新量子技术时代下的信息安全

张亮亮[1,2] 张翌维[2] 梁 洁[2] 孙瑞一[2] 王新安[1]
(北京大学信息科学技术学院 北京 100871)[1] (国民技术股份有限公司博士后科研工作站 深圳 518057)[2]

摘 要 量子技术将在未来深刻影响密码学以及信息安全行业。可以利用上千个量子比特运行量子算法的通用量子计算机将直接威胁信息安全基础算法,导致当前广泛使用的RSA等公钥密码被破解,也会使分组密码算法的密码强度减半。量子通信中量子密钥分发的实施会改变传统保密通信的物理结构。这些重大应用价值也是发展量子技术的驱动力。结合当前一些关于量子技术的热点新闻,从量子计算和量子通信两个方面分别综述了量子技术对信息安全技术的影响。同时简要介绍了这些技术的最新发展现状,包括通用型和专用型量子计算机的发展、量子密钥分发技术实验室环境的进展以及天地一体化量子通信网络的发展状况等。最后对信息安全技术的未来形态做了思考和总结。未来量子技术将会与现有各种技术深度融合,共同存在。

关键词 量子计算,量子通信,密码学,信息安全
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.07.001

Information Security in New Quantum Technology Age

ZHANG Liang-liang[1,2] ZHANG Yi-wei[2] LIANG Jie[2] SUN Rui-yi[2] WANG Xin-an[1]
(School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China)[1]
(Post-doctoral Scientific Research Station, Nationz Technologies Inc., Shenzhen 518057, China)[2]

Abstract Quantum technologies should have a profound impact on cryptography and information security industry in the coming age. The general quantum computers, which can run quantum algorithms by thousands of qubits, posing a serious threat to the fundamental algorithms of information security. The famous RSA algorithm and other public key ciphers will be broken and the cryptographic strength of block ciphers will be halved. The implementation of the quantum key distribution in quantum communication must alter the physical construction of traditional secure communication. These important application values are also the driving factors for developing quantum technologies. Combining with the current hot news of quantum technologies, the effects to information security technology were reviewed from two perspectives, quantum computation and quantum communication, respectively. Meanwhile, the status of the new developments in these technologies was briefly introduced, including the advances of general and specific quantum computers, the progress of quantum key distribution made in laboratory conditions and the state of development of the space-ground quantum communication network. In the end, the future form of information security technology was given with a summary. In future, the quantum technologies will deeply integrate and co-exist with various existing technologies.

Keywords Quantum computation, Quantum communication, Cryptography, Information security

当今信息技术时代具有划时代意义的产物是晶体管和集成电路相关制造技术的发明。这些发明让个人计算机和各种消费类数码产品成为了人们日常生活中必不可少的工具,进而也促进了互联网的发展。以对称密码算法和公钥密码算法为基础的信息安全技术保障了在互联网上进行的通信和金融交易等活动的安全,使人们可以放心地享受信息技术所带来的安全与便利[1]。这一切的起点便是量子力学。量子力学是研究微观尺度粒子运动规律的物理理论,利用量子力学原理,人们发展了半导体物理理论,成功地制造出了晶体管和集成电路[2-3]。随着量子力学相关调控技术的不断发展,例如对于量子计算和量子通信的深入研究,未来信息社会的形态将会发生巨大的变化。人们将享受到新量子技术带来的便利,同时,信息安全技术将会面临新的机遇和挑战[4-5]。本文将着重从量子计算和量子通信这两个方面讨论新的量子技术对信息

到稿日期:2017-03-02 返修日期:2017-04-24 本文受国家核高基科技重大专项(2014ZX01032-204),深圳市重点实验室基金(深发改[2013]993号)资助。

张亮亮(1986-),男,博士,主要研究方向为计算物理和密码芯片分析技术,E-mail:zhang.liangliang@nationz.com.cn(通信作者);张翌维(1980-),男,博士,高级工程师,主要研究方向为密码芯片的安全分析与VLSI设计技术;梁 洁(1961-),男,高级工程师,主要研究方向为集成电路设计与半导体工艺技术;孙瑞一(1980-),女,博士,主要研究方向为安全平台架构设计;王新安(1963-),男,教授,主要研究方向为系统集成芯片设计与设计方法学、阵列处理器架构与设计。

安全的影响。另外，最近许多关于量子技术的新闻报道也让越来越多的普通人开始关注和讨论“量子”，例如谷歌称其量子计算机速度比传统计算机快 1 亿倍[6]；IBM 提供了量子计算机的云平台[7]；我国要建设具有量子保密通信功能的“京沪干线”，以及量子卫星“墨子号”发射成功等[8-9]。本文也将对这些新闻背后所涉及的量子技术概念和现状进行相关解释和说明。

1 新量子技术时代

随着技术的不断发展，已经涌现出许多新颖、实用并具有巨大应用潜力的量子技术[4-5]，其中包括量子时钟、量子成像、量子传感和测量、量子计算以及量子通信等。这些新的量子技术提供的性能或解决方案一旦成熟，将迎来“第二次量子技术革命”，并给整个社会带来巨大影响。上述量子技术中，与信息安全关系比较密切的是量子计算和量子通信。

1.1 发展量子计算的意义

摩尔定律预测，在成本不变的情况下，每隔 18～24 个月，集成电路芯片上可容纳的晶体管数目会增加一倍。摩尔定律在过去大约 50 年内相当有效，但随着晶体管尺寸不断缩小到接近几个或十几个原子大小时，当前工艺下的半导体器件将由于散热和漏电等问题无法正常工作[10-11]。若要继续提升计算能力，需要另辟蹊径，其中可以运行量子算法的量子计算机是很有希望的路径，可以继续满足人们对计算能力的需求。

量子计算机对信息安全的一个重大影响是，一旦通用型量子计算机可处理的量子比特数目达到一定规模（见 2.3 节），现有的公钥密码体制将会被量子 Shor 算法轻而易举地攻破[12]，现在互联网上进行的通信和交易等活动的安全将会受到直接的威胁，其解决办法是将这些算法更换为可以抵抗量子计算攻击的密码算法[13]。

1.2 发展量子通信的意义

量子通信技术中比较成熟的应用是量子密钥分发及其相关技术[14-17]。传统密码技术的一个困难是无法真正保证通信双方共享的密钥是绝对安全的。因为经典的比特十分容易复制且不易被察觉，所以通信双方无法真正确认共享密钥是否已被恶意攻击者获取。

利用光子的量子特性，在传输量子信息时，一旦受到窃听和破坏，必然会引入干扰，这样就可以通过物理的方式将攻击行为检测出来，保证信息传输的安全，从根本上解决点对点的密钥分发问题，确保点对点通信的安全。因此，量子密钥分发有时也被称为量子密码（注意与可以抵抗量子计算攻击的后量子密码算法区分）[13,18]。量子密钥分发是可证明安全的[19-21]，这是经典的保密通信无法做到的，因此量子密钥分发是未来保密通信的重要发展方向。

1.3 各国对量子技术的投入和支持

包括量子计算和量子通信在内的量子技术，具有现有经典技术无法比拟的“量子优势”（quantum superiority）[5,22]，将成为未来科技、国防、经济战略的制高点和驱动力。世界各国都在予以极大关注和重视，不断推出相关扶持政策，增加科研投入。2013 年底，英国国家量子技术规划（National Quantum Technologies Programme）初期计划在 5 年内投入 2.7 亿英镑来将其量子物理研究成果转换为商业化产品[23-24]。同时，英国国防科技实验室（Defence Science and Technology Laboratory）也将投入大约 3 千万英镑来开发与国防和安全相关的量子技术[5]。欧盟委员会计划在 2018 年开始一个十年期的量子技术“旗舰工程”（Flagship project），投资总额高达 10 亿欧元[25]。在美国，包括国防部、能源部、国家自然科学基金委员会在内的各大联邦机构在量子信息相关领域每年总计投入大约 2 亿美元[4]。以中国科技大学和中国科学院为代表的中国学术机构在量子通信领域处于世界领先水平，并且国家十三五规划（2016 年—2020 年）中提到量子通信将作为体现国家战略意图的重大科技项目进行部署。此外，包括加拿大、澳大利亚、荷兰、日本等在内的世界其他主流国家都在不遗余力地向量子技术相关领域进行投入。量子技术领域已经形成了全球性的竞争态势。

2 量子计算

利用量子比特的特性来进行计算的方式被称为量子计算。量子计算在很多方面都与经典数字计算机的计算方式不同，这使得量子计算机在某些方面具有巨大的优势。

2.1 量子比特及其特性

众所周知，经典的数字系统使用二进制的比特来编码信息，每个比特可以取值为 0 或者 1，但是不能同时取 0 和 1。量子技术中采用的是量子比特（qubit）。量子比特不但可以表示 0 或者 1，而且可以同时有 0 的成分和 1 的成分，形成所谓的“叠加态”，如表 1 所列。当量子比特状态表达式中的某些系数为 0，则可以表示经典比特。通常在处理量子比特时可以同时对 0 和 1 进行操作，这种操作具有内在的并行特性，可以加快运算的速度。n 个量子比特可以同时保存的状态个数为 2^n，这种指数增长的规律正是量子计算威力的来源。另外，多个量子比特之间的量子纠缠是量子系统的重要特性，也是一种十分重要的计算资源，一些经典方式无法实现的效果，如隐形传态，可以利用量子纠缠来实现。实验上实现量子比特的方式有多种，例如超导环路、囚禁离子、量子点、拓扑量子比特和金刚石空位等[26]，这些方式各有利弊，都仍在不断发展。

表 1 比特和量子比特的对比

比特类型与数量	可以表示的状态
1 个比特	0 或 1
2 个比特	00 或 01 或 10 或 11
1 个量子比特	0，1 的线性组合，表示为 $\alpha\|0\rangle+\beta\|1\rangle$
2 个量子比特	00，01，10 和 11 的线性组合，表示为 $\alpha_{00}\|00\rangle+\alpha_{01}\|01\rangle+\alpha_{10}\|10\rangle+\alpha_{11}\|11\rangle$

2.2 量子计算机的类型

设计量子计算机的技术路线主要有两种类型：通用型和专用型，这两种类型的典型代表的对比如表 2 所列[27-28]。

经典数字计算机的基础部件是逻辑门电路，通过对比特进行逻辑运算来实现计算功能。与这种架构类似，对于量子比特来说，其也存在相应的量子逻辑门[12]。量子芯片上如果能制备出所需的量子比特以及对量子比特进行操作和运算的量子逻辑门，就可以制备成通用型量子计算机。这种量子计算机通过控制量子比特依次通过不同的量子逻辑门来达到编程的目的，通过组合不同的量子逻辑门可以实现各种量子算法。但是由于量子比特十分脆弱，很容易失去叠加和纠缠特

性，因此，通用型量子计算机建造难度很大，尤其是可以处理多个量子比特的情形。当前实验室环境可以做到同时处理 10 个左右的量子比特[29]。IBM 于 2016 年 5 月开放的量子计算平台是可以处理 5 个量子比特的通用型量子计算机，这种规模的量子计算机难以满足实用运算的要求，更倾向于技术的展示，现在所有人都可以通过 Web 访问的方式来体验量子编程和量子计算[27]。

与通用型量子计算机不同，总部位于加拿大的 D-Wave 系统公司制造了一种可以运行量子退火算法的专用型量子计算机，它的量子比特之间的连接方式是固定的，但是参数可调，因此制造难度较小。D-Wave 量子计算机已经实现商用，最新的产品 2000Q 集成了 2048 个量子比特[28]。然而，D-Wave 的量子计算机只能专门解决一类特殊的最优化求解问题[30-31]，由于优化问题在机器学习领域的重要性，D-Wave 的产品已经引起了包括谷歌在内的许多公司的注意。谷歌利用 D-Wave 的产品发现在处理某些特定问题上量子计算机的确具有很大的优势，比传统计算机单核运行速度快 1 亿倍[32]。因此 D-Wave 的产品可以称为“量子退火机”。参照通用型量子计算机的叫法，D-Wave 的产品可以说是属于一种专用型量子计算机，由于其应用局限性，目前还无法引入到与密码计算相关的领域中。

表 2　IBM 和 D-Wave 量子计算机对比

		IBM	D-Wave
相同点		基于超导环路量子比特 对硅芯片制造工艺进行改造制成特制芯片 正常工作需要低温、低磁场、真空等环境	
不同点	组成和工作方式	量子比特通过量子逻辑门进行操作	量子比特形成二维结构，量子比特之间的作用强度参数可调
	编程方式	通过控制量子逻辑门的操作顺序进行灵活编程	通过设定参数，经过绝热演化得到特定问题的解
	目前具有量子比特数目	5 个	最新产品为 2048 个
	扩展难度	高	较低
	已商用	否	是

2.3　量子算法

量子计算机的研制之所以受到各方重视的一个诱因是 1994 年 Peter Shor 发现了可以快速对大整数分解其素数因子的量子算法，这个算法可以破解现在广泛使用的 RSA、椭圆曲线等公钥密码[33]。

例如，RSA 密码算法的安全性需要基于以下事实：将某一具有两个素因子的长整数的素因子找出，当这个长整数很大时，是极其困难的，运算代价很大以至于实际上不可行。这个事实在没有发现量子 Shor 算法之前被认为是正确的，因为最好的分解整数的经典算法，其复杂度也是亚指数形式的[34-35]，这也是 RSA 算法可以被放心使用的原因。但是在量子 Shor 算法发现之后，这个结论在量子算法领域不再成立。

Shor 算法是一个多项式复杂度的算法[36]，若可以执行 Shor 算法的通用型量子计算机一旦制造成功，并且它能够处理的量子比特数目足够多，则现在经常使用的 1024 位和 2048 位 RSA 算法便不再安全。这意味着互联网上的信息安全保护基本完全失效，这是一个致命的威胁。理论上，Shor 算法分解一个 n 比特的长整数大约需要 $2n$ 个量子比特[37-38]，这意味着破解 RSA-1024 需要一台可以同时处理 2048 个量子比特的量子计算机。

就技术现状来说，通用型量子计算机的制造难度很大，到目前为止经过 20 年左右的发展，也只制造出处理大约 10 个量子比特的通用型量子芯片。当前实验室环境中可以用 Shor 算法分解的最大整数是 21[39-41]，因此 RSA 等密码算法当前还是安全的，但量子威胁仍然持续存在。

可以想象，当未来某天科学家发现了一种实现量子比特和量子逻辑门的方法容易进行大规模扩展时，也许量子芯片也会有类似摩尔定律那样的快速发展。那时，破解密钥长度很大的 RSA 算法将变得不再困难。这种情况的出现可能需要十年、几十年、甚至更久，目前已成为各大科研机构追逐的目标。

解决 Shor 算法威胁的更好办法是将 RSA 等公钥密码算法替换为可以同时抵抗经典算法和量子算法攻击的密码算法，这类算法被称为后量子密码算法或抗量子攻击密码算法。经典算法和量子算法都无法在多项式计算复杂度内解决的困难可用于构造后量子密码算法，这些算法早已开始研究，并且有多个候选方案，其中包括基于格困难问题构造的密码算法等[13]。

在对称密码的量子威胁方面，量子 Grover 算法是研究热点，该算法可以在无序的数据中进行快速查找[42-43]。在 n 个无序的数据中查找某个数据是否存在，经典方法是逐个元素进行判断（如穷举），平均查找次数为 $n/2$，复杂度为 $O(n)$。但是量子 Grover 算法的复杂度为 $O(\sqrt{n})$，相比传统方法有平方加速的效果。该算法可以辅助进行分组算法或哈希算法的穷举攻击[44-45]，这种攻击一旦实现，意味着现有对称密码算法的安全强度将大幅降低。若要达到之前的密码强度，需要将对称密钥长度加倍，例如需要将 AES-128 升级为 AES-256。Shor 算法和 Grover 算法对密码学算法的威胁和解决办法总结在表 3 中列出[46]。

表 3　大规模通用型量子计算机对密码算法的影响

密码算法	类型	用途	大规模通用型量子计算机的影响
AES，SM4	对称算法	加密	需要更长的密钥
SHA-2，SHA-3，SM3	杂凑算法	计算信息摘要	需要更长的摘要输出
RSA	公钥算法	签名，密钥协商	遭受直接攻击；需要更换为后量子密码算法
DSA 数字签名算法，ECDSA，ECDH，SM2 等椭圆曲线算法	公钥算法	签名，密钥交换	

3　量子通信

量子通信技术利用量子比特的特性，可以实现物理上安全的比特信息交换，交换之后得到的比特串可以作为分组密码算法或者“一次一密”算法的密钥来进行保密通信。这是未来保密通信技术的一个重要发展方向。量子通信中有两个重要的技术：量子密钥分发和量子隐形传态，它们的区别如表 4 所列。

表 4 量子通信技术对比

	量子密钥分发	量子隐形传态
传输的信息类型	经典比特	量子比特
是否用到量子纠缠	否	是
过程特点	一个比特编码成一个光子； 连续传输； 只有部分比特能作为最终的消息	传输一个量子比特需要一对纠缠量子比特； 通信双方需要事先各拥有纠缠量子比特对的其中一个量子比特； 需要通过经典信道将测量结果通知接收方

3.1 量子密钥分发和量子隐形传态

量子密钥分发的起点是 1984 年由 Bennett 和 Brassard 提出的 BB84 协议[47]，这个协议利用量子比特的不可克隆性质达到安全的比特信息传输。简单来说，量子比特的不可克隆性来源于：如果对量子比特进行窃取和观测，则这个量子比特便会塌缩为经典比特，原来的量子比特将不复存在，也无法恢复。

下面简述 BB84 协议的工作原理。若采用单光子的偏振态对经典比特信息进行编码，则可使用水平偏振(－)、垂直偏振(|)、45°方向偏振(/)和－45°方向偏振(\)这 4 个量子态。这 4 个量子态可构成两组正交基矢，分别记为“＋”基和“×”基。编码时可采用如下规则：若采用“＋”基，则用“－”表示“0”，“|”表示“1”；而在“×”基中，“/”代表“0”，“\”代表“1”。这两组基矢有如下特性：若编码和解码采用同样的基矢组，则会得到正确的比特。若采用不同的基矢组，则只有 50%的概率得到正确的比特。

例如，发送方 Alice 要发送比特“0”，并且采用了“×”基中的“/”方向偏振光子。当接收方 Bob 收到这个光子之后，他并不知道光子的状态，因此会随机选择一组基矢进行测量。假定选择的基矢组是“＋”，则 Bob 测量的结果可能是“－”或“|”方向偏振光子，并且得到这两个结果的概率是相同的。测量之后这个光子的状态也就变成“－”或“|”方向偏振光子，原来的“/”方向偏振状态将消失，无法恢复。类似地，在“＋”基中进行编码测量，而在“×”基中进行解码测量，结果也是一样的。

BB84 协议的过程如下：

(1)Alice 若想发送 n 个比特给 Bob，则她需要随机地从“＋”基或“×”基中选择 n 个基，并利用事先规定好的编码规则进行编码，然后将编码好的光子传送给 Bob。

(2)Bob 接收到光子之后，也随机选择 n 个基进行测量和解码，这样 Bob 也会得到 n 个比特。

(3)Alice 和 Bob 互相公开自己所使用的基，该过程可以通过公共经典信道完成。双方将基的选择不一致的比特去掉，剩下的比特即可作为已完成交换的信息。

表 5 列出了这个过程的一些例子，注意 Bob 的部分测量结果实际上是随机的，表 5 中列出的只是其中一种情况。

平均来说，Alice 和 Bob 现在手中只有 $n/2$ 个比特可用。为了检测是否有攻击者 Eve 存在，还需要进行 1 个步骤：

(4)Alice 和 Bob 公开比较一部分手中剩余的比特，该过程可以通过公共经典信道完成。如果对比发现密钥有不同，则证明 Eve 存在。如果没有不同，并且比较的比特足够多，则几乎可以肯定 Eve 没有进行攻击。那么最后剩余的没有比较的比特就可以作为安全的密钥来使用。

表 5 BB84 协议示例

Alice 随机生成的比特串	Alice 随机选择的基	Alice 编码的光子	Bob 随机选择的基	Bob 的测量结果	Bob 得到的比特串
0	×	/	×	/	0
0	＋	－	＋	－	0
1	＋	|	×	/	0
0	×	/	＋	|	1
1	×	\	＋	|	1
0	＋	－	＋	－	0
1	×	\	×	\	1
1	×	\	＋	|	1
⋮					

步骤(4)这样进行的原因为：若没有攻击者存在，Alice和 Bob 的比较结果应该完全相同。如果 Eve 截获了 Alice 发送的光子，并且进行了测量，则光子的量子态就会坍缩无法恢复。为了假扮 Alice 向 Bob 发送信息，Eve 最好的办法就是根据自己测量的结果再随机选择基进行编码，然后将编码的光子发送给 Bob。当 Alice 和 Bob 公开比较一部分剩余比特时，由于对于每个比特来说，Eve 编码时随机选择的基与Alice编码时选择的基只有 50%的概率相同，则在比较的比特串足够长的情况下，Alice 和 Bob 的比较结果仍然相同的概率非常低，意味着对窃听者失察的概率将非常小，这时就认为通信过程是安全的。最后，可用的密钥长度小于 $n/2$。

上述过程只是量子密钥分发系统的一种简单模型，实际系统会十分复杂，并且会使用多样的技术和方式[48-51]，包括利用传统密码技术进行身份相互认证、比特筛选、比特纠错和保密加强等。

量子隐形传态[52-53]是量子通信中的另一重要技术。尽管量子比特状态无法复制，但是可以进行传输，甚至可以不传递具有这个状态的量子比特本身，却在另外一个地方将该量子状态恢复出来，这个效果类似于“远距传送”：某个物体在一处突然消失，然后在遥远的另一处出现。由于其并没有直接传输量子比特的物理载体本身，因此也称为“隐形传态”。

量子隐形传态需要提前制备两个具有最大纠缠的量子比特，即量子态为 Bell 态的量子比特对。这两个量子比特的纠缠状态通常作为一个整体描述，不能简单地单独决定其中一个。当进行测量时，量子态会坍缩，而且当其中一个量子比特的状态确定之后，由于纠缠关系，另一个量子比特的状态不需要测量即可确定，即使这两个纠缠量子比特在空间上距离很远也是成立的。现在认为两个纠缠量子比特的空间距离即使在宇宙空间的尺度，也是纠缠在一起的。利用纠缠的量子比特对就可以进行量子隐形传态。

量子隐形传态过程简单描述如下：如图 1 所示，通信双方 A 和 B 各持有纠缠量子比特对中的一个量子比特。A 想要传送的量子比特为 X，他不需要知道 X 的具体状态。A 首先对 X 和其手中的纠缠量子比特进行一系列变换操作，然后进行测量。在测量的同时，B 持有的纠缠量子比特也会坍缩。A 将自己的测量结果通过经典信道传递给 B，B 根据测量结果进行相应的量子操作就可以使自己手中的纠缠量子比特的状态变成 X 的状态，从而达到传送的目的。量子隐形传态过程中使用了经典信道传输信息，因此整个过程无法超过光速，

这意味着量子隐形传态也无法进行超光速传输。

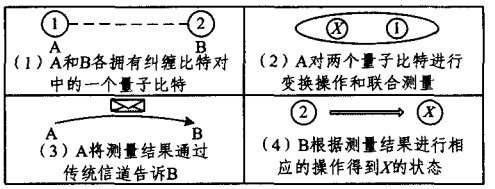

图 1　量子隐形传态过程

量子隐形传态技术可以在量子中继中用于传送未知量子比特，这种技术未来会是量子通信网络和分布式量子计算网络的重要组成部分[54-56]。

3.2　量子保密通信技术的进展

经过不断的发展，量子密钥分发技术的实用性逐渐增强，并且出现了量子密钥分发的商用设备[57-59]和网络[60]。量子密钥分发普遍使用的方案是利用光纤传递光量子[61-62]。BB84 协议的安全性可以得到保证的一个前提是通信双方传输的应该是单个光子，但实际上稳定可靠的单光子源难以制备，因此最初通常采用的是近似单光子源的弱激光源，这种方案的安全性一直受到很大的质疑[63-64]。2005 年以后发展起来的基于诱骗态(decoy state)的传输方法[65-71]的实用安全性有了很大提高，成为了当前广受关注的方案。实验室环境中，利用诱骗态和测量设备无关协议，最长的传输距离可达到 400km[71]。量子通信网络的广域长距离传送需要采用具有中继节点的分段网络，现在普遍采用的是经典可信中继节点，也就是在中继节点之间进行量子密钥分发，利用这些安全的密钥对发送方到接收方的真正密钥比特进行接力，直到传送至最终目的地，这种方案易于扩展和实施。比如，长度达到 2000km 的量子保密通信“京沪干线”具有 27 个中继节点和 5 个接入节点。可信中继节点的方案要求这些中继节点必须足够安全，如可采用物理隔绝和防护，但这并非量子力学原理可以保证的安全。真正安全的解决方案是中继节点也采用量子中继，使得整个网络都通过量子力学原理保证其物理安全。量子中继的实现需要量子纠缠分发、量子隐形传态和量子存储等技术[16]，由于量子存储还未有较好的解决方案[72-74]，因此其在技术上还无法实现实际可用的量子中继，但这是未来量子保密通信网络的发展方向。

除了通过光纤传输光量子之外，还可以通过大气层和太空等自由空间传递光量子[75-77]，这样就可以通过卫星来连接不同的广域量子网络。中国发射的全球第一颗量子通信实验卫星“墨子号”，其中一项任务就是验证星地之间的量子密钥分发功能。在地面量子通信网络和量子卫星的共同参与下，可以预见在不久的将来，实用的天地一体化量子通信网络会逐步形成并扩大应用规模，在全球范围内建设量子密钥分发网络值得期待。

利用并操控量子纠缠的量子隐形传态技术已经基本可以满足量子保密通信网络的需求。终端开放形式的、传送复合系统的和一次性传输多个自由度的隐形传态技术已在实验室环境实现[78-80]，其未来可用于增加量子网络的信道容量，也有助于量子计算的物理实现。

4　信息安全技术的新形态

未来，量子计算和量子通信技术将充分、成熟地发展，对信息安全领域会产生巨大的影响。这种影响一方面包括对现有技术的破坏性颠覆，例如量子 Shor 算法和大规模量子计算机的实现；另一方面，也可以提供更安全的保密通信方式，例如量子密钥分发。无论是哪种影响，信息安全领域都需要做好准备。

尽管可以运行 Shor 算法和 Grover 算法的大规模量子计算机还未制造出来，但是其威胁需要提前预防。一些涉及到个人隐私或国家机密的重要信息如果采用现行的公钥算法或分组算法保护，同时若被黑客或敌对组织获取并保存下来，等未来再采用量子计算机进行破解，后果是十分严重的。因此对安全等级要求高的领域需要提早更换后量子密码算法和增加分组算法的密钥长度。NIST 将依靠全世界密码学家的努力在未来 4～6 年内推出后量子密码算法的标准[46]，这种经过公开讨论和评审的算法应该会是未来公钥密码算法的重要组成部分。即使未来量子计算机出现，人们仍然可以进行保密通信，信息安全仍然可以得到保证。另外，量子计算机由于受到超导低温等环境因素限制，不会直接取代个人终端设备的计算内核，而更可能以“云”的形式提供服务，人们日常的工作、娱乐等活动仍旧会采用数字个人电脑和其他终端设备。因此，基于传统集成电路的密码芯片和密码终端仍会长期存在。

量子密钥分发系统未来的传输距离和传输速率将不断提高，实用安全性不断增强，它将成为信息安全网络的重要组成部分。量子通信网络需要通过光纤或自由空间传送量子比特，它需要额外的组件和设备，适用于对安全性要求较高的场景。未来的信息安全技术也不会是量子通信技术“一招鲜”解决所有问题，应该是与现有安全技术不断融合，保障人们通信和经济活动的安全。量子通信网络、设备与传统通信网络以及各种终端设备、便携设备，甚至物联网设备如何进行高效融合，量子通信协议和其他安全协议如何协同工作等仍是值得思考的问题。

结束语　就量子技术的发展现状来说，量子通信迎来大规模的商业应用仍需要时间，量子计算机的未来仍有很大的不确定性。信息安全领域相关问题是发展这些量子技术的重要诱因，未来的信息安全技术也会与新的量子技术深度结合，为信息安全增加新的内涵，形成新量子技术时代下的信息安全技术。信息安全领域的从业者需要持续关注量子技术，尤其是与信息安全相关的量子技术，并提前做好技术上的准备。

参 考 文 献

[1] STALLINGS W. Cryptography and Network Security: Principles and Practice (5th ed) [M]. Hong Kong: Pearson Prentice Hall, 2011.

[2] NEAMEN D A. Semiconductor Physics and Devices: Basic Principles (4th ed) [M]. New York: McGraw-Hill, 2011.

[3] LIN M B. Introduction to VLSI Systems: A Logic, Circuit, and System Perspective [M]. Boca Raton, FL: CRC Press, 2011.

[4] Interagency Working Group on Quantum Information Science of the Subcommittee on Physical Sciences. Advancing Quantum Information Science: National Challenges and Opportunities [R]. Washington, D. C.: National Science And Technology Council, 2016.

[5] WALPORT M, KNIGHT P. The Quantum Age: Technological Opportunities [R]. London: Government Office for Science, 2016.

[6] 腾讯数码. 谷歌:量子计算机比普通计算机速度快 1 亿倍 [N/OL]. (2015-12-11) [2017-03-01]. http://digi.tech.qq.com/a/20151211/024135.htm.

[7] 新浪科技. IBM 提供支持云的量子计算平台:开创量子计算新前沿 [N/OL]. (2016-05-09) [2017-03-01]. http://tech.sina.com.cn/d/2016-05-09/doc-ifxryhhi8539560.shtml.

[8] 新华网. 中国量子保密通信"京沪干线"工程 2016 年交付[N/OL]. (2014-11-03) [2017-03-01]. http://news.xinhuanet.com/tech/2014-11/03/c_1113095616.htm.

[9] 新华网. 我国成功发射世界首颗量子科学实验卫星"墨子号" [N/OL]. (2016-08-16) [2017-03-01]. http://news.xinhuanet.com/mil/2016-08/16/c_129233031.htm.

[10] WALDROP M M. The Chips Are Down for Moore's Law[J]. Nature, 2016, 530(7859): 144-147.

[11] THOMPSON S E, PARTHASATHY S. Moore's Law: the Future of Si Microelectronics[J]. Materials Today, 2006, 9(6): 20-25.

[12] NIELSEN M A, CHUANG I L. Quantum Computation and Quantum Information (10th Anniversary Edition) [M]. New York: Cambridge University Press, 2010.

[13] BERNSTEIN D J, BUCHMANN J, DAHMEN E. Post-Quantum Cryptography[M]. Heidelberg: Springer-Verlag Berlin Heidelberg, 2009.

[14] GISIN N, THEW R. Quantum Communication[J]. Nature Photonics, 2007, 11(1): 165-171.

[15] GUO G C. Quantum Information Technology [J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2010, 22(5): 521-525. (in Chinese)
郭光灿. 量子信息技术[J]. 重庆邮电大学学报(自然科学版), 2010, 22(5): 521-525.

[16] WU H, WANG X B, PAN J W. Quantum Communication: Status and Prospects [J]. SCIENTIA SINICA Informationis, 2014, 44(3): 296-311. (in Chinese)
吴华, 王向斌, 潘建伟. 量子通信现状与展望[J]. 中国科学:信息科学, 2014, 44(3): 296-311.

[17] PAN J W. Frontier Advances in Quantum Communication Technology [J]. Secrecy Science and Technology, 2016(11): 25-27. (in Chinese)
潘建伟. 量子通信技术前沿进展[J]. 保密科学技术, 2016(11): 25-27.

[18] GISIN N, RIBORDY G, TITTEL W, et al. Quantum Cryptography [J]. Reviews of Modern Physics, 2002, 74: 145-195.

[19] MAYERS D. Unconditional Security in Quantum Cryptography [J]. Journal of the ACM, 2001, 48(3): 351-406.

[20] SHOR P W, PRESKILL J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol[J]. Physical Review Letters, 2000, 85(2): 441-444.

[21] MAYERS D. Shor and Preskill's and Mayers's Security Proof for the BB84 Quantum Key Distribution Protocol [J]. The European Physical Journal D, 2002, 18(2): 161-170.

[22] ZHOU Z W, CHEN W, SUN F W, et al. A Survey on quantum Information Technology [J]. Chinese Science Bulletin, 2012, 57(17): 1498-1525. (in Chinese)
周正威, 陈巍, 孙方稳, 等. 量子信息技术纵览[J]. 科学通报, 2012, 57(17): 1498-1525.

[23] UK national quantum technologies programme. Homepage[OL]. http://uknqt.epsrc.ac.uk.

[24] CHEN Q. The Status of UK's Research and Development of Quantum Technologies [J]. Shanghai Informatization, 2015(2): 83-85. (in Chinese)
陈骞. 英国量子技术研究与发展现状[J]. 上海信息化, 2015(2): 83-85.

[25] GIBNEY E. Europe Plans Giant Billion-Euro Quantum Technologies Project [J]. Nature, 2016, 532(7600): 426.

[26] POPKIN G. Scientists Are Close to Building A Quantum Computer That Can Beat A Conventional One [N/OL]. (2016-12-01) [2017-03-01]. http://www.sciencemag.org/news/2016/12/scientists-are-close-building-quantum-computer-can-beat-conventional-one.

[27] IBM. IBM quantum experience [OL]. https://quantumexperience.ng.bluemix.net/qstage.

[28] D-Wave. Official Website of D-Wave [OL]. https://www.dwavesys.com.

[29] BARENDS R, SHABANI A, LAMATA L, et al. Digitized Adiabatic Quantum Computing With a Superconducting Circuit[J]. Nature, 2016, 534(7606): 222-226.

[30] OLIVER W D. Quantum Physics: Keep Your Feet on the Ground [J]. Nature, 2011, 473(7346): 164-165.

[31] JOHNSON M W, AMIN M H S, GILDERT S, et al. Quantum Annealing with Manufactured Spins [J]. Nature, 2011, 473(7346): 194-198.

[32] DEMEHEV V S, BOIXO S, ISAKOV S V, et al. What is the Computational Value of Finite-Range Tunneling?[J]. Physical Review X, 2016, 6(3): 031015.

[33] SHOR P W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer [J]. SIAM Journal on Computing, 1997, 26(5): 1484-1509.

[34] LENSTRA A K, LENSTRA H W. The Development of the Number Field Sieve [M]. Berlin: Springer-Verlag, 1993.

[35] WEISSTEIN E W. Number Field Sieve[OL]. http://mathworld.wolfram.com/NumberFieldSieve.html.

[36] BECKMAN D, CHARI A N, Devabhaktuni S, et al. Efficient Networks for Quantum Factoring [J]. Physical Review A, 1996, 54(2): 1034-1063.

[37] BEAUREGARD S. Circuit for Shor's Algorithm Using 2n+3 Qubits [J]. Quantum Information and Computation, 2003, 3(2): 175-185.

[38] PROOS J, ZALKA C. Shor's Discrete Logarithm Quantum Algorithm for Elliptic Curves [J]. Quantum Information and Computation, 2003, 3(4): 317-344.

[39] LUCERO E, BARENDS R, CHEN Y, et al. Computing Prime Factors with a Josephson Phase Qubit Quantum Processor [J]. Nature Physics, 2012, 8(10): 719-723.

[40] MARTÍN-LÓPEZ E, LAING A, LAWSON T, et al. Experimental Realization of Shor's Quantum Factoring Algorithm Using Qubit Recycling [J]. Nature Photonics, 2012, 6(11): 773-776.

[41] DATTANI N S, BRYANS N. Quantum Factorization of 56153

with Only 4 Qubits[J/OL].https://arxiv.org/abs/1411.6758v3.

[42] GROVER L K. A Fast Quantum Mechanical Algorithm for Database Search [C]// Proceedings of 28th Annual ACM Symposium on the Theory of Computing. New York: ACM Press, 1996:212-219.

[43] GROVER L K. Quantum Mechanics Helps in Searching for A Needle in A Haystack [J]. Physical Review Letters, 1997, 79(2):325-328.

[44] YE F. Research on Quantum Key Search Attack Based on Grover's Algorithm [D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2009. (in Chinese)
叶峰. 基于 Grover 算法的量子密钥搜索攻击研究 [D]. 南京：南京航空航天大学，2009.

[45] GRASSL M, LANGENBERG B, ROETTELER M, et al. Applying Grover's Algorithm to AES: Quantum Resource Estimates [C]// 7th International Workshop on Post-Quantum Cryptography, PQCrypto 2016. Fukuoka: Springer International Publishing, 2016:29-43.

[46] CHEN L D, JORDAN S P, LIU Y K, et al. Report on Post-Quantum Cryptography [R/OL]. (2016-04-28). https://dx.doi.org/10.6028/NIST.IR.8105.

[47] BENNETT C H, BRASSARD G. Quantum Cryptography: Public Key Distribution and Coin Tossing [C]// Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing. Bangalore: IEEE, 1984:175-179.

[48] ZHANG J. Long-Distance Quantum Communication[D]. Hefei: University of Science and Technology of China, 2007. (in Chinese)
张军. 远距离量子通信[D]. 合肥：中国科学技术大学，2007.

[49] PENG J. Research on Some Key Problems of the Experimental System in Quantum Communication [D]. Beijing: Beijing University of Posts and Telecommunications, 2009. (in Chinese)
彭建. 量子通信实验系统中若干关键问题的研究[D]. 北京：北京邮电大学，2009.

[50] WANG S. Research on the Key Technologies of Fiber Quantum Key Distribution [D]. Hefei: University of Science and Technology of China, 2011. (in Chinese)
王双. 光纤量子密钥分配关键技术研究[D]. 合肥：中国科学技术大学，2011.

[51] TANG Y L. Experimental Study of Security in Practical Quantum Key Distribution System [D]. Hefei: University of Science and Technology of China, 2015. (in Chinese)
汤艳琳. 实际量子密钥分发系统安全性的实验研究[D]. 合肥：中国科学技术大学，2015.

[52] BENNETT C H, BRASSARD G, CRÉPEAU C, et al. Teleporting an Unknown Quantum State Via Dual Classical and Einstein-Podolsky-Rosen Channels [J]. Physical Review Letters, 1993, 70(13):1895-1899.

[53] BOUWMEESTER D, PAN J W, MATTLE K, et al. Experimental Quantum Teleportation [J]. Nature, 1997, 390:575-579.

[54] DUAN L M, LUKIN M D, CIRAC J I, et al. Long-Distance Quantum Communication with Atomic Ensembles and Linear Optics [J]. Nature, 2001, 414(6862):413-418.

[55] ZHAO B, CHEN Z B, CHEN Y A, et al. Robust Creation of Entanglement between Remote Memory Qubits [J]. Physical Review Letters, 2007, 98(24):240502-240506.

[56] YIN Z Q. Quantum Cryptography and Quantum Repeaters [D]. Hefei: University of Science and Technology of China, 2010. (in Chinese)
银振强. 量子密码与量子中继研究 [D]. 合肥：中国科学技术大学，2010.

[57] ID Quantique. Official Website of ID Quantique [OL]. http://www.idquantique.com.

[58] 国盾量子. 国盾量子网站[OL]. http://www.quantum-comm.com.

[59] 问天量子. 问天量子网站[OL]. http://www.qasky.com.

[60] XU H X. Overview of the Development of Quantum Communication Networks [J]. Journal of China Academy of Electronics and Information Technology, 2014, 9(3):259-271. (in Chinese)
许华醒. 量子通信网络发展概述[J]. 中国电子科学研究院学报，2014, 9(3):259-271.

[61] GOBBY C, YUAN Z L, SHIELDS A J. Quantum Key Distribution Over 122 Km of Standard Telecom Fiber [J]. Applied Physics Letters, 2004, 84(19):3762-3764.

[62] YUAN Z, SHIELDS A. Continuous Operation of a One-Way Quantum Key Distribution System Over Installed Telecom Fiber [J]. Optics Express, 2005, 13(2):660-664.

[63] HUTTNER B, IMOTO N, GISIN N, et al. Quantum Cryptography with Coherent States [J]. Physical Review A, 1995, 51(3):1863-1869.

[64] BRASSARD G, LUTKENHAUS N, MOR T, et al. Limitations on Practical Quantum Cryptography [J]. Physical Review Letters, 2000, 85(6):1330-1333.

[65] WANG X B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography [J]. Physical Review Letters, 2005, 94(23):230503-230508.

[66] LO H K, MAX F, CHEN K. Decoy State Quantum Key Distribution [J]. Physical Review Letters, 2005, 94(23):230504-230509.

[67] ROSENBERG D, PETERSON C G, HARRINGTON J W, et al. Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber [J]. Physical Review Letters, 2007, 98:0105031-0105034.

[68] MANDERBACH T S, WEIER H, FURST M, et al. Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 Km [J]. Physical Review Letters, 2007, 98(1):0105041-0105044.

[69] PENG C Z, ZHANG J, YANG D, et al. Experimental long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding [J]. Physical Review Letters, 2007, 98:0105051-0105054.

[70] LIU Y, CHEN T Y, WANG J, et al. Decoy-State Quantum Key Distribution with Polarized Photons Over 200 Km [J]. Optics Express, 2010, 18(8):8587-8594.

[71] YIN H L, CHEN T Y, YU Z W, et al. Measurement-Device-Independent Quantum Key Distribution Over a 404 Km Optical Fiber [J]. Physical Review Letters, 2016, 117(19):190501.

[72] CLAUSEN C, USNANI I, BUSSIÉRES F, et al. Quantum Storage of Photonic Entanglement in a Crystal [J]. Nature, 2011, 469(7331):508-511.

（下转第 15 页）

USA: ACM Press, 2011: 1353-1355.

[66] SHARMA U, SHENOY P, SAHU S, et al. A cost-aware elasticity provisioning system for the cloud[C]// 2011 31st International Conference on Distributed Computing Systems (ICDCS). IEEE, 2011: 559-570.

[67] KNAUTH T, FETZER C. Scaling non-elastic applications using virtual machines[C]// 2011 IEEE International Conference on Cloud Computing (CLOUD). IEEE, 2011: 468-475.

[68] HERBST N R. Quantifying the Impact of Platform Configuration Space for Elasticity Benchmarking[D]. Informatics Institute, 2011.

[69] WEBER A, HERBST N, GROENDA H, et al. Towards a Resource Elasticity Benchmark for Cloud Environments[C]// Proceedings of the 2nd International Workshop on Hot Topics in Cloud service Scalability. ACM, 2014.

[70] HERBST N R, KOUNEV S, WEBER A, et al. BUNGEE: An Elasticity Benchmark for Self-Adaptive IaaS Cloud Environments [C]// Proceedings of the 10th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS 2015). 2015.

[71] LI Z, O'BRIEN L, ZHANG H, et al. On a catalogue of metrics for evaluating commercial cloud services[C]// Proceedings of the 2012 ACM/IEEE 13th International Conference on Grid Computing. IEEE Computer Society, 2012: 164-173.

[72] FERREIRA COUTINHO E, GONCALVES GOMESD, NEUMAN DE SOUZA J. An analysis of elasticity in cloud computing environments based on allocation time and resources[C]// 2nd IEEE Latin American Conference on Cloud Computing and Communications (LatinCloud). IEEE, 2013: 7-12.

[73] SHAWKY D M, ALI A F. Defining a measure of cloud computing elasticity[C]// 2012 1st International Conference on Systems and Computer Science (ICSCS). IEEE, 2012: 1-5.

[74] BREBNER P C. Is your cloud elastic enough?: performance modelling the elasticity of infrastructure as a service (iaas) cloud applications[C]// Proceedings of the 3rd ACM/SPEC International Conference on Performance Engineering. ACM, 2012: 263-266.

[75] BERSANI M M, BIANCULLI D, DUSTDAR S, et al. Towards the formalization of properties of cloud-based elastic systems[C]// Proceedings of the 6th International Workshop on Principles of Engineering Service-Oriented and Cloud Systems. ACM, 2014: 38-47.

[76] FOLKERTS E, ALEXANDROV A, SACHS K, et al. Benchmarking in the cloud: What it should, can, and cannot be[M]// Selected Topics in Performance Evaluation and Benchmarking. Springer Berlin Heidelberg, 2013: 173-188.

[77] SULEIMAN B. Elasticity economics of cloud-based applications [C]// 2012 IEEE Ninth International Conference on Services Computing (SCC). IEEE, 2012: 694-695.

[78] ISLAM S, LEE K, FEKETE A, et al. How a consumer can measure elasticity for cloud platforms[C]// Proceedings of the 3rd ACM/SPEC International Conference on Performance Engineering. ACM, 2012: 85-96.

[79] TINNEFELD C, TASCHIK D, PLATTNER H. Quantifying the elasticity of a database management system[C]// DBKDA 2014, The Sixth International Conference on Advances in Databases, Knowledge, and Data Applications. 2014: 125-131.

[80] MOLDOVAN D, COPIL G, TRUONG H L, et al. On Analyzing Elasticity Relationships of Cloud Services[C]// 2014 IEEE 6th International Conference on Cloud Computing Technology and Science (CloudCom). IEEE, 2014: 447-454.

[81] SHARMA U. Elastic resource management in cloud computing platforms[J]. Dissertations & Theses-Gradworks, 2013: 1-175.

[82] JOGALEKAR P, WOODSIDE M. Evaluating the scalability of distributed systems[J]. IEEE Transactions on Parallel and Distributed Systems, 2000, 11(6): 589-603.

[83] JMeter [EB/OL]. http://jakarta.apache.org/jmeter.

[84] Faban [EB/OL]. http://java.net/projects/faban.

[85] Siege [EB/OL]. http://www.joedog.org/siege-home.

[86] MENASCÉ D A. TPC-W: A benchmark for e-commerce[J]. IEEE Internet Computing, 2002, 6(3): 83-87.

[87] Amazon Cloudwatch [EB/OL]. http://aws.amazon.com/cn/cloudwatch.

[88] Yahoo Chukwa [EB/OL]. http://chuka.apache.org.

[89] Ganglia [EB/OL]. http://ganglia.info.

[90] Nagios [EB/OL]. http://www.nagios.org.

[91] Grenchmark [EB/OL]. http://grenchmark.st.ewi.tudelft.nl.

[92] NAJJAR A, SERPAGGI X, GRAVIER C, et al. Survey of elasticity management solutions in cloud computing[M]// Continued Rise of the Cloud. Springer London, 2014: 235-263

(上接第 7 页)

[73] GÜBDOĞAN M, LEDINGHAM P M, Almasi A, et al. Quantum Storage of a Photonic Polarization Qubit in a Solid [J]. Physical Review Letters, 2012, 108(19): 1905041-1905045.

[74] ZHOU Z Q, LING W B, YANG M, et al. Realization of Reliable Solid-State Quantum Memory for Photonic Polarization Qubit [J]. Physical Review Letters, 2012, 108(19): 190505-190507.

[75] PENG C Z, YANG T, BAO X H, et al. Experimental Free-Space Distribution of Entangled Photon Pairs Over 13 Km: Towards Satellite-Based Global Quantum Communication [J]. Physical Review Letters, 2005, 94(15): 150501-150504.

[76] JIN X M, REN J G, YABG B, et al. Experimental Free-Space Quantum Teleportation [J]. Nature Photon, 2010, 4(6): 376-381.

[77] YIN J, REB J G, LU H, et al. Quantum Teleportation and Entanglement Distribution Over 100-kilometre Free-Space Channels [J]. Nature, 2012, 488(7410): 185-188.

[78] ZHAO Z, CHEN Y A, ZHANG A N, et al. Experimental Demonstration of Five-Photon Entanglement and Open-Destination Teleportation [J]. Nature, 2004, 430(6995): 54-58.

[79] ZHANG Q, GOEBEL A, WAGENKNECHT C, et al. Experimental Quantum Teleportation of a Two-Qubit Composite System [J]. Nature Physics, 2006, 2(10): 678-682.

[80] WANG X L, CAI X D, SU Z, et al. Quantum Teleportation of Multiple Degrees of Freedom of a Single Photon [J]. Nature, 2015, 518(7540): 516-519.