(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111917710 B
(45)授权公告日 2022.06.24

(21)申请号 202010534695.7

(22)申请日 2020.06.12

(65)同一申请的已公布的文献号
申请公布号 CN 111917710 A

(43)申请公布日 2020.11.10

(73)专利权人 北京智芯微电子科技有限公司
地址 102200 北京市昌平区南邵镇南中路电网产业大厦
专利权人 国网信息通信产业集团有限公司

(72)发明人 崔永旭 李延 侯占斌 杜君 郭飞 田羽 季叶庆

(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
专利代理师 王佳璐

(51)Int.Cl.
H04L 9/40(2022.01)
G06F 21/78(2013.01)
G06F 21/77(2013.01)
G06F 21/62(2013.01)

(56)对比文件
CN 110765438 A,2020.02.07
CN 106027235 A,2016.10.12
CN 109145568 A,2019.01.04
CN 108683688 A,2018.10.19
CN 109962784 A,2019.07.02
CN 106953732 A,2017.07.14

审查员 肖敬伟

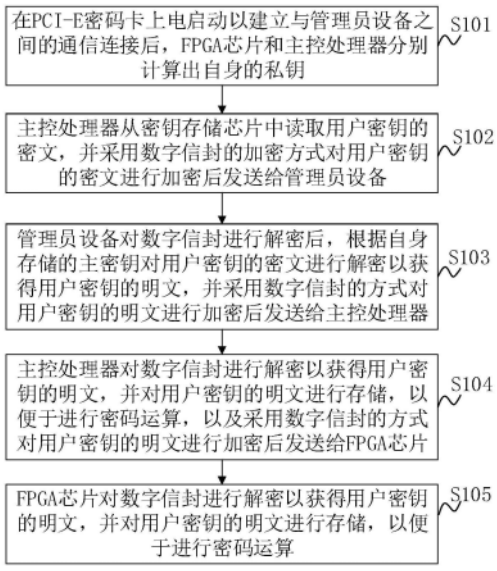
权利要求书2页 说明书10页 附图2页

(54)发明名称

PCI-E密码卡及其密钥保护方法、计算机可读存储介质

(57)摘要

本发明公开了一种PCI-E密码卡及其密钥保护方法、计算机可读存储介质，方法包括：在PCI-E密码卡上电启动后，FPGA芯片和主控处理器分别计算出自身的私钥；主控处理器从密钥存储芯片中读取用户密钥的密文，并采用数字信封的加密方式对其加密后发送给管理员设备；管理员设备对数字信封解密后，根据主密钥对用户密钥的密文解密以获得用户密钥的明文，并采用数字信封的方式对其加密后发送给主控处理器；主控处理器对数字信封解密以获得用户密钥的明文，并对其进行存储和使用，以及采用数字信封的方式对其加密后发送给FPGA芯片；FPGA芯片对数字信封解密以获得用户密钥的明文，并对其进行存储和使用。由此，有效保证了用户密钥在上述各个部件之间传输的安全性。



CN 111917710 B

1.一种PCI-E密码卡的密钥保护方法,其特征在于,所述PCI-E密码卡包括主控处理器、与所述主控处理器相连的密钥存储芯片、与所述主控处理器相连的FPGA芯片,所述主控处理器与外部的管理员设备进行通信,包括以下步骤:

在所述PCI-E密码卡上电启动以建立与所述管理员设备之间的通信连接后,所述FPGA芯片和所述主控处理器分别计算出自身的私钥;

所述主控处理器从所述密钥存储芯片中读取用户密钥的密文,并基于所述管理员设备的公钥采用数字信封的加密方式对所述用户密钥的密文进行加密后发送给所述管理员设备;

所述管理员设备基于自身的私钥对数字信封进行解密后,根据自身存储的主密钥对所述用户密钥的密文进行解密以获得所述用户密钥的明文,并基于所述主控处理器的公钥采用数字信封的方式对所述用户密钥的明文进行加密后发送给所述主控处理器;

所述主控处理器基于自身的私钥对数字信封进行解密以获得所述用户密钥的明文,并对所述用户密钥的明文进行存储,以便于进行密码运算,以及基于所述FPGA芯片的公钥采用数字信封的方式对所述用户密钥的明文进行加密后发送给所述FPGA芯片;

所述FPGA芯片基于自身的私钥对数字信封进行解密以获得所述用户密钥的明文,并对所述用户密钥的明文进行存储,以便于进行密码运算。

2.如权利要求1所述的PCI-E密码卡的密钥保护方法,其特征在于,当外部的计算机调用所述PCI-E密码卡进行密码运算时,所述FPGA芯片使用存储的用户密钥进行密码运算,并将运算结果返回给外部的计算机。

3.如权利要求1所述的PCI-E密码卡的密钥保护方法,其特征在于,在所述PCI-E密码卡上电启动时,通过所述管理员设备输入管理员登录口令,并在登录成功后建立所述PCI-E密码卡与所述管理员设备之间的通信连接,其中,

所述FPGA芯片读取随机数,并根据管理员登录口令、随机数和FPGA芯片ID计算自身的私钥,以及将自身的私钥存储在FPGA芯片的寄存器中;

所述主控处理器读取随机数,并根据管理员登录口令、随机数和主控处理器ID计算自身的私钥,以及将自身的私钥存储在主控处理器的内存中。

4.如权利要求1所述的PCI-E密码卡的密钥保护方法,其特征在于,当外部的计算机调用密钥生成、更新功能时,所述主控处理器将修改后的用户密钥以数字信封的加密方式发送给所述管理员设备,所述管理员设备对数字信封进行解密后,使用自身的主密钥对修改后的用户密钥进行加密后,并以数字信封的加密方式发送给所述主控处理器,以便所述主控处理器将修改后的用户密钥的密文存储在所述密钥存储芯片中,同时与所述FPGA芯片进行安全传输。

5.如权利要求1所述的PCI-E密码卡的密钥保护方法,其特征在于,当所述PCI-E密码卡掉电时,所述主控处理器和所述FPGA芯片中存储的用户密钥的明文自动消失。

6.如权利要求1-5中任一项所述的PCI-E密码卡的密钥保护方法,其特征在于,在所述PCI-E密码卡首次使用时,还对所述PCI-E密码卡进行初始化,以在所述管理员设备内部生成用于加密用户密钥的主密钥、密钥对,并以密钥对中的公钥为所述管理员设备申请数字证书,同时分别为所述主控处理器和所述FPGA芯片生成各自的密钥对,并分别以各自的密钥对中的公钥为所述主控处理器和所述FPGA芯片申请数字证书。

7.一种计算机可读存储介质,其特征在于,其上存储有PCI-E密码卡的密钥保护程序,该保护程序被处理器执行时实现如权利要求1-6中任一项所述的PCI-E密码卡的密钥保护方法。

8.一种PCI-E密码卡,其特征在于,包括主控处理器、与所述主控处理器相连的密钥存储芯片、与所述主控处理器相连的FPGA芯片,其中,

在所述PCI-E密码卡上电启动后,所述主控处理器建立与外部的管理员设备之间的通信连接,并计算出自身的私钥,所述FPGA芯片计算出自身的私钥;

所述主控处理器从所述密钥存储芯片中读取用户密钥的密文,并基于所述管理员设备的公钥采用数字信封的加密方式对所述用户密钥的密文进行加密后发送给所述管理员设备;

所述管理员设备基于自身的私钥对数字信封进行解密后,根据自身存储的主密钥对所述用户密钥的密文进行解密以获得所述用户密钥的明文,并基于所述主控处理器的公钥采用数字信封的方式对所述用户密钥的明文进行加密后发送给所述主控处理器;

所述主控处理器基于自身的私钥对数字信封进行解密以获得所述用户密钥的明文,并对所述用户密钥的明文进行存储,以便于进行密码运算,以及基于所述FPGA芯片的公钥采用数字信封的方式对所述用户密钥的明文进行加密后发送给所述FPGA芯片;

所述FPGA芯片基于自身的私钥对数字信封进行解密以获得所述用户密钥的明文,并对所述用户密钥的明文进行存储,以便于进行密码运算。

9.如权利要求8所述的PCI-E密码卡,其特征在于,所述FPGA芯片在与外部的计算机建立通信连接后,如果外部的计算机调用所述PCI-E密码卡进行密码运算,所述FPGA芯片使用存储的用户密钥进行密码运算,并将运算结果返回给外部的计算机。

10.如权利要求8所述的PCI-E密码卡,其特征在于,所述主控处理器通过所述管理员设备输入管理员登录口令,并在登录成功后建立与所述管理员设备之间的通信连接,其中,

所述FPGA芯片读取随机数,并根据管理员登录口令、随机数和FPGA芯片ID计算自身的私钥,以及将自身的私钥存储在FPGA芯片的寄存器中;

所述主控处理器读取随机数,并根据管理员登录口令、随机数和主控处理器ID计算自身的私钥,以及将自身的私钥存储在主控处理器的内存中。

11.如权利要求8所述的PCI-E密码卡,其特征在于,当外部的计算机调用密钥生成、更新功能时,所述主控处理器将修改后的用户密钥以数字信封的加密方式发送给所述管理员设备,所述管理员设备对数字信封进行解密后,使用自身的主密钥对修改后的用户密钥进行加密后,并以数字信封的加密方式发送给所述主控处理器,以便所述主控处理器将修改后的用户密钥的密文存储在所述密钥存储芯片中,同时与所述FPGA芯片进行安全传输。

12.如权利要求8所述的PCI-E密码卡,其特征在于,当所述PCI-E密码卡掉电时,所述主控处理器和所述FPGA芯片中存储的用户密钥的明文自动消失。

13.如权利要求8-12中任一项所述的PCI-E密码卡,其特征在于,所述PCI-E密码卡在首次使用时,还进行初始化,以便在所述管理员设备内部生成用于加密用户密钥的主密钥、密钥对,并以密钥对中的公钥为所述管理员设备申请数字证书,同时分别为所述主控处理器和所述FPGA芯片生成各自的密钥对,并分别以各自的密钥对中的公钥为所述主控处理器和所述FPGA芯片申请数字证书。

PCI-E密码卡及其密钥保护方法、计算机可读存储介质

技术领域

[0001] 本发明涉及计算机信息安全技术领域，尤其涉及一种PCI-E密码卡的密钥保护方法、一种计算机可读存储介质和一种PCI-E密码卡。

背景技术

[0002] 密码技术主要用于保障云计算、大数据、物联网、工业控制等各种信息系统中的信息安全，包括机密性、完整性、真实性和抗抵赖性。PCI-E(Peripheral Component Interconnect-Express，高速串行计算机扩展总线标准)密码卡是一种采用PCI-E总线接口的板卡设备，为计算机或服务器提供数据加解密、消息鉴别、数字签名、身份认证等功能，也是服务器密码机、签名验签服务器、SSL VPN(指采用SSL协议来实现远程接入的一种VPN技术)、IPSec VPN(指采用IPSec协议来实现远程接入的一种VPN技术)等密码设备的核心部件。

[0003] 密钥是PCI-E密码卡最重要的秘密信息，包括用户的私钥、对称密钥等，必须保证其在存储、传输、使用等过程中的安全。相关技术中，PCI-E密码卡中的密钥主要以密文的形式存储在密码卡的密钥存储芯片中，在密码卡上电启动且管理员登录成功后，密码卡上的CPU处理器读取密文密钥，并对该密文密钥解密后，以明文形式在CPU处理器、FPGA(Field Programmable Gate Array，现场可编程逻辑门阵列)芯片以及管理员设备之间实现密钥同步，用于数据加解密、数字签名等密码运算。

[0004] 该方式主要解决了PCI-E密码卡的密钥存储安全问题，即密钥以密文的形式存储在密码卡的密钥存储芯片中，从而可以有效防止通过拆卸密码卡上的存储芯片来读取密钥信息，但由于CPU处理器、FPGA芯片、管理员设备之间的数据传输是以明文形式传输的，因而存在密钥被监听、窃取的安全风险。

发明内容

[0005] 本发明旨在至少在一定程度上解决相关技术中的技术问题之一。为此，本发明的第一个目的在于提出一种PCI-E密码卡的密钥保护方法，通过在传输过程中采用数字信封的加密方式对用户密钥进行加密，即以对称和非对称相结合的加密方式对用户密钥进行加密，从而有效保证传输过程中密钥的安全性。

[0006] 本发明的第二个目的在于一种计算机可读存储介质。

[0007] 本发明的第三个目的在于一种PCI-E密码卡。

[0008] 为达到上述目的，本发明第一方面实施例提出了一种PCI-E密码卡的密钥保护方法，PCI-E密码卡包括主控处理器、与主控处理器相连的密钥存储芯片、与主控处理器相连的FPGA芯片，主控处理器与外部的管理员设备进行通信，包括以下步骤：在PCI-E密码卡上电启动以建立与管理员设备之间的通信连接后，FPGA芯片和主控处理器分别计算出自身的私钥；主控处理器从密钥存储芯片中读取用户密钥的密文，并采用数字信封的加密方式对用户密钥的密文进行加密后发送给管理员设备；管理员设备对数字信封进行解密后，根据

自身存储的主密钥对用户密钥的密文进行解密以获得用户密钥的明文,并采用数字信封的方式对用户密钥的明文进行加密后发送给主控处理器;主控处理器对数字信封进行解密以获得用户密钥的明文,并对用户密钥的明文进行存储,以便于进行密码运算,以及采用数字信封的方式对用户密钥的明文进行加密后发送给FPGA芯片;FPGA芯片对数字信封进行解密以获得用户密钥的明文,并对用户密钥的明文进行存储,以便于进行密码运算。

[0009] 根据本发明实施例的PCI-E密码卡的密钥保护方法,在PCI-E密码卡上电启动以建立与管理员设备之间的通信连接后,FPGA芯片和主控处理器分别计算出自身的私钥,并且主控处理器从密钥存储芯片中读取用户密钥的密文,并采用数字信封的加密方式对用户密钥的密文进行加密后发送给管理员设备。管理员设备对数字信封进行解密后,根据自身存储的主密钥对用户密钥的密文进行解密以获得用户密钥的明文,并采用数字信封的方式对用户密钥的明文进行加密后发送给主控处理器。主控处理器对数字信封进行解密以获得用户密钥的明文,并对用户密钥的明文进行存储,以便于进行密码运算,以及采用数字信封的方式对用户密钥的明文进行加密后发送给FPGA芯片;FPGA芯片对数字信封进行解密以获得用户密钥的明文,并对用户密钥的明文进行存储,以便于进行密码运算。由此,在用户密钥传输的过程中,采用数字信封的加密方式对用户密钥进行加密,即以对称和非对称相结合的加密方式对用户密钥进行加密,从而有效保证用户密钥在主控处理器、FPGA芯片和管理员设备之间传输的安全性。

[0010] 另外,根据本发明上述实施例的PCI-E密码卡的密钥保护方法,还可以具有如下的附加技术特征:

[0011] 根据本发明的一个实施例,当外部的计算机调用PCI-E密码卡进行密码运算时,FPGA芯片使用存储的用户密钥进行密码运算,并将运算结果返回给外部的计算机。

[0012] 根据本发明的一个实施例,在PCI-E密码卡上电启动时,通过管理员设备输入管理员登录口令,并在登录成功后建立PCI-E密码卡与管理员设备之间的通信连接,其中,FPGA芯片读取随机数,并根据管理员登录口令、随机数和FPGA芯片ID计算自身的私钥,以及将自身的私钥存储在FPGA芯片的寄存器中;主控处理器读取随机数,并根据管理员登录口令、随机数和主控处理器ID计算自身的私钥,以及将自身的私钥存储在主控处理器的内存中。

[0013] 根据本发明的一个实施例,当外部的计算机调用密钥生成、更新功能时,主控处理器将修改后的用户密钥以数字信封的加密方式发送给管理员设备,管理员设备对数字信封进行解密后,使用自身的主密钥对修改后的用户密钥进行加密后,并以数字信封的加密方式发送给主控处理器,以便主控处理器将修改后的用户密钥的密文存储在密钥存储芯片中,同时与FPGA芯片进行安全传输。

[0014] 根据本发明的一个实施例,当PCI-E密码卡掉电时,主控处理器和FPGA芯片中存储的用户密钥的明文自动消失。

[0015] 根据本发明的一个实施例,在PCI-E密码卡首次使用时,还对PCI-E密码卡进行初始化,以在管理员设备内部生成用于加密用户密钥的主密钥、密钥对,并以密钥对中的公钥为管理员设备申请数字证书,同时分别为主控处理器和FPGA芯片生成各自的密钥对,并分别以各自的密钥对中的公钥为主控处理器和FPGA芯片申请数字证书。

[0016] 为达到上述目的,本发明第二方面实施例提出了一种计算机可读存储介质,其上存储有PCI-E密码卡的密钥保护程序,该保护程序被处理器执行时实现上述的PCI-E密码卡

的密钥保护方法。

[0017] 根据本发明实施例的计算机可读存储介质，在用户密钥传输的过程中，采用数字信封的加密方式对用户密钥进行加密，即以对称和非对称相结合的加密方式对用户密钥进行加密，从而有效保证用户密钥在主控处理器、FPGA芯片和管理员设备之间传输的安全性。

[0018] 为达到上述目的，本发明第三方面实施例提出的一种PCI-E密码卡，包括主控处理器、与主控处理器相连的密钥存储芯片、与主控处理器相连的FPGA芯片，其中，在PCI-E密码卡上电启动后，主控处理器建立与外部的管理员设备之间的通信连接，并计算出自身的私钥，FPGA芯片计算出自身的私钥；主控处理器从密钥存储芯片中读取用户密钥的密文，并采用数字信封的加密方式对用户密钥的密文进行加密后发送给管理员设备；管理员设备对数字信封进行解密后，根据自身存储的主密钥对用户密钥的密文进行解密以获得用户密钥的明文，并采用数字信封的方式对用户密钥的明文进行加密后发送给主控处理器；主控处理器对数字信封进行解密以获得用户密钥的明文，并对用户密钥的明文进行存储，以便于进行密码运算，以及采用数字信封的方式对用户密钥的明文进行加密后发送给FPGA芯片；FPGA芯片对数字信封进行解密以获得用户密钥的明文，并对用户密钥的明文进行存储，以便于进行密码运算。

[0019] 根据本发明实施例的PCI-E密码卡，在其上电启动后，主控处理器建立与外部的管理员设备之间的通信连接，并计算出自身的私钥，FPGA芯片计算出自身的私钥，并且主控处理器从密钥存储芯片中读取用户密钥的密文，并采用数字信封的加密方式对用户密钥的密文进行加密后发送给管理员设备。管理员设备对数字信封进行解密后，根据自身存储的主密钥对用户密钥的密文进行解密以获得用户密钥的明文，并采用数字信封的方式对用户密钥的明文进行加密后发送给主控处理器。主控处理器对数字信封进行解密以获得用户密钥的明文，并对用户密钥的明文进行存储，以便于进行密码运算，以及采用数字信封的方式对用户密钥的明文进行加密后发送给FPGA芯片。FPGA芯片对数字信封进行解密以获得用户密钥的明文，并对用户密钥的明文进行存储，以便于进行密码运算。由此，在用户密钥传输的过程中，采用数字信封的加密方式对用户密钥进行加密，即以对称和非对称相结合的加密方式对用户密钥进行加密，从而有效保证用户密钥在主控处理器、FPGA芯片和管理员设备之间传输的安全性。

[0020] 另外，根据本发明上述实施例的PCI-E密码卡，还可以具有如下的附加技术特征：

[0021] 根据本发明的一个实施例，FPGA芯片在与外部的计算机建立通信连接后，如果外部的计算机调用PCI-E密码卡进行密码运算，FPGA芯片使用存储的用户密钥进行密码运算，并将运算结果返回给外部的计算机。

[0022] 根据本发明的一个实施例，主控处理器通过管理员设备输入管理员登录口令，并在登录成功后建立与管理员设备之间的通信连接，其中，FPGA芯片读取随机数，并根据管理员登录口令、随机数和FPGA芯片ID计算自身的私钥，以及将自身的私钥存储在FPGA芯片的寄存器中；主控处理器读取随机数，并根据管理员登录口令、随机数和主控处理器ID计算自身的私钥，以及将自身的私钥存储在主控处理器的内存中。

[0023] 根据本发明的一个实施例，当外部的计算机调用密钥生成、更新功能时，主控处理器将修改后的用户密钥以数字信封的加密方式发送给管理员设备，管理员设备对数字信封进行解密后，使用自身的主密钥对修改后的用户密钥进行加密后，并以数字信封的加密方

式发送给主控处理器,以便主控处理器将修改后的用户密钥的密文存储在密钥存储芯片中,同时与FPGA芯片进行安全传输。

[0024] 根据本发明的一个实施例,当PCI-E密码卡掉电时,主控处理器和FPGA芯片中存储的用户密钥的明文自动消失。

[0025] 根据本发明的一个实施例,PCI-E密码卡在首次使用时,还进行初始化,以便在管理员设备内部生成用于加密用户密钥的主密钥、密钥对,并以密钥对中的公钥为管理员设备申请数字证书,同时分别为主控处理器和FPGA芯片生成各自的密钥对,并分别以各自的密钥对中的公钥为主控处理器和FPGA芯片申请数字证书。

[0026] 本发明附加的方面和优点将在下面的描述中部分给出,部分将从下面的描述中变得明显,或通过本发明的实践了解到。

附图说明

[0027] 图1为根据本发明实施例的PCI-E密码卡的结构示意图;

[0028] 图2为根据本发明实施例的PCI-E密码卡的密钥保护方法的流程图。

具体实施方式

[0029] 下面详细描述本发明的实施例,所述实施例的示例在附图中示出,其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的,旨在用于解释本发明,而不能理解为对本发明的限制。

[0030] 下面参考附图描述本发明实施例提出的PCI-E密码卡的密钥保护方法、计算机可读存储介质和PCI-E密码卡。

[0031] 在本申请中,参考图1所示,PCI-E密码卡包括主控处理器、与主控处理器相连的密钥存储芯片、与主控处理器相连的FPGA芯片,主控处理器与外部的管理员设备进行通信。其中,主控处理器可以为DSP(Digital Signal Process,数字信号处理)、ARM(Advanced RISC Machines)等CPU处理器,密钥存储芯片为非易失性存储器,例如Flash芯片、EEPROM(Electrically Erasable Programmable Read Only Memory,带电可擦可编程只读存储器)等,FPGA芯片为可编程逻辑单元,支持PCI-E接口,用于实现密码运算。PCI-E密码卡通过USB接口或者串口等连接外部的管理员设备,管理员设备可以为智能密码钥匙(如USB KEY、U盾)、智能IC卡等,管理员通过持有管理员设备实现对PCI-E密码卡的权限控制和管理配置。

[0032] 图2为根据本发明实施例的PCI-E密码卡的密钥保护方法的流程图。参考图2所示,该PCI-E密码卡的密钥保护方法可包括以下步骤:

[0033] 步骤S101,在PCI-E密码卡上电启动以建立与管理员设备之间的通信连接后,FPGA芯片和主控处理器分别计算出自身的私钥。

[0034] 具体地,在PCI-E密码卡上电启动时,首先需要管理员将管理员设备插接在PCI-E密码卡上,并建立PCI-E密码卡与管理员设备之间的通信连接,只有在通信连接建立成功后,PCI-E密码卡才能正常工作,否则PCI-E密码卡不对外提供任何密码运算或密钥管理功能。

[0035] 根据本发明的一个实施例,在PCI-E密码卡上电启动时,通过管理员设备输入管理

员登录口令,并在登录成功后建立PCI-E密码卡与管理员设备之间的通信连接,其中,FPGA芯片读取随机数,并根据管理员登录口令、随机数和FPGA芯片ID计算自身的私钥,以及将自身的私钥存储在FPGA芯片的寄存器中;主控处理器读取随机数,并根据管理员登录口令、随机数和主控处理器ID计算自身的私钥,以及将自身的私钥存储在主控处理器的内存中。

[0036] 具体而言,在PCI-E密码卡上电启动时,首先由管理员将管理员设备插接在PCI-E密码卡上,并输入管理员登录口令,在管理员登录成功后,PCI-E密码卡与管理员设备之间建立通信连接,PCI-E密码卡开始正常工作。

[0037] 在PCI-E密码卡工作时,FPGA芯片读取预先存储的随机数,并根据管理员登录口令、随机数和FPGA芯片ID按照预设的密钥算法计算获得自身的私钥,例如,按照SM3算法计算出自身的SM2私钥,即SM2私钥=SM3(管理员登录口令+随机数+FPGA芯片ID),其中SM3()表示进行SM3密码杂凑运算,以保证FPGA芯片的私钥的安全性,然后将计算获得的私钥存储至自身的寄存器中。

[0038] 同时,主控处理器读取预先存储的随机数,并根据管理员登录口令、随机数和主控处理器ID按照预设的密钥算法计算获得自身的私钥,例如,按照SM3算法计算出自身的SM2私钥,即SM2私钥=SM3(管理员登录口令+随机数+主控处理器ID),以保证主控处理器的私钥的安全性,然后将计算获得的私钥存储至自身的内存中。

[0039] 由此,通过根据管理员登录口令、随机数和主控处理器ID/FPGA芯片ID按照预设的加密算法生成相应的私钥,如采用SM3杂凑运算生成SM2私钥,可保证主控处理器和FPGA芯片私钥的安全性。

[0040] 步骤S102,主控处理器从密钥存储芯片中读取用户密钥的密文,并采用数字信封的加密方式对用户密钥的密文进行加密后发送给管理员设备。

[0041] 具体而言,通常用户密钥以密文的形式存储在PCI-E密码卡的密钥存储芯片中,以保证用户密钥存储的安全性,同时,为了保证用户密文密钥的解密、传输等过程中的安全性,需要将用于加密用户密钥的主密钥安全存储在PCI-E密码卡之外,例如存储在管理员设备中。

[0042] 当需要在主控处理器、FPGA芯片和管理员设备之间同步用户密钥,以进行数据加解密、数字签名等密码运算时,先由主控处理器从PCI-E密码卡的密钥存储芯片中读取用户密钥的密文,并采用数字信封的加密方式对用户密钥的密文进行加密后,传输给管理员设备,由管理员设备通过主密钥对用户密钥的密文进行解密,以获得用户密钥的明文,然后再将该用户密钥的明文同步至主控处理器、FPGA芯片和管理员设备中。其中,数字信封是一种将对称密钥通过非对称加密的结果分发对称密钥的方法,即采用对称和非对称相结合的加密方式对用户密钥的密文进行加密,从而保证用户密钥传输过程中的安全性。

[0043] 例如,可产生随机SM4对称密钥,通过该对称密钥对用户密钥的密文进行加密,然后用预先存储的管理员设备的数字证书(如SM2数字证书)中的公钥加密SM4对称密钥,并将加密后的用户密钥的密文和加密后的SM4对称密钥一同发送给管理员设备。

[0044] 步骤S103,管理员设备对数字信封进行解密后,根据自身存储的主密钥对用户密钥的密文进行解密以获得用户密钥的明文,并采用数字信封的方式对用户密钥的明文进行加密后发送给主控处理器。

[0045] 具体而言,管理员设备在接收到主控处理器发送的数字信封后,对该数字信封进

行解密,以获得用户密钥的密文,例如,利用预先存储的自身的数字证书(如SM2数字证书)中的私钥对加密后的SM4对称密钥进行解密,得到SM4对称密钥,并利用SM4对称密钥对加密后的用户密钥的密文进行解密,得到用户密钥的密文。然后,管理员设备利用预先存储的主密钥对用户密钥的密文进行解密,得到用户密钥的明文。接着,管理员设备采用数字信封的加密方式对用户密钥的明文加密后,传输给主控处理器,例如,可产生随机SM4对称密钥,通过该对称密钥对用户密钥的明文进行加密,然后用预先存储的主控处理器的数字证书(如SM2数字证书)中的公钥加密SM4对称密钥,并将加密后的用户密钥的明文和加密后的SM4对称密钥一同发送给主控处理器。

[0046] 步骤S104,主控处理器对数字信封进行解密以获得用户密钥的明文,并对用户密钥的明文进行存储,以便于进行密码运算,以及采用数字信封的方式对用户密钥的明文进行加密后发送给FPGA芯片。

[0047] 具体而言,主控处理器在接收到管理员设备发送的数字信封后,对该数字信封进行解密,以获得用户密钥的明文,并对该用户密钥的明文进行存储,例如,利用步骤S101中计算出的主控处理器的私钥,也即预先存储的自身的数字证书(如SM2数字证书)中的私钥,对加密后的SM4对称密钥进行解密,得到SM4对称密钥,并利用SM4对称密钥对加密后的用户密钥的明文进行解密,得到用户密钥的明文,并将其存储至自身的内存中。然后,主控处理器采用数字信封的加密方式对用户密钥的明文加密后,传输给FPGA芯片,例如,可产生随机SM4对称密钥,通过该对称密钥对用户密钥的明文进行加密,然后用预先存储的FPGA芯片的数字证书(如SM2数字证书)中的公钥加密SM4对称密钥,并将加密后的用户密钥的明文和加密后的SM4对称密钥一同发送给FPGA芯片。

[0048] 步骤S105,FPGA芯片对数字信封进行解密以获得用户密钥的明文,并对用户密钥的明文进行存储,以便于进行密码运算。

[0049] 具体而言,FPGA芯片在接收到主控处理器发送的数字信封后,对该数字信封进行解密,以获得用户密钥的明文,并对该用户密钥的明文进行存储,例如,利用步骤S101中计算出的FPGA芯片的私钥,也即预先存储的自身的数字证书(如SM2数字证书)中的私钥,对加密后的SM4对称密钥进行解密,得到SM4对称密钥,并利用SM4对称密钥对加密后的用户密钥的明文进行解密,得到用户密钥的明文,并将其存储至自身的寄存器或RAM存储器中。

[0050] 至此,完成用户密钥在主控处理器、FPGA芯片和管理员设备之间的同步,且在同步过程中采用数字信封的加密方式对用户密钥的密文和明文进行加密,有效保证了用户密钥在主控处理器、FPGA芯片和管理员设备之间传输过程中的安全性。

[0051] 根据本发明的一个实施例,在PCI-E密码卡首次使用时,还对PCI-E密码卡进行初始化,以在管理员设备内部生成用于加密用户密钥的主密钥、密钥对,并以密钥对中的公钥为管理员设备申请数字证书,同时分别为主控处理器和FPGA芯片生成各自的密钥对,并分别以各自的密钥对中的公钥为主控处理器和FPGA芯片申请数字证书。

[0052] 具体来说,PCI-E密码卡在初始化之前,是一块没有任何密钥信息和管理配置信息的空白密码卡,因此在首次使用时,需要对其进行初始化。例如,可通过PCI-E密码卡的管理界面点击初始化功能以进行初始化,初始化可包括:

[0053] 设置PCI-E密码卡的管理员,为管理员配置管理员设备,并设置管理员登录口令,以及在管理员设备内部产生密钥对、用于加密用户密钥的主密钥,并以密钥对中的公钥为

管理员设备申请数字证书，例如，在管理员设备内部产生SM2密钥对，并以SM2密钥对中的公钥为管理员设备申请SM2数字证书。

[0054] 同时，为主控处理器生成密钥对，并以密钥对中的公钥为主控处理器申请数字证书。例如，可先生成随机数，然后根据随机数、管理员登录口令和主控处理器ID按照预设的密钥算法计算获得主控处理器的私钥，根据该私钥进一步获得主控处理器的公钥，以获得密钥对，并以该密钥对中的公钥为主控处理器申请数字证书，同时将产生的随机数存储至主控处理器中，以便于在PCI-E密码卡上电工作时，根据该随机数生成主控处理器的私钥，以进行数字信封的解密。例如，可为主控处理器生成SM2密钥对，该密钥对中的SM2私钥＝SM3(管理员登录口令+随机数+主控处理器ID)，相应的SM2公钥＝SM2私钥*G，其中G为椭圆曲线基点，计算完成后，将产生的随机数存储至主控处理器的程序存储芯片，并以主控处理器的SM2公钥申请主控处理器的SM2数字证书。

[0055] 同时，为FPGA芯片生成密钥对，并以密钥对中的公钥为FPGA芯片申请数字证书。例如，可先生成随机数，然后根据随机数、管理员登录口令和FPGA芯片ID按照预设的密钥算法计算获得FPGA芯片的私钥，根据该私钥进一步获得FPGA芯片的公钥，以获得密钥对，并以该密钥对中的公钥为FPGA芯片申请数字证书，同时将产生的随机数存储至FPGA芯片中，以便于在PCI-E密码卡上电工作时，根据该随机数生成FPGA芯片的私钥，以进行数字信封的解密。例如，可为FPGA芯片生成SM2密钥对，该密钥对中的SM2私钥＝SM3(管理员登录口令+随机数+FPGA芯片ID)，相应的SM2公钥＝SM2私钥*G，计算完成后，将产生的随机数存储至FPGA芯片的程序存储芯片，并以FPGA芯片的SM2公钥申请FPGA芯片的SM2数字证书。

[0056] 最后，将管理员设备、主控处理器和FPGA芯片三个部件的数字证书，如SM2数字证书，均存储在这三个部件的存储区，用于PCI-E密码卡上电工作时使用，以便于利用其采用数字信封的加密方式对用户密钥的密文或明文进行加密传输，或对数字信封进行解密以获得用户密钥的密文或明文。

[0057] 根据本发明的一个实施例，当外部的计算机调用PCI-E密码卡进行密码运算时，FPGA芯片使用存储的用户密钥进行密码运算，并将运算结果返回给外部的计算机。具体而言，当计算机需要通过PCI-E密码卡进行密码运算时，可将PCI-E密码卡插接在计算机的PCI-E插槽内，以与计算机进行物理连接，然后计算机通过API应用程序接口和驱动程序调用PCI-E密码卡，以进行密码运算。在进行密码运算时，FPGA芯片根据存储在寄存器或RAM存储器中的用户密钥的明文，以及预先存储在FPGA芯片中的密码运算功能，如SM2/3/4密码运算功能等，进行密码运算，并将运算结果反馈给计算机，至此完成密码的运算。由此，通过PCI-E密码卡进行密码运算，可保证密码的安全性。

[0058] 根据本发明的一个实施例，当外部的计算机调用密钥生成、更新功能时，主控处理器将修改后的用户密钥以数字信封的加密方式发送给管理员设备，管理员设备对数字信封进行解密后，使用自身的主密钥对修改后的用户密钥进行加密后，并以数字信封的加密方式发送给主控处理器，以便主控处理器将修改后的用户密钥的密文存储在密钥存储芯片中，同时与FPGA芯片进行安全传输。

[0059] 具体而言，当计算机需要通过PCI-E密码卡进行密钥管理，如密钥生成、更新、删除等功能时，可将PCI-E密码卡插接在计算机的PCI-E插槽内，以与计算机进行物理连接，然后计算机通过API应用程序接口和驱动程序调用PCI-E密码卡，以进行密钥管理等功能。

[0060] 在进行密钥管理如密钥更新时，PCI-E密码卡的主控处理器将修改后的用户密钥，以数字信封的加密方式发送给管理员设备，例如，可产生随机SM4对称密钥，通过该对称密钥对修改后的用户密钥进行加密，然后用预先存储的管理员设备的数字证书(如SM2数字证书)中的公钥加密SM4对称密钥，并将加密后的用户密钥和加密后的SM4对称密钥一同发送给管理员设备。

[0061] 管理员设备在接收到主控处理器发送的数字信封后，对该数字信封进行解密，以获得修改后的用户密钥，例如，利用预先存储的自身的数字证书(如SM2数字证书)中的私钥对加密后的SM4对称密钥进行解密，得到SM4对称密钥，并利用SM4对称密钥对加密后的用户密钥进行解密，得到修改后的用户密钥。然后，管理员设备使用预先存储的主密钥对修改后的用户密钥进行加密，以获得用户密钥的密文。接着，管理员设备以数字信封的加密方式将其发送给主控处理器，例如，可产生随机SM4对称密钥，通过该对称密钥对修改后的用户密钥的密文进行加密，然后用预先存储的主控处理器的数字证书(如SM2数字证书)中的公钥加密SM4对称密钥，并将加密后的用户密钥的密文和加密后的SM4对称密钥一同发送给主控处理器。

[0062] 主控处理器在接收到管理员设备发送的数字信封后，对该数字信封进行解密，以获得修改后的用户密钥的密文，例如，利用预先存储的自身的数字证书(如SM2数字证书)中的私钥对加密后的SM4对称密钥进行解密，得到SM4对称密钥，并利用SM4对称密钥对加密后的用户密钥的密文进行解密，得到修改后的用户密钥的密文，并将其存储至密钥存储芯片中，同时与FPGA芯片进行安全传输，以实时更新用户密钥。

[0063] 根据本发明的一个实施例，当PCI-E密码卡掉电时，主控处理器和FPGA芯片中存储的用户密钥的明文自动消失，以保证用户密钥的安全性，例如，在对用户密钥进行同步时，可将用户密钥的明文存储至主控处理器和FPGA芯片的内存、寄存器、RAM存储器等中，以便于用户密钥的明文在掉电时自动消失，保证用户密钥的安全性。

[0064] 综上所述，根据本发明实施例的PCI-E密码卡的密钥保护方法，通过将用户密钥以密文的形式存储至PCI-E密码卡的密钥存储芯片中，并将用于加密用户密钥的主密钥存储至管理员设备中，可保证用户密钥存储的安全性。同时，解密后的用户密钥，以数字信封加密的方式在主控处理器、FPGA芯片和管理员设备等各个设备之间进行传输，有效保证了用户密钥传输的安全性。另外，在采用数字信封加密方式对用户密钥进行加密传输时，通过采用SM2/3/4密码算法和数字证书技术，实现了各个部件之间的身份鉴别和相互之间的数据加密传输，有效防止了非法连接、部件替换等攻击，保证了用户密钥传输的安全性，尤其是用户密钥的明文传输的安全性。

[0065] 另外，本发明还提供了一种计算机可读存储介质，其上存储有PCI-E密码卡的密钥保护程序，该保护程序被处理器执行时实现上述的PCI-E密码卡的密钥保护方法。

[0066] 根据本发明实施例的计算机可读存储介质，在用户密钥传输的过程中，采用数字信封的加密方式对用户密钥进行加密，即以对称和非对称相结合的加密方式对用户密钥进行加密，从而有效保证用户密钥在主控处理器、FPGA芯片和管理员设备之间传输的安全性。

[0067] 此外，本发明还提供了一种PCI-E密码卡，参考图1所示，该PCI-E密码卡10可包括：主控处理器11、与主控处理器11相连的密钥存储芯片12、与主控处理器11相连的FPGA芯片13。

[0068] 其中，在PCI-E密码卡10上电启动后，主控处理器11建立与外部的管理员设备20之间的通信连接，并计算出自身的私钥，FPGA芯片13计算出自身的私钥；主控处理器11从密钥存储芯片12中读取用户密钥的密文，并采用数字信封的加密方式对用户密钥的密文进行加密后发送给管理员设备20；管理员设备20对数字信封进行解密后，根据自身存储的主密钥对用户密钥的密文进行解密以获得用户密钥的明文，并采用数字信封的方式对用户密钥的明文进行加密后发送给主控处理器11；主控处理器11对数字信封进行解密以获得用户密钥的明文，并对用户密钥的明文进行存储，以及采用数字信封的方式对用户密钥的明文进行加密后发送给FPGA芯片13；FPGA芯片13对数字信封进行解密以获得用户密钥的明文，并对用户密钥的明文进行存储。

[0069] 根据本发明的一个实施例，主控处理器11通过管理员设备20输入管理员登录口令，并在登录成功后建立与管理员设备20之间的通信连接，其中，FPGA芯片13读取随机数，并根据管理员登录口令、随机数和FPGA芯片ID计算自身的私钥，以及将自身的私钥存储在FPGA芯片13的寄存器中；主控处理器11读取随机数，并根据管理员登录口令、随机数和主控处理器ID计算自身的私钥，以及将自身的私钥存储在主控处理器11的内存中。

[0070] 根据本发明的一个实施例，PCI-E密码卡10在首次使用时，还进行初始化，以便在管理员设备20内部生成用于加密用户密钥的主密钥、密钥对，并以密钥对中的公钥为管理员设备20申请数字证书，同时分别为主控处理器11和FPGA芯片13生成各自的密钥对，并分别以各自的密钥对中的公钥为主控处理器11和FPGA芯片13申请数字证书。

[0071] 根据本发明的一个实施例，FPGA芯片13在与外部的计算机30建立通信连接后，如果外部的计算机30调用PCI-E密码卡10进行密码运算，FPGA芯片13使用存储的用户密钥进行密码运算，并将运算结果返回给外部的计算机30。

[0072] 根据本发明的一个实施例，当外部的计算机30调用密钥生成、更新功能时，主控处理器11将修改后的用户密钥以数字信封的加密方式发送给管理员设备20，管理员设备20对数字信封进行解密后，使用自身的主密钥对修改后的用户密钥进行加密后，并以数字信封的加密方式发送给主控处理器11，以便主控处理器11将修改后的用户密钥的密文存储在密钥存储芯片12中，同时与FPGA芯片13进行安全传输。

[0073] 根据本发明的一个实施例，当PCI-E密码卡10掉电时，主控处理器11和FPGA芯片13中存储的用户密钥的明文自动消失。

[0074] 需要说明的是，关于本申请中PCI-E密码卡的详细描述，请参考本申请中关于PCI-E密码卡的密钥保护方法的描述，具体这里不再赘述。

[0075] 根据本发明实施例的PCI-E密码卡，在用户密钥传输的过程中，采用数字信封的加密方式对用户密钥进行加密，即以对称和非对称相结合的加密方式对用户密钥进行加密，从而有效保证用户密钥在主控处理器、FPGA芯片和管理员设备之间传输的安全性。

[0076] 需要说明的是，在流程图中表示或在此以其他方式描述的逻辑和/或步骤，例如，可以被认为是用于实现逻辑功能的可执行指令的定序列表，可以具体实现在任何计算机可读介质中，以供指令执行系统、装置或设备(如基于计算机的系统、包括处理器的系统或其他可以从指令执行系统、装置或设备取指令并执行指令的系统)使用，或结合这些指令执行系统、装置或设备而使用。就本说明书而言，"计算机可读介质"可以是任何可以包含、存储、通信、传播或传输程序以供指令执行系统、装置或设备或结合这些指令执行系统、装置或设

备而使用的装置。计算机可读介质的更具体的示例(非穷尽性列表)包括以下:具有一个或多个布线的电连接部(电子装置),便携式计算机盘盒(磁装置),随机存取存储器(RAM),只读存储器(ROM),可擦除可编辑只读存储器(EPROM或闪速存储器),光纤装置,以及便携式光盘只读存储器(CDROM)。另外,计算机可读介质甚至可以是可在其上打印所述程序的纸或其他合适的介质,因为可以例如通过对纸或其他介质进行光学扫描,接着进行编辑、解译或必要时以其他合适方式进行处理来以电子方式获得所述程序,然后将其存储在计算机存储器中。

[0077] 应当理解,本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中,多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如,如果用硬件来实现,和在另一实施方式中一样,可用本领域公知的下列技术中的任一项或他们的组合来实现:具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路,具有合适的组合逻辑门电路的专用集成电路,可编程门阵列(PGA),现场可编程门阵列(FPGA)等。

[0078] 在本说明书的描述中,参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中,对上述术语的示意性表述不一定指的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0079] 此外,术语“第一”、“第二”仅用于描述目的,而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此,限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本发明的描述中,“多个”的含义是至少两个,例如两个,三个等,除非另有明确具体的限定。

[0080] 在本发明中,除非另有明确的规定和限定,术语“安装”、“相连”、“连接”、“固定”等术语应做广义理解,例如,可以是固定连接,也可以是可拆卸连接,或成一体;可以是机械连接,也可以是电连接;可以是直接相连,也可以通过中间媒介间接相连,可以是两个元件内部的连通或两个元件的相互作用关系,除非另有明确的限定。对于本领域的普通技术人员而言,可以根据具体情况理解上述术语在本发明中的具体含义。

[0081] 尽管上面已经示出和描述了本发明的实施例,可以理解的是,上述实施例是示例性的,不能理解为对本发明的限制,本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。

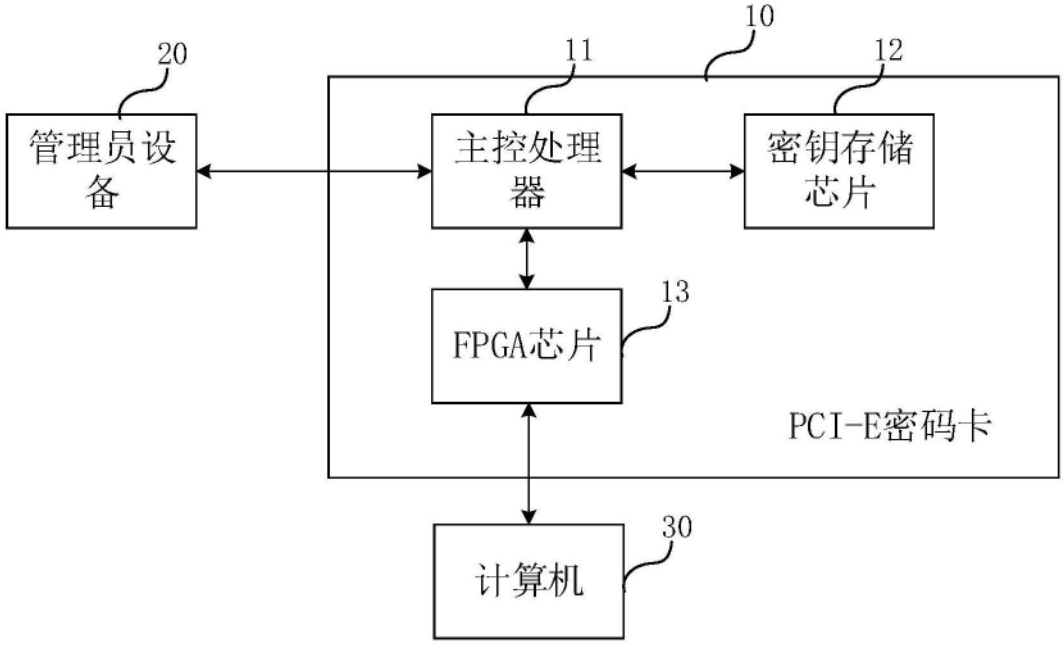


图1

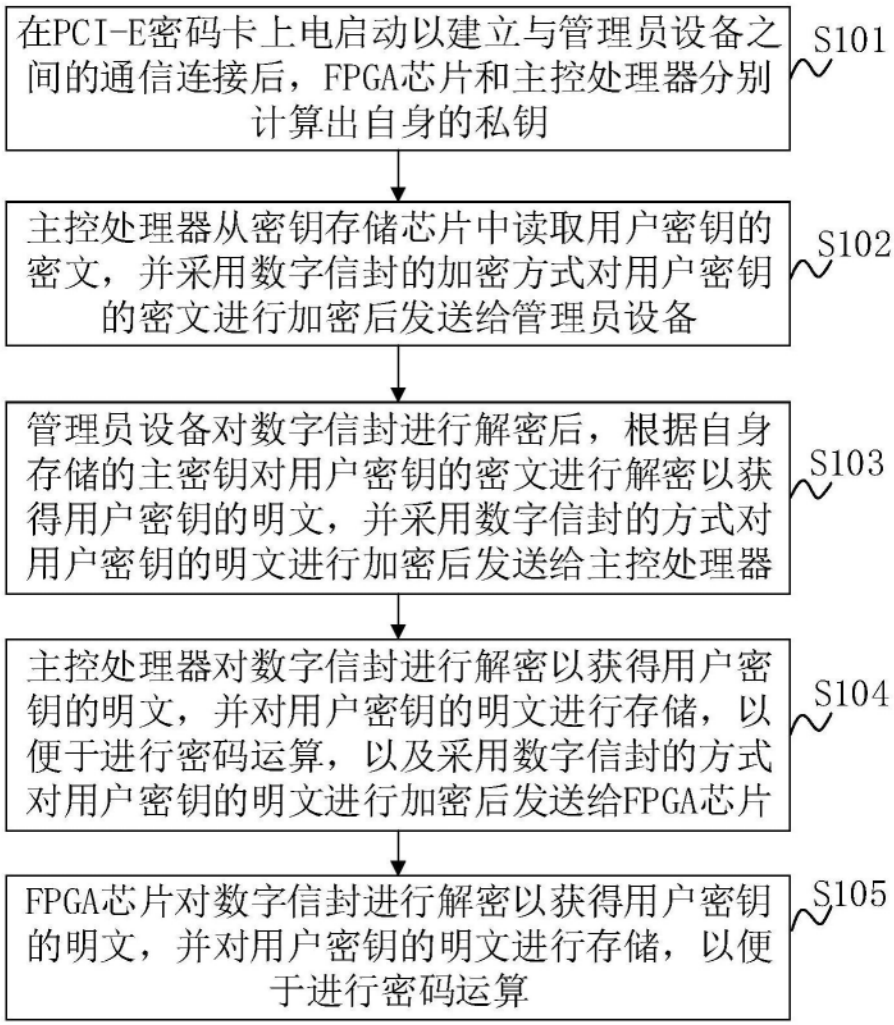

在PCI-E密码卡上电启动以建立与管理员设备之间的通信连接后，FPGA芯片和主控处理器分别计算出自身的私钥
S101
主控处理器从密钥存储芯片中读取用户密钥的密文，并采用数字信封的加密方式对用户密钥的密文进行加密后发送给管理员设备
S102
管理员设备对数字信封进行解密后，根据自身存储的主密钥对用户密钥的密文进行解密以获得用户密钥的明文，并采用数字信封的方式对用户密钥的明文进行加密后发送给主控处理器
S103
主控处理器对数字信封进行解密以获得用户密钥的明文，并对用户密钥的明文进行存储，以便于进行密码运算，以及采用数字信封的方式对用户密钥的明文进行加密后发送给FPGA芯片
S104
FPGA芯片对数字信封进行解密以获得用户密钥的明文，并对用户密钥的明文进行存储，以便于进行密码运算
S105

图2