(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114981860 B
(45)授权公告日 2025.06.27

(21)申请号 202080093276.2
(22)申请日 2020.01.20
(65)同一申请的已公布的文献号
申请公布号 CN 114981860 A
(43)申请公布日 2022.08.30
(85)PCT国际申请进入国家阶段日
2022.07.14
(86)PCT国际申请的申请数据
PCT/JP2020/001683 2020.01.20
(87)PCT国际申请的公布数据
WO2021/149106 JA 2021.07.29
(73)专利权人 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
(74)专利代理机构 北京市柳沈律师事务所 11105
专利代理师 金兰
(51)Int.Cl.
G09C 1/00(2006.01)
(56)对比文件
JP 2014164144 A,2014.09.08
US 2008240443 A1,2008.10.02
审查员 刘多纳

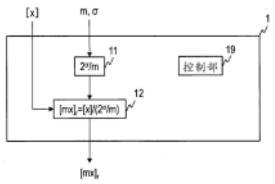
权利要求书1页 说明书7页 附图3页

(54)发明名称

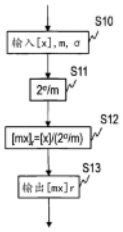
秘密计算装置、秘密计算方法、以及程序

(57)摘要

得到公开值$2^{\sigma}/m$,进行使用了秘密分散值[x]和所得到的所述公开值$2^{\sigma}/m$的公开值除法运算的秘密计算$[x]/(2^{\sigma}/m)$,得到使mx右移位了σ比特的值的秘密分散值$[mx]_r$并进行输出。其中,x为实数,[•]为•的秘密分散值,σ为表示右移位量的比特数的正整数,m为实数。



A



B

CN 114981860 B

1.一种秘密计算装置,其中,

x为实数,[•]为•的秘密分散值,σ为表示右移位量的比特数的正整数,m为实数,

所述秘密计算装置具有:

公开值计算部,得到公开值$2^{\sigma}/m$;以及

秘密计算部,进行使用了秘密分散值[x]和通过所述公开值计算部得到的所述公开值$2^{\sigma}/m$的公开值除法运算的秘密计算[x]/($2^{\sigma}/m$),得到使mx右移位了σ比特的值的秘密分散值$[mx]_r$并进行输出,

所述σ的值基于所述秘密计算装置的处理器能够处理的比特数而被确定。

2.一种秘密计算方法,其中,

x为实数,[•]为•的秘密分散值,σ为表示右移位量的比特数的正整数,m为实数,

所述秘密计算方法具有:

公开值计算步骤,公开值计算部得到公开值$2^{\sigma}/m$;以及

秘密计算步骤,秘密计算部进行使用了秘密分散值[x]和通过所述公开值计算部得到的所述公开值$2^{\sigma}/m$的公开值除法运算的秘密计算[x]/($2^{\sigma}/m$),得到使mx右移位了σ比特的值的秘密分散值$[mx]_r$并进行输出,

所述σ的值基于处理器能够处理的比特数而被确定。

3.一种计算机程序产品,其包括使计算机发挥作为权利要求1的秘密计算装置的功能的计算机程序。

秘密计算装置、秘密计算方法、以及程序

技术领域

[0001] 本发明涉及在秘密计算中进行实数值的乘法运算的技术。

背景技术

[0002] 在非专利文献1中,公开了一种将公开的实数值与秘密分散值进行乘法运算的秘密计算方法。

[0003] 现有技术文献

[0004] 非专利文献

[0005] 非专利文献1:五十岚大,“面向秘密计算AI的安装的秘密实数运算群的设计和安装-O(|p|)比特通信量O(1)圆的面向实数的右移位,”(五十嵐大,“秘密計算AIの実装に向けた秘密実数演算群の設計と実装-O(|p|)ビット通信量O(1)ラウンドの実数向け右シフト,”)In CSS2019,2019.

发明内容

[0006] 发明要解决的课题

[0007] 然而,非专利文献1的秘密计算方法中,为使不溢出而每当在乘法运算时在乘法运算的基础上还通过秘密计算进行右移位,存在计算成本大这一问题点。

[0008] 本发明鉴于这样的点而作出的,其目的在于削减将公开的实数值与秘密分散值进行乘法运算的秘密计算的计算成本。

[0009] 用于解决课题的手段

[0010] X为实数,[•]为•的秘密分散值,σ为表示右移位量的比特数的正整数,m为实数,得到公开值$2^{\sigma}/m$,进行使用了秘密分散值[x]和所得到的所述公开值$2^{\sigma}/m$的公开值除法运算的秘密计算[x]/($2^{\sigma}/m$),得到使mx右移位了σ比特的值的秘密分散值$[mx]_r$并进行输出。

[0011] 发明效果

[0012] 如上,在本发明中同时执行实数m的乘法运算和σ比特的右移位,因此能够削减计算成本。

附图说明

[0013] 图1A是示出实施方式的秘密计算装置的框图。

[0014] 图1B是用于示出实施方式的秘密计算方法的流程图。

[0015] 图2是示出与各初等函数有关的计算完成的参数的表。

[0016] 图3是用于说明硬件结构的框图。

具体实施方式

[0017] 以下,参考附图说明本发明的实施方式。

[0018] 在实施方式中,秘密计算装置将实数x的秘密分散值[x]、作为乘数的实数m、以及

表示右移位量的比特数的正整数σ作为输入,得到使mx右移位了σ比特的值的秘密分散值$[mx]_r$并进行输出。不限制秘密分散值的秘密分散方式(秘钥分享方式,secret sharing scheme),例如,能举例出加法秘密分散方式(additive secret sharing scheme)、Shamir秘密分散方式等。[•]的一例是将剩余环上的元素•进行线形秘密分散的秘密分散值(分享(share))。此外,能够为环上的整数选定了公开的小数点位置,从而视为固定小数点的实数。在实施方式中,将这样在环上表示的固定小数点的实数简记为实数。

[0019] 如图1A所示出,实施方式的秘密计算装置1具有公开值计算部11、秘密计算部12、以及控制部19。秘密计算装置1在控制部19的控制之下执行各处理。

[0020] 如图1B所示出,首先,秘密分散值[x]、实数m、以及正整数σ被输入到秘密计算装置1(步骤S10)。秘密分散值[x]被发送到秘密计算部12,实数m以及正整数σ被发送到公开值计算部11。

[0021] 实数m以及正整数σ被输入到公开值计算部11。公开值计算部11计算公开值$2^\sigma/m$并进行输出(步骤S11)。

[0022] 秘密分散值[x]以及从公开值计算部11输出的公开值$2^\sigma/m$被输入到秘密计算部12。秘密计算部12进行使用了秘密分散值[x]和由公开值计算部11得到的公开值$2^\sigma/m$的公开值除法运算的秘密计算$[x]/(2^\sigma/m)$,得到使mx右移位了σ比特的值的秘密分散值$[mx]_r$并进行输出(步骤S12)。

[0023] 秘密计算装置1输出秘密分散值$[mx]_r$(步骤S13)。

[0024] <本实施方式的特征>

[0025] 通常,在秘密计算中,在对秘密分散值[x]进行被公开的实数m的乘法运算和σ比特的右移位的情况下,变为先进行乘法运算再进行右移位或是先进行右移位再进行乘法运算的情况。在这种情况下,用于进行乘法运算的计算成本和用于进行右移位的计算成本成为必要。对此,在本实施方式中,着眼于右移位与除法运算等价这一点,首先,计算公开值$2^\sigma/m$,然后进行使用了秘密分散值[x]和得到的公开值$2^\sigma/m$的公开值除法运算的秘密计算$[x]/(2^\sigma/m)$。该秘密计算所得到的值与将乘法运算结果mx右移位了σ比特的值的秘密分散值$[mx]_r$是等价的。然而,通过低计算成本的公开值除法运算的秘密计算来同时实现乘法运算和右移位。其结果为,能大幅削减运算成本。秘密计算领域的本领域技术人员认识到除法运算是与乘法运算相比运算成本更大的处理,无法想到在乘法运算的处理中使用除法运算。然而,在本实施方式中,着眼于右移位与除法运算等价这一点而计算公开值$2^\sigma/m$,通过进行公开值除法运算的秘密计算$[x]/(2^\sigma/m)$,与分别进行乘法运算和右移位的情况相比,能够得到可以削减计算成本这一无法预测的显著效果。另外,溢出是基于安装了秘密计算的处理器的性能的问题,本方式提供用于解决基于该硬件上的制约的问题的手法。这样,本方式并非解决纯粹数学上的问题,而是解决硬件安装上的问题的、具有技术性特征的。表示右移位量的σ的值基于能用处理器来处理的比特数而确定。即,公开值$2^\sigma/m$是从硬件上的要求而确定的值。

[0026] [安装例]

[0027] 以下示出能够安装上述的方式的算法。

[0028] <实施例1>

[0029] 在实施例1中,基于条件$c\in\{0,1\}$而将2个公开值m_0、m_1中的某一个公开值乘以实数

x的秘密分散值[x]。若公开值m_0、m_1的大小较大,则乘法运算后的值的有效比特数(将该数以2进制来表达的而必要的比特数)上升,导致成为无法再次乘法运算的数,因此存在有右移位的必要的情况。在实施例1中,使这样的处理高效化。

[0030] 输入:[x],乘数m_0,m_1,条件c∈{0,1}的秘密分散值[c]

[0031] 输出:[m_0x]if(如果)c=0,[m_1x]if c=1

[0032] 秘密计算装置通过使用了秘密分散值[x]以及乘数m_0、m_1、以及模p的秘密计算来得到秘密分散值[m_0x]以及[m_1x]并进行输出(步骤S21)。关于步骤S21的处理的具体例将在后面叙述。

[0033] 秘密计算装置通过使用了秘密分散值[c]、[m_0x]、[m_1x]的秘密计算,得到m_cx的秘密分散值[c?m_0x:m_1x]并进行输出。即,秘密计算部22在c=0的情况下得到[m_0x]并进行输出,在c=1的情况下得到[m_1x]并进行输出(步骤S22)。

[0034] <步骤S21的处理的具体例>

[0035] 对步骤S21的处理的具体例进行说明。在这里,$d_0=1/m_0$以及$d_1=1/m_1$为除数,p为正整数的模,q为正整数的商。

[0036] 秘密计算装置通过使用了秘密分散值[x]以及模p的秘密计算,得到x/p的商q的秘密分散值[q]并进行输出(步骤S211)。

[0037] 秘密计算装置通过使用了秘密分散值[x]、[q]、除数$d_0,\cdots,d_{n-1}$以及模p的秘密计算,得到[m_0x]=[x/d_0]=[(x+qp)/d_0]-[q]p/d_0、[m_1x]=[x/d_1]=[(x+qp)/d_1]-[q]p/d_1并进行输出(步骤S212)。以下说明步骤S212的处理的具体例。

[0038] <步骤S212的处理的具体例>

[0039] 秘密计算装置的公开值计算部212a使用乘数m_0、m_1以及正整数σ0、σ1得到公开值$2^{\sigma0}/m_0$、$2^{\sigma1}/m_1$并进行输出。其中,σ0、σ1分别为表示在乘数m_0、m_1较大的情况下所需的右移位量的比特数的正整数(步骤S212a)。

[0040] 秘密计算装置进行使用了秘密分散值[x]、[q]以及模p和通过公开值计算部212a得到的公开值$2^{\sigma0}/m_0$、$2^{\sigma1}/m_1$的公开值除法运算的秘密计算[x+qp]/($2^{\sigma0}/m_0$)、[x+qp]/($2^{\sigma1}/m_1$),得到将(x+qp)m_0右移位了σ0比特的值的秘密分散值[(x+qp)m_0]以及将(x+qp)m_1右移位了σ1比特的值的秘密分散值[(x+qp)m_1]并进行输出(步骤S212b)。

[0041] 秘密计算装置通过使用了秘密分散值[(x+qp)m_0]、[(x+qp)m_1]、[q]和模p和乘数m_0、m_1的秘密计算来得到[m_0x]=[(x+qp)m_0]-[q]pm_0以及[m_1x]=[(x+qp)m_1]-[q]pm_1并进行输出(步骤S212c)。

[0042] <实施例2>

[0043] 在实施例2中,对任意的函数(例如初等函数)以多项式函数$f_t(x)$来进行近似,进一步地计算右移位前的函数$f_t(x)$和该函数$f_t(x)$的近似函数$f'_u(x)$的差分$f_t(x)-f'_t(x)$的秘密分散值$[f_t(x)-f'_t(x)]$,得到对$f_t(x)-f'_t(x)$进行右移位后的$(f_t(x)-f'_t(x))_r$的秘密分散值$[f_t(x)-f'_t(x)]_r$,通过秘密分散值$[f_t(x)-f'_t(x)]_r$和秘密分散值$[f'_t(x)]$的秘密计算,来得到将$f_t(x)-f'_t(x)$与$f'_t(x)$加法运算后的函数$f_t(x)$的秘密分散值$[f_t(x)]$。其中,x为实数,[•]为•的秘密分散值,n为1以上的整数(例如,n为2以上的整数),t=0,…,n-1,u=1,…,n-1,$f_t(x)$为对于实数x的函数,$f'_t(x)$为函数$f_t(x)$的近似函数,近似函数$f'_0(x)$的秘密分散值$[f'_0(x)]$为$[f'_0(x)]=c_{0,0}+c_{0,1}[x]$,近似函数$f'_u(x)$的秘密分散值$[f'_u(x)]$为

$[f'_u(x)]=c_{u,0}+c_{u,1}[x]+c_{u,2}[f_0(x)]+\cdots+[f_{u-1}(x)]$，$c_{t,0}$为公开值，$c_{t,1},\cdots,c_{t,n+1}$为系数。其中，$c_{t,1},\cdots,c_{t,n+1}$为有效比特数的小的值，$c_{t,1},\cdots,c_{t,n+1}$是即使被相乘也不会由于数字溢出(overflow)而需要移位的值。$f_t(x)-f'_t(x)$为正。对秘密分散方式没有限定，例如，能示例出加法秘密分散方式、Shamir秘密分散方式等。这里，由于$f_t(x)-f'_t(x)$的大比$f_t(x)$的大小还小，因此能够抑制秘密分散值$[f_t(x)-f'_t(x)]$的溢出。此外，由于计算右移位前的函数$f_t(x)$和该函数$f_t(x)$的近似函数$f'_u(x)$的差分$f_t(x)-f'_t(x)$的秘密分散值$[f_t(x)-f'_t(x)]$，因此能保持高精度。溢出是基于安装了秘密计算的处理器的性能的问题，本方式提供用于解决基于该硬件上的制约的问题的手法。这样，本方式并非解决纯粹数学上的问题，而是解决硬件安装上的问题的、具有技术性特征的。例如，若计算秘密分散值$[f_t(x)]$则会溢出但秘密分散值$[f_t(x)-f'_t(x)]$的计算则不会溢出的处理器的该技术特征很显著。

[0044] 秘密计算装置将实数x的秘密分散值$[x]\in[L,R)$作为输入，进行以下的秘密计算来输出目的函数$f_{n-1}(x)$的秘密分散值$[f_{n-1}(x)]$。另外，L、R是满足$L<R$的实数，$[L,R)$表示L以上且小于R的左闭右开区间。在这里，说明了以下情况的例子，即：$n=3$，a、b、c、d、f、g、h、i、j、k、s、m、n、o、p、q、α、β、γ、δ、ζ为实数，$f_0(x)=y=\delta x^2+ax$，$f_1(x)=z=y(\zeta y+b)+cx$，$f_2(x)=w=\gamma(z(\alpha z+d)+y(\beta x+f)+gx)$，$f'_0(x)=ix+j$，$f'_1(x)=ky+sx+m$，$f'_2(x)=nz+oy+px+q$。

[0045] 输入：$[x]\in[L,R)$

[0046] 设定完成的参数：a,b,c,d,f,g,H,i,j,k,s,m,n,o,p,q,α,β,γ,δ,ζ

[0047] 输出：与目的函数(例如初等函数)$f_{n-1}(x)$所对应的秘密分散值$[f_{n-1}(x)]$

[0048] 1：秘密计算装置通过乘积和(sum of products)的秘密计算得到$[y']=[x(\delta x+a-i)-j]$，通过右移位的秘密计算得到降低了小数点位置的y'_r的秘密分散值$[y']_r$。

[0049] 2：秘密计算装置通过使用了秘密分散值$[y']_r$的秘密计算来得到$[y]=[y'+(ix+j)]$。

[0050] 3：秘密计算装置通过乘积和的秘密计算得到$[z']=[y(\zeta y+b-k)+(c-s)x-m]$，通过右移位得到降低了小数点位置的$z'_r$的秘密分散值$[z']_r$。

[0051] 4：秘密计算装置通过使用了秘密分散值$[z']_r$的秘密计算来得到$[z]=[z'+(ky+sx+m)]$。

[0052] 5：秘密计算装置通过乘积和的秘密计算得到$[w'/\gamma]=[z(\alpha z+d-n/\gamma)+(\beta x+f-o/\gamma)y+(g-p)x+(H-q)/\gamma]$，进行设了$[x]=[w'/\gamma]$且$m=\gamma$的步骤S10～S13的处理，同时进行基于$\gamma$的乘法运算和小数点位置的下降来得到$[w']$。

[0053] 6：秘密计算装置通过秘密计算来得到并输出$[w]=[w'+(nz+oy+px+q)]$。

[0054] <实施例3>

[0055] 在实施例3中，得到实数x的秘密分散值[x]的指数函数值exp(x)的秘密分散值。由于指数函数的输入存在加法性(additivity)，因此输入被分解为以下的3个部分。

[0056] I.被设想的输入的最小值μ

[0057] II.$x-\mu$的小数点以下t比特以上的上位u比特$x_0,\cdots,x_{u-1}$

[0058] III.表示比$x-\mu$的x_0更下位的全部比特的数x_ρ

[0059] 设$\exp x=\exp\mu\exp 2^{-t}x_0,\cdots,\exp 2^{u-t-1}x_{u-1}\exp x_\rho$。$\exp\mu$为公开值，$\exp 2^{-t}x_0,\cdots,\exp 2^{u-t-1}x_{u-1}$是通过表而计算的位置。$\exp x_\rho$是通过近似而计算的位置，被$[0,2^{-t})$所归一化。

[0060] 输入:[x]

[0061] 输出:[exp(x)]

[0062] 设定完成的参数:t＝-1

[0063] 1:秘密计算装置通过秘密计算得到[x']＝[x]-μ。其中,μ为被设想的x的最小值。

[0064] 2:秘密计算装置通过秘密计算,将比小数点以下t比特更上位的比特通过比特分解而取出并进行mod p变换,得到[x'_0],…,[x'_{u-1}]。

[0065] 3:秘密计算装置通过秘密计算,在各0≤i<u中,将f_i,ε_i分别设为$\exp(2^{i-t})$的尾数部、指数部。

[0066] 4:秘密计算装置通过秘密计算,关于i＝0,…,u-1,若x'_i＝0则设F_i＝1,若x'_i＝1则设F_i＝f_i,得到

[0067] [数1]

[0068] $$[f'] = \left[\prod_{0 \le i \le u-1} F_i \right]$$

[0069] 5:秘密计算装置通过秘密计算,在各0≤i<u中,通过选项公开的if-then-else门(gate)来计算[ε'_i]:＝if[x'_i]then $2^{\varepsilon i}$ else 1。

[0070] 6:秘密计算装置通过秘密计算,得到与各i有关的[ε'_i]的积[ε'](ε'＝$\varepsilon'_0 \cdots \varepsilon'_{u-1}$)。这是exp(x')的上位比特部分的指数部的2的幂数值。

[0071] 7:秘密计算装置通过秘密计算得到如下数学式。

[0072] [数2]

[0073] $$[x'_\rho] = [x'] - \sum_{i<u} 2^{i-t}[x'_i]$$

[0074] 这是表示exp(x')的下位比特部分的数。

[0075] 8:秘密计算装置通过秘密计算,从[x'_ρ]得到[w]。其中,w是对x'_ρ的指数函数exp x_ρ进行近似的多项式。例如,秘密计算装置使用设x＝x'_ρ的实施例2的方法来得到[w]。

[0076] 9:秘密计算装置通过秘密计算,得到[w][f'][ε']exp(μ)并进行输出。其中,在exp(μ)的乘法运算中,进行设[x]＝[w][f'][ε']且m＝exp(μ)的步骤S10～S13的处理,同时进行基于exp(μ)的乘法运算和小数点位置的下降并得到[w][f'][ε']exp(μ)。

[0077] [与各初等函数有关的计算完成的参数的例]

[0078] 图2示出初等函数为倒数函数、平方根函数、平方根的倒数函数、指数函数、对数函数的情况下的计算完成的参数。另外,ex、ey、ez分别表示x、y、z的小数点位置。此外,e'x、e'y、e'z分别表示右移位前的x'、y'、z'的小数点位置。这些小数点位置表示从下位比特起计的小数点位置的比特位置。表示该比特位置的值从0开始,从下位比特起计第e1比特表示1时,小数点位置记为e1。

[0079] [硬件结构]

[0080] 实施方式中的秘密计算装置1是例如通过包括CPU(central processing unit,中央处理单元)等的处理器(硬件处理器)以及RAM(random-access memory,随机存取存储器)、ROM(read-only memory,只读存储器)等的存储器的通用或专用计算机来执行规定程序而构成的装置。该计算机可以具备一个处理器和存储器,也可以具备多个处理器和存储

器。该程序可以安装在计算机中,也可以预先记录在ROM等中。此外,也可以使用无需使用程序即可实现处理功能的电子电路来构成部分或全部处理部,而不是通过CPU之类的读取程序来实现功能结构的电子电路(circuitry)。此外,构成一个装置的电子电路也可以包括多个CPU。

[0081] 图3示出实施方式中的秘密计算装置1的硬件结构的框图。如图3所示出,该例的秘密计算装置1具有CPU(Central Processing Unit,中央处理器)10a、输入部10b、输出部10c、RAM(Random Access Memory,随机存取储存器)10d、ROM(Read Only Memory,只读存储器)10e、辅助存储装置10f以及总线10g。该例的CPU10a具有控制部10aa、运算部10ab以及寄存器10ac,依据被寄存器10ac加载的各种程序而执行各种各样的运算处理。此外,输出部10c为数据被输出的输出端子、显示器等、由加载了规定的程序的CPU10a所控制的LAN卡等。此外,RAM10d为SRAM(Static Random Access Memory,静态随机存取存储器)、DRAM(Dynamic Random Access Memory,动态随机存取存储器)等,具有存储规定的程序的程序区域10da以及存储各种数据的数据区域10db。此外,辅助存储装置10f为例如硬盘、MO(Magneto-Optical disc,磁光盘)、半导体存储器等,具有存储规定的程序的程序区域10fa以及存储各种数据的数据区域10fb。此外,总线10g以信息可交互的形式连接到CPU10a、输入部10b、输出部10c、RAM10d、ROM10e以及辅助存储装置10f。CPU10a依据被加载的OS(Operating System,操作系统)程序,将存储于辅助存储装置10f的程序区域10fa的程序写入RAM10d的程序区域10da。同样地CPU10a将存储于辅助存储装置10f的数据区域10fb的各种数据写入RAM10d的数据区域10db。并且,被写入了该程序、数据的RAM10d上的地址被存储到CPU10a的寄存器10ac。CPU10a的控制部10ab依次读取被存储到寄存器10ac的这些地址,从被读取的地址所表示的RAM10d上的区域读取程序、数据,让运算部10ab依次执行该程序表示的运算,将该运算结果存储到寄存器10ac。通过这样的结构实现图1A所示出的秘密计算装置1的功能结构。

[0082] 上述的程序能够预先记录在计算机可读取的记录介质中。计算机可读取的记录介质的例为非临时性(non-transitory)记录介质。这样的记录介质的例为磁记录装置、光盘、光磁记录介质、半导体存储器等。

[0083] 该程序的流通,例如,通过对记录了该程序的DVD、CD-ROM等可移动型记录介质进行贩卖、转让、租赁等来进行。进一步,也可以是,将该程序存储到服务器计算机的存储装置,并经由网络将该程序从服务器计算机转送到其他的计算机从而使该程序流通的结构。如上述,执行这样的程序的计算机,例如,首先将在可移动性记录介质中记录的程序或从服务器计算机转送的程序临时存储到自身的存储装置。然后,在执行处理时,该计算机读取在自身的存储介质中存储的程序,并执行按照所读取的程序的处理。此外,作为该程序的其他的实施方式,也可以是由计算机从可移动性记录介质直接读取程序,并执行按照该程序的处理,进一步也可以是,每当从服务器计算机对该计算机转送程序时,依次执行按照所获得的程序的处理。此外,也可以是,不从服务器计算机对该计算机转送程序,而是仅通过该执行指示与结果取得来实现处理功能的结构,即通过所谓的ASP(Application Service Provider,应用服务提供商)型的服务来执行上述的处理的结构。另外,假设在本方式的程序中包含用于电子计算机的处理的信息且在程序中参照的信息(虽然不是对于计算机的直接的指令,但是具有规定计算机的处理的性质的数据等)。

[0084] 在各实施方式中,设为通过在计算机上执行规定的程序而构成本装置,但也可以设为通过硬件来实现这些处理内容的至少一部分。

[0085] 另外,本发明并不限定于上述的实施方式。例如,上述的各种处理不仅限于依据记载而以时序执行,也可以基于执行处理的装置的处理能力或应于必要而并列或个别地执行。此外,不用说也可以在不脱离本发明的目的的范围内适当变更。

[0086] 工业上的可利用性

[0087] 本发明例如能够在将数据秘匿化并在秘密计算中进行的机械学习、数据挖掘中的实数值的乘法运算中使用。

[0088] 标号说明

[0089] 1秘密计算装置

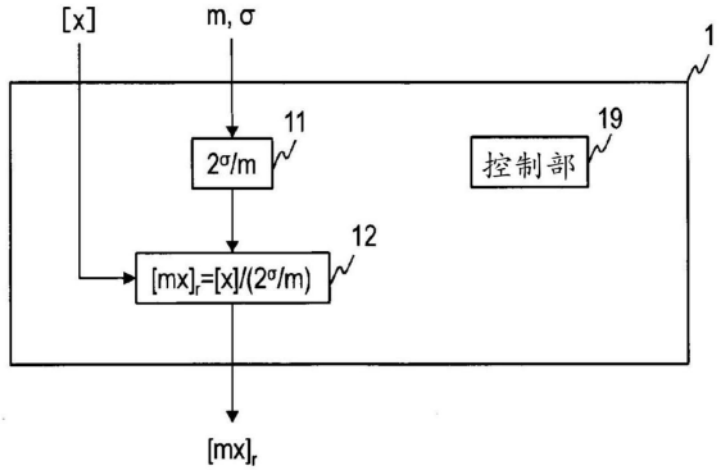

[x]
m, σ
1
11
2σ/m
19
控制部
12
[mx]r=[x]/(2σ/m)
[mx]r

图1A

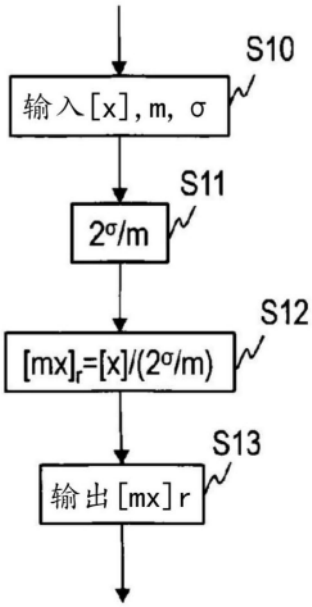

S10
输入[x], m, σ
S11
2σ/m
S12
[mx]r=[x]/(2σ/m)
S13
输出[mx]r

图1B

参数	倒数	平方根	平方根的倒数	指数	对数
L	0.75	1	0.5	0	2
R	1.125	2	1	2	4
a	-2.11046439323928	-0.4281414400291061	-1.696628555353	0.01502453639091 33	-0.8466962731211 07
b	2.43496077969272	0.4101200798768 74	1.5495740937688	0.4098527753215 8	0.7847029513335 29
c	-0.18413217288124 9	-0.0120309584327484	-0.1101568836543 84	0.2185722478671 26	-0.0353259366062005
d	9.88993287969575	-3.71795672639017	4.697457088531 76	6.6482695720843 3	-3.0265028140958 3
f	1.84381323555315	-0.6437799366295 6	0.9104182850141 27	-0.7379807723777 52	-0.5226874847453 2
g	-2.07484418218256	0.4470976389218 5	-0.9590536015546 54	-0.5809955761572 24	0.3780821789024 87
h	9.79270035795559	0.2329037414906 93	3.9712905990992 8	1.0000000030026 2	-1.6875537421762 5
i	0	0	-0.25	0.5	0
j	-1.11351498878271	-0.3666101172863 81	-0.5231835442906 77	-0.4704024006056 97	-1.4337891578343 4
k	1	0	0	1	0
s	0	0	-0.25	0	0
m	-0.5689151413065 3	-0.1067119305036 72	-0.5030258095510 99	0	-0.7487248781784 12
n	16	0	0	20	0
o	-4	0	0	0	0
p	2	0	0	-4	0
q	11.242088745771	0.765	-2.971290599099 28	-0.1051071104645 77	2.38
α	2.6875	-14.25	3	3.875	-1.75
β	-0.90625	0.125	-0.5	0.4375	0.0625
γ^-1	1.378714399100 87	1.074207336578 23	1.031634745737 52	0.9019835415086 8	1.033061782443 71
δ	1	2^-3	1	2^-3	2^-3
ζ	1	2^-1	1	2^-2	2^-2
ex	28	28	28	28	27
ey	29	29	30	29	28
ez	29	29	30	29	28
ew	27	28	28	27	28
e'y	61	62	62	60	61
e'x	63	64	63	61	62
e'w	63	60	60	61	59

图2

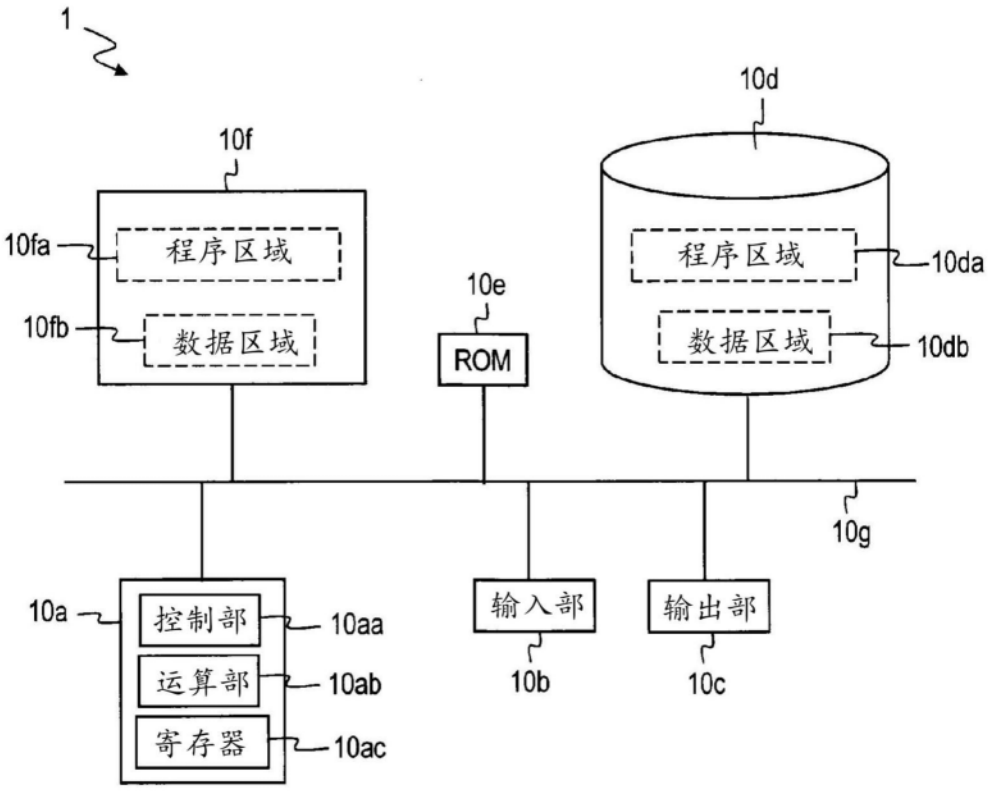

1
10f
10fa
程序区域
10fb
数据区域
10e
ROM
10d
程序区域
10da
数据区域
10db
10g
10a
控制部
10aa
运算部
10ab
寄存器
10ac
输入部
10b
输出部
10c

图3