OFDM-PON 系统中基于信道相位信息的动态加密方案

李春华[1,2,3]，吴雅婷[1,2,3]*，余衍[1,2,3]，张倩武[1,2,3]，孙彦赞[1,2,3]，王涛[1,2,3]

[1]上海大学特种光纤与光接入网重点实验室，上海 200444；

[2]上海先进通信与数据科学研究院，上海 200444；

[3]特种光纤与先进通信国际合作联合实验室，上海 200444

摘要 针对正交频分复用无源光网络(OFDM-PON)中静态密钥产生的风险，提出一种以信道相位信息作为动态密钥的物理层混沌加密方案。通信双方在相干时间内估计上下行信道相位，得到混沌密钥初值；利用一维混沌系统生成的混沌密钥流对下行数据进行异或(XOR)加密和解密。该方案所得到的动态密钥随着时间的改变而不断更新，因此物理层的安全性能得到提升。实验结果表明，速率为 3.625 Gb/s 的 16QAM 的光 OFDM 信号经长度为 25 km 标准单模光纤(SSMF)传输后，通信双方的密钥具有良好的一致性，密钥空间达到 10^{15}，系统传输的安全性得到有效增强，可成功阻止非法用户对传输数据的窃听。

关键词 光通信；正交频分复用无源光网络；信道；动态密钥；加密

中图分类号 TN929.11 **文献标志码** A **doi**：10.3788/AOS202040.1006004

Dynamic Encryption Scheme Based on Channel Phase Information in OFDM-PON System

Li Chunhua[1,2,3], Wu Yating[1,2,3]*, Yu Yan[1,2,3], Zhang Qianwu[1,2,3], Sun Yanzan[1,2,3], Wang Tao[1,2,3]

[1]*Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Shanghai University, Shanghai* 200444, *China*;

[2]*Shanghai Institute for Advanced Communication & Data Science, Shanghai* 200444, *China*;

[3]*Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai* 200444, *China*

Abstract Aiming at the risks arising from the static keys in an orthogonal frequency division multiplexing passive optical network (OFDM-PON), this study proposes a physical-layer chaotic encryption scheme using channel phase information as dynamic keys. In the coherence time, the initial values of chaotic keys can be extracted from the uplink and downlink channel phases, which are estimated using communication sides. The downlink data is encrypted and decoded by applying XOR operations with the chaotic key stream generated by a one-dimensional chaotic system. The dynamic key obtained using the proposed scheme can be continuously updated with the change of time, further improving the security performance of the physical layer. The experimental results demonstrate that the keys of both communication sides have a good consistency subsequent to the 16-quadrature-amplitude-modulation (16QAM) optical OFDM signal with a speed of 3.625 Gb/s passing through the standard single-mode fiber (SSMF) with a length of 25 km. The key space of the proposed encryption scheme reaches 10^{15}, enhancing the security of system transmission and effectively preventing illegal users from eavesdropping.

Key words optical communications; orthogonal frequency division multiplexing passive optical network; channel; dynamic key; encryption

OCIS codes 060.4510; 060.4785; 070.4340

收稿日期：2020-01-07；**修回日期**：2020-02-09；**录用日期**：2020-02-27

基金项目：国家自然科学基金(61420106011,61601279,61601277,61635006,61671011,61501289)、上海市科学发展基金(17010500400,16511104100)

* **E-mail**：ytwu@shu.edu.cn

1　引　言

随着社会的发展，各类网络应用对带宽的需求越来越大。目前，无源光网络（PON）已成为下一代光接入系统的宽带解决方案[1]。正交频分复用无源光网络（OFDM-PON）技术具有抗光纤色散强、频谱利用率高、成本低及资源分配灵活等优势，因而受到广泛关注[2-3]。然而，PON 系统通常采用广播架构，将下行数据广播到所有光网络单元（ONU）中，这使得下行数据更容易被非法用户窃听[4]。以往的加密研究都集中在介质访问控制（MAC）层，但 MAC 层只加密数据帧，没有保护控制帧和报头，一旦 MAC 层的管理信息被窃取，下行数据就容易被窃听[5]。因此，如果能对数据进行物理层加密，可以更有效地防止非法用户的恶意攻击[6]。

现阶段 OFDM-PON 的物理层加密分为光域加密[7-8]和电域加密[9]。光域加密系统的主要问题是参数空间维数受物理器件限制[10]。电域加密系统利用数字信号处理（DSP），具有灵活性高和性能稳定等优点[11]。常见的基于 DSP 的加密方法包括时域或频域扰乱[12]、分数阶傅里叶变换[13]、星座图符号置乱[14]、DNA（deoxyribonucleic acid）编码[15]及导频替换[16]等。这些方法都使用了混沌序列[17]，该序列由于具有高初值敏感性和遍历性等特点，密钥空间巨大。虽然电域加密系统具有不错的效果，但使用的都是静态密钥，这在一定程度上降低了系统的安全性。针对静态密钥存在的安全性问题，研究者们提出了一种利用上行数据加密下行数据的动态加密方案[18]，但该方案的上行密钥数据是明文传输，这在一定程度上也降低了密钥与系统的安全性。

因此，本文提出一种基于信道相位信息的密钥生成与物理层混沌加密方案。在相干时间内，通信双方通过估计信道相位得到各自密钥，并将其用于下行数据的加密和解密。在密钥生成过程中，需要在获得信道相位值后进行密钥的协调，保证所生成的密钥一致。不同 ONU 具有不同的信道传输函数，因此窃听者很难获取合法 ONU 的下行信道数据，提高了密钥的安全性。同时，信道的时变性保证了合法密钥能不定期地进行更新，实现了密钥的动态生成。所获得的密钥经过一维混沌系统后与下行数据进行异或运算得到加密数据，有效提高了系统的安全传输性能。实验结果表明，所提方案有效提高了密钥的安全性能，实现了物理层的高强度数据加密。

2　动态密钥生成与数据加密

2.1　密钥生成原理

基于信道特征的密钥生成方案包括信道探测、归一化处理、等概量化、纠错编码与校验等过程。光线路终端（OLT）和 ONU 端密钥生成过程如图 1 所示。从图 1(a)可以看出，OLT 接收 ONU 发来的合法信号，在不考虑噪声，也没有信道统计信息的情况下，采用最小二乘（LS）法先进行信道估计，表达式为

$$H = X^{-1}Y, \tag{1}$$

式中：H 表示信道的冲击响应；X 表示发送的频域信号；Y 表示接收的频域信号。

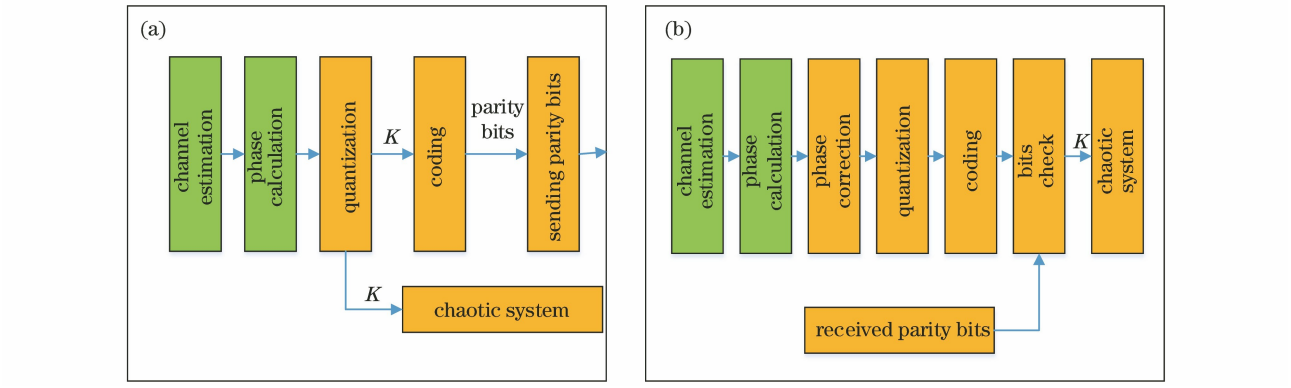

图 1　动态密钥生成框图。(a) OLT 密钥生成；(b) ONU 端密钥生成

Fig. 1　Block diagram of dynamic key generation. (a) Key generation of OLT; (b) key generation of ONU

由(1)式得到一个关于 OFDM 符号的有效数据子载波的信道响应 $H=\{H_1,H_2,\cdots,H_i,\cdots,H_N\}$，其中

$$H_i = |H_i| e^{j\theta_i}, \tag{2}$$

式中：H_i 表示第 i 个有效数据子载波的信道响应；θ_i 表示第 i 个有效数据子载波的信道相位。

根据 OFDM 系统实际的传输效果，选择(2)式中信道特性较好的 k 个数据子载波的信道相位

$\{\theta_1,\theta_2,\cdots,\theta_k\}$并进行量化，得到二进制量化值$\{q_1,q_2,\cdots,q_k\}$，将所得到的量化值依次连接，令加密密钥 K 为 $q_1q_2q_3q_4\cdots q_j\cdots q_k$。为了使 ONU 得到一致的密钥，需对密钥 K 纠错编码，最后将编码后的校验矩阵 $\boldsymbol{M}$ 发送给 ONU，从而完成 OLT 的密钥生成。

在 OLT 进行信道估计的相干时间内，ONU 进行下行信道估计。如图 1(b)所示，ONU 完成信道估计和相位计算后，根据实际的上下行信道响应将所得到的相位值进行修正。选择与上行信道相同的用于密钥生成的数据子载波对下行信道的相应子载波信道相位值进行和 OLT 同样的量化与连接操作，进而得到密钥 $\tilde{K}$。将 $\tilde{K}$ 按 OLT 的排列方式生成待校验的信息矩阵，并与接收到的校验矩阵 $\boldsymbol{M}$ 进行组合，进而对 $\tilde{K}$ 的相关错误位进行纠错，生成与 OLT 一致的密钥 K。

2.2　数据加密

基于生成的动态密钥，采用一维 Logistic 混沌映射来生成密钥流以加密数据[19]。一维混沌映射为

$$x_{n+1}=\mu x_n(1-x_n),\ x_n\in(0,1),\ \mu\in[1,4],\tag{3}$$

式中：μ 表示分岔参数；x_n 表示混沌初值 x_0 经过 n 次迭代后的混沌值。

当 $3.569945<\mu\leqslant4.000000$ 时，整个系统进入混沌状态。混沌状态下，初值 x_0 存在极微小的变化(约 1×10^{-15})，经过迭代后的 x_n 也完全不同，所以本文密钥空间达到了10^{15}。为了获得均匀分布的数字混沌序列，对 x_n 进行二进制处理，过程为

$$b_n=\begin{cases}0, & x_n\leqslant0.5\\ 1, & x_n>0.5\end{cases},\tag{4}$$

式中：b_n 表示混沌值 x_n 的量化二进制值。

令 $\mu=3.95$，迭代次数在 1000 次以上，初始值使用密钥 K。假设 K 的长度为 L，对 q_j 进行十进制运算得到 q_j'，则此时混沌序列的初值 x_0 为

$$x_0=(q_j'+1)/(2^L+1)。\tag{5}$$

通过(3)～(5)式的迭代处理，得到最终二进制混沌密钥流 K_s。最后，数据的加密过程为

$$D_{en}=K_s\oplus D,\tag{6}$$

式中：⊕表示异或运算；D 表示原始下行数据流；D_{en}表示经密钥流加密后的下行数据流。

发送端将得到的加密数据 D_{en}作为系统实际的下行发送数据，并将该数据加载到相应的 OFDM 子载波上，经过光纤系统传输后，接收端通过反向操作，将接收到的二进制数据与密钥流 K_s 进行异或运算，从而得到解密后的下行数据。

3　实验系统与结果分析

3.1　OFDM 实验系统

为验证所提加密算法的安全性能，搭建了一个用于密钥生成及混沌加密的 OFDM-PON 系统，实验结构如图 2 所示。本文采用的是全双工强度调制/直接检测(IM/DD)OFDM-PON 传输系统。整个系统分为两个部分，一是用于密钥生成，二是用于下行数据加密。

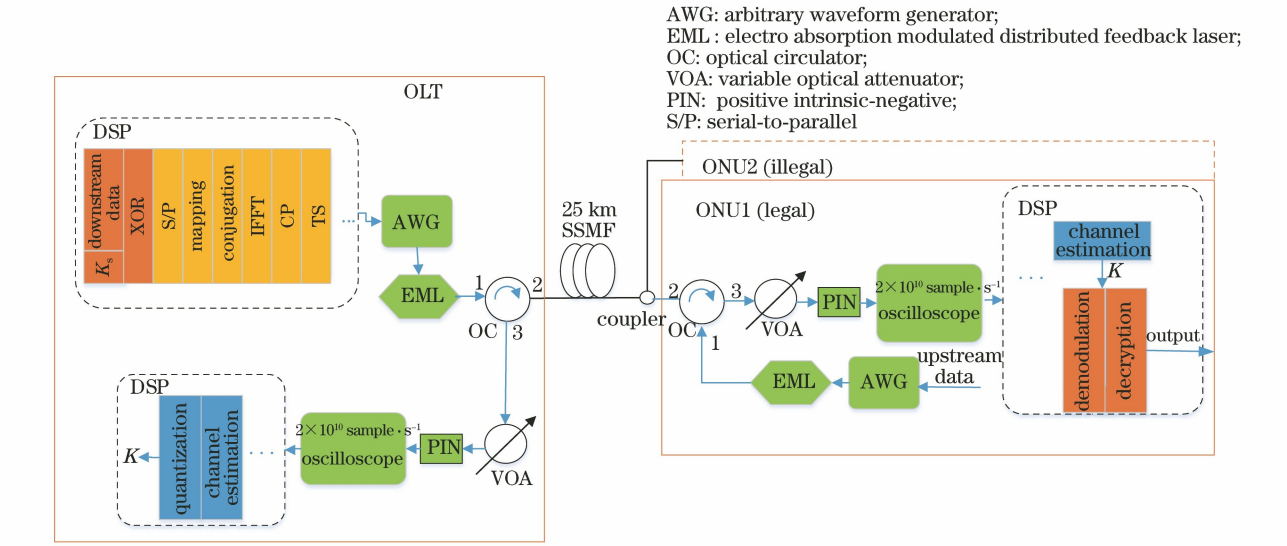

图 2　IM/DD OFDM-PON 加密系统实验图

Fig. 2　Experimental setup of IM/DD OFDM-PON encryption system

在密钥生成阶段，OLT 和 ONU1 分别向对方发送 OFDM 信号以估计信道，其中每个 OFDM 符号由 64 个子载波组成，数据子载波为 56 个，其余为虚拟子载波，用作保护间隔。在进行快速傅里叶逆变换(IFFT)之前，需要对 OFDM 信号进行共轭运算，最终有效数据子载波为 28 个。实验系统每隔 5 min进行一次信道估计以更新密钥。

在发送端，将 MATLAB 生成的数据文件加载到任意波形发生器(AWG)上，以 2×10^9 sample/s 采样速率产生模拟信号，并在波长为 1550 nm 时直接驱动电吸收调制激光器(EML)。随后，电 OFDM 信号被调制成速率为 3.625 Gb/s 的光 OFDM 信号，利用环形器(OC)将信号送入长度为 25 km 的标准单模光纤(SSMF)进行传输。

在接收端，光 OFDM 信号通过一个环形器和可变光衰减器(VOA)后，使用 12 GHz 带宽的光电转换器件(PIN)将光信号转换成电信号，接着将信号送入采样率为 2×10^{10} sample/s 的实时示波器进行采样，并将结果保存以用于后续数据处理。

在接收端的离线处理中，OLT 利用接收的数据文件进行子载波信道估计与相位计算，使用格雷码将信道特性较好的有效数据子载波信道的相位值进行量化并保存在本地以作为加密密钥 K。接着，用(6,3)线性分组码对 $\boldsymbol{K}$ 进行纠错编码，生成校验矩阵 $\boldsymbol{M}$。ONU1 选择与上行信道相同的用于密钥生成的子载波的信道进行相位计算，接着对相位值进行修正，通过前期对上下行信道的测量来确定修正值。然后，使用格雷码对修正后的相位值进行量化，得到密钥 $\tilde{K}$。最后，OLT 将校验矩阵 $\boldsymbol{M}$ 重新发送给 ONU1。ONU1 使用接收到的矩阵 $\boldsymbol{M}$ 对本地密钥 $\tilde{K}$ 进行纠错并将结果保存以作为合法 ONU1 的密钥 K。

在数据加密阶段，首先在 OLT 由 MATLAB 生成伪随机二进制序列(PRBS-15)以作为原始数据流；接着将原始数据流与得到的密钥流 K_s 进行异或运算(XOR)，生成待传输的加密数据 D_{en}；串并转换(S/P)后将数据调制成 16QAM 格式，经共轭运算后将数据加载到 56 个数据子载波上，经过 64 点 IFFT 后为每个 OFDM 符号添加 16 点的循环前缀(CP)和训练序列(TS)；最后将加密的 OFDM 信号加载到 AWG 上并以 2×10^9 sample/s 采样速率驱动发送波长为 1550 nm 的 EML，将调制后的光信号传入环形器和长度为 25 km 的单模光纤。在接收端，OFDM 信号通过耦合器被分为两路，一路是合法的 ONU1，另一路是非法的 ONU2。光 OFDM 信号通过环形器和衰减器后被 12 GHz 带宽的 PIN 转换成电信号。最后，用采样速率为 2×10^{10} sample/s 的实时示波器对接收到的电信号进行采样保存并进行离线处理。

3.2　实验结果与分析

为了验证光纤信道的可用性，测量了不同时间下的子载波信道相位。为了曲线的清晰与美观，同时不失一般性，取每隔 5 个子载波的子载波，研究其相位随时间的变化趋势，结果如图 3 所示。第 1 号和第 32 号子载波是空子载波，不用于信道估计，同时为保证选取的子载波间隔均匀，故从第 7 号子载波开始。实验所得的其他子载波的信道相位变化趋势同图 3 的 5 个子载波基本一致。从图 3 可以看出：由于光纤信道比较稳定，正常情况下相位的变化比较平稳；但 OFDM 信号的第 31 号子载波频率高，而高频受噪声影响较大，估计出的信道不准确，所以其信道变化大且不规律。因此将第 31、32 号子载波作为虚拟子载波。上述结果表明，在生成密钥时，选择特性较好的子载波信道同时控制好量化精度，则利用所得到的量化相位值能分辨出相位的变化，这也为利用信道相位实现动态密钥提供了可能。

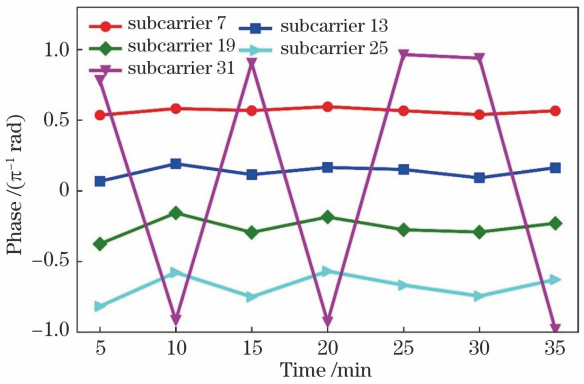

图 3　不同时间下的信道相位

Fig. 3　Channel phases under different time

图 4 显示了两个不同 ONU 的子载波信道相位，为不失一般性，取每隔 10 个子载波的子载波，研究其相位随时间的变化趋势，其余子载波信道变化趋势与图 4 基本一致。从图 4 可以看出，不同时间下的不同 ONU 得到的信道相位值不同。每隔一段时间进行相位测量和估计，由于信道噪声是随机变化的，因此某些时刻的相位可能呈现明显变化。图 4 中前 20 号子载波在 24 min 内的变化趋势一致，之后相位变化趋势出现不同，其他子载波信道

的变化趋势也存在差异。因此，不同信道的相位不同，从而保证了不同 ONU 具有不同的密钥，并且非法 ONU 很难通过信道的有效信息得到合法 ONU 的密钥。当密钥不同时，混沌系统所生成的密钥流也将不同且不可预测，这有效保证了加密系统的安全性。

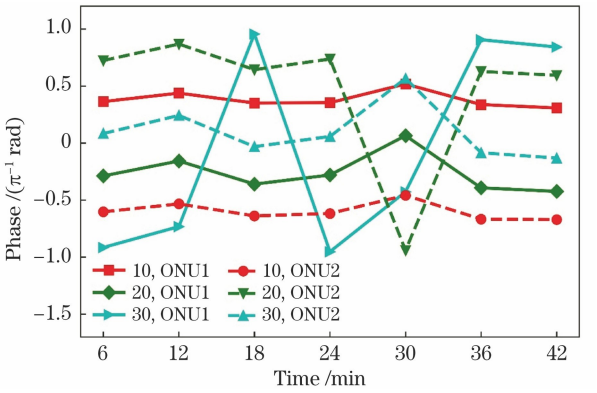

图 4　不同 ONU 的信道相位

Fig. 4　Channel phases of different ONUs

为了更好地利用上下行信道，需要对上下行信道进行测量，所使用的基于上下行信道的相位值如图 5 所示。从图 5(a)可以看出，整个系统的上下行信道在一些子载波上存在相似性。将下行子载波信道的相位值加上修正值，从而缩小上下行信道相位间的差异，其中相位修正值通过对已知的上下行信道相位求平均得到。

图 5(b)为未经修正的用于密钥生成的上下行信道相位值，其变化趋势与图 5(a)得到的上下行信道的趋势相似，这表明下行信道的相位能用修正值进行修正。图 5(c)为经过修正的上下行信道相位值，此时下行信道的大多数子载波信道的相位值接近上行信道的相位值，选择重合度较高的子载波相位值，进行归一化处理以生成密钥。

最后，基于图 2 分析信号经 25 km 光纤传输后的误码性能。图 6 为原始的 OFDM 信号、加密后的 OFDM 信号及非法 ONU 信号通过实验系统传输后，不同接收光功率下的误码率(BER)曲线和星座图。

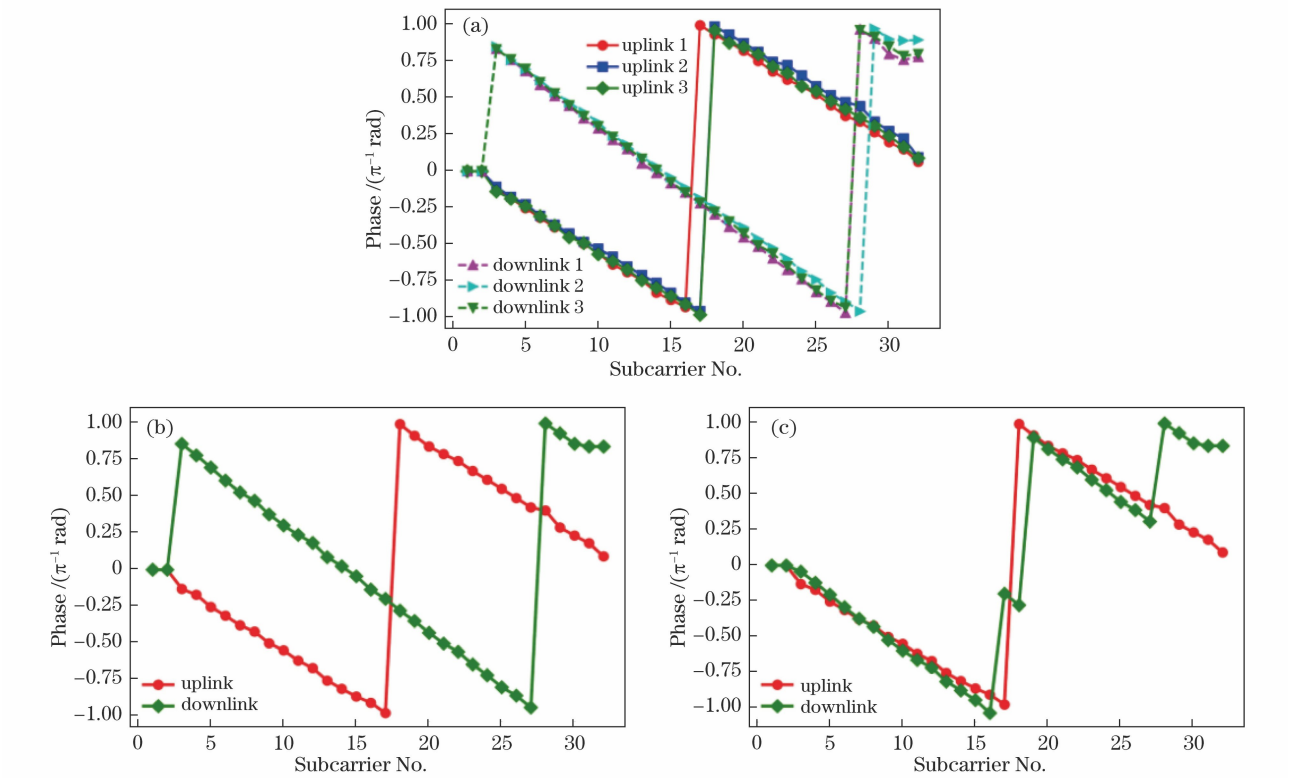

图 5　上行与下行信道相位。(a)多组上下行信道相位；(b) 修正前；(c)修正后

Fig. 5　Uplink channel and downlink channel phases. (a) Multi-group uplink channel and downlink channel phases; (b) before correction; (c) after correction

由图 6 可知，随着接收光功率的增加，整个系统的误码率都在逐渐减小。与原始的 OFDM 信号相比，混沌加密仅对二进制数据流进行了加密，原则上只要收发两端的加密和解密的密钥保持一致，加密与未加密的系统的误码率在性能上就没有区别。实际上，由于收发两端在对相位信息进行估计和量化过程中有可能产生误差，因此加密系统的误码率会略微高于未加密系统。经 25 km 光纤传输后，可以

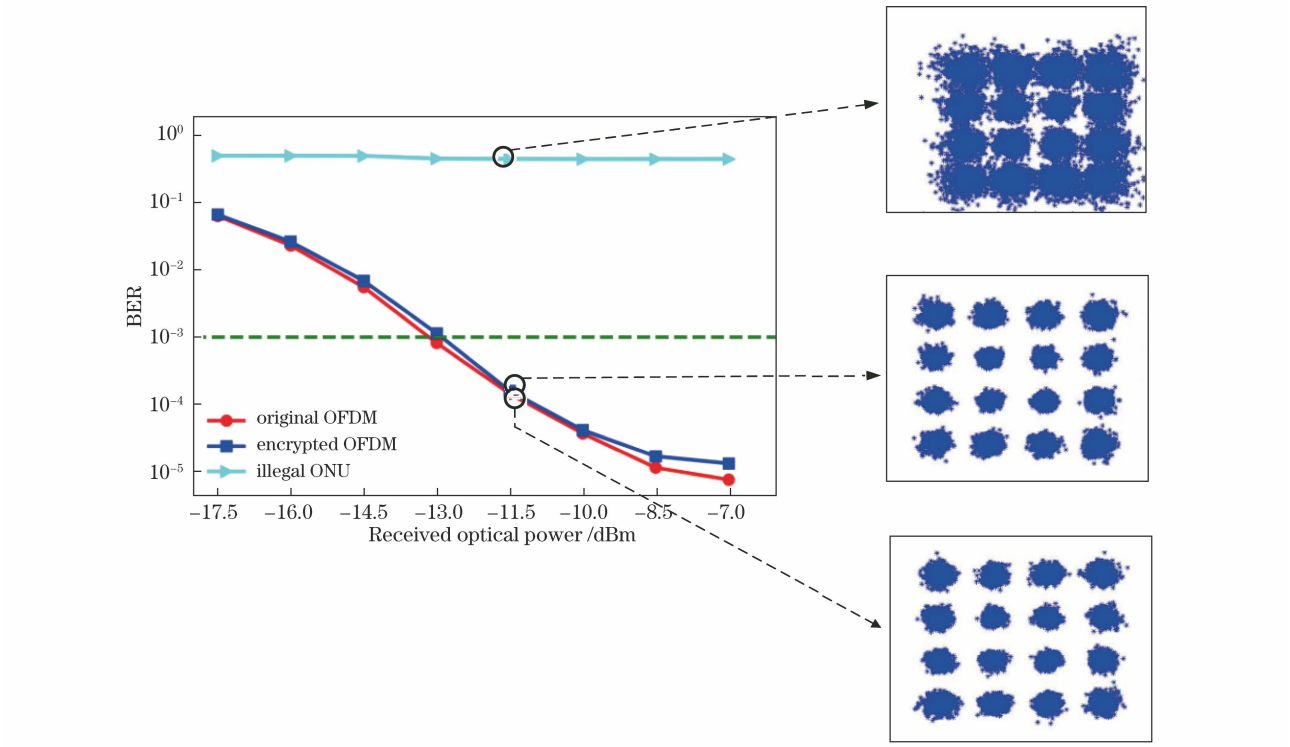

图 6　BER 性能

Fig. 6　BER performance

看到加密后系统的误码率与未加密系统的误码率非常接近，加密后信号的星座图也进一步表明本方案在增强系统安全性的同时并不会降低系统的传输性能。就非法 ONU 而言，每个接收光功率下的误码率几乎都为 0.5，说明非法 ONU 在没有密钥的前提下无法获取正确的传输数据。因此，本实验验证了信道提取的密钥可以被用于 OFDM 信号的物理层加密，经混沌系统加密后，传输系统具有很高的安全性。

4　结　　论

针对密钥的静态问题，提出了基于信道相位信息的动态密钥生成方案，并将该方案用于 OFDM-PON 物理层的混沌加密。为了研究光纤信道信息的可用性，测试了光纤信道随时间的变化和不同信道的信道响应。实验结果表明：光纤信道随时间变化且变化存在一定波动，当量化达到一定精度时，可以捕捉到信道随时间的变化趋势；不同信道的信道响应也存在差异。该方案可以在合法的通信双方间生成一致的密钥，并且该密钥可以利用两者间的信道进行不定期更新，真正实现了密钥的动态生成和保护。因此，所提方案有效地增强了系统传输的安全性，可成功阻止非法用户对传输数据的窃听，具有实用价值。

参　考　文　献

[1] Sotiropoulos N, Koonen A M J, de Waardt H. Next-generation TDM-PON based on multilevel differential modulation[J]. IEEE Photonics Technology Letters, 2013, 25(5): 418-421.

[2] Cvijetic N. OFDM for next-generation optical access networks [J]. Journal of Lightwave Technology, 2012, 30(4): 384-398.

[3] Xiao Y Q, Wang Z Y, Cao J, et al. Time-frequency domain encryption with SLM scheme for physical-layer security in an OFDM-PON system[J]. Journal of Optical Communications and Networking, 2018, 10(1): 46-51.

[4] Han M X, Wu Y T, Zhang Q W, et al. Secure algorithm for suppressing peak-to-average power ratio in OFDM-PON systems[J]. Acta Optica Sinica, 2019, 39(5): 0506004.
韩梦欣, 吴雅婷, 张倩武, 等. OFDM-PON 系统中一种抑制峰均功率比的安全算法[J]. 光学学报, 2019, 39(5): 0506004.

[5] Zhang L J, Xin X J, Liu B, et al. Secure OFDM-PON based on chaos scrambling[J]. IEEE Photonics Technology Letters, 2011, 23(14): 998-1000.

[6] Zhang J Q, Marshall A, Woods R, et al. Design of an OFDM physical layer encryption scheme[J]. IEEE Transactions on Vehicular Technology, 2017, 66(3):

2114-2127.

[7] Etemad S, Agarwal A, Banwell T, et al. An overlay photonic layer security approach scalable to 100 Gb/s [J]. IEEE Communications Magazine, 2008, 46(8): 32-39.

[8] Cheng M F, Deng L, Gao X J, et al. Security-enhanced OFDM-PON using hybrid chaotic system [J]. IEEE Photonics Technology Letters, 2015, 27(3): 326-329.

[9] Liu B, Zhang L J, Xin X J, et al. Piecewise chaotic permutation method for physical layer security in OFDM-PON [J]. IEEE Photonics Technology Letters, 2016, 28(21): 2359-2362.

[10] Cheng M, Deng L, Wang X, et al. Enhanced secure strategy for OFDM-PON system by using hyperchaotic system and fractional Fourier transformation[J]. IEEE Photonics Journal, 2014, 6(6): 1-9.

[11] Zhang W, Zhang C F, Chen C, et al. Experimental demonstration of security-enhanced OFDMA-PON using chaotic constellation transformation and pilot-aided secure key agreement [J]. Journal of Lightwave Technology, 2017, 35(9): 1524-1530.

[12] Zhang L J, Xin X J, Liu B, et al. Physical secure enhancement in optical OFDMA-PON based on two-dimensional scrambling[J]. Optics Express, 2012, 20(26): B32-B37.

[13] Deng L, Cheng M F, Wang X L, et al. Secure OFDM-PON system based on chaos and fractional Fourier transform techniques[J]. Journal of Lightwave Technology, 2014, 32(15): 2629-2635.

[14] Sultan A, Yang X L, Hajomer A A E, et al. Dynamic QAM mapping for physical-layer security using digital chaos[J]. IEEE Access, 2018, 6: 47199-47205.

[15] Zhang C F, Zhang W, Chen C, et al. Physical-enhanced secure strategy for OFDMA-PON using chaos and deoxyribonucleic acid encoding[J]. Journal of Lightwave Technology, 2018, 36(9): 1706-1712.

[16] Chen Q H, Bi M H, Fu X S, et al. Security scheme in IMDD-OFDM-PON system with the chaotic pilot interval and scrambling[J]. Optics Communications, 2018, 407: 285-289.

[17] Hu Z Y, Chan C K. A 7-D hyperchaotic system-based encryption scheme for secure fast-OFDM-PON [J]. Journal of Lightwave Technology, 2018, 36(16): 3373-3381.

[18] Cao P, Hu X F, Wu J Y, et al. Physical layer encryption in OFDM-PON employing time-variable keys from ONUs[J]. IEEE Photonics Journal, 2014, 6(2): 1-6.

[19] Bi M H, Fu X S, Zhou X F, et al. A key space enhanced chaotic encryption scheme for physical layer security in OFDM-PON[J]. IEEE Photonics Journal, 2017, 9(1): 1-10.