NFC 芯片与 SIM 卡连接的方案研究

石亦欣 复旦大学专用集成电路与系统国家重点实验室

李蔚 上海复旦微电子股份有限公司

摘要：

NFC 应用是目前移动通讯行业与 RFID 行业所关注的热点，NFC 技术将移动终端与 RFID 应用紧密的捆绑在一起，引发了一系列新的应用模式。作为 NFC 应用推动的主流力量，移动运营商提出了基于 SIM 卡实现 NFC 应用的需求。本文详细分析讨论了 NFC 芯片与 SIM 卡连接的方法，并提出合理的建议方案。

关键词：

NFC SWP

1、概述

IC 特别是非接触式 IC 卡经过十多年的发展，已深入现代生活的各个角落，被广泛应用于公交、门禁、小额电子支付等领域。近年来，在轨道交通、物流管理、物品防伪、身份识别等需求推动下，非接触式 IC 卡（或者电子标签）技术的不断进步，应用越来越普及，迫切需要各类非接触 IC 卡识别设备。与此同时，移动通讯设备经历 20 多年的迅速发展，已经几乎成为居民人手俱备的随身装置，普及率非常高，并且有向移动通讯终端集成更多功能的趋势。可以看到，RFID 应用技术和移动通讯技术相结合，将激发出无数的新型应用，将是今后 RFID 技术发展的热点。

NFC（Near Field Communication 近场通讯）是这几年飞速发展的一种新兴技术，由 Sony、Philips 和 Nokia 提出，它使得两个电子设备直接可以进行短程的通讯，工作在 13.56MHz 频段，工作距离几个厘米。NFC 技术目标是电子设备之间的近距离通讯，主要实现三类功能：非接触 IC 卡片模拟功能；点对点数据通讯功能；读卡机功能。NFC 技术的出现，极大地促进了 RFID 技术与移动通讯技术的融合进展，引发出许多新的应用模式。NFC 应用的推广需要移动终端的更新，需要跨行业的应用整合，是一个涉及多行业、多层次的复杂项目，难点非常大。移动运营商在 NFC 推广中扮演着十分重要的角色，根据移动运营商的需求，NFC 实现方案需要提供一种将 RFID 应用或者 NFC 应用与移动运营商关联在一起的方案，也即需要一种将 RFID 应用或者 NFC 应与 SIM 卡关联的方案。

2、NFC 硬件架构

下图是 NFC 硬件架构图。NFC 功能的实现由两部分组成：NFC 模拟前端（NFC Controller 与天线）和安全单元。根据应用需求的不同，安全单元可以是 SIM、SD、SAM 或其它芯片。本文将仅讨论 SIM 卡与 NFC 模拟前端的连接方法。

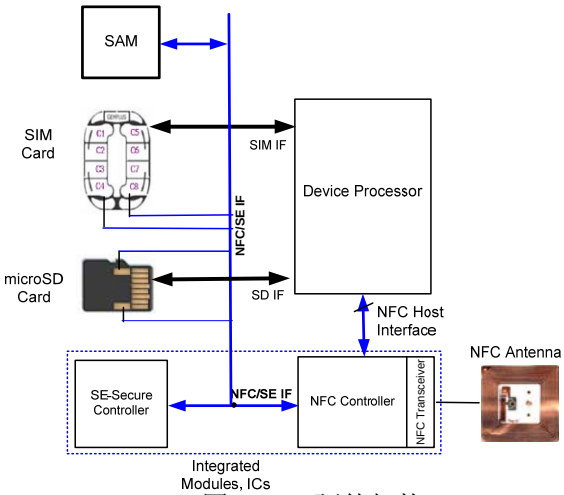


图 1 NFC 硬件架构

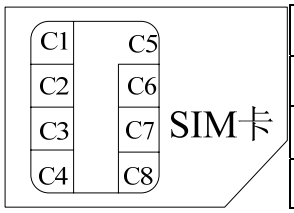
3、SIM 卡与 NFC 连接方式分析

不考虑 SD 等其它接口，一个典型的 NFC 移动

终端将简化为三部分构成：主控芯片（终端的基带芯片或 AP）、安全单元（SIM 卡）与 NFC 模拟前端芯片。

3.1、SIM 卡接口

SIM 卡引脚定义符合 ISO7816 带触点的集成电路卡规范，图 2 是 SIM 卡的引脚定义。



C1	VCC	C5	GND
C2	RST	C6	VPP
C3	CLK	C7	IO
C4	RFU	C8	RFU

图 2 SIM 卡引脚

其中 C1、C2、C3、C5、C7 五个引脚是常规 SIM 卡引脚；C6 作为 VPP（高压编程引脚）已失去作用(SIM 卡可以不必外部提供 VPP 信号即可在内部实现 EEPROM 的擦写功能)；C4、C8 已被国际标准组织扩展为新一代 SIM 卡的高速接口。SIM 卡与 NFC 模拟前端的连接需要在上述 8 个引脚内寻取解决方案。

3.2、C4、C8 接口方案

第一代出现的 NFC 方案基本上采用的是 NXP 的方案，由模拟前端芯片（PN511）与安全芯片（SmartMX）构成 NFC 方案，模拟前端与安全芯片通过 S2C 总线接口连接。因为 SmartMX 安全芯片本身可以作为 IC 卡使用，为了适应移动运营商的要求，可以基于 SmartMX 芯片开发 SIM 卡功能，并利用保留的 C4、C8 两个引脚作为 S2C 接口连线，从而实现 SIM 卡与 NFC 的连接。为了节约 SIM COS 移植的工作量，也有方案是将 SmartMX 芯片与标准 SIM 卡芯片合封在一个 SIM 卡模块中，形成复合卡，尽管物理上 NFC 功能和 SIM 功能是相互独立的，但是达到了由移动运营商同一管理 SIM 卡和 NFC 的目的。

基于 C4、C8 的方案还存在另外一种形式，即直接利用双界面 SIM 卡。双界面 SIM 卡可以实现手机的非接触卡片功能，但不具备 NFC 的读写器功能和点对点通讯功能。

利用 C4、C8 引脚的方案有现成的实现方案，但主要问题是 C4、C8 两个保留引脚已被国际标准组织定义为大容量 SIM 的高速接口，与 SIM 卡的未来发展存在冲突，因此该方案较少被接受。

3.3、C6 接口方案

由上节内容可以得知，采用 C4、C8 引脚的连接方案不被市场所认可，因此需要提出新的解决方案。分析 ISO7816 标准定义的卡片接口，可以看到唯一有潜力可挖的只有 C6 引脚。C6 引脚定义为 VPP，是卡片内部非挥发存储器编程用的高压信号。IC 卡内部使用的非挥发存储器以 EEPROM 为主，也有使用 Flash 存储器的，这类存储器的擦除和写入都需要较高的编程电压，通常在 12V～20V 左右，C6 引脚是被定义作为这个高压引入用的。随着半导体工艺和芯片设计技术的进步，现有的 IC 卡都采用芯片内部自带电荷泵电路，由 VCC 电源泵出非挥发存储器需要的编程高压，所以对于 C6 引脚而言，VPP 的电压已经不再需要由外部加入，VPP 的功能过时了。围绕着 C6 引脚的重新定义使用，产生了一系列的解决方案。

3.3.1、SWP

SWP（Single Wire Protocol）是由 Gemalto 公司提出的基于 C6 引脚的单线连接方案。下图是 SWP 方案连接示意图。

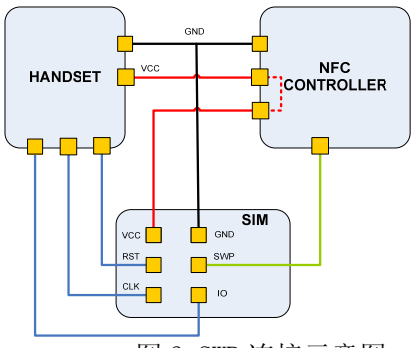


图 3 SWP 连接示意图

在 SWP 方案中，接口界面包括三根线：VCC（C1）、GND（C5）、SWP（C6），其中 SWP 一根信号线上基于电压和负载调制原理实现全双工通讯，这样可以实现 SIM 卡在 ISO7816 界面定义下同时

支持 7816 和 SWP 两个接口，并预留了扩展第三个高速（USB）接口的引脚。支持 SWP 的 SIM 卡必须同时支持 ISO 和 SWP 两个协议栈，需要 SIM 的 COS 是多任务的 OS 系统，并且这两部分需要独立管理的，ISO 界面的 RST 信号不能对 SWP 部分产生影响。

SWP 是在一根单线上实现全双工通讯，定义了 S1 和 S2 两个方向的信号，如图 4 所示。

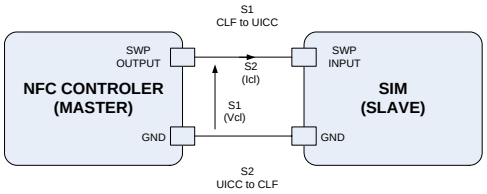


图 4 SWP 的信号定义

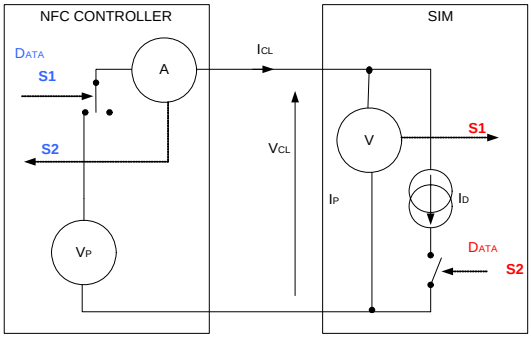


图 5 SWP 接口的等效电路图

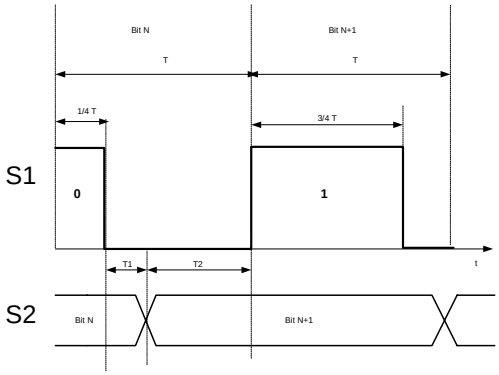


图 6 SWP 信号的编码

S1 是电压调制信号（RZ），S2 是电流调制信号，实际上采用的是负载调制方式，其中 S2 信号必须在 S1 信号为高电平时才有效。图 5 是该接口的等效电路图，图 6 是 SWP 信号的编码。S1 信号是标准的数字电压信号，SIM 卡通过电压表检测 S1 信号的高低变化，同时可以在 S1 信号的编码基础上恢复出时钟信号；S2 信号必须在 S1 信号为高的阶段才有效，NFC controller 芯片通过电流表检测 S2 信号的变化区分“1”、“0”信号。S2 信号和 S1 信号叠加在一起，可以看到在 SWP 线上传输的将是准数字信号，需要特定的接收和解调电路，信号的噪声容限稍低。SWP 传输的波特率可以从 106KBPS 最高上升至 2MBPS。

从 SWP 的定义看，SWP 方案同时满足 ISO7816、NFC 和大容量高速接口，并且是全双工通讯，可以实现较高波特率。SWP 系统地定义了从物理层、链路层到应用层的多层协议，并已经上升成为 ETSI 的标准，正在争取成为 ISO 的标准，目前得到的业界支持较多。从另一个角度看，SWP 方案要求 SIM 卡和 NFC 模拟前端芯片同时重新设计，涉及的面比较广，市场推进的难度较大。另外，NFC 应用非常关注掉电模式下的应用，SWP 的 S2 负载调制通讯方式带来接口的功耗损失，对掉电模式下的性能有不利影响。

3.3.2、CLFI

CLFI（ContactLess Frontend Interface）是由 Sony 公司提出的基于 C6 引脚的另一个方案。相较于 SWP 方案，CLFI 在 C6 引脚上除了传输数据信号和时钟外，还同时传输能量。图 7 是 CLFI 连接示意图，图 8 是 CLFI 信号波形。

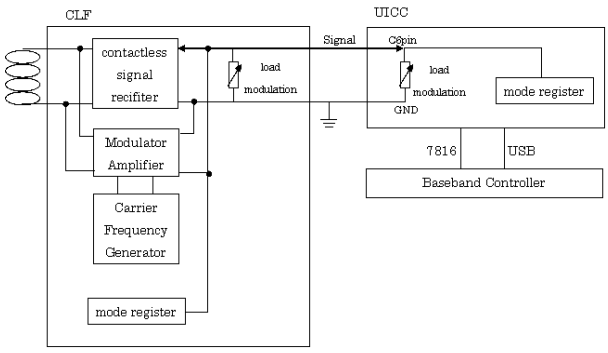


图 7 CLFI 连接示意图

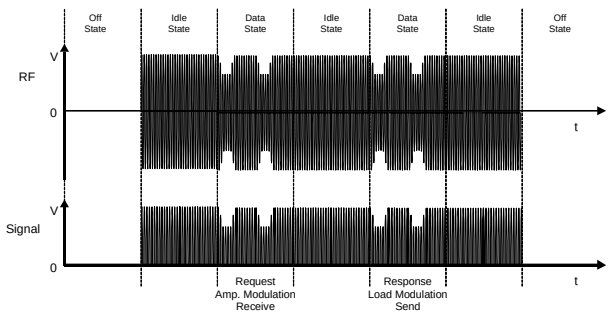


图 8 RF 信号和 CLFI 信号

CLFI 是 Sony 公司基于自有的 Felica 技术衍生出来的，Felica 是一种 13.56MHz 非接触 IC 卡实现技术，典型的应用如香港的“八达通”。和 SWP 不同，CLFI 不需要连接 SIM 卡的 VCC（C1）引脚，而是 SIM 卡直接由 CLFI 信号上提取能量。CLFI 信号是通过幅度调制和负载调制方式传送两个方向的信号，是半双工的通讯方式，但NFC 芯片(CLF)在接收状态下也必须持续提供载波信号以使 SIM 卡获得能量和时钟。

CLFI 方案同样需要 SIM 卡芯片和 NFC 芯片同时重新设计，可以支持该方案的 SIM 卡芯片还未在市场上见到。

3.3.3、MPI

MPI（Multi Protocol Interface）是 Nokia 公司提出的连接方案。MPI 方案同时接管 C6 引脚和 C1、C2、C3、C5、C7 五个常规 SIM 卡引脚，通过定义协议标识 PI（Protocol Identifier）来区分常规的 SIM 卡接口协议（TS 102 221）和非接触协议（ISO14443-4）。C6 引脚被 MPI 定义为非接触应用的时钟信号，数据信号仍然通过 C7 引脚交换。MPI 实现架构有两种，如图 9 所示。

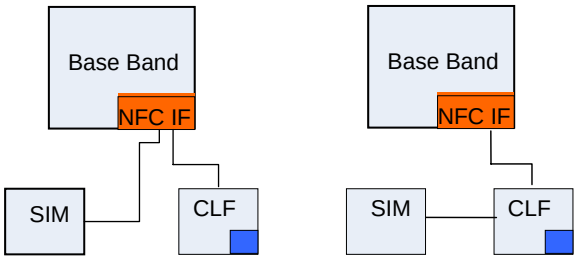


图 9 MPI 实现架构

第一种实现架构，要求手机端进行改造，不支持掉电工作模式；第二种实现架构，由 CLF（非接触模拟前端）接管 SIM 卡接口，可以支持掉电模式。

MPI 方案对 SIM 卡芯片改动要求较低，仅需要 SIM 芯片增加时钟输入端（C6）即可，其它功能都是在软件层解决。MPI 的主要问题是需要修改基带芯片的协议栈来支持新增的 MPI 协议，这除了 SIM 卡、NFC 芯片外，又多牵涉了基带芯片，推广的难度进一步加大。

3.4、Dual IO

从上述的几种业界出现的解决方案看，可以实现 NFC 应用与 SIM 卡的紧密连接，但都要求 SIM 卡、基带和 NFC 芯片几方面同时改动，涉及面较广，市场推广难度变高。综合上述方案的优缺点，本文提出了 Dual IO 方案。

Dual IO 方案将 C6 引脚扩展为 NFC 的数据 IO 接口，则 SIM 卡的 C1、C2、C3、C5、C6、C7 引脚扩展成双 IO 引脚的接口界面，C4、C8 保留作为高速接口升级用。由于 IC 卡的应用都是半双工通讯模式，因此 C6 接口的定义可以设计的和 C7 类同，通讯波特率可以采用 ISO14443 定义的 106KBPS，并可以倍频提高接口速度。这样，SIM 卡通过 C7 接口与基带芯片通讯，协议遵循 ISO7816-4（TS 102 221）；通过 C6 接口与 NFC 模拟前端通讯，协议可参考 ISO7816-4 和 ISO14443-4 自定义，也可以参考 SWP 等其它链路层协议（需要在 NFC 芯片端完成 SWP 等协议向 ISO14443 协议的转换）。Dual IO 接口需要解决的问题是 NFC 应用的时钟如何提供，这需要借用 C3 引脚。Dual IO 连接示意图参见图 10。

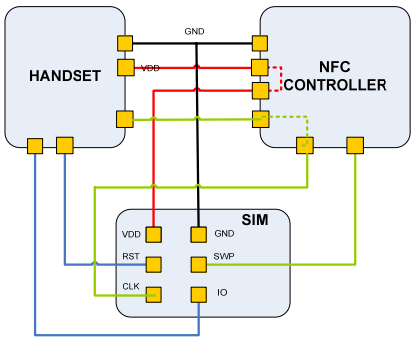


图 10 Dual IO 连接方式

由于 CLK 信号对 SIM 卡而言是单一输入信号，两种模式下相互借用 C3 引脚非常容易实现。在 7816 界面，只要基带发送时钟信号，NFC 芯片就转发基带时钟给 SIM 卡，基带和 NFC 数据的异步

转换由 NFC 芯片完成。当基带芯片处于省电模式停止输出时钟时，由 NFC 芯片提供射频时钟进行非接触应用操作。

采用 Dual IO 方案的优点是实现简洁，只要 SIM 卡内部的 MCU 性能足够，Dual IO 方案可以同时处理 7816 界面和 NFC 界面的数据。而市场上多数 SIM 芯片已具备额外的 IO 引脚，可以省去 SIM 卡芯片的重开发工作，比 SWP SIM 卡芯片更容易获得支持。因为 C6 引脚交换的是纯数字信号，不存在额外的功耗损失，对提高接口速度和掉电工作性能有较大优势。

3.5、Dual 7816 方案

Dual IO 是比较简洁的一种实现方案，但毕竟还是要求寻找具备额外 IO 引脚的 SIM 卡芯片，并不是所有芯片都能支持。因此本文进一步提出 Dual 7816 接口方案，可以在不涉及 C6 引脚的情况下实现 NFC 与 SIM 的接口。

Dual 7816 方案得以成立是基于以下两点：一是手机对 SIM 卡访问的时间短暂，手机在电话的接入和拨出、短信的收和发时，访问 SIM 卡的时间通常在开始的 1 秒至 2 秒左右，绝大部分时间 SIM 卡处于休眠状态;二是 NFC 作为卡片进行非接触交易的时间非常快，通常在几百毫秒以内可以完成。这意味这 SIM 卡可以时分复用 7816 接口。

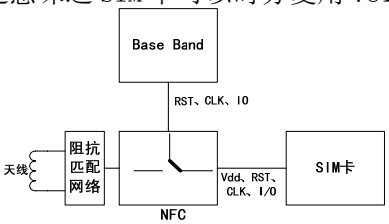


图 11 Dual 7816 方案连接示意图

Dual 7816 方案中 NFC 模拟前端芯片具有两套 7816 接口引脚，内部存在如图 11 所示的接口开关。SIM 卡与基带芯片的连接通过 NFC 芯片实现。正常模式下，NFC 芯片直接连通基带芯片和 SIM 卡，保持基带对 SIM 的访问。当 NFC 手机感应到非接触射频场时，NFC 芯片转换内部开关至 NFC 连接模式，SIM 卡和 NFC 芯片仍旧通过 7816 接口进行非接触通讯，这时通讯的波特率可以提高至 ISO14443 规定的波特率。在 NFC 进行 7816 接口切换时，可能遇到以下几种情况：

1，SIM 处于休眠状态，NFC 立即接管 7816 接口，提供时钟唤醒 SIM 卡开始非接触操作。由于非接触操作时间很短，在进入 NFC 模式后，基带再有访问 SIM 卡的请求时，将由 NFC 芯片直接处理（响应状态查询）或通知基带芯片延迟等待，完成非接触操作后立即切换回正常模式；

2，SIM 处于工作状态。这种状态存在两种情况，一是基带正在对 SIM 卡进行状态查询，二是有电话或者短信操作正在访问 SIM 卡。情况一，状态查询的时间非常短，几十毫秒就完成，非接触操作可以等待该操作完成后再接管接口，不会影响用户体验。情况二下，等待时间通常在 1～2 秒，然后才能进入非接触模式，但在这种情况下，用户需要处理接听电话等操作，通常不会进行非接触交易动作，因此对用户体验的影响也非常小。

Dual 7816 方案尽管在多任务处理性能上比 Dual IO 和 SWP 等方案要弱一些，但带来的好处是 SIM 卡无需硬件改动，仅仅需要开发一款支持 Dual 7816 接口的 NFC 芯片即可。

4、建议方案

以上分析了 NFC 与 SIM 卡连接的各种方案，并提出了 Dual IO 和 Dual 7816 两种方案。NFC 技术还是处于发展中的新技术，市场推广也仅现轮廓。为 NFC 应用推广的顺利，应该采用一种影响最小的方案。因此采用 Dual 7816 接口是最合适的，而 Dual IO 和 SWP 方案可以作为长远发展的备选方案。

5、总结

本文介绍和分析了 NFC 与 SIM 卡连接的多种方案，并提出了两种切实可行的建议方案，对 NFC 应用的推广具有现实的意义。