滚动式密钥新型加密算法的分析与设计

尹晓霈，付志娟，矫立新

(兰州理工大学 电气与信息工程学院，甘肃 兰州 730050)

摘 要：从整体角度给出了IC卡信息加密的安全体系结构，对IC卡安全体系结构采用的加密技术进行了全面分析与研究，用标准算法DES和KEELOQ设计了一种更安全的、用于IC卡的混合加密技术，并对加密技术给予了软件实现，为研究和实施IC卡提供了一个更完整、更安全的解决方案。

关键词：加密技术；DES算法；KEELOQ算法

中图分类号：TP309 **文献标识码：**A

Analysis and design of a roll secret key encryption algorithm

YIN Xiao Pei，FU Zhi Juan，JIAO Li Xin

(College of Electrical and Information Engineering，Lanzhou University of Technology，Lanzhou 730050，China)

Abstract: The paper described the secure frame system structure of IC card information encryption in detail，analyzed and studied the secure framework of IC card encryption techniques. It also designed a kind of more secure mix-encryption technology using symmetry standard algorithm DES and KEELOQ encryption technology. These researches provide a complete and secure solving program for researching of IC card.

Key words: encryption technology; DES encryption algorithm; KEELOQ algorithm

DES算法与KEELOQ算法的综合加密过程以DES加密算法为主，针对DES加密密钥容易被穷举法破解的缺点，在DES加密密钥的产生和运用过程中融合KEELOQ算法，利用KEELOQ加密算法能确定信息来源的真实性与用户身份的优点，解决了DES传统加密算法[1]的固有问题。同时利用DES加密速度快、运算需时少的优点，解决了KEELOQ算法传输效率较低、无法用于数据加密的问题，从而使明文的加密过程更为安全，做到IC卡的信息安全的传递。

1 设计流程

1.1 工作密钥A的设计

管理服务器里的伪随机序列发生器产生64 bit的密钥。弱密钥、半弱密钥被自动剔除。整个系统中所有卡和读卡机都编有产品序列号，管理服务器自动给每个产品序列号配以相应不同的密钥，制成密钥表待用，完成密钥分配。管理服务按产品序列号向用户卡注入相应的密钥，保密员用工作卡将密钥表传递给每一个读卡机。完成密钥分发任务[2]。

工作密钥A使用管理服务器里的伪随机序列发生器产生64bit的密钥，并写入片内E^2PROM，称之为工作密钥A。通过管理服务器将工作密钥A发给相应的IC卡和读卡器。

1.2 原始密钥B与同步数的设计

加密芯片使用前，由长度为64 bit的厂商代码与28 bit的序列号经相应算法产生原始密钥B，原始密钥B再对32 bit同步值进行KEELOQ加密，生成32 bit的同步数，同时，同步值自加1，并写入读卡器芯片内E^2PROM中。其中，厂家代码为64 bit，它唯一对应于整个混合系统，序列号可作为用户码，对应于IC卡。由于代表各制造商的序列号均不同，所产生的唯一原始密钥B均应与IC卡相对应。初始同步值采用随机序列发生器产生[3]。

1.3 各工作子密钥的设计

在DES加密算法中，16轮迭代子密钥由原始密钥通过置换表格和循环移位得来，而在新型混合加密算法中，加密主体仍旧以DES加密为主，16个子密钥的产生方法与原始方法一致，但在其产生前，需要用工作密钥A先去加密同步数，形成32 bit的加密密文，然后同步数自加1，用工作密钥A再次加密同步数，形成 32 bit的加密密文，与前一次密文合并，从而形成64 bit加密密钥C，使原始密钥在使用前做到一次加密，再按照DES子密钥的生成方法依次生

成16个子密钥[4]。原始密钥B与加密密钥C的设计流程如图1所示。

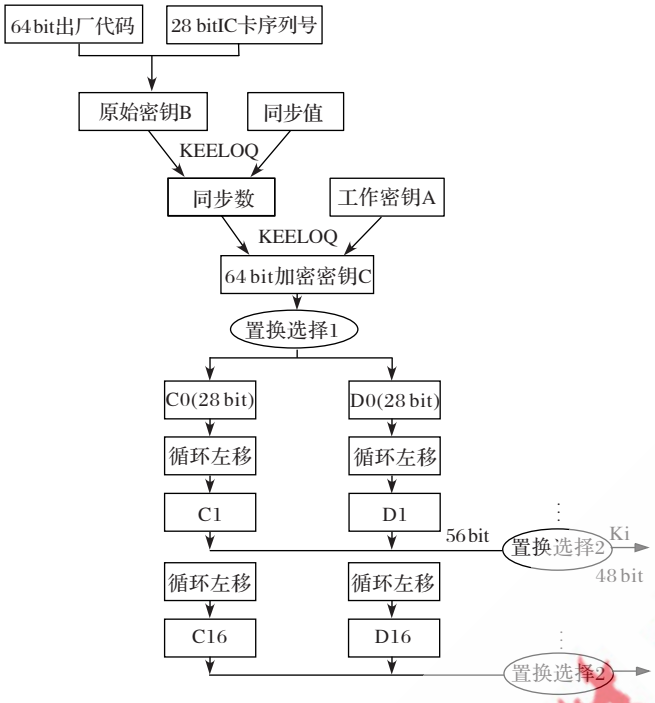

图1 原始密钥B与加密密钥C的设计

1.4 加密函数的设计

子密钥与扩展后的48 bit明文进行S盒选择后输出32 bit的代码，将此代码用工作密钥C按KEELOQ加密算法加密函数 $f(A, K_i)$。设计流程图如图2所示。

图2 加密函数 $f(A,K_i)$的设计

1.5 输出设计

64 bit的明文经过加密后，运用DES加密算法输出R_{16}、L_{16}，此时，不要急于通过IP^{-1}置换，而是在置换前用原始密钥A把R_{16}、L_{16}各自加密，形成新的R_{16}、L_{16}然后再将二者合并通过IP^{-1}置换，输出密文。

2 工作流程

设某台读卡机为A，其28 bit产品序列号为XA，设一张用户卡为B，其28 bit产品序列号为XB。

（1）读卡机A将28 bit产品序列号XA与伪随机序列发生器产生的36 bit随机数形成64 bit明文，用双方约定的DES工作密钥A进行加密形成64 bit密文M，读卡机不停地将密文M向周围作明码呼叫，表示自己准备好了，如图3所示。

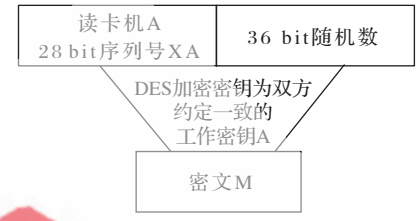

图3 读卡机发送学习信息

(2)当用户卡B进入读卡机A的场强范围，收到M后用相同的工作密钥A解密，将收到的随机数自加1形成新的随机数，然后发送用工作密钥A加密XB与新的随机数得到的密文N作回答表示已经收到密文M，学习完毕，如图4所示。

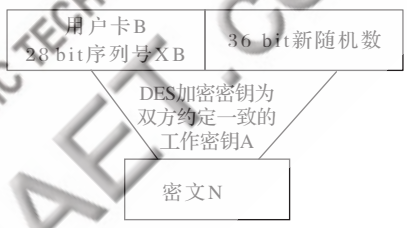

图4 用户卡回发的学习信息

(3)读卡机A收到N后，先用工作密钥A将其解密，得到XB与新随机数，此随机数取前32 bit作为以后KEELOQ加密的同步值，发送一次信息后，同步值自加1。然后，用长度为64 bit的厂商代码和28 bit的序列号XB经过运算得到原始密钥B，如图5所示。

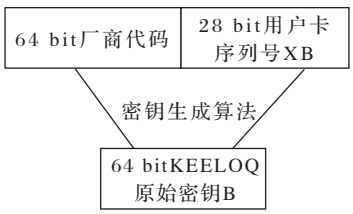

图5 读卡机生成原始密钥B

(4)原始密钥B对同步值进行KEELOQ加密，形成32 bit的同步数，如图6所示。

(5)读卡机A将工作密钥A去加密32 bit的同步数作为DES的加密密钥C；

(6)读卡机A将DES加密密钥C经过16轮迭代后产生16个子密钥，用于明文的加密。每一轮迭代过程中的加密函数需要以加密密钥C进行一次KEELOQ解密；

(7)读卡机A加密到R_{16}、L_{16}后再运用一次KEELOQ加密算法，用加密密钥C将R_{16}、L_{16}分别加密后，合并再通过一次置换输出密文。

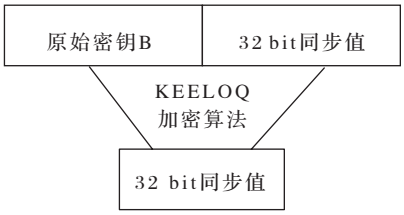

图6 读卡机生成32 bit同步数

(8)用户卡B接收到密文后，先用长度为64 bit的厂商代码和28 bit的本身序列号XB经过运算得到与A卡相同原始密钥B。

(9)用户卡B用先前收到的随机数的前32 bit作为同步值，用原始密钥B进行加密形成同步数。B卡用双方约定一致的工作密钥A以KEELOQ加密算法加密同步数形成加密密钥C，然后以此依次计算出16个加密子密钥。

(10)然后，用户卡B先将密文进行一次逆置换，分成2部分，前32 bit为一部分，后32bit为一部分，2部分分别用加密密钥C解密。

(11)用户卡B中用16个子密钥依次还原密文，每一轮迭代过程中的加密函数需要以加密密钥C进行一次KEELOQ解密。

(12)用户卡B中16轮解密完成后还原出64 bit明文。

(13)读卡机A继续向用户卡B发送密文，由于同步值的改变，使得最终的加密密钥改变，每发送一次信息，加密密钥都随之发生改变，进行明文的加密，同时，同步值也随之改变，为下一次的数据加密做准备。

(14)读卡机A中密文发送完毕，以工作密钥A加密XB为密文N送出，表示数据已经发送完毕。

(15)用户卡B收到N后，知道数据发送完毕后，然后，给A卡回发一个信息，表示已经接收完毕，信息格式是以出厂密钥加密XA形成的密文M。然后，B卡准备进行下一次的学习过程。

3 系统安全性分析

DES加密算法不能确证信息来源的真实性和用户的身份，而混合加密算法必须经过特定的学习才能得到正确的工作密码，不仅可以确定信息发送方的用户的身份，而且可以确定接收方的用户的合法性。混合加密算法能防止发送的码被截获后再转发带来的危害。接收方可以随时清除自己保存的学习信息，使原来的发送方不能控制自己，这样能有效避免第三方非法使用[5]。

对于KEELOQ算法很难用于数据加密的缺点，混合加密算法很好地弥补了这一点，对于数据加密选择DES算法，而对于密钥加密才选择KEELOQ算法，同样也很好地解决了KEELOQ算法传输效率低的缺点。同时，DES加密算法对于数据加密速度快、实现性高的优点完整地保存了下来，实现了数据加密速度快、密钥管理安全性高的要求。

因为每张卡的序列号均不相同，所以生成的密钥重复率几乎为零，实现了“一卡一密”，而为了保证系统安全，KEELOQ算法根据每张卡序列号以及同步值的改变使得每次加密出来的工作密钥都是唯一的、不规则的，且不重复。因此实现了加密密钥的“一次一密”，形成了滚动式的加密形式。由于非线性算法的复杂性及32 bit同步值每次传输时都更新，每次所传输的代码都与以前传输过的代码完全不同，在传输2^{32}次后才可能重复。

4 算法的软件实现

本设计过程中试验平台采用微软公司可视化编程工具套件Visual Basic。本设计主要用于Windows操作系统，在Windows环境下开发，用微软公司的集成开发环境VB6.0完成。运行环境Windows98/2000/XP。

厂商代码设置为0123456789ABCDEF，序列号设置为00001234，经过相应的计算得出原始密钥B：06B9CC9342459866。设置同步数为00000000，如图7所示。

图7 原始密钥B的生成

工作密钥A设置为1234567887654321，然后用KEELOQ加密算法，以原始密钥A加密同步值得出加密密钥C为F8225CE4A4C88261。如图8所示。

图8 加密密钥C的生成

密钥C生成后可以开始加密明文，输入明文“我是谁”。

生成明文的二进制为：1100111011010010110010101100011111100101110101101000000000000000。

经过加密计算后输出的密文为：

1110000101100001111001011111101011011111111110000000000000010010110。

根据输出的密文，进行解密后输出明文：我是谁。解密完毕。如图9所示。

(下转第12页)

其中，$\varphi(\cdot)$是sigmoid传递函数，w_{oj}表示隐藏层神经元j与输出神经元o的连接权重，其他类推。x_i表示输入向量的第i个分量。w是权重向量，其中的分量按照层号，层中神经元的个数及神经元序号顺序排列。系统多层感知器(MLP)结构如图3所示。

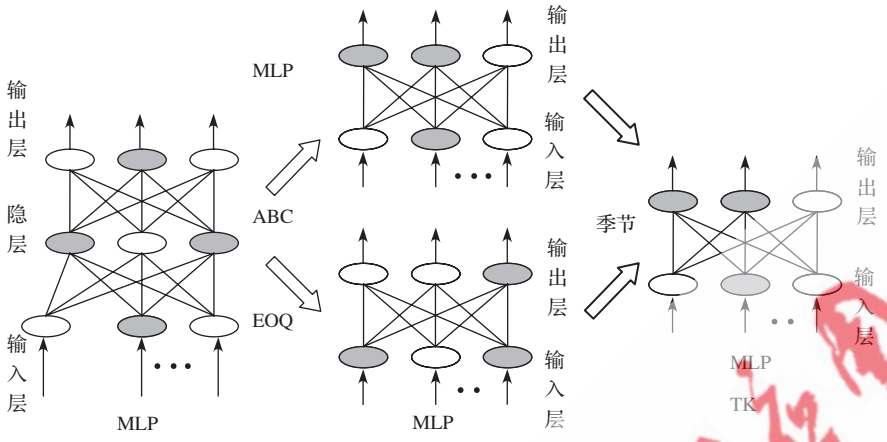

图3 库存多层感知器(MLP)

本文分别将ABC、EOQ和季节库存输入参数直接输入感知器，感知器输入层的神经元个数对应库存参数的个数。然后，利用S传递函数提取ABC库存参数，EOQ库存参数和季节库存参数。再将提取到的3种库存参数值合并为一个特征向量，输入感知器的下一层进行学习，压缩合并后的向量送入感知器。同时以数据库中保存的ABC-EOQ-季节模板为学习目标，试图预测出该库存的库存控制量。如果预测操作失败，回溯到特征合并前一步，分别将ABC库存控制参数向量和EOQ库存参数向量输入到ABC库存预测感知器和EOQ库存预测感知器，利用数据库中保存的ABC库存控制模板和EOQ库存模板进行预测，预测的结果再次与季节库存参数送入季节库存预测感知器，从而获得库存控制量的预测结果。

利用BP神经网络对库存进行库存控制量预测，可以提高系统性能。本文描述了BP神经网络算法，并提出用集中样本训练的方法和增加自适应因子改进BP算法。神经网络在某种程度上模拟了生物的感知特性，它是一种分布式并行处理结构的网络模型，具有自组织和自学习能力、很强的预测能力以及对不完全信息的鲁棒性。由于对库存控制量的综合预测有许多未知条件，神经网络方法可以通过学习获得对这些条件的隐性表达，使它的适应性更强，也易于实现。

下一步工作将对本文中提出的方法进行实验验证。同时，还将研究如何利用神经网络对EOQ、ABC管理以及季节控制库存预测及其相应的算法。

参考文献

[1] RUMEDE，HINTONGE，WILLIAMSR J. Learning representations by back-propagating errors[J]. Nature，1986，323: 533-536.
[2] 蒋宗礼. 人工神经网络导论[M].北京:高等教育出版社，2001.
[3] 何炎祥.神经网络技术在库存管理中的应用[J].计算机工程与应用，2002(15)：182-183.
[4] 谭坚坚，ABC分析法在库存管理中的应用研究[J].科教文汇，2006(4)：75-76.
[5] 杨帅.几类库存控制模型及其应用[D].重庆大学硕士学位论文，2005(6)：7-9.
[6] 刘振超，黄中鼎.面向不确知需求的库存控制问题[J].上海第二工业大学学报，2005，22(2)：32-33.

(收稿日期：2008-12-25)

上接第7页

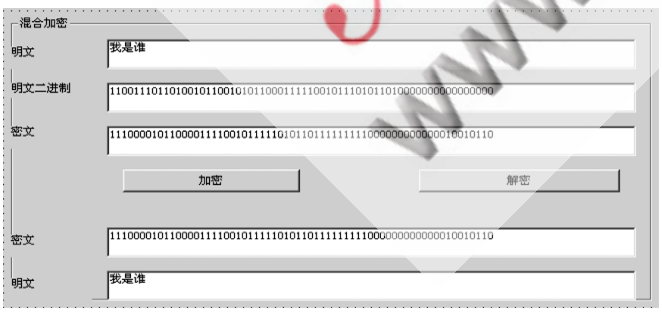

图9 加解密过程

本文详细介绍了混合加密算法各部分设计流程，并对混合后加密算法的安全性进行了分析，对于DES算法的密钥容易破解以及无法确定消息来源身份的缺点，混合加密算法在其运算过程中加入了KEELOQ算法，使DES的密钥破解的可能性大大降低，并且通过IC卡工作之前的特定学习步骤，可以确定消息来源的身份，解决了DES加密算法无法处理的问题。对于KEELOQ加密算法传输效率低以及无法用于数据加密的问题，混合加密算法采取了不用其加密数据，只是对加密密钥进行加密的办法，避开了KEELOQ无法解决的问题，很好地实现了IC卡既安全，加密速度又快的要求。

参考文献

[1] 陈鲁生,沈世镒. 现代密码学[M].北京:科学出版社,2002.
[2] 杨义先,钮心忻.应用密码学[M].北京:邮电大学出版社,2005.
[3] 李福平,金伟正,邓德祥.KEELOQ技术的软件实现[J].电子技术应用,2002,28(6):35-38.
[4] 章照止.现代密码学基础[M].北京:邮电大学出版社,2004.
[5] 求是科技.单片机通信技术与工程实践[M].北京：人民邮电出版社,2005.

(收稿日期：2008-12-27)