|  |  |  |
| --- | --- | --- |
| **广东财经大学** |  | **2017-JX16-** |
|  |

**

**本科毕业设计（论文）**

二维码支付模式与安全性研究

|  |  |
| --- | --- |
| **院 （系）** | 信息学院 |
| **专 业** | 信息管理与信息系统 |
| **班 级** | 2013信息管理与信息系统2班 |
| **学 号** | 13251101220 |
| **学生姓名** | 林烁 |
| **指导教师** | 张婧炜 |
| **提交日期** | 2017年 3 月 30 日 |

**毕业论文(设计)成绩评定表**

|  |
| --- |
| **毕业论文（设计）指导教师评语及成绩**  **成绩 指导教师签名**    **年 月 日** |
| **毕业论文（设计）复评教师评语及成绩**  **成绩 复评教师签名**  **年 月 日** |
| **毕业论文（设计）答辩评语及成绩**  **成绩 答辩委员会主席签名**  **年 月** |
| **毕业论文（设计）总成绩（五级记分制） 学院负责人签名**    **年 月 日** |

**TITLE:Research on two-dimensional code pament and its security**

**MAJOR: Information Management and Information System**

**APPLICANT: Lin Shuo**

**SUPERVISOR: Zhang Jingwei**

# **摘要**

随着互联网的快速发展和4G网络的普及，移动支付成为了一种广泛使用且高效的支付手段。二维码支付是移动支付的主要方式之一，具有信息存储量高、操作简便、服务拓展等特点。从而，二维码支付被广泛应用在线上和线下支付，交易金额持续上升。但由于二维码支付平台技术尚未成熟、流程不合理以及用户的信息安全意识不强，因此使用二维码支付仍存在着安全隐患，其中需要重点解决的问题是身份验证和信息可靠性两个方面。本文详细分析了二维码支付可能存在的风险性及其原因，学习了从多重身份验证、第三方认证和混合加密算法三种对二维码信息的处理方式，来进一步提高安全性。

关键词： 二维码 移动支付 安全性 混合加密

Abstract

With the rapid development of the Internet and the popularity of 4G networks, mobile payment has become a popular and efficient method. Two-dimensional code payment is one of the popular ways and has become the accelerator of business which has characteristics of vast storage capacity,easy to operate and provide value-added services. In recent years, the two-dimensional code payment has been widely used in online and offline payments with a continuously rising transaction amount. But the technology of

two-dimensional code payment platform is not yet mature, unreasonable processes and the shortage of protecting our personal information become typical threats.Thus the key issues that needed to be solved are authentication and information reliability. In order to improve the payment security, the paper studies the authentication and taking third-party certification and hybrid encryption algorithm to improve the security.

**Key words：** two-dimensional code mobile payment security hybrid

encryption algorithm

**目 录**

**1绪论**  …………………………………………………………………… 1

1.1研究背景和意义 ……………………………………………………… 1

1.2国内外的发展现状和方向 …………………………………………… 2

1.2.1二维码支付国外发展现状 ………………………………………… 2

1.2.2二维码支付国内发展现状 ………………………………………… 2

1.3论文研究的主要内容 ……………………………………………… 3

1.4论文的组织结构 ……………………………………………………… 4

**2二维码支付技术应用现状** …………………………………………… 5

2.1二维码支付技术原理…………………………………………………… 5

2.1.1什么是二维码技术 ………………………………………………… 5

2.1.2二维码技术的编码与解码 ………………………………………… 5

2.2二维码在移动支付中具体应用 ……………………………………… 6

2.2.1二维码支付的优势 ………………………………………………… 6

2.2.2二维码支付分类 ……………………………………………… 6

2.3二维码支付参与要素分析 ………………………………………… 7

2.3.1当前二维码支付系统架构 ………………………………………… 7

2.3.2二维码支付相关设备 …………………………………………………8

3、二维码支付技术安全风险性分析 …………………………………… 9

3.1二维码支付模式下相关风险分析 ………………………………… 9

3.1.1从支付流程分析存在风险性分析 ………………………………… 9

3.1.2二维码刷卡模式下存在的风险 …………………………………… 9

3.1.3二维码支付用户身份验证存在风险 ……………………………… 10

3.1.4用户成为非授权交易风险主要承担者 …………………………… 10

3.2从技术角度分析二维码支付的安全问题 …………………………… 11

3.3二维码支付安全总体目标 …………………………………………… 11

3.4二维码支付待解决的两大问题 ……………………………………… 12

**4、对二维码支付安全改进方案设计** …………………………………… 13

4.1多层身份验证提升安全性 …………………………………………… 13

4.2第三方认证 …………………………………………………………… 14

4.3特殊加密算法：混合加密提升二维码支付安全性 ………………… 15

4.3.1非对称算RSA………………………………………………………… 15

4.3.2 RSA算法和DES算法比较 ………………………………………… 16

4.3.3混合算法的加密解密过程 ………………………………………… 17

**5、混合加密算法与RSA、DES算法性能比较** ………………………… 18

5.1混合算法与DES、RSA时间性能比较 ……………………………… 18

5.2混合算法与DES、RSA安全性能比较 ……………………………… 19

5.3混合算法与DES、RSA密钥管理上的比较 ………………………… 19

5.4混合算法与DES、RSA应用比较 …………………………………… 20

**注释** ……………………………………………………………………… 21

**参考文献** ………………………………………………………………… 21

**致谢** ……………………………………………………………………… 22

**1绪论**

1.1研究背景和意义

互联网金融与移动支付技术的不断革新，移动支付走进了千家万户。数据时代的快速发展，同样要求支付行业革新与加速。近年来，移动支付呈现出爆发式增长，随着O2O模式带来的强劲需求和生物科技身份识别领域的进步，移动支付用户和支付规模持续攀升。图1-1为我国2013-2016年度中国移动支付业务交易量[[1]](#footnote-0)。

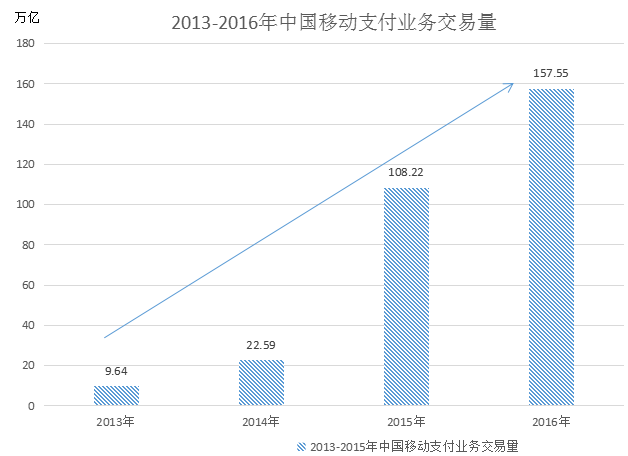
图1-1 2013-2016年中国移动支付业务交易量

Figure 1-1 Business volume of China Mobile payment from 2013 to 2016

作为四大主流移动支付技术之一的二维码支付普及度高，支付快速便捷且发展迅猛。2010年支付宝最先推出二维码支付，将线上延展到线下，淘宝购物场景贴近生活，故升级后被迅速推广，二维码的商业应用持续成为热点。2014年3月央行下发紧急文件暂停多家条码支付服务，其中针对社会隐患即是信息与资金安全问题。2016年，央行再次为二维码支付放行并于同年出台相关行业规范政策和行业标准。这一放一行，一方面肯定了二维码作为商业应用与信息传递的意义，可为社会创造无穷的价值。另一方面，从技术与安全的角度来看，证明其的确存在着风险与挑战，例如因扫码导致信息和账户资金被盗。

因此，本文着重从文献综述的角度研究当前国内支付现状与支付风险的分析与控制，从交易中的支付场景、流程、指令验证方式缺陷入手分析可能出现的潜在风险，通过研究如何改进流程与技术，提出一些有效的改良方案并进行对比分析。

1.2国内外的发展现状和方向

1.2.1二维码支付国外发展现状

纵观亚洲，移动支付市场增长速度最快、份额最高。日本与韩国发展最好且拥有先进的条码技术，虽然支付宝和微信支付已走进世界前沿，进驻日本、韩国、泰国、香港等国家和地区，日本最大的出租车公司也采用二维码支付业务。但实际上，二维码支付中的QR码技术源于日本并为其所垄断。上世纪90年代，日韩均开始将二维码应用到信息识别上。近年来，日韩的移动支付发展迅速，其中得益于移动运营商为用户使用移动支付提供良好的用户体验，虽然日本在各个领域技术领先，但是其政策或支付习惯使用，日本的感应式支付业务使用范围更广（如NFC支付）。

欧美国家移动支付普及率并不均衡，英国的移动支付使用率较高，而美国移动支付普及率较低、动力不足，主要原因在于其信用卡消费的使用习惯仍占主导，随着中国移动支付普及，中美两国的移动支付规模差距持续扩大[[2]](#footnote-1)。所以二维码支付的潜力较大，一旦移动支付流行起来，那么支付市场的竞争将会加大。可见，一个国家技术创新、通信运营商、金融体系、政策引导、使用习惯的发展，都会对该国支付方式产生关键影响。

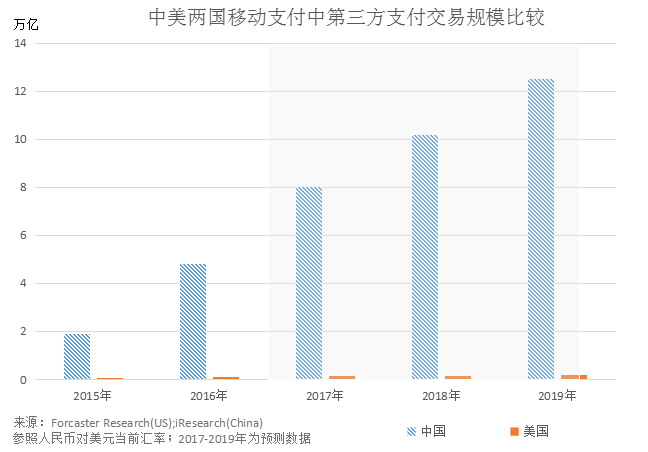


图1-2中美两国移动支付中第三方支付交易规模比较

Figure 1-2 Comparison of third party payment transaction inmobile payment between China and the United States

1.2.2二维码支付国内发展现状

随着国内外互联网发展态势增长，电子商务和智能手机的快速增长，国家“十三五”规划继续推进信息市场发展，让用户享受信息生活，移动支付如预期迎来了爆发式的增长。这一增长，是建立在政策支持、互联网平台技术创新、用户支付热情上。二维码是连接线上和线下的工具，它可以存储商品信息和支付信息。二维码支付实现了用户所绑定的银行卡账户支付集成，用户只需进行手机扫码及密码验证，第三方平台就能扣除用户的账户资金，而商家也能在支付平台进行支付结算。二维码的使用场景多样，应用广，如扫码关注品牌信息、关注服务账号，使用电子会员卡，同步积分等，二维码购物。近年来，以支付宝和微信支付为主的钱包类产品因为费率低、使用方便收到了商家和用户的欢迎。

支付宝和微信支付市场战略：培养用户粘性、开放平台、维持低门槛。最初，转账和提现均不需要手续费。支付宝还推出高回报率的理财产品宝吸引用户投资理财，余额宝中的零钱与账户零钱同步，可以用于二维码支付或在线购物。微信目标是目标是连接一切，利用通讯这一生活场景微信变成一个入口，它可以支持用户与商家、用户与用户之间产生一系列的联系，这样以微信红包、微信转账、扫码支付为核心微信钱包快速的发展起来。

同时，二维码的安全隐患引发关注。在今年315晚会上央视曝光了扫码支付的骗局，现场说明了扫描二维码后手机被植入病毒，支付账号、密码等个人信息被盗取等安全威胁。图1-3分析了我国公众关于二维码扫描情况[[3]](#footnote-2)。

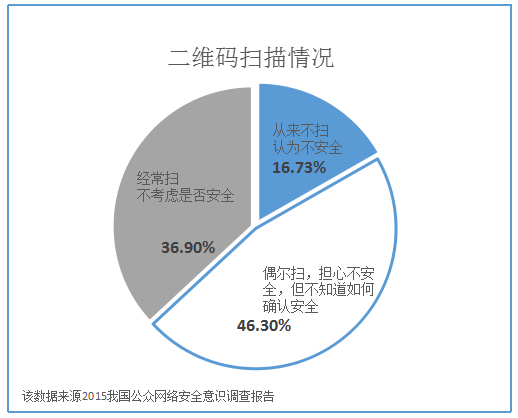


图1-3我国公众网络安全意识调查报告中公众二维码扫描情况

Figure1-3 China's public awareness of network security in the investigation of public two-dimen-

sional code scanning

1.3论文研究的主要内容和意义

本文在主要了解了我国公众使用二维码支付的情况和潜在安全性问题，着重分析从产品设计到消费者使用过程中可能存在的风险，分析出了二维码支付这种支付方式存在的不足，并认真解读相关文献中对二维码支付的安全评价和改进方法，重点学习了三种对二维码信息的处理方式。主要内容包括：

（1）研究二维码支付使用原理、技术、设备、流程等相关理论；

（2）研究和分析不同因素诱发的潜在风险和安全目标；

（3）研究和分析目前先阶段重点解决的安全性问题；

（4）从流程设计角度提出多层身份验证和第三方认证改进安全身份识别问题；

（5）提出混合加密方案改进二维码信息信息可靠性；

（6）分析混合算法与DES、RSA性能差异，突出混合加密的意义；

近几年来，二维码支付规模呈现爆发式增长，在享受技术创新红利的同时，也应该更加关注信息安全。因此本文的研究意义在于学习一些改进的方法，提出更加完善的且有利于解决二维码支付中存在的安全隐患的二维码支付体系，以保证个人、商户和机构信息支付交易和信息的安全。只有减少市场上的风险性，才利于移动支付规模的扩大和普及率的上升，促进移动支付的进一步发展。

1.4 论文的结构

第一章为绪论。这一章主要介绍了本文的研究背景与意义，二维码支付在国内外的发展现状和方向，提出二维码产生支付安全威胁，介绍文章的主要内容和意义。

第二章为二维码支付技术的相关理论介绍。本章主要介绍二维码支付的技术原理、应用场景分类、系统架构、使用设备等参与要素的介绍。

第三章为二维码支付安全风险性的分析。本章从使用流程、功能模块、技术分析存在的风险性，并根据移动支付安全目标提出待解决的问题。

第四掌为二维码支付安全改进方案设计。本章提出了针对风险性存在问题对应的改进方案，分别是多层身份验证、第三方认证和混合算法加密。

第五章为混合加密算法与RSA、DES算法性能比较。本章从时间性能、安全性能、密钥管理、实际应用上对三种算法进行比较，说明混合加密算法保证信息可靠性的优越性。

**2 二维码支付技术应用现状**

2. 1 二维码支付技术原理分析

2.1.1 什么是二维码技术

二维码（2-dimension bar code）是一种信息记录的符号，这种信息符号是将一些图形按照一定的规则组合而成，在二维的方向上它由黑白相间的图形排列组合而成。和计算机内部逻辑基础“0”、“1”二进制的概念一致，不同的二维码也对应着不同的文字和数值信息。

1. 叠堆式二维码

叠堆式二维码的编制原理是在一维码基础上的，按需要堆积成二行或多行，被称作“叠堆式”二维码，所以在设计原理、读取方式、校验上和一维码较为相似，代表码制有PDF417、Code 49，Code 16K等。

（2）矩阵式二维码

矩阵式二维码，顾名思义，在一个长宽相同的空间中分布着黑白像素，不同的分布规律也代表着不同的信息排列，矩阵中的点对应“1”“0”二进制，。矩阵式二维码包括DM、code one、QR Code等，由于QR码在解码、容量和成熟度等方面的优势，而且可以对中文编码，所以关于QR Code的应用广泛，在支付、购物、通讯等领域都得到了大量的使用。

2.1.2 二维码技术的编码与解码

二维码的编码流程是按照以下步骤完成的：数据分析、数据编码、纠错编码、构造最终数据、选择掩模、添加格式与版本数据、最终生成图像[2]。以QR code为例：

1. 原始数据分析：确定编码字符类型，选择数据类型，选定纠错等级。
2. 对数据编码：将数据转换成位流，构成一个数据的码字序列，代表二维码的数据内容。
3. 设置二维码纠错能力：选择设定纠错容量等级，生成对应纠错码子。当落实了二维码规格和纠错等级，也可以确定码子总数和纠错字数。
4. 最终数据确定：按照排列规则排列二维码中的数据，即能得到最终的数据。
5. 构造矩阵：把探测图形、定位图形、分隔符和校正图形和码字模块放入矩阵中，完整序列填充到二维码矩阵中。
6. 选择掩模：将掩模图形应用到二维码编码区域，增加二维码的可读性，黑白区域得到最优分布。
7. 生成图形：将格式和版本信息加入其中，生成二维码图形。

二维码的解码流程是按照以下步骤完成的：识别模块应用、识别格式与版本、消除掩模、恢复信息数据与纠错码字、检测错误、原始数据重组完成解码流程[3]。

2. 2 二维码在移动支付中具体应用

2.2.1 二维码支付的优势

和传统的收单业务比较，二维码支付采用扫描枪方式操作简便，那么商户就不用对软硬件大幅度的改进或重新采购设备旧即就能实现近程支付，从而实现了多种线下消费的支付新手段，又与传统的IC卡刷卡等方式相互补充，避免了利益方存在矛盾不利于推广等缺陷。二维码支付简化了客户支付中操作的步骤，缩短了消费时间，创新了服务体验，许多商家利用二维码支付绑定公众账号，对接消费者的会员信息、积分享用等服务。

2.2.2二维码支付分类

按照二维码支付的使用场景，可以分为二维码线上支付和二维码线下支付。

（1）二维码线上支付

二维码在线上支付中发挥着重要作用。传统的网上支付是按照用户选择购买商品或服务后生成网银链接在登陆选定的网上银行，登陆银行账户密码完成购买。二维码中的编码信息对应着不同的支付链接，用户在购物后确认付款，通过扫描平台生成的支付二维码自动跳转到手机支付，只需输入支付密码即实现“秒付”。除了节约流程外，还能避免因为购物平台没有与某些商业银行合作，而出现了该平台不支持用户手上持有的商业银行账号付款的问题，也就是说，只要购物网站与“支付宝”“微信支付”等支付平台作为第三方支付平台，那么也能推动网上购物的发展。

（2）二维码线下支付

二维码线下支付应用广，是许多支付平台业务竞争的重心，如翼支付、微信支付、支付宝支付等。从支付方式看，一般分为“主读”和“被读”两种，即用户扫码支付和商家扫码收款。以支付宝为例，“扫一扫”对应主读式支付，“付钱”“收钱”对应被读式。

按照二维码支付的读取方式进行分类，目前的支付二维码的读取方式分为主读式和被读式两种。被读式，即是在用户手机端形成动态的实时二维码后，由商家手持扫码枪扫描。生活中普遍使用的是以被读式为主的支付场景，因为其危险系数相对于用户直接扫描外部的二维码来说相对更低。

（1）主读式二维码支付流程：付款方打开支付客户端支付界面，对商家提供的二维码扫码，双方确认交易金额后输入付款数目，再通过身份验证（如支付密码）后提交给支付系统处理支付请求，支付成功系统将返回支付反馈结果[4]。

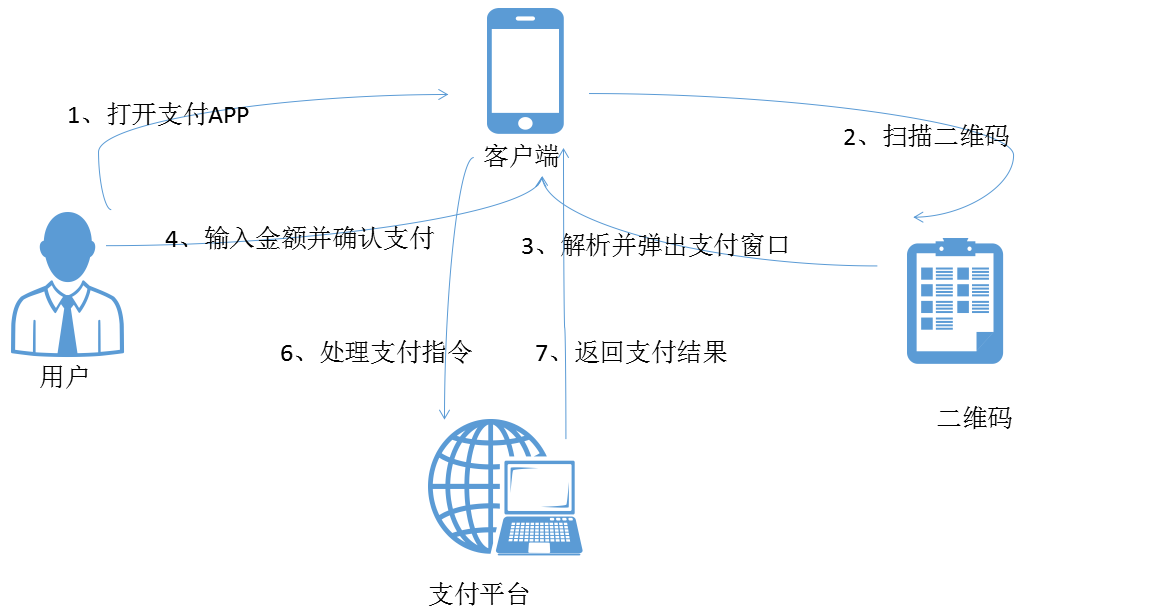


图2-1扫描式二维码支付流程

Figure 2-1 Operation flow of Scanned two-dimensional code payment

1. 被读式二维码支付流程：主读式二维码和被读式二维码区别在于后者需要向支付系统请求生成支付凭证的发码。付款用户打开手机支付软件，请求系统发码，收款商户通过扫描枪读取支付码，商户向提交支付请求最后要确认付款方支付成功，支付成功或失败，系统会发送支付结果给双方。

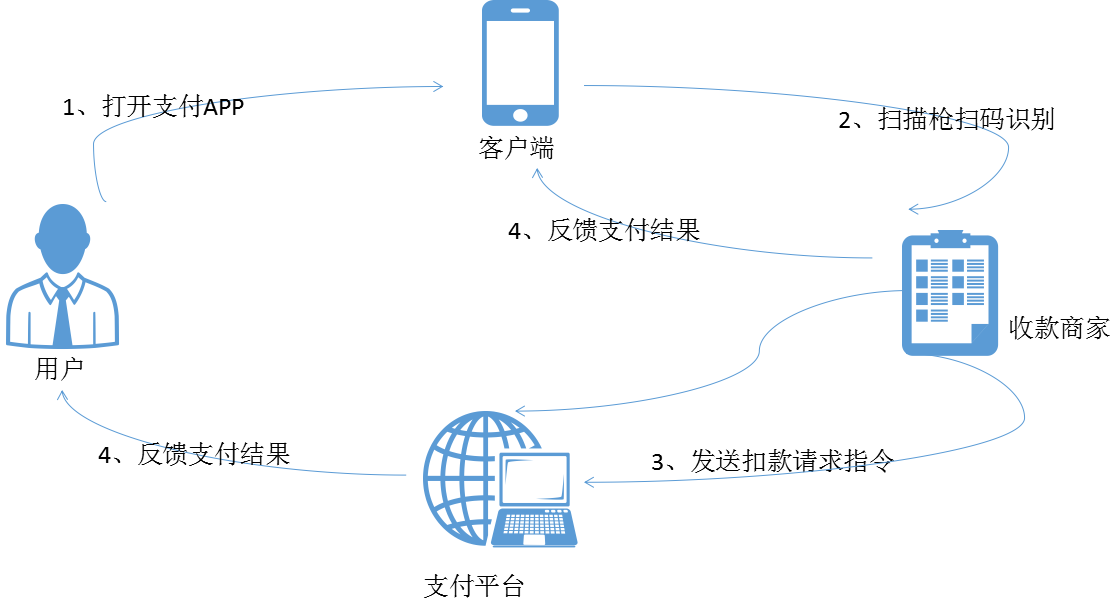


图2-2被读式二维码支付流程

Figure 2-2 Operation flow of of read two-dimensional code payment

2.3 二维码支付参与要素分析

二维码支付可以远程访问支付系统，所以要对二维码支付进行安全性分析，就必须了解支付的流程、移动支付的架构、支付设备、移动支付的安全需求多方面分析。

2.3.1 当前二维码支付系统架构

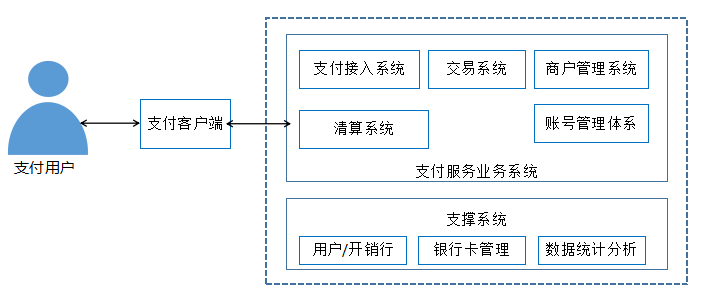
二维码支付系统架构与其他支付形式有个不同之处， 一个是访问支付内容平台和接入支付系统是通过支付的客户端完成的。第二个是支付系统访问方式不同，客户端将二维码中URL访问支付接入系统的解析，客户端即时生成了支付指令，二维码作为电子支付凭证，最后系统转接到后端交易系统处理。

图2-3 二维码支付系统架构图

Figure 2-3 System architecture diagram of the two-dimensional code payment

2.3.2二维码支付相关设备

（1）终端设备：终端设备及其操作系统的安全需求包括机密性、完整性。在用户所使用的终端设备中，比如手机或平板电脑可用于扫码支付，因而存储着用户的支付平台账号密码、绑定银行卡、存款余额等重要信息。同时操作系统是否完整直接影响支付平台的正常使用并有效防止外界破坏性行为。

（2）支付平台软件：支付平台实现了收付款功能，包括扫码识别或生成支付指令二维码、确认支付指令、反馈用户支付结果等涉及敏感信息操作。支付平台直接与用户账户余额、银行卡使用互相绑定，因此需保障其完整性、可认证性和秘密性。

**3 二维码支付技术安全风险性分析**

3.1 二维码支付模式下相关风险分析

二维码是移动互联网的入口，在购物、媒体宣传、社交传媒、移动通讯等方面随处可见。二维码支付仍存在信息识别的可靠性问题，虽然在二维码设计中实现了纠错机制，生成的二维码具备加密和唯一性，保障了信息的完整，但由于制码技术几乎零门槛，也存在许多不安全因素。

3.1.1从支付流程分析存在风险性分析

网络支付安全和效率均和网络支付风险相关，交易流程是经营风险的重要内生因素，其管理控制十分重要[5]。二维码支付因为其极短的支付时间、简便操作流程所以迅速得到推广和应用，满足了都市消费者对便捷性的要求，因此在二维码推广中，各平台为占领商业市场，都把效率放在首位，缺少了对风险的全方位控制。加上消费者缺乏安全和消费者权益教育，因此存在一定的支付风险。

（1）第二章中被读式风险在于现有的支付平台所设定的“隐形”服务协议[[4]](#footnote-3)，规定商户、收款人和用户在使用一定额度和次数限制内的支付交易时无需验证支付密码，这样平台就可以直接按照交易制定对“零钱”和关联银行账户进行资金扣划和归集操作。一旦账户被盗用或支付二维码被犯罪分子和黑客所掌握，那么账户所绑定的银行卡余额或账户零钱都可以被快速盗刷。

（2）主读式支付风险在于，因为二维码具有信息存储的功能和信息转译特征，普通用户无法通过二维码表面的图像特征分辨真假，那么一旦误扫提前被植入病毒的二维码，就有可能发生账户被盗、信息被窃取，同样危害用户银行卡余额和账户零钱安全。

3.1.2二维码刷卡模式下存在的风险

产品缺陷极有可能迅速引来外部欺诈团伙的聚集[6]。类似于信用卡免密支付，二维码刷卡模式不需要输入密码或生物识别、短信动态密码以及任何信息进行身份验证。信用卡免密支付中，商家有义务核对消费者签名与卡片签名来记录是否相同，但这依旧存在着信用卡盗刷风险。而在二维码支付中，很多商家没有使用签名凭证又缺乏身份认证流程，一旦用户手机被盗窃或丢失，风险不可估量。非授权交易风险在网络支付安全控制中尤为重要。

3.1.3二维码支付用户身份验证存在风险

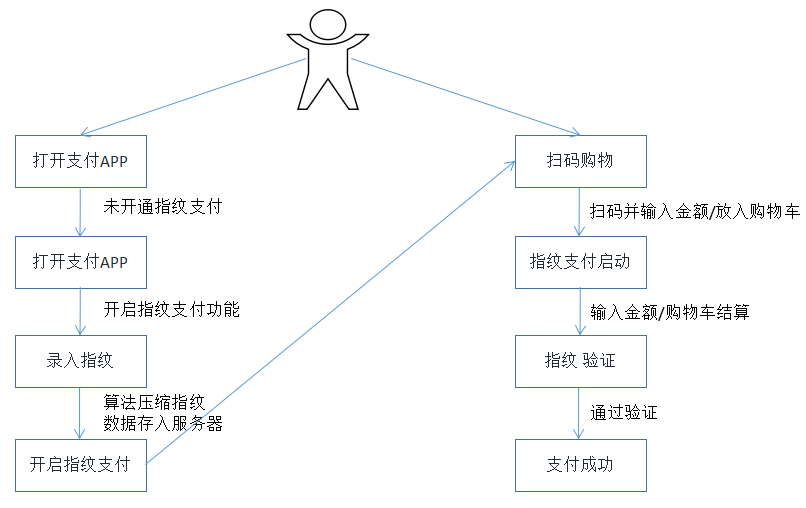
现有二维码支付平台基本实现身份验证支付指令，一些智能手机如苹果、华为部分机型已实现生物科技识别支付技术，如指纹、虹膜、声波、面部识别支付，开启指纹支付则默认情况下按指纹验证身份，通过则支付成功。智能程度较低的手机则仍使用密码支付。单一的密码支付或单一的生物识别都无法保障支付安全，以苹果为例：指纹支付是通过验证Touch ID验证后快速完成付款，意味着无论操作手机是否为本人，只需要通过验证智能端设备中指纹验证即可完成支付。

图3-1指纹支付使用流程

Figure 3-1 Operation flow of Fingerprint payment

3.1.4用户成为非授权交易风险主要承担者

当支付产品存在一定的风险性时，风险产生后的责任分担话题就引起了重视。一些支付平台通过不明确的用户协议设定用户为非授权风险承担者为。以微信支付为例，用户协议中只是注明一旦注册或使用该服务则视为接受相关协议，并没有在使用流程中告知用户协议内容和支付中可能存在的风险，图3-2为用户对协议的关注情况。在用户协议4.1中明确说明了微信登陆状态下支付指令均被视为本人操作，且需承担一切因支付相关信息泄露导致的风险；4.2中规定用户默认同意无验证支付指令；4.3中说明指纹支付一旦开启则仅凭移动终端发出指纹校验进行资金划扣。

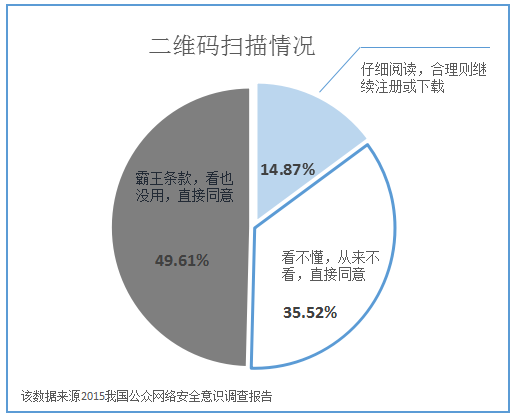


图3-2公众对支付协议的关注情况分析

Figure 3-2 Analysis of protocol when using two-dimensional pament in citizens

3.2从技术角度分析二维码支付的安全问题

技术风险因素关注点包括硬件系统运行的可靠性、应用系统的稳定性、系统运行安全保障、网络可靠性等。本文第二章重点分析二维码支付分类、支付流程、系统架构、设备归纳出三个可能存在的问题。

（1）支付终端：与传统支付设备不同，智能终端的专业性不强，因此被攻击的危险较大，存在信息泄露可能。

（2）支付指令单一易攻破、保护力度弱。二维码缺少防伪功能，身份验证过程简单，单一密码验证或指纹认证无法落实安全保障力度，验证通道和安全因子单一。

（3）生成机制和传输过程存在安全隐患。二维码的背后链接着一个网址，网址的内容是无法从码制表面看出来的，所以我们无法直观地分辨它是否会恶意地引诱用户扫描链接着病毒的不良网站，手机一旦中毒，犯罪分子还能够设置自动识别和屏蔽掉运营商发送给用户的消费提醒短信，如果病毒中安插插件，那么用户的账号和密码就暴露在不法分子面前了。

3.3二维码支付安全总体目标

中国银联二维码支付安全规范文件最新出台，要求各行业进行业务安全开通、二维码中信息不被泄露和篡改、安全的信息传输、安全的支付过程等多方面的安全目标来保证个人、商户和机构信息及支付交易的安全[[5]](#footnote-4)。从二维码的编码制作过程，到二维码提供方如商家、企业、个人发放、宣传到二维码的传输，整个生成和传输的过程都必须在“阳光”下进行，受到监管和监督，这样才能有效避免病毒程序以二维码为伪装，或者利用二维码恶意盗刷现象的出现，进而保证用户所扫描的二维码可信与安全。

移动支付作为一种电子商务模式，其基本安全需求包括可认证性、私密性、完整性、不可否认性。

（1）可认证性

认证在安全因素中最为重要，它是其他安全需求要素的基础，移动支付中有3种不同认证的方法：（1）主体使用只和验证方共享的密钥加密信息，验证方使用此信息验证主体身份；（2）主体用私钥进行消息签名，验证方使用此签名验证主体身份；（3）主体用可信第三方证明自身身份。二维码支付是引起交易双方的资金变动，因此身份认证最为重要。一旦缺少身份识别环节，则存在账户资金被盗取风险。

（2）秘密性

在二维码支付过程中，从支付方到商户存在着多方的数据交换，涉及多个账户个人、银行账号等敏感源。在移动支付安全中的秘密性是对消息加密，避免交易中的如用户身份、支付凭证、支付指令等敏感数据泄露给未被授权的人，导致资金被盗。所以，对信息加密即将消息从转成密文是维护敏感信息机密性的有力保障。

（3）完整性

假设支付过程中数据被修改、删除或者替代，则无法保证传送次序统一影响信息的完整统一，导致交易双方混淆真实支付信息。一般采用封装和签名的方式，即提取信息的摘要实现。Harsh函数产生摘要，与收到的摘要比较后可判断消息的完整性。

（4）不可否认性

不可否认性指交易双方提供参与协议交换的证据保护各自利益，协议双方事后不能不承认交易的存在。与传统的POS收单业务中产生的纸质凭证比较，二维码支付以数字信息凭证为主，如通过微信支付后的电子支付凭证，而电子化数据易伪造、修改。移动支付中一般以签名形式提供，许多商家采用最新的支付设备可支持电子签名，而支付方则可采用指纹支付或密码支付等方式来加强不可否认性。

3.4 二维码支付待解决的两大问题

（1）双方交易中身份验证。传统的交易方式可以通过身份证件、签名查验本人身份，二维码支付仅需登录账户和密码即可扫一扫秒付。

（2）如何保证二维码传递的支付信息可靠有效。二维码支付应用了密码学原理，通过特定不可逆算法，时间、终端、用户信息成为了支付主体的授权。如果该算法外泄或被破解，极易造成不可控的损失。另外，一般来说二维码包含的支付信息没有危害，但如果因为加密易攻破，或者因为用户的大意和外界的欺骗，那么就极有可能出现二维码被破译，支付信息被修改的信息泄露、金融诈骗案件。

**4对二维码支付安全改进方案设计**

4.1 多层身份验证提升安全性

针对第二部分中提出的安全问题，本章重点提出三则对策：提出多层身份验证、带第三方认证二维码支付和混合算法加密。

移动支付新举措：以流程设计的改进为基础，多层身份验证提升安全性[7]。如何利用有效方式识别用户安全身份:除了常用的密码支付外，利用生物科技识 别可以达到多层身份验证。在移动支付安全需求中，一般采用签名保证不可否认性。如果应用指纹、声音、面部特征和眼部特征等独一无二生物特征识别，可以进一步核对安全身份。

（1）眼部识别技术和虹膜技术：眼部识别原理和指纹类似，利用球网膜结构独一无二特性可以识别主体身份，基于用户眼睛虹膜两侧的眼纹进行身份识别的一种新的生物识别技术。虹膜技术被称为“最难伪造”的生物技术，它已被用于安防设备、智能手机、保险柜、ATM机等领域。精度高、速度快、高安全等特征都高度符合提升支付安全性要求。只是眼部识别技术难度

（2）指纹识别：指纹消费目前已被广泛应用，放入指纹识别区域实现秒付。指纹识是一种新生的支付方式[8]，因为识别方便、效率和防伪度较高被广泛用在身份识别。

（3）面部识别：面部识别以非接触的方式获取识别对象的面部图像，计算机系统在获取图像后与数据库图像进行比对后完成识别过程。识别的精度高、速度快，误识率、拒认率较低。面部识别已被应用在账号登陆，如支付宝刷脸登陆。在支付领域可作为补充性身份认证技术，支付平台通过人工智能、风控系统等对账户使用情况进行安全监测以确保安全。

（4）手势密码：进入钱包前验证手势密码可以降低微信钱包被盗刷的风险。

（5）二维码支付多层验证设想：双层或多层身份认证。在手机中录制眼球结构、虹膜、指纹、面部3D图像，经过算法压缩备用。支付主读式或被读式打开之前先弹出生物识别窗口进行身份认证，通过算法验证后，才能进入支付信息核对和密码支付操作或商家读取用户支付二维码。增加生物识别技术这个环节可以有效防止黑客破解身份认证。用户可以根据对支付安全系数的要求，自行设置多层的身份验证，比如先经过指纹验证后方能进入“扫一扫”功能，扫码后输入消费金额，确认支付前再输入提前设置好的“支付密码”。这样就能增加一层身份验证的屏障，如图4-1就是在支付过程中加入了眼球网膜验证，改变了单一的密码验证方式。

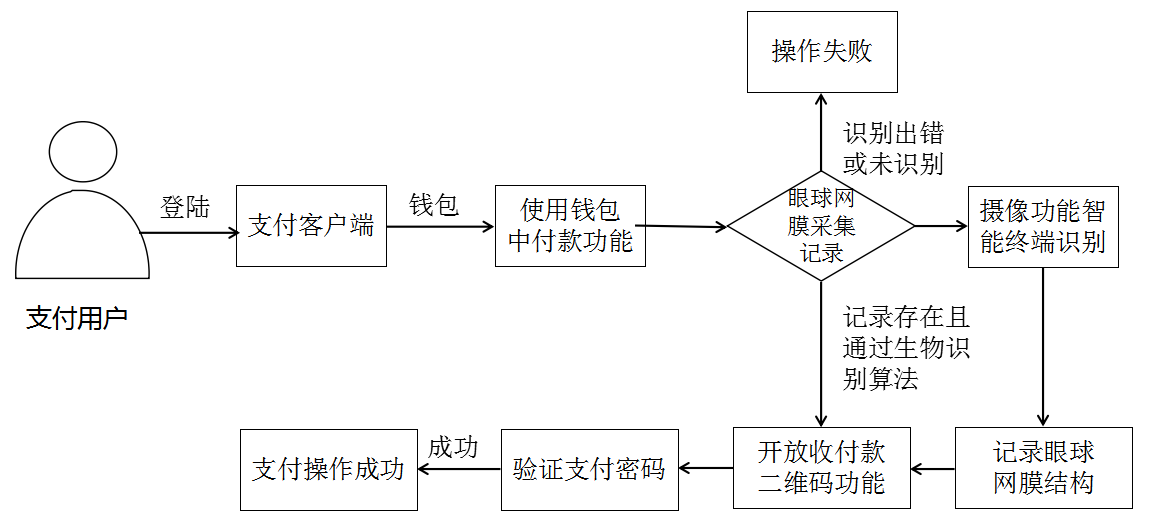


图4-1多层身份验证提升支付安全性

Figure 4-1 Multilayer authentication to enhance payment security

4.2 第三方认证

加入第三方认证的思想，是基于移动支付中身份验证的不足和商品信息中二维码不安全性。上一章中，分析了生成二维码机制和传输中存在安全隐患，二维码的防伪效果缺乏保障，比如在公共场所里的自主贩卖机里通过扫码购买商品时二维码经过违法份子的篡改后，保留二维码中链接的商品信息，而改变的支付环节中的支付对象或植入病毒，则商家无法获利，用户信息遭泄露，因此二维码支付安全性认证上缺少一环。

在移动支付中进行第三方认证指的是通过没有直接利益双方的主题参与对信息可靠性的认证，它可以帮助对交易双方身份验证，防止信息伪造给交易主体造成一定的经济损失，保证交易过程的安全合法。第三方认证是一种安全验证的模式，它能在商家和用户中建立一种互相认证的关系，经认证后产生的二维码即使被篡改也无法通过支付前的比对认证机制。

带三方认证的安全性改进方案可行性分析：

（1）方案可行性：可行性在于即使攻击者伪造二维码，更改商品信息，用户支付前请求认证也会失败[9]，用户所打开二维码链接的商品信息在制码和生成过程中带有第三方认证，支付前第三方会继续对数据认证，经过比对决定是否可以进行支付。图4-2分析了第三方认证在改进二维码支付流程设计中的作用。

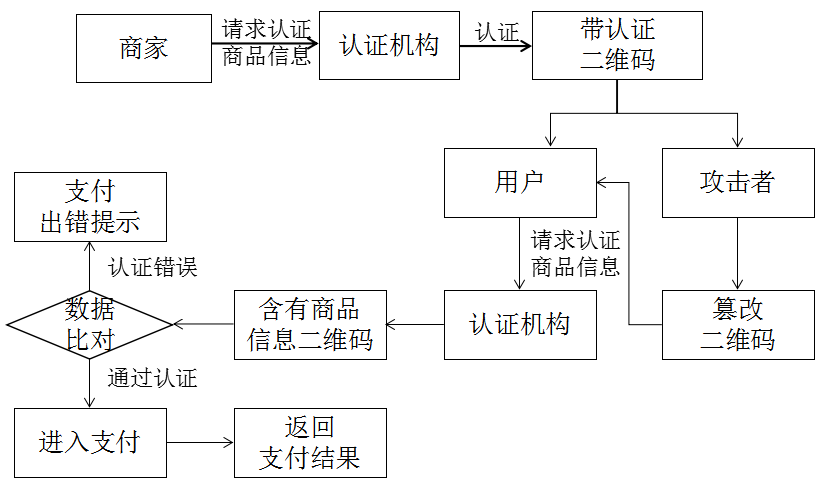


图4-2带第三方认证的二维码支付流程

Figure 4-2 Process of two-dimensional code payment with third party authentication

4.3特殊加密法设想：混合加密提升二维码支付安全性

在第二章详细介绍了二维码支付安全性风险和待解决的问题，其中一个是保证二维码传递信息的完整可靠，其安全性重点在被动扫码如何保证中单支付条码产生的算法不被破译。特殊的加密方式被认为是保证信息加密性的有效方式，在二维码支付安全性改进中，将特殊的加密方法引进用户和商家的终端软件中，扫描钓鱼二维码将终止支付操作。

在加密领域，以RSA和DES为代表的公钥系统和对称密钥系统在加密领域应用广泛，如POS机，U盾等。单独的DES算法在密钥传输中存在安全隐患，而RSA算法则被认为最有影响力的公钥加密算法，它能够抵御到目前为止已知的绝大部分密码攻击，已被 ISO 推荐为公钥数据加密标准。基于对DES和RSA的优劣势分析，一种混合制的加密算法被提出，混合加密信息的方法也被验证安全性优于单一算法。

4.3.1非对称算法RSA

（1）算法安全性与传输安全性分析

RSA算法是由美国三位计算机学家在1977年提出的[10]，通过密钥交换算法，避免了直接传递密钥的情况，其安全性的实质在大整数因子分解难度（此次引用文献）。RSA密钥长度较长，除了暴力破解，至今世界上未出现可靠的攻击RSA算法的方式，也由此奠定了RSA在加密领域地位。RSA具有非对称性特征，与DES算法不同，加密密钥和解密密钥不一致，传输方使用公钥（n,e）加密，接收方利用私钥（n,d），公私钥之间不存在推导关系，只要做到一个密钥管理即可。

1. RSA算法加密与解密原理

例1. 假设A和B之间传递信息M=65，运用RSA算法生成公钥与密钥，并进行加解密。

1、随机选择两个不同的质数p,q，质数越大，则乘积越大，分解难度上升：61和53；

2、计算质数乘积n,并计算n的欧拉函数Φ（n）:

n=p×q；Φ（n）=(p-1)(q-1)；

n=3233;Φ（3233）=60×52=3120；

1. 随机选择密钥e,使得e和Φ（n）互质：选择17；
2. 计算e对于Φ（n）的模反元素d可以让ed被Φ（n）除的余数为1；

e=17,Φ（n）=3120,方程经过化解可以得到d=2753；

1. 封装n和e为公钥，n和d为私钥：公钥=（n,e）;私钥=（n,d）；

根据已知n、e、d求解值，公钥=（3233,17），私钥=（3233,2753）；

6、加密和解密过程分解：利用公钥（n,e）加密，再用私钥（n,d）解密：

A欲向B发送生成信息M,假设M=65,经过加密运算C (mod n),得出密文C=2730；则A向B传递2730；B利用私钥对C解密：



,M=65；

1. RSA算法安全性验证：由公钥、私钥求解公式：

ed=1(modΦ（n）)；Φ（n）=(p-1)(q-1)；n=p×q；

可知，n进行因式分解才能得到p,q，而n位数越大，分解越难，无从得知p，q，也就无法知道Φ（n），从而无法求解d。

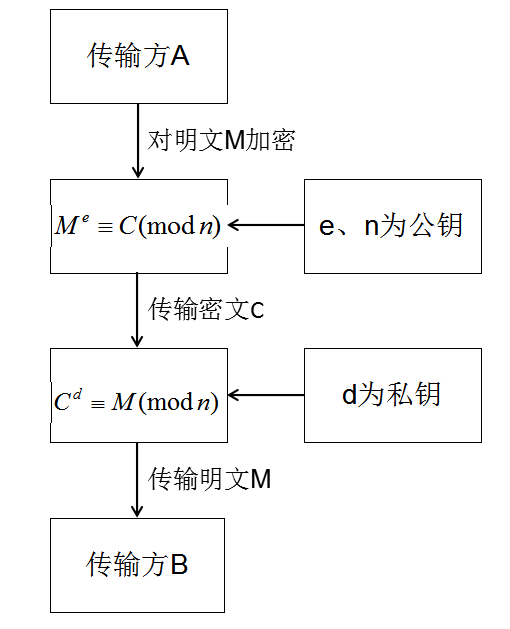


图4-3 RSA算法原理流程图

Figure 4-3 RSA algorithm flow chart

4.3.2 RSA算法和DES算法比较

（1）DES加密算法：DES是对称密码算法，从解密密钥中可推算加密密钥，具有速度快、处理简单和密钥较短等优点，但安全性有所降低，根据其性能特征常被用来加密大串信息。

（2）RSA加密算法：非对称性算法，故加解密密钥之间无法直接相互推算。特点是尺寸大、速度慢，RSA的核心是密钥的保护性强，破解难度较大，安全性能也相对于DES高。时间测算中，RSA耗时比DES更长，效率较低。

（3） RSA加密算法和DES加密算法优劣势互补：RSA和DES分别在安全和效率上各占优势，如RSA安全性更高但不适应大批量数据，DES加解密效率更高，RSA加密时间是DES的26倍，如表4-1为DES和RS加密用时比较[[6]](#footnote-5)。混合算法的原理是用对称密码对明文加密，用非对称密码对密钥传输加密，加强对密钥的管理。RAS和DES特点不同，结合实际应用能力则更强。DES与RSA两种算法加密二维码信息，可以解决信息完整性问题，不法分子无法破解系统加密方法进行解析，伪造的支付二维码由于解析失败导致用户无法完成支付操作，最终保证了支付安全性，在这个方法中，支付安全问题从二维码转移到终端[11]。

表4-1两个算法的加密时间比较

Table 4-1 Comparison of two algorithms for encryption time

|  |  |
| --- | --- |
| 算法类型 | 加密用时/S |
| DES | 0.0725289 |
| RSA | 1.88749 |

4.3.3 混合算法的加密解密过程

1. 传输方A确定传输的明文M；
2. 随机生成密钥K,用DES和密钥K对明文加密成密文C；
3. 获取公钥e和n，利用RSA算法对密钥K进行加密，产生加密后密钥Ck；
4. 生成传输的秘密文件组合：传输密钥Ck和密文C到接收方；
5. 将秘密文件组合解密，公钥n私钥d通过RSA算法对Ck密钥解密产生原始密钥K；
6. 利用DES算法和原始密钥K对密文C解密得到明文M,B接收到明文，传输完成。

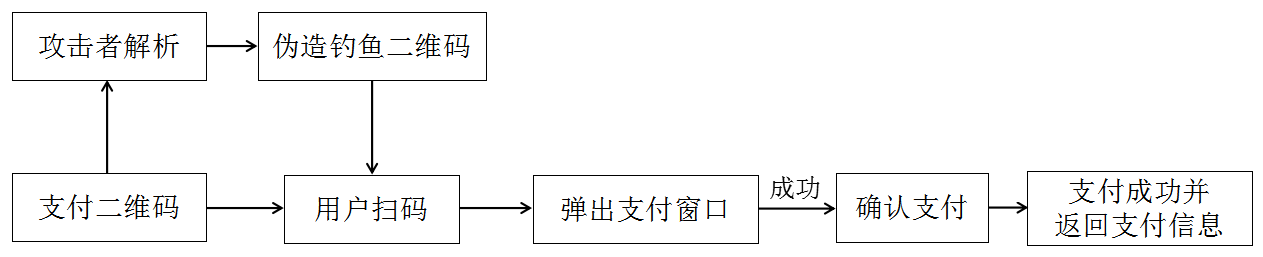


图4-4 RSA和DES混合加密传输信息流程图

Figure 4-4 The flow chart of Information transimission with hybrid enen-cryption algorithm

在第三章中重点分析了刷卡模式下存在的支付安全隐患，在身份验证流程单一的前提下，支付性二维码的生成和传输安全变得尤为重要。用户一旦扫描钓鱼伪造性二维码，而没有经过支付前的解析，则极有可能产生诱导性支付，该风险的出现如图4-5。

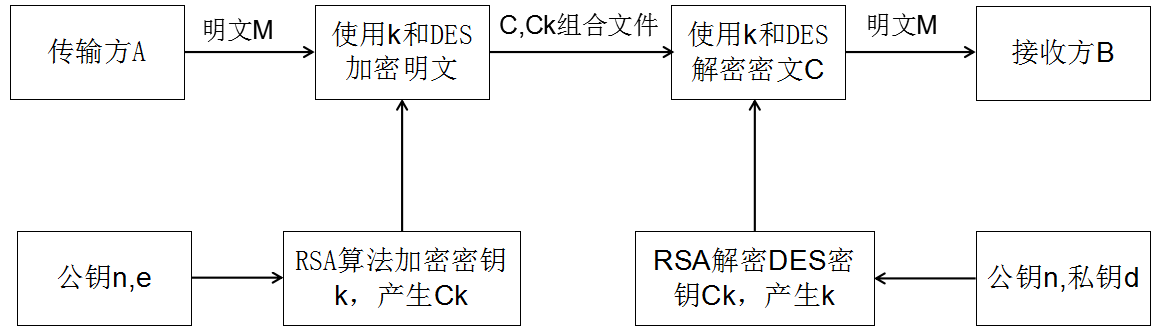


图4-5 二维码支付中存在风险

Figure 4-5 Possible risk in two-dimensional code payments

采用混合加密算法对支付二维码进行加密，配套同步的升级型客户端支付软件，一方面攻击者缺少混合加密算法中的密钥无法破解该算法，伪造失败；另一方面消费者即使扫描伪造二维码，也无法通过解析进入支付页面，支付失败。和传统的收单业务相似，此时的交易风险存在于使用的终端，则扫码支付风险性降低了。

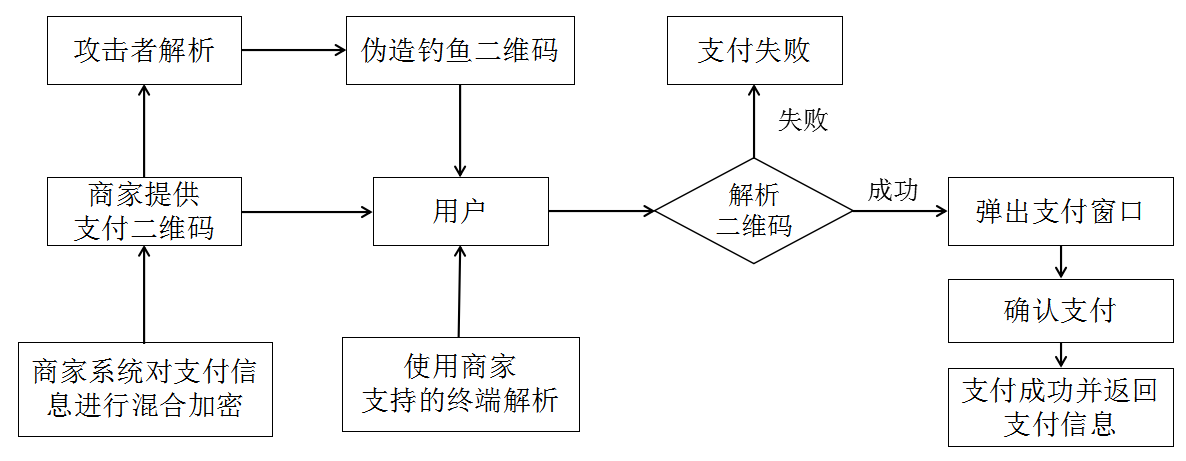


图4-6 混合加密算法在二维码支付中应用

Figure 4-6 hybrid encryption algorithm in the application of two-dimensional code payment

**5 混合加密算法与RSA、DES算法性能比较**

5.1 混合算法与DES、RSA时间性能比较

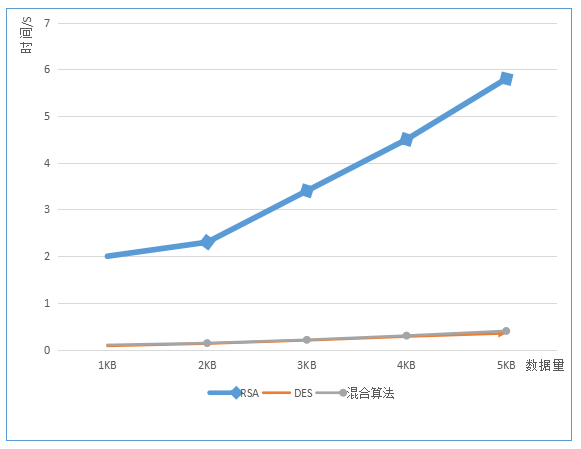
时间性能分析。图5-1[[7]](#footnote-6)记录了加密算法中三个算法RSA、DES、混合加密的时间效益。RSA远远高于另外两种算法，且趋势是随着加密数据量的加大，时间上成倍增长。RSA所耗用的时间与另外两个算法的比值快速增长，也证明了前者与后两者的时间优势无法比拟。这一差距也与RSA特征相匹配：解密难度大、时间效益低。而混合算法相较于DES在单位数据量加密时间上稍高，时间效益上可以说是比较接近的。从时间性能的比较中可以得出混合算法克服了RSA中的不足，获得良好的效率。

图5-1 三种加密算法时间性能比较

Figure5-1 comparison of time performance in three encryption algorithm

5.2 混合算法与DES、RSA安全性能比较

第二章学习了解到RSA的安全性能依赖于两个大的素数乘积分解难，要攻击RSA算法相当于要对大素数进行因式分子，假设被分解的素数位数少，如143通过从2开始的小素数的试除，可得到13与11的乘积。假设大素数取11位数的233333,33333，从2试除，难度可想而知。目前世界上被发现的最大素数长达2233万位。而DES虽然较前者安全性能稍弱主要是因其为单密钥系统又依赖于密钥。基于DES和RSA安全性能差异，可以理解为混合算法保留了前者又解决后者问题，因此是比较安全的。

5.3 混合算法与DES、RSA密钥管理上的比较

在密钥管理上，RSA与DES相比较，RSA更胜一筹。DES采用单密钥，通信对象需要产生和保管不同的密钥，在一次迭代运算中都会产生子密钥，DES算法对这些密钥的管理上除了难度大，还有加大对系统的负担，造成资源损耗。上一章中对RSA和混合算法加密过程详细介绍，我们了解到混合算法，只能通过私钥d解密密钥Ck，因此RSA和混合算法在密钥管理中的负担小。

5.4 混合算法与DES、RSA应用比较

混合加密具备良好的时间性能、又继承了RSA算法的安全性，在密钥管理上更优越。这样对于对加密性有更高要求的行业提供了安全可靠的信息传递过程。比如在通信、移动支付上既讲究时效性、更注重保密性，混合算法将可在二维码支付、个人隐私保护中得以应用。

表5-1算法性能总体对比

Figure 5-1 Comparision of the overall performance in 3 algorithms

|  |  |
| --- | --- |
| 性能 | 比较 |
| 时间性能 | DES>混合算法>RSA |
| 安全性能 | 混合算法≈RSA>DES |
| 密钥管理 | 混合算法>RSA>DES |
| 应用 | 混合算法更符合实际需求 |

**参 考 文 献**

[1] 王杨.二维码传播信息的应用和分析[D].山西：山西大学.2013.

[2] 于芳芳.二维码支付安全性.[J]Electronic world电子世界.2017(07)：157-158.

[3] 王春东,冯超然,高素梅.移动支付中二维码的安全性研究.[J] 天津理工大学报.2014.06(30)

15-16.

[4] 袁菲.二维码支付技术安全性分析框架[J].融科技时代.2014(10):64-66.

[5] 武鑫,禹路,朱海明.金融会计.网络支付机构面临的风险及其防范[J]. 2013(11):27-32.

[6] 巴曙松,杨彪,朱海明.中国网络支付安全白皮书：网络支付结构创新与风险治理[M].北京：中国发展出版社,2014.61-62.

[7] 冯韵.移动支付中身份认证分析与研究[J].信息通信.2013(3):108-109.

[8] 丛砚敏.移动金融支付革命[M].北京：清华大学出版社,2016.46-47.

[9] 冯超然.基于第三方的移动支付安全性研究[D]. 天津：天津理工大学,2014.

[10] Rivest, R. Shamir, A. Adleman, L.. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems[J].Communications of the ACM. 1983:V26 96-99.

[11] 刘宇.常用加密算法比较研究[J].科技风.2010 (19)：280.

[12] 江南燕.移动支付问题探讨——以二维码支付为视角[J].法制博览2015(01)：119-120.

**致 谢**

毕业论文的完成，也意味着四年的本科生活即将落下帷幕。回味着大学的四年愉快时光，不仅收获了学习和为人处事上的两笔财富，还有很多难得的情谊。在此，感谢曾经给与我帮助的老师、同学们、朋友们和家人们，感谢你们在生活和学习上给与我的理解与支持，尤其是各位老师严谨治学的教学态度，专业而耐心的教学方法，以及在学术上精益求精为我们树立了一个个榜样。

本文是在张婧炜老师的指导下完成的，感谢导师在论文写作、文献查阅、知识解读上对我们的指导和帮助，从最初选题的迷茫到开题的信息，再到论文的修改，在您的指导下，学会如何去完成一个学业任务，就像您所说的那样，力求静下心去完成一件事，这种精神可以让我们解决更多的人生课题。感谢您为我们提供的宝贵建议，也感谢您在论文之余对我们学习和工作的关心。

最后，对各位老师们对我的论文的审阅，以及提出的宝贵批评和建议致谢！

1. ① 周勤燕.央行发布2016年支付业务统计数据：移动支付笔数涨85.82%.[DB]

   http://www.donews.com/news/detail/1/2948964.html,2017-2-14/2017-3-26. [↑](#footnote-ref-0)
2. 纽约时报.2016年中国移动支付规模是美国的50倍.[DB]

   http://www.199it.com/archives/564464.html,2017-02-25/2015/-03-26. [↑](#footnote-ref-1)
3. 洪京一.公众网络安全意识调查报告(2015)[R].背景工业和信息化部电子科学技术情报研究所,2015 [↑](#footnote-ref-2)
4. 腾讯微信支付.微信支付用户服务协议.[DB]

   http://weixin.qq.com/cgi-bin/readtemplate?t=weixin\_business\_pay,2016-03-28/2017-03-26 [↑](#footnote-ref-3)
5. 2016年12月银联出台《中国银联二维码支付安全规范》

   http://member.unionpay.com/ [↑](#footnote-ref-4)
6. 陈侨川.一种基于DES和RSA算法的混合加密算法[D].云南:云南大学,2015年 [↑](#footnote-ref-5)
7. DES和RSA加密时间比较数据来自作者陈侨川《一种基于 DES 和 RSA 的混合加密算法研究》 [↑](#footnote-ref-6)