Contribution ID: **20** Type: **not specified**

应用于量子密钥分发系统的 TCPIP 卸载引擎的设计

Tuesday, 16 July 2019 15:00 (20 minutes)

目前基于诱骗态 BB84 协议的量子密钥分发系统（quantum key distribution）已经在一定范围内得到应用。量子密钥分发系统在工作过程中，需要使用两条信道：一条是量子信道，在量子信道中完成量子态的传输。另一条是经典信道，网络，量子密钥分发的双方 Alice 和 Bob 需要通过网络完成基矢比对等数据后处理过程中的信息交互。目前量子密钥分发系统的安全成码距离已经达到百公里以上。中科大在 2016 年实现了超过 400 公里的测量器件无关量子密钥分发。在如此远的距离上实现双方可靠的信息交互，需要使用可靠的网络通讯协议，即 TCPIP 协议。而且随着 QKD 系统对成码率要求的不断提高，数据后处理过程对网络带宽的需求也在不断提高，如何在 QKD 系统中实现安全的，快速的网络交互成为一个不可回避的问题。在目前的 QKD 系统中，通常使用 CPU 来实现 TCPIP 协议栈。在远距离网络交互的过程中，必然会出现报文乱序，报文丢失，报文比特翻转等网络中常见的错误。QKD 密钥分发的过程中需要进行大量的数据交互，要求 TCPIP 协议栈能够快速的处理大量报文的解析，重排，窗口滑动等过程。如果使用软协议栈的方式实现，一是由于软件易受攻击，安全性会降低，这对于 QKD 系统来说，是不能忍受的；二是处理网络报文会消耗 CPU 大量的资源。基于以上考虑，我们将 TCPIP 协议硬化，研发了 TCPIP 协议卸载引擎，将网络数据传输模块作为 CPU 的外设，来实现高效的、安全的网络通讯。同时，在 TCPIP 里面做了加密和解密模块。在发送端，所有通过 TCPIP 传输的数据都进行加密后再发送，在接收端，所有数据解密后再交给用户。并且加密解密的密钥都来自 QKD 系统，提高了网络通讯的安全性。

Primary author: Dr 钟, 晓东 (中国科学技术大学)

Co-author: Prof. JIN, Ge (University of Science and Technology of China)

Presenter: Dr 钟, 晓东 (中国科学技术大学)

Session Classification: 核电子学与探测技术 I

Track Classification: 科研信息化管理与系统