# KeeLoq 密码 Courtois 攻击方法的分析和修正

张 斌 王秋艳 金晨辉
(信息工程大学电子技术学院 郑州 450004)

**摘 要**：KeeLoq 密码是由 Willem Smit 设计的分组密码算法，广泛应用于汽车的无线门锁装置。Courtois 等人在 2007 年提出了破译 KeeLoq 的 4 种滑动-代数攻击方法，其中第 4 种滑动-代数攻击方法的计算复杂性最小。本文证明了 Courtois 的第 4 种滑动-代数攻击方法的攻击原理是错误的，因而无法实现对 KeeLoq 的破译。此外，本文还对该方法进行了修正，提出了改进的攻击方法，利用 $2^{32}$ 个已知明文能够以 $O(2^{48})$ 次加密的计算复杂性求出 KeeLoq 密码的密钥，成功率为 1。对于 KeeLoq 密码 26%的密钥，其连续 64 圈圈函数形成的复合函数至少具有两个不动点，此时改进的攻击方法的计算复杂性还可降至 $O(2^{43})$ 次加密。

**关键词**：密码分析；KeeLoq 密码；滑动-代数攻击；不动点
**中图分类号**：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2009)04-0946-04

# Analysis and Correction of Courtois Attack to KeeLoq Cipher

Zhang Bin Wang Qiu-yan Jin Chen-hui
(*Electronic Technology Institute*, *Information Engineering University*, *Zhengzhou* 450004, *China*)

**Abstract**: KeeLoq is a block cipher designed by Willem Smit which is used in wireless devices that unlock doors in cars. Four slide-algebraic attacks that can break KeeLoq in practice are presented by Courtois *et al.* in 2007. The computing complexity of the fourth slide-algebraic attack is the smallest. However, the principle of Courtois' fourth slide-algebraic attack is proved to be wrong in this thesis, so it can not break KeeLoq. The correction is made on Courtois' fourth slide-algebraic attack and the improving attack is proposed. With $2^{32}$ known plaintexts, the computing complexity of the improving attack is about $O(2^{48})$ KeeLoq encryptions for obtaining key and the success rate is 1. For 26% of keys in KeeLoq, the first 64 rounds of KeeLoq have 2 or more fixed points, then the computing complexity of the improving attack which uses algebraic attack could decrease to $O(2^{43})$ KeeLoq encryptions.

**Key words**: Cryptanalysis; KeeLoq cipher; Slide-algebraic attack; Fixed point

## 1 引言

KeeLoq 密码是由南非的 Willem Smit 在 20 世纪八十年代设计的分组密码算法，1995 年由一家芯片公司 Microchip Technology Inc 购买并广泛应用于汽车的无线门锁装置[1]。而代数攻击[2−4]是近年来信息安全领域研究的热点之一。Courtois 等人在文献[2]中提出了对 KeeLoq 的 4 种滑动-代数攻击方法。如果计算复杂性折合为 KeeLoq 加密运算的次数，则 Courtois 等人提出的第 1 种滑动-代数攻击的计算复杂性约为 $O(2^{76})$ 次加密，第 2 种滑动-代数攻击的计算复杂性约为 $O(2^{53})$ 次加密，第 3 种滑动-代数攻击的计算复杂性约为 $O(2^{45})$ 次加密，第 4 种滑动-代数攻击的计算复杂性约为 $O(2^{43})$ 次加密。因此，第 4 种滑动-代数攻击的计算复杂性最小，其主要思想是利用 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 16bit，再攻击剩余的 48bit。本文发现该方法在攻击密钥前 16bit 时区分真假密钥的原理是错误的，因而在攻击密钥前 16bit 时不能找到正确值，从而无法实现对 KeeLoq 的破译。本文对第 4 种攻击方法进行了修正，提出了能够区分密钥前 16bit 正确值和错误值的原理和方法，从而利用 $2^{32}$ 个已知明文能够以 $O(2^{48})$ 次加密的计算复杂性求出 KeeLoq 密码的密钥，成功率为 1。在 KeeLoq 密码连续 64 圈圈函数形成的复合函数至少具有两个不动点的条件下，修正的攻击方法能够以 $O(2^{43})$ 次加密的计算复杂性求出正确密钥。对于 KeeLoq 密码 26%的密钥，由于其连续 64 圈圈函数形成的复合函数平均至少具有两个不动点，因而改进的攻击方法能以 $O(2^{43})$次加密的计算复杂性对其 26%的密钥进行破译。

## 2 KeeLoq 分组密码算法介绍

KeeLoq 分组密码设计为一个不平衡 Feistel 结构，其分组长度为 32bit，加密圈数为 528 圈，每加密一圈仅改变 1bit，密钥长度为 64bit 并且在加密过程中循环使用。设密钥为 $k=(k_{63},\cdots,k_0)$，明文分组为 $P=(P_{31},\cdots,P_0)$，对应的密文

2007-12-25 收到，2008-05-30 改回
河南省杰出青年科学基金(0312001800)资助课题

为 $C=(C_{31},\cdots,C_0)$，记 $L_0,L_1,L_2,\cdots,L_{559}$ 均是 1bit 数，则加密过程为：

(1)初始化：$(L_{31},\cdots,L_0)=(P_{31},\cdots,P_0)$。

(2)对于 $i=0,\cdots,527$，依次计算

$$L_{i+32}=k_{i \bmod 64}\oplus L_i\oplus L_{i+16}\oplus \mathrm{NLF}(L_{i+31},L_{i+26},L_{i+20},L_{i+9},L_{i+2})$$

其中 $\mathrm{NLF}(a,b,c,d,e)=d\oplus e\oplus ac\oplus ae\oplus bc\oplus be\oplus cd\oplus de\oplus ade\oplus ace\oplus abd\oplus abc$。

(3)输出密文：$(C_{31},\cdots,C_0)=(L_{559},\cdots,L_{528})$。

## 3　KeeLoq 密码的 Courtois 攻击方法

Courtois 提出的 4 种滑动-代数攻击[2]属于已知明文攻击，其中第 4 种滑动-代数攻击的计算复杂性最小。下面对其攻击原理进行介绍。

第 4 种滑动-代数攻击的思路是：首先构造一个能够将密钥前 16bit 的正确值和错误值区分开的区分器，并据此求出密钥前 16bit 的值。接着在已获得密钥前 16bit 的基础上，攻击密钥的后 48bit，具体的攻击方法有两种。第 1 种方法是直接穷举剩余的 48bit，第 2 种方法是建立一个以圈函数输入、输出以及中间变量为未知变量的代数方程组，再将该方程组转化为 SAT 问题[5]并由 MiniSAT2.0[6]软件解出剩余的 48bit。

为了方便描述，首先引入如下概念：

**定义 1**　设 $f^{(1)}(x)=f(x)$，$f^{(n)}(x)=f(f^{(n-1)}(x))$，则称 $f^{(n)}(x)$ 是 $f(x)$ 的 $n$ 次复合函数。

在 KeeLoq 中，64bit 密钥是循环使用的。因此，若将前 16 圈加密函数记为 $g_k(x)$，前 64 圈加密函数记为 $f_k(x)$，则加密算法可以表为 $E_k(x)=g_k(f_k^{(8)}(x))$。

Courtois 设计的区分器的目的是将 $f_k^{(8)}(x)$ 与随机置换区分开，进而以此为基础，将密钥前 16bit 的正确值与错误值区分开。Courtois 提出的区分 $f_k^{(8)}(x)$ 与随机置换的原理如下：

**引理 1**[7,8]　令 $\sigma:\{0,1\}^{32}\to\{0,1\}^{32}$ 是 $Z/(2^{32})$ 上的置换，则置换 $\sigma$ 可表示成一些不相交的轮换的乘积，且在不考虑轮换次序的情况下表示法是唯一的。如果 $\sigma$ 是随机置换，则轮换个数的期望值近似为 23。

**定义 2**　设 $\lambda=(\alpha_1\alpha_2\cdots\alpha_m)$ 是 $\alpha_1,\alpha_2,\cdots,\alpha_m$ 的一个轮换，即对于 $1\le i\le m$，有 $\lambda(\alpha_i)=\alpha_{(i+1) \bmod m}$，则称 $m$ 是轮换 $\lambda$ 的长度。特别地，当 $m$ 是偶数时，称 $\lambda$ 是偶长度轮换；当 $m$ 是奇数时，称 $\lambda$ 是奇长度轮换。

文献[2]指出，当将 $f_k(x)$ 视为 $Z/(2^{32})$ 上的一个随机置换时，如果将 $f_k(x)$ 表示为不相交轮换乘积，则轮换的个数约为 23，且其中平均有 $23/2=11.5$ 个是偶长度轮换。由于 $f_k^{(2)}(x)=f_k(f_k(x))$，因而 $f_k(x)$ 的奇长度轮换仍为 $f_k^{(2)}(x)$ 的奇长度轮换，但是 $f_k(x)$ 的偶长度轮换都分裂成 $f_k^{(2)}(x)$ 的两个轮换的乘积，而置换 $f_k^{(2)}(x)$ 的偶长度轮换的个数将会减半，近似为 $11.5/2=5.75$ 个。依次类推，置换 $f_k^{(4)}(x)$ 平均有 $5.75/2=2.875$ 个偶长度轮换，置换 $f_k^{(8)}(x)$ 平均有 $2.875/2=1.4375$ 个偶长度轮换。因此，Courtois 指出，由于置换 $f_k^{(8)}(x)$ 平均有 1.4375 个偶长度轮换，而随机置换中平均有 11.5 个偶长度轮换，根据偶长度轮换的个数就可将 $f_k^{(8)}(x)$ 与随机置换区分开。

但是，下面将证明置换 $f_k^{(2)}(x)$ 中偶长度轮换的个数不会减半，并且置换 $f_k^{(2)}(x),f_k^{(4)}(x),f_k^{(8)}(x)$ 中偶长度轮换个数的数学期望都与随机置换的偶长度轮换的平均个数相同。这就是说，Courtois 提出的借助 $f_k^{(8)}(x)$ 的偶长度轮换的个数区分 $f_k^{(8)}(x)$ 与随机置换的原理是错误的，因而无法实现对 KeeLoq 密码的破译。

## 4　Courtois 攻击方法的分析和修正

首先证明 Courtois 的第 4 种滑动-代数攻击区分 $f_k^{(8)}(x)$ 与随机置换的原理是不正确的。

**定理 1**　记 $\lambda=(\alpha_1\alpha_2\cdots\alpha_m)$ 是一个轮换，令 $\lambda^2=\lambda(\lambda\cdot(\alpha_1\alpha_2\cdots\alpha_m))$，则当 $m=2k$ 是偶数时，$\lambda^2=(\alpha_1\alpha_3\cdots\alpha_{2k-1})\cdot(\alpha_2\alpha_4\cdots\alpha_{2k})$，当 $m=2k+1$ 是奇数时，$\lambda^2=(\alpha_1\alpha_3\cdots\alpha_{2k+1}\alpha_2\alpha_4\cdots\alpha_{2k})$。

定理 1 由代数知识容易证得，这里不再赘述。定理 1 说明，偶长度轮换经过 2 次作用后可表示为两个长度减半的轮换的乘积，奇长度轮换经过 2 次作用后仍是奇长度轮换。

**推论 1**　设 $\lambda=(\alpha_1\alpha_2\cdots\alpha_m)$ 是一个长度为 $2^ts$ 的轮换，$s$ 为奇数，则当 $i<t$ 时，$\lambda^{2^i}$ 只有 $2^i$ 个长度为 $2^{t-i}s$ 的偶长度轮换而没有其它长度的轮换，当 $i\ge t$ 时，$\lambda^{2^i}$ 只有 $2^t$ 个长度为 $s$ 的奇长度轮换而没有其它长度的轮换。

**证明**　利用数学归纳法证明。定理 1 说明推论 1 在 $i=1$ 时成立。

假设当 $i=n$ 时结论成立，故当 $1\le n\le t-1$ 时，$\lambda^{2^n}$ 只有 $2^n$ 个长度为 $2^{t-n}s$ 的轮换而没有其它长度的轮换。由于 $2^{t-n}$ 是偶数，故当 $i=n+1$ 时，由 $\lambda^{2^{n+1}}=(\lambda^{2^n})^2$ 和定理 1 知，$\lambda^{2^n}$ 的每个轮换均分裂成两个长度为 $2^{t-n-1}s$ 的轮换的乘积，因而 $\lambda^{2^{n+1}}$ 只有 $2\times 2^n=2^{n+1}$ 个长度为 $2^{t-n-1}s$ 的轮换而没有其它长度的轮换。这说明当 $i=n+1$ 且 $1\le n\le t-1$ 时推论 1 成立。

当 $n\ge t$ 时，由于 $2^{t-t}$ 是奇数，故本推论在 $i=n$ 时成立说明 $\lambda^{2^n}$ 只有 $2^t$ 个长度为 $s$ 的奇长度轮换而没有其它长度的轮换，从而由定理 1 知，$\lambda^{2^{n+1}}=(\lambda^{2^n})^2$ 只有 $2^t$ 个长度为 $s$ 的轮换而没有其它长度的轮换。这说明当 $i=n+1$ 且 $n\ge t$ 时推论 1 成立，故由归纳法知推论 1 总成立。　　证毕

**定理 2**　置换 $\sigma$ 的偶长度轮换的最大长度至少是置换 $\sigma^8$ 的偶长度轮换的最大长度的 8 倍。设 $\sigma$ 是随机置换，则有

(1)置换 $\sigma$ 与置换 $\sigma^2$，$\sigma^4$，$\sigma^8$ 的偶长度轮换个数的期望都相等；

(2)如果 $\sigma$ 的轮换个数的期望是 $r$，则 $\sigma^8$ 的轮换个数的期望是 $2.5r$；

(3)置换 $\sigma$ 的偶长度轮换的平均长度是置换 $\sigma^8$ 的偶长度轮换的平均长度的 8 倍。

**证明** 由推论 1 知，设 $\sigma^8$ 的偶长度轮换的最大长度为 $d$，则该偶长度轮换是由置换 $\sigma$ 的某个长度是 $8d$ 的偶长度轮换分裂得到，而置换 $\sigma$ 的该偶长度轮换的长度 $8d$ 不大于置换 $\sigma$ 的所有偶长度轮换的最大长度，故置换 $\sigma$ 的偶长度轮换的最大长度至少是置换 $\sigma^8$ 的偶长度轮换的最大长度的 8 倍。

设 $\sigma$ 的不相交轮换乘积表示为 $\sigma=\lambda_1\lambda_2\cdots\lambda_r$，记 $l(\lambda_i)=2^{t_i}s_i$ 为轮换 $\lambda_i$ 的长度，其中 $t_i$ 是非负整数，$s_i$ 是奇数，则置换 $\sigma$ 的偶长度轮换个数为 $\#\{i:l(\lambda_i)=2^{t_i}s_i,t_i>0\}$，奇长度轮换个数为 $\#\{i:l(\lambda_i)=2^{t_i}s_i,t_i=0\}$。令 $\#A$ 表示集合 $A$ 中元素的个数，则由 $\sigma^{2^k}=\lambda_1^{2^k}\lambda_2^{2^k}\cdots\lambda_r^{2^k}$ 和推论 1 知，置换 $\sigma^{2^k}$ 的偶长度轮换个数为 $2^k\times\#\{i:l(\lambda_i)=2^{t_i}s_i,t_i>k\}$，奇长度轮换个数为 $\sum_{j=0}^{k}[2^j\times\#\{i:l(\lambda_i)=2^js_i\}]$。

由于 $\sigma$ 是随机置换，故对于 $\sigma$ 的一个轮换 $\lambda$，有 $p\{l(\lambda)$是奇数的$2^t$倍$\}=2^{-(t+1)}$，因而有

$$p(i:l(\lambda_i)=2^{t_i}s_i,t_i>k)=\sum_{t_i=k+1}^{\infty}2^{-(t_i+1)}=2^{-k-1}$$

因而 $\#\{i:l(\lambda_i)=2^{t_i}s_i,t_i>k\}$ 的数学期望为 $r\times p(i:l(\lambda_i)=2^{t_i}s_i,t_i>k)=2^{-k-1}r$，从而置换 $\sigma^{2^k}$ 的偶长度轮换个数的数学期望为

$$2^k\times E(\#\{i:l(\lambda_i)=2^{t_i}s_i,t_i>k\})=r/2$$

置换 $\sigma^{2^k}$ 的奇长度轮换个数的数学期望为

$$\sum_{j=0}^{k}[2^j\times E(\#\{i:l(\lambda_i)=2^js_i\}])=\sum_{j=0}^{k}2^j\times2^{-j-1}r=\frac{1}{2}(k+1)r$$

从而置换 $\sigma^{2^k}$ 的轮换个数的数学期望为 $(1/2)(k+2)r$。特别地，$\sigma^8$ 的轮换个数的期望为 $2.5r$。这说明(1)和(2)成立。由于 $\sigma$ 是随机置换，故 $\sigma$ 的偶长度轮换与奇长度轮换的平均长度均为 $\left\lfloor\sum_{i=1}^{r}l(\lambda_i)\right\rfloor/r$。由推论 1 知，$\sigma^8$ 的每个偶长度轮换都是由置换 $\sigma$ 的某个长度是 16 的倍数的偶长度轮换分裂得到，故 $\sigma^8$ 的偶长度轮换的平均长度为 $\sum_{t_i>3}l(\lambda_i)/(r/2)$，而

$$\sum_{t_i>3}l(\lambda_i)=\left\{\left\lfloor\sum_{i=1}^{r}l(\lambda_i)\right\rfloor/r\right\}\times r\times p(i:l(\lambda_i)=2^{t_i}s_i,t_i>3)=2^{-4}\cdot\sum_{i=1}^{r}l(\lambda_i)$$

，故 $\sigma^8$ 的平均长度为 $2^{-3}\left\lfloor\sum_{i=1}^{r}l(\lambda_i)\right\rfloor/r$，这说明(3)成立。 证毕

定理 2 的(1)说明，当将置换 $f_k(x)$ 视为随机置换时，不能利用 $f_k^{(8)}(x)$ 的偶长度轮换个数将 $f_k^{(8)}(x)$ 与随机置换区分开，因而 Courtois 提出的 KeeLoq 的第 4 种滑动-代数攻击的攻击原理是不正确的；定理 2 的(2)说明，当将置换 $f_k(x)$ 视为随机置换时，可以借助于 $f_k^{(8)}(x)$ 的轮换个数与随机置换的轮换个数的差异，将 $f_k^{(8)}(x)$ 与随机置换区分开，此时随机置换平均有 23 个轮换，而 $f_k^{(8)}(x)$ 平均有 $2.5\times23=57.5$ 个轮换；定理 2 及(3)还说明，还可利用 $f_k^{(8)}(x)$ 的偶轮换的最大长度或平均长度，将 $f_k^{(8)}(x)$ 与随机置换区分开。此时，随机置换的偶长度轮换的平均长度是 $2^{32}/23\approx2^{27.5}$，而置换 $f_k^{(8)}(x)$ 的偶长度轮换的平均长度是 $2^{29}/23\approx2^{24.5}$。

下面给出在已知 $2^{32}$ 个明密对的条件下，对 Courtois 攻击方法的修正算法。

**算法 1**

步骤 1 攻击密钥的前 16bit。穷举密钥前 16bit 的可能值 $k'$，对于 $2^{32}$ 个明密对 $(P,C)$，计算出 $g_{k'}^{-1}(C)$ 从而得到 $Z/(2^{32})$ 上的一个置换 $P\to g_{k'}^{-1}(C)$。如果该置换的圈结构与随机置换 8 次幂的圈结构的内在规律吻合，则判断 $k'$ 为正确值，否则判定 $k'$ 为错误值。具体方法有以下 3 种：

第 1 种方法是统计该置换中轮换的个数 $t(k')$。当 $t(k')<46$ 时，判定 $k'$ 为错误值并返回步骤 1 穷举密钥前 16bit 的下一个可能值，否则判定 $k'$ 为正确值并执行步骤 2。第 2 种方法是计算该置换的偶长度轮换的平均长度 $l(k')$。当 $l(k')\geq2^{25}$ 时，判定 $k'$ 为错误值并返回步骤 1 穷举密钥前 16bit 的下一个可能值，否则判定 $k'$ 为正确值并执行步骤 2。第 3 种方法是计算该置换的偶长度轮换的最大长度 $l(k')$。当 $l(k')$ 显著小于随机置换的偶长度轮换的最大长度的期望值时，判定 $k'$ 为正确值并执行步骤 2，否则判定 $k'$ 为错误值并返回步骤 1 穷举密钥前 16bit 的下一个可能值。

步骤 2 攻击密钥的后 48bit。将步骤 1 得到密钥的前 16bit 的值代入 $f_k^{(8)}(P)$，并穷举剩余的 48bit 密钥，然后利用所有的已知明密对根据对应关系 $f_k^{(8)}(P)=g_{k'}^{-1}(C)$ 对之进行检验，从而求出正确密钥。

**定理 3** 算法 1 的计算复杂性为 $O(2^{48})$ 次 KeeLoq 加密，成功率为 1。

**证明** 步骤 1 需穷举密钥前 16bit 的所有可能值并对每个可能值均对 $2^{32}$ 个明密对计算出 $g_{k'}^{-1}(C)$。由于计算 $g_{k'}^{-1}(C)$ 仅需 16 次圈函数计算，因此步骤 1 的计算复杂性为 $(2^{16}\times2^{32}\times16)/528\approx O(2^{43})$ 次 KeeLoq 加密。步骤 2 穷举密钥后 48bit 时，仅需对每个可能值进行 512 次圈函数计算，故步骤 2 的计算复杂性为 $(2^{48}\times512)/528\approx O(2^{48})$ 次 KeeLoq 加密，因而修正算法的计算复杂性为 $O(2^{48})$ 次 KeeLoq 加密。由于算法 1 只有通过穷举检测后才输出正确密钥，因而最终必能找出正确密钥，故其成功率为 1。 证毕

定理 3 说明，算法 1 可将破译 KeeLoq 密码的计算复杂性由 $O(2^{64})$ 次加密操作降至 $O(2^{48})$ 次加密操作。

下面指出，如果利用文献[2]提出的基于 $f_k(x)$ 的不动点的代数攻击方法替换步骤 2，则算法 1 的计算复杂性对于 26% 的密钥都可进一步降低为 $O(2^{43})$ 次加密。下面具体介绍这个方法。

**定义 3** 如果函数 $y=f(x)$ 的定义域中存在点 $x_0$，使得 $x_0=f(x_0)$，则称 $x_0$ 是函数 $f$ 的不动点。

在 KeeLoq 中，如果 $P$ 是函数 $f_k(x)$ 的不动点，则有

$f_k^{(8)}(P)=f_k(P)$，因而有 $C=E_k(P)=g_k(f_k(P))$。此时就可按照文献[2]的方法，在 $g_k$ 的 16bit 密钥已知的条件下，利用 $f_k(P)=g_k^{-1}(C)$ 和使明文构成 $f_k(x)$ 的不动点的两个已知明密对 $(P,C)$，建立一个求解剩余 48bit 密钥的代数方程组。文献[2]指出，由于 $f_k(x)$ 只是 64 圈迭代，因而利用 MiniSAT2.0 软件求解该代数方程组的计算复杂性相当于 $2^{17}$ 次 KeeLoq 加密。

由于 $g_k$ 的 16bit 密钥已知，因而可以找出 $f_k^{(8)}(x)$ 的全部不动点，其个数平均为 4 个[8]。由于 $f_k(x)$ 的不动点一定是 $f_k^{(8)}(x)$ 的不动点，因而通过从 $f_k^{(8)}(x)$ 的不动点集合中取出两个，在它们都是 $f_k(x)$ 的不动点的假设下，求出对应的代数方程组。如果能求出正确密钥，则说明假设正确；如果求不出正确密钥，则说明假设错误，此时只需再测试其它假设即可。由于平均共有 $C_4^2=6$ 种取法，故步骤 2 求出剩余 48bit 密钥计算复杂性相当于 $6\times 2^{17}=1.5\times 2^{19}$ 次 KeeLoq 加密，因而新的改进算法的计算复杂性平均为 $O(2^{43})$ 次 KeeLoq 加密。

在将 $f_k(x)$ 视为随机置换的假设下，文献[2]证明了函数 $f_k(x)$ 至少存在 2 个不动点的概率约为 0.26。因此，对于 26% 的密钥 $k$，函数 $f_k(x)$ 都至少存在 2 个不动点。这说明改进后的算法 2 平均对 26%的密钥有效。即：

**定理 4**　当算法 1 的步骤 2 采用基于 $f_k(x)$ 的不动点的代数攻击方法时，对 26%的密钥可成功破译，其计算复杂性为 $O(2^{43})$ 次 KeeLoq 加密。

说明：　在算法 1 的步骤 2 中，也可直接利用 $f_k^{(8)}(P)=g_k^{-1}(C)$ 建立代数方程组，求解剩余的 48bit 密钥。但是，由于 $f_k^{(8)}(x)$ 相当于 512 圈的 KeeLoq 加密算法，而文献[2]已经指出，利用 MiniSAT2.0 求解 128 圈 KeeLoq 加密算法的密钥仅比穷举攻击稍快，但超过 128 圈则不能利用 MiniSAT2.0 求解。因此上述攻击算法在步骤 2 中不得不利用 64 圈 KeeLoq 加密形成的函数 $f_k(x)$ 的不动点建立方程组，从而将代数攻击降至有效的范围。

## 5　结束语

本文对 Courtois 提出的破译 KeeLoq 的第 4 种滑动-代数攻击进行了分析，发现该攻击方法对密钥前 16bit 攻击的原理是错误的，从而无法实现对 KeeLoq 的破译。同时，本文提出了能够求出密钥的前 16bit 的方法，并对 Courtois 的方法进行了修正，从而使得对 KeeLoq 的破译能够实现。

## 参 考 文 献


[1] Keeloq wikipedia article. http://en.wikipedia.org/wiki/KeeLoq, 2007, 25 January.

[2] Courtois N T and Bard G V. Algebraic and slide attacks on KeeLoq. http://eprint.iacr.org/2007/062.

[3] Brad G V, Courtois N T, and Jefferson C. Efficient methods for conversion and solution of sparse systems of low-degree multivariate polynomials over GF(2) via SAT-solvers. http://eprint.iacr.org/2007/024.

[4] Courtois N T and Bard G V. Algebraic cryptanalysis of data encryption standard. http://eprint.iacr.org/2006/402.

[5] Moskewicz M W, Madigan C F, and Zhao Y, *et al*.. Chaff: Engineering an efficient SAT solver. Proceedings of the 38th ACM/IEEE Design Automation Conference, Las Vegas, June 2001: 530–535.

[6] Een N and Sorensson N. MiniSAT 2.0. http://www.cs.chalmers. se/Cs/Research/FormalMethods/ MiniSat/.

[7] 聂灵沼, 丁石孙. 代数学引论. 第二版, 北京: 高等教育出版社, 2000: 27–30.
Nie Ling-zhao and Ding Shi-sun. An Introduction to Algebra. Second Edition, Beijing: Higher Education Press, 2000: 27–30.

[8] Riedel M R. The statistics of random permutations. http://www.geocities.com/markoriedelde/papers/randperms.pdf, 2006, June 8.



张　斌：　男，1982 年生，博士生，研究方向为密码学.

王秋艳：　女，1985 年生，硕士生，研究方向为密码学.

金晨辉：　男，1965 年生，教授，博士生导师，主要研究方向为密码学和信息安全.