计算机应用 2006 26 (05): 1058-1060 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

基于混沌映射的Hash函数及其在身份标识认证中的应用

何希平,朱庆生

重庆工商大学计算机科学与信息工程学院

收稿日期 2005-11-9 修回日期 网络版发布日期 接受日期

摘要 对用户身份标识进行加密、隐秘存储与认证是软件等版权保护所必须首先经历的步骤。论文首先给出了一个分段线性混沌映射，并构造了其复合函数，进而分析了它们的统计特性；为实现身份标识加密，构建了基于混沌映射的Hash函数，并在此基础上进一步构造了生成隐含身份标识的认证证书的Hash函数。试验结果表明，该算法准确、安全、高效、实用。

Abstract The encryption, secret storage, and authentication of user-identity-identifier are the necessary steps in the copyright protection for software, and so on. In this paper, we propose a piecewise-linear chaotic map and construct its composite function whose statistic characteristics are analyzed. For the purpose of encrypting user-identity-identifier, a chaotic-map-based Hash function is constructed. Based on the first function, other Hash functions are also constructed to generate certificate in which user-identity-identifier is hidden. The authors' experiment results show that the proposed algorithms are exact, security, efficient, and practical for information encryption and identity certification.

关键词 混沌映射,身份认证标识,Hash函数,加密

Key words chaotic map,identity identifier,Hash function,encryption

分类号

DOI:

通讯作者:
何希平 jsjhxp@ctbu.edu.cn;cqhxping@126.com

作者个人主页: 何希平;朱庆生