• 量子信息专栏 •

诱骗态量子密钥分发中不可区分假设的合理性和安全性验证

陈小明[1,2,3]，陈 雷[1,2*]，阎亚龙[3]

(1. 北京邮电大学网络空间安全学院 北京 海淀区 100876；2. 北京电子科技学院 北京 丰台区 100070；
3. 中国科学技术大学网络空间安全学院 合肥 230026)

【摘要】采用贝叶斯决策来区分单诱骗态量子密钥分发中的信号态和诱骗态。分析结果表明，仍然只能得到信号态和诱骗态拥有相同i光子透射率的结论，从而验证了信号态和诱骗态不可区分这一假设的合理性，也验证了诱骗态方法的安全性。此外，分别对比单信号态和信号态+单诱骗态两种情况下光子数分离攻击前后的安全密钥率，发现前者攻击成功，后者攻击失败，这证明了诱骗态存在的必要性，验证了诱骗态方法确实能够抵抗光子数分离攻击，同时也进一步验证了诱骗态方法的安全性。

关 键 词 贝叶斯决策； 诱骗态； 不可区分假设； 光子数分离攻击； 量子密钥分发
中图分类号 O431.2 **文献标志码** A doi:10.12178/1001-0548.2022068

Rationality and Security Verification of Indistinguishability Assumption in Decoy-State Quantum Key Distribution

CHEN Xiaoming[1,2,3], CHEN Lei[1,2*], and YAN Yalong[3]

(1. School of Cyberspace Security, Beijing University of Posts and Telecommunications Haidian Beijing 100876;
2. Beijing Electronic Science and Technology Institute Fengtai Beijing 100070;
3. School of Cyber Science and Technology, University of Science and Technology of China Hefei 230026)

Abstract In this paper, we use Bayesian decision to distinguish signal state from decoy state in one decoy-state quantum key distribution. The analysis results show that we can still only get the conclusion that the signal state and decoy state have the same *i*-photon transmittance, which verifies the rationality of the assumption that signal state and decoy state are indistinguishable, and also verifies the security of decoy-state method. In addition, by comparing the secure key rate of two cases including only signal state and signal state + one decoy state before and after photon number splitting attack, we find the former is successful and the latter is failed. This just proves the necessity of the existence of decoy state, verifies that the decoy-state method can indeed resist photon number splitting attack, and further verifies the security of decoy-state method.

Key words Bayesian decision; decoy state; indistinguishability assumption; photon number splitting attack; quantum key distribution

量子密钥分发 (quantum key distribution, QKD)[1-5] 是一种能够为远距离通信双方 (Alice 和 Bob) 提供信息论安全密钥的技术。密钥的安全性由量子力学原理[6-7] 来保证。由于实际设备的不完美性，QKD 可能面临来自源端和探测端的双重攻击。一方面，理想的 QKD 协议大多需要完美的单光子源。然而，由于当前技术的限制，实际的 QKD 系统经常采用相位随机化后的弱相干态 (weak coherent state, WCS) 光源来代替单光子源。WCS 光源发出的脉冲包含的光子数有时不只一个，窃听者 Eve 就可以利用多光子脉冲来获取密钥而不被 Alice 和 Bob 发现，这就是光子数分离 (photon number splitting, PNS)[8-14] 攻击。该攻击导致了极低的安全成码率和安全传输距离。早期的 PNS 攻击[8-12] 要求 Eve 具有极强的技术水平，不易实现。后来，改进型 PNS[13-14] 甚至在现有的条件下就能实现，这直接威胁了现有

收稿日期：2022－03－06；修回日期：2022－05－22
基金项目：部级基金 (JCKY2019102C001)
作者简介：陈小明 (1964－)，男，博士，研究员，主要从事量子密码方面的研究.
*通信作者：陈雷，E-mail：chenlei1992@bupt.edu.cn

采用 WCS 光源 QKD 协议的安全性。幸运的是，诱骗态方法[15-17]可以很好地抵抗各种类型的 PNS 攻击，显著提高安全成码率和最大安全传输距离。另一方面，QKD 还可能面临来自探测端的攻击，如伪态攻击[18]、时移攻击[19]等。测量设备无关的量子密钥分发 (measurement-device-independent quantum key distribution, MDI-QKD)[20]可以先天免疫所有探测端的攻击，但是其安全密钥率不高，不能突破 PLOB 界[21]。2018 年，陆续提出的双场量子密钥分发 (twin-field quantum key distribution, TF-QKD)[22-24] 成功突破了 PLOB 界，大大提高了安全密钥率和最大安全传输距离。需要注意的是，无论是 MDI-QKD 还是 TF-QKD，只要采用 WCS 光源，就会面临 PNS 攻击的威胁，因此同样需要使用诱骗态方法。总之，对于诱骗态方法的研究仍然很有意义。

在诱骗态 QKD 中，Alice 随机地从不同强度的 WCS 光源中发出信号态或诱骗态给 Bob。同时，Alice 和 Bob 假设 Eve 不能区分信号态和诱骗态，从而导致信号态和诱骗态拥有相同的i光子透射率，这在诱骗态方法中是一个至关重要的假设。并且，这个假设还被应用到诱骗态 QKD 的安全性证明中。实际上，由于信号态和诱骗态的强度差异，二者的光子数概率分布是不同的。基于此，Eve 可以以一定概率区分信号态和诱骗态。一旦 Eve 区分出了信号态和诱骗态，就可以分别对其执行不同的 PNS 攻击策略，使其分别具有不同的i光子透射率。进一步地，如果 Eve 还能够保证攻击前后信号态和诱骗态的测量统计量不变，那么它就可以获得最终密钥而不被 Alice 和 Bob 发现。根据以上分析，基于不同强度导致的光子数概率分布差异，本文采用贝叶斯决策来区分信号态和诱骗态，发现同样只能得到信号态和诱骗态具有相同i光子透射率的结论，这就验证了诱骗态 QKD 中信号态和诱骗态不可区分假设的合理性。另外，分别对比单信号态 QKD 和信号态+单诱骗态 QKD 两种情况下 PNS 攻击前后的安全密钥率，结果表明前者攻击成功，后者攻击失败，这就验证了诱骗态方法确实能够抵抗 PNS 攻击。综合来看，上述两项研究内容验证了诱骗态方法的安全性。

1　诱骗态 QKD

在诱骗态 QKD 中，Alice 随机地发送信号态(s)或者诱骗态(d)。信号态和诱骗态的强度分别为μ和ν。不失一般性，假设$1>\mu>\nu>0$，由于使用 WCS 光源，信号态和诱骗态的光子数均服从泊松分布。具体地，来自信号态和诱骗态的i光子态的概率分别为：

$$P_i^s=\frac{\mathrm{e}^{-\mu}\mu^i}{i!}\quad P_i^d=\frac{\mathrm{e}^{-\nu}\nu^i}{i!} \tag{1}$$

信号态和诱骗态的响应率和量子比特错误率 (quantum bit error rate, QBER) 分别为：

$$Q_\mu=\sum_{i=0}^{\infty}P_i^sY_i^s\quad Q_\nu=\sum_{i=0}^{\infty}P_i^dY_i^d \tag{2}$$

$$Q_\mu E_\mu=\sum_{i=0}^{\infty}P_i^sY_i^se_i^s\quad Q_\nu E_\nu=\sum_{i=0}^{\infty}P_i^dY_i^de_i^d \tag{3}$$

式中，$Y_i^s(Y_i^d)$和$e_i^s(e_i^d)$分别是来自信号态 (诱骗态) 的i光子态的透射率和量子比特错误率。在诱骗态方法中有一个重要假设，即 Eve 无法区分信号态和诱骗态，并由此有以下重要等式：

$$Y_i^s=Y_i^d=Y_i\quad e_i^s=e_i^d=e_i(i\geqslant 0) \tag{4}$$

实际上，由于信号态和诱骗态的强度差异，二者的光子数概率分布是不同的。基于此，Eve 是可以以一定概率区分信号态和诱骗态的，并由此导致式 (4) 可能不再成立。

在诱骗态 QKD[25] 中，使用 WCS 光源的安全密钥率下界为：

$$R^{\mathrm{decoy}}=q\left\{-Q_\mu f(E_\mu)H_2(E_\mu)+Y_1\mu\mathrm{e}^{-\mu}[1-H_2(e_1)]\right\} \tag{5}$$

式中，$q=1/2$表示 BB84 协议的基矢比对效率 (如果使用高效的 BB84 协议[26]，$q\approx 1$)；$f(x)$是双向纠错效率，通常$f(x)\geqslant 1$，香农极限时$f(x)=1$；$H_2(x)=-x\log_2(x)-(1-x)\log_2(1-x)$是二进制香农熵；$Y_1$和$e_1$分别是单光子态的透射率和量子比特错误率，它们可以通过诱骗态方法估计得到。

根据诱骗态 QKD 的后处理方案[25]，可以得到Y_1的下界和e_1的上界：

$$Y_1\geqslant\frac{\mu}{\mu\nu-\nu^2}\left(Q_\nu\mathrm{e}^\nu-Q_\mu\mathrm{e}^\mu\frac{\nu^2}{\mu^2}-E_\mu Q_\mu\mathrm{e}^\mu\frac{\mu^2-\nu^2}{e_0\mu^2}\right)$$
$$e_1\leqslant\frac{E_\mu Q_\mu\mathrm{e}^\mu}{Y_1\mu} \tag{6}$$

在正常信道中，信号态和诱骗态的响应率和量子比特错误率分别是：

$$\begin{aligned} Q_\mu &= Y_0 + 1 - \mathrm{e}^{-\eta\mu} \\ Q_\nu &= Y_0 + 1 - \mathrm{e}^{-\eta\nu} \\ E_\mu Q_\mu &= e_0 Y_0 + e_d(1-\mathrm{e}^{-\eta\mu}) \\ E_\nu Q_\nu &= e_0 Y_0 + e_d(1-\mathrm{e}^{-\eta\nu}) \end{aligned} \tag{7}$$

式中，Y_0和e_0分别是暗计数率和相应的量子比特错误率；e_d是一个光子触发错误探测器的概率，它刻画了光学系统的稳定性；η表示 Alice 和 Bob 之间的总透射率，记作$\eta=\eta_{\mathrm{Bob}}10^{-\alpha L\times 10}$，其中，$\eta_{\mathrm{Bob}}$是 Bob 端的传输效率，包括光学组件的内部传输效率和探测效率，α是衰减系数 (dB/km)，L是信道长度 (km)。

2 贝叶斯决策区分信号态和诱骗态

假设样本只可能来自两个类，并且已知样本的某项特征。在该特征条件下，确定样本来自条件概率较大的类，这就是贝叶斯决策或最大后验概率估计。

不失一般性，假设 Alice 等概率地发送信号态(s)或者诱骗态(d)给 Bob。Eve 拦截该量子态，然后通过量子非破坏性 (quantum non-demolition, QND)[27-28] 测量得到该量子态的光子数。根据贝叶斯决策理论，给定量子态的光子数，就判断该量子态来自信号态和诱骗态中条件概率较大的态。用随机变量M表示截获量子态的来源，$M\in\{s,d\}$，用随机变量N表示截获量子态包含的光子数，$N\in\{0,1,2,\cdots\}$。在光子数为i的条件下，截获的量子态来自信号态和诱骗态的概率分别为：

$$P(M=s|N=i)=\frac{P(M=s,N=i)}{P(N=i)}=\frac{P(M=s)P(N=i|M=s)}{P(N=i)} \tag{8}$$

$$P(M=d|N=i)=\frac{P(M=d,N=i)}{P(N=i)}=\frac{P(M=d)P(N=i|M=d)}{P(N=i)} \tag{9}$$

因为信号态和诱骗态是等概率地从 Alice 发出的，所以有$P(M=s)=P(M=d)=1/2$。式 (8) 和式 (9) 的分母相同，所以如果想比较$P(M=s|N=i)$和$P(M=d|N=i)$的大小，只需比较$P(N=i|M=s)$和$P(N=i|M=d)$的大小。实际上，$P(N=i|M=s)$就是P_i^s。$P(N=i|M=d)$就是P_i^d。给定光子数i、信号态强度μ和诱骗态强度ν，P_i^s和P_i^d很容易通过式 (1) 得到。因此，Eve 只需要知道截获量子态的光子数、信号态和诱骗态的强度，就可以根据贝叶斯决策判断出该量子态来自信号态还是诱骗态。

假设$1>\mu>\nu>0$，通过式 (1) 很容易得到$P_0^s<P_0^d, P_i^s>P_i^d, (i>1)$，就是说，凡是空脉冲，Eve 全都判为来自诱骗态；凡是非空脉冲，Eve 全都判为来自信号态。基于此，Eve 对信号态和诱骗态分别采用不同的透射率。定义Z_i^μ和Z_i^ν分别是 Eve 根据贝叶斯决策设置的信号态和诱骗态i光子的透射率。具体地：

$$Y_0^s=Y_0^d=Z_0^\nu \quad Y_i^s=Y_i^d=Z_i^\mu\ (i\geqslant 1) \tag{10}$$

综合来看，$Y_i^s=Y_i^d=Y_i\ (i\geqslant 0)$，式 (4) 仍然成立。也就是说，Eve 即使利用信号态和诱骗态的唯一差异——强度不同导致的光子数概率分布差异，结合贝叶斯决策来区分信号态和诱骗态，也无法得到更多关于信号态和诱骗态的有用信息，最后同样也只能得到信号态和诱骗态具有相同i光子透射率的结论，从而验证了诱骗态 QKD 中信号态和诱骗态不可区分这一假设的合理性。这里只分析了窃听者 Eve 的攻击对i光子透射率的影响，因为 Eve 的攻击可以做到对量子比特错误率的影响忽略不计[29]。

3 诱骗态方法抵抗光子数分离攻击

在诱骗态方法的后处理过程中，安全密钥只能从单光子成分中得到。在 Eve 执行 PNS 攻击之后，真正安全密钥率的上限[30] 是：

$$R^{\mathrm{Eve}}=Y_1\mu\mathrm{e}^{-\mu} \tag{11}$$

特别地，在文献 [29] 中，有一种 PNS 攻击成功的判别准则，即：

$$R^{\mathrm{sec}}>R^{\mathrm{Eve}} \tag{12}$$

式中，R^{sec}代表的是 Alice 和 Bob 认为安全的密钥率，如果这个值大于 Eve 攻击之后真正安全的密钥率R^{Eve}，这就意味着 Alice 和 Bob 生成的一部分密钥是不安全的。换言之，Eve 已经知道了关于最终密钥的部分信息。因此，可以说 Eve 的攻击是成功的，反之，攻击是失败的。

式 (5) 和式 (11) 中Y_1的值在计算上是不同的。R^{decoy}中的Y_1是 Alice 和 Bob 通过诱骗态方法的后处理过程估计得到的，即式 (6)。R^{Eve}中的Y_1是 Eve 在 PNS 攻击中优化得到的。当 Eve 执行 PNS 攻击时，她可以任意改变i光子的透射率。为了不被 Alice 和 Bob 发现，Eve 需要保持攻击前后的测量统计量不变。假设 Eve 的攻击对误码率的影响忽略不计，因此只需保证响应率这一个统计量不变。根

据文献 [31] 可知，只需考虑包含 6 光子及 6 光子以下脉冲带来的影响即可。即只需要优化$Y_1, Y_2, Y_3, Y_4, Y_5, Y_6$以求得真正的安全密钥率$R^{\mathrm{Eve}}$的上限。特别地，令优化后的$Y_0 = 0$，这是因为如果 Eve 收到了一个空脉冲，她转发任何光子给 Bob 都可能引入误码[29]。

3.1　单信号态 QKD

首先考虑最原始的 BB84-QKD 的情况，即只有一种 WCS 光源发出脉冲——信号态。此时，Alice 和 Bob 认为单光子脉冲和多光子脉冲都能够生成安全密钥，并且认为安全的密钥率为$R^{\mathrm{sec}} = R^{\mathrm{full}}$：

$$R^{\mathrm{full}} = qQ_\mu\left[1 - f(E_\mu)H_2(E_\mu) - H_2(E_\mu)\right] \tag{13}$$

在只有信号态的情况下，根据前面的分析，在 Eve 执行 PNS 攻击之后，真正安全的密钥率$R^{\mathrm{Eve}} = Y_1\mu\mathrm{e}^{-\mu}$的求解可以归结为：

$$\min_{\{Y_1,Y_2,Y_3,Y_4,Y_5,Y_6\}} Y_1\mu\mathrm{e}^{-\mu} \tag{14}$$

当满足以下条件：

$$Q_\mu = Y_0 + 1 - \mathrm{e}^{-\eta\mu} = \sum_{i=1}^{6} P_i^s Y_i \tag{15}$$

式中，$Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 \in [0,1]$。通过计算，可以得到$R^{\mathrm{Eve}}$。如果这个值小于 Alice 和 Bob 认为安全的密钥率R^{sec}，表明 Eve 攻击成功。否则，攻击失败。

利用 Matlab 进行仿真。仿真参数主要来源于文献 [32-33]，是单信号态 QKD 典型实验系统的参数，具体如表 1 所示。

表 1　单信号态 QKD 仿真参数表

方法	基矢比对效率q	暗计数错误率e_0	探测错误率e_d	暗计数率Y_0	Bob传输效率η_{Bob}	衰减系数α	信号态强度μ	纠错效率$f(E_\mu)$
文献[32]	1	0.5	0.033	1.7×10^{-6}	0.045	0.21	0.1	1.22
文献[33]	1	0.5	0.010	4.0×10^{-4}	0.143	0.20	0.1	1.00

采用文献 [32] 和 [33] 中的实验参数，当 QKD 协议中只有一个 WCS 光源发出脉冲即信号态，Eve 执行 PNS 攻击并且保证攻击前后信号态响应率Q_μ不变时，PNS 攻击前后的安全密钥率比较分别如图 1 和图 2 所示。由图 1 和图 2 可知，Alice 和 Bob 认为安全的密钥率R^{full}大于 Eve 攻击之后真正安全的密钥率R^{Eve}，即$R^{\mathrm{sec}} = R^{\mathrm{full}} > R^{\mathrm{Eve}}$，Eve 攻击成功。即，Alice 和 Bob 认为安全的密钥率并不安全。

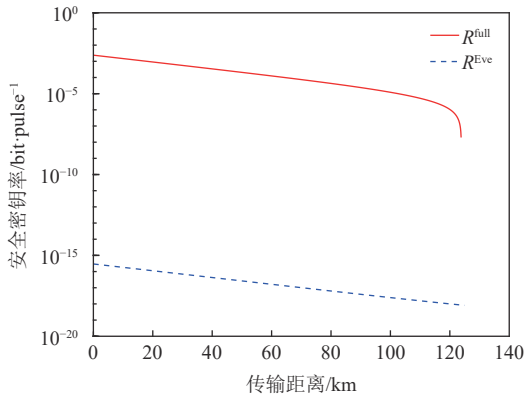

图 1　采用文献 [32] 的实验参数，只有信号态时，PNS 攻击前后的安全密钥率比较

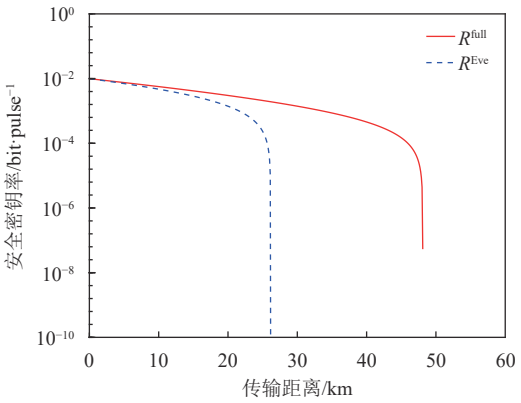

图 2　采用文献 [33] 的实验参数，只有信号态时，PNS 攻击前后的安全密钥率比较

3.2　信号态+单诱骗态 QKD

考虑信号态+单诱骗态 QKD 的情况。此时，Alice 和 Bob 认为只有单光子脉冲能够生成安全密钥，并且认为安全的密钥率为$R^{\mathrm{sec}} = R^{\mathrm{decoy}}$，可以通过式 (5) 计算得到。

在信号态+单诱骗态 QKD 的情况下，根据前面的分析，在 Eve 执行 PNS 攻击之后，真正安全的密钥率$R^{\mathrm{Eve}} = Y_1\mu\mathrm{e}^{-\mu}$的求解可以归结为一个优化问题。为了不被 Alice 和 Bob 发现，Eve 需要保持攻击前后信号态的响应率Q_μ和诱骗态的响应率

Q_ν均不变。上述优化问题具体描述如下：

$$\min_{\{Y_1,Y_2,Y_3,Y_4,Y_5,Y_6\}} Y_1\mu e^{-\mu} \tag{16}$$

当满足以下条件：

$$Q_\mu = Y_0 + 1 - e^{-\eta\mu} = \sum_{i=1}^{6} P_i^s Y_i \tag{17}$$

$$Q_\nu = Y_0 + 1 - e^{-\eta\nu} = \sum_{i=1}^{6} P_i^d Y_i \tag{18}$$

式中，$Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 \in [0,1]$。通过计算，可以得到$R^{\mathrm{Eve}}$。如果这个值小于 Alice 和 Bob 认为安全的密钥率$R^{\mathrm{sec}} = R^{\mathrm{decoy}}$，表明 Eve 攻击成功。否则，攻击失败。

利用 Matlab 进行仿真。仿真参数主要来源于文献 [29, 34]，是信号态+单诱骗态 QKD 典型实验系统的参数，具体如表 2 所示。

采用文献 [29] 和 [34] 的实验参数，在信号态+单诱骗态 QKD 中，Eve 执行 PNS 攻击并且保证攻击前后信号态响应率Q_μ和诱骗态响应率Q_ν均不变，PNS 攻击前后的安全密钥率比较分别如图 3 和图 4 所示。由图 3 和图 4 可知，Alice 和 Bob 认为安全的密钥率R^{decoy}小于 Eve 攻击之后真正安全的密钥率R^{Eve}，即$R^{\mathrm{sec}} = R^{\mathrm{decoy}} < R^{\mathrm{Eve}}$，Eve 攻击失败。换言之，Alice 和 Bob 认为安全的密钥率确实是安全的。特别地，虽然此时用式 (13) 计算的密钥率R^{full}可能仍然大于R^{Eve}，但是 Alice 和 Bob 已不再将其作为安全密钥率。

表 2 信号态+单诱骗态 QKD 仿真参数表

方法	基矢比对效率q	暗计数错误率e_0	探测错误率e_d	暗计数率Y_0	Bob传输效率η_{Bob}	衰减系数α	信号态强度μ	诱骗态强度ν	纠错效率$f(E_\mu)$
文献[29]	1	0.5	0.02	1.00×10^{-7}	0.05	0.21	0.5	0.10	1.00
文献[34]	1	0.5	8.27×10^{-3}	2.11×10^{-5}	2.27×10^{-2}	0.21	0.8	0.12	1.22

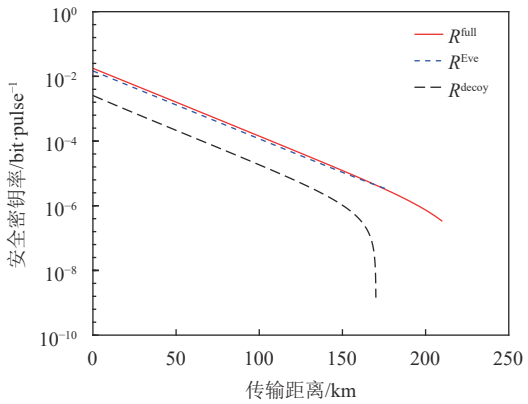

图 3 采用文献 [29] 的实验参数，信号态+单诱骗态 QKD 时，PNS 攻击前后的安全密钥率比较

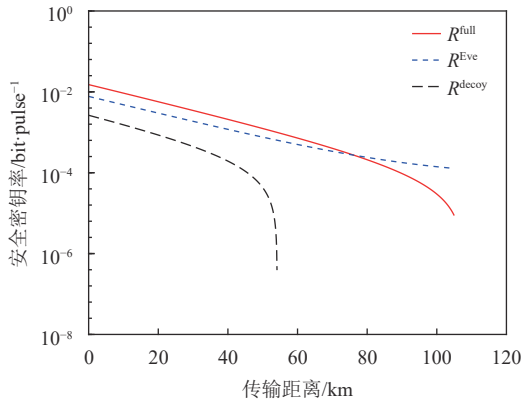

图 4 采用文献 [34] 的实验参数，信号态+单诱骗态 QKD 时，PNS 攻击前后的安全密钥率比较

结合单信号态 QKD 的攻击结果，综合来看，没有诱骗态时，Eve 的 PNS 攻击是成功的；有诱骗态时，Eve 的 PNS 攻击是失败的，这说明了诱骗态存在的必要性，验证了诱骗态方法确实能够抵抗 PNS 攻击。

4 结 束 语

本文首先利用诱骗态方法中信号态和诱骗态的唯一差异，即强度不同导致的光子数概率分布差异，结合贝叶斯决策，验证了诱骗态方法中信号态和诱骗态不可区分这一假设的合理性。另外，本文还通过单信号态 QKD 和信号态+单诱骗态 QKD 的两个例子，分别对比分析 PNS 攻击前后的安全密钥率，仿真结果表明没有诱骗态时，Eve 的 PNS 攻击是成功的；使用诱骗态时，Eve 的 PNS 攻击是失败的，这说明了诱骗态存在的必要性，验证了诱骗态方法确实能够很好地抵抗 PNS 攻击。综合来看，本文从以上两个方面验证了诱骗态方法本身的安全性。

参 考 文 献

[1] BENNETT C H, BRASSARD G. Quantum cryptography: Public key distribution and coin tossing[C]//Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. Bangalore: IEEE, 1984, 175-179.

[2] GISIN N, RIBORDY G, TITTEL W, et al. Quantum cryptography[J]. Reviews of Modern Physics, 2002, 74(1): 145-195.
[3] GISIN N, THEW R. Quantum communication[J]. Nature Photonics, 2007, 1(3): 165-171.
[4] 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.
[5] DUSEK M, LUTKENHAUS N, HENDRYCH M. Progress in optics[M]. [S.l.]: Elsevier, 2006.
[6] WOOTTERS W K, ZUREK W H. A single quantum cannot be cloned[J]. Nature, 1982, 299(5886): 802-803.
[7] DEUTSCH D, EKERT A, JOZSA R, et al. Quantum privacy amplification and the security of quantum cryptography over noisy channels[J]. Physical Review Letters, 1996, 77(13): 2818-2821.
[8] BRASSARD G, LUTKENHAUS N, MOR T, et al. Limitations on practical quantum cryptography[J]. Physical Review Letters, 2000, 85(6): 1330-1333.
[9] LUTKENHAUS N. Security against individual attacks for realistic quantum key distribution[J]. Physical Review A, 2000, 61(5): 052304.
[10] LUTKENHAUS N, JAHMA M. Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack[J]. New Journal of Physics, 2002, 4: 44.1-44.9.
[11] ACIN A, GISIN N, SCARANI V. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks[J]. Physical Review A, 2004, 69(1): 012309.
[12] SCARANI V, ACIN A, RIBORDY G, et al. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations[J]. Physical Review Letters, 2004, 92(5): 057901.
[13] LIU W T, SUN S H, LIANG L M, et al. Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution[J]. Physical Review A, 2011, 86(4): 042326.
[14] LIU D, WANG S, YIN Z Q, et al. The security of decoy state protocol in the partial photon number splitting attack[J]. Chinese Science Bulletin, 2013, 58(31): 3859.
[15] HWANG W Y. Quantum key distribution with high loss: Toward global secure communication[J]. Physical Review Letters, 2003, 91(5): 057901.
[16] WANG X B. Beating the photon-number-splitting attack in practical quantum cryptography[J]. Physical Review Letters, 2005, 94(23): 230503.
[17] LO H K, MA X F, CHEN K. Decoy state quantum key distribution[J]. Physical Review Letters, 2005, 94(23): 230504.
[18] MAKAROV V, ANISIMOV A, SKAAR J. Effects of detector efficiency mismatch on security of quantum cryptosystems[J]. Physical Review A, 2006, 74(2): 022313.
[19] ZHAO Y, FUNG C H F, QI B, et al. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems[J]. Physical Review A, 2008, 78(4): 042333.
[20] LO H K, CURTY M, QI B. Measurement-device-independent quantum key distribution[J]. Physical Review Letters, 2012, 108(13): 130503.
[21] PIRANDOLA S, LAURENZA R, OTTAVIANI C, et al. Fundamental limits of repeaterless quantum communications[J]. Nature Communications, 2017, 8: 15043.
[22] LUCAMARINI M, YUAN Z L, DYNES J F, et al. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters[J]. Nature, 2018, 557(7705): 400.
[23] MA X F, ZENG P, ZHOU H Y. Phase-Matching quantum key distribution[J]. Physical Review X, 2018, 8(3): 031043.
[24] WANG X B, YU Z W, HU X L. Twin-field quantum key distribution with large misalignment error[J]. Physical Review A, 2018, 98(6): 062323.
[25] MA X F, QI B, ZHAO Y, et al. Practical decoy state for quantum key distribution[J]. Physical Review A, 2005, 72(1): 012326.
[26] LO H K, CHAU H F, ARDEHALI M. Efficient quantum key distribution scheme and a proof of its unconditional security[J]. Journal of Cryptology, 2005, 18(2): 133-165.
[27] LECOCQ F, CLARK J B, SIMMONDS R W, et al. Quantum nondemolition measurement of a nonclassical state of a massive object[J]. Physical Review X, 2015, 5(4): 041037.
[28] ZHANG G Y, ZHAO K F. Quantum nondemolition measurement by pulsed oscillation[J]. Physical Review A, 2016, 93(3): 033841.
[29] TANG Y L, YIN H L, MA X F, at al. Source attack of decoy-state quantum key distribution using phase information[J]. Physical Review A, 2013, 88(2): 022308.
[30] MA X F, FUNG C H F, DUPUIS F, et al. Decoy-state quantum key distribution with two-way classical postprocessing[J]. Physical Review A, 2006, 74(3): 032330.
[31] MA X F, FUNG C H F, RAZAVI M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution[J]. Physical Review A, 2012, 86(5): 052305.
[32] GOBBY C, YUAN Z L, SHIELDS A J. Quantum key distribution over 122 km of standard telecom fiber[J]. Applied Physics Letters, 2004, 84(19): 3762-3764.
[33] BOURENNAN M, GIBSON F, KARLSSON A, et al. Experiments on long wavelength (1550nm) “plug and play” quantum cryptography systems[J]. Optics Express, 1999, 4(10): 383-387.
[34] ZHAO Y, QI B, MA X F, et al. Experimental quantum key distribution with decoy states[J]. Physical Review Letters, 2006, 96(7): 070502.

编　辑　蒋　晓