如何看待“量子通信被破解”

-  徐令予　加州大学洛杉矶分校物理系研究员
-  潘建伟　中国科学院院士、“墨子号”首席科学家

2019-03-15　08:17:13　来源：观察者网

https://www.guancha.cn/XuLingyu/2019_03_15_493648_s.shtml

【文/ 观察者网专栏作者 徐令予】

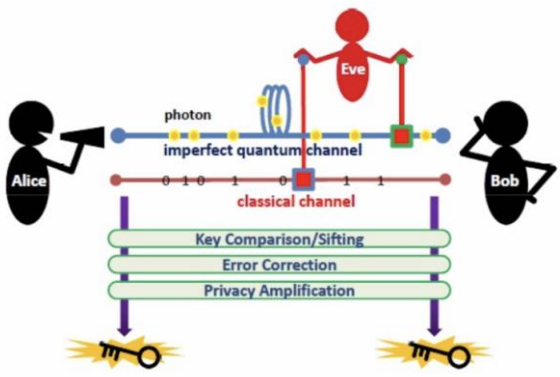
最近上海交通大学研究团队成功破解“量子通信”的消息在互联网上激起了一片浪花。该消息在观察者网转载后，不到半天点击破 15 万，评论数超过 300 条。一个科研项目、一个国家级的工程受到公众的关注是件好事。但是由于诸多原因，公众对“量子通信”存在许多误解和疑虑，深入的科普和耐心的引导仍是当务之急。

“量子通信”被破解看似意料之外，实在情理之中。“量子通信”被破解一点也不奇怪，问世以来它被黑客虐了已经不知有多少回，这既不是第一次，更不会是最后一回。

“量子通信”被黑何时了，漏洞知多少？这还真不是杞人忧天，上海交大破解团队的论文就是这么说的：“然而，我们希望在此提供的主要信息是，当我们认为 MDI-QKD 已经是一个非常成熟且商业化的解决方案时，可能存在许多其他未发现的物理漏洞。”

“量子通信”被破解是好事还是坏事？这得看对谁而言。此事对于“量子通信”的科学研究工作可能是好事，破解-反破解本是量子通信科研的重要组成部分，失败和教训是科学成长的维它命。但是“量子通信”被破解对于工程项目很难说是好消息。

“带病上岗”的京沪量子通信干线究竟该怎么办？第二天，论文作者又在量子通信团队的自媒体“墨子沙龙”紧急补漏，声称：“正如我们公开在预印本 arXiv 上文章中已经深入讨论了的，我们通过进一步理论分析和实验设计，证明了针对这一漏洞的窃听方案可以通过在源端（我们的实验系统已经内置了 30dB 隔离度）增加更高对比度光隔离器来解决，从而保证量子密钥分发的安全性。”但是论文的原文说的正好相反：“很显然，攻击者的激光功率不受限制的话，即使采用隔离保护，Eve 总能够破解 MDI-QKD 系统”（apparently with infinite laser power, Eve will always be able to hack MDI-QKD systems even with the isolation protection.）



让我们退一步，就算攻击者拥有激光武器不在他们学术上的考虑范围，而且已经找到了切实可行的解决方案。此条干线上数以百计的光量子发射源要不要都升级更换？设备更换后肯定会影响整体运行性能，系统参数的联调估计也不是件容易的事。

如果解决方案使“量子通信”的硬件设备变得更复杂更昂贵，增加的经费开支由谁来买单？京沪干线上自觉自愿的付费客户本没有几个，恐怕还得由包建设、包运营的政府再加上包修理。

如果量子通信仅局限在实验室中，上述所有问题都立马消失。核心技术的进步来自于实验室，这次发现的“量子通信”的安全隐患就是在实验室中，而不是在京沪量子干线上。科技可以在试错中进步，工程项目绝不能在试错中前行。

量子通信离开工程建设的可行性要求差之甚远。量子通信工程的技术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化石，这种端到端的通信协议完全不具备组成复杂多变网络结构的可能。最近出台的《量子保密通信技术白皮书》，看了其中关于量子保密通信组网部分，依然空洞无物。量子通信组网连“纸上谈兵”的水平都够不上，只能算是“梦中谈兵”这一层级。

量子通信工程中密钥协商分发的最大距离不超过百公里，远程量子通信工程必须使用可信中继站技术。可信中继站中密钥以明文格式接触连网的计算机，给量子通信工程带来极为严重的安全隐患。使用卫星作量子密钥分发的技术尚在实验阶段，事实上它很难跨越“最后一公里”这个技术障碍，本质上这还是被卡在中继技术的死穴里。

量子通信的BB84协议早在1984年就提出了，三十多年过去了，这样一个漏洞百出、技术上不成熟又没有多大实用价值的量子通信能大行其道，靠的是一张护身符——“量子通信”可以保证通信的无条件安全。其实“量子通信”在理论上的无条件安全性都是存疑的，“量子通信”工程的无条件安全性又何从说起？物理与工程之间有本质的区别，绝不能把物理原理中的理想结果偷换成工程指标。

著名物理学家费曼说过，“所有的物理定律都是对现实世界的近似，模型和现实之间永远存在无法磨灭的微小差异。”费曼之所以在这里使用“微小差距”，是为了强调现实与理论这二者之间的差距无论用什么方法都是无法完全消除的，是“永远”也无法磨灭的。

原理与现实之间永远存在无法磨灭的微小差异，这个微小差距对于大多数工程项目也许影响有限，但对于密码工程却可能是致命的。因为一个几百位的密钥，只要有几位被泄漏，就可能导致整个传输的密文被破解。

这次的“量子通信”被破解是每传送十个密钥有六个被破解，这六个密钥中的每个密钥的所有位都被黑客全部破解全部锁定，而通信的接收方仍一无所知。这简直是密码领域的天方夜谭，怪不得有好几个密码学界的朋友向我询问消息的可靠性，他们都不敢相信真有这回事。

在密码系统里，密钥全身必须包裹得严严实实一丝不露，连中东妇女那种只露二只眼睛的衣饰都是完全不合格的，而我们“量子通信”上传输的密钥却赤身裸体一丝不挂，连比基尼都忘了穿。这种“量子通信”密码工程究竟又有多少人敢于使用？

物理原理给出的结果都是在满足许多苛刻条件的理想环境下才能成立，在现实世界中，在工程实施时这些条件都是无法完全满足的，即使要部分满足这些条件，工程的代价也会高到无法忍受。工程都是性能和代价的折衷和优化，“量子通信”工程一定也逃脱不了这个规律，无

条件绝对安全的“量子通信”在现实中是根本不存在的，注定也得把“猫捉老鼠”的游戏继续玩下去。这次“量子通信”被“注入锁定”方式破解就是一个最好的证明。

说到底，信息安全技术的发展史就是一场“猫捉老鼠”的斗争史。传统密码技术如此，“量子通信”最多也只能是如此。但是基于数学原理用软件技术实现的传统密码在兼容性、效率和性能价格比各方面远远优于“量子通信”，失去了“无条件安全”这张护身符的“量子通信”又有什么资格与传统密码一较高下？

目前大多数实验室和工程建设中的“量子通信”并不是保证通信安全的独立完整的密码系统，密码系统的核心是加密解密的算法，“量子通信”使用的都是传统对称密码的加密解密算法。“量子通信”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密钥的一种硬件技术，简称“量子密钥分发”技术。

“量子密钥分发”基于量子物理的量子不可克隆原理，保证密钥传送过程中如果有窃听必被发现，追求密钥分发环节的保密性。许多人把通信保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保密性，但是只有通信的保密性并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。

由此可知，所谓的“量子通信”可以保证通信的无条件安全是没有任何科学依据的，这种宣传实在错得太离谱了。

就在昨天，潘建伟等《关于量子保密通信现实安全性的讨论》一文中还在宣传：学界将这种安全性称之为“无条件安全”或者“绝对安全”，它指的是有严格数学证明的安全性。20世纪90年代后期至2000年，安全性证明获得突破，BB84协议的严格安全性证明被Mayers，Lo，Shor-Preskill等人完成。

该文所引的有关量子保密通信安全性证明的论文大多是十多年前的论文，为什么不敢引用最近这几年的相关论文呢？不是说会“对经过同行评审并公开发表的学术论文进行评价”的吗？如果这个问题真的已有定论，为什么最近几年美国和日本的量子通信专家权威仍有不少质疑QKD安全性的论文呢？

这些新的论文尽管在QKD的理论安全性的分析评估方法上存在各种分歧和争论，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》，受到日本等国量子通信专家的赞同和支持[1]。为什么中国的同行们对此一字不提呢？

通信安全是一个很大很复杂的大系统，大多数人是门外汉，量子实验物理学家也不例外。有关通信和信息安全还是要向通信密码学界的专家学者们虚心学习。

前几天我在密码学界的一位专家朋友转发了一篇谈安全和科学的论文给我[2]，认真看了一下，受益匪浅。好文章不能独享，特把文章地址发于下，有兴趣的可以读读。希望有关专业人士都能从中受益，把通信和信息安全的认识提高到一个更新更高的水平。

[1] Security of Quantum Key Distribution

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

[2]《科学与安全，安全是科学追求的难以捉摸的目标》

https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/scienceAndSecuritySoK.pdf

翻页为：潘建伟等物理学家《关于量子保密通信现实安全性的讨论》

关于量子保密通信现实安全性的讨论

王向斌 1 马雄峰 1 徐飞虎 2 张强 2 潘建伟 2

（1.清华大学　2.中国科学院量子信息与量子科技创新研究院，中国科学技术大学）

近来，某微信公众号发表了一篇题为“量子加密惊现破绽”的文章，宣称“现有量子加密技术可能隐藏着极为重大的缺陷”。其实该文章最初来源于美国《麻省理工科技评论》的一篇题为“有一种打破量子加密的新方法”的报道，该报道援引了上海交通大学金贤敏研究组的一篇尚未正式发表的工作。

此文在微信号发布后，国内很多关心量子保密通信发展的领导和同事都纷纷转来此文询问我们的看法。事实上，我们以往也多次收到量子保密通信安全性的类似询问，但一直未做出答复。这是因为学术界有一个通行的原则：只对经过同行评审并公开发表的学术论文进行评价。但鉴于这篇文章流传较广，引起了公众的关注，为了澄清其中的科学问题，特别是为了让公众能进一步了解量子通信，我们特撰写此文，介绍目前量子信息领域关于量子保密通信现实安全性的学界结论和共识。

现有实际量子密码（量子密钥分发）系统主要采用 BB84 协议，由 Bennett 和 Brassard 于 1984 年提出[1] 。与经典密码体制不同，量子密钥分发的安全性基于量子力学的基本原理。即便窃听者控制了通道线路，量子密钥分发技术也能让空间分离的用户共享安全的密钥。学界将这种安全性称之为“无条件安全”或者“绝对安全”，它指的是有严格数学证明的安全性。20 世纪 90 年代后期至 2000 年，安全性证明获得突破，BB84 协议的严格安全性证明被 Mayers，Lo，Shor-Preskill 等人完成[2-4]。

后来，量子密钥分发逐步走向实用化研究，出现了一些威胁安全的攻击[5，6]，这并不表示上述安全性证明有问题，而是因为实际量子密钥分发系统中的器件并不完全符合上述（理想）BB84 协议的数学模型。归纳起来，针对器件不完美的攻击一共有两大类，即针对发射端--光源的攻击和针对接收端--探测器的攻击。

“量子机密惊现破绽”一文援引的实验工作就属于对光源的木马攻击。这类攻击早在二十年前就已经被提出[5]，而且其解决方案就正如文章作者宣称的一样[7]，加入光隔离器这一标准的光通信器件就可以了。该工作的新颖之处在于，找到了此前其他攻击没有提到的控制光源频率的一种新方案，但其对量子密码的安全性威胁与之前的同类攻击没有区别。尽管该工作可以为量子保密通信的现实安全性研究提供一种新的思路，但不会对现有的量子保密通信系统构

成任何威胁。其实，自 2000 年初开始，科研类和商用类量子加密系统都会引入光隔离器这一标准器件。举例来说，现有的商用诱骗态 BB84 商用系统中总的隔离度一般为 100dB，按照文章中的攻击方案，需要使用约 1000 瓦的激光反向注入。如此高能量的激光，无论是经典光通信还是量子通信器件都将被破坏，这就相当于直接用激光武器来摧毁通信系统，已经完全不属于通信安全的范畴了。

而对光源最具威胁而难以克服的攻击是“光子数分离攻击”[6]。严格执行 BB84 协议需要理想的单光子源。然而，适用于量子密钥分发的理想单光子源至今仍不存在，实际应用中是用弱相干态光源来替代。虽然弱相干光源大多数情况下发射的是单光子，但仍然存在一定的概率，每次会发射两个甚至多个相同量子态的光子。这时窃听者原理上就可以拿走其中一个光子来获取密钥信息而不被察觉。光子数分离攻击的威胁性在于，不同于木马攻击，这种攻击方法无需窃听者攻入实验室内部，原则上可以在实验室外部通道链路的任何地方实施。若不采用新的理论方法，用户将不得不监控整个通道链路以防止攻击，这将使量子密钥分发失去其“保障通信链路安全”这一最大的优势。事实上，在这个问题被解决之前，国际上许多知名量子通信实验小组甚至不开展量子密钥分发实验。2002 年，韩国学者黄元瑛在理论上提出了以诱骗脉冲克服光子数分离攻击的方法[8]；2004 年，多伦多大学的罗开广、马雄峰等对实用诱骗态协议开展了有益的研究，但未解决实用条件下成码率紧致的下界[9]；2004 年，华人学者王向斌在《物理评论快报》上提出了可以有效工作于实际系统的诱骗态量子密钥分发协议，解决了现实条件下光子数分离攻击的问题[10]；在同期的《物理评论快报》上，罗开广、马雄峰、陈凯等分析了诱骗态方法并给出严格的安全性证明[11]。在这些学者的共同努力下，光子数分离攻击问题在原理上得以解决，即使利用非理想单光子源，同样可以获得与理想单光子源相当的安全性。2006 年，中国科技大学潘建伟等组成的联合团队以及美国 Los-Alamos 国家实验室-NIST 联合实验组同时利用诱骗态方案，在实验上将光纤量子通信的安全距离首次突破 100km，解决了光源不完美带来的安全隐患[12-14]。后来，中国科技大学等单位的科研团队甚至把距离拓展到 200km 以上。

第二类可能存在的安全隐患集中在终端上。终端攻击，本质上并非量子保密通信特有的安全性问题。如同所有经典密码体制一样，用户需要对终端设备进行有效管理和监控。量子密钥分发中对终端的攻击，主要是指探测器攻击，假定窃听者能控制实验室内部探测器效率。代表性的具体攻击办法是，如同 Lydersen 等[15]的实验那样，输入强光将探测器“致盲”，即改变探测器的工作状态，使得探测器只对他想要探测到的状态有响应，或者完全控制每台探测器的瞬时效率，从而完全掌握密钥而不被察觉。当然，针对这个攻击，可以采用监控方法防止。因为窃听者需要改变实验室内部探测器属性，用户在这里的监控范围只限于实验室内部的探测器，而无需监控整个通道链路。

尽管如此，人们还是会担心由于探测器缺陷而引发更深层的安全性问题，例如如何完全确保监控成功，如何确保使用进口探测器的安全性等。2012 年，罗开广等[16]提出了“测量器件无关的（MDI）”量子密钥分发方案，可以抵御任何针对探测器的攻击，彻底解决了探测器攻击问题。另外，该方法本身也建议结合诱骗态方法，使得量子密钥分发在既不使用理想单光子源又不使用理想探测器的情况下，其安全性与使用了理想器件相当。2013 年，潘建伟团队首次实现了结合诱骗态方法的 MDI 量子密钥分发，后又实现了 200km 量子 MDI 量子密钥分发[17,

18]。至此，主要任务就变成了如何获得有实际意义的成码率。为此，清华大学王向斌小组提出了4强度优化理论方法，大幅提高了MDI方法的实际工作效率[19]。采用此方法，中国科学家联合团队将MDI量子密钥分发的距离突破至404 km[20]，并将成码率提高两个数量级，大大推动了MDI量子密钥分发的实用化。

总之，虽然现实中量子通信器件并不严格满足理想条件的要求，但是在理论和实验科学家的共同努力之下，量子保密通信的现实安全性正在逼近理想系统。目前学术界普遍认为测量器件无关的量子密钥分发技术，加上自主设计和充分标定的光源可以抵御所有的现实攻击[21, 22]。此外，还有一类协议无需标定光源和探测器，只要能够无漏洞地破坏Bell不等式，即可保证其安全性，这类协议称作“器件无关量子密钥分发协议”[23]。由于该协议对实验系统的要求极为苛刻，目前还没有完整的实验验证，近些年的主要进展集中在理论工作上。由于器件无关量子密钥分发协议并不能带来比BB84协议在原理上更优的安全性，加之实现难度更大，在学术界普遍认为这类协议的实用价值不高。

综上所述，正如我们目前应邀为国际物理学权威综述期刊《现代物理评论》所撰写的关于量子通信现实安全性的论文中所指出的那样[24]，过去二十年间，国际学术界在现实条件下量子保密通信的安全性上做了大量的研究工作，信息论可证的安全性已经建立起来。中国科学家在这一领域取得了巨大成就，在实用化量子保密通信的研究和应用上创造了多个世界记录，无可争议地处于国际领先地位[25]。令人遗憾的是，某些自媒体在并不具备相关专业知识的情况下，炒作出一个吸引眼球的题目对公众带来误解，对我国的科学研究和自主创新实在是有百害而无一利。

鉴于量子保密通信信息论可证的安全性已经成为国际量子信息领域的学界共识，此后，除非出现颠覆性的科学理论，我们将不再对此类问题专门回复和评论。当然，对量子通信感兴趣的读者，可参阅我们撰写的《量子通信问与答》了解更多的情况[26]。

参考文献：

[1]. C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp. 175 - 179.

[2]. H.-K. Lo, H.-F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science 283, 2050(1999).

[3]. P. W. Shor, J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Physical review letters 85, 441 (2000).

[4]. D. Mayers, Unconditional security in quantum cryptography, Journal of the ACM (JACM) 48, 351 (2001).

[5]. A. Vakhitov, V. Makarov, D. R. Hjelme, Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography, J. Mod. Opt. 48, 2023 (2001).

[6]. G. Brassard etal., Limitations on practical quantum cryptography, Physical Review Letters 85, 1330 (2000).
[7]. 庞晓玲，金贤敏，[声明]攻击是为了让量子密码更加安全，墨子沙龙，2019 年 3 月 13 日.
[8]. W.-Y. Hwang, Quantumkey distribution with high loss: toward global secure communication, Physical Review Letters 91, 057901 (2003).
[9]. X. Ma, Security of Quantum Key Distribution with Realistic Devices, Master Report, University of Toronto, June (2004).
[10]. X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Physical Review Letters 94, 230503 (2005).
[11]. H.-K. Lo, X. Ma, K. Chen, Decoy state quantum key distribution, Physical Review Letters 94, 230504 (2005).
[12]. C.-Z. Peng et al., Experimental long-distancedecoy-state quantum key distribution based on polarization encoding, Physical Review Letters 98, 010505 (2007).
[13]. D. Rosenberg, et al., Long-distance decoy-statequantum key distribution in optical fiber, Physical Review Letters 98, 010503 (2007).
[14]. T. Schmitt-Manderbach et al., Experimental demonstration of free-space decoy-state quantum key distribution over 144 km, Physical Review Letters 98, 010504 (2007).
[15]. L. Lydersen et al., Hacking commercial quantum cryptography systems by tailored bright illumination, Nature Photonics 4, 686 (2010).
[16]. H.-K. Lo, M. Curty, B. Qi, Measurement-device-independent quantum key distribution, Physical Review Letters 108, 130503 (2012).
[17]. Y. Liu et al.,Experimental measurement-device-independentquantum key distribution, Physical Review Letters 111, 130502 (2013).
[18]. Y.-L. Tang et al., Measurement-device-independent quantum key distribution over 200 km. Physical Review Letters 113, 190501 (2014).
[19]. Y.-H. Zhou, Z.-W. Yu, X.-B. Wang, Making the decoy-state measurement-device-independent quantum key distribution practically useful, Physical Review A 93, 042324 (2016).
[20]. H.-L. Yin, etal., Measurement-device-independent quantum key distribution over a 404 km optical fiber, Physical Review Letters 117, 190501 (2016).
[21]. H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nature Photonics 8, 595 (2014).
[22]. Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, J.-W. Pan, Large scale quantum key distribution: challenges and solutions, Opt.Express 26, 24260 (2018).

[23]. D. Mayers, A. C.-C. Yao, Quantum Cryptography with Imperfect Apparatus, in Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS' 98), p. 503(1998); A. Acín et al., Device-Independent Security of Quantum Cryptography against Collective Attacks, Physical Review Letters 98,230501 (2007).

[24]. F. Xu, X. Ma, Q. Zhang, H.-K. Lo, J.-W. Pan, Quantum cryptography with realistic devices, in preparation for Review of Modern Physics (invited in 2018).

[25]. 王向斌，量子通信的前沿、理论与实践，《中国工程科学》，第 20 卷第 6 期，087-092 页(2018).

[26]. 量子通信的问与答，墨子沙龙,2018 年 11 月 14 日.