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

基于混合编码的测量设备无关量子密钥分发的简单协议

杜聪 王金东 秦晓娟 魏正军 於亚飞 张智明

A simple protocol for measuring device independent quantum key distribution based on hybrid encoding

Du Cong Wang Jin-Dong Qin Xiao-Juan Wei Zheng-Jun Yu Ya-Fei Zhang Zhi-Ming

引用信息 Citation: Acta Physica Sinica, 69, 190301 (2020) DOI: 10.7498/aps.69.20200162
在线阅读 View online: https://doi.org/10.7498/aps.69.20200162
当期内容 View table of contents: http://wulixb.iphy.ac.cn

基于混合编码的测量设备无关量子密钥分发的简单协议*

杜聪[1)] 王金东[1)†] 秦晓娟[2)] 魏正军[1)] 於亚飞[1)] 张智明[1)]

1) (华南师范大学, 广东省量子调控工程与材料重点实验室, 信息光电子科技学院, 广州 510006)

2) (广东理工职业学院工程技术系, 广州 510091)

(2020 年 1 月 29 日收到; 2020 年 7 月 2 日收到修改稿)

测量设备无关量子密钥分发协议移除了所有测量设备的漏洞, 极大地提高了量子密钥分发系统的实际安全性, 然而, 该协议的安全密钥率相比于其他量子密钥分发协议来说仍然是较低的. 目前, 利用高维编码来提升量子密钥分发协议的性能已经在理论和实验上都得到证明, 最近有人提出了基于高维编码的测量设备无关量子密钥分发协议, 但是由于所提出的协议对实验设备性能有更高的要求, 所以在实际应用上仍然存在许多困难. 本文提出一种基于偏振和相位两种自由度的混合编码测量设备无关量子密钥分发协议, 并且利用四强度诱骗态方法分析该协议在实际条件下的安全性, 最后数值仿真结果表明, 该协议在实际条件下 40 km 和 50 km 处的最优安全码率相比于原 MDI-QKD 协议分别提升了 52.83% 和 50.55%. 而且, 相比于其他基于高维编码的测量设备无关量子密钥分发协议来说, 本文提出的协议只要求本地用户拥有相位编码装置和偏振编码装置, 探测端也只需要四台单光子探测器, 这些装置都可以利用现有的实验条件实现, 说明该协议的实用价值也很高.

关键词: 量子密钥分发, 测量设备无关, 高维编码, 混合编码

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.69.20200162

1 引 言

量子密钥分发 (quantum key distribution, QKD) 是指一种通过在公开信道中传输量子态来使通信双方之间分享密钥的方法, 它的安全性是由量子力学的基本原理, 而不是计算复杂度来保证的, 所以从理论上保证了密钥传输的绝对安全. 自 1984 年 Bennett 和 Brassard 提出了第一个 QKD 协议——BB84 协议 [1] 以来, QKD 在理论和实验上都得到了快速的发展 [2,3]. 尽管无条件安全性是 QKD 的主要优势, 但在实际应用中, 由于设备的不完美性可能带来的安全隐患使它的应用前景饱受争议. 人们普遍认为缺乏完美的单光子源和探测器的固有损耗会使系统产生安全漏洞并限制传输距离, 进而降低 QKD 的应用性能 [2]. 但幸运的是, Lo, Curty 和 Qi 在 2012 年提出测量设备无关量子密钥分发 (measurement device independent quantum key distribution, MDI-QKD) 协议 [4,5], 它不仅可抵御所有针对测量端的攻击漏洞, 而且当它与诱骗态方法结合 [6,7] 时, 还可以显著提升系统的传输距离. 由于这些优点, 到目前为止, MDI-QKD 已经吸引了领域内大量的关注, 并且出现了大量的理论 [8–16] 和实验 [17–22] 的后续工作. 值得注意的是, 在 2016 年, 有两个里程碑的实验被报道出来. 在第一个工作中, Yin 等 [23] 利用低损耗光纤和参数优化技术将 MDI-QKD 的距离延长到了 404 km. 在第二个工作中, Comandar 等 [24] 利用种子激光

* 国家自然科学基金 (批准号: 61771205)、广东省自然科学基金 (批准号: 2015A030313388) 和广东省科技计划 (批准号: 2015B010128012, 2017KZ010101).

† 通信作者. E-mail: wangjindong@m.scnu.edu.cn

器技术将 MDI-QKD 系统的时钟频率提高到了 1 GHz. 但是, 相对于原始的 BB84 协议来说, MDI-QKD 的安全码率仍然比较低, 一种解决方案就是基于高维 (high dimensional, HD) 编码的 QKD 协议.

目前大多数有关 HD QKD 协议的工作都集中于通过提升光子的某一种自由度的希尔伯特空间维度来提升 QKD 协议的信息容量[25], 例如基于空间模式、基于时间能量纠缠光子对以及基于轨道角动量的 HD QKD 协议等[26−31], 其中, Ali-Khan 等[26]在 2007 年完成第一个基于时间能量纠缠光子对的 HD QKD 协议, 而在 2017 年, Sit 等[29]在渥太华进行了基于轨道角动量的 HD QKD 协议的实地测试实验, 这些工作有力地证明了 HD QKD 协议的可行性. HD QKD 协议不仅可以在一个自由度 (degree of freedom, DOF) 上进行编码, 还可以同时在多个 DOF 上进行编码, 即混合编码协议[32]. 例如 2010 年 wang 等[33]提出的基于 DPS 编码和偏振编码的 HD QKD 协议, 2019 年 Mao 等[34]提出的基于 RRDPS 和偏振编码的 HD QKD 协议. 最近, 有人提出利用 HD 编码来提升 MDI-QKD 协议的安全码率, 例如 Dellantonio 等[31]在 2018 年提出的两种分别基于空间和时间模式的 HD MDI-QKD 协议和 Cui 等[35]于 2019 年提出的基于空间模式和偏振模式的混合编码 HD MDI-QKD 协议, 但是这两种协议在实际应用上都面临一些困难, 前者提出的基于空间模式编码的方案中其解码装置需要更多的单光子探测器, 基于时间模式编码的方案中对其编码装置的带宽要求更高, 而后者提出的混合编码方案需要分辨高维贝尔态, 所以目前该协议在实验上仍然是一个挑战[25].

本文提出了一种另外一种基于相位和偏振的混合编码 HD MDI-QKD 协议. 该协议利用了光子的相位和偏振两种自由度进行编码[4,8−9], 但是解码装置还是和原 MDI-QKD 协议一样, 只利用了 4 个单光子探测器 (single-photon detector, SPD) 进行部分贝尔态检测 (bell-state measurement, BSM)[4], 因此该协议完全可以利用现有实验条件实现. 而且该协议不需要用户端增加其设备的重复频率就可以增加系统的安全码率, 所以该协议可能在未来具有潜在的应用前景.

本文的安排如下. 第 2 节详细介绍了本协议的编解码规则. 第 3 节在考虑某些实际情况的影响下, 得出该协议的安全码率, 并且进行数值仿真, 证明该协议对于安全码率的提升. 第 4 节讨论该协议的实验实现需要满足的条件并且在第 5 节给出本文的结论.

2 协议介绍

本节提出了一种基于混合编码的 MDI-QKD 协议, 该协议编码部分利用了相位编码 MDI-QKD[8] 和偏振编码 MDI-QKD[4] 的方法, 解码部分的装置与原始提出的偏振编码 MDI-QKD 协议一样, 利用 4 个单光子探测器组成了一个部分 BSM 装置, 如图 1 所示. 假设 Alice 和 Bob 都拥有

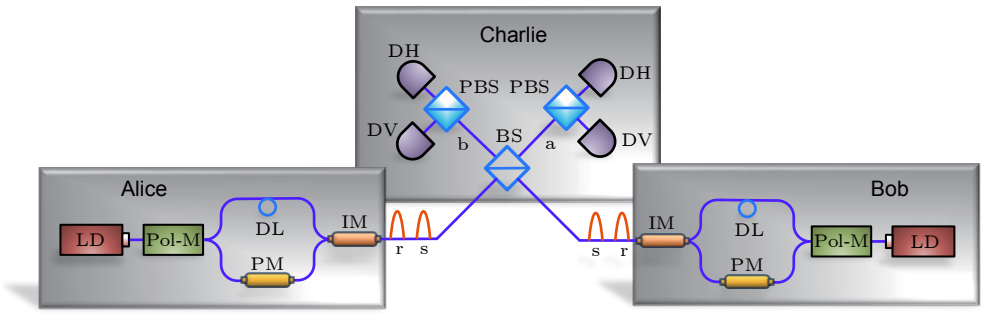

图 1 基于混和编码的 MDI-QKD 协议原理图. 其中, LD 为光源, Pol-M, PM 和 IM 分别为偏振调制器、相位调制器和强度调制器, DL 为光延时线, BS 为 50:50 的光分束耦合器, PBS 为偏振分束器, DH 和 DV 为单光子探测器. 首先, Alice 和 Bob 分别通过 Pol-M 将偏振信息加载到光脉冲上, 然后又通过 PM 和 IM 加载时间-相位信息. Charlie 将接收两者发出的光子并进行部分 BSM, 然后公开其测量结果. Alice 和 Bob 通过基比对然后利用 Charlie 所公开的 BSM 结果就能在他们原始密钥之间建立关联

Fig. 1. Schematic diagram of MDI-QKD protocol based on hyper-encoding. LD is the light source. Pol-M, PM and IM are polarization modulator, phase modulator and intensity modulator, respectively. DL is the optical delay line, BS is the 50:50 optical beam splitter, PBS is the polarization beam splitter, DH and DV are single-photon detector. First, Alice and Bob load the polarization information to the light pulse through Pol-M, respectively, and then load the phase information through PM and IM. Charlie or Eve will receive the photons emitted by both and perform part of the BSM, and then disclose their measurements. Alice and Bob can correlate their original keys by comparing the basis information and using Charlie's published BSM results.

完美的单光子源, 忽略信道和 SPD 的损耗以及暗计数. 而在下一节中会分析某些实际情况对该协议的影响.

本协议的编码过程与 BB84 协议类似, 不同之处在于要同时利用偏振和相位这两个自由度对光脉冲进行调制. 首先 Alice 和 Bob 分别从两组共轭的偏振基 Z 基和 X 基中随机选取一个偏振态, 然后通过 Pol-M 将偏振比特 (Po-bits) 信息加载到光脉冲上. 接着光脉冲通过 50∶50 的分束器 (BS) 和光延时线 (DL) 后被分为参考和信号两种模式, 在 Alice 端的两个模式分别标记为 $\mathrm{a_r}$, $\mathrm{a_s}$, 在 Bob 端的两个模式分别标记为 $\mathrm{b_r}, \mathrm{b_s}$, 如果相位态在 Z 基中选取, 那么相位比特 (Ph-bits) 将只加载在参考光脉冲中或者信号光脉冲中, 另外一个模式的光脉冲会被 IM 损耗掉, 如果 Ph-bits 在 X 基中选取, 那么信号光脉冲在经过 PM 时会被随机加载 $\{0, \pi\}$ 两种相位. 特别指出, 编码过程中偏振基和相位基的选择是独立的. 可以看出, 两个发送端相位基和偏振基的不同选择共有 16 种可能的组合类别, 下面将详细讨论这些组合的 BSM 结果, 并且给出对应的解码规则.

2.1 相位比特在 X 基中选择

首先考虑相位比特在 X 基中选取的情况, 在不考虑编码误差的情况下, Alice 和 Bob 制备的量子态可以表示为

$$\begin{aligned}|\psi_{\mathrm{in}}\rangle =& \frac{1}{2}(|1,j\rangle_{\mathrm{a_r}}|0\rangle_{\mathrm{a_s}} + \mathrm{e}^{\mathrm{i}\theta_{\mathrm{a}}}|0\rangle_{\mathrm{a_r}}|1,j\rangle_{\mathrm{a_s}}) \\ & \otimes (|1,k\rangle_{\mathrm{b_r}}|0\rangle_{\mathrm{b_s}} + \mathrm{e}^{\mathrm{i}\theta_{\mathrm{b}}}|0\rangle_{\mathrm{b_r}}|1,k\rangle_{\mathrm{b_s}}) \\ =& \frac{1}{2}(|1,j\rangle_{\mathrm{a_r}}|1,k\rangle_{\mathrm{b_r}}|0\rangle_{\mathrm{a_s}}|0\rangle_{\mathrm{b_s}} \\ & + \mathrm{e}^{\mathrm{i}\theta_{a}}|0\rangle_{\mathrm{a_r}}|1,k\rangle_{\mathrm{b_r}}|1,j\rangle_{\mathrm{a_s}}|0\rangle_{\mathrm{b_s}} \\ & + \mathrm{e}^{\mathrm{i}\theta_{\mathrm{b}}}|1,j\rangle_{\mathrm{a_r}}|0\rangle_{\mathrm{b_r}}|0\rangle_{\mathrm{a_s}}|1,k\rangle_{\mathrm{b_s}} \\ & + \mathrm{e}^{\mathrm{i}(\theta_{\mathrm{a}}+\theta_{\mathrm{b}})}|0\rangle_{\mathrm{a_r}}|0\rangle_{\mathrm{b_r}}|1,j\rangle_{\mathrm{a_s}}|1,k\rangle_{\mathrm{b_s}}) \\ =& \frac{1}{2}\Big\{|\phi_1\rangle + \mathrm{e}^{\mathrm{i}\theta_{\mathrm{b}}}\left[\mathrm{e}^{\mathrm{i}(\theta_{\mathrm{a}}-\theta_{\mathrm{b}})}|\phi_2\rangle + |\phi_3\rangle\right] \\ & + \mathrm{e}^{\mathrm{i}(\theta_{\mathrm{a}}+\theta_{\mathrm{b}})}|\phi_4\rangle\Big\}, \end{aligned} \tag{1}$$

其中, θ_{a}和θ_{b}分别表示 Alice 和 Bob 所调制的相位, j, k表示所调制的偏振态. 此处忽略了全局相位. 为了更好理解所提出的协议, 本节后面的讨论中会忽略实际情况下器件的非理想特性, 包括量子信道中的损耗, 环境扰动对偏振态和相对相位的影响以及单光子探测器的暗计数等的影响.

接下来, 将详细介绍该协议的解码过程. 从 (1) 式可以看出, 到达 Charlie 端进行干涉的光子模式分为两大类, 一类是双光子干涉, 包括第一项和第四项, 另一类是单光子干涉, 包括中间两项. 因此, 后文会继续分为两种情况讨论 BSM 的结果以及对应的解码规则.

2.1.1 双光子干涉

对于双光子干涉的一类, 加载的相位 $\mathrm{e}^{\mathrm{i}(\theta_{\mathrm{a}}+\theta_{\mathrm{b}})}$ 对最后的干涉结果不起作用, 即相位编码信息会舍弃掉. 因此, 在后面的讨论中忽略相位因子. 由式可得双光子干涉的两项可以分别写为

$$|\phi_1\rangle = a^{\dagger}_{\mathrm{r},j}|0\rangle_{\mathrm{a_r}}b^{\dagger}_{\mathrm{r},k}|0\rangle_{\mathrm{b_r}}|0\rangle_{\mathrm{a_s}}|0\rangle_{\mathrm{b_s}}, \tag{2}$$

$$|\phi_4\rangle = |0\rangle_{\mathrm{a_r}}|0\rangle_{\mathrm{b_r}}a^{\dagger}_{\mathrm{s},j}|0\rangle_{\mathrm{a_s}}b^{\dagger}_{\mathrm{s},k}|0\rangle_{\mathrm{b_s}}, \tag{3}$$

其中, $a^{\dagger}_{\mathrm{r(s)},j}, b^{\dagger}_{\mathrm{r(s)},k}$分别表示两个光脉冲经过 BS 后 a 模式和 b 模式的光子产生算符, 下标 r, s 分别表示参考光模式和信号光模式, j, k 分别表示 Alice 和 Bob 的偏振态模式. 容易得出, 上面两式具有下标 s 和 r 的交换对称性, 因此后面只需要讨论式 (2) 的干涉结果就可以了. 式 (2) 所描述的量子态经过 BS 后, 将会抹去其携带的路径信息, 最终 BSM 结果为

$$\begin{aligned}|\psi_1\rangle =& U_{\mathrm{BS}}|\phi_1\rangle \\ =& \frac{1}{2}(a^{\dagger}_{\mathrm{r},j} + b^{\dagger}_{\mathrm{r},j})(a^{\dagger}_{\mathrm{r},k} - b^{\dagger}_{\mathrm{r},k})|0000\rangle_{a_{\mathrm{r}},b_{\mathrm{r}},a_{\mathrm{s}},b_{\mathrm{s}}} \\ =& \frac{1}{2}(a^{\dagger}_{\mathrm{r},j}a^{\dagger}_{\mathrm{r},k} + b^{\dagger}_{\mathrm{r},j}a^{\dagger}_{\mathrm{r},k} - a^{\dagger}_{\mathrm{r},j}b^{\dagger}_{\mathrm{r},k} - b^{\dagger}_{\mathrm{r},j}b^{\dagger}_{\mathrm{r},k})\,|0000\rangle\,. \end{aligned} \tag{4}$$

在不引起歧义的情况下, 后文中量子态的下标都会和上式中最后一项一样被省略. 上式中U_{BS}表示 50∶50 的 BS 对光子产生算符的作用, 具体可以表示为

$$a^{\dagger}_{x,y} \xrightarrow{U_{\mathrm{BS}}} a^{\dagger}_{x,y} + b^{\dagger}_{x,y}, \tag{5}$$

$$b^{\dagger}_{x,y} \xrightarrow{U_{\mathrm{BS}}} a^{\dagger}_{x,y} - b^{\dagger}_{x,y}, \tag{6}$$

其中, x ($x = \mathrm{r}, \mathrm{s}$), y ($y = j, k$) 分别表示量子态的时间模式和偏振模式, 上式假设 BS 对量子态的时间模式和偏振模式没有影响.

将 BB84 协议的四种偏振态代入 (4) 式中就可以得到 BSM 的结果. 显然, 该协议的解码过程与偏振编码 MDI-QKD 协议类似, 唯一的区别是前者可能在 r 和 s 两个时刻发生符合计数事件. 根据 Charlie 公布的符合计数事件和 Alice 与 Bob 所使用的基, 他们就可以知道其数据比特之间的关联性. 这里以一个简单的例子进行说明, 当 $j=H$, $k=V$ 时, 有:

$$\begin{aligned}|\psi_1\rangle =& \frac{1}{2}(a^{\dagger}_{\mathrm{r},H}a^{\dagger}_{\mathrm{r},V}+b^{\dagger}_{\mathrm{r},H}a^{\dagger}_{\mathrm{r},V}-a^{\dagger}_{\mathrm{r},H}b^{\dagger}_{\mathrm{r},V}\\ &-b^{\dagger}_{\mathrm{r},H}b^{\dagger}_{\mathrm{r},V})\,|0000\rangle\\ =& \frac{1}{2}(|1,H\rangle_{a_{\mathrm{r}}}|1,V\rangle_{a_{\mathrm{r}}}|0\rangle_{b_{\mathrm{r}}}+|1,V\rangle_{a_{\mathrm{r}}}|1,H\rangle_{b_{\mathrm{r}}}\\ &-|1,H\rangle_{a_{\mathrm{r}}}|1,V\rangle_{b_{\mathrm{r}}}\\ &-|0\rangle_{a_{\mathrm{r}}}|1,H\rangle_{b_{\mathrm{r}}}|1,V\rangle_{a_{\mathrm{r}}})|00\rangle_{a_{\mathrm{s}},b_{\mathrm{s}}},\end{aligned}\tag{7}$$

类似地, 可以写出 $|\Psi_4\rangle$ 的表达式. 因此, 当 BSM 出现以下四种符合计数情况时, 可认为是成功事件, 即:

a) 事件 D1: a 端的两个探测器在 r 时刻或者 s 时刻同时响应;

b) 事件 D2: a 端的 DV 探测器和 b 端的 DH 探测器在 r 时刻或者 s 时刻同时响应;

c) 事件 D3: a 端的 DH 探测器和 b 端的 DV 探测器在 r 时刻或者 s 时刻同时响应;

d) 事件 D4: b 端的两个探测器在 r 时刻或者 s 时刻同时响应;

其他的情况也可以做类似的分析, 下面分析单光子干涉的情况.

2.1.2 单光子干涉

对于单光子干涉的情况, 入射态的剩余两项经过 50∶50 分束器的作用后的结果可以由式得到:

$$\begin{aligned}|\psi_2\rangle =& U_{\mathrm{BS}}\,|\phi_2\rangle\\ =& \frac{1}{2}(|1,k\rangle_{\mathrm{a_r}}|0\rangle_{\mathrm{b_r}}-|0\rangle_{\mathrm{a_r}}|1,k\rangle_{\mathrm{b_r}})\\ &(|1,j\rangle_{\mathrm{a_s}}|0\rangle_{\mathrm{b_s}}+|0\rangle_{\mathrm{a_s}}|1,j\rangle_{\mathrm{b_s}})\\ =& \frac{1}{2}(|1,k\rangle_{\mathrm{a_r}}|0\rangle_{\mathrm{b_r}}|1,j\rangle_{\mathrm{a_s}}|0\rangle_{\mathrm{b_s}}\\ &+|1,k\rangle_{\mathrm{a_r}}|0\rangle_{\mathrm{b_r}}|0\rangle_{\mathrm{a_s}}|1,j\rangle_{\mathrm{b_s}}\\ &-|0\rangle_{\mathrm{a_r}}|1,k\rangle_{\mathrm{b_r}}|1,j\rangle_{\mathrm{a_s}}|0\rangle_{\mathrm{b_s}}\\ &-|0\rangle_{\mathrm{a_r}}|1,k\rangle_{\mathrm{b_r}}|0\rangle_{\mathrm{a_s}}|1,j\rangle_{\mathrm{b_s}}),\end{aligned}\tag{8}$$

$$\begin{aligned}|\psi_3\rangle =& U_{\mathrm{BS}}\,|\phi_3\rangle\\ =& \frac{1}{2}(|1,j\rangle_{\mathrm{a_r}}|0\rangle_{\mathrm{b_r}}-|0\rangle_{\mathrm{a_r}}|1,j\rangle_{\mathrm{b_r}})\\ &(|1,k\rangle_{\mathrm{a_s}}|0\rangle_{\mathrm{b_s}}+|0\rangle_{\mathrm{a_s}}|1,k\rangle_{\mathrm{b_s}})\\ =& \frac{1}{2}(|1,j\rangle_{\mathrm{a_r}}|0\rangle_{\mathrm{b_r}}|1,k\rangle_{\mathrm{a_s}}|0\rangle_{\mathrm{b_s}}\\ &+|1,j\rangle_{\mathrm{a_r}}|0\rangle_{\mathrm{b_r}}|0\rangle_{\mathrm{a_s}}|1,k\rangle_{\mathrm{b_s}}\\ &-|0\rangle_{\mathrm{a_r}}|1,j\rangle_{\mathrm{b_r}}|1,k\rangle_{\mathrm{a_s}}|0\rangle_{\mathrm{b_s}}\\ &-|0\rangle_{\mathrm{a_r}}|1,j\rangle_{\mathrm{b_r}}|0\rangle_{\mathrm{a_s}}|1,k\rangle_{\mathrm{b_s}}).\end{aligned}\tag{9}$$

上式中利用到了从 (5) 式和式推导得出的公式:

$$|1,x\rangle_{\mathrm{a}}|0\rangle_{\mathrm{b}}\xrightarrow{U_{\mathrm{BS}}}\frac{1}{\sqrt{2}}(|1,x\rangle_{\mathrm{a}}|0\rangle_{\mathrm{b}}+|0\rangle_{\mathrm{a}}|1,x\rangle_{\mathrm{b}}),\tag{10}$$

$$|0\rangle_{\mathrm{a}}|1,x\rangle_{\mathrm{b}}\xrightarrow{U_{\mathrm{BS}}}\frac{1}{\sqrt{2}}(|1,x\rangle_{\mathrm{a}}|0\rangle_{\mathrm{b}}-|0\rangle_{\mathrm{a}}|1,x\rangle_{\mathrm{b}}),\tag{11}$$

其中 $x=j,\ k$. 从式和式可以看出, 干涉的结果与偏振态有关, 下面将分类讨论.

1)$j=k$ 且 $j,k\in Z$, 下面以 $j=k=H$ 为例. 将 j, k 代入 (8) 式和 (9) 式中可得:

$$|\psi_2\rangle=\frac{1}{2}(|H0H0\rangle+|H00H\rangle-|0HH0\rangle-|0H0H\rangle),\tag{12}$$

$$|\psi_3\rangle=\frac{1}{2}(|H0H0\rangle-|H00H\rangle+|0HH0\rangle-|0H0H\rangle).\tag{13}$$

由于相位基匹配, 那么现在可能出现两种干涉结果, 当 $\theta_{\mathrm{a}}-\theta_{\mathrm{b}}=0$ 时, $\mathrm{e}^{\mathrm{i}(\theta_{\mathrm{a}}-\theta_{\mathrm{b}})}=1$, 此时干涉的结果为

$$\mathrm{e}^{\mathrm{i}\theta_{\mathrm{b}}}\left[\mathrm{e}^{\mathrm{i}(\theta_{\mathrm{a}}-\theta_{\mathrm{b}})}\,|\psi_2\rangle+|\psi_3\rangle\right]=\mathrm{e}^{\mathrm{i}\theta_{\mathrm{b}}}(|H0H0\rangle-|0H0H\rangle).\tag{14}$$

而当 $\theta_{\mathrm{a}}-\theta_{\mathrm{b}}=\pm\pi$ 时, $\mathrm{e}^{\mathrm{i}(\theta_a-\theta_b)}=-1$, 此时干涉的结果为

$$\mathrm{e}^{\mathrm{i}\theta_{\mathrm{b}}}\left[\mathrm{e}^{\mathrm{i}(\theta_{\mathrm{a}}-\theta_{\mathrm{b}})}\,|\psi_2\rangle+|\psi_3\rangle\right]=\mathrm{e}^{\mathrm{i}\theta_{\mathrm{b}}}(|H00H\rangle-|0HH0\rangle).\tag{15}$$

由于这种干涉结果完全公开了编码的偏振态信息, 因此偏振信息需要被舍去. 但是, 这两项的干涉结果并没有泄露相位信息, 因此 Alice 和 Bob 可以利用与相位编码 MDI-QKD 协议相同的方式来获取 Ph-bits 信息. 即, 当两发送方偏振态都在 Z 基中选择时, 且出现在 r 时刻 a 端和 b 端的 DH(DV) 探测器同时响应的事件, 或者 s 时刻 a 端和 b 端的 DH(DV) 探测器同时响应的事件时, 两者 Ph-bits 相同, 当出现 r 时刻 a 端的 DH(DV)

探测器和 s 时刻 b 端的 DH(DV) 探测器同时响应的事件, 或者 r 时刻 b 端的 DH(DV) 探测器和 s 时刻 a 端的 DH(DV) 探测器同时响应的事件时, 两者 Ph-bits 相反.

2) $j \neq k$ 且 $j,k \in Z$, 下面以 $j = H$, $k = V$ 为例. 同样将 j, k 代入 (8) 式和 (9) 式中可得:

$$|\psi_2\rangle = \frac{1}{2}(|V0H0\rangle + |V00H\rangle - |0VH0\rangle - |0V0H\rangle), \tag{16}$$

$$|\psi_3\rangle = \frac{1}{2}(|H0V0\rangle + |H00V\rangle - |0HV0\rangle - |0H0V\rangle). \tag{17}$$

可以看出, 上面两式内部的 8 个子项各不相同, 因此两式的直接相加或相减并不能消去任何一个子项. 此时的干涉结果表明, BS 不仅抹去了输入态的路径信息, 同时也把相位信息抹去了. 但是, 正因为入射态的路径信息被抹去了, 那么最终的干涉结果只能表明两个发送方所加载的偏振态的相互关系, 而没有泄露关于两个发送方所编码信息的确切值, 因此, 可以利用此探测结果来获取 Po-bits 信息. 即, 当两发送方偏振态都在 Z 基中选择时, 干涉结果为 r 时刻和 s 时刻各有一个探测器响应, 而且这两个探测器所代表的偏振态不相同时, Alice 和 Bob 的 Po-bits 翻转.

3) $j = k$ 且 $j,k \in X$, 下面以 $j = k = +$ 为例. 同样将 j, k 代入 (8) 式和 (9) 式中可得:

$$\begin{aligned}|\psi_2\rangle = \frac{1}{4}&(|H0H0\rangle + |V0H0\rangle + |H0V0\rangle + |V0V0\rangle\\ &+ |H00H\rangle + |V00H\rangle + |H00V\rangle + |V00V\rangle\\ &- |0HH0\rangle - |0VH0\rangle - |0HV0\rangle - |0VV0\rangle\\ &- |0H0H\rangle - |0V0H\rangle - |0H0V\rangle - |0V0V\rangle)\\ = \frac{1}{4}&(|\psi_{2-1}\rangle + |\psi_{2-2}\rangle + |\psi_{2-3}\rangle + |\psi_{2-4}\rangle),\end{aligned} \tag{18}$$

$$\begin{aligned}|\psi_3\rangle = \frac{1}{4}&(|H0H0\rangle + |V0H0\rangle + |H0V0\rangle + |V0V0\rangle\\ &- |H00H\rangle - |V00H\rangle - |H00V\rangle - |V00V\rangle\\ &+ |0HH0\rangle + |0VH0\rangle + |0HV0\rangle + |0VV0\rangle\\ &- |0H0H\rangle - |0V0H\rangle - |0H0V\rangle - |0V0V\rangle)\\ = \frac{1}{4}&(|\psi_{3-1}\rangle + |\psi_{3-2}\rangle + |\psi_{3-3}\rangle + |\psi_{3-4}\rangle).\end{aligned} \tag{19}$$

容易看出, 上两式除了中间两项的符号相反外, 其余部分都相同, 即 $|\psi_{2-1}\rangle = |\psi_{3-1}\rangle, |\psi_{2-4}\rangle = |\psi_{3-4}\rangle, |\psi_{2-2}\rangle = -|\psi_{3-2}\rangle, |\psi_{2-3}\rangle = -|\psi_{3-3}\rangle$. 利用这个规律可以简化后面的计算. 当 $\theta_{\rm a} - \theta_{\rm b} = 0$ 时, $\mathrm{e}^{\mathrm{i}(\theta_{\rm a}-\theta_{\rm b})} = 1$, 此时干涉的结果为

$$\begin{aligned}&\mathrm{e}^{\mathrm{i}\theta_{\rm b}}\left[\mathrm{e}^{\mathrm{i}(\theta_{\rm a}-\theta_{\rm b})}|\psi_2\rangle + |\psi_3\rangle\right]\\ =\ &\frac{1}{2}\mathrm{e}^{\mathrm{i}\theta_{\rm b}}(|\psi_{2-1}\rangle + |\psi_{2-4}\rangle)\\ =\ &\frac{1}{2}(|H0H0\rangle + |V0H0\rangle + |H0V0\rangle + |V0V0\rangle\\ &- |0H0H\rangle - |0V0H\rangle - |0H0V\rangle - |0V0V\rangle).\end{aligned} \tag{20}$$

而当 $\theta_{\rm a} - \theta_{\rm b} = \pm\pi$ 时, $\mathrm{e}^{\mathrm{i}(\theta_{\rm a}-\theta_{\rm b})} = -1$, 此时干涉的结果为

$$\begin{aligned}&\mathrm{e}^{\mathrm{i}\theta_{\rm b}}\left[\mathrm{e}^{\mathrm{i}(\theta_{\rm a}-\theta_{\rm b})}|\psi_2\rangle + |\psi_3\rangle\right]\\ =\ &\frac{1}{2}\mathrm{e}^{\mathrm{i}\theta_{\rm b}}(|\psi_{2-2}\rangle + |\psi_{2-3}\rangle)\\ =\ &\frac{1}{2}(|H00H\rangle + |V00H\rangle + |H00V\rangle + |V00V\rangle\\ &- |0HH0\rangle - |0VH0\rangle - |0HV0\rangle - |0VV0\rangle).\end{aligned} \tag{21}$$

虽然上面两种干涉结果完全不相同, 似乎可以用来获取 Ph-bits 信息, 但是这只是在 $j = k = +$ 条件下的特殊情况, 事实上从下部分 $j = +, k = -$ 的推导结果可以看出, 干涉的结果会受到偏振态和相位的共同影响, 所以此类情况的解码规则将在下部分一起介绍.

4) $j \neq k$ 且 $j,k \in X$, 下面以 $j = +$, $k = +$ 为例. 此条件下的推导过程与上一种情况类似, 这里不再赘述, 下面直接写出结果. 当 $\theta_{\rm a} - \theta_{\rm b} = 0$ 时, $\mathrm{e}^{\mathrm{i}(\theta_{\rm a}-\theta_{\rm b})} = 1$, 此时干涉的结果为

$$\begin{aligned}&\mathrm{e}^{\mathrm{i}\theta_{\rm b}}\left[\mathrm{e}^{\mathrm{i}(\theta_{\rm a}-\theta_{\rm b})}|\psi_2\rangle + |\psi_3\rangle\right]\\ =\ &\frac{1}{2}\mathrm{e}^{\mathrm{i}\theta_{\rm b}}(|\psi'_{2-1}\rangle + |\psi'_{2-4}\rangle)\\ =\ &\frac{1}{2}(|H0H0\rangle - |V00H\rangle + |H00V\rangle - |V0V0\rangle\\ &- |0H0H\rangle + |0VH0\rangle - |0HV0\rangle + |0V0V\rangle).\end{aligned} \tag{22}$$

而当 $\theta_{\rm a} - \theta_{\rm b} = \pm\pi$ 时, $\mathrm{e}^{\mathrm{i}(\theta_{\rm a}-\theta_{\rm b})} = -1$, 此时干涉的结果为

$$\begin{aligned}&\mathrm{e}^{\mathrm{i}\theta_{\rm b}}\left[\mathrm{e}^{\mathrm{i}(\theta_{\rm a}-\theta_{\rm b})}|\psi_2\rangle + |\psi_3\rangle\right]\\ =\ &\frac{1}{2}\mathrm{e}^{\mathrm{i}\theta_{\rm b}}(|\psi'_{2-2}\rangle + |\psi'_{2-3}\rangle)\\ =\ &\frac{1}{2}(|H00H\rangle - |V0H0\rangle + |H0V0\rangle - |V00V\rangle\\ &- |0HH0\rangle + |0V0H\rangle - |0H0V\rangle + |0VV0\rangle).\end{aligned} \tag{23}$$

将 (22) 式、(23) 式与 (20) 式、(21) 式比较可得, 在$\theta_{\rm a}-\theta_{\rm b}=0(\pm\pi)$时, $|H0H0\rangle, |V0V0\rangle, |0H0H\rangle, |0V0V\rangle$ ($|H00H\rangle, |V00V\rangle, |0HH0\rangle, |0VV0\rangle$)这四种量子态被探测到的事件都会发生, 不会随着初始偏振态而变化, 而剩下几种量子态被探测到的事件是否会发生受到偏振态的影响. 定义事件

$$A0\in\{|H0H0\rangle, |V0V0\rangle, |0H0H\rangle, |0V0V\rangle\}. \quad (24)$$

表示$|H0H0\rangle, |V0V0\rangle, |0H0H\rangle, |0V0V\rangle$这四种量子态中某个量子态被探测到的事件. 同样可以写出:

$$A1\in\{|H00H\rangle, |V00V\rangle, |0HH0\rangle, |0VV0\rangle\}, \quad (25)$$

$$B0\in\{|V0H0\rangle, |H0V0\rangle, |0V0H\rangle, |0H0V\rangle\}, \quad (26)$$

$$B1\in\{|V00H\rangle, |H00V\rangle, |0VH0\rangle, |0HV0\rangle\}. \quad (27)$$

那么可以将第 3 类和第 4 类情况的 BSM 结果归纳在表 1 中.

表 1 当相位比特在 X 基中选择时, 本协议单光子干涉的第 3 类和第 4 类情况的 BSM 结果比较

Table 1. BSM results for class 3 and class 4 cases of single-photon interference in this protocol are compared when phase bits are selected in the X basis.

Alice & Bob	$\theta_{\rm a}-\theta_{\rm b}$	
	0	$\pm\pi$
$j=k$ 且 $j,k\in X$	A0, B0	A1, B1
$j\neq k$ 且 $j,k\in X$	A0, B1	A1, B0

由表 1 可知, 在第三类和第四类情况下, 只要事件 A0(A1) 发生, 那么就可以断定发送方的 Ph-bits 相同 (相反). 对于 B0 和 B1 事件, 发送方可以通过公布其 Po-bits 的信息, 来获取 Ph-bits 的信息.

5)j 与 k 所代表的 Po-bits 相同, 且 $j\in Z$, $k\in X$, 下面以 $j=H$, $k=+$为例. 将 j, k 的值代入 (8) 式和 (9) 式中可得:

$$\begin{aligned}|\psi_2\rangle=\frac{1}{2\sqrt{2}}(&|H0H0\rangle+|V0H0\rangle\\&+|H00H\rangle+|V00H\rangle-|0HH0\rangle\\&-|0VH0\rangle-|0H0H\rangle-|0V0H\rangle),\end{aligned} \quad (28)$$

$$\begin{aligned}|\psi_3\rangle=\frac{1}{2\sqrt{2}}(&|H0H0\rangle+|H0V0\rangle\\&-|H00H\rangle-|H00V\rangle+|0HH0\rangle\\&+|0HV0\rangle-|0H0H\rangle-|0H0V\rangle).\end{aligned} \quad (29)$$

当 $\theta_{\rm a}-\theta_{\rm b}=0$时, $\mathrm{e}^{\mathrm{i}(\theta_{\rm a}-\theta_{\rm b})}=1$, 此时干涉的结果为

$$\begin{aligned}&\mathrm{e}^{\mathrm{i}\theta_{\rm b}}\left[\mathrm{e}^{\mathrm{i}(\theta_{\rm a}-\theta_{\rm b})}|\psi_2\rangle+|\psi_3\rangle\right]\\&=\frac{1}{2\sqrt{2}}(|V0H0\rangle+|H0V0\rangle+|V00H\rangle-|H00V\rangle\\&\quad-|0VH0\rangle+|0HV0\rangle-|0V0H\rangle-|0H0V\rangle\\&\quad+2|H0H0\rangle-2|0H0H\rangle).\end{aligned} \quad (30)$$

而当 $\theta_{\rm a}-\theta_{\rm b}=\pm\pi$ 时, $\mathrm{e}^{\mathrm{i}(\theta_{\rm a}-\theta_{\rm b})}=-1$, 此时干涉的结果为

$$\begin{aligned}&\mathrm{e}^{\mathrm{i}\theta_{\rm b}}\left[\mathrm{e}^{\mathrm{i}(\theta_{\rm a}-\theta_{\rm b})}|\psi_2\rangle+|\psi_3\rangle\right]\\&=\frac{1}{2\sqrt{2}}(|V0H0\rangle-|H0V0\rangle+|V00H\rangle+|H00V\rangle\\&\quad-|0VH0\rangle-|0HV0\rangle-|0V0H\rangle+|0H0V\rangle\\&\quad+2|H00H\rangle-2|0HH0\rangle).\end{aligned} \quad (31)$$

可以看出, 干涉结果的最后两项与第 1 类情况的干涉结果, 即式和式的结果一样, 所以用同样的方法可以从这两项提取出 Ph-bits 信息. 而前面 8 项所引起的响应结果显然无法提取任何有效信息.

由于对称性, 容易得出关于偏振基不匹配的其他三种情况的干涉结果也是类似的, 这里就不再赘述. 上文对所有相位比特在 X 基中选择的情况进行了讨论, 下文将分别讨论相位比特在 Z 基中选择和相位比特在不同基中选择的情况.

2.2 相位比特在 Z 基中选择时

接下来讨论相位比特在 Z 基中选择的情况. 假设用 l 和 m 和分别表示 Alice 和 Bob 选取的 Ph-bits, 即 $l\,(m)=0$ (1) 时表示 Alice (Bob) 选择的 Ph-bits 为 0 (1). 下面分情况讨论解码过程.

1)$l=m$ 且 $l,m\in Z$, 下面以 $l=m=0$ 为例. 此时 Alice 和 Bob 入射的量子态为

$$\begin{aligned}|\psi_{\rm in}\rangle&=(|1,j\rangle_{\rm a_r}|0\rangle_{\rm a_s})\otimes(|1,k\rangle_{\rm b_r}|0\rangle_{\rm b_s})\\&=|1,j\rangle_{\rm a_r}|1,k\rangle_{\rm b_r}|00\rangle_{\rm a_s b_s}.\end{aligned} \quad (32)$$

显然, (32) 式与 (1) 式中的$|\phi_1\rangle$相同, 因此干涉结果和解码过程与双光子干涉类完全一样.

2)$l\neq m$ 且 $l,m\in Z$, 下面以 $l=0$, $m=1$ 为例. 此时 Alice 和 Bob 入射的量子态为

$$\begin{aligned}|\psi_{\rm in}\rangle&=(|0\rangle_{\rm a_r}|1,j\rangle_{\rm a_s})\otimes(|1,k\rangle_{\rm b_r}|0\rangle_{\rm b_s})\\&=|0\rangle_{\rm a_r}|1,k\rangle_{\rm b_r}|1,j\rangle_{\rm a_s}|0\rangle_{\rm b_s}.\end{aligned} \quad (33)$$

容易得出, 光脉冲对经过 BS 后路径信息会被抹去, 而 Po-bits 信息会被泄露出来, 所以这种条

件下, 通信双方无法提取任何 Po-bits 信息, 但是却可以获取所有的 Ph-bits 信息. 即当相位态在 Z 基中选择时, 无论通信双方偏振基的选择是什么, 只要 Charlie 端公布的探测结果为 r 时刻和 s 时刻分别各有一次探测器响应, 那么就可以断定两者的 Ph-bits 是相反的.

2.3 相位比特在不同的基中选择时

接下来讨论当相位比特的基不匹配的情况. 根据 l, m 是否相等以及属于两种不同的基, 可以分成四种不同的情况讨论, 但是又根据 Alice 和 Bob 的对称性以及比特 0, 1 之间的对称性, 发现只需要讨论其中一种情况就够了. 下面以 $l \in Z, m \in X$ 为例, 此时输入态可以写为

$$\begin{aligned}|\psi_{\text{in}}\rangle =& (|1,j\rangle_{\text{a}_\text{r}}|0\rangle_{\text{a}_\text{s}}) \otimes (|1,k\rangle_{\text{b}_\text{r}}|0\rangle_{\text{b}_\text{s}} \\ &+ \text{e}^{\text{i}\theta_\text{b}}|0\rangle_{\text{b}_\text{r}}|1,k\rangle_{\text{b}_\text{s}}) \\ =& |1,j\rangle_{\text{a}_\text{r}}|1,k\rangle_{\text{b}_\text{r}}|00\rangle_{\text{a}_\text{s},\text{b}_\text{s}} \\ &+ \text{e}^{\text{i}\theta_\text{b}}|1,j\rangle_{\text{a}_\text{r}}|0\rangle_{\text{b}_\text{r}}|0\rangle_{\text{a}_\text{s}}|1,k\rangle_{\text{b}_\text{s}}. \end{aligned} \tag{34}$$

显然, 上式无法提取任何 Ph-bits 信息, 但是上式前半部分却可以提取出 Po-bits 信息, 其解码规则与双光子干涉的情况也是一样的. 综上所述完成了所有情况下的解码规则的介绍, 结果整理在表 2 中.

2.4 高信息容量

本节将分析在理想单光子源的情况下, 本文提出的协议与原始协议相比的优势. 在后文中将比较在诱骗态协议下的优势.

将本协议所有情况下的信息容量总结在表 3 中. 假设选择两种基的概率相等, 那么由表中的数据可以计算出本协议每个光子传送的信息容量, 即光子利用效率为 11/32, 而原始 MDI-QKD 协议, 无论是基于相位编码还是偏振编码, 其光子利用效率都只有 1/4, 那么容易得出本协议相比于原始 MDI-QKD 协议提升的效率为

$$\frac{11/32 - 1/4}{1/4} \times 100\% = 37.5\%. \tag{35}$$

上式证明了在本协议相对于原始 MDI-QKD 协议在光子利用效率上的提升.

表 2 本协议的解码规则, 其中 flip 表示比特翻转, No flip 表示比特相同, C0 表示事件{在 r 时刻和 s 时刻分别有且只有一个探测器响应}, 0 表示没有成功事件

Table 2. The decoding rules of this protocol, where flip represents the bit flip, No flip represents the same bit, C0 represents the event {there is only one detector response at time r and time s respectively}, and 0 indicates that no success event occurred.

偏振基	相位基					
	$l, m \in Z$		$l, m \in X$		相位基不匹配	
	Flip	No flip	Flip	No flip	Flip	No flip
$j, k \in Z$	C0, D1, D2, D3, D4	0	A0, B0, B1, D1, D2, D3, D4	A1	D1, D2, D3, D4	0
$j, k \in X$	C0, D2, D3	D1, D4	A0, D2, D3, B0 $(j=k)$B1 $(j \neq k)$	A1, D1, D4, B0 $(j \neq k)$B1 $(j=k)$	D2, D3	D1, D4
偏振基不匹配	C0	0	A0	A1	0	0

表 3 本协议不同情况下可能获得的比特信息及其相应的概率. 其中 Ph (Po)-z (x) 表示获取以 Z(X) 基编码的 Ph-bits(Po-bits) 信息

Table 3. The bitwise information that may be obtained under different circumstances in this agreement and its corresponding probability. Where Ph(Po)-z(x) represents the Ph-bits (Po-bits) information encoded by z (x) basis.

偏振基		相位基				
		$l, m \in Z$		$l, m \in X$		相位基不匹配
		$l = m$	$l \neq m$	单光子干涉	双光子干涉	
$j, k \in Z$	$j = k$	0	1 Ph-z	1 Ph-x	0	0
	$j \neq k$	1 Po-z	1 Ph-z	1 Po-z	1 Po-z	1/2 Po-z
$j, k \in X$	$j = k$	1/2 Po-x	1 Ph-z	1 Ph-x	1/2 Po-x	1/4 Po-x
	$j \neq k$	1/2 Po-x	1 Ph-z	1 Ph-x	1/2 Po-x	1/4 Po-x
偏振基不匹配		0	1 Ph-z	1/2 Ph-x	0	0

3 实际性能评估

上节详细介绍了本协议在理想情况下的编解码过程, 本节将考虑实际情况下的器件的非理想特性, 首先引入 4 强度诱骗态方法 [36] 来解决实际光源的多光子问题, 除此之外还考虑了有限码长条件下的统计波动 [37]、信道损耗、实际单光子探测器的暗计数和探测效率问题, 最后利用全参数优化方法 [38,39] 得出该协议的最优安全码率.

3.1 诱骗态方法

众所周知, 诱骗态方法的目的是为了更加紧凑地估计单光子响应率的下界 S_{11}^{L} 和误码率的上界 e_{11}^{U}, 从而极大地提高协议的安全密钥速率 [6–7], 而 4 强度诱骗态方法不仅将不同强度诱骗态光源的统计波动联合求解 [37], 而且同时估计出 S_{11}^{L} 和 e_{11}^{U} 的值, 从而直接将安全密钥的最小值求解出来 [36]. 这种方法不仅直接提高了安全密钥率, 而且还缩短了产生新密钥所需的时间. 本节将详细介绍如何利用 4 强度诱骗态方法 [36] 来估计本协议的相关参数, 并且最终得出在有限码长条件下的安全码率.

用下标 A 或 B 来定义光源是属于 Alice 或者 Bob. 在光子数空间中, 四种不同强度光源发出的量子态可以分别表示为

$$\rho_{x_{\mathrm{A}}}=\sum_k a_x(k)\left|k\right\rangle\left\langle k\right|,\ \rho_{x_{\mathrm{B}}}=\sum_k b_x(k)\left|k\right\rangle\left\langle k\right|, \tag{36}$$

$$\rho_{y_{\mathrm{A}}}=\sum_k a_y(k)\left|k\right\rangle\left\langle k\right|,\ \rho_{y_{\mathrm{B}}}=\sum_k b_y(k)\left|k\right\rangle\left\langle k\right|, \tag{37}$$

$$\rho_{z_{\mathrm{A}}}=\sum_k a_z(k)\left|k\right\rangle\left\langle k\right|,\ \rho_{z_{\mathrm{B}}}=\sum_k b_z(k)\left|k\right\rangle\left\langle k\right|, \tag{38}$$

$$\rho_{o_{\mathrm{A}}}=\rho_{o\mathrm{B}}=\left|0\right\rangle\left\langle 0\right|, \tag{39}$$

其强度和概率分别为 $\mu_{i_{\mathrm{A(B)}}}$ 和 $p_{i_{\mathrm{A(B)}}}(i=x,y,z,o)$. 在本协议中, 当 Alice 选择源 z 发送光脉冲时, 其相位基和偏振基都选择 Z 基; 当 Alice 选择源 y 发送光脉冲时, 其相位基和偏振基的选择不相同, 且不相同的两种情况的概率都为 0.5; 当 Alice 选择源 x 发送光脉冲时, 其相位基和偏振基都选择 X 基. 诱骗态具体方案总结在表 4 中. 定义源 lr 表示 Alice 选择源 l, Bob 选择源 r 发送光脉冲 (l, $r=x$, y, z, o), 定义符号 $X_{lr,i}^{j}$, 其中当 X = S (D) 时, 该符号表示源 lr 中 X (Z) 基比特的响应率, 当 X = T, E 时, 该符号表示源 lr 中 X (Z) 基比特的误码率, 上标 $j=$ ph, po 分别表示该物理量从 ph-bits 和 po-bits 中获得, 下标 $i=$ o, h, r 分别表示该物理量由原 MDI 协议求得、由本协议所求得和由本协议求得的值再经过修正后求得. 例如 $S_{xx,\mathrm{r}}^{\mathrm{ph}}$ 表示本协议从源 xx 中获取的属于 X 基的 Ph-bits 的响应率的修正值.

显然, 本协议的诱骗态方法所获取的安全密钥由 Ph-bits 和 Po-bits 两部分组成. 但是, 与原 MDI-

表 4 本协议的诱骗态方案以及不同强度光源所获得的比特信息. 其中 Po-X(Z) 和 Ph-Z(X) 分别表示加载信息时偏振基选择 Z(X) 基和相位基选择 Z(X) 基, p_x,p_y,p_z 分别表示三种强度光源的概率, 分数表示获得比特信息的概率, z(x)-ph(po) 表示该信息是用相位 (偏振) 解码方式获得的 z(x) 基下的比特信息

Table 4. The scheme of decoy state and the bit information obtained by different intensity light sources. Where, Po-X (Z) and Ph-Z (X) respectively represent the polarization basis selection Z(X) basis and phase basis selection Z(X) basis when loading information, p_x,p_y,p_z respectively represent the probability of three intensity light sources, fraction represents the probability of obtaining bit information, and z(x) -ph(Po) represents the bit information under z(x) basis obtained by phase (polarization) decoding.

Bob			Alice			
			Po-Z		Po-X	
			Ph-Z	Ph-X	Ph-Z	Ph-X
			p_z	$1/2p_y$	$1/2p_y$	p_x
Po-Z	Ph-Z	p_z	1/4 z-po 1/2 z-ph	1/4 z-po	1/2 z-ph	0
	Ph-X	$1/2p_y$	1/4 z-po	1/4 x-ph 1/2 z-po	0	1/4 x-ph
Po-X	Ph-Z	$1/2p_y$	1/2 z-ph	0	1/4 x-po 1/2 z-ph	1/4 x-po
	Ph-X	p_x	0	1/4 x-ph	1/4 x-po	1/4 x-po 1/2 x-ph

表 5 本协议的诱骗态方法获得的比特信息. 其中 x, y, z 分别表示三种强度的光源, Ph 和 Po 分别表示相位比特和偏振比特, 数字表示获得比特信息的概率, z 和 x 表示获得信息所属的基

Table 5. The bit information obtained by the decoy state method of this protocol. Where x, y and z represent the light source of three kinds of intensity, Ph and Po respectively represent phase bit and polarization bit, fraction represents the probability of obtaining bit information, and z and x represent the basis to which the obtained information belongs.

Bob	Alice					
	z		y		x	
	Ph	Po	Ph	Po	Ph	Po
z	1/2 z	1/4 z	1/4 z	1/8 z	0	0
y	1/4 z	1/8 z	1/8 z1/16 x	1/8 z1/16 x	1/8 x	1/8 x
x	0	0	1/8 x	1/8 x	1/2 x	1/4 x

QKD 协议不同的是, 本协议不同源 lr 所获得的不同基的比特信息是不一样的 (如表 5 所示), 那么这就导致不同源的 X 基和 Z 基的单光子对的响应率不相等, 即 $S_{11}^{\mathrm{X}} \neq S_{11}^{\mathrm{Z}}$, 因此不能和原 MDI 协议一样直接利用 S_{11}^{X} 去估计 S_{11}^{Z}, 而是应先找出从源 $lr(l, r = x, y, o)$ 获取的 X 基的比特信息 B_{lr}^{X} 与从源 zz 获取的 Z 基比特信息 B_{lr}^{Z} 的比例关系, 如果定义它们的比例为一个正常数 M_{lr}, 那么有 $B_{\mathrm{zz}}^{\mathrm{Z}} = M_{lr}B_{lr}^{\mathrm{X}}$, 接着将 M_{lr} 与本协议对应源 lr 的响应率 $S_{lr,h}^{\mathrm{X}}$ 相乘就可以得到修正后的响应率 $S_{lr,r}^{\mathrm{X}}$, 即 $S_{lr,r}^{\mathrm{X}} = M_{lr}S_{lr,h}^{\mathrm{X}}$, 然后利用这个关系先求出 X 基的单光子对响应率 $s_{11,\mathrm{r}}^{\mathrm{X}}$, 最后再利用 $s_{11,\mathrm{r}}^{\mathrm{X}}$ 去估计 s_{11}^{Z} 就可以求出最终安全密钥.

下面以本协议获取的 Ph-bits 信息去估计单光子对响应率的下界 $S_{11}^{\mathrm{ph,L}}$ 为例来进行说明. 通过将表 5 和原 MDI 协议比较可知, 对于 Ph-bits 来说, 源 yy 的响应率为原 MDI 协议响应率的 1/8, 那么可以得到修正的响应率为

$$S_{yy,\mathrm{r}}^{\mathrm{ph}} = S_{yy} = 8S_{yy,\mathrm{h}}^{\mathrm{ph}}. \tag{40}$$

又由于响应率的降低表示此条件下的有效事件发生概率的降低, 因此源 yo 和 oy 的响应率也应该对应降低, 保守估计降低后的响应率为原协议响应率的 1/8, 即:

$$S_{yo,\mathrm{r}}^{\mathrm{ph}} = S_{yo} = 8S_{yo,\mathrm{h}}^{\mathrm{ph}}, \tag{41}$$

而其他源的响应率都不变, 即:

$$S_{lr,\mathrm{r}}^{\mathrm{ph}} = S_{lr} = S_{lr,\mathrm{h}}^{\mathrm{ph}}(lr \in \{oo, ox, xo, xx, zz\}), \tag{42}$$

确定了响应率变化的关系后, 还必须要考虑统计波动的影响. 根据文献 [37], 在考虑有限码长效应后, 需要引入响应率的均值 $\langle S_{lr}\rangle$ 来估计参数 S_{11}^{L}, 而均值 $\langle S_{lr}\rangle$ 与实验可观测值 S_{lr} 之间的关系为

$$\langle S_{lr}\rangle = S_{lr}(1+\delta_{lr}), \tag{43}$$

如果假设成功概率为 $1-\varepsilon$, 则有

$$|\delta_{lr}| \leqslant \gamma\sqrt{\frac{1}{S_{lr}N_{lr}}}, \tag{44}$$

其中 N_{lr} 表示源 lr 所发送光脉冲的总数, 如果将 (43) 式两边同时乘以一个系数 m $(m>0)$, 可以得到:

$$\langle mS_{lr}\rangle = mS_{lr}(1+\delta_{lr}) = mS_{lr}\left(1+\gamma\sqrt{\frac{1}{S_{lr}N_{lr}}}\right), \tag{45}$$

那么这就得到了由响应率 S_{lr}^{L} 表示的, 响应率 mS_{lr}^{L} 的均值 $\langle mS_{lr}^{\mathrm{L}}\rangle$ 的表达式, 此式与用定义式 (43) 得到的均值 $\langle mS_{lr}^{\mathrm{L}}\rangle$ 的表达式的不同之处就在于统计波动参数 δ_{lr}, 假设后者统计波动参数为 δ'_{lr}, 那么两者之间的关系为

$$\delta_{lr} = \sqrt{m}\delta'_{lr}. \tag{46}$$

也就是说, 在估计参数 $S_{11}^{\mathrm{ph,L}}$ 时, 虽然响应率本身可以通过乘以某个系数去修正, 但是统计波动的影响却无法消除. 将式 (40)—代入 S_{11}^{L} 的表达式 [36] 中, 可以得到 Ph-bits 单光子响应率的下界为

$$\begin{aligned} S_{11}^{\mathrm{ph}}(H) &\geqslant S_{11}^{\mathrm{ph,L}}(H) \\ &= \frac{s_1 - s_2 - a_y(1)b_y(2)H}{a_x(1)a_y(1)\left[b_x(1)b_y(2) - b_x(2)b_y(1)\right]}, \end{aligned} \tag{47}$$

$$\begin{aligned} s_1 = {} & a_y(1)b_y(2)\left\langle S_{xx,\mathrm{r}}^{\mathrm{ph}}\right\rangle + a_x(1)b_x(2)a_y(0)\left\langle S_{oy,\mathrm{r}}^{\mathrm{ph}}\right\rangle \\ & + a_x(1)b_x(2)b_y(0)\left\langle S_{yo,\mathrm{r}}^{\mathrm{ph}}\right\rangle, \end{aligned} \tag{48}$$

$$s_2 = a_x(1)b_x(2)\left\langle S_{yy,\mathrm{r}}^{\mathrm{ph}}\right\rangle + a_x(1)b_x(2)a_y(0)\left\langle S_{oo,\mathrm{r}}^{\mathrm{ph}}\right\rangle, \tag{49}$$

$$H = a_x(0)\left\langle S_{ox,\mathrm{r}}^{\mathrm{ph}}\right\rangle + b_x(0)\left\langle S_{xo,\mathrm{r}}^{\mathrm{ph}}\right\rangle - a_x(0)b_x(0)\left\langle S_{oo,\mathrm{r}}^{\mathrm{ph}}\right\rangle, \tag{50}$$

上式满足的约束条件为

$$N_{lr}S^{\rm ph}_{lr,r}+\gamma\sqrt{N_{lr}S^{\rm ph}_{lr,\rm r}}\geqslant N_{lr}\left\langle S^{\rm ph}_{lr,\rm r}\right\rangle$$
$$\geqslant N_{lr}S^{\rm ph}_{lr,\rm r}-\gamma\sqrt{N_{lr}S^{\rm ph}_{lr,\rm r}}(lr\in D_1),\tag{51}$$

$$N_{lr}S^{\rm ph}_{lr,\rm r}+\gamma\sqrt{8N_{lr}S^{\rm ph}_{lr,\rm r}}\geqslant N_{lr}\left\langle S^{\rm ph}_{lr,\rm r}\right\rangle$$
$$\geqslant N_{lr}S^{\rm ph}_{lr,\rm r}-\gamma\sqrt{8N_{lr}S^{\rm ph}_{lr,\rm r}}(lr\in D_2),\tag{52}$$

$$N_{yo}\left\langle S^{\rm ph}_{yo,\rm r}\right\rangle+N_{oy}\left\langle S^{\rm ph}_{oy,\rm r}\right\rangle\geqslant N_{yo}S^{\rm ph}_{yo,\rm r}$$
$$+N_{oy}S^{\rm ph}_{oy,\rm r}-\gamma\sqrt{8N_{yo}S^{\rm ph}_{yo,\rm r}+8N_{oy}S^{\rm ph}_{oy,\rm r}},\tag{53}$$

$$N_{xx}\left\langle S^{\rm ph}_{xx,\rm r}\right\rangle+N_{yo}\left\langle S^{\rm ph}_{yo,\rm r}\right\rangle+N_{oy}\left\langle S^{\rm ph}_{oy,\rm r}\right\rangle$$
$$\geqslant N_{yo}S^{\rm ph}_{yo,\rm r}+N_{oy}S^{\rm ph}_{oy,\rm r}+N_{xx}S^{\rm ph}_{xx,\rm r}$$
$$-\gamma\sqrt{8N_{yo}S^{\rm ph}_{yo,\rm r}+8N_{oy}S^{\rm ph}_{oy,\rm r}+N_{xx}S^{\rm ph}_{xx,\rm r}},\tag{54}$$

$$N_{yy}\left\langle S^{\rm ph}_{yy,\rm r}\right\rangle+N_{oo}\left\langle S^{\rm ph}_{oo,\rm r}\right\rangle\leqslant N_{yy}S^{\rm ph}_{yy,\rm r}$$
$$+N_{oo}S^{\rm ph}_{oo,\rm r}+\gamma\sqrt{8N_{yy}S^{\rm ph}_{yy,\rm r}+N_{oo}S^{\rm ph}_{oo,\rm r}},\tag{55}$$

$$N_{xo}\left\langle S^{\rm ph}_{xo,\rm r}\right\rangle+N_{ox}\left\langle S^{\rm ph}_{ox,\rm r}\right\rangle\leqslant N_{xo}S^{\rm ph}_{xo,\rm r}$$
$$+N_{ox}S^{\rm ph}_{ox,\rm r}+\gamma\sqrt{N_{xo}S^{\rm ph}_{xo,\rm r}+N_{ox}S^{\rm ph}_{ox,\rm r}}$$
$$N_{xo}\left\langle S^{\rm ph}_{xo,\rm r}\right\rangle+N_{ox}\left\langle S^{\rm ph}_{ox,\rm r}\right\rangle\geqslant N_{xo}S^{\rm ph}_{xo,\rm r}$$
$$+N_{ox}S^{\rm ph}_{ox,\rm r}-\gamma\sqrt{N_{xo}S^{\rm ph}_{xo,\rm r}+N_{ox}S^{\rm ph}_{ox,\rm r}},\tag{56}$$

其中, $D_1\in\{oo,ox,xo,xx\}$, $D_2\in\{oy,yo,yy\}$. 显然, 与文献 [36] 比较之后可以发现, 上面的表达式中只有约束条件中与源$lr(lr\in D_2)$相关的不等式才会发生变化, 其他的表达式都没有变化. 而且, 约束条件的这种变化表明了统计波动的范围变大了, 这也符合本协议源$lr(lr\in D_2)$的响应率下降这一事实.

得到$S^{\rm ph}_{lr}(H)$的表达式及其约束条件后, 再利用文献 [37] 中的方法就可以求出其最小值$S^{\rm ph,L}_{lr}(H)$的解析表达式. 接下来讨论 Ph-bits 单光子对的误码率上界$e^{\rm ph,U}_{11}(H)$. 可注意到, 针对每一个比特信息的获取过程, 都是利用特定的一种 MDI-QKD 协议规则去解码的, 要么是偏振 MDI-QKD 协议, 要么是时间相位 MDI-QKD 协议, 因此, 可认为本协议不同源的误码率$T^{\rm ph}_{lr}$与原 MDI 协议一样. 那么根据文献 [36] 可得$e^{\rm ph,U}_{11}(H)$为

$$e^{\rm ph}_{11}(H)\geqslant e^{\rm ph,U}_{11}(H)=\frac{T^{\rm ph}_{xx}+\gamma\sqrt{\dfrac{T^{\rm ph}_{xx}}{N_{xx}}-\dfrac{1}{2}H}}{a_x(0)b_x(0)S^{\rm ph,L}_{11}(H)},\tag{57}$$

那么可以得到安全码率关于 H 的函数表达式为

$$R_{\rm ph}(H)=R^{zz}_{\rm ph}(H)+R^{zy}_{\rm ph}(H)$$
$$+R^{yz}_{\rm ph}(H)+R^{yy}_{\rm ph}(H),\tag{58}$$

$$R^{lr}_{\rm ph}(H)=p_{l_{\rm A}}p_{r_{\rm B}}\times\left\{a_z(1)b_z(1)S^{\rm ph}_{11}(H)[1-h(e^{\rm ph}_{11}(H))]\right.$$
$$\left.-f_{\rm e}D^{\rm ph}_{lr}h(E^{\rm ph}_{lr})\right\}.\tag{59}$$

上式中, $R^{lr}_{\rm ph}(lr\in\{zz,zy,yy\})$表示可以从源$lr$的 Z 基相位比特中所提取的安全码率, $h(x)=-x\log_2(x)-(1-x)\log_2(1-x)$表示二进制的香农信息熵, $f_{\rm e}$表示误码纠错效率. 那么可以得到本协议相位比特安全码率的下界表达式为

$$R_{\rm ph}=\min\{R_{\rm ph}(H)\}H\in[h-\delta,h+\delta],\tag{60}$$
$$h=a_x(0)S^{\rm ph}_{ox,\rm r}+a_x(0)S^{\rm ph}_{xo,\rm r}-a^2_x(0)S^{\rm ph}_{oo,\rm r},$$
$$\delta=a_x(0)\gamma\sqrt{\frac{S^{\rm ph}_{ox,\rm r}+S^{\rm ph}_{xo,\rm r}}{N_{ox}}}+a^2_x(0)\gamma\sqrt{\frac{S^{\rm ph}_{oo,\rm r}}{N_{oo}}},\tag{61}$$

利用同样的方法, 可以求出本协议偏振比特安全码率的下界R_{po}(具体过程见附录 A), 那么总的安全码率为

$$R=R_{\rm ph}+R_{\rm po}.\tag{62}$$

3.2 数值仿真

本节将展现本协议的数值仿真结果, 并与文献 [36] 的结果进行比较. 为了简化计算, 只关注对称的情形, 即 Alice 端的实验装置与 Bob 端完全一样, 两者信道也完全相同. 并且假设 Charlie 端的 4 个探测器是相同的, 即它们有相同的暗计数和探测效率, 而且探测效率不依赖于入射的信号. 除此之外, 还假设两发送端都是随机弱相干态光源, 那么以强度为μ的相干态密度矩阵可以写为$\rho=\sum_k\dfrac{e^{-\mu}\mu^k}{k!}|k\rangle\langle k|$, 而且对于所有的$k$有$a_k=b_k,a'_k=b'_k,a'_k=b''_k$. 当$l=r$时, $p_{l_A}=p_{l_B}$. 关于统计波动的处理, 也与文献 [36] 一样, 假设当失败概率为$\epsilon=10^{-7}$时, 有$\gamma=5.3$.

首先利用文献 [38] 中的 MDI 的线性模型模拟出原始 MDI 协议中不同源和不同基的响应率和误码率, 当然, 与文献 [38] 中的模型不同的是, 在这一过程中考虑了本协议每个比特解码过程都会使用 8 个 SPD 的门, 也就是说通过时分复用的方法每台 SPD 都使用了两个门, 而不是 1 个门. 此时如果令$P(ij|l_il_j)$表示 Charlie 端第i个和第j个探

测器分别有 l_i 和 l_j 个光子入射并同时发生响应的概率, 那么有:

$$P(ij|l_il_j) = \begin{cases} (1-p_{\rm d})^6, & l_i>0 \ \text{且} \ l_j<0, \\ p_{\rm d}(1-p_{\rm d})^6, & l_i+l_j>0 \ \text{且} \ l_il_j=0, \\ p_{\rm d}^2(1-p_{\rm d})^6, & l_i=l_j=0. \end{cases} \tag{63}$$

由于在 MDI-QKD 数值模型中已经将探测器与光路的损耗合并计算, 所以上式中并没有出现探测器损耗参数. 接下来利用前文中推导出的本协议和原始 MDI 协议的关系, 得出本协议的响应率和误码率, 将其分别代入相位比特和偏振比特的单光子对的响应率和误码率的公式中, 通过文献 [37] 中的方法求出其解析表达式, 再代入安全码率公式中就可以求出最终安全密钥. 最后, 本文还对本协议进行了全参数优化[39], 但与文献 [39] 中待优化参数的初值可以利用其他文献的结果不同, 本文提出的是一个新的协议, 如果直接用其他文献的结果作为初值搜索最优参数可能迭代次数较多, 求解时间较长. 所以本文在进行每个参数的优化过程中, 首先以文献 [36] 中的最优化参数作为初值, l 利用进退法搜索待优化参数的最优值的可能存在区间, 然后再利用黄金分割法确定最优化参数的取值.

为了便于和文献 [36] 中的结果进行比较, 在仿真中也使用了两组不同的参数, 具体参数见表 6. 安全码率随距离变化的数值仿真结果见图 2 和图 3, 图中红色实线为本协议的结果, 黑色虚线为文献 [36] 的结果. 从图中可以看出, 本协议对于安全密钥确实有一定的提升作用. 具体来说, 本协议在两种条件下分别使最优安全码率提升了 52.83% 和 50.55%, 相关结果总结在表 8 中.

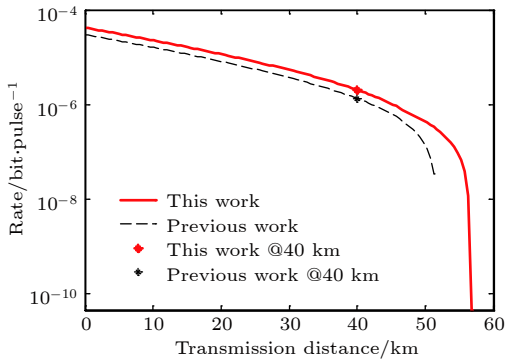

图 2 不同协议的最优安全码率比较. 这里我们利用了表 6 第 a 列的条件, 并且是以 40 km 处的安全码率为优化目标, 本协议的参数优化结果见表 7 第 a 列. 图中红色实线表示本协议的结果, 黑色虚线表示文献 [36] 的结果

Fig. 2. Comparison of optimal security key rates for different protocols. Here, we take advantage of the conditions in column a of Table 6, and take the security key rate at 40 km as the optimization objective. The parameter optimization results of this protocol are shown in column a of Table 7. The solid red line in the figure represents the result of this agreement, and the dotted black line represents the result of Ref. [33].

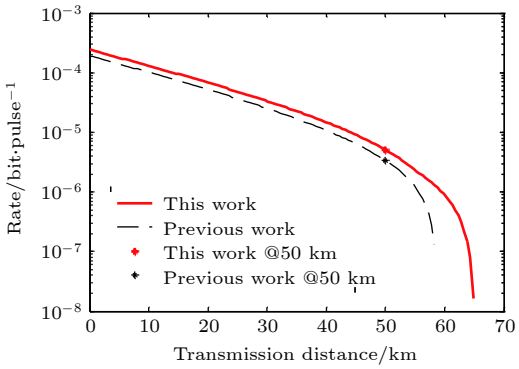

图 3 不同协议的最优安全码率比较. 这里利用了表 6 中第 b 列的条件, 并且是以 50 km 处的安全码率为优化目标, 本协议的参数优化结果见表 7 中第 b 列. 图中红色实线表示本协议的结果, 黑色虚线表示文献 [36] 的结果

Fig. 3. Comparison of optimal security key rates for different protocols. Here, we take advantage of the conditions in column b of Table 6, and take the security key rate at 50 km as the optimization objective. The parameter optimization results of this protocol are shown in column b of Table 7. The red solid line in the figure represents the result of this agreement, and the black dotted line represents the result of Ref. [36].

表 6 数值模拟相关参数. e_0 是当 Alice 或 Bob 发送空脉冲时的误码率; $e_{\rm d}$ 为参考系对准误差; $p_{\rm d}$ 为暗计数率; $\eta_{\rm d}$ 为探测效率; $f_{\rm e}$ 为误码纠错效率; N 为每个发送端发送的光脉冲总数

Table 6. Relevant parameters of numerical simulation. e_0 is the bit error rate when Alice or Bob sends an empty pulse; $e_{\rm d}$ is the reference system alignment error; $p_{\rm d}$ is the dark count rate; $\eta_{\rm d}$ is the detection efficiency; $f_{\rm e}$ is the error code correction efficiency; N is the the total number of light pulses sent by each sender.

	e_0	$e_{\rm d}$/%	$p_{\rm d}$	$\eta_{\rm d}$/%	$f_{\rm e}$	N	ϵ
a	0.5	1.5	6.02×10^{-6}	14.5	1.16	10^{10}	10^{-7}
b	0.5	1.5	10^{-7}	40	1.16	10^{9}	10^{-7}

表 7 本协议两种条件下的参数优化结果.

Table 7. Parameter optimization results under the two conditions of this agreement.

	L / km	μ_x	μ_y	μ_z	p_x	p_y	p_z
a	40	0.0601	0.2907	0.2992	0.4636	0.0310	0.4009
b	50	0.0659	0.3200	0.2744	0.5212	0.0351	0.3283

表 8 最优安全码率的比较. $R_{\rm p}$ 和 $R_{\rm t}$ 分别表示文献 [36] 中的工作和本工作在不同条件下的计算结果. Improvement 表示 $R_{\rm t}$ 相对于 $R_{\rm p}$ 提升的比例

Table 8. Comparison of optimal security key rates. $R_{\rm p}$ and $R_{\rm t}$ respectively represent the calculation results of the work in Ref. [36] and this work under different conditions. Improvement is the ratio of $R_{\rm t}$ to $R_{\rm p}$.

	L / km	$R_{\rm p}$	$R_{\rm t}$	Improvement/%
a	40	1.3394×10^{-6}	2.047×10^{-6}	52.83
b	50	3.3983×10^{-6}	5.116×10^{-6}	50.55

接下来将从两方面来说明为什么数值模拟部分只对文献 [36] 的结果进行比较. 一方面, 相比对于其他的基于高维编码的 MDI-QKD 协议来说, 本协议主要的优势在于实验实现更加简单, 而在安全码率上不一定有提升, 所以与其他的基于高维编码的 MDI-QKD 协议的数值模拟结果的比较并不能完全体现本协议的优势; 另一方面, 对于原 MDI-QKD 协议来说, 四诱骗态协议 [36] 是目前在实验中性能最好的诱骗态 MDI-QKD 协议. 因此, 基于上述理由, 证明本协议相比于原四诱骗态 MDI-QKD 协议在性能上的提升已经足够说明本协议的意义.

4 讨 论

本文提出了一种更加简单的基于相位自由度和偏振自由度的混合编码 MDI-QKD 协议. 首先, 相比于文献 [35] 中提出的基于空间模式和偏振模式两种自由度的混合编码 MDI-QKD 协议, 虽然码率的提升不如后者, 但是实验实现更简单, 特别是在 Charlie 端, 相对于原 MDI-QKD 协议来说不需要做出任何变化. 其次, 相比于文献 [31] 中提出的基于时间模式的 HD MDI-QKD 协议, 本协议优势在于不需要提升用户端的重复频率就可以提升系统的安全密钥率. 下面将讨论两种不同的 MDI-QKD 协议要改进为本协议需要在实验实施上有哪些变化.

一方面, 对于原始的时间编码 MDI-QKD 协议来说 [8], 要改进为本协议需要满足三个条件: 首先需要在发送方增加偏振编码装置, 其次信道中需要增加偏振补偿模块 [40–43], 最后接收方需要增加两台单光子探测器. 目前, 第一个条件很容易满足. 对于第二个条件, 最近的文献中已经报道了最远达到 68 km 的偏振补偿实地测试实验 [43], 说明基于偏振编码的协议已经可以满足在较短距离的应用. 对于第三个条件, 在星型量子网络结构中 [44–45], 接收方增加两台单光子探测器就可以使多个用户的密钥效率提高, 可认为这种成本增加是值得的.

另一方面, 对于原始的偏振编码 MDI-QKD 协议来说 [4], 与本协议不同的地方在于三点: 其一需要在发送方增加相位编码装置; 其二需要增加相位补偿装置; 其三为需要使接收方单光子探测器的饱和计数率增加一倍. 前两个条件都可以利用现有的实验设备实现 [23], 针对最后一个条件同样以星型量子网络为例来进行说明, 此时仅仅只需要一个接收方的成本增加, 而且所有的本地用户的设备重复频率不用变化, 就可以使全部本地用户的密钥率得到提高, 所以同样认为这种成本增加是可以接受的.

另外, 需要指出的是, 上述有关利用 4 强度诱骗态方法 [36] 来估计本协议单光子对的相关参数的分析还比较粗糙, 更加细致的讨论可能会进一步提升安全码率. 比如在估计参数 $s_{11}^{\rm L}$ 时, 与文献 [36] 一样, 只利用了源 lr $(l,r\in D_1,D_2)$ 的相关约束条件, 而没有利用可以获取更多 X 基比特信息的源 xy 和 yx 的相关约束条件, 这样就导致了估计参数时考虑了更大的统计波动, 从而降低了密钥率. 所以关于该协议更加完善的诱骗态方案还有待讨论.

5 结 论

本文提出了另外一种更加简单的基于相位和偏振两个自由度的混合编码 MDI-QKD 协议, 该协议不仅可以提高安全码率, 而且完全可以利用现有的实验设备实现. 首先详细介绍了该协议在理想条件下的编解码规则, 然后利用 4 强度诱骗态方法分析并得出该协议在实际条件下的安全码率, 当然, 本协议的诱骗态方法分析还不够完善, 还有待未来的工作去改进. 特别指出该协议非常适用于量子网络, 例如在星型量子网络结构中, 对于所有的本地用户来说, 只需要给其设备增加一个成本较低的相位编码器或偏振编码器和对应的补偿模块, 就可以实现比原始 MDI-QKD 协议更高的安全码率, 因此该协议在未来具有较大的应用价值.

感谢清华大学物理系于宗文博士的讨论.

附录 A

在本节中将推导 Po-bits 单光子响应率的下界表达式 $S_{11}^{\mathrm{po}}(H)$ 和对应的约束条件. 通过观察表 5 可得不同源中 Po-bits 的响应率的修正关系为

$$S_{lr,\mathrm{r}}^{\mathrm{po}}=\frac{1}{2}S_{lr}=S_{lr,\mathrm{h}}^{\mathrm{po}}(lr\in\{oo,ox,xo,xx,zz\}),\tag{A1}$$

$$S_{l'r',\mathrm{r}}^{\mathrm{po}}=\frac{1}{2}S_{l'r'}=4S_{l'r',\mathrm{h}}^{\mathrm{po}}(lr\in\{oy,yo,yy\}),\tag{A2}$$

利用上面两式和式 (43)—(45) 可得 $S_{11}^{\mathrm{po}}(H)$ 表达式为

$$\begin{aligned}S_{11}^{\mathrm{po}}(H)&\geqslant S_{11}^{\mathrm{po,L}}(H)\\&=\frac{s_1-s_2-a_y(1)b_y(2)H}{a_x(1)a_y(1)\left[b_x(1)b_y(2)-b_x(2)b_y(1)\right]},\end{aligned}\tag{A3}$$

$$\begin{aligned}s_1=&a_y(1)b_y(2)\left\langle S_{xx,\mathrm{r}}^{\mathrm{po}}\right\rangle+a_x(1)b_x(2)a_y(0)\left\langle S_{oy,\mathrm{r}}^{\mathrm{po}}\right\rangle\\&+a_x(1)b_x(2)b_y(0)\left\langle S_{yo,\mathrm{r}}^{\mathrm{po}}\right\rangle,\\s_2=&a_x(1)b_x(2)\left\langle S_{yy,\mathrm{r}}^{\mathrm{po}}\right\rangle+a_x(1)b_x(2)a_y(0)\left\langle S_{oo,\mathrm{r}}^{\mathrm{po}}\right\rangle,\\H=&a_x(0)\left\langle S_{ox,\mathrm{r}}^{\mathrm{po}}\right\rangle+\mathrm{b}_x(0)\left\langle S_{xo,\mathrm{r}}^{\mathrm{po}}\right\rangle\\&-a_x(0)b_x(0)\left\langle S_{oo,\mathrm{r}}^{\mathrm{po}}\right\rangle,\end{aligned}\tag{A4}$$

上式满足的约束条件为

$$\begin{aligned}&N_{lr}S_{lr,\mathrm{r}}^{\mathrm{po}}+\gamma\sqrt{N_{lr}S_{lr,\mathrm{r}}^{\mathrm{po}}}\geqslant N_{lr}\left\langle S_{lr,\mathrm{r}}^{\mathrm{po}}\right\rangle\geqslant N_{lr}S_{lr,\mathrm{r}}^{\mathrm{po}}-\gamma\sqrt{N_{lr}S_{lr,\mathrm{r}}^{\mathrm{po}}}(lr\in D_1),\\&N_{lr}S_{lr,\mathrm{r}}^{\mathrm{po}}+\gamma\sqrt{4N_{lr}S_{lr,\mathrm{r}}^{\mathrm{po}}}\geqslant N_{lr}\left\langle S_{lr,\mathrm{r}}^{\mathrm{po}}\right\rangle\geqslant N_{lr}S_{lr,\mathrm{r}}^{\mathrm{po}}-\gamma\sqrt{4N_{lr}S_{lr,\mathrm{r}}^{\mathrm{po}}}(lr\in D_2),\\&N_{yo}\left\langle S_{yo,\mathrm{r}}^{\mathrm{po}}\right\rangle+N_{oy}\left\langle S_{oy,\mathrm{r}}^{\mathrm{po}}\right\rangle\geqslant N_{yo}S_{yo,\mathrm{r}}^{\mathrm{po}}+N_{oy}S_{oy,\mathrm{r}}^{\mathrm{po}}-\gamma\sqrt{4N_{yo}S_{yo,\mathrm{r}}^{\mathrm{ph}}+4N_{oy}S_{oy,\mathrm{r}}^{\mathrm{po}}},\\&N_{xx}\left\langle S_{xx,\mathrm{r}}^{\mathrm{po}}\right\rangle+N_{yo}\left\langle S_{yo,\mathrm{r}}^{\mathrm{po}}\right\rangle+N_{oy}\left\langle S_{oy,\mathrm{r}}^{\mathrm{po}}\right\rangle\\\geqslant&N_{yo}S_{yo,\mathrm{r}}^{\mathrm{po}}+N_{oy}S_{oy,\mathrm{r}}^{\mathrm{po}}+N_{xx}S_{xx,\mathrm{r}}^{\mathrm{po}}-\gamma\sqrt{4N_{yo}S_{yo,\mathrm{r}}^{\mathrm{ph}}+4N_{oy}S_{oy,\mathrm{r}}^{\mathrm{ph}}+N_{xx}S_{xx,\mathrm{r}}^{\mathrm{ph}}},\\&N_{yy}\left\langle S_{yy,\mathrm{r}}^{\mathrm{po}}\right\rangle+N_{oo}\left\langle S_{oo,\mathrm{r}}^{\mathrm{po}}\right\rangle\leqslant N_{yy}S_{yy,\mathrm{r}}^{\mathrm{po}}+N_{oo}S_{oo,\mathrm{r}}^{\mathrm{po}}+\gamma\sqrt{4N_{yy}S_{yy,\mathrm{r}}^{\mathrm{po}}+N_{oo}S_{oo,\mathrm{r}}^{\mathrm{po}}},\\&N_{xo}\left\langle S_{xo,\mathrm{r}}^{\mathrm{po}}\right\rangle+N_{ox}\left\langle S_{ox,\mathrm{r}}^{\mathrm{po}}\right\rangle\leqslant N_{xo}S_{xo,\mathrm{r}}^{\mathrm{po}}+N_{ox}S_{ox,\mathrm{r}}^{\mathrm{po}}+\gamma\sqrt{N_{xo}S_{xo,\mathrm{r}}^{\mathrm{po}}+N_{ox}S_{ox,\mathrm{r}}^{\mathrm{po}}},\\&N_{xo}\left\langle S_{xo,\mathrm{r}}^{\mathrm{po}}\right\rangle+N_{ox}\left\langle S_{ox,\mathrm{r}}^{\mathrm{po}}\right\rangle\geqslant N_{xo}S_{xo,\mathrm{r}}^{\mathrm{po}}+N_{ox}S_{ox,\mathrm{r}}^{\mathrm{po}}-\gamma\sqrt{N_{xo}S_{xo,\mathrm{r}}^{\mathrm{po}}+N_{ox}S_{ox,\mathrm{r}}^{\mathrm{po}}},\end{aligned}\tag{A5}$$

其中 $D_1\in\{oo,ox,xo,xx\}$, $D_2\in\{oy,yo,yy\}$. 同样, 利用文献 [37] 中的方法可以求出 $S_{11}^{\mathrm{po,L}}(H)$ 的解析表达式. 关于 Po-bits 单光子对的误码率上界 $e_{11}^{\mathrm{po,U}}(H)$, 可认为本协议不同源的误码率 T_{lr} 与原 MDI-QKD 协议一样. 那么根据文献 [36] 可得:

$$e_{11}^{\mathrm{po}}(H)\geqslant e_{11}^{\mathrm{po,U}}(H)=\frac{T_{xx}^{\mathrm{po}}+\gamma\sqrt{\frac{T_{xx}^{\mathrm{po}}}{N_{xx}}}-\frac{1}{2}H}{a_x(0)b_x(0)S_{11}^{\mathrm{po,L}}(H)},\tag{A6}$$

那么可以得到 Po-bits 的安全码率关于 H 的函数表达式为

$$R_{\mathrm{po}}(H)=R_{\mathrm{po}}^{zz}(H)+R_{\mathrm{po}}^{zy}(H)+R_{\mathrm{po}}^{yy}(H),\tag{A7}$$

$$\begin{aligned}R_{\mathrm{po}}^{lr}(H)=&p_{l_{\mathrm{A}}}p_{r_{\mathrm{B}}}\times\Big\{a_z(1)b_z(1)S_{11}^{\mathrm{po}}(H)[1-h(e_{11}^{\mathrm{po}}(H))]\\&-f_{\mathrm{e}}D_{lr}^{\mathrm{po}}h(E_{lr}^{\mathrm{po}})\Big\},\end{aligned}\tag{A8}$$

上式中, $R_{\mathrm{po}}^{lr}(lr\in\{zz,zy,yy\})$ 表示可以从源 lr 的 Po-bits 中所提取 Z 基比特的安全码率, $h(x)=-x\log_2(x)-$

$(1-x)\log_2(1-x)$表示二进制的香农信息熵, f_e表示误码纠错效率. 那么可以得到本协议 Po-bits 安全码率的下界表达式为

$$R_{\rm po} = \min\{R_{\rm po}(H)\} H \in [h-\delta, h+\delta], \tag{A9}$$

$$\begin{aligned} h &= a_x(0)S^{\rm po}_{ox,{\rm r}} + a_x(0)S^{\rm po}_{xo,{\rm r}} - a_x^2(0)S^{\rm po}_{oo,{\rm r}}, \\ \delta &= a_x(0)\gamma\sqrt{\frac{S^{\rm po}_{ox,{\rm r}} + S^{\rm po}_{xo,{\rm r}}}{N_{ox}}} + a_x^2(0)\gamma\sqrt{\frac{S^{\rm po}_{oo,{\rm r}}}{N_{oo}}}. \end{aligned} \tag{A10}$$

参考文献

[1] Bennett C H, Brassard G 2014 *Theor. Comput. Sci.* **560** 7
[2] Xu F, Zhang X M, Lo H K, et al. 2019 arXiv: 1903.09051, [quant-ph]
[3] Pirandola S, Andersen U L, Banchi L, et al. 2019 arXiv: 1906.01645, [quant-ph]
[4] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[5] Braunstein S L, Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[6] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[7] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[8] Ma X, Razavi M 2012 *Phys. Rev. A* **86** 062319
[9] Tamaki K, Lo H K, Fung C H F, et al. 2012 *Phys. Rev. A* **85** 042307
[10] Wang X B 2013 *Phys. Rev. A* **87** 012320
[11] Curty M, Xu F, Cui W, et al. 2014 *Nat. Commn.* **5** 3732
[12] Xu F, Xu H, Lo H K 2014 *Phys. Rev. A* **89** 052333
[13] Du YN, Xie W Z, Jin X, Wang J D, Wei Z J, Qin X J, Zhao F, Zhang Z M 2015 *Acta Phys. Sin.* **64** 110301 (in Chinese) [杜亚男, 解文钟, 金璇, 王金东, 魏正军, 秦晓娟, 赵峰, 张智明 2015 物理学报 **64** 110301]
[14] Zhou Y H, Yu Z W, Wang X B 2016 *Phys. Rev. A* **93** 042324
[15] Hao Y U, Zhang Y, Zhuo W H, Wanyan S P, Liu J S 2019 *Chin. J. of Quan. Elec.* **36** 450 (in Chinese) [于浩, 张影, 卓文合, 完颜绍澎刘金锁 2019 量子电子学报 **36** 450]
[16] Gu W Y, Zhao S H, Dong C, Wang X Y, Yang D 2019 *Acta Phys. Sin.* **68** 240301 (in Chinese) [谷文苑, 赵尚弘, 东晨, 王星宇, 杨鼎 2019 物理学报 **68** 240301]
[17] Liu Y, Chen T Y, Wang L J, et al. 2013 *Phys. Rev. Lett.* **111** 130502
[18] Rubenok A, Slater J A, Chan P, et al. 2013 *Phys. Rev. Lett.* **111** 130501
[19] Ferreira da Silva T, Vitoreti D, Xavier G B, et al. 2013 *Phys. Rev. A* **88** 052303
[20] Tang Y L, Yin H L, Chen S J, et al. 2014 *Phys. Rev. Lett.* **113** 190501
[21] Tang Z, Liao Z, Xu F, et al. 2014 *Phys. Rev. Lett.* **112** 190503
[22] Tang Y L, Yin H L, Chen S J, et al. 2015 *IEEE. J. Sel. Top. Quant* **21** 116
[23] Yin H L, Chen T Y, Yu Z W, et al. 2016 *Phys. Rev. Lett.* **117** 190501
[24] Comandar L C, Lucamarini M, Fröhlich B, et al. 2016 *Nat. Photon.* **10** 312
[25] Cozzolino D, Da Lio B, Bacco D, et al. 2019 *Adv. Quantum Technol.* **2** 1900038
[26] Ali-Khan I, Broadbent C J, Howell J C 2007 *Phys. Rev. Lett.* **98** 060503
[27] Zhang P, Aungskunsiri K, Martın-López E, et al. 2014 *Phys. Rev. Lett.* **112** 130501
[28] Lee C, Zhang Z, Steinbrecher G R, et al. 2014 *Phys. Rev. A* **90** 062331
[29] Sit A, Bouchard F, Fickler R, et al. 2017 *Optica* **4** 1006
[30] Ding Y, Bacco D, Dalgaard K, et al. 2017 *NPJ Quantum Inf.* **3** 25
[31] Dellantonio L, Sorensen A S, Bacco D 2018 *Phys. Rev. A* **98** 062301
[32] Deng F G, Ren B C, Li X H 2017 *Sci. Bull.* **62** 46 68
[33] Wang J D, Wei Z J, Zhang H, et al. 2010 *J. Phys. B: At. Mol. Opt. Phys.* **43** 095504
[34] Mao Q P, Wang L, Zhao S M 2019 *Laser Physics* **29** 085201
[35] Cui Z X, Zhong W, Zhou L Sheng Y B 2019 *Sci. China Phys. Mech. Astron.* **62** 110311
[36] Zhou Y H, Yu Z W, Wang X B 2016 *Physical Review A* **93** 042324
[37] Yu Z W, Zhou Y H, Wang X B 2015 *Phys. Rev. A* **91** 032318
[38] Wang Q, Wang X B 2014 *Sci. Rep.* **4** 4612
[39] Xu F, Xu H, Lo H K 2014 *Physical Review A* **89** 052333
[40] Xavier G B, Vilela de Faria G, Temporao G P, et al. 2008 *Opt. Express* **16** 1867
[41] Ding Y Y, Chen H, Wang S, et al. 2017 *Opt. Express* **25** 27923
[42] Ding Y Y, Chen W, Chen H, et al. 2017 *Opt. Lett.* **42** 1023
[43] Li D D, Gao S, Li G C, et al. 2018 *Opt. Express* **26** 22793
[44] Tang Y L, Yin H L, Zhao Q, et al. 2016 *Phys. Rev. X* **6** 011024
[45] Zhang Q, Xu F H, Chen Y A, et al. 2018 *Opt. Express* **26** 24260

A simple protocol for measuring device independent quantum key distribution based on hybrid encoding*

Du Cong [1)] Wang Jin-Dong [1)†] Qin Xiao-Juan [2)] Wei Zheng-Jun [1)]
Yu Ya-Fei [1)] Zhang Zhi-Ming [1)]

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

2) (*Engineering and Technology Department, Guangdong Polytechnic Institute, Guangzhou* 510091, *China*)

(Received 29 January 2020; revised manuscript received 2 July 2020)

Abstract

Quantum key distribution technology refers to a method to share keys between communication parties by transmitting quantum states in public channels. Although unconditional security is the main advantage of QKD, its application prospect has been controversial in practical implementation due to the potential security risks caused by device imperfections. Fortunately, the measurement device independent quantum key distribution protocol removes the vulnerability of all measurement devices and greatly improves the practical security of the quantum key distribution system. However, the security key rate of this protocol is still lower than that of other quantum key distribution protocols. At present, using high-dimensional coding to improve the performance of the quantum key distribution protocol has been proved in theory and experiment, and recently, it has been proposed to use high-dimensional coding to improve the performance of measurement device independent quantum key distribution protocol, but because these protocols have higher requirements for the laboratory equipment performance, that the high-dimensional encoding is applied to the aforementioned protocol still has many difficulties in practical application. In this paper, we propose a hybrid coding based on the polarization and two-degree phase of freedom measurement device independent quantum key distribution protocol. In the first place in an ideal case, we introduce in detail the protocol decoding rules, then introduce 4intensity decoy-state method to solve the problem of actual light source multiphoton, in addition we also consider the statistical fluctuation effect under the condition of limited code length, channel loss, actual dark count of single photon detector and detection efficiency problem. Finally, the optimal security code rate and its corresponding optimal parameters are obtained by full parameter optimization method, And the numerical simulation results show that the security key rate of this protocol is increased by 50% by considering the practical implementation. We point out that compared with other measurement device independent quantum key distribution protocol, the proposed agreement requires local users only to have a phase encoding device and a polarization coding device, and 4 single photon detectors for detecting side. The proposed device can use the existing experimental condition, beyond that, compared with the time encoding based high dimensional measurement device independent quantum key distribution protocol, the proposed protocol possesses the advantage that the rate of system security key can be increased without increasing the repetition frequency of users. It is proved that this protocol has great application value in the future field of quantum communication, especially, in the field of quantum network communication.

Keywords: quantum key distribution, measurement device independent, high dimensional encoding, hyper-encoding

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.69.20200162

* Project supported by the National Natural Science Foundation of China (Grant No. 61771205), the National Natural Science Foundation of Guangdong Province (Grant No. 2015A030313388), and the Science and Technology Projects of Guangdong Province (Grants Nos. 2015B010128012, 2017KZ010101).

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