

基于量子密钥分发系统的 TCP/IP 模块实现

林弘伟 1 , 杨灿美 2 , 林福江 1

(1 中国科学技术大学 微纳电子系统集成研究中心, 安徽 合肥 230026;

2 科大国盾量子技术股份有限公司, 安徽 合肥 230088)

摘要: 量子保密通信设备集成化是目前的趋势, 而量子密钥分发系统是其中的关键. 本文对该系统中对安全性和系统性能的需求, 提出了一种基于硬件的 TCP/IP 协议处理结构. 该结构采用数字电路设计方法, 实现了 TCP/IP 协议中网络层和传输层的相关功能, 并通过 AHB 接口集成到系统芯片中. 该结构作为独立的网络数据处理模块能够减轻 CPU 的计算负担, 同时设置该模块以自定义端口方式工作, 将量子域与经典网络隔离, 降低密钥泄露风险. 测试结果显示该结构可达到 450 Mbps 的数据吞吐率, 能够满足量子密钥分发中网络带宽的需求.

关键词: TCP/IP 协议; 硬件实现; 保密通信; 量子密钥分发

An Implementation of TCP/IP Module Based on Quantum Key Distribution System

LIN Hong-wei 1 , YANG Can-mei 2 , LIN Fu-jiang 1

(1 Micro-/Nano-Electronic System Integration Center, University of Science and Technology of
China,

Hefei 230026, China; 2 QuantumCTek Co., Ltd., Hefei 230088, China)

Abstract: The integration of the quantum cryptography communication devices is a current trend, and quantum key distribution system is a crucial part. In this paper, a hardware based TCP/IP protocol processing structure is proposed to meet the requirements of the security and system performance in the design of quantum key distribution chip. The structure realizes the functions of the network layer and transport layer in the TCP/IP protocol by digital circuit design method, and it can be integrated into the system chip through the AHB interface. As an independent network processing module, this structure can reduce the computing burden of CPU. At the same time, by setting the module to work in a custom port mode and isolating the quantum domain from the classical network, the risk of key disclosure will be reduced. The test results show that the structure can achieve data throughput of 450Mbps, and it can meet the demand of network bandwidth in quantum key distribution.

Key words: TCP/IP protocol; hardware implementation; cryptography communication ; quantum key distribution

作者简介:

林弘伟 , (1991-), 硕士研究生.研究方向为电路与系统.Email: linhw@mail.ustc.edu.cn.

杨灿美 , (1965-), 博士, 研究员.研究方向为通信数字基带系统集成电路设计、SoC 架构与设计.

林福江 , (1958-), 博士, 教授.研究方向为微纳器件的射频建模、芯片设计、微波系统集成.