基于态关联性不完美的诱骗态量子密钥分配

周 淳,鲍皖苏,付向群
(解放军信息工程大学电子技术学院,河南郑州 450004)

摘 要: 本文提出了态关联性不完美条件下诱骗态量子密钥分配(QKD)的安全性理论分析模型.借助于 QKD 的保密放大分析方法,采用实际 QKD 系统广泛使用的诱骗态编码方案,使相位误码的估计更加准确,进而给出了态关联性不完美条件下诱骗态 QKD 的最终安全密钥生成率的表达式,刻画了密钥生成率与态关联性不完美、探测器性能和密钥传输距离之间的关系.数值模拟表明,诱骗态 QKD 的最终安全密钥生成率对态关联性不完美的容忍程度,随着密钥传输距离的增大而逐渐减小,随着探测器探测性能的提升而逐渐增大,因而验证了所给表达式的正确性.

关键词: 量子密钥分配; 态关联性不完美; 诱骗态; 实际安全性
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2012) 10-2015-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.10.019

Decoy-State Quantum Key Distribution Based on State-Dependent Imperfections

ZHOU Chun, BAO Wan-su, FU Xiang-qun
(*Institute of Electronic Technology, the PLA Information Engineering University, Zhengzhou, Henan* 450004, *China*)

Abstract: This paper proposes models for analyzing the security of decoy-state quantum key distribution (QKD) with state-dependent imperfections. With the privacy amplification method of QKD's post-processing techniques, we introduce the decoy-state method used widely in QKD system to estimate the phase error rate more accurately than the case without decoy-state method. Based on this, we obtain the formula of secret key generation rates for decoy-state QKD with state-dependent imperfections, and characterize the relationship among key generation rates, state dependent parameter, detection efficiency and transmission distance. Numerical simulations indicate that the secure key generation rates' tolerance to state-dependent imperfections decreases with the growing distance, but increases with the improving detection efficiency, which, to some extent, show the validity of the formula we obtain.

Key words: quantum key distribution; state-dependent imperfections; decoy state; practical security

1 引言

众所周知,密钥是密码安全的关键.长期以来,如何使密码通信双方安全地获取密钥一直是人们关注的热点[1~3].量子密钥分配(QKD)是通信双方(Alice 和 Bob)如何利用量子物理机制实现密钥安全分配的过程.自从第一个 QKD 协议—BB84[1]提出以来,QKD 的安全性从各个层面得到了充分证明[4~7],QKD 实验已经从简单的点对点发展到量子密钥分配网络[8,9].理想条件下 QKD 已被证明是无条件安全的[4,5],然而,实际条件下 QKD 系统不可能做到绝对完美,比如光源存在强度涨落、量子态制备与调制存在误差、实际信道存在固有损耗、探测器性能不理想等等.这些不完美因素都给 QKD 带来了许多潜在的安全隐患,探讨其对实际 QKD 系统安全性的影响一直是人们最关心的问题.

由于实际光源与探测器的设备器件存在缺陷,量子态在对照基进行制备和测量的过程中不可能做到完全精确,存在不可避免的偏差,称这种偏差为态不完美性偏差.Gottesman 等人[6]分析了光源与探测器不完美情形下 QKD 的安全性,首次给出了非理想条件下 QKD 安全密钥生成率的 GLLP 公式,但是其分析局限于态不完美性偏差非常小情形.若这种偏差完全由窃听者 Eve 控制,能够用与基信息无关的酉变换表示出来,就称这种因器件缺陷导致的态不完美性偏差为态独立性(state-independent)不完美.但是实际条件下这种偏差不可能受 Eve 的完全控制,必然与基信息相关联,此时就称这种

收稿日期:2011-04-29;修回日期:2011-09-19

态不完美性偏差为态关联性(state-dependent)不完美.针对一般情形的态关联性不完美 QKD,李宏伟等人[10]于2010年基于纠缠提纯给出了其详尽细致的安全性证明,同年,Marøy 等人[11]从另外一种角度出发,基于Koashi[12,13]的安全性分析方法给出了态关联性不完美QKD的另一种安全性证明,得到了态关联性不完美QKD准确的安全密钥生成率公式.

2003 年,Hwang[14]提出的诱骗态方法,不仅可以抵抗光子数分束攻击(PNS),也可以大幅度提高实际 QKD系统的最终密钥生成率(KGR)和最大安全传输距离(SCD)[15].2005 年,Lo[16]首次结合诱骗态与 GLLP 分析思想,给出了诱骗态 QKD 的无条件安全性证明,但是该安全性证明要求合法通信双方拥有无穷多个诱骗态,王向斌[17,18]给出了几种接近实用的有限诱骗态编码方案并给出了其无条件安全性证明.但是,针对广泛采用诱骗态编码方案的实际 QKD 系统,还未有人分析态关联性不完美对诱骗态 QKD 安全性的影响,因此研究态关联不完美如何影响诱骗态 QKD 安全性的问题具有重要的实际意义.

本文首先给出了态关联性不完美条件下诱骗态QKD的安全性分析理论模型,基于该模型并利用 QKD的保密放大分析方法,得到了态关联不完美条件下诱骗态 QKD 的最终安全密钥生成率表达式.数值模拟表明,诱骗态 QKD 的最终安全密钥生成率对态关联性不完美的容忍程度,随着密钥传输距离的增大而逐渐减小,随着探测器探测性能的提升而逐渐增大.

2 态关联性不完美诱骗态 QKD 理论模型及分析

诱骗态思想的关键之处在于通过随机地改变实际光脉冲的强度,能更加准确地估计出单光子计数的下界和量子比特错误率的上界.在实际的诱骗态 QKD 实验中,只需要在原有信号态光源的基础上增加一个诱骗态光源,其它设备保持不变.下面,基于 Marøy 的安全性分析模型[11],给出诱骗态 QKD 在态关联性不完美条件下的理论分析模型,该模型包括态制备、态测量、初始密钥协商、纠错和保密放大四个部分.

2.1 态制备

诱骗态光源和信号态光源唯一的不同就是光源强度不同,通常要求信号态光源强度大于诱骗态光源强度,即 $\mu \geqslant \mu'$.在态关联性不完美条件下,可以将信号态光源与诱骗态光源视为两个独立的光源.

对于信号态光源(或者诱骗态光源)发出的光子信号,Alice 首先通过随机变量 a 来选择基$Z=\{|0\rangle,|1\rangle$或基$X=\{|+\rangle,|-\rangle\}$(下文简称为基变量),然后对照所选择的基将光子信号制备成量子态$|\chi_a\rangle$,并将其发送给 Bob:

$$\begin{cases} a=Z \longrightarrow |\chi_Z\rangle=\sqrt{p_Z}|0\rangle|\beta_0\rangle+\sqrt{1-p_Z}|1\rangle|\beta_1\rangle \\ a=X \longrightarrow |\chi_X\rangle=\sqrt{p_X}|+\rangle|\beta_+\rangle+\sqrt{1-p_X}|-\rangle|\beta_-\rangle \end{cases}$$

其中态$|\beta_i\rangle(i=0,1,+,-)$(下文简称为 β 态)所在的系统与 Alice 的系统直接相关,并且 Eve 能够进入此系统对其中的态进行操作,因此 Eve 可以借助于 β 态来获取对她有利的信息.在下文中,我们将由信号态光源产生的光子制备成的量子态简称为信号态,将由诱骗态光源产生的光子制备成的量子态简称为诱骗态.

量子态在制备过程中必然存在态关联性不完美,若基变量为 a($a=X$ 或 $a=Z$),Alice 实际制备的量子态为 ρ_a,则态关联性不完美可由 ρ_Z 和ρ_X 之间的保真度 F 来刻画,F 满足

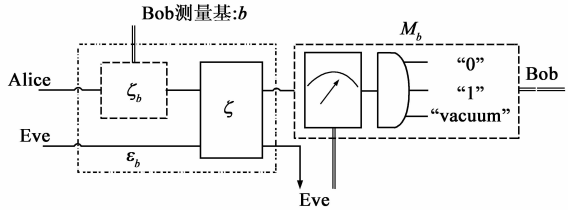
$$F=F(\rho_Z,\rho_X)\equiv Tr(\sqrt{\rho_Z}\rho_X\sqrt{\rho_Z})^{\frac{1}{2}}.$$

定义参数 Δ 使 F 存在下界 $1-2\Delta$,即 $F\geqslant 1-2\Delta$,则 Δ 反映了态关联性不完美的程度.根据 Uhlmann 定理[19],存在 ρ_a 的纯态$|\chi_a\rangle$,使得$\langle\chi_Z|\chi_X\rangle=1-2\Delta$.$\Delta$ 越小,态关联性不完美的程度越小,特殊情况当 $\Delta=0$ 时则说明态制备过程是理想的,称 Δ 为态关联性不完美参数.Marøy 具体给出了计算 Δ 的方法,分析得到了 Δ 的一个下界(下文中的式(3))[11].

信号态与诱骗态除了光强不一样外,其它性质都是相同的,从参数 Δ 的定义可以看出,Δ 并不能用来区分信号态与诱骗态.

2.2 态测量

Koashi 的分析模型[12,13]并不需要引入 Squash 操作,在态独立性不完美条件下,其对探测器的假设与实际的探测器模型并不完全等价,因此 Marøy 给出了态关联性不完美条件下的无诱骗态 QKD 的探测器模型,如图 1 所示[11].诱骗态的引入并不需要对探测器作任何改动,因而诱骗态 QKD 的探测器模型与无诱骗态情形是一样的.



说明:单线条代表量子态信息,双线条代表经典信息

图1 态关联性条件下探测器模型图

在上述的探测器模型中,ζ_b 为作用在量子态光学模式 Fock 空间上的量子变换,该变换由 Bob 选择的基变量 b 控制,刻画了 QKD 实际探测过程态关联性不完美对 QKD 安全性的影响;ζ 为作用在量子态上并与探测器固有自由度相关联的量子变换,可由 Eve 完全控

制,反映了实际探测器中噪声与 Eve 攻击的影响.将这两种影响分别进行考察能更加准确地考察实际 QKD 系统的安全性,这与文献[10]的分析模型是一致的.

2.3 初始密钥协商

初始密钥来源于信号态,约定如果探测器对任何一个信号态的测量结果为非"vacuum",则称探测器形成一次有效计数.若 $a = b = X$,Alice 和 Bob 都公布他们的测量结果,此时计数率记为 q_X;若 $a = Z, b = X$,Alice 和 Bob 公布测量结果,此时可以得到 X 基测量下的误码率 δ_X,此情况下的计数率记为 q_{ph}.若有 n 个态满足 $a = b = Z$,则最后 Alice 和 Bob 依据测量结果可以得到长度为 nq_Z 的初始密钥,其中 q_Z 为 $a = b = Z$ 时的计数率.

2.4 纠错与保密放大

纠错旨在估计量子比特错误包含的信息量,在此协议中即为 $a = b = Z$ 时发生误码事件的熵 $h(\delta_Z)$,其中函数 $h(\cdot)$为二进制 Shannon 熵.保密放大采用 Koashi 在文献[12]中的估计方法,这里就不再赘述,最终 Alice 与 Bob 可以获得安全的密钥长度为 $nq_Z - H$,其中 H 与 q_X、δ_X、q_{ph}的值有关.

以上我们给出了态关联性不完美条件下诱骗态 QKD 的安全性分析理论模型,其与 Marøy 等人模型相比,最本质的区别在于保密放大过程中对 H 的估计不同,诱骗态的引入可以更加准确地估计出 H 的上界.

态制备模型中 β 态的引入是为了与实际信道模型相符,信道噪声程度与 Eve 不同的攻击操作可由 β 态的不同属性来衡量,这里所说的属性是指 β 态的光子极性、波长以及统计数量等,Alice 经由 Eve 发送 N 个量子态给 Bob 的同时也产生了大量的 β 态.在 Koashi 的安全性分析中[12],为了达到保密放大的目的,假定 Alice 又对其所拥有的 nq_Z 个生成初始密钥的态在基 X 下进行了测量,Bob 通过测量算子 M_X 对自己手中的 nq_Z 个态实施测量,并结合 β 态的属性来对 Alice 的测量结果进行预测,此时的误码率记为 δ_{ph},δ_{ph}值决定了保密放大的效果,亦即影响对 H 值的估计,δ_{ph}与 H 的具体关系表达式参见文献[12].采用诱骗态方法,可以更好地界定 δ_{ph}的取值范围,在下文中将详细讨论.我们的模型结合了 Koashi 的安全性分析方法与诱骗态思想,与 Marøy 的模型是显著不同的.

以下给出态关联性不完美下诱骗态 QKD 密钥生成率关于 δ_{ph}、Δ 和 q_X 的准确表达式.

3 态关联性不完美下诱骗态 QKD 密钥生成率

在上述安全性分析模型下,最终的安全密钥生成率为:

$$R_Z \geqslant 1 - H/nq_Z - h(\delta_Z) \tag{1}$$

其中,n 代表满足基变量是 $a = b = Z$ 时的光子态,R_Z 表示协议中基变量为 $a = b = Z$ 时产生的安全密钥率,q_Z 是基变量为 $a = b = Z$ 时探测器的计数率,δ_Z 是基变量为 $a = b = Z$ 时的误码率,H 为保密放大过程估计 Eve 攻击获取的最大信息量.

表达式(1)与无诱骗态情形是相同的,H 的大小决定了密钥生成率的大小,但诱骗态方法能给出 H 上界值更加准确的估计.H 的取值必然与 Δ 的取值和变换 ζ_b 的作用相关,H、Δ 和 ζ_b 三者之间的关系刻画能反映态关联性不完美对诱骗态 QKD 安全性的影响.

Marøy 给出了无诱骗态下 H、Δ 和 ζ_b 三者之间的关系,得到了最终安全密钥生成率的表达式[11]:

$$R_Z \geqslant \omega_Z q_{ph}/q_Z[1 - h(\overline{\delta}_{ph})] - h(\delta_Z) \tag{2}$$

其中 ω_Z 为非空量子态被探测到结果为"0"或"1"的最低概率,用来衡量探测器的探测性能,γ_Z 代表探测器泄露给 Eve 的信息量,$\overline{\delta}_{ph} \leqslant \delta_{ph} + \dfrac{\gamma_Z}{q_X\omega_Z} \leqslant 0.277$,$\delta_{ph}$满足下式,即

$$1 - 2\Delta \leqslant \sqrt{q_X(1-\delta_X)q_{ph}(1-\delta_{ph})} + \sqrt{q_X\delta_X q_{ph}\delta_{ph}} + \sqrt{(1-q_X)(1-q_{ph})} \tag{3}$$

其中,q_X 是基变量为 $a = b = X$ 时探测器的计数率,q_{ph}、δ_X 分别为基变量为 $a = Z, b = X$ 时探测器的计数率和误码率,δ_{ph}为相位误码率.

在诱骗态情形下,式(1)中对 H 的有效估计转化为式(2)中对$\overline{\delta}_{ph}$的有效估计.

上面的式(3)并不能直接作为实际情形 QKD 系统计算安全密钥生成率的公式,QKD 系统必须与实际量子光源、量子信道及光学探测器相结合,比如实际量子光源采用的大多是带衰减的弱相干态光源,光子在量子光纤信道传输过程中不可避免地存在损耗,实际的光学探测器基本上属于阈值探测器等.下面,我们首先分析实际量子光源条件下态关联性不完美对 QKD 系统密钥生成率的影响,并结合诱骗态分析思想,得到态关联性不完美条件下诱骗态 QKD 的最终安全密钥生成率.

QKD 的安全性证明关键在于 Eve 所能获取的最大信息量的估计,体现在具体的协议及模型分析中,可以直观地概括为:若产生 1 比特初始密钥,必须消耗一部分用于估计 Eve 获取的信息量(亦即保密放大),一部分用于估计 QKD 过程所产生误码的信息量(亦即量子纠错),最终才能得到安全的共享密钥.依据这个思路,式(2)也可以表示为

$$R_Z \geqslant 1 - \{1 - \omega_Z q_{ph}/q_Z[1 - h(\overline{\delta}_{ph})]\} - h(\delta_Z) \tag{4}$$

其中 1 比特初始密钥中的 $1 - \omega_Z q_{ph}/q_Z[1 - h(\overline{\delta}_{ph})]$部分用于保密放大,$h(\delta_Z)$部分用于纠错.

实际的 QKD 系统中,假设光源发出的光子数服从分布 $P(\mu,n)$,其中 μ 为光源强度参数,n 代表光子数.对于 BB84 协议,初始密钥比特主要来源于单光子的贡献(还有少量来源于真空态脉冲),其中一部分用于保密放大,另外一部分用于量子纠错. QKD 实验中,平均光子计数 Q_μ、平均量子比特误码 E_μ、真空态计数 Q_0 都是可以通过实验直接测量的物理量,因此可借助于纠错算法对纠错部分的信息量 $h(\delta_Z)$ 进行估计,即假定[16]

$$h(\delta_Z)=\frac{Q_\mu f(E_\mu)h(E_\mu)}{Q_1}$$

其中 Q_1 为单光子计数.这样就得到态关联性不完美条件下实际 QKD 系统的最终安全密钥生成率

$$R\geqslant\frac{1}{2}\left\{-Q_\mu f(E_\mu)h(E_\mu)+Q_0+\frac{Q_1\omega_Z q_{ph}}{q_Z}[1-h(\overline{\delta}_{ph})]\right\} \tag{5}$$

其中 μ 为光源强度参数,Q_μ 为当光源强度为 μ 时 Bob 接收到的平均光子计数,E_μ 为光源的平均量子比特误码率(QBER),Q_0 为真空态计数,Q_1 为单光子计数,$f(E_\mu)$为实际纠错算法的纠错效率(通常取 1.22 作为其近似值).

本文的分析中,假定实际的量子信道对于噪声是对称的,即

$$\begin{cases}q_X=q_{ph}=q_Z=q\\ \delta_X=\delta_Z=e_1\end{cases} \tag{6}$$

此时式(3)转化为

$$\Delta\geqslant\frac{1}{2}q\left(1-\sqrt{(1-e_1)(1-\delta_{ph})}-\sqrt{e_1\delta_{ph}}\right) \tag{7}$$

从而式(5)简化为

$$R\geqslant\frac{1}{2}\{-Q_\mu f(E_\mu)h(E_\mu)+Q_0+Q_1\omega_Z[1-h(\overline{\delta}_{ph})]\} \tag{8}$$

其中$\overline{\delta}_{ph}\leqslant\delta_{ph}+\frac{\gamma_Z}{q\omega_Z}\leqslant 0.277$,$\delta_{ph}$满足式(7).

该表达式表明,实际 QKD 系统的最终安全密钥生成率受到探测器性能 ω_Z、态关联性不完美参数 Δ、单光子误码率 e_1、单光子计数率 q 的综合影响.通过诱骗态方法,可以更加清晰地给出态关联性不完美影响最终安全密钥生成率的具体过程.

诱骗态方法的本质在于,诱骗态光源和信号态光源产生相同光子数脉冲的计数率是相等的,亦即 $Y_n'=Y_n$,其中,Y_n' 代表诱骗态光源产生的 n 光子脉冲的计数率,Y_n 代表信号态光源产生的 n 光子脉冲的计数率.对于 n 光子脉冲的误码率,也存在类似的性质,即 $e_n'=e_n$,其中,e_n' 和 e_n 分别表示诱骗态光源和信号态光源产生的 n 光子脉冲的误码率.

实际 QKD 实验的信道模型中,Y_n 和 e_n 满足

$$\begin{cases}Y_n=\eta_n+(1-\eta_n)p_{dark}\\ e_n=(e_{\det}\eta_n+e_0p_{dark})/Y_n\end{cases} \tag{9}$$

其中 $\eta_n=1-(1-t_{AB}\eta_{Bob})^n$,$p_{dark}$表示 Bob 端单光子探测器的暗计数,$e_{\det}$表示 Bob 端接收装置固有的探测错误率,$e_0$ 的值取为 0.5,t_{AB}为信道传输效率,通常其可以表示为 $t_{AB}=10^{-\alpha d/10}$,α 为损耗系数,d 为光子传输距离,η_{Bob}表示 Bob 端探测装置的总体探测效率.

在本文中,为了刻画态关联性不完美对诱骗态 QKD 安全性的影响,采用理想情形的诱骗态编码方案,即无穷诱骗态编码方案.Lo 等人[16]的分析指出,存在无穷多个诱骗态时,可以通过解线性方程组,唯一地确定诱骗态 QKD 中 n 光子的计数率及误码率,即 Y_n 和 e_n.

因此,容易计算得到 Q_1 及 e_1

$$\begin{cases}Q_1=[\eta_1+(1-\eta_1)p_{dark}]P(\mu,1)\\ e_1=(e_{\det}\eta_1+e_0p_{dark})P(\mu,1)/Q_1\end{cases} \tag{10}$$

结合式(8)和式(10),假设探测器泄露给 Eve 的信息量为 0,即 $\gamma_Z=0$,注意到 $q=\eta_1$,就可以得到态关联性不完美条件下诱骗态 QKD 的最终安全密钥生成率

$$R\geqslant\frac{1}{2}\{-Q_\mu f(E_\mu)h(E_\mu)+Q_0+Q_1\omega_Z[1-h(\delta_{ph})]\}$$

$$\text{s.t.}\begin{cases}Q_1=[\eta_1+(1-\eta_1)p_{dark}]P(\mu,1)\\ \Delta\geqslant\frac{1}{2}\eta_1(1-\sqrt{(1-e_1)(1-\delta_{ph})}-\sqrt{e_1\delta_{ph}})\\ e_1=\frac{(e_{\det}\eta_1+e_0p_{dark})P(\mu,1)}{Q_1}\end{cases} \tag{11}$$

该表达式描述了诱骗态 QKD 密钥生成率与态关联性不完美参数 Δ、探测器性能 ω_Z 和密钥传输距离 L(与 η_1 相关)之间的关系,刻画了态关联性不完美对诱骗态 QKD 密钥生成率影响,可为实际 QKD 系统的完善提供参考.

实际 QKD 系统使用的是有限诱骗态编码方案,目前较为有效的是王向斌提出的三强度诱骗态编码方案[17,18],此时需要对单光子计数 Q_1 的上界及单光子误码 e_1 的下界进行估计.我们在下一步的研究中将重点考察这种情形.

4 数值模拟

下面将通过数值模拟来刻画态关联性不完美对诱骗态 QKD 最终密钥生成率的影响.不防采用弱相干态(WCP)光源作为量子光源,其光子数分布为 $P(\mu,n)=\mu^n e^{-\mu}/n!$,注意到 $Q_\mu=\sum_{n=1}^{\infty}Y_nP(\mu,n)$,$Q_\mu E_\mu=\sum_{n=0}^{\infty}Y_nP(\mu,n)e_n$,结合式(9)可得

$$Q_\mu = 1 + p_{dark} - e^{-\mu\eta_1}$$
$$E_\mu = \left(\frac{1}{2}p_{dark} + e_{\det}(1 - e^{-\mu\eta_1})\right) \Big/ Q_\mu \tag{12}$$

实验参数采用广泛使用的 GYS 实验参数[20],如表 1 所示.

表 1　量子密钥分配实验参数

α(dB/km)	$e_{\det}$(%)	Y_0	η_{Bob}	λ(nm)
0.21	3.3	1.7×10^{-6}	0.045	1550

在实际的 QKD 系统中,对式(11)中态关联性不完美参数 Δ 上界的估计还未完全解决,而且不同探测器 ω_Z 的下界并不一样,因此在表 1 的实验参数下并不能直接利用式(11)计算得到态关联性不完美条件下诱骗态 QKD 的最终密钥生成率.但是我们可以将式(11)看成是 R 关于 d、Δ、ω_Z 和 R 的优化不等式.通过考察密钥生成率的临界状态(亦即 $R=0$)来刻画态关联性不完美对实际 QKD 安全性的影响,此时的 Δ 称为态关联性容忍度,代表 QKD 对态关联性不完美可以容忍的偏差,Δ 越大,可容忍的偏差越大.取 $\mu=0.48$,我们在图 2、图 3 中给出了临界情形描述 d、Δ 与 ω_Z 三者之间关系的数值模拟图.

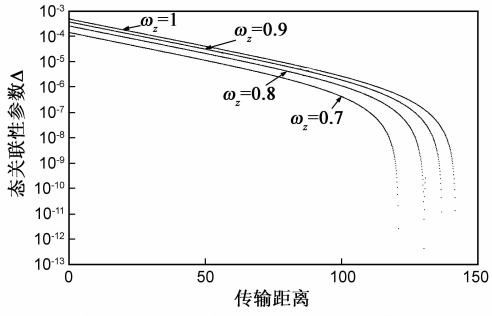


图2　临界情形不同ω_z下态关联性不完美参数Δ与密钥传输距离d的关系比较

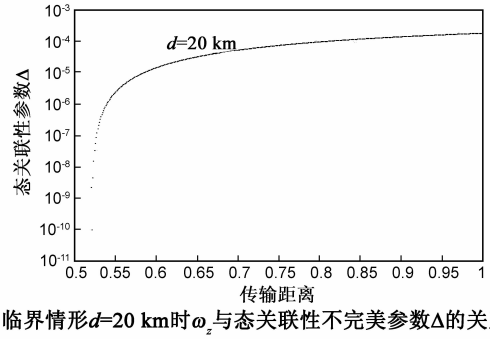


图3　临界情形d=20 km时ω_z与态关联性不完美参数Δ的关系比较

由图 2 可知,随着密钥传输距离的增大,态关联性容忍度 Δ 逐渐减小,当传输距离增大到特定距离时,Δ 的值趋于 0,这说明密钥传输距离越大,诱骗态 QKD 对态关联性不完美的容忍度越小,这意味着距离越大,对态制备与态测量设备的精度要求越高.考察特殊情形,当 $\Delta\to0$ 且 $\omega_Z=1$ 时,密钥传输的最大距离达到约 142km,这与无态关联性不完美诱骗态 QKD 安全密钥的最大传输距离是一致的.此外,从图 2 中还可以发现,随着 ω_Z 值的减小,Δ 的值会有所的降低,密钥传输的最大距离也会有一定程度的减小,这充分表明探测器的探测性能对 QKD 安全性的影响是不可忽略的,探测器的探测性能越差,对态制备与态测量设备的性能要求就越高.在图 3 中,我们给出了密钥传输距离为 $d=20$km 时,态关联容忍参数 Δ 与探测性能参数 ω_Z 之间关系比较的数值模拟图,从中可以看出,Δ 随着 ω_Z 的增大而递增,这充分表明,伴随着探测器的探测性能越来越好,QKD 的安全性对于态关联性不完美的容忍度逐渐增大.综上所述,诱骗态 QKD 的最终安全密钥生成率对态关联性不完美的容忍程度,随着密钥传输距离的增大而逐渐减小,随着探测器探测性能的提升而逐渐增大,这与人们通常的直观感觉是一致的,因而一定程度上验证了式(11)的正确性.

5　结论

在实际的 QKD 系统中,态关联性不完美对诱骗态 QKD 安全性的影响是不可忽略的,需要将态关联性不完美作为一项重要的实验参数,来考察其对 QKD 最终安全密钥生成率带来的影响.本文给出了态关联不完美条件下诱骗态 QKD 最终安全密钥生成率的表达式,通过数值模拟,刻画了诱骗态 QKD 最终安全密钥生成率对态关联性不完美的敏感程度并验证了所给表达式的正确性.本文的结论可为 QKD 实验的完善提供重要依据.

参考文献

[1] Bennett C H, Brassard G. Quantum cryptography: Publish-key distribution and coin tossing [A]. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing[C]. Bangalore, India. 1984. 175.

[2] 郭奋卓,高飞,温巧燕,朱甫臣.一种高效的量子秘密共享方案[J].电子学报,2006,34(5):883 – 886.
Guo Fenzhuo, Gao Fei, Wen Qiaoyan, Zhu Fuchen. A quantum secret sharing scheme with high efficiency[J]. Acta Electronica Sinica, 2006, 34(5): 883 – 886. (in Chinese)

[3] 曾贵华.不依赖于第三方的动态量子身份认证方案[J].电子学报,2004,32(7):1148 – 1151.
Zeng Guihua. Quantum identity authentication without trusted-party[J]. Acta Electronica Sinica, 2004, 32(7): 1148 – 1151. (in Chinese)

[4] Shor P, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Phys Rev Lett, 2001, 85: 441.

[5] Kraus B, Gisin N, Renner R. Lower and upper bounds on the

secret key rate for QKD protocols using one-way classical communication[J]. Phys Rev Lett, 2005, 95: 080501.
[6] Gottesman, Lo, Lutkenhaus, et al. Security of quantum key distribution with imperfect devices[J]. 2004, 4(5): 325.
[7] Zhou C, Bao W S, Fu X Q. Decoy-state quantum key distribution for the heralded pair coherent state photon source with intensity fluctuations[J]. SCIENCE CHINA Information Sciences, 2010, 53: 2485 – 2494.
[8] Xu F X, Chen W, Wang S, Yin Z Q, et al. Field experiment on a robust hierarchical metropolitan quantum cryptography network[J]. Chinese Science Bulletin, 2009, 54(17): 2991 – 2997.
[9] Wen H, Han Z F, Zhao Y B, et al. Multiple stochastic paths scheme on partially-trusted relay quantum key distribution network[J]. SCIENCE CHINA Information Sciences, 2009, 52(1): 18 – 22.
[10] Li H W, Yin Z Q, Han Z F, et al. Security of quantum key distribution with state-dependent imperfections[DB/OL]. arxiv: quant-ph/1009.1047
[11] Marøy Ø, Lydersen L, Skaar J. Security of quantum key distribution with arbitrary individual imperfection[J]. Phys. Rev. A, 2010, 82: 032337.
[12] Koashi M. Simple security proof of quantum key distribution via uncertainty principle[J]. New J. Phys, 2009, 11: 045018.
[13] Koashi M. Efficient quantum key distribution with practical sources and detectors[DB/OL]. arxiv: quant-ph/0609180.
[14] Hwang W Y. Quantum key distribution with high loss: toward global secure communication[J]. Phys. Rev. Lett, 2003, 91(5): 057901.
[15] Zhang S L, Zou X B, Li C F, et al. A universal coherent source for quantum key distribution[J]. Chinese Science Bulletin, 2009, 54(11): 1863 – 1871.
[16] Lo H K, Ma X F, Chen K. Decoy state quantum key distribution[J]. Phys Rev Lett, 2005, 94(23): 230504.
[17] Wang X B. Beating the PNS attack in practical quantum cryptography[J]. Phys. Rev. Lett. 2005, 94: 230503.
[18] Wang X B. A decoy-state protocol for quantum cryptography with 4 intensities of coherent light[J]. Phys. Rev. A, 2005, 72: 012322.
[19] Nielsen M A and Chuang I L. Quantum Computation and Quantum Information[M]. Cambridge, England: Cambridge University, 2000. p. 410.
[20] Gobby C, Yuan Z L, Shields A J. Quantum key distribution over 122 km of standard telecom[J]. Appl Phys Lett, 2004, 84: 3762 – 3674.

作者简介

周 淳 男, 1986 年生于湖南新宁, 解放军信息工程大学电子技术学院博士生, 研究方向为量子密码. E-mail: winmaxsky@sina.com

鲍皖苏(通讯作者) 男, 1966 年生于安徽天长, 解放军信息工程大学电子技术学院教授, 博士生导师, 主要研究方向序列密码, 公钥密码, 量子密码. E-mail: 2010thzz@sina.com

付向群 男, 1985 年生于江西进贤, 解放军信息工程大学电子技术学院博士生, 研究方向为量子密码. E-mail: fuxiangqun@126.com