文章编号：1672-2892(2009)04-0349-05

一种适用于RFID读写器的加密算法及其实现

程 振[1]，刘年生[2,3]，李 琳[1]，郭东辉[1,3]

(1.厦门大学 电子工程系，福建 厦门 361005；2.集美大学 计算机工程学院，福建 厦门 361021；
3.厦门睿智微电子技术有限公司，福建 厦门 361005)

摘 要：介绍一种适用于RFID读卡器的XXTEA算法，分析结果表明与原来的分组TEA相比，XXTEA算法具有更高的安全性能、更快的运行速度和较小的负载等特点。针对Mifare 1智能卡所面临的安全威胁，设计了一种基于XXTEA算法的Mifare 1智能卡安全通信方案，通过密码动态变换及存取数据加密的方法来降低RFID通信数据被盗取的可能性，并采用MF RC500芯片在RFID读写器中实现了这一安全方案。

关键词：RFID读写器；XXTEA算法；MF RC500芯片

中图分类号：TP309 **文献标识码**：A

Encryption algorithm for RFID reader and its implementation

CHENG Zhen[1]，LIU Nian-sheng[2,3]，LI Lin[1]，Guo Dong-hui[1,3]

(1.Department of Electronic Engineering，Xiamen University，Xiamen Fujian 361005，China；
2.School of Computer Engineering，Jimei University，Xiamen Fujian 361021，China；
3.Xiamen Rich IT Microelectronic Technology Ltd.，Xiamen Fujian 361005，China)

Abstract：An XXTEA(Corrected Block Tiny Encryption Algorithm) algorithm suitable for RFID reader was introduced. The results of algorithm analysis showed that the XXTEA possessed better characteristics of high-performance security, fast encryption speed, and small size in comparison with original Block TEA. Considering the security threats faced by Mifare 1 smart card, a communication security scheme based on XXTEA was proposed. It minimized the potential of data purloining during the RFID communication, by means of password dynamic transformation and data encryption. The scheme was implemented in the RFID reader by using MF RC500.

Key words：RFID reader；XXTEA algorithm；MF RC500

随着电子信息技术的发展，非接触式智能卡(如RFID卡)已经在我们的生活中随处可见。与传统的接触式卡、磁卡相比，利用射频识别技术开发的非接触式智能卡，具有高度安全保密性和使用简单等特点，正逐渐取代传统的接触式IC卡，成为智能卡领域的新潮流[1]。然而，由于RFID系统的数据交流处于开放的无线状态，外界容易对系统实施各种信息干扰及信息盗取。

鉴于RFID系统数据交流开放的安全性问题，人们做了大量的研究工作[2-5]，提出了很多安全机制设计方面的建议。在硬件物理实现方面，提出了如：Kill标签、法拉第电罩等方法[2]；在软件系统实现方面，提出了一系列安全协议，如：Hash锁、随机Hash锁、Hash链[3]以及改进的随机Hash锁[4]等方法，而这些方法都是针对RFID标签芯片的制造而设计的，对已经大规模投入使用的智能卡而言，不具备实用性。目前在智能卡应用系统中，比较流行采用兼容ISO/IEC 14443协议的Mifare 1系列智能卡，其本身具有3次相互认证的安全协议，但其安全性仍有漏洞[6-7]，有必要在它安全机制基础上，引入一种数据加密算法来进一步保障数据通信的安全性。TEA算法作为一种微型的加密算法，有着简单、快速、安全性能好等特点，在电子产品开发领域得到了广泛应用，例如PDA数据加密[8]、嵌入式通信加密[9]等领域，而TEA算法的广泛使用导致产生了针对该算法的攻击方法，所以有必要对TEA算法进行改进。

为此，本文提出利用TEA算法的改进算法——XXTEA算法进行RFID读卡器与RFID智能卡之间密码数据的动态变换，来解决RFID系统应用中所面对的非法读取、窃听、伪装哄骗及重放等攻击。

收稿日期：2009-06-24；修回日期：2009-07-13

1 XXTEA 加密算法原理

在数据的加解密领域，算法分为对称密钥与非对称密钥 2 种。对称密钥与非对称密钥由于各自特点，所应用的领域不尽相同。对称密钥加密算法由于其速度快，一般用于整体数据的加密，而非对称密钥加密算法的安全性能佳，在数字签名领域得到广泛应用。

TEA算法[10]是由剑桥大学计算机实验室的Wheeler D J和Needham R M于1994年提出，以加密解密速度快，实现简单著称。TEA算法每一次可以操作64 bit(8 byte)，采用128 bit(16 byte)作为Key，算法采用迭代的形式，推荐的迭代轮数是64轮，最少32轮。为解决TEA算法密钥表攻击的问题，TEA算法先后经历了几次改进，从XTEA到Block TEA[11]，直至最新的XXTEA[12]。XTEA也称作TEAN，它使用与TEA相同的简单运算，但4个子密钥采取不正规的方式进行混合以阻止密钥表攻击。Block TEA算法可以对32位的任意整数倍长度的变量块进行加解密的操作，该算法将XTEA轮循函数依次应用于块中的每个字，并且将它附加于被应用字的邻字。XXTEA使用跟Block TEA相似的结构，但在处理块中每个字时利用了相邻字，且用拥有2个输入量的MX函数代替了XTEA轮循函数，这一改变对算法的实现速度影响不大，但提高了算法的抗攻击能力[13]，使得对6轮加密次数的算法攻击所需的明文数量由2^{34}上升为2^{80}，基本排除了暴力攻击的可能性。本文描述的安全机制所采用的加密算法就是TEA算法中安全性能最佳的改进版本——XXTEA算法。

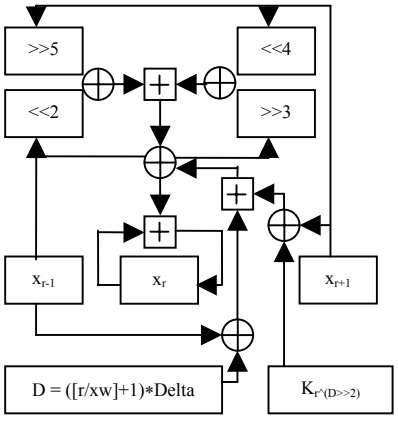

Fig.1 One round of XXTEA algorithm
图 1 XXTEA 算法的一轮循环过程

XXTEA的加密轮次视数据长度而定，最少为6轮，最多为32轮，对应的每轮加密过程如图1所示。图1中，⊞表示求和，⊕表示异或，>>表示右移，<<表示左移。

从图 1 中可知，XXTEA 算法主要包括加法、移位和异或等运算，它的结构非常简单，只需要执行加法、异或和寄存的硬件即可，且软件实现的代码十分短小，具有可移植性，非常适合嵌入式系统应用。由于 XXTEA 算法的以上优点，它可以很好地应用于嵌入式 RFID 系统当中。

2 RFID 读写器安全机制

整个RFID安全系统的整体框图如图2所示。本系统的设计思路是由上位PC机通过RS232接口控制MCU操作射频模块对Mifare 1智能卡进行操作，再将Mifare 1卡中的数据由MCU进行加解密运算，返回到主机的数据管理系统中。在此过程中，假设MCU与PC后台数据管理系统的数据通信是安全的，那么会被进行安全攻击的环节，就是智能卡与读写器之间的数据交换。Mifare 1智能卡的安全性能在最新的电子攻击面前变得日益单薄，且已被来自荷兰的黑客破译[5-6]，考虑到硬件升级的成本过大，本系统在不对基于Mifare 1的RFID读卡器硬件系统进行变动的情况下，将XXTEA算法嵌入到RFID系统中，设置特定的安全机制，以保护RFID数据的安全性。

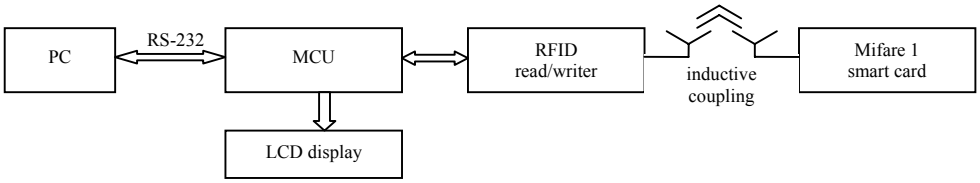

Fig.2 Architecture of RFID security system
图 2 RFID 安全系统的整体架构

整个系统的安全机制分为3个部分：对Mifare 1卡的读取控制密码的加密；对存入Mifare 1卡中的数据进行的加密；动态地进行密码的变换。加解密的函数设为：

$$\text{Data\_new} = \text{BTEA}(\text{Key}, n, \text{Data}) \tag{1}$$

式中：Data_new为数据进行加解密运算后的值；Key为XXTEA算法的密钥；n是数据组元的个数且用以控制加解密运算，$n > 0$表示进行加密，$n < 0$表示进行解密。在读卡器中，存放4个Key，Key_com,Key1,Key2,Key3分别作为4次XXTEA加解密运算的密钥，其中Key_com,Key1,Key2,Key3为16 byte且是固定在阅读器的存储器之中。根据XXTEA算法的输入与输出数据的长度限制，以2个长整数组元为加解密运算的基本单位，规定控制扇区读写权限的密钥KeyA,KeyB为XXTEA加密结果的前6个字节。

1) 对Mifare 1卡的控制密码的加密:由Mifare 1卡特性决定,任意扇区X与扇区Y的控制密码是完全不相关的。由于Mifare 1卡的独一无二的序列号特性，在整个系统所能支持的智能卡系列中，可以规定第X个扇区的密码是与该智能卡的序列号相关的。序列号的得到不需要经历密码校验，而只要对智能卡的操作到达防冲突这一步骤，就可以得到。序列号SNR为4字节，而每次XXTEA加密的数组都为2个长整型的数组，可以规定X扇区的密码为2个SNR所构成的1个64 bit数组与公用密钥Key_com进行加密的结果。假设扇区X的密钥为KeyA，则KeyA为BTEA(Key_com,2,SNR||SNR<<4)，取该结果的前6 byte为KeyA。有价值数据内容存在第Y个扇区内部，第Y个扇区的控制密码不固定，由第X个扇区的指定数据Data1经过XXTEA加密算法得来。具体过程如图3所示。系统的公钥Key_com是固定于阅读器内，虽然在公开信道上传递的信息中不包含此公钥的信息，但是还是有必要对其进行定期更新，才能确保安全性。

2) 对存入Mifare 1卡中的数据进行的加解密：经过一次加密运算得到扇区Y的密码后，通过Authentication命令完成对卡的认证后，就可以读取存放于扇区Y的有价值数据。读取到的是已经经过XXTEA算法进行加密完的数据。所以，有必要对其进行解密，才能得到真正的数据。而数据写入的过程与之对应，需要先将要写入Y扇区的数据以Key3进行XXTEA加密运算，再将运算结果写入到扇区Y中。由XXTEA算法的对称密钥特性可知，密钥是与加密该数据的密钥相同，固定存放于读卡器的存储器之中。具体过程如图3所示。

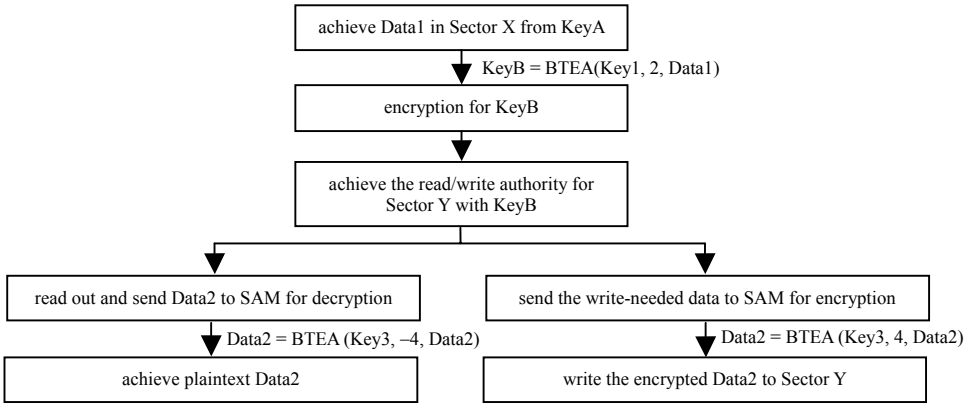

Fig.3 KeyB's got and en/decryption processing of data
图 3 KeyB 的得出和数据的加解密流程

3) 动态地进行密码的变换：在每次读写操作完智能卡之后，进行智能卡扇区Y密钥的动态变换。将扇区X内的数据，用Key2进行再次的XXTEA算法加密，变化得到一个新的数据。该新的数据写入扇区X。而对此Data_new进行Key1的加密运算得到扇区Y的新密钥，在已经验证扇区Y的密钥的情况下，更改此密钥为Data_new所对应的密钥，以便下次再次使用。具体如图4所示。

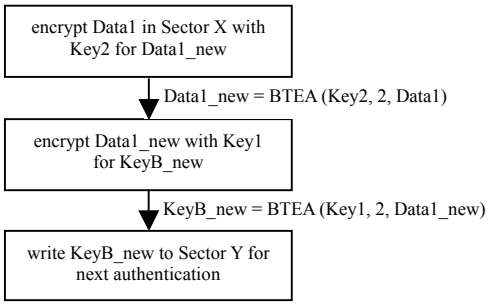

Fig.4 Dynamic change of password
图 4 密码的动态变化

3　RFID 应用系统实现

系统的硬件电路由NXP的专用读写芯片MF RC500和STC单片机STC89C52以及外部的天线滤波和接收回路组成，如图5所示。MF RC500读写芯片完全兼容于ISO/IEC 14443协议，且与MCU的接口多样化，特别适合于嵌入式系统应用。MCU除了操作读卡芯片进行常规的智能卡操作，也实现了系统所需的加密算法的嵌入，读取或写入数据的加解密运算都通过MCU进行。

MF RC500对Mifare 1卡的操作过程依照ISO14443[14]的协议规定，按先后的顺序为寻卡、防冲突、选择、密钥校验和之后的读写和增减值操作。MF RC500对Mifare 1卡的操作都是通过写入Transceive命令至Regcommand寄存器，再将操作Mifare 1卡的命令以数据的形式存放于Regfifodata寄存器中，设置完收发时钟的长度以后，就等待智能卡对读写命令的反应。在足够长的时间段之内，Mifare 1卡传输的数据就会在Regfifodata里面出现，此

时，先读取Regfifolength以确定数据的长度，根据长度写循环程序获取智能卡返回的信息。

图6给出了系统上位机的界面。通过上位机，在正常操作智能卡的基础上，进行动态更新密码的操作，以及隐藏在读写操作之下的加解密过程。

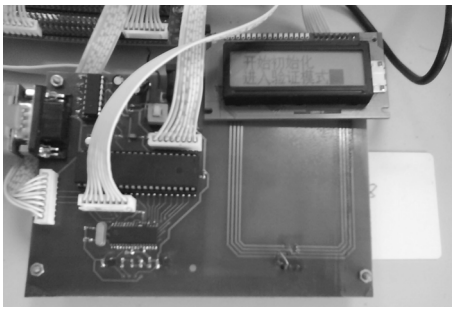

Fig.5 Hardware realization of system
图 5 系统的实物图

Fig.6 PC software UI for RFID system
图 6 系统的上位机软件运行用户界面

系统进行加密的试验如下：

1) 控制密码的得到：假设系统的公钥Key_com为{0x00112233,0x44556677,0x8899AABB,0xCCDDEEFF}，对于智能卡1，SNR为FDC711B8，根据系统的规定，扇区X的密码为KeyA与BTEA(Key_com,2,SNR||SNR<<4）相关，结果为{0xD3A7BA01,0x525F18FC}。取结果的前6个字节作为扇区X的控制密钥，即KeyA为D3A7BA0152。由此密码得到了扇区X的Data1，假设Data1为{0x00,0x11,0x22,0x33,0x44,0x55,0x66,0x77}。由此Data1和存储于MCU中的Key1通过XXTEA加密过程BTEA (key1,2,data1)，可以得到KeyB。假设Key1为{0x01234567,0x89ABCDEF,0x01234567,0x89ABCDEF}，通过加密，得到了{0x4CEFBEC2,0xC8CBACE0}，取前6 byte，则KeyB为4CEFBEC2C8。使用该密钥获得对扇区Y的控制权，就可以对价值数据进行读写操作，这样也避免了未经授权的读卡器想要非法对智能卡进行操作的情况。

2) 敏感数据的加解密：在Mifare 1智能卡中，数据是以块为单位来存储的，一块16 byte，可以由XXTEA直接运算得出加密结果。设需要写入的数据为{0x01,0x12,0x23,0x34,0x45,0x56,0x67,0x78,0x89,0x9A,0xAB,0xBC,0xCD,0xDE,0xEF,0xF0}，而密钥为Key3，设为{0xFEDCBA98,0x76543210,0xFEDCBA98,0x76543210}，通过该密钥进行XXTEA加密，得到加密后的数据为{0xA2,0xC6,0x6C,0x1A,0x3E,0x98,0x5E,0x48,0x7D,0xDA,0x68,0xC3,0x0C,0x23,0x1D,0x24}。将该数据写入智能卡中，读取时，对它用Key3作为密钥进行解密，得到所需数据。利用此种方法，使得明文在开放的传播空间内得到保护，保护了信息的安全。

3) 密码的动态变换：在进行完读写操作以后，为了保障智能卡的安全，要立刻进行密码的变换。Data1经过与key2的XXTEA运算后，变换为Data1_new。由此Data1_new推算出KeyB_new。假设Key2为{0xFEDCBA98,0x76543210,0x01234567,0x89ABCDEF}，则Data1_new为{0x23FF28AA,0xA76B4B04}，KeyB_new为3C7099D07F。此密码在智能卡中必须同步更新，防止出现读卡器未能取得智能卡扇区Y的读写控制权的问题。

通过对实验结果的分析可以看出，XXTEA所占用的代码空间为2 968 byte，占用内存空间124 byte，在24 MHz外部晶振条件下，加密速率为(3.26 ± 0.1) Kbps(p=0.01)，解密速率为(3.30 ± 0.1) Kbps(p=0.01)，抗攻击能力强，暂时没有一种可行的方法对该算法进行有效攻击[11]，而且防冲突性能好，微小的数据改变将导致结果的重大变化。控制密钥动态变换的根密钥和智能卡数据的加密密钥不经过明文传输，杜绝了RFID数据通信中出现的非法读取和监听等威胁。

4 结论

在XXTEA加密算法基础上的新RFID系统安全方案，具有安全性高、低成本和兼容性高的特点。实验结果表明，新方案能有效地提高RFID数据传输的安全性，可将RFID的应用范围推广到信息敏感的领域，包括金融交易、食品安全和公共安全等。

参考文献：

[1] Want R. An Introduction to RFID Technology[J]. IEEE Pervasive Computing, 2006,5(1):25-33.

[2] EPCGLOBAL INC[EB/OL]. [2009-06-24]. http://www.epcglobalinc.org/standards_technology/specifications.html.

[3] Kim H S, Oh J H,Choi J Y. Security Analysis of RFID Authentication for Pervasive Systems using Model Checking[C]// Proc. of the 30th Annual International Computer Software and Applications Conference. 2006.
[4] 曾丽华,熊璋,张挺. Key 值更新随机 Hash 锁对 RFID 安全隐私的加强[J]. 计算机工程, 2007,33(3):151-153,159.
[5] 王文闯,王可人. 基于数据缓存机制的 RFID 安全协议[J]. 信息与电子工程, 2008,6(5):371-374,382.
[6] Nohl K,Plotz H Mifare,little security, despite obscurity[C]// Presentation on the 24th Congress of the Chaos Computer Club. Berlin, 2007.
[7] Garcia F D,Koning Gans G,Muijrers R,et al. Dismantling MIFARE Classic[R/OL]. [2009-06-24]. http://www.sos.cs.ru.nl/applications/rfid/2008-esorics.pdf.
[8] 肖礼盛,朱绍文,李中正,等. 基于 PDA 电路加密模块的实现[J]. 信息安全与保密, 2007,(4):106-107,110.
[9] 程峰,刘昊钰,欧阳名三,等. 加密算法在智能抄表系统中的应用[J]. 计算机时代, 2004,(4):14-15.
[10] Wheeler D J,Needham R M. TEA, a Tiny Encryption Algorithm[C]// Fast Software Encryption. 1994:363-366.
[11] Needham R M,Wheeler D J. Tea extensions[R/OL]. [2009-06-24]. http://www.movable-type.co.uk/scripts/xtea.pdf.
[12] Needham R M,Wheeler D J. Correction to xtea[R/OL]. [2009-06-24]. http://www.movable-type.co.uk/scripts/xxtea.pdf.
[13] Saarinen M. Cryptanalysis of block tea[R/OL]. [2009-06-24]. http://www.cc.jyu.fi/ mjos/block_tea.ps.
[14] ISO/IEC 14443-3. Identification Cards-contactless Integrated Circuit(s) Cards-proximity Cards-Part 3: Initilization and anticollision[S]. 2001.

作者简介:

程　振(1983-),男,福建省莆田市人,在读硕士研究生,主要研究方向为 RFID 技术及其安全机制研究.email:jeanszhen@gmail.com.

刘年生(1967-),男,湖北红安县人,博士,副教授,主要研究方向为网络安全与人工智能.

李　琳(1982-),女,福建省福安市人,助理教授,主要研究方向为语音识别和集成电路设计.

郭东辉(1967-),男,福建省莆田市人,教授,博士生导师,主要研究方向为人工智能、网络通信和集成电路设计等.