姚期智：做研究最好的方法是提出深刻、大胆和关键性的问题

女士们，先生们，我很高兴来到这里。首先我要说，获得京都奖是一种莫大的荣幸。了解了历届获奖者和他们的辉煌成就后，我为自己被认为值得与他们齐名而深感谦卑，也很高兴和荣幸在这里发言。

今天，我想谈谈我的成长经历，如何进入计算机科学领域，以及一路走来的旅程。
更详细地，我将从我的背景开始，讲一讲我小时候对物理学的痴迷，这后来促成了我选择了第一个职业，然后，我会讲到我是如何偶然转换领域并成为一名计算机科学家的。之后我会简单介绍我的研究工作、我所思考的问题以及它们为什么有趣。
结束之前，我还要向几位对我的生活和工作产生重大影响的人致敬。
1946 年，我出生在中国上海。不久后，我的家人搬到了香港，然后又搬到了台湾。我在一个幸福的中产阶级家庭长大，有慈爱的双亲和两个非常亲密的兄弟/姐妹。我从小深受中国传统价值观熏陶，特别是对文化和学习非常重视。令我和我父母欣慰的是，我是一名优秀的学生，学生时期一直是名列前茅。
我记得我小时候喜欢数学、科学和历史。对历史人物着迷，是因为他们表现出不同寻常的勇敢和智慧。
像伽利略和牛顿这样的科学家，他们也是我心目中的英雄，因为他们的才华以及为自己的信仰挺身而出的勇气，让我大为震撼。我梦想有一天自己也会成为这样的人。

高中三年级，我偶然发现了亚瑟·爱丁顿爵士关于相对论的笔记副本，其中给出了相对论最生动、最简单的推导。

大致如下：

实验中，我们已经知道光具有恒定的速度。从这一事实，我们可以巧妙地推导出我们熟悉的时间概念不可能是一个绝对普遍的概念。而长期以来，这一点是每个人都认为理所当然的事情。
这个论点给我留下了深刻的印象。我发现，物理学可以像侦探故事一样吸引人，而且比“福尔摩斯”中任何聪明的情节都更具想象力。这令我深受鼓舞。

于是在 1963 年，我在大学选择了主修物理。

不久之后，理查德·费曼的物理学讲义发表。传说加州理工学院想从根本上重组他们的物理学大一课程，费曼同意这样做，条件是他只教一次。由此，传奇的三卷本物理学讲义《费曼物理学讲义》诞生了。

这个系列讲义让我大开眼界。难以解释的高级概念，结果其证明只用初级数学就可以解释和推导。这真是令人印象深刻，让我看到了物理学的深度和美妙。

事实上，这是我第一次觉得自己真正理解量子力学的原理。30 年后，当我开始从事量子计算领域的工作时，费曼对量子现象的解释在我看来仍然是最有启发性和最有用的解释。这让

我坚定下来，决定在大学毕业后继续在物理学深造。

1967 年，我大学毕业后服了一年兵役，之后前往哈佛大学攻读物理学研究生。1972 年，我在 Sheldon Glashow 教授的指导下获得了物理学博士学位。最终我成为了真正的物理学家，但这并没有持续多久。

1973 年，当时我在麻省理工学院攻读博士学位的妻子 Frances 向我介绍了“算法”。
算法这个词今天已频繁出现在日常生活中，但在当时，对大多数人来说，这是一个非常陌生的词汇。当时，我接触到 **Knuth 教授编写的《计算机程序设计艺术》**的早期草稿。这是一本很有名的关于算法的书，一部了不起的杰作，它介绍了一门引人入胜的新科学。

阅读后，我开始不断思考书中提出的研究问题，深陷其中而无法自拔，以至于我很快就辞去了物理学博士后的工作，转而全职攻读计算机科学研究生。

我记得我母亲当时很担心我，因为我似乎放弃了这么多年的物理工作，但我的妻子非常支持我，所以我成为了伊利诺伊大学的计算机科学研究生。非常感谢 CL Liu 教授愿意接受我。
接下来，我将讲述我的工作。

最初，我专注于解决算法中现有的开放问题，例如最小生成树、B 树等。但毕业后不久，我开始对开发计算机科学的新框架和新理论产生兴趣。
几十年来，我有机会在几所一流大学工作。我在伯克利、斯坦福度过了 10 年，随后在普林斯顿度过了 18 年。2004 年，我加入了清华大学，直至今日。
在每个时期，我都在做一些不同的事情。很有趣的是，我在不同时期关注的主题，它们与时代的变化和计算机科学作为一门学科的发展，以及身处的大学环境都有很大关系。
接下来，我想要介绍三个主题，极大极小算法(min max complexity)，通信复杂度(communication complexity)，以及密码学和 MPC。
我发现做研究最好的方法是提出深刻、大胆和关键性的问题。如果你能提出好问题，那么就一定会做好研究，得出对学术界来说实用且有重大意义的结论。
现在我将对每个主题的主要问题及其重要性进行讨论。
第一个是 1977 年提出的极大极小算法问题。它在我心中有很特殊的位置，因为这是我第一次提出了自己的研究问题，并找到了很好的解决方法。我们知道，算法本质上和食谱很像。例如在烹饪中，食谱会告诉你每步的步骤，例如放 3 盎司盐或几克肉。
20 世纪 70 年代中期，一种新的算法引起了人们的注意，即“随机化算法”（Randomized algorithm）。这种新算法结合了随机移动（stochastic moves）。如果用烹饪来比喻的话就是，不明确告诉你有放两勺盐的步骤，而是让你用扔硬币决定是放两勺盐，还是放一杯红酒。
因此，对于传统的思维方式来说，这看起来是一种疯狂的做事方式。但在 20 世纪 70 年代，人们已经证明以这种方式执行算法是有优势的，在某些情况下，它们会产生一些令人惊叹的结果。但人们还无法理解这些算法的局限性。
因此，这让我产生了一个问题。到底哪算法个更好？是当时刚刚提出的随机化方法，还是用传统的方法观察数据分布，并在执行过程中调整呢？
一旦用这种方式提出了这个问题，那么就出现了一种令人惊喜的联系，让人们可以对随机化算法有了很多的了解。
当把随机化算法与传统分布方法进行比较时，可以将其视为随机化算法和数据之间的博弈。

算法（可以根据数据）选择如何随机移动，而数据可以选择分布方式，从而使算法的运行变得更加困难。
在博弈论极大极小原理的作用下下这两种方法恰好达到了它们的极限。
这个联系给出了我们想要证明的定理，也就是说事实上这两种方法是相同的。这为理解随机化算法提供了新途径。在现在，这种在当时还算新颖的算法已经成为许多密码技术和人工智能算法的默认模式。
人们想了解随机化算法的局限性是有原因的。因此，在 40 多年的时间里，我发现的算法仍然被许多研究人员用来来解决他们的问题。
第二个主题是我在 1979 年提出的通信复杂性。
让我先解释一下这个数学问题，爱丽丝和鲍勃是两个在不同地点的人，他们各自持有一条 n 个比特的数据，比如 x 和 y。我们想要解决的问题是，假设它们想要联合计算某个量 f，它们之间需要通信多少比特，这就是这个函数的通信复杂度。
当然，这取决于你在计算什么函数，例如，要计算这两个整数的和是奇数还是偶数只需要两个比特的通信。每个人只需告诉对方它是偶数还是奇数，然后他们就可以知道答案了。
另一方面，如果你想计算 x 是否大于 y，那么它将需要 n 比特。你需要把整个字符串从一个人发送给另一个人才能解决这个问题。
更深一层的是，你必须意识到并证明，没有比这种方式来解决这个问题更好的方法了。一般来说，这是一个相当困难的问题。如果我给你一个关于 F 的计算复杂性，那需要相当深入的数学分析才能完成。
考虑通信复杂度的原因是，计算模式在 20 世纪 70 年代末发生了很明显的变化。从之前大家都熟悉的大型计算机，逐渐转向我们现在熟悉的计算机网络。人们对以分布式方式解决问题感兴趣，许多人愿意协作解决问题。
因此，这意味着我们必须把过去的计算模型调整为网络模型。在这个新的世界里，通信成本通常是很高的，因为我们必须移动数据。
因此，我刚刚向你们的介绍的通信复杂度的概念就是为了模拟和反映这种变化。自从该模型被提出和分析以来，通信复杂性在从芯片设计到数据流的各个领域都得到了广泛的应用。
我要讨论的最后一个话题是关于密码学和 MPC。
1982 年，我写了三篇论文，这些论文对现代密码学做出了重大贡献。这三篇论文涉及 Dolev-Yao 威胁模型、伪随机数生成算法（pseudo random number generation）和安全多方计算（MPC）。今天我只谈最后一个问题。
MPC 是一个加密概念，使我们可以对加密数据进行计算。如果您使用 MPC，就有可能让多个数据库在不泄露它们自己的数据的情况下进行联合计算。也就是说，我们可以在看不到数据的情况下共享数据。
让我用一个例子来解释一下这一点。我将引用在论文中提到的著名的亿万富翁的例子。
两个百万富翁，爱丽丝和鲍勃，他们希望在不透露任何数据信息的情况下知道谁更有钱。所以爱丽丝有 X 百万，鲍勃有 Y 百万。所以数学问题是，他们想要彼此交流来知道 X 是否小于 Y。问题是，是否有可能进行一次对话，让双方在不知道对方数据的情况下又知道谁更富有呢？
直觉上来说你会认为这是不可能的。我怎样才能在不透露任何一方任何信息的情况下找出谁更富有呢？如果你想几分钟你就会意识到，如果采用 1982 年的信息安全定义，也就是香农的信息论（ Shannons information theory），那确实是不可能的，你可以证明在那个模型下是不可能的。
但我认为，需求是所有发明之母。如果真的有需要的话你肯定会想尽一切办法。所以，如果

你跳出框框去思考，事实证明这是可能的。
说到跳出框框，我们的意思是需要丢弃香农在这种情况下规定的非常死板的条条框框，然后把艾伦·图灵纳入其中，我不会对此说太多。但事实证明，如果你把安全定义放宽一些，让它变成一个务实且足够好的标准，那么这个问题事实上是有解的。
具体地说，我用“乱码电路”（garble circuit）实现了解决方案。
在过去近 40 年的发展中，它在硬件和算法方面取得了进步，现在几乎是可行的。而这方面的研究工作也很多，准备在金融科技、数据交易、药物研发等方面开展工作。
目前我还有一些其他的研究课题，就不一一详述了。我的课题包括：革命性、有望实现指数级增长的量子计算技术；可以用博弈论来解决经济问题的拍卖理论；人工智能，这项技术见证了 AlphaGo 等机器学习算法取得的令人难以置信的壮举，但成功的原因仍然是个谜。
所有这些都是非常有趣的新领域，而且还在持续发展中。如你所见，我研究过很多不同的课题。这些丰富多彩的课题，实际上不仅反映了我个人的喜好，也反映了半个世纪以来信息科学的蓬勃发展，以及我们今天所看到的日益增长的跨学科联系。
最后，我想对我人生中遇到的人说几句话。
在这些年里，作为一名计算机科学家，我有幸遇到了许多才华横溢的人。我非常幸运地遇到了两位给我巨大灵感的导师，Glashow 教授和 Knuth 教授 。
Glashow 教授是我在哈佛大学的物理学博士导师。他是最先预言存在 Charm Quarks 这种粒子的人之一，也是这种粒子最积极的倡导者。
我从 Glashow 教授那里学到，在科学上你必须大胆，你必须坚持不懈地坚持你的信仰。
我从他身上学到的另一件事是，数学和物理是不同的。对于物理学家来说，最重要的是能够找出物理现实的真相，而不是坚持精确的数学论证。我认为这种务实精神对我以后的研究有很大帮助。
还有一件事是我从 Glashow 教授那里学到的：生活应该是有趣的。
1971 年春天，作为一个年轻的学生，我跟随他去法国马赛的 CNRS（Centre national de la recherche scientifique，法国国家科学研究中心）休假。这是一个多么神奇和迷人的城市，那也是我第一次来欧洲。那年夏天的晚些时候，他带我去了意大利西西里的一个暑期学校。这是一次非常美妙的经历。Gladshow 教授给我上的这一课让我明白，生活的乐趣和对知识的追求可以兼而有之。
现在，我想提一下 Knuth 教授。正如我之前所提到的，当我读到《计算机编程的艺术》时，它几乎改变了我的生活。在这本著作中，他确实开创了一个新的研究领域，也激励了一代又一代新的计算机科学家。例如，通过阅读他的书，我开启了自己的计算机科学生涯，并解决了一些他在书中所阐述的问题。
后来，我有幸成为他在斯坦福的同事。众所周知，除了数学和计算机科学之外，Knuth 教授在许多方面都很在行。他是一位才华横溢的管风琴演奏家。他还是一位作曲家、小说家等。他多才多艺，且真诚大方，总是在别人身上看到好的一面。
总而言之，虽然经历了一些曲折，但我在计算机科学领域还是度过了一段美好的旅程。我发现，一开始就走错方向可能并不是什么坏事。事实上，早期的物理训练至少在两个方面对我有很大帮助。
首先，我了解到好的理论在物理学中是什么样子的，比如经典的相对论和量子力学。在之后提出计算机科学的理论时，这对我有很大的帮助。
我从物理学中受益的第二件事是它的务实精神。它教会我解决手头的特定问题。不管用什么方法，你都应该根据情况使用、学习或发明解决问题的方法，最终目标是解决问题。
科学是对真理的追求。在这个过程中，我们会发现科学规律和科学的美，提升人类共同的精

神。它还带来了创新，可以改善人类的现状，为未来所面临的挑战做好准备。
我完全同意稻盛和夫基金会（Inamori Foundation）的愿景，即科学和人文应该为人类的进步而共同努力。我很荣幸能获得京都奖，也很荣幸能做这次演讲，与听众分享我的经历。非常感谢。