(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 116232593 B
(45)授权公告日 2023.08.25

(21)申请号 202310511756.1
(22)申请日 2023.05.05
(65)同一申请的已公布的文献号
申请公布号 CN 116232593 A
(43)申请公布日 2023.06.06
(73)专利权人 杭州海康威视数字技术股份有限公司
地址 310051 浙江省杭州市滨江区阡陌路555号
(72)发明人 王滨 陈达 陈加栋 沈剑 谭皓文 王晨
(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
专利代理师 杨春香
(51)Int.Cl.
*H04L 9/14*(2006.01)
*H04L 9/08*(2006.01)
*H04L 9/32*(2006.01)
(56)对比文件
CN 103763355 A,2014.04.30
CN 111159684 A,2020.05.15
CN 113965327 A,2022.01.21
EP 3965361 A1,2022.03.09
US 9524399 B1,2016.12.20
CN 109728909 A,2019.05.07
CN 108243166 A,2018.07.03
CN 108540426 A,2018.09.14
CN 109347625 A,2019.02.15
CN 110879880 A,2020.03.13
CN 114218592 A,2022.03.22
CN 115618403 A,2023.01.17
CN 115664712 A,2023.01.31
Zhishen Zhu;Junzheng Shi;Chonghua Wang;Gang Xiong;Zhiqiang Hao.MCFM: Discover Sensitive Behavior from Encrypted Traffic in Industrial Control System.《2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)》.2023,全文.
审查员 李华

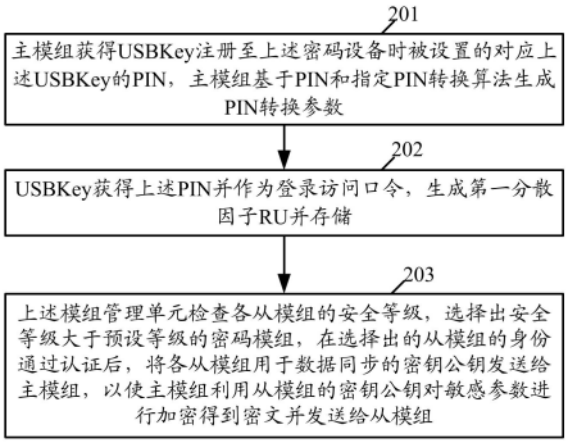
权利要求书3页 说明书13页 附图5页

(54)发明名称

多密码模组敏感数据分类分级与保护方法、设备及系统

(57)摘要

本申请实施例提供了多密码模组敏感数据分类分级与保护方法、设备及系统。本实施例通过对密码设备中的密码模组和敏感业务数据进行分级，并动态调整敏感业务数据流向级别匹配的密码模组进行密码运算处理，使得敏感业务数据在其匹配的密码模组流通，不再流出其匹配的密码模组的安全边界，这避免了现有敏感业务数据在所有密码模组流通所导致的敏感业务数据泄露的问题，保证了敏感业务数据的安全。




CN 116232593 B

1.一种多密码模组敏感数据分类分级与保护方法,其特征在于,该方法应用于密码设备中的模组管理单元,所述密码设备作为一个硬件被插入至服务器集群中任一服务器来使用,所述密码设备还包括至少两个密码模组,该方法包括:

基于当前登录所述密码设备的登录访问口令PIN,控制密码设备中的目标密码模组与智能密码钥匙USBKey进行身份认证,以使目标密码模组在完成与USBKey的身份认证后从USBKey获得第一分散因子RU并基于第一分散因子RU和目标密码模组已存储的PIN转换参数衍生出一级根密钥;所述PIN转换参数是基于指定PIN转换算法对所述PIN进行转换得到;所述目标密码模组是指所述密码设备中安全等级大于预设等级的其中一个密码模组;所述密码设备中各密码模组基于预设权重等级和/或当前状态信息被分配对应的安全等级;

控制所述密码设备中其它密码模组基于所述第一分散因子RU和所述其它密码模组已存储的所述PIN转换参数衍生出一级根密钥;所述其它密码模组是指除所述目标密码模组之外且安全等级大于预设等级的密码模组;

对待处理的各组敏感业务数据进行分级,基于各组敏感业务数据的级别和各密码模组的安全等级,分配各组敏感业务数据至对应的密码模组,以由密码模组利用衍生出的一级根密钥获得用于对敏感业务数据进行密码运算处理的目标密钥并基于目标密钥对敏感业务数据进行密码运算处理。

2.根据权利要求1所述的方法,其特征在于,所述控制所述密码设备中其它密码模组基于所述第一分散因子RU和所述其它密码模组已存储的所述PIN转换参数衍生出一级根密钥包括:

获得所述目标密码模组在衍生出所述一级根密钥后上送的所述第一分散因子RU;

将所述第一分散因子RU下发给其它密码模组,以由其它密码模组基于所述第一分散因子RU和所述其它密码模组已存储的所述PIN转换参数衍生出一级根密钥。

3.根据权利要求1或2所述的方法,其特征在于,该方法之前进一步包括:

在基于所述USBKey注册至所述密码设备的注册过程中,将各从模组用于数据同步的密钥公钥发送给主模组,以使主模组利用从模组的密钥公钥对敏感参数进行加密得到密文并发送给从模组,所述从模组被用于利用用于数据同步的密钥私钥对所述密文进行解密并存储解密得到的敏感参数;所述主模组为所述密码设备中安全等级最高的密码模组,所述从模组是指除所述主模组之外且安全等级大于预设等级的密码模组;所述敏感参数至少包括所述PIN转换参数;

所述第一分散因子RU是所述USBKey在所述注册过程中生成的。

4.根据权利要求1所述的方法,其特征在于,所述分配各组敏感业务数据至对应的密码模组包括:针对每一密码模组,将待分配给该密码模组的至少一组敏感业务数据添加数字水印信息并分配给该密码模组;所述数字水印信息被用于敏感业务数据对应的行为溯源和/或行为建模分析;

和/或,所述对待处理的各组敏感业务数据进行分级包括:

针对每一组敏感业务数据,按照设定的分类分级评估角度,确定敏感业务数据在各分类分级评估角度的评估分数;基于该组敏感业务数据在各分类分级评估角度的评估分数,确定该组敏感业务数据的敏感级别;其中,所述分类分级评估角度至少包括:所采用的协议报文合法性、数据格式合法性、敏感业务数据的源端的身份权限、敏感业务数据对应的操作

的重要程度、敏感业务数据的目标端执行所述敏感业务数据对应操作的身份权限。

5.一种多密码模组敏感业务数据分类分级与保护方法,其特征在于,该方法应用于密码设备中的任一密码模组,所述密码设备作为一个硬件被插入至服务器集群中任一服务器来使用,所述密码设备包括模组管理单元和至少两个密码模组,该方法包括:

任一密码模组,在基于所述密码设备的当前登录被所述模组管理单元选取为目标密码模组时,在所述模组管理单元的控制下,基于当前登录所述密码设备的登录访问口令PIN,与智能密码钥匙USBKey进行身份认证,并在与USBKey的身份认证后从USBKey获得第一分散因子RU并基于第一分散因子RU和本密码模组已存储的PIN转换参数衍生出一级根密钥;所述PIN转换参数是基于指定PIN转换算法对所述PIN进行转换得到;所述目标密码模组是指所述密码设备中安全等级大于预设等级的其中一个密码模组;所述密码设备中各密码模组基于预设权重等级和/或当前状态信息被分配对应的安全等级;

任一密码模组,在不为所述目标密码模组时,假如被分配的安全等级大于预设等级,则在目标密码模组衍生出一级根密钥后,在所述模组管理单元的控制下,基于所述第一分散因子RU和本密码模组已存储的所述PIN转换参数衍生出一级根密钥;

任一密码模组,在被分配敏感业务数据后,利用衍生出的一级根密钥获得用于对敏感业务数据进行密码运算处理的目标密钥,并基于目标密钥对敏感业务数据进行密码运算处理;密码模组被分配的敏感业务数据的敏感级别与密码模组的安全等级匹配。

6.根据权利要求5所述的方法,其特征在于,所述目标密码模组基于当前登录所述密码设备的登录访问口令PIN,与智能密码钥匙USBKey进行身份认证包括:

接收所述模组管理单元基于所述密码设备的当前登录发送的身份校验请求;

按照所述指定PIN转换算法对所述身份校验请求携带的PIN进行转换得到转换结果,并在所述转换结果和已存储的所述PIN转换参数满足设定匹配条件时生成随机数R1并向USBKey发送,以使得所述USBKey在所述PIN通过校验后对所述随机数R1和已生成的随机数R2进行签名得到第一数字签名;

接收所述USBKey发送的所述第一数字签名和USBKey数字证书,利用已预置的CA根证书验证所述USBKey数字证书和所述第一数字签名是否合法,并在验证合法后基于所述第一数字签名获得所述随机数R1和随机数R2,对所述随机数R1和随机数R2进行签名得到第二数字签名;将所述第二数字签名和密码模组数字证书发给所述USBKey以使所述USBKey基于预置的CA根证书验证所述密码模组数字证书和所述第二数字签名是否合法,并在验证合法后,确定目标密码模组基于当前登录所述密码设备的PIN与USBKey完成身份认证。

7.根据权利要求5所述的方法,其特征在于,所述从USBKey获得第一分散因子RU并基于第一分散因子RU和本密码模组已存储的PIN转换参数衍生出一级根密钥包括:

接收所述USBKey发送的第一分散因子密文;所述第一分散因子密文是所述USBKey使用所述目标密码模组的密钥公钥对第一分散因子RU加密得到,所述第一分散因子RU是USBKey在注册至所述密码设备的注册过程中生成的;

利用所述目标密码模组的密钥私钥对所述第一分散因子密文解密得到第一分散因子RU;

使用第一分散因子RU和本密码模组已存储的PIN转换参数衍生出一级根密钥。

8.根据权利要求6所述的方法,其特征在于,该方法之前进一步包括:

任一密码模组，在被选举为主模组时，所述主模组为所述密码设备中安全等级最高的密码模组，则在基于所述USBKey注册至所述密码设备的注册过程中，获得所述模组管理单元发送的各从模组用于数据同步的密钥公钥；所述从模组是指除所述主模组之外且安全等级大于预设等级的密码模组；之后利用从模组的密钥公钥对敏感参数进行加密得到密文并发送给从模组；

任一密码模组，在作为从模组时，利用本密码模组用于数据同步的密钥私钥对得到的密文进行解密并存储解密得到的敏感参数；所述敏感参数至少包括目标密码模组在与USBKey双向认证时所需的参数。

9.根据权利要求8所述的方法，其特征在于，所述敏感参数至少包括随机数RC和PIN转换参数，所述随机数RC为所述主模组生成的，所述PIN转换参数是基于指定PIN转换算法对所述注册过程中获得的所述PIN和所述随机数RC进行转换得到；

所述按照所述指定PIN转换算法对所述身份校验请求携带的PIN进行转换得到转换结果包括：基于指定PIN转换算法对所述身份校验请求携带的PIN和已存储的所述随机数RC进行转换得到转换结果。

10.根据权利要求5所述的方法，其特征在于，所述利用衍生出的一级根密钥获得用于对敏感业务数据进行密码运算处理的目标密钥包括：

获得被分配的敏感业务数据在被进行密码运算处理时所需的二级密钥索引和三级密钥信息；所述二级密钥索引对应的二级密钥是在所述USBKey成功注册至所述密码设备后生成的、且经由在注册时衍生出的一级根密钥加密；

基于衍生出的一级根密钥对二级密钥索引对应的二级密钥密文进行解密，得到二级密钥；

若所述三级密钥信息为与本地已有的三级密钥密文对应的三级密钥索引，则利用所述二级密钥对所述三级密钥密文进行解密，得到三级密钥，若所述三级密钥信息为三级密钥密文，则利用所述二级密钥对所述三级密钥密文进行解密，得到三级密钥，将所述三级密钥确定为所述目标密钥。

11.一种多密码模组敏感业务数据分类分级与保护系统，其特征在于，该系统包括多个密码设备；

任一密码设备包括模组管理单元和至少两个密码模组；

任一密码设备中的模组管理单元执行如权利要求1至4任一方法中的步骤，任一密码设备中的密码模组执行如权利要求5至10任一方法中的步骤；

不同密码设备之间备份敏感业务数据，其中一个密码设备中安全等级最高的密码模组对应的敏感业务数据被备份至另一密码设备中安全等级最高的密码模组。

12.一种密码设备，其特征在于，所述密码设备包括模组管理单元和至少两个密码模组；

所述模组管理单元执行如权利要求1至4任一方法中的步骤；

任一密码设备中的密码模组执行如权利要求5至10任一方法中的步骤。

# 多密码模组敏感数据分类分级与保护方法、设备及系统

## 技术领域

[0001] 本申请涉及数据安全技术，特别涉及多密码模组敏感数据分类分级与保护方法、设备及系统。

## 背景技术

[0002] 密码设备，比如密码卡、密码机等硬件，其作为保障大型系统数据安全的基础设施，形态越来越多样化。比如一个密码设备中集成多个密码模组。这里，密码模组是指相对独立的硬件密码模块，其具有密码运算功能，也称密码运算单元。

[0003] 相比仅集成一个密码模组的密码设备(如密码卡、密码机)，集成了多密码模组的密码设备在基于密码模组进行密码运算时极易造成敏感数据泄漏，这里的敏感数据比如为敏感业务数据等。而敏感数据的泄漏，会引起严重的安全危害。

## 发明内容

[0004] 本申请实施例提供了多密码模组敏感数据分类分级与保护方法、装置及系统，以解决由多密码模组引发的敏感数据泄露风险。

[0005] 本申请实施例提供了多密码模组敏感数据分类分级与保护方法，该方法应用于密码设备中的模组管理单元，所述密码设备还包括至少两个密码模组，该方法包括：

[0006] 基于当前登录所述密码设备的登录访问口令PIN，控制密码设备中的目标密码模组与智能密码钥匙USBKey进行身份认证，以使目标密码模组在完成与USBKey的身份认证后从USBKey获得第一分散因子RU并基于第一分散因子RU和目标密码模组已存储的PIN转换参数衍生出一级根密钥；所述PIN转换参数是基于指定PIN转换算法对所述PIN进行转换得到；所述目标密码模组是指所述密码设备中安全等级大于预设等级的其中一个密码模组；所述密码设备中各密码模组基于预设权重等级和/或当前状态信息被分配对应的安全等级；

[0007] 控制所述密码设备中其它密码模组基于所述第一分散因子RU和所述其它密码模组已存储的所述PIN转换参数衍生出一级根密钥；所述其它密码模组是指除所述目标密码模组之外且安全等级大于预设等级的密码模组；

[0008] 对待处理的各组敏感业务数据进行分级，基于各组敏感业务数据的级别和各密码模组的安全等级，分配各组敏感业务数据至对应的密码模组，以由密码模组利用衍生出的一级根密钥获得用于对敏感业务数据进行密码运算处理的目标密钥并基于目标密钥对敏感业务数据进行密码运算处理。

[0009] 一种多密码模组敏感业务数据分类分级与保护方法，该方法应用于密码设备中的任一密码模组，所述密码设备包括模组管理单元和至少两个密码模组，该方法包括：

[0010] 任一密码模组，在基于所述密码设备的当前登录被所述模组管理单元选取为目标密码模组时，在所述模组管理单元的控制下，基于当前登录所述密码设备的登录访问口令PIN，与智能密码钥匙USBKey进行身份认证，并在与USBKey的身份认证后从USBKey获得第一分散因子RU并基于第一分散因子RU和本密码模组已存储的PIN转换参数衍生出一级根密

钥;所述PIN转换参数是基于指定PIN转换算法对所述PIN进行转换得到;所述目标密码模组是指所述密码设备中安全等级大于预设等级的其中一个密码模组;所述密码设备中各密码模组基于预设权重等级和/或当前状态信息被分配对应的安全等级;

[0011] 任一密码模组,在不为所述目标密码模组时,假如被分配的安全等级大于预设等级,则在目标密码模组衍生出一级根密钥后,在所述模组管理单元的控制下,基于所述第一分散因子RU和本密码模组已存储的所述PIN转换参数衍生出一级根密钥;

[0012] 任一密码模组,在被分配敏感业务数据后,利用衍生出的一级根密钥获得用于对敏感业务数据进行密码运算处理的目标密钥,并基于目标密钥对敏感业务数据进行密码运算处理;密码模组被分配的敏感业务数据的敏感级别与密码模组的安全等级匹配。

[0013] 一种多密码模组敏感业务数据分类分级与保护系统,该系统包括多个密码设备;

[0014] 任一密码设备包括模组管理单元和至少两个密码模组;

[0015] 任一密码设备中的模组管理单元执行如上第一种方法中的步骤,任一密码设备中的密码模组执行如上第二种方法中的步骤;

[0016] 不同密码设备之间备份敏感业务数据,其中一个密码设备中安全等级最高的密码模组对应的敏感业务数据被备份至另一密码设备中安全等级最高的密码模组。

[0017] 一种密码设备,所述密码设备包括模组管理单元和至少两个密码模组;

[0018] 任一密码设备中的模组管理单元执行如上第一种方法中的步骤,任一密码设备中的密码模组执行如上第二种方法中的步骤。

[0019] 由以上技术方案可以看出,本申请中,通过对密码设备中的密码模组和敏感业务数据进行分级,并动态调整敏感业务数据流向级别匹配的密码模组进行密码运算处理,使得敏感业务数据在其匹配的密码模组流通,不再流出其匹配的密码模组的安全边界,这避免了现有敏感业务数据在所有密码模组流通所导致的敏感业务数据泄露的问题,保证了敏感业务数据的安全。

[0020] 进一步地,在本实施例提供的方法局限在安全等级大于预设等级的密码模组衍生出一级根密钥,这确保了安全等级小于或等于预设等级的密码模组(也即非可信密码模组)无法衍生出一级根密钥,也无法对已加密的二级密钥进行解密,这进一步降低密钥数据(比如衍生出一级根密钥所需要的第一分散因子RU、PIN转换参数等,也称敏感数据)的泄露风险。

[0021] 更进一步地,在本实施例中,在每次登录密码设备时,都会控制安全等级大于预设等级的各密码模组动态衍生出一级根密钥,而非固定住一级根密钥,这保证了一级根密钥(也称敏感数据)的泄露风险。

## 附图说明

[0022] 此处的附图被并入说明书中并构成本说明书的一部分,示出了符合本公开的实施例,并与说明书一起用于解释本公开的原理。

[0023] 图1为本申请实施例提供的密码设备的结构示意图;

[0024] 图2为本实施例提供的注册流程图;

[0025] 图3为本申请实施例提供的方法流程图;

[0026] 图4为本申请实施例提供的另一方法流程图;

[0027] 图5为本申请实施例提供的身份认证流程图；

[0028] 图6为本申请实施例提供的系统图；

[0029] 图7为本申请实施例提供的电子设备结构图。

## 具体实施方式

[0030] 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。以下示例性实施例中所描述的实施方式并不代表与本申请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、本申请的一些方面相一致的装置和方法的例子。

[0031] 在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请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。

[0032] 密码设备，比如密码卡、密码机等，其一般包括模组管理单元和密码模组。本实施例重点关注密码设备中有多个密码模组(至少两个密码模组)的情况，图1举例示出了密码设备的结构。

[0033] 作为一个实施例，上述的模组管理单元在具体实现时有很多实现形式，比如可为通过硬件实现的FPGA逻辑调度单元，本实施例并不具体限定。

[0034] 在本实施例中，密码设备相当于一个硬件，其可插入服务器集群中任一服务器来使用。一旦服务器在被插入密码设备时，服务器中的驱动程序会动态发现该新插入的密码设备，比如通过监听高速串行计算机扩展总线标准PCIE、USB等动态发现该新插入的密码设备。当服务器中的驱动程序发现新插入的密码设备后，其会先按照预设校验规则对该密码设备进行自检，比如检查该密码设备的安全状态(比如密码设备是否存在故障、密码设备是否存在安全风险如窃听攻击、软件攻击、故障生成攻击、探测攻击等)、该密码设备的算法正确性、该密码设备的可信等级等，一旦检查出异常，则会发出告警以提示密码设备管理员进行异常处理。而假若密码设备正常，则可对密码设备中的各密码模组进行分级。

[0035] 本实施例中，对密码设备中的各密码模组进行分级有很多实现方式。作为一个实施例，可基于密码模组被配置的权重，来实现对密码设备中的各密码模组进行分级。比如，密码模组被配置的权重与密码模组被分配的安全等级正相关，密码模组被配置的权重越高，密码模组被分配的安全等级越高，反之，密码模组被配置的权重越低，密码模组被分配的安全等级越低。

[0036] 作为另一个实施例，也可基于密码模组的当前状态信息为密码设备中各密码模组分配对应的安全等级。

[0037] 比如，密码模组的当前状态信息至少包括：密码模组所在的密码设备的安全状态信息、和/或密码模组的算法测试结果、和/或密码模组所在的密码设备可提供的安全措施、和/或密码模组所在的密码设备的可信等级、和/或密码模组所在的密码设备的业务流量负载、密码模组的数据同步性。

[0038] 基于此，本实施例中，则针对每一密码模组，可获得该密码模组的以下当前状态信息：该密码模组所在的密码设备的安全状态信息(比如密码设备是否存在故障、密码设备是否存在安全风险如窃听攻击、软件攻击、故障生成攻击、探测攻击等)、和/或该密码模组的

算法测试结果(比如国家密码管理局、联邦信息处理标准等核准的已知答案测试的结果)、和/或密码模组所在的密码设备可提供的安全措施(比如是否提供一次性可编程(OTP:One Time Programmable)一次性写入的存储区域、TEE/SGX可执行环境安全隔离等安全机制)、和/或该密码模组所在的密码设备的可信等级(包括安全认证等级、器件国产化程度)、和/或该密码模组所在的密码设备的业务流量负载(比如CPU、内存、DDR/FLASH指标和动态实时的业务数据流量和运算引擎负载等)、和/或该密码模组的数据同步性(密码模组应同步的关键敏感参数是否被非法篡改)等。

[0039] 之后,基于获得的上述当前状态信息,为该密码模组分配对应的安全等级。在本实施例中,为便于为该密码模组分配对应的安全等级,还可预先设置对应的等级分配规则,该等级分配规则用于指示如何基于当前状态信息,为密码模组分配对应的安全等级。

[0040] 具体地,假若密码设备中所有密码模组分为四个安全等级,一级为最高安全级别,四级为最低安全级别,则按照上述等级分配规则,当一密码模组的当前状态信息均满足要求,比如,密码模组所在的密码设备的安全状态信息满足要求(比如密码设备不存在故障、密码设备不存在安全风险如窃听攻击、软件攻击、故障生成攻击、探测攻击等)、该密码模组的算法测试结果满足要求(比如算法测试结果为:通过国家密码管理局、联邦信息处理标准等核准的已知答案测试)、密码模组所在的密码设备可提供的安全措施满足要求(比如提供一次性可编程(OTP:One Time Programmable)一次性写入的存储区域、TEE/SGX可执行环境安全隔离等安全机制)、该密码模组所在的密码设备的可信等级满足要求(包括满足安全认证等级、器件国产化程度)、该密码模组所在的密码设备的业务流量负载满足要求(比如CPU、内存、DDR/FLASH当前的可用量大于或等于设定阈值)、密码模组的数据同步性满足要求(密码模组应同步的关键敏感参数未被非法篡改),则确定该密码模组的安全等级为最高安全级别比如四级。假若一密码模组的当前状态信息有至少一个指定信息不满足要求比如密码模组的数据同步性不满足要求等,则确定该密码模组的安全等级为最低安全级别比如一级。当然,假若一密码模组的当前状态信息中指定信息均满足要求比如密码模组的数据同步性满足要求等,但其它非指定信息不满足要求比如密码模组所在的密码设备可提供的安全措施不满足要求(比如不能提供一次性可编程(OTP:One Time Programmable)一次性写入的存储区域、TEE/SGX可执行环境安全隔离等安全机制),则可依据不满足要求的信息的数量,确定该密码模组的安全等级,比如如果有至少两个信息不满足要求,则确定该密码模组的安全等级为二级,否则,确定该密码模组的安全等级为三级。

[0041] 以上只是举例描述如何基于等级分配规则为密码模组确定安全等级,并非用于限定。

[0042] 作为一个实施例,上述当前状态信息中,密码设备是否存在故障可基于对应的故障检测机制实现,比如上述驱动程序定时向上述密码设备发送故障检测包,以基于故障检测包检测密码设备是否存在故障。同样,上述密码设备是否存在安全风险如窃听攻击、软件攻击、故障生成攻击、探测攻击等,可基于对应的风险检测机制实现,比如上述驱动程序实时检测发向上述密码设备的数据包,以基于数据包检测密码设备是否存在安全风险如窃听攻击、软件攻击、故障生成攻击、探测攻击等。

[0043] 作为一个实施例,上述当前状态信息中,密码模组的算法测试结果比如国家密码管理局、联邦信息处理标准等核准的已知答案测试的结果,会配置在密码模组,本实施例可

基于密码模组的配置获得密码模组的算法测试结果。

[0044] 作为一个实施例，上述当前状态信息中，密码模组所在的密码设备可提供的安全措施比如是否提供OTP一次性写入的存储区域、TEE/SGX可执行环境安全隔离等安全机制、和/或该密码模组所在的密码设备的可信等级比如安全认证等级、器件国产化程度等也会配置在密码设备的指定存储区域，本实施例可基于密码模组的配置，获得密码模组所在的密码设备可提供的安全措施和/或可信等级。

[0045] 以上举例描述了如何对密码设备中的各密码模组进行分级。需要说明的是，本实施例并不局限对密码设备中各密码模组分级的具体实现方式。

[0046] 基于如上描述的密码模组的分级，为了使本申请实施例提供的方法更加清楚，下面先描述通过插入智能密码钥匙(USBKey)至密码设备实现USBKey注册至密码设备的过程：

[0047] 参见图2，图2为本申请实施例提供的注册流程图。本实施例中，该注册流程会涉及到主模组。这里，主模组为上述密码设备中安全等级最高的密码模组，剩余模组为从模组。为便于理解该注册流程，本注册流程不站在单侧描述，具体如图2所示。

[0048] 如图2所示，该流程可包括以下步骤：

[0049] 步骤201，主模组获得USBKey注册至上述密码设备时被设置的对应上述USBKey的PIN，主模组基于PIN和指定PIN转换算法生成PIN转换参数。

[0050] 作为一个实施例，在本步骤201之前，主模组会生成第二分散因子RC。比如，主模组通过国家密码管理局核准的算法随机生成一个随机数，该随机数可作为第二分散因子RC。主模组在生成第二分散因子RC后，会将第二分散因子RC存储在主模组的安全存储区。应用于本步骤201，主模组基于PIN和指定PIN转换算法生成PIN转换参数，可进一步借助于第二分散因子RC。比如，以指定PIN转换算法为SM3哈希算法为例，则PIN转换参数可通过下式表示：

[0051] PIN’=SM3(RC异或PIN)；其中，PIN’表示PIN转换参数。

[0052] 主模组在生成PIN转换参数之后，会将PIN转换参数存储在主模组的安全存储区。

[0053] 步骤202，USBKey获得上述PIN并作为登录访问口令，生成第一分散因子RU并存储。

[0054] 在本实施例中，上述PIN会传递给USBKey，如步骤202描述，当USBKey获得该PIN后，其会将该PIN作为登录访问口令，之后生成第一分散因子RU并存储。

[0055] 作为一个实施例，USBKey生成第一分散因子RU有很多实现形式，比如，USBKey生成随机数作为第一分散因子RU。

[0056] 步骤203，上述模组管理单元检查各从模组的安全等级，选择出安全等级大于预设等级的密码模组，在选择出的从模组的身份通过认证后，将各从模组用于数据同步的密钥公钥发送给主模组，以使主模组利用从模组的密钥公钥对敏感参数进行加密得到密文并发送给从模组。

[0057] 在本实施例中，密码设备中各密码模组被划分出安全等级后，会同步至上述模组管理单元。基于此，上述模组管理单元会基于同步的各密码模组的安全等级，选择出安全等级大于预设等级(比如二级)的密码模组。

[0058] 在本实施例中，对选择出的从模组进行身份认证有很多实现方式，比如，获得从模组最新上送的用于数据同步的密钥公钥，检查该密钥公钥与该从模组之前上送的用于数据同步的密钥公钥是否满足设定匹配条件(比如一致或者相似度大于设定阈值等)，如果是，

则确定该从模组的身份通过认证。当然，本实施例并不局限对选择出的从模组进行身份认证的具体实现方式。

[0059] 作为一个实施例，这里的敏感参数可为上述目标密码模组在与USBKey身份认证时所需的参数，比如可包括：上述PIN转换参数、上述第二分散因子RC。

[0060] 通过步骤203，则最终实现针对选择出的通过身份认证的每一从模组，主模组利用该从模组的密钥公钥对敏感参数进行加密得到密文并发送给该从模组。当从模组接收到密文后，会利用用于数据同步的密钥私钥对密文进行解密得到上述敏感参数并存储至本从模组的安全存储区。在本实施例中，各从模组用于数据同步的密钥公钥可为非对称密钥公钥，对应的密钥私钥为非对称密钥私钥。

[0061] 通过步骤203可以看出，本实施例只允许在安全等级大于上述预设等级的密码模组之间交互上述敏感参数(用于协商密钥和后续的密码运算，具体见下文描述)，确保了非安全密码模组(安全等级小于上述预设等级)无法获得上述敏感参数，进而无法协商密钥和后续的密码运算，降低敏感数据泄漏风险。

[0062] 需要说明的是，在本实施例中，如上描述，仅允许安全等级高于上述预设等级的密码模组存储上述敏感参数。若上述模组管理单元检测到一密码模组的安全等级由高于预设等级变为低于预设等级，则可立即控制该密码模组销毁上述敏感参数(比如先置零再清除)，以降低敏感参数泄漏的风险。

[0063] 至此，完成图2所示流程。

[0064] 通过图2所示流程实现了USBKey如何注册至上述密码设备。

[0065] 在USBKey成功注册至上述密码设备后，或者后续插入上述USBKey至上述密码设备来进行登录时，先站在上述模组管理单元的角度描述本实施例提供的方法：

[0066] 参见图3，图3为本申请实施例提供的方法流程图。该流程应用于上述模组管理单元。如图3所示，该流程可包括以下步骤：

[0067] 步骤301，基于当前登录密码设备的PIN，控制密码设备中的目标密码模组与USBKey进行身份认证。

[0068] 在USBKey成功注册至上述密码设备后，或者在每次检测到有USBKey插入密码设备并触发登录时，模组管理单元会从安全等级大于预设等级的所有密码模组中随机选择一个密码模组(记为目标密码模组)，之后向目标密码模组发送身份校验请求，以触发目标密码模组基于身份校验请求携带的PIN与上述USBKey进行身份认证。最终实现了步骤301中基于当前登录密码设备的PIN，控制目标密码模组与USBKey进行身份认证。

[0069] 至于目标密码模组与USBKey如何进行身份认证，下文图4和图5所示流程会有描述，这里暂不赘述。目标密码模组在完成与USBKey的身份认证后，会从USBKey获得第一分散因子RU并基于第一分散因子RU和目标密码模组已存储的PIN转换参数衍生出一级根密钥(下文会举例描述)。如上描述可知，第一分散因子RU是由USBKey在USBKey注册至密码设备的注册过程中生成的，PIN转换参数是由主模组在USBKey注册至密码设备的注册过程中生成并下发至各安全等级大于预设等级的从模组的。

[0070] 步骤302，控制密码设备中其它密码模组基于第一分散因子RU和其它密码模组已存储的PIN转换参数衍生出一级根密钥；其它密码模组是指除目标密码模组之外且安全等级大于预设等级的密码模组。

[0071] 作为一个实施例，目标密码模组衍生出一级根密钥之后，会上送上述第一分散因子RU给上述模组管理单元。模组管理单元在获得目标密码模组上送的述第一分散因子RU后，会下发给其它密码模组，以由其它密码模组基于第一分散因子RU和其它密码模组已存储的PIN转换参数衍生出一级根密钥。

[0072] 步骤303，对待处理的各组敏感业务数据进行分级，基于各组敏感业务数据的级别和各密码模组的安全等级，分配各组敏感业务数据至对应的密码模组，以由各密码模组基于衍生出的一级根密钥对已加密的二级密钥进行解密并基于解密出的二级密钥对被分配的敏感业务数据进行对应的密码运算处理。

[0073] 在本实施例中，待处理的各组敏感业务数据，为上述密码设备接收的来自外部的各组敏感业务数据。其中，任一组敏感业务数据可为重要程度比较高(比如大于设定阈值)的业务数据包，比如，请求和响应数据包、永久存储数据包、临时协商数据包等，本实施例并不具体限定。

[0074] 作为一个实施例，本实施例可预先设定分级评估角度，比如协议报文合法性、数据格式合法性、请求主体(发送敏感业务数据的源端)的身份权限、请求操作(敏感业务数据对应的操作)的重要程度、请求对象(敏感业务数据的目标端)执行上述敏感业务数据对应操作的身份权限等角度。

[0075] 之后，基于设定的分级评估角度，对待处理的各组敏感业务数据进行分级。比如，针对每一组敏感业务数据，按照设定的分类分级评估角度，确定敏感业务数据在各分类分级评估角度的评估分数；基于该组敏感业务数据在各分类分级评估角度的评估分数，确定该组敏感业务数据的敏感级别。

[0076] 作为一个实施例，本实施例可预先基于上述设定分级评估角度建立评估模型，之后针对任一组敏感业务数据确定敏感级别时，可将该敏感业务数据输入评估模型，以由评估模型确定敏感业务数据在各分类分级评估角度的评估分数，以及基于该组敏感业务数据在各分类分级评估角度的评估分数，确定该组敏感业务数据的敏感级别并输出。最终实现了任一组敏感业务数据的敏感级别，比如，敏感级别可分为四个等级，一级为最高敏感级别，四级为最低敏感级别。

[0077] 在确定出各组敏感业务数据的级别之后，即可基于各组敏感业务数据的级别和各密码模组的安全等级，对各组敏感业务数据进行分配。在具体实现时，可基于预设运算调度规则对各组敏感业务数据进行分配。比如，针对任一组敏感业务数据，可将该组敏感业务数据分配给级别高于该敏感业务数据的级别的密码模组中进行处理。

[0078] 在密码模组被分配敏感业务数据后，该密码模组即可基于衍生出的一级根密钥获得用于对敏感业务数据进行密码运算处理的目标密钥(比如下文描述的二级密钥、三级密钥等)，并基于目标密钥对敏感业务数据进行密码运算处理比如加解密，下文会有描述，这里暂不赘述。

[0079] 至此，完成图3所示流程。

[0080] 通过图3所示流程可以看出，在本实施例中，通过对密码设备中的密码模组和敏感业务数据进行分级，并动态调整敏感业务数据流向级别匹配的密码模组进行密码运算处理，使得敏感业务数据在其匹配的密码模组流通，不再流出其匹配的密码模组的安全边界，这避免了现有敏感业务数据在所有密码模组流通所导致的敏感业务数据泄露的问题，保证

了敏感业务数据的安全。

[0081] 进一步地,在本实施例提供的方法局限在安全等级大于预设等级的密码模组衍生出一级根密钥,这确保了安全等级小于或等于预设等级的密码模组(也即非可信密码模组)无法衍生出一级根密钥,也无法对已加密的二级密钥进行解密,这进一步降低密钥数据(比如衍生出一级根密钥所需要的第一分散因子RU、PIN转换参数等,也称敏感数据)的泄露风险。

[0082] 更进一步地,在本实施例中,在每次登录密码设备时,都会控制安全等级大于预设等级的各密码模组动态衍生出一级根密钥,而非固定住一级根密钥,这保证了一级根密钥(也称敏感数据)的泄露风险。

[0083] 结合上述图3所示流程,下面站在密码模组的角度描述本实施例提供的方法:

[0084] 参见图4,图4为本实施例提供的另一方法流程图。该流程可应用于任一密码模组。结合上述图3所示流程,则如图4所示,该流程可包括以下步骤:

[0085] 步骤401,任一密码模组,在基于上述密码设备的当前登录被上述模组管理单元选取为上述目标密码模组时,则在模组管理单元的控制下,基于当前登录上述密码设备的PIN,与USBKey进行身份认证,并在与USBKey的身份认证通过后从USBKey获得第一分散因子RU并基于第一分散因子RU和本密码模组已存储的PIN转换参数衍生出一级根密钥。

[0086] 下文图5举例描述了如何在模组管理单元的控制下,基于当前登录上述密码设备的PIN,与USBKey进行身份认证,这里暂不赘述。

[0087] 在本实施例中,当目标密码模组的身份通过USBKey的认证,且当USBKey的身份通过目标密码模组的认证(也即相互通过认证)后,USBKey会向目标密码模组发送第一分散因子密文;第一分散因子密文是USBKey使用目标密码模组的密钥公钥对已存储的第一分散因子RU进行加密得到。当目标密码模组接收USBKey发送的第一分散因子密文,利用目标密码模组的密钥私钥对第一分散因子密文解密得到第一分散因子RU,之后即可使用第一分散因子RU和本密码模组已存储的PIN转换参数衍生出一级根密钥。

[0088] 至于目标密码模组如何基于第一分散因子RU和本密码模组已存储的PIN转换参数衍生出一级根密钥,其有很多方式,比如,通过下式实现:

[0089] RootKey= SM3(PIN’异或RU)。其中,RootKey表示一级根密钥,SM3表示SM3哈希算法,PIN’表示PIN转换参数。

[0090] 步骤402,任一密码模组,在不为上述模组管理单元选取的目标密码模组时,假如被分配的安全等级大于预设等级,则在上述目标密码模组衍生出一级根密钥后,在模组管理单元的控制下,基于上述第一分散因子RU和本密码模组已存储的上述PIN转换参数衍生出一级根密钥。

[0091] 如前描述,上述目标密码模组衍生出一级根密钥后,会将第一分散因子RU上送给上述模组管理单元,当模组管理单元接收到第一分散因子RU后,会将第一分散因子RU下发给其它密码模组,以由其它密码模组基于第一分散因子RU和其它密码模组已存储的上述PIN转换参数衍生出一级根密钥。最终实现了未被选取为目标密码模组的其他任一密码模组,在模组管理单元的控制下,基于上述第一分散因子RU和已存储的上述PIN转换参数衍生出一级根密钥。

[0092] 步骤403,任一密码模组,在被分配敏感业务数据后,基于衍生出的一级根密钥获

得用于对敏感业务数据进行密码运算处理的目标密钥，利用目标密钥对被分配的敏感业务数据进行对应的密码运算处理。

[0093] 需要说明的是，在通过上述图2流程将上述USBKey成功注册至密码设备后，任一密码模组还会继续按照上述步骤401至步骤402衍生出一级根密钥。并且，任一密码模组还会基于外部指令(比如指示生成N个二级密钥)来生成N个二级密钥。N大于1。任一个二级密钥具有对应的二级密钥索引。当任一密码模组生成二级密钥后，则可采用上述衍生出的一级根密钥对二级密钥进行加密保存。需要说明的是，二级密钥对应的二级密钥索引不需要被加密。

[0094] 在本实施例中，在步骤403之前，当外部有密码运算处理需求时，外部会通过插入USBKey至密码设备来登录密码设备，以通过上述步骤401至步骤402衍生出一级根密钥。之后，外部会输入指定的二级密钥索引。任一密码模组在接收到该二级密钥索引，会基于衍生出的一级根密钥对与上述二级密钥索引对应的二级密钥密文进行解密，得到二级密钥。之后，密码模组随机生成三级密钥(也称会话密钥，具有对应的三级密钥索引)，并利用二级密钥对该三级密钥进行加密得到三级密钥密文。之后输出三级密钥密文和三级密钥索引给外部。后续外部在基于上述密码运算处理需求输出对应的敏感业务数据(比如携带敏感业务数据的报文)给密码设备时，会携带上述二级密钥索引、以及三级密钥密文或三级密钥索引(通称三级索引信息)。

[0095] 应用于本步骤403，利用衍生出的一级根密钥获得用于对敏感业务数据进行密码运算处理的目标密钥有很多方式，比如通过以下步骤a1至步骤a3实现：

[0096] 步骤a1，获得被分配的敏感业务数据在被进行密码运算处理时所需的二级密钥索引和三级密钥信息。

[0097] 作为一个实施例，上述二级密钥索引、三级密钥信息可携带在敏感业务数据所在的报文中，比如，报文中携带二级密钥索引字段、三级密钥信息字段和载荷字段，二级密钥索引字段用于指示上述二级密钥索引，三级密钥信息字段用于携带三级密钥信息，载荷字段，用于携带上述敏感业务数据。作为一个实施例，三级密钥信息可为三级密钥密文或三级密钥索引。

[0098] 步骤a2，基于衍生出的一级根密钥对与二级密钥索引对应的二级密钥密文进行解密，得到二级密钥。

[0099] 步骤a3，若三级密钥信息为与本地已有的三级密钥密文对应的三级密钥索引，则利用二级密钥对三级密钥密文进行解密，得到三级密钥，若三级密钥信息为三级密钥密文，则利用二级密钥对三级密钥密文进行解密，得到三级密钥，将三级密钥确定为目标密钥。

[0100] 最终，实现了如何利用衍生出的一级根密钥获得用于对敏感业务数据进行密码运算处理的目标密钥。

[0101] 在获得利用于对敏感业务数据进行密码运算处理的目标密钥之后，则可进一步基于目标密钥对敏感业务数据进行密码运算处理比如加密或解密等，本实施例并不具体限定。

[0102] 至此，完成图4所示流程。

[0103] 通过图4所示流程实现了通过对密码设备中的密码模组和敏感业务数据进行分级，并动态调整敏感业务数据流向级别匹配的密码模组进行密码运算处理，使得敏感业务

数据在其匹配的密码模组流通，不再流出其匹配的密码模组的安全边界，这避免了现有敏感业务数据在所有密码模组流通所导致的敏感业务数据泄露的问题，保证了敏感业务数据的安全。

[0104] 下面对上述步骤401中描述的如何在模组管理单元的控制下，基于当前登录密码设备的PIN，与USBKey进行身份认证进行描述：

[0105] 参见图5，图5为本申请实施例提供的身份认证流程图。为便于理解，本流程不再站在单侧角度描述。如图5所示，该流程可包括以下步骤：

[0106] 步骤501，模组管理单元基于密码设备的当前登录，从安全等级大于预设等级的所有密码模组中选择一个密码模组作为目标密码模组，向目标密码模组发送身份校验请求。

[0107] 身份校验请求携带当前登录密码设备时输入的登录访问口令PIN。

[0108] 在本实施例中，模组管理单元通过向目标密码模组发送身份校验请求，来触发目标密码模组基于身份校验请求携带的PIN与USBKey进行身份认证，具体见步骤502至步骤505。

[0109] 步骤502，目标密码模组接收上述身份校验请求，按照上述指定PIN转换算法对身份校验请求携带的PIN进行转换得到转换结果，并在转换结果和已存储的PIN转换参数满足设定匹配条件时生成随机数R1并向USBKey发送。

[0110] 如上PIN转换参数的描述，则本实施例中，目标密码模组可基于上述指定PIN转换算法比如SM3算法，对身份校验请求携带的PIN和目标密码模组已存储的上述随机数RC进行转换得到转换结果。

[0111] 在本实施例中，转换结果和已存储的PIN转换参数满足设定匹配条件，比如为转换结果和已存储的PIN转换参数一致，或者转换结果和已存储的PIN转换参数之间的相似度大于设定阈值，等，本实施例并不具体限定。

[0112] 步骤503，USBKey校验当前登录密码设备时输入的PIN，并在该PIN通过校验后对上述随机数R1和已生成的随机数R2进行签名得到第一数字签名，向目标密码模组发送第一数字签名和USBKey数字证书。

[0113] 在本实施例中，USBKey校验当前登录密码设备时输入的PIN比如为：USBKey比较当前登录密码设备时输入的PIN和已存储的PIN，若两者满足设定匹配条件比如一致或者相似度大于设定阈值，则确定当前登录密码设备时输入的PIN通过校验，否则，确定当前登录密码设备时输入的PIN未通过校验。这里，当前登录密码设备时输入的PIN未通过校验，则结束当前流程。

[0114] 作为一个实施例，本步骤503可利用SM2算法对上述随机数R1和已生成的随机数R2进行签名得到第一数字签名。

[0115] 步骤504，目标密码模组接收USBKey发送的述第一数字签名和USBKey数字证书，利用已预置的CA根证书验证USBKey数字证书和第一数字签名是否合法，并在验证合法后基于第一数字签名获得上述随机数R1和随机数R2，对随机数R1和随机数R2进行签名得到第二数字签名；将第二数字签名和密码模组数字证书发给USBKey。

[0116] 在本实施例中，USBKey和安全等级大于上述预设等级的密码模组（也称可信密码模组）会预置可信任的CA根证书。基于此，应用于本步骤504，目标密码模组利用已预置的CA根证书验证USBKey数字证书和第一数字签名是否合法。这里，验证方式类似现有验证方式，

不再赘述。

[0117] 作为一个实施例，本步骤504可利用SM2算法对上述随机数R1和已生成的随机数R2进行签名得到第二数字签名。

[0118] 步骤505，USBKey基于预置的CA根证书验证密码模组数字证书和第二数字签名是否合法，并在验证合法后，确定目标密码模组基于当前登录密码设备的PIN与USBKey完成身份认证。

[0119] 至此，完成图5所示流程。

[0120] 通过图5所示流程实现了目标密码模组基于当前登录密码设备的登录访问口令PIN，与USBKey进行身份认证。

[0121] 需要说明的是，在本实施例中，上述分配各组敏感业务数据至对应的密码模组可包括：针对每一密码模组，将待分配给该密码模组的至少一组敏感业务数据添加数字水印信息并分配给该密码模组；所述数字水印信息被用于敏感业务数据对应的行为溯源和/或行为建模分析，比如敏感数据的源端的标识、密码模组标识、敏感数据的敏感级别、密码模组的安全等级等。

[0122] 通过由模组管理单元将流通至各密码模组的敏感业务数据添加数字水印信息，可实现必要时在密码设备的驱动层进行敏感数据的数字水印溯源，比如将数字水印信息作为信息源输入至已部署的态势感知模块，以进行后续的行为建模分析、异常行为溯源等。

[0123] 另外，在本实施例还公开了敏感数据备份与恢复。这里的敏感数据可指上述的敏感参数、敏感业务数据、CA根证书等重要程度比较高的数据。

[0124] 作为一个实施例，在有敏感数据备份需求时，可先选取安全等级最高的密码模组中需要备份的敏感数据进行数据备份；针对密码模组中的差异性数据，仅备份高于预设等级的密码模组中的数据。恢复过程同理，针对需要恢复的数据，先在安全等级最高的密码模组进行数据恢复，之后由安全等级最高的密码模组作为主模组，利用从模组的密钥公钥对需要恢复的数据进行加密得到密文并发送给从模组，以由从模组利用用于数据同步的密钥私钥对密文进行解密并存储解密得到的需要恢复的数据。

[0125] 以上对本申请实施例提供的方法进行了描述，下面对本申请实施例提供的系统和装置进行描述：

[0126] 如图6所示，本实施例提供的系统包括多个密码设备。任一密码设备包括模组管理单元和至少两个密码模组；任一密码设备中的模组管理单元执行如图3所示方法中的步骤，任一密码设备中的密码模组执行如图4所示方法中的步骤。

[0127] 在本系统中，不同密码设备之间备份敏感业务数据，其中一个密码设备中安全等级最高的密码模组对应的敏感业务数据被备份至另一密码设备中安全等级最高的密码模组，并由另一密码设备中安全等级最高的密码模组作为主模组，利用从模组的密钥公钥对被备份的数据进行加密得到密文并发送给从模组，以由从模组利用用于数据同步的密钥私钥对密文进行解密并存储解密得到的被备份的数据。

[0128] 本身请实施例还提供了密码设备，其中，密码设备包括模组管理单元和至少两个密码模组；任一密码设备包括模组管理单元和至少两个密码模组；任一密码设备中的模组管理单元执行如图3所示方法中的步骤，任一密码设备中的密码模组执行如图4所示方法中的步骤。

[0129] 基于与上述方法同样的申请构思，本申请实施例还提供一种电子设备，该电子设备应用于上述的模组管理单元或密码模组，如图7所示，可包括：处理器和机器可读存储介质；所述机器可读存储介质上存储有若干计算机指令，所述计算机指令被处理器执行时，实现如上应用于模组管理单元或密码模组的方法中的步骤。

[0130] 基于与上述方法同样的申请构思，本申请实施例还提供一种机器可读存储介质，所述机器可读存储介质上存储有若干计算机指令，所述计算机指令被处理器执行时，能够实现本申请上述示例公开的方法。

[0131] 示例性的，上述机器可读存储介质可以是任何电子、磁性、光学或其它物理存储装置，可以包含或存储信息，如可执行指令、数据，等等。例如，机器可读存储介质可以是：RAM(Radom Access Memory，随机存取存储器)、易失存储器、非易失性存储器、闪存、存储驱动器(如硬盘驱动器)、固态硬盘、任何类型的存储盘(如光盘、dvd等)，或者类似的存储介质，或者它们的组合。

[0132] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[0133] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0134] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0135] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可以由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其它可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其它可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0136] 而且，这些计算机程序指令也可以存储在能引导计算机或其它可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或者多个流程和/或方框图一个方框或者多个方框中指定的功能。

[0137] 这些计算机程序指令也可装载到计算机或其它可编程数据处理设备上，使得在计算机或者其它可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其它可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0138] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

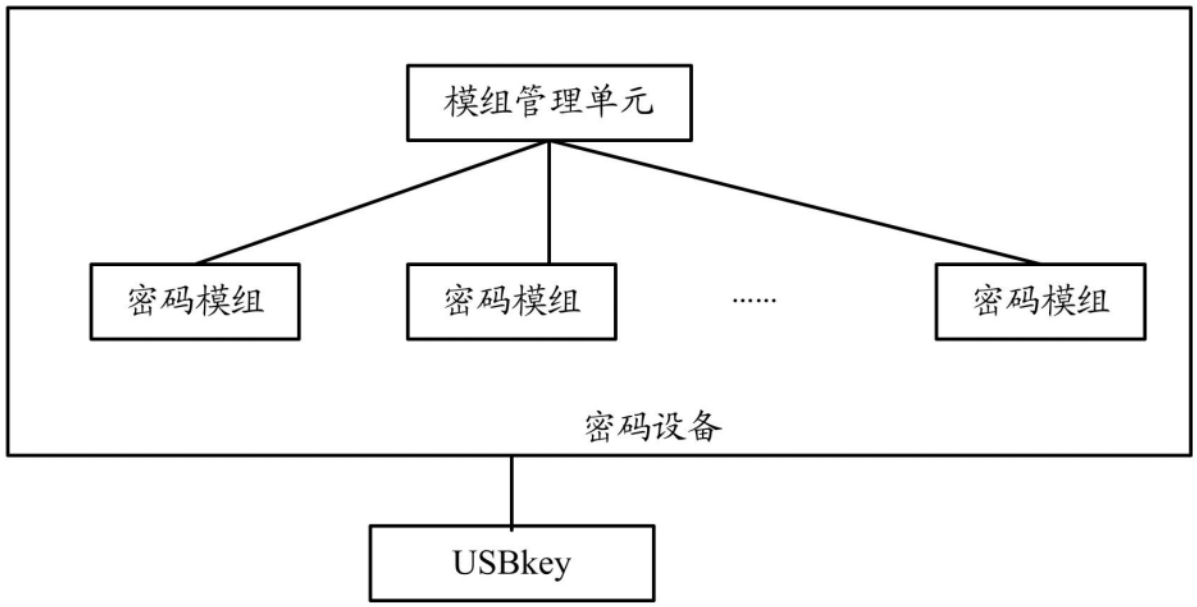

模组管理单元
密码模组
密码模组
……
密码模组
密码设备
USBkey

图 1

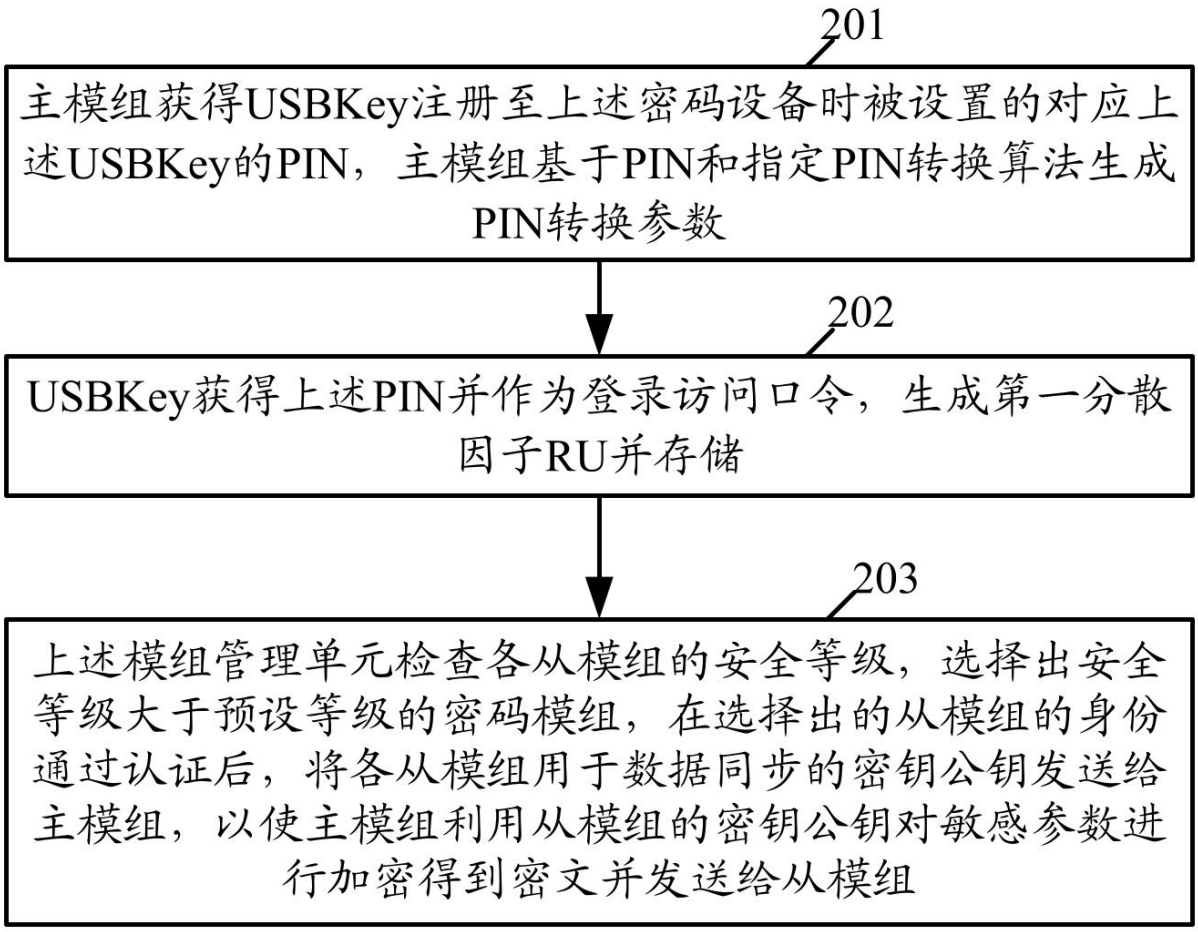

201
主模组获得USBKey注册至上述密码设备时被设置的对应上述USBKey的PIN，主模组基于PIN和指定PIN转换算法生成PIN转换参数
202
USBKey获得上述PIN并作为登录访问口令，生成第一分散因子RU并存储
203
上述模组管理单元检查各从模组的安全等级，选择出安全等级大于预设等级的密码模组，在选择出的从模组的身份通过认证后，将各从模组用于数据同步的密钥公钥发送给主模组，以使主模组利用从模组的密钥公钥对敏感参数进行加密得到密文并发送给从模组

图 2

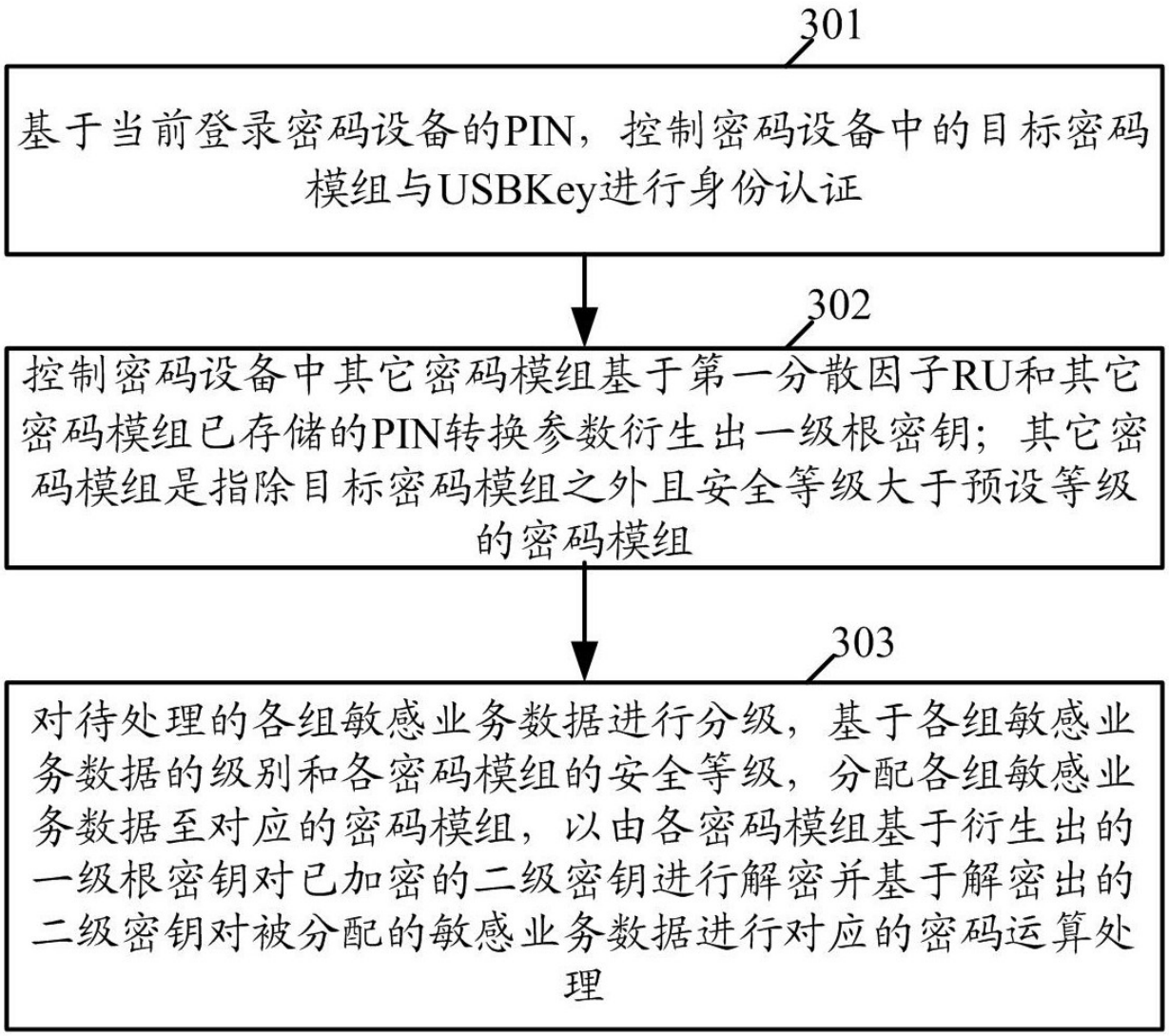

301
基于当前登录密码设备的PIN，控制密码设备中的目标密码模组与USBKey进行身份认证
302
控制密码设备中其它密码模组基于第一分散因子RU和其它密码模组已存储的PIN转换参数衍生出一级根密钥；其它密码模组是指除目标密码模组之外且安全等级大于预设等级的密码模组
303
对待处理的各组敏感业务数据进行分级，基于各组敏感业务数据的级别和各密码模组的安全等级，分配各组敏感业务数据至对应的密码模组，以由各密码模组基于衍生出的一级根密钥对已加密的二级密钥进行解密并基于解密出的二级密钥对被分配的敏感业务数据进行对应的密码运算处理

图 3

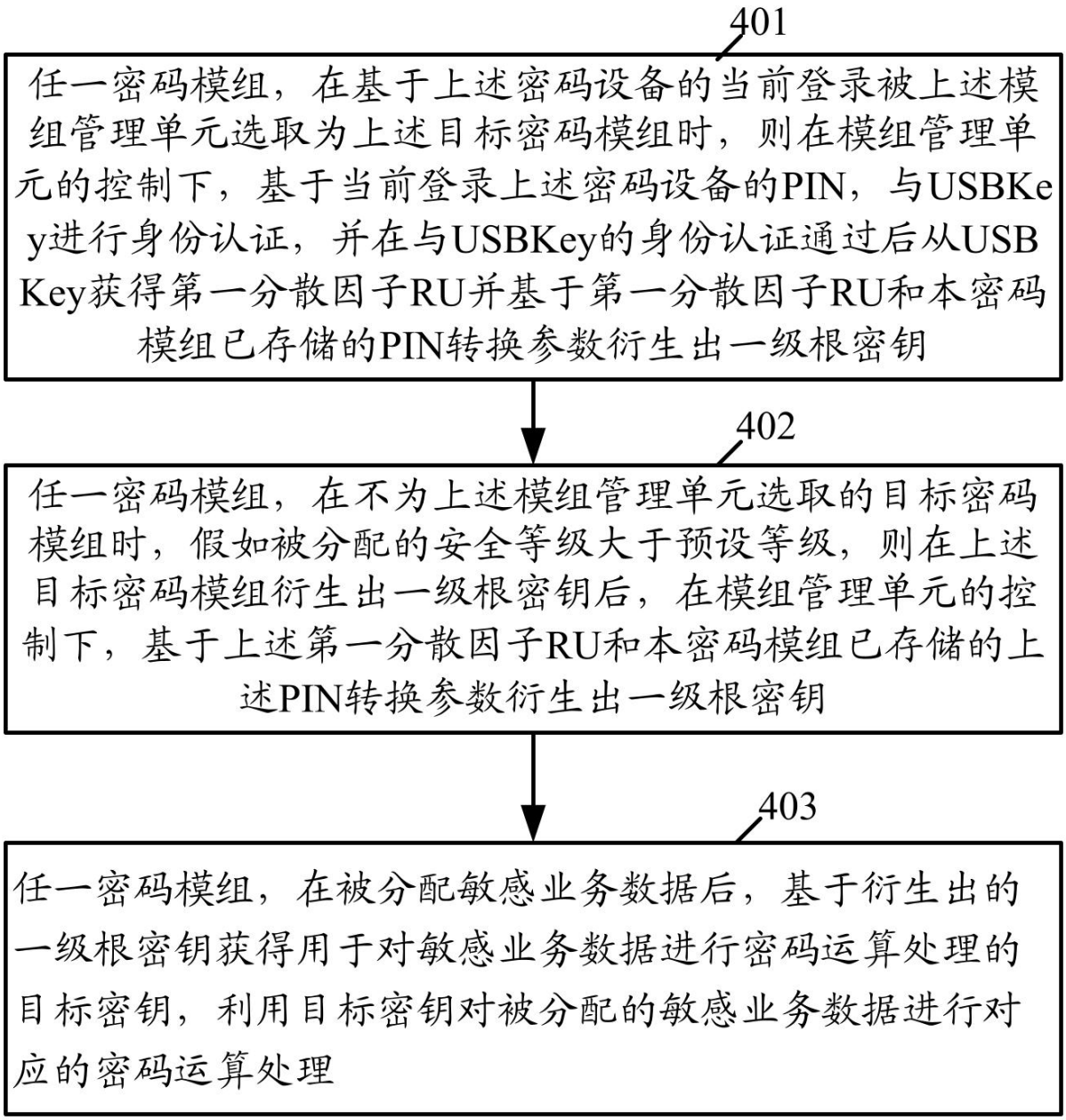

401
任一密码模组，在基于上述密码设备的当前登录被上述模组管理单元选取为上述目标密码模组时，则在模组管理单元的控制下，基于当前登录上述密码设备的PIN，与USBKey进行身份认证，并在与USBKey的身份认证通过后从USBKey获得第一分散因子RU并基于第一分散因子RU和本密码模组已存储的PIN转换参数衍生出一级根密钥
402
任一密码模组，在不为上述模组管理单元选取的目标密码模组时，假如被分配的安全等级大于预设等级，则在上述目标密码模组衍生出一级根密钥后，在模组管理单元的控制下，基于上述第一分散因子RU和本密码模组已存储的上述PIN转换参数衍生出一级根密钥
403
任一密码模组，在被分配敏感业务数据后，基于衍生出的一级根密钥获得用于对敏感业务数据进行密码运算处理的目标密钥，利用目标密钥对被分配的敏感业务数据进行对应的密码运算处理

图 4

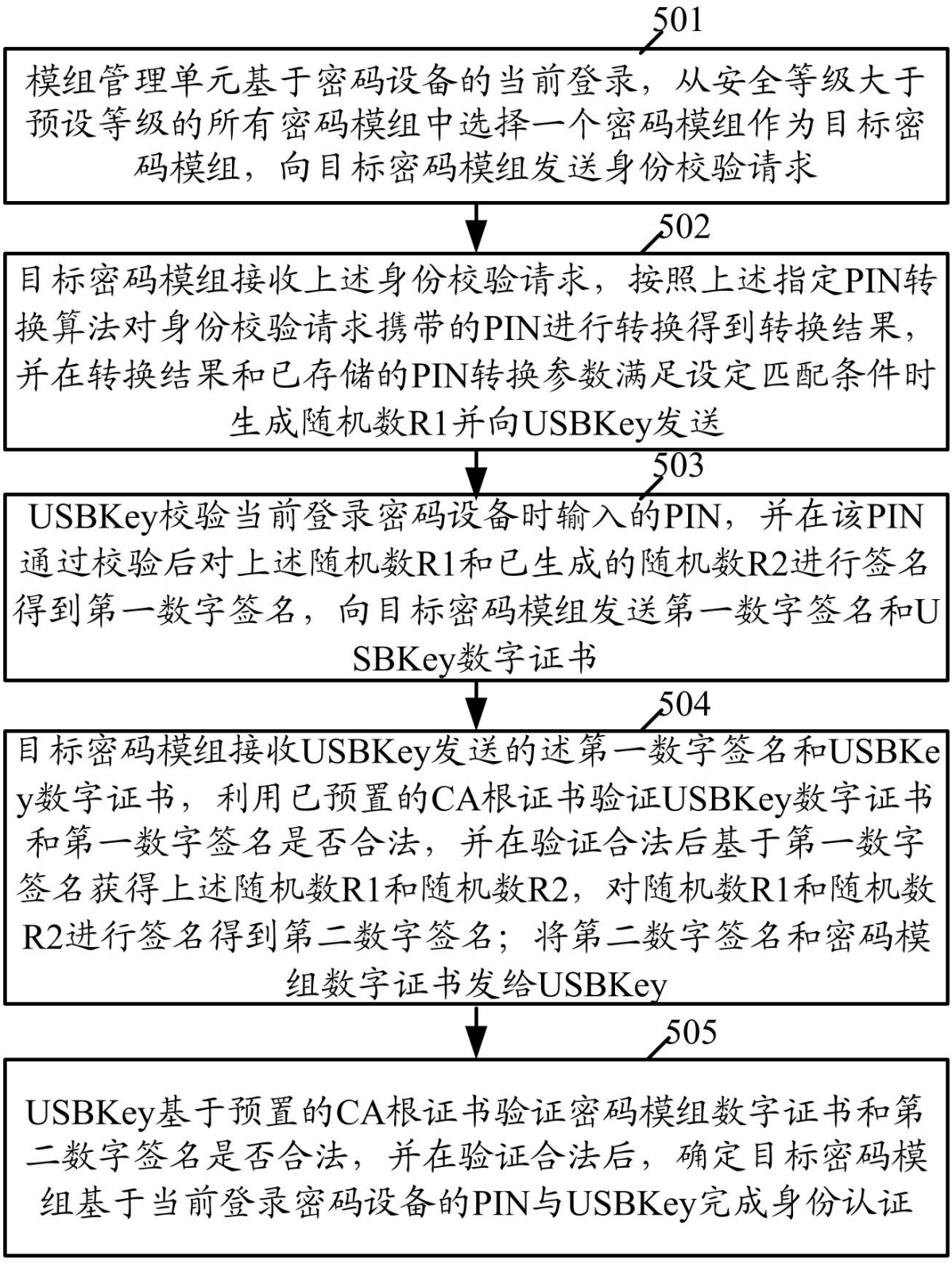

501
模组管理单元基于密码设备的当前登录，从安全等级大于预设等级的所有密码模组中选择一个密码模组作为目标密码模组，向目标密码模组发送身份校验请求
502
目标密码模组接收上述身份校验请求，按照上述指定PIN转换算法对身份校验请求携带的PIN进行转换得到转换结果，并在转换结果和已存储的PIN转换参数满足设定匹配条件时生成随机数R1并向USBKey发送
503
USBKey校验当前登录密码设备时输入的PIN，并在该PIN通过校验后对上述随机数R1和已生成的随机数R2进行签名得到第一数字签名，向目标密码模组发送第一数字签名和USBKey数字证书
504
目标密码模组接收USBKey发送的述第一数字签名和USBKey数字证书，利用已预置的CA根证书验证USBKey数字证书和第一数字签名是否合法，并在验证合法后基于第一数字签名获得上述随机数R1和随机数R2，对随机数R1和随机数R2进行签名得到第二数字签名；将第二数字签名和密码模组数字证书发给USBKey
505
USBKey基于预置的CA根证书验证密码模组数字证书和第二数字签名是否合法，并在验证合法后，确定目标密码模组基于当前登录密码设备的PIN与USBKey完成身份认证

图 5

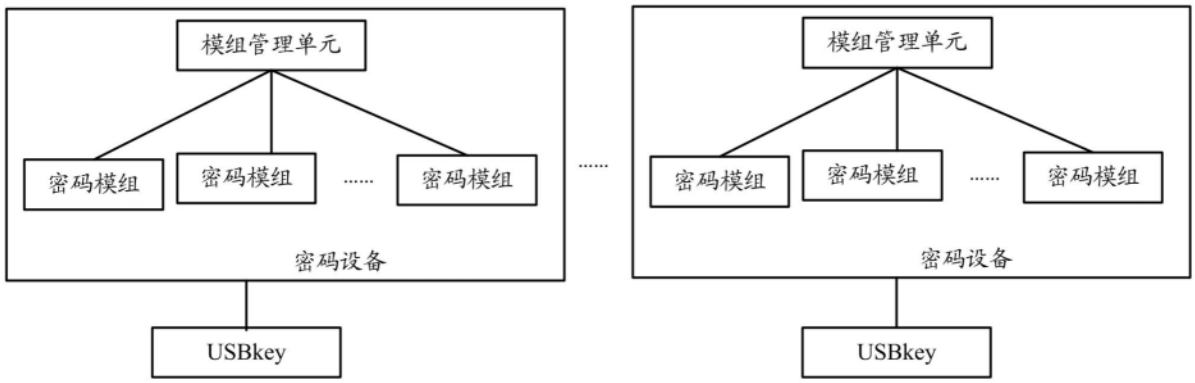

模组管理单元
密码模组
密码模组
.....
密码模组
密码设备
USBkey
.....
模组管理单元
密码模组
密码模组
.....
密码模组
密码设备
USBkey

图 6

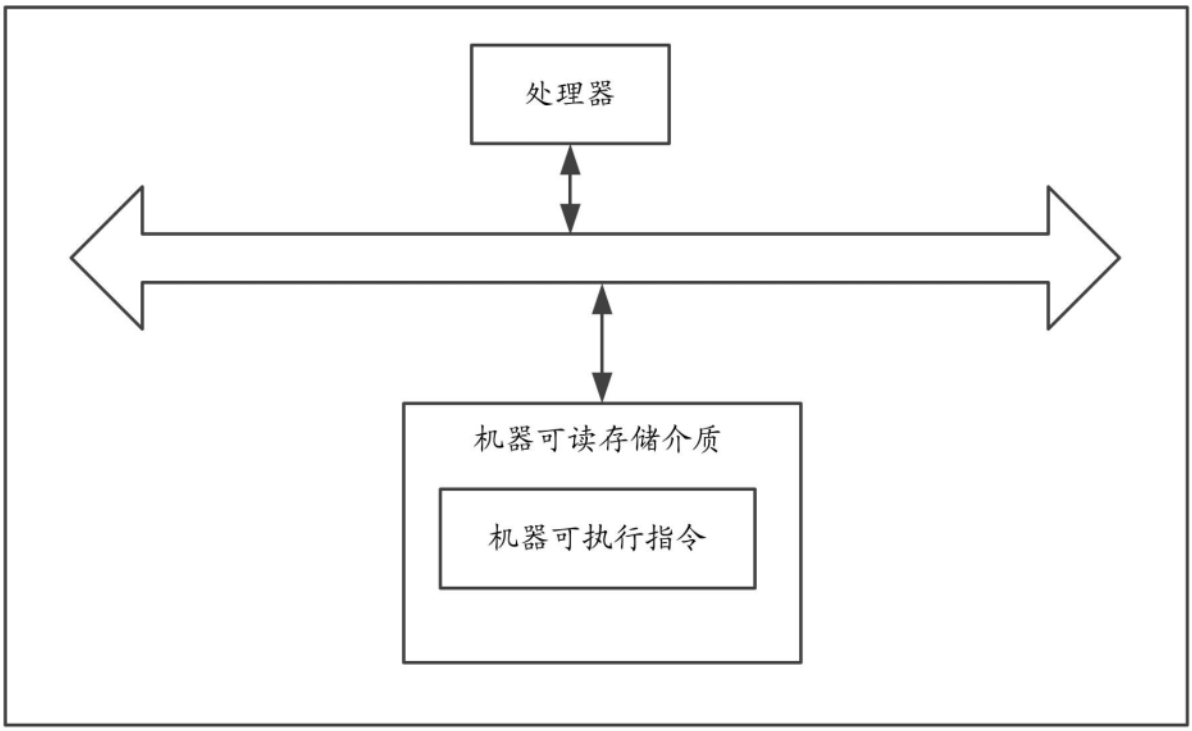

处理器
机器可读存储介质
机器可执行指令

图 7