(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114981859 B
(45)授权公告日 2025.03.07

(21)申请号 202080093270.5
(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 114981859 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/JP2020/001682 2020.01.20
(87)PCT国际申请的公布数据
WO2021/149105 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 金明顺
(51)Int.Cl.
G09C 1/00(2006.01)
(56)对比文件
JP 2004274320 A,2004.09.30
JP 2014164144 A,2014.09.08
审查员 刘多纳

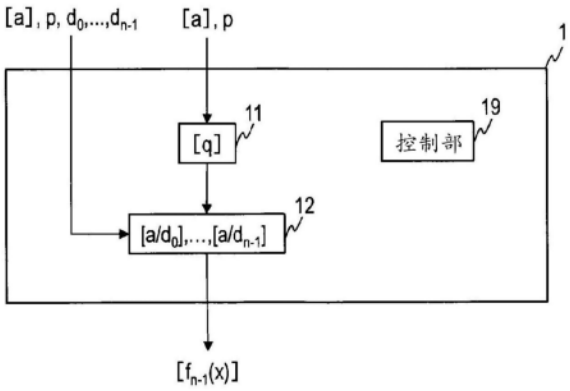
权利要求书2页 说明书6页 附图5页

(54)发明名称

秘密计算装置、秘密计算方法、计算机程序产品以及记录介质

(57)摘要

通过使用了秘密分散值[a]以及模p的秘密计算,得到a/p的商q的秘密分散值[q],通过使用了秘密分散值[a]、[q]、除数$d_0,\cdots,d_{n-1}$以及模p的秘密计算,得到$[a/d_0]=[(a+qp)/d_0]-[q]p/d_0,\cdots,[a/d_{n-1}]=[(a+qp)/d_{n-1}]-[q]p/d_{n-1}$并进行输出。其中,[μ]为μ的秘密分散值,a为实数,n为2以上的整数,$d_0,\cdots,d_{n-1}$为实数的除数,p为正整数的模,q为正整数的商。



1.一种秘密计算装置,其中,

[μ]为μ的秘密分散值,a为实数,n为2以上的整数,d_0,…,d_{n-1}为实数的除数,p为正整数的模,q为正整数的商,

所述秘密计算装置具有:

第1秘密计算部,通过使用了秘密分散值[a]以及模p的秘密计算,得到a/p的商q的秘密分散值[q];以及

第2秘密计算部,通过使用了所述秘密分散值[a]、[q]、所述除数d_0,…,d_{n-1}以及所述模p的秘密计算,得到$[a/d_0]=[(a+qp)/d_0]-[q]p/d_0$,…,$[a/d_{n-1}]=[(a+qp)/d_{n-1}]-[q]p/d_{n-1}$并进行输出。

2.一种秘密计算装置,其中,

[μ]为μ的秘密分散值,a为实数,m_0、m_1为实数的乘数,c为表示条件的0或1的值,

所述秘密计算装置具有:

第3秘密计算部,通过使用了秘密分散值[a]以及所述乘数m_0、m_1的秘密计算,得到$[m_0a]$以及$[m_1a]$;以及

第4秘密计算部,通过使用了秘密分散值[c]、$[m_0a]$、$[m_1a]$的秘密计算,得到在c=0的情况下为$[m_0a]$、在c=1的情况下为$[m_1a]$的m_ca的秘密分散值$[c?m_0a:m_1a]$并进行输出。

3.如权利要求2的秘密计算装置,其中,

$d_0=1/m_0$和$d_1=1/m_1$为除数,p为正整数的模,q为正整数的商,

所述第3秘密计算部具有:

第1秘密计算部,通过使用了秘密分散值[a]以及模p的秘密计算,得到a/p的商q的秘密分散值[q];以及

第2秘密计算部,通过使用了所述秘密分散值[a]、[q]、所述除数d_0、d_1以及所述模p的秘密计算,得到$[m_0a]=[a/d_0]=[(a+qp)/d_0]-[q]p/d_0$、$[m_1a]=[a/d_1]=[(a+qp)/d_1]-[q]p/d_1$并进行输出。

4.如权利要求3的秘密计算装置,其中,

σ0,σ1为表示右移位量的比特数的正整数,

所述第2秘密计算部具有:

公开值计算部,使用所述乘数m_0、m_1以及所述正整数σ0、σ1,得到公开值$2^{\sigma0}/m_0$、$2^{\sigma1}/m_1$;

第5秘密计算部,进行使用了所述秘密分散值[a]、[q]以及所述模p以及由所述公开值计算部得到的所述公开值$2^{\sigma0}/m_0$、$2^{\sigma1}/m_1$的公开值除法运算的秘密计算$[a+qp]/(2^{\sigma0}/m_0)$、$[a+qp]/(2^{\sigma1}/m_1)$,得到使$(a+qp)m_0$右移位了σ0比特的值的秘密分散值$[(a+qp)m_0]$以及使$(a+qp)m_1$右移位了σ1比特的值的秘密分散值$[(a+qp)m_1]$;以及

第6秘密计算部,通过使用了所述秘密分散值$[(a+qp)m_0]$、$[(a+qp)m_1]$、[q]和所述模p和乘数m_0、m_1的秘密计算,得到$[m_0a]=[(a+qp)m_0]-[q]pm_0$以及$[m_1a]=[(a+qp)m_1]-[q]pm_1$并进行输出。

5.一种秘密计算方法,其中,

[μ]为μ的秘密分散值,a为实数,n为2以上的整数,d_0,…,d_{n-1}为实数的除数,p为正整数的模,q为正整数的商,

所述秘密计算方法具有:

第1秘密计算步骤,第1秘密计算部通过使用了秘密分散值[a]以及模p的秘密计算,得到a/p的商q的秘密分散值[q];以及

第2秘密计算步骤,第2秘密计算部通过使用了所述秘密分散值[a]、[q]、所述除数$d_0,\cdots,d_{n-1}$以及所述模p的秘密计算,得到$[a/d_0]=[(a+qp)/d_0]-[q]p/d_0,\cdots,[a/d_{n-1}]=[(a+qp)/d_{n-1}]-[q]p/d_{n-1}$并进行输出。

6.一种秘密计算方法,其中,

[μ]为μ的秘密分散值,a为实数,m_0、m_1为实数的乘数,c为表示条件的0或1的值,

所述秘密计算方法具有:

第3秘密计算步骤,第3秘密计算部通过使用了秘密分散值[a]以及所述乘数m_0、m_1的秘密计算,得到$[m_0a]$以及$[m_1a]$;以及

第4秘密计算步骤,第4秘密计算部通过使用了秘密分散值[c]、$[m_0a]$、$[m_1a]$的秘密计算,得到在c=0的情况下为$[m_0a]$、在c=1的情况下为$[m_1a]$的m_ca的秘密分散值$[c?m_0a:m_1a]$并进行输出。

7.一种计算机程序产品,包括计算机程序,该计算机程序在由处理器执行时实现权利要求5或6所述的方法的步骤。

8.一种计算机可读的记录介质,存储有计算机程序,该计算机程序在由处理器执行时实现权利要求5或6所述的方法步骤。

秘密计算装置、秘密计算方法、计算机程序产品以及记录介质

技术领域

[0001] 本发明涉及秘密计算技术。

背景技术

[0002] 有如下情况:在通过秘密计算进行各种各样的计算时,将某1个秘密分散值(分享(share))除以多个除数或以多个移位量进行右移位(right shift)。在非专利文献1中,记载了通过秘密计算进行这样的计算的方法。

[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-0(|p|)比特通信量0(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-0(|p|)ビット通信量0(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,在非专利文献1所记载的方法中,存在计算成本大这一问题点。

[0008] 本发明是鉴于此点而作出的,目的在于削减在秘密计算中在将1个秘密分散值(秘钥分享值,secret share value)除以多个除数或以多个移位量进行右移位的情况下的计算成本。

[0009] 用于解决课题的手段

[0010] 根据使用了秘密分散值[a]以及模p的秘密计算,得到a/p的商q的秘密分散值[q],根据使用了秘密分散值[a],[q]、除数$d_0,\ldots,d_{n-1}$以及模p的秘密计算,得到$[a/d_0]=[(a+qp)/d_0]-[q]p/d_0,\ldots,[a/d_{n-1}]=[(a+qp)/d_{n-1}]-[q]p/d_{n-1}$并输出。其中,[μ]为μ的秘密分散值,a为实数,n我2以上的整数,$d_0,\ldots,d_{n-1}$为实数的除数,p为正整数的模,q为正整数的商。

[0011] 发明效果

[0012] 在本发明中,由于将秘密分散值[q]移用到多个$[a/d_0],\ldots,[a/d_{n-1}]$的计算中,因此能够削减在秘密计算中在将1个秘密分散值除以多个除数或以多个移位量进行右移位的情况下的计算成本。

附图说明

[0013] 图1是示出第1实施方式的秘密计算装置的功能结构的框图。

[0014] 图2是用于说明第1实施方式的处理的流程图。

[0015] 图3是示出第2实施方式的秘密计算装置的功能结构的框图。

[0016] 图4A是示出图3的秘密计算部21的详细内容的框图。

[0017] 图4B是示出图4A的秘密计算部212的详细内容的框图。

[0018] 图5A是用于说明第2实施方式的处理的流程图。

[0019] 图5B是用于示出图5A的步骤S21的详细内容的流程图。

[0020] 图5C是用于示出图5B的步骤S212的详细内容的流程图。

[0021] 图6是用于说明硬件结构的框图。

具体实施方式

[0022] 以下,使用附图来说明本发明的实施方式。

[0023] [第1实施方式]

[0024] 在秘密计算中,有将某1个秘密分散值(share)除以多个除数或以多个移位量进行右移位的情况。在本实施方式中,使这样的处理高效化。在右移位、除数公开除法中,一般而言,将成为运算对象的实数a以公式(1)这样表达,并加法秘密分散后的值(additive secret shared value)a_i作为秘密分散值[a]使用。

[0025] [数1]

[0026] $$a = \sum_{0 \le i < m} a_i \bmod p \qquad (1)$$

[0027] 其中,i=0,...,m-1,m为1以上的整数(例如,m为2以上的整数),p为正整数的模。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。这种情况下,若将实数a除以模p时的商作为q,则满足以下公式。

[0028] [数2]

[0029] $$\sum_{0 \le i < m} a_i = qp + a \qquad (2)$$

[0030] 在使用了这样的秘密分散值[a]=a_i的秘密计算中,使用商q的秘密分散值[q],但商q并不依赖于除数、移位量。因此,若求到一次秘密分散值[q],则能够将该秘密分散值[q]共用于通过秘密计算而求出将实数a除以多个除数的值或以多个移位量进行右移位的值的处理中。秘密计算中的商的计算的通信量大,若能削减该计算次数则能够使处理大幅地高效化。例如,在通过秘密计算求出将实数a除以2个公开除数的值的处理中,与通过秘密计算分别独立地进行公开值除法的情况相比,变得削减3成的通信量。在假定了无限个公开除数的情况下,与通过秘密计算分别独立地进行公开值除法的情况相比,变得削减6成的通信量。另外,由于右移位与通过2的幂数的除法为等价的,因此在通过秘密计算求出将实数a以多个移位量进行右移位的值的处理中也是相同的。以下详细地进行说明。

[0031] 如图1所示出,第1实施方式的秘密计算装置1具有秘密计算部11、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。在以下,设[μ]为μ的秘密分散值,a为实数,n为2以上的整数,$d_0,\ldots,d_{n-1}$为实数的除数,p为正整数的模,q为正整数的商。秘密分散值[μ]为将实数μ以公式(3)这样表达并进行加法秘密分散后的值μ_i。

[0032] [数3]

[0033] $$\mu = \sum_{0 \le i < m} \mu_i \bmod p \qquad (3)$$

[0034] 即,[μ]是对将p作为模的剩余环上的元素μ进行线性秘密分散后的秘密分散值(share)。

[0035] 如图2所示出,实数a的秘密分散值[a]、正整数的模p、除数$d_0,\ldots,d_{n-1}$被输入到秘密计算装置1(步骤S10)。

[0036] 秘密分散值[a]和模p被输入到秘密计算部11。秘密计算部11通过使用了秘密分散值[a]和模p的秘密计算,得到a/p的商q的秘密分散值[q]并输出(步骤S11)。

[0037] 秘密分散值[a],[q]、除数$d_0,\ldots,d_{n-1}$以及模p被输入到秘密计算部12。秘密计算部12通过使用了秘密分散值[a]、[q]、除数$d_0,\ldots,d_{n-1}$以及模p的秘密计算,得到$[a/d_0]=[(a+qp)/d_0]-[q]p/d_0,\ldots,[a/d_{n-1}]=[(a+qp)/d_{n-1}]-[q]p/d_{n-1}$并进行输出(步骤S12)。

[0038] 在本实施方式中,将在步骤S11中得到的1个秘密分散值[q]共用于多个$[a/d_0],\ldots,[a/d_{n-1}]$的秘密计算中,因此能削减计算成本。

[0039] [第2实施方式]

[0040] 在本实施方式中,基于条件$c\in\{0,1\}$将2个公开值m_0,m_1的其中一个公开值乘以实数a的秘密分散值[a]。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(为将该数以2进制表达而必要的比特数)上升,导致成为无法再次乘法运算的数,因此存在有必要右移位的情况。在本实施方式中,使这样的处理高效化。

[0041] 如图3所示出,本实施方式的秘密计算装置2具有秘密计算部21、22以及控制部29。秘密计算装置2在控制部29的控制之下执行各处理。如图4A所示出,本实施方式的秘密计算部21具有秘密计算部211、212。如图4B所示出,本实施方式的秘密计算部212具有公开值计算部212a、秘密计算部212b以及秘密计算部212c。

[0042] 如图5A所示出,在秘密计算装置2中,实数a的秘密分散值[a]、表示条件的0或1的值$c\in\{0,1\}$的秘密分散值[c]、作为公开值的实数的乘数m_0、m_1、以及模p被输入(步骤S20)。

[0043] 秘密分散值[a]、乘数m_0、m_1、以及模p被输入到秘密计算部21。秘密计算部21通过使用了秘密分散值[a]和乘数m_0、m_1、以及模p的秘密计算来得到秘密分散值$[m_0a]$以及$[m_1a]$并输出(步骤S21)。步骤S21的处理的具体例将在后面叙述。

[0044] 秘密分散值$[m_0a]$、$[m_1a]$、[c]被输入到秘密计算部22。秘密计算部22通过使用了秘密分散值[c]、$[m_0a]$、$[m_1a]$的秘密计算来得到m_ca的秘密分散值$[c?m_0a:m_1a]$并进行输出。即,秘密计算部22在c=0的情况下得到$[m_0a]$并进行输出,在c=1的情况下得到$[m_1a]$并进行输出(步骤S22)。

[0045] <步骤S21的处理的具体例>

[0046] 对步骤S21的处理的具体例进行说明。在此,使用第2实施方式的方法来使步骤S21的处理高效化。以下,$d_0=1/m_0$以及$d_1=1/m_1$为除数,p为正整数的模,q为正整数的商。

[0047] 如图5B所示出,秘密分散值[a]和模p被输入到秘密计算装置21(图4A)的秘密计算部211。秘密计算部21通过使用了秘密分散值[a]以及模p的秘密计算,得到a/p的商q的秘密分散值[q]并进行输出(步骤S211)。

[0048] 秘密分散值[a]、[q]、除数d_0、d_1以及模p被输入到秘密计算部212。秘密计算部212

通过使用了秘密分散值[a]、[q]、除数d_0、d_1以及模p的秘密计算,得到$[m_0a]=[a/d_0]=[(a+qp)/d_0]-[q]p/d_0$、$[m_1a]=[a/d_1]=[(a+qp)/d_1]-[q]p/d_1$并进行输出(步骤S212)。以下说明步骤S212的处理的具体例。

[0049] <步骤S212的处理的具体例>

[0050] 如前所述,在乘数m_0、m_1较大的情况下,在步骤S212中可能需要右移位。以下,通过同时进行右移位和基于公开值m_0、m_1的乘法运算来削减计算成本。以下,将表示这些右移位量的比特数的正整数分别表示为σ0、σ1。既可以是σ0=σ1,也可以是σ0≠σ1。

[0051] 如图5C所示出,乘数m_0、m_1以及正整数σ0、σ1被输入到秘密计算部212的公开值计算部212a。公开值计算部212a使用乘数m_0、m_1以及正整数σ0、σ1来得到公开值$2^{\sigma0}/m_0$、$2^{\sigma1}/m_1$并进行输出(步骤S212a)。

[0052] 秘密分散值[a]、[q]、模p、以及公开值$2^{\sigma0}/m_0$、$2^{\sigma1}/m_1$被输入到秘密计算部212b。秘密计算部212b进行使用了秘密分散值[a]、[q]以及模p和通过公开值计算部212a得到的公开值$2^{\sigma0}/m_0$、$2^{\sigma1}/m_1$的公开值除法的秘密计算$[a+qp]/(2^{\sigma0}/m_0)$、$[a+qp]/(2^{\sigma1}/m_1)$,得到使$(a+qp)m_0$右移位了σ0比特的值的秘密分散值$[(a+qp)m_0]$以及使$(a+qp)m_1$右移位了σ1比特的值的秘密分散值$[(a+qp)m_1]$并进行输出(步骤S212b)。

[0053] 秘密分散值$[(a+qp)m_0]$、$[(a+qp)m_1]$、[q]、模p、乘数m_0、m_1被输入到秘密计算部212c。秘密计算部212c通过使用了秘密分散值$[(a+qp)m_0]$、$[(a+qp)m_1]$、[q]和模p和乘数m_0、m_1的秘密计算,来得到$[m_0a]=[(a+qp)m_0]-[q]pm_0$以及$[m_1a]=[(a+qp)m_1]-[q]pm_1$并进行输出(步骤S212c)。

[0054] 通常,通过if-then-else门(gate)来生成基于秘密分散值[c]的秘密分散值$[m_c]$,即$[m_0]$或$[m_1]$,然后进行$[m_c]$和[a]的乘法运算$[m_ca]$。对此,在本实施方式中,得到秘密分散值$[m_0a]$以及$[m_1a]$(步骤S21),然后通过使用了秘密分散值[c]、$[m_0a]$、$[m_1a]$的秘密计算,来得到m_ca的秘密分散值$[c?m_0a:m_1a]$(步骤S22)。通过在步骤S22之前执行步骤S21,从而能够通过计算成本低的、公开值的乘数m_0、m_1和秘密分散值[a]的公开值乘法运算来实现秘密分散值$[m_ca]$。因此,本实施方式能够削减计算成本。尤其是,如步骤S212的处理的具体例那样,即使是在乘数m_0、m_1较大的情况下,在步骤S212中需要右移位的情况下,也可以通过同时进行右移位和基于公开值m_0、m_1的乘法运算来削减计算成本。能应用该处理是因为乘数m_0、m_1为公开值,这使得在步骤S21之后能够执行步骤S22。进一步地,如步骤S21的处理的具体例,通过使用第2实施方式的方法而使步骤S21的处理高效化,能进一步削减计算成本。

[0055] [硬件结构]

[0056] 实施方式中的秘密计算装置1、2,是例如通过具备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。该计算机既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,还可以预先记录在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。

[0057] 图6是示出实施方式中的秘密计算装置1、2的硬件结构的框图。如图6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、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秘密计算装置1、2的功能结构。

[0058] 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。

[0059] 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)。

[0060] 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。

[0061] 另外,本发明并不限定于上述的实施方式。例如,在上述的实施方式中得到$[a/d_0],\ldots,[a/d_{n-1}]$,但并不限于此,通过使用了秘密分散值[a]、[q]、所述除数$d_0,\ldots,d_{n-1}$以及所述模p的秘密计算,关于$\theta=0,\ldots,n-1$,还可以得到对右移位以及基于公开值d_θ的除法通过运算而得到的值的秘密计算值$f([a],[q],d_\theta)$。此外,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。

[0062] 工业上的可利用性

[0063] 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、数据挖掘中的倒数函数、平方根函数、指数函数、对数函数等初等函数的计算中进行利用。

[0064] 标号说明

[0065] 1、2秘密计算装置

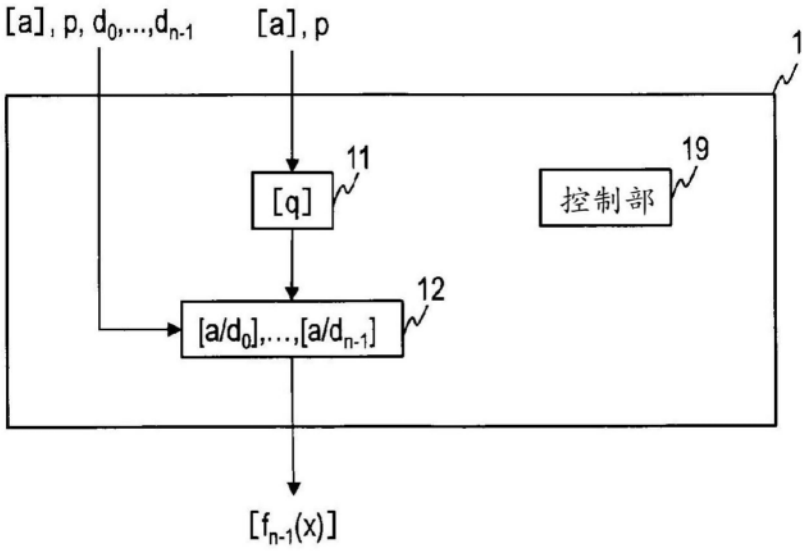

[a], p, d_0,...,d_{n-1}
[a], p
1
11
[q]
19
控制部
12
[a/d_0],...,[a/d_{n-1}]
[$f_{n-1}(x)$]

图1

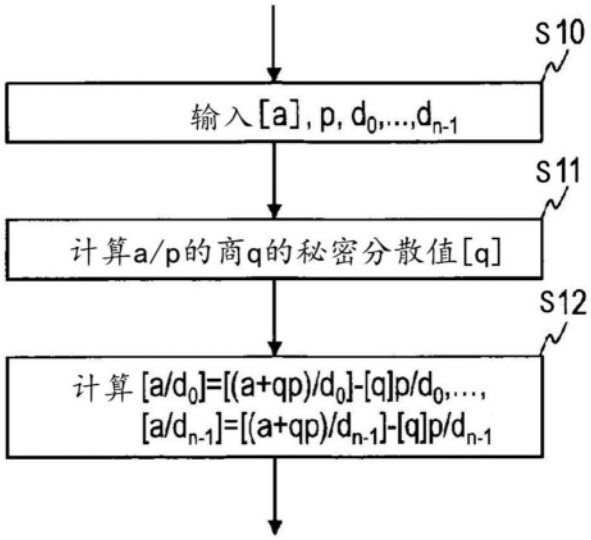

S10
输入[a], p, d_0,...,d_{n-1}
S11
计算a/p的商q的秘密分散值[q]
S12
计算 [a/d_0]=[(a+qp)/d_0]-[q]p/d_0,...,
[a/d_{n-1}]=[(a+qp)/d_{n-1}]-[q]p/d_{n-1}

图2

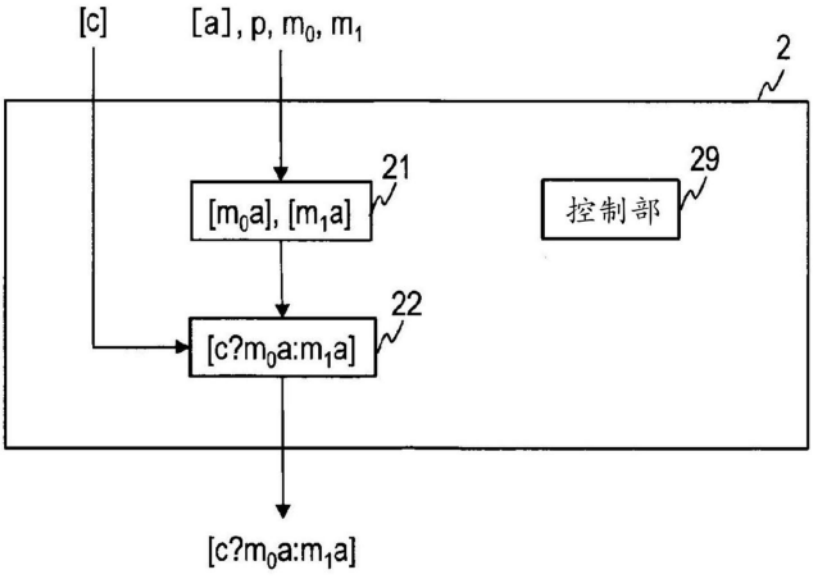

[c]
[a], p, m_0, m_1
2
21
[m_0a], [m_1a]
29
控制部
22
[c?m_0a:m_1a]
[c?m_0a:m_1a]

图3

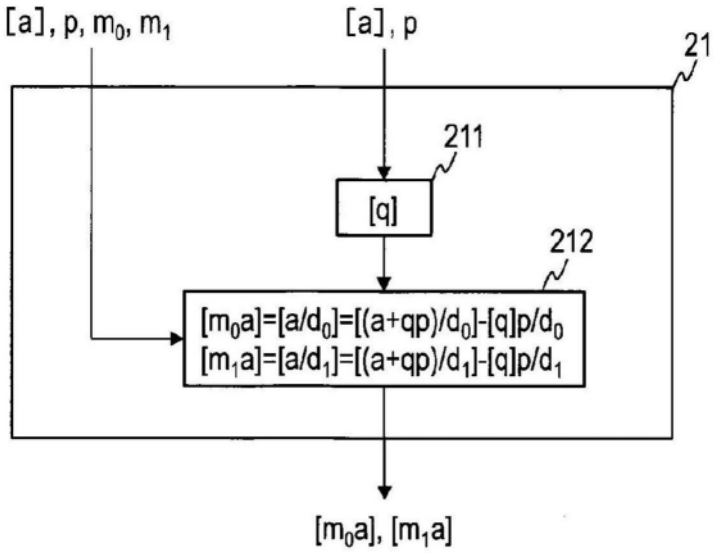

[a], p, m_0, m_1
[a], p
21
211
[q]
212
[m_0a]=[a/d_0]=[(a+qp)/d_0]-[q]p/d_0
[m_1a]=[a/d_1]=[(a+qp)/d_1]-[q]p/d_1
[m_0a], [m_1a]

图4A

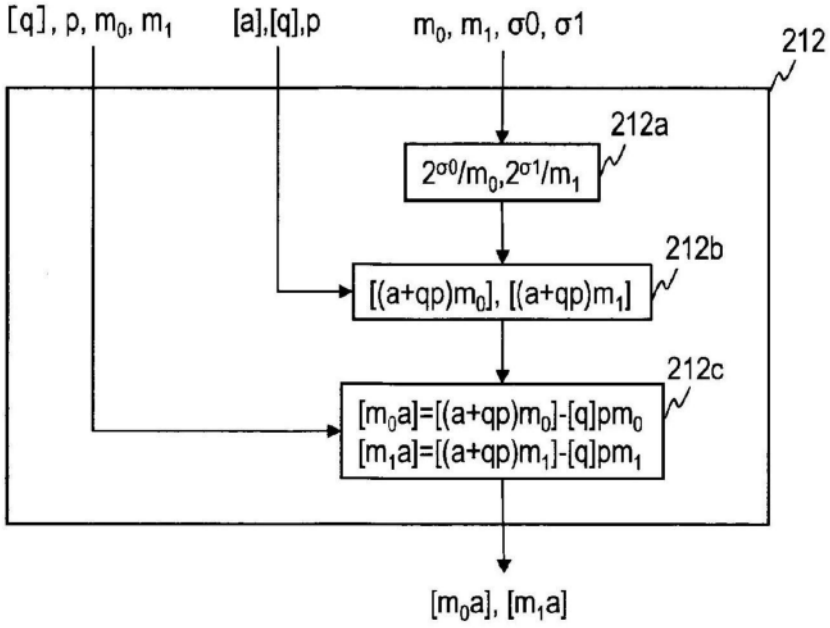

[q], p, m0, m1
[a],[q],p
m0, m1, σ0, σ1
212
212a
2σ0/m0,2σ1/m1
212b
[(a+qp)m0], [(a+qp)m1]
212c
[m0a]=[(a+qp)m0]-[q]pm0
[m1a]=[(a+qp)m1]-[q]pm1
[m0a], [m1a]

图4B

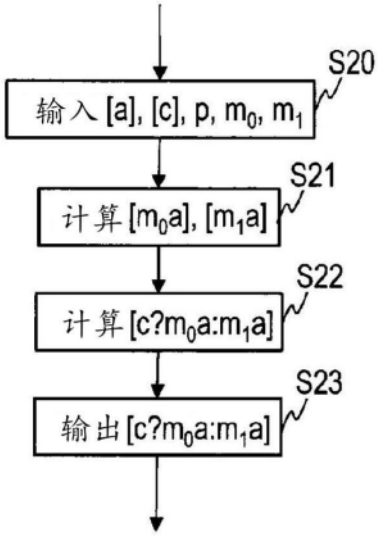

S20
输入 [a], [c], p, m0, m1
S21
计算 [m0a], [m1a]
S22
计算 [c?m0a:m1a]
S23
输出 [c?m0a:m1a]

图5A

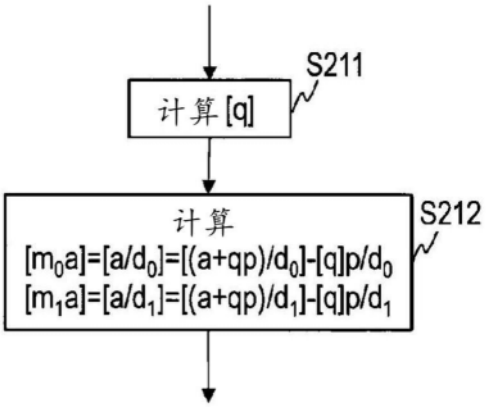

S211
计算 [q]
S212
计算
$[m_0a]=[a/d_0]=[(a+qp)/d_0]-[q]p/d_0$
$[m_1a]=[a/d_1]=[(a+qp)/d_1]-[q]p/d_1$

图5B

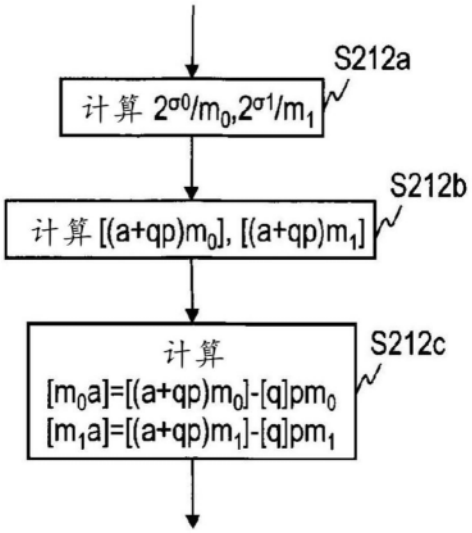

S212a
计算 $2^{\sigma 0}/m_0, 2^{\sigma 1}/m_1$
S212b
计算 $[(a+qp)m_0]$, $[(a+qp)m_1]$
S212c
计算
$[m_0a]=[(a+qp)m_0]-[q]pm_0$
$[m_1a]=[(a+qp)m_1]-[q]pm_1$

图5C

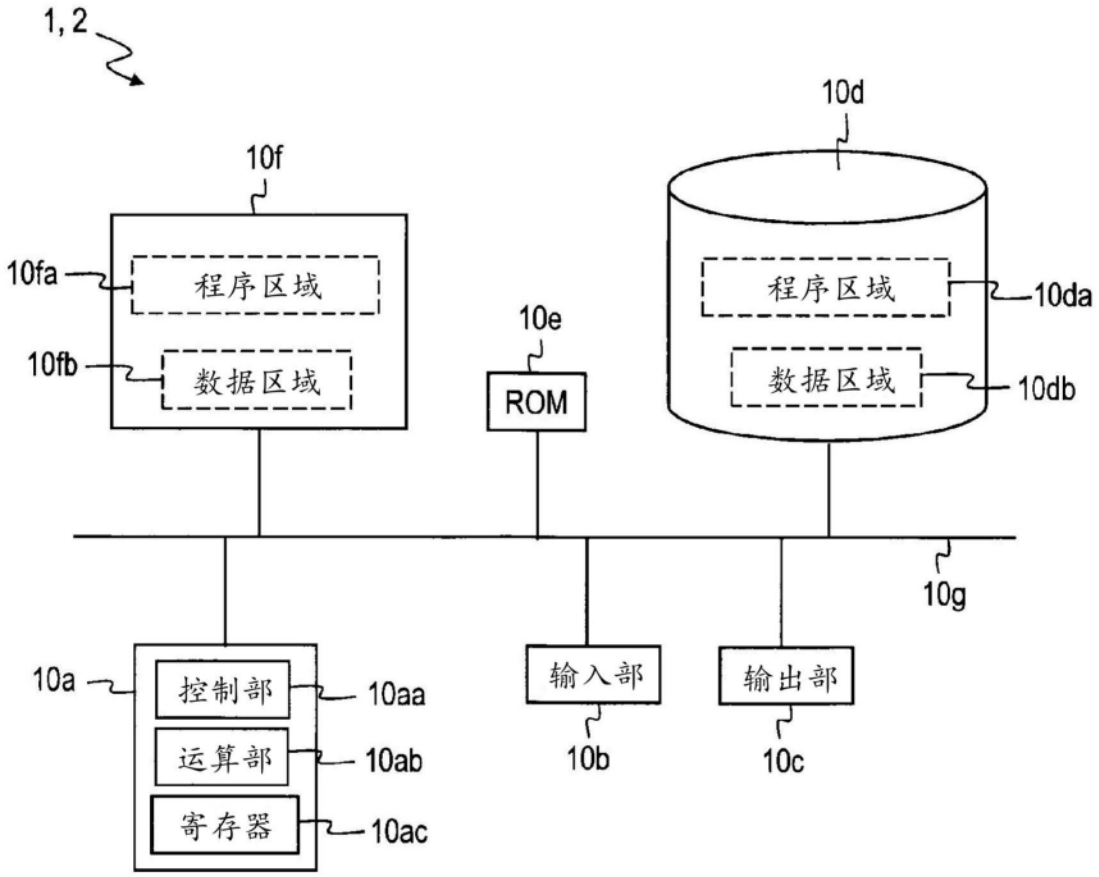

1, 2
10d
10f
10fa
程序区域
10fb
数据区域
10e
ROM
程序区域
10da
数据区域
10db
10g
10a
控制部
10aa
运算部
10ab
寄存器
10ac
输入部
10b
输出部
10c

图6