第 30 卷 第 11 期 信 号 处 理 Vol. 30 No. 11
2014 年 11 月 JOURNAL OF SIGNAL PROCESSING Nov. 2014

KeeLoq 算法的改进与实现

刘 璟[1,2] 陈惠滨[2] 叶文才[2]
(1. 厦门大学物理系，福建厦门 361005; 2. 集美大学信息工程学院，福建厦门 361021)

摘 要: 随着电子门控设备的普及，通过手机实现门锁智能化控制开始逐渐兴起，但是提升其通信安全性仍是值得研究的问题。本文通过详析 KeeLoq 加解密算法基本原理，归纳当前的主要攻击方法，指出其安全性上的不足。借鉴 3DES 算法，提出了三重 KeeLoq 算法，加大破解难度，进一步改善其安全性能。并结合蓝牙通信及 Android 应用程序设计方法，将该算法成功地应用于智能门控系统中，将多种门锁钥匙软件化，实现低成本、高安全性、人性化及绿色环保智能门控系统的设计。

关键词: 三重 KeeLoq 算法; Android; 16F630
中图分类号: TN918.4 **文献标识码**: A **文章编号**: 1003 - 0530(2014)11 - 1335 - 04

Improvement and Implementation of KeeLoq Algorithm

LIU Jing[1,2] CHEN Hui-bin[2] YE Wen-cai[2]
(1. Department of Physics, Xiamen University, Xiamen, Fujian 361005, China;
2. School of Information Engineering, Jimei University, Xiamen, Fujian 361021, China)

Abstract: As the popularity of electronic-controlled locks, the intelligent lock contorlled by cellphones begins to spring. However, it deserves to further study and improve its communication security. According to the detailed rationale of KeeLoq codec algorithm and the induction of previous attack researches, the security lack of KeeLoq codec algorithm was indicated. Taking example by 3DES algorithm, the triple KeeLoq codec algorithm was proposed to increase the crack difficulties, which its security was better improved. Associated with the bluetooth communication technology and the design method of Android applications, the triple KeeLoq codec algorithm was implemented in the design of intelligent locks. Due to multifarious software-based keys, the intelligent lock owns overwhelmed advantages of lowcost, high security, humanity and green environmental protection.

Key words: triple KeeLoq codec algorithm; Android; 16F630

1 引言

编解码算法不断推陈出新，及电路高度集成化发展，极大地推动了低成本、高安全性能的无线射频加解密技术的发展[1-2]。以前广泛应用的固定编解码技术和芯片[3]因为其低安全性已经逐渐开始被市场淘汰。滚动编解码[4-5]电路以其高安全性逐渐占据市场的主流。

Microchip 公司有一系列的滚动编码专用集成芯片。其核心是将 KeeLoq 加解密算法封装于专用集成芯片，并广泛应用于汽车防盗[1-2,6]、遥控车库门禁[5]等系统中。KeeLoq 是一种先进的非线性位加密算法，能产生具有极高保密性的滚动编码。每一次发送的代码都是惟一的、不规则的、且不重复，使得任何通过非法捕捉和扫描跟踪等破译手段都化为泡影。

本文将系统探讨 KeeLoq 算法及其实现机制，深入分析其存在的缺陷，并提出改进措施，以进一步提高它的安全性。最后基于 Android 平台智能手机设计一手机开锁应用软件，将用户的开锁操作采用 KeeLoq 加密编码，通过蓝牙通信模式，将密文传输至单片机端解密，实现用户开门操作。

2 KeeLoq 算法介绍

2.1 KeeLoq 运算规则

KeeLoq 算法的核心思想就是加密端用 64bits 密钥加密 32bits 明文，从而得到 32bits 密文。密文经无线发射，由解密端接收后再经过该 64bits 密钥解密 32bits 密文，还原出原 32bits 明文后执行用户操作。KeeLoq 算法演算过程需要定义一个数据寄存器，用于存放 32bits 明文 $y_{31\sim0}$ 或者 32bits 密文 $y_{31\sim0}$，和一个

收稿日期: 2014 - 07 - 03; 修回日期: 2014 - 09 - 05
基金项目: 厦门科技项目(3502Z20133019，3502Z20143020); 福建省教育厅科技项目(JA12200，JA11157); 集美大学潘金龙学科建设基金(C512038)

密钥寄存器，用于存放 64bits 密钥 $k_{63\sim0}$。

KeeLoq 数据加密过程模型图如图 1 所示，首先定义一个非线性表，这个非线性表有 5bits 输入码，1bit 输出码。它在数据寄存器中间隔均匀地取 5bits：y_{31}，y_{26}，y_{20}，y_9，y_1，通过式(1) NLF(Nonlinear Logic Function) 运算产生一个输出码。输出码再与数据寄存器中的 y_{16} 与 y_0 以及密钥寄存器中的 k_0 进行异或运算后生成 1bit 加密数据码。每生成 1bit 加密数据码，密钥寄存器和数据寄存器分别进行移位，密钥寄存器作循环移位，加密数据码作为数据寄存器移位的输入，重复上述步骤 528 次后，得到 32bits 的输出密文。

$$\mathrm{NLF}(x_4,x_3,x_2,x_1,x_0)=x_4x_3x_2\oplus x_4x_3x_1\oplus x_4x_2x_0\oplus x_4x_1x_0\oplus x_4x_2\oplus x_4x_0\oplus x_3x_2\oplus x_3x_0\oplus x_2x_1\oplus x_1x_0\oplus x_1\oplus x_0 \tag{1}$$

KeeLoq 数据解密模型图如图 2 所示，其过程的运算方法与数据加密过程的运算方法基本一致，只是其中运算数据的数据位发生变化。非线性表的 5bits 输入码改成从数据寄存器中间隔均匀地取固定 5bits：y_{30}，y_{25}，y_{19}，y_8，y_0。通过式(1) NLF 运算产生 1bit 输出码后输出码，再与数据寄存器中的 y_{31} 与 y_{15} 以及密钥寄存器中的 k_{15} 进行异或运算后生成 1bit 解密数据码。每输出 1bit 解密数据码后，密钥寄存器和数据寄存器分别进行移位，密钥寄存器作循环移位，解密数据码作为数据寄存器移位的输入，重复上述步骤 528 次后，还原出 32bits 的明文。

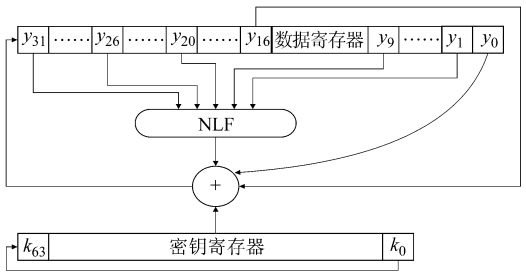

图 1 KeeLoq 加密模型图

Fig. 1 KeeLoq encryption model diagram

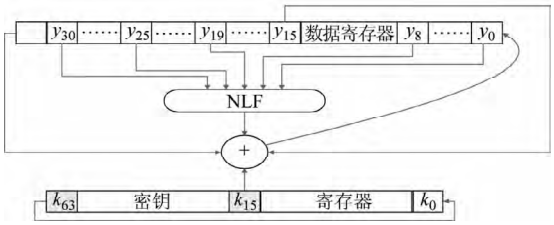

图 2 KeeLoq 解密模型图

Fig. 2 KeeLoq decryption model diagram

2.2 KeeLoq 实现机制

采用 KeeLoq 方法实现数据加密和解密，其通信过程需严格按照下述过程进行。首先，要求加密端和解密端都需要有非易失性存储空间以存储 64bits 密钥(用于加解密，可编程且不被发送不可泄露)、28bits 序列号(用于区分不同的加密端)、16bits 同步计数值(用于产生加密编码滚动效果，每完成一次数据传送后，其值自加 1 后更新)、10bits 识别码(序列号的低 10bits) 和 32bits 种子码(安全模式下用来生成密钥)。

当用户有按键操作时，KeeLoq 加密端将 4bits 功能键、10bits 识别码、16bits 同步计数值和 2bits 溢位组合成 32bits 明文，按照图 1 的 NLF 运算规则加密成 32bits 密文，再加上 34bits 固定码(28bits 序列号、4bits 功能键和 2bits 状态位)，组合成一组 66bits 的加密数据发送。由于每次发送过程，同步计数值自加 1，使得每次发送的 32bits 密文都是惟一的、不规则的、且不重复，故称之为滚动码，可以有效的防止密码捕捉和密码拷贝。由于 66bits 的加密组合达到 $2^{66}=7.38\times10^{19}$，因而可以有效的防止密码扫描。

解密端接收到 66bits 密文数据后，首先匹配加密端的序列号一致后，按照图 2 的 NLF 运算规则还原出 32bits 明文。再校验 32bits 明文中的识别码、功能键与固定码中的 28bits 序列号的低 10bits、功能键一致后，最后判断同步计数值是否合理增加(加密端同步计数值大于解密端同步计数值，且小于 4)。确认成功后根据功能键定义，控制相应执行机构动作。

3 KeeLoq 算法不足与改进

3.1 KeeLoq 算法的安全性与不足

KeeLoq 算法的 NLF 运算规则，使得一个很小的输入变化量，也会造成很大的输出变化量，产生的加密编码滚动效果。密码分析者就无法通过输入微小的变化来观察分析输出的变化，从而破解出密钥，使得 KeeLoq 算法具有安全性高特点[4]。

虽然 KeeLoq 算法发布于 20 世纪 80 年代，但直到 2007 年，Bogdanov[7] 才首次对 KeeLoq 算法进行攻击，他使用猜测-决定和滑动技术来完成攻击，攻击的时间复杂度为 252，空间复杂度为 16GB。在 2008 年，Courtois[8] 等人提出了 4 种滑动-代数攻击方法，其主要思想是利用 KeeLoq 算法连续 64 圈圈函数形成的置换和圈结构与随机置换圈结构的差异，先攻击密钥的前 16bits，再攻击剩余的 48bits。折合计算复杂性至少约为 $O(2^{43})$ 次加密。2010 年，游建雄[9] 等人提出 3 种不同采用面向字节的差分故障攻击方法，其中攻击效率最好的方法，恢复 1bit 密钥信息平均只需要 0.707617 个错误，恢复 64bits 的种子密钥只需要 46 个错误。

虽然 KeeLoq 算法发布后至今已经取得很多有效的攻击，大大降低了计算时间复杂度，但是也增加了计算空间复杂度，并且需要一定数量的已知前提。导致在实际密码破解过程中难度系数高，故其安全性足以保证，在实际应用当中有着广泛应用。

3.2　KeeLoq 算法的改进

KeeLoq 加密算法是 32bits 的分组密码，密钥长度较短，仅为 64bits。算法发布至今已有相关文献报导取得有效攻击，针对这一现状及上述算法不足之处，为了进一步提高 KeeLoq 算法安全性，本文分别对加解密过程进行改进。

由于 KeeLoq 编码过程利用同步计数值自加，使得每次发送的 32bits 密文具有惟一、不规则且不重复特性，从而有效的防止密码捕捉和密码拷贝。改进加解密过程借鉴了三重数据加密算法[10]（3DES，Triple Data Encryption Algorithm），提出如图 3 的三重 KeeLoq 编解码算法。加密过程采用三个不同密钥，按照图 1 NLF 编码流程分别对明文、第一重密文、第二重密文加密，得到 32bits 最终密文。所产生的第一重密文、第二重密文都有较多的数据位变化，所得到的最终密文随机性更强。采用不同方法破解的时间复杂度是单次时间复杂度的三次方倍，这将更加有效保证其安全性。解密过程反过来，采用三个相应密钥，按照图 2 NLF 解码流程分别对最终密文、第二重密文、第一重密文解密，得到 32bits 明文后，经匹配识别码、功能键与序列号后执行用户功能操作。

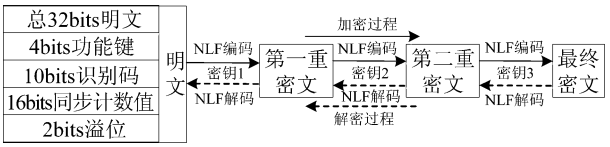

图 3　三重 KeeLoq 加解密流程

Fig. 3　Triple KeeLoq encryption diagram

4　KeeLoq 算法在智能门控系统中的应用

系统结构图如图 4 所示。智能门控系统分为手机用户端和门锁控制端。开发了 Android 手机开锁应用软件，将用户的开锁操作经三重 KeeLoq 加密后，由蓝牙无线信号发射出去。门锁控制端通过蓝牙通信模块获取该加密信号，采用三重 KeeLoq 解密后，还原出用户的操作后，触发门锁端执行开门操作。

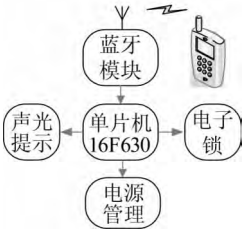

图 4　门锁控制端结构图

Fig. 4　Structure chart of lock control terminal

4.1　手机开锁应用软件设计

手机开锁应用软件基于 Android4.1 版本的操作系统，采用 Eclipse 为开发平台，使用 JAVA 语言设计。所设计应用软件主要流程如图 5 所示，应用软件启动前需要图形解码或者数字解码，进一步保证了门控系统的安全。密码解锁后进入用户操作界面，后台程序首先分别由 BluetoothAdapter. getDefaultAdapter()、BluetoothDevice 获取默认的本地蓝牙设备及远程蓝牙设备，通过蓝牙通信 Socket，使得本地蓝牙设备连接上远程蓝牙设备；然后从 SQL 轻型数据库中读取 3 组 64bits 密钥和 16bits 同步计数值，将用户的开关锁操作按图 4 流程经三重 KeeLoq 加密编码，并通过 OutputStream 输出流由蓝牙接口传输至智能门锁端，同时存储于数据库的同步计数值自加 1 并更新。用户长按开锁键 5s 以上，即发送包含安全学习的编码数据，在双方密钥匹配情况下，门锁将注册登记该手机客户端用户信息。程序支持用户设定三个密钥，利用三组不同的密钥提供多种种类“钥匙”供用户选择，如家庭钥匙、办公室钥匙等。

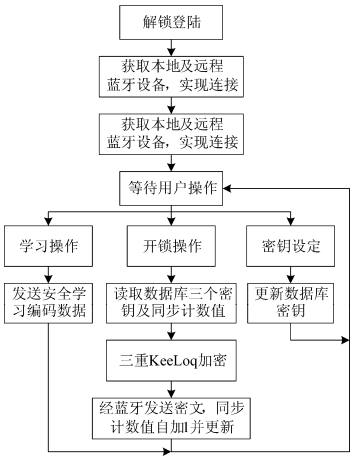

图 5　手机开锁应用程序

Fig. 5　Android applications for unlocking

4.2　门锁控制端

门锁控制端选用 16F630 单片机作为主控制器实现三重 KeeLoq 解密；扩展 BK3211 蓝牙模块，接收密文数据；外围配备门锁驱动电路实现开关门控制；提供声光电路给用户操作提示。系统工作流程如图 6 所示，系统上电后，复位并初始化外设，实时判断学习键是否按下或蓝牙模块是否有数据输入。若学习键长按超过 5s，即可擦除门锁控制端中的 EEPROM 中的已有的用户信息，手机端开锁软件长按学习按键 5s 后，通过蓝牙向门锁控制端发送学习资料，用于同步加解密端的参数。若模块有数据输入，单片机首先校验 EEPROM 存储的用户序列号与固定码中的序列号一致，再进行三重 KeeLoq 解密以获得明文；将解密后明文中的识别码、功能键分别与序列号的低 10bits、固定码的功能键匹配相同后，再判断解密后明文中同步计数值是否合理增加。明文中同步计数值必须大于存储于 EEPROM 中的

上一次接收的同步计数值，且不能大于 4 次，满足条件更新 EEPROM 中的同步计数值，并根据功能键控制门锁执行开门操作，扬声器短鸣 1s，LED 速闪 3 次，提示解锁成功；否则接收失败扬声器长鸣 5s，LED 慢闪 3 次，提示解锁失败。

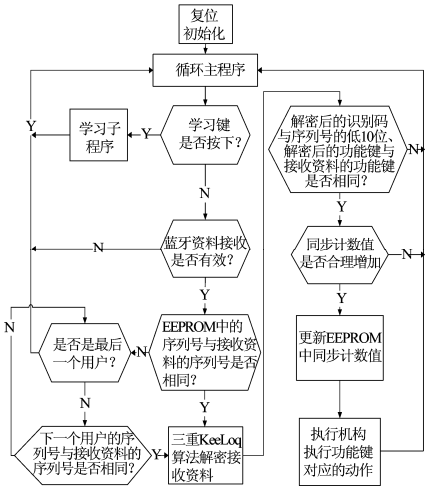

图 6 系统工作流程图

Fig. 6 System operation flowchart

5 结论

本文借鉴了 3DES 思想，提出采用三重 KeeLoq 加解密算法，以提高 KeeLoq 算法的可靠性和安全性。并成功将该算法应用于智能门控系统的开发，既可满足门锁智能化潮流，又保证高安全性能。该解决方案的克服了传统电子式钥匙携带不便且容易遗漏丢失或被盗取的不足，并可将多种钥匙功能集成于一个手机应用软件上，具有低成本、高安全性、人性化及绿色环保等特性。具有很好的推广价值和潜在的市场应用前景。

参考文献

[1] 张健. 无钥匙进入系统的开发与加密算法研究[D]. 哈尔滨: 哈尔滨工业大学航天学院，2013.
Zhang J. Development of passive entry passive start and research on encryption algorithm [D]. Harbin: School of Astronautics, Harbin Institute of Technology, 2013. (in Chinese)

[2] 代宇. 无线汽车门锁密码系统的研究与设计[D]. 哈尔滨: 哈尔滨工业大学深圳研究生院，2013.
Dai Y. Research and design of the encryption system applied on wireless vehicle lock [D]. Harbin: Shenzhen graduate school, Harbin Institute of Technology, 2013. (in Chinese)

[3] 赵春红，杨勇. 基于单片机和无线电遥控技术的密码锁设计[J]. 测控技术，2005，24(9)：9-11.
Zhao C H, Yang Y. Design of Password-Lock Based on Microcontroller and Remote Control Technology [J]. Measurement & Control Technology, 2005, 24(9): 9-11. (in Chinese)

[4] 赵烽. KEELOQ 加密算法安全性探究[J]. 信息网络安全，2011，(8)：29-31.
Zhao F. Security of KEELOQ Encryption Algorithm [J]. Netinfo Security, 2011, (8): 29-31. (in Chinese)

[5] 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.
Li L, Chen H B. Design of remote control parking lock system based on KEELOQ technology [J]. Application of Electronic Technique, 2013, 39(12): 52-54. (in Chinese)

[6] 王文虎，李建奇，陶曾杰. KEELOQ 滚动加密技术在汽车防盗系统中的应用[J]. 电子测量技术，2008，30(10)：197-199.
Wang W H, Li J Q, Tao Z J. Application of KEELOQ hopping encode technology in the automobile security system [J]. Electronic Measurement Science and Technology, 2008, 30(10): 197-199. (in Chinese)

[7] Andrey B. Linear slide attacks on the KeeLoq block cipher [C] // Information Security and Cryptology, Germany: Springer, 2008: 66-80.

[8] Nicolas T C, Gregory V B, David W. Algebraic and slide attacks on KeeLoq [C] // Fast Software Encryption, Germany: Springer, 2008: 97-115.

[9] 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.
You J X, Li R L, Li C. Fault Attack on Lightweight Block Cipher KeeLoq [J]. Acta Scientiarum Naturalium Universitatis Pekinensis, 2010, 46(5): 756-762. (in Chinese)

[10] 张祎江. 基于 3DES-ECC 算法的网络信息加密研究[J]. 科技通报，2014，30(4)：229-231.
Zhang Y J. Study on Network Information Based on 3DES-ECC Encryption Algorithm [J]. Bulletin of Science and Technology, 2014, 30(4): 229-231. (in Chinese)

作者简介

刘 璟 男，1982 年生，福建人，厦门大学物理系博士生，集美大学信息工程学院教师，讲师，主要研究方向为信号与信息处理、智能测试技术及系统等。
E-mail: jingliu@jmu.edu.cn

陈惠滨(通讯作者) 男，1978 年生，福建人，集美大学信息工程学院，副主任，副教授，主要研究方向为信号与信息处理、智能测试技术及系统。
E-mail: chbchb@jmu.edu.cn

叶文才 男，1964 年生，福建人，集美大学信息工程学院，教师，副教授，主要研究方向为信号与信息处理、智能测试技术及系统、工业自动化。
E-mail: yc646800@jmu.edu.cn