电子与信息学报 2010 32 (3): 613-616 ISSN: 1009-5896 CN: 11-4494/TN

论文

LDPC码在加密系统中应用的约束条件

林雪红, 牛 凯, 林家儒

北京邮电大学信息与通信工程学院 北京 100876

收稿日期 2009-2-9 修回日期 2009-9-25 网络版发布日期 2010-3-4 接受日期

摘要
该文首先给出了基于LDPC码公钥加密系统中授权用户获取明文的置信传播迭代译码算法，并得出了在明文信息等概的情况下授权用户要成功获取明文，私钥所需满足的必要条件。然后根据置信传播递归迭代算法分析了公钥参数设计的充分必要条件。最后通过仿真验证了私钥和公钥参数设计的正确性。

关键词 LDPC码 置信传播算法 加密系统

分类号 TN911.22

The Constraint Conditions for LDPC Codes in Cryptosystem

Lin Xue-hong, Niu Kai, Lin Jia-ru

School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract
This paper first presents Belief Propagation (BP) iteration algorithm in LDPC code-based public-key cryptosystems, and develops the necessary condition of private key if the probability of plaintext is equal. Then the necessary and sufficient condition of public key is deduced according to the recursion of BP iteration algorithm. Simulations show that the parameters of private key and public key are correct.

Key words LDPC codes Belief Propagation (BP) algorithm Cryptosystem

DOI: 10.3724/SP.J.1146.2009.00160

通讯作者 林雪红 lxh121@sina.com
作者个人主页 林雪红; 牛 凯; 林家儒