利用相干态进行相对论位置验证

Guan-Jie Fan-Yuan,[1]*2, 3,* * *Yang-Guang Shan,*[1]*2,3,* * *Cong Zhang,*[4], * *Yu-Long Wang,*[1, 2, 3]*Yu-Xuan Fan,*[1, 2, 3] *Wei-Xin Xie,*[1, 2, 3] *De-Yong He,*[1, 2, 3, 5] *Shuang Wang,*[1]*, 2, 3, 5,* † *Zhen-Qiang Yin,*[1, 2, 3, 5] *Wei Chen,*[1, 2, 3, 5] *Song-Nian Fu,*[4] *Guang-Can Guo,*[1, 2, 3, 5] 和 *Zheng-Fu Han*[1, 2, 3, 5]1 *Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*

[2] *Anhui Province Key Laboratory of Quantum Network,University of Science and Technology of China, Hefei 230026, China*[3] *CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China*[4] *Institute of Advanced Photonics Technology, School of Information Engineering,Guangdong Provincial Key Laboratory of Information Photonics Technology, and Key Laboratory of Photonic Technology for Integrated Sensing and Communication, Ministry of Education of China, Guangdong University of Technology, Guangzhou 510006, China*

[5] *Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China*

arXiv:2602.01787v1 [quant-ph] 2 Feb 2026

确定实体的位置是几乎所有活动的基本前提。然而，经典方法已被证明无法提供安全的位置验证，这意味着证明者可以误导验证者对其实际位置的判断。在本工作中，我们提出并实验实现了一种安全的位置验证协议，该协议在信息论框架内利用量子光学与相对论。利用相位随机化弱相干态，相距2公里的两名验证者能够以优于75米的精度安全地验证证明者的位置。这些结果将安全的基于位置的认证确立为一种切实可行的可能，为金融交易、灾害应对以及经认证的安全通信等应用铺平了道路。

I. 引言

自互联网普及以来，远程交易、在线通信和数字治理等活动重塑了社会的运作方式。然而，随着全球互联的加速，人们对信息来源地的信任能力却未能同步跟上。在身份、资产与自主代理远程交互的世界中，缺乏可验证的位置在数字信任中留下了关键缺口。因此，确定某一实体是否实际处于其所声称的位置，已成为身份认证的一项关键安全性凭证 [1–3]。

尽管安全地验证位置至关重要，但从根本上说，这一任务极具挑战性。典型的位置验证协议 [4] 使用多个验证者，向证明者发送协调一致的挑战消息；证明者必须根据收到的所有消息生成凭证并将其返回。由于往返时间受到相对论光速限制，验证者可以同时检查凭证及其到达时间，从而确定证明者的位置 [5]。然而，经典位置验证已被证明是不安全的 [1] ，因为经典信息可以在不被探测到的情况下复制和转发，这使不诚实证明者能够部署协同攻击者来截获并转发消息，在不增加延迟的情况下生成正确的凭证，从而欺骗验证者，使其误判证明者的位置。

防范不诚实证明者不能仅仅依赖相对论时空关系。将经典信息编码到量子比特中，可以使截获和重发行为被探测到，这构成了量子安全通信的基础 [6]。因此，将量子比特融入位置验证，为克服经典位置验证在安全定位方面的不可能性，提供了一种基于物理原理的方法 [7–13]。近期的协议 [7, 8]采用了这一方法，构造由 n 经典比特和单个量子比特组成的挑战消息，并要求对手拥有 $O(n)$ 个纠缠对才能发动成功攻击。由于制备经典比特远比制备纠缠态简单，这种设计符合密码学不对称性原理的基本要求：诚实证明者应能轻松通过验证者的检查，而任何试图冒充的对手都难以做到这一点。

尽管在概念上颇具吸引力，基于量子比特的位置验证协议在实现上极具挑战性，迄今尚无完整的实验演示 [4, 14]。首先，相对论约束使验证过程对延迟极其敏感。现代通信中常见的毫秒级额外延迟，按光速换算会造成数百公里的位置误差，这使该协议无法实际应用

* 这些作者贡献相同
† wshuang@ustc.edu.cn

。更重要的是，在信息论框架下，已有证明表明，证明者必须能够支持 2^{2^n} 双指数凭证计算，其计算量为 $n > 20$ [8]，即约为 10^{315653}, ，其中数值越大n ，安全性越强。这种规模带来了难以承受的计算需求，并导致显著延迟。最后，采用量子光学的协议需要单光子源、高重复频率，并且包括调制、传输和探测在内的总损耗不得超过 3 dB。每一项要求在实践中都极难实现，同时满足所有要求则更具挑战性。

本文在信息论框架下，通过实验将量子光学与相对论相结合，实现了完整的量子位置验证（QPV），验证精度优于 75 m，达到建筑尺度验证精度，与典型安全区域尺寸相当，表明其具有实际应用价值。在第二节中，我们建立了基于相位随机化弱相干态（PR-WCSs）的安全框架，解决了多光子安全问题，并消除了对单光子源的需求。其直接优势在于，相干态光源易于获得、不受调制损耗影响，并且天然兼容高重复频率。这使得高速、低损耗的偏振编码方案成为可能；该方案采用由微型组装旋转环行分束器（RCS）构成的 Sagnac架构实现，从而实现高保真度偏振态制备。在探测方面，我们开发了一种由高频高电压驱动的光开关，并将其与超导探测器结合，以实现低损耗偏振分析。整体量子光学效率达到 70%，同时错误率保持在 0.27%。

为解决与 n比特经典消息相关的延迟问题，我们进一步开发了专用经典链路，该链路基于密集波分复用开关键控（DWDM–OOK）信号生成、反谐振空芯光纤（AR-HCF）传输以及高速PIN光电二极管探测。此最简并行传输检测设计结合高带宽、近光速信道，可实现可扩展的 n，且几乎不会产生额外延迟。最后，我们利用基于现场可编程门阵列（FPGA）和双倍数据速率（DDR）存储器阵列构建的硬件查找表，实现大规模n 高速凭证计算；其计算空间超过 $10^{330985980541}$, ，对应于 $n = 40$，映射计算延迟低于118 ns。实现细节见第三节，进一步讨论见第四节。

II. 协议

量子位置验证的机制是：证明者根据验证者提供的信息执行所需操作，并返回结果以供验证。当证明者诚实行事时，信息交换的往返时间可用于界定证明者的位置。因此，量子位置验证协议可分为三个组成部分：（i）消息制备，（ii）凭证生成，以及（iii）位置推断。在消息制备环节，验证者创建并向证明者发送由经典比特和一个量子比特组成的挑战消息。随后，证明者进行凭证生成，按照约定规则生成凭证并立即返回。最后，在重复这些步骤 N 轮后，验证者根据 N 凭证的正确性进行位置推断；各轮中相对于光速限制的最大额外延迟决定了推断位置的不确定性。

图 1a 展示了该协议的结构，包括两名验证者 V_1 和 V_2，以及一名证明者 P；图中还展示了经典信息和量子信息的传递过程，分别用橙色箭头和蓝色箭头表示。两名验证者共同向证明者发送 n 个经典比特，每人贡献 $n/2$ 个比特，记为 $\{0,1\}^{n/2}$。此外， V_1 向证明者发送一个相干态$|\alpha_{b,\ c}\rangle$ ，而 b， $c \in \{0,1\}$ 共同决定该态的偏振。比特 b 指定两个本征基中的一个，而 c 指定两个本征值中的一个。 b的值由布尔函数f 确定： $\{0,1\}^n \to b$；如图中的 f 所示，这也是证明者执行的操作。证明者处的操作 $\mathcal{M}$表示在推断出的本征基下，对接收到的量子态进行投影测量，得到测量结果 c。该值 c 作为凭证返回给验证者以供验证。

在协议开始之前，验证者就总轮次数 N、经典字符串 $\{0,1\}^n$ 以及每一轮的比特 b 和 c 达成一致，并与证明者就一个布尔函数达成一致。该布尔函数从所有可能的映射中均匀随机选取；对于输入长度为 n 的情况，这类映射共有 2^{2^n} 个。

消息制备。 对于消息的经典部分，验证者各自发送当前轮次约定的 $\{0,1\}^{n/2}$ 字符串，并记录各自的经典消息进入信道的时间，分别记为 t_1 和 t_2。对于量子部分， V_1 制备一个弱相干态 $|\alpha\rangle$ ，并根据 b 和 c 调制其偏振，随后将该态发送给证明者。

凭证生成。 收到验证者发来的两个 $\{0,1\}^{n/2}$ 字符串后，证明者将它们组合成一个 n位输入，并应用布尔函数以得到 b。随后，证明者在 b指定的基中测量 V_1 发送的量子态，得到结果 c'。该值 c' 随后被返回给验证者。需要注意的是， V_1 可以调整量子态的传输时间，使其恰好在证明者执行测量时到达，从而无需使用量子存储器。由于态制备中的不完美以及

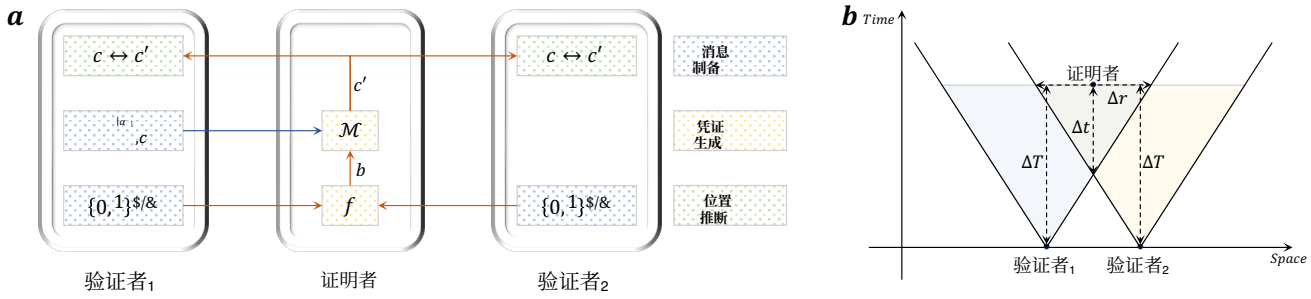

图 1. 使用相干态的量子位置验证协议。验证者通过空间上相互分离的两个验证者 V_1 和 V_2，验证证明者 P 的位置。**a.** 单轮位置验证中的信息流。 V_1 和 V_2 各向 P 发送 $n/2$ 个经典比特。与此同时， V_1 发送一个相干态 $|\alpha_{b,\ c}\rangle$，其平均光子数为 $|\alpha|^2$，偏振由本征基 b 和本征值 c 决定。 P 计算布尔函数 $f\colon \{0,1\}^n \to b$，得到 b，并据此测量（$\mathcal{M}$）量子态的偏振，然后将结果 c' 作为凭证返回给验证者进行验证。**b.** 位置精度的光锥解释。没有任何延迟时， P 精确位于来自 V_1 和 V_2 的光锥交点处。额外延迟 Δt 使范围 Δr 内的所有事件都满足验证条件，因此 P 的位置被限制在 Δr 之内。

测量， c' 可能与 c 不同。此外，由于光学损耗和有限的探测效率，证明者有时可能得不到测量结果，记为 $\perp$，从而 $c' \in \{0, 1, \perp\}$。

位置推断。 验证者接收值 c' ，并分别将其到达时间记录为 t_1' 和 t_2'。如果 $c' = c$，则该事件被归类为正确事件。如果 $c' \neq c$，则该事件被计为错误并丢弃事件。如果证明者未获得测量结果，则该事件被记录为无响应事件。经过 N 轮次后，正确事件的数量记为 n_c，错误并丢弃事件的数量记为 n_I，无响应事件的数量记为 $n_\perp$。通过设定评分方案和阈值来作出验证决定，使诚实的 P 能够超过阈值，而不诚实的 P 无法超过阈值。得分计算为 $\Gamma = \gamma_C n_c - \gamma_\perp n_\perp - \gamma_I n_I$，其中每一项的系数通过半定规划（SDP）[8, 15]获得。令 Γ_0 为阈值。通过适当选择 Γ_0，不诚实证明者的得分超过该阈值的概率可以小到呈指数级，而诚实证明者的得分几乎必然能够超过阈值。因此，如果 $\Gamma \geq \Gamma_0$，则认为 P 通过了验证，其可能的位置区域为以两位验证者为中心、半径分别为 $(t_1' - t_1)\ c_0/2$ 和 $(t_2' - t_2)\ c_0/2$ 的两个区域的交集，其中 c_0 表示真空中的光速。

图1b通过光锥表示法展示了延迟与允许位置范围之间的关系。假设验证者观测到接收凭证的往返时间为 $2\delta T$ ，即单程时间为 $\delta T = (t_1' - t_1)/2 = (t_2' - t_2)/2$。在光速限制下，每位验证者的允许区域对应其各自光锥内的蓝色和橙色区域，这些区域的交集则确定了证明者可能所在的位置。如果不存在额外延迟 δt ，两个区域便会相切，使证明者的位置能够被定位到单点。出现额外延迟后，证明者的位置则被限制在大小为 $\delta r = c_0 \delta t$ 的范围内。

与先前协议 [7, 8], 相比，我们的协议的关键区别在于使用相干态而非单光子。相干态可由激光源轻易产生，且不会因衰减而退化，因此特别适用于实现量子位置验证。然而，相干态中的多光子分量可通过分束攻击实现无法检测的偏振态克隆，从而引发安全性问题；而真空分量不携带任何信息，会降低验证效率。

为了解决这些问题，我们通过分别分析不同的光子数分量，并确定在对抗者最优条件下 Γ_0 的上界，构建了 Γ_0 的相干态版本。我们采用相位随机化相干态，它们是福克态的混合态，其光子数服从泊松分布 $\pi(|\alpha|^2)$。在这种表示下，每个协议轮次等同于 V_1 发送一个偏振编码福克态。

对于单光子态，我们采用先前协议中使用的方法。对于真空态，对手可以声明无响应事件，也可以以二分之一的概率产生正确事件。通过枚举所有可能性，我们推导出真空态对 Γ_0 上界的贡献。对于多光子态，我们假设最坏情况，即对手始终能够发动完美攻击，从而只产生正确事件。结合所有光子数贡献，即可得到 Γ_0 的期望上界。

此外，尽管三种光子数情形的概率是已知的，但有限轮次会引入统计涨落。利用切尔诺夫界，我们获得了 Γ_0 的严格有限尺寸上界。通过反向优化使诚实证明者得分最大化的平均光子数，我们进一步提高了验证的稳健性。 Γ_0 上界的分析，以及对统计涨落和相干态参数优化的处理，均在方法中的“相干态安全得分”部分进行了详细介绍。

该协议不仅通过使用相干态，解决了可用性、可操作性和损耗容忍度方面的关键实际瓶颈，还建立了有限尺寸安全界限，并引入了一种参数优化方法，以提高鲁棒性。这些贡献使量子位置验证从理论定义的概念迈向实际可实现的阶段，并为后续的实验实现奠定了基础。

III. 实现

实验系统遵循图2所示的协议架构。 V_1 由三个部分组成：用于消息制备的经典比特制备单元（CPU）和量子态制备单元（QPU），以及用于位置推断的凭证接收单元（CRU）。 V_2 的结构与 V_1 相同，但不包括QPU。 P包含用于凭证生成的布尔函数单元（BFU）和量子态测量单元（QMU）。在实现中，量子态传输和测量的损耗与错误率决定了协议能否成功执行，而经典比特传输和证明者操作带来的额外延迟会影响位置验证的精度。使用相干态可消除量子态制备损耗的影响。

包含 QPU 和 QMU 的量子部分需要足够高效，才能满足给定的安全阈值。一方面，必须控制损耗和错误率，使诚实证明者能够获得更高得分；另一方面，需要提高比特率，以提升攻击所需量子资源的阈值。我们为每个对损耗敏感的组件采用损耗最低的方案。信道采用衰减为 0.142 dB/km 的超低损耗光纤（ULL-F）；基选择通过插入损耗为 0.6 dB 的光开关实现；探测则使用效率为 90% 的超导单光子探测器。由此，整个系统的传输效率达到 70%。

然而，低损耗光开关的工作频率通常只有 kHz，这限制了比特率。为解决这一问题，我们开发了一种快速响应的高压驱动器，使光开关能够以 2 MHz 的频率工作，从而将安全资源阈值提高至 2($n/4-5$) Mbps。最后，为了制备错误率较低的量子态，我们采用萨格纳克干涉仪装置生成 $|H\rangle + e^{i\phi}|V\rangle$、 $\phi \in \{0, \pi, \pi/2, 3\pi/2\}$ 的四种偏振态。萨格纳克干涉仪中的分束器由微组装旋转器、环形器和偏振分束器组成，称为旋转环行分束器。该装置可实现简单而稳定的态编码，量子比特误码率低于 0.27%。具体细节见《方法》部分的“高保真量子态制备”一节。

延迟的测量范围是从验证者发送基信息到收到测量结果的时间。理想情况下，总延迟应接近光速在真空中的往返飞行时间。遗憾的是，经典比特和凭证的传输、布尔函数的执行，以及量子态的基选择与探测都会引入额外延迟。更具挑战性的是，布尔函数需要较大的 n ，而量子测量又要求高效率，这往往与低延迟的目标相冲突。

我们主要关注布尔函数的实现，因为它会直接影响延迟和 n。我们设计了一种基于现场可编程门阵列和DDR存储器的电路来实现布尔函数，其中基信息用作数据地址输入，相应存储的比特则作为输出。填入DDR的不同随机比特序列对应不同的布尔函数映射。DDR容量总计为1 Tb $= 2^{40}$ 比特，对应于 $n = 40$。通过利用并行性和组合逻辑，布尔函数的运行延迟为117.3 ns，主要由DDR访问延迟造成。具体细节见“方法”中的“大规模快速布尔函数运算”部分。

接下来，我们讨论传输延迟，尤其是 40 比特基信息的传输延迟。通过在验证者与证明者之间使用长度分别为 978.4 m 和 981.2 m 的 AR-HCF 链路，并采用密集波分复用开关键控编码同时传输比特， V_1 至 P 和 V_2 至 P 的额外延迟分别显著降低至 22.05 ns 和 22.39 ns。随后，低损耗光开关的高压驱动器采用氮化镓技术，可在 50 ns 内实现 400 V 峰峰值电压切换。由于内部布线，单光子探测器会引入约 17.7 ns 的延迟。其余约 20 ns 的延迟则由组件之间不可避免的光纤和电缆连接造成。关于这两部分的详细说明，请参阅《方法》中的“近光速信道”和“低延迟低损耗量子测量”章节。

在实验中，一段随机比特序列被载入布尔函数电路的存储器中，用以表示所选函数。两位验证者以 2 MHz 的频率向证明者发送验证流，同时 V_1

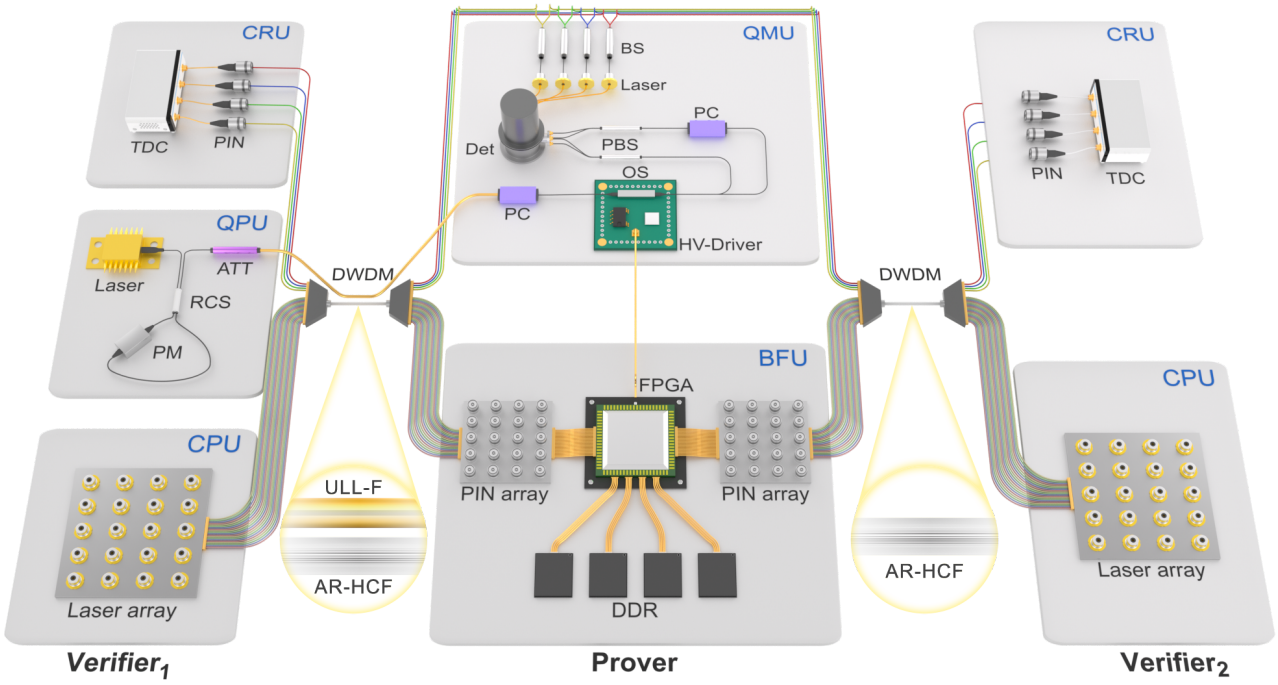

图2. 量子位置验证实验装置。从左到右依次为 V_1、 P和 V_2，彼此间隔约0.98千米。验证者的经典比特制备单元（CPU）和量子态制备单元（QPU）负责实现协议中的消息制备步骤，而凭证接收单元（CRU）负责实现位置推断步骤。证明者的布尔函数单元（BFU）和量子态测量单元（QMU）负责实现凭证生成步骤。量子态采用 $|H\rangle + e^{i\phi}|V\rangle$ 偏振制备，并通过包含相位调制器（PM）和微组装旋转环形分束器（RCS）的萨格纳克干涉仪，经超低损耗光纤（ULL-F）传输至 P。所有经典信号均采用激光器阵列，通过密集波分复用开关键控（DWDM-OOK）发送，并由高速PIN探测器接收；信号通过反谐振空芯光纤（AR-HCF）以接近光速传输。BFU通过现场可编程门阵列（FPGA）上的查表和逻辑运算实现，并配备1 Tb DDR存储器，其中PIN阵列信号用作地址，存储数据则作为输出测量基。QMU使用高电压驱动的低损耗光开关（OS）选择测量基，并使用超导探测器（DET）进行探测。 V_1 和 V_2 采用时间数字转换器（TDC）捕获返回的测量信号并记录延迟。ATT，衰减器；PC，偏振控制器；BS，分束器；PBS，偏振分束器。

以相同的速率向证明者发送量子比特。证明者解码基信息并据此测量量子比特，然后立即将单光子探测器结果发送回各位验证者。在我们的实验中，成功验证所需的轮次数和所发送弱相干态的强度分别为 10^7 和 0.52。这些参数根据量子子系统的错误率和透射率进行优化。

表 I. 实验结果

	总计数	正确计数	错误计数	无响应事件	得分/阈值
理论	3029620	3020530	9090	6970380	-242972
试验1	2985866	2977742	8124	7014134	-232811.47
试验2	2984683	2976707	7976	7015317	-232767.09
试验3	2987501	2979473	8028	7012499	-232559.41
试验4	2980645	2972696	7949	7019355	-233114.21
试验5	2982920	2975003	7917	7017080	-232869.41

表 I 列出了各类事件的理论值和实验值，其中理论分数 cor-

响应阈值 Γ_0。结果显示，在全部五次实验试验中获得的得分均超过 Γ_0，从而实现了成功验证。验证系统的平均得分为 -232824.32 ± 199.80，显著高于 Γ_0，这表明通过最优选择相干态实现的系统具有稳健性。证明者的最大响应延迟为 247.8 纳秒，对应的验证范围为 74.3 米，达到了具有实际意义的水平。

IV. 结论

我们展示了一种同时基于相对论和量子原理的安全位置验证方法。给定两名坐标已知的验证者，只需几秒钟，便可在 75 米精度范围内验证远程证明者所声称的位置，而这得益于处于纳秒量级的整体系统延迟。该方案的安全性依赖于光速限制，以及经典资源与量子资源之间的非互易性。在布尔规模为 $n = 40$、重复频率为 2 MHz 的情况下，攻击者每秒必须分发不少于 1000 万对具有完美保真度的纠缠量子比特对，这一要求比当前能力高出两个数量级以上 [16–19]。这标志着量子位置验证已从理论概念发展为可实际部署的技术。

在现实生活中，位置是人类活动的基本要素。我们的方法为基于位置的认证场景提供了解决方案：只有当用户实际位于特定位置时，才允许执行某些操作。例如，仅允许在自动取款机附近进行交易、仅允许在办公室内访问数据库、仅允许在演出场馆内解锁门票，或仅允许在租赁汽车旁访问车辆。此外，该方法还可用于跟踪关键目标的位置，例如灾害救援中的人员、高价值物品，以及武器和弹药等军事资产。

致谢

我们诚挚感谢 Florian Speelman、Andreas Bluhm 和 Lloren¸c Escol`a-Farr`as，感谢他们参与了许多富有帮助的讨论。本研究得到国家自然科学基金委员会（项目编号：62571508、62425507、62531023、62271463、62301524、62371437）、安徽省自然科学基金（项目编号：2308085QF216）以及量子科学与技术国家科技重大专项（2021ZD0300701）的资助。

作者贡献

G.-J.F.-Y.、Y.-G.S.、C.Z. 和 S.W. 提出了这一构想并设计了本研究。Y.-G.S.、Z.-Q.Y.. 和 W.C. 构建了理论框架。G.-J.F.-Y.、C.Z.、D.-Y.H.、S.W. 和 S.-N.F. 制定了实验方法。G.-J.F.-Y.、Y.-L.W.、Y.-X.F. 和 W.-X.X. 设计并搭建了实验装置。G.-J.F.-Y.、Y.-L.W. 开展了实验并收集了数据。G.-J.F.-Y.、Y.-G.S. 和 S.W. 在所有作者的意见基础上撰写了稿件。S.W.、S.-N.F.、G.-C.G. 和 Z.-F.H. 负责监督本项目。所有作者均审阅并批准了稿件的最终版本。

利益冲突

作者声明不存在利益冲突。

数据可用性

所有支持　　本文的研究结果可应要求向通讯作者索取　　.

附录 A：方法

1. 相干态的安全得分

在量子通信实践中，使用弱相干态比使用单光子源方便得多，因为只需对激光脉冲进行衰减，就能轻松制备弱相干态。这种方法有两大优势：对发送方设备中的损耗不敏感，并且能够实现较高的重复频率。这对量子位置验证至关重要，因为该协议对损耗敏感，且要求重复超过 10^6轮。

为便于进行安全性分析，我们采用相位随机化弱相干态，它们是福克态的混合态。这类光源很容易获得，使用增益开关激光器即可自然实现相位随机化。接下来，我们推导弱相干态情况下的 Γ_0 ，并考虑有限轮次导致的统计涨落，从而建立严格的安全界。

相位随机化弱相干态是福克态的混合态，即 $\int_0^{2\pi} \left|\alpha e^{\mathrm{i}\theta}\right\rangle \left\langle \alpha e^{\mathrm{i}\theta}\right| = \sum_{i=1}^{\infty} e^{-|\alpha|^2} \frac{|\alpha|^i}{i!} \left|i\right\rangle \left\langle i\right|$，其中 $\left|\alpha e^{\mathrm{i}\theta}\right\rangle$ 是复振幅为 $\alpha e^{\mathrm{i}\theta}$的相干态，而 $|i\rangle$ 是 i光子福克态。因此，每一轮量子态制备都可分为三种类型：真空态、单光子态和多光子态。对于单光子态，可以采用参考文献[8] 中的相同方法。真空态不携带信息，因此对手无法攻击它们。对于多光子态，我们采用最坏情形，假设对手能够完美地攻击它们。于是， Γ_0 可以写为

$$\Gamma_0 = S_0^u + S_1^u + S_{2+}^u, \tag{A.1}$$

其中， S_0、 S_1、 S_{2+} 分别表示真空态、单光子态和多光子态对应的得分。上标 u 表示不诚实证明者能够达到的上界。接下来，我们分别分析这些上界。在以下分析中，我们使用概率不等式 5 次，每次的失败概率为 ϵ 。因此，协议的失败概率为 5ϵ。在实验中，我们设定 $\epsilon = 10^{-10}$，因此总失败概率为5×10^{-10}。这意味着，不诚实证明者以大于 5×10^{-10}的概率无法超过阈值 Γ_0。

a. Upper bound for vacuum states

对于真空态，对手可以选择声明无响应事件或响应事件。无响应事件计入 $n_\perp$。响应事件以 50% 的概率产生正确结果，因此计入 n_c或 n_I。令 N_0 为真空态轮次的总数， x 为对手声明响应的轮次数，其余 $N_0 - x$ 轮对应无响应事件。令 Y_i 表示对手在声明响应的第 i轮获得的得分。那么，对于所有真空态轮次，对手的总得分 S_0为

$$S_0 = \sum_{i=1}^{x} Y_i - (N_0 - x)\,\gamma_\perp. \tag{A.2}$$

对于任意给定的响应轮次，由于真空态不会泄露任何编码信息，每一轮都相互独立且服从相同分布，正确或错误响应的概率均为 50%。将 Y_i 归一化为伯努利随机变量 $\frac{Y_i+\gamma_I}{\gamma_C+\gamma_I}$，并对独立随机变量应用切尔诺夫界 [20] ，可得

$$\sum_{i=1}^{x} Y_i \le \frac{\gamma_c - \gamma_I}{2} x + \frac{\gamma_c + \gamma_I}{2} \left(\ln\frac{1}{\epsilon} + \sqrt{\ln^2\frac{1}{\epsilon} + 4(\ln\frac{1}{\epsilon})x} \right), \tag{A.3}$$

其中 ϵ 是失败概率。因此， S_0 的上界为

$$S_0 \le \frac{\gamma_c - \gamma_I}{2} x + \frac{\gamma_c + \gamma_I}{2} \left(\ln\frac{1}{\epsilon} + \sqrt{\ln^2\frac{1}{\epsilon} + 4(\ln\frac{1}{\epsilon})x} \right) - (N_0 - x)\,\gamma_\perp. \tag{A.4}$$

注意到 $\max_x(ax + b\sqrt{c + dx}) \to x = -\frac{c}{d} + \frac{b^2 d}{4a^2}$，得分 S_0在 $x = -\frac{1}{4}\ln\frac{1}{\epsilon} + \frac{1}{(\gamma_c+\gamma_I)^2}(\gamma_c - \gamma_I + 2\gamma_\perp)^2 \ln\frac{1}{\epsilon}$ 时达到其上界 S_0^u。因此， S_0^u 为

$$S_0 \le S_0^u = \frac{(7\gamma_c^2 + 4\gamma_c\gamma_\perp + 4\gamma_\perp^2 + 10\gamma_c\gamma_I + 12\gamma_\perp\gamma_I - \gamma_I^2)\ln\frac{1}{\epsilon}}{8(\gamma_c + 2\gamma_\perp - \gamma_I)} + (\gamma_c + \gamma_I)\sqrt{\frac{(\gamma_c + \gamma_I)^2 \ln^2\frac{1}{\epsilon}}{(\gamma_c + 2\gamma_\perp - \gamma_I)^2}} - \gamma_\perp N_0. \tag{A.5}$$

当 $\gamma_c + 2\gamma_\perp - \gamma_I < 0$ 时，可进一步简化为

$$S_0 \leq S_0^u = -\frac{(\gamma_c - 2\gamma_\perp + 3\gamma_I)^2 \ln \frac{1}{\epsilon}}{8(\gamma_c + 2\gamma_\perp - \gamma_I)} - \gamma_\perp N_0. \tag{A.6}$$

b. Upper bound for single-photon states

对于单光子态，我们采用与文献 [8], 相同的分析，并得到如下结果。对于一个单光子轮次，若假设攻击者以小于 ξ的概率向两个验证者输出不同响应，则可采用半定规划得到一组参数 $\{\gamma_c, \gamma_\perp, \gamma_I\}$，使得对手在这些参数下的期望得分不超过零。本文中的参数即采用该方法选取。为保证 ξ的合理选择，我们注意到，在本实验中，诚实证明者始终报告相同的响应。若攻击者在超过 N_ξ 个轮次中采用超过 ξ 的策略，则未发现不同响应事件的概率将小于$(1-\xi)^{N_\xi}$。因此，在失败概率为 ϵ的条件下，我们可以得出 $N_\xi \leq \ln\ \epsilon / \ln(1-\xi)$。因此，设 N_1为单光子轮次的数量，则有少于 $N_\xi \leq \ln \epsilon / \ln(1-\xi)$个轮次的攻击未被纳入文献 [8]的分析。并且有超过 $N_1 - N_\xi \leq \ln \epsilon / \ln(1-\xi)$个轮次，攻击者的期望得分小于0。

为了进行最坏情况分析，我们假设在 $N_\xi \leq \ln \epsilon / \ln(1-\xi)$ 轮次中，攻击者能够完美地攻击系统，也就是说，攻击总是给出正确的响应。相应的得分上界为 $\gamma_c N_\xi \leq \ln \epsilon / \ln(1-\xi)$。对于剩余的 $N_1 - N_\xi \leq \ln \epsilon / \ln(1-\xi)$ 轮次，参考文献 [8] 已证明顺序重复的结论，并且可以使用 Azuma不等式[21] 来界定得分上界。我们仍将 Azuma不等式的失败概率设为 ϵ，则得分上界为 $\sqrt{2 \ln\ \frac{1}{\epsilon}(N_1 - \overline{\ln \epsilon \ln(1-\xi)}}$。该公式适用于 $\max\{|\gamma_c|, |\gamma_\perp|, |\gamma_I|\} \leq 1$. 的条件

结合上述两种情况，得分上界为

$$S_1^u = \gamma_c \left\lceil \frac{\ln \epsilon}{\ln(1-\xi)} \right\rceil + \sqrt{2 \ln \frac{1}{\epsilon}(N_1 - \left\lceil \frac{\ln \epsilon}{\ln(1-\xi)} \right\rceil)}, \tag{A.7}$$

其中我们加上了上取整符号，因为轮次数应为整数。

c. Upper bound for multi-photon states

对于多光子态，最坏的情况是对手能够实施完美攻击，始终给出正确响应。因此，得分为

$$S_{2+}^u = N_{2+}\gamma_c, \tag{A.8}$$

其中， N_{2+} 是包含两个或更多光子的轮次数。

d. Γ_0 under statistical fluctuations

相位随机化弱相干态的光子数分布服从平均光子数为 $\mu = |\alpha|^2$ 的泊松分布。然而，给定总轮次为 N，真空态、单光子和多光子事件的实际数量（分别记为 N_0、 N_1和 N_{2+}）会受到统计涨落的影响。在计算 Γ_0 时，应将这些涨落考虑在内。

根据公式 A.6–A.8， N_0 贡献的得分为负，而 N_1 和 N_{2+} 贡献的得分为正。因此， Γ_0的上界为 $\Gamma_0^u = \Gamma_0$（N_0^l, N_1^u， N_{2+}^u），其中上标 u和 l分别表示上界和下界。这些界可以使用切尔诺夫界获得，

$$N_1 \leq N_1^u = Ne^{-\mu}\mu + \frac{1}{2}\left(\ln \frac{1}{\epsilon} + \sqrt{\ln^2 \frac{1}{\epsilon} + 8(\ln \frac{1}{\epsilon})Ne^{-\mu}\mu}\right) \tag{A.9}$$

$$N_{2+} \leq N_{2+}^u = N(1 - e^{-\mu} - e^{-\mu}\mu) + \frac{1}{2}\left(\ln \frac{1}{\epsilon} + \sqrt{\ln^2 \frac{1}{\epsilon} + 8(\ln \frac{1}{\epsilon})N(1 - e^{-\mu} - e^{-\mu}\mu)}\right) \tag{A.10}$$

$$N_0 \geq N_0^l = N - N_1^u - N_{2+}^u \tag{A.11}$$

e. Experimental optimization

在实践中，确保诚实证明者即使其测量系统存在潜在的失准，也能够通过验证十分重要。令 p_e 表示失准误差，η 表示透射率。问题归结为寻找一个使 $\Gamma - \Gamma_0$最大化的最优平均光子数 μ ，其中诚实证明者的期望得分为

$$\Gamma = N\left(\gamma_c(1-e^{-\eta\mu})(1-p_e) - \gamma_\perp e^{-\eta\mu} - \gamma_I(1-e^{-\eta\mu})p_e\right). \tag{A.12}$$

基于参考文献[8]中当 $\xi = 0.001$时通过半定规划得到的归一化参数 $\gamma_c = 0.04275$、 $\gamma_\perp = 0.05019$和 $\gamma_I = 1$ ，以及实验参数 $p_e = 0.3\%$和 $\eta = 70\%$，针对 $N = 10^7$将平均光子数优化为 $\mu = 0.52$ 。在这种情况下， Γ_0 计算为 -242972。

2. 高保真量子态制备

偏振态制备的原理是将初始偏振态分成两个分量，通过调整其中一个分量的相位引入相对相位，再将两个分量正交地重新组合，从而生成态 $|H\rangle + e^{i\phi}|V\rangle$。这里我们采用萨格纳克结构。初始偏振态分成两部分后，分别沿顺时针和逆时针方向在萨格纳克环中传播。设置在偏离中心位置的相位调制器仅对一个传播方向的相位进行选择性调制，从而引入相对相位差。

这种结构的主要优势在于，顺时针和逆时针脉冲通过同一根光纤，因此其相对相位不会因路径长度差异而漂移。这带来了很高的稳定性，有利于高保真度量子态制备。然而，基于分束器的传统萨格纳克方案无法用于偏振态制备，因为它们不支持正交重组。若使用偏振分束器，则需要通过偏振控制器将初始偏振旋转 45° ，这会损害稳定性。

为解决这一局限，我们设计了一种微组装旋转环形分束器，将旋转器、环形器和偏振分束器集成在一起。微组装工艺能够实现精确的偏振旋转和准确的 50:50 分束，而加入环形器则可抑制与萨格纳克环相关的反射。因此，该设计实现了高保真度偏振态制备，测得的保真度为 99.73%。相应的低错误率使该协议能够容忍更高的损耗，并使证明者获得更高的得分，这是系统成功运行的关键因素之一。

3. 大规模快速布尔函数

为实现大规模、快速的布尔函数计算，我们采用由定制现场可编程门阵列和基于DDR的电路实现的查找表方法。快速计算通常依赖逻辑门，但由于逻辑门在资源消耗和延迟方面都不切实际，因此我们采用查找表方法。一方面，布尔函数的状态空间为 2^{2^n}。假设每个逻辑门可以表示 m 个状态，则所需逻辑门数量为$\log_m(2^{2^n})$，该数量会随 n 呈指数级增长，远远超出现有现场可编程门阵列的容量。另一方面，逻辑门不可避免地会引入电路延迟。当延迟累积于指数级数量的逻辑门时，最终延迟将变得难以接受。查找表方法将可扩展性挑战转化为存储空间问题。我们使用总容量为1Tb $= 2^{40}$bit的DDR芯片来实现布尔函数，对应于 $n = 40$。现场可编程门阵列接收到40位后，将其用作地址，以访问DDR存储器中存储的相应比特，并将结果作为基选择信号输出。通过向DDR写入不同的随机比特模式，每种配置都对应一个不同的布尔函数，从而支持全部 $2^{2^{40}}$ 种可能的布尔函数。由于现场可编程门阵列的固有延迟以及DDR存储器的随机访问性能，该部分引入的延迟约为117.3 ns。

4. 近光速信道

基信息和测量结果都是经典比特，可以用相同的方法传输。主要区别在于，基信息包含 $n/2$ 比特，而测量结果只有一位。为了实现经典信息的快速传输，我们采用了一种简单高效的开关键控方案，分别用强光和弱光表示 1 和 0。另一个挑战是，如果每比特以 τ 的周期时长传输，发送 $n/2$ 比特将引入 $(n/2-1)\tau$ 的延迟，这不利于

具有较大 n 的布尔函数。我们采用密集波分复用，使用不同波长的独立激光器同时发送特定比特。这样即可并行传输 $n/2$ 比特，消除对 n 的延迟依赖。光信号由高速 PIN光电二极管探测，并直接馈入后续电路进行判别。信号通过信道传输也需要时间。为尽量减小这一延迟，我们使用内芯充满空气的反谐振空芯光纤，使光能够以接近真空中的光速传播。再加上较低的色散，额外延迟可限制在约 22 ns。

5. 低时延低损耗量子测量

量子态测量中的损耗主要源于基选择装置的插入损耗和光子探测器的探测效率。为减小这些损耗，我们采用低损耗光开关和超导纳米线单光子探测器。此外，还采用保偏熔接以降低连接器损耗。因此，整体插入损耗约为 0.96 dB，主要来自光开关的插入损耗（约 0.6 dB）。探测效率达到 90%，使传输效率达到 72%。

然而，这种配置带来了延迟方面的挑战。高速、低损耗光开关需要超过 400 V 的驱动电压，无法直接与布尔函数电路的数字输出接口。此外，探测器产生的微弱点击信号无法直接远距离传输至验证者。信号转换不可避免地会引入延迟。为解决这一问题，我们开发了一种氮化镓高压驱动器，可在 50 ns 内将数字信号转换为高压信号，从而使光开关能够快速响应。同时，我们为探测器设计了集成信号处理单元，执行放大、判别和开关键控编码，以缩短探测信号的回传延迟。这些措施显著降低了延迟，同时不影响低损耗和高重复频率。

---

[1] N. Chandran、V. Goyal、R. Moriarty 和 R. Ostrovsky，《基于位置的密码学》，载于 *Advances in Cryptology - CRYPTO 2009* 2009 391 407，S. Halevi 编（Springer Berlin Heidelberg，柏林，海德堡，）第 – 页。[2] R. A. Malaney，《使用量子纠缠的位置相关通信》，《物理评论A》81，042319（2010）。[3] W. Y. Kon、I. W. Primaatmaja、K. Chakraborty 和 C. Lim，《使用基于位置的凭证进行量子安全密钥交换》（2025），arXiv:2506.03549 [量子信息]。[4] M. Bozzio、C. Cr´epeau、P. Wallden 和 P. Walther，《超越密钥分发的量子密码学：理论与实验》，《现代物理评论》97，045006（2025）。[5] S. Brands 和 D. Chaum，《距离界定协议》，载于 *Advances in Cryptology — EUROCRYPT '93*，T. Helle-seth 编（Springer Berlin Heidelberg，柏林，海德堡，1994），第 344–359 页。[6] C. H. Bennett 和 G. Brassard，《量子密码学：公钥分发与抛硬币》，载于 *International Conference on Computers Systems and Signal Processing* 1984 175 179，（IEEE，班加罗尔，印度，）第 – 页。[7] A. Bluhm、M. Christandl 和 F. Speelman，《一种能够抵御多量子比特攻击的单量子比特位置验证协议》，《自然·物理》18，623（2022）。[8] L. Escol`a-Farr`as 和 F. Speelman，《能够抵御纠缠攻击者的单量子比特容损量子位置验证协议》，《物理评论快报》131，140802（2023）。[9] R. Allerstorfer、A. Bluhm、H. Buhrman、M. Christandl、L. m. c. Escol`a-Farr`as、F. Speelman 和 P. Verduyn Lunel，《使现有量子位置验证协议能够抵御任意传输损耗》，《物理评论快报》135，260801（2025）。[10] Y. Wang、G. Smith 和 A. May，《安全量子测距》，《物理评论快报》135，260802（2025）。[11] A. Kent、W. J. Munro 和 T. P. Spiller，《量子标记：通过量子信息和相对论信号约束认证位置》，《物理评论A》84，012326（2011）。[12] A. Kent，《针对包含秘密经典数据的标签的量子标记》，《物理评论A》84，022335（2011）。[13] M. Tomamichel、S. Fehr、J. Kaniewski 和 S. Wehner，《纠缠单配博弈及其在设备无关量子密码学中的应用》，《新物理学杂志》15，103002（2013）。[14] K. Kanneworff、M. Poortvliet、D. Bouwmeester、R. Allerstorfer、P. V. Lunel、F. Speelman、H. Buhrman、P. Steindl 和 W. L¨offler，《使用单光子进行量子位置验证的实验演示》，《量子科学与技术》10，045004（2025）。[15] L. Vandenberghe 和 S. Boyd，《半定规划》，《SIAM评论》38，49（1996），https://doi.org/10.1137/1038003。[16] S. Wengerowsky、S. K. Joshi、F. Steinlechner、H. H¨ubel 和 R. Ursin，《基于纠缠的波分复用量子通信网络》，《自然》564，225（2018）。[17] X. Liu、X. Yao、H. Wang、H. Li、Z. Wang、L. You、Y. Huang 和 W. Zhang，《基于能时纠缠的色散光学量子密钥分发：通过 20 km 光纤传输》，《应用物理快报》114，141104（2019）。[18] S. P. Neumann、A. Buchner、L. Bulla、M. Bohmann 和 R. Ursin，《通过跨国 248 km 光纤链路进行连续纠缠分发》，《自然·通讯》13，6134（2022）。

[19] S.-C. Zhuang、B. Li、M.-Y. Zheng、Y.-X. Zeng、H.-N. Wu、G.-B. Li、Q. Yao、X.-P. Xie、Y.-H. Li、H. Qin、L.-X. You、F. Xu、J. Yin、Y. Cao、Q. Zhang、C.-Z. Peng 和 J.-W. Pan，《基于超亮纠缠的量子密钥分发：通过 404公里光纤》，《物理评论快报》**134**，230801（2025）。[20] H. Chernoff，《基于观测值之和的假设检验的渐近效率度量》，《数学统计年刊》**23**，493（1952）。[21] K. Azuma，《某些相关随机变量的加权和》，《东北数学杂志》第二辑**19**，357（1967）。