物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

量子存储式量子计算机与无噪声光子回波

周宗权

“Quantum memory” quantum computers and noiseless phton echoes

Zhou Zong-Quan

引用信息 Citation: Acta Physica Sinica, 71, 070305 (2022) DOI: 10.7498/aps.71.20212245
在线阅读 View online: https://doi.org/10.7498/aps.71.20212245
当期内容 View table of contents: http://wulixb.iphy.ac.cn

您可能感兴趣的其他文章
Articles you may be interested in

量子存储研究进展
Research progress of quantum memory
物理学报. 2019, 68(3): 030307 https://doi.org/10.7498/aps.68.20190039

多模式固态量子存储
Multimode solid-state quantum memory
物理学报. 2019, 68(3): 030303 https://doi.org/10.7498/aps.68.20182207

基于掺铒晶体的光量子存储和调控
Quantum memory and manipulation based on erbium doped crystals
物理学报. 2022, 71(6): 064203 https://doi.org/10.7498/aps.71.20211803

硅和锗量子计算材料研究进展
Research progress of silicon and germanium quantum computing materials
物理学报. 2021, 70(21): 217802 https://doi.org/10.7498/aps.70.20211492

基于拉曼协议的量子存储
Raman protocol-based quantum memories
物理学报. 2019, 68(3): 034203 https://doi.org/10.7498/aps.68.20182215

金刚石氮空位中心自旋量子调控
Quantum control of nitrogen-vacancy center in diamond
物理学报. 2018, 67(12): 120302 https://doi.org/10.7498/aps.67.20180755

专题: 量子计算新进展: 硬件、算法和软件

量子存储式量子计算机与无噪声光子回波*

周宗权[1)†]

1) (中国科学技术大学, 中国科学院量子信息重点实验室, 合肥 230026)

(2021 年 12 月 5 日收到; 2022 年 1 月 11 日收到修改稿)

量子计算机一个重要的应用是攻破经典密码. 以往的研究表明, 攻破广泛使用的 2048 位 RSA 密码所需要的量子比特数目在 2000 万左右, 远远超出了目前的技术水平. 近期法国研究人员提出, 如使用配备了多模式量子存储的量子计算机, 则只需要 1.3 万个量子比特即可攻破 2048 位的 RSA 密码. 这一研究把量子存储器的应用推广到量子计算领域, 为研制实用化量子计算机提供了一条新的技术路线. 量子存储式量子计算机需要微波段的量子存储器, 这是目前亟待开发的新技术. 基于对量子存储过程中原子辐射本质的分析,近期我们提出了无噪声光子回波方案, 成功解决了光子回波的自发辐射噪声难题, 有望进一步实现微波段量子存储并应用于量子存储式量子计算机中.

关键词: 量子计算, 量子存储, RSA, 光子回波

PACS: 03.67.Lx, 07.05.–t

DOI: 10.7498/aps.71.20212245

1 量子计算

量子计算有望为人类提供前所未有的强大算力, 引起了各国政府和大型公司的广泛重视和投入. 近年来该领域一个重要的研究进展是实现了量子优越性的证明[1,2], 即针对一个人为设计的特定问题, 证明量子计算机或量子模拟机相比经典计算机具有求解速度上的优势. 值得注意的是, 这个问题并非一个有用的问题, 量子优越性的证明只需要 100 个左右的物理量子比特. 求解一个有用的问题自然是量子计算机发展的终极目标, 其中一个最具代表性的例子就是攻破经典密码. 要完成这样的目标, 一般需要对物理量子比特进一步执行纠错编码获得逻辑量子比特并且需要大量的逻辑比特, 其资源需求是非常庞大的.

经典通信的加密原理主要是基于特定数学问题的计算复杂性. RSA 密码是目前最广泛使用的一类加密算法, 其对应的数学问题是质因数分解. 比如我们可以快速算出 $353 \times 797 = 281341$. 但是当问题变成 281341 应分解成哪两个质数的乘积, 这个问题求解起来就变困难很多了. 当 RSA 密码的位数长至 2048 位时, 即便使用目前最强大的超级计算机也无法在一个合理的时间内攻破它.

1994 年, 美国数学家 Shor 提出著名的 Shor 算法, 证明使用量子计算机可以快速地实现大数的因数分解. 2019 年, Google 公司 Gidney 和瑞典 KTH 皇家理工学院的 Ekera 证明量子计算机只需要 8 个小时即可攻破 2048 位的 RSA 密码, 但是需要 2000 万个物理量子比特[3]. 这一需求远远超出了目前量子计算研究的技术水平 (约 100 个物理量子比特), 看起来遥不可及. 如何降低实用化量子计算机的物理资源需求是理论研究的一个重要难题.

2 量子存储式量子计算机

在冯诺依曼架构的经典计算机中, 存储器扮演了一个重要的角色, 即用来保存处理器的中间计算

* 国家重点基础研究发展计划 (批准号: 2017YFA0304100) 资助的课题.

† 通信作者. E-mail: zq_zhou@ustc.edu.cn

© 2022 中国物理学会 Chinese Physical Society

结果. 冯诺依曼架构的量子计算机也早有实验研究, 但是由于量子存储器本身也较难实现, 目前大多量子计算实验研究都没有引入量子存储器. 近期, 法国国家科学中心的 Gouzien 和 Sangouard 在《物理评论快报》上发表论文[4], 证明使用配备量子存储器的量子计算机, 可以大幅度地降低量子计算机对物理量子比特数目的需求.

法国团队提出的方案示意图如图 1, 其基本结构是一个二维的超导量子计算芯片, 和一个三维 (二维空间加一维时间) 的多模式量子存储器. 每个量子比特由空间模式指数和时间模式指数来寻址. 当一个量子比特需要处理时, 相应的存储器将以微波光子的形式向计算芯片中对应的量子比特传输量子态信息. 当处理完成, 量子比特的量子态重新被存入存储器直到下一次操作. 量子计算芯片每个时间点处理存储单元中的一个切片 (即具有同样时间模式指数的所有存储单元), 整个过程可以形象地理解为借助量子存储器实现对量子计算芯片的时间域复用.

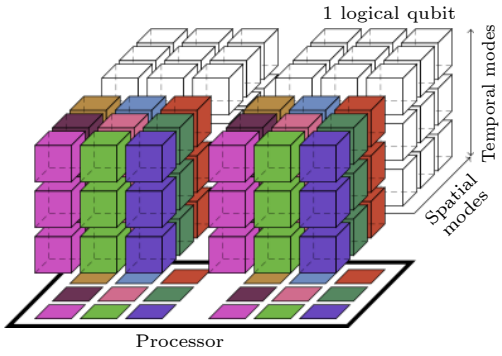

图 1 “量子存储”量子计算机的架构图[4]

Fig. 1. Quantum computing architecture with multimode quantum memories[4].

他们的理论分析表明, 这种量子存储式量子计算机求解 2048 位 RSA 密码只需要 1.3 万个物理量子比特和 177 天的时间. 其额外的代价是需要 2800 万空间模式和 45 个时间模式的量子存储器, 且存储时间约为 2 h. 对比前人的结果, 这个方案降低量子计算机的物理比特数目需求达 3 个量级, 进一步逼近了目前的技术水平, 而它对量子存储模式数和寿命的需求则较为苛刻. 当然, 在这个工作中存储器资源的需求并没有仔细优化, 后续研究也许会进一步缩减这方面的需求.

长寿命的量子存储必须基于长相干寿命的物质系统来实现. 本团队近期利用稀土掺杂晶体 (Eu:YSO 晶体) 实现了对光波段光场长达 1 h 的相干存储, 是目前光存储时间的最长记录[5]. 该工作中使用的存储方案是原子频率梳, 它要求光谱烧孔技术来制备梳状结构吸收带, 不能直接用于微波段量子存储. 在法国团队的论文中, 作者们提出在稀土离子掺杂晶体中执行光子回波方案来实现微波段的多模式量子存储. 光子回波方案无需裁剪原始吸收带, 故在微波段上也易于执行, 但是其应用到量子存储领域仍存在重大挑战.

3 无噪声光子回波量子存储

光子回波是原子系综在与电磁脉冲相互作用时产生的一种相干辐射. 1950 年, 美国物理学家 Hahn 在射频波段上首次发现了光子回波现象, 历史上也习惯称之为自旋回波或 Hahn 回波. 光子回波目前最重要的应用是医学上的核磁共振成像, 这一领域的研究已获得过多次诺贝尔奖.

如果能够把光子回波推向量子领域, 则有望实现任意频段的量子存储. 遗憾的是, 前人的理论研究表明标准光子回波不能用于量子存储[6], 这是因为大量原子被激发到激发态, 带来不可区分的自发辐射噪声并淹没量子信号. 这一本质困难导致近十年来有关光子回波量子存储的研究基本处于停滞状态. 为了探究光子回波的噪声是否本质上不可消除, 我们仔细研究了已有的量子存储方案及各种类型的光子回波方案.

在光与物质相互作用的过程中, 原子系综的辐射从本质上可分为两大类, 即受激辐射与自发辐射 (表 1). 进一步考虑其激励来源, 来自于信号所激励的受激辐射, 本质上正是我们所需要的输出信号. 而来自于其他控制光所激励的受激辐射, 是一种相干噪声. 这种噪声的模式 (包括空间、偏振、频率及位相) 由其激励光场所决定, 所以原理上是与信号光可区分的. 自发辐射必定源自激发态的布居数, 由于辐射位相随机, 其输出一定是噪声. 与相干噪声不同, 自发辐射的模式任意, 故无法通过选择信号的模式来滤除. 值得一提的是, 以上分析是普适的, 无论信号是经典信号还是量子信号. 经典数字光通讯的中继放大器之间的距离不能相距过远, 从量子不可克隆定律的角度来看待这个问题[7], 其本质是确保传输衰减后的信号大小, 来保证信号相比放大介质的自发辐射噪声仍占主导优势.

表 1 光与原子相互作用中的辐射分类

Table 1. 1. Radiations from the atomic ensemble when interacting with light.

辐射类型 Radiation Type	来源 Source	输出结果 Output
受激辐射 Stimulated emission	信号激励 Signal pulses	目标信号 Target signal
	控制光激励 Control pulses	特定辐射模式的相干噪声 Coherent noise with certain modes
自发辐射 Spontaneous emission	激发态布居数 Population in the excited state	辐射模式任意的非相干噪声 Incoherent noise with arbitrary modes

基于上述分析, 构造量子存储方案的本质可以理解为构造一种光与原子相互作用的方案, 以高效率地获取量子信号所激励的受激辐射, 同时避免引入不可区分的相干噪声或自发辐射噪声. 而光子回波方案从原理上必须使用光学 π 脉冲来使得原子系综演化相位重聚, 所以一定会激发大量原子到激发态, 带来不可避免的自发辐射噪声. 这也是前人工作 [6] 认为标准光子回波不可能实现量子存储的根本原因. 事实上, 已取得成功的所有量子存储方案, 包括原子频率梳、电磁感应致透明、可控非均匀加宽、失谐拉曼方案等, 全部都避免引入激发态布居数来避免自发辐射噪声问题.

自发辐射噪声在光子回波方案中不可避免, 但是否与信号完全不可能区分呢? 仔细考察所有的光子回波方案, 会发现它们的一个共性问题: 其发射信号的上能级发射信号的激发态正是被大量布居数占据的激发态, 这导致自发辐射噪声与信号不可区分, 所以消除自发辐射噪声的关键在于如何分离信号辐射的激发态与布居数占据的激发态.

基于这个思路, 我们提出了“无噪声光子回波”方案 (noiseless photon echo, 简称 NLPE), 成功地解决了光子回波中的自发辐射噪声问题 [8], 首次在有大量原子被激发的条件下仍然实现了量子存储. 我们扩大了原子系统的希尔伯特空间为包含两个激发态能级和两个基态能级的四能级结构, 并在其中施加与信号不同频率的四个 π 脉冲, 最终成功使得发射信号的激发态与布居数占据的激发态可区分, 借助频率滤波即可严格消除自发辐射噪声. 由于施加的 π 脉冲与信号光频率不同, 相干噪声也很容易滤除.本团队在 Eu:YSO 晶体中执行了光波段的 NLPE 实验演示 [8], 成功观察到单光子的光子回波且信噪比超过 42.5 ± 7.5, 并实现了 time-bin 量子比特的存储. 在掺 Eu 材料中, NLPE 取得的存储效率和信噪比相比此前唯一可用的原子频率梳方案 [9] 获得了超过四倍的提升. 在光量子 U 盘应用中, Eu:YSO晶体在磁场下的能级退简并及其尺寸限制将导致样品吸收很弱 [5], 如采用原子频率梳方案, 则需要进一步裁剪吸收带导致存储效率过于低下. 而 NLPE 方案完整利用了介质的原始吸收带, 故有望成为量子 U 盘应用的有效存储方案. 由于 NLPE方案无需裁剪原子吸收带, 与标准光子回波一样易于执行, 故也有望成为微波段量子存储的有效方案, 在量子存储式量子计算机中取得应用.

4 总 结

此前, 有关量子存储器的研究主要聚焦于量子通信领域的应用, 比如基于多模式量子存储建立量子中继 [10], 从而构建远程的量子互联网, 或者是基于超长寿命量子存储实现可移动的量子 U 盘 [5]. 而法国团队的这一成果 [4] 则定量地展现了量子存储器在量子计算机中的价值, 成功推广了量子存储器的应用范围.

法国团队的工作目前还没有考虑存储装置的效率、噪声和相干寿命等问题, 这些在实验上也是比较重大的挑战. 匹配多模式量子存储器的量子计算机是否会比不带量子存储的更大规模量子计算机更容易研制? 这个问题目前人们并没有完全确定的答案, 但法国团队的工作为实用化量子计算机的研制提供了一条可行的技术路线, 有待人们去进一步探索. 该技术路线面临的一项重大挑战在于微波段量子存储至今还没有在任何物质系统中实现过. 本团队的理论分析和光波段的实验已经证明 NLPE 是一种有效的量子存储方案 [8], 这一方案在微波段的实际表现也有待实验上的进一步探索.

参考文献

[1] Arute F, Arya K, Babbush R, et al. 2019 *Nature* **574** 505
[2] Zhong H S, Wang H, Deng Y H, et al. 2020 *Science* **370** 1460
[3] Gidney C, Ekerå M 2021 *Quantum* **5** 433
[4] Gouzien E, Sangouard N 2021 *Phys. Rev. Lett.* **127** 140503

[5] Ma Y, Ma Y Z, Zhou Z Q, et al. 2021 *Nat. Commun.* **12** 2381
[6] Ruggiero J, Le Gouët J L, Simon C, Chanelière T 2009 *Phys. Rev. A* **79** 053851
[7] Scarani V, Iblisdir S, Gisin N, et al. 2005 *Rev. Mod. Phys.* **77** 1225
[8] Ma Y Z, Jin M, Chen D L, Zhou Z Q, Li C F, Guo G C 2021 *Nat. Commun.* **12** 4378
[9] Jobez P, Laplane C, Timoney N, Gisin N, Ferrier A, Goldner P, Afzelius M 2015 *Phys. Rev. Lett.* **114** 230502
[10] Liu X, Hu J, Li Z F, Li X, Li P Y, Liang P J, Zhou Z Q, Li C F, Guo G C 2021 *Nature* **594** 41

SPECIAL TOPIC—Recent advances in hardware, algorithms and software of quantum computers

"Quantum memory" quantum computers and noiseless phton echoes*

Zhou Zong-Quan [1)†]

1) (*CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei* 230026, *China*)

(Received 5 December 2021; revised manuscript received 11 January 2022)

Abstract

One of the most important applications of quantum computing is to crack classical cryptosystem. Previous studies showed that the number of qubits required to crack the widely used 2048-bit RSA cipher is about 20 million, which is far beyond the current technology for quantum computing. Recently, É. Gouzien and N. Sangouard of the French Alternative Energies and Atomic Energy Commission proposed a quantum computing architecture based on a two-dimensional grid of superconducting qubits and a three-dimensional multimode quantum memory. They showed that only 13k qubits are required to crack a 2048-bit RSA integer with the help of a long-lived quantum memory with 28 million spatial modes and 45 temporal modes. Their results clearly demonstrate the values of quantum memories in quantum computing and provide an alternative approach for building practically useful quantum computers. Quantum computers require quantum memories to work at microwave band, which remains an outstanding challenge. Based on a detailed analysis of atomic radiations during the quantum storage process, we recently proposed a noiseless-photon-echo protocol which can successfully eliminate the spontaneous emission noise in photon echoes. This protocol is expected to further enable microwave quantum storage and the construction of "quantum memory" quantum computers.

Keywords: quantum computing, quantum memory, RSA, photon echoes

PACS: 03.67.Lx, 07.05.–t **DOI:** 10.7498/aps.71.20212245

* Project supported by the National Basic Research Program of China (Grant No. 2017YFA0304100).

† Corresponding author. E-mail: zq_zhou@ustc.edu.cn