(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 101420428 B
(45)授权公告日 2011.12.28

(21)申请号 200810177879.1

(22)申请日 2008.09.25

(30)优先权数据
2007-256316 2007.09.28 JP

(73)专利权人 东芝解决方案株式会社
地址 日本东京都
专利权人 株式会社横须贺电信研究园区

(72)发明人 宫崎真悟 中沟孝则 丹羽朗人
冈田光司 栃洼孝也 福岛茂之
石川千秋 越塚登 坂村健

(74)专利代理机构 北京银龙知识产权代理有限公司 11243
代理人 许静

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/00(2006.01)
G06F 17/30(2006.01)

(56)对比文件
CN 1798021 A,2006.07.05, 全文.
US 7096357 B1,2006.08.22, 全文.

审查员 高菲

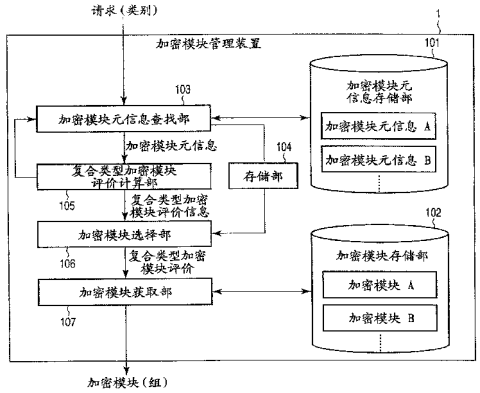
权利要求书 3 页 说明书 23 页 附图 21 页

(54)发明名称

加密模块管理装置和方法

(57)摘要

加密模块管理装置(1)基于所请求的加密模块的类别信息查找加密模块的元信息，并且如果在该加密模块元信息中包含关联加密模块类别信息，查找关联加密模块的加密模块元信息，从而基于该加密模块元信息产生复合类型的加密模块评价信息，基于该复合类型的加密模块评价信息选择加密模块，并且从加密模块存储部(102)读取该加密模块，并输出这种复合类型加密模块评价信息。



CN 101420428 B

1. 一种加密模块管理装置 (1)，其管理多个加密模块，以响应于加密模块选择请求来选择加密模块，并输出所选择的加密模块，所述加密模块管理装置的特征在于包括：

加密模块存储设备 (102)，其存储所述多个加密模块；

加密模块元信息存储设备 (101)，其存储加密模块元信息，所述加密模块元信息包含指示每个加密模块所属类别的类别信息，第一评价信息，所述第一评价信息指示每个加密模块的预定评价结果，类别信息，如果除了所述加密模块之外还需要任何关联加密模块，所述类别信息指示这种关联加密模块所属的类别，以及推导方法信息，所述推导方法信息指示从第一评价信息和第二评价信息推导复合类型加密模块评价信息的方法，其中，所述复合类型加密模块评价信息指示在所述加密模块和这种其它关联加密模块组合的情况下进行评价的预定评价信息，所述第二评价信息指示这种其它关联加密模块的预定评价结果；

加密模块元信息查找设备 (103)，将其配置为基于所请求的加密模块的类别信息，搜索加密模块元信息存储设备，以查找加密模块元信息；

如果由加密模块元信息查找设备查找到的加密模块元信息中包含关联加密模块的类别信息，则复合类型加密模块评价计算设备 (105) 被配置为基于第二评价信息以及在所述加密模块的加密模块元信息中包含的推导方法信息产生复合类型加密模块评价信息作为加密模块的评价信息，其中，所述第二评价信息是利用加密模块元信息查找设备并指定作为查找结果获得的每个关联加密模块的加密模块元信息，通过查找关联加密模块的加密模块元信息获得的复合类型加密模块评价信息，从而递归地调用该复合类型加密模块评价计算设备；

加密模块选择设备 (106)，将其配置为获得由所述复合类型加密模块评价计算设备计算的结果，并且基于该获得的计算结果，选择加密模块；以及

加密模块获取设备 (107)，将其配置为从所述加密模块存储设备读取由所述加密模块选择设备选择的加密模块，并输出这样的加密模块。

2. 根据权利要求 1 所述的加密模块管理装置，其特征在于，如果在加密模块元信息中不包含第二类别信息，复合类型加密模块评价计算设备产生所述加密模块的第一评价信息，作为所述复合类型加密模块的评价信息。

3. 一种加密模块管理装置 (2)，其管理多个加密模块，以响应于加密模块选择请求来选择加密模块，并输出所选择的加密模块，所述加密模块管理装置的特征在于包括：

加密模块存储设备 (206)，其存储所述多个加密模块；

复合类型元信息存储设备 (201)，其存储复合类型元信息，所述复合类型元信息包含指示要被组合的加密模块的最高级别加密模块的类别的类别信息，复合类型加密模块评价信息，所述复合类型加密模块评价信息指示在加密模块组合的情况下执行评价的预定评价信息，以及组合加密模块识别信息，所述组合加密模块识别信息包含识别在加密模块的组合中包含的每个加密模块的加密模块识别信息；

加密模块选择设备 (203,204)，将其配置为基于与选择请求对应的加密模块的类别信息，搜索复合类型元信息存储设备以查找多个复合类型的元信息块，并且基于获得的复合类型元信息中的复合类型加密模块评价信息，选择要在所述组合中包括的加密模块；以及

加密模块获取设备 (205)，将其配置为从加密模块存储设备中读取由加密模块选择设备选择的加密模块，并输出这样选定的加密模块，

其中复合类型加密模块评价信息是在加密模块组合的情况下执行评价的评价信息，基于每个要被组合的加密模块的评价信息，利用预定的推导方法计算所述评价信息。

4. 根据权利要求 3 所述的加密模块管理装置，其特征在于，进一步包括：

加密模块元信息存储设备 (201)，其存储加密模块元信息，所述加密模块元信息包含指示加密模块所属类别的类别信息，评价信息，所述评价信息指示加密模块评价的结果，关联加密模块类别信息，如果需要任何关联加密模块执行加密模块，所述关联加密模块类别信息指示所述关联加密模块所属的类别，以及推导方法信息，如果需要关联加密模块执行加密模块，所述推导方法信息指示给加密模块设置的评价信息和给关联加密模块设置的评价信息中推导复合类型评价信息的方法，所述复合类型评价信息指示在所述加密模块和关联加密模块组合的情况下执行评价的评价信息；

如果在加密模块元信息中包含关联加密模块类别信息，则复合类型加密模块评价计算设备 (211) 被配置为基于关联加密模块的评价信息以及在所述加密模块的加密模块元信息中包含的推导方法信息产生复合类型加密模块评价信息作为所述加密模块的评价信息，其中所述关联加密模块的评价信息是利用加密模块元信息查找设备并指定作为查找结果获得的每个关联加密模块的加密模块元信息，通过查找关联加密模块的加密模块元信息获得的，从而递归地调用该复合类型加密模块评价计算设备；以及

写设备 (212)，将其配置为将由所述复合类型加密模块评价计算设备计算的复合类型的加密模块评价写入所述复合类型元信息存储设备。

5. 根据权利要求 4 所述的加密模块管理装置，其特征在于，如果在加密模块元信息中不包含关联加密模块类别信息，复合类型加密模块评价计算设备产生该加密模块的评价信息作为复合类型加密模块评价信息。

6. 一种加密模块管理装置 (2) 中的加密模块管理方法，其管理多个加密模块，以响应于加密模块选择请求来选择加密模块，并输出所选择的加密模块，所述加密模块管理装置的特征在于包括：

加密模块存储设备 (206)，其存储所述多个加密模块；以及

加密模块元信息存储设备 (201)，其存储加密模块元信息，所述加密模块元信息包含指示每个加密模块所属类别的类别信息，第一评价信息，所述第一评价信息指示每个加密模块的预定评价结果，类别信息，如果需要任何关联加密模块来执行加密模块，所述类别信息指示这种关联加密模块所属的类别，以及推导方法信息，所述推导方法信息指示从第一评价信息和第二评价信息推导复合类型加密模块评价信息的方法，其中，所述复合类型加密模块评价信息指示在所述加密模块和其它关联加密模块组合的情况下执行评价的预定评价信息，所述第二评价信息指示其它关联加密模块的预定评价结果，

其中，加密模块元信息查找设备 (210) 基于所请求的加密模块的类别信息，搜索加密模块元信息存储设备，以查找加密模块元信息，

如果由加密模块元信息查找设备查找到的加密模块元信息中包含关联加密模块的类别信息，则复合类型加密模块评价计算设备 (211) 基于第二评价信息以及在那些加密模块的加密模块元信息中包含的推导方法信息产生复合类型加密模块评价信息作为加密模块的评价信息，并提供这种评价信息作为评价结果，其中，所述第二评价信息是利用加密模块元信息查找设备并指定作为查找结果获得的每个关联加密模块的加密模块元信息，通过查

找关联加密模块的加密模块元信息获得的复合类型加密模块评价信息，从而递归地调用该复合类型加密模块评价计算设备；

加密模块选择设备（204）通过响应于所述选择请求指定加密模块元信息，获得由所述复合类型加密模块评价计算设备计算的结果，并且基于该获得的计算结果，选择加密模块，以及

加密模块获取设备（205）从所述加密模块存储设备中读取由所述加密模块选择设备选择的加密模块，并将其输出。

加密模块管理装置和方法

技术领域

[0001] 本发明涉及一种用于响应于来自客户的加密模块传递请求，依照加密模块评价信息，选择和传递加密模块的加密模块管理装置和方法。

背景技术

[0002] 当处理机密信息时，按照惯例，通常执行加密处理。这种加密处理包括加密模块的使用。加密模块涉及需要执行加密处理的程序，包括执行加密处理的不同元件的程序（例如：散列函数计算、伪随机数生成处理，等等）。也就是，所述加密模块可以以单独的程序或多个程序组合的形式出现。在下面的描述中，所述加密模块可以以这两种情形中的任一种实现。

[0003] 值得注意的是，在一些情况下，多个加密模块中的特定一个可以在多个加密处理项目中重复使用。例如，诸如散列函数（SHA-1 等）的加密模块可以在数字签名的生成、认证码的生成和独立式散列函数计算中使用。对于在数字签名的生成中的使用，参看由 M.Bellare 和 P.Rogaway 在“The exact security ofdigital signatures—How to sign with RSA and Rabin”中描述的 RSAS SA，InAdvances in Cryptology-Eurocrypt’96，399-416 页，Springer-Verlag，1996。对于在认证码的生成中的使用，参看由 M.Bellare，R.Canetti 和 H.Krawczyk 在“Keying hash functions for message authentication”中描述的 HMAC，In Advancesin Cryptology-CRYPTO’96，1-15 页，Springer-Verlag，1996。

[0004] 下面将讨论例如移动终端对加密模块的管理和利用等情况，所述移动终端不具有大的存储容量。在这种情况下，为了节省移动终端中存储器的使用，优选地以这样的方式来设计加密模块，可以对每个加密处理元件提供每个所述模块，并且所述加密处理项目可以共同地使用相同的加密模块。

[0005] 然而，为了响应于来自终端设备的选择请求为每个元件传递加密模块，需要选择适合所述选择请求的加密模块组合。此外，为了在加密模块已经组合的情况下进行评价，将增加从接收选择请求到完成所述选择的过程的负荷，这是一个问题。

发明内容

[0006] 本发明的目的在于提供一种加密模块管理装置和方法，其能够在已经接收到选择请求时从保持的那些加密模块中选择加密模块的适当组合，并且减轻从接收加密模块选择请求到完成所述选择的过程的负荷。

[0007] 在本发明的第一方面中，提供了一种加密模块管理装置，其管理多个加密模块，以响应于加密模块选择请求来选择加密模块，并输出所选择的加密模块，所述加密模块管理装置包括：加密模块存储设备，其存储所述多个加密模块；加密模块元信息存储设备，其存储加密模块元信息，所述加密模块元信息包含指示每个所述加密模块所属类别的类别信息，第一评价信息，所述第一评价信息指示每个加密模块的预定评价结果，类别信息，如果除了所述加密模块之外还需要任何关联加密模块，所述类别信息指示这种其它关联加密模

块所属的类别，以及推导方法信息，所述推导方法信息指示从第一评价信息和第二评价信息推导复合类型加密模块评价信息的方法，其中，所述复合类型加密模块评价信息指示在所述加密模块和这种其它关联加密模块组合的情况下进行评价的预定评价信息，所述第二评价信息指示这种其它关联加密模块的预定评价结果；加密模块元信息查找设备，将其配置为基于所请求的加密模块的类别信息，搜索加密模块元信息存储设备，以查找加密模块元信息；复合类型加密模块评价计算设备，将其配置为如果由加密模块元信息查找设备查找的加密模块元信息中包含关联加密模块的类别信息，基于第二评价信息产生复合类型加密模块评价信息作为加密模块的评价信息，其中，第二评价信息是利用加密模块元信息查找设备并指定作为查找结果获得的每个关联加密模块的加密模块元信息，通过查找关联加密模块的加密模块元信息获得的复合类型加密模块评价信息，从而递归地调用该复合类型加密模块评价计算设备，以及在所述加密模块的加密模块元信息中包含的推导方法信息；加密模块选择设备，将其配置为获得由所述复合类型加密模块评价计算设备计算的结果，并且基于该获得的计算结果，选择加密模块；以及加密模块获取设备，将其配置为从所述加密模块存储设备读取由所述加密模块选择设备选择的加密模块，并输出这样的加密模块。

[0008] 因此，依照第一方面，当已经从外界接收到加密模块选择请求时，查找其类别对应于该选择请求中的类别信息的加密模块元信息。在这种情形中，由于关于可组合的加密模块的加密模块元信息适合于关联加密方法类别信息，所述关联加密方法类别信息依次与其它加密模块元信息的类别信息相关联，作为起始点，通过利用其类别与所述选择请求中的类别信息相对应的加密模块元信息，递归地调用所述可组合的加密模块元信息块是有可能的，从而在加密模块已经组合的情况下产生评价信息。基于在相关加密模块元信息中存储的推导方法信息，通过利用在加密模块元信息中存储的评价信息和在加密模块元信息中包含的评价信息，将生成该评价信息，其是所述相关加密模块元信息的关联加密模块。然后，基于所产生的评价信息，将选择和输出加密模块。

[0009] 在本发明的第二方面中，提供了一种加密模块管理装置，其管理多个加密模块，以响应于加密模块选择请求来选择加密模块，并输出所选择的加密模块，所述加密模块管理装置包括：加密模块存储设备，其存储所述多个加密模块；复合类型元信息存储设备，其存储复合类型元信息，所述复合类型元信息包含指示要被组合的加密模块的最高级别加密模块的类别的类别信息，复合类型加密模块评价信息，所述复合类型加密模块评价信息指示在加密模块组合的情况下执行评价的预定评价信息，以及组合加密模块识别信息，所述组合加密模块识别信息包含识别在加密模块的组合中包含的每个加密模块的加密模块识别信息；加密模块选择设备，将其配置为基于与选择请求对应的加密模块的类别信息，搜索复合类型的元信息存储设备以查找多个复合类型的元信息块，并且基于获得的复合类型元信息中的复合类型加密模块评价信息，选择要在所述组合中包括的加密模块；以及加密模块获取设备，将其配置为从加密模块存储设备中读取由加密模块选择设备选择的加密模块，并输出这样选定的加密模块，其中复合类型加密模块评价信息是在加密模块组合的情况下执行评价的评价信息，基于每个要被组合的加密模块的评价信息，利用预定的推导方法计算所述评价信息。

[0010] 因此，依照第二方面，在加密模块已经组合的情况下，将评价信息的计算结果存储为复合类型元信息。在这种情况下，将在组合加密模块上进行评价的信息存储为基于那些

组合的加密模块中的每一个的评价信息，利用预定推导方法进行计算的结果。以这样的方式，根据预定的推导方法，在加密模块已经组合的情况下产生和存储评价信息，从而当已经接收到选择请求时，通过参考该评价信息，不需要产生评价信息即可选择加密模块。

[0011] 依照第三方面，根据第二方面的加密模块管理装置进一步包括加密模块元信息存储设备，其存储加密模块元信息，所述加密模块元信息包含指示加密模块所属类别的类别信息，评价信息，所述评价信息指示加密模块评价的结果，关联加密模块类别信息，如果需要任何关联加密模块执行加密模块，所述关联加密模块类别信息指示所述关联加密模块所属的类别，以及推导方法信息，如果需要关联加密模块执行加密模块，所述推导方法信息指示给加密模块设置的评价信息和给关联加密模块设置的评价信息中推导复合类型评价信息的方法，所述复合类型评价信息指示在所述加密模块和关联加密模块组合的情况下进行评价的评价信息；复合类型加密模块评价计算设备，将其配置为如果在指定的加密模块元信息中包含关联加密模块类别信息，基于关联加密模块的评价信息产生复合类型加密模块评价信息作为所述加密模块的评价信息，其中所述关联加密模块的评价信息是利用加密模块元信息查找设备并指定作为查找结果获得的每个关联加密模块的加密模块元信息，通过查找关联加密模块的加密模块元信息获得的，从而递归地调用该复合类型加密模块评价计算设备，以及在所述加密模块的加密模块元信息中包含的推导方法信息；以及写设备，将其配置为将由所述复合类型加密模块评价计算设备计算的复合类型的加密模块评价写入所述复合类型元信息存储设备。

[0012] 因此，在第三方面中，预先存储加密模块元信息，从而基于该存储的加密模块元信息，在加密模块已经组合的情况下，产生评价信息并将其写入复合类型加密元信息存储部分。相应地，如果出现加密模块管理装置管理新的加密模块的需要，在那些新的加密模块组合的情况下，产生评价信息并存储该信息是有可能的。

附图说明

[0013] 图 1 是依照本发明第一实施例的加密模块传递系统的组成框图；

[0014] 图 2 是依照相同实施例的加密客户装置的组成框图；

[0015] 图 3 是依照相同实施例的加密模块管理服务器装置的组成框图；

[0016] 图 4 是依照本发明第二实施例的加密模块传递系统的组成框图；

[0017] 图 5 是依照相同实施例的加密客户装置的组成框图；

[0018] 图 6 示出了依照相同实施例的选择数据库的数据组成实例；

[0019] 图 7 示出了依照相同实施例的加密模块链接数据库的数据组成实例；

[0020] 图 8 示出了依照相同实施例的加密模块数据库的数据组成实例；

[0021] 图 9 示出了依照相同实施例的密钥信息数据库的数据组成实例；

[0022] 图 10 示出了依照相同实施例的加密处理数据库的数据组成实例；

[0023] 图 11 示出了依照相同实施例的数据库的逻辑组成；

[0024] 图 12 是依照相同实施例的加密模块管理服务器装置的组成框图；

[0025] 图 13 是依照本发明第三实施例的加密模块管理装置的功能框图；

[0026] 图 14 示出了依照相同实施例的加密模块元信息的一个实例；

[0027] 图 15 示出了依照相同实施例的加密模块评价信息的一个实例；

[0028] 图 16 是利用关联加密方法类别信息的加密模块元信息的说明图；

[0029] 图 17 是依照本发明第三实施例的加密模块管理装置的操作的说明性流程图；

[0030] 图 18 是依照相同实施例的变型例，加密模块管理装置的操作的说明性流程图；

[0031] 图 19 是依照第四实施例的加密模块管理装置的组成框图；

[0032] 图 20 是复合类型元信息的说明表；

[0033] 图 21 是加密模块管理装置的操作的说明性流程图；

[0034] 图 22 是依照本发明第五实施例的加密模块管理装置组成框图的略图；以及

[0035] 图 23 是示出依照相同实施例的元信息关联表的一个实例的表。

具体实施方式

[0036] 下面将参照附图，描述依照本发明的一个实施例的加密模块传递系统。

[0037] 首先，下面将概述本系统。在本系统中，服务器和客户装置彼此连接，因此能够互相发送和接收信息，所述信息已经利用加密模块进行了加密。在这种情况下，也可以周期地切换所述加密模块。由于这样的加密系统能够切换加密模块，可以利用几种构架，所述构架独立于每种加密技术的加密方法建立接口，并且能够由各密码系统的提供商实施。例如，它们包括 Microsoft™ 的 CyptAPI，Sun™ 的 JCA(Java™ 加密体系)/JCE(Java™ 加密扩展)，以及 Group™ 的 CDSA(公共数据安全体系)。

[0038] 在那些构架中，建立接口是有可能的，其中通过所述接口访问诸如加密 / 解密、签名产生 / 验证和认证码产生 / 验证的各种加密技术的加密模块，从而依照所述接口，可以实施如同 DES(数据加密标准) 和 AES(高级加密标准) 这样的加密方法。相应地，当建立起系统时，密码或安全专家可以预先从那些实施的加密方法中选择适当的加密方法，并向所述构架输入指示要被利用的加密方法的加密参数，从而加密方法可以在彼此之间进行切换。

[0039] 当正在利用这样的构架，并且如果应用系统的正在施行的安全策略发生改变时，密码或安全专家按照惯例不得不重新选择适合所述系统的加密方法，这个事实导致人力资源以及密码或安全方面的专家的费用问题。此外，如果已经发现现有的加密方法存在缺陷或者已经宣布了新的加密方法，新近改变的加密方法不能平稳地应用到运行中的系统。而且，如果实施安全的不同环境需要不同的安全级别和处理速度，会发现常规的系统很难实现最佳安全。

[0040] 在本系统中，任何能够切换加密方法的加密系统都可以解决这个问题。

[0041] < 第一实施例 >

[0042] 图 1 是依照本发明第一实施例的加密模块传递系统组成框图的略图。

[0043] 本加密系统包括传送加密包 307 的加密模块管理服务器装置 350，所述加密包包括加密模块 308 和加密模块评价描述文件 309，以及利用接收到的加密包 307 执行加密处理的加密客户装置 150。在所述加密模块评价描述文件 309 中描述的加密模块的评价涉及包含对应的加密模块 308 的加密方法的置信度等的数字表示的信息，例如，在加密模块中可以利用的实施的加密方法的安全性、加密处理速度以及密钥长度。

[0044] 所述加密模块管理服务器装置 350 包括累积加密模块 308 的加密模块数据库 353、累积加密模块评价描述文件 309 的加密模块评价数据库 354、管理加密模块数据库 353 和加密模块评价数据库 354 的加密模块管理部 351、在加密模块数据库 353 和加密模块评价数据

库 354 中注册新信息的加密模块注册部 355，以及响应于来自加密客户装置 150 的请求，从加密模块数据库 353 和加密模块评价数据库 354 读取最佳加密包 307 并传送所述加密包的加密包发送部 352。

[0045] 所述加密客户装置 150 由作为应用程序或中间件进行服务的高级别系统部 151、加密控制管理器部 152、防干扰加密硬件部 450、以及所实施的加密模块部 153 组成，其中，所述高级别系统部 151 通过加密控制管理器部 152 调用由实施的加密模块部 153 提供的加密功能，并利用这种功能，所述加密控制管理器部 152 接收由加密模块管理服务器装置 350 传送的加密包 307，或者切换由实施的加密模块部 153 提供的加密功能，所述防干扰加密硬件部 450 利用主要的加密方法，通过硬件实现加密处理，所述实施的加密模块部 153 在能够执行和利用其中已经实施了加密方法的加密模块 308 的条件下提供加密功能。所述加密模块管理服务器装置 350 基于来自加密客户装置 150 的请求而执行初始注册、传递和更新加密模块的三个过程，从而将适当的加密包 307 传送到加密客户装置 150。

[0046] 应注意的是，在加密客户装置 150 不具有加密模块 308 并且不包括实施的加密模块部 153 的情况下，加密模块的初始注册涉及利用加密客户装置 150 的加密硬件部 450，从而安全地从加密模块管理服务器装置 350 到所实施的加密模块部 153 传送应用所必需的加密模块 308。

[0047] 加密模块的传递涉及加密模块管理服务器装置 350，其响应于从加密客户装置 150 接收的加密模块选择请求来选择适当的加密模块 308 或加密包 307，并将所选择的加密模块或加密包传送到加密客户装置 150。加密模块选择请求包含关于加密模块的条件信息，所述条件信息包括例如加密或签名生成的加密方法的类别（种类）、创建加密模块 308 的制造机 (maker)、其上运行加密模块 308 的硬件信息以及加密模块的评价信息。在本实施例的情况下，加密模块评价信息可以作为独立于加密模块 308 的加密模块评价描述文件 309 进行处理。

[0048] 如果已经注册了新的加密模块 308、已经删除了利用危险加密方法的加密模块 308、在现有加密模块 308 中已经发现了错误以及因此已经更新了该模块 308 和正在执行该模块 308 的实施的加密模块部 153、或者已经改变了加密模块评价以适应计算机处理速度的提高，加密模块的更新涉及更新存储在加密模块管理服务器装置 350 中的加密模块数据库 353 或加密模块评价数据库 354 中的信息、然后以固定的周期或响应于来自加密客户装置 150 的请求周期地将加密包 307 的该更新后的信息传送到加密客户装置 150、从而通知加密模块管理服务器装置 350 正在传送新的加密模块 308 或者现有的实施的加密模块部已经停止服务。

[0049] 图 2 是加密客户装置 150 的详细构成图。加密控制管理器部 152 由具有加密处理信息数据库 157 的加密处理控制部 156、具有加密模块数据库 164、加密模块评价数据库 163、加密模块选择策略 158 以及硬件概况 160 的加密模块选择部 159、具有密钥信息数据库 165 和其中已经描述了该密钥信息数据库 165 的访问控制策略的访问控制策略 161 的密钥信息管理部 162、具有加密控制管理器策略 167 的加密模块管理部 166、与加密硬件部 450 通信的加密硬件管理控制部 170、与外界通信的通信功能 155、与通信功能 155 连接的算法协商部 168、以及与通信功能 155 连接的安全通信管理部 169 构成。

[0050] 当所述高级别系统部 151 已经调用了加密处理时，加密处理控制部 156 执行密钥

产生处理、密钥注册处理以及加密处理。

[0051] 加密模块数据库 164 是存储从加密模块管理服务器装置 350 接收的加密模块 308 的存储部。

[0052] 加密模块评价数据库 354 是存储从加密模块管理服务器装置 350 接收的加密模块评价描述文件 309 的存储部。

[0053] 加密模块选择部 159 基于关于加密模块的条件信息，从那些在加密模块数据库 164 中存储的加密模块中选择最适合的加密模块 308，其中所述条件信息包括诸如加密或签名生成的加密类别、创建加密模块 308 的制造机、其上运行加密模块 308 的硬件信息、以及已经从所述高级别系统部 151 输入的加密模块的评价信息。实际上，选择这样的加密模块 308，从而匹配已经描述了加密客户装置 150 的硬件信息的硬件概况 160，并且也符合已经描述了加密客户装置 150 的用户策略的加密模块选择策略 158。

[0054] 所述硬件概况 160 涉及的信息包含例如加密客户装置 150 的 CPU 的结构、CPU 时钟信号、以及安装的多个存储器。加密模块选择策略 158 涉及的信息包括 :例如如果基于输入条件已经选择了多个加密模块而用户愿意优选其它加密模块的条件、用户在应用中愿意优选的加密模块的制造机、用户愿意禁用的加密方法。

[0055] 以这种方式，加密模块选择部 159 参考来自所述高级别系统部 151 的输入信息、硬件概况 160、以及加密模块选择策略 158，从而选择匹配输入信息的加密模块 308。如果加密模块选择部 159 已经唯一地选择了加密模块 308，从加密模块数据库 164 取出所选择的加密模块 308。如果加密模块选择部 159 不能唯一地选择加密模块 308，它将输出错误。

[0056] 密钥信息管理部 162 将数据存入密钥信息数据库 165 并从密钥信息数据库 165 读取数据，例如包括当调用所实施的加密模块部 153 时指定的密钥信息和加密方法参数信息的信息。如果要被指定的密钥信息或加密方法参数信息的块的数量不是 1，密钥信息管理部 162 将多个信息块联合成一个块，从而可以取出这样的信息，然后在密钥信息数据库 165 中注册这样的信息。此外，当从密钥信息数据库 165 提取密钥信息或加密方法参数信息时，密钥信息管理部 162 依照加密模块选择策略 158，控制对来自多个高级别系统 151 的密钥信息的访问。

[0057] 加密模块管理部 166 通过通信功能 155 与加密模块管理服务器装置 350 建立通信，从而依照初始注册、传递和更新加密模块的过程接收加密包 307 等。当从加密模块管理服务器装置 350 接收到加密包 307 等时，加密模块管理部 166 依照加密控制管理器策略 167 的内容执行处理。加密控制管理器策略 167 的内容包括例如下列五项。第一项是在与加密模块管理服务器装置 350 通信时允许 / 不允许服务器认证。第二项是在从加密模块管理服务器装置 350 接收加密包 307 等时，允许 / 不允许加密包 307 等的加密。第三项是在从加密模块管理服务器装置 350 接收加密包 307 等时，允许 / 不允许消息认证码 (MAC) 的增加。第四项是允许 / 不允许对所接收的加密包 307 等的认证码进行验证。第五项是设置关于允许 / 不允许周期更新存储在加密模块评价数据库 163 和加密模块数据库 164 中的加密包 307、表示更新频率的周期更新等的信息。

[0058] 加密硬件管理控制部 170 与加密硬件部 450 建立通信，从而依照加密模块初始注册的过程从加密模块管理服务器装置 350 接收加密包 307。当正在接收加密包 307 时，如果它自身已经被加密，由加密硬件部 450 对它进行解码。此外，如果已经检测到消息认证码增

加到加密模块 308，则加密硬件部 450 检测加密模块 308 中的错误。

[0059] 算法协商部分 168 与通信功能 155 连接，以在两个加密客户装置之间建立安全通信会话之前协商在安全通信会话中要被应用的加密方法，以及在其建立时应用的另一种加密方法。

[0060] 安全通信管理部 169 与通信功能 155 连接，从而与其它加密客户装置 150 建立安全通信会话。当建立安全会话时，在算法协商部 168 已经确定通信会话中应用的加密方法和在其建立时应用的另一种加密方法之后，安全通信管理部 169 共享会话密钥。在已经建立了安全通信会话之后，依照所确定的加密方法应用会话密钥，以使得能够增加认证码以加密通信数据或使其抗干扰。此外，安全通信管理部 169 使得保持曾经建立的通信会话成为可能，从而可以在恒定的时间间隔内再次使用它。

[0061] 图 3 是加密模块管理服务器装置 350 的详细构成图。加密模块管理服务器装置 350 由加密模块数据库 353、加密模块评价数据库 354、加密模块管理部 351、加密模块注册部 355、以及加密包发送部 352 构成，其中，所述加密模块管理部 351 执行例如读取和更新存储在加密模块数据库 353 和加密模块评价数据库 354 中的信息的处理，所述加密模块注册部 355 在加密模块数据库 353 和加密模块评价数据库 354 中注册信息，所述加密包发送部 352 将加密模块传递到加密客户装置 150。

[0062] 加密模块数据库 353 是存储要被用户预先存储或输入的加密模块 308 的数据库。

[0063] 加密模块评价数据库 354 是存储要被用户预先存储或输入的加密模块评价描述文件 309 的数据库。

[0064] 加密模块管理部 351 包括接口，利用所述接口，通过搜索加密模块数据库 353 和加密模块评价数据库 354 以查找在其中存储的加密模块 308 和加密包 307、显示加密模块评价部的内容、显示被管理的加密模块列表、更新现有的加密模块、删除现有的加密模块、注册新的加密模块、以及激活 / 去活加密包发送部，为加密模块管理服务器装置 350 的用户服务。当注册新的加密模块时，加密模块管理部 351 向加密模块注册部 355 请求对其进行注册。

[0065] 加密模块注册部 355 包括加密包注册部 357 和复合类型描述生成部 358。

[0066] 加密包发送部 352 包括加密包传递控制部 359、具有分发策略 371 的加密包分发配置部 370、以及具有分发策略 371 的分发加密模块选择部 360。加密包发送部 352 实施等待服务，以解释来自加密客户装置 150 的请求，并执行初始注册、传递、和更新加密模块的三个过程。此外，所述等待服务包括记录处理内容的日志。

[0067] 分发加密模块选择部 360 基于初始注册、传递、和更新加密模块的三个过程，以及来自加密客户装置 150 的请求，选择适当的要被传递的加密模块 308。在加密模块初始注册的情况下，将要被传递的加密模块 308 规定为不可缺少的，从而提供在分发策略 371 中描述的加密方法。

[0068] 基于由分发加密模块选择部 360 选择的加密模块 308，根据分发策略 371，加密包分发配置部 370 执行配置处理，以将加密模块 308 和与加密模块 308 对应的加密模块评价描述文件 309 转换为可以作为加密包 307 分发的格式。在分发策略 371 中，例如，描述了下列四项。

[0069] 第一项是在其分发时允许 / 不允许对加密包 307 进行加密。第二项是对加密包

307 进行加密的方法。第三项是在分发加密包 307 时允许 / 不允许增加消息认证码。第四项是为加密包 307 加密消息认证码的方法。

[0070] 在加密包分发配置部 370 执行的配置处理中，以一种特殊的格式将存储在加密模块评价数据库 354 中的内容生成作为加密模块评价描述文件 309，将认证码添加到所述加密模块评价描述文件 309，从而该代码分发到加密包 307 可以由加密模块管理服务器装置 350 证明，并与加密模块 308 组合到加密包 307 中。

[0071] 此外，加密包分发配置部 370 可以将其中组合了多个加密模块的加密模块 308 和分别对应于所述多个加密模块 308 的加密模块评价描述文件 309 集成到一个加密包中。此外，在由加密包分发配置部 370 执行的配置处理中，依照加密客户装置 150 的加密控制管理器策略和加密模块管理服务器装置 350 的分发策略 371，对加密包 307 进行加密，并且对其添加消息认证码，并且为了这些目的，产生和管理密钥。

[0072] < 第二实施例 >

[0073] 相对于已经参照加密客户装置处理选择最优加密方法的情况对其进行了描述的第一实施例，在第二实施例中，在加密模块管理服务器装置的主动下，选择最优的加密方法。也就是，图 4 所示的加密模块传递系统使用了服务器链接机制，其中模块选择策略存储部 110 管理和利用由加密模块管理服务器装置 1350 选择的加密方法的结果信息。特别地，如果模块选择策略存储部 110 的计算能力差，加密模块管理服务器装置 1350 可以帮助计算，从而改善加密客户装置 1100 中的响应性能。

[0074] 详细地，加密模块管理服务器装置 1350 响应于来自高级别系统部 1151 的请求，选择最优加密模块 308，加密客户装置 1100 中的加密控制管理器部 1152 接收所述选择的结果，而该装置中的加密信息存储部 1600 管理该请求的条件和所述最优加密模块 308 的条件之间的关系。基于来自所述高级别系统部 151 的请求和该请求的最优加密模块 308 之间的关系，加密控制管理器部 1152 执行处理以匹配来自所述高级别系统部 151 的加密处理控制请求。因此，相对于第一实施例，加密客户装置 1100 不必管理所需的加密模块 308 或加密包 307 的所有选择功能，以选择加密模块 308 或者从加密模块管理服务器装置 1350 接收信息。

[0075] 图 4 是根据本发明第二实施例的加密模块传递系统的组成框图的略图。本系统包括至少一个加密客户装置 1100、至少一个加密硬件单元 1450 以及加密模块管理服务器装置 1350。加密硬件 1450 与第一实施例中的相同。应注意的是，多个加密硬件单元 1450 可以连接到各个加密客户装置 1100。此外，加密硬件 1450 可以安装在加密客户装置 1100 中。

[0076] 图 5 是加密客户装置 1100 的组成框图。加密客户装置 1100 包括高级别系统部 1151、加密控制管理器部 1152、实施的加密模块部 1153 以及通信功能 1155。此外，选择策略 1158 是其中设置了安全、处理速度和资源优先信息的文件。所述高级别系统部 1151 和实施的加密模块部 1152 具有与第一实施例相同的构造和功能。

[0077] 加密控制管理器部 1152 包括加密处理控制部 1156、密钥管理部 1162、加密信息存储部 1600、加密包管理部 1166、以及加密硬件管理控制部 1170。

[0078] 加密处理控制部 1156 具有从所述高级别系统部 1151 接受包含加密处理条件的加密处理控制请求的功能，通过参照加密信息存储部 1600 指定链接到加密处理条件的加密模块 1153 的功能，根据加密处理执行定时向实施的加密模块部 1153 请求加密处理的功能，

为加密处理发布加密处理标识符、将它与关于该加密处理的信息关联、并将它存储在加密信息存储部 1600 的功能，以及将来自实施的加密模块部 1153 的加密处理结果和关于该加密处理的加密处理标识符输出到所述高级别系统部 1151 的功能。

[0079] 密钥管理部 1162 具有响应于来自所述高级别系统部 1151 的请求，利用加密信息存储部 1600 中的密钥信息数据库 1165 注册、删除、获取、查找、和更新密钥信息的功能，如果已经正常注册了加密密钥，发布密钥标识符、将所述密钥标识符与关于该注册处理的信息关联、并将它存储在加密信息存储部 1600 中的功能，以及根据情况将包括加密处理标识符和密钥标识符的每个处理单元的结果输出到所述高级别系统部 1151 的功能。

[0080] 加密信息存储部 1600 具有存储选择数据库 1601、加密模块连接数据库 1602、加密模块数据库 1603、密钥信息数据库 1165、以及加密处理数据库 1604 的功能。此外，可以将加密信息存储部 1600 假定为具有响应于来自密钥管理部 1162、加密处理控制部 1156、和加密包管理部 1166 的请求，控制和管理加密信息存储部 1600 的那些数据库的功能。

[0081] 所述选择数据库 1601 具有如图 6 所示的这种数据结构。加密模块连接数据库 1602 具有如图 7 所示的这种数据结构。加密模块数据库 1603 具有如图 8 所示的这种数据结构。密钥信息数据库 1165 具有如图 9 所示的这种数据结构。加密处理数据库 1604 具有如图 10 所示的这种数据结构。图 11 示出了加密信息存储部 1600 的数据库之间的逻辑组成。

[0082] 加密包管理部 1166 具有下列功能。

[0083] 首先，加密包管理部 1166 具有在加密信息存储部 1600 中注册所选择的加密包 307 的算法标识符、加密模块评价描述标识符、加密模块标识符、和推荐的密钥长度信息的功能，上述信息是通过传输包括选择条件、选择策略、和硬件概况的信息获得，其中通过通信功能 1155 已经将所述选择条件、选择策略、和硬件概况从所述高级别系统部 1151 输入到加密模块管理服务器装置 1350。

[0084] 此外，加密包管理部 1166 具有基于从所述高级别系统部 1151 输入的请求，通过通信功能 1155，利用最后的初始注册日期和最后的初始注册域作为输入，在加密模块管理服务器装置 1350 上执行加密包初始注册协议的功能，从而可以从加密模块管理服务器装置 1350 下载最小需求数量的加密包 307，并在加密信息存储部 1600 中对它们进行注册。

[0085] 此外，加密包管理部 1166 具有将要在终端中保存的包括选择条件、选择策略、硬件概况、和加密包 307 的列表的信息通过通信功能 1155 传送到加密模块管理服务器装置 1350 的功能，其中已经从所述高级别系统部 1151 输入了所述选择条件、选择策略、硬件概况和在加密包 307 的列表，从而可以获得在该加密模块管理服务器装置 1350 中已经选择的加密包 307 实体及其附带信息（算法标识符、加密模块评价描述标识符和加密模块标识符），并在加密信息存储部 1600 中对它们进行注册。

[0086] 此外，加密包管理部 1166 具有在注册发生时或更新来自加密模块管理服务器装置 1350 的更新通知的目的地时，代替加密控制管理器部 1152 执行策略选择的功能。

[0087] 此外，加密包管理部 1166 具有基于所述高级别系统部 1151 请求的内容和在加密控制管理器部 1152 中保存的最后更新通知标识符，通过通信功能 1155，与加密模块管理服务器装置 1350 协作更新在加密控制管理器部 1152 中保存的加密包 307 实体和它的选择策略及链接之间的链接的功能。

[0088] 此外，加密包管理部 1166 具有通过从加密信息存储部 1600 删除该加密包 307 的

实体，来删除已经链接到由所述高级别系统部 1151 请求的加密包 30 的加密信息存储部 1600 的数据库之间的关联的功能。

[0089] 此外，加密包管理部 1166 具有将已经从所述高级别系统 1151 输入的包括在相关装置中保存的传递目的域信息、硬件概况和加密包 307 的列表的信息通过通信功能 1155 传送到加密模块管理服务器装置 1350 的功能，从而可以获取加密模块管理服务器装置 1350 已经选择的接受取出控制的加密包的信息，并从加密客户装置 1100 删除那些目标包。

[0090] 加密管理控制部 1170 具有响应于来自加密控制管理器部 1152 中的各个部的请求，通过通信功能 1155，在加密硬件上执行通信控制的功能。

[0091] 通信功能 1155 具有这样的功能，加密包管理部 1166 和硬件管理控制部 1170 可以与它们的伙伴通信装置或加密硬件互相通信。

[0092] 图 12 是加密模块管理服务器装置 1350 构成的功能框图。加密模块管理服务器装置 1350 包括服务器高级别系统部 1380、通信功能 1356、加密模块管理服务器控制部 1352、加密包存储部 1355、以及服务器加密控制管理器部 1390。

[0093] 服务器高级别系统部 1380 具有与加密客户装置 1100 的服务器高级别系统部 1380 相同的功能，并且另外还具有将来自系统管理器的涉及加密模块管理的控制请求传送到加密模块管理服务器控制部 1352 的功能。

[0094] 通信功能 1356 具有这样的功能，加密模块管理服务器控制部 1352 和服务器加密控制管理器部 1390 可以与它们的伙伴通信装置、加密硬件、或模拟该加密硬件操作的模拟器互相通信。

[0095] 加密模块管理服务器控制部 1352 包括加密包控制部 1359、加密包管理部 1351、加密包分发配置部 1370 和分发加密包选择部 1373。

[0096] 加密包控制部 1359 具有响应于来自服务器高级别系统部 1380 的请求注册加密包 307 的功能，响应于来自服务器高级别系统部 1380 的请求更新已经注册的加密包的功能，当从提供商分发加密包时，对确认相关加密包来源所需的证明提供商的认证码进行验证的功能，通过组合多个独立式加密模块评价描述部和多个复合类型加密模块评价描述部，产生复合类型加密模块评价描述部的功能，搜索加密模块数据库 1355 以查找在其中注册的加密包 307 并获取它们的列表的功能，响应于来自服务器高级别系统部 1380 的请求，从加密模块数据库 1355 删除加密模块 308 和相关的加密包 307 的功能，以及为在加密包存储部 1355 上执行的注册、更新、和删除处理输出日志的功能。

[0097] 加密包管理部 1351 具有并发执行处理来自多个加密客户装置 1100 的控制请求的功能，执行加密包 370 初始注册处理、传递处理、更新处理、选择处理、以及更新通知处理和加密模块管理域传递处理的功能，建立通信路径的功能，所述通信路径在加密客户装置 1100 和加密模块管理服务器装置 1350 之间的安全已经得到保护，管理在该加密模块管理服务器装置 1350 管理的域中出现的加密客户装置目前位置的功能，以及为加密包 370 初始注册处理、传递处理、更新处理、选择处理、以及更新通知处理和加密模块管理域传递处理产生日志的功能。

[0098] 加密包分发配置部 1370 具有从加密模块数据库 1355 获取由分发加密包选择部 1373 选择的加密包 307 的功能，将存储在加密模块数据库 1355 中的每个描述项目的数据配置为例如 XML 的加密模块评价描述格式并输出这种数据的功能，通过向服务器加密控制管

理器部 1390 请求进行与为密钥指定的安全方法相对应的处理，生成加密包控制部 1359 在安全通信中使用的密钥的功能，基于包括加密客户装置 1100 的标识符和安全方法的信息，管理密钥信息的功能，以及依照加密模块管理服务器装置 1350 的分发策略中定义的安全方法和安全级别，执行关于从加密模块管理服务器装置 1350 传送到加密客户装置 1100 的信息的数据保密和数据认证的安全处理的功能。

[0099] 分发加密包选择部 1373 具有执行初始注册决定、加密方法选择、以及在加密包初始注册处理中加密包选择的功能，在加密包传递处理中执行传递决定和加密包选择的功能，在加密包更新处理中执行传递决定的功能，在加密包更新处理中执行更新加密模块列表获取和加密包选择的功能，在加密包选择处理中执行选择决定和加密包选择的功能，在加密模块管理域传递处理中执行移动决定和域移动处理信息生成的功能，以及搜索加密包存储部以查找符合选择条件、选择策略、和硬件策略的加密包的功能。

[0100] 加密模块数据库 1355 包括加密模块数据库 1353 和加密模块评价数据库 1354，所述加密模块数据库 1353 记录和管理已经注册的加密模块 308，所述加密模块评价数据库 1354 记录和管理加密模块评价描述文件 309。

[0101] 服务器加密控制管理器部 1390 具有与加密客户装置 1100 中的加密控制管理器部 1152 几乎相同的功能，并且为了在加密模块管理服务器装置 1350 中执行加密资产管理控制和与任何其它通信装置进行安全认证通信，另外具有与加密模块管理服务器控制部 1352 链接的功能。

[0102] 其次，在使用由上述加密模块传递系统中的加密模块组成的复合加密模块的情况下，下面将描述加密模块管理装置，所述加密模块管理装置计算复合加密模块的评价值，利用该计算结果选择匹配选择请求的加密模块，并输出所选择的模块。

[0103] < 第三实施例 >

[0104] 下面将参照附图描述第三实施例。

[0105] 图 13 是根据本发明第三实施例的加密模块管理装置组成框图的略图。加密模块管理装置 1 包括加密模块元信息存储部 101、加密模块存储部 102、加密模块元信息查找部 103、存储部 104、复合类型加密模块评价计算部 105、加密模块选择部 106、以及加密模块获取部 107。该加密模块管理装置 1 响应于来自例如以无线或有线方式连接的终端设备的选择请求，选择加密模块，并向已经发送该选择请求的所述终端设备输出所选择的加密模块。

[0106] 来自终端设备的选择请求可以以加密方法或请求一起使用的形式出现，所述请求与要执行加密处理的环境相应发生，例如“需要安全数字签名生成模块”、“需要高速公共密钥加密模块”、或“需要要求少量使用存储器的散列函数模块”。该选择请求至少包括例如公共密钥加密和数字签名的加密模块的类别信息，并且可以进一步包括例如安全、速度、和使用存储量的条件，例如可执行平台、最大输入长度、和最大密钥长度的限制信息，以及已经创建加密模块的提供商的标识。

[0107] 加密模块元信息存储部 101 存储参与加密模块的加密模块元信息。加密模块存储部 102 存储多个加密模块。加密模块元信息查找部 103 基于来自终端设备的选择请求中包含的加密模块的类别信息，搜索加密模块元信息存储部 101 以查找加密模块元信息，并将所获得的加密模块元信息写入存储部 104。存储部 104 存储加密模块元信息查找部 103 的查找结果和复合类型加密模块评价计算部 105 的计算结果。

[0108] 如果由加密模块选择部 106 指定的加密模块元信息中包含关联加密模块类别信息，复合类型加密模块评价计算部 105 利用加密模块元信息查找部 103，查找关联加密模块的加密模块元信息，并将获得的每个关联加密模块的加密模块元信息指定为查找的结果，从而递归地调用它自身（复合类型加密模块评价计算部 105），由此基于作为结果获得的关联加密模块的评价信息和这些加密模块的加密模块元信息中包含的推导方法信息，产生复合类型加密模块评价信息。

[0109] 此外，如果由加密模块选择部 106 指定的加密模块的加密模块元信息中不包含关联加密模块类别信息，复合类型加密模块评价计算部 105 产生该加密模块的评价信息作为复合类型加密模块评价信息。

[0110] 加密模块选择部 106 响应于选择请求，基于由加密模块元信息查找部 103 指定的加密模块的加密模块元信息，调用复合类型加密模块评价计算部 105，从而获得复合类型加密模块评价信息。基于该获得的复合类型加密模块评价信息，加密模块选择部 106 选择加密模块。在该选择中，例如，选择这样的加密模块，它在从复合类型加密模块评价计算部 105 输出的复合类型加密模块评价信息中具有最高的分数。

[0111] 基于由加密模块选择部 106 指定的加密模块的加密模块名，加密模块获取部 107 从加密模块存储部 106 读取加密模块，并将它输出给已经发布选择请求的请求源（例如终端设备）。

[0112] 图 14 示出了加密模块元信息的一个实例。该加密模块元信息涉及每个加密模块并由已经创建加密模块或加密模块评价引擎的提供商创建。在加密模块管理装置 1 的加密模块元信息存储部 101 中与加密模块一起预先注册加密模块元信息，从而在加密模块元信息存储部 101 和加密模块存储部 102 中可以分别存储加密模块元信息和加密模块。

[0113] 该加密模块元信息包括加密模块名、加密模块类别（其对应上述类别信息）、和加密模块评价信息（其对应上述评价信息）。加密模块名（其对应上述加密模块识别信息）是识别相关加密模块的信息。加密模块类别是表示相关加密模块可以执行的加密处理的类别信息。应注意的是，加密模块类别包括例如普通密钥加密、公共密钥加密、数字签名、散列函数、伪随机数产生等。加密模块评价信息指示相关加密模块的评价结果，给出数值表示，例如加密模块的安全、速度、使用的存储量等的分数。该信息可以进一步描述相关加密模块可以执行的平台信息以及例如最大输入长度和最大密钥长度的使用限制。

[0114] 图 15 示出了加密模块评价信息的一个实例。在每块加密模块元信息的评价项目和评价分数彼此关联的条件下，预先存储该加密模块评价信息，所述评价分数是关于该评价项目的评价结果。所述评价项目包括例如安全、速度、使用存储量等等，从而这些评价项目中的每个评价项目与对应该评价项目的分数（例如 60、20 或 30）关联并进行存储。假定根据预定计算公式计算该评价分数。

[0115] 此外，如果需要关联加密模块执行相关加密模块，加密模块元信息也包含指示关联加密模块所属类别的关联加密模块类别信息。该“需要关联加密模块执行加密模块的情况”可以是，换句话说，加密模块在独立模式中不能执行加密处理的情况。例如，在一些情况中，不能执行诸如 RSASSA 的加密模块，除非它与执行散列函数和伪随机数生成的这种加密模块等进行组合。在这种情况中，加密模块的关联加密方法类别信息在其中存储需要与执行散列函数和伪随机数生成的这种模块进行组合的加密模块的类别，作为关联加密方法类

别信息。

[0116] 此外，如果相关加密模块为了它的执行需要关联加密模块，加密模块元信息包含指示推导复合类型加密模块评价信息的方法的复合类型加密模块评价计算公式信息（其对应上述推导方法信息），所述复合类型加密模块评价信息是基于在相关加密模块中设置的评价信息和在该关联加密模块中设置的评价信息，在相关加密模块已经与该关联加密模块进行组合的条件下已经执行了相关加密模块的情况的评价信息。该复合类型加密模块评价计算公式信息是包括复合类型加密模块评价计算公式的计算程序，所述复合类型加密模块评价计算公式用于在已经组合那些模块的情况下计算评价信息。类似于每块加密模块评价信息，复合类型加密模块评价信息在已经组合并执行相关加密模块和该关联加密模块的情况下给出了数字表示，例如，安全、速度、使用的存储量等的分数，并且可以进一步包含那些加密模块可以执行的平台信息，以及例如最大输入长度和最大密钥长度的使用限制。

[0117] 例如，在已经组合了执行数字签名的加密模块、计算散列函数的模块和生成伪随机数的加密模块的情况下计算关于安全的复合类型加密模块评价信息的情况中，数字签名模块的复合类型加密模块评价计算公式信息包含下列信息块。也就是，在分别利用加权因子 w1、w2 和 w3 累加指示数字签名模块安全的评价值和指示散列函数及伪随机数生成的每个类别安全的评价值，以提供所述组合的评价安全值的情况中，复合类型加密模块评价计算公式信息描述了下列计算公式 (1)：

[0118] （数字签名的评价安全值）＝ w1×（数字签名模块的评价安全值）+w2×（散列函数的评价安全值）+w3×（伪随机生成的评价安全值）(1)

[0119] 在该情况中，作为数字签名模块的评价安全值，替换在该数字签名模块的加密模块元信息中描述的评价值；并且如果进一步需要在要被组合或关联加密模块以执行这些加密模块的散列函数模块和伪随机数生成模块的每一个的加密模块元信息中描述的评价值，散列函数的评价安全值和伪随机数生成的评价安全值作为变量，在所述变量中替换从那些加密模块元信息块中描述的复合类型加密模块评价计算公式信息计算得到的评价值。

[0120] 此外，该复合类型加密模块评价计算公式信息包含加权因子 w1、w2 和 w3。

[0121] 图 16 是利用关联加密方法类别信息的加密模块元信息的说明图。

[0122] 如果加密模块元信息 A 包含关联加密方法类别信息，并且该关联加密方法类别信息具有设置在其中的类别“伪随机数生成”，被设置成“伪随机数生成”以作为加密模块类别的加密模块元信息（例如，在该情况中的加密模块元信息 C）所参与的加密模块 C 是关联加密模块之一。在这种情况中，加密模块元信息 A 具有较高的级别，而包含设置的加密模块类别信息的加密模块元信息具有较低级别，所述设置加密模块类别信息与关联加密方法类别信息相一致。

[0123] 此外，在这种情况中，如果加密模块元信息 C 也包含关联加密方法类别信息，并且该关联加密方法类别信息具有“散列函数”的类别，被设置成“散列函数”以作为加密模块类别的加密模块元信息（在该情况中的加密模块元信息 D）所参与的加密模块 D 是关联加密模块之一。在这种情况中应注意的是，加密模块元信息 D 不包含关联加密方法类别信息，并且因此相对于加密模块元信息 A 是最低级别的加密模块元信息。在这种情况中，在加密模块元信息 C 中也包含复合类型加密模块评价计算公式信息，描述下列计算公式 (2)，为例如计算伪随机数生成的模块和计算散列函数的模块的组合，计算复合类型加密模块安全评

价信息。

[0124] （伪随机数生成的评价安全值）＝w4×（伪随机数生成模块的评价安全值）+w5×（散列函数的评价安全值）(2)

[0125] 与计算公式 (1) 中的情况一样，作为伪随机数生成的评价安全值，替换在该数字签名的模块的加密模块元信息中描述的评价值；并且如果进一步需要在要被组合和关联加密模块以执行所述散列函数的加密模块的每个散列函数的加密模块元信息中描述的评价值，散列函数的评价安全值作为变量，在所述变量中替换从散列函数的加密模块元信息中描述的复合类型加密模块评价计算公式信息计算得到的评价值。此外，该复合类型加密模块评价计算公式信息包含加权因子 w4 和 w5。

[0126] 同样，如果加密模块元信息 A 进一步包含不同于“伪随机数生成”的关联加密方法类别信息，并且该关联加密方法类别信息具有设置在其中的类别“散列函数”，被设置成“散列函数”以作为加密模块类别的加密模块元信息（例如，在该情况中的加密模块元信息 B）所参与的加密模块 B 是关联加密模块之一。在该情况中，加密模块元信息 B 不包含关联加密方法类别信息，从而没有更低级别的加密模块元信息。

[0127] 其次，将参照图 16 进一步描述由复合类型加密模块评价计算部 105 所进行的计算。

[0128] 例如，如果在终端设备一侧需要“安全数字签名生成模块”，将包含要被选择的类别“数字签名”和评价项目“安全”的选择请求从终端设备传送到加密模块管理装置 1。然后，作为加密模块元信息查找部 103 的查找结果，如果加密模块元信息查找部 103 已经获得加密模块 A 的加密模块元信息 A 作为已经设置类别“数字签名”的加密模块，复合类型加密模块评价计算部 105 读取加密模块元信息 A 的关联加密方法类别信息，从而加密模块元信息查找部 103 查找加密模块元信息，在所述加密模块元信息中将该关联加密方法类别信息描述为加密模块类别。在这种情况中，在加密方法类别信息 A 的关联加密方法类别信息中描述类别“伪随机数生成”，从而加密模块元信息查找部 103 获取加密模块元信息 C 作为它的查找结果，在所述加密模块元信息 C 中将该“伪随机数生成”的类别描述为加密模块类别。

[0129] 如果找到加密模块元信息 C，复合类型加密模块评价计算部 105 判定该加密模块元信息 C 是否包含关联加密方法类别信息。在这种情况中，描述关联加密方法类别信息，从而复合类型加密模块评价计算部 105 从加密模块元信息 C 读取关联加密方法类别信息，并利用加密模块元信息查找部 103 由此查找加密模块元信息，在所述加密模块元信息中将该关联加密方法类别信息描述为加密模块类别。在这种情况中，在加密方法类别信息 C 的关联加密方法类别信息中描述类别“散列函数”，从而加密模块元信息查找部 103 获取加密模块元信息 D 作为它的查找结果，在所述加密模块元信息 D 中将该“散列函数”的类别描述为加密模块类别。

[0130] 如果找到加密模块元信息 D，复合类型加密模块评价计算部 105 判定该加密模块元信息 D 是否包含关联加密方法类别信息。在这种情况中，不包含关联加密方法类别信息，所以复合类型加密模块评价计算部 105 返回到前面的步骤，以进一步判定加密模块元信息 C 的关联加密方法类别信息是否包含其中所描述的类别。在这种情况中，在加密模块元信息 C 的关联加密方法类别信息中除了“散列函数”之外没有描述更多的类别，使得复合类型加

密模块评价计算部 105 返回到更前面的步骤，以进一步判定加密模块元信息 A 的关联加密方法类别信息是否包含其中所描述的类别。在这种情况中，在加密模块元信息 A 的关联加密方法类别信息中描述了除“伪随机数生成”之外的类别“散列函数”，使得加密模块元信息查找部 103 用于进一步查找加密模块元信息，在所述加密模块元信息中将“散列函数”描述为加密模块类别。在这种情况中，获取加密模块元信息 B 作为它的查找结果。在这种情况中，可以替代地获取散列函数的加密模块元信息 D，所述加密模块元信息 D 作为伪随机数生成的较低级别模块已经被找到。如果找到加密模块元信息 B，复合类型加密模块评价计算部 105 判定该加密模块元信息 B 是否包含关联加密方法类别信息。在这种情况中，不包含关联加密方法类别信息，使得它返回到前面的步骤，以进一步判定加密模块元信息 A 的关联加密方法类别信息是否包含其中所描述的类别。在这种情况中，由于没有描述更多的类别，所述过程结束查找加密模块元信息。

[0131] 随后，复合类型加密模块评价计算部 105 利用作为查找结果获得的元信息块 A、B、C 和 D 的加密模块的块，生成复合类型加密模块评价信息。

[0132] 首先，复合类型加密模块评价计算部 105 利用包括最低级别加密模块元信息 D 的加密模块元信息块 C 和 D，从而产生伪随机数生成的复合类型加密模块评价信息。从加密模块元信息 C 和 D 的加密模块评价信息块中，复合类型加密模块评价计算部 105 读取与加密模块元信息查找部 103 接收的“安全”评价项目一致的评价项目中的评价分数。在这种情况中，例如，如果加密模块元信息 C 中的“安全”评价分数是“40”并且加密模块元信息 D 中的“安全”评价分数是“60”，复合类型加密模块评价计算部 105 读取这些分数中的每一个。

[0133] 接着，复合类型加密模块评价计算部 105 依照计算公式 (2) 计算复合类型加密模块评价信息，以得到在加密模块元信息 C 的复合类型加密模块评价计算公式信息中描述的伪随机数生成的评价安全值。在这种情况中，如果在复合类型加密模块评价计算公式信息中包含为 0.3 的 W4 值和为 0.5 的 W5 值，复合类型加密模块评价计算部 105 基于那些公式和值计算 0.3×40+0.5×60，作为伪随机数生成的评价安全值，从而获得 42 作为伪随机数生成的评价安全值的计算结果。应注意的是，在加密模块元信息 C 和加密模块元信息 D 组合的情况下，该计算结果是评价安全值，使得例如如果存在不同于加密模块元信息 D 的散列函数类别的加密模块元信息 E，在加密模块元信息 C 的复合类型加密模块评价计算公式信息的计算中利用该加密模块元信息 E 的评价安全值；由此，在一些情况中，即使属于同一“散列函数”类别的加密模块元信息也可以出现不同的评价结果。

[0134] 在加密模块元信息 C 和加密模块元信息 D 组合的情况下，如果获得伪随机数生成的安全评价结果，复合类型加密模块评价计算部 105 利用上述伪随机数生成、加密模块元信息 A 和级别上直接位于元信息 A 下面的加密模块元信息 B 的安全评价计算结果，计算数字签名的评价安全值，所述数字签名的评价安全值是在级别上比加密模块元信息 C 高的加密模块元信息 A 的组合的评价安全值。在这种情况中，复合类型加密模块评价计算部 105 利用加密模块元信息 A 的加密模块评价信息（作为一个实例将其假定为 60）、通过上面的计算获得的伪随机数生成的评价安全值的计算结果 42、加密模块元信息 B 的加密模块评价信息（作为一个实例将其假定为 50）、以及计算公式 (1)，计算数字签名的评价安全值，所述计算公式 (1) 提供加密模块元信息 A 的复合类型加密模块评价计算公式信息，所述加密模块元信息 A 在级别上比那些信条息高。在这种情况中，如果在复合类型加密模块评价计算公

式信息中将 W1、W2 和 W3 分别描述为 0.7、0.4 和 0.3，复合类型加密模块评价计算部 105 基于这样的公式和值，计算 0.7×60+0.4×50+0.3×42 作为数字签名的评价安全值，从而获得数字签名的评价安全值的计算结果 74.6。

[0135] 此外，复合类型加密模块评价计算部 105 利用加密模块元信息查找部 103，从而同样也为除了加密模块元信息块 A、B、C 和 D 之外的所有信息块组合计算复合类型加密模块评价信息。例如，如果除了加密模块元信息 B 之外，加密模块元信息查找部 103 找到其中将“散列函数”描述为加密模块类别的加密模块元信息 F，同样在元信息 A、F、C 和 D 的加密模块的块组合的情况下，复合类型加密模块评价计算部 105 计算复合类型加密模块评价信息。在这种情况中，复合类型加密模块评价计算部 105 利用通过对加密模块元信息 A 的加密模块评价信息、加密模块元信息 F 的加密模块评价信息（例如将其假定为 20）、以及元信息 C 和 D 的加密模块的块和计算公式 (1) 进行组合获得的伪随机数生成的评价安全值的结果，计算复合类型加密模块评价信息，所述计算公式 (1) 提供加密模块元信息 A 的复合类型加密模块评价计算公式信息，所述加密模块元信息 A 在级别上比那些信息块高。也就是，在这种情况中，复合类型加密模块评价计算部 105 计算 0.7×60+0.4×20+0.3×42，从而获得所述组合的评价安全值的计算结果 62.6。

[0136] 如果已经为这样找到的加密模块元信息块的所有组合获得复合类型加密模块评价信息，复合类型加密模块评价计算部 105 对于加密模块元信息块的所有组合中的每一个组合，将一组指示在复合类型加密模块评价信息的计算中利用的加密模块元信息块的组合的信息和所获得的复合类型加密模块评价信息输出到加密模块选择部 106。例如，在上面的组合情况中，将指示加密模块元信息块 A、B、C 和 D 已经组合的信息和指示该组合的复合类型加密模块评价信息为 74.6 的信息输出到加密模块选择部 106。

[0137] 应注意的是，在关于例如使用存储量的评价值的复合类型评价信息的计算中已经找到加密模块元信息 D 而不是找到加密模块元信息 B，并且所计算的复合类型加密模块评价信息具有加密模块元信息块 A、B、C 和 D 的组合的情况下，如果将类似于上述复合类型加密模块安全评价信息的复合类型加密模块评价计算公式信息描述为加密模块元信息 A 的复合类型加密模块评价计算公式信息，可能冗余地增加加密模块元信息 D 使用的存储量的评价值，因而给出复合类型加密模块评价的不适当值。在这种情况中，复合类型加密模块评价计算公式信息可以具有其中描述的这样的条件表达式，即不需要冗余地增加同一加密模块的评价信息。

[0138] 接着，下面将描述依照上述第三实施例的加密模块管理装置 1 的操作。图 17 是加密模块管理装置 1 的操作的说明性流程图。首先，如果终端设备一侧需要“安全数字签名模块”，从终端设备向加密模块管理装置 1 传送包含类别“数字签名”和所选评价项目“安全”的选择请求。

[0139] 如果从终端设备向加密模块管理装置 1 传送选择请求，加密模块管理装置 1 中的加密模块元信息查找部 103 接收该选择请求（步骤 S101）。接着，加密模块元信息查找部 103 搜索加密模块元信息存储部 101，以查找指示在接收的选择请求中包含的类别“数字签名”的类别的加密模块元信息（步骤 S102）。然后，加密模块元信息查找部 103 将作为它的查找结果获得的加密模块元信息写入存储部 104（步骤 S103）。在这种情况中，如果已经找到多个加密模块元信息块作为查找的结果，将那些获取的加密模块元信息块中的每一块写

入存储部 104。

[0140] 如果将加密模块元信息写入存储部 104，复合类型加密模块评价计算部 105 利用在存储部 104 中作为起点存储的加密模块元信息，判定在该加密模块元信息中是否包含关联加密方法类别信息（步骤 S104）。

[0141] 如果在加密模块元信息中不包含关联加密方法类别信息（步骤 S104 的否），复合类型加密模块评价计算部 105 产生加密模块元信息的加密模块评价信息（在这种情况中为“安全”评价项目的评价分数）作为复合类型评价信息（步骤 S105）。

[0142] 另一方面，如果在加密模块元信息中包含关联加密方法类别信息（步骤 S104 的是），复合类型加密模块评价计算部 105 利用加密模块元信息查找部 103 在与该关联加密方法类别信息的类别一致的类别中查找加密模块的加密模块元信息，并指定作为查找结果获得的每个关联加密模块的加密模块元信息，从而递归调用它自身，由此基于作为结果获得的关联加密模块的评价信息（在这种情况中为“安全”评价项目的评价分数）和在这些加密模块的加密模块元信息中包含的复合类型加密模块评价计算公式信息，产生复合类型加密模块评价信息（步骤 S106）。

[0143] 如果产生复合类型加密模块评价信息，加密模块选择部 106 判定是否为在存储部 104 中存储的所有加密模块元信息块计算复合类型加密模块评价信息（步骤 S107），并且如果其上仍要计算复合类型加密模块评价信息的加密模块元信息块的组合在那些存储在存储部 104 中的加密模块元信息块之中出现，转移到步骤 S104（步骤 S107 的否）以指定加密模块元信息，以便复合类型加密模块评价计算部 105 可以计算复合类型加密模块评价信息。

[0144] 另一方面，如果为在存储部 104 中存储的所有加密模块元信息块计算复合类型加密模块评价信息（步骤 S107 的是），加密模块选择部 106 基于由复合类型加密模块评价计算部 105 计算的加密模块评价信息的复合类型块的组合的复合类型加密模块评价信息，以及在那些复合类型加密模块评价信息块的计算中使用的加密模块元信息块，选择这种具有最高评价分数的复合类型加密模块评价信息（步骤 S108），并将要与该复合类型加密模块评价信息进行组合的这种加密模块元信息输出到加密模块获取部 107。

[0145] 如果从加密模块选择部 106 输出加密模块元信息，加密模块获取部 107 基于在加密模块元信息中包含的加密模块名，读取在加密模块存储部 102 中存储的加密模块，并将所读取的加密模块传递到已经请求选择的终端设备（步骤 S109）。

[0146] 接着，下面将参照图 18 的流程图描述根据第三实施例的加密模块管理装置 1 的变体。

[0147] 首先，如果在终端设备一侧需要“安全数字签名生成模块”，从所述终端设备向加密模块管理装置 1 传送包含类别“数字签名”和所选评价项目“安全”的选择请求。

[0148] 如果从终端设备向加密模块管理装置 1 传送选择请求，加密模块管理装置 1 中的加密模块元信息查找部 103 接收该选择请求（步骤 S201）。接着，加密模块元信息查找部 103 搜索加密模块元信息存储部 101，以查找指示在接收的选择请求中包含的类别“数字签名”的类别的加密模块元信息（步骤 S202）。然后，加密模块元信息查找部 103 将作为它的查找结果获得的加密模块元信息写入存储部 104（步骤 S203）。在这种情况中，如果已经找到多个加密模块元信息块作为查找的结果，加密模块元信息查找部 103 将那些获取的加密

模块元信息块都写入存储部 104。

[0149] 如果将加密模块元信息块写入存储部 104，复合类型加密模块评价计算部 105 从存储部 104 中存储的那些加密模块元信息块中选择性地读取其上仍要计算复合类型加密模块评价信息的加密模块元信息（步骤 S204），并判定在该读取的加密模块元信息中是否包含关联加密方法类别信息（步骤 S205）。

[0150] 如果在加密模块元信息中不包含关联加密方法类别信息（步骤 S205 的否），复合类型加密模块评价计算部 105 生成加密模块元信息的加密模块评价信息（在这种情况中为“安全”评价项目的评价分数）作为复合类型评价信息（步骤 S206）。

[0151] 另一方面，如果在加密模块元信息中包含关联加密方法类别信息（步骤 S205 的是），复合类型加密模块评价计算部 105 利用加密模块元信息查找部 103 在与该关联加密方法类别信息的类别一致的类别中递归查找加密模块的加密模块元信息（步骤 S206）。重复该查找，并且加密模块元信息查找部 103 将其结果存储到存储部 104 中，直至遇到不包含关联加密方法类别信息的加密模块元信息。

[0152] 然后，如果将查找结果存储在存储部 104 中，假定不包含关联加密方法类别信息的加密模块元信息具有较低的级别，并且从存储部 104 读取的加密模块元信息具有较高的级别，复合类型加密模块评价计算部 105 基于在存储部 104 中存储的该查找结果按照递升的顺序计算信息块（步骤 S208）。在该计算中，基于加密模块元信息的加密模块评价信息、属于相关加密模块元信息的关联加密方法类别信息的关联加密模块的加密模块评价信息、以及在相关加密模块的加密模块元信息中包含的复合类型加密模块评价计算公式信息，复合类型加密模块评价计算部 105 产生计算结果作为加密模块的复合类型加密模块评价信息。

[0153] 如果产生复合类型加密模块评价信息，复合类型加密模块评价计算部 105 判定是否为在存储部 104 中存储的所有加密模块元信息块计算复合类型加密模块评价信息（步骤 S209），并且如果其上仍要计算复合类型加密模块评价信息的加密模块元信息块的组合在那些存储在存储部 104 中的加密模块元信息块之中出现，处理转移到步骤 S204（步骤 S209 的否）。

[0154] 另一方面，如果为存储部 104 中存储的所有加密模块元信息块计算复合类型加密模块评价信息（步骤 S209 的是），复合类型加密模块评价计算部 105 向加密模块选择部 106 输出所计算的复合类型加密模块评价信息和在该复合类型加密模块评价信息的计算中使用的加密模块元信息的组合。如果计算多个加密模块评价信息的复合类型块，它意味着存在所计算的复合类型加密模块评价信息和在该复合类型加密模块评价信息的计算中使用的加密模块元信息的多个组合，并将那些多个组合中的每个组合输出到加密模块选择部 106。

[0155] 如果从复合类型加密模块评价计算部 105 输出复合类型加密模块评价信息和加密模块元信息的组合，加密模块选择部 106 基于复合类型加密模块评价信息块，从由复合类型加密模块评价信息和自复合类型加密模块评价计算部 105 输出的加密模块元信息构成的组合中选择这种具有最高分数的复合类型加密模块评价信息（步骤 S210），并将该复合类型加密模块评价信息和与其进行组合的加密模块元信息输出到加密模块获取部 107。

[0156] 如果从加密模块选择部 106 输出加密模块元信息，加密模块获取部 107 基于在加

密模块元信息中包含的加密模块名，读取在加密模块存储部 102 中存储的加密模块，并将所读取的加密模块传递到已经请求选择的终端设备（步骤 S211）。

[0157] 根据上述第三实施例，如果需要关联加密模块以执行加密模块，在评价中将加密模块和关联加密模块进行组合，从而基于评价的结果，响应于选择请求，可以从加密模块的组合中选择加密模块，并将这种加密模块传递到已经请求选择的终端设备。

[0158] 虽然已经参照将评价项目和评价分数彼此关联作为加密模块评价信息并进行存储的情况描述了上面的第三实施例，但是也可以存储例如加密模块可以执行的平台、最大输入长度、和最大密钥长度的使用限制信息，从而将终端设备的选择请求从终端设备传送到包含终端使用环境信息的加密模块管理装置，所述终端使用环境信息指示该终端设备的使用环境（例如，终端设备可以执行的平台、最大输入长度和最大密钥长度）。

[0159] 在这种情况中，加密模块管理装置 1 中的加密模块选择部 105 可以计算复合类型加密模块评价信息、按照该计算的复合类型加密模块评价信息的递减顺序分类加密模块、然后按照复合类型加密模块评价信息的递减顺序比较参与加密模块的加密模块评价信息的使用限制信息块和已经请求选择的终端设备的终端使用环境信息块，从而选择附带这种满足由终端设备的终端使用环境信息指示的环境的使用限制信息的加密模块。例如，如果终端使用环境信息中包含的最大输入长度和最大密钥长度分别与使用限制信息中的最大输入长度和最大密钥长度一致，所述使用限制信息包含与终端设备可以执行的平台一致的可执行平台，并且在附加到加密模块的加密模块评价信息中包含所述使用限制信息，将选择这种满足由终端设备的终端使用环境信息指示的环境的使用限制信息。因此，在符合终端设备使用条件的同时，选择具有最高评价的加密模块是有可能的。

[0160] < 第四实施例 >

[0161] 接着，下面将描述第四实施例。相对于已经参照在从终端设备接收选择请求时评价加密模块的组合，从而基于评价的结果可以选择加密模块并将其传递到终端设备的情况所描述的第三实施例，将参照预先评价并存储加密模块组合的情况描述第四实施例。

[0162] 下面将参照附图描述第四实施例。图 19 是根据第四实施例的加密模块管理装置的构成图。在该图形中，加密模块管理装置 2 包括元信息存储部 201、加密模块注册装置 202、元信息查找部 203、加密模块选择部 204、加密模块获取部 205 和加密模块存储部 206。加密模块选择部 204、加密模块获取部 205 和加密模块存储部 206 对应第三实施例中的加密模块选择部 106、加密模块获取部 107 和加密模块存储部 102，并且分别具有同样的功能。

[0163] 元信息存储部 201 存储加密模块元信息和复合类型元信息。该加密模块元信息与第三实施例中描述的加密模块元信息非常相似。加密模块注册装置 202 具有关联加密模块查找部 210、复合类型加密模块评价计算部 211 和复合类型元信息生成部 212。

[0164] 关联加密模块查找部 210 接收从注册请求装置传送的加密模块和该加密模块的加密模块元信息，所述注册请求装置以无线或有线方式连接到外界。然后，首先，如果在该加密模块元信息的关联加密方法类别信息中描述了类别，关联加密模块查找部 210 搜索元信息存储部 201，以查找复合类型元信息，所述复合类型元信息的复合类型加密方法类别与该类别一致（较低级别模块的复合类型元信息），并输出一组作为查找结果获得的该加密模块元信息和复合类型元信息。另一方面，如果在该加密模块元信息的关联加密方法类别信息中没有描述类别，首先关联加密模块查找部 210 仅输出该加密模块元信息。此外，依照

该加密模块元信息中的加密模块类别，关联加密模块查找部 210 查找这种关联加密方法类别信息中描述的类别可与该加密模块类别一致的加密模块元信息（较高级别模块的加密模块元信息），并输出作为查找结果获得的一组该加密模块元信息、较低级别复合类型元信息、和较高级别加密模块元信息。在这种情况中，如果在找到的加密模块元信息的关联加密方法类别信息中描述了类别，关联加密模块查找部 210 进一步搜索元信息存储部 201 以查找这种复合类型加密方法类别可与该关联加密方法类别信息中的类别一致的复合类型元信息，并且也输出作为结果获得的复合类型元信息。关联加密模块查找部 210 进一步递归搜索元信息存储部 201 以查找这种在所获得的较高级别加密模块元信息中的加密模块类别可与关联加密模块类别信息一致的加密模块元信息（进一步的较高级别的加密模块元信息），并输出这对信息。重复该过程直至找不到较高级别的加密模块元信息。简而言之，关联加密模块查找部 210 查找并输出对应于加密模块组合的所有加密模块元信息和复合类型元信息组，所述加密模块组合在包括从注册请求装置传送的加密模块的条件下可以执行。在这种情况中，只需要搜索复合类型元信息块以查找较低级别的加密模块组合，从而减少查找的麻烦。

[0165] 复合类型加密模块评价计算部 211 利用加密模块元信息中的加密模块评价信息，和在属于加密模块元信息的关联加密方法类别信息中描述的加密模块类别的加密模块（较低级别的模块）的加密模块元信息中描述的加密模块评价信息，或者在关联加密模块查找部 210 已经找到的加密模块元信息和复合类型元信息的组合的复合类型元信息中描述的复合类型加密模块评价信息，并且依照该较低级别模块所属的较高级别模块的复合类型加密模块评价计算公式信息，计算复合类型加密模块评价信息，所述复合类型加密模块评价信息是这些组合的评价值。

[0166] 复合类型元信息生成部 212 基于复合类型加密模块评价计算部 211 的计算结果，产生复合类型元信息，并将它写入元信息存储部 201。在这个实施例中，复合类型元信息生成部 212 也将关联加密模块查找部 210 接收的加密模块元信息写入元信息存储部 201。

[0167] 图 20 示出了复合类型元信息的一个实例。复合类型元信息包含复合类型名、复合类型加密方法类别、复合类型评价信息和关联加密模块名。

[0168] 在这个实施例中，复合类型名是标识加密模块组合的信息。存储这种在加密模块的组合中指示最高级别加密模块类别的类别作为复合类型加密方法类别。存储这种复合类型加密模块评价计算部 211 已经生成的复合类型加密模块评价信息作为复合类型评价信息。存储在复合类型加密模块评价信息的计算中已经组合的加密模块的加密模块名作为关联加密模块名。

[0169] 接着，下面将参照图 21 描述这样构成的加密模块管理装置 2 的操作。下面，描述在已经将多个加密模块、加密模块元信息、和复合类型加密元信息存储在加密模块管理装置 2 中的情况下，将还要存储在加密模块管理装置 2 中的加密模块存储到其中的操作。图 21 是根据第四实施例的加密模块管理装置 2 的操作的说明性流程图。

[0170] 如果将加密模块和加密模块元信息与注册请求一起从连接到加密模块管理装置 2 外部的注册请求装置传送到加密模块管理装置 2，关联加密模块查找部 210 接收这些加密模块和加密模块元信息（步骤 S301）。如上所述，关联加密模块查找部 210 搜索元信息存储部 201，以查找一组加密模块元信息和复合类型元信息（步骤 S302）。

[0171] 如果关联加密模块查找部 210 获得这组加密模块元信息和复合类型元信息，复合类型加密模块评价计算部 211 为如上所述的这些组合生成复合类型加密模块评价信息（步骤 S303）。

[0172] 然后，如果产生复合类型加密模块评价信息，复合类型加密元信息生成部 212 生成复合类型加密元信息（步骤 S304），并将所生成的复合类型加密元信息和关联加密模块查找部 210 接收的加密模块元信息写入元信息存储部 201（步骤 S305）。在这种情况中，基于复合类型加密模块评价计算部 211 已经为其生成复合类型加密模块评价信息的加密模块元信息和复合类型元信息的组合，复合类型加密元信息生成部 212 生成标识该组合的信息，并将它作为复合类型加密方法名写入元信息存储部 201 中的复合类型元信息。此外，复合类型加密元信息生成部 212 将复合类型加密模块评价计算部 211 已经为其生成复合类型加密模块评价信息的加密模块元信息组合中的最高级别加密模块的加密模块元信息的类别与该生成的复合类型加密方法名相关联，并将这种信息写入元信息存储部 201 中的复合类型元信息。此外，复合类型加密元信息生成部 212 将复合类型加密模块评价计算部 211 计算的复合类型加密模块评价信息与该生成的复合类型加密方法名相关联，并将这种加密模块评价信息写入元信息存储部 201 中的复合类型加密模块评价信息。此外，如果复合类型加密模块评价计算部 211 计算复合类型加密模块评价信息，复合类型加密元信息生成部 212 将各组合加密模块元信息块的加密模块名与该生成的复合类型加密方法名相关联，并将结果信息作为关联加密模块名写入元信息存储部 201 中的复合类型元信息。

[0173] 然后，如果找到还没有生成复合类型加密元信息的加密模块元信息组合作为关联加密模块查找部 210 为多个组合进行查找的结果，复合类型加密元信息生成部 212 转移到步骤 S303(S306 的否），并且如果没有找到这样的组合，结束处理（S306 的是）。按照这种方式，生成复合类型元信息并将其存储在元信息存储部 201。

[0174] 在元信息存储部 201 中这样注册复合类型元信息之后，在终端设备一侧需要“安全数字签名生成模块”的情况中，如果将包含类别“数字签名”和所选评价项目“安全”的选择请求从终端设备传送到加密模块管理装置 2，元信息查找部 203 依照来自终端设备的选择请求中包含的类别，查找元信息存储部 201，并获得其复合类型加密方法类别与该类别一致的复合类型元信息，然后将所获得的复合类型加密元信息输出到加密模块选择部 204。

[0175] 与第三实施例中的情况一样，加密模块选择部 204 基于复合类型元信息中描述的评价信息选择符合需求的最优复合类型元信息，基于所选的复合类型加密元信息的关联加密模块名从加密模块存储部 206 读取加密模块，并将它输出到终端设备。

[0176] 如上所述，在接收到加密模块注册请求的时间点，计算每个加密模块组合的加密模块评价并将其写入元信息存储部 201，从而消除了在接收到选择请求的时间点计算评价信息的需要。因此，当与接收选择请求之后计算评价信息的情况进行比较时，从接收选择请求到选择加密模块的处理负荷可以减少计算评价信息的处理那么多。因而容纳来自多个客户的加密模块选择请求是可能的。

[0177] < 第五实施例 >

[0178] 接着，下面将描述第五实施例。将参照如果加密模块是危险的，从加密模块管理装置删除该加密模块的情况描述该第五实施例。

[0179] 图 22 是根据第五实施例的加密模块管理装置 3 的组成框图的略图。在该图形中，

元信息关联表存储部 301 存储加密模块和该加密模块所需的关联加密模块之间的关系。元信息存储部 302 存储复合类型元信息和加密模块元信息。这些复合类型元信息和加密模块元信息与例如第四实施例中的那些相同。加密模块存储部 303 存储加密模块。

[0180] 删除部 304 从连接到加密模块管理装置 3 的外部的管理装置接收危险加密模块的加密模块名和删除请求，基于所接收的加密模块名查找元信息关联表存储部 301，并且基于查找的结果删除与接收的加密模块名相匹配的加密模块。

[0181] 图 23 是示出元信息关联表的一个实例的表，所述元信息关联表存储在元信息关联表存储部 301 中。在该图形中，元信息关联表由较高级别的模块名和较低级别的模块名组成。在当前实施例中，将加密模块元信息中的加密模块名关联到较高级别模块名的加密模块名，在所述加密模块元信息中设置了与包含所述较高级别模块名的该加密模块名的加密模块元信息中的关联加密方法类别一致的类别。

[0182] 此外，如果在具有作为较低级别模块名存储的加密模块名的加密模块中包括关联加密模块，将作为该较低级别信息存储的加密模块名和关联加密模块的加密模块名分别作为较高级别模块名和较低级别模块名存储在元信息关联表中。

[0183] 在图 23 中，对于加密模块名 a，分别关联和存储较低级别加密模块名 b 和 c。同样，对于加密模块名 c，关联和存储较低级别加密模块名 d。

[0184] 下面将描述这样构成的加密模块管理装置 3 的操作。在此假定在较高级别加密模块名和较低级别加密模块名彼此关联的条件下，将较高级别加密模块名和较低级别加密模块名存储在元信息关联表存储部 301 中。

[0185] 如果从外部管理装置向加密模块管理装置 3 传送加密模块名和删除请求，删除部 303 搜索元信息关联表存储部 301 以查找较低级别模块名，从而判定它们是否包括任何与请求要被删除的加密模块名一致的加密模块名。如果那些较低级别的模块名不包括与请求要被删除的加密模块名一致的加密模块名，删除部 303 结束处理，如果那些较低级别模块名包括与请求删除的加密模块名一致的加密模块名，从元信息关联表存储部 301 删除那些较低级别模块名和对应那些较低级别模块名的较高级别模块名的加密模块名，基于删除的加密模块名从元信息存储部 201 删除加密模块元信息，并且此外，基于这样删除的加密模块名从加密模块存储部 303 删除加密模块。

[0186] 作为根据该第五实施例的另一个效果，同样如果你想知道多少个较低级别的模块参考了加密模块，以便于知道如果那个加密模块是危险的，对系统的影响程度，你可以通过参考该元信息管理表了解那些较高级别模块的数量。

[0187] 应注意的是，在加密模块传递系统中，可以将上述加密模块管理装置 1、2 和 3 安装到服务器装置一侧或客户终端一侧。例如，如果在客户终端一侧可以预先保存多个加密模块，所述客户终端中的该加密模块管理装置可以管理那些加密模块。因而，响应于来自应用程序的加密模块请求，仅在客户中有效地选择和管理加密模块是可能的。

[0188] 可以将执行图 2、3、5、12、13、19 和 22 中的加密客户装置、加密模块管理服务器和加密模块管理装置的功能所需的程序记录在计算机可读记录介质中，以便于将其读入计算机系统并执行，从而管理加密模块。应注意的是，这里将术语“计算机系统”假定为包括操作系统和例如外围设备的硬件。

[0189] 此外，如果利用了 WWW 系统，将术语“计算机系统”假定为包括主页提供环境（或

显示环境）。

[0190] 此外，术语“计算机可读记录介质”涉及可移动介质，例如软盘、磁光盘、ROM、或CD-ROM或例如硬盘的内置在计算机系统中的存储设备。而且，将术语“计算机可读记录介质”假定为也包括短时期内动态保存程序的介质，例如通过诸如因特网的网络来传输程序的情况中的通信电线、或者例如电话线路的通信线路，以及某个时期内保存程序的介质，例如计算机系统内部的易失性存储器，在这种情况中所述计算机系统作为服务器或客户使用。此外，可以提供该程序以实现某些上述功能，或者甚至可以通过组合计算机系统中已经记录的程序来实现那些功能。

[0191] 虽然已经参照附图详细描述了本发明的实施例，但是应该理解，本发明不局限于那些实施例的特定构成，并且包含了这种不背离本发明要点的设计等。

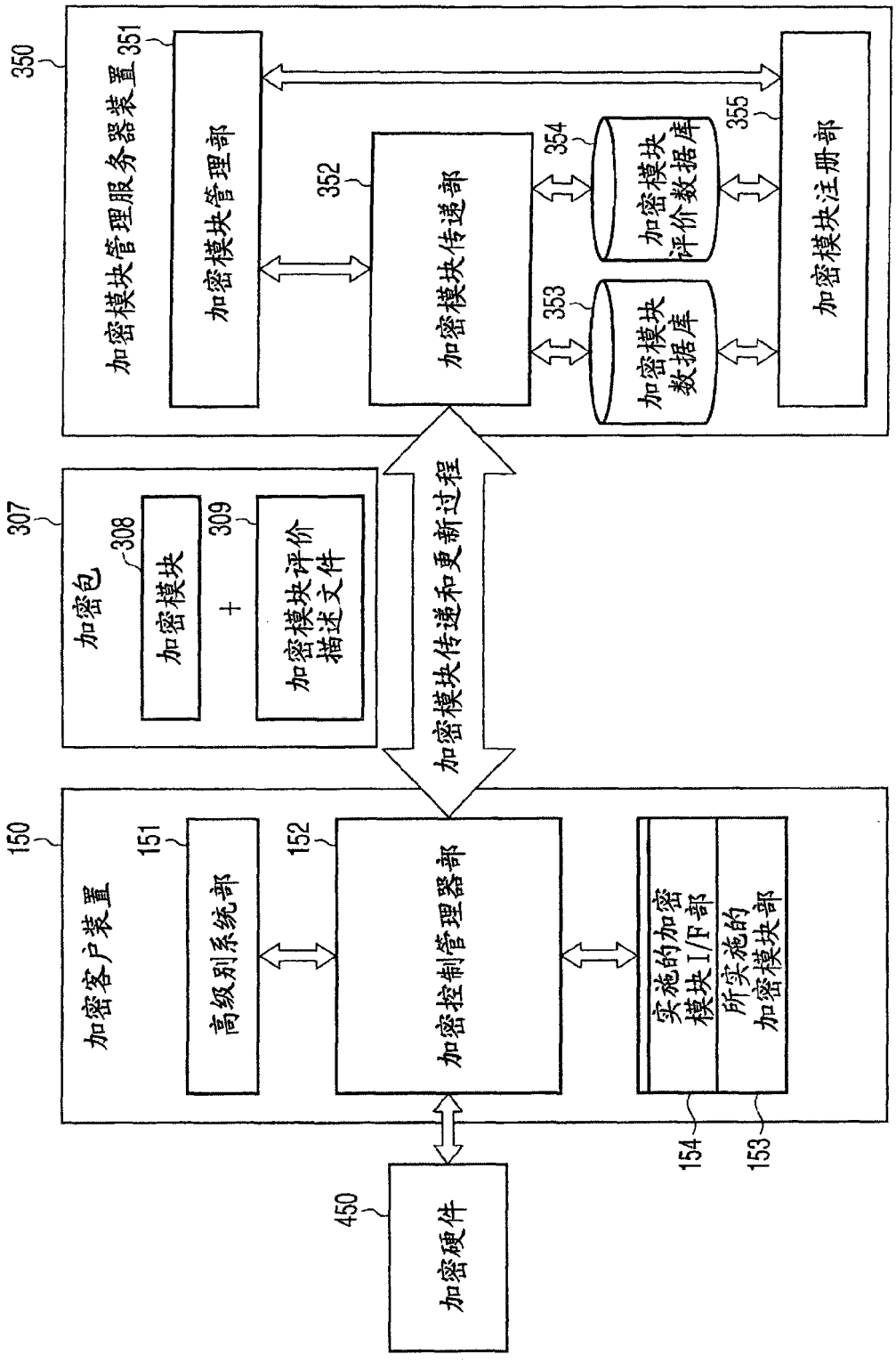
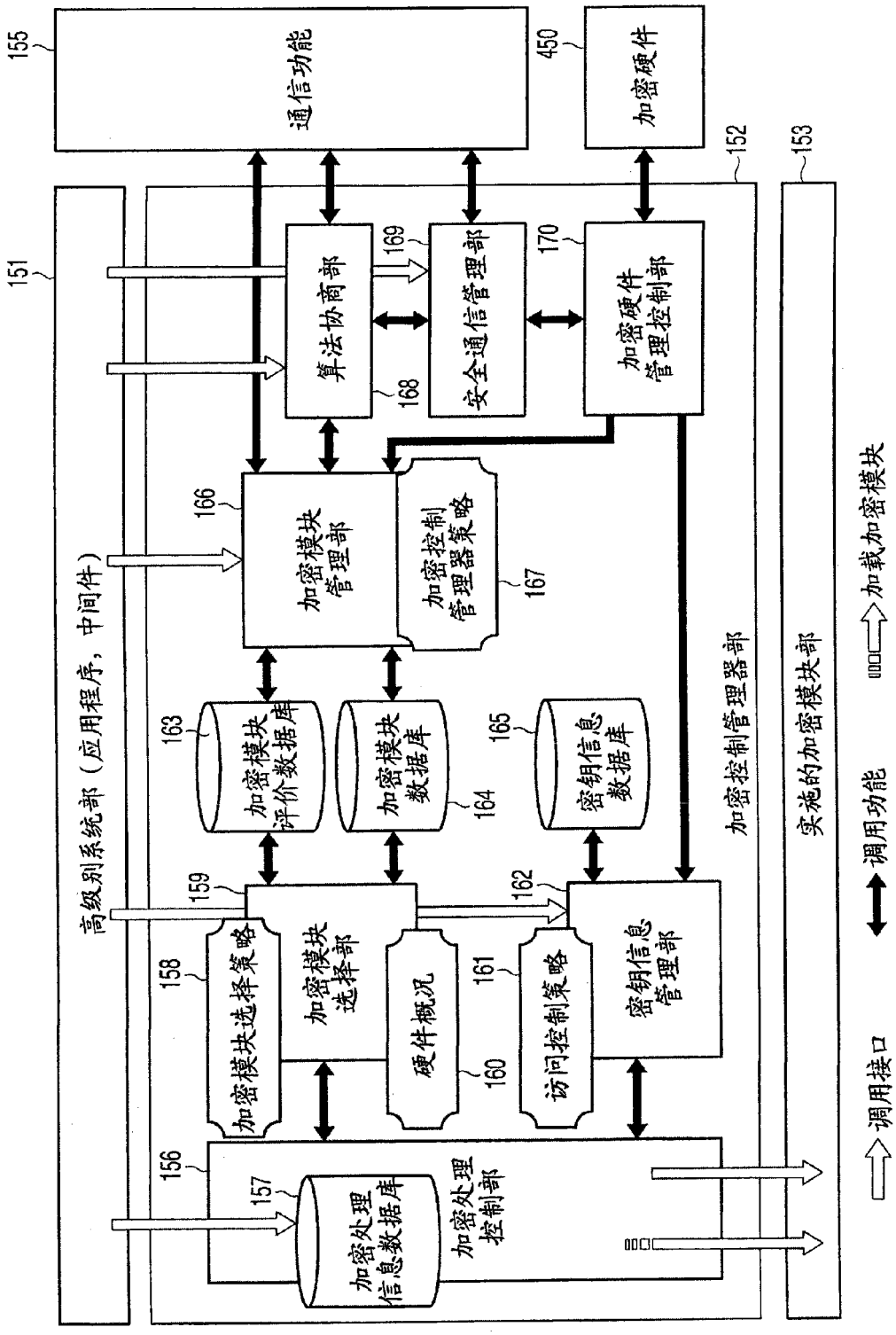

350
加密模块管理服务器装置
351
加密模块管理部
352
加密模块/传递部
354
加密模块评价数据库
355
加密模块注册部
353
加密模块数据库
加密模块传递和更新过程
307
加密包
308
加密模块
+
309
加密模块评价描述文件
150
加密客户装置
151
高级别系统部
152
加密控制管理器部
实施的加密模块I/F部
所实施的加密模块部
154
153
450
加密硬件

图 1


155
通信功能
450
加密硬件
152
153
151
算法协商部
169
安全通信管理部
170
加密硬件管理控制部
168
166
加密模块管理部
加密控制管理器策略
167
163
加密模块评价数据库
加密模块数据库
164
165
密钥信息数据库
高级别系统部（应用程序，中间件）
加密控制管理器部
实施的加密模块部
159
162
加密模块选择策略
158
加密模块选择部
硬件概况
161
访问控制策略
密钥信息管理部
160
156
157
加密处理信息数据库
加密处理控制部
调用接口
调用功能
加载加密模块
图 2

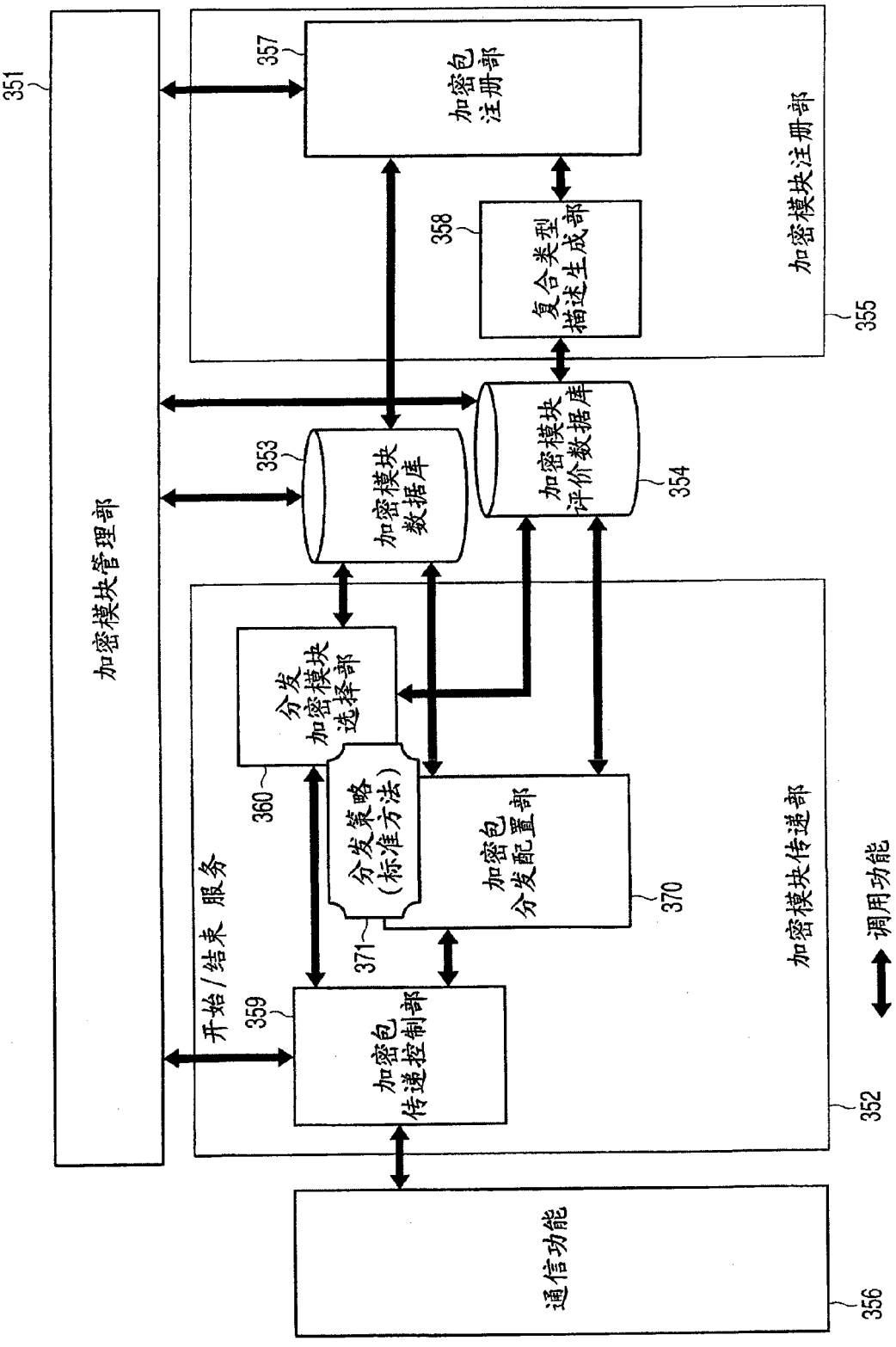

351
加密模块管理部
357
加密包注册部
358
复合类型描述生成部
加密模块注册部
355
353
加密模块数据库
354
加密模块评价数据库
分发加密模块选择部
360
分发策略（标准方法）
371
加密包分发配置部
370
开始/结束 服务
359
加密包传递控制部
加密模块传递部
352
调用功能
通信功能
356

图 3

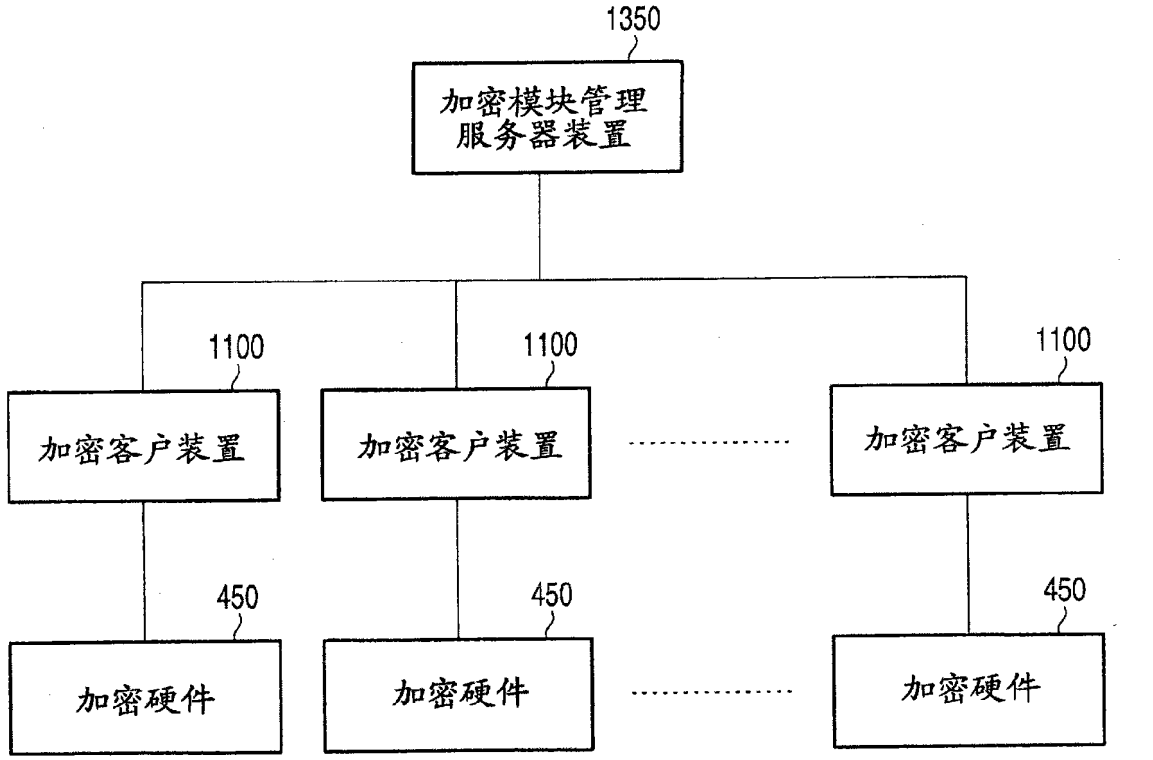

1350
加密模块管理
服务器装置
1100
1100
1100
加密客户装置
加密客户装置
加密客户装置
450
450
450
加密硬件
加密硬件
加密硬件

图 4

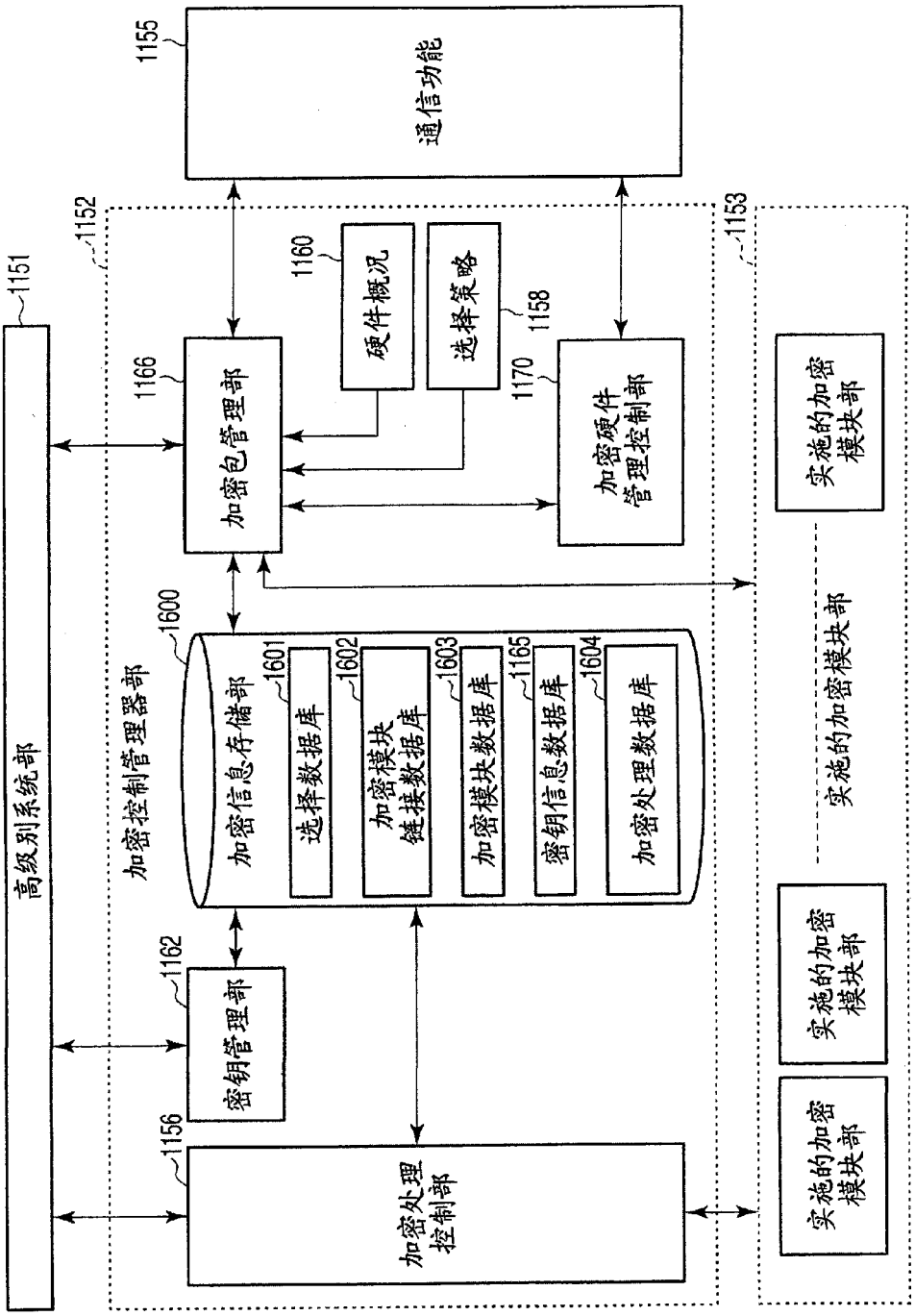

1155
通信功能
1152
1151
1160
硬件概况
选择策略
1158
1166
加密包管理部
1170
加密硬件
管理控制部
1153
实施的加密
模块部
1600
加密信息存储部
1601
选择数据库
1602
加密模块
链接数据库
1603
加密模块数据库
1165
密钥信息数据库
1604
加密处理数据库
加密控制管理器部
高级别系统部
1162
密钥管理部
1156
加密处理
控制部
实施的加密模块部
实施的加密模块部
实施的加密模块部

图 5

[密钥]策略(将包含类别信息的加密模块的条件信息转换为字符串)	
最高级别加密模块评价描述部标识符	与该策略关联的加密模块的最高级别加密模块评价描述部分标识符
算法标识符	与该策略关联的算法标识符
要被链接的加密模块的数目	与该策略关联的终端加密模块的数目
要被链接的加密模块标识符组	与该策略关联的(多个)终端加密模块标识符
密钥长度	在执行加密处理时使用的加密密钥的长度

图 6

[密钥]加密模块评价描述部标识符	
附带版本的加密模块评价描述部标识符	包含版本号的加密模块评价描述识别符
加密模块标识符	在终端加密模块评价描述部处于树结构中的情况下实施的加密模块部标识符，否则为空
类别标识符	该加密模块评价描述部的类别标识符
自己的加密模块评价描述部的参考数目	该加密模块评价描述部的参考源计数（存在选择数据库和该加密模块链接数据库两种参考源）
要被链接的加密模块评价描述部的数目	在树结构中级别低于该加密模块评价描述部的加密模块评价描述部的数目
要被链接的加密模块评价描述部标识符的数目	在树结构中级别低于该加密模块评价描述部的加密模块评价描述部标识符

图 7

[密钥]加密模块评价描述部标识符	
附带版本的加密模块评价描述部标识符	包含版本号的加密模块评价描述识别符
链接的加密模块评价描述部标识符	对应该加密模块的终端加密模块评价描述标识符
类别标识符	该加密模块的类别标识符
加密模块数据号	该加密模块的数据号
模块类型	该加密模块的类型
加密模块文件名	该加密模块的文件名
要被链接的选择策略数目	与该加密模块并联的选择数据库中的策略数目
要被链接的选择数据库中的策略组	与该加密模块并联的选择数据库中的策略

图 8

[密钥]密钥标识符	
存储位置信息	存储信息(无，在终端中，在加密硬件中)
密钥类型	加密方法类型信息(密钥数据，特定算法参数，特定系统参数，证书)
密钥文件名	密钥的文件名
密钥实体	密钥实体的数据
密钥数据加密信息	关于密钥数据加密信息的信息(无加密，加密硬件应用)
密钥，参数长度	密钥和参数的长度信息
类别标识符	对应于该密钥的类别标识符
算法标识符	对应于该密钥的算法标识符
调制机	关于该密钥的调制机的信息
有效期	关于该密钥有效期的信息
使用次数的限制	关于使用该密钥的次数限制的信息

图 9

[密钥]加密处理标识符	
处理类型	处理信息(包括密钥加入，密钥创建，加密处理)
算法标识符	该处理的算法标识符
加密模块评价描述标识符	作为加密处理或密钥创建处理使用的加密模块评价描述标识符
类别标识符	该处理的类别标识符
间接参考密钥标识符	要被间接参考的密钥数据库中的密钥标识符
参数数目	参数信息组的数目
参数信息组	除了参数体之外包含参数类型和大小的信息
密钥信息组	包含密钥参数类型，密钥标识符和密钥大小的信息

图 10

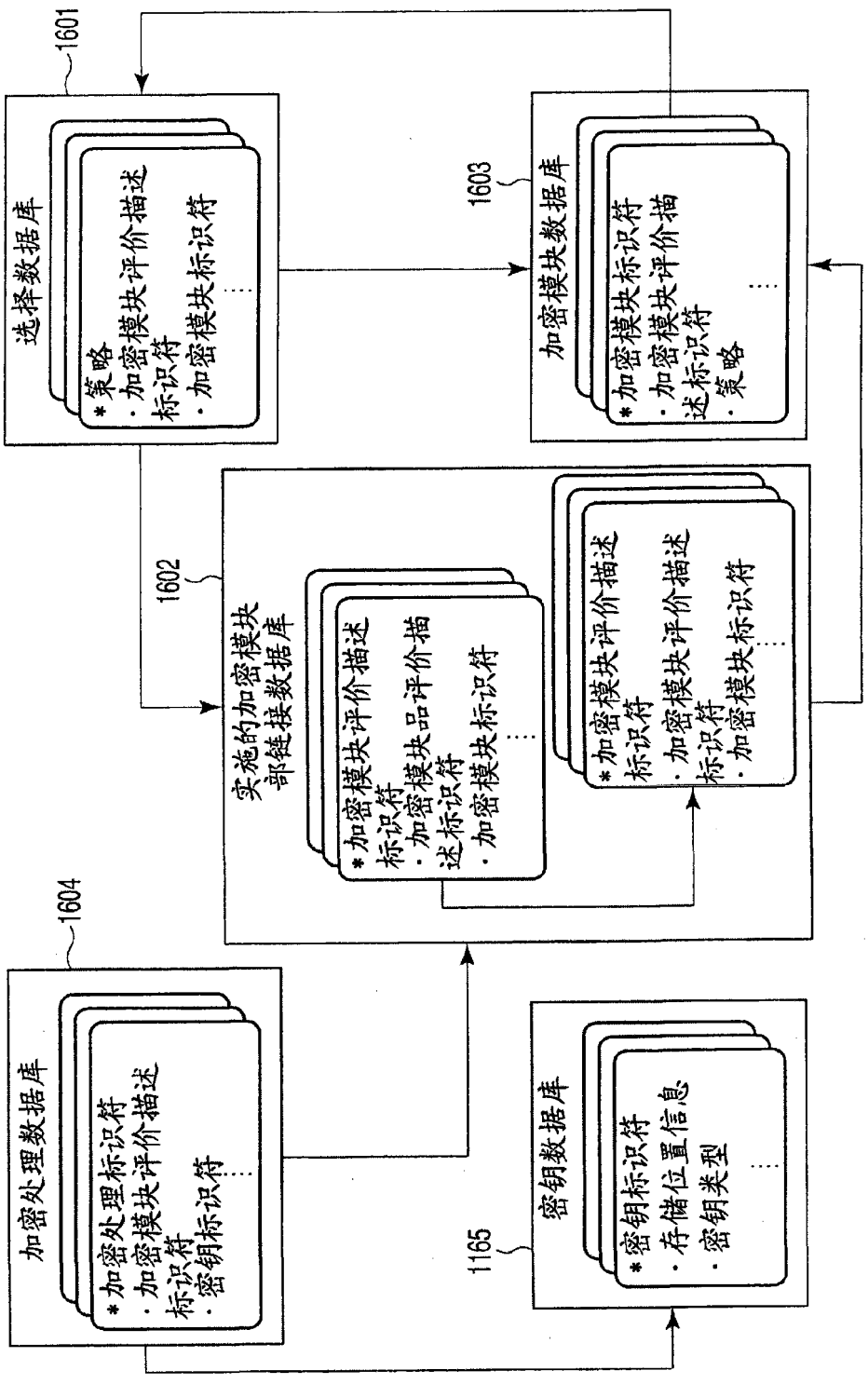

选择数据库
1601
*策略
·加密模块评价描述标识符
·加密模块标识符
加密模块数据库
1603
*加密模块标识符
·加密模块评价描述标识符
·策略
实施的加密模块部链接数据库
1602
*加密模块评价描述标识符
·加密模块品评价描述标识符
·加密模块标识符
*加密模块评价描述标识符
·加密模块评价描述标识符
·加密模块标识符
加密处理数据库
1604
*加密处理标识符
·加密模块评价描述标识符
·密钥标识符
密钥数据库
1165
*密钥标识符
·存储位置信息
·密钥类型

图 11

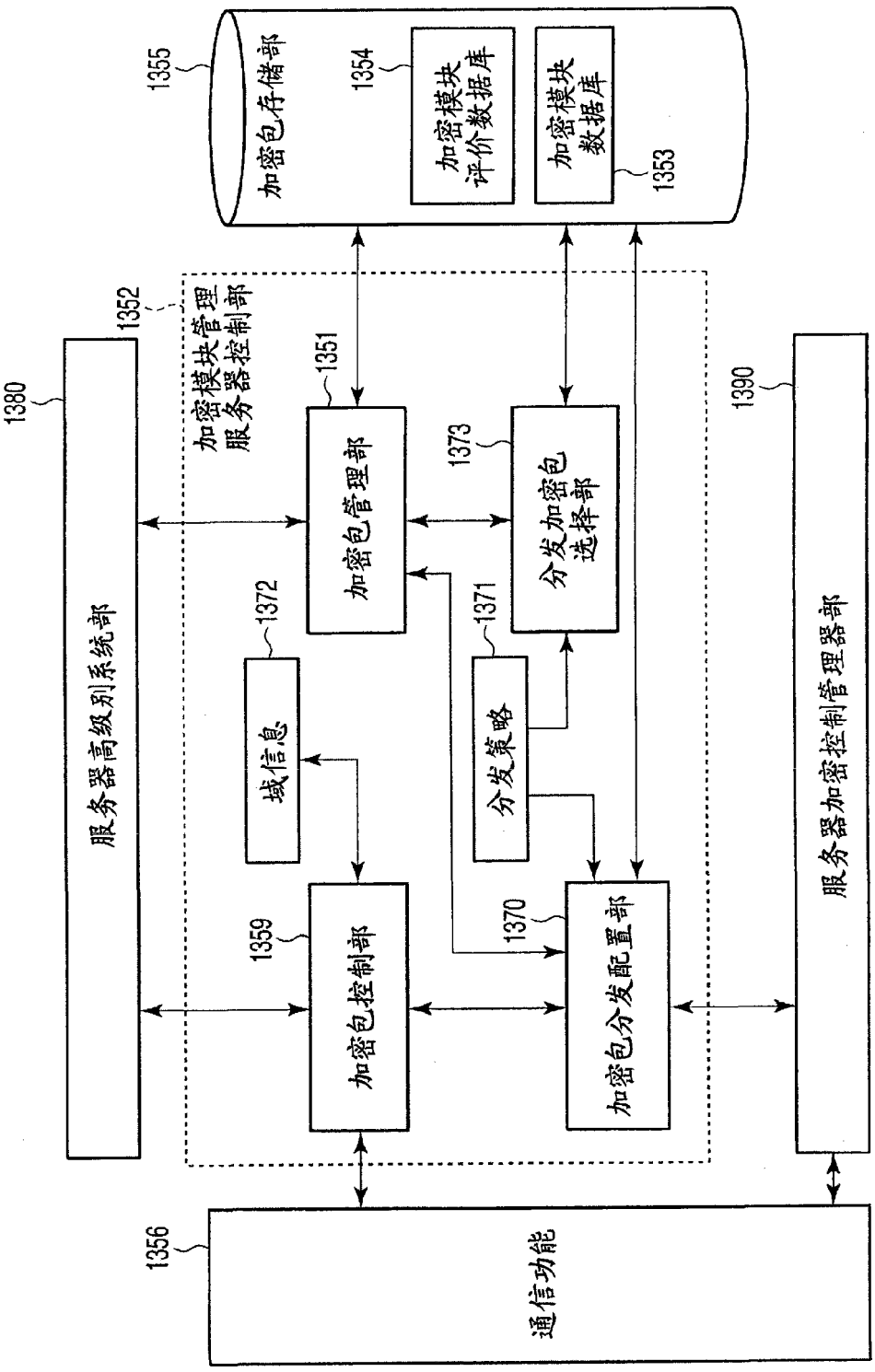

1355
加密包存储部
1354
加密模块评价数据库
加密模块数据库
1353
1352
加密模块管理服务器控制部
1380
服务器高级别系统部
1351
加密包管理部
1373
分发加密包选择部
1390
服务器加密控制管理器部
1372
域信息
1371
分发策略
1359
加密包控制部
1370
加密包分发配置部
1356
通信功能

图 12

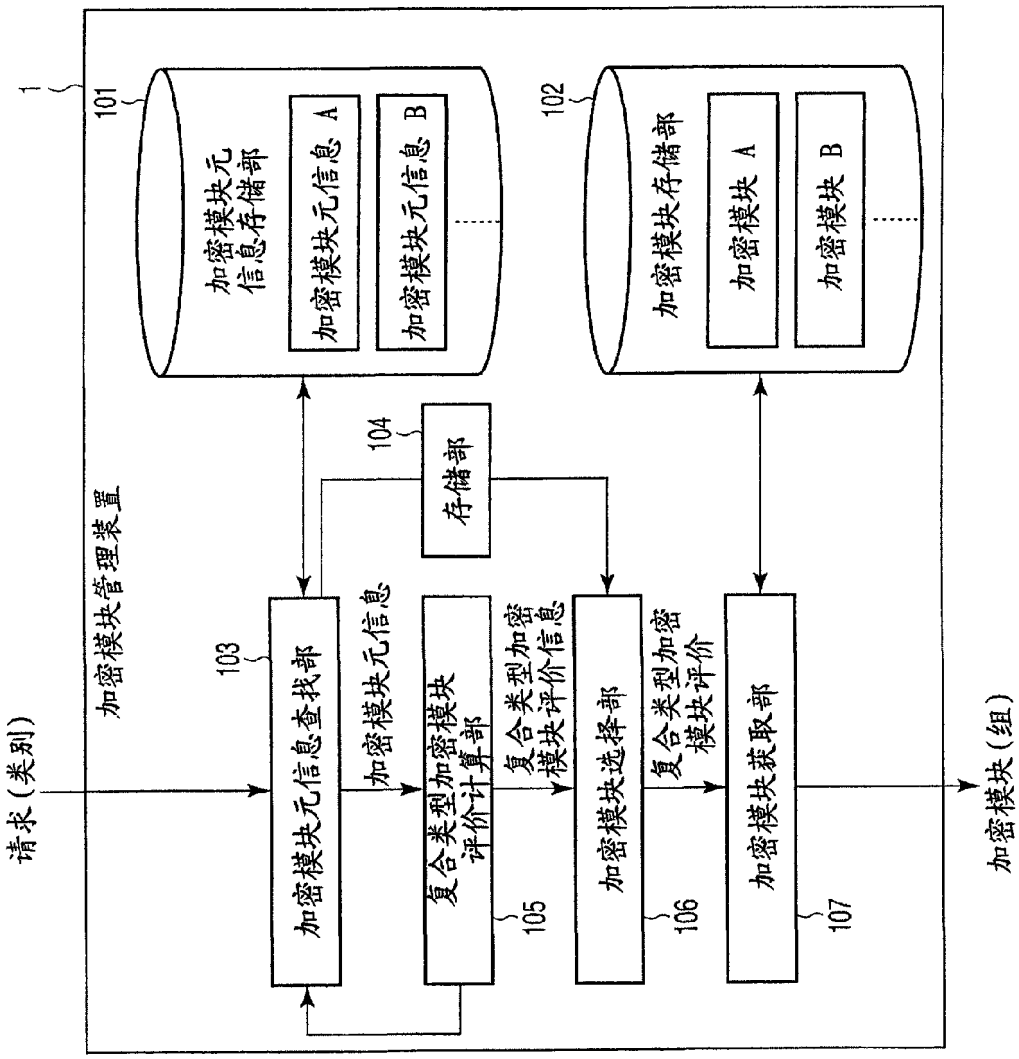

1
加密模块管理装置
101
加密模块元信息存储部
加密模块元信息 A
加密模块元信息 B
102
加密模块存储部
加密模块 A
加密模块 B
104
存储部
103
加密模块元信息查找部
加密模块元信息
复合类型加密模块评价计算部
105
复合类型加密模块评价信息
加密模块选择部
106
复合类型加密模块评价
加密模块获取部
107
请求（类别）
加密模块（组）

图 13

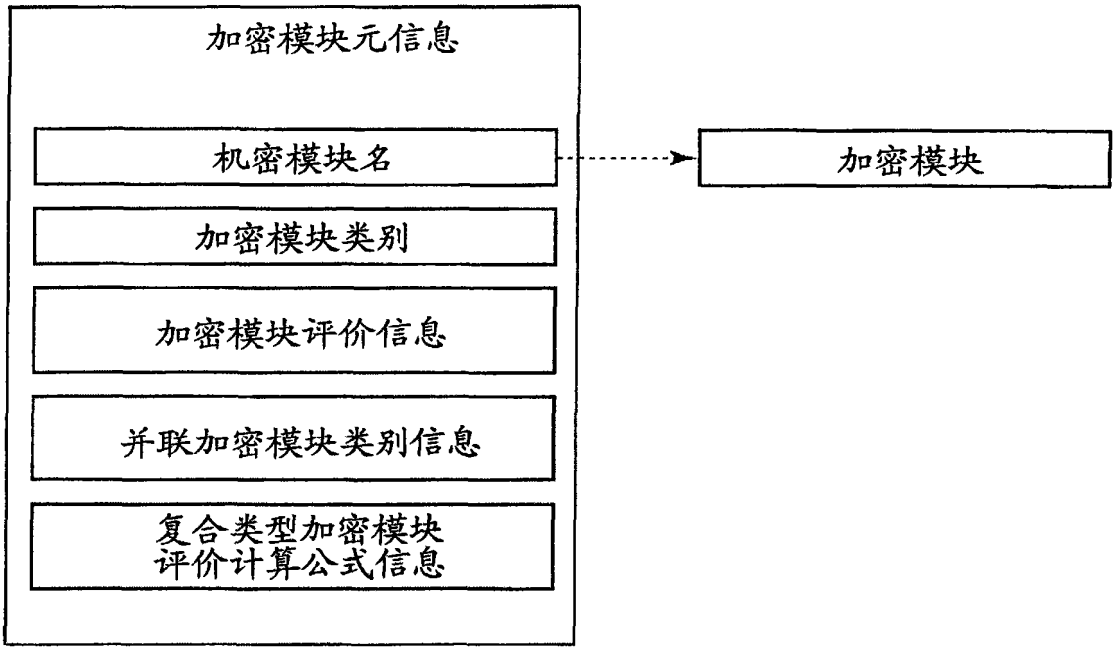


图 14

评价项目	评价分数 (单位：分)
安全	60
速度	20
使用的存储器量	30

图 15

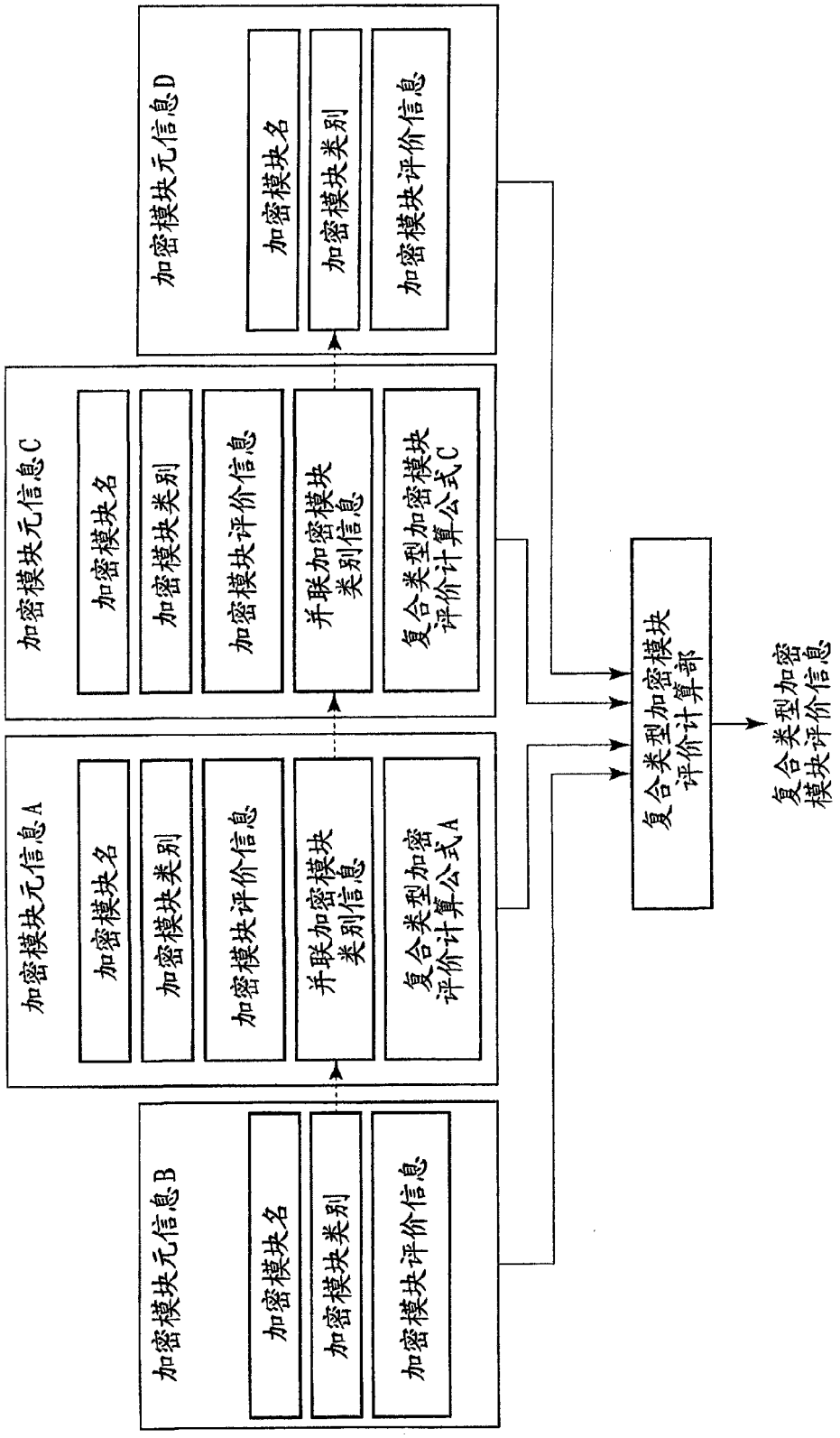

加密模块元信息A
加密模块名
加密模块类别
加密模块评价信息
并联加密模块类别信息
复合类型加密评价计算公式A
加密模块元信息B
加密模块名
加密模块类别
加密模块评价信息
加密模块元信息C
加密模块名
加密模块类别
加密模块评价信息
并联加密模块类别信息
复合类型加密模块评价计算公式C
加密模块元信息D
加密模块名
加密模块类别
加密模块评价信息
复合类型加密模块评价计算部
复合类型加密模块评价信息

图 16

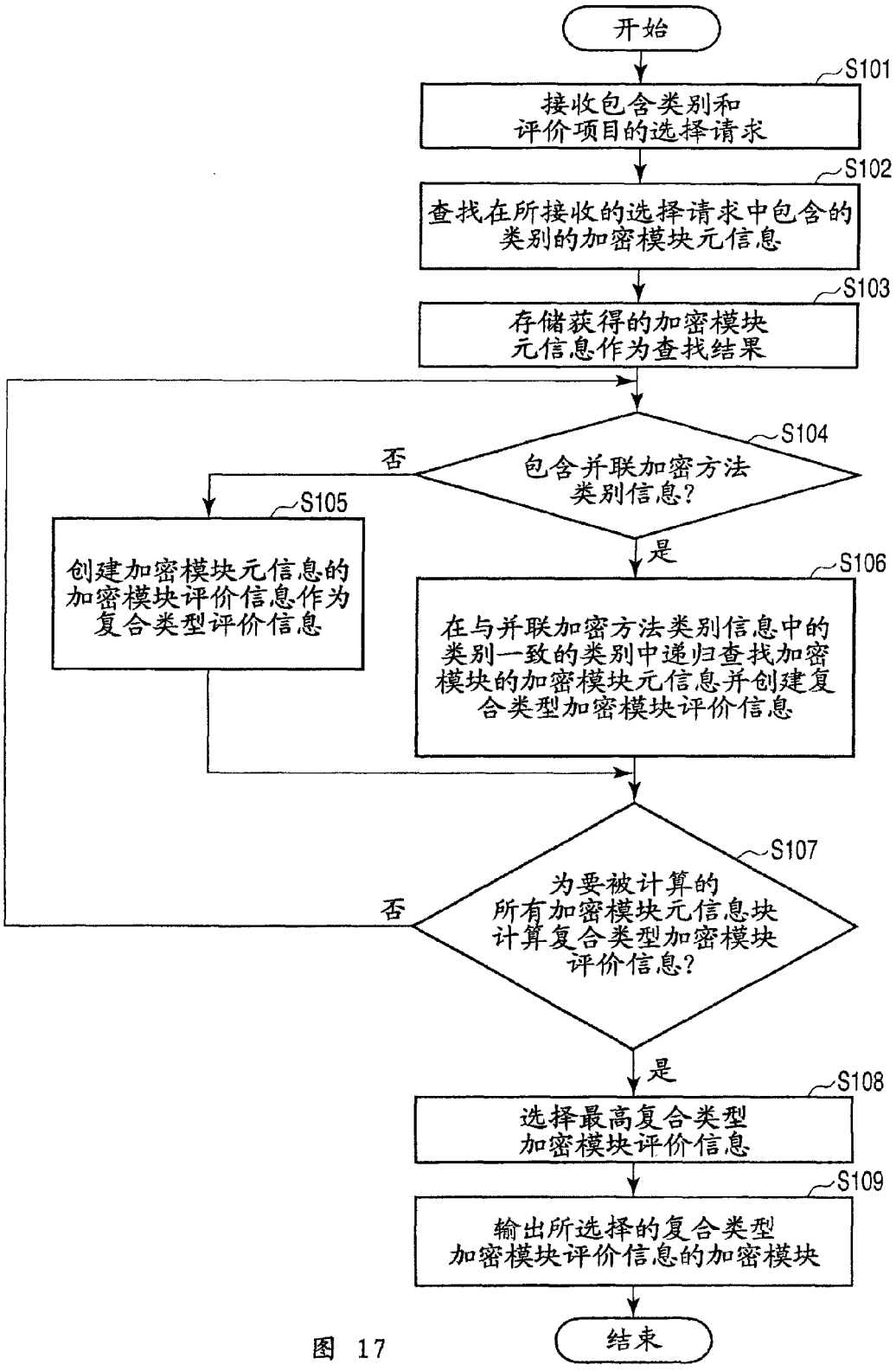

开始
S101
接收包含类别和评价项目的选择请求
S102
查找在所接收的选择请求中包含的类别的加密模块元信息
S103
存储获得的加密模块元信息作为查找结果
S104
包含并联加密方法类别信息?
否
是
S105
创建加密模块元信息的加密模块评价信息作为复合类型评价信息
S106
在与并联加密方法类别信息中的类别一致的类别中递归查找加密模块的加密模块元信息并创建复合类型加密模块评价信息
S107
为要被计算的所有加密模块元信息块计算复合类型加密模块评价信息?
否
是
S108
选择最高复合类型加密模块评价信息
S109
输出所选择的复合类型加密模块评价信息的加密模块
结束

图 17

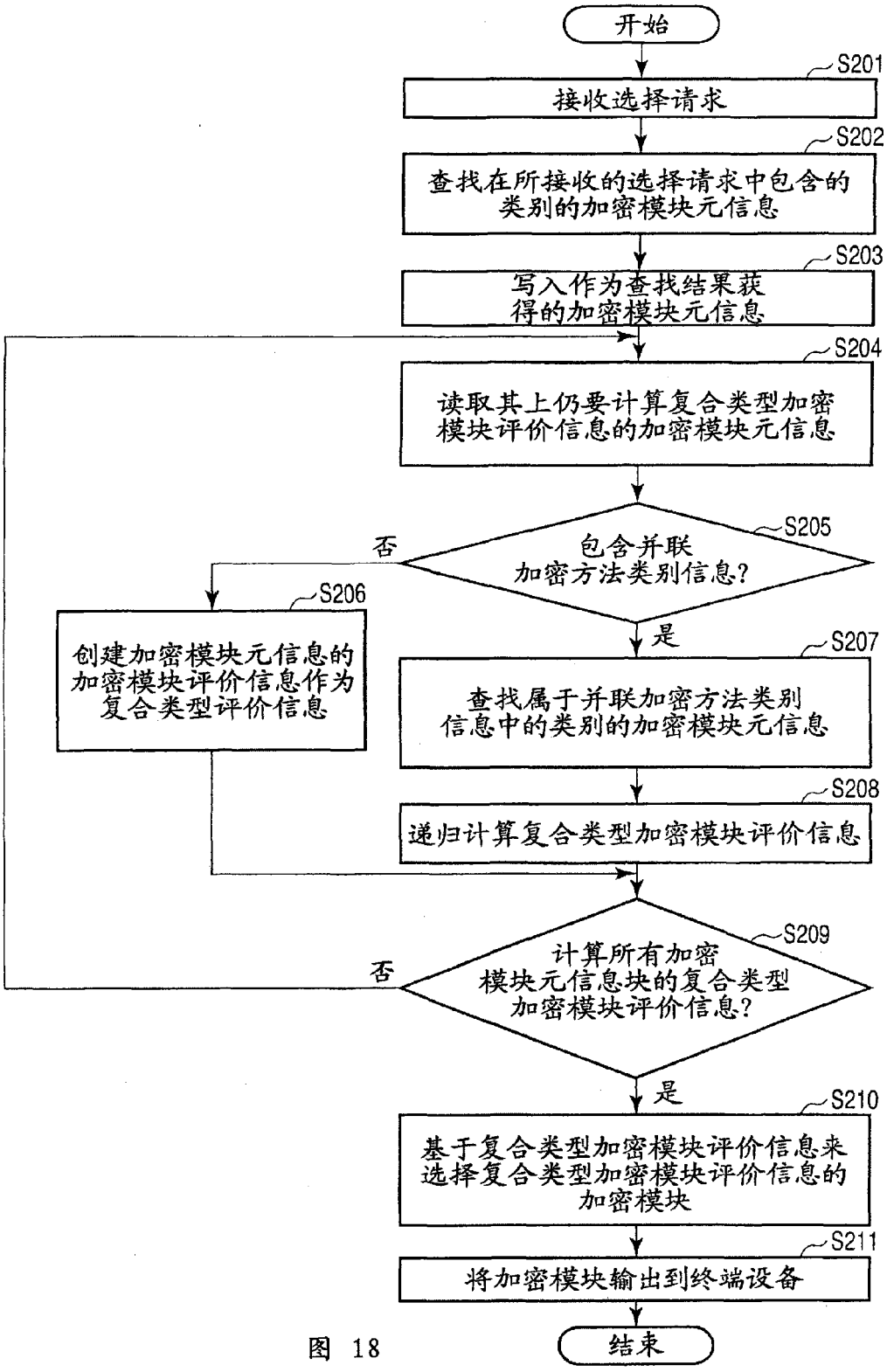

开始
S201
接收选择请求
S202
查找在所接收的选择请求中包含的类别的加密模块元信息
S203
写入作为查找结果获得的加密模块元信息
S204
读取其上仍要计算复合类型加密模块评价信息的加密模块元信息
S205
包含并联加密方法类别信息?
否
是
S206
创建加密模块元信息的加密模块评价信息作为复合类型评价信息
S207
查找属于并联加密方法类别信息中的类别的加密模块元信息
S208
递归计算复合类型加密模块评价信息
S209
计算所有加密模块元信息块的复合类型加密模块评价信息?
否
是
S210
基于复合类型加密模块评价信息来选择复合类型加密模块评价信息的加密模块
S211
将加密模块输出到终端设备
结束

图 18

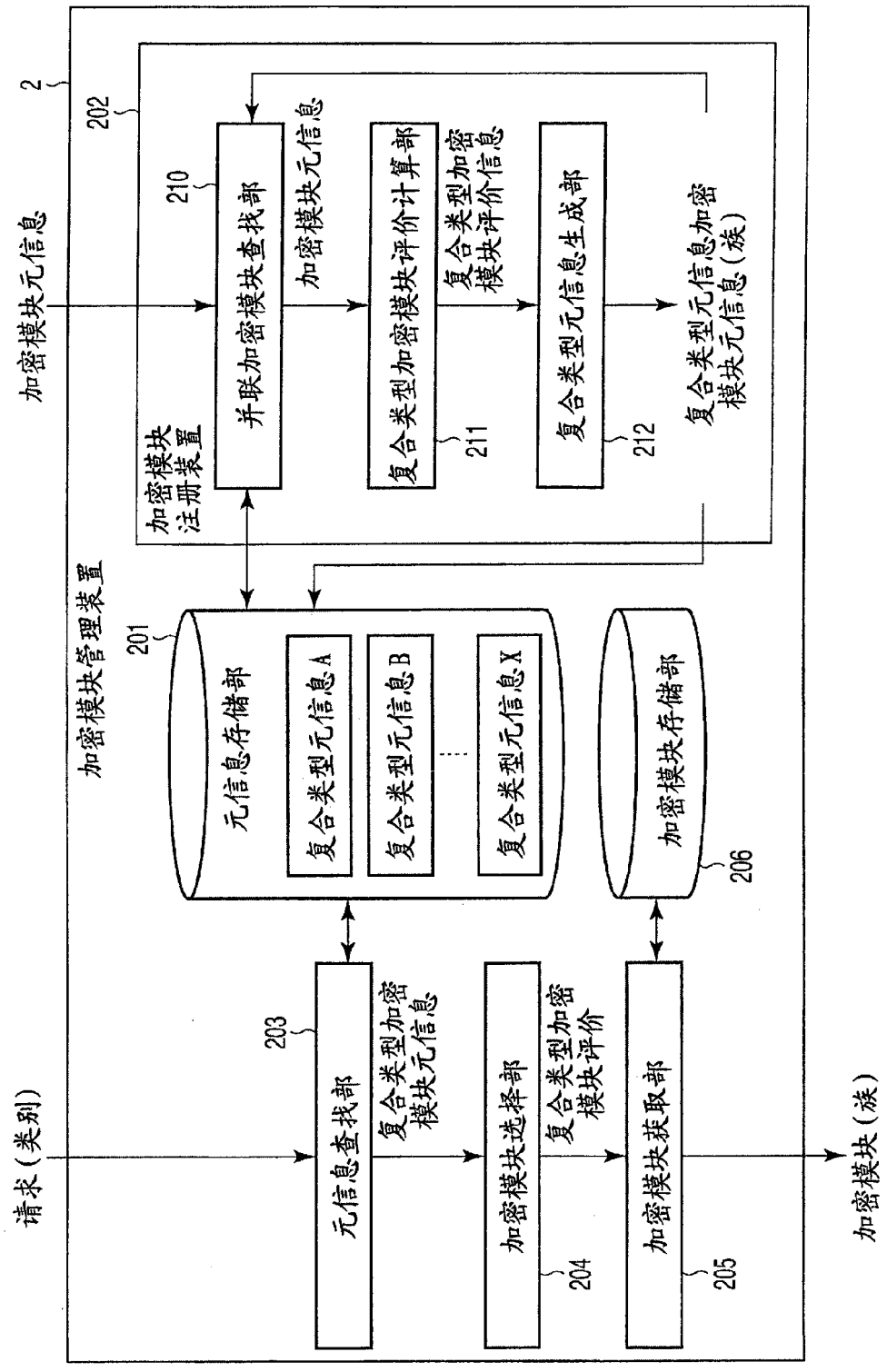

加密模块元信息
2
202
210
并联加密模块查找部
加密模块元信息
复合类型加密模块评价计算部
复合类型加密模块评价信息
复合类型元信息生成部
复合类型元信息加密模块元信息(族)
加密模块注册装置
211
212
加密模块管理装置
201
元信息存储部
复合类型元信息A
复合类型元信息B
复合类型元信息X
加密模块存储部
206
请求(类别)
203
元信息查找部
复合类型加密模块元信息
加密模块选择部
复合类型加密模块评价
204
加密模块获取部
205
加密模块(族)

图 19

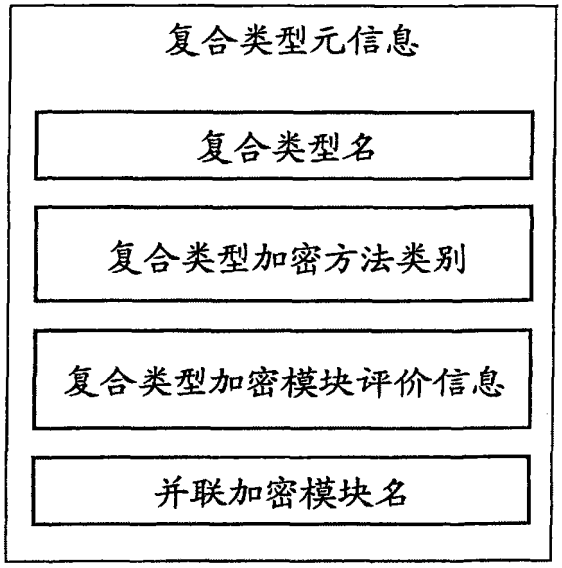

复合类型元信息
复合类型名
复合类型加密方法类别
复合类型加密模块评价信息
并联加密模块名

图 20

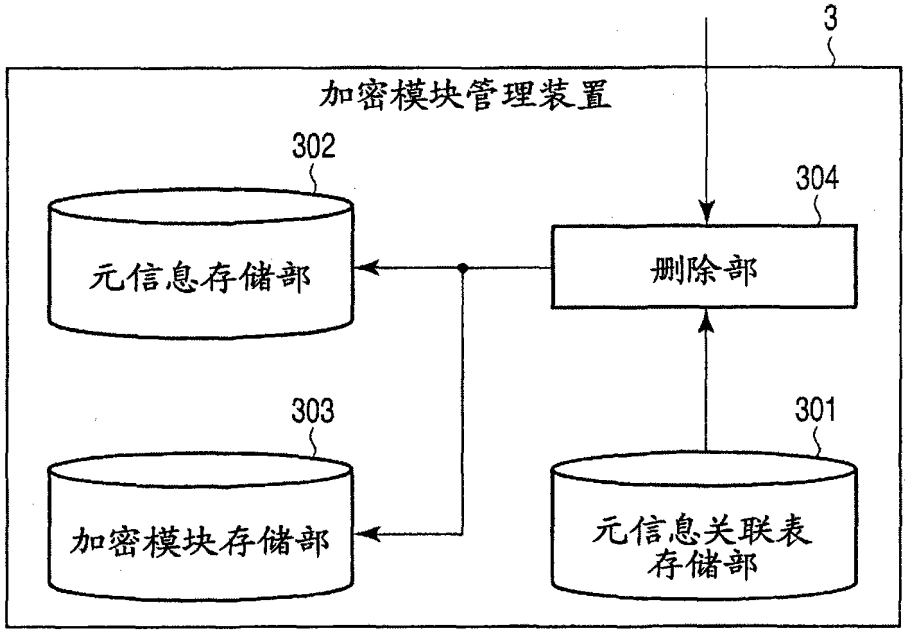

3
加密模块管理装置
302
304
元信息存储部
删除部
303
301
加密模块存储部
元信息关联表
存储部

图 22

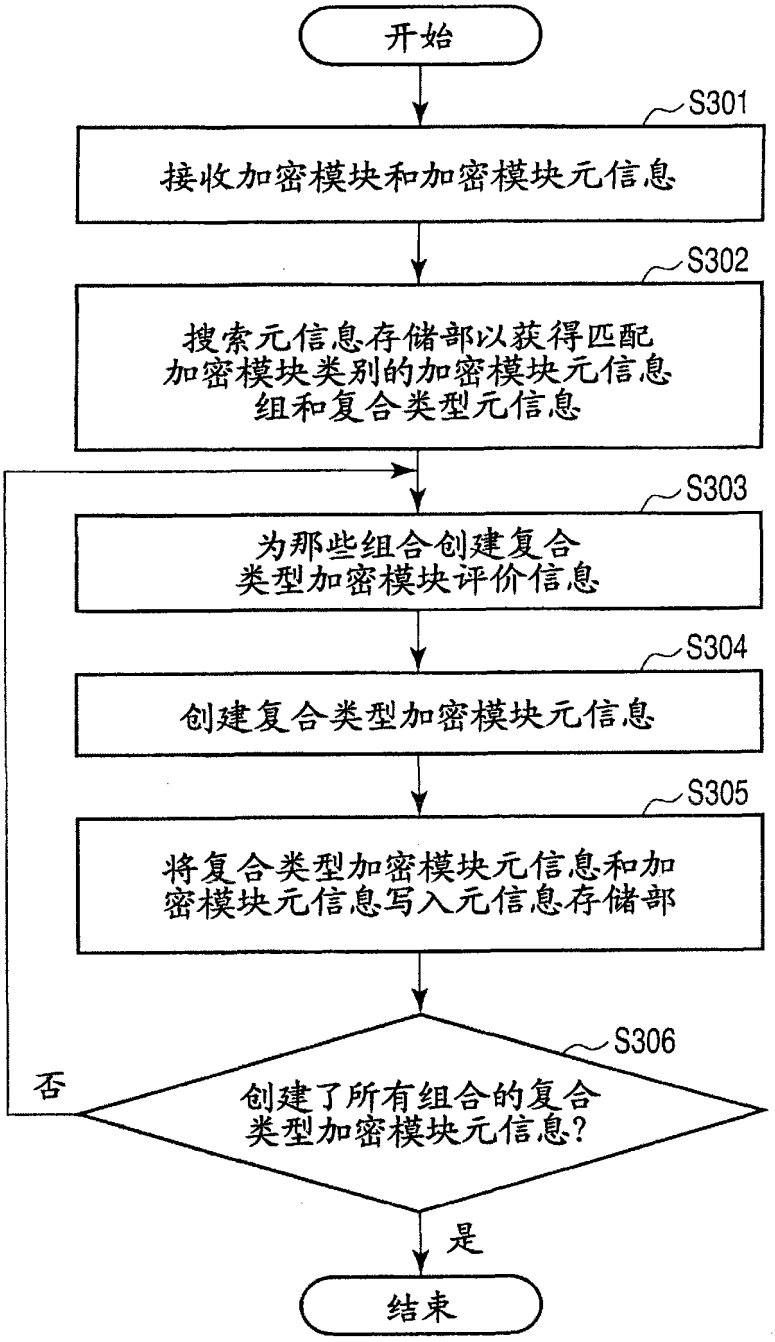

开始
S301
接收加密模块和加密模块元信息
S302
搜索元信息存储部以获得匹配加密模块类别的加密模块元信息组和复合类型元信息
S303
为那些组合创建复合类型加密模块评价信息
S304
创建复合类型加密模块元信息
S305
将复合类型加密模块元信息和加密模块元信息写入元信息存储部
S306
创建了所有组合的复合类型加密模块元信息?
否
是
结束

图 21

元信息关联表

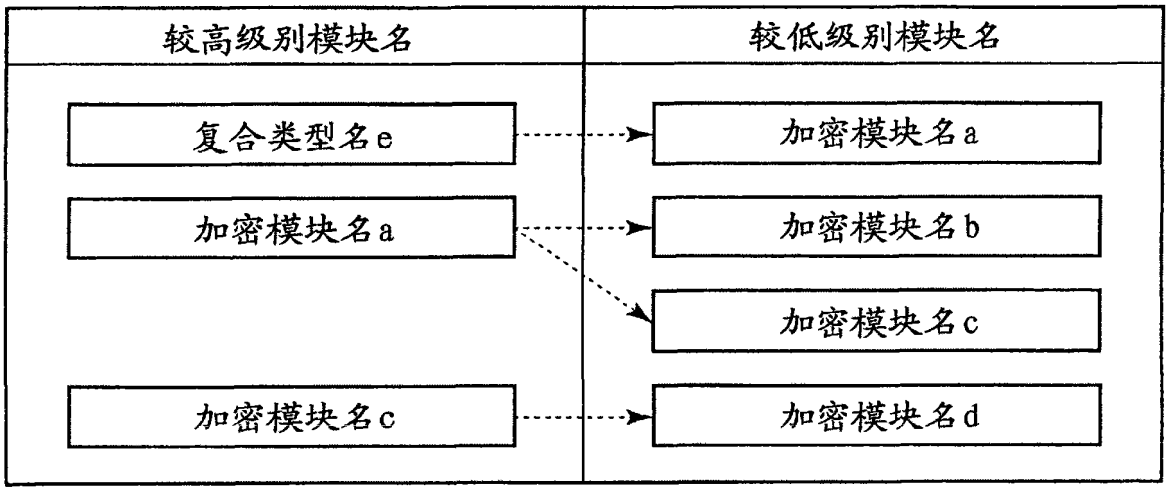

较高级别模块名
较低级别模块名
复合类型名e
加密模块名a
加密模块名a
加密模块名b
加密模块名c
加密模块名c
加密模块名d

图 23