量子保密通讯及经典密码

陈锦俊[1,2] 吴令安[1,2,†] 范 桁[1,2,††]
(1 中国科学院物理研究所 北京 100190)
(2 中国科学院大学物理科学学院 北京 100049)

2016－11－24收到
† email: wula@iphy.ac.cn
†† email: hfan@iphy.ac.cn
DOI: 10.7693/wl20170301

Quantum and classical cryptography

CHEN Jin-Jun[1,2] WU Ling-An[1,2,†] FAN Heng[1,2,††]
(1 Institute of Physics, Chinese Academy of Sciences, Beijing 100190, China)
(2 School of Physical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China)

摘 要 密码技术的发展经历了古典密码、现代密码和量子密钥分发三个阶段。首颗量子卫星“墨子号”的成功发射，使量子密钥分发技术迈向新里程。文章介绍了密码发展的各个进程，并详细介绍了目前广泛应用的RSA公钥密码系统，以及量子密钥分发使用的BB84协议，E91协议等。文末简要介绍了量子保密通信进展，并对“墨子号”量子科学实验卫星实验任务及重要意义做出解读。

关键词 RSA公钥密码，量子密钥分发，BB84协议，E91协议，“墨子号”量子科学实验卫星

Abstract Cryptography has gone through the stages of classical cryptography, modern cryptography, and quantum key distribution. The successful launching of the first quantum satellite "Mozi" is now leading quantum key distribution onto a new journey. We present a review of the development of cryptography, with a detailed discussion of RSA public key cryptography. We also explain the Bennett—Brassard and Ekert protocols which are used in quantum key distribution. Then we describe the development of quantum communication, as well as the experimental tasks and significance of the Mozi satellite.

Keywords RSA public key cryptography, quantum key distribution, BB84 protocol, E91 protocol, Mozi quantum experiment satellite

1 引言

密码学是一门古老的学科，其历史极为久远，可以追溯到几千年前的古文明时期。古典密码的设计和破解通常凭借灵感和技巧，而不是推理和证明，充满艺术性。密码学也是一门新兴的学科，1949年香农(Shannon)将信息论引入了密码学，为现代密码学建立了理论基础。随着Data Encryption Standard(DES)密码系统，Rivest—Shamir—Adleman(RSA)公钥密码系统等在军事、商业和民用领域的广泛应用，密码学作为一门学科迸发出巨大的生命力。1994年，P. Shor在理论上提出一种在量子计算机上运行的算法，可以破解RSA公钥密码体系；随着量子力学的发展，基于经典算法的密钥将无密可保！而基于量子力学基本原理、理论上是无条件安全的真随机数量子密钥分发的出现，引起了各国科学家极大的兴趣。量子密钥分发(quantum key distribution，简称QKD)成为量子信息领域中第一个走向实用的技术。中国凭借中国科学技术大学潘建伟等小组的工作，在这一领域走在了世界的前沿。2016年8月16日1时40分，我国自主研发的世界首颗量子科学实验卫星“墨子号”在酒泉卫星发射中心成功升空。人类朝实现全球量子保密通信的进程又

跨进了一步。

下面我们将对古典密码、现代密码以及QKD三个部分做介绍。

2 古典密码

早在公元前400多年，人类已经有意识地利用一些技巧对信息加密。古希腊人发明了用于传递军事机密的密码棒(图1)，即把长条的皮革螺旋形地斜绕在一个多棱棒上；将情报内容沿棒的径向方向写下。解下皮革后，文字乱杂无规，这就是密文，对敌人毫无价值。而接收消息的友方有一根同样尺寸的棒子，将皮革绕到棒子上，情报即会显现。这种密码技术有如下特点：(1)加密和解密的方法难度一致；(2)知道加密的方法即知道解密的方法；(3)加密方法除敌方外，对第三者也是保密的，所以第三者无法对友方发送加密信息。

我国古代也早有将“密语”隐藏在诗文、画卷或棋盘中特定位置的记载。在荷兰汉学家高罗佩(R. H. van Gulik)所著的中国公案小说《大唐狄公案》中，有描述狄仁杰解开层层通关密码破获一出谋反案的“湖滨案”。故事讲述一个歌女被害，留下的线索是一张棋谱残局，狄公百思不得其解。在继续追查的过程中，得到了另外一个线索，一幅金牒玉版的经文(图2)。种种推断失败后，狄公灵机一动，将棋谱中的黑子与经文进行对比，显现信息：“若汝明吾言，即指其玄，乃得入此门，享大吉。”然后凭此打开密室门，找到谋反的军火库，破获大案。

图1 古希腊密码棒(摘自网络)

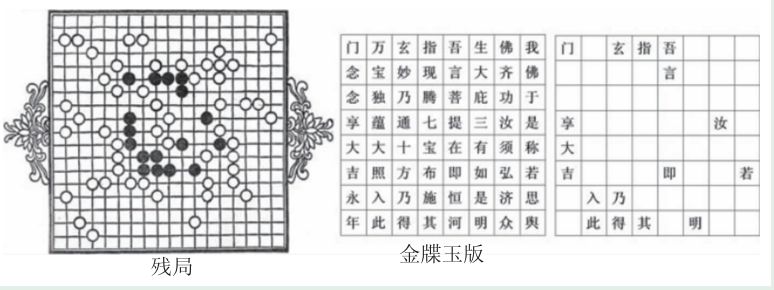

图2 湖滨案中的密码、明文以及解密后的信息(摘自《大唐狄公案》)

在此案中，棋盘残局是密码，本身无特点；金牒玉版的经文对应明文，是加密过的信息，也要求无敏感词。

3 现代密码学

现代密码学是一门快速发展的学科，现有的密码体制可以分为单钥密码(对称密码体制)如DES密码，和公钥密码(非对称加密体制)如RSA密码。前者使用相同的密钥，并且加密、解密过程一致；后者使用不同的公钥和密钥。本文主要介绍广泛应用于网络、电子银行系统等领域的RSA公钥密码系统。

1976年Whitfield Diffie和M. Hellman在《密码新方向》中提出了著名的Diffie—Hellman密钥交换协议[1]，标志着公钥密码体制的出现。1978年，R.L. Rivest，A. Shamir和L. Adleman实现了RSA公钥密码体制[2]。

3.1 RSA密码系统工作原理

RSA算法基于简单的数论事实：将两个大的质数相乘十分容易，但是想要对其乘积进行因式分解却极其困难。在RSA密码体制中，加密协议和解密协议(算法)是公开的。加密密钥是公开信息，即公钥(public key)，而解密密钥是需要保密的，即私钥(private key)。公钥决定私钥，但无法根据公钥计算出私钥。这样的密码体制，使任何人(第三者)都可以给私钥拥有者传送经过公钥加密过的信息(多对

一)，但是经过加密的信息第三者很难破解。

RSA算法的核心问题是产生公钥、私钥的密钥对，分如下几步：

(1)随机选定两个相距较远的大质数p和q，计算乘积$N=p*q$；N是公钥和私钥的公共模数，其二进制表示形式的位数，就是密钥长度。

(2)计算模数N的欧拉函数$f(N)=(p-1)*(q-1)$。

(3)随机选择一个整数c，满足$1<c<f(N)$，且c与$f(N)$互质；

(4)计算c对于$f(N)$的模反元素d，使得$c*d=1 (\mathrm{mod}\, f(N))$。

这样，就生成一个密钥对，其中(N，c)是公钥，(N，d)是私钥(除N和c外，其他数都不能公开)。利用生成的密钥对，甲方将需要传送的信息X(明文)经公钥加密，$X^c=Y(\mathrm{mod}\ N)$，变成密文Y，传送给乙方；乙方利用私钥解密，得到$Y^d=X^{cd}=X^{1+kf(N)}=XX^{kf(N)}(\mathrm{mod}\ N)=X(\mathrm{mod}\ N)$，就是甲方传送的信息(图3)。

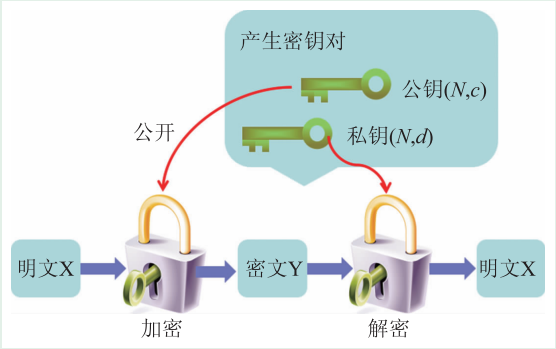

图3 RSA公钥密码系统工作原理

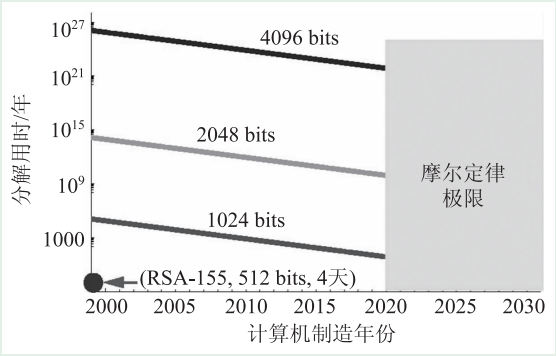

图4 RSA不同位数公钥密码随年份被分解时间展示(摘自参考文献[3])

3.2 RSA密码系统现状

RSA算法广泛应用于数据加密和数字签名，当前商业、民用等领域一般使用1024比特的密钥。攻击RSA算法最普遍的方式是分解模数N，基于大数分解极其困难，RSA目前能够抵抗已知的绝大多数密码攻击，已被国际标准化组织(ISO)推荐为公钥数据加密标准。历史上，曾对破解RSA密码有过一次悬赏。1977年，M. Gardner用RSA方法设计了一段密码，并公开悬赏100美元。他将一个英文句子转换为明文的字符串(对应方式：将26个英文字母用01-->26表示，空格用00表示)，将这个字符串用公钥(N，c)加密，其中，模数N是一个129位的十进制数(RSA-129)，c=9007。密码破解的关键是将模数RSA-129因式分解。1995年，互联网上1600台工作站大约用了8个月的时间，估计微处理器5000 MIPS年(MIPS指每秒百万指令)，终于破解了这个密码，并获得隐藏的神秘信息：The Magic Words are Squeamish Ossifrage(咒语是易恶心的秃鹫)。随着处理器能力的提高，RSA-130，RSA-140相继被分解；到1999年，RSA-155(512 bits)被成功分解，用时五个月(约8000 MIPS年)[3]。

假设计算机处理能力遵循摩尔定律，即每18个月翻一番，考虑1000台工作站联合计算分解RSA模数。以RSA-155的破解时间做参考，在2000年，计算机处理能力约为800 MIPS，则1000台处理器同时计算，需要4天破解。可以估算出模数N分别为1024 bits、2048 bits、4096 bits时在不同年限下需要的分解时间，结果如图4所示[3]。其中，横轴表示年份，纵轴表示分解需要的时间(以年为单位)。从图4中我们可以看出，目前广泛应用的1024 bits密钥长度是安全的。

可以总结得到，RSA密码系统的安全性建立在N很难分解的基础上，或者说利用已知的算法N很难分解；破解RSA密码系统，需要很大的计算资源。所以，在考虑采取的RSA密码时，只需考虑在现有计算能力基础上，需要一个较长时

间(比如10年)才能破解，就可以被认为是安全的。因此，RSA密码系统的安全性是一个动态的过程。

3.3 RSA密码系统的未来——量子计算机将使基于算法的密钥无密可保

对于因子分解，经典算法的计算量随位数的变化是指数增长。1994年Shor宣布了量子算法求质因子方法，计算量随位数的变化是多项式增长，计算速度指数地快于经典算法。Shor算法的数学原理依赖于计算取N模时X^2=1有除正负1之外的非平庸解，并从而实现因子分解N，其优势依赖于可快速实现的量子傅里叶变换。假设有一台频率为100 MHz的可以运行此算法的量子计算机，分解时间随整数N位数的变化情况如图5所示[3]。其中，横轴表示被分解整数的二进制位数，纵轴表示分解需要的时间(以分钟为单位)。Shor算法展示了量子计算机上可以有效解决因子分解问题，一个足够大的量子计算机可以破解RSA公钥密码系统。这鼓励科学家去建立量子计算机和研究新的量子计算机算法。

2001年，IBM的一个小组利用核磁共振资源，在实验上实现了Shor的量子分解算法，将15分解成3×5[4]。2012年，中国科学技术大学微尺度国家实验室的杜江峰等人利用核磁共振系统成功地在实验上实现了143=11×13的量子分解[5]。目前，D-wave公司也已建成千量级量子比特(qubit)的特定结构量子计算机——量子退火机(quantum annealing machine)。可以展望，量子计算机是有希望研制成功的，届时，基于算法的密钥系统将无密可保！

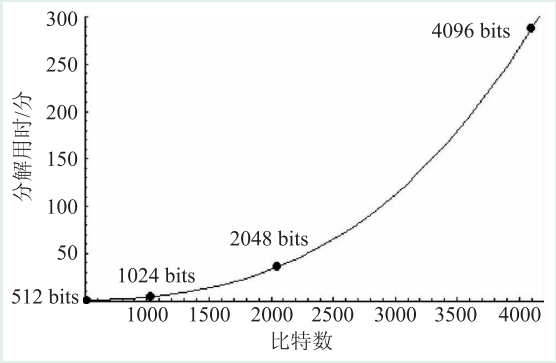

图5 利用100 MHz量子计算机分解二进制整数需要的时间(摘自参考文献[3])

3.4 一次一密密码本

量子计算机如果研制成功，目前广泛应用的经典密码系统将彻底失效，那世界上没有安全的密码了吗？科学家们想到了已经从数学上严格证明了“一次一密”的密码本(one-time pad)是绝对安全的。一次一密要求：密钥完全随机，密钥长度和明文长度一样长，密钥本身只使用一次。这使分配密钥成为十分重要的环节，然而现实中存在以下问题：(1)发射方Alice和接收方Bob之间的密码本需要传递，才能异地共享；(2)密码本在传送信息用之前就存在，时间上靠前；(3)Alice和Bob即使有身份认证，不能防止敌对方也有一个相同的密码本，即对泄密无感知！

量子力学对安全通信关上一扇窗的同时，也打开了一扇门。科学家发现，利用量子力学的基本原理，既可以轻松实现一次一密，又能保证密钥分发过程绝对安全；是原理上无条件安全的保密通讯。

4 量子密钥分发

量子信息中一些概念，如量子密码、量子保密通信等，会让公众产生是用量子的方法直接进行通信的误解。实际上，只是用量子力学原理保证安全地把一个真随机数密钥本分配给通信的双方，用于以后进行加密和解密。密文的发送仍然通过经典的通信手段来完成(图6)。因此我们可以使用更确切的说法“量子密钥分发”。

4.1 BB84量子密钥分发协议及工作原理

1984年，H.Bennett和G.Brassard受到S.Wiesner量子钞票概念的启发[6]，提出一种产生密钥的方法，后称为Bennett—Brassard(BB84)协议，从此

QKD理论诞生了[7]。

量子密码用量子比特元替代经典比特元。经典比特只有0和1两种状态，而根据量子态叠加原理，量子比特既可以处于0，1两种状态，也可以处于0，1的叠加态上，例如电子自旋态、光子偏振态等。

假设用单光子的偏振态表示量子比特。一个单光子可以用两种编码方式：(1)水平和垂直两种偏振态；(2)45°斜向上和－45°斜向下偏振态。利用码元0对应水平或斜向下－45°的光子偏振方向；而码元1对应垂直或斜向上45°的偏振方向。这样共有4种偏振态，两种编码方式对应于两组互为共轭的测量基(图7左图)。Alice发射一系列偏振态给Bob，Bob随机选择水平垂直或正负斜向两个共轭基之一的检偏器测量光子的偏振方向。如果测量基与Alice用的发射基一样，则能精确地测定原偏振方向；如果测量基选错了，偏振信息则完全不确定，只有50%的概率会是正确的(图7右图)。

具体的BB84协议流程如下(图8)：

(1)单光子源产生一个一个的单光子；

(2)发送方Alice使用偏振片随机生成垂直、水平、＋45°或－45°的偏振态，将选定偏振方向的光子通过量子通道传送给接收方Bob；

(3)Bob随机选用两种测量基测量光子的偏振方向；

(4)Bob将测量结果保密，但将所用的测量基通过经典通道告知Alice；

(5)Alice对比Bob选用的测量基与自己的编码方式，然后通过经典通道告诉Bob哪些基和她用的不同；

(6)Bob扔掉错误基的测量结果(统计上会扔掉一半的数据)；

(7)Alice和Bob选取一部分保留的密码来检测错误率，如果双方的0、1序列为一致，则判定没有窃听者Eve窃听，剩下未公开的比特序列就留作量子密钥本。

使用BB84协议进行QKD，Eve如果想窃听，不仅需要窃听公开信道上的全部信息，还需

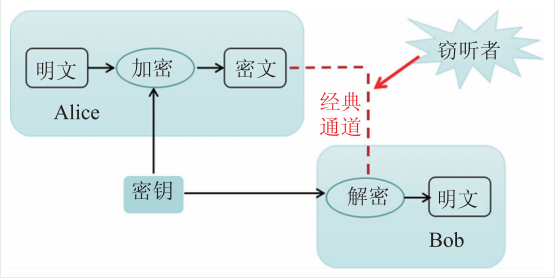

图6　密码通讯的基本原理图

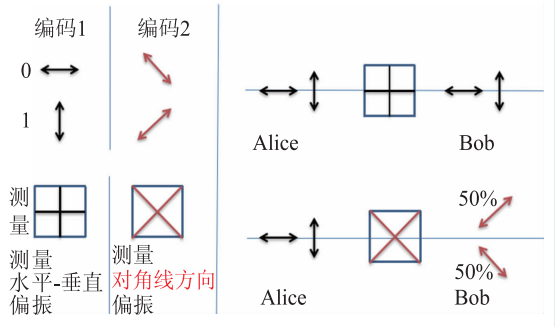

图7　单光子偏振态编码方式、测量基以及选用不同测量基的结果

窃听量子信道才能还原出最终的密钥。根据量子力学基本原理，当测量的量子态不是测量算符的本征态，会导致波包塌缩，从而破坏初始的量子态。所以Eve如果冒充Bob劫持量子信道，由于她也不知道测量基，必然有50%的测量结果也不准，而她还得冒充Alice把所测偏振态发送给Bob，所以Alice和Bob在抽检比特串时会发现至少25%的误码率。同时由于量子不可克隆原理(处于未知的量子态的单量子态不可100%精确复制)，Eve无法克隆Alice发送的单光子。Bob和Alice通过检测误码率来判断是否存在窃听者Eve；若发现被窃听，就停止通信。因此，BB84协议是原理上绝对安全的QKD协议。

4.2　BB84协议现状

在实验上，BB84协议依赖于多项技术条件，如高效产出的单光子源、无噪声干扰量子信道以及能高效读出单光子态的探测器；同时还要求通信双方选择发送、测量基的随机性品质

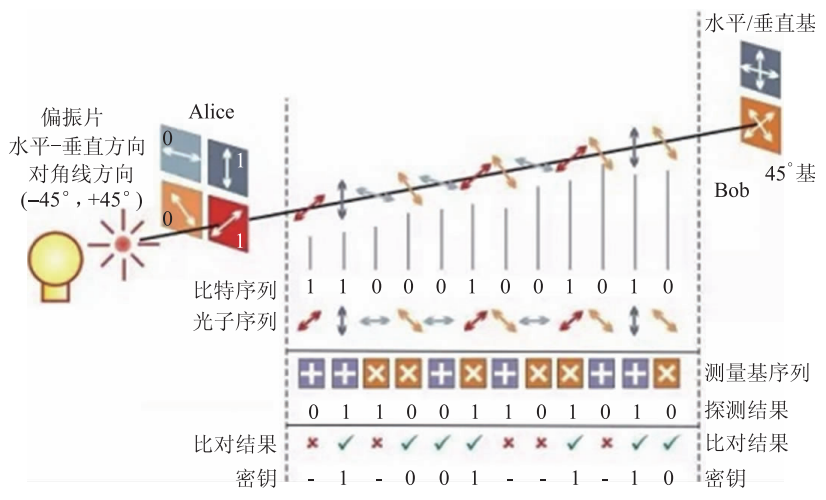

图8 BB84协议流程(摘自参考文献[8])

好，最好采用真随机数调制。然而现实中有很多不理想情况，攻击者可利用这些漏洞进行攻击。情况如下：(1)实际中的单光子源效率低，品质差，会有一定几率的多光子，这个现象可被利用进行光子数分离攻击(photon-number splitting)[9, 10]，例如单光子源同时出现两个光子，一个被窃听者拿去，另一个传送到接收方，会造成接收方对泄密无感知；(2)现实中单光子探测器效率低，“量子黑客”可以以此作为攻击点，致盲BB84态测量中对应某一个基的探测器，使光子探测器只剩一个基[11]；(3)窃听者可针对伪随机数，实施木马病毒等经典攻击方法；(4)文献[12]中介绍了一种基于原理上的攻击方式，将BB84单光子态近似量子克隆为两个态，一个保留，一个发送，引起的误差是14%左右，小于直接窃听的误差25%，误差上的减少也可能导致攻击。

针对实验器件和方案中的漏洞，世界范围内各个实验组展开了很多新工作，使BB84协议从原理上安全走向可实用的技术。例如，韩国Hwang提出诱骗态(decoy state)[13]，克服单光子源的多个光子问题；王向斌和加拿大Lo小组2005年同时对此提出改进方案[14, 15]。针对光子探测器致盲攻击、器件缺陷等问题，也有诸多小组展开研究，如英国Braunstein组[16]，加拿大Lo组[17]等提出的仪器无关量子保密通讯方案。同时，有多个小组致力于真随机数产生工作。

4.3 与BB84协议等价的E91协议

在BB84协议中，巧妙的是密钥比特是在异地同时产生的，Alice起先并不知道会产生什么样的比特序列。密钥的来源也可以视为Alice和Bob提前共享一组最大纠缠态，如处于n个状态为$(|00\rangle+|11\rangle)/\sqrt{2}$的量子比特纠缠对。基于纠缠光子对的E91协议由Ekert于1991年提出[18]。量子纠缠态保证Alice和Bob在测量基相同的情况下，测量结果完全一致(对应)，结果与直接发送BB84单光子态一样，所以两个协议可视为等价的。然而纠缠光子对的产生和分发是E91协议的技术瓶颈。2012年，潘建伟小组实现了100 km自由空间纠缠分发[19]。2015年，荷兰Hanson小组在无漏洞Bell不等式测量的工作中利用220小时得到245个有效的Bell不等式测试数据，即约1个小时可以确保在相距1.3 km的两个实验室中的金刚石色心中产生一个共享的纠缠态[20]，但大规模量子纠缠分发技术上还不成熟。

4.4 量子保密通讯进展以及墨子星

从1991年开始，世界各国就开始了QKD实验。中国科学院物理研究所吴令安小组也于1995年用单光子偏振态进行了自由空间QKD实验[21]。各国QKD早期实验情况如表1所示。

目前，QKD技术已经进入实用阶段，世界上各个国家有很多应用实例，特别是在安全网络领域。2005年，美国军方DARPA项目最早实现光开关技术和可信中继技术的组网结合，并建成包括10个节点的量子保密通信网络。2008年，维也

纳建成跨越12个国家，41个小组的全可信任中继网络——欧洲SECOQC网络。日本也于2010年建成东京量子保密通信网。美国Los Alamos实验室自2011年以来一直使用内部的QKD网络。

表1　世界各国早期QKD实验

自由空间中

	年份	协议	量子态	波长/μm	距离	比特率/Hz	误码率/%
IBM Bennett	1991	BB84	偏振	0.55	32 cm	1.2 k	4
中国科学院物理研究所	1995	BB84	偏振	0.56	30 cm	4 k	6
Franson	1996	B92	偏振	0.633	150 m	1 k	2
华东师范大学物理系	1997	B92	偏振	0.63；0.67	30 cm	10 k	6；2.1
美国Los Alamos	1999	B92	偏振	0.77	500 m	5 k	1.6

光纤中

英国DRA	1992	E91	相位	0.883			
英国BT Labs	1993	BB84	相位	1.3	10 km	20 k	
美国Johns Hopkins	1995	BB84	偏振	0.633	1 km	5 k	0.4
瑞士Geneva Univ.	1995	BB84	偏振	1.3	23 km		0.54
英国BT Labs	1995	BB84	相位	1.3	30 km	30 k	4
美国Los Alamos	1999	BB84 B92	相位	1.3	48 km	10	9.3
中国科学院物理研究所	2000	BB84	相位	0.85	1.1 km	3	9

要使用QKD技术实现广域量子保密通讯，需要三级量子网络。首先通过光纤实现量子城域网络；然后通过可信中继器实现城际量子通讯网络；最后通过卫星中转实现远距离的量子通讯网络，如图9所示。

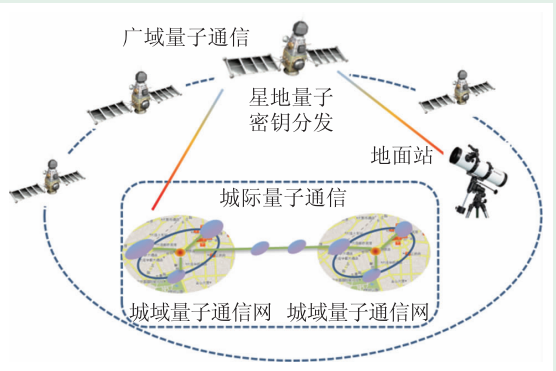

图9　未来全球量子通信网络构想图

由潘建伟和郭光灿分别领导的小组带领中国在量子保密通信领域走在了世界的前沿，先后在合肥、北京、济南实现了城市内QKD网络；潘建伟小组主导的贯穿多个城市的城际通讯网络“量子京沪干线”已于2016年底开通。同时，世界首颗量子卫星“墨子号”于2016年8月16日在我国酒泉卫星发射中心成功升空。量子通信网络已经从城域、城际开始迈向星地一体的进程。

墨子星升空的第一要务是借助科学卫星，进行星地QKD。目前公开报道的数据显示，每一圈工作时间7分钟，数据量为202 MB。除此之外，“墨子星”还将进行多个量子力学实验，包括进行广域的量子纠缠分发、量子远程传态(teleportation)，以及量子力学完备性检验等实验研究。墨子星升天是向建设广域量子保密通信网络迈出的重要一步。未来，将有更多量子通讯卫星与之携手作战，从而实现全球化的广域量子保密通信网络，我们期待着这一天的到来。

致　谢　本文是根据范桁和吴令安在中国科学院物理研究所“前沿讲座”中的主要内容，由陈锦俊完善而成，感谢诸位同事的热烈讨论，使得文章内容趋于完整。文中技术上的内容已基本省略，有兴趣的读者可以查看专业文献。部分工作得到科技部、基金委和科学院基金的支持。

参考文献

[1] Diffie W, Hellman M. IEEE transactions on Information Theory, 1976, 22: 644
[2] Rivest R L, Shamir A, Adleman L. Communications of the ACM, 1978, 21: 120
[3] Galindo A, Martin-Delgado M A. Reviews of Modern Physics, 2002, 74: 347
[4] Vandersypen L M, Steffen M, Breyta G *et al*. Nature, 2001, 414: 883
[5] Xu N, Zhu J, Lu D *et al*. Physical Review Letters, 2012, 109: 269902
[6] Wiesner S. ACM Sigact News, 1983, 15: 78
[7] Bennett C H. International Conference on Computer System and Signal Processing, IEEE, 1984, pp.175-179
[8] http://swissquantum.idquantique.com/?Key-Sifting
[9] Huttner B, Imoto N, Gisin N *et al*. Physical Review A, 1995, 51: 1863
[10] Brassard G, Lütkenhaus N, Mor T *et al*. Physical Review Letters, 2000, 85: 1330
[11] Lydersen L, Wiechers C, Wittmann C *et al*. Nature Photonics, 2010, 4: 686
[12] Fan H, Wang Y N, Jing L *et al*. Physics Reports, 2014, 544: 241
[13] Hwang W Y. Physical Review Letters, 2003, 91: 057901
[14] Wang X B. Physical Review Letters, 2005, 94: 230503
[15] Lo H K, Ma X, Chen K *et al*. Physical Review Letters, 2005, 94: 230504
[16] Braunstein S L, Pirandola S. Physical Review Letters, 2012, 108: 130502
[17] Lo H K, Curty M, Tamaki K. Nature Photonics, 2014, 8: 595
[18] Ekert A K. Physical Review Letters, 1991, 67: 661
[19] Yin J, Ren J G, Lu H *et al*. Nature, 2012, 488: 185
[20] Hensen B, Bernien H, Dréau A *et al*. Nature, 2015, 526: 682
[21] 邵进, 吴令安. 量子光学学报, 1995, 1(1): 41

《物理》有奖征集封面素材

读者和编者

为充分体现物理科学的独特之美，本刊编辑部欢迎广大读者和作者踊跃投寄与物理学相关的封面素材。要求图片清晰，色泽饱满，富有较强的视觉冲击力和很好的物理科学内涵。

一经选用，均有稿酬并赠阅该年度《物理》杂志。

请将封面素材以附件形式发至：physics@iphy.ac.cn；联系电话：010-82649470；82649029

《物理》编辑部