doi: 10.3969/j.issn.1671-1122.2011.08.011

KEELOQ 加密算法安全性探究

赵烽

（公安部第三研究所，上海 200031）

摘 要： 文章首先简要介绍了KEELOQ加密算法的基本概念和在实践中的应用，通过分析KEELOQ加密算法的原理及特点，提出了攻击KEELOQ加密算法的具体方法。

关键词： KEELOQ算法；加密；攻击

中图分类号： TP393.08 **文献标识码：** A **文章编号：** 1671-1122（2011）08-0029-03

Security of KEELOQ Encryption Algorithm

ZHAO Feng

(*The Third Research Institute of Ministry of Public Security, Shanghai* 200031, *China*)

Abstract: This paper firstly introduces the concept and the practical application of the KEELOQ encryption algorithm, through the analysis principle and feature of KEELOQ encryption algorithm, it was pointed out that the method of KEELOQ encryption algorithm attacked.

Key words: KEELOQ algorithm; encryption; attack

0 引言

数据加密系统的两个基本要素是加密算法和密钥管理。密钥是控制加密算法和解密算法的关键信息，其产生、传输、存储等工作十分重要。随着信息社会的发展，人们对密码的研究进一步深化，要求也越来越高[1]。目前数据加密技术可以分为两类，即对称型加密、不对称型加密。对称型加密算法使用单个密钥对数据进行加密或解密，不对称型加密算法则使用公用和私有两个密钥来完成数据加密和解密过程。一般来说，密钥长度是以二进制数的位数来衡量，密钥越长，破译密码越困难，加密系统就越可靠。密码破译是随着密码的使用而逐步产生和发展的，常见的破译方法有密钥的穷尽搜索和密码分析，另外针对系统中的漏洞进行攻击也是一种常用且有效的方法。

目前，在点对点无线遥控系统中，数据的编码与发送方式主要有固定编码和滚动编码（也称跳码编码）两种。固定编码方式由于每次发送的数据固定不变或是编码组合次数有限，易被攻击，而滚动编码方式发送的数据一般是用某个不可逆的加密算法产生的，具有抗截获特点，因而滚动编码方式逐渐替代固定编码方式成为主流，其中较为典型的是基于KEELOQ加密算法的滚动编码方式。KEELOQ密码最初是由南非的Willem Smit在上世纪八十年代设计的分组密码算法，1995年由Microchip公司购买并以此推出了系列专用编解码芯片。它是一个32比特分组、64比特密钥的轻型密码。尽管密钥很短，仍广泛用于无密钥输入系统和其他无线认证领域，如遥控无钥门禁、遥控报警系统、身份识别令牌等。

1 KEELOQ加密技术原理

KEELOQ分组密码设计为一个不平衡Feistel（Unbalanced Feistel）结构[2]，其分组长度为32位，加密圈数为528圈，每加密一圈仅改变1位，密钥长度为64位并且在加密过程中循环使用。KEELOQ技术的核心思想就是用64位密钥加密32位明文从而得到32位密文。即使明文中只有1位数据发生变化，用KEELOQ算法得到的密文也会有50%以上的数据位发生变化。

1.1 KEELOQ加密过程

KEELOQ加密算法模型如图1所示，设数据寄存器中存放32位明文，密钥寄存器中存放64位密钥。

收稿时间：2011-07-12

作者简介：赵烽（1972-），男，上海，副研究员，主要研究方向：技术侦察。

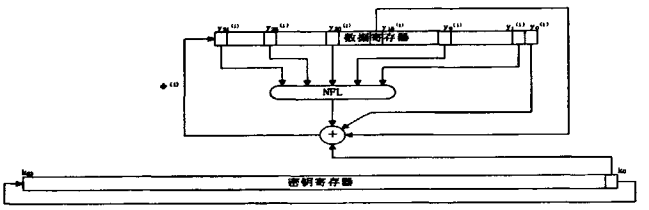

图1 KEELOQ加密模型图

其数学表达式：

$\phi^{(i)}=NLF(y_{31}^{(i)},y_{26}^{(i)},y_{20}^{(i)},y_9^{(i)},y_1^{(i)}) \oplus y_{16}^{(i)} \oplus y_0^{(i)} \oplus k_{i \bmod 64}$

$Y^{(i+1)}=(\phi^{(i)}, y_{31}^{(i)},\cdots, y_1^{(i)})$

i 的范围从 0 到 527

式中 NLF 为非线性逻辑函数

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

加密过程为：首先定义一个非线性表，这个非线性表有 5 位输入，1 位输出。它在数据寄存器中间隔均匀地取固定 5 位，通过非线性运算产生一个输出码，这一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 进行异或运算后输出第一位输出码。每输出一位后，分别进行移位，并重复上述过程共 528 次，最后在数据寄存器中得到 32 位加密数据。

1.2 KEELOQ解密过程

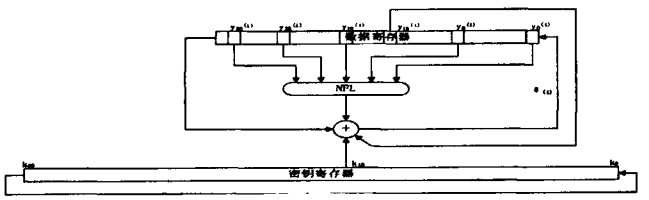

图2 KEELOQ解密模型图

KEELOQ 解密算法模型如图 2 所示。设数据寄存器中存放 32 位密文，密钥寄存器中存放 64 位密钥。

其数学表达式：

$\theta^{(i)}=NLF(y_{30}^{(i)},y_{25}^{(i)},y_{19}^{(i)},y_8^{(i)},y_0^{(i)}) \oplus y_{15}^{(i)} \oplus y_{31}^{(i)} \oplus k_{i-1 \bmod 64}$

$Y^{(i-1)}=(y_{30}^{(i)},\cdots, y_0^{(i)},\theta^{(i)})$

i 的范围从 528 到 1

式中 NLF 为非线性逻辑函数

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

解密过程为：首先定义一个非线性表，这个非线性表有 5 位输入，1 位输出。它在数据寄存器中间隔均匀地取固定 5 位，通过非线性运算产生一个输出码，这一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} 进行异或运算后输出第一位输出码。每输出一位后，分别进行移位，并重复上述过程共 528 次，最后在数据寄存器中得到 32 位解密数据。

1.3 KEELOQ加密算法特点

对上述加密过程进行分析，可以看到明文中的 5 位数据作为非线性逻辑函数的输入，经运算得到的输出又与密钥寄存器中的 1 位和数据寄存器中的 2 位异或。随后进行移位，前一轮得到的密文作为数据寄存器最高位输入，且密钥循环移位。由于每一轮的输出都会作为下一轮的输入，输入的微小变化会迅速扩散。使得即使输入只有一位变化，输出也会有超过一半的位数改变，因而称为雪崩效应。具有雪崩效应的算法可以有效地阻止已知的任何基于统计特性的密码分析以及差分密码分析。因此这样分析者就无法通过对输入进行很小的变化来观察输出的变化，从而分析密码算法。

2 KEELOQ 加密算法的硬件实现

Microchip 公司以 KEELOQ 技术为基础开发了一系列滚动码专用编解码芯片，该编码芯片将数据加密后通过射频技术发出，在接收端既可以使用解码芯片进行硬件解码也可以通过解密算法进行软件解码。其中 HCS201、HCS301 是较典型的两款编码芯片。与典型的固定编码芯片 PT2262 比较，PT2262 发出的编码信号由 8 位地址码（包含 3 种不同状态）、4 位数据码以及同步码组成，地址编码不重复为 38 即 6561 种，可见组合次数极为有限。以 HCS201[3] 为例，该芯片具有 3 个按键输入接口，内部有 192 位的 E2PROM 存储空间，分别用以存储密钥（64 位）、同步计数值（16 位）、序列号（32 位其中 28 位有效）、种子值（32 位）、识别字（16 位）以及配置字（16 位）等信息。当有按键按下时其发出的编码信号由引导码、32 位滚动码以及 34 位固定码组成的共 66 位编码数据，其总计编码组合达到 266 即 7.38×1019 种，可见组合次数已趋于无穷。由于使用 HCS201 的系统每次发送的数据都不相同，因而有效防止了空中截获、扫描和数据重传带来的安全隐患。

2.1 编码字的构成

当有按键按下时，HCS201 会发送一组 66 位的编码字。这一组 66 位的码字由 34 位固定编码部分和 32 位加密编码部分组成，如图 3 所示。其中 32 位的加密数据由 4 个按键位，12 个识别位和 16 个同步计数值位生成，有 2^{32}（超过 40 亿）种不同的编码组合；34 位固定码数据由 2 个状态位、4 个按键位和 28 位序列号组成。固定与加密的部分组合在一起将编码组合的数量提升到了 7.38×10^{19}。

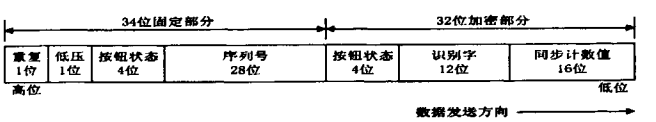

图3 编码字构成图

2.2 密钥生成方式

如上所述，使用前需要向芯片内写入唯一序列号及加密密钥，密钥生成过程如图 4 所示。其中厂商代码由系统制造商编码定义，是整个系统至关重要的部分，而密钥生成算法一般也不公开。

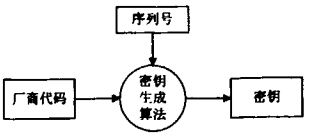

图4 密钥生成图

2.3 数据发送与接收过程

当编码器检测到有按键按下时，就会读取按键输入并更

新同步计数器。如图3所示，同步计数值、按键状态以及识别位（一般使用序列号的低12位数据）共32位作为输入明文，然后用图4方式生成的64位密钥使用KEELOQ加密算法进行加密，从而得到32位加密数据，再与34位明码共同组成66位编码数据发送出去。由于每次按键后，同步计数值都会发生变化，因而即使每次按同一按键，得到的加密数据均不相同。

由于每一个发送方都具有唯一且不重复的序列号，在使用前发送与接收方必须通过学习方式进行配对。之后，当接收方在收到数据后，首先比对序列号，判断是否为合法的发送方发来的数据，然后利用在学习过程中获得并存储的加密密钥对接收的加密部分数据进行解密，接着检查同步计数器是否匹配，在确认其匹配后，再去处理接收到的按键指令，并根据接收到的按键指令作出相应的动作反应。

通过对数据发送与接收过程的分析，可以看到其中有一个重要的步骤即学习。Microchip公司为该系列芯片定义了三种学习模式。第一种是简单学习，发送方使用厂商代码作为加密密钥，接收方也使用同样的密钥来解密接收到的编码数据的加密部分，然而一旦厂商代码泄露数据将无安全性可言；第二种是标准学习，密钥是由厂商代码与序列号通过密钥生成算法产生，该算法不公开，接收方一般不直接存储解密密钥，而是存储厂商代码与密钥生成算法，通过学习得到序列号后再计算出密钥，然后解密接收到的编码数据的加密部分；第三种是安全学习，在该学习模式中引入了种子码概念，即发送方通过同时按下多个按键的特殊按键方式产生种子码，接收方利用种子码经密钥生成算法产生密钥的低32位，再利用学习过程中得到的序列号经密钥生成算法产生密钥的高32位，合成为真正的解密密钥，解密接收到的编码数据的加密部分。

3 KEELOQ加密算法的攻击方法

所谓密码，就是对任何人都能看懂的明文信息，进行某种变换，产生只有掌握了变换规律和变换参数（即密钥）的特定人群才能解读的密文信息。事实上人们很早就开始探索并利用密码对重要信息进行加密，同时密码学的发展又使人们对密钥与密码破译产生了浓厚兴趣。一般来说，密码的破译主要有密钥的穷尽搜索和密码分析两种方法，此外也包括针对系统中的弱点进行攻击，它是一种分析、查找应用中漏洞的方法，而不是攻击加密算法本身。以下对这三种方法分别进行分析。

1）穷尽搜索法。如前所述，KEELOQ算法就是用64位密钥加密32位明文从而得到32位密文，然后再通过同样过程解密并恢复原文。在实际应用中，由于加密数据采用射频方式发送出去，比较容易截获。根据KEELOQ解密过程可知，穷举密钥的次数为2^{64}，显然运算量巨大，虽最终总会有一个密钥经运算得到原文，但需要花费很长时间，其时效性是最大问题。

2）密码分析法。尽管KEELOQ加密算法提出的时间较早，但直到2007年Bogdanov才首次对KEELOQ加密算法进行了分析，使用了滑动及猜测与决定方法完成攻击，攻击的时间复杂度为2^{52}。之后，Courtois等人提出了破译KEELOQ密码的4种滑动－代数攻击方法，而代数攻击法又是近年来信息安全领域研究的热点之一[4]。其中第1种和第2种滑动－代数攻击方法需要2^{16}个已知明密对，第3种和第4种滑动－代数攻击方法需要2^{32}个已知明密对。该攻击方法的主要思想是利用KEELOQ加密算法连续64圈圈函数形成的置换的圈结构与随机置换圈结构的差异，先攻击密钥的前16位，再攻击剩余的48位。第4种攻击的时间复杂度为2^{43}，成功率为1。可见，与穷尽搜索法相比，通过密码分析法可以大大降低攻击的时间复杂度，以及与之相对应的计算空间复杂度，使得密钥破解进入了实用阶段，但还需要建立在一定的已知条件下。另外，由于破解的前提是需要已知一定数量的明密对数据，因而要花费一段时间来获得数据，同时根据计算复杂性在计算上也要花费几天、一周或者更长时间，计算时间的长短完全取决于CPU的处理能力，因而其时效性仍未彻底解决。

3）漏洞攻击法。除了对密钥的穷尽搜索和进行密码分析外，在实际应用中，也可能针对系统的弱点进行攻击，比如通过偷窃欺骗等手段得到密码或密钥，而不是攻击加密算法本身。正如前面所分析的，在具体应用中，密钥是由厂商代码与序列号通过密钥生成算法产生的，而厂商代码和密钥生成算法通常被固化在接收方的硬件系统中，这就存在泄露的可能。如采用固件代码破解加逆向工程的方法，就可以得到厂商代码和分析出密钥生成算法，这也是值得引起注意的问题。与上述的穷尽搜索法、密码分析法相比，漏洞攻击法显然具有快速、成功率高的特点，但不同应用系统往往采用不同的控制与处理器，对固件代码的破解以及之后通过逆向工程生成的汇编语言代码的具体分析则提出了较高要求。总之，密码破解仍是一项艰巨的工程。

4 结束语

本文详细叙述了KEELOQ加密算法的原理，分析了该算法加密与解密的过程。目前，KEELOQ算法主要是通过硬件芯片来实现，该算法属于对称加密算法，采用分组加密，其安全性可以达到数据加密标准（DES）。KEELOQ加密算法虽有很多优点，但还存在一些不足，如安全性基于出厂密钥、密钥短、数据传输效率低等，这在实际应用中需引起注意。●（责编 张岩）

参考文献：

[1] 汤润斌．密码学在汽车防盗系统中的应用初探[J]．中国集体经济，2008：（15）：172-173.

[2] 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，2007，30（10）：197-199.

[3]Microchip公司．HCS201 KEELOQ跳码编码器（DS41098C_CN）[EB/OL]. http://www.microchip.com, 2006/2011-07-12.

[4] 张斌，王秋艳，金晨辉．KeeLoq密码Courtois攻击方法的分析和修正[J]．电子与信息学报，2009，31（4）：946-949.