Contribution ID: **124** Type: **not specified**

基于 Hash 函数的安全密钥扩展算法的研究

Thursday, 16 August 2012 11:20 (15 minutes)

摘要：本文针对目前 QKD(Quantum Key Distribution) 系统中密钥产生速率不高的情况, 提出了一种基于安全哈希算法的密钥扩展算法，以提高密钥的产生率，能符合一些对密钥生成率较高的应用，比如视频会议等，并基于 FPGA(Field Programmable Gate Array) 进行了实现。对扩展后的密钥进行随机性检测，以检测其安全性。实验表明，扩展倍数在 32 以内都通过了 NIST 的检测，说明随机性符合安全要求。

关键字：量子密钥分发，秘钥扩展，安全哈希算法，现场可编程逻辑阵列

Primary author: Mrs 罗, 春丽 (中国科学技术大学)

Presenter: Mrs 罗, 春丽 (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