对基于 NLFSR 分组密码 KTANTAN32 的相关密钥中间相遇代数攻击

张文英[1,3,4],刘祥忠[2]

(1.山东师范大学信息科学与工程学院,山东济南 250014;
2.山东师范大学第二附属中学,山东济南 250014;
3.山东省分布式计算机软件新技术重点实验室,山东济南 250014;
4.中国科学院信息工程研究所信息安全国家重点实验室,北京 100093)

摘 要: 本文分析了 KTANTAN32 的代数学弱点.使用相关密钥中间相遇攻击,用代数推导的方法得到了在 240 轮之后所使用某些密钥的一元线性方程,解这些方程便可迅速逐比特恢复相应密钥.因只须一对相关密钥和 2 个明密文,即可恢复部分密钥比特,攻击的时间复杂度和空间复杂度都可以忽略不计.分析表明 KTANTAN32 是一个很弱的算法.同时也说明使用 NLFSR 和线性密钥编排是 KTANTAN32 的致命弱点,为抵抗相关密钥中间相遇攻击,设计者应在密钥编排中加入非线性因素.

关键词: 分组密码; KTANTAN32; 相关密钥攻击; 中间相遇攻击; 非线性反馈移位寄存器
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2012) 10-2097-04
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.10.032

An Related-Key Meet-in-the-Middle Algebraic Attack on the NLFSR Based Block Cipher KTANTAN32

ZHANG Wen-ying[1,3,4], LIU Xiang-zhong[2]

(1. *School of Information Science and Engineering, Shandong Normal University, Jinan, Shandong* 250014, *China*;
2. *No.2 Middle School Attached to Shandong Normal University, Jinan, Shandong* 250014, *China*;
3. *Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology Jinan, Shandong* 250014, *China*;
4. *State Key Lab of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*)

Abstract: In this paper, we analyze the algebraic weakness of KTANTAN32. Using related-key and meet-in-the-middle match attack, by algebraic deducing, we get some single-variable linear equations on some key bits and can recover these key bits instantly by solving these algebraic equations one by one. We can recover the key bits with only one pairs of related-keys, 2 plaintext/ciphertext pairs. The time complexity and the memory complexity are all negligible. Which indicates that the KTANTAN32 is a very weaker cryptographic system. We conclude that using the NFSR update mode and the linearity of the key schedule together is the fatal weakness of KTANTANs. In order to prevent the cipher from meet in the middle and match attack, it is important to introduce some nonlinearity in the key schedule of this block cipher.

Key words: block cipher; KTANTAN32; related-key attack; meet-in-the-middle attack; Non-linear feedback shift register (NLFSR)

1 引言

随着物联网、卫星通信网和移动通信网等的发展,近年来对射频识别技术(Radio Frequency Identification RFID)需求日益旺盛,为射频识别而设计的加密算法层出不穷.因射频卡和传感器网络的工作环境是计算能力相对较薄弱的嵌入式处理器,而传统加密算法能耗太大,不能满足其加密要求,一些面向资源受限环境的轻量级分组密码算法应运而生[1~3].

KTANTAN[2]系列分组密码是由 Christophe De Canniere, Orr Dunkelman and Miroslav Knezevic 在 2009 年密码硬件和嵌入式系统国际会议(CHES)上提出的,为减少

收稿日期:2011-12-31;修回日期:2012-06-05
基金项目:国家自然科学基金(No.61173134,No.61272434);山东省自然基金(No.ZR2012FM004);山东省青年骨干教师国内访问学者项目(No.2011A115)

硬件实现的门数,它采用了基于非线性反馈移位寄存器(NLFSR)的轮函数结构和线性密钥编排.设计者声称无比穷尽搜索更快的分析算法.然而文献[4]却给出了复杂度为 $2^{75.17}$的分析;文献[5]把文献[4]中速度提高一倍;文献[6]首次指出了 KTANTAN32 中第 32 比特密钥首次被使用的时间太晚的缺点,并给出恢复部分密钥的方法.

正是因为 KTANTAN 系列分组密码是在硬件资源受限条件下提出的密码体制,使得大规模猜测密钥借助计算机搜索的方法缺乏现实性,本文用相关密钥中间相遇攻击方法,抓住 k_{32}在 230 轮才被首次使用的弱点,脱离了计算机,仅用代数分析的方法就推导得到了 KTANTAN 32 某些密钥比特的一元线性方程,通过解方程便恢复一些密钥比特,只须一对相关密钥和 2 个明密文对即可恢复部分密钥比特.在文献[6]中,作者提出一种"无法解释"的奇怪现象:即使穷尽搜索 218 轮之后所用的 44 比特密钥,却也只能确定其中的 28 比特.本文从代数角度揭示了该现象发生的原因.本文的分析结果表明,同时使用 NLFSR 和线性密钥编排的分组密码体制存在很大的安全隐患,强烈建议设计者在密钥编排中加入非线性因素.

2 KTANTAN32 算法描述

2.1 轮函数和密文

作为一种新型的轻量分组密码,KTANTAN-32[2]具有 80 比特密钥,明文分组为 32 比特,加密轮数为 254.它像流密码那样使用了两个非线性反馈移位寄存器作为互控的轮函数,明文作为非线性移位寄存器的初态,每轮使用两比特密钥,末轮的状态便是密文.状态更新方式如图 1 所示.

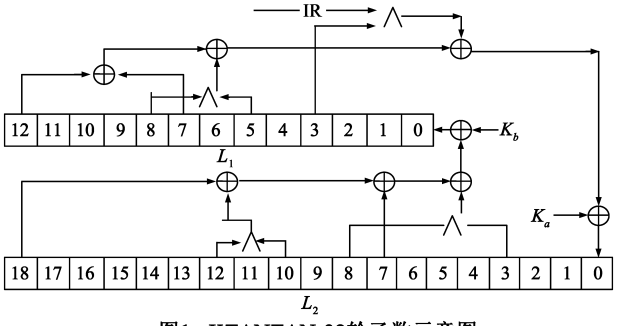

图1 KTANTAN-32轮函数示意图

状态更新函数为

$$f_{1,r} = u_{12} \oplus u_7 \oplus u_8 u_5 \oplus u_3 \ IR(r) \oplus K_a$$

$$f_{2,r} = v_{18} \oplus v_7 \oplus v_{12} v_{10} \oplus v_8 v_3 \oplus K_b$$

$$(u_{12}, u_{11}, \cdots, u_1) \leftarrow (u_{11}, u_{10}, \cdots, u_0), u_0 = f_{2,r},$$

$$(v_{18}, v_{17}, \cdots, v_1) \leftarrow (v_{17}, v_{16}, \cdots, v_0), v_0 = f_{1,r}.$$

这里 $IR(r)$是轮常数,K_a, K_b 是 2 比特密钥.算法的详细描述请见文献[2].

2.2 密钥编排

KTANTAN32 使用 80 比特原始密钥,每轮使用原始密钥中两个比特.因本文只讨论后 36 轮和篇幅所限,只列出 219 – 254 轮各轮所使用的密钥,依次为 $k_{32}k_{64}$ $k_{64}k_0$ $k_{49}k_{65}$ $k_{18}k_{50}$ $k_{37}k_{37}$ $k_{11}k_{27}$ $k_{22}k_{70}$ $k_{28}k_{60}$ k_9k_{57} k_2k_{50} k_4k_{52} k_8k_{40}(230 轮) k_0k_0 $k_{48}k_{64}$ $k_{32}k_{32}$ $k_{65}k_1$ $k_{67}k_{67}$ $k_{54}k_{22}$ $k_{29}k_{61}$ $k_{27}k_{59}$ k_7k_{55} $k_{14}k_{62}$ $k_{12}k_{60}$ k_8k_{56} k_0k_{32} k_0k_{16} $k_{16}k_{64}$ $k_{32}k_{32}$ k_1k_{17} $k_{34}k_{66}$ $k_{68}k_4$ $k_{73}k_{73}$ $k_{66}k_2$ $k_{69}k_5$ $k_{75}k_{11}k_{71}k_7$.这里第 $i(1 \leqslant i \leqslant 36)$组表示第 $218+i$ 轮所使用的两比特密钥.在这 36 轮,由于同一密钥被多次使用,不考虑重数,仅使用 44 比特原始密钥.

3 KTANTAN32 的代数弱点和相关密钥中间相遇攻击

相关密钥攻击首次由 Knudsen 提出[7],其原理是攻击者用有一定关系的两个密钥分别对同一明文加密,根据密文差分得到关于密钥的一些信息.

3.1 KTANTAN32 密钥编排的弱点和相关密钥中间相遇攻击

从 KTANTAN32 的密钥表中可以看出 k_{32}在第 219 轮才首次被使用,换言之,它仅在算法的后 36 轮被使用.由其移位寄存器结构特点知道,从 219 轮到 230 轮,扣除移位因素,状态向量至少有 8 比特没变.以 $\boldsymbol{e}_i$ 记只有第 i 位是 1 其余位都是 0 的 80 比特向量.Key 表 80 比特原始密钥.当用 $\boldsymbol{Key}$ 和 $\boldsymbol{Key} + \boldsymbol{e}_{32}$分别对同一明文加密时,在 230 轮末,它们的中间状态至少有 8 比特完全相同.这 8 比特相等与否成了我们判断猜测密钥是否正确的依据.图 2 生动的展示了这一现象的成因.这里"+"表示两向量逐比特模 2 加,W, N 表用两相关密钥 $\boldsymbol{Key}$ 和 $\boldsymbol{Key} + \boldsymbol{e}_{32}$对同一明文加密所得两密文.

文献[6]使用了以下攻击方法:用计算机穷尽搜索 219 轮之后所使用 44 比特密钥,使用两相关密钥分别解密相应的密文 W, N 到 218 轮,根据 218 状态是否相等来判断猜测密钥是否正确,恢复了 219 轮之后所使用的 44 比特密钥密钥中的 28 比特.以下我们从用两相关密钥加密所得中间状态的差分出发,脱离计算机搜索,仅用代数推导的方法解方程便恢复了部分密钥比特.

3.2 用两相关密钥对同一明文加密所得中间状态在 230 轮和 243 轮的差分

以 $u_{12}, \cdots, u_0, \cdots, v_{18}, \cdots, v_0$,记 218 轮末即 219 轮初的状态,当 $i \leqslant 0$ 时,以 u_{i-1}, v_{i-1}记 u_i, v_i 的下一个状态,则第 230 轮的状态是:

$$\boldsymbol{U}_{230}=(u_0, v_{18}\oplus v_7\oplus v_{12}v_{10}\oplus v_8v_3\oplus k_{64}, v_{17}\oplus v_6\oplus v_{11}v_9\oplus v_7v_2\oplus k_0, v_{16}\oplus v_5\oplus v_{10}v_8\oplus v_6v_1\oplus k_{65}, v_{15}\oplus v_4\oplus v_9v_7\oplus v_5v_0\oplus k_{50}, v_{14}\oplus v_3\oplus v_8v_6\oplus v_4v_{-1}\oplus k_{37}, \cdots)$$

$$\boldsymbol{V}_{230}=(v_6, \cdots, v_0, u_{12}\oplus u_7\oplus u_5u_8\oplus u_3\ IRr\oplus k_{32}, u_{11}\oplus u_6\oplus u_4u_7\oplus u_2\ IRr\oplus k_{64}, u_{10}\oplus u_5\oplus u_3u_6\oplus u_1\ IRr\oplus k_{49}, u_9\oplus u_4\oplus u_2u_5\oplus u_0\ IRr\oplus k_{18}, u_8\oplus u_3\oplus u_1u_4\oplus u_{-1}\ IRr\oplus k_{37}, u_7\oplus u_2\oplus u_0u_3\oplus u_{-2}\ IRr\oplus k_{11}, u_6\oplus u_1\oplus u_{-1}u_2\oplus u_{-3}\ IRr\oplus k_{22}, u_5\oplus u_0\oplus u_{-2}u_1\oplus u_{-4}\ IRr\oplus k_{28}, u_4\oplus u_{-1}\oplus u_{-3}u_0\oplus u_{-5}\ IRr\oplus k_9, u_3\oplus u_{-2}\oplus u_{-4}u_{-1}\oplus u_{-6}\ IRr\oplus k_2, \cdots)$$

如果 k_{32}有差分,则 $v_{-1}=u_{12}\oplus u_7\oplus u_5\ u_8\oplus u_3\ IRr\oplus k_{32}$处必然有差分,在 $u_{-1}, \cdots, u_{-4}, v_{-2}, \cdots, v_{-8}, v_{-10}$处无差分.若以 $D_r(\boldsymbol{W})$、$D_r(\boldsymbol{N})$记对 $\boldsymbol{W}, \boldsymbol{N}$ 解密 r 轮所得中间状态,则由上述讨论得:

$$D_{24}(\boldsymbol{W})+D_{24}(\boldsymbol{N})=00000********\ 000000010000000*0**\quad(1)$$

这里"*"表示一未知比特.由式(1)知,同一明文在一对相关密钥加密 230 轮的中间状态,有 20 比特一定相等,1 比特完全相反共 21 比特条件.这比从图 2 中直观看到的 8 比特相等的条件多出了 13 比特条件.由式(1)知,在 243 轮的两中间状态有如下关系式

$$D_{11}(\boldsymbol{W})+D_{11}(\boldsymbol{N})=**********00*0\ **********\quad(2)$$

3.3　恢复最后 15 轮所使用密钥的代数方法

本节介绍恢复最后 15 轮所使用密钥比特的代数方法.假设 $\boldsymbol{W}=(u_{12}, \cdots, u_0, v_{18}, \cdots, v_0)$, $\boldsymbol{N}=(u'_{12}, \cdots, u'_0, v'_{18}, \cdots, v'_0)$是同一明文 P 在两相关密钥 Key 和 Key + e_{32} 加密下所得密文,以 V_r^W, V_r^N 表示在第 r 轮两个中间状态的第 2 个寄存器 L_2 的内容,根据状态转移公式可推得 $V_{243}{}^W$ 的左数第 1,2,4 比特的代数表达式如下:

$$u_{10}\oplus v_{18}\oplus(u_4\oplus v_{12}\oplus v_{17}v_{15}\oplus v_{13}v_8\oplus k_{73})(u_2\oplus v_{10}\oplus v_{15}v_{13}\oplus v_{11}v_6\oplus k_5)\oplus(u_0\oplus v_8\oplus v_{13}v_{11}\oplus v_9v_4\oplus k_7)v_{14}\oplus k_{16}\quad(3)$$

$$u_9\oplus v_{17}\oplus(u_3\oplus v_{11}\oplus v_{16}v_{14}\oplus v_{12}v_7\oplus k_2)(u_1\oplus v_9\oplus v_{14}v_{12}\oplus v_{10}v_5\oplus k_{11})\oplus v_{18}v_{13}\oplus k_{64}\quad(4)$$

$$u_7\oplus v_{15}\oplus(u_1\oplus v_9\oplus v_{14}v_{12}\oplus v_{10}v_5\oplus k_{11})v_{18}\oplus v_{16}v_{11}\oplus k_{17}\quad(5)$$

由式(2)、(5)得到关于 k_{11}的方程

$$u_7\oplus v_{15}\oplus(u_1\oplus v_9\oplus v_{14}v_{12}\oplus v_{10}v_5\oplus k_{11})v_{18}\oplus v_{16}v_{11}\oplus k_{17}\oplus[u'_7\oplus v'_{15}\oplus(u'_1\oplus v'_9\oplus v'_{14}v'_{12}\oplus v'_{10}v'_5\oplus k_{11})v'_{18}\oplus v'_{16}v'_{11}\oplus k_{17}]=0\quad(6)$$

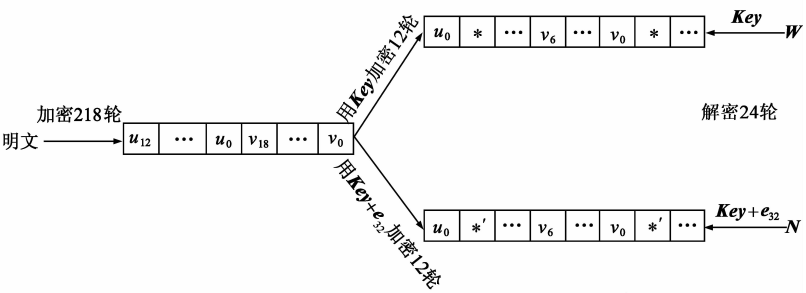

图2　KTANTAN-32相关密钥中间相遇8比特相等示意图

因 k_{17}在模 2 加时抵消,u_i, u'_i, v_i, v'_i 均已知,整理得

$$u_7\oplus v_{15}\oplus(u_1\oplus v_9\oplus v_{14}v_{12}\oplus v_{10}v_5)v_{18}\oplus v_{16}v_{11}\oplus[u'_7\oplus v'_{15}\oplus(u'_1\oplus v'_9\oplus v'_{14}v'_{12}\oplus v'_{10}v'_5)v'_{18}\oplus v'_{16}v'_{11}=k_{11}\oplus(v_{18}\oplus v'_{18})\quad(7)$$

这是关于 k_{11}的一元线性方程,解式(7)可得 k_{11}.把所求得 k_{11}代入如下由两个状态在左数第二比特相等所得方程

$$u_9\oplus v_{17}\oplus(u_3\oplus v_{11}\oplus v_{16}v_{14}\oplus v_{12}v_7\oplus k_2)(u_1\oplus v_9\oplus v_{14}v_{12}\oplus v_{10}v_5\oplus k_{11})\oplus v_{18}v_{13}\oplus k_{64}=u'_9\oplus v'_{17}\oplus(u'_3\oplus v'_{11}\oplus v'_{16}v'_{14}\oplus v'_{12}v'_7\oplus k_2)(u'_1\oplus v'_9\oplus v'_{14}v'_{12}\oplus v'_{10}v'_5\oplus k_{11})\oplus v'_{18}v'_{13}\oplus k_{64}\quad(8)$$

即可求得 k_2.对于后 15 轮所使用的其它密钥比特可列出类似方程组.

必须指出的是如果式(7)中等式左边为 0,右边 k_{11} 的系数也为 0,这时式(7)成为恒等式,导致无法确定 k_{11},此时必须再换一个明文.该事件发生的概率为 0.5,于是平均使用两个明文即可恢复 k_{11}.

在文献[6]中作者指出一种"难以解释"的现象:在使用计算机穷尽搜索 219 轮之后原来使用的 44 比特密钥时,若对第 254 轮所使用的密钥 k_{71}和 k_7 猜测错误,则把两个密文解密到 219 轮所得结果不会相等,即系统会显示猜测错误,但若对第 219 轮所使用密钥猜测错误,错误密钥照样能通过测试,即离 219 轮约越近的轮所使用的密钥对于判据的影响越小.产生该现象的原因可用式(8)解释如下:式(8)等式两边是 240 轮寄存器状态更新公式,在列方程时,本轮所使用密钥 k_{64}在模 2 加时抵消,对方程成立与否无任何影响,离末轮愈近的轮使用的密钥,方程对其依赖性愈小,离本轮愈远的轮使用的密钥(例如 k_2, k_{11}),方程愈非线性的依赖于它们,错误猜测愈难逃过检测,于是也就能够被确定了.

3.4　攻击的时间复杂度和空间复杂度

因为我们推得几个线性方程并逐个解出一些密钥比特,所以攻击成功的概率为 1,时间复杂度和空间复杂度可以忽略不计.

4 结论

由于轻量密码本身是在计算能力相对较薄弱的嵌入式处理器上工作,我们提出了一个对 KTANTAN32 的无须依赖于计算机辅助计算的纯代数攻击方法.运用代数推导,可以得到最后 15 轮所使用密钥比特的方程,其中部分方程甚至是一元一次的.求解这样的方程代数复杂度很低,无需任何存储空间,这表明 KTANTAN32 是一个很弱的密码体制.

我们认为 KTANTAN 系列轻量分组密码的不足之处在于其将非线性反馈状态更新模式和线性密钥编排一起使用.另外,k_{32}首次使用太晚,是导致相关密钥攻击的根本原因.与线性密钥编排方法相比,我们还是更赞成和支持 Eli Biham 所提出的密钥编排应引入一些非线性成分的分组密码设计理念[8],使用非线性密钥编排是增强密码体制抵抗相关密钥攻击能力的重要手段[9,10].

参考文献

[1] Andrey Bogdanov, Christian Rechberger. A 3-subset meet-in-the-middle attack: Cryptanalysis of the lightweight block cipher KTANTAN[A]. SAC 2010, LNCS 6544[C]. Berlin: Springer-Verlag, 2010. 229 – 240.

[2] Christophe De Cannière, Orr Dunkelman, Miroslav Knezevic. KATAN, KTANTAN-A family of small and efficient hardware-oriented block ciphers[A]. CHES 2009, LNCS 5747[C]. Berlin: Springer-Verlag, 2009. 272 – 288.

[3] Wenling Wu, Lei Zhang. LBlock: A light weight block cipher [A]. ACNS 2011, LNCS 6715[C]. Berlin: Springer-Verlag, 2011. 327 – 344.

[4] Simon Knellwolf, Willi Meier, Marfa Naya-Plasencia. Conditional differential cryptanalysis of NLFSR-based cryptosystems [A]. ASIACRYPT 2010, LNCS 6744[C]. Berlin: Springer-Verlag, 2010. 130 – 145.

[5] Lei Wei, Christian Rechberger, Jian Guo, Hongjun Wu, Huaxiong Wang, San Ling. Improved meet-in-the-Middle cryptanalysis of KTANTAN[A]. ACISP 2011, LNCS 6812[C]. Berlin: Springer-Verlag, 2011. 433 – 438.

[6] Martin Agren. Some instant and practical time related-key attack on KTANTAN32/48/64[OL]. http://eprint.iacr.org/2011/140.

[7] L. R. Knudsen. Cryptanalysis of LOKI[A]. ASIACRYPT 91, LNCS 739[C]. Berlin: Springer-Verlag, 22 – 35.

[8] Eli Biham, Orr Dunkelman, Nathan Keller. New cryptanalytic results on IDEA[A]. ASIACRYPT 2006, LNCS 4284[C]. Berlin: Springer-Verlag, 2006. 412 – 427.

[9] 唐学海,孙兵,李超.对 8 轮 CLEFIA 算法的一种现实攻击[J].电子学报,2011,39(7):1608 – 1612.
Tang Xue-hai, Sun Bing, Li Chao, A real-world attack of 8-round CLEFIA[J]. Acta Electronica Sinica, 2011, 39(7): 1608 – 1612. (in Chinese)

[10] Zhiqiang Liu, Dawu Gu, Jing Zhang. Multiple linear cryptanalysis of reduced-round SMS4 block cipher[J]. Chinese Journal of Electronics, 2010, 19(3): 389 – 393.

作者简介

张文英 女,1970 年生于山东鄄城,教授,信息安全国家重点实验室出站博士后,研究方向为密码学,在国内外核心期刊发表学术论文 20 余篇,其中多篇被 SCI、EI 检索.曾主持十一五国防科技预研课题,中国博士后科学基金,山东省自然基金等.
E-mail: wenyingzh@is.iscas.ac.cn

刘祥忠 男,1969 年 11 月生于山东烟台,中学一级教师,主要研究方向为网络安全与密码学.