(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105339995 B
(45)授权公告日 2018.04.06

(21)申请号 201480034506.2

(22)申请日 2014.06.30

(65)同一申请的已公布的文献号
申请公布号 CN 105339995 A

(43)申请公布日 2016.02.17

(30)优先权数据
2013-149156 2013.07.18 JP

(85)PCT国际申请进入国家阶段日
2015.12.17

(86)PCT国际申请的申请数据
PCT/JP2014/067352 2014.06.30

(87)PCT国际申请的公布数据
WO2015/008607 JA 2015.01.22

(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 吉田丽生 山本刚 小林铁太郎

(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)
H04L 9/08(2006.01)

(56)对比文件
JP 2012212031 A,2012.11.01,
CN 102549576 A,2012.07.04,
CN 102594570 A,2012.07.18,
JP H11161164 A,1999.06.18,
US 2005066174 A1,2005.03.24,
David Galindo.THE SECURITY OF PSEC-KEM VERSUS ECIES-KEM.《Twenty-sixth Symposium onInformation Theory in the Benelux》.2005,17-27.

审查员 路丽芳

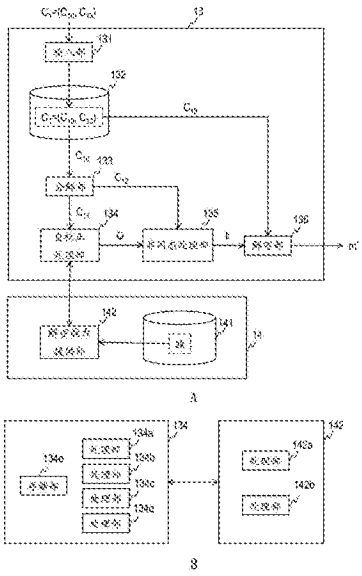
权利要求书4页 说明书14页 附图10页

(54)发明名称

解密装置、解密能力提供装置、其方法、以及记录介质

(57)摘要

解密装置(13)在与解密能力提供装置之间进行自校正处理，得到第一密文的解密值，进行使用了对应于或来自于第一密文的解密值的值和附加值的非同态运算，输出明文，该解密能力提供装置保持用于对能够通过同态运算而解密的第一密文进行解密的解密密钥。



CN 105339995 B

1.一种解密装置,其特征在于,

在解密装置中,具有:

自校正处理部,在与解密能力提供装置之间进行自校正处理,得到第一密文的解密值,该解密能力提供装置保持用于对能够通过同态运算而解密的所述第一密文进行解密的解密密钥;以及

非同态处理部,进行使用了所述第一密文的解密值、和附加值的非同态运算,输出明文,

所述明文是对应于或来自于包含所述第一密文的信息的第二密文的解密值,

所述第一密文包含对对应于或来自于随机值的值进行加密而得到的值,

所述附加值包含对应于或来自于包含所述明文和所述随机值的信息的值。

2.一种解密装置,其特征在于,

在解密装置中,具有:

自校正处理部,在与解密能力提供装置之间进行自校正处理,得到第一密文的解密值,该解密能力提供装置保持用于对能够通过同态运算而解密的所述第一密文进行解密的解密密钥;以及

非同态处理部,进行使用了所述第一密文的解密值、和附加值的非同态运算,输出明文,

所述明文是对应于或来自于包含所述第一密文的信息的第二密文的解密值,

所述第一密文包含对对应于或来自于包含所述明文的信息的值进行加密而得到的值,

所述附加值包含对应于或来自于包含所述第一密文和随机值的信息的值。

3.一种解密装置,其特征在于,

在解密装置中,具有:

自校正处理部,在与解密能力提供装置之间进行自校正处理,得到第一密文的解密值,该解密能力提供装置保持用于对能够通过同态运算而解密的所述第一密文进行解密的解密密钥;以及

非同态处理部,进行使用了所述第一密文的解密值、和附加值的非同态运算,输出明文,

所述明文是对应于或来自于包含所述第一密文的信息的第二密文的解密值,

所述第一密文是对对应于或来自于包含所述明文和随机值的信息的值进行加密而得到的值,

所述附加值是对应于或来自于包含所述随机值的信息的值。

4.如权利要求1-3的任一项所述的解密装置,其中,

所述第一密文关于所述第一密文的解密值而OW－CPA安全,

所述第二密文关于所述明文而IND－CCA安全。

5.一种解密能力提供装置,其特征在于,

在解密能力提供装置中,具有:

存储部,保持用于对能够通过同态运算而解密的第一密文进行解密的解密密钥;以及

解密能力提供部,从进行使用了所述第一密文的解密值、和附加值的非同态运算而输出明文的解密装置,得到对应于或来自于所述第一密文的信息,将用于所述解密装置通过

自校正处理而得到所述第一密文的解密值的信息输出至所述解密装置而不是使用所述解密密钥而向所述解密装置提供所述解密密钥的信息，

所述明文是对应于或来自于包含所述第一密文的信息的第二密文的解密值，

所述第一密文包含对对应于或来自于随机值的值进行加密而得到的值，

所述附加值包含对应于或来自于包含所述明文和所述随机值的信息的值。

6.一种解密能力提供装置，其特征在于，

在解密能力提供装置中，具有：

存储部，保持用于对能够通过同态运算而解密的第一密文进行解密的解密密钥；以及

解密能力提供部，从进行使用了所述第一密文的解密值、和附加值的非同态运算而输出明文的解密装置，得到对应于或来自于所述第一密文的信息，将用于所述解密装置通过自校正处理而得到所述第一密文的解密值的信息输出至所述解密装置而不是使用所述解密密钥而向所述解密装置提供所述解密密钥的信息，

所述明文是对应于或来自于包含所述第一密文的信息的第二密文的解密值，

所述第一密文包含对对应于或来自于包含所述明文的信息的值进行加密而得到的值，

所述附加值包含对应于或来自于包含所述第一密文和随机值的信息的值。

7.一种解密能力提供装置，其特征在于，

在解密能力提供装置中，具有：

存储部，保持用于对能够通过同态运算而解密的第一密文进行解密的解密密钥；以及

解密能力提供部，从进行使用了所述第一密文的解密值、和附加值的非同态运算而输出明文的解密装置，得到对应于或来自于所述第一密文的信息，将用于所述解密装置通过自校正处理而得到所述第一密文的解密值的信息输出至所述解密装置而不是使用所述解密密钥而向所述解密装置提供所述解密密钥的信息，

所述明文是对应于或来自于包含所述第一密文的信息的第二密文的解密值，

所述第一密文包含对对应于或来自于包含所述明文和随机值的信息的值进行加密而得到的值，

所述附加值包含对应于或来自于包含所述随机值的信息的值。

8.如权利要求5-7的任一项所述的解密能力提供装置

所述第一密文关于所述第一密文的解密值而OW－CPA安全，

所述第二密文关于所述明文而IND－CCA安全。

9.一种解密方法，其特征在于，

在解密方法中，具有：

自校正处理部在与解密能力提供装置之间进行自校正处理，得到第一密文的解密值的步骤，该解密能力提供装置保持用于对能够通过同态运算而解密的所述第一密文进行解密的解密密钥；以及

非同态处理部进行使用了所述第一密文的解密值、和附加值的非同态运算，输出明文的步骤，

所述明文是对应于或来自于包含所述第一密文的信息的第二密文的解密值，

所述第一密文包含对对应于或来自于随机值的值进行加密而得到的值，

所述附加值包含对应于或来自于包含所述明文和所述随机值的信息的值。

10.一种解密方法,其特征在于,

在解密方法中,具有:

自校正处理部在与解密能力提供装置之间进行自校正处理,得到第一密文的解密值的步骤,该解密能力提供装置保持用于对能够通过同态运算而解密的所述第一密文进行解密的解密密钥;以及

非同态处理部进行使用了所述第一密文的解密值、和附加值的非同态运算,输出明文的步骤,

所述明文是对应于或来自于包含所述第一密文的信息的第二密文的解密值,

所述第一密文包含对对应于或来自于包含所述明文的信息的值进行加密而得到的值,

所述附加值包含对应于或来自于包含所述第一密文和随机值的信息的值。

11.一种解密方法,其特征在于,

在解密方法中,具有:

自校正处理部在与解密能力提供装置之间进行自校正处理,得到第一密文的解密值的步骤,该解密能力提供装置保持用于对能够通过同态运算而解密的所述第一密文进行解密的解密密钥;以及

非同态处理部进行使用了所述第一密文的解密值、和附加值的非同态运算,输出明文的步骤,

所述明文是对应于或来自于包含所述第一密文的信息的第二密文的解密值,

所述第一密文是对对应于或来自于包含所述明文和随机值的信息的值进行加密而得到的值,

所述附加值是对应于或来自于包含所述随机值的信息的值。

12.一种解密能力提供方法,其特征在于,

在解密能力提供方法中,具有:

解密能力提供部从进行使用了能够通过同态运算而解密的第一密文的解密值、和附加值的非同态运算而输出明文的解密装置,得到与所述第一密文对应的信息的步骤;以及

所述解密能力提供部将用于所述解密装置通过自校正处理而得到所述第一密文的解密值的信息输出至所述解密装置而不是使用用于对所述第一密文进行解密的解密密钥而向所述解密装置提供所述解密密钥的信息的步骤,

所述明文是对应于或来自于包含所述第一密文的信息的第二密文的解密值,

所述第一密文包含对对应于或来自于随机值的值进行加密而得到的值,

所述附加值包含对应于或来自于包含所述明文和所述随机值的信息的值。

13.一种解密能力提供方法,其特征在于,

在解密能力提供方法中,具有:

解密能力提供部从进行使用了能够通过同态运算而解密的第一密文的解密值、和附加值的非同态运算而输出明文的解密装置,得到与所述第一密文对应的信息的步骤;以及

所述解密能力提供部将用于所述解密装置通过自校正处理而得到所述第一密文的解密值的信息输出至所述解密装置而不是使用用于对所述第一密文进行解密的解密密钥而向所述解密装置提供所述解密密钥的信息的步骤,

所述明文是对应于或来自于包含所述第一密文的信息的第二密文的解密值,

所述第一密文包含对对应于或来自于包含所述明文的信息的值进行加密而得到的值，

所述附加值包含对应于或来自于包含所述第一密文和随机值的信息的值。

14.一种解密能力提供方法，其特征在于，

在解密能力提供方法中，具有：

解密能力提供部从进行使用了能够通过同态运算而解密的第一密文的解密值、和附加值的非同态运算而输出明文的解密装置，得到与所述第一密文对应的信息的步骤；以及

所述解密能力提供部将用于所述解密装置通过自校正处理而得到所述第一密文的解密值的信息输出至所述解密装置而不是使用用于对所述第一密文进行解密的解密密钥而向所述解密装置提供所述解密密钥的信息的步骤，

所述明文是对应于或来自于包含所述第一密文的信息的第二密文的解密值，

所述第一密文包含对对应于或来自于包含所述明文和随机值的信息的值进行加密而得到的值，

所述附加值包含对应于或来自于包含所述随机值的信息的值。

15.一种计算机可读取的记录介质，

存储了用于使计算机作为权利要求1至4的任一项所述的解密装置而发挥作用的程序。

16.一种计算机可读取的记录介质，

存储了用于使计算机作为权利要求5至8的任一项所述的解密能力提供装置而发挥作用的程序。

解密装置、解密能力提供装置、其方法、以及记录介质

技术领域

[0001] 本发明涉及云密钥管理型的解密技术。

背景技术

[0002] 为了对通过公开密钥密码方式、公共密钥密码方式等密码方式而加密的密文进行解密，需要特定的解密密钥。没有保持解密密钥的解密装置用于得到密文的解密结果的以往方法之一是，保持有解密密钥的外部装置向解密装置提供解密密钥，解密装置使用该解密密钥来进行密文的解密的方法。用于解密装置得到密文的解密结果的其他以往方法是，解密装置将密文提供给外部装置，外部装置对密文进行解密而将其解密结果提供给解密装置的方法。

[0003] 但是，在前者的方法中，由于解密密钥本身被提供给解密装置，所以存在安全性的问题。另一方面，在后者的方法中，解密装置不能验证解密结果的正确性。

[0004] 作为解决这样的问题的技术，存在使用了自校正(Self-Correcting)技术的云密钥管理型的解密技术(例如，参照专利文献1～3等)。自校正技术是，使用不一定输出正确的计算结果的计算机、系统而始终进行正确的计算(在使用了输出正确的计算结果的计算机的情况下输出正确的计算结果，在使用了不一定输出正确的结果的计算机的情况下，得到正确的计算结果或者得到不能计算的意旨的结果)的技术。在使用了自校正技术的云密钥管理型的解密技术中，保持解密密钥的解密能力提供装置不将解密密钥提供给解密装置，而仅将用于解密装置对密文进行解密的信息提供给解密装置。解密装置能够使用该信息而始终进行正确的解密运算。

[0005] 现有技术文献

[0006] 专利文献

[0007] 专利文献1:国际公开WO/2012/057134号公报

[0008] 专利文献2:国际公开WO/2011/086992号公报

[0009] 专利文献3:国际公开WO/2012/121152号公报

发明内容

[0010] 发明要解决的课题

[0011] 但是，在包含同态运算和非同态运算的解密处理的情况下，不能进行使用了自校正技术的云密钥管理型的解密。

[0012] 用于解决课题的手段

[0013] 解密装置在与解密能力提供装置之间进行自校正处理，得到第一密文的解密值，进行使用了对应于或来自于第一密文的解密值的值和附加值的非同态运算，输出明文，该解密能力提供装置保持用于对能够通过同态运算而解密的第一密文进行解密的解密密钥。

[0014] 发明效果

[0015] 在本发明中，由于仅在能够通过同态运算而解密的第一密文的解密处理中使用自

校正处理，所以即使在解密处理包含同态运算和非同态运算的情况下，也能够进行使用了自校正技术的云密钥管理型的解密。

附图说明

[0016] 图1是实施方式的安全系统的框图。

[0017] 图2是第一实施方式的加密装置的框图。

[0018] 图3A是第一实施方式的解密装置以及解密能力提供装置的框图。图3B是例示第一实施方式的自校正处理部以及解密能力提供部的细节的框图。

[0019] 图4是用于说明第一实施方式的解密处理的图。

[0020] 图5是第二实施方式的加密装置的框图。

[0021] 图6是第二实施方式的解密装置以及解密能力提供装置的框图。

[0022] 图7是用于说明第二实施方式的解密处理的图。

[0023] 图8是第三实施方式的加密装置的框图。

[0024] 图9是第三实施方式的解密装置以及解密能力提供装置的框图。

[0025] 图10是用于说明第三实施方式的解密处理的图。

具体实施方式

[0026] 以下，说明本发明的实施方式。

[0027] [原理]

[0028] 在各实施方式中，解密装置在与解密能力提供装置之间进行自校正处理，得到第一密文的解密值，进行使用了对应于或来自于第一密文的解密值的值和附加值的非同态运算，从而输出明文，该解密能力提供装置保持用于对能够通过同态运算而解密的第一密文进行解密的解密密钥。明文是与包含第一密文的信息对应的第二密文的解密值。“来自(derive)于A的值B”意味着(1)A或A的一部分的信息、或者(2)A或A的一部分的信息的函数值、或者(3)包含A或A的一部分的信息以及其他信息在内的信息的函数值。“来自于A的值B”的例子是“与A对应的B”。“来自于A的值B”的其他例是“基于A的B”。此外“包含A的B”意味着(1)B是A、或者(2)B将A包含于要素、或者(3)B的一部分是A(例如，B的一部分比特表示A)。

[0029] ＜第二密文的例1＞

[0030] 第二密文例如是与能够通过同态运算而解密的第一密文和在解密时成为非同态运算的被运算符的附加值对应的密文(例如，包含第一密文和附加值的密文)。进行这样的第二密文的解密的解密装置在与保持用于对第一密文进行解密的解密密钥的解密能力提供装置之间进行自校正处理，得到第一密文的解密值。第一密文能够通过同态运算而解密，这样的第一密文的解密能够通过使用了自校正技术的公知的云密钥管理型的解密方式来执行(例如，参照专利文献1～3等)。进而，解密装置进行使用了该第一密文的解密值和附加值的非同态运算，输出第二密文的解密值。像这样，由于仅在能够通过同态运算而解密的第一密文的解密处理中使用自校正处理，所以即使第二密文包含在其解密时成为非同态运算的被运算符的附加值，也能够进行使用了自校正技术的云密钥管理型的解密。

[0031] 第一密文的例子包含对来自于随机值的值进行加密而得到的值(例如，是对与随机值对应的值进行加密而得到的值)，此时的附加值的例子是包含与包含明文和随机值的

信息对应的值的值(例如,与明文和随机值对应的值)。在该第一密文的例子中,优选的是,仅从第一密文的解密值难以(例如不可能)得到第二密文的解密值。“难以得到解密值”例如意味着在多项式时间内不能得到解密值。“多项式时间”例如意味着能够通过解密密钥的大小(长度)的多项式来表现的时间(计算时间)。换言之,“多项式时间”例如意味着在将解密密钥的长度(例如比特长)设为x的情况下的能够通过关于x的任意的多项式来表现的时间(计算时间)。第一密文的其他例是包含对来自于包含明文的信息的值进行加密而得到的值的值(例如,是对与明文对应的值进行加密而得到的值),此时的附加值是包含来自于包含第一密文和随机值的信息的值的值(例如,与第一密文和随机值对应的值)。与值θ(例如,随机值、明文等)对应的值的例子是表示值θ的信息或者其映射、示出表示值θ的信息的一部分的信息或者其映射、包含表示值θ的信息在内的信息或者其映射、包含示出表示值θ的信息的一部分的信息在内的信息或者其映射、用于得到值θ的映射的原像的其他映射,包含表示用于得到值θ的映射的原像的信息在内的信息的其他映射。

[0032] 在此,第一密文包含对来自于随机值的值进行加密而得到的值(例如,是对与随机值对应的值进行加密而得到的值),附加值是包含与包含明文和随机值的信息对应的值的值(例如,是与明文和随机值对应的值),在仅从第一密文的解密值难以得到第二密文的解密值的情况下(例如,这不可能的情况下),即使第一密文的信息被提供给解密能力提供装置,只要附加值的信息不被提供给解密能力提供装置,第二密文的解密值的信息就不会泄露给解密能力提供装置。因此,在这样的情况下,也可以是解密装置不扰乱第一密文的信息地将其提供给解密能力提供装置(例如,解密装置将表示第一密文的信息提供给解密能力提供装置),且从解密能力提供装置得到用于得到第一密文的解密值的信息而不是从解密能力提供装置得到解密密钥的信息。由此,能够削减解密装置用于扰乱第一密文的信息的运算量。其中,这是一例,在这样的情况下,也可以是解密装置将扰乱了第一密文的信息提供给解密能力提供装置,从解密能力提供装置得到用于得到解密值的信息。

[0033] 另一方面,在从第一密文的解密值得到第二密文的解密值的信息的情况下,优选解密装置是,将扰乱了第一密文的信息提供给解密能力提供装置,且从解密能力提供装置得到用于得到第一密文的解密值的信息而不是从解密能力提供装置得到解密密钥的信息的结构。

[0034] 第一密文的具体例是具有同态的OW－CPA安全的密码方式的密文(关于第一密文的解密值而OW－CPA安全的密文),与第一密文和附加值对应的第二密文的具体例是不具有同态的IND－CCA安全的密码方式的密文(关于明文而IND－CCA安全的密文)。以下,例示OW－CPA安全的密码方式、和基于其的IND－CCA安全的密码方式。

[0035] ＜方式例1＞

[0036] 方式例1是基于公开密钥密码方式的方式。

[0037] 《OW－CPA安全的密码方式1－1》

[0038] 密钥生成算法:$KeyGen(1^{\lambda}) \rightarrow (pk, sk)$

[0039] 加密算法:$Enc(pk, M_1) \rightarrow C_0$

[0040] 解密算法:$Dec(sk, C_0) \rightarrow M_1'$

[0041] 其中,λ表示是1以上的整数的安全参数,1^{λ}表示由λ个1构成的串,pk表示公开密钥密码方式的公开密钥(加密密钥),sk表示与其对应的秘密密钥(解密密钥)。$KeyGen(1^{\lambda}) \rightarrow$

(pk,sk)表示使用1^{λ}得到(pk,sk)的运算,Enc(pk,M_1)→C_0表示使用pk遵照公开密钥密码方式对M_1进行加密而得到C_0的同态的运算,Dec(sk,C_0)→M_1'表示使用sk遵照公开密钥密码方式对C_0进行解密而得到M_1'的同态的运算。OW－CPA安全的密码方式1－1的例子是RSA密码、ElGamal密码、modified－ElGamal密码、Paillier密码等。

[0042] 《基于OW－CPA安全的密码方式1－1的IND－CCA安全的密码方式1－2》

[0043] 密钥生成算法:KeyGen(1^{λ})→(pk,sk)

[0044] 加密算法:Enc__FO(pk)→C＝(C_1,C_2)＝(Enc(pk,α),FO(Q,r))

[0045] 解密算法:Dec__FO(sk,C)→k

[0046] 其中,r表示随机值,α以及k表示来自于r的值(例如,与r对应的值)。Enc__FO(pk)→C表示使用pk得到与随机值r对应的密文C的运算,Enc(pk,α)→C_1表示使用pk对α进行加密而得到密文C_1的同态的运算。FO(Q,r)→C_2表示得到来自于包含Q和r的信息的值C_2的非同态的运算。其中,Q是来自于α的值。由于α以及k是来自于r的值,所以Q是与明文k对应的值。Dec__FO(sk,C)→k表示使用sk对C进行解密而得到k的非同态的运算。该Dec__FO(sk,C)包含使用秘密密钥sk对密文C_1进行解密而得到复原值Q的同态的运算Dec(sk,C_1)→Q、以及是FO的逆运算的非同态的运算FO^{-1}(Q,C_2)→r。在方式例1的情况下,第一密文是C_1,附加值是C_2,第二密文是C＝(C_1,C_2)。明文是k,例如是公共密钥。其中,明文k也可以是消息。方式例1的具体例是PSEC－KEM方式(参照参考文献1、2等)。

[0047] 参考文献1:PSEC－KEM仕様書、日本電信電話株式会社、NT T情報プラットフォーム研究所、平成20年4月14日

[0048] 参考文献2:INTERNATIONAL STANDARD ISO/IEC 18033-2“Information technology-Security techniques-Encryption algorithms-Part 2:Asymmetric ciphers”

[0049] ＜方式例2＞

[0050] 方式例2是基于基于ID的密码方式的例子。

[0051] 《OW－CPA安全的密码方式2－1》

[0052] 设定算法:Setup(1^{λ})→(PK,msk)

[0053] 密钥生成算法:KeyGen(PK,id,msk)→sk_{id}

[0054] 加密算法:Enc(PK,id,M)→c_0

[0055] 解密算法:Dec(PK,sk_{id},c_0)→M'

[0056] 封装算法:

[0057] $Setup_{EC}$(1^{λ})→pub

[0058] S(1^{λ},pub)→(r,com,dec)

[0059] R(pub,com,dec)→r' or{⊥}

[0060] 其中,PK表示基于ID的密码方式的公开密钥(公开参数),msk表示其主秘密密钥,id表示识别符,sk_{id}表示与识别符id对应的秘密密钥。pub表示封装的公开参数,r、com、dec分别表示随机值,{⊥}表示错误。Setup(1^{λ})→(PK,msk)表示使用1^{λ}得到(PK,msk)的运算,KeyGen(PK,id,msk)→sk_{id}表示使用PK、id、msk得到sk_{id}的运算,Enc(PK,id,M)→c_0表示使用PK、id遵照基于ID的密码方式对M进行加密而得到c_0的同态的运算,Dec(PK,sk_{id},c_0)→M'表示使用PK、sk_{id}遵照基于ID的密码方式对c_0进行解密而得到M'的同态的运算。$Setup_{EC}$(1^{λ})→

pub表示使用1^{λ}得到pub的运算，S(1^{λ},pub)→(r,com,dec)表示使用(1^{λ},pub)得到(r,com,dec)的运算，R(pub,com,dec)→r' or{⊥}表示使用(pub,com,dec)得到r'或者{⊥}的运算。关于基于ID的密码方式的一例，例如在参考文献3中被公开。

[0061] 参考文献3:D.Boneh and M.Franklin,"Identity-Based Encryption from the Weil Pairing,"Adv.in Cryptology|Crypto 2001,LNCS vol.2139,Springer-Verlag,pp.213-229,2001.Full version in SIAM J.Computing 32(3):586-615,2003.

[0062] 《基于OW－CPA安全的密码方式2－1的IND－CCA安全的密码方式2－2》

[0063] 设定算法：

[0064] Setup(1^{λ})→(PK,msk)

[0065] $Setup_{EC}$(1^{λ})→pub

[0066] 加密算法：

[0067] S(1^{λ},pub)→(r,com,dec)

[0068] Enc(PK,com,M|dec)→c_0

[0069] MAC(r,c_0)→tag

[0070] C＝(com,c_0,tag)

[0071] 解密算法：

[0072] KeyGen(PK,com,msk)→sk_{com}

[0073] Dec(PK,sk_{com},c_0)→M'|dec'

[0074] R(pub,com,dec')→r'

[0075] 若r'≠{⊥}则Vefy(r',c_0,tag)

[0076] 若Vefy(r',c_0,tag)≠{⊥}则输出M'。

[0077] 其中，M|dec示出表示M的信息和表示dec的信息之间的连结值，MAC(r,c_0)→tag表示得到对于(r,c_0)的消息认证符tag的运算，Vefy(r',c_0,tag)表示对于(r',c_0)的消息认证符tag的验证结果。

[0078] 在方式例2的情况下，第一密文是对来自于明文M的值(与明文M对应的值)M|dec进行加密而得到的值c_0，附加值是来自于包含第一密文c_0和随机值r的信息(与第一密文c_0和随机值r对应)的消息认证符tag。第二密文是C＝(com,c_0,tag)。方式例2的具体例是对基于ID的密码方式进行了BK变换的方式(参考文献4)。在参考文献4的方式的情况下，明文M是消息。

[0079] 参考文献4:Dan Boneh1,Jonathan Katz,"Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption,"In proceedings of RSA-CT'05,LNCS 3376,pp.87-103,2005.

[0080] ＜第二密文的例2＞

[0081] 第二密文也可以是包含能够通过同态运算而解密的第一密文(例如，第二密文是第一密文，但仅通过第一密文的解密处理不会解密出明文)，且通过使用了来自于第一密文的解密值的值和来自于该第一密文的解密值的附加值的非同态运算而能够复原明文。进行这样的第二密文的解密的解密装置在与保持用于对第一密文进行解密的解密密钥的解密能力提供装置之间进行自校正处理，得到第一密文的解密值。第一密文能够通过同态运算而解密，这样的第一密文的解密能够通过使用了自校正技术的公知的云密钥管理型的解密

方式来执行(例如,参照专利文献1～3等)。进而,解密装置进行使用了来自于该第一密文的解密值的值和来自于该第一密文的解密值的附加值的非同态运算,得到明文并进行输出。像这样,由于仅在能够通过同态运算而解密的第一密文的解密处理中使用自校正处理,所以即使包含在明文的复原时成为非同态运算的被运算符的附加值,也能够进行使用了自校正技术的云密钥管理型的解密。

[0082] 在第二密文的例2的情况下,第一密文也是具有同态的OW－CPA安全的密码方式的密文(关于第一密文的解密值而OW－CPA安全的密文)。第二密文是关于明文而IND－CCA安全的密文。以下,例示第二密文的例2中的IND－CCA安全的密码方式(参照参考文献5)。在该例中也基于前述的OW－CPA安全的密码方式1－1。

[0083] 参考文献5:RSAES-OAEP Encryption Scheme:Algorithm specification and supporting documentation,RSA Laboratories,RSA Security Inc.

[0084] 《基于OW－CPA安全的密码方式1－1的IND－CCA安全的密码方式3－1》

[0085] 密钥生成算法:KeyGen(1^{λ})→(pk,sk)

[0086] 加密算法:Enc(pk,Encode(M_3,P))→C_{31}

[0087] 解密算法:Decode(Dec(sk,C_{31}),P)→M_3'

[0088] 其中,M_3是明文,P是编码参数。P也可以是空(Empty)。Enc(pk,Encode(M_3,P))→C_{31}表示使用pk对Encode(M_3,P)进行加密而得到密文C_{31}的同态的运算。Encode(M_3,P)表示将M_3以及P作为输入,对作为随机值的seed进行内部生成,得到来自于包含M_3、P、seed的信息的值MS＝Encode(M_3,P)的非同态的运算。非同态的运算Encode的具体例是包含参考文献5的EME－OAEP－Encode的运算。Decode(Dec(sk,C_{31}),P)→M_3'表示通过使用了sk的同态的运算Dec而得到C_{31}的解密值MS'＝Dec(sk,C_{31}),通过使用了C_{31}的解密值MS'和来自于MS'的附加值seed'和P的非同态的运算Decode(MS',P)而得到明文M_3'的运算。附加值seed'与随机值seed一致。非同态的运算Decode的具体例是包含参考文献5的EME－OAEP－Decode的运算。第一密文C_{31}是对来自于明文M_3和包含作为随机值的seed的信息的值MS进行加密而得到的值。附加值seed'是来自于包含随机值seed的信息的值。该例的第二密文是第一密文C_{31}。

[0089] 以下,参照附图说明各实施方式。

[0090] [第一实施方式]

[0091] 说明第一实施方式。第一实施方式是对参考文献1中记载的PSEC－KEM方式的第二密文C_{10}进行解密的例子。在本方式中,第一密文是对来自于随机值r的值(与r对应的值)α进行加密而得到的值C_{11},附加值是与包含明文(公共密钥)k(与随机值r和值α对应的值)和随机值r的信息对应的值C_{12}。换言之,附加值C_{12}是来自于包含α以及r的信息的信息。仅从第一密文C_{11}的解密值Q难以得到随机值r,第二密文C_{10}的解密值是从随机值r得到的公共密钥k。也就是说,仅从第一密文C_{11}的解密值Q,难以得到作为第二密文C_{10}的解密值的公共密钥k。

[0092] ＜结构＞

[0093] 如图1所例示那样,第一实施方式的安全系统1具有密钥生成装置11、加密装置12、解密装置13、以及解密能力提供装置14,其构成为能够通过网络进行信息的交换。另外,为了说明的简化,在图1中,将密钥生成装置11、加密装置12、解密装置13、以及解密能力提供装置14各图示一个,但这些的至少一部分装置也可以存在多个。

[0094] 如图2所例示那样,本方式的加密装置12具有存储部121、随机值生成部122、对应

值生成部123、同态加密部124、非同态处理部125、合成部126、加密部127、以及输出部128。如图3所例示那样，本方式的解密装置13具有输入部131、存储部132、分解部133、自校正处理部134、非同态处理部135、以及解密部136。如图3所例示那样，本方式的解密能力提供装置14具有存储部141、以及解密能力提供部142。密钥生成装置11、加密装置12、解密装置13、以及解密能力提供装置14分别是例如通过具备CPU(中央处理单元，central processing unit)等处理器(硬件处理器)、RAM(随机存取存储器，random-access memory)和ROM(只读存储器，read-only memory)等存储器等的通用或者专用的计算机执行规定的程序而构成的装置。计算机也可以具备一个处理器、存储器，也可以具备多个处理器、存储器。该程序也可以被安装在计算机中，也可以预先被记录在ROM等中。此外，也可以不是如CPU那样通过读入程序而实现功能结构的电子电路(circuitry)，而是单独使用实现处理功能的电子电路来构成一部分或者全部的处理部。此外，构成一个装置的电子电路也可以包含多个CPU。从各处理部输出的信息被储存在未图示的临时存储器中，根据需要读出而用于各处理部的处理。

[0095] ＜处理＞

[0096] 密钥生成装置11执行密钥生成算法$KeyGen(1^{\lambda})$，得到公开密钥pk和秘密密钥sk。公开密钥pk被储存在加密装置12(图2)的存储部121中。进而公开密钥pk在其他装置中也被设定。秘密密钥sk被安全地储存在解密能力提供装置14(图3)的存储部141中。

[0097] 之后，如图4所例示那样，加密装置12的随机值生成部122生成随机值r并进行输出(步骤S101)。对应值生成部123将随机值r作为输入，生成来自于随机值r的值(与r对应的值)α、k并进行输出(步骤S102)。例如，H是表示包含表示随机值r的信息在内的信息的哈希(Hash)值的比特串，$H=t|k$，α是t的函数值。K是公共密钥。其中，A|B表示比特串A和B之间的连结(concatenation)。将H的哪个位置设为t以及k事先被决定。

[0098] 同态加密部124将值α和公开密钥pk作为输入，得到第一密文$C_{11}=Enc(pk,\alpha)$并进行输出(步骤S103)。第一密文C_{11}是能够通过同态运算而解密的密文。例如，对于椭圆曲线E上的点P_E，满足$pk=sk\cdot P_E\in E$，$\alpha\in E$，$C_{11}=Enc(pk,\alpha)=\alpha\cdot P_E\in E$。

[0099] 非同态处理部125将随机值r、第一密文C_{11}、以及值α作为输入，得到附加值$C_{12}=FO(\alpha,r)$并进行输出(步骤S104)。附加值C_{12}是在解密时成为非同态运算的被运算符的值。例如，$C_{12}=FO(\alpha,r)$是表示包含表示C_{11}的信息以及表示$Q=\alpha\cdot pk=\alpha\cdot sk\cdot P_E\in E$的信息在内的信息的哈希值的比特串、和表示随机值r的比特串的异或。另外，值α以及明文k与随机值r对应。因此，附加值$C_{12}=FO(\alpha,r)$与明文k和随机值r对应。

[0100] 合成部126将第一密文C_{11}和附加值C_{12}作为输入，得到与其对应的第二密文C_{10}并进行输出(步骤S105)。例如，C_{10}是包含表示C_{11}的信息和表示C_{12}的信息的信息，例如是表示C_{11}的信息(例如，比特串)和表示C_{12}的信息(例如，比特串)的连结值。

[0101] 加密部127将输入消息m和公共密钥k作为输入，遵照公共密钥密码方式通过公共密钥k对输入消息m进行加密，输出公共密钥密文C_{13}(步骤S106)。公共密钥密码方式的例子是AES、Cameria(注册商标)。

[0102] 输出部128将第二密文C_{10}和公共密钥密文C_{13}作为输入，输出包含其的密文$C_1=(C_{10},C_{13})$(步骤S107)。密文C_1通过网络被送出至解密装置13。

[0103] 密文C_1被输入至解密装置13(图3)的输入部131，并被储存至存储部132(步骤

S108)。分解部133将密文$C_1=(C_{10},C_{13})$中包含的第二密文C_{10}作为输入，从第二密文C_{10}得到第一密文C_{11}和附加值C_{12}，输出第一密文C_{11}和附加值C_{12}(步骤S109)。

[0104] 自校正处理部134将第一密文C_{11}作为输入，在与将用于对第一密文C_{11}进行解密的秘密密钥(解密密钥)sk保持在存储部141中的解密能力提供装置14的解密能力提供部142之间进行自校正处理(使用了自校正技术的云密钥管理型的解密处理)，得到第一密文C_{11}的解密值$Q=Dec(sk,C_{11})$并进行输出(步骤S110、S111)。如前述那样，第一密文C_{11}能够通过同态运算而解密。例如，是对于椭圆曲线E上的点sk以及C_{11}的$Q=sk\cdot C_{11}\in E$(其中，$C_{11}=\alpha\cdot P_E\in E$)。

[0105] 《使用了自校正技术的云密钥管理型的解密处理》

[0106] 使用了自校正技术的云密钥管理型的解密处理是在专利文献1～3等中记载的公知技术。以下示出其概要。

[0107] 自校正处理部134将与第一密文C_{11}对应的信息提供给解密能力提供装置14的解密能力提供部142，且从解密能力提供装置14得到用于在自校正处理部134中得到第一密文C_{11}的解密值Q的信息而不是从解密能力提供装置14得到秘密密钥(解密密钥)sk的信息。换言之，解密能力提供装置14的解密能力提供部142从自校正处理部134得到与第一密文C_{11}对应的信息，将用于自校正处理部134通过自校正处理而得到第一密文C_{11}的解密值Q的信息输出至自校正处理部134而不是将秘密密钥(解密密钥)sk的信息提供给解密装置13。自校正处理部134使用从解密能力提供部142提供的信息得到解密值Q。在此，为了避免解密值Q泄露给解密能力提供装置14，被提供给解密能力提供部142的“与第一密文C_{11}对应的信息”必须是扰乱了第一密文C_{11}的信息。但是，在本方式中，仅从解密值Q难以得到作为第二密文C_{10}的解密值的公共密钥k。因此，即使假设解密值Q泄露给解密能力提供装置14，公共密钥k的信息也不会泄露给解密能力提供装置14。在这样的情况下，自校正处理部134不扰乱第一密文C_{11}的信息地提供给解密能力提供部142(将未被扰乱的第一密文C_{11}的信息提供给解密能力提供部142)，也可以从解密能力提供部142得到用于在自校正处理部134中得到解密值Q的信息。

[0108] 使用了自校正技术的云密钥管理型的解密处理的具体例：

[0109] 以下例示使用了自校正技术的云密钥管理型的解密处理。在以下的例子中，G、H是群(例如，循环群等的有限可换群)，f(x)是用于通过秘密密钥sk对作为群H的元的第一密文$x=C_{11}$进行解密而得到群G的元的同态解密函数，X_1、X_2是在群G中具有值的概率变量，x_1是概率变量X_1的实现值，x_2是概率变量X_2的实现值，a、b是互质的自然数。其中，以下的例子不限定本发明，也可以使用其他自校正技术。

[0110] 步骤110a：自校正处理部134的处理部134a输出与第一密文$x=C_{11}$对应的、作为群H的元的第一输入信息τ_1以及第二输入信息τ_2。例如，群H是循环群，循环群H的生成元是μ_h，r1、r2为0以上的随机的自然数，$\tau_1=\mu_h^{r1}x^b$，$\tau_2=\mu_h^{r2}x^a$。a、b的一方也可以是1等的常数。另外，在自校正处理部134的处理部134a不扰乱第一密文C_{11}的信息地将其提供给解密能力提供部142的情况下，自然数r1、r2为1以上的常数，例如$\tau_1=\mu_h x^b$，$\tau_2=\mu_h x^a$。在自然数r1、r2为常数的情况下，不需要随机生成自然数r1、r2的处理。第一输入信息τ_1以及第二输入信息τ_2被送出至解密能力提供部142。

[0111] 步骤111a：解密能力提供部142的处理部142a使用被送出的第一输入信息τ_1以及

在存储部141中储存的秘密密钥sk，以比某概率更大的概率准确地计算$f(\tau_1)$，将所得到的计算结果设为第一输出信息z_1。即，若存在$z_1=f(\tau_1)$的情况，则还存在$z_1\neq f(\tau_1)$的情况。换言之，解密能力提供部142能够计算$f(\tau_1)$，但存在输出包含有意或无意的误差的计算结果的可能性。“某概率”是小于100％且为0％以上的概率。“某概率”的例子是不能忽略的概率，“不能忽略的概率”的例子是在将作为针对安全参数k的广义单调递增函数的多项式设为多项式$\psi(k)$的情况下的$1/\psi(k)$以上的概率。第一输出信息z_1被送出至自校正处理部134。

[0112] 步骤111b：解密能力提供部142的处理部142b使用被送出的第二输入信息τ_2以及在存储部141中储存的秘密密钥sk，以比某概率更大的概率准确地计算$f(\tau_2)$，将所得到的计算结果设为第二输出信息z_2。即，若存在$z_2=f(\tau_2)$的情况，则还存在$z_2\neq f(\tau_2)$的情况。换言之，解密能力提供部142能够计算$f(\tau_2)$，但存在输出包含有意或无意的误差的计算结果的可能性。第二输出信息z_2被送出至自校正处理部134。

[0113] 步骤110b：自校正处理部134的处理部134b根据被送出的第一输出信息z_1生成计算结果$u=f(x)^{b}x_1$。例如，$v=f(\mu_h)$，$u=z_1v^{-r1}$。b以及r1与在处理部134a中所使用的相同。计算结果u被储存至存储部134e。

[0114] 步骤110c：自校正处理部134的处理部134c根据被送出的第二输出信息z_2生成计算结果$v=f(x)^{a}x_2$。例如，$v=z_2v^{-r2}$。a以及r2与在处理部134a中使用的相同。计算结果v被储存至存储部134e。

[0115] 步骤110d：自校正处理部134的处理部134d判定在存储部134e中储存的哪个u以及v的组满足$u^a=v^b$，在满足的情况下，将关于满足$u^a=v^b$的u以及v的组以及满足$a'a+b'b=1$的整数a'、b'的$u^{b'}v^{a'}$作为解密值Q而进行输出。

[0116] 在即使将步骤110a～110d、111a、111b的处理反复规定次数，计算结果u以及v也不满足$u^a=v^b$的情况下，自校正处理部134输出不能解密的意旨的错误信息。另外，在存储部134e中储存有1个以上的v的情况下，在步骤110b和步骤110c之间也可以进行步骤110d的处理。(《使用了自校正技术的云密钥管理型的解密处理》的说明结束)。

[0117] 非同态处理部135将解密值Q和附加值C_{12}作为输入，进行使用了解密值Q和附加值C_{12}的非同态运算$FO^{-1}(Q,C_{12})$而得到r，然后得到第二密文C_{10}的解密值(明文)k并进行输出(步骤S112)。例如，非同态处理部135使用解密值Q和附加值C_{12}得到随机值$r=FO^{-1}(Q,C_{12})$，输出与随机值r对应的公共密钥k。例如，首先，非同态处理部135得到表示包含表示C_{11}的信息以及表示解密值Q的信息在内的信息的哈希值的比特串、和表示附加值C_{12}的比特串的异或，作为表示随机值r的比特串。接着，非同态处理部135得到表示包含表示随机值r的信息在内的信息的哈希值的比特串h，得到满足$h=t|k$的公共密钥k。进而，非同态处理部135使用t的函数值α确认是否满足$C_{11}=\alpha\cdot P_E\in E$，若满足其则输出公共密钥k，若不满足则输出错误。

[0118] 解密部136将公共密钥密文C_{13}和公共密钥k设为输入，遵照公共密钥密码方式通过公共密钥k对公共密钥密文C_{13}进行解密，得到解密值m'并进行输出(步骤S113)。

[0119] [第二实施方式]

[0120] 说明第二实施方式。第二实施方式是对将在参考文献4中记载的基于ID的密码方式进行了BK变换的方式的第二密文进行解密的例子。在本方式中，第一密文是对与明文m对应的值$m|dec$进行加密而得到的值C_{21}，附加值是与第一密文C_{21}和随机值r对应的消息认证

符tag。

[0121] ＜结构＞

[0122] 如图1所例示那样，第二实施方式的安全系统2具有密钥生成装置21、加密装置22、解密装置23、以及解密能力提供装置24，其构成为能够通过网络进行信息的交换。另外，为了说明的简化，在图1中，将密钥生成装置21、加密装置22、解密装置23、以及解密能力提供装置24各图示一个，但这些的至少一部分装置也可以存在多个。

[0123] 如图5所例示那样，本方式的加密装置22具有存储部221、随机值生成部222、同态加密部224、非同态处理部225、以及输出部228。如图6所例示那样，本方式的解密装置23具有输入部231、存储部232、自校正处理部234、非同态处理部235、以及输出部236。如图6所例示那样，本方式的解密能力提供装置24具有存储部241、解密能力提供部242、以及秘密密钥取得部243。如图6所例示那样，本方式的密钥生成装置21具有存储部211、秘密密钥生成部212、以及设定部213。密钥生成装置21、加密装置22、解密装置23、以及解密能力提供装置24分别是例如通过在前述的计算机中读入规定的程序而构成的装置。从各处理部输出的信息被储存至未图示的临时存储器，根据需要读出而用于各处理部的处理。

[0124] ＜处理＞

[0125] 密钥生成装置21的设定部213执行设定算法$Setup(1^{\lambda})$以及$Setup_{EC}(1^{\lambda})$，得到公开密钥(PK,pub)和主秘密密钥msk。公开密钥(PK,pub)被储存至加密装置22(图5)的存储部221。进而公开密钥(PK,pub)在其他装置中也被设定。主秘密密钥msk被安全地储存在密钥生成装置21的存储部211中。

[0126] 如图7所例示那样，加密装置22的随机值生成部222通过$S(1^{\lambda},pub)\rightarrow(r,com,dec)$生成随机值(r,com,dec)并进行输出(步骤S201)。com作为识别符而发挥作用。

[0127] 同态加密部224将公开密钥PK和随机值dec和识别符com和明文m作为输入，通过$Enc(PK,com,m|dec)\rightarrow C_{21}$，对与明文m对应的值m|dec进行加密而得到第一密文C_{21}并进行输出(步骤S203)。第一密文C_{21}是能够通过同态运算而解密的密文。

[0128] 非同态处理部225将随机值r和第一密文C_{21}作为输入，通过$MAC(r,C_{21})\rightarrow tag$，得到对于随机值r和第一密文$C_{21}$的消息认证符tag作为附加值并进行输出(步骤S204)。附加值tag是在解密时成为非同态运算的被运算符的值。

[0129] 输出部228将识别符com和第一密文C_{21}和附加值tag作为输入，输出与其对应的第二密文$C_2=(com,C_{21},tag)$(步骤S207)。例如，第二密文C_2是包含表示识别符com的信息和表示第一密文C_{21}的信息和表示附加值tag的信息的信息，例如是表示识别符com的信息(例如，比特串)和表示第一密文C_{21}的信息(例如，比特串)和表示附加值tag的信息(例如，比特串)之间的连结值。第二密文C_2通过网络被送出至解密装置23。

[0130] 第二密文C_2被输入至解密装置23(图6)的输入部231，被储存至存储部232(步骤S208)。输出部236输出第二密文$C_2=(com,C_{21},tag)$所包含的识别符com(步骤S209a)。识别符com被输入至解密能力提供装置24的秘密密钥取得部243。秘密密钥取得部243将识别符com输出至密钥生成装置21(步骤S209b)。密钥生成装置21的秘密密钥生成部212将识别符com和主秘密密钥msk作为输入，通过$KeyGen(PK,com,msk)\rightarrow sk_{com}$，得到与识别符com对应的秘密密钥$sk_{com}$并进行输出。秘密密钥$sk_{com}$被输入至秘密密钥取得部243，被安全地储存在存储部241中(步骤S209c)。

[0131] 自校正处理部234将第二密文C_2=(com,C_{21},tag)中包含的第一密文C_{21}作为输入，在与保持用于对第一密文C_{21}进行解密的秘密密钥(解密密钥)sk_{com}的解密能力提供装置24的解密能力提供部242之间进行自校正处理(使用了自校正技术的云密钥管理型的解密处理)，得到第一密文C_{21}的解密值m'|dec'=Dec(PK,sk_{com},C_{21})并进行输出(步骤S210、S211)。

[0132] 即，自校正处理部234将与第一密文C_{21}对应的信息提供给解密能力提供装置24的解密能力提供部242，且从解密能力提供装置24得到用于在自校正处理部234中得到第一密文C_{21}的解密值m'|dec'的信息而不是从解密能力提供装置24得到秘密密钥(解密密钥)sk_{com}的信息。换言之，解密能力提供装置24的解密能力提供部242从自校正处理部234得到与第一密文C_{21}对应的信息，将用于自校正处理部234通过自校正处理而得到第一密文C_{21}的解密值m'|dec'的信息输出至自校正处理部234而不将秘密密钥sk_{com}的信息提供给解密装置23。自校正处理部234使用从解密能力提供部242提供的信息得到解密值m'|dec'。在此，为了避免解密值m'|dec'泄露给解密能力提供装置24，优选被提供给解密能力提供部242的“与第一密文C_{21}对应的信息”是扰乱了第一密文C_{21}的信息。另外，步骤S210、S211的具体例是，设为x=C_{21}，设为秘密密钥sk=sk_{com}，将自校正处理部134置换为自校正处理部234，将解密能力提供部142置换为解密能力提供部242而进行的前述的“使用了自校正技术的云密钥管理型的解密处理的具体例”。

[0133] 非同态处理部235进行使用了第一密文C_{21}的解密值m'|dec'和附加值tag的非同态运算，输出第二密文C_2的解密值m'(步骤S212)。例如，非同态处理部235将解密值m'|dec'和第二密文C_2=(com,C_{21},tag)中包含的识别符com和附加值tag作为输入，通过R(pub,com,dec')→r'得到r'，若r'≠{⊥}则判定是否Vefy(r',C_{21},tag)≠{⊥}，若Vefy(r',C_{21},tag)≠{⊥}则输出m'。在其他情况下进行错误结束。

[0134] [第三实施方式]

[0135] 说明第三实施方式。第三实施方式基于前述的<第二密文的例2>。本方式的第一密文是对来自于包含明文m和随机值seed的信息的值MS=Encode(m,P)进行加密而得到的值C_{31}，附加值是随机值seed。

[0136] <结构>

[0137] 如图1所例示那样，第三实施方式的安全系统3具有密钥生成装置31、加密装置32、解密装置33、以及解密能力提供装置34，其构成为能够通过网络进行信息的交换。另外，为了说明的简化，在图1中，将密钥生成装置31、加密装置32、解密装置33、以及解密能力提供装置34各图示一个，但这些至少一部分装置也可以存在多个。

[0138] 如图8所例示那样，本方式的加密装置32具有存储部321、随机值生成部322、同态加密部324、非同态处理部325、变换部326、以及输出部328。如图9所例示那样，本方式的解密装置33具有输入部331、存储部332、复原部333、自校正处理部334、非同态处理部335、输出部236、以及变换部337。如图9所例示那样，本方式的解密能力提供装置34具有存储部341、以及解密能力提供部342。密钥生成装置31、加密装置32、解密装置33、以及解密能力提供装置34分别是例如通过在前述的计算机中读入规定的程序而构成的装置。从各处理部输出的信息被储存至未图示的临时存储器，根据需要读出而用于各处理部的处理。

[0139] <处理>

[0140] 密钥生成装置31执行密钥生成算法KeyGen(1^{λ})，得到公开密钥pk和秘密密钥sk。

公开密钥pk被储存至加密装置32(图8)的存储部321。进而公开密钥pk在其他装置中也被设定。秘密密钥sk被安全地储存在解密能力提供装置34(图9)的存储部341中。在参考文献5的例子中,公开密钥pk是RSA公开密钥(e,n),秘密密钥sk是与RSA公开密钥(e,n)对应的RSA秘密密钥(n,d)。此外,密钥生成装置31输出编码参数P。编码参数P被储存至加密装置32的存储部321以及解密能力提供装置34的存储部341。

[0141] 之后,如图10所例示那样,加密装置32的随机值生成部322以及非同态处理部325将明文m、以及从存储部321读出的编码参数P作为输入,进行非同态运算Encode(m,P)→MS而得到MS。即,随机值生成部322生成随机值seed(步骤S301),非同态处理部325进行与明文m、随机值seed、编码参数P对应的非同态运算而得到MS=Encode(m,P)。例如,非同态处理部325如以下那样得到MS。

[0142] pHash=Hash(P)

[0143] DB=pHash|PS|01|m

[0144] dbMask=MGF(seed)

[0145] makedDB=DB(+)dbMask

[0146] seedMask=MGF(makedDB)

[0147] maskedSeed=seed(+)seedMask

[0148] EM=maskedSeed|maskedDB

[0149] MS=OS2IP(EM)

[0150] 其中,Hash表示P的哈希函数,PS表示零比特串,MGF是掩码生成函数,A(+)B表示A和B的异或,OS2IP是变换函数(步骤S302)。

[0151] 同态加密部324将MS(来自于包含明文m和随机值seed的信息的值)、以及从存储部321读出的公开密钥pk作为输入,通过Enc(pk,MS)→C_{31}对MS进行加密而得到第一密文C_{31}并进行输出(步骤S303)。第一密文C_{31}是能够通过同态运算而解密的密文。

[0152] 变换部326将第一密文C_{31}作为输入,将其输入至变换函数I2OSP而得到密文C_3=I2OSP(C_{31})并进行输出(步骤S305)。密文C_3通过网络被送出至解密装置33。

[0153] 密文C_3被输入至解密装置33(图3)的输入部331,被储存至存储部332(步骤S306)。变换部337从存储部332读出密文C_3,将其输入至I2OSP的反变换函数OS2IP而得到第一密文C_{31}=OS2IP(C_3)并进行输出(步骤S307)。

[0154] 自校正处理部334将第一密文C_{31}作为输入,在与保持用于对第一密文C_{31}进行解密的秘密密钥(解密密钥)sk的解密能力提供装置34的解密能力提供部342之间进行自校正处理(使用了自校正技术的云密钥管理型的解密处理),得到第一密文C_{31}的解密值MS=Dec(sk,C_{31})并进行输出(步骤S310、S311)。

[0155] 即,自校正处理部334将与第一密文C_{31}对应的信息提供给解密能力提供装置34的解密能力提供部342,且从解密能力提供装置34得到用于在自校正处理部334中得到第一密文C_{31}的解密值MS的信息而不是从解密能力提供装置34得到秘密密钥(解密密钥)sk的信息。换言之,解密能力提供装置34的解密能力提供部342从自校正处理部334得到与第一密文C_{31}对应的信息,将用于自校正处理部334通过自校正处理而得到第一密文C_{31}的解密值MS的信息输出至自校正处理部334而不将秘密密钥sk的信息提供给解密装置33。自校正处理部334使用从解密能力提供部342提供的信息而得到解密值MS。在此,为了避免解密值MS泄露给解

密能力提供装置34，优选被提供给解密能力提供部342的“与第一密文C_{31}对应的信息”是扰乱了第一密文C_{31}的信息。另外，步骤S310、S311的具体例是，设为$x=C_{31}$，将自校正处理部134置换为自校正处理部334，将解密能力提供部142置换为解密能力提供部342而进行的前述的“使用了自校正技术的云密钥管理型的解密处理的具体例”。

[0156] 复原部333以及非同态处理部335将解密值MS、以及从存储部332读出的编码参数P作为输入，通过同态运算Decode(MS,P)→m对明文m进行复原并进行输出。即，复原部333根据MS对与明文m对应的值maskedDB和随机值seed进行复原(步骤S312)，非同态处理部335根据其而对明文m进行复原并进行输出，输出部336输出明文m(步骤S313)。这些处理是非同态运算。例如，复原部333使用OS2IP的反变换函数I2OSP得到EM＝I2OSP(MS)，将EM分离为满足EM＝maskedSeed|maskedDB的maskedSeed和maskedDB，得到seedMask＝MGF(makedDB)，可得到seed＝maskedSeed(+)seedMask(步骤S312)。非同态处理部335使用所得到的maskedDB以及seed，得到dbMask＝MGF(seed)，得到DB＝makedDB(+)dbMask，得到pHash＝Hash(P)，得到满足DB＝pHash|PS|01|m的明文m，输出部336输出明文m(步骤S313)。

[0157] [其他变形例等]

[0158] 另外，本发明不限定于上述的实施方式。例如，也可以是至少一部分组的装置经由可移动记录介质来交换信息而不是各装置通过网络交换信息。或者，也可以是至少一部分组的装置经由非可移动的记录介质来交换信息。即，也可以是由这些装置的一部分构成的组合是相同的装置。

[0159] 此外自校正技术不限定于前述。例如，也可以是，群H是群G的直积群$G\times G$，群G是循环群，循环群G的生成元是μ_g，第一密文$x=(c_1,c_2)$，(V,W)是群H的元，$f(V,W)=Y$，r4～r7为0以上的自然数的随机数，$\tau_1=(c_2{}^{b}W^{r4},c_1{}^{b}V^{r4}\mu_g{}^{r5})$，$\tau_2=(c_2{}^{a}W^{r6},c_1{}^{a}V^{r6}\mu_g{}^{r7})$，$u=z_1Y^{-r4}\mu_g{}^{-r5}$，$v=z_2Y^{-r6}\mu g^{-r7}$。

[0160] 在第三实施方式中编码参数P也可以是空。此时，编码参数P不被生成，P作为空而被处理。此外，在各实施方式中比特串也可以是字节串。

[0161] 上述的各种处理不仅按照记载而时序地执行，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地或单独地执行。此外，在不脱离本发明的意旨的范围内能够进行适当变更是不言而喻的。

[0162] 在通过计算机来实现上述的结构的情况下，各装置应具有的功能的处理内容通过程序而记述。该程序在计算机中执行，从而上述处理功能在计算机上被实现。记述了该处理内容的程序能够记录至计算机能够读取的记录介质。计算机能够读取的记录介质的例子是非临时的(non-transitory)记录介质。这样的记录介质的例子是磁记录装置、光盘、光磁记录介质、半导体存储器等。

[0163] 该程序的流通例如通过对记录有该程序的DVD、CD－ROM等可移动记录介质进行销售、转让、借出等而进行。进而，也可以是通过将该程序储存至服务器计算机的存储装置，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从服务器计算机转发的程序临时储存在自己的存储装置中。在执行处理时，该计算机读取在自己的记录装置中储存的程序，执行按照所读取的程序的处理。作为该程序的另一执行方式，也可以是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，也可以在每

次从服务器计算机向该计算机转发程序时，依次执行按照所接受到的程序的处理。

[0165] 在上述实施方式中，在计算机上执行规定的程序而实现了本装置的处理功能，但这些处理功能的至少一部分也可以通过硬件来实现。

[0166] 标号说明

[0167] 1、2、3 安全系统

[0168] 11、21、31 密钥生成装置

[0169] 12、22、32 加密装置

[0170] 13、23、33 解密装置

[0171] 14、24、34 解密能力提供装置

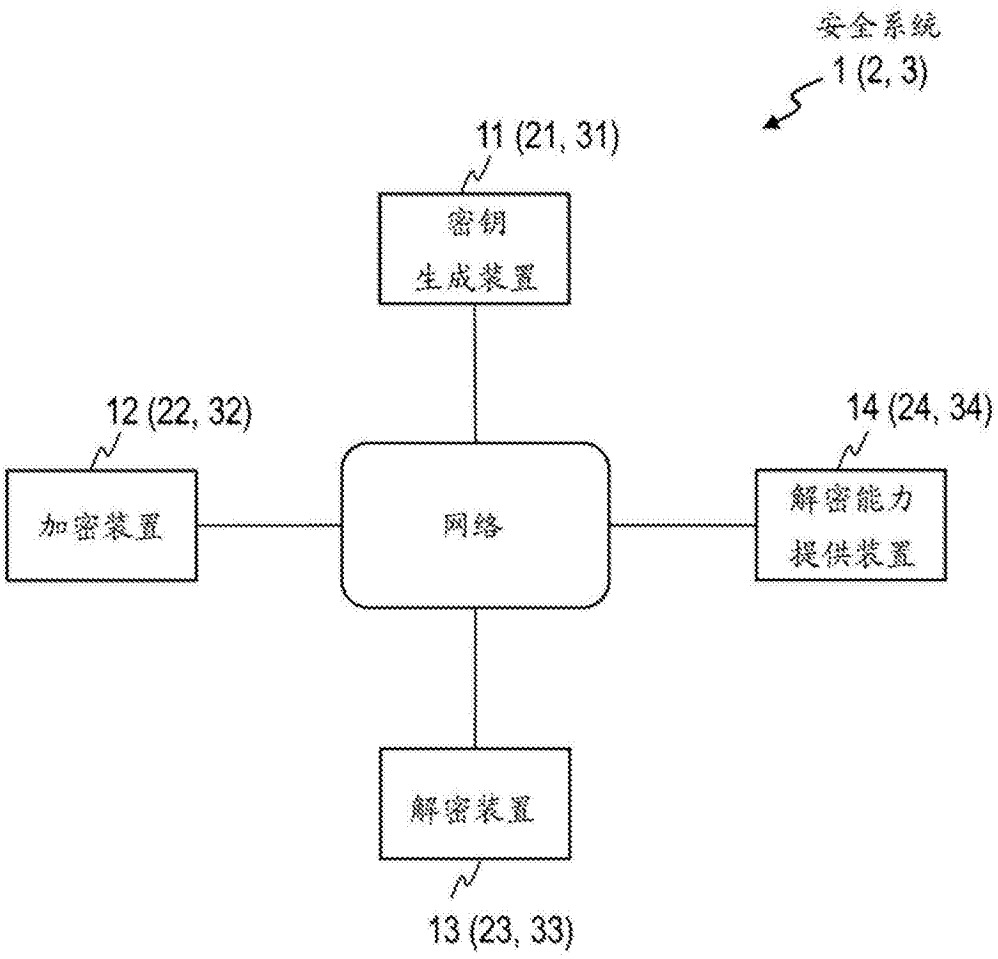

安全系统
1 (2, 3)
11 (21, 31)
密钥
生成装置
12 (22, 32)
加密装置
网络
14 (24, 34)
解密能力
提供装置
解密装置
13 (23, 33)

图1

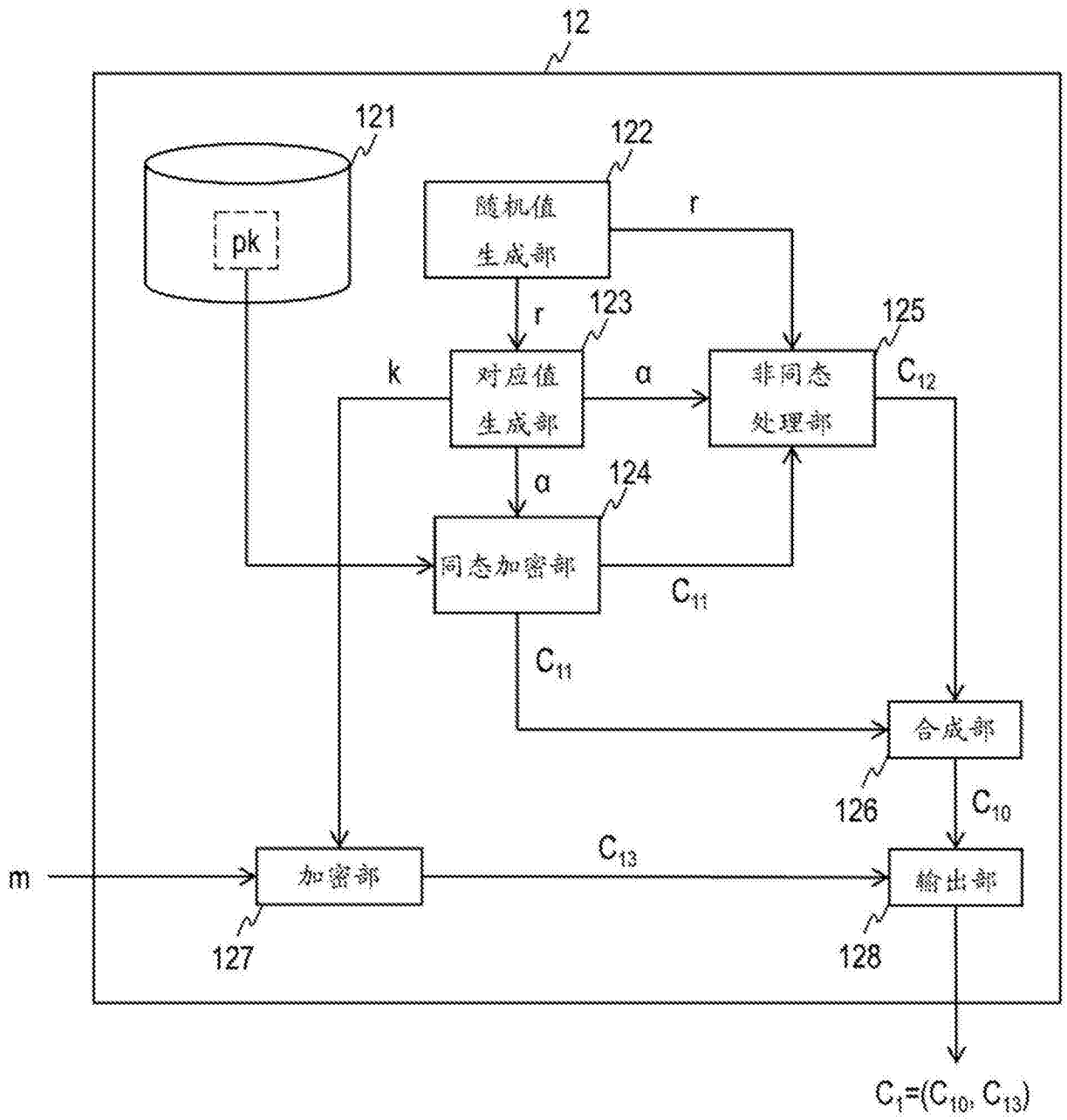

12
121
pk
122
随机值
生成部
r
r
123
对应值
生成部
k
α
125
非同态
处理部
C_{12}
α
124
同态加密部
C_{11}
C_{11}
合成部
126
C_{10}
m
加密部
C_{13}
输出部
127
128
$C_1=(C_{10}, C_{13})$

图2

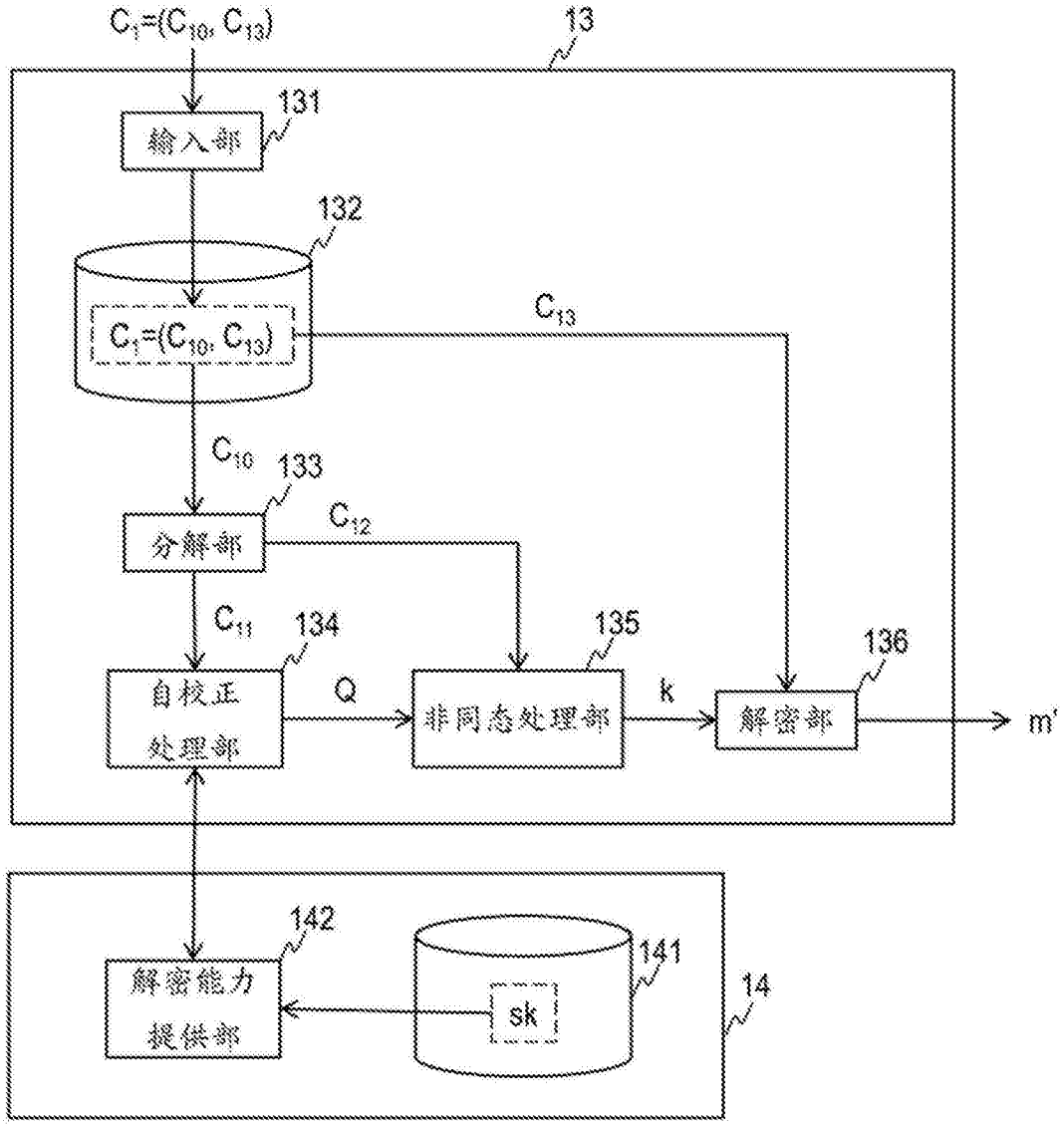

C1=(C10, C13)
13
131
输入部
132
C1=(C10, C13)
C13
C10
133
分解部
C12
C11
134
135
136
自校正
处理部
Q
非同态处理部
k
解密部
m'
142
解密能力
提供部
141
sk
14

图3A

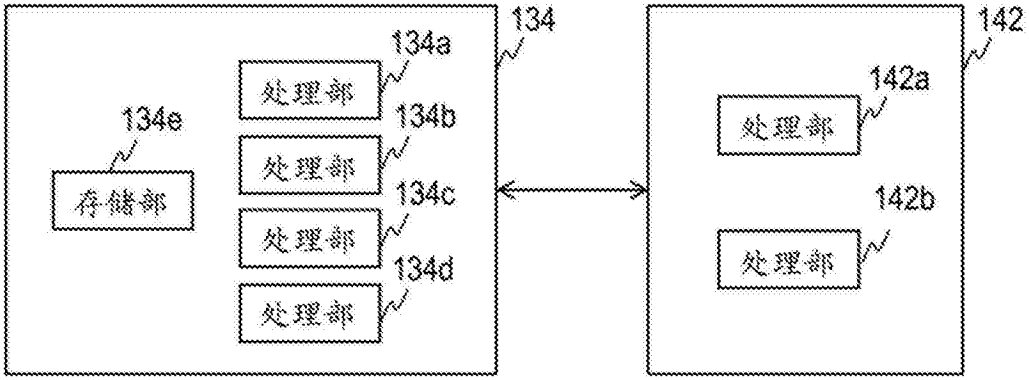

134
134a
处理部
134b
处理部
134c
处理部
134d
处理部
134e
存储部
142
142a
处理部
142b
处理部

图3B

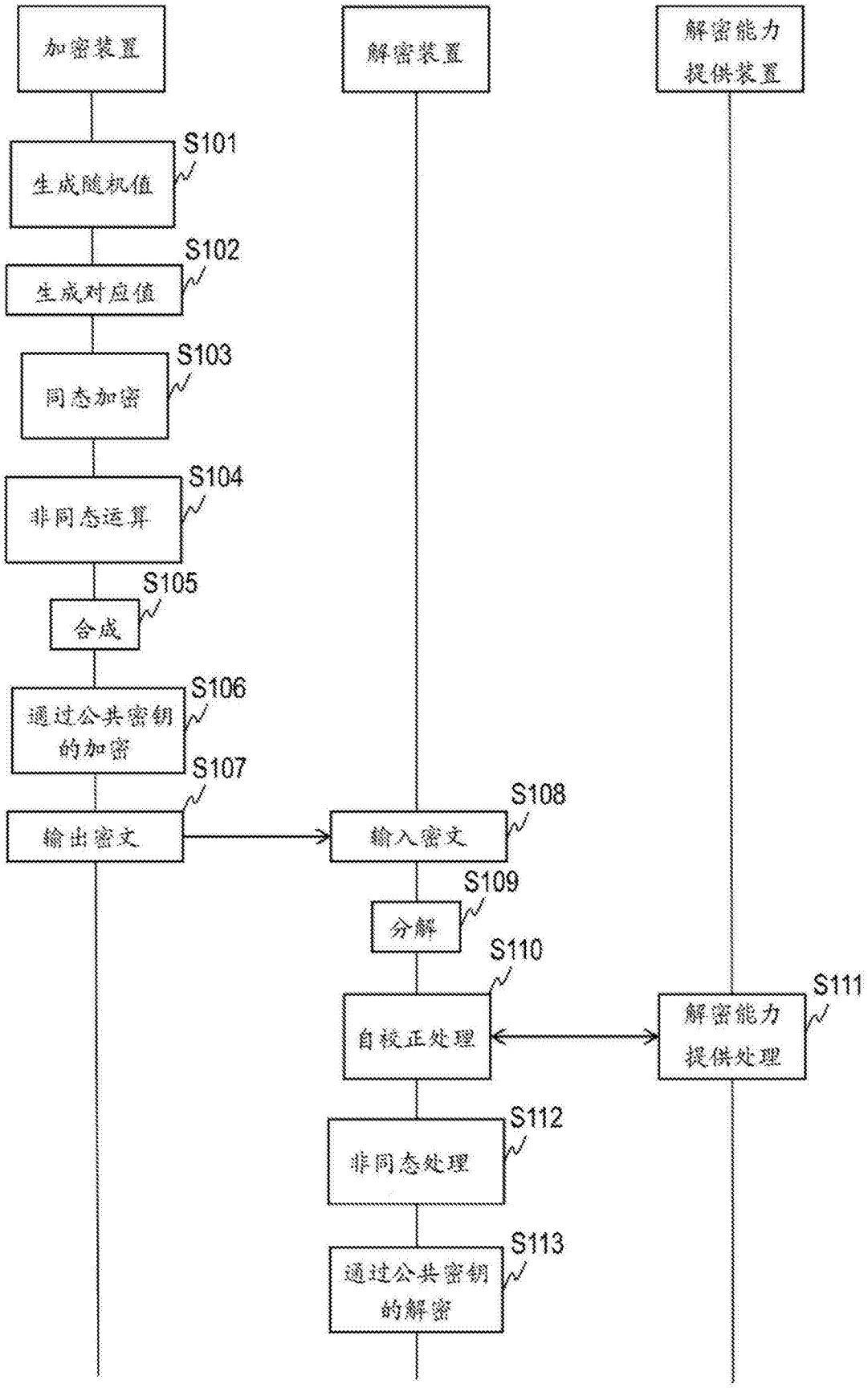

加密装置
解密装置
解密能力提供装置
生成随机值
S101
生成对应值
S102
同态加密
S103
非同态运算
S104
合成
S105
通过公共密钥的加密
S106
输出密文
S107
输入密文
S108
分解
S109
自校正处理
S110
解密能力提供处理
S111
非同态处理
S112
通过公共密钥的解密
S113

图4

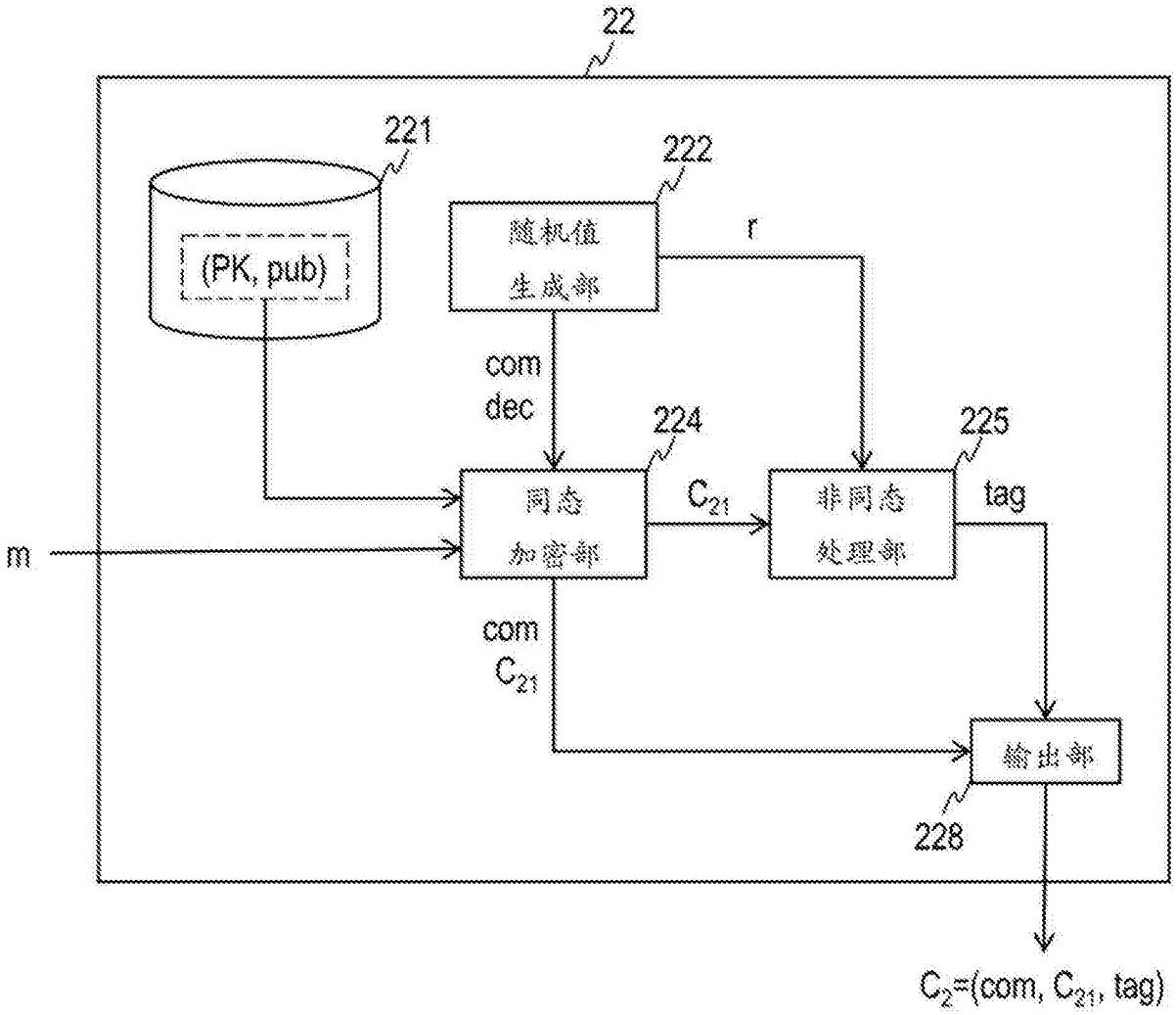

22
221
(PK, pub)
222
随机值
生成部
r
com
dec
224
同态
加密部
C21
225
非同态
处理部
tag
m
com
C21
输出部
228
C2=(com, C21, tag)

图5

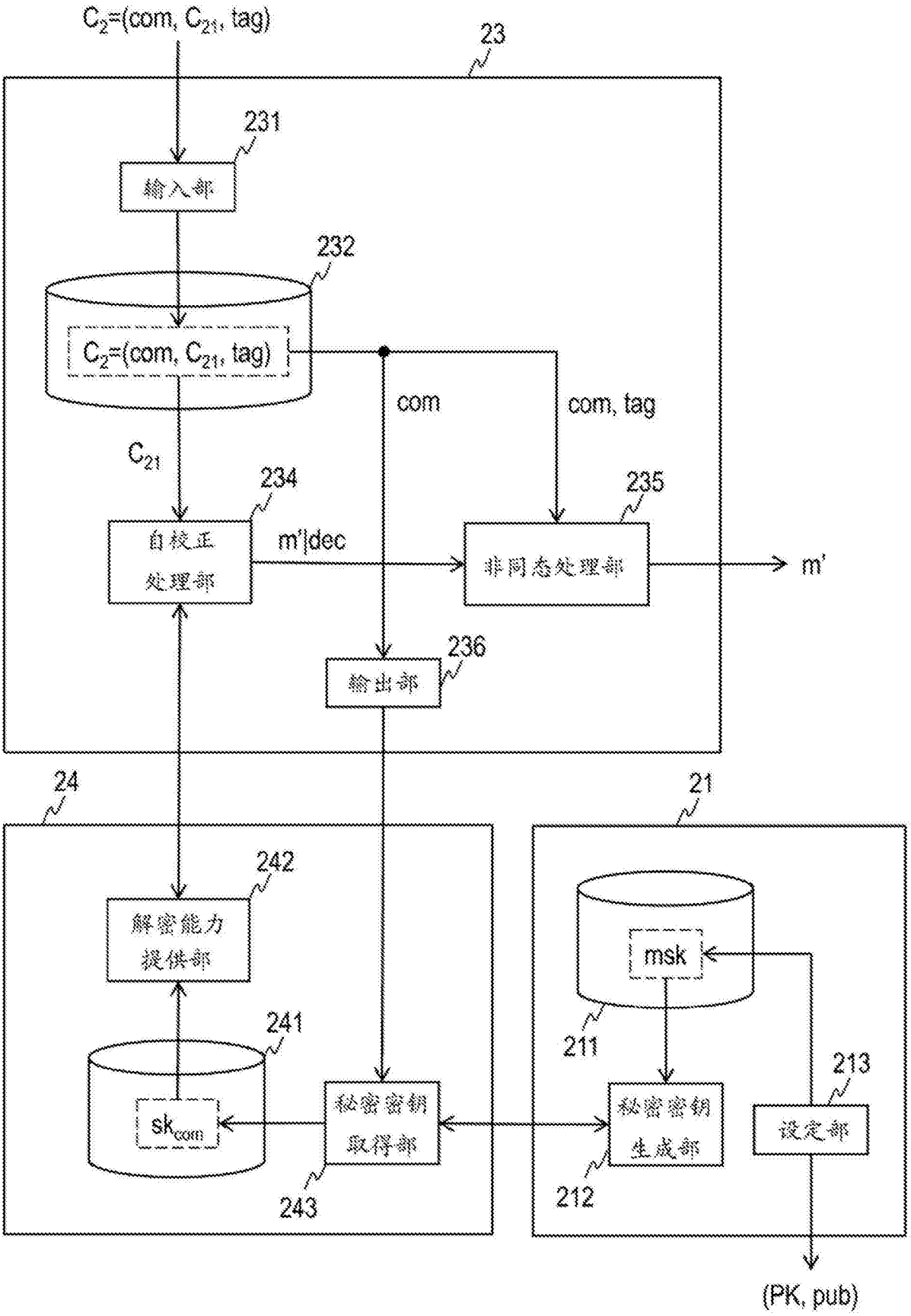

C_2=(com, C_{21}, tag)
23
231
输入部
232
C_2=(com, C_{21}, tag)
com
com, tag
C_{21}
234
自校正处理部
m'|dec
235
非同态处理部
m'
236
输出部
24
21
242
解密能力提供部
241
sk_{com}
秘密密钥取得部
243
msk
211
秘密密钥生成部
212
213
设定部
(PK, pub)

图6

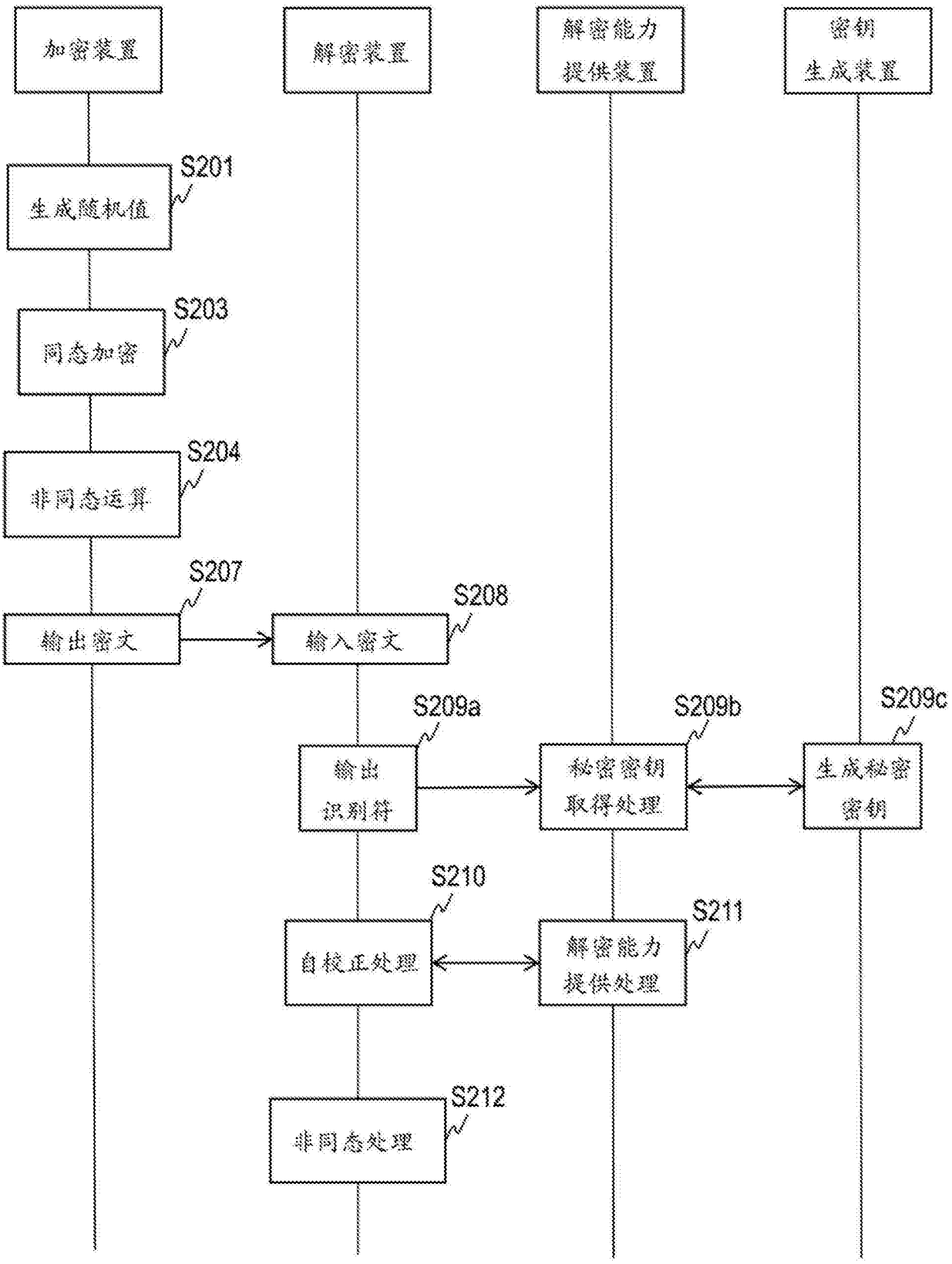

加密装置
解密装置
解密能力提供装置
密钥生成装置
S201
生成随机值
S203
同态加密
S204
非同态运算
S207
输出密文
S208
输入密文
S209a
输出识别符
S209b
秘密密钥取得处理
S209c
生成秘密密钥
S210
自校正处理
S211
解密能力提供处理
S212
非同态处理

图7

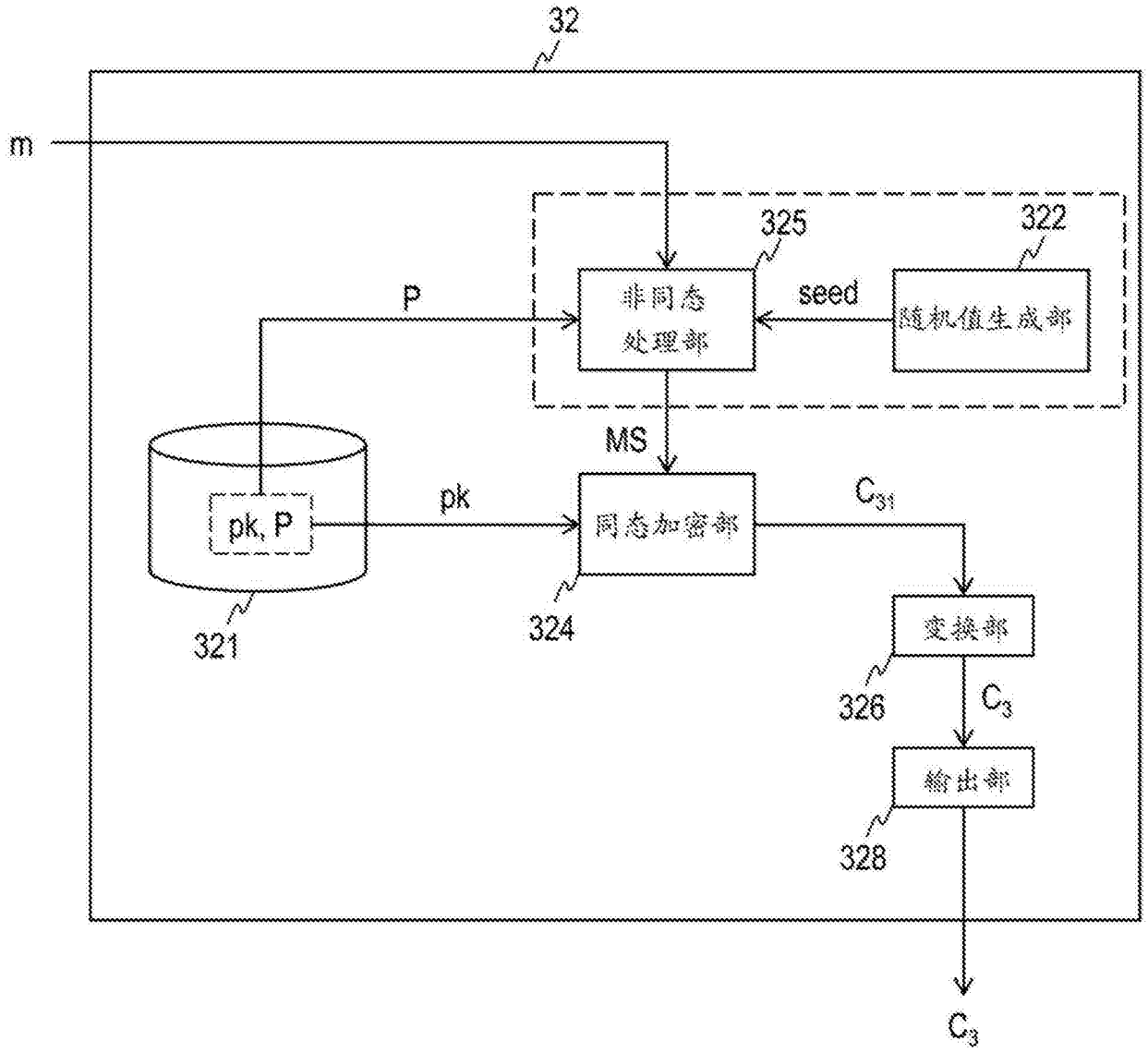

32
m
325
322
非同态
处理部
seed
随机值生成部
P
MS
pk, P
pk
同态加密部
C_{31}
321
324
变换部
326
C_3
输出部
328
C_3

图8

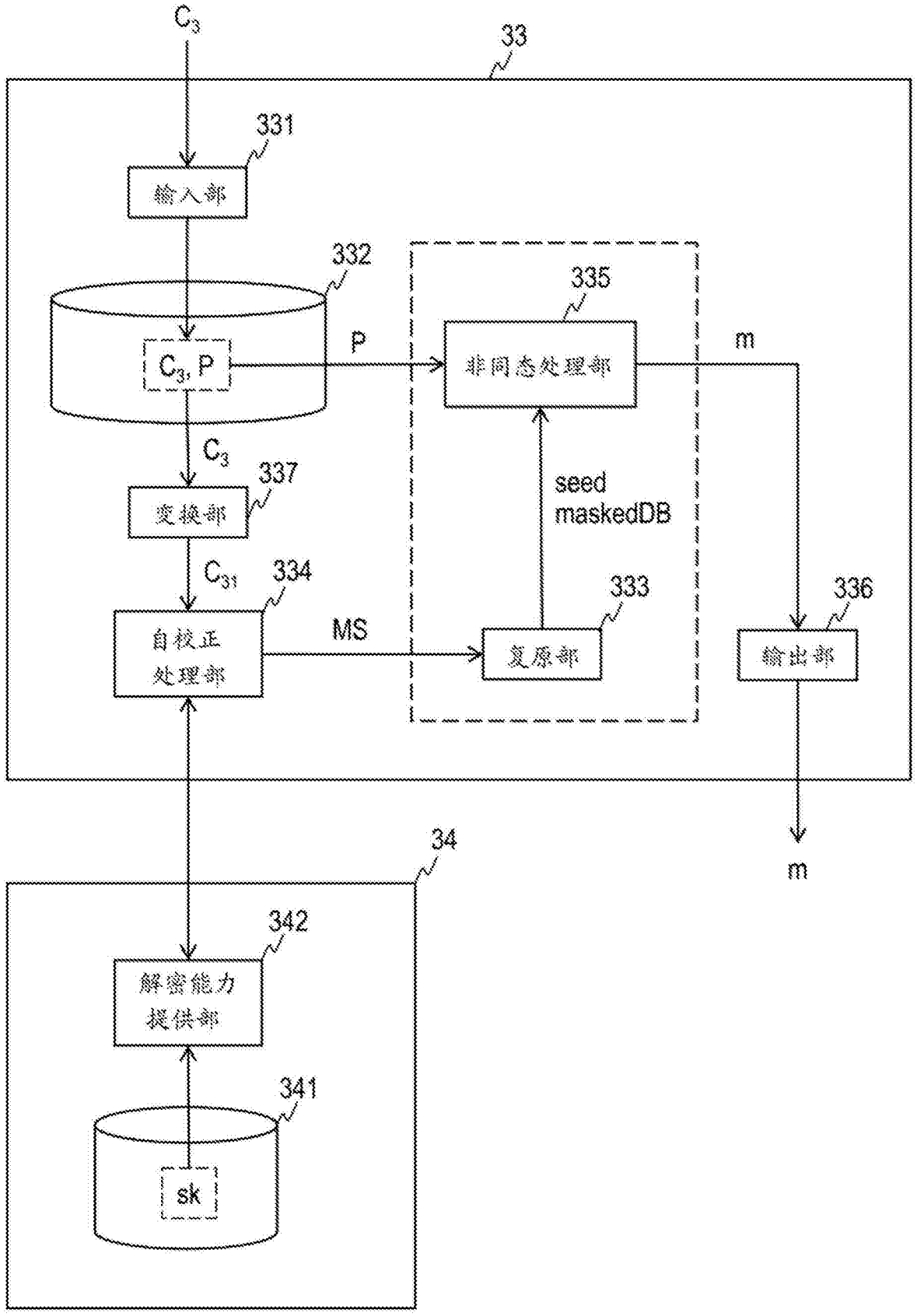

C3
33
331
输入部
332
C3, P
P
335
非同态处理部
m
C3
337
变换部
seed
maskedDB
C31
334
333
336
自校正
处理部
MS
复原部
输出部
m
34
342
解密能力
提供部
341
sk

图9

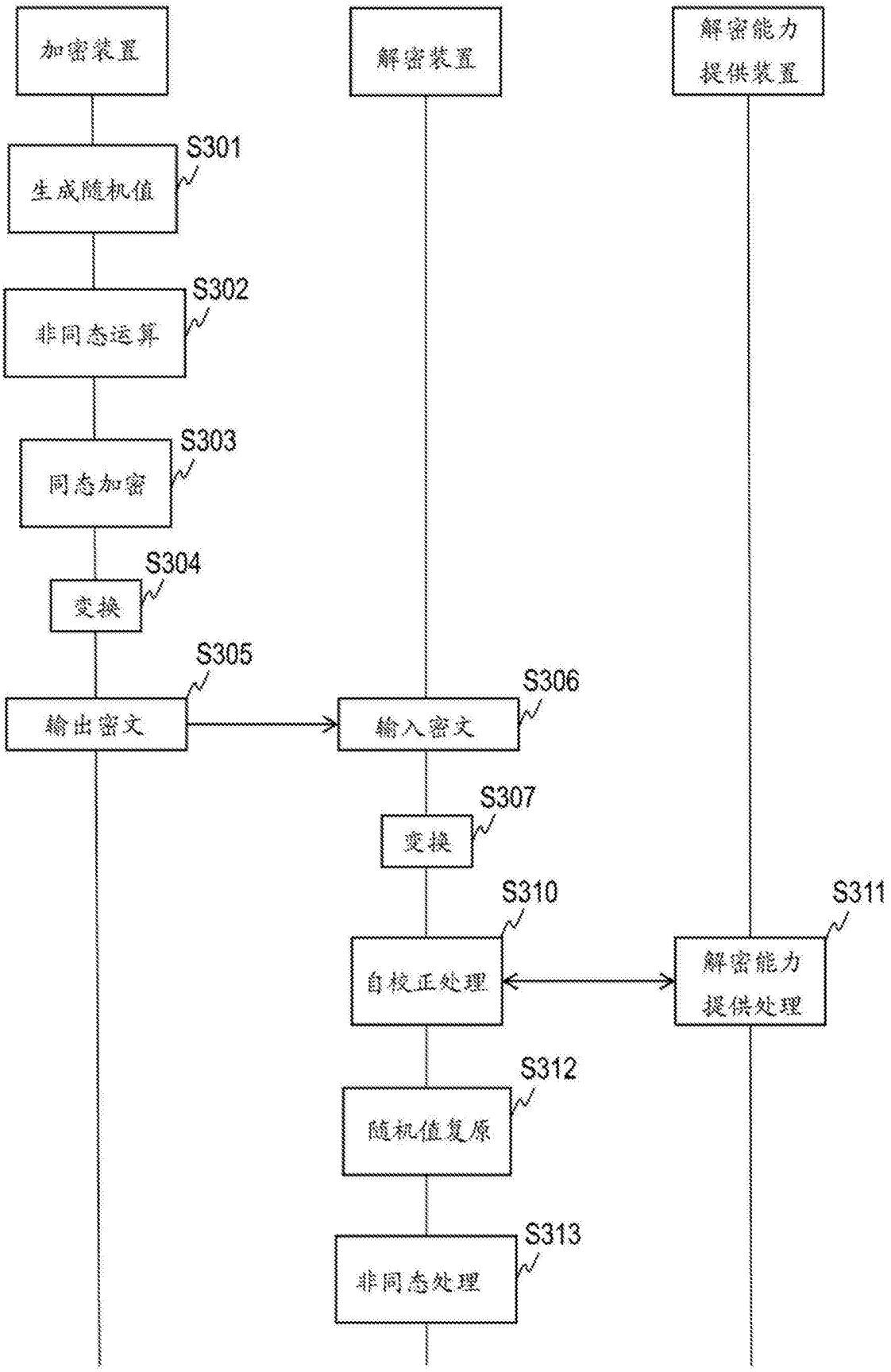

加密装置
解密装置
解密能力提供装置
S301
生成随机值
S302
非同态运算
S303
同态加密
S304
变换
S305
输出密文
S306
输入密文
S307
变换
S310
自校正处理
S311
解密能力提供处理
S312
随机值复原
S313
非同态处理

图10