第 37 卷 第 2 期
Vol.37 No.2

计 算 机 工 程
Computer Engineering

2011 年 1 月
January 2011

• 工程应用技术与实现 •　　文章编号：1000—3428(2011)02—0229—03　　文献标识码：A　　中图分类号：TN929.5

融合 NFC 的 3G 智能卡系统

夏文栋，林 凯

(嘉应学院计算机学院，广东 梅州 514015)

摘 要：针对 NFC 技术和 3G 智能卡技术的可融合性，提出一种多功能 3G 智能卡系统。介绍近场通信的连接和传输及 3G 智能卡，研究两者融合的方法。该系统以 3G 智能卡的 USIM 卡为载体，利用近场通信技术将非接触的应用功能应用在 USIM 卡上，给出融合系统模型和设计方案。分析结果表明，该系统具有较好的融合性。

关键词：近场通信；智能卡；卡的操作系统；第 3 代通信

3G Smart Card System Fused on NFC

XIA Wen-dong, LIN Kai

(Faculty of Computer, Jiaying University, Meizhou 514015, China)

【Abstract】 Aiming at the fusion of Near Field Communication(NFC) technology and 3G smart card technology, this paper proposes smart card system with multi-function. It introduces the link and transmission technology of NFC communication and 3G smart card technology-related contents, further studies the fusion method. Adopting NFC technology and USIM card as a carrier, the system uses contactless application functions in USIM card. According to the the fusion system model and design scheme, analyzing results show that the system has good fusion performance.

【Key words】 Near Field Communication(NFC); smart card; operating system of card; 3G

DOI: 10.3969/j.issn.1000-3428.2011.02.080

1 概述

随着通信技术的高速发展、3G 时代的到来，手机不再局限于语音和短信功能，各国的研究机构和相关企业的研发部正不断开发新的产品。近场通信[1](Near Field Communication, NFC)业务结合了近场通信技术和移动通信技术，实现了电子支付、身份认证、票务、数据交换、防伪、广告等多种功能，是移动通信领域的一种新型业务。近场通信业务改变了用户使用移动电话的方式，使用户的消费行为逐步走向电子化，建立了一种新型的用户消费和业务模式。本文采用 NFC 技术与 3G 智能卡融合的模式，实现集电信通信、非接触等应用的 3G 智能卡系统的开发。介绍近场通信技术及第 3 代移动通信智能卡操作系统的各个重要模块，根据 2 种技术进行融合性的分析，并研究实现具有近场通信技术的 3G 智能卡系统的融合性系统模型。

2 NFC 技术

NFC 由非接触式射频识别(RFID)及互连互通技术整合演变而来，通过在单一芯片上集成感应式读卡器、感应式卡片和点对点通信的功能，利用移动终端实现移动支付、电子票务、门禁、移动身份识别、防伪等应用。NFC 的短距离交互简化了整个认证识别过程，使电子设备之间互相访问更为直接、安全和清楚。通过 NFC 技术，手机、数码相机、电脑、PDA 等多个设备之间可以方便快捷地进行无线连接，从而实现数据交换和服务。

2.1 NFC 中的连接与传输技术

在 NFCIP-1 标准中，连接和传输过程规定了调制机制、编码、传输速率、帧结构、射频接口，同时还有初始化过程、冲突检测和传输协议等规则[2]。

(1)传输帧结构

在 NFC 中存在 3 种传输速度，不同的传输速率具有不同的帧结构。106 Kb/s 的速率下存在以下 3 种帧结构：1)短帧，用于通信的初始化过程，由起始位、7 位指令码和结束位 3 个部分顺序组成；2)标准帧，用于数据的交换，由起始位、字节指令或数据和结束位顺序组成；3)检测帧，用于多个设备同时进行通信的冲突检测。在 212 Kb/s 和 424 Kb/s 的速率下的帧结构相同，则由前同步码、同步码、载荷长度、载荷和校验码顺序组成。

(2)冲突检测

冲突检测是 NFC 设备初始化过程中的重要过程，包括以下 2 种情况：1)冲突避免，即防止干扰其他正在通信的 NFC 设备和同样也工作在此频段的电子设备；2)单设备检测。通过主要检测 NFC 设备识别码或信号时隙的 SDD 算法用于区分和选择发起设备射频场内存在的多个目标设备。

(3)初始化过程

初始化过程如图 1 所示。

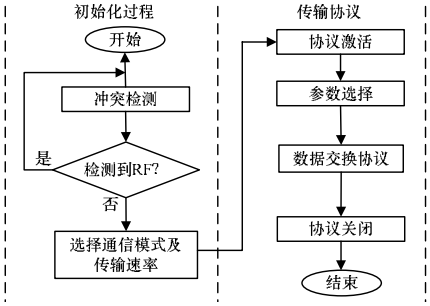

图 1 NFC 初始化过程

基金项目：广东省自然科学基金资助项目(07300421)

作者简介：夏文栋(1973－)，男，讲师、硕士，主研方向：NFC 智能卡，嵌入式系统，片上网络，3G 网络；林 凯，讲师、硕士

收稿日期：2010-06-10　**E-mail：**gdmzxwd@163.com

在初始化过程中，NFC 设备的默认状态均为目标状态[3]。目标设备不产生射频场，保持静默以等待来自于发起者的指令。应用程序能控制设备主动从目标状态转换为发起状态。设备进入发起状态后，开始冲突检测，只有在没有检测到外部射频场时，才激活自身的磁场。在确定通信模式和传输速率后，应用程序开始建立连接传输数据。

(4)传输过程

NFC 传输过程是由 NFCIP-1 标准中制定的传输协议负责数据的传输。在图 1 中，传输协议包含协议激活、数据交换和协议关闭 3 个主要过程：1)协议激活负责发起设备和目标设备间属性请求和参数选择的协商；2)数据交换协议为半双工工作方式，以数据块为单位进行传输，包含错误处理机制；3)数据交换完成后，发起设备执行协议关闭过程，包括撤消选中和释放连接。

NFC 设备在传输有效数据前必须先通过有关协议选定一种通信模式和传输数据速率，在数据传输过程中，选定的通信模式和传输数据速率不能改变。数据传输速率 R 与射频 f_c 之间的关系为：$R=(f_c \cdot D/128)$ Kb/s，其中，D 是一个乘数因子。

2.2 NFC 技术的安全性研究

NFC 技术的安全性研究主要从链接和设备身份验证 2 个方面进行：(1)安全的链接：NFC 的无线加密链接需要一个公钥，而且在带内通道必须是不可见的。链接密钥通过如在蓝牙中手动 PIN 或 Diffie-Hellman 如在无线 USB 中自动交换“实时”生成。建立链接密钥后，便可启用基于 3DES 和 AES 等加密算法的对称加密。(2)设备身份验证：设备身份验证即确保链接密钥以预期的验证设备而不是伪装的被动/主动中间人生成。此设置的一般方法是通过连接一根线缆，以便关联和交换链接密钥，或要求用户在两台设备上输入 PIN 码。将此方法与使用 NFC 来关联和设置相比较，其优点是无需浏览查阅菜单或配置屏幕；只需将 2 台设备彼此靠拢即可触发相关软件和用户界面；建立此环境以后将自动交换相关数据等。

2.3 NFC 技术的应用系统模型

NFC 技术的应用系统采用 NFC 通信技术用作连接通信，把移动支付、电子票务、门禁、移动身份识别等非接触应用作为 NFC 系统功能应用。NFC 非接触应用的操作系统，包括通信传输，文件系统、安全保护、命令模块、硬件结构等。实现系统的模型如图 2 所示。

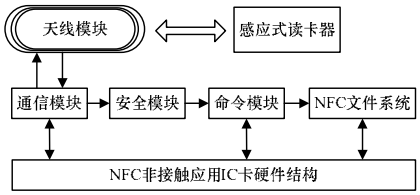

图 2 NFC 非接触应用系统模型

3 3G 智能卡技术

3G 智能卡内的操作系统的主要功能是控制智能卡同外界的信息交换，管理卡内的存储器并在卡内部完成各种命令的执行、管理文件、管理和执行加密算法。在智能卡操作系统中[4]，当智能卡上电时，系统应向终端发送上电复位指令 ATR，同时与终端协商应该使用的通信协议物理特性，完成初始化后，系统等待终端发送命令，系统会分析接收到指令进行相应处理，包括文件的添加删除、数据的更新，安全状态的更新、数据加密/解密等。3G 智能卡应用系统模型以 USIM 卡作为硬件载体的结构如图 3 所示。

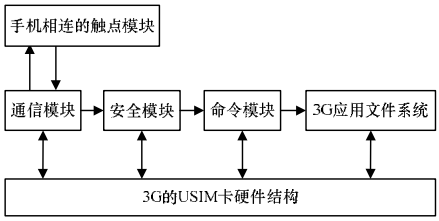

图 3 3G 智能卡应用系统模型

从 3G 智能卡应用系统模型可知，操作系统[5]包括通信模块、安全模块、命令模块、文件系统等部件。通信模块采用 T=0 和 T=1 协议进行通信，以 APDU 命令格式实现数据的传输。安全模块以安全鉴权和加密算法为主体。在 3G 通信系统中，3G 智能卡采用双向鉴权机制，包含网络到卡的鉴权和卡对网络的鉴权[6]。加密算法是为防止破坏 3G 应用和 NFC 应用接收和发送的数据的完整性和机密性，以及卡内保存的重要数据的安全。命令模块以 APDU 命令为结构，不同的命令实现不同的操作功能。文件系统是关于数据单元或卡中记录的有组织的集合，卡的操作系统通过给每种应用建立一个对应文件的方法来实现它对各个应用的存储及管理。

4 NFC 与 3G 智能卡的融合性研究

4.1 NFC 与 3G 智能卡融合性的基础分析

NFC 应用系统和 3G 智能卡的操作系统具有共同的地方，如文件系统、安全保护、通信传输、命令模型。在硬件和软件上有共通的地方，因此具有可以把两者融合在一起的理论基础。考虑到与国际规范兼容问题，NFC 应用与 3G 智能卡通信协议将采用单线协议。单线协议本身是一个全双工的通信协议，使用电压和电流调制在 USIM 卡片及 NFC 硬件组件之间传输数据[7-8]。3G 智能卡(如 USIM 卡)上包含的非接触模块被划分为以下 2 个部分：

(1)NFC 应用组件：NFC 应用硬件与天线一起被设计在 USIM 卡中。主要用来处理射频 RF 协议本身，可将射频信号转换为帧信号从 USIM 卡上的 C6 管脚传送到 USIM 卡中，或将从 USIM 卡同一管脚接收到的帧信号转换为射频信号。

(2)USIM 卡：USIM 卡主要用于存储 Java 应用并处理非接触交易，卡片须支持单线协议并能与 NFC 处理器进行通信。

另外，在共同的文件系统中存储任何与应用发行、电子钱包消费、充值过程相关的密钥、证书，降低被破解风险。

4.2 NFC 与 3G 智能卡技术的融合系统设计

4.2.1 融合系统总体设计

3G 通信业务可通过 USIM 卡、EVDO 卡等具体电信卡实现[9]。本研究以 3G 的 USIM 卡为载体，将 NFC 技术融合进 USIM 卡的操作系统中，设计的系统结构如图 4 所示。

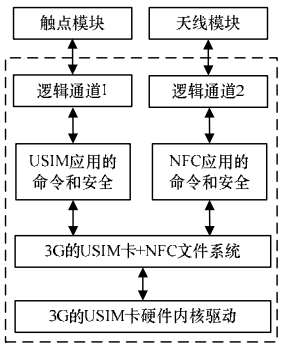

图 4 NFC 和 3G 智能卡融合系统结构

NFC 应用系统和 3G 智能卡操作系统中采用 3G 的 USIM

卡作为硬件平台，接通和 NFC 非接触通信技术用作连接，融合 NFC 应用和 3G 电信应用。

4.2.2 融合系统的硬件设计

在融合系统中，通过文件访问控制和防火墙等安全部件可保证 USIM 卡上交易应用的安全性及交易应用的空中下载，并按 Global Platform 要求实现 USIM 卡的应用管理架构[10]。为保证应用提供商及可信任的第三方能独立开发交易应用和 NFC 非接触应用，USIM 卡应同时支持 Java 卡标准，以保证卡片及应用的互操作性。USIM 卡融合 NFC 应用的硬件架构如图 5 所示。

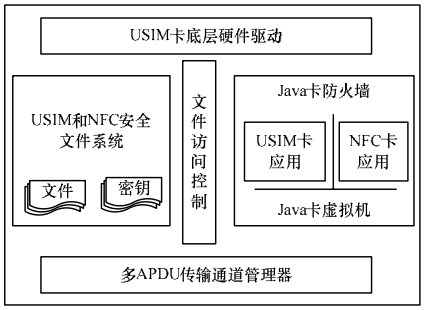

图 5 融合系统的硬件架构

将融合系统应用到 3G 智能卡生产上，通过有关电信测试部门的测试，数据分析结果表明，该系统具有较好的融合性。

5 结束语

NFC 技术和 3G 网络的发展在中国刚刚起步，只有部分地区应用了近场通信业务，相应的各方面的技术在国内很薄弱。今后电信智能卡将会提供更大的存储容量、更高的通信速率、更强的计算能力以及更完善的功能应用。建立近场通信业务能进一步提高用户消费行为的电子化程度，从而成为移动通信行业增值业务新的增长点。因此，需要进一步研究两者的融合性，在交通系统、电子钱包支持等领域推广，为给电信智能卡带来新的发展业务。

参考文献

[1] 许海翔, 伏京生. 近场通信技术拓展电信智能卡应用[J]. 今日电子, 2007, 12(12): 39-42.

[2] 吴思楠, 周世杰, 秦志光. 近场通信技术分析[J]. 电子科技大学学报, 2007, 36(6): 1296-1298.

[3] International Organization for Standardization. ISO/IECl8092-2004 Information Technology-telecommunications and Information Exchange Between Systems — — Near Field Com- munication Interface and Protocol(NFCIP-1)[S]. 2004

[4] International Organization for Standardization. ISO7816-4-2005 Organization, Security and Commands for Interchanges[S]. 2005.

[5] 3GPP. 3GPP TS 102.221-2007 Smart Cards; UICC-Terminal Interface; Physicalandlogical Characteristics[S]. 2007.

[6] 3GPP. 3GPPTS 35.205-2007 3G Security; Specification of the MILENAGE Algorithm[S]. 2007.

[7] NFC Forum. NFC Data Exchange Format(NDEF)[J/OL]. (2006-07-24). http://www.nfc-forum.org/specs/.

[8] NFC Forum. NFC Record Type Definition(RTD)[J/OL]. (2006-07-24). http://www.nfc-forum.org/specs/.

[9] 刘志武, 李代平. 绑定式近场通信 3GCOS 安全性研究[J]. 计算机工程, 2009, 35(23):164-165 .

[10] 许海翔, 伏京生. 近场通信技术促进智能卡应用的前景展望[J]. 金卡工程, 2008, 12(2): 23-25.

编辑 金胡考

(上接第 228 页)

结合本文算法，在三维空间中利用 Hilbert 曲线对图像进行置乱处理，其基本思想是：将图像像素点虚拟到一个三维空间中，即将图像像素点存入到一个空间立方体数组中，按三维 Hilbert 曲线遍历顺序对空间立方体中的像素点进行顺序扫描存储，如图 7(c)所示。

6 结束语

从曲线生成算法和图 7(b)、图 7(c) 2 组置乱的对比结果可以得出，相比二维 Hilbert 曲线图像置乱，三维 Hilbert 曲线图像置乱有如下优点：(1)形状多样化。由于三维曲线基元在空间中的形态呈现多样化，因此可通过不同算法设计，获得不同空间形状的三维曲线，实现灵活运用。(2)像素相关性。三维 Hilbert 曲线运用于图像置乱处理中能够获得相对较低的像素相关性，具有更好的应用性。例如，图像置乱应用于数字水印技术的预处理过程，在对水印预处理时，常通过图像置乱方式降低图像像素点之间的相关性，从而有效提高水印嵌入的不可见性及鲁棒性[7]。(3)空间复杂度。三维 Hilbert 曲线的空间复杂度较二维要高，使其在图像的遍历扫描(即置乱过程)中能够获得置乱度较高的图像，从而更好地保证图像加密的安全性。

参考文献

[1] Li Chenyang, Zhu Hong, Wang Nengchao. Fast *n*-dimensional Hilbert Mapping Algorithm[C]//Proc. of ICCSA'08. Perugia, Italy: [s. n.], 2008.

[2] Zhang Jian, Kamata S. A Pseudo-hilbert Scan for Arbitrarily-sized Cuboid Region[C]//Proc. of IEEE International Symposium on Signal Processing and Information Technology. Vancouver, Canada: [s. n.], 2006.

[3] Zhang Jian, Kamata S. An N-dimensional Pseudo-hulbert Scan Algorithm for an Arbitrarily-sized Hypercuboid[C]//Proc. of the 33rd Annual Conference of the IEEE Industrial Electronics Society. Taipei, China: IEEE Press, 2007.

[4] 徐红波, 郝忠孝. 基于 Hilbert 曲线的近似 k-最近邻查询算法[J]. 计算机工程, 2008, 34(12): 47-49.

[5] 罗传松. 三维 Hilbert 曲线的构造与绘制[J]. 安庆师范学院学报: 自然科学版, 1997, 3(4): 24-27.

[6] 林雪辉, 蔡利栋, 基于 Hilbert 曲线的数字图像置乱方法研究[J]. 中国体视学与图像分析, 2004, 9(4): 224-227.

[7] 罗 斌, 顾 伟, 吕皖丽, 等. 基于主分量分析的矢量量化数字水印算法[J]. 计算机工程, 2010, 36(2): 167-169.

编辑 陆燕菲