计算机应用 2006 26 (08): 1824-1826 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

基于3DES算法的电话加密研究及其FPGA实现

阎磊[1];侯春萍[1];曹达仲[2];戴居丰[2,2]

天津大学[1]

收稿日期 2006-3-6 修回日期 2006-4-7 网络版发布日期 2006-8-1 接受日期

摘要 针对通信安全性问题，分析了三重数据加密的密钥保管问题和语音加密的实时处理技术，提出了将算法移植到电话中加密语音信号的系统结构并进行了硬件设计。开发了加密运算的软件功能模块，并将算法模块移植到现场可编程门阵列中，在公用电话网上试验成功。研究表明,该加密功能模块可用于点对点的语音通信和其他低速率数据通信模型。

Abstract With regard to communication security, the safekeeping of password and real-time processing in speech signal encryption based on triple Data Encryption Standard (3DES) were analyzed. In addition, the basic framework of speech encryption and the hardware system design in encryption telephone were presented. The functional module of system software was designed and the compiled program was loaded into the FPGA. The encryption telephone was validated in the public telephone net. This research indicates that the encryption functional module can be applied to point-to-point speech communication and other low speed data traffic.

关键词 三重数据加密标准 语音信号 现场可编程门阵列

Key words triple Data Encryption Standard(3DES);speech signal;Field Programmable Gate Array(FPGA)

分类号

DOI:

通讯作者:
阎磊 keluyifu_2000@163.com

作者个人主页: 阎磊 侯春萍 曹达仲 戴居丰