基于四态协议的半量子密钥分发诱骗态模型的有限码长分析*

詹绍康[1)] 王金东[1)†] 董双[1)] 黄偲颖[1)] 侯倾城[1)] 莫乃达[1)] 弥赏[1)]
向黎冰[2)] 赵天明[2)] 於亚飞[2)] 魏正军[1)] 张智明[2)]

1) (华南师范大学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) (华南师范大学信息光电子科技学院, 广东省微纳光子功能材料与器件重点实验室, 广州 510006)

(2023 年 5 月 24 日收到; 2023 年 7 月 18 日收到修改稿)

半量子密钥分发允许一个全量子用户 Alice 和一个经典用户 Bob 共享一对由物理原理保障的安全密钥. 在半量子密钥分发被提出的同时其鲁棒性获得了证明, 随后半量子密钥分发系统的无条件安全性被理论验证. 2021 年基于镜像协议的半量子密钥分发系统的可行性被实验验证. 然而, 可行性实验系统仍旧采用强衰减的激光脉冲, 已有文献证明, 半量子密钥分发系统在受到光子数分裂攻击时仍旧面临密钥比特泄露的风险, 因此, 在密钥分发过程中引入诱骗态并且进行有限码长分析, 可以进一步合理评估密钥分发的实际安全性. 本文基于四态协议的半量子密钥分发系统, 针对仅在发送端 Alice 处加入单诱骗态的模型, 利用 Hoeffding 不等式进行了有限码长情况的安全密钥长度分析, 进而求得安全密钥率公式, 其数值模拟结果表明, 当选择样本量大小为 10^5 时, 能够在近距离情况下获得 10^{-4} bit/s 安全密钥速率, 与渐近情况下的安全密钥率相近, 这对半量子密钥分发系统的实际应用具有非常重要的意义.

关键词: 半量子密钥分发, 诱骗态, Hoeffding 不等式, 有限码长

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.72.20230849

1 引 言

理论上, 基于量子物理定律, 量子密钥分发 (quantum key distribution, QKD) 允许两个量子用户——Alice 和 Bob 无条件安全地共享一对密钥. QKD 的首个协议 [1] 在 1984 年提出并对其理论安全性进行了充分的证明, 之后各种实验方案 [2–4] 的提出和实际 QKD 系统的安全评估的逐渐完善 [5,6] 证明 QKD 的实际可行性. 然而实际 QKD 系统各环节的技术特性和 QKD 理论协议之间存在差别, 使得密钥分发过程会受到各种各样的量子黑客攻击 [7–16]. 例如, QKD 普遍使用的光源是强衰减的激光脉冲, 这使得密钥分发过程中易受到光子数分裂 (photon number splitting, PNS) 攻击 [7–10] 的威胁. 此外, 针对单光子探测器的具体技术特性, 可以展开致盲攻击、探测效率不匹配攻击、后向荧光边信道攻击等 [11–16], 导致通信双方在不知情的情况下被窃听者窃取密钥信息. 为了抵抗针对单光子探测器的攻击, 测量设备无关量子密钥分发 (MDI-QKD)[17] 被提出, 随后双场量子密钥分发协议 (TF-QKD)[18] 和模式匹配量子密钥分发协议 (MP-QKD)[19] 等能够抵御针对单光子探测器的攻击, 同时使传输距离变得更长的协议被提出. 由于 TF-QKD 在实验上

* 国家自然科学基金 (批准号: 62071186, 61771205) 和广东省重点实验室基金 (批准号: 2020B1212060066) 资助的课题.

† 通信作者. E-mail: wangjindong@m.scnu

© 2023 中国物理学会 Chinese Physical Society

对于实验条件要求较高, 许多 TF-QKD 的变体[20–23]提出, 它们在实验上相较于 TF-QKD 比较容易实现. 2022 年谢元梅等[24]提出异步 MDI-QKD, 在 TF-QKD 的基础上进一步提高测量设备无关量子密钥分发的传输距离. 诱骗态协议[25–30]和单光子类协议——SARG04[31]协议被提出以抵御 PNS 攻击, 其中诱骗态协议得到了广泛应用. 考虑实际应用发送的脉冲数量是有限的, 有限码长情况下 QKD 系统的分析相继完成[32–34], 此外 Lim 等[35]和 Rusca 等[36]分别完成了双诱骗态 QKD 系统和单诱骗态 QKD 系统的有限码长情况下安全密钥速率的分析, 并指出有限码长情况下单诱骗态 QKD 系统的密钥传输速率相较于双诱骗态 QKD 系统有一定的优势.

半量子密钥分发 (semi-quantum key distribution, SQKD) 在 2007 年由 Boyer 等[37]提出, 它 (四态协议, BKM-07) 允许一个量子用户 Alice 和一个经典用户 Bob 安全的共享一对密钥. 随后基于实际实现的角度, 小于四态协议[38]、镜像协议[39]被提出, 这些协议提出的同时, 它们的理论安全性得到了证明, 尤其是对于独立攻击和集体攻击[40–44], 同时也确定了安全比特率. 2021 年王金东课题组[45]实现了基于镜像协议的 SQKD 实验实现, 验证了实际 SQKD 系统的实验可行性. 与 QKD 系统相对应地, SQKD 的理论安全性证明都是基于单光子源进行的, 因此实际系统的 SQKD 也会受到 PNS攻击的威胁. 弥赏等[46]在 2022 年提出了针对于 SQKD 系统的联合 PNS 攻击, 证明了一定条件下的PNS 攻击能使窃听者 Eve 在通信双方没有察觉的情况下窃取信息. 与 QKD 系统相似, SQKD 系统在密钥分发过程中添加诱骗态能较好地抵抗 PNS攻击, 因此基于 Alice 发送有限脉冲的有限码长安全评估是必要的, 传输的脉冲数量过少会导致安全密钥速率过低, 需要较多的时间生成安全密钥, 使通信效率降低; 反之传输的脉冲数量过多会需要较多的光资源, 使通信成本提高, 因此需要寻找一个合适的样本量大小来获得最佳的安全密钥速率并确定安全密钥速率的大小.

本文首先建立了基于 BKM-07 协议的仅量子用户端加入单诱骗态 SQKD 系统的模型, 随后为该系统提供了有限码长情况下简洁而严密的安全密钥界限: 基于熵的不确定关系和 Hoeffding 不等式[47]对有限的传输脉冲数量进行错误估计, 推导出针对一般攻击有效的安全密钥界限, 它可以通过几个简单的探测事件界限公式进行推导; 随后模拟实际探测情况, 以 Alice 探测响应的数量固定为前提, 推导出 Alice 需要发送的总脉冲数, 进而求出安全密钥率公式并进行数值模拟; 最后对数值模拟结果进行了讨论和总结.

2 基于四态协议 SQKD 系统的诱骗态模型

本节将会介绍四态协议 (BKM-07 协议) 的模型, 随后提出添加诱骗态的方法并详细说明密钥分发过程. BKM-07 协议的密钥分发过程见图 1.

1) Alice 随机均匀地选择一个比特值并将该值记录到集合 y_i 中, 接着, 它随机均匀地从 X 基和 Z 基中选择一个作为对应比特的基并记录到集合 a_i, Alice 根据两个集合中位置 i 的值对光脉冲进行调制, 最后将光脉冲发送给 Bob.

2) Bob 随机均匀地选择对到达的光脉冲实施 SIFT 操作或 CTRL 操作, 并将所选择的操作记录到集合 c_i. 对于选择 SIFT 操作的脉冲, Bob 以 Z

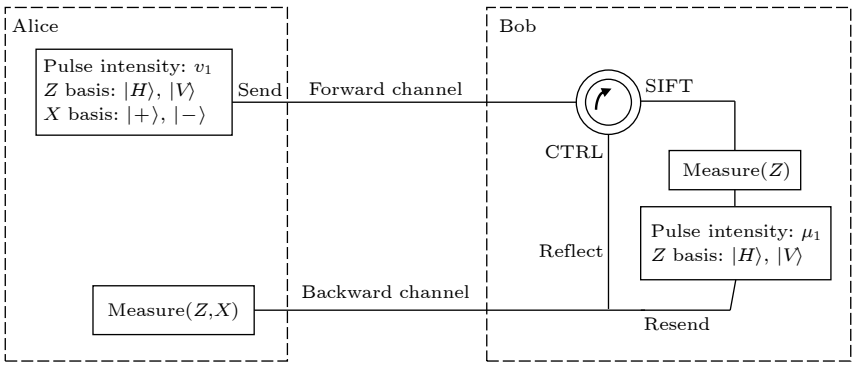

图 1 BKM-07 协议模型

Fig. 1. BKM-07 protocol model.

基进行测量, 并将结果记录到集合 s_i, 随后根据测量结果, 以 Z 基和脉冲强度 μ_1 在相同位置重发光脉冲; 对于选择 CTRL 操作的脉冲, Bob 不进行任何操作, 将光脉冲反射回到 Alice 端.

3) Alice 对返回的每一个脉冲根据自己发送时使用的基进行测量, 并将以 Z 基进行测量得到的结果记录到集合 z_i, 以 X 基进行测量得到的结果记录到集合 x_i.

4) Alice 和 Bob 在经典信道公布集合 a_i 和 c_i, 随后双方计算响应率及错误率是否符合预期, 若不符合预期则认为密钥分发过程被窃听, 停止本次密钥分发; 若符合预期则生成期望长度的初始密钥执行后处理步骤, 最后生成安全密钥.

实际情况中, 即便 SQKD 系统中包含着天然诱骗态 (CTRL 操作), 但它仍有可能受到 PNS 攻击而导致密钥信息泄露, 并且实际情况中生成的初始密钥长度是与各个事件探测响应的数量密切相关的, 因此以下将描述诱骗态模型下密钥分发的过程并说明通信双方如何得到长度为 l 的安全密钥, 同时为了进行有限码长分析给出相应的变量定义, 如图 2 所示.

1) Alice 随机均匀地选择一个比特值并将该值记录到集合 y_i 中, 接着, 它随机均匀地从 X 基和 Z 基中选择一个作为对应比特的基并记录到集合 a_i, 并以概率 p_{v_1} 和 $1-p_{v_1}$ 选择脉冲强度 v_1 或 v_2 ($v_1>v_2>0$) 并将数据记录到集合 b_i, 最终 Alice 根据 3 个集合中位置 i 的值对光脉冲进行调制, 随后发送给 Bob.

2) Bob 随机均匀地选择对到达的光脉冲实施 SIFT 操作或 CTRL 操作, 并将所选择的操作记录到集合 c_i. 对于选择 SIFT 操作的脉冲, Bob 以 Z 基进行测量, 并将结果记录到集合 s_i, 随后根据测量结果, 以 Z 基和脉冲强度 μ_1 ($\mu_1>v_1+v_2$) 在相同位置重发光脉冲; 对于选择 CTRL 操作的脉冲, Bob 不进行任何操作, 将光脉冲反射回到 Alice 端.

3) Alice 对返回的每一个脉冲根据自己发送时使用的基进行测量, 并将以 Z 基进行测量的结果记录到集合 z_i, 以 X 基进行测量的结果记录到集合 x_i.

4) Alice 和 Bob 在经典信道公布集合 a_i, b_i, c_i, 随后双方计算各脉冲强度的响应率是否符合预期, 若符合预期则筛选生成由 Alice 选择 Z 基且 Bob 选择 SIFT 操作发送的光脉冲导致测量响应的结果组成的、双方共享的集合 SZ, Alice 分别生成由 Bob 选择 CTRL 操作且 Alice 以 Z 基发送和以 X 基发送的光脉冲导致测量响应的结果组成的集合 CZ 和 CX; 重复步骤 1)—步骤 3) 直到 $|SZ|\geqslant n_{\rm SZ}$, $|CZ|\geqslant n_{\rm CZ}$ 和 $|CX|\geqslant n_{\rm CX}$.

5) Alice 和 Bob 从集合 SZ 中随机选择大小为 $n_{\rm SZ}$ 的样本作为初始密钥 ($SZ_{\rm A}, SZ_{\rm B}$), 随后 Alice 根据集合 CX 估计相应的错误比特数 $m_{{\rm CX},k}$, 接着它们计算初始密钥中的真空事件 $s_{{\rm SZ},0}$ 和单光子事件 $s_{{\rm SZ},1}$, 最后它们计算初始密钥中单光子事件的相位错误的数量 $c_{{\rm SZ},1}$, 并估计实际相位错误率 $\phi_{\rm SZ}=c_{{\rm SZ},1}/s_{{\rm SZ},1}$, 同时判断实际相位错误率是否低于预期值, 若不满足则终止密钥分发, 若满足则进行步骤 6).

6) 首先 Alice 和 Bob 进行错误校验, 假设它们根据预期的相位错误率进行校正, 则它们会揭示 $\lambda_{\rm EC}$ 位信息; 接着, 它们执行错误验证步骤, 确保两者共享相同的密钥, 这个过程中它们使用两个通用哈希函数 [14], 会揭示 $\log_2 1/\varepsilon_{\rm hash}$ 位信息, 其中 $\varepsilon_{\rm hash}$

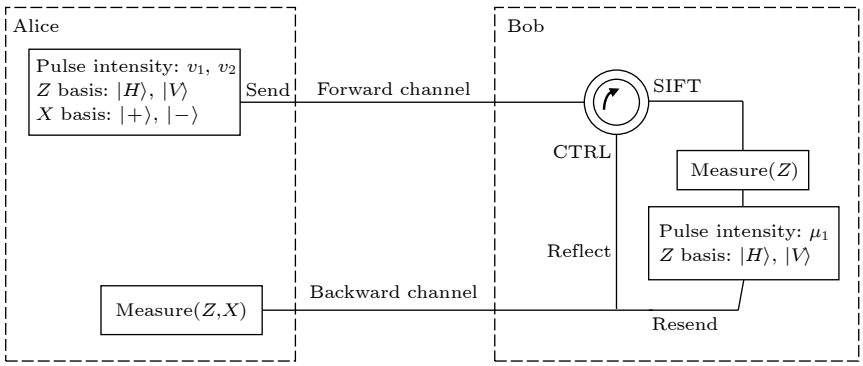

图 2 基于 BKM-07 协议的诱骗态 SQKD 模型

Fig. 2. Decoy SQKD model based on BKM-07 protocol.

是指一对非相同密钥能够通过错误验证步骤的概率; 最后, 它们对密钥进行隐私放大, 提取长度为 l 的密钥对 $(S_{\rm A}, S_{\rm B})$.

3 有限码长分析

本节将基于第 2 节提出的 SQKD 模型进行有限码长的安全密钥速率分析, 分为 4 部分: 安全分析、事件界限、探测和错误模拟、数值模拟. 安全分析利用熵的不确定关系推导出以 Eve 所获得的信息为条件的原始安全密钥的最小长度公式; 事件界限根据密钥长度公式中的项, 基于 Hoeffding 不等式对所需探测事件的数量进行有限码长情况下的界限值估计; 探测模拟和错误模拟将根据模拟分析各类光脉冲的探测概率及各类探测事件之间预期数目的关系; 数值模拟将基于光纤通信的信道模型对有限码长分析的结果进行数据模拟. 最后对数值模拟的结果进行了详细的讨论.

3.1 安全分析

安全分析主要思路是利用熵不确定性关系来建立以 Eve 获得的信息为条件的原始密钥的最小平滑熵的界限. 首先, 定义 E' 为窃听者 Eve 获得的关于初始密钥 $SZ_{\rm A}$ 的信息, E 为经过纠错及错误验证步骤后窃听者 Eve 获得的关于初始密钥 $SZ_{\rm A}$ 的信息. 使用两个通用哈希函数 [48] 进行隐私放大可以获得长度为 l 的 $\varepsilon_{\rm sec}$-安全密钥:

$$l = H_{\min}^{v}\left(SZ_{\rm A}|E'\right) - 2\log_2\frac{1}{\bar{v}}, \tag{1}$$

其中 $\varepsilon_{\rm sec} \geqslant v + \bar{v}$, $H_{\min}^{v}\left(SZ_{\rm A}|E'\right)$ 为条件最小平滑熵.

由于 Alice 和 Bob 在纠错和错误校验过程中会揭露 $\lambda_{\rm EC}$ 和 $\log_2(2/\varepsilon_{\rm cor})$ 位信息, 因此可以得到 $H_{\min}^{v}\left(SZ_{\rm A}|E'\right)$ 与 $H_{\min}^{v}\left(SZ_{\rm A}|E\right)$ 的不等关系:

$$H_{\min}^{v}\left(SZ_{\rm A}|E'\right) \geqslant H_{\min}^{v}\left(SZ_{\rm A}|E\right) - \lambda_{\rm EC} - \log_2\frac{2}{\varepsilon_{\rm cor}}, \tag{2}$$

将 $SZ_{\rm A}$ 分解为 $SZ_{\rm A}^{\rm V}$, $SZ_{\rm A}^{\rm S}$ 和 $SZ_{\rm A}^{\rm M}$, 即将初始密钥中的各个比特分解成由探测单光子脉冲、空脉冲及多光子脉冲得到的比特, 由于 Eve 具有光子数分辨能力, 因此认为 Eve 能执行这种分解. 为了方便后面的计算, 令误差项 $v = 2\alpha_1 + \alpha_2 + (\alpha_3 + 2\alpha_4 + \alpha_5)$, α_1, α_2, α_3, α_4 和 α_5 均大于 0, 随后应用最小平滑熵的广义链式规则 [49] 可以得到:

$$\begin{aligned} &H_{\min}^{v}\left(SZ_{\rm A}|E\right) \\ \geqslant\ &H_{\min}^{\alpha_1}(SZ_{\rm A}^{\rm S}|SZ_{\rm A}^{\rm V}SZ_{\rm A}^{\rm M}E) \\ &+H_{\min}^{\alpha_3+2\alpha_4+\alpha_5}(SZ_{\rm A}^{\rm V}SZ_{\rm A}^{\rm M}|E) - 2\log_2\frac{1}{\alpha_2} - 1, \end{aligned} \tag{3}$$

$$\begin{aligned} &H_{\min}^{\alpha_3+2\alpha_4+\alpha_5}\left(SZ_{\rm A}^{\rm V}SZ_{\rm A}^{\rm M}|E\right) \\ \geqslant\ &H_{\min}^{\alpha_4}\left(SZ_{\rm A}^{\rm M}|SZ_{\rm A}^{\rm V}E\right) + H_{\min}^{\alpha_5}\left(SZ_{\rm A}^{\rm V}|E\right) \\ &- 2\log_2\frac{1}{\alpha_3} - 1. \end{aligned} \tag{4}$$

对于 (4) 式的 $H_{\min}^{\alpha_4}\left(SZ_{\rm A}^{\rm M}|SZ_{\rm A}^{\rm V}E\right)$, 我们认为多光子脉冲中的信息是能被 Eve 全部窃取的, 因此不等式 $H_{\min}^{\alpha_4}\left(SZ_{\rm A}^{\rm M}|SZ_{\rm A}^{\rm V}E\right) \geqslant 0$ 成立; 对于空脉冲产生响应而形成的密钥信息, Eve 是完全不知道的, 并且该脉冲以相同的概率生成比特 0 或比特 1, 因此可以得到下面不等式成立:

$$\begin{aligned} H_{\min}^{\alpha_5}\left(SZ_{\rm A}^{\rm V}|E\right) &\geqslant E_{\min}\left(SZ_{\rm A}^{\rm V}|E\right) = E_{\min}(SZ_{\rm A}^{\rm V}) \\ &= \log_2 2^{s_{\rm SZ,0}} = s_{\rm SZ,0}. \end{aligned} \tag{5}$$

同时, 应用熵的不确定性 [50] 并考虑 Eve 通过 PNS 攻击无法窃取单光子脉冲中的信息, 即 Eve 关于 $SZ_{\rm A}^{\rm S}$ 的确定性不会大于 $SZ_{\rm A}^{\rm S}$ 中的错误比特数可得

$$H_{\min}^{\alpha_1}\left(SZ_{\rm A}^{\rm S}|SZ_{\rm A}^{\rm V}SZ_{\rm A}^{\rm M}E\right) \geqslant s_{\rm SZ,1}\left[1 - h\left(\frac{c_{\rm SZ,1}}{s_{\rm SZ,1}}\right)\right], \tag{6}$$

其中 $c_{\rm SZ,1}$ 为 $SZ_{\rm A}^{S}$ 与 $SZ_{\rm B}^{S}$ 之间不相同比特的数目, 使用文献 [51] 中给出的无替换结果的随机抽样进行估计, 基于超几何分布的近似技术, 可以得到下面的不等式以至少的 $1-\alpha_1$ 概率被满足:

$$\frac{c_{\rm SZ,1}^{u}}{s_{\rm SZ,1}^{\rm l}} \leqslant \frac{v_{\rm CX,1}^{u}}{s_{\rm CX,1}^{\rm l}} + \sqrt{\frac{\left(s_{\rm SZ,1}^{\rm l} + s_{\rm CX,1}^{\rm l}\right)\left(1 - \dfrac{v_{\rm CX,1}^{u}}{s_{\rm CX,1}^{\rm l}}\right)\dfrac{v_{\rm CX,1}^{u}}{s_{\rm CX,1}^{\rm l}}}{s_{\rm SZ,1}^{\rm l}s_{\rm CX,1}^{\rm l}\ln 2}\log_2\frac{s_{\rm SZ,1}^{\rm l} + s_{\rm CX,1}^{\rm l}}{\alpha_1^2 s_{\rm SZ,1}^{\rm l}s_{\rm CX,1}^{\rm l}\left(1 - \dfrac{v_{\rm CX,1}^{u}}{s_{\rm CX,1}^{\rm l}}\right)\dfrac{v_{\rm CX,1}^{u}}{s_{\rm CX,1}^{\rm l}}}}. \tag{7}$$

综合以上所有的公式, 能够得到密钥长度公式为

$$l \leqslant s^{\mathrm{l}}_{\mathrm{SZ},0} + s^{\mathrm{l}}_{\mathrm{SZ},1}\left[1 - h\left(\frac{c^{u}_{\mathrm{SZ},1}}{s^{\mathrm{l}}_{\mathrm{SZ},1}}\right)\right] - \lambda_{\mathrm{EC}} - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}\beta}, \tag{8}$$

其中 β 为误差项, 考虑有限码长情况引入的误差项以及密钥长度公式推导中引入的误差项, 设 $\alpha_4 = \alpha_5 = 0$ 可以得到安全性误差 $\varepsilon_{\mathrm{sec}}$ 为

$$\varepsilon_{\mathrm{sec}} = 2(2\alpha_1 + \alpha_2 + \alpha_3) + \bar{v} + 5\varepsilon_1 + 2\varepsilon_2 + 3\varepsilon_3, \tag{9}$$

式中, ε_1, ε_2 和 ε_3 均为有限码长情况下引入的误差项, 其前面的系数为各自对应的 Hoeffding 不等式 (10) 式、(12) 式、(14) 式在密钥长度公式中满足的次数. 为了得到较好的安全性, 令每一个误差项均为同一个值 ε, 得到 $\varepsilon_{\mathrm{sec}} = 19\varepsilon$, 由于有 7 个误差项且 $\log_2(1/\beta)$ 为所有误差项对安全密钥长度的影响, 最终取 $\beta = (\varepsilon_{\mathrm{sec}}/19)^7$, 因此密钥长度公式表示为

$$\begin{aligned} l \leqslant\ & s^{\mathrm{l}}_{\mathrm{SZ},0} + s^{\mathrm{l}}_{\mathrm{SZ},1}\left[1 - h\left(\frac{c^{u}_{\mathrm{SZ},1}}{s^{\mathrm{l}}_{\mathrm{SZ},1}}\right)\right] - \lambda_{\mathrm{EC}} \\ & - 7\log_2\frac{19}{\varepsilon_{\mathrm{sec}}} - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}}, \end{aligned} \tag{10}$$

式中, 未知项 $s^{\mathrm{l}}_{\mathrm{SZ},0}$, $s^{\mathrm{l}}_{\mathrm{SZ},1}$, $\dfrac{c^{u}_{\mathrm{SZ},1}}{s^{\mathrm{l}}_{\mathrm{SZ},1}}$ 的界限将在 3.2 节中进行详细推导.

3.2 事件界限

本节提供了密钥长度公式中将会使用到的探测事件界限 $s_{\mathrm{SZ},0}$, $s_{\mathrm{SZ},1}$ 和 ϕ_{SZ} 的详细信息, 界限的分析基于强衰减激光脉冲的泊松分布和 Hoeffding 不等式结合. 由于 SQKD 系统中 Z 基与 X 基的光脉冲的探测概率显然不同, 因此分析中将区分 X 基与 Z 基的光脉冲进行分析.

根据诱骗态 SQKD 的模型可以得到, 从 Bob 端发送出来的脉冲 (不区分 SIFT 操作和 CTRL 操作) 强度的可能值为 $\mu_1, \eta_{\mathrm{c}}v_1$和$\eta_{\mathrm{c}}v_2$, 令 $\mu_2 = \eta_{\mathrm{c}}v_1$, $\mu_3 = \eta_{\mathrm{c}}v_2$ 和 $K = [\mu_1, \mu_2, \mu_3]$, 根据预先的设定可得 $\mu_1 \geqslant \mu_2 + \mu_3$, $\mu_2 > \mu_3 \geqslant 0$, 由于每个脉冲只有强度不相同, 对于窃听者 Eve 而言, 无法区分每个脉冲的强度, 这使得 Eve 即使实施 PNS 攻击, 通信双方也能察觉.

考虑 Bob 以 Z 为基对脉冲进行编码的情况, 并且设 $s_{Z,n}$ 为 Bob 发送 Z 基下 n 光子脉冲且 Alice 探察到的次数, $n_{\mathrm{Z}} = \sum_{n=0}^{\infty} s_{Z,n}$ 为预期 Bob 发送 Z 基光脉冲且 Alice 探测到的次数, 在渐近极限中, 脉冲强度为 k 的探测次数 $n^{*}_{\mathrm{Z},k}$ 为

$$n^{*}_{\mathrm{Z},k} = \sum_{n=0}^{\infty} p_{n|k}s_{\mathrm{Z},n},\ \forall k \in K. \tag{11}$$

此时考虑一个有限码长的统计场景, 可以使用 Hoeffding 不等式 [47] 进行估计. 通过 Hoeffding 不等式可以得到探测到的次数 $n_{\mathrm{Z},k}$ 与相应渐近情况的 $n^{*}_{\mathrm{Z},k}$ 之差满足一定约束关系的概率为

$$\left(\left|n^{*}_{\mathrm{Z},k} - n_{\mathrm{Z},k}\right| \leqslant \delta(n_{\mathrm{Z}}, \varepsilon_1)\right) \geqslant 1 - 2\varepsilon_1, \tag{12}$$

其中 $\delta(n_{\mathrm{Z}}, \varepsilon_1) = \sqrt{n_{\mathrm{Z}}\ln(1/\varepsilon_1)/2}$.

相同的考虑对于 Bob 以 X 为基对脉冲进行编码的情况也是成立的. 设 $s_{\mathrm{CX},n}$ 为 Bob 发送 X 基下 n 光子脉冲且 Alice 探察到的次数, $n_{\mathrm{CX}} = \sum_{n=0}^{\infty} s_{\mathrm{CX},n}$ 为预期 Bob 发送 X 基的光脉冲且 Alice 探测到的次数, 在渐近极限中, 脉冲强度为 k 的探测次数 $n^{*}_{\mathrm{CX},k}$ 为

$$n^{*}_{\mathrm{CX},k} = \sum_{n=0}^{\infty} p_{n|k}s_{\mathrm{CX},n},\ \forall\, k \in K. \tag{13}$$

与前面的情况类似, 对于有限码长统计情况下的约束如下:

$$\left(\left|n^{*}_{\mathrm{CX},k} - n_{\mathrm{CX},k}\right| \leqslant \delta(n_{\mathrm{CX}}, \varepsilon_2)\right) \geqslant 1 - 2\varepsilon_2. \tag{14}$$

接着考虑 Bob 以 X 基对脉冲进行编码而 Alice 探测结果出现错误的错误率估计. 相似地, 设 $v_{\mathrm{CX},n}$ 为 Bob 发送 X 基下 n 光子脉冲且 Alice 探测结果出现错误的次数, $m_{\mathrm{CX}} = \sum_{n=0}^{\infty} v_{\mathrm{CX},n}$ 为预期 Bob 发送 X 基的所有光脉冲中 Alice 探测结果出现错误的次数, 在渐近极限中, 脉冲强度为 k 的探测次数 $m^{*}_{\mathrm{CX},k}$ 为

$$m^{*}_{\mathrm{CX},k} = \sum_{n=0}^{\infty} p_{n|k}v_{\mathrm{CX},n},\ \forall\, k \in K. \tag{15}$$

类似地, 对于有限码长统计情况下的约束如下:

$$Pr\left(\left|m^{*}_{\mathrm{CX},k} - m_{\mathrm{CX},k}\right| \leqslant \delta(m_{\mathrm{CX}}, \varepsilon_3)\right) \geqslant 1 - 2\varepsilon_3. \tag{16}$$

为了找到各个事件的解析解, 必须定义条件概率 $p_{n|k}$. 通过使用贝叶斯规则和相干态脉冲中光子分布可以得到下式成立:

$$p_{n|k} = \frac{p_k}{\tau_n}p_{k|n} = \frac{p_k}{\tau_n}\cdot\frac{\mathrm{e}^{-k}k^n}{n!}, \tag{17}$$

其中 $\tau_n = \sum_{k\in K} p_k\mathrm{e}^{-k}k^n/n!$ 表示 Bob 发送一个 n 光子脉冲的总概率. 后文中将会分别计算 $s_{\mathrm{Z},0}$, $s_{\mathrm{Z},1}$ 和 $s_{\mathrm{CX},1}$ 的下限以及 $v_{\mathrm{CX},1}$ 的上限.

1) Z 基中真空脉冲事件 $s_{\mathrm{Z},0}$ 的下限.

将 (11) 式代入具有不同脉冲强度的两个方程可以得到:

$$\begin{aligned}&\frac{\mu_2 \mathrm{e}^{\mu_3} n^*_{\mathrm{Z},\mu_3}}{p_{\mu_3}} - \frac{\mu_3 \mathrm{e}^{\mu_2} n^*_{\mathrm{Z},\mu_2}}{p_{\mu_2}} \\ &= \frac{(\mu_2-\mu_3)\, s_{\mathrm{Z},0}}{\tau_0} - \mu_2\mu_3 \\ &\quad \times \sum_{n=2}^{\infty} \frac{\left(\mu_2^{n-1} - \mu_3^{n-1}\right) s_{\mathrm{Z},n}}{n!\cdot\tau_n},\end{aligned} \tag{18}$$

其中等式右边的第二项对于 $\mu_2-\mu_3$ 是非负的, 因此通过对上式进行重写可以得到 $s_{\mathrm{Z},0}$ 的下限为

$$s^*_{\mathrm{Z},0} \geqslant \frac{\tau_0}{(\mu_2-\mu_3)} \left(\frac{\mu_2 \mathrm{e}^{\mu_3} n^*_{\mathrm{Z},\mu_3}}{p_{\mu_3}} - \frac{\mu_3 \mathrm{e}^{\mu_2} n^*_{\mathrm{Z},\mu_2}}{p_{\mu_2}} \right). \tag{19}$$

随着 μ_3 趋于 0, 界限会变紧.

2) Z 基中单光子脉冲事件 $s_{\mathrm{Z},1}$ 的下限.

类似地, 根据两个方程之差 $\dfrac{\mathrm{e}^{\mu_2} n^*_{\mathrm{Z},\mu_2}}{p_{\mu_2}} - \dfrac{\mathrm{e}^{\mu_3} n^*_{\mathrm{Z},\mu_3}}{p_{\mu_3}}$ 可以得到:

$$\begin{aligned}&\frac{\mathrm{e}^{\mu_2} n^*_{\mathrm{Z},\mu_2}}{p_{\mu_2}} - \frac{\mathrm{e}^{\mu_3} n^*_{\mathrm{Z},\mu_3}}{p_{\mu_3}} \\ &= \frac{(\mu_2-\mu_3)\, s_{\mathrm{Z},1}}{\tau_1} + \sum_{n=2}^{\infty} \frac{\left(\mu_2^n - \mu_3^n\right) s_{\mathrm{Z},n}}{n!\cdot\tau_n}.\end{aligned} \tag{20}$$

对于 $\mu_1 \geqslant \mu_2+\mu_3$ 和 $n \geqslant 2$ 可得以下不等式成立:

$$\begin{aligned}&\mu_2^n - \mu_3^n = \mu_2^2\mu_2^{n-2} - \mu_3^2\mu_3^{n-2} \\ &\leqslant \left(\mu_2^2 - \mu_3^2\right)\mu_1^{n-2} = \frac{\left(\mu_2^2-\mu_3^2\right)}{\mu_1^2}\mu_1^n.\end{aligned} \tag{21}$$

将不等式 (20) 式代入 (19) 式可得

$$\begin{aligned}&\frac{\mathrm{e}^{\mu_2} n^*_{\mathrm{Z},\mu_2}}{p_{\mu_2}} - \frac{\mathrm{e}^{\mu_3} n^*_{\mathrm{Z},\mu_3}}{p_{\mu_3}} \\ &\leqslant \frac{(\mu_2-\mu_3)\, s_{\mathrm{Z},1}}{\tau_1} + \frac{\left(\mu_2^2-\mu_3^2\right)}{\mu_1^2} \sum_{n=2}^{\infty} \frac{\mu_1^{\mathrm{n}} s_{\mathrm{Z},n}}{n!\cdot\tau_n},\end{aligned} \tag{22}$$

其中不等式右边的求和项可由下式表示:

$$\sum_{n=2}^{\infty} \frac{\mu_1^n s_{\mathrm{Z},n}}{n!\cdot\tau_n} = \frac{\mathrm{e}^{\mu_1} n^*_{\mathrm{Z},\mu_1}}{p_{\mu_1}} - \frac{s_{\mathrm{Z},0}}{\tau_0} - \frac{\mu_1 s_{\mathrm{Z},1}}{\tau_1}. \tag{23}$$

将不等式右边的求和项使用 (23) 式替代并重写后, 可以得到 $s_{\mathrm{Z},1}$ 的下限.

$$\begin{aligned}s^*_{\mathrm{Z},1} \geqslant \frac{\mu_1\tau_1}{\mu_1(\mu_2-\mu_3) - \left(\mu_2^2-\mu_3^2\right)} &\left[\frac{\mathrm{e}^{\mu_2} n^*_{\mathrm{Z},\mu_2}}{p_{\mu_2}} - \frac{\mathrm{e}^{\mu_3} n^*_{\mathrm{Z},\mu_3}}{p_{\mu_3}} \right. \\ &\left. + \frac{\left(\mu_2^2-\mu_3^2\right)}{\mu_1^2} \left(\frac{s_{\mathrm{Z},0}}{\tau_0} - \frac{\mathrm{e}^{\mu_1} n^*_{\mathrm{Z},\mu_1}}{p_{\mu_1}} \right) \right].\end{aligned} \tag{24}$$

3) X 基中单光子脉冲事件 $s_{\mathrm{CX},1}$ 的下限.

采用与 $s_{\mathrm{Z},1}$ 的下限估计相同的计算, 可以得到:

$$\begin{aligned}&\frac{\mathrm{e}^{\mu_3} n^*_{\mathrm{CX},\mu_3}}{p_{\mu_3}} - \frac{\mathrm{e}^{\mu_2} n^*_{\mathrm{CX},\mu_2}}{p_{\mu_2}} \\ &= \frac{(\mu_3-\mu_2)\, s_{\mathrm{CX},1}}{\tau_1} + \sum_{n=2}^{\infty} \frac{\left(\mu_3^n - \mu_2^n\right) s_{\mathrm{CX},n}}{n!\cdot\tau_n}.\end{aligned} \tag{25}$$

对于 X 基中的光脉冲考虑 $\mu_2 \geqslant \mu_3$ 和 $n \geqslant 2$ 的情况, 因此得到的成立不等式为

$$\mu_3^n - \mu_2^n \leqslant \frac{\left(\mu_3^2-\mu_2^2\right)}{\mu_2^2}\mu_2^n. \tag{26}$$

将不等式代入 (25) 式, 同时考虑 $\sum_{n=2}^{\infty} \dfrac{\mu_2^n s_{\mathrm{CX},n}}{n!\cdot\tau_n} = \dfrac{\mathrm{e}^{\mu_2} n^*_{\mathrm{CX},\mu_2}}{p_{\mu_1}} - \dfrac{s_{\mathrm{CX},0}}{\tau_0} - \dfrac{\mu_1 s_{\mathrm{CX},1}}{\tau_1}$ 得到 $s_{\mathrm{CX},1}$ 的下限:

$$\begin{aligned}s^*_{\mathrm{CX},1} \geqslant \frac{\mu_2\tau_1}{\mu_3(\mu_2-\mu_3)} &\left[\frac{\mathrm{e}^{\mu_3} n^*_{\mathrm{CX},\mu_3}}{p_{\mu_3}} - \frac{\mu_3^2}{\mu_2^2} \frac{\mathrm{e}^{\mu_2} n^*_{\mathrm{CX},\mu_2}}{p_{\mu_2}} \right. \\ &\left. - \frac{\left(\mu_2^2-\mu_3^2\right)}{\mu_2^2} \frac{s_{\mathrm{CX},0}}{\tau_0} \right].\end{aligned} \tag{27}$$

为了得到 $s_{\mathrm{CX},1}$ 的下限, 还必须求出 $s_{\mathrm{CX},0}$ 的上限. 由真空事件出现错误的期望值 ($v^*_{\mathrm{CX},0}$) 应该是相应总真空事件数量的一半的事实和 $v_{\mathrm{CX},0}$ 的有限码长估计, 可以得到:

$$s_{\mathrm{CX},0} = 2v^*_{\mathrm{CX},0}, \tag{28}$$

$$v^*_{\mathrm{CX},0} \leqslant v_{\mathrm{CX},0} + \delta\left(n_{\mathrm{CX}}, \varepsilon_2\right). \tag{29}$$

同时考虑, 对于 X 基下任意一个脉冲强度的总错误事件的数量都是大于等于相应空脉冲的错误事件的数量, 即

$$m^*_{\mathrm{CX},k} = \sum_{n=0}^{\infty} \frac{p_k}{\tau_n} \frac{\mathrm{e}^{-\mathrm{k}} k^n}{n!} v_{\mathrm{CX},n} \geqslant \frac{p_0}{\tau_0} v_{\mathrm{CX},0}. \tag{30}$$

综合 (28) 式、(29) 式和 (30) 式, 可以得到 $s_{\mathrm{CX},0}$ 的上限为

$$s^*_{\mathrm{CX},0} \leqslant 2\left[\frac{\tau_0 \mathrm{e}^k}{p_k} m^*_{\mathrm{CX},k} + \delta\left(n_{\mathrm{CX}}, \varepsilon_2\right) \right]. \tag{31}$$

4) X 基中单光子脉冲中出现错误的事件 $v_{\mathrm{CX},1}$ 的上限.

通过将 $\dfrac{\mathrm{e}^{\mu_2} m^*_{\mathrm{CX},\mu_2}}{p_{\mu_2}} - \dfrac{\mathrm{e}^{\mu_3} m^*_{\mathrm{CX},\mu_3}}{p_{\mu_3}}$ 代入 (15) 式可以得到 $v_{\mathrm{CX},1}$ 的上限为

$$v^*_{\mathrm{CX},1} \leqslant \frac{\tau_1}{\mu_2-\mu_3} \left(\frac{\mathrm{e}^{\mu_2} m^*_{\mathrm{CX},\mu_2}}{p_{\mu_2}} - \frac{\mathrm{e}^{\mu_3} m^*_{\mathrm{CX},\mu_3}}{p_{\mu_3}} \right). \tag{32}$$

目前为止, 所求的各个界限都不适用于实际探测情况的统计, 因为各个事件界限不等式中都包含渐近情况下的项, 通过使用 (12) 式、(14) 式、(16) 式

的变式可以解决这个问题, 即将以下公式:

$$n^{*}_{\mathrm{Z},k} \leqslant n_{\mathrm{Z},k} + \delta\left(n_{\mathrm{Z}}, \varepsilon_1\right) := \widehat{n}^{+}_{\mathrm{Z},k}, \tag{33}$$

$$n^{*}_{\mathrm{Z},k} \geqslant n_{\mathrm{Z},k} - \delta\left(n_{\mathrm{Z}}, \varepsilon_1\right) := \widehat{n}^{+}_{\mathrm{Z},k}, \tag{34}$$

$$n^{*}_{\mathrm{CX},k} \leqslant n_{\mathrm{CX},k} + \delta\left(n_{\mathrm{CX}}, \varepsilon_2\right) := \widehat{n}^{+}_{\mathrm{CX},k}, \tag{35}$$

$$n^{*}_{\mathrm{CX},k} \geqslant n_{\mathrm{CX},k} - \delta\left(n_{\mathrm{CX}}, \varepsilon_2\right) := \widehat{n}^{-}_{\mathrm{CX},k}, \tag{36}$$

$$m^{*}_{\mathrm{CX},k} \leqslant m_{\mathrm{CX},k} + \delta\left(m_{\mathrm{CX}}, \varepsilon_3\right) := \widehat{m}^{+}_{\mathrm{CX},k}, \tag{37}$$

$$m^{*}_{\mathrm{CX},k} \geqslant m_{\mathrm{CX},k} - \delta\left(m_{\mathrm{CX}}, \varepsilon_3\right) := \widehat{m}^{-}_{\mathrm{CX},k}. \tag{38}$$

代入 (19) 式、(24) 式、(27) 式、(31) 式和 (32) 式得:

$$s^{\mathrm{l}}_{\mathrm{Z},0} \geqslant \frac{\tau_0}{\left(\mu_2-\mu_3\right)}\left(\frac{\mu_2 \mathrm{e}^{\mu_3}\widehat{n}^{-}_{\mathrm{Z},\mu_3}}{p_{\mu_3}} - \frac{\mu_3 \mathrm{e}^{\mu_2}\widehat{n}^{+}_{\mathrm{Z},\mu_2}}{p_{\mu_2}}\right), \tag{39}$$

$$s^{\mathrm{l}}_{\mathrm{Z},1} \geqslant \frac{\mu_1\tau_1}{\mu_1\left(\mu_2-\mu_3\right)-\left(\mu_2^2-\mu_3^2\right)}\left[\frac{\mathrm{e}^{\mu_2}\widehat{n}^{-}_{\mathrm{Z},\mu_2}}{p_{\mu_2}} - \frac{\mathrm{e}^{\mu_3}\widehat{n}^{+}_{\mathrm{Z},\mu_3}}{p_{\mu_3}} + \frac{\left(\mu_2^2-\mu_3^2\right)}{\mu_1^2}\left(\frac{s_{\mathrm{Z},0}}{\tau_0} - \frac{\mathrm{e}^{\mu_1}\widehat{n}^{+}_{\mathrm{Z},\mu_1}}{p_{\mu_1}}\right)\right], \tag{40}$$

$$s^{\mathrm{l}}_{\mathrm{CX},1} \geqslant \frac{\mu_2\tau_1}{\mu_3\left(\mu_2-\mu_3\right)}\left[\frac{\mathrm{e}^{\mu_3}\widehat{n}^{-}_{\mathrm{CX},\mu_3}}{p_{\mu_3}} - \frac{\mu_3^2}{\mu_2^2}\frac{\mathrm{e}^{\mu_2}\widehat{n}^{+}_{\mathrm{CX},\mu_2}}{p_{\mu_2}} - \frac{\left(\mu_2^2-\mu_3^2\right)}{\mu_2^2}\frac{s_{\mathrm{CX},0}}{\tau_0}\right], \tag{41}$$

$$s^{u}_{\mathrm{CX},0} \leqslant 2\left[\frac{\tau_0 \mathrm{e}^{k}}{p_k}\widehat{m}^{+}_{\mathrm{CX},k} + \delta\left(n_{\mathrm{CX}}, \varepsilon_2\right)\right], \tag{42}$$

$$v^{u}_{\mathrm{CX},1} \leqslant \frac{\tau_1}{\mu_2-\mu_3}\left(\frac{\mathrm{e}^{\mu_2}\widehat{m}^{+}_{\mathrm{CX},\mu_2}}{p_{\mu_2}} - \frac{\mathrm{e}^{\mu_3}\widehat{m}^{-}_{\mathrm{CX},\mu_3}}{p_{\mu_3}}\right). \tag{43}$$

令系数 c_{s} 表示渐近情况下 Alice 在 Z 基中探测到全部事件中 Alice 在 Z 基中探测且 Bob 同时选择了 SIFT 操作的事件所占的比率, 因此可以得到:

$$s^{\mathrm{l}}_{\mathrm{SZ},0} \geqslant \frac{c_{\mathrm{s}}\tau_0}{\left(\mu_2-\mu_3\right)}\left(\frac{\mu_2 \mathrm{e}^{\mu_3}\widehat{n}^{-}_{\mathrm{Z},\mu_3}}{p_{\mu_3}} - \frac{\mu_3 \mathrm{e}^{\mu_2}\widehat{n}^{+}_{\mathrm{Z},\mu_2}}{p_{\mu_2}}\right), \tag{44}$$

$$s^{\mathrm{l}}_{\mathrm{SZ},1} \geqslant \frac{c_{\mathrm{s}}\mu_1\tau_1}{\mu_1\left(\mu_2-\mu_3\right)-\left(\mu_2^2-\mu_3^2\right)}\left[\frac{\mathrm{e}^{\mu_2}\widehat{n}^{-}_{\mathrm{Z},\mu_2}}{p_{\mu_2}} - \frac{\mathrm{e}^{\mu_3}\widehat{n}^{+}_{\mathrm{Z},\mu_3}}{p_{\mu_3}} + \frac{\left(\mu_2^2-\mu_3^2\right)}{\mu_1^2} \times \left(\frac{s_{\mathrm{Z},0}}{\tau_0} - \frac{\mathrm{e}^{\mu_1}\widehat{n}^{+}_{\mathrm{Z},\mu_1}}{p_{\mu_1}}\right)\right], \tag{45}$$

其中, c_{s} 的值会在 3.3 节中讨论并给出表达式. 至此, 已经求出了密钥长度公式中会使用到每一个安全界限.

3.3 探测模拟和错误模拟

前文中我们的计算模拟均是将 Alice 在 Z 基中探测总数 n_{Z} 作为固定值进行的, 而密钥长度公式中还需要使用到 Alice 在 X 基中探测总数 n_{CX} 及其探测结果出现错误的数量 m_{CX} 还有各类事件分配到各个脉冲强度的事件, 因此下文中会展示各类事件之间的关系, 用于根据 n_{Z} 推导 n_{CX}, m_{CX} 等.

首先探测次数 n_{Z,μ_1} 对应模拟探测次数 n_{SZ} 中强度为 μ_1 的部分, 可以将 n_{Z} 的相应分数计算为:

$$\frac{n_{\mathrm{SZ}}}{n_{\mathrm{Z}}} = \frac{n_{\mathrm{Z},\mu_1}}{n_{\mathrm{Z}}} = c_{\mathrm{s}} = \frac{p_{\mathrm{Z,det,A},\mu_1}}{p_{\mathrm{Z,det,A,tot}}}, \tag{46}$$

式中, $p_{\mathrm{Z,det,A},\mu_1}$ 是 Alice 以 Z 基发送光脉冲且 Bob 选择 SIFT 操作后被 Alice 探测到的概率, $p_{\mathrm{Z,det,A,tot}}$ 表示 Alice 以 Z 基发送光脉冲最终被 Alice 探测到的概率. 概率 $p_{\mathrm{Z,det,A},\mu_1}$ 的值为

$$\begin{aligned} & p_{\mathrm{Z,det,A},\mu_1} \\ =\ & c_{\mathrm{DT,A}}c_{\mathrm{DT,B}}P_{\mathrm{Z}}P_{\mathrm{S}}\left\{P_{v_1}\left[\left(1-\mathrm{e}^{-\eta_{\mathrm{B}}\eta_{\mathrm{C}}v_1}\right)+P_{\mathrm{DC,B}}\right]\right. \\ & \left.+P_{v_2}\left[\left(1-\mathrm{e}^{-\eta_{\mathrm{B}}\eta_{\mathrm{C}}v_2}\right)+P_{\mathrm{DC,B}}\right]\right\} \\ & \times\left[\left(1-\mathrm{e}^{-\eta_{\mathrm{A}}\eta_{\mathrm{C}}\mu_1}\right)+P_{\mathrm{DC,A}}\right]. \end{aligned} \tag{47}$$

相应地, 强度为 μ_2, μ_3 的探测次数 n_{Z,μ_2}, n_{Z,μ_3} 可以写为

$$\frac{n_{\mathrm{CZ},\mu_j}}{n_{\mathrm{Z}}} = \frac{n_{\mathrm{Z},\mu_j}}{n_{\mathrm{Z}}} = \frac{p_{\mathrm{Z,det,A},\mu_j}}{p_{\mathrm{Z,det,A,tot}}},\ \forall j \in (2,3), \tag{48}$$

$$p_{\mathrm{Z,det,A},\mu_j} = c_{\mathrm{DT,A}}P_{\mathrm{Z}}P_{\mathrm{C}}P_{v_{j-1}}\left[\left(1-\mathrm{e}^{-\eta_{\mathrm{A}}\eta_{\mathrm{C}}^2 v_{j-1}}\right)+P_{\mathrm{DC,A}}\right],\ \forall j \in (2,3). \tag{49}$$

综合 (47) 式、(49) 式可以得到:

$$p_{\mathrm{Z,det,A,tot}} = p_{\mathrm{Z,det,A},\mu_1} + p_{\mathrm{Z,det,A},\mu_j},\ \forall\, j \in (2,3). \tag{50}$$

上式中 $P_{\mathrm{DC,A}}$, $P_{\mathrm{DC,B}}$ 分别为 Alice 和 Bob 探测器的暗计数概率; P_{v_1} 和 P_{v_2} 为 Alice 发送脉冲强度为 v_1 和 v_2 的概率, P_{Z} 和 P_{S} 分别为 Alice 以 Z 基发送光脉冲的概率和 Bob 选择 SIFT 操作的概率; $c_{\mathrm{DT,A}}$ 和 $c_{\mathrm{DT,B}}$ 是由于探测器的死时间 $t_{\mathrm{DT,A}}$ 和 $t_{\mathrm{DT,B}}$ 而产生的校正因子, 表示为

$$c_{\mathrm{DT,A}} = \frac{1}{1+Rt_{\mathrm{DT,A}}\left(p_{\mathrm{Z,det,A,tot}}+p_{\mathrm{X,det,A,tot}}\right)}, \tag{51}$$

$$c_{\mathrm{DT,B}} = \frac{1}{1+Rt_{\mathrm{DT,B}}p_{\mathrm{Z,det,B,tot}}}. \tag{52}$$

式中 R 为光源的发射频率, 概率 $p_{\mathrm{Z,det,B,tot}}$ 表示为

$$p_{\mathrm{Z,det,B,tot}} = c_{\mathrm{DT,B}} P_{\mathrm{Z}} P_{\mathrm{S}} \left\{ P_{v_1} \left[\left(1 - \mathrm{e}^{-\eta_{\mathrm{B}}\eta_{\mathrm{C}} v_1}\right) + P_{\mathrm{DC,B}} \right] + P_{v_2} \left[\left(1 - \mathrm{e}^{-\eta_{\mathrm{B}}\eta_{\mathrm{C}} v_2}\right) + P_{\mathrm{DC,B}} \right] \right\}. \tag{53}$$

为得到 Alice 在 X 基中探测事件的数量, 需要给出对于脉冲强度 v_1 和 v_2, Alice 选择发送 X 基且 Bob 选择 CTRL 操作的概率 $p_{\mathrm{X,det,A},v_1}$ 和 $p_{\mathrm{X,det,A},v_2}$ 及相应错误概率分别为

$$p_{\mathrm{X,det,A},\mu_j} = c_{\mathrm{DT,A}} P_{\mathrm{X}} P_{\mathrm{C}} P_{v_{j-1}} \left[\left(1 - \mathrm{e}^{-\eta_{\mathrm{A}}\eta_{\mathrm{C}}^2 v_{j-1}}\right) + P_{\mathrm{DC,A}} \right], \quad \forall\, j \in (2,3), \tag{54}$$

$$p_{\mathrm{X,det,A,tot}} = \sum\nolimits_j p_{\mathrm{X,det,A},\mu_j}, \quad \forall\, j \in (2,3), \tag{55}$$

$$\frac{n_{\mathrm{CX},\mu_j}}{n_{\mathrm{Z}}} = \frac{p_{\mathrm{X,det,A},\mu_j}}{p_{\mathrm{Z,det,A,tot}}}, \quad \forall\, j \in (2,3), \tag{56}$$

$$p_{\mathrm{X,err,A},\mu_j} = c_{\mathrm{DT,A}} P_{\mathrm{X}} P_{\mathrm{C}} P_{v_{j-1}} \left[\left(1 - \mathrm{e}^{-\eta_{\mathrm{A}}\eta_{\mathrm{C}}^2 v_{j-1}}\right) P_{\mathrm{err}} + P_{\mathrm{DC,A}}/2 \right], \quad \forall\, j \in (2,3). \tag{57}$$

式中, 概率 P_{err} 为传输过程中由于设置的未对准而导致的错误概率. 类似于 (48) 式, 可以得到强度为 μ_j 引起的错误事件:

$$\frac{m_{\mathrm{CX},\mu_j}}{n_{\mathrm{Z}}} = \frac{p_{\mathrm{X,err,A},\mu_j}}{p_{\mathrm{Z,det,A,tot}}}, \quad \forall\, j \in (2,3). \tag{58}$$

由概率的可加性, 可以得到 Alice 在 X 基下探测事件 n_{CX} 及相应错误事件 m_{CX} 可以表示为

$$n_{\mathrm{CX}} = n_{\mathrm{CX},\mu_2} + n_{\mathrm{CX},\mu_3}, \tag{59}$$

$$m_{\mathrm{CX}} = m_{\mathrm{CX},\mu_2} + m_{\mathrm{CX},\mu_3}. \tag{60}$$

因此, 为了获得样本大小 n_{Z} 所需要 Alice 发送的脉冲总数 N_{total} 可以由下式得出:

$$N_{\mathrm{total}} = \frac{n_{\mathrm{Z}}}{p_{\mathrm{Z,det,A,tot}}}. \tag{61}$$

最后, 取密钥长度 (10) 式与发送的脉冲总数 N_{total} 的比值, 得到每个脉冲的密钥率为

$$R_{\mathrm{SKR}} = \frac{l}{N_{\mathrm{total}}}. \tag{62}$$

3.4 数值模拟

模拟中考虑了一个基于光纤的 SQKD 模型, 该模型借用了诱骗态 SQKD 和我们实验室中单光子探测器的参数. 表 1 为在 0.1—1.0 范围内, 取 0.01 为步进的所有值作为脉冲强度 μ_1, v_1, v_2 的取值进行多次模拟得到的 0—50 km 的传输距离中每 5 km 处能取得最大安全密钥率的各个脉冲强度值, 可以发现 μ_1取 0.68, v_1 取 0.48 和 v_2 取 0.07 在大部分情况下能够取得最大安全密钥率, 因此对于光脉冲生成与调制系统, 考虑 Alice 端生成的光脉冲强度 v_1, v_2 分别为 0.48 和 0.07, Bob 端生成的光脉冲强度 μ_1 为 0.68, 脉冲频率为 $R = 1$ GHz, Alice 和 Bob 均以相同的概率发送强度 v_1 或 v_2 的光脉冲和选择 SIFT 操作或 CTRL 操作. 假设光纤具有 0.2 dB/km 的衰减系数, 即光纤的透过率为 $\eta_{\mathrm{C}} = 10^{-\frac{0.2L}{10}}$ (L 为传输长度). 探测系统中, 设置单光子探测器的暗计数概率 $P_{\mathrm{DC}} = 10^{-8}$, 死时间 $t_{\mathrm{DT}} = 100$ ns, 经过光纤传输后由于光学误差引起探测错误的概率 $P_{\mathrm{err}} = 10^{-2}$. 与参考文献相同, 考虑参数 λ_{EC} 为一个简单的函数 $f_{\mathrm{EC}} e_{\mathrm{obs}}$ [23], 其中 f_{EC} 为纠错效率, e_{obs} 为观察到的 Z 基中 SIFT 操作的事件的错误率的平均值, 实际应用中 λ_{EC} 应为实际公布的比特位数; 对于保密性参数 $\varepsilon_{\mathrm{sec}}$ 和正确性参数 $\varepsilon_{\mathrm{cor}}$ 与文献 [13] 中一致, 分别假设为 $\varepsilon_{\mathrm{sec}} = 10^{-9}$ 和 $\varepsilon_{\mathrm{cor}} = 10^{-15}$.

表 1 50 km 传播距离中每 5 km 处取得最大安全密钥率时脉冲强度 μ_1, v_1, v_2 的取值和得到的安全密钥率

Table 1. Pulse strength μ_1, v_1, v_2 and the number of Secret key ratio every 5 km in a 50 km transmission distance.

传输距离/km	μ_1	v_1	v_2	密钥率
0	0.68	0.48	0.07	0.001745822
5	0.68	0.48	0.07	0.000785235
10	0.68	0.48	0.07	0.000483058
15	0.68	0.48	0.07	0.000331894
20	0.68	0.48	0.07	0.000240990
25	0.68	0.48	0.07	0.000180301
30	0.68	0.48	0.08	0.000137404
35	0.68	0.48	0.08	0.000105438
40	0.68	0.49	0.09	0.000081846
45	0.68	0.49	0.10	0.000063533
50	0.68	0.49	0.10	0.000049545

图 3 为根据以上密钥分发模型与计算公式绘制的安全密钥率与光纤长度的关系. 由图 3(a) 可以看到, 在有限码长的影响下, 即便是在近距离传输的情况下, 诱骗态 SQKD 的最大安全密钥速率能够达到约 10^{-3} 量级, 相较于诱骗态 QKD 的 10^{-2} 量级小了约 1 个数量级, 并且诱骗态 SQKD 的安全密钥率随着光纤长度的增长而衰减的速率更快, 这是因为 SQKD 中能够成码的 SIFT 操作脉冲还有 Bob 重发时光脉冲时由于脉冲强度较小

而产生大量空脉冲引入的衰减, 该衰减是 QKD 系统无需考虑的. 这一项衰减使得对于相同的样本量 n_Z, 诱骗态 SQKD 能够生成的安全密钥少且需要 Alice 发送的脉冲总数多, 进而导致安全密钥率小. 但是由于 SQKD 系统的其中一方为经典方, 通过集成化能够使得这一方的通信设备小巧便携, 这使得诱骗态 SQKD 系统即便安全密钥速率较低, 但是在近距离的情况下仍有重要的应用价值.

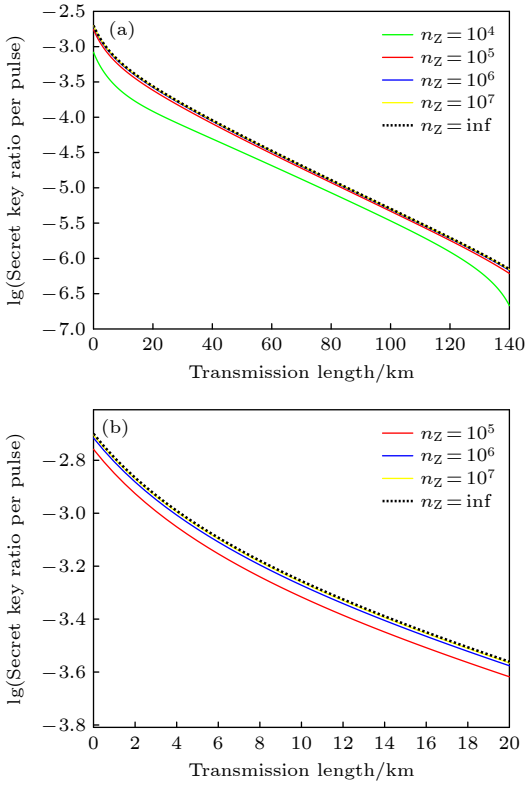

图 3 (a) 使用 1 GHz 的脉冲频率时不同码长 n_Z 之间的安全密钥率的比较, n_Z 的取值为 10^s ($s = [4, 5, 6, 7]$), 当 $n_Z = 10^5$ 时安全密钥速率与渐近情况的安全密钥率相近, 安全密钥率随光纤长度的增长而急剧衰减, 但在约 30 km 内能够保持 10^{-5} 的安全密钥率; (b) 考虑 1 GHz 的脉冲频率时三种不同 n_Z 之间近距离安全密钥率的比较, n_Z 的取值为 10^s ($s = [5, 6, 7]$)

Fig. 3. (a) The comparison of secret key rate of different key sizes n_Z, when using the pulse frequency of 1 GHz. The value of n_Z are 10^s (where $s = [4, 5, 6, 7]$). When 10^5 is chosen to be n_Z, the secret key rate is close to the asymptotic limit's. The secret key rate decreases sharply with the increase of fiber length, but it can maintain a secret key rate of 10^{-5} for about 30 km; (b) the comparison of the proximity security key rates between six different n_Z when considering a pulse frequency of 1 GHz. The value of n_Z are 10^s (where $s = [5, 6, 7]$).

图 3(b) 中绘制近距离情况下诱骗态 SQKD 的密钥速率图, 由于从图 3(a) 中可以发现, 当样本量 n_Z 选择为 10^4 时, 近距离情况下的安全密钥率相比于渐近情况具有较大的衰减, 而当样本量 n_Z 选择大于 10^4 时, 近距离情况下的安全密钥率与渐近情况的安全密钥率十分贴合, 故我们认为 10^4 对于 n_Z 并不是合适的大小, 在考虑绘制近距离情况下安全密钥率与光纤长度的关系图时不考虑 $n_Z = 10^4$. 发现在大部分样本量中, 诱惑态 SQKD 能够在 70 km 长的光纤中保持 10^{-5} 量级以上的安全密钥率, 而在 GLLP 理论验证得到的渐近情况下 SQKD 的安全传输距离 [52] 仅有 2 km, 相较之下说明诱惑态的加入一定程度上增长了传输距离. 从图 3(b) 可以看出, 近距离情况下, 渐近情况下的安全密钥速率仅约为 $n_Z = 10^5$ 时的安全密钥速率的 1.14 倍, 因此实际应用中为避免消耗较多的资源, 选择样本量 $n_Z = 10^5$ 比较合适. 当考虑 $n_Z = 10^5$ 时, 在近距离情况下可以得到约为 10^{-4} bit/s 的安全密钥率, 若对应于 1 GHz 的光源重复频率可以得到每秒钟可以产生约 10^5 个安全比特. 对于实际场景中传输约为几千比特的常规的指纹信息量, 采用一次一密的无条件安全加密方式, 只需要 ms 级别的时间即可. 此外, 应用到量子数字签名中, 10^{-4} bit/s 的安全密钥率能够在极短的时间内保证 OTUH-QDS 协议 [53] 中 Alice 与 Bob 和 Charlie 分别生成两对密钥, 随后 Alice 利用这两个密钥进行异或操作生成与 Bob 的不对称密钥进行量子数字签名, 同时由于经典方的设备可以做得易于携带, 这使签署方轻易快速地与较多人完成安全性签署成为可能.

4 结论与展望

本文首先描述了基于四态协议的 SQKD 诱骗态模型, 随后基于该模型对有限码长情况下 SQKD 系统的安全密钥率进行了分析与数值模拟, 最终发现, 设定探测到的 Z 基下光脉冲数量为 10^5 可以得到与渐近情况相近的安全密钥率, 意味着实际应用中, 只需设定 Z 基下探测到的光脉冲数量为 10^5 便可获得与理论情况相近的安全密钥率, 其中最坏情况下, 实际安全密钥率为理论的 0.87 倍. 还发现安全密钥率在近距离情况下保持较好的安全密钥率, 详细地说, 在距离小于 20 km 的情况下基于四态协议的 SQKD 诱骗态模型能保证 10^{-4} 量级的安全密钥率, 这证明了实际近距离情况下诱骗态 SQKD 系统进行信息传输、交换的可行性. 由于经典方 Bob

的设备要求较低, 分析中也并未限制 Bob 的个数, 并且多个经典方的 SQKD 系统的鲁棒性也已得到证明[54], 所以我们认为本文的分析对未来实现同一个 Alice 端与不同 Bob 端使用 SQKD 系统进行信息交换, 如指纹信息交换进行身份认证和生成量子数字签名的非对称密钥等实际应用具有积极意义.

正如前文所说, 有限码长情况下诱骗态 SQKD 的安全密钥率较低是因为 Bob 重发光脉冲时空脉冲占比较大导致的. 实际中, Bob 对于一个脉冲测量之后重发会导致密钥分发过程不安全, 这不是我们希望的, 因此后续会继续考虑基于镜像协议、随机调制再生光脉冲强度的镜像协议实验对诱骗态 SQKD[45] 进行有限码长的分析. 针对于 Alice 使用多个诱骗态以及 Bob 再生新光脉冲时加入一个或多个诱骗态的各种情况, 这也包括两端都不加入诱骗态的情况, 本文未进行分析, 我们会将对密钥分发过程使用诱骗态的个数进行优化作为后续工作.

参考文献

[1] Bennett C H, Brassard G 2014 *Theor. Comput. Sci.* **560** 7
[2] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H, Gisin N 1997 *Appl. Phys. Lett.* **70** 793
[3] Wang J, Qin X, Jiang Y, Wang X, Chen L, Zhao F, Wei Z, Zhang Z 2016 *Opt. Express* **24** 8302
[4] Mo X F, Zhu B, Han Z F, Gui Y Z, Guo G C 2005 *Opt. Lett.* **30** 2632
[5] Kraus B, Gisin N, Renner R 2005 *Phys. Rev. Lett.* **95** 080501
[6] Hwang W Y, Ahn D, Hwang S W 2001 *Phys. Lett. A* **279** 133
[7] Dušek M, Haderka O, Hendrych M 1999 *Opt. Commun.* **169** 103
[8] Lutkenhaus N, Jahma M 2002 *New J. Phys.* **4** 44.1
[9] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[10] Huttner B, Imoto N, Gisin N, Mor T 1995 *Phys. Rev. A* **51** 1863
[11] Chaiwongkhot P, Zhong J Q, Huang A, Qin H, Shi S C, Makarov V 2022 *EPJ Quantum Technol.* **9** 23
[12] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov A 2010 *Nat. Photonics* **4** 686
[13] Lim C C W, Walenta N, Legré N, Gisin N, Zbinden H 2015 *IEEE J. Sel. Top. Quantum Electron.* **21** 6601305
[14] Carlos N M, Juan Carlos G E 2021 *Quantum Inf. Process.* **20** 196
[15] Kim C M, Kim Y W, Park Y J 2011 *Curr. Appl. Phys.* **11** 1006
[16] Lu H, Fung C H F, Cai Q Y 2013 *Phys. Rev. A* **88** 044302
[17] Chen Y P, Liu J Y, Sun M S, Zhou X X, Zhang C H, Li J, Wang Q 2021 *Opt. Lett.* **46** 3729
[18] Zhou X Y, Zhang CH, Zhang C M, Wang Q 2019 *Phys. Rev. A* **99** 062316
[19] Zeng P, Zhou H Y, Wu W J, Ma X F 2022 *Nat. Commun.* **13** 3903
[20] Gu J, Cao X Y, Fu Y, He Z W, Yin Z J, Yin H L, Chen Z B 2022 *Sci. Bull.* **67** 2167
[21] Cui C H, Yin Z Q, Wang R, Chen W, Wang S, Guo G C, Han Z F 2019 *Phys. Rev. A* **11** 034053
[22] Xie Y M, Weng C X, Lu Y S, Fu Y, Wang Y, Yin H L, Chen Z B 2023 *Phys. Rev. A* **107** 042603
[23] Curty M, Azuma K, Lo H K 2019 *NPJ Quantum Inf.* **5** 64
[24] Xie Y M, Lu Y S, Weng C X, Cao X Y, Jia Z Y, Bao Y, Wang Y, Fu Y, Yin H L, Chen Z B 2022 *PRX Quantum* **3** 020315
[25] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[26] Lo H K, Ma X, Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[27] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[28] Ma X, Qi B, Zhao Y, Lo H K 2005 *Phys. Rev. A* **72** 012326
[29] Wang Q, Wang X B, Guo G C 2007 *Phys. Rev. A* **75** 012312
[30] Ma X, Fung C H F, Dupuis F, Chen K, Tamaki K, Lo H K 2006 *Phys. Rev. A* **74** 032330
[31] Scarani V, Acín A, Ribordy G, Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[32] Curty M, Xu F, Cui W, Lim C C W, Tamaki K, Lo H K 2014 *Nat. Commun.* **5** 3732
[33] Mafu M, Garapo K, Petruccione F 2013 *Phys. Rev. A* **88** 1
[34] Zhao L Y, Li H W, Yin Z Q, Chen W, You J, Han Z F 2014 *Chin. Phys. B* **23** 100304
[35] Lim C C W, Curty M, Walenta N, Xu F H, Zbinden H 2014 *Phys. Rev. A* **89** 022307
[36] Rusca D, Boaron A, Grünenfelder F, Martin A, Zbinden H 2018 *Appl. Phys. Lett.* **112** 171104
[37] Boyer M, Kenigsberg D, Mor T 2007 *Phys. Rev. Lett.* **99** 140501
[38] Zou X, Qiu D, Li L, Wu L, Li L 2009 *Phys. Rev. A* **79** 052312
[39] Boyer M, Katz M, Liss R, Mor T 2017 *Phys. Rev. A* **96** 062335
[40] Amer O, Krawec W O 2019 *Phys. Rev. A* **100** 022319
[41] Krawec W O 2015 *IEEE International Symposium Information Theory* Hong Kong, China, June 14–19, 2015 p686
[42] Boyer M, Liss R, Mor T 2018 *Entropy* **20** 536
[43] Krawec W O, Liss R, Mor T 2023 *IEEE Trans. Quantum Eng.* **4** 2100316
[44] Zhang W, Qiu D, Mateus P 2020 *Int. J. Quantum Inf.* **18** 2050013
[45] Han S Y, Huang Y F, Mi S, Qin X, Wang J D, Yu Y F, Wei Z J, Zhang Z M 2021 *EPJ Quantum Technol.* **8** 28
[46] Mi S, Dong S, Hou Q C, Wang J D, Yu Y F, Wei Z J, Zhang Z M 2022 *Front. Phys.* **10** 1029552
[47] Hoeffding W 1963 *J. Amer. Stat. Assoc.* **58** 13
[48] Renner R 2008 *Int. J. Quantum Inf.* **6** 1
[49] Vitanov A, Dupuis F, Tomamichel M, Renner R 2013 *IEEE Trans. Inf. Theory* **59** 2603
[50] Tomamichel M, Renner R 2011 *Phys. Rev. Lett.* **106** 110506
[51] Fung C H F, Ma X F, Chau H F 2010 *Phys. Rev. A* **81** 012318
[52] Dong S, Mi S, Hou Q C, Huang Y T, Wang J D, Yu Y F, Wei Z J, Zhang Z M, Fang J B 2023 *EPJ Quantum Technol.* **10** 18
[53] Yin H L, Fu Y, Li C L, Weng C X, Li B H, Gu J, Lu Y S, Huang S, Chen Z B 2023 *Nati. Sci. Rev.* **10** nwac228
[54] Zhang X Z, Gong W G, Tan Y G, Ren Z Z, Guo X T 2009 *Chin. Phys. B* **18** 2143

Finite-key analysis of decoy model semi-quantum key distribution based on four-state protocol*

Zhan Shao-Kang [1)] Wang Jin-Dong [1)†] Dong Shuang [1)] Huang Si-Ying [1)]
Hou Qing-Cheng [1)] Mo Nai-Da [1)] Mi Shang [1)] Xiang Li-Bing [2)]
Zhao Tian-Ming [2)] Yu Ya-Fei [2)] Wei Zheng-Jun [1)] Zhang Zhi-Ming [2)]

1) (*Guangdong Provincial Key Laboratory of Quantum Control Engineering and Materials, School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou* 510006, *China*)

2) (*Guangdong Provincial Key Laboratory of Micro-nanophotonic Functional Materials and Devices, School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou* 510006, *China*)

(Received 24 May 2023; revised manuscript received 18 July 2023)

Abstract

Semi-quantum key distribution allows a full quantum user Alice and a classical user Bob to share a pair of security keys guaranteed by physical principles. Semi-quantum key distribution is proposed while verifying its robustness. Subsequently, its unconditional security of semi-quantum key distribution system is verified theoretically. In 2021, the feasibility of semi-quantum key distribution system based on mirror protocol was verified experimentally. However, the feasibility experimental system still uses the laser pulse with strong attenuation. It has been proved in the literature that the semi-quantum key distribution system still encounters the risk of secret key leakage under photon number splitting attack. Therefore, the actual security of key distribution can be further reasonably evaluated by introducing the temptation state and conducting the finite-key analysis in the key distribution process. In this work, for the model of adding one-decoy state only to Alice at the sending based on a four state semi-quantum key distribution system, the length of the security key in the case of finite-key is analyzed by using Hoeffding inequality, and then the formula of the security key rate is obtained. It is found in the numerical simulation that when the sample size is 10^5, the security key rate of 10^{-4}, which is close to the security key rate of the asymptotic limits, can be obtained in the case of close range. It is very important for the practical application of semi-quantum key distribution system.

Keywords: semi-quantum key distribution, decoy state, Hoeffding's inequality, finite-key

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.72.20230849

* Project supported by the National Natural Science Foundation of China (Grant Nos. 62071186, 61771205) and the Key Laboratory Foundation of Guangdong Province, China (Grant No. 2020B1212060066).

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

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

基于四态协议的半量子密钥分发诱骗态模型的有限码长分析

詹绍康 王金东 董双 黄偲颖 侯倾城 莫乃达 弥赏 向黎冰 赵天明 於亚飞 魏正军 张智明

Finite-key analysis of decoy model semi-quantum key distribution based on four-state protocol

Zhan Shao-Kang Wang Jin-Dong Dong Shuang Huang Si-Ying Hou Qing-Cheng Mo Nai-Da Mi Shang Xiang Li-Bing Zhao Tian-Ming Yu Ya-Fei Wei Zheng-Jun Zhang Zhi-Ming

引用信息 Citation: Acta Physica Sinica, 72, 220303 (2023) DOI: 10.7498/aps.72.20230849
在线阅读 View online: https://doi.org/10.7498/aps.72.20230849
当期内容 View table of contents: http://wulixb.iphy.ac.cn

您可能感兴趣的其他文章

Articles you may be interested in

一种基于标记单光子源的态制备误差容忍量子密钥分发协议
State preparation error tolerant quantum key distribution protocol based on heralded single photon source
物理学报. 2022, 71(3): 030301 https://doi.org/10.7498/aps.71.20211456

基于混合编码的测量设备无关量子密钥分发的简单协议
A simple protocol for measuring device independent quantum key distribution based on hybrid encoding
物理学报. 2020, 69(19): 190301 https://doi.org/10.7498/aps.69.20200162

基于高维单粒子态的双向半量子安全直接通信协议
Bi-directional semi-quantum secure direct communication protocol based on high-dimensional single-particle states
物理学报. 2022, 71(13): 130304 https://doi.org/10.7498/aps.71.20211702

基于CHSH不等式几何解释的“X”态量子非局域关联检验
Quantum nonlocal test of “X” state based on geometric interpretation of CHSH inequality
物理学报. 2022, 71(17): 170302 https://doi.org/10.7498/aps.71.20220445

基于量子催化的离散调制连续变量量子密钥分发
Discrete modulation continuous-variable quantum key distribution based on quantum catalysis
物理学报. 2020, 69(6): 060301 https://doi.org/10.7498/aps.69.20191689

标记单光子源在量子密钥分发中的应用
Overview of applications of heralded single photon source in quantum key distribution
物理学报. 2022, 71(17): 170304 https://doi.org/10.7498/aps.71.20220344