(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 119325696 A
(43)申请公布日 2025.01.17

(21)申请号 202280096866.X

(22)申请日 2022.06.14

(85)PCT国际申请进入国家阶段日
2024.12.06

(86)PCT国际申请的申请数据
PCT/JP2022/023823 2022.06.14

(87)PCT国际申请的公布数据
WO2023/242955 JA 2023.12.21

(71)申请人 三菱电机株式会社
地址 日本东京都

(72)发明人 广政良

(74)专利代理机构 北京三友知识产权代理有限公司 11127
专利代理师 马建军 欧阳柳青

(51)Int.Cl.
H04L 9/14(2006.01)
G09C 1/00(2006.01)
H04L 9/08(2006.01)

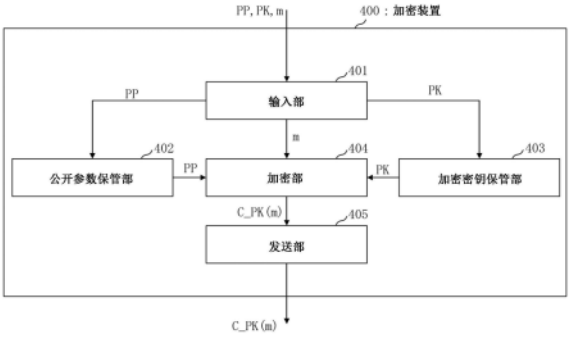
权利要求书3页 说明书14页 附图11页

(54)发明名称

隐匿信息处理系统、隐匿信息处理方法和隐匿信息处理程序

(57)摘要

对应于满足强电路隐匿性的量子同态加密技术的隐匿信息处理系统具有加密装置(400)。加密装置(400)具有加密部(404),该加密部(404)使用第1公开参数和第1加密密钥对第1明文进行加密,由此生成第1密文,使用第2公开参数和第2加密密钥对第2明文进行加密,由此生成第2密文。第1公开参数和第2公开参数分别是使用安全参数生成的参数。第1加密密钥是使用第1公开参数和第1解密密钥生成的加密密钥,该第1解密密钥是使用安全参数生成的解密密钥。第2加密密钥是使用第2公开参数和第2解密密钥生成的加密密钥,该第2解密密钥是使用安全参数生成的解密密钥。



CN 119325696 A

1.一种隐匿信息处理系统,其对应于满足强电路隐匿性的量子同态加密技术,其中,

所述隐匿信息处理系统具有加密装置,该加密装置具有加密部,该加密部使用第1公开参数和第1加密密钥对第1明文进行加密,由此生成第1密文,使用第2公开参数和第2加密密钥对第2明文进行加密,由此生成第2密文,

所述第1公开参数和所述第2公开参数分别是使用安全参数生成的参数,

所述第1加密密钥是使用所述第1公开参数和第1解密密钥生成的加密密钥,该第1解密密钥是使用所述安全参数生成的解密密钥,

所述第2加密密钥是使用所述第2公开参数和第2解密密钥生成的加密密钥,该第2解密密钥是使用所述安全参数生成的解密密钥。

2.根据权利要求1所述的隐匿信息处理系统,其中,

所述隐匿信息处理系统还具有密钥生成装置,该密钥生成装置具有加密密钥生成部,该加密密钥生成部使用所述第1公开参数和所述第1解密密钥生成所述第1加密密钥,使用所述第2公开参数和所述第2解密密钥生成所述第2加密密钥。

3.根据权利要求1或2所述的隐匿信息处理系统,其中,

所述隐匿信息处理系统还具有同态运算装置,该同态运算装置具有同态运算部,该同态运算部使用运算电路、所述第1公开参数、所述第2公开参数、所述第1密文、所述第2密文、所述第1加密密钥和所述第2加密密钥执行量子计算,由此生成第3密文,该第3密文是对针对所述第1明文和所述第2明文应用所述运算电路所示的运算而得到的运算结果进行加密而生成的密文。

4.根据权利要求3所述的隐匿信息处理系统,其中,

所述同态运算部在未生成所述第1加密密钥、所述第2加密密钥、所述第1密文和所述第2密文中的至少任意一方的情况下,生成随机的量子数据作为所述第3密文。

5.根据权利要求3或4所述的隐匿信息处理系统,其中,

所述第1解密密钥由第1同态解密密钥和第1量子同态解密密钥构成,

所述第2解密密钥由第2同态解密密钥和第2量子同态解密密钥构成,

所述第1加密密钥由根据所述第1同态解密密钥生成的第1同态公开密钥和根据所述第1量子同态解密密钥生成的第1量子同态公开密钥构成,

所述第2加密密钥由根据所述第2同态解密密钥生成的第2同态公开密钥和根据所述第2量子同态解密密钥生成的第2量子同态公开密钥构成,

所述第1密文根据所述第1公开参数、第1一次性密码本密钥、所述第1同态公开密钥、所述第1量子同态公开密钥和第1随机数来生成,

所述第2密文根据所述第2公开参数、第2一次性密码本密钥、所述第2同态公开密钥、所述第2量子同态公开密钥和第2随机数来生成。

6.根据权利要求5所述的隐匿信息处理系统,其中,

所述运算电路包含如下部位的各个部位:

根据所述安全参数、所述第1一次性密码本密钥、第1一次性密码本密钥密文数据、所述第1量子同态公开密钥和所述第1随机数计算用于对所述第3密文进行解密的随机数即第1解密随机数的部位;以及

根据所述安全参数、所述第2一次性密码本密钥、第2一次性密码本密钥密文数据、所述

第2量子同态公开密钥和所述第2随机数计算用于对所述第3密文进行解密的随机数即第2解密随机数的部位，

所述第1一次性密码本密钥密文数据是根据所述第1一次性密码本密钥、所述第1量子同态公开密钥和所述第1随机数生成的密文数据，

所述第2一次性密码本密钥密文数据是根据所述第2一次性密码本密钥、所述第2量子同态公开密钥和所述第2随机数生成的密文数据，

所述同态运算部根据是否生成了所述第1解密随机数来判定是否通过所述加密装置生成了所述第1加密密钥，根据是否生成了所述第2解密随机数来判定是否通过所述加密装置生成了所述第2加密密钥。

7.根据权利要求5所述的隐匿信息处理系统，其中，

所述运算电路包含如下部位的各个部位：

根据所述安全参数、所述第1一次性密码本密钥、第1一次性密码本密钥密文数据、所述第1量子同态公开密钥和所述第1随机数计算用于对所述第3密文进行解密的随机数即第1解密随机数的部位；以及

根据所述安全参数、所述第2一次性密码本密钥、第2一次性密码本密钥密文数据、所述第2量子同态公开密钥和所述第2随机数计算用于对所述第3密文进行解密的随机数即第2解密随机数的部位，

所述第1一次性密码本密钥密文数据是根据所述第1一次性密码本密钥、所述第1量子同态公开密钥和所述第1随机数生成的密文数据，

所述第2一次性密码本密钥密文数据是根据所述第2一次性密码本密钥、所述第2量子同态公开密钥和所述第2随机数生成的密文数据，

所述同态运算部根据是否生成了所述第1解密随机数来判定是否通过所述加密装置生成了所述第1密文，根据是否生成了所述第2解密随机数来判定是否通过所述加密装置生成了所述第2密文。

8.一种隐匿信息处理方法，对应于满足强电路隐匿性的量子同态加密技术，其中，

计算机使用第1公开参数和第1加密密钥对第1明文进行加密，由此生成第1密文，使用第2公开参数和第2加密密钥对第2明文进行加密，由此生成第2密文，

所述第1公开参数和所述第2公开参数分别是使用安全参数生成的参数，

所述第1加密密钥是使用所述第1公开参数和第1解密密钥生成的加密密钥，该第1解密密钥是使用所述安全参数生成的解密密钥，

所述第2加密密钥是使用所述第2公开参数和第2解密密钥生成的加密密钥，该第2解密密钥是使用所述安全参数生成的解密密钥。

9.一种隐匿信息处理程序，该隐匿信息处理程序对应于满足强电路隐匿性的量子同态加密技术，其中，

所述隐匿信息处理程序使作为计算机的加密装置执行如下的加密处理：使用第1公开参数和第1加密密钥对第1明文进行加密，由此生成第1密文，使用第2公开参数和第2加密密钥对第2明文进行加密，由此生成第2密文，

所述第1公开参数和所述第2公开参数分别是使用安全参数生成的参数，

所述第1加密密钥是使用所述第1公开参数和第1解密密钥生成的加密密钥，该第1解密

密钥是使用所述安全参数生成的解密密钥，

所述第2加密密钥是使用所述第2公开参数和第2解密密钥生成的加密密钥，该第2解密密钥是使用所述安全参数生成的解密密钥。

隐匿信息处理系统、隐匿信息处理方法和隐匿信息处理程序

技术领域

[0001] 本公开涉及隐匿信息处理系统、隐匿信息处理方法和隐匿信息处理程序。

背景技术

[0002] 量子同态加密是能够在对数据进行了加密的状态下进行量子运算的加密技术。近来,云服务的利用正在扩大,但是,从担心破解或云的可靠性等出发,考虑在云中对数据进行加密并保管。在量子同态加密中,能够不对被加密的数据进行解密地对被加密的数据实施运算。因此,量子同态加密是能够不损害安全性地利用使用了量子计算的云服务的技术。

[0003] 用于提高量子同态加密的安全性的、实现了不会从在对数据进行了加密的状态下进行量子运算而得到的结果泄露与运算处理有关的信息的安全性的加密技术,是满足电路隐匿性的量子同态加密。特别地,在满足电路隐匿性的量子同态加密中,实现不会从针对未通过加密算法生成的密文的量子同态运算的结果泄露与量子运算有关的信息的安全性的量子同态加密,也是满足强电路隐匿性的量子同态加密。在对加密后的数据执行运算时,在确认输入的正当性后,在通过通常的满足电路隐匿性的量子同态加密对数据进行了加密的状态下执行运算,由此实现满足强电路隐匿性的量子同态加密。具体而言,输入的正当性是指,作为运算的输入的加密密钥通过密钥生成算法来生成,作为运算的输入的密文通过加密算法来生成。通常的满足电路隐匿性的量子同态加密是电路隐匿性仅针对通过加密算法生成的密文成立的量子同态加密。

[0004] 非专利文献1公开了满足强电路隐匿性的量子同态加密的结构例,此外,还公开了能够对使用彼此不同的加密密钥进行加密后的密文彼此执行同态运算的满足强电路隐匿性的量子同态加密的结构例。

[0005] 现有技术文献

[0006] 非专利文献

[0007] 非专利文献1:Chardouvelis,O.et al.,“Rate-1 QuantumFully Homomorphic Encryption”,TCC 2021:Theory ofCryptography,pp.149-176,2021.

发明内容

[0008] 发明要解决的课题

[0009] 非专利文献1公开的现有的满足电路隐匿性的量子同态加密将被称作Decisional Small PolynomialRatio(DSPR:决定性小多项式比)问题的特殊的计算问题设为安全性的依据。但是,公知DSPR问题能够通过使用量子计算机而简单地解读。特别地,在非专利文献1公开的量子同态加密技术中,用作结构要素的满足电路隐匿性的同态加密的安全性依赖于DSPR问题的困难性。因此,非专利文献1公开的满足强电路隐匿性的量子同态加密针对量子计算机也不安全。

[0010] 本公开的目的在于,实现如下的满足强电路隐匿性的量子同态加密技术:针对量子计算机安全,并且,能够针对通过彼此不同的加密密钥进行加密后的密文彼此进行基于

量子计算的同态运算。

[0011] 用于解决课题的手段

[0012] 本公开的隐匿信息处理系统对应于满足强电路隐匿性的量子同态加密技术,其中,所述隐匿信息处理系统具有加密装置,该加密装置具有加密部,该加密部使用第1公开参数和第1加密密钥对第1明文进行加密,由此生成第1密文,使用第2公开参数和第2加密密钥对第2明文进行加密,由此生成第2密文,所述第1公开参数和所述第2公开参数分别是使用安全参数生成的参数,所述第1加密密钥是使用所述第1公开参数和第1解密密钥生成的加密密钥,该第1解密密钥是使用所述安全参数生成的解密密钥,所述第2加密密钥是使用所述第2公开参数和第2解密密钥生成的加密密钥,该第2解密密钥是使用所述安全参数生成的解密密钥。

[0013] 发明效果

[0014] 根据本公开,能够实现如下的满足强电路隐匿性的量子同态加密技术:针对量子计算机安全,并且,能够针对通过彼此不同的加密密钥进行加密后的密文彼此进行基于量子计算的同态运算。

附图说明

[0015] 图1是示出实施方式1的隐匿信息处理系统100的结构例的图。

[0016] 图2是示出实施方式1的公开参数生成装置200的结构例的图。

[0017] 图3是示出实施方式1的密钥生成装置300的结构例的图。

[0018] 图4是示出实施方式1的加密装置400的结构例的图。

[0019] 图5是示出实施方式1的同态运算装置500的结构例的图。

[0020] 图6是示出实施方式1的解密装置600的结构例的图。

[0021] 图7是示出实施方式1的各装置的硬件结构例的图。

[0022] 图8是示出实施方式1的隐匿信息处理系统100的动作的流程图。

[0023] 图9是示出实施方式1的隐匿信息处理系统100的动作的流程图。

[0024] 图10是示出实施方式1的隐匿信息处理系统100的动作的流程图。

[0025] 图11是示出实施方式1的变形例的各装置的硬件结构例的图。

具体实施方式

[0026] 在实施方式的说明和附图中,对相同的要素和对应的要素标注相同的标号。标注了相同标号的要素的说明适当地省略或简化。图中的箭头主要表示数据流或处理流。此外,也可以适当地将“部”改写成“设备”、“电路”、“工序”、“顺序”、“处理”、“步骤”或“线路”。

[0027] 实施方式1

[0028] 下面,参照附图对本实施方式进行详细说明。

[0029] ***结构的说明***

[0030] 图1示出本实施方式的隐匿信息处理系统100的系统结构例。如图1所示,隐匿信息处理系统100具有公开参数生成装置200、密钥生成装置300、加密装置400、同态运算装置500和解密装置600。

[0031] 互联网101是连接公开参数生成装置200、密钥生成装置300、多个加密装置400、同

态运算装置500和解密装置600的通信路径。互联网101是网络的具体例。也可以使用其他种类的网络以代替互联网101。

[0032] 作为具体例,公开参数生成装置200是PC(Personal Computer:个人计算机)。公开参数生成装置200制作用于分别生成加密密钥、解密密钥和密文的公开参数,经由互联网101向密钥生成装置300、加密装置400和同态运算装置500分别发送表示制作出的公开参数的数据。另外,表示制作出的公开参数的数据也可以通过邮寄等直接发送。

[0033] 作为具体例,密钥生成装置300是PC。密钥生成装置300分别制作加密中使用的加密密钥和解密密钥,经由互联网101向加密装置400和同态运算装置500分别发送表示制作出的加密密钥的数据,向解密装置600发送表示制作出的解密密钥的数据。另外,表示制作出的各密钥的数据也可以通过邮寄等直接发送。

[0034] 解密密钥是秘密的信息,因此,解密密钥以不会泄露的方式保管于密钥生成装置300和解密装置600各自的内部。

[0035] 作为具体例,加密装置400是PC。加密装置400使用用所保管的公开参数和加密密钥对从工厂的传感器等得到的明文数据进行加密,由此生成密文数据,将生成的密文数据经由互联网101发送到同态运算装置500。

[0036] 作为具体例,同态运算装置500是具有大容量的存储介质的计算机。另外,同态运算装置500也被称作电路隐匿量子同态运算装置。

[0037] 同态运算装置500还作为数据保管装置发挥功能。即,如果存在来自加密装置400的密文数据的保管请求,则同态运算装置500保管与保管请求对应的密文数据。

[0038] 同态运算装置500还作为对所保管的密文数据即保管密文数据进行同态运算的装置发挥功能。即,同态运算装置500根据所保管的公开参数、所保管的加密密钥和保管密文数据,生成与针对明文数据的运算结果对应的密文数据,将生成的密文数据经由互联网101发送到解密装置600,明文数据与保管密文数据对应。

[0039] 作为具体例,解密装置600是PC。解密装置600还作为解密密钥保管装置发挥功能,该解密密钥保管装置接收密钥生成装置300发送的表示解密密钥的数据,保管接收到的数据所示的解密密钥。

[0040] 解密装置600还是作为密文数据解密装置进行动作的PC,该密文数据解密装置接收同态运算装置500发送的密文数据,使用所保管的解密密钥对接收到的密文数据进行解密,由此取得运算结果。

[0041] 另外,也可以在同一PC内同时包含公开参数生成装置200、密钥生成装置300、加密装置400、同态运算装置500和解密装置600中的至少2个。

[0042] 下面,对本实施方式的结构进行说明。另外,各装置制作的要素的数量也可以是2个以上。

[0043] 图2是示出公开参数生成装置200的结构例的框图。如图2所示,公开参数生成装置200具有输入部201、公开参数生成部202和发送部203。另外,虽然没有图示,但是,公开参数生成装置200具有存储在公开参数生成装置200的各部中使用的数据的存储介质。

[0044] 输入部201接收表示安全参数λ的数据,将接收到的表示安全参数λ的数据发送到公开参数生成部202。

[0045] 公开参数生成部202将从输入部201接受的数据所示的安全参数λ作为输入,生成

用于分别生成加密密钥和解密密钥的参数即公开参数PP。然后,公开参数生成部202将表示所生成的公开参数PP的数据发送到发送部203。

[0046] 发送部203将表示公开参数生成部202生成的公开参数PP的数据分别发送到密钥生成装置300、加密装置400和同态运算装置500。

[0047] 图3是示出密钥生成装置300的结构例的框图。如图3所示,密钥生成装置300具有输入部301、公开参数保管部302、解密密钥生成部303、加密密钥生成部304和发送部305。另外,虽然没有图示,但是,密钥生成装置300具有存储在密钥生成装置300的各部中使用的数据的存储介质。

[0048] 输入部301接收公开参数生成装置200发送的表示公开参数PP的数据,将接收到的数据所示的公开参数PP发送到公开参数保管部302。

[0049] 此外,输入部301接收表示安全参数λ的数据,将接收到的表示安全参数λ的数据发送到解密密钥生成部303。

[0050] 公开参数保管部302保管从输入部301接受的数据所示的公开参数PP。

[0051] 解密密钥生成部303使用从输入部301接受的数据所示的安全参数λ生成解密密钥SK,将表示所生成的解密密钥SK的数据分别发送到加密密钥生成部304和发送部305。

[0052] 加密密钥生成部304将从公开参数保管部302接受的数据所示的公开参数PP和从解密密钥生成部303接受的数据所示的解密密钥SK作为输入,生成加密密钥PK,将表示所生成的加密密钥PK的数据发送到发送部305。

[0053] 另外,加密密钥生成部304使用第1公开参数和第1解密密钥生成第1加密密钥,使用第2公开参数和第2解密密钥生成第2加密密钥。这里,第1公开参数和第2公开参数分别是使用安全参数λ生成的参数。第1解密密钥和第2解密密钥分别是使用安全参数λ生成的解密密钥。

[0054] 发送部305将表示解密密钥生成部303生成的解密密钥SK的数据发送到解密装置600。

[0055] 此外,发送部305将表示加密密钥生成部304生成的加密密钥PK的数据分别发送到加密装置400和同态运算装置500。

[0056] 图4是示出加密装置400的结构例的框图。如图4所示,加密装置400具有输入部401、公开参数保管部402、加密密钥保管部403、加密部404和发送部405。另外,虽然没有图示,但是,加密装置400具有存储在加密装置400的各部中使用的数据的存储介质。

[0057] 输入部401接收公开参数生成装置200发送的表示公开参数PP的数据,将接收到的表示公开参数PP的数据发送到公开参数保管部402。

[0058] 此外,输入部401接收密钥生成装置300发送的表示加密密钥PK的数据,将接收到的表示加密密钥PK的数据发送到加密密钥保管部403。

[0059] 此外,输入部401接收明文数据m,将接收到的明文数据m发送到加密部404。

[0060] 公开参数保管部402保管从输入部401接受的数据所示的公开参数PP。

[0061] 加密密钥保管部403保管从输入部401接受的数据所示的加密密钥PK。

[0062] 加密部404使用从公开参数保管部402接受的公开参数PP、从加密密钥保管部403接受的加密密钥PK和从输入部401接受的明文数据m,生成与明文数据m对应的密文数据C_PK(m),将生成的密文数据C_PK(m)发送到发送部405。下面,将使用加密密钥PK对明文数据m

进行加密而得到的密文数据表示为密文数据C_PK(m)。

[0063] 加密部404使用第1公开参数和第1加密密钥对第1明文进行加密,由此生成第1密文,使用第2公开参数和第2加密密钥对第2明文进行加密,由此生成第2密文。

[0064] 发送部405从加密部404接受密文数据C_PK(m),将接受的密文数据C_PK(m)发送到同态运算装置500。

[0065] 图5是示出同态运算装置500的结构例的框图。如图5所示,同态运算装置500具有输入部501、公开参数保管部502、加密密钥保管部503、密文保管部504、同态运算部505和发送部506。另外,虽然没有图示,但是,同态运算装置500具有存储在同态运算装置500的各部中使用的数据的存储介质。

[0066] 输入部501接收公开参数生成装置200发送的表示公开参数PP1的数据和表示公开参数PP2的数据,将接收到的表示公开参数PP1的数据和表示公开参数PP2的数据发送到公开参数保管部502。这里,在表示各要素的标号的末尾标注的数字是用于相互区分存在有多个的相同种类的要素的标记。作为具体例,关于公开参数PP1和公开参数PP2,为了区分公开参数生成装置200生成的2个公开参数PP,在末尾标注1或2。此外,公开参数PP1相当于第1公开参数。公开参数PP2相当于第2公开参数。

[0067] 此外,输入部501接收密钥生成装置300发送的表示加密密钥PK1的数据和表示加密密钥PK2的数据,将接收到的表示加密密钥PK1的数据和表示加密密钥PK2的数据发送到加密密钥保管部503。这里,加密密钥PK1相当于第1加密密钥。加密密钥PK2相当于第2加密密钥。第1加密密钥由根据第1同态解密密钥生成的第1同态公开密钥和根据第1量子同态解密密钥生成的第1量子同态公开密钥构成。第2加密密钥由根据第2同态解密密钥生成的第2同态公开密钥和根据第2量子同态解密密钥生成的第2量子同态公开密钥构成。

[0068] 此外,输入部501接收加密装置400发送的密文数据C_PK(m1)和密文数据C_PK(m2),将接收到的密文数据C_PK(m1)和密文数据C_PK(m2)发送到密文保管部504。这里,明文数据m1对应于第1明文。明文数据m2对应于第2明文。密文数据C_PK(m1)对应于第1密文。密文数据C_PK(m2)对应于第2密文。第1密文是根据第1公开参数、第1一次性密码本密钥、第1同态公开密钥、第1量子同态公开密钥和第1随机数生成的密文。第2密文是根据第2公开参数、第2一次性密码本密钥、第2同态公开密钥、第2量子同态公开密钥和第2随机数生成的密文。

[0069] 此外,输入部501接收表示运算电路f的数据,将接收到的表示运算电路f的数据发送到同态运算部505。运算电路f也可以由多个运算电路构成。

[0070] 公开参数保管部502保管从输入部501接受的数据所示的公开参数PP1和公开参数PP2。

[0071] 加密密钥保管部503保管从输入部501接受的数据所示的加密密钥PK1和加密密钥PK2。

[0072] 密文保管部504保管从输入部501接受的密文数据C_PK(m1)和密文数据C_PK(m2)。

[0073] 同态运算部505使用从输入部501接受的数据所示的运算电路f、从公开参数保管部502接受的公开参数PP1和公开参数PP2、从加密密钥保管部503接受的加密密钥PK1和加密密钥PK2、以及从密文保管部504接受的密文数据C_PK(m1)和C_PK(m2)计算密文数据C_PK(M),将计算出的密文数据C_PK(M)发送到发送部506。这里,密文数据C_PK(M)是表示与运算

结果数据M(＝f(m1,m2))对应的密文的数据,该运算结果数据M(＝f(m1,m2))是表示针对明文数据m1和明文数据m2应用运算电路f所示的运算而得到的运算结果的数据。此外,f(m1,m2)表示将2个明文数据即明文数据m1和明文数据m2作为输入而执行了运算电路f所示的运算的结果。下面,将与由加密密钥PK1和加密密钥PK2构成的集合{PK1,PK2}有关的运算结果数据M的同态运算后密文数据表示为C_PK(M)。C_PK(M)也被称作同态运算后密文数据。这里,明文数据m1对应于第1明文。明文数据m2对应于第2明文。C_PK(M)对应于第3密文。另外,通过对密文数据C_PK(M)使用解密密钥SK1和解密密钥SK2,能够对运算结果数据M进行解密。这里,解密密钥SK1相当于第1解密密钥。解密密钥SK2相当于第2解密密钥。第1解密密钥由第1同态解密密钥和第1量子同态解密密钥构成。第2解密密钥由第2同态解密密钥和第2量子同态解密密钥构成。

[0074] 同态运算部505使用第1公开参数、第2公开参数、第1密文、第2密文、第1加密密钥和第2加密密钥执行量子计算,由此生成第3密文。这里,第3密文是对针对第1明文和第2明文应用运算电路f所示的运算而得到的运算结果进行加密而生成的密文。运算电路f也可以包含计算第1解密随机数的部位和计算第2解密随机数的部位的各个部位。第1解密随机数是根据安全参数、第1一次性密码本密钥、第1一次性密码本密钥密文数据、第1量子同态公开密钥和第1随机数计算出的随机数,并且是用于对第3密文进行解密的随机数。第2解密随机数是根据安全参数、第2一次性密码本密钥、第2一次性密码本密钥密文数据、第2量子同态公开密钥和第2随机数计算出的随机数,并且是用于对第3密文进行解密的随机数。另外,同态运算部505在未生成第1加密密钥、第2加密密钥、第1密文和第2密文中的至少任意一方的情况下,生成随机的量子数据作为第3密文。

[0075] 同态运算部505根据是否生成了第1解密随机数来判定是否通过加密装置生成了第1加密密钥,根据是否生成了第2解密随机数来判定是否通过加密装置生成了第2加密密钥。同态运算部505根据是否生成了第1解密随机数来判定是否通过加密装置生成了第1密文,根据是否生成了第2解密随机数来判定是否通过加密装置生成了第2密文。

[0076] 发送部506将从同态运算部505接受的运算后密文数据C_PK(M)发送到解密装置600。

[0077] 图6是示出解密装置600的结构例的框图。如图6所示,解密装置600具有输入部601、解密密钥保管部602、解密处理部603和解密结果保管部604。另外,虽然没有图示,但是,解密装置600具有存储在解密装置600的各部中使用的数据的存储介质。

[0078] 输入部601接收密钥生成装置300发送的表示解密密钥SK1的数据和表示解密密钥SK2的数据,将接收到的表示解密密钥SK1的数据和表示解密密钥SK2的数据发送到解密密钥保管部602。

[0079] 此外,输入部601接收同态运算装置500发送的与加密密钥的集合PK＝{PK1,PK2}有关的运算结果数据M的运算后密文数据C_PK(M),将接收到的运算后密文数据C_PK(M)发送到解密处理部603。

[0080] 解密密钥保管部602保管从输入部601接受的数据所示的解密密钥SK1和解密密钥SK2。

[0081] 解密处理部603从输入部601接受运算后密文数据C_PK(M),从解密密钥保管部602接受解密密钥SK1和解密密钥SK2,针对所接受的运算后密文数据C_PK(M)使用所接受的解

密密钥SK1和解密密钥SK2,由此对被加密的运算结果数据M进行解密,将解密出的运算结果数据M发送到解密结果保管部604。

[0082] 解密结果保管部604从解密处理部603接受运算结果数据M,保管所接受的运算结果数据M。

[0083] 图7是示出本实施方式的各装置的硬件资源的一例的图。如图7所示,各装置是具有处理器11(CentralProcessingUnit:中央处理单元)的一般的计算机。

[0084] 作为具体例,处理器11是CPU(CentralProcessingUnit:中央处理单元)、DSP(DigitalSignalProcessor:数字信号处理器)或GPU(Graphics Processing Unit:图形处理单元)。处理器11经由总线12与ROM(Read Only Memory:只读存储器)13、RAM(RandomAccess Memory:随机存取存储器)14、通信板15、显示器31(显示装置)、键盘32、鼠标33、驱动器34、磁盘装置20等硬件设备连接,对这些硬件设备进行控制。驱动器34是对FD(Flexible Disk Drive:软磁碟机)、CD(Compact Disc:光盘)、DVD(DigitalVersatile Disc:数字多功能盘)等存储介质进行读写的装置。

[0085] ROM13、RAM14、磁盘装置20和驱动器34是存储装置的一例。

[0086] 键盘32、鼠标33和通信板15是输入装置的一例。

[0087] 显示器31和通信板15是输出装置的一例。

[0088] 通信板15以有线或无线方式与LAN(Local Area Network:局域网)、互联网或电话线路等通信网连接。

[0089] 磁盘装置20存储有OS(操作系统)21、程序组22和文件组23。

[0090] 在程序组22中包含执行在本实施方式中作为“部”进行说明的功能的程序。程序由处理器11读出并执行。即,程序使计算机作为“部”发挥功能,此外,使计算机执行“部”的步骤和方法。

[0091] 在文件组23中包含在本实施方式中说明的“部”中使用的各种数据(输入、输出、判定结果、计算结果或处理结果等)。

[0092] 根据流程图等说明的本实施方式的处理使用处理器11、存储装置、输入装置或输出装置等硬件来执行。

[0093] 作为“部”说明的部分也可以通过固件、软件、硬件或它们的组合中的任意方来实现。

[0094] 本说明书中记载的任何程序都可以记录于计算机能读取的非易失性记录介质。作为具体例,非易失性记录介质是光盘或闪存。本说明书中记载的任何程序都可以作为程序产品来提供。

[0095] ***动作的说明***

[0096] 隐匿信息处理系统100的动作步骤相当于隐匿信息处理方法。隐匿信息处理方法也是与构成隐匿信息处理系统100的各装置的动作步骤对应的方法的总称。此外,实现隐匿信息处理系统100的动作的程序相当于隐匿信息处理程序。隐匿信息处理程序也是实现构成隐匿信息处理系统100的各装置的动作的程序的总称。

[0097] 图8是示出隐匿信息处理系统100中的公开参数的生成和保管处理的一例的流程图。使用图8对公开参数的生成和保管处理进行说明。

[0098] 另外,步骤S701～步骤S703是由公开参数生成装置200执行的处理,步骤S704～步

骤S705是由密钥生成装置300执行的处理,步骤S706～步骤S707是由加密装置400执行的处理,步骤S708～步骤S709是由同态运算装置500执行的处理。

[0099] (步骤S701)

[0100] 输入部201接收安全参数λ。

[0101] (步骤S702)

[0102] 公开参数生成部202将在步骤S701中由输入部201接收到的安全参数λ作为输入,生成公开参数PP。

[0103] (步骤S703)

[0104] 发送部203接受在步骤S702中由公开参数生成部202生成的公开参数PP,将表示所接受的公开参数PP的数据分别发送到密钥生成装置300、加密装置400和同态运算装置500。

[0105] (步骤S704)

[0106] 输入部301接收在步骤S703中由发送部203发送的表示公开参数PP的数据。

[0107] (步骤S705)

[0108] 公开参数保管部302保管在步骤S704中由输入部301接收到的数据所示的公开参数PP。

[0109] (步骤S706)

[0110] 输入部401接收在步骤S703中由发送部203发送的表示公开参数PP的数据。

[0111] (步骤S707)

[0112] 公开参数保管部402保管在步骤S706中由输入部401接收到的数据所示的公开参数PP。

[0113] (步骤S708)

[0114] 输入部501接收在步骤S703中由发送部203发送的表示公开参数PP的数据。

[0115] (步骤S709)

[0116] 公开参数保管部502保管在步骤S708中由输入部501接收到的数据所示的公开参数PP。

[0117] 图9是示出隐匿信息处理系统100中的加密密钥和解密密钥的生成和保管处理的一例的流程图。使用图9对加密密钥和解密密钥的生成和保管处理进行说明。

[0118] 另外,步骤S801～步骤S804是由密钥生成装置300执行的处理,步骤S805～步骤S806是由加密装置400执行的处理,步骤S807～步骤S808是由同态运算装置500执行的处理,步骤S809～步骤S810是由解密装置600执行的处理。

[0119] (步骤S801)

[0120] 输入部301接收表示安全参数λ的数据。

[0121] (步骤S802)

[0122] 解密密钥生成部303将在步骤S801中由输入部301接收到的数据所示的安全参数λ作为输入,生成以[数学式1]这样的形式表示的解密密钥SK。

[0123] 【数学式1】

[0124] $SK=(sk,qsk)$

[0125] 这里,同态解密密钥sk是将安全参数λ作为输入而使用[参考文献1]记载的同态密钥生成算法生成的。此外,量子同态解密密钥qsk是将安全参数λ和随机数r作为输入而使用

[参考文献2]记载的量子同态密钥生成算法生成的。

[0126] [参考文献1]

[0127] Ostrovsky,R.et al.,“Maliciously Circuit-private FHE.”,CRYPTO 2014:Advances in Cryptology-CRYPTO 2014,pp.536-553,2014.

[0128] [参考文献2]

[0129] Agarwal,A.et al.,“Post-Quantum Multi-Party Computation”,EUROCRYPT 2021:Advances in Cryptology-EUROCRYPT 2021,pp.435-464,2021.

[0130] (步骤S803)

[0131] 加密密钥生成部304将在步骤S802中由解密密钥生成部303生成的解密密钥SK和公开参数保管部302中保管的公开参数PP作为输入,生成以[数学式2]这样的形式表示的加密密钥PK。

[0132] 【数学式2】

[0133] PK＝(pk,qpk,[r])

[0134] 这里,同态公开密钥pk是将同态解密密钥sk作为输入而使用[参考文献1]记载的同态密钥生成算法生成的。量子同态公开密钥qpk是将公开参数PP、量子同态解密密钥qsk和随机数r作为输入而使用[参考文献2]记载的量子同态密钥生成算法生成的。进而,随机数密文[r]是将随机数r和同态公开密钥pk作为输入而使用[参考文献1]记载的同态加密算法生成的。

[0135] (步骤S804)

[0136] 发送部305接受表示在步骤S802中由解密密钥生成部303生成的解密密钥SK的数据、以及表示在步骤S803中由加密密钥生成部304生成的加密密钥PK的数据,向加密装置400和同态运算装置500分别发送所接受的表示加密密钥PK的数据,向解密装置600发送所接受的表示解密密钥SK的数据。

[0137] (步骤S805)

[0138] 输入部401接收在步骤S804中由发送部305发送的表示加密密钥PK的数据。

[0139] (步骤S806)

[0140] 加密密钥保管部403保管在步骤S805中由输入部401接收到的数据所示的加密密钥PK。

[0141] (步骤S807)

[0142] 输入部501接收在步骤S804中由发送部305发送的表示加密密钥PK的数据。

[0143] (步骤S808)

[0144] 加密密钥保管部503保管在步骤S807中由输入部501接收到的数据所示的加密密钥PK。

[0145] (步骤S809)

[0146] 输入部601接收在步骤S804中由发送部305发送的表示解密密钥SK的数据。

[0147] (步骤S810)

[0148] 解密密钥保管部602保管在步骤S809中由输入部601接收到的数据所示的解密密钥SK。

[0149] 另外,解密密钥SK是秘密信息,因此,解密密钥保管部602需要严格地保管,以使解

密密钥SK不会向外部泄露。

[0150] 图10是示出隐匿信息处理系统100中的同态运算的一例的流程图。使用图10对同态运算进行说明。

[0151] 另外,步骤S901～步骤S903是由加密装置400执行的处理,步骤S904～步骤S908是由同态运算装置500执行的处理,步骤S909～步骤S911是由解密装置600执行的处理。

[0152] (步骤S901)

[0153] 作为具体例,输入部401接收从传感器等收集到的明文数据m1和明文数据m2,将接收到的明文数据m1和明文数据m2发送到加密部404。

[0154] (步骤S902)

[0155] 加密部404根据在步骤S901中由输入部401接收到的明文数据m1和明文数据m2、公开参数保管部402中保管的公开参数PP1和公开参数PP2、以及加密密钥保管部403中保管的加密密钥PK1和加密密钥PK2,生成以[数学式3]这样的形式表示的密文数据C_PK(m1)和密文数据C_PK(m2)。另外,根据能够表现的字符形式的情况,数学式中的标记和正文中的标记有时不同。

[0156] 【数学式3】

[0157] $C_{PK}(m1)=(c1,[[otk1]]_1,[otk1,s1]_1)$

[0158] $C_{PK}(m2)=(c2,[[otk2]]_2,[otk2,s2]_2)$

[0159] 这里,量子密文数据c1和量子密文数据c2分别是将一次性密码本密钥otk1和一次性密码本密钥otk2作为输入而使用[参考文献2]记载的量子一次性密码本加密算法生成的。这里,一次性密码本密钥otk1相当于第1一次性密码本密钥。一次性密码本密钥otk2相当于第2一次性密码本密钥。作为一次性密码本密钥密文数据的[[otk1]]_1和[[otk2]]_2分别是将一次性密码本密钥otk1或一次性密码本密钥otk2、量子同态公开密钥qpk1或量子同态公开密钥qpk2、以及随机数s1或随机数s2作为输入而使用[参考文献2]记载的多个密钥量子同态加密算法生成的。这里,量子同态公开密钥qpk1相当于第1量子同态公开密钥。量子同态公开密钥qpk2相当于第2量子同态公开密钥。另外,公开参数PP1和公开参数PP2分别用作多个密钥量子同态加密算法的输入。进而,作为一次性密码本密钥和随机数密文数据的[otk1,s1]_1和[otk2,s2]_2分别是将一次性密码本密钥otk1或一次性密码本密钥otk2、同态公开密钥pk1或同态公开密钥pk2、以及随机数s1或随机数s2作为输入而使用[参考文献1]记载的同态加密算法生成的。这里,同态公开密钥pk1相当于第1同态公开密钥。同态公开密钥pk2相当于第2同态公开密钥。随机数s1相当于第1随机数。随机数s2相当于第2随机数。加密部404将密文数据C_PK(m1)和密文数据C_PK(m2)分别发送到加密装置400的发送部405。

[0160] (步骤S903)

[0161] 发送部405接受在步骤S902中由加密部404发送的密文数据C_PK(m1)和密文数据C_PK(m2),将接受的密文数据C_PK(m1)和密文数据C_PK(m2)发送到同态运算装置500。

[0162] (步骤S904)

[0163] 输入部501接受从发送部405发送的密文数据C_PK(m1)和密文数据C_PK(m2),将接受的密文数据C_PK(m1)和密文数据C_PK(m2)发送到密文保管部504。

[0164] (步骤S905)

[0165] 密文保管部504接受在步骤S904中从输入部501发送的密文数据C_PK(m1)和密文数据C_PK(m2),保管所接受的密文数据C_PK(m1)和密文数据C_PK(m2)。

[0166] (步骤S906)

[0167] 输入部501接收从键盘、鼠标或存储装置等输入的运算电路f,将接收到的运算电路f发送到同态运算部505。

[0168] (步骤S907)

[0169] 同态运算部505将从输入部501接收到的运算电路f、公开参数保管部502中保管的公开参数PP1和公开参数PP2、加密密钥保管部503中保管的加密密钥PK1和加密密钥PK2、以及密文保管部504中保管的密文数据C_PK(m1)和密文数据C_PK(m2)作为输入,生成与对应于以[数学式4]的形式表示的加密密钥集合{PK1,PK2}的运算结果数据M(=f(m1,m2))对应的运算后密文数据C_PK(M),将生成的运算后密文数据C_PK(M)发送到发送部506。

[0170] 【数学式4】

[0171] $C_{PK}(M)=(c',(c1',c2'))$

[0172] 这里,量子同态运算后密文数据c'是通过[数学式5]记载的方法生成的。作为量子同态运算后部分密文数据的c1'和c2'分别是将[数学式7]或[数学式8]记载的运算电路、同态公开密钥pk1或同态公开密钥pk2、随机数密文数据[r1]_1或随机数密文数据[r2]_2、以及作为一次性密码本密钥和随机数密文数据的[otk1,s1]_1或[otk2,s2]_2作为输入而使用[参考文献1]记载的同态运算算法生成的。

[0173] 【数学式5】

[0174] $c'=QOTP.Enc(otk',c'')$

[0175] 这里,算法QOTP.Enc是[参考文献2]记载的量子一次性密码本加密算法,一次性密码本密钥otk'是随机选择出的比特列。此外,c"是将利用[数学式6]表示的量子电路G、量子同态公开密钥qpk1和量子同态公开密钥qpk2、以及作为一次性密码本密钥密文数据的[[otk1]]_1和[[otk2]]_2作为输入而使用[参考文献2]记载的量子同态运算算法生成的。另外,公开参数PP1和公开参数PP2分别用作量子同态运算算法的输入。

[0176] 【数学式6】

[0177] $G_{c1,c2}(otk1,otk2)=f(QOTP.Dec(otk1,c1),QOTP.Dec(otk2,c2))$

[0178] 这里,算法QOTP.Dec是[参考文献2]记载的量子一次性密码本解密算法。

[0179] 【数学式7】

$$T_{qpk1,[[otk1]]_1,\rho_1}(r1,otk1,s1)$$

[0180]

$$=\begin{cases}\rho 1 & if \begin{array}{c}(\cdot,qpk1)=MKQFHE.Gen(1^{\lambda},r1)\\ and\ [[otk1]]_1=MKQFHE.Enc(qpk1,otk1,s1)\end{array}\\ 0 & otherwise\end{cases}$$

[0181] 【数学式8】

$$T_{qpk2,[[otk2]]_2,\rho_2}(r2,otk2,s2)$$

[0182]
$$=\begin{cases}\rho 2 & if \begin{matrix}(\cdot,qpk2)=MKQFHE.Gen(1^{\lambda},r2)\\ and\ [[otk2]]_2=MKQFHE.Enc(qpk2,otk2,s2)\end{matrix}\\ 0 & otherwise\end{cases}$$

[0183] 这里,算法MKQFHE.Gen和MKQFHE.Enc分别是[参考文献2]记载的量子同态密钥生成算法和量子同态加密算法。此外,随机数ρ1和随机数ρ2是用于对密文数据进行解密的随机数,是针对一次性密码本密钥otk'满足[数学式9]的关系的数。这里,[数学式7]相当于计算第1解密随机数的部位。[数学式8]相当于计算第2解密随机数的部位。随机数ρ1相当于第1解密随机数。随机数ρ2相当于第2解密随机数。

[0184] 另外,同态运算部505在对数据进行了加密的状态下执行[数学式7]和[数学式8]分别记载的运算电路f所示的运算,由此确认是否正确地生成了各加密密钥PK和各密文数据C_PK(m)。这里,根据[数学式7]和[数学式8]分别记载的运算电路f的结构,当在同态运算部505中利用了未通过密钥生成装置300生成的加密密钥的情况下,在解密装置600内无法得到随机数ρ1和随机数ρ2。此外,当在同态运算部505中利用了未通过加密装置400生成的密文数据的情况下,也同样地在解密装置600内无法得到随机数ρ1和随机数ρ2。

[0185] 【数学式9】

[0186] otk'=XOR(ρ1,ρ2)

[0187] 这里,运算电路XOR是计算作为电路的输入的ρ1和ρ2的每个比特的XOR的电路。

[0188] (步骤S908)

[0189] 发送部506将在步骤S907中从同态运算部505发送的运算后密文数据C_PK(M)发送到解密装置600。

[0190] (步骤S909)

[0191] 输入部601接收在步骤S908中从发送部506发送的运算后密文数据C_PK(M),将接收到的运算后密文数据C_PK(M)发送到解密处理部603。

[0192] (步骤S910)

[0193] 解密处理部603使用在步骤S909中从输入部601发送的运算后密文数据C_PK(M)、以及解密密钥保管部602中保管的解密密钥SK1和解密密钥SK2进行解密处理,由此得到解密结果M。这里,关于与运算后密文数据C_PK(M)对应的加密密钥集合{PK1,PK2},仅在将解密密钥SK1作为输入而在加密密钥生成部304中生成加密密钥PK1、且将解密密钥SK2作为输入而在加密密钥生成部304中生成加密密钥PK2的情况下,解密处理部603能够对解密结果M(=f(m1,m2))进行解密。

[0194] 解密处理部603将解密结果M发送到解密结果保管部604。

[0195] (步骤S911)

[0196] 解密结果保管部604保管在步骤S910中由解密处理部603发送的解密结果M。

[0197] 另外,解密装置600受理的密文是应用了同态运算后的密文。因此,在希望对应用同态运算之前的密文进行解密的情况下,要求同态运算装置500执行直接输出与输入相同的值的同态运算,与步骤S910中的处理同样地对执行同态运算而得到且应用了同态运算后的密文进行解密,由此,能够解密出与应用同态运算之前的密文对应的明文数据。

[0198] 通过步骤S911,隐匿信息处理系统100的同态运算处理结束。

[0199] ***实施方式1的效果的说明***

[0200] 如上所述,在本实施方式中,在内部使用针对量子计算机安全的满足电路隐匿性的同态加密。这里,[参考文献1]和[参考文献2]记载的加密技术分别具有针对量子计算机的安全性。因此,本实施方式的满足强电路隐匿性的量子同态加密方式也具有针对量子计算机的安全性。另一方面,在现有技术中,在内部使用针对量子计算机不安全的满足电路隐匿性的同态加密,因此,不具有针对量子计算机的安全性。

[0201] 此外,本实施方式具有针对量子计算机的安全性,因此,能够更加高效地设定参数来实现加密方式。另一方面,在现有技术中,不具有针对量子计算机的安全性,因此,需要计算尺寸大到足以具有针对量子计算机的安全性的密文。

[0202] 因此,根据本实施方式,不需要生成针对量子计算机安全且尺寸足够大的密文,因此,效率性提高。

[0203] ***其他结构***

[0204] <变形例1>

[0205] 图11示出本变形例的各装置的硬件结构例。

[0206] 各装置具有处理电路18,以代替处理器11、处理器11和ROM13、处理器11和RAM14、或处理器11和ROM13和RAM14。

[0207] 处理电路18是实现各装置具有的各部的至少一部分的硬件。

[0208] 处理电路18可以是专用的硬件,此外,也可以是执行RAM14中存储的程序的处理器。

[0209] 在处理电路18是专用的硬件的情况下,作为具体例,处理电路18是单一电路、复合电路、程序化的处理器、并行程序化的处理器、ASIC(ApplicationSpecific Integrated Circuit:专用集成电路)、FPGA(Field Programmable Gate Array:现场可编程门阵列)或它们的组合。

[0210] 各装置也可以具有代替处理电路18的多个处理电路。多个处理电路分担处理电路18的作用。

[0211] 在各装置中,也可以是,一部分功能通过专用的硬件来实现,其余功能通过软件或固件来实现。

[0212] 作为具体例,处理电路18通过硬件、软件、固件或它们的组合来实现。

[0213] 将处理器11、ROM13、RAM14和处理电路18统称作“处理线路”。即,各装置的各功能结构要素的功能通过处理线路来实现。

[0214] ***其他实施方式***

[0215] 说明了实施方式1,但是,也可以组合实施本实施方式中的多个部分。或者,也可以部分地实施本实施方式。除此之外,本实施方式可以根据需要进行各种变更,也可以作为整体或部分地任意组合实施。

[0216] 另外,所述的实施方式是本质上优选的例示,并不意图限制本公开、其应用物和用途的范围。使用流程图等说明的步骤也可以适当地变更。

[0217] 标号说明

[0218] 11:处理器;12:总线;13:ROM;14:RAM;15:通信板;18:处理电路;20:磁盘装置;21:

OS;22:程序组;23:文件组;31:显示器;32:键盘;33:鼠标;34:驱动器;100:隐匿信息处理系统;101:互联网;200:公开参数生成装置;201:输入部;202:公开参数生成部;203:发送部;300:密钥生成装置;301:输入部;302:公开参数保管部;303:解密密钥生成部;304:加密密钥生成部;305:发送部;400:加密装置;401:输入部;402:公开参数保管部;403:加密密钥保管部;404:加密部;405:发送部;500:同态运算装置;501:输入部;502:公开参数保管部;503:加密密钥保管部;504:密文保管部;505:同态运算部;506:发送部;600:解密装置;601:输入部;602:解密密钥保管部;603:解密处理部;604:解密结果保管部。

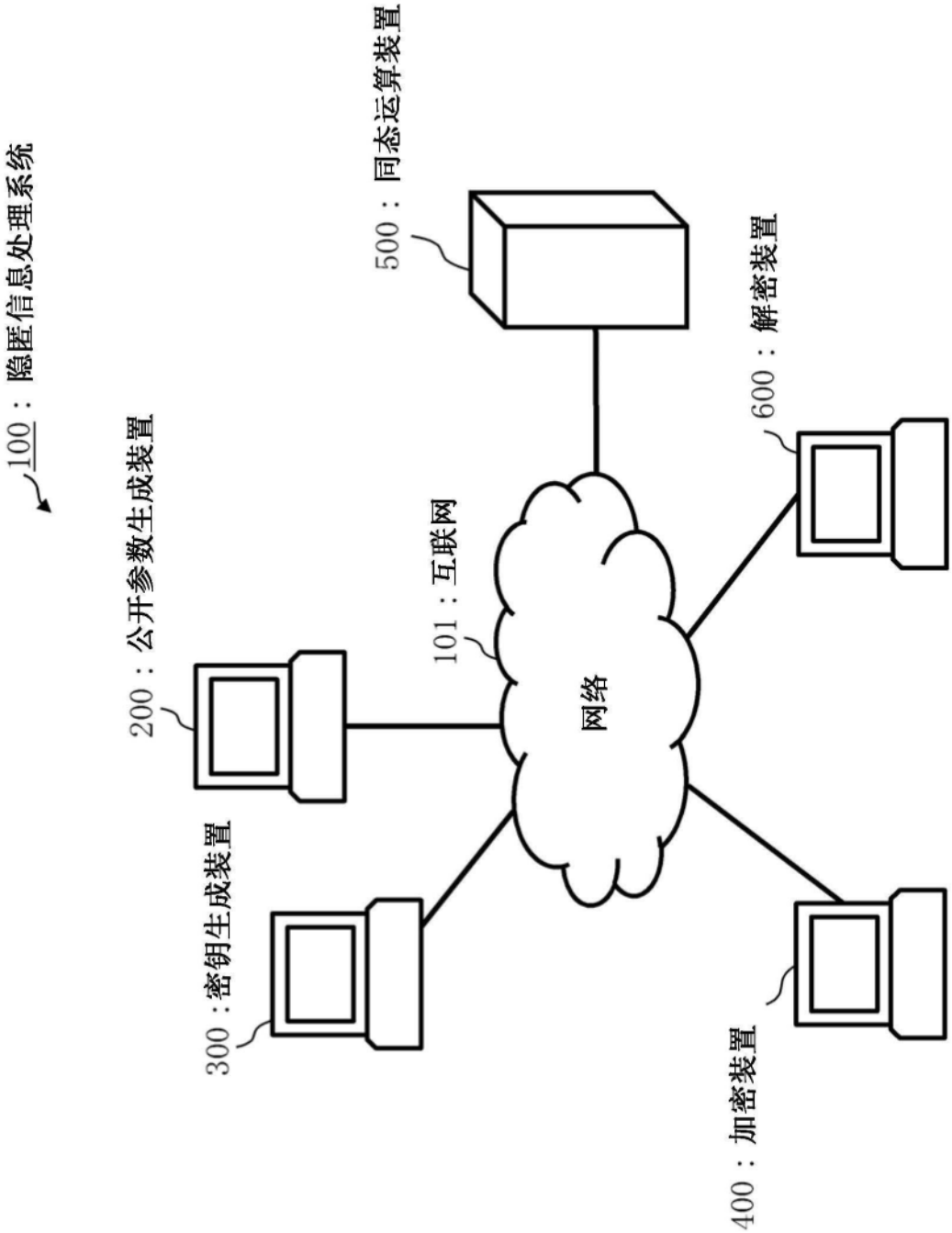

100：隐匿信息处理系统
500：同态运算装置
600：解密装置
200：公开参数生成装置
101：互联网
网络
300：密钥生成装置
400：加密装置

图1

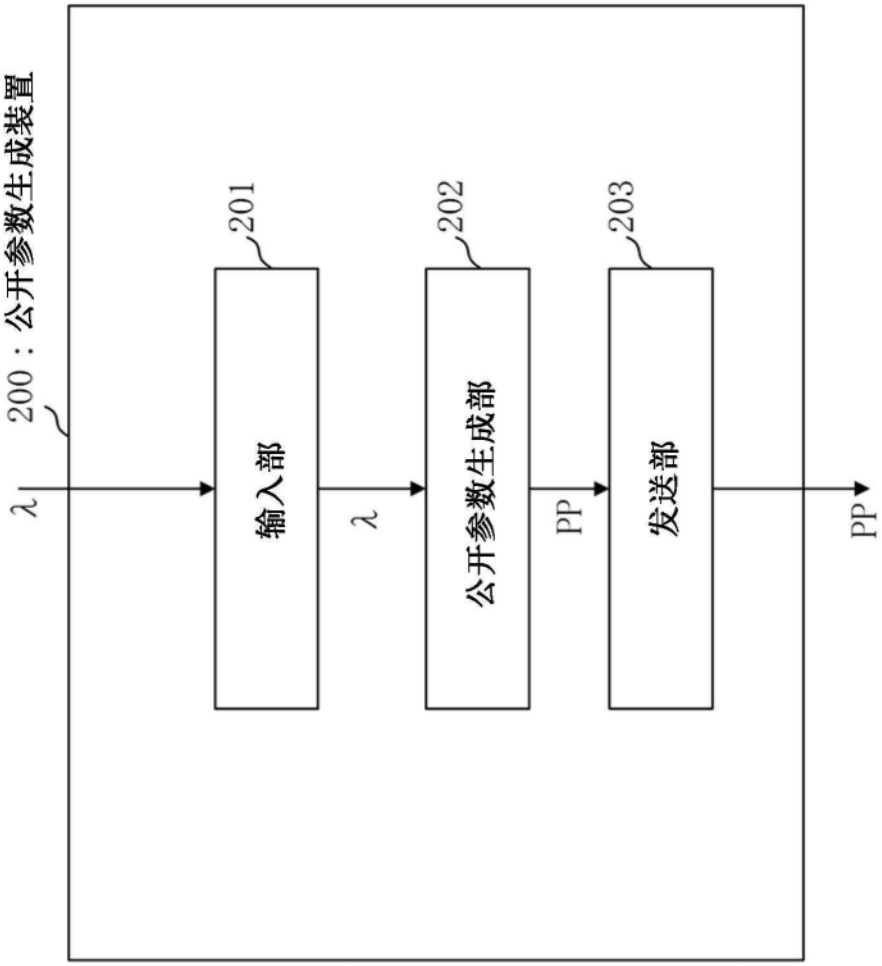


图2

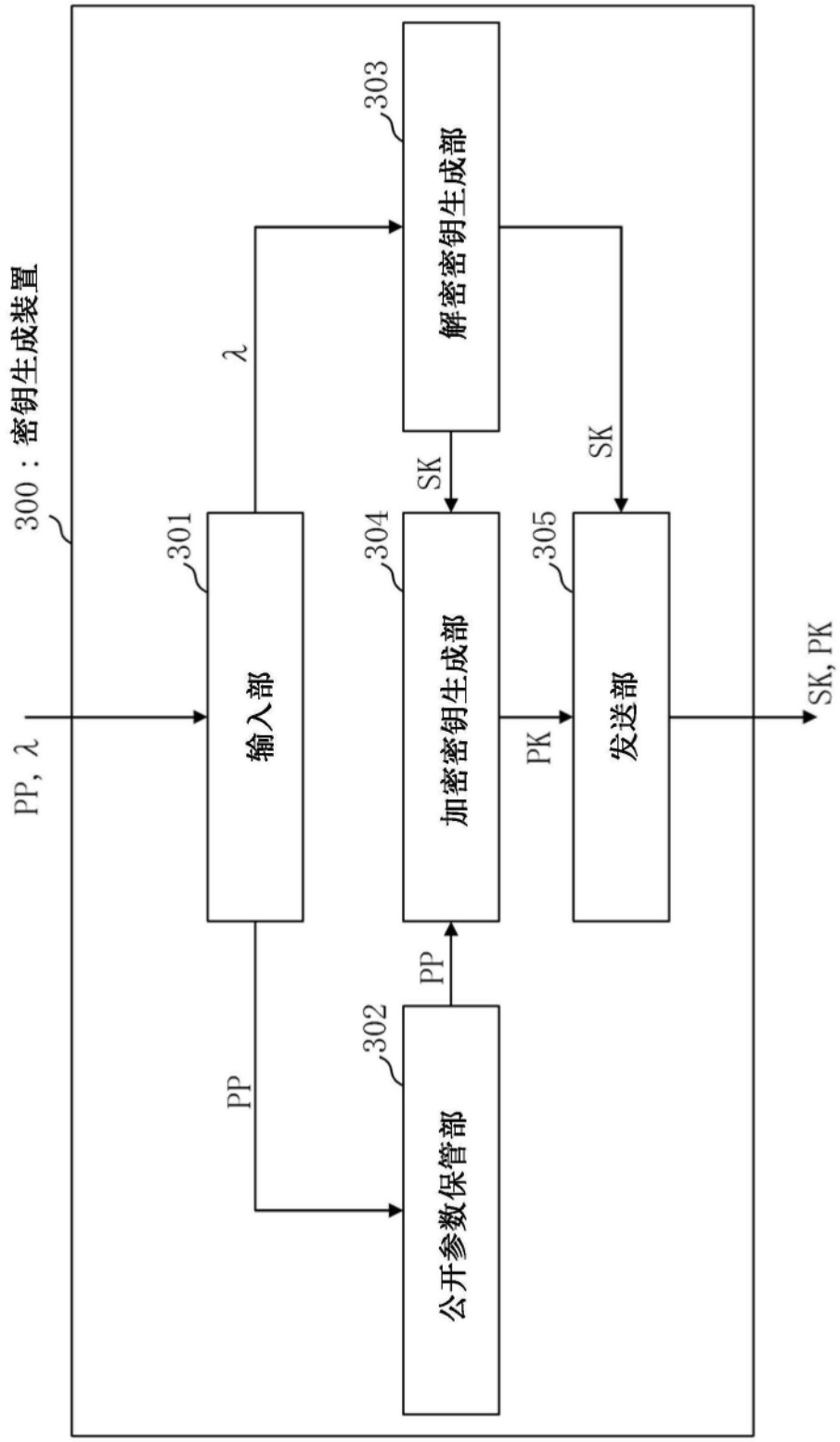

300：密钥生成装置
PP, λ
301
输入部
λ
303
解密密钥生成部
SK
304
加密密钥生成部
PK
305
发送部
SK, PK
PP
302
公开参数保管部
PP
SK

图3

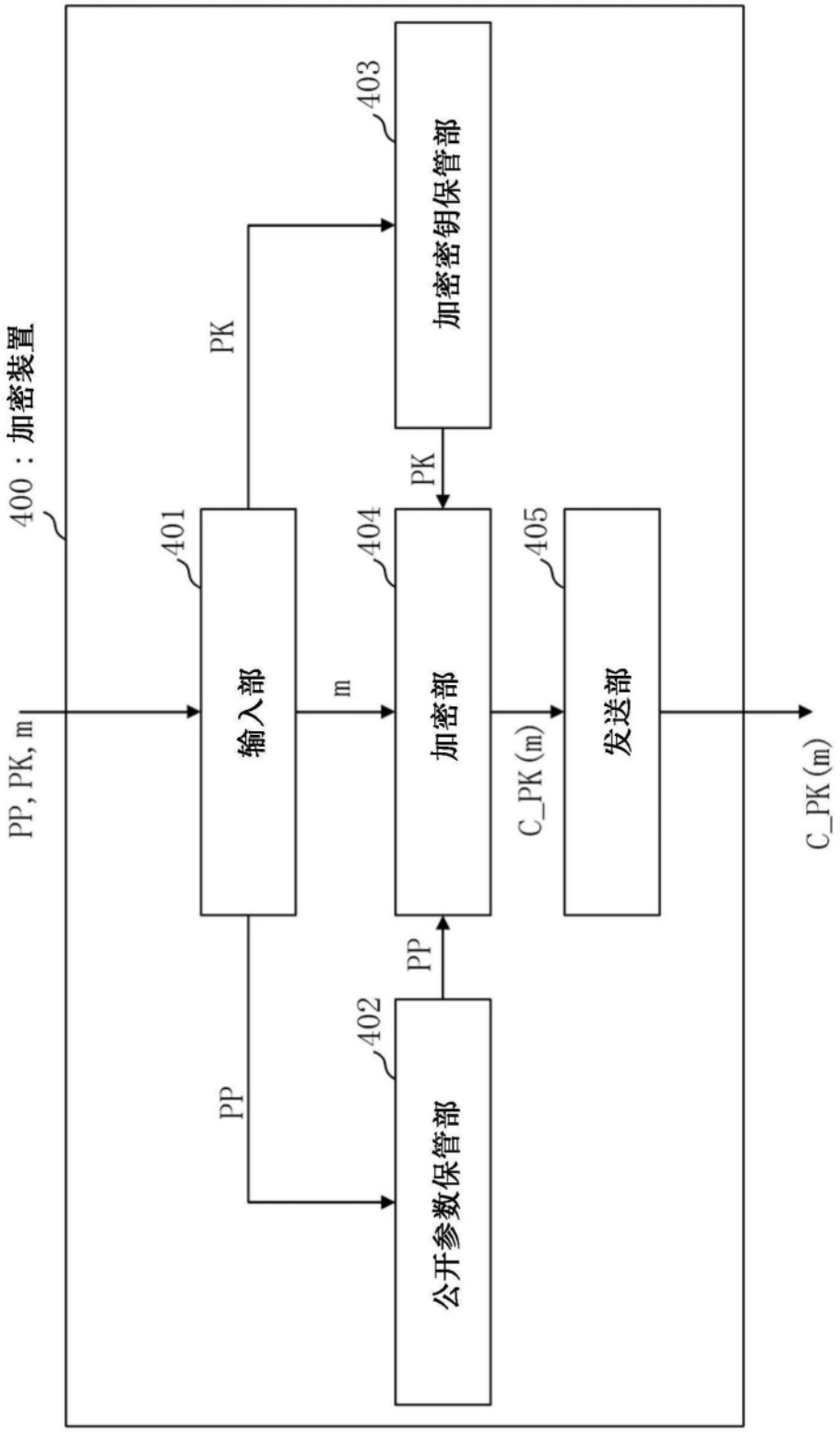

400：加密装置
PP, PK, m
输入部
401
PK
加密密钥保管部
403
PK
m
加密部
404
C_PK(m)
发送部
405
C_PK(m)
PP
公开参数保管部
402
PP

图4

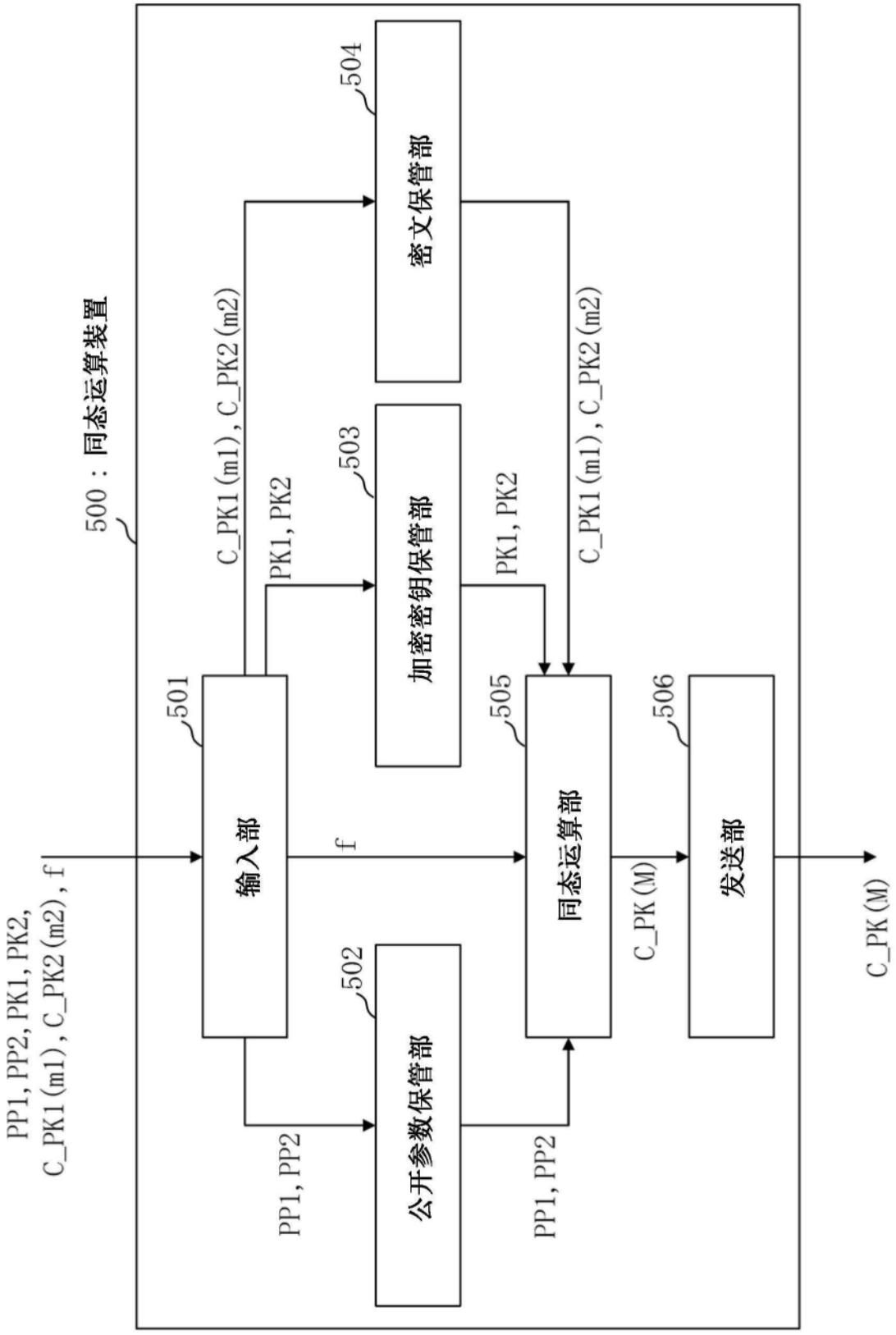

500：同态运算装置
PP1, PP2, PK1, PK2,
C_PK1(m1), C_PK2(m2), f
501
输入部
502
公开参数保管部
503
加密密钥保管部
504
密文保管部
505
同态运算部
506
发送部
C_PK1(m1), C_PK2(m2)
PK1, PK2
f
PP1, PP2
C_PK(M)
C_PK(M)

图5

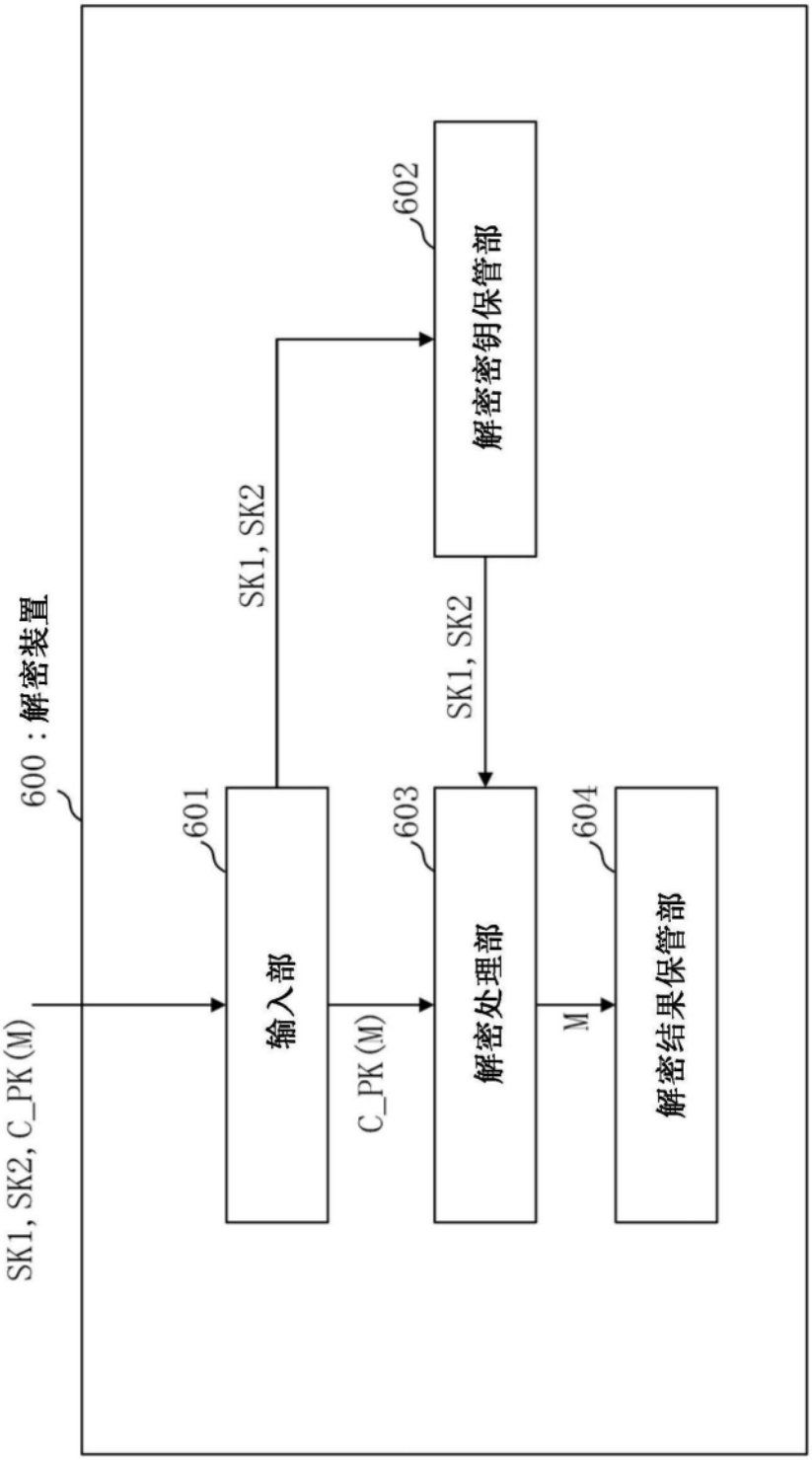

600：解密装置
SK1, SK2, C_PK(M)
601
输入部
C_PK(M)
603
解密处理部
M
604
解密结果保管部
SK1, SK2
602
解密密钥保管部
SK1, SK2

图6

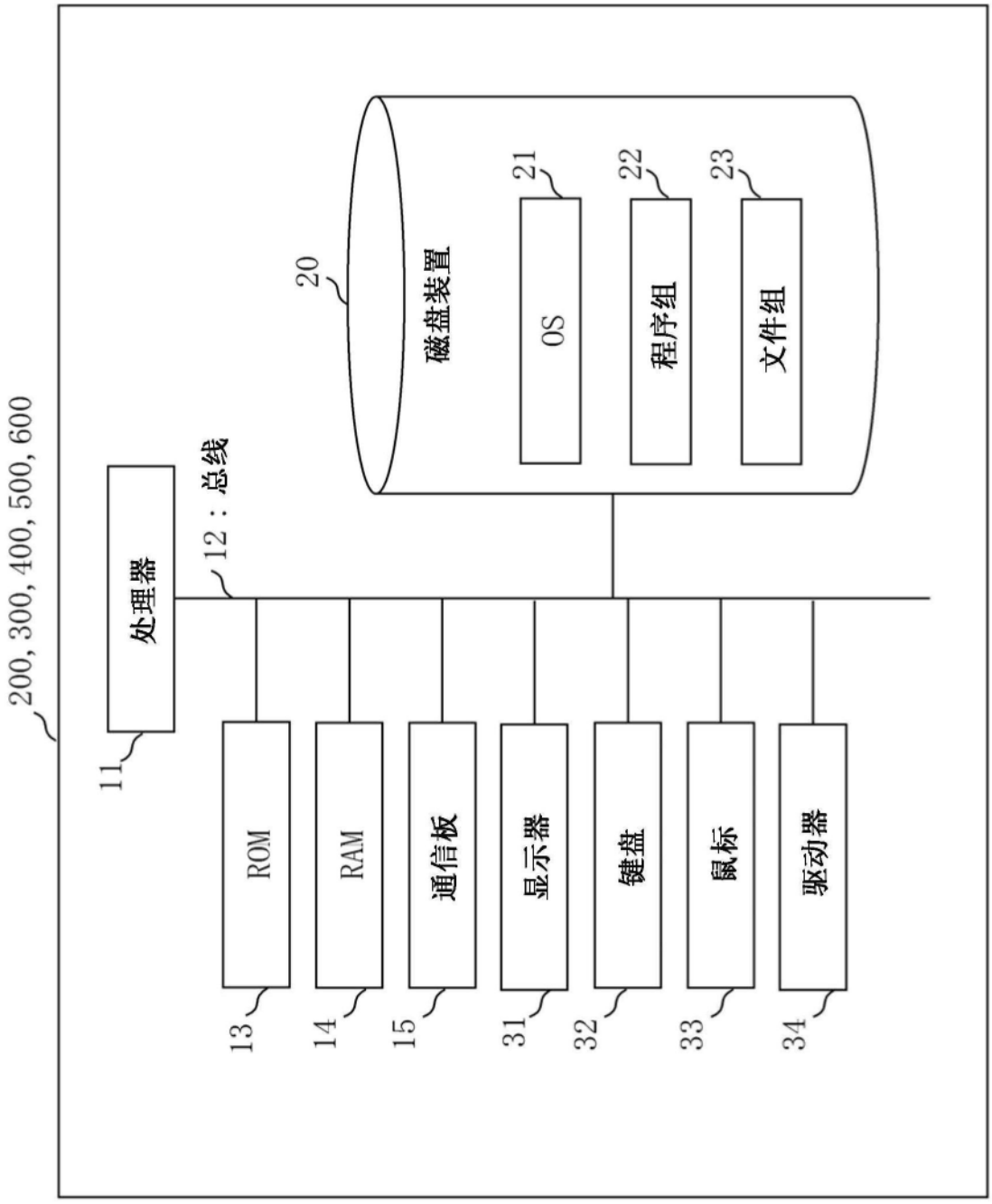

200, 300, 400, 500, 600
处理器
11
12：总线
磁盘装置
20
OS
21
程序组
22
文件组
23
ROM
13
RAM
14
通信板
15
显示器
31
键盘
32
鼠标
33
驱动器
34

图7

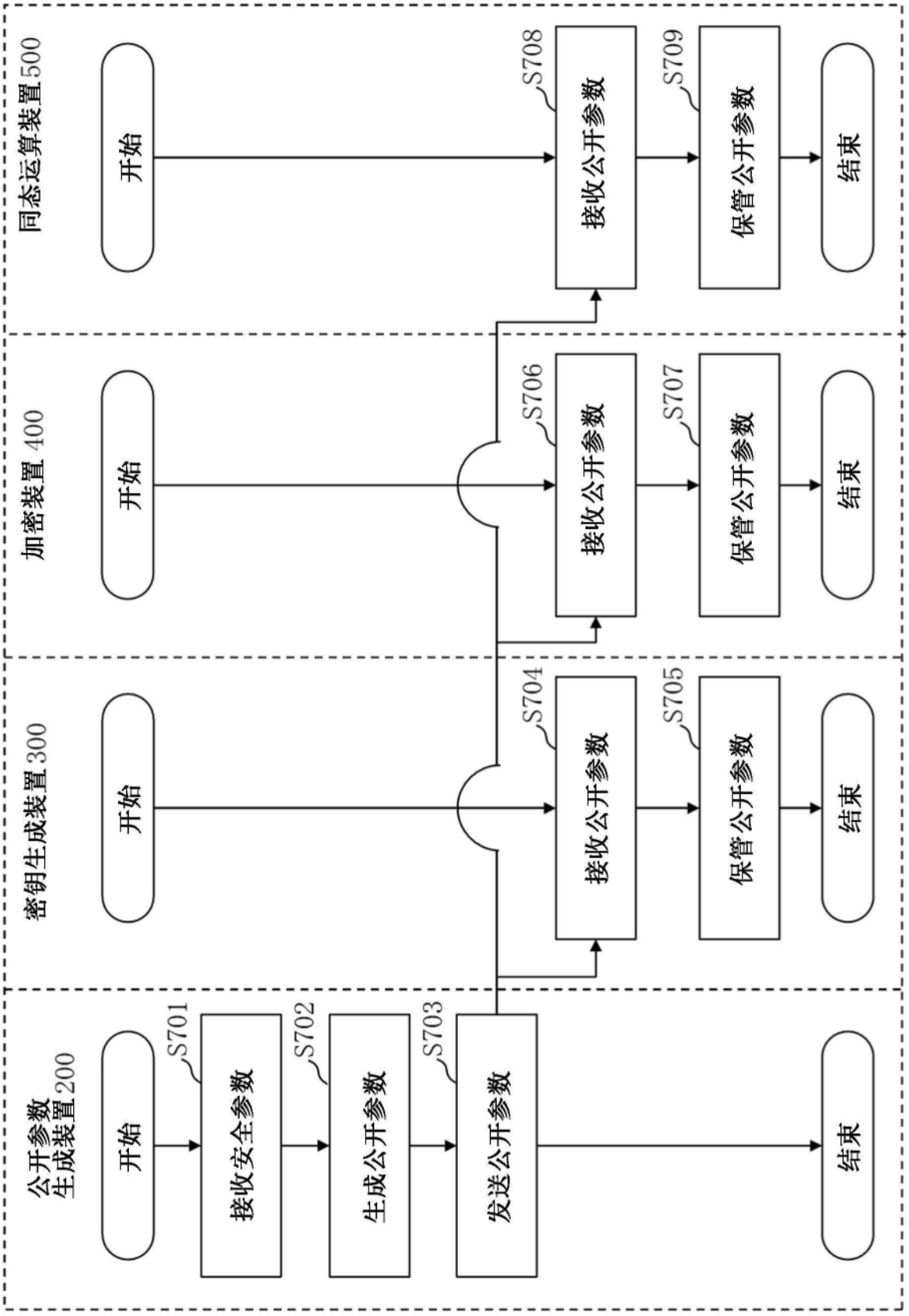

公开参数生成装置200
开始
S701
接收安全参数
S702
生成公开参数
S703
发送公开参数
结束
密钥生成装置300
开始
S704
接收公开参数
S705
保管公开参数
结束
加密装置400
开始
S706
接收公开参数
S707
保管公开参数
结束
同态运算装置500
开始
S708
接收公开参数
S709
保管公开参数
结束

图8

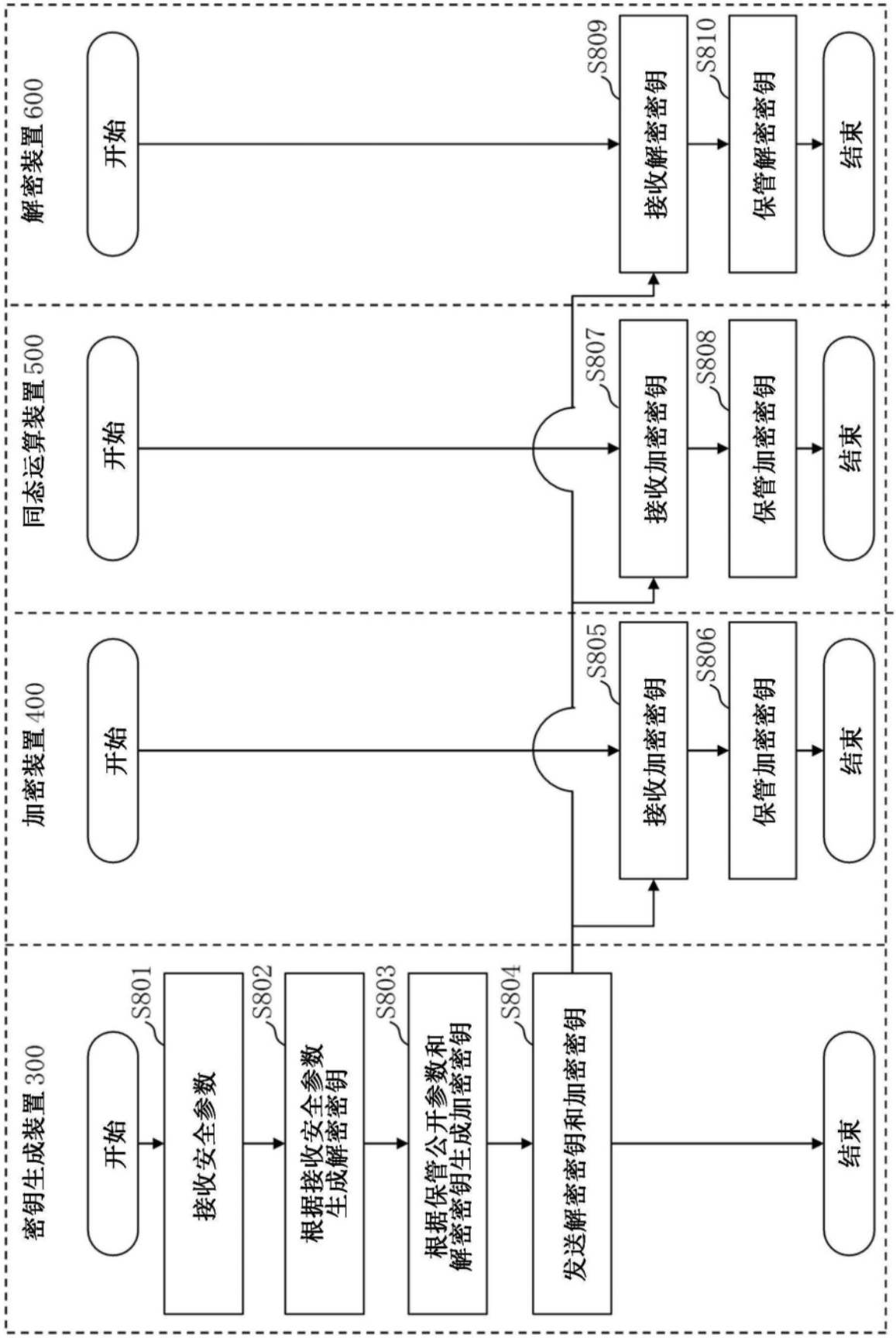

密钥生成装置 300
开始
S801
接收安全参数
S802
根据接收安全参数生成解密密钥
S803
根据保管公开参数和解密密钥生成加密密钥
S804
发送解密密钥和加密密钥
结束
加密装置 400
开始
S805
接收加密密钥
S806
保管加密密钥
结束
同态运算装置 500
开始
S807
接收加密密钥
S808
保管加密密钥
结束
解密装置 600
开始
S809
接收解密密钥
S810
保管解密密钥
结束

图9

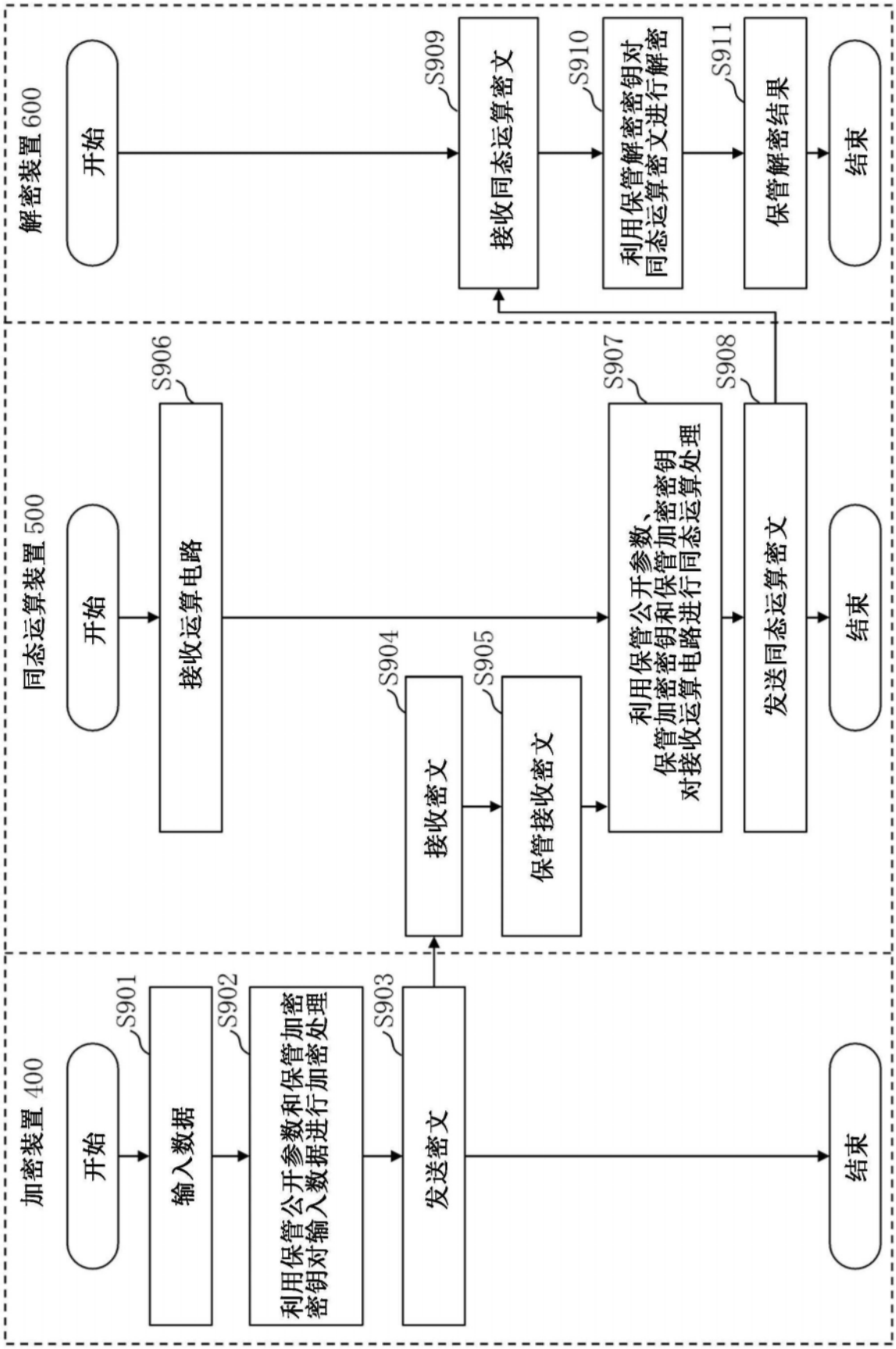

加密装置 400
开始
S901
输入数据
S902
利用保管公开参数和保管加密密钥对输入数据进行加密处理
S903
发送密文
结束
同态运算装置 500
开始
S906
接收运算电路
S904
接收密文
S905
保管接收密文
S907
利用保管公开参数、保管加密密钥和保管加密密钥对接收运算电路进行同态运算处理
S908
发送同态运算密文
结束
解密装置 600
开始
S909
接收同态运算密文
S910
利用保管解密密钥对同态运算密文进行解密
S911
保管解密结果
结束

图10

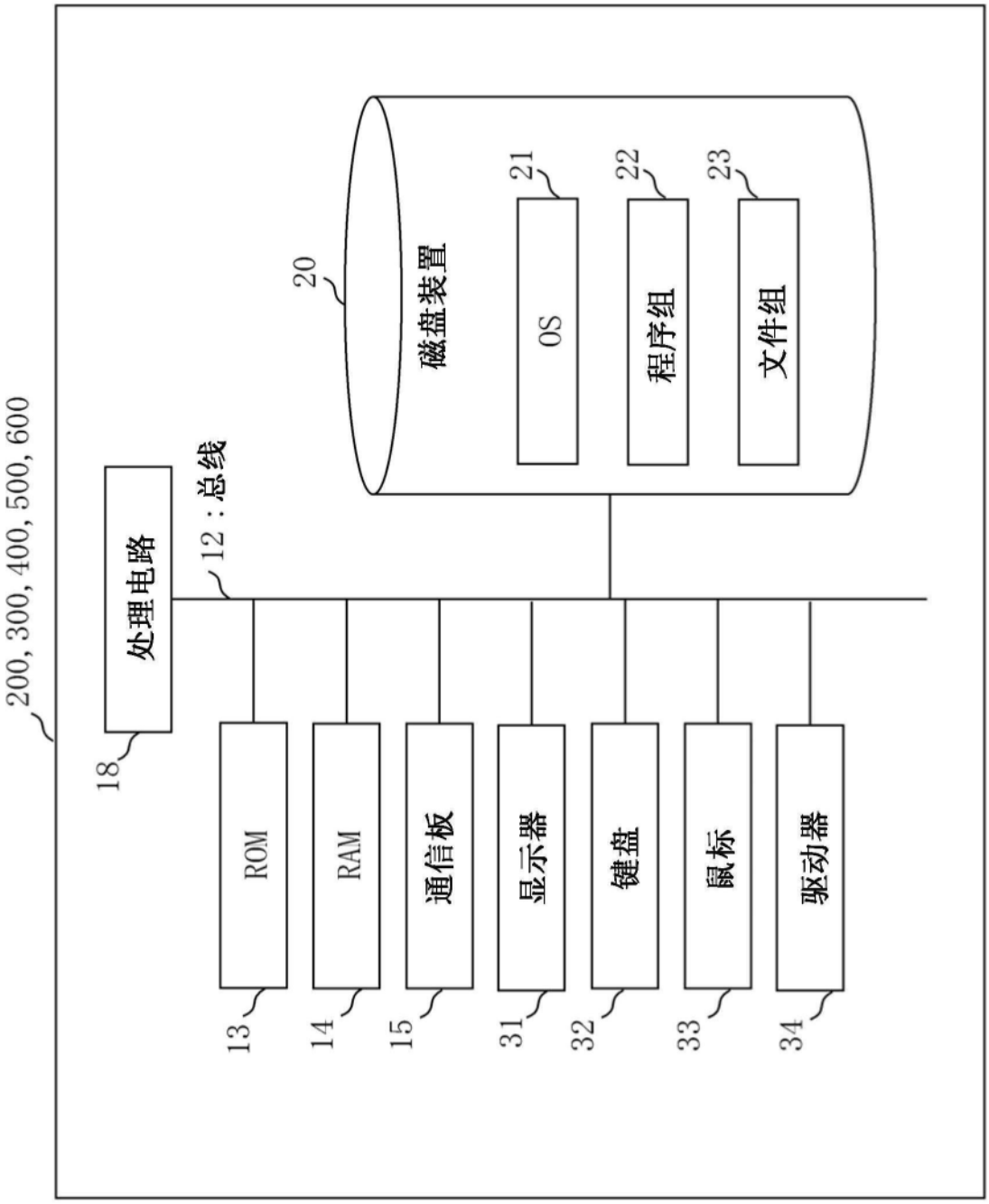

200, 300, 400, 500, 600
处理电路
18
12：总线
磁盘装置
20
OS
21
程序组
22
文件组
23
ROM
13
RAM
14
通信板
15
显示器
31
键盘
32
鼠标
33
驱动器
34

图11