电子与信息学报 2004 26 (12): 1990-1995 ISSN: 1009-5896 CN: 11-4494/TN

论文

描述Rijndael的一个新的方程组

李娜, 陈卫红

信息工程大学信息工程学院应用数学系 郑州 450002

收稿日期 2003-7-25 修回日期 2004-1-12 网络版发布日期 2008-4-24 接受日期

摘要

由于Rijndael的S盒的代数表达式是逆函数合成$GF(2^8)$上一个q-多项式，该文合理假设S盒的变量并通过讨论各变量之间的关系，把Rijndael用$GF(2^8)$上一个多变量二次方程组来表示，使得Rijndael的密钥恢复等同于求解这个方程组. 该方程组较Murphy-Robshaw方程组更简单，用XSL技术求解复杂度更低。

关键词 XSL攻击 多变量二次方程组 Rijndael

分类号 TN918.1

A New System of Multivariate Quadratic Equations for Rijndael

Li Na, Chen Wei-hong

Dept of Appl. Math.,Info. Eng. Inst.,Info. Eng. Univ., Zhengzhou 450002 China

Abstract

Because the algebraic expression of Rijndael S box is a composition of the converse function with a q-polynomial over $GF(2^8)$, in this paper the variables of S box are supposed rationally and the relations between these variables are analyzed, then a new system of multivariate quadratic equations over $GF(2^8)$ are used to describe completely Rijndael, the cryptanalysis of Rijndael can be written as a problem of solving the system of multivariate quadratic equations. This system is simpler than Murphy and Robshaw's, and has a lower complexity while applying XSL technique.

Key words XSL attack System of multivariate quadratic equations Rijndael

DOI:

通讯作者

作者个人主页 李娜; 陈卫红