改进的关联源量子密钥分发*

李思莹[1)] 朱顺[1)] 胡飞飞[1)] 黄昱[1)] 林旭斌[1)]
覃楚珺[1)] 曹渊[2)] 刘云[2)†]

1) (中国南方电网电力调度控制中心, 广州 510000)
2) (安徽省量子安全工程技术研究中心, 芜湖 241000)

(2025 年 3 月 3 日收到; 2025 年 4 月 10 日收到修改稿)

量子密钥分发为远程安全通信提供了理论保障, 但现有的关联源量子密钥分发协议在处理源关联性时容忍能力较弱, 导致密钥率低、传输距离短, 限制了其应用. 本文提出了一种改进的关联源量子密钥分发协议, 摒弃传统的基于损耗容忍的安全性分析, 转而采用标准 BB84 协议进行安全性分析. 通过对比不同参数下的性能, 结果表明, 改进协议在密钥率和传输距离上具有显著提升, 展示了更强的应用潜力.

关键词: 量子密钥分发, 实际安全性, 源关联性, BB84 协议
PACS: 03.67.Hk, 42.50.–p, 42.65.–k **DOI:** 10.7498/aps.74.20250268
CSTR: 32037.14.aps.74.20250268

1 引 言

量子密钥分发技术为远距离通信提供了理论上的信息安全保障, 允许通信双方在窃听者存在的情况下安全地交换密钥[1]. 然而, 尽管量子密钥分发在理论研究和实验实现方面取得了显著进展, 实际应用中的安全性与理想模型所承诺的信息理论安全性之间仍存在显著差距[2,3]. 特别在实际设备的实现中, 许多因素可能导致安全性下降, 尤其是设备与理想假设之间的差异.

对于量子密钥分发中的源端而言, 安全性漏洞主要来源于几个方面. 首先, 由于调制器精度的限制, 光源的状态制备可能存在缺陷[4], 这会影响密钥分发的安全性. 其次, 调制器的侧信道或特洛伊木马攻击可能会导致信息泄露, 使得窃听者能够间接获取密钥信息[5–9]. 此外, 调制器带宽的限制也可能引发不同脉冲之间的经典关联性, 这种关联性会破坏量子密钥分发的独立性假设, 进而影响系统的安全性[10–17].

为了解决这些问题, 研究者们已经提出了一些针对关联光源的安全性证明方法[16–19], 其中一种较为成熟的技术是基于参考技术的安全性分析, 被称为关联源量子密钥分发[18]. 该方法能够有效处理源的关联性问题, 从而在一定程度上弥补了实验设备与理想模型之间的差异.

然而, 现有的关联源量子密钥分发协议[18]在容忍关联性方面存在显著不足, 导致其在实际应用中表现出较低的密钥率、有限的性能以及较短的传输距离. 这些限制使得现有协议在大规模应用中的前景不容乐观. 针对这些问题, 本文提出了一种改进的关联源量子密钥分发协议, 摒弃了传统协议中基于损耗容忍的安全性分析框架[4], 采用标准的 BB84 协议[1]新的安全性分析.

在本研究中, 首先给出了改进协议的分析过程, 详细阐述了其在面对关联源时的安全性框架.

* 中国南方电网有限责任公司科技项目 (批准号: 000005KK52220034 (ZDKJXM20222036)) 资助的课题.
† 通信作者. E-mail: liuyun@qasky.com

通过与传统协议在不同参数设置下的对比, 展示了新协议在性能上的显著提升, 特别是在密钥率和传输距离方面的改进. 本文结果表明, 改进后的协议在容忍源关联性方面表现更为优越, 能有效提高系统的整体性能, 使得关联源量子密钥分发技术向实际应用迈出了更为坚实的一步.

2 非完美性质描述

实际制备的态, 其非完美性质可以主要分为 3 部分[18]. 其一是态制备不完美 (state preparation flaw, SPF), 此外还有侧信道与关联性. 其中, 对于态制备不完美, 本文进行一个基础的假设, 即态制备不完美会使得 BB84 协议的 4 个态产生偏差, 即:

$$|0z_{\rm per}\rangle = |0{\rm Z}\rangle\,, \tag{1}$$

$$|1z_{\rm per}\rangle = -\sin\left(\frac{\delta}{2}\right)|0{\rm Z}\rangle + \cos\left(\frac{\delta}{2}\right)|1{\rm Z}\rangle\,, \tag{2}$$

$$|0x_{\rm per}\rangle = \cos\left(\frac{\delta+\pi}{4}\right)|0{\rm Z}\rangle + \sin\left(\frac{\delta+\pi}{4}\right)|1{\rm Z}\rangle\,, \tag{3}$$

$$|1x_{\rm per}\rangle = \cos\left(\frac{3\delta+3\pi}{4}\right)|0{\rm Z}\rangle + \sin\left(\frac{3\delta+3\pi}{4}\right)|1{\rm Z}\rangle\,. \tag{4}$$

其中 $|j_{\rm per}\rangle$ ($j = 0z,\ 1z,\ 0x,\ 1x$) 代表在 Z 基与 X 基下制备的 bit 为 0, 1 的态, δ 表示态制备不完美的大小.

对于侧信道与关联性, 首先考虑单独一个回合. 在存在侧信道与关联性的情况下, 可认为第 $k-1$ 回合的态能够影响第 k 回合的态. 则在第 $k-1$ 回合选择 j_{k-1} 确定的情况下, 第 k 回合选择 j_k 制备的态 $\left|\Psi_{j_k|j_{k-1}}\right\rangle$ 满足:

$$\left|\Psi_{j_k|j_{k-1}}\right\rangle = \sqrt{1-\varepsilon}\left|j_{k_{\rm per}}\right\rangle + \sqrt{\varepsilon}\left|j^{\perp}_{k_{\rm per}}\right\rangle, \tag{5}$$

其中 $\left|j^{\perp}_{k_{\rm per}}\right\rangle$ 表示未知维度与具体形式, 但是与 $\left|j^{\perp}_{k_{\rm per}}\right\rangle$ 正交的态, 即侧信道态, ε 表示侧信道与关联性的大小, $\varepsilon \in [0,1]$, 其值越大表示关联性与侧信道越大.

为了分析协议的安全性, 将所有受到第 k 回合选择 j_k 的态全部写出, 这个态整体可以表示为

$$\begin{aligned}|\Psi_{j_k}\rangle &= \left|\Psi_{j_k|j'_{k-1}}\right\rangle \sum_{j_{k+1}} |j_{k+1}\rangle\left|\Psi_{j_{k+1}|j_k}\right\rangle : \\ &= (1-\varepsilon)\left|j'_{k_{\rm per}}\right\rangle + \sqrt{1-(1-\varepsilon)^2}\left|j'^{\perp}_{k_{\rm per}}\right\rangle,\end{aligned} \tag{6}$$

其中 $\left|j'_{k_{\rm per}}\right\rangle$ 为不存在侧信道与关联性的完美态, 具体形式为

$$\left|j'_{k_{\rm per}}\right\rangle = \left|j_{k_{\rm per}}\right\rangle \sum_{j_{k+1}} |j_{k+1}\rangle\left|j_{k+1_{\rm per}}\right\rangle. \tag{7}$$

本协议仅需要表征态制备不完美参数 δ, 关联范围 ξ, 以及关联性与侧信道参数 ε, 即可完成安全性分析.

3 安全性分析

进行关联源下的安全性分析, 实际上就是要分析这种情况下的相位误码. 不同于普通的 BB84 协议, 在存在侧信道与关联性的情况下, X 基发送的态并不能直接用以估计相位误码, 因为真实的相位基的两个态在这种情况下并非与 X 基发送的态相同. 此时, 为了分析相位误码, 需要利用现有的测量值进行估计. 利用柯西-施瓦茨约束[18], 可以在衡量 X 基发送态与真实相位基偏差的情况下, 估计真实的相位误码的值.

3.1 改进的关联源量子密钥分发协议流程

在开始安全性分析前, 首先介绍协议流程.

1) 系统准备. 在执行 QKD 流程前, Alice 预先表征态制备不完美参数 δ, 关联范围 ξ, 以及关联性与侧信道参数 ε.

2) 量子通信. 完成系统准备后, Alice 和 Bob 双方进行 QKD 流程. 该协议在物理流程上与标准 BB84 类似. 在 QKD 流程的每一个回合, Alice 与 Bob 双方分别执行:

① 态制备. 在每一回合, Alice 以 $p_{\rm Z}$ 的选基概率选取 Z 基, 以余下的概率选取 X 基. 对于任意一个基, Alice 以等概率选取比特 0 或 1. Alice 尝试按上述选择制备对应的 4 个 BB84 态, 形如 (1) 式—(4) 式.

② 测量. Bob 以另一个选基概率进行对应的测量. Bob 记录本回合的基选择与测量结果 $\in \{\varnothing,\ 0,\ 1\}$, 其中 $\varnothing$ 代表失败, 0 与 1 代表测量到对应基下的比特值.

3) 密钥筛选. Alice 在公开信道上公布各轮的基选择, Bob 在此基础上进一步公布该轮是否成功测量. 然后, 他们在成功测量的回合中都选 Z 基的部分生成密钥, 而都选 X 基的部分用于参数估计.

4) 参数估计. Alice 与 Bob 利用 X 基的比特误码率, 估计 Z 基下的相位误码率大小.

5) 密钥生成. Alice 和 Bob 进行经典后处理过程, 最终生成相同的安全密钥.

3.2 相位误码定义

由纠缠等价协议, 真实的相位误码定义为 Z 基实际发送的态在其辅助粒子 X 基下测量得到的态. 简而言之, 相位误码发生的概率为

$$P(\mathrm{ph}) := p_{1x}^{\mathrm{vir}} p_{\mathrm{Z_B}} \cdot \mathrm{Tr}\left[\left|\Psi_{1x}'\right\rangle\left\langle\Psi_{1x}'\right| \hat{M}_{0x}\right] + p_{0x}^{\mathrm{vir}} p_{\mathrm{Z_B}} \cdot \mathrm{Tr}\left[\left|\Psi_{0x}'\right\rangle\left\langle\Psi_{0x}'\right| \hat{M}_{1x}\right]. \tag{8}$$

其中, $p_{ax}^{\mathrm{vir}} = \frac{p_{\mathrm{Z_A}}}{2} \cdot [1+(-1)^a \langle 0z_{\mathrm{per}}|1z_{\mathrm{per}}\rangle]$, $p_{\mathrm{Z_B}}$ 为 Bob 测量选 Z 基的概率, $\hat{M}_{ax}$ 为在 Eve 攻击后, Bob 在 X 基下的 bit a 对应的测量算符, $|\Psi_{ax}'\rangle$ 为真实的相位基, 其具体形式为

$$\left|\Psi_{ax}'\right\rangle = \frac{|\Psi_{0\mathrm{z}}\rangle + (-1)^a |\Psi_{1\mathrm{z}}\rangle}{\sqrt{2\left[1+(-1)^a \langle\Psi_{0\mathrm{z}}|\Psi_{1\mathrm{z}}\rangle\right]}}. \tag{9}$$

然而正如上文所述, 由于关联性, 实际发送的 $|\Psi_{0x}\rangle$, $|\Psi_{1x}\rangle$, $|\Psi_{0x}'\rangle$, $|\Psi_{1x}'\rangle$ 并不相同.

3.3 实际相位基与发送态的内积

为了利用实际测得的 $\left[|\Psi_{ax}\rangle\langle\Psi_{ax}|\hat{M}_{bx}\right]$ 结果约束 $\left[|\Psi_{ax}\rangle\langle\Psi_{ax}|\hat{M}_{bx}\right]$ 的大小, 需要衡量 $\left|\langle\Psi_{ax} \mid \Psi_{ax}{}'\rangle\right|$ 的大小, 以进行下一步分析. 首先, 由第 3.1 节的定义式可得

$$\left|\left\langle\Psi_{j_k} \mid j'_{\mathrm{per}}\right\rangle\right| = 1-\varepsilon. \tag{10}$$

又因为协议没有对 $\left|j'^{\perp}_{k_{\mathrm{per}}}\right\rangle$ 的具体形式做出假设, 则在对内积进行估计时, 需对 $\left|a'^{\perp}_{k_{\mathrm{per}}}\right\rangle$ 与 $\left|b'_{k_{\mathrm{per}}}\right\rangle$ 的内积进行最差的估计. 在这个思想下, 计算可得

$$\left|\left\langle\Psi_{0z} \mid 0x'_{\mathrm{per}}\right\rangle\right| \geqslant \cos\left(\frac{\delta+\pi}{4}\right)(1-\varepsilon) - \sin\left(\frac{\delta+\pi}{4}\right)\sqrt{1-(1-\varepsilon)^2}, \tag{11}$$

$$\left|\left\langle\Psi_{1z} \mid 0x'_{\mathrm{per}}\right\rangle\right| \geqslant \sin\left(\frac{-\delta+\pi}{4}\right)(1-\varepsilon) - \cos\left(\frac{-\delta+\pi}{4}\right)\sqrt{1-(1-\varepsilon)^2}. \tag{12}$$

由于本文对 $|\Psi_{ax}'\rangle$ 的定义, 进一步计算可得

$$\left|\left\langle\Psi_{0x}' \mid 0x'_{\mathrm{per}}\right\rangle\right| \geqslant (1-\varepsilon)^2 - \frac{\cos(\delta/4)+\sin(\delta/4)}{\cos(\delta/4)-\sin(\delta/4)} \cdot \left[1-(1-\varepsilon)^2\right] = 1 - \left[1+\frac{\cos(\delta/4)+\sin(\delta/4)}{\cos(\delta/4)-\sin(\delta/4)}\right] \cdot \left(2\varepsilon-\varepsilon^2\right). \tag{13}$$

又由定义式, 可得 $\left|\langle\Psi_{0x}| 0x'_{\mathrm{per}}\rangle\right| = 1-\varepsilon$, 则进一步放缩, 可得:

$$\left|\langle\Psi_{0x}'|\Psi_{0x}\rangle\right| \geqslant \Delta, \tag{14}$$

其中

$$\Delta = (1-\varepsilon)\cdot\left\{1-\left[1+\frac{\cos(\delta/4)+\sin(\delta/4)}{\cos(\delta/4)-\sin(\delta/4)}\right]\cdot\left(2\varepsilon-\varepsilon^2\right)\right\} - \left(2\varepsilon-\varepsilon^2\right)^{3/2} \times \sqrt{2\left(1+\frac{\cos(\delta/4)+\sin(\delta/4)}{\cos(\delta/4)-\sin(\delta/4)}\right) - \left(1+\frac{\cos(\delta/4)+\sin(\delta/4)}{\cos(\delta/4)-\sin(\delta/4)}\right)^2 \cdot \left(2\varepsilon-\varepsilon^2\right)}. \tag{15}$$

同理, 可以计算 $\left|\langle\Psi_{1x}'|\Psi_{1x}\rangle\right| \geqslant \Delta$. Δ 代表了真实相位基与发送的相位基的偏差. 有了这一区分度, 就可以利用柯西-施瓦茨约束[18] 对协议的相位误码率进行估计.

3.4 实际相位基相位误码估计

首先, 需要给出柯西-施瓦茨约束的具体形式, 其满足

$$g^l\left(\mathrm{Tr}\left[|A\rangle\langle A|\hat{M}\right], |\langle A \mid R\rangle|\right) \leqslant \mathrm{Tr}\left[|R\rangle\langle R|\hat{M}\right] \leqslant g^u\left(\mathrm{Tr}\left[|A\rangle\langle A|\hat{M}\right], |\langle A \mid R\rangle|\right), \tag{16}$$

其中

$$g^l(x,y) = \begin{cases} 0, & x < 1-y^2 \\ x+\left(1-y^2\right)(1-2x) - 2y\sqrt{\left(1-y^2\right)(1-x)\,x}, & x \geqslant 1-y^2, \end{cases} \tag{17}$$

$$g^u(x,y) = \begin{cases} x+\left(1-y^2\right)(1-2x) + 2y\sqrt{\left(1-y^2\right)(1-x)\,x}, & x < y^2 \\ 0, & x \geqslant y^2. \end{cases} \tag{18}$$

满足 $0 < \hat{M} < 1$.

记实际测到的两个相位误码事件的条件计数率为

$$Q_{1x0x} := \mathrm{Tr}\left[|\Psi_{1x}\rangle\langle\Psi_{1x}|\hat{M}_{0x}\right], \tag{19}$$

$$Q_{0x1x} := \mathrm{Tr}\left[|\Psi_{0x}\rangle\langle\Psi_{0x}|\hat{M}_{1x}\right]. \tag{20}$$

则真实的相位误码可以由两个相位误码事件的计数率约束:

$$P(\mathrm{ph}) \leqslant p_{\mathrm{Z_B}} g^{u}\left(\frac{p_{1x}^{\mathrm{vir}}Q_{1x0x}+p_{0x}^{\mathrm{vir}}Q_{0x1x}}{p_{1x}^{\mathrm{vir}}+p_{0x}^{\mathrm{vir}}}, \Delta\right). \tag{21}$$

这就完成了对相位误码的分析, 进而完成了安全性分析.

3.5 密钥率公式与仿真结果

完成对相位误码的分析, 由 GLLP 公式, 可以给出密钥率公式满足:

$$R \geqslant Y_{\mathrm{Z}}\left[1-h(e_x)\right]-fh(e_{\mathrm{Z}}), \tag{22}$$

其中比特误码率 e_{Z} 满足:

$$e_{\mathrm{Z}} = \frac{p_{\mathrm{Z_B}}p_{1\mathrm{z}}Q_{1\mathrm{z}0\mathrm{z}}+p_{\mathrm{Z_B}}p_{0\mathrm{z}}Q_{0\mathrm{z}1\mathrm{z}}}{Y_{\mathrm{Z}}}. \tag{23}$$

Z 基计数率满足:

$$Y_{\mathrm{Z}} = p_{\mathrm{Z_B}}\left[\sum_{a=\{0,1\},b=\{0,1\}}(p_{az}Q_{azbz})\right], \tag{24}$$

而相位误码率满足:

$$e_x = \frac{P(\mathrm{ph})}{Y_{\mathrm{Z}}}. \tag{25}$$

图 1 为本协议与现有的关联源量子密钥分发协议 [18] 进行性能的对比. 其中探测器暗计数率 $P_{\mathrm{d}} = 10^{-7}$, 纠错效率 $f = 1.16$, Alice 与 Bob 选 Z 基的概率分别为 2/3 与 1/2.

在仿真中, 态制备不完美参数 $\delta = 0$, 0.3, 侧信道与关联性参数 $\varepsilon = 10^{-3}$, 10^{-4}, 分析 4 种情况下的密钥率. 可以看到, 在全部的情况中, 本文的改进协议都比现有的协议有更高的密钥率与极限距离. 同时, 关联性越大, 改进协议相较于现有协议的提升也越大; 在 $\delta = 0$ 的情况下, $\varepsilon = 10^{-3}$ 时, 0 dB 处改进协议对于现有协议有 3 倍左右的密钥率提升, 且极限距离由 6 dB 提升至 13 dB; $\varepsilon = 10^{-4}$ 时, 0 dB 处改进协议对于现有协议有 1.5 倍左右的密钥率提升, 且极限距离由 16 dB 左右提升至 22 dB. 但是, 改进的协议对于态制备不完美的容忍性要低于现有协议; 在 $\varepsilon = 10^{-4}$ 的情况下, $\delta = 0$ 时, 0 dB 处改进协议对于现有协议有 3 倍左右的密钥率提升, 且极限距离由 6 dB 提升至 13 dB; $\delta = 0.3$ 时, 0 dB 处改进协议对于现有协议有 1.6 倍左右的密钥率提升, 且极限距离由 4 dB 左右提升至 6 dB 左右.

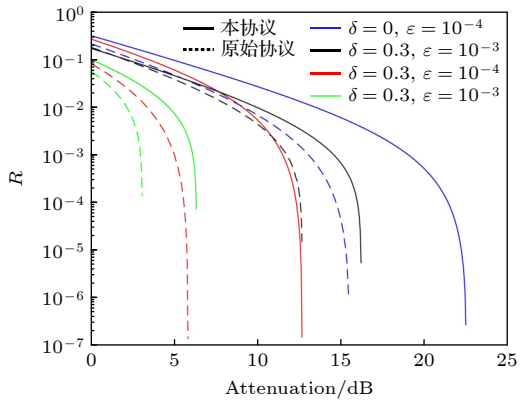

图 1 不同关联性与态制备不完美情况下本协议与现有关联源量子密钥分发性能对比

Fig. 1. Comparison of the performance of this protocol with existing entanglement-based QKD under different entanglement and imperfect state preparation conditions.

仿真结果显示, 在各种关联性大小与态制备不完美的情况下, 改进的协议都有优于现有协议的密钥率表现. 且关联性大小越大, 改进协议的效果越好. 但是, 由于改进的协议放弃了现有协议以制备三态的损耗容忍协议 [4] 为基础, 转而采用四态协议为基础, 其对态制备不完美的容忍能力略低于现有协议.

4 结 论

本文提出了一种改进的关联源量子密钥分发协议, 摒弃了传统基于损耗容忍的协议框架, 转而采用标准的 BB84 协议进行安全性分析. 通过分析和对比, 展示了改进协议在不同参数下的优势, 特别是在提高密钥率和延长传输距离方面. 具体来说, 我们的协议相比于现有协议, 在常规的态制备不完美大小下有 1.5—3 倍的密钥率提升以及 2—6 dB 的极限距离提升. 理论分析表明, 改进后的协议不仅能够有效应对源的关联性问题, 而且在实际应用中展现出更强的稳定性和更高的性能. 此外, 由于该协议在实现层面与 BB84 协议完全相同, 仅在参数估计步骤有所区别, 所以在引入诱骗

态后, 该协议能在现有的 BB84 实验系统上运行.

未来的研究可以进一步探索该协议在不同实验条件下的表现, 结合更多的实验数据验证其实际可行性. 此外, 结合本文的想法, 进一步引入一些容忍态制备偏差类协议以进一步容忍态制备不完美也是此类协议的发展目标之一. 同时, 要将改进的协议与现有的量子通信网络和安全体系相结合. 随着量子密钥分发技术的不断发展, 改进后的协议将在量子通信和量子网络的实际部署中发挥重要作用, 推动量子信息技术的广泛应用和普及.

参考文献

[1] Bennett C H, Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing Bangalore, India,* 1984 pp175–179

[2] Jiao R Z, Ding T, Wang W J, Ma H Q 2013 *Acta Phys. Sin.* **62** 180302 (in Chinese) [焦荣珍, 丁天, 王文集, 马海强 2013 物理学报 **62** 180302]

[3] Chen Y H, Wang J D, Du C, Ma R L, Zhao J Y, Qin X J, Wei Z J, Zhang Z M. 2019 *Acta Phys. Sin.* **68** 130301 (in Chinese) [陈艳辉, 王金东, 杜聪, 马瑞丽, 赵家钰, 秦晓娟, 魏正军, 张智明 2019 物理学报 **68** 130301]

[4] Tamaki K, Curty M, Kato G, Lo H K, Azuma K 2013 *Phys. Rev. A* **90** 052312

[5] Gisin N, Fasel S, Kraus B, Zbinden H, Ribordy G 2006 *J. Mod. Opt. A* **73** 022320

[6] Vakhitov A, Makarov V, Hjelme D R 2001 *J. Mod. Opt.* **48** 2023

[7] Lucamarini M, Choi I, Ward M B, Dynes J F, Yuan Z L, Shields A J 2015 *J. Mod. Opt. X* **5** 031030

[8] Tamaki K, Curty M, Lucamarini M 2016 *New J. Phys.* **18** 065008

[9] Wang W, Tamaki K, Curty M 2018 *New J. Phys.* **20** 083027

[10] Grünenfelder F, Boaron A, Rusca D, Martin A, Zbinden H 2020 *Appl. Phys. Lett.* **117** 144003

[11] Kobayashi T, Tomita A, Okamoto A 2014 *Phys. Rev. A* **90** 032320

[12] Roberts G L, Pittaluga M, Minder M, Lucamarini M, Dynes J F, Yuan Z L, Shields A J 2018 *Opt. Lett.* **43** 5110

[13] Yoshino K I, Fujiwara M, Nakata K, Sumiya T, Sasaki T, Sasaki M, Takeoka M, Sasaki A, Tajima A, Koashi M, Tomita A 2018 *NPJ Quantum Inf.* **4** 8

[14] Lu F Y, Lin X, Wang S, Fan Y G J, Ye P, Wang R, Yin Z Q, He D Y, Chen W, Guo G C, Han Z F 2021 *NPJ Quantum Inf.* **7** 75

[15] Lu F Y, Wang Z H, Wang S, Yin Z Q, Chen J L, Kang X, He D Y, Chen W, Fan Y G J, Guo G C, Han Z F 2023 *J. Lightwave Technol.* **41** 4895

[16] Zapatero V, Navarrete A, Tamaki K, Curty M 2021 *Quantum* **5** 602

[17] Sixto X, Zapatero V, Curty M 2022 *Phys. Rev. A* **18** 044069

[18] Pereira M, Kato G, Mizutani A, Curty M, Tamaki K 2020 *Sci. Adv.* **6** eaaz4487

[19] Kang X, Lu F Y, Wang S, Chen J L, Wang Z H, Yin Z Q, He D Y, Chen W, Fan Y G J, Guo G C, Han Z F 2022 *J. Lightwave Technol.* **41** 75

Improved source-correlated quantum key distribution*

LI Siying [1)] ZHU Shun [1)] HU Feifei [1)] HUANG Yu [1)] LIN Xubin [1)]
QIN Chujun [1)] CAO Yuan [2)] LIU Yun [2)†]

1) (*Power Dispatching Control Center of China Southern Power Grid Co., Ltd., Guangzhou* 510000, *China*)

2) (*Anhui Quantum-Safe Engineering Technical Research Center, Wuhu* 241000, *China*)

(Received 3 March 2025; revised manuscript received 10 April 2025)

Abstract

Based on the basic principles of quantum mechanics, quantum key distribution (QKD) provides unconditional security for long-distance communication. However, existing QKD with relevant source protocols have limited tolerance for source correlation, which greatly reduces the key generation rate and limits the secure transmission distance, thereby limiting their practical deployment. In this work, we propose an improved QKD with correlated source protocol to overcome these limitations by discarding the traditional loss-tolerant security frameworks. Our approach adopts the standard BB84 protocol for the security analysis, under the assumption that the source correlation has a bounded range and characterized inner product of the states. We theoretically analyze the performance of the improved protocol at different levels of source correlation and channel loss. Numerical simulations show that our protocol achieves a much higher secret key rate and longer transmission distance than traditional schemes. In the case of typical parameters and 0 dB loss, our protocol achieves about 1.5–3 times improvement in secret key rate. Additionally, the maximum tolerable loss is enhanced by about 2–6 dB. This highlights a promising direction for enhancing the robustness and practicality of QKD with correlated sources systems, paving the way for their deployment in real-world quantum communication networks.

Keywords: quantum key distribution, practical security, source entanglement, BB84 protocol

PACS: 03.67.Hk, 42.50.–p, 42.65.–k **DOI:** 10.7498/aps.74.20250268

CSTR: 32037.14.aps.74.20250268

* Project supported by the China Southern Power Grid Project of Science and Technology (Grant No. 000005KK52220034 (ZDKJXM20222036)).

† Corresponding author. E-mail: liuyun@qasky.com

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

改进的关联源量子密钥分发

李思莹 朱顺 胡飞飞 黄昱 林旭斌 覃楚珺 曹渊 刘云

Improved source-correlated quantum key distribution

LI Siying ZHU Shun HU Feifei HUANG Yu LIN Xubin QIN Chujun CAO Yuan LIU Yun

引用信息 Citation: Acta Physica Sinica, 74, 140302 (2025) DOI: 10.7498/aps.74.20250268
CSTR: 32037.14.aps.74.20250268
在线阅读 View online: https://doi.org/10.7498/aps.74.20250268
当期内容 View table of contents: http://wulixb.iphy.ac.cn