评“诱骗态量子密钥分发中不可区分假设的合理性和安全性验证”

杨国武

量子密钥分发 (QKD) 是一种安全通信方法，它实现了涉及量子力学组件的加密协议。由于技术限制，实际 QKD 使用的是弱相干态光源 (WCS)。而 WCS 光源发出的光子脉冲可能具有一些概率特征，从而可能被攻击者利用，导致通信不安全。而诱骗态方法可以很好地解决这一问题。诱骗态方法假设了第三方攻击者不能区分信号态和诱骗态，但这一假设的合理性还有待进一步验证。

该文采用贝叶斯决策分析方法验证了诱骗态方法的合理性、安全性和必要性。根据强度不同导致光子数概率分布的差异，得到了信号态和诱骗态拥有相同的光子透射率的结论，验证了信号态和诱骗态不可区分这一假设的合理性。此外，根据单信号态和信号态+单诱骗态两种情况下光子数分离攻击前后的安全密钥率的对比结果，验证了诱骗态方法确实能够抵抗光子数分离攻击。

评“基于 Bell 态的两方互认证量子密钥协商协议”

杨国武

随着量子理论和技术的不断发展，量子密码学成为一个热点研究领域。量子密钥协商 (QKA) 作为量子密码学的一个分支，在 2004 年首次被提出。相比于量子密钥分发 (QKD)，QKA 在生成会话密钥时要求所有参与者一同决定，因而更加公平。已有的互认证量子密钥协商协议需引入可信或半可信监督者才能实现，通信复杂度较高。如何进一步降低量子密钥协商协议的复杂度，保证其安全性，提高实际可操作性等，是该领域需要解决的重要问题。

为了解决以上问题，该文提出了一个基于 Bell 态的无需第三方监督者就能实现的两方互认证 QKA 协议。协议双方身份的认证是通过对量子态的制备和测量来实现的。该协议量子通信次数少，能抵挡外部攻击和参与者攻击，还有较高的量子比特利用率。此外，该 QKA 协议仅用到了单粒子测量和 Bell 态测量，在现阶段量子技术上更容易实现，具有一定的应用价值。