计算机应用 2007 (12): 2940-2941 ISSN: 1001-9081 CN: 51-1307/TP

网络与信息安全

Blowfish密码系统分析

钟黔川[1];朱清新[2]

电子科技大学计算机学院[1]

电子科技大学 计算机科学与工程学院[2]

收稿日期 2007-6-22 修回日期 网络版发布日期 2007-12-1 接受日期

摘要 Blowfish算法自提出以后便得到了广泛应用，很多针对它的攻击也随之出现，但未见对它有实质性的挑战。针对Blowfish算法加密过程中出现的缺陷，给出了从Blowfish算法更新后得到的子密钥数组直接导出密钥数组K的详细过程，指出在应用中可能造成整个Blowfish算法被攻破。另外，用反证法证明了由于不满足前提条件,因而滑动攻击对Blowfish算法失效。

Abstract Since Blowfish algorithm has been proposed and applied widely, a lot of attacks aiming at it have appeared, but none of them has substantial challenge to it. Concerning the weakness of Blowfish algorithm that appeared in the encrypting process, the detailed process was given that the subkey array renewed from Blowfish algorithm could educe a key array K directly, which may result in that the whole Blowfish algorithm was broken in applications. Moreover, slide attack was proved to be not effective to Blowfish algorithm with reduction to absurdity, its precondition was not satisfied.

关键词 Blowfish 滑动攻击 分组密码

Key words Blowfish;slide attacks;block cipher

分类号 TP309

DOI:

通讯作者:
钟黔川 qczhong@163.com,qczhong@sina.com

作者个人主页: 钟黔川 朱清新