西安电子科技大学学报 2013, 40(3) 172-179+200 DOI: 10.3969/j.issn.1001-2400.2013.03.026 ISSN: 1001-2400 CN: 61-1076/TN

研究论文

一种抵抗能量攻击的线性反馈移位寄存器

赵永斌[1,2];胡予濮[1];贾艳艳[3]

(1. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071;
2. 石家庄铁道大学 信息科学与技术学院，河北 石家庄 050043;
3. 西安科技大学 计算机学院，陕西 西安 710054)

摘要：

通过分析延迟序列和初始状态之间的关系，给出了能够完全抵抗能量攻击所需触发器数目的下界；提出了一种抵抗能量攻击的流密码线性反馈移位寄存器(LFSR)的设计方案．在抵抗LFSR能量攻击时，附加触发器的个数最多为5个，大大减少了LFSR的附加功耗．

关键词： 密码学 流密码 能量攻击 线性反馈移位寄存器 触发器 布尔函数

New design of LFSR based stream ciphers to resist power attack

ZHAO Yongbin[1,2];HU Yupu[1];JIA Yanyan[3]

(1. State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071， China;
2. School of Information Science and Technology, Shijiazhuang Tiedao Univ., Shijiazhuang 050043，China;
3. College of Computer Science and Technology, Xi'an Univ. of Science and Technology, Xi'an 710054，China)

Abstract:

An additional large number of flip-flops are required for available linear feedback shift register (LFSR) design which can completely resist power attack on the stream cipher based on LFSR. By analyzing the relations between the delayed sequence and the initial states, the lower bound on the number of flip-flops in the design of LFSR based stream ciphers to resist the power attack is given and a novel lightweight design to resist power attack is proposed. With this method, the number of flip-flops required is decreased to five and the power consumption is significantly reduced.

Keywords: cryptography stream ciphers power analysis attack linear feedback shift registers flip-flop Boolean functions

收稿日期 2012-02-24 修回日期 网络版发布日期

DOI: 10.3969/j.issn.1001-2400.2013.03.026

基金项目:

973资助项目(2007CB311201)；国家自然科学基金资助项目(60833008)；保密通信重点实验室基金资助项目(9140C110201110C1102)

通讯作者: 赵永斌

作者简介: 赵永斌(1972-)，男，副教授，西安电子科技大学博士研究生，E-mail: zhaoyb@stdu.edu.cn.

作者Email: zhaoyb@stdu.edu.cn

参考文献：

［1］ Kocher P C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems［G］//CRYPTO'1996, LNCS 1440. Berlin: Springer, 1996: 104-113.
［2］ Kocher P C, Jaffe J, Jun B. Differential Power Analysis［C］//CRYPTO'1999, LNCS 1666. Berlin: Springer, 1999: 388-397.
［3］ Lano J, Mentens N, Preneel B, et al. Power Analysis of Synchronous Stream Ciphers with

Resynchronization Mechanism ［C］//SASC 2004, Workshop Record. Berlin: Springer-Verlag, 2004: 327-333.
［4］ Gierlichs B, Batina L, Clavier C, et al. Susceptibility of eSTREAM Candidates Towards Side Channel Analysis ［EB/OL］. ［2012-02-23］. http://www.ecrypt.eu.org/stvl/sasc2008/index.html
［5］ Fischer W, Gammel B M, Kniffler O, et al. Differential Power Analysis of Stream Ciphers ［C］//Advances in Cryptology-CT-RSA 2007, LNCS 4377. Berlin: Springer, 2006: 257-270.
［6］ Burman S, Mukhopadhyay D, Veezhinathan K, et al. LFSR Based Stream Ciphers are Vulnerable to Power Attacks ［C］//Advances in Crptology-INDOCRYPT'2007, LNCS 4859. Berlin: Springer, 2007: 384-392.
［7］ Jia Yanyan, Hu Yupu, Gao Juntao. Correlation Power Analysis of the Software Implementation of DECIMv2 ［J］. The Journal of China Universities of Posts and Telecommunications, 2011, 18(5): 118-123.
［8］ Steve B, Julia B, Vesselin V. The eSTREAM Portfolio in 2012 (Jan 2012) ［EB/OL］. ［2012-02-23］. http://www.ecrypt.eu.org/stream/.
［9］ Kumar S, Lemke K, Paar C. Some Thoughts about Implementation Properties of Stream Ciphers ［C］//SASC 2004, Workshop Record. Berlin: Springer-Verlag, 2004: 311-319.
［10］ Key E L. An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators ［J］. IEEE Trans on Information Theory, 1976, 22(11): 732-736.
［11］ Tu Ziran, Deng Yingpu. Boolean Functions Optimizing Most of the Cryptographic Criteria ［J］. Discrete Applied Mathematics, 2012, 160(4-5): 427-435.
［12］ Zhang Weiguo, Xiao Guozhen. Construction of Almost Optimal Resilient Functions Via Concatenating Maiorana-mcfarland Functions ［J］. Science China Information Sciences, 2011, 54(4): 909-912.
［13］ 何业锋, 马文平. 一类具有高非线性度的密码函数［J］. 西安电子科技大学学报, 2010, 37(6): 1107-1110.
He Yefeng,Ma Wenping. One Class of Highly Nonlinear Cryptographic Functions ［J］. Journal of Xidian University, 2010, 37(6): 1107-1110.
［14］ Hell M, Johansson T, Meier W. Grain-a Stream Cipher for Constrained Environments ［EB/OL］. ［2012-02-23］. http://www.ecrypt.eu.org/stream/grainp3.html.

本刊中的类似文章

1．魏仕民;董庆宽;肖国镇.确定周期序列k-错线性复杂度的一个快速算法[J]. 西安电子科技大学学报, 2001,28(4): 421-425
2．傅晓彤;张宁;肖国镇.对Chang等人的消息可恢复式签名方案的安全性分析[J]. 西安电子科技大学学报, 2005,32(6): 920-921
3．胡予濮;白国强;肖国镇.GF(q)上的广义自缩序列[J]. 西安电子科技大学学报, 2001,28(1): 5-8
4．王宏(1);肖鸿(2);邱刚(2);冯登国(1).安全分布式乘积产生方案[J]. 西安电子科技大学学报, 2006,33(1): 156-159
5．魏仕民;王宏;肖国镇.q元缩减发生器[J]. 西安电子科技大学学报, 2001,28(2): 187-190
6．暂时无作者信息.m阶相关免疫函数的构造与计数[J]. 西安电子科技大学学报, 1997,24(1): 0-0
7．谷大武;李继红;肖国镇.基于正形置换的密码函数的构造[J]. 西安电子科技大学学报, 1999,26(1): 0-0
8．暂时无作者信息.关于有限域上多项式因式分解[J]. 西安电子科技大学学报, 1998,25(3): 0-0
9．张育斌;葛方晖;肖国镇.一种基于有限扩域的公钥密码体制[J]. 西安电子科技大学学报, 2000,27(4): 496-500
10．胡予濮;肖国镇;杨礼珍.非齐进位模加群及其在密码体制中的应用[J]. 西安电子科技大学学报, 1999,26(4): 428-431
11．杨礼珍;傅晓彤;肖国镇.对非线性组合生成器的相关攻击[J]. 西安电子科技大学学报, 2001,28(5): 566-569
12．许春香;魏仕民;肖国镇.关于周期序列的线性复杂度[J]. 西安电子科技大学学报, 2001,28(4): 434-438
13．张应辉；李晖；马华.Schnorr类有序多重签名中的阈下信道的封闭协议[J]. 西安电子科技大学学报, 2011,38(3): 140-144
14．刘景伟;韦宝典;吕继强;王新梅.AES S盒的密码特性分析[J]. 西安电子科技大学学报, 2004,31(2): 255-259
15．白恩健;董庆宽;肖国镇.自缩控生成器[J]. 西安电子科技大学学报, 2004,31(2): 264-268