量子密钥分配技术
——信息时代安全之“盾”

徐令予

美国加州大学洛杉矶分校等离子体物理实验中心,美国洛杉矶 90095

摘要 介绍了密码技术,解释了密码危机的由来。对称密码体制中的密钥分配是维护信息安全的核心问题,自20世纪70年代研发的公钥密码体制存在多种隐患,它们难以保证密钥分配中的绝对安全。论述了量子密钥分配技术的原理及研发进展。

关键词 密码技术;公钥;量子密钥分配

长久以来人们都把密码与军事、外交联系在一起,事实上今天每个普通人都离不开密码,密码技术已经进入平常百姓家。当你在网上购物,当你用手机通话或收发微信,所有信息都在开放共享的网络上传输,现代通信技术使得信息的传输变得十分方便、迅速和高效,但同时它也使信息很容易被黑客截获,没有密码技术保护,在网上使用信用卡,在无线网上通话将会是难以想象的。据估计,每天全世界生产总值一半以上的金钱财产在国际银行金融电信网络(SWIFT)上流动,这样大规模的金融活动,如果失去可靠有效的密码技术保护必将引起世界级灾难。

当然现代化的军队也比过去更依赖于密码技术。如果遥测遥控的信息被盗,敌方可以隐藏保护自己,或者可以改变导弹的轨迹,甚至操纵无人机据为已有。事实上对今日的攻击方而言,使用导弹和飞机已是多余,如果能破解对方的密码系统,发个命令就可以秒杀对方城市的供电、公交和通信系统,真正达到“不战而屈人之兵”的最佳效果。

毫不夸张地说,密码学是信息时代-后工业时代健康发展的根本保证。密码技术对于政府、军队和大众生活,已是不可须臾离者也,它像空气一样,人们一刻也离不开,但却常常为人忽视。今天的密码技术正面临着严峻的挑战,新技术的研发已经刻不容缓。

1 密码技术和破密技术

简单地讲,密码技术就是发送方通过双方认同的某种规律把明文加密后得到密文,然后通过不安全信道送给接送方,接收方再按照该规律把密文解密后还原成明文。最古典的两种加密方法无非是字母的置换和替代。

替代法是按规律地将一组字母换成其他字母或符号,例如明文“fly at once”变成密文“gmz bu podf”(每个字母用字母序列中下一个字母取代)。使用同样方法,只要改变一个参数(每个字母用下两个字母取代),密文就变成“hna cv qpeg”(图1)。在密码学中,把这种加密解密方法称为密码算法,而算法中的秘密参数称为密钥(key),它只为通信双方共享。

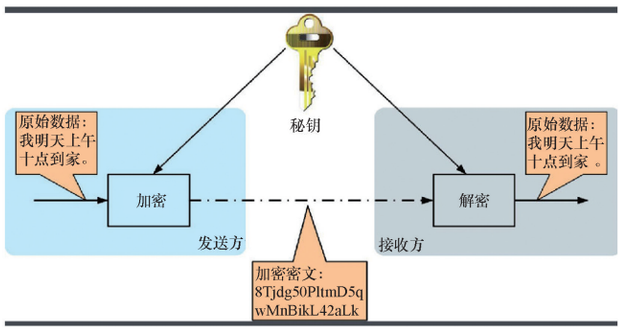


图1 对称密码体制中用相同的密钥作为加密和解密算法中的秘密参数

Fig. 1 In symmetric cryptosystem, the same key is used as the secret parameter in encryption and decryption algorithms

自密码技术诞生起,破密技术的发展就从未停止过。例如,字母替代法因为太容易被敌方破译,早已停止使用。因为每个英文字母在明文中出现的概率不同,只要把密文中的字母作一次出现率统计,不难找出字母之间替代的规律,从而破解密文。

而高级的加密算法使字母的替代不是固定一一对应关

收稿日期:2016-10-31;修回日期:2017-08-31

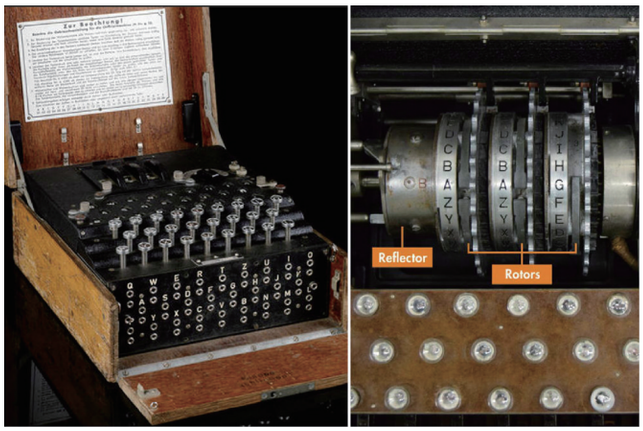
作者简介:徐令予,教授,研究方向为等离子体物理,电子信箱:lingyu.xu1@gmail.com

引用格式:徐令予. 量子密钥分配技术——信息时代安全之“盾”[J]. 科技导报, 2017, 35(19): 85-90; doi: 10.3981/j.issn.1000-7857.2017.19.012

系,字母替代的次序与出现概率也不是固定的,可以参考维热纳尔方阵算法,这种算法虽不难理解,但如果没有密钥就很难破译[1]。

2 恩尼格玛密码机

第二次世界大战中,德国军队使用的恩尼格玛(Enigma,图2)密码机把密码技术推到了当时的顶峰。恩尼格玛密码机在密码技术上有3个突破:1)密码机依靠机电设备自动完成加密和解密过程,因而可以高效正确地完成高度复杂的密码算法;2)密码机上的转轮的设置和面板对接孔联线方式决定了字母复杂多变的替代关系,它们就是系统的密钥,密钥可以轻松地每天一变,使得对密文的破译变得更为困难;3)由于算法与密钥的彻底分离,使得获得密码机没有多大用处,通信的安全是靠复杂多变的密钥得到保障。该密码机像部电动打字机,机器由26个字母按键和26个字母显示灯以及一些机电机电连接部件组成,决定了加密和解密的算法;另外有3个可以装卸的转动轮和两排字母对接孔,这些转动轮排列的次序和开始的位置和字母对接孔的连线每天按照约定设置,它们即为每天通信的密钥。发送时把明文字母用按键一一输入,经过机器复杂的变换后点亮不同的字母显示灯,这些字母出现的序列就是密文,把它用电报发送出去,接收方用同样的机器,按同样的密钥设置,键入密文,从字母显示灯的序列中读出的就是明文。



密码机上的转轮的配置和起始点的变化再加上机子正下方的对接孔不同的联接方式共同构成了系统的密钥(右图)

图2 第二次世界大战期间德军使用的恩尼格玛密码机

Fig. 2 The German Enigma machine used during the Second World War

第二次世界大战期间,英国情报机关为了破译德国的恩尼格玛密码伤足了脑筋,电影《Imitation Game》回顾了这段历史,但其中过分夸大了英国情报机关的功绩。事实上,战前波兰破译小组对恩尼格玛密码机的深入研究和德国内部叛徒提供的有关资料都为英国的破译帮了大忙。而英国数学家、逻辑学家艾伦·麦席森·图灵(Alan Mathison Turing)为破译恩尼格玛作出了巨大贡献。图灵首先意识到机器成生的密码只能依靠机器破译,为此他向英国首相丘吉尔报告,申请十万英镑研制破译机器。丘吉尔批准了这个看似极不靠谱的项目,而且在百忙之中亲自探望了图灵为首的破译小组。

英国情报部门对恩尼格玛密码机破译始终守口如瓶、滴水不漏,到第二次世界大战结束,德军仍不知自己许多重要军事行动已被英国掌握。战后英国把缴获的成千上万台恩尼格玛密码机送给了原殖民地的英国盟国,这些国家长期使用它们直到20世纪70年代初期,而有关破译恩尼格玛密码机的故事到20世纪70年代中期才被逐步透露出来。

3 密钥分配是现代密码技术的核心问题

有了计算机以后,现代密码技术的算法更为高度复杂化。现今普遍使用的美国数据加密标准DES算法具有极高安全性,到目前为止,除了用穷举搜索法对DES算法进行攻击外,还没有发现更有效的办法。而近年来提出了高级加密标准AES算法和三重DES的变形方式,使破译变得更加困难。由于密钥中每位的数值是完全随机选取的,一个128位长的密钥有2128的不同组合,在超级计算机天河2号上用穷举搜索法攻击也至少要花1万亿年才能完成。

有必要再次强调密码系统包括算法和密钥两部分。一个好的密码系统的算法可以是公开的,就像上面提到的DES算法,只要通信双方保护好密钥,加密后的资料就是安全的。这个原则又被称为柯克霍夫原则(Kerckhoffs´ principle)。认为所有加密法都可以被破解是大众的误解。理论上已经证明,只要密钥不再重新使用,信息被与其等长或更长的密钥加密后是不可能破密的。

既然如此,那么信息安全危机究竟在哪里呢?到目前为止讨论的所有密码体制中通信双方使用相同的密钥进行加密和解密,在这种对称密码体制中信息的安全靠密钥保证。需要改变密钥时,通信双方必须直接碰头交换,或者由可信任的第三方配送。所有问题也就发生在密钥分配过程中。

美国政府的密钥是通信安全局(COMSEC)掌管和分发的,20世纪70年代,每天分发的密钥数以吨计。当装载着COMSEC密钥的船靠港时,密码分发员会上船收集各种卡片、纸带以及其他一切储存密钥的介质,然后把它们分送给各处的客户。依靠第三方配送密钥增加了通信双方的开支,而且第三方配送者本身也构成了严重的安全隐患。

为确保信息的安全必须经常更换密钥,但今天的通信者往往相隔甚远,让通信双方见面交换密钥非常不现实,依靠第三方配送密钥一般人根本负担不起,而且也不一定及时可靠。密钥的配送问题长期困扰着密码学的专家们。

20世纪70年代,一种称为非对称密码体制(又称为公钥密码体制)应运而生。对称密码体制中通信双方使用同一个

密钥进行加密和解密,而非对称密码通信时加密和解密使用一对公钥和私钥,用公钥加密后的文件只能被与其对应的私钥解密,反之亦然。图3展示了公钥密码体制的流程,右边接收方通过计算产生一对公钥和私钥(分别为绿色和红色),接收方把绿色的公钥通过公开信道送给左边的发送方,发送方用接收方送来的公钥对文件加密后通过公开信道送给接收方,接收方用红色的私钥对文件解密,文件安全可靠地从发送方送到了接收方。

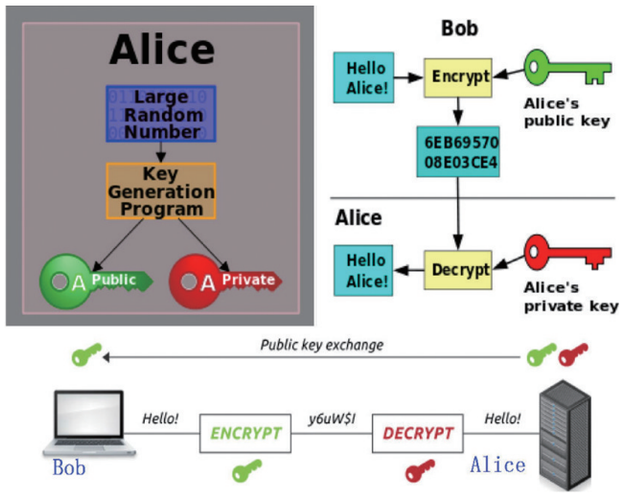


图3 非对称密码体制(即公钥密码体制)的原理示意

Fig. 3 Principle of asymmetric cryptosystem (public key cryptography)

公钥密码体制的关键是用了公钥和私钥,一个公开一个隐秘,第三者拿了公钥没有任何用处,公钥能用来加密但不能解密,也推算不出私钥。而通信双方可以随时产生新的密钥对,把公钥通过开放信道送给发送方,把私钥藏妥,通信双方无需直接碰头。这里介绍的是公钥密码体制的基本原理,实际应用中略为复杂一点,但原理相差无几[2]。

为更好地理解公钥密码体制,可以把公钥看成一把打开的锁,私钥就是开锁的钥。接收方B把打开的锁通过公共渠道传给发送方A,A把文件放于箱中并用B送来的锁把箱子锁上,加锁后的箱子再通过公共渠道返还B,B用私钥把锁打开取出箱中文件。在传送过程中截获打开的锁毫无意义,事实上B乐意把许多打开的锁送出去并为众人所有,这样大家可以加锁给他送密信,而这把锁一旦锁上任何人再也无法打开,除了握有私钥的接收方B。

公钥密码体制中加密和解密的算法很复杂,计算量大,事实上很少直接用它加密文件,它真正的用途是用来传送前面所介绍的对称密码体制中的那个通信双方共用的密钥。所以实际上文件传送流程应该是这样:A方先决定一个密钥,然后用B送来的公钥加密后传给B,B用自己的私钥对其解密后获得真正的密钥,然后双方就用此密钥对文件加密后传送给对方,收到方用该密钥对文件解密。这样的系统很安全,因为密钥可以随时改变并被公钥密码体制保护后在公共讯道上传输不被截获,这才是通信安全的根本保证。

4 危机四伏的密码系统

至此是否就此太平无事了呢?答案却是否定的。黑客攻击的重点是公钥系统,RSA公钥的产生基于两个大质数的乘积,它不是一个完全的随机数,这就是整个密码系统中的阿喀琉斯的脚后根,一旦公钥系统破解,密钥就可能被截获,整个系统就会崩溃。山东大学王小云发现这些公钥算法存在安全隐患[3]。近年来,美国国家标准与技术研究院(National Institute of Standards and Technology,NIST)强烈建议将RSA公钥从1024位提高到2048位。

提高公钥密码位数极大地增加了加密和解密所花的时间,给日常的应用带来了诸多不便,却并没有从根本上阻止黑客攻击的热情和力度,提高位数给使用者增添的困难远超对黑客的阻力。而2014年的一条爆炸性新闻更是震惊了密码学界,从美国国家安全局(NSA)叛逃的斯诺顿(Edward Snowden)披露了NSA有一个绝密项目 Penetrating Hard Targets,计划建造一台专用于破密的量子计算机。据传NSA已经存放了大量外国政府的密电,一旦项目成功立刻对它们动手解密。量子计算机虽然还在试制中,但贝尔实验室的一位数学家已经为此设计好了攻击RSA的算法,并声称已经写成可以在量子计算机运用的程序,它可以轻松地破解公钥密码体制。

量子计算机的研发进展是世界各国的最高机密,很有可能用以破译的专用量子计算机已经接近完工,这绝不是危人耸听,密码世界从来是波诡云谲莫测高深。即使按专家们保守预测,量子计算机的实际应用也许还要等10~15年,但寻找新的密码系统,特别是开发密钥分配的新技术已经刻不容缓,因为新技术从开发到系统的建立和实用也需要时日,所以人们已经到了最危险的时刻。

5 量子密钥技术——维护信息安全的忠诚卫士

面对危局,物理学再次挺身而出力挽狂澜,利用"单量子不可克隆定理"实现密钥配送的绝对安全。"不可克隆定理"(No-Cloning Theorem)是"海森堡测不准原理"的推论,它是指量子力学中对任意一个未知的量子态进行完全相同的复制的过程是不可实现的,因为复制的前提是测量,而测量必然会改变该量子的状态。

图4为量子密钥分配(BB84规约)的原理示意图,图4左图中的小黄球代表单个光子,黑色箭头代表光子的偏振方向,左边蓝色人是信息发送方,而绿色人是接收方。收发双方都手持偏振滤色片,发送方有4种不同的滤色片,分别为上下、左右偏振(第一组)、上左下右、上右下左偏振(第3组)4种滤色片,发送方把不同的滤色片遮于光子源前,就可分别得到4种不同偏振的光子,分别用来代表"0"和"1"。每个代码对应于两种不同的光子偏振状态,它们出自两组不同偏振滤

色片(图4中的左下角,它和通常光通信的编码不尽相同)。接收方就只有两种偏振滤色片,上下左右开缝的“+”字式和斜交开缝的“×”字式。由于接收方无法预知到达的每个光子的偏振状态,他只能随机挑选两种偏振滤色片的一种。接收方如果使用了“+”字滤色片,上下或左右偏振的光子可以保持原量子状态顺利通过(见图4中上面的第一选择,接收方用了正确的滤色片),而上左下右、上右下左偏振的光子在通过时量子状态改变,变成上下或左右偏振且状态不确定(见图4中第四选择,用了错误的滤色片)。接送方如果使用“×”字滤色片情况正好相反,见图4中第2选择(错误)和第3选择(正确)。

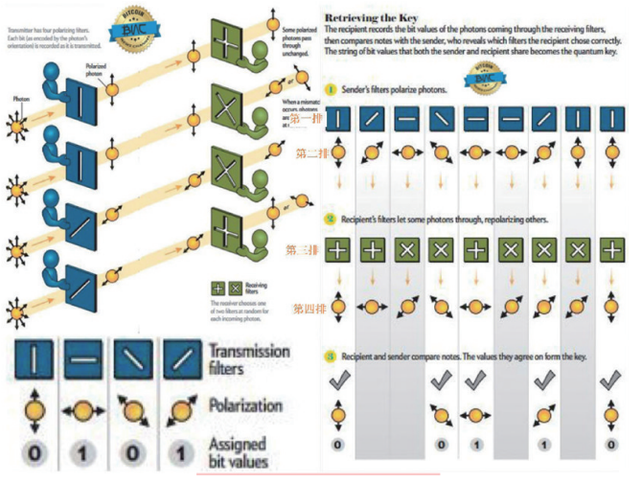


图4　量子密钥分配技术原理示意

Fig. 4　Principle of quantum key distribution

图4右图第1横排是发送方使用的不同偏振滤色片,从左至右将9个不同偏振状态的光子随时间先后逐个发送给下面绿色接收方,这些光子列于第2排。接收方随机使用“+”字或“×”字偏振滤色片将送来的光子逐一过滤,见第3排,接收到的9个光子的状态显示在第4排。

这里是密钥(key)产生的关键步骤:接收方通过公开信道(电子邮件或电话)把自己使用的偏振滤色片的序列告知发送方,发送方把接收方滤色片的序列与自己使用的序列逐一对照,然后告知接收方哪几次用了正确的滤色片(图5,“√”的1,4,5,7,9)。对应于这些用了正确滤色片后接收到的光子状态的代码是:00110,这组代码就是接发双方共享的密钥。

为什么第三者不可能截获这个密钥?假设窃密者在公开信道上得知了接送方使用的偏振滤色片序列,也知道了发送方的确认信息(图5,“√”的1,4,5,7,9),但是窃密者依旧无法确认密钥序列。譬如对第一列,窃密者知道接收方用的是“十”字滤色片,而且发送方确认是对的,但这可能对应于上下或左右偏振的两种不同的光子,它们分别代表“1”或“0”,除了发送和接收双方都清楚知道,窃密者是无法确认的。窃密者真要确认的话,也要在中途插入偏振滤色片来观察,但它又无法事先知道应该使用“+”还是“×”滤色片,一旦使用错误滤色片,光子状态改变,窃密的行为立即暴露。再以第一列光子为例,如果窃密者在接收端前插入“×”滤色片,光子偏振状态可能改变成上右下左的斜偏振,接收方仍使用“+”滤色片,得到左右偏振光子,经确认后此位变成“1”。结果通信双方的密钥在第一位不一致,这种出错经过奇偶校验核对非常容易发现和纠正。通常的做法是通信双方交换很长的光子序列,得到确认的密钥后分段使用奇偶校验核对,出错段被认为是技术误差或已被中间窃听,则整段予以删除,留下的序列就是绝对可靠的共享密钥。量子密钥分配方法除了BB84规约外,还有E91规约。

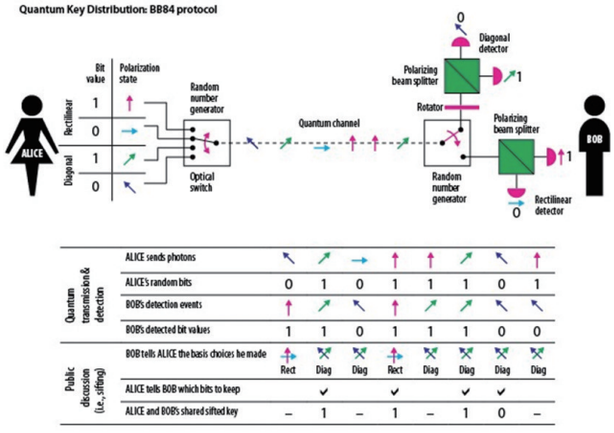


图5　量子密钥分配技术工程示意

Fig. 5　Engineering presentation of quantum key distribution technology

量子密钥分配技术中的密钥的每一位是依靠单个光子传送的,单个光子的量子行为使得窃密者企图截获并复制光子的状态而不被察觉成为不可能。而普通光通信中每个脉冲包含千千万万个光子,其中单个光子的量子行为被群体的统计行为所淹没,窃密者在海量光子流中截取一小部光子根本无法被通信两端用户所察觉,因而传送的密钥是不安全的,用不安全密钥加密后的数据资料一定也是不安全的。量子密钥分配技术的关键是产生、传送和检测具有多种偏振态的单个光子流,特种的偏振滤色片、单光子感应器和超低温环境使得这种技术成为可能。

必须再一次强调,量子密钥分配光纤网络上传送的是单个光子序列,所以数据传输速度远远低于普通光纤通信网络,它不能用来传送大量的数据文件和图片,它是专门用来传送对称密码体制中的密钥,当通信双方交换并确认共享了绝对安全的密钥后,再用此密钥对大量数据加密后在不安全的高速网络上传送。“量子通信”这个词容易使人误解,到目前为止,实际上量子通信指的就是量子密钥分配技术。量子密钥分配光纤虽然是低速网络,但每秒种传送上千位的密钥没有任何问题,通信双方有确保安全的几百位长的密钥,而

且可以随时更换密钥,通信安全就有了非常可靠的保障。量子密钥分配技术的基础是物理而不是数学。面对信息安全危机,物理学再次充当了救世主的角色,它为信息科学的进一步发展筑起了坚实的基础。

6 量子密钥分配技术现状

2013年10月10日,Battelle公司建立了第一条商用量子密钥分配网络,一条全长110 km的专用光纤线路连结了俄亥俄州哥伦布市公司总部和在都柏林分部的办公室,使用的是ID Quantique提供的硬件设备,用来保护公司的财务资料、知识产权、图纸和设计数据。

100 km已经接近量子密钥分配的光纤网络的长度极限了,这是由单个光子在光纤中可以传播的最大距离所决定的。这个问题严重影响该技术的实用价值,目前的解决方案是设立光子传送中继站。这种中继站与通常光通信的放大中继站有本质区别,因为让中继站接收单个光子后又送出一个量子状态不变的光子十分困难,这个中继站必须为通信双方所信任,实际上量子密钥是通过这个可信任中继站接力递送的。

使用量子密钥分配技术的通信双方必须建立点对点连接的专用光纤,但点到点直接相连的网络结构非常不易拓展,这个问题将成为该技术推广应用中更大的障碍。目前一组英国剑桥大学的研究小组开发成功一种新技术,使得量子密钥分配过程能在普通光纤通信线路上进行。这种技术有些像"时分复用"通信,通常的高强度数据激光与微弱的光量子流传送在同一根光纤上按时间分隔高速切换。该技术有相当的难度,通信中的收发两端对两种讯号必须保持精准的同步,而且感应器必须正确适应强度差异十分巨大的两种光信号,犹如一会儿面对太阳,一会儿感应微弱的星光。这种技术使得通信双方可以在同一条光纤上交换密钥,用他人无法截获的密钥对数据加密后按通常方式传送,再也不必担心泄密。

为了让量子密钥分配技术飞入寻常百姓家,美国Los Alamos国家实验室研发了一种QKarD技术(图6)。只要带有闪存U盘大小的一只专用光纤接口,任何用户终端通信设备诸如便携式计算机和手机就可以通过光纤与邻近的中央服务器交换量子密钥。QKarD服务器有些像电话中继交换中心,各终端客户发送光量子向各自邻近的QKarD服务器配送密钥,当各个终端与服务器之间的密钥配送完毕,同时各个服务器之间密钥也配送完毕后,终端用户A将信息用密钥加密后以传统方式送达邻近的QKarD服务器,信息在服务器解密和重新加密后转交另一个服务器,直到接力传送至最终用户B为止。一个QKarD的示范网络已经试运行。据估计,一个连接1000个终端的QKarD服务器价格约1万美元,QKarD终端接口约50美元。量子密钥配送技术正在向人们走近。

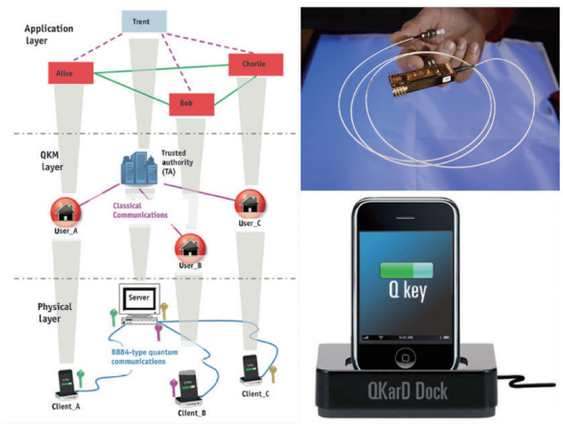


图6 QKarD示意

Fig. 6 QKarD sketch map

7 结论

量子密码技术刚跚跚起步,针对它的黑客早已蠢蠢欲动。目前针对量子密码技术的黑客手段有下列3种。

1)量子密钥的关键是通过一个又一个光子传递密码,中间窃听者无法截取光子而又不改变光子的状态。工程实施时很难保证发射端每个脉冲只含有一个光子,如果每个脉冲有两个以上光子,黑客仍可以只截取一个光子并设法放过另一个光子,让接收端无法感觉到信号已被截取。

2)一组挪威的研究人员通过激光束短暂"致盲"光子感应设备成功地破获传送的量子密钥。这种方法和设备过于专业和复杂,目前还没有构成现实的威胁。

3)针对光子通信的精密脆弱,直接用强激光长时间野蛮干涉,使得量子密码传递双方通过微弱的光子交换过程根本进行不下去。

量子密码技术的应用和推广肯定不会一帆风顺,但有一点必须指出:与其他密码技术不同,量子密钥分配技术从原理上保证密钥配送是安全可靠的,上面所提针对量子密码技术的黑客手段均是工程实施中的问题。原理与实施是完全不同的两个概念,毕竟实施中的技术问题可以逐步解决,不可破译的原理才是该项技术具有发展前途的根本保证,它使人们对量子密钥分配技术的将来充满了信心。

参考文献(References)

[1] Vigenere 密码[EB/OL]. [2017-04-30]. http://blog.sciencenet.cn/home.php?mod=attachment&id=81252.

[2] Public Key. [2017-04-30]. http://blog.sciencenet.cn/home.php?mod=attachment&id=81253.

[3] Han L D, Wang X Y, Xu G W. On an attack on RSA with small CRT-exponents[J]. Science China Information Sciences, 2010, 53(8): 1511-1518.

Quantum key distribution and unhackable communication

XU Lingyu

Plasma Physics Experiment Center, University of California at Los Angeles, Los Angeles, CA 90095, United States

Abstract Quantum key distribution (QKD) uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages. The security of encryption that uses quantum key distribution relies on the foundation of quantum mechanics, in contrast to the traditional public key cryptography, which relies on the computational difficulty of certain mathematical functions and cannot provide any mathematical proof as to the actual complexity of reversing the one-way functions used. The history and future development of quantum cryptography are also briefly discussed.

Keywords cryptography; public key; quantum key distribution

（责任编辑　刘志远）