

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和至少一个次密码模块，各密码模块具有主密钥；所述密码服务平台包括：

注册模块，用于：调用所述次密码模块生成包括目标公钥和目标私钥的非对称密钥对，获取所述次密码模块返回的目标公钥后存储；

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，以所述次密码模块的目标公钥为输入，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，以及所述次密码模块的目标公钥加密的工作密钥密文；以所述次密码模块的目标公钥加密的工作密钥密文为输入，调用所述次密码模块，获取所述次密码模块返回的：以所述目标私钥解密输入的工作密钥密文后，以自身主密钥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，所述注册模块存储的目标私钥以所述次密码模块的主密钥加密。

3、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：获取所述次密码模块的主密钥加密的目标私钥指示数据；

所述工作密钥创建模块在调用所述次密码模块时，还以所述目标私钥指示数据为输入，以供所述次密码模块利用主密钥解密获取目标私钥后，解密输入的工作密钥密文。

4、根据权利要求 3 所述的密码服务平台，所述次密码模块的主密钥加密的目标私钥指示数据，包括：以所述次密码模块的主密钥对所述目标私钥加密的目标私钥密文，或以所述次密码模块的主密钥加密的目标私钥标识。

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：

以所述目标公钥为输入调用所述主密码模块，由所述主密码模块对所述目标公钥进行认证，获取主密码模块对所述目标公钥进行消息鉴别码值计算得到的密钥校验值；

所述密钥校验值由所述工作密钥创建模块在调用所述主密码模块时作为输入，以供所述主密码模块对输入的次密码模块的目标公钥进行校验。

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；

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，所述密码模块具有主密钥；

- 5 获取与所述目标密码模块的工作密钥密文，所述工作密钥密文预先通过如下方式获得：以所述次密码模块预先生成的目标公钥为输入，调用所述主密码模块为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，以及所述次密码模块的目标公钥加密的工作密钥密文；以所述次密码模块的目标公钥加密的工作密钥密文为输入，调用所述次密码模块，获取所述次密码模块返回的：以所述目标私钥解密输入的工作密钥密文后，以自身主密钥加密的工作密钥密文；
- 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，所述注册模块存储的目标私钥以所述次密码模块
- 15 的主密钥加密。

8、根据权利要求 6 所述的方法，还包括：获取所述次密码模块的主密钥加密的目标私钥指示数据；

在调用所述次密码模块时，还以所述目标私钥指示数据为输入，以供所述次密码模块利用主密钥解密获取目标私钥后，解密输入的工作密钥密文。

- 20 9、根据权利要求 8 所述的方法，所述次密码模块的主密钥加密的目标私钥指示数据，包括：以所述次密码模块的主密钥对所述目标私钥加密的目标私钥密文，或以所述次密码模块的主密钥加密的目标私钥标识。

10、根据权利要求 7 所述的方法，所述方法还包括：

- 25 以所述目标公钥为输入调用主密码模块，获取主密码模块对所述目标公钥进行消息鉴别码值计算得到的密钥校验值；

在调用所述主密码模块为业务系统生成工作密钥时，还以所述密钥校验值为输入，以供所述主密码模块对输入的次密码模块的目标公钥进行校验。

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：

- 30 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，所述密码模块具有主密钥；

获取与所述目标密码模块的工作密钥密文，所述工作密钥密文预先通过如下方式获得：以所述次密码模块预先生成的目标公钥为输入，调用所述主密码模块为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，以及所述次密码模块的目标公钥加密的工作密钥密文；以所述次密码模块的目标公钥加密的工作密钥密文为输入，调用所述次密码模块，获取所述次密码模块返回的：以所述目标私钥解密输入的工作密钥密文后，以自身主密钥加密的工作密钥密文；

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；

以次密码模块的目标公钥为输入，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，以及所述次密码模块的目标公钥加密的工作密钥密文；

以所述次密码模块的目标公钥加密的工作密钥密文为输入，调用所述次密码模块，获取所述次密码模块返回的：以目标私钥解密输入的工作密钥密文后，以自身主密钥加密的工作密钥密文；其中，所述目标公钥和目标私钥由所述次密码模块预先生成。

20 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；

以次密码模块的目标公钥为输入，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，以及所述次密码模块的目标公钥加密的工作密钥密文；

以所述次密码模块的目标公钥加密的工作密钥密文为输入，调用所述次密码模块，获取所述次密码模块返回的：以所述目标私钥解密输入的工作密钥密文后，以自身主密钥加密的工作密钥密文；其中，所述目标公钥和目标私钥由所述次密码模块预先生成。