第 42 卷 第 14 期/2022 年 7 月/光学学报 研究论文

光学学报

基于双驱马赫-曾德尔调制器的加密调制一体化系统

闫焕友[1]，唐先锋[1*]，朱海龙[1]，王红艳[2]，房博海[1]，申晨雨[1]，刘芝付[1]，詹鹏[3]，张晓光[1]

[1]北京邮电大学信息光子学与光通信国家重点实验室，北京 100876；

[2]国网信息通信产业集团安徽继远软件有限公司，安徽 合肥 230088；

[3]国网湖北省电力有限公司信息通信公司，湖北 武汉 430000

摘要 为提高光通信系统的物理层安全性能，设计并实现了一种基于双驱马赫-曾德尔调制器的加密调制一体化方案，该方案利用双驱马赫-曾德尔调制器中的矢量调制机制对明文和密钥在光域中进行异或加密操作，同时实现了加密和调制的功能复用。阐述了所提方案的基本工作原理和提升加密信号消光比的优化过程，并基于所提方案成功研制了加密调制一体化发射样机。实验结果表明，所提方案可以对传输速度为 32 Gb/s 的信号实现调制和加密，且信号消光比高达 13.2 dB。仿真结果表明，在不同传输距离下，所提方案的接收信号消光比相比普通通断键控(OOK)系统有明显的提升。

关键词 光通信；信息安全传输；加密调制一体化；双驱马赫-曾德尔调制器；异或逻辑门加密；高消光比

中图分类号 TN918.6+1 **文献标志码** A **DOI**：10.3788/AOS202242.1406001

Encryption-Modulation Integrated System Based on Dual-Drive Mach-Zehnder Modulator

Yan Huanyou[1], Tang Xianfeng[1*], Zhu Hailong[1], Wang Hongyan[2], Fang Bohai[1], Shen Chenyu[1], Liu Zhifu[1], Zhan Peng[3], Zhang Xiaoguang[1]

[1]*State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*;

[2]*Anhui Jiyuan Software Co. Ltd., State Grid Information & Telecommunication Group, Hefei* 230088, *Anhui, China*;

[3]*Information and Communication Branch of Hubei Electric Power Company, State Grid, Wuhan* 430000, *Hubei, China*

Abstract To improve the physical layer security of the optical communication system, an encryption-modulation integrated scheme based on the dual-drive Mach-Zehnder modulator (DD-MZM) is proposed. In this scheme, the XOR encryption operation is realized between plaintext and key in the optical domain on the basis of the vector modulation mechanism in the DD-MZM, and the function reuse of encryption and modulation is achieved. The basic working principle of the proposed scheme and the optimization process of improving the extinction ratio of encrypted signals are described, and the prototype of an encryption-modulation integrated transmitter is successfully developed based on this scheme. The experimental results reveal that the modulation and encryption of signals with a transmission speed of 32 Gb/s can be successfully realized by this scheme, and the signal extinction ratio is as high as 13.2 dB. In addition, simulation analysis indicates that compared with the common on-off keying (OOK) system, the proposed system has a better extinction ratio for its received signals.

Key words optical communications; secure transmission of information; encryption-modulation integration; dual-drive Mach-Zehnder modulator; XOR logic gate encryption; high extinction ratio

收稿日期：2021-12-14；**修回日期**：2022-01-04；**录用日期**：2022-01-20

基金项目：国家自然科学基金(62001040)、国家电网有限公司总部科技项目资助(5700-202119188A-0-0-00)、北京邮电大学信息光子学与光通信国家重点实验室基金资助(IPOC2021ZT12)、北京邮电大学大学生研究创新基金

通信作者：*tangxianfengbupt@bupt.edu.cn

1 引　　言

随着信息社会的发展，通信网络数据流量呈现爆炸式增长。信息安全传输关系到个人隐私、商业机密和国家安全等，日渐成为一个热点研究方向。各种通信加密技术层出不穷[1-4]，传统的加密技术大多数是基于密码学原理在通信网络上层进行加密。然而，随着超级计算机计算能力的不断提升，这些以高复杂度、大运算量为基础的加密技术受到越来越严重的安全威胁，其加密机制极易被暴力破解[5-7]。物理层加密技术具有协议透明、全数据加密、时延低和速率高等突出优势，逐渐发展成未来十分具有应用前景的加密传输方式[8-9]。

现今，在开放式系统互联通信参考模型(OSI)中，物理层的有线通信媒介以光纤为主，在物理层对光纤链路信号进行加密能够为整个通信网络提供全方位、更高效的安全服务，因此研究光物理层安全具有十分重要的意义[10-12]。同时，相比电域，在光域中对信号进行加密的方法克服了电功率因素的限制，且具备大带宽、高速率和抗电磁干扰等优点[13]。传统光域加密方案大多基于高非线性光纤或者半导体光放大器，需要在原有的系统上引入额外的加密处理模块，使得系统的复杂度和成本增加，并且对系统性能也产生了一定的影响[14]。本文基于一次一密的加密思想，设计了一种基于双驱马赫-曾德尔的加密调制一体化方案。该方案利用双驱马赫-曾德尔调制器(DD-MZM)中的矢量调制机制对明文和密钥在光域中进行异或加密操作，具有良好的传输性能。在大部分专网系统中，包括电力通信系统，通信以强度调制为主且传输速率较低，最重要的是安全性问题，这些专网系统直接关系民生和经济发展。本文针对强度调制信号设计方案实现了加密和调制的功能复用，结构简单，性能优越，并且研制出了实际样机。经实验测试和仿真分析发现，与普通通断键控(OOK)系统相比：在同等系统参数下，该加密调制一体化系统具有更优良的传输性能；在不同传输距离下，该系统的消光比(ER)均明显提升。

2 基本原理

2.1 系统原理

如图 1 所示，典型的光安全通信系统一般包括两条传输信道，其中：一条信道是密钥协商信道，即秘密信道；另一条信道是加密信息传输信道，即密文信道。密钥协商信道可以采用量子密钥分发系统或其他密钥分发方案实现密钥的协商[15-17]，在系统的收发两端协商生成密钥池，并且实现密钥的同步。本文主要对加密信息传输信道进行研究，设计利用密钥在发送端对信号进行加密的实现方案。提出了一种基于 DD-MZM 的光异或逻辑门加密方案，能够在光域对明文序列和密钥进行异或加密运算，同时完成了信号的电光调制，进而实现了加密和调制功能复用的一体化系统。

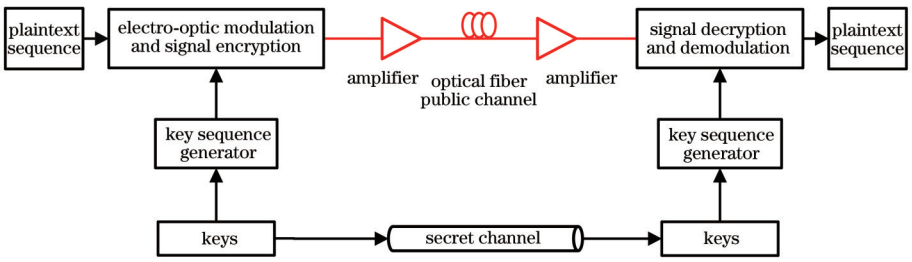

图 1　基于 DD-MZM 的光异或逻辑门的加密调制一体化通信系统框图

Fig. 1　Block diagram of encryption-modulation integrated optical communication system based on optical XOR logic gate using DD-MZM

在图 1 所示的框图中，基于光域异或加密调制一体化方案，系统在对明文序列进行电光调制的同时，使用密钥序列产生器产生伪随机二进制序列与明文序列进行异或逻辑运算，实现对原始信息的加密，使得信息在公共信道中以密文的方式进行传输，进而提高了整个系统的安全性。密文信息在经过光纤链路传输之后，在接收端可以利用对称的异或解密操作得到原始的明文序列。

2.2 加密调制工作原理

所提的光域异或逻辑方案主要是基于光信号的干涉原理，对明文信号与密钥序列进行异或逻辑运算，得到密文信号。如图 2 所示，该系统由一个连续波激光器和一个 DD-MZM 组成。DD-MZM 由两个平行相位调制器组成，每个相位调制器由单独的直流偏置和加载到电极上的射频信号进行驱动，可以实现对光学相位的精确控制。所提方案将明文信号和密钥序列分别加载在上下两个支路中，通过设置偏置电压和信号电压实现对两路光载波的相位调制，利用输出耦合器对两路光信号进行矢量叠加，进而得到具有异或逻辑特性的光信号输出。

DD-MZM 上下两臂相位调制器的输出可表示为

$$E_1(t)=\frac{\sqrt{2}}{2}E_{\mathrm{in}}(t)\mathrm{e}^{\frac{\pi\left[V_{\mathrm{RF1}}(t)+V_{\mathrm{bias1}}\right]}{V_\pi}},\tag{1}$$

$$E_2(t)=\frac{\sqrt{2}}{2}E_{\mathrm{in}}(t)\mathrm{e}^{\frac{\pi\left[V_{\mathrm{RF2}}(t)+V_{\mathrm{bias2}}\right]}{V_\pi}},\tag{2}$$

式中：$E_{\mathrm{in}}(t)$为连续波激光器发射光的输出电场；$V_{\mathrm{RF1}}(t)$和$V_{\mathrm{RF2}}(t)$为两路射频信号电压值；V_{bias1}和V_{bias2}为两路偏置电压值。改变式(1)和式(2)中的偏置电压值(V_{bias1}和V_{bias2})和射频信号电压值[$V_{\mathrm{RF1}}(t)$和$V_{\mathrm{RF2}}(t)$]就可以改变上下两臂光信号的相位。

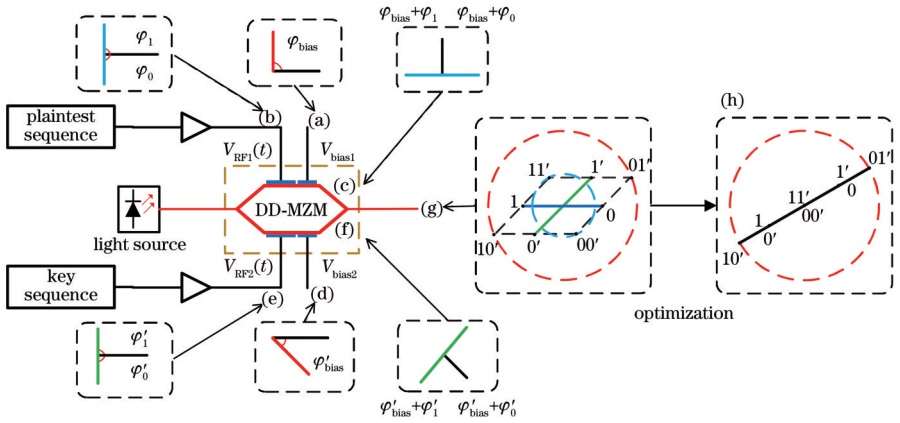

图 2　加密调制一体化系统的实现原理图。(a)上臂相位偏移量;(b)上臂中的原始信号相位;(c)上臂中原始信号经过偏置之后的相位;(d)下臂相位偏移量;(e)下臂中的原始信号相位;(f)下臂中原始信号经过偏置之后的相位;(g)两臂光信号进行矢量叠加的结果;(h)优化后两臂光信号进行矢量叠加的结果

Fig. 2　Implementation schematic diagram of encryption-modulation integrated system. (a) Phase offset of upper arm; (b) phase of original signal in upper arm; (c) phase of original signal in upper arm after offset; (d) phase offset of lower arm; (e) phase of original signal in lower arm; (f) phase of original signal in lower arm after offset; (g) result of vector superposition of optical signals of two arms; (h) result of vector superposition of optical signals of two arms after optimization

基于 DD-MZM 异或逻辑门实现加密的过程可以用图 2(a)～(g)所示的星座图演变来描述。假设直流偏置电压和射频信号电压在 DD-MZM 的两臂上产生的光信号的相位满足

$$\begin{cases}\left(\varphi_0,\varphi_1\right)=\left(-\dfrac{\pi}{2},\dfrac{\pi}{2}\right)\\ \varphi_{\mathrm{bias}}=\dfrac{\pi}{2}\end{cases},\tag{3}$$

$$\begin{cases}\left(\varphi_0',\varphi_1'\right)=\left(-\dfrac{\pi}{2},\dfrac{\pi}{2}\right)\\ \varphi_{\mathrm{bias}}'=-\dfrac{\pi}{4}\end{cases},\tag{4}$$

式中:$\left(\varphi_0,\varphi_1\right)$和$\left(\varphi_0',\varphi_1'\right)$分别是由上下两路输入的 0、1 信号产生的原始相位;φ_{bias}和φ_{bias}'分别是由两路偏置电压引起的相位偏移量。图 2(a)～(c)和图 2(d)～(f)所对应的星座图分别代表上下两臂的相位偏移量、原始信号相位和原始信号经过偏置之后的相位。图 2(g)为两臂的光信号进行矢量叠加的星座图,其中 1、0、1′、0′表示上下两臂原始信号经过相位偏置后的星座点,这 4 个点强度相同,但相位不同。两路信号进行矢量叠加以后:(0,1)和(1,0)两种输入状态分布在一个半径较大的圆上,对应输出光信号的逻辑运算结果为 1;(0,0)和(1,1)两种输入状态分布在一个半径较小的圆上,对应输出光信号的逻辑运算结果为 0。因此,最终可实现光的异或逻辑门加密。

在所设计的结构下,有多种实现异或逻辑的配置,在硬件结构不变的情况下,可以通过调节调制器上的偏置电压和驱动电压对异或逻辑性能进行优化配置。通过调整直流偏置电压和射频信号电压可以改变图 2(a)、(b)、(d)、(e)中的相位,此时图 2(g)中的平行四边形也会随之变化,进而改变输出信号的消光比。改变直流偏置电压能够对两路信号相位进行旋转,当两臂光信号的相位正好相反时,异或逻辑的结果能够实现内圆半径为 0,外圆半径加倍,如图 2(h)所示,此时消光比理论值达到无穷大,即此时可以得到加密调制一体化系统的最优配置。此时,两臂信号相位满足

$$\left(\varphi_1,\varphi_0\right)=\left(\varphi_0',\varphi_1'\right),\tag{5}$$

根据式(5)可以推导得到偏置相位的约束方程组,即

$$\begin{cases}\varphi_0+\varphi_{\mathrm{bias}}=\varphi_1'\\ \varphi_1+\varphi_{\mathrm{bias}}=\varphi_0'\\ \varphi_0'+\varphi_{\mathrm{bias}}'=\varphi_1\\ \varphi_1'+\varphi_{\mathrm{bias}}'=\varphi_0\end{cases},\tag{6}$$

进一步化简,可以得到最终的约束公式,即

$$\varphi_{\mathrm{bias}}+\varphi_{\mathrm{bias}}'=0。\tag{7}$$

3　分析与讨论

3.1　实验结果

基于所提设计方案,搭建了如图 3(a)所示的实验系统,并且成功研制了如图 3(b)所示的加密调制一体化发射样机。如图 3(a)所示,实验采用中心波长为 1550 nm,线宽小于 100 kHz 的连续波外腔激光器(ECL)作为光源,激光器的输出功率为 9 dBm,DD-MZM 的调制带宽为 25 GHz,二进制码型发生器(BPG)生成的两路速率为 32 Gb/s 的伪随机二进制序列分别代表明文序列和密钥序列,经过 38 GHz 的电放大器放大后驱动 DD-MZM,调节偏置电压和信号电压使明文序列和密钥序列进行异或逻辑运算后输出密文序列。在输出端使用一个带宽为 80 GHz 的宽带示波器(OSC)检测光信号并记录波形。图 3(c)为明文序列、密钥序列和密文序列的逻辑门的时域波形。图 3(d)为加密信号的眼图,其信号消光比为 13.2 dB。

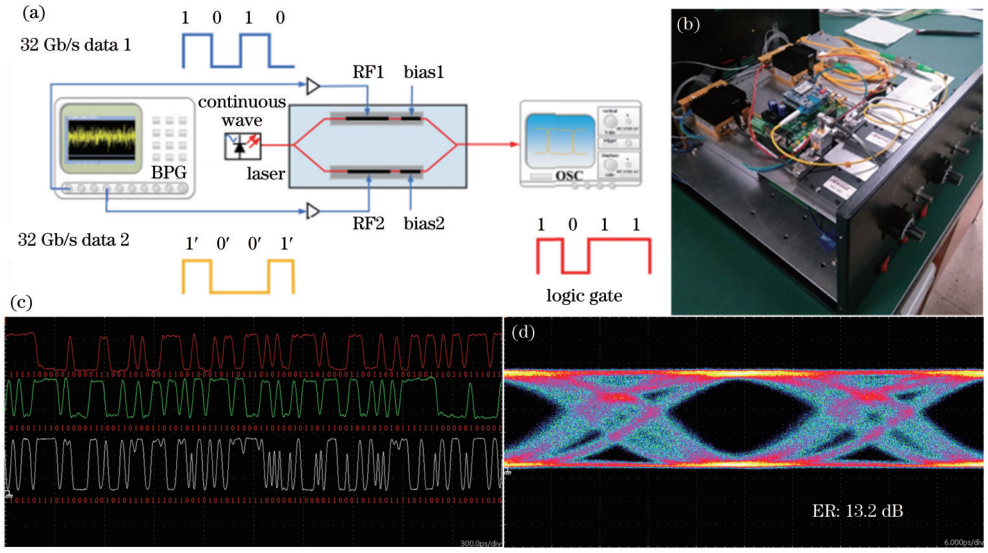

图 3　实验系统和结果。(a)加密调制一体化系统实验框图;(b)加密调制一体化发射样机;(c)信号时域波形图;(d)加密信号眼图

Fig. 3　Experimental setup and results. (a) Experimental block diagram of encryption-modulation integrated system; (b) prototype of encryption-modulation integrated transmitter; (c) temporal waveforms of signals; (d) eye diagram of encrypted signal

通过图 3(c)中的时域波形可以看出,采用所提调制加密一体化方案可以实现对明文序列和密钥序列的异或逻辑运算,即在光域中对信号完成了加密,得到了密文序列。同时,经过调节优化可以看到,加密信号的“0”输出电压接近于 0 V,实验测得消光比高达 13.2 dB,眼图张开度较大,因此该加密调制一体化系统具备较大的噪声容限,可以适应更多的应用场景。眼图中心区域畸变较小,信号最佳采样时刻明显,眼图边沿交会区域宽度较大,过零点畸变比较明显,该现象主要是边沿竞争冒险带来的毛刺信号造成的,但是该毛刺信号不影响数字信号的正确接收和判决。

3.2　传输性能分析

为了分析所提加密调制一体化系统的传输性能,基于所提方案搭建仿真系统,该系统以伪随机序列作为明文序列,调制加密后得到了传输速度为 10 Gb/s 的加密信号。通过对比所提系统和传统的 OOK 信号在不同传输距离下的消光比,得到如图 4 所示的结果。通过对比可以看出,所提加密调制一体化系统在完成加密和调制的同时,采用优化配置使得接收信号消光比也得到了很大的提升。仿真结果表明,经过不同传输距离后,加密信号相比原始 OOK 信号消光比要明显高出 5 dB 以上。因此,基于 DD-MZM 的光域逻辑加密系统不仅提升了光传输系统的安全性,还具有结构简单、性能优良的优点,进而具备了很强的应用潜力。

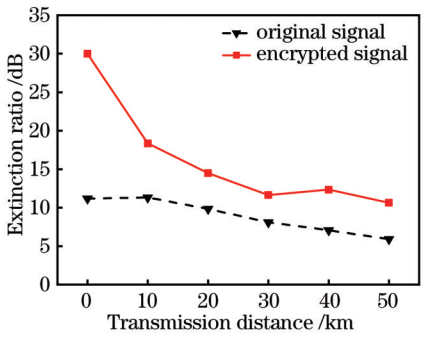

图 4　加密调制一体化系统与传统 OOK 系统在不同距离传输下的信号消光比

Fig. 4　Signal extinction ratios of encryption-modulation integrated system and traditional OOK system under different transmission distances

4　结　　论

针对光通信专网系统的安全问题,设计了一种基于双驱马赫-曾德尔调制器的加密调制一体化发射机,阐述了该方案的工作原理,并进行了设计优化。实验结果表明,按照理论最优配置设置调制器偏置电压和信号电压,所提方案能够有效地对传输速度为 32 Gb/s 的信号进行光域异或逻辑加密,且加密信号消光比高达 13.2 dB。信号眼图张开度较大,说明所提系统具有较强的抗噪声能力。眼图中心采样位置畸变较小,最佳采样时刻明显,过零点畸变较大,这主要是由信号边沿竞争冒险带来的毛刺引起的,但是对数字信号的正确接收和判决影响不大。此外,仿真结果表明,与传统 OOK 信号相比,加密调制一体化信号在经过 0~50 km 的不同传输距离后,接收信号消光比提升了至少 5 dB。所提方案仅需一个双驱马赫-曾德尔调制器即可实现高性能的异或加密过程,同时还可完成信号的调制过程。所提系统结构简单,性能优越,尤其对于专网系统具有很强的应用价值。

参　考　文　献

[1] 杨竞. 同态加密关键技术研究[D]. 成都: 电子科技大学, 2019: 14-16.
Yang J. Research on key technologies of homomorphic encryption[D]. Chengdu: University of Electronic Science

and Technology of China, 2019: 14-16.

[2] 岳荷荷, 王文革, 陈晓蕾, 等. 全双工混沌激光保密通信的仿真和实验实现[J]. 光学学报, 2014, 34(s2): s206010.
Yue H H, Wang W G, Chen X L, et al. Simulation and experimental demonstration of full duplex chaotic optical secure communication[J]. Acta Optica Sinica, 2014, 34(s2): s206010.

[3] 秦怡, 张帅, 巩琼, 等. 基于干涉原理的虚拟光学加密系统[J]. 光学学报, 2012, 32(10): 1007001.
Qin Y, Zhang S, Gong Q, et al. Virtual optical image encryption based on interference[J]. Acta Optica Sinica, 2012, 32(10): 1007001.

[4] 张位. 光接入网络的安全性及其增强技术研究[D]. 成都: 电子科技大学, 2017: 59-69.
Zhang W. Research on security of optical access networks and its improvement techniques[D]. Chengdu: University of Electronic Science and Technology of China, 2017: 59-69.

[5] 李琼, 邓涛, 吴正茂, 等. 安全性增强的双向长距离混沌保密通信[J]. 中国激光, 2018, 45(1): 0106001.
Li Q, Deng T, Wu Z M, et al. Security-enhanced bidirectional long-distance chaos secure communication [J]. Chinese Journal of Lasers, 2018, 45(1): 0106001.

[6] 周玉鑫, 毕美华, 滕旭阳, 等. 基于混沌映射的OFDM-PON物理层加密及系统性能增强算法[J]. 光学学报, 2021, 41(16): 1606002.
Zhou Y X, Bi M H, Teng X Y, et al. Physical layer encryption and system performance enhancement algorithm based on chaos mapping in OFDM-PON[J]. Acta Optica Sinica, 2021, 41(16): 1606002.

[7] 李云坤, 蒲涛, 郑吉林, 等. 基于并联强度调制的量子噪声随机加密实现方案研究[J]. 中国激光, 2021, 48(17): 1706002.
Li Y K, Pu T, Zheng J L, et al. Realization scheme of quantum noise randomized cypher based on parallel intensity modulation[J]. Chinese Journal of Lasers, 2021, 48(17): 1706002.

[8] Fok M P, Wang Z X, Deng Y H, et al. Optical layer security in fiber-optic networks[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 725-736.

[9] 赵文. 基于信道非线性变换的物理层加密方法与技术[D]. 武汉: 华中科技大学, 2019: 25-39.
Zhao W. Physical layer encryption methods and technologies basing on channel state information nonlinear transformation[D]. Wuhan: Huazhong University of Science and Technology, 2019: 25-39.

[10] Zhao J, Tang X F, Ding M, et al. Optical encryption scheme based on spectrum aliasing using a pair of filter banks[C]//14th Pacific Rim Conference on Lasers and Electro-Optics, August 3-5, 2020, Sydney, Australia. Washington, D.C.: OSA, 2020: C4F_3.

[11] Ding M, Tang X F, Zhao J, et al. Experimental demonstration of a 32 Gb/s reconfigurable logic gate using a dual-drive Mach-Zehnder modulator[C]// Conference on Lasers and Electro-Optics Pacific Rim, August 2-6, 2020, Sydney, NSW, Australia. New York: IEEE Press, 2020: 20195081.

[12] Liu L, Tang X F, Jiang X, et al. Physical layer encryption scheme based on cellular automata and DNA encoding by hyper-chaos in a CO-OFDM system[J]. Optics Express, 2021, 29(12): 18976-18987.

[13] Shao W D, Fu Y D, Cheng M F, et al. Chaos synchronization based on hybrid entropy sources and applications to secure communication[J]. IEEE Photonics Technology Letters, 2021, 33(18): 1038-1041.

[14] Agarwal V, Chaurasia V. All optical SOA-MZI-based encryption decryption system using co propagating optical pulses and CW wave at 40 Gb/s[M]//Satapathy C S, Raju K S, Mandal J K, et al. Proceedings of the second international conference on computer and communication technologies. Advances in intelligent systems and computing. New Delhi: Springer, 2015, 381: 201-208.

[15] Zhang L M, Hu W S, Yang X L. Gb/s secure key distribution based on synchronization of polarization states [C]//Optical Fiber Communication Conference, June 6-11, 2021, Washington, D. C., USA. Washington, D. C.: OSA, 2021: Tu1l.3.

[16] 阎金, 王晓凯, 郭大波, 等. 量子高斯密钥分发中后处理的安全性分析[J]. 光学学报, 2016, 36(3): 0327003.
Yan J, Wang X K, Guo D B, et al. Security analysis of post-processing in quantum Gaussian key distributed[J]. Acta Optica Sinica, 2016, 36(3): 0327003.

[17] Hajomer A A E, Zhang L M, Yang X L, et al. 284.8-Mb/s physical-layer cryptographic key generation and distribution in fiber networks[J]. Journal of Lightwave Technology, 2021, 39(6): 1595-1601.