利用囚禁离子和单光子实现可验证盲量子计算

P. Drmota,[1] D. P. Nadlinger,[1] D. Main,[1] B. C. Nichol,[1] E. M. Ainley,[1] D. Leichtle,[2] A. Mantri,[3] E. Kashefi,[4,2] R. Srinivas,[1] G. Araneda,[1] C. J. Ballance,[1] 和 D. M. Lucas[1]

[1] *Department of Physics, University of Oxford, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, U.K.* [2] *Laboratoire d'Informatique de Paris 6, CNRS, Sorbonne Université, Paris 75005, France* [3] *Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, U.S.* [4] *School of Informatics, University of Edinburgh, Edinburgh EH8 9AB, United Kingdom.*（日期：2024年4月8日）

我们报告了首个可验证盲量子计算的混合物质-光子实现。我们采用囚禁离子量子服务器，并通过光纤量子链路将其与客户端光子探测系统连接。存储量子比特和确定性纠缠门的可用性，使得无需后选择即可实现交互式协议——这是任何可扩展盲服务器的关键要求，而以往的实现都无法满足。我们量化了隐私性，每个量子比特泄露的经典比特数为 $\lesssim 0.03$ 。这项实验展示了实现完全验证的云端量子计算的路径。

arXiv:2305.02936v3 [quant-ph] 5 Apr 2024

量子计算机有望超越世界上最强大的超级计算机，其应用涵盖药物发现到网络安全等领域。这些计算机利用纠缠和叠加等量子现象执行计算，而这些计算被认为是经典计算机难以处理的。由于量子处理器需要操控脆弱的量子态，它们必然结构复杂，而且高性能系统的物理访问受到限制。云端方案允许用户远程访问量子服务器，可能会成为近期及未来的工作模式；许多用户已经在商用设备上开展计算，以进行前沿研究 [1–5]。

然而，将量子计算委托给服务器会带来与经典云计算相同的隐私和安全性问题。当前，在经典模拟变得不可处理的情况下，用户既无法向服务器隐藏自己的工作，也无法独立验证结果。值得注意的是，使量子计算成为可能的相同现象，可以让服务器以一种"盲"的方式运行，从而隐藏客户端的输入、输出和算法 [6–8]；由于量子信息无法被复制，且测量会不可逆地改变量子态，存储在这些系统中的信息可以通过信息论安全性得到保护，并且服务器的错误操作或蓄意攻击都能够被检测出来——这是一个令人惊讶的可能性，在经典计算中没有对应方案。盲量子计算（盲量子计算）不仅要求服务器具备通用量子计算机，还需要一条将其与客户端连接起来的量子链路 [9, 10]。光子是提供这条链路的自然选择，事实上，最早的盲量子计算 演示就是在纯光子系统中完成的 [11–14]。然而，不可避免的光子损失，无论是由于有限的光子探测效率还是链路中的吸收，都会带来潜在的安全风险 [11, 13] ，并且由于后选择所造成的资源开销，这种方法的可扩展性也受到严格限制 [15]。理想情况下，服务器上的量子信息应当被存储在稳定的量子存储器中，该存储器可进行高保真操作，同时还能轻松接入光子链路。随后，服务器保留量子信息的能力使客户端能够进行自适应电路中途调整，从而确定性且安全地执行目标计算。在单量子层面结合两种截然不同的平台，技术上颇具挑战性 [16, 17]；迄今为止，集成存储量子比特的量子网络节点已通过固态系统 [18, 19] 和囚禁原子 [20, 21] 实现。

在此，我们展示了使用囚禁离子量子处理器（服务器）实现的盲量子计算，该处理器将编码于 $^{43}Ca^{+}$ 中的高鲁棒性存储量子比特与基于 $^{88}Sr^{+}$ 的单光子接口相结合，从而与客户端（光子探测系统）建立量子链路。我们实现了一种交互式协议，客户端可以利用实时经典前馈控制，根据每次实验结果自适应地在服务器上远程制备单量子比特态。通用量子计算所需的复杂性完全包含在服务器内，而客户端只是一个与算法的规模和复杂性无关的简单光子偏振测量设备，并且从设计上支持近乎完美的盲性。客户端和服务器由相互独立的硬件控制，彼此之间仅通过经典信号总线和光纤连接。我们的系统实现了低于某一阈值的噪声水平；对于该阈值，从理论上可以任意提升协议安全性和成功率（鲁棒性） [22]。

协议。 量子算法可以用基于测量的量子计算模型来描述，该模型规定了在高度纠缠的资源态上执行一系列测量 [23, 24]。即使面对恶意运行的服务器，只要态制备或测量由客户端执行，就可以实现信息论盲性 [6, 25–27]。

存在噪声时，即使服务器忠实运行，也会产生无法区分的错误结果。

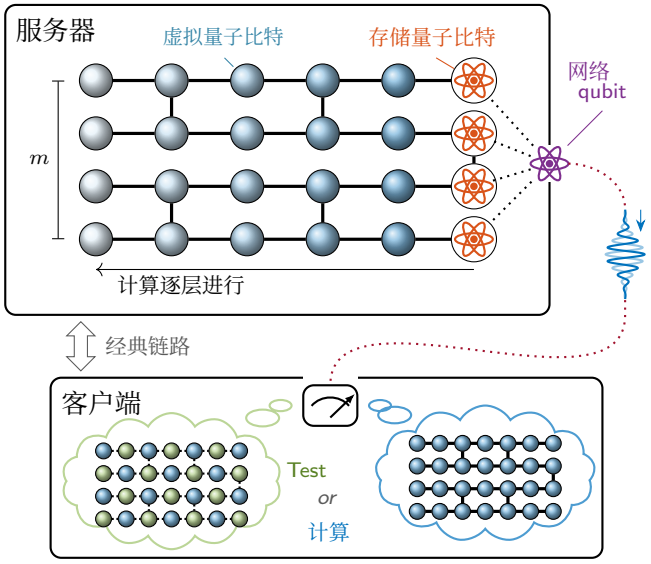

图 1. 基于测量的模型中的可验证盲量子计算。计算表示为在砖墙态上执行的一系列测量（由顶点代表虚拟量子比特、由边表示 CZ 门的二维图）。服务器持有 m 个物理存储量子比特（橙色原子）和一个物理网络量子比特（紫色原子）。服务器可以确定性地使这些量子比特彼此纠缠。网络量子比特也可以与光子纠缠；通过测量该光子，客户端可以在服务器端远程操控网络量子比特，而不让服务器获知其状态。这使客户端能够向服务器隐藏计算（输入、输出和电路）。此外，客户端可以通过（随机）穿插测试轮次来验证计算未遭篡改；测试轮次会产生可经典模拟的结果，且服务器无法将其与实际计算区分开来。

能够抵御对诚实协议 [7, 8, 28, 29]的恶意篡改。盲性允许客户端秘密测试服务器提供的量子资源。本文实现的协议通过交错进行“计算”轮次和“测试”轮次来实现这一点。对于一类重要的有界误差量子多项式时间（BQP）判定问题，统计论证给出了该协议安全性和鲁棒性的界限 [22]。如果观测到的测试轮次失败比例 p_{fail}低于选定的阈值 ω，客户端就会接受结果。如果ω 低于理论阈值 $\omega_{\max}$，重复带来的开销就很低：接受错误结果的概率会随着轮数增加而呈指数级下降。 ω 的最小值取决于设备中的噪声量。客户端假设测试轮次失败率的最大期望值为 $p_{\max}$，并选择$\omega > p_{\max}$，使拒绝任何结果的概率也随着轮数增加而呈指数级下降，从而使协议能够抵御有限程度的噪声。

对于通用量子计算，特定图送彩金

状态以及一组离散的单量子比特测量，即 $\hat{}\{B_\alpha = \cos(\alpha)\mathrm{X} + \sin(\alpha)\mathrm{Y}\}_{\alpha\in\Theta}$，就足够了 [30], where $\Theta = \{0, \pi/4, \ldots, 7\pi/4\}$，且 X, Y 是泡利算符。图态是一种特殊的多量子比特状态，其中顶点表示初始化于 $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ 的量子比特，边表示通过双量子比特 CZ门创建的纠缠 [Fig. 1], where $\mathrm{CZ} = |0\rangle\langle 0| \otimes 1 + |1\rangle\langle 1| \otimes \mathrm{Z}$。$\hat{}$ 量子比特按固定顺序测量，在节点 ℓ 使用基 B_{α_ℓ}，其中 α_ℓ 取决于算法和先前的测量结果。

为使用测量角度 α_ℓ 盲目运行上述协议，客户端通过远程态制备（远程态制备）制备至 $|\theta_\ell\rangle = \exp(-\mathrm{i}\frac{\theta_\ell}{2}\mathrm{Z})|+\rangle$，并对每个量子比特 $\bar{}\ell = 1, 2, \ldots\ldots, q$施加秘密相位移$\theta_\ell \in \Theta$，同时相应地调整测量角度。这样，$\theta_\ell$ 便充当经典加密密钥，使得 α_ℓ 对客户端保密。为确保相应的测量结果 $m_\ell \in \{0, 1\}$不泄露信息，客户端在一半由秘密密钥比特 $r_\ell \in \{0, 1\}$ [Eq. (1)]指示的测量角度中隐藏比特翻转。客户端可以恢复未加密的测量结果，即 $m_\ell \oplus r_\ell$。

在此，我们在线性簇态上实现盲量子计算 [Fig. 2]。两个物理量子比特足以实现任意长度的线性簇，因为每次电路中途测量后都可以重新初始化量子比特。第一个量子比特——网络量子比特——可由客户端利用远程态制备 [31], 引导至任意状态；第二个量子比特——存储量子比特——则承载编码在线性簇态扩展过程中前导节点中的信息。我们将簇态分解为服务器与客户端之间离散的相互作用步骤，从初始化步骤开始 [Fig. 2], ，该步骤将存储量子比特制备为 $|\theta_1\rangle$。在每一计算轮次的相互作用中，客户端执行远程态制备，将网络量子比特引导至 $|\theta_{\ell+1}\rangle$，并通信

$$\delta_\ell = (-1)^{R_{\ell-1}}\alpha_\ell + \theta_\ell + \pi r_\ell \qquad (1)$$

发送给服务器，其中 $R_\ell = \bigoplus_{1\le j<\ell/2}(m_{\ell-2j} \oplus r_{\ell-2j})$ 是根据解密后的先前测量结果进行的自适应前馈校正。应用 CZ门和 SWAP$\hat{}$ 门后，服务器在 B_{δ_ℓ}基下测量网络量子比特，并将结果 m_ℓ 返回给客户端 [，如图 2] 所示的交互模块中。此过程使首个簇态节点留在存储量子比特上，并由 R_ℓ [32] 加密，同时网络量子比特可用于进一步的远程态制备。

客户端随机为每一轮分配一个秘密标签，将其标记为计算轮次或测试轮次。在测试轮次中，客户端将每隔一个量子比特制备为 Z本征态 $|r_\ell\rangle$，这些量子比特称为“虚拟量子比特”。这一步使其余所谓的“陷阱量子比特”处于可分离态。因此，客户端可以高效地预测使用 $\delta_\ell = \theta_\ell + \pi r_\ell$ 测量这些陷阱量子比特的结果 $m_\ell \,!= r_\ell$。

服务器。服务器控制一台离子阱量子处理器，其中包含一枚 $^{88}\mathrm{Sr}^+$ 离子和一枚 $^{43}\mathrm{Ca}^+$ 离子。离子——

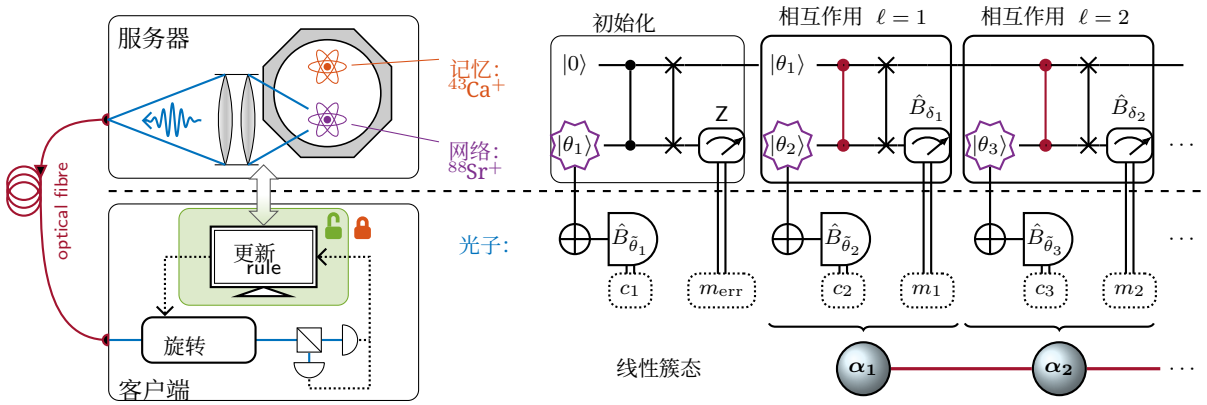

图2. 使用囚禁离子量子服务器和光子客户端生成线性簇态的协议。客户端通过测量光子的偏振，使用基ˆ $B_{\tilde{\theta}_\ell}$ 并以$c_\ell \in \{0,1\}$ 作为测量结果，可将网络量子比特操控至 $|\theta_\ell\rangle = |\tilde{\theta}_\ell + c_\ell\pi\rangle$。在初始化步骤中，服务器将该状态转移至存储量子比特，使网络量子比特能够再次被操控 [21]。之后的每个交互步骤都会扩展簇态的大小；客户端远程将网络量子比特操控至 $|\theta_{\ell+1}\rangle$，服务器将其纠缠（CZ门），并在基 B_{δ_ℓ}下进行测量，其中 δ_ℓ 由客户端提供。详情请参阅正文。

用于远程态制备 的光子纠缠通过快速激发和自发衰变产生，[37] 发生在 $^{88}Sr^+$的422纳米跃迁上。单光子由自由空间光学元件收集，并耦合到单模光纤 [38], 中，该光纤与客户端构成量子链路。存储量子比特编码在 $^{43}Ca^+$中，它具有较长的相干时间（$\sim 10\,s$），且不受对 $^{88}Sr^+$ [21]进行并行操控的影响。因此， $^{88}Sr^+$ 可用于线路中途测量，并在交互步骤之间进行辅助冷却。构建簇态所需的CZ门与SWAP门结合为iSWAP门。这样便可重复使用 $^{88}Sr^+$ 进行远程态制备，同时将当前计算状态保留在存储量子比特上。初始化步骤中的误差会被实时检测 [$m_{\text{err}} = 1$ 如图 2] 所示；若检测到误差，则重复该步骤。

客户端。 客户端通过光纤从服务器接收单光子。客户端的量子能力仅限于对这些光子进行投影偏振测量，测量所用的基可通过改变两个电光调制器（电光调制器）上的电压进行动态重构 [32] [图 3]。该测量会远程将网络量子比特制备到某个状态，该状态仅取决于偏振测量基和测量结果，这些信息˜仅客户端知晓 [θ_ℓ 且 c_ℓ 如图 2]所示。光纤中的双折射会在光子到达客户端之前改变其状态，这种变化由一个未知的酉操作造成，并会因热效应而以 ~ 10 分钟的时间尺度漂移。为补偿这种漂移，客户端会定期重新校准电光调制器 的电压 [32] [图 3(c)]。

盲性。 我们考虑可能通过由恶意服务器控制的网络量子比特，以及通过经典信号，泄露给恶意服务器的有关客户端偏振测量的信息，而这些经典信号】【。

由客户端控制。我们利用量子态层析，量化了服务器通过测量网络量子比特所能获取的信息量，为每个交互步骤 0.031(4) 比特，与独立估算结果 [32]吻合良好。在我们的演示中，不同偏振测量结果之间不匹配的电子延迟是导致信息泄漏的主要原因。然而，由于客户端控制着相关的经典信号，因此可以使这些延迟保持一致。剩余的每个交互步骤 ~ 0.001 比特的信息泄漏将主要由客户端所使用的偏振光学器件的不完善所导致。

结果。 我们实现了具有一个和两个交互步骤的不同量子计算，分别见图 4(a) 和图 4(b)。我们可以在后续交互步骤中使用输出量子比特，或者在基 $B_{\delta_{q+1}}$ 中进行最终测量 ˆ，以完成 $(q+1)$ 节点簇态计算。不过，在本演示中，输出量子比特始终在 Z基中测量。由于该测量与其前面的 CZ门对易，因此此计算等价于节点数少一个的簇态。因此，一个和两个步骤的交互分别实现计算 $HZ(\alpha_1)|+\rangle$ 和$X(\alpha_2)Z(\alpha_1)|+\rangle$，其中 H 是哈达玛门， $X(\alpha) = \exp(-i\frac{\alpha}{2}X)$ 和 $Z(\alpha) = \exp(-i\frac{\alpha}{2}Z)$ 是单量子比特旋转，而 α_1 和 α_2 在协议期间使用公式 (1) 加密。从服务器的角度来看，由于比特翻转加密，结果呈现为随机的 [方块（图 4(a)）]；客户端在计算轮次和测试轮次中都会应用该加密 $\delta_\ell \propto r_\ell\pi$。另一方面，客户端可以利用轮次类型（计算或测试）和加密密钥（r_ℓ）对结果进行解码。解码后的计算结果以图 4(a) 中的圆圈和图 4(b) 中的色彩图表示，与预期的条纹图样相符，具体取决于功能（func-】【。

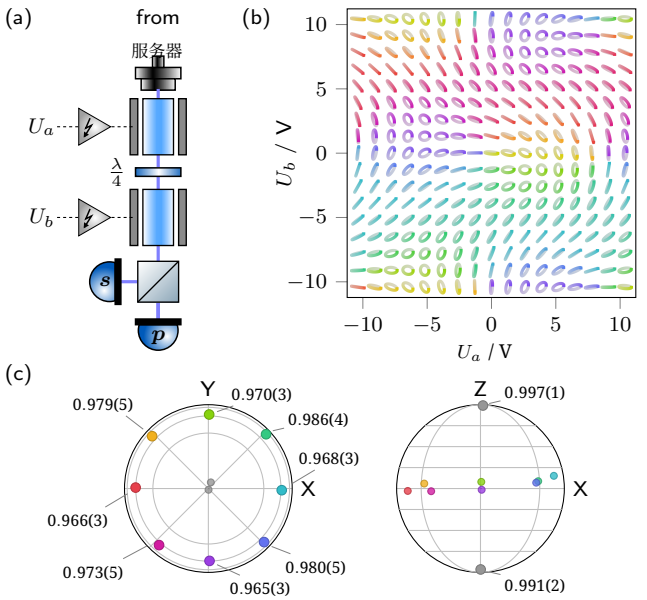

图 3. 客户端使用快速切换偏振分析器执行远程态制备（RSP）。（a）两个由 $\lambda/4$波片隔开的电光调制器 的控制电压（U_a, U_b）使客户端能够任意旋转由偏振分束器定义的测量基。（b）使用激光为不同的 U_a, U_b重建此基。图中显示了由探测器 p标记的基态对应的偏振椭圆，颜色表示其相位。（c）为找出能使各目标态保真度 F 最大化的 U_a, U_b （这些目标态在协议中需要用到），我们在远程态制备（RSP）后对网络量子比特进行层析。图中以网络量子比特的布洛赫球表示展示了两周内 36 次校准的平均结果。数值表示 F，标准差通过自助法获得。

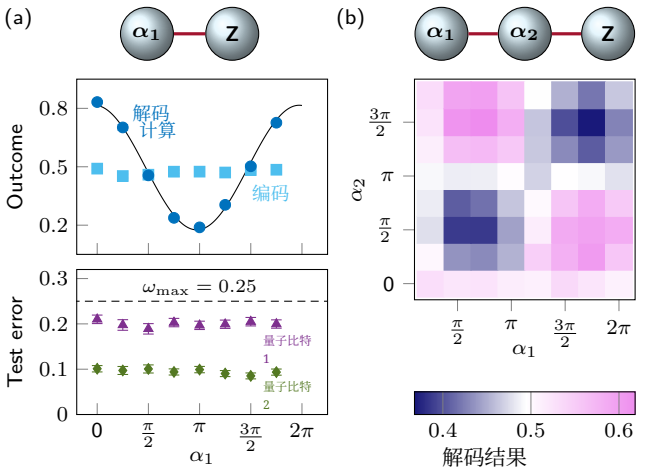

图4. 扩展线性簇态的实验结果，其中在客户端与服务器之间进行（a）一个和（b）两个交互步骤后，在Z基中测量首个量子比特。（a）尽管服务器观测到的是混合结果（方块），每个 ∼2000 测试轮次和计算轮次各占一半，但对于每个α_1，客户端都可以使用密钥解码结果。图中还显示了解码后的计算结果（圆圈）的拟合曲线，以便直观观察。误差区间表示二项式标准误差。测试轮次的误差显著低于验证双节点簇态的阈值（虚线）。（b）针对不同的盲测量设置（α_1, α_2），显示了解码结果；每种设置均包含 ∼3100 个计算轮次（交错的测试轮次结果见补充材料 [32] ）。

盲测量角 α_1 和 α_2。实验瑕疵会导致对比度降低和相移。客户端在第一个量子比特上观测到错误率$p^{(1)}_{\text{fail}} = 0.201(3)$，在第二个量子比特上观测到错误率 $p^{(2)}_{\text{fail}} = 0.095(2)$ [见图 4(a) 下图]，，这些结果与已知误差源一致 [32]。通过将最终测量基从 Z 改为 $B_{\delta_{q+1}}$ 并额外施加一个 $\pi/2$脉冲（这对误差预算不会产生显著影响），同时在每个测试轮次中随机选择一个量子比特作为陷阱量子比特，我们发现可以用我们的实验装置验证双节点簇态计算 [32]；其测试轮次平均失败概率的预期值为 ~ 0.18，显著低于$\omega_{\max} = 0.25$ 对该状态进行安全、稳健验证所要求的值。三节点簇态计算对应的测试轮次结果见补充材料 [32]；观测到的失败率表明，在这种情况下无法进行验证，主要原因是 iSWAP 门 [21]的保真度 ≈ 0.91受到技术限制（运动加热）的影响。

结论。 我们已实现一种协议，可将量子计算盲态委托给一个离子阱中的陷阱-离子量子处理器，采用的客户端装置只需进行单光子偏振测量和经典通信。我们已对实现中存在的经典信道和量子信道上的信息泄漏设定了界限。我们已证明，可以在不增加服务器中物理量子比特数量、也不改动客户端硬件的情况下增大簇态的规模。如果在服务器中增加更多存储量子比特 [39, 40], ，计算空间就可以扩展到更高维的簇态。我们已采取措施将验证纳入协议；测得的测试轮次误差表明，对双节点簇态进行的计算能够得到稳健可靠的验证。我们预测，对于固有算法误差较小且 $p_{\max} = 0.185$ 的BQP 判定问题，经过 24 000 次重复（包括 14 400 个测试轮次）后，接受错误结果和拒绝任何结果的概率都将为 10^{-5} ；每增加 1200 次重复，这一概率就会减半 [32]。只要误差低于依赖于规模的阈值，该方法有望为更大的簇态和其他算法提供安全性与稳健性，$\omega_{\max} \approx 1-(3/4)^{2/q}$，其中 q 是簇态中的量子比特总数。我们实现的协议未包含纠错；为了验证

更大的簇态，需要降低每个交互步骤的误差。iSWAP门的非保真度是主要误差来源 [21], ，但值得注意的是，在其他系统中， $^{88}Sr^{+}$ 与 $^{43}Ca^{+}$ 之间保真度为 0.998 的CZ门已得到演示 [41]。目前最先进的离子-光子纠缠保真度为 0.979(1)（本实验装置），其限制因素主要是光学装置中的技术缺陷（对准误差）。

与此前基于纯光子平台且不使用量子存储器的实验实现相比 [11–14], ，本研究克服了实际部署盲量子计算所面临的若干重大挑战。由于服务器中的量子逻辑操作是确定性的，且与客户端的相互作用可通过预告信号确认，我们的实现无需后选择，从而避免了相关的效率、可扩展性和安全问题 [11, 12, 14]。特别是，光子损失不会构成安全威胁；结合使用存储量子比特与快速自适应硬件，还能实时对所有协议参数进行真正的逐次随机化。

未来的实现方案可能涉及由服务器和客户端组成的复杂网络。可以利用光开关将光子路由至多个客户端，并通过将光子转换为电信波长 [42] 或采用光纤技术的最新进展 [43]来增加与服务器之间的距离。

此处展示的光子接口囚禁离子量子信息平台，为客户端以最少的量子资源，将机密量子计算安全地委托给功能完备但不可信的量子服务器铺平了道路。

我们感谢桑迪亚国家实验室提供本实验所用的HOA2 离子阱，并感谢实验控制系统 AR-TIQ [44] 的开发者。DPN 感谢牛津默顿学院的支持。DL 感谢 ANR 项目 SecNISQ 的支持。AM 和 DM 感谢美国陆军研究办公室的支持（参考编号：W911NF-20-1-0015 和 W911NF-18-1-0340）。GA 为 Nu Quantum Ltd 提供咨询服务，并感谢牛津沃尔夫森学院的支持。RS 部分受雇于 Oxford Ionics Ltd，并感谢 EPSRC Fellowship EP/W028026/1 和牛津贝利奥尔学院提供的资助。CJB 是 Oxford Ionics 的董事，并感谢 UKRI FL Fellowship 的支持。EK 感谢资助项目（参考编号：EP/X026167/1）的支持。我们感谢 VeriQloud（EK 是其联合创始人）在本项目初期设计阶段提供的技术和资金支持，该支持通过 NQIT 量子技术中心的产业合作伙伴资助项目 EP/M013243/1 提供。本研究得到了英国 EPSRC“量子计算与模拟”中心 EP/T001062/1 以及欧盟量子技术旗舰项目 AQTION（编号：820495）的支持。

《囚禁离子与单光子实现的可验证盲量子计算》的补充材料

数据处理

我们尽最大努力在能够代表真实部署的条件下开展实验。客户端和服务器分别由独立的个人计算机以及 ARTIQ 开源控制系统的硬件 [44] 控制。实验和校准的时间安排通过以太网进行协调。对于时间要求严格的通信，例如协议执行期间的交互，则采用低延迟电子信号。在整个数据采集和分析过程中，客户端不会向服务器透露任何协议秘密。

线性簇态

在计算轮次中，经过q 次相互作用后，存储量子比特的状态为

$$|\psi_{q+1}\rangle = \hat{Z}(\theta_{q+1})\mathsf{X}^{R_q}\mathsf{Z}^{R_{q-1}}\left(\mathsf{H}\hat{Z}(\alpha_q)\cdots\mathsf{H}\hat{Z}(\alpha_1)\right)|+\rangle\,,$$
$$\hat{Z}(\alpha) := \exp\left(-\mathrm{i}\frac{\alpha}{2}\mathsf{Z}\right),$$

其中，X 和 Z 是泡利算符，H 是哈达玛门。

序列时序

处理簇态的一个节点所需的时间包括：客户端成功探测到单光子平均需要100 µs（受量子链路中的光子损失限制），在 ^{43}Ca中逻辑量子比特与存储量子比特之间传输需要 $\sim 400\,\mu$s，^{88}Sr^{+} 与 ^{43}Ca^{+}之间的iSWAP门需要 $\sim 340\,\mu$s，读出 ^{88}Sr^{+}需要 $\sim 135\mu$s，去搁置 ^{88}Sr^{+}需要50 µs，使用 ^{88}Sr^{+}进行协同基态冷却需要 $\sim 230\,\mu$s，以及将测量结果从服务器传送至客户端需要$\sim 150\,\mu$s。

每次光子生成尝试持续 1 µs，其中包括服务器端的快速 ^{88}Sr^{+} 态制备（~ 350 ns 激光切换延迟、 + 300 ns 脉冲持续时间、 + 50ns 延迟）、服务器端在 12.5ns 窗口内进行的脉冲激发、客户端的光子探测窗口（~ 30 ns），以及结果通信，即是否接收到光子（~ 64 ns）。客户端和服务器循环进行尝试，直到客户端探测到光子或达到超时（1 ms）。若发生超时（概率为 $< 10^{-4}$），则会执行一系列系统检查（离子损失、激光锁定状态），然后继续协议。

客户端装置

为满足快速操控光子偏振的时序要求，选用了电光调制器（Thor- labs，EO-AM-NR-C4），因其具有快速切换能力。为实现普适性，两个串联的电光调制器可提供必要的自由度，从而能够实现任意偏振测量

基。

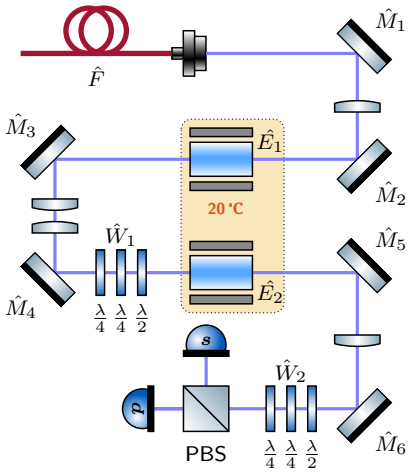

图 S5. 客户端所用快速光子偏振分析仪的详细光路。电光调制器采用热屏蔽，并主动稳定在 20 °C，稳定度为 0.1 mK。波片三联组 ˆ W_1 和 ˆ W_2 用于抵消由 $\{M_3, M_4\}$和 $\{$ ˆE_2，ˆM_5，ˆ $M_6\}$组成部分中的非预期双折射。组件 $\{F, M_1, M_2, E_1\}$ 中的双折射则通过设备校准予以补偿。

预备知识

Temperature stability of EOMs

尽管电光调制器采用双晶体配置制造，可被动抵消普通轴与非普通轴之间的温度依赖性差异，但在初步研究中仍观察到显著的温度依赖性偏振漂移 [33]。因此，客户端装置的最终光学布局采用电光调制器 [的共享温度稳定设计，见图 S5]。带有额外隔热层的双层外壳包围着电光调制器模块。此外，还在安装座的顶面使用珀尔帖元件进行主动稳定，并配备散热器和风扇以引导排热。通过以下方法校准反馈增益：

采用齐格勒-尼科尔斯方法的一种变体 [34], 后，温度在 ~ 2 分钟内稳定下来，并在典型运行条件下达到低于 0.1 mK 的稳定度。

Optical impurities in EOMs

入射光经 300 mm 平凸透镜聚焦到第一个电光调制器中，随后准直并聚焦到第二个电光调制器中。使光聚焦通过晶体，可显著降低电光调制器晶体中空间不均匀性导致的退偏振效应。

Polarising beam splitter

偏振分束器（偏振分束器）的缺陷会降低正交偏振态的可区分性。我们测量了偏振分束器对于纯 s 和 p 偏振的消光比，并分别得到透射功率和反射功率中的 $T_s/T_p = 0.5\times10^{-4}$和 $R_p/R_s = 1.3\times10^{-4}$。我们注意到，这一缺陷不会影响该实现的盲性；它只会降低远程态制备的保真度。

Internal birefringence cancellation

理想电光调制器的作用是使偏振绕由酉变换表示的固定轴旋转

$$\hat{R}(U) = \exp\left[-\mathrm{i}\frac{\phi(U)}{2}\hat{X}\right] ,$$

其中，旋转角度 ϕ 是施加在晶体两端的电压 U 的函数，而 $X = |H\rangle\langle V| + |V\rangle\langle H|$则是在由电光调制器的非常轴定义的基中表示的。对于一对理想的电光调制器，若要能够将任意输入偏振转换为任意输出偏振，旋转轴必须彼此正交。原则上，可以在电光调制器之间放置一个四分之一波片来实现这一点；然而在实践中，包括电光调制器晶体和反射镜在内的每个光学元件都存在未知量的静态双折射。为了精确补偿这一点，必须利用光学元件构造逆酉操作。可以证明，至少需要一组三元波片（例如两个四分之一波片和一个半波片），才能实现作用于偏振量子比特 [35]的最一般酉操作。在图 S5 中，所有可能影响偏振的光学元件都标记有酉算符。算符 E_1 和 E_2 描述了两个电光调制器中未知的静态双折射。我们调节波片三元组 W_1 和 W_2，以近似抵消所有不需要的来源双折射，使得

$$\hat{P}_{\mathrm{BS}}\underbrace{\hat{W}_2\hat{M}_6\hat{M}_5\hat{E}_2}_{1}\hat{R}(U_b)\underbrace{\hat{W}_1\hat{M}_4\hat{M}_3}_{\hat{Q}_{\mathrm{WP}}}\hat{R}(U_a)\underbrace{\hat{E}_1\hat{M}_2\hat{M}_1\hat{F}\,|\psi\rangle}_{|\tilde{\psi}\rangle}$$
$$= \hat{P}_{\mathrm{BS}}\hat{R}(U_b)\hat{Q}_{\mathrm{WP}}\hat{R}(U_a)\,|\tilde{\psi}\rangle ,$$

其中，$\hat{P}_{\mathrm{BS}} = \hat{Z} = |H\rangle\langle H| - |V\rangle\langle V|$ 是由偏振分束器实现的投影算符，而 $Q_{\mathrm{WP}} = \exp(\mathrm{i}\frac{\pi}{4}Z)$是沿主轴对齐的理想四分之一波片的酉算符。我们不校正从输入状态 $\tilde{}$到 $|\psi\rangle$ 至 $|\psi\rangle$ 的变换，因为这只会使整个坐标系发生旋转。

Switching dynamics

改变晶体 [33]两端的电场后，观察到了显著的漂移行为。这可以归因于连接在晶体上的高压电极使晶体带电。因此，在每个脉冲之后，我们施加一个持续时间和幅度相同但符号相反的补偿脉冲，以使时间平均电场归零。对脉冲持续时间、稳定时间和占空比进行系统分析表明，加入补偿脉冲后，原本占主导地位的不利影响可以被完全消除。我们通过记录透射比例的强度随时间的变化来确定切换速度。强度在 18 µs 内稳定到最终值的 1%，并与驱动电压的稳定同步；因此，我们将其确定为限制速度的因素。

预表征

为了表征客户端装置对任意偏振输入的作用，我们在输入端的格兰-泰勒偏振片后使用电动波片。在此表征中，我们使用 ~ 1 mW、波长为 422 nm 的连续波激光。水平偏振输出功率的占比包含状态振幅的信息，但不包含相位信息。若要获知相位，必须结合线性无关输入状态的振幅信息。我们以随机顺序采集四分之一波片（测得的相位延迟为$2\pi \times 0.2584(4)$ rad）角度 $q \in \{-\pi/4, 0, \pi/4\}$ rad和半波片（测得的相位延迟为 $2\pi \times 0.5000(1)$ rad）角度 $h \in \{-\pi/8, 0, \pi/8, \pi/4\}$ rad 的所有组合对应的数据。对于每个电光调制器电压设定，我们使用模型对波片扫描数据进行非线性拟合

$$t = \left|\langle\psi|\,\hat{Q}_{\mathrm{WP}}(q)\hat{H}_{\mathrm{WP}}(h)\,|H\rangle\right|^2 \qquad (2)$$

对于透射比例 t，其中 $|\psi\rangle = \cos(\vartheta/2)\,|H\rangle + \sin(\vartheta/2)\exp(\mathrm{i}\varphi)\,|V\rangle$，扫描时改变波片角度 $(q,\ h)$，分别为

化，而在优化过程中调整 $(\vartheta,\ \varphi)$。该分析结果见正文图 3(b)。使用式 (2) 的密度矩阵表述，发现重构状态的纯度与所有使用的电光调制器 电压设置下的 $\mathrm{Tr}(\rho^2)\ = 1$ 一致。

Orthogonal measurements

为了实现完美的盲性，客户端装置实施的测量不得向服务器泄露信息。一种可能的泄露方式是依赖于秘密的噪声，例如取决于电光调制器 电压设置的缺陷。我们使用本节开头所述的相同测量设置，针对四分之一波片和半波片角度的完整列表记录数据（相邻偏振状态之间的重叠 $\approx 3\times10^{-4}$）。对于每一对扫描的电光调制器电压 (U_a, U_b)，我们选取由这些波片产生的两个输入偏振状态 $|\psi^+_{ab}\rangle$ 和 $|\psi^-_{ab}\rangle$，它们分别使偏振分束器透射和反射的功率达到最大。图 S6 中所示的重叠 $\left|\langle\psi^-_{ab}|\psi^+_{ab}\rangle\right|^2$ 平均为 0.0016 （中位数）。

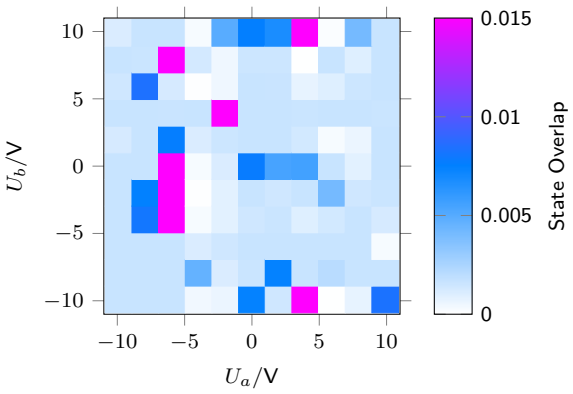

图 S6. 产生正交偏振测量结果的偏振输入状态的重叠。

长期稳定性

Ion-photon entanglement

通过双量子比特层析持续监测离子-光子接口的性能，该方法可以重构描述网络量子比特和偏振量子比特联合状态的密度矩阵 [图 S7(a)], ，如参考文献 [38] 所述。

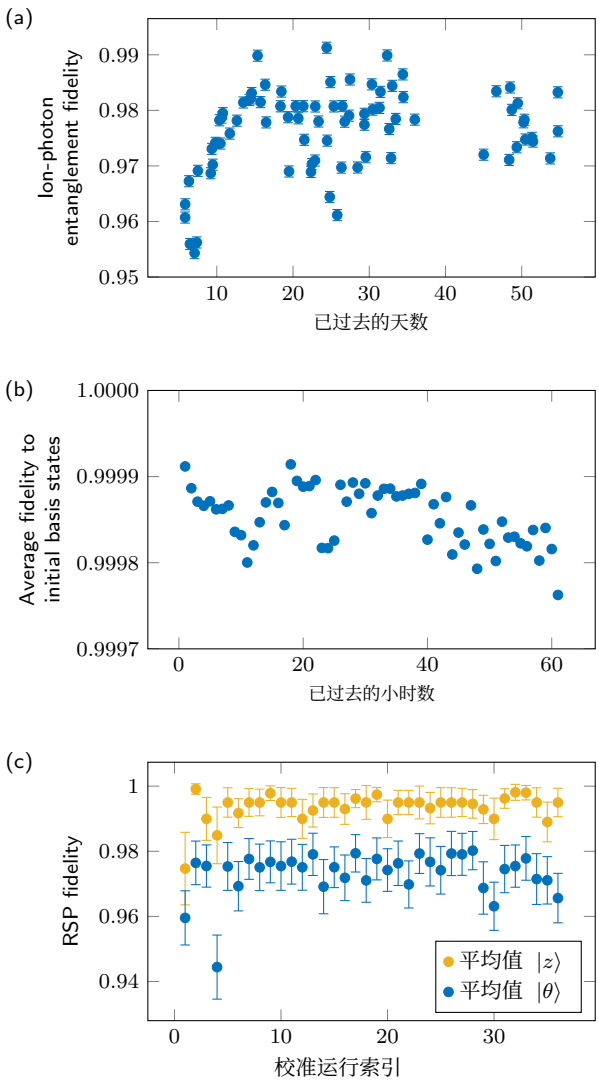

图 S7. (a) 光子量子网络链路、(b) 客户端实验装置以及 (c) 组合系统的长期稳定性。(a)、(b) 和 (c) 中的测量是在不同时间进行的。

Polarisation analyser

偏振分析器的稳定性通过在相同的一组电光调制器控制电压下，连续进行层析测量，独立地进行了离线检验，持续时间为 62h [Fig. S7(b)]。在此期间，由偏振漂移引起的保真度损失小于 3×10^{-4}，其限制因素为测量的精度。

Remote state preparation fidelity

我们使用最大似然层析重建网络量子比特的“受引导”状态，[36] 对两种偏振预示信号分别进行测量，并计算其对每个

可验证盲量子计算协议所需目标态的保真度。制备叠加态 $|\theta\rangle = (|0\rangle + \exp(i\theta)|1\rangle)/\sqrt{2}$ 的平均保真度为 $\theta \in \{0, \frac{\pi}{4}, \frac{2\pi}{4}, \ldots, \frac{7\pi}{4}\}$，制备 Z 基本征态 $|z\rangle$（其中 $z \in \{0,1\}$）的平均保真度为 $\mathcal{F}_\theta = 0.973(7)$ 和 $\mathcal{F}_z = 0.996(3)$，分别对应 [图 S7(c)]。

远程态制备校准

由于连接服务器与客户端的光纤会自然受到温度和应变变化的影响，因此需要定期校准其双折射。为此，客户端指示服务器按照规则的 21×21网格，以随机的总体顺序，对EOM 电压进行 X、Y 和 Z 基测量。对于雪崩光电二极管（APD） s 的预示信号，离子读出结果会取反，APD p的结果也会与之合并。令 $\Sigma^{\mathsf{B}}_{|y\rangle}$ 表示在 $\mathsf{B} \in \{\mathsf{X},\mathsf{Y},\mathsf{Z}\}$ 基测量时，结果为$y \in \{s,p\}$ 的读出观测次数。使用直接反演层析术重建布洛赫矢量 $\vec{b} = (b_\mathsf{X}, b_\mathsf{Y}, b_\mathsf{Z})$，其分量为

$$b_\mathsf{B} = \frac{\Sigma^{\mathsf{B}}_{|1\rangle} - \Sigma^{\mathsf{B}}_{|0\rangle}}{\Sigma^{\mathsf{B}}_{|1\rangle} + \Sigma^{\mathsf{B}}_{|0\rangle}} \ .$$

随后，客户端确定EOM 电压设置 $\vec{\ }$，使 b 与布洛赫球上对应于可验证盲量子计算协议所需的 5 个目标基中每一个基的轴之间的角偏差最小。

结合两个雪崩光电二极管 s 的p 读出结果，会导致远程态制备 保真度降低，前提是不同预示信号产生的状态并非完全正交，例如预示信号链中存在系统性延迟失配 [图 S9(a)]。在开展实验时，这导致簇态中每个量子比特产生 $\sim5\,\%$的不保真度。通过匹配预示信号的延迟，或分别分析两个不同预示信号对应的数据，可以消除这种失配，例如图 S7(c)所示的保真度数据。

2 个交互步骤的离子阱失效概率

陷阱量子比特错误率受到远程制备的影响 $|\theta\rangle$（保真度 $\mathcal{F}'_\theta \approx 0.924$低于 $\mathcal{F}_\theta$，这是由于在收集正文所示数据时雪崩光电二极管[图 S9(a)]之间未计及的时序失配所致）、错误检测iSWAP门（保真度 $\mathcal{F}'_{\mathsf{iS}} \approx 0.973$）、以及将 $\{|F=4,\, m_F=4\rangle, |F=3,\, m_F=3\rangle\}$逻辑量子比特与 $\{|F=4,\, m_F=0\rangle, |F=3,\, m_F=0\rangle\}$ Ca^+ 基态超精细结构中的磁场不敏感$\{|F=4,\, m_F=0\rangle, |F=3,\, m_F=0\rangle\}$ 量子比特之间的叠加态进行映射（保真度 $\mathcal{F}_{\mathrm{map}} \approx 0.98$），以及未进行错误检测的iSWAP门（保真度 $\mathcal{F}_{\mathsf{iS}} \approx 0.913$）。我们忽略态制备，测量和单量子比特旋转误差（保真度$\gtrsim 0.99$）。因此，预计陷阱量子比特的失败率为

$$p^{\mathrm{trap}_1}_{\mathrm{fail}} = 1 - \mathcal{F}_{\mathrm{map}}\mathcal{F}_{\mathsf{iS}}\mathcal{F}_{\mathrm{map}}\mathcal{F}'_{\mathsf{iS}}\mathcal{F}'_\theta \approx 0.21 \ .$$

虚拟量子比特错误率受远程制备到 $|z\rangle$（保真度 $\mathcal{F}_z \approx 0.996$）以及最终 iSWAP 门的影响：

$$p^{\mathrm{dummy}}_{\mathrm{fail}} = 1 - \mathcal{F}_{\mathsf{iS}}\mathcal{F}_z \approx 0.09 \ .$$

正文中给出的测量值 $p^{(1)}$ 失败 和 $p^{(2)}$ 失败 与这些估算值相当吻合。我们注意到，簇态中的最后一个量子比特不得从存储量子比特交换回网络量子比特；因此，影响该量子比特的 iSWAP 门数量会减少一个。对于双量子比特簇态，可以通过将最终测量基从 Z 改为 $B_{\theta_{q+1}}$，采用相同的序列实现；我们需要考虑第二种陷阱量子比特的位置安排：第一个量子比特为虚拟量子比特，第二个量子比特为陷阱量子比特时，我们预计

$$p^{\mathrm{trap}_2}_{\mathrm{fail}} = 1 - \mathcal{F}_{\mathsf{iS}}\mathcal{F}'_\theta \approx 0.16 \ ,$$

预期的平均测试轮次失败率为 $\frac{1}{2}p^{\mathrm{trap}_1} + p^{\mathrm{trap}_2} \approx 0.18$ $p_{\mathrm{fail}} =$ （失败 失败）。

如果在电光调制器电压校准中考虑雪崩光电二极管 的时序失配（使用 $\mathcal{F}_\theta$ 而非 $\mathcal{F}'_\theta$），预期的平均测试轮次失败率将降低 ≈ 0.14。

3 个交互步骤的测试轮次结果

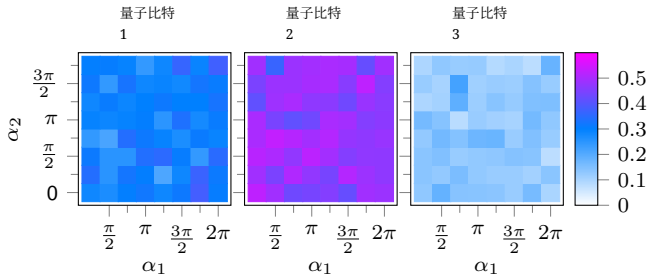

图 S8. 三节点簇态中各量子比特的观测陷阱失败率（其中量子比特 3 在 Z基下测量）。

我们在图 S8 中绘制了三节点簇态中各量子比特观测到的错误。在此实现中，线性簇态的首个和末个量子比特的错误率低于中间的量子比特。首个量子比特的错误较小，这是由于初始化轮次中的 iSWAP 错误检测

。最后一个量子比特在最终测量前不会从存储量子比特传回网络量子比特，因此影响该量子比特的 iSWAP 门数量减少了一个。

错误检测

初始化步骤中的误差会被实时检测（误差概率为 ~ 0.1），在这种情况下，当前轮次将被中止，并在经过一段冷却时间 [21] 后重新开始。由于重复此步骤所产生的开销与簇态的大小无关，因此不会影响所实现协议的可扩展性。在这里，客户端可以保持相同的随机变量 θ_1，因为相位偏移 $a_1\pi$ 取决于光子偏振测量结果，而该结果本质上是随机的。因此，服务器在网络量子比特上获得最大混合态。由于重复使用 θ_1 而通过经典通信泄露的信息也可以被消除，因为客户端控制着所有相关信号。错误检测概率与 iSWAP 门不保真度密切相关；通过降低这种不保真度，错误检测将变得不再必要。

光子损失

获得单光子先兆的平均时间为 $\approx 100\mu s$；因此，在 1 ms 的超时时间内未出现先兆的概率为 $< 10^{-4}$。如果在此期间未接收到光子，客户端会在进行一系列系统检查后，指示服务器从初始化步骤开始重复当前轮次。超时机制使服务器能够从可能暂时阻碍单光子生成的罕见事件中恢复，例如离子损失、光子收集光学器件未对准或激光器故障。这些轮次中由于重复而导致的信息泄漏完全是经典的，客户端可以将其消除，因为所有相关信号都由客户端控制。或者，客户端可以在每次重试时引入新的随机性，以避免这一问题。由光子损失导致的确定性损失受超时时间影响；如果客户端在操控尝试失败后仍继续执行协议，则可以完全消除这种损失。在这种情况下，服务器会在客户端完成本轮协议后检查系统故障。由于光子损失，这种方法产生的计算错误会随着超时时间的增加而呈指数级降低。

盲性

在此，我们考虑可能对协议的盲性造成不利影响的实验缺陷。盲性的特征在于恶意服务器能够获知多少关于客户端光子测量基选择的信息 θ_ℓ（每次实验包含 3 比特信息）。表 S1 总结了本节中量化的信息泄漏来源。在每次实验中

信道	来源	方法	泄漏量 / 比特	
			观测值	优化值
经典	测量角度强制设为 0		0	
	预示效率	推断值 0.00006	0.00006	
	预告延迟	推断值 0.35	0.00007	
量子	测量基	推断值 0.035	0.0007	
	推断出的不平衡结果为 0.00029		0.00029	0.00026
	—	测得为 0.031(4)	—	

表 S1. 单次交互步骤中的信息泄漏来源。优化后的数值假设先导延迟相匹配（从激发 $^{88}Sr^+$ 到电子探测），且偏振测量结果平衡。我们使用量子态层析来量化服务器通过测量网络量子比特可能获得的信息，并发现该结果与根据已知缺陷（测量基、结果不平衡）推断出的独立估计吻合良好。这些数值应与指定制导态 $|\theta_\ell\rangle$ 所需的信息量（3 比特）进行比较。

在实验中，索引为 ℓ，我们假设服务器拥有不受限制的访问权限，可以访问】【。

- 量子比特测量角 δ_ℓ（经典信号），
- 由光子探测时间（经典信号）设定的相位参考，
- 直到出现单光子预告（经典信号）之前的尝试次数，
- 以及记忆和网络量子比特的状态。

如果上述可观测量与 θ_ℓ 相关，则盲性会受到损害。

经典信息泄漏

在本节中，我们分析系统中存在的经典信息泄漏源所产生的影响。这些信息源不包括侧信道攻击，因为侧信道攻击通常难以进行系统性处理。我们注意到，在实际部署中，客户端可以直接监测并消除所有经典信道上的泄漏。

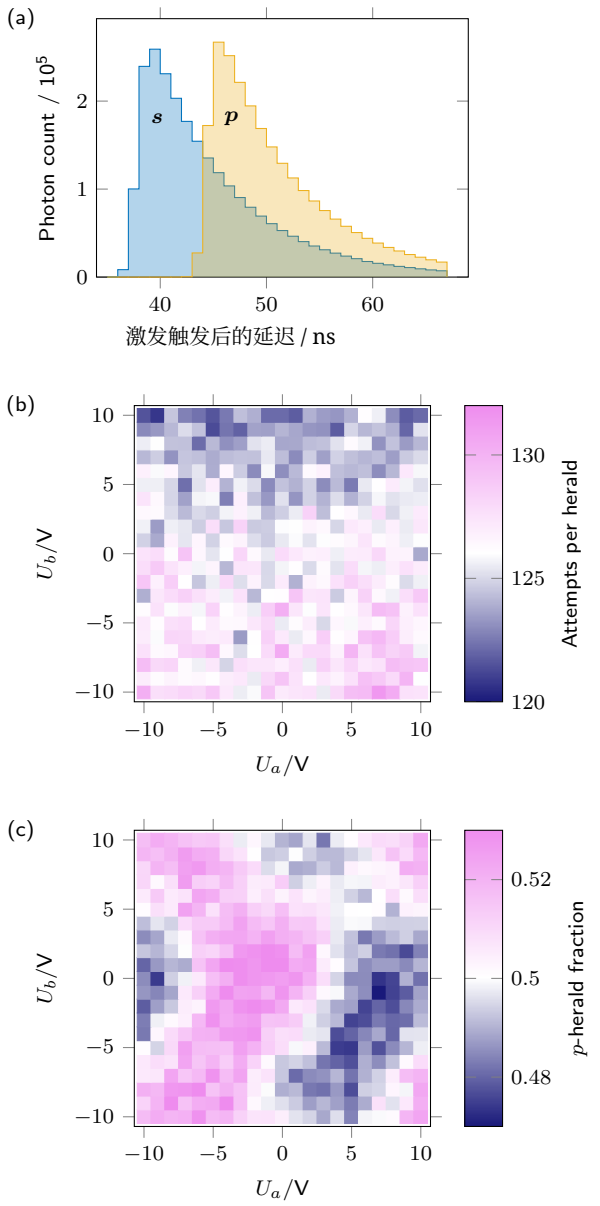

图 S9。（a） $^{88}Sr^+$ 脉冲激发与探测器 s 和 p探测到单光子预告之间延迟的直方图。（b）客户端宣布收到单光子预告前的平均尝试次数（每次尝试 1µs）随电光调制器 控制电压的变化。（c）结果为p 的预示信号占所有预示信号的比例随电光调制器控制电压的变化。

Encrypted measurement angle

δ_ℓ 不会泄漏信息，因为客户端在每次运行时都使用私有随机性对其进行加密。我们注意到，只要伪随机数生成器的实现具备密码学安全性，使用伪随机数生成器就不会损害盲性（针对计算受限的攻击者）。

Single-photon heralding delays

由于自发衰变的本质，光子到达雪崩光电二极管 的时间相对于 $^{88}Sr^+$的脉冲激发而言具有内在随机性。由于这些预示信号的时间决定了网络量子比特的相位参考，因此必须将其传达给服务器。因此，服务器可能利用预告信号时间分布之间的统计差异，推断偏振测量结果。

服务器可以采用最大似然策略来猜测光子测量结果。服务器可能知道探测器的属性，包括探测器 s 和探测器 p 在时间 x 出现预示信号的概率分布 $\Pr_s(x)$ 和 $\Pr_p(x)$。如果 $\Pr_s(x) > \Pr_p(x)$，服务器会假定在时间 x 预示的光子是在探测器 s 中观测到的，反之亦然。该最大似然策略成功的概率为 $\sigma(x)$。预期信息增益为 $\mathcal{R}_{\mathrm{ML}} = \sum_x \Pr(x)\mathcal{R}(\sigma(x))$，其中$\mathcal{R}(q) = 1 + q\log_2(q) + (1-q)\log_2(1-q)$ 是成功概率为 q的二元猜测的互熵，而 $\Pr(x)$ 是观测到到达时间 x的总概率。

在此次演示中，没有采取任何措施来均衡雪崩光电二极管的探测器响应。观测到的差异 [Fig. S9(a)] 主要源于电子信号链中的延迟未匹配，差值为 6.57(2) ns，导致 $\mathcal{R}_{\mathrm{ML}} \approx 0.35$ 位的信息泄漏。通过对其中一路信号增加延迟（例如，将电缆延长 ≈ 1.3m），可以最大限度地减少这一缺陷。校正延迟失配后，信息量将降至 $\mathcal{R}_{\mathrm{ML}} \approx 7\times10^{-5}$ 位，主要由高阶电子失真造成，例如用于时间戳标记的电子输入之间时序抖动的差异。此处使用现场可编程门阵列进行时间戳标记，其分辨率仅为 1 ns，且不同输入之间的抖动不一致。我们指出，这并非根本性限制；客户端可以通过适当调节经典预告信号来消除此类泄漏。

Single-photon heralding probability

由于客户端会公开宣布光子何时成功触发，因此服务器能够获知所尝试的次数，从而了解客户端实验装置的探测效率。如果探测效率取决于客户端选择的秘密测量设置，服务器原则上可能获取信息，从而损害协议的盲性。本文分析了这一因素对我们盲量子计算演示的影响程度。

我们观察到探测效率会根据 $\approx$ $\pm5\%$ 的电光调制器 电压设置而变化。

[图 S9(b)]。客户端每接收到一个光子后，都会改变电光调制器 电压。[1] 因此，服务器针对每个测量设置仅获得一个尝试次数样本。在每次测量时，由于这种逐次随机化，服务器的先验 知识都会重置为指数分布，其期望值 λ_0 根据此前各次测量中的尝试次数估计得出。费 Fisher 信息 $\mathcal{I}(\lambda) = \lambda^{-2}$量化了每个样本为更新底层分布估计所贡献的信息，即本次测量中期望值取决于秘密的指数分布 λ。需要将该量与期望值分别为 λ 和 λ_0 的指数分布之间的相对熵 $\mathcal{S}(\lambda_0, \lambda)$ 进行比较。

对于观测到的平均尝试次数 λ_0 =126 和最大偏差 $\Delta\lambda = |\lambda - \lambda_0| = 6$，每次测量获得的信息 $\mathcal{I}(\lambda) \lesssim 10^{-4}$ 可以忽略不计。即使对于给定的测量设置可获得无限次尝试次数样本，服务器获得的信息也绝不会超过 $\mathcal{S}(\lambda_0, \lambda) \sim 10^{-1}$ 比特。

量子信息泄漏

我们根据 Holevo 界 χ，分析服务器在 RSP 后测量网络量子比特平均能够获取的信息。对于完美盲性，$\chi = 0$，而一个量子比特最多可以传输 $\chi = 1$ 比特。本分析不包括测试轮次，在这些轮次中，客户端会将网络量子比特操控为 Z 基本征态。纳入虚拟量子比特会严格降低 Holevo信息，因为这些状态与θ_ℓ不相关。因此，整体隐私的提升取决于测试轮次所占的比例。

服务器接收通过操控网络量子比特而生成的量子态。对于计算中的每个量子比特，客户端会秘密选择 4 种测量基之一，即 B_i，$i \in \{1, 2, 3, 4\}$，以操控网络量子比特，使其以 q_i 的概率处于 ρ_i^+，或以 $(1 - q_i)$ 的概率处于 ρ_i^-，具体取决于测量结果。对测量结果 [2]，取平均后，服务器接收到这些状态

$\rho_i = q_i\rho_i^+ + (1 - q_i)\rho_i^-$ 且频率相同：

$$\rho = \frac{1}{4}\sum_{i=1}^{4} \rho_i \ .$$

Holevo信息用于界定包含在此量子态中的信息量，其表达式为

$$\chi(\rho) = S(\rho) - \frac{1}{4}\sum_{i=1}^{4} S(\rho_i) \ , \tag{3}$$

其中 $S(\rho) = -\mathrm{Tr}\,(\rho \log_2(\rho))$.

在我们的实验中，ρ_i^+ 和 ρ_i^- 由对纠缠子系统（光子）的测量进行引导，这种测量可用正算子值测量（正算子值测量）来描述。我们使用光子与环境之间的最大纠缠贝尔态 $\left(|s\rangle\,|0\rangle + |p\rangle\,|1\rangle\right)/\sqrt{2}$ 来模拟远程态制备，其合理性由“通过引导进行远程态制备”一节中的证明给出。

Imbalanced and mixed outcomes

我们使用描述具有消光比 ϵ_s 和 ϵ_p 的 偏振分束器 的 正算子值测量 $\{\hat{F}\}$，估算 远程态制备 的盲性；该偏振分束器接收 s-和 p-偏振输入，并在其（理想情况下） s-和 p-偏振输出端口放置了两个 雪崩光电二极管，其探测效率分别为 η_s 和 η_p：

$$\begin{aligned}
\hat{F}_p &= \eta_p(1 - \epsilon_s)\,|p\rangle\langle p| + \eta_s\epsilon_p\,|s\rangle\langle s| \ , \\
\hat{F}_s &= \eta_s(1 - \epsilon_p)\,|s\rangle\langle s| + \eta_p\epsilon_s\,|p\rangle\langle p| \ , \\
\hat{F}_0 &= 1 - \hat{F}_p - \hat{F}_s \ ,
\end{aligned}$$

其中，F_p 和 F_s 分别对应于在APD p和APD s处探测到光子，而 F_0 对应于一次光子损失事件。只要 PBS 的缺陷表现为退极化噪声，例如偏振消光有限，这些效应就不会影响Holevo信息。因此，不失一般性，我们可以假设 $\forall i$，ρ_i^+ 和ρ_i^- 是正交纯态，出现概率为 $q_i = \frac{\eta_p}{\eta_p + \eta_s} \approx \frac{1}{2}$。选择更有利的测量基配置[3], 后，一个量子比特所含的平均信息量上限为

$$\chi = \frac{(6 - \sqrt{2})\left(q - \frac{1}{2}\right)^2}{4\log_2(2)} + \mathcal{O}\left(\left(q - \frac{1}{2}\right)^4\right) \ . \tag{4}$$

[1] 在当前实现中，$\lesssim$5% 的情况下，重试（由于初始化步骤中的误差，概率为 $\sim$0.1，以及未能在超时时间间隔内生成单光子预告，概率为 $< 10^{-4}$）是在客户端未更改测量设置的情况下进行的。然而，这些额外信息并不会改变本分析的结论，并且通过在每次重试时也引入新的随机性即可消除这一问题。[2] 如果基角 θ_ℓ 被泄露，对网络量子比特进行简单测量也会确定性地揭示客户端的测量结果。

[3]令 $\rho_j^+ = |j\pi/4\rangle\langle j\pi/4|$ 不太有利，因为不平衡速率造成的误差会相加。然而，例如使用$\{\rho_1^+, \rho_2^-, \rho_3^+, \rho_4^+\}_j = |j\pi/4\rangle\langle j\pi/4|$ 时，部分误差会相互抵消。

根据图 S9(c) 所示测量结果并在正文中说明的平均不平衡$\langle|0.5-q|\rangle_{U_a,\ U_b}$，我们推断这种效应导致的信息泄漏为 $\chi \approx 2.9\times10^{-4}$ 比特。即使引入静态光子损耗以平衡两个探测器的探测效率，依赖于秘密的变化仍是信息泄漏的主要来源：我们估计在这种情况下泄漏 $\chi \approx 2.6\times10^{-4}$ 比特。虽然尚未确认图 S9(c) 所示变化的来源，但我们怀疑EOMs 会扰乱光子的波前，从而影响光子耦合进入光纤的模式匹配；为方便起见，我们使用这些光纤将光子耦合至APDs。由于量子信息编码在光子的偏振中，其空间模式与我们的实现无关，因此这一电压依赖的预示信号不平衡现象在实际中影响很小。或者，如果客户端根据本地随机性筛选预示信号，也可以彻底消除这一信息泄漏来源（代价是总预示率降低 50 %）。

Rotated POVMs

使用光子偏振和网络量子比特的乘积空间中的正算子值测量，

$$\hat{G}_p = \hat{F}_p \otimes 1\ ,$$
$$\hat{G}_s = \hat{F}_s \otimes \hat{Z}(\phi)\ ,$$
$$\hat{G}_0 = (1\otimes 1) - \hat{G}_p - \hat{G}_s\ ,$$

Holevo信息可以通过 $\chi \approx 0.103\times\phi^2$近似得到。

图 S9(a) 中所示正交预示信号之间的电子信号延迟，不仅会通过经典参考时间信号泄露信息，还会根据光子测量结果导致网络量子比特发生相对 Z旋转。代入 $\phi = \Omega_Z\Delta t$，其中 $\Omega_Z \approx 2\pi\times 14$MHz 为 $^{88}Sr^+$ 塞曼量子比特劈裂， $\Delta t = 6.57(2)$ ns 为两个预示信号之间测得的延迟差 [图 S9(a)]，，我们得到 $\chi \approx 0.035$ 比特。

一旦预示延迟相匹配，光子偏振测量中的不完美预计将成为通过此信道造成信息泄漏的主要因素。使用与不同预示信号对应的投影算符之间 0.0016 的平均重叠度 [图 S6]，我们得到$\phi \approx 0.08$弧度，因此潜在的信息泄漏为 $\chi \approx 7\times10^{-4}$ 比特。

或者，客户端可以不依赖偏振测量的正交性，而是利用每个偏振测量基都可通过两种不同的电光调制器 电压设置实现这一事实，并在两者之间随机切换。这种方法的有效性取决于电压校准的准确度，而通过获取校准数据可以提高其准确度，具有足够精度的校准数据。

测量量子信息泄漏

我们使用量子态层析重构基于测量的协议中网络量子比特在全部八个赤道目标态下的制导态（参见图 S7(c) 中相对于 $|\theta\rangle$ 的平均保真度）。利用估计得到的密度矩阵，我们根据公式 (3) 计算 Holevo 信息，并得到每个量子比特 0.031(4) 比特；该结果是在偏振测量基与上文推导公式 (4) 时所假设的（更有利的）配置相匹配的所有运行中取平均所得。

二维量子比特线性簇态的安全性与鲁棒性

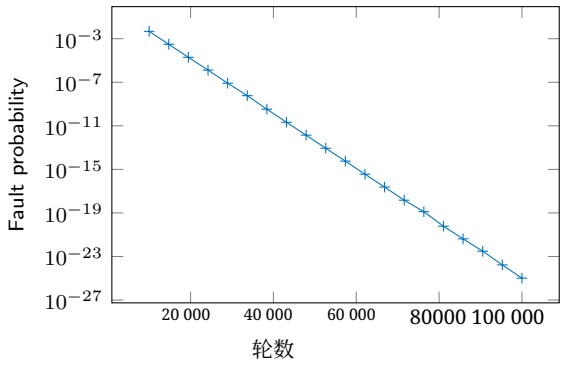

图 S10。我们评估 p_{fault} 随所提出协议中的轮数变化的情况，该协议见参考文献 [22]，，并假设 $p_{\max} = 0.185$。对于所示的所有数据点（十字标记），我们得到 $\tau \approx 0.6$ 和 $\omega_{\max} \approx 0.205$ 。

我们通过数值最小化参考文献 [22] 中的式 (E5)，评估参考文献 [22] 提出的验证协议下客户端接受错误结果的概率上界，Pr[fail]，，其中量子比特数为 $k = 2$，内在算法错误概率为 $p = 0$。在最小化过程中，我们通过设定 $p_{\text{rej}} = \Pr[\text{fail}]$，限制客户端因噪声而拒绝任何结果的概率 p_{rej}。最小故障概率，$p_{\text{fault}} := \min_{\mathcal{C}}\Pr[$ fail]，，其中 $\mathcal{C}$ 表示约束条件，在图 S10 中展示；总轮数 n 可变，且包括 τn 个测试轮次。最优阈值 ω、测试轮次占比 τ 以及安全参数（$\varphi, \epsilon_1, \epsilon_2, \epsilon_3$）由最小化器调整。故障概率，即安全性问题（接受错误结果，Pr[fail]）和鲁棒性问题（拒绝任何结果， p_{rej}）发生的概率，均随轮数增加而呈指数下降。

通过导引实现的远程态制备

在本节中，我们将展示如何利用导引安全地实现远程态制备。具体而言，只需从服务器到客户端进行单向量子通信即可，而且无需信任服务器制备纠缠对。

资源 1 远程态制备

输入：

- 客户端：单量子比特幺正变换的经典描述 U。
- 服务器：无输入。

输出：

- 客户端：无输出。
- 服务器：单量子比特状态 $U|0\rangle$。

协议 1 通过引导进行远程态制备

输入：

- 客户端：单量子比特酉算符 U 的经典描述。
- 服务器：无输入。

所需资源：

- 从服务器到客户端的安全单向量子信道。
- 从客户端到服务器的安全单向经典信道。

说明：

1. 服务器制备一个双量子比特贝尔态 $|\Psi\rangle = \frac{1}{\sqrt{2}}($ $|00\rangle \mp |11\rangle)$，并将其中一个量子比特发送给客户端。2. 客户端从哈尔测度中随机抽取一个单量子比特酉算符 U_1 ran- domly，然后将其作用于服务器接收的状态 U_1，并在计算基下对其进行测量，得到测量结果 m。3. 客户端将单量子比特酉算符 $U_2 = U\mathrm{X}^m U_1$ 的经典描述发送给服务器。.

4 服务器将 U_2 作用于剩余的单量子比特状态，并将其设为输出。

引理 1。 协议 *1* 以完美正确性实现资源 *1*。

证明。客户端测量后，服务器量子寄存器中剩余的单量子比特状态可描述为 $U_1^\dagger \mathrm{X}^m|0\rangle$。因此，服务器的输出变为 $U_2 U_1^\dagger \mathrm{X}^m|0\rangle = U|0\rangle$。

□

引理 2. 协议 *1* 实现了资源 *1*，且能够完美抵御恶意服务器。

证明。 作为证明的一部分，令 σ 按模拟器 1 中的定义给出。

模拟器 1

说明：

1. 模拟器期望从其左侧接口的理想功能接收一个单量子比特量子态$|\phi_1\rangle$ 作为输入。 2. 它期望从区分器的右侧接口接收一个单量子比特量子态 $|\phi_2\rangle$ 作为输入。 3. 它从哈尔测度中随机采样一个单量子比特酉算符 U_1 。 4. 它将双量子比特酉算符 $U_1 \otimes \mathrm{I}$ 作用于状态$|\phi_1\rangle|\phi_2\rangle$ ，并对其执行贝尔测量，得到测量结果 m_1 和 m_2。 5. 然后它令 $U_2 = U_1^\dagger \mathrm{Z}^{m_1}\mathrm{X}^{m_2}$ ，并在其右侧接口向区分器输出 U_2 的经典描述。

尚需证明，Re- source1 与 σ （理想世界）的组合，在其接口上生成的分布与客户端在协议 1 中的指令（真实世界）相同。

令 $|\psi\rangle$ 为区分器在将其寄存器的第一个量子比特发送给客户端之前的量子寄存器的净化。于是，在真实世界中，客户端完成测量后，服务器量子寄存器的状态（相差一个全局相位）可描述为

$$\langle 0|(\mathrm{X}^m U_1 \otimes \mathrm{I})|\psi\rangle,$$

以及来自客户端的经典消息包含酉算符 $UX^m U_1$ 的描述，其中 U_1 根据哈尔测度选取。将 U_1 代入 $\mathrm{X}^m U_1$ 得到

$$\langle 0|(U_1 \otimes \mathrm{I})|\psi\rangle,$$

以及在不改变 U_1 的分布的情况下，对 UU_1 进行经典描述。

在理想情况下，模拟器测量后，服务器的量子寄存器状态可以（除一个全局相位外）表示为

$$\langle \Phi^+|(\mathrm{Z}^{m_1}\mathrm{X}^{m_2}U_1 \otimes \mathrm{I})(U|0\rangle \otimes |\psi\rangle),$$

而来自客户端的经典消息包含酉算符 $U_1^\dagger \mathrm{Z}^{m_1}\mathrm{X}^{m_2}$ 的描述，其中 U_1 根据哈尔测度选取。这可以等价地改写为

$$\langle 0|(U^\dagger U_1^\dagger \mathrm{Z}^{m_1}\mathrm{X}^{m_2} \otimes \mathrm{I})|\psi\rangle.$$

将变量从 U_1 换为 $\mathrm{Z}^{m_1}\mathrm{X}^{m_2}U_1^\dagger U^\dagger$，同时不改变 U_1 的分布，可得

$$\langle 0|(U_1 \otimes \mathrm{I})|\psi\rangle,$$

以及 $(\mathrm{Z}^{m_1}\mathrm{X}^{m_2}U_1^\dagger U^\dagger)^\dagger \mathrm{Z}^{m_1}\mathrm{X}^{m_2} = UU_1$ 的经典描述，由此完成证明。

□

[1] A. Sarma、R. Chatterjee、K. Gili 和 T. Yu，超导处理器上的量子无监督与监督学习，Quantum Inf. Comput. **20**，541（2019）。[2] J. Alcazar、V. Leyton-Ortega 和 A. Perdomo-Ortiz，机器学习中的经典模型与量子模型：来自金融应用的见解，Mach. Learn.: Sci. Technol. **1**，035003（2020）。[3] T. Proctor、K. Rudinger、K. Young、E. Nielsen 和 R. Blume-Kohout，量子计算机能力的测量，Nat. Phys. **18**，75（2022）。[4] D. Amaro、C. Modica、M. Rosenkranz、M. Fioren- tini、M. Benedetti 和 M. Lubasch，用于组合优化的过滤变分量子算法，Quantum Sci. Technol. **7**，015021（2022）。[5] J. J. M. Kirsopp、C. Di Paola、D. Z. Manrique、M. Krompiec、G. Greene-Diniz、W. Guba、A. Meyder、D. Wolf、M. Strahm 和 D. Mu˜noz Ramo，蛋白质–配体相互作用的量子计算量化，Int. J. Quantum Chem. **122**，e26975（2022）。[6] A. Broadbent、J. Fitzsimons 和 E. Kashefi，通用盲量子计算，载于 *50th Annu. IEEE Symp. Foundations Comput. Sci.* 2009 517 526 ( ) 第 – 页。[7] J. F. Fitzsimons 和 E. Kashefi，无条件可验证的盲量子计算，Phys. Rev. A **96**，012303 2017( )。[8] A. Gheorghiu、T. Kapourniotis 和 E. Kashefi，量子计算验证：现有方法概述，Theory Comput. Syst. **63**，715（2019）。[9] C. Badertscher、A. Cojocaru、L. Colisson、E. Kashefi、D. Leichtle、A. Mantri 和 P. Wallden，经典客户端委托量子计算的安全性限制，载于 *Advances in Cryptology – ASIACRYPT 2020*，S. Moriai 和 H. Wang 编（Springer International Publishing）第 667–696 页。[10] A. Cojocaru、L. Colisson、E. Kashefi 和 P. Wallden，经典客户端盲量子计算的可能性，Cryptography **5**，10.3390/cryptography5010003（2021年）。[11] S. Barz、E. Kashefi、A. Broadbent、J. F. Fitzsimons、A. Zeilinger 和 P. Walther，盲量子计算演示，Science **335**，303（2012）。[12] S. Barz、J. F. Fitzsimons、E. Kashefi 和 P. Walther，量子计算的实验验证，Nat. Phys. **9**，727（2013）。[13] K. A. G. Fisher、A. Broadbent、L. K. Shalm、Z. Yan、J. Lavoie、R. Prevedel、T. Jennewein 和 K. J. Resch，加密数据上的量子计算，Nat. Commun. **5**，3074（2014）。[14] C. Greganti、M.-C. Roehsner、S. Barz、T. Morimae 和 P. Walther，仅测量盲量子计算演示，New J. Phys. **18**，013020（2016）。

[15] Y. Li、P. C. Humphreys、G. J. Mendoza 和 S. C. Benjamin，《容错线性光学量子计算的资源成本》，Phys. Rev. X **5**，041007（2015）。[16] W. Pfaff、B. J. Hensen、H. Bernien、S. B. van Dam、M. S. Blok、T. H. Taminiau、M. J. Tiggelman、R. N. Schouten、M. Markham、D. J. Twitchen 和 R. Hanson，《远距离固态量子比特之间的无条件量子隐形传态》，Science **345**，532（2014）。[17] D. Hucul、I. V. Inlek、G. Vittorini、C. Crocker、S. Deb- nath、S. M. Clark 和 C. Monroe，《利用光子和声子实现原子量子比特的模块化纠缠》，Nat. Phys. **11**，37（2015）。[18] N. Kalb、A. A. Reiserer、P. C. Humphreys、J. J. W. Bakermans、S. J. Kamerling、N. H. Nickerson、S. C. Benjamin、D. J. Twitchen、M. Markham 和 R. Hanson，《固态量子网络节点之间的纠缠蒸馏》，Science **356**，928（2017）。[19] P.-J. Stas、Y. Q. Huan、B. Machielse、E. N. Knall、A. Su- leymanzade、B. Pingault、M. Sutula、S. W. Ding、C. M. Knaut、D. R. Assumpcao、Y.-C. Wei、M. K. Bhaskar、R. Riedinger、D. D. Sukachev、H. Park、M. Lon˘car、D. S. Levonian 和 M. D. Lukin，《集成式错误检测的稳健多量子比特量子网络节点》，Sci- ence **378**，557（2022）。[20] T. Wilk、S. C. Webster、A. Kuhn 和 G. Rempe，《单原子—单光子量子接口》，Science **317**，488（2007）。[21] P. Drmota、D. Main、D. P. Nadlinger、B. C. Nichol、M. A. Weber、E. M. Ainley、A. Agrawal、R. Srinivas、G. Araneda、C. J. Ballance 和 D. M. Lucas，《囚禁离子量子网络节点中的稳健量子存储器》，Phys. Rev. Lett. **130**，090803（2023）。[22] D. Leichtle、L. Music、E. Kashefi 和 H. Ollivier，《以极低开销在含噪设备上验证 BQP 计算》，PRX Quantum **2**，040302（2021）。[23] R. Raussendorf 和 H. J. Briegel，《单向量子计算机》，Phys. Rev. Lett. **86**，5188（2001）。[24] M. A. Nielsen，《簇态量子计算》，Rep. Math. Phys. **57**，147（2006）。[25] A. M. Childs、D. W. Leung 和 M. A. Nielsen，《量子计算基于测量方案的统一推导》，Phys. Rev. A **71**，032318（2005）。[26] T. Morimae 和 K. Fujii，《一种 Alice 只需进行测量的盲量子计算协议》，Phys. Rev. A **87**，050301(R)（2013）。[27] J. F. Fitzsimons，《私密量子计算：盲量子计算及相关协议导论》，《npj量子信息》**3**，23（2017）。[28] D. Aharonov、M. Ben-Or、E. Eban 和 U. Mahadev，《量子计算的交互式证明》（2017），arXiv:1704.04487。[29] A. Broadbent，《如何验证量子计算》，Theory Comput. **14**，1（2018）。[30] A. Mantri、T. F. Demarie 和 J. F. Fitzsimons，《簇态与 (x, y) 平面测量实现量子计算的普适性》，Sci. Rep. **7**，42861（2017）。[31] C. H. Bennett、D. P. DiVincenzo、P. W. Shor、J. A. Smolin、B. M. Terhal 和 W. K. Wootters，《远程态制备》，Phys. Rev. Lett. **87**，077902（2001）。[32]实验方法、实验装置，以及从客户端到服务器的信息泄漏定量分析的详细内容，参见补充材料。[33] T.-M. Tomescu, *Qubit Encryption by Rotation of Po-larization States* ，硕士论文 ，牛津大学

（2019）。[34] J. G. Ziegler 和 N. B. Nichols，自动控制器的最佳设定，《美国机械工程师学会会刊》**64**，759 1942( )。[35] B. N. Simon、C. M. Chandrashekar 和 S. Simon，将哈密顿旋转用作设计单量子比特酉门的可视化工具箱，Phys. Rev. A **85**，022323（2012）。[36] J. ˇReh´aˇcek、Z. Hradil、E. Knill 和 A. I. Lvovsky，用于量子层析的稀释最大似然算法，Phys. Rev. A **75**，042108（2007）。[37] B. B. Blinov、D. L. Moehring、L.-M. Duan 和 C. Mon- roe，观测到单个囚禁原子与单光子之间的纠缠，《自然》**428**，153（2004）。[38] L. J. Stephenson、D. P. Nadlinger、B. C. Nichol、S. An、P. Drmota、T. G. Ballance、K. Thirumalai、J. F. Good- win、D. M. Lucas 和 C. J. Ballance，基本量子网络中量子比特的高速率、高保真度纠缠，Phys. Rev. Lett. **124**，110501（2020）。[39] K. Wright、K. M. Beck、S. Debnath、J. M. Amini、Y. Nam、N. Grzesiak、J.-S. Chen、N. C. Pisenti、M. Chmielewski、C. Collins、K. M. Hudek、J. Mizrahi、J. D. Wong-Campos、S. Allen、J. Apisdorf、P. Solomon，

M. Williams, A. M. Ducore, A. Blinov, S. M. Kreike- meier, V. Chaplin, M. Keesan, C. Monroe, and J. Kim, 对一台 11 量子比特量子计算机进行基准测试, Nat. Commun. **10**, 5464 (2019). [40] J. Keller, T. Burgermeister, D. Kalincev, A. Didier, A. P. Kulosa, T. Nordmann, J. Kiethe, and T. E. Mehlst¨aubler, 在线性库仑晶体中将系统频率不确定度控制在 10^{-19} 水平, Phys. Rev. A **99**, 013405 2019( ). [41] A. C. Hughes, V. M. Sch¨afer, K. Thirumalai, D. P. Nadlinger, S. R. Woodrow, D. M. Lucas, and C. J. Bal- lance, 对一种高保真度混合物种纠缠门进行基准测试, Phys. Rev. Lett. **125**, 080504 (2020). [42] V. Krutyanskiy, M. Meraner, J. Schupp, V. Krcmarsky, H. Hainzer, and B. P. Lanyon, 跨越 50 km 光纤的光-物质纠缠,《npj量子信息》 **5**, 72 (2019). [43] E. N. Fokoua, S. A. Mousavi, G. T. Jasion, D. J. Richard- son, and F. Poletti, 空芯光纤中的损耗：机制、标度规律与极限, Adv. Opt. Photon. **15**, 1 (2023). [44] S. Bourdeauducq *et al.*, m-labs/artiq：6.0（版本 6.0）（2021年）。