

密码运算、创建工作密钥的方法、密码服务平台及设备

技术领域

[01]本说明书涉及密码技术领域，尤其涉及密码运算、创建工作密钥的方法、密码服务平台及设备。

5 背景技术

[02]随着互联网技术的发展，各类业务系统层出不穷，给人们的工作、生活带来了极大的便利，也促进了经济的增长和社会的进步。密码技术是保护银行、证券或交易等业务系统在数据存储、传输、访问控制中确保数据机密性、完整性、抗抵赖及可用性的重要手段。

- 10 [03]例如，企业可配置密码服务平台，密码服务平台是基于密码模块提供密钥管理、密码运算服务的系统平台，该平台作为业务系统的服务端，能够为业务系统提供消息验证、数据加密与解密、签名验签等应用层密码服务，保障数据在存储、传输及应用过程中的安全性，防止数据被窃取或恶意篡改。基于此，如何提供一个更为稳定的密码服务平台成为亟待解决的技术问题。

15 发明内容

[04]为克服相关技术中存在的问题，本说明书提供了密码运算、创建工作密钥的方法、密码服务平台及设备。

[05]根据本说明书实施例的第一方面，提供一种密码服务平台，所述密码服务平台连接有主密码模块，所述密码服务平台包括：

- 20 [06]注册模块，用于：调用所述主密码模块为新增的次密码模块生成主密钥；
- [07]工作密钥创建模块，用于：接收业务系统的工作密钥创建请求，调用所述主密码模块为所述业务系统生成工作密钥，获取所述主密码模块返回的：所述主密码模块的主密钥加密的工作密钥密文，以及各个已连接次密码模块的主密钥分别加密的工作密钥密文；
- [08]密码运算调用模块，用于：接收业务系统的密码运算请求，所述密码运算请求携带
- 25 有待运算数据；确定响应所述密码运算请求的目标密码模块；以所述目标密码模块对应

的工作密钥密文和所述待运算数据作为输入，调用所述目标密码模块，获得所述目标密码模块的运算结果，所述运算结果由所述目标密码模块利用已存储主密钥对所述工作密钥密文解密得到工作密钥后，利用解密得到的工作密钥对所述待运算数据进行加密得到。

[09]可选的，所述注册模块，还用于通过如下方式配置所述次密码模块的主密钥：

5 [10]获取所述次密码模块生成的目标公钥；

[11]以所述目标公钥作为输入，调用所述主密码模块，由所述主密码模块生成所述次密码模块的主密钥，利用所述目标公钥对所述生成的主密钥进行加密获得主密钥密文；

[12]将所述主密钥密文发送给所述次密码模块，由所述次密码模块利用与所述目标公钥对应的目标私钥解密获得主密钥。

10 [13]可选的，所述注册模块，还用于：

[14]获取所述主密码模块对所述目标公钥进行消息鉴别码计算获得的公钥校验值；

[15]以所述目标公钥和公钥校验值为输入，调用所述主密码模块，由所述主密码模块基于所述公钥校验值校验输入的目标公钥的合法性后，生成所述次密码模块的主密钥。

[16]可选的，所述注册模块，还用于通过如下方式配置所述次密码模块的主密钥：

15 [17]调用主密码模块，由主密码模块产生所述次密码模块的主密钥后，获取所述主密钥的两个或以上的密钥分量；

[18]将所述两个或以上的密钥分量分别输出给各个密钥管理实体，由所述密钥管理实体分别传输给所述次密码模块，以供次密码模块根据各个密钥分量生成主密钥。

[19]可选的，所述注册模块，还用于：

20 [20]接收所述主密码模块返回的所述次密码模块的主密钥密文后并存储，所述主密钥密文以主密码模块的主密钥加密。

[21]根据本说明书实施例的第二方面，提供一种密码运算方法，包括：

[22]接收业务系统发起的密码运算请求，所述密码运算请求携带有待运算数据；

[23]确定响应所述密码运算请求的目标密码模块，所述目标密码模块为主密码模块或至

25 少一个次密码模块中的一个，所述次密码模块的主密钥由所述主密码模块生成；

[24]获取与所述目标密码模块的工作密钥密文，所述工作密钥密文为：所述主密码模块利用所述目标密码模块的主密钥对工作密钥加密得到的密文，所述工作密钥由所述主密

码模块为所述业务系统创建;

- [25]以所述工作密钥密文和所述待运算数据为输入,调用所述目标密码模块,获取所述目标密码模块返回的运算结果并发送给所述业务系统,所述运算结果由所述目标密码模块利用已存储主密钥对所述工作密钥密文解密得到工作密钥后,利用解密得到的工作密钥对所述待运算数据进行加密得到。

[26]可选的,所述次密码模块的主密钥通过如下方式获得:

[27]获取所述次密码模块生成的目标公钥;

[28]以所述目标公钥作为输入,调用所述主密码模块,由所述主密码模块生成所述次密码模块的主密钥,利用所述目标公钥对所述生成的主密钥进行加密获得主密钥密文;

- 10 [29]将所述主密钥密文发送给所述次密码模块,由所述次密码模块利用与所述目标公钥对应的目标私钥解密获得主密钥。

[30]可选的,所述以所述目标公钥作为输入,调用所述主密码模块,由所述主密码模块生成所述次密码模块的主密钥,包括:

[31]获取所述主密码模块对所述目标公钥进行消息鉴别码计算获得的公钥校验值;

- 15 [32]以所述目标公钥和公钥校验值为输入,调用所述主密码模块,由所述主密码模块基于所述公钥校验值校验输入的目标公钥的合法性后,生成所述次密码模块的主密钥。

[33]可选的,所述次密码模块的主密钥通过如下方式获得:

[34]调用主密码模块,由主密码模块产生所述次密码模块的主密钥后,获取所述主密钥的两个或以上的密钥分量;

- 20 [35]将所述两个或以上的密钥分量分别输出给各个密钥管理实体,由所述密钥管理实体分别传输给所述次密码模块,以供次密码模块根据各个密钥分量生成主密钥。

[36]可选的,所述方法还包括:

[37]接收所述主密码模块返回的所述次密码模块的主密钥密文后并存储,所述主密钥密文以主密码模块的主密钥加密。

- 25 [38]根据本说明书实施例的第三方面,提供一种密码服务设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其中,所述处理器执行所述程序时实现如下方法:

- [39]接收业务系统发起的密码运算请求，所述密码运算请求携带有待运算数据；
- [40]确定响应所述密码运算请求的目标密码模块，所述目标密码模块为主密码模块或少一个次密码模块中的一个，所述次密码模块的主密钥由所述主密码模块生成；
- [41]获取与所述目标密码模块的工作密钥密文，所述工作密钥密文为：所述主密码模块
- 5 利用所述目标密码模块的主密钥对工作密钥加密得到的密文，所述工作密钥由所述主密码模块为所述业务系统创建；
- [42]以所述工作密钥密文和所述待运算数据为输入，调用所述目标密码模块，获取所述目标密码模块返回的运算结果并发送给所述业务系统，所述运算结果由所述目标密码模块利用已存储主密钥对所述工作密钥密文解密得到工作密钥后，利用解密得到的工作密钥对所述待运算数据进行加密得到。
- 10 [43]根据本说明书实施例的第四方面，提供一种创建工作密钥的方法，包括：
- [44]接收业务系统的工作密钥创建请求；
- [45]调用主密码模块为所述业务系统生成工作密钥，获取所述主密码模块返回的：所述主密码模块的主密钥加密的工作密钥密文，以及各个已连接次密码模块的主密钥分别加密的工作密钥密文；其中，所述次密码模块的主密钥通过调用所述主密码模块，由所述主密码模块为所述次密码模块生成。
- 15 [46]根据本说明书实施例的第五方面，提供一种密码服务设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现如下方法：
- 20 [47]接收业务系统的工作密钥创建请求；
- [48]调用主密码模块为所述业务系统生成工作密钥，获取所述主密码模块返回的：所述主密码模块的主密钥加密的工作密钥密文，以及各个已连接次密码模块的主密钥分别加密的工作密钥密文；其中，所述次密码模块的主密钥通过调用所述主密码模块，由所述主密码模块为所述次密码模块生成。
- 25 [49]本说明书的实施例提供的技术方案可以包括以下有益效果：
- [50]本说明书实施例中，密码服务平台所连接的密码模块中，其中一个作为主密码模块，密码服务平台的密钥管理功能中由主密码模块提供，主密码模块用于生成密钥，主密码模块和其他次密码模块提供密码服务平台所需要的密码运算功能。

[51]其中，次密码模块的主密钥由主密码模块生成，业务系统的工作密钥也由主密码模块生成，并且密码服务平台保存有主密码模块的主密钥加密的工作密钥密文，以及各个次密码模块的主密钥分别加密的工作密钥密文，因此，本实施例中主密钥由主密码模块保存，主密钥作为敏感安全参数明文不会超出密码模块的边界，不会损失密钥的安全性，

5 因此满足密钥的安全性要求。而密码服务平台可调用任一密码模块响应业务系统的密码运算请求，因此密码服务平台能够兼容多种密码模块，密码服务平台不会被单一的密码模块厂商绑定，满足使用多种密码模块的需求，也使得密码服务平台能够提供更为稳定的密码服务。

[52]应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能

10 限制本说明书。

附图说明

[53]此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本说明书的实施例，并与说明书一起用于解释本说明书的原理。

[54]图 1 是本说明书根据一示例性实施例示出的一种密码服务平台的应用场景图。

15 [55]图 2A 是本说明书根据一示例性实施例示出的密码服务平台的框图。

[56]图 2B 是本说明书根据一示例性实施例示出的次密码模块的注册过程示意图。

[57]图 2C 是本说明书根据一示例性实施例示出的创建工作密钥的过程示意图。

[58]图 2D 是本说明书根据一示例性实施例示出的密码运算示意图。

[59]图 3 是本说明书实施例密码服务平台所在计算机设备的一种硬件结构图。

20 [60]图 4 是本说明书根据一示例性实施例示出的一种密码运算方法的流程图。

[61]图 5 是本说明书根据一示例性实施例示出的一种创建工作密钥的方法的流程图。

具体实施方式

[62]这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施

25 例中所描述的实施方式并不代表与本说明书相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书的一些方面相一致的装置和方法的例子。

[63]在本说明书使用的术语是仅仅出于描述特定实施例的目的,而非旨在限制本说明书。在本说明书和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式,除非上下文清楚地表示其他含义。还应当理解,本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

5 [64]应当理解,尽管在本说明书可能采用术语第一、第二、第三等来描述各种信息,但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如,在不脱离本说明书范围的情况下,第一信息也可以被称为第二信息,类似地,第二信息也可以被称为第一信息。取决于语境,如在此所使用的词语“如果”可以被解释成为“在...时”或“当...时”或“响应于确定”。

10 [65]如图1所示,是本说明书根据一示例性实施例示出的一种密码服务平台的应用场景图,图1中密码服务平台与应用系统主机通信,应用系统主机通过调用密码服务平台提供的接口来使用密码服务,底层的密码运算等服务由密码服务平台调用密码模块来完成。

[66]密码模块(security module)含有密码算法和安全功能,是实现密钥管理机制的相对独立的软件、硬件、固件或其组合,被包含在密码边界内。密码边界(cryptographic boundary)是指:明确定义的连续边线,该边线建立了密码模块的物理和/或逻辑边界,并包括了密码模块的所有硬件、软件、和/或固件部件。

15

[67]目前,各家厂商都推出有密码模块,其主密钥的生成算法各不相同,为避免被单一厂商绑定、提高密码服务平台的健壮性,本说明书实施例的密码服务平台基于多种密码模块来建设,因此密码服务平台连接有多种密码模块,在接入有多种密码模块的情况下,需要考虑如何兼容各种密码模块以统一为业务系统提供密码服务,并且还要满足密码服务的安全性。

20

[68]本说明书实施例的方案是,密码服务平台所连接的密码模块中,其中一个作为主密码模块,密码服务平台的密钥管理功能中由该主密码模块生成密钥,除了主密码模块之外的其他密码模块,本说明书实施例称为次密码模块,次密码模块和主密码模块都可提供密码服务平台所需要的密码运算功能。

25

[69]其中,次密码模块的主密钥由主密码模块生成,业务系统的工作密钥也由主密码模块生成,并且密码服务平台保存有主密码模块的主密钥加密的工作密钥密文,以及各个次密码模块的主密钥分别加密的工作密钥密文,因此,本实施例中主密钥由主密码模块保存,作为敏感安全参数的主密钥、工作密钥明文均不会超出密码模块的边界,因此不

会损失密钥的安全性，满足密钥的安全性要求。而密码服务平台可调用任一密码模块响应业务系统的密码运算请求，因此密码服务平台不会被单一的密码模块厂商绑定，满足使用多种密码模块的需求，也使得密码服务平台能够提供更为稳定的密码服务。

[70]作为例子，如图 2A 所示，本说明书实施例的密码服务平台可包含有注册模块 21、
5 工作密钥创建模块 22 和密码运算调用模块 23，分别用于注册次密码模块、创建业务系统的工作密钥，以及调用密码模块响应业务系统的密码运算请求。

[71]其中，注册模块 21，用于：调用所述主密码模块为新增的次密码模块生成主密钥；

[72]工作密钥创建模块 22，用于：接收业务系统的工作密钥创建请求，调用所述主密码模块为所述业务系统生成工作密钥，获取所述主密码模块返回的：所述主密码模块的主
10 密钥加密的工作密钥密文，以及各个已连接次密码模块的主密钥分别加密的工作密钥密文；

[73]密码运算调用模块 23，用于：接收业务系统的密码运算请求，所述密码运算请求携带有待运算数据；确定响应所述密码运算请求的目标密码模块；以所述目标密码模块对应的工作密钥密文和所述待运算数据作为输入，调用所述目标密码模块，获得所述目标
15 密码模块的运算结果，所述运算结果由所述目标密码模块利用已存储主密钥对所述工作密钥密文解密得到工作密钥后，利用解密得到的工作密钥对所述待运算数据进行加密得到。

[74]接下来进行详细说明。

[75]（一）次密码模块的注册

[76]密码模块在工作前需要设置工作用的主密钥，密码模块利用主密钥对待保护密钥进行加密。密码模块本身会有密钥派生算法生成密钥，而本实施例中，由主密码模块为次密码模块生成主密钥。具体的，可以是密码服务平台调用主密码模块的生成密钥接口，主密码模块在被调用后，利用密钥派生算法生成次密码模块的主密钥。本实施例采用主密码模块为次密码模块生成主密钥的方式，可以令主密码模块获得各个次密码模块的主
20 密钥，以在创建业务系统的工作密钥时，可利用次密码模块的主密钥对工作密钥加密（此过程在后续进行详细说明）。

[77]其中，主密码模块为次密码模块的主密钥后，可通过加密方式等传输给次密码模块，具体的加密传输方式可根据实际需要灵活配置，以保证传输过程的安全性。作为例子，主密码模块在生成主密钥后，基于主密钥生成两个或两个以上的密钥分量，将所述各个

密钥分量分别输出给各个密钥管理实体，由所述密钥管理实体分别传输给所述次密码模块，以供次密码模块根据各个密钥管理实体输入的密钥分量生成主密钥。其中，所述密钥管理实体可以是密钥管理员，每个密钥管理员分别获得其中一个密钥分量，各密钥管理员可通过次密码模块的控制输入接口输入其持有的密钥分量的方式，次密码模块在获取到所有密钥分量后可生成用于工作的主密钥。本实施例通过生成密钥分量、并通过多个密钥管理实体传输给次密码模块，由于各个密钥管理实体只拥有密钥分量，即使有密钥分量泄露，由于获取所有密钥分量的难度较大，因此可降低密钥泄露和攻击的风险，提升主密钥传输的安全性。

[78]在另一些例子中，可利用非对称密码技术对主密钥进行加密传输。作为例子，次密码模块可生成包括目标公钥和目标私钥的非对称密钥，密码服务平台可获取到次密码模块的目标公钥。密码服务平台可调用主密码模块，并且向主密码模块传输该目标公钥，由所述主密码模块生成所述次密码模块的主密钥后，利用该目标公钥对所述生成的主密钥进行加密获得主密钥密文；主密码模块向密码模块服务平台返回该主密钥密文，密码服务平台接收后发送给所述次密码模块，由所述次密码模块利用目标私钥解密获得主密钥。

[79]上述过程涉及目标公钥的传输，可选的，本实施例可进一步通过如下实施例降低目标公钥在传输过程中被篡改等风险，从而保证次密码模块的主密钥的安全传输。作为例子，可以是：密码服务平台调用主密码模块，并且向主密码模块传输该目标公钥，由主密码模块对所述目标公钥进行认证，认证的过程是：主密码模块利用自身的主密钥对该目标公钥进行消息鉴别码计算，获得消息鉴别码值（也即是目标公钥的校验值）。主密码模块将计算得到的消息鉴别码值返回给密码服务平台，密码服务平台调用主密码模块，并且向主密码模块传输该目标公钥和消息鉴别码值。主密码模块基于消息鉴别码值校验目标公钥，确定目标公钥合法（表示目标公钥安全，未被篡改等）后为次密码模块生成次密码模块的主密钥，利用该目标公钥对所述生成的主密钥进行加密获得主密钥密文返回给密码服务平台。

[80]接下来结合图 2B 再次说明上述注册过程，如图 2B 所示，是本说明书根据一示例性实施例示出的次密码模块的注册过程：

[81]1、密码服务平台管理员向密码服务平台发出注册一个次密码模块的操作指令，密码服务平台收到指令后，执行如下操作：

[82]1.1、密码服务平台调用主密码模块的认证公钥服务接口，由主密码模块对次密码模

块的目标公钥进行认证（次密码模块预先生成了包括目标公钥和目标私钥的非对称密钥对，并提供给密码服务平台）。

[83]1.2、主密码模块利用其主密钥对该目标公钥进行消息鉴别码计算，获得公钥校验值并返回给密码服务平台。

5 [84]1.3、密码服务平台调用主密码模块的生成对称密钥指令，并且传输次密码模块的目标公钥和公钥校验值。

[85]1.4、主密码模块基于公钥校验值校验目标公钥的合法性，在通过校验后，生成对称密钥，利用该目标公钥对对称密钥进行加密后返回。

10 [86]1.5、密码服务平台调用次密码模块的设置主密钥控制输入接口，并且传输上一步的以目标公钥加密的对称密钥。

[87]1.6、次密码模块接收上述设置主密钥指令，用目标私钥解密得到对称密钥，设置为工作主密钥。

15 [88]可选的，可以由主密码模块保存各个次密码模块的主密钥，也可以是主密码模块利用自身主密钥对次密码模块的主密钥进行加密，获得次密码模块的主密钥密文后传输给密码服务平台进行保存。

[89]（二）为业务系统创建工作密钥

[90]本实施例中，工作密钥是指密码模块为业务系统提供密码运算功能、针对业务系统创建的密钥。创建工作密钥的过程可以是：

20 [91]接收业务系统的工作密钥创建请求，调用所述主密码模块为所述业务系统生成工作密钥，获取所述主密码模块反馈的：所述主密码模块的主密钥加密的工作密钥密文，以及各个已连接次密码模块的主密钥分别加密的工作密钥密文。

[92]本实施例中，业务系统的工作密钥由主密码模块生成后，由主密码模块生成多份工作密钥密文并提供给密码服务平台保存，以供后续的密码运算处理过程中使用。

25 [93]作为例子，如图 2C 所示，是本说明书根据一示例性实施例示出的创建工作密钥的过程：

[94]1、密钥管理员发起创建密钥的操作指令，密码服务平台收到操作指令后，执行如下操作：

[95]1.1、密码服务平台调用主密码模块的创建工作密钥接口，同时传入各个次密码模块

的主密钥密文（该密文由主密码模块的主密钥加密）。

[96] 1.2、主密码模块被调用后，利用密钥派生模块产生工作密钥，并分别使用主密码模块的主密钥加密、各个次密码模块的主密钥分别加密后返回。（其中，工作密钥可能包括多个，私钥和秘密密钥可进行加密，而公钥可以不加密直接明文返回，当然，也可以根据需要对公钥加密，实际应用中可以灵活配置）

[97] 执行完成后，密码服务平台记录下多份工作密钥密文：由主密码模块主密钥加密的密文，以及由各个次密码模块的主密钥加密的密文内容。

[98] （三）密码运算

[99] 本实施例中，密码服务平台向业务系统提供密码运算服务，密码服务平台可接收业务系统的密码运算请求，所述密码运算请求携带有待运算数据。通常，密码服务平台可能面向多个业务系统提供服务，每个业务系统也可能对应多个工作密钥，因此密码运算请求中还携带有密钥标识，以供密码服务平台确定该利用哪个工作密钥提供密码运算服务。

[100] 由于接入有多个密码模块，密码服务平台可以从中选取其中一个密码模块响应密码运算请求，为了便于区分，本实施例称为目标密码模块。可选的，密码服务平台的选取方式可以根据需要灵活配置，例如可以基于各个密码模块当前的处理能力、正在处理的任务数量等等方式。

[101] 在确定响应密码运算请求的目标密码模块后，密码服务平台可以从已存储多份工作密钥密文中，获取目标密码模块对应的工作密钥密文。密码服务平台可以以该工作密钥密文作为输入，调用所述目标密码模块。目标密码模块在被调用后，可以利用自身已存储主密钥对所述工作密钥密文解密得到工作密钥，进而利用该工作密钥对所述待运算数据进行运算，运算结果可返回给密码服务平台，由密码服务平台返回给业务系统。

[102] 作为例子，如图 2D 所示，是本说明书根据一示例性实施例示出的密码运算示意图：

[103] 1.1、密码服务平台接收到密码运算请求后，确定选择本次运算该使用哪一个密码模块，具体的选择逻辑不限，可以根据密码服务平台对密码模块进行流量管理的需求来制定该逻辑。

[104] 1.1.1、如果选择结果为主密码模块，密码服务平台调用主密码模块的密码运算接口，输入数据为工作密码的密钥内容（由主密码模块加密）和待运算数据。

- [105] 1.1.2、主密码模块使用内部的主密钥解密得到工作密钥明文，对待运算数据进行密码运算，将运算结果返回给密码服务平台。
- [106] 2.2.1、如果选择结果为次密码模块，密码服务平台调用次密码模块的密码运算接口，输入数据为工作密码的密钥内容（由次密码模块加密）和待运算数据。
- 5 [107] 2.2.2、次密码模块使用内部的主密钥解密得到工作密钥明文，对待运算数据进行密码运算，将运算结果返回给密码服务平台。
- [108] 与前述密码服务平台的实施例相对应，本说明书还提供了密码运算方法及密码服务平台所应用的计算机设备的实施例。
- [109] 本说明书密码服务平台的实施例可以应用在计算机设备上，例如服务器等。装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为一个逻辑意义上的装置，是通过其所在的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，如图 3 所示，为本说明书实施例密码服务平台所在计算机设备的一种硬件结构图，除了图 3 所示的处理器 310、内存 330、网络接口 320、以及非易失性存储器 340 之外，实施例中密码服务平台 331 15 所在的服务器，通常根据该计算机设备的实际功能，还可以包括其他硬件，对此不再赘述。
- [110] 如图 4 所示，图 4 是本说明书根据一示例性实施例示出的一种密码运算方法的流程图，包括以下步骤：
- [111] 在步骤 402、接收业务系统发起的密码运算请求，所述密码运算请求携带有待运算数据。 20
- [112] 在步骤 404、确定响应所述密码运算请求的目标密码模块，所述目标密码模块为主密码模块或至少一个次密码模块中的一个，所述次密码模块的主密钥由所述主密码模块生成。
- [113] 在步骤 406、获取与所述目标密码模块的工作密钥密文，所述工作密钥密文为： 25 所述主密码模块利用所述目标密码模块的主密钥对工作密钥加密得到的密文，所述工作密钥由所述主密码模块为所述业务系统创建。
- [114] 在步骤 408、以所述工作密钥密文和所述待运算数据为输入，调用所述目标密码模块，获取所述目标密码模块返回的运算结果并发送给所述业务系统，所述运算结果由所述目标密码模块利用已存储主密钥对所述工作密钥密文解密得到工作密钥后，利用解

密得到的工作密钥对所述待运算数据进行加密得到。

[115] 可选的, 所述次密码模块的主密钥通过如下方式获得:

[116] 获取所述次密码模块生成的目标公钥;

[117] 以所述目标公钥作为输入, 调用所述主密码模块, 由所述主密码模块生成所述
5 次密码模块的主密钥, 利用所述目标公钥对所述生成的主密钥进行加密获得主密钥密文;

[118] 将所述主密钥密文发送给所述次密码模块, 由所述次密码模块利用与所述目标公钥对应的目标私钥解密获得主密钥。

[119] 可选的, 所述以所述目标公钥作为输入, 调用所述主密码模块, 由所述主密码模块生成所述次密码模块的主密钥, 包括:

10 [120] 获取所述主密码模块对所述目标公钥进行消息鉴别码计算获得的公钥校验值;

[121] 以所述目标公钥和公钥校验值为输入, 调用所述主密码模块, 由所述主密码模块基于所述公钥校验值校验输入的目标公钥的合法性后, 生成所述次密码模块的主密钥。

[122] 可选的, 所述次密码模块的主密钥通过如下方式获得:

[123] 调用主密码模块, 由主密码模块产生所述次密码模块的主密钥后, 获取所述主
15 密钥的两个或以上的密钥分量;

[124] 将所述两个或以上的密钥分量分别传输给各个密钥管理实体, 由所述密钥管理实体分别传输给所述次密码模块, 以供次密码模块根据各个密钥分量生成主密钥。

[125] 可选的, 所述方法还包括:

[126] 接收所述主密码模块返回的所述次密码模块的主密钥密文后并存储, 所述主密
20 钥密文以主密码模块的主密钥加密。

[127] 上述密码运算方法中各个步骤的实现过程可详见上述密码服务平台中各个模块的功能和作用的实现过程, 在此不再赘述。

[128] 如图 5 所示, 图 5 是本说明书根据一示例性实施例示出的一种创建工作密钥的流程图, 包括以下步骤:

25 [129] 在步骤 502 中, 接收业务系统的工作密钥创建请求;

[130] 在步骤 504 中, 调用主密码模块为所述业务系统生成工作密钥, 获取所述主密码模块返回的: 所述主密码模块的主密钥加密的工作密钥密文, 以及各个已连接次密码

模块的主密钥分别加密的工作密钥密文；其中，所述次密码模块的主密钥通过调用所述主密码模块，由所述主密码模块为所述次密码模块生成。

[131] 本说明书实施例中，密码服务平台所连接的密码模块中，其中一个作为主密码模块，密码服务平台的密钥管理功能中由主密码模块提供，主密码模块用于生成密钥，主密码模块和其他次密码模块提供密码服务平台所需要的密码运算功能。

[132] 其中，次密码模块的主密钥由主密码模块生成，业务系统的工作密钥也由主密码模块生成，并且密码服务平台保存有主密码模块的主密钥加密的工作密钥密文，以及各个次密码模块的主密钥分别加密的工作密钥密文，因此，本实施例中主密钥由主密码模块保存，主密钥作为敏感安全参数明文不会超出密码模块的边界，不会损失密钥的安全性，因此满足密钥的安全性要求。

[133] 相应的，本说明书实施例还提供一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现如下方法：

[134] 接收业务系统发起的密码运算请求，所述密码运算请求携带有待运算数据；

[135] 确定响应所述密码运算请求的目标密码模块，所述目标密码模块为主密码模块或至少一个次密码模块中的一个，所述次密码模块的主密钥由所述主密码模块生成；

[136] 获取与所述目标密码模块的工作密钥密文，所述工作密钥密文为：所述主密码模块利用所述目标密码模块的主密钥对工作密钥加密得到的密文，所述工作密钥由所述主密码模块为所述业务系统创建；

[137] 以所述工作密钥密文和所述待运算数据为输入，调用所述目标密码模块，获取所述目标密码模块返回的运算结果并发送给所述业务系统，所述运算结果由所述目标密码模块利用已存储主密钥对所述工作密钥密文解密得到工作密钥后，利用解密得到的工作密钥对所述待运算数据进行加密得到。

[138] 相应的，本说明书实施例还提供一种密码服务设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现如下方法：

[139] 接收业务系统的工作密钥创建请求；

[140] 调用主密码模块为所述业务系统生成工作密钥，获取所述主密码模块返回的：

所述主密码模块的主密钥加密的工作密钥密文，以及各个已连接次密码模块的主密钥分别加密的工作密钥密文；其中，所述次密码模块的主密钥通过调用所述主密码模块，由所述主密码模块为所述次密码模块生成。

- [141] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理模块，即可以位于一个地方，或者也可以分布到多个网络模块上。可以根据实际的需要选择其中的部分或者全部模块来实现本说明书方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。
- 10 [142] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。
- 15 [143] 本领域技术人员在考虑说明书及实践这里申请的发明后，将容易想到本说明书的其它实施方案。本说明书旨在涵盖本说明书的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本说明书的一般性原理并包括本说明书未申请的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本说明书的真正范围和精神由下面的权利要求指出。
- 20 [144] 应当理解的是，本说明书并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本说明书的范围仅由所附的权利要求来限制。
- [145] 以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保护的范围内。
- 25