(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 106027235 B
(45)授权公告日 2019.05.17

(21)申请号 201610320081.2

(22)申请日 2016.05.13

(65)同一申请的已公布的文献号
申请公布号 CN 106027235 A

(43)申请公布日 2016.10.12

(73)专利权人 北京三未信安科技发展有限公司
地址 100101 北京市朝阳区北苑路170号3号楼22层1单元2602

(72)发明人 张玉国 桑洪波

(74)专利代理机构 北京轻创知识产权代理有限公司 11212
代理人 杨立

(51)Int.Cl.
H04L 9/08(2006.01)

(56)对比文件
CN 1996321 A,2007.07.11,
CN 101938359 A,2011.01.05,
CN 201527654 U,2010.07.14,
CN 102664739 A,2012.09.12,
CN 102006162 A,2011.04.06,
山东渔翁信息技术有限公司.PCI密码卡产品详情.《PCI密码卡产品详情》.2014,

审查员 吴超

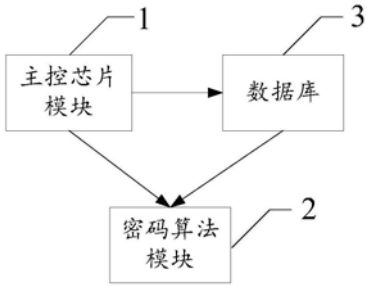
权利要求书1页 说明书5页 附图2页

(54)发明名称

一种PCI密码卡和海量密钥密码运算方法及系统

(57)摘要

本发明涉及一种PCI密码卡和海量密钥密码运算方法及系统，其中PCI密码卡，其特征在于，包括主控芯片模块，所述主控芯片模块将PCI密码卡中的多种明文密钥加密生成密文密钥。本发明的密文密钥存储的大小可以根据操作系统灵活配置，支持几百M甚至上G字节，可以满足客户的对海量密钥的需求。本发明杜绝密钥以明文形式出现在操作系统内存中，确保密钥的安全性。客户灵活配置存储空间大小，满足客户对海量密钥的需求。



CN 106027235 B

1.一种PCI密码卡,其特征在于,包括主控芯片模块和密码算法模块,所述主控芯片模块将PCI密码卡中的多种明文密钥加密生成密文密钥;

所述主控芯片模块通过设定的系统保护密钥对所有明文密钥进行加密并存入外部数据库;

所述系统保护密钥以SM2数字信封格式进行保存;

当主控芯片模块接收密码运算业务时,所述密码算法模块根据主控芯片模块的控制调用数据库中的密文密钥并解密得到明文密钥,并将明文密钥返回到主控芯片模块。

2.如权利要求1所述的一种PCI密码卡,其特征在于,所述密码算法模块通过设定的系统保护密钥对密文密钥进行解密。

3.如权利要求1或2所述的一种PCI密码卡,其特征在于,所述明文密钥包括对称密钥、SM2密钥对和RSA密钥对。

4.如权利要求3所述的一种PCI密码卡,其特征在于,所述主控芯片模块采用对称加密算法对所述明文密钥进行加密。

5.一种海量密钥密码运算系统,其特征在于,包括如权利要求1-4任一项所述的PCI密码卡和存储有密文密钥的数据库;

所述PCI密码卡接收密码运算业务,读取数据库中的密文密钥;

所述PCI密码卡并对密文密钥进行解密得到明文密钥,对密码运算业务根据得到的明文密钥进行密码运算,得到运算结果并反馈。

6.如权利要求5所述的一种海量密钥密码运算系统,其特征在于,还包括API接口,所述API接口将接收到的密码运算业务分配对应的命令码,并将对应的密钥类型和密码运算业务数据根据命令码进行打包为数据包,并将数据包传输到PCI密码卡;

所述API接口将PCI密码卡得到运算结果进行反馈。

7.一种海量密钥密码运算方法,其特征在于,其应用如权利要求1-4任一项所述的PCI密码卡,包括以下步骤:

步骤1:PCI密码卡接收密码运算业务,读取数据库中的密文密钥;

步骤2:对密文密钥进行解密得到明文密钥,对密码运算业务根据得到的明文密钥进行密码运算,得到运算结果并反馈。

一种PCI密码卡和海量密钥密码运算方法及系统

技术领域

[0001] 本发明涉及一种PCI密码卡和海量密钥密码运算方法及系统，属于信息安全领域。

背景技术

[0002] 中国信息产业发展迅速，电子商务、电子政务应用逐渐普及，网上银行、网上证券、网上购物等应用平台不断的推陈出新。大数据、云存储也蓬勃发展。不仅仅是行业用户，企业和个人用户对安全的认识也逐步加深，尤其近几年，基于企业级的安全应用平台和相关的产品得到了广泛的应用。PCI密码卡是以PCI局部总线或者PCI Express为接口，具有密码运算功能、密钥管理功能、物理随机数产生功能和设备自身安全保护措施的密码设备，PCI密码卡可以应用在需要密码运算和密钥管理等安全功能的、具有PCI局部总线或者PCI Express的通信设备、计算机设备、安全保密设备上，例如：虚拟专网(VPN)设备、证书中心(CA)系统的有关设备、网络密码机、安全服务器、安全终端、安全管理中心、密钥管理设备等。SM2椭圆曲线公钥密码算法和RSA算法都是公钥密码算法，SM2算法是一种更先进安全的算法，在我们国家商用密码体系中被用来替换RSA算法。

[0003] PCI密码卡设备提供最基本的密码运算、密钥管理功能。通用的PCI密码卡管理模式采用数字信号处理芯片(DSP)等芯片做为PCI密码卡的主控芯片，EEPROM或SPI FLASH做为PCI密码卡的密钥的存储介质。PCI密码卡可以对对称密钥、RSA密钥对、SM2密钥对等进行存储和管理。密钥存储在PCI密码卡内部与操作系统隔离，应用中也不会出现在操作系统的内存中，基于PCI密码卡可以研发成为服务器密码机、VPN、签名验证服务器、安全网关等密码安全设备。

[0004] 随着互联网应用的不断发展，安全技术逐渐深入到信息领域的各个方面，用户对安全设备在高效性、稳定性、易用性、可管理性和可移植性等各方面的需求会不断提高。PCI密码卡在实际应用中面临新的需求，客户使用的密钥数量愈发的增多，出现了需要成千上万个密钥的需求等，作为密钥安全存储介质的PCI密码卡，因存储功能有限越来越不能满足人们的日常需求。

[0005] 解决海量密钥管理现存方案是增大PCI密码卡的存储芯片，换用更大的存储芯片可以暂时缓解PCI密码卡存储空间不足的问题，但是治标不治本。且换用大型存储芯片需要考虑芯片的封装对原有PCI密码卡PCB制版的兼容性，新的存储芯片很有可能导致PCI密码卡硬件版图重新设计，硬件的变动周期较长且可能对PCI密码卡的稳定性造成影响。面对客户对密钥数量日益增多的需求，更换芯片的方案从长远角度看来不可行。

发明内容

[0006] 本发明所要解决的技术问题是提供一种解决了PCI密码卡海量密钥管理的问题，密钥使用过程中安全可靠的PCI密码卡和海量密钥密码运算方法及系统。

[0007] 本发明解决上述技术问题的技术方案如下：一种PCI密码卡，包括主控芯片模块，所述主控芯片模块将PCI密码卡中的多种明文密钥加密生成密文密钥。

[0008] 本发明的有益效果是:密文密钥存储的大小可以根据操作系统灵活配置,支持几百M甚至上G字节,可以满足客户的对海量密钥的需求。本发明杜绝密钥以明文形式出现在操作系统内存中,确保密钥的安全性。客户灵活配置存储空间大小,满足客户对海量密钥的需求。

[0009] 在上述技术方案的基础上,本发明还可以做如下改进。

[0010] 进一步,所述主控芯片模块将PCI密码卡中的多种明文密钥加密生成密文密钥。

[0011] 进一步,所述主控芯片模块通过设定的系统保护密钥对所有明文密钥进行加密并存入外部数据库。

[0012] 进一步,所述系统保护密钥以SM2数字信封格式进行保存。

[0013] 进一步,还包括密码算法模块;

[0014] 当主控芯片模块接收密码运算业务时,所述密码算法模块根据主控芯片模块的控制调用数据库中的密文密钥并解密得到明文密钥,并将明文密钥返回到主控芯片模块。

[0015] 采用上述进一步方案的有益效果是,杜绝了操作系统或上层应用程序通过任何形式获取,保证了密钥的安全性。

[0016] 进一步,所述密码算法模块通过设定的系统保护密钥对密文密钥进行解密。

[0017] 进一步,所述明文密钥包括对称密钥、SM2密钥对和RSA密钥对。

[0018] 进一步,所述主控芯片模块采用对称加密算法对所述明文密钥进行加密。

[0019] 本发明解决上述技术问题的技术方案如下:一种海量密钥密码运算系统,包括如上所述的PCI密码卡和存储有密文密钥的数据库;

[0020] 所述PCI密码卡接收密码运算业务,读取数据库中的密文密钥;

[0021] 所述PCI密码卡并对密文密钥进行解密得到明文密钥,对密码运算业务根据得到的明文密钥进行密码运算,得到运算结果并反馈。

[0022] 本发明的有益效果是:本发明通过灵活的访问数据库,产生密钥时,将密文密钥写入数据库;密码运算时,通过驱动程序读取数据库密文密钥;本发明杜绝密钥以明文形式出现在操作系统内存中,确保密钥的安全性。客户灵活配置存储空间大小,满足客户对海量密钥的需求。

[0023] 在上述技术方案的基础上,本发明还可以做如下改进。

[0024] 进一步,还包括API接口,所述API接口将接收到的密码运算业务分配对应的命令码,并将对应的密钥类型和密码运算业务数据根据命令码进行打包为数据包,并将数据包传输到PCI密码卡;

[0025] 所述API接口将PCI密码卡得到运算结果进行反馈。

[0026] 本发明解决上述技术问题的技术方案如下:一种海量密钥密码运算方法,应用如上所述的PCI密码卡,包括以下步骤:

[0027] 步骤1:PCI密码卡接收密码运算业务,读取数据库中的密文密钥;

[0028] 步骤2:对密文密钥进行解密得到明文密钥,对密码运算业务根据得到的明文密钥进行密码运算,得到运算结果并反馈。

[0029] 本发明的有益效果是:本发明通过灵活的访问数据库,产生密钥时,将密文密钥写入数据库;密码运算时,通过驱动程序读取数据库密文密钥;本发明杜绝密钥以明文形式出现在操作系统内存中,确保密钥的安全性。客户灵活配置存储空间大小,满足客户对海量密

钥的需求。

[0030] 在上述技术方案的基础上，本发明还可以做如下改进。

[0031] 进一步，所述步骤1具体包括以下内容：

[0032] 将接收到的密码运算业务分配对应的命令码，并将对应的密钥类型和密码运算业务数据根据命令码进行打包为数据包，并将数据包传输到PCI密码卡；

[0033] 所述PCI密码卡根据接收的命令码对数据包解析，获得密钥类型和密码运算业务数据；并根据密钥类型调用数据库中的密文密钥。

[0034] 目前基于密钥机制的密码算法有对称算法和公开算法两种，对称算法国际上应用较多的是DES、3DES、AES等算法而国内主要使用SM1、SM4等算法，对称算法其应用的密钥统称对称密钥。与之对应的是公开算法，国际上应用较多的是RSA算法而国内主推的是SM2算法，公开算法使用的密钥称为RSA密钥对和SM2密钥对。因对称加密算法的性能较公开算法性能高且对称加密算法的密钥为16字节随机数便于作为系统主密钥。因此，当产生对称密钥、SM2密钥对、RSA密钥时，主控芯片控制系统使用系统主密钥采用对称加密算法将对称密钥、SM2密钥对、RSA密钥对进行加密包装形成密文密钥。

附图说明

[0035] 图1为本发明所述的一种PCI密码卡结构示意图；

[0036] 图2为本发明所述的一种海量密钥密码运算系统结构框图；

[0037] 图3为本发明所述的一种海量密钥密码运算方法流程图。

[0038] 附图中，各标号所代表的部件列表如下：

[0039] 1、主控芯片模块，2、密码算法模块，3、数据库，4、API接口，10、PCI密码卡。

具体实施方式

[0040] 以下结合附图对本发明的原理和特征进行描述，所举实例只用于解释本发明，并非用于限定本发明的范围。

[0041] 如图1所示，为本发明所述的一种PCI密码卡，一种PCI密码卡，包括主控芯片模块1，所述主控芯片模块1将PCI密码卡中的多种明文密钥加密生成密文密钥。

[0042] 所述主控芯片模块1将PCI密码卡中的多种明文密钥加密生成密文密钥。

[0043] 所述主控芯片模块1通过设定的系统保护密钥对所有明文密钥进行加密并存入外部数据库3。

[0044] 所述系统保护密钥以SM2数字信封格式进行保存。

[0045] 还包括密码算法模块2；

[0046] 当主控芯片模块1接收密码运算业务时，所述密码算法模块2根据主控芯片模块1的控制调用数据库3中的密文密钥并解密得到明文密钥，并将明文密钥返回到主控芯片模块1。

[0047] 所述密码算法模块2通过设定的系统保护密钥对密文密钥进行解密。

[0048] 所述明文密钥包括对称密钥、SM2密钥对和RSA密钥对。

[0049] 所述主控芯片模块1采用对称加密算法对所述明文密钥进行加密。

[0050] 如图2所示，为本发明所述的一种海量密钥密码运算系统，包括如上所述的PCI密

码卡10和存储有密文密钥的数据库3；

[0051] 所述PCI密码卡10接收密码运算业务，读取数据库3中的密文密钥；

[0052] 所述PCI密码卡10并对密文密钥进行解密得到明文密钥，对密码运算业务根据得到的明文密钥进行密码运算，得到运算结果并反馈。

[0053] 还包括API接口4，所述API接口4将接收到的密码运算业务分配对应的命令码，并将对应的密钥类型和密码运算业务数据根据命令码进行打包为数据包，并将数据包传输到PCI密码卡；

[0054] 所述API接口4将PCI密码卡得到运算结果进行反馈。

[0055] 如图3所示，为本发明所述的一种海量密钥密码运算方法，其应用如上所述的PCI密码卡，包括以下步骤：

[0056] 步骤1:PCI密码卡接收密码运算业务，读取数据库中的密文密钥；

[0057] 步骤2:对密文密钥进行解密得到明文密钥，对密码运算业务根据得到的明文密钥进行密码运算，得到运算结果并反馈。

[0058] 所述步骤1具体包括以下内容：

[0059] 将接收到的密码运算业务分配对应的命令码，并将对应的密钥类型和密码运算业务数据根据命令码进行打包为数据包，并将数据包传输到PCI密码卡；

[0060] 所述PCI密码卡根据接收的命令码对数据包解析，获得密钥类型和密码运算业务数据;并根据密钥类型调用数据库中的密文密钥。

[0061] 本发明具体示例所述的一种海量密钥密码运算方法，包括以下步骤：

[0062] 1.客户应用程序调用接口服务程序提供的API接口发起密码运算请求，API接口会将各密码算法转换为不同的命令码并将密钥号及业务数据等数据打包；

[0063] 2.为接口服务程序通过驱动程序将数据包传送至PCI密码卡；

[0064] 3.PCI密码卡的主控芯片模块，根据命令码对请求包进行解析得到待运算的算法类型、待运算的密钥号等信息，并通过驱动程序读取数据库密文密钥信息并调用对称密码算法解密密文密钥；

[0065] 4.主控芯片模块使用明文密钥调用密码算法模块，进行密码运算；

[0066] 5.主控芯片模块，通过驱动将业务返回接口服务程序。

[0067] 接口服务程序运行在操作系统上，客户可以在本机上或通过网络调用接口库，接口库接收业务并将业务通过驱动程序发送给PCI密码卡主控芯片模块，PCI密码卡主控芯片模块解析业务并访问数据库或者调用PCI密码卡算法模块，处理业务后通过驱动程序返回接口服务程序。

[0068] 主控芯片模块的系统主密钥体系有完善的产生、导入及销毁的体制。系统主密钥由用户产生及安全存储，以SM2数字信封方式导入PCI密码卡。系统主密钥不会以明文形式出现在传输过程中。

[0069] 产生密钥时，密钥使用PCI密码卡内部系统主密钥和对称算法加密成密钥密文，密钥密文由主控芯片控制系统写入数据库中。

[0070] 运算时主控芯片控制系统解析业务并读取密文密钥，在PCI密码卡主控芯片中解密密钥并调用密码算法模块完成密码运算并将将运算数据返回接口服务程序。

[0071] 根据需求调整数据库大小，PCI密码卡可以访问自定义的密钥数量，完善主控芯片

控制系统访问数据库机制，可以进一步实现密钥的产生、导出公钥、导入密钥、备份恢复等功能，使得PCI密码卡具备完整的密钥管理功能。

[0072] 以上实施过程在已有PCI密码卡上进行了验证，并取得成功。本发明使用已有硬件设备，结合新型PCI密码卡软件系统(接口服务程序、主控芯片模块及数据库)，PCI密码卡可以灵活使用大量的密钥，满足了客户使用海量密钥的需求。

[0073] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

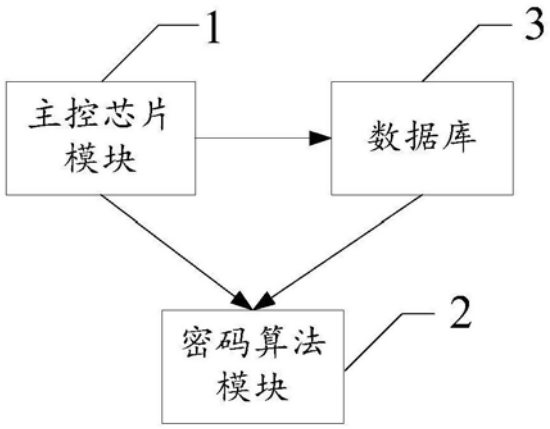

1
3
主控芯片模块
数据库
密码算法模块
2

图1

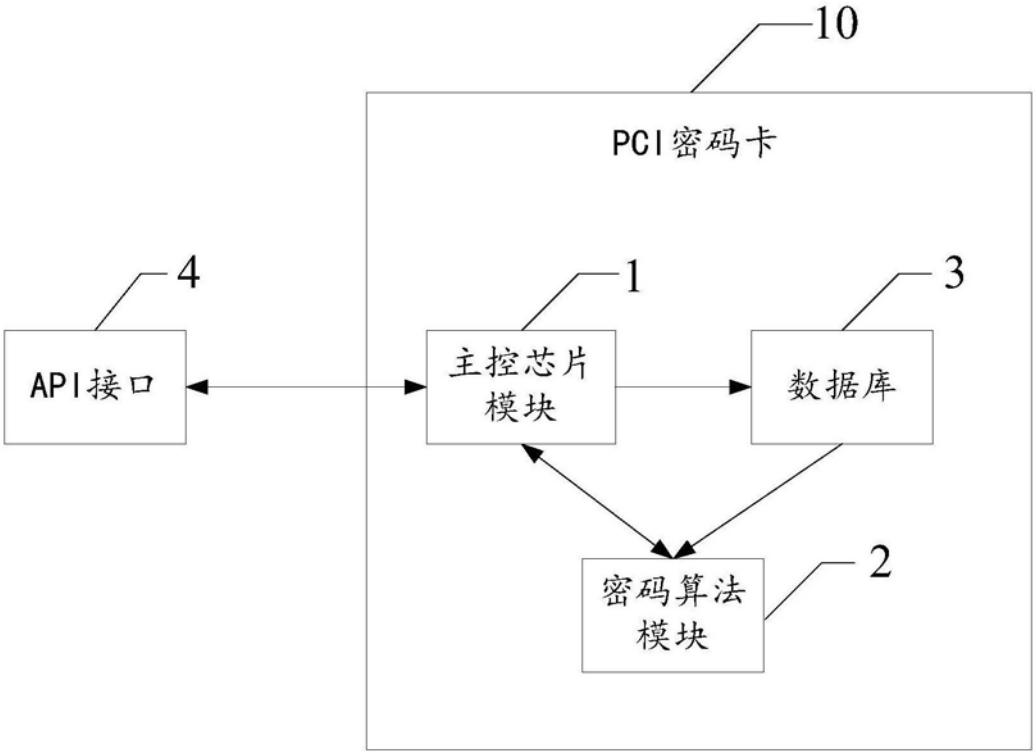

10
PCI密码卡
4
1
3
API接口
主控芯片模块
数据库
密码算法模块
2

图2

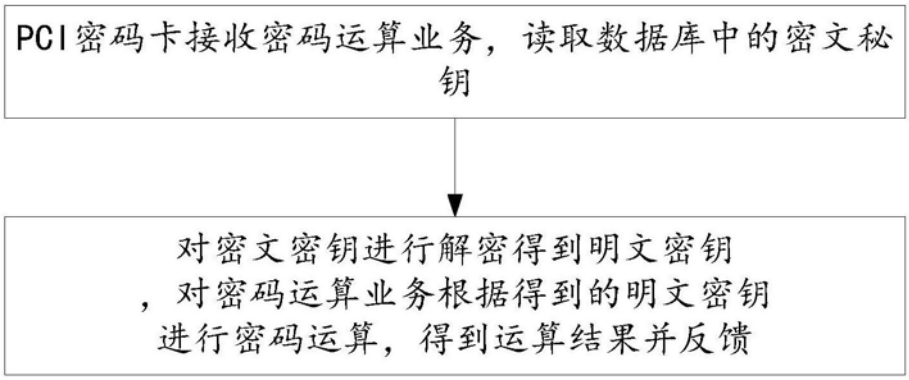

PCI密码卡接收密码运算业务，读取数据库中的密文秘钥
对密文密钥进行解密得到明文密钥，对密码运算业务根据得到的明文密钥进行密码运算，得到运算结果并反馈

图3