超越基于发送或不发送方案的量子密钥分发当前可达距离

Georgi Bebrov*Department of Communication Engineering, Technical University of Varna, Varna, Bulgaria 9000*（日期：2026年2月4日）

近年来，基于 *sending-or-not-sending* （SNS）原理的协议受到广泛研究，并已证明能够实现量子密钥分发（QKD）中最长的传输距离。在本研究中，我们提出一种 *sending-or-not-sending phase-matching* 量子密钥分发协议（SNS-PM-QKD），该协议提高了对相位失配的容忍度，从而延长了可达传输距离。我们针对集体攻击，在渐近（无限密钥）情形下对SNS-PM-QKD进行了安全性分析。我们将所提出的协议的性能与标准相位匹配量子密钥分发、理论上的SNS型双场量子密钥分发协议（SNS-TF-QKD），以及在最长达1002km的传输距离上运行的实验SNS-TF-QKD进行了比较。结果表明，SNS-PM-QKD实现的传输距离超过了这些现有协议，凸显了其在远距离量子通信中的潜力。

arXiv:2602.03173v1 [quant-ph] 3 Feb 2026

I. 引言

量子密钥分发（QKD）使空间上彼此分离的参与方能够通过不可信量子信道建立共享的安全密码密钥，并辅以完全经认证的经典信道 [1]。多年来，人们提出了多种量子密钥分发协议，以解决实现漏洞和性能限制[2–6]。量子密钥分发部署的一项核心限制，仍然是其有限的实际传输距离，这受到光学损耗、通信信道中的相位（或偏振）漂移，以及设备缺陷引起的错误率的制约。量子密钥分发协议的可达距离取决于其密钥率对信道透射率的依赖关系，以及密钥率对错误的容忍度。密钥率随信道透射率变化的最佳标度遵循平方根定律 [7–10]，而可容忍的错误率通常可达百分之几十 [11]。双场量子密钥分发（TF-QKD）协议 [7–11]这一类协议实现了信道透射率的平方根标度。这是通过双体相干态在分束器处发生单光子干涉实现的。这一类协议的代表是所谓的相位匹配测量设备无关量子密钥分发协议，以下称为相位匹配量子密钥分发（PM-QKD） [9, 10]。与原始TF-QKD相比，它的特点是密钥生成机制更为简化，不需要随机化 [10]，。值得注意的是，这种简化并不会降低协议的安全性。一般而言，可以通过两种方式实现对错误的容忍：一是采用完全（或部分）独立于错误率的密钥生成机制；二是通过适当的密钥生成机制和合适的后选择程序来抑制错误的引入 [11, 12]。所谓的发送或不发送量子密钥分发协议（SNS-QKD）是TF-QKD的一种变体，其错误容忍度相对较高 [11–19]。这是由于密钥生成事件中不存在任何干涉，并且采用了特定的后选择标准；因此，该协议能够表现出对较大错位误差的容忍度，因此可以证明其能够容忍错位误差。

迄今为止，在光纤量子密钥分发方案中，SNS-TF-QKD 实现了最长的距离范围。在渐近极限下，理论研究 [11–14] 实现了最远约 910km 距离的安全密钥生成，而实验则展示了创纪录的安全传输距离，最远约为 1002km [19]。

由于长距离运行是量子密钥分发的核心目标，尤其对于广域量子网络而言，因此进一步改进协议设计、在保障安全性的同时扩展速率-距离覆盖至关重要。受这一挑战的启发，我们提出了一种受发送或不发送 方法启发的新型量子密钥分发协议，专门用于在现实条件下提升传输距离。在此，我们构建了一种协议，通过将测量结果 后选择和发送或不发送 范式引入 PM-QKD 框架，进一步降低错误率。在 PM-QKD 中，合法参与方（*Alice* 和*Bob*）制备的相干态在不可信中间节点 [10] 处进行单光子干涉。密钥生成过程基于干涉结果（相长或相消），分别对应于*Alice* 和*Bob*所选相干态相位之间的关联或反关联，密钥比特则编码在这些相位中。在此处提出的协议中，每个合法参与方都制备两个相干态（一个信号态和一个次级态），二者相位相同，并决定是否将其发送至中间节点。在中间节点处，*Alice* 和*Bob* 制备的信号态（次级态）在最终联合干涉测量之前，先在耦合器处进行初步干涉。耦合器会在其中一个发生干涉的相干态上固有地产生 π 相移。因此，两个相位和强度相同的相干态（理想的仅损耗情形）在耦合器处相遇时会发生相消干涉。因此，依据发送或不发送 的选择——即发送—不发送 （不发送—发送）、发送—发送或不发送—不发送情形——联合测量寄存器记录到的结果要么是

没有点击，要么仅在对应于相消干涉的探测器处发生点击。在理想的仅损耗情形下，只有发送—不发送（或不发送—发送配置会产生探测事件。与原始 SNS-QKD 协议一样，所提出方案中的密钥生成同样基于发送或不发送 选择。在现实条件下，由于耦合器和最终干涉分束器均存在暗计数和失配，所有发送或不发送 配置中都会出现相关探测事件。所提出的量子密钥分发模型的一个显著特点是，筛除除对应相消干涉的确定性探测之外的所有测量结果（测量结果后选择），从而降低错误率。这种降低会改善密钥率与误码率之比，进而实现更远的工作距离。

在安全性分析中，我们采用文献 [10]中引入的框架。为评估新提出协议的性能，我们将其与PM-QKD[10], 、理论SNS-TF-QKD模型 [11, 12], 以及实验S NS-TF-QKD实现 [19] 在可实现传输（运行）距离方面进行比较。文献 [12] 和 [19] 分别报告了迄今为止理论与实验发送或不发送协议的最大可实现距离。

本文其余部分组织如下。在第II节中，我们给出所提出的协议的详细描述。在第III节中，我们给出安全性分析。数值模拟和性能结果在第IV节中报告。最后，第 V 节总结主要结论，并讨论未来工作的可能方向。

II. 所提出的协议

A. 发送或不发送相位匹配量子密钥分发

在本节中，我们基于图1的装置提出一种协议。该协议称为发送或不发送相位匹配量子密钥分发（ SNS-PM-QKD）。它包括以下步骤：

步骤 *1*。$Alice$ （Bob）根据概率分布$\{p_a, 1-p_a\}$ （$\{p_b, 1-p_b\}$） [10]生成一个随机数 m_a（m_b） $\in \{0,1\}$ 。如果$Alice$和Bob 分别选择$m_a = 0$ 和 $m_b = 0$，则当前协议轮次视为信号轮次。如果$Alice$ 和 Bob选择 $m_a = 1$ 和 $m_b = 1$，则该轮次视为测试轮次。

步骤 *2*。态制备—在测试轮次中，***Alice*** （Bob）以概率 ϵ 选择是否向***Charlie*** 发送相干态（测试态和辅助态（或参考态））。当采用发送-不-发送 方法 [11]时，随后会出现几种情形：发送-不发送或 不发送-发送（**sns**）、不发送-不发送（**nn**）以及发送-发送（**ss**）。如果$Alice$ （Bob）选择向***Charlie***发送相干态，则她 （他）制备测试相干态 $|e^{i\omega_a}\sqrt{\mu_a}\rangle$ （$|e^{i\omega_b}\sqrt{\mu_b}\rangle$）以及辅助态（或参考）相干态 $|e^{i\theta_a}\sqrt{\mu_a}\rangle$ （$|e^{i\theta_b}\sqrt{\mu_b}\rangle$），其中 $\theta_{a(b)} \in [0, 2\pi)$ 、$\omega_{a(b)} \in [0, 2\pi)$ 和$\mu_{a(b)}$ 均随机选取。因此，该协议的测试轮次配置（$\mu_{a(b)}$、 $\theta_{a(b)}$、 $\omega_{a(b)}$）与参考文献 [10]中所采用的配置相同。注意，在测试轮次中，$Alice$ 和Bob 公布其发送或不发送 选择、$\mu_{a(b)}$ 选择、$\omega_{a(b)}$以及 $\theta_{a(b)}$ 选择。

在信号轮次中，Alice（Bob）以概率 ϵ 选择是否向 Charlie 发送相干态（信号态和次级态）。采用发送或不发送方法时，会出现几种场景 [11]: 发送-不发送或不发送-发送（sns）、不发送-不发送（nn）以及发送—发送（ss）。如果 Alice（Bob）选择向 Charlie 发送相干态，她（他）会制备一个信号相干态 $|e^{i\varphi_a}\sqrt{\mu}\rangle_Q$ $\left(|e^{i\varphi_b}\sqrt{\mu}\rangle_{Q'}\right)$ 和一个次级相干态 $|e^{i\tau_a}\sqrt{\mu}\rangle_T$ $\left(|e^{i\tau_b}\sqrt{\mu}\rangle_{T'}\right)$，其中 $\tau_a = 0$、$\tau_b = 0$ $\varphi_a = 0$ $\varphi_b = 0$ 、以及 。请注意，在无噪声（无相位漂移）量子信道的情况下，如果双方都选择发送相干态，它们的态会在耦合器 C_S、C_T 处相互抵消——Alice 和 Bob 的次级态在 C_T 处发生相消干涉，而它们的信号态在 C_S 处发生相消干涉。还要注意，在无噪声量子信道的情况下，当出现发送-不发送场景时，只有探测器 D_- 应当点击（$\Delta\phi_{a(b)} = |\varphi_{a(b)} - \tau_{a(b)}| = \pi$） [20]; 见图1。

步骤3. 测量——Alice 和 Bob 将各自的相干态（信号/测试态和次级态）发送至中间节点 Charlie。在 Charlie 一侧的入口处，无论是测试轮次还是信号轮次，Alice 和 Bob 的信号/测试相干态都会在耦合器 C_S处发生干涉，而 Alice 和 Bob 的次级相干态则会在耦合器 C_T处发生干涉：C_S 的输出态为 $|e^{i\varphi_a}\sqrt{\mu} - e^{i\varphi_b}\sqrt{\mu}\rangle$；$C_T$ 的输出态为 $|e^{i\tau_b}\sqrt{\mu} - e^{i\tau_a}\sqrt{\mu}\rangle$。耦合器处发生的干涉过程见附录 A。这些耦合器的输出（即上述干涉过程的结果）随后被导向分束器 BS。对于每个轮次，Charlie 都会执行一次联合（分束器）测量，其特征由 POVM 元素 $F^{\varkappa}$ [10] 描述。他会公布测量结果 $\varkappa \in \{+, -, ?\ d\}$，其中“+”表示仅探测器 D_+发生点击，“–”表示仅探测器 D_-发生点击，“?”表示探测器未发生点击，而“d”表示探测器 [10]均发生点击；见图1。

步骤 *1–3* 重复执行 N 次（$N \to \infty$），考虑在渐近区间内运行。

步骤 *4*。公开通信与筛选——在此步骤中，通过经过认证的经典公开信道公开信息。$Alice$ 和Bob首先公布各自的 m_a、 m_b 值——他们进行轮次类型筛选。若为共同信号轮次（$m_{a(b)} = 0$），$Alice$ 和Bob 还会进行结果筛选——他们保留共同信号轮次（$m_a = m_b =$

0）当且仅当登记并由*Charlie*公布测量结果 $\varkappa = -$ 时。请注意，结果筛选后保留的信号轮次将用于提取密钥比特。

在一次共同的测试轮次 ($m_{a(b)} = 1$)中，*Alice*和*Bob* 公布各自的强度$\mu_{a(b)}$、各自的 相位$\theta_{a(b)}$ 和$\omega_{a(b)}$，以及各自选择发送 还是不发送 （*Alice* 和*Bob* 由此确定本轮的情形——**sns**、**nn**或**ss**情形）。*Alice* 和*Bob* 还会执行场景筛选 （仅保留**sns** 情形），如前所述。经场景筛选后保留的所有测试轮次，均参与参数估计过程。

步骤*5*。 参数估计——这里我们采用 量子信道层析 [10], 以评估窃听者对以下各项的影响： $|e^{i\varphi_a}\sqrt{\mu}\rangle$、$e^{i\tau_a}\sqrt{\mu}\rangle_{QT}$ 和$|e^{i\varphi_b}\sqrt{\mu}\rangle$，$e^{i\tau_b}\sqrt{\mu}\rangle_{Q'T'}$ 相干态对。根据 步骤*3* 和步骤*4* 中与测试轮次相关的公告，***Alice*** 和Bob 估算窃听者（*Eve*）从协议中传输的相干态中获取的信息量。如果*Eve* 获取的信息超过某一阈值，那么*Alice* 和 *Bob* 将终止协议 [10]。否则，他们将继续执行后续步骤。

步骤 *6*。建立密钥比特——给定一个共同信号轮次以及公布的测量结果 $\varkappa = -$，*Alice* 和*Bob* 分别根据以下表达式建立各自的原始密钥比特 k 和 y

$$k = \begin{cases} 0, \ sending \\ 1, \ not \ sending \end{cases} \quad ; \quad y = \begin{cases} 0, \ sending \\ 1, \ not \ sending \end{cases} . \ (1)$$

也就是说，$k \equiv y$ 是*Alice* 和*Bob* 共享关联密钥比特的必要条件。请注意，公布的测量结果$\varkappa = -$ 表示 k和 y之间存在布尔反转关系——当 $\varkappa = -$发生时（$y \to y$），Bob 会反转其密钥比特 y。

步骤 *7*。*Alice* 和*Bob* 对各自的原始密钥进行纠错和隐私放大，以提取共同的密钥。

B. 采用相位随机化的 SNS-PM-QKD

为与 SNS-QKD 框架保持一致， [11,12], 下面介绍一种采用相位随机化的 SNS-PM-QKD 协议。该协议基于图2所示的装置，该装置是对图1的略微修改。协议包含以下步骤。

步骤 *1′*。此步骤与步骤 *1*相同。

步骤 *2′*。态制备——在测试轮次中，***Alice*** （*Bob*）以概率 ϵ 选择是否向*Charlie* 发送相干态（包括测试态和辅助态（或参考态））。如果*Alice* （*Bob*）选择向*Charlie*发送相干态，她（他）就制备一个测试相干态$|e^{i\omega_a}\sqrt{\mu_a}\rangle$ ($|e^{i\omega_b}\sqrt{\mu_b}\rangle$) 和一个辅助态（或参考）相干态 $|e^{i\theta_a}\sqrt{\mu_a}\rangle$ ($|e^{i\theta_b}\sqrt{\mu_b}\rangle$)，其中 $\theta_{a(b)} \in [0, 2\pi)$、$\omega_{a(b)} \in [0, 2\pi)$ 和 $\mu_{a(b)}$ 均为随机选取。

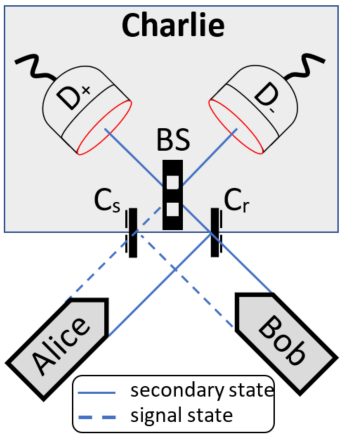

图1. SNS-PM-QKD 的示意装置。 *Alice* (*Bob*)独立选择发送或不发送 *her* (*his*)信号态和辅助相干态给第三方 *Charlie*。 *He* 对来自耦合器 C_s 和 C_r的相干态进行 *joint* (*beam splitter*) *measurement* 。耦合器的输出为：1） *Alice*和 *Bob*的信号态（C_s的输出）之间的干涉，以及 *Alice*和*Bob*的辅助态（参考态）（C_r的输出）之间的干涉——*sending-sending* 发送—发送（ss）情形；或 2） *Alice*的信号态（C_s的输出）和 *Alice's* 的次级态（C_r的输出）——*sending-not sending* (sns)情形；或 3） *Bob*的信号态（C_s的输出）和 *Bob*的次级态（C_r的输出）——*notsending-sending* (sns)情形；或 4）无输出（C_s 和 C_r 均不输出相干态）——*not sending-not sending* (不发送—不发送（nn）)情形。接下来， *Charlie* 公开宣布测量结果。BS——平衡分束器；D——单光子探测器；C——耦合器。

在信号轮次中，*Alice* （*Bob*）以概率 ϵ选择是否向*Charlie* 发送相干态（包括信号态和辅助态）。如果*Alice* （*Bob*）选择向 Charlie 发送相干态，她（他）就制备一个信号相干态 $|e^{i\nu_a}\sqrt{\mu}\rangle_Q$ ($|e^{i\nu_b}\sqrt{\mu}\rangle_{Q'}$) 和一个辅助态（或参考）相干态 $|e^{i\nu_a}\sqrt{\mu}\rangle_T$ ($|e^{i\nu_b}\sqrt{\mu}\rangle_{T'}$)，其中 ν_a，$\nu_b \in [0, 2\pi)$] 是彼此独立地随机选取的。 ν_a （ν_b）的选择方式如下。*Alice* （*Bob*）随机选取两个不相交相位区间 $[0, \pi)$ 或 $[\pi, 2\pi)$ 中的一个。随后，她（他）从选定的区间中随机选取一个相位，并将其赋给 ν_a （ν_b）。*Alice* 的相位区间记为 Δ_a，*Bob* 的相位区间记为 Δ_b。注意，$\max(|\nu_a - \nu_b|) = \pi$。

步骤 *3′*. 测量——Alice 和 Bob 将他们的相干态（信号/测试态和次级态）发送到中间节点 Charlie。在 Charlie 一侧的入口处，无论是测试轮次还是信号轮次，Alice 和 Bob 的信号/测试相干态都在耦合器 C_s 处发生干涉，而 Alice 和 Bob 的次级相干态则在耦合器 C_r 处发生干涉：C_s 的输出态为 $|e^{i\nu_a}\sqrt{\mu} - e^{i\nu_b}\sqrt{\mu}\rangle$；$C_s$ 的输出态为 $|e^{i\nu_a}\sqrt{\mu} - e^{i\nu_b}\sqrt{\mu}\rangle$。在此协议中（见图2），Alice 和 Bob 的次级相干态在干涉过程中互换；请参见步骤3，并对照图1和图2进行验证。

耦合器中的干涉过程详见附录 A。随后，耦合器的输出（即上述干涉过程的结果）被导向分束器**BS**。在每一轮中，*Charlie* 执行一次联合（分束器）测量，该测量由 POVM 元素 $F^{\varkappa}$ [10]表征。他公布测量结果 $\varkappa \in \{+,-,?\ d\}$，其中“+”表示仅探测器 D_+检测到点击，“–”表示仅探测器 D_-检测到点击，“?”表示探测器未检测到点击，而“*d*”表示两个探测器均检测到点击 [10]。

步骤 $1'$–$3'$ 重复 N 次（$N \to \infty$），考虑渐近区间的运行方式。

步骤 $4'$。公开通信和筛选—在此步骤中，通过经认证的公开经典信道公开信息。*Alice* 和*Bob*首先宣布他们的 m_a、 m_b值—他们 进行轮次类型 筛选。接下来，对于一个共同信号轮次，*Alice* 和*Bob* 宣布他们的 相位区间 Δ_a 和Δ_b—他们 进行相位区间 筛选。当存在一个共同信号 轮次（$m_{a(b)} = 0$）和一个共同相位区间 （$\Delta_a = \Delta_b$）时，如果且仅当*Charlie*记录并随后宣布了测量结果 $\varkappa = -$，Alice 和 Bob 还会进行结果筛选—他们 保留共同信号轮次（$m_a = m_b = 0$）和共同的相位区间选择。请注意，结果筛选后保留的信号轮次用于提取密钥比特。

在共同的测试轮次（$m_{a(b)} = 1$）中，*Alice*和*Bob* 宣布各自的强度$\mu_{a(b)}$、相位$\theta_{a(b)}$ 和$\omega_{a(b)}$，以及选择发送还是不发送（因此，*Alice* 和*Bob* 确定了该轮次的情形——**sns**、**nn**或**ss** 情形）。他们随后进行情形筛选（仅保留 **sns** 情形），如前文所述。情形筛选后保留的所有测试轮次均用于参数估计过程。

步骤 $5'$。此步骤与步骤 *5*相同。步骤 $6'$。此步骤与步骤 *6*相同。步骤 $7'$。此步骤与步骤 *7*相同。

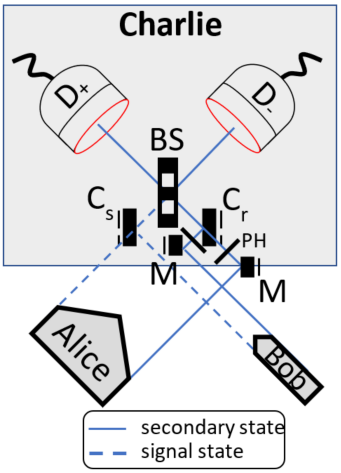

图2。采用相位随机化的 SNS-PM-QKD 示意性装置。 *Alice* （*Bob*）独立选择发送或不发送 *her* （*his*）信号态和辅助相干态给第三方 *Charlie*。 *He* 对来自耦合器 C_s 和 C_r 的相干态进行 *joint* （*beam splitter*） *mea-surement*。耦合器的输出为：1）*Alice*的信号态与 *Bob*的信号态发生干涉（C_s的输出），以及 *Alice*的辅助（参考）态与 *Bob*的辅助（参考）态发生干涉（C_r的输出）——*sending-sending* ss 情形；或 2） *Alice*的信号态（C_s的输出）和 *Alice's* 辅助态（C_r的输出）——*sending-not sending* （sns）情形；或 3） *Bob*的信号态（C_s的输出）和 *Bob*的辅助态（C_r的输出）——*not sending-sending* （sns）情形；或 4）无输出（C_s 和 C_r 均不输出相干态）——（nn）情形。在上述示意图中， *Alice* 和 *Bob* 的辅助态通过反射镜 M 和相移 PH 交换位置，相移为 π [弧度]。需要注意的是，PH 的作用是抵消相干态从反射镜反射时所产生的相移。进行确定性测量后， *Charlie* 公开宣布相应的测量结果。BS——平衡分束器；D——单光子探测器；C_x——耦合器（x = r——辅助（参考）态耦合器；x = s——信号态耦合器）；M——反射镜；PH—— π [弧度]的相移。

为了获取由*Alice*和*Bob*建立的密钥比特的信息，窃听者（Eve）应当了解发送或不发送配置（场景）。我们考虑一种*POVM* 攻击[10]；见图3——*Eve* 观察在$F^{\varkappa}$ Charlie一侧（中间节点）执行的联合测量结果。

如果窃听者（*Eve*）只能访问该方案的中间节点，那么所提出协议的安全性分析可沿用文献 [10] 中的分析。在这种情况下，*Eve* 只能观测耦合器之后的状态（分束器的输入态）。根据这些状态，*Eve* 无法获得由*Alice* 和*Bob*建立的密钥比特——仅观测测量结果时，她无法获知*Alice* 和*Bob* 的发送或不发送 情形（该情形决定密钥比特的值） $\varkappa$。SNS-PM-QKD（以及带随机化的 SNS-PM-QKD）的安全性（安全性证明）与文献中所述的完全相同

III. 安全性

A. 安全性证明

本节针对渐近运行区间（无限密钥极限）下的集体攻击，对所提出的协议（第II节）进行安全性证明。本文采用了参考文献 [10]中的安全性证明框架。安全性证明包括应用所谓的源替换方案、应用完全正迹保持映射并执行正算符值测量（发起攻击），进而评估密钥生成率。

。 [10] 当*Eve* 仅限于观测测量结果时。

注。下文给出的安全性证明针对 SNS-PM-QKD（第 II A节）进行表述；不过，只要同时考虑相位区间选择及其相应的筛选过程，该证明也适用于此协议的相位随机化变体（第 IIB节）。相位区间筛选只影响安全性证明所得密钥率的整体缩放，也就是说，它引入了一个乘法因子 s，如式 45 （仅损耗情形）和式 62所示。

下面给出一些预备知识

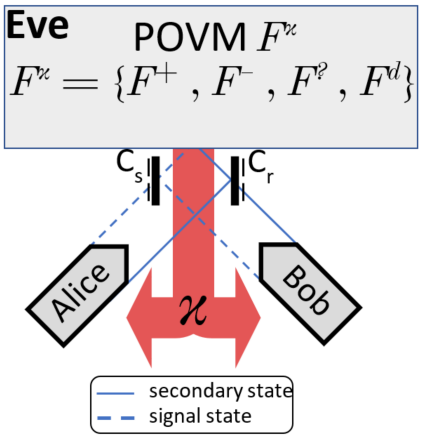

图 3. SNS-PM-QKD 示意装置中的 *POVM attack* 模型。该攻击符合参考文献 [10]。*Eve* 对来自耦合器输出端的相干态实施 POVM $F^{\varkappa}$。 *Eve* 公开宣布测量（POVM）结果 $\varkappa \in \{+, -, ?, d\}$（$+$ 表示探测器 D_+ 发生点击（见图 1）； $-$ 表示探测器 D_- 发生点击（见图 1）；？ 表示所有探测器均未发生点击；d 表示两个探测器均发生点击）。 δ—相位失配； η_t—量子信道透射率；C_x—耦合器（$x = r$—参考态耦合器；$x = s$—信号态耦合器）。

行。在 SNS-PM-QKD 中，*Alice* 根据先验概率分布 $\{p_w\}$ 选择发送（$w = 0$）或不发送（$w = 1$）信号 $|\varphi\rangle_Q$ 和参考 $|\tau\rangle_T$ 相干态——该选择记录在经典寄存器A 中，其状态 $\{|w\rangle_A\}$ 构成一个正交归一基。*Alice* 的信号态和次级态根据先验概率分布 $\{p_u\}$，按照轮次类型 $u \in \{Z, X\}$ （Z→信号轮，X→测试轮）制备——轮次类型的选择记录在经典寄存器 U 中，其状态 $\{|u\rangle_U\}$ 构成一个正交归一基。因此，信号 $|\varphi\rangle_Q$ 和参考 $|\tau\rangle_T$ 相干态取决于发送或不发送选择和轮次类型选择，即也就是$|\varphi_{w,\ u}\rangle_Q$ 和$|\tau_{w,\ u}\rangle_T$。 随后，*Alice*的源在源替换方案 [10, 21]中由以下状态表征

$$|\psi\rangle_{AUQT} = \sum_{w,u} \sqrt{p_w}\sqrt{p_u}\,|w\rangle_A\,|u\rangle_U\,|\varphi_{w,u}\rangle_Q\,|\tau_{w,u}\rangle_T\,. \quad (2)$$

在所提出的协议中，*Bob* 根据先验概率分布 $\{q_y\}$选择发送（$y = 0$）或不发送（$y = 1$）信号$|\varphi\rangle_{Q'}$和参考 $|\tau\rangle_{T'}$相干态——该选择记录在经典寄存器B 中，其状态 $\{|y\rangle_B\}$ 构成一个正交归一基。*Bob* 的信号态和次级态根据先验概率分布 $\{q_v\}$，按照轮次类型 $v \in \{Z, X\}$ （Z→信号轮，X→测试轮）制备——轮次类型的选择记录在经典寄存器 V 中，其状态 $\{|v\rangle_V\}$ 构成一个正交归一基。因此，信号 $|\varphi\rangle_{Q'}$和参考 $|\tau\rangle_{T'}$相干态取决于发送或不发送选择和轮次类型选择，即也就是$|\varphi_{y,\ v}\rangle_{Q'}$和$|\tau_{y,\ v}\rangle_{T'}$。 随后，*Bob*的源在源替换方案 [10, 21]中由以下状态表征

$$|\psi\rangle_{BVQ'T'} = \sum_{y,v} \sqrt{q_y}\sqrt{q_v}\,|y\rangle_B\,|v\rangle_V\,|\varphi_{y,v}\rangle_T\,|\tau_{y,v}\rangle_{T'}\,. \quad (3)$$

*Alice*和*Bob*的光源整体态为

$$\begin{aligned}|\Psi\rangle_{ABUVQTQ'T'} &= |\psi\rangle_{AUQT} \otimes |\psi\rangle_{BVQ'T'} \\ &= \sum_{w,u,y,v} \sqrt{p_w p_u q_y q_v}\,|w,y\rangle_{AB}\,|u,v\rangle_{UV}\,|\varphi_{w,u},\varphi_{y.v}\rangle_{QQ'} \otimes \\ &\quad |\tau_{w,u},\tau_{y,v}\rangle_{TT'}\end{aligned} \quad (4)$$

请注意，*Eve* 无法访问上述任何经典寄存器——既无法访问*Alice*的寄存器，也无法访问*Bob*的寄存器。请注意，系统 Q、 Q'、 T和 T'被发送给*Charlie* (*Eve*)。根据图 3，在到达分束器（它们的最终目的地）之前，系统 QQ' 应经过耦合器$\mathbf{C_s}$，系统 TT' 应经过$\mathbf{C_r}$。如附录$\mathbf{C_s}$所示，其操作A由以下变换表征

$$|\varphi_{w,u},\varphi_{y,v}\rangle_{QQ'} \mapsto \left|\varphi_{w,u} - \mathrm{e}^{i\delta}\sqrt{V}\varphi_{y,v}\right\rangle_{A'} = |\varphi_{w,y,u,v}\rangle_{A'} \quad (5)$$

δ 表示耦合器处系统 Q和 Q' 的状态之间的相位失配，而 V 表示这些状态之间的强度（模式）失配。类似地，$\mathbf{C_r}$的操作由以下变换表征

$$|\tau_{w,u},\tau_{y,v}\rangle_{TT'} \mapsto \left|\tau_{y,v} - \mathrm{e}^{i\delta}\sqrt{V}\tau_{w,u}\right\rangle_{B'} = |\tau_{w,y,u,v}\rangle_{B'} \quad (6)$$

请注意，在不发生干涉的情况下（发送—不发送情形），或考虑理想（仅有损耗）情形时，上述表达式中的 $\delta = 0$ 和 $V = 1$ 。因此，经过耦合器 $\mathbf{C_s}$ 和$\mathbf{C_r}$后，整体态$|\Psi\rangle_{ABUVQTQ'T'}$变为

$$\begin{aligned}|\Psi\rangle_{ABUVQTQ'T'} &\mapsto |\Psi\rangle_{ABUVA'B'} \\ &= \sum_{w,u,y,v} \sqrt{p_w p_u q_y q_v}\,|w,y\rangle_{AB}\,|u,v\rangle_{UV}\,|\varphi_{w,y,u,v}\rangle_{A'} \otimes \\ &\quad |\tau_{w,y,u,v}\rangle_{B'}\end{aligned} \quad (7)$$

Eve 的攻击Eve 由一个完全正迹保持映射刻画 $\mathcal{E}_{A'B'\to EC}$ [10]定义如下

$$\mathcal{E}_{A'B'\to EC}(\rho)=\sum_{\varkappa} p_{\varkappa}(\sqrt{F^{\varkappa}}\rho\sqrt{F^{\varkappa}})_E\otimes|\varkappa\rangle\langle\varkappa|_C \tag{8}$$

其中 $\varkappa$ 表示被公布的测量结果，经典寄存器 C 记录该测量结果，并且 $F^{\varkappa}$ 是用于对系统 $A'B'$ [10] [进行测量的*POVM*算符。注：POVM算符 $F^{\varkappa}$ （与本工作相关）的矩阵表示见附录B]。应用于系统$ABUVA'B'$，该映射得到如下结果

$$\begin{aligned}\rho_{ABUVEC}&=(I_{ABUV}\otimes\mathcal{E}_{A'B'\to EC})(|\Psi\rangle\langle\Psi|_{ABUVA'B'})\\&=\sum_{w,u,y,v,w',u',y',v'}\sqrt{p_w p_u p_{w'} p_{u'} q_y q_v q_{y'} q_{v'}}\,|w,y\rangle\langle w',y'|_{AB}\,|u,v\rangle\langle u',v'|_{UV}\otimes\\&\sum_{\varkappa}(\sqrt{F^{\varkappa}}\,|\varphi_{w,y,u,v},\tau_{w,y,u,v}\rangle\langle\varphi_{w',y',u',v'},\tau_{w',y',u',v'}|\,\sqrt{F^{\varkappa}})_E\otimes|\varkappa\rangle\langle\varkappa|_C\end{aligned} \tag{9}$$

按照协议步骤（第 IIA 节），*Alice* 和Bob 应先执行轮次类型筛选 和测量结果筛选，然后再进行密钥蒸馏（执行密钥映射）。轮次类型筛选包括公布变量 u和v，并丢弃满足 $u\neq v$ 的轮次。这些操作通过应用如下形式的算子来表征：

form

$$\begin{aligned}\Pi_{\text{round}}&=I_{ABEC}\otimes|u=v,v=u\rangle\langle u=v,v=u|_{UV}\\&=I_{ABEC}\otimes|u,u\rangle\langle u,u|_{UV}\,.\end{aligned} \tag{10}$$

请注意，只有 $u=v=Z$ 这一情形用于密钥生成，参见第 IIA 节的协议步骤。因此

$$\begin{aligned}\Pi_{\text{round}}(\rho_{ABUVEC})\Pi_{\text{round}}&=\rho'_{ABUVEC}\\&=\sum_{w,y,w',y'}p_{u=Z,v=Z}\sqrt{p_w p_{w'} q_y q_{y'}}\,|w,y\rangle\langle w',y'|_{AB}\,|Z,Z\rangle\langle Z,Z|_{UV}\otimes\\&\sum_{\varkappa}(\sqrt{F^{\varkappa}}\,|\varphi_{w,y,Z,Z},\tau_{w,y,Z,Z}\rangle\langle\varphi_{w',y',Z,Z},\tau_{w',y',Z,Z}|\,\sqrt{F^{\varkappa}})_E\otimes|\varkappa\rangle\langle\varkappa|_C\end{aligned} \tag{11}$$

其中 $p_{u=Z,\ v=Z}=p_{u=Z}q_{v=Z}=\sqrt{p_{u=Z}p_{u'=Z}q_{v=Z}q_{v'=Z}}$。考虑到运行处于渐近区间，

可以选择 $p_{u(v)=Z}\to 1$ $p_{u=Z\ v=Z}\to 1$ $p_{u(v)=X}\to$ （因此，）。这意味着 0. 从而

$$\begin{aligned}&\rho'_{ABUVEC}\\&=\sum_{w,u,y,w',y'}\sqrt{p_w p_{w'} q_y q_{y'}}\,|w,y\rangle\langle w',y'|_{AB}\,|Z,Z\rangle\langle Z,Z|_{UV}\otimes\\&\sum_{\varkappa}(\sqrt{F^{\varkappa}}\,|\varphi_{w,y,Z,Z},\tau_{w,y,Z,Z}\rangle\langle\varphi_{w',y',Z,Z},\tau_{w',y',Z,Z}|\,\sqrt{F^{\varkappa}})_E\otimes|\varkappa\rangle\langle\varkappa|_C\end{aligned} \tag{12}$$

测量结果筛选包括公布变量 $\varkappa$ 并丢弃满足 $\varkappa\neq-$ 的轮次。这些操作通过应用如下形式的算子来表征

$$\Pi_{\text{outcome}}=I_{ABUVE}\otimes|\varkappa=-\rangle\langle\varkappa=-|_C\,. \tag{13}$$

回顾一下，只有 $\varkappa=-$ 这一情形用于密钥生成；参见第 II节的协议步骤。因此

$$\begin{aligned}\Pi_{\text{outcome}}(\rho'_{ABUVEC})\Pi_{\text{outcome}} &= \rho''_{ABUVEC}\\ &= \sum_{w,y,w',y'} \sqrt{p_w p_{w'} q_y q_{y'}}\, |w,y\rangle\langle w',y'|_{AB} |Z,Z\rangle\langle Z,Z|_{UV} \otimes \\ &(\sqrt{F^-}\,|\varphi_{w,y,Z,Z},\tau_{w,y,Z,Z}\rangle\langle\varphi_{w',y',Z,Z},\tau_{w',y',Z,Z}|\sqrt{F^-})_E \otimes |\varkappa=-\rangle\langle\varkappa=-|_C\end{aligned} \tag{14}$$

现在我们继续安全性证明的第三部分，即评估密钥生成率。与文献[10]，评估密钥率的方法类似，我们首先对 ρ''_{ABUVEC} 应用密钥映射，然后采用Devetak-Winter公式[22]。为生成密钥比特，Alice 和 Bob 分别执行正算子值测度 M_A 和 M_B——Alice 对系统 A执行测量 M_A (M_A ={$|w\rangle\langle w|$})，而 Bob 执行测量M_B (M_B = {$|y\rangle\langle y|$})。 M_A (M_B)的测量结果存储在寄存器 W (Y)中。随后对系统 W应用密钥映射 $\mathcal{K}$ 。该映射是平凡的，其特征由以下变换给出

$$\mathcal{K}_{A\to K}(\rho_W) = I_W(|w\rangle\langle w|_W)I_W = |k\rangle\langle k|_K\,. \tag{15}$$

与参考文献 [10]，类似，执行一个完全正迹保持映射 $\mathcal{G}$，该映射由正算子值测度 M_A、 M_B 和密钥映射 $\mathcal{K}$ 组合而成。将 $\mathcal{G}$ 应用于 ρ''_{ABUVEC} 的结果为

$$\begin{aligned}&\rho_{KYUVEC}\\ &= \sum_{k,y} \times p_{\varkappa=-} p_{k,y|\varkappa=-}\, |k\rangle\langle k|_K \otimes |y\rangle\langle y|_Y \otimes\\ &|Z,Z\rangle\langle Z,Z|_{UV} \otimes \rho_E^{k,y,\varkappa,u,v} \otimes |\varkappa=-\rangle\langle\varkappa=-|_C\\ &= \sum_{k,y} \times p_{\varkappa=-} p_{k,y|\varkappa=-}\, |k\rangle\langle k|_K \otimes |y\rangle\langle y|_Y \otimes\\ &|Z,Z\rangle\langle Z,Z|_{UV} \otimes \rho_E^{k,y,-,Z,Z} \otimes |\varkappa=-\rangle\langle\varkappa=-|_C\,.\end{aligned} \tag{16}$$

$p_{\varkappa=-}$ 和 $p_{k、\ y|\varkappa=-}$ 的乘积给出联合分布 $p_{k、\ y、\ \varkappa=-} = p_{\varkappa=-} \times p_{k、\ y|\varkappa=-}$。

Devetak-Winter公式 [22] 用于确定集体攻击下量子密钥分发协议的密钥率。对于 SNS-PM-QKD，Devetak-Winter公式应用于由*Alice*、*Bob*和*Eve*[10]共享的状态 ρ_{KYUVEC}。系统 $KYUVEC$ 的状态可改写为

$$\begin{aligned}&\rho_{KYUVEC}\\ &= p_{\varkappa=-} \times \rho_{KYE}^{\varkappa,u,v} \otimes |Z,Z\rangle\langle Z,Z|_{UV} \otimes |\varkappa=-\rangle\langle\varkappa=-|_C\\ &= p_{\varkappa=-} \times \rho_{KYE}^{-,Z,Z} \otimes |Z,Z\rangle\langle Z,Z|_{UV} \otimes |\varkappa=-\rangle\langle\varkappa=-|_C\end{aligned} \tag{17}$$

其中，*Alice*、*Bob*和*Eve*共享的条件态

$$\rho_{KYE}^{-,Z,Z} = \sum_{k,y} p_{k,y|\varkappa=-}\, |k\rangle\langle k|_K \otimes |y\rangle\langle y|_Y \otimes \rho_E^{k,y,-,Z,Z} \tag{18}$$

取决于公告 $\varkappa$、 u 和 v。根据 Devetak-Winter公式 [22]，在给定公告 $\varkappa$、 u 和 v 的情况下，可生成的密钥比特数可从 ρ^-_{KYE} 中建立，为 [10]

$$\begin{aligned}r(\rho_{KYE}^{-,Z,Z}) &= I(K:Y)_{\rho_{KYE}^{-,Z,Z}} - I(K:E)_{\rho_{KYE}^{-,Z,Z}}\\ &= 1 - \delta_{\text{EC}}^{-,Z,Z} - \chi(K:E)_{\rho_{KYE}^{-,Z,Z}}\end{aligned} \tag{19}$$

其中， $\delta^{-,\ Z,\ Z}_{\text{EC}}$ [23] 是量子密钥分发纠错过程中公告 $\varkappa=-$、 $u=Z$ 和 $v=Z$ 所对应的平均信息泄漏量。该数量通过以下方式计算：

$$\delta_{\text{EC}}^{-,Z,Z} = f_{\text{EC}} H(e^{-,Z,Z}) \tag{20}$$

f_{EC} 表示纠错过程的效率 $e^{-,\ Z,\ Z}$ 表示在（$\varkappa$， u， v）=（−， Z， Z）情况下的错误率，而 H（·）是所谓的香农熵。数量 χ（K： E）$_{\rho^{-,\ Z\ Z}_{KYE}}$ 是定义为下式的*Holevo*信息

$$\begin{aligned}\chi(K:E)_{\rho_{KYE}^{\varkappa,u,v}} &= S(\rho_E^{\varkappa,u,v}) - \sum_k p_{k|\varkappa,u,v} \times S(\rho_E^{k,\varkappa,u,v})\\ &= S(\rho_E^{-,Z,Z}) - \sum_k p_{k|-,Z,Z} \times S(\rho_E^{k,-,Z,Z})\end{aligned} \tag{21}$$

其中， S（ρ）表示所谓的冯·诺依曼（量子）熵。注意，[10]

$$\begin{aligned}\rho_E^{k,-,Z,Z} &= \sum_y p_{y|k,-,Z,Z} \times \rho_E^{k,y,-,Z,Z},\\ \rho_E^{-,Z,Z} &= \sum_k p_{k|-,Z,Z} \times \rho_E^{k,-,Z,Z}.\end{aligned} \tag{22}$$

状态 $\rho^{k,\ y-\ Z\ Z,\ ,\ ,}_{E}$ 表示为

$$\rho_E^{k,y,-,Z,Z} = \left|\Theta_{k,y}^{-,Z,Z}\right\rangle\left\langle\Theta_{k,y}^{-,Z,Z}\right| \tag{23}$$

根据下式（9）[10]。Eve的条件态 $\left|\Theta^{-,\ \ Z\ Z,\ ,\ ,\ y}_{k}\right\rangle$ 定义为

$$\left|\Theta_{k,y}^{-,Z,Z}\right\rangle = \frac{\sqrt{F^-}\,|\varphi_{k,y,Z,Z},\tau_{k,y,Z,Z}\rangle}{\sqrt{\langle\varphi_{k,y,Z,Z},\tau_{k,y,Z,Z}|\,F^-\,|\varphi_{k,y,Z,Z},\tau_{k,y,Z,Z}\rangle}} \tag{24}$$

密钥比特的总数量，即 Alice 和 *Bob*基于 ρ_{KYUVEC}能够建立的密钥比特数量，由 [10]给出

$$\begin{aligned}R(\rho_{KYUVEC}) &= \sum_{\varkappa,u,v} p_{\varkappa,u,v} \times r(\rho_{KYE}^{\varkappa,u,v})\\ &= p_{\varkappa=-,Z,Z} \times r(\rho_{KYE}^{-,Z,Z}).\end{aligned} \tag{25}$$

B. 安全问题

本节分析一种针对所提出的协议的特定攻击，称为双 POVM 攻击。Eve 发动这种攻击，旨在获知 Alice 和 Bob 双方的发送或不发送选择。图 4 所示的方案展示了双 POVM 攻击。如图所示，在这种攻击中，Eve 对 Alice 的相干态执行 POVM $F^{\varkappa'}$，并对 Bob 的相干态执行 POVM $F^{\varkappa''}$。根据测量结果 $\varkappa'$ 和 $\varkappa''$，Eve 决定公告 $\tilde{\varkappa}$—$\tilde{\varkappa}=f(\varkappa',\varkappa'')$。请注意，在双 POVM 攻击中，Eve 试图尽可能精确地复制 POVM 攻击（图 3）中的公告部分。

攻击的成功取决于在观测 $[\varkappa'=+,\varkappa''=?]$或 $[\varkappa'=?,\varkappa''=+]$ 发生时，区分**sns** 与**ss**（或 **nn**）情形。换言之，该攻击的特征在于区分**sns** 与**ss** （或 **nn**）的错误概率，$e_{\text{distinguish}}$—$e_{\text{distinguish}}$ 实际上是*Eve* 实施双 POVM 攻击所引入的错误率。下文将确定错误概率，以验证双 POVM 攻击是否能够被*Alice* 和*Bob*检测到。需要注意的是，**sns** 会使*Alice* 和*Bob* 共享关联密钥比特，而**ss** （或**nn**）会使*Alice* 和*Bob* 共享反关联密钥比特——**ss** （或**nn**）会引入错误。我们在两种情形下考察 $e_{\text{distinguish}}$ ： 仅损耗 和现实 情形。

仅损耗情形。为找出 $e^{\text{loss-only}}$ 区分，我们分别考察在给定**sns** 的情况下，以及在给定**ss** 的情况下，获得观测 $[\varkappa'=+,\varkappa''=?]$ [24] 的概率。需要注意的是，在考虑仅损耗情形时，对于**nn** 配置，观测$[\varkappa'=+,\varkappa''=?]$ 不可能发生。我们假设*Alice*和*Bob*共享一个共同信号轮次。给定 $[\varkappa'=+,\varkappa''=?]$, , **sns** 情形的特征是*Alice* 向中间节点发送相干态，而*Bob* 不发送相干态。在**sns**情形下，获得所关注观测的概率可由以下乘积求得

$$\begin{aligned}
&p^{\mathbf{sns(loss)}}_{\varkappa'=+,\varkappa''=?}=[p_{\text{sending}}\times p_{\varkappa'=+|\text{sending}}]\times\\
&[p_{\text{not-sending}}\times p_{\varkappa''=?|\text{not-sending}}] \qquad (26)\\
&=[\epsilon\times\langle+\sqrt{\mu},+\sqrt{\mu}|\,F^{+'}\,|+\sqrt{\mu},+\sqrt{\mu}\rangle]\times[(1-\epsilon)\times 1]\\
&=[\epsilon\times\langle+\sqrt{\mu},+\sqrt{\mu}|\,F^{+'}\,|+\sqrt{\mu},+\sqrt{\mu}\rangle]\times(1-\epsilon)
\end{aligned}$$

注意到 $p_{\varkappa'=?\ |\text{不发送}}=1$ 在仅损耗情形下。该 POVM 算子 $F^{+'}$ 见附录 B。回想一下，在信号轮次中，*Alice*的相干态形式为 $\left|\mathrm{e}^{i\varphi_a}\sqrt{\mu},\ \mathrm{e}^{i\tau_a}\sqrt{\mu}\right\rangle_{QT}=\left|+\sqrt{\mu},\ +\sqrt{\mu}\right\rangle$。

给定 $[\varkappa'=+,\varkappa''=?]$, 发送—发送（ss）情形的特点是*Alice* 和*Bob* 均向中间节点发送相干态。在**发送—发送（ss）**情形下，所关注观测结果的概率由乘积给出

$$\begin{aligned}
&p^{\mathbf{ss(loss)}}_{\varkappa'=+,\varkappa''=?}\\
&=[p_{\text{sending}}\times p_{\varkappa'=+|\text{sending}}]\times[p_{\text{sending}}\times p_{\varkappa''=?|\text{sending}}]\\
&=[\epsilon\times\langle+\sqrt{\mu},+\sqrt{\mu}|\,F^{+'}\,|+\sqrt{\mu},+\sqrt{\mu}\rangle]\times\\
&[\epsilon\times\langle+\sqrt{\mu},+\sqrt{\mu}|\,F^{?''}\,|+\sqrt{\mu},+\sqrt{\mu}\rangle]
\end{aligned}\qquad (27)$$

该 POVM 算子 $F^{?''}$ 见附录 B。回想一下，在信号轮次中，*Bob*的相干态形式为 $\left|\mathrm{e}^{i\varphi_b}\sqrt{\mu},\ \mathrm{e}^{i\tau_b}\sqrt{\mu}\right\rangle_{Q'T'}=\left|+\sqrt{\mu},\ +\sqrt{\mu}\right\rangle$——它们与 *Alice*的相同。

因此，区分**sns** 和**ss**的错误概率可表示为

$$e^{\text{loss-only}}_{\text{distinguish}}=\min\{\tilde{p}^{\mathbf{sns(loss)}}_{\varkappa'=+,\varkappa''=?},\tilde{p}^{\mathbf{ss(loss)}}_{\varkappa'=+,\varkappa''=?}\} \qquad (28)$$

其中

$$\begin{aligned}
\tilde{p}^{\mathbf{sns(loss)}}_{\varkappa'=+,\varkappa''=?}&=\frac{p^{\mathbf{sns(loss)}}_{\varkappa'=+,\varkappa''=?}}{p^{\mathbf{sns(loss)}}_{\varkappa'=+,\varkappa''=?}+p^{\mathbf{ss(loss)}}_{\varkappa'=+,\varkappa''=?}},\\
\tilde{p}^{\mathbf{ss(loss)}}_{\varkappa'=+,\varkappa''=?}&=\frac{p^{\mathbf{ss(loss)}}_{\varkappa'=+,\varkappa''=?}}{p^{\mathbf{sns(loss)}}_{\varkappa'=+,\varkappa''=?}+p^{\mathbf{ss(loss)}}_{\varkappa'=+,\varkappa''=?}}
\end{aligned}\qquad (29)$$

我们绘制了 $e^{\text{loss-only}}$ 区分 随距离 L 变化的曲线，见图5。我们假设 ϵ 为常数（$\epsilon=0.05$）。图中显示，在实施双 POVM 攻击时，*Eve* 会在*Alice* 和*Bob* 的原始密钥中引入错误。因此，为了检测双 POVM 攻击，*Alice* 和*Bob* 需要牺牲部分他们的原始密钥比特，用于参数估计 过程——*Alice* 和*Bob* 评估量子信道的错误率。如果观测到非零错误率，他们就继续执行所提出协议的下一步（仅损耗情形）；否则，他们终止当前协议会话，并重新开始一个新的会话。

现实情形。为求得 $e^{\text{realistic}}_{\text{distinguish}}$，我们考察在**sns** 条件下获得观测 $[\varkappa'=+,\varkappa''=$ 的概率], 以及在**ss** （或**nn**）条件下获得该观测的概率。我们假设*Alice* 和*Bob*共享一个共同信号轮次。给定 $[\varkappa'=+,\varkappa''=,\ ]$, **sns**情形的特征是*Alice* 向中间节点发送相干态，而*Bob* 不发送相干态。在**sns** 情形下，获得所关注观测的概率可由以下乘积计算

$$\begin{aligned}
&p^{\mathbf{sns(real)}}_{\varkappa'=+,\varkappa''=?}=[p_{\text{sending}}\times p_{\varkappa'=+|\text{sending}}]\times\\
&[p_{\text{not-sending}}\times p_{\varkappa''=?|\text{not-sending}}]\\
&=[\epsilon\times\langle+\sqrt{\mu},+\sqrt{\mu}|\,F^{+'}_{\text{imp}}\,|+\sqrt{\mu},+\sqrt{\mu}\rangle]\times\\
&[(1-\epsilon)(1-p_{\text{dark}})^2]
\end{aligned}\qquad (30)$$

POVM 算子 $F^{+'}$ imp 见附录B。术语 $(1-p_{\text{dark}})^2$ 表示没有探测器在

当 Bob 不发送相干态时，给定一个 POVM $F^{\varkappa''}$。回想一下，在信号轮次中，$Alice$ 的相干态形式为 $|e^{i\varphi_a}\sqrt{\mu}, e^{i\tau_a}\sqrt{\mu}\rangle_{QT} = |+\sqrt{\mu}, +\sqrt{\mu}\rangle$。给定 $[\varkappa' = +, \varkappa'' = ?]$，，**发送—发送（ss）**情形的特点是$Alice$ 和Bob 都向中间节点发送相干态。另一方面，**不发送—不发送（nn）**情形的特点是$Alice$ 和Bob 都不向中间节点发送相干态。在**发送—发送（ss）**情形下，所关注观测的获取概率由以下乘积计算得出

$$\begin{aligned} & p^{\mathbf{ss(real)}}_{\varkappa'=+,\varkappa''=?} \\ & = [p_{\text{sending}} \times p_{\varkappa'=+|\text{sending}}] \times [p_{\text{sending}} \times p_{\varkappa''=?|\text{sending}}] \\ & = [\epsilon \times \langle +\sqrt{\mu}, +\sqrt{\mu}| F^{+'}_{\text{imp}} |+\sqrt{\mu}, +\sqrt{\mu}\rangle] \times \\ & [\epsilon \times \langle +\sqrt{\mu}, +\sqrt{\mu}| F^{?''}_{\text{imp}} |+\sqrt{\mu}, +\sqrt{\mu}\rangle] \end{aligned} \tag{31}$$

POVM 算子 $F^{?''}$ imp 见附录B。回顾一下，在信号轮次中，Bob的相干态形式为 $|e^{i\varphi_b}\sqrt{\mu}, e^{i\tau_b}\sqrt{\mu}\rangle_{QT'} = |+\sqrt{\mu}, +\sqrt{\mu}\rangle$——它们与$Alice$的相同。在不发送—不发送（nn）情形下，所关注观测的获取概率由以下乘积计算得出

$$\begin{aligned} & p^{\mathbf{nn(real)}}_{\varkappa'=+,\varkappa''=?} = [p_{\text{not-sending}} \times p_{\varkappa'=+|\text{not-sending}}] \times \\ & [p_{\text{not-sending}} \times p_{\varkappa''=?|\text{not-sending}}] \\ & = [(1-\epsilon) \times (1-p_{\text{dark}}) p_{\text{dark}}] \times [(1-\epsilon) \times (1-p_{\text{dark}})^2]. \end{aligned} \tag{32}$$

在“**发送—发送（ss）**（或**不发送—不发送（nn）**）”情形下，所关注观测的获取概率随后由下式计算：

$$p^{\mathbf{ss+nn(real)}}_{\varkappa'=+,\varkappa''=?} = p^{\mathbf{ss(real)}}_{\varkappa'=+,\varkappa''=?} + p^{\mathbf{nn(real)}}_{\varkappa'=+,\varkappa''=?} \tag{33}$$

因此，区分**sns** 与**发送—发送（ss）**（或**不发送—不发送（nn）**）的错误概率可通过以下方式计算：

$$e^{\text{realistic}}_{\text{distinguish}} = \min\{\tilde{p}^{\mathbf{sns(real)}}_{\varkappa'=+,\varkappa''=?}, \tilde{p}^{\mathbf{ss+nn(real)}}_{\varkappa'=+,\varkappa''=?}\} \tag{34}$$

其中

$$\begin{aligned} \tilde{p}^{\mathbf{sns(real)}}_{\varkappa'=+,\varkappa''=?} &= \frac{p^{\mathbf{sns(real)}}_{\varkappa'=+,\varkappa''=?}}{p^{\mathbf{sns(real)}}_{\varkappa'=+,\varkappa''=?} + p^{\mathbf{ss+nn(real)}}_{\varkappa'=+,\varkappa''=?}}, \\ \tilde{p}^{\mathbf{ss+nn(real)}}_{\varkappa'=+,\varkappa''=?} &= \frac{p^{\mathbf{ss+nn(real)}}_{\varkappa'=+,\varkappa''=?}}{p^{\mathbf{sns(real)}}_{\varkappa'=+,\varkappa''=?} + p^{\mathbf{ss+nn(real)}}_{\varkappa'=+,\varkappa''=?}} \end{aligned} \tag{35}$$

现在我们考察双 POVM 攻击的错误率 $e^{\text{realistic}}_{\text{distinguish}}$与 POVM 攻击（图 e^{-}）的错误率z, z 之间的比值。通过这样做，可以定量验证$Alice$ 和Bob 能否检测到双 POVM 攻击的存在。

显然，$e^{\text{realistic}}_{\text{distinguish}}$ 和 e^{-}, z, z 仅取决于 L，前提是协议参数 V，δ，η_{det}，p_{dark} 固定（参见方程（B1）—（B7））， 且 ϵ 固定或视为 L的函数。在图 6中，我们比较 $e_{\text{distinguish}}$ 与 e^{-}、z、z——错误概率在图中表示为 L 的函数。比值 $e^{\text{realistic}}_{\text{distinguish}}$： e^{-}、z、z 也绘制在该图中。该图表明，双 POVM 攻击导致的错误率（$e_{\text{distinguish}}$）明显大于错误率 e^{-}、z、z（POVM 攻击，图 3），这在 SNS-PM-QKD 以及带随机化的 SNS-PM-QKD 中均成立。因此可以推断，$Alice$ 与 Bob 能够通过观察错误率的数值察觉双 POVM 攻击的存在。

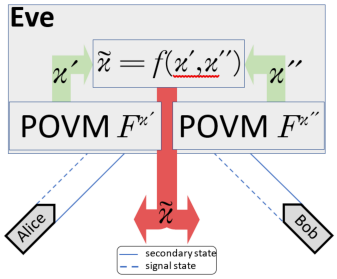

图 4. SNS-PM-QKD 示意装置中 $double\text{-}POVM\ attack$ 的模型。Eve 对 $F^{\varkappa'}$ 的 $Alice$相干态实施 POVM，并对 $F^{\varkappa''}$ 的 Bob相干态实施 POVM。根据这些 POVM 的测量结果 $\varkappa'$ 和 $\varkappa''$， Eve 决定 $\tilde{\varkappa}$的取值，即实际的结果公告。 Eve 旨在复制 POVM 攻击（图3）的结果公告。

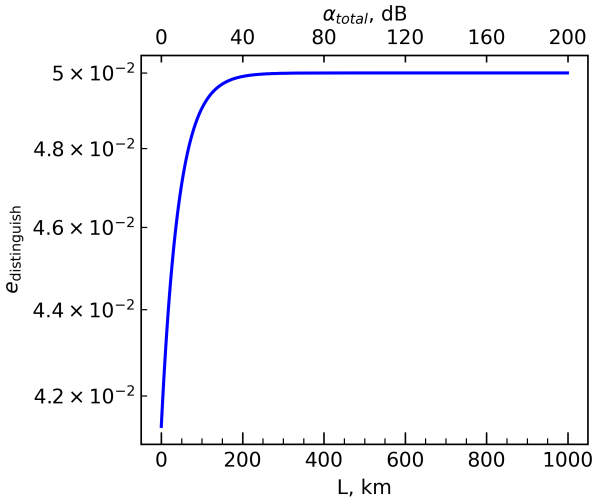

图 5. 错误率 $e^{\text{loss-only}}$ 区分 在 SNS-PM-QKD 的仅损耗操作下的双 POVM 攻击中。上述曲线针对以下协议参数进行评估：信道衰减 $\alpha = 0.2$dB，探测效率 $\eta_{\text{det}} = 1$，暗计数率 $p_{\text{dark}} = 10^{-11}$，模式（强度）失配 $V = 0.95$，相位失配 $\delta = \frac{\pi}{60}$，相干态强度 $\mu = 0.1$，以及发送概率函数 $\epsilon(L)$ 的形式如图 8 所示，其中 $\epsilon_0 = 0.05$，$\epsilon_{\max} = 0.45$，$L_{\max} = 950$km。

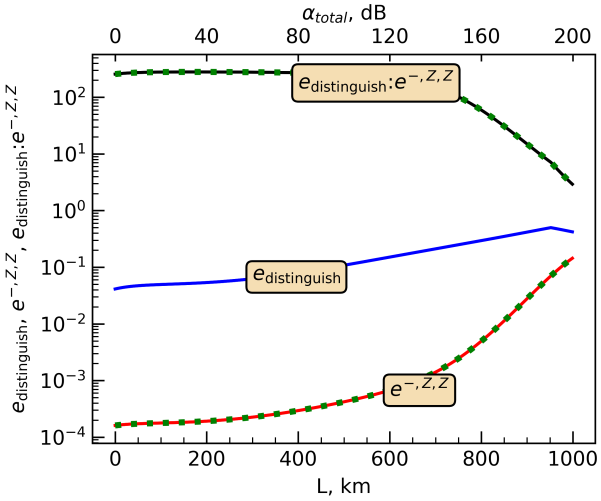

图 6. 在 SNS-PM-QKD（带随机化的SNS-PM-QKD）的实际运行条件下，比较 POVM 攻击中的错误率 $e^{-,z,z}$ 与双 POVM 攻击中的错误率 $e^{\text{realistic}}_{\text{distinguish}}$。这些错误率之间的差距用比值 $e^{\text{realistic}}_{\text{distinguish}}:e^{-,z,z}$定量表示。针对 SNS-PM-QKD（实线）和带随机化的 SNS-PM-QKD（绿色虚线），分别评估错误率及其比值。注意，$e^{\text{realistic}}_{\text{distinguish}}$ 在这两种协议中取相同的值。以上曲线对应的协议参数为：信道衰减 $\alpha = 0.2$dB、探测效率 $\eta_{\text{det}} = 1$、暗计数率 $p_{\text{dark}} = 10^{-11}$、模式（强度）失配 $V = 0.95$、相位失配 $\delta = \frac{\pi}{60}$、纠错效率 $f_{\text{EC}} = 1.1$、相干态强度 $\mu = 0.1$，以及形式如图8所示的发送概率函数 $\epsilon(L)$，其中 $\epsilon_0 = 0.05$, $\epsilon_{\max} = 0.45$ $L_{\max} = 950$ km。注意，参数 $e^{-,z,z}$, $e^{\text{realistic}}_{\text{distinguish}}$, $e^{\text{realistic}}_{\text{distinguish}}$: $e^{-,z,z}$之间的关系对于其他协议参数取值也成立（例如，$\alpha = 0.2$dB、$\eta_{\text{det}} = 0.145$, $p_{\text{dark}} = 8 \times 10^{-8}$, $V = 0.95$, $\delta = \frac{\pi}{8}$, $f_{\text{EC}} = 1.15$ $\mu = 0.1$ ϵ $L|\epsilon_0 = 0.05$ $\epsilon_{\max} = 0.45$ $L_{\max}$, , $^{-}$)).

IV. 数值模拟

A. 仅损耗情形

在本节中，我们确定 SNS-PM-QKD（以及带随机化的 SNS-PM-QKD）的密钥率，依据第 III 节的安全性证明，前提是量子信道 *Alice*-*Charlie* 与 *Bob*-*Charlie* 被视为有损无噪信道（仅损耗情形）。我们假设*Alice* 与 *Bob* 距 *Charlie*的距离相等。仅损耗情形意味着探测器效率为 $\eta_{\text{det}} = 1$，探测器的暗计数率为 $p_d = 0$，信道透射率 $\eta_{\text{t}} = 10^{-\frac{\alpha L}{10}} = 10^{-\frac{0.2L}{10}}$（即，信道衰减为 $\alpha = 0.2$），分束器与耦合器以理想方式工作——不存在相位失配（$\delta = 0$）。因此，根据所提出协议的描述（见第 II节），仅 **sns**配置会产生相关测量结果（公告） $\varkappa$ （$\varkappa = -$）在仅损耗情形下。注意，**sns**配置在整体中出现的概率为 $2\epsilon(1-\epsilon)$——对于发送-不发送，概率为$\epsilon(1-\epsilon)$；对于不发送-发送 配置，概率为$(1-\epsilon)\epsilon$。这意味着，在仅损耗情形下，任何相关测量结果出现的概率为 $2\epsilon(1-\epsilon) \times p_{\varkappa=-,\ Z,\ Z|\varphi_{a(b)},\ \tau_{a(b)}}$ 其中，$\varphi_{a(b)}$ 和$\tau_{a(b)}$ 分别表示 *Alice*（*Bob*）所选择的信号态和辅助相干态，$u(v)$表示 *Alice*（*Bob*）选择并公布的基。由于仅损耗情形意味着SNS-PM-QKD中不存在噪声，纠错过程中信息泄漏量为 $\delta^{\varkappa,\ u\ v}_{EC} = 0$。也就是说，不执行纠错。

为了确定SNS-PM-QKD的密钥率，我们需要获得给定 $\chi(K:\ E)$的Holevo信息 $\varkappa = -$，$u = Z$，以及 $v = Z$（密钥生成轮次）。为此，需要求出 $\rho^{k,\ y-z\,z}_{E}$、、、，$\rho^{k,\ -z\,z}_{E}$、、，以及 $\rho^{-,\ z\,z}_{E}$；参见表达式（21）。利用表达式（22），我们得到

$$\begin{aligned}\rho_E^{k,-,Z,Z} &= \sum_y p_{y|k,-,Z,Z} \times \rho_E^{k,y,-,Z,Z} \\ &= p_{y=\bar{k}|k,-,Z,Z} \times \rho_E^{k,y=\bar{k},-,Z,Z} \\ &= 1 \times \rho_E^{k,y=\bar{k},-,Z,Z} \overset{(23)}{=} \left|\Theta^{-,Z,Z}_{k,y=\bar{k}}\right\rangle\!\left\langle\Theta^{-,Z,Z}_{k,y=\bar{k}}\right|\end{aligned} \tag{36}$$

and

$$\begin{aligned}\rho_E^{-,Z,Z} &= \sum_k p_{k|-,Z,Z} \times \rho_E^{k,-,Z,Z} \\ &= p_{0|-,Z,Z} \times \rho_E^{0,-,Z,Z} + p_{1|-,Z,Z} \times \rho_E^{1,-,Z,Z} \\ &= \frac{1}{2}\left|\Theta^{-,Z,Z}_{0,1}\right\rangle\!\left\langle\Theta^{-,Z,Z}_{0,1}\right| + \frac{1}{2}\left|\Theta^{-,Z,Z}_{1,0}\right\rangle\!\left\langle\Theta^{-,Z,Z}_{1,0}\right|.\end{aligned} \tag{37}$$

方程（36）的结果表明，$\rho^{k,\ -z\,z}_{E}$ $\forall k \in \{0,1\}$ 是一个纯态，即其冯·诺依曼熵$S(\rho^{k,\ -z\,z}_{E})$为零——$S(\rho^{k,\ -z\,z}_{E}) = 0$；这与参考文献 [10]一致。请注意上文中的$p_{y=k|k,-,Z,Z} = 1$。这是因为在仅损耗情形下，给定公告 $\varkappa = -$, $u = Z$和$v = Z$，$k = y$ 或 $y = k$都是可能的。还要注意恒等式$p_{0|-,Z,Z} = p_{1|-,Z,Z}$。这是因为Alice和Bob以相同的概率 ϵ $(1-\epsilon)$ 发送（不发送）状态。也就是说，在sns配置中，Alice在一半情况下发送相干态，Bob则在另一半情况下发送相干态。可能的 $\rho^{k,\ y-z\,z}_{E}$,,状态如下：

$$\begin{aligned}\rho_E^{0,1,-,Z,Z} &= \left|\Theta^{-,Z,Z}_{0,1}\right\rangle\!\left\langle\Theta^{-,Z,Z}_{0,1}\right| \\ \rho_E^{1,0,-,Z,Z} &= \left|\Theta^{-,Z,Z}_{1,0}\right\rangle\!\left\langle\Theta^{-,Z,Z}_{1,0}\right|\end{aligned} \tag{38}$$

其中

$$\begin{aligned}\left|\Theta_{0,1}^{-,Z,Z}\right\rangle &= \frac{\sqrt{F^-}\left|\varphi_{0,1,Z,Z},\tau_{0,1,Z,Z}\right\rangle}{\sqrt{\left\langle\varphi_{0,1,Z,Z},\tau_{0,1,Z,Z}\right|F^-\left|\varphi_{0,1,Z,Z},\tau_{0,1,Z,Z}\right\rangle}}\\ &= \frac{\sqrt{F^-}\left|+\sqrt{\mu},-\sqrt{\mu}\right\rangle}{\sqrt{\left\langle+\sqrt{\mu},-\sqrt{\mu}\right|F^-\left|+\sqrt{\mu},-\sqrt{\mu}\right\rangle}},\\ \left|\Theta_{1,0}^{-,Z,Z}\right\rangle &= \frac{\sqrt{F^-}\left|\varphi_{1,0,Z,Z},\tau_{1,0,Z,Z}\right\rangle}{\sqrt{\left\langle\varphi_{1,0,Z,Z},\tau_{1,0,Z,Z}\right|F^-\left|\varphi_{1,0,Z,Z},\tau_{1,0,Z,Z}\right\rangle}}\\ &= \frac{\sqrt{F^-}\left|-\sqrt{\mu},+\sqrt{\mu}\right\rangle}{\sqrt{\left\langle-\sqrt{\mu},+\sqrt{\mu}\right|F^-\left|-\sqrt{\mu},+\sqrt{\mu}\right\rangle}}.\end{aligned} \tag{39}$$

给定公告 $\varkappa=-$，$u=Z$和 $v=Z$，相干态$|\varphi_{k,y,Z,Z},\tau_{k,y,Z,Z}\rangle$ 根据密钥映射（15）和关系式（5）-（6）具有以下形式

$$\begin{aligned}&\left|\varphi_{k,y,Z,Z},\tau_{k,y,Z,Z}\right\rangle\\ &=\left|\varphi_{w,y,Z,Z},\tau_{w,y,Z,Z}\right\rangle=\left|\varphi_{0,1,Z,Z},\tau_{0,1,Z,Z}\right\rangle\\ &=\left|\varphi_{k,Z}-\mathrm{e}^{i\delta}\sqrt{V}\varphi_{y,Z},\tau_{y,Z}-\mathrm{e}^{i\delta}\sqrt{V}\tau_{k,Z}\right\rangle\\ &=\left|\varphi_{0,Z}-\mathrm{e}^{i\delta}\sqrt{V}\varphi_{1,Z},\tau_{1,Z}-\mathrm{e}^{i\delta}\sqrt{V}\tau_{0,Z}\right\rangle\\ &\overset{\delta=0,V=1}{=}\left|\varphi_{0,Z},-\tau_{0,Z}\right\rangle=\left|\sqrt{\mu},-\sqrt{\mu}\right\rangle,\\ &\left|\varphi_{k,y,Z,Z},\tau_{k,y,Z,Z}\right\rangle\\ &=\left|\varphi_{w,y,Z,Z},\tau_{w,y,Z,Z}\right\rangle=\left|\varphi_{1,0,Z,Z},\tau_{1,0,Z,Z}\right\rangle\\ &=\left|\varphi_{1,Z}-\mathrm{e}^{i\delta}\sqrt{V}\varphi_{0,Z},\tau_{0,Z}-\mathrm{e}^{i\delta}\sqrt{V}\tau_{1,Z}\right\rangle\\ &\overset{\delta=0,V=1}{=}\left|-\varphi_{0,Z},\tau_{0,Z}\right\rangle=\left|-\sqrt{\mu},\sqrt{\mu}\right\rangle.\end{aligned} \tag{40}$$

在上述表达式中，$\delta=0$ 和 $V=1$ 对应于前文所述的理想（仅损耗）情形。回想一下，**sns** 配置（$k=y$_或 $y=k$）可由公告 $\varkappa=-$ 本身推知。显然，冯·诺依曼熵 $S(\rho^-_{E,Z\,Z,})$等于 $H\left(\frac{1-|\langle\Theta^-_{0,Z\,Z,,1}|\Theta^-_{1\,0,Z\,Z}\rangle|}{2}\right)$，其中 $H(\cdot)$为香农熵 [10]。注意，$\rho^-_{E,Z\,Z,}$的特征值为 $\frac{1}{2}\left(1\pm\left|\left\langle\Theta_{0,1}^{-,Z,Z}\middle|\Theta_{1,0}^{-,Z,Z}\right\rangle\right|\right)$。根据参考文献 [10],

$$\begin{aligned}&H\left(\frac{1-\left|\left\langle\Theta_{0,1}^{-,Z,Z}\middle|\Theta_{1,0}^{-,Z,Z}\right\rangle\right|}{2}\right)\\ &=H\left(\frac{1-\mathrm{e}^{-4\mu(1-\sqrt{\eta})}\mathrm{e}^{-2\mu\sqrt{\eta}}}{2}\right).\end{aligned} \tag{41}$$

现在，我们可以利用定义（21）来评估 $\chi(K:E)$。考虑到结果（41）以及$S(\rho^k_{E,-Z\,Z,})=0$，我们得到 $\chi(K:E)$

$$\chi(K:E)=H\left(\frac{1-\mathrm{e}^{-4\mu(1-\sqrt{\eta})}\mathrm{e}^{-2\mu\sqrt{\eta}}}{2}\right). \tag{42}$$

因此，根据定义（19），速率 $r(\rho^-_{KYE,Z\,Z,})$ 可表示为

$$\begin{aligned}r(\rho_{KYE}^{-,Z,Z})&=1-\delta_{\mathrm{EC}}^{-,Z,Z}-\chi(K:E)\\ &=1-H\left(\frac{1-\mathrm{e}^{-4\mu(1-\sqrt{\eta})}\mathrm{e}^{-2\mu\sqrt{\eta}}}{2}\right).\end{aligned} \tag{43}$$

根据（25），总速率 R 因此为

$$\begin{aligned}R=p_{-,Z,Z}\times r(\rho_{KYE}^{-,Z,Z})=2\epsilon(1-\epsilon)(1-\mathrm{e}^{-2\mu\sqrt{\eta}})\times\\ \left[1-H\left(\frac{1-\mathrm{e}^{-4\mu(1-\sqrt{\eta})}\mathrm{e}^{-2\mu\sqrt{\eta}}}{2}\right)\right].\end{aligned} \tag{44}$$

经过相位随机化的 SNS-PM-QKD 的总速率为

$$\begin{aligned}R'=s\times 2\epsilon(1-\epsilon)(1-\mathrm{e}^{-2\mu\sqrt{\eta}})\times\\ \left[1-H\left(\frac{1-\mathrm{e}^{-4\mu(1-\sqrt{\eta})}\mathrm{e}^{-2\mu\sqrt{\eta}}}{2}\right)\right].\end{aligned} \tag{45}$$

其中，s ($s=0.5$) 是相位区间筛选因子——即$Alice$ 和 Bob 选取相同相位区间（$[0,\pi)$ 或 $[\pi,2\pi)$）的概率。

上面的$p_{-、Z、Z}$ 的取值，是结合表I应用于以下表达式后得到的

$$\begin{aligned}&p_{\varkappa,u,v}\\ &=p_{-,Z,Z}=\sum_{\varphi,\tau}p_{-,Z,Z|\varphi,\tau}\times p_{\varphi,\tau}\\ &=p_{-,Z,Z|+\sqrt{\mu},-\sqrt{\mu}}\times p_{+\sqrt{\mu},-\sqrt{\mu}}+p_{-,Z,Z|-\sqrt{\mu},+\sqrt{\mu}}\times\\ &p_{-\sqrt{\mu},+\sqrt{\mu}}=(1-\mathrm{e}^{-2\mu\sqrt{\eta}})2\epsilon(1-\epsilon).\end{aligned} \tag{46}$$

概率$p_{-、Z、Z|+\sqrt{\mu}、-\sqrt{\mu}}$和 $p_{-、Z、Z|-\sqrt{\mu}、+\sqrt{\mu}}$由表达式 [10]计算得出

$$\begin{aligned}&p_{-,Z,Z|+\sqrt{\mu},-\sqrt{\mu}}\\ &=\left\langle+\sqrt{\mu},-\sqrt{\mu}\right|F^-\left|+\sqrt{\mu},-\sqrt{\mu}\right\rangle\\ &=\mathrm{e}^{-\frac{\sqrt{\eta}|+\sqrt{\mu}+(-\sqrt{\mu})|^2}{2}}(1-\mathrm{e}^{-\frac{\sqrt{\eta}|+\sqrt{\mu}-(-\sqrt{\mu})|^2}{2}})\\ &p_{-,Z,Z|-\sqrt{\mu},+\sqrt{\mu}}\\ &=\left\langle-\sqrt{\mu},+\sqrt{\mu}\right|F^-\left|-\sqrt{\mu},+\sqrt{\mu}\right\rangle\\ &=\mathrm{e}^{-\frac{\sqrt{\eta}|-\sqrt{\mu}+(+\sqrt{\mu})|^2}{2}}(1-\mathrm{e}^{-\frac{\sqrt{\eta}|-\sqrt{\mu}-(+\sqrt{\mu})|^2}{2}})\end{aligned} \tag{47}$$

概率 $p_{\varphi,\tau}$ 与发送或不发送的选择有关:

$$\begin{aligned}&p_{\varphi,\tau}=p_{\varphi=\varphi_{0,1,Z,Z},\tau=\tau_{0,1,Z,Z}}=\epsilon(1-\epsilon)\\ &\quad\text{given } \textit{sending-not sending}\quad \textbf{sns},\\ &p_{\varphi,\tau}=p_{\varphi=\varphi_{1,0,Z,Z},\tau=\tau_{1,0,Z,Z}}=(1-\epsilon)\epsilon\\ &\quad\text{given } \textit{not sending-sending}\quad \textbf{sns},\\ &p_{\varphi,\tau}=p_{\varphi=\varphi_{1,1,Z,Z},\tau=\tau_{1,1,Z,Z}}=(1-\epsilon)^2\\ &\quad\text{given } \textit{not sending-not sending}\quad \textbf{nn},\\ &p_{\varphi,\tau}=p_{\varphi=\varphi_{0,0,Z,Z},\tau=\tau_{0,0,Z,Z}}=\epsilon^2\\ &\quad\text{given } \textit{sending-sending}\quad \textbf{ss}\end{aligned} \tag{48}$$

在**不发送—不发送（nn）**和**发送—发送（ss）**配置下，当认为 SNS-PM-QKD（或带随机化的SNS-PM-QKD）在仅存在损耗的情况下运行时，D_- 探测器不会记录到任何点击。因此，在这些配置下不会出现 $\varkappa=-$。对于 SNS-PM-QKD，这是因为

$$\begin{aligned}
&|\varphi_{1,1,Z,Z},\tau_{1,1,Z,Z}\rangle\\
&=\left|\varphi_{1,Z}-\mathrm{e}^{i\delta}\sqrt{V}\varphi_{1,Z},\tau_{1,Z}-\mathrm{e}^{i\delta}\sqrt{V}\tau_{1,Z}\right\rangle\\
&\overset{\delta=0,V=1}{=}\left|\sqrt{0}-\sqrt{0},\sqrt{0}-\sqrt{0}\right\rangle=|0,0\rangle,\\
&|\varphi_{0,0,Z,Z},\tau_{0,0,Z,Z}\rangle\\
&=\left|\varphi_{0,Z}-\mathrm{e}^{i\delta}\sqrt{V}\varphi_{0,Z},\tau_{0,Z}-\mathrm{e}^{i\delta}\sqrt{V}\tau_{0,Z}\right\rangle\\
&\overset{\delta=0,V=1}{=}|+\sqrt{\mu}-(+\sqrt{\mu}),+\sqrt{\mu}-(+\sqrt{\mu})\rangle\\
&=|0,0\rangle
\end{aligned}$$

因此

$$\begin{aligned}
p^{\mathrm{nn}}_{-,Z,Z|0,0}&=\langle 0,0|\,F^-\,|0,0\rangle=0,\\
p^{\mathrm{ss}}_{-,Z,Z|0,0}&=\langle 0,0|\,F^-\,|0,0\rangle=0
\end{aligned}$$

因此，p^{nn}_{-}、Z、$Z|0$、$_0p_{\varphi=\varphi_1}$、$\mathbf{1}$、z、z、$\tau=\tau_1$、$\mathbf{1}$、z、z 以及 p^{ss}_{-}、Z、$Z|0$、$_0p_{\varphi=\varphi_0}$、$\mathbf{0}$、z、z、$\tau=\tau_0$、$\mathbf{0}$、z、z 均消失，不会对式（46）中的求和作出贡献。类似地，对于采用相位随机化的 SNS-PM-QKD，我们有

$$\begin{aligned}
p^{\mathrm{nn}}_{-,Z,Z|0,0}&=\langle 0,0|\,F^-\,|0,0\rangle=0,\\
p^{\mathrm{ss}}_{-,Z,Z|\sqrt{\psi},\sqrt{\psi}}&=\left\langle\sqrt{\psi},\sqrt{\psi}\right|F^-\left|\sqrt{\psi},\sqrt{\psi}\right\rangle=0
\end{aligned}$$

其中 $\sqrt{\psi}$ 表示 ss 配置下耦合器输出态的强度；参见附录 A 作为参考。

与仅损耗情形相关的密钥率-距离函数 $R(L)$ 和 $R'(L)$ 绘于第 IVC节。

B. 现实情形

本节考察现实情形（通信装置存在不完善之处）下所提出的协议的行为。类似于 [10]，

表 I. 在仅损耗情形下，给定可能的相干态（信号态和参考态）时，公告 $\varkappa$、$u=Z$ 和 $v=Z$ 的条件概率分布。请注意，这里仅考虑密钥生成情形（$u=Z$ 和 $v=Z$）。$|\varphi_0,\mathbf{1},z,z,\tau_0,\mathbf{1},z,z\rangle$ 对应表中的 $|+\sqrt{\mu},-\sqrt{\mu}\rangle$，而 $|\varphi_1,\mathbf{0},z,z,\tau_1,\mathbf{0},z,z\rangle$ 对应 $-|-\sqrt{\mu},+\sqrt{\mu}\rangle$。请注意，此表与参考文献 [10] 中的表完全相同——本文的相干态 $|\varphi,\tau\rangle$ 和 POVM $F^{\varkappa}$ 与 [10] 中的相同。

$\lvert\varphi,\tau\rangle$	$\lvert\varphi_{0,1,Z,Z},\tau_{0,1,Z,Z}\rangle$	$\lvert\varphi_{1,0,Z,Z},\tau_{1,0,Z,Z}\rangle$
$p_{-,Z,Z\|\varphi,\tau}$	$1-\mathrm{e}^{-2\mu\sqrt{\eta}}$	$1-\mathrm{e}^{-2\mu\sqrt{\eta}}$
$p_{?,Z,Z\|\varphi,\tau}$	$\mathrm{e}^{-2\mu\sqrt{\eta}}$	$\mathrm{e}^{-2\mu\sqrt{\eta}}$

现实情形包括：非理想的探测效率 η_{det} 探测器的（$\eta_{\mathrm{det}}<1$）、非零的暗计数率 p_{dark} 探测器的（$p_{\mathrm{dark}}\neq 0$）、非零的相位失配 δ 在分束器或耦合器处发生的干涉过程中（$\delta\neq 0$）、非理想的模式（强度）失配 V 在干涉过程中（$V<1$）、非理想的纠错效率 f_{EC}（$f_{\mathrm{EC}}>1$）。请注意，这些非理想因素用于模拟图1所示通信装置各部分的非理想行为。

上述两个量用于表征探测系统（探测器）的不完美因素——分别是探测器的探测效率 η_{det} 和暗计数率 p_{dark}。我们假设装置中的两个探测器（见图1）具有相同的效率（在下文 η 的表达式中为 $\eta^{D_+}_{\mathrm{det}}=\eta^{D_-}_{\mathrm{det}}\to\eta^2_{\mathrm{det}}$），且暗计数率相同（$p^{D_+}_{\mathrm{dark}}=p^{D_-}_{\mathrm{dark}}$）。探测器效率包含在装置的总透射率中 $\eta=\eta^2_{\mathrm{det}}\eta_{\mathrm{t}}=\eta^2_{\mathrm{det}}10^{-\alpha L/10}$，其中 η_{t} 表示信道透射率，α（单位为 dB/km）表示信道每公里衰减，而 L（单位为 km）表示装置的传输（工作）距离。

装置中发生的任何干涉过程都涉及相位失配和模式（强度）失配。这些量用于表征干涉过程中相干态之间的不对称性。这种不对称性由分束器、耦合器或量子信道的非理想行为导致。量子信道可能会使相干态发生所谓的相位漂移。根据[10]的安全性证明分析，在分束器处考虑相位和强度失配时，到达分束器的态为 $|\varphi,\mathrm{e}^{i\delta}\tau\rangle$；考虑模式（强度）失配时，到达的态在原模式中为 $\left|\varphi,\sqrt{V\tau}\right\rangle$，在第二模式中为 $|0,\sqrt{1-V\tau}\rangle$。在耦合器处，按照附录A中的描述考虑相位和强度（模式）失配。

若存在装置不完美因素，SNS-PM-QKD（第IIA节）的总速率变为

$$\begin{aligned}
R_{\mathrm{real}}&=p_{-,Z,Z}\times r(\rho^{-,Z,Z}_{KYE})\\
&=\left(2\epsilon(1-\epsilon)P_{\mathrm{sns}}+\epsilon^2P_{\mathrm{ss}}+(1-\epsilon)^2P_{\mathrm{nn}}\right)\times\\
&\quad[1-\chi(K:E)^{-,Z,Z}-\delta^{-,Z,Z}_{\mathrm{EC}}].
\end{aligned}\tag{49}$$

量 P_{sns} 是在*Alice* 发送相干态而*Bob* 不发送，或 *Alice* 不发送而*Bob*发送相干态的情况下，$\varkappa=-$ 在 Z（信号）轮中发生的概率。其表达式为

$$\begin{aligned}
P_{\mathrm{sns}}&=\langle\varphi_{0,1,Z,Z},\tau_{0,1,Z,Z}|\,F^-_{\mathrm{imp}}\,|\varphi_{0,1,Z,Z},\tau_{0,1,Z,Z}\rangle+\\
&\quad\langle\varphi_{1,0,Z,Z},\tau_{1,0,Z,Z}|\,F^-_{\mathrm{imp}}\,|\varphi_{1,0,Z,Z},\tau_{1,0,Z,Z}\rangle\\
&=\langle+\sqrt{\mu},-\sqrt{\mu}|\,F^-_{\mathrm{imp}}\,|+\sqrt{\mu},-\sqrt{\mu}\rangle+\\
&\quad\langle-\sqrt{\mu},+\sqrt{\mu}|\,F^-_{\mathrm{imp}}\,|-\sqrt{\mu},+\sqrt{\mu}\rangle.
\end{aligned}\tag{50}$$

F^{-} 不完美因素 下对应测量结果 $\varkappa=-$ 的 POVM 算子[10]。其矩阵形式F^{-} 不完美因素 下的形式见附录 B。量 P_{ss} 是 $\varkappa=-$ 在 *Alice* 和 *Bob*均在一个 Z （信号）轮中发送相干态时发生的概率。其表达式为

$$P_{\mathrm{ss}}=\langle\sqrt{\gamma},\sqrt{\gamma}|\,F_{\mathrm{imp}}^{-}\,|\sqrt{\gamma},\sqrt{\gamma}\rangle \tag{51}$$

其中 $|\sqrt{\gamma}\rangle$ 表示输入态发生相位失配时耦合器的输出态 δ ，输入态为$|+\sqrt{\mu}\rangle_{Q(T)}$和$|+\sqrt{\mu}\rangle_{Q'(T')}$；参见附录 A （公式（A6））以供参考。量 P_{nn} 表示在 $\varkappa=-$发生的概率，条件是 *Alice* 和 *Bob* 在一个 Z （信号）轮中均未发送相干态。其表达式为

$$P_{\mathrm{nn}}=p_{\mathrm{dark}}(1-p_{\mathrm{dark}}). \tag{52}$$

因此，该概率对应于一个探测器发生暗计数，而另一个探测器未发生暗计数的情况。

根据（20）， $\delta^{-,Z,Z}$ EC 表示为

$$\delta_{\mathrm{EC}}^{-,Z,Z}=f_{\mathrm{EC}}H(e^{-,Z,Z}). \tag{53}$$

这里通过 $e^{-,Z,Z}$ 进行评估

$$e^{-,Z,Z}=e_1^{-,Z,Z}+e_2^{-,Z,Z} \tag{54}$$

其中

$$e_1^{-,Z,Z}=\frac{\epsilon^2P_{\mathrm{ss}}}{2\epsilon(1-\epsilon)P_{\mathrm{sns}}+\epsilon^2P_{\mathrm{ss}}+(1-\epsilon)^2P_{\mathrm{nn}}} \tag{55}$$

and

$$e_2^{-,Z,Z}=\frac{(1-\epsilon)^2P_{\mathrm{nn}}}{2\epsilon(1-\epsilon)P_{\mathrm{sns}}+\epsilon^2P_{\mathrm{ss}}+(1-\epsilon)^2P_{\mathrm{nn}}}. \tag{56}$$

因此，与配置（情形）ss 和 nn 对应的所有事件$(-,Z,Z)$均视为错误。注意， e^{-}， $_{1}{}^{Z\,Z}{}_{k=1}=p_{k=1}$, $_{,y=1|\varkappa=-}$ 和 e^{-}， $_{2}{}^{Z\,Z}{}_{k=0}=p_{k=0}$, $_{,y=0|\varkappa=-}$。回想一下，Alice 和 Bob 需要 $k=y$ （$k=0,y=1$ 或 $k=1,y=0$）才能建立关联密钥比特（参见第二节中的步骤 6）。

为了确定 $\chi(K:E)^{-,Z,Z}$，我们利用其可约化为 $H\left(1-\left|\left\langle\Theta_{0,1}^{-,Z,Z}\middle|\Theta_{1,0}^{-,Z,Z}\right\rangle\right|/2\right)$（见第 IVA 节）这一事实。在实际条件（不完美因素）下，*Eve* 的条件态之间的重叠具有如下形式

$$\left\langle\Theta_{0,1}^{-,Z,Z}\middle|\Theta_{1,0}^{-,Z,Z}\right\rangle=\frac{\langle+\sqrt{\mu},-\sqrt{\mu}|\,F_{\mathrm{imp}}^{-}\,|-\sqrt{\mu},+\sqrt{\mu}\rangle}{\sqrt{\langle+\sqrt{\mu},-\sqrt{\mu}|\,F_{\mathrm{imp}}^{-}\,|+\sqrt{\mu},-\sqrt{\mu}\rangle\,\langle-\sqrt{\mu},+\sqrt{\mu}|\,F_{\mathrm{imp}}^{-}\,|-\sqrt{\mu},+\sqrt{\mu}\rangle}} \tag{57}$$

如参考文献 [10] 所示。

若执行主动奇宇称配对 （AOPP） [13, 14] ，则 SNS-PM-QKD 的总密钥率具有如下形式

$$\tilde{R}_{\mathrm{real}}=s\times\left(2\epsilon(1-\epsilon)P_{\mathrm{sns}}+\epsilon^2P_{\mathrm{ss}}+(1-\epsilon)^2P_{\mathrm{nn}}\right)\times\left[1-\chi(K:E)^{-,Z,Z}-\tilde{\delta}_{\mathrm{EC}}^{-,Z,Z}\right]. \tag{58}$$

其中

$$s=\frac{1}{2}[(1-e^{-,Z,Z})^2+(e^{-,Z,Z})^2] \tag{59}$$

是 AOPP 的筛选因子 ， 且

$$\tilde{\delta}_{\mathrm{EC}}^{-,Z,Z}=f_{\mathrm{EC}}H(\tilde{e}^{-,Z,Z}) \tag{60}$$

是在采用 AOPP 算法时，纠错过程中信息泄漏的平均量。请注意，

$$\tilde{e}^{-,Z,Z}=\frac{(e^{-,Z,Z})^2}{(1-e^{-,Z,Z})^2+(e^{-,Z,Z})^2} \tag{61}$$

是经 AOPP程序缓解后的错误率。

采用相位随机化的 SNS-PM-QKD（第 IIB 节）的总密钥率具有如下形式

$$R'_{\mathrm{real}}=\frac{1}{2}\left(2\epsilon(1-\epsilon)P_{\mathrm{sns}}+\epsilon^2P'_{\mathrm{ss}}+(1-\epsilon)^2P_{\mathrm{nn}}\right)\times\left[1-\chi(K:E)^{-,Z,Z}-\tilde{\delta}_{\mathrm{EC}}^{-,Z,Z}\right] \tag{62}$$

其中，分数 1/2表示相位区间筛选因子。量 P'_{ss} 的计算方式为

$$P'_{\mathrm{ss}}=\left\langle\sqrt{\psi},\sqrt{\psi}\middle|\,F_{\mathrm{imp}}^{-}\,\middle|\sqrt{\psi},\sqrt{\psi}\right\rangle \tag{63}$$

其中 $|\sqrt{\psi}\rangle$ 表示输入态发生相位失配时耦合器的输出态 δ ，输入态为$|e^{i\nu_a}\sqrt{\mu}\rangle_{Q(T)}$和$|e^{i\nu_b}\sqrt{\mu}\rangle_{Q'(T')}$；参见附录 A7中的公式 (A ， 以供参考。因此

$$\tilde{R}'_{\mathrm{real}}=\frac{1}{2}s\times\left(2\epsilon(1-\epsilon)P_{\mathrm{sns}}+\epsilon^2P'_{\mathrm{ss}}+(1-\epsilon)^2P_{\mathrm{nn}}\right)\times\left[1-\chi(K:E)^{-,Z,Z}-\tilde{\delta}_{\mathrm{EC}}^{-,Z,Z}\right] \tag{64}$$

是采用随机化和 AOPP 过程的 SNS-PM-QKD 的总密钥率。

关于密钥率-距离函数的结果 $R_{\mathrm{real}}(L)$,~ ~ $R'_{\mathrm{real}}(L)$, $R_{\mathrm{real}}(L)$, 以及 $R'_{\mathrm{real}}(L)$见第 IVC节。这些函数用于评估本工作的贡献（SNS-PM-QKD 以及带随机化的 SNS-PM-QKD），并将其与同类现有协议进行比较。

C. 结果

为客观评估本工作的贡献，我们进行以下比较：(i)SNS-PM-QKD（以及带随机化的 SNS-PM-QKD）与文献 [10] 中 PM-QKD 的范围和容错比较；(ii)SNS-PM-QKD（以及带随机化的 SNS-PM-QKD）与文献 [11] 中 SNS-TF-QKD 及采用相位后选择的 SNS-TF-QKD[12]进行范围比较；(iii) SNS-PM-QKD（以及带随机化的 SNS-PM-QKD）与文献 [19] 中实验性 SNS-TF-QKD 进行范围比较。

比较（i）。该比较（图7）用于表明，所提出的协议（SNS-PM-QKD和带随机化的SNS-PM-QKD）相较于文献 [10]中的PM-QKD具有更优的范围性能。同时考虑了仅损耗情形和实际情形。在仅损耗情形中，SNS-PM-QKD（带随机化的SNS-PM-QKD）的密钥率由式(44)（式(45)）计算。为在现实情形中进行恰当比较，SNS-PM-QKD（式(49)和式(62)）与PM-QKD的密钥率均针对相同的协议参数进行计算：$p_{\mathrm{dark}} = 8 \times 10^{-8}$, $\delta = \frac{\pi}{60}$,$V = 0.95$, $\eta_{\mathrm{det}} = 0.145$, $f_{\mathrm{EC}} = 1.15$。需注意，μ（信号态和辅助相干态的强度）在SNS-PM-QKD中取最优值0.1，$\mu = 0.1$。为与SNS-PM-QKD中发送或不发送方法 [11, 12], 的本质保持一致，我们采用图8所示形式的发送概率 $\epsilon(L)$（传输距离 L的函数）。函数 $\epsilon(L)$表示为

$$\epsilon(L) = \epsilon_0 + (\epsilon_{\max} - \epsilon_0)\left(\frac{L}{L_{\max}}\right)^3 \tag{65}$$

其中 $\epsilon_0 = 0.05$ 和 $\epsilon_{\max} = 0.45$。 $L_{\max}$ 的取值取决于 SNS-PM-QKD 在 $\delta \to 0$—$\epsilon(L)$ 情况下的速率-距离范围，需要覆盖该速率-距离范围。在此比较中， $L_{\max} = 450$km。

如图7所示，与文献[10]中的PM-QKD相比，SNS-PM-QKD和带随机化的SNS-PM-QKD均实现了更大的速率-距离范围。在此比较中，所提出的两种协议均可达到442 km的距离。与文献[10]中的PM-QKD相比，SNS-PM-QKD（带随机化的SNS-PM-QKD）具有更大的速率-距离范围，原因有二：原因1：SNS-PM-QKD（带随机化的SNS-PM-QKD）的错误率更低于文献 [10]中的PM-QKD；原因2：与文献 [10]中的PM-QKD相比，SNS-PM-QKD（带随机化的SNS-PM-QKD）具有更高的密钥率与误码率之比（密钥率：错误率）。SNS-PM-QKD的错误率较低，这是因为采用了结果筛选，且在$\varkappa = -$条件下，**发送—发送（ss）**和**不发送—不发送（nn）**情形中获得密钥生成POVM结果的概率较低。SNS-PM-QKD具有更高的密钥率与误码率之比，这归因于原因1以及采用了距离相关的发送概率 $\epsilon(L$（其取值最高约为0.45），从而获得了相应的速率-距离范围（图7）。

此外，比较(i)用于说明，与文献 [10] （见图9）中的 PM-QKD 协议相比，所提出的协议（SNS-PM-QKD 和带随机化的 SNS-PM-QKD）具有更高的误差容忍度。容错比较通过分析带随机化的 SNS-PM-QKD 和 PM-QKD 在若干相位失配 δ取值下的表现进行。具体而言，考虑以下四个取值：$\delta = \pi/60$， $\delta = \pi/10$, $\delta = \pi/8$， $\delta = \pi/3$。如图9所示，带随机化的 SNS-PM-QKD 对相位失配（失配）具有相对较高的容忍度，显著高于 PM-QKD。随着 δ增大，带随机化的 SNS-PM-QKD 的可达距离比 PM-QKD 的可达距离下降得更慢。此外，当 $\delta = \pi/3$时，PM-QKD 无法产生正密钥率；因此，图中未显示相应的速率-距离曲线。

比较（ii）。此比较（图 10）用于说明，与 SNS-TF-QKD [11]以及带后选择的 SNS-TF-QKD [12]相比，所提出的协议（有或无随机化的 SNS-PM-QKD）具有更好的范围性能。我们仅关注 SNS-TF-QKD 和带后选择的 SNS-TF-QKD 的最大可实现距离：分别为 176 dB 和 181 dB。此比较中各协议的性能均涉及主动奇宇称配对（AOPP）过程。在图 10 中，SNS-PM-QKD 和带随机化的 SNS-PM-QKD 分别由密钥率-距离 ~ ~函数 $R_{\mathrm{real}}(L)$（见式（58））和 $R'_{\mathrm{real}}(L)$（见式（64））表示。对于这些密钥率-距离函数，我们采用发送概率曲线 $\epsilon(L)$，其中 $\epsilon_0 = 0.05$、$\epsilon_{\max} = 0.45$ 和 $L_{\max} = 950$ km（见图8和式（65））。为进行适当比较，我们根据协议参数 $p_{\mathrm{dark}} = 10^{-11}$、$\eta_{\mathrm{det}} = 1$、 $\alpha = 0.2$ dB/km、 $f_{\mathrm{EC}} = 1.1$ 评估 SNS-PM-QKD（带随机化的 SNS-PM-QKD）的密钥率。这些协议参数取自参考文献 [12]。~此外，我们还给出了三种情形下的函数 $R'_{\mathrm{real}}(L)$ 和 $R'_{\mathrm{real}}(L)$： $(\delta = \frac{\pi}{60}$, $V = 0.95)$； $(\delta = \frac{\pi}{60}$,—$V = 0.95)$； $(\delta =$—$\frac{\pi}{60}$, $V = 0.95)$。需要注意的是，在 SNS-PM-QKD（带随机化的 SNS-PM-QKD）中， μ （信号态和辅助相干态的强度）取值为 0.1。

如图所示。10，SNS-PM-QKD和带随机化的 SNS-PM-QKD均超过了SNS-TF-QKD的最大可达距离 [11] 以及带后选择的 SNS-TF-QKD [12]——这对所有

本比较中考察的（δ，V）情形（（**a**）、（**b**）和（**c**））。根据上述协议参数，SNS-PM-QKD（带随机化的SNS-PM-QKD）的最大距离可达973公里。

比较（iii）。此项比较（图 11）旨在说明，与文献[19]中介绍的实验实现的SNS-TF-QKD相比，所提出的协议（SNS-PM-QKD）具有更优的范围性能。我们只关注实验SNS-TF-QKD的最大可实现距离：1002km。本项比较中各协议的性能也包含主动奇宇称配对（AOPP）步骤。图11中，SNS-PM-QKD和带随机化的SNS-PM-QKD分别以密钥率-距离函数 $R_{\mathrm{real}}(L)$（见式（58））和 $R'_{\mathrm{real}}(L)$（见式（64））表示。对于这些密钥率-距离函数，我们采用发送概率曲线 $\epsilon(L)$，其中 $\epsilon_0 = 0.05$、$\epsilon_{\max} = 0.45$和 $L_{\max} = 1200$km（见图8和式（65））。为了进行恰当的比较，我们在协议参数为 $\eta_{\mathrm{det}} = 0.6$、$\alpha = 0.157$dB/km、$f_{\mathrm{EC}} = 1.16$时，计算SNS-PM-QKD（带随机化的SNS-PM-QKD）的密钥率。这些协议参数取自文献 [19]。此外，我们给出函数 $R_{\mathrm{real}}(L)$和 $R'_{\mathrm{real}}(L)$，对应三种情形：($\delta = \frac{\pi}{60}$, $V = 0.95$,$p_{\mathrm{dark}} = 10^{-11}$)；($\delta = \frac{\pi}{35}$,$V$ =0.95, $p_{\mathrm{dark}} = 5 \times 10^{-11}$)；($\delta = \frac{\pi}{3}$,$V = 0.95$,$p_{\mathrm{dark}} = 10^{-10}$)。请注意，在SNS-PM-QKD（带随机化的SNS-PM-QKD）中，μ（信号态和辅助相干态的强度）的值为0.1。

如图11所示，SNS-PM-QKD 和带随机化的SNS-PM-QKD 均超过了参考文献[19]中实验SNS-TF-QKD的密钥率-距离极限——这对本次比较中考虑的所有（δ，V，p_{dark}）情形（（**a**）、（**b**）和（**c**））均成立。给定上述协议参数，SNS-PM-QKD（带随机化的 SNS-PM-QKD）可实现的最大距离范围为 1211 km。

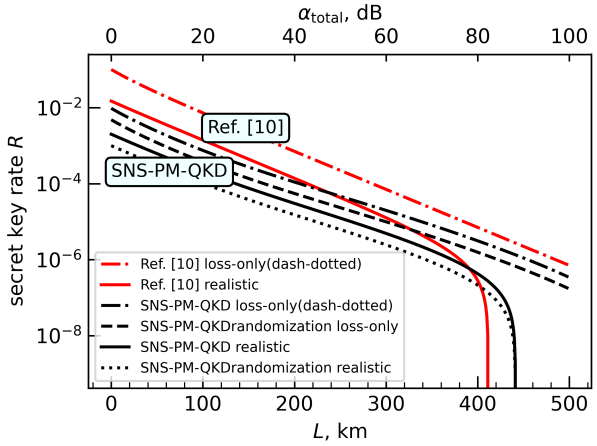

图7. SNS-PM-QKD 的密钥率比较（R_{real}（L）用黑色实线表示，R'_{real}（L）用黑色点线表示，R（L）用黑色点划线表示，R'（L）用黑色虚线表示）与参考文献 [10] 中的 PM-QKD（仅损耗密钥率用红色点划线表示，实际密钥率用红色实线表示）。比较涵盖仅损耗情形（R（L）和 R'（L））以及实际情形（R_{real}（L）和 R'_{real}（L））。函数 R（L）和 R'（L）分别通过使用方程（44）和方程（45），针对 $\mu = 0.1$ 和距离相关的发送概率 ϵ（L）进行评估（见图 8）。对于实际情形，SNS-PM-QKD（带随机化的 SNS-PM-QKD）的密钥率-距离图使用方程49（方程62）针对 $\mu = 0.1$ 和形式如图所示的距离相关发送概率 ϵ $\epsilon_{\max} = 0.45$ $L_{\max} = 450$ 8 （$L|\epsilon_0 = 0.05$， ，km）进行评估。为确保与参考文献 [10], 一致，实际情形下的密钥率在协议参数 $p_{\mathrm{dark}} = 8 \times 10^{-8}$、$\delta = \frac{\pi}{60}$ 、$V = 0.95$、$\eta_{\mathrm{det}} = 0.145$、$f_{\mathrm{EC}} = 1.15$ 下进行评估。对于仅损耗和实际情形，我们均假设衰减为 $\alpha = 0.2$ dB/km。在实际情形下，SNS-PM-QKD（带随机化的 SNS-PM-QKD）的距离范围为 441 km。

V. 总结

我们提出了一种基于发送或不发送 方案的 PM-QKD 协议，称为 SNS-PM-QKD。我们使用参考文献 [10] 中提出的框架，评估了该协议在集体攻击下的渐近密钥率。我们还分析了所提方案在双 POVM 攻击下的表现，这是一种协议特定形式的集体攻击。经验证，双 POVM 攻击可以被检测到，因为在参考文献 [10] 的框架下，它导致的错误率高于一般集体攻击所预测的错误率。我们从最大可实现传输距离的角度，将 SNS-PM-QKD 的密钥率—距离表现与 PM-QKD [10], 、SNS-TF-QKD、带后选择的 SNS-TF-QKD [12], 以及实验SNS-TF-QKD实现 [19], 进行了比较。SNS-PM-QKD 对相位具有相对较高的容忍度失配（失准误差），显著高于 PM-QKD。与所有其他参与比较的协议相比，它也能实现更远的工作距离。图 10 和11 表明，所提协议的表现超越了当前理论 SNS-TF-QKD 的密钥率—距离表现 [12] 以及参考文献 [19]中的实验SNS-TF-QKD实现。未来一个值得探索的方向是研究 SNS-PM-QKD 在有限密钥区间内的表现。此外，考察 SNS-PM-QKD 实验实现中可达到的密钥率—距离特性也很有意义。

致谢

本研究在保加利亚瓦尔纳技术大学开展。本研究得到瓦尔纳技术大学科学项目计划的资助，资助编号：НП6/2025。

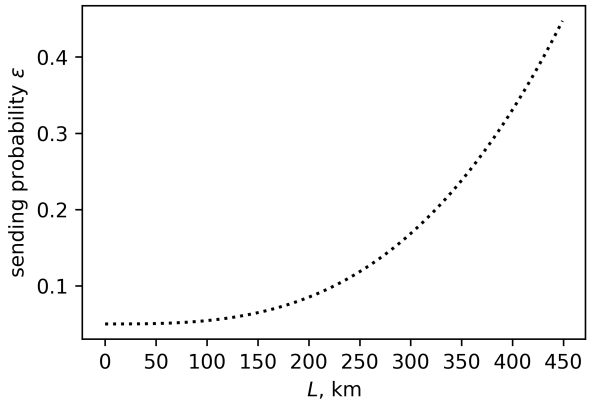

图8. 用于评估SNS-PM-QKD密钥率的 $\epsilon(L)$曲线。注意， $\epsilon(L) = \epsilon_0 + (\epsilon_{\max} - \epsilon_0) \times (L/L_{\max})^3$ ，其中我们选择 $\epsilon_0 = 0.05$、$\epsilon_{\max} = 0.45$ ，使得 $\epsilon(L)$与 [12]中采用的方法一致——在该协议的距离范围内使用变化的发送概率 ϵ 。 $L_{\max}$ 的值取决于比较条件：(i) $L_{\max} = 450$千米；(ii) $L_{\max} = 950$千米；(iii) $L_{\max} = 1100$千米。选择 $L_{\max}$ 的值，使得在给定 $\delta \to 0$的情况下，曲线 $\epsilon(L)$覆盖SNS-PM-QKD的速率-距离范围。在上图中，我们给出了 $L_{\max} = 450$千米时的 $\epsilon(L)$。

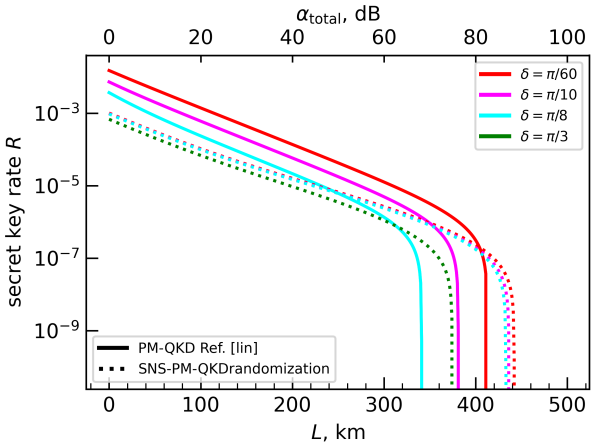

图9. 带随机化的SNS-PM-QKD（$R'(L)$、式（62）与参考文献 [10]中的PM-QKD的容错比较。为确保适当的容错比较，带随机化的SNS-PM-QKD和参考文献[10] 中的PM-QKD的速率-距离图均针对协议参数 $\mu = 0.1$、$k_{\max}$距离相关的发送概率0.45 $L_{\max} = 450$ 8 $p_{\text{dark}} = 8 \times 10^{-8}$ $V = 0.95$ （$L|\epsilon_0 = 0.05$、、千米）（见图），、、$\eta_{\text{det}} = 0.145$ $f_{\text{EC}} = 1.15$ δ 、以及若干个的取值进行评估。如图所示，考虑了的四个取值： δ $\delta = \pi/60$、$\delta = \pi/10$、$\delta = \pi/8$ $\delta = \pi/3$ 以及。

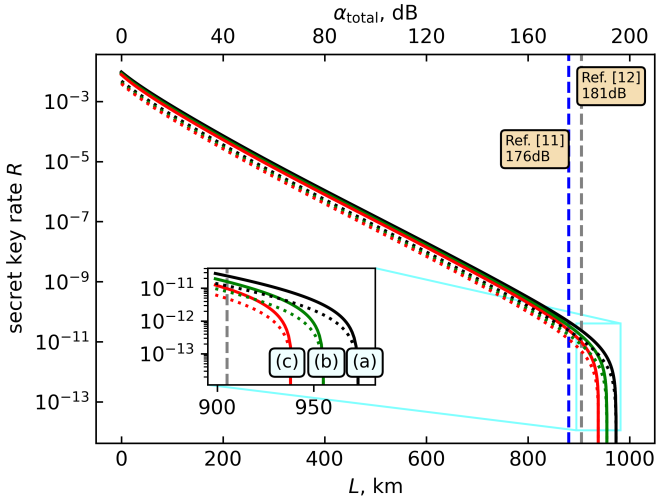

图 10。SNS-PM-QKD（实线表示$\tilde{R}_{\text{real}}(L)$，虚线表示$\tilde{R}'_{\text{real}}(L)$）与SNS-TF-QKD [11]以及带相位后选择的SNS-TF-QKD [12]的距离范围比较。请注意，比较中考虑了主动奇宇称配对（AOPP）。对于图8中给出的 $\epsilon = f(L)$，SNS-PM-QKD的密钥率 $\tilde{R}_{\text{real}}(L)$ 和 $\tilde{R}'_{\text{real}}(L)$ 分别通过公式（58）和公式（64）计算，其中 $L_{\max} = 900$千米。根据[12]，中给出的结果，SNS-TF-QKD的最大可实现距离为 $L = 880$千米（对应于 $\alpha_{\text{total}} = 176$ dB），而带相位后选择的SNS-TF-QKD的最大可实现距离为 $L = 905$千米（对应于$\alpha_{\text{total}} = 181$ dB）。为与参考文献 [12]的结果保持一致，SNS-PM-QKD的密钥率在协议参数 $p_{\text{dark}} = 10^{-11}$、$\eta_{\text{det}} = 1$、$\alpha = 0.2$ dB/km和 $f_{\text{EC}} = 1.1$下进行评估。强度参数 μ 取为0.1，从而使SNS-PM-QKD达到最大距离。请注意，SNS-PM-QKD中的失配建模方式不同于参考文献 [12]。为进行适当的距离范围比较，我们给出了若干对（δ，V）取值下的SNS-PM-QKD速率-距离图：（a）（$\delta = \frac{\pi}{60}$，$V = 0.95$）；（b）（$\delta = \frac{\pi}{4}$，$V = 0.9$）；（c）（$\delta = \frac{\pi}{3}$，$V = 0.85$）。SNS-PM-QKD的密钥率是在 $\mu = 0.1$下获得的。对于（a）、（b）和（c），SNS-PM-QKD（带随机化的SNS-PM-QKD）的距离范围分别为973千米、955千米和938千米。

附录 A：耦合器操作

耦合器由两个输入端和一个输出端组成。输出端发生相消干涉，即，出现状态 $\left|T(\mathrm{e}^{i\varphi}\alpha) - R(\mathrm{e}^{i\phi}\beta)\right\rangle$。请注意， α 和β 是输入相干态的强度（振幅），而 φ和 ϕ 则是它们各自的相位。

此外， T 和 R 分别是耦合器的透射率 和反射率 。我们假设 $T = R = 1$。上述输出态表示一种理想情形，其中输入态之间既不存在相位失配，也不存在模式（强度）失配 。若考虑相位失配，则需在其中一个输入态中引入相移。就此而言，我们假设相位失配角 δ 被引入反射态，即输出态取如下形式$\left|\mathrm{e}^{i\varphi}\alpha - \mathrm{e}^{i\delta}\mathrm{e}^{i\phi}\beta\right\rangle$ [注：参数 δ 可视为常数 [10]]。若考虑模式（强度）失配，我们在输入强度中引入不对称性——$\left|\mathrm{e}^{i\varphi}\alpha - \mathrm{e}^{i\delta}\mathrm{e}^{i\phi}\sqrt{V}\beta\right\rangle$，其中 $V < 1$ 处于非理想情形。

为便于说明，下面我们举一个简单的例子。考虑这样一种情形： $\alpha = \beta = \sqrt{\mu}$，

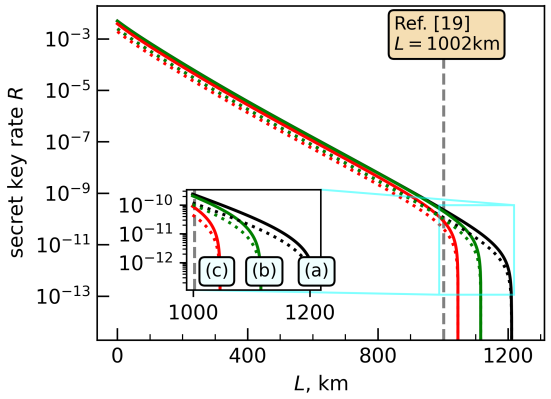

图 11. SNS-PM-QKD（实线表示 $\tilde{R}_{\rm real}(L)$，虚线表示 $\tilde{R}'_{\rm real}(L)$）与文献 [19] 中实验SNS-TF-QKD的距离范围比较。请注意，比较中考虑了主动奇偶配对（AOPP）。对于图8中给出的 $\epsilon = f(L)$，SNS-PM-QKD的密钥率根据公式（58）计算，其中 $L_{\max} = 1200$ km。根据 [19], 中给出的结果，实验SNS-TF-QKD的最大可实现距离为 $L = 1002$km。为与文献 [19], 的结果保持一致，SNS-PM-QKD的密钥率采用协议参数 $\eta_{\rm det} = 0.6$、$\alpha_{\rm average} = 0.157$ $f_{\rm EC} = 1.16$ dB/km 计算。强度参数 μ 取 0.1，使 SNS-PM-QKD 达到最大距离。请注意，SNS-PM-QKD中的失配和暗计数率建模方式均与文献 [19] 不同。为进行恰当的距离范围比较，我们给出了三元组（$p_{\rm dark}$、$\delta = V$、10^{-11} $\delta = \frac{\pi}{35}$ $V = 0.9$ $p_{\rm dark} = 5 \times 10^{-11}$）

取若干数值时SNS-PM-QKD的速率-距离图：(a)（$\delta = \frac{\pi}{60}$、$V = 0.95$、）；(b)（、、）；(c)（$\delta = \frac{\pi}{3}$、$\overline{V} = 0.85$、$p_{\rm dark} = 10^{-10}$）。对于(a)，SNS-PM-QKD（采用随机化的SNS-PM-QKD）的距离范围为1211km；对于(b)为1116km；对于(c)为1046km。

$\varphi = \phi = 0$， $\delta = \frac{\pi}{60}$， $V = 0.95$——这一情形对应于**发送—发送（ss）**配置，以及 Z 由双方选定的（信号）轮次 *Alice* 和 *Bob* 在SNS-PM-QKD 协议中（见第IIA节）。耦合器的输出态通常可表示为

$$\left|e^{i\varphi}\sqrt{\mu} - e^{i\delta}e^{i\phi}\sqrt{V}\sqrt{\mu}\right\rangle = \left|e^{i\phi}(e^{i(\varphi-\phi)} - e^{i\delta}\sqrt{V})\sqrt{\mu}\right\rangle = \left|e^{i\phi}(e^{i\Delta} - e^{i\delta}\sqrt{V})\sqrt{\mu}\right\rangle = |\sigma\rangle\,.$$

该态可以改写为

$$\left||\sigma|\cdot e^{i\omega}\right\rangle$$

其中

$$|\sigma| = \sqrt{\mathrm{Re}(\sigma)^2 + \mathrm{Im}(\sigma)^2} = \sqrt{(1 + V - 2\sqrt{V}\cos(\Delta - \delta))\mu},$$
$$\omega = \mathrm{atan}\left(\frac{\mathrm{Im}(\sigma)}{\mathrm{Re}(\sigma)}\right).$$

给定 $\varphi = \phi = 0$、$\delta = \frac{\pi}{60}$ 和 $V = 0.95$，耦合器的输出态变为

$$\left|\sqrt{0.00427\mu}e^{i\omega}\right\rangle = \left|\sqrt{\gamma}e^{i\omega}\right\rangle.$$

现在我们按照参考文献 [10]，将上述相干态用标准基表示。单个相干态

$$\left|\sqrt{\gamma}e^{i\omega}\right\rangle = e^{-\frac{1}{2}|\sqrt{\gamma}e^{i\omega}|^2}\sum_{n=0}^{\infty}\frac{(\sqrt{\gamma}e^{i\omega})^n}{\sqrt{n!}}|n\rangle\,, \tag{A1}$$

可以用基 $\{|e_0\rangle, |e_1\rangle\}$ [10] 表示为

$$\left|\sqrt{\gamma}e^{i\omega}\right\rangle = c_0(e^{i\omega})^{2n}|e_0\rangle + c_1(e^{i\omega})^{2n+1}|e_1\rangle\,, \tag{A2}$$

其中

$$\begin{aligned}|e_0\rangle &= \frac{1}{\sqrt{\cosh(|\sqrt{\gamma}e^{i\omega}|^2)}}\sum_{n=0}^{\infty}\frac{(\sqrt{\gamma})^{2n}}{\sqrt{2n!}}|2n\rangle\,,\\ |e_1\rangle &= \frac{1}{\sqrt{\sinh(|\sqrt{\gamma}e^{i\omega}|^2)}}\sum_{n=0}^{\infty}\frac{(\sqrt{\gamma})^{2n+1}}{\sqrt{(2n+1)!}}|2n+1\rangle\,,\end{aligned} \tag{A3}$$

and

$$\begin{aligned}c_0(\gamma) &= e^{-\frac{|\sqrt{\gamma}e^{i\omega}|^2}{2}}\sqrt{\cosh(|\sqrt{\gamma}e^{i\omega}|^2)},\\ c_1(\gamma) &= e^{-\frac{|\sqrt{\gamma}e^{i\omega}|^2}{2}}\sqrt{\sinh(|\sqrt{\gamma}e^{i\omega}|^2)}.\end{aligned} \tag{A4}$$

如文献 [10], 所述，复因子 $e^{i\omega}$ （式（$i\omega$）中的系数 e^{2n} 和（$e^{i\omega}$）$^{2n+1}$）可以吸收到 A2 的定义中，以及 $|e_0\rangle$ 和 $|e_1\rangle$ 的定义中。也就是说，式（A3）变为

$$\begin{aligned}|e'_0\rangle &= \frac{(e^{i\omega})^{2n}}{\sqrt{\cosh(|\sqrt{\gamma}e^{i\omega}|^2)}}\sum_{n=0}^{\infty}\frac{(\sqrt{\gamma})^{2n}}{\sqrt{2n!}}|2n\rangle\,,\\ |e'_1\rangle &= \frac{(e^{i\omega})^{2n+1}}{\sqrt{\sinh(|\sqrt{\gamma}e^{i\omega}|^2)}}\sum_{n=0}^{\infty}\frac{(\sqrt{\gamma})^{2n+1}}{\sqrt{(2n+1)!}}|2n+1\rangle\,.\end{aligned} \tag{A5}$$

因此，对于**发送—发送（ss）**配置，耦合器的输出态可以写成具有实值振幅的规范形式，如下所示

$$\left|\sqrt{\gamma}\cdot e^{i\omega}\right\rangle \to |\sqrt{\gamma}\rangle = c_0(\gamma)\,|e'_0\rangle - c_1(\gamma)\,|e'_1\rangle\,. \tag{A6}$$

在**发送—发送（ss）**配置的情况下，对于给定的具有相位随机化的 SNS-PM-QKD（见第IIB节），耦合器的输出态取如下形式

$$\left|e^{i\nu_b}(e^{i(\nu_a-\nu_b)} - e^{i\delta}\sqrt{V})\sqrt{\mu}\right\rangle = \left||\lambda|\cdot e^{i\zeta}\right\rangle$$

其中

$$|\lambda| = \sqrt{(1 + V - 2\sqrt{V}\cos((\nu_a - \nu_b) - \delta))\mu},$$
$$\zeta = \mathrm{atan}\left(\frac{\mathrm{Im}(\lambda)}{\mathrm{Re}(\lambda)}\right).$$

请注意，对于给定的相位区间（$\nu_{a(b)} \in [0, \pi)$ 或 $\nu_{a(b)} \in [\pi, 2\pi)$）。考虑到强度 $|\lambda|$ 越高，**发送—发送（ss）**配置引起的错误率就越高。因此，最坏情况

对于**发送—发送（ss）**配置而言，最坏情况（max(|λ|)）是耦合器输出态的强度为

$$\max_{\nu_a-\nu_b}(|\lambda|)=\sqrt{(1+V-2\sqrt{V}\cos((\delta-\pi)-\delta))\mu}=\sqrt{\psi}.$$

这意味着，在带随机化的SNS-PM-QKD中，发送—发送（ss）**配置**的最坏情况出现在 $\nu_a-\nu_b=\delta-\pi$ （即， $\nu_b>\nu_a$ 给定 $\delta<\pi$）。相

应的输出相干态具有规范形式

$$\left|\sqrt{\psi}\cdot e^{i\zeta}\right\rangle\rightarrow\left|\sqrt{\psi}\right\rangle=c_0(\psi)\left|e_0'\right\rangle-c_1(\psi)\left|e_1'\right\rangle. \quad \text{(A7)}$$

考虑方程（A2）-（A6）后。我们利用$\left|\sqrt{\psi}\right\rangle$ 来计算协议密钥率的最小值（方程（62）和（64）），从而得到最坏情形下的密钥率（即错误率达到最大值时）。

附录 B：POVM算符

POVM 算子 F^-、 F^+、 $F^?$（仅损耗情形）的矩阵表示如下 [10]

$$F^-=(1-\xi^2)\begin{bmatrix}\frac{1-\xi^2\Omega^2}{8c_0^4} & \frac{-1+\xi^2\Omega^2}{8c_0^2c_1^2} & 0 & 0\\ \frac{-1+\xi^2\Omega^2}{8c_0^2c_1^2} & \frac{1-\xi^2\Omega^2}{8c_1^4} & 0 & 0\\ 0 & 0 & \frac{1+\xi^2\Omega^2}{8c_0^2c_1^2} & \frac{-1-\xi^2\Omega^2}{8c_0^2c_1^2}\\ 0 & 0 & \frac{-1-\xi^2\Omega^2}{8c_0^2c_1^2} & \frac{1+\xi^2\Omega^2}{8c_0^2c_1^2}\end{bmatrix} \quad \text{(B1)}$$

$$F^+=(1-\xi^2)\begin{bmatrix}\frac{1-\xi^2\Omega^2}{8c_0^4} & \frac{1-\xi^2\Omega^2}{8c_0^2c_1^2} & 0 & 0\\ \frac{1-\xi^2\Omega^2}{8c_0^2c_1^2} & \frac{1-\xi^2\Omega^2}{8c_1^4} & 0 & 0\\ 0 & 0 & \frac{1+\xi^2\Omega^2}{8c_0^2c_1^2} & \frac{1+\xi^2\Omega^2}{8c_0^2c_1^2}\\ 0 & 0 & \frac{1+\xi^2\Omega^2}{8c_0^2c_1^2} & \frac{1+\xi^2\Omega^2}{8c_0^2c_1^2}\end{bmatrix} \quad \text{(B2)}$$

$$F^?=\xi^2\begin{bmatrix}\frac{(1+\Omega)^2}{4c_0^4} & 0 & 0 & 0\\ 0 & \frac{(1-\Omega)^2}{4c_1^4} & 0 & 0\\ 0 & 0 & \frac{1-\Omega^2}{4c_0^2c_1^2} & 0\\ 0 & 0 & 0 & \frac{1-\Omega^2}{4c_0^2c_1^2}\end{bmatrix} \quad \text{(B3)}$$

POVM 算子 F^- 不完美因素、 F^+ 不完美因素 （现实情形，不完美因素）的矩阵表示为

$$F^-_{\text{imp}}=(1-p_{\text{dark}})F^-_{\text{mis}}+(1-p_{\text{dark}})p_{\text{dark}}F^?_{\text{mis}} \quad \text{(B4)}$$

$$F^+_{\text{imp}}=(1-p_{\text{dark}})F^+_{\text{mis}}+(1-p_{\text{dark}})p_{\text{dark}}F^?_{\text{mis}} \quad \text{(B5)}$$

其中

$$
F_{\text{mis}}^{-}=\begin{bmatrix}
\frac{a+b+2c+2d+o+p}{8c_0^4} & -\frac{a+b-o-p}{8c_0^2c_1^2} & 0 & 0\\
-\frac{a+b-o-p}{8c_0^2c_1^2} & \frac{a+b-2c-2d+o+p}{8c_1^4} & 0 & 0\\
0 & 0 & \frac{a-b+o-p}{8c_0^2c_1^2} & -\frac{a-b+2c-2d-o+p}{8c_0^2c_1^2}\\
0 & 0 & -\frac{a-b-2c+2d-o+p}{8c_0^2c_1^2} & \frac{a-b+o-p}{8c_0^2c_1^2}
\end{bmatrix}
$$

$$
F_{\text{mis}}^{+}=\begin{bmatrix}
\frac{a+b+2c+2d+o+p}{8c_0^4} & \frac{a+b-o-p}{8c_0^2c_1^2} & 0 & 0\\
\frac{a+b-o-p}{8c_0^2c_1^2} & \frac{a+b-2c-2d+o+p}{8c_1^4} & 0 & 0\\
0 & 0 & \frac{a-b+o-p}{8c_0^2c_1^2} & \frac{a-b+2c-2d-o+p}{8c_0^2c_1^2}\\
0 & 0 & \frac{a-b-2c+2d-o+p}{8c_0^2c_1^2} & \frac{a-b+o-p}{8c_0^2c_1^2}
\end{bmatrix}
\tag{B6}
$$

$$
F_{\text{mis}}^{?}=\xi^2\begin{bmatrix}
\frac{(1+\Omega)^2}{4c_0^4} & 0 & 0 & 0\\
0 & \frac{(1-\Omega)^2}{4c_1^4} & 0 & 0\\
0 & 0 & \frac{1-\Omega^2}{4c_0^2c_1^2} & 0\\
0 & 0 & 0 & \frac{1-\Omega^2}{4c_0^2c_1^2}
\end{bmatrix}
$$

注意，$\xi = e^{-\sqrt{\eta}\mu}$、$\Omega = \eta_{\text{det}}^2\eta_t = \eta_{\text{det}}^2 10^{-\frac{0.2L}{10}}$ = − η = $e^{-2(1-\sqrt{\eta})\mu}$，其中 是总 透射率，适用于距-程 L [千米]。请注意， [10]

$$
\begin{aligned}
&a=(1-\xi^{1+\sqrt{V}\cos\delta})\xi^{1-\sqrt{V}\cos\delta},\quad b=(\xi^{2(1+\sqrt{V}\cos\delta)}-\xi^{1+\sqrt{V}\cos\delta})\xi^{1-\sqrt{V}\cos\delta}\Omega^2,\quad c=(\xi^{1+i\sqrt{V}\sin\delta}-\xi)\xi\Omega,\\
&d=(\xi^{1-i\sqrt{V}\sin\delta}-\xi)\xi\Omega,\quad o=(1-\xi^{1-\sqrt{V}\cos\delta})\xi^{1+\sqrt{V}\cos\delta},\quad p=(\xi^{2(1-\sqrt{V}\cos\delta)}-\xi^{1-\sqrt{V}\cos\delta})\xi^{1+\sqrt{V}\cos\delta}\Omega^2
\end{aligned}
\tag{B7}
$$

系数 c_0 和 c_1 定义见公式 A4。

[1] C. Bennett 和 G. Brassard，载于 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*（IEEE计算机学会出版社，印度班加罗尔，1984年），第 175–179 页。[2] A. Ekert，《物理评论快报》67，661（1991年）。[3] C. Bennett，《物理评论快报》68，3121（1992年）。[4] W.-Y. Hwang，《物理评论快报》91，057901（2003年）。[5] H.-K. Lo、H. Chau 和 M. Ardehali，《密码学杂志》18，133（2005年）。[6] H.-K. Lo、M. Curty 和 B. Qi，《物理评论快报》108，130503（2012年）。[7] M. Lucamarini、Z. Yuan、J. Dynes 和 A. Shields，《自然》557，400（2018年）。[8] M. Curty、K. Azuma 和 H.-K. Lo，npj Quantum Information 5，64（2019年）。[9] X. Ma、P. Zeng 和 H. Zhou，《物理评论X》8，031043（2018年）。[10] J. Lin 和 N. L¨utkenhaus，《物理评论A》98，042332（2018年）。[11] X.-B. Wang、Z.-W. Yu 和 X.-L. Hu，《物理评论A》**98**，062323（2018年）。[12] Y.-G. Shan、Y. Zhou、Z.-Q. Yin、S. Wang、W. Chen、D.- Y. He、G.-C. Guo 和 Z.-F. Han，《物理评论应用》**22**，024056（2024年）。[13] H. Xu、Z.-W. Yu、C. Jiang、X.-L. Hu 和 X.-B. Wang，《物理评论A》**101**，042330（2020年）。[14] C. Jiang、X.-L. Hu、H. Xu、Z.-W. Yu 和 X.-B. Wang，《新物理学杂志》**22**，053048（2020年）。[15] H. Liu、C. Jiang、H.-T. Zhu、M. Zou、Z.-W. Yu、X.-L. Hu、H. Xu、S. Ma、Z. Han、J.-P. Chen、Y. Dai、S.-B. Tang、W. Zhang、H. Li、L. You、Z. Wang、Y. Hua、H. Hu、H. Zhang、G. Zhou、Q. Zhang、X.-B. Wang、T.-Y. Chen 和 J.-W. Pan，《物理评论快报》**126**，250502（2021年）。[16] J.-P. Chen、C. Zhang、Y. Liu、C. Jiang、W. Zhang、X.- L. Hu、J.-Y. Guan、Z.-W. Yu、H. Xu、J. Lin、M.-J. Li、H. Chen、H. Li、L. You、Z. Wang、X.-B. Wang、Q. Zhang 和 J.-W. Pan，《物理评论快报》**124**，070501（2020年）。[17] J.-P. Chen、C. Zhang、Y. Liu、C. Jiang、W.-J. Zhang、Z.-

Y. Han、S.-Z. Ma、X.-L. Hu、Y.-H. Li、H. Liu、F. Zhou、H.-F. Jiang、T.-Y. C. an H. Li、L.-X. You、Z. Wang、X.-B. Wang、Q. Zhang 和 J.-W. Pan，《自然·光子学》**15**，570（2021年）。[18] Y. Liu、Z.-W. Yu、W. Zhang、J.-Y. Guan、J.-P. Chen、C. Zhang、X.-L. Hu、H. Li、C. Jiang、J. Lin、T.-Y. Chen、L. YOu、Z. Wang、X.-B. Wang、Q. Zhang 和 J.-W. Pan，《物理评论快报》**123**，100505（2019）。[19] Y. Liu、W.-J. Zhang、C. Jiang、J.-P. Chen、C. Zhang、W.-X. Pan、D. Ma、H. Dong、J.-M. Xiong、C.-J. Zhang、H. Li、R.-C. Wang、J. Wu、T.-Y. Chen、L. You、X.-B. Wang、Q. Zhang 和 J.-W. Pan，《物理评论快报》**130**，210801（2023）。[20] *Note*：相位 φ_b 和 τ_a 选取一个额外值π（$\varphi_b = 0 + \pi$，$\tau_a = 0 + \pi$) 在耦合器$\mathbf{C_s}$ 和 $\mathbf{C_r}$，分别如此，因为对应的相干态$\left|e^{i\varphi_b}\sqrt{\mu}\right\rangle_{Q'}$ 和 $\left|e^{i\tau_a}\sqrt{\mu}\right\rangle_{T}$ 在这些器件处发生反射。[21] A. Ferenczi，*Security proof methods for quantum key distribution protocols*，博士论文，加拿大滑铁卢大学（2013）。[22] I. Devetak 和 A. Winter，《皇家学会学报A辑》**461**，207（2005）。[23] 该量由实验观测确定。它与变量 k 和 y之间的相关性（反相关性）成正比。[24] 注意，观测 $[\varkappa' =? \varkappa'' = +]$ 会得出相同的结果。