(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 1878055 B
(45)授权公告日 2010.11.03

(21)申请号 200510074866.8

(22)申请日 2005.06.07

(73)专利权人 北京握奇数据系统有限公司
地址 100015 北京市朝阳区首都机场路万红西街2号

(72)发明人 胡鹏 李勇

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 李欣

(51)Int.Cl.
H04L 9/00(2006.01)

(56)对比文件
CN 2691172 Y,2005.04.06,说明书第3页第10行至第4页第16行、图1-2、权利要求1-4.
CN 1571399 A,2005.01.26,说明书第4页第4-20行.

审查员 阎赛

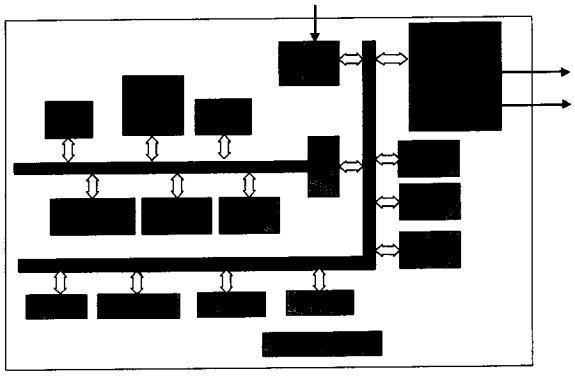
权利要求书 1 页 说明书 7 页 附图 5 页

(54)发明名称

一种分离式大数据量加/解密设备及实现方法

(57)摘要

本发明为一种分离式大数据量加/解密设备及实现方法。包括微处理器、存储器、安全检测与保护模块、协处理器、随机数函数发生器、中断控制器等,还包括一外部通讯接口模块,它连接外围数据总线,用于在加/解密设备与外部终端之间传递数据。加/解密设备通过通用串行总线接口接收终端发送的需要进行加/解密处理的数据包;加/解密设备将数据包存储到加/解密设备的存储器中;微处理器判断数据包中是否包含加/解密命令控制字,不是则用基本处理方式处理数据,是则调用对称或非对称算法对数据进行加/解密处理,并存入存储器;加/解密设备将经过加/解密的数据包以批传送方式通过通用串行总线接口发送给终端。



CN 1878055 B

1. 一种分离式大数据量加 / 解密设备，包括微处理器、电可擦除只读数据存储器、静态存储器、闪存、乘法协处理器、存储管理保护模块、安全检测与保护模块、非对称算法协处理器、对称算法协处理器、随机数函数发生器、时钟处理模块、电源管理模块、中断控制器、定时器，所述微处理器、可擦除只读数据存储器、静态存储器、闪存、乘法协处理器、存储管理保护模块通过核心数据总线相连，并通过桥连接器与连接有安全检测与保护模块、非对称算法协处理器、对称算法协处理器、随机数函数发生器、时钟处理模块，电源管理模块、中断控制器、定时器的外围总线相连接，其特征在于，该设备还包括 ：

一外部通讯接口模块，外部通讯接口模块连接外围数据总线，用于在加 / 解密设备与外部终端之间采用数据通讯协议命令传递数据，所述数据通讯协议命令包括卡头选择命令字、通讯选择命令字、流控制字、数据长度字、数据域 ；

所述微处理器，用于判断接收到的数据中是否包含加 / 解密命令控制字，不是则用基本处理方式处理数据，是则根据存储器中本地产生的密钥调用对称或非对称算法对所述加 / 解密命令控制字对应通道中的数据进行加 / 解密处理，并存入存储器中。

2. 根据权利要求 1 所述的分离式大数据量加 / 解密设备，其特征在于，所述微处理器为 32 位的多级流水线精简指令计算处理器，能支持硬件的安全访问控制和外围组件的访问控制。

3. 根据权利要求 1 所述的分离式大数据量加 / 解密设备，其特征在于，所述外部通讯接口模块至少包括通用串行总线架构接口模块、IS07816 接口模块。

4. 一种分离式大数据量加 / 解密实现方法，其特征在于，该方法包括以下步骤 ：

步骤 1、加 / 解密设备通过通用串行总线接口接收终端发送的根据数据通讯协议命令整合后的需要进行加 / 解密处理的数据包，所述数据通讯协议命令包括卡头选择命令字、通讯选择命令字、流控制字、数据长度字、数据域 ；

步骤 2、加 / 解密设备将数据包存储到加 / 解密设备的存储器中 ；

步骤 3、微处理器判断数据包中是否包含加 / 解密命令控制字，不是则用基本处理方式处理数据，是则根据加 / 解密设备存储器中本地产生的密钥调用对称或非对称算法对所述加 / 解密命令控制字对应通道中的数据进行加 / 解密处理，并存入存储器中 ；

步骤 4、加 / 解密设备将经过加 / 解密的数据包以批传送方式通过通用串行总线接口发送给终端。

5. 根据权利要求 4 所述的分离式大数据量加 / 解密实现方法，其特征在于，所述步骤 1 中的终端为有线终端、无线终端或手持终端。

6. 根据权利要求 4 所述的分离式大数据量加 / 解密实现方法，其特征在于，所述步骤 2 中的数据包为 64 字节。

7. 根据权利要求 4 所述的分离式大数据量加 / 解密实现方法，其特征在于，所述步骤 3 中的加 / 解密命令控制字的长度为 2 字节。

8. 根据权利要求 4 所述的分离式大数据量加 / 解密实现方法，其特征在于，所述步骤 3 中的加 / 解密命令控制字的低 3 位为进行流信息加 / 解密操作的通道标识。

9. 根据权利要求 4 所述的分离式大数据量加 / 解密实现方法，其特征在于，所述步骤 3 还包括对密钥进行加 / 解密的步骤。

一种分离式大数据量加/解密设备及实现方法

技术领域

[0001] 本发明涉及通信和信息安全技术领域，尤其涉及一种分离式大数据量加/解密设备及实现方法。

[0002] 技术背景

[0003] 随着计算机技术和互联网技术的迅猛发展，许多政府部门、企业和其它机构以及个人建立了自己的计算机网络系统，利用互联网在自己与大众之间建立了一条快速、高效的网络通道，电子商务和电子政务成为他们通过网络提供各种服务和获得信息的主要方式之一。基于互联网的信息服务系统具有明显的行业特点，所以网络中数据传输的安全性显得尤为重要，如网上银行交易、网上税务申报、网上企业年检等。系统中有大量需要保密的信息，在网络传递过程中必须采用加密保护的方式，以保护敏感数据的安全传输。同时，除了在网络应用中的数据传递外，用户终端内的数据，如硬盘中的数据也存在加密保护存取的需求，当攻击者从用户的终端中拆卸下硬盘，并在安装在另一个终端上时，由于其硬盘上的大量系统数据采用了加密保存的方式，攻击者就无法轻易了解和破解其信息，从而保护了数据的安全性。

[0004] 虽然人们对于网络信息服务系统和用户本地数据需要采用加密技术已经达成共识，并采用各种加密技术手段进行保护，如用集成电路卡（IC）技术和软件模块等来提高身份认证等加密技术的可靠性，但由于资金，技术成熟度等客观条件的限制，目前绝大部分的系统仍然采用软加密的方式，进行简单的数据加密保护。

[0005] 软加密技术是指加/解密密钥由密钥的生成端如IC卡或软件模块产生，利用终端的中央处理器（CPU）和内存完成加/解密操作。但由于“软加密”技术使用的密钥需要由生成端通过系统的通讯层提供给终端并保存在终端内存中，当攻击者监听用户终端的通讯层或窃取终端内存数据时，就可简单地获取加/解密密钥，从而轻易地破解加密数据。同时，由于需要加/解密的数据都要利用终端的CPU和内存完成计算，系统的大量宝贵资源也将被占用。

[0006] 针对上述软加密技术中存在的易破解和占用系统资源等问题，人们提出了使用硬加密技术的方式来实现对数据的加密操作。在现有技术中，硬加密技术多采用在终端内部安装一块加密芯片或插入一块加密卡的方式，利用此设备上自带的微处理器产生加/解密密钥，同时在芯片内部完成对需要加/解密的数据的加/解密计算。但是，由于此方法需要在终端内部安装一块加密芯片或插入一块加密卡，给用户带来了使用上的较大不便，而且，由于此加密芯片或加密卡多数都是由国外厂商提供，所以其价格昂贵，即便是国产的一般也在几千元至几万元不等，不利于向普通用户推广使用。

发明内容

[0007] 为克服现有技术的不足，本发明的目的在于提供一种分离式大数据量加/解密设备及实现方法，对高速传递的大数据量进行加/解密，安全性高，成本相对低廉。

[0008] 为了完成上述发明目的，本发明采取的整体技术方案为：一种分离式大数据量加

/ 解密设备，包括微处理器、电可擦出只读数据存储器、静态存储器、闪存、乘法协处理器、存储管理保护模块、安全检测与保护模块、非对称算法协处理器、对称算法协处理器、随机数函数发生器、时钟处理模块、电源管理模块、中断控制器、定时器，所述微处理器、可擦出只读数据存储器、静态存储器、闪存、乘法协处理器、存储管理保护模块通过核心数据总线相连，并通过桥连接器与连接有安全检测与保护模块、非对称算法协处理器、对称算法协处理器、随机数函数发生器、时钟处理模块，电源管理模块、中断控制器、定时器的外围总线相连接，该设备还包括：

[0009] 一外部通讯接口模块，外部通讯接口模块连接外围数据总线，用于在加 / 解密设备与外部终端之间采用数据通讯协议命令传递数据，所述数据通讯协议命令包括卡头选择命令字、通讯选择命令字、流控制字、数据长度字、数据域；

[0010] 所述微处理器，用于判断接收到的数据中是否包含加 / 解密命令控制字，不是则用基本处理方式处理数据，是则根据存储器中本地产生的密钥调用对称或非对称算法对所述加 / 解密命令控制字对应通道中的数据进行加 / 解密处理，并存入存储器中。

[0011] 所述微处理器为 32 位的多级流水线精简指令计算处理器，能支持硬件的安全访问控制和外围组件的访问控制。

[0012] 所述外部通讯接口模块至少包括通用串行总线架构接口模块、IS07816 接口模块。

[0013] 一种分离式大数据量加 / 解密实现方法，包括以下步骤：

[0014] 步骤 1、加 / 解密设备通过通用串行总线接口接收终端发送的根据数据通讯协议命令整合后的需要进行加 / 解密处理的数据包，所述数据通讯协议命令包括卡头选择命令字、通讯选择命令字、流控制字、数据长度字、数据域；

[0015] 步骤 2、加 / 解密设备将数据包存储到加 / 解密设备的存储器中；

[0016] 步骤 3、微处理器判断数据包中是否包含加 / 解密命令控制字，不是则用基本处理方式处理数据，是则根据加 / 解密设备存储器中本地产生的密钥调用对称或非对称算法对所述加 / 解密命令控制字对应通道中的数据进行加 / 解密处理，并存入存储器中；

[0017] 步骤 4、加 / 解密设备将经过加 / 解密的数据包以批传送方式通过通用串行总线接口发送给终端。

[0018] 所述步骤 1 中的终端为有线终端、无线终端或手持终端。

[0019] 所述步骤 2 中的数据包为 64 字节。

[0020] 所述步骤 3 中的加 / 解密命令控制字的长度为 2 字节。

[0021] 所述步骤 3 中的加 / 解密命令控制字的低 3 位为进行流信息加 / 解密操作的通道标识。

[0022] 所述步骤 3 还包括对密钥进行加 / 解密的步骤。

[0023] 本发明具有明显的优点和积极效果。本发明采用硬件为加密载体，利用硬件设备上自带的微处理器产生加 / 解密密钥，并在芯片的内部完成对需要加 / 解密计算，有效地提高了大数据量在传输过程中的安全性，同时本发明提供了灵活、快捷的通信方法，大大方便了用户的使用。1、密钥产生与更换的灵活性、随机性。终端可利用加 / 解密设备内随机产生的密钥或将密钥值传送给加 / 解密设备进行加 / 解密运算，此密钥一经产生或写入，就保存在硬件设备加密保护区内，外部无法再次读取。当需要更换密钥时，终端可发送命令由硬件设备内部自行更新密钥或再次将密钥传送设备。同时，在密钥的传递过程中也可采用

加密方法保护密钥值，从而彻底防止了前面提到的内存窃听、通讯层监听等攻击方式。2、高速、强大的数据处理能力。本发明的加/解密设备和终端之间直接采用USB相连接，并且本发明设备可以支持USB全速每秒12兆字节(Mbps)的通讯速率，或USB高速480Mbps的通讯速率。由于加/解密设备内的微处理器是32位或以上，因此本发明的设备具有强大的数据运算和处理能力；同时，设备内制非对称算法协处理器模块，对称算法协处理器模块，在进行数据加/解密运算时，可以提高对数据的处理速度，并且也可以缓解由于对大数据量进行计算而占用的微处理器资源，使微处理器可以进行其他的数据处理，以此提高加速设备的整体运算能力。3、使用方便灵活。采用USB接口与终端相连接，支持即插即用，支持热插拔。用户无须在终端中安装芯片或插入加密卡，即可实现对大数据量的加/解密操作；同时，硬件设备的安装与拆卸非常简单，方便了用户的使用。用户只需要携带加/解密设备在任何一台安装了支持此设备的驱动程序的终端上都可享受其所提供的加/解密服务，如果将本发明的加/解密设备与闪存(FLASH)技术相结合使用自动运行(AUTORUN)功能，则此设备可实现自动安装驱动程序的功能，用户可以加更方便地使用。4、高安全性、可靠性。采用硬件为加密载体，并利用硬件设备上自带的微处理器产生加/解密密钥，并在芯片内部完成对需要加/解密的数据的加/解密计算，有效地提高了大数据量在传输过程中的安全性和可靠性。由于本发明的加/解密设备可实现非对称算法，如1024位公开密钥加密算法(RSA)、2048位RSA算法和纠错码算法(ECC)等，因此，它可以与公钥加密平台PKI(Pubic Key Infrastructure)技术相结合，保存用户的公私钥，存放用户的证书，并且进行签名、验证、加密及解密的计算全部由设备内部完成。这样更提高了系统的安全性，可靠性，实现真正的端对端的安全。5、加密智能设备的经济性。本发明由于采用具有USB接口的32位或以上的微处理器的智能卡芯片，因此大大降低了硬件成本，本发明的设备可以是一张自带USB接口的智能卡、电子钥匙(USBKEY)、USB鼠标、USB键盘、人工智能设备(HID)等USB外设装置。

[0024] 本发明可广泛应用于网络上信息传递和终端硬盘数据的加密存储或移动保护，特别是银行、证券、保险、公安、国防等对数据安全性要求较高的应用系统中。也可应用于下一代网络技术Ipv6中的加/解密保护功能中，成为现有网络I pv4升级到I pv6的IP安全协议(IPSEC)加密智能设备。由于现有网络I pv4协议中考虑是的如何在互连网上实现互通互连，忽略了网络中数据传输的安全问题，所以，人们在规划下一代网络协议I pv6中，将IPSEC引入其中，并成为网际协议(IP)数据包中必须要有的加/解密保护功能。本发明中加/解密智能设备可提供对大数据量的高速对称加/解密、非对称加/解密的特性，将会成为下一代网络中IPSEC加/解密功能的有利补充。

附图说明

[0025] 图1是本发明的加/解密设备的构成模块图；

[0026] 图2是本发明的加解设备与终端之间进行通讯的原理示意图；

[0027] 图3是本发明的加/解密设备通讯协议与其它部分关系示意图；

[0028] 图4是本发明的加/解密设备通信数据处理方法流程；

[0029] 图5是本发明的主流程图；

[0030] 图6是终端利用加/解密设备对大数据量加/解密的流程图；

[0031] 图 7 是基于手机的加 / 解密设备数据加 / 解密过程示意图。

具体实施方式

[0032] 下面结合说明书附图来说明本发明的具体实施方式。

[0033] 如图 1 所示，本发明加 / 解密设备的构成模块图。包括微处理器，闪存 FLASH、电可擦出只读存储器 EEPROM、静态存储器 SRAM 块、乘法协处理器模块、存储管理保护模块、安全检测与保护模块、非对称算法协处理器、对称算法协处理器、随机数函数发生器、时钟处理模块、电源管理模块、中断控制器、定时器，此智能设备中的微处理器、FLASH、EEPROM、SRAM、乘法协处理器、存储管理保护模块与数据总线相连，并通过桥连接器与连接到数据总线的安全检测与保护模块、非对称算法协处理器、对称算法协处理器、随机数函数发生器、时钟处理模块、电源管理模块、中断控制器、定时器相连接，它还包括外部通讯接口模块，通讯接口模块都可分别通过数据总线与微处理器、FLASH、EEPROM、SRAM4、乘法协处理器、存储管理保护模块、安全检测与保护模块、非对称算法协处理器、对称算法协处理器相连，用于在加 / 解密设备与外部终端之间传递数据。外部通讯接口模块包括通用串行总线架构接口模块、ISO7816 接口模块。

[0034] 本发明的加 / 解密设备所采用的芯片是一个基于 32 位或以上的精简指令及计算机 (RISC) 处理器的高安全芯上系统 (SOC) 芯片，具备高处理能力、高安全性、低功耗、低成本等特点。该芯片关键特性 ：

[0035] 一、处理器性能。微处理器为专门定制的高安全 CPU 核，它是 32 位或以上的 RISC，采用 5 级流水线，频率可变，主频可工作在 100MHz 以上，硬件有乘法协处理器 ；微处理器采用整体安全概念，具有优异的安全性能和处理能力 ；它采用高性能的高速缓冲存储器 (CACHE)，包括 1K 字节指令 CACHE 和 1K 字节数据 CACHE ；存储管理和保护单元 (MMU) 可以配置关闭，关闭后支持段管理模式，最大支持空间为 128MB，面向应用的存储分区，支持可变页长，采用多级查找结构，支持虚拟存储空间管理，支持硬件安全访问控制，外围组件访问受控。

[0036] 二、芯上存储单元。本发明的电可擦出只读存储器 (EEROM) 为 32KB，用于数据和程序的存储空间，可进行单字节的读、擦除、写，可进行单字节或多字节最大为 64 字节的擦除、写，最少擦写次数 30 万次，室温下数据保持时间最少 10 年，在擦写性能方面，单字节写时间为 20 微秒 (us)，页擦除时间为 4 毫秒 (ms)，EEPROM 的编程电压在芯片内产生。FLASH 为 128KB，用于存储、函数库以及设备驱动存储空间，128 字节页的擦除、写，最少檫写次数 2 万次，室温下数据保持时间最少 10 年，擦写性能为单字节写时间 20us，页擦除时间 4ms，其静态存储器大小为 8KB。

[0037] 三、外围组件。外围组件包括 ：1、硬件纠错码 (ECC) 协处理器。2、硬件数据加密标准 (DES) 协处理器。硬件数据加密标准 (DES) 协处理器支持 DES、包括 2 KEY 和 3 KEY 的 3DES 算法的加密解密，支持电子密本方式 (EBC) 和链式块处理方式 (CBC) 的加密和解密，优化的数据传送通道，端口数据加 / 解密速度双向达到 3Mbps。3、高速真随机数发生器。其随机数发生码率为 2Mbps，通过国家密码管理委员会办公室测试。4、USB 接口。它支持 USB1.1 协议全速率或更高，支持三端点，每一个端点支持双缓冲器 (Buffer)，端口利用率高，有 1 个串行接口，符合 ISO7816-3 标准，时钟最大支持 5MHz，速率最高支持 310Kbps，1 个 GPIO 接

口，2 个 32 位定时器，内置振荡控制器和相同步逻辑 (PLL)，可外部接 4MHz 晶体，支持上电复位。

[0038] 四、安全特性。具有硬件存储管理和保护、高低电压检测、高低频率检测、防止差分能量分析 / 静态能量分析 (DPA/SPA) 攻击、存储区域加密、总线加扰、时钟和复位信号脉冲过滤、安全优化布线功能，每一个芯片唯一序列号。

[0039] 五、电气特性。整个芯片的功耗小于 200mw(5V 情况下)，3 级低功耗模式控制，即维持模式、休眠模式、掉电模式。电源有 ISO 模式 :2.7-5.5V 和 USB 模式 :3.6V-5.5V。防静电技术指标 (ESD) 保护在 4000V 以上。芯片管脚导线接出 (Bond) 位置符合 ISO7816-2 规范。

[0040] 如图 2 所示，本发明的加解设备与终端之间进行通讯的原理示意图。终端包括有线终端、无线终端，手持终端、手机等，由图可见，加 / 解密设备通过 USB 接口与移动终端进行数据信息的传递。

[0041] 如图 3 所示，本发明的加 / 解密设备通讯协议与其它部分关系示意图。加 / 解密设备采用 USB 接口进行通讯，所以和其它 USB 设备一样，需要有对应的驱动程序支持，以保证设备在终端操作系统上正常运行。由于此设备要对大量信息数据进行处理，因此需要在其自身的驱动程序中增加处理大数据量的功能。本发明在 USB 接口通讯时，使用特殊的数据通讯协议命令包，其格式为“NAD PCBSTR LEN DATA BCC”，其中 NAD 是卡头选择命令字，BCB 是通讯选择命令字，STR 是流控制字，LEN 是数据长度字，DATA 是数据域，BCC 是校验字，对数据进行编码后传递，以保证数据高速、完整的传递，提高大数据量的加 / 解密速度。加 / 解密设备加 / 解密数据流命令包报文编码及功能如表 1 所示 :

[0042] 表 1 加 / 解密数据流命令包报文编码及功能表

[0043]

<table>
<tr><th>代码</th><th>取值</th><th>意义</th></tr>
<tr><td>NAD</td><td>00/12/13H</td><td>卡头选择 NAD=0x00/0x12 主卡头 NAD=0x13 SAM 卡头</td></tr>
<tr><td>PCB</td><td>00H</td><td>与通讯无关，CPU 卡 T=1 时使用，若 CPU 无特别说明，PCB 通常设置为 0x00</td></tr>
<tr><td>STR</td><td>00H
0XH</td><td>当为 00H 时，表示采用智能卡命令格式（APDU）方式处理命令;
当为 0XH 时，表示采用流信息方式处理命令，并指定在对应的通道上进行流加/解密操作。
为了减少加/解密数据流命令长度，在命令字中将低 3 位（b2、b1、b0）表示为进行流加/解密操作的通道标识。
<table>
<tr><th>b7</th><th>b6</th><th>b5</th><th>b4</th><th>b3</th><th>b2</th><th>b1</th><th>b0</th></tr>
<tr><td colspan="4">0</td><td>1</td><td>X</td><td>X</td><td>X</td></tr>
</table>
</td></tr>
<tr><td>LEN</td><td>XXXXH</td><td>指定进行流加/解密操作的数据长度，长度：2 字节</td></tr>
<tr><td>DATA</td><td>数据</td><td></td></tr>
<tr><td>BCC</td><td>XXH</td><td>异或校验字节</td></tr>
</table>

[0044] 加 / 解密设备返回主机数据域中可能回送的状态码如表 2 所示 :

[0045] 表 2 返回主机数据域中可能回送的状态码表

[0046]

SW1 SW2	意义
9000	命令成功执行
6700	错误的长度
6A81	功能不支持
9401	通道标识错误

[0047] 图 4 所示是本发明的加 / 解密设备通信数据处理方法流程图。用户在终端调用加 / 解密设备对应的动态库编写对应的应用程序，动态库除了提供给用户基本的针对智能卡的操作函数功能如设备通讯、控制、操作等外，还提供一个专门的处理大数据量的加 / 解密的功能函数。结合表 1 和表 2 所示，本发明在加 / 解密设备加 / 解密数据流命令包中定义了设备传输所需要的流控制字 (STR)，此控制字的作用是区分用户是在使用基本的智能卡命令操作设备还是在使用流加 / 解密命令对设备进行操作，基本智能卡命令符合 ISO 7816 规范，流加 / 解密命令不符合 ISO 7816 规范。另外，定义 LEN 命令字为两字节，其目的是要增加数据 Data 的字节数量，保证加 / 解密命令可以尽可能多地处理数据。

[0048] 如图 5 所示，图 5 是本发明的主流程图。终端将需要处理的数据通过动态库下传给设备驱动层，驱动层按照通讯协议命令将数据整合后，继续传给终端自带的 USB 底层驱动 (USBD) 和终端中 USB 硬件控制器接口 (UHCI/E) 层，UHCI/E 为标准的 USB 设备。在此，数据被分别拆分为多个 64 字节的数据包，并分别按照数据包的先后顺序发送给加 / 解密设备。加 / 解密设备采用中断方式接收终端下发的数据包。当设备端的 USB 硬件接口 USB IF 接收到第一个数据包时，程序开始处理判断此数据包中是否包含加 / 解密命令控制字。如果包含，则进行大数据量信息的处理 ；否则就使用现有基本处理方式处理数据。在大数据量信息处理中，程序通过加 / 解密设备中的固件 (Firmware) 调用智能卡操作系统 (COS) 中的对称或非对称算法加 / 解密函数对数据信息进行处理。同时，采用中断方式不断接受终端的数据，以节省传输数据所用的时间，提高流处理速度。最后，将加 / 解密智能终端处理完成的数据批量上传给终端。

[0049] USB 有四种传输类型。1、控制传送。控制传送是双向传送，数据量通常比较小。USB 系统程序用来主要进行查询、配置和给 USB 设备发送通用的指令。该传送方式可以包括 8、16、32 以及 64 字节的数据，这依赖于 USB 设备和传输速率。控制传输典型地用于主计算机和 USB 外设之间的端点 (Endpoint)0 之间的传输。2、同步传送。同步传输提供了确定的带宽和间隔时间 (Latency)。它被用于时间严格并具有较强容错性的流数据传输，或者用于要求恒定的数据传送率的即时应用中。例如在执行即时通话的网络电话应用时，使用同步传输模式是较好的选择。同步数据要求确定的带宽值和确定的最大传送次数。对于同步传送来说，即时的数据传递比准确的数据精度和数据的完整性更重要一些。

[0050] 3、中断传送 (Interrupt) 方式传送。中断方式传输主要用于定时查询设备是否有中断数据要传送。设备的端点模式器的结构决定了它的查询频率，在 1ms-255ms 之间。这种传输方式典型地应用在少量的、分散的、不可预测数据的传输。键盘、操纵杆和鼠标就属于这一类型。中断方式传送是单向的并且对于主计算机 (Host) 来说只有输入的方式。在本实施例中，可以一次传送 2-6K 字节数据。4、批传送。该方式主要应用在数据大量传送和接收数据上，同时又没有带宽和间隔时间要求的情况下，要求保证传输。打印机和扫描仪属于这种类型。这种类型的设备适合于传输非常慢和大量被延迟的传输，可以等到所有其他类型的数据的传送完成之后再传送和接收数据。

[0051] 本发明选用USB传输类型中的中断传送和批传送相结合的方式，即中断方式接受数据，批传送方式输出数据。这种通信方式提高了加/解密设备的大数据量加/解密处理速度。

[0052] 请参阅如图6、图7，图6是终端利用加/解密设备对大数据量加/解密的流程图，图7是基于手机的加/解密设备数据加/解密过程示意图。在图7中，主计算机接收手机通过全球通(GSM)网络发送的数据包并保存在缓存(RAM)区，等待处理，手机终端准备流数据；手机终端获得设备的控制权(Handle)，通过密钥认证取得设备的控制权；判断是否获得设备的控制权？没有则向应用程序报告，是则发送加/解密数据流命令；进一步判断是否接到数据返回9000，否则向应用程序报告，是则关闭加/解密数据流命令并向应用程序报告。随着无线技术，电信技术的发展，手机的功能也是越来越强。加/解密设备本身也可以以短信中心(SIM)卡的形态提供给用户在手机中使用。利用此加密智能设备的强大数据处理能力，手机上的语音信息，短信信息都可以采用加密方式在无线网络中传输，这样可以保护用户的个人信息无法被攻击者窃取。

[0053] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。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权利要求范围之内。

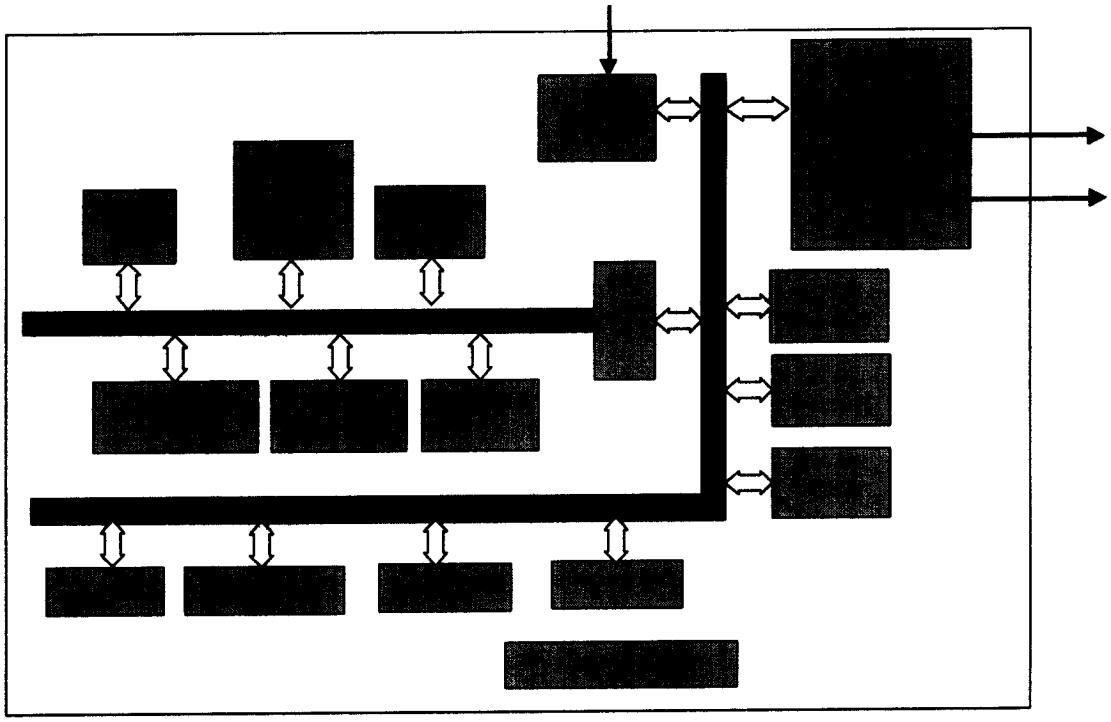


图 1

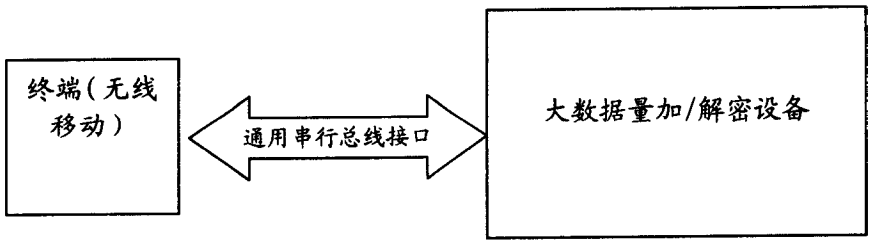

终端(无线移动)
通用串行总线接口
大数据量加/解密设备

图 2

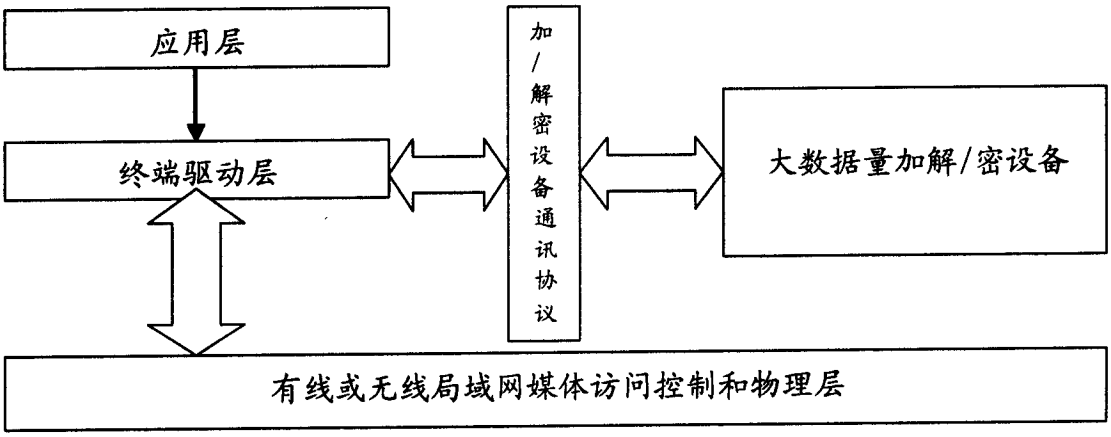

应用层
终端驱动层
加/解密设备通讯协议
大数据量加解/密设备
有线或无线局域网媒体访问控制和物理层

图 3

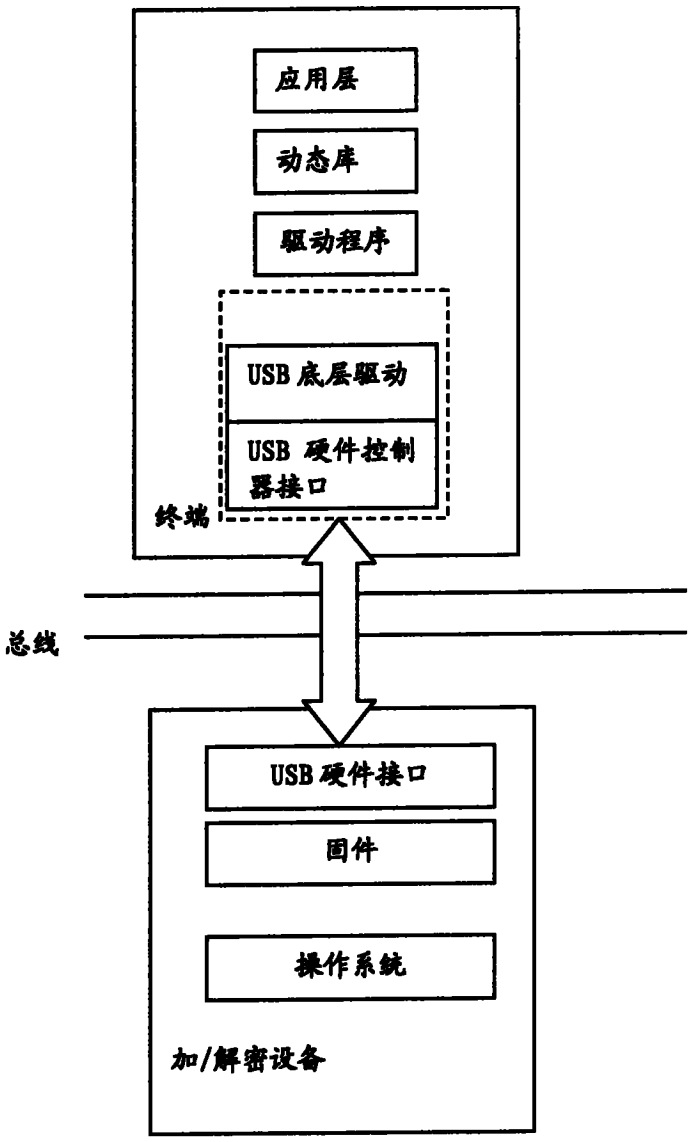


图 4

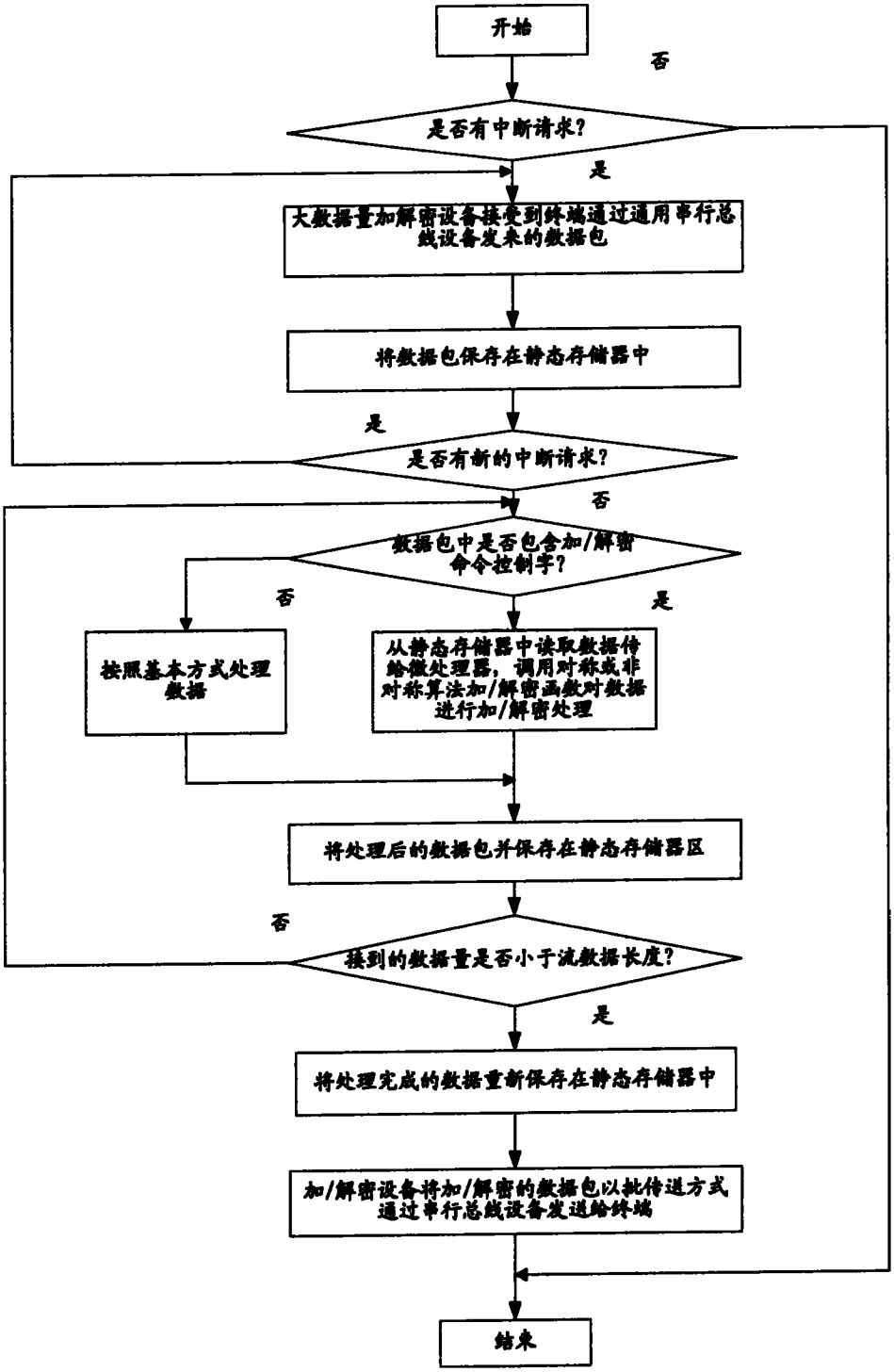

开始
否
是否有中断请求?
是
大数据量加解密设备接受到终端通过通用串行总线设备发来的数据包
将数据包保存在静态存储器中
是
是否有新的中断请求?
否
数据包中是否包含加/解密命令控制字?
否
是
按照基本方式处理数据
从静态存储器中读取数据传给微处理器，调用对称或非对称算法加/解密函数对数据进行加/解密处理
将处理后的数据包并保存在静态存储器区
否
接到的数据量是否小于流数据长度?
是
将处理完成的数据重新保存在静态存储器中
加/解密设备将加/解密的数据包以批传送方式通过串行总线设备发送给终端
结束

图 5

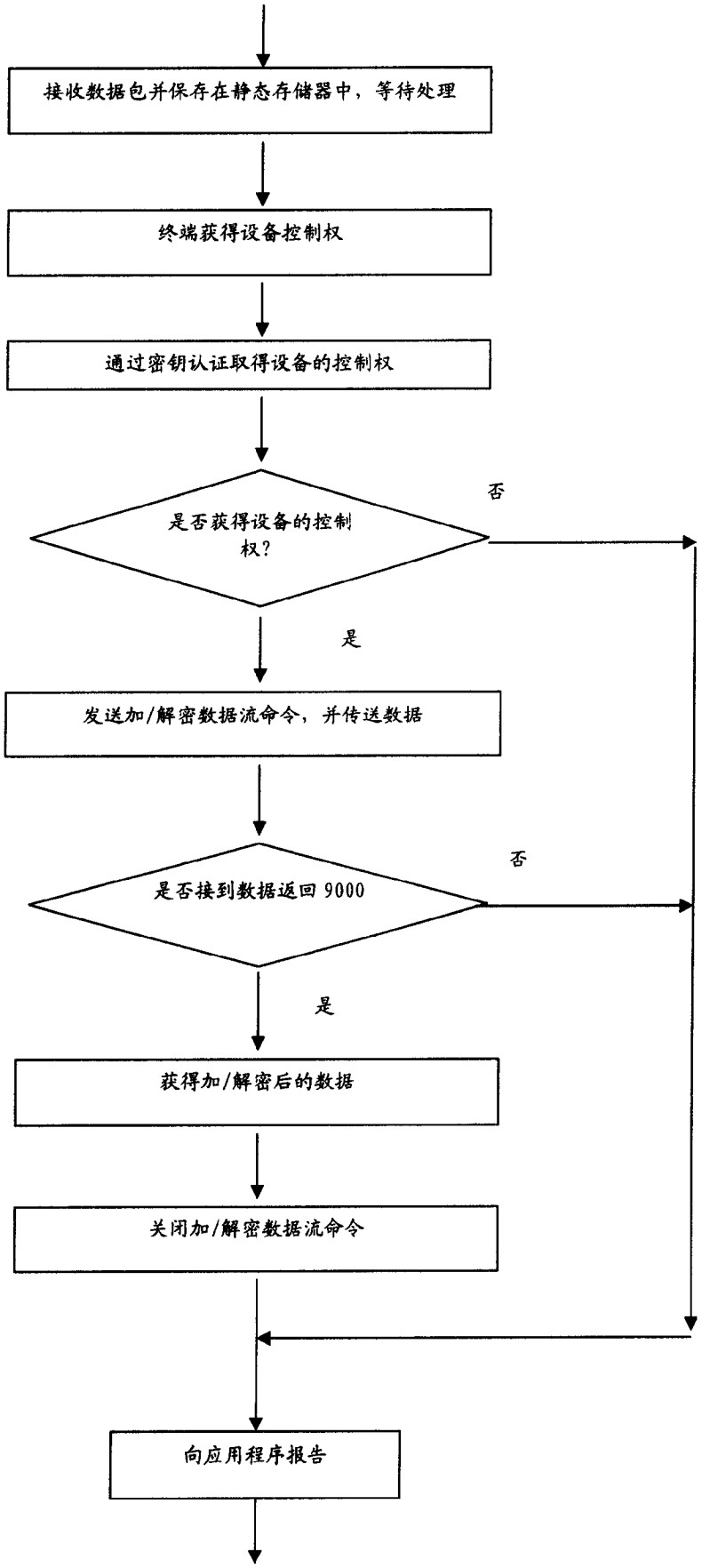

接收数据包并保存在静态存储器中，等待处理
终端获得设备控制权
通过密钥认证取得设备的控制权
是否获得设备的控制权?
否
是
发送加/解密数据流命令，并传送数据
是否接到数据返回 9000
否
是
获得加/解密后的数据
关闭加/解密数据流命令
向应用程序报告

图 6

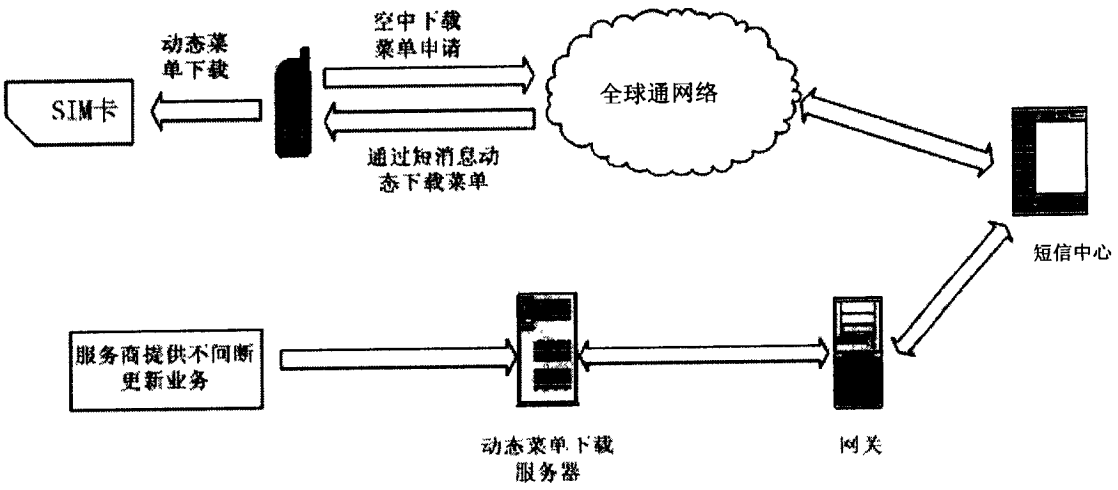

动态菜单下载
空中下载菜单申请
SIM卡
全球通网络
通过短消息动态下载菜单
短信中心
服务商提供不间断更新业务
动态菜单下载服务器
网关

图 7