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

电子与信息学报 » 2010, Vol. 32 » Issue (8) :1953-1955 DOI: 10.3724/SP.J.1146.2009.01313

对强化MD结构杂凑函数的一个新的“牧群”攻击

陈士伟 金晨辉*

信息工程大学电子技术学院 郑州 450004

A New Herding Attack on Hash Functions with Strengthening Merkle-Damagard (MD) Construction

Chen Shi-wei Jin Chen-hui*

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

摘 要 该文构造了具有2^k个起始点的变长“钻石树”结构的多碰撞，并据此提出了对强化MD结构杂凑函数的一个新的选择目标强制前缀且原像长度为$2k+3$块的原像攻击(即“牧群”攻击)。由于增大了攻击过程中可利用的中间链接值的数量，故当$k\geq n/4-1.05$时，新的牧群攻击可将该攻击的计算复杂性由现有结果$O(2^{n-2(k+1)}+2^{n/2+k+5/2})$降至$O(2^{n-k}/3+2^{n/2+k+2})$。

关键词： 密码学 杂凑函数 强化MD结构 原像攻击 牧群攻击 多碰撞

Abstract： This paper constructs a “diamond structure” multicollision with 2^k initial values and variant lengths, which is used to propose a new chosen target forced prefix preimage attack (herding attack) on hash functions with Strengthening Merkle-Damagard (SMD) construction to find a preimage with $2k+3$ blocks. Since the number of the chaining values available in herding attack is increased, the computational complexity of herding attack is reduced to $O(2^{n-k}/3+2^{n/2+k+2})$ from $O(2^{n-2(k+1)}+2^{n/2+k+5/2})$ for $k\geq n/4-1.05$.

Keywords： Cryptography Hash functions SMD construction Preimage attack Herding attack Multicollision

Received 2009-10-09;

本文基金:

河南省杰出青年科学基金(0312001800)资助课题

通讯作者: 陈士伟 Email: chenshiwei1012@sohu.com

引用本文:

陈士伟, 金晨辉.对强化MD结构杂凑函数的一个新的“牧群”攻击[J] 电子与信息学报, 2010,V32(8): 1953-1955

Chen Shi-Wei, Jin Chen-Hui.A New Herding Attack on Hash Functions with Strengthening Merkle-Damagard (MD) Construction[J] , 2010,V32(8): 1953-1955

链接本文:

http://jeit.ie.ac.cn/CN/10.3724/SP.J.1146.2009.01313 或 http://jeit.ie.ac.cn/CN/Y2010/V32/I8/1953