计算机工程与应用 2010 46 (5): 111-113 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

AES的差分－代数攻击

刘连浩，温从剑

中南大学 信息科学与工程学院，长沙 410083

收稿日期 2008-8-21 修回日期 2008-11-10 网络版发布日期 2010-2-8 接受日期

摘要 差分－代数攻击是一种新的攻击方法，此方法结合了差分分析和代数攻击的思想。差分分析和代数攻击都是对高级加密标准（AES）最有效的攻击算法之一。对差分－代数如何在AES中应用进行了分析，并成功地应用此方法对5轮AES-256进行了攻击，使之比穷尽攻击更有效。

关键词 差分－代数 差分分析 代数攻击 高级加密标准（AES）

分类号 TP309

Differential-algebraic attack on AES

LIU Lian-hao，WEN Cong-jian

College of Information Science and Engineering，Central South University，Changsha 410083，China

Abstract

Differential-algebraic，which combines differential cryptanalysis and algebraic cryptanalysis，is a new cryptanalysis method.Either differential cryptanalysis or algebraic cryptanalysis is one of the most impactful cryptanalysis methods for AES.In this text how differential-algebraic is used in the AES is analyzed and this method is successfully used to attack the 5-round of the AES-256.The result shows that this method is better than the exhaustive search.

Key words differential-algebraic differential cryptanalysis algebraic cryptanalysis Advanced Encryption Standard（AES）

DOI: 10.3778/j.issn.1002-8331.2010.05.033

通讯作者 刘连浩 wcj2325@yahoo.com.cn