arXiv:2603.07930v1 [quant-ph] 9 Mar 2026

量子　　基于贝尔不等式的量子信息优势　　es

Rahul Jain新加坡国立大学
计算机科学系量子技术中心
dcsrahul@nus.edu.sg

Srijita Kundu
鸿海（富士康）研究院量子计算研究中心 srijita.kundu@foxconn.com.sg

摘要

近期，Kretschmer 等人 [KGD+25] 展示了他们提出的量子信息优势协议的实验验证。

我们提出了另一种方案，其依据是从并行重复 CHSH 博弈中导出的一个关系。我们的存储度量基于一种信息度量，不同于 [KGD+25]，后者计算的是量子比特的数量。我们的方案具有高效的验证者和抗噪量子证明者；可以说，与 [KGD+25]相比，效率高得多。

1 引言

量子信息科学中的一个重要研究方向，是展示量子在计算任务中的优势，即证明某些问题可以用比同类经典资源更少的量子资源来解决。

量子优势最早的例子之一是贝尔非定域性。在非局域博弈中，空间上彼此分离的参与方 Alice 和 Bob 会分别获得各自私有的输入，并需要给出满足特定条件的输出。参与方可以采用共享随机性的经典策略，也可以采用共享纠缠的量子策略来赢得此类博弈。在某些非局域博弈中，量子策略能够取得远高于经典策略的获胜概率，这种现象称为贝尔不等式违背。

然而，贝尔不等式违背背后的实际计算任务并非难以用经典资源完成——其难点仅在于各方彼此分离，无法通信（因而无法得知对方的输入）。后来的量子优势演示则聚焦于这样的任务：对经典计算机而言计算难度很高，但即便使用近期或当前已有的量子设备，也能轻松完成。

在展示量子设备在计算困难任务中的量子优势方面，大多数研究都采用了基于采样的方法：证明量子设备能够高效地从某个分布（本质上是量子电路的输出分布）中进行采样，而经典设备却无法高效地从该分布中采样 [AAB+19，WBC+21，ZCC+22，MLA+22，MVM+24，GFZ+25，DHL+25]。然而，我们实际上无法证明这些采样任务对经典设备而言是困难的。虽然有一些复杂性理论证据 [AA13，AG20]表明这些任务很困难，但这里所声称的量子优势最终仍依赖于尚未得到证明的复杂性理论假设。

Kretschmer 等人的一项近期研究 [KGD+25] 旨在通过展示一种能够无条件地证明量子优势的采样任务，来缓解这一局面。关键在于，这种量子优势并非体现在运行时间上，而是体现在内存方面。作者表明，有一项计算任务，量子设备只需少量（12 个）量子比特内存即可解决，而经典设备则可证明需要多得多的比特内存（62 至 382 个）才能解决。他们将这一成果称为量子信息优势。

对 [KGD+25] 的构造基于通信复杂度设定中的一个问题。在通信复杂度设定中，与非局域博弈设定类似，空间上彼此分离的两方 Alice 和 Bob 获得私有输入，并且必须通过经典方式或量子方式进行通信，以计算这些输入上的一个关系（目标是尽可能少地进行通信）。此前已经证明了许多问题在量子通信代价与经典通信代价之间存在分离。工作 [KGD+25] 将一个通信复杂度分离（在双设备设定中）转化为单设备设定中经典内存代价与量子内存代价之间的分离。

更具体地说， [KGD+25] 考虑一个将单向经典通信复杂度与量子通信复杂度区分开的任务，其中存在一项限制：Alice 只能向 Bob 发送一条经典消息或量子消息。在其关于量子信息优势的设定中，他们不再将 Alice 和 Bob 视为空间上彼此分离的两方，而是将其重新表述为同一设备在时间上分离的两个阶段。该设备在通信问题的时刻 x 接收 Alice 的输入 t_0，，并在稍后的时刻 y 接收 Bob 的输入 t_1。关注的量是：为了在 t_0 和 t_1 之间存储信息，并计算 x 和 y上的相关关系，该设备需要多少经典内存或量子内存。很容易看出，这里的内存需求恰好等于在通信复杂度设定中 Alice 需要就其输入 x 向 Bob 进行通信的信息量，因此可以利用通信复杂度中经典与量子之间的分离结果。

1.1 我们的方案

我们提出了一个不同的问题，可用于展示量子信息优势，并采用了不同于 [KGD+25] 的内存度量。与 [KGD+25] 不同，我们将从时间 t_0 到 t_1，必须传递的关于输入 x 的信息，作为我们的度量，并用平滑最大互信息 $I^{\delta}_{\max}(X:M)$ 对其进行量化，其中 M 是证明者在 t_0 和 t_1 之间维护的内存寄存器。这与 X 和 M 之间更标准的互信息 I(X : M) 有关；关于这两个量的定义，请参见第 2 节。我们认为，这是量子信息优势的一种有效度量，因为要将内存中的量子比特维持在能够保留输入信息的量子态，比将其维持在任意量子态都更加困难。我们正式定义如下的量子信息优势证明。

定义 1（量子信息优势证明）。令 c（n），s（n） 为 n 的多项式函数，并令γ_0 为 $[0,1]$ 中的一个常数。一个（c， s， γ_0） 抗噪声量子信息优势证明，是验证者与证明者之间的交互式协议，其中验证者是一个 *PPT*（概率多项式时间）算法，而证明者可以是 *PPT* 或 *QPT*（量子多项式时间）算法。在该协议中，验证者测试证明者是否能够计算关系 R（n） $\subseteq$（$\mathcal{X}$（n） $\times\mathcal{Y}$（n）） $\times$（$\mathcal{A}$（n） $\times\mathcal{B}$（n），其中 n 是输入参数。

1. 验证者和证明者都将 1^n作为输入。*2.* 在时间 t_0，，验证者采样 $x \in \mathcal{X}$并发送给证明者。令 X 表示与 x 对应的随机变量。*3.* 证明者回复一个 $\in \mathcal{A}$。*4.* 随后，在时间 t_1，，验证者采样 $y \in \mathcal{Y}$ 并发送给证明者。*5.* 证明者回复 $b \in \mathcal{B}$。*6.* 如果 $(x,y,a,b) \in R$，则验证者接受。

我们有以下要求。

- 完备性：存在一个QPT证明者，能使验证者以概率 $1-\mathrm{negl}(n)$接受。证明者在t_0 与t_1 之间维护的量子存储寄存器M满足$\mathsf{I}^{\mathrm{negl}(n)\max}_{\max}(X:M) \leq c(n)$。
- 噪声鲁棒性：存在一个噪声阈值 $\gamma_0 \in (0,1)$，使得若QPT证明者针对 $\gamma \leq \gamma_0$在 γ含噪设备上运行，验证者仍以概率 $1-\mathrm{negl}(n)$接受。
- 可靠性：任何经典证明者（无论是否在多项式时间内运行），若其从t_0 到t_1传输一个满足$\mathsf{I}^{\mathrm{negl}(n)\max}_{\max}(X:M) \leq s(n)$ 的经典内存寄存器M，将使验证者以$\mathrm{negl}(n)$的概率接受。

在上述定义中，我们有意不指定噪声模型，因为它属于实际考量，而在不同硬件上实现的不同协议会具有不同类型的噪声。尽管如此，由于量子协议的任何实现都会存在噪声，噪声鲁棒性是一种理想性质；我们的意图是，在本定义中针对每一类协议使用相应类型的噪声模型。

关于量子信息优势定义的结果，正式表述如下，见定理1。

定理1。 存在一种$(0,\Omega(n),0.01)$ 量子信息优势抗噪声证明。此外，该协议满足$\mathsf{I}(X:M) = \mathsf{I}^0_{\max}(X:M) = 0$。

令 $\delta := 2^{-n/((\ln 2)\times 10^4)}$。任何经典存储器满足以下条件的经典证明者

$$\mathsf{I}^{\delta}_{\max}(X:M) \leq \frac{4n}{(\ln 2)\times 10^4} - \log\log\frac{1}{\delta} - 19,$$

将使验证者以至多 $72\delta^2$的概率接受。

协议描述。 我们的量子信息优势证明协议基于贝尔不等式违背，具体而言，是 CHSH 游戏中的贝尔不等式违背。通过要求 Alice 和 Bob 生成输出，使得根据非局域游戏获胜条件计算出的正确输出比例接近该游戏的量子获胜概率，可以将贝尔不等式违背转化为关系问题中的通信分离。这样的非局域游戏称为阈值并行重复游戏。我们考虑t-取自-n 阈值并行重复游戏 $\mathrm{CHSH}^{t/n}$，其输入集和输出集均为n位比特串。该游戏的获胜条件是字符串$x_1\ldots x_n$,$y_1\ldots y_n$, $a_1\ldots a_n$,$b_1\ldots b_n$ 满足

$$|\{i : a_i \oplus b_i = x_i \cdot y_i\}| \geq t,$$

具有 $t = 0.83n$。由于基于非局域游戏，与 [KGD+25]相比，我们的方案的优势在于所需的量子态和测量远没有那么复杂。该协议如图1所示。

噪声模型。我们现在阐明在本设定中噪声的含义。如果一个非局域游戏的量子值为 ω^*，则我们将能够达到值 $\omega^* - \gamma$， γ-含噪设备的量子设备称为含噪设备。我们并不试图对导致该值的设备内部工作机制进行建模——这与许多贝尔场景中噪声的建模方式一致，例如参见 [NDN+22，ZvLR+22]。每个单量子比特门中都存在一定程度的恒定噪声，从而导致该值为 γ。

具体参数。

1. 设 $n = 1$。1697×10^4 且平滑参数 $\delta = \frac{1}{12}$（此处 n 和 δ 的关系与定理1中的关系不同，参见定理4）。

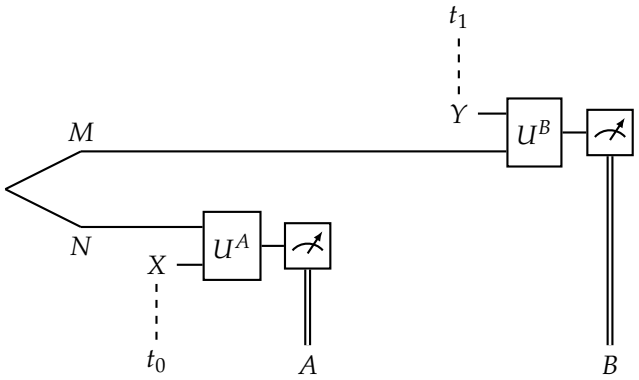


图1：我们证明量子信息优势协议时，量子证明者所实现的电路。酉算子U^A 和U^B 分别是 Alice 和 Bob 在 CHSH^n 博弈中最优量子策略所用的酉算子。寄存器M 是量子存储器。

2. 在我们的协议中，量子证明者的成功概率（其中 $\mathrm{I}(X:M) = \mathrm{I}^0_{\max}(X:M) = 0$) 至少为 $1 - e^{-2n/10^4} = 0.903$（参见定理 1）. 3. 拥有经典内存 $\mathrm{I}^{1/12}_{\max}(X:M) \leq 100$ 的经典证明者，其成功概率至多为 $72\delta^2 = \frac{1}{2^\circ}$

–

因此，要实现 0 对 100 的量子-经典分离，我们需要能够并行执行 CHSH 获胜策略，作用于 1.1697×10^4 个副本，并且噪声为 $\gamma = 0.01$。

1.2 与先前工作的比较

现在，我们将更详细地比较我们方案与 [KGD+25] 的工作。在 [KGD+25] 中用于证明量子信息优势的任务，是分布式线性交叉熵基准测试的一种变体。在该任务中，证明者在时刻t_0, 获得一个 Haar 随机的 m 量子比特量子态 $|\psi\rangle$ 的经典描述；在时刻t_1，他们获得一个 Haar 随机酉算子U的描述。要求输出一个 m位字符串$z_{\psi,U}$，使得

$$\mathop{\mathbb{E}}_{\psi,U}\left[\left|\langle z_{\psi,U}|\, U\,|\psi\rangle\right|^2\right] \geq \frac{1+\varepsilon}{2^m}.$$

~请注意，一个m量子比特的 Haar 随机量子态需要$O(2^m)$ 比特来描述，因此这里的输入参数是 $n = 2^m$。[KGD+25] 使用 ε 来刻画其协议的正确性：要达到 $\varepsilon = 0$ 很容易。他们证明，使用 m 量子比特量子存储器的量子证明者可以达到 $\varepsilon = 1$，而使用 s 比特经典存储器的经典证明者则满足

$$\varepsilon = O\left(\max\left\{\sqrt{\frac{s}{2^m}}, \frac{sm}{2^m}\right\}\right).$$

这里对经典证明者和量子证明者而言， ε 的定义本质上都是平均情形。我们还注意到，时刻t_1 的酉算子也可以取自若干较小的酉算子集合，这些酉算子同样能够高效实现，例如 2-设计或单量子比特 Clifford 门的乘积；他们证明，当U 取自这些集合时， ε 也有类似的上界。

我们注意到 我们提出的方案与文献 [KGD+25中的方案有以下几点比较].

• **关系：** 我们使用的关系有两个输出，a 和b。 [KGD+25]中考虑的采样问题有两个输入x 和y，与我们相同，但只有一个输出，并且必须在给定y 后的t1时产生。

对我们而言，重要的是在t_0 时给定x 后产生输出a ，而只有输出b 稍后才会产生。不过，我们并不认为方案的这一特点有多大缺陷，因为与只有一个输出相比，拥有两个输出并非特别不自然。

- **存储度量：**KGD 中使用的信息度量 [KGD+25] 是从$t0$ 到$t1$ 必须传递的量子比特或比特总数。

  对我们而言，它是关于输入x 的信息度量，以比特或量子比特表示。值得注意的是，在经典和量子情形下，从t_0 到t_1 分别需要传递的比特或量子比特数量，对我们而言都是 $\Omega(n)$ ；区别仅在于量子情形下，量子比特不携带关于x的信息。

- **完备性和可靠性错误：**我们所采用的完备性和可靠性错误概念要标准得多。

  据我们理解， [KGD+25] 中的协议并未明确表述为具有标准完备性和可靠性错误概念的交互式证明。这是因为他们研究的是采样问题，验证者不会根据某个条件接受或拒绝，而是计算KGD ε。

- **验证者的效率：**我们的验证者可以直接在$O(n)$ 时间内检查，对于每个输入和输出，CHSH 获胜条件是否在 0.83 比例的i中成立。
  在 [KGD+25] 中，对于给定的 U，经典验证者可以在 poly(2^m) 时间内计算 $|\langle z|U\ |\psi\rangle|^2$ 和 $|\psi\rangle$ ，这对于 $n = 2^m$ 来说是高效的。但据我们所知，验证者必须多次运行线性交叉熵协议，并据此估算 ε 。这要求验证者在 t_0 发送多个 $|\psi\rangle$-，并在 t_1 发送多个 U-。KGD [中似乎没有明确说明需要发送多少个 $|\psi\rangle$- 和 U-（其数量取决于 ε）。此外，也不清楚针对这种并行重复协议的经典存储器下界是否成立。

- **量子证明者的效率：**我们的态制备和测量过程比 [KGD+25] 中的要简单得多。我们只需制备 EPR 对，并使用 4 种单量子比特量子门（对应于 CHSH 非局域游戏中的测量），这些操作应该能够在现有量子设备上实现。

  [KGD+25] 可以使用 2-设计或随机Clifford门来实现U，但实际上他们确实需要制备一个m量子比特的 Haar 随机量子态。精确的 Haar 随机量子态需要 $\Omega(2^m)$ 个量子门和 $\Omega(2^m/m)$ 深度才能制备，在他们的实际实现中可能难以实现。因此，他们在实际实现中改用砖墙式拟设，其电路规模和深度都小得多。然而，据我们所知，他们的经典信息下界实际上并不适用于这种拟设，因为这种拟设可以用 poly(m) 大小的描述来表示。

- **噪声鲁棒性：** [KGD+25] 没有对其量子协议进行渐近抗噪性分析。如果每个量子门都有恒定误差，那么他们的砖墙式拟设（它没有经典下界）或许仍能得到非平凡的输出；但他们实际的下界要求使用 Haar 随机态。如果制备 Haar 随机态所需的 $\Omega(2_n)$ 个量子门都以恒定误差实现，我们怀疑他们的量子协议将无法达到非平凡的 ε 值。

  相比之下，我们的协议具有鲁棒性，即使每个量子门都存在恒定噪声，单拷贝 CHSH 获胜概率仍可达到 0.84。

- **量子存储器的具体数量：**在我们的方案中，要实现量子信息优势为 0 与 100，所需的量子比特实际数量约为 10_4。不过，使用现有技术对 10_4 个 EPR 对仅进行 CHSH 测量是可行的，而且在展示贝尔不等式违背和设备无关密码学的背景下，已经以我们要求的错误率完成过此类实验 [NDN+22，ZvLR+22]。不过，我们注意到，这些设备无关协议中的测量是依次进行的，并且需要在两组设备之间保持一定的空间分离。我们的测量需要并行进行，但不需要这种空间分离。

正如我们之前所述，在 [KGD+25] 的协议中，量子证明者所需的确切内存大小尚不清楚，因为没有说明需要发送多少次 $(|\psi\rangle, U)$。他们证明，单次重复只需要 12 个量子比特。

2 预备知识

2.1 尾界

事实 1 (Chernoff界)。 设 $X_1,\ldots,X_n$ 为独立同分布的伯努利变量，且 $\mathbb{E}[X_i]=\delta$。则，

$$\Pr\left[\sum_{i=1}^{n} X_i \geq \gamma n\right] \leq e^{-2(\gamma-\delta)^2 n};$$
$$\Pr\left[\sum_{i=1}^{n} X_i \leq \gamma n\right] \leq e^{-2(\gamma-\delta)^2 n}.$$

事实 2 (广义切尔诺夫界， [PS97])。 设 $X_1,\ldots,X_n$ 为布尔随机变量，满足存在某个$\delta \in [0,1]$，使得对每个子集 $S \subseteq [n], \Pr[\wedge_{i\in S} X_i] \leq \delta^{|S|}$。那么，对任意 $\gamma \in [\delta,1]$，有，

$$\Pr\left[\sum_{i=1}^{n} X_i \geq \gamma n\right] \leq e^{-2(\gamma-\delta)^2 n}.$$

2.2 信息度量

设 XY 是两个随机变量，其联合分布为p_{XY}。我们用$p^{Y|x}$ 表示在Y 条件下$X = x$的分布。

定义 2 （平滑最大信息）。 对于 $\gamma \in [0,1]$，量子态 ρ_{XY} 中寄存器 X 和 Y 之间的 γ-平滑最大互信息$\mathrm{I}_{\max}$定义为

$$\mathrm{I}^{\gamma}_{\max}(X:Y)_\rho = \inf\left\{c : \rho'_{XY} \preceq 2^c \rho_X \otimes \rho_Y, \frac{1}{2}\|\rho'_{XY} - \rho_{XY}\|_1 \leq \gamma\right\}.$$

当 X 和 Y 都是经典随机变量，且它们的联合经典分布为 p_{XY} 时，我们省略记号中的下标，此时该量可化简为

$$\mathrm{I}^{\gamma}_{\max}(X:Y) = \inf\left\{c : p'_{XY}(xy) \leq 2^c p(x)p(y)\,\forall x,y, \frac{1}{2}\|p'_{XY} - p_{XY}\|_1 \leq \gamma\right\}.$$

定义 3 （经典平滑谱最大信息， [ABJT20]）。 对于经典随机变量 XY，它们之间的 γ-平滑谱最大互信息定义为

$$\mathrm{I}^{\gamma}_{\mathrm{s}}(X:Y) = \inf\left\{c : \Pr_{(x,y)\sim p_{XY}}\left[\frac{p_{Y|x}(y)}{p_Y(y)} > 2^c\right] \leq \gamma\right\}.$$

对于 $\mathrm{I}^{\gamma}_{\max}$ 和 $\mathrm{I}^{\gamma}_{\mathrm{s}}$，不难看出它们都是 γ 的增函数。我们简单地用 $\mathrm{I}_{\max}(X:Y)_\rho$ 和 $\mathrm{I}_{\mathrm{s}}(X:Y)$ 分别表示 $\mathrm{I}^{0}_{\max}(X:Y)_\rho$ 和 $\mathrm{I}^{0}_{\mathrm{s}}(X:Y)$。

此外，如果两个随机变量 X 和Y 不相关，那么 $\mathrm{I}_{\max}(X:Y) = \mathrm{I}_{\mathrm{s}}(Y:X) = 0$。

对于经典变量，可以证明这两个最大互信息量满足以下关系。

事实 3([ABJT20], 定理1 和 定理 2)。 对于 $\gamma \leq 1/\sqrt{12}$,

$$I_s^{18\gamma^2}(X:Y) \leq I_{\max}^{\gamma}(X:Y) + \log\left(\frac{8+\gamma^2}{\gamma^2}\right) + 2.$$

两个变量或量子寄存器之间更标准的信息度量是互信息，定义如下。

定义 4。 量子态 ρ_{XY} 中寄存器 X 和 Y 之间的互信息定义为

$$I(X:Y)_\rho = H(X)_\rho + H(Y)_\rho - H(XY)_\rho,$$

其中$H(A)_\rho = -\operatorname{Tr}(\rho_A \log \rho_A)$。对于经典随机变量 X，$H(X)$ 可化为 $\sum_x p_X(x)\log(1/p_X(x))$。

我们始终具有 $I(X:Y)_\rho \leq I_{\max}(X:Y)_\rho$，特别是如果$I_{\max}(X:Y) = 0$，那么 $I(X:Y) = 0$.

2.3 非局域博弈

双人非局域博弈G 描述为$(p, \mathcal{X}\times\mathcal{Y}, \mathcal{A}\times\mathcal{B}, V)$，其中$p$ 是输入集上的概率分布，$\mathcal{X}\times\mathcal{Y}$, $\mathcal{A}\times\mathcal{B}$ 是输出集，$V: \mathcal{X}\times\mathcal{Y}\times\mathcal{A}\times\mathcal{B} \to \{0,1\}$ 是一个谓词。游戏按如下方式进行：裁判按照p选择输入(x,y)，将x 发送给Alice，将y 发送给Bob。在G的经典策略中，Alice和Bob向裁判返回输出a 和b，它们分别只是x 和y 的函数 [1]在量子策略中，Alice和Bob可以共享纠缠；他们根据各自的输入，对纠缠态各自一半进行测量，并将输出(a,b) 返回给裁判。当且仅当$V(x,y,a,b) = 1$时，裁判接受，Alice和Bob赢得游戏。

定义 5. 游戏 $G = (p, \mathcal{X}\times\mathcal{Y}, \mathcal{A}\times\mathcal{B}, V)$的经典值，记作 $\omega(G)$，是指在所有针对 G 的经典策略中，*Alice* 和 *Bob* 的获胜概率按分布 p 取平均后的最大值。

游戏 G 的量子值，记作 $\omega^*(G)$，是指在所有针对 G 的量子策略中，*Alice* 和 *Bob* 的获胜概率按分布 q 取平均，并考虑策略中固有的随机性后得到的最大值。

对于任意游戏 G，我们可以定义它的并行重复版本和阈值并行重复版本，如下所示。

- 在 G 的标准并行重复版本中，记作 Gn，Alice 和 Bob 根据乘积输入分布 $p^{\otimes n}$，从 $\mathcal{X}^n \times \mathcal{Y}^n$ 中分别获得输入 $x_1, \ldots, x_n$ 和 $y_1 \ldots y_n$，并必须分别输出 $a_1 \ldots a_n$ 和 $b_1 \ldots b_n$，使得对所有 $i \in [n]$, $V(x_i, y_i, a_i, b_i)$ 均成立。

- 在t取n 阈值版本的G中，记作$G_{t/n}$，Alice 和 Bob 获得与G_n中相同的输入，并且必须从 $\mathcal{A}^n \times \mathcal{B}^n$中给出输出，使其输入和输出满足

$$|\{i \in [n] : V(x_i, y_i, a_i, b_i) = 1\}| \geq t.$$

我们尤其关注 CHSH 游戏。在单个 CHSH 游戏中，输入和输出都是比特，并且必须满足$a \oplus b = x \cdot y$。单次 CHSH 的经典值为 34，而量子值为 $\cos^2(\pi/8) \approx 0.85$。

并行重复游戏的最优策略并不总是将单次游戏n 的最优策略执行多次。因此，并行重复游戏的精确值往往未知。不过，对于 CHSH 游戏，其并行重复后的经典值和量子值实际上已有很好的刻画。

事实 4 ([CSUU08]). n 次 *CHSH* 游戏的量子值为

$$\omega^*(\mathrm{CHSH}^n) = \cos^{2n}\left(\frac{\pi}{8}\right).$$

[1]原则上，他们也可以共享随机性，并生成既取决于各自输入又取决于共享随机性的输出，但可以证明这并没有帮助。

CHSH 的经典值的以下上界^n 是 Ambainis 在 DS [之后14]提出的一项未发表结果。

事实 5（[DS14],另见 [Aar14]）。 n 份 *CHSH* 游戏的经典值满足

$$\omega(\mathrm{CHSH}^n) \leq \left(\frac{1+\sqrt{5}}{4}\right)^n \approx (0.81)^n.$$

此外，当 n 足够大时，不等式取等号。

3 任务：实现量子信息优势

在本节中，我们证明定理1，其表述如下。

定理1。 存在一个（0， Ω（n），0.01）抗噪声量子信息优势证明。此外，该协议满足I（X： M） $=\mathrm{I}^0_{\max}$（X： M） $=0$。

令 δ： $=2^{-}n/$（（ln2）$\times 10^4$）。任何经典证明者，只要其经典存储器满足

$$\mathrm{I}^{\delta}_{\max}(X:M) \leq \frac{4n}{(\ln 2)\times 10^4} - \log\log\frac{1}{\delta} - 19,$$

将使验证者以至多 $72\delta^2$的概率接受。

定理证明 *1.* 如前所述，我们将 $\mathrm{CHSH}^{t/n}$ 作为量子信息优势协议证明中的关系。使用该关系的协议可描述如下：

1. 验证者和证明者获得 1^n。2. 在时间t_0, ，验证者均匀采样$x \in \{0,1\}^n$ 并发送给证明者。3. 证明者回复$a \in \{0,1\}^n$，验证者将其存储起来。4. 在时间t_1, ，验证者均匀采样$y \in \{0,1\}^n$ 并发送给证明者。5. 证明者回复$b \in \{0,1\}^n$。6. 若x、y、a、b 满足

$$|\{i : a_i \oplus b_i = x_i \cdot y_i\}| \geq 0.83n.$$

关于该协议的可靠性，我们使用定理4，其中取 $\varepsilon = \frac{2}{100}$ 和 $\delta = n/(\ln 2)\times 10^4$。这意味着满足条件的经典证明者的获胜概率存在上界 $72\delta^2$

$$\mathrm{I}^{\delta}_{\max}(X:M) \leq \frac{4n}{(\ln 2)\times 10^4} - \log\log\frac{1}{\delta} - 19.$$

现在我们将证明定理中关于完备性和噪声鲁棒性的部分。$\mathrm{CHSH}^{t/n}$ 的量子策略就是重复执行最优量子策略n 次，不过 Alice 在t_0 时进行测量，而 Bob 在t_1时进行测量。在 CHSH 的最优量子策略中，Alice 和 Bob 共享一个 EPR 对，最优量子获胜概率为 $\cos^2\left(\frac{\pi}{8}\right)$ ≈0.85。如果模型中 Alice 和 Bob 接触到的不是n 个精确的 EPR 对，而是n 个含噪EPR对，并且他们可以在每个副本上执行与 CHSH 策略对应的含噪测量，使得单个 CHSH 副本的获胜概率至少为 $0.85-\gamma$。由于每个副本上的获胜彼此独立，根据 Chernoff 界（事实1），至少在$(0.85-2\gamma)n = 0.83n$ 个副本上满足获胜条件的概率至少为 $1-e^{-2\gamma^2 n}$。

需要在t_0 与t_1 之间保留的量子存储器M 是 Bob 的含噪 EPR 对中的一部分。根据无信号原理，Bob 的系统与 Alice 的输入X不相关。因此，我们有 $\mathrm{I}_{\max}(X:M) = 0$。

□

3.1 经典下界

我们首先在无通信的标准非局域游戏设定下，证明阈值并行重复 CHSH 游戏的经典值上界，然后将其推广到通信设定。

引理 2。 在 n 场 *CHSH* 游戏中赢得 t 场的经典值，当 $t = ((1+\sqrt{5})/4+\varepsilon)n$ 时，其上界为

$$\omega(\mathrm{CHSH}^{t/n}) \leq e^{-2\varepsilon^2 n}.$$

证明。首先我们论证，对于 n 个 CHSH 游戏，在任意子集 S 中获胜的概率至多为 $\left(\frac{1+\sqrt{5}}{4}\right)^{|S|}$。假设某个子集 S 中并非如此。那么我们可以如下给出 $\mathrm{CHSH}^{|S|}$ 的策略：使用 CHSH^n 的策略，将 $\mathrm{CHSH}^{|S|}$ 的实际 $|S|$ 输入嵌入到 n 个输入的子集 S 中，并按照 CHSH 分布对其余 $n-|S|$ 个输入进行采样。使用该策略赢得 $\mathrm{CHSH}^{|S|}$ 的概率，恰好等于原策略中赢得 CHSH^n 的子集 S 的概率。因此，根据事实 5，在 S 中获胜的概率不可能高于 $\left(\frac{1+\sqrt{5}}{4}\right)^{|S|}$。

根据上述论证，并利用广义切尔诺夫界（事实 2），即可得到所需结论。

□

推论 3. 假设 *Alice* 和 *Bob* 共享随机性但没有纠缠，他们获得 *CHSH* 的 n 份副本的输入。*Alice* 生成自己的输出，并向 *Bob* 发送一条包含 c 比特的经典消息；*Bob* 则利用 *Alice* 发来的这条经典消息生成自己的输出。那么，他们在 *CHSH* 的 n 份副本中获胜至少 t 次的概率，对于 $t = ((1+\sqrt{5})/4+\varepsilon)n$，满足

$$\Pr\left[Win\ \mathrm{CHSH}^{t/n}\right] \leq 2^c \cdot e^{-2\varepsilon^2 n}.$$

证明。 假设该上界不成立。那么，我们就能给出一个无需通信的 $\mathrm{CHSH}^{t/n}$ 策略，其获胜概率大于 $e^{-2\varepsilon^2 n}$，这与引理 2矛盾。该策略的做法是让 Bob 假装自己的私有随机性就是 Alice 发来的消息。由于 Alice 的消息包含 c 比特，Bob 的私有随机性恰好等于 Alice 原本会发送的消息的概率为 2^{-c}。因此，如果通过通信获胜的概率大于 $2^c \cdot e^{-2\varepsilon^2 n}$，那么无需通信时获胜的概率就大于 $2^{-c} \cdot 2^c \cdot e^{-2\varepsilon^2 n} = e^{-2\varepsilon^2 n}$。

□

现在我们可以证明本节的主要结果：通过消息所传达的关于X的信息来刻画通信，并将其与 $\mathrm{CHSH}^{t/n}$ 的获胜概率联系起来。

定理 4。 假设 *Alice* 和 *Bob* 共享随机性但不共享纠缠，获得 n 份 *CHSH* 的输入 X 和 Y。*Alice* 生成自己的输出，并发送一条满足以下条件的经典消息 M：

$$\mathrm{I}^{\delta}_{\max}(X:M) < \frac{2\varepsilon^2 n}{\ln 2} - 4\log(1/\delta) - \log\log(1/\delta) - 19$$

对于某个 δ，$\varepsilon > 0$，*Bob* 使用 *Alice* 发送的这条经典消息生成自己的输出。那么，他们在 n 份 *CHSH* 中赢得 t 份的概率（其中 $t = ((1+\sqrt{5})/4+\varepsilon)n$）满足

$$\Pr\left[Win\ \mathrm{CHSH}^{t/n}\right] < 72\delta^2.$$

为了证明这一理论，我们使用以下关于压缩经典消息的结果。

事实 6 ([JRS03, Jai15])。 假设 M 是 *Alice* 和 *Bob* 之间某个单向私有硬币经典通信协议的通信记录 $\mathcal{P}$，*Alice* 和 *Bob* 的输入分别为来自某个乘积分布的 X 和 Y；对于某个关系，该协议在此分布下的成功概率为 α。如果 $\mathrm{I}^{\beta}_{\mathrm{s}}(X:M) \leq c$，对于 $\beta \in (0, \alpha/2]$，，那么存在另一个 *Alice* 和 *Bob* 之间的确定性单向通信协议 $\mathcal{P}'$，使得：

(i) $\mathcal{P}'$ 中的通信量至多为 $c + \log(2/\beta) + \log\log(2/\beta)$ 比特；

（*ii*） $\mathcal{P}'$ 对于该关系的成功概率至少为 $\alpha - 2\beta$。

定理4的证明。 设 $\delta' = 72\delta^2$。假设原始协议在 CHSH 中的获胜概率$^{t/n}$（我们称之为 $\mathcal{P}$）至少为 δ'。我们将证明 $c = \mathrm{I}^{\delta'}/^{4}_{\mathrm{s}}(X:M)$的下界，再由事实3得出结论。若

$$c < \frac{2\varepsilon^2 n}{\ln 2} - \log(16/\delta') - \log\log(8/\delta')$$

在 $\mathcal{P}$中，则根据事实 6，存在另一个协议 $\mathcal{P}'$，其成功概率至少为 $\delta' - 2\cdot\frac{\delta'}{4}$，且 Alice 与 Bob 通信_

$$c' = c + \log(8/\delta') + \log\log(8/\delta')$$

比特。根据推论 3，必有：

$$\frac{\delta'}{2} \le 2^{c'}\cdot e^{-2\varepsilon^2 n} \qquad \Rightarrow \qquad c' \ge \frac{2\varepsilon^2 n}{\ln 2} - \log(2/\delta').$$

代入 c' 的值，得到：

$$c \ge \frac{2\varepsilon^2 n}{\ln 2} - \log(2/\delta') - \log(8/\delta') - \log\log(8/\delta'),$$

这与 c 的上界矛盾。

代入 δ'的值，我们由事实3得到，

$$\begin{aligned}\mathrm{I}^{\delta}_{\max}(X:M) &\ge \frac{2\varepsilon^2 n}{\ln 2} - \log(1152/\delta^2) - \log\log(576/\delta^2) - \log((8+\delta^2)/\delta^2) - 2\\ &\ge \frac{2\varepsilon^2 n}{\ln 2} - 4\log(1/\delta) - \log\log(1/\delta) - 19\end{aligned}$$

对于 $\delta \le \frac{1}{2}$。 □

参考文献

[AA13] Scott Aaronson与Alex Arkhipov。线性光学的计算复杂性。*Theory ofComputing*，9:143–252，2013。

[AAB+19] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Buell, Brian Burkett, Yu Chen, Zi- jun Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, Edward Farhi, Brooks Foxen, Austin Fo wler, Craig Gidney, Marissa Giustina, Rob Graff, Keith Guerin, Steve Habegger, Matthew P. Harrigan, Michael J. Hartmann, Alan Ho, Markus Hoffmann, Trent Huang, Travis S. Humble, Sergei V. Isakov, Evan Jeffrey, Zhang Jiang, Dvir Kafri, Kostyantyn Kechedzhi, Julian Kelly, Paul V. Klimov, Sergey Knysh, Alexander Korotkov, Fedor Kostritsa, David Landhuis, Mike Lindmark, Erik Lucero, Dmitry Lyakh, Salvatore Mandr`a, Jarrod R. Mc- Clean, Matthew McEwen, Anthony Megrant, Xiao Mi, Kristel Michielsen, Masoud Mohseni, Josh Mutus, Ofer Naaman, Matthew Neeley, Charles Neill, Murphy Yuezhen Niu, Eric Os- tby, Andre Petukhov, John C. Platt, Chris Quintana, Eleanor G. Rieffel, Pedram Roushan, Nicholas C. Rubin, Daniel Sank, Kevin J. Satzinger, Vadim Smelyanskiy, Kevin J. Sung, Matthew D. Trevithick, Amit Vainsencher, Benjamin Villalonga, Theodore White, Z. Jamie Yao, Ping Yeh, Adam Zalcman, Hartmut Neven, and John Matthew Martinis。《使用可编程超导处理器实现量子霸权》。《自然》，574:505–510，2019。

[Aar14] Scott Aaronson。《量子计算中最令人恼火的十个新问题》。https: //scottaaronson.blog/?p=1792，2014。[ABJT20] Anurag Anshu、Mario Berta、Rahul Jain 和 Marco Tomamichel。部分平滑信息度量。IEEE信息论汇刊，66(8):5022–5036，2020。[AG20] Scott Aaronson 和 Sam Gunn。关于伪造线性交叉熵基准测试的经典难度。Theory of Computing，16:1–34，2020。[CSUU08] Richard Cleve、William Slofstra、Falk Unger 和 Sarvagya Upadhyay。量子XOR证明系统的完美并行重复定理。计算复杂性，17(2):282–299，2008。[DHL+25] Matthew DeCross、Reza Haghshenas、Minzhao Liu、Enrico Rinaldi、Johnnie Gray、Yuri Alex- eev、Charles H. Baldwin、John P. Bartolotta、Matthew Bohn、Eli Chertkov、Julia Cline、Jonhas Colina、Davide DelVento、Joan M. Dreiling、Cameron Foltz、John P. Gaebler、Thomas M. Gat- terman、Christopher N. Gilbreth、Joshua Giles、Dan Gresh、Alex Hall、Aaron Hankin、Azure Hansen、Nathan Hewitt、Ian Hoffman、Craig Holliman、Ross B. Hutson、Trent Jacobs、Jacob Johansen、Patricia J. Lee、Elliot Lehman、Dominic Lucchetti、Danylo Lykov、Ivaylo S. Madjarov、Brian Mathewson、Karl Mayer、Michael Mills、Pradeep Niroula、Juan M. Pino、Conrad Roman、Michael Schecter、Peter E. Siegfried、Bruce G. Tiemann、Curtis Volin、James Walker、Ruslan Shaydulin、Marco Pistoia、Steven A. Moses、David Hayes、Brian Neyenhuis、Russell P. Stutz 和 Michael Foss-Feig。任意几何结构下随机量子电路的计算能力。《物理评论X》，15:021052，2025。[DS14] Irit Dinur 和 David Steurer。并行重复的解析方法。载于第四十六届ACM计算理论研讨会论文集（STOC 2014），第624–633页，2014。[GFZ+25] Dongxin Gao、Daojin Fan、Chen Zha、Jiahao Bei、Guoqing Cai、Jianbin Cai、Sirui Cao、Xiang- dong Zeng、Fusheng Chen、Jiang Chen、Kefu Chen、Xiawei Chen、Xiqing Chen、Zhe Chen、Zhiyuan Chen、Zihua Chen、Wenhao Chu、Hui Deng、Zhibin Deng、Pei Ding、Xun Ding、Zhuzhengqi Ding、Shuai Dong、Yupeng Dong、Bo Fan、Yuanhao Fu、Song Gao、Lei Ge、Ming Gong、Jiacheng Gui、Cheng Guo、Shaojun Guo、Xiaoyang Guo、Tan He、Linyin Hong、Yisen Hu、He-Liang Huang、Yong-Heng Huo、Tao Jiang、Zuokai Jiang、Honghong Jin、Yunxiang Leng、Dayu Li、Dongdong Li、Fangyu Li、Jiaqi Li、Jinjin Li、Junyan Li、Junyun Li、Na Li、Shaowei Li、Wei Li、Yuhuai Li、Yuan Li、Futian Liang、Xuelian Liang、Nanxing Liao、Jin Lin、Weiping Lin、Dailin Liu、Hongxiu Liu、Maliang Liu、Xinyu Liu、Xuemeng Liu、Yancheng Liu、Haoxin Lou、Yuwei Ma、Lingxin Meng、Hao Mou、Kailiang Nan、Binghan Nie、Meijuan Nie、Jie Ning、Le Niu、Wenyi Peng、Haoran Qian、Hao Rong、Tao Rong、Huiyan Shen、Qiong Shen、Hong Su、Feifan Su、Chenyin Sun、Liangchao Sun、Tianzuo Sun、Yingxiu Sun、Yimeng Tan、Jun Tan、Longyue Tang、Wenbing Tu、Cai Wan、Jiafei Wang、Biao Wang、Chang Wang、Chen Wang、Chu Wang、Jian Wang、Liangyuan Wang、Rui Wang、Shengtao Wang、Xinzhe Wang、Zuolin Wei、Jiazhou Wei、Dachao Wu、Gang Wu、Jin Wu、Shengjie Wu、Yulin Wu、Shiyong Xie、Lianjie Xin、Yu Xu、Chun Xue、Kai Yan、Weifeng Yang、Xinpeng Yang、Yang Yang、Yangsen Ye、Zhenping Ye、Chong Ying、Jiale Yu、Qinjing Yu、Wenhu Yu、Shaoyu Zhan、Feifei Zhang、Haibin Zhang、Kaili Zhang、Pan Zhang、Wen Zhang、Yiming Zhang、Yongzhuo Zhang、Lixiang Zhang、Guming Zhao、Peng Zhao、Xianhe Zhao、Xintao Zhao、Youwei Zhao、Zhong Zhao、Luyuan Zheng、Fei Zhou、Liang Zhou、Na Zhou、Naibin Zhou、Shifeng Zhou、Shuang Zhou、Zhengxiao Zhou、Chengjun Zhu、Qingling Zhu、Guihong Zou、Haonan Zou、Qiang Zhang、Chao-Yang Lu、Cheng-Zhi Peng、XiaoBo Zhu 和 Jian-Wei Pan。利用105量子比特祖冲之三号处理器，确立量子计算优势的新基准。《物理评论快报》，134:090601，2025。[Jai15] Rahul Jain。通信复杂度中新的强直积结果。《ACM学报》，62(3)，2015。[JRS03] Rahul Jain、Jaikumar Radhakrishnan 和 Pranab Sen。通过消息压缩证明通信复杂度中的直和定理。载于自动机、语言与编程国际研讨会（ICALP 2003），第300–315页，2003。

[KGD+25] William Kretschmer、Sabee Grewal、Matthew DeCross、Justin A. Gerber、Kevin Gilmore、Dan Gresh、Nicholas Hunter-Jones、Karl Mayer、Brian Neyenhuis、David Hayes 和 Scott Aaron- son。《证明量子与经典信息资源之间存在无条件分离》。https://arxiv.org/abs/2509.07255，2025年。[MLA+22] Lars Skovgaard Madsen、Fabian Laudenbach、Mohsen Falamarzi Askarani、Fabien Rortais、Trevor Vincent、Jacob F. F. Bulmer、Filippo M. Miatto、Leonhard Neuhaus、Lukas G. Helt、Matthew J. Collins、Adriana E. Lita、Thomas Gerrits、Sae Woo Nam、Varun D. Vaidya、Mat- teo Menotti、Ish Dhand、Zachary Vernon、nicol´as Quesada 和 Jonathan Lavoie。《利用可编程光子处理器实现量子计算优势》。《自然》，606：75–81，2022年。[MVM+24] A. Morvan、B. Villalonga、X. Mi、S. Mandr`a、A. Bengtsson、P. V. Klimov、Z. Chen、S. Hong、C. Er- ickson、I. K. Drozdov、J. Chau、G. Laun、R. Movassagh、A. Asfaw、L. T.A.N. Brand˜ao、R. Peralta、D. Abanin、R. Acharya、R. Allen、T. I. Andersen、K. Anderson、M. Ansmann、F. Arute、K. Arya、J. Atalaya、J. C. Bardin、A. Bilmes、G. Bortoli、A. Bourassa、J. Bovaird、L. Brill、M. Broughton、B. B. Buckley、D. A. Buell、T. Burger、B. Burkett、N. Bushnell、J. Campero、H. S. Chang、B. Chiaro、D. Chik、C. Chou、J. Cogan、R. Collins、P. Conner、W. Courtney、A. L. Crook、B. Curtin、D. M. Debroy、A. Del Toro Barba、S. Demura、A. Di Paolo、A. Dunsworth、L. Faoro、E. Farhi、R. Fatemi、V. S. Ferreira、L. Flores Burgos、E. Forati、A. G. Fowler、B. Foxen、G. Garcia、E. Genois、W. Gi- ang、C. Gidney、D. Gilboa、M. Giustina、R. Gosula、A. Grajales Dau、J. A. Gross、S. Habeg- ger、M. C. Hamilton、M. Hansen、M. P. Harrigan、S. D. Harrington、P. Heu、M. R. Hoffmann、T. Huang、A. Huff、W. J. Huggins、L. B. Ioffe、S. V. Isakov、J. Iveland、E. Jeffrey、Z. Jiang、C. Jones、P. Juhas、D. Kafri、T. Khattar、M. Khezri、M. Kieferov´a、S. Kim、A. Kitaev、A. R. Klots、A. N. Korotkov、F. Kostritsa、J. M. Kreikebaum、D. Landhuis、P. Laptev、K. M. Lau、L. Laws、J. Lee、K. W. Lee、Y. D. Lensky、B. J. Lester、A. T. Lill、W. Liu、W. P. Livingston、A. Locharla、F. D. Malone、O. Martin、S. Martin、J. R. McClean、M. McEwen、K. C. Miao、A. Mieszala、S. Montaz- eri、W. Mruczkiewicz、O. Naaman、M. Neeley、C. Neill、A. Nersisyan、M. Newman、J. H. Ng、A. Nguyen、M. Nguyen、M. Yuezhen Niu、T. E. O’Brien、S. Omonije、A. Opremcak、A. Petukhov、R. Potter、L. P. Pryadko、C. Quintana、D. M. Rhodes、E. Rosenberg、C. Rocque、P. Roushan、N. C. Rubin、N. Saei、D. Sank、K. Sankaragomathi、K. J. Satzinger、H. F. Schurkus、C. Schuster、M. J. Shearn、A. Shorter、N. Shutty、V. Shvarts、V. Sivak、J. Skruzny、W. C. Smith、R. D. Somma、G. Sterling、D. Strain、M. Szalay、D. Thor、A. Torres、G. Vidal、C. Vollgraff Heidweiller、T. White、B. W. K. Woo、C. Xing、Z. J. Yao、P. Yeh、J. Yoo、G. Young、A. Zalcman、Y. Zhang、N. Zhu、N. Zo- brist、E. G. Rieffel、R. Biswas、R. Babbush、D. Bacon、J. Hilton、E. Lucero、H. Neven、A. Megrant、J. Kelly、I. Aleiner、V. Smelyanskiy、K. Kechedzhi、Y. Chen 和 S. Boixo。《随机线路采样中的相变》。《自然》，634：328–333，2024年。[NDN+22] 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(7920)：682–686，2022年。[PS97] Alessandro Panconesi 和 Aravind Srinivasan。《通过扩展 Chernoff–Hoeffding 界实现随机化分布式边着色》。《SIAM 计算杂志》，26(2)：350–368，1997年。[WBC+21] Yulin Wu、Wan-Su Bao、Sirui Cao、Fusheng Chen、Ming-Cheng Chen、Xiawei Chen、Tung-Hsun Chung、Hui Deng、Yajie Du、Daojin Fan、Ming Gong、Cheng Guo、Chu Guo、Shaojun Guo、Lianchen Han、Linyin Hong、He-Liang Huang、Yong-Heng Huo、Liping Li、Na Li、Shaowei Li、Yuan Li、Futian Liang、Chun Lin、Jin Lin、Haoran Qian、Dan Qiao、Hao Rong、Hong Su、Lihua Sun、Liangyuan Wang、Shiyu Wang、Dachao Wu、Yu Xu、Kai Yan、Weifeng Yang、Yang Yang、Yangsen Ye、Jianghan Yin、Chong Ying、Jiale Yu、Chen Zha、Cha Zhang、Haibin Zhang、Kaili Zhang、Yiming Zhang、Han Zhao、Youwei Zhao、Liang Zhou、Qingling Zhu、Chao-Yang Lu、Cheng-Zhi Peng、Xiaobo Zhu 和 Jian-Wei Pan。《利用超导量子处理器实现强量子计算优势》。《物理评论快报》，127：180501，2021年。[ZCC+22] Qingling Zhu、Sirui Cao、Fusheng Chen、Ming-Cheng Chen、Xiawei Chen、Tung-Hsun Chung、Hui Deng、Yajie Du、Daojin Fan、Ming Gong、Cheng Guo、Chu Guo、Shaojun Guo、Lianchen

Han、Linyin Hong、He-Liang Huang、Yong-Heng Huo、Liping Li、Na Li、Shaowei Li、Yuan Li、Futian Liang、Chun Lin、Jin Lin、Haoran Qian、Dan Qiao、Hao Rong、Hong Su、Lihua Sun、Liangyuan Wang、Shiyu Wang、Dachao Wu、Yulin Wu、Yu Xu、Kai Yan、Weifeng Yang、Yang Yang、Yangsen Ye、Jianghan Yin、Chong Ying、Jiale Yu、Chen Zha、Cha Zhang、Haibin Zhang、Kaili Zhang、Yiming Zhang、Han Zhao、Youwei Zhao、Liang Zhou、Chao-Yang Lu、Cheng-Zhi Peng、Xiaobo Zhu 和 Jian-Wei Pan。《通过 60 量子比特、24 周期随机线路采样实现量子计算优势》。《科学通报》，67：240–245，2022年。

[ZvLR+22] Wei Zhang、Tim van Leent、Kai Redeker、Robert Garthoff、Ren´e Schwonnek、Florian Fertig、Sebastian Eppelt、Wenjamin Rosenfeld、Valerio Scarani、Charles C.-W. Lim 和 Harald Weinfurter。《面向远距离用户的设备无关量子密钥分发系统》。《自然》，607(7920):687–691，2022年。