通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

邹剑1,2,吴文玲1,吴双1,董乐1,2.对缩减轮数DHA-256的原像与伪碰撞攻击[J].通信学报,2013,(6):8~15

对缩减轮数DHA-256的原像与伪碰撞攻击

Preimage and pseudo collision attacks onround-reduced DHA-256 hash function

投稿时间： 2012-08-30

DOI：10.3969/j.issn.1000-436x.2013.06.002

中文关键词：DHA-256散列函数 原像攻击 伪碰撞攻击 中间相遇攻击

英文关键词:DHA-256 hash function preimage attack pseudo collision attack meet-in-the-middle

基金项目:国家重点基础研究发展计划（“973”计划）基金资助项目（2013CB338002）；国家自然科学基金资助项目（61272476，61232009）

作者	单位
邹剑1,2，吴文玲1，吴双1，董乐1,2	1. 中国科学院 软件研究所 可信计算与信息保障实验室，北京 100190；2. 中国科学院 研究生院，北京 100190

中文摘要:

提出了对DHA-256散列函数37轮的原像攻击以及39轮的伪碰撞攻击。基于中间相遇攻击，利用Biclique方法可以改进之前对DHA-256的原像分析结果，将攻击轮数从原来的35轮提高到了37轮。通过上述方法还可以构造对DHA-256的39轮伪碰撞。最终，以2255.5的时间复杂度以及23的空间复杂度构造了对DHA-256的37轮原像，并以2127.5的时间复杂度以及常数2的空间复杂度构造了对DHA-256的39轮伪碰撞。这是目前对DHA-256最好的原像与碰撞攻击结果。

英文摘要:

A preimage attack on DHA-256 hash function reduced to 37-round and a pseudo collision attack on the function reduced to 39-round were proposed respectively. Based on the meet-in-the-middle attack, the Biclique technique was used to improve the preimage attack from 35-round to 37-round. A 39-round pseudo collision was achieved using the Biclique technique. Overall, a preimage of DHA-256 was constructed with a complexity of and a memory of . Besides, a pseudo collision of DHA-256 was proposed with a complexity of . These are the best results of preimage and collision attack on DHA-256 hash function.

查看全文 查看/发表评论 下载PDF阅读器

关闭