中国科学院研究生院学报 2011, **28**(2) 266-273 **DOI**: **ISSN**: **CN**:

论文

6轮ARIA的最优不可能差分分析

张磊, 郭建胜

解放军信息工程大学电子技术学院, 郑州 450004

摘要:

研究了ARIA在不可能差分分析下的安全性.通过对算法扩散层的分析,给出了ARIA中间状态在加密过程的差分传递性质.在此基础上证明了6轮ARIA不存在使得输入输出差分重量小于10的不可能差分路径,同时证明了在输入输出差分重量为10的情况下6轮ARIA只存在2类形式的不可能差分路径.利用构造出的这2类不可能差分路径,从理论上证明了6轮ARIA不可能差分攻击的最优结果为:2^{120}个选择明文和$2^{94.5}$次6轮加密.

关键词: 分组密码 不可能差分分析 ARIA 数据复杂性 时间复杂性

Best impossible differential cryptanalysis of 6-round ARIA

ZHANG Lei, GUO Jian-Sheng

Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004, China

Abstract:

The security of the block cipher ARIA against impossible differential cryptanalysis is studied. First, we analyze the diffusion layer of ARIA and indicate some differential characters of the intermediate state through the encryption transformation. On the basis of these, we show that there is no 6-round impossible differential with the input-and-output differential weight less than ten and that there are only two kinds of 6-round impossible differential with the input-and-output differential weight of ten. Both kinds of the best impossible differentials can be found and can be used to attack the 6-round ARIA with the best results: the data complexity being 2^{120} chosen plaintexts and the time complexity being $2^{94.5}$ encryptions of 6-round ARIA.

Keywords: block cipher impossible differential cryptanalysis ARIA data complexity time complexity

收稿日期 2010-03-23 **修回日期** 2010-05-28 **网络版发布日期**

DOI:

基金项目:

通讯作者:

作者简介:

作者Email: zzll2000@163.com

参考文献:

[1] Daesung K, Jaesung K, Sangwoo P, et al. New block cipher: ARIA //Proceedings of the Information Security and Cryptology, ICISC’03. Springer-Verlag, LNCS 2971, 2003: 432-445.

[2] Wu W L, Zhang L. The state-of-the-art of research on impossible differential cryptanalysis [J]. Journal of Systems Science and Mathematical Sciences, 2008, 28(8): 971-983(in Chinese). 吴文玲,张蕾. 不可能差分密码分析研究进展 [J].系统科学与数学, 2008, 28(8):971-983.

[3] Kim J, Hong S, Sung J, et al. Impossible differential cryptanalysis for block cipher structures //Proceedings of Indocrypt 2003. Springer-Verlag, LNCS 2904, 2003: 82-96.

[4] Zhang W T, Wu W L, Feng D G.. New results on impossible differential cryptanalysis of reduced AES //Proceeding of ICISC 2007. LNCS 4817, 2007: 239-250.

[5] Tsunoo Y, Tsujihara E, Shigeri M, et al. Impossible differential cryptanalysis of CLEFIA //FSE 2008. Springer-Verlag, LNCS 5086, 2008: 289-302.

[6] Alex B, Christophe D C, Joseph L, et al. Security and performance analysis of ARIA:Version 1.2 . 2003 . http://homes.esat.kuleuven.be/abiryuko/ARIA-COSICreport.pdf.

[7] Wu W L, Zhang W T, Feng D G. Impossible differential cryptanalysis of reduced-round ARIA and Camellia [J]. Journal of Computer Science and Technology, 2007, 22(3): 449-456.

[8] Peng Z, Ruilin L, Bing S, et al. New impossible differential cryptanalysis of ARIA . . Cryptology ePrint Archive, Report 2008. http://eprint.iacr.org/.

[9] Li S H. Cryptanalysis of two symmetric encryption algorithms ARIA and SALSA20 . Jinan: Institute of Mathematics and System Science, Shandong University, 2008(in Chinese). 李申华. 对称密码算法ARIA和Salsa20的安全性分析 . 济南:山东大学数学与系统科学学院, 2008.

本刊中的类似文章

1．汤仲埙, 陈祖铿, 王伏雄.香椿有性生殖周期的研究[J]. 中国科学院研究生院学报, 1986,24(6): 447-453
2．王大印; 林东岱; 吴文玲; 姜中华.XOR-MAC消息认证码的安全性新证明[J]. 中国科学院研究生院学报, 2006,23(2): 257-262
3．李伟博 解永宏 胡磊.分组密码S盒的代数方程[J]. 中国科学院研究生院学报, 2008,25(4): 524-529
4．王 鹏; 冯登国.基于可调分组密码的MAC构造[J]. 中国科学院研究生院学报, 2005,16(6): 746-750
5．叶国梁.石笔木的学名考正：Tutcheria championii 还是 T. spectabilis?[J]. 中国科学院研究生院学报, 2004,42(6): 575-576