物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

光纤偏振编码量子密钥分发系统荧光边信道攻击与防御

陈艳辉 王金东 杜聪 马瑞丽 赵家钰 秦晓娟 魏正军 张智明

Eavesdropping and countermeasures for backflash side channel in fiber polarization-coded quantum key distribution

Chen Yan-Hui Wang Jin-Dong Du Cong Ma Rui-Li Zhao Jia-Yu Qin Xiao-Juan Wei Zheng-Jun Zhang Zhi-Ming

引用信息 Citation: Acta Physica Sinica, 68, 130301 (2019) DOI: 10.7498/aps.68.20190464
在线阅读 View online: https://doi.org/10.7498/aps.68.20190464
当期内容 View table of contents: http://wulixb.iphy.ac.cn

光纤偏振编码量子密钥分发系统荧光边信道攻击与防御*

陈艳辉[1)] 王金东[1)†] 杜聪[1)] 马瑞丽[1)] 赵家钰[1)]
秦晓娟[2)] 魏正军[1)] 张智明[1)]

1) (华南师范大学, 广东省微纳光子功能材料与器件重点实验室 (信息光电子科技学院), 广东省量子调控工程与材料重点实验室, 广州 510006)

2) (广东理工职业学院工程技术系, 广州 510091)

(2019 年 4 月 1 日收到; 2019 年 4 月 12 日收到修改稿)

实际安全性是目前量子密钥分发系统中最大的挑战. 在实际实现中, 接收单元的单光子探测器在雪崩过程的二次光子发射 (反向荧光) 会导致信息泄露. 目前, 已有研究表明该反向荧光会泄露时间和偏振信息并且窃听行为不会在通信过程中产生额外误码率, 在自由空间量子密钥分发系统中提出了利用反向荧光获取偏振信息的攻击方案, 但是在光纤量子密钥分发系统中暂未见报道. 本文提出了在光纤偏振编码量子密钥分发系统中利用反向荧光获取信息的窃听方案与减少信息泄露的解决方法, 在时分复用偏振补偿的光纤偏振编码量子密钥分发系统的基础上对该方案中窃听者如何获取密钥信息进行了理论分析. 实验上测量了光纤偏振编码量子密钥分发系统中反向荧光的概率为 0.05, 并对本文提出的窃听方案中的信息泄露进行量化, 得出窃听者获取密钥信息的下限为 2.5×10^{-4}.

关键词: 量子密钥分发, 偏振编码, 时分复用偏振补偿, 反向荧光

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.68.20190464

1 引 言

量子密钥分发[1−6](quantum key distribution, QKD) 是一种采用单光子加载密钥信息, 并通过通信双方 (Alice 和 Bob) 之间协调生成密钥的一种保密通信技术, 以量子力学基本原理和性质为基础, 在理论上能够保证通信双方密钥分配的安全性, 是量子保密通信领域[1−11] 的重要研究内容. 自从 BB84 协议[6] 提出以来, 量子密钥分发的发展也越来越快速, 其安全性也被人们所关注. 在完美的理论模型的前提下, 其物理原理保证了量子密钥分发在理论上的安全性[12−19]. 实际上, 通信器件存在不完美性, 因此窃听者可以利用器件的不完美特性进行窃听[20−24]. 如今, 单光子雪崩光电二极管是 QKD 中应用最广泛的探测器[25], 也是最容易遭受攻击的部分. 针对单光子探测器 (avalanche photodetector, APD) 提出的攻击方案有很多, 比如, 探测器致盲攻击[21,22], 利用探测效率不匹配进行攻击[23,24] 等. 最近比较受关注的是 APD 雪崩过程中会伴随着光子发射[26−40], 该光子被称为反向荧光, 窃听者 Eve 可以分析反向荧光的时间特性, 判断是哪个探测器响应, 从而获得密钥信息. 在基

* 国家自然科学基金 (批准号: 61771205)、广东省自然科学基金 (批准号: 2015A030313388) 和广东省科技计划 (批准号: 2015B010128012, 2017KZ010101) 资助的课题.

† 通信作者. E-mail: wangjindong@m.scnu.edu.cn

于偏振编码的 QKD 中, 反向荧光经过 Bob 端偏振分束器 (polarization beam splitter, PBS) 时会携带偏振信息, 所以 Eve 也可以通过测量反向荧光的偏振态获得密钥信息[39,40]. 1995 年, Newman[26] 第一个对反向荧光进行观测, 在此之后 Lacaita 等人对荧光进行了定量分析[31], 并且在实验上探测了 Si APD[33,34] 和 InGaAs APD[36,39] 产生的反向荧光. 2016 年, Meda 等[37] 通过实验对荧光特性进行研究, 分析了 APD 不同偏压和门时间内光子到达时刻对产生反向荧光的概率的影响, 以及反向荧光的光谱分布. 在此基础上, 2018 年, Pinheiro 等[40] 提出了自由空间 QKD 中的荧光边信道攻击与防御方案, 该方案是通过测量荧光的偏振信息来判断探测器的响应. 但是在光纤 QKD 中利用荧光进行边信道攻击的方法尚未见报道. 因此, 本文提出了一种在光纤偏振编码 QKD 中通过探测荧光的偏振态获取密钥信息的方法.

由于在光纤中偏振态容易发生变化, 所以基于光纤的偏振编码 QKD 需要对偏振态进行补偿, 常见的偏振补偿方式有中断式偏振补偿[41]、波分复用偏振补偿[42] 和时分复用偏振补偿[41,43]. 本文主要针对在时分复用偏振补偿的光纤偏振编码 QKD 中提出一种利用反向荧光获取密钥信息的窃听方案和防御方法.

本文第 2 节中描述了在时分复用偏振补偿的光纤偏振编码 QKD 中利用反向荧光获取密钥信息的窃听方案, 并对该方案中如何利用反向荧光获取偏振信息进行了理论推导, 介绍了针对该方案的防御方法; 第 3 节描述了测量光纤偏振编码 QKD 中携带有偏振信息的反向荧光概率的实验, 并利用实验结果对第 2 节中攻击方案的信息泄露进行量化; 第 4 节给出结论.

2 光纤偏振编码 QKD 中利用反向荧光获取密钥信息的窃听方案与防御方法

本节介绍了一种在时分复用偏振补偿的光纤偏振编码 QKD 中利用反向荧光获取密钥信息的窃听方案, 从理论上分析了 Eve 如何获取反向荧光的偏振态从而区分 Bob 的哪个探测器响应. 并根据反向荧光的波长特性提出了针对上述窃听方案的防御方法.

时分复用偏振补偿的光纤偏振编码 QKD 系统[43] 如图 1 所示, 在 BB84 协议的基础上, Alice 通过时分复用的方法将脉冲光分为参考光和信号光, 在 HV($\mathrm{H}=0°$, $\mathrm{V}=90°$) 基下参考光和信号光的时间差为 50 ns, 在 QR($\mathrm{Q}=45°$, $\mathrm{R}=135°$) 基下参考光和信号光的时间差为 90 ns. Bob 通过测量参考光的偏振消光比 T 来判断是否需要纠偏, 当 $T\geqslant 0.99$ 时, 则不需要进行偏振补偿; $T\leqslant 0.97$ 时, 此时的数据无用; 当 $T\leqslant 0.98$ 时, 电压放大器 (amplifier, AMP) 将产生两个偏置电压 V_1 和 V_2 驱动电动偏振控制器 (electronicpolarization-controllers, EPC) 挤压光纤改变偏振态, 直到 $T\geqslant 0.99$ 时, 保持 V_1 和 V_2 不变, 此时的偏振态变回原来的状态[43]. Bob 探测时产生的反向荧光分为信号荧光和参考荧光, 返回到信道中通过环形器被 Eve 探测. Eve 探测反向荧光的偏振信息的理论推导描述如下.

在上述时分复用偏振补偿系统的基础上, 我们假设 Alice 发送量子态为 $\mathrm{V}(|e_y\rangle)$ 态的光脉冲给 Bob, 该脉冲光分为信号光和参考光, 时间差为 50 ns, 并且两者的偏振态一样, 而因为时间差很短, 所以两者的偏振变化也一样. Alice 和 Bob 之间由光纤信道引起的偏振变换算符为 $\widehat{F_1}$, 当脉冲光到 Bob 端时, 量子态变为 $\widehat{F_1}\,|e_y\rangle$. Bob 端的器件 BS_1, PC_5, PC_6, EPC_1 和 EPC_2 的偏振作用算符分别为 $\widehat{B_1}$, $\widehat{P_5}$, $\widehat{P_6}$, $\widehat{E_1}$ 和 $\widehat{E_2}$, 在基匹配的情况下, 当光脉冲到达 Bob 的探测器 APD_3 时量子态将变为 $\widehat{E_2}\widehat{P_6}\widehat{B_1}\widehat{F_1}\,|e_y\rangle$. Bob 通过测量参考光的偏振消光比知道变化后的量子态, 通过 AMP 控制 EPC_2 改变偏振作用算符 $\widehat{E_2}$, 使得

$$\widehat{E_2}=\left(\widehat{P_6}\widehat{B_1}\widehat{F_1}\right)^{-1}, \tag{1}$$

那么纠偏后的量子态将变回原始状态

$$\widehat{E_2}\widehat{P_6}\widehat{B_1}\widehat{F_1}\,|e_y\rangle=|e_y\rangle\,. \tag{2}$$

当探测器 APD_3 和 APD_6 响应后会产生反向荧光, 分别为信号荧光和参考荧光, 两者时间差为 50 ns. 假设反向荧光的量子态为 $|C\rangle$, PBS 的作用算符为 $\widehat{H}$, 使得反向荧光的量子态变为

$$\widehat{H}\,|C\rangle=\cos^2\theta\,|e_x\rangle+\sin^2\theta\,|e_y\rangle\,. \tag{3}$$

从上式可知, 返回到信道中的反向荧光量子态为 $|e_y\rangle$, 所以信号荧光和参考荧光返回到信道的量子态为 $|e_y\rangle$, 并且在传输过程信号荧光和参考荧光

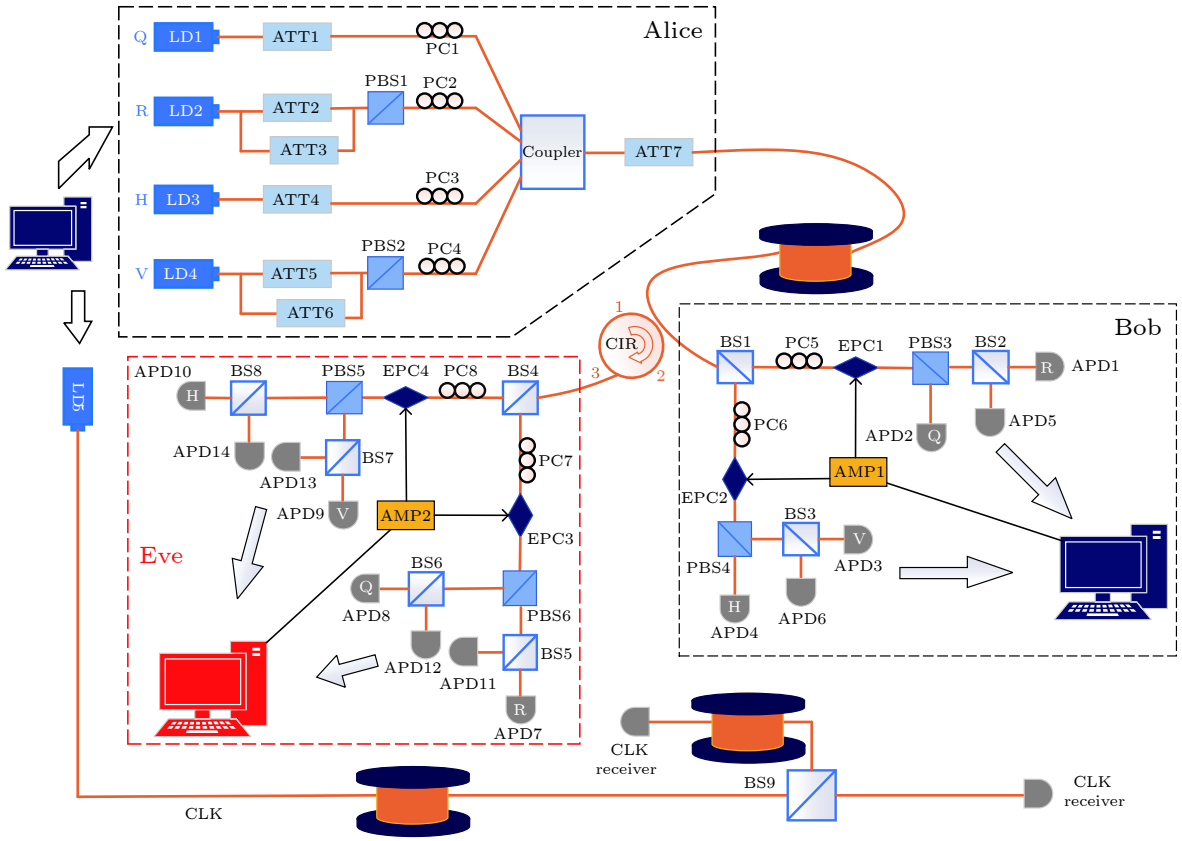

图 1 在时分复用的光纤偏振编码 QKD 中利用反向荧光窃取偏振信息, 其中 LD_{1-5} 为激光器; ATT_{1-7} 为可调谐光衰减器; PBS_{1-6} 为偏振分束器; PC_{1-8} 为手动偏振控制器; BS_{1-9} 为分束器; EPC_{1-4} 为电动偏振控制器; AMP 为电压放大器; APD_{1-14} 为雪崩光电探测器; CIR 为环形器

Fig. 1. Polarization information is obtained by backflash in a TDM fiber polarization coded QKD. LD_{1-5}, laser; ATT_{1-7}, variable optical attenuators; PBS_{1-6}, polarization beam splitters; PC_{1-8}, manual polarization-controllers; BS_{1-9}, beam splitters; EPC_{1-4}, electronic polarization-controllers; AMP, voltage amplifier; APD_{1-14}, avalanche photodetector; CIR, circulator.

的偏振变化一样. 当反向荧光 (信号荧光和参考荧光) 反向经过 Bob 端的器件时, 偏振态将变为 $\widehat{B_1}'\widehat{P_6}'\widehat{E_2}'|e_y\rangle$ ($\widehat{B_1}'$, $\widehat{P_6}'$ 和 $\widehat{E_2}'$ 为光脉冲反向经过 BS_1, PC_6 和 EPC_2 的偏振变换算符).

Eve 通过环形器接收反向荧光, 并测量反向荧光的偏振态. Alice 和 Eve 之间由光纤信道引起的偏振变换算符为 $\widehat{F_2}$, 环形器的偏振变换算符为 $\widehat{C}$, Eve 的器件 BS_4, PC_7, PC_8, EPC_3 和 EPC_4 的偏振作用算符分别为 $\widehat{B_4}$, $\widehat{P_7}$, $\widehat{P_8}$, $\widehat{E_3}$ 和 $\widehat{E_4}$. 此时到达 Eve 探测器 APD_9 的反向荧光的偏振态为 $\widehat{E_4}\widehat{P_8}\widehat{B_4}\widehat{F_2}\widehat{C}\widehat{B_1}'\widehat{P_6}'\widehat{E_2}'|e_y\rangle$, Eve 可以通过测量参考荧光的偏振消光比来判断偏振变化, 从而控制 EPC_4 进行纠偏, 改变算符 $\widehat{E_4}$, 使得

$$\widehat{E_4} = \left(\widehat{P_8}\widehat{B_4}\widehat{F_2}\widehat{C}\widehat{B_1}'\widehat{P_6}'\widehat{E_2}'\right)^{-1}, \tag{4}$$

从而 Eve 可以探测到反向荧光的偏振态为

$$\widehat{E_4}\widehat{P_8}\widehat{B_4}\widehat{F_2}\widehat{C}\widehat{B_1}'\widehat{P_6}'\widehat{E_2}'|e_y\rangle = |e_y\rangle. \tag{5}$$

通过以上的推导, Eve 可以获取反向荧光的偏振态, 知道是哪个探测器响应, 从而获取密钥信息. 该理论推导的前提是 Bob 和 Eve 都选对了基. Eve 可以在 Alice 和 Bob 对基时判断自己是否选对了基, 只是减少了 Eve 的信息获取量. Bob 选对了基的情况下 Eve 选对基的概率为 1/2.

在上述窃听的基础上, Eve 还可以利用参考荧光判断 Bob 的 APD_1 和 APD_3 是否响应. APD_3 和 APD_6 产生的参考荧光和信号荧光时间差为 50 ns, APD_9 和 APD_{13}(APD_{14}) 门触发延迟时间为 50 ns, 所以, 若 APD_9 和 APD_{13} 同时响应或者 APD_{14} 响应, 那么 Eve 便可以判断是 APD_3 响应. 同理, 若 APD_7 和 APD_{11} 同时响应或者 APD_{12} 响应, 那么 Eve 便可以知道是 APD_1 响应.

针对上述窃听方案, 讨论了减少信息泄露的应对措施. 在此之前, Meda 等 [37] 在实验上测量过荧光的光谱分布, 由于反向荧光是探测器倍增区域产生的光子, 所以反向荧光的波长范围较宽, 其光子

数在某一个波长处为峰值, 不同的探测器的荧光峰值波长不一样, 所以我们可以利用可调谐滤波器减少荧光的泄露量, 从而减少信息泄露. 我们还可以使用隔离器, 使反向荧光返回到信道中的概率进一步减少.

3 光纤偏振编码 QKD 中的信息泄漏率

本节通过实验测量了光纤偏振编码 QKD 系统中反向荧光的概率, 结合第 2 节中的窃听方案得出信息泄露率. Pinheiro 等[40] 通过实验验证过反向荧光经过 PBS 时会携带偏振信息, 并且在自由空间 QKD 中探测到了反向荧光的偏振信息, 其探测到的水平态 (H) 的偏振信息泄露率为3.5×10^{-3}, 竖直态 (V) 的偏振信息泄露率为2.0×10^{-3}. 但是在光纤 QKD 中偏振态容易发生变化, 无法确定探测到的荧光的偏振态是否正确, 则需要对偏振态进行补偿.

在第 2 节中时分复用偏振补偿 QKD 系统的基础上, 测量了没有偏振补偿的光纤偏振编码 QKD 中携带有偏振信息的反向荧光概率如图 2 所示, 将实验结果带入窃听方案推导出信息泄露率. 首先需要将激光器和探测器进行同步处理, Alice 发送偏振态为 H 的脉冲光给 Bob, 脉宽为 500 ps, 频率为 2 MHz, 探测器 $\mathrm{APD_1}$(ID200) 响应后产生反向荧光返回信道, 通过环形器被探测器 $\mathrm{APD_3}$ (ID201) 探测, 用示波器 (oscilloscope, waverunner 8404 M) 记录 Eve 和 Bob 之间的符合响应次数, 得到直方图如图 3 所示.

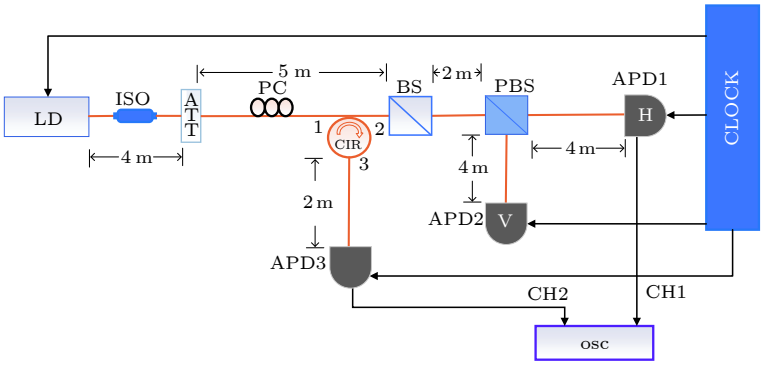

图 2 探测光纤偏振编码 QKD 中携带有偏振信息的反向荧光概率 LD 为激光器 (QCL-102); ATT 为衰减器 (SM3301); $\mathrm{APD_{1-3}}$ 为单光子探测器 (ID200, ID200, ID201); CLOCK 为时钟信号源 (DG645); OSC 为示波器 (WAVERUNNER 8404 M); 电线长度相同

Fig. 2. Probability detection of the backflash of the polarization-encoded QKD carrying polarization information. LD, laser (qcl-102); ATT, attenuator (SM3301); $\mathrm{APD_{1-3}}$, avalanche photodetector (ID200, ID200, ID201); CLOCK, clock (DG645); OSC, oscilloscope (WAVERUNNER 8404 M); the cables are the same length.

在图 2 所示的系统中, 我们记录 $\mathrm{APD_1}$ 响应的总次数 $N=10^6$, 得到如图 3 所示的符合计数直方图. 通过测量路径和门控延时, 可得 $\mathrm{APD_1}$ 产生的反向荧光到达 $\mathrm{APD_3}$ 的时间间隔为 50 ns, 而反向荧光是探测器发生雪崩产生电流时发射的光子, 所以反向荧光计数分布和电流形状相匹配[26–35], 从图 3 中可知, 第三个峰值为反向荧光计数分布, 而其他峰值为仪器的端面反射光等. 实验测量得出反向荧光的符合响应计数 $N_\mathrm{b}=1752$, Bob 的反向传输效率 $T_\mathrm{b}=0.28$ (假设反向荧光的偏振态是随机的, 那么由于 PBS 的偏振相关性, Bob 的反向传输效率应减半), 图 2 中 Eve 的信道传输效率为 $T_\mathrm{e}=0.99$, $\mathrm{APD_3}$ 的探测效率 $\eta_\mathrm{e}=25\%$, 那么我们可以计算得出反向荧光概率为

$$P_\mathrm{b}=N_\mathrm{b}/\frac{1}{2}T_\mathrm{b}T_\mathrm{e}\eta_\mathrm{e}N\approx0.05. \tag{6}$$

从以上结果可知, 在上述光纤偏振编码 QKD 系统中反向荧光的概率为 0.05.

在实验测得的反向荧光概率的基础上, 对第 2 节中窃听方案的信息泄漏进行量化. 窃听方案如图 1 所示, 经过测量可知 Bob 的反向传输率 $T_\mathrm{B}=0.16$ 和 Eve 的信道传输率 $T_\mathrm{E}=0.25$, Eve 的探测器探测效率为 $\eta_\mathrm{E}=0.25$, 因为 Eve 测量反向荧光的偏振态时选对基的概率为 1/2, 所以反向荧光泄漏信息的概率为

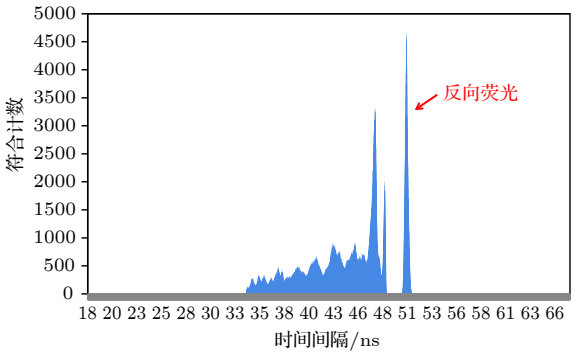

图 3 Eve 和 Bob 之间的符合计数直方图, 第三个峰为探测到的反向荧光光子数分布, 其他峰值为光学仪器的端面反射光

Fig. 3. Coincidence count histogram between Bob and Eve. The third peak is the detected backflash photon number distribution, and the other peaks denote the reflected light of the optical instrument.

$$P_{\mathrm{B}} = \eta_{\mathrm{E}} T_{\mathrm{E}} T_{\mathrm{B}} P_{\mathrm{b}}/2 \approx 2.5 \times 10^{-4}. \tag{7}$$

由于反向荧光概率偏低, 所以我们假设环形器与 Eve 所连接的光纤要尽可能地短, 减少荧光的损耗. Eve 尽可能地提高 EPC 的偏振补偿速率, 从而提高信息窃听率.

实际上, 在 Bob 进行偏振控制时, Eve 也需要时间对反向荧光进行偏振控制, 那么 Eve 在两个偏振控制时间内会增加无效数据, 所以 Eve 还需要结合后处理采取适当的对策. 该窃听方案中 Eve 的窃听装置不是最理想的装置, 所以我们得出的只是信息泄露的下限.

从以上的结论中可知, 在时分复用偏振补偿的光纤偏振编码 QKD 中 Eve 可以通过监测反向荧光的偏振信息获得少量的密钥信息并且还不会产生误码率. 信息泄露的下限为 $P_{\mathrm{B}} \approx 2.5 \times 10^{-4}$.

上述窃听方案的主要优势在于解决了反向荧光的偏振态在光纤中会发生变化的问题, 在时分复用偏振补偿的偏振编码 QKD 系统的基础上对反向荧光进行纠偏从而获得准确的偏振信息, 利用参考荧光和信号荧光的时间差获得部分密钥信息. 但是该方案中需要对偏振态进行纠偏, 所以在纠偏过程中会增加无效信息, 故信息泄露的下限比自由空间 QKD 中的信息泄露率要低.

4 结 论

本文提出了在时分复用偏振补偿的光纤偏振编码 QKD 中利用反向荧光获取信息的窃听方案和防御方法, 从理论上证明了该窃听方案中 Eve 可以利用反向荧光获取偏振信息, 从而获取少量的密钥信息. 在实验上探测了在光纤偏振编码 QKD 中反向荧光的泄漏率为 0.05, 从而得出 Eve 获取信息的下限为 $P_{\mathrm{B}} \approx 2.5 \times 10^{-4}$. 该结论是在没有使用滤波器的基础上得出的, 反向荧光的波长范围比较大, 在某一个波段的反向荧光的泄漏率有最大值, 所以可以通过使用滤波器降低信息泄露. 希望我们的工作能对光纤 QKD 中边信道的实际安全性研究有一定的帮助.

参考文献

[1] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Xu G, Chen X B, Dou Z, Yang Y X, Li Z 2015 *Quantum Inf. Process* **14** 2959
[3] Yue X L, WangJ D, Wei Z J, Guo B H, Liu S H 2012 *Acta Phys. Sin.* **61** 184215 (in Chinese) [岳孝林, 王金东, 魏正军, 郭邦红, 刘颂豪 2012 物理学报 **61** 184215]
[4] Yang L, Ma H X, Zhen C, Ding X L, Gao J C, Long G L 2017 *Acta Phys. Sin.* **66** 230303 (in Chinese) [杨璐, 马鸿洋, 郑超, 丁晓兰, 高健存, 龙桂鲁 2017 物理学报 **66** 230303]
[5] Deng G F, Li X H, Li T 2018 *Acta Phys. Sin.* **67** 130301 (in Chinese) [邓富国, 李熙涵, 李涛 2018 物理学报 **67** 130301]
[6] Bennett C H, Brassard G 1984 *IEEE International Conference on Computers New York* **198** 4
[7] Chen X B, Tang X, Xu G, Dou Z, Chen Y L, Yang Y X 2018 *Quantum Inf. Process* **17** 225
[8] Chen X B, SunY R, Xu G, Jia H Y, Qu Z, Yang Y X 2017 *Quantum Inf. Process* **16** 244
[9] Xu G, Xiao K, Li Z, Niu X X, Ryan M 2019 *Comput. Mater. Con.* **58** 809
[10] Xu G, Chen X B, Li J, Wang C, Yang Y X, Li Z 2015 *Quantum Inf. Process* **14** 4297
[11] Chen X B, Wang Y L, Xu G, Yang Y X 2019 *IEEE Access* **7** 13634
[12] Liu H W, Qu W X, Dou T Q, Wang J P, Zhang Y, Ma H Q 2018 *Chin. Phys. B* **27** 212
[13] Zhang H, Mao Y, Hang D, Guo Y, Wu X D, Zhang L 2018 *Chin. Phys. B* **27** 90307
[14] Lo H 1999 *Science* **283** 2050
[15] Norbert L 2000 *Phys. Rev. A* **61** 052304
[16] Shor P W, Preskill J 2000 *Appl. Phys. Lett.* **85** 441
[17] Renner R 2005 *Phys. Rev. A* **72** 012332
[18] Wu C F, Du Y N, Wang J D, Wei Z J, Qin X J, Zhao F, Zhang Z M 2016 *Acta Phys. Sin.* **65** 100302 (in Chinese) [吴承峰, 杜亚男, 王金东, 魏正军, 秦晓娟, 赵峰, 张智明 2016 物理学报 **65** 100302]
[19] Wang J D, Qin X J, Jiang Y Z, Wang X J, Chen L W, Zhao F, Wei Z J, Zhang Z M 2016 *Opt. Express* **24** 8302
[20] Brassard G, Lütkenhaus N, Mor T, Sanders B C 2000 *Appl. Phys. Lett.* **85** 1330
[21] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V 2010 *Nat. Photon.* **4** 686
[22] Wang J D, Wang H, Qin X J, Wei Z J, Zhang Z M 2016 *Eur. Phys. J. D* **70** 1

[23] Vadim M, Hjelme D R 2005 *J. Mod. Opt.* **52** 691
[24] Qi B, Fung C H F, Lo H K, Ma X 2007 *Quantum Inf. Comput.* **7** 73
[25] Hadfield R H 2009 *Nat. Photon.* **3** 696
[26] Newman R 1955 *Phys. Rev.* **100** 700
[27] Chynoweth A G, Mckay K G 1956 *Phys. Rev.* **102** 369
[28] Childs P A, Eccleston W 1984 *J. Appl. Phys.* **55** 4304
[29] Waldschmidt M, Wittig S 1968 *Nucl. Instrum. Meth.* **64** 189
[30] Gautam D K, Khokle W S, Garg K B 1988 *Solid State Electron* **31** 219
[31] Lacaita A L, Zappa F, Bigliardi S, Manfredi M 1993 *IEEE Trans. Electron Dev.* **40** 577
[32] Lacaita A, Cova S, Spinelli A, Zappa F 1993 *Appl. Phys. Lett.* **62** 606
[33] Villa S, Lacaita A L, Pacelli A 1995 *Phys. Rev. B* **52** 10993
[34] Akil N, Kerns S E, Kerns D V, Charles J P 1998 *Appl. Phys. Lett.* **73** 871
[35] Kurtsiefer C, Zarda P, Mayer S, Weinfurter H 2001 *J. Mod. Opt.* **48** 2039
[36] Acerbi F, Tosi A, Zappa F 2013 *IEEE Photon. Tech. L.* **25** 1778
[37] Meda A, Degiovanni I P, Tosi A, Yuan Z, Brida G, Genovese M 2017 *Light-Sci. Appl.* **6** e16261
[38] Marini L, Camphausen R, Xiong C, Eggleton B J, Palomba S 2016 *Conference on Optical Fibre Technology* Australian OSA, September, 2016pAW5C-4
[39] Shi Y, Lim J Z J, Poh H S, Tan P K, Tan P A, Ling A, Kurtsiefer C 2017 *Opt. Express* **25** 30388
[40] Pinheiro P V P, Chaiwongkhot P, Sajeed S, Horn R T, Bourgoin J P, Jennewein T, Makarov V 2018 *Opt. Express* **26** 21020
[41] Chen J, Wu G, Li Y, Wu E, Zeng H 2007 *Opt. Express* **15** 17928
[42] Temporao G P 2009 *New J. Phys.* **11** 045015
[43] Chen J, Wu G, Xu L, Gu X, Wu E, Zeng H 2009 *New J. Phys.* **11** 065004

Eavesdropping and countermeasures for backflash side channel in fiber polarization-coded quantum key distribution*

Chen Yan-Hui [1)] Wang Jin-Dong [1)†] Du Cong [1)] Ma Rui-Li [1)] Zhao Jia-Yu [1)]
Qin Xiao-Juan [2)] Wei Zheng-Jun [1)] Zhang Zhi-Ming [1)]

1) (*Guangdong Provincial Key Laboratory of Nanophotonic Functional Materials and Devices, Key Laboratory of Quantum Engineering and Quantum Materials, South China Normal University, Guangzhou* 510006, *China*)

2) (*Guangdong Polytechnic Institute, Guangzhou* 510091, *China*)

(Received 1 April 2019; revised manuscript received 12 April 2019)

Abstract

Nowadays, the practical security of quantum key distribution (QKD) is the biggest challenge. In practical implementation, the security of a practical system strongly depends on its device implementation, and device defects will create security holes. The information leakage from a receiving unit due to secondary photon emission (backflash) is caused by a single-photon detector in the avalanche process. Now studies have shown that the backflash will leak the information about time and polarization and the eavesdropping behavior will not generate additional error rate in the communication process. An eavesdropping scheme obtaining time information by using backflash is proposed. Targeting this security hole for backflash leaking polarization information, an eavesdropping scheme for obtaining polarization information by using backflash is proposed in free-space QKD; however, it has not been reported in fiber QKD. In this study, the eavesdropping scheme and countermeasures for obtaining information by using backflash in fiber polarization-coded QKD is proposed. Since the polarization state of the fiber polarization-coded QKD system is easy to change, the scheme is proposed based on the time-division multiplexing polarization compensation fiber polarization-coded QKD system. In theory, the eavesdropper in this scheme obtaining the key information by using the backflash is theoretically deduced, and corrects the polarization change of the backflash by time-division multiplexing polarization compensation method, thus obtaining the accurate polarization information. The probability of backflash in the fiber polarization-coded QKD is measured to be 0.05, and the information leakage in the proposed eavesdropping scheme is quantified. The lower limit of the information obtained by the eavesdropper is 2.5×10^{-4}. Due to the fact that the polarization compensation process increases invalid information in actual operation, the information obtained by the eavesdropper will be further reduced, thus obtaining the lower limit of information leakage. The results show that the backflash leaks a small amount of key information in a time-multiplexed polarization-compensated fiber polarization-coded QKD system. The wavelength characteristics of the backflash can be utilized to take corresponding defense methods. Backflash has a wide spectral range, and the count of backflash has a peak wavelength. So, tunable filters and isolators can be used to reduce backflash leakage, thereby reducing the information leakage.

Keywords: quantum key distribution, polarization-coded, time division multiplexing polarization compensation, backflash

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.68.20190464

* Project supported by the National Science Foundation of China (Grant No. 61771205), the National Science Foundation of Guangdong Province, China (Grant No. 2015A030313388), and the Science and Technology Projects of Guangdong Province, China (Grant Nos. 2015B010128012, 2017KZ010101).

† Corresponding author. E-mail: wangjindong@m.scnu.edu.cn