智能电视安全存储数据访问方法

任 飞[1]，刘贤洪[2]，秦志光[1]

(1. 电子科技大学计算机科学与工程学院 成都 610054; 2. 四川长虹电器股份公司多媒体产业集团规划设计院 四川 绵阳 621000)

【摘要】基于智能电视电子支付对安全存储、数据存取的应用需求，提出了一种基于通信双方的ID作为公钥进行认证和密钥协商的机制，利用对称加密算法，实现智能电视与安全芯片之间的数据传输的安全保护，降低了安全芯片的实现规模和系统复杂度。结果表明，在同等安全保护强度下，基于这种机制的安全芯片实现规模约为ECC的1/6和RSA的1/4，降低了系统的总体成本。

关 键 词 安全认证; 密钥协商; 安全存储访问; 智能电视; 电视支付
中图分类号 TP301 文献标志码 A doi:10.3969/j.issn.1001-0548.2014.01.024

Data Access Method for Smart TV Secure Storage

REN Fei[1], LIU Xian-hong[2], and QIN Zhi-guang[1]

(1. School of Computer Science and Engineering, University of Electronic Science and Technology Chengdu 610054;
2. Planning and Design Institute of Sichuan Changhong Electronic Co. Ltd. Mianyang Sichuan 621000)

Abstract An authorization method and a simple key agreement protocol based on both sides' IDs of participants are proposed to meet the requirements for secure storage and secure access of smart TV payment. Combined with symmetric encryption algorithms, the data transmission and data access protections between smart TV and security storage chip are realized and the scale and complexion of the security storage chip are reduced also. The result shows that the chip gate complexity has been reduced to about 1/6 of ECC and 1/4 of RSA with the same encryption strength.

Key words authorization; key agreement protocol; security storage; smart TV; TV payment

电视已进入智能时代，智能电视的特点之一就是开放，包括硬件平台、软件平台以及应用和服务。智能电视硬件平台的开放，就是将硬件的资源，包括存储、接口、外设等全部虚拟成标准的API接口供第三方调用。智能电视软件平台的开放是指将智能电视的API标准化和公开化，同时提供SDK供第三方开发者调用。这种开放将吸引众多的开发者，为智能电视提供丰富的应用和服务。

智能电视改变了传统电视的一次性交易模式，为电视厂商开创了持续交易的新商业机会。传统的电视重点在于终端产品的销售，而智能电视还将依托于终端用户群，开展服务运营，获得持续性收益。智能电视对信息安全提出了非常高的要求。

开放与安全，是一把双刃剑。传统的封闭系统，安全性相对较高，但只有出厂预装的少量应用。而智能电视为了应用的丰富性，必须把产品平台开放给更多的开发者，随之而来的就是安全问题。

本文将讨论在开放平台下，智能电视安全存储以及安全访问的问题。

1 电视支付对安全存储的要求

电视支付是智能电视开展其他业务的基础，是智能电视必须具备的基本功能之一。智能电视应用中支付客户端的安全是电视支付的重要环节，客户端将获取到用户输入的支付密码、金融IC卡信息等关键数据，因此，客户端的安全防护显得尤其重要。

2011年6月，中国银联发布了《中国银联电视支付技术规范》[1]，对终端提出了以下安全要求：

1) 客户端数据输入安全。

客户端输入的安全，要求在遥控发送模块与电视接收模块之间的传输信道加密；支付客户端的界面必须是支付模块自带界面，且不能被其他系统截取；个人账户密码、CVN2等敏感信息，需要采用数字随机分布的软键盘或混序排列，防止传输过程被

收稿日期：2012 – 06 – 25；修回日期：2013 – 11 – 18
基金项目：国务院核高基重大专项(2009ZX01039-003-001)；四川省战略性新兴产业关键技术产业化重大专项(SC2011510703006)
作者简介：任飞(1968 –)，男，博士，主要从事安全、智能多媒体终端可信软件平台、云计算安全、分布式内容网等方面的研究.

侦听。

2) 客户端数据存储安全。

智能电视支付客户端应具备安全存储机制，其安全存储区可分为3个部分：公钥安全存储区、脱机交易数据安全存储区和敏感数据安全存储区。对存储区的访问需要有防止侦听机制。

3) 系统数据传输安全。

支付应用安全体系应在技术上保证交易数据、银行卡信息、交易授权信息和客户输入信息等在传输过程中的安全性和完整性，能防止安全加密数据在第三方机构传输过程中被破解、篡改或仿造。

从以上要求看出，银联电视支付要求终端必须具备安全的存储区，具备密钥安全存储功能以及敏感数据安全存储功能，同时，要求对所有的数据访问和传输过程具备防侦听功能、防破解、防篡改、防伪造功能，这就对数据的安全存储、安全访问、安全传输提出了较高的要求。

2　智能电视安全存储方案以及存在的安全问题

智能电视安全存储，一般采用安全存储芯片进行。而安全存储芯片一般采用IC卡芯片。IC卡芯片一般有以下3种类型[2-4]：

1) 存储卡。相当于普通串行E2PROM存储器，这类卡信息存储方便，使用简单，价格便宜，很多场合可替代磁卡，但由于其本身不具备信息保密功能，因此，只能用于保密性要求不高的应用场合。

2) 逻辑加密卡。加密存储器卡内嵌芯片在存储区外增加了控制逻辑，在访问存储区之前需要核对密码，只有密码正确，才能进行存取操作，这类信息保密性较好，使用与普通存储器卡相类似。

3) CPU卡。CPU卡内嵌芯片相当于一个特殊类型的单片机，内部除了带有控制器、存储器、时序控制逻辑等外，还带有算法单元和操作系统。由于CPU卡有存储容量大、处理能力强、信息存储安全等特性，常被广泛用于信息安全性要求特别高的场合。

在电视支付领域，由于密钥、用户敏感数据等，涉及用户财产的安全，对安全性要求比较高，一般采用CPU卡芯片进行安全存储。

如图1所示为一个典型的IC卡安全芯片数据读取流程，智能电视基于IC卡的数据存取过程[5]如下：

1) 选择主文件。主要指IC卡芯片中根目录的文件结构。

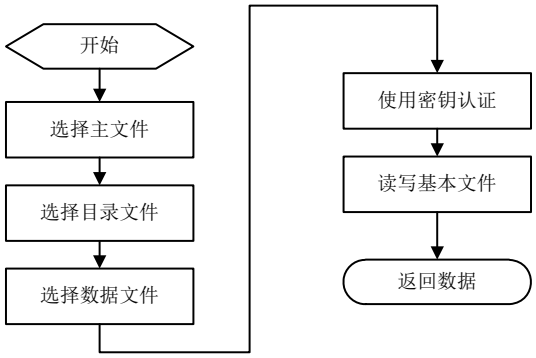

图1　典型的安全芯片数据读取流程

2) 选择专有文件。包括文件的控制信息和任选的供分配用的存储器的文件。

3) 选择基本文件。指共享同意文件标识符的数据单元或者记录的集合。

4) 使用数据文件读写密码进行认证。以IC卡为基础的安全芯片，主要采用口令认证的方式实现对访问的控制，即将外部输入的口令与内部的数据进行对比，如果相同，则认证通过，允许读写数据；否则，则认为是非法访问。

5) 读写文件。在认证通过后，则允许实现对指定数据文件的读写。

安全芯片与电视主芯片之间的数据通信，主要通过I/O引脚进行，没有任何保密措施。结合对以上过程的分析可以看出，在文件选择、密码认证、数据读写等传输过程，由于全部为明文传送，通过转接器或者抓数据的方式，可以将保密的数据或者敏感数据全部获取[6]。同时，在认证完成后，只要芯片不重新复位，任何程序都可以访问芯片通过认证的数据，这些都对安全形成了严重的威胁，也给黑客等造成了可乘之机。本文研究如何采用高效简洁的方式保护传输数据的安全。

3　现有的数据安全读取方法

综上所述，通过对I/O口数据的分析，可以获得安全芯片保存的密钥、敏感信息等，有可能黑客将I/O的数据通过网络共享出去，而被第三方非法使用，如数字电视条件接收系统的CW共享就是基于以上原理。防止安全芯片数据泄漏的方式之一就是对安全芯片到主芯片传输的数据进行加密传输。目前，对传输内容进行处理的方式有以下3种[7-9]：

1) 采用固定密钥方式进行加密传输。

采用固定密钥加密的方式，指智能电视厂商预先在安全芯片和智能电视中，预置相同的密钥。智能电视与安全芯片的所有操作均采用该密钥加密。

该方式实现比较简洁，方案的实现只需要在安全芯片的COS系统以及数字电视对应的模块中进行修改，基本不需要增加硬件成本，与明文方式传输相比，安全性有所提高。但是该方式存在非常明显的缺陷，即传输数据虽然已经加密，但是由于采用的是相同的加密密钥，因此，把加密的信息获取而共享出去，在其他相同的智能电视仍然可以实现正确的解密，获取信息的内容。

2) 基于固定密钥的一次一密方式。

该方式是在第一种方式基础上的增强，其实现的原理是：首先在安全芯片与智能电视主芯片约定相同的密钥，在安全芯片与智能电视主芯片通信开始时，由通信双方各自产生随机数并相互交换；然后在安全芯片与智能电视主芯片中按照相同的方法，生成新的通信密钥，如使用约定的密钥对两个随机数运算的结果进行加密，使用加密后的结果作为后续通信的密钥。该方式同样不增加硬件成本，与第一种方式比较，安全性有了非常大的提高。该方式下，利用随机数的机制，可以做到不同的安全芯片与智能电视主芯片之间通信的密钥完全不同，同时，相同的安全芯片与数字电视之间的通信，不同的时刻可能也不同。采用简洁的将加密后的敏感信息共享出去的方式，在其他智能终端中已经没有办法直接使用。但是该方式也存在比较大的缺陷，如果将安全芯片与智能电视主芯片之前的握手数据全部进行分析，也可将其用于其他的智能电视。

3) 采用非对称加密体制进行加密传输。

采用非对称加密体制，指借助于PKI的思想，采用ECC、RSA等非对称密钥体制进行密钥协商，从而从根本上实现对通信过程加密的一次一密；采用密钥协商形成对称加密密钥，再利用对称加密的方式对通信的过程进行加密。基于ECC、RSA的密钥协商是目前非公钥体制的常用方法，此处不再赘述。

基于非对称加密体制的密钥协商，从根本上解决了数据安全传输问题。但是RSA、ECC算法非常复杂[10]，运算耗用的CPU资源大、耗用的存储空间非常大，在安全芯片上直接采用软件实现性能影响非常大，如果采用协处理器实现，则安全芯片的成本将成倍增加，这将影响家电行业微薄的利润。

以上3种方式，都有明显的缺点：第一、二种方式安全性太低或者存在较大的安全性隐患，第三种方式安全性高，但是成本高，商用推广困难。

4 一种新的智能电视存储芯片安全访问方案

现有的安全芯片，一般均已经支持多种对称加密算法，安全芯片本身已经支持数据的加解密，数据加密传输的基础已经具备，需要设计一种有效的密钥协商机制，在不增加硬件成本的情况下，实现安全芯片通信密钥协商的安全要求。本方案密钥协商的基本原理是，为安全芯片和智能电视主芯片配不同的公钥/私钥对，然后基于双方的公钥与私钥进行密钥协商，利用协商的结果作为后续通信的加密密钥进行安全通信。

首先，为参与通信的智能电视U与安全存储装置V分别分配两个指数向量为公钥和私钥：

$$\boldsymbol{\alpha}=(\alpha_1 \quad \alpha_2 \quad \cdots \quad \alpha_n)_{1\times n}$$

$$\boldsymbol{\beta}=(\beta_1 \quad \beta_2 \quad \cdots \quad \beta_n)_{1\times n}$$

式中，$\alpha_i \in Z_p$，为公开参数(公钥)；$\beta \in Z_p$，为秘密参数(私钥)；Z_p 表示有限整数域。要求对 $\boldsymbol{\alpha}_{\mathrm{U}}$、$\boldsymbol{\beta}_{\mathrm{U}}$ 和 $\boldsymbol{\alpha}_{\mathrm{V}}$、$\boldsymbol{\beta}_{\mathrm{V}}$ 均满足：

$$\boldsymbol{\alpha}_{\mathrm{V}} \times \boldsymbol{\beta}_{\mathrm{U}}{}^{\mathrm{T}} \bmod p = \boldsymbol{\alpha}_{\mathrm{U}} \times \boldsymbol{\beta}_{\mathrm{V}}{}^{\mathrm{T}} \bmod p$$

4.1 认证及密钥协商流程

U、V间认证的密钥协商流程如下：

1) U将 $\boldsymbol{\alpha}_{\mathrm{U}}$ 传送给V，发起认证流程。

2) V收到 $\boldsymbol{\alpha}_{\mathrm{U}}$ 后，生成一个随机数 R_{I}，随即将 R_{I} 和 $\boldsymbol{\alpha}_{\mathrm{V}}$ 传送给U。

3) U完成 $K_{\mathrm{V,U}} = \boldsymbol{\alpha}_{\mathrm{V}} \times \boldsymbol{\beta}_{\mathrm{U}}{}^{\mathrm{T}} \bmod p$ 计算后，随即计算函数 $K = f(K_{\mathrm{V,U}}, R_{\mathrm{I}})$。其中，$f(K,R)$ 为事先约定的一个函数，可以是hash函数、加密函数或者其他的不可逆函数，或者是这些函数的组合(下同)。

4) V完成 $K_{\mathrm{U,V}} = \boldsymbol{\alpha}_{\mathrm{U}} \times \boldsymbol{\beta}_{\mathrm{V}}{}^{\mathrm{T}} \bmod p$ 计算后，随即计算函数 $K = f(K_{\mathrm{U,V}}, R_{\mathrm{I}})$。

5) U将再次生成的随机数 R_{U} 传给V，并计算函数 $C_{\mathrm{U,V}} = E(R_{\mathrm{U}}, K)$。

6) 同时，V也将生成的随机数 R_{V} 传给U，并计算函数 $C_{\mathrm{V,U}} = E(R_{\mathrm{V}}, K)$。

7) U用自己计算出的K值作为加密密码，对 R_{V} 进行加密，即 $C_{\mathrm{U}} = E(R_{\mathrm{V}}, K)$，随后将加密的结果 C_{U} 传给V。其中，$E(R,K)$ 为预先定义的加密函数，可以是AES、3DES等通用的加密算法以及芯片自身支持的其他加密算法(下同)。

8) V用自己计算出的K值作为加密密码，对 R_{U} 进行加密，即 $C_{\mathrm{V}} = E(R_{\mathrm{U}}, K)$，随后将加密的结果 C_{V} 传给U。

9) U收到V端传送的 C_{V} 后，将 C_{V} 与 $C_{\mathrm{U,V}}$ 进行比

较，如果相同则认为对方已经产生了与自己相同的密钥。

10) V收到U端传送的C_{U}后，将C_{U}与$C_{\mathrm{V,U}}$进行比较，如果相同则认为对方已经产生了与自己相同的密钥。

协议的时序图如图2所示。

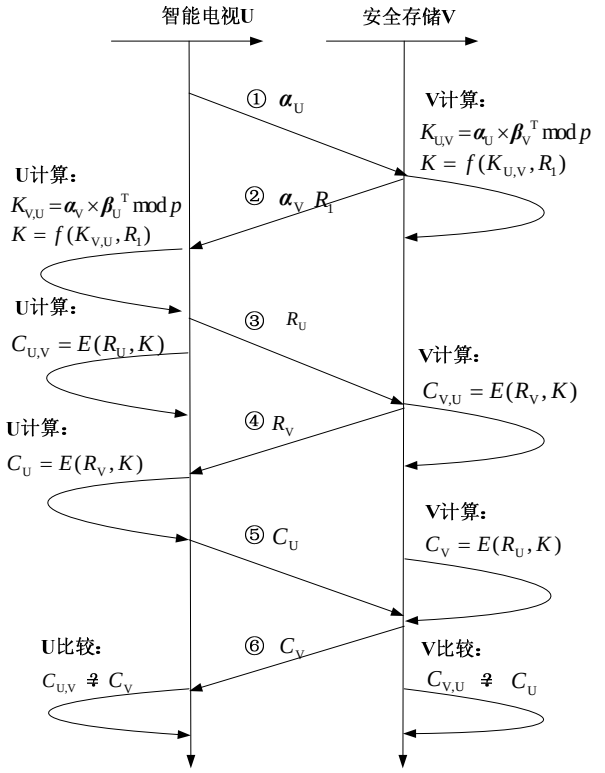

图2　认证协议时序

以上过程全部通过，则可以进行w数据的访问等运算，并采用K作为共同密钥进行后续通信；或者使用K加密传送后续通信的密钥。

4.2　加密传输

在密钥协商完成后，可将认证过程中协商的密钥K作为通信的加密密钥：

$$C=E(K,\mathbf{IV},\mathrm{data})$$

传输的内容为：

$$C \,\|\, \mathrm{Hmac}(K,C)$$

式中，K为协商过程中形成的加密密钥；**IV**为初始向量；data为待加密的数据内容。

4.3　应用举例

假设有智能电视U和安全存储装置V，分别给其分配不同向量对(为简洁起见，设在GF(2^8)有限域中进行计算)。

智能电视U：公钥$\boldsymbol{\alpha}_1=(34\quad 124\quad 3\quad 87)$，私钥为$\boldsymbol{\beta}_1=(130\quad 62\quad 182\quad 146)$；

安全存储V：公钥$\boldsymbol{\alpha}_2=(234\quad 236\quad 211\quad 166)$，私钥为$\boldsymbol{\beta}_2=(93\quad 205\quad 219\quad 69)$；

设备3：公钥$\boldsymbol{\alpha}_3=(123\ \ 200\ \ 141\ \ 39)$，私钥为$\boldsymbol{\beta}_3=(89\ 45\ 47\ 33)$。

如果智能电视U和安装存储V进行通信，则按照以下过程进行：

1) U将$\boldsymbol{\alpha}_{\mathrm{U}}=\boldsymbol{\alpha}_1=(34\quad 124\quad 3\quad 87)$发给V。

2) V收到$\boldsymbol{\alpha}_{\mathrm{U}}$后，将$\boldsymbol{\alpha}_{\mathrm{V}}=\boldsymbol{\alpha}_2=(234\quad 236\quad 211\quad 166)$和随机数$R_1$一起传给U。

3) U先计算$K_{\mathrm{V,U}}=\boldsymbol{\alpha}_{\mathrm{V}}\times\boldsymbol{\beta}_{\mathrm{U}}^{\mathrm{T}} \bmod p$，即：

$$K_{\mathrm{V,U}}=(234\quad 236\quad 211\quad 166)\times$$
$$(130\quad 62\quad 182\quad 146)^{\mathrm{T}} \bmod p=170$$

U随即计算$K=f(K_{\mathrm{V,U}},R_1)$。

4) 如果f函数为sha1，即$K=\mathrm{sha1}(K_{\mathrm{V,U}},R_1)$。

5) V先计算$K_{\mathrm{U,V}}=\boldsymbol{\alpha}_{\mathrm{U}}\times\boldsymbol{\beta}_{\mathrm{V}}^{\mathrm{T}} \bmod p$，即：

$$K_{\mathrm{U,V}}=(34\quad 124\quad 3\quad 87)\times$$
$$(93\quad 205\quad 219\quad 69)^{\mathrm{T}} \bmod p=170$$

V随即计算：$K=f(K_{\mathrm{U,V}},R_1)$。

6) 由以上分析得知，$K_{\mathrm{V,U}}=K_{\mathrm{U,V}}=170$，后续一定能产生相同的$K$值，其协商过程不再赘述。

5　协议安全性分析

5.1　安全性分析

1) 数据机密性保护。在该协议1)～4)中，R_1、$\boldsymbol{\alpha}_{\mathrm{U}}$、$\boldsymbol{\alpha}_{\mathrm{V}}$、$R_{\mathrm{U}}$、$R_{\mathrm{V}}$以明文的方式在接口上传输，其中，$\boldsymbol{\alpha}_{\mathrm{U}}$、$\boldsymbol{\alpha}_{\mathrm{V}}$本身为公钥数据，可以向任何的第三方公开。而$R_1$、$R_{\mathrm{U}}$、$R_{\mathrm{V}}$为双方产生的随机数，对随机数的获取或者篡改，不会引起造成机密数据的丢失。而在认证完成后，后续数据的传输，均是加密传输，所以数据的机密性得到了有效的保护。

2) 数据完整性保护。在认证以及密钥协商过程中，任意的数据篡改，将会导致认证和密钥协商的失败；在加密传输过程中，加入了加密初始向量，任意的数据块篡改或者丢失，均会造成后续数据无法正确解密，同时，对传输的数据进行了Hmac运算，可以有效识别传输数据是否完整。

3) 身份认证分析。协议通过对方的公钥，确定对方的身份；通过让对方加密随机数与自身解密结果对比，可以核实对方是否是真实的公钥持有者，也可以同时核实对方是否形成了与自己相同的密钥。

4) 数据源确认。数据加密的传输，对原始的数据采用加密传输，采用Hmac(K,C)对传输内容进行了散列运算，只有K的密钥持有者才可以对C进行散

列运算，可以识别数据源的来源。

5.2 抗攻击性分析

1) 非法访问。从协议的流程看出，只有通过了全部的认证，才可以进行存储区的访问，有效地防止非法的访问。同时，认证过程采用了公钥与私钥的方式，避免了现有传输认证过程中通信密钥的泄漏。

2) 恶意跟踪。在整个认证过程中，密钥等私密信息均不在信道上传送，攻击者不能通过窃听实现对双方私密信息的获取。在数据传输过程中，数据仅以密文方式存在。除公钥外，其他的所有数据均不会出现重复，攻击者无法获得通过传输的数据的跟踪获得原数据信息。

3) 窃听。虽然攻击者可以窃听在信道上传输的所有的数据，但是除公钥数据外，其余的均是不需要保密的随机数以及加密后的数据信息，通过窃听无法获得有效的数据。

4) 伪造。信道上传输的数据，均以加密的信息进行传输，每次传输的内容均不同，同时，对加密后的数据进行了HMAC运算，攻击者无法通过窃听整个通信的过程，伪造出具有一个完整数据的传输过程，从而伪造数据信息。

5) 重放。由于每次存储区读取的认证是由智能电视发起，随机数 R_1 是由存储区产生，因此确保了每次通信的密钥是不同的。在信道上传输的数据消息，数据内容、加密密码每次均不同，可以有效防止攻击者利用重放以前的数据来伪装成合法者读取数据。

6 结 束 语

本文分析了智能电视中电子支付对安全存储、数据存取的应用需求，以及现有方案的不足，提出的智能电视主芯片与安全芯片的密钥协商方案，算法简洁、运算量小，非常适合于具备较低的处理能力和较少运算存储空间的安全芯片或IC卡等，且对安全性要求非常高的场合。在同等安全等级下，基于ECC的安全芯片的规模约200万门，基于RSA的安全芯片规模约120万门，而采用本方案的安全芯片的规模为30万门，降低了系统成本开销。该方案已在长虹公司的智能电视、智能机顶盒上开始应用，对基于智能电视的运营安全、隐私保护、可管可控等起了关键的作用。

参 考 文 献

[1] 吴潇, 金正博. Q/CU038-2011中国银联智能电视支付技术规范[S]. 上海: 中国银联股份有限公司, 2011: 2-129.
WU Xiao, JIN Zheng-bo. Q/CU038-2011 technical specifications on smart TV payment of China unionPay[S]. Shanghai: China UnionPay Co. Ltd., 2011: 2-129.

[2] 杨振野. IC卡技术及其应用[M]. 北京: 科学出版社, 2006.
YANG Zhen-ye. Technologies and application of integrated circuit card[M]. Beijing: Science Press, 2006.

[3] 喻涛. IC卡的分类及性能[J]. 现代通信，1997(10): 21-22.
YU Tao. Classification and performancev of integrated circuit card[J]. Modern Communication, 1997(10): 21-22.

[4] 夏志远. 智能卡操作系统的研究与实现[D]. 武汉: 华中科技大学, 2003.
XIA Zhi-yuan. Research and implementation of a smart card OS[D]. Wuhan: Huzhong University of Science and Technology, 2003.

[5] 宋光旭, 方维林. 数字电视CW共享的原理及应用[J]. 卫视传媒, 2010(13): 66-70.
SONG Guang-xu, FANG Wei-lin. Principle and application of digital TV CW sharing[J]. Guardian Media, 2010(13): 66-70.

[6] 魏辉. IC卡安全的基础——IC卡用芯片的安全[J]. 电脑与信息技术, 2006, 14(5): 42-44.
WEI Hui. Security aspects of IC card chip—fundamentals underlying security of IC card system[J]. Computer and information Technology, 2006,14(5): 42-44.

[7] 冯志兴, 李建华. 金融IC卡认证体系及其安全性分析[J]. 信息安全与通信保密, 2009(3): 58-63.
FENG Zhi-xing, LI Jian-hua. Analysis of financial IC card authentication system and its security[J]. Information Security and Communications Privacy, 2009(3): 58-63.

[8] 俞林, 甘骏人. 一个适用于逻辑加密IC卡的认证加密方案[J]. 应用科学学报, 2000,18(2): 109-115.
YU Lin, GAN Jun-ren. An authentication and encryption method suitable for intelligent memory IC card[J]. Journal of Applied Sciences, 2000, 18(2): 109-115.

[9] 潘峥嵘. 一种IC卡混合加密算法的分析与设计[J]. 自动化仪表, 2008, 29(5): 33-35.
PAN Zheng-rong. Analysis and design of a mixed encryption a lgorithm for IC card[J]. Automatic Instrument, 2008, 29(5): 33-35.

[10] 景为平, 陈海进. 智能IC卡RSA密钥生成研究[J]. 电子测量与仪器学报, 2002, 16(3): 71-76.
JING Wei-ping, CHEN Hai-jin. Research of RSA key generation in smart IC card[J]. Journal of Electronic Measurement and Instrument, 2002, 16(3): 71-76.

编 辑 张 俊