(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 110190950 B
(45)授权公告日 2021.04.27

(21)申请号 201910503324.X
(22)申请日 2019.06.11
(65)同一申请的已公布的文献号
申请公布号 CN 110190950 A
(43)申请公布日 2019.08.30
(73)专利权人 飞天诚信科技股份有限公司
地址 100085 北京市海淀区学清路9号汇智大厦B楼17层
(72)发明人 陆舟 于华章
(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 106921497 A,2017.07.04
CN 104104505 A,2014.10.15
CN 105553672 A,2016.05.04
US 2010242102 A1,2010.09.23
US 2018152297 A1,2018.05.31
黎艳.《基于用户卡的数字签名技术研究》.《基于用户卡的数字签名技术研究》.2016,全文.

审查员 陈玲珑

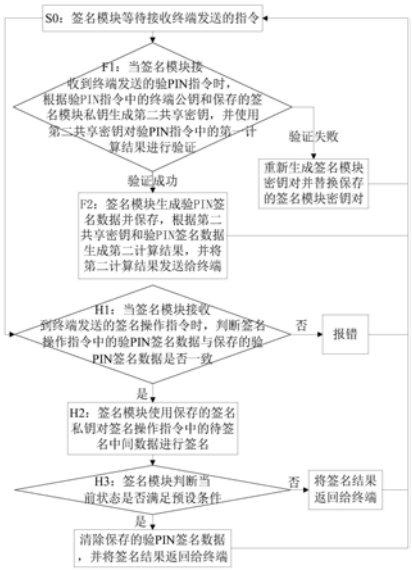
权利要求书11页 说明书29页 附图8页

(54)发明名称

一种安全签名的实现方法及装置

(57)摘要

本发明公开一种安全签名的实现方法及装置，该方法包括：当签名模块接收到验PIN指令时，根据终端公钥和签名模块私钥生成第二共享密钥，根据第二共享密钥对指令中的第一计算结果进行验证，如验证失败则重新生成签名模块密钥对并替换保存的签名模块密钥对；如验证成功则生成验PIN签名数据并保存，根据第二共享密钥和验PIN签名数据生成第二计算结果并发送给终端；当接收到签名操作指令时，判断指令中的验PIN签名数据与保存的验PIN签名数据是否一致，是则使用签名私钥对签名操作指令中的待签名中间数据进行签名；判断当前状态是否满足预设条件，是则清除保存的验PIN签名数据，将签名结果返回给终端，否则将签名结果返回终端。



CN 110190950 B

1.一种安全签名的实现方法,其特征在于,包括:

步骤F1:当签名模块接收到终端发送的验PIN指令时,根据所述验PIN指令中的终端公钥和保存的签名模块私钥生成第二共享密钥,并使用所述第二共享密钥对所述验PIN指令中的第一计算结果进行验证,如验证成功则执行步骤F2;如验证失败则重新生成签名模块密钥对并替换保存的签名模块密钥对;所述签名模块密钥对包括签名模块私钥和签名模块公钥;

步骤F2:所述签名模块生成验PIN签名数据并保存,根据所述第二共享密钥和所述验PIN签名数据生成第二计算结果,并将所述第二计算结果发送给所述终端;

步骤H1:当签名模块接收到终端发送的签名操作指令时,判断所述签名操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致,是则执行步骤H2,否则报错;

步骤H2:所述签名模块使用保存的签名私钥对所述签名操作指令中的待签名中间数据进行签名;

步骤H3:所述签名模块判断当前状态是否满足预设条件,是则清除保存的所述验PIN签名数据,并将签名结果返回给所述终端,否则将签名结果返回所述终端;

所述步骤F2还包括:将签名次数设为初始值;

所述签名模块判断当前状态是否满足预设条件,包括:更新所述签名次数,并判断所述签名次数是否等于预设值,是则满足预设条件,否则不满足预设条件,

或,所述步骤F2还包括:设置签名有效时间;

所述签名模块判断当前状态是否满足预设条件,包括:判断当前时间是否在签名有效时间内,是则不满足预设条件,否则满足预设条件。

2.如权利要求1所述的方法,其特征在于,所述根据所述第二共享密钥对所述验PIN指令中的第一计算结果进行验证之前包括:

所述签名模块解析接收到的验PIN指令,并判断是否解析成功,是则继续,否则报错;

所述步骤H1中的判断所述签名操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致之前,还包括:所述签名模块解析接收到的签名操作指令,并判断是否解析成功,是则继续,否则报错。

3.如权利要求1所述的方法,其特征在于,所述使用所述第二共享密钥对所述验PIN指令中的第一计算结果进行验证,包括:

所述签名模块使用生成的第二共享密钥对所述验PIN指令中的第一计算结果进行解密运算得到第二结果数据,获取内部保存的PIN码转换成第二字节流数据,对所述第二字节流数据进行哈希运算并提取哈希结果中的前16字节数据作为提取数据,判断提取数据是否与所述第二结果数据一致,是则验证成功,否则验证失败。

4.如权利要求1所述的方法,其特征在于,所述根据所述验PIN指令中的终端公钥和保存的签名模块私钥生成第二共享密钥,包括:所述签名模块将所述验PIN指令中的终端公钥与保存的签名模块私钥进行计算得到第一计算值,对所述第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥。

5.如权利要求1所述的方法,其特征在于,所述根据生成的第二共享密钥对所述验PIN指令中的第一计算结果进行验证之前包括:所述签名模块判断PIN码重试次数是否为预定数据,是则报错,提示PIN码锁定;否则继续;

所述步骤F1中验证失败时还包括：

步骤C1:所述签名模块更新所述PIN码重试次数；

步骤C2:所述签名模块判断所述PIN码重试次数是否为预定数据,是则提示PIN码锁定,否则执行步骤C3；

步骤C3:所述签名模块判断验证PIN码是否连续三次出错,是则提示PIN码认证报文错误,否则提示输入PIN码错误；

所述步骤F2还包括:将所述PIN码重试次数改为初始值。

6.如权利要求1所述的方法,其特征在于,所述根据所述第二共享密钥和所述验PIN签名数据生成第二计算结果,并将所述第二计算结果发送给所述终端包括:使用第二共享密钥对验PIN签名数据进行加密得到密文数据,并将所述密文数据发送给所述终端。

7.如权利要求1所述的方法,其特征在于,所述步骤H1和H2替换为：

步骤P1:当签名模块接收到所述终端发送的设置安全环境操作指令时,判断所述设置安全环境操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致,是则执行步骤P2,否则结束；

步骤P2:所述签名模块根据所述设置安全环境指令中的算法ID和密钥容器ID判断设置签名算法是否合法,是则执行步骤P3,否则结束；

步骤P3:所述签名模块根据所述密钥容器ID打开对应的密钥容器,根据所述算法ID设置对应的算法,并给所述终端返回成功设置安全环境响应；

步骤T1:当签名模块接收到所述终端发送的哈希操作指令时,判断所述哈希操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致,是则执行步骤T2,否则结束；

步骤T2:所述签名模块对所述哈希操作指令进行解析得到待签名数据并保存；

步骤T3:所述签名模块根据设置的算法对所述待签名数据进行哈希运算得到哈希值并保存,给所述终端返回哈希计算成功响应；

步骤Q1:当签名模块接收到终端发送的签名操作指令时,判断所述签名操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致,是则执行步骤Q2,否则结束；

步骤Q2:所述签名模块从保存的待签名数据中提取关键信息并判断是否提取成功,是则执行步骤Q3,否则结束；

步骤Q3:所述签名模块显示所述关键信息并判断是否接收到用户确认信息,是则所述签名模块使用与所述签名操作指令中的容器ID所对应的容器中的签名私钥对保存的哈希值进行签名得到签名结果并保存,否则结束；

步骤Q4:所述签名模块判断当前状态是否满足预设条件,是则清除保存的所述验PIN签名数据,并给所述终端返回签名成功信息,否则给所述终端返回签名失败信息；

步骤L1:当签名模块接收到终端发送的获取签名结果指令时,将签名结果返回给终端。

8.如权利要求7所述的方法,其特征在于,所述步骤P2包括：

步骤P21:所述签名模块根据所述密钥容器ID判断对应的密钥容器是否存在,是则执行步骤P22,否则结束；

步骤P22:所述签名模块根据所述算法ID判断是否支持对应的算法,是则执行步骤P3,否则结束。

9.如权利要求7所述的方法,其特征在于,所述步骤T3还包括:所述签名模块给所述终

端返回所述哈希值。

10.如权利要求1或7所述的方法，其特征在于，所述步骤F2还包括：将验PIN签名标识设为有效；

所述步骤H1、步骤P1、步骤T1、步骤Q1中还包括：所述签名模块判断所述验PIN签名标识是否有效，是则继续，否则报错；

所述步骤H3中判断为是时还包括：将所述验PIN签名标识设为无效。

11.如权利要求10所述的方法，其特征在于，所述将所述验PIN签名标识设为有效，具体为：将验PIN签名标识置位；

所述判断所述验PIN签名标识是否有效，具体为：判断所述验PIN签名标识是否置位；

所述将所述验PIN签名标识设为无效，具体为：将所述验PIN签名标识复位。

12.如权利要求1所述的方法，其特征在于，还包括：

当签名模块接收到设置PIN码指令时，所述签名模块判断PIN码是否已设置，是则报错，否则对所述设置PIN码指令进行验证，如验证成功则根据所述设置PIN码指令中的第一密文生成PIN码并保存，如验证失败则结束。

13.如权利要求12所述的方法，其特征在于，所述签名模块对所述设置PIN码指令进行验证，包括：

步骤M1：所述签名模块将保存的签名模块私钥与所述设置PIN码指令中的终端公钥进行计算得到第一计算值，对第一计算值进行哈希运算，将哈希结果作为第二共享密钥；

步骤M2：所述签名模块使用所述第二共享密钥、对所述设置PIN码指令中的第一密文进行HMAC运算得到第二运算结果，并提取第二运算结果中的前16个字节数据得到提取数据；

步骤M3：所述签名模块判断所述提取数据是否与所述设置PIN码指令中的第一结果数据一致，是则验证成功，否则验证失败。

14.如权利要求13所述的方法，其特征在于，所述步骤M1之前还包括：

所述签名模块对接收到的所述设置PIN码指令进行解析，并判断是否解析成功，是则执行步骤M1，否则报错。

15.如权利要求13所述的方法，其特征在于，所述根据所述设置PIN码指令中的第一密文生成PIN码并保存，包括：

步骤N1：所述签名模块使用所述第二共享密钥对所述设置PIN码指令中的第一密文进行解密得到第一解密值，去除所述第一解密值中的填充数据得到密码中间值；

步骤N2：所述签名模块判断所述密码中间值是否小于第一预设值，是则报错，否则执行步骤N3；

步骤N3：所述签名模块对所述密码中间值进行哈希运算得到哈希结果，提取哈希结果中的前16个字节数据并保存为PIN码。

16.如权利要求15所述的方法，其特征在于，还包括：

当所述签名模块接收到修改PIN码指令时，对所述修改PIN码指令进行验证，如验证成功则用所述修改PIN码指令中的PIN码替换保存的PIN码，如验证失败则报错。

17.如权利要求16所述的方法，其特征在于，所述对所述修改PIN码指令进行验证，包括：

步骤W1：所述签名模块对保存的签名模块私钥与所述修改PIN码指令中的终端公钥进

行计算得到第一结果数据，对第一结果数据进行哈希运算得到第二共享密钥；将所述修改PIN码指令中的第一加密值和所述修改PIN码指令中的第二加密值进行拼接得到第二拼接结果；

步骤W2：所述签名模块使用第二共享密钥、对第二拼接结果进行HMAC运算得到第二运算结果，并从第二运算结果中提取前16个字节数据得到提取数据；

步骤W3：所述签名模块判断所述修改PIN码指令中的中间数据与所述提取数据是否一致，是则执行步骤W4，否则报错；

步骤W4：所述签名模块使用所述第二共享密钥对所述第一加密值进行解密得到第一解密值；

步骤W5：所述签名模块判断所述第一解密值与内部保存的PIN码是否一致，是则验证成功，否则验证失败，重新生成签名模块密钥对并替换保存的签名模块密钥对。

18.如权利要求17所述的方法，其特征在于，所述用所述修改PIN码指令中的PIN码替换保存的PIN码，包括：

步骤K1：所述签名模块使用所述第二共享密钥对所述第二加密值进行解密得到第二解密值，去除所述第二解密值中的填充数据得到第一中间值；

步骤K2：所述签名模块判断第一中间值的长度是否小于第一预设值，是则报错，否则执行步骤K3；

步骤K3：所述签名模块对所述第一中间值进行哈希运算得到哈希结果，提取所述哈希结果的前16个字节数据并替换所述内部保存的PIN码。

19.如权利要求18所述的方法，其特征在于，所述步骤W1之前还包括：

所述签名模块解析接收到的修改PIN码指令，并判断是否解析成功，是则执行步骤W1，否则报错。

20.如权利要求18所述的方法，其特征在于，所述步骤N3还包括：所述签名模块将PIN码重试次数设为初始值；

所述步骤K3还包括：所述签名模块将所述PIN码重试次数改为初始值；

所述步骤W1之前还包括：所述签名模块判断PIN码重试次数是否为预定数据，是则提示PIN码锁定，否则执行步骤W1；

所述步骤W5中验证失败之后还包括：

步骤W6：所述签名模块更新所述PIN码重试次数；

步骤W7：所述签名模块判断PIN码重试次数是否为预定数据，是则提示PIN码锁定，否则执行步骤W8；

步骤W8：所述签名模块判断验证PIN码是否连续三次出错，是则提示PIN码认证报文错误，否则提示输入PIN码错误。

21.如权利要求15所述的方法，其特征在于，还包括：

当签名模块接收到获取验PIN签名数据指令时，对所述获取验PIN签名数据指令进行验证，如验证成功则生成验PIN签名数据并发送给所述终端，如验证失败则结束。

22.如权利要求21所述的方法，其特征在于，所述对所述获取验PIN签名数据指令进行验证，包括：

步骤R1：所述签名模块将所述获取验PIN签名数据指令中的终端公钥与保存的签名模

块私钥进行计算得到第一计算值，对第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥；

步骤R2：所述签名模块使用第二共享密钥、对所述获取验PIN签名数据指令中的第一计算结果进行解密运算得到第二结果数据，获取内部保存的PIN码，将PIN码转换成字节流数据，对字节流数据进行哈希运算并提取哈希结果中的前16字节数据得到提取数据；

步骤R3：所述签名模块判断所述第二结果数据是否与提取数据相同，是则验证成功，否则验证失败，重新生成签名模块密钥对并替换保存的签名模块密钥对。

23.如权利要求21所述的方法，其特征在于，所述生成验PIN签名数据并发送给所述终端，包括：生成第一随机数作为验PIN签名数据，使用所述第二共享密钥对验PIN签名数据进行加密得到密文数据，并将密文数据返回给终端。

24.如权利要求22所述的方法，其特征在于，所述步骤R1之前还包括：

步骤R0：所述签名模块解析接收到的获取验PIN签名数据指令，并判断是否解析成功，是则执行步骤R1，否则报错。

25.如权利要求22所述的方法，其特征在于，所述步骤N3还包括：所述签名模块将PIN码重试次数设为初始值；

所述步骤R3验证成功时还包括：所述签名模块将所述PIN码重试次数改为初始值；

所述步骤R1之前还包括：所述签名模块判断PIN码重试次数是否为预定数据，是则提示PIN码锁定；否则执行步骤R1；

所述步骤R3判断为否还包括：

步骤R4：所述签名模块更新PIN码重试次数；

步骤R5：所述签名模块判断PIN码重试次数是否为预定数据，是则提示PIN码锁定，否则执行步骤R6；

步骤R6：所述签名模块判断验证PIN码是否连续三次出错，是则提示PIN码认证报文错误，否则提示输入PIN码错误。

26.如权利要求4或13或17或22所述的方法，其特征在于，还包括：

当所述签名模块接收到协商共享密钥指令时，生成签名模块密钥对并保存，将所述签名模块密钥对中的签名模块公钥返回给所述终端。

27.一种安全签名的实现装置，其特征在于，包括签名模块，所述签名模块：

接收子模块，用于接收终端发送的验PIN指令和签名操作指令；

第一生成子模块，用于当所述接收子模块接收到验PIN码指令时，根据所述验PIN指令中的终端公钥和保存的签名模块私钥生成第二共享密钥；

第一验证子模块，用于使用所述第一生成子模块生成的第二共享密钥对所述验PIN指令中的第一计算结果进行验证，如验证成功则触发第三生成子模块；如验证失败则触发第二生成子模块；

所述第二生成子模块，用于重新生成签名模块密钥对并替换保存的签名模块密钥对；所述签名模块密钥对包括签名模块私钥和签名模块公钥；

所述第三生成子模块，用于生成验PIN签名数据并保存；根据所述第一生成子模块生成的第二共享密钥和所述验PIN签名数据生成第二计算结果；

第一判断子模块，用于当所述接收子模块接收到终端发送的签名操作指令时，判断所

述签名操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致，是则触发签名子模块，否则报错；

所述签名子模块，用于使用保存的签名私钥对所述签名操作指令中的待签名中间数据进行签名；

判断清除子模块，用于判断当前状态是否满足预设条件，是则清除保存的所述验PIN签名数据；

发送子模块，用于将所述第三生成子模块生成的第二计算结果发送给所述终端，还用于在所述判断清除子模块判断为是或否时将所述签名子模块得到的签名结果发送给所述终端；

所述第三生成子模块还用于将签名次数设为初始值；

所述判断清除子模块，具体用于更新所述签名次数，并判断所述签名次数是否等于预设值，是则清除保存的所述验PIN签名数据；或

所述第三生成子模块还用于设置签名有效时间；

所述判断清除子模块，具体用于判断当前时间是否在签名有效时间内，是则清除保存的所述验PIN签名数据。

28.如权利要求27所述的装置，其特征在于，所述签名模块还包括：

第一解析子模块，用于解析所述接收子模块接收到的验PIN指令，并判断是否解析成功，是则触发所述第一验证子模块，否则报错；

第二解析子模块，用于解析所述接收子模块接收到的签名操作指令，并判断是否解析成功，是则触发所述第一判断子模块，否则报错。

29.如权利要求27所述的装置，其特征在于，所述第一验证子模块具体用于使用生成的第二共享密钥对所述验PIN指令中的第一计算结果进行解密运算得到第二结果数据，获取内部保存的PIN码转换成第二字节流数据，对所述第二字节流数据进行哈希运算并提取哈希结果中的前16字节数据作为提取数据，判断提取数据是否与所述第二结果数据一致，是则验证成功，触发第三生成子模块；否则验证失败，触发第二生成子模块。

30.如权利要求27所述的装置，其特征在于，所述第一生成子模块具体用于将所述验PIN指令中的终端公钥与保存的签名模块私钥进行计算得到第一计算值，对所述第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥。

31.如权利要求27所述的装置，其特征在于，所述签名模块还包括：

第二判断子模块，用于判断PIN码重试次数是否为预定数据，是则报错，提示PIN码锁定；否则触发所述第一验证子模块；

第一更新子模块，用于在所述第一验证子模块验证失败后更新所述PIN码重试次数；

第三判断子模块，用于判断所述PIN码重试次数是否为预定数据，是则提示PIN码锁定，否则触发第四判断子模块；

所述第四判断子模块，用于判断验证PIN码是否连续三次出错，是则提示PIN码认证报文错误，否则提示输入PIN码错误；

第一修改子模块，用于在所述第一验证子模块验证成功后将所述PIN码重试次数改为初始值。

32.如权利要求27所述的装置，其特征在于，所述第三生成子模块具体用于使用第二共

享密钥对验PIN签名数据进行加密得到密文数据作为第二计算结果。

33.如权利要求27所述的装置,其特征在于,所述接收子模块还用于接收所述终端发送的设置安全环境操作指令、哈希操作指令、获取签名结果指令;

所述签名模块还包括:

第五判断子模块,用于当所述接收子模块接收到所述终端发送的设置安全环境操作指令时,判断所述设置安全环境操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致,是则触发第六判断子模块,否则结束;

所述第六判断子模块,用于根据所述设置安全环境指令中的算法ID和密钥容器ID判断设置签名算法是否合法,是则触发打开设置子模块,否则结束;

所述打开设置子模块,用于根据所述密钥容器ID打开对应的密钥容器,根据所述算法ID设置对应的算法;

第七判断子模块,用于当所述接收子模块接收到所述终端发送的哈希操作指令时,判断所述哈希操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致,是则触发解析保存子模块,否则结束;

所述解析保存子模块,用于对所述哈希操作指令进行解析得到待签名数据并保存;

哈希运算子模块,用于根据设置的算法对所述待签名数据进行哈希运算得到哈希值并保存;

提取判断子模块,用于在所述第一判断子模块判断为是时从保存的待签名数据中提取关键信息并判断是否提取成功,是则触发显示判断子模块,否则结束;

所述显示判断子模块,用于显示所述提取判断子模块提取的关键信息并判断是否接收到用户确认信息,是则触发所述签名子模块,否则结束;

所述签名子模块,具体用于使用与所述签名操作指令中的容器ID所对应的容器中的签名私钥对保存的哈希值进行签名得到签名结果并保存;

所述发送子模块还用于在所述打开设置子模块设置完对应算法之后给所述终端返回成功设置安全环境响应;还用于在哈希运算子模块运算完成之后给所述终端返回哈希计算成功响应;还用于当所述判断清除子模块判断为是时给所述终端返回签名成功信息,当所述判断清除子模块判断为否时给所述终端返回签名失败信息;还用于当所述接收子模块接收到终端发送的获取签名结果指令时,将所述签名保存子模块保存的签名结果返回给终端。

34.如权利要求33所述的装置,其特征在于,所述第六判断子模块具体用于根据所述密钥容器ID判断对应的密钥容器是否存在且根据所述算法ID判断是否支持对应的算法,如判断均为是则触发打开设置子模块,否则结束。

35.如权利要求33所述的装置,其特征在于,所述发送子模块还用于在所述哈希运算子模块运算完成之后给所述终端返回所述哈希值。

36.如权利要求33所述的装置,其特征在于,所述第三生成子模块还用于将验PIN签名标识设为有效;

所述第一判断子模块还用于判断所述验PIN签名标识是否有效;

所述第五判断子模块还用于判断所述验PIN签名标识是否有效;

所述第七判断子模块还用于判断所述验PIN签名标识是否有效;

所述判断清除子模块还用于判断当前状态满足预设条件时将所述验PIN签名标识设为无效。

37.如权利要求36所述的装置,其特征在于,所述第三生成子模块还用于将验PIN签名标识设为有效,具体为:所述第三生成子模块还用于将验PIN签名标识置位;

所述第一判断子模块还用于判断所述验PIN签名标识是否有效,具体为:所述第一判断子模块还用于判断所述验PIN签名标识是否置位;

所述第五判断子模块还用于判断所述验PIN签名标识是否有效,具体为:所述第五判断子模块还用于判断所述验PIN签名标识是否置位;

所述第七判断子模块还用于判断所述验PIN签名标识是否有效,具体为:所述第七判断子模块还用于判断所述验PIN签名标识是否置位;

所述判断清除子模块还用于判断当前状态满足预设条件时将所述验PIN签名标识设为无效,具体为:所述判断清除子模块还用于判断当前状态满足预设条件时将所述验PIN签名标识复位。

38.如权利要求27所述的装置,其特征在于,所述接收子模块还用于接收设置PIN码指令;

所述签名模块还包括:

第八判断子模块,用于当所述接收子模块接收到设置PIN码指令时,判断PIN码是否已设置,是则报错,否则触发第二验证子模块;

所述第二验证子模块,用于对所述设置PIN码指令进行验证,如验证成功则根据所述设置PIN码指令中的第一密文生成PIN码并保存,如验证失败则结束。

39.如权利要求38所述的装置,其特征在于,所述第二验证子模块具体包括:

计算哈希单元,用于将保存的签名模块私钥与所述设置PIN码指令中的终端公钥进行计算得到第一计算值,对第一计算值进行哈希运算,将哈希结果作为第二共享密钥;

第一运算提取单元,用于使用所述第二共享密钥、对所述设置PIN码指令中的第一密文进行HMAC运算得到第二运算结果,并提取第二运算结果中的前16个字节数据得到提取数据;

第一判断单元,用于判断所述提取数据是否与所述设置PIN码指令中的第一结果数据一致,是则触发生成保存单元,否则结束;

所述生成保存单元,用于根据所述设置PIN码指令中的第一密文生成PIN码并保存。

40.如权利要求39所述的装置,其特征在于,所述第二验证子模块还包括:

第一解析判断单元,用于对接收到的所述设置PIN码指令进行解析,并判断是否解析成功,是则触发所述计算哈希单元,否则报错。

41.如权利要求39所述的装置,其特征在于,所述生成保存单元具体包括:

解密去除子单元,用于使用所述第二共享密钥对所述设置PIN码指令中的第一密文进行解密得到第一解密值,去除所述第一解密值中的填充数据得到密码中间值;

第一判断子单元,用于判断所述密码中间值是否小于第一预设值,是则报错,否则触发哈希提取子单元;

所述哈希提取子单元,用于对所述密码中间值进行哈希运算得到哈希结果,提取哈希结果中的前16个字节数据并保存为PIN码。

42.如权利要求41所述的装置,其特征在于,所述接收子模块还用于接收修改PIN码指令;

所述签名模块还包括:

第三验证子模块,用于当所述接收子模块接收到修改PIN码指令时,对所述修改PIN码指令进行验证,如验证成功则触发替换保存子模块,如验证失败则报错;

所述替换保存子模块,用于用所述修改PIN码指令中的PIN码替换保存的PIN码。

43.如权利要求42所述的装置,其特征在于,所述第三验证子模块具体包括:

计算拼接单元,用于对保存的签名模块私钥与所述修改PIN码指令中的终端公钥进行计算得到第一结果数据,对第一结果数据进行哈希运算得到第二共享密钥;将所述修改PIN码指令中的第一加密值和所述修改PIN码指令中的第二加密值进行拼接得到第二拼接结果;

第二运算提取单元,用于使用第二共享密钥、对第二拼接结果进行HMAC运算得到第二运算结果,并从第二运算结果中提取前16个字节数据得到提取数据;

第二判断单元,用于判断所述修改PIN码指令中的中间数据与所述提取数据是否一致,是则触发第一解密单元,否则报错;

所述第一解密单元,用于使用所述第二共享密钥对所述第一加密值进行解密得到第一解密值;

第三判断单元,用于判断所述第一解密值与内部保存的PIN码是否一致,是则触发替换保存子模块,否则报错,重新生成签名模块密钥对并替换保存的签名模块密钥对。

44.如权利要求43所述的装置,其特征在于,所述替换保存子模块具体包括:

解密去除单元,用于使用所述第二共享密钥对所述第二加密值进行解密得到第二解密值,去除所述第二解密值中的填充数据得到第一中间值;

第四判断单元,用于判断第一中间值的长度是否小于第一预设值,是则报错,否则触发哈希替换单元;

所述哈希替换单元,用于对所述第一中间值进行哈希运算得到哈希结果,提取所述哈希结果的前16个字节数据并替换所述内部保存的PIN码。

45.如权利要求44所述的装置,其特征在于,所述第三验证子模块还包括:

第二解析判断单元,用于解析接收到的修改PIN码指令,并判断是否解析成功,是则触发所述计算拼接单元,否则报错。

46.如权利要求44所述的装置,其特征在于,所述哈希提取子单元还用于将PIN码重试次数设为初始值;

所述哈希替换单元还用于将所述PIN码重试次数改为初始值;

所述第三验证子模块还包括:

第五判断单元,用于判断PIN码重试次数是否为预定数据,是则提示PIN码锁定,否则触发所述计算拼接单元;

第一更新判断单元,用于当第三判断单元判断为否时,更新所述PIN码重试次数;判断PIN码重试次数是否为预定数据,是则提示PIN码锁定,否则触发第六判断单元;

所述第六判断单元,用于判断验证PIN码是否连续三次出错,是则提示PIN码认证报文错误,否则提示输入PIN码错误。

47.如权利要求27所述的装置，其特征在于，所述接收子模块还用于接收获取验PIN签名数据指令；

所述签名模块还包括：

第四验证子模块，用于当所述接收子模块接收到获取验PIN签名数据指令时，对所述获取验PIN签名数据指令进行验证，如验证成功则触发第四生成子模块，如验证失败则结束；

所述第四生成子模块，用于生成验PIN签名数据；

所述发送子模块，还用于将所述第四验证子模块生成的验PIN签名数据发送给所述终端。

48.如权利要求47所述的装置，其特征在于，所述第四验证子模块具体包括：

计算哈希单元，用于将所述获取验PIN签名数据指令中的终端公钥与保存的签名模块私钥进行计算得到第一计算值，对第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥；

解密提取单元，用于使用第二共享密钥、对所述获取验PIN签名数据指令中的第一计算结果进行解密运算得到第二结果数据，获取内部保存的PIN码，将PIN码转换成字节流数据，对字节流数据进行哈希运算并提取哈希结果中的前16字节数据得到提取数据；

第七判断单元，用于判断所述第二结果数据是否与提取数据相同，是则验证成功，触发第四生成子模块，否则验证失败，重新生成签名模块密钥对并替换保存的签名模块密钥对。

49.如权利要求47所述的装置，其特征在于，所述第四生成子模块具体用于生成第一随机数作为验PIN签名数据，使用所述第二共享密钥对验PIN签名数据进行加密得到密文数据；

所述发送子模块，还用于将所述第四验证子模块生成的验PIN签名数据发送给所述终端，具体为：所述发送子模块，还用于将所述第四验证子模块生成的密文数据返回给终端。

50.如权利要求48所述的装置，其特征在于，所述第四验证子模块还包括：

第三解析判断单元，用于解析接收到的获取验PIN签名数据指令，并判断是否解析成功，是则触发计算哈希单元，否则报错。

51.如权利要求48所述的装置，其特征在于，所述哈希提取子单元还用于将PIN码重试次数设为初始值；

所述第七判断单元判断为是时还用于将所述PIN码重试次数改为初始值；

所述第四验证子模块还包括：

第八判断单元，还用于判断所述PIN码重试次数是否为预定数据，是则提示PIN码锁定；否则触发所述计算哈希单元；

第二更新判断单元，用于当第七判断单元判断为否时，更新PIN码重试次数；判断PIN码重试次数是否为预定数据，是则提示PIN码锁定，否则触发第九判断单元；

所述第九判断单元，用于判断验证PIN码是否连续三次出错，是则提示PIN码认证报文错误，否则提示输入PIN码错误。

52.如权利要求30或39或43或48所述的装置，其特征在于，所述接收子模块还用于接收终端发送的协商共享密钥指令；

所述签名模块还包括：

第五生成子模块，用于当所述接收子模块接收到协商共享密钥指令时，生成签名模块

密钥对并保存；

所述发送子模块还用于将所述签名模块密钥对中的签名模块公钥返回给所述终端。

53.如权利要求27所述的装置，其特征在于，所述签名模块为硬件设备或计算机程序或硬件设备与计算机程序的组合。

一种安全签名的实现方法及装置

技术领域

[0001] 本发明涉及信息安全领域，尤其涉及一种安全签名的实现方法及装置。

背景技术

[0002] 随着信息安全的发展，智能密钥设备签名模块开始广泛的应用于安全领域，用户使用签名模块(例如智能密钥设备)对传输报文进行签名来保证用户信息的安全性。在现有技术中，首先通过验PIN操作对用户身份的合法性进行确认，确认合法后再对传输报文进行签名操作。由于验PIN操作和签名操作是通过两条彼此独立的指令来实现的，验PIN操作和签名操作无任何数据关联，有可能存在以下问题：验PIN操作之后很久才进行签名操作，在这期间会出现验一次PIN而进行多次签名操作，多次签名操作中可能是合法用户操作也可能是非法用户操作，导致用户信息泄露，而无法保证签名操作的安全性。故亟待提供一种更安全签名方法来保护用户信息的安全性。

发明内容

[0003] 本发明的目的是为了克服现有技术的不足，提供一种安全签名的实现方法及装置。

[0004] 本发明提供了一种安全签名的实现方法，包括：

[0005] 步骤F1：当签名模块接收到终端发送的验PIN指令时，根据所述验PIN指令中的终端公钥和保存的签名模块私钥生成第二共享密钥，并使用所述第二共享密钥对所述验PIN指令中的第一计算结果进行验证，如验证成功则执行步骤F2；如验证失败则重新生成签名模块密钥对并替换保存的签名模块密钥对；所述签名模块密钥对包括签名模块私钥和签名模块公钥；

[0006] 步骤F2：所述签名模块生成验PIN签名数据并保存，根据所述第二共享密钥和所述验PIN签名数据生成第二计算结果，并将所述第二计算结果发送给所述终端；

[0007] 步骤H1：当签名模块接收到终端发送的签名操作指令时，判断所述签名操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致，是则执行步骤H2，否则报错；

[0008] 步骤H2：所述签名模块使用保存的签名私钥对所述签名操作指令中的待签名中间数据进行签名；

[0009] 步骤H3：所述签名模块判断当前状态是否满足预设条件，是则清除保存的所述验PIN签名数据，并将签名结果返回给所述终端，否则将签名结果返回所述终端。

[0010] 进一步地，所述根据所述第二共享密钥对所述验PIN指令中的第一计算结果进行验证之前包括：

[0011] 所述签名模块解析接收到的验PIN指令，并判断是否解析成功，是则继续，否则报错；

[0012] 所述步骤H1中的判断所述签名操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致之前，还包括：所述签名模块解析接收到的签名操作指令，并判断是否解析成

功,是则继续,否则报错。

[0013] 进一步地,所述使用所述第二共享密钥对所述验PIN指令中的第一计算结果进行验证,包括:

[0014] 所述签名模块使用生成的第二共享密钥对所述验PIN指令中的第一计算结果进行解密运算得到第二结果数据,获取内部保存的PIN码转换成第二字节流数据,对所述第二字节流数据进行哈希运算并提取哈希结果中的前16字节数据作为提取数据,判断提取数据是否与所述第二结果数据一致,是则验证成功,否则验证失败。

[0015] 进一步地,所述根据所述验PIN指令中的终端公钥和保存的签名模块私钥生成第二共享密钥,包括:所述签名模块将所述验PIN指令中的终端公钥与保存的签名模块私钥进行计算得到第一计算值,对所述第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥。

[0016] 进一步地,所述根据生成的第二共享密钥对所述验PIN指令中的第一计算结果进行验证之前包括:所述签名模块判断PIN码重试次数是否为预定数据,是则报错,提示PIN码锁定;否则继续;

[0017] 所述步骤F1中验证失败时还包括:

[0018] 步骤C1:所述签名模块更新所述PIN码重试次数;

[0019] 步骤C2:所述签名模块判断所述PIN码重试次数是否为预定数据,是则提示PIN码锁定,否则执行步骤C3;

[0020] 步骤C3:所述签名模块判断验证PIN码是否连续三次出错,是则提示PIN码认证报文错误,否则提示输入PIN码错误;

[0021] 所述步骤F2还包括:将所述PIN码重试次数改为初始值。

[0022] 进一步地,所述根据所述第二共享密钥和所述验PIN签名数据生成第二计算结果,并将所述第二计算结果发送给所述终端包括:使用第二共享密钥对验PIN签名数据进行加密得到密文数据,并将所述密文数据发送给所述终端。

[0023] 进一步地,所述步骤H1和H2替换为:

[0024] 步骤P1:当签名模块接收到所述终端发送的设置安全环境操作指令时,判断所述设置安全环境操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致,是则执行步骤P2,否则结束;

[0025] 步骤P2:所述签名模块根据所述设置安全环境指令中的算法ID和密钥容器ID判断设置签名算法是否合法,是则执行步骤P3,否则结束;

[0026] 步骤P3:所述签名模块根据所述密钥容器ID打开对应的密钥容器,根据所述算法ID设置对应的算法,并给所述终端返回成功设置安全环境响应;

[0027] 步骤T1:当签名模块接收到所述终端发送的哈希操作指令时,判断所述哈希操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致,是则执行步骤T2,否则结束;

[0028] 步骤T2:所述签名模块对所述哈希操作指令进行解析得到待签名数据并保存;

[0029] 步骤T3:所述签名模块根据设置的算法对所述待签名数据进行哈希运算得到哈希值并保存,给所述终端返回哈希计算成功响应;

[0030] 步骤Q1:当签名模块接收到终端发送的签名操作指令时,判断所述签名操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致,是则执行步骤Q2,否则结束;

[0031] 步骤Q2:所述签名模块从保存的待签名数据中提取关键信息并判断是否提取成功,是则执行步骤Q3,否则结束;

[0032] 步骤Q3:所述签名模块显示所述关键信息并判断是否接收到用户确认信息,是则所述签名模块使用与所述签名操作指令中的容器ID所对应的容器中的签名私钥对保存的哈希值进行签名得到签名结果并保存,否则结束;

[0033] 步骤Q4:所述签名模块判断当前状态是否满足预设条件,是则清除保存的所述验PIN签名数据,并给所述终端返回签名成功信息,否则给所述终端返回签名失败信息;

[0034] 步骤L1:当签名模块接收到终端发送的获取签名结果指令时,将签名结果返回给终端。

[0035] 进一步地,所述步骤P2包括:

[0036] 步骤P21:所述签名模块根据所述密钥容器ID判断对应的密钥容器是否存在,是则执行步骤P22,否则结束;

[0037] 步骤P22:所述签名模块根据所述算法ID判断是否支持对应的算法,是则执行步骤P3,否则结束。

[0038] 进一步地,所述步骤T3还包括:所述签名模块给所述终端返回所述哈希值。

[0039] 进一步地,所述步骤F2还包括:将验PIN签名标识设为有效;

[0040] 所述步骤H1、步骤P1、步骤T1、步骤Q1中还包括:所述签名模块判断所述验PIN签名标识是否有效,是则继续,否则报错;

[0041] 所述步骤H3中判断为是时还包括:将所述验PIN签名标识设为无效。

[0042] 进一步地,所述将所述验PIN签名标识设为有效,具体为:将验PIN签名标识置位;

[0043] 所述判断所述验PIN签名标识是否有效,具体为:判断所述验PIN签名标识是否置位;

[0044] 所述将所述验PIN签名标识设为无效,具体为:将所述验PIN签名标识复位。

[0045] 进一步地,所述步骤F2还包括:将签名次数设为初始值;

[0046] 所述签名模块判断当前状态是否满足预设条件,包括:更新所述签名次数,并判断所述签名次数是否等于预设值,是则满足预设条件,否则不满足预设条件。

[0047] 进一步地,所述步骤F2还包括:设置签名有效时间;

[0048] 所述签名模块判断当前状态是否满足预设条件,包括:判断当前时间是否在签名有效时间内,是则不满足预设条件,否则满足预设条件。

[0049] 进一步地,所述方法还包括:

[0050] 当签名模块接收到设置PIN码指令时,所述签名模块判断PIN码是否已设置,是则报错,否则对所述设置PIN码指令进行验证,如验证成功则根据所述设置PIN码指令中的第一密文生成PIN码并保存,如验证失败则结束。

[0051] 进一步地,所述签名模块对所述设置PIN码指令进行验证,包括:

[0052] 步骤M1:所述签名模块将保存的签名模块私钥与所述设置PIN码指令中的终端公钥进行计算得到第一计算值,对第一计算值进行哈希运算,将哈希结果作为第二共享密钥;

[0053] 步骤M2:所述签名模块使用所述第二共享密钥、对所述设置PIN码指令中的第一密文进行HMAC运算得到第二运算结果,并提取第二运算结果中的前16个字节数据得到提取数据;

[0054] 步骤M3:所述签名模块判断所述提取数据是否与所述设置PIN码指令中的第一结果数据一致,是则验证成功,否则验证失败。

[0055] 进一步地,所述步骤M1之前还包括:

[0056] 所述签名模块对接收到的所述设置PIN码指令进行解析,并判断是否解析成功,是则执行步骤M1,否则报错。

[0057] 进一步地,所述根据所述设置PIN码指令中的第一密文生成PIN码并保存,包括:

[0058] 步骤N1:所述签名模块使用所述第二共享密钥对所述设置PIN码指令中的第一密文进行解密得到第一解密值,去除所述第一解密值中的填充数据得到密码中间值;

[0059] 步骤N2:所述签名模块判断所述密码中间值是否小于第一预设值,是则报错,否则执行步骤N3;

[0060] 步骤N3:所述签名模块对所述密码中间值进行哈希运算得到哈希结果,提取哈希结果中的前16个字节数据并保存为PIN码。

[0061] 进一步地,所述方法还包括:

[0062] 当所述签名模块接收到修改PIN码指令时,对所述修改PIN码指令进行验证,如验证成功则用所述修改PIN码指令中的PIN码替换保存的PIN码,如验证失败则报错。

[0063] 进一步地,所述对所述修改PIN码指令进行验证,包括:

[0064] 步骤W1:所述签名模块对保存的签名模块私钥与所述修改PIN码指令中的终端公钥进行计算得到第一结果数据,对第一结果数据进行哈希运算得到第二共享密钥;将所述修改PIN码指令中的第一加密值和所述修改PIN码指令中的第二加密值进行拼接得到第二拼接结果;

[0065] 步骤W2:所述签名模块使用第二共享密钥、对第二拼接结果进行HMAC运算得到第二运算结果,并从第二运算结果中提取前16个字节数据得到提取数据;

[0066] 步骤W3:所述签名模块判断所述修改PIN码指令中的中间数据与所述提取数据是否一致,是则执行步骤W4,否则报错;

[0067] 步骤W4:所述签名模块使用所述第二共享密钥对所述第一加密值进行解密得到第一解密值;

[0068] 步骤W5:所述签名模块判断所述第一解密值与内部保存的PIN码是否一致,是则验证成功,否则验证失败,重新生成签名模块密钥对并替换保存的签名模块密钥对。

[0069] 进一步地,所述用所述修改PIN码指令中的PIN码替换保存的PIN码,包括:

[0070] 步骤K1:所述签名模块使用所述第二共享密钥对所述第二加密值进行解密得到第二解密值,去除所述第二解密值中的填充数据得到第一中间值;

[0071] 步骤K2:所述签名模块判断第一中间值的长度是否小于第一预设值,是则执行步骤K3,否则报错;

[0072] 步骤K3:所述签名模块对所述第一中间值进行哈希运算得到哈希结果,提取所述哈希结果的前16个字节数据并替换所述内部保存的PIN码。

[0073] 进一步地,所述步骤W1之前还包括:

[0074] 所述签名模块解析接收到的修改PIN码指令,并判断是否解析成功,是则执行步骤W1,否则报错。

[0075] 进一步地,所述步骤N3还包括:所述签名模块将PIN码重试次数设为初始值;

[0076] 所述步骤K3还包括:所述签名模块将所述PIN码重试次数改为初始值;

[0077] 所述步骤W1之前还包括:所述签名模块判断PIN码重试次数是否为预定数据,是则提示PIN码锁定,否则执行步骤W1;

[0078] 所述步骤W5中验证失败之后还包括:

[0079] 步骤W6:所述签名模块更新所述PIN码重试次数;

[0080] 步骤W7:所述签名模块判断PIN码重试次数是否为预定数据,是则提示PIN码锁定,否则执行步骤W8;

[0081] 步骤W8:所述签名模块判断验证PIN码是否连续三次出错,是则提示PIN码认证报文错误,否则提示输入PIN码错误。

[0082] 进一步地,所述方法还包括:

[0083] 当签名模块接收到获取验PIN签名数据指令时,对所述获取验PIN签名数据指令进行验证,如验证成功则生成验PIN签名数据并发送给所述终端,如验证失败则结束。

[0084] 进一步地,所述对所述获取验PIN签名数据指令进行验证,包括:

[0085] 步骤R1:所述签名模块将所述获取验PIN签名数据指令中的终端公钥与保存的签名模块私钥进行计算得到第一计算值,对第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥;

[0086] 步骤R2:所述签名模块使用第二共享密钥、对所述获取验PIN签名数据指令中的第一计算结果进行解密运算得到第二结果数据,获取内部保存的PIN码,将PIN码转换成字节流数据,对字节流数据进行哈希运算并提取哈希结果中的前16字节数据得到提取数据;

[0087] 步骤R3:所述签名模块判断所述第二结果数据是否与提取数据相同,是则验证成功,否则验证失败,重新生成签名模块密钥对并替换保存的签名模块密钥对。

[0088] 进一步地,所述生成验PIN签名数据并发送给所述终端,包括:生成第一随机数作为验PIN签名数据,使用所述第二共享密钥对验PIN签名数据进行加密得到密文数据,并将密文数据返回给终端。

[0089] 进一步地,所述步骤R1之前还包括:

[0090] 步骤R0:所述签名模块解析接收到的获取验PIN签名数据指令,并判断是否解析成功,是则执行步骤R1,否则报错。

[0091] 进一步地,所述步骤N3还包括:所述签名模块将PIN码重试次数设为初始值;

[0092] 所述步骤R3验证成功时还包括:所述签名模块将所述PIN码重试次数改为初始值;

[0093] 所述步骤R1之前还包括:所述签名模块判断PIN码重试次数是否为预定数据,是则提示PIN码锁定;否则执行步骤R1;

[0094] 所述步骤R3判断为否还包括:

[0095] 步骤R4:所述签名模块更新PIN码重试次数;

[0096] 步骤R5:所述签名模块判断PIN码重试次数是否为预定数据,是则提示PIN码锁定,否则执行步骤R6;

[0097] 步骤R6:所述签名模块判断验证PIN码是否连续三次出错,是则提示PIN码认证报文错误,否则提示输入PIN码错误。

[0098] 进一步地,所述方法还包括:

[0099] 当所述签名模块接收到协商共享密钥指令时,生成签名模块密钥对并保存,将所

述签名模块密钥对中的签名模块公钥返回给所述终端。

[0100] 本发明又提供了一种安全签名的实现装置，包括签名模块，所述签名模块：

[0101] 接收子模块，用于接收终端发送的验PIN指令和签名操作指令；

[0102] 第一生成子模块，用于当所述接收子模块接收到验PIN码指令时，根据所述验PIN指令中的终端公钥和保存的签名模块私钥生成第二共享密钥；

[0103] 第一验证子模块，用于使用所述第一生成子模块生成的第二共享密钥对所述验PIN指令中的第一计算结果进行验证，如验证成功则触发第三生成子模块；如验证失败则触发第二生成子模块；

[0104] 所述第二生成子模块，用于重新生成签名模块密钥对并替换保存的签名模块密钥对；所述签名模块密钥对包括签名模块私钥和签名模块公钥；

[0105] 所述第三生成子模块，用于生成验PIN签名数据并保存；根据所述第一生成子模块生成的第二共享密钥和所述验PIN签名数据生成第二计算结果；

[0106] 第一判断子模块，用于当所述接收子模块接收到终端发送的签名操作指令时，判断所述签名操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致，是则触发签名子模块，否则报错；

[0107] 所述签名子模块，用于使用保存的签名私钥对所述签名操作指令中的待签名中间数据进行签名；

[0108] 判断清除子模块，用于判断当前状态是否满足预设条件，是则清除保存的所述验PIN签名数据；

[0109] 发送子模块，用于将所述第三生成子模块生成的第二计算结果发送给所述终端，还用于在所述判断清除子模块判断为是或否时将所述签名子模块得到的签名结果发送给所述终端。

[0110] 进一步地，所述签名模块还包括：

[0111] 第一解析子模块，用于解析所述接收子模块接收到的验PIN指令，并判断是否解析成功，是则触发所述第一验证子模块，否则报错；

[0112] 第二解析子模块，用于解析所述接收子模块接收到的签名操作指令，并判断是否解析成功，是则触发所述第一判断子模块，否则报错。

[0113] 进一步地，所述第一验证子模块具体用于使用生成的第二共享密钥对所述验PIN指令中的第一计算结果进行解密运算得到第二结果数据，获取内部保存的PIN码转换成第二字节流数据，对所述第二字节流数据进行哈希运算并提取哈希结果中的前16字节数据作为提取数据，判断提取数据是否与所述第二结果数据一致，是则验证成功，触发第三生成子模块；否则验证失败，触发第二生成子模块。

[0114] 进一步地，所述第一生成子模块具体用于将所述验PIN指令中的终端公钥与保存的签名模块私钥进行计算得到第一计算值，对所述第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥。

[0115] 进一步地，所述签名模块还包括：

[0116] 第二判断子模块，用于判断PIN码重试次数是否为预定数据，是则报错，提示PIN码锁定；否则触发所述第一验证子模块；

[0117] 第一更新子模块，用于在所述第一验证子模块验证失败后更新所述PIN码重试次

数；

[0118] 第三判断子模块，用于判断所述PIN码重试次数是否为预定数据，是则提示PIN码锁定，否则触发第四判断子模块；

[0119] 所述第四判断子模块，用于判断验证PIN码是否连续三次出错，是则提示PIN码认证报文错误，否则提示输入PIN码错误；

[0120] 第一修改子模块，用于在所述第一验证子模块验证成功后将所述PIN码重试次数改为初始值。

[0121] 进一步地，所述第三生成子模块具体用于使用第二共享密钥对验PIN签名数据进行加密得到密文数据作为第二计算结果。

[0122] 进一步地，所述接收子模块还用于接收所述终端发送的设置安全环境操作指令、哈希操作指令、获取签名结果指令；

[0123] 所述签名模块还包括：

[0124] 第五判断子模块，用于当所述接收子模块接收到所述终端发送的设置安全环境操作指令时，判断所述设置安全环境操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致，是则触发第六判断子模块，否则结束；

[0125] 所述第六判断子模块，用于根据所述设置安全环境指令中的算法ID和密钥容器ID判断设置签名算法是否合法，是则触发打开设置子模块，否则结束；

[0126] 所述打开设置子模块，用于根据所述密钥容器ID打开对应的密钥容器，根据所述算法ID设置对应的算法；

[0127] 第七判断子模块，用于当所述接收子模块接收到所述终端发送的哈希操作指令时，判断所述哈希操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致，是则触发解析保存子模块，否则结束；

[0128] 所述解析保存子模块，用于对所述哈希操作指令进行解析得到待签名数据并保存；

[0129] 哈希运算子模块，用于根据设置的算法对所述待签名数据进行哈希运算得到哈希值并保存；

[0130] 所述提取判断子模块，用于在所述第一判断子模块判断为是时从保存的待签名数据中提取关键信息并判断是否提取成功，是则触发显示判断子模块，否则结束；

[0131] 所述显示判断子模块，用于显示所述提取判断子模块提取的关键信息并判断是否接收到用户确认信息，是则触发所述签名子模块，否则结束；

[0132] 所述签名子模块，具体用于使用与所述签名操作指令中的容器ID所对应的容器中的签名私钥对保存的哈希值进行签名得到签名结果并保存；

[0133] 所述发送子模块还用于在所述打开设置子模块设置完对应算法之后给所述终端返回成功设置安全环境响应；还用于在哈希运算子模块运算完成之后给所述终端返回哈希计算成功响应；还用于当所述判断清除子模块判断为是时给所述终端返回签名成功信息，当所述判断清除子模块判断为否时给所述终端返回签名失败信息；还用于当所述接收子模块接收到终端发送的获取签名结果指令时，将所述签名保存子模块保存的签名结果返回给终端。

[0134] 进一步地，所述所述第六判断子模块具体用于根据所述密钥容器ID判断对应的密

钥容器是否存在且根据所述算法ID判断是否支持对应的算法，如判断均为是则触发打开设置子模块，否则结束。

[0135] 进一步地，所述发送子模块还用于在所述哈希运算子模块运算完成之后给所述终端返回所述哈希值。

[0136] 进一步地，所述第三生成子模块还用于将验PIN签名标识设为有效；

[0137] 所述第一判断子模块还用于判断所述验PIN签名标识是否有效；

[0138] 所述第五判断子模块还用于判断所述验PIN签名标识是否有效；

[0139] 所述第七判断子模块还用于判断所述验PIN签名标识是否有效；

[0140] 所述判断清除子模块还用于判断当前状态满足预设条件时将所述验PIN签名标识设为无效。

[0141] 进一步地，所述第三生成子模块还用于将验PIN签名标识设为有效，具体为：所述第三生成子模块还用于将验PIN签名标识置位；

[0142] 所述第一判断子模块还用于判断所述验PIN签名标识是否有效，具体为：所述第一判断子模块还用于判断所述验PIN签名标识是否置位；

[0143] 所述第五判断子模块还用于判断所述验PIN签名标识是否有效，具体为：所述第五判断子模块还用于判断所述验PIN签名标识是否置位；

[0144] 所述第七判断子模块还用于判断所述验PIN签名标识是否有效，具体为：所述第七判断子模块还用于判断所述验PIN签名标识是否置位；

[0145] 所述判断清除子模块还用于判断当前状态满足预设条件时将所述验PIN签名标识设为无效，具体为：所述判断清除子模块还用于判断当前状态满足预设条件时将所述验PIN签名标识复位。

[0146] 进一步地，所述第三生成子模块还用于将签名次数设为初始值；

[0147] 所述判断清除子模块，具体用于更新所述签名次数，并判断所述签名次数是否等于预设值，是则清除保存的所述验PIN签名数据。

[0148] 进一步地，所述第三生成子模块还用于设置签名有效时间；

[0149] 所述判断清除子模块，具体用于判断当前时间是否在签名有效时间内，是则清除保存的所述验PIN签名数据。

[0150] 进一步地，所述接收子模块还用于接收设置PIN码指令；

[0151] 所述签名模块还包括：

[0152] 第八判断子模块，用于当所述接收子模块接收到设置PIN码指令时，判断PIN码是否已设置，是则报错，否则触发第二验证子模块；

[0153] 所述第二验证子模块，用于对所述设置PIN码指令进行验证，如验证成功则根据所述设置PIN码指令中的第一密文生成PIN码并保存，如验证失败则结束。

[0154] 进一步地，所述第二验证子模块具体包括：

[0155] 计算哈希单元，用于将保存的签名模块私钥与所述设置PIN码指令中的终端公钥进行计算得到第一计算值，对第一计算值进行哈希运算，将哈希结果作为第二共享密钥；

[0156] 第一运算提取单元，用于使用所述第二共享密钥、对所述设置PIN码指令中的第一密文进行HMAC运算得到第二运算结果，并提取第二运算结果中的前16个字节数据得到提取数据；

[0157] 第一判断单元，用于判断所述提取数据是否与所述设置PIN码指令中的第一结果数据一致，是则触发生成保存单元，否则结束；

[0158] 所述生成保存单元，用于根据所述设置PIN码指令中的第一密文生成PIN码并保存。

[0159] 进一步地，所述第二验证子模块还包括：

[0160] 第一解析判断单元，用于对接收到的所述设置PIN码指令进行解析，并判断是否解析成功，是则触发所述计算哈希单元，否则报错。

[0161] 进一步地，所述所述生成保存单元具体包括：

[0162] 解密去除子单元，用于使用所述第二共享密钥对所述设置PIN码指令中的第一密文进行解密得到第一解密值，去除所述第一解密值中的填充数据得到密码中间值；

[0163] 第一判断子单元，用于判断所述密码中间值是否小于第一预设值，是则报错，否则触发哈希提取子单元；

[0164] 所述哈希提取子单元，用于对所述密码中间值进行哈希运算得到哈希结果，提取哈希结果中的前16个字节数据并保存为PIN码。

[0165] 进一步地，所述接收子模块还用于接收修改PIN码指令；

[0166] 所述签名模块还包括：

[0167] 第三验证子模块，用于当所述接收子模块接收到修改PIN码指令时，对所述修改PIN码指令进行验证，如验证成功则触发替换保存子模块，如验证失败则报错；

[0168] 所述替换保存子模块，用于用所述修改PIN码指令中的PIN码替换保存的PIN码。

[0169] 进一步地，所述第三验证子模块具体包括：

[0170] 计算拼接单元，用于对保存的签名模块私钥与所述修改PIN码指令中的终端公钥进行计算得到第一结果数据，对第一结果数据进行哈希运算得到第二共享密钥；将所述修改PIN码指令中的第一加密值和所述修改PIN码指令中的第二加密值进行拼接得到第二拼接结果；

[0171] 第二运算提取单元，用于使用第二共享密钥、对第二拼接结果进行HMAC运算得到第二运算结果，并从第二运算结果中提取前16个字节数据得到提取数据；

[0172] 第二判断单元，用于判断所述修改PIN码指令中的中间数据与所述提取数据是否一致，是则触发第一解密单元，否则报错；

[0173] 所述第一解密单元，用于使用所述第二共享密钥对所述第一加密值进行解密得到第一解密值；

[0174] 第三判断单元，用于判断所述第一解密值与内部保存的PIN码是否一致，是则触发替换保存子模块，否则报错，重新生成签名模块密钥对并替换保存的签名模块密钥对。

[0175] 进一步地，所述替换保存子模块具体包括：

[0176] 解密去除单元，用于使用所述第二共享密钥对所述第二加密值进行解密得到第二解密值，去除所述第二解密值中的填充数据得到第一中间值；

[0177] 第四判断单元，用于判断第一中间值的长度是否小于第一预设值，是则触发哈希替换单元，否则报错；

[0178] 所述哈希替换单元，用于对所述第一中间值进行哈希运算得到哈希结果，提取所述哈希结果的前16个字节数据并替换所述内部保存的PIN码。

[0179] 进一步地,所述所述第三验证子模块还包括:

[0180] 第二解析判断单元,用于解析接收到的修改PIN码指令,并判断是否解析成功,是则触发所述计算拼接单元,否则报错。

[0181] 进一步地,所述哈希提取子单元还用于将PIN码重试次数设为初始值;

[0182] 所述哈希替换单元还用于将所述PIN码重试次数改为初始值;

[0183] 所述第三验证子模块还包括:

[0184] 第五判断单元,用于判断PIN码重试次数是否为预定数据,是则提示PIN码锁定,否则触发所述计算拼接单元;

[0185] 第一更新判断单元,用于当第三判断单元判断为否时,更新所述PIN码重试次数;判断PIN码重试次数是否为预定数据,是则提示PIN码锁定,否则触发第六判断单元;

[0186] 所述第六判断单元,用于判断验证PIN码是否连续三次出错,是则提示PIN码认证报文错误,否则提示输入PIN码错误。

[0187] 进一步地,所述接收子模块还用于接收获取验PIN签名数据指令;

[0188] 所述签名模块还包括:

[0189] 第四验证子模块,用于当所述接收子模块接收到获取验PIN签名数据指令时,对所述获取验PIN签名数据指令进行验证,如验证成功则触发第四生成子模块,如验证失败则结束;

[0190] 所述第四生成子模块,用于生成验PIN签名数据;

[0191] 所述发送子模块,还用于将所述第四验证子模块生成的验PIN签名数据发送给所述终端。

[0192] 进一步地,所述第四验证子模块具体包括:

[0193] 计算哈希单元,用于将所述获取验PIN签名数据指令中的终端公钥与保存的签名模块私钥进行计算得到第一计算值,对第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥;

[0194] 解密提取单元,用于使用第二共享密钥、对所述获取验PIN签名数据指令中的第一计算结果进行解密运算得到第二结果数据,获取内部保存的PIN码,将PIN码转换成字节流数据,对字节流数据进行哈希运算并提取哈希结果中的前16字节数据得到提取数据;

[0195] 第七判断单元,用于判断所述第二结果数据是否与提取数据相同,是则验证成功,触发第四生成子模块,否则验证失败,重新生成签名模块密钥对并替换保存的签名模块密钥对。

[0196] 进一步地,所述第四生成子模块具体用于生成第一随机数作为验PIN签名数据,使用所述第二共享密钥对验PIN签名数据进行加密得到密文数据;

[0197] 所述发送子模块,还用于将所述第四验证子模块生成的验PIN签名数据发送给所述终端,具体为:所述发送子模块,还用于将所述第四验证子模块生成的密文数据返回给终端。

[0198] 进一步地,所述第四验证子模块还包括:

[0199] 第三解析判断单元,用于解析接收到的获取验PIN签名数据指令,并判断是否解析成功,是则触发计算哈希单元,否则报错。

[0200] 进一步地,所述哈希提取子单元还用于将PIN码重试次数设为初始值;

[0201] 所述第七判断单元判断为是时还用于将所述PIN码重试次数改为初始值；

[0202] 所述第四验证子模块还包括：

[0203] 第八判断单元，还用于判断所述PIN码重试次数是否为预定数据，是则提示PIN码锁定；否则触发所述计算哈希单元；

[0204] 第二更新判断单元，用于当第七判断单元判断为否时，更新PIN码重试次数；判断PIN码重试次数是否为预定数据，是则提示PIN码锁定，否则触发第九判断单元；

[0205] 所述第九判断单元，用于判断验证PIN码是否连续三次出错，是则提示PIN码认证报文错误，否则提示输入PIN码错误。

[0206] 进一步地，所述接收子模块还用于接收终端发送的协商共享密钥指令；

[0207] 所述签名模块还包括：

[0208] 第五生成子模块，用于当所述接收子模块接收到协商共享密钥指令时，生成签名模块密钥对并保存；

[0209] 所述发送子模块还用于将所述签名模块密钥对中的签名模块公钥返回给所述终端。

[0210] 进一步地，所述签名模块为硬件设备或计算机程序或硬件设备与计算机程序的组合。

[0211] 本发明与现有技术相比，具有以下优点：

[0212] 在本发明技术方案通过验PIN签名数据将验PIN码操作与签名操作进行关联，保证签名安全性；且验PIN操作失败后更新签名模块密钥对使得下次验PIN操作与本次验PIN操作的共享第二密钥不同，进一步提高签名安全性。

附图说明

[0213] 图1为本发明实施例一提供的一种安全签名的实现方法流程图；

[0214] 图2为本发明实施例二提供的一种设置PIN码的方法流程图；

[0215] 图3为本发明实施例三提供的一种修改PIN码的方法流程图；

[0216] 图4为本发明实施例四提供的一种获取验PIN签名数据的方法流程图；

[0217] 图5为本发明实施例五提供的一种安全签名的实现方法流程图；

[0218] 图6和图7为本发明实施例六提供的一种安全签名的实现方法流程图；

[0219] 图8为本发明实施例七提供的一种安全签名的实现装置方框图。

具体实施方式

[0220] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0221] 本发明具体实施例方式中的签名模块可以为为硬件设备或计算机程序或硬件设备与计算机程序的组合，只要是能实现的该技术方案的软件、硬件均包括在内。

[0222] 实施例一

[0223] 本发明实施例一提供一种安全签名的实现方法，如图1所示，包括：

[0224] 步骤S0:签名模块等待接收终端发送的指令;

[0225] 步骤F1:当签名模块接收到终端发送的验PIN指令时,根据验PIN指令中的终端公钥和保存的签名模块私钥生成第二共享密钥,并使用第二共享密钥对验PIN指令中的第一计算结果进行验证,如验证成功则执行步骤F2;如验证失败则重新生成签名模块密钥对并替换保存的签名模块密钥对,返回步骤S0;签名模块密钥对包括签名模块私钥和签名模块公钥;

[0226] 可选的,在本实施例中,根据第二共享密钥对验PIN指令中的第一计算结果进行验证之前包括:签名模块解析接收到的验PIN指令,并判断是否解析成功,是则继续,否则报错。

[0227] 具体的,在本实施例中,使用第二共享密钥对验PIN指令中的第一计算结果进行验证,包括:

[0228] 签名模块使用生成的第二共享密钥对验PIN指令中的第一计算结果进行解密运算得到第二结果数据,获取内部保存的PIN码转换成第二字节流数据,对第二字节流数据进行哈希运算并提取哈希结果中的前16字节数据作为提取数据,判断提取数据是否与第二结果数据一致,是则验证成功,否则验证失败。

[0229] 具体的,在本实施例中,根据验PIN指令中的终端公钥和保存的签名模块私钥生成第二共享密钥,包括:签名模块将验PIN指令中的终端公钥与保存的签名模块私钥进行计算得到第一计算值,对第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥。

[0230] 具体的,在本实施例中,根据第二共享密钥和验PIN签名数据生成第二计算结果,并将第二计算结果发送给终端包括:使用第二共享密钥对验PIN签名数据进行加密得到密文数据,并将密文数据发送给终端。

[0231] 步骤F2:签名模块生成验PIN签名数据并保存,根据第二共享密钥和验PIN签名数据生成第二计算结果,并将第二计算结果发送给终端,返回步骤S0;

[0232] 步骤H1:当签名模块接收到终端发送的签名操作指令时,判断签名操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致,是则执行步骤H2,否则报错,返回步骤S0;

[0233] 在本实施例中,步骤H1中的判断签名操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致之前,还包括:签名模块解析接收到的签名操作指令,并判断是否解析成功,是则继续,否则报错;

[0234] 步骤H2:签名模块使用保存的签名私钥对签名操作指令中的待签名中间数据进行签名;

[0235] 步骤H3:签名模块判断当前状态是否满足预设条件,是则清除保存的验PIN签名数据,并将签名结果返回给终端,返回步骤S0,否则将签名结果返回给终端,返回步骤S0。

[0236] 可选的,在本实施例中,根据生成的第二共享密钥对验PIN指令中的第一计算结果进行验证之前包括:签名模块判断PIN码重试次数是否为预定数据,是则报错,提示PIN码锁定;否则继续;

[0237] 步骤F1中验证失败时还包括:

[0238] 步骤C1:签名模块更新PIN码重试次数;

[0239] 步骤C2:签名模块判断PIN码重试次数是否为预定数据,是则提示PIN码锁定,否则

执行步骤C3；

[0240] 步骤C3：签名模块判断验证PIN码是否连续三次出错，是则提示PIN码认证报文错误，否则提示输入PIN码错误；

[0241] 步骤F2还包括：将PIN码重试次数改为初始值。

[0242] 在本实施例中，签名操作既可以为普通签名也可以为复核签名，如为复核签名，则上述步骤H1和H2替换为：

[0243] 步骤P1：当签名模块接收到终端发送的设置安全环境操作指令时，判断设置安全环境操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致，是则执行步骤P2，否则结束；

[0244] 步骤P2：签名模块根据设置安全环境指令中的算法ID和密钥容器ID判断设置签名算法是否合法，是则执行步骤P3，否则结束；

[0245] 具体的，在本实施例中，步骤P2包括：

[0246] 步骤P21：签名模块根据密钥容器ID判断对应的密钥容器是否存在，是则执行步骤P22，否则结束；

[0247] 步骤P22：签名模块根据算法ID判断是否支持对应的算法，是则执行步骤P3，否则结束。

[0248] 步骤P3：签名模块根据密钥容器ID打开对应的密钥容器，根据算法ID设置对应的算法，并给终端返回成功设置安全环境响应；

[0249] 本实施例中的步骤T3还包括：签名模块给终端返回哈希值。

[0250] 步骤T1：当签名模块接收到终端发送的哈希操作指令时，判断哈希操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致，是则执行步骤T2，否则结束；

[0251] 步骤T2：签名模块对哈希操作指令进行解析得到待签名数据并保存；

[0252] 步骤T3：签名模块根据设置的算法对待签名数据进行哈希运算得到哈希值并保存，给终端返回哈希计算成功响应；

[0253] 步骤Q1：当签名模块接收到终端发送的签名操作指令时，判断签名操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致，是则执行步骤Q2，否则结束；

[0254] 步骤Q2：签名模块从保存的待签名数据中提取关键信息并判断是否提取成功，是则执行步骤Q3，否则结束；

[0255] 步骤Q3：签名模块显示关键信息并判断是否接收到用户确认信息，是则签名模块使用与签名操作指令中的容器ID所对应的容器中的签名私钥对保存的哈希值进行签名得到签名结果并保存，否则结束；

[0256] 步骤Q4：签名模块判断当前状态是否满足预设条件，是则清除保存的验PIN签名数据，并给终端返回签名成功信息，否则给终端返回签名失败信息；

[0257] 步骤L1：当签名模块接收到终端发送的获取签名结果指令时，将签名结果返回给终端。

[0258] 在本实施例的方法中，步骤F2还包括：将验PIN签名标识设为有效；

[0259] 步骤H1、步骤P1、步骤T1、步骤Q1中还包括：签名模块判断验PIN签名标识是否有效，是则继续，否则报错；

[0260] 步骤H3中判断为是时还包括：将验PIN签名标识设为无效。

[0261] 优选的，将验PIN签名标识设为有效，具体为：将验PIN签名标识置位；判断验PIN签名标识是否有效，具体为：判断验PIN签名标识是否置位；将验PIN签名标识设为无效，具体为：将验PIN签名标识复位。

[0262] 本实施例的方法适合一次验PIN一次签名、一次验PIN多次签名、一次验PIN后在签名有效时间内进行签名；

[0263] 可选的，在本实施例中步骤F2还包括：将签名次数设为初始值；签名模块判断当前状态是否满足预设条件，包括：更新签名次数，并判断签名次数是否等于预设值，是则满足预设条件，否则不满足预设条件。

[0264] 例如一次验PIN多次签名，则签名次数设为初始值0或N(N为非1正整数)，更新签名次数为自加1或自减1，预设值为N(N为非1正整数)或0；

[0265] 例如一次验PIN一次签名，则签名次数设为初始值N(N为非1正整数)或N+1，更新签名次数为自加1或自减1，预设值为N+1(N为非1正整数)或N；

[0266] 如为一次验PIN后在签名有效时间内进行签名，步骤F2还包括：设置签名有效时间；签名模块判断当前状态是否满足预设条件，包括：判断当前时间是否在签名有效时间内，是则报错，否则清除验PIN签名数据。

[0267] 本实施例的方法还包括：当签名模块接收到设置PIN码指令时，签名模块判断PIN码是否已设置，是则报错，否则对设置PIN码指令进行验证，如验证成功则根据设置PIN码指令中的第一密文生成PIN码并保存，如验证失败则结束。

[0268] 具体的，签名模块对设置PIN码指令进行验证，包括：

[0269] 步骤M1：签名模块将保存的签名模块私钥与设置PIN码指令中的终端公钥进行计算得到第一计算值，对第一计算值进行哈希运算，将哈希结果作为第二共享密钥；

[0270] 可选的，在步骤M1之前还包括：

[0271] 签名模块对接收到的设置PIN码指令进行解析，并判断是否解析成功，是则执行步骤M1，否则报错。

[0272] 步骤M2：签名模块使用第二共享密钥、对设置PIN码指令中的第一密文进行HMAC运算得到第二运算结果，并提取第二运算结果中的前16个字节数据得到提取数据；

[0273] 步骤M3：签名模块判断提取数据是否与设置PIN码指令中的第一结果数据一致，是则验证成功，否则验证失败。

[0274] 具体的，在本实施例中，根据设置PIN码指令中的第一密文生成PIN码并保存，包括：

[0275] 步骤N1：签名模块使用第二共享密钥对设置PIN码指令中的第一密文进行解密得到第一解密值，去除第一解密值中的填充数据得到密码中间值；

[0276] 步骤N2：签名模块判断密码中间值是否小于第一预设值，是则报错，否则执行步骤N3；

[0277] 步骤N3：签名模块对密码中间值进行哈希运算得到哈希结果，提取哈希结果中的前16个字节数据并保存为PIN码。

[0278] 具体的，本实施例方法还包括：

[0279] 当签名模块接收到修改PIN码指令时，对修改PIN码指令进行验证，如验证成功则用修改PIN码指令中的PIN码替换保存的PIN码，如验证失败则报错。

[0280] 具体的，在本实施例中，对修改PIN码指令进行验证，包括：

[0281] 步骤W1：签名模块对保存的签名模块私钥与修改PIN码指令中的终端公钥进行计算得到第一结果数据，对第一结果数据进行哈希运算得到第二共享密钥；将修改PIN码指令中的第一加密值和修改PIN码指令中的第二加密值进行拼接得到第二拼接结果；

[0282] 可选的，步骤W1之前还包括：

[0283] 签名模块解析接收到的修改PIN码指令，并判断是否解析成功，是则执行步骤W1，否则报错。

[0284] 步骤W2：签名模块使用第二共享密钥、对第二拼接结果进行HMAC运算得到第二运算结果，并从第二运算结果中提取前16个字节数据得到提取数据；

[0285] 步骤W3：签名模块判断修改PIN码指令中的中间数据与提取数据是否一致，是则执行步骤W4，否则报错；

[0286] 步骤W4：签名模块使用第二共享密钥对第一加密值进行解密得到第一解密值；

[0287] 步骤W5：签名模块判断第一解密值与内部保存的PIN码是否一致，是则验证成功，否则验证失败，重新生成签名模块密钥对并替换保存的签名模块密钥对。

[0288] 具体的，在本实施例中，用修改PIN码指令中的PIN码替换保存的PIN码，包括：

[0289] 步骤K1：签名模块使用第二共享密钥对第二加密值进行解密得到第二解密值，去除第二解密值中的填充数据得到第一中间值；

[0290] 步骤K2：签名模块判断第一中间值的长度是否小于第一预设值，是则执行步骤K3，否则报错；

[0291] 步骤K3：签名模块对第一中间值进行哈希运算得到哈希结果，提取哈希结果的前16个字节数据并替换内部保存的PIN码。

[0292] 在本实施例中，步骤N3还包括：签名模块将PIN码重试次数设为初始值；

[0293] 步骤K3还包括：签名模块将PIN码重试次数改为初始值；

[0294] 步骤W1之前还包括：签名模块判断PIN码重试次数是否为预定数据，是则提示PIN码锁定，否则执行步骤W1；

[0295] 步骤W5中验证失败之后还包括：

[0296] 步骤W6：签名模块更新PIN码重试次数；

[0297] 步骤W7：签名模块判断PIN码重试次数是否为预定数据，是则提示PIN码锁定，否则执行步骤W8；

[0298] 步骤W8：签名模块判断验证PIN码是否连续三次出错，是则提示PIN码认证报文错误，否则提示输入PIN码错误。

[0299] 可选的，本实施例的方法还包括：

[0300] 当签名模块接收到获取验PIN签名数据指令时，对获取验PIN签名数据指令进行验证，如验证成功则生成验PIN签名数据并发送给终端，如验证失败则结束。

[0301] 具体的，对获取验PIN签名数据指令进行验证，包括：

[0302] 步骤R1：签名模块将获取验PIN签名数据指令中的终端公钥与保存的签名模块私钥进行计算得到第一计算值，对第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥；

[0303] 可选的，步骤R1之前还包括：步骤R0：签名模块解析接收到的获取验PIN签名数据

指令，并判断是否解析成功，是则执行步骤R1，否则报错。

[0304] 步骤R2：签名模块使用第二共享密钥、对获取验PIN签名数据指令中的第一计算结果进行解密运算得到第二结果数据，获取内部保存的PIN码，将PIN码转换成字节流数据，对字节流数据进行哈希运算并提取哈希结果中的前16字节数据得到提取数据；

[0305] 步骤R3：签名模块判断第二结果数据是否与提取数据相同，是则验证成功，否则验证失败，重新生成签名模块密钥对并替换保存的签名模块密钥对。

[0306] 具体的，生成验PIN签名数据并发送给终端，包括：生成第一随机数作为验PIN签名数据，使用第二共享密钥对验PIN签名数据进行加密得到密文数据，并将密文数据返回给终端。

[0307] 可选的，在本实施例中，步骤N3还包括：签名模块将PIN码重试次数设为初始值；

[0308] 步骤R3验证成功时还包括：签名模块将PIN码重试次数改为初始值；

[0309] 步骤R1之前还包括：签名模块判断PIN码重试次数是否为预定数据，是则提示PIN码锁定；否则执行步骤R1；

[0310] 步骤R3判断为否还包括：

[0311] 步骤R4：签名模块更新PIN码重试次数；

[0312] 步骤R5：签名模块判断PIN码重试次数是否为预定数据，是则提示PIN码锁定，否则执行步骤R6；

[0313] 步骤R6：签名模块判断验证PIN码是否连续三次出错，是则提示PIN码认证报文错误，否则提示输入PIN码错误。

[0314] 本实施例的方法还包括：

[0315] 当证器接收到协商共享密钥指令时，生成签名模块密钥对并保存，将签名模块密钥对中的签名模块公钥返回给终端。

[0316] 实施例二

[0317] 本发明实施例二提供一种设置PIN码的方法，如图2所示，包括：

[0318] 步骤201：终端提示用户输入PIN码；

[0319] 步骤202：当终端接收到用户输入的PIN码时，判断PIN码的字符长度是否小于第一预设值，是则报错，否则执行步骤203；

[0320] 例如，在本实施例中，第一预设值为4；

[0321] 步骤203：终端将PIN码转换成字节流数据，并判断字节流数据是否小于第二预设值，是则执行步骤204，否则报错；

[0322] 例如，在本实施例中，第二预设值为255；

[0323] 步骤204：终端生成第一共享密钥；对字节流数据进行填充；

[0324] 具体的，在本实施例中，步骤204中的终端生成第一共享密钥包括：

[0325] 步骤A1：终端给签名模块发送获取共享密钥指令；

[0326] 步骤A2：当签名模块接收到协商共享密钥指令时，生成签名模块密钥对并保存，将签名模块密钥对中的签名模块公钥返回给终端；

[0327] 步骤A3：终端接收签名模块返回的签名模块公钥，生成终端密钥对，并将终端密钥对中的私钥与签名模块公钥进行计算得到第一数据，对第一数据进行哈希运算得到哈希值作为第一共享密钥；

[0328] 具体的，在本实施例中，对字节流数据进行填充包括：终端判断字节流数据的长度是否为64的倍数，是则执行步骤205，否则用0x00对字节流数据进行填充，直至字节流数据的长度为64的倍数，执行步骤205；

[0329] 步骤205：终端使用第一共享密钥对填充后的字节流数据进行加密得到第一密文；

[0330] 步骤206：终端使用第一共享密钥、对第一密文进行HMAC运算得到第一运算结果，将第一运算结果的前16字节数据作为第一结果数据；

[0331] 步骤207：终端将包含终端公钥、第一密文和第一结果数据的验PIN指令发送给签名模块；

[0332] 步骤208：签名模块判断是否接收到终端发送的数据，是则执行步骤209，否则报错；

[0333] 步骤209：签名模块判断PIN码是否已设置，是则报错，否则执行步骤210；

[0334] 步骤210：签名模块对接收到的验PIN指令进行解析，并判断是否解析成功，是则执行步骤211，否则报错；

[0335] 步骤211：签名模块将签名模块私钥与终端公钥进行计算得到第一计算值，对第一计算值进行哈希运算，将哈希结果作为第二共享密钥；

[0336] 步骤212：签名模块使用第二共享密钥、对解析得到的第一密文进行HMAC运算得到第二结果数据，并提取第二结果数据中的前16个字节数据得到提取数据；

[0337] 步骤213：签名模块判断提取数据是否与解析得到的第一结果数据一致，是则执行步骤214，否则报错；

[0338] 步骤214：签名模块使用第二共享密钥对解析得到的第一密文进行解密得到第一解密值，去除第一解密值中的填充数据得到密码中间值；

[0339] 步骤215：签名模块判断密码中间值是否小于第一预设值，是则报错，否则执行步骤216；

[0340] 步骤216：签名模块对密码中间值进行哈希运算得到哈希结果，提取哈希结果中的前16个字节数据并保存为PIN码，将PIN码重试次数设为初始值；

[0341] 例如，本实施例中的预定数据为8。

[0342] 实施例三

[0343] 本发明实施例三提供一种修改PIN码的方法，如图3所示，包括：

[0344] 步骤301：终端提示用户输入当前PIN码，当接收到当前PIN码时提示用户输入新PIN码；

[0345] 步骤302：当终端接收到新PIN码后，判断新PIN码的字符长度是否小于第一预设值，是则报错，否则执行步骤303；

[0346] 例如，在本实施例中，第一预设值为4；

[0347] 步骤303：终端分别将当前PIN码和新PIN码转换成字节流数据得到第一字节流数据和第二字节流数据；

[0348] 步骤304：终端判断第一字节流数据和第二字节流数据的长度是否均小于第二预设长度，是则执行步骤305，否则报错；

[0349] 例如，在本实施例中，第二预设值为255；

[0350] 步骤305：终端生成第一共享密钥，对第一字节流数据进行哈希运算，并提取运算

结果中的前16个字节数据得到第一中间数据;使用第一共享密钥对第一中间数据进行加密运算得到第一加密值;

[0351] 具体的,本实施例中步骤305的实现过程与步骤204相同,在此不再赘述;

[0352] 步骤306:终端对第二字节流数据进行填充,使用第一共享密钥对填充后的第二字节流数据进行加密得到第二加密值;

[0353] 具体的,在本实施例中,终端判断第二字节流数据的长度是否为64的倍数,如不为64的倍数则用0x00对第二字节流数据进行填充,直至第二字节流数据的长度为64的倍数;

[0354] 步骤307:终端将第二加密值和第一加密值进行拼接得到拼接值,使用第一共享密钥、对拼接值进行HMAC运算得到第一运算结果,并从第一运算结果中提取前16个字节数据得到中间数据;

[0355] 步骤308:终端将包括终端公钥、第一加密值、第二加密值和中间数据的修改PIN指令发送给签名模块;

[0356] 步骤309:签名模块判断是否接收到终端发送的数据,是则执行步骤310,否则报错;

[0357] 步骤310:签名模块判断PIN码重试次数是否为预定数据,是则提示PIN码锁定,否则执行步骤311;

[0358] 步骤311:签名模块解析接收到的修改PIN指令,并判断是否解析成功,是则执行步骤312,否则报错;

[0359] 步骤312:签名模块将签名模块私钥与解析得到的终端公钥进行计算得到第一计算结果,对第一计算结果进行哈希运算得到第二共享密钥;将解析得到第一加密值和第二加密值进行拼接得到第二拼接结果;

[0360] 步骤313:签名模块使用第二共享密钥、对第二拼接结果进行HMAC运算得到第二运算结果,并从第二运算结果中提取前16个字节数据得到提取数据;

[0361] 步骤314:签名模块判断解析得到的中间数据与提取数据是否一致,是则执行步骤315,否则报错;

[0362] 步骤315:签名模块使用第二共享密钥,对第一加密值进行解密得到第一解密值;

[0363] 步骤316:签名模块判断第一解密值与内部保存的PIN码是否一致,是则执行步骤317,否则执行步骤320;

[0364] 步骤317:签名模块使用第二共享密钥对解析得到的第二加密值进行解密得到第二解密值,去除第二解密值中的填充数据得到第一中间值;

[0365] 步骤318:签名模块判断第一中间值的长度是否小于第一预设值,是则执行步骤319,否则报错;

[0366] 步骤319:签名模块对第一中间值进行哈希运算,提取哈希结果的前16个字节数据并替换保存的PIN码,将PIN码重试次数改为初始值;

[0367] 步骤320:签名模块重新生成签名模块密钥对并替换保存的签名模块密钥对,更新PIN码重试次数;

[0368] 在本实施例中,如PIN码重试次数初始值为0,则更新PIN码重试次数具体为:PIN码重试次数自加1;如PIN码重试次数初始值为正整数,则更新PIN码重试次数具体为:PIN码重试次数自减1;

[0369] 步骤321:签名模块判断PIN码重试次数是否为预定数据,是则提示PIN码锁定,否则执行步骤322;

[0370] 在本实施例中,如PIN码重试次数初始值为0,则预定数据为正整数;如PIN码重试次数初始值为正整数,则预定数据为0;

[0371] 步骤322:签名模块判断验证PIN码是否连续三次出错,是则提示PIN码认证报文错误,否则提示输入PIN码错误。

[0372] 实施例四

[0373] 本发明实施例四提供一种获取验PIN签名数据的方法,如图4所示,包括:

[0374] 步骤401:终端提示用户输入PIN码;

[0375] 步骤402:当终端接收到用户输入的PIN码时,判断PIN码的字符长度是否小于第一预设值,是则报错,否则执行步骤403;

[0376] 例如,在本实施例中,第一预设值为4;

[0377] 步骤403:终端将PIN码转换成字节流数据,并判断字节流数据是否小于第二预设值,是则执行步骤404,否则报错;

[0378] 例如,在本实施例中,第二预设值为255;

[0379] 步骤404:终端生成第一共享密钥,对字节流数据进行哈希运算并提取运算结果中的前16字节数据作为第一中间数据,使用第一共享密钥对第一中间数据进行加密运算得到第一结果数据;

[0380] 本实施例中的终端密钥对包括终端公钥和终端私钥;生成第一共享密钥的过程与步骤204相同,在此不再赘述;

[0381] 步骤405:终端将包括终端公钥和第一结果数据的获取验PIN签名数据指令发送给签名模块;

[0382] 步骤406:签名模块判断是否接收到终端发送的数据,是则执行步骤407,否则报错;

[0383] 步骤407:签名模块判断PIN码重试次数是否为预定数据,是则提示PIN码锁定;否则执行步骤408;

[0384] 步骤408:签名模块解析接收到的获取验PIN签名数据指令,并判断是否解析成功,是则执行步骤409,否则报错;

[0385] 步骤409:签名模块将解析得到的终端公钥与签名模块私钥进行计算得到第一计算值,对第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥;

[0386] 步骤410:签名模块使用第二共享密钥、对解析得到的第一结果数据进行解密运算得到第二运算结果,获取内部保存的PIN码,将PIN码转换成字节流数据,对字节流数据进行哈希运算并提取哈希结果中的前16字节数据得到提取数据;

[0387] 步骤411:签名模块判断第二运算结果是否与提取数据相同,是则执行步骤412,否则执行步骤413;

[0388] 步骤412:签名模块生成第一随机数作为验PIN签名数据,使用第二共享密钥对验PIN签名数据进行加密得到密文数据,并将密文数据返回给终端,将PIN码重试次数改为初始值;

[0389] 优选的,本实施例中的第一随机数的长度为16字节;

[0390] 步骤413:签名模块重新生成签名模块密钥对并替换保存的签名模块密钥对,更新PIN码重试次数;

[0391] 步骤414:签名模块判断PIN码重试次数是否为预定数据,是则提示PIN码锁定,否则执行步骤415;

[0392] 在本实施例中,如PIN码重试次数初始值为0,则预定数据为正整数;如PIN码重试次数初始值为正整数,则预定数据为0;

[0393] 步骤415:签名模块判断验证PIN码是否连续三次出错,是则提示PIN码认证报文错误,否则提示输入PIN码错误。

[0394] 实施例五

[0395] 本发明实施例五提供了一种安全签名的实现方法流程图,如图5所示,包括:

[0396] 步骤501:终端提示用户输入PIN码;

[0397] 步骤502:当终端接收到用户输入的PIN码时,判断PIN码的字符长度是否小于第一预设值,是则报错,否则执行步骤503;

[0398] 例如,在本实施例中,第一预设值为4;

[0399] 步骤503:终端将PIN码转换成字节流数据,并判断字节流数据是否小于第二预设值,是则执行步骤504,否则报错;

[0400] 例如,在本实施例中,第二预设值为255;

[0401] 步骤504:终端生成第一共享密钥,对字节流数据进行哈希运算并提取哈希结果中的前16字节数据作为第一中间数据,使用第一共享密钥对第一中间数据进行加密运算得到第一结果数据;

[0402] 本实施例中的终端密钥对包括终端公钥和终端私钥;

[0403] 具体的,在本实施例中,步骤504中的终端生成第一共享密钥包括:

[0404] 步骤A1:终端给签名模块发送获取共享密钥指令;

[0405] 步骤A2:当签名模块接收到共享密钥指令时,将保存的签名模块密钥对中的签名模块公钥返回给终端;

[0406] 步骤A3:终端接收签名模块返回的签名模块公钥,生成终端密钥对,并将终端密钥对中的私钥与签名模块公钥进行计算得到第一数据,对第一数据进行哈希运算得到哈希值作为第一共享密钥;

[0407] 步骤505:终端将包括终端公钥和第一结果数据的验PIN指令发送给签名模块;

[0408] 步骤506:签名模块判断是否接收到终端发送的数据,是则执行步骤507,否则报错;

[0409] 步骤507:签名模块判断PIN码重试次数是否为预定数据,是则提示PIN码锁定;否则执行步骤508;

[0410] 步骤508:签名模块解析接收到的验PIN指令,并判断是否解析成功,是则执行步骤509,否则报错;

[0411] 步骤509:签名模块将解析得到的终端公钥与签名模块私钥进行计算得到第一计算值,对第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥;

[0412] 步骤510:签名模块使用第二共享密钥对解析得到的第一结果数据进行解密运算得到第二结果数据,签名模块获取内部保存的PIN码转换成字节流数据,对字节流数据进行

哈希运算并提取哈希结果中的前16字节数据作为提取数据；

[0413] 步骤511：签名模块判断提取数据是否与第二结果数据一致，是则执行步骤512，否则执行步骤513；

[0414] 步骤512：签名模块置位验PIN签名标识，生成第一随机数作为验PIN签名数据并保存，使用第二共享密钥对验PIN签名数据进行加密得到密文数据，并将密文数据返回给终端，将PIN码重试次数改为初始值，执行步骤516；

[0415] 在本实施例中，验PIN签名标识初始状态为0；

[0416] 优选的，本实施例中的第一随机数的长度为16字节；

[0417] 步骤513：签名模块重新生成签名模块密钥对并替换保存的签名模块密钥对，更新PIN码重试次数；

[0418] 在本实施例中，替换后的签名模块密钥在下一次进行签名时进行使用；

[0419] 步骤514：签名模块判断PIN码重试次数是否为预定数据，是则提示PIN码锁定，否则执行步骤515；

[0420] 在本实施例中，如PIN码重试次数初始值为0，则预定数据为正整数；如PIN码重试次数初始值为正整数，则预定数据为0；

[0421] 步骤515：签名模块判断验证PIN码是否连续三次出错，是则提示PIN码认证报文错误，否则提示输入PIN码错误；

[0422] 步骤516：终端对待签名数据进行哈希运算得到第一哈希值，使用第一共享密钥对接收到的密文数据进行解密得到验PIN签名数据；使用验PIN签名数据作为密钥、对第一哈希值进行HMAC操作得到第一中间值，提取第一中间值的前16个字节数据得到待签名中间数据；

[0423] 步骤517：终端将包含待签名中间数据和验PIN签名数据的签名操作指令发送给签名模块；

[0424] 步骤518：签名模块判断验PIN签名标识是否置位且判断签名操作指令中的验PIN签名数据和保存的验PIN签名数据是否一致，是则执行步骤519，否则报错；

[0425] 步骤519：签名模块使用签名私钥对签名操作指令中的待签名中间数据进行签名得到签名结果并返回给终端，将验PIN签名标识复位，清除保存的验PIN签名数据；

[0426] 本实施例为一次验PIN一次签名的实现过程，还可有其他方式，如一次验PIN多次签名，一次验PIN后在签名有效时间内进行签名等；

[0427] 可选的，一次验PIN多次签名方式实现，则在步骤512中还包括：将签名次数设为初始值，在步骤519中的将验PIN签名标识复位之前还包括：更新签名次数，并判断所述签名次数是否等于预设值，是则将验PIN签名标识复位，清除保存的验PIN签名数据，否则报错；

[0428] 可选的，一次验PIN后在签名有效时间内进行签名，则在步骤512中还包括：设置签名有效时间，在步骤519中的将验PIN签名标识复位之前还包括：判断当前时间是否在签名有效时间内，是则报错，否则将验PIN签名标识复位，清除保存的验PIN签名数据。

[0429] 实施例六

[0430] 本发明实施例六提供了一种安全签名的实现方法，如图6和图7所示，包括：

[0431] 步骤601：终端提示用户输入PIN码；

[0432] 步骤602：当终端接收到用户输入的PIN码时，判断PIN码的字符长度是否小于第一

预设值，是则报错，否则执行步骤603；

[0433] 例如，在本实施例中，第一预设值为4；

[0434] 步骤603：终端将PIN码转换成字节流数据，并判断字节流数据是否小于第二预设值，是则执行步骤604，否则报错；

[0435] 例如，在本实施例中，第二预设值为255；

[0436] 步骤604：终端生成第一共享密钥，对字节流数据进行哈希运算并提取哈希结果中的前16字节数据作为第一中间数据，使用第一共享密钥对第一中间数据进行加密运算得到第一结果数据；

[0437] 本实施例中的终端密钥对包括终端公钥和终端私钥；生成第一共享密钥的过程与步骤204相同，在此不再赘述；

[0438] 步骤605：终端将包括终端公钥和第一结果数据的验PIN指令发送给签名模块；

[0439] 步骤606：签名模块判断是否接收到终端发送的验PIN指令，是则执行步骤607，否则报错；

[0440] 步骤607：签名模块判断PIN码重试次数是否为预定数据，是则提示PIN码锁定；否则执行步骤608；

[0441] 步骤608：签名模块解析接收到的验PIN指令，并判断是否解析成功，是则执行步骤609，否则报错；

[0442] 步骤609：签名模块将解析得到的终端公钥与签名模块私钥进行计算得到第一计算值，对第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥；

[0443] 步骤610：签名模块使用第二共享密钥对解析得到的第一中间数据进行解密运算得到第二结果数据，获取内部保存的PIN码并将PIN码转换成字节流数据，对字节流数据进行哈希运算并提取哈希结果中的前16字节数据作为提取数据；

[0444] 步骤611：签名模块判断第二结果数据是否与提取数据相同，是则执行步骤615，否则执行步骤612；

[0445] 步骤612：签名模块重新生成签名模块密钥对并替换保存的签名模块密钥对，更新PIN码重试次数；

[0446] 步骤613：签名模块判断PIN码重试次数是否为预定数据，是则提示PIN码锁定，否则执行步骤614；

[0447] 在本实施例中，如PIN码重试次数初始值为0，则预定数据为正整数；如PIN码重试次数初始值为正整数，则预定数据为0；

[0448] 步骤614：签名模块判断验证PIN码是否连续三次出错，是则提示PIN码认证报文错误，否则提示输入PIN码错误；

[0449] 步骤615：签名模块置位验PIN签名标识，生成第一随机数作为验PIN签名数据并保存，使用第二共享密钥对验PIN签名数据进行加密得到密文数据，并将密文数据返回给终端，将PIN码重试次数改为初始值，执行步骤616；

[0450] 步骤616：终端使用第一共享密钥对接收到的密文数据进行解密得到验PIN签名数据，并将包含验PIN签名数据、算法ID、密钥容器ID的设置安全环境指令发送给签名模块；

[0451] 步骤617：签名模块判断验PIN签名标识是否置位，是则执行步骤618，否则报错；

[0452] 步骤618：签名模块判断设置安全环境指令中的验PIN签名数据与保存的验PIN签

名数据是否一致，是则执行步骤619，否则报错；

[0453] 在本实施例中，步骤617与步骤618的顺序可调换；

[0454] 步骤619：签名模块根据设置安全环境指令中的密钥容器ID判断对应的密钥容器是否存在，是则执行步骤620，否则报错；

[0455] 步骤620：签名模块根据设置安全环境指令中的算法ID判断是否支持对应的算法，是则执行步骤621，否则报错；

[0456] 步骤621：签名模块根据密钥容器ID打开对应的密钥容器，根据算法ID设置对应的算法，并给终端返回成功设置安全环境响应；

[0457] 步骤622：终端将包含待签名数据、验PIN签名数据的哈希操作指令发送给签名模块；

[0458] 步骤623：签名模块判断验PIN签名标识是否置位，是则执行步骤624，否则报错；

[0459] 步骤624：签名模块判断哈希操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致，是则执行步骤625，否则报错；

[0460] 步骤625：签名模块对哈希操作指令进行解析得到待签名数据并保存；

[0461] 步骤626：签名模块根据设置的算法对待签名数据进行哈希运算得到哈希值并保存，将哈希值返回给终端；

[0462] 可选的，本实施例中在步骤626中签名模块也可不发送哈希值而发送哈希计算成功信息；

[0463] 步骤627：终端将包含验PIN签名数据的签名操作指令发送给签名模块；

[0464] 优选的，在本实施例的步骤627之前还包括：终端接收到哈希值后，对待签名数据进行哈希计算，比较计算结果是否与接收到的哈希值一致，是则执行步骤627，否则报错；

[0465] 步骤628：签名模块判断验PIN签名标识是否置位，是则执行步骤629，否则报错；

[0466] 步骤629：签名模块判断签名操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致，是则执行步骤630，否则报错；

[0467] 步骤630：签名模块从保存的待签名数据中提取关键信息并判断是否提取成功，是则执行步骤631，否则报错；

[0468] 步骤631：签名模块显示关键信息判断是否接收到用户确认信息，是则签名模块使用对应容器中的签名私钥对保存的哈希值进行签名得到签名结果并保存，否则报错；

[0469] 步骤632：签名模块判断当前状态是否满足预设条件，是则删除保存的验PIN签名数据，将验PIN签名标识复位，并给所述终端返回签名成功信息，否则给终端返回签名失败信息；

[0470] 步骤633：当终端接收到签名成功信息时，发送获取签名结果指令给签名模块；

[0471] 步骤634：签名模块将保存的签名结果返回给终端。

[0472] 在本实施例中，步骤619与步骤620的顺序可调换、步骤617与步骤618的顺序可调换、步骤623与步骤624的顺序可调换、步骤628与步骤629的顺序可调换。

[0473] 实施例七

[0474] 本发明实施例七提供一种安全签名的实现装置，如图8所示，包括签名模块，签名模块：

[0475] 接收子模块71，用于接收终端发送的验PIN指令和签名操作指令；

[0476] 第一生成子模块72，用于当接收子模块71接收到验PIN码指令时，根据验PIN指令中的终端公钥和保存的签名模块私钥生成第二共享密钥；

[0477] 在本实施例中，第一生成子模块72具体用于将验PIN指令中的终端公钥与保存的签名模块私钥进行计算得到第一计算值，对第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥；

[0478] 第一验证子模块73，用于使用第一生成子模块72生成的第二共享密钥对验PIN指令中的第一计算结果进行验证，如验证成功则触发第三生成子模块75；如验证失败则触发第二生成子模块74；

[0479] 在本实施例中，第一验证子模块73具体用于使用生成的第二共享密钥对验PIN指令中的第一计算结果进行解密运算得到第二结果数据，获取内部保存的PIN码转换成第二字节流数据，对第二字节流数据进行哈希运算并提取哈希结果中的前16字节数据作为提取数据，判断提取数据是否与第二结果数据一致，是则验证成功，触发第三生成子模块；否则验证失败，触发第二生成子模块74；

[0480] 第二生成子模块74，用于重新生成签名模块密钥对并替换保存的签名模块密钥对；签名模块密钥对包括签名模块私钥和签名模块公钥；

[0481] 第三生成子模块75，用于生成验PIN签名数据并保存；根据第一生成子模块72生成的第二共享密钥和验PIN签名数据生成第二计算结果；

[0482] 在本实施例中，第三生成子模块75具体用于使用第二共享密钥对验PIN签名数据进行加密得到密文数据作为第二计算结果；

[0483] 第一判断子模块76，用于当接收子模块71接收到终端发送的签名操作指令时，判断签名操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致，是则触发签名子模块77，否则报错；

[0484] 签名子模块77，用于使用保存的签名私钥对签名操作指令中的待签名中间数据进行签名；

[0485] 判断清除子模块78，用于判断当前状态是否满足预设条件，是则清除保存的验PIN签名数据；

[0486] 发送子模块79，用于将第三生成子模块75生成的第二计算结果发送给终端，还用于在判断清除子模块78判断为是或否时将签名子模块77得到的签名结果发送给终端。

[0487] 可选的，本实施例的签名模块还包括：

[0488] 第一解析子模块，用于解析接收子模块71接收到的验PIN指令，并判断是否解析成功，是则触发第一验证子模块73，否则报错；

[0489] 第二解析子模块，用于解析接收子模块71接收到的签名操作指令，并判断是否解析成功，是则触发第一判断子模块76，否则报错。

[0490] 可选的，本实施例的签名模块还包括：

[0491] 第二判断子模块，用于判断PIN码重试次数是否为预定数据，是则报错，提示PIN码锁定；否则触发第一验证子模块73；

[0492] 例如，本实施例中的预定数据为0；

[0493] 第一更新子模块，用于在第一验证子模块73验证失败后更新PIN码重试次数；

[0494] 例如，更新PIN码重试次数具体为：PIN码重试次数自减1；

[0495] 第三判断子模块，用于判断PIN码重试次数是否为预定数据，是则提示PIN码锁定，否则触发第四判断子模块；

[0496] 第四判断子模块，用于判断验证PIN码是否连续三次出错，是则提示PIN码认证报文错误，否则提示输入PIN码错误；

[0497] 第一修改子模块，用于在第一验证子模块73验证成功后将PIN码重试次数改为初始值；

[0498] 例如，本实施例中的初始值为8；

[0499] 本实施例中的装置还可用于复核签名，则接收子模块71还用于接收终端发送的设置安全环境操作指令、哈希操作指令、获取签名结果指令；

[0500] 相应的，签名模块还包括：

[0501] 第五判断子模块，用于当接收子模块71接收到终端发送的设置安全环境操作指令时，判断设置安全环境操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致，是则触发第六判断子模块，否则结束；

[0502] 第六判断子模块，用于根据设置安全环境指令中的算法ID和密钥容器ID判断设置签名算法是否合法，是则触发打开设置子模块，否则结束；

[0503] 在本实施例中，第六判断子模块具体用于根据密钥容器ID判断对应的密钥容器是否存在且根据算法ID判断是否支持对应的算法，如判断均为是则触发打开设置子模块，否则结束；

[0504] 打开设置子模块，用于根据密钥容器ID打开对应的密钥容器，根据算法ID设置对应的算法；

[0505] 第七判断子模块，用于当接收子模块71接收到终端发送的哈希操作指令时，判断哈希操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致，是则触发解析保存子模块，否则结束；

[0506] 解析保存子模块，用于对哈希操作指令进行解析得到待签名数据并保存；

[0507] 哈希运算子模块，用于根据设置的算法对待签名数据进行哈希运算得到哈希值并保存；

[0508] 提取判断子模块，用于在第一判断子模块76判断为是时从保存的待签名数据中提取关键信息并判断是否提取成功，是则触发显示判断子模块，否则结束；

[0509] 显示判断子模块，用于显示提取判断子模块提取的关键信息并判断是否接收到用户确认信息，是则触发签名子模块77，否则结束；

[0510] 签名子模块77，具体用于使用与签名操作指令中的容器ID所对应的容器中的签名私钥对保存的哈希值进行签名得到签名结果并保存；

[0511] 发送子模块79还用于在打开设置子模块设置完对应算法之后给终端返回成功设置安全环境响应；还用于在哈希运算子模块运算完成之后给终端返回哈希计算成功响应；还用于当判断清除子模块78判断为是时给终端返回签名成功信息，当判断清除子模块判断为否时给终端返回签名失败信息；还用于当接收子模块71接收到终端发送的获取签名结果指令时，将签名保存子模块保存的签名结果返回给终端。

[0512] 可选的，发送子模块79还用于在哈希运算子模块运算完成之后给终端返回哈希值。

[0513] 在本实施例中，第三生成子模块75还用于将验PIN签名标识设为有效；具体为，将验PIN签名标识置位；

[0514] 第一判断子模块76还用于判断验PIN签名标识是否有效；具体为：判断验PIN签名标识是否置位；

[0515] 第五判断子模块还用于判断验PIN签名标识是否有效；具体为：判断验PIN签名标识是否置位；

[0516] 第七判断子模块还用于判断验PIN签名标识是否有效；具体为：判断验PIN签名标识是否置位；

[0517] 判断清除子模块78还用于判断当前状态满足预设条件时将验PIN签名标识设为无效；具体为，将验PIN签名标识复位。

[0518] 如本实施例中的装置适用于一次验PIN多次签名，则第三生成子模块75还用于将签名次数设为初始值；

[0519] 判断清除子模块78，具体用于更新签名次数，并判断签名次数是否等于预设值，是则清除保存的验PIN签名数据。

[0520] 如本实施例中的装置适用于一次验PIN后在预设时间内进行签名，则第三生成子模块75还用于设置签名有效时间；

[0521] 判断清除子模块78，具体用于判断当前时间是否在签名有效时间内，是则清除保存的验PIN签名数据。

[0522] 在本实施例中，接收子模块71还用于接收设置PIN码指令；

[0523] 相应的，签名模块还包括：

[0524] 第八判断子模块，用于当接收子模块71接收到设置PIN码指令时，判断PIN码是否已设置，是则报错，否则触发第二验证子模块；

[0525] 第二验证子模块，用于对设置PIN码指令进行验证，如验证成功则根据设置PIN码指令中的第一密文生成PIN码并保存，如验证失败则结束。

[0526] 在本实施例中，第二验证子模块具体包括：

[0527] 计算哈希单元，用于将保存的签名模块私钥与设置PIN码指令中的终端公钥进行计算得到第一计算值，对第一计算值进行哈希运算，将哈希结果作为第二共享密钥；

[0528] 第一运算提取单元，用于使用第二共享密钥、对设置PIN码指令中的第一密文进行HMAC运算得到第二运算结果，并提取第二运算结果中的前16个字节数据得到提取数据；

[0529] 第一判断单元，用于判断提取数据是否与设置PIN码指令中的第一结果数据一致，是则触发生成保存单元，否则结束；

[0530] 生成保存单元，用于根据设置PIN码指令中的第一密文生成PIN码并保存。

[0531] 具体的，本实施例中的生成保存单元具体包括：

[0532] 解密去除子单元，用于使用第二共享密钥对设置PIN码指令中的第一密文进行解密得到第一解密值，去除第一解密值中的填充数据得到密码中间值；

[0533] 第一判断子单元，用于判断密码中间值是否小于第一预设值，是则报错，否则触发哈希提取子单元；

[0534] 哈希提取子单元，用于对密码中间值进行哈希运算得到哈希结果，提取哈希结果中的前16个字节数据并保存为PIN码；

[0535] 可选的，第二验证子模块还包括：

[0536] 第一解析判断单元，用于对接收到的设置PIN码指令进行解析，并判断是否解析成功，是则触发计算哈希单元，否则报错。

[0537] 在本实施例中，接收子模块71还用于接收修改PIN码指令；

[0538] 相应的，签名模块还包括：

[0539] 第三验证子模块，用于当接收子模块71接收到修改PIN码指令时，对修改PIN码指令进行验证，如验证成功则触发替换保存子模块，如验证失败则报错；

[0540] 具体的，本实施例中的第三验证子模块具体包括：

[0541] 计算拼接单元，用于对保存的签名模块私钥与修改PIN码指令中的终端公钥进行计算得到第一结果数据，对第一结果数据进行哈希运算得到第二共享密钥；将修改PIN码指令中的第一加密值和修改PIN码指令中的第二加密值进行拼接得到第二拼接结果；

[0542] 第二运算提取单元，用于使用第二共享密钥、对第二拼接结果进行HMAC运算得到第二运算结果，并从第二运算结果中提取前16个字节数据得到提取数据；

[0543] 第二判断单元，用于判断修改PIN码指令中的中间数据与提取数据是否一致，是则触发第一解密单元，否则报错；

[0544] 第一解密单元，用于使用第二共享密钥对第一加密值进行解密得到第一解密值；

[0545] 第三判断单元，用于判断第一解密值与内部保存的PIN码是否一致，是则触发替换保存子模块，否则报错，重新生成签名模块密钥对并替换保存的签名模块密钥对；

[0546] 替换保存子模块，用于用修改PIN码指令中的PIN码替换保存的PIN码。

[0547] 具体的，本实施例中的替换保存子模块具体包括：

[0548] 解密去除单元，用于使用第二共享密钥对第二加密值进行解密得到第二解密值，去除第二解密值中的填充数据得到第一中间值；

[0549] 第四判断单元，用于判断第一中间值的长度是否小于第一预设值，是则触发哈希替换单元，否则报错；

[0550] 哈希替换单元，用于对第一中间值进行哈希运算得到哈希结果，提取哈希结果的前16个字节数据并替换内部保存的PIN码。

[0551] 可选的，第三验证子模块还包括：

[0552] 第二解析判断单元，用于解析接收到的修改PIN码指令，并判断是否解析成功，是则触发计算拼接单元，否则报错。

[0553] 优选的，哈希提取子单元还用于将PIN码重试次数设为初始值；

[0554] 哈希替换单元还用于将PIN码重试次数改为初始值；

[0555] 第三验证子模块还包括：

[0556] 第五判断单元，用于判断PIN码重试次数是否为预定数据，是则提示PIN码锁定，否则触发计算拼接单元；

[0557] 第一更新判断单元，用于当第三判断单元判断为否时，更新PIN码重试次数；判断PIN码重试次数是否为预定数据，是则提示PIN码锁定，否则触发第六判断单元；

[0558] 第六判断单元，用于判断验证PIN码是否连续三次出错，是则提示PIN码认证报文错误，否则提示输入PIN码错误。

[0559] 在本实施例中，接收子模块71还用于接收获取验PIN签名数据指令；

[0560] 相应的，签名模块还包括：

[0561] 第四验证子模块，用于当接收子模块71接收到获取验PIN签名数据指令时，对获取验PIN签名数据指令进行验证，如验证成功则触发第四生成子模块，如验证失败则结束；

[0562] 具体的，第四验证子模块具体包括：

[0563] 计算哈希单元，用于将获取验PIN签名数据指令中的终端公钥与保存的签名模块私钥进行计算得到第一计算值，对第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥；

[0564] 解密提取单元，用于使用第二共享密钥、对获取验PIN签名数据指令中的第一计算结果进行解密运算得到第二结果数据，获取内部保存的PIN码，将PIN码转换成字节流数据，对字节流数据进行哈希运算并提取哈希结果中的前16字节数据得到提取数据；

[0565] 第七判断单元，用于判断第二结果数据是否与提取数据相同，是则验证成功，触发第四生成子模块，否则验证失败，重新生成签名模块密钥对并替换保存的签名模块密钥对；

[0566] 第四生成子模块，用于生成验PIN签名数据；

[0567] 优选的，第四生成子模块具体用于生成第一随机数作为验PIN签名数据，使用第二共享密钥对验PIN签名数据进行加密得到密文数据；

[0568] 发送子模块79，还用于将第四验证子模块生成的验PIN签名数据发送给终端。

[0569] 相应的，发送子模块79还用于将第四验证子模块生成的密文数据返回给终端。

[0570] 可选的，第四验证子模块还包括：

[0571] 第三解析判断单元，用于解析接收到的获取验PIN签名数据指令，并判断是否解析成功，是则触发计算哈希单元，否则报错。

[0572] 优选的，哈希提取子单元还用于将PIN码重试次数设为初始值；

[0573] 第七判断单元判断为是时还用于将PIN码重试次数改为初始值；

[0574] 第四验证子模块还包括：

[0575] 第八判断单元，还用于判断PIN码重试次数是否为预定数据，是则提示PIN码锁定；否则触发计算哈希单元；

[0576] 第二更新判断单元，用于当第七判断单元判断为否时，更新PIN码重试次数；判断PIN码重试次数是否为预定数据，是则提示PIN码锁定，否则触发第九判断单元；

[0577] 第九判断单元，用于判断验证PIN码是否连续三次出错，是则提示PIN码认证报文错误，否则提示输入PIN码错误。

[0578] 本实施例中的接收子模块71还用于接收终端发送的协商共享密钥指令；

[0579] 相应的，签名模块还包括：

[0580] 第五生成子模块，用于当接收子模块71接收到协商共享密钥指令时，生成签名模块密钥对并保存；

[0581] 发送子模块79还用于将签名模块密钥对中的签名模块公钥返回给终端。

[0582] 本实施例中的签名模块为硬件设备或计算机程序或硬件设备与计算机程序的组合。

[0583] 以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明公开的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围

为准。

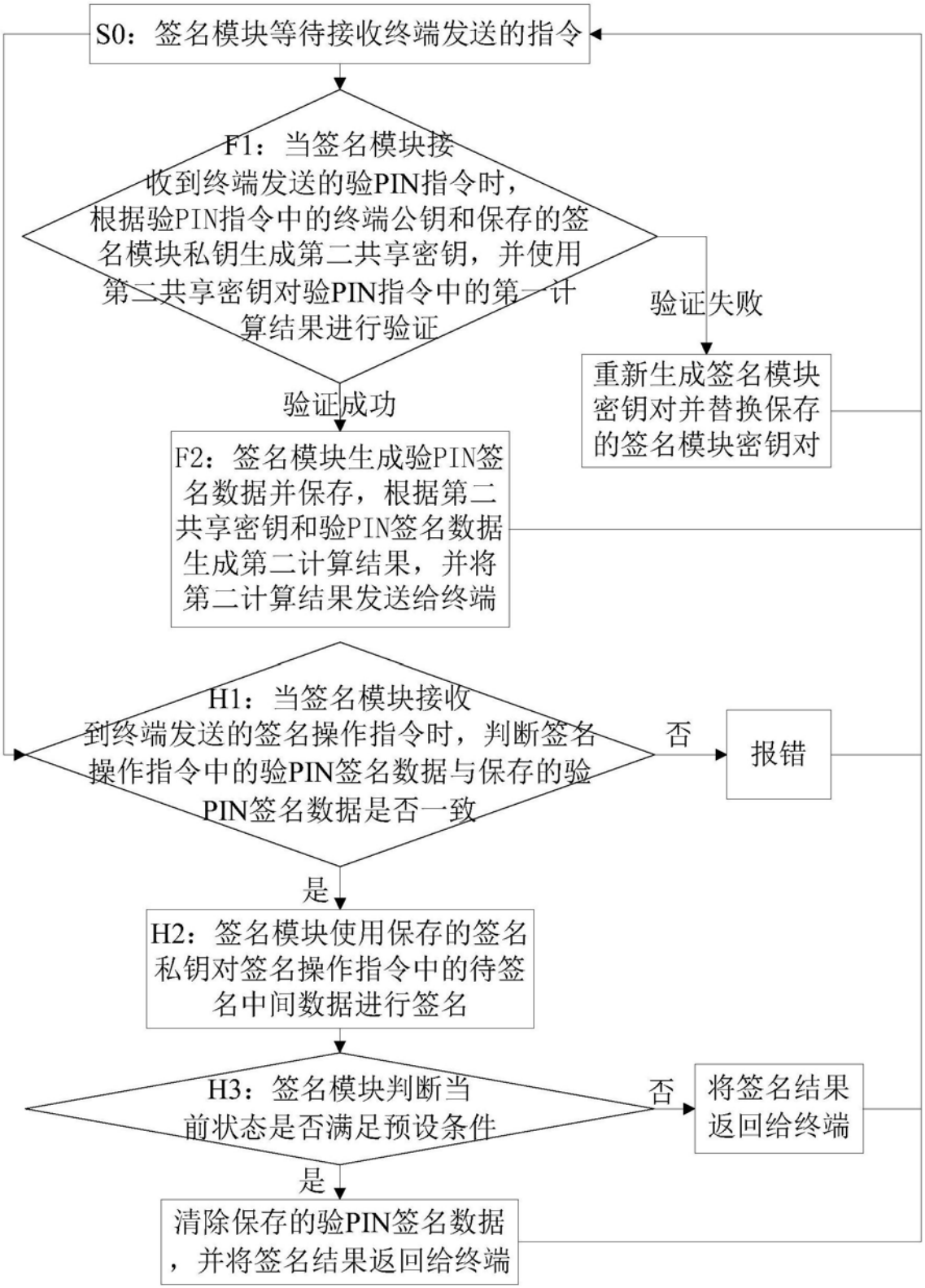

S0：签名模块等待接收终端发送的指令
F1：当签名模块接收到终端发送的验PIN指令时，根据验PIN指令中的终端公钥和保存的签名模块私钥生成第二共享密钥，并使用第二共享密钥对验PIN指令中的第一计算结果进行验证
验证失败
重新生成签名模块密钥对并替换保存的签名模块密钥对
验证成功
F2：签名模块生成验PIN签名数据并保存，根据第二共享密钥和验PIN签名数据生成第二计算结果，并将第二计算结果发送给终端
H1：当签名模块接收到终端发送的签名操作指令时，判断签名操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致
否
报错
是
H2：签名模块使用保存的签名私钥对签名操作指令中的待签名中间数据进行签名
H3：签名模块判断当前状态是否满足预设条件
否
将签名结果返回给终端
是
清除保存的验PIN签名数据，并将签名结果返回给终端

图1

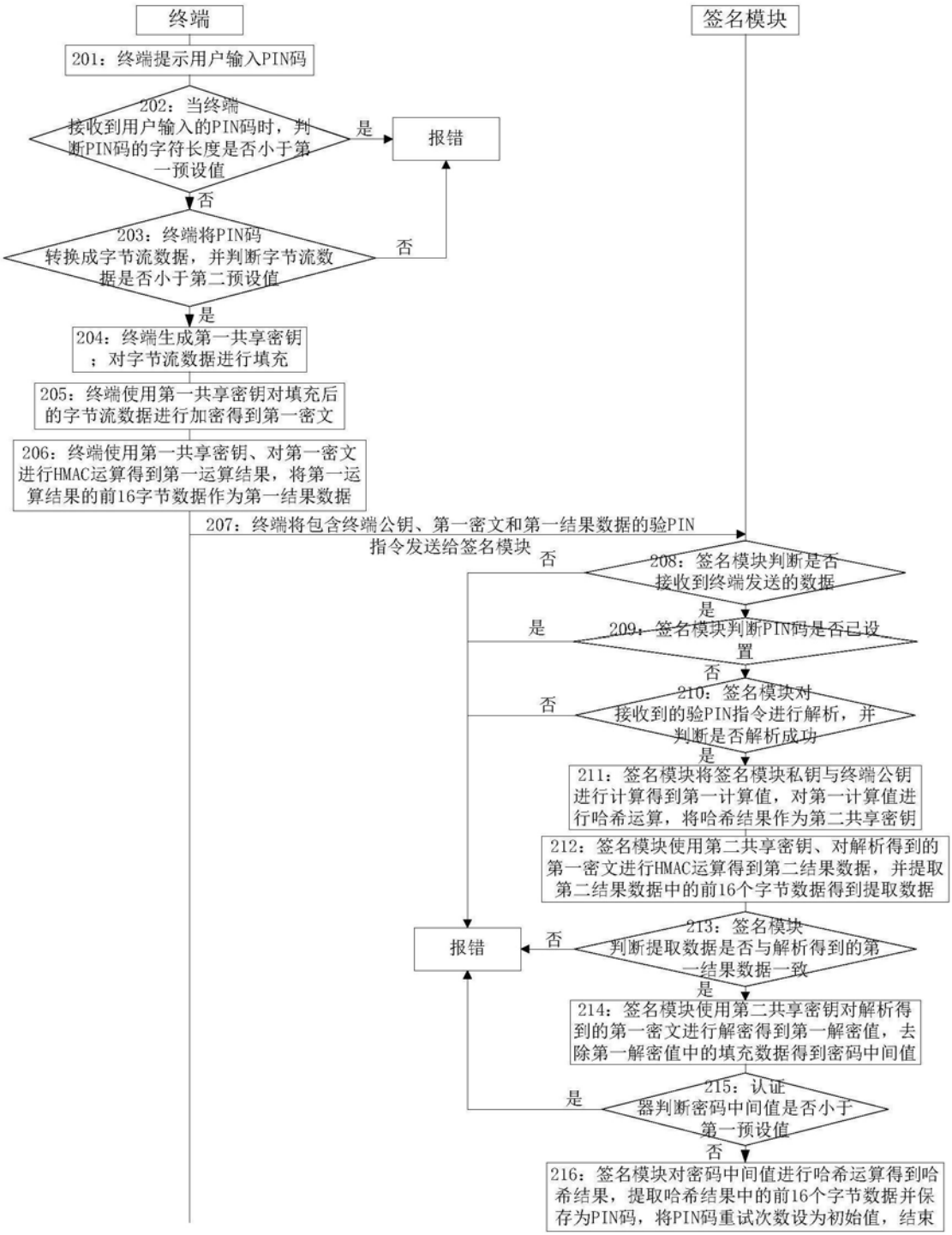

终端
签名模块
201：终端提示用户输入PIN码
202：当终端接收到用户输入的PIN码时，判断PIN码的字符长度是否小于第一预设值
是
报错
否
203：终端将PIN码转换成字节流数据，并判断字节流数据是否小于第二预设值
否
是
204：终端生成第一共享密钥；对字节流数据进行填充
205：终端使用第一共享密钥对填充后的字节流数据进行加密得到第一密文
206：终端使用第一共享密钥、对第一密文进行HMAC运算得到第一运算结果，将第一运算结果的前16字节数据作为第一结果数据
207：终端将包含终端公钥、第一密文和第一结果数据的验PIN指令发送给签名模块
否
208：签名模块判断是否接收到终端发送的数据
是
是
209：签名模块判断PIN码是否已设置
否
否
210：签名模块对接收到的验PIN指令进行解析，并判断是否解析成功
是
211：签名模块将签名模块私钥与终端公钥进行计算得到第一计算值，对第一计算值进行哈希运算，将哈希结果作为第二共享密钥
212：签名模块使用第二共享密钥、对解析得到的第一密文进行HMAC运算得到第二结果数据，并提取第二结果数据中的前16个字节数据得到提取数据
报错
否
213：签名模块判断提取数据是否与解析得到的第一结果数据一致
是
214：签名模块使用第二共享密钥对解析得到的第一密文进行解密得到第一解密值，去除第一解密值中的填充数据得到密码中间值
是
215：认证器判断密码中间值是否小于第一预设值
否
216：签名模块对密码中间值进行哈希运算得到哈希结果，提取哈希结果中的前16个字节数据并保存为PIN码，将PIN码重试次数设为初始值，结束

图2

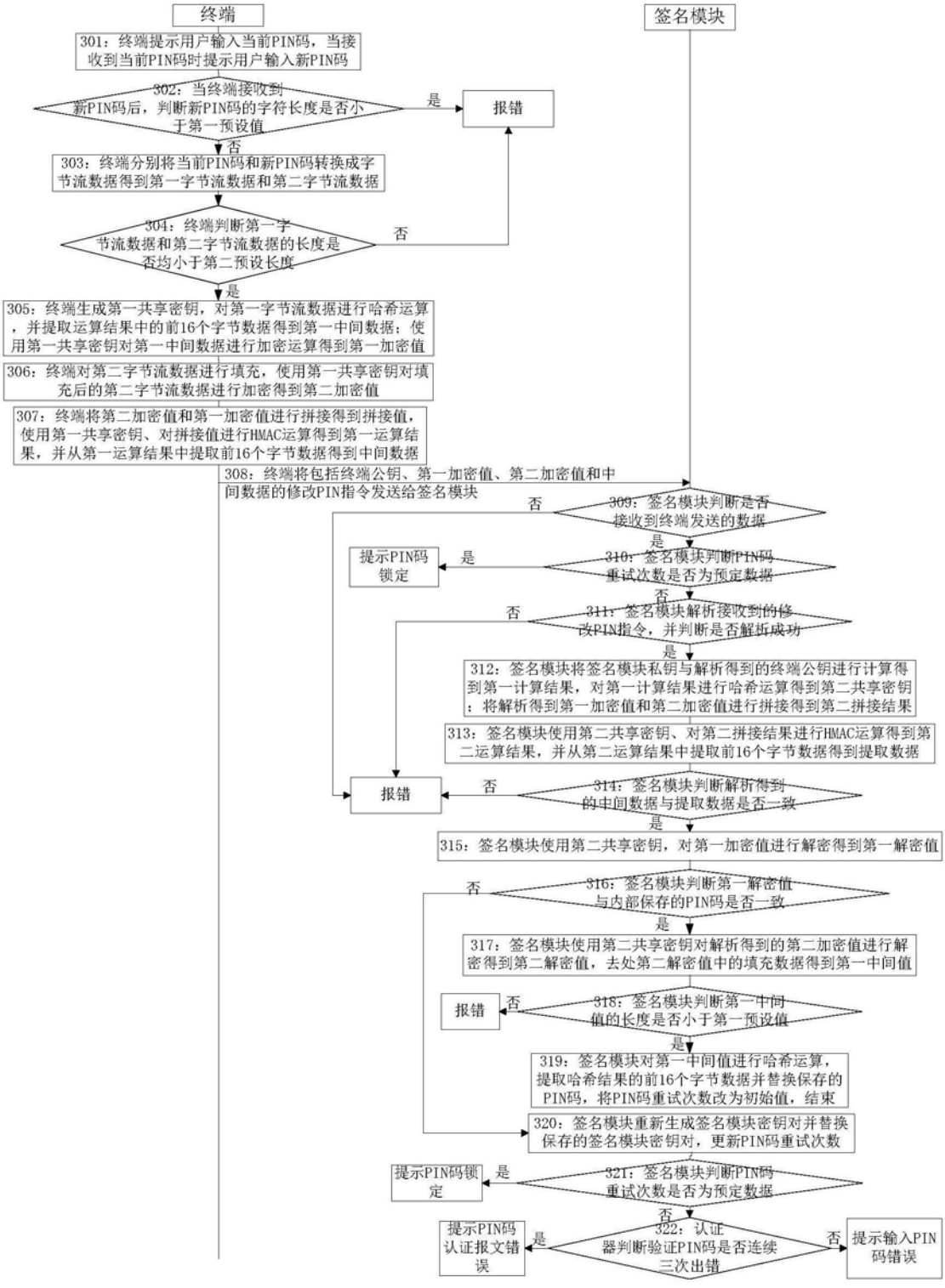

终端
签名模块
301：终端提示用户输入当前PIN码，当接收到当前PIN码时提示用户输入新PIN码
302：当终端接收到新PIN码后，判断新PIN码的字符长度是否小于第一预设值
是
报错
否
303：终端分别将当前PIN码和新PIN码转换成字节流数据得到第一字节流数据和第二字节流数据
304：终端判断第一字节流数据和第二字节流数据的长度是否均小于第二预设长度
否
是
305：终端生成第一共享密钥，对第一字节流数据进行哈希运算，并提取运算结果中的前16个字节数据得到第一中间数据；使用第一共享密钥对第一中间数据进行加密运算得到第一加密值
306：终端对第二字节流数据进行填充，使用第一共享密钥对填充后的第二字节流数据进行加密得到第二加密值
307：终端将第二加密值和第一加密值进行拼接得到拼接值，使用第一共享密钥、对拼接值进行HMAC运算得到第一运算结果，并从第一运算结果中提取前16个字节数据得到中间数据
308：终端将包括终端公钥、第一加密值、第二加密值和中间数据的修改PIN指令发送给签名模块
309：签名模块判断是否接收到终端发送的数据
否
是
提示PIN码锁定
是
310：签名模块判断PIN码重试次数是否为预定数据
否
否
311：签名模块解析接收到的修改PIN指令，并判断是否解析成功
是
312：签名模块将签名模块私钥与解析得到的终端公钥进行计算得到第一计算结果，对第一计算结果进行哈希运算得到第二共享密钥；将解析得到第一加密值和第二加密值进行拼接得到第二拼接结果
313：签名模块使用第二共享密钥、对第二拼接结果进行HMAC运算得到第二运算结果，并从第二运算结果中提取前16个字节数据得到提取数据
报错
否
314：签名模块判断解析得到的中间数据与提取数据是否一致
是
315：签名模块使用第二共享密钥，对第一加密值进行解密得到第一解密值
否
316：签名模块判断第一解密值与内部保存的PIN码是否一致
是
317：签名模块使用第二共享密钥对解析得到的第二加密值进行解密得到第二解密值，去处第二解密值中的填充数据得到第一中间值
报错
否
318：签名模块判断第一中间值的长度是否小于第一预设值
是
319：签名模块对第一中间值进行哈希运算，提取哈希结果的前16个字节数据并替换保存的PIN码，将PIN码重试次数改为初始值，结束
320：签名模块重新生成签名模块密钥对并替换保存的签名模块密钥对，更新PIN码重试次数
提示PIN码锁定
是
321：签名模块判断PIN码重试次数是否为预定数据
否
提示PIN码认证报文错误
是
322：认证器判断验证PIN码是否连续三次出错
否
提示输入PIN码错误

图3

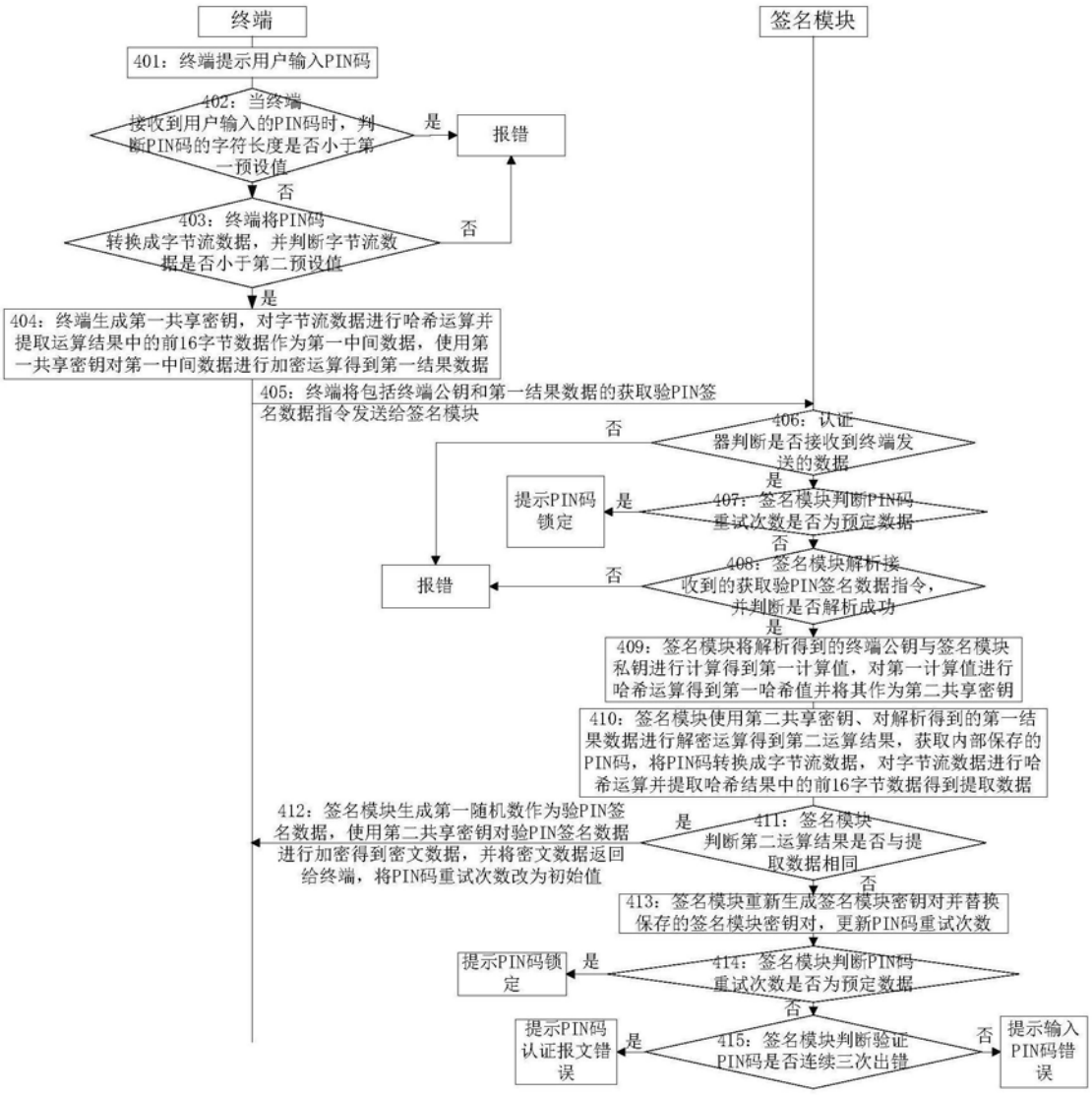

终端
签名模块
401：终端提示用户输入PIN码
402：当终端接收到用户输入的PIN码时，判断PIN码的字符长度是否小于第一预设值
是
报错
否
403：终端将PIN码转换成字节流数据，并判断字节流数据是否小于第二预设值
否
是
404：终端生成第一共享密钥，对字节流数据进行哈希运算并提取运算结果中的前16字节数据作为第一中间数据，使用第一共享密钥对第一中间数据进行加密运算得到第一结果数据
405：终端将包括终端公钥和第一结果数据的获取验PIN签名数据指令发送给签名模块
406：认证器判断是否接收到终端发送的数据
否
是
提示PIN码锁定
是
407：签名模块判断PIN码重试次数是否为预定数据
否
报错
否
408：签名模块解析接收到的获取验PIN签名数据指令，并判断是否解析成功
是
409：签名模块将解析得到的终端公钥与签名模块私钥进行计算得到第一计算值，对第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥
410：签名模块使用第二共享密钥、对解析得到的第一结果数据进行解密运算得到第二运算结果，获取内部保存的PIN码，将PIN码转换成字节流数据，对字节流数据进行哈希运算并提取哈希结果中的前16字节数据得到提取数据
412：签名模块生成第一随机数作为验PIN签名数据，使用第二共享密钥对验PIN签名数据进行加密得到密文数据，并将密文数据返回给终端，将PIN码重试次数改为初始值
是
411：签名模块判断第二运算结果是否与提取数据相同
否
413：签名模块重新生成签名模块密钥对并替换保存的签名模块密钥对，更新PIN码重试次数
提示PIN码锁定
是
414：签名模块判断PIN码重试次数是否为预定数据
否
提示PIN码认证报文错误
是
415：签名模块判断验证PIN码是否连续三次出错
否
提示输入PIN码错误

图4

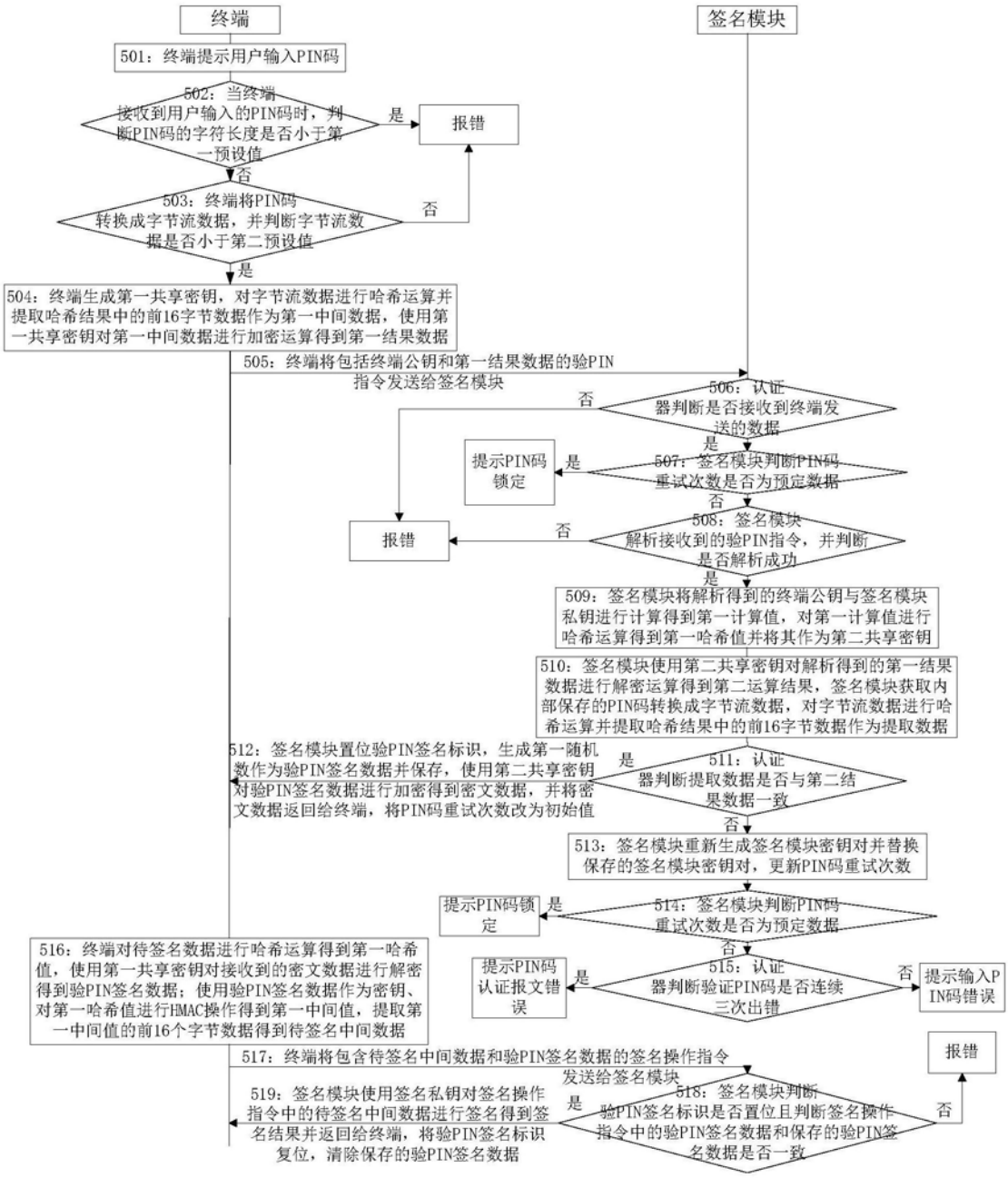

终端
签名模块
501：终端提示用户输入PIN码
502：当终端接收到用户输入的PIN码时，判断PIN码的字符长度是否小于第一预设值
是
报错
否
503：终端将PIN码转换成字节流数据，并判断字节流数据是否小于第二预设值
否
是
504：终端生成第一共享密钥，对字节流数据进行哈希运算并提取哈希结果中的前16字节数据作为第一中间数据，使用第一共享密钥对第一中间数据进行加密运算得到第一结果数据
505：终端将包括终端公钥和第一结果数据的验PIN指令发送给签名模块
506：认证器判断是否接收到终端发送的数据
否
是
507：签名模块判断PIN码重试次数是否为预定数据
是
提示PIN码锁定
否
508：签名模块解析接收到的验PIN指令，并判断是否解析成功
否
报错
是
509：签名模块将解析得到的终端公钥与签名模块私钥进行计算得到第一计算值，对第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥
510：签名模块使用第二共享密钥对解析得到的第一结果数据进行解密运算得到第二运算结果，签名模块获取内部保存的PIN码转换成字节流数据，对字节流数据进行哈希运算并提取哈希结果中的前16字节数据作为提取数据
511：认证器判断提取数据是否与第二结果数据一致
是
512：签名模块置位验PIN签名标识，生成第一随机数作为验PIN签名数据并保存，使用第二共享密钥对验PIN签名数据进行加密得到密文数据，并将密文数据返回给终端，将PIN码重试次数改为初始值
否
513：签名模块重新生成签名模块密钥对并替换保存的签名模块密钥对，更新PIN码重试次数
514：签名模块判断PIN码重试次数是否为预定数据
是
提示PIN码锁定
否
515：认证器判断验证PIN码是否连续三次出错
是
提示PIN码认证报文错误
否
提示输入PIN码错误
516：终端对待签名数据进行哈希运算得到第一哈希值，使用第一共享密钥对接收到的密文数据进行解密得到验PIN签名数据；使用验PIN签名数据作为密钥、对第一哈希值进行HMAC操作得到第一中间值，提取第一中间值的前16个字节数据得到待签名中间数据
517：终端将包含待签名中间数据和验PIN签名数据的签名操作指令发送给签名模块
518：签名模块判断验PIN签名标识是否置位且判断签名操作指令中的验PIN签名数据和保存的验PIN签名数据是否一致
是
否
报错
519：签名模块使用签名私钥对签名操作指令中的待签名中间数据进行签名得到签名结果并返回给终端，将验PIN签名标识复位，清除保存的验PIN签名数据

图5

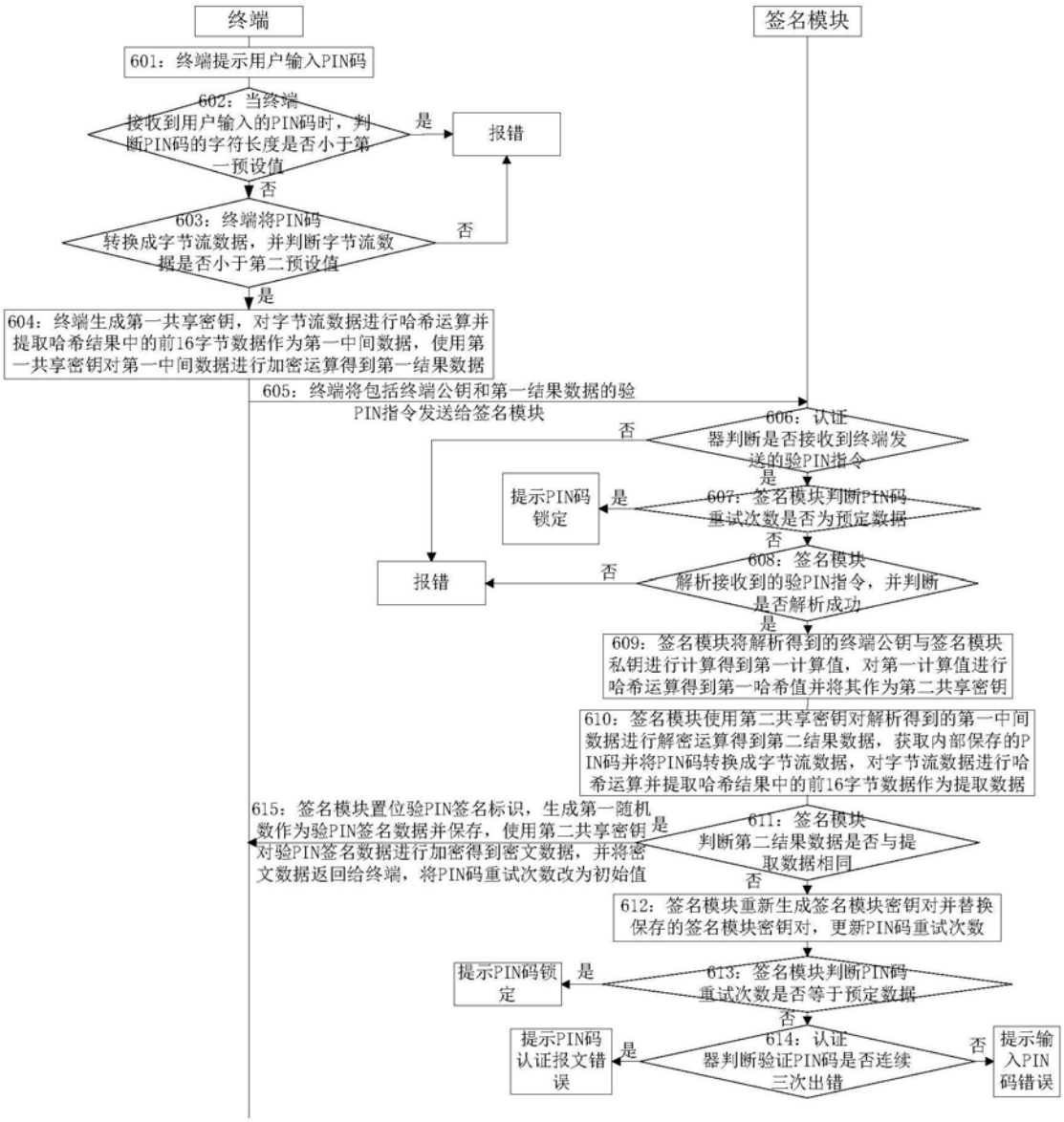

终端
签名模块
601：终端提示用户输入PIN码
602：当终端接收到用户输入的PIN码时，判断PIN码的字符长度是否小于第一预设值
是
报错
否
603：终端将PIN码转换成字节流数据，并判断字节流数据是否小于第二预设值
否
是
604：终端生成第一共享密钥，对字节流数据进行哈希运算并提取哈希结果中的前16字节数据作为第一中间数据，使用第一共享密钥对第一中间数据进行加密运算得到第一结果数据
605：终端将包括终端公钥和第一结果数据的验PIN指令发送给签名模块
606：认证器判断是否接收到终端发送的验PIN指令
否
是
提示PIN码锁定
是
607：签名模块判断PIN码重试次数是否为预定数据
否
报错
否
608：签名模块解析接收到的验PIN指令，并判断是否解析成功
是
609：签名模块将解析得到的终端公钥与签名模块私钥进行计算得到第一计算值，对第一计算值进行哈希运算得到第一哈希值并将其作为第二共享密钥
610：签名模块使用第二共享密钥对解析得到的第一中间数据进行解密运算得到第二结果数据，获取内部保存的PIN码并将PIN码转换成字节流数据，对字节流数据进行哈希运算并提取哈希结果中的前16字节数据作为提取数据
615：签名模块置位验PIN签名标识，生成第一随机数作为验PIN签名数据并保存，使用第二共享密钥对验PIN签名数据进行加密得到密文数据，并将密文数据返回给终端，将PIN码重试次数改为初始值
是
611：签名模块判断第二结果数据是否与提取数据相同
否
612：签名模块重新生成签名模块密钥对并替换保存的签名模块密钥对，更新PIN码重试次数
提示PIN码锁定
是
613：签名模块判断PIN码重试次数是否等于预定数据
否
提示PIN码认证报文错误
是
614：认证器判断验证PIN码是否连续三次出错
否
提示输入PIN码错误

图6

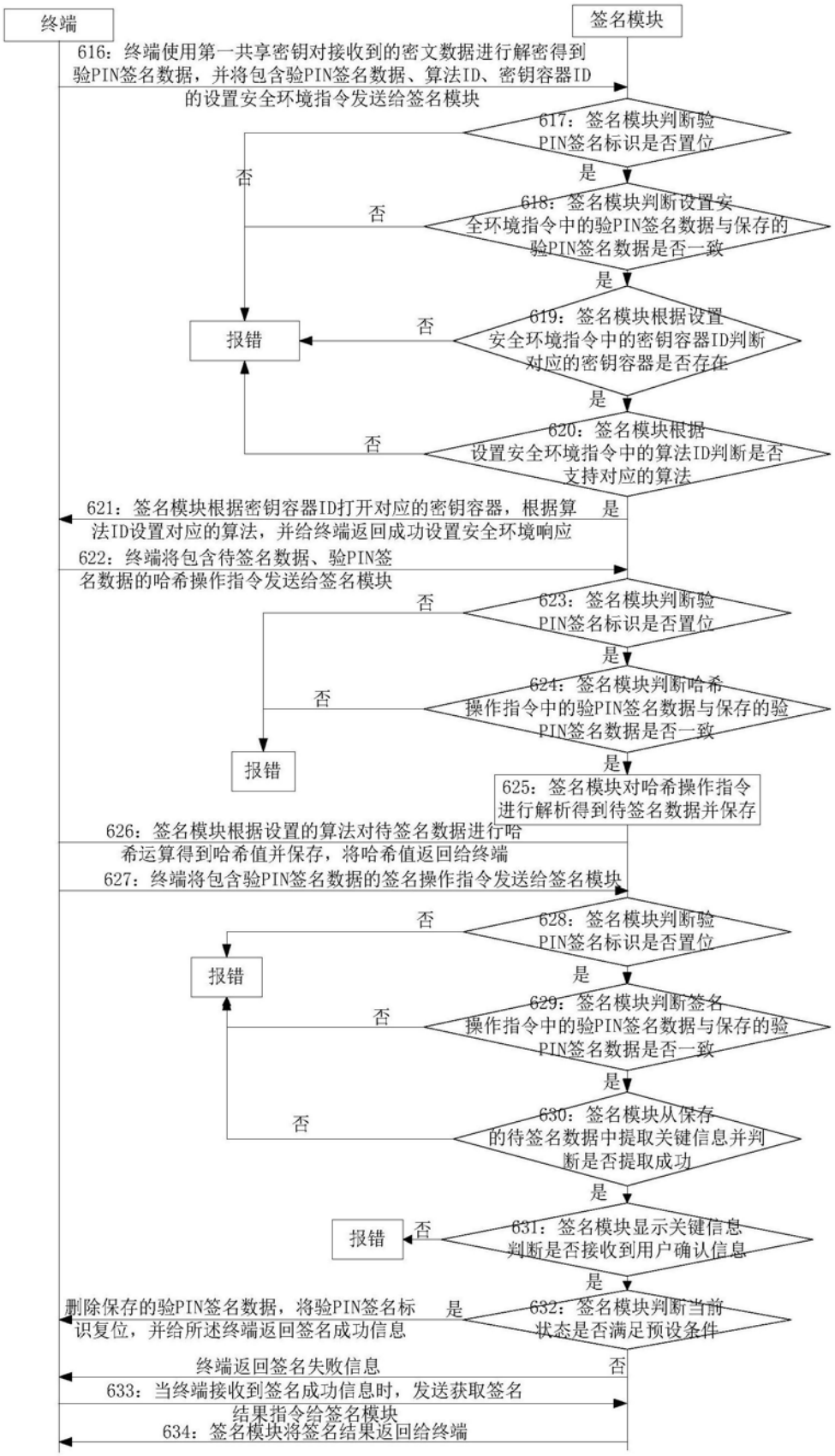

终端
签名模块
616：终端使用第一共享密钥对接收到的密文数据进行解密得到验PIN签名数据，并将包含验PIN签名数据、算法ID、密钥容器ID的设置安全环境指令发送给签名模块
617：签名模块判断验PIN签名标识是否置位
否
是
618：签名模块判断设置安全环境指令中的验PIN签名数据与保存的验PIN签名数据是否一致
否
是
619：签名模块根据设置安全环境指令中的密钥容器ID判断对应的密钥容器是否存在
否
报错
是
620：签名模块根据设置安全环境指令中的算法ID判断是否支持对应的算法
否
是
621：签名模块根据密钥容器ID打开对应的密钥容器，根据算法ID设置对应的算法，并给终端返回成功设置安全环境响应
622：终端将包含待签名数据、验PIN签名数据的哈希操作指令发送给签名模块
623：签名模块判断验PIN签名标识是否置位
否
是
624：签名模块判断哈希操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致
否
报错
是
625：签名模块对哈希操作指令进行解析得到待签名数据并保存
626：签名模块根据设置的算法对待签名数据进行哈希运算得到哈希值并保存，将哈希值返回给终端
627：终端将包含验PIN签名数据的签名操作指令发送给签名模块
628：签名模块判断验PIN签名标识是否置位
否
报错
是
629：签名模块判断签名操作指令中的验PIN签名数据与保存的验PIN签名数据是否一致
否
是
630：签名模块从保存的待签名数据中提取关键信息并判断是否提取成功
否
是
631：签名模块显示关键信息判断是否接收到用户确认信息
报错
否
是
632：签名模块判断当前状态是否满足预设条件
是
删除保存的验PIN签名数据，将验PIN签名标识复位，并给所述终端返回签名成功信息
否
终端返回签名失败信息
633：当终端接收到签名成功信息时，发送获取签名结果指令给签名模块
634：签名模块将签名结果返回给终端

图7


一种安全签名的实现装置
签名模块
接收子模块71
第一生成子模块72
第一判断子模块76
第一验证子模块73
签名子模块77
第二生成子模块74
判断清除子模块78
第三生成子模块75
发送子模块79

图8