基于国密技术的 NFC 通信模型设计*

潘文杰　黄赢　陈积常**　李建

南宁学院信息工程学院，南宁 530200

摘 要 基于近场通信(Near Field Communication, NFC)的工作原理和系统架构，分析 NFC 移动支付系统中存在的安全威胁和安全性需求，构建一种基于国密技术的 NFC 移动支付通信模型，设计了相应的 NFC 移动支付认证协议。该模型使用 Xshell 终端模拟软件和 GmSSL 密码工具箱实现身份认证和通信双方身份鉴别功能，并在传输过程保证了关键交易数据的保密性和完整性。协议的安全性分析表明，对于窃听、假冒、重放、业务否认以及篡改等攻击都有很好的防御效果。实验对比结果表明，本文的模型在抵抗篡改攻击、抵御重放攻击、抵御假冒攻击、双方认证等方面均有明显的优势。

关键字 近场通信(NFC)，移动支付系统，密码体制，数字签名，国家商用密码算法

Design of NFC Communication Mode l Based on National Commercial Cryptography Technology

Pan Wenjie　Huang Ying　Chen Jichang　Li Jian

School of Information Engineering Nanning University
Nanning 530200, China;
943667593@qq.com

Abstract—Based on the working principle and system architecture of near field communication(NFC), this paper analyzes the security threats and requirements in NFC mobile payment systems, constructs a NFC mobile payment communication model based on national security technology, and designs the corresponding NFC mobile payment authentication protocol. This model uses Xshell terminal simulation software and GmSSL cipher toolbox to achieve identity authentication and authentication functions for both communication parties, and ensures the confidentiality and integrity of key transaction data during transmission. The security analysis of the protocol shows that it has good defense effects against attacks such as eavesdropping, impersonation, replay, business denial, and tampering. The experimental comparison results show that the model in this paper has obvious advantages in resisting tampering attacks, resisting Replay attack, resisting counterfeiting attacks, and authentication of both parties.

Keywords—Near field communication(NFC), Mobile payment system; Cryptographic system; Digital signature; National commercial cryptography algorithm

1 引 言

随着无线通信技术发展,尤其是智能手机的普及，移动支付应用也越来越大众化，使传统支付方式发生很大程度改变，对人们日常生活及工作均产生很大的影响。在移动支付方面，移动支付安全技术是保证移动支付业务顺利完成的基础[1]。

近场通信（Near Field Communication，NFC）技术，是一种能够在高频和短距离之间实现无线通信的先进技术,其应用范围广泛。无线近距离通信技术中，该技术具有低功耗、低成本的特点，可应用于各种便携式电子装置中。在 10 厘米的范围内，电子设备能够实现无需接触的通信方式，从而实现了点对点传输和数据交换[2]。由于其具有安全、便捷的特点，近年来受到越来越多的关注和应用，被认为是下一代移动电子商务的核心技术之一[3]。相对于二维码的支付方式来说，NFC 移动支付拥有更高的安全性和便捷性，发展前景十分广阔，并在国内外得到了广泛的应用。

NFC 移动支付技术需要越来越多的移动通信设备支持，银行、运营商、手机制造商等相关部门从中获取了极大的便利，普通消费者也从中享受到 NFC 移动支付带来的便利。但是，现在的 NFC 技术仍存在许多安全漏洞问题，如容易受到窃听、数据篡改、中间人攻击、数据破坏、网络钓鱼和未经授权访问等，用户个人隐私数据面临着被泄露的风险，这对于财务信息和用户的财产安全构成了极大的威胁。

*基金资助：本文得到南宁学院一流专业培育项目(2020YLZYPY01) 的资助。
**通讯作者：陈积常，教授，943667593@qq.com。

目前，国外研究人员对 NFC 技术的安全问题进行了广泛、深入的研究。文献[4]提出一个新的框架，首次使用 HCE 模式设备来实现 NFC 安全单元（SE）的相互身份认证和物联网访问控制。文献[5]研究分析了 NFC 应用中出现 DoS 攻击的原因，给出并通过无限循环的 URL 和超长字符的 APP 名字等试验验证了所提出的解决方案的可行性。

中国是世界上最大的移动支付市场之一。我国政府和科技人员对 NFC 技术的安全问题也开展了比较深入的技术应用研究。例如，文献[6]对基于 NFC 技术的移动支付安全应用进行分析研究；文献[7]提出了一种 NFC 技术的门禁系统认证协议，并针对安全性进行了设计；文献[8]提出手机端软件技术改进方法和后台使用数据风险监控三级预警方法,采用双重安全机制以规避安全威胁,确保 NFC 技术在地铁应用中的收益安全,尽可能地避免收益漏洞;文献[9]采用双线性对设计了一个安全高效的 NFC 点对点认证方案；文献[10]设计了一种基于椭圆曲线密码的 RFID/NFC 安全认证协议，能抵抗跟踪攻击、假冒攻击、拒绝服务攻击等各类攻击；文献[11]设计了一款面向 NFC 的安全轻量级芯片；文献[12]提出了一种基于假名的安全认证协议，并证明了该协议的安全性。

本文分析了 NFC 通信过程中存在的身份假冒、数据窃听、数据篡改、数据重放、交易抵赖等风险，根据安全需求构建了一种基于国密算法的 NFC 移动支付模型，设计了相应的 NFC 移动支付认证协议，并用 C 语言程序实现模型的安全通信功能，分析 NFC 通信协议的安全性。

2 NFC 移动支付模型系统需求分析

2．1 系统安全需求

虽然 NFC 移动支付能给人们带来非常大的便利，但也还有很多不可避免安全威胁和漏洞。一个完整的 NFC 移动支付交易行为，一般有四个参与者组成：一是带有安全单元的 NFC 移动终端，一般为消费客户持有，用来完成支付操作；二是商家的 POS 机或者其他读取设备作为受理终端，且作为交易的发起者向可信认证平台（TSM）提供交易数据。三是 TSM 平台，接收交易信息并与银行确认账户及交易信息的完整性、有效性。四是银行系统，主要作为结算系统和账户管理系统，对交易资金进行结算，对用户账户扣费和对商家账户进行转账。

一般来讲，用户或者商家与 TSM 和银行相互之间，只存在身份的识别和认证的问题，可以认为他们之间的数据通信是安全的。而安全威胁主要发生在用户的 NFC 移动支付终端设备和商家的 POS 机进行交易信息交互的时候。由于 NFC 移动支付过程中需要输入用户和商家的账户信息以及其他个人私密信息，所以在 NFC 移动支付过程中要保证数据的传输安全。

2．2 NFC 移动支付安全性需求

一个完整的NFC移动移动支付系统，除了拥有良好的业务需求模型，还要能够应付各种形式的安全威胁保证系统可靠地运行。从交易过程的安全完整性考虑，一个完整的NFC移动支付系统需要满足以下需求：

（1）数据的安全性。在NFC移动支付中，除了涉及商品内容和交易金额等信息外，还很多敏感信息。因此必须保证数据信息的安全。使攻击者无法获取该信息，即便被窃取也无法读取和破解出信息的具体内容。数据的安全性是移动支付安全的前提。

（2）身份的确认性。在移动支付过程中，交易双方要互相认证对方的身份，只有在确认对方身份之后才会进行数据交易、完成移动支付的过程。

（3）交易的不可抵赖性。不管是通过匿名化的假名，还是通过ID的方式完成交易，都能够唯一地确认交易双方的真实身份。在交易出现问题或者存在疑问的情况下，能够通过唯一的标识证明交易的真实性和不可抵赖性，从而对交易行为进行确认。

此外，在当前NFC移动支付技术实际应用过程中，还应注意的另外一个安全性问题就是数据容易被窃取，从而导致信息泄露，因此在实际应用过程中必须加强信息安全性，加强防御以应对外界不良攻击，在此基础上才能够保证其移动支付得到更好应用效果[13-14]。

3 基于国密技术的 NFC 通信模型

3．1 NFC 通信模型架构

NFC 移动支付即近场支付，这是一种非接触式的支付方式，NFC 移动支付的系统架构如图 1 所示。由图 1 可知，该 NFC 移动支付模型系统中各部分设计功能如下：

（1）移动终端：一般为在移动支付过程中，用户使用的支持 NFC 功能的移动支付设备。

（2）受理终端：通常为 pos 机或其他读取设备等，参与移动支付的商家所使用的终端设备。

（3）账户管理系统：如银行等，提供账务结算和资金管理的系统。

（4）TSM：如支付宝、手机钱包等，是第三方可信服务平台，可以实现移动支付的安全管理。

（5）安全单元：用于存储如交易过程中的关键数据，用户银行卡信息等的敏感数据或者用户隐私数据，确保数据的安全性和交易的不可否认性。

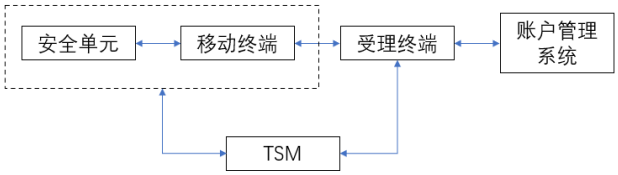

图 1 NFC 移动支付系统

4 NFC 移动支付安全方案设计

4．1 NFC 移动支付认证协议设计

本文提出的 NFC 移动支付认证协议设计思路是：利用数字签名技术、SM2、SM3 算法实现客户 NFC 手机 C、商家支付设备 D 和支付平台 T 三方之间的双向认证，使用私钥加密交易过程中的关键数据，用公钥获取交易过程中的关键数据。为了方面协议的介绍，首先对协议中用到的符号进行解释，表 1 所示。安全认证协议流程图设计如图 2 所示。

表 1 协议通信符号说明

符号	说 明
IDc	客户NFC手机C的身份信息
ID_D	商家支付设备D的身份信息
ID_T	支付平台T的身份信息
T	时间戳
H	杂凑值
E_{SK}	用私钥进行加密
D_{PK}	用公钥进行解密
TD	T产生的交易数据
Req C	客户NFC手机C的认证请求信息
ARQC	移动端发送的授权请求信息
ARPC	支付平台发送的授权确认信息
Password	支付密码
Pay	交易确认信息

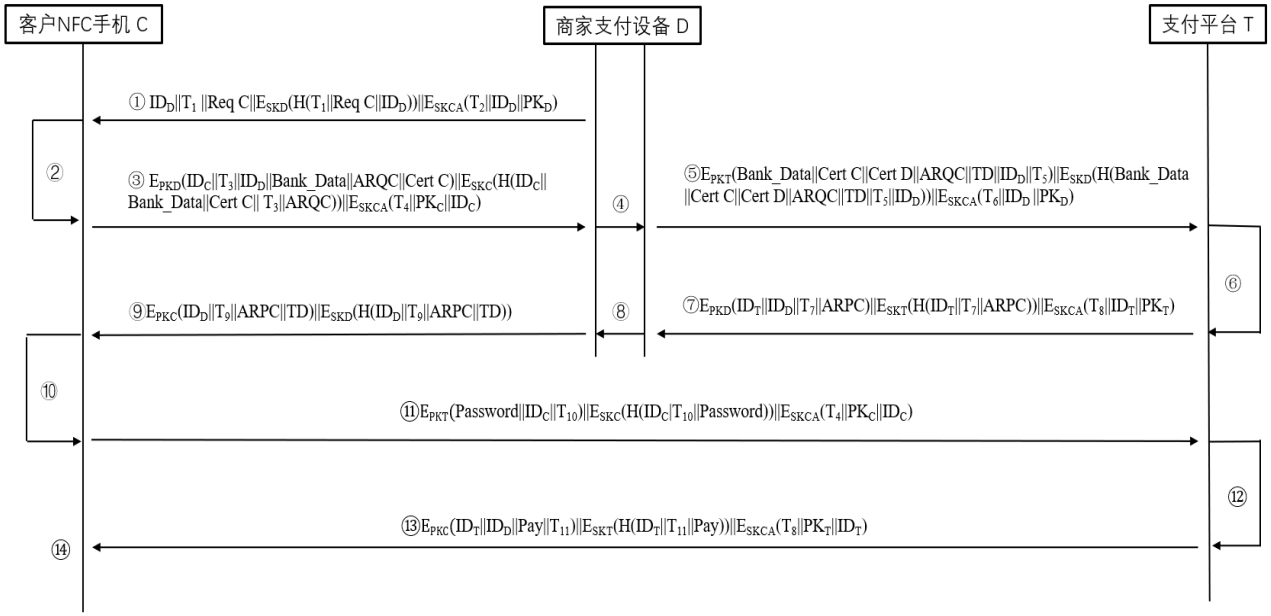

图 2 NFC移动支付认证协议流程图

4．2 NFC 移动支付认证协议流程图说明

（1）$ID_D||T_1||Req\ C||E_{SKD}(H(T_1||Req\ C||ID_D))||E_{SKCA}(T_2||ID_D||PK_D)$

商家支付设备D对身份ID_D、时间戳T_1、交易请求进行签名，并将其和商家支付设备D的CA签发的证书$E_{SKCA}(T_2||ID_D||PK_D)$一起发送给客户NFC手机。

（2）客户NFC手机C验证商家支付设备D的身份

① 客户NFC手机用CA公钥验证商家支付设备D证书:

$Cert\ D = D_{PKCA}[E_{SKCA}(PK_D||ID_D||T_2)] = T_2||ID_D||PK_D$

② 用商家支付设备D的公钥验证商家支付设备D的签名:

$H_1 = D_{PKD}[E_{SkD}(H(T_1||Req\ C||ID_D))] = H(T_1||Req\ C||ID_D)$

③ 客户NFC手机C计算哈希值$H2=H(T_1||Req\ C||ID_D)$。

④ 判断H_1、H_2是否相等，如果相等则确认对方就是商家支付设备D，否则交易中断。

（3）$E_{PKD}(ID_C||T_3||ID_D||Bank\_Data||ARQC||Cert\ C)||E_{SKC}(H(ID_C||Bank\_Data||Cert\ C||T_3||ARQC))||E_{SKCA}(T_4$

$||PK_C||ID_C)$ 。

客户NFC手机C向商家支付设备D发送身份ID_C、时间戳、C对客户NFC手机银行账户信息、授权请求的签名，以及CA签发给C的证书。

（4）商家支付设备D对客户手机C进行身份鉴别

① 验证用户NFC手机C证书的真实性:

$Cert\ C=D_{PKCA}[E_{SKCA}(T_4||PK_C||ID_C)]= T_4||PK_C||ID_C$

② 用C公钥验证C的签名:

$H_3=D_{PKC}[E_{SKC}(H(ID_C||Bank\_Data||Cert\ C||T_3||ARQC))]=H(ID_C||Bank\_Data||Cert\ C||T_3||ARQC)$

（3）商家支付设备D解密帐号信息并计算哈希值H_4

$D_{SKD}(E_{PKD}(ID_C||T_3||ID_D||Bank\_Data||ARQC||Cert\ C))=ID_C||T_3||ID_D||Bank\_Data||\ ARQC||Cert\ C$

$H_4 = H(ID_C||Bank\_Data||Cert\ C||T_3||ARQC)$

（4）判断H_3、H_4是否相等，如果相等则商家支付设备D确认对方就是客户手机C，否则无法确认对方的身份。

（5）$E_{PKT}(Bank\_Data||ARQC||TD||ID_D||T_5||Cert\ C||Cert\ D)||E_{SKD}(H(Bank\_Data||Cert\ C||Cert\ D||ARQC||\ TD||T_5||ID_D))||E_{SKCA}(T_6||ID_D\ ||PK_D)$

商家支付设备D向支付平台T发送身份ID_D、时间戳T_5、商家和客户之间的交易信息TD，以及③中生成的客户信息、CA签发的D的证书$E_{SKCA}(T_6||ID_D||PK_D)$ 。

（6）支付平台T鉴别商家支付设备D的身份鉴别

① 支付平台T校验D的证书:

$Cert\ D=D_{PKCA}[E_{SKCA}(ID_D\ ||PK_D||T_6)] = T_6||ID_D||\ PK_D$

② 用商家支付设备D的公钥验证D的签名得到哈希值:

$H_5 = D_{PKD}[E_{SkD}(H(Bank\_Data||Cert\ D||Cert\ C||ARQC||TD||\ T_5||ID_D))]$

$=H(Bank\_Data||Cert\ D||Cert\ C||ARQC||TD||T_5||ID_D)$

③ 支付平台T计算哈希值:

$D_{SKT}(E_{PKT}(Cert\ C||Cert\ D||Bank\_Data||ARQC||TD||ID_D||T_5))$

$=Cert\ C||Cert\ D||Bank\_Data||\ ARQC||\ TD||ID_D||T_5$

$H_6 = H(Bank\_Data||Cert\ C||Cert\ D||\ ARQC||TD||T_5||ID_D)$

④ 判断哈希值H_5、H_6是否相等，相等则确认对方就是商家支付设备D，否则交易中断。

（7）$E_{PKD}(ID_T||ID_D||T_7||ARPC)||E_{SKT}(H(ID_T||T_7||ARPC))||E_{SKCA}(T_8||ID_T||PK_T)$

支付平台T向商家支付设备D发送身份ID_T、时间戳7、授权确认信息以及CA签发的证书$E_{SKCA}(T_8||ID_T||PK_T)$ 。

（8）同（2）、（4）、（6）步骤，商家支付设备D对对方身份进行鉴别，鉴别通过则对方身份就是支付平台T。

（9）$E_{PKC}(ID_D||T_9||ARPC||TD)||E_{SKD}(H(ID_D\ ||\ T_9||ARPC||\ TD))$

商家支付设备D向客户手机C发送身份信息ID_D、时间戳9、授权确认信息、交易信息。

（10） 客户手机C对商家支付设备D发来的信息进行鉴别

① 用D的公钥验证D的签名:

$H_9 = D_{PKD}[E_{SPD}(H(ID_D||T_9||ARPC||TD))]$

$= H(ID_D||T_9||ARPC||TD)$

② C解密信息并计算哈希值H_{10}:

$D_{SKC}(E_{PKC}(ID_D||T_9||ARPC||TD))=ID_D||T_9||ARPC||TD$

$H_{10} = H(ID_D|T_9||ARPC||TD)$

③ 判断H_9、H_{10}是否相等，如果相等则确认该信息由商家支付设备D发送，否则无法确认该信息的来源。

（11）$E_{PKT}(Password||ID_C||T_{10})\ ||E_{SKC}(H(ID_C||\ T_{10}||\ Password))\ ||E_{SKCA}(T_4||PK_C||ID_C)$

客户手机C向支付平台T发送身份信息ID_C、时间戳T_{10}、支付密码以及CA签发的证书。

（12）同（2）、（4）、（6）步骤，支付平台T对对方进行身份鉴别，鉴别通过确认对方身份就是客户手机C。

（13）$E_{PKC}(ID_T||ID_D||Pay||T_{11})\ ||\ E_{SKT}(H(ID_T\ ||\ T_{11}||\ Pay))||E_{SKCA}(T_8||PK_T||ID_T)$

支付平台T向客户手机发送身份信息ID_T、时间戳11、交易确认信息Pay以及CA签发的证书E_{SKCA}（$T_8||PK_T||ID_T$)。

（14）同（2）、（4）、（6）、（8）、（12）步骤，客户手机C对消息发送方进行身份认证，确定是支付平台T发来的消息。

最后完成交易。

4．3 安全性分析

（1） 抵抗身份假冒攻击

本方案是由客户 NFC 手机 C、商家支付设备 D、支付平台 T 三方之间相互进行双向身份认证。CA 向

用户颁发已签名的证书。证书包含主体的公钥，只有有效主体才能获得与签名公钥对应的私钥。[19]。商家支付设备 D 发送 $ID_D||Req\ C||E_{SKD}(H(T_1||Req\ C||ID_D))||E_{SKCA}(T_2||ID_D||PK_D)$给客户手机 C。客户手机 C 通过运用商家支付设备 D 的公钥解密 $D_{PKD}[E_{SkD}(H(T_1||Req\ C||ID_D))]$，并计算哈希值是否等于 $H(T_1||Req\ C||ID_D)$来认证 D 的身份。如果相等则表明消息是来自于商家支付设备 D。同样的，商家支付设备 D 通过计算 $D_{PKC}[E_{SKC}(H(ID_C||\ Bank\_Data\ ||Cert\ C||T_3||ARQC))]$ 是否等于 $H(ID_C||\ Bank\_Data\ ||Cert\ C||T_3||ARQC)$，来验证消息是否来自客户手机。由此，C、D 之间实现双向身份认证，C 与 T、D 与 T 之间同理。

如果要仿造签名，则需要从获取对方公钥所对应的私钥，而私钥则是不公开，只有拥有者自己知道。因此签名方只要保管好自己的私钥，其他人就无法伪造签名，从而达到防假冒攻击的作用[15]。

（2） 抵抗重放攻击

在每次的交易信息交互时，每个设备都会产生一个时间戳，并且所产生的时间戳要经过交易方的验证是否正确，$ID_D||T_1||Req\ C||E_{SKD}(H(|T_1||Req\ C||ID_D))||E_{SKCA}(T_2||ID_D||PK_D)$消息中包含了由密文传输的时间戳，因此，如果攻击者重放一条来自之前商家支付设备 D 的消息，客户手机能够通过计算 $D_{PKD}[E_{SKD}(H(T_1||Req\ C||ID_D))]$来验证$|T_1$ 是否一致，只有在验证正确之后才能进行下一步，因此应当能抵御重放攻击。

（3） 抵抗数据窃密攻击

在双方进行敏感数据传输时，为了保证敏感数据不被窃取，采用了公钥加密算法进行保护，例如第 3 步：$E_{PKD}(ID_C||T_3||ID_D||Bank\_Data||ARQC||Cert\ C)$.....，手机就向商家支付设备发送银行账户等敏感数据时，就使用商家支付设备 D 的公钥加密敏感信息，黑客要通过解密得到银行账户信息时，就得取得商家支付设备 D 的私钥，从公钥得到私钥就需要解决椭圆曲线上的离散对数问题，迄今为止还没有解决这个难题，所以，协议保护了数据不被非法接收方获取。

（4） 抵抗数据篡改和业务否认攻击

协议在双向身份认证时,身份信息使用私钥签名，商家支付设备 D 在与客户手机 C 相互认证 $ID_D||T_1||Req\ C||E_{SKD}(H(T_1||Req\ C||ID_D))||E_{SKCA}(T_2||ID_D||PK_D)$，如果黑客改变了身份信息 ID_D，那么在计算哈希值时，$H_1=H(T_1||Req\ C||ID_D)$的哈希值就会改变，即与验证签名时 H_1 不等于 H_2，则客户手机可以判断出对方不是合法的商家支付设备 D，那么客户手机 C 就会中断交易。

同理，在信号 $ID_D||T_1||Req\ C||E_{SKD}(H(|T_1||Req\ C||ID_D))||E_{SKCA}(T_2||ID_D||PK_D)$中，由于商家支付设备计算了 $T_1||Req\ C||ID_D$ 的哈希值，并用私钥进行了加密，即得到了商家支付设备 D 对信息 $T_1||Req\ C||ID_D$ 的签名，如果今后商家支付设备否认发出此信号给用户手机，那么任何人都可以用商家支付设备的公钥对签名进行验证，如果通过签名验证，则商家支付设备 D 就无法否认向用户手机发出过 $T_1||Req\ C||ID_D$ 信号。

4．4 方案比较

参照 GB/T39786-2021《信息安全技术 信息系统应用基本要求》，我们将本文提出的方案与参考文献[16]、[17]提出的方案进行了多方面比较。基于 NFC 的移动支付过程的安全通信实验环境是利用 X shell 终端仿真软件及 GmSSL 加密工具包实现的。Xshell 可以使用国密算法对 SSH 连接进行加密和认证，保护用户的数据安全；同时，Xshell 还支持使用国密 NFC 进行身份认证，可以通过读取用户设备 NFC 标签来验证用户的身份，从而提高系统的安全性。而 GmSSL 可以用于生成和验证数字证书，保证支付过程中的身份认证和数据完整性。GmSSL 还可以用于生成和验证数字签名，确保支付指令的真实性和不可抵赖性。此外，GmSSL 还支持 SM4 算法，可以用于加密和解密支付数据，保证支付过程中的数据保密性。

方案对比结果如表 2 所示。从对比的结果来看，文献[16]使用 MD5 密码算法且没有提供双向认证，存在安全缺陷；文献[17]使用 NFC 技术将 SIM 卡中存储的身份信息与读取设备进行交互，以验证用户的身份，没有提供双向认证，仅能抵御篡改、重放攻击。本文的方案提供双向认证，采用国密算法 SM2、SM3、SM4，能够有效抵御篡改、假冒、重放攻击，安全性高。

表 2 各身份认证方案安全性能比较

安全性能	文献[16]方案	文献[17]方案	本文方案
身份验证	AES	SM卡	数字签名、数字证书
密码算法	MD5	无	SM2、SM3、SM4
安全协议	有	有	有
抵抗篡改攻击	否	能	能
抵抗假冒攻击	否	否	能
抵抗重放攻击	否	能	能
提供双向认证	否	否	能

5 结束语

为了保障用户的资金安全，需要采用更加安全可靠的支付方式。本文提出了一种基于国密技术的 NFC 移动支付双向认证模型系统，旨在提高移动支付的安全性和可靠性。该系统通过 Linux 操作系统实现双向身份认证，鉴别通信双方身份的功能，实现在传输过程关键交易数据的完整和不可被窃取。NFC 移动支付认证协议的安全性分析表明，本文系统对于抵抗窃听、假冒、重放以及篡改等攻击都有很好的效果。

参 考 文 献

[1] CNNIC.第 50 次中国互联网络发展状况统计报告[R].中国互联网络信息中心,2022.

[2] 王亮.针对 NFC 移动支付的安全问题探讨[J].知识经济,2018,464(11):38-39..

[3] 余浩.面向 NFC 移动支付的安全技术研究[D].广州：广东工业大学,2019

[4] Sethia D, Gupta D, Saran H.NFC Secure Element-Based Mutual Authentication and Attestation for IoT Access[J].IEEE Transactions on Consumer Electronics, 2018,64(4): 470-479.

[5] Fahrianto F , Lubis M F , Fiade A. Denial-of-service attack possibilities on NFC technology[C]//4th International Conference on Cyber & It Service Management. IEEE, 2016:1-6

[3] A Manjeshwar，D P Agrawal. TEEN:A protocol for enhanced efficiency in Wireless Sensor Networks[C]. The 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing. San，Francisco，CA，2001:2009-2015

[4] Younis. O, Fahmy. S. HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks[J]. IEEE Transactions on Mobile Computing, Volume 3, Dec. 2004: 366-379.

[5] Handy MJ, Haase M, Timmermann D. Low energy adaptive clustering hierarchy with deterministic cluster-head selection[C]. In: Proc. of the 4th IEEE Conf. on Mobile and Wireless Communications Networks. Stockholm: IEEE Communications Society, 2002:368−372.

[6] 闵晓玲.基于 NFC 技术的移动支付安全应用研究[J]. 网络安全技术与应用. 2017,(12):97-98

[7] 金志刚，解冰珊.一种高安全的融合指纹识别与 NFC 技术的门禁系统认证协议[J].南开大学学报(自然科学版). 2017,50(05):1-7

[8] 陶克，程玉柱.NFC 技术在 AFC 系统中的安全研究[J].都市快轨交通. 2019,32(05):133-137

[9] 李艳俊,汪书北,杨晓桐.基于移动端的轻量级 NFC 安全认证方案[J].计算机工程与应用. 2020,56(16):84-89

[10] 韦永霜,陈建华,韦永美.基于椭圆曲线密码的 RFID/NFC 安全认证协议[J].信息网络安全. 2019(12):64-71

[11] 李江海,方舟,刘皖熠.面向 NFC 的安全轻量级芯片[J].物联网技术. 2020,10(11):7-8

[12] 赵兴文,段懿入.基于假名的 NFC 安全支付认证协议[J].信息安全研究. 2022,8(12):1178-1186

[13] 徐苏宁.NFC 与移动支付安全专利技术分析[J].中国新通信，2015.

[14] 董钢，王泽芳，刘陈.基于 NFC 技术的手机移动支付模式探析[J].科学咨询(科技·管理)，2012.

[15] 吕良,李瑞. 基于数字签名和 SM2 算法的终端接入认证协商协议[J]. 计算机与数字工程,2021,49(3):530-535

[16] 潘雪峰.基于 NFC（近场通信技术）的“智能卡包”系统模型的设计和研究[D].上海：华东师范大学,2014.

[17] 秦亮. 基于 802.1x 协议网络认证系统的设计与实现[D].武汉：华中科技大学,2006.