

量子计算机的商业化进展及对信息安全的挑战

王潮¹, 王云江², 胡风¹

(1. 上海大学特种光纤与光接入网重点实验室, 上海 200072;

2. 西安电子科技大学综合业务网理论及关键技术国家重点实验室, 陕西 西安 710071)

摘要: 通用量子计算机器件进展缓慢, 对实用化 1024 bit 的 RSA 密码的破译尚不构成威胁, 现代密码依旧是安全的。首次提出了对 Shor 算法的改进应考虑量子器件约束, 第一和第二量子寄存器器件要求需从设计理论的 1 000~2 000 Qubit 降至 100 Qubit 以下。基于量子人工智能的专用量子计算机的商业化进展迅猛, 已列为应对美国国家战略计算计划的新一代计算思想, 在机器学习和模式识别领域应用广泛, 不能忽视其对互联网大数据信息安全的影响。首次提出了将量子计算机应用于密码设计, 从量子人工智能角度提出了国外尚未开展的量子计算密码研究。

关键词: 加拿大量子计算机; 量子人工智能; 量子隧穿效应; 量子纠错; 量子认知

中图分类号: TN918

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00026

Shaping the future of commercial quantum computer and the challenge for information security

WANG Chao¹, WANG Yun-jiang², HU Feng¹

(1. Key Laboratory of Special Fiber Optics and Optical Access Networks(SCIE), Shanghai University, Shanghai 200072, China;

2. State Key Laboratory of Integrated Services Networks (ISN), Xidian University, Xi'an 710071, China)

Abstract: The progress on universal quantum computer devices is show, so that attacking the 1 024 bit RSA by Shor algorithm is impractical currently. The modern cryptography still has strong security. Take the quantum devices constraints into consideration was proposed for the first time, the storage of former registers in the Shor algorithm should be 100 or less Qubits theoretically decreased from 1 000 or more Qubits. Quantum artificial intelligence, as the rapid progress of special quantum computer, was regarded as the new generation computing idea which met the goal of national strategic computing initiative(NSCI). With the wide applications in the field of machine learning and artificial intelligence, importance to the influences of quantum artificial intelligence on the big data security on internet should be attached. Additionally, it was the first time to use the quantum computer for designing cryptography and it shed an interesting light on cryptography design based on the quantum artificial intelligence which had not been reported anywhere before.

Key words: Canadian quantum computer, quantum artificial intelligence, quantum tunneling effect, quantum error correction, quantum cognition

收稿日期: 2016-02-14; 修回日期: 2016-02-20。通信作者: 王潮, wangchao@staff.shu.edu.cn

基金项目: 国家自然科学基金重点资助项目 (No.61332019); 国家自然科学基金资助项目 (No.61572304, No.61272096, No.61301172, No.61502376); 上海市教委创新基金资助项目 (No.14ZZ089); 上海市特种光纤与光接入网重点实验室开放课题基金资助项目 (No.SKLSFO2014-06); 国家教育部博士点基金资助项目 (No.20120203120001); 高等学校基本科研基金资助项目 (No.JB140105, No. JB151204); 国家 111 基地基金资助项目 (No.B08038)

Foundation Items: Key Program of National Science Foundation of China (No.61332019), The National Natural Science Foundation of China (No.61572304, No.61272096, No.61301172, No.61502376), The Innovation Grant of Shanghai Municipal Education Commission(No.14ZZ089), Shanghai Key Laboratory of Specialty Fiber Optics and Optical Access Networks (No.SKLSFO2014-06), Ph.D. Program Foundation of Ministry of Education of China(No.20120203120001), The Fundamental Research Fund for the Central University (No.JB140105, No. JB151204), The 111 Program (No.B08038)

1 引言

现有2类量子计算机。一是通用量子计算机,器件进展极其缓慢,对于当前的实用密码尚不能构成威胁。二是2011年加拿大D-Wave公司率先推出的专用量子计算机,其商业化进展迅猛,目前Google也在加紧研发。这2类量子计算机执行的量子计算算法、依据的量子理论和可实现的功能完全不同,器件进展程度也有很大差异。

由于学科跨度较大,极易混淆这2类量子计算机,将可以运行Shor算法破译公钥密码、但是器件进展缓慢远不能实用化的通用量子计算机,与商业化迅猛进展、无法运行Shor算法的专用量子计算机混淆,误以为通用量子计算机破译现有电子政务CA系统的RSA公钥密码指日可待。这样的混淆对于判断现代密码的安全性会产生很大的误解,错误地认为现代密码已经不再安全。

本文将介绍2类量子计算机的器件进展情况、应用特点,并首次分析目前唯一实用化的专用量子计算机对密码学和大数据时代信息安全的挑战。

2 通用量子计算机进展

业内对通用量子计算机最关注的是其运行Shor算法破译RSA等公钥密码的能力。然而,通用量子计算机器件进展缓慢,破译实际运行的RSA等公钥密码尚需时日。

2014年12月,《Nature》在调研了欧洲和美国的多个著名量子研究中心后,撰文“30年的奋斗,科学家终于在量子计算找到可达目标(after a 30-year struggle to harness quantum weirdness for computing, physicists finally have their goal in reach)”^[1],判断通用量子计算机的器件进展缓慢,近期无法实现破译实用化1 024 bit RSA公钥密码所需的千位量子比特(Qubit)通用量子计算机。

从二十世纪七、八十年代美国著名物理学家Richard Feynman、阿贡(Argonne)国家实验室的Paul Benioff、牛津大学的David Deutsch等国际学者提出量子计算机的概念至今已经30多年,对量子效应的操控依旧是个难题,一旦受到例如来自外界的杂散光子或振动造成的干扰,量子计算将崩溃。

2014年12月,瑞士联邦理工学院的国际著名量子物理专家Matthias Troyer教授在《Nature》阐述其观点^[1]:由于器件进展缓慢,通用量子计算机缺乏杀手级应用,通用量子计算机已知的2个典型应用——基于Shor算法的公钥密码破译和基于Grover算法的数据库搜索都无法成功实现。而且,百位量子比特实现难度很大,即使能够得以实现,也需要投入大量财力。Matthias Troyer对通用量子计算机和加拿大D-Wave商业化专业量子计算机的进展都非常熟悉,也参加了南加州大学的加拿大量子计算机测试。

事实上,根据《Nature》和《Science》近年来的报道,尚无对1 024 bit以上的RSA的成功攻击实验,或者说目前的进展距离此实用化破译要求差距甚远。2011年,美国UCSB的John Martinis团队^[2]通过量子电路成功实现了冯·诺依曼结构、量子傅里叶变换和三量子比特Toffoli门,这是攻击RSA公钥密码的Shor算法的核心量子电路。2012年,John Martinis团队^[3]还宣布完成了采用量子电路分解素数的实验,完成攻击小规模RSA的实验,成功实现了解析 $15=3\times 5$ 。

尽管在原理上验证了Shor计算攻击RSA的可行性,John Martinis依旧认为通用量子计算机还处于类似二战期间第一台电子计算机的阶段^[1]。根据《Nature》的近年文献,UCSB的John Martinis团队已经完成了5 Qubit的通用量子计算机的研制,且能制造出9 Qubit的通用量子计算机,这是目前已经实现的通用量子计算机的最大规模^[4]。由Hanson和Vandersypen等领导的荷兰量子研究中心(QuTech centre)的目标是5年后实现17 Qubit的通用量子计算机,10年后设计100 Qubit的通用量子计算机^[1]。国际上最顶级的通用量子计算机器件进展距离破译1 024 bit RSA公钥密码所需的千位量子比特差距甚远。

值得注意的是,根据《Nature》2014年9月2日^[5]的报道,研究通用量子计算机的UCSB John Martins团队的20人已经整建制转入Google“建造能解决实际问题的量子计算机”,即John Martins所认为的“30年的奋斗,科学家终于在量子计算找到可达目标”^[1]。John Martins团队不再继续从事通用量子计算机的研究,旨在加速Google

自己研制 1000 Qubit 量子退火芯片即专用量子计算机的进程,需要说明的是,量子退火芯片的原理并不能运行破译公钥密码的 Shor 算法。

3 商业化专用量子计算机研制进展

3.1 专用量子计算机商业化进展

近年来,专用量子计算机商业化进展迅速,其原理是基于量子人工智能独特的量子隧穿效应 (quantum tunneling effect), 完全不同于通用量子计算机,也不能运行破译 RSA 密码的 Shor 算法,对 Shor 算法破译 RSA 密码没有任何直接帮助。

根据《Nature》2011 年 5 月的报道^[6], Lockheed Martin 率先以 1000 万美元(液氮冷却装置价格另计)购置了第一代 128 Qubit 的商业化加拿大专用量子计算机 D-Wave One,用于先进武器设计、F35 战机缺陷分析、开发和测试雷达、航天和航空器系统等。2013 年 5 月, Google 正式宣布以 1500 万美元购买了年初推出的第二代 512 Qubit 商业化专用量子计算机 D-Wave Two,专用量子计算机已正式进入实际商用阶段。

2013 年 8 月底,国内也有研究量子计算的学者与从事神舟七号飞船软件测试的专家共同成功分析了加拿大量子计算机用于飞控软件测试的技术路线可行性。

作为商业化和产业化的一个成熟标志,量子计算机在投资、融资的同时也在发热,一些互联网公司开始投资量子计算机。如 2012 年 10 月,

亚马逊创始人 Jeff Bezos 和美国中情局旗下投资机构 In-Q-Tel 投资了 3 000 万美元给 D-Wave 公司,到 2015 年,高盛集团 (Goldman Sachs)、BDC Capital、Harris & Harris Group 及 DFJ 等开始投资专用量子计算机, D-Wave 获得了新一轮 2 900 万加元(约 2 310 万美元)的融资。而 2013 年黑莓之父 Mike Lazaridis 也投资一亿美金给 Quantum Valley Investment。2014 年, IBM 公司也表示未来 5 年将投入 30 亿美元用于下一代半导体研究,其中也包括量子计算。Microsoft、Intel 和 HP 等也将在量子计算机方面投资。

3.2 商业化专用量子计算机原理

Lockheed Martin 购买的第一代 128 Qubit 商业化加拿大量子计算机 D-Wave One 系统已经成功实现了具有量子隧穿效应的量子退火算法,量子退火与模拟退火示意如图 1 所示。在低温液氮作用下,运行在接近绝对 0℃的-273.145 超导状态,系统功耗为 15.5 kW。D-Wave One 系统采用国际通用做法,基于铌的低温超导性质实现量子比特,电流有顺时针、逆时针以及顺逆同时存在的混合状态,量子比特通过由超导铌合金组成的超导回路 (coupler) 实现。

量子波动使量子具有穿透比它自身能量更高的势垒能力,即量子隧穿效应。量子退火算法利用量子波动产生的量子隧穿效应可以使算法跳出局部亚优解、有望以较大概率逼近全局最优。如图 1 所示,这是与模拟退火及其他众多计算搜索算法相比的一个独特优势。

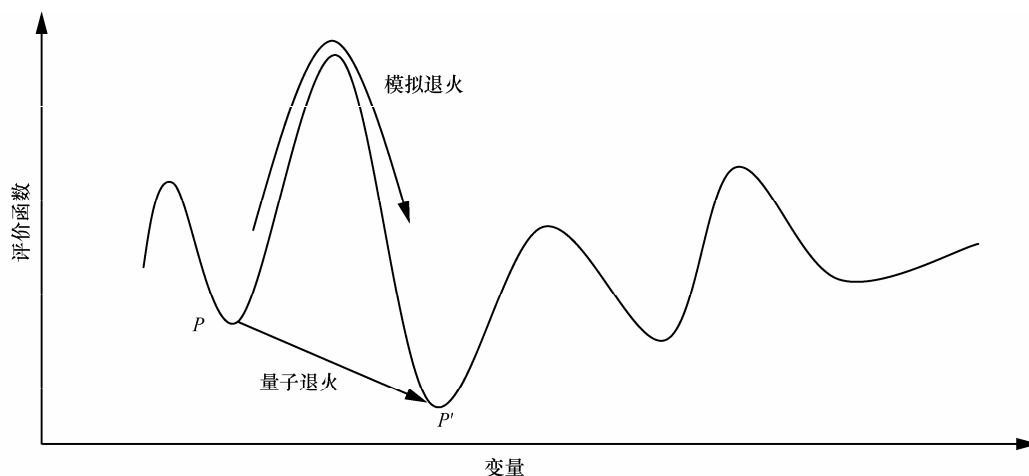


图1 量子退火与模拟退火示意

从量子器件角度分析，实现量子退火难度很大，量子比特可以通过 2 种方式改变自旋方向：通过量子力学的隧穿机制，或者通过经典的热运动。由于加热会破坏量子比特的量子性质，必须使用一种通过隧穿效应使自旋反转的方法。量子的热运动和隧穿效应各自有一个“冻结”时间，量子退火计算依赖于基态和第二低能的态的能量差。对系统施以冷却，直到隧穿和热运动导致的转换都已经停止，量子比特被“冻结”。通过在不同温度下重复这一过程，就能够确定如何使用隧穿效应完成量子退火。

D-Wave One 占地 100 平方英尺，远小于当初的第一台电子计算机，也小于过去的 VAX 系列小型机。整个系统采用 2.4 万个超导约瑟夫森结^[7]，如表 1 所示，充分验证了利用超导约瑟夫森结研究量子计算机小型化成为可能。事实上，D-Wave One 系统的量子处理器实际芯片大小为 1 英寸见方，由美国宇航局喷气推进实验室制造。

D-Wave 芯片组示意^[8-10]如图 2 所示，D-Wave 芯片均采用量子簇矩阵单元设计，每个单元（量子簇）由 8 个量子比特组成。D-Wave One 采用 SFQ 信号分离器来进行寻址，D-Wave Two

表 1 D-Wave One Rainier 芯片和 D-Wave Two Vesuvius 芯片约瑟夫森结				
unit cells	Qubits	couplers	digital to analog converters	Josephson junctions
1	8	16	56	1 500
4	32	72	232	6 000
16 (Rainier)	128	328	968	24 000
64 (Vseuvius)	512	1 416	3 976	96 000
256	2 048	5 896	16 136	384 000

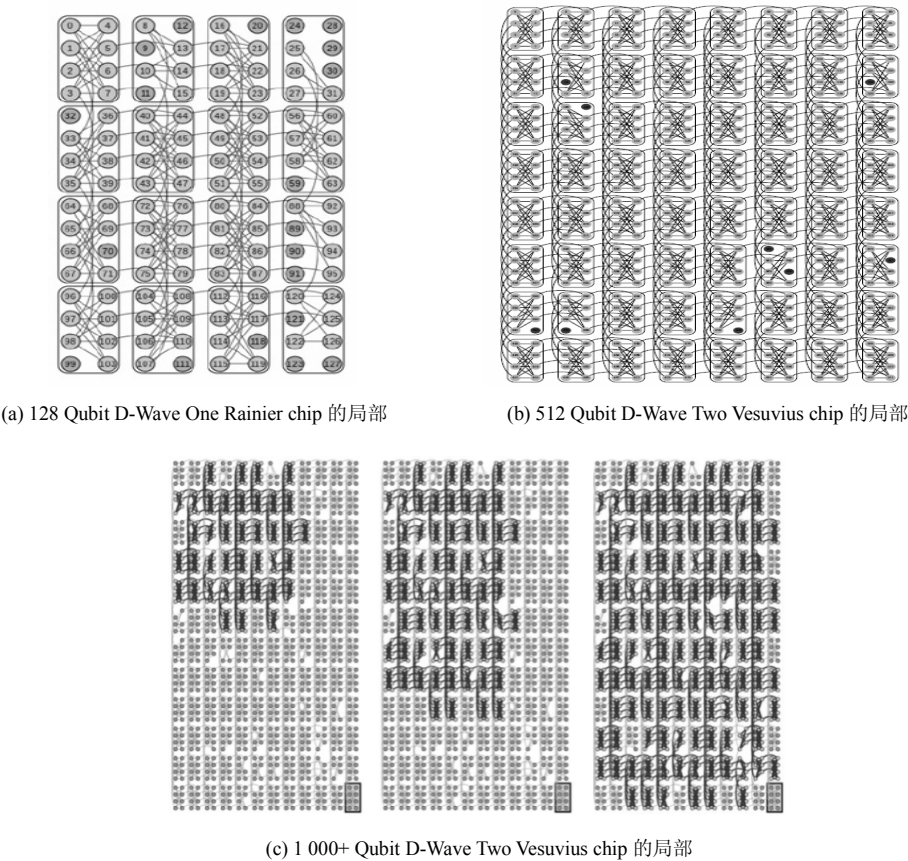


图 2 D-Wave 芯片组示意

采用 XYZ 结构来寻址。对于 2015 年 6 月最新推出的 1 000+ Qubit D-Wave 2X, 其 6 道 $0.25\ \mu\text{m}$ 金属层的平面中共有 12.8 万多个约瑟夫森结 (带超导电极的隧道结), 被认为是目前最复杂的超导集成电路。

仿效摩尔定律, D-Wave 公司的 CTO Geordie Rose 提出了专业量子计算机的发展路线^[11], 如图 3 所示。目前, 16 Qubit (2007 年)、48 Qubit (2008 年)、128 Qubit (2011 年)、512 Qubit (2013 年) 的推出时间均符合预想, 最新的 1 000 Qubit D-Wave 2X 专用量子计算机也已经于 2015 年底推出。

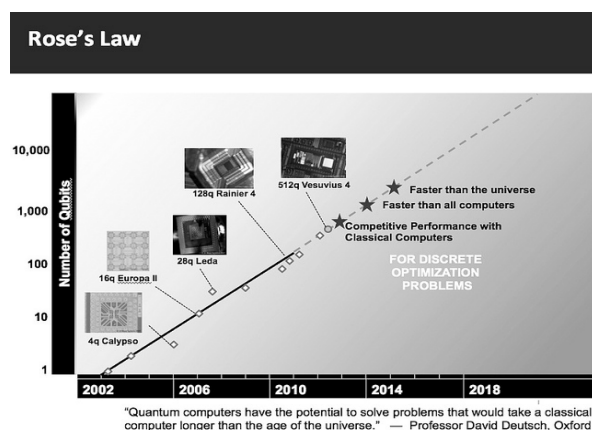


图3 Geordie Rose 的 D-Wave 路线

3.3 D-Wave 的应用领域

尽管 D-Wave 系统是专用量子计算机, 但是本文认为其用途是广泛的, 完全不同于当年电子计算机发展历程中只有单一功能的王安电脑等专用电子计算机^[12]。

D-Wave 公司的设计构思非常巧妙, 利用量子隧穿效应实现了量子退火, 可以将一些组合优化问题求解的 NP 难题在多项式时间解决, 《Nature》认为可广泛用于密码学、人工智能、图像搜索、图像识别和模式分类、金融风险分析、生物信息学、情感分析等众多领域。

本文分析认为, 在科学问题基础性质和理论不清楚的情况下, 即没有多项式时间求解的数学公式可用的情况下, 可利用量子退火增强指数级解空间的搜索能力, 并通过量子隧穿效应跳出局部亚优解, 有望以更大的概率接近全局最优解, 这是与经典的模拟退火算法相比具有很大优势。

通过 Google 和哈佛^[13]2009 年以来利用量子退火芯片在图像处理、蛋白质折叠等方面的成功实验, 业内认为基于量子退火的专用量子计算机对计算机科学非常重要: 有利于解决“有指数级可能性的答案”搜索, 即有望以更大的概率搜索指数级解空间, 逼近全局最优解。《Nature》相关文献报道也对商业化专用量子计算机解决一系列各类组合优化问题抱有很大期望。

3.4 专用量子计算机的关键技术

通用量子计算机的一些关键技术进展同样有助于专用计算机的发展。

事实上, 近年来, 在美国 DARPA 等量子研究计划的支持下, 众多量子计算机的关键技术在发展, 包括美国多家大学依次采用固态量子计算技术突破目前量子计算机所依赖的低温超导, IBM 公司也联合耶鲁大学试图解决量子脱散问题, 提升量子计算机商业化过程中不可避免的量子纠错这一难题。如伦敦大学学院实验物理学家 John Morton 所言, 对量子比特出错率的改进以及代码处理错误能力的提高, 已经极大改变了该领域的发展前景, “可以把焦点放在量子计算机的升级上”^[1]。

John Martinis 的研究则可以提升量子比特相干态维持时间, 使量子退火工作时间更长^[14]。事实上, 根据《Nature》报道, 在 2015 年 4 月已经实现了 5 个量子比特阵列的 1% 纠错成果^[4]。

IEEE^[15]和《Nature》^[16]在 2015 年 3 月 4 日报道了 Google 与 John Martinis 合作的第一个成果: 测试量子退火芯片的纠错性能, 也验证了在 2014 年 9 月的一个猜想——双方的合作旨在利用 John Martinis 团队在量子态控制和芯片可靠性方面的超强实力, 进一步提升量子退火芯片的可靠性和实用性。

事实上, 近年来 John Martinis 团队在《Nature》发表了 surface code 纠错码技术、Xmons 量子比特技术等一系列研究成果^[17,18], 提升了量子逻辑和量子计算的精度; John Martinis 团队将量子态持续时间从 nanoseconds 提升到 30 microseconds, 对于量子计算的实用性而言这是一个很大的飞跃。这一系列成果^[14,17,18]将有助于量子比特相干态维持更久, 使量子退火工作得更好。

2015 年 4 月 29 日, IBM 演示了使用四量子位方形超导量子比特点阵(约四分之一英寸见方)的纠错运算。首次成功实现了检测 2 类量子计算错误, 即比特翻转(bit-flip)和相位翻转(phase-flip)。IBM 认为这是迈向构建大型量子计算机的重要一步^[19]。

3.5 D-Wave 测试情况分析

由于 D-Wave 专用量子计算机的量子人工智能原理完全不同于业内熟悉的通用量子计算机, 业内对其也有一些误解。

1) 误以为能运行 Shor 算法, 认为 D-Wave 的成功将加速破译 RSA 等公钥密码

事实上, D-Wave 专用量子计算机的设计初衷与密码破译无关。

2) 误以为可以求解任意数学问题

事实上, D-Wave 专用量子计算机的设计初衷是基于量子人工智能算法求解组合优化问题, 因此也具有广泛的应用, 模式识别和机器学习等人工智能领域有很多科学问题可以转化为组合优化问题求解。

3) 是否是量子计算机, 有没有量子效应

D-wave 公司的 CEO Vern Brownell 于 2014 年 4 月 21 日接受 IEEE Spectrum 采访, 对加拿大量子计算机的特点做出如下评价: ①加拿大量子计算机的原理不同于已有的量子计算机, 是基于 MIT 的绝热量子计算原理; ②3 个用途是蒙特卡洛模拟、优化问题、深度学习; ③目前能肯定具有 8 Qubit 级别的量子纠缠状态(8 Qubit 是 D-Wave 量子计算机体系结构中的一个基本量子电路单元, 如图 3 所示)。

Matthias Troyer 教授在寻找适用于量子计算的杀手级应用的同时, 也一直参与、跟踪 D-Wave 的各项测试研究^[1]。2014 年 2 月, Matthias Troyer 教授等在《Nature Physics》撰文^[8], 通过 108 Qubit D-Wave 的伊辛模型测试实验, 证明了 D-Wave 量子计算机确实具备量子效应。

3.6 与传统数学方法及智能算法的比较

2015 年 12 月, Google 量子人工智能实验室主任 Harmut Neven 及其团队^[10]声明在一个涉及近 1 000 个二进制变量的问题实例上, 与单处理器传统计算机对比, D-Wave 得到了 1 亿倍的提

速。需要说明的是, 所测试的问题是一些特定的、精心设计的问题, 并非通用问题。

尽管如此, 本文分析认为, 这个测试可以说明 D-Wave 专业量子计算机的搜索速率非常快, 有利于算法的问题求解。

通常情况下, 智能算法适合在科学性质未知情况下的问题求解, 此时传统数学方法难以奏效, 即没有多项式时间求解的数学公式。此时, 往往指数级解空间的解分布和解结构未知, 即求解成功率具有随机性, 初始点选择、搜索策略及单位时间的搜索速率、搜索覆盖范围是影响求解的几个关键因素。

加之量子隧穿效应的作用, D-Wave 从其量子人工智能原理上说, 有望跳出局部亚优解, 扩大解空间搜索范围, 有助于获得较优的解。对于组合优化问题求解, 单位时间内搜索逼近全局最优解的概率应该超过传统智能算法。

4 Shor 算法的量子器件约束分析

需要重视 Shor 算法对 RSA 密码攻击所面临的通用量子计算机器件约束问题。

如前文分析, 通用量子计算机器件进展缓慢, 短期内破译 1 024 bit 的 RSA 公钥密码所需的千位 Qubit 差距极大。因此可以判断, 在通用量子计算机的进展情况下, 现代密码依旧是安全的, 二代身份证、电子政务 CA 系统中涉及的 RSA 和 ECC 算法公钥密码也是安全的。

尽管 Shor 算法攻击 RSA 密码在理论上是成熟的, 但对量子比特 Qubit 需求较大, 从目前通用量子计算机实际器件进展而言, 需要进一步评估其可行性、现实性。

事实上, 采用量子器件实现 Shor 算法破译 RSA 密码, 理论上第一量子寄存器需要的量子比特数 $n_1 = 2\lceil \lg N \rceil$, 第二量子寄存器需要的量子比特数 $n_2 = \lceil \lg N \rceil$, N 为 RSA 密码中需要分解的大数。记 $L = \lg N$, 量子器件的空间复杂度为 $(2L, L)$, 时间复杂度为 $T = O(L^3)$ 。如破解 1 024 bit 的 RSA, 需要 2 048 量子比特 Qubit。

目前, 国内外文献表明, Shor 算法的改进算法很多, 但是第一量子寄存器和第二量子寄存器还不能做到全部都降低到 L 规模之下, 破解 1 024 bit 的

RSA 不仅仅需要千位 Qubit 量子计算机，也需要高精度和长时间的量子态维系能力等。而目前通用量子计算机的最大规模是 9 Qubit，实际器件进展距离破译 RSA 密码的理论需求比较遥远。

因此，需要考虑在通用量子计算机的器件受条件限制的实际情况，研究公钥密码 RSA 的小 Qubit 量子计算攻击方法，降低对通用量子计算机的器件要求。

目前，最乐观的通用量子计算机器件进展情况，可以考虑荷兰量子研究中心提出的 10 年后设计 100 Qubit 通用量子计算机这一背景。Shor 算法攻击 RSA 等公钥密码的可行性研究，建议以此约束条件为前提。

因此，如何改进 Shor 算法，使第一量子寄存器和第二量子寄存器从现有理论设计要求的 1 000~2 000 Qubit 降低至 100 Qubit 以下，是一个业内还没有考虑的实际问题。

5 专用量子计算机对信息安全的影响分析

以量子人工智能为基础的专用量子计算机作为下一代战略计算（NSCI）的核心思想，对机器学习和互联网内容分析能力有重大影响。

斯诺登事件之后，应该重视专用量子计算机机器的学习能力对互联网大数据内容分析和行为隐私分析所构成的潜在威胁。

5.1 专业量子计算机对机器学习能力的影响

需要重视加拿大商用量子计算机的搜索能力对量子机器学习的影响。

2013 年 5 月，Google 正式宣布购买 512 Qubit 加拿大量子计算机 D-Wave Two 的同时，与 NASA（National Aeronautics and Space Administration）Ames 中心联合成立量子人工智能实验室（QuAIL，Quantum Artificial Intelligence Lab）。Google 希望量子计算技术可以推动机器学习领域的发展，在疾病治疗、跟踪气候变化和开发语音识别技术方面发挥作用，更好地解决空中交通管制、机器人、任务规划和调度等领域的问题。NASA 则利用量子计算机模拟太空气象、行星大气层、星系碰撞，研究磁动流体力学、超音速飞行器以及处理大量数据等。

事实上，早在 2009 年，Google 图像识别技

术组负责人 Hartmut Neven 在 Google Research 博客公布了 Google 近年来正在研究 D-Wave 量子退火芯片用于图像搜索，核心算法采用 MIT 物理系 Edward Farhi 发现的 quantum adiabatic 算法。在神经信息处理系统（NIPS）2009 大会上，Google 演示了此项研究的进展，通过测试识别 2 万张图片中的汽车，证明了该研究的效果优于传统软件。

SanDiego 超算中心研究员 Allan Snabelly 曾经使用过 D-Wave 系统的算法，对其进行了评价：对计算机科学非常重要；有利于解决“有指数级可能性的答案”搜索。2013 年 10 月，国内有专家评论：如果能解决图像处理问题，也是很有意义的。

2012 年 8 月，哈佛大学的一个研究团队利用 D-Wave One 解决了最大的蛋白质折叠问题。Google 进一步利用 D-Wave 量子计算机应用于无人驾驶汽车的研究，期望以更加接近人脑的方式对障碍物进行判断，提供更好的导航。

Google 在 2014 年 9 月 2 日宣布与 John Martinis 团队合作的同时，也引进了一批人工智能专家，如 Toronto 的 Deep Neural Network 专家 Geoff Hinton，并收购其公司 DNNresearch。Google QuAIL 的研究员 Masoud Mohseni 认为量子计算机适合处理互联网海量数据。著名信息安全专家王育民教授分析认为 Google 此举有助于互联网内容分析。

2015 年，Google 量子人工智能实验室主任 Hartmut Neven 判断，10 年后将是量子机器学习的天下。

5.2 专业量子计算机成为新一代计算思想

从 2015 年 9 月起，Lockheed Martin、Google 和 NASA 的 QAIL 陆续与 D-wave 签署多年合作协议并升级到最新 1 000+Qubit D-Wave 2X。2015 年 11 月，美国能源部 DOE 下属的 2 个核武器国家实验室之一 Los Alamos 确定在 2016 年安装 1 000+Qubit D-Wave 2X，将量子退火作为响应美国国家战略计算计划的重要一步（power step）。此前，Los Alamos 已经取消了对量子密码的研究。

Alamos 国家实验室选择将量子退火作为新一代计算方法，意欲突破传统计算已经达到的瓶颈（摩尔定律：能耗随计算规模和计算性能指数

级增长)。旨在作为重要一步,响应奥巴马2015年7月29日颁布的“美国国家战略计算计划”。

NSCI的3个领导机构是美国国家自然科学基金委(NSF, National Natural Science Foundation)、能源部(DOE, Department of Energy)、国防部(DOD, Department of Defense);基础研究机构是IARPA(Intelligence Advanced Research Projects Activity)、NIST(National Institute of Standards and Technology);实施机构包括FBI(Federal Bureau of Investigation)、NASA、海洋与大气署等。

白宫网站公布NSCI的几条建设目标如下。

第一条:Exascale(百亿亿次计算,百倍现在的10 Petaflop, 30倍天河二的运算速度);

第二条:用于数据分析计算(包括后续从政府、工业界等搜集的数据);

第三条:15年内突破目前的计算限制,实现后摩尔定律(the “post-Moore’s Law era”);

第四条、第五条略。

加拿大专用量子计算机及其量子退火算法符合第二条、第三条要求。

2015年9月底,最新的1 000 + Qubit D-wave 2X 安装在NASA Ames 中心的QAIL之后,IEEE Spectrum 随即在10月5日也专门刊文讨论需要多少能耗(How much power will quantum computing need?).但是,事实上D-Wave 2X 能耗还是在15 kW 以下,与512 Qubit D-Wave Two 相比没有增长。和传统的电子计算机相比,其能耗是很大的优势。

关于传统计算已经达到的瓶颈,Alamos 国家实验室的几个部门(理论仿真计算部和实验武器物理部等)都一致认为:“传统计算从每瓦能耗可达的计算规模和计算性能来看,已经到了尽头。需要研究新的技术来支持未来需求”。

Alamos 国家实验室认为:选择研究和优化量子退火并使之作为新方法的基础,以应对未来的棘手问题,是重要而有力的一步。

5.3 量子认知进展

2015年,加州大学圣芭芭拉分校物理学家Matthew P.A. Fisher 首次通过核自旋给出了人脑认知思维可能是一种量子效应的结果,再一次把

大脑量子计算机化推到了世人面前。Matthew 的工作之所以这么引人注目,就在于他对于人们关于在人脑潮湿、温热的环境下如何能保持量子相干态的疑虑有了初步的科学解释^[20]。当然,现在讲人脑其实是一个量子计算机还为时过早。Matthew 的工作也引起了部分争议,比如来自生命科学领域的学者认为,目前神经科学已经取得了丰硕成果,解决了很多问题,没有必要从量子力学的角度来理解人脑的运行和思维机理。

另一方面,Matthew 的工作也得到了来自各个领域专家学者的支持,比如生命科学领域的施一公教授,就在其最近的一次研究中提到以后可能需要从量子的层面去理解人脑的思维与意识。还有著名的量子信息科学家加州理工大学的John Preskill 教授认为该项跨学科的研究非常有价值,事实上,Matthew 下一步的工作,正是联合来自神经科学、化学等领域的科学家进一步从微观领域入手研究量子力学和人脑思维之间的联系。可以预见的是,目前人类关于自己大脑的科学认识还远远达不到令人满意的程度,基于目前的神经科学,还有很多关于大脑思维和意识存储的未解之谜。

除了从微观领域出发开展人脑运行的量子机制,目前也出现了基于量子力学原理建模人脑思维和判断等认知过程。2014年,俄亥俄州立大学Wang 等^[21]学者提出了量子问题等价性原理(quantum question equality),用来解释人脑对一些顺序相关问题的反应,用来支撑人脑思维是遵从量子逻辑而不是经典的概率论这一假说。同时,文章指出,人脑对很多问题的反应回答和问题的提问顺序有关,换句话说,当先回答A问题,再回答B问题时,会受到刚才回答A问题思维的影响。当然这里设计的问题A和问题B是有一定的相关性的,他们认为这和量子力学里某些测量算子的不可对易性紧密相关,为此提出了用人脑在某些问题下的基于量子理论的概率思维模型。2015年,Busemeyer 和 Wang^[22]给出了关于量子理论中的完备性理论(complementarity)和叠加原理(superposition)在认知心理学中的应用。

从量子科学的角度出发,开展人脑认知研究,不失为一个重要并新颖的途径。另外,多学科交

又融合的过程，也许会对未来量子人工智能领域带来积极的促进作用，进而也会给量子机器学习以及与此相关的大数据网络带来深远影响。

5.4 专用量子计算机对密码学的影响

量子时代的密码学研究可以概括为以下几个特点。

1) 无论通用量子计算机还是专用量子计算机，都未涉及密码设计。

2) 已有的量子时代的密码学研究包括量子密码、抗量子密码均为国外提出。

3) 目前量子计算对现代密码的攻击均由贝尔实验室提出。

其一，1996年提出的 Grover 算法，其搜索复杂度是 $O(\sqrt{N})$ （相当于把所破译密码的密钥长度减少一半），对公钥密码不构成致命威胁。

其二，1994年发明的 Shor 算法，其扩展算法能在多项式时间内破译可以转换成广义离散傅里叶变换的公钥密码，包括 RSA 等。

问题之一：除了 Shor 算法对 RSA 等公钥密码破译，量子时代还能攻击哪些密码算法？是否能形成普适性的攻击算法？目前还没有结论。

问题之二：Grover 算法能否找到对公钥密码有效的攻击途径？目前也还没有结论。

由于通用量子计算机的器件进展缓慢，尚未具有实用性。因此，探索采用商业化专用量子计算机用于密码设计和分析，具有现实意义。事实上，尽管量子人工智能算法已经应用于诸多组合优化问题，比如旅行商问题^[23,24]、图像识别问题^[25]、蛋白质折叠问题^[13]等，但有关密码设计和分析的问题还未涉及。

2014年12月2日，Matthias Troyer 教授在 Google 做了一个主题为“High performance quantum computing”的报告，提出了四大量子计算研究方向：解码与编码、量子化学和材料模拟、处理线性问题以及机器学习。Matthias Troyer 认为，为量子计算机寻找新的杀手级应用是一个挑战。

需要中国学者从量子计算、量子人工智能的角度研究商业化专用量子计算机对密码分析和设计的理论和技术，提出国外尚未开展的量子计算密码研究，主要有以下2个方面。

1) 重视加拿大商用量子计算机的搜索能力对现代密码攻击的影响

需要研究论证 D-Wave One 系统对密码系统实施穷举破译的可能性。D-Wave 系统利用量子隧穿效应实现了量子退火，可以将组合优化问题求解的 NP 难题在多项式时间解决，有助于解决指数级解空间的搜索问题，预计可以减少密码攻击所需搜索空间的量级^[12]。

2) 重视加拿大商用量子计算机的搜索能力对现代密码设计的影响

现代密码设计大多基于一定的数学难题使安全性更高。在某些密码函数设计中，如果密码性质、结构、分布等基本性质不清楚，且密码函数的参数解空间达到指数级，传统密码设计将遭遇瓶颈。同时，利用穷举法或传统优化算法搜索这类密码函数的参数犹如“大海捞针”，会在指数级空间中陷入“止步不前”的现象。

因此，加拿大专业量子计算机 D-Wave 的核心算法量子退火，可以考虑作为新的计算搜索方法，利用量子波动产生量子隧穿效应跳出局部亚优解，增强系统指数级解空间搜索能力，并以较大概率逼近全局最优解，有望突破传统瓶颈。

而且，Google 的测试也已表明 D-Wave 的搜索速度极快这一巨大优势。从理论上说，结合隧穿效应，针对传统计算机无法有效解决的指数级空间搜索难题，D-Wave 商用量子计算机的搜索覆盖面和搜索速度会更好。

通过初步性实验，利用量子退火设计多指标安全密码函数，得到的参数结果优于 IEEE Transactions on Information Theory 期刊上发布的由传统数学理论构造的最好结果。这也在一定程度上初步验证了量子计算密码的可行性。

6 量子纠错对量子计算机实用化的推动

安全可靠的量子信息处理过程包括通用量子计算机、D-Wave 那样的专用量子计算机以及量子通信，这些都离不开差错控制。事实上，目前限制通用量子计算机进一步发展的一个重要原因就是量子计算过程中的差错控制。

这包含2个方面的工作：一方面，提高量子逻辑器件本身的操控精度；另一方面，由于量子

态本身非常敏感和脆弱,必须设计有效的纠错机制来克服外界噪声带来的退相干影响,从而实现量子信息的保护。对于后者,目前广泛采用的是和经典信息处理同样的思路,即通过差错编码来对抗噪声的影响。事实上,自从 Shor 于 20 世纪 90 年代初提出量子纠错编码的思想以来,量子纠错码的研究获得了长足的进步,几乎所有在经典信息领域应用的纠错编码机制都被成功地引入到量子领域中来,这其中也包括本文作者王云江提出的量子稀疏图码的译码算法以及和国外的本领域专家学者提出的量子级联编码思想。

近些年的理论研究表明,在量子差错控制领域,一方面需要借鉴经典编码理论上的经验和成功理论,开展量子码的研究,构造出资源消耗和性能均达到较优的量子纠错码,比如采用拓扑结构和图论的思想设计量子纠错码^[26,27]。另一方面,应该进一步意识到量子纠错码和经典纠错码的不同之处,开展与具体的量子计算的物理实现机制相结合的纠错体系设计,实现量子编码与相应的物理实现深度融合,这样才能更好地为量子计算得到量身定做的差错控制方案。前文所述的 UCSB 的 Martinis 课题组基于超导量子线路模型所采用的 surface code,就是利用了 surface code 的纠错机制和超导量子比特的邻接物理模型的匹配性^[4]。2015 年,IBM 沃森研究中心也提出了类似的量子差错控制方案,并通过了物理实验的验证^[19]。值得指出的是,上面的量子差错控制方案虽然是基于通用量子计算机为背景提出的,事实上,对于类似 D-Wave 的专用量子计算机,上面的量子差错控制思想仍然适用,比如南加州大学的 Lidar 课题组针对目前已经商用的 D-Wave 量子计算机,利用 344 个超导量子比特实现了量子退火纠错,大大提高了 D-Wave 的运算可靠度^[28]。

从上面的研究可以看出,近些年来有关量子差错控制方面的研究频频出现在国际顶级的期刊上,是量子信息与量子计算领域中的重要方向,对可靠量子信息处理的出现起到至关重要的作用。因此,一方面需要加强对量子计算的应用研究,特别是对目前已有的量子计算技术(如 D-Wave 量子计算机)的应用研究;另一方面,为了保证量子计算的实现(包括 D-Wave 量子计算机的进一步提升),也需要

加强量子计算的差错控制研究。这其中值得关注 2 个方向:一是采用新的原理和方法来设计好的量子纠错码;二是开展与物理原理和量子计算的物理模型相融合的量子差错控制机制研究。

7 结束语

受到量子器件进展的限制,通用量子计算机距离破译电子政务中 RSA 密码所需要的千位 Qubit 遥遥无期。如果采用 Shor 算法破译实用化的 RSA 等公钥密码,首先需要考虑对 Shor 算法的改进,同时降低第一量子寄存器和第二量子寄存器,使之对器件的要求降低到百位 Qubit。目前,现代密码还是安全的,量子计算机的器件进展还远不能投入实际运行,无法破译现代密码。

量子计算机的商业化还涉及到量子纠错、量子计算模型和理论及软件方法等一系列关键理论和技术。

需要重视商业化专用量子计算机对密码学和互联网大数据时代信息安全的影响。商业化专用量子计算机实现了量子人工智能算法,可以成功应用于大量的可以转化为组合优化的机器学习、模式识别等科学问题,不能忽视其对互联网大数据时代的信息安全形成的挑战。

目前,无论是通用量子计算机还是商业化专用量子计算机,都没有涉及密码设计,且有关量子时代的密码研究均为国外提出。

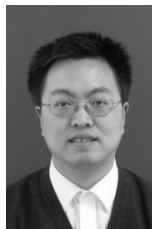
展望未来,将考虑采用商业化专用量子计算机的理论。中国学者从量子计算、量子人工智能的角度在国际上率先提出了量子计算密码的研究,在国际上首次考虑了量子计算对密码设计的作用,同时也会开辟不同于 Shor 算法的量子计算密码破译之路。

参考文献:

- [1] GIBNEY E. Physics:quantum computer quest[EB/OL]. <http://www.nature.com/news/physics-quantum-computer-quest-1.16457#b4>.
- [2] MARIANTONI M, WANG H, YAMAMOTO T, et al. Implementing the quantum von neumann architecture with superconducting circuits[J]. Science, 2011, 334(6052): 61-65.
- [3] ERIK L, BAREDNS R, CHEN Y, et al. Computing prime factors with a Josephson phase qubit quantum processor[J]. Nature Physics, 2012, 8(10): 719-723.
- [4] BAREDNS R, KELLY J, MEGRANT A, et al. Superconducting quantum circuits at the surface code threshold for fault tolerance[J]. Nature, 2014, 508(7497): 500-503.

- [5] Seven days: 5-11 september 2014[EB/OL]. <http://www.nature.com/news/seven-days-5-11-september-2014-1.15881>.
- [6] JOHNSON M W, AMIN M H, GILDERT S, et al. Quantum annealing with manufactured spins[J]. Nature, 2011, 473(7346): 194-198.
- [7] LUCAS B. Adiabatic quantum computing[R/OL]. <http://www.hqcc.unical.it/hqc2012/pdfs/lucas.pdf>.
- [8] BOIXO S, RONNOW T F, ISAKOV S V, et al. Evidence for quantum annealing with more than one hundred qubits[J]. Nature Physics, 2014, 10(3): 218-224.
- [9] RONNOW T F, WANG Z, JOB J. Defining and detecting quantum speedup[J]. Science, 2014, 345(6195):420-424.
- [10] DENCHEV V S, BOIXO S, ISAKOV S V, et al. What is the computational value of finite range tunneling[EB/OL]. <http://arxiv.org/pdf/1512.02206v4.pdf>.
- [11] Rose's law for quantum computers[EB/OL]. <http://www.33rdsquare.com/2012/10/roser-law-for-quantum-computers.html>.
- [12] 王潮, 张焕国. 加拿大商用量子计算机对密码学的影响[J]. 信息安全与通信保密, 2012, 2(35): 31-32.
WANG C, ZHANG H G. The influence of Canadian commercial quantum computer in cryptography[J]. China Information Security, 2012, 2(35): 31-32.
- [13] PERDOMO-ORTIZ A, DICKSON N, DREW-BROOK M, et al. Finding low-energy conformations of lattice protein models by quantum annealing[J]. Scientific Reports, 2012, 2(8):571.
- [14] HSU J. Google's first quantum computer will build on D-Wave's approach[EB/OL].<http://spectrum.ieee.org/tech-talk/computing/hardware/googles-first-quantum-computer-will-build-on-dwaves-approach>.
- [15] HSU J. Google tests first error correction in quantum computing[EB/OL].http://spectrum.ieee.org/tech-talk/computing/hardware/google-tests-first-error-correction-in-quantum-computing/?utm_source=techart&utm_medium=email&utm_campaign=030515.
- [16] KELLY J, BARENDT R, FWLER A G, et al. State preservation by repetitive error detection in a superconducting quantum circuit[J]. Nature, 2015, 519(7541):66-69.
- [17] CHOW J M, BAMBETTA J M, MAGESAN E, et al. Implementing a strand of a scalable fault-tolerant quantum computing fabric[J]. Nature Communications, 2013, 5: 4015.
- [18] BARENDT R, KELLY J, MEGRANT A, et al. Superconducting quantum circuits at the surface code threshold for fault tolerance[J]. Nature, 2014, 508(7497): 500-503.
- [19] CORCOLES A D, MAGESAN E, SRINIVASAN S J, et al. Demonstration of a quantum error detection code using a square lattice of four superconducting qubits[J]. Nature Communications, 2015, 6: 6979.
- [20] MATTHEW P A. Quantum cognition: the possibility of processing with nuclear spins in the brain[J]. Annals of Physics, 2015, 362: 593-602.
- [21] ZHENG W, TYLER S, RICHARD M S, et al. Context effects produced by question orders reveal quantum nature of human judgments[J]. Proceedings of The National Academy of Sciences of the United States of America, 2014, 111(26):9431-9436.
- [22] BUSEMEYER J R, ZHENG W. What is quantum cognition, and how is it applied to psychology[J]. APS Association for Psychological Science, 2015, 24(3):163-169.
- [23] MARTONÁK R, SANTORO G E, TOSATTI E. Quantum annealing of the traveling salesman problem[J]. Physical Review E Statistical Nonlinear & Soft Matter Physics, 2004, 70(5):057701.
- [24] CHEN H, KONG X, CHONG B, et al. Experimental demonstration of a quantum annealing algorithm for the traveling salesman problem in a nuclear-magnetic-resonance quantum simulator[J]. Physical Review A, 2011, 83(3):6541-6548.
- [25] NEVEN H, ROSE G, MACREADY W G. Image recognition with an adiabatic quantum computer[EB/OL]. <http://arxiv.org/pdf/0804.4457v1.pdf>.
- [26] NIGG D, MULLER M, MARTINEZ E A, et al. Quantum computations on a topologically encoded qubit[J]. Science, 2014, 345(6194): 302-305.
- [27] BELL B A, HERRERA-MART D A, TAMEM S D, et al. Experimental demonstration of a graph state quantum error-correction code[J]. Nature Communications, 2014, 5(4): 3658.
- [28] PUDENZ K L, ALBASH T, LIDAR D A. Error-corrected quantum annealing with hundreds of qubits[J]. Nature Communications, 2014, 5(2): 163-180.

作者简介:



王潮 (1971-), 男, 江苏镇江人, 上海大学教授、博士生导师, 主要研究方向为网络信息安全与椭圆曲线密码学、量子计算密码、社会网络等。



王云江 (1980-), 男, 河南新乡人, 博士, 西安电子科技大学副教授, 主要研究方向为量子信息与量子计算, 涉及量子差错控制、量子智能与量子认知、量子计算、量子通信等。



胡风 (1991-), 男, 浙江温州人, 上海大学博士生, 主要研究方向为信息安全、量子计算密码、社会网络。