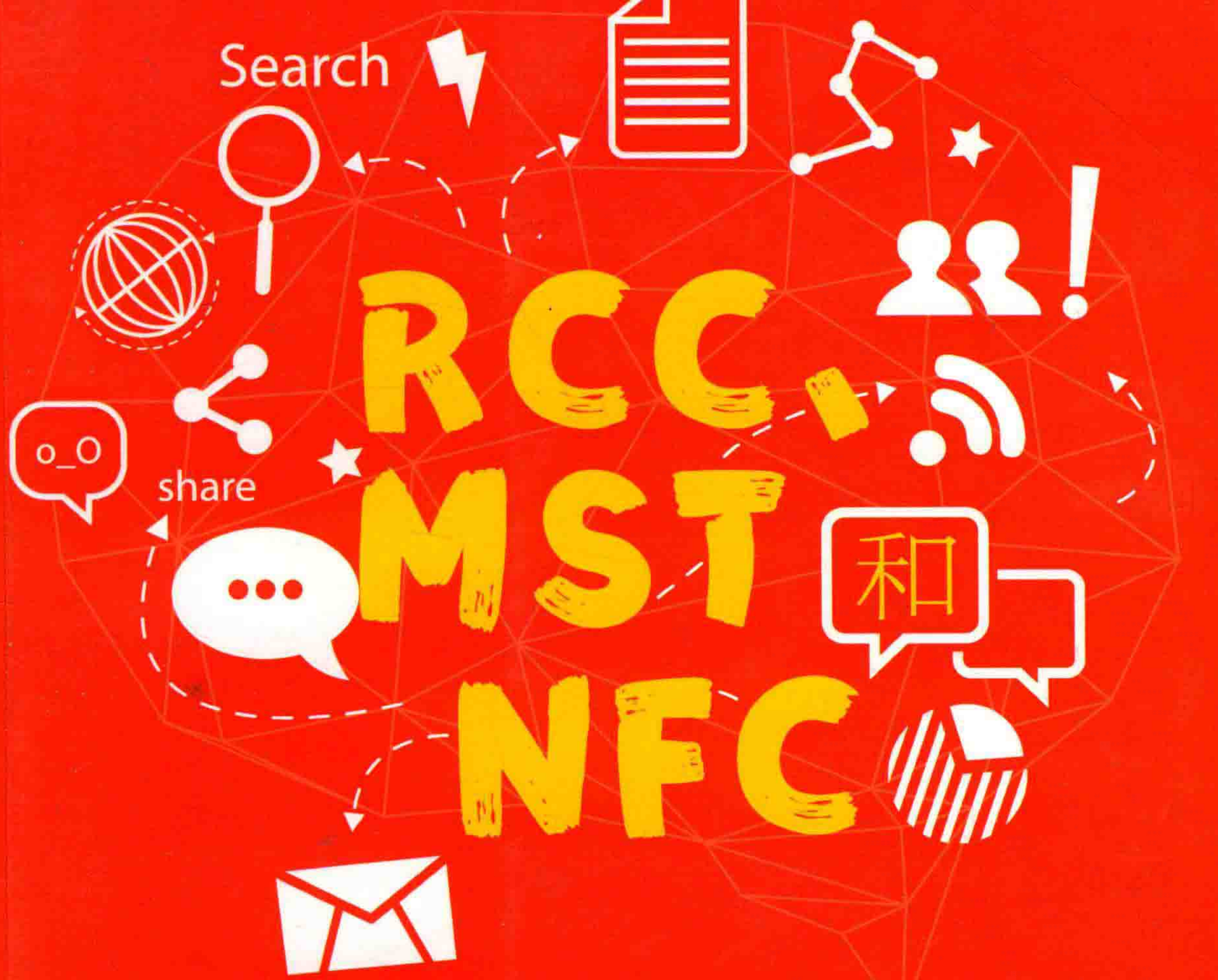

RCC、MST和NFC标准及技术应用

王晓华　编著

- 移动支付技术的“战地手册”
- 雅观科技、恩智浦、小米、蚂蚁金服、腾讯科技移动支付领域专家推荐

北京航空航天大学出版社
BEIHANG UNIVERSITY PRESS

RCC、MST 和 NFC 标准及技术应用

王晓华　编著

北京航空航天大学出版社

内 容 简 介

本书重点介绍基于硬件安全技术的移动支付应用系统，涵盖 NFC 技术细节描述和规划、系统安全及密码学、Android 系统中 NFC 的设计和示例代码、13.56 MHz 的硬件和射频技术等；主要内容包括 RCC 限域通信支付系统、MST 磁安全传输支付系统、基于 Android 系统的 NFC 实现框架。

本书适合 RCC、MST 和 NFC 移动支付开发人员阅读。

图书在版编目(CIP)数据

RCC、MST 和 NFC 标准及技术应用 / 王晓华编著. -- 北京 ：北京航空航天大学出版社，2018.3

ISBN 978-7-5124-2676-4

Ⅰ. ①R… Ⅱ. ①王… Ⅲ. ①移动通信－通信技术－应用－支付方式－中国 Ⅳ. ①F832.2-39

中国版本图书馆 CIP 数据核字(2018)第 048034 号

RCC、MST 和 NFC 标准及技术应用

王晓华　编著

责任编辑　杨　昕

*

北京航空航天大学出版社出版发行

北京市海淀区学院路 37 号(邮编 100191)　http://www.buaapress.com.cn

发行部电话：(010)82317024　传真：(010)82328026

读者信箱：emsbook@buaacm.com.cn　　邮购电话：(010)82316936

涿州市新华印刷有限公司印装　　各地书店经销

*

开本：710×1 000　1/16　印张：16.75　字数：299 千字

2018 年 4 月第 1 版　2018 年 4 月第 1 次印刷　印数：3 000 册

ISBN 978-7-5124-2676-4　定价：49.00 元

前　言

在当今市面上基于硬件安全技术的移动支付应用系统除了 NFC 外，还有一些其他的支付应用方案，例如 RCC 技术和 MST 技术。但是目前介绍 RCC 和 MST 这两项技术的中文书籍较少，业内的朋友曾看过我之前出版的一本关于 NFC 基础入门的书籍，希望我能把与 RCC 和 MST 相关的技术和协议结集成册出版，我没有接受这个建议。

其主要原因有两个：第一，据出版关于 NFC 技术基础方面书籍的经验，要把答应别人的事情做完，其实不那么容易，即使已经有一些写作材料的积累或者在某一项技术、产品方面有大量的工作经验，但当你准备把它做成一本书时，还是需要付出大量的业余时间和精力去查阅和确认相关资料等，另外要想把它做得好一些、质量高一些，那更是一种压力和责任；第二，当初我正开始准备达到自己下一个阶段工作以外的个人学习目标，即以归零的心态系统地学习一些关于 IoT 物联网安全和 AI 人工智能方面的东西，如果答应写书这件事，那么我工作之外的学习重心就可能在一段时间内又会被重新拉回到 RCC、MST 和 NFC 的主题上来，这样就需要我在一个近半年的工作以外的时间里做出一个选择。

以前我特别羡慕那些能同时做两件或者多件重要的事情，而且还能把它们做得很好，并且还能来回灵活切换和平衡得不错的人。可惜我天生鲁钝笨拙，尝试过几次同一时间处理两个线程的事，发现每次得到的结果都差强人意，后来也就慢慢想通了、释怀了，觉得把一件事做得好一点这才是最最重要的！如果还能有其他的收获那就需要感激，没有的话也感觉再正常不过。

最后我答应胡编辑来写这本书，自己做出这个决定还是比较迅速的。因为此刻我感兴趣的两件事的时效性还是有本质区别的，其中一件是关于自己制订的那个学习计划，学习本身就是一个长期的过程，不可能是一蹴而就的事。我喜欢的有一个心理仪式感的学习计划的本质是，提醒自己去主动地远离心理上面的舒适区，不要

在里面停留太久，空闲时间尽可能地学习和补充一些自己知识结构上面的短板，多接触一些有趣的人和事，总结过往的学习和工作经验，进行资料检查和复核，然后把它们汇总到一本书上去，何尝不是一种学习和有意思的体验呢！

我认为的学习就如罗振宇先生主讲的《罗辑思维》节目中每次上来都反复说的那句话“和你一起终生学习”。当下正处在一个各种技术日新月异、急速变化的时代，不可能说离开学校就可以不学习或者就可以减少知识的汲取。

现在连六七十岁的老人都开始接受新知识、新事物，如智能手机、智能电视的使用等，不学习只能与时代和社会脱节。未来的生活环境会越来越好，那么在接下来的几十年里：依赖传统纸质媒介了解国内外大事和新闻的人将越来越少，更多的是通过网络进行阅读；在有些重要时刻虽然无法亲临现场，但可以使用网络通信工具与亲人们实时互动、分享喜悦。

长辈尚且如此，我辈又怎能不去适应和拥抱那种终生学习的心态呢。我认为上学期间的学习，更多的是去掌握一种适合自己且行之有效的学习方法，并且应多学习和掌握一些基础类学科的知识，如文学、数学、物理和艺术等，其中一些知识有助于在生活和工作中能比较高效地学习和掌握新东西；而大部分知识因为需要比较大块的连续时间的学习才有可能修成一点结果，而这些知识一旦进入社会工作后，又因无法挤出大块时间潜心于此，因此除专业人士或者天才外，对于绝大部分人而言，想在这些领域里自学并有所突破真是非常非常的难！ 而工作之后的学习呢，我认为有两部分的含义：其一是当下网络经常提及的“刷新认知边界”，这个词语是一个比较好的概括，直白点说就是有些知识大量地蕴藏在生活中，在自己身边的人身上，在网络上面，这时就需要自己有一种主动学习的能力，主动地把这些金芝麻给挑选出来为己所用；其二就是新型类的东西，特别是偏应用类的技术，例如新型的商用模式、新型的应用型技术等，学习了这些东西对于工作后的人来讲，就会有比较大的优势。

有人说当下正处于刘慈欣先生的科幻小说《三体》里所解释的“技术爆炸”那样的年代。首先，对于这个观点我个人并不完全认同，因为从近些年诺贝尔科技类的获奖名单和获奖理由看，能够有石破天惊的那种发现并不多。但是近些年来人类在应用技术方面却取得了快速发展，从量子计算、生物科技、医疗技术、无人驾驶、

AR、VR、物联网技术到 AI 人工智能等，确实能明显地感觉应用技术的发展速度越来越快，如果从这个应用技术的发展速度角度去解释“技术爆炸”，也确实不为过。

上面提及的这些新型应用技术，量子计算为基于量子力学发展出来的一种应用技术，熟悉《三体》的人都知道里面描述过三体人用来监视地球的“智子”就是靠量子纠缠来运行的。人类从发现半导体技术开始，到当代计算机所遵循的冯·诺依曼架构，现代的信息技术产业如硬件、软件、通信、网络等都是基于这些技术展开的。到目前为止，集成电路芯片的量产制造工艺大多处于 10～14 nm，更小的尺寸工艺如 5～7 nm 正处于研发阶段。尽管科学技术人员还在努力通过各种手段进一步延续晶体管的制造工艺并进一步缩小其尺寸，但是在可预见的未来，将达到控制电子的物理极限。当经典的冯·诺依曼架构无法满足一些超性能架构的计算时，研究新型的计算技术就变得尤为重要，其中量子计算就是当前人类正在攀登的高峰。该技术拥有超强的计算能力，理论数据上显示，拥有 50 个量子比特的量子计算机就能超过当今世界上最先进的超级计算机“天河二号”，拥有 300 个量子比特的量子计算机就能将标准服务器需要数万年才能处理完的复杂问题缩短到几秒钟。

我个人认为的“技术爆炸”只是与基础科学相关，与应用科学本质上是没有关系的，那么是不是我们就可以不重视应用科学呢？这个观点我也是不认同的。应用科学有三个重要的特征：第一，针对实际的问题，目的性明确；第二，与人类实践活动的关系密切；第三，直接体现了人类的需求。可以认为应用科学就是我们现代人类生活的空气和水，这能说不重要吗？

本书主要针对的人群是职业技术高中生、在校大学生、移动支付行业的从业者、有工程背景的读者或者自学爱好者们，此书如其书名，是一本介绍硬件安全技术应用于移动支付的书籍。为了让读者看完后能快速地做一些测试实验，书中也穿插了一些示例代码供读者参考。

本书有关 RCC 限域通信技术领域方面的内容得到了泰尔终端实验室高级工程师朱亮博士的大力支持和帮助；全书的框架设计、NFC 技术细节描述和规划、系统安全和密码学、Android 系统中 NFC 的设计和示例代码、13.56 MHz 的硬件和射频技术及新型互联网移动支付市场方面的内容分别得到了杭州雅观科技的田陌晨先生，恩智浦(中国)管理有限公司的陈奕镇先生、罗煜华先生、杨春燕女士、林国辉博士、

李竟先生、程恒先生、吴剑先生、徐海先生的鼎力帮助，在此向他们表示衷心地感谢。

最后还要感谢给予大力支持的社群以及小伙伴们：北京航空航天大学出版社、恩智浦中国、小米科技、易宝支付、京东商城、华为北研、Rock NFC、IDEN Team、NFC 移动支付行业交流群、NFC Mobile、NFC Wearable、Mobile CBG、Mobile DD、一起走过的日子、一卡通世界、移动支付网以及许多曾经的同事们，可爱可敬的 Lily 小姐、低调的技术大牛姜彦儒先生、极富洞察力和激情的 Wilson 和 Martin 先生及终身学习者榜样申宇博士等。

由于作者水平有限，书中的错误与不妥之处在所难免，恳请广大读者批评指正。

王晓华

2017/12/6

于北京市海淀区牡丹园

目　　录

1 概 述

移动支付技术在全球范围内发展迅速，在中国尤其是以 QR 条码为代表的移动支付应用场景和用户体量更是让人瞠目结舌，人们衣食住行的支付都可以通过一部智能手机来完成，支付场景包括线上与线下。线上支付场景，如在 12306 官网或其他第三方购票平台购买车票时，可以很方便地选择使用支付宝或微信进行应用内支付或扫码支付；线下支付场景，如菜市场、跳蚤市场、夜市小摊、社区小卖部、饭店、宾馆等，现在都支持便捷的手机扫码支付。

上面提到的移动支付技术主要是基于 QR 条码技术。目前这个技术得到大规模的商用主要得益于 3G、4G 网络和智能设备终端的普及，这样就为运维一套闭环的支付体系扫清了底层的技术障碍。对于智能设备终端来讲，只需要支持数据联网以及有基本功能的摄像头和屏幕就可以，并不需要额外的硬件。而对于原先收单的 POS 端硬件系统来讲，只需要增加或者改造一把扫码枪，再简单一点就直接把收单的条码张贴出来，由智能设备终端去对它进行扫描进而完成整个支付流程。这种条码技术的核心以及安全主要放置在后台系统，例如金融支付账户体系、风险控制系统、收单管理系统、清结算网关、绑解卡系统等，都主要放置在后台服务端。可以这样理解，对于前端的条码扫描部分主要完成的是对一个需要进行支付的订单的确认，而鉴权和风险控制管理在扫码部分这里处理的量并不大。

可以看出，现有的基于 QR 条码支付的系统，对终端硬件本身的要求并不高，这从某种意思上预示着两种不同的安全思路：一种是基于底层和硬件技术发展出来的完全被动式的防攻击的设计，它是从底层芯片硬件设计开始做安全防护，到软件安全再到系统安全，这个思路有点类似于“防弹衣”的保护技术，当发现安全隐患或者软硬件系统被攻破时，进行安全升级的主要是通过事后打补丁或再多穿几件“防弹衣”实现的，属于一种完全被动式的安全防守方式；另外一种是以互联网企业为主发展出来的主动防守的风险控制管理方式，通过结合已有的大量用户互联的行为数据，包括支付场景的时间、地点、行为、习惯、逻辑等，当发现有异常支付行为时会主动提升安全等级的验证要求，如果评定为恶性攻击或者支付环境不满足，那么系统

就可以终止这笔交易，这样相当于把风险提前识别出来，达到一个主动防守的功效。

目前，主流市场对于上面两种安全思路的看法：未来它们之间不会是谁代替谁的问题，而是如何把二者融合得更好更紧密的问题，既能把两种安全方式的优势利用起来，又能给消费者带来极致的用户体验，这是未来一个很重要的课题。包括 IoT 物联网的安全，未来海量的设备终端会连接到主干网上，如果这些智能设备不能保证连接是安全的，想象一下当汽车在启动无人驾驶时，控制系统被攻破和被坏人接管了，或者晚上休息后，家中厨房的那些智能设备生火做饭了，城市公交指挥系统如红绿灯和网络摄像头等完全失去了控制，那后果是相当可怕的。还有一个就是现在发展得如火如荼的区块链技术，这个技术从本质上讲就属于上面提到的第二种主动防守技术，它是这类技术的代表，假如这个技术应用在当下的移动支付场景中，就相当于对每一次的交易数据节点都会做周边节点的安全确认，只有当别的节点也能证明这笔交易是安全可信的时，此次交易才会发生。例如，张三突然发起一笔面对面 QR 扫码，支付购车款项到李四那边，那么当系统认为这笔款项属于额度较大的款项，且对此笔交易的时间、地点和用户行为有疑虑时，会开启例如手机短信验证码或人脸识别确认，待短信验证码通过或人脸识别没有问题后，后台系统才会对李四是否真实拥有这辆车的相关节点的数据进行确认，当发现多于 3 个节点的数据都无法证明李四拥有这笔财产时，会标识这笔交易风险等级较高，如需要延时 24 小时或 48 小时后才能进行款项交接，这样就可以给张三足够的时间去检查和确认这笔交易。

综合上面说到的 IoT 物理网和基于区块链技术支付的例子，其涉及两个问题：第一，对于这种海量的智能设备连接到网络后，如果全部的安全由云端来保护，不管对于技术实现还是负荷来讲都是天方夜谭，想象一下如果智能设备端没有安全保护措施，那攻击方是完全可以轻易仿照出伪终端来欺骗服务端并且发起对云端的攻击的，所以在设备终端重点采用“防弹衣”式的被动防守模式，可以确保需要接入的设备终端是安全可信的，不能被仿制的；第二，即使使用了类似区块链的技术，核心问题还是如何保证遍历的周边节点的数据是安全可靠的，前提是不仅需要所有的数据已经备份到了云端，而且是数据在备份上传时是安全可靠的，这样就必须结合终端的“防弹衣”式的被动安全防守，再加上云端大数据处理后的主动安全防卫。

本书重点描述的是基于硬件安全技术的移动支付应用系统，对于云端主动安全防卫的技术不做过多介绍。那么在现有的基于硬件安全方式的应用系统主要是以

NFC 技术结合 SE 安全单元为主的，例如目前苹果公司的 Apple Pay、华为公司的 Huawei Pay 和小米公司的 Mi Pay 都是以 NFC 技术为主，可以支持手机银行卡或者城市公交卡等业务，另外三星公司的 Samsung Pay 底层技术既包含 NFC 技术也包含 MST。本书重点介绍的是 NFC 结合 SE 安全单元的应用技术，虽然 MST 技术也可以理解成是一种基于硬件的支付应用系统，但是 MST 主要还是一项传输技术，本身对于硬件安全并没有过多的涉及，单独拉出来看这项技术，它和 NFC 传输技术比较像，都是一个在支付场景中实现的一个数据传输功能，本身并不会涉及过多的安全。

在国内以国民技术公司为主推广的 2.45 GHz RCC 技术，从技术创新层面来讲可圈可点的地方确实很多，特别是在终端支付设备上用户无需更换或者改造手机，只需要更换一张 SIM 卡就可以，非接触的射频前端、天线以及原来的 SIM 卡的电信功能全部集成在一张 SIM 卡上，天线就内嵌在 SIM 卡上。RCC 技术最大的优势在于基于 2.45 GHz 的通信频率还能控制通信和交易的距离，无需特别硬件的手机，只要支持 SIM 卡接口的智能设备就可以；最大的缺点就是，需要去改造或者增加已经在市面上运营的 13.56 MHz 的 POS 机或者闸机读头以实现对 RCC 的支持，另外就是 RCC 技术整个供应链上的厂家没有支持 13.56 MHz 的 NFC 的公司多，所以要去推动重新改造一番底层的基础支付设备终端确实非常有挑战性。综上也就解释了为什么国内外现在主流的银行或者公交的非接触支付系统使用 13.56 MHz 频率更多的原因，其他的非接触频段支付主要应用在一些相对闭环的场景。

相较于以扫码为代表的互联网移动支付技术，以 NFC 和 RCC 为代表的近场支付技术具有多项优势：第一，如上面介绍过的，除去服务器端提供风险安全控制外，支付终端采用硬件安全机制，支付环境的安全优势比条码支付的要显著许多；第二，可以支持离线支付，例如在无网络或者网络信号差的地铁里，支付场景不受网络环境影响，可以真正实现全场景的支付覆盖；第三，对于一些要求高稳定、高频次、高密度的支付场景，例如公交车的振动、上下班地铁公交系统的高人次通行、高亮度阳光对屏幕的反射等问题，对于扫码支付来讲就会是比较大的问题，而对于射频非接触的支付方式就不会有类似的问题。

NFC 技术是从 13.56 MHz 的 RFID 基础上发展起来的一项技术，从单独的 NFC 技术本身来讲已经发展了十几年，所以在成熟的商业应用方面对比其他的射频段或者非接触技术（例如 RCC 技术）就会有很大的继承关系的优势，例如在公交领

域、芯片银行卡应用和一些行业应用方面，它们大部分都使用 13.56 MHz 这个通信频段，而且在数据通信链路协议上面，NFC 技术采用了与 ISO/IEC 7816 接触技术相同的应用数据协议。这样对于支付系统来讲，POS 机或者读头可以不需要改动，重点改造智能支付终端就可以，例如在智能手机中需要加入 NFC 和 SE 的硬件模块，如果希望 NFC 支持 READER 和 P2P 的功能则需要集成 NFC 协议栈来支持。

从 2002 年 3 月 25 日索尼公司与荷兰飞利浦公司(后来独立拆分出半导体业务成立了恩智浦半导体公司)共同宣布了一个 NFC 的粗略技术框架开始，再到后来加入的诺基亚公司，经过多方长时间的磨合，包括协商出来 P2P 点对点传输技术，在底层射频通信层面同时适配支持了恩智浦半导体为主导的 Type A 技术和索尼公司主导的 Type F 技术，并且在诺基亚功能机时代就尝试加入 NFC 的支付应用，但是 NFC 技术一直处于不温不火的境况。直到 2010 年 Google 公司发布了 Nexus S 并且把 NFC 的协议栈开源出来，相当于把 NFC 正式拉上了高速列车，这个时候 NFC 技术才在运营商、银行、公交公司得到了蓬勃发展。但是多方商业机构因为支付的主导权问题，大家又进入了一个群雄争霸的时代，SE 安全模块是选择放置在 SIM 卡里，由运营商来主导；还是 SE 安全模块放置在扩展 SWP 接口的 SD 卡上，由银行机构来管理；还是 SE 内嵌在手机电路板中，由 OEM 厂家来主导。不过庆幸的是争执的这几年技术本身并没有停滞下来，全球范围内以中国的三大运营商为主力军，在持续不断地给 NFC 产业输入血液，运营商主导的 SIM 卡方案并没有取得消费者的完全认可。

再接下来就是 2016 年，当 Apple Pay 在中国市场上推出时确实形成了不小的化学效应，其分别推出了线下非接触支付和集成在应用程序端或网页端的支付应用。前者使用的场景为可以通过网络新发的一张卡或者绑定一张银行卡到手机里，然后把手机靠近 POS 机就可以完成支付；后者则可以在第三方开发的应用程序或者网站上面集成 Apple Pay 提供的 SDK 套件，这样就可以通过手机硬件上面提供的 SE 安全单元里的支付程序完成支付。这些功能在苹果公司最新的官方产品定义中把它们分别叫做 Pay in Stores、Pay within Apps 和 Pay within Websites，后两者其实就相当于把线上和线下打通了，在线上选购完商品后，通过线下手机内置的 SE 安全模块提供的安全支付通道支付。对比上面刚讲的 QR 条码支付体系几乎完全依靠云端保证安全，如能把这种已经内嵌 SE 安全模块的功能结合使用，那么会有一个很大的安全提升和用户体验提升。

除去上面介绍的一些近距离通信技术以外，平时生活中接触得比较多的无线电连接技术有用途广泛的移动电话、Wi-Fi 和音响等，在把通信的距离缩小到半径 200 m 左右及通信支持上下行技术的情况下，我们能看到下面将要介绍的这些已有的技术。但是当下使用这些技术进行支付或者移动支付的应用并没有或者准确来说并不是行业主流，毕竟技术设计的方向不尽相同，所以本书也不会过多地介绍下面几种技术的细节。

蓝牙无线技术：当初设计这个技术的时候就是为了代替两台手机或电脑之间传送数据时使用的线缆，现在它们之间的理论通信距离半径为 10 m 左右，目前广泛应用于蓝牙耳机、音响以及车载电子设备。

Wi-Fi 技术：在一个相对比较固定的环境下使用这个技术能大大降低室内布线的复杂度，例如在宾馆、家庭、办公室等这个技术随处可见。这个技术设计的初心是为了能更好地优化局域网络(LAN)，在一个相对没有金属障碍的环境里使通信距离能到达半径 100 m 或更远。

ZigBee 无线技术：主要应用于组网规模相对较大的一些工业自动化领域，这个技术的通信范围在半径 100 m 内，目前广泛应用于餐馆使用的手持订单终端。

红外无线技术(IrDA)：是一个短程小于 1 m 的通过红外线进行数据交换的技术，红外线接口经常用于电脑、手机和数码产品之间。

无线射频识别(RFID)：此技术本身的定义比较宽泛，有高低频之分，以及有源和无源通信之分。其工作原理为通过读头可以发起对外部的无线识别标签进行远程存储和检索数据。

非接触技术：一般大家说的这个技术都是约定俗成的泛指 ISO 14443 和日本的 FeliCa 技术。这个技术其实也是属于 RFID 中的一种，主机读头为有源工作，而卡片则是无源的。在工作时读头发起射频场强并且附加通信数据给卡片，卡片在收到无线射频场强时会把这个能量转换成工作电压供自己启动和工作，并且能快速处理发送过来的数据信息进行响应和处理。

NFC 与其他短距离通信协议的比较如表 1-1 所列。

综上所述，本书基于硬件安全技术的移动支付应用系统会把重点放在 MST、2.45 GHz RCC 和 NFC 技术基于 Android 系统的应用方案介绍。

表 1-1　NFC 与其他短距离通信协议的比较

通信参数	NFC	Bluetooth	Bluetooth Low Energy	RFID	IrDA
无线射频兼容	ISO 18000-3	主动模式	主动模式	ISO 18000-3	主动模式
参考标准	ISO/IEC ECMA ETSI NFC Forum	Bluetooth SIG	Bluetooth SIG	ISO/IEC	ISO
网络协议	ISO 13157 etc.	IEEE 802.15.1	IEEE 802.15.1	ISO 13157 etc.	
网络类型	P2P	WPAN	WPAN	P2P	P2P
密码技术	无	有	有	无	无
通信距离	约 10 cm	约 10 m(class 2)	约 100 m	约 10 cm	约 1 m
通信频率	13.56 MHz	2.4～2.5 GHz	2.4～2.5 GHz	13.56 MHz	3.8 MHz
通信速率	424 kbit/s	2.1 Mbit/s	约 1.0 Mbit/s	424 kbit/s	115 200 kbit/s (SIR)
准备时间	<0.1 s	<6 s	<0.006 s	<0.1 s	< 0.5 s
功耗	<15 mA(读/写)		<15 mA 接收/发送	约 250 mA	约 300 mA
易用性	方便、快捷	一般	一般	快捷	方便
交互性	高效、安全	要求配对	要求配对	高效	无障碍
应用场景	支付、门禁、名片分享、配对	大数据交换	大数据交换	物流追踪	控制与数据交换

2 术语和缩略语

本书中将会出现一些专业术语等，其中大量的是以英文字母缩写为主的。本章主要介绍书中出现或者使用的符号、术语和缩略语，阅读本章有助于读者对术语的形成有一个大概的了解，以方便阅读本书。

2.1 硬件部分

硬件类术语和缩略语如表 2-1 所列。

表 2-1 硬件类术语和缩略语

标 识	出处和解释
RFID	Radio Frequency Identification，无线射频识别技术
NFC	Near Field Communication，近场通信技术
RCC	Range Controlled Communication，限域通信
SE	Secure Element，安全单元
eSE	embedded Secure Element，嵌入式安全单元
CLF	Contact Less Front - end，射频前端
CLT	Contact Less Tunnel，接触通道
SiP	System in Package，系统级封装
SMT	Surface - Mount Technology，表面贴装技术
BB	BaseBand，基带
AP	Application Processor，应用处理器
IoT	Internel of Things，物联网
AI	Artificial Intelligence，人工智能
VR	Virtual Reality，虚拟现实
AR	Augmented Reality，增强现实
PCB	Printed Circuit Board，印刷电路板
PCBA	Printed Circuit Board Assembly，印刷电路板组件

续表 2-1

标　识	出处和解释
ECO	Engineering Change Orde，工程更改号
I^2C	Inter-Integrated Circuit，I^2C 总线
ACK	Acknowledgment，应答响应
UART	Universal Asynchronous Receiver Transmitter，通用异步收发传输器
SPI	Serial Peripheral Interface，串行外设接口
SIM	Subscriber Identification Module，用户身份识别卡
UICC	Universal Integrated Circuit Card，通用集成电路卡片
SWP	Single Wire Protocol，单线协议
SWIO	Single Wire protocol Input/Output (aka SWP)，单线协议包括信号进和出
CICC	Close-Coupled Integrated Circuit Card，密耦合卡片
CCD	Close-Coupled Device，密耦合读头
PICC	Proximity Integrated Circuit Card，近耦合卡片
PCD	Proximity Coupling Device，近耦合读头
VICC	Vicinity Integrated Circuit Cards，疏耦合卡片
VCD	Vicinity Coupling Device，疏耦合读头
UID	Unique Identifier，唯一标识号码
POS	Point of Sale，销售终端
MC	Magnetic Channel，磁通道
RC	RF Channel，射频通道
DME	Differential Manchester Encoding，差分曼彻斯特编码
ISM	Industrial Scientific Medical，工业、科学和医用频段
MST	Magnetic Secure Transmission，磁安全传输

2.2　软件部分

软件类术语和缩略语如表 2-2 所列。

表 2-2　软件类术语和缩略语

标　识	出处和解释
SDK	Software Development Kit，软件开发工具包