引用本文：于浩，张杰，李亚杰，等：基于光纤信道特征的物理层密钥分发技术[J]. 光通信技术，2019，43(11)：43-48.

基于光纤信道特征的物理层密钥分发技术

于 浩[1]，张 杰[2*]，李亚杰[2]，雷 超[2]，付颖雯[2]，张引强[1]

（1.国网安徽省电力有限公司 信息通信分公司，合肥 230061；2.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）

摘要：以“内生安全光通信理论与技术研究”国家自然基金重点项目为研究背景，详细介绍了物理层密钥分发的3种现有技术方案。为了实现高速率与现有通信系统兼容的物理层密钥分发，提出了一种基于光纤信道特征的物理层密钥分发技术；基于光纤信道传输误比特率特性和密钥分发技术，发送端和接收端使用双端环回测量误比特率方式提取和量化生成密钥。研究结果表明：该技术实现了光纤传输速率为10 Gb/s的200 km距离传输，物理层安全协商密钥生成速率达到400 kb/s时，安全协商密钥误比特率不超过2%。

关键词：物理层密钥分发；光纤信道特征；双端环回测量；误比特率

中图分类号：TN914　**文献标识码**：A　**文章编号**：1002-5561(2019)11-0043-06

DOI：10.13921/j.cnki.issn1002-5561.2019.11.011　**开放科学(资源服务)标识码(OSID)**：

Physical layer key distribution technology based on fiber channel characteristics

YU Hao[1], ZHANG Jie[2*], LI Yajie[2], LEI Chao[2], FU Yingwen[2], ZHANG Yinqiang[1]

(1. State Grid Anhui Electric Power Co. Ltd., Information & Communication Branch, Hefei 230061, China; 2.State key laboratoryof information photonicsand optical communications, Beijing University of posts and telecommunications, Beijing100876, China)

Abstract: Based on the national natural fundkey project "Intrinsic security optical communication theory and technology research", three prior art solutions for physical layer key distribution are described in detail. In order to achieve high-rate physical layer key distribution compatible with existing communication devices, this paper proposes a physical layer key distribution technology based on fibre channel features. The transmitter and the receiver extract the quantized generation key by using the double-ended loopback measurement bit error rate method based on the fiber channel transmission bit error rate characteristic and key distribution technique. The research results show that the optical fiber transmission rate is 10 Gb/s and the transmission distance is over 200 km. When the physical layer secure key generation rate reaches 400 kb/s, the bit error rate of secure keys does not exceed 2%.

Key words: physical layer key distribution; fiber channel characteristics; double-ended loopback measurement; bit error rate

0 引言

密钥分发是通信安全中的重要环节。现有的通信传输的安全性往往由应用层的加密和解密算法来完成[1]，安全密钥分发系统的理论基础是数学上的困难问题，如大整数的分解问题(RSA公钥系统)和计算离散对数的问题(DH密钥交换)等。随着量子计算的发展，基于算法复杂度来保证安全性的经典加密技术面临失效的严重威胁，业界预计小规模通用量子计算机可能在未来5~10年内出现，可能构成对密码加密体制安全性的重大威胁。虽然量子密钥分配与一次一密的有机结合，可在理论上确保量子密钥的安全性[2]。但是以量子密钥分发为代表的新型网络信息安全技术仍有待完善，目前存在诸多制约因素，如现阶段量子密钥分发系统在密钥生成速率和可用传输距离等方面性能有限，难以大规模推广。而量子密钥分发所需的关键器件研发、量子中继和星地量子通信中的多项关键技术尚待突破。同时，实际量子密钥分发器件和

收稿日期：2019-04-17。

基金项目：国家自然科学基金(61831003)资助；国家电网公司科学技术项目(B1120718003P)资助。

作者简介：于浩(1973-)男，汉族，安徽临泉人，大学本科学历，正高级工程师，现任职于国网安徽省电力有限公司信息通信分公司，主要从事电力信息通信保密技术、电力通信光传输技术和数据通信技术研究，长期从事电力信息通信运行维护和管理工作。

*** 通信作者**：张杰(E-mail: lgr24@bupt.edu.cn)。

系统的不理想特性可能导致安全漏洞,并且长距离传输中采用授信节点进行密码中继也会成为系统安全的风险点。采用物理层密钥分发手段,基于物理层特性,其安全程度与数据信息内容无关。

现有的几种物理层密钥分发技术虽然可以克服密钥预分配机制的缺陷[3],但是都存在传输距离短、密钥生成速率低等问题。因此,本文提出一种基于光纤信道特征的物理层密钥分发技术,该技术是在非量子领域提出的一种适合长距离传输,且密钥生成速率高的光纤物理层密钥分发技术。

1 光纤信道现有密钥分发技术

1.1 基于正交偏振模式(OPM)之间随机相位波动的密钥分发方案

2018 年,上海交通大学 Adnan A. E. Hajomer 等人提出了基于 OPM 之间的随机相位波动共享密钥方案。该方案主要利用了可变长度保偏光纤生成波形的相位具备与环境相关的随机性和信道相关的唯一性,并且在另一客户端可产生高度相关的波形,提取该波形的物理特性,可生成高安全性的种子密钥[4]。

延时干涉仪(DI)的密钥分发原理如图 1 所示。该方案主要由 DI、保偏光纤等器件组成[5]。其中,DI 被放置在保偏光纤的两端以提取波长的相位变化,可变长度保偏光纤是该方案主要的波动源,1–I 和 I 表示光纤的分光强度比。

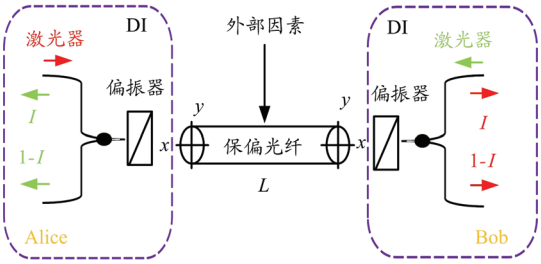


图 1 DI 的密钥分发原理

具体的实现流程为:Alice 端通过激光器向系统中发射线性偏振光,并通过偏振器形成偏振角为 α 的偏振光。随后经过长度为 L、物理环境(温度、压力或机械改变)随机的保偏光纤使得光信号的波动差迅速变化并具有很好的随机性。最后光信号经过偏振角为 β 的偏振器。

此时 DI 提取到的波动相位差 $\Delta\varphi$ 与 L 成线性关系:

$$\Delta\varphi=\varphi_f-\varphi_s=2\pi\Delta nL/\lambda \tag{1}$$

其中,Δn 是 2 个 OPM 的折射率之差,φ_f、φ_s 是 2 个正交偏振模的相位,该相位差 $\Delta\varphi$ 又可引起光强 I 的变化,光强度 I 与偏振角 α、β(γ 是 α 和 β 互相关)和相位波动差 $\Delta\varphi$ 满足函数关系:

$$I(L)=\frac{1}{2}[1+\cos2\alpha\sin2\beta+|\gamma|\sin2\alpha\sin2\beta\cos\Delta\varphi] \tag{2}$$

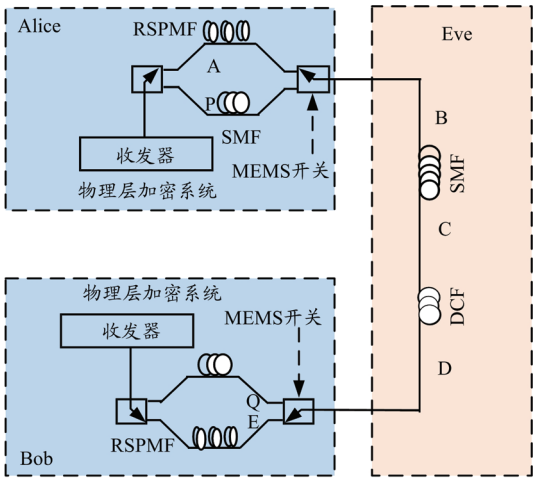
随后 Bob 在短时间内也进行上述过程,由于来自 DI 的输出信号在 2 个方向上都经过了相同的光纤路径,因此它们会经历相同的环境影响,则 DI 可提取到高度相关的光强信号。该光强信号经采样、量化可得种子密钥。

由于保偏光纤中与环境相关的随机性和与信道相关相位波动的唯一性,所提出方案的安全性具有抵抗各种攻击的能力。实验验证结果表明:在 25 km 标准单模光纤上成功演示了 220 b/s 的密钥生成速率,误比特率为 5%。此外,由于该方案可应用光学放大器,具有成本低,与现有光纤网络兼容并且适合长距离传输的优点。

1.2 利用光纤链路偏振模色散(PMD)的物理层密钥分发方案

加利福尼亚大学尔湾分校的 Imam Uz Zaman 等人通过利用 PMD 作为随机和独特的信道特性,提出了一种基于对称物理层 PMD 的密钥生成方案,用于点对点光链路(PPOL)通信。该方案由随机拼接偏振保持光纤(RSPMF)、单模光纤(SMF)和色散补偿光纤(DCF)组成光纤通信链路[6],其具体实现流程如下:Alice 和 Bob 通过向彼此发送预定义的探测信号(比特序列)来启动密钥生成机制。这些预定义的脉冲信号经历随机偏振旋转,由于脉冲离散,脉冲信号在 2 个正交偏振态之间将会引起脉冲分裂[7]。由于 PMD 的强随机性可导致随机的幅度调制,随机幅度调制又可被光电探测器提取为随机的电流值,之后由 Alice 和 Bob 将随机电流值独立采样、处理和量化,即可生成密钥。由于 Alice 和 Bob 经历相同的物理信道,因此在光纤两端测量的幅度调制将是高度相关的。另外,Alice 和 Bob 执行不匹配删除步骤以降低双方的不匹配率。

基于上述理论,本文构建了一个对称加密通信模型,其原理图如图 2 所示。在该模型中,Alice 和 Bob 是 2 个希望通过对称的安全通信信道进行通信的合法方。对称加密通信模型有 2 种模式,密钥生成模式和通信模式。在密钥生成模式中,Alice 和 Bob 之间的通信链路是图 2 中的 A–B–C–D–E。由于来自长距离



MEMS：微电子机械系统

图 2 基于 RSPMF 的原理图

SMF 的高 PMD 效应，2 个主要极化状态(PSP)之间的差分群延迟(DGD)将更高并且具备更高的随机性。此路径中的 RSPMF 和 SMF 尾纤之间有 28 根光纤，在 Alice 和 Bob 之间的密钥建立协议之后，系统将进入通信模式并通过 P–B–C–D–Q 路径发送信号，就像在传统的点对点光纤链路中一样。本方案提出的 PMD 密钥生成技术使 Alice 和 Bob 能够生成并交换强对称加密密钥以对其明文进行编码，由于 PMD 的随机性，Eve 将无法生成与 Alice 和 Bob 相同的密钥，编码的明文不会面临安全传输挑战。

基于 PMD 生成的加密密钥的随机性和安全性强度非常高。该方案中基于 PMD 的加密密钥通过了美国国家标准与技术研究院(NIST)的测试。由 50 km 的模拟链路显示，通过最佳密钥生成设置，可以生成具有高随机性(NIST 随机性测试为高 P 值)和足够生成率(>50%)的对称密钥。

1.3 基于新型超长光纤激光器的安全密钥分发方案

来自以色列特拉维夫大学物理电子学系电气工程学院的 Omer Kotlicki 和 Jacob Scheuer 提出了基于超长光纤激光器的安全密钥分发。该方案通过使用标准光纤组件，配置了可调谐激光器在 2 个通信方之间建立激光振荡，使 2 个用户之间具备提取另一个用户所选择激光镜像的能力，从而建立共享密钥，而攻击链路的对手 Eve 并不能使用时间和频谱攻击策略来重建该方案生成密钥[8]。该方案的简单性和鲁棒性使其成为光学领域中安全且实用的密钥分发方案[9]。

图 3 为基于超长光纤激光器的密钥分发系统的示意图。该系统由耦合器、光纤放大器、环形器、光开关和干涉仪等部分组成。首先，使用可调谐激光器作

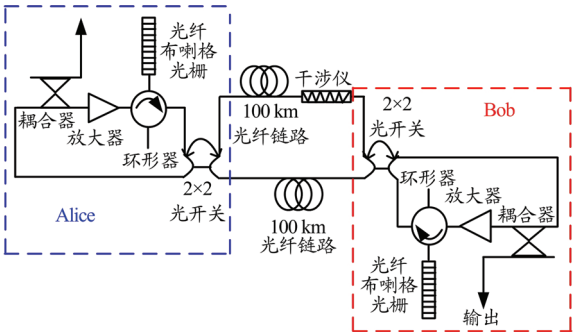


图 3 基于超长光纤激光器的安全密钥分发方案

为参考在每个位置分别执行压电电压的校准，同时使用 2×2 光开关将每个位置与外部分离，使 Alice、Bob 和光纤链路各自独立。待校准完成后，光开关再打开整个回路，允许信号在站点之间循环传输。腔体中在 Alice 端和 Bob 端放置窄带宽干涉滤光片可以实现镜像频率的特定选择。因此，Alice 和 Bob 都具有包括 2 个光谱的镜子组，每组中的每个镜子在不同频率处具有谐振腔的峰值反射率 ω_A 和 ω_B。

在协商过程中，Alice 和 Bob 可独立选择其中一个镜子，并将其用作激光反射器。Alice、Bob 端反射镜的峰值频率(ω_A 和 ω_B)被调谐到腔内的干涉仪中，该干涉仪允许(0,0)和(1,1)状态产生连续高透射峰值的激光，同时急剧降低(0,1)和(1,0)状态的净光学增益。若它们选择了相同的镜子，则在 ω_A((0,0)状态)或 ω_B((1,1)状态)处产生清晰信号，此时是非安全状态，应舍弃。如果选择互补反射镜((1,0)或(0,1)状态)，则谐振腔中的增益不足以建立激光，该状态难以区分并且仅表现出噪声。此时，窃听对手 Eve 只能检测噪音，无法确定哪个用户选择了哪个镜像，因此为安全状态。协商过程中将该状态保留。

实验证明了该方案能实现超过 200 km、密钥生成速率为 0.5 kb/s 的安全通信。通过研究频谱和时间攻击策略的弹性，也证明了该方案的高安全性。此外，该方案中密钥生成速率会随着链路长度线性减小，因此更适用于长距离通信链路。

2 基于光纤信道特征的物理层密钥分发技术

2.1 原理概述

在通信系统中，误比特率是衡量光纤通信系统正确传输码元能力的参数，表征的是二进制比特流经过系统传输后发生错误的概率，误比特率为 m/n，m、n 分别为传输中发生错误的比特数和总比特数。误比特率直接受信道质量的影响，也是信道质量的直接体现。

本文提出的信道特征提取方案中,利用光纤信道传输误比特率特性和误比特率的密钥分发技术,发送端和接收端使用双端环回测量误比特率方式,提取和量化生成密钥。本方案中,发送信号使用离散傅里叶变换-正交频分复用(DFTs-OFDM)调制,每个子载波被映射成正交振幅调制(QAM)格式,并使用量子噪声流密码(QNSC)方案进行加密[10]。通过测量接收信号误比特率的动态变化,提取信道特征。由于信道受各种随机干扰和物理参数(如光学非线性、色散和噪声等)的影响,测量的误比特率随机变化,当发射机和接收机同时测量光纤环路的误比特率时,保证了测量结果的一致性。

基于误比特率的密钥分发技术如图 4 所示,Alice 和 Bob 的数据通过时分复用(TDM)在光纤环路中传输。Alice 的比特时间是奇数,Bob 的比特时间是偶数。图 4 中,数据发送/接收单元使用伪随机数发生器(PRNG)产生数据和 QNSC 使用的基,PRNG 保证了基的随机性;QNSC 加密映射/解映射单元使用高阶 QAM;误比特分析单元处理环回一圈信息,计算环回误比特率,同时 Alice 和 Bob 使用均衡算法;量化变换单元对误比特分析单元输出信号量化判决。双端环回测误比特率:Alice 和 Bob 同时把所传信息用基加密传送,收到对方信息后不做任何额外处理,仅(同时)判决并用本地基加密回传,再次传送后完成环回测量,将第二次收到的信息与己方初次发送的信息对比测量,得到误比特率,作为实时信道特征。至此,信道特征提取已经完成,再加以量化后得到安全密钥。量化规则是:若量化误比特率大于判决门限 $T_{high}=\mu+\alpha\delta$,则判决为 1;若量化误比特率大于判决门限 $T_{low}=\mu-\alpha\delta$,则判决为 0,中间部分丢弃。其中,μ 是误比特均值,δ 是误比特方差。

密钥分发步骤如下:

①Alice(Bob)通过 PRNG 生成随机数据 Data_A(Data_B)和随机基 Base_A(Base_B)。

②Alice(Bob)中的数字信号处理器(DSP)用 Data_A(Data_B)和 Base_A(Base_B)来产生信号 T_A(T_B)。在光纤传输后,信号 T_A(T_B)到达 Bob(Alice)端,信道噪声 N_AB(N_BA)包含各种干扰。

③Bob(Alice)中的 DSP 以随机基 Base_B(Base_A)处理接收到的 R_B(R_A)信号,生成数据 Data_AB(Data_BA)。使用基 Base 处理数据 Data_AB 或 Data_BA 时,基态 Base 是公开的。使用基 Base 处理数据 Data_A 或 Data_B 时,基态 Base 是保密的。

④Bob(Alice)将 Data_AB(Data_BA)和 Base_B(Base_A)发送到发射机的 DSP 中,生成信号 T_B(T_A)。信号经光纤传输后到达 Alice(Bob)端,信道噪声 N_BA(N_AB)包含各种干扰。

⑤接收端 DSP 利用接收到的信号 R_A(R_B)和随机基 Base_A(Base_B)生成数据 Data_ABA(Data_BAB)。在 Base_A(Base_B)等于 Base_B(Base_A)的条件下,将数据 Data_A(Data_B)与 Data_ABA(Data_BAB)进行比较,得到光纤环路的误比特率性能 ber1(ber2)。

⑥对测得的误比特率进行分段量化,即可在 Alice 端和 Bob 端生成初始密钥,根据误比特率均值和方差按照判决规则对初始密钥进行变换,生成最终密钥。

本文提出了一种分光窃听方法,来分析基于光纤信道特征的物理层密钥分发技术生成密钥的安全性。Eve 窃听方法的实验方案图如图 5 所示。发送端加密信号使用随机信号发生器产生,通过 I/Q 调制器,经由光放大器放大发送到接收端,接收端使用 50:50 的光耦合器,将信号分成两部分:一部分是 Alice/Bob 接收

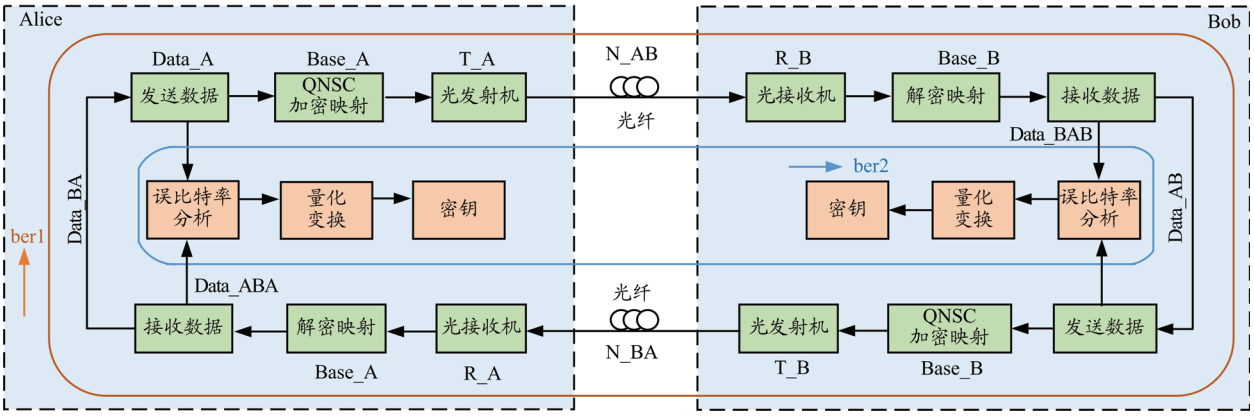


图 4 基于误比特率的密钥分发技术

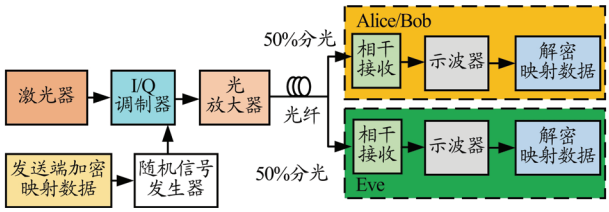


图 5 Eve 窃听方法

然后使用示波器采样，通过 DSP 后处理解密映射数据；另一部分是 Eve 接收使用示波器采样，通过 DSP 后处理解密映射数据,Eve 和 Alice/Bob 使用的基 Base 不同。

2.2 实验验证

基于光纤信道特征的物理层密钥分发系统结构图如图 6 所示。系统实验使用的主要仪器参数如表 1 所示。

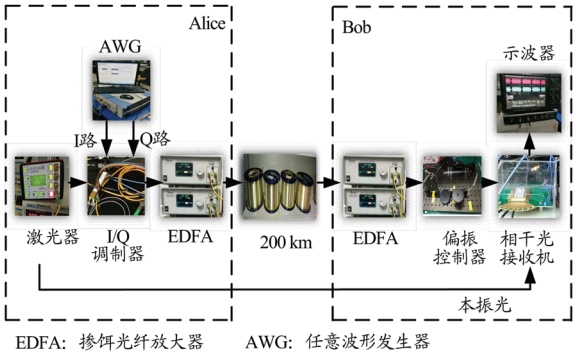


图 6 基于光纤信道特征的物理层密钥分发系统结构图

表 1 主要实验仪器参数设置

器件参数	参数值	器件参数	参数值
激光器波长	1550 nm	AWG 输出电压	600 mV
激光器输出功率	10 dBm	发送/接收端 EDFA 输出功率	10.1 dBm/0.5 dBm
AWG 输出速率	10 Gb/s	示波器采样速率	20 GS/s

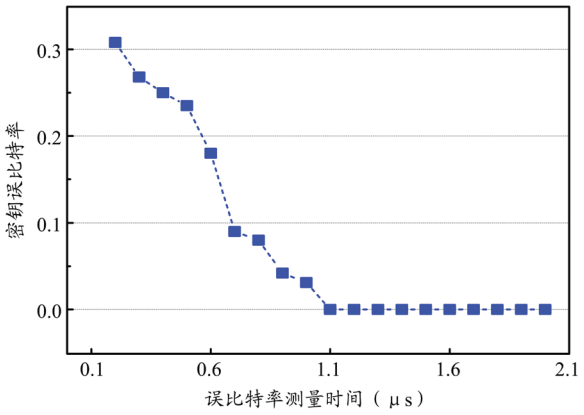
本方案实现了光纤传输速率为 10 Gb/s、传输距离为 200 km 的物理层安全密钥协商,实验结果表明:安全协商密钥生成速率达到 400 kb/s 时,安全协商密钥误比特率不超过 2%。同时,通过分析光纤窃听攻击原理(图 5),分析了密钥协商方案的安全性。

200 km 光纤信道一致性实验结果如图 7(a)所示,随着误比特率测量时间逐渐增加,Alice 和 Bob 的密钥误比特率逐渐降低。这是因为随着误比特率测量时间增加,计算误比特率时比特数量对应的测量分段时间变长,则一个时段内计算得到的误比特率降低,信道误比特特性更加相似。另外,随着误比特率测量时间增加,误比特曲线更加平滑,误比特起伏变小,因此可通过增加误比特测量时间降低 Alice 和 Bob 密钥的误比特率。

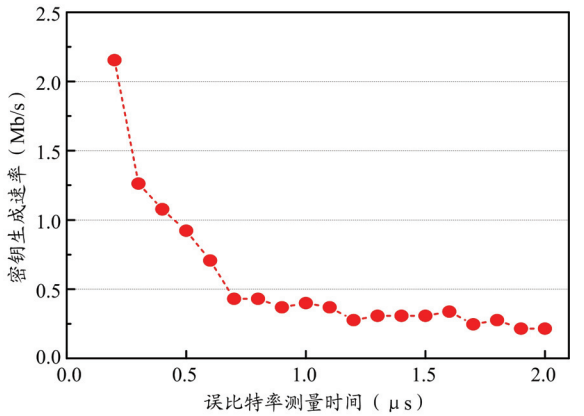
200 km 光纤信道生成率实验结果如图 7 (b)所示,随着误比特率测量时间逐渐增加,密钥生成速率呈指数降低。这是因为随着误比特率测量时间增加,一个时段内计算得到的误比特率降低，因此 Alice 和 Bob 量化得到的密钥也相应减少。

为了平衡系统密钥生成速率和密钥误比特率,实验进一步分析了两者的关系,如图 8 所示。随着密钥生成速率提高,密钥误比特率呈指数上升。当密钥误比特率到达 2%时,得到的密钥生成速率约为 400 kb/s,保证了系统生成密钥具有低误比特率的同时具有高的生成速率。

为了进一步说明本方案生成密钥的安全性,本文分析了一种窃听攻击。Eve 模拟合法接收端截获 Alice 和 Bob 传输数据,模拟 Alice 和 Bob 的误比特率信息,



(a) 200 km 光纤信道一致性实验结果



(b) 200 km 光纤信道生成率实验结果

图 7 200 km 光纤信道一致性和生成率实验结果

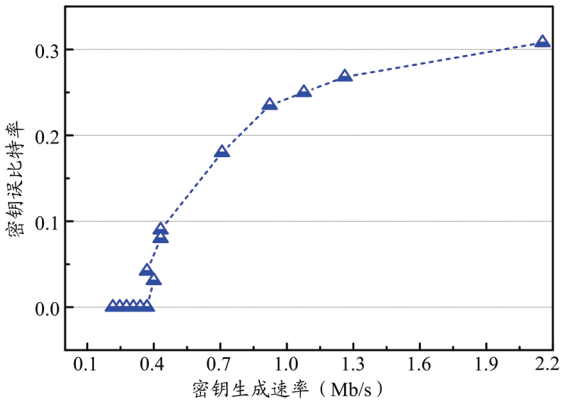


图 8 200 km 密钥一致性与密钥生成速率的关系

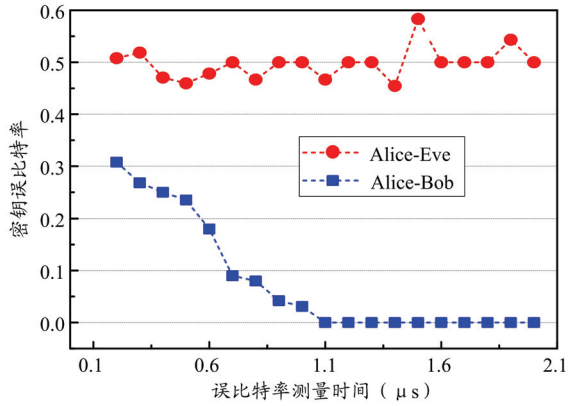


图 9 密钥误比特率与误比特率测量时间关系

量化生成有效的密钥。Alice–Bob、Alice–Eve 之间密钥误比特率与误比特率测量时间关系的对比情况如图 9 所示，随着误比特测量时间增加，Alice 和 Bob 的密钥误比特率逐渐减小，接近于 0；Alice 和 Eve 的密钥误比特率一直维持在 50%附近。该结果表明：本文采用的基于光纤信道特征的物理层密钥分发技术可以保证密钥协商的安全性。

3 结束语

本文提出的基于光纤信道特征的物理层密钥分发技术，利用信道传输误比特率特性，通过环回测量方式提取信道误比特特性，保证 Alice 和 Bob 具有相同的无码特性，从而量化判决生成协商密钥。实验证明了本方案可实现传输速率为 10 Gb/s、传输距离为 200 km 的物理层安全密钥协商。安全协商密钥生成速率达到 400 kb/s 时，安全协商密钥误比特率不超过 2%。同时，通过分析一个光纤窃听攻击，分析了密钥协商的安全性。本方案可进一步应用于超长跨距光纤通信系统的安全密钥分发。

参考文献：

[1] 于浩，王伟，柏思瑶. 宽带电力线 MIMO 通信物理层安全传输方法[J]. 电力信息与通信技术，2017，5(1)：94–97.

[2] 刘国军，张小建，吴鹏，等. 电力量子保密通信安全测试指标体系研究[J]. 电力信息与通信技术，2017，15(10)：50–54.

[3] WU Y, XIA H, CHENG C. Improved Mult-bit Adaptive Quantization algorithm for Physical Layer Security based on Channel Charscteristics[C]// International Conference on Systems and Informatics （ICSAI), November 10–12, 2018, Nanjing, China. Piscataway: IEEE, 2018.

[4] HAJOMER A, YANG X, SULTAN A, et al. Key distribution based on phase fluctuation between polarization modes in optical channel [J]. IEEE Photonics Technology Letters, 30(8): 704–707, 2018

[5] HAJOMER A, YANG X, SULTAN A, et al. Key Generation and Distribution Using Phase Fluctuation in Classical Fiber Channel [C]// International Conference on Transparent Optical Networks （ICTON), July 1–5, 2018, Bucharest, Romania. Piscataway: IEEE, 2018.

[6] ZAMAN I U, LOPEZ A B, AL FARUQUE M A, et al. Physical Layer Cryptographic Key Generation by Exploiting PMD of an Optical Fiber Link [J]. Journal of Lightwave Technology, 2018, 36(24): 5903–5911.

[7] ZAMAN I U, LOPEZ A B, AL FARUQUE M A, et al. Polarization mode dispersion-based physical layer key generation for optical fiber link security [C]//Optical Sensors, April 24–27, 2017, Prague, Czech Republic. Bellingham: SPIE, 2017.

[8] EL-TAHER A E, KOTLICKI O, SCHEUER J, et al. Long-range, high bit-rate secure key distribution link utilizing Raman Ultra-long fiber laser （UFL）[C]//The European Conference on Lasers and Electro-Optics, May 12–16, 2013, Munich, Germany.Piscataway: IEEE, 2013.

[9] SCHEUER J. Secure long-range and high bit-rate distribution of shared key using dark states ultra-long fiber laser （UFL）[C]//Broadband Access Communication Technologies XII, January 29 –31, 2018, San Francisco, United States. Bellingham: SPIE, 2018.

[10] NAKAZAWA M, YOSHIDA M, HIROOKA T, et al. QAM quantum noise stream cipher transmission over 100 km with continuous variable quantum key distribution [J]. IEEE Journal of Quantum Electronics, 2017, 53(4): 1–16.