**量子通信在理论上真的是无条件安全吗？错、错、错！**

**作者：徐令予**

所有已建和在建的量子通信工程都不是新的通信技术，它们也不是保证通信安全的独立完整的密码系统。量子通信工程也与量子纠缠毫无关系，它们其实只是利用量子偏振态为通信双方协商获得共享密钥的一种硬件技术，简称“量子密钥分发”技术(QKD)。

BB84协议是QKD的技术实施方案，它早在1984年就提出来了。三十多年过去了，环顾全球，量子通信究竟又争得了多少自愿付费的热诚用户呢？比起互联网技术、公钥密码、数码相机和无线移动设备数十亿的用户数，量子通信用户的真实数字从来都不好意思晒出来的。请注意，这些几乎都是同时代的技术，数码相机和无线移动技术开始得还要晚一些。这些技术从无到有迅猛发展，很快飞入了寻常百姓家，成为了现代人的生活必需品，唯有量子通信名落孙山。这背后是有着深刻的原因的。

其于量子力学原理的QKD本质上是一种硬件技术，与传统密码这种基于数学原理的软件技术相比，QKD工程的建设维护成本昂贵、组网困难、密钥分发效率低下、可靠性差。它既不可能替代传统密码技术，又很难与传统密码兼容配合。量子通信一开始就站到了历史的错误一方，背离了这几十年互联网引起的通信技术发展的主潮流。

QKD的这些先天基因缺陷阻碍了该技术的发展和推广。但是人们却迷信“量子通信在理论上是无条件安全的”，量子通信就是靠着这根救命稻草勉强维持到了今天。

如果“量子通信在理论上是无条件安全的”这个命题是正确的，那么就必须证明以下三个命题全都是正确的：1）量子通信为通信甲、乙双方分发密钥时只发生了量子物理过程，是量子物理的“不可克隆定理”保证了量子密钥分发具有绝对的私密性；2）甲方使用绝对私密性的密钥加密产生密文，这样的密文只能被乙方解密，没有任何第三方可以破解；3）由于传递的密文是不可破解的，甲乙双方之间的通信就是无条件安全的。

不幸的是，这三个命题却是错、错、错！第一个命题违反了物理学原理；第二个命题是以偏概全，缺乏对香农的“保密系统的通信理论”的全面理解；第三个命题是对密码学通信安全标准的误解。本文将列出三篇有代表性的相关论文作为依据，对上述三个方面的错误逐一作出分析和批评。

**一）物理学原理不支持“量子密钥分发具有绝对的私密性”**

“量子密钥分发具有绝对的私密性”的护身符是“量子不可克隆定理”，只有量子物理的“不可克隆定理”才能保证传递密钥信息的光子的量子状态不可能被任何第三方截取、测试而又不改变它们，也就是说“任何窃听必然被发现”。这是“量子密钥分发具有绝对私密性”的唯一原因。

但是请注意，“量子密钥分发”所分发的绝不是“量子的密钥”，而是以电信号形式存在的传统密钥，QKD的精确定义是以量子方式分发传统密钥。所以量子密钥分发的过程中必然存在从电磁信号转换为光子量子态，再从光子量子态转换为电磁信号这样一系列的物理过程。认为量子通信中只发生了量子物理过程是极其严重的误解。

量子通信分发密钥的对象其实都是生活在宏规世界中的人，他们需要的只能是宏观意义上的传统物理量。所以QKD必须使用传统物理方法转换、制备、测试光子的量子状态，必然需要调控光源、变更滤波器件、和转换光电信号，这一系列过程就必须依靠电磁效应，甚至会涉及机械效应。这就必然会产生相应的电磁辐射，如果有机械运动则还会有声波产生。测试、复制这些电磁辐射和声波是不受“量子不可克隆定理”约束限制的，因而第三方攻击者完全可以通过探测相应的电磁辐射和声波来窃取相应的密钥信息，这种窃密行为是很难被察觉的。

当然这些电磁辐射和声波都非常微弱，但是在理论上它们绝不是零存在。我们千万不能低估现代探测技术的威力，要知道现代信号处理技术甚至可以探测到十多亿光年之外的引力波，认为几十米外的电磁辐射无法探测是毫无科学根据的。当然在QKD二端可以设置法拉第屏蔽网，但是这只能降低但不能彻底消灭电磁辐射，对声波的绝对隔离也极为困难。QKD的通信二端又有光纤连接，另外还一定要有电气线路连接用作信号对比和纠错，要完全消除这些地方的电磁泄漏是不可能的任务。

原则上，我们完全可以在QKD的线路两端建立针对电磁辐射和声波的高灵敏度多频段的接收设备，然后把所有信号先记录下来。每年一百万美元的小额预算将足够让攻击者每秒存储一千兆字节的数据。有了这些大数据，再加上AI算法，攻击者就可以获得甲乙双方通过量子通信传递的密钥的部分或全部信息。

如果目前的算法和计算机的能力还不足以破解QKD传递的密钥，但是我们可以把所有相关数据先存放下来，随着技术的飞速进步，这些量子通信传递的密钥总有破解之时，至少你是无法证明永远无法破解的。嘿嘿，怎么听上去有些“似曾相识”。

一点没错，这里用的逻辑完全拷贝来自量子通信的推动者，我可不敢掠人之美。明明目前的公钥密码没有问题，量子计算机对它的安全威胁还在遥远的未来。但量子通信的推动者辩称：虽然对公钥密码目前是无法破解，但是敌人可以先把密文截取并存放下来，你没有办法证明以后的技术也破解不了吧？为了应对将来潜在的风险，所以量子通信工程技术尽管不成熟也必须仓促上马。

但是现在用同样的逻辑推理可以证明量子通信与传统密码都不具有长时效的安全性。对量子通信的攻击也不需要“实时”完成，攻击者也可以保存信息供将来解密，攻击者而且也可利用未来更强大的技术获取密钥。量子通信比他们想要替代的公钥密码具有更严重的安全隐患，而且量子通信也根本无法替代公钥密码，那么现在建设量子通信工程的理由究竟又在哪里呢？我这是“以其人之道，还治其人之身。”

量子通信的收发方可以通过屏蔽等方法降低电磁辐射，但是公钥密码也可以通过加长密钥字长让破解变得更加困难。一般而言，电磁辐射的降低对攻击者困难会带来多项式增长，但是密钥字长的增加会给破解困难造成指数式增长，换言之，破解量子通信比破解公钥密码更简单容易。能够攻击公钥密码的量子计算机还在遥远的未来，但是攻击量子通信只需功能强大的电子计算机，攻击现在就可开始。须知破解密码有非常强的时间性，密码被今年破解与十年后破解的意义差之十万八千里。既然破解量子通信更早更容易，那么急于要用量子通信去替代公钥密码究竟用意何在？

千万别以为前面的分析仅是纸上谈兵。相反，自从BB84协议问世以来，通过类似手法成功破解量子密钥分发的例子已经发生多起，此类攻击方法已经被定义为“旁道攻击”，成为了QKD的一个研究分支。

量子通信专家Gilles Brassard对量子通信的安全性的评价十分幽默：

“unconditionally secure against any eavesdropper who happened to be deaf!”

译文：量子通信可以“无条件地抵御任何失聪的窃听者！”（讽刺量子通信只能够防御那些侦探行为受到限制的攻击者）。他的批评其实与前面的分析殊途同归、不谋而合，都是从全息原则(holographic principle)出发否定了量子通信密钥分发具备绝对私密性。

其实除了全息原则外，在物理原理层面上，量子通信的理论安全性还受到诸多其他的批评和质疑。比较特出的有：量子近似克隆攻击；利用将来的量子计算机对BB84传送的量子位作纠缠、存贮和事后测试；量子引力场的潜在风险等等。对这些问题感兴趣的请先阅读本文参考文献[1]，然后顺藤摸瓜可以找到许多更有价值的资料。

通过以上的分析可以确定：“量子密钥分发具有绝对的私密性”是经受不了物理学原理验证的。

**二）香农的“保密系统的通信理论”不能保证“QKD生成的密文是绝对不可破解的”**

现在我们退一步，让我们立法不准使用物理全息原理收集和存贮广谱的电磁辐射，用法律和更多的警察来保护密钥分发的绝对私密性，假设通过量子通信获得了绝对私密的密钥，由此生成的密文就绝对不能被破解了吗？遗憾的是，这个结论依旧是完全错误的。错误的根源是对香农的“保密系统的通信理论”的偏见。

首先需要说明，目前的所谓量子通信指的就是量子密钥分发(QKD)。甲乙双方通过QKD传递的不可能是任何有意义的秘密，发送方通过QKD甚至无法送出“Hello”这样一串简单的字符。QKD只是让甲乙双方协商出一串毫无含义的0和1的二进制数字。甲乙双方共享了这串数字后用它作为密钥，甲方用此密钥对需要传递的信息加密后把密文通过任何不安全信道发送给乙方，乙方用共享的密钥对密文解密，得到明文。

即使量子通信可以保证密钥分发具有绝对的私密性，使用量子通信产生的密钥对文件加密后产生的密文就绝对不能被破解了吗？又错了!

理论上要保证甲乙双方通信内容绝对不会被第三者破解，香农列出了以下三个条件：

1）密钥的长度跟明文一样；

2）密钥是一串真随机字符串；

3）每传送一次密文后立即更换密钥，即“一次一密”。

满足这三个条件的密钥又称为“一次性便笺”(one-time pad)。信息论鼻祖香农(Claude E. Shannon)从数学上证明了：密钥如果满足这三个条件，就能确保密文绝对不可被破解(unbreakable)。意思是攻击方无论有多强的计算能力，都不可能从密文中得到任何信息，密码学者又把此定义为信息理论级安全(information theoretic security)，用来替代“无条件”、“绝对”这类非专业词汇。

用上述三个条件来审视量子通信。条件1和3在实际应用中很难满足，这里先按下不表，对此我会另写专文作详细分析。我们现在先把目光聚焦在条件2上，这是本文的第二个重要内容。

密钥是一个真随机数是保证密文不可破解的关键。一个二进制的真随机数就是其中每位出现“1”和“0”的几率完全相等各为50%，而且所有位于位之间的取值必须完全独立。真随机数的定义看似简单明了，但实现起来却非常非常的困难。产生真随机数的密钥不仅长年来困扰着传统密码界，事实上也一直是QKD发展的重要障碍。

这里必需强调指出，量子物理中利用量子态随机坍缩产生真随机数与QKD通过BB84协议产生随机密钥是二个完全不同的概念。在BB84的过程中，代表密钥的量子状态在产生后要经历：传输、干涉、测试、比对、纠错等一系列复杂的过程。其中的干涉不仅有被动的噪声干扰，更有攻击者的主动干涉。攻击者甚至可以截取光量子后把某些特定状态的光量子丢弃，破坏密钥的随机性。攻击者也可通过在量子信道的干涉同时，观察通信双方在公开信道上交换对比信息来获取密钥的随机性规律。总之，QKD交换分发的密钥不可能是真随机数。由此可知，“量子通信产生的密文是绝对不可破解的”是没有科学依据的。

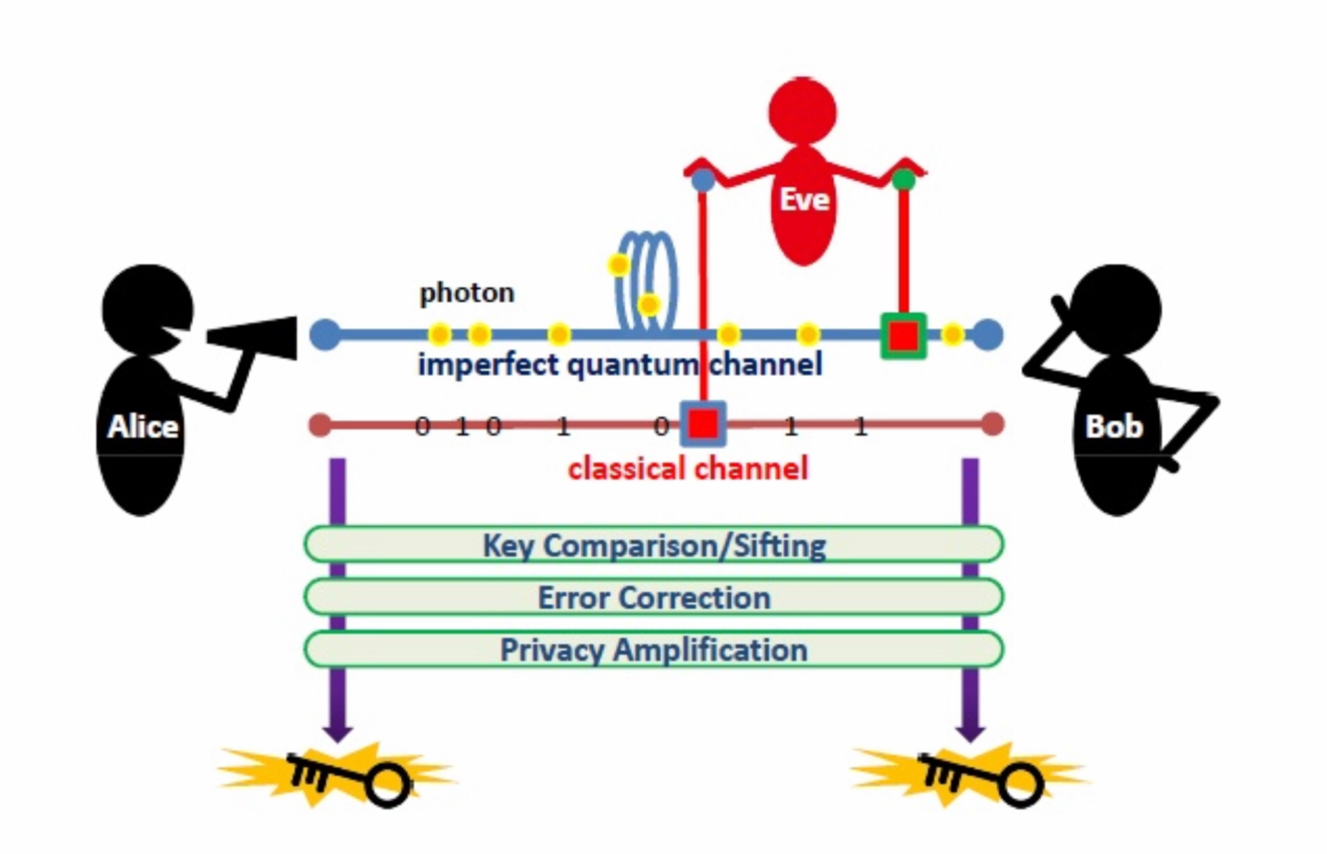


图1：QKD的典型协议。 两个用户Alice和Bob，通过量子子信道和经典信道进行通信以建立初始密钥，然后对其进行纠正，并通过隐私放大（用于提高安全级别）进行压缩生成最终的密钥。攻击者Eve可以同时拦截量子和经典两个频道。

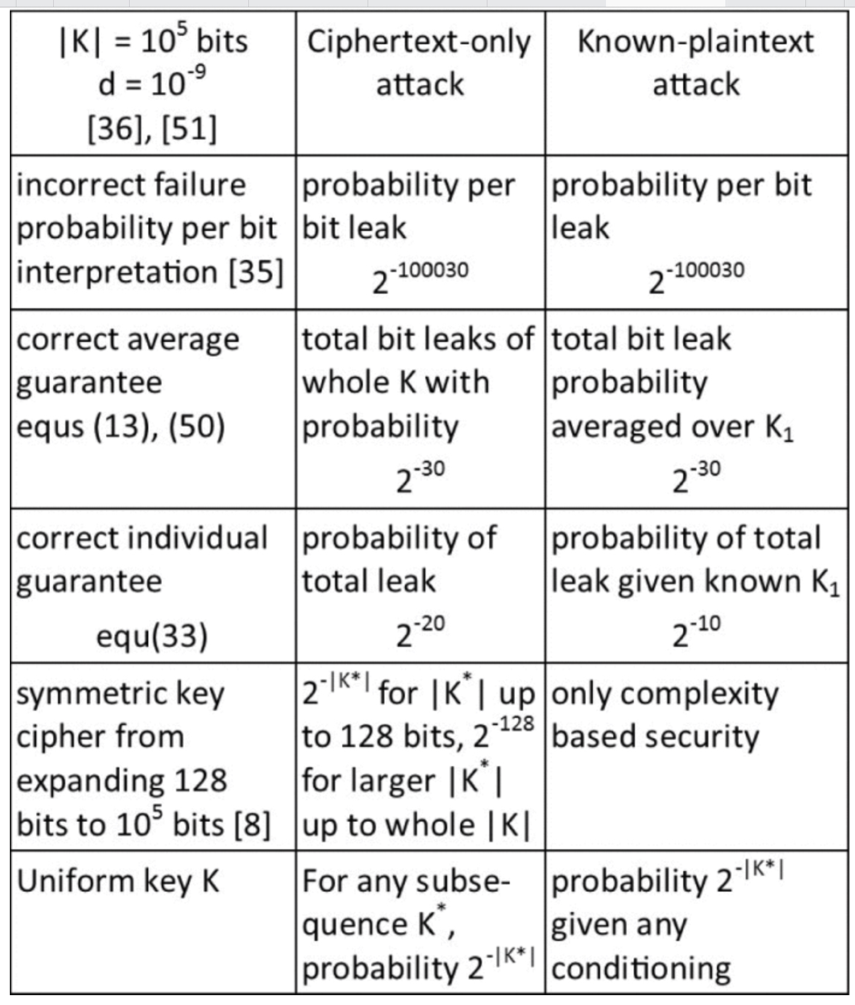
密码学界都知道，密钥稍微偏离真随机数会导致密码保密性的大幅下降。特别对于“已知明文攻击”，攻击者根据密文与部分明文的映射中得出密钥的部分信息，由于密钥非真随机数，攻击者可以利用密钥位于位之间的关联性，大大提高密钥被破解的可能性。

密钥的随机性就是密码的生命线，所以密钥随机性的机制和定量分析就成了研究量子通信理论安全性的关键。在网上你只要查询这些讨论QKD安全性的论文，绕不开的就是密钥随机性的定量分析。从这些论文可以看出专家们对QKD的安全的定量分析模型和算法至今仍未达成共识。这也从另一个角度告诉我们，关于QKD安全的理论基础远未夯实。

尽管在QKD的理论安全性的分析评估方法上存在分歧和争论，但是专家们的认识有一点是共同的：QKD离开“信息理论级安全”差距甚远。

Horace P. Yuen（美国西北大学电子和物理系教授，1996年获得国际量子通信奖，2008年他又获得了IEEE光子学会的量子电子奖。）是量子通信安全领域国际上公认的学术权威，他对QKD安全性发表了一系列重量级论文，受到了国际上不少同行的支持。

Yuen教授2016年发表在IEEE上的论文：量子通信安全性(Security of Quantum Key Distribution)[2]。下面就是该论文的第一张图表。



该图表显示了当密钥的总位数为10^5(100000位)时，各种不同质量的密钥（横排）对应于纯密文攻击和已知明文攻击（竖列）的成功概率。图表含有许多信息，但有一点非常明显：理论上，一个100000位的真随机数密钥被破解的成功几率约为1/2^100000，而QKD产生的密钥的被成功破解的几率升高为1/2^30。如果折算成十进制破解几率大致分别为1/10^30000 和 1/10^10 ，（ 1/10^30000 << 1/10^10）

由此可见，QKD与信息理论级安全（即俗称的无条件安全）差了三个数量级都不止。请注意，这里的数据是理论分析的上限，QKD的各种实验和工程项目的安全性比理论数据还要再差近一个数量级。

至此可以肯定：“量子通信在理论上是无条件安全的”这个结论是错误的。因为：

1）物理学原理不能保证通过QKD分发的密钥具有绝对的私密性；

2）QKD也不能保证分发的密钥是真随机数；

使用QKD加密得到的密文就存在被第三方破解的风险。

更可怕的是攻击者可以同时利用上述二个漏洞，一方面利用物理全息原理收集、贮存和分析大数据，得到QKD分发密钥的部分信息，然后在此基础上从密钥随机性的不完善中得到密钥的更多信息，再依靠已知明文的片断，极大地提升破解密文的概率。对量子通信安全性的担心才是英国情报部和美国空军拒绝使用量子通信的最重要的原因[3]。

本文引举的论文作者Horace P. Yuen教授是量子通信安全领域公认的权威，他又是美国西北大学物理系教授，所以他的批评更受人注目，他的众多支持者中包括了好几位日本量子通信领域的专家教授，请阅读相关论文[4]。

**三）量子通信远未达到密码学意义上的通信安全标准**

现在让我们再退一万步，让我们立法不准使用物理全息原理收集和存贮广谱的电磁辐射，以保证密钥分发的绝对私密性。再退一步，假设研究人员彻底放弃BB84协议发明了一种全新的QKD的方案，该方案保证分发的密钥是真随机数（而且相关人员因此获得了诺贝尔物理学奖）。那么这种新的量子通信技术就真能保证通信的无条件安全了吗？非常不幸，答案依然是否定的。

这里存在一个严重的常识和逻辑错误。许多人把通信私密性错认为就是通信的安全性。当然通信安全一定要求通信内容的私密性，但是只有通信的私密性不等于通信就是安全的。通信的安全性有着比私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私密性、真实性、完整性、和可用性。

没有通信的真实性和完整性，通信双方无法确认对方的真实身份，就会出大乱子。在量子通信开始时如果甲乙双方的真实身份无法确认，攻击者在通信线路中间对甲方冒充乙方，同时对乙方冒充甲方。甲方与攻击者之间、攻击者与乙方之间照样可以顺利分发得到二个密钥，然后甲方把通信内容加密后传送给了攻击者，攻击者用第一个密钥解密获得了全部通信内容，然后再把通信内容用第二个密钥加密后传送给乙方，乙方用密钥解密得到通信内容。甲乙双方还以为依靠量子通信完成了无条件安全的通信，谁知攻击者在暗处偷笑：量子通信传递的秘密“尽入吾彀中矣。”

量子通信推动者一头钻进通信的私密性里，误以为绝对的私密性就等于通信的无条件安全性，把自己带入了深坑中。事实上，通信安全远非只是通信的私密性，在一些应用场合通信的私密性甚至不是很重要的。举个例子，客户通过支付宝或微信购买大并油条，在这个通信过程中，客户买的大并油条究竟付了几元几角，对于这一类数据作严格保密意义很大吗？但是必须确保客户的钱是付给了确定的商家，没有被隔壁老王家收去了，这恰恰才是最为重要的。客户当然更不希望由于量子通信的低效率而在上班的早高峰时段因为买大并油条而耽误了几个小时[5]。

由此可知，互联网不仅极大的改变了人们相互通信的方式，同时也对通信安全提出了全新的标准和要求。量子通信的BB84协议初创于互联网的婴儿期，对互联网发展缺乏预见。量子通信用物理原理依靠硬件去追求通信的绝对私密性，从一开始就站到了历史的错误一方，完全脱离了这几十年互联网引起的通信技术发展的主潮流。

通信的私密性、真实性、完整性、和可用性共同保证了通信的安全，它们是不可分割的整体，缺一不可。量子通信不仅在理论上无法保证通信的绝对私密性，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、难有作为。“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。

最后总结一下。

1）物理学原理不支持“量子密钥分发具有绝对的私密性”；2）信息学理论指出，由于量子通信分发的密钥不是真随机数，用QKD分发密钥所生成的密文的绝对不可破解性是得不到保证的；3）密码学定义的通信安全包括了通信的私密性、真实性、完整性、和可用性，它们是通信安全不可分割的组成部分。无论具有多强的私密性也不能保证量子通信系统的无条件安全性。

简而言之，量子通信既没有能力保证密钥分发的私密性，又无法保证密钥是真随机数，所以量子通信在理论上不具备绝对的私密性。量子通信理论上的私密性的上限仅与传统对称密码持平，而在通信的真实性、完整性、和可用性三个方面的纪录都不及格。量子通信相比传统密码的优势就只剩下戴在头上的“量子”这个光环了。

量子通信头上的这个“量子光环”必须拿出来天天讲、年年夸，原因很简单，一项技术没有了真功夫它还能怎么玩？这与没自信的人最喜爱名牌服饰的道理是一样的。相反，真正有底气的技术都不希罕外包装的，其实半导体和激光这两种技术均与量子物理关系非常紧密，为什么就没人反复宣传“量子半导体”和“量子激光”？其实道理很简单，因为这些有着强大生命力的技术是根本不屑于头顶“量子光环”的。量子通信从起名开始就心术不正、误导大众，最后必定难以行稳走远。正所谓“机关算尽太聪明，反误了卿卿前程。”

**参考文献**

[1]https://sidechannels.cr.yp.to/qkd/holographic-20180312.pdf

[2]Security of Quantum Key Distribution

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

[3] https://www.guancha.cn/XuLingyu/2018\_10\_31\_477593.shtml

[4] A Correct Security Evaluation of Quantum Key Distribution

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

[5] Spooky Security at a Distance: The Controversy of Quantum Key Distribution

https://asz.ink/2016/10/07/spooky-security-at-a-distance-the-controversy-of-quantum-key-distribution/