

计算机

报告日期：2024 年 12 月 11 日

量子计算&通信：面向未来的超级算力

——量子通信报告

投资要点

□ 谷歌推出“量子芯片”大幅提升算力，巨头纷纷入局

谷歌公司于 2024 年 12 月 9 日宣布研发出一款运算能力超强、适用量子计算机的芯片，宣称这种芯片只用 5 分钟即可完成现有运行速度最快的计算机要 10 尧（10 的 25 次方）年才能完成的任务。谷歌宣称，除了高速运算能力，这款名为“威洛”的芯片还有突出的纠错能力，为研制“实用的大规模量子计算机铺平了道路”。除谷歌外，微软、亚马逊、英伟达等公司也纷纷入局量子计算。2024 年 8 月以来华为多条量子计算专利申请公布，其中量子计算方法及设备申请日期早在 2020 年 1 月，表明华为对量子计算早有布局。量子计算一旦实现应用，许多传统加密算法将被快速破解，而量子通信作为迄今唯一被严格证明无条件安全的通信方式，有望得到大规模应用。

□ 我国在量子计算与量子通信领域领先

1) 量子计算：根据日本 VALUENEX 统计，自 20 世纪 90 年代以来，量子计算机方面中国累计拥有 3217 项相关专利，超过了拥有 2740 项专利的美国。其中，本源量子公司跃居为全球公开专利数首位，2021 年至 2024 年，本源量子新增了 363 项专利，超过同一时期美国 IBM 公司的 212 件。**2) 量子通信：**我国多次开创先河，“墨子号”量子科学实验卫星在国际上首次实现 1000 千米级基于纠缠的量子密钥分发，国家广域量子保密通信骨干网络是全球首个大规模广域量子网络。量子通信专利数也位居全球第一。

□ 传统加密面临量子计算挑战，量子通信推广大势所趋

量子通信是利用量子力学原理对量子态进行操控的一种通信形式，可以有效解决信息安全问题。量子通信是迄今唯一被严格证明无条件安全的通信方式，由于测量坍缩效应，窃听者对量子通信进行的任何观测行为都会对量子态造成改变。目前，上海大学王潮团队利用 D-Wave 的量子退火计算机，成功分解了 50 位的 RSA 整数，已经展示除量子机器破坏加密实践的潜力。可以预见，伴随着量子计算芯片以及算法的进步，传统的加密手段在量子计算的超强算力面前将越来越脆弱。如果基于量子计算强大算力的密码破解实现突破，则作为保密技术的量子通信技术的大范围推广将势在必行。

□ 相关标的

国盾量子、科大国创、复旦复华、浙江东方、格尔软件、禾信仪器、神州信息、三未信安、信安世纪、吉大正元、国芯科技、雄帝科技、普源精电、华工科技、飞利信、天融信、天奥电子。

□ 风险提示

技术进展不及预期、商业化落地不及预期、市场竞争风险、政府财政不及预期。

行业评级：看好(维持)

分析师：刘雯蜀

执业证书号：S1230523020002
liuwenshu03@stocke.com.cn

分析师：童非

执业证书号：S1230524050005
tongfei01@stocke.com.cn

研究助理：张致远

zhangzhiyuan@stocke.com.cn

相关报告

- 1 《“满血” o1 大模型重磅亮相，引领新一轮多模态 AI 迭代浪潮》 2024.12.07
- 2 《华为赋能传统车企转型》 2024.12.05
- 3 《Salesforce 三季度业绩超预期，AI Agent 赛道有望加速商业化》 2024.12.04

并购家 免费行业报告网

IPOIPO.CN 每日更新 不用注册会员 无广告 永久免费

正文目录

1 谷歌研发出超强运算能力“量子芯片”	4
2 量子通信保障通信安全	4
2.1 量子通信：让通信更安全	4
2.2 量子密钥分发：利用测量坍缩防窃听	5
2.3 量子隐形传态：利用量子纠缠传输量子态	7
3 量子竞争日趋激烈，中国量子技术领先	8
3.1 我国量子通信领域多次开创先河	8
4 量子通信实现初步商用	11
4.1 量子通信已实现初步商用	11
5 风险提示	14

图表目录

图 1: 量子纠缠图示.....	5
图 2: 电磁波通信使用大量光子, 通过不同的幅度和频率表达信息	5
图 3: 量子密钥分配技术工程示意.....	6
图 4: 量子隐形传输图示.....	7
图 5: 量子信息各领域企业数量.....	8
图 6: 墨子号科学成就示意图.....	9
图 7: “京沪干线”	10
图 8: 合肥量子城域网.....	10
图 9: 量子通信组网以及安全应用产品.....	11
表 1: 华为量子计算专利申请情况.....	4
表 2: 量子隐形传态重要科学进展.....	7
表 3: “墨子号”量子卫星科学成果.....	9
表 4: 国盾量子量子保密通信网络核心设备.....	12
表 5: 国盾量子推出一系列量子安全应用产品.....	13

1 谷歌研发出超强运算能力“量子芯片”

谷歌于 2024 年 12 月 9 日宣布研发出一款运算能力超强、适用量子计算机的芯片，宣称这种芯片只用 5 分钟即可完成现有运行速度最快的计算机要 10 尧（10 的 25 次方）年才能完成的任务，相关研究成果发表于 9 日出版的英国《自然》杂志。这款芯片名为“威洛”，虽然量子比特多，但错误率却减少了一半，而且还具备适时纠错的能力，谷歌宣称其为研制“实用的大规模量子计算机铺平了道路”。除谷歌外，微软、英伟达、亚马逊也纷纷入局量子计算。

国内方面，2024 年 8 月以来，华为多条量子计算相关专利申请公开，其中量子计算方法及设备早在 2020 年 1 月 14 日就已经申请。

表1：华为量子计算专利申请情况

申请日	专利名称	专利类型	专利状态	申请号	公开(公布)号	公开(公告)日
2020-07-15	超导量子计算系统和量子比特操控方法	发明专利	授权	CN202010682678.8	CN114021727B	2024-11-22
2020-01-14	量子计算方法及设备	发明专利	授权	CN202010039098.7	CN113191499B	2024-11-22
2023-04-07	一种量子计算方法、装置、存储介质以及芯片系统	发明专利	专利的公布	CN202310384743.2	CN118780379A	2024-10-15
2023-02-21	一种费米子算符稀疏化方法及量子计算装置	发明专利	实质审查	CN202310187289.1	CN118536612A	2024-08-23

资料来源：天眼查、浙商证券研究所

量子计算是一种遵循量子力学规律调控量子信息单元进行计算的新型计算模式。量子计算机作为执行量子计算任务的设备，以量子比特（qubit）为基本运算单元。在量子计算中，基于量子叠加原理，量子比特的不同状态可被同时存储和处理。量子计算为解决某些经典计算机难以处理的复杂问题提供了新的可能性，有望在密码破译、材料设计以及人工智能等方面得到广泛应用。

2 量子通信保障通信安全

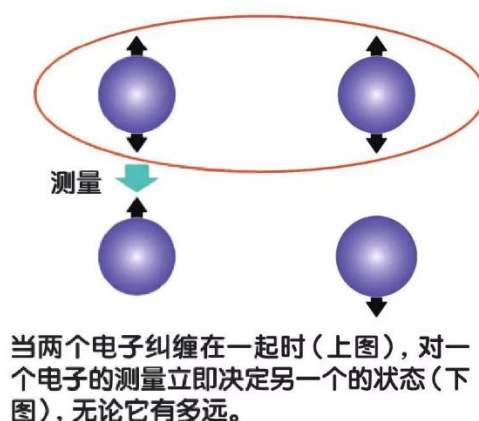
2.1 量子通信：让通信更安全

量子通信是利用量子力学原理对量子态进行操控的一种通信形式，可以有效解决信息安全问题。量子通信是迄今唯一被严格证明无条件安全的通信方式，量子通信所依赖的信息载体是量子态，由于量子具备测量坍缩的特点，因此窃听者对量子通信进行的任何观测行为都会对量子态造成改变，从而通信的双方就能够迅速察觉到窃听行为，及时终止通信，并在之后根据需要更改信道。量子密钥分发和量子隐形传态是量子通信的两项主要技术。

测量坍缩是量子通信中重要的基本原理，表明测量会导致量子的状态发生改变。微观粒子无法用确定的动量和位置描述，但微观系统的运动状态可以完备地用量子态描述，也就是使用波函数。波函数包含了粒子所有可能状态的信息，这些状态可能是多个本征态的叠加。对这个微观粒子进行测量时，粒子的波函数会从多个可能状态的叠加态突然变成其中一个确定的本征态，称之为量子坍缩。

量子纠缠是量子通信工作的另一个基本原理，微观世界中，纠缠的粒子即使各自相隔距离很遥远，之间也没有任何介质，但是其中一个粒子的行为将立即影响到另一个粒子的状态。

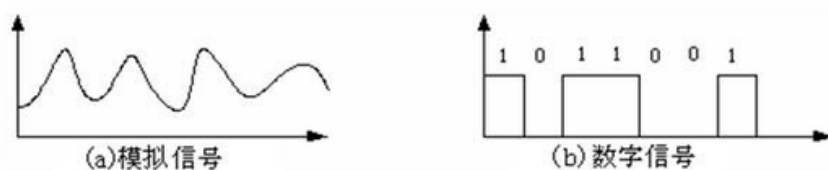
图1: 量子纠缠图示



资料来源: 大科技杂志社、浙商证券研究所

量子通信使用少数量子态传递信息, 比如光子。传统的电磁波通信虽然使用到了光子, 但是使用到的光子数量多且冗余, 窃听者观测或窃取少量光子即可获取通信信息, 而对电磁波产生的影响却难以被察觉。

图2: 电磁波通信使用大量光子, 通过不同的幅度和频率表达信息



资料来源: 仪表网、浙商证券研究所

2.2 量子密钥分发: 利用测量坍缩防窃听

量子密钥分发本质是利用量子的不可复制性以及测量的随机性来生成量子密钥, 主要用于给传统的通信加密。加密通信广泛地应用于军事、金融、商业等领域。用户传输机密的信息时, 无论是通过网络还是无线电传输, 信息都存在被第三方截取窃听的可能, 因此需要对机密信息加密。然而加密信息理论上存在着被破解的可能, 且未来如果量子计算技术能够大幅提升计算机的计算能力, 则现在的许多密码都可能被暴力破解。量子密钥分发技术利用了量子态测量坍缩的特点, 可在双方发送一段信息用于判定通信是否正在被第三方窃听。

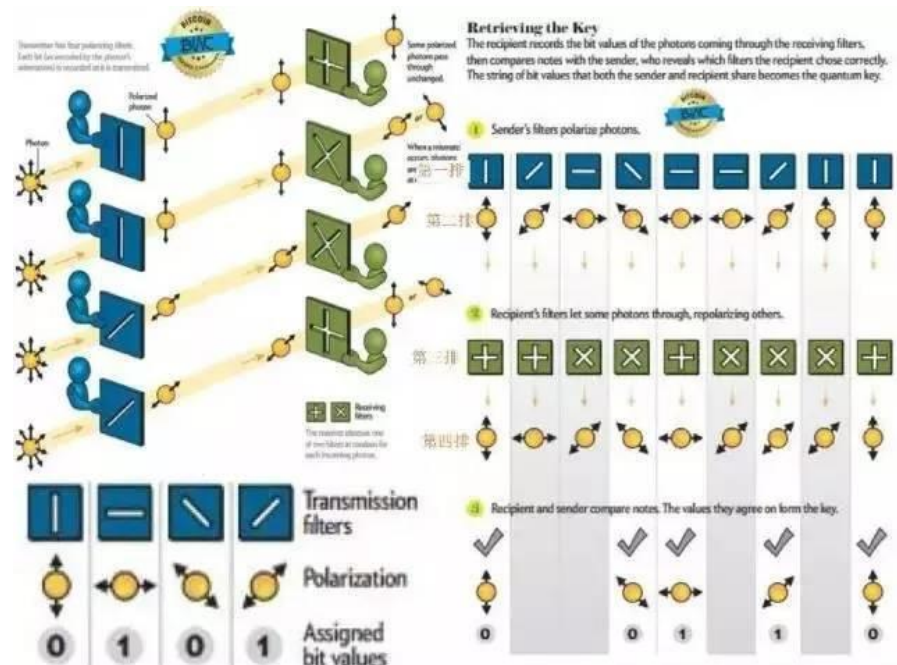
如下图所示, 蓝色为发送方, 绿色为接收方, 发送方和接收方拥有不同类型的偏振滤色片, 只有偏振方向与偏振滤色片符合的光子才能够通过滤色片。其中, 发送方拥有为上下偏振、左右偏振、上左下右偏振、上右下左偏振 4 种滤色片, 接收方则只有 2 种偏振滤色片, 分别是上下+左右、上左下右+上右下左。对于光子, 假设上下偏振和上左下右偏振代表 0, 左右偏振和上右下左偏振代表 1 (也就是说, 光子的 2 种不同的偏振对应于同一个代码, 另外 2 种偏振对应于另一个代码), 那么光子的偏振态就可以转化为二进制编码。

通信开始时，发送方（下称 Alice）通过随机选取 9 次滤色片，将 9 个光子依次发送给接收方（下称 Bob）。Bob 随机选取 9 次“+”字或“×”字偏振滤色片将送来的光子逐一过滤。下一步是关键步骤，Bob 通过常规通信手段将自己使用的偏振滤色片的序列（“+”或“×”）告知 Alice，Alice 把 Bob 所告知的滤色片的序列与自己使用的序列逐一对照，然后告知 Bob 哪几次用了正确的滤色片。如果传输没有受到窃听或干扰，那么下图中，Alice 会告诉 Bob 第 1、4、5、7、9 次使用了正确的滤色片。上述代码依次排列后，为 00110，可作为双方共享的密钥，双方对此都心知肚明。

对于窃听者，如果不观测传输中的光子，那么至多只能知道 Bob 通过常规通信手段所发出的 Bob 使用偏振滤色片的序列，以及 Alice 告知 Bob 哪几次使用了正确的滤色片。但是仅凭这两点无法推算出代码信息，因为 Bob 的偏振滤色片同时支持 2 种偏振态的光子通过，且这两种光子对应的代码分别是 0 和 1（比如 Bob 告知 Alice 第 1 次接收时自己用的是“+”，Alice 告知 Bob 用的偏振滤色片是正确的，对窃听者而言，只能知道光子可能是上下偏振或者左右偏振，但缺乏更多信息来判断究竟是哪一种。又由于上下对应于“1”，左右对应于“0”，因此这种设计使得窃听者无法进一步推算出对应的代码是哪一个）。

而如果窃听者观测到了传输中的光子，则光子的偏振态会发生改变，Bob 接收到的光子偏振态可能与 Alice 发射的不一致，这样双方经过上文所述的沟通后，能够察觉到窃听者。以第一列光子为例，如果窃密者在接收端前插入“×”滤色片，光子偏振状态可能改变成上右下左的斜偏振，接收方仍使用“+”滤色片，得到左右偏振光子，经确认后此位变成“1”。此时，Alice 认为第一位为“0”，而 Bob 认为第一位为“1”。这种出错经过奇偶校验核对非常容易发现和纠正，双方将出错段予以删除后留下的部分就是共享密钥。

图3：量子密钥分配技术工程示意



资料来源：知识分子、浙商证券研究所

量子密钥分配所传输的是单个光子序列，因此传输速度低，无法传输大量文件数据，只能用于密钥共享。当双方确认了密钥的安全性后，再使用经过密钥加密后的数据在网络上进行常规传输。因此，可以认为，量子密钥分发技术应用的本质是加密，而主要信息的传输则依赖于传统的通信手段。

2.3 量子隐形传态：利用量子纠缠传输量子态

量子隐形传态是一种利用量子纠缠进行信息传输的技术，可将一个粒子的量子态以不超过光的速度传输给另一个粒子。量子不可克隆、不可观测，因此在不改变原量子的前提下，直接将一个量子的所有信息完全复制并转移给另一个量子是无法实现的。而量子隐形传态，基于量子纠缠，可以在不测量原来量子全部信息、复制后原量子状态改变的前提下，将原来的量子状态，完全转移给另一个量子。由于量子隐形传态过程中需要借助常规信息传输，因此速度无法超越光速。

如下图所示，假设有一对纠缠的光子，光子1在厦门，光子2在北京。此时，希望把位于厦门的光子3的量子态传递给北京的光子2。此时使用一块立方晶体（分束器），将光子1和光子3分别从2个端面打入（如下图所示）。如果2个探测器同时探测到光子，则可以断定光子2的量子态已经与原来的光子3一样，此时 Alice 将这一信息告知 Bob 后，Bob 就可以确认传输已经完成。一般地，Alice 对光子1和光子3进行测量，将测量结果告知 Bob 后，Bob 根据信息对光子2做么正变换，即可将光子2的量子态转换为光子3原来的量子态。

图4：量子隐形传输图示



资料来源：中国物理学会、厦门大学、浙商证券研究所

当前的量子隐形传态传输能力有限，要真正实现复杂量子物理系统的完整态传输，并把它应用于可扩展的量子信息技术，量子隐形传态就需要走向多体、多终端、多自由度、高维度和远距离。

表2：量子隐形传态重要科学进展

时间	研究者	成果
1997	塞林格团队	单一自由度量子隐形传态
2006	潘建伟团队	两光子复合系统的量子隐形传态
2009	潘建伟团队	证实了量子隐形传态过程穿越大气层的可行性
2015	潘建伟团队	单光子多自由度量子隐形传态
2019	潘建伟团队	实现高维度量子隐形传态

资料来源：百度百科、中国科普博、央视新闻、浙商证券研究所

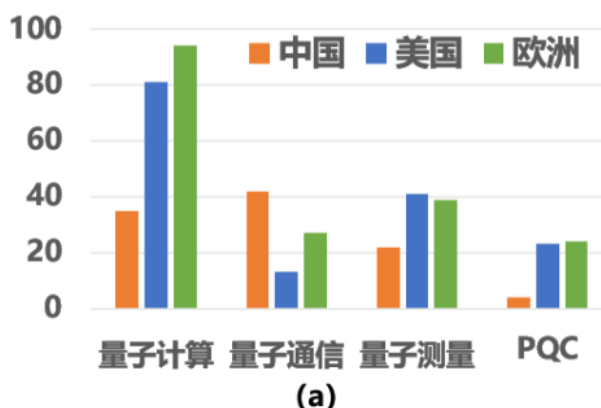
3 量子竞争日趋激烈，中国量子技术领先

量子信息领域国际科技竞争日趋激烈：截至 2023 年 10 月，29 个国家和地区制定和推出了量子信息领域的发展战略规划或法案文件，投资总额累计超过 280 亿美元。以 2018 年欧盟“量子旗舰计划”和美国《国家量子倡议（NQI）》法案为重要标志，各国在量子信息领域规划布局持续加速。

在量子计算专利数方面，中国本源量子公司超越美国 IBM 位居首位。根据日本 VALUENEX 统计，自 20 世纪 90 年代以来，量子计算机方面中国累计拥有 3217 项相关专利，超过了拥有 2740 项专利的美国。其中，本源量子公司跃居为全球公开专利数首位，2021 年至 2024 年，本源量子新增了 363 项专利，超过同一时期美国 IBM 公司的 212 项。本源量子成立于 2017 年 9 月 11 日，是国内首家将量子计算正式推向商用领域的量子计算企业，由中国科学院院士郭光灿和中国科学技术大学郭国平教授带领中科大博士团队创立。

中国在量子通信科研领先。截至 2023 年 9 月中国量子通信发文量约为 5000 篇，是第二名美国的 2 倍以上。截至 2023 年 9 月，全球有 98 家量子通信企业，其中 42 家为中国企业。

图5：量子信息各领域企业数量



资料来源：信通院、浙商证券研究所

3.1 我国量子通信领域多次开创先河

我国在量子通信领域的重要实践，包括“墨子号”量子卫星发射、量子保密通信“京沪干线”建设、城市量子通信网络建设等。

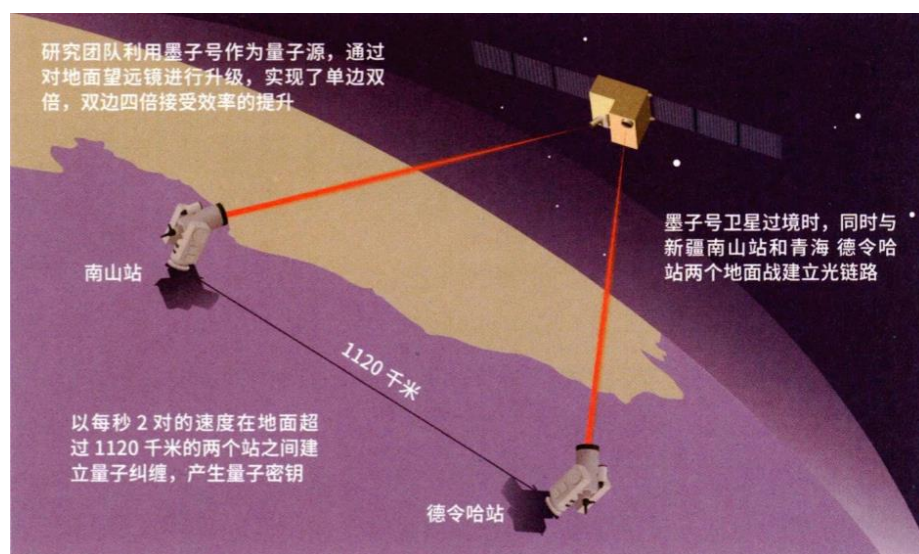
量子卫星：墨子号是中国研制的首颗空间量子科学实验卫星，于 2016 年发射升空，计划开展星地高速量子密钥分发实验、广域量子通信网络实验、星地量子纠缠分发实验、地星量子隐形传态实验。中国后续还计划发射“墨子二号”“墨子三号”，并在 2030 年力争率先建成全球化的广域量子保密通信网络，构建信息充分安全的“量子互联网”。

表3: “墨子号”量子卫星科学成果

时间	成果
2017.6	“墨子号”量子卫星在世界上首次实现 1000 千米量级的量子纠缠。
2018.1	中国和奥地利之间首次实现距离达 7600 千米的洲际量子密钥分发，标志着“墨子号”已具备实现洲际量子保密通信的能力。
2020.6	“墨子号”量子科学实验卫星在国际上首次实现 1000 千米级基于纠缠的量子密钥分发，该实验成果不仅将以往地面无中继量子密钥分发的空间距离提高了一个数量级，并且通过物理原理确保了即使在卫星被他方控制的极端情况下依然能实现安全的量子密钥分发。
2022.4	首次实现了地球上相距 1200 千米两个地面站之间的量子态远程传输，向构建全球化量子信息处理和量子通信网络迈出重要一步。

资料来源：百度百科、浙商证券研究所

图6: 墨子号科学成就示意图



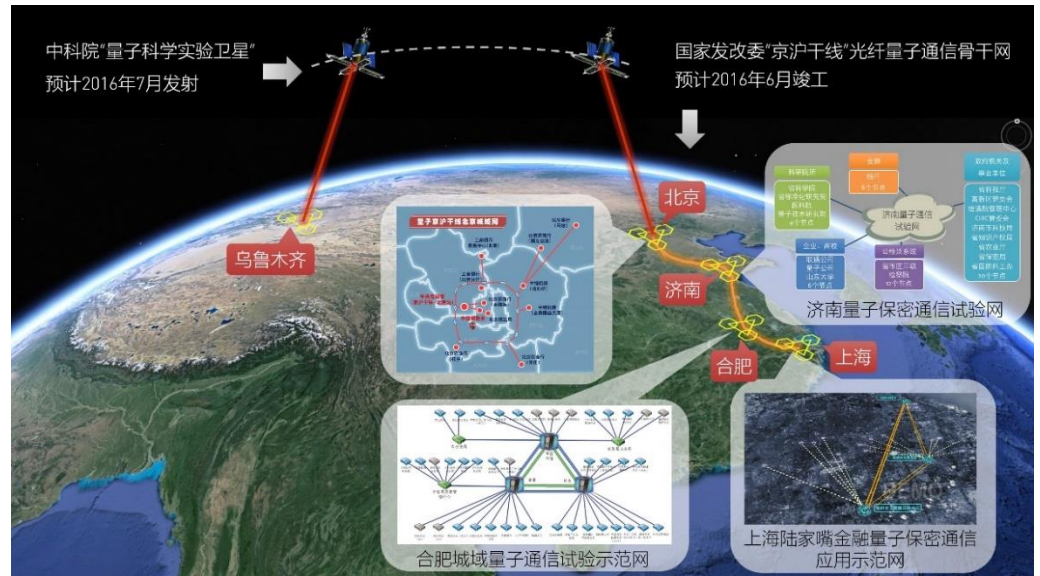
资料来源：百度百科、浙商证券研究所

量子通信骨干网络是一种基于量子通信技术构建的，连接多个重要节点城市或地区的大型通信网络。它就像是交通网络中的高速公路，承担着大量信息的快速、安全传输任务。我国已拥有全球唯一的大规模广域量子网络。

“京沪干线”：量子通信骨干网络“京沪干线”项目于 2013 年 7 月立项，2017 年 9 月 29 日正式开通，是世界上最远距离的基于可信中继方案的量子安全密钥分发干线。可满足上万户的密钥分发业务需求，已实现北京、上海、济南、合肥、乌鲁木齐南山地面站和奥地利科学院 6 点间的洲际量子通信视频会议。整个网络覆盖我国四省三市 32 个节点，包括北京、济南、合肥和上海 4 个量子城域网，通过两个卫星地面站与“墨子号”相连，已接入金融、电力、政务等行业的 150 多家用户。

国家广域量子保密通信骨干网络：在“京沪干线”基础上进一步拓展，一期工程于 2022 年全线贯通并通过验收，覆盖京津冀、长三角、粤港澳大湾区、成渝双城经济圈等国家重要战略区域，地面干线总里程超 10000 公里，是全球首个大规模广域量子网络。

图7: “京沪干线”



资料来源: 百度百科、浙商证券研究所

量子城域网: 早在 2012 年, 合肥就率先建成了我国乃至全球首个规模化量子通信网络——合肥城域量子通信试验示范网。2022 年 8 月, 安徽合肥开通了当时全国最大、覆盖最广、应用最多的量子城域网——合肥量子城域网, 包含 8 个核心网站点和 159 个接入网站点, 光纤全长 1147 公里。项目由中电量子科技有限公司承建、科大国盾量子技术股份有限公司提供核心设备。在加密技术领域, 合肥量子城域网已实现“量子+政务”“量子+移动办公”, 未来可向“量子+数据库”“量子+防伪”等扩展。

图8: 合肥量子城域网



资料来源: 量子信息、浙商证券研究所

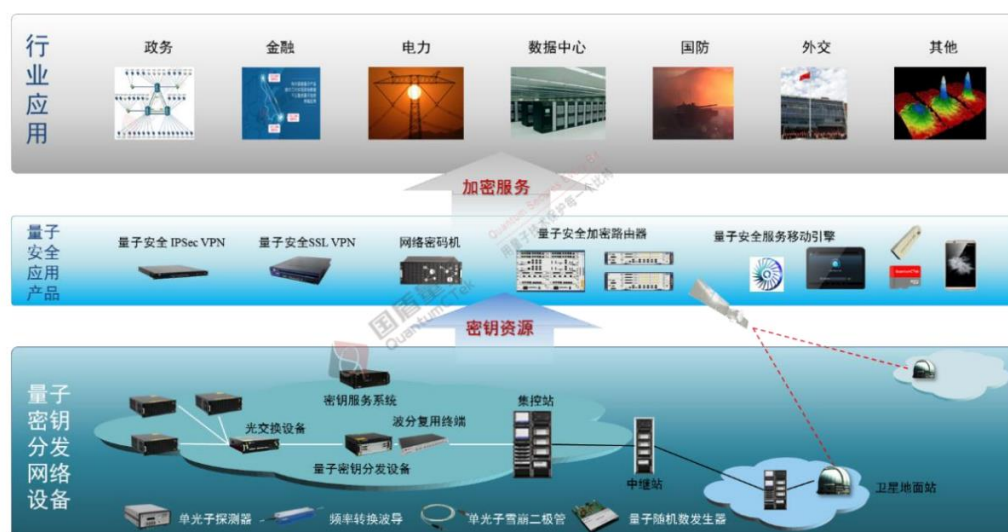
4 量子通信实现初步商用

4.1 量子通信已实现初步商用

量子通信在国防、政府、金融等对保密要求高的领域拥有重要价值。例如，包括对数据中心的加密、构建量子保密通信城域网、骨干网及星地量子通信网络，向用户提供安全加密的通信服务，目前中国已实现广域量子保密通信网络的构建。除传统的保密领域外，量子通信的实际应用范围非常广泛，对安全保密有需求的个人、家庭和企业，都可以接入量子保密通信网络。

量子密钥分发（QKD）技术已经实现初步商用。例如，国盾量子作为国内第一家从事量子科技产业化的企业。在量子通信领域，公司已经推出了量子保密通信以及量子安全应用产品。

图9：量子通信组网以及安全应用产品



资料来源：国盾量子招股书、浙商证券研究所

量子保密通信产品主要用于构建量子保密通信网络，包括应用于城域和骨干网的 QKD 产品，用于量子密钥的分发和存储；量子卫星地面站产品是星-地量子密钥分发的核心设备，协同微纳量子卫星可实现量子密钥分发、密钥中继与数据传递等功能；光量子交换设备用于实现量子信道时分复用，解决了量子通信组网的复杂性以及成本高等问题；密钥系统交换密码机适用于数据机房场景，在量子保密通信网络中属于管控层终端设备，该设备可以与量子层设备、管控层服务系统、应用层设备共同搭建量子保密通信网络。

表4：国盾量子量子保密通信网络核心设备

城域 QKD 产品	偏振编码 QKD 产品		偏振编码 QKD 和 QKDM 均可用于构建城域、局域量子密钥链路，偏振编码 QKD 类型分为发射端、接收端或收发双工，偏振编码 QKDM 类型分为发射端、接收端，附带密钥管理功能。二者均具有高成码率和灵活组网等优势。 城域 QKD 集控站整合了量子密钥分发、光纤信道交换和密钥中继交换等功能，用于实现网络区域管理、网络拓展和信道交换。
	偏振编码 QKDM 产品		
	城域 QKD 集控站		
骨干网 QKD 产品	高速偏振编码 QKD 产品		高速偏振编码 QKD 产品和时间-相位编码 QKD 产品均可用于构建骨干量子密钥链路，二者类型上均分为发射端、接收端。时间-相位编码产品具备抗光纤信道扰动等优势，可用于架空光缆等线路场景。 骨干可信中继站在骨干网可信节点间完成量子密钥分发，再利用“一次一密”方式对量子密钥进行加密传输，以实现更远距离的密钥分发。
	时间-相位编码 QKD 产品		
	骨干可信中继站		
信道与密钥组网交换产品	量子密钥管理机		量子密钥管理机用于存储、调度和使用量子密钥分发设备所生成的密钥。
	光量子交换机		光量子交换机用于切换光纤量子信道，用于局域网和城域网的多终端组网和扩展。
	波分复用终端		量子-经典波分复用终端使 QKD 设备和经典光通信设备在单纤上同时工作；量子波分复用终端使多对 QKD 设备在单纤上同时工作。

资料来源：国盾量子招股书、浙商证券研究所

量子安全应用产品范围相当广泛，涵盖 G 端、B 端与 C 端。产品包括：量子安全服务移动引擎（为用户提供本地接入和漫游接入的功能）、国密邮盾（安全邮件客户端产品，防止邮件泄露）、国盾密语蓝牙耳机（基于量子密钥保护语音通讯隐私，防窃听）、量子身份安全系统（有效保障应用系统访问控制安全）、量子安全智能办公本（实现终端数据加密上云）、量子安全执法记录仪（保障音视频通话中数据传输链路的安全）、国盾密会（保障会议隐私安全）、量子安全高清对讲机（对讲信息安全加密）。

量子通信应用潜力巨大：除了传统的国防、政府、金融机构对保密需求较高外，实际上企业与个人对于通信的保密需求与日俱增。考虑到量子通信技术可以防止任何第三方窃听，因此，如果能够实现完全防窃听，相关应用有望对企业与消费者产生较高吸引力。

表5: 国盾量子推出一系列量子安全应用产品

图片	名称	介绍
 量子安全服务移动引擎 Quantum Safe Service-Mobile Engine Powered by QSD solution from QuantumCTek and CAS QUANTUMNET	量子安全服务移动引擎	量子安全服务移动引擎（QSS-ME）将量子密钥资源通过量子安全介质产品（例如量子安全 U 盾和量子安全 TF 卡）融合到各种移动通信设备中，并对移动密钥进行动态管理，为用户提供任意多点间密钥协商、接入认证、访问控制、安全存储等功能服务。
	量子安全 U 盾	量子安全 U 盾（QUKey）采用自主知识产权的高性能专用安全处理芯片，结合国盾量子推出的量子安全服务移动引擎（QSS-ME），实现了量子密钥资源到移动终端的“最后一公里”配送以及移动量子安全应用。
	量子安全 TF 卡	量子安全 TF 卡（QTCard）物理外观、接口和标准 tf 卡完全一致，采用低功耗的高速专用安全处理芯片，结合国盾量子推出的量子安全服务移动引擎（QSS-ME），可将量子密钥方便的融入手机、PAD 等移动通信终端应用，在满足移动智能设备外扩存储需求的同时提供基于量子密钥的移动安全服务。
	国盾密邮	国盾密邮是国盾量子自主研发的安全邮件客户端产品。本产品采用一邮一密的加密方式，结合高强度国密算法，保障邮件数据在传输、存储全过程的安全性。产品拥有完善的邮件加解密与保护机制，贴身保护用户的每一封邮件，满足企业和用户更高等级的安全需求。
	国盾密语蓝牙耳机	国盾密语蓝牙耳机（QuantumBuds）是由国盾量子自主研发的一款全新量子安全应用产品。该产品支持蓝牙 V5.2 协议，不仅具备市场高端 TWS 蓝牙耳机的降噪品质和音质，同时融合了国盾量子自主研发的语音通讯隐私保护技术，可以有效保护用户在通话、语音消息留言等过程中的隐私信息，让用户在沟通交流中更加安心。
	量子身份安全系统	量子身份安全系统由国盾量子 and 竹云科技联合研发，可有效保障应用系统访问控制安全。基于量子安全加密、量子密钥分发、SDP 架构、MSG 微隔离、IAM 身份和访问管理等技术，产品建立了设备信任、用户信任、流量信任、应用信任的量子零信任可信链条。产品同时提供身份管理、访问控制、权限控制、单点登录、安全审计等统一身份认证相关功能，为城市、政府、企业、科研院所的数字化转型构建多层次动态安全防护体系。
	量子安全智能办公本	量子安全智能办公本是一款集成人工智能核心技术和量子加密技术的智能办公设备。
	量子安全执法记录仪	量子安全执法记录仪是一款能够实现执法现场音视频取证的设备，具备摄像、录音、拍照、语音对讲等多功能，配合后端指挥调度平台，实现可视化远程指挥调度。
	量子安全高清对讲机	量子安全高清对讲机是一款双向移动通信工具，支持可视对讲、集群会议、电子地图等功能。产品融合量子加密技术，在满足高清对讲、高效协作的基础上，配合后端指挥调度系统，对终端对讲信息进行安全加密，有效保障用户通信的可靠性和安全性。
	国盾密会	量子安全视频会议是由国盾量子牵头研发的会议系统系列产品。本产品采用量子密钥加密在线会议音视频数据流，结合高强度国密算法，保障会议数据在互联网上的传输、存储、编解码、加解密等全过程的安全性。产品具有覆盖基础构架、数据存储、网络传输、权限控制及应用管理等全方位的安全性设计，同时提供高清高质量的视频画面，能够适配多类型终端，可为用户提供便捷安全的视频会议体验。

资料来源：国盾量子官网、浙商证券研究所

5 风险提示

技术进展不及预期：如果量子计算的技术进展放慢，则对量子通信的需求不再急迫。

商业化落地不及预期：量子技术较为前沿，商业化落地过程中存在多种不确定性，只有找到真正有需求的场景，才能实现推广。

市场竞争风险：如果大量企业进入，可能造成竞争加剧。

政府财政不及预期：政府、军队等领域对加密通信要求高，是量子通信的重要市场，如果财政不及预期，可能会影响相应的采购。

股票投资评级说明

以报告日后的 6 个月内，证券相对于沪深 300 指数的涨跌幅为标准，定义如下：

1. 买入：相对于沪深 300 指数表现 + 20% 以上；
2. 增持：相对于沪深 300 指数表现 + 10% ~ + 20%；
3. 中性：相对于沪深 300 指数表现 - 10% ~ + 10% 之间波动；
4. 减持：相对于沪深 300 指数表现 - 10% 以下。

行业的投资评级：

以报告日后的 6 个月内，行业指数相对于沪深 300 指数的涨跌幅为标准，定义如下：

1. 看好：行业指数相对于沪深 300 指数表现 + 10% 以上；
2. 中性：行业指数相对于沪深 300 指数表现 - 10% ~ + 10% 以上；
3. 看淡：行业指数相对于沪深 300 指数表现 - 10% 以下。

我们在此提醒您，不同证券研究机构采用不同的评级术语及评级标准。我们采用的是相对评级体系，表示投资的相对比重。

建议：投资者买入或者卖出证券的决定取决于个人的实际情况，比如当前的持仓结构以及其他需要考虑的因素。投资者不应仅仅依靠投资评级来推断结论。

法律声明及风险提示

本报告由浙商证券股份有限公司（已具备中国证监会批复的证券投资咨询业务资格，经营许可证编号为：Z39833000）制作。本报告中的信息均来源于我们认为可靠的已公开资料，但浙商证券股份有限公司及其关联机构（以下统称“本公司”）对这些信息的真实性、准确性及完整性不作任何保证，也不保证所包含的信息和建议不发生任何变更。本公司没有将变更的信息和建议向报告所有接收者进行更新的义务。

本公司的客户作参考之用。本公司不会因接收人收到本报告而视其为本公司的当然客户。

本报告仅反映报告作者的出具日的观点和判断，在任何情况下，本报告中的信息或所表述的意见均不构成对任何人的投资建议，投资者应当对本报告中的信息和意见进行独立评估，并应同时考量各自的投资目的、财务状况和特定需求。对依据或者使用本报告所造成的一切后果，本公司及/或其关联人员均不承担任何法律责任。

本公司的交易人员以及其他专业人士可能会依据不同假设和标准、采用不同的分析方法而口头或书面发表与本报告意见及建议不一致的市场评论和/或交易观点。本公司没有将此意见及建议向报告所有接收者进行更新的义务。本公司的资产管理公司、自营部门以及其他投资业务部门可能独立做出与本报告中的意见或建议不一致的投资决策。

本报告版权均归本公司所有，未经本公司事先书面授权，任何机构或个人不得以任何形式复制、发布、传播本报告的全部或部分内容。经授权刊载、转发本报告或者摘要的，应当注明本报告发布人和发布日期，并提示使用本报告的风险。未经授权或未按要求刊载、转发本报告的，应当承担相应的法律责任。本公司将保留向其追究法律责任的权利。

浙商证券研究所

上海总部地址：杨高南路 729 号陆家嘴世纪金融广场 1 号楼 25 层

北京地址：北京市东城区朝阳门北大街 8 号富华大厦 E 座 4 层

深圳地址：广东省深圳市福田区广电金融中心 33 层

上海总部邮政编码：200127

上海总部电话：(8621) 80108518

上海总部传真：(8621) 80106010

浙商证券研究所：<https://www.stocke.com.cn>