(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 111104696 B
(45)授权公告日 2020.09.22

(21)申请号 201911305029.X

(22)申请日 2019.12.17

(65)同一申请的已公布的文献号
申请公布号 CN 111104696 A

(43)申请公布日 2020.05.05

(73)专利权人 北京力天世技系统集成有限公司
地址 100025 北京市朝阳区八里庄西里98号13层1603

(72)发明人 向明亮

(74)专利代理机构 北京润平知识产权代理有限公司 11283
代理人 肖冰滨 王晓晓

(51)Int.Cl.
G06F 21/76(2013.01)
G06F 21/77(2013.01)
G06F 21/60(2013.01)
G06F 13/40(2006.01)
G06F 13/42(2006.01)

(56)对比文件
CN 101567052 A,2009.10.28
CN 207573357 U,2018.07.03
CN 102447082 A,2012.05.09

审查员 罗捷

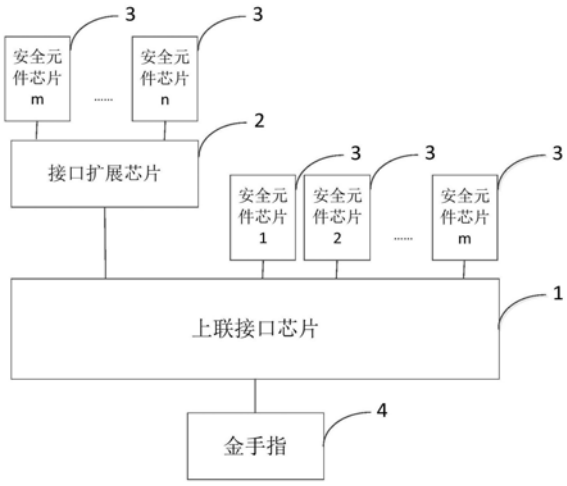
权利要求书2页 说明书4页 附图9页

(54)发明名称

一种多路安全元件集群板卡

(57)摘要

本发明的目的旨在提供一种多路安全元件集群板卡及其软硬件实现方法，作为密码模块，集群板卡可以非常容易地与主机进行软硬件集成、供上位机软件调用并且高效(多线程)地完成数据加解密等运算。为了满足以上功能和性能需求，本发明主要基于专用芯片实现，包括上联接口芯片、接口扩展芯片、安全元件芯片、金手指；其中，上联接口芯片使用通过金手指插入计算机主板扩展槽，实现板卡与计算机系统之间的高速通讯；上联接口芯片可以直接连接安全元件芯片，也可以通过接口扩展芯片间接连接安全元件芯片，以达到多路集成的目的。本发明还公开了一种多路安全元件集群板卡的软件实现及应用方法，以达到上述易集成、高效多线程效果。



CN 111104696 B

1.一种多路安全元件集群板卡,包括上联接口芯片(1)、接口扩展芯片(2)、安全元件芯片(3)以及金手指(4),其特征在于,

所述上联接口芯片(1)通过所述金手指(4)插入计算机主板扩展槽,实现板卡与计算机系统之间的高速通讯;

所述上联接口芯片(1)连接所述接口扩展芯片(2),接口扩展芯片(2)再连接多片安全元件芯片(3),用于实现多路集群;

所述上联接口芯片(1)连接多片所述安全元件芯片(3),用于实现多路集群。

2.如权利要求1所述的多路安全元件集群板卡,其特征在于,所述上联接口芯片(1)包括上联接口,所述上联接口是外设部件互连标准PCI通讯接口、高速串行计算机扩展总线标准PCI-E通讯接口、总线的更新版本PCI-XPCI通讯接口、串行高级技术附件SATA通讯接口、通用串行总线USB通讯接口以及以太网通讯接口中的一者。

3.如权利要求1所述的多路安全元件集群板卡,其特征在于,所述接口扩展芯片(2)包括通用串行总线集线器USB hub,通过USB对上连接所述上联接口芯片(1)、对下连接所述安全元件芯片(3)。

4.如权利要求1所述的多路安全元件集群板卡,其特征在于,所述接口扩展芯片(2)包括智能卡读卡器芯片,通过USB或者串口对上连接所述上联接口芯片(1)、通过符合ISO/IEC 7816-3接口规范的智能卡读卡器接口对下连接所述安全元件芯片(3)。

5.如权利要求1所述的多路安全元件集群板卡,其特征在于,所述接口扩展芯片(2)包括串行外设接口SPI芯片,通过SPI从接口、USB或者串口对上连接所述上联接口芯片(1)、通过SPI接口对下连接所述安全元件芯片(3)。

6.如权利要求1所述的多路安全元件集群板卡,其特征在于,所述接口扩展芯片(2)包括集成电路片间总线I^2C扩展芯片,通过I^2C接口、USB或者串口对上连接所述上联接口芯片(1)、通过I^2C接口对下连接所述安全元件芯片(3)。

7.如权利要求1所述的多路安全元件集群板卡,其特征在于,所述接口扩展芯片(2)包括串口扩展芯片,通过串口对上连接所述上联接口芯片(1)、通过多个串口对下连接所述安全元件芯片(3)。

8.如权利要求1所述的多路安全元件集群板卡,其特征在于,所述接口扩展芯片(2)包括输入输出IO扩展芯片,通过I^2C接口、USB或者串口等对上连接所述上联接口芯片(1)、通过直接IO对下连接所述安全元件芯片(3)。

9.如权利要求1所述的多路安全元件集群板卡,其特征在于,所述上联接口芯片(1)直接连接所述安全元件芯片(3)的接口包括USB、串口、SPI、ISO/IEC 7816-3接口、I^2C以及直接IO中的至少一者。

10.如权利要求1所述的多路安全元件集群板卡,其特征在于,所述上联接口芯片(1)、所述接口扩展芯片(2)和所述安全元件芯片(3)都需要加载各自的固件,计算机操作系统将每个安全元件枚举成独立的实例,安全元件的枚举遵循标准的技术规范、采用操作系统广泛支持的驱动程序,上层应用软件单独操作每一个安全元件。

11.如权利要求1所述的多路安全元件集群板卡,其特征在于,所述多路安全元件集群板卡可以多线程、多进程访问,每个线程或者进程访问一个独立的安全元件实例。

12.如权利要求1所述的多路安全元件集群板卡,其特征在于,所述安全元件芯片(3)彼

此独立,每个安全元件都拥有自己的系统和存储空间,安全元件装载相同的对称加解密密钥,也发行独立的密钥。

13.如权利要求1所述的多路安全元件集群板卡,其特征在于,所述安全元件芯片(3)支持常用的对称、非对称加密算法和摘要算法。

一种多路安全元件集群板卡

技术领域

[0001] 本发明涉及计算机扩展板卡领域，尤其涉及带有多路数据加解密功能集群计算能力的计算机扩展板卡的设计与实现方法。

背景技术

[0002] 计算机网络的普及让人与人之间、人与物之间以及物与物之间的连接变得十分普遍，互联网和物联网的发展与壮大让数据信息加密的作用显得日益重要。无论是互联网空间里人的隐私保护，还是物联网中联网设备的信息安全，都离不开数据加密。在现代信息安全技术领域，常见的加密设备有加密机、密码卡、USB Key(加密锁)和智能卡等，其中的加密机和密码卡经常应用于局端加密。由于可以安装在服务器的PCI(Peripheral Component Interconnect，外设部件互连标准)或者PCI-E(Peripheral Component Interconnect Express，高速串行计算机扩展总线标准)扩展槽上直接使用，密码卡能灵活、方便地部署在需要实现数据加解密功能的服务器上，而随着物联网、工业互联网等新兴网络技术的发展与普及，这类密码卡必将得到更加广泛的应用。

[0003] 纵观现有的PCI或PCI-E密码卡技术，较为显著的特点和不足有一下三方面：

[0004] 其一，采用FPGA(Field Programmable Gate Array，现场可编程门阵列) 作为板卡的核心。作为可重构器件，FPGA的优势可以缩短密码卡产品的研发周期，从而获得更短的上市时间，但同时FPGA的局限性也非常明显。首先，与专用定制芯片(ASIC，Application Specific Integrated Circuit)相比， FPGA功耗高、速度慢；其次，最为关键的一点，FPGA的成本更高，在密码卡需要大批量生产时，生产和测试的成本将更为突出。

[0005] 其二，关注密码卡本身的设计与实现，对上位机(服务器)操作系统如何枚举密码卡设备以及上位机软件如何调用密码卡功能关注较少。作为硬件的密码卡在安装(插入)计算机主板扩展槽之后，一经上电复位，其后续的枚举、应用功能通讯等都是依靠板上软件和上位机软件(包括操作系统和应用软件)来完成的，作为软件实例的密码卡在实际使用中一直存在而且至关重要。

[0006] 其三，由于没有关注密码卡的软件实现，也就没有重视密码卡在实际使用中的多线程调用方案等问题，不便于并行计算，而多任务并行处理恰恰是服务器(或工控机)在使用密码卡完成数据加解密时所必须的面临的功能和性能问题。

[0007] 综上所述，密码卡现在和将来在信息安全领域有着宽广的用途，但现有的密码卡技术对于其批量生产和大面积推广仍存在限制和制约，因此，提出一种新的基于板卡的密码模块来实现易管理、易使用、多线程、多任务、高安全、高性能的应用目的在商用密码广泛推广的今天显得尤为重要。

发明内容

[0008] 本发明的目的旨在提供一种多路安全元件集群板卡及其软硬件实现方法，作为密码模块，集群板卡可以非常容易地与主机进行软硬件集成、供上位机软件调用并且高效(多

线程)地完成数据加解密等运算。

[0009] 为了满足以上功能和性能需求,本发明提供一种多路安全元件集群板卡,包括上联接口芯片(1)、接口扩展芯片(2)、安全元件芯片(3)、金手指(4),所述的上联接口芯片(1)使用通过金手指(4)插入计算机主板扩展槽,实现板卡与计算机系统之间的高速通讯。

[0010] 优选地,所述的上联接口芯片(1)可以连接接口扩展芯片(2),接口扩展芯片(2)再连接多片安全元件芯片(3),用于实现多路集群。

[0011] 所述上联接口芯片(1)包括上联接口,所述上联接口是外设部件互连标准PCI通讯接口、高速串行计算机扩展总线标准PCI-E通讯接口、总线的更新版本PCI-XPCI通讯接口、串行高级技术附件SATA通讯接口、通用串行总线USB通讯接口以及以太网通讯接口中的一者。

[0012] 所述接口扩展芯片(2)包括通用串行总线集线器USB hub,通过USB 对上连接所述上联接口芯片(1)、对下连接所述安全元件芯片(3)。

[0013] 所述接口扩展芯片(2)包括智能卡读卡器芯片,通过USB或者串口对上连接所述上联接口芯片(1)、通过符合ISO/IEC 7816-3接口规范的智能卡读卡器接口对下连接所述安全元件芯片(3)。

[0014] 所述接口扩展芯片(2)包括串行外设接口SPI芯片,通过SPI从接口、USB或者串口对上连接所述上联接口芯片(1)、通过SPI接口对下连接所述安全元件芯片(3)。

[0015] 所述接口扩展芯片(2)包括集成电路片间总线I^2C扩展芯片,通过I^2C 接口、USB或者串口对上连接所述上联接口芯片(1)、通过I^2C接口对下连接所述安全元件芯片(3)。

[0016] 所述接口扩展芯片(2)包括串口扩展芯片,通过串口对上连接所述上联接口芯片(1)、通过多个串口对下连接所述安全元件芯片(3)。

[0017] 所述接口扩展芯片(2)包括输入输出IO扩展芯片,通过I^2C接口、USB 或者串口等对上连接所述上联接口芯片(1)、通过直接IO对下连接所述安全元件芯片(3)。

[0018] 所述上联接口芯片(1)直接连接所述安全元件芯片(3)的接口包括 USB、串口、SPI、ISO/IEC 7816-3接口、I^2C以及直接IO中的至少一者。

[0019] 所述上联接口芯片(1)、所述接口扩展芯片(2)和所述安全元件芯片 (3)都需要加载各自的固件,计算机操作系统将每个安全元件枚举成独立的实例,安全元件的枚举遵循标准的技术规范、采用操作系统广泛支持的驱动程序,上层应用软件单独操作每一个安全元件。

[0020] 所述多路集群板卡可以多线程、多进程访问,每个线程或者进程访问一个独立的安全元件实例。

[0021] 所述安全元件芯片(3)彼此独立,每个安全元件都拥有自己的系统和存储空间,安全元件装载相同的对称加解密密钥,也发行独立的密钥。

[0022] 所述安全元件芯片(3)支持常用的对称、非对称加密算法和摘要算法。

附图说明

[0023] 为了更加清晰地阐述本发明及其实施例,下面将对说明书附图做介绍,对于本领域普通技术人员,在不付出创造性劳动的前提下,亦可根据这些附图获得其他实施。

[0024] 图1为本发明实施例提供的一种通用多路安全元件集群板卡的结构图;

[0025] 图2为本发明实施例提供的一种采用通用串行总线作为扩展接口的多路安全元件集群板卡的结构图；

[0026] 图3为本发明实施例提供的一种采用智能卡接口作为扩展接口的多路安全元件集群板卡的结构图；

[0027] 图4为本发明实施例提供的一种采用SPI接口作为扩展接口的多路安全元件集群板卡的结构图；

[0028] 图5为本发明实施例提供的一种采用I^2C接口作为扩展接口的多路安全元件集群板卡的结构图；

[0029] 图6为本发明实施例提供的一种采用串口作为扩展接口的多路安全元件集群板卡的结构图；

[0030] 图7为本发明实施例提供的一种采用直接IO作为扩展接口的多路安全元件集群板卡的结构图；

[0031] 图8为本发明实施例提供的多路安全元件集群板卡软件工作流程图；

[0032] 图9为本发明实施例提供的多线程并发访问时的线程与安全元件实例映射关系图；

[0033] 图10为本发明实施例提供的软件调用环节单个安全元件芯片的工作流程图。

具体实施方式

[0034] 参看图1至图7，本发明所提供的多路安全元件集群板卡主要由上联接口芯片(1)、接口扩展芯片(2)、安全元件芯片(3)、金手指(4)及其附属电子元器件和电路组成，整张板卡以印刷电路板作为载体，将上联接口芯片(1)、接口扩展芯片(2)、安全元件芯片(3)、金手指(4)及其配套元器件和电路等连接成一个整体。

[0035] 其中，上联接口芯片(1)可以包括上联接口，上联接口可以是PCI (Peripheral Component Interconnect，外设部件互连标准)、PCI-E(Peripheral Component Interconnect Express，高速串行计算机扩展总线标准)、PCI-X(PCI 总线的更新版本)、SATA(串行高级技术附件，Serial Advanced Technology Attachment)、USB(通用串行总线，Universal Serial Bus)、以太网等通讯接口。

[0036] 如图1所示，上联接口芯片(1)使用通过金手指(4)插入计算机主板扩展槽，实现板卡与计算机系统之间的高速通讯。更具体地，上联接口芯片 (1)可以是上联接口为PCI-E的USB(通用串行总线)主机控制器专用芯片(ASIC)，安全元件芯片(3)作为从设备通过主机控制器的USB端口加载到上位机。金手指(4)作为上联接口芯片(1)PCI-E上联接口的物理接口。

[0037] 如图2所示的具体实施例中，接口扩展芯片(2)可以是通用串行总线集线器(USB hub)专用芯片，实现USB接口一变多扩展，安全元件芯片(3) 作为从设备通过集线器的USB端口加载到上位机。接口扩展芯片(2)还可以级联，实现多级扩展以满足集群板卡多路安全元件挂载的需求。

[0038] 图3-图7中，接口扩展芯片(2)分别为智能卡读卡器芯片、SPI(串行外设接口，Serial Peripheral Interface)主接口芯片、I^2C(集成电路片间总线，Inter-Integrated Circuit)扩展芯片、串口扩展芯片以及IO(输入输出)扩展芯片，具体实施例与上文图2的实

施例类似,在此不再赘述。

[0039] 本发明所提供的一种多路安全元件集群板卡的实现方法,不仅包括上述的硬件实现方法,也包括软件实现方法,所述的上联接口芯片(1)、接口扩展芯片(2)和安全元件芯片(3)都需要加载各自的固件,计算机操作系统将每个安全元件枚举成独立的实例,安全元件的枚举遵循标准的技术规范、采用操作系统广泛支持的驱动程序,上层应用软件(程序)可以单独操作每一个安全元件。

[0040] 如图8所示,多路安全元件集群板卡在上电复位后的枚举过程包括 PCI-E枚举(上联接口芯片(1))、USB集线器枚举(上联接口芯片(1)、接口扩展芯片(2))、USB功能设备枚举(安全元件芯片(3)),然后是 USB设备驱动加载(安全元件芯片(3)),之后进入应用软件调用环节(上位机软件、安全元件实例)。实施例中将安全元件芯片(3)固件实现为USB CCID(USB Integrated Circuit(s)Cards Interface Device,USB集成卡接口设备),在枚举完成加载驱动之后通过操作系统可见到多个智能卡读卡器,其数量为集群板卡上安全元件芯片(3)的个数。

[0041] 如图10所示,在软件调用环节,每个安全元件都在等待上位机软件发送指令,接受完成指令之后进行处理并对上发送响应数据。

[0042] 如图9所示,在软件调用环节,上位机软件可以多线程并发访问集群板卡上的安全元件,每个线程对应一个安全元件芯片(3)物理实体,效率更高;上位机软件也可以灵活地将待加解密数据分段交给多个安全元件进行计算,集群板卡作为整个参与运算提高数据吞吐率。

[0043] 以上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。

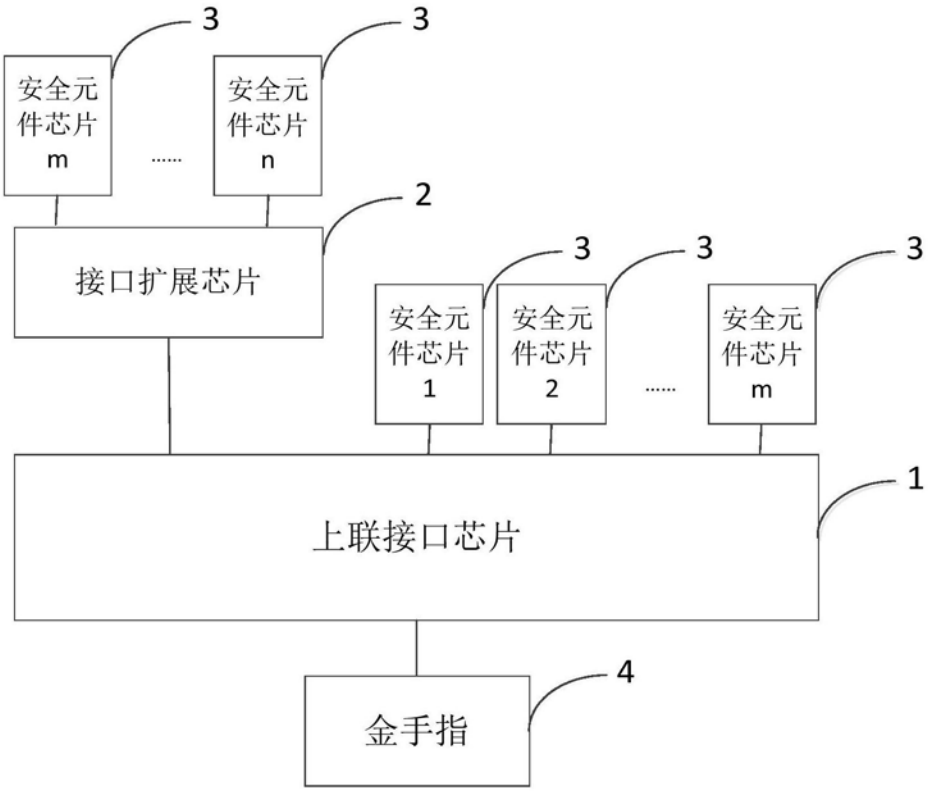

3
3
安全元件芯片m
……
安全元件芯片n
2
接口扩展芯片
3
3
3
安全元件芯片1
安全元件芯片2
……
安全元件芯片m
1
上联接口芯片
4
金手指

图1

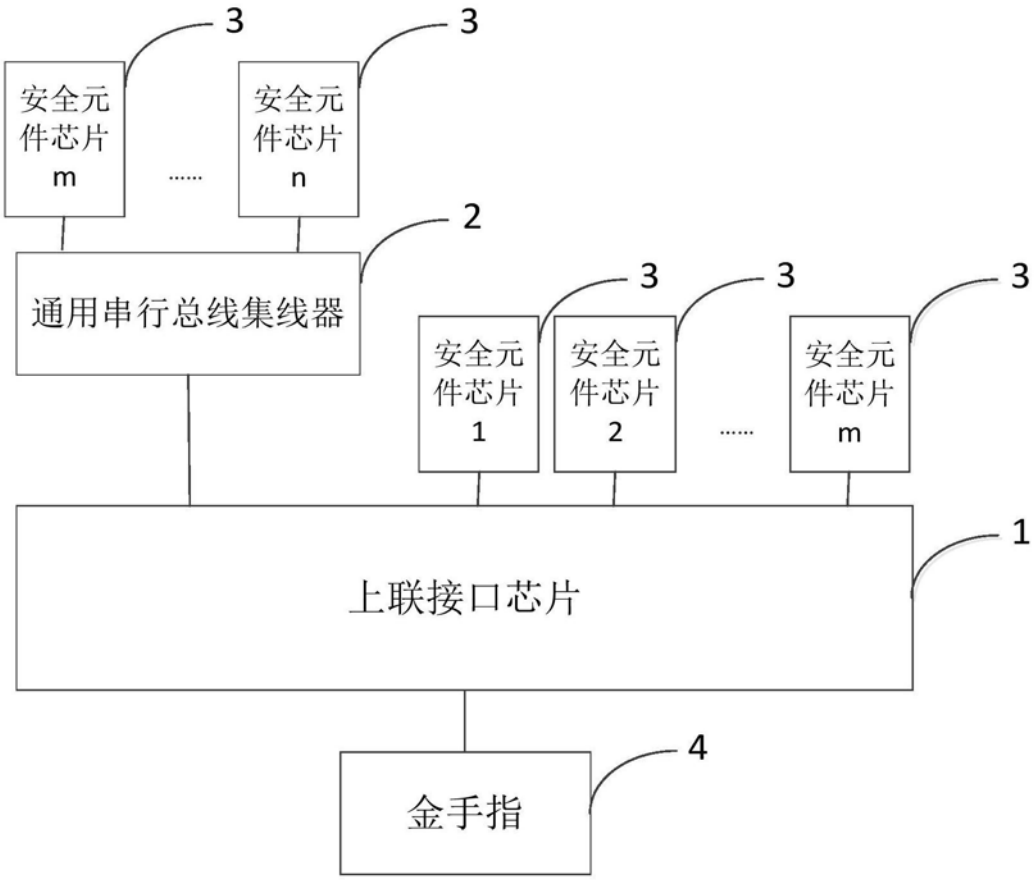

3
3
安全元件芯片m
……
安全元件芯片n
2
通用串行总线集线器
3
3
3
安全元件芯片1
安全元件芯片2
……
安全元件芯片m
1
上联接口芯片
4
金手指

图2

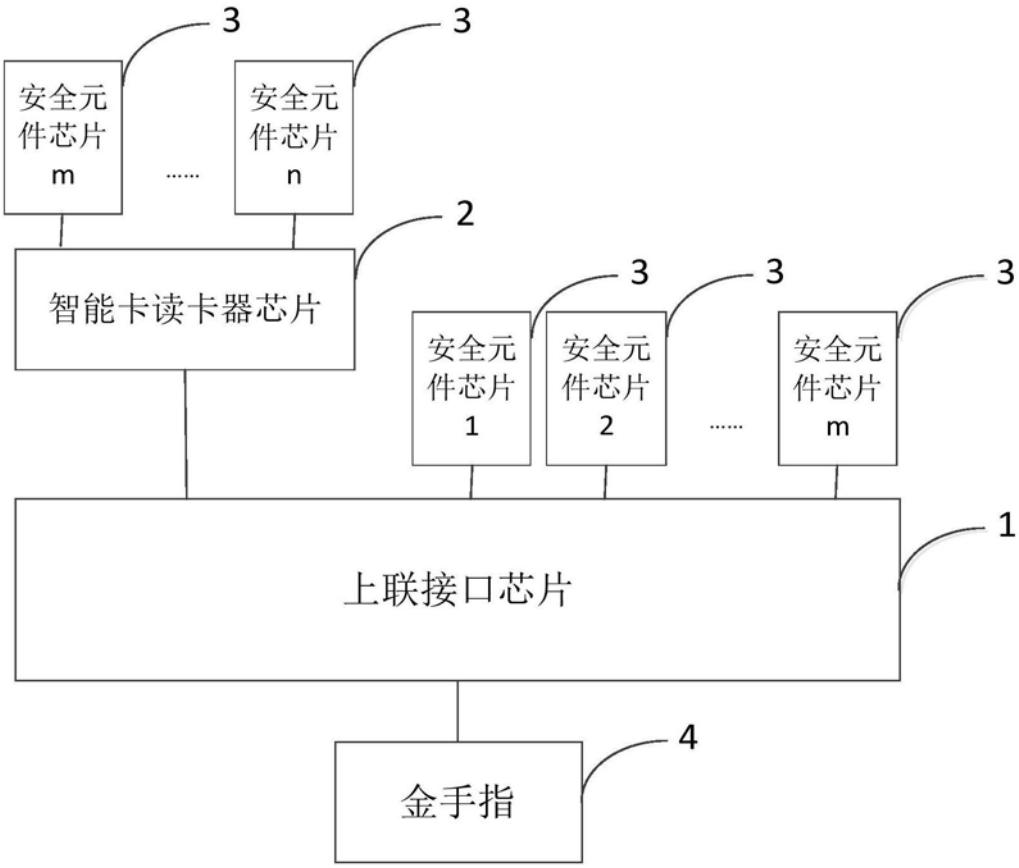

3
3
安全元件芯片m
……
安全元件芯片n
2
智能卡读卡器芯片
3
3
3
安全元件芯片1
安全元件芯片2
……
安全元件芯片m
1
上联接口芯片
4
金手指

图3

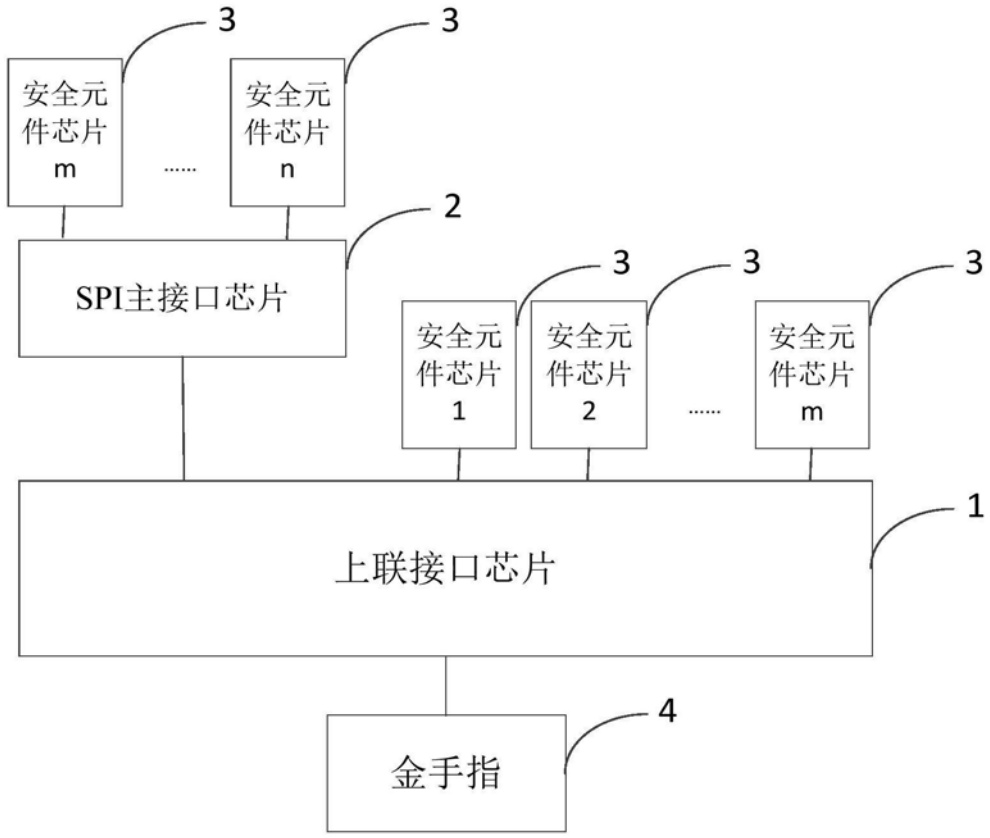

3
3
安全元件芯片m
……
安全元件芯片n
2
SPI主接口芯片
3
3
3
安全元件芯片1
安全元件芯片2
……
安全元件芯片m
1
上联接口芯片
4
金手指

图4

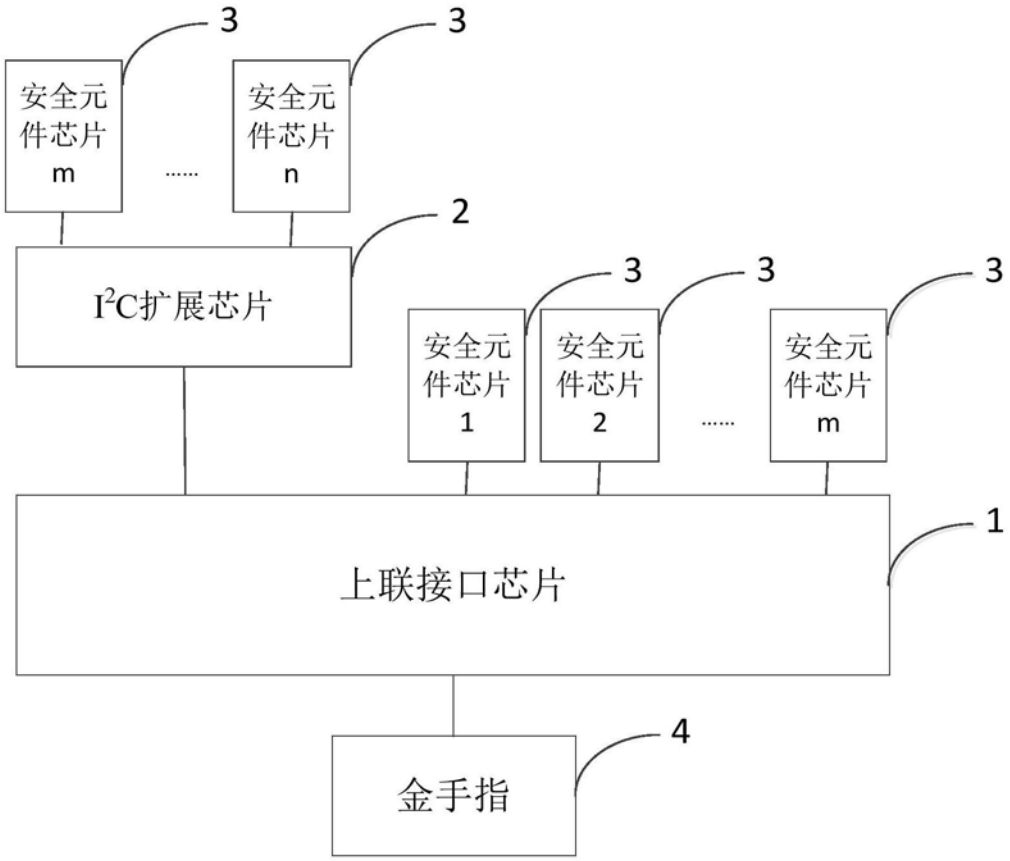

3
3
安全元件芯片m
……
安全元件芯片n
2
I²C扩展芯片
3
3
3
安全元件芯片1
安全元件芯片2
……
安全元件芯片m
1
上联接口芯片
4
金手指

图5

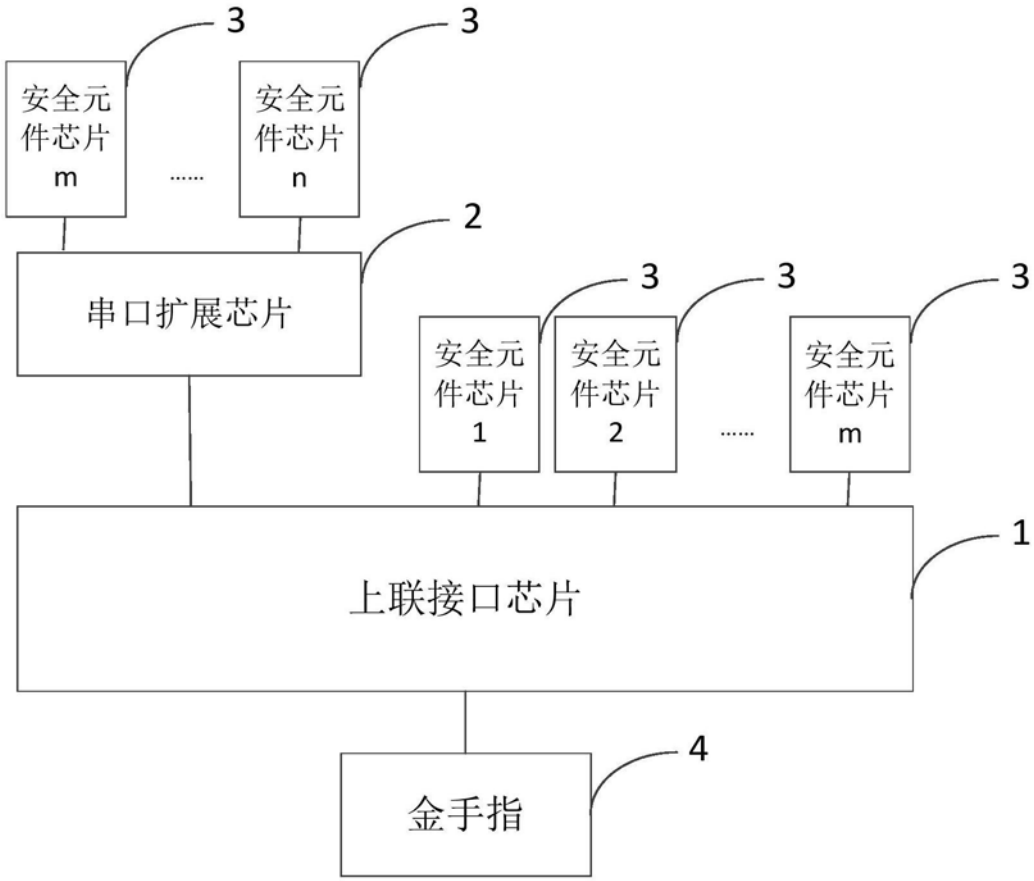

3
3
安全元件芯片m
……
安全元件芯片n
2
串口扩展芯片
3
3
3
安全元件芯片1
安全元件芯片2
……
安全元件芯片m
1
上联接口芯片
4
金手指

图6

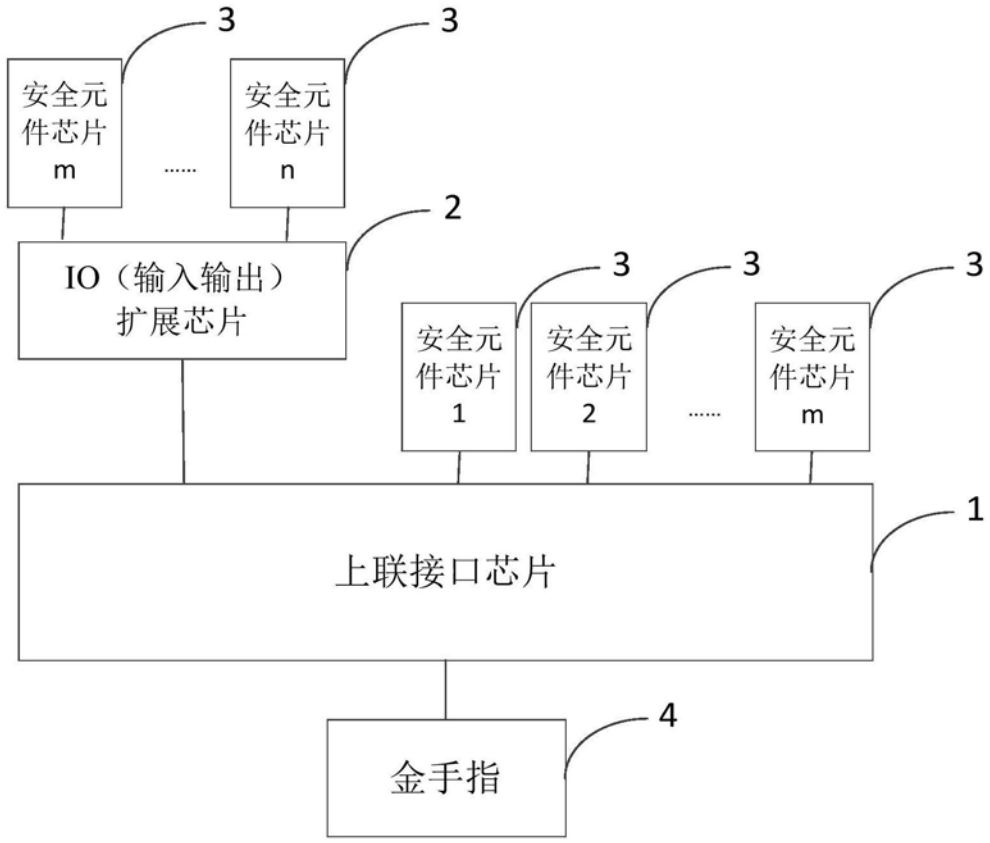

3
3
安全元件芯片m
……
安全元件芯片n
2
IO（输入输出）扩展芯片
3
3
3
安全元件芯片1
安全元件芯片2
……
安全元件芯片m
1
上联接口芯片
4
金手指

图7

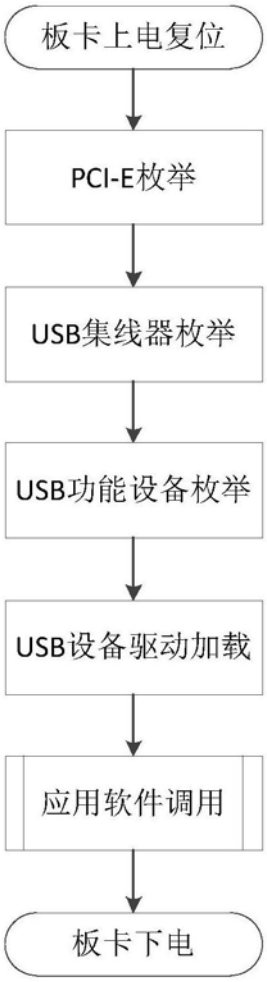


图8

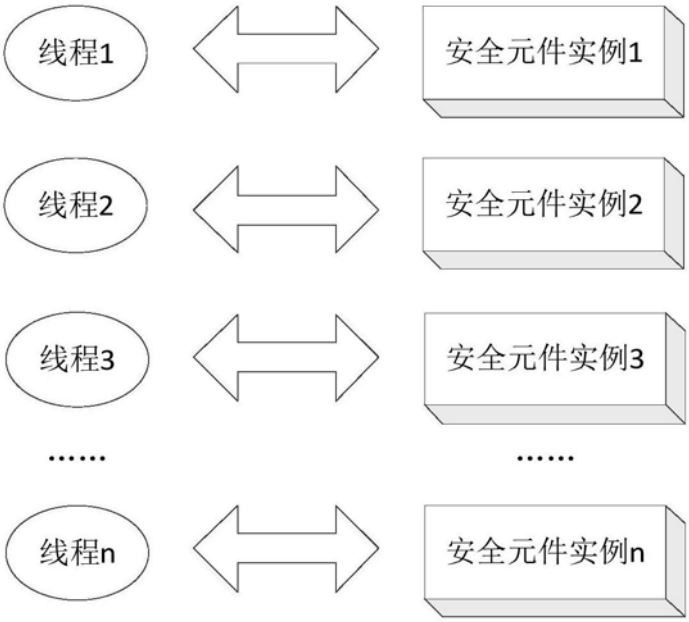

线程1
安全元件实例1
线程2
安全元件实例2
线程3
安全元件实例3
.....
.....
线程n
安全元件实例n

图9

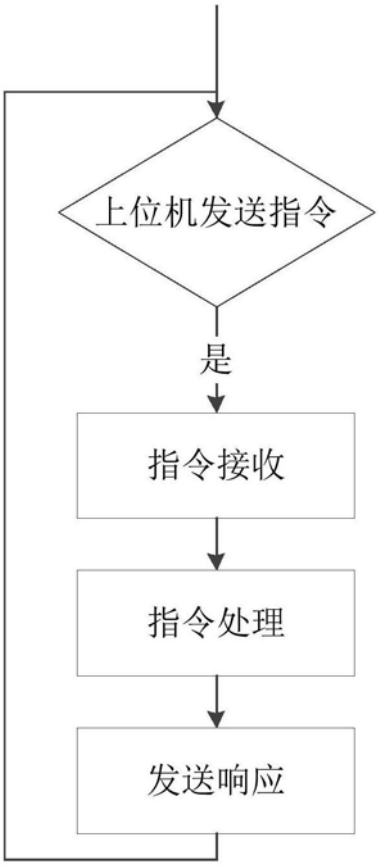

上位机发送指令
是
指令接收
指令处理
发送响应

图10