**量子通信工程走下神坛的原因与真相**

     —京沪量子通信干线开通二周年反思

**作者：徐令予**

**导读**

2017年9月29日是一个不应忘却的日子。二年前的这一天，连接北京、上海，贯穿济南和合肥全长2000余公里的京沪量子通信骨干网络全线开通。当年，被捧上神坛的“京沪量子通信干线”给人们带来了海市蜃楼般的幻觉。

量子通信工程的推动者们通过主流媒体向大众承诺：

“2019年前后，量子通信将会服务于消费者的网上转款和支付。全国性的组网建设将由运营商主导，量子网络标准将建立。2023年有望建成全国量子通信网。”[1]

“量子通信将在不到10年的时间里辐射千家万户。”

“到2030年左右，中国将建成全球化的广域量子通信网络。”[2]

可是在二年过去后的今天，媒体却选择了全体沉默，京沪量子通信干线失去了夺目的光彩，跌落神坛不复返。据可靠消息透露，原计划中的其它量子通信干线建设已经全部停工。中科大的“科大国盾”是全国量子通信设备制造的龙头企业，数据显示，该公司的营收从2016年开始就增长乏力，去年已经出现负增长，到了今年竟然发生了80%的断崖式暴跌[3]。

在数字经济时代，每种有生命力的新技术一旦进入市场，用户数字都是按指数规律增长的，个人电脑、互联网、数码相机、智能手机的发展无不遵循这样的普遍规律。为什么只有“量子通信”反其道而行之，成了市场的弃儿呢？

如果说实践是检验真理的唯一标准，那么市场就是鉴定工程技术的最终手段。一个工程项目如果没有用户的追捧、没有稳定的收益，那么它被市场无情的抛弃只是时间问题，头顶着“量子”的光环又有何用？

众所周知，量子通信还处于基础研究阶段，相关的应用研究刚刚开始，工程建设的可行性、必要性、和经济实用性根本无从谈起。在这种情况下仓促建设京沪、武合等量子通信工程是严重的决策失误，工程项目陷入困境是必然的结果。

导致量子通信工程决策错误原因诸多，密码系统的神秘再加上量子物理的奥妙无疑是造成判断失误的重要因素。工程的推动者对传统密码系统理解不深、把握不准，把工程引入了歧路。某些人甚至掺杂私心杂念故意混淆概念，借科普之名行欺骗之实，致使错误迟迟得不到纠正。所以正本清源还得从严肃的科普教育着手，用科学事实和逻辑推理彻底清除有关“量子通信”中的诸多谬误，把真相还给公众。

本文分成上、下二篇：

《上篇》从密码系统基本原理出发，着重分析量子通信(QKD)的工程用途和实际价值。通信密码可分为对称密码和公钥密码两个系统。QKD是分发“一个”共享密钥的硬件技术，属于对称密码系统中的一个子功能。在对称密码系统中，传统的密钥分发技术安全成熟、价廉物美，QKD由于性能和价格上均处劣势所以难有作为；在公钥密码系统中，需要公钥、私钥“一对”密钥，QKD只能分发一个共享密钥所以与公钥密码系统毫无关系。量子通信工程在整个密码系统中都难有立足之处。

保卫现代信息系统安全的主战场在计算机的操作系统、硬件和应用软件上，不在密码系统方面；而密码系统安全的关键在于密码算法，不在密钥分发。量子通信工程对于国家的信息系统的整体安全而言，好似在飞机上装备安全气囊，它除了添乱不会带来任何益处。把量子通信工程吹捧成国之重器不仅有违事实，而且也是对奋战在信息系统安全领域前沿的科技工作者的不尊重。

《下篇》从量子通信的基本工作原理出发，着重分析QKD技术层面的一系列问题。“极低的成码率”、“不能与互联网兼容”和“极不安全的可信中继站”是QKD的三大技术困境，它们就是量子通信迈向工程实用化道路上难以逾越的三座大山。这里需要特别强调，量子通信所面临的这三大技术困境是被物理原理所决定了的，单靠工程技术的进步是极难取得实质性改变的。

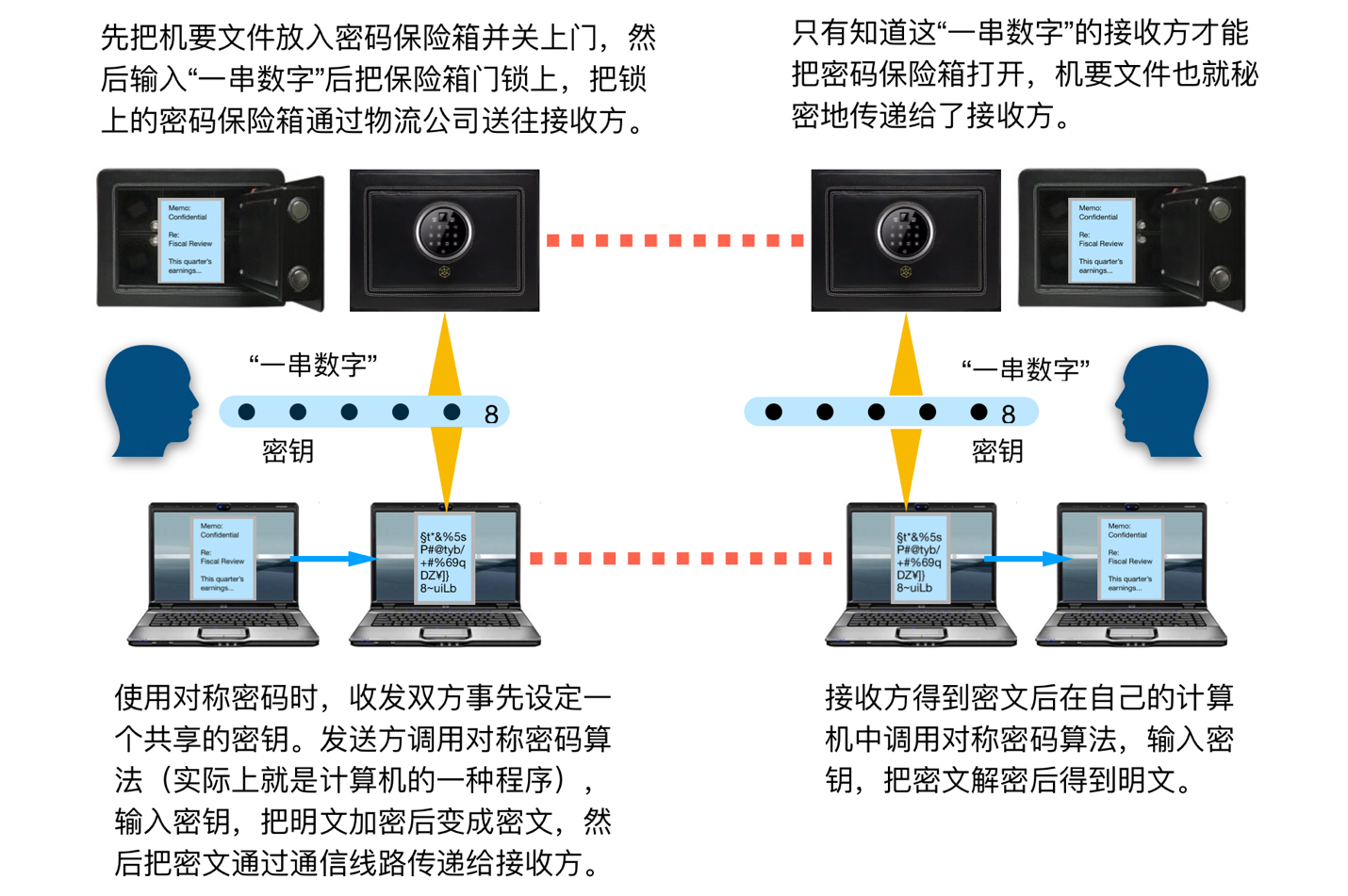
“量子通信的无条件安全性是可以用数学证明的”，“只有量子通信可以拯救公钥密码危机。”是两个毫无科学依据的神话故事，目的是转移视线掩盖量子通信的三大技术困境。虚假的神话故事与真实的工程困境是硬币的两面。量子通信面临的工程困境越是残酷真实，走入歧途的工程推动者越发需要依赖虚幻的神话去掩盖自己的窘态；神话故事越是虚假离奇，只能说明故事的编导者面对的困境太真实太严酷了，他们除了骗人骗已经束手无策。

某些物理学家钻进了理论却远离了现实，执着于知识而忘记了常识。量子通信工程的许多错误其实都是常识性错误，只要通过摆事实讲道理，认清这些错误并非难事。下面的科普文章中没有数学公式，说的都是白话、实话，相信大多数人读了之后，对量子通信工程中的是非对错都不难作出自己独立的判断。言归正传，让量子通信的科普之旅就从这里再次启航。

**上篇 量子通信工程在密码系统中的作用和地位**

为了对量子通信工程在密码系统中的作用和地位作出实事求是的判断，首先要对密码系统中的对称密码和公钥密码的工作原理有正确全面的理解。

密码系统的工作原理很像宾馆中常见的密码保险箱（见图1），有了它就可以安全地保存和传递信息。先把机要文件放入密码保险箱并关上门，然后输入“一串数字”后把保险箱门锁上，只有正确无误地输入同“一串数字”方能打开保险箱取得那份机要文件，因此机要文件的私密性就得到了保障。如果把锁上的密码保险箱通过邮政或者物流公司送达远方，只有知道这“一串数字”的接收方才能把密码保险箱打开，机要文件也就秘密地传递给了接收方。

 图1（上篇）

在密码保险箱传送的整个过程中，只要这“一串数字”始终控制在通信双方的手中，他们就不担心密码保险箱在传送过程中使用什么方法、走什么路线，也不在乎它经过多少黑客间谍之手，因为不知道这“一串数字”谁也甭想打开那个保险箱，信息在传递过程中的机密性就得到了充分的保障。

细心的读者看到这里可能会有一个疑问，不在一处的通信双方如何商量协调出这“一串数字”呢？或者更正确的说怎样才能让通信双方共享“一串数字”呢？当然通信双方只要有过一次“零距离接触”就不存在问题，两人找一个僻静的角落约定“一串数字”就可以了。有了这个“第一次”以后就可驾轻就熟了，担心反复使用同“一串数字”不安全？好办啊，把新的“一串数字”写在纸上，放进密码保险箱送给对方，以后双方就可启用新的“一串数字”。这样的变动可以“天天做”、“月月做”、“年年做”，私密通信绝对有保障。

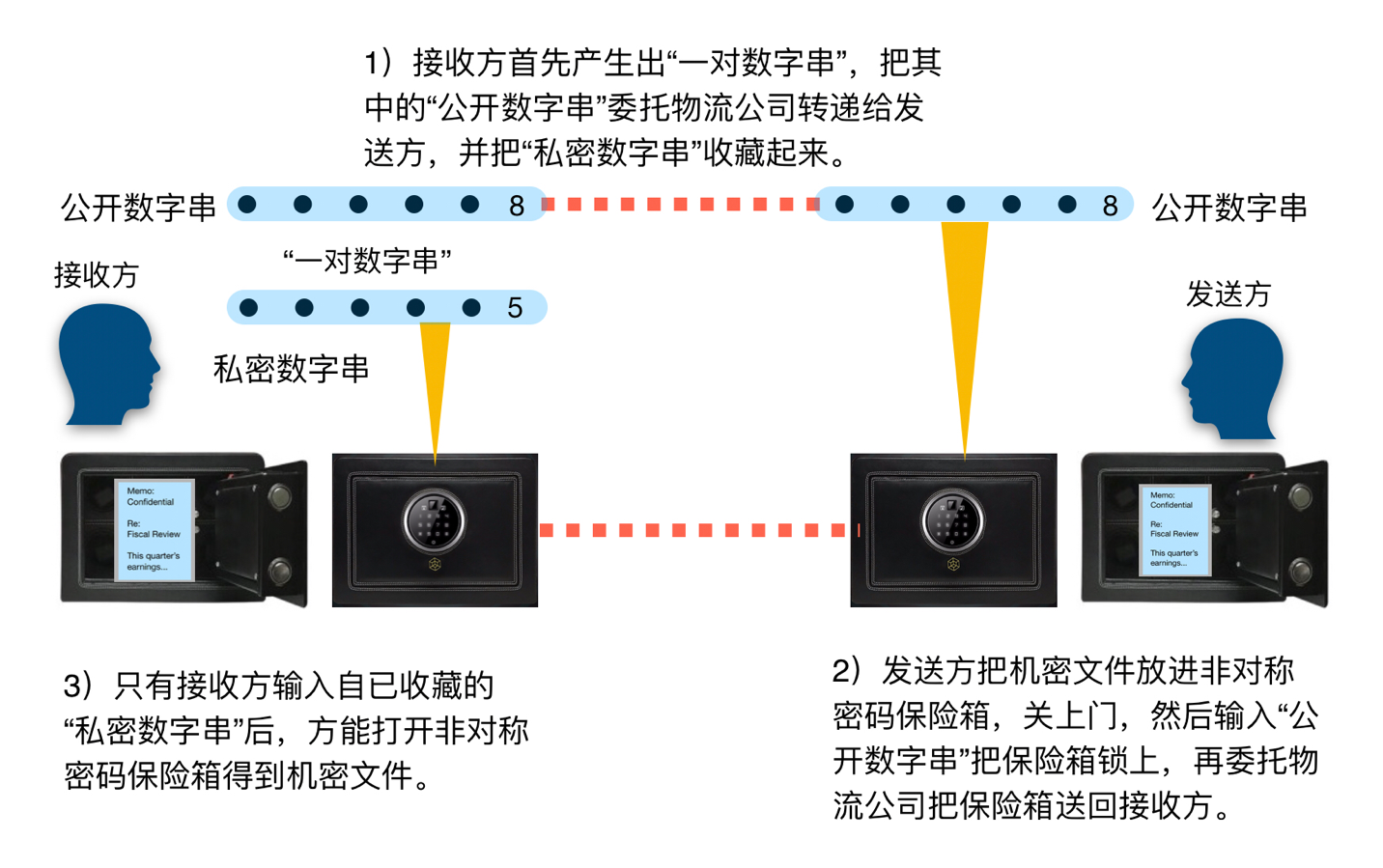
为了后面讨论的方便，我们把锁门和开门使用同“一串数字”的称为“对称密码保险箱”，这也是宾馆中常用的保险箱。这种对称密码保险箱方案适合用在有过“零距离接触”的熟人之间和有严格隶属关系的机构内部，在这种环境中设定用作锁门开门的“一串数字”没有技术困难，使用对称密码保险箱可以保证这些人群和机构之间通信的高度私密性。

但是互联网的出现让“对称密码保险箱”方案遇到了巨大的挑战。难题一，使用“对称密码保险箱”的必要条件是通信双方至少要有过一次“零距离接触”，这个条件在互联网世界很难满足。没有“零距离接触”过的通信双方是无法安全地协商出共享的“一串数字”，因为他们使用电话、电报或者信件传递协商“一串数字”都是不安全的，谁也不能排除“隔墙有耳”，而第三者只要窃取了这“一串数字”就可以打开密码保险箱取得机要文件。难题二，每两个用户使用“对称密码保险箱”前必须通过“零距离接触”建立起“一串数字”，如果互联网的一个通信群体的用户数到达一千万，每个用户就要存放管理好9999999个不同的“一串数字”！这两个难题使得“对称密码保险箱”方案在互联网环境中很难发挥作用。但是没有密码系统保护的互联网通信又是难以想像的。

“需求乃发明之母”，保证互联网通信安全的强大需求推动了一种新型的密码保险箱——“非对称密码保险箱”方案的出台。可以毫不夸张的说，“非对称密码保险箱”方案就是保护互联网通信安全的利器，没有它就不会有互联网今天的风光。

非对称密码保险箱的工作原理其实也不难理解，它也是一只密码保险箱。对称密码保险箱锁门、开门用的是同“一串数字”；非对称密码保险箱使用“一对数字串”，用其中的“一串数字”（又称“公开数字串”）锁门后只能用另“一串数字”（又称“私密数字串”）方能开门，而这二串数字之间的关系又非常复杂，单从“一串数字”极难推算出另“一串数字”。

“非对称密码保险箱”方案使得互联网上非熟人之间也可进行保密通信。使用非对称密码保险箱的通信过程可分解为三个动作，注意这个过程起始于接收方（见图2）。1）接收方首先产生出“一对数字串”，把其中的“公开数字串”写在标签上，然后委托物流公司把写有“公开数字串”的标签转递给发送方，并把“私密数字串”收藏起来；2）发送方先把机密文件放进非对称密码保险箱，然后输入标签上的“公开数字串”后把保险箱的门锁上，再委托物流公司把保险箱送回接收方；3）被“公开数字串”锁上的那个保险箱任何人再也打不开，只有接收方输入自已收藏的“私密数字串”后，才能打开非对称密码保险箱得到机密文件。

 图2（上篇）

在上述通信过程中，“公开数字串”没有一点秘密可言，可对任何人公开。复制、窃取“公开数字串”没有一点用处，因为它只能用来为密码箱锁门，锁上后的保险箱谁也打不开来，除非用“私密数字串”，而“私密数字串”又仅掌握在接收者手中。“非对称密码保险箱”方案使用“公开数字串”和“私密数字串”，由“一对数字串”之间的巧妙配合保证了收发者之间文件传递的私密性。

使用“非对称密码保险箱”方案，收发双方不需要事先商定一个共享的秘密——“一串数字”，他们之间就不需要有“零距离接触”，一次也不需要!通信的接收者只要保护好自己的“私密数字串”，而“公开数字串”是可以公开地、大大方方地传递给发送者，甚至广播通知也行。“非对称密码保险箱”方案使用公、私不同的“一对数字”，使得通信双方可以跨越“零距离接触”这个巨大的障碍，让分隔天南地北的非“熟人”之间都可以方便快捷地进行秘密通信，它对互联网安全功莫大矣！

“对称密码保险箱”和“非对称密码保险箱”这两个方案的关键技术当然都在于设计和制作坚不可摧的密码保险箱。“对称密码保险箱”必须保证在输入“一串数字”锁门后，能且仅能被相同的“一串数字”把门打开；“非对称密码保险箱”存在“一对数字串”，输入其中的“一串数字”锁门后，能且仅能被另外的“一串数字”把门打开。当然如何管理保存好这“一串数字”或“一对数字串”也很重要，但这仅是管理层面的问题，并没有多少技术含量。

明白了上述的道理，就非常容易理解现代通信中的密码系统的工作原理。现代通信使用电报、电话、电邮、微信等等方式，通信过程中传输的是各种电信号（又称明文）。我们当然可以把电讯号录在磁带上，然后放在上述的密码保险箱中，锁上门后传递给对方。但是这样的传递效率太低，我们反其道而行之：不是用密码箱把信息藏匿起来，而是让信息在线路上敞开传输。但是在传输前，先把明文使用某种复杂的变换规则按特定的参数把内容完全打乱，生成无人能看得懂的天书（又称密文），任何人取得这些密文后都无法从中得到任何有用的信息，只有掌握这个特定参数的接收方使用逆向的变换规则才能把密文还原成明文。这就是现代密码学的基本出发点。

日常生活中的密码保险箱与通信密码系统的基本工作原理是十分相似的，区别只是前者把信息藏匿起来不让别人“看到”，而后者把信息彻底打乱不让别人“看懂”，目的都是保障信息的私密性。

现代密码系统使用数学方法把信息彻底打乱，这种专用的数学方法称为“密码算法”。密码算法就对应于密码保险箱，前者把信息打乱、后者把信息藏匿；密码算法对信息加密和解密就对应于密码保险箱的锁门和开门；密码算法加密、解密时使用的参数称为“密钥”，密钥就对应于密码保险箱锁门、开门时输入的“一串数字”。

“对称密码算法”使用共享的“密钥”对明文加密、解密，如同“对称密码保险箱”使用“一串数字”锁上、打开保险箱；“非对称密码算法”（又称为公钥密码算法）使用一对密钥分别称为“公钥”和“私钥”，用公钥对明文加密后只能用私钥解密，如同“非对称密码保险箱”使用“一对数字串”，用其中的“一串数字”锁门后只能用另外“一串数字”开门。

密码算法分成“对称密码算法”和“公钥密码算法”两大类，每一类中又有许多种，就像密码保险箱有许多不同的型号是一个道理。通信双方只要使用同一种密码算法就可以了。

使用对称密码算法时，收发双方事先设定一个共享的密钥。发送方调用对称密码算法（实际上就是计算机的一种程序），输入密钥，把要传递的明文加密后变成密文，然后把密文通过通信线路传递给接收方，接收方得到密文后在自己的计算机中调用对称密码算法，输入密钥，把密文解密后得到明文（见图3）。

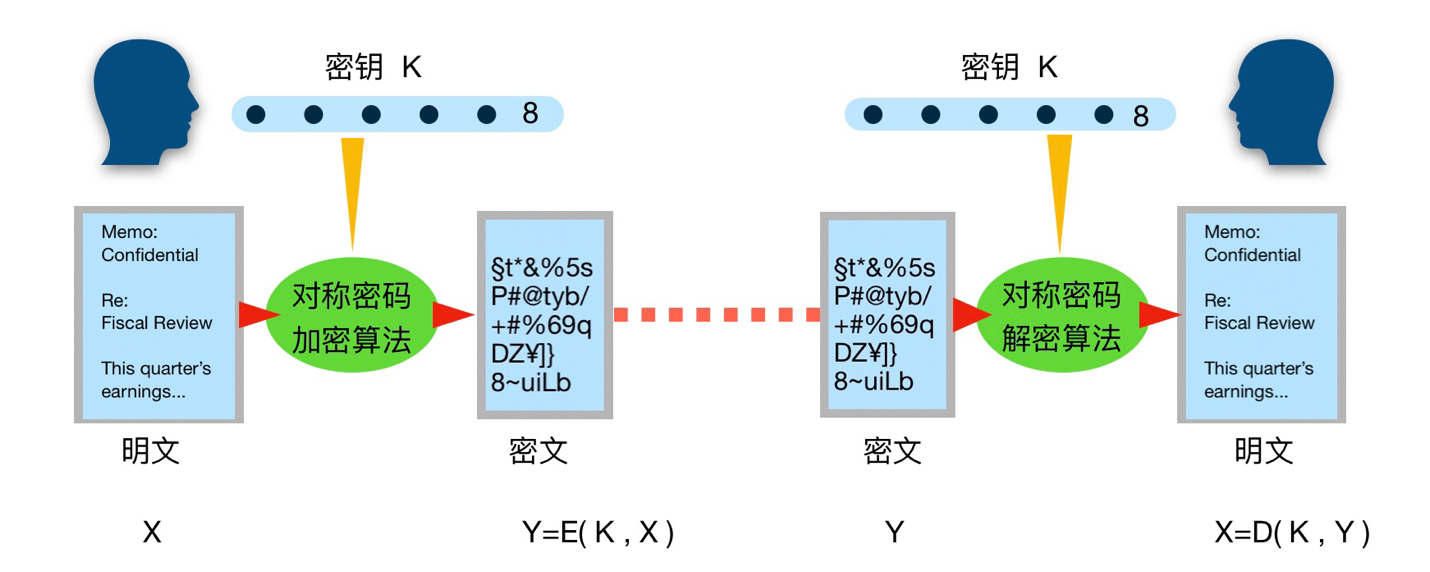


图3（上篇）

使用对称密码算法要求通信双方事先必须设定一个共享的密钥，有了这个初始密钥，双方的保密通信就得到了充分的保障。密钥的更新再也不成问题，因为密钥就是一串字符串，也是一种信息，可以用初始密钥对其加密后传递给对方。在熟人之间和有严格上下级关系的机构内部，通信双方设定初始密钥从来就不是问题。有了初始密钥通信双方可以使用对称密码秘密地传递信息，当然也可以使用对称密码为通信双方不断地更新密钥。

在互联网环境中，通信的接收方产生一对密钥，把公钥通过网络送给发送方，收藏好私钥；发送方调用公钥密码算法，输入接收方送来的公钥，然后把信息加密后产生的密文传递给接收方，接收方得到密文后调用公钥密码算法，输入私钥后把密文解密得到明文。互联网的通信双方常常是先用公钥密码传递密钥，一旦通信双方获得一致的密钥后，再用对称密码保护文件的传递。

有了以上密码系统的基本知识后，就不难看清量子通信工程在密码系统中真实的用途和地位。

所有已建或在建的量子通信工程都不是新的通信技术。量子通信工程与量子纠缠也毫无关系，它们其实只是利用量子偏振态为通信双方分发密钥的一种硬件方法，简称“量子密钥分发”(QKD)。量子通信工程为用户协商出密钥后，还得依赖传统密码算法进行加密解密，因为它根本就没有自己的密码算法，所以量子通信工程从来就不是一个独立完整的密码系统。把“量子密钥分发”(QKD)称为“量子密码工程”是猪鼻子里插大葱——装象，把QKD称为量子通信那更是错得离谱。密码系统的关键技术是密码算法，从来就是算法为王，密钥的分发保存仅是应用层面的问题，并没有多少技术含量。这在前面关于密码系统工作原理的分析中已经阐述得很清楚了。

量子通信工程用硬件分发密钥有什么用处呢？QKD分发的是“一个”共享密钥，再强调一遍：是“一个”密钥，所以QKD只能用在对称密码系统中，仅为对称密码的用户分发一个共享密钥。因为量子通信工程没有自己的密码算法，它依赖于对称密码算法，说到底，量子通信工程仅是对称密码系统中的一个子功能。

我们前面已经反复强调，使用对称密码的用户之间更新和分发密钥没有任何问题。如果对称密码算法是安全的，那么用对称密码算法更新分发密钥也一定是安全的，另辟蹊径使用量子通信工程分发密钥纯属多余；如果对称密码算法本身是不安全的，那么建设量子通信工程为不安全的对称密码分发密钥又有何意义？由此可知，建设量子通信工程毫无现实意义。

事实上，在具有严格上下级关系的企事业环境中，密钥的分发、存放和管理是有专门的机构——密钥分发中心(KDC)负责的。两个终端用户是在KDC的支持和监督下使用对称密码算法取得共享密钥，而且也把身份认证等相关安全问题也一併解决了[4]。在专用企业网环境中，量子通信工程要为对称密码作密钥分发根本没有切入口，它除了添乱不带来任何益处。

在互联网环境中给亿万非熟人之间分发密钥，公钥密码成了唯一的选择。公钥密码把加密解密的核心机密分解在公钥与私钥这样两个密钥中，一个可以公开，把另一个隐藏起来，公钥和私钥的密切配合使得互联网上亿万非熟人之间分发密钥成为可能。量子通信工程用硬件为通信双方只能分发“一个”密钥，而不是“一对”密钥，QKD仍然是对称密码的思维与公钥密码毫不相干，它是无法为互联网上亿万非熟人之间分发密钥的。而且量子通信工程为两个用户之间分发密钥时，必须在两用户之间建立一条点到点直接相连的物理通道，即然用户之间已经“熟悉”到这个程度，那么他们完全可以设定出一个初始密钥，然后用对称密码分发更新密钥，这样岂不是更方便更安全吗？

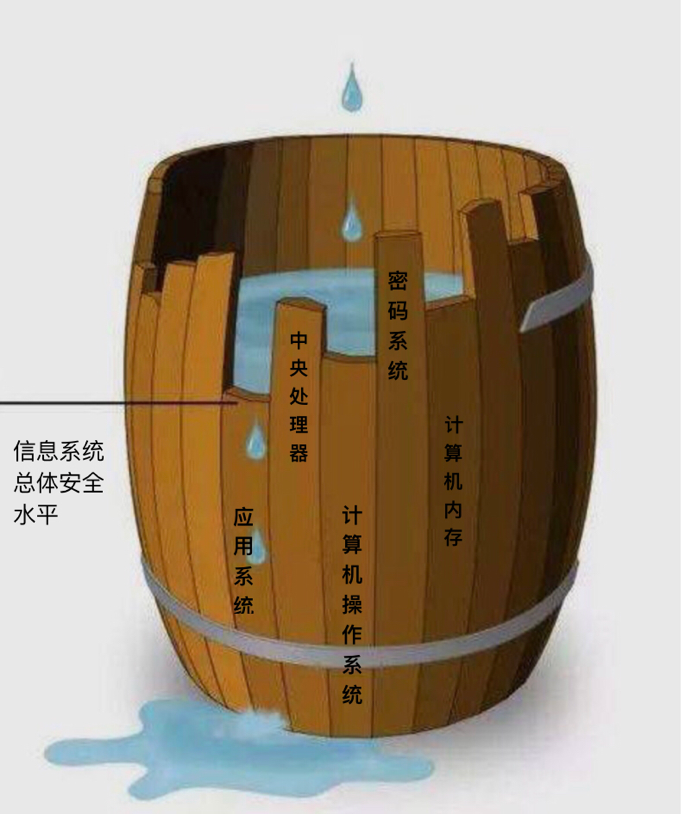
归根结底，公钥密码可以为互不相识而且空间位置不固定的用户之间交换密钥，而QKD完全无法做到这一点，认为量子通信工程这种原始落后的方式可以为互联网亿万用户分发密钥只是异想天开。

量子通信工程从本质上与互联网无法融合，它对于互联网通信安全不可能有丝毫贡献；在企事业环境中QKD性能上不具备优势，价格成本又难以让用户承受。量子通信工程在现代通信的舞台上没有寸土立足之地。

我们还必须认识到，量子通信工程只是为对称密码系统分发密钥，它最多也只能保证密钥分发的机密性。但是密码系统由密码算法和密钥两部分组成，单有密钥的机密性不足以保证密码系统的机密性。密码系统的机密性也远远不能保障通信过程（信道）的安全性。

许多人把通信保密性错认为通信的安全性。当然通信安全一定要求通信内容的保密性，但是只有通信的保密性却不等于通信就是安全的。通信的安全性有着比保密性更高更强的要求，它不仅要求通信双方传送的内容不能被任何第三者知道，还要确认收发双方各自的真实身份，还必须确认通信内容的完整性和不可篡改性，另外还要保证通信的稳定性和可靠性。所以通信的安全性至少应该包括通信的保密性、真实性、完整性、和可用性。在许多通信的应用场景中，通信的真实性和完整性甚至比保密性更重要。因此宣传量子通信工程可以保证通信绝对安全就是个彻头彻尾的谎言。

一个信息系统可以分为信源和信道两个方面，过去安全隐患主要在信道上，保卫信道安全的密码系统就成为了关注的焦点。但是隨着信息系统的数字化，目前信息系统的安全隐患主要发生在计算机的操作系统、中央处理器硬件、计算机内存等方面，信息系统安全的严峻挑战全都来自这些信源、信宿方面。信源、信宿成了保卫信息系统安全的战略前沿，密码系统的地位已经进不了前三甲。



信息系统的总体安全性遵循木桶短板效应。木桶的盛水量受限于木桶的短板高度，同理，信息系统的总体安全性受制于系统中最不安全的因素。提高国家信息系统安全水平最有效的方法应该是增高短板，即把安全工作的重点放在计算机操作系统和各种硬件设备这些短板上。不惜代价增高密码系统这块长板一点也不会改善国家信息系统安全的总体态势，更何况量子通信工程也没有能力增高密码系统的这块长板。鼓吹和推动毫无实用价值的量子通信工程不只是浪费了国家的宝贵资源，它的最大危害性是干涉误导国家信息安全的整体策略。

综上所述，量子通信工程是为用户双方分发“一个”密钥的硬件技术，QKD与使用“一对”密钥的公钥密码系统毫无关系；在对称密码系统中传统的密钥分发技术安全成熟、价廉物美，釆用QKD在性能和价格上均无优势，所以量子通信工程对于密码系统没有任何实用价值。保卫现代信息系统安全的主战场在计算机的操作系统、硬件和应用软件上，不在密码系统方面；而密码系统安全的重点是密码算法上，不在密钥分发上。

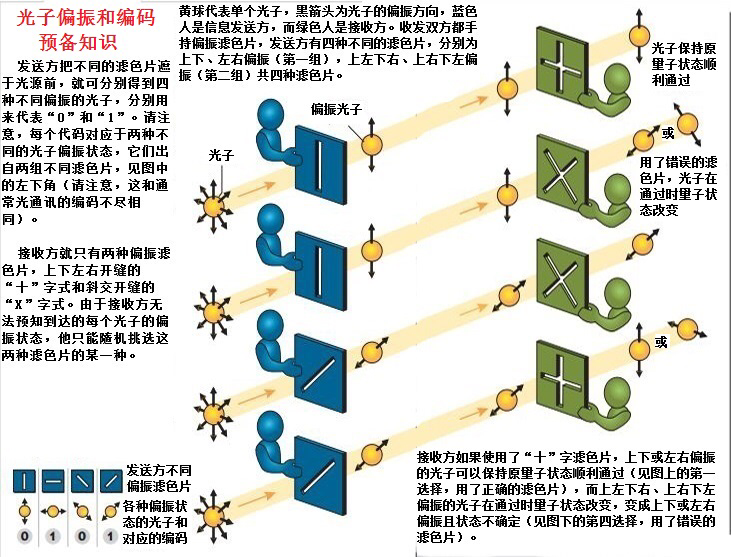
对于国家的信息系统的整体安全而言，量子通信工程不仅毫无用处，而且也无关紧要，把量子通信工程吹捧成国之重器非常幼稚可笑，也是对奋战在信息系统安全领域前沿的科技工作者的不尊重。

**下篇 量子通信工程的可行性分析**

本篇从量子通信(QKD)的基本原理出发，对量子通信工程化的可行性和实用性作出科学的分析判断。

1984年，物理学家Bennett和密码学家Brassard提出了利用“量子不可克隆定理”实现密钥分发的方案，后称BB84协议。协议就是完成通信或服务所必须遵循的基本规则和约定，BB84协议是中国已建和在建的所有量子通信工程的技术基础。

BB84协议与量子纠缠无关，它只是利用光子的偏振态的不可克隆原则秘密地传送密钥。只需对照下面两张示意图并耐心地读完相关的解说文字，对量子密钥分发就不会再有神秘感。图1是提供预备知识，图2是QKD的原理图，BB84协议的工作机制全在这张图中。

 图1（下篇）

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，发送方有四种不同的滤色片，分别为上下、左右偏振（第一组）、上左下右、上右下左偏振（第二组）四种滤色片，发送方把不同的滤色片遮于单光子源前，就可分别得到四种不同偏振的光子，分别用来代表“0”和“1”。请注意，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（见图1中的左下角，它和通常光通讯的编码不尽相同）。接收方就只有两种偏振滤色片，上下左右开缝的“十”字式和斜交开缝的“X”字式。接收方如果使用了“十”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（见图中第四选择，用了错误的滤色片）。接送方如果使用X字滤色片情况正好相反，见图中第二选择（错误）和第三选择（正确）。

有了以上的预备知识，就不难理解QKD技术了。图2第一横排是发送方使用的不同偏振滤色片，从左至右将九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，这些光子列于第二排。由于接收方无法预知到达的每个光子的偏振状态，他只能隨机挑选使用“十”字或“X”字偏振滤色片将送达的光子逐一过滤，见第三排，接收到的九个光子的状态显示在第四排。

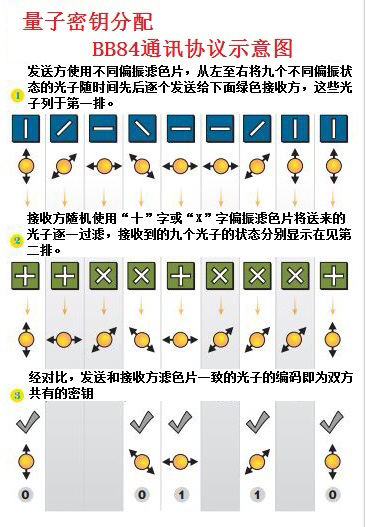


图2（下篇）

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（打勾✔️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，接发双方对此都心知肚明、毫无疑义，这组代码就是它们两人共享的密钥。

为什么第三者不可能截获这个密钥呢？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（打勾✔️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，它们分别代表的是“1”或“0”，当然发送和接收的双方对“1”还是“0”的认定不存在问题，而窃密者无法在公开信道上获取确定值。

窃密者如真要确认的话，必须在光子传送途中插入偏振滤色片进行观察，但它又无法事先知道应该使用“十”还是“X”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“X”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“十”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，只要出错，无论是技术误差、信号干扰还是被人窃听，一律整段予以刪除，防止密钥被窃。

BB84协议分发的密钥的每一位是依靠单个光子的量子偏振态传送的，窃密者企图截获并复制单个光子的量子状态而不被察觉原则上是不可能的，这是由“量子不可克隆定理”决定的。“量子不可克隆定理”(No-Cloning Theorem)是“海森堡测不准原理”的推论，即对任意一个未知的量子态进行完全相同的复制是不可实现的，因为复制的前提是测量，而测量必然会改变该量子的状态。所以BB84协议分发的密钥具有较强的保密性。

BB84协议虽在理论上具有较强的保密性，但为此也付出了沉重的代价。首先，该方案要求使用理想的单光子源和单光子探测器；其次，为了分发密钥必须在通信双方的两点之间建立两个通道：传统的公共信道和通信双方之间直接相连的量子信道；更令人纠结的是该方案很难分辨出干涉信号和窃密行为之间的区别，只要受到任何轻微干涉必须放弃密钥分发过程。“量子通信”使用的BB84协议就是温室䁔房中弱不经风的林妹妹—“心比天高命比纸薄”。说到底，BB84协议就是一个物理实验室中的示范方案。

量子通信从象牙塔走向工程化的征途上有以下三条难以跨越的鸿沟：

一）**量子通信技术困境之一：极低的成码率**

理想单光子源价格太过昂贵，是BB84协议走向实用的不可承受之重。BB84的升级版“诱骗态量子密钥分发”放弃了单光子方案改用微弱激光，但是密钥的传输仍然依靠数量极其有限的光子，量子通信过程中有效信号太弱的本质没有什么改变。

众所周知，任何通信环境中都有噪声污染。在具有噪声环境中保证信号传递的准确无误的对策很简单，要想在嘈杂的酒吧里与人交谈，无非就是“放开嗓门加大音量”或是“放慢语速不断重复”这两个办法，研究数据最大传输速率的香农定律讲的就是这个道理。在量子密钥分发中量子信号太弱，所以“放慢语速不断重复”就成了唯一可选项，用专业术语来描述，就是QKD的成码率极低。

密钥分发的成码率是单位时间内生成有效的共享密钥总位数。成码率是密钥分发最重要的技术指标，它反应了密钥分发的效率，也决定了该技术的应用范围。目前QKD在百公里距离上的成码率仅为Kbps量级，而目前光纤数据通信速率可达Tbps量级，两者相差了9个数量级，也就是十亿倍！

而所谓绝对安全的“量子通信“又必须要求“密钥与明文等长”和“一次一密”，也就是说QKD的成码率必须不低于光纤的数据通信速率。由此可知，蜗牛般低速的成码率使得量子通信要为现代化通信保驾护航永远只能是不切实际的幻想。如果强制使用量子通信，其结果必然把目前的通信速度至少降低千万倍！

二）**量子通信技术困境之二：不能与互联网兼容**

QKD的基础是美国科学家在1984年制定的BB84协议，BB84是前互联网时代留下的技术活化石。这种点到点的密钥分发技术要求在通信双方之间建立一条被双方独占的直接的物理通路，这种通信方式只能使用电路交换协议（Circuit Switching）。电路交换协议与分组交换协议（Packet Switching )从基础原理上水火不容，而分组交换协议正是构建现代互联网的基础。这就从根本上断绝了QKD组成现代通信网络与互联网兼容的可能性，它为互联网通信安全提供有效的服务也就无从谈起。这是京沪量子通信干线工程至今未有广泛应用的一个根本原因。

三）**量子通信技术困境之三：极不安全的可信中继站**

由于QKD的光子带有量子特性，所以在QKD的量子信道中不能使用放大器，这就决定了QKD的最大有效距离不会超过百公里。远程QKD工程只能使用可信中继站技术，密钥在每个可信中继站转换成不加密的电信号，一站又一站接力传递至远方。京沪量子通信干线就在沿线设立了三十多个可信中继站，中继站之间距离约为60公里。

密钥在两个中继站之间是以量子状态传递的，中间窃听可以被发现，但是密钥在每个可信中继站是以传统电信号的明文格式存在的，而这些可信中继站对密钥进行处理存贮的计算机又必须联网的，QKD窃听必被察觉的原理不适用任何一个可信中继站内部，这就给QKD工程带来极为严重的安全隐患。使用卫星QKD技术尚在实验阶段，事实上它也不能跨越“最后一公里困境”，本质上还是被卡在可信中继技术的死穴里。

传统加密通信系统中，信道包括光纤、中继器、路由器、交换机、防火墙等，信息在这些地方都是以密文方式传送，安全是有保障的。但是量子通信的可信中继站其实已经不只是单纯的信道了，由于密钥以明文形式出现，使得每个中继站变成了信源、信宿。传统京沪通信光缆就是一个完整单一的信道，加密生成的密文不怕被窃取，但是京沪量子通信干线这个2000多公里的信道切成30多段，每段的中继站都是信源、信宿。这在原本很安全的系统中，人为添加了30多个极为严重的安全隐患！

攻击传统通信干线的唯一手段是破解密码，而攻击京沪量子通信干线除了破解密码以外，京沪量子通信干线的30多个可信中继站全都可能成为黑客的攻击目标。黑客既可利用这些中继站的计算机系统的安全漏洞发起攻击，也可在中继站的上百个工作人员中寻找突破口。黑客通过以上手段窃取密钥比直接破解密码要容易得多，所以京沪量子通信干线的安全性远低于传统加密通信干线。

这里需要特别强调，量子通信所面临的这三大技术困境是被物理原理所决定了的，单靠工程技术的进步是极难取得实质性改变的。

面对上述三大技术困境，正确的方法应审时度势，静下心来加强基础研究，应该考虑扬弃三十多年前IBM的BB84协议，寻找量子通信的全新模式。可惜中国的量子通信团队反其道而行之，非要吊在BB84这棵枯树上，把技术上不成熟又毫无使用价值的BB84协议包装成为工程项目，完全置工程的实用性、可行性、必要性和经济效益于不顾，实属罕见。

为了掩盖量子通信的三大技术困境，就转移视线泡制了两个神话故事。1）“量子通信的无条件安全性是可以用数学证明的”；2）“只有量子通信可以拯救公钥密码危机。”

这两个神话故事就成了对付量子通信批评质疑的挡箭牌。神话故事背后的潜台词就是：虽然量子通信工程有许多技术障碍，但它是无条件绝对安全的，“一好遮百丑”，所有的技术缺陷只能将就吧；虽然量子通信并不具备工程建设的可行性，但传统密码的天空都要塌了，甭多想了不惜代价先上工程再说吧。

以上两个神话故事成了某些人对抗量子通信批评质疑的护身符，也是他们陷入量子通信建设泥潭后手握的最后两根救命稻草。这两个神话误导了许多人、也欺骗了很长时间，现在该是揭露其真相的时候了。

四）**量子通信神话之一：量子通信的无条件安全性可以用数学证明**

众所周知，传统密码系统基于数学原理，而量子通信是基于物理原理。“量子通信专家”反复宣称：基于数学原理的传统密码的绝对安全性是无法用数学证明的，但是基于物理原理的量子通信的绝对安全性却是可以用数学证明的。能编造出这样离奇的谎言大概也算是创新吧。

“量子通信的无条件安全性是可以用数学证明的”实际上来自两个完全独立的命题：“量子通信的物理过程可以抽象出一个数学模型”，“量子通信的数学模型的无条件安全性是可以用数学证明的”。而“量子通信的无条件安全性是可以用数学证明的”是由前两个命题拼湊出来的一个新命题，它不是三段论逻辑推演的结果，即使前两个命题都是真命题，也不能保证这个新命题就是真命题。

举个例子，气象专家把大气运动过程抽象出一个数学模型，然后利用大型电子计算机求解数学模型中的动力学方程组来制作天气预报。这几十年来，数学建模做得尽善尽美，电子计算机求解方程组的精度要多高可以有多高，但是谁也不会认为天气预报是绝对无条件正确的。从技术水平和成熟程度上来看，量子通信的数学建模和建模后的数值分析的二个方面都较气象预报差之甚远，因此“量子通信的无条件安全性是可以用数学证明的”只能是个伪命题。

事实上到目前为止，“量子通信数学模型的无条件安全性是可以用数学证明的”命题的真实性也一直有争议的，只需查查有关量子通信安全性证明的论文就一清二楚了[5][6]。退一万步，即使量子通信的抽象数学模型将来被证明是无条件安全的，也不能证明量子通信真实的物理过程是无条件绝对安全的，因为数学模型不等于真实的物理过程。无论数学模型做得多完美，它只可能是真实世界部分的和近似的反映，对模型的任何分析和证明只能是真实世界特性的近似结果。

通过QKD取得共享密钥的全过程不单纯是量子力学过程，所以量子力学的不可克隆原理无法保证通过QKD获得的密钥具有绝对的私密性，QKD也不能保证分发的密钥是真随机数，因而使用QKD得到密钥作加密就存在被第三方破解的风险。更可笑的是量子通信推动者错误地把宝都压在了通信的保密性上，殊不知，通信的保密性、真实性、完整性、和可用性共同保证了通信的安全，它们是不可分割的集体。量子通信不仅在理论上无法保证通信的绝对保密性，它对保证通信的真实性、完整性、和可用性等方面更是捉襟见肘、无能为力。“量子通信在理论上是无条件安全的”这句话听上去更像是一种讽刺。

五）**量子通信神话之二：QKD可以拯救公钥密码危机**

第二个神话编造了如下一个故事：传统公钥密码的安全性无法得到证明，更可怕的是，当量子计算机进入实用阶段后，公钥密码会被轻易破解，这将导致通信系统的灾难。敌对势力甚至现在可能就在收集那些依靠公钥密码保护的文件，等待量子计算机出来后将逐一破解，因此不顾一切地投入量子通信建设是情有可原的。

利用量子计算机在基础研究中的一些成果，宣传量子计算机可以轻易地破解公钥密码，这已经太夸张了，同时又把量子通信工程打扮成拯救公钥密码危机的白马王子，那更是错上加错。

事实上，能够破解1024位字长公钥密码的量子计算机如果真能造出来的话，那也是在遥远的将来。公钥密码远不是想像中那样的脆弱，抗量子攻击的公钥密码算法（PQC）的研究已经取得实质性成果，新一代的量子计算机无法破解的公钥密码算法产品已经投入测试阶段，公钥密码无需英雄救美。

把量子通信打扮成拯救公钥密码危机的白马王子更是自作多情、不自量力。量子通信工程没有自己的密码算法，它只能为确定的“熟人”之间分发一个共享密钥，本质上仅是对称密码中的一个子功能。如果把公钥密码比作智能手机，那么量子通信工程顶多只能算作固定座机电话。认为固定座机可以代替智能手机的想象力实在也太丰富了。

西方有这样一句谚语:“Be careful what you wish for, it might just come true”（许愿要小心，预想成真并非是好事。）我劝量子通信的推动者就不要再天天咀咒公钥密码了，如果有一天公钥密码真的崩溃了，量子通信才真正脸面扫地走到尽头了。因为到那时人们恍然大悟量子通信原来是百无一用的银样蜡枪头。

“量子通信的无条件安全性是可以用数学证明的”、“只有量子通信可以拯救公钥密码危机”是两个毫无科学根据的神话故事，“极低的成码率”、“不能与互联网兼容”和“极不安全的可信中继站”是量子通信工程无法逾越的三座大山。编造和宣传这两个虚假的神话故事目的是为了掩盖量子通信面临的实实在在难以解决的工程困境。虚假的神话故事与真实的工程困境是硬币的两面。量子通信面临的工程困境越是残酷真实，走入歧途的工程推动者越发需要依赖虚幻的神话去掩盖自己的窘态；神话故事越是虚假离奇，只能说明故事的编导者面对的困境太真实太严酷了，他们除了意淫没有任何其它的对策。

“假作真时真亦假，骗的多是吃瓜人。”京沪量子通信工程完工已有二年，上述三大技术困境一个也没有得到解决，量子通信工程的现在只剩下各级政府买单了。工程投资的费用就不去说它了，现在估计连日常运营维护都无法自理。

工程项目都是效益为王，用户说了算。京沪量子通信工程建成开通已经整整二年过去了，经济效益和用户体验揭示了问题的本质，在这些铁的事实面前一切文字也许是多余的。

“言者谆谆、听者藐藐”，笔者从不奢望能劝醒某些装睡的人。“我们坚持做一件事情,并不是因为这样做一定会有什么效果，而是坚信这样做是对的。”只要有读者能从本文的科普中有所收获和感悟，笔者就心满意足了。

参考文献

[1]2016年08月16日2016年08月16日08:42 来源：科技日报

https://kknews.cc/zh-my/science/oxb6jo.html

[2]新华网 2016年08月16日 08:46:51 | 来源：新华社

http://www.xinhuanet.com//politics/2016-08/16/c\_129232685\_4.htm

[3]根据容诚会计所出具的《审计报告》(会审字[2019]6719 号)，2016年度、2017年度、2018年度、2019年 1-6月，科大国盾的主营业务收入分别为 21,029.28万元、27,248.17万元、25,690.88万元和 2,255.83万元。

[4] https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture10.pdf

[5] Security of Quantum Key Distribution

https://ieeexplore.ieee.org/document/7403842

[6] A Correct Security Evaluation of Quantum Key Distribution

https://www.tamagawa.jp/en/research/quantum/bulletin/pdf/Tamagawa.Vol.4-1.pdf