电子与信息学报 2009 31 (9): 2260-2263 ISSN: 1009-5896 CN: 11-4494/TN

学术讨论

CLEFIA密码的Square攻击

唐学海[①], 李 超[①②], 谢端强[①]

[①]国防科技大学数学与系统科学系 长沙 410073; [②]东南大学移动通信国家重点实验室 南京 210096

收稿日期 2008-9-19 修回日期 2009-4-28 网络版发布日期 2009-9-2 接受日期

摘要
该文根据CLEFIA密码的结构特性，得到了Square攻击的新的8轮区分器，并指出了设计者提出的错误8轮区分器。利用新的8轮区分器对CLEFIA密码进行了10到12轮的Square攻击，攻击结果如下：攻击10轮CLEFIA-128\192\256的数据复杂度和时间复杂度分别为2^{97}和$2^{92.7}$；攻击11轮CLEFIA-192\256的数据复杂度和时间复杂度分别为2^{98}和$2^{157.6}$；攻击12轮CLEFIA-256的数据复杂度和时间复杂度分别为$2^{98.6}$和2^{222}。攻击结果表明：在攻击10轮CLEFIA时，新的Square攻击在数据复杂度和时间复杂度都优于设计者给出的Square攻击。

关键词 密码 CLEFIA 区分器 Square攻击

分类号 TN918.1

Square Bttack on CLEFIA

Tang Xue-hai[①], Li Chao[①②], Xie Duan-qiang[①]

[①]Department of Mathematics and System Science, National University of Defense Technology, Changsha 410073, China; [②]National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China

Abstract
According to the structure properties of CLEFIA , new 8-round distinguishers for Square attack are presented, and the wrong 8-round distinguishers originally found by the designers are pointed out. Based on the new distinguisher, the square attack on CLEFIA can be improved as follows: 10-round CLEFIA-128\192\256 is attacked with data complexity 2^{97} and time complexity $2^{92.7}$, 11-round CLEFIA-192/256 is attacked with data complexity 2^{98} and time complexity $2^{157.6}$, and 12-round CLEFIA-256 is breakable with data complexity $2^{98.6}$ and time complexity 2^{222}. These results demonstrate that under the case of 10-round CLEFIA, both data and time complexity of our attack are better than those given by the designers.

Key words Cryptograph CLEFIA Distinguisher Square attack

DOI:

通讯作者

作者个人主页 唐学海[①]; 李 超[①②]; 谢端强[①]