arXiv:2305.01946v1 [quant-ph] 3 May 2023

用于量子密码学的受控纠缠源

Qiang Zeng, [1], * Haoyang Wang, [1,2] Huihong Yuan, [1] Yuanbin Fan,
[1] Lai Zhou, [1] Yuanfei Gao, [1] Haiqiang Ma, [2] 和 Zhiliang Yuan[1], †

[1] *Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
[2] *School of Science and State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China*(日期：2023年5月4日)

量子纠缠已成为量子信息处理中的一种重要资源。现有研究利用纠缠量子态执行各种任务，但很少关注对这一资源的控制。在本研究中，我们提出了一种简单的协议，通过对光泵浦进行相位随机化，为纠缠源添加访问控制功能。增强后的纠缠源能够有效控制所有用户对纠缠资源的使用，从而实现量子密码学。此外，我们证明，这种控制方式可以作为一种实用的对策，以极低的成本抵御针对设备无关量子密钥分发的记忆攻击。为验证该协议的可行性，我们仅使用现成的标准组件搭建了实验装置，并对其性能进行了相应表征。

I. 引言

现代社会建立在可靠、安全的通信之上。当前的密码系统能够防御窃听以及基于计算复杂度的攻击，但随着量子技术的发展，这些系统正变得脆弱 [1]。量子密钥分发 [2–7] 使相距遥远的用户能够建立密钥，其安全性不依赖于攻击者的计算能力，而是基于基本物理原理，从而保证信息论安全性 [8]。特别是，基于纠缠的量子密钥分发协议 [3, 9]相较于使用弱相干脉冲的量子密钥分发 [10–12] 无需强度调制 [4, 5]，且天然适用于多用户 [13–17]。此外，量子安全通信的终极形式—— [18], 设备无关量子密钥分发协议 [19, 20], 利用量子纠缠中超越经典区域的强关联，彻底消除了对量子密钥分发用户所用装置的信任需求。其背后的核心思想是，设备无关量子密钥分发的安全性要求排除局域隐变量模型的存在 [21] 这些装置的，而这样的模型可被视为某种预设的共谋，在传统量子密钥分发中无法加以区分 [22]。

确实，对信任程度较低的要求，意味着对实际设备性能提出了更高的要求。要忠实地实现设备无关量子密钥分发，高质量的纠缠资源是防御集体攻击的先决条件 [23]。此外，从该资源到两位用户都需要具备较高的探测效率，以确保统计数据无偏，从而防御探测效率攻击 [24, 25]。此外，测量设备应当是 无记忆 的，以防止通过追踪重复使用设备的历史统计数据而泄露信息，这种攻击被称为记忆攻击 [26]。幸运的是，近期的研究进展表明，上述问题可以得到妥善解决，从而满足最先进设备的能力要求。值得注意的是，近期已经展示了三项实际的设备无关量子密钥分发实验 [18, 27, 28]。

量子纠缠有望在未来网络中作为一种有用的资源发挥作用，成为一种量子公用事业，就像当今能源电网中的电力和天然气一样。例如，经销商将纠缠态分发给用户以建立密钥——这些纠缠态通常由光子承载，因为光子是远距离传输信息的最佳载体。然而，尽管资源控制显然十分重要，这一主题却鲜有讨论。如图1所示，传统的纠缠服务器会持续向通信用户对分发最大纠缠态。然而，服务器无法控制所分发的光子是否确实由授权用户使用。未授权用户可以从信道中截取纠缠光子，用于生成自己的密钥，而不会被察觉。

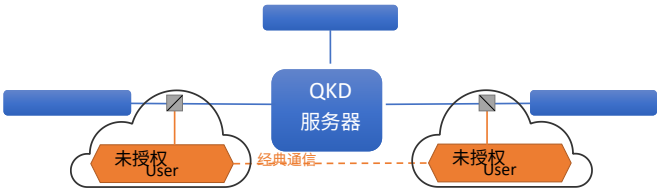

图 1：基于纠缠的量子密钥分发网络示意图，其中包含授权用户和未授权用户。

令人惊讶的是，对纠缠源进行控制也能防范设备无关量子密钥分发中的存储器攻击 [26] 。在这类攻击中，当测量设备被重复使用时，攻击者可以在不被发现的情况下，获取此前会话中生成的安全密钥。现有的应对措施 [26, 29], 包括销毁用过的测量设备、严格隔离纠缠生成设备，或使用额外的备用设备；这

* zengqiang@baqis.ac.cn
† yuanzl@baqis.ac.cn

些措施本质上能阻止攻击者获取（可能已被记录的）信息，但会大幅增加系统的复杂性，更不用说高昂的成本。

量子力学通过量子秘密共享（QSS）提供了一种优雅的解决方案来解决控制问题 [30, 31]。其实现最初需要使用特殊的多光子 Greenberger-Horne-Zeilinger（GHZ）态 [32, 33], ，但通过使用伪GHZ态，已大幅简化。这种态仅由光子对组成，因此得以实现基于时间箱纠缠的量子秘密共享演示 [34]。最近，双光子量子秘密共享方案成功扩展到了偏振编码 [35]。

受双光子量子秘密共享协议 [34], 的启发，我们提出了一种简单却极为实用的方案：对传统纠缠源进行升级，使其具备访问控制功能，并引入二元伪随机性。进一步引入混合态后，我们表明，这种增强型纠缠源能够以可忽略的代价有效保护设备无关量子密钥分发免受存储器攻击。我们在时间箱编码系统中对该方案进行了实验验证。

II. 将相位调制用于纠缠源

我们首先简要回顾三方量子秘密共享协议。假设三方（例如 Alice、Bob 和 Coy）共享一个三量子比特 GHZ态 $|\Psi\rangle_{\mathrm{GHZ}} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$。若 Alice 在本地进行测量 σ_{X} 或σ_{Y} ，其中 σ_{X} 和 σ_{Y} 为泡利矩阵，则根据 Alice 本地测量的结果，另外两方之间共享的状态会被投影到以下四种可能状态之一：

$$\mathsf{X}_A^{\pm} \rightarrowtail |\phi^{\pm}\rangle_{BC} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle),$$
$$\mathsf{Y}_A^{\pm} \rightarrowtail |\psi^{\mp}\rangle_{BC} = \frac{1}{\sqrt{2}}(|00\rangle \mp i|11\rangle),$$

其中，$\mathsf{X}^{\pm} = \frac{1}{\sqrt{2}}$({v2)、$\mathsf{Y}^{\pm} = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle$分别是 σ_{X} 和 σ_{Y}的本征态。因此，如果 Bob 和 Coy 想要执行传统的纠缠基量子密钥分发协议，就需要获知 Alice 的测量结果；从这个意义上说，Alice 可被视为量子密钥分发的控制器，这也称为第三方量子密码学 [33]。有研究指出，与其使用真正的三量子比特GHZ态，不如由控制器在本地制备并随机分发四种可能的双量子比特态 [34, 35], 因为控制器实际上无需对该状态进行测量。需要注意的是，Alice 的测量选择属于公开信息，因此在实际实现中，每次运行只有一比特信息是保密的。出于控制目的，我们在此指出，固定一种测量设置就足够了。

在我们的方案中，我们以相同的概率随机地为纠缠量子比特赋予 0 和 π 相对相位，这等价于在控制器一侧执行测量 σ_{X} ，因此，该源向终端用户分发状态 $|\phi^+\rangle$ 和 $|\phi^-\rangle$ 的随机混合态。请注意，这两个状态相对于测量 σ_{X}、 σ_{Y} 以及叠加态 $\sigma_{\mathsf{X}\pm\mathsf{Y}}$ 具有相反的关联。纠缠基量子密钥分发的安全性分析通常需要证明贝尔型不等式（例如 Clauser-Horne-Shimony-Holt (CHSH) 不等式 [36]）被违反。具体而言，CHSH 参数 [36] 可写为

$$S_{\mathrm{CHSH}} := E(\sigma_{\mathsf{X}}, \sigma_{\mathsf{X}+\mathsf{Y}}) + E(\sigma_{\mathsf{Y}}, \sigma_{\mathsf{X}+\mathsf{Y}}) + E(\sigma_{\mathsf{X}}, \sigma_{\mathsf{X}-\mathsf{Y}}) - E(\sigma_{\mathsf{Y}}, \sigma_{\mathsf{X}-\mathsf{Y}}), \tag{1}$$

其中

$$E(\alpha, \beta) := p^{++}_{\alpha,\beta} + p^{--}_{\alpha,\beta} - p^{+-}_{\alpha,\beta} - p^{-+}_{\alpha,\beta} \tag{2}$$

是相关函数，由测量 α 和 β时四种可能结果组合的概率构成。相关函数 E 量化了光子对的关联，假设输出“++”和“−−”的符合事件表示相关，而“+−”和“−+”表示反相关。在经典区域的局域性假设下， S_{CHSH}的上限为 2。然而，在量子区域，纠缠态具有很强的关联，突破了局域性限制 [37]，其上限为 $2\sqrt{2}$。因此，$S_{\mathrm{CHSH}} > 2$ 可确保该源确实是量子的（或更一般地说，满足无信号条件 [20]），且未受到攻击者操纵。

对于状态 $|\phi^+\rangle$ ，S_{CHSH} 的期望值为 $2\sqrt{2}$；而对于 $|\phi^-\rangle$ ，则为 $-2\sqrt{2}$。因此，如果未能正确区分这两种状态，它们的均匀混合态$|\phi^+\rangle$ 和 $|\phi^-\rangle$ 会得到 $S_{\mathrm{CHSH}} = 0$。换言之，两个用户对每种状态的确切关联了解得有多充分，决定了是否能够认证这种违背。我们将在下一节量化相位调制的影响。

上述方案存在一个主要技术问题：如何高效地将调制信息传递给合法用户。在量子秘密共享协议的忠实执行过程中，经销商持有的原始密钥对应于调制信息，其长度与每位用户持有的原始密钥相同。这迫使控制器主动参与实施过程，并为用户探测到的每个符合事件记录一个相位比特，从而增加了实施的复杂性。更理想的做法是，控制器预先与合法用户共享一串调制信息，由他们选择与光子探测相对应的比特。但这样一来，为抵消传输过程中的显著损耗，该字符串必须远长于最终的原始密钥。人们或许会认为，重复一个固定长度的随机二进制字符串即可作为预共享调制字符串。然而，正如我们在附录A中所解释的那样，无论预共享调制字符串的长度有限，无授权用户总能协作并揭示其中的模式。由于信源需要在整个会话期间生成随机比特，一种实用的解决方案是使用分组密码算法 [，例如高级加密标准（AES），[38]]

采用流加密模式，这种模式常用于制备-测量型量子密钥分发实现中的比特扩展 [39]。这样，只需少量预共享随机数作为种子。

III. 真正的相位随机化及防御记忆攻击

尽管上述方案能够防止非预期使用，但无法直接用于防御记忆攻 [26], 击，因为在这类攻击中，攻击者能够完全获知用户的测量选择和结果。如果攻击者将前一轮会话中记录的密钥生成数据结合起来，正如我们在附录A中所讨论的，由于测量结果与调制比特相对应，他们可以立即根据原始密钥获知调制字符串。问题在于，即使原始密钥完全暴露，是否仍能防止调制信息泄露。下文将证明，这确实可以做到。

基本思路是将可检测的二元伪随机性隐藏在真正的随机性中。具体而言，我们以 p 的概率对最大纠缠态施加随机相位，从而破坏相位关联。这在实际效果上等同于向用户分发一个混合态，可写为

$$\hat{R} = (|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|)/2. \tag{3}$$

因此，信源现在会向用户随机分发三种可能的状态：$|\phi^+\rangle$、$|\phi^-\rangle$ 和 $\hat{R}$，其对应概率分别为 $(1-p)/2$、$(1-p)/2$ 和 p。由于每位用户的本地状态保持不变（$\mathbb{1}/2$），恶意设备无法从测量结果中泄露控制字符串，因为在缺乏足够辅助信息的情况下，不可能从混合态中还原出特定形式的分解。即使设备记录了原始密钥并设法将其发送出去，窃听者仍无法获取先前会话中的安全密钥，因为密钥生成过程经过加密。更确切地说，有效原始密钥是通过从测量结果中筛选出真正随机的比特而获得的。我们指出，测量结果应传输至隔离且可信的计算机，并在这些持有调制信息的计算机上进行后处理。

IV. 受控纠缠源协议

现在，我们详细说明该协议的执行过程。

(1) 与传统的基于纠缠的量子密钥分发协议类似，分发者和用户需要协调各自装置的配置，包括时钟同步时钟 [13], ，但还需额外使用一个参数，即预共享种子的令牌。

(2) 通过同一分组密码算法在流加密模式下运行，将选定的种子在本地扩展为连续的随机字符串。根据某种规则，将该随机字符串（最可能是二进制的）转换为三进制，并适当设定三进制位“2”的比例。规则可以非常简单。例如，检查随机字符串中每两个连续的比特：如果这两个比特是“11”，则在生成的三进制随机字符串中赋值为“2”；否则，若这两个比特分别是“00”“01”或“10”，则相应赋值为“00”“01”或“10”。控制器根据三进制随机字符串，不断向用户分发三种元素态之一：$|\phi^+\rangle$（三进制位“0”）、$|\phi^-\rangle$（三进制位“1”）和 $\hat{R}$（三进制位“2”）。

(3) 用户随机为其设备选择测量基，并在光子探测时获得一个二元结果（“+”或“−”）。请注意，如果实施记忆攻击，测量选择及其对应结果可能会被记录并泄露。

(4) 在进行足够多轮后，控制器停止分发，且不再参与后续过程。与此同时，用户公开宣布各自的测量基，并筛除协议中不需要的测量基组合。

(5) 在其余结果中，用户选择公开宣布与安全性分析相关的部分测量结果，例如测量 σ_X、σ_Y 和 $\sigma_{X\pm Y}$。每种测量组合的结果在双方各自形成经典比特串 $\boldsymbol{T}^{1(2)}{}_{\mathrm{O}}$，其中上标表示用户。由于时钟已同步，若用户是合法用户，则可根据光子探测的时间，从阶段 (1) 中准备的本地随机数字符串推导出解码字符串 $\boldsymbol{T}_{\mathrm{D}}$。进一步从 $\boldsymbol{T}_{\mathrm{D}}$ 中省略三进制位“2”，并从 $\boldsymbol{T}^{1(2)}{}_{\mathrm{O}}$ 中省略对应的比特后，任一用户都可以根据 $\boldsymbol{T}^{1}{}_{\mathrm{O}} \oplus \boldsymbol{T}_{\mathrm{D}}$ 和 $\boldsymbol{T}^{2}{}_{\mathrm{O}}$，或 $\boldsymbol{T}^{1}_{\mathrm{O}}$ 和 $\boldsymbol{T}^{2}_{\mathrm{O}} \oplus \boldsymbol{T}_{\mathrm{D}}$ 的统计数据计算 CHSH 函数，从而验证安全性。在此阶段，未授权用户将无法通过测试，因为他们不持有有效的 $\boldsymbol{T}_{\mathrm{D}}$。

为使这一点更加具体，方便起见，假设用户实际持有字符串 $\boldsymbol{T}_{\mathrm{U}}$，并且我们使用 $\boldsymbol{T}_{\mathrm{U}}$ 与 $\boldsymbol{T}_{\mathrm{D}}$ 之间的关联来定义控制的有效性：

$$U := \sum_{j\in\boldsymbol{T}}^{N} \frac{(-1)^j}{N}, \tag{4}$$

其中 $\boldsymbol{T} = \boldsymbol{T}_{\mathrm{U}} \oplus \boldsymbol{T}_{\mathrm{D}}$ 省略了三进制数“2”，N 是 $\boldsymbol{T}$的长度。注意，混合态 R的关联始终为零，选中纠缠元素的概率为 $(1-p)$。因此，经过调制后，相关函数可写为

$$E_{\mathrm{mod}} = U(1-p)E, \tag{5}$$

其中 E 由方程（2）定义。例如，如果 T_{D} =“01010101，”且 T_{U} = “00000000，”那么 U = 0。在

在这种情况下，用户无法完全区分应采用的正确关联，这将导致 $E_{\mathrm{mod}} = 0$，因此获得的 $S_{\mathrm{CHSH}} = 0$（经过调制），并且他们将不得不中止以避免安全性风险。对于一般的 T_{D}，我们在附录B中推导了未授权用户的最优 U，在给定合理长度的调制字符串时，该值远低于证明不等式违背的要求。

(6) 一旦安全性得到认证，用户便可以基于在相同测量基下获得的测量结果，采用传统的纠错和隐私放大方法来获得最终的安全密钥。然而，这意味着如果测量结果被公开，攻击者总能生成相同的密钥，因为纠错和隐私放大方法实际上是公开的，而这正是记忆攻击得以攻破系统的方式。通过引入混合态，在后处理阶段，双方会舍弃一定比例的不相关原始测量结果，而攻击者无法知晓具体舍弃了哪些结果。因此，尽管采用相同的纠错和放大方法，攻击者一侧根据原始测量结果推导出的安全密钥仍然无效。不过，混合态的比例需要权衡，因为混合态不携带任何信息，却能够干扰攻击。我们注意到，p 的设置取决于实际情况，例如信道损耗。

我们承认，对抗记忆的安全性最终源自经典密钥，而量子密钥分发协议不会产生额外的永久安全数据。因此我们强调，为确保协议的长期可靠性，控制器需要定期（例如每天用一小部分时间）与其他用户通信，以刷新种子，而不是使用固定的预共享种子。值得一提的是，尽管控制器控制着量子密钥分发实现，但它无法获得任何关于用户安全密钥的信息。

我们将上述方案命名为受控纠缠源（*CES*）协议，在该协议下，S_{mod} 与 U 和 p 之间的估计关系为

$$S_{\mathrm{mod}} = 2\sqrt{2}(1-p)U, \tag{6}$$

这是由公式（5）直接推导出的结果。由于在实际实现中，人们只关心 S_{CHSH}的绝对值，因此我们引入 $B = h\left((1+U)/2\right)$ 以便将 S_{mod} 化为正半轴，简洁起见，其中$h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$为二进制

熵函数。注意，B 本身具有明确的物理意义，即用户为获取关联而需要消除的不确定性量。图 S_{mod} 展示了2中的表达式，形成一个曲面。绿色平面表示 CHSH 违背的阈值，其交点表明用户要演示这种违背所需的信息量（或区分混合态的能力）。例如，根据（B，x）平面上的交点（对应于无 z）处，若熵小于 0.6 比特，则可能出现违背。

涉及混合态），这相当于超过 85.3% 的用户解码字符串与调制字符串（或其补码）相同。

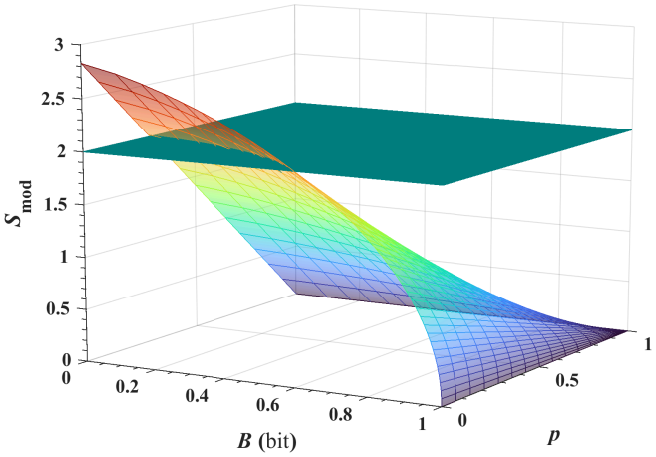

图 2： S_{CHSH} 作为关于 B 二元熵和 p 混合态比例的函数的示意图。

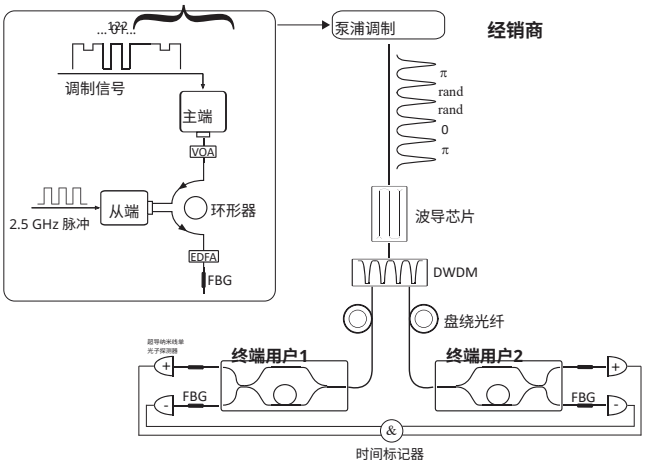

图 3：受控纠缠源的实验装置。请注意，调制字符串中的数字“2”表示真正随机化的相位。VOA，可变光衰减器；掺铒光纤放大器；FBG，光纤布拉格光栅；SNSPD，超导纳米线单光子探测器。

V. 实验装置与结果

为证明我们协议的可行性，我们使用现成组件搭建了实验装置，如图 3所示。在经销商一侧，一串经过相位调制的 [40] 泵浦脉冲被发送至硅波导芯片 [41, 42], ，其中通过自发

四波混频（SFWM）效应实现时间 bin 纠缠态。请注意，在我们的装置中，传统上部署于泵浦端、用于诱导时间 bin 叠加态的非对称干涉仪 [34]被省略了，这意味着我们源的时间 bin 延迟是可重构的。随后，所得的宽带信号-闲频光谱被导入密集波分复用器（DWDM）模块，从而被分成多个信道。在此演示中，我们选取了国际电信联盟（ITU）信道栅格中的信道 C30 和 C37（半高全宽：25 GHz）；需要指出的是，我们的系统还直接支持更多信道。在这一原理验证演示中，每条量子链路中的光纤盘均由一个 5 dB 固定衰减器进行模拟。最后，终端用户接收受控纠缠态，以实施量子密码学。关于调制信号生成和关联测试的详细说明见附录 C。

实验结果如下：实验装置的整体预示效率为 1.6%，其中包括光子波导芯片（−6.5dB）、传输和耦合（−7 dB）、光谱滤波（−4 dB）以及光子探测（−0.5 dB）造成的损耗。观测到的最大符合计数率超过 2 kHz，其中包括在时间基中探测到的符合（旁峰），符合-偶然符合比（CAR）为 50。在图 4a和 4b中，我们展示了调制后的 CHSH 参数结果，其与理论模型高度吻合。数据与理论之间的差异主要源于干涉不完美；观测到的纠缠可见度为 96.1(5)%（更多结果见附录 D），这一结果本身已充分满足在设备无关场景中防御集体攻击的要求 [43]。请注意，集体攻击独立于其他攻击。

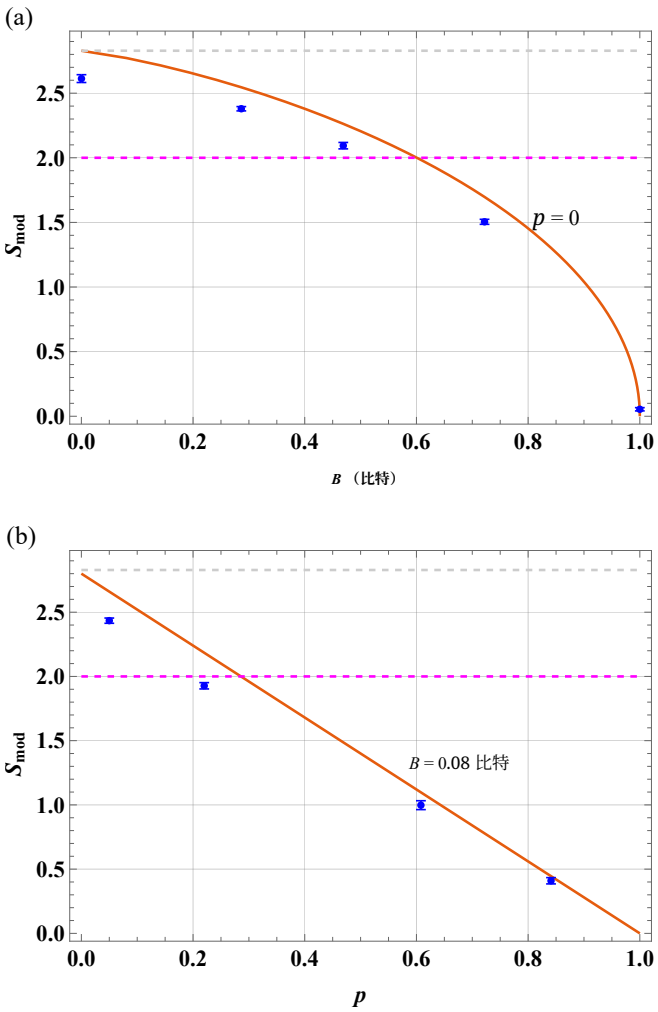

图 4：CHSH 参数在不同控制配置下的实验结果。红色实线表示理论预测，蓝色圆点表示实验结果。洋红色虚线表示不等式违背的阈值。

VI. 结论

研究表明，对纠缠资源的访问进行控制，对于防止量子密码学遭到滥用和恶意攻击至关重要。受量子秘密共享协议的启发，我们提出了一种协议，通过引入双重相位随机化，为传统纠缠源赋予访问控制能力。我们证明，在单重相位随机化下采用我们的协议，可以有效地控制纠缠分发方对用户的控制。此外，该协议还能防御针对测量装置的记忆攻击

在采用双重相位随机化的协议下，测量设备可以在我们的协议中安全地重复使用，因此成本可以忽略不计。

我们在使用现成器件的时间 bin 编码系统中，实验验证了协议的可行性，并精确展示了对纠缠源的控制。在我们的装置中，泵浦端的干涉仪得到了简化，这显著提高了系统的稳健性，并使时间 bin 延迟的可重构性得以提升至纠缠源。实验观测到的装置纠缠可见度超过 96%，表明传统的集体攻击得到了单独应对。我们相信，基于协议对现有纠缠源进行升级，能够显著提升其在量子密码学应用中的性能和灵活性。

致谢

作者感谢张伟教授在研究初期提供硅波导芯片。本研究得到中国国家自然科学基金资助，项目编号为 62105034（L. Z.）、12105010（Q. Z.）和 62250710162（Z. Y.）。

附录A：未授权用户的欺骗方案

我们首先指出，在原始的三方量子秘密共享协议中，假设参与者中只有一方不诚实，且经销商会与诚实的一方共享信息。值得注意的是，如果双方参与者都不诚实，量子秘密共享便毫无意义。在控制场景中，两名未授权用户都无法从光源获取任何信息，但如果他们合作（他们必然会这么做），就有可能推断出他们实际共享的是哪种状态；这不同于量子秘密共享，而更符合第三方量子密码学场景。显然，对于状态 $|\phi^+\rangle$，如果两人都测量 σ_X，他们几乎必然会在端口“++”或“−−”观测到符合事件（具体概率取决于纠缠可见度）。采用相同的测量设置时，如果他们轮流共享状态 $|\phi^-\rangle$，则很可能会在输出端“+−”或“−+”观测到符合事件。因此，只要事件数量足够多，无论调制字符串有多长（只要有限），他们最终都能找出其中的规律。

唯一的限制是，在公开调制字符串时，他们无法同时进行安全性认证，因为这需要切换非正交测量基；他们也无法生成密钥，因为此过程禁止通信测量结果。因此，源需要在整个会话期间持续分发随机比特，而不是重复使用固定长度的随机字符串，以确保未授权用户无法利用某种模式来实施量子密钥分发协议。

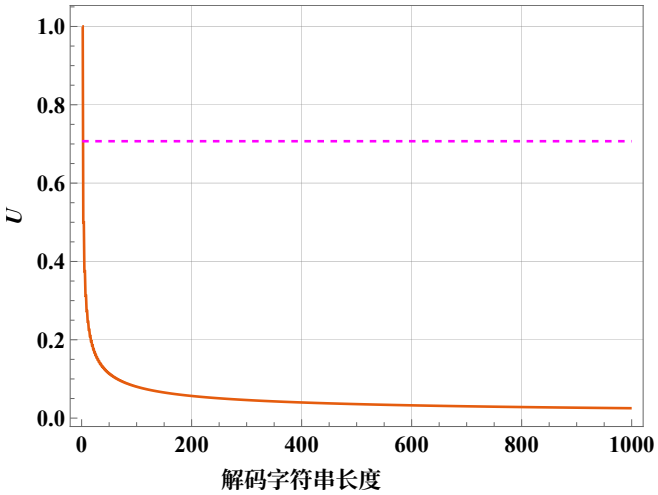

图5：未授权用户的 U 期望值随 N 的变化。品红色虚线表示不等式违背的阈值。

附录B：未授权用户的最优 U

在没有辅助信息的情况下，未授权用户只能猜测一个 $\boldsymbol{T}_{\mathrm{D}}$。为简单起见，我们假设 $\boldsymbol{T}_{\mathrm{D}}$完全由“0”组成。例如，如果 $\boldsymbol{T}_{\mathrm{D}}$ 和 $\boldsymbol{T}_{\mathrm{U}}$ 只有一位不同（不同位的具体位置并不重要），那么 $U = (N-2)/N$，因为存在两个相反的比特，它们会彼此抵消。通常我们可以推导出

$$U = \frac{1}{2^{N-1}N}\sum_{i=0}^{\lfloor N/2\rfloor}\binom{i}{N}(N-2i), \tag{B1}$$

未授权用户的期望值。注意，“$\boldsymbol{T}_{\mathrm{D}}$ 和 $\boldsymbol{T}_{\mathrm{U}}$ 相差 n 比特”的概率为$\frac{1}{2^N}\binom{n}{N}$，并且我们这里只考虑正的 U。在图 5 中，我们给出了 U 随 N变化的关系，可以发现$U = 1$ 因此只有在$1/\sqrt{2}$ 高于阈值 $N = 0$时，1. 对于足够长的调制字符串，未授权用户不可能重现 $\boldsymbol{T}_{\mathrm{D}}$ 并证明贝尔型不等式违背。

附录C：调制信号的生成与关联测试

由于 CES协议需要三种元素状态，我们采用直接相位调制技术 [40]，以精确地为时间箱纠缠态引入所需的相移或相位随机化。一对增益开关分布式反馈（DFB）激光器（Gooch & Housego，典型线宽为 1 MHz；脉冲持续时间为 80 ps）由 2.5-GHz 信号调制，并采用光注入锁定配置。该装置的一大优势是，只需切换主激光器的驱动信号，使其跨越激射阈值，即可轻松实现相位随机化。具体而言，如正文图3的插图所示，状态 $|\phi^+\rangle$ 对应于向主激光器施加常规驱动电压（信号“0”）；状态 $|\phi^-\rangle$ 对应于施加较低的驱动电压（信号“1”），而状态 $\hat{R}$ 对应于施加反向电压（信号“2”）。中心波长为 1550.52 nm 的主激光器，其光功率约为 80 μW，并随调制信号而变化。向从激光器施加 2.5-GHz 方波信号以制备脉冲。掺铒光纤放大器的输出功率为 10 mW。

在探测部分，两个不等臂马赫-曾德尔干涉仪分别设置在两位终端用户处，可通过改变温度来控制相位，从而设定所需的测量基。该干涉仪为自制器件，由两个保偏 50:50光纤耦合器和一组温度控制模块组成，并封装在盒内，以避免受到环境温度波动的影响。干涉仪的时间延迟为 400 ps，与泵浦脉冲重复频率相匹配。干涉仪的相位基于温度进行主动稳定，并使用一束波长为 1550.52 nm 的连续波参考光束（图中未示出）提供反馈控制，

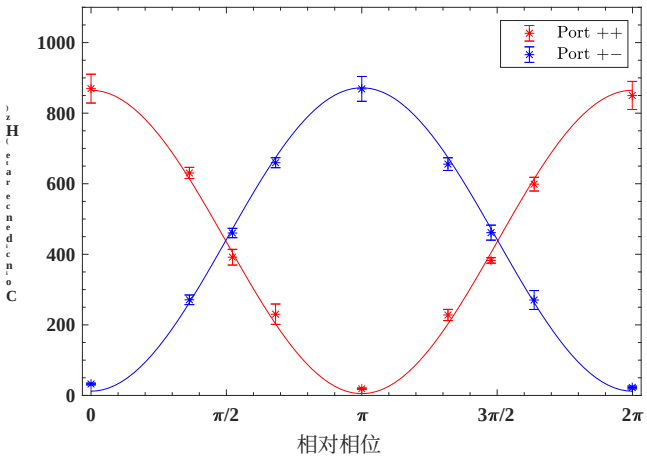

图6：不等臂马赫-曾德尔干涉仪相对于$|\phi^+\rangle$的干涉条纹。

（图）以 1550.52 nm 为中心的光谱用于提供反馈控制。

为模拟未授权用户或恶意设备以某种方式部分获取调制信息的情况，我们有意设置了几种非平凡的调制配置，并实施 CHSH 测试。也就是说，我们预先准备了若干非均匀分布的随机字符串，使调制中存在“偏差”，这种偏差可视为遭到入侵的结果。在后处理中，我们不对结果字符串实施任何操作，这等价于设置一个纯 $\boldsymbol{T}_{\mathrm{U}}$（全为“0”或全为“1”），因此 U 完全取决于 $\boldsymbol{T}_{\mathrm{D}}$

在我们的实验中。通过上述设置，我们实质上刻画了在给定 B 和 p的指定值时， S_{mod} 如何变化。需要注意的是，在实际实施中，我们首先获得 U的值，然后计算B。调制字符串的生成通过台式计算机上的随机数生成器完成。在这一原理验证演示中，我们没有使用分组密码算法生成大型连续随机字符串，而是采用由 5000 个随机经典三值符号组成的随机字符串，然后将字符串序列加载到任意波形发生器（AWG，Tektronix，70002B）上，并重复播放以生成调制信号。在用户端，使用时间标记器（ID Quantique，ID900）同时记录四对输出的光子符合事件，时间 bin 宽度为 100 ps。对于每一对输出，光子有三种可能的到达时间，从而在到达时间直方图中产生三个等间距的符合峰。中央峰中的符合事件会在相位基下产生探测结果，据此我们通过改变测量基计算相关性 E，进而得到调制后的 CHSH 参数 S_{mod}

附录D：干涉仪的表征

在图6 中，我们展示了其中一个不等臂马赫-曾德尔干涉仪输出端“++”和“+−的双光子干涉条纹实验结果，此时光源固定在状态$|\phi^+\rangle$。红点表示输出端“++”的符合计数率，蓝点表示输出端“+−”的符合计数率。实线为光子符合计数率的拟合正弦曲线。

[1] F. Xu、X. Ma、Q. Zhang、H.-K. Lo 和 J.-W. Pan，《采用现实器件的安全量子密钥分发》，《现代物理评论》92，025002（2020）。[2] C. H. Bennett 和 G. Brassard，《量子密码学：公钥分发与抛硬币》，《理论计算机科学》560，7（2014）。[3] A. K. Ekert，《基于贝尔定理的量子密码学》，物理评论快报 67，661（1991）。[4] H.-K. Lo、X. Ma 和 K. Chen，《诱骗态量子密钥分发》，物理评论快报 94，230504（2005）。[5] X.-B. Wang，《在实用量子密码学中击败光子数分裂攻击》，物理评论快报 94，230503（2005）。[6] 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）。[7] M. Lucamarini、Z. L. Yuan、J. F. Dynes 和 A. J. Shields，《在无需量子中继器的情况下突破量子密钥分发的速率-距离极限》，《自然》557，400（2018）。[8] R. Renner、N. Gisin 和 B. Kraus，《量子密钥分发协议的信息论安全性证明》，物理评论A辑 72，012332（2005）。

[9] 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）。[10] G.-J. Fan-Yuan、F.-Y. Lu、S. Wang、Z.-Q. Yin、D.-Y. He、W. Chen、Z. Zhou、Z.-H. Wang、J. Teng、G.-C. Guo 和 Z.-F. Han，无需可信节点的稳健且灵活的量子密钥分发网络，Optica **9**，812（2022年）。[11] S. Wang、Z.-Q. Yin、D.-Y. He、W. Chen、R.-Q. Wang、P. Ye、Y. Zhou、G.-J. Fan-Yuan、F.-X. Wang、W. Chen、Y.-G. Zhu、P. V. Morozov、A. V. Divochiy、Z. Zhou、G.-C. Guo 和 Z.-F. Han，通过830公里光纤实现双场量子密钥分发，Nat. Photon. **16**，154（2022年）。[12] L. Zhou、J. Lin、Y. Jing 和 Z. Yuan，无需光学频率传递的双场量子密钥分发，Nat. Commun. **14**，928（2023年）。[13] E. Fitzke、L. Bialowons、T. Dolejsky、M. Tippmann、O. Nikiforov、T. Walther、F. Wissel 和 M. Gunkel，通过基于纠缠的时间箱编码实现同时成对量子密钥分发的可扩展网络，PRX Quantum **3**，020341（2022年）。[14] J.-H. Kim、J.-W. Chae、Y.-C. Jeong 和 Y.-H. Kim，利用时间箱纠缠实现量子通信

基于波长复用光纤网络，APL Photonics 7, 016106（2022年）。[15] S. P. Neumann、A. Buchner、L. Bulla、M. Bohmann 和 R. Ursin，通过跨国248 km光纤链路实现连续纠缠分发，《自然·通讯》13, 6134（2022年）。[16] S. K. Joshi、D. Aktas、S. Wengerowsky、M. Lonˇcari´c、S. P. Neumann、B. Liu、T. Scheidl、G. C. Lorenzo、ˇZ. Samec、L. Kling、A. Qiu、M. Razavi、M. Stipˇcevi´c、J. G. Rarity 和 R. Ursin，一个无需可信节点的八用户城域量子通信网络，《科学进展》6, eaba0959（2020年）。[17] S. Wengerowsky、S. K. Joshi、F. Steinlechner、H. H¨ubel 和 R. Ursin，一个基于纠缠的波长复用量子通信网络，《自然》564, 225（2018年）。[18] W. Zhang、T. van Leent、K. Redeker、R. Garthoff、R. Schwonnek、F. Fertig、S. Eppelt、W. Rosenfeld、V. Scarani、C. C.-W. Lim 和 H. Weinfurter，一个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年）。[19] D. Mayers 和 A. Yao，采用不完美设备的量子密码学，载于 *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*（IEEE计算机学会，美国加利福尼亚州帕洛阿尔托，1998年），第503–509页。[20] J. Barrett、L. Hardy 和 A. Kent，无信号传输与量子密钥分发，《物理评论快报》95, 010503（2005年）。[21] N. Brunner、D. Cavalcanti、S. Pironio、V. Scarani 和 S. Wehner，贝尔非局域性，《现代物理评论》86, 419（2014年）。[22] A. Ac´ın、N. Gisin 和 L. Masanes，从贝尔定理到安全的量子密钥分发，《物理评论快报》97, 120405（2006年）。[23] A. Ac´ın、N. Brunner、N. Gisin、S. Massar、S. Pironio 和 V. Scarani，抵御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）。[24] N. Gisin 和 B. Gisin，一种利用探测漏洞的量子关联局域隐变量模型，《物理快报A辑》260, 323（1999年）。[25] M. Ho、P. Sekatski、E. Y.-Z. Tan、R. Renner、J.-D. Bancal 和 N. Sangouard，噪声预处理有助于实现光子设备无关量子密钥分发，《物理评论快报》124, 230502（2020年）。[26] J. Barrett、R. Colbeck 和 A. Kent，针对设备无关量子密码学的记忆攻击，《物理评论快报》110, 010503（2013年）。[27] W.-Z. Liu、Y.-Z. Zhang、Y.-Z. Zhen、M.-H. Li、Y. Liu、J. Fan、F. Xu、Q. Zhang 和 J.-W. Pan，迈向设备无关量子密钥分发的光子实验演示，《物理评论快报》129, 050502（2022年）。[28] 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）。[29] M. Curty 和 H.-K. Lo，防范量子密钥分发中的隐蔽信道和恶意经典后处理单元，《npj量子信息》5, 1（2019年）。[30] M. Zukowski、A. Zeilinger、M. Horne 和 H. Weinfurter，对GHZ态的探索，《波兰物理学报A辑》93, 187（1998年）。[31] R. Cleve、D. Gottesman 和 H.-K. Lo，《如何共享量子秘密》，物理评论快报 83，648（1999年）。[32] M. Hillery、V. Bu˘zek 和 A. Berthiaume，《量子秘密共享》，物理评论A辑 59，1829（1999年）。[33] Y.-A. Chen、A.-N. Zhang、Z. Zhao、X.-Q. Zhou、C.-Y. Lu、C.-Z. Peng、T. Yang 和 J.-W. Pan，《实验性量子秘密共享与第三方量子密码学》，物理评论快报 95，200502（2005年）。[34] W. Tittel、H. Zbinden 和 N. Gisin，《量子秘密共享的实验演示》，物理评论A辑 63，042301（2001年）。[35] B. P. Williams、J. M. Lukens、N. A. Peters、B. Qi 和 W. P. Grice，《利用偏振纠缠光子对实现量子秘密共享》，物理评论A辑 99，062311（2019年）。[36] J. F. Clauser、M. A. Horne、A. Shimony 和 R. A. Holt，《检验局域隐变量理论的实验方案》，物理评论快报 23，880（1969年）。[37] B. Hensen、H. Bernien、A. E. Dr´eau、A. Reiserer、N. Kalb、M. S. Blok、J. Ruitenberg、R. F. L. Vermeulen、R. N. Schouten、C. Abell´an、W. Amaya、V. Pruneri、M. W. Mitchell、M. Markham、D. J. Twitchen、D. Elkouss、S. Wehner、T. H. Taminiau 和 R. Hanson，《利用相隔1.3公里的电子自旋进行无漏洞贝尔不等式违背》，《自然》526，682（2015年）；M. Giustina、M. A. M. Versteegh、S. Wengerowsky、J. Handsteiner、A. Hochrainer、K. Phelan、F. Steinlech-ner、J. Kofler、J.-˚A. Larsson、C. Abell´an、W. Amaya、V. Pruneri、M. W. Mitchell、J. Beyer、T. Gerrits、A. E. Lita、L. K. Shalm、S. W. Nam、T. Scheidl、R. Ursin、B. Wittmann 和 A. Zeilinger，《利用纠缠光子对贝尔定理进行显著无漏洞检验》，物理评论快报 115，250401（2015年）；L. K. Shalm、E. Meyer-Scott、B. G. Christensen、P. Bierhorst、M. A. Wayne、M. J. Stevens、T. Gerrits、S. Glancy、D. R. Hamel、M. S. All-man、K. J. Coakley、S. D. Dyer、C. Hodge、A. E. Lita、V. B. Verma、C. Lambrocco、E. Tortorici、A. L. Migdall、Y. Zhang、D. R. Kumor、W. H. Farr、F. Marsili、M. D. Shaw、J. A. Stern、C. Abell´an、W. Amaya、V. Pruneri、T. Jennewein、M. W. Mitchell、P. G. Kwiat、J. C. Bi-enfang、R. P. Mirin、E. Knill 和 S. W. Nam，《对局域实在论进行有力的无漏洞检验》，物理评论快报 115，250402（2015年）。[38] J. Daemen 和 V. Rijmen，*The design of Rijndael: AES — the Advanced Encryption Standard*（施普林格出版社，2002年）第238页；《高级加密标准规范（AES）》，《联邦信息处理标准出版物》197（2001年）。[39] N. Walenta、A. Burg、D. Caselunghe、J. Constantin、N. Gisin、O. Guinnard、R. Houlmann、P. Junod、B. Ko-rzh、N. Kulesza、M. Legr´e、C. W. Lim、T. Lunghi、L. Monat、C. Portmann、M. Soucarros、R. T. Thew、P. Trinkler、G. Trolliet、F. Vannel 和 H. Zbinden，《一种具备硬件密钥蒸馏和波长复用功能的快速灵活量子密钥分发系统》，《新物理学杂志》16，013047（2014年）。[40] Z. L. Yuan、B. Fr¨ohlich、M. Lucamarini、G. L. Roberts、J. F. Dynes 和 A. J. Shields，《直接相位调制光源》，物理评论X辑 6，031044（2016年）。[41] D. Llewellyn、Y. Ding、I. I. Faruque、S. Paesani、D. Bacco、R. Santagati、Y.-J. Qian、Y. Li、Y.-F. Xiao、M. Huber、M. Malik、G. F. Sinclair、X. Zhou、K. Rot-twitt、J. L. O'Brien、J. G. Rarity、Q. Gong、L. K. Ox-enlowe、J. Wang 和 M. G. Thompson，《芯片间量子隐形传态与多光子纠缠》

在硅中，《自然·物理》**16**，148（2020）。[42] X. Chen、Z. Fu、Q. Gong 和 J. Wang，《光子芯片上的量子纠缠：综述》，《先进光子学》**3**，064002（2021）。

[43] S. Pironio, A. Ac´ın、N. Brunner、N. Gisin、S. Massar 和 V. Scarani，能够抵御集体攻击的设备无关量子密钥分发，《新物理学杂志》**11**，045021（2009年）。