行业专题（第一期）

再也不怕被“窃听”，浅谈量子通讯

2020 年 7 月

主要观点摘录：

1、传统的通讯加密方式利用算法的复杂性提高安全度，超级计算机和量子计算机的出现极大提升了算力，使得破译密钥变得容易。

2、量子通讯准确地说是一种通讯加密方式，利用量子的不可复制和不可分割的物理特性，实现了 “一次一密”，理论上是一种无条件安全的通信加密方式。

3、在信息传递过程中，量子通讯仅仅作为密钥存在，传播信息的载体仍然是人类使用了数个世纪的电磁波，加密方式由传统的数学算法加密改为量子加密。

4、量子通讯技术被少量用于政务、国防等特殊领域；未来随着终端设备小型化、移动化以及成本下降，将扩展到电信网、企业网、个人与家庭、云存储等应用领域。

5、技术、人才、行业经验等是主要行业壁垒。

6、面临挑战。分发能力等底层技术需进一步突破；核心技术供应能力有限；国产高性能元件选择较少；行业标准、资质、测评、认证等体系目前基本处于空白状态；这些是行业发展面临的主要挑战。

目 录

一、量子通讯是什么？ 3
二、量子通讯的原理是什么？ 3
1、量子的特性 3
2、量子通信有两种技术方案 4
三、传统通信加密方式有什么安全“隐患”？ 5
1、窃听手段简单和窃听无法被察觉是传统通讯加密方式的主要缺陷 5
2、面临超级计算机及量子计算机算力极大提升的威胁，更加容易被破译 6
3、量子通讯为什么是安全的？ 6
四、量子通讯的加密方式是如何实现的？ 7
1、“一次一密”加密方式的提出 7
2、BB84 协议的提出解决了密钥传输过程中被窃听的风险 8
五、量子通讯的产业链 9
1、上游产业链情况 9
2、中游产业链情况 10
3、下游产业链情况 10
4、各环节产业链情况 11
六、量子通讯主要有哪些应用？ 12
七、行业内的主要企业情况 12
1、国盾量子 12
2、瑞士 ID Quantique 13
3、安徽问天量子 13
4、浙江九州量子 13
八、行业机遇与挑战 14
1、行业机遇 14
2、面临的挑战 15
九、行业主要壁垒 17
1、技术壁垒 17
2、人才壁垒 18
3、行业经验壁垒 18
4、品牌壁垒 19
十、市场前景 19

一、量子通讯是什么？

量子通讯（Quantum Communication）确切的说应该叫做量子保密通讯，是利用量子力学原理对量子态进行操控的一种通信加密方式。量子通信是迄今唯一被严格证明无条件安全的通信加密方式，可以有效解决信息安全问题。

二、量子通讯的原理是什么？

与传统的密码学不同，量子通讯是密码学与量子力学相结合的产物，现阶段利用量子力学的一些基本物理原理来保护信息的传递。

1、量子的特性

量子一词来自拉丁语 quantus，意为“有多少”，代表“相当数量的某物质”。在物理学中被定义为最小的不可分割的基本单位，是指组成世界各种物质最小的微粒。量子具有不可复制性和不可分割性，也是这两个特性决定了量子密钥的绝对安全。

（1）不可复制性。可以简单的理解为量子在未被观测的情况下可以是任意态的，一旦被观测就会坍塌而被确定下来。比如著名的双缝干涉实验，在未被观测的情况下，光子以波的形式存在，一旦被观测就具有了粒子的特性。

（2）不可分割性。量子是组成物质的最小单位，不能被分割成两部分，从而也就无法实现在窃听过程中截获部分量子从而不改变量子的形态。

2、量子通信有两种技术方案

关于量子通讯，主要有直接通讯方案（量子隐形传态和量子纠缠交换）和量子密钥分发方案，第一种方案尚处在实验阶段，目前应用最广、发展最快的是量子密钥分发方案，是一种通讯加密方案。

（1）直接通信方案

采用量子通信手段直接传送信息，也叫量子隐形传态或量子纠缠交换，这种方案目前处于实验室阶段。也有学者认为量子纠缠只是一种状态，无法用来传递信息，因此在这个领域争议较大。

- **量子隐形传态&量子纠缠交换。**这种方式是真正意义上的量子通讯，利用量子纠缠的物理特性，将信息瞬时传递至目标区域。

（2）量子密钥分发方案

量子密钥分发是通信加密方式，并非信息传递方式，目前应用最广、发展势头正猛，包含两个信道：

- **首先，**仍然使用传统的电磁波传递信息，称为经典信道；
- **其次，**每发送一次信息，就发射一次光子（量子），主要是利用光子的偏振方向，目的是为

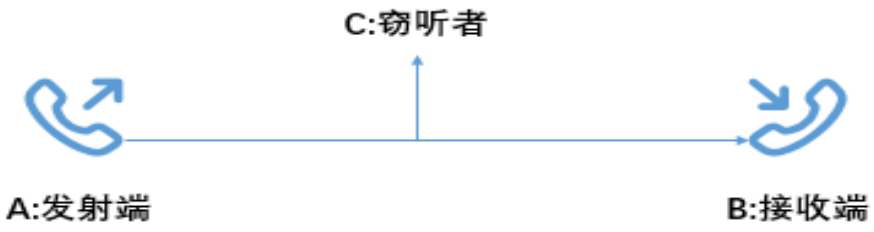
了重新生成新的密钥，即每次加密的密钥都不一样，实现了报文发送的“一次一密”，并且在密钥发送的过程中是不可复制的，可以在原理上实现绝对安全可靠的通信。

三、传统通信加密方式有什么安全“隐患”？

1、窃听手段简单和窃听无法被察觉是传统通讯加密方式的主要缺陷

如下图，在使用传统加密方式通讯中，假如 A 为发送者，B 为接收者，C 为窃听者，在通信中，C 只需要把类似万用表或者示波器一样的东西，接在 A 和 B 之间的电缆上，便能够轻松且听到所有信息，窃听者 C 并不会改变和影响信息的信号，包括波形和强度。这样会导致 B 根本无法发现窃听者 C 的存在。同样，对于光纤通信，也存在类似的问题，例如利用弯曲光缆的方式使信号外泄进行窃听。

图表 1：传统通讯方式



2、面临超级计算机及量子计算机算力极大提升的威胁，更加容易被破译

传统密码学中经常使用的经典 RSA 公钥加密算法，基于一个十分简单的数论事实：将两个大质数相乘十分容易，但是想要对其乘积进行因式分解却极其困难，因此可以将乘积公开作为加密密钥。其破解难度很高。比如说，用 2×3 很容易得成 6，那么 6 却可以再分解为 2×3、3×2、1×6 等，如果是一百位的数分解的话，可逆的程度就是相当难，就需要大量的计算能力去破解。但随着超级计算机和量子计算机的出现，计算能力的大幅提升对上述情况造成了威胁，密码破译变得容易了。

3、量子通讯为什么是安全的？

量子通信利用了量子的不可复制和不可观测的特性来保证传输过程的保密。简单来说就是如果窃听者窃听了信息，那么必然会对加密信息的信号产生影响，接收端接受的密钥信号会发生一定改变，接收端可以通过检测误码率，或者是跟发送端对比，通过分析信号是否正常，来判断是否存在窃听者，如果存在窃听者，可以立即停止信息传输，从而保证信息传递的安全性。

四、量子通讯的加密方式是如何实现的？

1、“一次一密”加密方式的提出

首先保密通信需要使用密钥，分别在发送端对信息进行加密，然后使用相同密钥在接收端解密。信息论创始人克劳德·香农，在上世纪 50 年代对此做出过开创性的研究，提出“一次一密”（One Time Password，简称“OTP”）的二进制无条件安全的加密方式。比如说，通讯双方都是用二进制（1 或者 0）的方式进行信息传递，同时每次都使用不同的二进制密钥来进行异或运算从而实现解密（比如 1&1 对应的是 0，1&0 对应的是 1）。该方法被严格的理论证明为理论上不可破译，**但其缺点是需要大量密钥，同时由于信息传递和密钥传递仍然使用的仍然是电磁波方式，依然存在被窃听的可能性。**

图表 2：“一次一密”OTP 加密方式（举例）

原本	1	1	0	0	1	0	1	1	0
密钥	1	0	1	0	1	1	0	0	1
密文	0	1	1	0	0	1	1	1	1

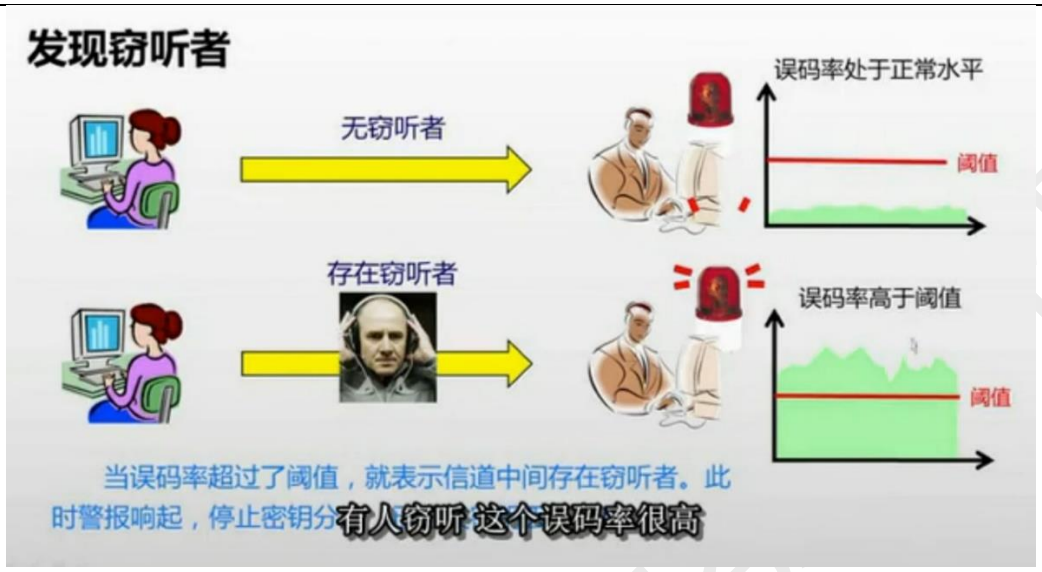
2、BB84 协议的提出解决了密钥传输过程中被窃听的风险

在 1984 年，IBM 公司的 Bennett 和加拿大的 Brassard 提出来了量子密钥分配（Quantum Key Distribution，简称 QKD）的新概念，和对应的量子密钥分配协议—BB84 协议（BB 就是两人的名字首字母，84 代表 84 年提出的），是世界上首个量子密钥分发协议。简单理解就是利用光子的四个偏振方向（横、竖、45°和 135°），选择两个方向代表 1，剩下两个方向代表 0。

举例说明，随机把不同偏振态的光子发送给接收方，接收方使用十字检偏器进行检偏，摆放方向随机，同时把摆放的顺序通知发射方，发射方便可以大致判断接收方得到的结果，然后通知接收方对的留下，错的去掉，比如去掉 2、3、6、8，这个过程还是通过传统的电磁方式传递信息，不怕被窃听，因为即使听到了也不知道 2、3、6、8 对应的是 1 还是 0，最后通过正确率判断是否被窃听，如果没有被窃听，正确率大概是 50%，最终确定留下的便是最终的解码密钥，再次使用 OTP 进行解密即可；如果被窃听，由于光子的不确定性，在窃听过程中改变了原有形态，正确率很低，可以立马停止信息传递，保证信息安全。这就解决了密钥在使用传统

信道传输过程中被窃取的风险，理论上是无风险的。

图表 3：QKD+OPT 量子通讯方式



2001 年，科学家从理论上证明完美的 BB84 协议，具有无条件的安全性，但完美实现 BB84 需要完美的单光子光源，目前人类还无法做出完美的单光子光源，还是会发出多个光子，因此会存在安全漏洞。 同时，由于信道衰减的存在，接收端收到的光子数本身就小于发送端发送的光子数。因此，在目前情况下还无法实现完全安全。

五、量子通讯的产业链

量子通讯的产业链简单可以分成上、中、下游。

1、上游产业链情况

上游主要为量子通信的元器件、光纤、终端，与欧美发达国家相比我国存在先天的发展弱势，国内能够提供核心设备的公司并不多，主要有科大国盾量子技术股份有限公司、安徽问天量子科技股份

有限公司和浙江神州量子通信技术有限公司。国外厂商主要包括瑞士 IDQ、美国 Bennet 公司等。

2、中游产业链情况

中游主要包括网络传输干线提供商和系统集成商，以量子保密通信“京沪干线”技术验证及应用示范项目为例，提供传输干线服务的公司是中国有线电视网络有限公司，提供系统集成服务的公司包括神州信息子公司神州数码系统集成服务有限公司、中国通服子公司中国通信建设集团有限公司等。

3、下游产业链情况

下游主要是各种行业应用，如金融、军事、政务、商务等领域，提供的产品包括量子电话、基于量子保密技术的 IDC、量子白板等。新思界投资分析师指出，由于量子通信行业目前整体处于寡头垄断市场，供应商具有较强的议价能力，再加上当前相关产品的生产成本较高，产品售价较传统通信方式昂贵很多，从而限制了产品的大范围应用。

图表 4 量子通讯产业链

4、各环节产业链情况

上、中游主要包含三个流派，一是中国科技大学潘建伟教授团队，旗下包括国科量子和国盾量子，其中国科量子主要做网络建设集成和运营；国盾量子是提供量子的核心设备，或者是叫方案的提供商。**二是**中国科技大学郭光灿院士，旗下问天量子，主要是做量子保密通信的核心的元器件的研发和设备的解决方案。**三是**九州量子的局部市场，主要做设备和元器件的提供。

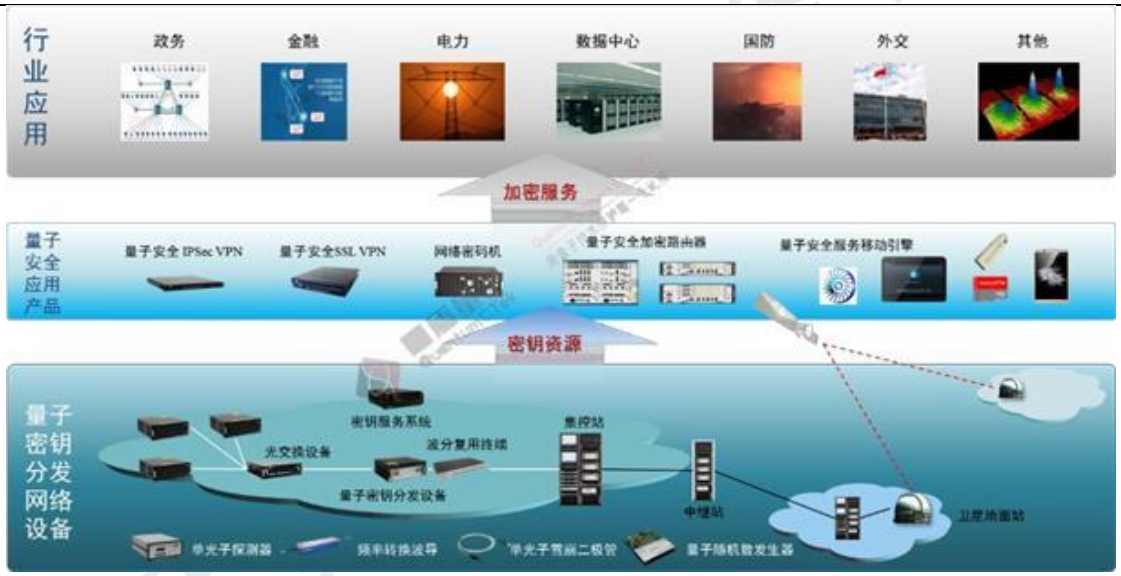
下游市场非常广阔。主要面向 2B 和 2G 用户，这种用户量级还是非常大的。比如量子保密通信墨子号卫星，以及航天五院、航天一院、航天八院都

有一些产业链方面的协作。

六、量子通讯主要有哪些应用？

量子通信具有传统通信方式所不具备的绝对安全特性，同时相比经典通信还有时效性高、传输速度快、抗干扰能力强、传输能力强等优点。不但在国家安全、金融等信息安全领域有着重大的应用价值和前景，而且逐渐走进人们的日常生活。

图表 5：量子通讯的主要应用



七、行业内的主要企业情况

量子保密通信行业属于信息安全行业的分支，目前处于推广期，具有高技术壁垒，供应商较少。

1、国盾量子

发源于中国科学技术大学，创办于 2009 年 5 月以来，经过 10 余年的探索和实践，已成长为全

球领先的量子通信设备制造商和量子安全解决方案供应商，是量子通信产业化的开拓者、实践者和引领者。

2、瑞士 ID Quantique

瑞士 ID Quantique 公司成立于 2001 年，位于瑞士日内瓦，韩国 SK 电信是其单一最大股东。该公司目前有三个业务单元：量子安全加密、光子计数（PhotonCounting）、随机数发生器，主要产品有量子密钥分发设备、量子网络加密机、量子随机数发生器等，主要客户有欧洲本土的银行、博彩、电信等企业。

3、安徽问天量子

安徽问天量子科技股份有限公司成立于 2009 年 7 月，位于安徽省芜湖市。安徽问天量子科技股份有限公司的单一最大股东为宁波梅山保税港区徽缘投资管理合伙企业（有限合伙）该公司产品有量子密码通信终端设备、网络交换/路由设备、核心光电子器件、开放式实验系统、科学仪器以及网络化安全管控和应用软件等，产品主要应用于宁苏量子干线等，主要客户有政府与亨通光电股份有限公司等。

4、浙江九州量子

浙江九州量子信息技术股份有限公司(证券代

码：837638）成立于 2012 年，位于浙江省杭州市，其前身为桐乡市都飞通信科技有限公司，于 2017 年更名为浙江九州量子信息技术股份有限公司。2018 年 7 月，曹文钊、赵义博、芮逸明、黄翔通过投资关系、协议方式成为该公司实际控制人。该公司主要从事量子通信相关业务。

八、行业机遇与挑战

1、行业机遇

（1）政策支持

我国量子通信技术的快速发展得益于国家的提前布局和支持。早在 2013 年，我国就前瞻部署建设世界首条远距离量子保密通信“京沪干线”，率先开展了相关技术的应用示范并取得系列宝贵经验。为进一步保持我国在量子通信产业化发展的领跑地位，近年来从国家到地方各级政府和部门，都给予量子通信高度的关注和推动，支持量子技术发展和开展量子保密通信网络的建设。安徽、山东、北京、上海、江苏、浙江、广东、新疆等众多省份将发展量子信息技术、建设量子通信网络写入 2018 年政府工作报告并推动落实。特别是，长三角地区城市群量子保密城际干线建设已列入十三五规划。

（2）量子通信产业链初步成型

在十余年的发展过程中，我国的量子保密通信技术已经逐渐走到了世界前列，产业化更是先行于世界，初步形成了一条探索型产业链。作为一项以全新物理学手段解决安全问题的量子密码技术，其在安全领域施展拳脚必须满足传统商业客户所要求的成本、性能、适用性等多方面要求，这也促进着 QKD 技术不断地演化发展。

（3）量子计算促进了量子安全技术的发展

基于量子物理基本原理的量子密钥分发技术，即使通过不安全的信道分发密钥也可以保证安全，进一步结合“一次一密”方案或其他加密算法，可以有效地提高信息安全性，抵御量子计算带来的安全威胁。

图表 6：量子通讯的发展历程

从国家战略、技术引领、产业推动、工程建设，多角度支持量子通信技术产业化发展

2、面临的挑战

（1）底层技术需进一步突破

量子保密通信的核心——量子密钥分发技术操控处理的是单量子级别的微观物理对象，高效率的单光子探测、高精度的物理信号处理、高信噪比的信息调制、保持和提取等技术，是量子密钥分发能力进一步突破的“拦路虎”。光学/光电集成、深度制冷集成、高速高精度专用集成电路等技术，是量子保密通信设备小型化、高可靠、低成本发展方向上必须迈过的“门槛”。这些底层技术的突破在较大程度上依赖于新材料、新工艺、新方法的研究和微纳加工集成领域的支撑，有较高的技术难度和不确定性，还面对着高投入、高风险、国际技术竞争和技术限禁等不利局面。

（2）产业链建设需要进一步完善

量子保密通信作为前沿新兴技术，其发展壮大所需的产学研支撑目前还不够均衡，企业参与量子保密通信底层核心技术研究的力量不足；掌握产品研发核心技术的企业数量较少，供应能力有限；部分核心元器件的国产供应能力还不足，特别是高性能元件选择较少；产品和应用缺少全面、体系化的解决方案。这些产业链环节的建设和培育需要多个方向的协同和

积淀，包括量子保密通信行业上下游队伍的壮大、与现有电信网络的融合、产品体系的丰富等。

（3）市场生态需要加快培育

从用户层面来说，目前量子保密通信技术仍然具有一定的“神秘感”，有安全需求的行业用户对于应用量子保密通信的方法和保障程度还缺少充分认识；另一方面，行业标准、资质、测评、认证等体系目前基本处于空白状态，亟待建设。类似于计算机、互联网等行业的发展初期，量子保密通信需要时间通过应用、推广、认证、监管来形成市场互动，推动产业不断升级。

九、行业主要壁垒

1、技术壁垒

量子通信具有跨学科、高精尖的技术特点，产品研发和技术创新要求企业具备较强的技术实力、配置丰富的技术研发资源。量子通信的核心技术架构有别于传统的信息通信技术、密码技术和信息安全技术，研发工作要求对量子信息理论深刻理解，并在光学、微电子学、软件和集成技术等方面形成系统性支撑。另外，不同行业、不同领域的用户对

信息安全的技术需求也不尽相同，行业内企业必须在深刻了解量子通信技术的同时，了解传统信息通信系统和安全技术，才能够研发出匹配用户当前真实需求、兼顾用户安全需求发展空间的产品和应用解决方案。

2、人才壁垒

量子通信行业属于知识密集型行业，需要拥有大量专业知识扎实、创新意识强、经验丰富的研发人员、管理人员和市场人员。虽然国内已有不少高校和科研院所开展量子技术相关课程和研究工作，但是学业有成者还需要经过较长时间产业化的实践经验积累，尤其是量子通信的产品开发，要求对通信、光学、电子学和安全攻防有跨学科的理解。与此同时，管理人才和市场人才不但需要在量子保密通信行业本身，而且需要在信息安全整体行业上通过参与竞争进行培养。行业新进者在短期内难以吸引、培养出一支深刻理解量子信息技术、充分了解市场需求、具备相关企业管理经验的人才队伍。

3、行业经验壁垒

一方面，量子保密通信网络的建设环境各不相同，对方案配置、项目实施以及后期运维提出了高要求。网络建设方案的经济性、项目的快速交付以及业务连续性往往是用户关注的重点，只有具备相

当的行业应用经验，才能够科学合理地配置方案，实现现场快速部署，并高效解决网络运行故障问题。另一方面，量子保密通信主要应用于政务、金融、电力、国防等行业和领域，这些行业和领域具有各异的 IT 建设特征，对信息安全的需求和应用场景特征不尽相同，只有在顺应技术趋势的情形下，深刻了解行业用户的特点，分析、建立用户需求模型，才能为用户提供最优解，实现用户安全价值的提升。这就要求行业内企业具有长期且丰富的解决方案经验积累，新进入者在短时间内难以推出对现有厂商构成实质性竞争的产品和解决方案。

4、品牌壁垒

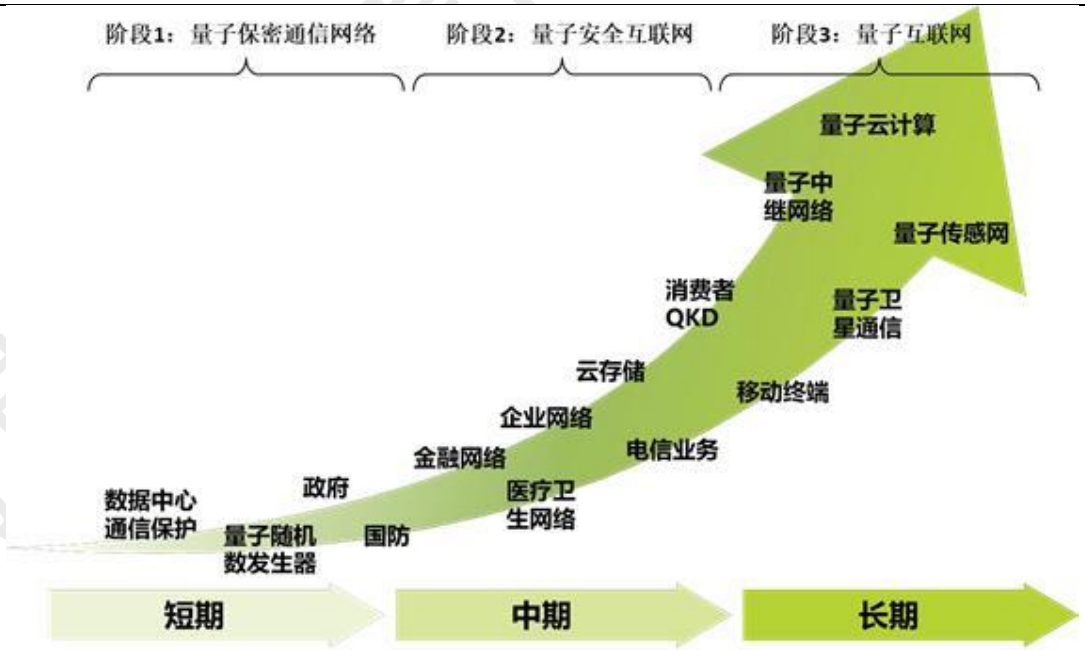
信息安全产品是保障用户数据安全、防止商业秘密和敏感信息泄露的重要手段，用户的采购动机往往出于长期稳健的考虑，关注产品的功能、性能、稳定性和可靠性，希望厂商的技术和产品具有可持续创新发展的特点，对市场主流品牌以及口碑较好的产品具有倾向性。用户一旦形成采购、将厂商产品部署进入信息系统并取得预期的效果后，用户认可的品牌将会形成较高的黏着力和忠诚度，这对于新进入者则构成了品牌壁垒。

十、市场前景

随着量子信息技术的发展，量子通信网络及其

应用不断演进。目前，量子保密通信的应用主要集中在利用 QKD 链路加密的数据中心防护、量子随机数发生器，并延伸到政务、国防等特殊领域的安全应用；未来，随着 QKD 组网技术成熟，终端设备趋于小型化、移动化，QKD 还将扩展到电信网、企业网、个人与家庭、云存储等应用领域；长远来看，随着量子卫星、量子中继、量子计算、量子传感等技术取得突破，通过量子通信网络将分布式的量子计算机和量子传感器连接，还将产生量子云计算、量子传感网等一系列全新的应用。英国政府科学办公室发布的“量子时代的机会”研究报告中描绘了量子通信应用发展趋势，如下图所示：

图表 7：量子通讯的发展阶段



编辑部：河南投资集团国资研究院，战略发展部 0371-69158059