计算机工程 2012, 38(3) 141-144 DOI: 10.3969/j.issn.1000-3428.2012.03.048 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

CLEFIA-128算法的不可能差分密码分析

郑秀林[1,2]，连至助[1,2]，鲁艳蓉[1,2]，袁 征[1]

(1. 北京电子科技学院信息安全系，北京 100070；2. 西安电子科技大学通信工程学院，西安 710071)

摘要： 研究13轮CLEFIA-128算法，在9轮不可能差分攻击的基础上，提出一种未使用白化密钥的不可能差分密码分析方法。猜测每个密钥，筛选满足轮函数中S盒输入输出差分对的数据对。利用轮密钥之间的关系减少密钥猜测量，并使用Early Abort技术降低计算复杂度。计算结果表明，该方法的数据复杂度和时间复杂度分别为2120和2125.5。

关键词： 分组密码 CLEFIA-128算法 密码分析 不可能差分密码分析 Early Abort技术

Impossible Differential Cryptanalysis of CLEFIA-128 Algorithm

ZHENG Xiu-lin [1,2], LIAN Zhi-zhu [1,2], LU Yan-rong [1,2], YUAN-Zheng [1]

(1. Department of Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China; 2. School of Telecommunications Engineering, Xidian University, Xi'an 710071, China)

Abstract: This paper presents an impossible differential cryptanalysis of 13-round CLEFIA-128 no whitening key, which use the 9-round impossible differential. In the process of cryptanalysis, it guesses each key and filter the data pairs using the output and input differences of S-box. It utilizes the keys relations to reduce the number of guessed keys, and introduces the early abort technique to reduce the time complexity. Computing result shows that the complexity of the cryptanalysis is about 2120 data and 2125.5 encryptions

Keywords: block cipher CLEFIA-128 algorithm cryptanalysis impossible differential cryptanalysis Early Abort

收稿日期 2011-08-16 **修回日期** **网络版发布日期** 2012-02-05

DOI: 10.3969/j.issn.1000-3428.2012.03.048

基金项目:

国家自然科学基金资助项目(61070250)；北京市自然科学基金资助项目(4102055)

通讯作者:

作者简介: 郑秀林(1956－)，男，教授，主研方向：对称密码学； 连至助、鲁艳蓉，硕士研究生；袁 征，副教授

通讯作者E-mail: lzz600@126.com

参考文献：

[1] Sony Corporation. The 128-bit Blockcipher CLEFIA, Security and Performance Evaluations,

Revision 1.0[EB/OL]. (2007-06-01). http://www.sony.net/Products/cryptography/clefia/.

[2] Shirai T.[J].Shibutani K, Akishita T, et al. The 128-bit Blockcipher CLEFIA(Extended Abstract)[C]//Proc. of FSE'07. Dubrovnik, Croatia: [s. n..2007,:-

[3] Wang Wei, Wang Xiaoyun. Improved Impossible Differential Cryptanalysis of CLEFIA [EB/OL]. (2008-05-05). http://eprint.iacr. org/2007/466.

[5] Zhang Wenying, Han Jing. Impossible Differential Analysis of Reduced Round CLEFIA [C]//Proc. of Inscrypt'08. Beijing, China: [s. n.]: 181-191.

本刊中的类似文章

1. 崔杰, 仲红.基于Feistel网络的十进制加密算法[J]. 计算机工程, 2012,38(3): 22-24,33
2. 刘树凯, 关杰, 常亚勤.针对流密码K2算法的猜测决定攻击[J]. 计算机工程, 2011,37(7): 168-170
3. 韩睿, 赵耿, 刘山鸣, 赵菲.基于混沌映射的分组密码算法[J]. 计算机工程, 2011,37(16): 120-122
4. 张聪娥, 刘军霞.Akelarre分组密码算法的奇偶校验分析[J]. 计算机工程, 2011,37(16): 111-113
5. 汪海明, 李明, 金晨辉.对LZ混沌序列密码算法的分割攻击[J]. 计算机工程, 2011,37(01): 137-138,141
6. 王保仓;刘 辉;胡予濮.对一个公钥密码体制的连分式攻击算法[J]. 计算机工程, 2010,36(8): 150-151
7. 孙克泉.基于完全平方数的RSA密码分析算法机理[J]. 计算机工程, 2010,36(7): 153-155,
8. 崔亚磊;戴紫彬.面向分组密码的NCL电路处理模型[J]. 计算机工程, 2010,36(4): 128-130
9. 常亚勤.针对自同步HBB算法的改进差分攻击[J]. 计算机工程, 2010,36(21): 134-136
10. 张庆贵.不可能差分攻击中的明文对筛选方法[J]. 计算机工程, 2010,36(2): 127-129

文章评论

反馈人		邮箱地址	
反馈标题		验证码	3538