国内外主流移动支付技术特性及应用场景研究

赵云辉[1]，张慧琳[2]，佟秋利[2]
（1.北京江南天安科技有限公司，北京100085；
2.清华大学信息化技术中心，北京100084）

摘 要：随着智能终端和移动网络的迅猛发展，移动支付进入了千万人的生活，互联网企业以及第三方支付厂商推出了各式各样的支付方式和支付设备，论文将从安全性、便捷性等方面介绍目前国内外主流的移动支付技术特性及应用场景。

关键词：移动支付技术；近场支付；远程支付
中图分类号：TN409 **文献标识码：**A

Research on the characteristics and application scenarios of domestic and foreign mainstream mobile payment technologies

Zhao Yunhui[1], Zhang Huilin[2], Tong Qiuli[2]
(*1.Beijing JN TASS Technology Co.,Ltd, Beijing 100085;*
2.Information Technology Center, Tsinghua University, Beijing 100084)

Abstract: With the rapid development of intelligent terminals and mobile networks, Mobile payments have entered the lives of millions of people. Internet companies and third-party payment companies have launched a variety of payment methods and payment devices. This article introduces the characteristics and application scenarios of domestic and foreign mainstream mobile payment technologies from the aspects of safety, convenience, etc.

Key words: mobile payment technology; near field communication payment; remote payment

1 引言

随着智能终端和移动网络的迅猛发展，移动支付进入了千万人的生活。移动支付技术的发展过程中，主要关注的是三个方面的问题：一通过智能终端及互联网等途径进行便捷充值、支付业务；二是支付过程中良好的用户体验；三是支付过程中需要针对可能出现的安全风险进行防范。网络支付类业务涵盖内容很多，近几年来，国内外的网络支付业务增长很快，与支付技术、应用模式等相关的领域也倍受关注。

网络支付是指电子交易的当事人，包括消费者、厂商和金融机构，使用安全电子支付手段通过网络进行的货币支付或资金流转，主要包括有电子货币类、电子信用卡类、电子支票类。随着移动互联网的发展，个人智能终端越来越普及，越来越多的网络支付也支持了在智能终端进行相关的支付操作，即移动支付。

网络支付的方式主要有两种：一是网银支付，即通过开通网上银行后，在支付时，跳转到网上银行，输入用户名、密码、支付凭据等后完成支付操作；另一种是快捷支付，即将网上银行账户绑定到第三方支付平台，在支付时由第三方支付平台调用保存的用户凭据与网上银行在后台进行交互完成支付过程，这个过程中用户不进入网上银行，这种支付手段快捷，

可以免密码、免认证介质等，安全性较网银支付差，但用户体验好于网银方式。

移动支付是目前倍受关注的支付手段，技术发展最快，以安全和便捷为目标。移动支付就是使用智能移动终端（通常是手机）进行账务支付的一种方式。移动支付整合了电信运营商、支付服务商（银行、银联、第三方支付等），应用提供商（电商平台、公交、电信等），设备提供商（终端厂商、卡供应商、芯片提供商等），系统集成商，商家和终端用户等主体。移动支付的方式主要有近场支付和远程支付两种：近场支付主要是应用NFC、蓝牙等技术；远程支付主要是短信支付、二维码支付、指纹支付、声波支付等方式。

2 国外主流移动支付技术

在电子支付领域，国外的研究起步比较早，国内很多主流应用的支付技术都来源于国外。

2.1 NFC（Near Field Communication）技术

NFC技术产生于2003年，最初是菲利普公司、诺基亚与索尼公司一起开发的一种无线短距离（10厘米左右）通讯技术，后来经过改良，与非接触智能卡技术结合，最终形成了一种兼容当前 ISO14443 非接触式卡协议的无线通讯技术，取名NFC（Near Field Communication）。

NFC技术最初就是希望应用到移动终端设备，实现非接触卡所不能实现的功能，最吸引用户的是实现了三种模式。

（1）卡仿真模式：将移动终端设备仿真成一张非接触智能卡，结合移动应用，实现更灵活的卡应用方式。

（2）Reader模式：使移动终端设备成为一台能对非接触智能卡进行读写的称动读写器，满足用户随时操作非接触智能卡的需求。

（3）通讯模式：类似于蓝牙通讯，实现两个NFC终端设备近距离交互数据的功能。

NFC技术发布之后，并未引起移动终端厂商的很大兴趣，主要原因是支持NFC功能需要在终端设备内安装NFC芯片、天线等，这需要重新设计产品结构、规划功能，并且还增加了设备成本，终端厂商如手机厂商离智能卡的业务比较远，所以在NFC技术出现的前几年里，支持NFC技术的终端产品少之又少。

转机发生在2006年，智能卡厂商雅思拓与恩智普公司联合开发了SWP（单线）协议。SWP协议是采用终端内的电信SIM卡实现NFC技术中的SE（安全模块）的功能，即通过电信运营商发行的SIM卡上的C6管脚与NFC控制器进行通讯，从而替代单独的NFC安全芯片，节省了NFC模块的成本投入，使终端上的NFC功能与电信运营商建立了关联。对一直想进入移动支付领域的电信运营商来说，这是一个对电信业务有利的支付通道，安全模块能够控制在电信运营商手中。由此，NFC技术开始得到了国内外终端厂商的推崇，国内外开始出现大量具备NFC功能的智能手机，并由此产生了众多移动支付方式，并且支持公交卡应用的NFC手机也大量出现，“刷手机坐地铁、公交”也成为很多城市公交一卡通的宣传口号。

NFC技术借助于电信运营商的支撑并没有为其带来更广阔的发展，反而由于安全模块受限于运营商的SIM卡，而使其在小额支付领域受到很多限制，由此手机生产商和Android厂商开始谋划更好的SE解决方案。早在2006年，法国使用诺基亚手机进行过NFC公交应用的测试。在国内，由于早期NFC手机普及度低，后来受电信运营商的制约，运用NFC技术的应用很少。

2.2 基于Android　HCE架构NFC支付技术

在NFC技术获得了电信运营商支持的同时，也受到了电信运营商的限制。NFC技术所使用的SE（安全模块）是电信运营商发行的SIM卡。这个方案对促进智能手机集成NFC技术起到了很好的促进作用，但也为NFC手机在其他领域拓展应用形成了壁垒。为了打破这个壁垒，占智能手机大半江山的操作系统Android厂商谷歌（Google）在Android 4.4中集成了HCE（Host Card Emulation）架构。

HCE即主机模拟卡片技术，该技术最初是

SimplyTapp公司提出并实现的，HCE架构主要是改变之前NFC手机应用依赖于SIM作为安全模块SE的模式，将传统的NFC实体安全模块SE远程托管到云端SE或本地模拟，这样即使移动设备没有SE模块，也可实现安全的NFC应用，如银行卡、公交卡等应用。

HCE架构的提供对中国市场尤为重要，主要体现在两个方面：一是在国内目前智能手机操作系统应用中，Android占有近70%的市场占有率，国内企业开发基于HCE架构的NFC应用具有广阔的市场空间；二是中国三大电信运营商垄断了中国的电信市场，也间接控制了NFC手机的应用市场，鉴于国内电信运营商一直以较低的市场敏感度，限制了国内APP应用开发商的业务推广和各行业应用NFC手机的进程。因此，HCE架构的推出，使国内众多的应用开发商可以越过电信运营商直接与NFC手机的用户建立联系，促进NFC手机应用的推广。

目前此种方式应用很多，并且Google进一步完善了Android体系，融合生物识别（指纹等）安全技术，为各类应用提供了安全的底层安全的便捷的支付体验。

2.3 标记支付技术

标记支付技术是一种将国外完善的信用卡应用与NFC技术完美的结合起来的应用模式，标记支付技术由苹果公司在其手机产品iPhone 6上于2014年推出，2016年进入中国市场。

标记支付技术是由苹果公司与国际芯片卡标准化组织EMVCo共同研发，并在2014年正式发布的一项新的支付技术，这一技术充分考虑了信用卡交易时的安全保护，核心是设计了一个支付标记（Token），用Token来代替信用卡卡号进行交易，从而避免卡号信息泄露带来的风险。

标记支付的过程：在用户使用NFC手机注册时，先录入生物识别信息（指纹），然后录入信用卡信息，信用卡信息经由TSP（标记代理服务商）提交到EMV组织后，生成一个支付标记，此标记再经由TSP返回到NFC手机的SE中保存。交易时，先验证用户生物信息，验证通过后，自SE中读取支付标记，通过NFC技术将支付标记发送到收款方POS终端，由POS终端发送到TSP，再由TSP发送到EMV组织，由EMV组织将支付标记转换为信用卡号与银行进行支付交易，然后将交易结果返回TSP，最终返回的收款POS终端，完成交易。此交易的整个过程可分为两部分网络环节；一部分是不安全的网络，即容易发生卡号窃取的不可信网络，即扣款POS到EMV组织之前，此过程采用了支付标记（Token）来替代信用卡号，使卡号泄露风险降到最低；另一部分是EMV组织与银行之间，此网络为可信网络，不存在安全风险。

标记支付技术经苹果手机推出，基于苹果手机极佳的用户体验和生物识别与NFC的结合，使标记支付技术实现了既安全又具有极好的易用性。

苹果公司首创了将生物识别技术与支付技术整合，为移动支付领域提供了新的支付安全方式，在国内与多个银行进行了合作，Apple Pay相对广泛地应用到了国内各类商场等支付场景。

继苹果支付技术之后，业务开始学习这种将生物识别技术整合到支付技术中，并在此之后陆续有厂商推出了人脸识别支付、超声波支付、虹膜支付等技术。

3 国内特色移动支付技术

近几年来，随着移动网络的普及，国内移动支付技术不断推陈出新，技术上紧跟国际发展，应用上也多有创新，产品技术、应用模式上的研究也非常深入。

国内的互联网公司极其关注创新支付技术并积极推广，如腾讯、阿里巴巴等都推出基于手机、互联网的支付工具，同时国内第三方支付公司也积极跟进。据统计，2015年中国第三方移动支付市场交易总规模达9.31万亿元，同比增长57.3%；2016年第一季度中国第三方移动支付交易规模达到62011 亿元，同比增速202.6%，环比增速33.4%。

纵观国内支付技术的发展，可以说，很多技术起源于国外，但结合中国国情后又进行了创新，并且在应用方面已经逐步领先于国外。

3.1 SIMPass技术

SIMpass技术出现在2010年前后，是国内的智能卡厂商的技术专利，SIMpass技术在国内也被称为贴片卡技术。

SIMpass技术主要是为了解决没有NFC模块的手机模拟刷卡的功能，实现的原理是借鉴了双界面IC卡的实现方式。

智能IC卡一般分为接触式和非接触式两种界面，接触式就是带有金属触点的IC卡，进行读写操作时，将IC卡插入终端设备内，使IC卡触点与终端内的触点一对一接触，通过这种物理连接实现对IC卡的读写操作；非接触式就是通过天线线圈耦合产生能量使IC芯片工作的一种方式，非接触式在读写操作时不与终端设备发生物理接触，所有通信在空中完成。

SIMpass的实现方式是设计了一款双界面的IC芯片，将其封装成为手机SIM卡形式，将SIM卡上没有定义的触点（C4、C8）定义为非接触天线的接口，同时设计了一款FPC柔性天线，这个天线将SIM卡的触点（C4、C8）连接到FPC柔性天线上，天线的连接线绕过手机电池，放置在手机电池上面，盖上手机后盖后，既实现了通过双界面IC卡模拟NFC手机卡仿真的功能，可以让此手机在刷卡终端上进行刷卡操作。

SIMpass技术出现后，得到了国内众多公交领域企业的支持，很多城市的公交系统也进行了相应的技术和产品测试，也有一些城市测试后批量发行了一些产品，在2014年前后，国内有一定量的用户在使用。

SIMpass技术对于在NFC模块没有成为手机标配模块的情况下，不失为一种很好的移动支付替代方案，但是目前国内使有此技术的设备、城市公交很少，主要原因是SIMpass技术的自身缺陷。

（1）对手机的限制很大，要求手机不能使用金属外壳、后盖可拆卸，但目前国内的手机大部分都使用了不可拆卸的金属后盖。

（2）适配手机型号有限，这种技术对手机的环境要求高，每一款手机要想使用这个技术必须进行测试、适配，可能需要重新定制SIMPass天线，比较复杂。

（3）NFC手机越来越多，目前带有NFC模块的手机型号越来越多，公交客户更愿意对此类手机进行适配。

综上所述，SIMpass的方案是一个比较简便的替代，在NFC手机不成主流之前有一定优势，但智能手机作为时尚的消费类电子产品，更新快，样式多变，这也就注定了SIMpass的局限性。早期有部分城市公交卡采用了这种方式，但受手机限制，应用数量并不太多，应用场景也很受限。

3.2 SD卡支付技术

与SIMpass支付方式的历史时期和产生背景相同，SD卡支付是中国银联主导的一种移动支付方案，目标也是在NFC手机不普及的情况下实现手机模拟刷卡功能。

SD卡支付方案的原理是将安全模块和射频天线集成到SD卡上，SD卡一般是指Micro SD

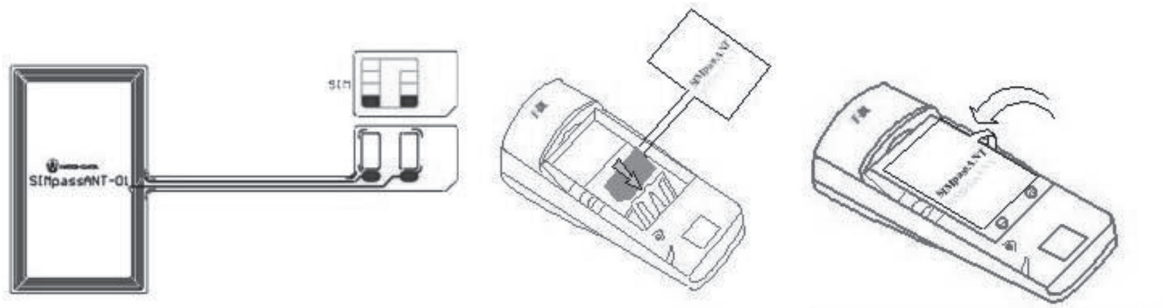

图1 SIMPass示意图

卡，将SD卡置入手机的SD卡插槽，内置在SD上的IC芯片和天线可以在普通刷卡终端上进行刷卡交易，同时手机的操作系统上安装了管理的APP，通过SD卡的物理接口可以对内置在SD卡上的安全模块进行管理。

SD卡支付方案对手机没有进行任何改动，只需要将SD卡置入手机的相应插槽内即可，与SIMPass方案相比，SD卡支付方案更简便。由于SD卡支付方案实际推广方是中国银联，所以国内一些芯片厂商和支付类企业都积极参与了这个方案的推广。

在实际推广过程中，SD卡支付方案遇到了与SIMPass方案同样的问题：一个是刷卡效果不理想，与手机的结构相关，金属后盖的手机刷卡效果尤其不好；另一个问题是智能手机开始不提供SD卡插槽。随着苹果手机的风靡，国内手机厂商纷纷效仿，固定手机内存容量，取消SD卡扩展槽位，金属外壳广泛使用，这也使SD卡支付方案也慢慢被抛弃。

图2 SD卡支付方案示意图

3.3 RF-SIM技术

考虑到手机模拟刷卡的需求以及主流手机终端的结构特性，为了改善刷卡效果，中国移动联合国民技术公司推出了RF-SIM移动支付方案。

RF-SIM的射频基于2.45G超高频，本身具备远距离传输能力，并且由于频点高、波长短，所以也具备了一定的对金属等的穿透能力。RF-SIM的这些能力使其具备了集成到手机内并实现稳定数据传输的能力。

通过对接收设备的调试，将RF-SIM的信号接收距离限制在10厘米左右，把射频芯片、功放、天线等集成到SIM卡中，通过手机为射频进行供电；在外部使用偶极子阵列天线实现与手机内2.45G射频芯片进行通讯，模拟13.56M射频卡短距离信息传输模式，从而实现手机刷卡的功能。

RF-SIM的移动支付方案既回避了NFC手机在中国尚未普及的问题，又实现了电信运营商通过手机端SIM卡实现对移动支付的相对控制权，应该说是电信运营商的一个极佳的移动支付解决方案。事实上，中国移动与中兴下属公司国民技术以及卡商东信和平、恒宝等厂商合作，中国联通、中国电信与厦门盛华电讯合作在国内取得了非常多的应用案例，其中最典型的是校园卡方案，电信运营商通过赠送手机、手机号的方式，使在校学生使用RF-SIM实现校园一卡通。

目前出于对技术安全性的考虑，2014年中国移动支付标准出台后，对RF-SIM要求仅能在封闭环境内使用，不可作为全社会公开的支付方案使用，这对RF-SIM是致命打击。因此，目前这种方案仅存于校园一卡通领域，用于配合电信运营进行校园一卡通类项目建设。

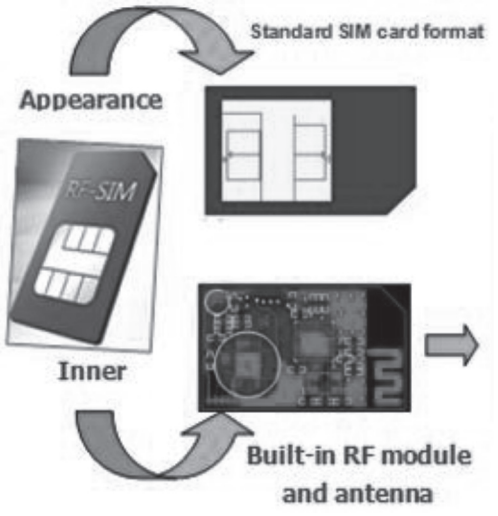

图3 RF-SIM示意图

3.4 二维码支付技术

2013年以来，二维码支付可以说在移动支付领域飞速发展，国内以支付宝、微信支付为

代表，以支付简捷、便利、对移动设备依赖极少等特点见长。

二维码支付可以认为是标记支付技术的国产化。它原理很简单，通过安装在智能手机内的APP，将用户账户以二维码的形式展示，每分钟变化一次；收费终端通过条码识别器描扫二维码获取到用户账户信息，收费终端通过网络向用户账户发起扣费操作。用户账户信息并非是一个真实的银行账号或系统用户账号，而是一个随时间变化的数字，这个数据在服务器端与用户真实账号关联，扣款成功后此数据即在手机上变为新的数字，以保证每次扣款关系的数据不同，以此来保证用户账户安全。我们简单分析可知，这个模式与EMV和苹果公司推崇的“标记支付”很类似，只不过在这个交易过程中没有银行的参与，只发生在扣款方、用户移动设备、用户后台账户之间。

二维码支付因为简单、快捷、不受银行限制等特点在中国倍受第三方支付公司喜爱。另外凭借着极低的交易手续费，二维码支付抢占了原来中国银联POS终端的传统市场，国内大部分的商场、餐厅都支持了二维码收款。二维码支付在国内蓬勃发展的同时，触角伸展到各行各业，如在支付宝进入了校园卡领域，同时也积极寻求进入城市公交支付领域，国内个别城市也在探讨在公交车上使用二维码来进行扣款操作。

事实上，二维码支付与标记支付在安全方面差别很大，二维码自身无法抵御复制拍照等简单窃取操作。中央人民银行曾在2014年3月13日下发了文件叫停二维码支付，但是在国内强势的互联网金融公司的推动下，采用了一些密码技术改善了二维码安全强度，在安全层面有了一定的提升，二维码支付几乎成了目前的支付技术的主流。

目前，二维码支付技术在国内小额支付领域达到了垄断地位，基于国内移动网络的发展，二维码的快捷体验得到了广大用户的接受，国内大到商场购物、公共事业交费等，小到街边小店都实现了二维码的支持。

二维码就是小额支付的终结技术吗？肯定不会是。随着智能终端设备以及AI技术的发展，相信以后还会有更便捷的支付技术出现。

4 结束语

支付技术的先进性和便利性决定了是否能够被用户接纳，支付技术的安全性决定了是否能够广泛的应用。理论上说，安全性与便利性是有一定冲突性的，既安全又便利又适合广泛应用的支付技术较难实现，但是对具备便利性的支付技术辅以安全技术的支撑，那么我们需要的又好用又有保障的支付技术就可以有多种了，而这种安全技术无疑就是密码技术。

参考文献

[1] 余一帆.浅议在线支付的安全与可行性[J].科技信息,2010(26):228-229,231.

[2] 毛颖奇,郁振康. STK卡OTA（空中下载）技术的实现与应用[J].江苏通信技术,2003(06):35-38.

[3] 吕芙蓉,林发全.关注HCE:安全挑战及解决方案[J].金融电子化,2015(05):38-41,7.

[4] 胡芸.在线支付网络安全风险与防范技术研究[J].网络安全技术与应用,2014(04):120-124.

[5] 刘嵩岩,毛志刚,叶以正.智能卡的研究与发展[J].微处理机,2000(02):1-5.

[6] 赵皓.SIMpass/RF-SIM/NFC及其在非接触移动支付中的应用[C].中国通信学会第六届学术年会论文集（中）,2009:5-8.

[7] 郝晓丽.利用WiFi实现支付时应注意的安全问题[J].网络空间安全,2017(Z1):70-72.

[8] 刘莹莹.移动支付安全问题研究[J].网络空间安全,2017,08(08):16-18.

作者简介：

赵云辉（1977-），男，本科，北京江南天安科技有限公司，高级工程师；主要研究方向和关注领域：RFID与信息安全。

张慧琳（1983-），女，硕士，清华大学信息化技术中心，工程师；主要研究方向和关注领域：校园卡建设、财务信息化。

佟秋利（1970-），男，硕士，清华大学信息化技术中心，副研究员；主要研究方向和关注领域：信息系统顶层设计、财务信息化。