利用 W 态实现多方设备无关量子密钥分发

Makoto Ishihara,[1], * Wojciech Roga,[1], † 和 Masahiro Takeoka[1], ‡
[1] *Department of Electronics and Electrical Engineering, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama 223-8522, Japan*（日期：2026年3月3日）

多方设备无关量子密钥分发（DI-QKD），也称为设备无关会议密钥协商，使两个以上的远程参与方能够共享一个共同密钥，即便不信任设备，也能保证信息论安全性。迄今为止，已有若干多方设备无关量子密钥分发协议被提出，其中采用格林伯格-霍恩-蔡林格（GHZ）态作为多方纠缠。由此自然引出一个问题：能否利用其他类型的多方纠缠构建多方 DI-QKD？ W 态尤其值得关注，因为它与GHZ态有本质区别，而且在某些情况下更容易通过光学方式实现。本文证明，利用 W 态也可以实现多方设备无关量子密钥分发。为此，我们构造了由 W 态大幅违反的贝尔不等式，可用于多方设备无关量子密钥分发。此外，我们还考察了若干不同的实现方案。首先，我们分析了提取有限密钥所需的最低探测效率。随后，我们提出一种采用单光子干涉的远距离多方设备无关量子密钥分发协议，并对若干物理实现方案进行了详细分析。我们表明，与现有基于 GHZ态的多方设备无关量子密钥分发协议相比，该协议能够在更长距离上实现秘密密钥分发。本研究为多方纠缠与设备无关量子信息处理之间的关系提供了新的见解，也为实现远距离多方设备无关量子密钥分发开辟了另一条途径。

arXiv:2603.00937v1 [quant-ph] 1 Mar 2026

I. 引言

量子密钥分发（QKD）是最重要的量子信息技术之一，它使两个远程参与方能够共享信息论安全的密钥 [1–4]。自Bennett和Brassard 的开创性论文发表以来 [1], , 人们提出了许多量子密钥分发协议，并在实验中进行了验证 [5, 6], , 例如，世界各地已建成用于实现量子密钥分发的测试平台 [7–14]。在量子密钥分发协议中，两个远程参与方共享密钥；而在多方量子密钥分发协议中，两个以上的参与方共享同一密钥（有时称为会议密钥协商）。与量子密钥分发一样，多方量子密钥分发已在理论上 [15–22] 和实验上 [23–25]得到广泛研究（另见参考文献 [26]）。

标准量子密钥分发或多方量子密钥分发协议的安全性依赖于这样一个假设：实现过程中所用的设备都经过了完整表征。然而，在实际场景中满足这一假设颇具挑战。为放宽这一要求，人们提出了测量设备无关协议，这类协议无需对探测器进行完整表征 [27–29]。尽管如此，这些协议仍要求用于制备量子态的设备必须经过完美表征。

设备无关量子密钥分发（DI-QKD）无需对设备的内部工作原理作出任何假设，即可保证其安全性 [30, 31]。设备无关量子密钥分发协议的安全性通过无漏洞地违反贝尔不等式来认证 [32, 33]。违反贝尔不等式可阻止窃听者 Eve 实施那些不会导致不等式被违反的窃听策略，并保证共享密钥的安全性。与标准量子密钥分发协议一样，已有研究提出了多种多方设备无关量子密钥分发协议 [34–40], , 其中采用 Greenberger-Horne-Zeilinger（GHZ）态 [41] 作为多方纠缠。

W态 [42] 是另一种多方纠缠态，其本质上不同于GHZ态。众所周知，W态在一些量子信息技术中具有优势 [43], , 例如，与GHZ态相比，W态对损耗更加稳健，而且我们可以以较高的速率在远距离分发W态 [44]。尽管利用W态研究贝尔非定域性的工作已广泛开展 [45–57], , 但W态是否适用于多方设备无关量子密钥分发协议仍是一个悬而未决的问题。基于W态实现多方设备无关量子密钥分发协议并非易事，因为与GHZ态不同，我们无法从单个W态中提取一位完全相关的密钥。换言之，即使不存在任何实验不完美性，采用W态的多方设备无关量子密钥分发协议在密钥蒸馏过程中也不可避免地会出现一定程度的密钥率降低。这使得实现基于W态的设备无关量子密钥分发颇具挑战性。

在本文中，我们对上述开放问题给出了肯定回答，即证明了可以利用 W 态构建多方设备无关量子密钥分发。为此，我们通过数值优化构造了贝尔不等式；当 W 态违反这些不等式时，Eve 对秘密密钥的不确定性很大。对于这些贝尔不等式，我们计算了多方设备无关量子密钥分发密钥率，并证明

* llmakomako.arg1076@keio.jp
† wojciech.roga@keio.jp
‡ takeoka@elec.keio.ac.jp

利用W态的多方设备无关量子密钥分发协议是可行的。随后，我们考察其实现所面临的现实条件。首先，在理想W态分发给远程参与方时，我们分析了提取有限数量密钥所需的探测效率。我们考察了两种不同的测量建模：任意泡利测量，以及由光学位移操作和后续光子探测构成的测量；二者分别适用于基于量子存储器的探测和全光学探测。此外，我们还考虑了将W态传送给远程参与方时存在信道损耗的场景。我们提出了结合参考文献 [44] 中所开发的高效 W 态分发协议的长距离多方设备无关量子密钥分发协议。我们证明，与基于本地生成 GHZ态的多方设备无关量子密钥分发协议 [34–36] 相比，采用该协议的多方设备无关量子密钥分发能够在更长距离上分发密钥。我们还考察了采用高斯态实现该协议的情况。众所周知，自发参量下转换（SPDC）产生的光学纠缠态是高斯态，因此我们研究了该协议采用全光学装置实现的可行性。

本文结构如下。第二节描述我们使用W态的多方 DI-QKD 协议。第三节介绍多方设备无关量子密钥分发密钥率，以及使用W态实现多方设备无关量子密钥分发协议的难点。第四节构造了基于W 态实现多方设备无关量子密钥分发所需的贝尔不等式。我们还计算了这些贝尔不等式的经典界限和量子界限，并表明W 态能够大幅违反这些贝尔不等式。第五节分析了获得正的多方设备无关量子密钥分发密钥率所需的探测效率。第六节将高效的W态分发协议应用于多方设备无关量子密钥分发；第七节则通过考察高斯态和测量，分析该协议在实验上的可行性。最后，第八节总结全文。

II. 协议

我们介绍使用W 态的多方 DI-QKD 协议，其示意图见图1。我们考虑一个$(N,\ m,\ d)$场景，其中 N参与方、爱丽丝和鲍勃$_i$($i \in \{1,\ldots,N-1\}$)共享一个密钥，且每个参与方有 m种不同的测量设置，每种设置有 d个结果。

首先， N 个合法参与方共享一个 N方W 态$|W_N\rangle$

$$|W_N\rangle = \frac{1}{\sqrt{N}}(|00\cdots01\rangle + |00\cdots10\rangle + \cdots + |10\cdots00\rangle), \tag{1}$$

其中， $|0\rangle$ 和 $|1\rangle$ 可以通过物理方式制备，例如分别制备水平和垂直偏振态，或真空态和单光子态。我们考虑两种不同的分发W态的方式，即直接传输和Roga-Ikuta-Horikiri-Takeoka（RIHT）协-议 [44]。在图1（a）所示的直接传输中， W 态在本地生成并分发给各参与方。另一方面，在图1（b）所示的RIHT协议中，每个参与方在本地制备一个双模式纠缠态，并将其中一部分发送至中央站。在中央站，对这些模式进行单光子干涉；若干涉测量成功，则W态便会分发给各参与方。关于RIHT协议的详细信息将在后文介绍，见第六节。

分发W 态后，参与方对W 态进行一些测量。令 $M_{a|x}$ 表示爱丽丝测量的正算子值测度（POVM），其中 $x \in \{0,\ldots,m-1\}$ 是测量输入， $a \in \{0,\ldots,d-1\}$ 是测量输出。此外，对于 $i \in \{1,\ldots,N-1\}$，令 $N_{b_i|y_i}$ 表示鲍勃$_i$的测量所对应的 POVM，其中 $y_i \in \{0,\ldots,m\}$ 是测量输入， $b_i \in \{0,\ldots,d-1\}$ 是测量输出。爱丽丝选择 $x=0$ 且鲍勃$_i$ （$i \in \{1,\ldots,N-1\}$）选择 $y_i = 0$ 的一部分事件被归类为密钥生成轮次，用于生成共同的密钥。其余事件则归类为测试轮次，用于安全性测试。令 p（$a,\ b_1,\ \ldots,\ b_{N-1}|x,\ y_1,\ \ldots,\ y_{N-1}$）表示合法参与方在测试轮次中的联合概率分布。此外，参与方执行噪声预处理 [58]。在噪声预处理中，爱丽丝以概率 p_n翻转她的密钥比特。此过程会降低爱丽丝与其他参与方之间的相关性，但也会降低爱丽丝与 Eve 之间的相关性。因此，净效应可能是正面的。最后，合法参与方执行纠错和隐私放大，共享密钥。

III. 设备无关量子密钥分发密钥率

在此，我们描述本协议的密钥率。我们重点关注渐近密钥率，并假设设备在实现过程中独立同分布地运行。本协议的多方设备无关量子密钥分发密钥率表示如下 [59]

$$r = P_{\mathrm{succ}}(H(A|x^*,E) - \max_i H(A|B_i,x^*,y_i^*)), \tag{2}$$

其中 A、 B_i 和 E 分别表示爱丽丝、鲍勃$_i$和Eve的系统， x^* 和 y_i^* 表示爱丽丝和鲍勃$_i$在密钥生成轮次中的测量输入，P_{succ} 是W 态在各参与方之间成功分发的概率。第一项是爱丽丝与Eve之间的条件冯·诺依曼熵，对应于Eve对爱丽丝测量结果的不确定性。第二项表示爱丽丝与鲍勃们之间的纠错代价。

使用W态的多方设备无关量子密钥分发协议，其实施面临的挑战在于密钥率公式（2）中的第二项。参与方可以从无噪声的 GHZ

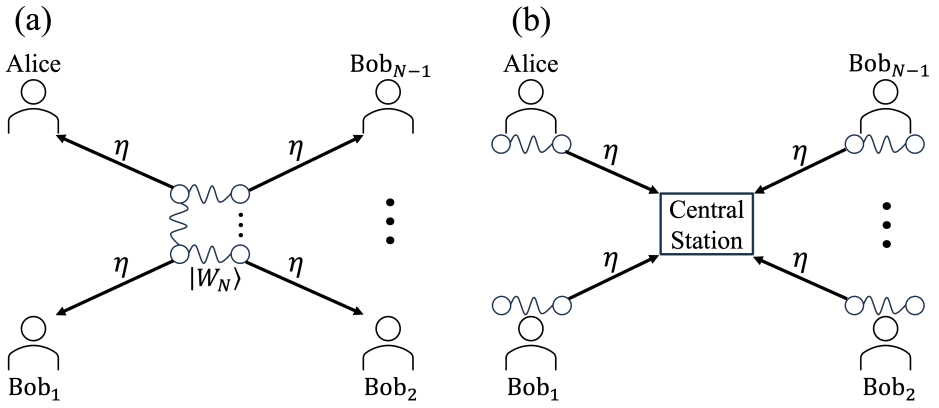

图1. 使用 W态的多方设备无关量子密钥分发示意图。 N参与方、爱丽丝和鲍勃$_i$($i \in \{1,\ldots,N-1\}$)共享一个共同的密钥。首先在各参与方之间分发一个 W态，各参与方对所分发的W态执行一些测量。各参与方根据测量结果共享一个共同的密钥。(a) 直接传输。在本地生成一个 W态，并通过透射率为 η的纯损耗信道将其分发给各参与方。(b) RIHT协议。每个参与方在本地制备一个纠缠态，并通过透射率为η的纯损耗信道将其中一部分发送至中央站。当中央站的单光子干涉成功时，各参与方之间便会分发一个 W 态。

态中提取完全相关的密钥比特，但即使状态是理想的，也无法从W 态中做到这一点。因此，使用W 态的多方设备无关量子密钥分发协议不可避免地需要纠错。具体而言，当所有参与方都对 W态执行 σ_X 测量时，纠错代价为

$$h\left(\frac{1}{2}-\frac{1}{N}\right), \tag{3}$$

其中， h是二元熵， N 是参与方 [20]的数量。

为了实现使用W态的多方设备无关量子密钥分发协议，式(2)中的第一项必须足够大，以补偿纠错代价。第一项可以通过贝尔不等式的违背程度 [33,60–63]计算。然而，据我们所知，目前尚无已知的贝尔不等式能够使第一项足够大，从而实现使用W 态的设备无关量子密钥分发协议。因此，在本研究中，我们构造了W态能够大幅违背的贝尔不等式，使得基于W态的设备无关量子密钥分发协议成为可能。

IV. 针对 W态设计的贝尔不等式

A. 构造贝尔表达式

我们构造贝尔不等式，使其在式（2）中给出足够大的条件冯·诺依曼熵。首先，贝尔不等式 $\mathcal{B}$ 通常表示为以下形式

$$\mathcal{B}=\sum_{x,\boldsymbol{y},a,\boldsymbol{b}} h_{x\boldsymbol{y}}^{a\boldsymbol{b}}\, p(a,\boldsymbol{b}|x,\boldsymbol{y}) \le L_c \le L_q, \tag{4}$$

其中， $h_{x\boldsymbol{y}}^{a\boldsymbol{b}}$ 表示一个系数， L_c 是经典极限，L_q是量子极限。为简便起见，我们记 $\boldsymbol{y}=y_1,\ldots,y_{N-1}$和 $\boldsymbol{b}=b_1,\ldots,b_{N-1}$。我们定义以下两个向量

$$\boldsymbol{h}=[h_{x\boldsymbol{y}}^{a\boldsymbol{b}}], \tag{5}$$

$$\boldsymbol{p}=[p(a,\boldsymbol{b}|x,\boldsymbol{y})], \tag{6}$$

其中 $\boldsymbol{h},\boldsymbol{p}\in\mathbb{R}^{m^N d^N}$并且我们采用如下顺序

$$\begin{aligned}\boldsymbol{p}=[&p(0,\ldots,0|0,\ldots,0),\quad \ldots,p(d,\ldots,d|0,\ldots,0),\\ &\vdots\\ &p(0,\ldots,0|m,\ldots,m),\ldots,p(d,\ldots,d|m,\ldots,m)].\end{aligned} \tag{7}$$

那么，我们可以用这些向量表示一个贝尔不等式

$$\mathcal{B}=\boldsymbol{h}^T\boldsymbol{p}\le L_c\le L_q. \tag{8}$$

我们寻找一个贝尔表达式 $\boldsymbol{h}$，使得 W 态对某个贝尔不等式产生较大的违背。为此，我们采用参考文献 [64]中提出的数值优化方法。在该方法中，我们考虑一个猜测概率优化问题 $p_{\text{guess}}(A|x^*,E)$，即 Eve 在密钥生成轮次中正确猜出爱丽丝测量结果的概率。根据其与条件最小熵 [65]的关系，猜测概率可用于给密钥率公式 (2) 中的第一项提供下界

$$\begin{aligned}H(A|x^*,E)&\ge H_{\min}(A|x^*,E)\\ &=-\log_2(p_{\text{guess}}(A|x^*,E)).\end{aligned} \tag{9}$$

令 $B(\mathcal{H})$ 表示希尔伯特空间 $\mathcal{H}$ 上有界算符的集合。那么，猜测概率对应于以下优化问题的解

$$
\begin{aligned}
p_{\text{guess}}(A|x^*,E) = \sup \quad & \sum_a \text{Tr}[\rho M_{a|x^*} Z_a] \\
\text{s.t.} \quad & \text{Tr}[\rho M_{a|x} N_{b_1|y_1} \cdots N_{b_{N-1}|y_{N-1}}] = p(a,\boldsymbol{b}|x,\boldsymbol{y}) \qquad \text{for all } a,b_i,x,y_i \\
& M_{a|x} \geq 0, \quad N_{b_i|y_i} \geq 0, \quad Z_c \geq 0 \qquad \text{for all } a,b_i,c,x,y_i \\
& \sum_a M_{a|x} = \sum_{b_i} N_{b_i|y_i} = \sum_c Z_c = I \qquad \text{for all } x,y_i \\
& \left[M_{a|x}, N_{b_i|y_i}\right] = \left[M_{a|x}, Z_c\right] = \left[N_{b_i|y_i}, Z_c\right] = 0 \qquad \text{for all } a,b_i,c,x,y_i,i
\end{aligned} \tag{10}
$$

其中，上确界取遍所有量子态 ρ以及有界算符 $M_{a|x}$、$N_{b_i|y_i}$ 和 Z_c。该优化问题对应于寻找 Eve 的最优策略，该策略在测试轮次的概率分布约束下使猜测概率最大化。

我们没有高效的方法来求解这个优化问题。因此，我们利用 Navascu´es-Pironio-Ac´ın (NPA) 层级 [66] 将该问题松弛为半定规划（SDP）。借助 NPA 层级，我们可以将这个优化问题重新表述为一个 SDP，其中优化变量是所谓的矩矩阵（见附录 A）。接下来，对于松弛后的 SDP，我们可以考虑其对偶问题 [67]。我们在附录 B 中简要说明 SDP 的对偶性。对偶问题也是 SDP，因此可以高效求解。猜测概率优化的对偶问题对应于寻找一个使猜测概率最小化的显式贝尔表达式 [64]。因此，通过提取一个对偶解，我们可以针对测试轮次中观测到的给定概率分布，找到一个最优贝尔表达式。

我们为 (3, 2, 2)、(3, 3, 2)、(4, 2, 2) 和 (5, 2, 2) 场景寻找适用于 W 态的贝尔表达式。这里，我们给出 (3, 2, 2) 场景的显式结果。定义 POVM $\Pi(\theta) = \cos\,\theta\sigma_Z + \sin\,\theta\sigma_X$。我们计算量子态 $|W_3\rangle$ 以及以下测量对应的概率分布 $p(a,\ b_1,\ b_2|x,\ y_1,\ y_2)$

$$M_{0|0} = 0.5(I + \Pi(\pi/2)), \quad M_{1|0} = I - M_{0|0}, \tag{11}$$
$$M_{0|1} = 0.5(I + \Pi(0)), \qquad M_{1|1} = I - M_{0|1}, \tag{12}$$
$$N_{0|0} = 0.5(I + \Pi(2\pi/3)) \quad N_{1|0} = I - N_{0|0}, \tag{13}$$
$$N_{0|1} = 0.5(I + \Pi(\pi/3)), \quad N_{1|1} = I - N_{0|1}. \tag{14}$$

这里，鲍勃$_1$ 和鲍勃$_2$ 执行相同的测量，并且 I 是恒等算符。于是，我们得到以下贝尔

表 I. 在(3，2，2)，(3，3，2)，(4，2，2)和(5，2，2)场景中，式(2)第一项、第二项和密钥率的值。

场景	$H(A\|x^*,\ E)$	最大值$_i$ $H(A\|B_i,\ x^*,\ y_i^*)$	r
(3, 2, 2)	0.998	0.650	0.348
(3, 3, 2)	0.999	0.650	0.349
(4, 2, 2)	0.999	0.811	0.188
(5, 2, 2)	0.999	0.881	0.118

表达式 $\boldsymbol{h}$

$$
\begin{bmatrix}
-291.223, & 159.065, & 159.065, & -144.647, \\
1146.316, & -701.375, & -701.375, & 1235.672, \\
149.171, & -270.272, & -180.496, & 197.614, \\
80.769, & -56.324, & -54.657, & 78.917, \\
149.171, & -180.496, & -270.272, & 197.614, \\
80.769, & -54.657, & -56.324, & 78.917, \\
1288.666, & -2489.561, & -2489.561, & 933.615, \\
-128.785, & 167.864, & 167.864, & -133.405, \\
37.170, & -55.645, & -55.645, & -28.406, \\
37.801, & -49.508, & -49.508, & 234.402, \\
241.203, & -299.824, & -1103.213, & 253.583, \\
35.804, & -47.550, & 58.961, & 55.206, \\
241.203, & -1103.213, & -299.824, & 253.583, \\
35.804, & 58.961, & -47.550, & 55.206, \\
-23.943, & -66.800, & -66.800, & 52.173, \\
248.758, & -75.853, & -75.853, & 84.785].
\end{bmatrix} \tag{15}
$$

我们计算了该贝尔表达式在 (2) 中的第一项，得到条件熵为 0.998。假设每一方在密钥生成轮次中都进行 σ_X 测量，则与 (2) 中第二项相对应的纠错代价为 0.650。因此，该贝尔表达式实现了适用于 (3，2，2) 场景的多方设备无关量子密钥分发协议。我们还在表 I 中给出了其他场景的结果。可以看出，在这些场景下，采用 W 态的多方设备无关量子密钥分发协议是可行的。

B. 计算经典极限和量子极限

上述方法给出了一个贝尔表达式 $\boldsymbol{h}$，但没有给出与该贝尔表达式对应的贝尔不等式的经典界限和量子界限。在这里，我们计算所找到的贝尔表达式对应的这些界限。

首先，我们说明如何计算经典极限 L_c。定义以下向量 $\boldsymbol{v}_k \in \mathbb{R}^{m^N d^N}$，其中（$k \in \{1,2,\ldots,d^{Nm}\}$）对应于经典关联多面体 [68] 的极点。记 $k =$（a_1、.....、a_m、b_1^1、.....、b_m^1、.....、b_1^{N-1}、.....、b_m^{N-1}），其中 a_x 表示爱丽丝选择输入 x 时的测量输出，而 $b_{y_i}^i$ 表示鲍勃选择输入 y_i 时的测量输出，$_i$ 对于 $i \in \{1,\ldots,N-1\}$。于是，$\boldsymbol{v}_k$ 的各项可表示如下

$$v_k(a,\boldsymbol{b}|x,\boldsymbol{y}) = \begin{cases} 1 & \text{if } a = a_x \text{ and } b_i = b_{y_i}^i \text{ for all } i, \\ 0 & \text{otherwise.} \end{cases} \tag{16}$$

接着，经典关联 $\mathbf{P}_{\text{cl}}$ 可表示为这些向量的线性组合

$$\mathbf{P}_{\text{cl}} = \sum_{k=1}^{d^{Nm}} \lambda_k \boldsymbol{v}_k, \tag{17}$$

其中 $\lambda_k \geq 0$ 和 $\sum \lambda_k = 1$。对于给定的贝尔表达式 $\boldsymbol{h}^T\boldsymbol{p}$，我们可以通过以下线性规划计算其经典极限

$$\begin{aligned} \min_{L_c} \quad & L_c \\ \text{s.t.} \quad & \boldsymbol{h}^T\boldsymbol{v}_k \leq L_c \quad \text{for all } k. \end{aligned} \tag{18}$$

该问题的一个解对应于贝尔不等式的经典极限

$$\mathcal{B} = \boldsymbol{h}^T\boldsymbol{p} \leq L_c. \tag{19}$$

接下来，我们介绍如何计算贝尔表达式的量子极限 L_q。贝尔表达式$\boldsymbol{h}^T\boldsymbol{p} = \sum_{x,\boldsymbol{y},a,\boldsymbol{b}} h_{x\boldsymbol{y}}^{a\boldsymbol{b}} p(a,\boldsymbol{b}|x,\boldsymbol{y})$ 的量子极限对应于以下问题的一个解

$$\begin{aligned} \max \quad & \sum_{x,\boldsymbol{y},a,\boldsymbol{b}} h_{x\boldsymbol{y}}^{a\boldsymbol{b}} \text{Tr}[\rho M_{a|x} N_{b_1|y_1} \cdots N_{b_{N-1}|y_{N-1}}] \\ \text{s.t.} \quad & \sum_a M_{a|x} = \sum_{b_i} N_{b_i|y_i} = I \quad \text{for all } x, y_i \\ & M_{a|x} \geq 0, \quad N_{b_i|y_i} \geq 0 \quad \text{for all } a, b_i, x, y_i \\ & \left[M_{a|x}, N_{b_i|y_i}\right] = 0 \quad \text{for all } a, b_i, x, y_i \\ & M_{a|x}, N_{b_i|y_i} \in B(\mathcal{H}) \quad \text{for all } a, b_i, x, y_i \end{aligned} \tag{20}$$

其中，最大值是在所有量子态ρ和算符 $M_{a|x}$、$N_{b_1|y_1}$、.....、$N_{b_{N-1}|y_{N-1}}$上取的。由于该优化问题的目标函数可以表示为矩矩阵各元素的线性组合，因此我们可以利用

表 II. 对于我们在 (3, 2, 2), (3,3,2), (4,2, 2) 和 (5, 2, 2) 场景中找到的贝尔表达式，经典极限为 L_c，使用 W 个态时的违背量为 L_W，量子极限为 L_q。

场景	L_c	L_W	L_q
(3, 2, 2)	1791.419	1794.3624230	1794.3624540
(3, 3, 2)	1713.456	1831.4136783	1831.4136786
(4, 2, 2)	1476.978	1514.9137399	1514.9137408
(5, 2, 2)	2409.119	2441.8495037	2441.8495040

NPA层级。我们在表II中展示了所找到的贝尔表达式的经典极限和量子极限的计算结果。此外，我们还展示了这些贝尔表达式在W 态 L_W下的最大违反程度。可以看到，在所有场景中，W 态 L_W 下的最大贝尔值 L_q几乎与量子极限重合。然而，在所有场景中，L_q 略高于 L_W。这可能是因为NPA层级的级数有限。我们在这些计算中采用了第三级NPA层级。因此，如果考虑无限级的NPA层级，贝尔表达式的 L_q 可能会与 L_W重合。对这些贝尔不等式的量子极限进行解析分析，是未来一项有趣的工作。

V. 分析所需探测效率

本节中，我们考虑探测效率不完美的现实探测器，并分析采用W 态的多方设备无关量子密钥分发协议所需的最低探测效率。如果不存在实验不完美性，上一节使用的猜测概率方法效果相当不错。然而，我们发现该方法极易受到各种不完美因素的影响，包括有限的探测效率。因此，本节采用另一种方法来计算密钥率，即基于参考文献 [63] 中提出的准相对熵进行数值优化。这里，我们考虑一个 N 方W 态通过直接传输进行分发的情形，其中W 态在某处本地产生，随后分发给各参与方（图1(a)）。我们假设W态的生成成功概率为 1，即 $P_{\text{succ}} = 1$，并且该态无传输损耗和噪声地被各参与方共享（即图1(a)中的 $\eta = 1$）。我们仅考虑非单位探测效率这一不完美因素。

A. 测量建模

首先，我们来说明如何对探测效率进行建模。我们考虑每一方有两种测量设置、每种设置有两个结果的场景，即（N, 2, 2）场景。对于 $i \in \{1,\ldots,N-1\}$，我们定义相应于

爱丽丝和鲍勃$_i$的测量的 POVM，如下所示

$$M_{0|x} = 0.5\eta_e(I + \Pi(\theta_x^A)),\ M_{1|x} = I - M_{0|x}, \quad (21)$$
$$N_{0|y_i} = 0.5\eta_e(I + \Pi(\theta_{y_i}^{B_i})), N_{1|y_i} = I - N_{0|y_i}, \quad (22)$$

其中，η_e 对应于探测效率，$\Pi(\theta) = \cos\theta\sigma_Z + \sin\theta\sigma_X$。我们通过数值优化参数 $\theta_x^A, \theta_{y_1}^{B_1}, \ldots, \theta_{y_{N-1}}^{B_{N-1}}$以最大化密钥率。此外，我们还考虑另一种测量模型，以分析使用 W 态的多方设备无关量子密钥分发协议在实验上的可行性。一种实用的W 态制备方法是用多个分束器分束单光子。由于以这种方式制备的W 态是在光子数基中编码的，其测量也应在同一基中进行。尽管原则上可以在该基中实现任意泡利测量 [69] ，且其原理验证已得到展示 [70]，但要以接近完美的效率实现仍不容易。因此，我们考虑其近似版本，即先进行光学位移操作，再进行光子探测。这种测量可表示为

$$\{|\alpha\rangle\langle\alpha|, I - |\alpha\rangle\langle\alpha|\}, \quad (23)$$

其中 $|\alpha\rangle$ 是一个相干态

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle . \quad (24)$$

尽管参考文献 [57], 分析了使用这种测量和W 态时贝尔不等式的违背，但作者并未考虑多方设备无关量子密钥分发协议。在此，我们将探测效率 η_e 建模为位移操作之前透射率为 η_e 的纯损耗信道，因为我们可以通过增大振幅来补偿光子探测器中的任何损耗。经过透射率为 η_e 的纯损耗信道传输后，一个 N 方 W 态 $|W_N\rangle$ 变为

$$|W_N\rangle\langle W_N| \to \eta_e |W_N\rangle\langle W_N| + (1-\eta_e)|0_N\rangle\langle 0_N| . \quad (25)$$

$|0_N\rangle$ 表示一个量子态，其中所有 N 模式均为真空态。

B. 密钥率计算

在该方法中，我们可以通过求解以下优化问题 [63], 得到(2)中条件冯·诺依曼熵的下界

$$\begin{aligned}
c_m + \inf \quad & \sum_{i=1}^{m-1} \frac{w_i}{t_i \ln 2} \sum_{a=0}^{1} \mathrm{Tr}[\rho \hat{M}_{a|x^*}(Z_{a,i} + Z_{a,i}^* + (1-t_i)Z_{a,i}^* Z_{a,i}) + t_i Z_{a,i} Z_{a,i}^*] \\
\text{s.t.} \quad & \mathrm{Tr}[\rho M_{a|x} N_{b_1|y_1} \cdots N_{b_{N-1}|y_{N-1}}] = p(a, \boldsymbol{b}|x, \boldsymbol{y}) \qquad \text{for all } a, b_i, x, y_i \\
& \sum_a M_{a|x} = \sum_{b_i} N_{b_i|y_i} = I \qquad \text{for all } x, y_i \\
& M_{a|x} \geq 0, \quad N_{b_i|y_i} \geq 0 \qquad \text{for all } a, b_i, x, y_i \\
& Z_{c,i}^* Z_{c,i} \leq \alpha_i^2, \quad Z_{c,i} Z_{c,i}^* \leq \alpha_i^2 \qquad \text{for all } c, i \\
& \left[M_{a|x}, N_{b_i|y_i}\right] = \left[M_{a|x}, Z_{c,i}^{(*)}\right] = \left[N_{b_i|y_i}, Z_{c,i}^{(*)}\right] = 0 \qquad \text{for all } a, b_i, c, x, y_i, i \\
& M_{a|x}, N_{b_i|y_i}, Z_{c,i} \in B(\mathcal{H}) \qquad \text{for all } a, b_i, c, x, y_i, i
\end{aligned} \quad (26)$$

其中下确界取遍所有量子态 ρ以及有界算符 $M_{a|x}$、$N_{b_i|y_i}$和$Z_{c,i}$、$t_1, \ldots, t_m$和 $w_1, \ldots, w_m$是 $[0,1]$ 上的 m 点高斯-拉道求积的节点与权重，端点为 $t_m = 1$，$M_{a|x^*} = (1-p_n)M_{a|x^*} + p_n M_{a\oplus 1|x^*}$，$c_m = \frac{2p_n(1-p_n)}{m^2 \ln 2} + \sum_{i=1}^{m-1} \frac{w_i}{t_i \ln 2}$，$\alpha_i = \frac{3}{2}\max\{\frac{1}{t_i}, \frac{1}{1-t_i}\}$和$p(a, \boldsymbol{b}|x, \boldsymbol{y})$是测试轮次的观测概率分布。该优化问题也可利用NPA层级松弛为半定规划。

C. 结果

我们展示对所需探测效率进行分析的结果。在此，我们固定高斯–拉杜求积的节点数 $m = 8$，并通过数值优化测量设置以及爱丽丝翻转其密钥比特的概率 p_n，以最大化密钥率。

首先，我们展示每个参与方均可对W态进行任意泡利测量时的结果，见图2。蓝色圆圈表示(3, 2, 2)场景的密钥率，红色三角形表示(4, 2, 2)场景的密钥率。

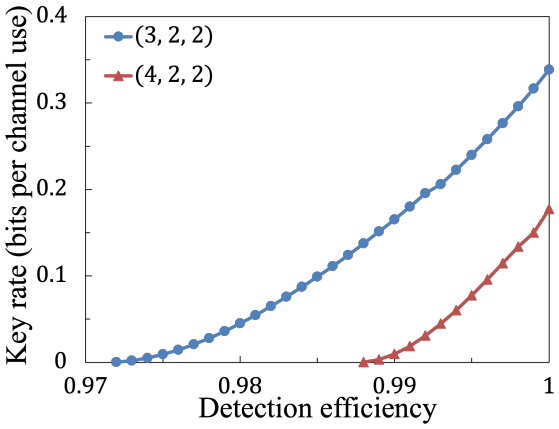

图2. 合法参与方进行任意泡利测量时，(3, 2, 2)场景和(4, 2, 2)场景的密钥率随探测效率的变化。蓝色圆点表示(3, 2, 2)场景的密钥率，红色三角形表示(4, 2, 2)场景的密钥率。我们通过数值优化测量参数 θ_x^A，$\theta_{y_1}^{B_1}$、……、$\theta_{y_{N-1}}^{B_{N-1}}$以及概率 p_n，使密钥率最大化。

我们发现，生成密钥所需的最低探测效率在设置(3, 2,2)和(4, 2, 2)下分别为97.2%和98.8%。密钥生成轮次的最优测量接近泡利 σ_X 测量。 N越高，所需的探测效率就越高。对此可作如下解释。如果仅考虑纠错代价，且参与方数量 N 足够大，则密钥生成轮次的最优测量是泡利 σ_Z测量，因为几乎所有参与方都能获得相同的测量结果“0”。然而，这意味着窃听者很容易猜出爱丽丝的测量结果，从而使条件熵 $H(A|x^*,E)$变小。因此，若考虑对密钥率的净效应，泡利 σ_X 测量是最优的，因为我们能得到较大的条件冯·诺依曼熵取值。当每个参与方在密钥生成轮次中执行 σ_X 测量时，纠错代价为 $h($ $1/2-1/N)$，并且该代价随参与方数量的增加而增大。于是，参与方数量越多，所需的探测效率就越高。虽然用全光学装置实现超过97%的探测效率相当具有挑战性，但我们可以借助基于物质的系统 [71–73]实现如此高的探测效率。

在图 3 中，我们展示了远程参与方执行基于位移的测量时，(3，2，2) 和 (4，2，2) 场景下的密钥率。蓝色圆点和红色三角形分别表示 (3，2，2) 和 (4，2，2) 场景的密钥率。我们发现，(3，2，2) 场景所需的最低探测效率为 99.5 %，而 (4，2，2) 场景所需的最低探测效率为 99.96 %。这些数值高于参与方能够执行任意泡利测量时的数值，因为使用位移算符时，我们无法执行此类任意测量。

子和光子探测器。

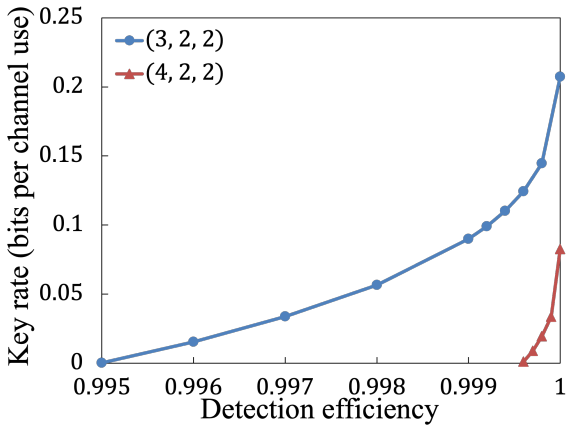

图3. 合法参与方进行基于位移的测量时，(3, 2, 2)场景和(4, 2, 2)场景的密钥率随探测效率的变化。蓝色圆点表示(3, 2, 2)场景的密钥率，红色三角形表示(4, 2, 2)场景的密钥率。我们通过数值优化所有合法参与方的位移 α 以及概率p_n，使密钥率最大化。

VI. 基于 W 态的长距离多方设备无关量子密钥分发

到目前为止，我们考虑 N 个参与方通过直接传输共享一个 W 态，也就是说，一个 N 方 W 态在中央站本地制备后分发给各参与方。然而，如果中央站与各参与方之间的信道损耗为 η，W 态的分发率会按 $O(\eta^N)$ 缩放，随参与方数量增加而呈指数下降。最近，我们在文献 [44] 中提出了高效分发 W 态的方案。我们称之为RIHT协议。通过该协议，参与方可以共享一个 N 方 W 态，其分发率为 $O(\eta)$。因此，本节中我们考虑采用RIHT协议的多方设备无关量子密钥分发协议。

RIHT协议的示意图如图4所示。与直接传输相同，我们考虑一个(N,m,d)场景，其中 N 个参与方共享一个共同密钥，且每个参与方具有 m 种不同的测量设置，每种设置有 d个结果。首先，每个参与方制备一个由两个模式 X 和 X'组成的纠缠态，

$$\sqrt{q}\,|00\rangle_{XX'}+\sqrt{1-q}\,|11\rangle_{XX'}, \tag{27}$$

其中，$q\approx 1$ 是一个可自由选择的参数，模式X 保留在各参与方所在位置，模式 X' 则发送至中央站。随后，各参与方通过透射率为 η的纯损耗信道，将模式 X'传送至中央站。中央站由一个干涉仪 U、50:50分束器以及 N 个暗计数概率为 p_d的单光子探测器组成。当

$N = 2^n$时，干涉仪 U 的一种操作可表示为

$$U = u^{\otimes n}, \tag{28}$$

其中

$$u = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}. \tag{29}$$

当其中一个 N 单光子探测器探测到一个光子时， N方 W态 $|W_N\rangle$便分布在各参与方之间。我们称此类事件为成功事件。这是单光子干涉的多体扩展，单光子干涉广泛应用于双场量子密钥分发等量子密钥分发协议中 [29]。发生成功事件时，各参与方以与直接传输相同的方式，对分布的W态进行测量。此外，在密钥生成轮次中，爱丽丝以 p_n的概率翻转她的比特。最后，各参与方执行纠错和隐私放大，并像在直接传输场景中那样提取出一条共同的密钥。我们在附录C中计算了 $N = 3$,4方分布式 W 态的显式表达式。

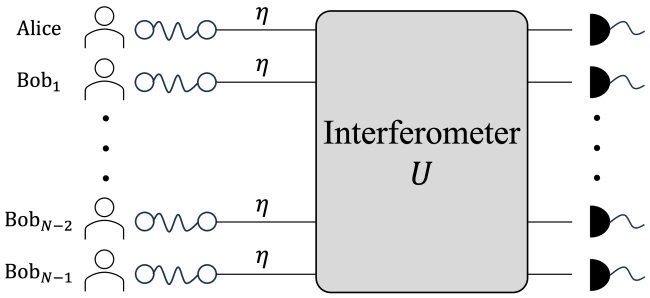

图4. RIHT协议示意图。每个参与方制备一个双模纠缠态 $\sqrt{q}\,|00\rangle + \sqrt{1-q}\,|11\rangle$，并通过透射率为 η的纯损耗信道将其中一部分传输至中央站。中央站由一个带有50:50分束器的干涉仪 U 和 N 个单光子探测器组成。各参与方从仅有一个单光子探测器探测到一个光子的事件中提取密钥。

我们可以像直接传输的情况一样计算该协议的密钥率。我们假设所有参与方都以单位探测效率执行由式（21）表示的任意泡利测量 $\eta_e = 1$。在实验中，我们可以利用物质量子比特实现此类测量。我们对参与方的测量参数和概率 p_n 进行数值优化，以最大化密钥率。

A. 结果

在图 5 和图 6 中，我们分别展示了 (3, 2, 2)场景和 (4, 2, 2)场景下，当式（27）中的参数 q 取不同值时的密钥率。我们绘制了密钥率随各参与方与中心之间距离的变化中央站 L 处的距离（单位为千米）与透射率 η 之间的关系为 $\eta = 10^{-0.02L}$ ，对应于损耗为 0.2 dB/km 的标准光纤。我们将中央站处单光子探测器的暗计数概率固定为 $p_d = 10^{-6}$。我们还绘出了基于 GHZ态的多方设备无关量子密钥分发协议的密钥率；在该协议中，GHZ态在本地生成并分发给合法参与方，密钥率根据违反奇偶CHSH不等式的程度计算 [34–36]。可以看出，RIHT协议的密钥率优于基于 GHZ态的协议。GHZ协议只能在几千米范围内分发密钥，而我们的协议可实现超过 100 千米的传输距离。这是因为利用单光子干涉，我们可以有效地将信道损耗的影响视为 W 态的概率性生成。此外，我们发现密钥率会随参数 q显著变化。当 q 较小时，合法参与方可以共享保真度较高的 W 态，因为较小的 q 意味着每个参与方向中央站发送单光子的概率较低。由于多光子事件（即多个参与方发送光子，而只有一个光子到达中央站），分发的 W 态保真度会降低。尽管这些事件被归类为成功事件，但分发的状态并非所需的 W 态。当 q 较大时，此类多光子事件的影响很大，我们无法远距离分发密钥。然而，较大的 q 意味着我们能够获得较高的成功概率，因此与 q 较小时相比，短距离下的密钥率更高。与直接传输协议相同，参与方数量 N 增加时，密钥率会降低。

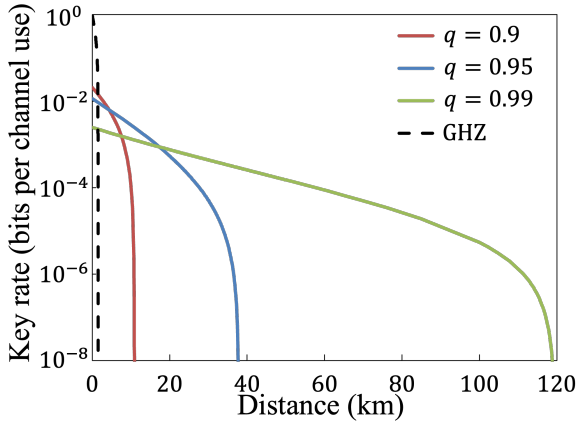

图 5. 在 (3, 2, 2)场景下，使用 RIHT协议时密钥率随距离 L的变化，其中展示了各参与方制备的纠缠态参数 q 取不同值时的结果。我们采用探测效率 $\eta_e = 1$ 和暗计数概率 $p_d = 10^{-6}$。黑色虚线表示采用本地产生的 GHZ态的多方设备无关量子密钥分发协议的密钥率。

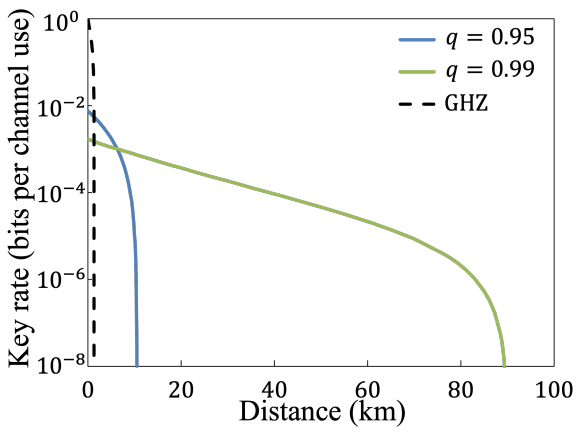

图6. RIHT协议的密钥率随距离 L的变化，针对场景 (4, 2, 2) 展示纠缠态中不同参数值 q 时的结果，其中各方制备该纠缠态。我们采用探测效率 $\eta_e = 1$ 和暗计数概率 $p_d = 10^{-6}$。黑色虚线表示采用本地产生的 GHZ态的多方设备无关量子密钥分发协议的密钥率。

VII. 使用高斯形式的 W 态进行长距离设备无关量子密钥分发

本节中，我们研究 RIHT协议在全光学装置中的可行性。在全光学装置中，广泛使用自发参量下转换过程，该过程会生成称为双模压缩真空态（TMSV）的纠缠态。TMSV属于高斯态范畴，本节将高斯形式及其详细分析总结于附录E中。这里，我们考虑一种与上一节协议等效的方案，唯一不同之处在于，每个参与方制备平均光子数为 $\bar{n}$ 的 TMSV，而非式（27）中的量子比特纠缠态，并执行基于位移的测量，而非任意泡利测量。此外，中央站的探测器现在为开关探测器，只能区分零个光子与一个或多个光子。

由于分束器的操作是一种高斯操作，经过信道传输和干涉仪 U 操作后的量子态是高斯态，也就是说，它完全由位移向量和协方差矩阵表征。开关型探测器的测量算符表示为

$$\{(1-p_d)\left|0\right\rangle\!\left\langle 0\right|, I-(1-p_d)\left|0\right\rangle\!\left\langle 0\right|\}, \tag{30}$$

其中， p_d 表示暗计数概率。接着，将中央站 $\rho_{\boldsymbol{X}\boldsymbol{X}'}$ 处探测前的量子态记为 $\boldsymbol{X}$ ，其中表示由参与方测量的模式； $\boldsymbol{X}'$ 表示发送至中央站的模式，则探测后的未归一化量子态可表示如下

$$\begin{aligned}\tilde{\sigma}_{\boldsymbol{X}} = \mathrm{Tr}[\rho_{\boldsymbol{X}\boldsymbol{X}'}\{&(1-p_d)^{N-1}\left|0\cdots0\right\rangle\!\left\langle 0\cdots0\right|_{\boldsymbol{X}'/D_1} \\ &-(1-p_d)^{N}\left|0\cdots0\right\rangle\!\left\langle 0\cdots0\right|_{\boldsymbol{X}'}\}],\end{aligned} \tag{31}$$

其中， $\left|0\right\rangle$ 表示真空态， $\boldsymbol{X}'/D_1$ 表示除模式 D_1 以外的所有模式，而在模式 D_1 处，开关型探测器会产生点击。成功概率 P_{succ} 可表示为该量子态的迹

$$P_{\mathrm{succ}} = \mathrm{Tr}[\tilde{\sigma}_{\boldsymbol{X}}]. \tag{32}$$

对量子态 σ 进行归一化 $\tilde{\sigma}$后，我们可以计算概率分布 $p(a, \boldsymbol{b}|x, \boldsymbol{y})$。利用该概率分布，我们可以计算此协议的密钥率。关于此协议概率分布的显式计算，请参见附录E。

图 7 展示了该协议的密钥率计算结果。我们考虑 (3，2，2) 场景，以及双模压缩态的平均光子数 $\bar{n} = 0.01$。蓝色实线表示采用高斯态和测量的 RIHT 协议的密钥率，黑色虚线表示基于 GHZ态的协议的密钥率，其中理想 GHZ态通过直接传输进行分发。我们发现，即使使用实验上可行的态和测量，RIHT 协议实现的传输距离也比基于理想 GHZ态的协议更长。

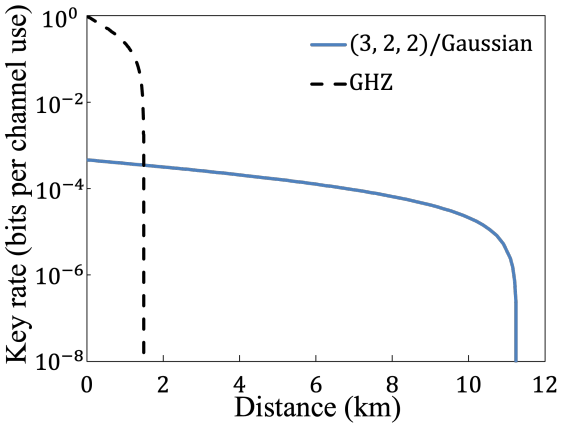

图 7. 采用 RIHT 协议时，(3, 2, 2) 设置下密钥率随距离的变化 L，使用高斯态和测量。我们采用探测效率 $\eta_e = 1$ 和暗计数概率 $p_d = 10^{-6}$。黑色虚线表示采用 GHZ态的多方设备无关量子密钥分发协议的密钥率。

VIII. 结论

本文从理论上证明，可以利用 W 态构建多方设备无关量子密钥分发。我们通过数值方法构造了 W 态能够大幅违反的贝尔不等式。利用这些贝尔不等式，我们构建了一种多方设备无关量子密钥分发协议，并证明可以从 W态中提取设备无关秘密密钥。我们还讨论了实际情形。首先，在 W态理想分发的情况下，我们分析了基于 W态的设备无关量子密钥分发协议所需的探测效率。此外，我们还考虑了信道损耗对

W 态分发的影响。我们提出采用 RIHT 协议，通过有损信道高效分发 W态，并证明即使采用实验上可行的实现方式，该协议也能达到比基于 GHZ态的多方设备无关量子密钥分发协议更远的距离。我们的结果揭示了 W 态在设备无关量子密钥分发中的潜力。i

这项研究有几个值得探讨的方向。本文通过数值计算表明，我们的贝尔不等式的量子界限几乎可以由 W 态达到。从基础理论的角度看，一个重要方向是对这一结果进行解析证明，这将使我们更深入地理解 W 态与贝尔不等式之间的关系。在实际应用方面，改进基于 W态的多方设备无关量子密钥分发，或应用其他多方纠缠态（如 Dicke态和 $N00N$ 态），也是值得探索的未来研究方向。

致谢

本研究得到 JST SPRING（资助编号：JPMJSP2123）、JST Moonshot R&D（资助编号：JPMJMS226C 和 JPMJMS2061）、JST CRONOS（资助编号：JPMJCS24N6）、JST ASPIRE（资助编号：JPMJAP2427）以及 JST COI-NEXT（资助编号：JPMJPF2221）的支持。

附录 A：NPA层级

下面我们来介绍 NPA层级。本文使用 NPA层级计算式 (2) 中的条件冯·诺依曼熵以及贝尔不等式的量子界限。完整说明请参见原论文 [66]。

首先，我们构造一个优化问题，随后使用NPA层级将其松弛为半定规划。令 $\mathcal{H}$ 表示一个希尔伯特空间， ρ 为定义在 $\mathcal{H}$上的量子态。我们在同一希尔伯特空间 $\mathcal{O}$上定义一组算符。此外，我们考虑这组算符的期望值 $\left\langle O_i^\dagger O_j \right\rangle = \mathrm{Tr}[\rho O_i^\dagger O_j]$，其中 $O_i \in \mathcal{O}$。我们考虑一个优化问题：在所有量子态ρ 和算符 O_i上，最小化这些期望值的线性组合。式（10）、（20）和（26）中的优化问题的目标函数均以这种方式表示。由于我们要在希尔伯特空间维数不受任何约束的情况下，对所有量子态和算符进行优化，因此该优化问题无法直接求解。随后，我们使用NPA层级将该优化问题松弛为可高效求解的半定规划。在NPA层级的第 k级，我们从一组算符中选取 l 个算符，该组算符由爱丽丝的测量算符、鲍勃们的测量算符、Eve的测量算符以及 $1 \le l \le k$的恒等算符组成。随后，我们考虑由 l 这些算符构成的乘积集合 $\mathcal{O}_k$。我们构造一个 k阶矩矩阵 $\Gamma^{(k)}$ ，其元素为 $\Gamma^{(k)}_{ij} = \left\langle (O_i^{(k)})^\dagger O_j^{(k)} \right\rangle$ ，其中 $O_i^{(k)} \in \mathcal{O}_k$。已知以这种方式构造的矩矩阵是半正定的。此外，优化问题的目标函数可表示为矩矩阵元素的线性组合。因此，该优化问题被视为一个以矩矩阵为变量的半定规划。需要注意的是， k阶矩矩阵不一定对应原优化问题的可行点，并且NPA层级第 k级中的优化范围比原优化问题的优化范围更广。然而，在 $k \to \infty$的极限下，已知这些优化问题的最优值会重合。我们使用NCPOL2SDPA [74]执行NPA层级，并使用MOSEK [75]求解半定规划。

附录 B：半定规划对偶性

我们介绍半定规划的对偶性 [67]。考虑以下半定规划：

$$\begin{aligned} \min_X \quad & \mathrm{Tr}[CX] \\ \text{s.t.} \quad & \mathrm{Tr}[A_i X] = b_i \quad (i = 1, \dots, m) \\ & X \ge 0 \end{aligned} \tag{B1}$$

其中， C和 A_i是 $n \times n$矩阵， $b \in \mathbb{R}^m$ 是约束向量；我们对所有半正定矩阵 X进行最小化。我们将这一优化称为原问题。可以按如下方式构造与原问题对应的对偶问题：

$$\begin{aligned} \max_{y,Z} \quad & \sum_{i=1}^m y_i b_i \\ \text{s.t.} \quad & C - \sum_i y_i A_i - Z = 0 \\ & Z \ge 0 \end{aligned} \tag{B2}$$

其中，我们对所有向量 y 和半正定矩阵 Z进行最大化。

原问题与对偶问题之间存在一个重要关系，即以下不等式成立

$$\mathrm{Tr}[CX] \ge \sum_{i=1}^m y_i b_i. \tag{B3}$$

换言之，原问题的最优值不小于对偶问题的最优值。这个不等式的推导如下。

$$\begin{aligned} \mathrm{Tr}[CX] - \sum_i b_i y_i &= \mathrm{Tr}[(\sum_i y_i A_i + Z)X] - \sum_i b_i y_i \\ &= \sum_i b_i y_i + \mathrm{Tr}[ZX] - \sum_i b_i y_i \\ &= \mathrm{Tr}[ZX] \\ &\ge 0 \end{aligned} \tag{B4}$$

这里，该不等式成立是因为当A 和 B 均为半正定时，Tr $[AB] \geq 0$ 。

附录C：RIHT协议的状态计算

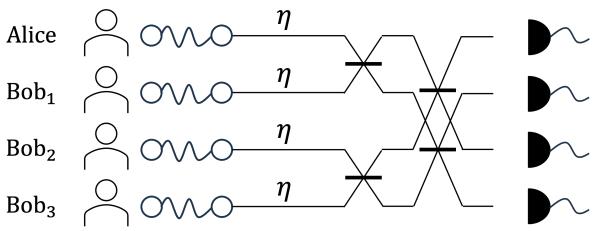

图 8. RIHT协议示意图，其中 $N = 4$。每位参与方制备一个双模纠缠态 $\sqrt{q}\,|00\rangle + \sqrt{1-q}\,|11\rangle$，并通过透射率为 $\bar{\eta}$ 的纯损耗信道将其中一部分传送至中央站。中央站由一个包含四个50:50分束器和四个单光子探测器的干涉仪组成。参与方从仅有一个单光子探测器探测到单光子的事件中提取密钥。

我们计算了 RIHT协议中成功事件发生时参与方共享的联合量子态。这里，我们为图 8 中的 $N = 4$ 提供论证。

首先，每位参与方制备如下形式的纠缠态

$$\sqrt{q}\,|00\rangle_{XX'} + \sqrt{1-q}\,|11\rangle_{XX'}\,, \tag{C1}$$

其中，模式 X 保留在每位参与方所在的位置，而模式 X' 被发送至中央站。经过信道传输后，量子态变为如下形式

$$|S\rangle_{XE}\,|1\rangle_{X'} + |V\rangle_{XE}\,|0\rangle_{X'}\,, \tag{C2}$$

其中

$$\begin{aligned} |S\rangle &= \sqrt{1-q}\sqrt{\eta}\,|10\rangle_{XE}\,, \\ |V\rangle &= \sqrt{q}\,|00\rangle_{XE} + \sqrt{1-q}\sqrt{1-\eta}\,|11\rangle_{XE}\,. \end{aligned} \tag{C3}$$

这里， E 表示与信道传输对应的环境系统， $|S\rangle$对应于向干涉仪输入单光子的状态 U ，而 $|V\rangle$对应于输入真空态的状态。

接下来，我们关注中央站的操作。对于 $N = 4$, 干涉仪的操作可以表示为

$$\begin{aligned} U &= u^{\otimes 2} \\ &= \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \end{aligned} \tag{C4}$$

令 D_1, D_2, D_3 和 D_4 表示中央站的四个单光子探测器。我们将单光子探测器 D_1 探测到一个单光子的事件称为成功事件。对于其他单光子探测器探测到一个单光子的情形，我们可以采用相同的分析。单光子探测器的测量操作可以表示为

$$\{(1-p_d)\,|0\rangle\langle 0|\,, |1\rangle\langle 1| + p_d\,|0\rangle\langle 0|\}. \tag{C5}$$

这里，我们假设单光子探测器能够分辨光子数，并丢弃有两个或更多光子到达同一探测器的事件。于是，仅当单光子探测器 D_1 探测到一个单光子时，其测量操作为

$$\begin{aligned} &(|1\rangle\langle 1| + p_d\,|0\rangle\langle 0|)_{D_1}((1-p_d)\,|0\rangle\langle 0|)_{D_2} \\ &\otimes((1-p_d)\,|0\rangle\langle 0|)_{D_3}((1-p_d)\,|0\rangle\langle 0|)_{D_4} \\ =&(1-p_d)^3\,|1000\rangle\langle 1000| + p_d(1-p_d)^3\,|0000\rangle\langle 0000|\,. \end{aligned} \tag{C6}$$

我们可以看到有两种测量模式：第一项对应于未发生暗计数的事件，第二项对应于在 D_1处发生暗计数的事件。令 $|\phi_1\rangle$和 $|\phi_2\rangle$ 分别表示第一种和第二种模式发生时分发的量子态。根据干涉仪的变换矩阵（C4），我们可以将这两种量子态明确表示如下

$$\begin{aligned} |\phi_1\rangle = \frac{1}{2}&(|SVVV\rangle + |VSVV\rangle \\ &+ |VVSV\rangle + |VVVS\rangle)_{\boldsymbol{X}}, \end{aligned} \tag{C7}$$

$$|\phi_2\rangle = |VVVV\rangle_{\boldsymbol{X}}\,. \tag{C8}$$

于是，参与方 ρ 之间的联合量子态如下

$$\rho = \frac{1}{P}((1-p_d)^3\,|\phi_1\rangle\langle\phi_1| + p_d(1-p_d)^3\,|\phi_2\rangle\langle\phi_2|), \tag{C9}$$

其中

$$P = P_1 + P_2 \tag{C10}$$

$$P_1 = \mathrm{Tr}[(1-p_d)^3\,|\phi_1\rangle\langle\phi_1|], \tag{C11}$$

$$P_2 = \mathrm{Tr}[p_d(1-p_d)^3\,|\phi_2\rangle\langle\phi_2|]. \tag{C12}$$

那么，成功事件发生的成功概率P_{succ} 如下

$$P_{\mathrm{succ}} = P. \tag{C13}$$

我们可以通过考虑第4个模式的输入为真空，计算分布在合法参与方之间的 $N = 3$ 联合量子态。在这种情况下，我们同样可以将 $|\phi_1\rangle$ 和 $|\phi_2\rangle$ 表示为

$$\begin{aligned} |\phi_1\rangle = \frac{1}{2}&(|SVV0\rangle + |VSV0\rangle \\ &+ |VVS0\rangle + |VVV1\rangle)_{\boldsymbol{X}}, \end{aligned} \tag{C14}$$

$$|\phi_2\rangle = |VVV0\rangle_{\boldsymbol{X}}\,. \tag{C15}$$

由于第4个模式处于真空态，因此，

$$|\phi_1\rangle = \frac{1}{2}(|SVV\rangle + |VSV\rangle + |VVS\rangle)_{\boldsymbol{X}}, \tag{C16}$$

$$|\phi_2\rangle = |VVV\rangle_{\boldsymbol{X}}\,. \tag{C17}$$

利用这些量子态，我们可以将分布在各参与方之间的量子态表示为 $N = 3$ as (C9)。

附录D：被 W态大幅违背的贝尔不等式

在本节中，我们将介绍针对 $(3,3,2)$、$(4,2,2)$ 和 $(5,2,2)$ 场景构造的贝尔不等式。

1. (3,3,2) 场景

对于 $(3,3,2)$ 场景，我们假设参与方执行以下测量，并求解优化问题。

$$M_{0|0} = 0.5(I + \Pi(\pi/2)),\;\; M_{1|0} = I - M_{0|0}, \tag{D1}$$
$$M_{0|1} = 0.5(I + \Pi(0)),\;\;\;\; M_{1|1} = I - M_{0|1}, \tag{D2}$$
$$M_{0|2} = 0.5(I + \Pi(\pi/4)),\;\; M_{1|2} = I - M_{0|2}, \tag{D3}$$
$$N_{0|0} = 0.5(I + \Pi(2\pi/3)),\; N_{1|0} = I - N_{0|0}, \tag{D4}$$
$$N_{0|1} = 0.5(I + \Pi(\pi/3)),\;\; N_{1|1} = I - N_{0|1} \tag{D5}$$
$$N_{0|2} = 0.5(I + \Pi(0)),\;\;\;\; N_{1|2} = I - N_{0|2}. \tag{D6}$$

我们还假设鲍勃$_1$ 和鲍勃$_2$ 进行相同的测量。于是得到以下贝尔表达式。

$$\begin{aligned}
&[0.247,\;\; 13.080,\;\; 13.080,\; -72.982,\; -5.801,\; -22.874,\; -22.874,\;\; 170.097,\;\; 76.615,\;\; -43.969,\\
&-47.512,\; 6.441,\; -52.987,\; 14.794,\; 14.381,\; 36.414,\; -86.001,\; 214.380,\; 22.513,\;\; -93.969,\; 6.937,\\
&\;\; -40.572,\;\; -3.913,\; 78.416,\; 76.615,\; -47.512,\; -43.969,\; 6.441,\; -52.987,\; 14.381,\; 14.794,\; 36.414,\\
&196.613,\; -97.512,\; -97.512,\; 31.031,\; -100.764,\; 34.582,\; 34.582,\; 16.530,\; -39.867,\; 64.520,\;\; -0.277,\\
&\;\; -35.502,\; 27.964,\; -80.522,\;\; -24.228,\; 204.149,\; -86.001,\; 22.513,\; 214.380,\;\; -93.969,\; 6.937,\;\; -3.913,\\
&-40.572,\; 78.416,\;\; -39.867,\;\; -0.277,\; 64.520,\;\; -35.502,\; 27.964,\;\; -24.228,\;\; -80.522,\; 204.149,\\
&-30.035,\;\; -7.201,\;\; -7.201,\; 24.816,\; -55.651,\; 61.994,\; 61.994,\;\; -34.047,\; 92.225,\;\; -20.682,\; -20.682,\\
&15.662,\; -104.003,\; 10.995,\; 10.995,\; 6.796,\; 173.331,\;\; -33.981,\; -231.123,\; 186.357,\; -95.361,\; 7.696,\\
&68.780,\;\; -36.319,\; -16.427,\; 88.784,\; 120.053,\; -142.446,\;\; -37.728,\;\; -17.368,\; -65.610,\; 116.228,\\
&173.331,\; -231.123,\; -33.981,\; 186.357,\; -95.361,\; 68.780,\; 7.696,\;\; -36.319,\; 24.245,\;\; -34.600,\;\; -34.600,\\
&221.081,\;\; -9.877,\; 2.065,\; 2.065,\;\; -30.735,\; 124.730,\; -168.674,\; -18.698,\; 98.759,\; -247.755,\; 130.879,\\
&\;\; -4.775,\;\; -20.071,\; -16.427,\; 120.053,\; 88.784,\; -142.446,\; -37.728,\;\; -65.610,\;\; -17.368,\; 116.228,\\
&124.730,\;\; -18.698,\; -168.674,\; 98.759,\; -247.755,\;\; -4.775,\; 130.879,\;\; -20.071,\;\; -29.883,\; 275.227,\\
&275.227,\; -1154.797,\; -54.086,\;\; -40.034,\;\; -40.034,\; 433.671,\; 47.449,\;\; -17.500,\;\; -17.500,\;\; -7.461,\\
&-55.911,\; 7.990,\; 7.990,\; 33.021,\; 99.826,\;\; -42.233,\; -63.291,\; 24.590,\;\; -67.393,\; 13.525,\; 23.663,\\
&15.686,\; -20.685,\; 52.625,\; 27.461,\;\; -69.950,\; -32.289,\;\; -6.489,\;\; -7.916,\; 60.800,\; 99.826,\;\; -63.291,\\
&-42.233,\; 24.590,\;\; -67.393,\; 23.663,\; 13.525,\; 15.686,\; 106.177,\;\; -67.836,\; -67.836,\; 43.0166,\; -63.472,\\
&22.062,\; 22.062,\; 7.759,\; 20.049,\;\; -8.242,\;\; -14.055,\; 0.605,\; -30.694,\; 1.279,\; -9.196,\; 45.204,\;\; -20.685,\\
&27.461,\; 52.625,\;\; -69.950,\;\; -32.289,\;\; -7.916,\;\; -6.489,\; 60.800,\; 20.049,\;\; -14.055,\;\; -8.242,\; 0.605,\\
&-30.694,\;\; -9.196,\; 1.279,\; 45.204,\; -43.090,\; 53.739,\; 53.739,\;\; -71.156,\;\; -39.214,\;\; -2.950,\;\; -2.950,\\
&\;\; 54.100]
\end{aligned} \tag{D7}$$

2. (4,2,2) 情形

对于（4，2，2）场景，我们假设各参与方进行以下测量，并求解优化问题

tion问题。

$$M_{0|0} = 0.5(I + \Pi(\pi/2)),\;\; M_{1|0} = I - M_{0|0}, \tag{D8}$$
$$M_{0|1} = 0.5(I + \Pi(0)),\;\;\;\; M_{1|1} = I - M_{0|1}, \tag{D9}$$
$$N_{0|0} = 0.5(I + \Pi(2\pi/3)),\; N_{1|0} = I - N_{0|0}, \tag{D10}$$
$$N_{0|1} = 0.5(I + \Pi(\pi/3)),\;\; N_{1|1} = I - N_{0|1}, \tag{D11}$$

其中，我们假设鲍勃$_1$, 鲍勃$_2$ 和鲍勃$_3$ 对 W 态 $|W_4\rangle$进行相同的测量。于是，我们得到以下贝尔表达式。

$$
\begin{aligned}
&[-175.500,\ 157.364,\ 157.364,\ -61.255,\ 157.364,\ -61.255,\ -61.255,\ -81.627,\ 31.906,\ -45.094,\\
&-45.094,\ -21.089,\ -45.094,\ -21.089,\ -21.089,\ 395.608,\ -20.805,\ 13.390,\ 182.787,\ -74.300,\ 182.787,\\
&-74.300,-440.494,\ 55.609,\ 84.976,\ -102.482,-167.082,\ 62.336,-167.082,\ 62.336,\ 92.223,\ 84.100,\\
&-20.805,\ 182.787,\ 13.390,\ -74.300,\ 182.787,-440.494,\ -74.300,\ 55.609,\ 84.976,-167.082,-102.482,\\
&62.336,-167.082,\ 92.223,\ 62.336,\ 84.100,\ 76.176,\ 42.004,\ 42.004,-113.982,\ 84.863,-186.739,-186.739,\\
&150.889,\ 70.580,-143.281,-143.281,\ 93.027,-419.395,\ 211.812,\ 211.812,\ -5.681,\ -20.805,\ 182.787,\\
&182.787,-440.494,\ 13.390,\ -74.300,-74.300,\ 55.609,\ 84.976,-167.082,-167.082,\ 92.223,-102.482,\\
&62.336,\ 62.336,\ 84.100,\ 76.176,\ 42.004,\ 84.863,-186.739,\ 42.004,\ -113.982,-186.739,\ 150.889,\ 70.580,\\
&-143.281,-419.396,\ 211.812,-143.281,\ 93.027,\ 211.812,\ -5.681,\ 76.176,\ 84.863,\ 42.004,-186.739,\\
&42.004,-186.739,-113.982,\ 150.889,\ 70.580,\ -419.395,-143.281,\ 211.812,-143.281,\ 211.812,\ 93.027,\\
&-5.681,\ 514.847,\ -45.192,\ -45.192,\ -48.576,\ -45.192,\ -48.576,\ -48.576,\ 72.284,-36.318,\ -91.061,\\
&-91.061,\ 136.543,\ -91.061,\ 136.543,\ 136.543,\ -32.732,-415.077,\ 152.143,\ 152.143,-222.524,\\
&152.143,-222.524,-222.524,\ 94.050,\ 97.836,\ -42.045,\ -42.045,\ 69.817,-42.045,\ 69.817,\ 69.817,\ 22.189,\\
&9.454,\ -80.168,\ 26.822,\ -56.515,\ 26.822,\ -56.515,-735.028,\ 226.965,\ 48.963,\ -2.637,\ -20.330,\\
&45.615,\ -20.330,\ 45.615,\ 125.958,\ -16.209,\ 9.454,\ 26.822,\ -80.168,\ -56.515,\ 26.822,\ -735.028,\\
&-56.515,\ 226.965,\ 48.963,\ -20.330,-2.637,\ 45.615,\ -20.330,\ 125.958,\ 45.615,\ -16.209,\ 350.080,\\
&-196.220,-196.220,\ 8.327,-1257.239,\ 43.335,\ 43.335,\ 51.046,\ -37.404,\ 68.115,\ 68.115,\ -22.020,\\
&151.249,\ -33.866,-33.866,\ 65.404,\ 9.454,\ 26.822,\ 26.822,\ -735.028,\ -80.168,\ -56.515,\ -56.515,\\
&226.965,\ 48.963,\ -20.330,\ -20.330,\ 125.958,\ -2.637,\ 45.615,\ 45.615,\ -16.209,\ 350.080,-196.220,\\
&-1257.239,\ 43.335,-196.220,\ 8.327,\ 43.335,\ 51.046,\ -37.404,\ 68.115,\ 151.249,\ -33.866,\ 68.115,\ -22.020,\\
&-33.866,\ 65.404,\ 350.080,-1257.239,-196.220,\ 43.335,-196.220,\ 43.335,\ 8.327,\ 51.046,\ -37.404,\\
&151.249,\ 68.115,\ -33.866,\ 68.115,\ -33.866,\ -22.020,\ 65.404,\ 307.995,-915.232,-915.232,\ 160.203,\\
&-915.232,\ 160.203,\ 160.203,\ -67.435,\ -8.768,\ 102.174,\ 102.174,\ -61.625,\ 102.174,\ -61.625,\ -61.625,\\
&116.453]
\end{aligned}
\tag{D12}
$$

3. (5,2,2) 场景

对于 (5, 2,2) 场景，我们假设各参与方执行以下测量并求解该优化问题。

$$
\begin{aligned}
M_{0|0} &= 0.5(I + \Pi(\pi/2)), \quad M_{1|0} = I - M_{0|0}, && \text{(D13)}\\
M_{0|1} &= 0.5(I + \Pi(0)), \quad\ \ M_{1|1} = I - M_{0|1}, && \text{(D14)}\\
N_{0|0} &= 0.5(I + \Pi(2\pi/3)) \quad N_{1|0} = I - N_{0|0}, && \text{(D15)}\\
N_{0|1} &= 0.5(I + \Pi(\pi/3)), \quad N_{1|1} = I - N_{0|1}. && \text{(D16)}
\end{aligned}
$$

与其他场景相同，我们假设鲍勃们对W 态 $|W_5\rangle$进行相同的测量。

附录E：使用高斯形式进行状态计算

我们计算合法参与方的联合概率分布。在此，我们给出一个关于 $N = 3,4$ 的论证。

首先，记 N 对湮灭和产生算符 $\{\hat{a}_i,\ \hat{a}_i^\dagger\}_{i=1}^N$，它们满足以下对易关系

$$[\hat{a}_i, \hat{a}_j^\dagger] = \delta_{ij}. \tag{E1}$$

利用这些算符，我们将正交分量场算符 $\{\hat{}q_i,\ \hat{}p_i\}_{i=1}^N$ 定义如下

$$\hat{q}_i = \hat{a}_i + \hat{a}_i^\dagger, \tag{E2}$$

$$\hat{p}_i = i(\hat{a}_i^\dagger - \hat{a}_i). \tag{E3}$$

在 N 模玻色系统中，量子态 ρ 由其特征函数表征

$$\chi(x) = \mathrm{Tr}[\rho \mathcal{W}(x)], \tag{E4}$$

其中， $\mathcal{W}$ 是定义为如下形式的 Weyl算符

$$\mathcal{W}(x) = \exp\left[-ix^T r\right], \tag{E5}$$

$x \in \mathbb{R}^{2N}$是一个实向量，而 $r = [\hat{q}_1, \hat{p}_1, \ldots\ldots, \hat{q}_N, \hat{p}_N]^T$ 是由正交分量算符组成的向量。

平均光子数为 $\bar{n}$ 的双模压缩态的协方差矩阵如下

$$\Gamma^{\mathrm{TMSV}}(\bar{n}) = \begin{bmatrix} vI_2 & \sqrt{v^2-1}Z \\ \sqrt{v^2-1}Z & vI_2 \end{bmatrix}, \tag{E6}$$

其中， I_n 是 $n \times n$ 恒等算符的单位矩阵，而 d

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{E7}$$

参数 v 对应于双模压缩态的压缩程度，并且与该态的平均光子数 $\bar{n}$ 之间满足关系 $v = 1 + 2\bar{n}$。这里，我们省略了位移向量的参数，因为它始终是零向量。于是，初始态的协方差矩阵如下

$$\Gamma^{\mathrm{initial}} = \Gamma^{\mathrm{TMSV}}_{\boldsymbol{XX'}}(\bar{n}) \oplus I_{\boldsymbol{EF}}, \tag{E8}$$

其中

$$\begin{aligned} \Gamma^{\mathrm{TMSV}}_{\boldsymbol{XX'}}(\bar{n}) = \Gamma^{\mathrm{TMSV}}_{AA'}(\bar{n}) \oplus \Gamma^{\mathrm{TMSV}}_{B_1B_1'}(\bar{n}) \\ \oplus \Gamma^{\mathrm{TMSV}}_{B_2B_2'}(\bar{n}) \oplus \Gamma^{\mathrm{TMSV}}_{B_3B_3'}(\bar{n}), \end{aligned} \tag{E9}$$

模式 A 和 B_i 由爱丽丝和鲍勃$_i$ 在$i \in \{1, \ldots, N-1\}$ 探测，模式 A'和 B_i'发送至中央站， $\boldsymbol{E}$ 表示纯损耗信道的环境模， $\boldsymbol{F}$ 则分别表示参与方开关探测器的环境模。我们可以将透射率为 η 的纯损耗信道建模为一个分束器，其中一个输入模式为真空。此外，我们可以通过改变振幅来补偿探测器的任何损耗，因此可以在各参与方站点的位移操作之前，有效地调整开关探测器的探测效率。透射率为 η 的分束器操作可表示如下

$$S^{\mathrm{BS}}(\eta) = \begin{bmatrix} \sqrt{\eta}\, I_2 & \sqrt{1-\eta}\, I_2 \\ -\sqrt{1-\eta}\, I_2 & \sqrt{\eta}\, I_2 \end{bmatrix}. \tag{E10}$$

对标记为 $\boldsymbol{X'}$ 和$\boldsymbol{E}$的模式应用此操作后，我们可以得到信道传输后的量子态。接下来，我们考虑中央节点的操作。50:50 分束器的操作为

$$S^{50:50\mathrm{BS}} = S^{\mathrm{BS}}\left(\frac{1}{2}\right) = \frac{1}{\sqrt{2}} \begin{bmatrix} I_2 & I_2 \\ -I_2 & I_2 \end{bmatrix}. \tag{E11}$$

接着，对量子态适当地应用此操作，我们便可计算干涉仪 U 之后的量子态。我们考虑各方站点处开关探测器的探测效率。这些操作可用透射率为η_e的分束器表示。因此，应用这些操作后，我们可以得到单光子干涉前的量子态，并分别用 σ 和 Γ^{σ} 表示该量子态及其协方差矩阵。

接下来，我们考虑中央节点的探测。我们假设发生这样的事件：模式A' 的探测器点击，而其他模式的探测器均未点击。对应于开关探测器的 POVM 为

$$\{(1-p_d)\left|0\right\rangle\!\left\langle 0\right|, I - (1-p_d)\left|0\right\rangle\!\left\langle 0\right|\}, \tag{E12}$$

其中， I 是恒等算符。于是，成功预示条件下参与方之间的联合量子态为

$$\rho_{\boldsymbol{X}} = q_1 \rho^{(1)}_{\boldsymbol{X}} - q_2 \rho^{(2)}_{\boldsymbol{X}}, \tag{E13}$$

其中

$$\rho^{(1)}_{\boldsymbol{X}} = \tilde{\rho}^{(1)}_{\boldsymbol{X}} / \mathrm{Tr}[\tilde{\rho}^{(1)}_{\boldsymbol{X}}], \tag{E14}$$

$$\rho^{(2)}_{\boldsymbol{X}} = \tilde{\rho}^{(2)}_{\boldsymbol{X}} / \mathrm{Tr}[\tilde{\rho}^{(2)}_{\boldsymbol{X}}], \tag{E15}$$

$$\tilde{\rho}^{(1)}_{\boldsymbol{X}} = \mathrm{Tr}_{\boldsymbol{X'EF}}[\sigma \left|000\right\rangle\!\left\langle 000\right|_{\boldsymbol{X'}/A'}], \tag{E16}$$

$$\tilde{\rho}^{(2)}_{\boldsymbol{X}} = \mathrm{Tr}_{\boldsymbol{X'EF}}[\sigma \left|0000\right\rangle\!\left\langle 0000\right|_{\boldsymbol{X'}}], \tag{E17}$$

$$q_1 = \frac{(1-p_d)^3 \mathrm{Tr}[\sigma \left|000\right\rangle\!\left\langle 000\right|_{\boldsymbol{X'}/A'}]}{P}, \tag{E18}$$

$$q_2 = \frac{(1-p_d)^4 \mathrm{Tr}[\sigma \left|0000\right\rangle\!\left\langle 0000\right|_{\boldsymbol{X'}}]}{P}, \tag{E19}$$

且 P 是成功事件发生的概率；

$$\begin{aligned} P = (1-p_d)^3 \mathrm{Tr}[\sigma \left|000\right\rangle\!\left\langle 000\right|_{\boldsymbol{X'}/A'}] \\ - (1-p_d)^4 \mathrm{Tr}[\sigma \left|0000\right\rangle\!\left\langle 0000\right|_{\boldsymbol{X'}}]. \end{aligned} \tag{E20}$$

此处， $\boldsymbol{X'}/A'$ 表示模式 $B_1'B_2'B_3'$。

通过对除 $\boldsymbol{X'}/A'$和 $\boldsymbol{X'}$之外的模式从 Γ^{σ}中进行偏迹，我们分别得到协方差矩阵 $\Gamma_{\boldsymbol{X'}/A'}$ 和 $\Gamma_{\boldsymbol{X'}}$。利用这些协方差矩阵，我们计算出以下概率

$$\begin{aligned} \mathrm{Tr}(\sigma \left|000\right\rangle\!\left\langle 000\right|_{\boldsymbol{X'}/A'}) &= \frac{8}{\sqrt{\det\{\Omega_6(\Gamma_{\boldsymbol{X'}/A'} + I_6)\Omega_6^T\}}}, \\ \mathrm{Tr}(\sigma \left|0000\right\rangle\!\left\langle 0000\right|_{\boldsymbol{X'}}) &= \frac{16}{\sqrt{\det\{\Omega_8(\Gamma_{\boldsymbol{X'}} + I_8)\Omega_8^T\}}}, \end{aligned} \tag{E21}$$

其中 $\boldsymbol{\Omega}_n$ 定义如下

$$\Omega_n = \bigoplus_{k=1}^{n/2} \omega_k = \begin{pmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{pmatrix}, \omega = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \tag{E22}$$

然后，我们计算概率分布$p(a,\boldsymbol{b}|x,\boldsymbol{y})$。为此，我们推导分别对应于 $\rho_{\boldsymbol{X}}^{(1)}$ 和 $\rho_{\boldsymbol{X}}^{(2)}$ 的协方差矩阵$\Gamma^{(1)}$ 和 $\Gamma^{(2)}$。令$\Gamma_{AA'B_1B_1'B_2B_2'B_3B_3'}$ 表示通过对 Γ^{σ}求迹消去环境模而得到的协方差矩阵。通过改变模式的排序，我们得到 $\Gamma_{AB_1B_2B_3A'B_1'B_2'B_3'}$，该协方差矩阵具有如下形式

$$\Gamma_{AB_1B_2B_3A'B_1'B_2'B_3'}=\begin{bmatrix}\Gamma_{AB_1B_2B_3A'B_1'B_2'} & C_{B_3'}\\ C_{B_3'}^T & \Gamma_{B_3'}\end{bmatrix}. \tag{E23}$$

由于真空投影可视为异频测量，因此在模式B_3' 上进行真空投影后的协方差矩阵为

$$\begin{aligned}\Gamma'_{AB_1B_2B_3A'B_1'B_2'}&=\Gamma_{AB_1B_2B_3A'B_1'B_2'}\\&\quad-C_{B_3'}(\Gamma_{B_3'}+I_2)^{-1}C_{B_3'}^T\\&=\begin{bmatrix}\Gamma_{AB_1B_2B_3A'B_1'} & C_{B_2'}\\ C_{B_2'}^T & \Gamma_{B_2'}\end{bmatrix}.\end{aligned} \tag{E24}$$

通过重复这一过程，我们得到 $\Gamma^{(1)}$ 和 $\Gamma^{(2)}$。设 α、β、γ 和 δ 分别为各参与方的位移。那么，在执行这些位移操作后，参与方之间的联合量子态的位移向量变为

$$\begin{aligned}d_{\boldsymbol{X}}=2[&\mathrm{Re}(\alpha),\mathrm{Im}(\alpha),\mathrm{Re}(\beta),\mathrm{Im}(\beta),\\&\mathrm{Re}(\gamma),\mathrm{Im}(\gamma),\mathrm{Re}(\delta),\mathrm{Im}(\delta)]^T.\end{aligned} \tag{E25}$$

我们计算所有参与方的开关探测器均未点击的概率 $p(0,\ldots\ldots,0|x,\boldsymbol{y})$。这些探测器的 POVM 可表示为

$$\{|0\rangle\langle 0|, I-|0\rangle\langle 0|\}. \tag{E26}$$

接下来，我们按以下方式计算该概率

$$\begin{aligned}&p(0,\ldots,0|x,\boldsymbol{y})\\&\quad=\mathrm{Tr}\left[\rho_{\boldsymbol{X}}\,|0000\rangle\langle 0000|_{\boldsymbol{X}}\right]\\&\quad=\mathrm{Tr}\left[q_1\rho_{\boldsymbol{X}}^{(1)}\,|0000\rangle\langle 0000|_{\boldsymbol{X}}\right]\\&\qquad-\mathrm{Tr}\left[q_2\rho_{\boldsymbol{X}}^{(2)}\,|0000\rangle\langle 0000|_{\boldsymbol{X}}\right].\end{aligned} \tag{E27}$$

这里，令 $\chi^{(1)}(x)$ 为 $\rho_{\boldsymbol{X}}^{(1)}$ 的特征函数，令$\chi_0(x)$ 为真空投影的特征函数，其定义如下

$$\chi^{(1)}(x)=\exp\left(\frac{1}{2}x^T(\Omega_8\Gamma^{(1)}\Omega_8^T)x-i(\Omega_8 d_{\boldsymbol{X}})^T x\right), \tag{E28}$$

$$\chi_0(x)=\exp\left(-\frac{1}{2}x^T(\Omega_8 I_8\Omega_8^T)x\right), \tag{E29}$$

其中，$x\in\mathbb{R}^8$ 为实向量。于是有

$$\begin{aligned}\mathrm{Tr}\left[q_1\rho_{\boldsymbol{X}}^{(1)}\,|0000\rangle\langle 0000|_{\boldsymbol{X}}\right]&=\frac{q_1}{\pi^2}\int\chi^{(1)}(x)\chi_0(x)\,dx\\&=\frac{16q_1}{\sqrt{\det\left(\Omega_8(\Gamma^{(1)}+I_8)\Omega_8^T\right)}}\exp\left(-\frac{1}{2}(\Omega_8 d_{\boldsymbol{X}})^T(\Omega_8(\Gamma^{(1)}+I_8)\Omega_8^T)^{-1}(\Omega_8 d_{\boldsymbol{X}})\right)\end{aligned} \tag{E30}$$

我们可以类似地计算 $\mathrm{Tr}\left[q_2\rho_{\boldsymbol{X}}^{(2)}\,|0000\rangle\langle 0000|_{\boldsymbol{X}}\right]$，并可推导出概率 $p(0,0,0,0|x,\boldsymbol{y})$。通过应用相同的过程，我们可以计算出其他概率。

[1] C. H. Bennett 和 G. Brassard，《量子密码学：公钥分发与掷币》，《理论计算机科学》**560**，7（2014年）。[2] A. K. Ekert，《基于贝尔定理的量子密码学》，《物理评论快报》**67**，661（1991年）。[3] C. H. Bennett、G. Brassard 和 N. D. Mermin，《无需贝尔定理的量子密码学》，《物理评论快报》**68**，557（1992年）。[4] C. H. Bennett，《使用任意两个非正交态的量子密码学》，《物理评论快报》**68**，3121（1992年）。[5] F. Xu、X. Ma、Q. Zhang、H.-K. Lo 和 J.-W. Pan，《Secure quantum key distribution with realistic devices》，《现代物理评论》**92**，025002（2020年）。[6] S. Pirandola、U. L. Andersen、L. Banchi、M. Berta、D. Bunandar、R. Colbeck、D. Englund、T. Gehring、C. Lupo、C. Ottaviani、J. L. Pereira、M. Razavi、J. S. Shaari、M. Tomamichel、V. C. Usenko、G. Vallone、P. Vil- loresi 和 P. Wallden，量子密码学进展，《Adv. Opt. Photonics》**12**，1012（2020年）。[7] C. Elliott，构建量子网络，《新物理学杂志》**4**，46（2002年）。[8] C. Elliott、A. Colvin、D. Pearson、O. Pikalo、J. Schlafer,

以及 H. Yeh，DARPA量子网络的当前状况，《Proc. SPIE》**5815**，138（2005年）。[9] M. Peev、C. Pacher、R. All´eaume、C. Barreiro、J. Bouda、W. Boxleitner、T. Debuisschert、E. Diamanti、M. Dianati、J. F. Dynes、S. Fasel、S. Fossier、M. F¨urst、J.-D. Gautier、O. Gay、N. Gisin、P. Grangier、A. Happe、Y. Hasani、M. Hentschel、H. H¨ubel、G. Humer、T. L¨anger、M. Legr´e、R. Lieger、J. Lodewyck、T. Lor¨unser、N. L¨utkenhaus、A. Marhold、T. Matyus、O. Maurhart、L. Monat、S. Nauerth、J.-B. Page、A. Poppe、E. Querasser、G. Ri- bordy、S. Robyr、L. Salvail、A. W. Sharpe、A. J. Shields、D. Stucki、M. Suda、C. Tamas、T. Themel、R. T. Thew、Y. Thoma、A. Treiber、P. Trinkler、R. Tualle-Brouri、F. Vannel、N. Walenta、H. Weier、H. Weinfurter、I. Wim- berger、Z. L. Yuan、H. Zbinden 和 A. Zeilinger，维也纳SECOQC量子密钥分发网络，《新物理学杂志》**11**，075001（2009年）。[10] M. Sasaki、M. Fujiwara、H. Ishizuka、W. Klaus、K. Wakui、M. Takeoka、S. Miki、T. Yamashita、Z. Wang、A. Tanaka、K. Yoshino、Y. Nambu、S. Takahashi、A. Tajima、A. Tomita、T. Domeki、T. Hasegawa、Y. Sakai、H. Kobayashi、T. Asai、K. Shimizu、T. Tokura、T. Tsurumaru、M. Matsui、T. Honjo、K. Tamaki、H. Takesue、Y. Tokura、J. F. Dynes、A. R. Dixon、A. W. Sharpe、Z. L. Yuan、A. J. Shields、S. Uchikoga、M. Legr´e、S. Robyr、P. Trinkler、L. Monat、J.-B. Page、G. Ribordy、A. Poppe、A. Allacher、O. Maurhart、T. L¨anger、M. Peev 和 A. Zeilinger，东京量子密钥分发网络中的量子密钥分发现场测试，《Opt. Express》**19**，10387（2011年）。[11] J. F. Dynes、A. Wonfor、W. W.-S. Tam、A. W. Sharpe、R. Takahashi、M. Lucamarini、A. Plews、Z. L. Yuan、A. R. Dixon、J. Cho、Y. Tanizawa、J.-P. Elbers、H. Greißer、I. H. White、R. V. Penty 和 A. J. Shields，剑桥量子网络，npj Quantum Inf. **5**，101（2019年）。[12] Y.-A. Chen、Q. Zhang、T.-Y. Chen、W.-Q. Cai、S.-K. Liao、J. Zhang、K. Chen、J. Yin、J.-G. Ren、Z. Chen、S.-L. Han、Q. Yu、K. Liang、F. Zhou、X. Yuan、M.-S. Zhao、T.-Y. Wang、X. Jiang、L. Zhang、W.-Y. Liu、Y. Li、Q. Shen、Y. Cao、C.-Y. Lu、R. Shu、J.-Y. Wang、L. Li、N.- L. Liu、F. Xu、X.-B. Wang、C.-Z. Peng 和 J.-W. Pan，跨越4600公里的天地一体化量子通信网络，《自然》**589**，214（2021年）。[13] T.-Y. Chen、X. Jiang、S.-B. Tang、L. Zhou、X. Yuan、H. Zhou、J. Wang、Y. Liu、L.-K. Chen、W.-Y. Liu、H.-F. Zhang、K. Cui、H. Liang、X.-G. Li、Y. Mao、L.-J. Wang、S.-B. Feng、Q. Chen、Q. Zhang、L. Li、N.-L. Liu、C.-Z. Peng、X. Ma、Y. Zhao 和 J.-W. Pan，46节点量子城域网的实施，npj Quantum Inf. **7**，134（2021年）。[14] V. Martin、J. P. Brito、L. Ort´ız、R. B. M´endez、J. S. Bu- ruaga、R. J. Vicente、A. Sebasti´an-Lombra˜na、D. Rinc´on、F. P´erez、C. S´anchez、M. Peev、H. H. Brunner、F. Fung、A. Poppe、F. Fr¨owis、A. J. Shields、R. I. Woodward、H. Griesser、S. Roehrich、F. de la Iglesia、C. Abell´an、M. Hentschel、J. M. Rivas-Moscoso、A. Pastor-Perales、J. Folgueira 和 D. L´opez，MadQCI：部署于生产设施中的异构且可扩展的软件定义网络量子密钥分发网络，npj Quantum Inf. **10**，80（2024年）。[15] Y. Wu、J. Zhou、X. Gong、Y. Guo、Z.-M. Zhang 和 G. He，连续变量测量设备无关的多方量子通信，《物理评论A》**93**，022325（2016年）。[16] M. Epping、H. Kampermann、C. Macchiavello 和 D. Bruß，纠缠可加速网络中的量子密钥分发，《新物理学杂志》**19**，093012（2017年）。[17] Z. Zhang、R. Shi 和 Y. Guo，具有中间纠缠的多方连续变量量子会议网络，Appl. Sci. **8**，1312（2018年）。[18] F. Grasselli、H. Kampermann 和 D. Braß，多方量子密钥分发协议中的有限密钥效应，《新物理学杂志》**20**，113014（2018年）。[19] C. Ottaviani、C. Lupo、R. Laurenza 和 S. Pirandola，用于高速率量子会议的模块化网络，Commun. Phys. **2**，118（2019年）。[20] F. Grasselli、H. Kampermann 和 D. Bruß，利用单光子干涉进行会议密钥协商，《新物理学杂志》**21**，123002（2019年）。[21] S. Zhao、P. Zeng、W.-F. Cao、X.-Y. Xu、Y.-Z. Zhen、X. Ma、L. Li、N.-L. Liu 和 K. Chen，相位匹配量子密码会议，Phys. Rev. Appl. **14**，024010（2020年）。[22] G. Carrara、G. Murta 和 F. Grasselli，突破量子会议密钥协商的基本界限，Phys. Rev. Appl. **19**，064017（2023年）。[23] M. Proietti、J. Ho、F. Grasselli、P. Barrow、M. Malik 和 A. Fedrizzi，实验性量子会议密钥协商，Sci. Adv. **7**，eabe0395（2021年）。[24] A. Pickston、J. Ho、A. Ulibarrena、F. Grasselli、M. Proietti、C. L. Morrison、P. Barrow、F. Graffitti 和 A. Fedrizzi，量子网络中的会议密钥协商，npj Quantum Inf. **9**，82（2023年）。[25] K.-X. Yang、Y.-L. Mao、H. Chen、X. Dong、J. Zhu、J. Wu 和 Z.-D. Li，实验性测量设备无关量子会议密钥协商，《物理评论快报》**133**，210803（2024年）。[26] G. Murta、F. Grasselli、H. Kampermann 和 D. Bruß，量子会议密钥协商：综述，Adv. Quantum Technol. **3**，2000025（2020年）。[27] H.-K. Lo、M. Curty 和 B. Qi，测量设备无关量子密钥分发，《物理评论快报》**108**，130503（2012年）。[28] S. Pirandola、C. Ottaviani、G. Spedalieri、C. Weedbrook、S. L. Braunstein、S. Lloyd、T. Gehring、C. S. Jacobsen 和 U. L. Andersen，高速率测量设备无关量子密码学，Nat. Photonics **9**，397（2015年）。[29] M. Lucamarini、Z. L. Yuan、J. F. Dynes 和 A. J. Shields，无需量子中继器即可突破量子密钥分发的速率-距离极限，《自然》**557**，400（2018年）。[30] V. Zapatero、T. van Leent、R. Arnon-Friedman、W.-Z. Liu、Q. Zhang、H. Weinfurter 和 M. Curty，设备无关量子密钥分发的进展，npj Quantum Inf. **9**，10（2023年）。[31] I. W. Primaatmaja、K. T. Goh、E. Y.-Z. Tan、J. T.-F. Khoo、S. Ghorai 和 C. Lim，设备无关量子密钥分发协议的安全性：综述，Quantum **7**，932（2023年）。[32] A. Ac´ın、N. Brunner、N. Gisin、S. Massar、S. Pironio 和 V. Scarani，针对集体攻击的量子密码学设备无关安全性，《物理评论快报》**98**，230501（2007年）。[33] S. Pironio、A. Ac´ın、N. Brunner、N. Gisin、S. Massar 和 V. Scarani，针对集体攻击安全的设备无关量子密钥分发，《新物理学杂志》**11**，

045021（2009）。[34] J. Ribeiro、G. Murta 和 S. Wehner，《完全设备无关的会议密钥协商》，《物理评论A》97，022307（2018）。[35] T. Holz、D. Miller、H. Kampermann 和 D. Bruß，《关于“完全设备无关的会议密钥协商”的评论》，《物理评论A》100，026301（2019）。[36] J. Ribeiro、G. Murta 和 S. Wehner，《对“关于‘完全设备无关的会议密钥协商’的评论”的回复》，《物理评论A》100，026302（2019）。[37] T. Holz、H. Kampermann 和 D. Bruß，《用于设备无关会议密钥协商的真正多体贝尔不等式》，《物理评论研究》2，023251（2020）。[38] F. Grasselli、G. Murta、H. Kampermann 和 D. Bruß，《利用三方非定域性增强设备无关密码学》，Quantum 7，980（2023）。[39] L. Wooltorton、P. Brown 和 R. Colbeck，《标准设备无关会议密钥协商并不需要真正多体纠缠》，《物理评论快报》135，220803（2025）。[40] M. Ishihara、A. J. E. Bjerrum、W. Roga、J. B. Brask、U. L. Andersen 和 M. Takeoka，《长距离设备无关会议密钥协商》，《物理评论A》112，032429（2025）。[41] D. M. Greenberger、M. A. Horne、A. Shimony 和 A. Zeilinger，《无不等式的贝尔定理》，《美国物理学杂志》58，1131（1990）。[42] W. D¨ur、G. Vidal 和 J. I. Cirac，《三个量子比特可以以两种不等价的方式纠缠》，《物理评论A》62，062314（2000）。[43] J. Miguel-Ramiro、F. Riera-S`abat 和 W. D¨ur，《用于 W 态的量子中继器》，《PRX量子》4，040323（2023）。[44] W. Roga、R. Ikuta、T. Horikiri 和 M. Takeoka，《有损信道网络中的高效Dicke态分发》，《物理评论A》108，012612（2023）。[45] A. Cabello，《三量子比特格林伯格-霍恩-蔡林格态和 W 态的有无不等式贝尔定理》，《物理评论A》65，032108（2002）。[46] A. S. De、U. Sen、M. Wie´sniak、D. Kaszlikowski 和 M. ˙Zukowski，《多量子比特 W 态比格林伯格-霍恩-蔡林格态具有更强的非经典性》，《物理评论A》68，062306（2003）。[47] L. Heaney、A. Cabello、M. F. Santos 和 V. Vedral，《单光子极端非定域性》，《新物理学杂志》13，053054（2011）。[48] N. Brunner、J. Sharam 和 T. V´ertesi，《利用贝尔不等式检验多体纠缠的结构》，《物理评论快报》108，110501（2012）。[49] J. B. Brask 和 R. Chaves，《利用基于位移的测量进行稳健非定域性检验》，《物理评论A》86，010103(R)（2012）。[50] Z. Wang 和 D. Markham，《对称态的非定域性与纠缠》，《物理评论A》87，012104（2013）。[51] J. B. Brask、R. Chaves 和 N. Brunner，《在没有共享参考系的情况下检验单光子的非定域性》，《物理评论A》88，012111（2013）。[52] J.-D. Bancal、J. Barrett、N. Gisin 和 S. Pironio，《多体非定域性的定义》，《物理评论A》88，014102（2013）。[53] A. Sohbi、I. Zaquine、E. Diamanti 和 D. Markham，《退相干对对称态非定域性的影响》，《物理评论A》91，022101（2015）。[54] T. J. Barnea、G. P¨utz、J. B. Brask、N. Brunner、N. Gisin 和 Y.-C. Liang，《受损耗影响的 W 态和 Dicke 态的非定域性》，《物理评论A》91，032108（2015年）。[55] K. F. P´al 和 T. V´ertesi，《利用 W 态在三方贝尔检验中消除探测漏洞》，《物理评论A》92，022103（2015年）。[56] P. Divi´anszky、R. Trencs´enyi、E. Bene 和 T. V´ertesi，《界定 W 态非定域性的持久性》，《物理评论A》93，042113（2016年）。[57] A. J. E. Bjerrum、J. B. Brask、J. S. Neergaard-Nielsen 和 U. L. Andersen，《利用纠缠交换和基于位移的测量进行远距离非定域性检验的方案》，《物理评论A》107，052611（2023年）。[58] M. Ho、P. Sekatski、E. Y.-Z. Tan、R. Renner、J.-D. Ban-cal 和 N. Sangouard，《噪声预处理有助于实现光子版设备无关量子密钥分发》，《物理评论快报》124，230502（2020年）。[59] I. Devetak 和 A. Winter，《从量子态中蒸馏密钥和纠缠》，《英国皇家学会会刊A辑》461，207（2005年）。[60] L. Masanes、S. Pironio 和 A. Ac´ın，《利用因果独立的测量设备实现安全的设备无关量子密钥分发》，《自然·通讯》2，238（2011年）。[61] E. Y.-Z. Tan、R. Schwonnek、K. T. Goh、I. W. Primaat-maja 和 C. C.-W. Lim，《利用不可信设备计算量子密码学的安全密钥率》，npj Quantum Inf. 7，158（2021年）。[62] P. Brown、H. Fawzi 和 O. Fawzi，《计算量子关联的条件熵》，《自然·通讯》12，575（2021年）。[63] P. Brown、H. Fawzi 和 O. Fawzi，《条件冯·诺依曼熵的设备无关下界》，Quantum 8，1445（2024年）。[64] O. Nieto-Silleras、S. Pironio 和 J. Silman，《利用完整测量统计实现最优的设备无关随机性评估》，《新物理学杂志》16，013035（2014年）。[65] R. K¨onig、R. Renner 和 C. Schaffner，《最小熵和最大熵的操作意义》，IEEE Trans. Inf. Theory 55，4337（2009年）。[66] M. Navascu´es、S. Pironio 和 A. Ac´ın，《刻画量子关联集合的收敛半定规划层级》，《新物理学杂志》10，073013（2008年）。[67] S. Boyd 和 L. Vandenberghe，《凸优化》，*Convex optimization*（剑桥大学出版社，2004年）。[68] N. Brunner、D. Cavalcanti、S. Pironio、V. Scarani 和 S. Wehner，《贝尔非定域性》，《现代物理评论》86，419（2014年）。[69] M. Takeoka、M. Sasaki 和 N. L¨utkenhaus，《利用线性光学和光子计数实现二元投影测量》，《物理评论快报》97，040502（2006年）。[70] S. Izumi、J. S. Neergaard-Nielsen 和 U. L. Andersen，《光子探测反馈测量的层析》，《物理评论快报》124，070502（2020年）。[71] D. P. Nadlinger、P. Drmota、B. C. Nichol、G. Araneda、D. Main、R. Srinivas、D. M. Lucas、C. J. Ballance、K. Ivanov、E. Y.-Z. Tan、P. Sekatski、R. L. Urbanke、R. Renner、N. Sangouard 和 J.-D. Bancal，《经贝尔定理认证的实验量子密钥分发》，《自然》607，682（2022年）。[72] W. Zhang、T. van Leent、K. Redeker、R. Garthoff、R. Schwonnek

V. Scarani、C. C.-W. Lim 和 H. Weinfurter，《面向远距离用户的设备无关量子密钥分发系统》，《自然》**607**，687（2022）。[73] B.-W. Lu、C.-W. Yang、R.-Q. Wang、B.-F. Gao、Y.-Z. Zhen、Z.-G. Wang、J.-K. Shi、Z.-Q. Ren、T. A. Hahn、E. Y.-Z. Tan、X.-P. Xie、M.-Y. Zheng、X. Jiang、J. Zhang、F. Xu、Q. Zhang、X.-H. Bao 和 J.-W. Pan，利用单原子，《科学》**391**，592（2026年）。[74] P. Wittek，算法950：用于非对易变量多项式优化问题的Ncpol2sdpa-sparse半定规划松弛，《ACM数学软件汇刊》**41**，1（2015年）。[75] M. APS，*MOSEK Optimizer API for Python 10.2.8*（2024年）。