《量子安全技术白皮书（2022年1月修订版）》发布

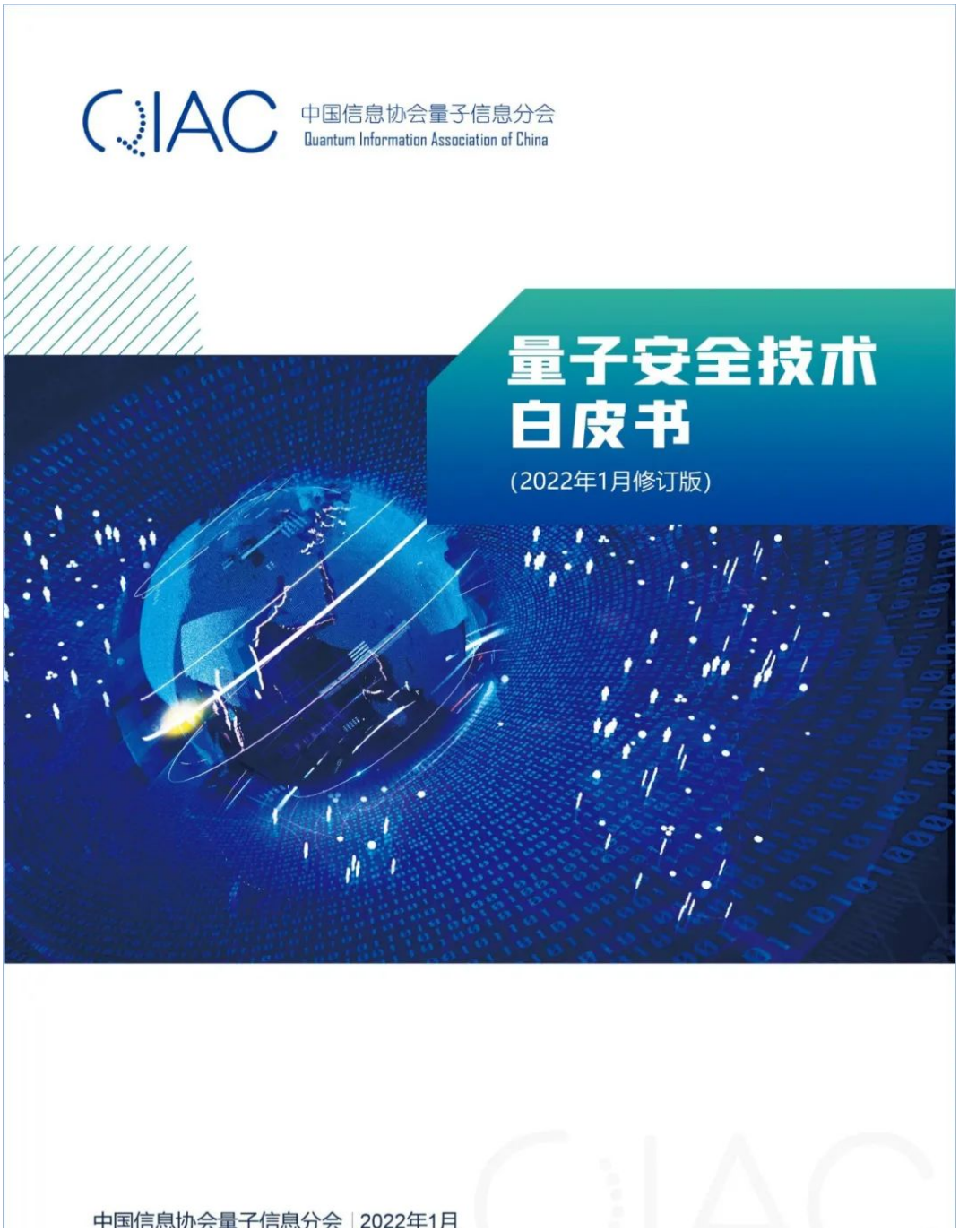
原创 QIAC 中国信息协会量子信息分会 2022-01-31 10:04 发表于北京

中国信息协会量子信息分会于2020年12月发布的《2020量子安全技术白皮书》得到了各界的广泛关注，在促进量子科学与密码科学交叉融合方面起到了积极作用，在凝聚学术和产业共识方面尽了一份社会力量。

本着追求客观公正、凝聚共识的原则，我们持续更新和丰富白皮书内容，并于2022年元月完成了新的修订版。时至牛年岁末、虎年新春，中国信息协会量子信息分会向大家呈现《量子安全技术白皮书（2022年1月修订版）》。

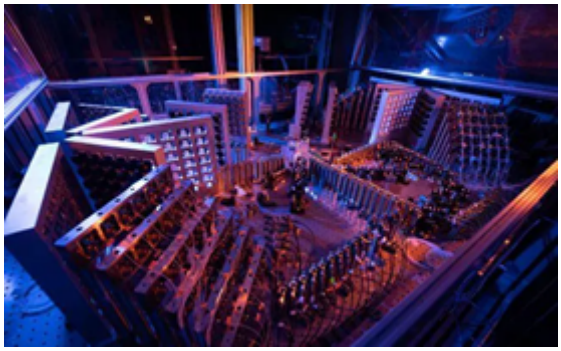
感谢所有协会会员、所有量子信息行业的奋斗者、关心和爱护量子信息技术发展的各界朋友们！

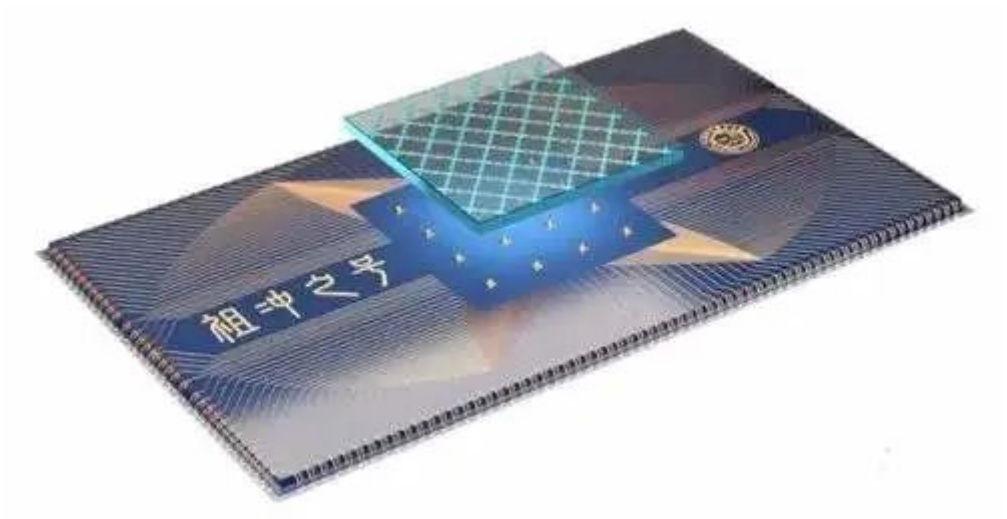
祝虎年幸福安康！



2022年1月修订版 前言

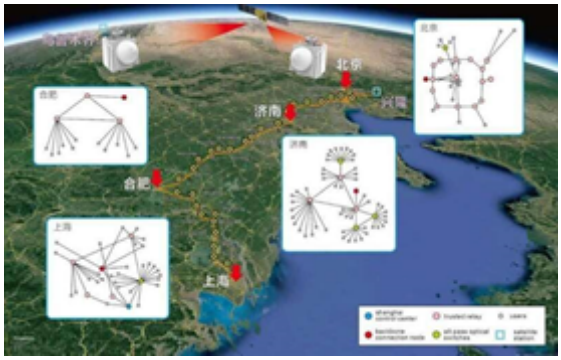
在过去的2021年，量子计算在全球范围内激起了科技创新的新热潮，更多的行业开始入局量子计算的应用探索。量子计算硬件方面，中国科学技术大学“九章号2.0”及“祖冲之号2.0”两台量子计算原型机更新了量子优越性的记录，也令现实量子计算机向着挑战现有密码体系更进了一步。与此同时，量子优越性的达成也激发了经典计算机算法的研究，谷歌“悬铃木”量子计算机2019年实现的量子霸权已经受到了来自超级计算机经典算法的反攻。精彩的“量子-经典”互动极大地提升了人类的算力。





与量子计算的快速进展相对应，量子密钥分发技术及后量子密码技术的发展也进入加速期。2021年量子密钥分发国际、国内标准陆续发布；国家商用密码检测中心也对国内市场上的主流量子密钥产品进行了检测认证；无中继的现场光纤量子密钥分发距离世界纪录已达500km以上，实验室记录已达800km以上；可融入现有通信及密码系统的小型化和芯片化

QKD终端正在成为产品新趋势；更多的能执行量子通信任务的卫星和地面系统已经被规划设计出来。2021年，美国国家标准局（NIST）的后量子密码筛选工作也进入了新的阶段，来自学术界和产业界的目光持续聚焦，也令NIST倍感压力。未来如何部署和使用后量子密码技术，正在成为技术创新之外的亟需研究和探讨的焦点问题。2021年，围绕量子安全，科学与工程、技术与市场的活力正在被进一步激发，也促进了我们对安全的理解。



因此，中国信息协会量子信息分会于2021年组织了修订编写组，对2020年版白皮书进行更新和修订。较为全面地收录和展现了2021年量子安全技术的最新进展，对“密码技术的内涵”以及“量子安全的概念”等内容做了进一步的充实，在文字及章节结构上做进一步改进与完善，并将一些介绍性、拓展性文字放入文本框以示与正文的区分，便于根据需要选择阅读。希望此修订版能为各领域的专家学者及社会关切提供沟通交流的有益参考。

修订版在编写过程中还得到了密码专家孙林红老师、中国科学技术大学徐飞虎教授、清华大学马雄峰教授等专家的帮助和指导。在此，编写组和协会向他们以及对2020年版白皮书编写给予了指导和帮助的各位专家表示深深的谢意！

QIAC

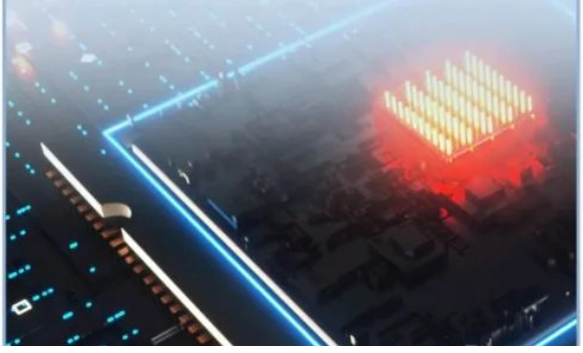
三、量子安全技术应用

QIAC

四、量子安全技术发展现状

QIAC

五、量子安全技术面临的挑战



北京市海淀区西北旺东路10号院互联网创新中心
100193
010-59403206
010-59403200
WWW.QIAC.ORG.CN

点击下载附件👇

《量子安全技术白皮书（2022年1月修订版）》

> QIAC是由量子科技及ICT企业和机构组成的专业性行业团体，致力于服务与量子科技产业化相关的科技创新和成果转化。当前，我们从市场和更广泛的信息安全行业的角度，从能抵御量子计算挑战的安全技术角度，不仅关注量子密钥分发技术的产业化，同时也关注传统密码领域的后量子密码技术的发展，并于2020年12月发布了行业白皮书《量子安全技术白皮书（2020）》，迈出了跨领域凝聚共识、协同发展的重要一步。