# 二重 keeloq 算法在智能门禁系统中的应用研究

吴伟坚 陈世国 李 丹
(贵州师范大学物理与电子科学学院 贵阳 550001)

**摘 要** 门禁系统一直是智能建筑的重要组成部分,而 Keeloq 滚动码技术在智能门禁系统、无线门锁装置等领域都具有广泛的应用。分析了 keeloq 算法对门禁系统钥匙码的加密解密原理和其在应用上的不足,归纳了单重 keeloq 算法和多重 keeloq 算法的一些问题,提出了二重 keeloq 算法。二重 keeloq 算法并不是简单地对一个钥匙码进行二次 keeloq 算法加密,而是在一重 keeloq 算法加密的基础上对钥匙码中所包含的一些关键信息再进行部分加密,两次加密的明文长度和加密资料均不相同。这种加密方式在增加钥匙码复杂度的同时,相对于多重 keeloq 加密方式减少了系统在钥匙码加密和解密过程中所带来的计算开销。

**关键词** keeloq 算法,智能门禁系统,密码攻击,系统安全性
**中图法分类号** TN918.4 **文献标识码** A

## Application of Dual Keeloq Algorithm in Intelligent Access Control System

WU Wei-jian CHEN Shi-guo LI Dan
(School of Physics and Electronic Science, Guizhou Normal University, Guiyang 550001, China)

**Abstract** Access control system has always been an important part of access control system , and Keeloq rolling code technology has a wide range of applications in intelligent access control systems, wireless door locks and other fields. This paper analyzed the encryption and decryption principle of keeloq algorithm and its application in the key code of the access control system. Summarizing some problems of single keeloq algorithm and multiple keeloq algorithm, this paper provided a kind of scheme called dual keeloq algorithm to improve its security. The dual keeloq algorithm is not a simple secondary keeloq algorithm for a key code encryption, it's another keeloq algorithm encryption of the important field of key code on the basis of single keeloq algorithm encryption. The required information and the code length are different in the two encryption. This encryption method increases the complexity of key code. At the same time, compared to multiple keeloq encryption, it reduces the overhead of system calculation in the key code encryption and decryption process.

**Keywords** Keeloq algorithm, Intelligent access control system, Password attack, System security

20 世纪 80 年代,南非学者 Willem Smit 设计出了一种名为 keeloq 的非线性密码算法。随后,美国的 Microchip 公司将具有不规则加密密码、高安全性等特点的 keeloq 滚动码技术成功地应用在无线门锁系统、遥控开关、PEPS 系统[1]等领域。2008 年,Courtois 等提出了能破解 keeLoq 密码的 4 种滑动-代数攻击方法[2]。2010 年,游建雄等[3]提出差分故障攻击方法,有效提高了对 keeloq 算法的攻击效率。2012 年,Courtois T 等[4]又指出只需要两个明文即可破解 keeloq 算法的加密密匙,并提出了自相似攻击方法。但这些破解方法都是基于对明文的单重 keeloq 加密方式上的破解。目前,在 keeloq 算法的应用研究方面,为了提高密码复杂度和系统安全性,三重 keeloq 算法已被提出。但它只是对同一个加密明文作简单的三次加密,其加密的密码长度都是一样的。本文研究了 keeloq 算法对门禁系统钥匙码二重加密的改进方案,二次加密的密码长度和加密资料都不一样。这种加密方式在不大幅增加系统计算开销的情况下,增大了钥匙码的复杂度,从而提高了系统的安全性。

## 1 keeloq 算法介绍与分析

### 1.1 32 bits 的明文加密方式

keeloq 滚动码技术的本质就是一种基于不平衡 Feistel 结构的非线性分组密码算法,其标准实现是采用 64 bits 加密密钥经过 528 次迭代将 32 bits 明文加密成 32 bits 密文。在解密过程也是利用 64 bits 加密密钥经过 528 次迭代将 32 bits 密文解密成 32 bits 明文。

32 位 keeloq 加密算法的数学表达式为:

$$\Phi^i = NLF(L_{31}^i, L_{26}^i, L_{20}^i, L_9^i, L_1^i) \oplus L_{16}^i \oplus L_0^i \oplus k_{i \bmod 64}$$

$$L^{i+1} = (\Phi^i, L_{31}^i, \cdots, L_1^i), i = 0, 1, 2, \cdots, 527 \quad (1)$$

其解密算法的数学表达式为:

$$\theta^i = NLF(L_{30}^i, L_{25}^i, L_{19}^i, L_8^i, L_0^i) \oplus L_{15}^i \oplus L_{31}^i \oplus k_{i-1 \bmod 64}$$

$$L^{i-1} = (L_{30}^i, \cdots, L_0^i, \theta^i), i = 528, \cdots, 2, 1 \quad (2)$$

其中,$L$ 是 32 位的明文,$i$ 是滚动次数,$NLF$ 是非线性布尔函数,其标准表达式为:

本文受贵州省科学技术基金(黔科合 J 字[2007]2213 号,黔科合 J 字[2010]2145 号)资助。
吴伟坚(1991－),男,硕士生,主要研究方向为嵌入式应用技术、物联网、智能家居,E-mail:870268314@qq.com;陈世国(1967－),男,博士,教授,主要研究方向为核信号处理及原子分子物理,E-mail:924678590@qq.com(通信作者)。

$$NLF(a,b,c,d,e)=abc\oplus abd\oplus ace\oplus ade\oplus de\oplus cd\oplus be\oplus bc\oplus ae\oplus ac\oplus e\oplus d \quad (3)$$

### 1.2 16 bits 的明文加密方式

在 NLF 非线性布尔函数的运算规则下，若明文码中有 1 位码发生改变，则整个输出密文将变得完全不同。经实验发现，keeloq 算法不仅能对 32 位的明文加密，还可以对 16 位、8 位、64 位的明文进行加密，其迭代不限于 528 次，这个特点增加了 keeloq 算法对密码加密的灵活性和安全性，也是本文提出的二重 keeloq 算法的来源依据。以 16 位明文加密为例，NLF 函数有 5 位输入码，分别获取 16 位明文 $S$ 的 $S_{15}^i$，$S_{12}^i$，$S_{10}^i$，$S_5^i$，$S_1^i$ 5 位，输出码再与明文中的 $S_8^i$ 和 $S_0^i$ 以及钥匙 $K$ 进行异或运算，经 256 次迭代移位后，得出 16 位的加密密文。

16 位 keeloq 加密算法的数学表达式为：

$$\Phi^i=NLF(S_{15}^i,S_{12}^i,S_{10}^i,S_5^i,S_1^i)\oplus S_8^i\oplus S_0^i\oplus k_{i \bmod 64}$$

$$S^{i+1}=(\Phi^i,S_{15}^i,\cdots,S_1^i),i=0,1,2,\cdots,255 \quad (4)$$

其解密算法的数学表达式为：

$$\theta^i=NLF(S_{14}^i,S_{11}^i,S_9^i,S_4^i,S_0^i)\oplus S_7^i\oplus S_{15}^i\oplus k_{i-1 \bmod 64}$$

$$S^{i-1}=(S_{14}^i,\cdots,S_0^i,\theta^i),i=256,\cdots,2,1 \quad (5)$$

### 1.3 二重明文加密模型

二重 keeloq 算法对明文码加密的模型如图 1 所示，其过程是先对一部分重要的数据进行一重加密，加密后的一重密文与另一部分信息进行拼接后再作 32 位的二重加密，模型以 16 位明文码为例进行一重加密。

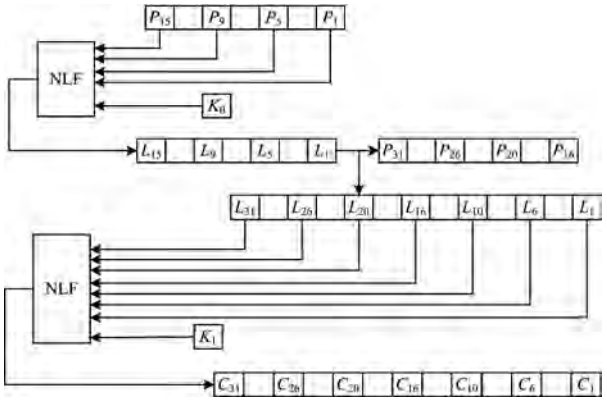


图 1 二重 keeloq 加密过程

## 2 门禁系统中二重 keeloq 算法的应用

无线门禁系统包含钥匙端和锁系统端，钥匙端的作用是对钥匙码进行算法加密，锁系统端是对接收到的密文码进行算法解密及判断，并调用相应处理程序。每个厂商对门禁系统的设计都有自己的方式，本文利用上文中 keeloq 加密算法的改进方案来设计门禁系统。

### 2.1 钥匙码的设计

本文设计的是 32 位的钥匙码，它是由 16 位的同步计数值(SYNC)、2 位溢出位、10 位的厂商的识别码(SN)和 4 位的按键值(S0，S1，S2，S3)组成。钥匙码加密一次，同步计数值就加一，所以每次通过 keeloq 算法加密后输出的密文码都变得面目全非，而且每次密文都具有唯一、不重复的特点。图 2 为 32 位钥匙码的设计模型。

| 按钮信息 4 bits | 溢出位 2 bits | 识别码 10 bits | 同步计数值 16 bits |
|---|---|---|---|

图 2 32 位钥匙码的设计模型

### 2.2 改进方案的钥匙端设计

钥匙端采用 Microchip 公司的 HCS365 芯片作为主控制器，实现二重 keeloq 算法的加密。其内置的 EEPROM 用于存储同步计数码(SYNC)、10 位由厂商提供的识别码(SN)、加密钥匙(KEY)、滚动次数(ROLL_TIMES)等。外置无线收发模块用来发送已加密的密文和与锁系统端进行身份验证等信息交互。智能钥匙端的工作流程图如图 3 所示。


图 3 改进方案中智能钥匙端的工作流程

智能钥匙端有 4 个按键(S0，S1，S2，S3)，当其中一个按键或按键组合被按下后，其信息都会经过二重 keeloq 算法加密后发出。信息到达锁端并被解密后，将根据按键的不同做出不同的响应。识别码(SN)是用来匹配钥匙与锁的码，两端具有共同性。由于钥匙端使用嵌入式芯片实现，keeloq 算法所需参数的封闭性极高，这使得很多攻击方式因获取不了足够的信息而失败。钥匙端所使用的加密钥匙(KEY)有 2 把，其位数不一样，加密对象的长度也不一样，keeloq 加密时所滚动的次数也不一样。keeloq 算法加密的特点之一是只要滚动次数不一样，产生的密文也不一样；即便密钥不小心被泄露，也还有一把长度未知的密钥；即便都被泄露，二重加密的明文长度依旧未知，滚动次数也未知等。这些因素无疑增加了密码的复杂度和破解的难度。

### 2.3 改进方案的锁端设计

锁端也同样选用 Microchip 公司的 HCS365 芯片作为解码主控制器，扩展无线收发模块进行身份验证与接收密文。外围配置门锁驱动电路实现控制门锁的开关和声光电路以供用户操作提示。锁端会根据从钥匙端接收到的按键码调用相应程序，按键码可作为系统功能的扩展资源。智能门禁系统的锁端与钥匙端进行信息交互之前会有一段身份认证。若是非法钥匙，则直接将其传输过来的数据视为无效。其工作流程图如图 4 所示。

若合法的钥匙有数据进入锁端，系统则会对接收到的密文进行一重解密，解密后会截取识别码(SN)与 EEPROM 中存储的信息进行校验，若校验失败，则直接返回，不进行第二

次解密，以减少系统解密时带来的开销；若校验成功，则进行二重解密。二重解密后再校验重要的 16 位同步计数值信息是否正确。若正确，锁端则给钥匙端发送开锁反馈，自身的同步计数值加一，并执行相应的按键响应。

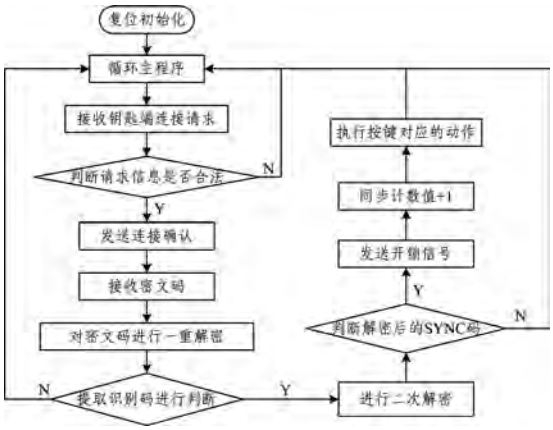


图 4　改进方案中锁端的工作流程

### 2.4　系统的学习过程

门禁系统的学习是应对钥匙丢失或加密密码和钥匙码泄露的情况，也可能是当系统被使用很久后为了安全起见，系统需要重新学习 keeloq 算法中加密所需的资料，如加密密码(KEY)、识别码(SN)等。钥匙端和锁端都具备重新学习的功能，目的是使 keeloq 算法在加解密时所需资料库可同步更新。系统进入学习模式后，通过以下几个步骤完成学习过程，以获得最新的加解密资料库。

步骤 1　用户把自定义的新资料库输入学习器。

步骤 2　学习器通过无线的方式给钥匙端输入学习命令，使钥匙进入学习模式；调用学习程序，把用户自定义的资料存储到钥匙端的 EEPROM。

步骤 3　学习器以同样的方式对锁端执行相同的操作，以确保两端使用的资料库是配对的。

## 3　改进方案的安全性与性能分析

### 3.1　安全性分析

keeloq 标准算法利用 64 bits 的加密钥匙 $K=(k_{63},k_{62},\cdots,k_0)$把 32bits 的明文数据 $P=(p_{31},p_{30},\cdots,p_0)$经过 528 轮的计算迭代，生成一个面目全非的 32 bits 密文数据$C=(c_{31},c_{30},\cdots,c_0)$。假设按相关比特位来衡量密码的复杂度，经过一重 keeloq 算法加密后的密文数据的复杂度记为 O(64×32)。对于原三重 keeloq 加密[5]，每次加密的明文长度都一样，三重加密后的密码复杂度是 O(64×32+64×32+64×32)，比一重加密的方式提高了 200%。明文经过改进的二重 keeloq 加密后，由于不确定第二次加密明文的长度，因此能加密的明文长度都需纳入计算，则其复杂度为 O(64×32+64×24+64×16+64×8)。相比于一重 keeloq 加密，其密码复杂度提高了 150%。

即便使用通用的密码穷尽搜索法和密码分析的手段[6]破解出了第一轮的加密数据，但在改进的二重 keeloq 算法中，还有另一重未知长度的加密密文和未知加密钥匙需要破解，这无疑大大地增加了实际应用中的密码破解难度。

### 3.2　性能分析

智能门禁系统引入改进的二重 keeloq 算法后，其通信代价与原来的系统差异不大，都是传输 32 bits 的密文数据和一些必要的交互信息。但从系统加密解密的计算开销方面进行比较就能发现二重 keeloq 加密的优势。整个算法在系统的实现上分为加密和解密两个阶段，分别对原 keeloq 算法、三重 keeloq 算法以及改进的二重 keeloq 算法实现的系统进行比较，结果如表 1 所列。

表 1　系统计算开销对比

| | 原 keeloq | 三重 keeloq | 改进的二重 keeloq |
|---|---|---|---|
| 加密 | 迭代 528 次 | 迭代 528×3 次 | 迭代 528+256 次 |
| 解密 | 迭代 528 次 | 迭代 528×3 次 | 迭代 528+256 次/528 次 |
| 安全系数 | 低 | 较高 | 较高 |

从表 1 和上述复杂度分析可知，在加密过程中，改进的二重 keeloq 算法的计算开销上与原 keeloq 算法相比增加 50%，但密码的复杂度却提高了 150%，原三重 keeloq 算法的复杂度相对于一重加密提高了 200%，计算开销也增加了 200%。

在解密过程中，改进的二重 keeloq 算法的计数开销取决于输入密文的正确性。如果输入密文是正确的，则需要两次解密；若输入密文是错误的，则解密一次后就返回，减少了系统对错误密文的计算投入。

**结束语**　文中介绍了 keeloq 算法的一种改进应用并在智能门禁系统中实现了对钥匙码的加密和解密。改进的二重 keeloq 算法是对明文码中的一部分再次进行加密。这个改进方案的灵感来源于本人在对标准的 keeloq 算法做研究时的发现，keeloq 算法不仅可以对 32 位的明文进行加、解密，还可以对不同长度的明文做加密和解密，这只需在 keeloq 算法的公式和实现代码中做相应的改动即可。同时，keeloq 算法所需要的加密参数规格是可以改变的，如加密钥匙的长度、明文的长度、滚动次数等。本文在参考 3DES 算法[8]及三重 keeloq 算法等的相关文献后，把其改进算法应用到智能门禁系统中，提高了系统的安全性。

## 参 考 文 献

[1]　李娟，王宏大，祝慧，等. 一种基于功能安全的汽车 PEPS 系统[J]. 农业装备与车辆工程，2014(4)：57-59.

[2]　COURTOIS N T，BARD G V. Algebraic and slide attacks on KeeLoq[OL]. http://eprint.iacr.org/2007/062.

[3]　游建雄，李瑞林，李超. 轻量级分组密码 Keeloq 的故障攻击[J]. 北京大学学报(自然科学版)，2010，46(5)：756-762.

[4]　COURTOIS N T. Self-similarity attacks on block ciphers and application to keeloq [M]// Cryptography and Security：From Theory to Applications. Springer Berlin Heidelberg，2012：55-66.

[5]　刘璟，陈惠滨，叶文才. KeeLoq 算法的改进与实现[J]. 信号处理，2014，30(11)：1335-1338.

[6]　赵烽. KEELOQ 加密算法安全性探究[J]. 信息网络安全，2011(8)：29-31.

[7]　王秋燕，金晨辉. KeeLoq 密码第 1 种滑动-代数攻击的改进[J]. 计算机工程，2009，35(16)：133-137.

[8]　张健，任洪娥，陈宇. 密码学原理及应用技术[M]. 北京：清华大学出版社，2014.

[9]　李玲，陈惠滨. 基于 KEELOQ 的无线遥控车位锁系统设计[J]. 电子技术应用，2013，39(12)：52-54.

[10]　游子毅，李丹，肖文君. 改进的 keeloq 算法及其在无钥匙进入与启动系统中的应用[J]. 科学技术与工程，2017，17(20)：181-183.