

文章编号: 0258-7025(2008)12-1894-07

基于混沌映射的偏振移位键控光通信系统

罗 璠 方 捻* 郭小丹 王春华 黄肇明

(上海大学通信与信息工程学院, 特种光纤与光接入网省部共建重点实验室, 上海 200072)

摘要 提出了一种基于数字混沌与偏振移位键控(PolSK)技术的光保密通信系统。该系统选取几种偏振态部分或完全相同的 PolSK 方式, 在系统不同时钟周期, 发送端根据实时产生的数字混沌序列选用不同的 PolSK 方式调制信息, 接收端利用同步的混沌序列与相应的 PolSK 方式解调信息。数字混沌序列的伪随机特性使得该系统的 PolSK 调制方式呈现无规则变化。当星座点个数不少于 6 且选用的 PolSK 方式不少于 4 种时, 可选的 PolSK 组合超过 10^{60} 种, 系统的密钥空间庞大。用 OptiSystem 和 Matlab 软件相结合的方法进行了系统仿真, 并做了一定的数值分析。仿真与分析结果表明, 该光通信系统通信正常, 具有较强的保密性。

关键词 光通信; 保密通信; 数字混沌; 偏振移位键控; 偏振态; 混沌序列

中图分类号 TN 929.1; TN 918 **文献标识码** A **doi**: 10.3788/CJL20083512.1894

Polarization Shift Keying Optical Communication System Based on Chaotic Maps

Luo Fan Fang Nian Guo Xiaodan Wang Chunhua Huang Zhaoming

(Key Laboratory of Special Fiber Optics and Optical Access Networks,

School of Communication and Information Engineering, Shanghai University, Shanghai 200072, China)

Abstract An optical secure communication system based on digital chaos and polarization shift keying (PolSK) technology is proposed. Several PolSK schemes are employed, in which states of polarization are partially or totally uniform. In different cycles of the system clock, different PolSK schemes are selected in the transmitter to modulate the information according to the real-time generated digital chaotic sequences, and corresponding PolSK schemes are used in the receiver to demodulate the information according to the synchronous chaotic sequences. The pseudo-random of the digital chaotic sequences makes the PolSK modulation schemes randomly vary. When the point number of constellation is not less than 6 and number of selected PolSK schemes is not less than 4, the optional PolSK schemes exceed 10^{60} kinds. Therefore, the secret key space of the system is huge. Simulation is carried out with OptiSystem and Matlab softwares, and the numerical analysis is also presented. Simulation and analytical results indicate that this system works well in transmitting information and has strong anti-attack ability.

Key words optical communication; secure communication; digital chaos; polarization shift keying; state of polarization; chaotic sequence

1 引 言

人们已对保密通信做了大量的研究^[1~3]。从通信系统分层观点来分析, 现在的保密措施是对物理层和数据层进行一些加密处理。物理层加密主要是

让攻击者不能直接在信道中发现载有信息的已调信号或很难进行同步解调, 比如混沌掩盖、混沌键控等技术。数据层加密是密码学的主要研究内容。按照现代密码学的观点, 可将密码体制分为两大类: 对称

收稿日期: 2008-01-02; 收到修改稿日期: 2008-04-30

基金项目: 国家自然科学基金(60577042)和上海市重点学科(T102)资助项目。

作者简介: 罗 璠(1983—), 男, 江苏人, 硕士研究生, 主要从事偏振移位键控、光混沌通信等方面的研究。

E-mail: luofanblue@163.com

导师简介: 黄肇明(1937—), 男, 福建人, 教授, 博士生导师, 目前主要从事光混沌通信方面的研究。

E-mail: zmhuang@mail.shu.edu.cn

* 通信联系人。E-mail: nfang@staff.shu.edu.cn

密码体制(单钥密码)和非对称密码体制(双钥密码)。流密码就是对称密码体制的一种。1989年 R. Mathews, D. Wheeler 等^[4]首次将数字混沌用于流密码与保密通信中,数字混沌开始引起人们的关注。

Benedetto 等^[5]在 90 年代将基于偏振调制的偏振移位键控(PolSK)技术引入到光数字通信中,开始引起人们的注意。PolSK 系统与传统的光通信系统相比具有在光纤传输过程中免受光源相位噪声、量子限噪声的影响等优点,适合于多电平调制。

本文提出了一种新的光保密通信系统方案。该系统不对物理层进行处理,也不属于纯粹的数据层加密,而是通过对数据层和物理层之间关系的处理来达到保密的效果。事实上,该系统的保密方案体现为一种基于数字混沌、多种偏振移位键控的编码加密。

2 问题的提出

2.1 多种偏振移位键控方案

光波的偏振态可用一个四维矢量(S_0, S_1, S_2, S_3)即 Stokes 矢量来表示。其中 S_0 表示光强度, $S_0^2 = S_1^2 + S_2^2 + S_3^2$ 。 S_1, S_2, S_3 表示在以 S_0 为半径, x, y, z 为主轴的邦加球面上一个点的坐标,对应一个偏振光的状态。邦加球面上的每一点都对应着一个光的偏振状态,整个球面表示所有偏振状态。偏振移位键控用不同的偏振态来表示不同的码元,因此可以在邦加球面上用一个星座图来表示偏振键控调制的方式。例如,图 1 列出了 4 种不同的 PolSK 星座图。其中图 1(a)表示一种二进制的 2-PolSK 星座图,它用 -45° 和 45° 的线偏振态表示二进制的“0”码与“1”码。图 1(b)用 -45° 和 45° 的线偏振态以及右旋圆偏振态三个偏振态的星座图表示 Duobinary-PolSK^[6](DPolSK 为差分偏振移位键控技术)或 2-DPolSK。图 1(c)由两个线偏振态和两个圆偏振态组成,为四电平 DD(直接检测)-PolSK 系统的星座图^[7],也可用于 3-DPolSK。图 1(d)与图 1(c)相比增加了 0° 和 90° 两个线偏振态,可作为 6-PolSK 或

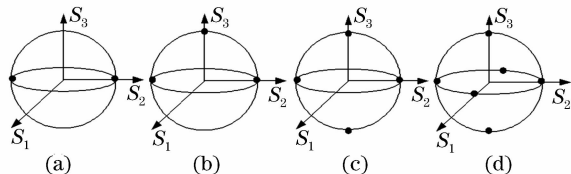


图 1 4 种 PolSK 星座图

Fig. 1 Constellation diagrams of four kinds of PolSKs

4-DPolSK 信号调制的星座图。图 1 中左右、上下和前后 6 个小黑点的 Stokes 矢量分别为 $(1, 0, 1, 0)$, $(1, 0, -1, 0)$, $(1, 0, 0, 1)$, $(1, 0, 0, -1)$, $(1, 1, 0, 0)$, $(1, -1, 0, 0)$, 分别对应 -45° 和 45° 的线偏振态,右、左旋圆偏振态以及 0° 和 90° 的线偏振态。

综合图 1 可知, -45° 线偏振态在图 1(a)中调制了一位二进制信息;在图 1(b)中,如采用 2-DPolSK,则 -45° 线偏振态本身不调制任何信息,而它与前一码元周期内偏振态的相互关系被调制了一位二进制信息。图 1(c)中, -45° 线偏振态代表 2 位二进制信息。同时,在图 1(d)中,可能表示 3 位二进制信息。由此可见,一个偏振态在不同的 PolSK 方式中调制了不同的信息(位数和数值)。

2.2 两种数字混沌

如能使偏振移位键控方案随机地改变,就能达到保密的效果。一种可取的方法是利用伪随机序列来控制多种偏振移位键控方案。与传统的伪随机序列构造方法相比,基于混沌映射的伪随机序列发生器性能更好,更易于实现,这些特点使它成为了研究热点。其中,Logistic 映射^[8,9]与 Henon 映射^[10,11]是研究得最多的两个映射,人们提出了很多基于这两种混沌映射的伪随机序列产生算法。

2.3 加密方案

图 2 为一种新的光保密通信系统框图。该系统在物理层适当选取几个固定的偏振态作为信息载体,并选取若干种基于上述偏振态的 PolSK 作为系统的调制方式,系统在混沌序列的实时控制下,在不同时钟周期采用不同的 PolSK 调制方式。系统发送端和接收端均有一组相同的基于混沌映射的高速伪随机序列发生器,通过同步时间基准的发送和接收可将两混沌序列发生器置于同步状态,即在每个系统时钟周期内,产生相同的混沌序列。同步后,在每个系统时钟周期内,发送端基于多种 PolSK 调制的编码模块根据实时产生的几路混沌序列控制相应的 PolSK 调制编码,用此 PolSK 方式将明文序列调制到一个偏振态上,即向偏振调制模块输入几路调制器驱动电压,以驱动偏振调制模块向信道发送偏振态,该偏振态所调制的信息由混沌序列和与之相应的 PolSK 方式共同决定。系统接收端在同一时钟周期内,根据同步的混沌序列发生器产生的数字混沌序列,采用相应的 PolSK 调制解码模块,将检测出的 Stokes 参数解调并输出明文序列。

传统的光保密系统往往采用一种调制方案,当攻击者窃取了调制信号后通过调制方式的识别,便

能得到发送的比特流信息。但对于本文提出的系统,由于攻击者不了解系统采用何种 PolSK 调制方

式组合和特定的混沌序列发生器组合,就无法根据物理层破解出数据层的比特流信息。

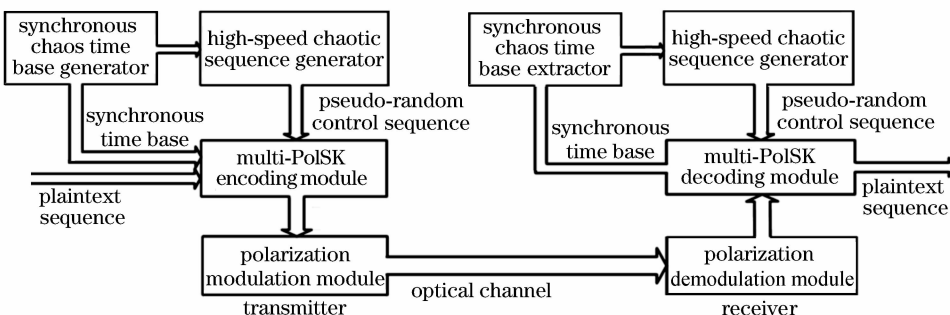


图 2 光保密通信系统框图

Fig. 2 Schematic diagram of the optical secure communication system

3 系统设计

3.1 偏振态的选择

根据 2.3 节中的加密思想,选取的偏振态应当越多越好。因为随着偏振态数量的增加,可选 PolSK 方式与 PolSK 方式组合便会急剧增多,这给攻击者带来了更大的破解困难。但同时也使系统更复杂,对系统的实现提出了更高的要求。本文提出的仿真系统选用了如图 3 所示的六个最常用的偏振态,这些偏振态易于产生和接收。对于图 3 这样的星座图,有 $C_6^2 \times P_2^1 = 30$ 种 2-PolSK 方式, $C_6^3 \times P_3^1$

= 120 种 DPolSK 方式, $C_6^3 \times C_3^2 \times P_2^1 = 120$ 种 2-DPolSK 方式, $C_6^4 \times P_4^1 = 360$ 种 4-PolSK 调制方式,至少 $(C_6^4 \times P_4^1)^6 = 2.18 \times 10^{15}$ 种 4-DPolSK 方式。如采用 4 种 PolSK 调制方式,约有 9.4×10^{59} 种组合选择,如选用 8 种则有约 1.28×10^{118} 种组合选择。对于多于 6 个偏振态或调制方式多于 8 种的系统来说,则可选的调制方式组合将远大于 1.28×10^{118} 种。如此庞大的组合选择使得攻击者很难破解出系统选用的 PolSK 调制方式组合。

3.2 系统总体设计

系统结构如图 4 所示。发送端主要由偏振调制模块、高速数字混沌模块与基于多种 PolSK 调制的编码模块构成。其中数字混沌模块与调制编码模块均在编码芯片内实现,编码芯片将明文用不同的 PolSK 调制并输出 3 路调相器驱动电压 $d1, d2, d3$, 以驱动偏振调制模块向光纤链路发送相应的偏振态 (SOP), 对应关系如表 1 所示。接收端构成与发送端相同,其中偏振解调模块为一个 Stokes 接收机^[12],用于检测出 S_1, S_2, S_3 三个 Stokes 参数并输入解码芯片。解码芯片利用相应的 PolSK 方式及表 1 的对应关系解调 Stokes 参数,并输出明文。

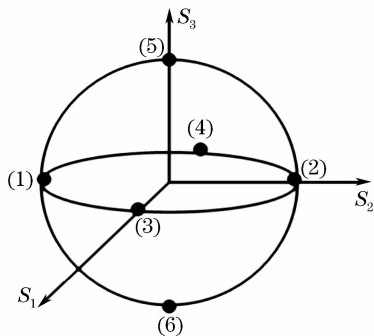


图 3 系统星座图

Fig. 3 Constellation diagram of the system

表 1 $d1, d2, d3, S_1, S_2, S_3$ 与偏振态的对应关系

Table 1 Correspondence of $d1, d2, d3$ and S_1, S_2, S_3 to state of polarization (SOP)

$d1, d2, d3$	(0,0,0)	(1,0,0)	(0,1,1)	(1,1,1)	(1,1,0)	(0,1,0)
SOP	(1)	(2)	(3)	(4)	(5)	(6)
S_1, S_2, S_3	(0, -1, 0)	(0, 1, 0)	(1, 0, 0)	(-1, 0, 0)	(0, 0, 1)	(0, 0, -1)

3.3 高速混沌序列发生器的设计

数字混沌由于采用有限精度计算导致混沌特性退化,产生了周期性。为了克服这一缺点,人们提出了增加计算精度,吸引子转换, m 序列扰动^[10,13], 双分辨率,非线性变换等方法来提高数字混沌周期。

通过这些方法数字混沌的周期可以提高到 10 的几十次方的量级,完全满足了系统长时间高速率通信的要求。随着专用集成电路 (ASIC) 技术的不断发展,通过高速现场可编程门阵列 (FPGA) 的并行处理能够实现适合本系统所需的高速数字混沌和编解

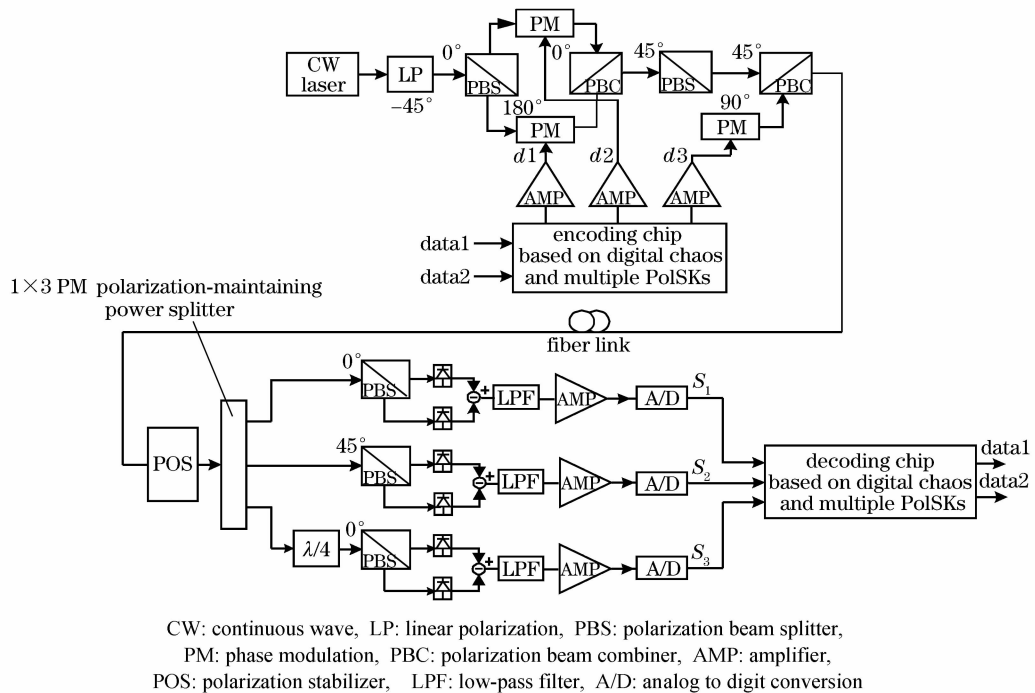


图 4 系统结构

Fig. 4 Structure of the system

表 2 4 种偏振移位键控方案

Table 2 Four kinds of PolSK schemes

High-speed chaotic sequences	00	01	10	11
Corresponding PolSK Scheme	4-PolSK: (1)—"00" (3)—"01" (4)—"10" (6)—"11"	4-PolSK: (2)—"00" (1)—"01" (6)—"10" (5)—"11"	4-DPolSK: Differential codes are shown in Table 3	4-PolSK: (3)—"00" (4)—"01" (2)—"10" (5)—"11"

码模块的硬件。

4 系统仿真

4.1 仿真系统设置

采用 OptiSystem 结合 Matlab 进行仿真,其中系统光路、部分电路由 OptiSystem 自带的原器件构成;PolSK 编码,PolSK 解码,数字混沌模块及部分电路由 Matlab 组件调用 Matlab 程序来实现。由于受 OptiSystem 的限制,无法实现可变速率的通信,所以必须选取相同电平数调制的 PolSK。本文仿真系统采用 4 种四电平调制 PolSK 的组合。

系统传输码率 620.8 Mb/s,光纤链路为长度 50 km 的单模光纤,光源波长 1550 nm,光功率 5 mW。两数字混沌模块选用 Logistic 和 Henon 两混沌映射产生两路二进制混沌序列,根据表 2 的对应关系控制采用 4 种不同的四电平 PolSK 调制。仿真系统没有对数字混沌作周期延长等处理,实际

应用中这些处理是必不可少的。Logistic 混沌映射参数为 4,初值 0.375, Henon 混沌映射初值为 -1, 0.65,初始参考偏振态为(1)。明文序列 Data1 为“01101011100101100101011010100010”, Data2 为“11100101010101101001000110110001”。

4.2 仿真分析

由于发送端、接收端两数字混沌 Matlab 模块的混沌映射相同、初值相等,且接收端 DataRecovery 模块自动作了延时补偿,使得两数字混沌在系统仿真运行过程中始终同步,即处于自同步状态,所以在发送信息序列之前无需发送同步时间基准序列。

发送端两路明文序列同时送入调制编码模块,根据数字混沌产生三路调制器驱动序列。图 5 为驱动序列 d_1, d_2, d_3 的返回映射图(重复发送序列 Data1, Data2 1000 次,序列长度 32000)。序列 d_1 很好地继承了发送端两数字混沌的混沌特性;由于表 1 的特殊规定,导致 d_2 等于 1 的概率大于等于 0 的概率,以至返回映射图上的点大部分集中于右上

平面,混沌随机性有所退化;同理, d_3 的返回映射图大部分集中于左下平面,混沌随机性退化严重。由于驱动序列的混沌随机性,使得系统产生的偏振态流也呈现一定的混沌状态。表 3 记录了重复发送序

列 Data1,Data2 运行 320~3200000 个系统时钟周期时 6 偏振态的出现次数,可见 6 偏振态分布基本均匀,均匀分布的偏振态使得攻击者很难分析系统采用了什么 PolSK 方式组合。

表 3 偏振态点数分布

Table 3 Distribution of SOP points

SOP	(1)	(2)	(3)	(4)	(5)	(6)
320 points	52	46	57	56	54	55
3200 points	535	520	536	511	538	560
32000 points	5427	5111	5508	5100	5601	5253
320000 points	53855	50066	55437	51971	56280	52391
3200000 points	541425	502333	552503	517504	560998	525237

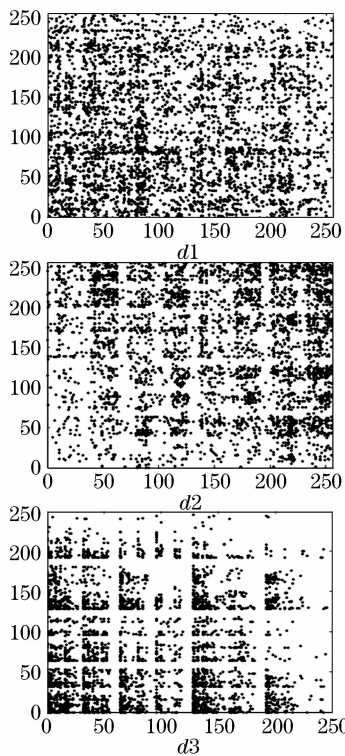


图 5 d_1, d_2, d_3 的返回映射图

Fig. 5 Return map of d_1, d_2, d_3

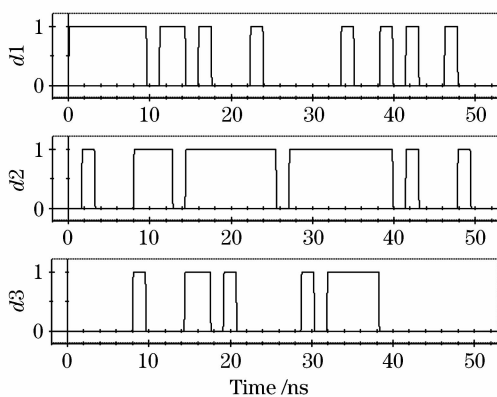


图 6 d_1, d_2, d_3 序列

Fig. 6 Sequences of d_1, d_2, d_3

表 4 差分编码表

Table 4 Table of differential codes

$(d_1 d_2 d_3)_{n-1}$	$(Data1 Data2)_n$	$(d_1 d_2 d_3)_n$
000	00,01,10,11	111,100,110,000
101	00,01,10,11	100,000,111,011
011	00,01,10,11	111,000,011,110
111	00,01,10,11	000,111,011,010
110	00,01,10,11	010,000,011,111
010	00,01,10,11	011,100,010,111

如图 6 所示,序列 d_1, d_2, d_3 经非归零脉冲产生器产生单位电压驱动三个调相器以发送相应的偏振态。在仿真的第一个系统时钟周期内,经过计算得两路混沌序列为“10”。由表 2 知,应采用 4-DPolSK 调制两路明文序列“01”。因假设系统初始偏振态为(1),根据编码表 4 推得,当前周期内发送(2)偏振态,对应驱动序列 d_1, d_2, d_3 为“100”,与仿真波形图 6 相符合。

接收端通过非相干 Stokes 参数提取模块,提取出混沌的 Stokes 参数,波形如图 7 所示。第一个系统时钟周期内, $S_1 = 0$ mV, $S_2 = 1$ mV, $S_3 = 0$ mV, 对应 Stokes 矢量 $(0, 1, 0)$, 即图 3 中的 (2) 偏

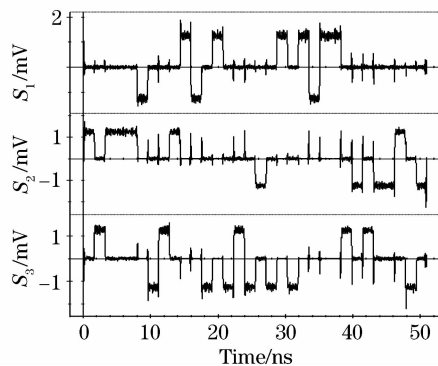


图 7 接收的 Stokes 参数

Fig. 7 Received Stokes parameters

振态。图 7 所示的 Stokes 参数信号经判决和脉冲电压形成后变成单位电压 Stokes 参数, 由于该信号有 -1 值的存在, 不能直接转换为 OptiSystem 中的二进制信号, 因此需通过 Matlab 模块将单位电压 Stokes 参数转化为与之对应的单位电压驱动序列 $d1, d2, d3$, 之后转换成二进制信号送入解调解码模块, 根据数字混沌便能恢复序列 Data1, Data2, 如图 8(a), (b) 所示。这两路解调的序列与明文序列完全一致。当 PolSK 调制方式组合选取正确, Logistic

混沌映射参数为 3.987, 初值 0.425, Henon 混沌映射初值为 $-0.96, 0.73$ 时, 解调结果如图 8(c), (d) 所示; 当混沌映射参数与初值选取正确, PolSK 调制方式组合选取错误时, 一种解调结果如图 8(e), (f) 所示。从图 8 可知, 该仿真系统的接收端如果没有特定的 PolSK 解码模块和同步的数字混沌, 便无法根据偏振态流恢复出信息序列, 这样便达到了保密的效果。

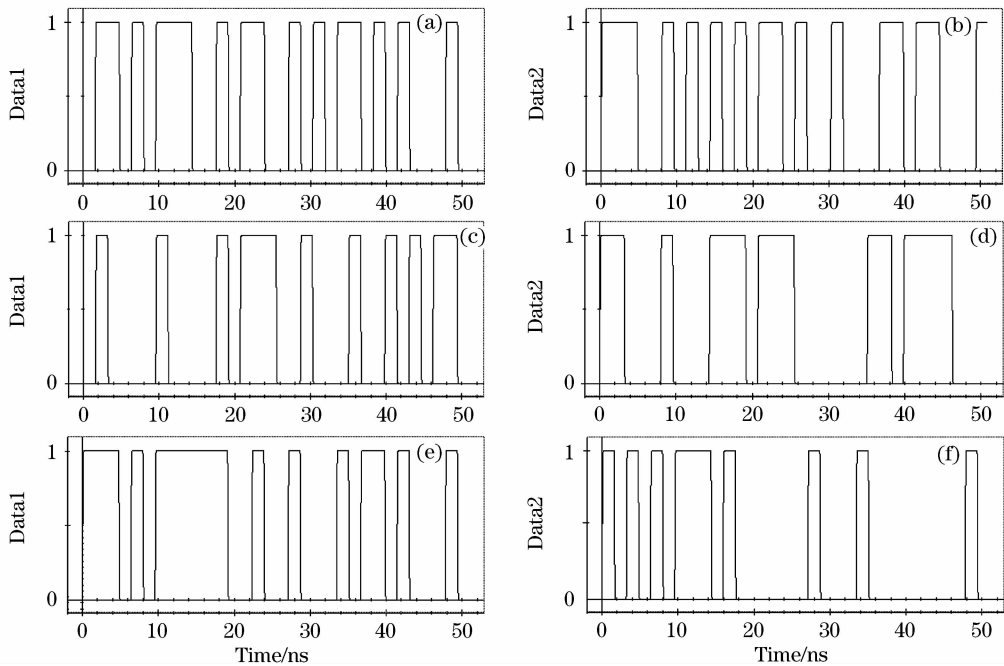


图 8 三种解调结果。(a), (b) 正确解调结果; (c), (d) 混沌初值错误的解调结果; (e), (f) 调制方式组合错误的解调结果

Fig. 8 Three kinds of demodulation results. (a), (b) correct demodulated results; (c), (d) demodulated results with incorrect initial value of the chaos; (e), (f) demodulated results with incorrect combination of the modulation modes

5 结 论

提出了一种基于数字混沌和多种 PolSK 调制的编码加密方案, 对数据层和物理层之间的关系进行加密处理, 可用于 PolSK 光保密通信。采用 OptiSystem 与 Matlab 仿真了一种基于 Logistic 和 Henon 两数字混沌与 4 种 PolSK 方式的 PolSK 光保密通信系统。仿真结果表明, 该系统通信良好, 具有较强的保密性。该保密方案易于实现, 具有一定的实用价值, 还可以与物理层、数据层加密相结合来提高光通信系统的整体保密性能。

参 考 文 献

- 1 Chen Yan, Deng Ke, Hu Yu. Effect of fiber coupling on photon-detection probability of quantum key distribution systems [J]. *Acta Optica Sinica*, 2007, **27**(8):1401~1404

- 陈彦, 邓科, 胡渝. 光纤耦合对量子密钥分配系统光子探测的影响[J]. *光学学报*, 2007, **27**(8):1401~1404
- 2 Fang Nian, Wang Lutang, Guo Shuqin *et al.*. Security of polarization-shift keying chaos optical communication system [J]. *Acta Optica Sinica*, 2006, **26**(6):812~817
- 方捻, 王陆唐, 郭淑琴等. 偏振态移位键控光混沌通信系统的保密性[J]. *光学学报*, 2006, **26**(6):812~817
- 3 He Guangqiang, Zeng Guihua, Zhu Jun *et al.*. An integrable optic-fiber coherent state quantum identification system [J]. *Chinese J. Lasers*, 2007, **34**(7):924~929
- 何广强, 曾贵华, 朱俊等. 可光纤集成的相干态量子身份认证系统[J]. *中国激光*, 2007, **34**(7):924~929
- 4 L. Kocarev. Chaos-based cryptography: a brief overview [J]. *IEEE Circuits and Systems*, 2001, **1**(3):6~21
- 5 S. Benedetto, P. Poggiolini. Theory of polarization shift keying modulation [J]. *IEEE Transactions on Commun.*, 1992, **40**(4):708~721
- 6 J. Y. Fan, Z. M. Huang, L. T. Wang. Duo-binary encoded polarization shift keying (PolSK) modulation in long haul optic transmission [C]. *SPIE*, 2003, **5281**:136~144
- 7 E. Hu, Y. Hsueh, K. Wong *et al.*. 4-level direct-detection

- polarization shift-keying (DD-PolSK) system with phase modulators [C]. *OFC*, 2003, **2**:647~649
- 8 Zhang Yong, Chen Tianqi, Chen Bin. A practical method of chaos secret coding [J]. *Journal of UEST of China*, 2005, **34**(1):29~32
张 勇, 陈天麒, 陈 滨. 一种实用的混沌保密编码方法[J]. *电子科技大学学报*, 2005, **34**(1):29~32
- 9 Deng Hao, Hua Yiman, Ni Wansun. Chaos pseudo-random sequence and digital speech secure communication [J]. *Journal of China Institute of Communications*, 1999, **20**(4):29~35
邓 浩, 华一满, 倪皖苾. 混沌伪随机序列和数字语音保密通信[J]. *通信学报*, 1999, **20**(4):29~35
- 10 Wei Pengcheng, Zhang Wei, Yang Huaqian. A novel chaotic stream cryptographic algorithm based on Henon map and m -sequences [J]. *Computer Science*, 2005, **32**(6):69~72
韦鹏程, 张 伟, 杨华千. 一种基于 Henon 映射和 m -序列的混沌序列密码算法研究[J]. *计算机科学*, 2005, **32**(6):69~72
- 11 D. Erdmann, S. Murphy. Henon stream cipher [J]. *Electron. Lett.*, 1992, **28**(9):893~895
- 12 S. Benedetto, R. Gaudino, P. Poggiolini. Direct detection of optical digital transmission based on polarization shift keying modulation [J]. *IEEE J. Sel. Areas Commun.*, 1995, **13**(3):531~542
- 13 Zhou Hong, Ling Xieting. Realizing finite precision chaotic systems via perturbation of m -sequences [J]. *Acta Electronica Sinica*, 1997, **25**(7):95~97
周 红, 凌燮亭. 有限精度混沌系统的 m 序列扰动实现[J]. *电子学报*, 1997, **25**(7):95~97

2008 年度“大珩杯”《中国激光》优秀论文名单

论 文 题 名	作 者	发表时间
光子晶体光纤非线性光学研究新进展	王清月; 胡明列; 柴 路	2006
短脉冲在色散平坦光纤中传输前后波形、相位和啁啾测量的实验研究	刘山亮; 郑宏军	2006
毫米波副载波光纤通信技术的研究进展	方祖捷; 叶 青; 刘 峰等	2006
两个光纤激光器的相位锁定及高相干功率输出	何 兵; 楼祺洪; 周 军等	2006
激光推进自由飞行实验	郑义军; 谭荣清; 张阔海等	2006
基于等效相移光栅的光码分多址编/解码实验	燕 萌; 姚敏玉; 张洪明等	2006
用于激光核聚变的玻璃	姜中宏	2006
超强固体激光及其在前沿学科中的应用(1)	彭翰生	2006
车载直接探测多普勒测风激光雷达光学鉴频器	刘继桥; 卜令兵; 周 军等	2006
激光二极管双端面抽运 Tm:Ho:GdVO ₄ 2 μm 激光器	王月珠; 贺万骏; 姚宝权等	2006