基于国密技术的金融 IC 卡发卡系统模型设计*

梁卓山　　李雁星　　李建**

南宁学院信息工程学院，　南宁　530200

摘 要　通过分析目前银行的发卡系统存在的漏洞和面临的安全威胁，构建出基于国密技术的金融 IC 卡发卡系统框架，设计发卡系统安全协议，分析了协议的安全性。系统模型采用 C/S 架构，分为 CA 服务器、密钥管理服务器、数据库服务器、IC 卡业务管理服务器、数据准备服务器、个人化应用等六个部分，使用 SM2 签名算法、SM3 哈希算法、SM4 对称分组密码算法来保护发卡系统信息安全。安全性分析和性能比较结果表明，该发卡系统模型功能正常，安全性能稳定。

关键字　金融 IC 卡发卡系统，PKI 技术，国家商用密码算法，数字签名

Design of Financial IC Card Issuing System Model based on National Commercial Cryptographic Technology

Liang Zuoshan　Li Yanxing　Li Jian

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

Abstract—This paper analyzes the security threats and vulnerabilities faced by the current bank's card issuance system, constructs a financial IC card issuance system framework based on national cryptographic technology, designs a card issuance system security protocol. The system model adopts a C/S architecture and is divided into six parts: CA server, key management server, database server, IC card business management server, data preparation server, and personalized application. This model uses SM2 signature algorithm, SM3 hash algorithm and SM4 symmetric Block cipher algorithm to protect the information security of the card issuing system. The security analysis and performance comparison results indicate that the card issuing system model functions normally and the security performance is stable.
Keywords—Financial IC card issuing system, PKI technology, National commercial cryptographic algorithm, digital signature

1 引　言

随着计算机和网络技术的发展，我国金融业进入了信息化时代，目前，各家银行都在贯彻执行《中华人民共和国密码法》，并大力推进 GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》落地实施。如何保护银行信息系统的安全成为重要研究课题。

伴随着银行 IC 卡产业升级，非接触式金融 IC 卡的发卡量将逐步增加[1]。国内外不少学者对发卡系统和身份认证的研究，如文献[2]设计了基于 RSA 和 DES 算法的发卡系统，文献[3]研发了金融 IC 卡证书签发系统，文献[4]设计开发了金融 IC 卡密钥管理系统。

文献[5]使用 MD5、SHA1 生成用于身份认证的摘要。文献[6]研究了银行卡交易量与金融 IC 卡在多个行业的应用。这些研究均运用了国外的存在安全漏洞的算法，安全性不足以满足要求。因此，开发一个基于国家商用密码算法的银行卡发卡系统成为了当务之急。

中国人民银行一直致力于推动国密算法在金融领域的应用，以期使金融安全可控，摆脱对国外技术和产品的过度依赖，建设金融网络安全环境，增强我国金融信息系统的安全可控[7]。国家商用密码管理办公室从国家信息安全的角度出发，制定了一系列国家商用密码算法标准[8]。人们也在广泛开展国家商用密码算法的应用，如文献[9]研究了基于国密算法证书的多 CA 统一平台关键技术，文献[10]研究了基于国密算法的智能移动终端安全防护技术。

本文在分析目前银行卡发卡系统面临的安全威胁，以及现有应用系统存在的问题和漏洞的基础上，构建了一个基于国家商用密码技术的银行发卡系统安全模型，设计了相应的密码应用的安全协议，并对其安全性进行分析。最后，通过安全性分析和性能对比分析，验证所提出模型的可行性和安全性。

*基金资助：本文得到南宁学院一流专业培育项目(2020YLZYPY01) 和南宁学院教学质量与教学改革工程项目《网络安全》核心课程（2022BKHXK09）资助。
**通讯作者：李建，教授，943667593@qq.com

2 金融 IC 卡发卡系统安全模型需求分析

2．1 需求分析

金融 IC 卡发卡系统是银行中非常重要的一个系统，在发卡时人们会在系统中输入许多个人信息，包括银行卡密码等极为隐私的信息，因此需要对系统可能面临的安全威胁进行详细分析，分析出黑客可能的攻击方法并对其加以防范，网络上常见的黑客攻击方法主要分为主动攻击、被动攻击两种。

● 主动攻击：黑客假冒 CA 给合法服务器颁发证书。黑客假冒合法服务器给其他服务器发送数据。黑客截获通信信道中的数据，在之后的某个时间发送给接收方，或者对数据进行修改后再发送给接收方。黑客读取 IC 卡的数据，并对其中数据进行修改，修改完毕后再存储回 IC 卡中。

● 被动攻击：黑客对服务器之间的交互数据进行窃取，从数据中分析出对黑客有用的信息，如申请发卡人的身份信息和银行卡密码等。黑客对 IC 卡中存储的数据进行读取，从而得到 IC 卡存储的各种信息。

2．2 模型功能性需求分析

（1）服务器、受理设备的身份鉴别需求。

在银行系统中通常有好几个服务器，每个服务器负责一部分的工作，通常需要各个服务器之间传输数据，在受理设备发起请求时也需要跟服务器交换数据，这时，就需要身份鉴别来对通信双方进行认证，确保在发送数据前，对方的身份是真实的，防止假冒的服务器或受理设备获取到数据或者传输非法数据，满足金融IC卡发卡系统防主动攻击的需求。

（2）存储的数据完整性和保密性需求。

在发卡的最后流程，个人化应用会将银行中的一些数据存储到银行卡中，由于银行卡可能会被黑客获得，所以需要对里面的数据进行加密存储，同时需要进行完整性保护，防止数据被篡改，满足金融IC卡发卡系统防被动攻击的需求。

（3）数据传输的完整性和保密性需求。

由于个人化应用可能会离数据准备应用较远，可能需要经过公用网络信道传输数据，为了防止数据被窃取和篡改，在个人化应用向数据准备应用发送数据前，需要对数据进行加密，同时进行完整性保护，满足金融IC卡发卡系统的防被动攻击需求和防主动攻击需求。

（4）银行卡密码的保密性需求

在银行系统中，我们需要对银行卡密码进行存储，为了防止密码被窃取，需要对密码进行加密存储，满足金融IC卡发卡系统的防被动攻击需求和防主动攻击需求。

3 金融 IC 卡发卡系统安全模型设计

金融 IC 卡发卡系统模型模拟了银行制卡流程，它是由用户填入申请信息、发卡系统下发银行卡给用户、发卡系统由密钥管理应用、数据准备应用、IC 卡业务管理应用、个人化应用等部分组成，系统对数据的保密性、完整性要求较高。为了防止第三方假冒服务器，密码应用的重点在于服务器之间的身份鉴别，以及为了防止申请人信息经过公网信道时受到窃取、篡改、重放等风险，需要在传输申请人信息前对信息进行保密性和完整性保护。

金融 IC 卡发卡系统安全模型可归结为一个层次模型，分为密钥管理层、数据准备层、IC 卡业务层、个人化层，模型中各层之间相互提供支持，相互依赖。金融 IC 卡发卡系统整体设计的架构和部署图如图 1 所示。各个部分介绍如下：

● 密码管理应用服务器负责对密钥的管理、生成 IC 卡的公私钥、使用 MDK 对卡号和序列号进行分散得到 IC 卡的应用密文主密钥 UDK，并使用发卡行私钥和发卡行证书签发 IC 卡数字证书。

● 数据准备应用服务器负责接收申请人信息，并存储到数据库中，然后分别从 IC 业务管理应用服务器、密钥管理应用服务器导入业务数据，输出目标制卡数据，并对制卡数据进行保密性和完整性保护。

● IC 卡业务管理应用服务器负责接收和处理所有 IC 卡业务，包括 IC 卡交易请求，发卡参数管理等。

● 个人化应用负责发送申请人信息，并对申请人信息进行保密性和完整性保护，并将发卡行数字证书、IC 卡数字证书、IC 卡私钥、IC 卡应用密文主密钥 UDK 等数据写入卡片，并通过发卡行主密钥 KMC 保护装载数据的保密性和完整性。

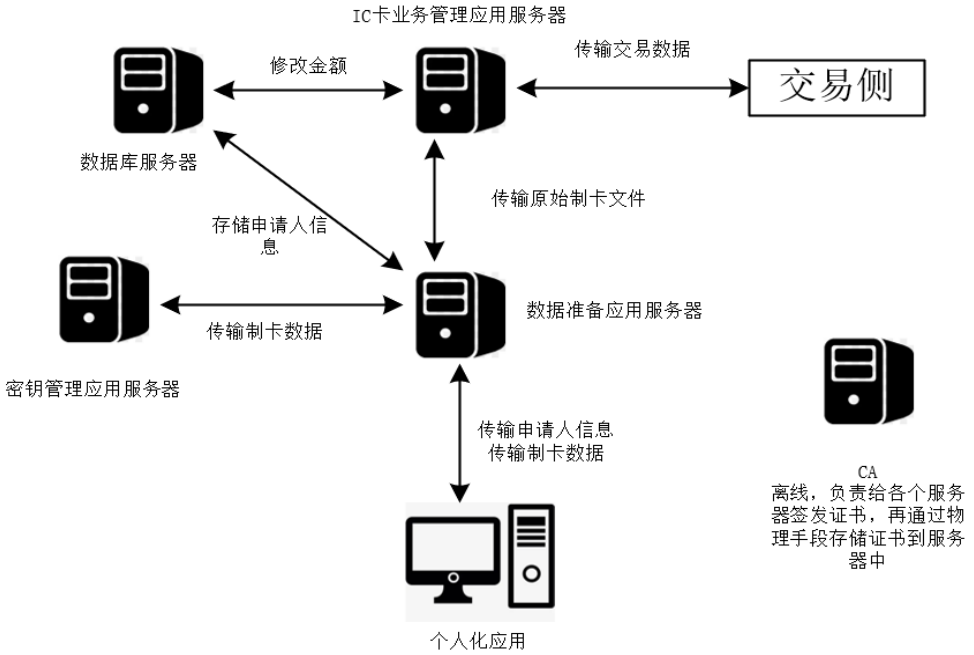

图 1 金融 IC 卡发卡系统整体架构和部署图

4 密码应用工作流程

4．1 密码应用工作流程

为了方便后面的叙述，这里首先对通信协议中用到的符号进行解释，如表 1 所示。

基于国家商用密码算法和数字签名等技术发卡系统通信协议流程图，如图 2 所示。

4．2 发卡系统通信协议流程图说明

（1）数据准备应用X向IC卡业务应用C发送身份、时间戳、X对$ID_X||T_1$的签名，以及CA签发的X的证书。

$T_1||ID_X||E_{SKX}[H(ID_X||T_1)]||E_{SKCA}(T_2||ID_X||PK_X)$

（2）IC卡业务应用C进行身份鉴别的过程

① IC卡业务应用使用证书中心CA的公钥验证X证书的真实性并取得数据准备应用的公钥,通过X证书的ID值知道对方是数据准备应用。

$CertX = D_{PKCA}[E_{SKCA}(T_2||ID_X||PK_X)]=T_2||ID_X||PK_X$

② 用数据准备应用的公钥验证X的签名。

$H_1 = D_{PKX}[E_{SKX}(H(ID_X||T_1))]=H(ID_X||T_1)$

③ C计算哈希值$H_2 = H(ID_X||T_1)$ 。

④ 判断H_2、H_1是否相等，如果相等则IC卡业务应用C确认对方就是数据准备应用X，否则无法确认对方的身份。

表 1 协议通信符号说明

符号	说 明
ID_Z	密钥管理应用Z身份
ID_X	数据准备应用X身份
ID_V	个人化应用V身份
ID_C	IC卡业务应用C身份
T	时间戳
H	杂凑值
||	拼接操作
CA_{PK}	证书机构CA用SM2算法的公钥
X_{PK}	数据准备应用X用SM2算法的公钥
Z_{PK}	密钥管理应用Z用SM2算法的公钥
C_{PK}	IC卡业务应用C用SM2算法的公钥
V_{PK}	个人化应用V用SM2算法的公钥
Z_{SK}	密钥管理应用Z用SM2算法的私钥
X_{SK}	数据准备应用X用SM2算法的私钥
V_{SK}	个人化应用V用SM2算法的私钥
C_{SK}	IC卡业务应用C用SM2算法的私钥
KEK	制卡数据保护密钥
$E_{KEK}[Y]$	用KEK对Y进行加密
$D_{KEK}[Y]$	用KEK对Y进行解密
O	使用数据认证算法生成
IC_{SN}	IC卡SN号
IC_{NO}	IC卡卡号
IC_{ID}	IC卡证书ID值
IC_{SK}	IC卡私钥
IC_{PK}	IC卡公钥
IC_{UDK}	IC卡UDK密钥
CMD	请求数据命令
file	制卡文件

（3） IC卡业务应用C向数据准备应用X发送身份、时间戳、C对($ID_C||T_3$)的签名，CA签发的C的证书。

$T_3||ID_C||E_{SKC}[H(ID_C||T_3)]||E_{SKCA}(T_4||ID_C||PK_C)$

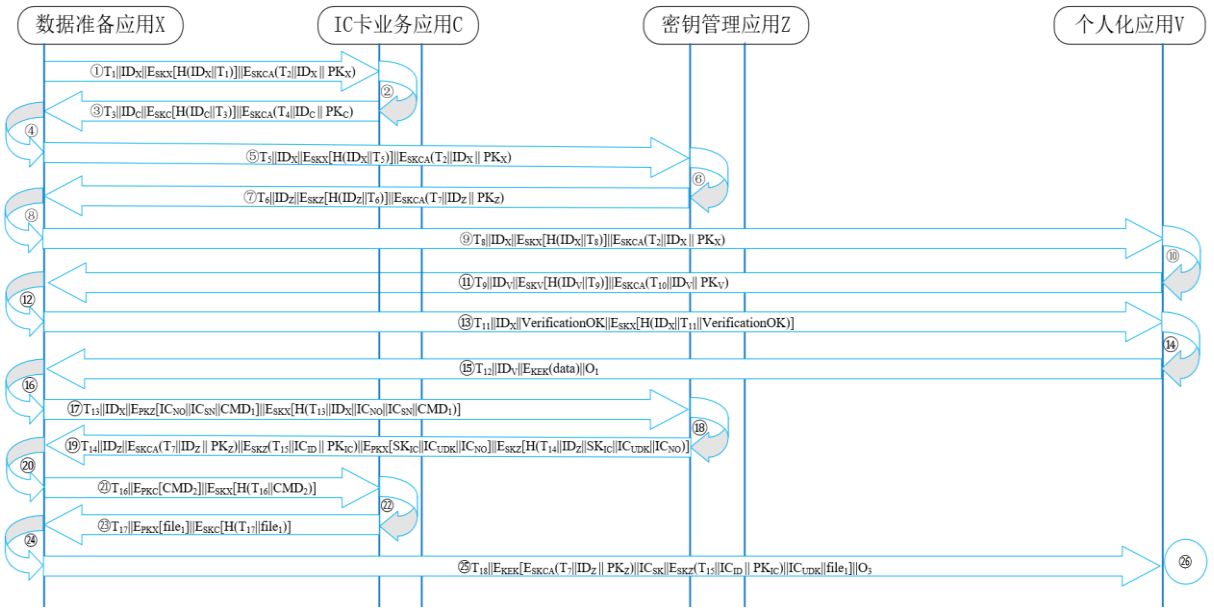

图 2 发卡系统通信协议流程图

（4）数据准备应用对C进行身份鉴别过程如下：

① 数据准备应用用证书中心CA的公钥验证C证书的真实性并取得IC卡业务应用的公钥,通过证书的ID值知道对方是IC卡业务应用。

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

② 用IC卡业务应用的公钥验证C的签名。

$H_3 = D_{PKC}[E_{SKC}(H(ID_C||T_3))]=H(ID_C||T_3)$

③ X计算哈希值$H_4 = H(ID_C||T_3)$ 。

④ 判断H_3、H_4是否相等，如果相等则数据准备应用X和IC卡业务应用C完成双向认证，可以开始传输业务数据，否则无法确认对方的身份。

（5）数据准备应用X向密钥管理应用Z发送身份、时间戳、X对$ID_X||T_5$的签名，以及CA签发的X的证书。

$T_5||ID_X||E_{SKX}[H(ID_X||T_5)]||E_{SKCA}(T_2||ID_X||PK_X)$

（6）密钥管理应用Z对X进行身份鉴别过程如下：

① 用证书中心CA的公钥验证X证书的真实性并取得数据准备应用的公钥，通过证书的ID值知道对方是数据准备应用。

② 用数据准备应用的公钥验证X的签名。

③ Z计算哈希值。

④ 判断哈希值是否相等，如果相等数据准备应用Z则确认对方就是数据准备应用X，否则无法确认对方的身份。

（7）密钥管理应用Z向数据准备应用X发送身份、时间戳、Z对$ID_Z||T_7$的签名，以及CA签发的Z的证书。

$T_6||ID_Z||E_{SKZ}[H(ID_Z||T_6)]||E_{SKCA}(T_7||ID_Z||PK_Z)$

（8）数据准备应用X进行身份鉴别的过程如下：

① 用证书中心CA的公钥验证Z证书的真实性并取得密钥管理应用的公钥，通过证书的ID值知道对方是密钥管理应用。

② 用密钥管理应用的公钥验证Z的签名。

③ X计算哈希值。

④ 判断哈希值是否相等，如果相等则密钥管理应用Z和数据准备应用X完成双向认证，可以开始传输业务数据，否则无法确认对方的身份。

（9）数据准备应用X向个人化应用V发送身份、时间戳、X对$ID_X||T_8$的签名，以及CA签发的X的证书。

$T_8||ID_X||E_{SKX}[H(ID_X||T_8)]||E_{SKCA}(T_2||ID_X||PK_X)$

（10）个人化应用对X进行身份鉴别的过程如下：

① 用证书中心CA的公钥验证X证书的真实性并取得数据准备应用的公钥，通过证书的ID值知道对方是数据准备应用。

② 用数据准备应用的公钥验证X的签名。

③ V计算哈希值。

④ 判断哈希值是否相等，如果相等个人化应用V则确认对方就是数据准备应用X，否则无法确认对方的身份。

（11）个人化应用V向数据准备应用X发送身份、时间戳、V对$ID_V||T_9$的签名，以及CA签发的V的证书。

$T_9||ID_V||E_{SKV}[H(ID_V||T_9)]||E_{SKCA}(T_{10}||ID_V||PK_V)$

（12）数据准备应用对C进行身份鉴别过程如下：

① 用证书中心CA的公钥验证V证书的真实性并取得个人化应用的公钥，通过证书的ID值知道对方是个人化应用。

② 用个人化应用的公钥验证V的签名。

③ X计算哈希值。

④ 判断哈希值是否相等，如果相等则个人化应用V和数据准备应用X完成双向认证，可以开始传输业务数据，否则无法确认对方的身份。

（13）系统初始化完毕，数据准备应用向个人化应用发送初始化完毕信息。

$T_{11}||ID_X||VerificationOK||E_{SKX}[H(ID_X||T_{11}||VerificationOK)]$

（14）个人化应用收到后，知道身份鉴别成功，界面解锁，用户可在界面上输入信息申请发卡。

（15）个人化应用向数据准备应用发送申请人填写的信息。

$T_{12}||ID_V||E_{KEK}(data)||O_1$

$O_1 = E_{MD}(data)$

data:申请人信息，包含申请人姓名、身份证号码、手机号、PIN码等。

（16）数据准备应用收到后。

① 使用KEK解密获取到申请人信息data。

$D_{KEK}[E_{KEK}(data)] = data$

② 生成$O_2 = E_{MD}(data)$。

③ 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。

（17）数据准备应用向密钥管理应用申请IC卡信息。

$T_{13}||ID_X||E_{PKZ}[IC_{NO}||IC_{SN}||CMD_1]||E_{SKX}[H(T_{13}||ID_X||IC_{NO}||IC_{SN}||CMD_1)]$

其中，IC_{NO} 为IC卡卡号，IC_{SN}为IC卡SN号，CMD_1是请求IC卡信息命令。

（18）密钥管理应用收到后。

① 使用自己的私钥解密获得IC卡卡号，IC卡SN号，请求命令。

$D_{SKZ}[E_{PKZ}(IC_{NO}||IC_{SN}||CMD_1)] = IC_{NO}||IC_{SN}||CMD_1$

② 生成哈希值$H_5 = H(T_{13}||ID_X||IC_{NO}||IC_{SN}||CMD_1)$。

③ 使用数据准备应用的公钥解密获得H_6，同时对比H_5和H_6，如果一致，则证明该数据是由数据准备应用发送的且数据未受到篡改。

$H_6 = D_{PKX}[E_{SKX}(H(T_{13}||ID_X||IC_{NO}||IC_{SN}||CMD_1))]$

④ 使用卡号和SN号生成UDK。

取卡号的前十二个数字，每两个数字拼成一个字节，得到6个字节。

取SN的前8bit为一个字节，后8bit为一个字节，得到2个字节。

把前面获取到的6字节和2字节拼接，共得到8个字节，对8个字节取反，得到取反的8个字节，把原始8字节和取反的8字节拼接，得到16字节数据。

使用MDK对16字节数据使用SM4算法加密，得到IC卡的UDK。

⑤ 生成IC卡私钥和证书。

生成IC卡私钥，使用IC卡私钥生成证书请求，使用发卡行私钥（密钥管理应用私钥）和发卡行证书（密钥管理应用证书）签发IC卡数字证书。

（19）密钥管理应用向数据准备应用发送发卡行证书、IC卡私钥、使用发卡行私钥和证书签发的IC卡证书、IC卡UDK。

$T_{14}||ID_Z||E_{SKCA}(T_7||ID_Z||PK_Z)||E_{SKZ}(T_{15}||IC_{ID}||IC_{PK})||E_{PKX}[IC_{SK}||IC_{UDK}||IC_{NO}]||E_{SKZ}[H(T_{14}||ID_Z||IC_{SK}||IC_{UDK}||IC_{NO})]$

（20）数据准备应用收到后。

① 使用自己的私钥解密获得IC卡私钥，IC卡UDK，IC卡卡号。

$D_{SKX}[E_{PKX}(IC_{SK}||IC_{UDK}||IC_{NO})] = IC_{SK}||IC_{UDK}||IC_{NO}$

② 生成哈希值$H_7 = H(T_{14}||ID_Z||SK_{IC}||IC_{UDK}||IC_{NO})$。

③ 使用密钥管理应用的公钥解密获得H_8，同时对比H_7和H_8，如果一致，则证明该数据是由密钥管理应用发送的且数据未受到篡改,然后将该数据暂存。

$H_8 = D_{PKZ}[E_{SKZ}(H(T_{14}||ID_Z||SK_{IC}||IC_{UDK}||IC_{NO}))]$

（21）数据准备应用向IC卡业务管理应用申请IC卡制卡文件。

$T_{16}||E_{PKC}[CMD_2]||E_{SKX}[H(T_{16}||CMD_2)]$

CMD_2：请求IC卡制卡文件命令。

（22）IC卡业务管理应用收到后。

① 使用自己的私钥解密获得请求制卡文件命令。

$CMD_2 = D_{SKC}[E_{PKC}(CMD_2)]$

② 生成哈希值H_9，使用数据准备应用公钥解密获取H_{10}，同时对比H_9和H_{10}，如果一致，则证明该数据是由数据准备应用发送的且该数据未受到篡改。

$H_9 = H(T_{16}||CMD_2)$

$H_{10} = D_{PKX}[E_{SKX}(H(T_{16}||CMD_2))]$

（23）IC卡业务管理应用将制卡数据文件发送给数据准备应用。

$T_{17}||E_{PKX}[file_1]||E_{SKC}[H(T_{17}||file_1)]$

$file_1$：制卡数据文件（文件包含：国家代码、货币代码等）。

（24）数据准备应用收到后。

① 使用自己的私钥解密获得制卡文件。

$file_1 = D_{SKX}[E_{PKX}(file_1)]$

② 生成哈希值H_{11}，使用IC卡业务应用公钥解密获取H_{12}，同时对比H_{11}和H_{12}，如果一致，则证明该数据是由IC卡业务应用发送的且该数据未受到篡改。

$H_{11} = H(T_{17}||file_1)$

$H_{12} = D_{PKC}[E_{SKC}(H(T_{17}||file_1))]$

③ 将申请人信息存储到数据库中，PIN码加密存储。

④ 使用数据认证算法生成O_3。

$O_3 = E_{MD}(E_{SKCA}(T_7||ID_Z || PK_Z)||IC_{SK}||IC_{NO}||E_{SKZ}(T_{15}||IC_{ID} || IC_{PK})||IC_{UDK}||file_1)$

⑤ 将IC卡信息和制卡数据文件拼接，数据使用KEK密钥加密

（25）数据认证应用向个人化应用发送IC卡数据。

$T_{18}||E_{KEK}[E_{SKCA}(T_7||ID_Z || PK_Z)||IC_{SK}||IC_{NO}||E_{SKZ}(T_{15}||IC_{ID} || IC_{PK})||IC_{UDK}||file_1]||O_3$

（26）个人化应用收到后。

① 使用KEK解密

$D_{KEK}[E_{KEK}(E_{SKCA}(T_7||ID_Z||PK_Z)||SK_{IC}||IC_{NO}||E_{SKZ}(T_{15}||IC_{ID}||IC_{PK})||IC_{UDK}||file_1)] = E_{SKCA}(T_7||ID_Z||PK_Z)||IC_{SK}||IC_{NO}||E_{SKZ}(T_{15}||IC_{ID}||IC_{PK})||IC_{UDK}||file_1$

② 生成O_4，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。

$O_4 = E_{MD}(E_{SKCA}(T_7||ID_Z || PK_Z)||IC_{SK}||E_{SKZ}(T_{15}||IC_{ID} || IC_{PK})||IC_{UDK}||file_1)$

③ 将UDK、IC卡私钥和制卡文件信息使用KMC密钥加密。

$enfile = E_{KMC}(IC_{UDK} || file_1||IC_{SK})$

④ 使用数据认证算法生成O_5。

$O_5 = E_{KMC}(IC_{UDK} || file_1||IC_{SK})$

⑤ 将enfile 、O_5、发卡行证书、IC卡证书装载到IC卡中。

4．3 安全性分析

（1）抗身份假冒攻击

本次方案每个发送方和接收方之间发送数据前都需要进行双向身份认证，每个部分的服务器的私钥均由 SM2 算法生成，存储在 CA 和需要用到服务器中，生成时需要输入口令，使用时也需要输入，如果没有口令，即使获取到私钥也无法使用。在 CA 上生成私钥，使用私钥生成证书请求，在生成证书请求时，输入参数表明该证书适用于哪个服务器，CA 使用私钥签署证书，把私钥和证书通过物理手段存储到需要使用的服务器中。证书包括服务器的公钥，只用合法的服务器才会拥有跟公钥对应的签名私钥。在首次连接时，假设连接方为 X，被连接方为 Y，X 首先发送 $T_1||ID_X||E_{SKX}[H(ID_X||T_1)]||E_{SKCA}(T_2||ID_X||PK_X)$给 Y。Y 通过验证 $D_{PKX}[E_{SKX}(H(ID_X||T_1))]$是否等于 $H(ID_X||T_1)$，如果相等，则表明消息的发送方持有 X 的私钥。同样的，X 通过计算 $D_{PKCA}[E_{SKCA}(T_2||ID_Y||PK_Y)]$是否等于 $H(ID_Y||T_2)$来认证 Y。如果黑客要伪造签名，他就要试图从对方的公钥获取对应的私钥，其难度就相当于求椭圆曲线上的离散对数，到目前为止，这个问题是无解的。也就是说只要签名方保护好自己的私钥，其他人就不能伪造他的签名，即不能伪造其身份，从而达到抗身份假冒攻击的要求。

（2）抗重放攻击

发送方发送给接收方的数据传输中包含时间戳，时间戳是每一秒都不同的，在身份认证流程中，签名的对象包括原始文件信息、签名参数、签名时间戳等信息。其消息为 $T_1||ID_X||E_{SKX}[H(ID_X||T_1)]||E_{SKCA}(T_2||ID_X||PK_X)$，即由密文传输。因此,如果攻击者重放一条之前来自于发送方的消息给接收方,接收方能够通过计算 $D_{PKX}[E_{SKX}(H(ID_X||T_1))]$与 $H(ID_X||T_1)$，确定消息未被篡改后，验证明文时间戳的新鲜性。因此,即使攻击者发送相同的消息给接收方,接收方验证时间戳的新鲜性确定此数据过期，可选择让发送方重新发送数据。从而达到抗重放攻击的要求。

（3）抗篡改攻击

协议在通信双方发送数据时，数据经过算法生成杂凑值，在身份认证阶段使用 SM3 算法生成，身份认证完毕后使用 SM4 算法生成，如在身份认证阶段连接放与被连接方的相互认证中 $T_1||ID_X||E_{SKX}[H(ID_X||T_1)]||E_{SKCA}(T_2||ID_X||PK_X)$，如果黑客改变了时间错或 ID 值，在计算哈希值时，得出来的哈希值就会改变，即不等于验证签名时等到的哈希值 $H(ID_X||T_1)$，不能通过身份验证，被连接方可以判断对方不是合法的服务器，或者连接方的身份信息在网络传输过程中被黑客篡改，或因为其他不可预知的原因引起改变，被连接方可以根据不同的情形来处理。如果黑客企图篡改身份信息的同时，篡改发送方的签名信息，那么他就要从发送方的公钥得到私钥，正如前述理由，这是不可行的。有效地抗击了黑客发起的篡改攻击，有效地保护了信息的完整性，从而达到抗篡改攻击的要求。

（4）抗数据窃密和业务否认攻击

数据在发送时，如果是采用公钥密码体制，就用对方的公钥加密，对方收到加密后的数据时，采用自身的私钥进行解密。如数据准备应用向密钥管理应用申请 IC 卡信息时，数据准备应用就采用密钥管理应用的公钥 PKZ 对数据进行加密，如果黑客要从公钥求出私钥，就需要求椭圆曲线上的离散对数，实践证明这是不可行的。如果采用对称密码体制，就需要黑客对 128 位的密钥进行穷举攻击，运算量达到 $O(2^{128})$，这是黑客难以达到的，因此，通过加密有效地保护了数据安全。

同理，数据准备应用向密钥管理应用申请 IC 卡信息时，由数据准备应用用自身的私钥对 $T_{13}||ID_X||IC_{NO}||IC_{SN}||CMD_1$ 信息进行了数字签名，而密钥管理应用使用数据准备应用的公钥可以验证这个签名，所以数据准备应用不能否认对 $T_{13}||ID_X||IC_{NO}||IC_{SN}||CMD_1$ 信息进行了数字签名。因为任何人要伪造这个签名，就要知道产生这个签名所使用的私钥，而要从公钥反推出公钥，相当于求椭圆曲线的离散对数，因此，也是不可行的。这就保证了任何一方对它所从事的业务均不能否认。

表 2 各身份认证方案安全性能比较

安全性能	文献[3]方案	文献[2]方案	本文方案
身份验证	数字签名、数字证书	数字签名、数字证书	数字签名、数字证书
密码算法	SM2、SM3	DES、RSA	SM2、SM3、SM4
安全协议	无	无	有
抵抗篡改攻击	是	是	是
抵抗假冒攻击	是	是	是
抵抗重放攻击	否	否	是
提供双向认证	是	是	是
抵抗密钥攻击	否	否	是
密码应用正确	是	否	是
密码应用合规	是	否	是
密码应用有效	否	否	是

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》，现将本文方案与参考文献[6][10]在身份验证、密码算法、安全协议、抵抗篡改攻击、抵抗假冒攻击、抵抗重放攻击、提供双向认证、抗密钥攻击、密码应用正确、密码应用合规、密码应用有效等方面进行比较。

实验平台是在 Linux 操作系统环境下，综合运用 PKI 技术和 Gmssl 工具箱，用 C++语言编码实现的，平台基本能够实现金融 IC 卡发卡系统中设备之间的数据传输、存储、身份鉴别的数据安全性和完整性保护等功能。实验对比结果如表 2 所示。

性能比较的结果表明，文献[3]虽然使用了数字签名和数字证书方式进行身份认证，但是没有提供抗重放攻击的方案；文献[2]也没有提供抗重放攻击的实际方案，且使用了不安全的密码算法，具有较大的安全隐患。本文设计的密码方案使用了国密算法 SM2/SM3/SM4，算法安全程度高，且在方案中提供了防身份假冒，防数据篡改，防数据重放的设计方法，具有较高的安全性。

5 结束语

本文分析了当前银行制卡系统面临的安全风险，提出了金融 IC 卡发卡系统的安全需求，构建了金融 IC 卡发卡系统安全模型，设计了基于国家商用密码算法的金融 IC 卡系统通信协议，并应用 PKI 技术、Gmssl 工具、Linux 操作系统等，实现了金融 IC 卡发卡系统中设备之间的数据传输、存储、身份鉴别的数据安全性和完整性保护等功能。本文设计的密码方案使用了国密算法 SM2/SM3/SM4，使得算法安全程度高。此外，方案提供了防身份假冒，防数据篡改、防数据重放等方法，使系统具有较高的安全性。

参 考 文 献

[1] 罗慧,谢程祥.广州地铁金融 IC 卡基于 ODA 技术的应用探讨[J].都市快轨交通,2019,32(1):93-97

[2] 曾向昀.银行金融 IC 卡发卡系统的设计与实现[D].北京：北京工业大学,2016

[3] 高利伟.金融 IC 卡证书签发系统设计与实现[D].北京：北京交通大学,2015.

[4] 范春鹏.金融 IC 卡密钥管理系统的设计与实现[D].北京：北京交通大学,2015.

[5] 刘秉凯.基于 PKI 的统一身份认证服务系统的设计与实现[D].太原：太原理工大学,2013

[6] 王一平,陈云田,盛唯悦,等.关于银行卡交易量与金融 IC 卡多行业应用的研究[J].现代商业,2017(31):95-97

[7] 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.

[8] 赵宇亮,胡威,张冰,毛一凡,张攀,宋文婷. 国家商用密码算法综述[C]//2016 电力行业信息化年会论文集.,2016:140-142.

[9] 李孝猛,梁宵,耿方,黄艳丽,刘茜,张骏温.基于国密算法证书的多 CA 统一平台关键技术研究[C]//.中国计算机用户协会网络应用分会 2019 年第二十三届网络新技术与应用年会论文集,2019:313-317.

[10] 秦宁丽,李博,姚学鹏.基于国密算法的智能移动终端安全防护技术研究[C]//.电力通信技术研究及应用,2019:386-390.