

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06K 19/077 (2006.01)



[12] 发明专利说明书

专利号 ZL 200610170452.X

[45] 授权公告日 2009年5月13日

[11] 授权公告号 CN 100487728C

[22] 申请日 2006.12.30

[21] 申请号 200610170452.X

[73] 专利权人 凤凰微电子(中国)有限公司
地址 100084 北京市海淀区中关村东路清
华科技园科技大厦 A 座 18 层

[72] 发明人 杨延辉 卜冀春 黄正全

[56] 参考文献

JP8-315100A 1996.11.29

CN1449542A 2003.10.15

CN201041677Y 2008.3.26

CN1696972A 2005.11.16

US2006/0186211A1 2006.8.24

WO2006/111781A1 2006.10.26

US2003/0102380A1 2003.6.5

CN1795457A 2006.6.28

审查员 马红梅

[74] 专利代理机构 北京英赛嘉华知识产权代理有
限责任公司

代理人 田明 王达佐

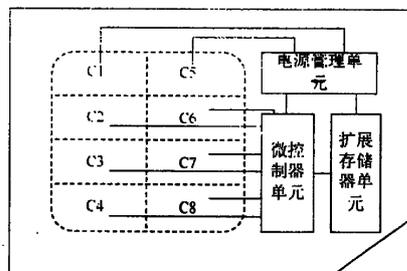
权利要求书 3 页 说明书 26 页 附图 6 页

[54] 发明名称

支持快速计算、大容量存储、高速传输的新型智能卡

[57] 摘要

本发明属于智能卡/集成电路芯片设计 and 应用领域, 尤其涉及高计算性能、超大存储容量、高速传输接口的智能卡设计 and 应用。该智能卡包括微控制器单元、电源管理单元和扩展存储器单元三部分, 根据 ISO/IEC 7816-3 协议定义的管脚编号, 电源管理单元连接 C1、C5 管脚, 微控制器单元连接其余 6 条管脚, 扩展存储器单元分别连接电源管理单元和微控制器单元。本发明可大大扩展和增强智能卡的存储和处理能力, 如进行海量数据的存储和管理, 高速率数据的传输, 还可以集成多种数据传输接口, 作为独立的存储设备使用。该智能卡可通过转换插座与多种数码设备相适配, 并具备强大的网络数据下载存储能力、多媒体数据编码处理能力和安全计算能力。



1. 一种支持快速计算、大容量存储、高速传输的新型智能卡，由卡基和装配在卡基上的芯片模块组成，其特征在于：该智能卡的芯片包括微控制器单元、电源管理单元和扩展存储器单元三部分，根据 ISO/IEC 7816-3 协议定义的管脚编号，电源管理单元连接 C1、C5 管脚，微控制器单元连接其余 6 条管脚，扩展存储器单元分别连接电源管理单元和微控制器单元。

2. 根据权利要求 1 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：微控制器单元、电源管理单元和扩展存储器单元或者采用单一的系统芯片来实现，或者采用多个芯片集成的方式实现。

3. 根据权利要求 1 或 2 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：微控制器单元采用双总线结构实现数据传输，一条总线用于处理高速数据传输，一条总线用于处理低速数据传输，两条总线之间采用总线桥接器或数据邮箱装置连接，进行不同速率的数据交换。

4. 根据权利要求 1 或 2 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：微控制器单元的微处理器采用 16/32/64 位或更高位的嵌入式微处理器。

5. 根据权利要求 3 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：微控制器单元还设有协处理器，微处理器与协处理器之间采用片上总线方式或 DMA 方式进行连接。

6. 根据权利要求 3 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：在微控制器单元内设有一些存储器，包括用于存储用户软件的程序存储器、用于存储智能卡基本应用数据的数据存储器、用于存储临时存放数据的随机缓存，存储器通过地址/数据总线直接连接在微处理器上，或者通过片上总线间接与微处理器连接。

7. 根据权利要求 6 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：所述的程序存储器、数据存储器采用非挥发性存储器。

8. 根据权利要求 6 所述的支持快速计算、大容量存储、高速传输的

新型智能卡，其特征在于：微控制器单元内还设有用于实现各种类型存储介质的控制接口的存储控制器和用于保障卡内数据的安全性和完整性的内存保护单元。

9. 根据权利要求 3 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：该智能卡的低速片上总线连接 ISO/IEC 7816 接口，高速片上总线通过管脚信号复用连接高速传输接口。

10. 根据权利要求 9 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：高速传输接口包括 USB、SD、MMC 接口。

11. 根据权利要求 3 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：微控制器单元内还设有高速接口控制器来实现与外部设备的高速数据传输。

12. 根据权利要求 11 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：高速接口控制器控制高速传输接口 USB、SD、MMC 的开启和关闭，三种高速传输接口中同一时间只有一种接口处于工作状态。

13. 根据权利要求 11 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：微控制器单元内还设有直接与片上总线连接的 DMA 控制器，高速接口控制器通过高速片上总线与 DMA 控制器相连。

14. 根据权利要求 11 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：高速接口控制器通过高速片上总线与微处理器相连。

15. 根据权利要求 3 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：微控制器单元内还设有用于管理外部中断请求的中断控制器，中断控制器通过片上总线与微处理器相连。

16. 根据权利要求 3 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：微控制器单元内还设有时钟/复位管理单元。

17. 根据权利要求 16 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：时钟/复位管理单元包括分别与片上总线连接的时钟分频及门控制电路、复位信号产生模块和数字锁相环、晶振器及其控制器。

18. 根据权利要求 1 或 2 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：电源管理单元的输入端通过智能卡的电源触点与片外电源连接，输出端与智能卡内部各个芯片及分离元器件的电源引脚连接。

19. 根据权利要求 17 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：电源管理单元为线性稳压器 LDO、DC-DC 转换器或升压电荷泵当中的一种。

20. 根据权利要求 1 或 2 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：扩展存储器单元是采用闪存来扩展存储空间，使用 NOR Flash 闪存来存储和执行代码，使用 NAND Flash 闪存来存储数据。

21. 根据权利要求 20 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：微控制器单元内设有闪存控制器，闪存控制器与微控制器单元中的闪存相连，并且与扩展的闪存存储单元连接。

22. 根据权利要求 1 或 2 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：扩展存储器单元还能够采用 FeRAM 或分子存储器来扩展存储空间。

23. 根据权利要求 1 或 2 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：微控制器单元、电源管理单元和扩展存储器单元被封装在经过宽度延展的金属条带内。

24. 根据权利要求 1 或 2 所述的支持快速计算、大容量存储、高速传输的新型智能卡，其特征在于：该智能卡的软件体系包括硬件驱动、实时操作系统、应用编程接口以及具体的应用/业务；

所述的硬件驱动主要是支持操作系统，提供各类设备或接口的驱动程序，完成硬件初始化，以及时钟/电源管理；

所述的实时操作系统控制着应用编程接口与硬件平台的相互通信，负责管理系统资源，提供高效的实时多任务调度；

所述的应用编程接口为各种应用程序提供一个开放的、统一、标准的应用程序接口，支持上层应用程序的开发，应用程序通过应用编程接口调用各种低层系统资源。

支持快速计算、大容量存储、高速传输的新型智能卡

技术领域

本发明属于智能卡/集成电路芯片设计 and 应用领域,尤其涉及高计算性能、超大存储容量、高速传输接口的智能卡设计 and 应用。

背景技术

智能卡又叫 IC 卡,是一种将具有存储、加密及数据处理能力的集成电路芯片镶嵌于塑料基片中的卡片。智能卡根据嵌装的芯片来划分,可分成存储器卡和微处理器卡两大类。存储器卡采用存储器芯片作为卡芯,只有“硬件”组成,包括数据存储器和安全逻辑控制等;微处理器卡采用微处理器芯片作为卡芯,由硬件和软件共同组成。硬件部分通常包括用于计算和控制的硬件微处理器、用于存储运行时或工作数据的随机存取存储器(SRAM/DRAM/SDRAM)、用于存储程序代码的只读存储器(通常用 ROM 实现,最新进展是采用非挥发性可改写存储器,如 EEPROM/FLASH 来实现),用于存储用户数据的非挥发性可改写存储器(EEPROM/FLASH)。软件部分包括监控程序或 COS(Card Operating System, 卡片操作系统)以及各类应用程序等。本发明中的智能卡就是指微处理器卡。

智能卡的基本特性和功能在 ISO/IEC 7816 系列标准中有所规定。智能卡集成电路的典型结构如图 1 所示,除了作为芯片核心的微处理器外,通常还包括四个附加功能模块:存储运行时工作数据的随机存取存储器(SRAM/DRAM/SDRAM)、用于存储程序代码的存储器(ROM/EEPROM/FLASH)、用于存储用户数据的非挥发性可改写存储器(EEPROM/FLASH)和串行通信单元(I/O 接口)。通过逻辑电路将上述五部分模块连接起来并集成在一块集成电路中,电路和数据的安全性通过半导体工艺及软件有效地进行保障。

IC 卡具有突出的 3S 特点,即 Standard(国际标准化)、Smart(灵巧智能化)和 Security(安全性),具有存储量大、可靠性强、安全性高等

优点。目前，智能卡已广泛用于电信、金融、政府、交通、医疗、公共管理、互联网等领域。

以智能卡在移动通信领域内的应用为例，SIM (Subscriber Identity Module, 用户识别模块) 卡装载在手机终端中，完成了 GSM 网络上的用户身份识别和鉴权、语音通信支撑、短消息业务以及其它各类基于 STK 的增值业务。SIM 卡技术在 GSM 网络中获得成功后，目前已大量应用在各类移动通信网络中，如 CDMA 网络中使用了 UIM 卡、PHS 网络中使用了 PIM 卡、3G 网络中使用了 USIM 卡等。本发明所描述的新型智能卡技术可以使用在上述的各个行业和应用中。

长期以来，智能卡集成电路和软件技术一直沿用了其诞生以来的基本设计理念和内部架构。一方面，智能卡技术获得了巨大的商业成功；另一方面，智能卡技术也受到越来越多其它新技术的挑战，如果不能在技术平台上尽快地实施升级，智能卡也面临着被淘汰的危险。传统 SIM 卡的容量在 16K 至 128K 字节之间，并采用 8 位 CPU。由于存储容量有限，8 位微处理器的处理能力也很低，传统 SIM 卡能开展的业务极其有限；而运营商已经从价格战转入应用和服务的竞争，推出的业务越来越复杂，大量的新型移动增值业务，如手机电视、移动电子商务、多媒体应用，都需要进行大量的数学计算和数据吞吐；当今社会对信息安全也提出了更高的要求，相应的密码算法也越来越复杂，如数字签名、数字证书、DRM (Digital Rights Management, 数字版权管理) 也需要进行大量的计算和高速的处理。由于传统智能卡只集成了 ISO/IEC 7816 接口通讯协议，该协议只能在特定的智能卡终端设备上读取智能卡内容，由于接口的不通用导致无法与使用标准接口的计算机设备、电信设备等直接相连。这种局限性限制了智能卡在相关领域的应用和发展。运营商渴望能够推出高附加值或杀手级的应用，有效提升其业务收入，这就需要作为连接运营商与用户之间唯一桥梁的 SIM 卡具有超过兆字节的存储量和高性能的微处理器，显然，传统的 SIM 卡是无法满足这些要求的，无法帮助运营商在新业务推广上取得大的突破。

随着移动通信技术的迅速发展和普及应用，对智能卡的功能要求越来越高；例如，在 SIM 卡上实现 RFID 功能、实现双用户识别模块/多用户识别模块集成功能(多电信运营商)、集成应用处理器或其它对外控制的功能

(MP3, MPEG4, LCD 控制) 等等; 即使这些新型智能卡具备了高速数据传输, 海量数据处理的特点, 但是由于仍采用传统的物理接口形式 (ISO7816 标准, 8 个 Pad), 其功能的扩展和能力的发挥受到极大的限制。

另外, 新的应用要求智能卡能够承受外部供给的 2.7V 到 5.5V 电源。并在卡内部同时提供 1.8V、3V 和 5V 等多路工作电压; 并且这种对电源的管理是不依赖于外部终端设备, 而是在智能卡内部实现的。但是, 想要在智能卡内的逻辑芯片上实现电源管理是非常困难的, 必须寻求新的解决方案, 实现智能卡内部的电源管理。

运营商为了增强自己在产业链上的绝对优势地位, 不断发展自己的增值业务, 并设法通过各种手段尝试对手机厂家和业务进行控制, 但由于手机厂家众多和手机特有的销售模式使得运营商无法很好地在手机平台上建立和统一其业务, 所以这种尝试收效甚微。而 SIM 卡作为运营商唯一完全可控的环节, 如能具备超大容量和超强计算能力, 并能够支撑运营商的业务发展, 无疑将成为运营商推广自己业务和获得产业控制权、防止终端和业务失控的一个重要手段。

发明内容

本发明的目的旨在解决上述传统智能卡在产业发展和技术演进中遇到的问题, 提供一种具有能够支持复杂运算业务的高性能处理平台的新型智能卡。该新型智能卡可进行海量数据的存储和管理, 高速率数据的传输, 并可以集成多种数据传输接口, 作为独立的存储设备使用。该智能卡可通过转换插座与多种数码设备相适配, 并具有强大的网络下载能力、多媒体数据编码处理能力和安全计算能力。

由上述目的可以看出, 本发明的新型智能卡是对传统智能卡的一次革命性的突破, 在功能和性能上都有一个质的提升。为此, 在分析传统智能卡局限性的基础上, 下面提出本发明新型智能卡需要解决的一些关键技术问题:

首先, 目前市场上多数智能卡的 CPU 为 8 位或 16 位处理器, 如 Intel 8051、Motorola 6502 等, 典型的时钟工作频率为 3.57MHz (时钟范围介于

1MHz~10MHz), CPU运行速度一般为0.5MIPS (Million Instruction Per Second, 每秒百万条指令)左右, 进行一般文字类的应用处理尚可支持, 对于需要大量计算的图像处理、图像计算、密码计算等则无法很好地支持。如常用的RSA签名算法, 通常会要求最低位数为1024位, 有些场合则要求达到2048位; 即使采用计算量相对较小的ECC算法, 其最低位数也要求是160位, 甚至192、256位; 在多媒体数据处理领域, 为了提高精度和速度, 通常也需要采用32位以上数据带宽的处理器, 由此可见, 传统智能卡的计算能力已经不能满足应用的发展需求了。所以, 高性能的计算是新型智能卡要解决的首要问题。

其次, 随着社会信息化程度的提升, 信息产生的速度和数量都迅速地加快, 相应地, 对智能卡的存储能力提出了新的需求。目前市场上普遍使用的SIM卡容量多数为16KB/32KB/64KB, 最大不超过128KB。64KB的存储容量相当于250个电话联系人条目、30条短消息和3到5个下载铃声, 由此可见, 智能卡目前的存储能力无法支持电信运营业务发展和最终客户的应用需求; 运营商和最终客户希望在手机终端中除了可以存储通讯录、短信、手机号码等信息外, 还可以存储网页、文档、电影、歌曲和游戏等海量数据。目前一种过渡的做法是采用SIM卡以外的扩展卡来增加容量, 这不但给手机终端开发和使用带来了诸多的不便和开销, 同时因为扩展卡在销售和使用上采用与SIM卡完全不同的商业模式, 运营商无法有效利用和控制扩展卡资源, 也就无法有效地利用扩展卡支撑其增值业务的发展。通过扩展SIM卡的存储容量, 使SIM卡集成更大的存储器可达到兆字节, 甚至G字节, 不但解决了手机设计的复杂度、降低了终端的成本、满足了最终客户对存储的要求, 更可以对运营商的增值业务提供有效支撑。所以, 超大容量存储是新型智能卡要解决的第二个关键技术问题。

第三, 由于网络的普及, 手机终端内大量的数据需要通过网络进行传输和交换, 海量储存也相应地提高了对数据传输速率的要求。ISO/IEC 7816接口的传输速率通常在几kbps (kilobits per second, 千位/秒)到几百kbps之间, 实际上最常用的速率一般不超过115.2kbps。以该速率传输一首大小在4.5M左右的MP3歌曲需要三百多秒, 如果考虑到传输的开销和容错等因素, 时间还会加长。另一方面, 由于手机终端已不再是一个纯粹的

话音通讯设备，其上集成了大量的附加业务，SIM卡应具备不但可以支持话音业务，还可以同时支持其它应用的能力，需要在ISO/IEC7816接口之外扩展新的接口。再者，由于集成电路和软件的复杂度巨大提高，芯片上集成了大量的附属设备。这些附属设备也需要保持与芯片外持续的通信，这就要求传输接口的协议处理应具备更强的扩展能力。另外，一些复杂应用，如多媒体码流的传输、对外的网络连接都需要高速接口支持，除了需要支持诸如流传输等协议外，还要考虑最简单和适用的方案与手机终端的基带处理器和个人电脑方便连接。上述需求通过采用当今流行的几种数据传输总线协议，如USB、SD、MMC，传输速率可达到Mbps (Megabits per second, 兆位/秒)数量级，并且具备了更强的协议扩展能力。所以，高速传输是新型智能卡要解决的第三个关键技术问题。

第四，通过上述分析可看到这种支持高性能计算、超大容量存储、高速传输的新型智能卡已经大大超越了传统的智能卡技术。由于要实现诸多复杂功能，相应的内部硬件和软件资源需求迅速提升，如更大容量的SRAM、更高速的定时器、高效率的DMA (Direct Memory Access, 直接存储器访问)等，这就要求在集成电路设计上采用新型架构以提高内部数据交换和管理能力。采用SoC器件设计方法、合适的架构、高性能的片上总线(On-Chip Bus, OCB)来管理和连接内部不同的模块资源是新型智能卡要解决的第四个关键技术问题。

第五，诸多复杂的功能可能无法由一颗芯片来全部完成，新型智能卡设计要面临将多颗芯片，甚至分立元器件集成在一个卡片内的技术难题。通过特殊的智能卡金属条带设计可以在水平面上延展可封装器件的面积，通过特殊的封装工艺可实现在卡内进行上百条金属线的连接，从而实现多芯片封装的目的。多芯片封装是新型智能卡要解决的又一个关键技术问题。

第六，为了兼容传统智能卡的外封装以及大量终端上集成的智能卡座，新型智能卡仍然采用八条管脚的外连接形式。所以，要利用这八条管脚完成诸多功能和传输接口，巧妙地设计管脚复用的方法是新型智能卡要解决的又一个关键技术问题。

第七，本发明在芯片上集成了ISO/IEC 7816、USB、SD、MMC等众多接口，通过管脚复用方式连接到芯片外部，芯片需要在协议规定的时间内判

断数据类型、自动扫描和识别接口种类、开启硬件接口保护装置，然后及时做出应答和实现对高速设备即插即用的管理，所以，如何有效扫描管脚复用信号和自动识别接口协议是新型智能卡需要解决又一个关键技术问题。

第八，本发明的新型智能卡具有 ISO/IEC 7816、USB、SD、MMC 多个不同的外时钟源，而集成电路内部高速运行又需要一个稳定的、不依赖于外部的、频率高的时钟，所以需要设计一套高效的、稳定的、无毛刺的时钟管理单元。同时由于移动设备节省能源的要求，需要通过可控制的时钟网络来降低芯片的功耗。所以，高效节能的时钟管理是新型智能卡需要解决的又一个关键技术问题。

第九，本发明所需要的工作电压由外部提供，如手机终端或其它终端设备，输入的工作电压根据不同的终端将会有很大的变化，可能的工作电压范围为 1.8V~3.0V~5.0V。同时，芯片内部逻辑正常工作所需要的电压与半导体工艺相关，变化也比较大，需要在卡片内放置特殊的电压转换模块以提供芯片内所需的各种工作电压。所以，支持宽电压工作范围和多路/多种电压输出的高效、稳定的电源管理是新型智能卡需要解决的又一个关键技术问题。

第十，本发明采用 Flash 器件来提供超大容量的存储空间。Flash 接口种类很多，仅成熟的工业标准接口就有几十种，目前主要有 NOR Flash 和 NAND Flash 两种规格，主流工艺为 65nm-130nm。所以，设计和实现高效、灵活并具有广泛兼容性的 Flash 接口控制器是新型智能卡需要解决的又一个关键技术问题。

第十一，在本发明的智能卡内具有多个存储器区域，分别可以存放代码、指令和用户数据，所以，如何有效地保护卡内数据的安全性和完整性，即内存保护机制，是新型智能卡需要解决的又一个关键技术问题。

第十二，本发明使用非挥发性存储器来存储操作系统和应用程序，在保证数据安全的前提下需要提供一套带有高强度认证功能的程序下载电路。

第十三，目前多数智能卡采用专用的 COS，只能面向一个或少数几个固定的应用，其主要问题为：传统 SIM 卡所使用的 STK 应用开发接口主要

用于处理文本类的菜单业务，无法实现诸如图形、多媒体、网络等复杂应用，用户体验差；其次，传统智能卡的软件系统还不具备真正的操作系统功能，在结构上无法支持由应用开发商甚至最终客户灵活地更改和增删应用。通过引入实时操作系统可以支持更丰富的通讯协议、支持多任务的操作、支持图形化及窗口应用、支持应用的动态更改和增删，大大提升了新型智能卡业务承载能力。所以，在芯片上设计和实现高效的操作系统是新型智能卡支持新型应用开发和运营部署需要解决的又一个关键技术问题。

第十四，为了与目前主流的个人电脑、数码相机、MP3/MP4 播放机等数码设备共享和交换数据，需要建立通用的、兼容性强的、成熟和稳定的文件系统，如 Microsoft Windows、Linux 采用的文件系统。所以，设计和实现一个功能完整的、通用的、兼容性强的文件系统是新型智能卡要解决的又一个关键技术问题。

本发明的技术方案如下：一种支持快速计算、大容量存储、高速传输的新型智能卡，由卡基和装配在卡基上的芯片模块组成，该智能卡的芯片包括微控制器单元、电源管理单元和扩展存储器单元三部分，根据 ISO/IEC 7816-3 协议定义的管脚编号，电源管理单元连接 C1、C5 管脚，微控制器单元连接其余 6 条管脚，扩展存储器单元分别连接电源管理单元和微控制器单元。

上述的微控制器单元、电源管理单元和扩展存储器单元采用单一的系统芯片来实现，或者采用多个芯片集成的方式实现，三个单元被封装在经过宽度延展的金属条带内，微控制器单元的微处理器采用 16/32/64 位或更高位的嵌入式微处理器。

进一步，如上所述的支持快速计算、大容量存储、高速传输的新型智能卡，该智能卡采用双总线结构实现数据传输，一条总线用于处理高速数据传输，一条总线用于处理低速数据传输，两条总线之间采用总线桥接器或数据邮箱装置连接，进行不同速率的数据交换。

进一步，在上述支持快速计算、大容量存储、高速传输的新型智能卡

中，微控制器单元还设有协处理器，微处理器与协处理器之间采用总线方式或 DMA 方式进行连接。

另外，在微控制器单元内围绕微处理器周边设有一些存储器，包括用于存储用户软件的程序存储器、用于存储智能卡基本应用数据的数据存储器、用于存储临时存放数据的随机缓存。所述存储器可通过地址/数据总线直接连接在微处理器上，也可通过片上总线间接与微处理器连接。所述存储器采用非挥发性存储器。

在上述微控制器单元内还设有用于实现各种类型存储介质的控制接口的存储控制器和用于保障卡内数据的安全性和完整性的内存保护单元。

进一步，如上所述的支持快速计算、大容量存储、高速传输的新型智能卡，该智能卡的低速片上总线连接 ISO/IEC 7816 接口，高速片上总线通过管脚信号复用连接多种高速传输接口，高速传输接口包括 USB、SD、MMC 接口。

该智能卡内还设有直接与片上总线连接的 DMA 控制器。在智能卡内设有高速接口控制器来实现与外部设备的高速数据传输，高速接口控制器通过高速片上总线与微处理器或 DMA 控制器相连。

上述高速接口控制器控制高速传输接口 USB、SD、MMC 的开启和关闭，三种高速传输接口中同一时间只能有一种接口处于工作状态。

另外，该智能卡内还设有用于管理外部中断请求的中断控制器，中断控制器通过片上总线与微处理器相连。智能卡内还设有时钟/复位管理单元，时钟/复位管理单元包括分别与片上总线连接的时钟分频及门控制电路、复位信号产生模块和数字锁相环、晶振器及其控制器。

进一步，如上所述的支持快速计算、大容量存储、高速传输的新型智能卡，其中，电源管理单元的输入端通过智能卡的电源触点与片外电源连接，输出端与智能卡内部各个芯片及分离元器件的电源引脚连接。

另外，该智能卡的扩展存储器单元是采用闪存来扩展存储空间，使用 NOR Flash 闪存来存储和执行代码，使用 NAND Flash 闪存来存储数据，微控制器单元内设有闪存控制器，闪存控制器与微控制器单元中的闪存相连，

并且与扩展的闪存存储单元连接。或者，扩展存储器单元采用 FeRAM 或分子存储器来扩展存储空间。

进一步，如上所述的支持快速计算、大容量存储、高速传输的新型智能卡，该智能卡的软件体系包括硬件驱动、实时操作系统、应用编程接口以及具体的应用/业务。其中，硬件驱动主要是支持操作系统，提供各类设备或接口的驱动程序，完成硬件初始化，以及时钟/电源管理；实时操作系统控制着应用编程接口与硬件平台的相互通信，负责管理系统资源，提供高效的实时多任务调度；应用编程接口为各种应用程序提供一个开放的、统一、标准的应用程序接口，支持上层应用程序的开发，应用程序通过应用编程接口调用各种低层系统资源。

通过本发明的智能卡，可以得到如下明显的效益：

利用其高性能计算的能力，可以直接应用到复杂计算行业，如安全认证、多媒体、移动视频等，不仅能大幅度提高数据的安全性，而且也能极大地扩展其使用范围。

利用其高速接口，可以快速地交换数据，缩短通讯和操作时间，提高工作效率。

利用其通用的标准接口，不需要专用的智能卡终端设备即可使用，大大方便了智能卡的使用。

利用其大容量存储功能，可以当作移动存储器使用，替代其它种类的移动存储器，既方便了使用，又节约了成本。

利用其层次化、结构化的软件体系结构和统一的编程接口，可以灵活、高效、快速地开发和部署新应用、新业务。

利用其智能卡+存储卡多合一的功能，可以有效解决移动通信终端面临的功能和体积冲突的问题。

附图说明

图 1 为传统智能卡的典型结构示意图。

图 2 为传统智能卡的触点编号、定义示意图。

图 3 为本发明将芯片条带进行延展的示意图。

图 4 为本发明将芯片条带经过延展后的内部封装示意图。

图 5 为本发明的内部结构与外部触点的电学连接示意图。

图 6 为本发明的软件结构示意图。

图 7 为本发明实施例的微控制器单元的总体结构组成示意图。

图 8 为本发明实施例的时钟和复位管理单元的结构图。

图 9 为本发明实施例的电源管理单元结构示意图。

图 10 为本发明实施例的新型智能卡的软件详细结构示意图。

图 11 为对多种高速数据接口的输入/输出进行集中统一控制的电路结构示意图。

图 12 为各高速通信模块自行控制高速数据接口输入/输出的电路结构示意图。

具体实施方式

下面结合说明书附图和具体实施方式对本发明作进一步描述。

本发明包括一套强大、完整的硬件平台和高效、灵活的软件体系。硬件平台实现基本的通信与计算功能，在此基础上，软件体系实现和完成复杂的业务/应用。

本发明的硬件平台包括微控制器单元、电源管理单元和扩展存储器单元三部分。这几部分功能和结构可以根据需要进行灵活组合。既可以采用单芯片封装方式，只将微控制器单元或者全部三部分单元封装成一颗独立的 SoC (System on Chip, 系统芯片) 芯片进行使用；也可以采用多芯片方式，将所有的三部分分别进行封装，每部分封装成一颗芯片，然后将多颗芯片，以及相应的分立元器件集成在一个卡片内。

无论采用何种封装实现方式，智能卡内部所有芯片和器件都必须完全封装在其外部金属条带所覆盖的范围里面，并与外部条带的 8 个触点电气连接。传统智能卡芯片的条带形状和触点名称如图 2 所示。由于本发明的新型智能卡功能众多、性能强大，连接关系复杂，所以导致芯片面积急剧膨胀，如果采用多芯片集成方案，卡片内将集成众多的器件，上述原因直接导致芯片封装面积过大，很难在传统智能卡的条带面积范围内（如图 2

中的虚线所示)进行封装。本发明的新型智能卡采用特殊的金属条带设计技术,在保证智能卡触点排列次序、触点相对位置和电学连接关系不变的前提下,在水平面上对条带宽度进行延展,如图3所示,使条带的有效覆盖面积扩大,相应地也就扩大了其下面可用来封装器件的面积。这样,就可以将一颗或多颗芯片封装在一张智能卡内。

一种可能的集成方案如图4所示,在智能卡与外部的电学连接关系保持不变的前提下,通过上述扩展可在一张卡内集成电源管理单元、微控制器单元、扩展存储器单元三类器件。这些器件的对外连接可实现为电源管理单元连接C1、C5管脚,微控制器单元连接其余6条管脚,扩展存储器单元分别连接电源管理单元和微控制器单元,如图5所示。在卡片内部通过金属线和条带上所带有的PCB(Printed Circuit Board, 印刷电路板)电路进行连接即可实现多芯片封装。

封装方法可以依照如下步骤实现:(1)根据芯片和元件组合之间的逻辑连接关系,设计并制作双层或者多层PCB基板;(2)采用表面贴装工艺将表面贴装元件逐一贴装在PCB基板上预先设计的元件位置,过回流焊使之固化;(3)用贴片胶将芯片逐一贴装在PCB基板上预先设计的芯片位置,并把芯片上的焊盘和PCB基板上的相关信号线焊接在一起;(4)将包含矩形腔体的塑封模具置于PCB基板加工位置上,把所要塑封的元件、芯片以及焊线完全覆盖起来,将塑封料灌入模具腔体,使之填充满芯片、元件和模具之间的空隙,并加热使之固化,形成多芯片和表面贴元件组合的智能卡模块;(5)将塑封后的模块用设计好形状的冲切工具,冲切出所需要的外部形状;(6)根据模块形状和尺寸,在智能卡卡体规定位置上铣出与被贴装模块尺寸一致的矩形槽体;(7)采用冷胶或者热融胶工艺,将塑封封装的模块植入到智能卡片的槽体中;(8)在已经封装好的智能卡片上根据标准尺寸冲切出Plug-in SIM卡形状。或者,在步骤(5)中,直接冲切成所要的Plug-in SIM卡。

下面对本发明的新型智能卡的硬件平台的三个主要功能模块进行描述。

本发明的新型智能卡的硬件平台一般情况下至少包括微控制器单元、

电源管理单元和扩展存储器单元三部分,如图4所示。微控制器单元完成计算和控制功能;电源管理单元对从智能卡外部触脚输入的电源进行管理、调整和分配给微控制器单元和扩展存储器单元使用;扩展存储器单元则用于代码和数据存储。微控制器单元对智能卡触脚上输入的信号进行分析和处理,根据需要从扩展存储器单元获取代码和数据,完成相应的处理后将数据或结果保存到扩展存储器单元,或者输出到外部终端设备。

微控制器单元用于对智能卡信号进行传输、控制、计算和处理,其主要的功能单元包括微处理器、片上总线、内存单元、ISO/IEC 7816 接口、高速接口控制器、DMA 控制器、中断控制器、时钟/复位管理单元。

微处理器主要用于计算、控制和通信。为了提高智能卡的处理能力,本发明采用 16/32/64 位(或更高位)的嵌入式微处理器,CPU 运行速度可根据应用进行配置和调整,通常可达到几十或几百 MIPS,大大提升了处理能力;除此之外,为了进一步提高智能卡的处理能力,根据实际应用情况,还可以采用各种类型的协处理器,如多媒体协处理器、DSP、密码协处理器,在微处理器的控制和协调下,针对具体应用进行指令优化和计算加速,微处理器与协处理器之间可采用总线方式、DMA 方式或其它数据通信方式进行连接。

由于新型智能卡的复杂度和规模相对于传统智能卡急剧增加,采用传统的集成电路设计方法已无法实现。由于 SoC 具有高集成性能,是实现复杂功能的主要解决方案,片上总线设计是关键技术问题。在本发明中,涉及到大量的高速数据传输和众多的功能模块集成,因此,本发明的新型智能卡采用片上总线来提高其内部组/部件之间或与外部接口之间的数据吞吐率。工业界有多个成熟的片上总线标准,如 CoreConnect、CAN bus、AMBA(Advanced Microcontroller Bus Architecture)和 Wishbone 等可用于本发明的新型智能卡中。

由于本发明的新型智能卡既有高速接口,如 DMA 通道、USB 接口,也有低速接口,如 ISO/IEC 7816 接口、中断控制器,因此,本发明的新型智能卡一种可能的实现方式是:采用改进的总线结构,如双总线结构,一条

总线用于处理高速数据传输，一条总线用于处理低速数据传输，两条总线之间采用总线桥接器或数据邮箱装置连接，进行不同速率的数据交换。根据双总线结构，ISO/IEC7816 接口接到一条总线上，高速数据接口则接到另一条总线上，将低速接口控制器和高速数据接口控制器分别接到不同的总线上，由 SoC 控制器来选择和控制总线的使用。SoC 控制器既可以单独启用一条总线来选择一种接口进行数据传输，也可以同时启用两条总线在 ISO/IEC 7816 接口和高速数据接口上同时传输数据独立控制数据传输，既可以提高数据吞吐量和传输效率，还可以提高智能卡接口的扩展性和适应性，扩大其应用范围。双总线既可以是同一类型的总线，如均是高速总线，也可以是不同类型的总线，如一个是高速总线，另一个是低速总线。为了与高速数据接口适配，与高速数据接口一同工作的总线必须是高速总线，以保证实现数据的高速传输。这样，新型智能卡可以根据不同的应用场合来选择不同的总线工作模式，从而提高新型智能卡的兼容性，扩大其使用范围。

内存单元是围绕在微处理器周边的一些存储器，利用这些存储器，微处理器可完成一个基本的计算系统。一般包括用于存储用户软件的程序存储器、用于存储智能卡基本应用数据的数据存储器、用于存储临时存放数据的随机缓存、必要时可增加存储控制器和内存保护单元等。程序存储器和数据存储器一般可使用各类非挥发类存储器实现。随机缓存一般可使用 SRAM 或 DRAM 实现。存储器可通过地址/数据总线直接连接在微处理器上，也可通过片上总线间接与微处理器连接。有些情况下，为了使可集成的存储器种类更加灵活，也可在片上设计存储控制器，用于实现与各种类型的存储介质（如 FLASH、RAM、SRAM、SDRAM、ROM、EEPROM 等）的控制接口。

由于智能卡产品的安全性要求，对于片内各类存储器要有一定的存取条件限制，通常设计 MPU（Memory Protection Unit，内存保护单元）用于保障卡内数据的安全性和完整性，实现对数据和代码的保护。新型智能卡在硬件上将存储区域分为几部分，它对不同的存储器或存储区域设置不同的访问控制条件，如读、写、删除都必须经过相应的安全认证后才能进行，防止未经授权的装载和访问，一旦产生非法访问时产生硬中断通知微处理

器。在软件上则分为不同的工作模式，不同的工作模式具有不同的访问权限。如果是系统工作模式，则可以对所有的存储区域进行访问或控制；如果是用户模式，则权限受到部分限制，只能访问和使用对其开放的区域；如果试图访问受控区域，则产生非法访问中断通知微处理器。

新型智能卡仍支持传统的 ISO/IEC 7816 接口，采用传统的五线连接方式。由于此接口的传输速率较低，因此将其连接到低速的片上总线上，实现 ISO/IEC 7816 协议的传输功能。

为了提高新型智能卡的接口速率，在实现 ISO/IEC 7816 接口的基础上，采用管脚复用和协议自动扫描识别技术，同时集成多种主流的高速传输接口，如 USB、SD、MMC。这样，一方面可以大幅度提高新型智能卡的传输速度，另一方面，由于集成的是主流的、标准的接口总线，不仅可以支持广泛的应用，而且协议处理也具备较强的扩展能力。同时，这些协议可以支持流媒体传输，而且与其它设备的使用连接关系也相对简单。

为了在智能卡中实现多种接口传输协议，同时保持新型智能卡与传统的读卡终端设备实现最大的兼容性，一方面必须保证传统智能卡 8 个触点的排列次序和连接形式不变（以实现兼容性），另一方面必须对部分管脚进行信号复用（以实现多种数据传输接口协议）。在新型智能卡的所有接口中，智能卡传统的和基本的功能要求决定了 ISO/IEC 7816 接口信号具有优先权，所有其他接口信号不能与它产生冲突和复用。根据对智能卡管脚排列的分析，可以看出，ISO/IEC 7816 接口信号实际上只使用了其中的 5 条管脚触点，有 3 条管脚（C4、C6、C8）未用，因此，本发明就利用这三条管脚实现其它高速信号复用，在此基础上，再根据传输的具体信号的不同，来识别不同的传输接口。具体的管脚信号复用的方法可以是将管脚 C4、C8 分别作为 USB 接口的差分数据线 D+、D-，并在此基础上，将管脚 C4 作为 SD 接口的 DAT0 线以及 MMC 接口的 DAT 线，将管脚 C8 作为 SD 接口及 MMC 接口的 CMD 线，将管脚 C6 作为三种接口的时钟信号线。在管脚复用的基础上，新型智能卡内部采用专用的高速接口控制器来实现与外部设备的高速数据传输。高速接口控制器主要完成三方面的功能：首先实现各种高速接

口协议的自动扫描和识别。其次，实现各种高速通信接口协议，如 USB、SD、MMC，完成通讯功能；最后，控制和协调各个外部数据接口的接通、关闭或切换，使 USB、SD、MMC 三种接口中同一时间只能有一种接口处于工作状态，其余两种接口处于关闭状态；并根据内部控制命令对这三种接口进行状态切换。高速接口控制器通过高速片上总线与微处理器或 DMA 控制器相连。

高速数据接口的输入/输出控制可以有两种实现方案，一种为集中统一控制方案，由 SoC 控制器对高速数据接口的输入/输出进行集中统一控制；另一种为分散独立控制方案，高速数据接口的输入/输出控制由各个高速通信模块自己控制，通过控制各个通信模块的工作与否来控制同一时间只有一种输出电路处于工作状态。

如图 11 所示，在第一种方案中，每个通信模块负责对一种接口信号进行识别和处理，UART (ISO/IEC 7816) 通信模块 2 负责处理 ISO/IEC7816 接口信号，USB 通信模块 7 负责处理 USB 接口信号，SD 通信模块 9 负责处理 SD 接口信号，MMC 通信模块 10 负责处理 MMC 接口信号。若某通信模块对输入的信号判断为有效信号，则它向 SoC 控制器 5 发出中断请求；SoC 控制器 5 根据此中断请求的类型，开始控制相应的通信模块进行通信。

UART (ISO/IEC 7816) 通信模块 2 通过低速总线 3 与 SoC 控制器 5 相连。USB 通信模块 7、SD 通信模块 9、MMC 通信模块 10 通过高速总线 8 与 SoC 控制器 5 相连。在智能卡上电时，若接口 1 有信号，UART (ISO/IEC 7816) 通信模块 2 产生 ISO/IEC 7816 中断请求，发送给 SoC 控制器 5；SoC 控制器 5 根据此中断类型，通过低速总线 3 与 UART (ISO/IEC 7816) 通信模块 2 进行通信，启动 ISO/IEC 7816 接口信号处理流程，实现传统智能卡的功能。

输入控制电路 15 和输出控制电路 11、12、13 由 SoC 控制器 5 来控制其是否选通，同一时间只有一个电路处于工作状态，即或者输入控制电路 15 工作，或者输出控制电路 11、12、13 三个中的一个电路工作。

如图 12 所示，在第二种方案中，高速数据接口的输入/输出电路 16、17、18 是由各个高速通信模块独立控制的。通过高速通信模块选择电路 6 来选择一个高速通信模块工作，同时保证只有一个输出电路可以工作；然

后由该模块来控制其输入/输出电路是处于输入状态还是处于输出状态。

高速通信模块选择电路6是一个两输入三输出电路。由于两线输入最多只有四种输出状态,因此,选用其中的三种状态作为三种高速通信模块的使能控制信号,剩下一种状态作为三种高速通信模块均不接通的信号,从而保证同一时间最多只有一种高速通信模块被选通,也就实现了同一时间最多只有一种高速数据接口工作的功能。

在启用 ISO/IEC 7816 接口后,若需要同时启用某个高速通信接口,则可以通过 ISO/IEC 7816 接口发送相应的 APDU 指令给 SoC 控制器,由 SoC 控制器启动相应接口的工作电路。

DMA 控制器用于按 DMA 方式传送大量数据。DMA 是一种完全由硬件执行数据交换的工作方式,一般用于高速传送成组的数据。DMA 控制器直接与片上总线连接。外设通过发送/接收信号来触发 DMA 传输。DMA 控制器可根据命令代替微处理器完全接管对片上总线的控制,产生地址、数据信号和控制信号,使数据交换不经过微处理器而直接在存储器之间或者存储器与外设之间进行。在传输过程中 DMA 控制器可以自动增加地址,对传送的字的个数计数,并且以中断方式向微处理器报告传送结束,之后把对片上总线的控制权交还给微处理器。

中断控制器用于管理外部中断请求,如当外部信号输入/输出操作结束或系统内部产生故障时输出中断请求信号,以便微处理器进行控制和处理。中断控制器通过片上总线与微处理器相连,通常可以将其连接在低速率总线上。中断控制器应支持多级中断请求,可通过编程设定优先级。

本发明的新型智能卡的时钟源既可以由智能卡终端设备等外设提供,也可以由智能卡内部提供;新型智能卡所需要的内部工作时钟必须是一个稳定的、不依赖于外部的时钟,因此本发明的新型智能卡采用时钟/复位管理单元来对卡内的时钟信号和复位信号进行统一控制和管理,一方面提供高效的、稳定的、无毛刺的系统工作时钟,另一方面通过钟控网络和上电复位电路来管理和切换芯片不同的工作模式,以降低芯片功耗。

具体地讲，时钟/复位管理单元主要实现如下几方面的功能：

首先，用于对智能卡内部和外部的时钟源信号进行管理和控制，如根据 GSM11.11 协议，手机终端将向 SIM 卡提供一个 1MHz-5MHz 的时钟源信号，为了使芯片可靠地工作并且不依赖于外部时钟源信号的有无，芯片内可再放置一个基准时钟源，时钟/复位管理单元负责根据应用不同和外界环境变化来切换不同的时钟源。该电路应具备毛刺滤除能力并应保证切换时不会产生因时钟源相位不同而导致的窄脉冲信号。其次，芯片在完成各类高速运算时提供高速工作时钟，可通过高精度的数据锁相环电路进行时钟源倍频。第三，为了降低芯片的功耗，时钟管理单元可以根据应用的要求，切换芯片工作模式，对系统工作时钟进行分频，关闭或开启某些模块的时钟信号。第四，由于新型智能卡具备 USB 接口，需要一个 48MHz/2500ppm 以下抖动的高精度时钟作数据采样，卡片内部提供该时钟信号。最后，时钟/复位管理单元可以通过编程实现对芯片各个工作模块（除电源管理单元、时钟/复位管理单元外）进行软复位。

本发明使用非挥发性存储器来存储操作系统和应用程序，在保证数据安全的前提下，提供一套带有高强度认证功能的程序下载电路 ISP (In System Programming, 在系统编程)，用于程序下载或更新。只有当安全认证通过后，才能进行程序的下载或更新。

本发明的新型智能卡的硬件平台的第二部分是电源管理单元。

由上述的微控制器结构和功能可以看出，新型智能卡需要给内部复杂的电路提供工作电源，由于芯片内部电路正常工作所需要的电压与半导体工艺相关，不同工艺所需要的工作电压不同，这就要求在新型智能卡内部可能需要提供诸如 1.8V、2.5V、3V 或 5V 等其中一种或多种工作电压；同时，由于智能卡的工作电源是由外部终端提供的，不同的终端提供的工作电压不同，波动范围较大，可能的工作电压范围为 1.8V ~ 3.0V ~ 5.0V，这就要求本发明的新型智能卡能够承受外部供给的各种电压范围并适配到芯片内部所需的供电电压，即要支持宽工作电压范围。因此，需要在卡片内放置电源转换和管理模块（如升压降压型电源转换器）以提供芯片内所需要

的各种工作电压，为此，本发明采用电源管理单元来对外部输入的各种电源进行统一适配和分配。

电源管理单元的输入端通过智能卡的电源触点（Vcc管脚）与片外电源连接，输出端与智能卡内部各个芯片及分离元器件的电源引脚连接。它既可以与智能卡其它组/部件集成在一颗芯片上，也可以使用单独的器件。在新型智能卡中，考虑到使用的方便性和扩展性，常使用单独的电源管理器件。经过选型，有3类电源管理器件可以满足要求：线性稳压器（LDO）、DC-DC转换器和升压电荷泵（CHARGE PUMP）。

本发明的新型智能卡的硬件平台的第三部分是扩展存储器单元。

传统智能卡的存储容量有限，市面上常见智能卡的最大容量不超过128K字节。利用新型存储技术（特别是闪烁存储器 FLASH MEMORY，简称闪存）以及存储器控制技术和先进的封装技术，可以大大扩充智能卡的存储容量。本发明的新型智能卡中的扩展存储器单元用于扩展智能卡的存储容量。

闪存是一类非易失性存储器（Non-Volatile Memory, NVM），即使在供电电源关闭后仍然能保留信息，可以对存储器单元块进行擦除和再编程，并且不需要额外的编程电压；而诸如 DRAM、SRAM 这类易失性存储器，当供电电源关闭时片内信息随即丢失。闪存具有工作电压低、擦写速度快、存储容量大、掉电数据不丢失、功耗低、寿命长、价格低廉、控制方法灵活、体积小以及可多次擦写等诸多优点，作为一种数据存储载体，它可以方便、快捷地保存大量数据。

NOR Flash 和 NAND Flash 是现在市场上两种主要的非易失闪存技术。NOR Flash 具有速度快的特点，可以实现程序的芯片内执行（XIP, eXecute In Place），即应用程序可以直接在闪存内运行，不必再把代码读到系统 RAM 中。NAND Flash 是一种新技术，与 NOR Flash 相比，在同样大小的芯片面积上可集成更大的存储容量。NOR Flash 适合于（低密度）代码存储，NAND Flash 适合于高密度数据存储。在新型智能卡中，主要采用闪存来扩展存储空间，其中，NOR Flash 主要用于存储和执行代码，而 NAND Flash 专用于存储数据。

扩展存储器也可采用其它各类新型的存储技术。如 FeRAM、分子存储

器等来进行扩展。既可以将扩展存储器与上述的微控制器集成在一颗芯片上，也可以采用物理上分开的办法。微控制器与扩展存储器之间的连接通过专用存储控制器电路实现。Nor Flash 控制器和 NAND Flash 控制器由于接口协议的不同需要使用各自独立的电路。

为了实现本发明的新型智能卡与外部终端或读卡设备通信，需要设计新型的或改造传统的终端或读卡设备的接口。下面进行具体说明。

(1) 与传统的符合 ISO/IEC 7816 标准的智能卡读卡器连接

由于新型智能卡仍然遵从了 ISO/IEC 7816 标准的接口，常规的读卡器可以直接使用新型智能卡，使用其符合 ISO/IEC 7816 标准的基本功能和应用；若要使用新增加的接口功能，读卡器就必须保证其卡座为 8 个触点（目前，很多读卡器使用了 6 个管脚的卡座，以控制生产成本），即完全符合 ISO/IEC 7816-3 协议中定义的管脚定义和分布标准。这样，硬件上可支持与新型智能卡的连接。

(2) 与存储卡类读卡器的连接

存储卡类读卡器是指用来读取存储卡的读卡器，如 USB 读卡器、SD 卡读卡器、MMC 卡读卡器。由于新型智能卡的物理形态受 ISO/IEC7816 标准的限制，与传统存储类读卡器的接口形态不匹配，因此可通过适配器装置，或者对传统的存储卡类读卡器的接口物理形态进行适当的改动，可与新型智能卡连接。智能卡读卡连接设备可以包括一个可承载智能卡的物理载体，该物理载体的一端具有 USB 插口或 SD/MMC 插口，另一端或其它侧面能够将智能卡插入或嵌入，该物理载体上设有与标准智能卡的触点位置相吻合的 8 个信号接触点，信号接触点与 USB 插口或 SD/MMC 插口连接；其中 5 个信号接触点的信号线根据 ISO/IEC 7816 协议分别定义为电源、地、复位、时钟和数据线，其余 3 个信号接触点的信号线分别定义为智能卡高速数据接口的数据、控制信号线和时钟信号线。

在功能强大的硬件平台基础上，本发明的新型智能卡的软件体系自底向上，可分为硬件驱动、RTOS（Real Time Operating System，实时操作系统）、API（Application Program Interface，应用编程接口）以及具体

的应用/业务等几个层次，如图6所示。

本发明的智能卡内部包含众多的电路模块并承载了大量的新型应用，调度和管理的复杂度极高，因此采用 RTOS 来做智能管理，以提供一个高效、稳定的多任务、多应用的工作环境。RTOS 控制着应用编程接口与硬件平台的相互通信，负责管理系统资源，提供高效的实时多任务调度。主要功能包括：处理器管理、中断管理、任务管理、时间管理、消息队列、内存管理、文件管理、设备管理等。当多个程序同时运行时，操作系统负责规划以及优化每个程序的处理时间。

硬件驱动主要是支持操作系统，提供各类设备或接口的驱动程序（如 FLASH、ISO/IEC7816、USB、SD、MMC），完成硬件初始化，以及时钟/电源管理。

API 为各种应用程序提供一个开放、统一、标准的应用程序接口，支持上层应用程序的开发。同时，应用程序也通过 API 调用各种底层系统资源。将一些典型应用（如 GSM 应用、JAVA 应用、移动邮件、移动多媒体）的功能和接口（如 STK 虚拟机、JAVA 虚拟机、IMAP4、MMAPI）提取出来，形成标准组件，以进一步降低开发的难度和工作量，在此基础上可以方便地、快速地进行具体的应用开发。

为了使本发明的新型智能卡能与目前主流的个人电脑、数码相机、MP3/MP4 播放机等数码设备共享和交换数据，在新型智能卡内部建立了通用的文件系统，可以兼容 Windows、Linux 等操作系统中常用的文件格式，如 FAT16、FAT32、NTFS、Ext2、Ext3 等，以提供最大的兼容性和方便；而且，还可以根据用户的选择，具体确定选用其中的何种文件格式。由此可见，本发明的新型智能卡不仅可以作为独立的存储器/卡（U 盘、SD 卡、MMC 卡）使用，而且可以作为一种数据交换平台，成为手机终端、个人电脑以及其它读卡终端设备的扩展存储器。

在上述强大的硬件平台和灵活、高效的软件体系的基础上，新型智能卡既支持传统的移动应用，如 GSM 应用、EMV 应用、移动银行等等，同时还支持大量的新型应用，如 DRM、网络下载、多媒体服务、网络游戏、网

络通信服务、互联网浏览服务、无线接入服务等应用。在新型智能卡中，可以通过绑定其 ICCID 以及 IMSI 来实现 DRM。同时借助其安全计算功能，完成个人身份的鉴别、增值业务的鉴权和计费。实现音乐、图片、彩铃等内容的安全下载和版权保护。

由于新型智能卡具有强大的计算能力、超大容量的存储空间以及高速传输接口，可以用软件或协处理器配合的方式来设计各种多媒体编解码器，如 MP3、MP4、VoIP (Voice/Video over Internet Protocol, 基于互联网协议的音频/视频) 等，对多媒体数据进行编解码处理，实现网络电话、电话录音、音视频播放等功能。

本发明的新型智能卡的工作原理和流程如下：

根据时钟来源不同，以及不同应用时所需要打开和关闭的电路状态，本发明的新型智能卡芯片可支持多种工作模式，包括：正常工作模式、低功耗工作模式和休眠模式。本发明的时钟源主要有两种：外部时钟和内部时钟。外部时钟是指由智能卡终端设备提供，从智能卡外部触点输入的时钟信号，包括智能卡工作时钟信号（简称 SIM 时钟，由智能卡 CLK 触点输入）、SD 卡工作时钟信号、MMC 工作时钟信号；内部时钟则是指智能卡内部时钟源振荡器；工作时钟是指通过数字锁相环电路倍频及分频后得到的时钟信号，可提供系统工作时钟以及 USB 接口所需要的高精度时钟信号。由时钟/复位管理单元负责芯片内部各种工作模式的切换。各模式的含义如下：

- 正常工作模式：使用内部或外部提供的时钟作为信号源，经过锁相环（PLL）提供系统工作所需要的各种时钟。此时内部各个电路模块的时钟是打开的。
- 低功耗工作模式：使用内部或外部提供的时钟作为信号源，关闭锁相环（PLL），打开 SIM 基本功能工作时所需要的最少硬件模块（如 CPU、SRAM、FLASH、MPU）的时钟，其它电路此时关闭。
- 休眠模式：使用内部或外部提供的时钟作为信号源，关闭锁相环（PLL），打开 ISO/IEC 7816 接口、中断控制器等模块电路，关闭 CPU、各个存储器等大多数模块电路，此时 SIM 基本功能也没有工

作，整个系统处于等待唤醒状态。

本发明的新型智能卡在各个工作状态时，ISO/IEC 7816 接口一直处于开启状态；而 USB、SD、MMC 三种接口同一时间只有一种接口处于开启状态，或者全部关闭。因此，根据接口的工作状态，新型智能卡有四种工作状态：SIM 状态、USB 状态、SD 状态、MMC 状态。SIM 状态是指只有 ISO/IEC 7816 接口处于工作状态，而其它三种接口均关闭的情况，后三种状态是指相应的某种外部高速接口与 ISO/IEC 7816 接口处于同时工作（开启）状态。

本发明的新型智能卡在上电初始化芯片后，根据外设输入的接口信号的不同选择进入到不同的工作状态。如果是 SIM 状态，则芯片进入低功耗工作模式，按照传统智能卡的工作流程进行工作；如果是 USB、SD、MMC 状态之一，则芯片进入正常工作模式，按照相应的传输协议进行工作。如果在某一状态，智能卡在一段时间内没有任何操作，则芯片进入休眠模式；当有新的指令到来后，芯片就恢复到原来的工作状态。当新型智能卡在智能卡终端设备（如手机终端）中使用，可以通过专用的状态切换指令，从 SIM 状态切换到其它三种状态之一，或者反向切换。

当本发明的新型智能卡在手机终端之类的智能卡终端设备中使用时，既可以当作传统的智能卡/SIM 卡使用其 ISO/IEC 7816 接口，也可以同时使用其高速传输接口。

当本发明的新型智能卡放在存储卡类的读卡设备中使用时，则使用其高速传输接口和功能，当作普通的存储卡（如 U 盘、SD 卡、MMC 卡）使用。

下面参照附图来描述本发明的优选实施例，以在 SIM 卡中同时实现 USB/ SD/MMC 接口为例进行描述。

由于本发明的新型智能卡功能众多，采用多芯片封装工艺；为了能将所有芯片封装在一起，采用金属条带工艺来扩大芯片的有效封装面积。最终芯片的封装形式如图 3 所示。

微控制器单元的总体结构如图 7 所示，主要包括微处理器、片上总线、内存单元、I/O 控制器、ISO/IEC 7816、DMA 控制器、中断控制器、闪存控

制器、时钟/复位管理单元 (CPMU)，时钟/复位管理单元 (CPMU) 为其他所有单元提供时钟/复位信号。

微处理器选择通用的嵌入式 CPU，可以是 16/32/64 位的微处理器，比如 ARM 公司的 ARM7TDMI。协处理器根据具体的应用场合和要求来选择，如用密码算法协处理器来进行模幂计算、多媒体协处理器进行矢量模乘运算等等。

在本实施例中，优先选择 AMBA 2.0 总线规范作为片上总线。由 ARM 公司推出的 AMBA 片上总线受到了广大 IP 开发商和 SoC 系统集成者的青睐，已成为一种流行的工业标准片上结构。AMBA 规范主要包括了 AHB (Advanced High performance Bus) 系统总线和 APB (Advanced Peripheral Bus) 外围总线。在本实施例中，OCB1 采用 AHB，用于连接片内高速部件，如 ARM 核、DSP 核等核心模块，OCB2 采用 APB，用于连接低速部件，如中断控制器、ISO/IEC 7816 接口。两总线之间用 AMBA 总线桥连接。

内存单元包括 ROM、RAM、EEPROM、FLASH。ROM 和 EEPROM 用于下载和存储 RTOS 以及系统信息，RAM 是工作存储器，用于交换临时数据。FLASH 用于存储用户数据或代码。

在本实例中，按下表所示方案实现对智能卡管脚的复用。

工作模式 管脚含义 管脚编号	ISO/IEC 7816	USB	SD	MMC
C1	Vcc	--	--	--
C2	RST	--	--	--
C3	CLK	--	--	--
C4	--	D+	DATA0	DAT
C5	GND	--	--	--
C6	---	--	CLK	CLK
C7	I/O	--	--	--
C8	---	D-	CMD	CMD

在管脚复用的基础上，I/O 控制器主要实现 USB、SD、MMC 三种高速接口以及接口信号扫描和协议自动识别功能，并协调不同接口状态的切换。ISO/IEC 7816 接口实现 ISO/IEC 7816 协议的通信功能。

本发明的新型智能卡在上电初始化芯片后，根据外设输入的接口信号的不同选择进入到不同的工作状态。如果是 SIM 状态，则芯片进入低功耗工作模式，按照传统智能卡的工作流程进行工作；如果是 USB、SD、MMC 状态之一，则芯片进入正常工作模式，按照相应的传输协议进行工作。如果在某一状态，智能卡在一段时间内没有任何操作，则芯片进入休眠模式；当有新的指令到来后，芯片就恢复到原来的工作状态。新型智能卡外部的读卡设备可以通过扩展 APDU (Application Protocol Data Unit, 应用协议数据单元) 指令来通知智能卡切换工作状态。

DMA 控制器连接在高速片上总线上，独立于微处理器，可以替代微处理器来接管对总线的控制，数据交换不经过微处理器而直接在存储器之间（如 SRAM 与 Flash 之间）以及存储器和外设之间（如 Flash 与 USB 接口设备之间）进行。

闪存控制器除了与微控制器单元内部的闪存相连外，其主要功能是提供与微控制器片外闪存存储器相连的接口，以供在微控制器外部扩展闪存存储器使用。闪存控制器主要提供对 NOR、NAND 两种 FLASH 的扩展和控制，一方面有效提高智能卡的存储容量，另一方面有效降低大容量智能卡的成本。

时钟/复位管理单元 (CRMU) 的总体结构框图如图 8 所示，包括分别与片上总线连接的时间分频及门控制电路、复位信号产生模块和数字锁相环 (PLL)、晶振器 (OSC) 及其控制器。锁相环用于获取高频时钟源，晶振器用于获得低频基准时钟源。图中只表示出了芯片内部时钟源和外部 SIM 卡时钟源，没有列出 SD、MMC 的时钟信号，是因为时钟/复位管理单元对这两种时钟信号不做任何处理，直接输送到相应的 I/O 控制器。总线控制信号控制晶振器、锁相环控制器来选择芯片工作时钟是外部时钟还是内

部时钟，并控制输出时钟、复位信号。时钟分频及门控电路以及复位信号产生模块均为公知结构，此处不再过多介绍。

电源管理单元（PMU）的功能结构如图9所示，以两路输出为例。要在智能卡内部实现电源管理，因此必须选择能够在硅裸片上实现的方案。经过选型，有3类电源管理器件可以满足要求：线性稳压器（LDO）、DC-DC转换器和升压电荷泵（CHARGE PUMP）。本实施例采用线性稳压器，其结构示意图如图9所示，以两路输出为例。当智能卡外部电压在1.5V~5.5V区间变化时，可以通过PMU为智能卡内部的用电元件供电；当外部电压超出标准范围或负载电流超出电源管理单元负载上限时，PMU将关断，并保护智能卡内部核心芯片组及周边用电元件不被电学烧毁。

将PMU的输入端（VIN）与智能卡标准触点C1相连，地（GND）与智能卡标准触点C5相连，并通过智能卡触点连接智能卡外部的电源设备；将PMU的使能信号端（EN1/EN2）与VIN连接，以使PMU的多路输出有效；PMU的输出可以接到微控制器和/或扩展存储器。

本发明的新型智能卡的软件按分层结构设计，分为硬件驱动、RTOS、API、以及具体的应用/业务等几层，详细结构如图10所示。本发明的智能卡内部包含众多的设备器件和应用程序，调度和管理的复杂度高，因此采用RTOS来做智能管理，以提供一个高效、稳健的多任务、多应用的工作环境，主要功能包括任务调度管理、文件管理、内存管理、中断管理、时间管理、设备管理。硬件驱动主要是支持操作系统，提供各类设备或接口的驱动程序（如FLASH、ISO/IEC7816、USB、SD、MMC），完成硬件初始化，以及时钟/电源管理。API提供一个开放的、统一、标准的应用程序接口，如图形用户界面（GUI）、多媒体API（MMAPI），方便应用程序的开发。将一些常用的协议或标准（如GSM 11.11协议、GSM 11.14协议、EMV 2000协议、JAVA虚拟机、STK虚拟机等）以及其它一些常用的功能接口（如浏览器、解析器等）做成组件，预置在智能卡内，方便使用和开发。

业务/应用则确定了新型智能卡的具体应用形态。除了可以作为单独的移动存储设备（如U盘、SD卡、MMC卡）以及传统的应用（如GSM应用、

EMV 应用)外,可以利用本发明强大的计算能力、超大容量的存储空间和高速的外部接口来开发和部署大量的移动增值业务。如 DRM、音乐下载、移动商务、电子钱包、移动电视等等,既可以方便用户的使用,也能有效提高运营商的 ARPU (Average Revenue Per User, 每用户平均收入)值,并有助于其加强对产业链的控制权。

考虑到在此公开的对本发明的描述和特殊的实施例,本发明的其他实施例对于本领域的技术人员来说是显而易见的。这些说明和实施例仅作为例子来考虑,它们都属于由所附权利要求所指示的本发明的保护范围和精神之内。

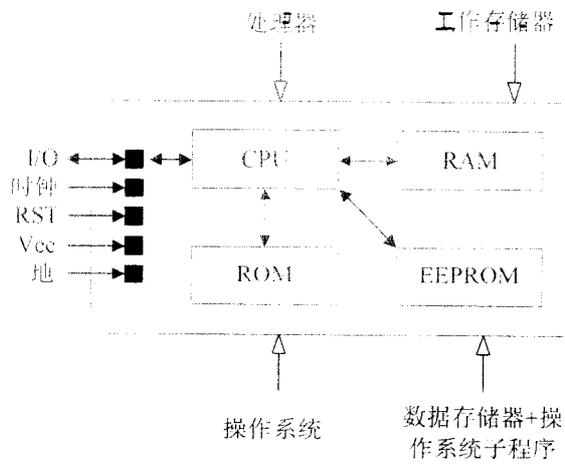


图 1

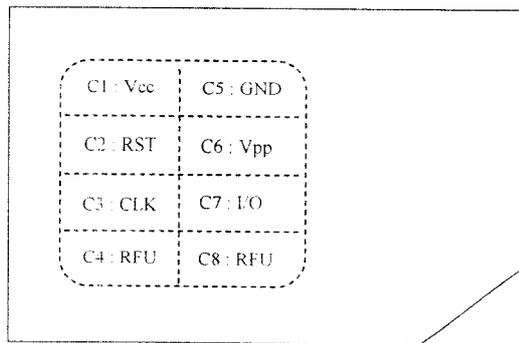


图 2

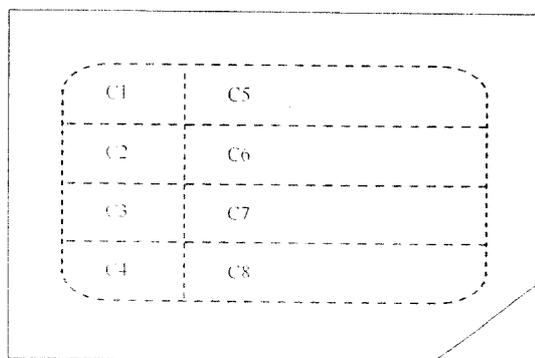


图 3

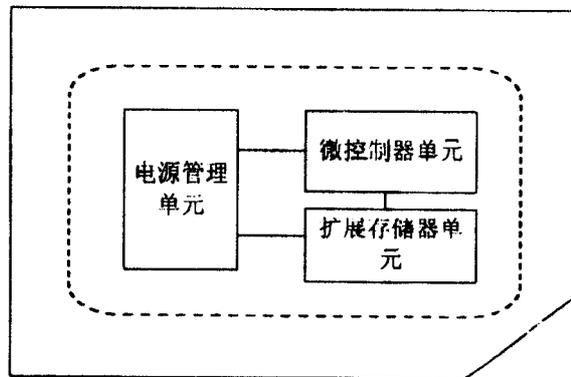


图 4

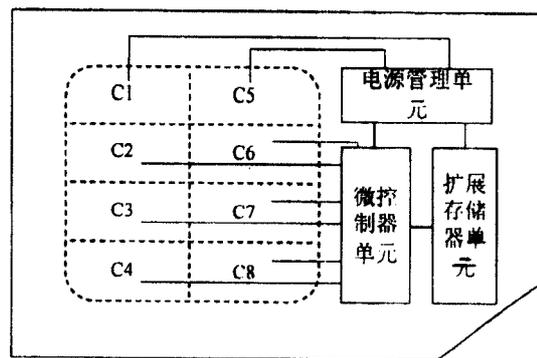


图 5

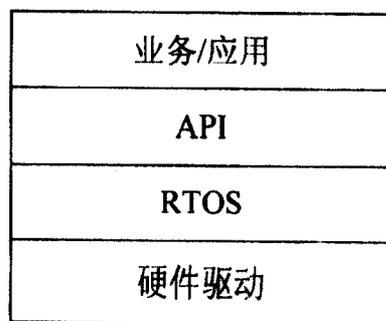


图 6

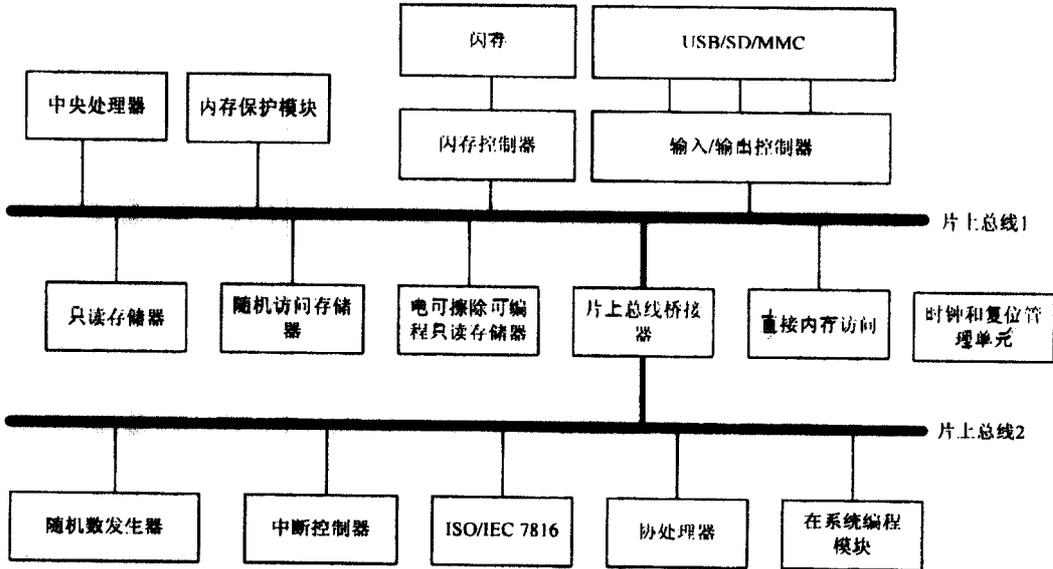


图 7

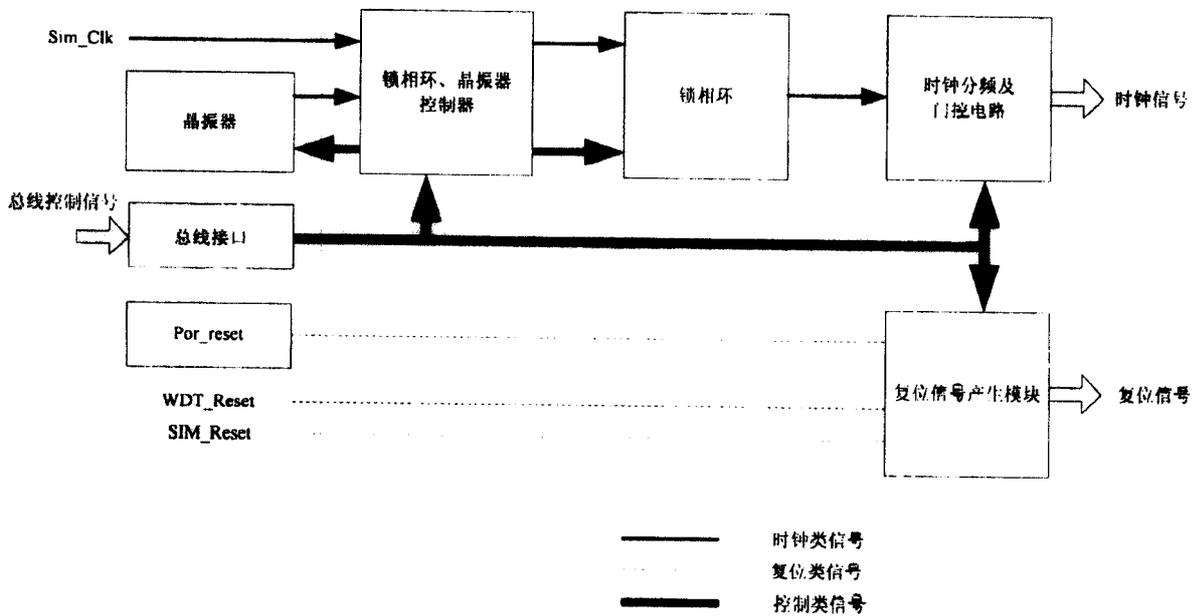


图 8

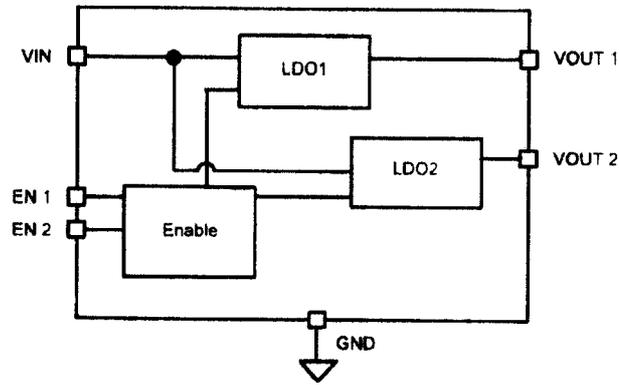


图 9

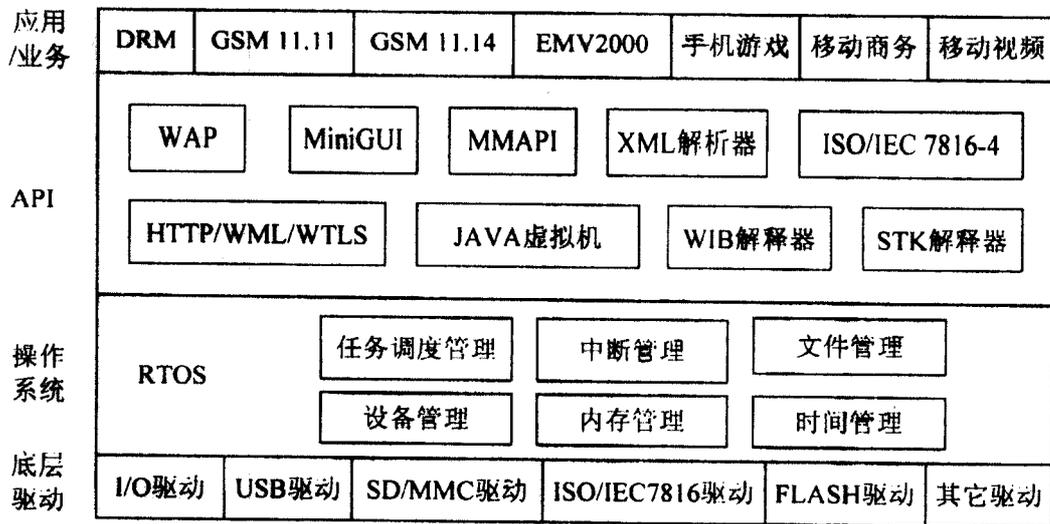


图 10

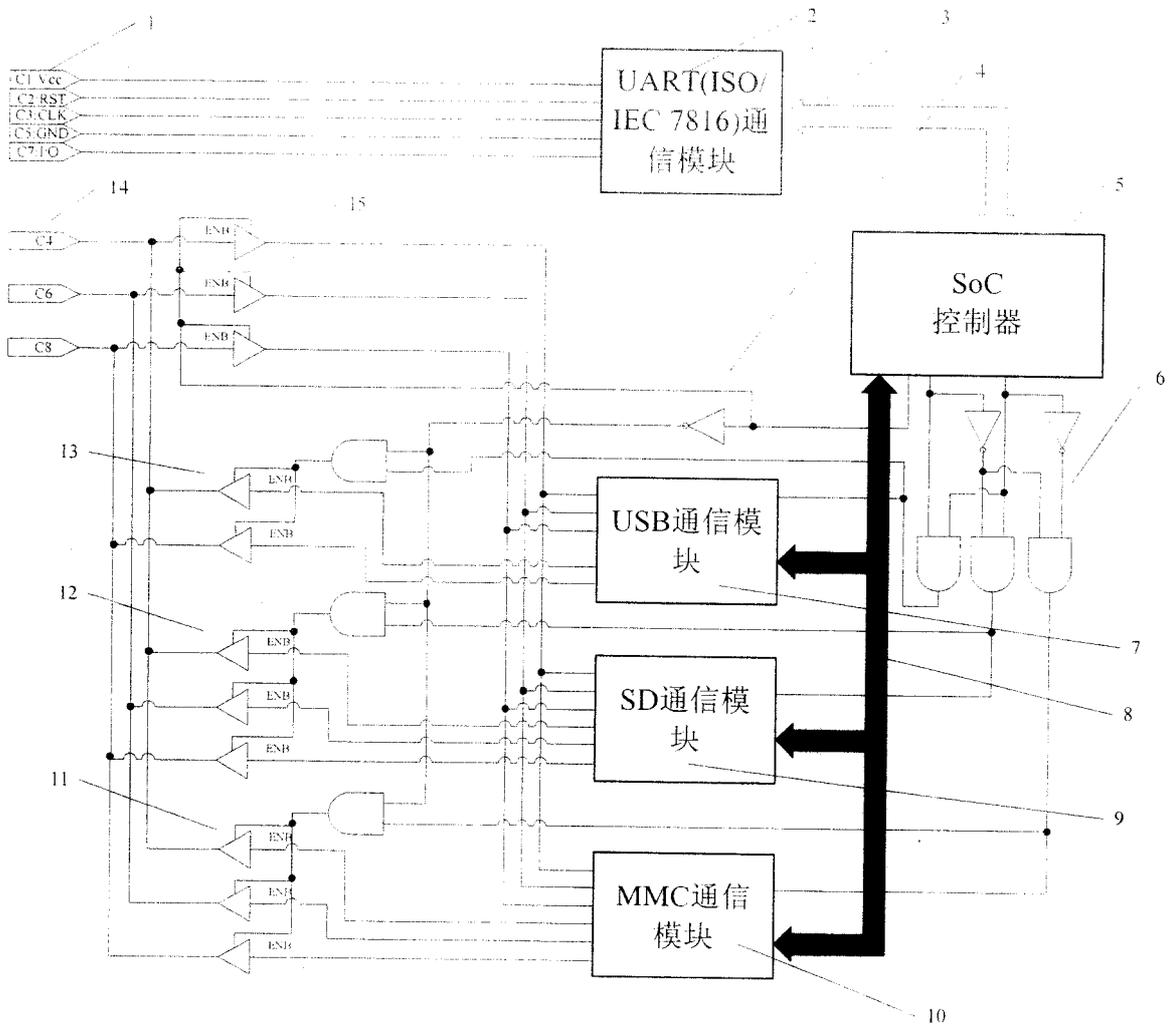


图 11

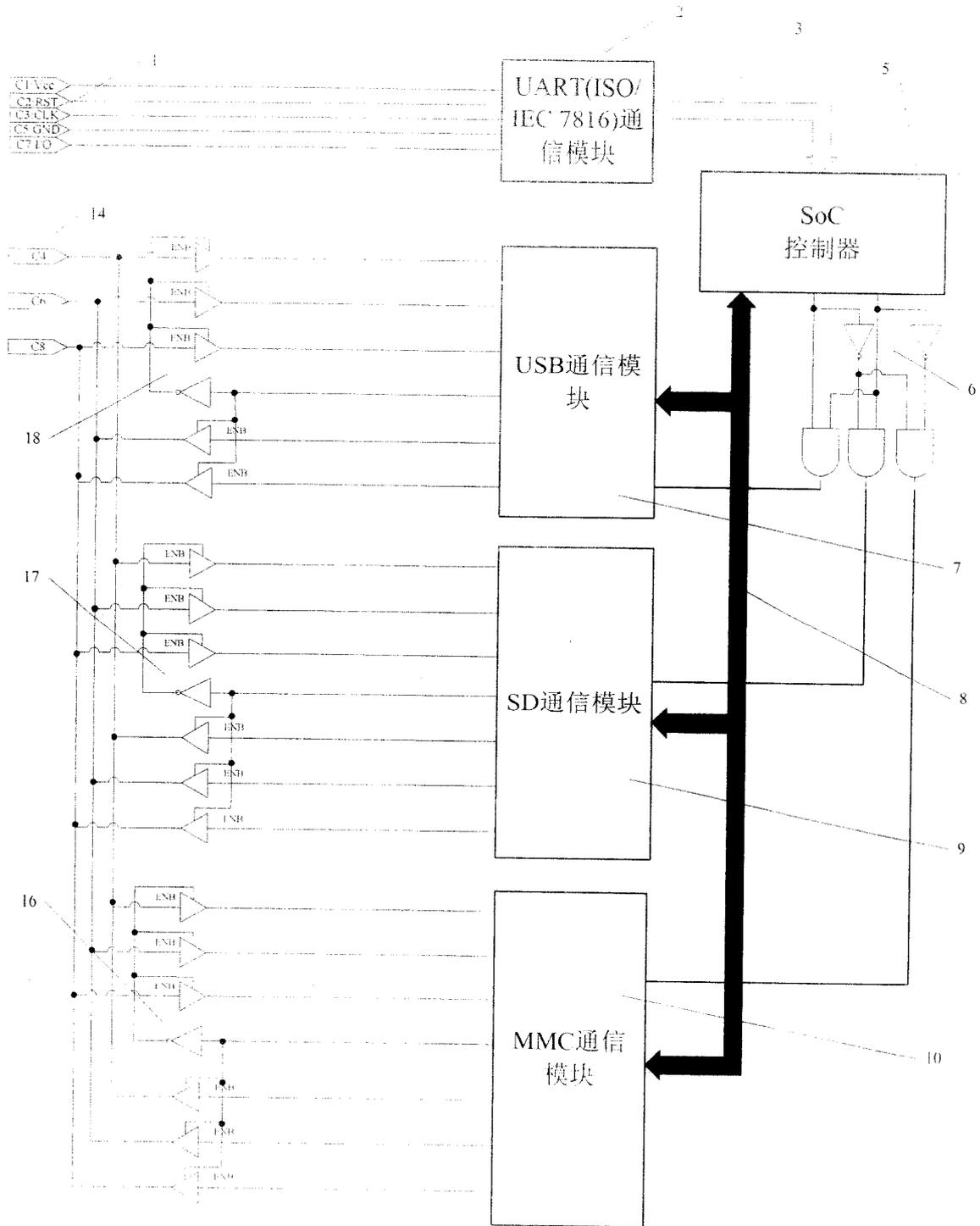


图 12