学术期刊可以用微信做什么，快来看看！

微信自动应答服务平台
微时代 微革命

微服务
移动互联网时代的营销革命

简单快捷 • 高效互动 • 随时随地 • 广泛传播

微信扫一扫
开启智慧“微服务”
Effects of Photon-Number-Splitting Attacks on the Security of Satellite-to-Ground Quantum Key Distribution Systems

Chen Yan¹ Yang Hongyu² Deng Ke³

¹ Institute of Astronautics and Aeronautics, University of Electronic Science and Technology of China, Chengdu, Sichuan 610054, China
² College of Automation, University of Electronic Science and Technology of China, Chengdu, Sichuan 610054, China

Abstract The security of practical quantum key distribution (QKD) systems based on weak coherent pulse (WCP) sources is imperiled by photon number splitting (PNS) attacks due to imperfections of devices and channel loss. The relation between the zenith angle and the mean photon number for security of a satellite-to-ground QKD system based on the WCP source against PNS attacks which operates with the optimal eavesdropping strategy is provided. The theoretical and calculation results shows the upper limits of key parameters for satellite-to-ground QKD systems, such as the zenith angle and the mean photon number, are limited by PNS attacks, and eventually the key exchange rate and the capacity of QKD systems are limited as well. The zenith angle and the mean photon number have an incompatibility effect on the capacity of a satellite-to-ground QKD system. At the same time, a method of parameter estimation of the zenith angle and the mean photon number for security of practical satellite-to-ground QKD systems against PNS attacks is provided.

Key words optical communications; parameter estimation; statistical analysis; photon number splitting attacks; satellite-to-ground quantum key distribution; security; zenith angle; mean photon number

1 引 言

基于弱相干脉冲 (WCP) 光源的量子密钥分配 (QKD) 技术是目前研究最广泛、最接近实用水平的量子密码术。理论上量子密码术提供了前所未有的安全性。但在实际应用中仪器设备性能的不完美和传输信道损耗的存在，给密钥分发 (Eve) 留下了攻击
QKD 系统的脆弱性。目前已有文献从信息论的角度分析了各种攻击（如选择性攻击、联合性攻击、路径攻击、克隆攻击等）对理想 QKD 系统，基于 WCP 光源的 QKD 系统和光纤 QKD 网络的脆弱性的影响。实际上基于攻击的攻击对基于 WCP 光源的 QKD 系统的安全性构成严重威胁。因此，光子数分解 PNS(PPS) 攻击。理论上 PPS 攻击可以检测传输通道上是否有 PNS 攻击存在。PNS 攻击会改变传输光路中的光子数，通过随机发送错误信号并公开检测这些诱骗信号即可判断是否有光子数分解行为发生。在自由空间 QKD 系统（例如使用无限链路和星形链路）中，信道传输损耗的变化具有随机性，因此即使在没有光子数分解的情况下，信道损耗中的光子数也会发生变化，诱骗信号的适用性大大降低。因此，对于基于 WCP 光源的自由空间 QKD 系统，如何保证系统的 QKD 攻击下的安全性成为量子密钥实验化面临的重要挑战之一。

量子密钥术的最终目的是要实现全球化的量子保密通信网络。因此，基于 WCP 光源和自由空间 QKD 线路的量子通讯网络的构建，实现全球化的量子保密通信网络。本文以基于 WCP 光源和 BB84 协议的量子密钥系统为研究对象，提供一种在采用最佳信号策略的 PNS 攻击下，保证密钥安全性的最大关链角和光子数数数等关键技术参数的估算方法，还将对 PNS 攻击时上述关键技术参数对信号 QKD 系统的密钥交换速率和传输容量的影响进行理论分析。

2. 量子脉冲光路与光子数分束攻击

2.1 弱相干脉冲光路

对基于单光子源的偏振编码 QKD 系统，实际系统均采用 WCP 光源来代替理想单光子源。WCP 光源发出的光脉冲的参数 n 服从泊松分布

$$P_{n}(n) = \exp(-\mu) \frac{\mu^n}{n!}$$

其中 \(\mu\) 为每个脉冲所含的平均光子数。为减少多光子脉冲的随机性，一般 \(\mu < 1\)。这种光源的某些脉冲中会出现多于一个光子的情况。例如，对于平均光子数为 \(\mu = 0.1\) 的 WCP 光源，它发出的所有脉冲当中，有 90% 的脉冲是单脉冲，9.5% 的脉冲含有一个光子，0.5% 的脉冲为多光子脉冲（含有一个以上光子）。虽然多光子脉冲的比率很低，但仍然给 Eve 留下了窃听的机会。

2.2 最佳窃听策略的光子数分束攻击

PNS 攻击通常在量子传输路径中插入分光器，以便截取信号脉冲中的部分光子，并通过测量获得干涉密钥的信息。由于 WCP 光源发出的多光子脉冲，PNS 攻击不可不被发现的情况下访问光子，并获得干涉密钥的信息。当单光子探测器无法检测入射光子的数目，即无法分辨光子数态 \(m\) 和 \(n\) \((m \neq n, m > 0, n > 0)\)，因此无法察觉 PNS 存在。另外接收到的信号设备以及量子传输信道均存在传输损耗，因此更容易察觉 PNS 攻击的存在。

由于量子不可克隆定理的限制，Eve 无法窃取单光子。因此在 PNS 攻击时，Eve 的最佳窃听策略是：拦截所有单光子脉冲，窃听所有多光子脉冲，并使被窃听过的多光子脉冲中所含剩余光子都成为密钥。因此，Eve 进行分光所获得的光子数越少，对最后获得更多的密钥信息越有利。Eve 选择部分分光子脉冲中的一个光子，将剩余 \(n - 1\) 个光子转送给 Bob。之后，Eve 将单光子态“真实的”保存下来，直到 Alice 和 Bob 在公开信道上讨论编码为止。通过公开信道的窃听，Eve 撅得用于量子传输的密钥，就可以获得所有由多光子脉冲产生的密钥的确定信息。

为实现上述攻击策略，PNS 攻击应具有以下能力和特性。

（1）Eve 可以对量子数进行量子无损测量 (QND) 因而可以保存单光子数态 \(|n\rangle\) 下的情况波分单光子脉冲和多光子脉冲；

（2）Eve 有能力从单光子数中仅分离出一个光子，将剩余 \(n - 1\) 个光子发送给 Bob；

（3）Eve 可用无损信道替代有损信道，使光子数态 \(|n\rangle\) 直达 Bob；

（4）Eve 具备量子存储和存储，可将分光器取到的量子存储“真实地”保存。

对于 PNS 攻击特性描述中的部分操作（如 QND、量子存储）在当前的技术水平下无法完成，一个实际 QKD 系统的有条件安全性必须在假设 QND 和量子存储的情况下进行分析才是最合适的。因此假定 Eve 具备上述能力。

使用最佳窃听策略进行 PNS 攻击时，Eve 只对光子数态 \(|n\rangle\) (n > 2) 的信号脉冲进行窃听，并且总是触发光子数态 \(|n\rangle\) 到 Bob。因此，不考虑传输损耗时，光子数态 \(|n\rangle\) 到达 Bob 的概率为
\[
S(n) = \begin{cases} 
0, & n = 0, 1 \\
\rho_{n=21} (n+1) = \exp(-\mu) \frac{\mu^{n+1}}{(n+1)!}, & n \geq 2 
\end{cases}
\]

当传输信道上存在采取最佳窃听策略的 PNS 攻击时，Bob 可探测到的光子均来源于多光子脉冲，其光子探测概率为

\[
\rho_n = \left( \prod_{n=1}^{\infty} \left[ 1 - \exp(-\mu) \frac{\mu^n}{n!} \right] \right) \sum_{n=1}^{\infty} \frac{n^2}{2!} \exp(-\mu) \frac{\mu^n}{n!} (1-\eta)^n = \frac{1-\exp(-\mu \eta)}{1-\eta}.
\]

其中 \( \eta \) 为 Bob 侧的光子接收效率，\( \eta \) 为 Bob 侧的光子探测效率。

\section*{3 光子数分束攻击对星地量子密钥分发系统安全传输的影响}

\subsection*{3.1 最大安全传输天顶角}

信道中不存在窃听时，Bob 接收到的光子来源于多光子脉冲和多光子脉冲，其数量为

\[
N_{\eta} = \frac{N}{2} \sum_{n=1}^{\infty} \frac{n^2}{2!} \exp(-\mu \eta) \frac{\mu^n}{n!} (1-\eta)^n = \frac{1}{2} [1-\exp(-\mu \eta)].
\]

其中 \( N \) 为 WCP 光源所发出的总光子数。

3.2 光子数分束攻击对星地量子密钥分配系统容量的影响

当传输信道上存在采取最佳窃听策略的 PNS 攻击时，Bob 接收到的光子来源于多光子脉冲和多光子脉冲，其数量为

\[
N_{\eta} = \frac{N}{2} \sum_{n=1}^{\infty} \frac{n^2}{2!} \exp(-\mu) \frac{\mu^n}{n!} (1-\eta)^n = \frac{1}{2} [1-\exp(-\mu \eta)].
\]

其中 \( \eta \) 为 Bob 侧的光子接收效率，\( \eta \) 为 Bob 侧的光子探测效率。

当使用最佳窃听策略时，QKD 系统安全传输条件为

\[
N_{\eta} \geq N_{\text{max}},
\]

即要求 Bob 接收到的光子数 \( N_{\eta} \) 大于 Eve 通过窃听可以获得的最大光子数 \( N_{\text{max}} \)。由(4)式～(6)式可得

\[
\eta \geq \frac{1}{\mu} \ln \left[ \frac{1-\exp(-\mu \eta)}{\eta} \frac{\eta}{\exp(-\mu \eta)} \right].
\]

(7) 式说明，对于一个实际 QKD 系统，在给定的系统参数下（如平均光子数，接收端光子效率等），光子数传输效率有一个安全下限，小于光子数传输效率使得系统不再安全。QKD 系统光子传输效率 \( \eta \) 取决于量子信道传输速率和信道所用光电子仪器和 QKD 协议，

\[
\eta = \langle T_{\text{vec}} \rangle, \quad \text{g}_{\text{vec}},
\]

其中 \( T_{\text{vec}} \) 描述了量子传输信道的光子传输效率；它往往是一个随机变量。\( g_{\text{vec}} \) 与接收光学天线的功率耦合系数，对实际 QKD 系统，\( g_{\text{vec}} \) 为小于 1 的值。

对星地 QKD 系统，\( T_{\text{vec}} \) 是大气衰减系数 \( \alpha \) 和天顶角 \( \varphi \) 的函数

\[
T_{\text{vec}} = \exp \left[ -\text{sinc} \frac{\theta}{\eta_{\text{vec}}} \alpha(x) dl \right],
\]

由(7)式～(9)式可得，为保证星地 QKD 系统在 PNS 攻击下的绝对安全性，必须满足以下条件：

\[
\Phi \leq \Phi_{\text{vec}} = \arcsin \left\{ \frac{\ln(1/(\eta_{\text{vec}} \eta_{\text{vec}})) - \ln(1-\eta_{\text{vec}}/[\exp(-\mu \eta_{\text{vec}}) - \eta_{\text{vec}} \exp(-\mu \eta_{\text{vec}})])}{\int_{\frac{x \alpha}{\eta_{\text{vec}}}}^{1} \alpha(x) dl} \right\},
\]

(10) 式说明，为保证系统在 PNS 攻击下的安全性，星地 QKD 系统天顶角的取值存在上限，即 \( \Phi_{\text{vec}} \)。
随着发射的平均光子数减小，WCP 光源发出的多光子脉冲（即 Eve 可窃听的脉冲）所占的比例也减小，系统受到 PNS 攻击的可能性变小，但同时 QKD 系统的密钥交换速率也大大降低，最终将导致系统传输容量减小。另外，较小的发射平均光子数可允许较大的传输天顶角，导数系统密钥交换时间的增加，将使系统传输容量有所增加。考虑两种极端情况：1）当 $\phi_{\text{max}} \leq 0 \text{ rad}$ 时，平均光子数 $\mu$ 达到上限，密钥交换速率 $R_{K}$ 达到上限，但系统可进行密钥交换的时间仅为地面站天顶位置的一瞬间，系统容量 $C_{QK}$ 为 0，没有实际意义；2）当 $\phi_{\text{max}} > 0 \text{ rad}$ 时，天顶角 $\phi$ 可取最大值 $\phi_{\text{max}}$，密钥交换时间达到上限，但过小的密钥交换速率 $R_{K}$ 导数，系统容量 $C_{QK}$ 也为 0，没有实际意义。因此平均光子数 $\mu$ 和天顶角 $\phi$ 的取值对 QKD 系统容量的影响是矛盾的，实际应用中需要综合考虑两方面影响，适当选取 $\mu$ 和 $\phi$ 的值。

### 表 1 不同大气衰减时平均光子数与最大天顶角的关系

<table>
<thead>
<tr>
<th>$\mu$/ (photon /pulse)</th>
<th>$\langle a \rangle = 0.023$</th>
<th>$\langle a \rangle = 0.063$</th>
<th>$\langle a \rangle = 0.138$</th>
<th>$\langle a \rangle = 0.184$</th>
</tr>
</thead>
<tbody>
<tr>
<td>km$^{-1}$</td>
<td>km$^{-1}$</td>
<td>km$^{-1}$</td>
<td>km$^{-1}$</td>
<td>km$^{-1}$</td>
</tr>
<tr>
<td>0.05</td>
<td>88</td>
<td>79</td>
<td>58</td>
<td>69</td>
</tr>
<tr>
<td>0.1</td>
<td>86</td>
<td>77</td>
<td>63</td>
<td>74</td>
</tr>
<tr>
<td>0.2</td>
<td>84</td>
<td>73</td>
<td>55</td>
<td>10</td>
</tr>
<tr>
<td>0.3</td>
<td>83</td>
<td>70</td>
<td>48</td>
<td>25</td>
</tr>
<tr>
<td>0.5</td>
<td>82</td>
<td>65</td>
<td>30</td>
<td>70</td>
</tr>
<tr>
<td>$\Delta \phi_{\text{max}}$ ($^\circ$)</td>
<td>4</td>
<td>14</td>
<td>38</td>
<td>70</td>
</tr>
</tbody>
</table>

由于图中所示，大气衰减越大，最大安全传输天顶角减小得越迅速。当大气衰减很小时，随着平均光子数的增加传输天顶角呈缓慢减小趋势。如 $\langle a \rangle = 0.023$ km$^{-1}$ 时，无论 QKD 系统的最优安全传输天顶角仅仅从 $86^\circ$ ($\mu = 0.05$ photon /pulse) 减小到 $82^\circ$ ($\mu = 0.5$ photon /pulse)，$\Delta \phi_{\text{max}} = 4^\circ$。此时，PNS 攻击对最大安全传输天顶角的影响不明显，而当大气衰减较大时，如 $\langle a \rangle = 0.138$ km$^{-1}$，$\Delta \phi_{\text{max}} = 38^\circ$；$\langle a \rangle = 0.184$ km$^{-1}$，$\Delta \phi_{\text{max}}$ 超过了 $70^\circ$。此时，随着大气衰减的增加，PNS 攻击愈发明显地显现出来。对系统可使用的天顶角的限制。因此选择在大气衰减较小的地点建立 QKD 链路，可使系统受 PNS 攻击的影响更小。

图 2 中曲线为实际星地 QKD 系统的平均光子数 $\mu$ 和天顶角 $\phi$ 的取值提供了一个安全上限。即处于图 2 中曲线下方区域内的 $\mu$ 和 $\phi$ 的取值可保证
QKD系统面临 PNS 攻击时得到的密钥仍然安全；任何超过 (10) 式限位的 μ 和 φ 的取值（见图 2 中的曲线下方区域）都使系统面临 PNS 攻击时，所得量子密钥不再安全。在实际应用中，人们可对大衰减进行实际测量，再根据 (10) 式对 μ 和 φ 取值进行估算，（计算中取实测所得最大衰减值），使这两个系统参数值选取在安全区域内，保证密钥在 PNS 攻击下的安全性。

5 结论

实用化的 QKD 系统面临的重要挑战之一是保证密钥在各种窃听方式下的绝对安全性。量子密钥分发 (QKD) 攻击可以拦截单光脉冲并窃听多光子脉冲，这是一种极具威胁的攻击方式。由于 WCP 光源发出的多光子脉冲，传送传输损耗和探测器性能缺陷的存在，窃听者 Eve 通过 PNS 攻击可以窃听所有形成量子密钥的光脉冲而不被察觉，从而对实际 QKD 系统的安全性构成极大威胁。本文给出了基于 WCP 光源的 QKD 系统在 PNS 攻击下的最大安全传输天顶角 

与系统可用平均光子数之和传输信道上的大衰减的关系。通过分析证明，PNS 攻击限制了量子密钥系统中的最大安全传输天顶角和可使用的平均光子数，最终限制了系统的安全密钥交换速率和传输容量。在实际应用中，可对针对不同的大气衰减情况，根据 (11) 式来估算基于 WCP 光源的 QKD 系统在 PNS 攻击下的安全传输天顶角和系统可采用的平均光子数的上限。

参考文献

5. Zhao Chenguang, Li Fei, Zhang Xueyi. The security and attack under spherical case/rewound attack on quantum key distribution under spherical case/rewound attack. Journal of Electronics & Information Technology, 2003, 27(10), 1633-1642
6. Zhao Luming, Li Fei, Zhang Xueyi. The security and attack on quantum key distribution under spherical case/rewound attack[J]. Journal of Electronics & Information Technology, 2005, 27(10), 1633-1642