电子与信息学报
JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

电子与信息学报 » 2011, Vol. 33 » Issue (1) :190-193 DOI: 10.3724/SP.J.1146.2009.01626

论文

对Shannon算法的线性区分攻击

常亚勤* 金晨辉*

信息工程大学电子技术学院 郑州 450004

Linear Distinguishing Attack on Shannon Algorithm

Chang Ya-qin Jin Chen-hui*

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

摘要 该文基于对Shannon算法非线性反馈移位寄存器反馈函数和非线性滤波函数进行线性逼近，得到了优势为2^{-28}的32个新的区分器，给出了一个对流密码算法Shannon的新的线性区分攻击。该区分攻击大约需要2^{52}密钥字就能将Shannon算法的密钥流序列从随机序列中区分出来。

关键词： 序列密码 区分攻击 线性逼近 非线性反馈移位寄存器 Shannon算法

Abstract： A new distinguishing attack is presented on Shannon algorithm. The distinguish attack is built by using linear approximations of both the non-linear feedback shift register and the non-linear filtration function, and 32 distinguishers are derived which the bias is 2^{-28}. Therefore, the Shannon algorithm is distinguishable from truly random cipher after observing 2^{52} keystreams words on average.

Keywords： Stream ciphers Distinguishing attack Linear approximations Non-linear Feedback Shift Register (NFSR) Shannon algorithm

Received 2009-12-22;

通讯作者: 常亚勤 Email: Chyq1980@yahoo.cn

引用本文:

常亚勤, 金晨辉.对Shannon算法的线性区分攻击[J] 电子与信息学报, 2011,V33(1): 190-193

Chang Ya-Qin, Jin Chen-Hui.Linear Distinguishing Attack on Shannon Algorithm[J] , 2011,V33(1): 190-193

链接本文:

http://jeit.ie.ac.cn/CN/10.3724/SP.J.1146.2009.01626 或 http://jeit.ie.ac.cn/CN/Y2011/V33/I1/190