

权利要求书

1、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：

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；

5 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；

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。

2、根据权利要求 1 所述的密码服务平台，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 获取所述次密码模块生成的目标公钥；

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；

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。

20 3、根据权利要求 2 所述的密码服务平台，所述注册模块，还用于：

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；

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。

25 4、根据权利要求 1 所述的密码服务平台，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：

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；

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。

30 5、根据权利要求 1 所述的密码服务平台，所述注册模块还用于：

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。

6、一种密码运算方法，包括：

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；

- 5 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；

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；

- 10 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。

7、根据权利要求6所述的方法，所述次密码模块的主密钥通过如下方式获得：

获取所述次密码模块生成的目标公钥；

- 15 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；

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。

- 20 8、根据权利要求7所述的方法，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：

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；

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。

9、根据权利要求6所述的方法，所述次密码模块的主密钥通过如下方式获得：

- 25 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；

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。

10、根据权利要求6所述的方法，所述方法还包括：

- 30 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。

11、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：

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；

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；

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；

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。

12、一种创建工作密钥的方法，包括：

接收业务系统的工作密钥创建请求；

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。

13、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：

接收业务系统的工作密钥创建请求；

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。