DOI: 10.3969/j.issn.1007-5461.2023.03.013

E91-QKD 中集体攻击上限的研究

贾 玮[1], 张强强[1], 卞宇翔[1], 李 威[2*]

(1 南京南瑞国盾量子技术有限公司, 江苏 南京 211106;
2 南京邮电大学通信与信息工程学院, 江苏 南京 210003)

摘 要: 安全性分析是实用化量子密钥分发 (QKD) 协议中不可或缺的一部分, 它不仅可以用来表征外界的窃听能力, 还可以为系统的密钥率提供安全的范围。量子通道攻击能力的表征是QKD安全性分析的主要内容, 其中集体攻击被认为是最强大的量子通道攻击之一。构造了由两体耦合作用和正定算子测度 (POVM) 构成的广义的集体攻击操作, 给出了E91-QKD相对于集体攻击的安全性分析。仿真结果显示, 在集体攻击下窃听者与通信方之间的互信息要小于基于纠缠纯化协议所提供的界限, 因此系统的密钥率和对误比特率的容忍度有了显著的提升。所提出的安全性分析将为实用化QKD的密钥率提升提供一个解决途径, 且该方法可与其他实验方法兼容。

关 键 词: 量子信息; 量子密码; E91量子密钥分发; 集体攻击; 两体耦合

中 图 分 类 号 : O431.2 **文 献 标 识 码 :** A **文章编号:** 1007-5461(2023)03-00407-08

Research on the upper bound of collective attack in E91−QKD

JIA Wei[1], *ZHANG Qiangqiang*[1], *BIAN Yuxiang*[1], *LI Wei*[2*]

(1 NRGD Quantum Technology Co., Ltd., Nanjing 211006, China;
2 College of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Security analysis is an indispensable part of practical quantum key distribution (QKD) protocol, which can not only evaluate the eavesdropping ability of external attacks, but also provide a security bound for the key rate of system. Quantum channel attack is the main content of QKD security analysis, among which collective attack is considered to be one of the most powerful quantum channel attacks. In this paper, a generalized collective attack operation, composed of generalized bipartite coupling and the optimal positive operator-valued measurement (POVM) is constructed, and a theoretical study on the security analysis of E91-QKD against collective attack is carried out. The simulation results show that under collective attack, the mutual information between the eavesdropper and the communicator is less than that proposed by the entanglement purification protocol, and the key rate and bit error rate tolerance have been significantly improved. The security analysis developed in this work provides a theoretical method to increase the key rate for practical QKDs, which can be compatible with other experimental methods.

Key words: quantum information; quantum encryption; E91-quantum key distribution; collective attack; bipartite coupling

基金项目: 南京南瑞国盾量子技术有限公司科技项目(5246MI200002)
作者简介: 贾 玮 (1988 -), 安徽宿州人, 高级工程师, 主要从事电力系统通信技术、量子保密通信技术方面的研究。
E-mail: jiawei@sgepri.sgcc.com.cn
收稿日期: 2021-08-23; **修改日期:** 2021-10-13
*通信作者。E-mail: alfred_wl@njupt.edu.cn

0 引 言

E91-量子密钥分发 (QKD) 最早由Ekert[1]在1991年提出, 是具有纠缠形式的BB84-QKD, 密钥分配由量子离域关联实现。在E91-QKD中, Charlie制备一组纠缠对, 并将纠缠对中的两部分别发送给通信认证的双方, 即Alice和Bob, 一般认为纠缠对是双光子纠缠。光子态在量子信道中传输会受到窃听者Eve各种可能的通道攻击, 在这种情况下, 需要通过表征通道攻击的能力来为QKD提供安全性分析[2−5]。迄今为止, 研究人员提出了不同的量子通道攻击, 包括相干攻击[6, 7]、集体攻击[8−13]和个体攻击[14−16], 其中辅助量子态被用来与传输的光子态作用。量子通道攻击的一个显著优势是可以充分利用Alice和Bob在QKD过程中的对基信息去寻找最优的攻击策略。

相干攻击是一种概念上的高维攻击, 之前有很多工作利用纠缠纯化协议 (EPP) 来证明量子密钥分配在该攻击方案下的安全性[6, 17, 18]。然而该安全性证明并没有具体分析相干攻击可能的窃听操作, 因此对于通道攻击的窃听能力以及系统的密钥率只给出了一个较为宽松的上限。个体攻击也被认为是一种最优的通道窃听方案, 每个传输量子态被分别独立地进行窃听[14]。集体攻击被认为是渐进最优的量子通道攻击方案, 通常认为只考虑集体攻击足以分析QKD的安全性[19]。然而在E91-QKD中并没有关于集体攻击的报道, 相关研究只出现在设备无关 (DI) 的QKD中[9, 11]。在这些研究中认为所有设备均是不可信的, 而且并没有具体分析集体攻击操作, 所得的密钥率远低于基于纠缠纯化协议的密钥率, 因此该协议很难实用化。实际上与外界隔离的设备均可以被精确表征, 例如利用诱骗态方法表征光源来提高QKD的密钥率[20−22]。因此, 对于E91-QKD中集体攻击的研究是可行的。

本文研究了E91-QKD中集体攻击的窃听能力, 假设Eve无法访问Alice和Bob所拥有的测量设备, 并且这些测量设备是可以被严格表征的。利用两体耦合作用构造了广义的集体攻击操作, 其中两体耦合作用由相位耦合和能级跃迁耦合构成, Eve可获取的关于Alice和Bob的密钥量通过选取最优正定算子测度(POVM)计算得到, 最后对比了E91-QKD基于集体攻击和基于纠缠纯化协议的安全性证明。

1 E91-QKD中的集体攻击

本研究中所用到的E91-QKD实验线路以及Eve的集体攻击示意图如图1所示。第三方Charlie制备一系列相互独立的Bell态$\left|\Phi_{\mathrm{AB}}^{+}\right\rangle$, 将纠缠双方通过两侧的量子信道发送给Alice和Bob。在这里假设Charlie与Eve之间是隔离的, 他们的联合态可以表示为$\left|\Sigma_{\mathrm{ABE}}\right\rangle=\left|\Phi_{\mathrm{AB}}^{+}\right\rangle\otimes|E\rangle$, 其中$|E\rangle$是Eve所制备的辅助量子态。Alice和Charlie的量子信道与Bob和Charlie之间的量子信道虽然是相互独立的, 但是Alice和Bob在生成密钥的过程中地位是等价的。首先, 他们各自所获得的随机比特串之间是相互关联的, 比特翻转错误发生的位置 (无论是Alice侧还是Bob侧) 对最终生成的密钥串没有影响; 其次, 在后处理过程中, 关于纠错和保密放大的信息可以从Alice发送给Bob, 或者相反。为了简化讨论, 可以假设比特翻转错误只发生在一侧的量子信道上, 因此Eve只需要对单侧的信道进行集体攻击。Alice和Bob随机地选取两组互无偏基对所接收到的量子态进行测量, 并通过经典信道公布他们的测量基信息。Eve根据Alice和Bob的对基信息选取最优的POVM测量以尽可能多地获取他们之间的密钥信息。

集体攻击的核心部分是两体耦合作用, 即Eve的辅助量子态与传输量子态之间的耦合作用。在两体耦

合作用中选取传输量子态的一对计算基$|0\rangle$、$|1\rangle$, 它们也是Alice 和Bob进行量子态编码时所用的Z基, 其与X基的关系为

$$\begin{cases} |+\rangle = \dfrac{\sqrt{2}}{2}\left[|0\rangle + |1\rangle\right] \\ |-\rangle = \dfrac{\sqrt{2}}{2}\left[|0\rangle - |1\rangle\right] \end{cases}. \tag{1}$$

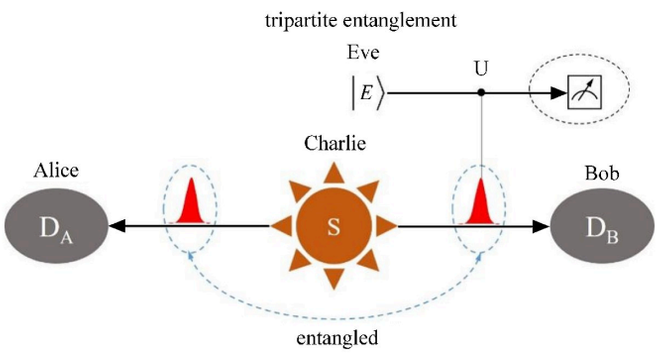

图 1　E91-QKD中集体攻击的示意图

Fig. 1　Schematic diagram of collective attack in E91-QKD

窃听者实施集体攻击操作可能用到的两体耦合作用如图 2 所示, 两体耦合作用可以分为两大类, 分别对应于相位耦合和能级跃迁耦合。两体相位耦合是量子计算中最常用到的量子比特操作, 可以用量子可控相位门操作U_1表示。如图 2(a) 所示, 把传输量子态看作控制量子态, 辅助量子态$|E\rangle$看作目标态, 在相位耦合下$|E\rangle$在布洛赫球上沿着某一纬度线旋转, 旋转的角度由作用强度和作用时间共同决定。在这里假设量子态$|E\rangle$的维度不受限制, 图 2(a) 显示的是在相位耦合中$|E\rangle$处在n维布洛赫球中, 其初始态为$|E\rangle = \dfrac{1}{\sqrt{n}}\sum_{j=0}^{n-1} \mathrm{e}^{\mathrm{i}\theta_j}\left|j\right\rangle_{\mathrm{E}}$。假设$|E\rangle$的初始相位$\theta_{\mathrm{i}} = 0$, 在相位耦合操作下$|E\rangle$的演化可以表示为

$$\begin{cases} U_1|0\rangle|E\rangle = |0\rangle\left|p\right\rangle \\ U_1|1\rangle|E\rangle = |1\rangle\left|q\right\rangle \end{cases}, \tag{2}$$

式中: $\left|p\right\rangle = \dfrac{1}{\sqrt{n}}\sum_{j=0}^{n-1}\mathrm{e}^{\mathrm{i}j\theta_p}\left|j\right\rangle_E$, $\left|q\right\rangle = \dfrac{1}{\sqrt{n}}\sum_{j=0}^{n-1}\mathrm{e}^{\mathrm{i}j\theta_q}\left|j\right\rangle_E$, $\left\langle p|q\right\rangle = \dfrac{1}{n}\sum_{j=0}^{n-1}\mathrm{e}^{\mathrm{i}j\left(\theta_q-\theta_p\right)}$. 通过连续调节$\theta_p$和$\theta_q$的值, 可以得到$\left|\left\langle p|q\right\rangle\right| \in [0,1]$。

图 2(b) 显示的是两体能级跃迁耦合操作U_2, 在U_2的作用下量子态的演化可表示为

$$\begin{cases} U_2|0\rangle|E\rangle = |1\rangle|r\rangle \\ U_2|1\rangle|E\rangle = |0\rangle|s\rangle \end{cases}, \tag{3}$$

式中$|0\rangle$、$|1\rangle$代表某种耦合作用下Hamiltonian的两个能级, 它们之间存在能级差。总的两体耦合算子可以表示为$U = \sqrt{1-f}U_1 + \sqrt{f}U_2$, 其中

$$\begin{cases} U|0\rangle|E\rangle = \sqrt{1-f}|0\rangle\left|p\right\rangle + \sqrt{f}|1\rangle|r\rangle \\ U|1\rangle|E\rangle = \sqrt{1-f}|1\rangle\left|q\right\rangle + \sqrt{f}|0\rangle|s\rangle \end{cases}, \tag{4}$$

式中f为能级跃迁的概率。因为$|E\rangle$由n个量子态线性叠加而成, 则 $0\le|\langle r|s\rangle|<\frac{n-2}{n}$, 以及 $\lim\limits_{n\to\infty}\frac{n-2}{n}=1$, 并且$|p\rangle$、$|q\rangle$、$|r\rangle$、$|s\rangle$之间的内积关系可完全由Eve调控。从 (4) 式可以看出, $\{\langle r|,\langle s|\}\{|p\rangle,|q\rangle\}=0$对Eve的窃听操作最有利。

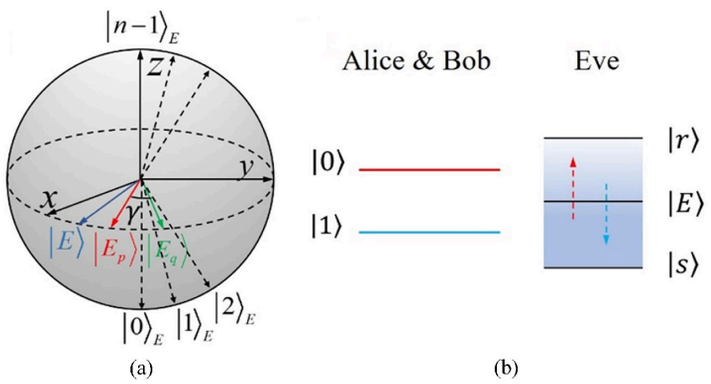

图 2 两体耦合示意图。(a) 两体相位耦合; (b) 两体能级跃迁耦合

Fig. 2 Schematic diagram of bipartite coupling. (a) Bipartite phase coupling; (b) Bipartite energy level transfer coupling

如图 1 所示, 假设Eve只对Bob侧信道进行攻击, 所得到的结论与两侧均进行攻击是一致的。设Charlie发送的纠缠态为

$$|\Phi^+_{\rm AB}\rangle=\frac{\sqrt{2}}{2}\left[|0\rangle_{\rm A}|0\rangle_{\rm B}+|1\rangle_{\rm A}|1\rangle_{\rm B}\right], \tag{5}$$

将 (4) 式中的集体攻击作用到Bell态$|\Phi^+_{\rm AB}\rangle$的Z基上, 则

$$U|\Phi^+_{\rm AB}\rangle|E\rangle=\frac{\sqrt{2}}{2}\sqrt{p_{r,{\rm Z}}}\left[|0\rangle_{\rm A}|0\rangle_{\rm B}|p\rangle_{\rm Z}+|1\rangle_{\rm A}|1\rangle_{\rm B}|q\rangle_{\rm Z}\right]+\frac{\sqrt{2}}{2}\sqrt{p_{e,{\rm Z}}}\left[|0\rangle_{\rm A}|1\rangle_{\rm B}|r\rangle_{\rm Z}+|1\rangle_{\rm A}|0\rangle_{\rm B}|s\rangle_{\rm Z}\right], \tag{6}$$

式中$p_{r,{\rm Z}}$、$p_{e,{\rm Z}}$分别表示两体操作中Z基上无比特翻转和有比特翻转的概率, $p_{r,{\rm Z}}=1-f$, $p_{e,{\rm Z}}=f$。(6) 式在X基上可以表示为

$$U|\Phi^+_{\rm AB}\rangle|E\rangle=\frac{\sqrt{2}}{2}\sqrt{p_{r,{\rm X}}}\left[|+\rangle_{\rm A}|+\rangle_{\rm B}|p\rangle_{\rm X}+|-\rangle_{\rm A}|-\rangle_{\rm B}|q\rangle_{\rm X}\right]+\frac{\sqrt{2}}{2}\sqrt{p_{e,{\rm X}}}\left[|+\rangle_{\rm A}|-\rangle_{\rm B}|r\rangle_{\rm X}+|-\rangle_{\rm A}|+\rangle_{\rm B}|s\rangle_{\rm X}\right], \tag{7}$$

式中$|p\rangle_{\rm X}$、$|q\rangle_{\rm X}$、$|r\rangle_{\rm X}$、$|s\rangle_{\rm X}$可以表示为

$$\begin{cases}
|p\rangle_{\rm X}=\dfrac{\sqrt{1-f}\left(|p\rangle_{\rm Z}+|q\rangle_{\rm Z}\right)+\sqrt{f}\left(|r\rangle_{\rm Z}+|s\rangle_{\rm Z}\right)}{2\sqrt{p_{r,{\rm X}}}}\\
|q\rangle_{\rm X}=\dfrac{\sqrt{1-f}\left(|p\rangle_{\rm Z}+|q\rangle_{\rm Z}\right)-\sqrt{f}\left(|r\rangle_{\rm Z}+|s\rangle_{\rm Z}\right)}{2\sqrt{p_{r,{\rm X}}}}\\
|r\rangle_{\rm X}=\dfrac{\sqrt{1-f}\left(|p\rangle_{\rm Z}-|q\rangle_{\rm Z}\right)-\sqrt{f}\left(|r\rangle_{\rm Z}-|s\rangle_{\rm Z}\right)}{2\sqrt{p_{e,{\rm X}}}}\\
|s\rangle_{\rm X}=\dfrac{\sqrt{1-f}\left(|p\rangle_{\rm Z}-|q\rangle_{\rm Z}\right)+\sqrt{f}\left(|r\rangle_{\rm Z}-|s\rangle_{\rm Z}\right)}{2\sqrt{p_{r,{\rm X}}}}
\end{cases}, \tag{8}$$

式中$p_{r,\mathrm{X}}$、$p_{e,\mathrm{X}}$分别表示两体操作中X基上无比特翻转和有比特翻转的概率, 可表示为

$$\begin{cases} p_{e,\mathrm{X}}=\dfrac{1}{2}\left[1-(1-f)\langle p|q\rangle_{\mathrm{Z}}-f\langle r|s\rangle_{\mathrm{Z}}\right] \\ p_{r,\mathrm{X}}=1-p_{e,\mathrm{X}} \end{cases}. \tag{9}$$

将下标Z舍去, 在不做特殊说明的情况下默认$|p\rangle$、$|q\rangle$、$|r\rangle$、$|s\rangle$是在Z基表象下Eve的辅助量子态, 可得到系统的误比特率为

$$p_e=\frac{1}{2}\left(p_{e,\mathrm{Z}}+p_{e,\mathrm{X}}\right)=\frac{1}{4}\left[1-(1-f)\langle p|q\rangle+f\left(2-\langle r|s\rangle\right)\right]. \tag{10}$$

2　POVM测量

在Alice和Bob对接收到的量子态完成测量之后, 他们分别得到一组随机数K_{A}、K_{B}, 其差错图案为$E_{\mathrm{AB}}=K_{\mathrm{A}}\oplus K_{\mathrm{B}}$, 其中⊕为Xor操作。由于Alice和Bob的地位是等价的, 因此任意一方均可以作为密钥协商的密钥参考标准。下面分析在集体攻击下Eve可窃取关于密钥K_{A}或K_{B}的最大信息量。在Alice和Bob公布完他们的测量基后, 三体纠缠态为

$$\rho_{\mathrm{ABE}}=\sum_{K_{\mathrm{A}}}p\left(K_{\mathrm{A}}\right)|K_{\mathrm{A}}\rangle\langle K_{\mathrm{A}}|\otimes\sum_{K_{\mathrm{B}}}p\left(K_{\mathrm{B}}|K_{\mathrm{A}}\right)|K_{\mathrm{B}}\rangle\langle K_{\mathrm{B}}|\otimes\rho_{K_{\mathrm{B}}|K_{\mathrm{A}}}(E), \tag{11}$$

式中: K_{A}、K_{B}是测量结果的典型序列, $\rho_{K_{\mathrm{B}}|K_{\mathrm{A}}}(E)$是对应的Eve的辅助量子态序列。由于在集体攻击中, Eve独立地对每一个Bell态进行攻击, 因此有

$$\rho_{K_{\mathrm{B}}|K_{\mathrm{A}}}(E)=\rho_{k_{\mathrm{B}}^1|k_{\mathrm{A}}^1}\left(E_1\right)\otimes\rho_{k_{\mathrm{B}}^2|k_{\mathrm{A}}^2}\left(E_2\right)\otimes\cdots\otimes\rho_{k_{\mathrm{B}}^n|k_{\mathrm{A}}^n}\left(E_n\right), \tag{12}$$

式中: n为比特串的长度, $k_{\mathrm{A(B)}}^i$为比特串$K_{\mathrm{A(B)}}$中第i个比特的值, $|E_i\rangle\in\left\{|p\rangle_{\mathrm{Z(X)}},|q\rangle_{\mathrm{Z(X)}},|r\rangle_{\mathrm{Z(X)}},|s\rangle_{\mathrm{Z(X)}}\right\}$, 于是Eve与Bob之间的互信息满足

$$\chi\left(E;K_{\mathrm{B}}|K_{\mathrm{A}}\right)\le\sum_{i=1}^{n}\chi\left(E_i;k_{\mathrm{B}}^i|k_{\mathrm{A}}^i\right). \tag{13}$$

该公式给出了Eve可获取关于Alice和Bob的每个比特的信息量。

在Alice和Bob通过经典信道公布完测量基后, Eve对辅助量子态选取合适的POVM测量来区分$|p\rangle_{\mathrm{Z(X)}}$和$|q\rangle_{\mathrm{Z(X)}}$、$|r\rangle_{\mathrm{Z(X)}}$和$|s\rangle_{\mathrm{Z(X)}}$。对于区分两个非正交量子态, 可以证明投影测量是其中一种最佳的POVM测量方案[14], 区分非正交量子态$|a\rangle$、$|b\rangle$可获取的最大信息量为$1-H\left(\dfrac{1+\sin 2\alpha}{2}\right)$, 其中$|\langle a|b\rangle|=\cos 2\alpha$为被区分的两个量子态之间的交叠, $H(x)=-x\log_2 x-(1-x)\log_2(1-x)$表示Shannon熵, $\forall x\in[0,1]$。图3给出了Eve可窃取的信息量对$\langle p|q\rangle$和$\langle r|s\rangle$的依赖关系, p_{e}为(10)式给出的系统的平均误比特率。根据(10)式, 蓝色区域将得到$f<0$, 这与概率大于等于0相违背, 因此将这部分的互信息设为0。在仿真中, 选取$p_{\mathrm{e}}=0.08$, 仿真结果发现, 当$\langle p|q\rangle=\langle r|s\rangle=1-2p_{\mathrm{e}}$时$\chi_{\mathrm{E;AB}}$有最大值, 即

$$\chi_{\mathrm{E;AB}}^{\mathrm{M}}=1-H\left[\frac{1+2\sqrt{p_{\mathrm{e}}(1-p_{\mathrm{e}})}}{2}\right]. \tag{14}$$

此时$p_{e,X}=p_{e,Z}=p_e$, 即X基和Z基上有相同的误比特率。在集体攻击方案下系统的密钥率上限为

$$r_{\mathrm{coll}}=H\left[\frac{1+2\sqrt{p_e(1-p_e)}}{2}\right]-H(p_e). \tag{15}$$

基于纠缠纯化协议的安全性证明是QKD中最广泛用到的安全性证明方案, 该证明方案可以不考虑外界具体的窃听行为。它所提供的密钥率上限为$r_{\mathrm{EPP}}=1-H(e_Z)-H(e_X)$, 等于通过纠缠纯化协议可从Alice和Bob的联合量子态所提纯出的最大Bell态的数目。然而该方案由于对Eve可能的窃听方式缺少具体的分析, 所得密钥率的上限理论上是较为宽松的。图4为E91-QKD基于纠缠纯化协议和基于集体攻击的安全性证明的密钥率对比。从图中可以发现, 相对于纠缠纯化协议, 基于集体攻击的安全性证明在考虑外界具体可能的窃听操作之后, 可以有效地提高系统的密钥率, 同时还将对误比特率的容忍度从11% 提升到了14.6%。

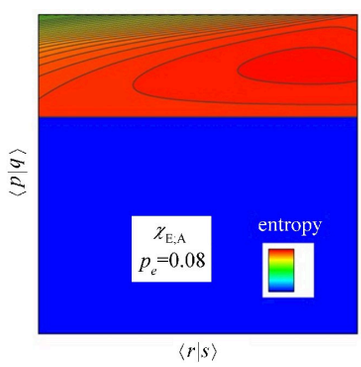

图3 $\chi_{\mathrm{E;A}}$的值对$\langle p|q\rangle$和$\langle r|s\rangle$依赖关系的仿真图

Fig. 3 Simulation of $\chi_{\mathrm{E;A}}$ with respect to $\langle p|q\rangle$ and $\langle r|s\rangle$

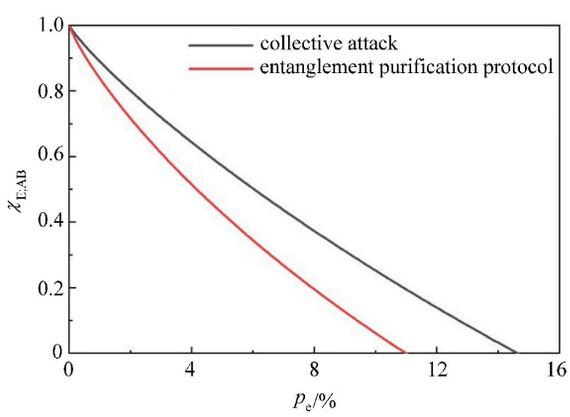

图4 基于集体攻击和纠缠纯化协议的E91-QKD密钥率的对比

Fig. 4 Comparison of the key rate for the security proofs of E91-QKD based on collective attack and entanglement purification protocol

3 结 论

研究并分析了在E91-QKD中集体攻击的窃听能力。假设Alice和Bob的测量设备是可以被完全表征的, 并且Eve无法访问。广义的集体攻击操作可由量子两体耦合算子构成, 包含两体相位耦合和能级跃迁耦合。

在最佳的集体攻击方案中, Z基和X基上的窃听是对称的。与基于纠缠纯化的安全性证明对比, 可以发现基于集体攻击的安全性证明对Eve的窃听能力的评估提供了更加紧致的上限, 并有效地提升了系统的密钥率和对误比特率的容忍度。

参考文献:

[1] Ekert A K. Quantum cryptography based on Bell's theorem [J]. *Physical Review Letters*, 1991, 67(6): 661-663.

[2] 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.

[3] Xu F H, Ma X F, Zhang Q, *et al*. Secure quantum key distribution with realistic devices [J]. *Reviews of Modern Physics*, 2020, 92(2): 025002.

[4] Ye W, Zhong H, Liao Q, *et al*. Improvement of self-referenced continuous-variable quantum key distribution with quantum photon catalysis [J]. *Optics Express*, 2019, 27(12): 17186-17198.

[5] Hu L Y, Al-amri M, Liao Z Y, *et al*. Continuous-variable quantum key distribution with non-Gaussian operations [J]. *Physical Review A*, 2020, 102: 012608.

[6] Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances [J]. *Science*, 1999, 283 (5410): 2050-2056.

[7] Fröhlich B, Lucamarini M, Dynes J F, *et al*. Long-distance quantum key distribution secure against coherent attacks [J]. *Optica*, 2017, 4(1): 163-167.

[8] Biham E, Mor T. Security of quantum cryptography against collective attacks [J]. *Physical Review Letters*, 1997, 78(11): 2256-2259.

[9] Acín A, Brunner N, Gisin N, *et al*. Device-independent security of quantum cryptography against collective attacks [J]. *Physical Review Letters*, 2007, 98(23): 230501.

[10] Biham M, Boyer G, Brassard J, *et al*. Security of quantum key distribution against all collective attacks [J]. *Algorithmica*, 2002, 34(4): 372-388.

[11] Pironio S, Acín A, Brunner N, *et al*. Device-independent quantum key distribution secure against collective attacks [J]. *New Journal of Physics*, 2009, 11(4): 045021.

[12] Li W, Wang L, Zhao S M. Phase matching quantum key distribution based on single-photon entanglement [J]. *Scientific Reports*, 2019, 9: 15466.

[13] Yin Z Q, Fung C H F, Ma X F, *et al*. Measurement-device-independent quantum key distribution with uncharacterized qubit sources [J]. *Physical Review A*, 2013, 88(6): 062322.

[14] Fuchs C A, Gisin N, Griffiths R B, *et al*. Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy [J]. *Physical Review A*, 1997, 56(2): 1163-1172.

[15] Bennett C H, DiVincenzo D P, Smolin J A, *et al*. Mixed-state entanglement and quantum error correction [J]. *Physical Review A*, 1996, 54(5): 3824-3851.

[16] Bruß D. Optimal eavesdropping in quantum cryptography with six states [J]. *Physical Review Letters*, 1998, 81(14): 3018-3021.

[17] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol [J]. *Physical Review Letters*, 2000, 85(2): 441-444.

[18] 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.

[19] Renner R. Security of quantum key distribution [J]. *International Journal of Quantum Information*, 2008, 6(1): 1-127.

[20] Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography [J]. *Physical Review Letters*, 2005, 94 (23): 230503.

[21] Lo H K, Ma X F, Chen K. Decoy state quantum key distribution [J]. *Physical Review Letters*, 2005, 94(23): 230504.

[22] Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution [J]. *Physical Review Letters*, 2012, 108 (13): 130503.