(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109934020 A
(43)申请公布日 2019.06.25

(21)申请号 201910261789.9

(22)申请日 2019.04.02

(71)申请人 山东渔翁信息技术股份有限公司
地址 264210 山东省威海市高区初河北路12号

(72)发明人 郭刚 宋志华 成盼青

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 罗满

(51)Int.Cl.
G06F 21/72(2013.01)
G06F 21/60(2013.01)

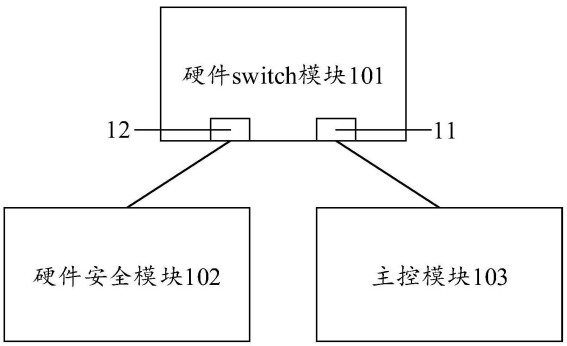
权利要求书1页 说明书6页 附图1页

(54)发明名称

一种密码设备

(57)摘要

本发明公开了一种密码设备，包括：硬件switch模块、硬件安全模块和主控模块；其中，硬件switch模块设有第一接口和第二接口；硬件switch模块通过第一接口与主控模块连接，通过第二接口与硬件安全模块连接；硬件switch模块，用于通过第一接口接收主控模块发送的操作数据，并将操作数据通过第二接口传输至硬件安全模块；硬件安全模块，用于根据操作数据实现密码操作。如此当硬件安全模块和主控模块具有同级接口时，二者也能建立通信连接，即：本发明打破了现有技术中的同级接口无法建立通信连接的限制，使得密码设备具有良好的通用性和灵活性，同时也提高了密码设备的性能。



CN 109934020 A

1.一种密码设备,其特征在于,包括:硬件switch模块、硬件安全模块和主控模块;

其中,所述硬件switch模块设有第一接口和第二接口;所述硬件switch模块通过所述第一接口与所述主控模块连接,通过所述第二接口与所述硬件安全模块连接;

所述硬件switch模块,用于通过所述第一接口接收所述主控模块发送的操作数据,并将所述操作数据通过所述第二接口传输至所述硬件安全模块;

所述硬件安全模块,用于根据所述操作数据实现密码操作;

其中,所述操作数据包括:操作指令和/或待实现密码操作的数据。

2.根据权利要求1所述的密码设备,其特征在于,所述第一接口和所述第二接口为USB接口、PCIE接口、串口、网口、SATA口或并口。

3.根据权利要求1所述的密码设备,其特征在于,所述硬件switch模块还设有第三接口,所述第三接口用于与外部设备建立通信连接。

4.根据权利要求1所述的密码设备,其特征在于,所述硬件安全模块设有外接接口。

5.根据权利要求4所述的密码设备,其特征在于,所述外接接口为插拔式接口。

6.根据权利要求5所述的密码设备,其特征在于,所述外接接口为USB接口、PCIE接口、串口、网口、SATA口或并口。

7.根据权利要求1-6任意一项所述的密码设备,其特征在于,所述硬件安全模块设有第四接口,所述主控模块设有第五接口,所述硬件安全模块和所述主控模块通过所述第四接口和所述第五接口实现通信连接。

8.根据权利要求7所述的密码设备,其特征在于,所述第四接口和所述第五接口的接口类型为USB或串口。

9.根据权利要求1-6任意一项所述的密码设备,其特征在于,所述第二接口为多个。

10.根据权利要求1-6任意一项所述的密码设备,其特征在于,所述主控模块设有用于与外接设备连接的通信接口。

一种密码设备

技术领域

[0001] 本发明涉及数据加密技术领域，更具体地说，涉及一种密码设备。

背景技术

[0002] 在现有技术中，硬件安全模块一般与主控模块连接，从而构成密码设备。主控模块用于发送密码操作指令至硬件安全模块，以实现密钥管理、数据加密等密码操作。

[0003] 但是，当硬件安全模块和主控模块的接口为同级接口时，硬件安全模块和主控模块无法实现通信连接。例如：硬件安全模块和主控模块仅有PCIE接口，且硬件安全模块和主控模块的PCIE接口均为从PCIE接口，即：硬件安全模块和主控模块的PCIE接口为同级接口，因此无法实现通信连接。

[0004] 其中，硬件安全模块(Hardware Security Module，缩写HSM)是一种用于保护和管理强认证系统所使用的密钥，并同时提供相关密码学操作的计算机硬件设备。主控模块即为设有处理芯片的微型处理装置，其能够进行简单的程序逻辑处理，也可实现较复杂的密码算法。

[0005] 因此，如何使具有同级接口的硬件安全模块和主控模块实现通信连接，是本领域技术人员需要解决的问题。

发明内容

[0006] 本发明的目的在于提供一种密码设备，以使具有同级接口的硬件安全模块和主控模块实现通信连接。

[0007] 为实现上述目的，本发明提供了如下技术方案：

[0008] 一种密码设备，包括：硬件switch模块、硬件安全模块和主控模块；

[0009] 其中，所述硬件switch模块设有第一接口和第二接口；所述硬件switch模块通过所述第一接口与所述主控模块连接，通过所述第二接口与所述硬件安全模块连接；

[0010] 所述硬件switch模块，用于通过所述第一接口接收所述主控模块发送的操作数据，并将所述操作数据通过所述第二接口传输至所述硬件安全模块；

[0011] 所述硬件安全模块，用于根据所述操作数据实现密码操作；

[0012] 其中，所述操作数据包括：操作指令和/或待实现密码操作的数据。

[0013] 优选地，所述第一接口和所述第二接口为USB接口、PCIE接口、串口、网口、SATA口或并口。

[0014] 优选地，所述硬件switch模块还设有第三接口，所述第三接口用于与外部设备建立通信连接。

[0015] 优选地，所述硬件安全模块设有外接接口。

[0016] 优选地，所述外接接口为插拔式接口。

[0017] 优选地，所述外接接口为USB接口、PCIE接口、串口、网口、SATA口或并口。

[0018] 优选地，所述硬件安全模块设有第四接口，所述主控模块设有第五接口，所述硬件

安全模块和所述主控模块通过所述第四接口和所述第五接口实现通信连接。

[0019] 优选地，所述第四接口和所述第五接口的接口类型为USB或串口。

[0020] 优选地，所述第二接口为多个。

[0021] 优选地，所述主控模块设有用于与外接设备连接的通信接口。

[0022] 通过以上方案可知，本发明提供了一种密码设备，包括：硬件switch模块、硬件安全模块和主控模块；其中，所述硬件switch模块设有第一接口和第二接口；所述硬件switch模块通过所述第一接口与所述主控模块连接，通过所述第二接口与所述硬件安全模块连接；所述硬件switch模块，用于通过所述第一接口接收所述主控模块发送的操作数据，并将所述操作数据通过所述第二接口传输至所述硬件安全模块；所述硬件安全模块，用于根据所述操作数据实现密码操作；其中，所述操作数据包括：操作指令和/或待实现密码操作的数据。

[0023] 可见，该设备在硬件switch模块上设置了第一接口和第二接口，通过第一接口与主控模块连接，通过第二接口与硬件安全模块连接。其中，当硬件安全模块和主控模块需要通信时，主控模块先将数据传输至硬件switch模块，硬件switch模块再将数据传输至硬件安全模块。如此当硬件安全模块和主控模块具有同级接口时，二者也能建立通信连接，即：本发明打破了现有技术中的同级接口无法建立通信连接的限制，使得密码设备具有良好的通用性和灵活性，同时也提高了密码设备的性能。

附图说明

[0024] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0025] 图1为本发明实施例公开的一种密码设备示意图；

[0026] 图2为本发明实施例公开的另一种密码设备示意图。

具体实施方式

[0027] 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，本领域普通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。

[0028] 本发明实施例公开了一种密码设备，以使具有同级接口的硬件安全模块和主控模块实现通信连接。

[0029] 参见图1，本发明实施例提供的一种密码设备，包括：硬件switch模块101、硬件安全模块102和主控模块103；

[0030] 其中，所述硬件switch模块101设有第一接口11和第二接口12；所述硬件switch模块101通过所述第一接口11与所述主控模块103连接，通过所述第二接口12与所述硬件安全模块102连接；

[0031] 所述硬件switch模块101，用于通过所述第一接口11接收所述主控模块103发送的

操作数据，并将所述操作数据通过所述第二接口12传输至所述硬件安全模块102；

[0032] 所述硬件安全模块102，用于根据所述操作数据实现密码操作；其中，所述操作数据包括：操作指令和/或待实现密码操作的数据。

[0033] 本实施例中的第一接口11和第二接口12可以为USB接口、PCIE接口、串口、网口、SATA口或并口。也就是说，第一接口11可以为USB接口、PCIE接口、串口、网口、SATA口或并口；第二接口12的接口类型也可以为USB接口、PCIE接口、串口、网口、SATA口或并口。当然，第一接口11和第二接口12还可以根据实际应用情况设置为其他类型的接口。

[0034] 需要说明的是，所述密码操作指令包括：加密指令、解密指令、签名验证指令、密钥管理指令和权限管理指令中的任意一种或组合。密钥管理指令至少包括密钥备份和同步指令。权限管理指令即为用户对硬件安全模块进行管理的操作指令。

[0035] 可见，本实施例提供了一种密码设备，该设备在硬件switch模块上设置了第一接口和第二接口，通过第一接口与主控模块连接，通过第二接口与硬件安全模块连接。其中，当硬件安全模块和主控模块需要通信时，主控模块先将数据传输至硬件switch模块，硬件switch模块再将数据传输至硬件安全模块。如此当硬件安全模块和主控模块具有同级接口时，二者也能建立通信连接，即：本发明打破了现有技术中的同级接口无法建立通信连接的限制，使得密码设备具有良好的通用性和灵活性，同时也提高了密码设备的性能。

[0036] 本发明实施例公开了另一种密码设备，相对于上一实施例，本实施例对技术方案作了进一步的说明和优化，本实施例与上述实施例可相互参照。

[0037] 参见图2，本发明实施例提供的另一种密码设备，包括：硬件switch模块201、主控模块202和多个硬件安全模块；

[0038] 本实施例的特别之处在于，本实施例中的硬件switch模块201设有第一接口21和多个第二接口22，硬件switch模块201通过第一接口21与主控模块202连接，通过多个第二接口22与多个硬件安全模块连接。同时，本实施例中的硬件switch模块201还设有第三接口23，第三接口23用于与外部设备建立通信连接。第三接口23可以为USB接口、PCIE接口、串口、网口、SATA口或并口，当然也可设置为其他，以满足实际应用的需要。

[0039] 其中，硬件switch模块201上的第二接口22的数量可大于硬件安全模块的数量，在建立通信连接时，一个第二接口22连接一个硬件安全模块。本实施例中的其他部件的功能和具体组成部分可参见现有技术和上述实施例，故本实施例在此不再赘述。

[0040] 在本实施例中，多个第二接口22的接口类型可以相同，也可以不同。例如：全部设置为USB接口，或全部设置为PCIE接口，或全部设置为串口，或全部设置为网口、SATA口、并口，或设置一部分USB接口、一部分PCIE接口、一部分串口、一部分网口、一部分SATA口和一部分并口。当然，也可以选择任意几种类型的接口进行设置。第二接口的接口类型也可设置为其他，以满足实际应用的需要。

[0041] 本实施例中的多个硬件安全模块即为图2中的硬件安全模块1、硬件安全模块2、硬件安全模块3……硬件安全模块N。

[0042] 在本实施例中，外部设备用于发送操作指令至主控模块202或硬件安全模块，外部设备发送给主控模块202的操作指令一般为控制主控模块202工作的指令，主控模块202的工作一般包括：对数据进行清洗、降维、计算、加密等。外部设备发送给硬件安全模块的操作指令一般为：加密指令、解密指令、签名验证指令、密钥管理指令和权限管理指令等。

[0043] 其中,外部设备一般为电脑和服务器等具有主机的设备,外部设备一般包括输入输出设备等必要操作设备,其具体组成部分可参考现有技术。需要说明的是,本实施例中的外部设备可以为任意能够与硬件switch模块建立通信连接的、具有数据处理功能的设备。

[0044] 在外部设备的控制下,主控模块202和硬件安全模块的数据交互过程可以为:外部设备通过硬件switch模块发送操作指令至主控模块202,主控模块根据操作指令实现对应的操作,并向外部设备反馈操作结果;外部设备在收到返回结果后,根据返回结果通过硬件switch模块发送对应的指令至硬件安全模块,以使硬件安全模块根据接收到的指令实现对应的密码操作。

[0045] 若基于外部设备控制硬件安全模块实现加密操作,具体过程可以为:用户输入加密指令,则外部设备发送加密指令至硬件switch模块200的第一接口25,以便硬件switch模块200通过自身的第二接口传输加密指令至指定的硬件安全模块;接着用户在外部设备上选择待加密数据,外部设备发送待加密数据至硬件switch模块200的第一接口25,以便硬件switch模块200通过自身的第二接口传输待加密数据至指定的硬件安全模块,以便接收到加密指令和待加密数据的硬件安全模块利用自身加密算法对待加密数据进行加密。加密完成后,将加密结果反馈至外部设备。需要说明的是,外部设备发送其他操作数据给硬件安全模块的过程可参考上述加密过程,故本说明书在此不再赘述。

[0046] 可见,本实施例提供了另一种密码设备,该设备在硬件switch模块上设置了第一接口和第二接口,通过第一接口与主控模块连接,通过第二接口与硬件安全模块连接。其中,当硬件安全模块和主控模块需要通信时,主控模块先将数据传输至硬件switch模块,硬件switch模块再将数据传输至硬件安全模块。如此当硬件安全模块和主控模块具有同级接口时,二者也能建立通信连接,即:本发明打破了现有技术中的同级接口无法建立通信连接的限制,使得密码设备具有良好的通用性和灵活性,同时也提高了密码设备的性能。

[0047] 基于上述实施例,需要说明的是,硬件安全模块设有外接接口。外接接口为插拔式接口,外接接口可以为USB接口、PCIE接口、串口、网口、SATA口或并口。硬件安全模块的外接接口可以与存储介质连接,以将硬件安全模块中的密钥备份至所述存储介质,或将所述存储介质中存储的密钥同步至硬件安全模块。其中,存储介质可以为移动设备key、TF卡、IC卡或SD卡。

[0048] 将硬件安全模块中的密钥备份至所述存储介质,或将所述存储介质中存储的密钥同步至硬件安全模块时,密码设备需要与外部设备建立通信连接。即:密码设备中的硬件switch模块的第三接口需要通过通信连接线与外部设备建立通信连接。

[0049] 其中,若存储介质为普通存储介质,例如U盘、硬盘等,那么可以在外部设备的控制下将硬件安全模块中的密钥备份至存储介质,或将存储介质中存储的密钥同步至硬件安全模块,以对硬件安全模块中的密钥进行管理。

[0050] 其中,若存储介质为移动设备key,则每个硬件安全模块的外接接口用于与移动设备key插拔式连接,以将硬件安全模块中的密钥同步至所述移动设备key,或将所述移动设备key中存储的密钥备份至硬件安全模块。具体的,当硬件安全模块的外接接口连接有移动设备key,则外部设备可通过硬件switch模块向硬件安全模块发送密钥备份指令,使当前硬件安全模块中的密钥备份至移动设备key;若外部设备向硬件安全模块发送密钥同步指令,则可使移动设备key中密钥同步至当前硬件安全模块。因此使用同一个移动设备key可将一

个硬件安全模块中的密钥同步至其他硬件安全模块中，从而可实现密钥同步。

[0051] 其中，密钥同步的具体过程可以为：

[0052] 当一硬件安全模块的外接接口连接有移动设备key，则外部设备首先对该移动设备key进行认证，当认证通过后，外部设备通过硬件switch模块向该硬件安全模块发送密钥备份指令，从而可使硬件安全模块中的密钥备份至移动设备key。其中，在将密钥备份至移动设备key时，移动设备key会利用自身密钥对密钥进行加密。

[0053] 当另一硬件安全模块的外接接口连接有存储上述密钥的移动设备key，则外部设备首先对移动设备key进行认证，当认证通过后，外部设备通过硬件switch模块向当前硬件安全模块发送密钥同步指令，从而可使移动设备key中的、其他硬件安全模块中的密钥存储至当前硬件安全模块。其中，在将密钥存储至当前硬件安全模块时，移动设备key会利用自身密钥对密钥进行解密。

[0054] 其中，移动设备key可以为任意具有加密功能的存储介质，例如USB Key。对移动设备key进行认证的过程可参考现有技术，故本说明书在此不再赘述。再者，移动设备key利用自身密钥对密钥进行加密后，得到的加密密钥也可以在外部设备的控制下，存储于其他存储设备中，其他存储设备例如：与外部设备连接的硬盘、与当前硬件安全模块连接的硬盘等。

[0055] 基于上述任意实施例，需要说明的是，硬件安全模块设有第四接口，主控模块设有第五接口，硬件安全模块和主控模块通过第四接口和第五接口实现通信连接。其中，第四接口和第五接口的接口类型为USB或串口。

[0056] 也就是说，硬件安全模块在特定情况下，可直接与主控模块进行数据交互。其中，当硬件安全模块的接口与主控模块的接口处于同级时，硬件安全模块仅连接于硬件switch模块的第三接口；当硬件安全模块的接口与主控模块的接口不处于同级时，硬件安全模块可直接与主控模块连接。需要说明的是，第四接口和第五接口一般同为USB接口或同为串口，即当第四接口为USB接口，则第五接口为USB接口；当第四接口为串口，则第五接口为串口。

[0057] 基于上述任意实施例，需要说明的是，主控模块设有用于与外接设备连接的通信接口。该通信接口可使主控模块与外接设备实现数据交互。当然，外部设备、主控模块和硬件安全模块上均设有用于连接通信连接线的接口，外部设备上的接口可通过通信连接线与硬件switch模块上的第三接口相连，主控模块上的接口可通过通信连接线与硬件switch模块上的第一接口相连，硬件安全模块上的接口可通过通信连接线与硬件switch模块上的第二接口相连，上述具体情况可参见现有技术，连接外部设备、硬件switch模块和硬件安全模块的通信连接线的类型可根据接口类型灵活调整，具体调整情况可参见本领域内的现有技术，故本说明书在此不再赘述。

[0058] 其中，主控模块上的通信接口和主控模块上的、与硬件switch模块上的第一接口相连的接口一般不是同一个接口。硬件安全模块的外接接口和硬件安全模块上的与硬件switch模块上的第二接口连接的接口一般也不是同一个接口。

[0059] 基于上述任意实施例，需要说明的是，硬件安全模块可实现各种密码算法，例如SM1算法、SM2算法、SM3算法和SM4算法，SM1算法、SM2算法、SM3算法和SM4算法均为我国国家密码局认定的国产密码算法。该算法均为金融领域内常用的密码算法，因此本实施例提供

的密码设备可为银行、证券等金融机构的资金安全提供数据安全保护。硬件安全模块中实现的密码算法也可为其他密码算法。

[0060] 其中，SM1算法为对称加密算法，该算法不公开，在调用时，需要通过加密芯片的接口进行调用。SM2算法为非对称加密算法，用于实现数字签名密钥协商和数据加密等功能，该算法的签名速度与密钥生成速度均较快。SM3算法用于密码应用中的数字签名和验证消息认证码的生成与验证以及随机数的生成。SM4算法用于实现数据的加密/解密运算，能够保证数据和信息的机密性。

[0061] 本说明书中各个实施例采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似部分互相参见即可。

[0062] 专业人员还可以进一步意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

[0063] 结合本文中所公开的实施例描述的方法或算法的步骤可以直接用硬件、处理器执行的软件模块，或者二者的结合来实施。软件模块可以置于随机存储器(RAM)、内存、只读存储器(ROM)、电可编程ROM、电可擦除可编程ROM、寄存器、硬盘、可移动磁盘、CD-ROM、或技术领域内所公知的任意其它形式的存储介质中。

[0064] 对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下，在其它实施例中实现。因此，本发明将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

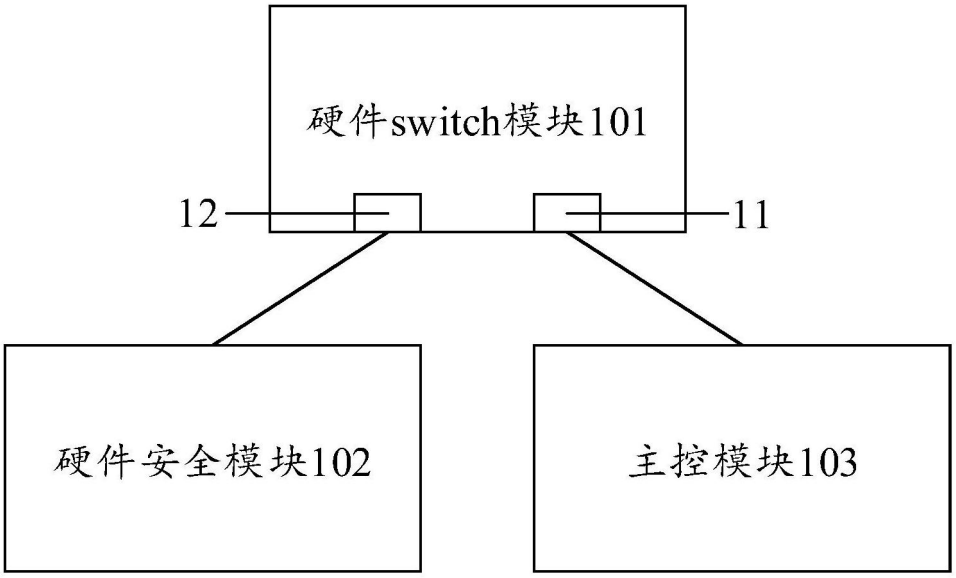

硬件switch模块101
12
11
硬件安全模块102
主控模块103

图1

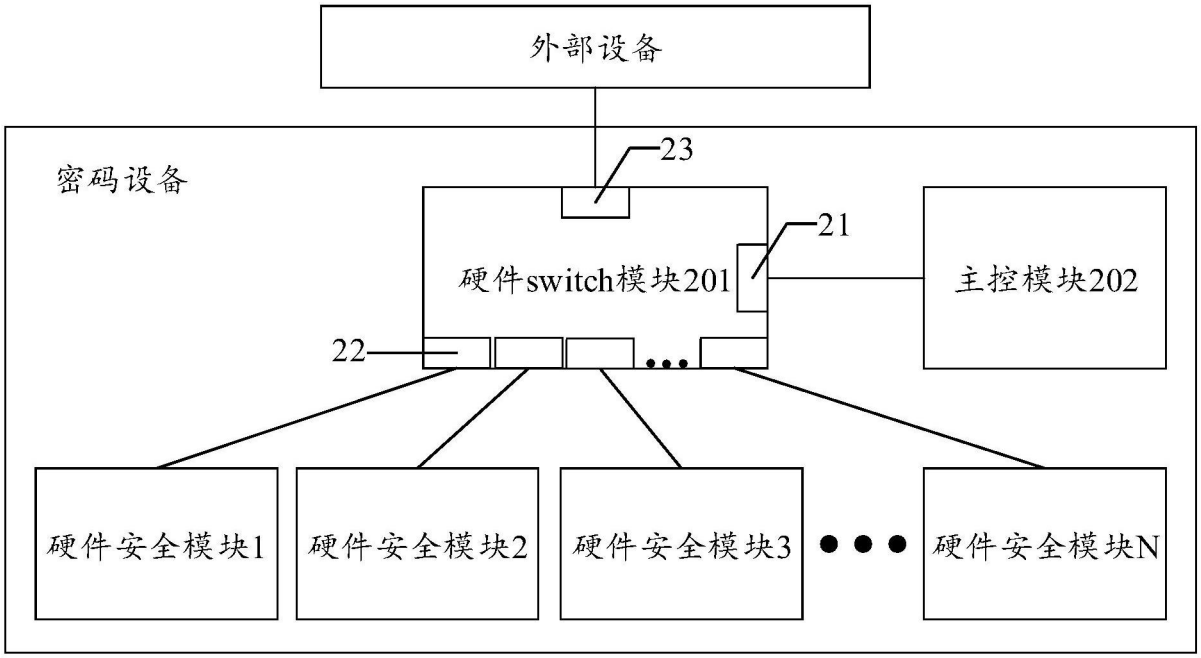

外部设备
密码设备
23
21
硬件switch模块201
主控模块202
22
硬件安全模块1
硬件安全模块2
硬件安全模块3
硬件安全模块N

图2