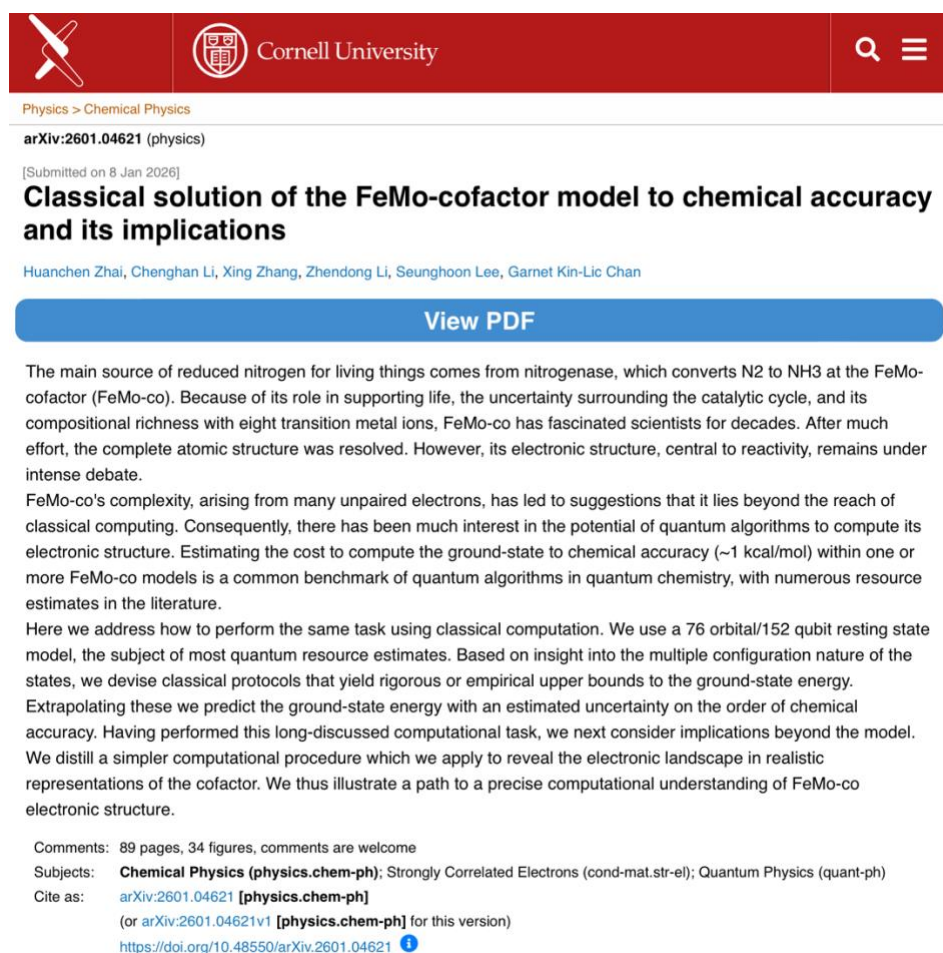


无需量子计算机也能破解关键化学难题

文 | 徐令予

《Quanta Magazine》报道了加州理工学院 Garnet Chan 团队于 2026 年 1 月发表的研究成果。该团队使用纯经典计算方法，对固氮酶铁钼辅因子模型的基态能量达到了接近“化学精度”的结果。



The screenshot shows the top navigation bar of the Cornell University website with the Cornell logo and search icons. Below the navigation bar, the breadcrumb trail reads "Physics > Chemical Physics". The preprint ID is "arXiv:2601.04621 (physics)" and it was submitted on 8 Jan 2026. The title is "Classical solution of the FeMo-cofactor model to chemical accuracy and its implications" by Huanchen Zhai, Chenghan Li, Xing Zhang, Zhendong Li, Seunghoon Lee, and Garnet Kin-Lic Chan. A blue button labeled "View PDF" is visible. The abstract text discusses the complexity of the FeMo-cofactor and the use of classical computation to solve for its ground-state energy. It mentions a 76 orbital/152 qubit model and the prediction of ground-state energy with chemical accuracy. The bottom section contains metadata: "Comments: 89 pages, 34 figures, comments are welcome", "Subjects: Chemical Physics (physics.chem-ph); Strongly Correlated Electrons (cond-mat.str-el); Quantum Physics (quant-ph)", and "Cite as: arXiv:2601.04621 [physics.chem-ph] (or arXiv:2601.04621v1 [physics.chem-ph] for this version) https://doi.org/10.48550/arXiv.2601.04621".

一、文章简介

长期以来，模拟复杂分子的电子结构一直被认为是量子计算机最有希望率先发挥作用的领域之一。理由看起来十分自然：分子中的电子遵循量子力学规律，多个电子之间又可能存在强烈关联和量子纠缠；随着电子数量增加，可能的状态组合会爆炸式增长，经典计算机似乎无法承担如此庞大的计算任

务。因此，不少研究者认为，要准确理解某些复杂化学反应，最终必须依靠能够直接操纵量子状态的量子计算机。

固氮酶中的铁钼辅因子，简称 FeMo-co，正是这一观点最常引用的例子。固氮酶能够把大气中十分稳定的氮气转化成生命可以利用的氨，是地球生命循环中最重要的酶之一。它完成了现代化工必须在高温、高压条件下才能完成的固氮反应，但其具体反应机制至今仍未完全揭示。

问题的难点集中在固氮酶的活性中心——一个由七个铁原子、一个钼原子以及硫、碳等元素组成的复杂原子团。多个铁原子分别携带若干未成对电子，这些电子的轨道、旋转方向和能量彼此关联，不能被当作相互独立的粒子处理。为了计算这一体系的最低能量状态，也就是基态，理论上必须考虑大量电子构型及其叠加关系。

2017 年，微软研究人员曾将 FeMo-co 列为量子计算机模拟化学体系的重要目标。此后，许多论文估算了使用容错量子计算机求解这一问题所需的量子比特和计算资源。它逐渐成为量子化学领域的一个标志性案例：经典计算似乎已经走到极限，只有量子计算机才能继续前进。

然而，加州理工学院化学家 Garnet Chan 及其合作者对此一直持怀疑态度。他们认为，量子态的理论空间虽然极其庞大，但真正对基态能量产生重要影响的构型可能只占其中很小一部分。经典算法没有必要逐一计算所有可能状态，而可以通过物理结构和数学压缩方法，找出真正重要的部分。

研究团队采用了两种彼此独立的经典计算方法。第一种方法从一个近似电子状态出发，逐步增加参与联合变化的电子数量，并观察计算结果是否继续发生显著改变。当涉及更多电子的修正已经不能明显降低能量时，便可以判断剩余大量构型的贡献很小。

第二种方法与密度矩阵重整化群和矩阵乘积态有关。研究人员把复杂量子态拆分成若干部分，并限制各部分之间需要传递的信息量。如果不断提高信息容量后，计算结果逐渐收敛，便可以外推得到接近真实的基态能量。

两种方法最终得到了相互一致的结果，并与现有实验认识相符。研究人员估计，其误差已经接近量子化学中通常所说的“化学精度”，即每摩尔约 1 千

卡。这意味着，一个曾被广泛视为必须由量子计算机解决的标杆问题，至少在其静止状态的基态能量计算上，已经可以由经典计算机完成。

这项成果并不意味着固氮酶已经被彻底破解。研究团队目前计算的主要是铁钼辅因子的静止基态，而真正理解固氮反应，还需要追踪氮分子结合、质子和电子转移、化学键断裂与形成等一系列中间状态。模拟整个反应随时间的演化，仍然可能比计算单一基态困难得多，也可能成为量子计算机更有优势的领域。

因此，这项研究既不能证明量子计算机对化学没有价值，也不能排除未来出现量子优势。它真正动摇的是一种过于简单的推论：因为化学体系遵循量子力学，所以经典计算机必然无法模拟它。

实际上，量子计算机和经典计算机都必须面对同一个关键问题：如何找到一个足够合理的初始状态。量子计算并不能凭空从所有可能状态中自动识别正确答案。如果量子算法需要借助经典化学知识准备一个接近真实基态的初始状态，那么这些知识往往也可能帮助经典算法压缩问题、排除无关构型。

这项研究提醒人们，评价量子计算的实用价值，不能只比较理论上完整状态空间的大小，也不能简单地把“量子体系”等同于“量子计算机专属问题”。真正有意义的问题是：在达到相同精度的条件下，最好的量子算法是否能够稳定地、可扩展地超过最好的经典算法。

经典算法仍在不断进步。量子计算机未来也可能成为重要的化学研究工具，但在宣称某个问题只有量子计算机能够解决之前，必须先认真检验经典方法究竟已经走到了哪里。科学的本质就是实事求是，千万不可先入为主和想当然。

二、读后感想

量子计算在量子模拟和理论化学领域中受到严峻挑战，量子计算在自己的主场都难定输赢，在客场的表现也就可想而知了。

近二十多年来，量子计算被捧上神坛，被宣传可以成为通用量子计算机，秒破公钥密码。捧得越高，跌得必惨，量子计算在破解密码上遭遇了严重挫败[1]。

RSA 公钥密码的安全性，根植于一个极简的数学事实：将两个大素数相乘很容易，但要把它们的乘积重新分解开，却极其困难。破解公钥密码 RSA 的本质是对大整数的质因数分解。

奋斗了二十多年，量子计算在“分解质因数”上始终无法突破 $21=3*7$ ，相关论文和实验报告中的结果令人非常失望。因为 21 仅对应于 5 bit，而现在使用的 RSA 至少是 1024 bit，量子计算执行 Shor's 算法要破解目前使用的公钥密码几乎没有可能。

退一步，即使有一天量子计算机能够破解 1024 bit RSA，其实天也塌不下来。理论分析和实验数据证明，RSA 可以轻松把 1024 bit 提高几倍，甚至几个数量级，这将大幅提高量子计算机的硬件资源的门槛，迫使量子计算的恶意攻击在工程实施上成为不可行[2]。

再退一步，公钥密码的算法也不止 RSA 一种，何必吊死在一棵树上，只需换一种算法足以让量子计算找不到北。

事实上抗量子攻击的公钥密码(PQC)技术已经趋于成熟，大规模的布置应用只是时机和成本问题。认为量子计算会对信息安全产生颠覆性影响仅是炒作而已，实践已经证明，开发通用量子计算机破解密码此路不通。

当前量子计算的发展路径，事实上正在回归其最初、也是最现实的设想——量子模拟。即利用量子系统去模拟量子系统，这正是费曼在 1980 年提出的原始构想。从物理原理上看，这一方向比较现实可行，也确实在若干实验中展现出价值。

但是必须注意到，早在 2023 年，加州理工大学 Chan 等人便系统分析过量子化学中的“指数级量子优势”，结论是：对于一般的基态量子化学问题，目前尚无充分证据证明量子计算机普遍具有指数级优势；即使未来存在优势，也可能更多表现为多项式加速，而不是经常被宣传的指数级飞跃。

总而言之，量子计算在量子化学领域没有打赢经典计算，量子计算在破解密码问题上已经失败，神化量子计算真的可以休矣！

注释

[1] 量子计算能否破解公钥密码？

<https://blog.wenxuecity.com/myblog/64367/202605/4326.html>

[2] Post-quantum RSA

<https://eprint.iacr.org/2017/351.pdf>

徐令予 于美国南加州 (2026年6月15日)