一种态制备误差容忍的量子数字签名协议*

马洛嘉[1)2)] 丁华建[1)2)] 陈子骐[1)2)] 张春辉[1)2)] 王琴[1)2)†]

1) (南京邮电大学, 量子信息技术研究所, 南京 210003)

2) (南京邮电大学, 宽带无线通信与传感网教育部重点实验室, 南京 210003)

(2023 年 7 月 24 日收到; 2023 年 10 月 9 日收到修改稿)

量子数字签名 (quantum digital signature, QDS) 能够以信息论安全保证签名消息的不可伪造性、不可否认性和可转移性, 近年来备受关注与研究. 其中, 利用正交编码方式提出的信息论安全的实用化 QDS 协议, 成为目前 QDS 研究的主流范式. 然而, 现有 QDS 理论和实验都忽视了态制备过程中由于调制器件的不完美性可能引入调制误差. 本文针对此问题提出态制备误差容忍的 QDS 协议. 仿真结果表明, 相比原来的 QDS 协议, 本协议对态制备误差具有较好的容忍度, 能实现更高的签名率和签名距离. 另外, 本协议在密钥产生阶段只需要制备 3 个量子态, 降低了实验要求和难度. 因此, 本协议将对未来 QDS 的实际应用提供重要的参考价值.

关键词: 量子数字签名, 态制备误差, 诱骗态

PACS: 03.67.Dd, 42.79.Sz, 03.67.Hk **DOI:** 10.7498/aps.73.20231190

1 引 言

数字签名[1] 能够保证消息的真实性、完整性和不可抵赖性, 被广泛应用于金融交易、电子邮件、文件传输和电子文件的签名等方面, 是保证当前互联网安全的重要基石. 绝大多数经典数字签名协议的安全性都依赖于大数质因子分解的计算复杂度, 例如非对称加密算法, 数据签名算法以及椭圆曲线数字签名算法. 然而, 随着量子计算机的发展, 这些协议的安全性受到威胁. 因此, 在量子计算时代发展更高安全性的数字签名协议至关重要.

相比经典的数字签名, 基于量子力学基本原理的量子数字签名 (quantum digital signature, QDS) 拥有更高级别的安全性. 第一个 QDS 协议由 Gottesman 和 Chuang[2] 于 2001 年提出, 简称 GC-01 协议. 尽管该协议要求非破坏性的量子态比较、长时间的量子存储和安全的量子信道, 在当前技术条件下难以实现, 但该协议具有重要启发意义. 此后, 实验友好型的协议相继被提出并得到验证. 其中, Clarke 等[3] 利用相干态编码和光学多端干涉仪完成了第 1 个 QDS 实验; Collins 等[4] 进一步降低了使用长寿命量子存储器的技术要求; Amiri 等[5] 基于现有的量子密钥分发设备首次提出了无需安全量子信道的实用化 QDS 方案, 并给出了诱骗态 QDS 的一般模型. 此后, 研究人员相继实现了测量设备无关的 QDS[6]、GHz 时钟频率的高速 QDS[7]、被动式诱骗态的 QDS[8], 远距离传输的 QDS[9] 和基于一次哈希的高效 QDS[10].

QDS 是一个涉及多用户的加密体制, 其包括密钥分发阶段和消息认证阶段[11,12]. 三用户场景中, 假设 Alice 为签名消息发送方, Bob 和 Charlie 为消息的接收方. 在分发阶段, Alice 和 Bob、Alice 和 Charlie 通过密钥产生协议 (key generation

* 国家自然科学基金 (批准号: 12074194, 11774180) 、江苏省自然科学基金前沿技术项目 (批准号: BK20192001) 和江苏省重点研发计划产业前瞻与关键核心技术项目 (批准号: BE2022071) 资助的课题.

† 通信作者. E-mail: qinw@njupt.edu.cn

protocol, KGP)、密钥交换操作等步骤构建对称密钥; 在消息阶段, Alice 签名消息并发送给 Bob, Bob 验证接收到的签名消息, 并转发给 Charlie 进行验证. KGP 过程其实是量子密钥分发的量子部分, 即产生筛后密钥即可, 无需再进行纠错和保密放大等后处理过程. 但是, 关于安全性分析仍需要计算最小熵来估计窃听者 Eve 获取的信息量, 以保证后续签名申明的不匹配数小于预设值, 为此需要考虑 Alice 和 Bob (Alice 和 Charlie) 的相位误码率. 例如, 在没有光源缺陷的情况下, 即 Bob 或 Charlie 的光源满足基矢无关性, 可以根据随机抽样理论利用 X 基矢的比特误码率来估计 Z 基矢的相位误码率, 反之亦然. 但是, 实际系统中由于带宽不足、校准错误以及环境的影响等问题, 制备的量子态都存在误差 [13–15], 尽管这一误差很小但可以被窃听者以某种方式增强. 这一态制备误差问题可以通过量子硬币的思想来解决 [16], 但是该方法考虑最坏的情况, 即窃听者可以通过信道损耗来增强缺陷, 协议的最终性能大幅度下降.

在量子密钥分发 (quantum key distribution, QKD) 应用中, Tamaki 等 [17] 曾提出过一种损耗容忍 (loss tolerant, LT) 量子密钥分发 (quantum key distribution, QKD) 协议, 降低了态制备误差对 QKD 系统性能的影响. 本文将以上损耗容忍思想引入 QDS 协议模型之中, 提出了一种态制备误差容忍的 QDS 协议, 并构建相应的模型, 对改进协议的签名率和安全性能进行仿真. 仿真结果显示, 当态制备误差增大时, 本文提出的方法的签名率曲线变化并不明显, 对态制备误差有较高的容忍度, 相较于此前该方向研究者常常使用的 GLLP (Gottesman-Lo-Lütkenhaus-Preskill, GLLP) 方法的结果, 有显著的性能提升; 另外本方案只需要制备 3 个量子态, 降低了实验的难度.

2 理论模型分析与计算方法

假设每轮协议中用于密钥传输的总脉冲数为 $N_{\rm tot}$, 然后从得到的原始密钥串中选择 L 长度的密钥用于签名半比特消息. 协议具体流程如下.

分发阶段 Bob(Charlie) 制备 $N_{\rm tot}$ 个光脉冲, 每个脉冲等概地调制为 $\{|0\rangle, |1\rangle, |+\rangle\}$ 中的一个, 并发送给 Alice. 其中 $|0\rangle$ 和 $|+\rangle$ 对应经典比特 0, $|1\rangle$ 对应经典比特 1, 并且 $|0\rangle$ 和 $|1\rangle$ 对应 Z 基, $|+\rangle$ 对应 X 基. Alice 也等概率地选择 X 基或 Z 基对收到的脉冲测量. 当他们都选择 Z 基时, 相应的比特用作签名密钥串, 但 Alice 选择 X 基时, 相应的比特用作参数估计. 接着他们从 $N_{\rm tot}$ 个光脉冲中选取占比为 d 的一部分密钥串 $n_{\rm test}$ 估算误码率 $e_{\rm AB}$ ($e_{\rm AC}$), 剩下的作为签名的密钥池并记作 $n_{\rm pool}$. 对未来可能的消息 $m=0$ 或 $m=1$ 签名, Alice 和 Bob (Charlie) 从 $n_{\rm pool}$ 中选择长度为 L 的密钥串来构造签名序列 $K_m^{\rm B}$ 和 $B_m^{\rm A}$ ($K_m^{\rm C}$ 和 $C_m^{\rm A}$), 其中 $K_m^{\rm B}$ 和 $K_m^{\rm C}$ 由 Alice 持有, $B_m^{\rm A}$ ($C_m^{\rm A}$) 由 Bob (Charlie) 持有. 最后, Bob (Charlie) 随机选择一半的密钥, 通过一个经典认证信道将它们及其相对应的位置转发给 Charlie (Bob), 我们将保留的那一半密钥称为 $B_{m,\rm keep}^{\rm A}$ ($C_{m,\rm keep}^{\rm A}$), 另一半称为 $B_{m,\rm forward}^{\rm A}$ ($C_{m,\rm forward}^{\rm A}$). 此时 Bob 和 Charlie 持有的对称密钥为 $S_m^{\rm B}=(B_{m,\rm keep}^{\rm A}, C_{m,\rm forward}^{\rm A})$ 和 $S_m^{\rm C}=(C_{m,\rm keep}^{\rm A}, B_{m,\rm forward}^{\rm A})$.

根据测试密钥串 $n_{\rm test}$ 的误码率 $e_{\rm AB}$, Alice 和 Bob 可以使用 Serfling 不等式 [18] 估计误码率上界 $e_{\rm AB}^{\rm U}$:

$$e_{\rm AB}^{\rm U}=e_{\rm AB}+\frac{2}{L}\sqrt{\frac{\ln(1/\varepsilon_{\rm PE})}{2n_{\rm test}}(L/2+1)(L/2+n_{\rm test})}, \tag{1}$$

其中 $\varepsilon_{\rm PE}$ 为 (1) 式的失败概率. 类似地, Alice 和 Charlie 估计误码率 $e_{\rm AC}$ 上界 $e_{\rm AC}^{\rm U}$, 并且定义 $e^{\rm U}=\max(e_{\rm AB}^{\rm U}, e_{\rm AC}^{\rm U})$. 接着考虑由窃听者 Eve 窃听时引入的最小误码率 $e_{\rm min}$, 其满足

$$H_2(e_{\rm min})=2S_{Z,1}^{\rm L}\left[1-H_2(\varphi_{Z,1}^{\rm U})\right]/N_Z, \tag{2}$$

其中 $H_2(x)=-x\log_2 x-(1-x)\log_2(1-x)$ 表示 2 进制香农熵函数, $s_{Z,1}^{\rm L}$ 为 Z 基下单光子脉冲响应计数的下界, $\phi_{z,1}^{\rm U}$ 表示 Z 基下单光子脉冲的相位误码率的上界, N_Z 表示双方都选择 Z 基时的响应计数.

消息阶段 Alice 发送签名 $(m, {\rm Sig}_m)$ 给 Bob, 其中 ${\rm Sig}_m=(K_m^{\rm B}, K_m^{\rm C})$. Bob 将他手上的验证密钥 $S_m^{\rm B}$ 和接收到的签名 ${\rm Sig}_m$ 进行比较, 并且记录不匹配的数量. 如果 $S_m^{\rm B}$ 两部分的不匹配数目都小于 $s_\alpha L/2$, 那么 Bob 接收该签名消息并转发给 Charlie; 否则, Bob 拒绝消息并宣布中止协议. 其中 s_α 表示和 QDS 安全所需要的身份验证的阈值, 并且 $0<s_\alpha<0.5$. Charlie 以相同方法检查 Bob 转发而来的签名消息, 与先前不同的是这次的阈值为 s_v, 并且 $0<s_\alpha<s_v<0.5$, 如果不匹配数目仍然小于 $s_vL/2$, 那么 Charlie 就接收消息.

考虑 QDS 协议的三大安全性分析: 鲁棒性 P (robust) 、不可抵赖性 P (repudiation) 和不可伪造性 P (forge) [5], 为了保证协议的安全性, 系统的安全参数 $P_{\rm sec}$ 需满足:

$$P_{\rm sec} \geqslant \max\left\{\mathrm{P(Robust)}, \mathrm{P(Re(pudiation)}, \mathrm{P(Forge)}\right\}. \tag{3}$$

以往的 QDS 分发阶段的研究里, 在 KGP 过程中通常会假设态制备的完美性, 此时 Z 基的相位误码率可以由 X 基的比特误码率所表征, 然而当存在态制备误差时, Z 基的相位误码率会受到信道损耗的影响, 之前的方法便不再适用. 由于实际系统在制备量子态时不可避免地存在态制备误差, 如果忽略这些误差, 那么系统的安全性会大打折扣, 如果考虑这些制备误差, 前期研究结果的性能又会大幅度降低. 针对该问题, 我们提出了态制备误差容忍的 QDS 协议, 将态制备误差刻画进协议中. 使得理论分析不仅贴近于实际实现, 而且提高协议对态制备误差的容忍度. 根据损耗容忍分析方法 [17,19], 在态制备阶段只需要制备 3 个量子态, 可以分别记作:

$$\begin{aligned}
&|\phi_{0Z}\rangle = |0_Z\rangle,\\
&|\phi_{1Z}\rangle = -\sin\frac{\delta_1}{2}|0_Z\rangle + \cos\frac{\delta_1}{2}|1_Z\rangle,\\
&|\phi_{0X}\rangle = \cos\left(\frac{\pi}{4}+\frac{\delta_2}{4}\right)|0_Z\rangle + \sin\left(\frac{\pi}{4}+\frac{\delta_2}{4}\right)|1_Z\rangle,
\end{aligned}$$

其中 δ_1 ($\delta_1 \geqslant 0$) 为衰减器或者强度调制器引发的态制备误差, δ_2 ($\delta_2 \geqslant 0$) 为分束器的误差造成的. 需要说明的是, 这里假定 $|\phi_{0Z}\rangle$ 的态制备误差为 0, 主要由于实验中可以将 $|\phi_{0Z}\rangle$ 当作参考量子态, 然后使用相对误差 (δ_1 和 δ_2) 来刻画制备 $|\phi_{1Z}\rangle$ 和 $|\phi_{0X}\rangle$ 所产生的误差大小.

为方便后面计算公式表示, 进行如下定义: $\beta = \eta C_{s\alpha|j\gamma}$, $D = 1 - P_{\rm d}$, 其中 $\eta = \eta_{\rm d}10^{-\alpha L/10}$ 表示光子从发送端到接收端的整体效率 (不包含投影测量效率); $\eta_{\rm d}$ 指接收端探测器的探测效率; α 代表信道损耗系数; L 是传输的距离; $C_{s\alpha|j\gamma}$ 代表接收端选择 α 作为测量基对 $|\phi_{j\gamma}\rangle$ 态进行测量并获得比特值 s 的概率; $P_{\rm d}$ 代表探测器的暗计数率, 强度为 $\lambda \in (\mu, v, w)$ 时对应的光子态增益可以分别表示为

$$\begin{aligned}
Q_{\lambda,s\alpha,j\gamma} &= \sum_{n=0}^{\infty} Y_n \frac{\lambda^n}{n!}\mathrm{e}^{-\lambda}\\
&= \frac{1}{2}\left\{1 + D\left[\mathrm{e}^{(-\eta+\beta)\lambda} - \mathrm{e}^{-\beta\lambda} - D\mathrm{e}^{-\eta\lambda}\right]\right\},
\end{aligned} \tag{4}$$

其中 Y_n 代表发射端发送包含 n 光子态的光脉冲在接收端产生响应的条件概率. 使用三强度诱骗态方法 [19], 可以得到单光子条件计数率的下界:

$$\begin{aligned}
Y^L_{s\alpha,j\gamma} &= \frac{\mu}{\mu\nu - v^2}\\
&\times\left(Q_{v,s\alpha,j\gamma}\mathrm{e}^{v} - Q_{\mu,s\alpha,j\gamma}\mathrm{e}^{\mu}\frac{v^2}{\mu^2} - \frac{\mu^2 - v^2}{\mu^2}Y_0\right),
\end{aligned} \tag{5}$$

其中 $Y_0 = P_{\rm d}(1 - P_{\rm d}/2)$, 表示真空态条件响应率; $N_{Z,\lambda}$ 表示双方都选择 Z 基时不同强度脉冲响应的计数个数; 考虑到统计起伏的影响, 将 $N^*_{Z,\lambda}$ 表示为考虑统计起伏响应的计数. 使用独立随机变量的 Hoeffding 不等式 [20] 给出 $N^*_{Z,\lambda}$ 的上下界: $N^{\rm U}_{Z,\lambda} = N_{Z,\lambda} + \delta(N_Z, \varepsilon_{\rm PE})$ 和 $N^{\rm L}_{Z,\lambda} = N_{Z,\lambda} - \delta(N_Z, \varepsilon_{\rm PE})$, 其中 $\delta(m,n) = \sqrt{m\ln(1/n)/2}$. 求解单光子响应计数的下界 $s^{\rm L}_{Z,1}$, 先求解零光子脉冲响应计数下界 $s^{\rm L}_{Z,0}$:

$$s^L_{Z,0} \geq \frac{\tau_0}{v - w}\left(\frac{v\mathrm{e}^{w}N^L_{Z,w}}{P_w} - \frac{w\mathrm{e}^{v}N^U_{Z,v}}{P_v}\right), \tag{6}$$

其中 P_λ 表示选择 λ 强度光子发射的概率. 对于单光子脉冲响应计数的下界 $s^{\rm L}_{Z,1}$:

$$\begin{aligned}
s^L_{Z,1} \geq \frac{\mu\tau_1}{\mu v - \mu w - v^2 + w^2}&\left[\frac{\mathrm{e}^{v}N^L_{Z,v}}{P_v} - \frac{\mathrm{e}^{w}N^U_{Z,w}}{P_w}\right.\\
&\left.+ \frac{v^2 - w^2}{\mu^2}\left(\frac{s^L_{Z,0}}{\tau_0} - \frac{\mathrm{e}^{\mu}N^U_{Z,\mu}}{P_\mu}\right)\right].
\end{aligned} \tag{7}$$

为计算相位误码率 $\varphi^{\rm U}_{Z,1}$, 将其表征为 X 基的虚拟比特误码率 e_X. 下面考虑一个与真实协议安全性等价的虚拟协议, 计划由虚拟协议推导出相位误码率 $\varphi^{\rm U}_{Z,1}$ 的表达式. 在该虚拟协议中, 发送端制备 $|\psi_Z\rangle_{\rm A_eAB}$ 后进行虚拟态的传输, 其中 A 代表发送端需要选基测量的粒子, B 代表需要发送给接收端的粒子, $\rm A_e$ 代表辅助粒子; 接下来, 发送端选择 X 基去测量粒子 A, 接收端同样选择 X 基去测量粒子 B, 此时发送端发射的虚拟量子态位于 X-Z 平面, 可以表示为

$$\hat{\sigma}_{\mathrm{B};j_X,\mathrm{vir}} = \mathrm{Tr}_{\mathrm{A,A_e}}\left[\hat{P}\left(|j_X\rangle_{\rm A}\right)\otimes\hat{1}_{\rm A_eB}\hat{P}\left(|\Psi_Z\rangle_{\rm AA_eB}\right)\right], \tag{8}$$

其中 $\mathrm{Tr}_{\rm A,\,A_e}$ 表示对系统 A 和 $\rm A_e$ 求偏迹的过程.

虚拟协议在 X 基的比特误码率 e_X 可以写成下面形式:

$$e_X = \frac{Y^{(Z),\mathrm{vir}}_{1_X,0_X} + Y^{(Z),\mathrm{vir}}_{0_X,1_X}}{Y^{(Z),\mathrm{vir}}_{0_X,0_X} + Y^{(Z),\mathrm{vir}}_{1_X,0_X} + Y^{(Z),\mathrm{vir}}_{0_X,1_X} + Y^{(Z),\mathrm{vir}}_{1_X,1_X}}, \tag{9}$$

其中虚拟协议下的传输速率 $Y^{(Z),\mathrm{vir}}_{s_X,j_X}$ 可以由发送端和接收端分别测得比特值 j 和 s 的联合概率表示:

$Y_{s_X,j_X}^{(Z),\mathrm{vir}}=\mathrm{Tr}[\hat{\sigma}_{B;j_X,\mathrm{vir}}]\,\mathrm{Tr}\left(\hat{D}_{s_X}\hat{\sigma}'_{B;j_X,\mathrm{vir}}\right)/2$. $\mathrm{Tr}[\hat{\sigma}_{B;j_X,\mathrm{vir}}]$ 是发送虚拟态 $\hat{\sigma}_{B;j_X,\mathrm{vir}}$ 的概率, $\hat{D}_{s_X}$ 表示考虑了窃听方 Eve 操作的测量算符, $\hat{\sigma}'_{B;j_X,\mathrm{vir}}$ 是虚拟态 $\hat{\sigma}_{B;j_X,\mathrm{vir}}$ 的归一化形式. 归一化形式下, 虚拟态 $\hat{\sigma}'_{B;j_X,\mathrm{vir}}$ 又可以写成一组单位矩阵和泡利矩阵的线性组合:

$$\hat{\sigma}'_{B;j_X,\mathrm{vir}}=\frac{1}{2}\left(\hat{1}+\sum_{t=X,Y,Z}P_t^{j_X,(\mathrm{vir})}\hat{\sigma}_t\right), \tag{10}$$

其中 $P_t^{j_X,(\mathrm{vir})}$ 为泡利矩阵 $\hat{\sigma}_t$ 对应的 Bloch 系数, 同时泡利矩阵 $\hat{\sigma}_t$ 对应的信道传输速率和对应基成功测量概率关系为: $q_{s_X|t}=\mathrm{Tr}\left(\hat{D}_{s_X}\hat{\sigma}_t\right)/2$. 如果求得泡利矩阵的传输速率, 那么就可以求解虚拟态的传输速率:

$$\begin{aligned}Y_{s_X,j_X}^{(Z),\mathrm{vir}}=&\,\mathrm{Tr}\left[\hat{\sigma}_{B;j_X,\mathrm{vir}}\right]\left(q_{s_X|\mathrm{Id}}+P_X^{j_X,(\mathrm{vir})}q_{s_X|X}\right.\\&\left.+P_Z^{j_X,(\mathrm{vir})}q_{s_X|Z}\right).\end{aligned} \tag{11}$$

为了计算 $q_{s_X|\mathrm{Id}}$, $q_{s_X|X}$ 和 $q_{s_X|Z}$, 考虑到真实的量子态也位于 X-Z 平面, 由实验数据可得实际传输速率为

$$Y_{s_X,j_\alpha}^{(Z)}=P\left(j_\alpha\right)\left(q_{s_X|\mathrm{Id}}+P_X^{j\alpha}q_{s_X|X}+P_Z^{j\alpha}q_{s_X|Z}\right)/2, \tag{12}$$

其中 $P\left(j_\alpha\right)$ 是发送方发送量子态 $\hat{\rho}_{j\alpha}$ 的概率, $1/2$ 表示接收方的选基概率, $q_{s_X|t}$ 表示 $\hat{\sigma}_t$ 的传输速率. 实际传输速率的表达式:

$$\begin{aligned}&\left(q_{s_X|\mathrm{Id}},q_{s_X|X},q_{s_X|Z}\right)\\&=6\left(Y_{s_X,0_Z}^{(Z)},Y_{s_X,1_Z}^{(Z)},Y_{s_X,0_X}^{(X)}\right)\hat{A}^{-1},\end{aligned} \tag{13}$$

其中 $\hat{A}=\left(\boldsymbol{V}_{0Z}^{\mathrm{T}},\boldsymbol{V}_{1Z}^{\mathrm{T}},\boldsymbol{V}_{0X}^{\mathrm{T}}\right)$, $\boldsymbol{V}_{j\alpha}=\left(1,P_X^{j\alpha},P_Z^{j\alpha}\right)$, T 表示转置.

为了保证 QDS 协议的安全性, 需要确保 Eve 在窃听时引入的最小误码率 $e_{\min}$ 小于通信双方由于正常通信引起的误码率 e^{U} . 为了量化 $e_{\min}$, 首先计算 Z 基下单光子脉冲响应计数下界 $s_{Z,1}^{\mathrm{L}}$; 接着结合损耗容忍分析方法, 由真实态的传输速率求得虚拟态的传输速率, 进而获得相位误码率 $\varphi_{Z,1}^{\mathrm{U}}$ 的大小, 由此得出 $e_{\min}$. 最后考虑 QDS 的三大安全性分析, 构造出与密钥串相关的方程, 最终得到签名率大小.

3 数值分析及仿真结果讨论

本节主要介绍态制备误差容忍 QDS 协议的仿真思路和结果. 根据前面的分析, 在求出 e^{U} 和 $e_{\min}$ 后, 由 (3) 式构造出发射端发射的脉冲数和安全性系数的关系式, 以此求出签名率. 定义签名率 $R=1/L$. 在 QDS 协议中, 保证协议安全性为 $P_{\mathrm{sec}}=10^{-4}$ 的前提下, 协议的安全性主要与抵赖概率相关. 通过构造 L 与 P_{sec} 的关系式, 得到一个临界值所对应的脉冲数 L 就是签名消息 m 所需的最短密钥串.

考虑到对于态制备误差容忍的 QDS 协议, 系统变量的不同取值对签名率的影响比较大, 在仿真过程中利用全局优化算法对几个参数做了优化, 其中包括信号态强度 μ 、诱骗态强度 v 、选择信号态发射的概率 P_μ 和选择诱骗态发射的概率 P_v . 为了简单起见, 仿真中假定态制备误差 $\delta_1=\delta_2=\delta$, 见表 1.

图 1 中的虚线表示态制备误差 $\delta=0$, 0.2, 0.3 时, 态制备误差容忍分析方法下的签名率曲线随传输距离变化的结果, 实线则是使用 GLLP 分析方法时对应的结果. 当误差 $\delta=0.2$, 0.3 时, 态制备误差容忍分析方法下的签名率随传输距离变化曲线, 与不存在误差即 $\delta=0$ 时非常接近, 最终的传输距离都在 180 km 左右. 在使用 GLLP 分析方法的对应结果中, 虽然当 $\delta=0$ 时, 签名率曲线最好并且安全传输距离也能达到 181 km, 但是当 $\delta=0.3$ 时, 安全传输距离直接下降到了 40 km, 可见该方法的签名率对态制备误差极为敏感, 相比之下, 本文方法对态制备误差具有更好的鲁棒性.

图 2 展示了态制备误差不同时, 态制备误差容忍方法和 GLLP 分析方法的错误率对比结果, 其中实线代表 $e_{\min}$, 虚线代表 e^{U}, 当 $e_{\min}>e^{\mathrm{U}}$ 时保证协议是安全的. 态制备误差容忍的 QDS 协议中, $e_{\min}$ 和 e^{U} 受态制备误差影响较小. 然而在 GLLP 分析方法的 QDS 协议之中, 协议的安全性参数对

表 1 基于量子数字签名的态制备误差容忍协议仿真使用的参数列表[21]

Table 1. The parameter list used for simulation of state preparation error tolerance protocol based on quantum digital signature protocol[21].

接收方探测器暗计数率 P_{d}	接收方探测器探测效率 η_{d}	信道损耗系数 $\alpha/(\mathrm{dB}\cdot\mathrm{km}^{-1})$	KGP过程中估参长度比例 d	发射的总脉冲数 N_{tot}	失败概率 $\varepsilon_{\mathrm{PE}}$	最弱诱骗态强度 w
1.5×10^{-6}	0.145	0.2	1/21	10^{14}	10^{-5}	0.002

态制备误差较为敏感, 特别是当 $\delta = 0.3$ 时, $e_{\min}$ 和 e^{U} 下降较快. 可以看出在态制备误差容忍的 QDS 协议中, 态制备误差对协议安全性能的影响较小, 最终的安全传输距离变化不大.

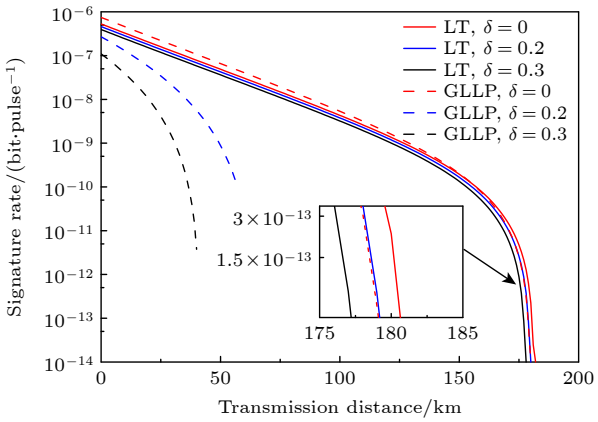

图 1 态制备误差容忍方法和 GLLP 分析方法签名率大小对比结果

Fig. 1. Comparison on the signature rate between the state-preparation-error tolerance scheme and GLLP method.

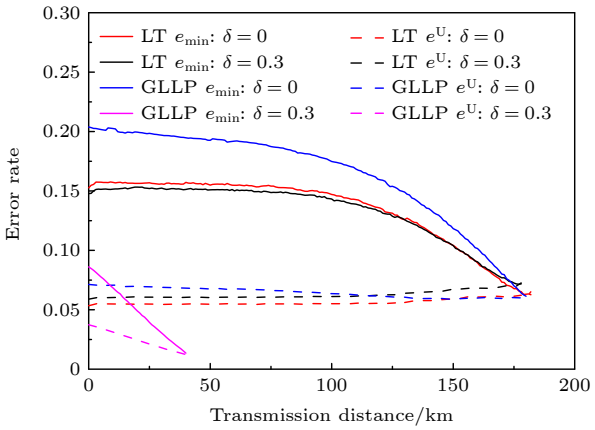

图 2 态制备误差容忍方法和 GLLP 分析方法的错误率对比结果

Fig. 2. Comparison on the error rate between the state-preparation-error tolerance scheme and GLLP method.

图 3 展示了态制备误差容忍方法和 GLLP 分析方法下, 传输距离固定为 20 km 时, 用于密钥传输的总脉冲数 N_{tot} 不同时, 签名率曲线随着态制备误差变化的曲线. 从图 3 可以看到, 使用态制备误差容忍协议的签名率曲线随着态制备误差增大而缓慢下降, 与之相反, 使用 GLLP 分析方法的签名率曲线随着态制备误差增大而快速下降, 显示了本方法对态制备误差的良好的鲁棒性. 此外, 在不同的总脉冲数下, 该趋势基本没有变化, 显示了本方法对有限长效应也具有良好的鲁棒性.

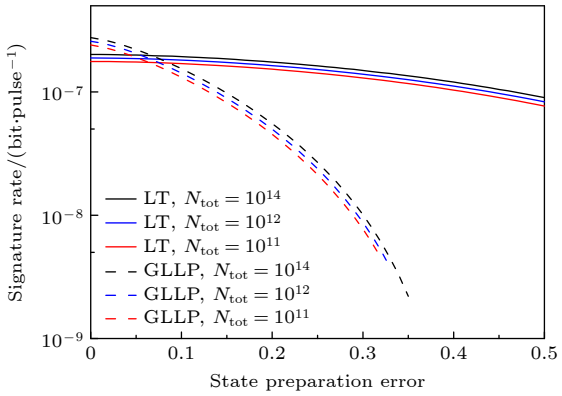

图 3 传输距离为 20 km 时, 不同总脉冲数下, 态制备误差容忍方法和 GLLP 分析方法签名率随着态制备误差变化对比

Fig. 3. The signature rate *vs.* state preparation error for the state-preparation-error tolerance scheme and GLLP method under different total number of pulses. Here the transmission distance is fixed at 20 km.

4 结 论

本文将损耗容忍分析方法结合到 QDS 协议中, 以三强度诱骗态为例, 提出了态制备误差容忍的 QDS 协议, 并进行签名率的仿真. 移除了原来完美态制备的假设之后, 使得理论分析更加贴近于实际实现. 当误差取值不同时, 本文提出的方法下的签名率随态制备误差变化较小, 最终传输距离能够稳定在 180 km 左右, 并且安全性能曲线变化较小. 而基于 GLLP 分析方法的 QDS 协议, 签名率随态制备误差变化较大, 在态制备误差较大时性能较差. 因此从协议的整体性能来看, 本文提出的方法对态制备误差有良好的鲁棒性, 提高了协议性能. 并且由于本方法只涉及 3 个量子态的制备, 因此也降低了实验的难度. 工作的分析方法也可以与测量设备无关协议的 QDS 协议 [6] 和双场的 QDS 协议 [22] 相结合, 进一步增加协议的安全性能. 因此本工作将会对 QDS 的实现应用和安全性提高起到促进作用.

参考文献

[1] Diffie W, Helman M E 1976 *IEEE Trans. Inf. Theory* **22** 644
[2] Gottesman D, Chuang I 2001 arXiv: quant-ph/0105032v2
[3] Clarke P J, Collins R J, Dunjko V, Andersson E, Jeffers J, Buller G S 2012 *Nat. Commun.* **3** 1174
[4] Collins R J, Donaldson R J, Dunjko V, Wallden P, Clarke P J, Andersson E, Jeffers J, Buller G S 2014 *Phys. Rev. Lett.* **113** 040502
[5] Amiri R, Wallden P, Kent A, Andersson E 2016 *Phys. Rev. A*

93 032325
[6] Puthoor I V, Amiri R, Wallden P, Curty M, Andersson Erika 2016 *Phys. Rev. A* **94** 022328
[7] An X B, Zhang H, Zhang C M, Chen W, Wang S, Yin Z Q, Wang Q, He D Y, Hao P L, Liu S F, Zhou X Y, Guo G C, Han Z F 2019 *Opt. Lett.* **44** 139
[8] Zhang C H, Zhou X Y, Ding H J, Zhang C M, Guo G C, Wang Q 2018 *Phys. Rev. Appl.* **10** 034033
[9] Ding H J, Chen J J, Li J, Zhou X Y, Zhang C H, Zhang C M, Wang Q 2020 *Opt. Lett.* **45** 1711
[10] 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 *Natl. Sci. Rev.* **10** 1093
[11] Lo H K, Ma X F, Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[12] Zeng G, Keitel C H 2002 *Phys. Rev. A* **65** 042312
[13] Tamaki K, Lo H K, Fung C H F, Qi B 2011 *Phys. Rev. A* **85** 042307
[14] Koashi M 2009 *New J. Phys.* **11** 045018
[15] Lo H K, Preskill J 2007 *Quant. Inf. Comput.* **8** 431
[16] Gottesman D, Lo H K, Lütkenhaus N, Preskill J 2004 *Quant. Inf. Comput.* **4** 325
[17] Tamaki K, Curty M, Kato G, Lo H K, Azuma K 2014 *Phys. Rev. A* **90** 052314
[18] Serfling R J 1974 *Ann. Statist.* **2** 39
[19] Ma X, Sun M S, Liu J Y, Ding H J, Wang Q 2022 *Acta Phys. Sin.* **71** 030301 (in Chinese) [马啸, 孙铭烁, 刘靖阳, 丁华建, 王琴 2022 物理学报 **71** 030301]
[20] Hoeffding W 1994 *Probability Inequalities for Sums of Bounded Random Variables* (New York: Springer) pp409–426
[21] Gobby C, Yuan Z L, Shields A J 2004 *Appl. Phys. Lett.* **84** 3672
[22] Zhang C H, Zhou X Y, Zhang C M, Li J, Wang Q 2021 *Opt. Lett.* **46** 3757

A quantum digital signature protocol with state preparation error tolerance*

Ma Luo-Jia [1)2)] Ding Hua-Jian [1)2)] Chen Zi-Qi [1)2)]
Zhang Chun-Hui [1)2)] Wang Qin [1)2)†]

1) (*Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)
2) (*Key Laboratory of Broadband Wireless Communication and Sensor Network of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)

(Received 24 July 2023; revised manuscript received 9 October 2023)

Abstract

The quantum digital signature (QDS) has attracted much attention as it ensures the nonrepudiation, unforgeability, and transferability of signature messages based on information-theoretic security. Amiri et al. (*Phys. Rev. A* **93** 032325) proposed the first practical QDS protocol based on orthogonal coding, which has realized information-theoretic security and become the mainstream paradigm in QDS research. The procedure of QDS involves two essential stages, the one is the distribution stage, in which Alice-Bob and Alice-Charlie individually utilize the three-intensity decoy-state quantum key distribution protocol but without error correction or privacy amplification, namely, key-generation protocol, to generate correlated bit strings, the other is the messaging stage, in which Alice transmits signature messages to the two recipients.

However, previous theoretical and experimental studies both overlooked the modulation errors that may be introduced in the state preparation process due to the imperfections in modulator devices. Under the traditional framework of GLLP analysis method, these errors will significantly reduce the actual signature rates. Therefore, we propose a state-preparation-error tolerant QDS and use parameter analysis to characterize the state preparation error to make the simulation analysis more realistic. In addition, we analyze the signature rates of the present scheme by using the three-intensity decoy-state method.

Compared with previous QDS protocols, our protocol almost shows no performance degradation under practical state preparation errors and exhibits a maximum transmission distance around 180 km. Furthermore, state preparation errors do not have a significant influence on the bit error rate induced by normal communication between the legitimate users or the one produced by an eavesdropper. These results prove that the method proposed in this paper has excellent robustness against state preparation errors and it can achieve much higher signature rates and signature distances than other standard methods. Besides, signature rates are basically unchanged under different total pulse numbers, which shows that our protocol also has good robustness against the finite-size effect. Additionally, in the key generation process, our method is only required to prepare three quantum states, which will reduce the difficulty of experiment realizations.

Furthermore, the proposed method can also be combined with the measurement-device-independent QDS protocol and the twin-field QDS protocol to further increase the security level of QDS protocol. Therefore, our work will provide an important reference value for realizing the practical application of QDS in the future.

Keywords: quantum digital signature, state preparation errors, decoy state

PACS: 03.67.Dd, 42.79.Sz, 03.67.Hk **DOI:** 10.7498/aps.73.20231190

* Project supported by the National Natural Science Foundation of China (Grant Nos. 12074194, 11774180), the Leading-edge Technology Program of Natural Science Foundation, China (Grant No. BK20192001), and the Industrial Prospect and Key Core Technology Projects of Jiangsu Provincial key R & D Program, China(Grant No. BE2022071).

† Corresponding author. E-mail: qinw@njupt.edu.cn

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

一种态制备误差容忍的量子数字签名协议

马洛嘉 丁华建 陈子骐 张春辉 王琴

A quantum digital signature protocol with state preparation error tolerance

Ma Luo-Jia Ding Hua-Jian Chen Zi-Qi Zhang Chun-Hui Wang Qin

引用信息 Citation: Acta Physica Sinica, 73, 020301 (2024) DOI: 10.7498/aps.73.20231190
在线阅读 View online: https://doi.org/10.7498/aps.73.20231190
当期内容 View table of contents: http://wulixb.iphy.ac.cn
