电子与信息学报 2006 28 (3): 542-545 ISSN: 1009-5896 CN: 11-4494/TN

论文

基于LFSR高次剩余问题构造公钥密码体制的研究

姜正涛, 柳 毅, 王育民

西安电子科技大学综合业务网国家重点实验室 西安 710071

收稿日期 2004-9-9 修回日期 2005-4-21 网络版发布日期 2007-12-18 接受日期

摘要
该文对用线性反馈移位寄存器(LFSR)构造公钥密码体制做了进一步的研究，定义了LFSR的高次(非)剩余问题，基于新的困难问题探讨了构造一种加解密不同于GH的密码原型，并给出了具体的加解密过程，证明了它的可行性；在此基础上，进一步把该体制改进为概率加密体制，克服了GH加密确定性的缺点，同时对体制的安全性和效率做了初步分析，具有单向性和语意安全性，最后证明了该体制的单向性等价于LFSR高次剩余问题，语意安全性等价于LFSR判断高次剩余问题。

关键词 公钥加密体制 LFSR 高次(非)剩余 单向性 语意安全性

分类号 TP309$^{+}_{-}$.7

Research on the Construction of Public-Key Cryptosystems Based on LFSR Residuosity Problem

Jiang Zheng-tao, Liu Yi, Wang Yu-min

National Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China

Abstract
Further research on the construction of public-key cryptosystem based on Linear Feedback Shift Register (LFSR) is provided, and the LFSR higher (non) residuosity problem is defined. Based on new intractability problems a new public-key encryption primitive with encryption/decryption procedures differ from GH is investigated. The encryption and decryption procedures are specified. It is further improved to be a probabilistic encryption scheme. Efficiency and security analysis of the proposed encryption scheme is provided. It has properties of one-wayness and semantic security. The one-wayness and semantic security are equivalent to higher LFSR residuosity and decisional LFSR residuosity problems respectively.

Key words Public-key encryption scheme LFSR higher (non) residuosity One-wayness Semantic security

DOI:

通讯作者

作者个人主页 姜正涛; 柳 毅; 王育民