基于 PON 网络的安全量子 VPN 方案

黄　鹏[①]　刘　晔[①]　周南润[①]　曾贵华[②]
[①](南昌大学电子信息工程系　南昌　330031)
[②](上海交通大学区域光纤通信网与新型光通信系统国家重点实验室　上海　200240)

摘　要：该文提出了一个新的无源光网络 PON 组成模型。利用该模型设计了一个具有身份认证功能的高效量子密钥分配方案，以满足无源光网络中光线路终端对光网络单元的身份认证和两者间的相互量子密钥分配，以及实现光虚拟专用网内部光网络单元间的量子密钥分配。安全性分析和实验方案表明了该协议的绝对安全性和可行性。将共享密钥作为通信双方的会话密钥，对内部传输数据进行加密，最终实现量子虚拟专用网。

关键词：无源光网络；虚拟专用网；量子密钥分配
中图分类号：TP393; TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2009)07-1758-05

A Secure Quantum Virtual Private Network Scheme in Passive Optical Network

Huang Peng[①]　Liu Ye[①]　Zhou Nan-run[①]　Zeng Gui-hua[②]
[①](*Department of Electronics Information Engineering*, *Nanchang University*, *Nanchang* 330031, *China*)
[②](*State Key Laboratory of Advanced Optical Communication Systems and Networks*, *Shanghai Jiaotong University*, *Shanghai* 200240, *China*)

Abstract: A novel Passive Optical Network (PON) model is proposed. By exploiting this architecture, an efficient Quantum Key Distribution (QKD) protocol with Quantum Identity Authentication (QIA) is designed. In this scheme, both the QIA and QKD between optical line terminal and optical network units in this PON are implemented. Also, the QKD is implemented between each two optical network units in the same optical virtual private network with the simple operations of optical line terminal. The security proofs and the proposed experimental scheme show this protocol is feasible and absolutely secure. Quantum virtual private network can be ultimately realized by using the conversation key generated by QKD protocol to encrypt the intra-communication data.

Key words: Passive Optical Network (PON); Virtual Private Network (VPN); Quantum Key Distribution (QKD)

1　引言

接入网在网络通信系统中起着重要的作用，其中，无源光网络(Passive Optical Network, PON)技术由于消除了局端与用户端之间的有源设备，使得网络的维护变得简单，而且可靠性高、成本低，成为打破“最后一公里”瓶颈中引起人们兴趣的核心技术。然而 PON 中的安全问题一直没有很好的解决方案。一个 PON 中只能有一个光线路终端(Optical Line Terminal, OLT)，但是可以有若干个光网络单元(Optical Network Unit, ONU)，即 ONU 用户端共享一段光纤，这给 PON 网络带来了不可靠性。根据 PON 接入网的特点，通信中要求所有 ONU 用户发出和接收的信号均通过 OLT，这种通信方式不仅浪费了通信资源，而且给通信过程带来了很大的安全问题(几乎无安全可言)。为此，光通信领域的一些学者发展了两个 ONU 用户在通信时绕过 OLT 的光通信机制[1−3]。文献[4]对 PON 中存在的安全问题做了详细分析并提出了相应的解决方案。但是，这些改进仍然没有从根本上解决 PON 中的安全问题。因为在通信的过程中，OLT 始终处于主动地位，OLT 可随时获取 ONU 用户发送的任何信息。

为了解决 PON 中的安全问题，本文将量子保密通信思想引入传统的光虚拟专用网中，提出了量子虚拟专用网(VPN)的概念，设计了一个 PON 组成模型，并提出一个具有认证功能的量子密钥分配协议(Quantum Key Distribution, QKD)，不仅可以解

2008-04-16 收到，2009-03-17 改回
国家自然科学基金(60773085, 10647133)，江西省自然科学基金(2007GQS1906)，省教育厅科技项目(赣教技字[2007]22)，省教育科学“十一五”规划项目重点课题(07ZD017)和省研究生创新专项资金(YC07A033)资助课题

决 VPN 中的认证的关键问题，而且可以实现虚拟专用网内部 ONU 用户间的量子密钥分配。因为 OLT 不会参与 ONU 用户间的密钥分配，即 ONU 用户间的通信对于 OLT 是保密的，从而能有效地降低 OLT 的工作负担，提高 ONU 用户间通信的安全性。

2　基于直接安全通信的量子 VPN 协议

2.1 PON 网络中 OLT 与 ONU 之间具有认证功能的 QKD 协议

图 1 为 PON 组成模型，OLT 由 Einstein-Podolsky-Rosen(EPR)纠缠光子源、光环行器以及连接在光环行器光路上的反射镜，从与 EPR 源的连接光路到与 ONUi(第 i 个 ONU 用户)的连接光路(图中双箭头连线即指代光路)，分别对反射镜编号为 $0\sim i$。其中反射镜为微机电系统(MEMS)器件，全部由 OLT 自动控制闭合，它们和光环行器组合在 PON 中起选路作用。首先考虑 OLT 和 ONU 用户间的身份认证及密钥分配协议。当 OLT 端向同一个虚拟专用网内部 ONU 用户 ONUi 发起通信时(或当通信发起方为 ONUi 时)，OLT 关闭反射镜 0。在 GPON 标准中，一个 OLT 最多可带 32，64 或者 128 个 ONU，本方案中一个 OLT 可带的 ONU 数量没有具体的限制，但增加 ONU 的个数会提高 OLT 的密钥管理难度。设 OLT 与每一个 ONUi 共享一串初始认证密钥 $K_i=\{k_i^1,k_i^2,\ldots,k_i^r\}$。根据共享密钥构造对应的测量基集合 $M_i=\{m_i^1,m_i^2,\ldots,m_i^r\}$，其中 $m_i^j\in\{\sigma_z,\sigma_x\}$，$j=1,2,\cdots,r$。即当 $k_i^j=0$ 时，$m_i^j=\sigma_z$；当 $k_i^j=1$ 时，$m_i^j=\sigma_x$。定义 4 个 Bell 态为 $\left|\psi^{xy}\right\rangle\equiv(\left|0,y\right\rangle+(-1)^x\left|1,\overline{y}\right\rangle)/\sqrt{2}$，其中 $\overline{y}$ 是 y 的逻辑非，$x,y\in\{0,1\}$。协议流程描述为

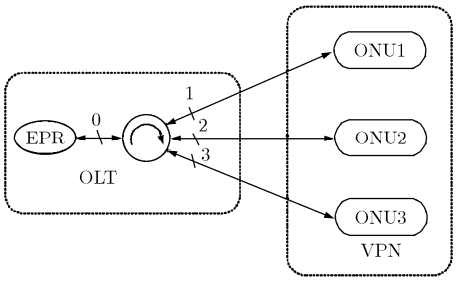

图 1 使用光环行器和反射镜的 PON

(1)OLT 确定并验证通信对象，根据参与通信的 ONUi，调节支路反射镜的闭合。例如，要和 ONU1 通信，则关闭反射镜 1，而如果要和 ONUi 通信，则打开除第 i 个反射镜以外的所有反射镜。

(2)OLT 由 EPR 源制备 n 对纠缠光子处于以下的 Bell 态：

$$\begin{aligned}\left|\psi_{ht}^{01}\right\rangle&=1/\sqrt{2}\left(\left|0_h1_t\right\rangle+\left|1_h0_t\right\rangle\right)\\&=1/\sqrt{2}\left(\left|x+\right\rangle_h\left|x+\right\rangle_t-\left|x-\right\rangle_h\left|x-\right\rangle_t\right)\end{aligned}\quad(1)$$

其中下标 h 表示本地光子，下标 t 表示传输光子。OLT 保留其中的 h 光子序列，将 t 光子序列通过 PON 网络发出，经过第(1)步对反射镜的调节，保证 t 光子序列送达 ONUi。

(3)检测信道的完善保密性。ONUi 随机选取 k ($k\ll n$) 个 t 光子组成检测序列，随机使用 σ_z 或 σ_x 基对它们进行测量，然后将选择的光子位置、测量基和测量结果告诉 OLT。OLT 根据收到的信息使用相同的测量基测量相应的 h 光子，并比较测量结果，当错误率小于一定的阈值，则协议继续；否则停止协议。

(4)OLT 对 ONUi 进行身份认证。ONUi 随机选取 r ($r\ll n$) 个 t 光子组成认证序列，用测量基集合 M_i 对应地对该光子序列进行测量并告知 OLT 选取的光子位置和相应的测量结果。OLT 根据共享的认证密钥同样构造测量基集合 M，并使用该测量基对相应的 h 光子进行测量。当共享密钥为 0 时，OLT 和 ONUi 的测量结果相反；当共享密钥为 1 时，两者的测量结果相同。当所有结果相符时，认证通过，协议继续；否则认证失败，停止协议。

(5)ONUi 随机选取操作 $U_0=\left|0\right\rangle\left\langle0\right|+\left|1\right\rangle\left\langle1\right|$ 或 $U_1=\left|0\right\rangle\left\langle1\right|+\left|1\right\rangle\left\langle0\right|$ 对剩余的 $n-r-k$ 个 t 光子的信息序列做操作，并告知 OLT 他选用的操作。然后 ONUi 根据选取的操作制备一个新光子(记为 m 光子)，即当选取的操作为 I 时，制备的 m 光子的状态为 $\left|\psi_i^m\right\rangle=\left|0\right\rangle$；当选取的操作为 X 时，制备的 m 光子的状态为 $\left|\psi_i^m\right\rangle=\left|1\right\rangle$，并作用一个受控量子非门在 t、m 光子上。经过操作，整个系统随机处于以下两种状态：

$$\begin{aligned}G_i&=C_{tm}\left[\left(U_i\left|\psi_{ht}^{01}\right\rangle\right)\otimes\left|i_m\right\rangle\right]\\&=\frac{1}{\sqrt{2}}\left(\left|0_h\right\rangle\left|\bar{i}_t1_m\right\rangle+\left|1_h\right\rangle\left|i_t0_m\right\rangle\right)\\&=\frac{1}{\sqrt{2}}\left[\left|x+\right\rangle_h\left|\psi_{tm}^{0i}\right\rangle-(-1)^i\left|x-\right\rangle_h\left|\psi_{tm}^{1i}\right\rangle\right]\end{aligned}\quad(2)$$

其中 $i\in\{0,1\}$，$\bar{i}$ 是 i 的逻辑非。

(6)获取共享密钥。ONUi 用 Bell 基依次测量每对 t，m 光子，测量结果 $\left|\psi^{00}\right\rangle$,$\left|\psi^{01}\right\rangle$,$\left|\psi^{10}\right\rangle$ 和 $\left|\psi^{11}\right\rangle$ 分别解码为 00，01，10 和 11。OLT 用 σ_x 基测量 h 光子，根据 ONUi 使用的操作可以推得 ONUi 的测量结果。OLT 随机选取一些位置要求 ONUi 公布密钥，OLT 比较测量结果，如果错误率小于一定的阈值，协议继续，最终获取共享密钥 $\tilde{K}$；否则停止协议，抛弃以前的测量结果。ONUi 选取的操作与 OLT 和

ONUi 测量结果之间的关系如表 1 所示。

表 1 ONUi 选取的操作与 OLT 和 ONUi 测量结果之间的关系

OLT 的测量结果	$\|x-\rangle_h$		$\|x+\rangle_h$	
ONUi 的操作	U_0	U_1	U_0	U_1
ONUi 的测量结果	$\left\|\psi_{tm}^{10}\right\rangle$	$\left\|\psi_{tm}^{11}\right\rangle$	$\left\|\psi_{tm}^{00}\right\rangle$	$\left\|\psi_{tm}^{01}\right\rangle$
共享密钥 $\tilde{K}$	10	11	00	01

(7)更新认证密钥。OLT 和 ONUi 从 $\widetilde{K}$ 中选取 r 个比特构成新的认证密钥 K_i'，其他密钥构成信息密钥 K，同时放弃原来的认证密钥。

2.2 PON 网络中 ONU 之间的 QKD 协议

(1)VPN 内部用户通信的发起者 ONUi 首先向 OLT 提出与 ONUj(第 j 个 ONU 用户，$j \neq i$)通信申请，OLT 对 ONUi 和 ONUj 分别进行身份认证，认证步骤与 2.1 节中的第(1)-(4)步相同，这里 OLT 只要制备 $2r$ 对 EPR 光子作为认证序列。

(2)OLT 确定通信双方为 ONUi 和 ONUj 后，关闭反射镜 i 和 j，打开反射镜 0 和其他所有反射镜，保证 ONUi 发出的光子能到达 ONUj。

(3)ONUi 由 EPR 源制备 n 对纠缠光子处于以下的 Bell 态 $\left|\psi_{ht}^{01}\right\rangle$，ONU$i$ 与 ONUj 进行信道完善性检测，检测步骤与 2.1 节中第(3)步相同。通过则进行下一步密钥分配，分配方案与 2.1 节中第(5)-(6)步相同；否则，停止协议。这时 ONUi 相当于 OLT，是通信的发起者，ONUj 是通信的对象。保证 ONUi 和 ONUj 之间获得共享密钥 $\tilde{K}$。

(4)更新认证密钥。ONUi 和 ONUj 分别选取 r 比特作为新的认证密钥 K_i' 和 K_j'，并分别将 $K_i \oplus K_i'$ 和 $K_j \oplus K_j'$ 告诉 OLT。OLT 用原始密钥与收到的认证密钥进行模二加操作，可以与 ONUi 和 ONUj 分别获取新的共享认证密钥，并放弃原来的认证密钥。ONUi 和 ONUj 从剩余的密钥中获取信息密钥 K。

2.3 基于 PON 网络的量子 VPN 协议

当通信双方顺利完成了密钥分配以后，通信双方将共享的信息密钥作为会话密钥，选择适当的数据加密算法对传输数据进行加密，保证数据在通信传输过程中的安全。如果选用适用于可以加密经典比特的量子加密算法，可以使该方案更加有效、安全，如文献[5]提出了一个密钥可以重复利用的量子分组加密算法，很好地降低了密钥管理的难度。

由于未授权的用户不能共享安全密钥，所有被授权的 ONU 用户将组成一个 VPN 网络，当使用安全有效的算法对传输的明文数据进行加密和解密，不仅可以与 OLT 之间交换数据，而且任意两个 ONU 之间也可以实现安全通信，即可以最终可实现安全、高效的量子 VPN。

3 协议效率及安全性分析

在一些典型的量子密钥分配方案中，都需要一个经典信道用来比较通信双方的测量基，但经典信道不仅会泄漏信息，而且会使得通信效率大大降低。而从实际密钥分发效率来分析，著名的 BB84 协议，B92 协议及 EPR 协议中，假设由于信道不理想而损失的比特为 l，要发送 L 比特的量子密钥，实际的效率为 $\eta_1 = L/2(L+l) < 50\%$。在乒乓协议中，粒子经过了两次传输，可以得到它的传输效率为 $\eta_2 = L/(L+2l)$。在本方案中，由于引入一个新光子，而且采用了确定性测量方式，除去检测信道完善性和认证部分消耗的少量 EPR 对，一个 EPR 对可以产生两比特共享密钥。在忽略某些器件损耗的情况下，传输距离是乒乓协议的两倍，因此实用性更好。以下首先分析 OLT 和 ONUi 之间通信的安全性。

本方案中我们考虑两种针对认证协议的攻击，即模拟欺骗攻击和代替欺骗攻击。假设 ONUi 是假冒的，由于他不知道认证密钥，在第(3)步就会暴露他的身份，因此模拟欺骗攻击不会成功。代替攻击的前提是获取合法通信者的认证密钥。为了获取有关密钥的信息，窃听者 Eve 有两种典型的窃听手段，即截取重发攻击和纠缠攻击策略。当 Eve 采取截取重发攻击时她将得不到最终密钥。Eve 将在第(2)步中截获 t 光子，做测量以后制备一串新的光子发送给 ONUi，但 Eve 的操作将在第(3)步的信道完善性检测中被检测出来，所以聪明的窃听者将会采用纠缠攻击来获取信息。设 Eve 利用辅助态 ε 对 OLT 发送给 ONUi 的光子 t 进行一个幺正纠缠操作 E，然后将 t 光子再发送给 ONUi。这里假设 Eve 是在量子力学规律中具有无限计算能力的窃听者。Eve 的纠缠操作可以描述为

$$
\begin{aligned}
&\left|0_t\varepsilon\right\rangle \to A_\varepsilon\left|0_t\varepsilon_{00}\right\rangle + B_\varepsilon\left|1_t\varepsilon_{01}\right\rangle,\\
&\left|1_t\varepsilon\right\rangle \to B_\varepsilon\left|0_t\varepsilon_{10}\right\rangle + A_\varepsilon\left|1_t\varepsilon_{11}\right\rangle,\\
&\left|\pm_C\varepsilon\right\rangle \to \frac{1}{2}\left|+_C\right\rangle\left[A_\varepsilon\left(\left|\varepsilon_{00}\right\rangle \pm \left|\varepsilon_{11}\right\rangle\right) + B_\varepsilon\left(\left|\varepsilon_{01}\right\rangle \pm \left|\varepsilon_{10}\right\rangle\right)\right]\\
&\quad + \frac{1}{2}\left|-_C\right\rangle\left[A_\varepsilon\left(\left|\varepsilon_{00}\right\rangle \mp \left|\varepsilon_{11}\right\rangle\right) - B_\varepsilon\left(\left|\varepsilon_{01}\right\rangle \mp \left|\varepsilon_{10}\right\rangle\right)\right] \qquad (3)
\end{aligned}
$$

其中 $\left|\varepsilon_{00}\right\rangle, \left|\varepsilon_{01}\right\rangle, \left|\varepsilon_{10}\right\rangle$ 和 $\left|\varepsilon_{11}\right\rangle$ 都是由测量操作 E 唯一决定的辅助量子态，$\left|A_\varepsilon\right|^2 + \left|B_\varepsilon\right|^2 = 1$，不失一般性，假设 $\left\langle\varepsilon_{00}\middle|\varepsilon_{01}\right\rangle = \left\langle\varepsilon_{00}\middle|\varepsilon_{10}\right\rangle = \left\langle\varepsilon_{01}\middle|\varepsilon_{11}\right\rangle = \left\langle\varepsilon_{10}\middle|\varepsilon_{11}\right\rangle = 0$，$\left\langle\varepsilon_{00}\middle|\varepsilon_{11}\right\rangle = \cos\theta$，$\left\langle\varepsilon_{01}\middle|\varepsilon_{10}\right\rangle = \cos\varphi$，其中 $\theta, \varphi \in [0, \pi/2]$。由于 Eve 的攻击，ONU$i$ 将会收到经过 Eve 扰动的光子。经过第(2)步的纠缠操作，Eve 在第(3)

步的信道完善性检测和第(4)步的身份认证中造成的误码率分别为

$$d_{ht}^{k}=d_{ht}^{r}=\frac{1}{4}\left[\left|A_{\varepsilon}\right|^{2}(1-\cos\theta)+\left|B_{\varepsilon}\right|^{2}(3-\cos\varphi)\right] \quad (4)$$

同样，可计算得到 Eve 在第(5)步中造成的误码率为 $d_{ht}^{m}=0.5$。考虑 Eve 的最佳攻击策略，Eve 在这次通信中被检测出的概率可表示为

$$P_{d}=1-(1-d_{ht}^{k})(1-d_{ht}^{r})(1-d_{ht}^{m}) \quad (5)$$

当取 $\left|A_{\varepsilon}\right|^{2}=1,\ \left|B_{\varepsilon}\right|^{2}=0$，Eve 被检测出的概率最小为 $d=(P_{d})_{\min}=1-(3+\cos\theta)^{2}/32$，因为 Eve 会尽力减少 P_{d} 的值。此时当 $\cos\theta=0$ 时，Eve 可以获取最大互信息量，d 取最大值为 $d=23/32$。根据 Shannon 定理，OLT 和 ONUi 之间的互信息表示为 $I_{AB}=h(A)+h(B)-h(A,B)$，其中 $h(A),h(B)$ 和 $h(A,B)$ 分别表示 OLT 和 ONUi 的 Shannon 熵以及他们之间的联合熵(以下将 OLT 方编码共享的密钥表示为 A，ONUi 解码共享的密钥表示为 B，Eve 窃听得的密钥为 E)。展开得到

$$I_{AB}=2-h[(1-\cos\theta)/2] \quad (6)$$

为了获取信息，Eve 将会测量她的辅助量子态来获取有关密钥信息。考虑 $\left|A_{\varepsilon}\right|^{2}=1,\ \left|B_{\varepsilon}\right|^{2}=0$，通过计算可得 ONU$i$ 和 Eve 之间的互信息量 I_{BE} 为

$$\begin{aligned}I_{BE}&=2+\sum_{B}\sum_{E}P(B)P(E\mid B)\log_{2}P(E\mid B)\\&=2+\log_{2}\frac{1}{2}=1\end{aligned} \quad (7)$$

只有 OLT 和 ONUi 之间的互信息量 I_{AB} 大于 ONUi 和 Eve 之间的互信息量 I_{BE}，才能保证通信的安全。图 2 为互信息量 I_{AB} 对检测概率的分布曲线，当检测概率取最大值 23/32 时，有 $\min(I_{AB})=1$，即在 Eve 的检测范围 $[0.5,23/32]$ 内都有 $I_{BE}<I_{AB}$。因此本方案中，Eve 针对本协议的代替攻击也不能成功。

当 ONU 用户间进行密钥分配时，Eve 通过纠缠窃听方式同样不能获得任何有关密钥的信息，而在 ONU 与 OLT 进行认证密钥更新时，由于新认证密钥经过了旧认证密钥的加密(模二加)，Eve 由于不知道旧认证密钥则她最终还是不能获取有关密钥的信息。以上认证部分假设 OLT 为可信的，而当他是不诚实的(这里只考虑 OLT 的个人攻击)，即他想窃听用户间的通信也同样不会成功，因为他在获取 ONU 用户间的共享密钥时一定会被发现。因此，ONU 用户间的密钥分发协议也是安全的。

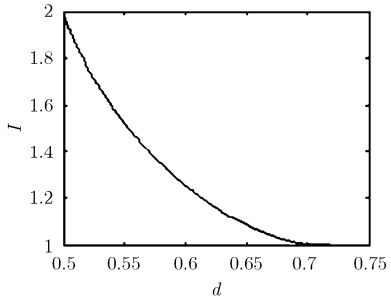

图 2 互信息量对检测概率的函数分布

4　实验方案设计

该方案是基于现有的 PON 网络架构设计的，而其中的量子密钥分发协议可以通过实验实现。基于文献[6]提出的一对一的发送端和接收端的量子密钥实验方案，提出一个在 PON 网络中实现虚拟专用网的实验方案，如图 3 所示。本方案将 OLT 和 ONU 的发送器和接收器分离，并将两者分别用一个光环行器相连接，实现收发自动转换。OLT 和 ONU 都含有 EPR 纠缠光子源，并能进行发送和检测功能，即它们由发送器和接收器两部分组成，图中 Laser 表示超短脉冲激光器，Pump interference 表示光学 Michelson 干涉仪，LBO 为非线性晶体，SF 为单模光纤，WDM 为波分复用器，U 为 I 或 X 幺正操作门，BS 为分束器，$D1$–$D3$ 为雪崩二极管，Delay loop 为光延迟线。

例如，当 OLT 向 ONU2 发起通信时，OLT 发送器关闭反射镜 0、2、3，打开反射镜 1，利用从激光器发出的超短脉冲($\Delta t=150$ fs, $\lambda=710$ nm, $f_{\mathrm{rep}}=75$ MHz)产生 Bell 态 $\left|\varphi^{+}\right\rangle$。首先对 ONU2 进行身份认证，具体方法是让所产生的超短激光脉冲进入一个光学 Michelson 干涉仪(光程时间差 $\Delta T=1.2$ ns)，然后通过一个线性晶体(LBO)，产生两个波长不同的量子光信号，分别为 1330 nm 和 1550 nm。这对纠缠的量子光信号被耦合到光纤中。通过波分复用器将两个量子信号分离，其中波长为 1330 nm 的光信号作为 h 光子留在 OLT 端，而把 1550 nm 的光信号作为 t 光子通过光环行器 $C0$ 通过反射镜 0 到达光环行器 C，经过反射镜 1 的反射后通过反射镜 2 送达 ONU2 的光环行器 $C2$，最终送达 ONU2 的接收器。ONU2 直接对接收到的 t 光子按照共享密钥选择测量基进行测量。

通过认证以后，进行密钥分发操作。当 t 光子到达 ONU2 的接收器端时，在 ONU2 的接收器端，按照 OLT 发送器相似的方法，产生一个波长为 1550 nm 的信号，将此信号作为 m 光子，它的初始状态 $|0\rangle$ 可以通过调节 Michelson 干涉仪的相对相位来调整。然后将 m 光子和经过逻辑门 U (I 或 X)的 t 光子信号通过一个分束器(BS)完成量子受控非操作。最后采用雪崩光电二极管($D1$–$D3$)测量所有光信号，得

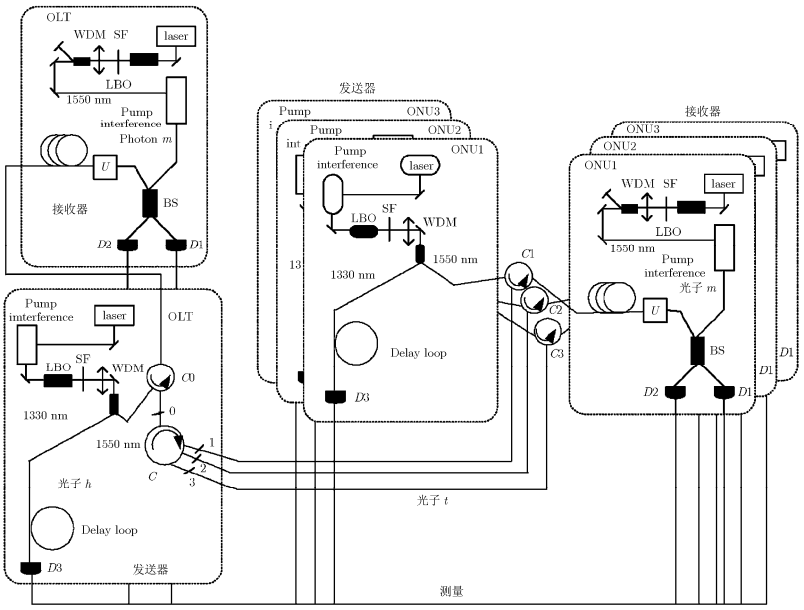

图 3 基于直接安全通信的 QKD 实现 PON 网络中的量子 VPN

到结果。当 ONU2 主动向 OLT 发起通信时，OLT 将反射镜 0、1、2 关闭，打开反射镜 3，ONU2 发送器发出的光子 t 经过 ONU2 光环行器 $C2$ 到达 OLT 选路光环行器 C，通过反射镜 2 再经反射镜 3 的反射到达 OLT 连接收发器的光环行器 $C0$，最后送达 OLT 的接收器，其他操作类似。

同样，如果 ONUi 对 ONUj 进行通信时，OLT 先对双方进行认证，通过认证则继续下面的操作。OLT 打开反射镜 0，ONUi 的发送器产生 h、t 纠缠光子对，先通过 OLT 中的选路光环行器 C 进行选路，到达 ONUj 方的连接收发器的光环行器 Cj，最后将发送的光子 t 送达 ONUj 的接收器，经过逻辑门 U 和受控非操作，最后通过检测，实现他们内部的密钥分配。

5 结论

本文提出了一个基于 PON 网络的量子 VPN 方案。首先设计了一个利用环行器和反射镜实现自动选路的 PON 网络模型，基于该模型设计了一个具有身份认证功能的高效量子密钥分配协议，该协议不仅满足 PON 网络中 OLT 对 ONU 的认证，而且可以保证 OLT 和 ONU 间及 ONU 用户间的安全量子密钥分配。由于避免了由不同的测量基引发的错误比特，从而显著地提高了方案的效率。在协议的安全性分析中，不仅证明了协议可以抵抗假冒欺骗攻击，而且可以抵抗代替欺骗攻击，证明了该协议的绝对安全性。最后提出了一个可行的实验实现方案。将共享密钥作为通信双方的会话密钥，对内部传输数据进行加解密，最终可实现安全量子 VPN。

参 考 文 献

[1] Chae C J, Lee S J, and Kim G Y, *et al*.. A PON system suitable for internetworking optical network units using a fiber bragg grating on feeder fiber [J]. *IEEE Photonics Technology Letters*, 1999, 11(12): 1686–1688.

[2] Sun X F, Chan C K, and Chen L K. A survivable WDM-PON architecture with centralized alternate-path protection switching for traffic restoration [J]. *IEEE Photonics Technology Letters*, 2006, 18(4): 631–633.

[3] Su Y K, Tian X Q, and Hu W S, *et al*.. Optical VPN in PON using TDM-FDM signal format[C]. Proceedings of Optical Fiber Communication Conference, Anehaim, CA, Mar. 2006, OTuJ5.

[4] Meng Y, Jiang T, and Xiao D. Analysis and solutions of security issue in Ethernet PON[C]. Proceedings of The International Society for Optical Engineering, Bellingham, WA, 2005, 5626(1): 391–393.

[5] Zhou N R, Zeng G H, and Nie Y Y, *et al*.. A novel quantum block encryption algorithm based on quantum computation [J]. *Physica A*, 2006, 362(2): 305–313.

[6] 曾贵华. 量子密码学[M]. 北京: 科学出版社, 2006: 99–100. Zeng G H. Quantum Cryptography [M]. Beijing: Science Press, 2006: 99–100.

黄 鹏： 男，1985 年生，硕士生，研究方向为量子保密通信.

周南润： 男，1976 年生，博士，副教授，主要研究方向为通信与信息安全.

刘 晔： 女，1957 年生，教授，副院长/系主任，主要研究方向为通信安全.