基于诱骗态的量子安全通信新基建在实时语音通信中的应用研究

成彦波

郑州信大先进技术研究院 河南 郑州 450001

【摘　要】为确保语音通信中的数据安全问题，提出了一种基于诱骗态的量子安全通信解决方案。本文从密码通信安全基本原理引出通信过程中存在的安全问题，通过诱骗态量子密钥分配过程阐述量子通信过程的特性，并将其应用于实时通信中。

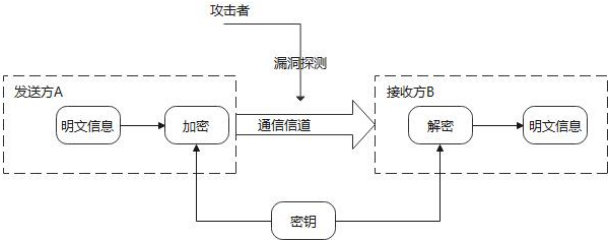
【关键词】数据安全；密码通信安全；诱骗态

1.引言

随着 2022 年诺贝尔物理学奖的揭晓，量子信息科学技术再一次引起世界的广泛关注。Alain Aspect、John Clauser 和 Anton Zeilinger 用纠缠量子态进行了开创性的实验标志着量子科学由理论走向技术。与其他通信方式相比，量子通信技术在信息安全防御上具有先天的优势：信息的不可复制性、量子态传输方式、通信信道容量大[1]。2022 年诺贝尔物理学奖的颁发一方面是对三位科学家在量子科学方面的杰出贡献的肯定，更重要的是开启了量子信息科学逐渐产业化的趋势。本文立足于诱骗态的量子安全通信新基建视角，探索量子安全通信技术在实时语音通信中的应用，为数字经济背景下数字通信的安全防护提供借鉴思路。

2.诱骗态的量子安全通信

数据安全是一个国家、企事业单位等的“生命线”，实时语音通信本身具有多样性、体积大、速度快的特点，确保信息传递的安全就变得尤为重要。关键信息在通讯过程中、传递过程中可能由于软硬件的漏洞而遭到攻击，如图所示。



图：关键信息安全传递过程

如图，如果用户 A 要将语音消息发送给用户 B，会使用某一特定密钥将此明文信息进行加密形成密文消息，然后将该密文消息通过通信信道传递给用户 B；B 接收到该消息后需要完全一致的密钥才能进行解密，从而得到对应的明文信息。可以看出，在这一过程中，密钥内容本身并没有什么特殊的地方，但其所起的作用却至关重要，该密钥是保证 A 和 B 通信安全性的枢纽。由于密文信息是在直接通过通道传输的，如果在通信过程中，密钥被攻击者获取，则 A、B 双方通信的内容很容易被攻击者破解。因此，不难得出，在传统的通信加解密过程中，通信密钥的生成、存储、传输与管理是保证通信安全的关键。

因此，可以考虑，如果能找到一个安全的通信信道，则可以使得通信双方建立无条件安全的密钥。基于不可克隆原理、单光子不可再分理论、量子态测量塌缩理论等建立起来的量子信息科学为通信信道安全提供了新的思路。其中，量子密钥是基于量子态实现的，其安全性建立在量子态不可克隆、量子不可分割和量子不确定性原理基础之上, [2]因此，与传统对通信信道的监控方式不同，量子密钥凭借其一次一密、无条件安全的密钥分发机制与特性极大的保障了通信过程中密钥的安全。

诱骗态的量子安全通信最重要的实践之一是密钥分配机制的应用，与传统 BB84 协议相比，无论是在密钥的生成率方面还是在信息的最大传输距离方面都有显著的提高，且卫星通信服务技术、40MHZ 量子密码网络系统、量子秘钥分发技术、量子广域加密通信网、应对网络空间威胁的“一密通”等。这些诱骗态的量子安全通信衍生物已经在地学探测、油矿勘探、心率监测、建筑物沉降监测、个人云信息存储、云服务器数据传输等方面已顺利落地。比如采用诱骗态 BB84 量子密钥分配技术研制的与我国“量子京沪干线”同批次产品 40MHZ 量子密码网络系统，通过偏振编码技术进行量子密钥分配，为量子安全保密通信网络提供不可窃听的量子密钥。

3.基于诱骗态的量子安全通信新基建在实时语音通信中的应用

语音通信作为当前沟通的重要桥梁，其通信内容的保密重要性不言而喻。与一般消息不同的是，实时语音通信以数模转换为基础，因此，为了保障实时语音通信

过程中的数据安全，需要基于波形在数字通信系统中引入加解密技术。本文提出的实时语音安全通信方案是基于诱骗态的量子安全通信新基建实现的，其中，采用的光源的光子分布近似符合泊松分布，密钥生成协议采用的是基于诱导态的 BB84 量子密钥分发协议，通信总体过程包括：发送方随机地发送相干态、接收方基于“零差检查”原则随机选择待测分量、接收方基于公开通信信道通知发送方其测量的分量信息、双方通过公开信道公开部分数据信息以判断消息的安全性、双方通过“纠错”和“保密放大”算法生成安全一致的密钥信息。

在方案实现过程中，通过模/数转换器将实时语音模拟信号转换为数字信号脉冲信号，然后通过数字密码产生器进行密钥的生成。在这一过程中，发送方和接收方的调制器采用的是非平衡干涉方式。发送方在经过自己的非平衡干涉处理后，变为两个光脉冲信号，由于量子态由调制器对相位角进行了调制处理，此时，攻击者是无法窃听到发送方相位角调整的所有信息；调相结束后，光脉冲会通过量子通信信道发送到接收方；接收方在收到消息后，采用同样的方式采用非平衡干涉将收到的脉冲信号扩增；在此基础上，通过数/模转换将数字信号转换为模拟信号，从而实现对实时语音通信信息的安全传输。

4.总结

本文以实时语音通信为抓手探究基于诱骗态的量子安全通信新基建的应用，提高了实时语音通信过程中的信息安全性能。随着量子信息科学技术的不断发展与完善，数据信息安全治理能力必将得到很大提升，量子保密通信在军队、科研院所、关键基础设施领域也必将发挥不可替代的作用。基于诱骗态的量子安全通信新基建在实时语音通信中的实际应用，不仅验证了量子通信在安全保密方面的安全可行性，并为其在相关领域的推广提供了较好的范例支撑。

【参考文献】

[1]林碧涓.量子通信技术助力产业安全发展[J].通信信息报,2023.02(003):1

[2]高翔.实际情况下的诱骗态量子密钥分配理论研究[D].国防科技大学,2009.