通信级数如下式所示，所以若各路径的通信级数成为均等，则高效。

[0076] 【数4】

[0077] $$\max_{i<k}(\text{从}p_i\text{的路径的通信级数})$$

[0078] 且

[0079] $$\sum_{i<k}(\text{从}p_i\text{的路径的通信级数})=|P|$$

[0080] 以下，详细说明本发明的实施方式。另外，对附图中具有相同的功能的构成部分赋予相同的序号，省略重复说明。

[0081] [第一实施方式]

[0082] 参照图1，说明第一实施方式所涉及的秘密计算系统的结构例。秘密计算系统包含n(≥2)台随机置换装置$1_1,\cdots\cdots,1_n$和网络9。随机置换装置$1_1,\cdots\cdots,1_n$分别连接到网络9。网络9构成为各个随机置换装置$1_1,\cdots\cdots,1_n$能够相互通信即可，例如能够由互联网、LAN、WAN等构成。此外，各个随机置换装置$1_1,\cdots\cdots,1_n$不一定要能够经由网络9以在线的方式进行通信。例如，也可以构成为将某随机置换装置1_i($1\leq i\leq n$)输出的信息存储在USB存储器等可移动记录介质中，从该可移动记录介质向不同的随机置换装置1_j($1\leq j\leq n$、$i\neq j$)以离线的方式进行输入。

[0083] 参照图2，说明秘密计算系统中包含的随机置换装置1的结构例。随机置换装置1包含事先变换部10、单位置换部12、再分散部14、事后变换部16以及存储部18。随机置换装置1例如是在具有中央运算处理装置(中央处理单元(Central Processing Unit)、CPU)、主存

储装置(随机存取存储器(Random Access Memory)、RAM)等的公知或专用的计算机中读入特殊的程序而构成的特殊的装置。随机置换装置1例如在中央运算处理装置的控制下执行各处理。向随机置换装置1输入的数据、各处理中得到的数据例如被储存在主存储装置中，在主存储装置中储存的数据根据需要而被读出并被利用于其他处理。随机置换装置1所具备的存储部18例如能够由RAM(随机存取存储器(Random Access Memory))等主存储装置；由硬盘、光盘或者闪速存储器(Flash Memory)那样的半导体存储器元件构成的辅助存储装置；或关系数据库(relational database)、键值存储(key value store)等中间件构成。

[0084] 在与小块p对应的随机置换装置1_p所具备的存储部18中，存储有明文a的(k,n)-秘密分散值$[a]_p$或者公开值a、与包含小块p的k小块的组ρ对应的置换数据π的子份额π_ρ以及N×k个种子$s_{0,1},\cdots\cdots,s_{N-1,k}$。另外，种子$s_{0,1},\cdots\cdots,s_{N-1,k}$是为了在后述的再分散部14的处理中在生成随机数时无通信地进行而预先存储的种子，但在每次协调而进行随机数生成的情况下也可以不存储。

[0085] 参照图3，按照实际进行的动作过程的顺序说明第一实施方式所涉及的秘密计算系统所执行的秘密计算方法的处理流程的一例。

[0086] 在步骤S10中，k台随机置换装置$1_{\rho 0}$所具备的事先变换部10将在存储部18中存储的(k,n)-秘密分散值$[a]_{pi}$或者公开值a变换为加法秘密分散值$\langle\langle a\rangle\rangle^{\rho 0}$。$\rho_0$是k小块组的串$P=(\rho_0,\cdots\cdots,\rho_{N-1})$的第0个要素，随机置换装置$1_{\rho 0}$是与$\rho_0=(p_0,\cdots\cdots,p_{k-1})$对应的k台随机置换装置$1_{p0},\cdots\cdots,1_{pk-1}$。

[0087] 从(k,n)-秘密分散值或者公开值变换为加法秘密分散值的方法通过已知的方法进行即可。

[0088] 在输入为公开值的情况下，向加法秘密分散值的变换例如能够如以下那样进行。将ρ设为k台随机置换装置$1_{p0},\cdots\cdots,1_{pk-1}$的组，将$a\in G$设为所输入的公开值，设为随机置换装置$1_{p0}$已知公开值a。从公开值a向加法秘密分散值$\langle\langle a\rangle\rangle^{\rho}$的变换关于$i=0,\cdots\cdots,k-1$，通过下式进行即可。

[0089] 【数5】

[0090] $$\langle\langle a\rangle\rangle^{P}_{p_i}:=\begin{cases}a & \text{if } i=0\\ 0 & \text{otherwise}\end{cases}$$

[0091] 在输入为(k,n)-秘密分散值的情况下，向加法秘密分散值的变换例如能够通过在下述的参考文献1以及参考文献2中记载的方法来进行。在参考文献1中，记述了从包含Shamir秘密分散的线性秘密分散无通信地变换为加法秘密分散的方法。在参考文献2中，记述了从复制秘密分散无通信地变换为线性秘密分散的方法，所以从复制秘密分散向加法秘密分散的变换通过将参考文献2中记载的方法和参考文献1中记载的方法进行组合从而无通信地实现。

[0092] 〔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0(1)ビット通信ビット分解および0(|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

[0093] 〔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.3378of Lecture Notes in Computer Science,pp.342-362,2005.

[0094] 在步骤S1a中，k台随机置换装置$1_{\rho 0}$将表示置换处理的执行次数的计数器i初始化为0。

[0095] 在步骤S12中，k台随机置换装置$1_{\rho i}$所具备的单位置换部12使用在存储部18中存储的置换数据的子份额$\pi_{\rho i}$对加法秘密分散值《a》$^{\rho i}$进行置换。ρ_i是k小块组的串$P=(\rho_0,\cdots\cdots,\rho_{N-1})$的第i个要素，随机置换装置$1_{\rho i}$是与$\rho_i=(p_0,\cdots\cdots,p_{k-1})$对应的k台随机置换装置$1_{p0},\cdots\cdots,1_{pk-1}$。置换的方法通过以往的置换数据秘密分散的方法进行即可。

[0096] 在步骤S1b中，k台随机置换装置$1_{\rho i}$判定是否执行了规定次数的置换处理。具体而言，将$N={}_nC_k$设为单位置换的总执行次数，判定计数器i的值是否达到了N-1。若i<N-1，则将处理前进至步骤S14。若i≥N-1，则将处理前进至步骤S16。

[0097] 在步骤S14中，k台随机置换装置$1_{\rho i+1}$所具备的再分散部14通过1-加法再分散协议进行加法秘密分散值《a》$^{\rho i}$的再分散。以下，将随机置换装置1_{p0}设为被包含于随机置换装置$1_{\rho i}$而不被包含于随机置换装置$1_{\rho i+1}$的随机置换装置，将随机置换装置1_{pk}设为不被包含于随机置换装置$1_{\rho i}$而被包含于随机置换装置$1_{\rho i+1}$的随机置换装置。此外，将随机置换装置1_{pj}(j=1,……,k-1)设为表示除随机置换装置1_{pk}之外的随机置换装置$1_{\rho i+1}$中包含的k-1台随机置换装置。

[0098] 首先，随机置换装置$1_{\rho i+1}$所具备的再分散部14生成k个随机数$r_1,\cdots\cdots,r_k\in G$。随机数$r_1,\cdots\cdots,r_k$也可以由k台随机置换装置$1_{\rho i+1}$协调而生成共享的随机数$r_1,\cdots\cdots,r_k$，也可以使用在存储部18中存储的种子$s_{i,1},\cdots\cdots,s_{i,k}$来生成伪随机数$r_1,\cdots\cdots,r_k$。若使用预先共享的种子$s_{i,1},\cdots\cdots,s_{i,k}$来生成伪随机数，则能够无随机置换装置间的通信地进行随机数生成，因此非常高效。

[0099] 接着，随机置换装置1_{p0}所具备的再分散部14使用加法秘密分散值《a》$^{\rho i}{}_{p0}$以及随机数$r_0,\cdots\cdots,r_{k-1}$通过下式来生成用于随机置换装置1_{pk}的加法秘密分散值《a》$^{\rho i+1}{}_{pk}$，并发送给随机置换装置1_{pk}。

[0100] 【数6】

[0101] $$\langle\langle a\rangle\rangle_{p_k}^{\rho_{i+1}}=\langle\langle a\rangle\rangle_{p_0}^{\rho_i}-\sum_{1\le i<k}r_i$$

[0102] 并且，随机置换装置1_{pj}所具备的再分散部14使用加法秘密分散值《a》$^{\rho i}{}_{pj}$以及随机数r_j，通过下式来生成加法秘密分散值《a》$^{\rho i+1}{}_{pj}$。

[0103] 【数7】

[0104] $$\langle\langle a\rangle\rangle_{p_j}^{\rho_{i+1}}=\langle\langle a\rangle\rangle_{p_j}^{\rho_i}-r_j$$

[0105] 在步骤S1c中，k台随机置换装置$1_{\rho i+1}$对表示置换处理的执行次数的计数器i加上1。以后，直至在步骤S1b中判定为计数器i达到了N-1为止，反复进行步骤S12的单位置换和步骤S14的再分散。

[0106] 在步骤S16中，k台随机置换装置$1_{\rho N-1}$所具备的事后变换部16将加法秘密分散值变换为(k,n)-秘密分散值或者公开值。从加法秘密分散值变换为其他形式的方法能够比较少量地进行。另外，下述的变换方法为一例，不意味着在其他变换方法中不能应用。

[0107] 在输出为公开值的情况下，存在对于想要得到输出的随机置换装置1_p($1\le p\le n$)，

最后执行了置换处理的k台随机置换装置$1_{\rho N-1}$发送加法秘密分散值《a》$^{\rho N-1}{}_{pj}$(j=0,……,k-1),随机置换装置1_p进行复原的方法。此外,还存在对于从想要得到输出的多台随机置换装置1_ρ($\rho\subseteq\{1,\ldots\ldots,n\}$)选择的一台随机置换装置$1_p$($p\in\rho$),最后执行了置换处理的k台随机置换装置$1_{\rho N-1}$发送加法秘密分散值《a》$^{\rho N-1}{}_{pj}$(j=0,……,k-1),随机置换装置$1_p$进行复原,向其他随机置换装置$1_\rho$发送复原结果的方法。

[0108] 在输出为(k,n)-秘密分散值的情况下,具有线性秘密分散、复制秘密分散等加法同态性,也就是说对于能在秘密分散值上无通信地进行加法的秘密分散,例如能够通过以下的过程进行变换。首先,k台随机置换装置$1_{\rho N-1}$通过变换目标的(k,n)-秘密分散对加法秘密分散值《a》$^{\rho N-1}{}_{pj}$进行秘密分散,向n台随机置换装置1_P分发(k,n)-秘密分散值[《a》$^{\rho N-1}{}_{pj}$]$_p$(p=1,……,n)。并且,n台随机置换装置1_P将所接收到的k个(k,n)-秘密分散值[《a》$^{\rho N-1}{}_{pj}$]$_p$全部相加。

[0109] 像这样,第一实施方式的秘密计算系统通过将输入变换为加法秘密分散值,从而能够使再分散的处理中的通信量降低,能够比以往的随机置换更高效地进行处理。

[0110] [第二实施方式]

[0111] 在秘密随机置换的输入为公开值的情况下能够比第一实施方式更高效化。在非专利文献1、第一实施方式的方法中,为了使随机置换的置换数据成为秘密,需要对任意k-1小块组ρ,进行其中一个补集$\bar{\rho}_i$满足$\rho\subseteq\bar{\rho}_i$的k小块组的串P的要素数次的单位置换。但是,在某小块p具有的公开值为输入的情况下,也可以进行更少次数的单位置换。由于输入为公开值,所以最初小块p能够以1小块进行置换,这是因为能够将小块p已知的量的置换全部汇总进行。

[0112] 在至少1台随机置换装置1_{p0}所具备的存储部18中,存储有公开值a。公开值a由至少1台持有即可,也可以由几台随机置换装置持有。

[0113] 设为在除了随机置换装置1_{p0}之外的n-1台随机置换装置1_{p1},……,1_{pn-1}所具备的存储部18中,存储有与包含小块p_i的k小块的组ρ_i对应的置换数据π的子份额$\pi_{\rho i}$以及N×k个种子$s_{0,1}$,……,$s_{N-1,k}$。其中,N为$_{n-1}C_k$。与第一实施方式同样,不一定存储种子$s_{0,1}$,……,$s_{N-1,k}$。

[0114] 参照图4,按照实际进行的动作过程的顺序说明第二实施方式所涉及的秘密计算系统所执行的秘密计算方法的处理流程的一例。

[0115] 在步骤$S12_{p0}$中,随机置换装置1_{p0}所具备的单位置换部12生成随机的置换数据π,通过置换数据π对公开值a进行置换。置换的方法与以往的置换方法同样。

[0116] 在步骤$S10_{p0}$中,随机置换装置1_{p0}所具备的事先变换部10将置换后的公开值a变换为加法秘密分散值《a》$^{\rho-1}$。变换的方法与第一实施方式的步骤S10同样。加法秘密分散值《a》$^{\rho-1}$被分发给随机置换装置$1_{\rho0}$之中任意选择的k-1台。在此,设为被分发给随机置换装置1_{p1},……,1_{pk-1}。

[0117] 在步骤$S14_{p0}$中,k台随机置换装置$1_{\rho0}$所具备的再分散部14通过1-加法再分散协议进行加法秘密分散值《a》$^{\rho-1}$的再分散。再分散的方法与第一实施方式的步骤S14同样。

[0118] 以后,通过除了随机置换装置1_{p0}之外的n-1台随机置换装置1_{p1},……,1_{pn-1},执行步骤S1a至S16的处理。

[0119] 像这样,在第二实施方式的秘密计算系统中,在通过1台随机置换装置汇总而进行

了置换之后通过n-1台随机置换装置进行随机置换，所以置换处理的次数成为$_{n-1}C_k+1$，能够比第一实施方式的秘密计算系统更高效地进行处理。

[0120] [第三实施方式]

[0121] 与秘密随机置换的输入为公开值的情况同样，在秘密随机置换的输出为公开值的情况下，也能够比第一实施方式更高效化。这是因为输出为公开值，所以在n-1小块进行了随机置换之后，向剩余的1小块发送秘密分散值，能够对复原后的公开值汇总而进行置换。

[0122] 设为在除了随机置换装置1_{p0}之外的n-1台随机置换装置1_{p1}，……，1_{pn-1}所具备的存储部18中，存储有与包含小块p_i的k小块的组ρ_i对应的置换数据π的子份额$\pi_{\rho i}$以及N×k个种子$s_{0,1}$，……，$s_{N-1,k}$。其中，N为$_{n-1}C_k$。与第一实施方式同样，不一定存储种子$s_{0,1}$，……，$s_{N-1,k}$。

[0123] 参照图5，按照实际进行的动作过程的顺序说明第三实施方式所涉及的秘密计算系统所执行的秘密计算方法的处理流程的一例。

[0124] 通过除了随机置换装置1_{p0}之外的n-1台随机置换装置1_{p1}，……，1_{pn-1}来执行步骤S10至S1b中判定为i≥N-1为止的处理。

[0125] 在步骤$S16_{p0}$中，随机置换装置1_{p0}所具备的事后变换部16将加法秘密分散值变换为公开值。变换的方法与第一实施方式的步骤S16同样。具体而言，对随机置换装置1_{p0}，最后执行了置换处理的k台随机置换装置$1_{\rho N-1}$发送加法秘密分散值$\langle a\rangle^{\rho N-1}{}_{pj}$(j=0，……，k-1)，随机置换装置$1_{p0}$所具备的事后变换部16对加法秘密分散值$\langle a\rangle^{\rho N-1}$进行复原。

[0126] 在步骤$S12_{p0}$中，随机置换装置1_{p0}所具备的单位置换部12生成随机的置换数据π，对复原后的公开值进行置换。置换的方法与以往的置换方法同样。

[0127] 像这样，在第三实施方式的秘密计算系统中，在通过n-1台随机置换装置进行了随机置换之后通过1台随机置换装置汇总而进行置换，所以置换处理的次数成为$_{n-1}C_k+1$，能够比第一实施方式的秘密计算系统更高效地进行处理。

[0128] [第四实施方式]

[0129] 第四实施方式是能够对本发明的秘密随机置换检测秘密计算中的篡改的实施方式。作为检测秘密计算中的篡改的秘密篡改检测方法，提出了下述参考文献3中记载的方法。在参考文献3中，在三个阶段中进行秘密计算中的篡改检测。在随机化阶段中，将分散值变换为能够进行合法性验证的随机化分散值。在计算阶段中，使用由semi-honest的运算构成的随机化分散值用的运算来执行期望的秘密计算。此时，一边收集为了在后续的合法性证明阶段中计算校验和所需的随机化分散值一边进行计算。在合法性证明阶段中，对在计算阶段中收集到的随机化分散值，一并计算校验和并进行合法性证明。若校验和合法则输出基于计算阶段的计算结果，若不合法则不输出计算结果而仅输出不合法的意旨。

[0130] 〔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-1maliciousモデル上秘密分散ベースマルチパーテイ計算の構成法”，SCIS2013、2013年

[0131] 但是，为了应用参考文献3中记载的方法，在秘密计算中执行的各运算需要是tamper-simulatable(参考文献4)。

[0132] 〔参考文献4〕D.Ikarashi，R.Kikuchi，K.Hamada，and K.Chida，“Actively Private and Correct MPC Scheme in t<n/2from Passively Secure Schemes with Small Overhead”，IACR Cryptology ePrint Archive，vol.2014，p.304，2014

[0133] 因此，在第四实施方式中，表示将参考文献3中记载的秘密篡改检测方法应用于第

一实施方式的秘密随机置换以满足上述的条件的结构例。另外，以下表示应用于第一实施方式的例子，但通过同样的想法，还能够应用于第二实施方式以及第三实施方式。

[0134] 参照图6，说明第四实施方式所涉及的随机置换装置2的结构例。随机置换装置2与上述的实施方式所涉及的随机置换装置1同样，包含事先变换部10、单位置换部12、再分散部14、事后变换部16以及存储部18，还包含随机化部20、单位变换部22以及合法性证明部24。

[0135] 参照图7，按照实际进行的动作过程的顺序说明第四实施方式所涉及的秘密计算系统所执行的秘密计算方法的处理流程的一例。

[0136] 在步骤S20中，k台随机置换装置$1_{\rho 0}$所具备的随机化部20将所存储着的(k,n)-秘密分散值$[a]_{pi}$变换为随机化分散值。在存储部18中存储有公开值a的情况下，在将公开值a变换为(k,n)-秘密分散值$[a]_{pi}$的基础上，变换为随机化分散值。随机化分散值是值$a\in R$的分散值$[a]_{pi}$、和值$a\in R$与随机数$r\in A$的结合值(積算値，integrated value)ar的分散值$[ar]_{pi}$的组($[a]_{pi}$,$[ar]_{pi}$)。在此，R是环，A是环R上的结合代数(結合多元環)。结合代数是结合的环，且具备与其兼容的某些域(体，field)上的线性空间的构造。结合代数也可以说在矢量空间中处理的值不是域而可以是环。随机化分散值的第0分量($[a]_{pi}$)也称为R分量，第1分量($[ar]_{pi}$)也称为A分量。

[0137] 在生成随机化分散值时使用的随机数在利用多个同一环上的秘密分散的情况下，将用于一方的秘密分散的分散值变换为用于另一方的秘密分散的分散值，从而进行生成以使随机数的值成为相同。在该形式变换中，也必须能够进行篡改检测或者不能进行篡改。例如，从复制型秘密分散(replicated secret sharing)变换为线性秘密分散(linear secret sharing)的不能篡改的方法被记载于上述参考文献2。

[0138] 在步骤S22中，k台随机置换装置$1_{\rho i}$所具备的单位变换部22将由单位置换部12置换后的加法秘密分散值$\langle\!\langle a\rangle\!\rangle^{\rho i}$变换为基于(k,n)-秘密分散的随机化分散值并积蓄在存储部18中。所积蓄的随机化分散值为了在后述的合法性证明部24中计算校验和而利用。随机化分散值的积蓄不一定在全部单位置换之后，也可以仅在一部分单位置换时进行。

[0139] 在步骤S24中，合法性证明部24执行关于全部秘密分散直至全部秘密计算结束为止进行待机的同步处理(SYNC)。若检测到关于全部秘密分散全部秘密计算结束，则使用在随机化部20中使用的随机数$r_0,\cdots\cdots,r_{J-1}$的分散值$[r_0],\cdots\cdots,[r_{J-1}]$来验证校验和$C_0,\cdots\cdots,C_{J-1}$，对作为秘密随机置换的结果而得到的(k,n)-秘密分散值或者公开值的合法性进行验证。对校验和$C_0,\cdots\cdots,C_{J-1}$进行验证的结果，判定为没有篡改的情况下将处理前进至步骤S16。在判断为有篡改的情况下输出表示该意旨的信息(例如，“⊥”等)。

[0140] 校验和的验证关于$j=0,\cdots\cdots,J-1$，计算对校验和C_j中包含的随机化分散值的R分量的总和乘以分散值$[r_j]$后的分散值$[\varphi_j]$、和校验和C_j中包含的随机化分散值的A分量的总和即分散值$[\psi_j]$，对减去了分散值$[\varphi_j]$和分散值$[\psi_j]$后的分散值$[\delta_j]=[\varphi_j]-[\psi_j]$进行复原，若值$\delta_0,\cdots\cdots,\delta_{J-1}$全部为0则判定为在秘密随机置换整体上没有篡改。若其中一个值δ_j为0以外，则判定为在秘密随机置换的其中一个运算中有篡改。

[0141] 在J个秘密分散之中存在同一环上的秘密分散的情况下，若尽可能汇总而进行合法性证明，则所公开的值的数目变少，所以能够更提高保密性。例如，在第α($\alpha=0,\cdots\cdots,J-1$)个秘密分散和第β($\beta=0,\cdots\cdots,J-1,\alpha\neq\beta$)个秘密分散为同一环上的秘密分散的情况下，

如以下那样进行合法性证明。首先，将根据校验和C_α如上述那样算出的分散值$[\varphi_\alpha]$、和根据校验和C_α如上述那样算出的分散值$[\psi_\alpha]$分别变换为第β个秘密分散。并且，对于减去了将变换后的分散值$[\varphi_\alpha]$与根据校验和C_β而同样算出的分散值$[\varphi_\beta]$相加的分散值$[\varphi_\alpha+\varphi_\beta]$、和将变换后的分散值$[\psi_\alpha]$与根据第β个校验和$C_\beta$而同样算出的分散值$[\psi_\beta]$相加的分散值$[\psi_\alpha+\psi_\beta]$后的分散值$[\delta]=([\varphi_\alpha]+[\varphi_\beta])-([\psi_\alpha]+[\psi_\beta])$进行复原，若复原值δ为0则判定为没有篡改，若复原值δ为0以外则判定为有篡改。这样，关于全部同一环上的秘密分散的组合进行验证，对在秘密随机置换整体上没有篡改的情况进行验证。在本方式中说明了2个秘密分散为同一环上的秘密分散的例子，但在3个以上的秘密分散为同一环上的秘密分散的情况下，也能够通过同样的方法进行合法性证明。

[0142] 在步骤S16中，事后变换部16将加法秘密分散值变换为(k,n)-秘密分散值或者公开值。在上述的实施方式中，构成为在输出为公开值的情况下，将进行了最后的置换处理后的加法秘密分散值$\langle\langle a\rangle\rangle^{\rho N-1}$发送给随机置换装置$1_p$，该随机置换装置$1_p$通过加法秘密分散的复原方法而得到公开值a。在本方式中，为了检测公开时的篡改，构成为在将加法秘密分散值暂时变换为(k,n)-秘密分散值的基础上，通过(k,n)-秘密分散的复原方法而得到公开值a。

[0143] 在根据(k,n)-秘密分散值而得到公开值时，需要基于能够进行篡改检测的公开方法。作为能够进行篡改检测的公开方法，存在上述参考文献4的appendix中记载的方法。或者，如以下那样进行公开从而能够进行篡改检测。

[0144] 随机置换装置1_p从任意k-1台随机置换装置接收对加法秘密分散值$\langle\langle a\rangle\rangle^{\rho N-1}$进行了形式变换的(k,n)-秘密分散值。此外，从剩余的n-k台随机置换装置接收对加法秘密分散值$\langle\langle a\rangle\rangle^{\rho N-1}$进行了形式变换的(k,n)-秘密分散值的Hash值等校验和。校验和也可以不是Hash值，还能够使用更安全的信息理论的校验和。信息理论的校验和例如将校验和的计算对象设为a_i，是随机数r和$a_i r^{i+1}$的组。随机置换装置1_p根据包括自身所具有的(k,n)-秘密分散值的k个(k,n)-秘密分散值来恢复n-k个(k,n)-秘密分散值，根据所恢复的各个(k,n)-秘密分散值来计算校验和。另外，恢复是在失去了一部分分散值时，根据能够利用的k个分散值来再构筑成为不能利用的n-k个分散值而不丧失保密性的方法。

[0145] 接下来，随机置换装置1_p确认从n-k台随机置换装置接收到的(k,n)-秘密分散值的校验和、和所恢复的(k,n)-秘密分散值的校验和是否一致。在全部校验和一致的情况下判定为没有篡改，输出(k,n)-秘密分散值或者公开值。在其中一个校验和不同的情况下判定为有篡改，输出表示该意旨的信息(例如，“⊥”等)。

[0146] 若如本方式那样构成，则在本发明的秘密随机置换中，能够进行篡改检测，安全性提高。

[0147] [结构例的组合]

[0148] 本发明除了上述的实施方式之外，通过四个独立的观点的组合，能够设为各种结构。

[0149] 第一个观点是输入输出型的观点。在该观点中，考虑四个结构方法。第一个结构是输入为线性秘密分散值且输出为线性秘密分散值的情况。第二个结构是输入为线性秘密分散值且输出为复制秘密分散值的情况，或者相反地输入为复制秘密分散值且输出为线性秘

密分散值的情况。第三个结构是输入为公开值且输出为秘密分散值的情况。第四个结构是输入为线性秘密分散值且输出为公开值的情况。

[0150] 第二个观点是随机数生成方法的观点。在该观点中，考虑两个结构方法。第一个结构是随机数为根据预先共享的种子而生成的伪随机数的情况。第二个结构是随机数在执行协议时共享的情况。

[0151] 第三个观点是随机置换的种类的观点。在该观点中，考虑两个结构方法。第一个结构是置换数据为任意的情况，想要完全随机地打乱(shuffle)的情况。第二个结构是置换数据被限制为轮转(rotation)的情况，也就是说置换数据以某$r\in N_m$来表现，成为$\pi(i)=i+r \bmod m$，想要保密绝对的位置但也可以不保密相对的排列顺序的情况。

[0152] 第四个观点是限定了k,n的反复置换的具体例的观点。第一个结构是k＝2,n＝3的结构。第二个结构是k＝3,n＝5的结构。在该观点中，考虑对各结构进一步加入了输入输出的观点的共六个具体例。

[0153] 第一个具体例是在k＝2,n＝3的结构中，输入输出都是秘密分散值的情况。参照图6，说明该具体例的反复置换。在图6中，纵轴表示小块，横轴表示单位置换的次数。圆形记号表示在单位置换中进行处理的小块。实线的箭头表示在再分散中被发送秘密分散值的小块的方向。虚线的箭头表示在再分散中同一小块继续保持秘密分散值。在图6的例子中，k小块组的顺序$P=(\rho_0,\rho_1,\rho_2)$被设定为$\rho_0=(p_0,p_1)$，$\rho_1=(p_1,p_2)$，$\rho_2=(p_0,p_2)$。在第一次单位置换中小块p_0,p_1进行处理，在第一次再分散中从小块p_0向小块p_2发送秘密分散值。在第二次单位置换中小块p_1,p_2进行处理，在第二次再分散中从小块p_1向小块p_0发送秘密分散值。在第三次单位置换中小块p_0,p_2进行处理，反复置换完成。

[0154] 第二个具体例是在k＝3,n＝5的结构中，输入输出都是秘密分散值的情况。参照图7，说明该具体例的反复置换。图的记法与图6同样。在图7的例子中，k小块组的顺序$P=(\rho_0,\cdots\cdots,\rho_9)$被设定为$\rho_0=(p_0,p_1,p_2)$，$\rho_1=(p_1,p_2,p_3)$，$\rho_2=(p_2,p_3,p_4)$，$\rho_3=(p_0,p_3,p_4)$，$\rho_4=(p_0,p_1,p_4)$，$\rho_5=(p_1,p_3,p_4)$，$\rho_6=(p_0,p_1,p_3)$，$\rho_7=(p_0,p_2,p_3)$，$\rho_8=(p_0,p_2,p_4)$，$\rho_9=(p_1,p_2,p_4)$。在第一次单位置换中小块$p_0$,$p_1$,$p_2$进行处理，在第一次再分散中从小块$p_0$向小块$p_3$发送秘密分散值。在第二次单位置换中小块$p_1$,$p_2$,$p_3$进行处理，在第二次再分散中从小块$p_1$向小块$p_4$发送秘密分散值。在第三次单位置换中小块$p_2$,$p_3$,$p_4$进行处理，在第三次再分散中从小块$p_2$向小块$p_0$发送秘密分散值。在第四次单位置换中小块$p_0$,$p_3$,$p_4$进行处理，在第四次再分散中从小块$p_3$向小块$p_1$发送秘密分散值。在此，从小块$p_3$向小块$p_1$发送的秘密分散值是在第一次再分散中从小块$p_0$向小块$p_3$发送的秘密分散值，因此在第五次再分散之前小块$p_1$发生接收等待。从而，至第四次再分散为止成为通信的第一级。以后，同样反复进行置换和再分散，从而在该具体例中反复置换以三级通信级数来完成。

[0155] 第三个具体例是在k＝2,n＝3的结构中，输入为公开值且输出为秘密分散值的情况。参照图8，说明该具体例的反复置换。图的记法与图6同样。在图8的例子中，k小块组的顺序$P=(\rho_0,\rho_1,\rho_2)$被设定为$\rho_0=\rho_1=(p_0)$，$\rho_2=(p_1,p_2)$。在第一次和第二次单位置换中仅小块p_0进行处理。该单位置换也可以单纯地反复两次，还能够汇总两次量的置换而进行。在第二次再分散中从小块p_0向小块p_1,p_2发送秘密分散值。在第三次单位置换中小块p_1,p_2进行处理，反复置换完成。

[0156] 第四个具体例是在k＝3,n＝5的结构中，输入为公开值且输出为秘密分散值的情

况。参照图9，说明该具体例的反复置换。图的记法与图6同样。在图9的例子中，k小块组的顺序 $P=(\rho_0,\cdots\cdots,\rho_9)$ 被设定为 $\rho_0=\rho_1=\rho_2=\rho_3=\rho_4=\rho_5=(p_0)$，$\rho_6=(p_2,p_3,p_4)$，$\rho_7=(p_1,p_3,p_4)$，$\rho_8=(p_1,p_2,p_4)$，$\rho_9=(p_1,p_2,p_3)$。在第一次至第六次单位置换中仅小块 p_0 进行处理。该单位置换也可以单纯地反复六次，还能够汇总六次量的置换而进行。在第六次再分散中从小块 p_0 向小块 p_2,p_3,p_4 发送秘密分散值。在第七次单位置换中小块 p_2,p_3,p_4 进行处理，在第七次再分散中从小块 p_2 向小块 p_1 发送秘密分散值。在第八次单位置换中小块 p_1,p_3,p_4 进行处理，在第八次再分散中从小块 p_3 向小块 p_2 发送秘密分散值。在第九次单位置换中小块 p_1,p_2,p_4 进行处理，在第九次再分散中从小块 p_4 向小块 p_3 发送秘密分散值。在第十次单位置换中小块 p_1,p_2,p_3 进行处理，反复置换完成。如图7所示，在该具体例中反复置换以二级通信级数来完成。

[0157] 第五个具体例是在 $k=2,n=3$ 的结构中，输入为秘密分散值且输出为公开值的情况。参照图10，说明该具体例的反复置换。图的记法与图6同样。在图10的例子中，k小块组的顺序 $P=(\rho_0,\rho_1,\rho_2)$ 被设定为 $\rho_0=(p_1,p_2)$，$\rho_1=\rho_2=(p_0)$。在第一次单位置换中小块 p_1,p_2 进行处理，从小块 p_1,p_2 向小块 p_0 发送秘密分散值。小块 p_0 进行秘密分散值的复原，进行第二次和第三次单位置换。该单位置换也可以单纯地反复两次，还能够汇总两次量的置换而进行。以上，反复置换完成。

[0158] 第六个具体例是在 $k=3,n=5$ 的结构中，输入为秘密分散值且输出为公开值的情况。参照图11，说明该具体例的反复置换。图的记法与图6同样。在图11的例子中，k小块组的顺序 $P=(\rho_0,\cdots\cdots,\rho_9)$ 被设定为 $\rho_0=(p_2,p_3,p_4)$，$\rho_1=(p_1,p_3,p_4)$，$\rho_2=(p_1,p_2,p_4)$，$\rho_3=(p_1,p_2,p_3)$，$\rho_4=\rho_5=\rho_6=\rho_7=\rho_8=\rho_9=(p_0)$。在第一次单位置换中小块 p_2,p_3,p_4 进行处理，在第一次再分散中从小块 p_2 向小块 p_1 发送秘密分散值。以后，通过小块 p_1,p_2,p_3,p_4 反复进行置换和再分散，在第 $N(={}_4C_3=4)$ 次置换完成后，从小块 p_1,p_2,p_3 向小块 p_0 发送秘密分散值。小块 p_0 进行秘密分散值的复原，进行第五次至第十次单位置换。该单位置换也可以单纯地反复六次，还能够汇总六次量的置换而进行。以上，反复置换完成。

[0159] 本发明不限定于上述的实施方式，能够在不脱离本发明的宗旨的范围内进行适当变更是不言而喻的。上述实施方式中说明的各种处理不仅按照记载的顺序而时序地执行，也可以根据执行处理的装置的处理能力或根据需要而并行或单独执行。

[0160] [程序、记录介质]

[0161] 在通过计算机实现在上述实施方式中说明的各装置中的各种处理功能的情况下，各装置应具有的功能的处理内容通过程序来记述。并且，通过由计算机来执行该程序，上述各装置中的各种处理功能在计算机上实现。

[0162] 记述了该处理内容的程序能够记录在能够由计算机读取的记录介质中。作为能够由计算机读取的记录介质，例如也可以是磁记录装置、光盘、光磁记录介质、半导体存储器等任意记录介质。

[0163] 此外，该程序的流通例如通过对记录了该程序的DVD、CD-ROM等可移动记录介质进行销售、转让、借出等来进行。进而，也可以设为通过将该程序储存在服务器计算机的存储装置中，经由网络，从服务器计算机向其他计算机转发该程序，从而使该程序流通的结构。

[0164] 执行这样的程序的计算机例如首先将在可移动记录介质中记录的程序或者从服务器计算机转发的程序暂时储存在自己的存储装置中。并且，在执行处理时，该计算机读取

在自己的记录介质中储存的程序，进行按照所读取到的程序的处理。此外，作为该程序的其他执行方式，也可以设为计算机从可移动记录介质直接读取程序，执行按照该程序的处理，进而也可以设为在每次从服务器计算机向该计算机转发程序时，逐次执行按照所接受到的程序的处理。此外，也可以设为通过不进行从服务器计算机向该计算机的程序的转发，而是仅通过其执行指示和结果取得来实现处理功能的所谓ASP(应用服务提供商(Application Service Provider))型的服务来执行上述的处理的结构。另外，设为在本方式中的程序中，包含供于电子计算机的处理用的信息并且是遵循程序的信息(不是对于计算机的直接的指令但具有规定计算机的处理的性质的数据等)的程序。

[0165] 此外，在本方式中，设为通过在计算机上执行规定的程序而构成本装置，但也可以将这些处理内容的至少一部分在硬件上实现。

秘密计算系统

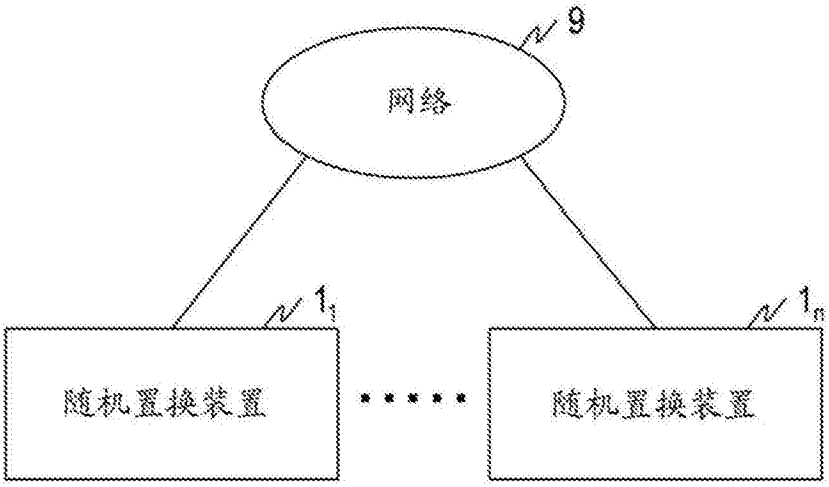

9
网络
1_1
1_n
随机置换装置
随机置换装置

图1

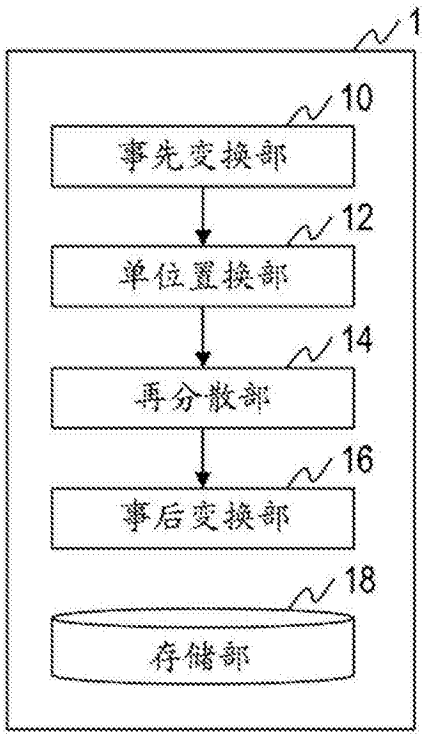

1
10
事先变换部
12
单位置换部
14
再分散部
16
事后变换部
18
存储部

图2

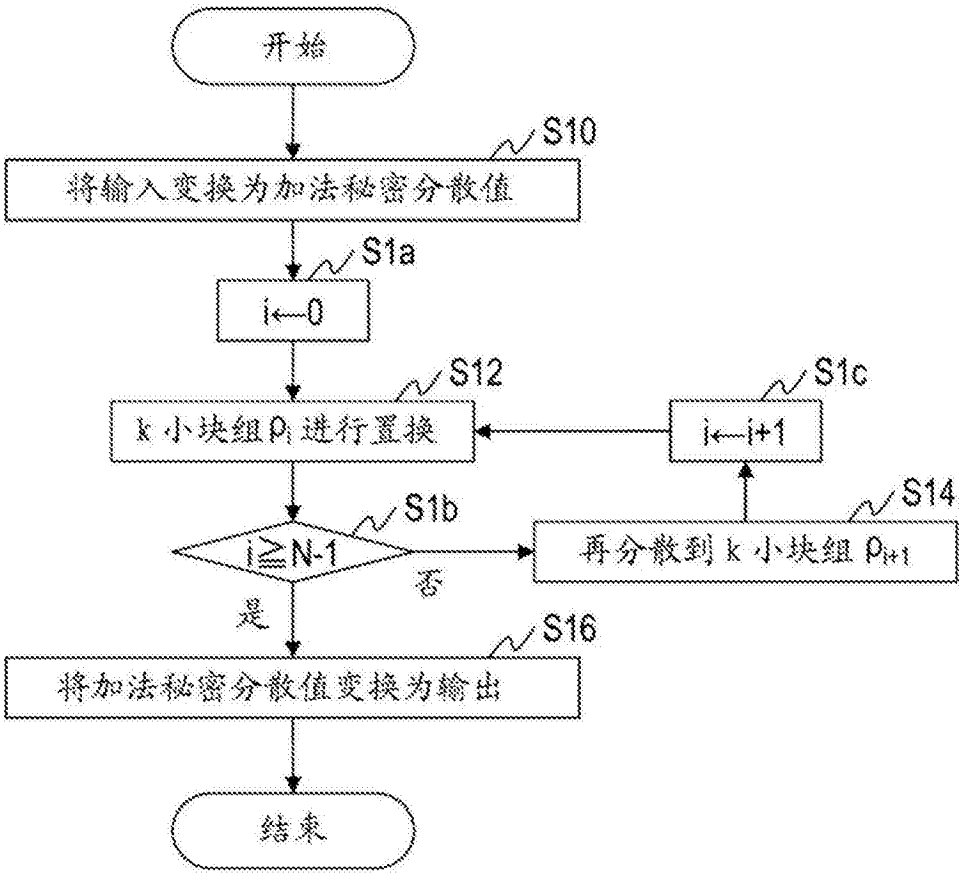

开始
S10
将输入变换为加法秘密分散值
S1a
i←0
S12
k 小块组 P_i 进行置换
S1c
i←i+1
S1b
i≧N-1
否
S14
再分散到 k 小块组 P_{i+1}
是
S16
将加法秘密分散值变换为输出
结束

图3

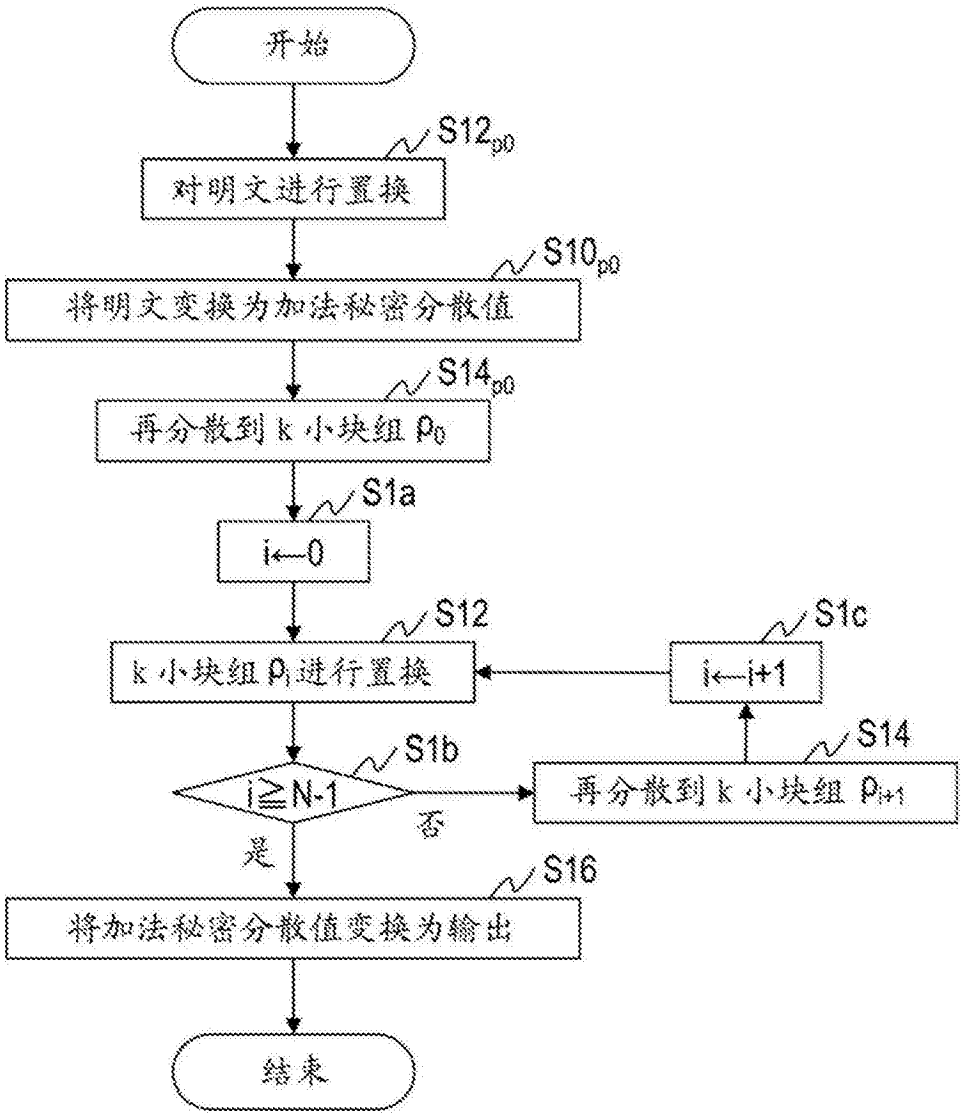

开始
S12p0
对明文进行置换
S10p0
将明文变换为加法秘密分散值
S14p0
再分散到 k 小块组 p0
S1a
i←0
S12
k 小块组 pi 进行置换
S1c
i←i+1
S1b
i≧N-1
否
S14
再分散到 k 小块组 pi+1
是
S16
将加法秘密分散值变换为输出
结束

图4

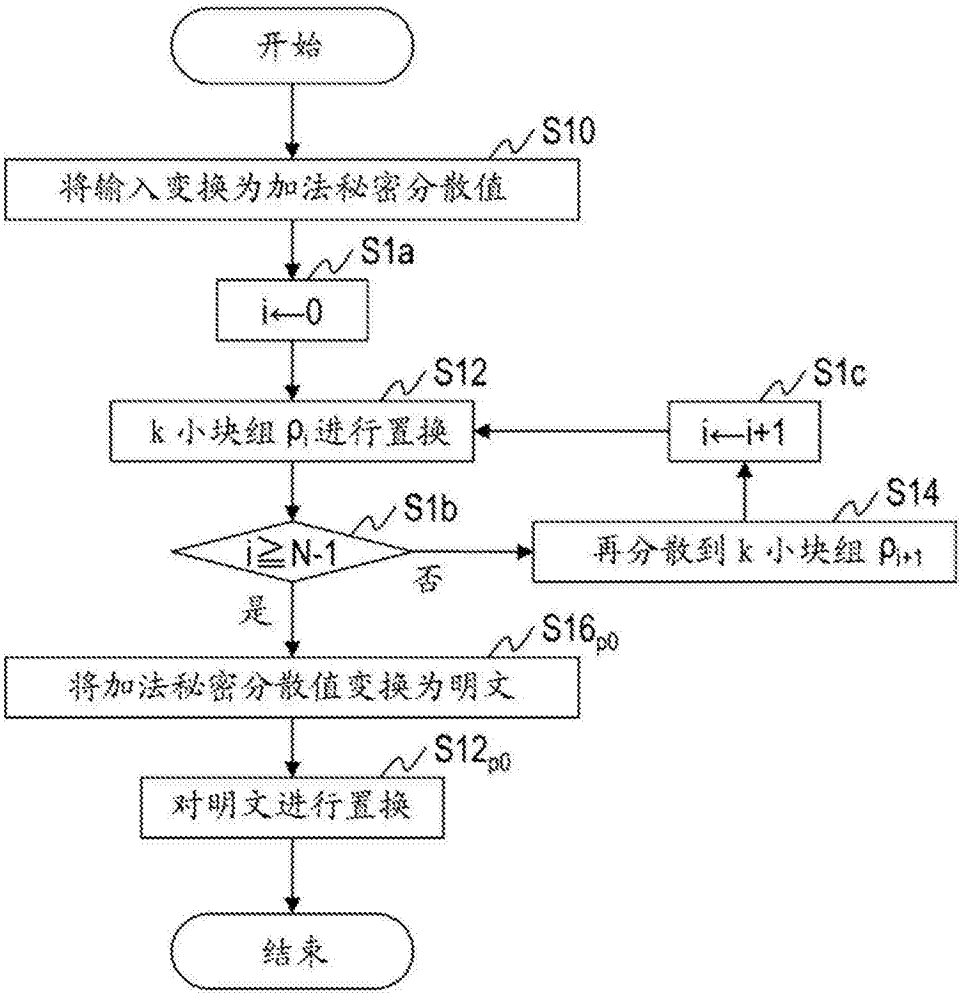

开始
S10
将输入变换为加法秘密分散值
S1a
i←0
S12
k 小块组 ρi 进行置换
S1c
i←i+1
S1b
i≧N-1
否
S14
再分散到 k 小块组 ρi+1
是
S16ρ0
将加法秘密分散值变换为明文
S12ρ0
对明文进行置换
结束

图5

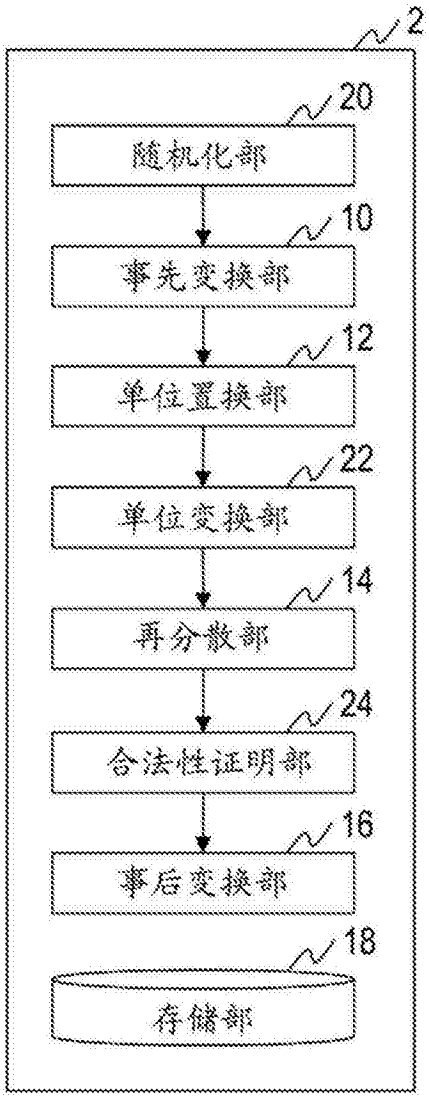

2
20
随机化部
10
事先变换部
12
单位置换部
22
单位变换部
14
再分散部
24
合法性证明部
16
事后变换部
18
存储部

图6

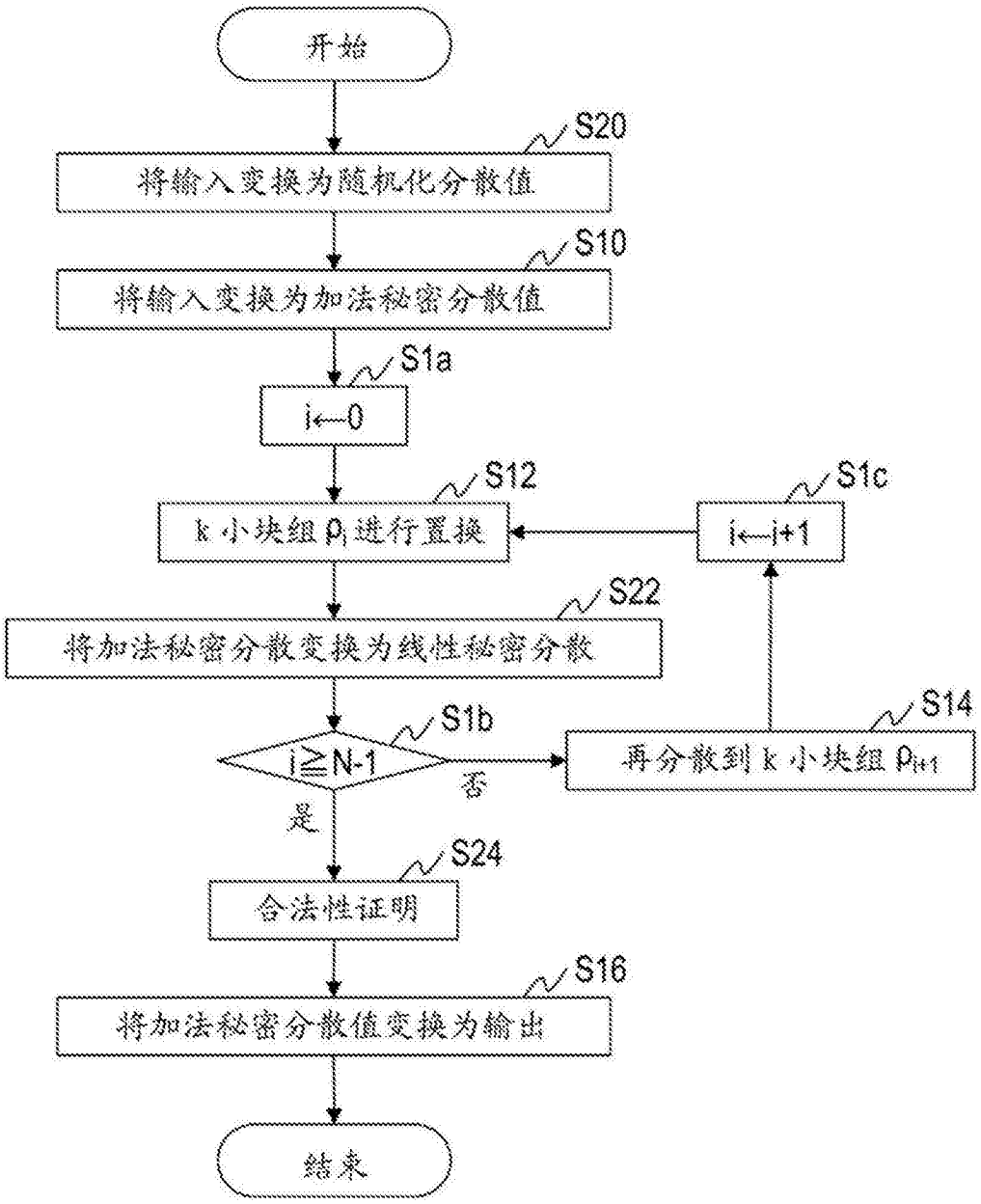

开始
S20
将输入变换为随机化分散值
S10
将输入变换为加法秘密分散值
S1a
i←0
S12
k小块组p_i进行置换
S1c
i←i+1
S22
将加法秘密分散变换为线性秘密分散
S1b
i≧N-1
否
S14
再分散到k小块组p_{i+1}
是
S24
合法性证明
S16
将加法秘密分散值变换为输出
结束

图7

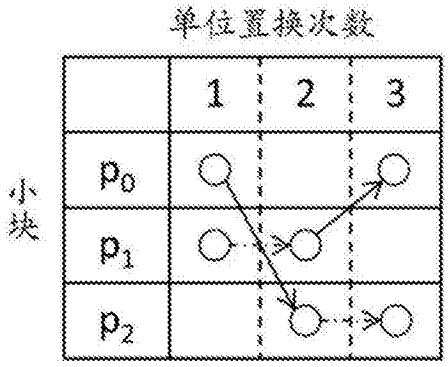

单位置换次数
1
2
3
小块
p_0
p_1
p_2

图8

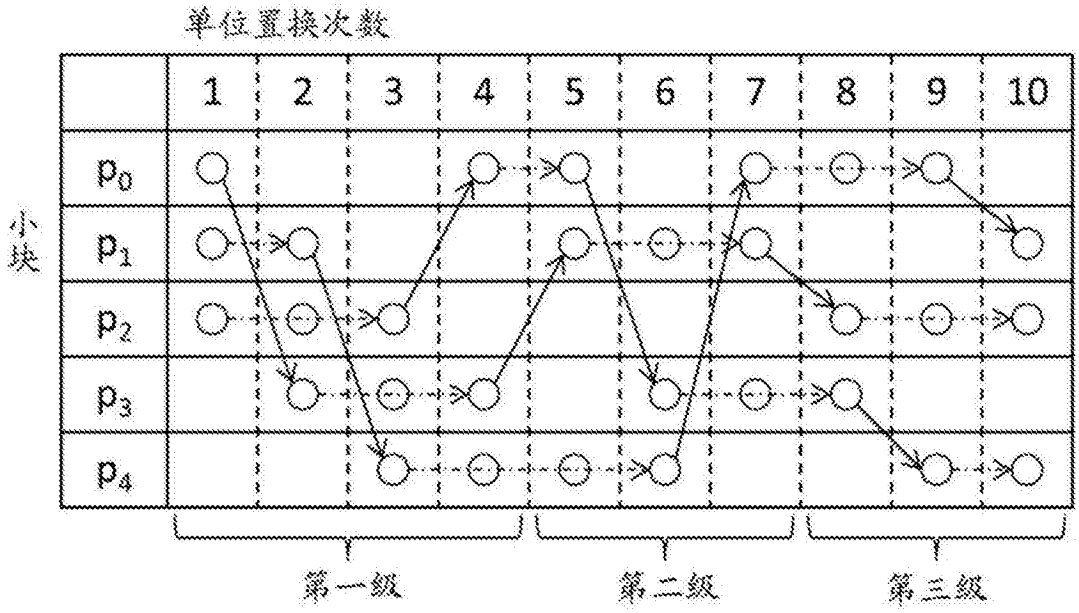

单位置换次数
1
2
3
4
5
6
7
8
9
10
小块
p_0
p_1
p_2
p_3
p_4
第一级
第二级
第三级

图9

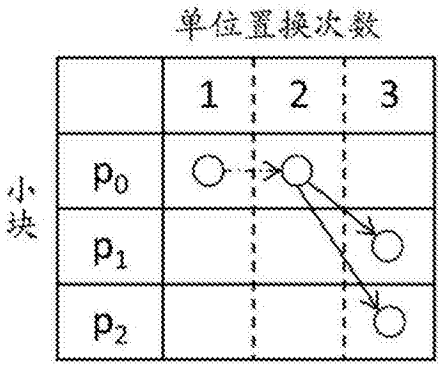

单位置换次数
1
2
3
小块
p_0
p_1
p_2

图10

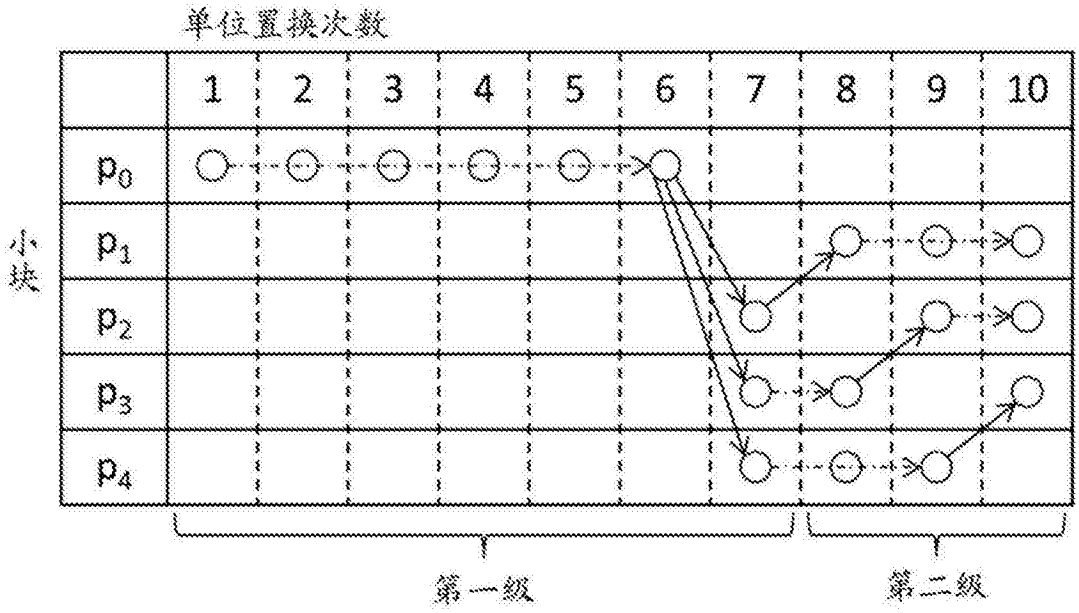

单位置换次数
1
2
3
4
5
6
7
8
9
10
小块
p_0
p_1
p_2
p_3
p_4
第一级
第二级

图11

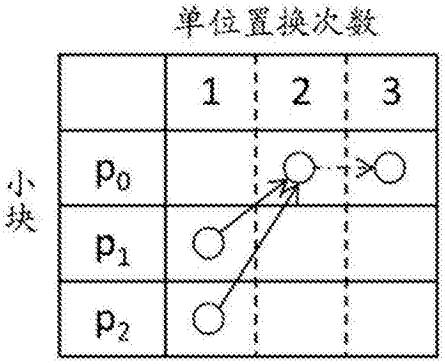

单位置换次数
1
2
3
小块
p_0
p_1
p_2

图12

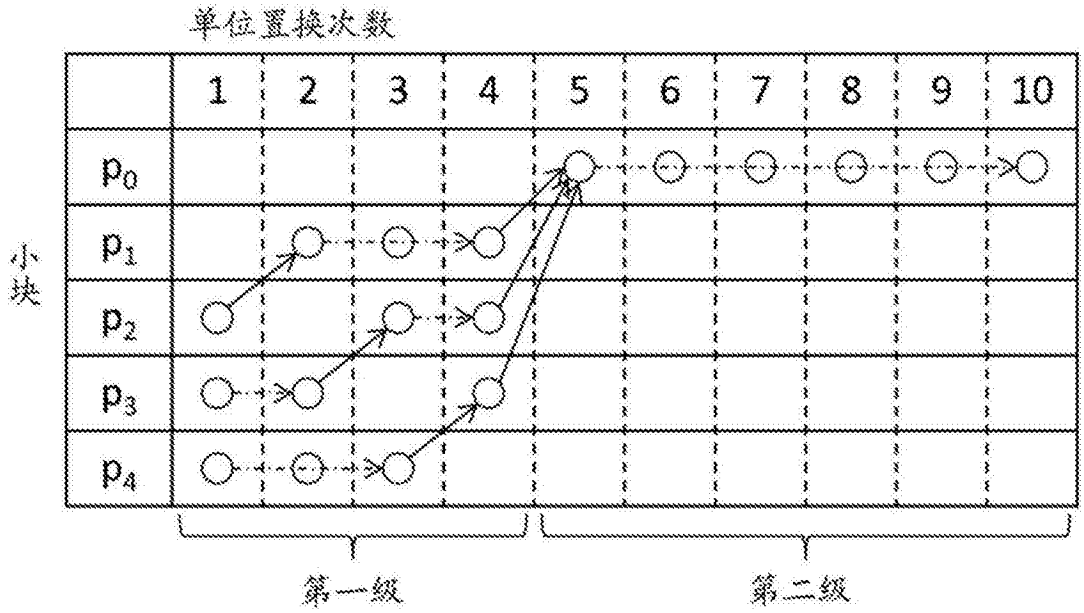


图13