**基于NFC技术的SWP方案以及在SIM卡中的实现方法**

近几年，手机已经不再是简单的通信工具，它已经成为便携的娱乐工具，将来有望发展为可信赖的支付工具，在消费、购物、交通等领域通过手机方便、快捷地完成支付。基于手机的新需求，移动支付应运而生，并逐渐成为移动运营商、手机制造商、SIM卡制造商研究的热点问题。移动支付的解决方案比较多，其中双界面SIM卡方案和近距离通信(Near Field Communication，NFC)方案比较可行。双界面SIM卡方案已经有产品面世，近距离通信方案正在研发阶段。

　　双界面SIM卡方案通过在SIM卡中增加非接触IC卡界面进行非接触通信。天线连接在SIM卡尚未使用的C4和C8这两个接口上。双界面SIM卡在手机中增加了非接触IC卡的功能，但没有实现阅读器和点对点通信功能。NFC是由NXP公司和索尼公司提出的超短距离无线通信技术，它使得两台兼容NFC的设备之间可以直观、便捷、安全地通信。NFC的主要应用是移动小额支付，还可以应用于门禁、公交等领域。

　　与双界面SIM卡方案相比，NFC方案的优势体现在以下方面：

　　①NFC方案可以实现更多的应用;

　　②在NFC芯片与SIM卡的连接使用C6(SWP)触点，并不影响SIM卡高速空中数据下载;

　　③NFC方案是一套完善的解决方案，可以提供可靠、安全、便捷的通信;

　　④NFC方案完全兼容现有的读写器，不需要对读写器进行任何更改。

　　综上所述，近距离通信NFC是移动非接触支付业务最可行的解决方案，而SWP连接方案则是NFC技术的一部分。

**1、近距离通信概述**

　　近距离通信是短距离非接触式的一种，工作于13.56 MHz频带，传输距离在10 cm以内;传输速度目前可以达到106 kbps、212 kbps、424 kbps，理想速率可以达到1 Mbps左右。NFC所使用的频率与目前流行的非接触智能卡相同，同时兼容以ISO14443 A/B为基础的感应式非接触通信，以及Philips公司的MIFARE技术和索尼公司的FeliCa技术。

　　1.1 近距离通信原理

　　根据ISO18092标准，近距离通信可以工作在主动模式和被动模式。进行通信之前，可以选择传输速率106 kbps、212 kbps、424 kbps中的一种，并可以在这三者间任意切换。

　　1.1.1 被动模式通信原理

　　在被动模式下，近距离通信的通信原理与RFID一样，都是依靠电磁感应耦合原理完成通信。NFC手机有一块NFC芯片，内置有天线，用来接收和发送无线数据。

　　NFC工作在被动模式时，阅读器启动NFC通信，称为NFC发起设备(主设备)，在整个通信过程中提供射频域。NFC发起设备选择3种速率的一种传输数据，ISO18092标准规定了每种传输速率使用的调制、编码技术。NFC目标设备(从设备)不必产生射频域，而使用负载调制(load modulation)技术，以相同的速度将数据传回发起设备。此通信机制与基于ISO14443 A/B、Mifare和FeliCa的非接触式智能卡兼容，因此，在被动模式下，NFC发起设备可以用相同的连接和初始化过程检测非接触式智能卡或NFC目标设备，并与之建立联系。

　　就近距离通信应用的角度而言，其应用模式分为3种：标签模式、阅读器模式、点对点模式。标签模式，即NFC芯片作为被动设备使用，其作用相当于应答器。为了保证数据的安全性，在更换手机后不至于重新设置密钥信息，需要在SIM卡中保存移动支付的密钥信息。通信设备包括阅读器、NFC芯片和SIM卡。此时，NFC芯片提供射频接口，负责转发射频数据给SIM卡。对SIM卡而言，不需要像双界面SIM卡那样增加非接触接口，而使用SWP接口实现与NFC芯片的连接。在标签模式下，NFC芯片类似于桥接器，在阅读器和SIM卡之间转发数据。

　　NFC芯片是嵌入手机中的芯片，由手机的电源系统供电。为了保证手机没电时移动支付的正常进行，标签模式需要支持无源工作，其工作原理基于电磁感应。阅读器的天线线圈产生高频的强电磁场，这种磁场穿过线圈横截面和线圈周围的空间。发射磁场的一部分磁力线穿过距阅读器线圈有一定距离的应答器的天线线圈。通过感应在天线线圈上产生电压，将其整流后作为电源提供给NFC芯片和SIM卡。

　　1.1.2 主动模式通信原理

　　在主动模式下，NFC发起设备要发送数据给目标设备时，必须产生自己的射频场;被读NFC设备发送响应给发起设备时，也要产生自己的射频场。发起设备和目标设备都要产生自己的射频场，这是对等网络通信的标准模式，可以获得非常快速的连接设置。

　　移动设备主要工作在被动模式，可以大幅降低功耗，并延长电池寿命。主动模式主要是针对点对点模式，用于笔记本、手机、数码相机之间的数据交换。

　　1.2 近距离通信与RFID的关系

　　NFC是一种基于RFID的无线通信技术，二者都工作在13.56 MHz频带。在标签模式下，NFC利用RFID的通信原理，都基于无线频率的电磁感应耦合原理。

　　但是NFC技术是无线通信的新技术，与RFID还是有区别的：NFC技术增加了点对点通信功能，可以快速建立蓝牙设备之间的P2P(点对点)无线通信，NFC设备彼此寻找对方并建立通信连接。P2P通信的双方设备是对等的，而RFID通信的双方设备是主从关系。

**2、SWP标准及连接方案**

　　2.1 SWP标准

　　SWP连接方案基于ETSI(欧洲电信标准协会)的SWP标准，该标准规定了SIM卡和NFC芯片之间的通信接口。

　　SWP(单线协议)是在一根单线上实现全双工通信，即S1和S2这两个方向的信号，如图1所示。通信的双方是UICC(Universal Integrated Circuit Card，通用集成芯片卡)和CLF(Contactless Frontend,非接触前端)。S1是电压信号，SIM卡通过电压表检测S1信号的高低电平，采用电平宽度调制;S2信号是电流信号，采用负载调制方式。S2信号必须在S1信号为高电平时才有效，S1信号为高电平时导通其内部的一个三极管，S2信号才可以传输。S1信号和S2信号叠加在一起，在一条单线上实现全双工通信。

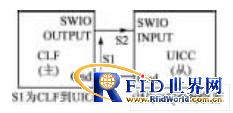


图1 SWP信号定义

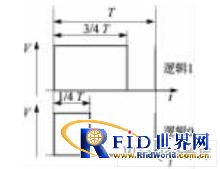


图2 S1信号的编码

　　S1信号的编码如图2所示，逻辑1在3/4周期(3/4T)内为高电平，逻辑0在1/4周期(1/4T)内为高电平。S2信号在S1信号为高时有效，在S1信号为低时才能进行由低电平到高电平之间的切换。SWP有3种传输速率：212 kbps、424 kbps、848 kbps，对数据位进行扩展之后，传输速率可以达到1 696 kbps。

　　SWP协议是关于物理层和数据链路层的协议。物理层负责UICC和CLF之间物理链路的激活、保持、解除等工作。SWP协议要求UICC的工作电压为1.8～3.3 V。

　　与OSI协议类似，数据链路层分为MAC(媒介访问控制)层和链路控制层。在MAC层采用位填充的成帧方法。链路控制层包括3种类型的帧协议：ACT协议、SHDLC协议以及CLT(非接触通道)协议。在SWP接口的设计中，使用了前两种协议。

　　ACT协议是接口激活协议，用于激活SWP接口。在没有射频场时，SWP接口处于去激活状态。在标签模式下，感应到外界存在射频场后，NFC芯片被激活，UICC收到NFC芯片的高电平信号后，使用ACT帧建立物理链路的连接。

　　SHDLC协议是ISO制定的高级数据链路控制规范的简单版本，也是面向位的同步链路。该协议主要用来传输交互的数据信息，其信息帧承载上层HCP(主机控制协议)的包数据。此外，SHDLC协议还具有流控管理、错误检查、出错后数据重传等功能。为了保证数据的正确发送与接收，兼容NFC芯片与UICC不同速率传输的通信能力，在使用SHDLC协议通信前，首先要建立数据链路，双方协商滑动窗口的大小。

2.2 SWP连接方案

　　本文中，CLF嵌入在手机内部，UICC使用的是SIM卡，手机通过SIM卡与NFC芯片通信。NFC芯片与SIM卡的连接方案有多种，本文提出的是基于C6引脚的SWP(单线协议)方案。SWP协议连接手机NFC芯片与SIM卡，规定两者之间的通信接口。图3是SWP连接方案的示意图。

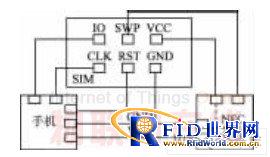


　　图3 SWP连接方案示意图

　　本方案中使用了SIM卡的3个引脚连接NFC芯片：C1(VCC)、C5(GND)、C6(SWP)。其中，SWP引脚在一根单线上基于电压和负载调制原理实现全双工通信。SIM卡支持ISO7816和SWP两个接口，在大容量卡项目中还支持高速下载接口，通过预留的C4和C8接口来实现。支持SWP的SIM卡必须同时支持两个协议栈：ISO7816和SWP协议栈，这需要SIM卡的COS(片上操作系统)是多任务系统。

　　SIM卡需要单独管理这两个协议栈。SWP方案加入SIM卡系统后，不能影响ISO7816接口。举个例子，SIM卡有8个引脚，RST引脚用于复位SIM卡的ISO7816接口，SWP方案加入SIM卡后，RST引脚的Reset信号对SWP接口没有作用，SWP接口通过SWP引脚复位。

**3、SWP连接方案在SIM卡中的设计**

　　3.1 系统结构

　　大容量SIM卡是一种支持大容量存储、高速传输、具有新型应用的智能卡。我们研发的大容量SIM卡项目基于ARM Secure Core SC100内核，采用 AHB(高性能总线)+APB(高级外设总线)总线结构。AHB总线提供高速的数据传输，它连接SIM卡内部存储器和高速外部接口(USB接口)。APB总线通过桥接器与AHB总线相连，SIM卡的低速接口(SWP接口、ISO7816接口)挂靠在外设总线上。

　　3.2 硬件设计

　　SWP硬件设计基于SWP标准，即ETSI(欧洲电信标准协会)制订的的TS 102 613。SWP控制器和SWP接口共同组成了SWP方案的硬件设备。SWP控制器负责处理物理层和数据链路层逻辑。图4为硬件实现数据链路层逻辑时SIM卡内部SWP控制器的结构图。

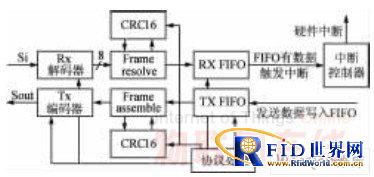


图4 SWP控制器结构图

　　3.2.1 接收数据设计

　　在SIM卡和NFC芯片通信期间，SWP控制器在激活、挂起、去激活三种状态间切换。交换数据时，处于激活状态。Rx 解码器不停地检测Si信号，并将来自NFC芯片的单位数据解析为字节输出。Frame. resolve分析接收到的每一字节的数据，若为7E(帧头)，则继续接收数据，直到接收到7F(帧尾)，表明SWPC接收到一帧完整的数据。Frame. resolve进一步解析接收到的数据帧，首先根据MAC协议剥离帧头和帧尾，然后根据接收方的生成多项式对数据帧进行校验。如果数据正确，则识别出SHDLC数据帧的类型并作相应处理;如果数据错误，则发送拒收帧，要求对方重新发送。对于正确的信息帧，SWP控制器提取信息帧的信息数据(包)写入RX FIFO，并根据接收到的数据帧的字节个数设置控制器的状态寄存器。SWP控制器每接收一帧数据就发起一个硬件中断。

　　3.2.2 发送数据设计

　　SWP控制器发送数据和接收数据是相反的过程。如果上层应用有数据要发送时，会把数据写入TX FIFO。TX FIFO一旦检测到FIFO有数据，就启动发送模块把数据从TX FIFO中取出，经Frame. assemble按照SWP协议的SHDLC协议组装信息帧，添加帧头、帧尾、校验码。把生成的MAC帧数据交给Tx编码器，完成输出数据的物理层组装，将数据转换成单个位电平输出。

　　3.3 软件驱动设计

　　SWP软件设计基于SWP标准和HCP(主机控制协议)标准。HCP标准是SWP协议之上的标准协议，定义了数据链路层之上的协议层——HCP路由层、HCP消息层以及应用层。底层SWP协议和上层HCP协议组成的协议栈共同完成NFC芯片与UICC通信的完整协议。

　　在大容量SIM卡中采用SWP方案，要实现ISO7816协议栈和SWP协议栈。SIM卡的操作系统使用μC/OS。μC/OS是一种结构小巧、抢占式的实时操作系统。其内核提供任务调度和管理、时间管理、任务同步和通信、内存管理和中断服务等功能。在软件系统中，SWP软件模块是μC/OS的任务之一。

　　SWP任务依靠硬件中断驱动，SWP任务没有被激活前，一直处于等待中断的状态。通过SWP接口通信时，一旦检测到存在射频场，NFC芯片便被激活。NFC芯片发送Si信号给SIM卡，SIM卡检测到Si电压信号后，触发si\_act中断通知软件做好准备通信。此时，软件设置通信参数，然后等待硬件建立物理链路成功的中断。如果接收到init\_sync中断，软件开始设置SHDLC协议的滑动窗口大小M，等待建立SHDLC链路的中断。这个中断带有NFC芯片SHDLC层的滑动窗口的参数N。若M≥N，则SWP任务修改自己的滑动窗口大小为N，然后发送确认帧，这样便建立了SHDLC链路;若M

　　SHDLC链路建立成功后，SWP任务等待信息帧中断。接收到信息帧中断，根据硬件写入的状态寄存器的接收字节数从RX FIFO中读取数据，然后由软件解析收到的数据包;通过HCP的路由层把数据包递交给应用层，应用层根据消息的类型进行相应的处理。

**结束语**

　　本文提出一种SWP连接方案，并在大容量SIM卡中加以实现。SWP接口的硬件和软件设计方法，对于近距离通信技术应用于其他移动支付具有一定借鉴意义;同时，在SIM卡中实现SWP接口，也促进了SIM卡技术的发展。