星地量子广域网转入实网运行

文/特约通讯员朱新均 李毅中 肖世校 记者朱培斌 宁钰燕

近日,国家自主研发的星地一体量子广域网络已由试验验证转入实网运行,在政务、金融、能源场景承载真实业务,为国家信息安全构筑起新型防线。这是江教授及其团队持续攻坚的成果。这位深耕量子与区块链交叉领域的科研领军者,鲜少有人知晓,他原是半路转行的文科生。

在茂名一中偶遇量子书籍,埋下好奇种子;英语"从零起步、死磕到底"的经历,为后来钻研英美计算机原版书籍、走上科研道路打下基础。暨南大学"五度播迁"的校史触动了他铸造科研的志向。大学毕业考取国家高级程序员资格,完成从商科到信息技术领域的跨越。考研面试从区块链前身技术谈到行业未来趋势,独到的见解打消了考官对其商科背景的疑虑,最终成功被东北财经大学录取,选择跨专业攻读信息系统方向研究生。后来扎根量子与区块链的交叉赛道。常被质疑为什么非要将两个艰难的方向揉在一起。他说,读研期间导师支持搭建在线教育系统的经历让他体会到,陌生人之间建立信任的成本极高,怎样让陌生人不打听、不求人担保,也能放心相信对方。

量子与区块链相遇,就是这道题在更大尺度上的重做。区块链像一本谁也撕不掉、改不了的公共账本,可它锁门的办法是"这道数学题你算不出来";量子计算机一旦成熟,这题不再难算,今天所有签过名的信任都可能一夜作废。所以不能只打补丁,而要换一把锁:把安全从"算不出来"改成"动了就留痕"。量子密钥一被偷看,状态立刻就变,像有人翻过你的信;量子随机数不是程序编出来的,而是取自真空里真实的涨落;量子签名支撑的共识,也不用再假设"大多数人老实"。就像过去确认一件事,得挨个打电话问一圈人,人越多越慢;现在一次对上暗号就完成了从"请你相信我"到"你不用信我,你自己就能验"。这份信任交给物理定律去保管。

星地量子广域网已开始干活:一把密钥,先问时间,再问身份

一把量子密钥从北京送到南非,飞了12900公里。但它落地那一刻还不算数——得先报出自己是哪一瞬出生的、归谁、几点作废,才准开门。

这三句话听着像较真,却是江教授团队早在2022年就垒完的一道专利墙:授时、编址、分片、加密,四层各管一摊,顺序一步不能错。墙立稳三年之后,中国科大"济南一号"才把星地密钥的尺子拉到12900公里。墙在前,尺子在后——前者决定钥匙送得到,后者决定它送到时还算不算数。近日团队确认,这张网已从试验台走下,在政务、金融、能源场景背着真实流量跑。

第一层:先对表,再说话

网络启动的第一步不是发密钥,是校准时间。

根链节点上的天线与移相器朝卫星"要时间",节点随即调用移相器接口,先在机器里预演两笔账:信号落下来飞多久,天线和移相器把它拆成时间戳又耗多久。两笔一加就是这颗星的误差。算完,从满天可见卫星里只挑误差落进3—50ns的一主一备两颗,往后只认这两颗。



量子圣杯。(源于中国物理学会期刊网)

见功力的是"代授时"。大量老终端没有直连北斗的能力,让它们自己对表,等于拿一块停摆的表去校准别人。系统于是把"根链节点再递到终端"那一跳也记进误差账,反过来挑由谁代取:本地合格节点不够,就越界就近借;节点是手机、汽车这类会走动的,名单每次重算,终端只采最先撞线的那一个。

硬件上还有一手取巧:移相器里管算的那部分被摘出来交还根链扛,前端瘦成"天线+空壳移相器",能钉在机房,也能卡扣式装上电脑、基站、矿车。同一副天线顺带覆盖微波——荒漠远海,短报文只够喊一句"救命",它却能把现场画面和伤情整包甩给通信卫星。

第二层:把时间焊进地址

对完表,给每个节点发身份证。

根链地址不是一串死字符串:身份标识、服务标识、时间戳、有效期四样先一起哈希,再把明文的时间戳和有效期拼在后头。校验方拿同样四样重算,一字不差才放行。B/S走MD5、物理标识取公钥地址;C/S走SHA-256、服务标识留空;应用侧64位哈希;再进一版,连由时间戳反解出的物理位置都单独哈希焊进去。

于是这串地址一次说清四件事:你是谁、供什么、在哪儿、这话多久有效。重放和冒用,在协议第一层就没门可敲——地址一过期,连敲门声都发不出来。

第三层:借别家的路,先签合约

网元把组网诉求写成一笔交易递给根链,写明要哪种共识、自己是谁。根链按NFV/SDN切出分片,把人塞进去再回一句"你进的是这片"。同意才上链,拒绝也上链,两条结局都留痕。每片配一个独立IP协议栈实例,终端同挂八个切片也不撞IP。

借别家运营商资源,走链上"转换合约":把乙方接口翻译成甲方认得的模样。核验分两步——密钥哈希先与链上存根对一遍,对上了,再用这把钥匙以AES-256解开身份密文。此后每次进门的时刻、流量、频带占用、该结多少钱,全部上链,天然就是结算单;打包统一盖国家授时中心时间戳,以防几家账本事后对不上时序。

第四层:加密交给物理定律

前三层管"谁、何时、走哪条路",这一层才管内容会不会被看走。

经典比特经转换单元翻成量子比特,量子智能合约扣动分发:量子信道只搬密钥,经典信道只做签名确认。协议按链路脾气挑——短距SARG04、纠缠型Ekert91/BBM92、测量设备不可信用MDI-QKD、长距骨干上孪生双场TF-QKD;再远请卫星当可信中继,地面光纤按百公里一级布点,把那条"衰减随距离指数塌方"的长坡剁成短段。

团队给了两个不肯客气的时间:同样一份数据,"哈希+时间戳"生成指纹约1秒,改走"时间戳+量子密钥分发"只要15毫秒;同规模跨链访问从30毫秒压到10毫秒。量子最动人的不是快,是窃听会留下尸检报告——谁偷看过,量子态就变、误码率就抬,双方当场知道;钥匙丢了也不必掀桌,还能从别的通信方找回。

墙外第一站:3800公里的中俄链路

四层墙在国内立稳,拉出国境线才见成色。

2022年3月1日,莫斯科郊外兹韦尼哥罗德天文台临时架起的地面站,与新疆乌鲁木齐南山站完成中俄首次"完整周期"量子通信,跨距约3800公里。起封用了两把密钥:一段《墨子》,一段朗道方程。次年10月论文披露,双方已在这条链路上把一张加密图片平安送到对岸。

可量子链路只保证一件事——天上没人偷得走。它不回答另外三件:这把钥匙那一瞬铸的、授权给谁、几点作废。跨国对账历来是扯皮重灾区,各家日志各说各话。团队的办法朴素得近乎霸道:把时间戳和有效期直接焊进地址。中俄链路上每一把密钥要开的那个API地址、那条跨链接口,都带着双方能各自独立复算的哈希。钥匙过了境,身份和时效不跟着漂。这正接住俄方的红线——QKD为主、PQC为辅,最要紧的是授权链条条可溯;一份不需要互信第三方的账本,比一百页备忘录管用。

墙外第二站:三年后,尺子拉到12900公里

2025年3月20日,《自然》在线刊出中国科大的答案。潘建伟、彭承志、廖胜凯团队联合济南量子技术研究院、上海技物所、微小卫星创新研究院,用国际首颗微纳量子卫星"济南一号"——载荷约23公斤,仅是"墨子号"十分之一,成本约是其四十五分之一,光源频率提了约6倍——把济南、合肥、南山、武汉、北京、上海与南非斯坦陵布什串成一条链。

星上诱骗态光源每秒吐2.5亿个信号光子,单次过境攒出25万至100万比特安全密钥,平均约3kbps。以卫星作可信中继,北京—南非跨12900多公里共享密钥,并把一张图像做了"一次一密"传输。地面站从第一代13吨瘦到100公斤以内,可拖进城市、山区、高原,南半球第一次亮起量子地面站。《自然》同期简报标题写得直白:《向长距离安全量子通信的现实飞跃》,审稿人称之为"卫星QKD走向成熟的里程碑"。

这12900公里,恰好把三年前那道墙里最较真的两根柱子顶到极限。

一根叫长时延:低轨星过境只几分钟,一次中继握手要横穿半个地球,地址里的"有效期"就不许写死——写死一秒,链就断在南大西洋上空,只能由时间戳当场推。一根叫移动性:百公斤级地面站能拖着跑,"物理位置哈希进地址"从专利文本里的一句可选方案,逼成日更刚需,站一挪,地址当场重算。

廖胜凯说下一步要与经典安全体系、地面光纤保密网融合并多星组网。江教授团队交出的正是这道接缝:微纳星座负责把钥匙搬过来,根链负责给每把钥匙盖上时钟、身份和失效期。于是3kbps不再是漂亮的实验读数,而成了能计费、能审计、能跨国结算的链上分片。

顺序,就是护城河

"破纪录是中国科大的本事,我们管的是顺序。"江教授说,"顺序一反,量子密钥就只是给一条不可信的通道配了把好锁。他们证明了钥匙送得到;我们这一层,保证它送到时还认得出是谁的,还作不作数。"

难处照实摆着:大规模量子中继还没从实验室模块长成在网设备;天线—移相器前端离"装机即配"尚有体积与成本两道坎;单星3kbps喂一次一密够,喂大流量还得多星叠加混着经典加密;而跨境最硬的从来不是物理层,是规则层——时间戳基准怎么互认、地址字段的跨国语义怎么对齐、密级数据的链上存证在他国法庭算不算证据,都得一条条谈。下一步团队将推进500公里级量子中继与Gbps级密钥速率,并在中俄、中南两线试点这套跨域结算规范。