Contribution ID: **125** Type: **not specified**

基于 FPGA 的量子密钥分发系统中身份认证的设计

Thursday, 16 August 2012 11:35 (15 minutes)

摘要：本文介绍了一种在面向 FPGA 实现的应用于量子密钥分发系统（QKD 系统）的身份认证方案。该方案采用基于 LFSR-Teoplitz 的哈希矩阵，易于 FPGA 实现，并且安全系数高。通过采用从 QKD 系统中分流一小部分密钥用于身份认证功能的实现，这种方案的安全性可以达到很高的水平。结合 FPGA 的特性和实现过程中可能出现的问题，本文设计了一种相对完善的身份认证流程，可以满足各种类型 QKD 系统的身份认证需求。
关键字：身份认证，QKD 系统

Primary author: Mr 崔, 珂 (中国科学技术大学)

Presenter: Mr 崔, 珂 (中国科学技术大学)

Session Classification: 第二分会场（核电子学、核医学电子学、计算技术应用）

Track Classification: 核电子学