



(12)发明专利申请

(10)申请公布号 CN 106295374 A

(43)申请公布日 2017.01.04

(21)申请号 201610711941.5

(22)申请日 2016.08.23

(71)申请人 记忆科技(深圳)有限公司

地址 518057 广东省深圳市南山区蛇口后海大道东角头厂房D22/F、D13/F、D23/F、D14/F、D24/F、D15/F

(72)发明人 卞兴中 左文 贾宗铭 周振宇 张薇薇

(74)专利代理机构 广东广和律师事务所 44298 代理人 叶新民

(51)Int.Cl. G06F 21/60(2013.01) G06F 13/16(2006.01)

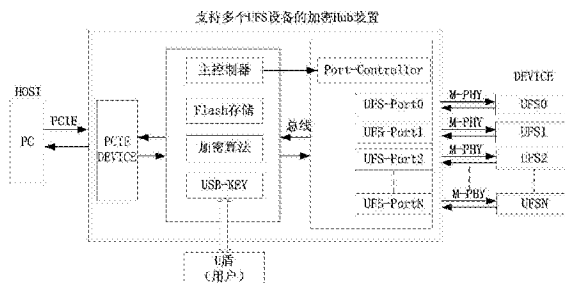
权利要求书2页 说明书3页 附图3页

(54)发明名称

一种支持多个UFS设备的加密Hub装置

(57)摘要

本发明提供了一种支持多个UFS设备的加密Hub装置,包括控制器、Flash存储模块、加解密模块和USB-KEY模块组成Hub加解密模块,Hub加解密模块与PCIE传输模块PCIE Device相连,通过PCIE接口与外部支持PCIE的外部PC主机相连;Hub加解密模块与端口控制器通过数据总线相连;端口控制器上设有多个M-PHY扩展接口;PC主机将要写入的数据经过Hub加解密模块实现加密后写入相应的M-PHY扩展接口上连接的UFS设备;Hub加解密模块实现将UFS设备上的加密数据进行解密后传输给PC主机。基于M-PHY接口的加密Hub实现了对M-PHY接口的扩展,且能够提高UFS数据传输的安全性,保证了UFS数据的安全性,同时具有USB-KEY自身兼容性高的特点,能够满足特殊用户的需求,灵活性大大提高。



1. 一种支持多个UFS设备的加密Hub装置,其特征在于包括主控制器、Flash存储模块、加解密算法模块、USB-KEY模块、PCIE传输模块PCIE Device和端口控制器Port-Controller;其中主控制器、Flash存储模块、加解密模块和USB-KEY模块组成Hub加解密模块,Hub加解密模块与PCIE传输模块PCIE Device相连,通过PCIE传输模块PCIE Device与外部支持PCIE的外部PC主机相连;Hub加解密模块与端口控制器Port-Controller通过数据总线相连;端口控制器Port-Controller上设有多个M-PHY扩展接口;PC主机将要写入的数据经过Hub加解密模块实现加密后写入相应的M-PHY扩展接口上连接的UFS设备;Hub加解密模块实现将UFS设备上的加密数据进行解密后传输给PC主机。

2. 根据权利要求1所述的支持多个UFS设备的加密Hub装置,其特征在于Hub加解密模块对数据的加解密包括2级控制,第一层加密通过USB-KEY模块实现对用户身份的认证;第二层加密通过加解密算法模块中的硬件加密模块进行加密或解密。

3. 根据权利要求2所述的支持多个UFS设备的加密Hub装置,其特征在于PC主机按照如下步骤进行写入操作:

步骤3.1:PC主机提出写入操作请求,对连接的UFS设备进行写入操作;

步骤3.2:主控制器接收到写入操作请求后,先启动USB-KEY模块对用户身份进行认证;主控制器从Flash存储模块的用户数据中取得正确的用户序列号;同时通过USB-KEY模块向用户发送验证要求,要求用户输入PIN码,并进行认证,认证通过后取得自定义序列号反馈给主控制器;

步骤3.3:主控制器接收到自定义序列号后,验证序列号是否正确;正确则从数据库中取得用户信息;主控制器启动特定运算获得内部摘要;同时向USB-KEY模块发送验证要求,在USB-KEY模块内部进行相应运算获得验证摘要,并发送回主控制器;

步骤3.4:将内部摘要和验证摘要进行校验,当校验失败返回PC主机本次数据写入失败;当校验成功允许用户对UFS设备进行数据写入;

步骤3.5:主控制器和PC主机软件自动确认UFS设备是否正常接入;如果是则允许PC主机给UFS设备分配地址,并通过端口控制器Port-Controller对该UFS设备进行初始化;

步骤3.6:PC主机的数据通过PCIE接口传送至PCIE传输模块PCIE Device,将数据存放至高速数据缓存区;

步骤3.7:主控制器通过加密算法模块,将数据进行加密之后,形成密文传经过总线发送至相应的M-PHY端口UFS-Port,端口控制器Port-Controller对数据包中的地址进行校验;校验成功则将加密后的密文件写入M-PHY扩展接入的UFS设备中,完成本次UFS设备的数据写入。

4. 根据权利要求2所述的支持多个UFS设备的加密Hub装置,其特征在于PC主机按照如下步骤进行读取操作:

步骤4.1:PC主机提出读操作请求,对连接的UFS设备进行读取操作;

步骤4.2:主控制器接收到写入操作请求后,先启动USB-KEY模块对用户身份进行认证;主控制器从Flash存储模块的用户数据中取得正确的用户序列号;同时通过USB-KEY模块向用户发送验证要求,要求用户输入PIN码,并进行认证,认证通过后取得自定义序列号反馈给主控制器;

步骤4.3:主控制器接收到自定义序列号后,验证序列号是否正确;正确则从数据库中

取得用户信息；主控制器启动特定运算获得内部摘要；同时向USB-KEY模块发送验证要求，在USB-KEY模块内部进行相应运算获得验证摘要，并发送回主控制器；

步骤4.4：将内部摘要和验证摘要进行校验，当校验失败返回PC主机本次数据读出失败；当校验成功允许用户对UFS设备进行数据读出；

步骤4.5：主控制器和PC主机软件自动确认UFS设备是否正常接入；如果是则允许PC主机给UFS设备分配地址，并通过端口控制器Port-Controller对该UFS设备进行初始化；M-PHY端口上的UFS设备发送数据通过UFS-Port发送至数据总线；

步骤4.6：主控制器通过加密算法模块将数据进行解密操作，将解密后数据传送至PCIE传输模块PCIE Device，将数据存放至高速数据缓存区；

步骤4.7：数据最后经过PCIE接口电路将读出至PC主机中；完成本次UFS设备数据读出操作。

一种支持多个UFS设备的加密Hub装置

技术领域

[0001] 本发明涉及数据传输安全领域,特别涉及一种支持多个UFS设备的加密Hub装置。

背景技术

[0002] 在电子信息高速发达的时代,人们越来越注重信息安全,信息安全本身包括的范围很大,大到国家军事政治机密,小到企业机密以及个人信息,任何一个安全漏洞都可能造成信息泄露。传输信息的方式很多,信息在存储、处理和交换的过程中,都存在泄密或被截收、窃听、篡改和伪造的可能性。单一的保密措施通常也难以保证通信和信息的安全,必须通过综合应用各种层次的保密措施实现信源、信号、信息三个环节的保护。

[0003] 在UFS存储领域,通常是通过M-PHY接口实现一对一的通讯,无法实现同时对多个UFS设备的管理,人们对于UFS接口的拓展需求越来越高。另外人们通常选择在UFS主控中植入加密模块,实现数据的密文存储,但仍存在数据在传输通道上被截取的可能性,存在较大的数据泄露风险,且无法满足用户特殊的需求,灵活性较差。

发明内容

[0004] 针对以上缺陷,本发明目的如何解决通过M-PHY标准进行数据传输通道中发生数据泄密的问题。

[0005] 为了解决以上问题,本发明提供了一种支持多个UFS设备的加密Hub装置,其特征在于包括主控制器、Flash存储模块、加解密算法模块、USB-KEY模块、PCIE传输模块PCIE Device和端口控制器Port-Controller;其中主控制器、Flash存储模块、加解密模块和USB-KEY模块组成Hub加解密模块,Hub加解密模块与PCIE传输模块PCIE Device相连,通过PCIE传输模块PCIE Device与外部支持PCIE的外部PC主机相连;Hub加解密模块与端口控制器Port-Controller通过数据总线相连;端口控制器Port-Controller上设有多个M-PHY扩展接口;PC主机将要写入的数据经过Hub加解密模块实现加密后写入相应的M-PHY扩展接口上连接的UFS设备;Hub加解密模块实现将UFS设备上的加密数据进行解密后传输给PC主机。

[0006] 所述的支持多个UFS设备的加密Hub装置,其特征在于Hub加解密模块对数据的加解密包括2级控制,第一层加密通过USB-KEY模块实现对用户身份的认证;第二层加密通过加解密算法模块中的硬件加密模块进行加密或解密。

[0007] 本发明所述的加密Hub实现了对M-PHY接口的扩展,且能够提高数据传输的安全性,保证了硬盘数据的安全性,同时具有USB-KEY自身兼容性高的特点,能够满足特殊用户的需求,灵活性大大提高。

附图说明

[0008] 图1是支持多个UFS设备的加密Hub装置系统框图;

[0009] 图2是写入操作流程示意图;

[0010] 图3是读取操作流程示意图。

具体实施方式

[0011] 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作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。

[0012] 图1是支持多个UFS设备的加密Hub装置系统框图;加密Hub装置包括主控制器、Flash存储模块、加解密算法模块、USB-KEY模块、PCIE传输模块PCIE Device和端口控制器Port-Controller;其中主控制器、Flash存储模块、加解密模块和USB-KEY模块组成Hub加解密模块,Hub加解密模块与PCIE传输模块PCIE Device相连,通过PCIE传输模块PCIE Device与外部支持PCIE的外部PC主机相连;Hub加解密模块与端口控制器Port-Controller通过数据总线相连;端口控制器Port-Controller上设有多个M-PHY扩展接口;PC主机将要写入的数据经过Hub加解密模块实现加密后写入相应的M-PHY扩展接口上连接的UFS设备;Hub加解密模块实现将UFS设备上的加密数据进行解密后传输给PC主机。

[0013] 图2是写入操作流程示意图;PC主机通过PCIE接口实现的加密Hub装置对UFS设备进行写入操作的流程:

[0014] 步骤3.1:PC主机提出写入操作请求,对连接的UFS设备进行写入操作;

[0015] 步骤3.2:主控制器接收到写入操作请求后,先启动USB-KEY模块对用户身份进行认证;主控制器从Flash存储模块的用户数据中取得正确的用户序列号;同时通过USB-KEY模块向用户发送验证要求,要求用户输入PIN码,并进行认证,认证通过后取得自定义序列号反馈给主控制器;

[0016] 步骤3.3:主控制器接收到自定义序列号后,验证序列号是否正确;正确则从数据库中取得用户信息;主控制器启动特定运算获得内部摘要;同时向USB-KEY模块发送验证要求,在USB-KEY模块内部进行相应运算获得验证摘要,并发送回主控制器;

[0017] 步骤3.4:将内部摘要和验证摘要进行校验,当校验失败返回PC主机本次数据写入失败;当校验成功允许用户对UFS设备进行数据写入;

[0018] 步骤3.5:主控制器和PC主机软件自动确认UFS设备是否正常接入;如果是则允许PC主机给UFS设备分配地址,并通过端口控制器Port-Controller对该UFS设备进行初始化;

[0019] 步骤3.6:PC主机的数据通过PCIE接口传送至PCIE传输模块PCIE Device,将数据存放至高速数据缓存区;

[0020] 步骤3.7:主控制器通过加密算法模块,将数据进行加密之后,形成密文传经过总线发送至相应的M-PHY端口UFS-Port,端口控制器Port-Controller对数据包中的地址进行校验;校验成功则将加密后的密文件写入M-PHY扩展接入的UFS设备中,完成本次UFS设备的数据写入

[0021] 用户输入验证key可通过用户插入U盾的方式实现用户验证数据的输入。

[0022] 图3是读取操作流程示意图;PC主机通过PCIE接口实现的加密Hub装置对UFS设备进行读出操作的流程:

[0023] 步骤4.1:PC主机提出读操作请求,对连接的UFS设备进行读取操作;

[0024] 步骤4.2:主控制器接收到写入操作请求后,先启动USB-KEY模块对用户身份进行

认证;主控制器从Flash存储模块的用户数据中取得正确的用户序列号;同时通过USB-KEY模块向用户发送验证要求,要求用户输入PIN码,并进行认证,认证通过后取得自定义序列号反馈给主控制器;

[0025] 步骤4.3:主控制器接收到自定义序列号后,验证序列号是否正确;正确则从数据库中取得用户信息;主控制器启动特定运算获得内部摘要;同时向USB-KEY模块发送验证要求,在USB-KEY模块内部进行相应运算获得验证摘要,并发送回主控制器;

[0026] 步骤4.4:将内部摘要和验证摘要进行校验,当校验失败返回PC主机本次数据读出失败;当校验成功允许用户对UFS设备进行数据读出;

[0027] 步骤4.5:主控制器和PC主机软件自动确认UFS设备是否正常接入;如果是则允PC主机给UFS设备分配地址,并通过端口控制器Port-Controller对该UFS设备进行初始化;M-PHY端口上的UFS设备发送数据通过UFS-Port发送至数据总线;

[0028] 步骤4.6:主控制器通过加密算法模块将数据进行解密操作,将解密后数据传送至PCIE传输模块PCIE Device,将数据存放至高速数据缓存区;

[0029] 步骤4.7:数据最后经过PCIE接口电路将读出至PC主机中;完成本次UFS设备数据读出操作。

[0030] 以上所揭露的仅为本发明一种实施例而已,当然不能以此来限定本权利范围,本领域普通技术人员可以理解实现上述实施例的全部或部分流程,并依本发明权利要求所作的等同变化,仍属于本发明所涵盖的范围。

支持多个UFS设备的加密Hub装置

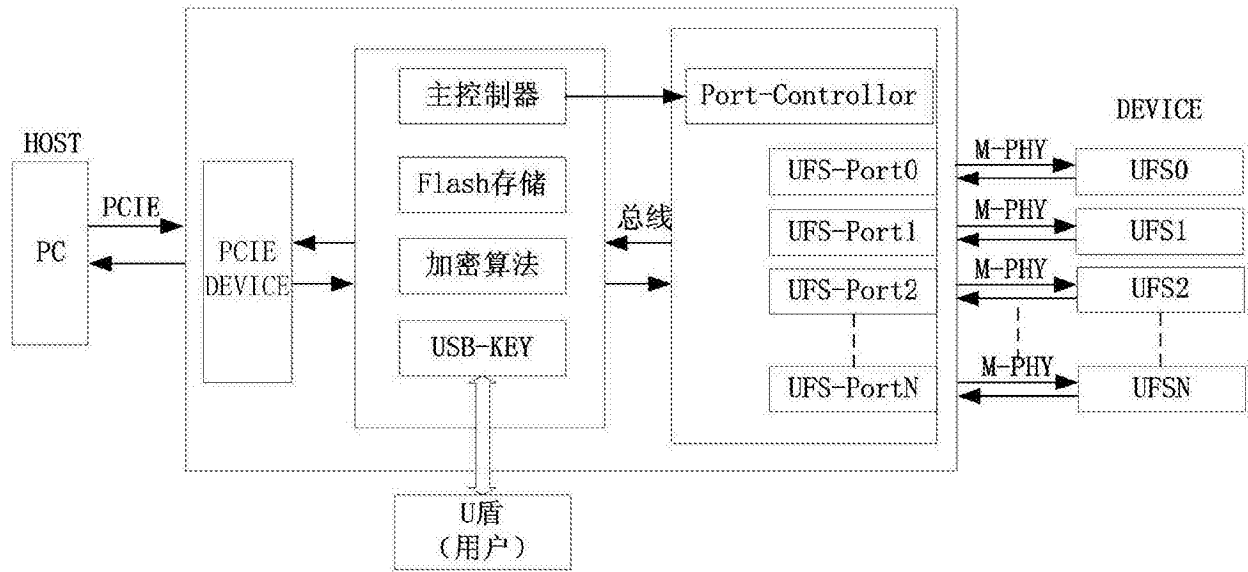


图1

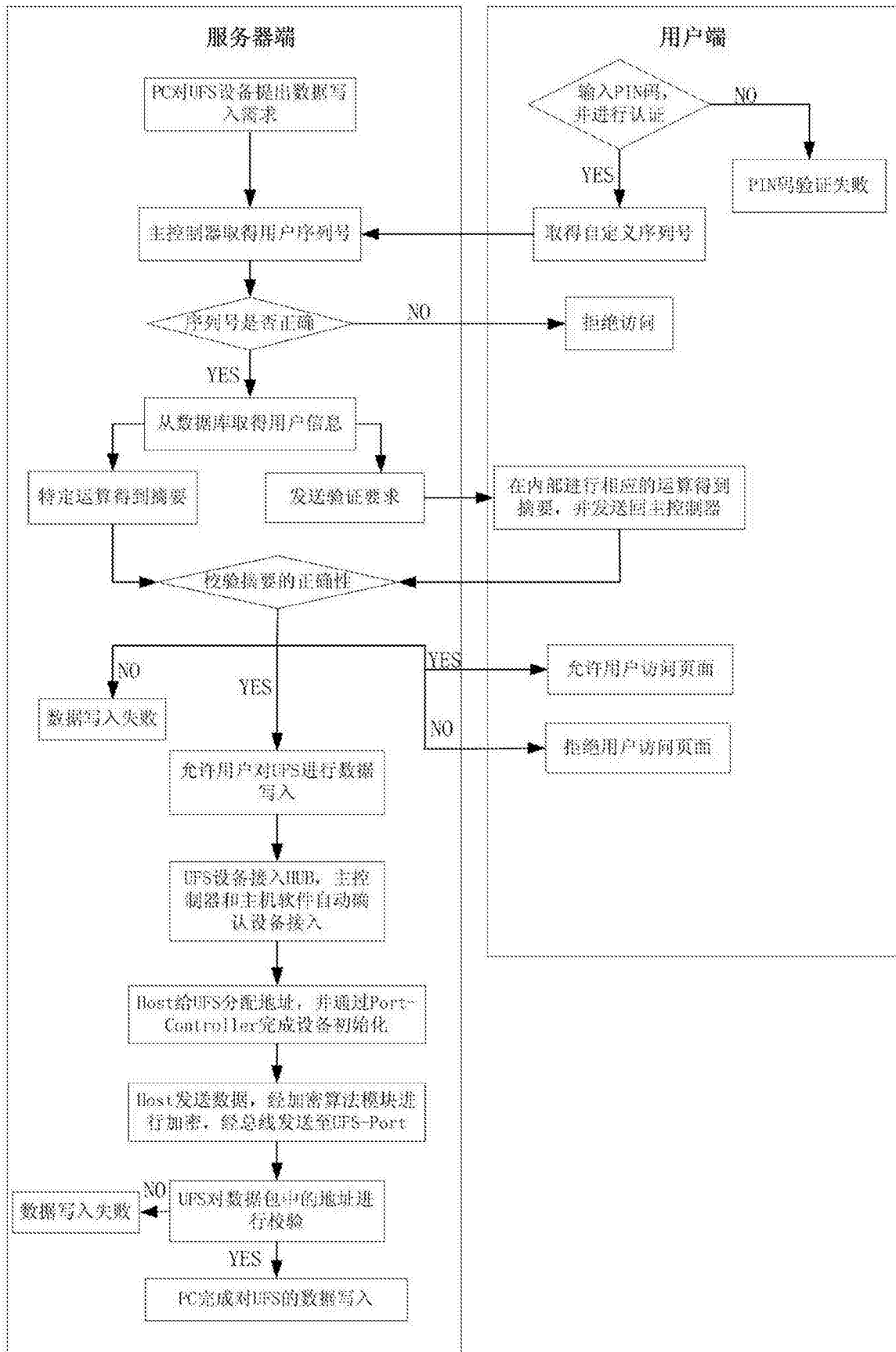


图2

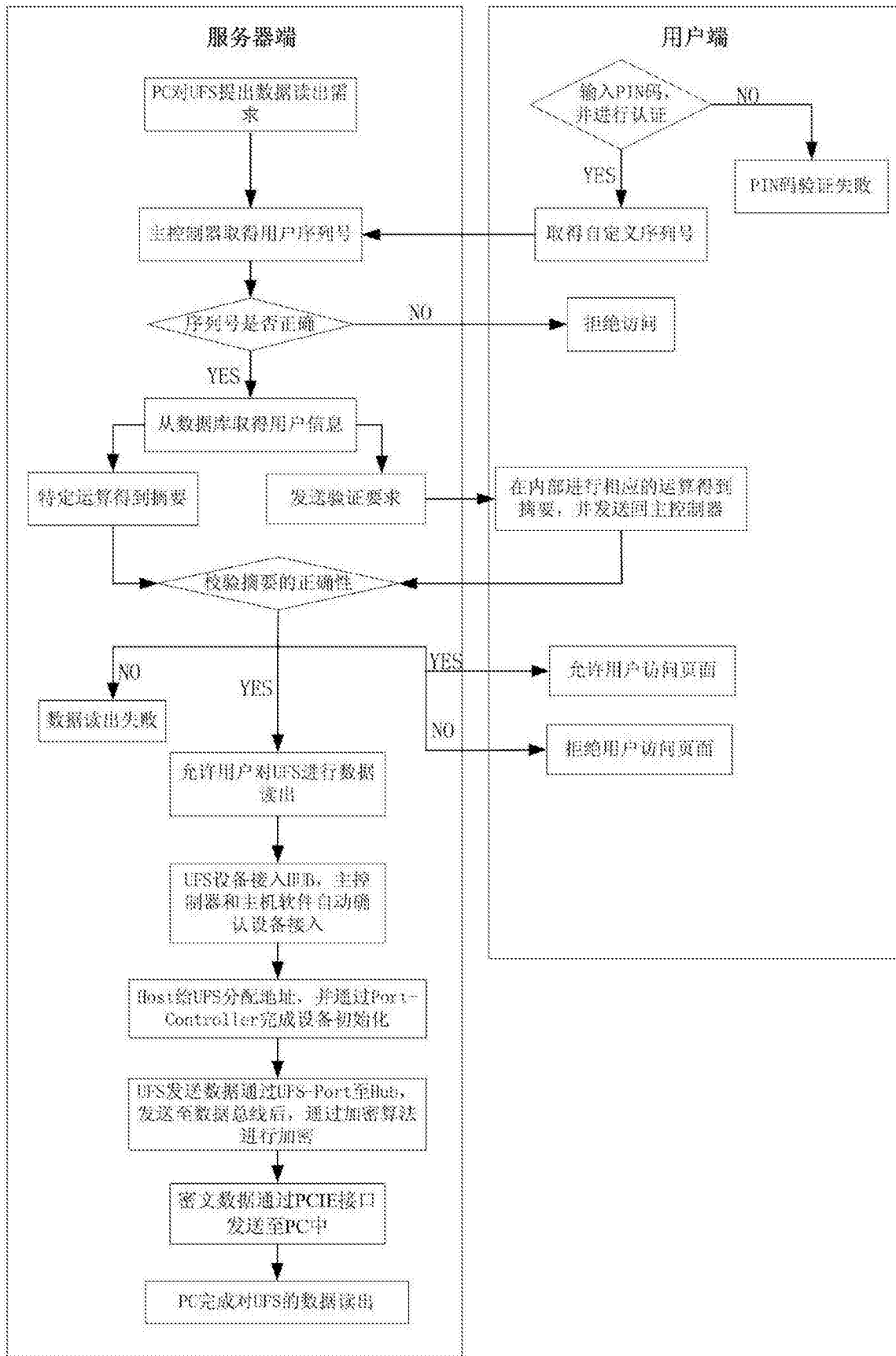


图3