探索的动机

各位同学，晚上好！

我今天报告的题目是“探索的动机”。这个题目，来自于爱因斯坦为了庆祝普朗克60岁生日而作的一个演讲。我当年，1987年进中国科大，大约是1989年读到了《爱因斯坦文集》，里面收录了那篇《探索的动机》，那是我最喜欢的一篇文章。出乎我意料的是，爱因斯坦不仅科学研究做得非常好，他的文章也是写得相当好的。

No.1 一、基础研究的永恒话题

我们中国科大主要是以基础研究来立身立命。基础研究，都有一个永恒的话题，就是（探寻）能够用来回答“我们从哪里来，到哪里去”（的答案）。其实在我们小时候，有了意识之后，对这个问题就开始感兴趣了。我的童年是在农村度过的，我仍然记得，一个晚上我母亲带我到邻村去看电影，看完电影回来的路上，天特别黑，我很害怕，因为传说这条路上有鬼，会出来抓人。我母亲就给我讲，不用害怕，人死了会重新去投胎，哪怕万一被鬼给抓了，也没什么关系。虽然这不科学，但我当时感到特别安慰，哦，原来是这样子，人是可以永生的！所以我们潜意识就想搞清楚，我们是怎么来的？我们的未来又将怎样？

其实，在科学发展到一定程度之前，对于宇宙起源、人类归宿等大问题，人们只能从宗教的范畴来解释。有一段时间，我特别希望搞清楚，为什么基督教会得到如此广泛的喜爱和接受，尤其在西方；我专门去读了《圣经》，并没有真正搞明白。后来，偶然看了一本书，美国作家房龙写的《圣经的故事》，我开始明白了。当时的社会分“奴隶”、“平民”和“贵族”等几个阶层，奴隶就是奴

隶，平民就是平民，贵族就是贵族。于是，奴隶就以为因为自己是奴隶，永远不如贵族，被欺压是命中注定的。可是，《圣经》却告诉你：其实所有的人都是平等的，不管你是贫贱富贵，是黑人白人，我们都是兄弟，都是上帝的子民，宇宙万物和人类都是由上帝创造的！这样一来，你就会觉得我们在这个世界上并不是孤零零的，这个世界是有秩序的，有上帝在关怀着我们；而且，因为信奉上帝，人死后还可以进入天堂，你心里就会感到特别平和安宁。正因为此，爱因斯坦在少年时代深深地信仰宗教。但在他12岁那年，他的这种信仰突然中止了，由于读了通俗的科学书籍，他很快明白《圣经》里的故事有许多不可能是真实的。

那么要解答这些问题，主要还是得益于科学的发展。15世纪时，哥白尼在长期观测天体运动的基础之上发现，按照基督教的说法，如果把地球当作宇宙的中心，那么周围这些行星的轨道就特别复杂。但他如果把太阳当作宇宙的中心的话，结果其实每个星体都是以圆周围绕着这个太阳在运转，这样解释起来就特别简单。所以他当时得出一个结论，写在他的书《天体运行论》中：其实地球不是宇宙的中心。当然他既有基于观测的内容，也有猜测的成分。之后大概100多年，伽利略，其实是我们的“现代科学之父”，首次建立了用实验和数学的方法来研究自然的规律，他有个非常伟大的发明，就是望远镜。他用望远镜去看太空，看到土星环是在变化的、木星环有围绕木星转的卫星等，然后他真实地相信，地心说不成立，而更坚信日心说了。但当时的教皇是他的好朋友，他觉得伽利略这样说，对教会不利。教会想伽利略胆子比较小，我们把他抓起来吓唬他一下，然后让他放弃他的观点就可以了。所以，当时伽利略就被逮进去了。但是伽利略是大学者，不能真的对他用刑，当时也确实没对他用刑。伽利略确实在被捕几天之后，表面上放弃了他的观点了，当然布鲁诺是另外一回事。但不管怎么说，伽利略是现代科学之父。他确实是告诉我们，地球是围绕太阳转的。当然跟他同时期还有另外一个科学家，比他生得晚一点，死得早一点，是开普勒。开普勒非常仔细地收集了很多天体的观测数据，相关的内容高中的时候就已经学过了。他认为，行星围绕太阳运动的轨道，单位时间扫过的面积都是一样的。那么有了这些数据之后，终于一个幸运儿在17世纪出现了。1686年，牛顿发表了经典巨著《自然哲学的数学原理》。他带来了我们人类历史上的第一次真正的科学革命。根据牛顿的观点，所有一切的力学现象，都可以统一为一个简单的公式：

$F=ma$。然后，所有物体之间都有引力，$F=GMm/r^2$。有了这么两个简单的公式之后，哪怕是被认为是神圣的星辰的运动都可以计算。这么一来，他感到非常激动，因为他发现了大自然的奥秘。随后，又在很多科学家，比如麦克斯韦、法拉第、安培，等等，做出了许多科学发现，在此基础上，1864年，也就是在牛顿之后将近200年后，麦克斯韦又发表了另外一部巨著，叫《电磁场的动力学理论》，在书中他把光、电、磁的现象都统一为一个方程组。所以当年在高中的时候，我为什么后来选物理作为我的专业，因为物理需要记忆的东西比较少。你看，所有的东西其实就这么一些基本的公式就可以推导出来了。相对地，像化学以及其他需要记忆非常繁杂的内容，对我来说就太困难了。所以，后来我就选择了学物理。在我们中国科大，在大家以后一年多的学习时间里面，我们是通识教育，会给你们讲很多数学和物理。我觉得非常好，因为这比较简单。

那么，第一次科学革命开始指引人类突破宗教的束缚，因为天上和地上都是由同一规律所统治的。观念上的进步，必然会带来生产力的解放。以牛顿力学为代表的第一次科学革命，马上就催生了以蒸汽机为代表的第一次工业革命（图1）。正因为抓住了这个机会，英国在18世纪末就崛起了，变成了世界上头号强国。随后，因为电力技术的发展，在这个过程当中，德国抓住了机会，19世纪中成为工业强国；美国抓住了机会，在20世纪就变成了头号强国。随着电力技术的发展，导致了第二次工业革命。所以我们就知道科学是如此重要！其实在第一次科学革命之前，我们都是农耕文明，用的都是生物能源，比如驯驯牛、驯驯

图 1

马，然后让它们来帮我们干活。到了第一次科学革命之后，我们才能够用更多新的能源，来改变这个世界。

但是我不知道同学们都想过没有，大家在高中的时候其实就已经可以发现经典物理学有一个非常大的困惑，那就是，只要确定了粒子的初始状态，按照力学的方程一算，所有粒子未来的运动状态原则上都是可以精确预言的。那么，构成世界甚至人类本身的原子、分子，它们在未来的运动状态，是否也是早已预知的呢？这么一来是否意味着决定论呢？而且还是一种比较机械的宿命论，就是一切事件包括我今天的报告都是早已确定好的。这么一来的话，谁最后成为爱因斯坦，谁最后成为杨振宁，谁只能比如说成为潘建伟，好像是确定的，个人的努力都是毫无意义的。而且牛顿力学还告诉我们时间是均匀流逝的，空间是无穷无尽的，而且是光滑的、平直的、无始无终的。那么怎么解释这个宇宙的起源和未来呢？这时候，你可能会觉得还是《圣经》好一点，至少它告诉我们上帝还有一个创世纪。经典物理学否认了《圣经》，但是又没办法解释宇宙有没有起源？有没有未来？而且告诉我们，我们是宿命的。

No.2 二、第二次科学革命

但非常有意思的是，到20世纪初，第二次科学革命又来了。这里面首先要归功于这两位科学家，普朗克和爱因斯坦。当时他们都在德国，普朗克提出了量子论。量子论稍后我会解释，它是揭示我们微观世界特殊运动规律的。爱因斯坦提出了相对论，他告诉我们时间和空间都是相对的，而且空间和时间都是可以弯曲的。所以我们平时所认为的平直的时空，其实是一种“近似”，是一种相对的真理。

更有意思的是，量子力学里面，有很多非常新奇的现象发生了。那么什么是量子，其实在高中的时候大家都学过，比如氢原子的光谱，原子的轨道，还有杂化轨道等，我们都学过了。那么这个到底是什么？首先要讲一下量子的概念。量子是构成物质的最基本单元，它是能量的最基本携带者，它具有一个特征，不可分割。什么意思呢？就是比如我有一瓶水，我可以把它倒出来二分之一瓶水，再倒出四分之一瓶水，再倒出八分之一瓶水，然后这里面的水就越来越少，越来越少。到最后变成什么呢？其实你们都知道，变成一个个水分子了。水分子就是构

成水的最小单元，因为水分子再分就成了氢原子和氧原子，不再是水了。我们这个电灯泡也是这样的，比如说一个15瓦的电灯泡，如果你用一个很小的仪器来测一下，发现它每秒钟会发射出10^{20}个小颗粒。我们把这样的小颗粒，称为光子。原子，我们也知道，从化学的角度来说，是最小的单元了，它是构成各种各样确定物性的最基本单元，它是不能分割的，分割完之后它本来的信息就被摧毁了。这么一来之后，它有一个非常奇怪的特征，就是量子叠加。我们每天的生活当中，比如说某人如果在合肥，他就不会在北京。所以只能是here or there（在这里或在那里），某一时刻，他只能在某个具体的地方，不可能同时在好多地方。但到了量子世界中，其实，量子力学告诉我们，在某些特定的条件下，微观的个体可以同时在好多地方。我们就把这个现象叫作量子叠加。我们每天生活当中，从来没遇到过这种现象，它具体是什么意思呢？我可以举一个形象一点的例子。这个例子不是完全严格的。假定，我到法国、德国去访问了。然后访问完回来，我要到北京。又假定我的航班有两条航线，一条是从莫斯科过来，莫斯科的天很冷，已经下雪了；另一条是从新加坡过来，新加坡很暖和的，现在还是30多度。那么到了北京之后，正好周从照老师到机场去接我，他就问，建伟啊，你这次是从莫斯科航线过来的，还是从新加坡那条航线过来的？但不巧的是，因为我在飞机上太累睡着了，没有去看到底是从哪条航线过来的，结果等我到了北京见到周老师之后，咦，我怎么感觉浑身又冷又热，一会儿感到冷一会儿感到热，就像打摆子一样。然后，周从照说，你不要跟我开玩笑，严肃一点，你下次出国的时候，你就不要睡觉了，睁大眼睛看看你到底是从哪条航线过来的。那么，我刚讲的那种感觉，难道意味着我是同时从两边过来的吗？不然的话，新加坡是很暖和的，莫斯科是很冷的，我应该要么觉得热，要么觉得冷，怎么会又冷又热呢？然后我也很老实，我以后每次去出访、开会，我在飞机上都睁大眼睛不睡觉，看看到底是从哪边过来的。结果我做了一万次实验，我发现随机地有5000次是从莫斯科过来的，我感到浑身冷飕飕的；然后，有5000次是从新加坡过来的，我觉得很暖和。那么，可能我第一次坐飞机太累了，发生错觉了，以后我又可以安心地睡觉了。结果我又坐了一万次飞机，我又睡着了，但是我每次到北京的时候，我醒来的时候，我再次感到又冷又热。那么这不就麻烦了吗？所以只能假定，就是我在睡觉的时候，没在看从哪里过来的时候，我就是又在莫斯科的那条航线上，又

在新加坡的那条航线上。但是你们也肯定会说，潘建伟你别蒙我了，我们也坐过飞机，我坐飞机也睡觉，从来没有这种感觉啊。那么我说不是这样的，其实我们每天的生活当中，不会发生这种现象，为什么？因为我潘建伟睡着了，我旁边那个人他可能醒着的，如果旁边那个人也睡着了，还经常有空姐过来端茶送水的，她会来看你一下，或者说这个飞行员来看你一下。但是，量子力学就告诉我们，在整个宇宙当中，当没有任何一台仪器、没有任何一个人能告诉你，你在什么地方的时候，你就可以处于这种又冷又热的叠加的状态。这是什么意思呢？其实很简单，我们空气当中，是有很多氧分子、氢分子，尽管灯光照过去了，其实你眼睛是看不到它的，光照过去了，大多数物质是不跟这些光子相互作用的。所以这个时候没有人在看那些原子在什么地方。所以看人可以，我始终可以看着你，你没办法同时处于两个地方了，但是看原子就不行，没有一台机器能始终看着它，微观世界里面这种现象时时刻刻在发生着。那么通过这么一个分析也告诉我们一个结论，微观世界，或者说量子颗粒的状态，你去测量是会对它有不可避免的影响的。那么从这个角度上讲，量子力学的哲学，比牛顿力学和经典电动力学的机械决定论要积极得多了。量子力学告诉我们，你这个人去睁开眼睛看一下，这个世界就会变得如此不同。因而人的行为和测量是会影响这个世界的进程的，所以你自己的努力是有意义的。当年有几位科学家思考了牛顿力学的机械决定论之后，就自杀了，他说，我今天要来决定一下自己的命运。其实当他了解量子力学之后，就会知道没有必要那么做了。

量子力学带来了一个非常有意义的进步。利用我们宇宙当中所观测的一些数据，我们其实也可以构建一个所谓的大爆炸理论，大爆炸理论做了许多预言，实验当中也证实了。它告诉我们，现在的宇宙，是在大约138亿年前， 诞生于奇点的爆炸，叫作量子涨落。大爆炸1秒钟之后，质子、中子、光子、电子等基本粒子形成了；然后到3分钟之后，氢、氦元素就形成了。宇宙在膨胀的过程中要慢慢冷却，30万年的时候，原子形成了。然后慢慢受到了引力的影响，开始凝聚，形成了第一代的恒星，就开始燃烧了。然后有的恒星核聚变的原料耗尽之后，抵抗不了它自身引力的收缩，就开始崩塌了。恒星崩塌的能量是如此之高，把质子和电子都聚集到一起了，就形成了中子星，这就是所谓的超新星爆发。最初宇宙中只有氢、氦这些轻元素，在核聚变和超新星爆发的过程中才能产生碳、氧、铁

这些重元素，没有重元素的话，是不可能产生出生命体的。所以讲，宇宙能把我们地球创造出来，能把我们人类创造出来，堪称一位伟大的母亲，它历尽了辛苦。它是要经过100多亿年的努力，到大概35亿年前的时候才有生命出现。那么我们的宇宙有多大？其实我们大家在高中的时候都知道的，我们一个银河系里面，大概有数千亿颗恒星。那么在我们的可见宇宙里面，又有数千亿个银河系。所以我们地球在宇宙里面真的是非常小非常小的一个在阳光中飘浮的颗粒，如同当时一个科普作家所讲的。我们人类的始祖是在500万年之前才出现的。那么到了500万年之前，猿人出现了，然后是早期智人、晚期智人，10000年之前，就出现了晚期智人，我们现代人也属于晚期智人，这是我们人类进化的大致过程。

NO.3 三、信息与社会的进步

那么讲到这个地方之后，就跟今天报告的主题：探索的动机，开始有点挂上钩了。在这里面，其实大家如果对古人类学感兴趣的话，会发现，大概在10万年前，在欧洲同时存在着两种人，一种是尼安德特人，一种是智人。智人最后成为我们的祖先。古人类学告诉我们，尼安德特人更强壮，就是比智人更厉害一点。比如说跟野兽打架，身体也更好一点，跑得也快一点，智人则是比较瘦弱的。而且尼安德特人的脑容量比现代人大，可能比我们祖先智人也聪明一点。但是，为什么在进化的过程当中，智人胜出了，成为我们的祖先？后来考古发现，尽管脑子比较小，身体也比较弱，但智人发明了基本的符号和语言。有了这个符号和语言之后，智人就能有效地共享所获取的知识。比如今天吃了一个东西，我嘴巴肿了起来，然后另外一个人也要吃，我就告诉他别吃了，那东西有毒。我们就能很有效地进行信息的交互，然后就形成了部落，形成几个人、几十个人、几百个人的部落，就形成社会化的群体。所以有社会化的群体之后，是几十个人、几百个人去打一只大象，打一只野兽，并且对付自然界的灾难的能力比较强大，这些使智人在进化过程中更胜于尼安德特人。所以，信息的交互在我们人类的进化当中是非常有用的。从某种意义上讲，一个部落就是一个互联网，只不过现在是全球是一个互联网。那么光有信息的交互还不行，还要能感知信息，能感受自然界。所以后来，出现了诸如大禹治水时需要拿着“规”和“矩”来测量地形，慢

慢地，人们记录了天文观测，形成了历法，懂得按历法耕种、收获等，这都是对自然界的感知。所以感知也是非常重要的。那么另外还有一个非常重要的，就是对隐私的保护。在我们人类的进化当中，大脑是可以保护隐私的。对于传统计算机，这个计算机里面存的是什么你可以去登录看一下而且你也可以把里面的东西拷贝出来。但至少目前，这种操作不适用于我们的大脑。我不知道你在想什么，我也不能把你大脑里的东西给拷出来。如果说我在看某个同学在听我报告的时候，我能知道他心里在骂我，或者他心里对我的观点比较认可，最后就会导致他没办法进行自由的思考了。思想本身的多样性和隐私的保护是紧密联系在一起的，只有这样，我们才能创新和进步。我们既需要交互和感知，同时又需要隐私。从某种意义上讲，信息的感知和交互，已经并将一直伴随着我们人类的进化和社会的发展。

那么这里面有三个永恒的话题，信息交互的效率、对隐私的保护，还有信息感知的能力，某种意义上讲，这是跟我们的当代的信息社会紧密相关的，就是计算能力、信息安全和测量精度。这三个者，随着量子力学、第二次科学革命的诞生，正好催生了现代信息技术的发展。我们用的计算机就是在原子弹的研制过程当中把它制造出来的，因为我们用笔算不动了。所以后来我们国内造原子弹的时候，就造了两台计算机，大概每秒钟可以算 5000 次，好一点的可以算 5 万次，那时很先进，不过比我们现在的手机差远了。随后，科学家为了探索宇宙的本源，来检验这个所谓的标准模型是不是对的，就修建了一个很大的加速器，每天让粒子碰撞，产生了大量的数据。但这些科学家有些在中国，有些在美国、欧洲。中国人不可能老是坐飞机到欧洲去，把数据取回来分析。我们当年上大学的时候，就通过越洋电话线把数据取过来。所以当时在西欧核子中心的一位科学家、物理学家，他提出了万维网的雏形，2017 年他获得了信息界的最高奖——“图灵奖”。其实做物理研究，确实很有意思，他也可以得信息界的最高奖。后来更进一步，要检验相对论到底是不是对的，所以人们制造了非常精密的原子钟。目前最精密的原子钟，大概是从宇宙诞生以来只误差 1 秒钟。这个时候，我在地上放着一个原子钟，在天上放着一个原子钟。地球在自转的过程中，上面和下面的速度不一样，引力也不一样，那么这两个钟过一会之后走的时间就不一样了。你把数据拿来对比，就可以检验相对论。有原子钟之后，就发明了 GPS。GPS 的原理是这样的，

天上有几颗卫星，每颗卫星均有一个星载原子钟，卫星往接收机上发信号。接收机收到三个时间的信号，它自己又有当地的时钟，之后，它就可以求解一个四元一次方程组，就可以把 x、y、z、t 求解出来的，求解出来之后，它就知道这个接收机现在是在哪儿了。互联网、现代通用计算机和 GPS，都是由量子科技革命所带来的附属品。所以从某种意义上讲，前面讲了两次工业革命。相对论和量子力学带来了第二次科学革命，马上就催生了以信息技术为代表的第三次工业革命（图 2）。这个时候，日本抓住机会成为了工业强国。大家都能看到，科学的机会抓住了，工业革命的机会就能抓住，对国家变成强国会起到很好地推动作用。

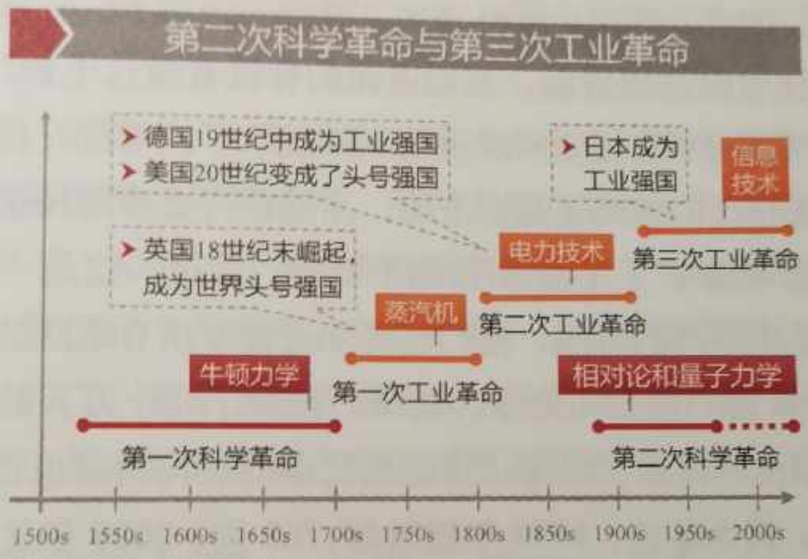


图 2

信息科学经过七八十年的发展，慢慢地遇到了一些非常严重的问题。第一个就是信息安全的瓶颈。为什么我们国家要搞一个网信办——网络安全与信息化办公室，因为我们目前面临的网络信息安全形势日益严峻。其实信息安全是我们人类千百年来的一个梦想。早在古希腊的时候，约公元前 7 世纪，斯巴达人就知道使用一种“加密棒”来进行信息的安全传输。“加密棒”是什么意思，就是这里有个棍子，然后把布带给绕上去，写上信息，比如“attack tomorrow”，就是“明天发动攻击”。然后把布带取下来，交给传递兵去送，如果拿到该布带的人，没有加密棒的话，或者半径不对的话，绕上去就读不出来，也就不知道是什么意思。所以其实老早就有加密术了。然后到公元前 1 世纪，凯撒大帝发明了用一种叫“字母替换”的方法来进行加密。原理是把 ABC 等字母依次往前移三格，原来的 A 就变成 D 了，B 就变成 E 了，C 就变成 F 了，等等。那么 attack tomorrow 就

变成了 dwwdfn…但是非常不幸的是，后来有一位阿拉伯数学家，Al-Kindi，他发现对于此类文字，利用字母出现的频率就可以破译密码。比如就英语而言，A 这个字母出现的概率有 8% 左右，用 E 的频率是 12% 左右。假如你用这种方法写一封信，如果给别人看见，他只要把这些字母出现的频率统计一下，你再怎么替换，别人也可以知道，那个字母频率 8% 的那个就是 A 了，12% 的就是那个 E 了，所以很容易破解。所以历史经验告诉我们，有矛必有盾，你发明一种密码我就可以破解，搞另一种密码我也可以破解。所以就有如下非常著名的事例，在第二次世界大战的时候，德军发明了一种非常有名的密码，叫 Enigma 密码，当时一直无人能破。后来，图灵，现代计算机之父，就把它破解了。破解了之后，盟军没有让德军看出来该密码已被破解。不知道你们有没有看过电影《模仿游戏》，盟军有一次知道德军的海军潜艇要来攻击他们的舰队了，却没有告诉这个舰队，这样才能让德军以为自己的密码还是安全的，才能获得更多的秘密信息。所以盟军不得已选择了“丢卒保车”，让舰队被德军炸翻、炸沉，这是一个非常悲壮的故事。所以等到诺曼底登陆的时候，他们已经知道德军所有军队的分布了，因为德军始终在用 Enigma 密码在发布命令。结果，拯救了几十万人的生命。现代我们广为使用的是公钥密码体系。但是，这些更复杂的现代密码也存在安全隐患。比如 RSA 加密算法，其 512 位，1999 年被破解；768 位，2009 年又被破解；1024 位，尽管现在还没有被宣布破解，但是美国国安局建议最好不要用。再如，2017 年 2 月，谷歌破解了广泛应用于文件数字证书中的 SHA-1 算法，这个是很重要的加密算法。所以这么一来，历史告诉我们一个经验教训：所有依赖于计算复杂度的经典加密算法原则上都会被破解！所以早在 100 多年以前，有位作家就写了一段非常悲观的话，他就开始怀疑：以人类的才智无法构造出人类智破解不了的密码。所以他的意思是，你构造一个密码，总有人能破掉，所以，信息不可能永远是安全的，这是目前遇到的第一个问题。

同时，还遇到另外一个问题。大家经常讲的人工智能，大家都觉得它很厉害，但是其实人工智能它下一盘棋所消耗的能量相当于十吨标准煤，而我们人下一盘棋，吃一碗饭就可以了。所以从这个角度上讲，人工智能它虽然下棋比较厉害，但能源消耗也很厉害。另外我们说大数据。每天我们都产生大量的数据，但这些数据你如果没办法将其中有用的信息给提取出来，那它就是垃圾，你如果

能把有用的信息给提取出来，那么它就是黄金。问题是目前全世界所有的计算能力总和加起来，都无法在一年内完成对2^{80}个数据的穷举搜索。这个数据库看起来很大，但其实也很小，因为每个原子可以同时处于两个状态，80个原子，小得不得了的体系，就能同时2^{80}的状态都存在。所以从这个角度上讲，我们的计算能力是非常有限的。那么全世界都在努力，希望把晶体管的体积越做越小，有一个非常有名的定律叫摩尔定律。摩尔定律告诉我们，单位面积集成电路上可容纳的半导体晶体管数目约每隔18个月便会增加一倍。这是什么意思呢？就是说每隔18个月，晶体管的尺寸变小了，你这个计算机计算速度就变快了，成本就降低了。到了2017年，就达到了22纳米，估计到2022年，可以达到4纳米，达到4纳米的时候它就达到原子的尺寸了。到了原子以后，你就不能老看着它了，这个0也不再是0了，1也不再是1了。它这个0和1就会在里面换来换去。原来晶体管里面，我们基于二进制的0101电路原理将不再适用。另外大家也知道，目前的超级计算机的能耗巨大，我刚才讲了，AlphaGo下一盘棋要消耗相当于10吨标准煤的能量，超级计算机每年用的电量达到十几兆瓦。但是，用一台量子计算机，一年的电费可能几千块就可以了。所以，量子力学在第三次工业革命当中催生了现代信息技术，现代信息技术经过了几十年的发展已经遇到瓶颈问题了。

No.4 四、量子信息与第二次量子革命

其实量子力学，已经为解决这些重大问题做好了准备。

它到底是怎么准备的？量子力学里有一只猫很出名，叫薛定谔的猫。薛定谔举了一个例子，他说在我们的生活当中，每天都在看这只猫，是死的还是活的，它只能处于死的状态或者活的状态。这两个状态如果可以变的话，像开关一样，就可以用来加载1个比特的信息。如果说到了量子世界的话，当没有人可以看这只猫是死的还是活的，在某些时候，它就可以处在死和活状态的相干叠加。那么有的人说，你讲这么多，那猫也不可能又死又活啊？到底怎么实现死和活的相干叠加？其实光就可以。光是有偏振方向的，它会沿着水平方向偏振，沿着竖直方向偏振，等等。我们就把沿着水平方向偏振的光叫作0，沿着竖直方向偏振的光叫作1。然后你放一个半波片，光通过后会转一个方向，它沿着45°的斜线偏振的

时候，其实就是0+1这两个波列的相干叠加。所以，这就是量子相干叠加的一个最简单的实现。那么这里面有一个原理，告诉我们，对于一个事先你不知道的量子态，它本来是又冷又热的，如果你测一下，它就会变成冷的状态，或者热的状态。所以在这种状况下，你就没办法把这个态精确测准了。所以，这里我就不说明了，你们将来学量子理论会学到，所以它就告诉我们一个未知的量子态是没有办法被精确复制的，是测不准的，这是最基本的原理。

有了这个原理之后，爱因斯坦就非常的不满。他说这就等于上帝是在扔骰子了，你看就是50%的概率处于冷的状态，再一看又是50%的概率处于热的状态。他说一只猫可以处于死和活的相干叠加，那么两只猫是不是可以说是死死加活活相干状态的叠加？就像这个公式（图3），我当年学量子力学的时候就很怕这个公式。其实后来，慢慢理解之后，它就相当于右边的这种现象。如果说下面有个同学手里一个骰子，我手里一个，这两个骰子属于纠缠态的话，那么我们在扔的时候，两个骰子扔出的结果都是3，再扔一下都是2。就是不管这两个骰子相隔有多远，只要有一个骰子的点数被确定了，另外一个骰子的点数也瞬间被确定出来。爱因斯坦把这个现象称为“遥远地点之间的诡异互动”，他说这种事情是不应该发生的，毕竟它们都相距那么远了。所以，爱因斯坦进一步对这个事情做了思考。他说，如果说有两个粒子是属于纠缠的，相距非常遥远，它的距离是L，相当于我在扔这个骰子的时候，这个骰子点数定下来所需要的时间是Δt。我们知道世界当中传递最快的是光速，光速乘以Δt如果小于这两个粒子的距离的话，就是类空间隔。也就是说，我扔这个骰子之后，等它的结果确定，它无论如何没有任何能量，没有任何相互作用，能够传递到另外一个骰子。所以，我对一个粒子测量，如果它们之间也是类空间隔的话，就不会对另一个粒子产生影响，这就叫作“定域实在论”。但是量子力学却告诉我们，这个骰子的点数确定是2的时候，另一个骰子也停留到2了。这两个粒子，哪怕空间相距多么遥远，但它还是处于集体态，对一个粒子的测量会瞬间改变另一个粒子的状态，是量子力学的观点。那么爱因斯坦和玻尔有一个非常有名的争论。爱因斯坦说，玻尔，难道你相信上帝会掷骰子的吗？然后玻尔说，这个我不知道，但是你不要告诉上帝可以做什么，不可以做什么。所以爱因斯坦1935年的时候写了一篇文章，他说估计这个量子力学不是对我们物理实在的完备描述。所以我当时学了量子力学之后，树立

量子纠缠

量子纠缠

$$|\cdot\rangle|\cdot\rangle + |\cdot\rangle|\cdot\rangle$$

两光子极化纠缠态

$$|\Phi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|H\rangle_2 \pm |V\rangle_1|V\rangle_2)$$

$$|\Psi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 \pm |V\rangle_1|H\rangle_2)$$

“遥远地点之间的诡异互动”

——爱因斯坦

图 3

了一个宏愿，我就一直想证明爱因斯坦是对的。但是最后，没有办法，所有的实验都证明，爱因斯坦的观点，到目前为止是不对的。这个东西还是非常有意思，但是他们的讨论，当时还没办法通过实验来检验。那么一直到了29年之后，有一位核物理学家叫作John Bell，他提出了一个不等式。他说这两个粒子，其实我们可以来测一个物理量，这边测它沿水平/竖直在振动的光子，那边测它是不是沿45°在振动，等等。测完之后，他说，如果爱因斯坦是对的，这个值应该是小于等于2；如果量子力学是对的，这个值最大可以到2倍根号2。那么这样的话就可以用实验来检验到底是不是有在遥远的地点之间这种诡异的互动。所以从20 世纪70年代开始，其实这里面最早做纠缠的物理学家是我们华裔的科学家，叫吴健雄，她当年为了证实李政道和杨振宁的CP破缺的时候，已经涉及这个现象了，但当时因为没有提出Bell不等式，很遗憾她当时没做这个实验，她如果这个实验也做的话，她一辈子其实就做了两项“诺贝尔奖”级的工作了，真的是非常了不起。那么后来，在伯克利有位科学家叫 Clauser，他做了一个实验，证明它可以达到2.6；到20世纪80年代，法国一位科学家，叫作Aspect，证明它可以达到2.7。然后我的老师 Zeilinger又做了一个实验，到2015年荷兰科学家Hensen又做了一个实验，所有的实验都证明，量子力学是正确的，因为这个值可以大于2。但这些实验仍然存在一些漏洞。

漏洞主要有几个，我想这估计需要你们在座的有些人一起参与进来，一起来

解决这个问题。也许在漏洞解决的时候，新的科学就诞生了。所以我今天还要把它讲得略微深入一点。什么漏洞呢？因为要测这个值的时候，必须有随机数来控制，因为沿着哪个方向测，必须是随机的。如果测量方向不是随机的，而是预先确定好的，那么这个粒子可能会变换状态。因此，需要这两个地方产生随机数，来控制测量装置，而且这两地的随机数必须是完全独立的。但是问题是这个随机数产生器已经放在那里了，所以就不可能保证这两台随机数产生器本身是类空间隔的。所以随机数产生器可能预先存在某种关联，这样的话，测量方向的选择可能不是真正随机的，这就是在2014年的时候，在这篇RMP中提出的问题。另外，我们也知道只有我们人去看它的时候，波函数才真正塌缩，你从又冷又热的状态，变成或者冷或者热的状态。但是问题是，如果我们没有去看，这个仪器可能始终在不停地测，一直没出结果，然后我们人跑去看一下，只有看到结果的时候这个波函数塌缩才真正发生了，所以对两个粒子的测量可能花了很长时间，没有真正处于类空间隔。Leggett是在2003年获得了诺贝尔物理学奖，他写了一本书专门讨论这个问题。所以为了实现这个终极的检验，我们必须实现量子纠缠的超远距离分发。因为你要让人去做实验，你用机器不行了，不相信机器，要相信人。但是我们人的反应速度是很慢的，大概100毫秒才能做出一个选择，那么100毫秒乘以这个光速的话，要保证这个纠缠粒子的分发距离要达到3万公里（km）以上才能进行。这就是为什么，我稍后会讲到，我们希望以后能够来做这个实验。

尽管大家可能觉得这是吃饱了没事干，不停地来证明量子力学是正确的，其实在做这些工作的过程当中，尽管没有实现最终的检验，但是人们已经慢慢地发展了很多很精致的技术了。利用这些技术已经能够对量子状态进行人工制备了，对多个量子间相互作用进行主动操纵了，这样的话，人们的能力也在发生大的飞跃，所以说目前正在产生第二次量子革命。那么为什么把它叫作“第二次量子革命”？大家在中学都学过“孟德尔遗传定律”。田里面的豌豆，有几种是长高的，有的是比较矮的豌豆；有时候开白花，有时候开红花，有些长得大一点，有些长得小一点，等等。这些都是被动观测，大家都知道“种瓜得瓜，种豆得豆”这些规律，但是不知道它背后的原因是什么。那么到了后面DNA双螺旋结构发现以后，然后才发现生物的性状其实是有遗传学方面的基础，是有分子生物学的

基础，就是由DNA决定的。这样的话，通过主动调控即可改变这个性状，这就是基因工程。对于量子，也是这样的，从前我们只能对量子被动观测，然后看到什么现象，做什么改造。但你现在能够主动地组装起来，我把这个原子拿过来，这边动一下，那边动一下，其实就产生了非常强的能力。这种能力就直接导致了第二次量子革命的诞生。

第二次量子革命即“量子信息技术”。量子信息技术可以有三个方面。第一，利用量子通信，可以提供原理上无条件安全的通信方式。第二，利用量子计算，可以提供一种超快的计算能力，揭示复杂系统规律。第三，利用量子精密测量，可以提供一种非常强的感知能力。对于世界很多发生的事情，就可以知道得很清楚。比如，我们现在利用量子精密测量可以探测到引力波了，有三位科学家凭借着引力波相关研究，获得了2017年诺贝尔奖。我们已邀请这3位诺奖获得者12月中旬到我们中国科大来访问。那么，他们当时就利用量子精密测量的手段，以至于在地球和太阳之间，这么远的距离，只要改变一个原子的距离，它都可以测出来。所以这种感知能力是非常重要的。所以说，量子信息从根本上为信息安全、计算能力、感知能力都带来了革命性的进步，非常有可能带来第四次工业革命。

具体来说，利用量子通信，可以实现无条件的、安全的密钥分发。它是怎么来实现的？比如说，张三可以给李四送一系列的单光子，有冷的、热的、又冷又热的。如果一个窃听者中间来窃听一下，因为他不知道哪个是冷的、哪个是热的、哪个是又冷又热的，他中间测一下之后，他就会对那些又冷又热的产生影响。产生影响之后，本来测量之前它是处于又冷又热的状态，结果到了李四的手里后，变成了冷的或热的状态，于是就知道中间被别人窃听过了，那这个密钥就不能用了。这是它的基本原理（图4）。但具体实验要复杂得多，我这里只是为了简单一点表述。另外，窃听者说我可不可以把光子给分割一下，我把它拿走一半啊？不行，它不能分割，分割完了之后，基本状态就没有了。所以不可分割、不可复制，同时保证了存在窃听者一定会被发现。那你可能会说，平时窃听者随便搞一下就不行了，就算不能窃取密钥，但这个密钥也废掉了，你也无法通信了，是不是很脆弱？我说不是的，只要窃听者捣乱的概率小于11.4%，那么他偷走的那些密码，可以通过技术手段将其给过滤掉。窃听者如果在线路上老是在捣

乱，我们还可以借助网络予以解决，从另一条线上走。例如原本的线路是从北京到山东到合肥，如果这条线被控制住，我就改为从北京到武汉到合肥，这是可以换的。然后这个密钥产生之后，就能产生一次一密、完全随机的加密，这样加密的信息就是无法被破解的。这是量子通信的第一种应用，叫“量子密钥分发”。

量子通信中还有另外一种应用，叫“量子隐形传态”（图5）。这种隐形传态就有点像*Star Trek*（《星际旅行》）穿越里面的情形。假定我今天在北京出差，晚上要赶回来作报告，但是航班误了。那么我想紧急赶回来，怎么办呢？别的方法都没有，只有一种方法，用量子隐形传态。在北京和合肥之间具有很多很多纠缠粒子，那么这时候我潘建伟和北京这边的粒子做一个测量，测量之后就把我身上的每一个原子的状态和北京的这一团原子纠缠在一起。那么它到底处于哪种纠缠态呢，会有一个测量结果。把这些测量结果通过无线电台发射到合肥，然后在我们合肥的那个机器里面，我们就开始根据这些结果对合肥这边的粒子进行操作，最后我们就可以在合肥把我潘建伟完整地构造出来了。我的重量、原子的数目、我的头发有几根白了，我的记忆是什么，都一模一样，在量子力学里面原理上是允许这么做的。当然能不能传送人，将来还有没有一些生物学规律、化学规律方面的限制，我还不知道。但是至少这种手段，我来送几十个原子的状态、几百个原子的状态是可以的。当你这么多的信息，0101…的信息在网络里面传来传去的时候，它其实就是一台计算机了。计算机是什么意思，就是有好多存储单元。先读一下，这是0，然后传送到另一个地方，按照需要把这个0变成1，然后

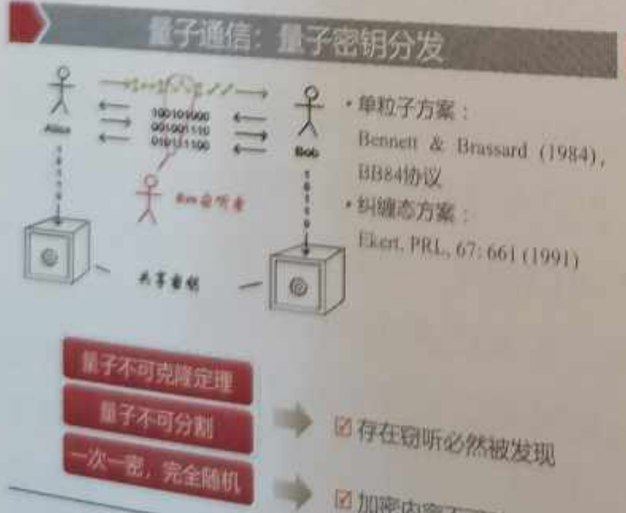


图 4

图 5

再到第三个、第四个地方，看看这到底是什么，最后再测这个结果就是计算结果了。所以一般信息在一个网络里面传送的时候，我们就可以来构建计算机。那么这个传送量子状态的计算机我们就把它叫作“量子计算机”。

量子计算机是什么概念？（图6）在经典计算机里面，一个存储单元，它存一个比特，0或者1的状态。但到量子世界，它处于0+1，这两种状态同时存在。如果说你有两个比特，在经典世界里面，只能属于00、01、10、11这四种组合里的某一种。但到了量子世界，这两个原子，这4种状态可以同时存在。这样一来，如果你有100个粒子，那么系统里的存在状态，就约为原来的2^{100}倍，这个数据是很大的。我觉得大家可能都看过一个故事，就是从前国际象棋的发明者，他发明了国际象棋之后，国王非常高兴，说我要给你奖赏。发明者说，那奖赏很简单，你在我的棋盘里面，第一个格子放一粒麦子，第二个放两粒，第三个放4粒……总共有64个棋格，最后是2^{63}粒。国王说很好啊，你到我的仓库里去拿几麻袋麦子就行了。结果大臣一算2^{63}啊，那个国家好几年的产量都不够。所以到了2^{100}的时候，这个数字就变得特别大了。所以利用这种系统，你就可以同时对2^N个数进行数学运算，相当于经典计算机重复实施2^N次操作。这里我可以举个例子，有一台万亿次的经典计算机，你要分解一个300位的大数的话，需要150000年；但是利用万亿次量子计算机，大概需要“滴答”1秒钟就行。或者你要去求解一个10^{24}个变量的线性方程组，利用目前最快的超级计算机需要100年，但是利用万亿次量子计算机，只需0.01秒就行了。如果利用这么强大的计算能力之后，RSA 公钥密码就立马可以被破解掉了；气象预报可以算得更准确；还可以用于金融分析炒股；也可以用于药物设计；等等。它的用途是非常广泛的。那么我这里为什么举这么一个例子，10^{24}。因为有一个非常有名的事件，本·拉登的“撞举”，这是一个非常恶性的事件。911事件发生之后，美国的中央情报局到它的数据库里查，结果发现，恐怖分子当时打电话联络，哪天计划发起攻击等等电话信息其实已经存在数据库里面。当时怎么就没发现呢，因为他们的数据库太大了，要“大海捞针”地把这些信息发现大概需要100年。就相当于求解我之前讲到的那个10^{24}个变量的线性方程组，100年之后，还有什么作用呢。但是如果分析出这些数据只要0.01秒，那么恐怖分子还没行动，就可以抓起来了。所以从这种角度上讲，量子计算会在很大程度上改变我们的生活。

图 6

另外量子信息里面的技术还在精密测量里面非常有用（图7）。我这里只举一个例子。比如说，我们用来做自主导航，最好的传统导航技术，在航行100天后误差大概在数十公里。假如你要驾驶潜水艇去打恐怖分子，你还需定期上浮利用卫星定位修正，否则就不知道打到什么地方去了。但是利用量子精密测量技术，目前已经比较成熟了，航行100天后定位误差小于数百米，甚至将来可以到米级，所以它不需卫星定位修正，可长期潜伏。从长远上来讲，它可以用于引力波探测、医学检测、自主导航等，所以说精密测量是非常有用的。

那么有人会问，量子信息这些技术，凭什么是你们物理学家给发展出来，而不是计算机学家，或者数学家？比如说数学家应该能更好地把密码给破解掉，或者把密码的方法给发展起来。或者信息学家应该把这个量子信息给发展起来，凭什么是物理学家呢？这个例子我想你们都能回答上来。假如有3个电灯泡，分别对应另一个房间里的3个开关。你怎么能只在这边房间把开关动一次，过去发现哪根灯泡跟哪根线连在一起。数学家是永远解决不了这个问题的。3个开关都打开，那3个灯泡都亮；2个开关打开，那2个灯泡都亮；只开一个有两个灯泡都不亮，他没办法跑一次就解决这个问题。但物理学家可以。物理学家开2个开关，过一会关掉其中一个开关，然后过去看，黑的那个，是跟你没开的开关连在一起的；那个不亮但是还在发热的灯泡，就是那个跟你刚刚关掉的那个开关连在一起的；亮的那

个是跟你一直打开的这个连在一起的，对吧。由此可知，物理学家是可以利用物理规律的。因而，有些时候，思考问题的时候，没有出路的时候，用物理学家的方法，尤其是量子的方法，来思考的话，其实有时候会有很好的收获。

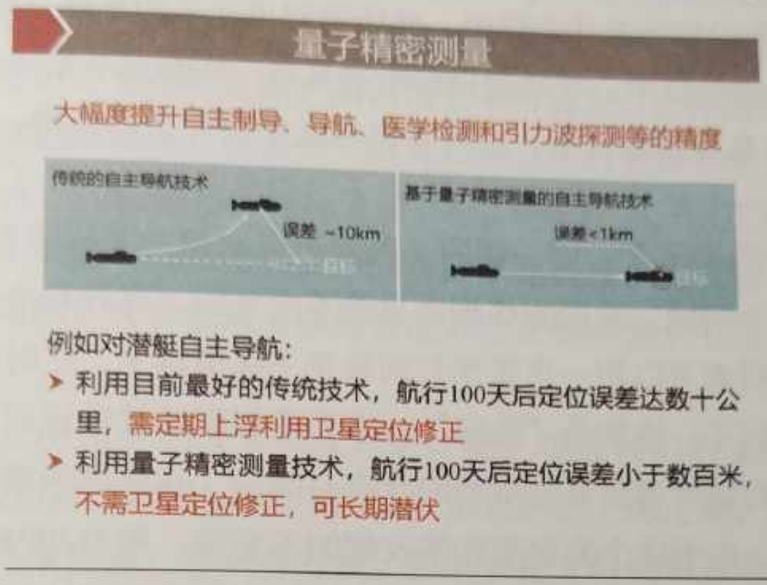


图 7

No.5 五、量子信息技术的实验实现

那么，讲了这么多，大家说量子到底能不能有实际用途啊？我们说，是可以的。首先，为了产生量子密码，我们首先要产生单光子。大家也许会说，单光子很简单啊，反正资源这么丰富，每秒钟可以有万亿个光子飞过来，拿一个送走，拿一个又送走就是了。但问题是光子太多了。比如说我们这里坐的总共大概2000人不到，我突然想把哪个人找出来，也是比较困难的。更加不用说，万亿个光子从你面前飞过，你要一个一个捡出来，加上信息送出去，其实这就变成非常非常困难的问题了。所以我们目前的方法是把普通的激光衰减成很弱的光脉冲，然后保证在每一个脉冲里面找到一个光子的概率只有0.01左右，或者0.1左右。单光子的能量是非常微弱的，用单光子探测器可以探测到，这个非常好。其实我们人的眼睛，在黑暗的房间里面呆了几天之后，一个单光子进来也是能看到的，所以大自然给我们的眼睛是非常灵敏的。商用的单光子探测器拿来就可以用，不用先关进黑屋子里。探测器有半导体的、硅的、超导的、等等，各种各样的。有了这些

东西以后，第一个实验是在IBM做的，量子密码能够传送32厘米。然后经过10多年的努力，又能传到100多公里。但是这里就存在一个问题了。因为所用的光源是不完美的，比如说有P的概率产生一个单光子，那么就有P平方的概率同时产生2个单光子。假设窃听者非常聪明，他能够把单光子的事件全部去掉，因为在量子密码的安全性论证中，必须假设窃听者具备一切物理学原理允许的能力。在张三到李四的信息传送过程中，窃听者把单光子事件全部阻隔，而对有2个光子的事件，他拿走一个光子，把另外一个光子送到李四那里。好了，窃听者拿到的光子和李四收到的光子是一模一样的，他就可以对这一密码进行100%的窃听。然后还有另外一个问题，我们的探测器也是不完美的，有种攻击方式叫作“强光致盲攻击”。窃听者可以用一束强光打到单光子探测器上，这时候单光子探测器对弱光就没有响应了，这就是“致盲”。单光子探测器被致盲后，窃听者就可以操纵它，让它只对窃听者想要它看到的状态有响应，这样等于密钥就全都是由窃听者发给你的了。由于这个发射端和接收端的不完美，所有2005年之前的方案都不安全。等到2005年的时候， 有一位中国科大的校友，当时在日本工作，提出了一个所谓的诱骗态方案。他有了方案之后，首先就跟我们联系，希望我们能够在实验上实现这一方案。结果在2007年我们在国际上首次实现了诱骗态方案，光源哪怕有时候是不完美的，我用诱骗态的方法，也照样可以把安全距离提高到100公里以上。这是在2007年的时候，我们把光源上的问题解决了。到了2012年的时候，有几位科学家又提出来测量器件无关的量子密钥分发方案，对于一切针对探测器的黑客攻击，它都是“免疫”的。就该方案，我们在2013年的时候做了一个实验，当年入选了美国物理学会的年度重大进展。到了2016年，我们把安全距离也提升到突破400公里了，所以在现实条件下的安全性，就很好地建立起来了。所以从2008年我们做一个示范网， 到2012年我们建成了城域网，最后在2012年下半年的时候，这些技术综合在一起，在十八大的时候就用上了。所以后来，到现在十九大，包括全国两会等等，就一直都在用我们这样一个高安全通信保障系统，就是在城域范围里面已经开始走向实用了。

那现在看起来，是不是很好啊，400公里，800公里，一直往下去推进，但是答案是否定的。因为光在光纤里面传输的时候，存在固有的损耗。在经典光通信里面，有损耗也不要紧，把光信号放大一下就行了。但是量子通信不行，因为不

可克隆的性质，是没办法将这个信号放大的，要去放大本质上就要去测量它，看它处于什么状态。比如说，你有一张传真，我再复印一张，就有两张，再复印一张变成三张，每张的信息都一样。在送的时候，有一张或两张纸丢掉了，那这张纸还可以继续往后传，再复印三张，再继续往后传，所以经典信息是可以这么传。但量子信息不行，它不可复制，所以信号不可放大。这样的话，它在光纤传输的过程中信号就越来越弱。所以在长度为1200公里的光纤当中，就是相当于从北京到上海传过去，即使每秒钟可以发射100亿个单光子，而且我们探测器是完美的，那么数百年只能做一个密码。所以有同学说，我只能在城市范围内做一做了，那就没什么用啊，其实我最希望的是能够全世界或整个中国大地上，都能做这件事。

那怎么办呢，所以我们就采取权宜之计吧。现在我们的保密通信用的是专网。专网什么意思呢？就是从北京专门拉一条光纤到上海过来，然后保密信息在这条光纤在里面传来传去，不对外开放。但其实把光纤略微弯曲一下的话，利用泄露出来的一点点光，是可以进行窃听的，所以即使是专网，原理上线路上的每一点都不安全。那么在量子保密通信中，我就把这个1200公里分成30或者20段，每段之间用一个中继站连接。我们需要人为保证的是每一个中继站点的安全，就相当于送鸡毛信一样，北京送到济南是安全的，然后济南送到合肥是安全的，等等。你只要保证北京、济南、上海这几个点有人看守不要被人窃听就行。但传统的专网，你要真的保证它安全的话，每个点都要保障。这就是远距离量子保密通信“京沪干线”的工作原理，我们在国家发改委的支持之下，在2017年9月29号，正式开通了，已实现有各种各样的应用，比如说中国有线、银监会、工商银行、国家安全部门等等，在金融领域的应用主要是银行的同城数据传输，银行数据的远程再备、银行数据的监管、金融信息交易，还有一些政务国防的应用等。

但是这样的方法还不是特别有效，你要保证30多个中继站是安全的，总之不太好。所以其实在2003年，我们就考虑另外一种更有效的解决方案，就叫自由空间量子通信。大家知道，在外层空间都是真空，所以是没有光的吸收的。而且我们计算了一下，整个垂直大气只有地面水平大气5到10公里的等效厚度。5到10公里的水平大气的话，其实80%的光是可以到达接收站的。但是在光纤里就不一样，100公里的光纤，大概只有1%的光可以到达终端。那么，200公里就

只有万分之一了，300公里就只有百万分之一了，是指数衰减。有了这个想法之后，我们其实从2003年开始，花了10多年的时间，进行了星地量子通信的地面验证实验。到了2004年底，我们在合肥的大蜀山做了一个实验，把量子纠缠往两边送，证明13公里之后，这个量子纠缠还是可以很好地存活的，也就证明光子在穿透大气层后，它的量子态还没被人看过。因为看过的话，本来又冷又热的，就变成了冷或者热的。那么第二步，我们在青海湖，验证了在高损耗星地链路中进行量子通信的可行性。因为大气的损耗只有20%，但是从天上送下来，经过近千公里之后，这个光斑是会变大的，所以不可能把所有的信号全接收进来。那么我们发现，哪怕光斑变大之后，我们所接收的信号，也是可以进行量子通信的。那么最后，卫星是飞得非常快的，那么在卫星各种运动姿态下能不能进行星地量子通信？低轨卫星每秒钟飞八点几公里，我们也验证了进行星地量子通信的可行性。所以经过十多年的努力，我们在地面上发展了各种各样尖端的技术证明这个事情是可以做的。我们发展了非常好的技术，例如高灵敏的能量分辨率，相当于如果有个人现在躲在月球上，他要吸烟，划了一根火柴，用我们的装置，在地面上，我是可以看到的。

我们从2003年有这个想法，所以有的时候还真是十年磨一剑啊，用很长时间，我们的“墨子号”终于在酒泉卫星发射中心成功发射。发射成功之后，我们有几个使命，第一个要实现千公里级星地量子密钥分发，结果我们发现量子密钥分发的速率比在相同距离的光纤里面可以提高20个数量级。然后发现，我们也可以进行千公里级星地量子纠缠分发。我们真的在地面上看到了，在青海德令哈和云南丽江之间，这两个光子，还真的有那种遥远地点之间的诡异的互动。另外我们也做了一个千公里级地星量子隐形传态，最远的距离是1400公里。我们可以把地面的量子态传到卫星上去，但没有把这个粒子本身送到卫星上面去。这三项工作，以封面标题或封面文章的形式，发表在*Nature*和*Science*杂志上了。

当年在读中学的时候，我看过有个实验，说大气压多么厉害，两个半球密闭在一起抽真空后，八匹马都拉不开，就是那个马德堡半球实验，我觉得那个实验是非常有意思的。科学是非常美的，在野外做实验更加美。你看我们做实验的时候，也是非常有意思的，所以其实你们在放暑假的时候，可以跟我们实验室联系，你们可以到这些很漂亮的地方晚上看看我们的实验。这个是我们在实验时

拍摄的照片（图8），卫星每次过顶大概在300秒左右，照相机每次曝光5到10秒钟，然后把卫星过顶的整个轨迹拍下来，最后合成在一张照片上，就是我们现在所看到的情况，而且你用肉眼也是可以看到的。所以其实做实验是很有意思的。而且那个地方在乌鲁木齐的南山，草原上还可以骑骑马，烤烤羊肉啊什么的。科学家不是那么苦的，其实是蛮有意思的。

图 8 “墨子号”量子科学实验卫星过境

拍摄于新疆南山天文观测站（多张照片合成）

在量子计算方面我们国家也是取得了非常好的成果的。我们从2005年开始，发表这个领域国内第一篇*Nature*的文章，实现终端开放的量子隐形传态，然后到了2007年实现了快速搜索算法，到了2007年又做了快速质因数分解，然后又做了线性方程组求解，到了2015年做了量子机器学习，等等。特别是在2012年，我们在拓扑量子纠错方面取得了很好的成果，当时我们的工作是发表在*Nature*纪念图灵诞辰100周年的那期专刊上。我们已经实现了所有重要量子算法的实验验证，那么当然这些都是小儿科的，15等于5乘3、21等于7乘3，都没什么用，你一下就能算出来了。我们能不能算得比经典计算机快一点呢？到了2017年我们有了比较好的结果。这是我们构建的可编程光量子计算的原型机，首次演示了超越早期经典计算机（ENIAC、TRADIC）的能力。随后我们又实现十个超导量子比特的量子计算芯片，在这个基础之上我们又实现快速求解线性方程组的量子算法。所以

我们从1997年开始做量子计算，经过了20年的努力，我们总算赶上了经典计算机的尾巴，就是赶上它们1946年的水平了。但是，这“赶上”很了不起，为什么呢，因为可能在以后的5年里面，我们在某些能力上，就有可能会超越目前最快的超级计算机了。也就是说从第一台经典计算机到现在超级计算机，花了大概70年时间。而量子计算机一旦赶上了第一台经典计算机，再过3至5年就有可能超越超级计算机了。这是一个非常好的进展，那么它可以用于很多东西，比如说，用于优化交通网络，优化治疗，也可以实现高效的全局搜索，尽可能地减少堵车，也可以加速机器学习训练速度等。

六、量子信息的未来发展

其实目前在国际上，比如说欧盟和英国，2015年就大概投入4亿英镑用来开展量子技术专项。2016年4月，欧盟跟各个成员国一起投入30多亿欧元来启动量子技术旗舰项目，2018年正式启动。他们计划开展原子钟、量子传感器、星地量子通信、量子模拟机、量子互联网等研究。欧洲还有一个广域量子通信网络计划，等等。美国也非常重视，2017年10月，美国国会开了一个听证会，听证会形成了一个结论，就是美国绝对无法承受量子技术革命竞争中失败的代价。而在2018年6月，美国众议院科学技术委员会立法启动总额约13亿美元的国家量子计划行动，主要研究领域为超精密量子传感、防黑客量子通信以及量子计算等。所以确实我们面临着非常激烈的国际竞争。当然企业也在积极地参与，像俄罗斯的国家开发银行，他们建立了俄罗斯的国家量子中心；而谷歌、IBM，还有英特尔等都有相关的投资，在量子计算领域开展相关的工作。

我想，通过10到15年的努力，我们非常有希望在量子通信领域形成一个完整的空地一体广域量子通信网络体系，在国防、政务、金融等领域得以广泛应用（图9）。到时，可能在15年之后，我们平时的网上转款等都非常有可能会用上这方面的技术了，这是第一方面。当然有些人喜欢搞有用的技术，那么量子通信技术到底有没有基础研究方面的价值呢，也是有的。比如利用星地之间的量子隐形传态，把分布在全世界的望远镜接收到的光都汇集起来，就可以得到一个口径相当于整个地球截面的望远镜，那样就可以得到非常高的空间分辨率。用这个技

术，如果有一辆汽车漂在木星的轨道上，那汽车的牌照是可以很清楚地看到的。其实这跟引力波探测的很多技术都是紧密相关的。另外，在GPS里面，基于卫星的微波授时长期稳定度是10^{-15}。如果用光频率传输的话，这个长期稳定度大概就可以达到10^{-19}。这就为我们的导航定位带来非常革命性的变化。利用我们自由空间里的纠缠分发，还可以把世界各地原子钟的原子纠缠起来，再和光的频率传输结合在一起，可以来大幅度提高原子钟本身的短期的稳定度。如果有100个原子纠缠，短期内的稳定度可以提高10倍；如果有10000个原子纠缠，短期内的稳定度可以提高100倍，因为是根号N的关系。

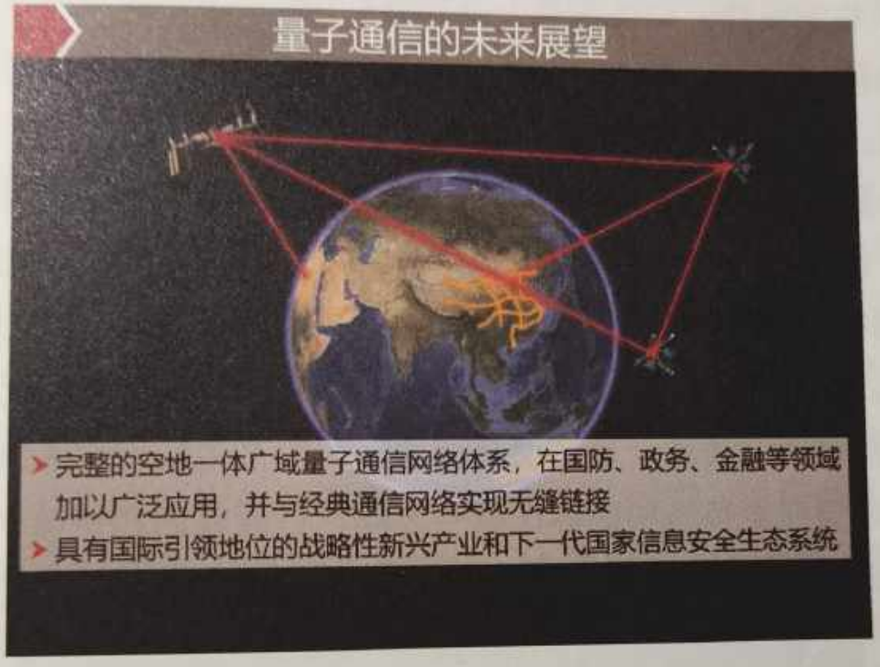


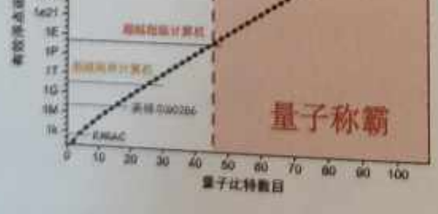
图 9

非常有意思的是，我们这个领域是来自爱因斯坦的好奇心，经过实验的进展，逐渐发展出来非常有用的技术。那么随着自由空间量子通信的发展，我们又可以反过来做一些基于空间量子实验平台的物理学基本原理检验。我们都知道相对论和量子力学一直都没有很好地统一在一起。尤其是广义相对论，时间和空间一直没有量子化。有些理论告诉我们，在极其微小的尺度下，有普朗克长度、普朗克时间，那么到了如此微小尺度之后，我们的时空是光滑的呢，还是像光子那样一份份不连续的呢，这个就不清楚了。所以有些理论叫量子引力理论。比如在2009年有篇*Nature*的文章谈道，如果这个量子引力理论是对的，到了小区间的时候，时空就不再光滑了，那么光子在不光滑的时空中飞行的时候，就像它在真空

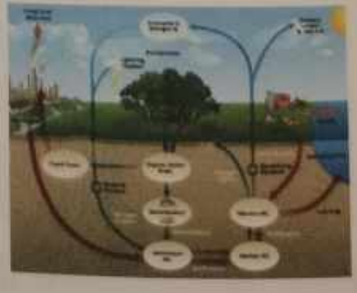
中飞行一样也会有“色散”，就是不同的频率有不同的速度。如果光经过很长距离的飞行，速度的不同会使得到达时间有微小的差异，就可以用来判断这个理论到底对不对。另外，因为时空不光滑以后，光子的极化可能有些微小的、随机的极化扰动，如果测出来以后可以用来判断量子引力理论到底对不对。所以非常有意思，从好奇心出发，通过理论和技术，现在又可以向好奇心前进了。此外，我刚才讲到的量子力学非定域性的检验，这个故事其实并没有结束。那么未来的发展方向，我们希望能够进行30万公里的量子纠缠分发，就是比方说一个宇航员在天宫2号上，一个在月球上。在这种情况下，你用眼睛盯着然后再来做实验，再来看这个量子非定域性，如果还是大于2的话，那么这才算真正完成了量子力学非定域性的检验，这个故事才能结束。完成这个任务还需要若干年，我觉得不一定我能够完成，可能需要在座的各位加入了。

在量子计算方面，我想可能在5年左右我们就可以达到100个量子比特的纠缠了。那时候，它的计算能力，就可以在某些特定问题的求解上，比现在全球计算能力的总和大100万倍。所以量子计算是如此的强大，你在一个小小的实验室里做出一个东西来，它的计算能力就可以比全球计算能力的总和大100万倍（图10），心中还是非常激动的。现在，很多国家和地区，很多科研机构和高校，包括我们中国科大，都希望在竞争当中能够在第一方阵。目前我们还是第一方阵。我们希望，不敢说全面领跑，但至少还要在第一方阵里继续跑下去。这是非常重要的。

量子计算与模拟的未来展望



- 数百个量子比特的相干操纵，对特定问题的求解超越经典超级计算机，实现“量子称霸”



- 量子模拟应用于揭示高温超导、新材料设计、人工固氮等重大问题的机制，并指导相关产业
- 研制具备基本功能的通用量子计算原型机，探索在密码分析、大数据分析等重大问题方面的应用

图 10

另外，在量子精密测量方面，我们会有原子陀螺仪、原子重力仪、磁场精密探测、激光测风雷达等各方面的研究（图11）。

图 11

那么更远的未来我们还想做些什么呢？在这里我愿意跟大家分享一下。1609年，开普勒给伽利略写了一封信，当时他就讲，“应该建造适合飞向神圣天空的船与帆，然后也会有这样的先驱者，面对无边的太空，他们毫不退缩。”在他们这封信将近350年之后，1961年4月12日，人类首次进入太空；在360年之后，1969年7月20日，人类首次登月。那么我们说，1997年，我们首次实现量子隐形传态，十年之后可以传送两个粒子的状态，再10年之后，可以传输1000公里。那么是不是在将来，我们可以用这种量子隐形传态来实现星际旅行呢？这个真的是非常期待。为什么你要这样想，如果你把人加速到光速，太困难了，需要几乎无限的能量，把整个地球的能量全花掉都不行，没办法做到。那么你用那种普通推进器把你往前推，也不行。为什么呢，你还没飞出太阳系，就已经老死了。那么也许有这样一种很好的方式，我们真的能够在很遥远的地方探索宇宙。我觉得我们也希望将来会有这样的机器，当然造出这个机器可能需要很长的时间，可能光靠你们都不行。另外，还有一个我觉得可能是近一点的。大家觉得人工智能很可怕，人工智能的到来会不会把我们人类给毁灭？其实现在我们不用担心，现在的人工智能、经典计算机都是决定论的。就是每台计算机本质上都是可以把它的信

息给拷贝出来的，所以我有两台计算机，买了两台iPhone，如果里面装的所有软件都一样，所有的微信 message全都一样，结果你就区分不了了。又比如我前面讲的量子隐形传态，我要从北京传到合肥来，那么是不是搞出两个潘建伟来了，那就麻烦了，我的孩子就不知道叫哪个人爸爸了，那就有伦理问题了。但是量子力学的测量原理告诉我们，要把潘建伟从北京传到合肥来，在北京的那个潘建伟一定要还原成一些原始的东西。所以这个时候我还是独一无二的，从这种意义上讲，我们真正的物质体系，跟大家讨论的经典计算机、经典人工智能机器人，是有很大区别的。所以，现在我们对我们自己的大脑目前是远远没能理解。不用说我们的大脑，连一个原子的状态，在原理上来讲，都不可能精确复制。但量子力学第一次把观测者的意识，就是我们的consciousness，与我们物理世界演化结合起来了。例如这是《新科学家》封面的文章，说*Your Quantum Mind*。还有位物理学家，他是霍金的好朋友，也是黑洞方面的权威，叫彭罗斯。他写过一本书就叫《皇帝的新脑》。他认为量子力学是首次跟意识的产生联系在一起的。也许量子计算与我们人类大脑的思考方式是紧密相关的。所以也许对这方面的研究，能回答人为什么会有意识。

最后做一个总结，我引用一下黑洞的提出者惠勒的观点，他说，我们这个宇宙本来是毫无生机的，后来慢慢演化出星球，进化出我们人类，万物之灵，然后用我们精巧的大脑和眼睛回过来看我们这个宇宙。所以，我们研究物理学、自然科学，我们活着干什么，很大程度上就是希望能够对我们这个有趣的世界，做一个探索。

谢谢大家，我就讲到这里！