基于光编/解码技术的抗截获通信系统研究

谭业腾, 蒲涛*, 郑吉林, 周华, 苏国瑞
陆军工程大学通信工程学院, 江苏 南京 210007

摘要 为了增强光纤通信系统的物理层安全性,提出了一种基于光编/解码技术的新型抗截获通信系统。由于传统地址码的码字容量都相对较小,合法用户使用的地址码容易受到窃听者的强力搜索攻击。一旦用户地址码被获得,光纤信道中传输的所有用户信息将可被窃听者窃取。为了解决这个问题,构造了一种大容量的二维跳频/扩时地址码,并描述了可重构编/解码器的实现方法;设计了一种新型的抗截获通信系统方案,建立了窃听信道模型;最后,利用 VPI transmission Maker Optical Systems 仿真软件,验证了抗截获通信系统的传输性能和安全性能。仿真结果表明,基于光码分多址的编/解码技术,可以实现一种高速率、长距离的抗截获通信系统。

关键词 光通信; 抗截获通信; 光码分多址; 物理层安全性; 光编/解技术
中图分类号 TN911.2; TN918 **文献标志码** A **doi**: 10.3788/AOS202040.0906001

Anti-Interception Communication System Based on an Optical Encoding/Decoding Technology

Tan Yeteng, Pu Tao*, Zheng Jilin, Zhou Hua, Su Guorui
Communications Engineering College, Army Engineering University of PLA, Nanjing, Jiangsu 210007, *China*

Abstract To enhance the physical-layer security of optical fiber communication systems, a novel anti-interception communication system based on an optical encoding/decoding technology is proposed in this study. Owing to the relatively small capacity of the traditional address codes, the address codes used by the legitimate users are vulnerable to the brute-force searching attacks by eavesdroppers. Once the user's address code is obtained, all the information transmitted in the fiber channel will be stolen by the eavesdropper. To address this problem, a new type of 2D-wavelength-hopping/time-spreading (WH/TS) code is first constructed, and the implementation of the reconfigurable encoder/decoder is described. Then, the novel scheme of anti-interception communication system is designed, and a wiretap channel model is established. Finally, the transmission and security performances of the anti-interception communication system are studied using the VPI transmission Maker Optical Systems simulation software. The simulation results show that a high-speed and long-distance anti-interception communication system can be achieved based on the proposed optical code-division multiple-access coding/decoding technology.

Key words optical communications; anti-interception communication; optical code-division multiple-access; physical-layer security; optical encoding/decoding technology
OCIS codes 060.2330; 060.4785; 060.2360; 220.4830

1 引 言

随着信息技术的飞速发展,人类社会的信息化程度不断加深,越来越多的信息承载于光纤通信网络上进行传输。由于光纤窃听技术的逐渐成熟[1-2]以及传统加密技术不断显现的安全威胁[3-4],光纤通信的安全性也越来越引起人们的关注和重视[5-6]。理论上,量子密钥分发(QKD)能够为合法通信的双方提供无条件安全的密钥[7-8],结合一次一密(OTP)加密,可以实现绝对安全的通信。然而,OTP 要求密钥流的长度与数据流一样长,QKD 系统的密钥分发速率(~Mbit/s[9])无法满足动辄 Gbit/s 的高速光纤通信系统的数据加密。但是,QKD 毕竟能够生成无条件安全的密钥流,可为安全通信提供安全性的基础,故解决上述问题的关键是寻找一种更加有效的加密方法。

收稿日期: 2019-11-27; **修回日期**: 2020-01-09; **录用日期**: 2020-01-17
基金项目: 国家自然科学基金(61475193, 61673393, 61504170)、江苏省自然科学基金(BK20140069)
* **E-mail**: nj_putao@163.com

基于物理层编码的安全通信方法已成为当前信息抗截获技术的主要研究方向，其能够将信息在物理层加密防护，以实现信息的抗截获。光码分多址（OCDMA）技术依据预先分配的地址码对传输信号进行扩频编码，经过多用户码分复用后，光信号呈宽谱类噪声特性。只有拥有匹配解码器的接收机才能将特定信号从多用户信号中恢复出来，窃听者通过使用非匹配解码器无法获得原始光信号，只能获得类噪声信号。因此，增强通信安全经常被认为是OCDMA技术的一个重要优势，在抗截获通信领域具有广阔的应用前景。Shake等[10-13]对OCDMA技术的安全性进行了分析，对于单用户的OCDMA来说，无论是开关键控（OOK）调制方式，还是色移键控（CSK）调制方式或差分相移键控（DPSK）调制方式都存在安全风险，窃听者无需获知地址码，仅仅实施能量侦听攻击等手段就能窃取信息。对于多用户OCDMA系统来说，由于各地址码相互之间需要满足正交性要求，故地址码的码字容量都相对较小。例如，对于码长为511位的双极性Gold码，其码字容量为513；对于码重为23、码长为529位的二维PC/PC码来说，其码字容量为506。同时，由于光编/解码器一般是采用相对固定的地址码及其编/解结构，窃听者可以对合法用户的地址码实施暴力搜索攻击，一旦用户地址码被窃听者得到，则光纤信道中传输的所有信息将可被窃听者窃取。为了解决这一问题，合法通信双方可以采用安全增强策略（动态可重构编/解码以及多用户传输等方法）来增加OCDMA系统的安全性[14-18]，而以上文献中地址码的码字容量都相对较小，窃听者可以通过暴力搜索攻击来随机寻找用户使用的地址码，当窃听者得到地址码后，其可以获得码字重构期间内所有用户信息。

本文提出了一种基于OCDMA编/解码技术的新型抗截获通信系统方案，并仿真验证了系统的可靠性和安全性。针对传统地址码的码字容量较小的问题，构造了一种大容量的跳频/扩时（WH/TS）地址码，并提出了动态可重构编/解码器的物理实现方法；详细地描述了抗截获通信系统的具体设计方案及其窃听信道模型；利用VPI transmission Maker Optical Systems（VPI）商用仿真软件，搭建了基于光编/解码技术的抗截获通信系统的仿真系统，并分析了抗截获系统的传输性能和安全性能。

2　抗截获通信系统的设计方案

2.1　具体方案

对于传统的多用户OCDMA系统来说，因为各个用户的地址码之间需要保证较好的互相关特性，故地址码的码字容量须相对较小。本研究提出了一种新型的基于OCDMA编/解码技术的抗截获通信系统方案，如图1所示。该方案中只有主用户（Alice）会发送信息给合法接收者（Bob），而干扰用户仅被用于防止窃听者（Eve）通过能量截获攻击来窃取信息，且主用户和干扰用户彼此之间是相互独立的。因此，主用户的地址码与各个干扰用户的地址码之间必须满足正交性需求，而干扰用户的地址码之间不需要满足正交性需求。

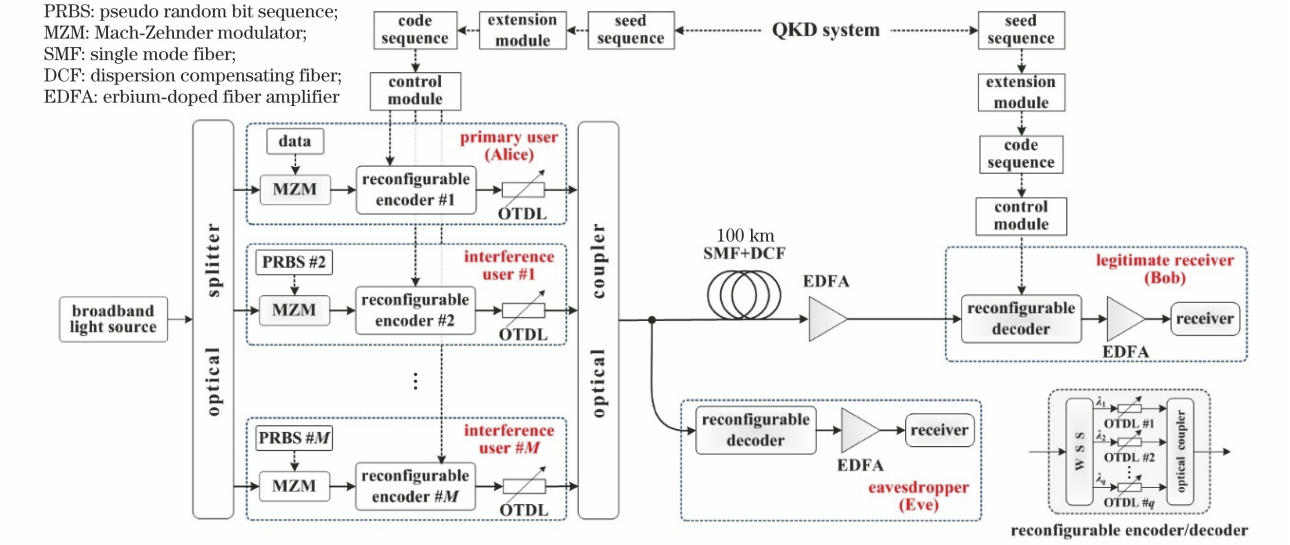

图1　基于OCDMA编/解码技术的抗截获通信系统的示意图

Fig. 1　Diagram of anti-interception communication system based on OCDMA encoding/decoding technology

合法发送方(Alice)与合法接收方(Bob)通过QKD系统共享一个种子序列 K,经过序列扩展模块 ENC(•)后得到一个 WH/TS 序列 $E^{N}_{\mathrm{WH/TS}}$,即 $E^{N}_{\mathrm{WH/TS}}=\mathrm{ENC}(K)$,上标 N 表示序列长度。控制模块根据 WH/TS 序列对主用户(Alice)和所有干扰用户的光编码器进行码字重构,同时,合法接收方(Bob)的解码器也进行相应的码字重构。在发送端,Alice 发送的光信号 S 经过可重构编码器后得到编码信号 S_{D},然后与干扰用户的编码信号 $S_{\mathrm{I}}=\{I_1,I_2,\cdots\}$ 一起被耦合进光纤信道中进行传输;在接收端,合法接收者(Bob)利用匹配的解码器将主用户信号从多用户编码信号中恢复出来。由于地址码之间的互相关特性的影响,部分的干扰用户信号会混入到主用户的解码信号中,并产生多址接入干扰(MAI)。为了防止 Eve 对传输信号实施能量侦听攻击,根据主用户发送的数据比特,适当地选择干扰用户发送的数据比特来使得多用户编码信号的功率始终保持相同,即各个时刻中所有用户发送数据比特"1"的数目保持相同。

另外,抗截获通信系统中还可能存在一个窃听者(Eve)可以窃取光纤信道中传输光信号的情况。由于地址码的码字容量较大,Eve 无法通过暴力搜索攻击来获得主用户的地址码。根据 Kerckhoffs 原则,窃听者(Eve)除了不知道合法用户正在使用的具体码字外,其他系统参数(包括编码类型、码字结构和数据速率等)均已知,也就是说,窃听者 Eve 只能随机地从码字集合中选择解码器的码字。因此,虽然 Eve 能从光纤信道中接收到与 Bob 相同的光信号,但通过非匹配的解码器无法还原出 Alice 发送的光信号,仅能获得类噪声信号。

动态可重构编/解码器主要由波长选择开关(WSS)、光可调延时线(OTDL)以及光耦合器(OC)构成,WSS 的所有输出端口都会连接一个 OTDL,并利用 OC 将所有 OTDL 的输出端耦合到一起。WSS 负责控制不同波长光脉冲对应的输出端口,即不同波长的光脉冲 λ_k 所在的子码字块 s_i,而每个 OTDL 被用于控制相应的子码字块 s_i 中光脉冲 λ_k 所在的时隙位置 τ_j。可重构 WH/TS 编码器($0\lambda_1 00\lambda_2 000000\lambda_3 00\lambda_4 0$)以及可重构 WH/TS 解码器($0\lambda_4 00\lambda_3 000000\lambda_2 00\lambda_1 0$)的编/解码过程如图 2、3 所示。

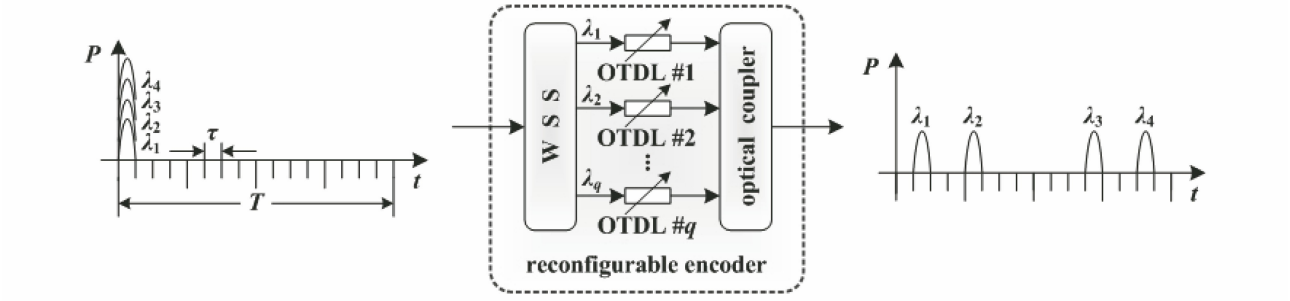

图 2　可重构 WH/TS 编码器($0\lambda_1 00\lambda_2 000000\lambda_3 00\lambda_4 0$)的编码过程

Fig. 2　Encoding process of reconfigurable WH/TS encoder ($0\lambda_1 00\lambda_2 000000\lambda_3 00\lambda_4 0$)

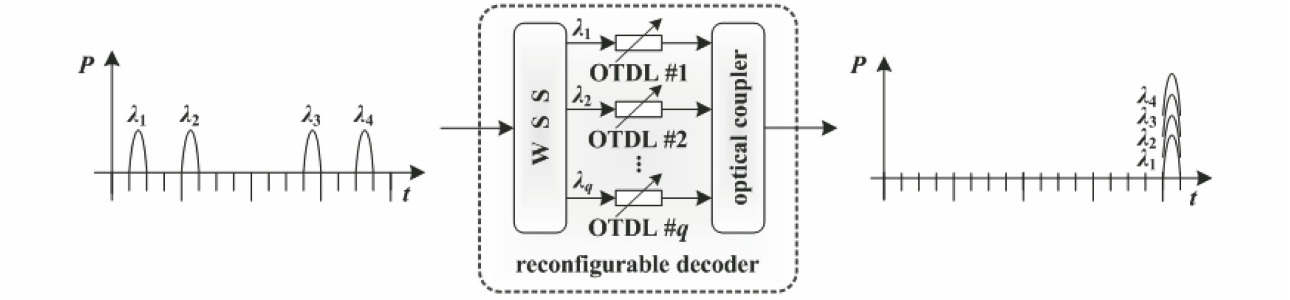

图 3　可重构 WH/TS 解码器($0\lambda_4 00\lambda_3 000000\lambda_2 00\lambda_1 0$)的解码过程

Fig. 3　Decoding process of reconfigurable WH/TS decoder ($0\lambda_4 00\lambda_3 000000\lambda_2 00\lambda_1 0$)

2.2　地址码的构造方法

由于传统地址码的码字容量均相对较小,本文构造了一种新的二维 WH/TS 码,其关键的设计参数包括:波长数 q、码字长度 L,码字容量 C 以及最大互相关峰值 λ_c。具体的构造方法如下:

1) 选择一个波长数 $q\in\{2^p\mid p=1,2,\cdots\}$,则光

脉冲的波长集合可以被表示为 $A^q=\{\lambda_1,\lambda_2,\cdots,\lambda_q\}$。

2）构建一个 WH/TS 序列 $E^{N}_{\mathrm{WH/TS}}$，其包括跳频(WH)序列 $E^{N_W}_{\mathrm{WH}}$ 和扩时(TS)序列 $E^{N_T}_{\mathrm{TS}}$。WH 序列 $E^{N_W}_{\mathrm{WH}}$ 的长度为 $l=\mathrm{lb}\ q$ 比特，其取值范围为 0～$q-1$。TS 序列 $E^{N_T}_{\mathrm{TS}}=\{e_1,e_2,\cdots,e_q\}$ 包括 q 个子序列 e_i，每个子序列 e_i 的长度也为 l 比特，因此，$e_i\in\{0,1,\cdots,q-1\}$ 及 $E^{N_T}_{\mathrm{TS}}$ 的长度为 $N_T=l\times q$。

3）根据 WH/TS 序列 $E^{N}_{\mathrm{WH/TS}}$ 来确定主用户的 WH/TS 码 S^L。WH/TS 码 $S^L=\{s_1,s_2,\cdots,s_q\}$ 包括 q 个子码字块 s_i，每个子码字块 s_i 包含 q 个时隙 τ_j，则 WH/TS 码 S^L 的码字长度为 $L=q^2$。并且，每个子码字块 s_i 有且仅有一个光脉冲 λ_k 位于某一时隙 τ_j，而各子码字块 s_i 对应的脉冲波长按照一定的顺序，即通过对初始顺序 $\lambda_1\lambda_2\cdots\lambda_q$ 执行一个 $E^{N_W}_{\mathrm{WH}}$ 位的循环移位来获取。例如，当波长顺序为 $\lambda_1\lambda_2\cdots\lambda_q$ 时，第一个子码字块中的脉冲波长为 λ_1、第二个子码字块中的脉冲波长为 λ_2，依次类推。对于 $q=4$ 的情况，WH 序列 00、01、10 以及 11 对应的波长顺序分别为 $\lambda_1\lambda_2\lambda_3\lambda_4$、$\lambda_2\lambda_3\lambda_4\lambda_1$、$\lambda_3\lambda_4\lambda_1\lambda_2$ 以及 $\lambda_4\lambda_1\lambda_2\lambda_3$。而各个子码字块 s_i 中光脉冲 λ_k 所在时隙 τ_j 由子序列 e_i 决定，例如，子序列 00、01、10 以及 11 对应的光脉冲时隙位置分别为 λ000、0λ00、00λ0 以及 000λ。因此，WH/TS 码 S^L 的码字容量为 $C=q^{q+1}$，其极大地提高了地址码的容量。例如，当 $q=16$ 时，其码字长度和码字容量分别为 $L=256$ 和 $C=3\times10^{20}$。

4）确定干扰用户的 WH/TS 码。基于主用户的 WH/TS 码 S^L，通过对各子码字块 s_i 中光脉冲 λ_k 所在时隙 τ_j 执行一个不同的循环移位来获得干扰用户的码字。具体的操作如下：对于第 n 个干扰用户来说，对每个光脉冲 λ_k 执行 $(n+k-1)$ 个时隙的循环移位，$k=1,2,\cdots,q$。因此，主用户与干扰用户的码字之间的最大互相关峰值为 $\lambda_c=1$。

5）确定光解码器的 WH/TS 码。光解码器的 WH/TS 码可以通过将主用户的 WH/TS 码 S^L 按照相反的顺序排列而得到。对于 $q=4$ 的情况下，部分 WH/TS 序列及其码字如表 1 所示。

表 1　对于 $q=4$ 的情况下，部分跳频/扩时(WH/TS)序列及码字

Table 1　For the case of $q=4$, part of wavelength-hopping/time-spreading (WH/TS) sequences and codes

WH/TS sequence	WH/TS code of encoder		WH/TS codes of decoder
00/01 10 11 01	Primary user	$0\lambda_1 00\ 00\lambda_2 0\ 000\lambda_3\ 0\lambda_4 00$	$00\lambda_4 0\ \lambda_3 000\ 0\lambda_2 00\ 00\lambda_1 0$
	Interference user ♯1	$00\lambda_1 0\ \lambda_2 000\ 00\lambda_3 0\ 0\lambda_4 00$	
	Interference user ♯2	$000\lambda_1\ 0\lambda_2 00\ 000\lambda_3\ 00\lambda_4 0$	
	Interference user ♯3	$\lambda_1 000\ 0\lambda_2 00\ \lambda_3 000\ 000\lambda_4$	
	Interference user ♯4	$0\lambda_1 00\ 000\lambda_2\ 0\lambda_3 00\ \lambda_4 000$	
01/00 11 01 10	Primary user	$\lambda_2 000\ 000\lambda_3\ 0\lambda_4 00\ 0\lambda_1 00$	$00\lambda_1 0\ 00\lambda_4 0\ \lambda_3 000\ 000\lambda_2$
	Interference user ♯1	$0\lambda_2 00\ 0\lambda_3 00\ \lambda_4 000\ 0\lambda_1 00$	
	Interference user ♯2	$00\lambda_2 0\ 00\lambda_3 0\ 0\lambda_4 00\ 00\lambda_1 0$	
	Interference user ♯3	$000\lambda_2\ 000\lambda_3\ 00\lambda_4 0\ 000\lambda_1$	
	Interference user ♯4	$0\lambda_2 00\ 00\lambda_3 0\ 000\lambda_4\ \lambda_1 000$	
10/10 00 11 11	Primary user	$00\lambda_3 0\ \lambda_4 000\ 000\lambda_1\ 000\lambda_2$	$\lambda_2 000\ \lambda_1 000\ 000\lambda_4\ 0\lambda_3 00$
	Interference user ♯1	$000\lambda_3\ 00\lambda_4 0\ 00\lambda_1 0\ 000\lambda_2$	
	Interference user ♯2	$\lambda_3 000\ 000\lambda_4\ 000\lambda_1\ \lambda_2 000$	
	Interference user ♯3	$0\lambda_3 00\ \lambda_4 000\ \lambda_1 000\ 0\lambda_2 00$	
	Interference user ♯4	$00\lambda_3 0\ 0\lambda_4 00\ 0\lambda_1 00\ 00\lambda_2 0$	
11/11 10 01 10	Primary user	$000\lambda_4\ 00\lambda_1 0\ 0\lambda_2 00\ 00\lambda_3 0$	$0\lambda_3 00\ 00\lambda_2 0\ 0\lambda_1 00\ \lambda_4 000$
	Interference user ♯1	$\lambda_4 000\ \lambda_1 000\ \lambda_2 000\ 00\lambda_3 0$	
	Interference user ♯2	$0\lambda_4 00\ 0\lambda_1 00\ 0\lambda_2 00\ 000\lambda_3$	
	Interference user ♯3	$00\lambda_4 0\ 00\lambda_1 0\ 00\lambda_2 0\ \lambda_3 000$	
	Interference user ♯4	$000\lambda_4\ 000\lambda_1\ 000\lambda_2\ 0\lambda_3 00$	

3　抗截获通信系统性能的仿真分析

利用 VPI 仿真软件，搭建了基于光编/解码技术的抗截获通信系统的仿真系统，如图 4 所示。1)从宽谱光源发出的光载波经过光纤分束器后，各输出端口的光载波分别进入主用户(Alice)和干扰用户的发送端；2)光载波经过调制器进行数据调制后经过光编码器进行物理层编码，最终得到编码信号；3)利用光纤耦合器将各用户的编码信号耦合到光纤链路中进行传输。在接收端，合法接收者(Bob)使用匹配解码器从多个用户的编码信号中恢复出 Alice 的原始光信号，经过光电二极管(PD)、时钟数据恢复(CDR)以及阈值判决后得到原始数据。其中，光编/解码器由波分解复用器(DEMUX)、光纤延时线(OTDL)以及光耦合器(OC)等构成，其负责对信号进行二维 WH/TS 编/解码。对于 $q=4$ 的情况下，光编/解码器的仿真结构如图 5 所示。

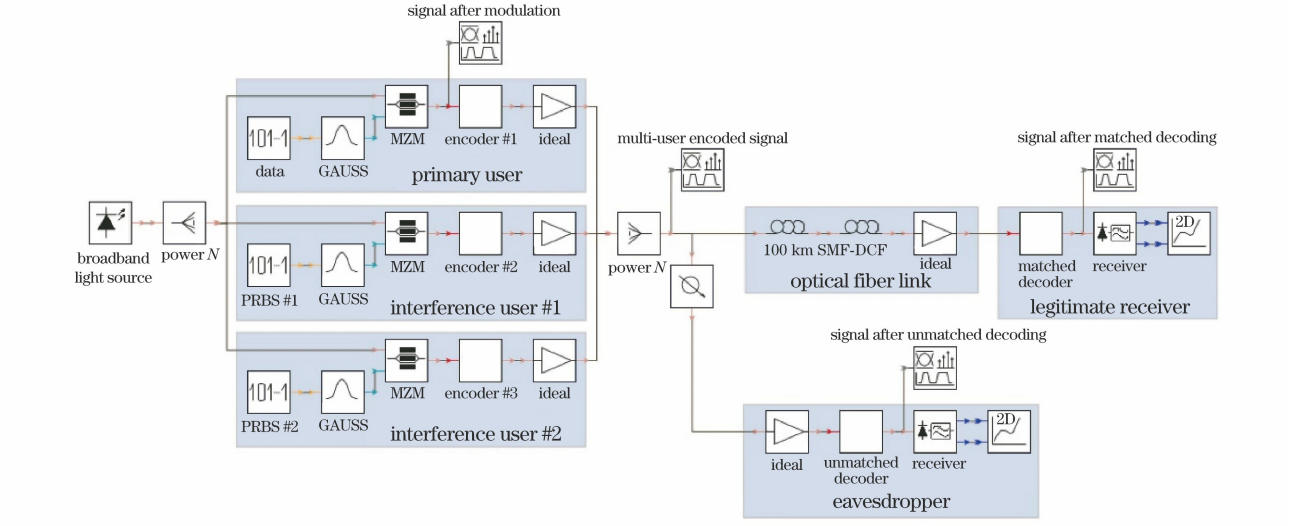

图 4　基于光编/解码技术的抗截获通信系统的仿真框图

Fig. 4　Simulation block diagram of anti-interception communication system based on optical encoding/decoding technology

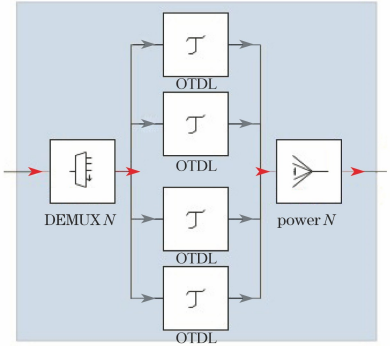

图 5　编解码器的仿真结构图($q=4$)

Fig. 5　Simulation architecture diagram of encoder/decoder ($q=4$)

对于窃听者(Eve)来说，为了避免被合法用户发现，其窃取的信号比例不能超过 1%。本研究利用一个 −20 dB 的衰减器来实现 1%的窃听比例。然后，窃听者将光信号先经过掺铒光纤放大器(EDFA)放大后再进入到光解码器进行解码。窃听者使用的光解码器是非匹配的。仿真中，具体的系统仿真参数以及各个用户使用 WH/TS 码分别如表 2 和表 3 所示。

基于 VPI 仿真软件中搭建的抗截获通信系统，分别得到了调制后信号的波形图和眼图、多用户编码信号的波形图和眼图、匹配解码后信号的波形图和眼图以及非匹配解码后信号的波形图和眼图，如图 6 所示。通过比较图 6(a)和图 6(c)、图 6(b)和图 6(d)，可以发现：经过多用户编码后，光信号的波形呈现宽谱类噪声特性，其眼图也相应地发生了严重的劣化。通过对比图 6(c)和图 6(e)、图 6(d)和图 6(f)，可以发现：结果匹配解码后，主用户(Alice)的信号可从多用户编码信号中恢复出来；但通过对比图 6(a)和图 6(e)、图 6(b)和图 6(f)，可以发现：经过光纤传输及编/解码后，自发辐射(ASE)噪声以及 MAI 噪声等将会混入 Alice 的解码信号，使得匹配解码后信号发生劣化，误码率(BER，R_{BE})相应地增大。通过比较图 6(c)和图 6(g)、图 6(d)和图 6(h)，可以发现：经过非匹配解码后，无法将 Alice 的信号从多用户编码信号中恢复出来，其仍呈现类噪声特性，这也直观地说明了抗截获通信系统

表 2　具体的仿真参数

Table 2　Specific simulation parameters

Parameter	Value	Parameter	Value
Bit rate /(Gbit·s^{-1})	2.5	Attenuation coefficient /(dB·km^{-1})	0.2
Input optical power /dBm	0	Transmission distance /km	100
Wavelength range /nm	1549.3～1550.8	Dispersion coefficient of SMF /(ps·nm^{-1}·km^{-1})	16
Wavelength space /nm	0.1	Dispersion coefficient of DCF /(ps·nm^{-1}·km^{-1})	−80
Gain of EDFA /dB	20	Responsivity of receiver /(A·W^{-1})	1
Noise index of EDFA /dB	4	Spectral density of thermal noise /(10^{-23} W·Hz^{-1})	5

表 3　仿真中各个用户使用的跳频/扩时(WH/TS)码

Table 3　Wavelength-hopping/time-spreading(WH/TS) codes used by each user in the simulation

User name	Wavelength-hopping/time-spreading (WH/TS) code
Primary user	λ_1 000000000000000 0λ_2 000000000000000 00λ_3 0000000000000 000λ_4 000000000000 0000λ_5 00000000000 00000λ_6 0000000000 000000λ_7 000000000 0000000λ_8 00000000 00000000λ_9 0000000 000000000λ_{10} 000000 0000000000λ_{11} 00000 00000000000λ_{12} 0000 0000000000000λ_{13} 000 00000000000000λ_{14} 00 000000000000000λ_{15} 0 0000000000000000λ_{16}
Interference user ＃1	λ_1 000000000000000 00λ_2 0000000000000 0000λ_3 00000000000 000000λ_4 000000000 00000000λ_5 0000000 00000000000λ_6 00000 000000000000λ_7 000 0000000000000λ_8 0 λ_9 000000000000000 00λ_{10} 0000000000000 0000λ_{11} 00000000000 000000λ_{12} 000000000 00000000λ_{13} 0000000 000000000λ_{14} 00000 000000000000λ_{15} 000 0000000000000λ_{16} 0
Interference user ＃2	0000000λ_1 00000000 000000000λ_2 000000 000000000000λ_3 0000 00000000000000λ_4 00 λ_5 000000000000000 00λ_6 0000000000000 0000λ_7 00000000000 000000λ_8 000000000 00000000λ_9 0000000 000000000λ_{10} 00000 000000000000λ_{11} 000 0000000000000λ_{12} 00 λ_{13} 000000000000000 00λ_{14} 0000000000000 0000λ_{15} 00000000000 000000λ_{16} 000000000
Legitimate receiver	λ_{16} 000000000000000 0λ_{15} 00000000000000 00λ_{14} 0000000000000 0000λ_{13} 00000000000 0000λ_{12} 00000000000 00000λ_{11} 0000000000 000000λ_{10} 000000000 0000000λ_9 00000000 00000000λ_8 0000000 000000000λ_7 000000 00000000000λ_6 00000 000000000000λ_5 0000 0000000000000λ_4 000 00000000000000λ_3 00 000000000000000λ_2 0 0000000000000000λ_1
Eavesdropper	λ_{11} 000000000000000 λ_{12} 000000000000000 λ_{13} 000000000000000 λ_{14} 000000000000000 λ_{15} 000000000000000 λ_{16} 000000000000000 λ_1 000000000000000 λ_2 000000000000000 λ_3 000000000000000 λ_4 000000000000000 λ_5 000000000000000 λ_6 000000000000000 λ_7 000000000000000 λ_8 000000000000000 λ_9 000000000000000 λ_{10} 000000000000000

具有很好的安全性，能够很好地抵抗“窃听者利用非匹配解码器对编码信号进行解码后接收”。

另外，还分别得到了不同发送光功率(1.0，0.5，0.1，0.05 mW)的情况下，合法用户和窃听者的误码率随接收光功率的变化关系曲线，如图 7 所示。可以发现：随着接收光功率的不断增大，合法用户和窃听者的误码率都会逐渐减小且最终会趋于一个定值。对于合法用户来说，当发送光功率大于 0.05 mW 时，可以通过增大接收光功率使误码率优于 10^{-9}，从而使抗截获通信系统能够满足数据传输的稳定性要求。例如，对于发送光功率 P_s=0.1 mW 的情况，当接收光功率 P_r 增加到−24 dBm 左右时，合法用户的误码率就能够达到 10^{-9}。而对于窃听者来说，其误码率远远大于合法用户的误码率，例如，在发送光功率 P_s=0.1 mW 的情况下，窃听者能够达到的最小误码率约为0.1，因此，无法正常接收到合法用户的数据信息。通过对比不同发送光功率的误码率曲线，可以发现：合法用户和窃听者的误码率都会随着发送光功率的减小而不断增大，即发送光功率的降低会导致抗截获通信系统的传输性能发生劣化，但选择合适的发送光功率可以增大系统的安全性水平。

4　结　　论

基于光码分多址(OCDMA)编/解码技术，提出了一种新型的抗截获通信系统的设计方案，并构造

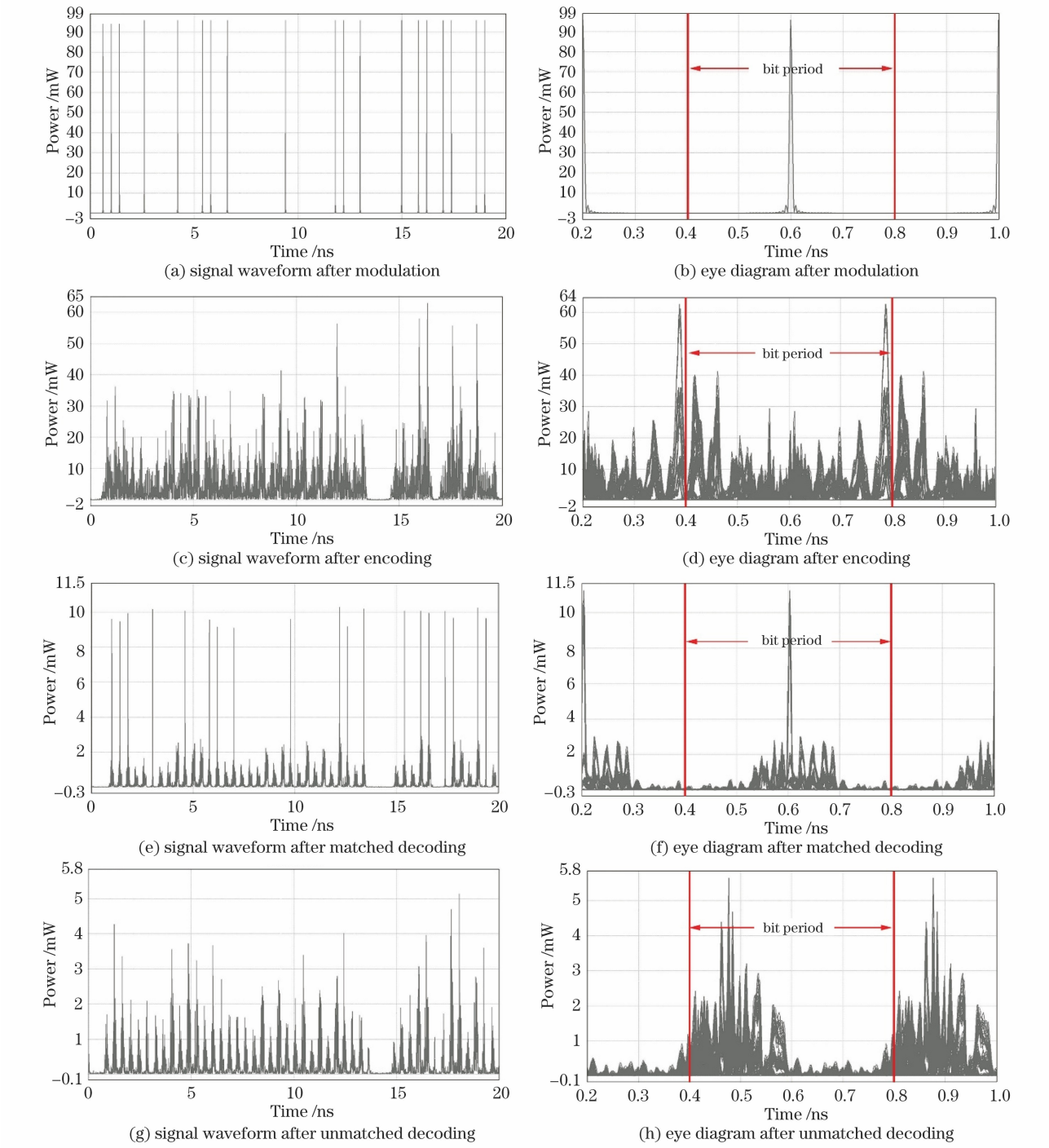

图 6　抗截获通信系统中信号的波形及眼图

Fig. 6　Waveforms and eye diagrams of signals in anti-interception communication system

了一种大容量的二维 WH/TS 地址码，提出了动态可重构编解码器的实现方法。利用 VPI 仿真软件，对抗截获通信系统的传输性能和安全性能进行了仿真研究。研究结果表明，合法接收者（Bob）利用匹配的解码器能够将主用户（Alice）信号从多用户编码信号中恢复出来，而窃听者（Eve）利用非匹配的解码器无法还原出 Alice 的原始光信号，仅可以获得类噪声信号。基于光编/解码技术的抗截获通信系统能够实现一种高速率、长距离的安全传输。

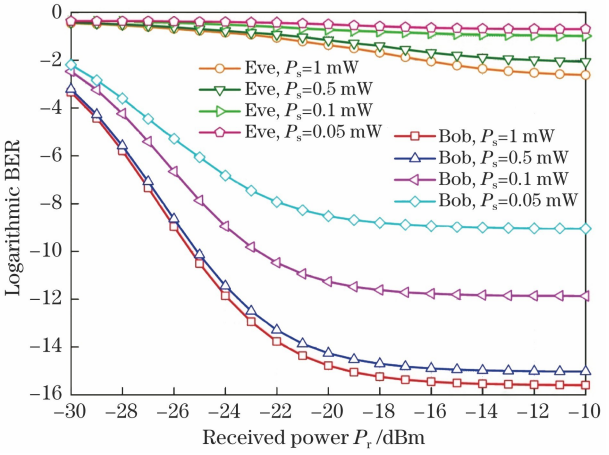

图 7　误码率随接收光功率的变化关系曲线

Fig. 7　Relationship of the BER and the received optical power

参　考　文　献

[1] Deng D P, Li H S, Lin C S, et al. Study on a new fiber-optic cable tapping and detection technology[J]. Study on Optical Communications, 2007(4): 55-58.
邓大鹏, 李洪顺, 林初善, 等. 一种新型光纤光缆窃听及监测技术研究[J]. 光通信研究, 2007(4): 55-58.

[2] Chen H, Zhu S X. Exploration on optical fiber wiretapping and intrusion detection[J]. China Information Security, 2012, 10(1): 61-63.
陈晖, 祝世雄. 光纤通信窃听及其检测技术探讨[J]. 信息安全与通信保密, 2012, 10(1): 61-63.

[3] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Review, 1999, 41(2): 303-332.

[4] Grover L K. A fast quantum mechanical algorithm for database search[C]// Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing-STOC '96, May 22-24, 1996, Philadelphia, Pennsylvania, USA. New York, USA: ACM Press, 1996: 212-219.

[5] 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.

[6] Kitayama K I, Sasaki M, Araki S, et al. Security inphotonic networks: threats and security enhancement [J]. Journal of Lightwave Technology, 2011, 29(21): 3210-3222.

[7] Lo H. Unconditional security of quantum key distribution over arbitrarily long distances [J]. Science, 1999, 283(5410): 2050-2056.

[8] Scarani V, Bechmann-Pasquinucci H, Cerf N J, et al. The security of practical quantum key distribution [J]. Reviews of Modern Physics, 2009, 81(3): 1301-1350.

[9] Patel K A, Dynes J F, Lucamarini M, et al. Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks[J]. Applied Physics Letters, 2014, 104(5): 051123.

[10] Shake T H. Security performance of optical CDMAA gainst eavesdropping[J]. Journal of Lightwave Technology, 2005, 23(2): 655-670.

[11] Leaird D E, Huang C B, Jiang Z, et al. DPSK based eavesdropper vulnerability in two-code keyed O-CDMA systems[C]// 2008 Conference on Optical Fiber Communication/National Fiber Optic Engineers Conference, February 24-28, 2008, San Diego, CA, USA. New York: IEEE, 2008: OTuP2.

[12] Wang Z X, Chang J, Prucnal P R. Theoretic alanalysis and experimental investigation on the confidentiality of 2-D incoherent optical CDMA system[J]. Journal of Lightwave Technology, 2010, 28(12): 1761-1769.

[13] Ji J H, Zhang G R, Li W J, et al. Performance analysis of physical-layer security in an OCDMA-based wiretap channel[J]. Journal of Optical Communications and Networking, 2017, 9(10): 813-818.

[14] Ji J H, Huang Q, Chen X M, et al. Performance analysis and experimental investigation of physical-layer security in OCDMA-based hybrid FSO/fiber wiretap channel[J]. IEEE Photonics Journal, 2019, 11(3): 1-20.

[15] Gupta S, Goel A. Advance method for security enhancement in optical code Division multiple access system[J]. IETE Journal of Research, 2018, 64(1): 17-26.

[16] Nasaruddin, Tsujioka T, Hara S. A code reconfiguration design for two dimensional OCDMA system to enhance security[C]// 2007 IFIP International Conference on Wireless and Optical Communications Networks, July 2-4, 2007, Singapore. IEEE, 2007: 9793863.

[17] Singh S, Kaur R, Singh A, et al. Novel security enhancement technique against eavesdropper for OCDMA system using 2-D modulation format with code switching scheme[J]. Optical Fiber Technology, 2015, 22: 84-89.

[18] Jyoti V, Kaler R S. Security enhancement of OCDMA system against eavesdropping using code-switching scheme[J]. Optik, 2011, 122(9): 787-791.