量子计算会威胁比特币安全吗？（上）

——谷歌白皮书披露了什么新数据？

文丨徐令予

最近，一篇来自 Google Quantum AI 的白皮书引发广泛关注。有些媒体将其核心论点提炼为一句话：“量子计算机已经接近破解比特币。”但这显然误读了谷歌的白皮书。更为精准的比喻应该是，这篇白皮书并不是宣布造出了一颗原子弹，而只是在重新分析和计算后发现：造原子弹所需的铀，可能比以前设想的要少很多。

关于制造原子弹所需浓缩铀-235（U-235）临界质量的科学估算，从根本上重塑了原子弹试验的历史进程：它导致德国的核计划陷入停滞，却加速了美国的研发步伐。

以维尔纳·海森堡（Werner Heisenberg）为首的德国科学家错误地高估了所需的 U-235 用量，将其估算在 13 吨（13,000 千克）左右，从而断定制造原子弹是不可能的任务。由于认定制造原子弹遥不可及，加之缺乏行之有效的铀浓缩技术，纳粹政府于 1942 年决定将核计划的规模大幅缩减，仅保留小规模的理论研究工作。这一决定直接导致德国境内从未开展过任何实质性的原子弹试验。

相比之下，美国科学家则确定浓缩铀的实际需求量不到 100 磅（即不足 50 千克），这使得制造原子弹成为一项现实可行——尽管依然充满挑战——的宏伟工程。在理论估算的正确指导下，美国不惜一切代价开展了一项疯狂的工业计划，旨在生产 60 至 100 千克的浓缩铀-235，从而制造出了可以投入实战的致命性核武器。

历史经验表明，对制造原子弹所需铀的准确估算，确实对其最终成功起到了关键作用；但同样必须看到，这与原子弹真正被制造并成功爆炸，毕竟不是同一回事。认清这两者之间的关联与差别，正是理解 Google 今日这份白皮书关键。

一、白皮书改变的是“理论门槛”，而不是现实能力

白皮书的核心，是对椭圆曲线离散对数问题（ECDLP）的量子攻击资源进行重新估算。作者构造了一套新的量子“逻辑电路”，并给出结果：在理想条件下，破解所需资源约为 1200 个逻辑量子比特，以及 7000 万至 9000 万个 Toffoli 门。相较此前研究，攻击的成本下降了一个数量级。

这当然是一个值得重视的进展。但它回答的，只是一个理论问题：如果未来存在一台理想的容错量子计算机，那么攻击所需资源，可能比我们过去认为的更低。换句话说，它讨论的是：

- 需要多少资源
- 如何组织计算
- 理论门槛是否下降

而不是：

- 机器是否已经存在
- 攻击是否已经可行

该白皮书改变的，是“需要多少铀”；而不是“原子弹已经造出来了”。白皮书中所谓“构造了逻辑电路”，本质上只是将算法写成量子门操作序列的设计图。它更接近芯片的电路图，而不是已经制造完成的芯片。这一点，看似技术细节，却是整个问题的分界线。

从这个角度看，这篇白皮书的意义在于，它可能在修正过去对量子攻击难度的某种高估。但问题在于，它仍然停留在“设计图”的层面。

二、从理论到现实的三道关卡

即使接受白皮书的全部计算结果，其结论仍然需要经过至少三重检验。

首先，估算本身未必一定正确。量子电路的构造与优化路径存在多种可能，不同方案之间的资源开销可以相差几个数量级。因此，“1200 个逻辑量子比特”更应被理解为一种特定设计下的推测，而不是已经被严格证明的科学结论，这与当年试制原子弹时对铀的需求估算完全不在一个档次上。

其次，这些估算依赖一组理想条件。稳定而高效的量子纠错、持续的资源供给、高度并行的执行能力，这些条件在逻辑层面可以成立，但在现实工程中是否能够同时满足，是完全不同的问题。知道了需要多少铀，并不意味着我们已经具备提炼、纯化并稳定控制这些铀的能力。

再次，工程实现本身仍然极其困难。一个逻辑量子比特通常需要成千上万个物理量子比特支撑，这意味着论文中的“1200 个逻辑比特”，在现实中很可能对应数百万量级的物理系统。而今天最先进的量子计算设备，仍停留在数百到数千物理比特的规模。更重要的是，还必须实现长时间稳定运行、数千万级操作不中断，以及整个系统的精密协调。这些问题，正是当前量子工程最不确定的部分。

换句话说，这里至少有三道关卡：

- 估算是否可靠
- 条件是否成立
- 工程是否可行

任何一道未过，都意味着距离量子计算机破解密码的现实能力仍然非常遥远。

三、“分钟级攻击”：理想推演而非现实能力

白皮书中提到的“分钟级攻击”，正是建立在上述理想条件之上的推测。假设物理错误率为 10^{-3} 且具备平面连接架构的超导量子计算平台上，上述电路仅需不到 50 万个物理量子比特，便可在数分钟内攻破 256 位椭圆曲线离散对数公钥密码。这类“快时钟”型量子计算机将能够针对某些加密货币的公共内存池交易发起“即时花费”（on-spend）攻击。但这不是实验结果，而是在一台尚不存在的理想机器上的推演。只要其中任一前提无法满足，计算时间便会迅速上升，甚至使攻击不可行。

如果把视角再拉远一步，还会看到一个更直接的现实：Shor's algorithm 提出至今已有三十年，但在实验层面，人类能够分解的整数仍停留在极小规模，例如 35=5×7。这并不意味着算法无效，而是说明，从理论可行迈向工程可行，是一条极其漫长的路径。

结语

因此，这篇白皮书真正改变的，是我们对“理论难度”的认识，而不是现实世界中的能力边界。它缩短的是纸面上的距离，而不是工程上的距离。

回到最初的比喻，我们或许重新估算了“需要多少铀”，但距离真正造出原子弹，仍有极其漫长的路要走。在这样的技术问题上，冷静或许比惊讶更为重要。