基于国密技术的金融 IC 卡交易系统模型设计*

廖林梅　李雁星　陈积常**　李建

南宁学院信息工程学院，南宁 530200

摘 要 分析目前金融交易系统存在的身份假冒、数据篡改、敏感信息窃取、交易业务否认、数据重放等安全风险，提出基于 SM2/SM3/SM4 商用密码算法的应用需求，构建基于国家商用密码算法的金融 IC 卡交易系统安全模型，设计了金融 IC 卡交易系统安全通信协议。在现有的工作流程中，使用国家商用密码技术来改进金融 IC 卡交易模型，通过使用 Linux 系统，在系统上安装 Gmssl 国密工具箱，搭建了金融 IC 卡交易系统运行环境，实现了数据的安全传输。协议的安全性分析和评估分析表明：该金融 IC 卡交易系统模型能够抵御黑客发动的主动攻击和被动攻击，安全性达到了求椭圆曲线离散对数的水平。

关键字 金融 IC 卡交易系统，国家商用密码算法，安全模型，通信协议

Design of Financial IC Card Transaction System Model based on National Commercial Password Technology

Liao Linhai　Li Yanxing　Chen Jichang　Li Jian

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

Abstract—This paper analyzes the financial transaction system with current design flaws and security risks in the technology used. A security model for the financial IC card transaction system based on the national commercial cryptographic algorithm is constructed, and a secure communication protocol for the financial IC card transaction system is designed. In the existing workflow, national commercial encryption technology is used while improving the financial IC card transaction model. By using Linux system and installing Gmssl national encryption toolbox on the system, the operating environment of the financial IC card transaction system is established, achieving secure data transmission. Security analysis shows that the financial IC card trading system model can resist active and passive attacks launched by hackers, and its security reaches the level of finding the discrete logarithm of an elliptic curve.

Keywords—Financial IC card trading system, National commercial password algorithm, security model, communication protocol

1 引　言

为了保护密码安全和国家安全，我国自主研发一系列的商用密码算法，并制定相关的法律法规，以国家标准和行业标准贯彻实施[1]。但是，由于国家商用密码每一款都不一样，如何结合这些算法和技术搭建安全模型，让模型应用于适当的场合，还是非常值得研究的问题[2]。

从 2013 年开始，银行金融 IC(Integrated Circuit Card)卡系统的密码技术从国际密码算法逐步换为使用商用密码算法[3-4]。截至 2020 年底，全国累计发行支持商用密码算法的金融 IC 卡规模超十亿量级，网银证书设备规模超亿量级，银联转接清算系统、二代支付系统、二代国库信息处银联转接清算系统、二代支付系统、二代国库信息处理系统等金融基础设施也累计与千家银行机构实现商用密码接入，满足了银行卡安全、便捷的需要[5-7]。

随着互联网技术的飞速发展，人们可以很方便地在移动设备或者终端设备上输入数据，传输到服务器端进行存储。但是从设备到服务器这段传输过程有可能被黑客被动攻击，通过分析获得的数据再进行主动攻击，所以，金融 IC 卡交易系统安全模型应用具备要防范主动攻击和被动攻击的功能。此外，密码技术已经广泛应用于银行金融 IC 卡系统中，像手机密码、银行卡密码、支付密码等这些重要的密码一旦泄露，将会造成信息泄露和系统瘫痪，使银行的金融交易系统面临极大的挑战和风险[8-10]。

*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

本文通过对国家密码算法的研究，使用国家商用密码算法技术构建一个金融 IC 卡交易系统安全模型，通过分析其安全需求，设计数据传输安全协议，并从理论上，分析该协议能够在数据传输中可以高程度地防御主动攻击和被动攻击。

2 系统安全模型需求分析

金融 IC 卡交易系统安全模型的功能需求如下：

● 身份鉴别需求。金融 IC 卡交易系统设备与服务器之间进行数据传输时需要进行身份鉴别，保证通信时双份身份的真实性，防止非法第三方冒充设备或者服务器做一些非法操作，满足金融 IC 卡交易系统防主动攻击的需求。

● 数据传输的完整性和安全性需求。服务器与设备之间进行数据传输时，由于设备本身就不安全或者通信信道不安全，需要使用密码加密技术保证在传输过程中数据的完整性和机密性保护，防止数据被非法窃取到后被解析或者将数据篡改后发送给接收方，满足金融 IC 卡交易系统防主动攻击和被动攻击的需求。

● 重放数据的鉴别需求。由于数据可能会被窃取，该数据未经更改时是有效的，如果黑客将该数据再次发送到接收方，如果接收方不能识别该数据为重放数据，将会带来严重后果，所以需要有鉴别重放数据的需求，满足金融 IC 卡交易系统防主动攻击的需求。

3 安全模型整体设计

3．1 系统整体架构与密码应用部署

金融 IC 卡交易系统是用于读取金融 IC 卡信息，并对信息进行验证，负责接收 IC 卡交易请求信息，并把请求信息发送给发卡侧进行交易处理，交易系统由 IC 卡前置应用服务器、收单前置应用服务器、受理终端设备三部分组成，对高并发处理尤其要求高。为了防范黑客假冒用户和防范数据被获取并解密等风险，系统密码应用方案设计重点在与 IC 卡前置应用对收单前置应用收集到的 IC 卡信息进行身份鉴别，以及交易数据在传输过程中的安全性和保密性保护。

金融 IC 卡交易系统安全模型可归结为一个层次模型，分为终端设备层、集中收集信息层、安全验证和交易处理层，三层模型之间互相依赖和提供支持。金融 IC 卡交易系统安全模型整体架构和部署设计图如图 1 所示。三层的功能部署如下：

● 终端设备层（ATM、POS 机等）：负责读取金融 IC 卡信息，通过与金融 IC 卡、收单前置服务器通信交互，实现金融交易信息和密钥信息的传输、处理，包括 ATM 机、POS 机等。

● 集中收集信息层（收单前置应用服务器）：负责接收、处理或转发受理终端设备的交易请求信息，并向受理终端设备返回交易结果信息。

● 安全验证和交易处理层（IC 卡前置应用服务器）：负责接收、处理金融 IC 卡交易请求信息，完成金融 IC 卡业务预处理功能，包括安全报文验证、应用密文验证及产生、金融 IC 卡柜面类业务等。

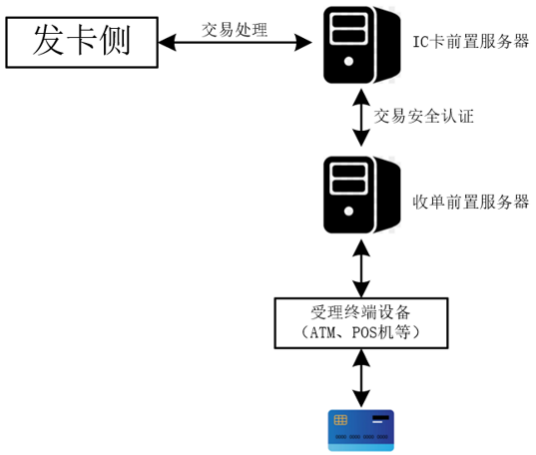

图 1 金融 IC 卡交易系统整体架构和部署图

3．2 密钥体系及其功能

(1) 系统的对称密钥

金融 IC 卡交易系统对称密钥遵循经典的三层密钥体系，有金融数据密码机主密钥 MK、终端主密钥 TMK 和 MAC 计算密钥 MAK，PIN 加密密钥 PIK。

● 金融数据密码机主密钥 MK：保存在金融数据密码机内的顶层密钥，起作用是将所有存放在本地的其他密钥和待加密数据进行加密，在金融数据密码机以外的地方不会以明文形式存放，是三级密钥体系中最高级别的密钥；生成其他密钥并对其他密钥进行加密保护。

● 终端主密钥 TMK：用于保护需要传输的工作密钥，实现工作密钥的联机实时传输或其他形式的异地传输，它在本地存放时，处于本地 MK 的加密保护下。

● MAC 计算密钥 MAK，PIN 加密密钥 PIK：通常称为数据加密密钥或工作密钥，用于加密交易数据中的 PIN（使用 PIK）和对交易数据做 MAC 校验（使用 MAK），从而实现身份鉴别和传输数据的保密性、完整性保护。示例：不能用如下做标题：

(2) 非对称密钥体系

金融 IC 卡系统涉及的非对称密钥体系基于 PKI 技术实现，分为三层证书体系。

● CA 公钥：CA 证书是非对称密钥体系的信任源。CA 为发卡行提供证书服务器，负责受理发卡行证书申请，签发发卡行证书。

● 发卡行签名密钥对：发卡行证书是发卡行合法性标识，用于发卡行的身份鉴别。公钥有 CA 签发后形成发卡行证书，私钥存放在金融数据密码机内。用于签发 IC 卡静态数据签名及 IC 卡数字证书。

● IC 卡签名密钥对：IC 卡证书是 IC 卡合法性标识，用于金融 IC 卡真实性和完整性的鉴别。采用脱机数据认证方式的卡片需要此密钥对，公钥由发卡行私钥签发形成 IC 卡证书，存储在 IC 卡中，私钥存放在 IC 卡内部。

4 密码应用工作流程

4．1 系统通信协议流程设计

为了叙述金融 IC 卡交易系统通信协议流程，首先对通信协议中用到的符号进行解释，表 1 所示。

基于国家商用密码算法、对称/非对称密钥密码技术、数字证书、数字签名、证书发放机构（ CA ）、公开密钥的安全策略等技术设计 IC 卡交易系统协议流程图，如图 2 所示。

表 1 协议通信符号说明

符号	说 明
ID_N	发卡行N身份
ID_B	受理终端设备B身份
ID_Y	IC卡Y身份
T	时间戳
H	杂凑值
||	拼接操作
PK_{CA}	证书机构CA用SM2算法的公钥
PK_N	发卡行N用SM2算法的公钥
PK_B	受理终端设备B用SM2算法的公钥
PK_Y	IC卡Y用SM2算法的公钥
SKN	发卡行N用SM2算法的私钥
SKB	受理终端设备B用SM2算法的私钥
SKY	IC卡Y用SM2算法的私钥
O	使用数据认证算法生成认证码
KMC	发卡行主密钥
PIK	PIN加密密钥
arqc	授权请求报文
arpc	授权响应报文
Request	请求IC卡发送认证信息
file	IC卡信息

4．2 通信协议流程图说明

（1） $T_1||ID_B||C_1||E_{SKB}[H(ID_B||T_1)]||E_{SKCA}(T_2||ID_B||PK_B)$

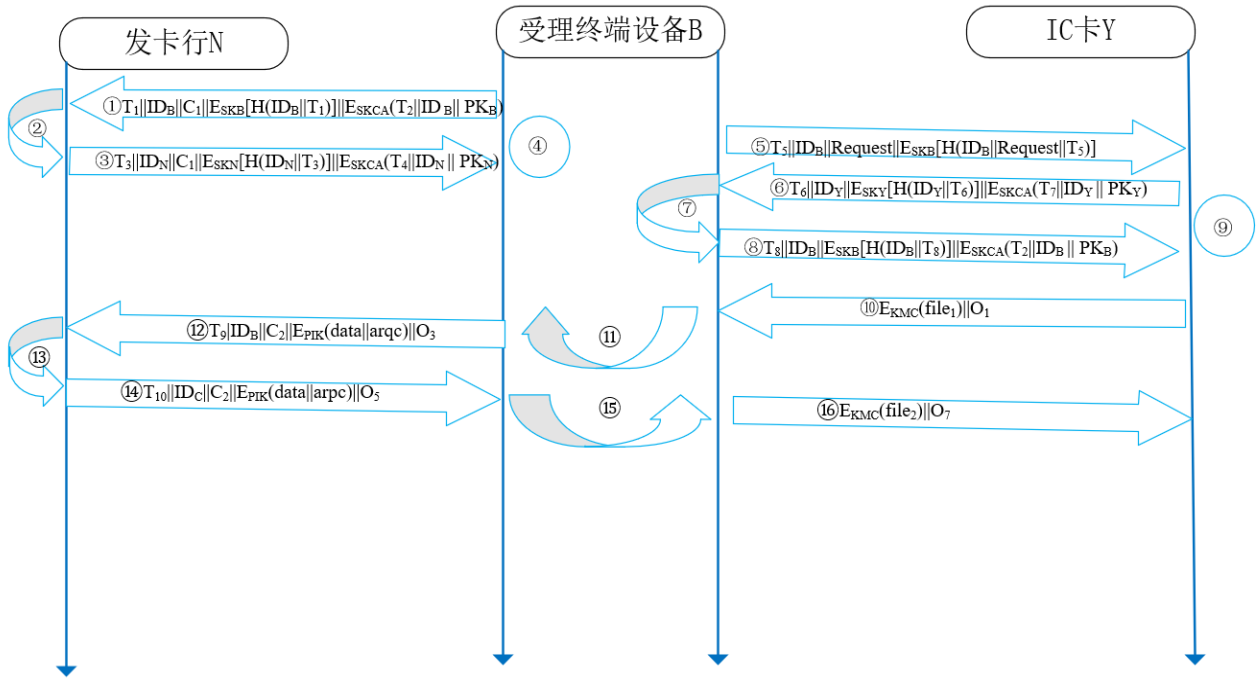

图 2 交易系统通信协议流程图

受理终端设备B向发卡行N发送时间戳、发送计数C1、B对$ID_B||T_1$的签名，以及CA签发的B的证书。

（2）发卡行N对对方进行身份鉴别的过程如下：

① 发卡行用证书中心CA的证书验证B证书的真实性并取得B的公钥(PK_B)。

$CertM=D_{PKCA}[E_{SKCA}(T_2||ID_B||PK_B)]=T_2||ID_B||PK_B$

② 用受理终端设备B公钥验证B的签名并取得对$ID_B||T_1$的哈希值。

$H_1=D_{PKB}[E_{SKB}(H(ID_B||T_1))]=H(ID_B||T_1)$

③ 发卡行N使用ID_B和T_1计算哈希值H_2。

$H_2=H(ID_B||T_1)$

④判断H_2、H_1是否相等，如果相等则发卡行N确认对方就是受理终端设备B，否则无法确认对方的身份。

（3） $T_3||ID_N||C_1||E_{SKN}[H(ID_N||T_3)]||E_{SKCA}(T_4||ID_N||PK_N)$

发卡行N向终端设备B发送身份、时间戳、发送计数C、N对$(ID_N||T_3)$的签名，以及CA签发的N的证书。

（4）终端设备B对对方进行身份鉴别：

① 用证书中心CA的证书验证N证书的真实性并取得N的公钥(PK_N)。

$CertC=D_{PKCA}[E_{SKCA}(T_4||ID_N||PK_N)]=T_4||ID_N||PK_N$

② 发卡行N的公钥验证N的签名并取得对IDN||T3的哈希值。

$H_3=D_{PKN}[E_{SKN}(H(ID_N||T_3))]=H(ID_N||T_3)$

③ 终端设备B计算哈希值$H4=H(ID_N||T_3)$ 。

判断H_3、H_4是否相等，如果相等终端设备B则确认对方就是发卡行N，否则无法确认对方的身份。

（5）$T_5||ID_B||Request||E_{SKB}[H(ID_B||Request||T_5)]$

终端设备 向IC卡Y发送信息请求IC卡发送认证数据

（6）$T_6||ID_Y||E_{SKY}[H(ID_Y||T_6)]||E_{SKN}(T_7||ID_Y||PK_Y)$

IC卡Y向终端设备B发送身份、时间戳、Y对$ID_Y||T_6$的签名，以及发卡行N签发的Y的证书。

（7）终端设备B对对方进行身份鉴别：

①用发卡行N的公钥证书验证Y证书的真实性并取得Y的公钥

② 用IC卡Y的公钥验证Y的签名。

③ B计算哈希值。

④判断哈希值是否相等，如果相等终端设备B则确认对方就是IC卡Y，否则无法确认对方的身份。

（8）$T_8||ID_B||E_{SKB}[H(ID_B||T_8)]||E_{SKCA}(T_2||ID_B||PK_B)$

终端设备B向IC卡Y发送身份、时间戳、B对$ID_B||T_7$的签名，以及CA签发的B的证书。

（9）同（2）、（4）、（6）步骤：IC卡Y对对方进行身份鉴别；鉴别通过确认对方就是终端设备B。

（10）$E_{KMC}[file_1]||O_1$

IC卡Y向终端设备B发送IC卡信息。

（11）终端设备B收到后，使用KMC解密获取到IC卡信息：

$D_{KMC}[E_{KMC}(file_1)]=file_1$

生成$O_2 = E_{KMC}(file_1)$ 。

通过对比O_1和O_2，如果相等，证明数据在传输中未发生改变。

（12）$T_9||ID_B||C_2||E_{PIK}(data||arqc)||O_3$

受理终端设备B向发卡行N发送交易报文和arqc和数据认证算法生成的O_3。

$O_3=E_{MAK}(data||arqc)$

（13）发卡行N收到后

使用PIK解密获取到交易报文data和arqc

$D_{PIK}[E_{PIK}(data||arqc)]=data||arqc$

生成$O_4 = E_{MAK}(data||arqc)$。

通过对比O_3和O_4，如果相等，证明数据在传输中未发生改变。校验arqc成功则说明对方拥有udk。

（14）$T_{10}||C_2||ID_N||E_{PIK}(data||arpc)||O_5$

发卡行N向受理终端设备B发送处理结果和arpc和O_5。

（15）受理终端设备B收到后，使用PIK解密获取到处理结果data和arpc

$D_{PIK}[E_{PIK}(data||arpc)]=data||arpc$

生成$O_6= E_{MAK}(data||arpc)$。

通过对比O_5和O_6，如果相等，证明数据在传输中未发生改变。校验arpc成功则说明对方拥有udk。

（16）$E_{KMC}[file_2]||O_7$

交易成功后，受理终端设备B将更改过的IC卡信息，使用KMC加密，发送给IC卡Y中。

4．3 安全性分析

（1） 数字证书安全性分析

网络技术的飞速发展使得它在各行各业的广泛应用，让人们可以足不出户，在手机和电脑上就可以完成许多事情，但也带来了许多安全问题，身份认证是保障网络安全的一种重要手段，数字证书又是身份认证中重要的一环。

用户自己生成公私钥对时，可以将公钥和身份信息等数据生成一个证书请求发送给证书授权中心(CA)等第三方受信任的机构，证书授权中心可以用它的私钥为用户签发证书，然后发送给用户，用户就可以通过这个证书和私钥来证明自己的身份。

由于证书是由证书授权中心的私钥加密的，所以只能用证书授权中心的公钥解密，如果我们用一个受信任的第三方机构的公钥解密了证书，就说明该证书的信息是经过认证的，除非该机构的私钥被窃取，否则证书是不能伪造的。

（2） 使用到的商用密码算法安全分析

① SM2 椭圆曲线算法和传统 RSA 算法比较：

一是加密程度更高，传统 SSL 证书通常是 RSA 算法，RSA 是目前最有影响力和最常用的公钥加密算法，它能够抵抗到目前为止已知的绝大多数密码攻击，已被 ISO 推荐为公钥数据加密标准，但随着密码技术和计算机技术的发展，目前 1024 位 RSA 算法已经被证实存在被攻击的风险，美国国家标准技术研究院在 2010 年要求全面禁用 1024 位 RSA 算法，并升级到了 2048 位 RSA 算法。我国现阶段使用的国密 SM2 算法是在椭圆曲线密码理论基础进行改进而来，其加密强度比 RSA 算法（2048 位）更高。

二是安全性能更强，作为传统 SSL 证书的核心算法，RSA 算法虽然仍占据着 SSL 证书市场的主流地位，但是随着计算机技术的发展，加上对因子分解的改进，对低位数的密钥攻击已成为可能，传统的 SSL 证书也面临着更多的未知风险。而基于 ECC 椭圆曲线算法的 SM2 算法，则普遍采用 256 位密钥长度，它的单位安全强度相对较高，在工程应用中比较难以实现，破译或求解难度基本上是指数级的。因此，SM2 算法可以用较少的计算能力提供比 RSA 算法更高的安全强度，而所需的密钥长度却远比 RSA 算法低。此外，若要不断提高安全强度，则必须增加密钥长度，SM2 算法密钥长度增长速度较慢（例如：224-256-384），而 RSA 算法密钥长度则需呈倍数增长（例如：1024-2048-4096），这使得 SM2 算法的安全性能表现更佳。

三是传输速度更快，在通讯过程中，更长的密钥意味着必须来回发送更多的数据以验证连接。256 位的 SM2 算法相对于 2048 位的 RSA 算法可以传输更少的数据，也就意味着更少的传输时间，在 Web 服务器中采用 SM2 算法，Web 服务器新建并发处理响应时间比 RSA 算法快十几倍。

② SM3 是一种密码散列函数标准，由国家密码管理局于 2010 年 12 月 17 日发布。在商用密码体系中，SM3 主要用于数字签名及验证、消息认证码生成及验证、随机数生成等，其算法公开。据国家密码管理局表示，其安全性及效率与 SHA-256 相当。对长度位 L（L<264）比特的消息 m，SM3 杂凑算法经过填充、迭代压缩、生成杂凑值，杂凑值输出长度为 256 比特。SM3 算法采用 Merkle-Damgard 结构，消息分组长度为 512 位，摘要值长度为 256 位。MD5 输出 128 比特杂凑值，输出长度太短，影响其安全性。SHA-1 算法的输出长度为 160 比特，SM3 算法的输出长度为 256 比特，因此 SM3 算法的安全性要高于 MD5 算法和 SHA-1 算法。SM3 算法的压缩函数与 SHA-256 的压缩函数具有相似的结构,但是 SM3 算法的设计更加复杂,比如压缩函数的每一轮都使用 2 个消息字。现今为止，SM3 算法的安全性相对较高。

③ SM4 分组密码算法是一种对称加密算法。其分组长度为 128bit，密钥长度也为 128bit。加密算法与密钥扩展算法均采用 32 轮非线性迭代结构，以字（32 位）为单位进行加密运算，每一次迭代运算均为一轮变换函数 F。SM4 算法加/解密算法的结构相同，只是使用轮密钥相反，其中解密轮密钥是加密轮密钥的逆序。要保证一个对称密码算法的安全性的基本条件是其具备足够的密钥长度，SM4 算法与 AES 算法具有相同的密钥长度分组长度 128 比特，因此在安全性上高于 3DES 算法。

（3） 时戳作用分析

时间戳主要是用来防止重放攻击的，发送端通过在信息中放入明文时间戳和密文时间戳，接收方通过解密密文时间戳，通过和明文时间戳对比可以知道该时间戳没有被修改，再通过接收到的时间进行比较，可以知道该信息是否是重放攻击，但是双方需要较高程度的时间同步。

（4） 数字签名安全性分析

数字签名是对需要完整性保护的数据进行哈希运算，得到数据的哈希值，发送方使用它的私钥对哈希值进行加密，得到数字签名，接收方使用发送方的公钥对数字签名进行解密，得到发送前数据的哈希值，然后对数据进行同样的哈希运算，得到另一个哈希值，通过比较两个哈希值，可以知道数据是否被篡改。除非发送方的私钥被窃取，否则数字签名无法被伪造。数字签名可以让接收方知道发送方的身份及数据是否被篡改，实现可认证性和不可抵赖性。

（5） 抗虚假 IC 卡攻击

ATM 机读取 IC 卡中的数据，使用 KMC 密钥对数据中的数据段生成摘要，通过对比数据中的摘要段可以知道 IC 卡中的数据是否被篡改，同时也可以知道该 IC 卡是否有效，如果该 IC 卡是虚假 IC 卡，那么使用 KMC 密钥生成的摘要就会跟 IC 卡中的摘要不一致。

5 结束语

本文基于国家商用密码技术，构建了使用国家商用密码技术的金融 IC 卡交易系统模型，设计了金融 IC 卡交易系统安全通信协议，并从数据传输和身份鉴别两个方面设计密码应用工作流程。该协议把现有流程中使用的国外密码技术更换成国家商用密码技术，同时改进金融 IC 卡交易模型。安全性分析表明：该金融 IC 卡交易系统模型能够抵御黑客发动的主动攻击和被动攻击，安全性达到了求椭圆曲线离散对数的水平。我们还使用 Linux 系统，在系统上安装 Gmssl 国密工具箱，搭建金融 IC 卡交易系统运行环境，并使用 C++ 语言网络编程技术编写服务器，实现了数据的安全传输。

参 考 文 献

[1] 张一梅.国产商用密码算法应用研究[J].网络安全技术与应用,2023(04):23-25.

[2] 马壮壮,王伟,刘叶翔.商用密码算法在网络安全保护中的应用[J].无线互联科技,2023,20(06):146-150

[3] 张鑫.浅谈新密评标准下商用密码应用[J].中国信息化,2021(12):91-92

[4] 阳青松,王志斌.长沙银行国产密码金融 IC 卡商用起航[J].金融电子化,2015,(3):82-84

[5] 赵本阳.商业银行发展金融 IC 卡行业应用探究[J].上海金融,2011(09):94-98.

[6] 曾伟.推进金融 IC 卡国密算法应用关注的问题[J].金融科技时代,2021,29(04):87-89+92

[7] 李海.地铁金融 IC 卡系统的设计与实现[D].成都:电子科技大学,2020.

[8] 张震.城市商业银行金融 IC 卡系统的设计与应用[D].河北工业大学,2017

[9] 刘永清.IC 卡安全性研究与应用分析[J].江苏通信,2021,37(04):112-116

[10] 金融 IC 卡应用与安全[J].中国信用卡,2017(03):8.