在量子通信中遏制木马攻击

(中国科学院理化技术研究所　戴　闻　编译自 Ana Lopes, *Physics* September 9, 2015)

就像古代神话“特洛伊木马”所描述的，木马攻击是一种策略，它秘密潜入到受安全保护的空间。按照光学量子密钥分发(QKD)协议的说明，这种攻击涉及“木马光子”潜入到光学量子密钥分发系统，企图获取密钥。此前，一类无需外部供电便能工作的被动式光学元件，一直被建议作为一种阻止木马入侵的手段。但是，研究人员至今缺乏一种量化的方法，用以评估这样的被动防御系统的有效性。现在，来自东芝研究-欧洲有限公司(英国)的 Andrew Shields 和同事们，已经设计出了一个定量评估方法：借助于量子信息泄漏问题，监察木马攻击。

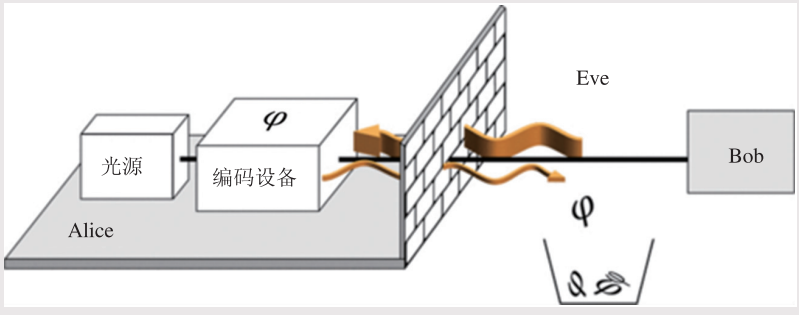
量子密钥分发允许两个远程方，通常称为 Alice(发送者)和 Bob(接收者)，他们共享一个公共密钥，理论上信息是安全的。量子密钥分发的安全性基于量子物理的定律，并且它的实现一定要利用精准完善的物理系统。任何被忽视的偏离预期的行为，都可能被攻击者 Eve 利用，从而损害系统安全。按照右图，木马攻击可以被简化描述。Eve 利用连接 Alice 和 Bob 的光通道，发射包含大量木马光子的强光脉冲，进入 Alice 所认定的安全模块。光脉冲到达编码装置，一个个木马光子以特定的信息 φ 被编码，这里信息 φ 是指与 Alice 制备光子(然后发送给 Bob)全同的编码信息。信息 φ 是私密的，然而一些木马光子被反射回来，它们将信息传回到 Eve，从而损害系统的安全性。

为抵抗木马攻击，研究人员提出了不同的解决方案，即主动方案和被动方案。按照主动方案，Alice 可以拥有一台主动的随机位相发生器和一台看门狗探测器，用以检测来自 Eve 一边木马光子的位相值，并去除入侵光脉冲的能量。然而，主动协议通常对量子密钥分发的设置增加了额外的复杂性，可能为攻击者提供更多的“迂回空间”，并且通常更贵。例如，最近的研究显示，一个商业 QKD 系统的监控探测器很容易被旁通掉。

Shields 和同事们提出的光学量子密钥分发系统，属于被动方案，它包括一系列在发送端的无源组件(包括光纤环路、滤波器和隔离器等)，这些组件过滤掉和衰减掉的不是来自发送者 Alice 的光子，从而限制了木马光子的数量；否则，这些木马光子可能被注入系统，并且从系统中被攻击者抽取。最终，Shields 等遏制了通过抽取木马光子泄露给攻击者的信息量。这种完全被动的方法比主动架构具有实际的优势。

在这项工作中，Shields 等分析了一个用以抵抗木马攻击的完全被动的架构；定量评估了被动光学元件对于维护 QKD 系统安全的价值。关键点在于把木马攻击解释为一个侧通道。通常情况下，Alice 不知道这个侧通道，并认为自己制备密钥的工作没有瑕疵。上述误解会导致未被觉察的信息泄露(从她的模块到 Eve 的领地)。然而，Shields 等证明，Alice 可以束缚信息泄露，并通过适当水平的隐私放大，实现安全。

更多内容详见：M.Lucamarini et al. *Phys. Rev. X*, 2015, 5: 031030。



木马攻击光学量子密钥分发设施的示意图。攻击者 Eve 将大量的木马光子(宽厚箭头)送入信息发送者 Alice 的防御系统。某些木马光子到达 Alice 的编码设备，并以 Alice 和接收者 Bob 共享的私人信息 φ 编码，进而反射回到 Eve 处(细箭头)。Eve 通过测量这些返回光子，抽取 Alice 的保密信息