Shor’s Algorithm

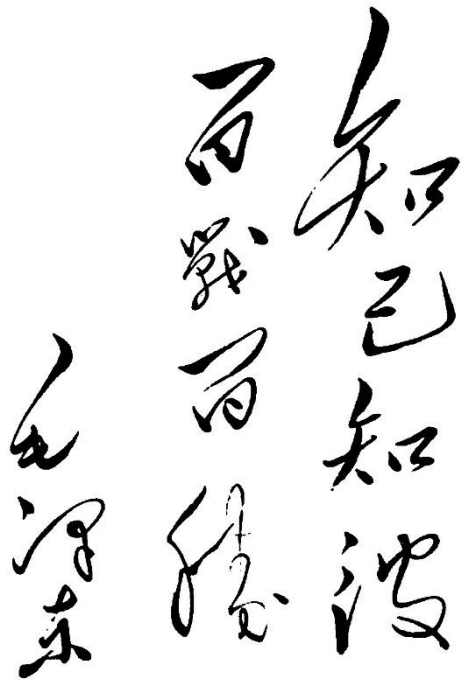
第1讲： 背景介绍

1. 加密与解密

本源量子

本源量子

密码学介绍



知己知彼，百战不殆

在军事，信息的保密被认为是取得胜利的关键因素。

本源量子

密码学分类

古典密码学

现代密码学

计算机时代讨论：现代密码学

本源量子

对称加密

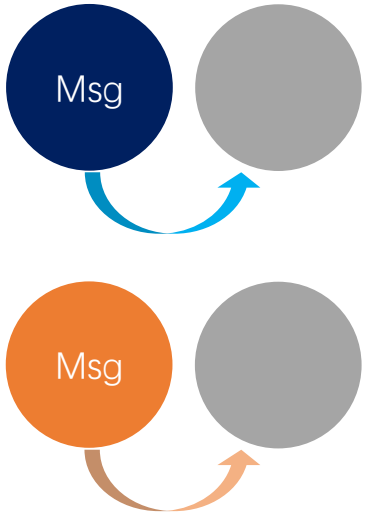
加密和解密用的是同一个密钥，这种加密称为：

对称加密（Symmetric encryption）

本源量子

非对称加密

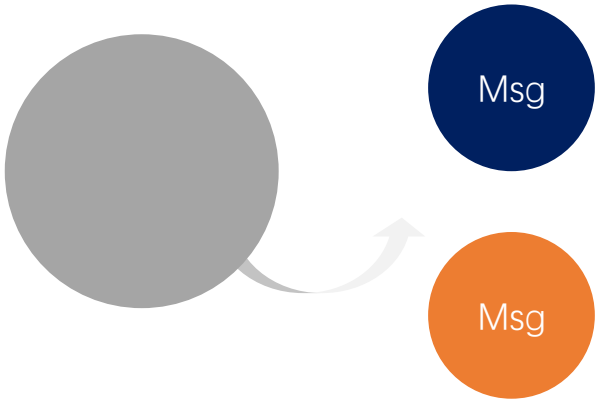
公钥加密



发送方

信 道

密钥解密



接受方

仅仅解密用一个密钥时，这种加密称为：

非对称加密（Asymmetric encryption）

RSA

非对称加密的著名算法是RSA算法，它是一个数论与计算机科学相结合产物。目前，很多加密方式，都采用这个原理。而Shor算法所威胁的正是RSA的加密方式.

本源量子

RSA公开密钥系统背景

- RSA是Internet上的标准加密算法。该方法是公知的，但非常难以破解。
- 它使用两个密钥进行加密。公钥是公开的，客户端使用它来加密随机会话密钥。截获加密密钥的任何人都必须使用第二个密钥（私钥）对其进行解密。否则，得到的是没有任何含义的垃圾。
- 会话密钥解密后，服务器使用它以更快的算法加密和解密更多消息。因此，只要保证私钥安全，通信就是安全的。

本源量子

RSA加密的核心

两质数相乘容易，但是反过来，分解非常困难。

易	$104322269 \times 1998585857 = 208497011393549533$
难	$208497011393549533 = 104322269 \times 1998585857$

2. 量子计算简要描述

本源量子

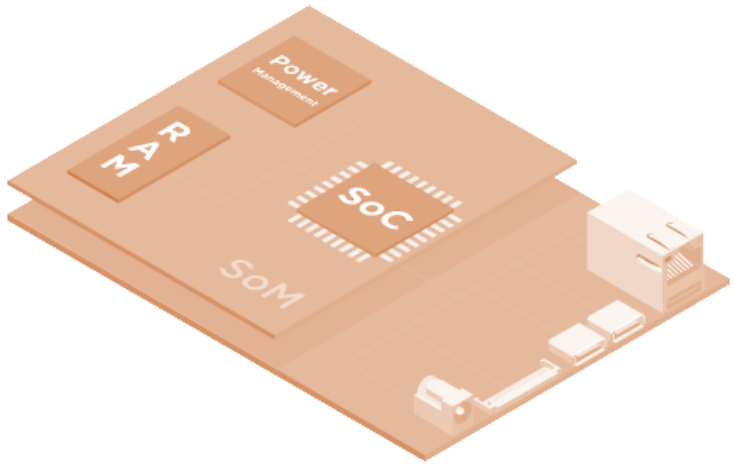
本源量子

计算简述

计算机

- 计算设备，对应了一个具体的物理系统

计算：使用该目标系统的物理特性，来完成信息的处理。



本源量子

量子计算

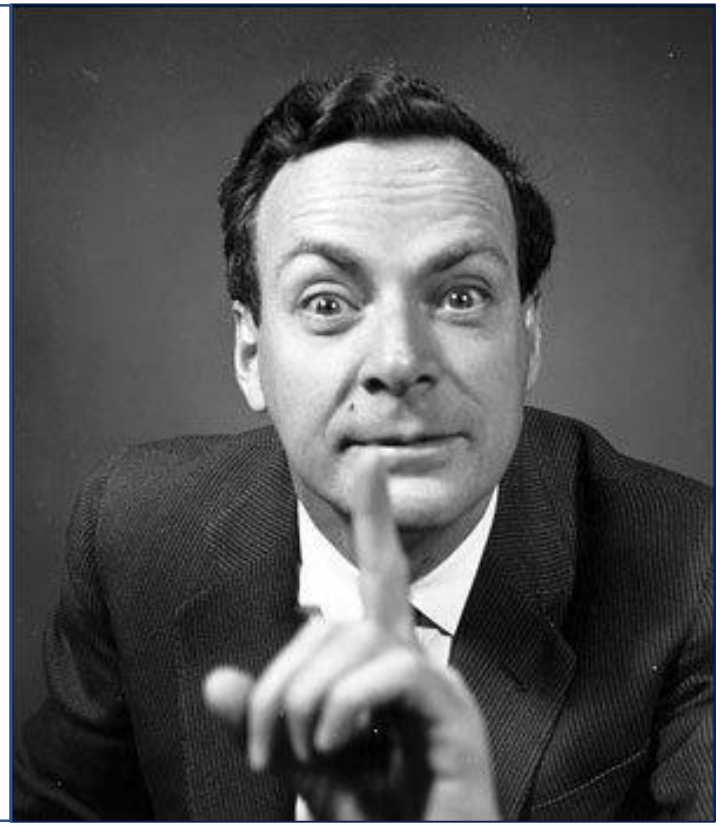
Simulating Physics with Computers

Richard P. Feynman

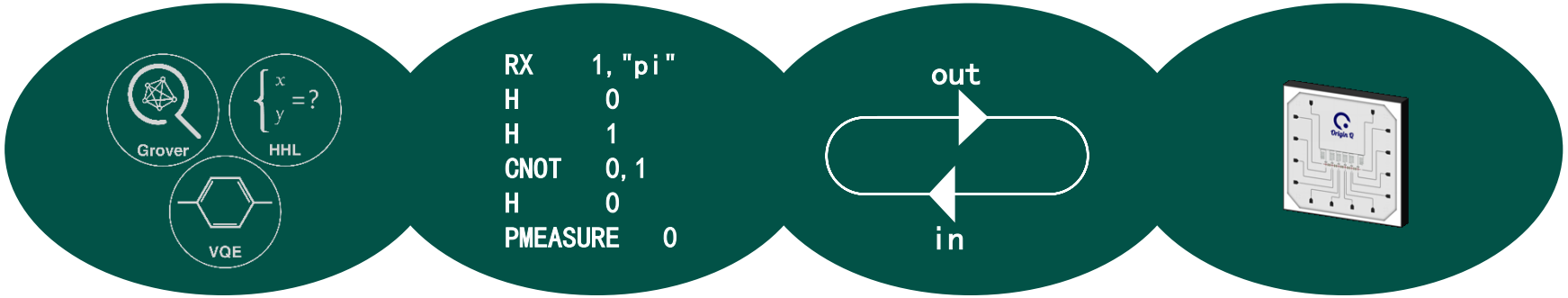
Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

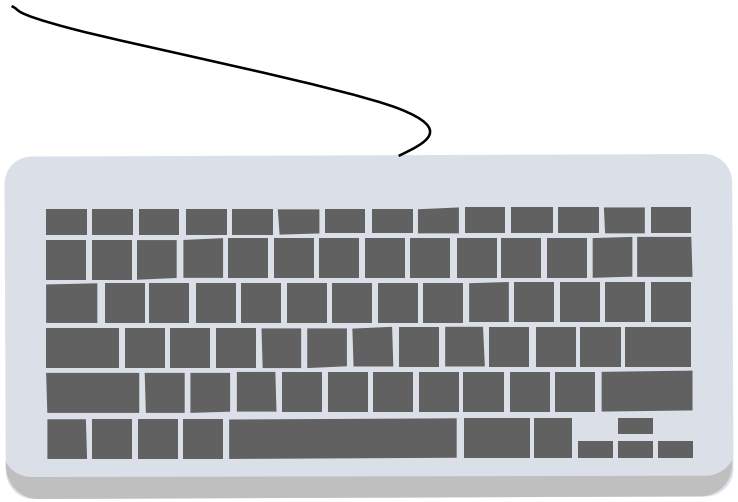
要模拟自然，就需要用**量子计算系统！**



量子编程语言的结构

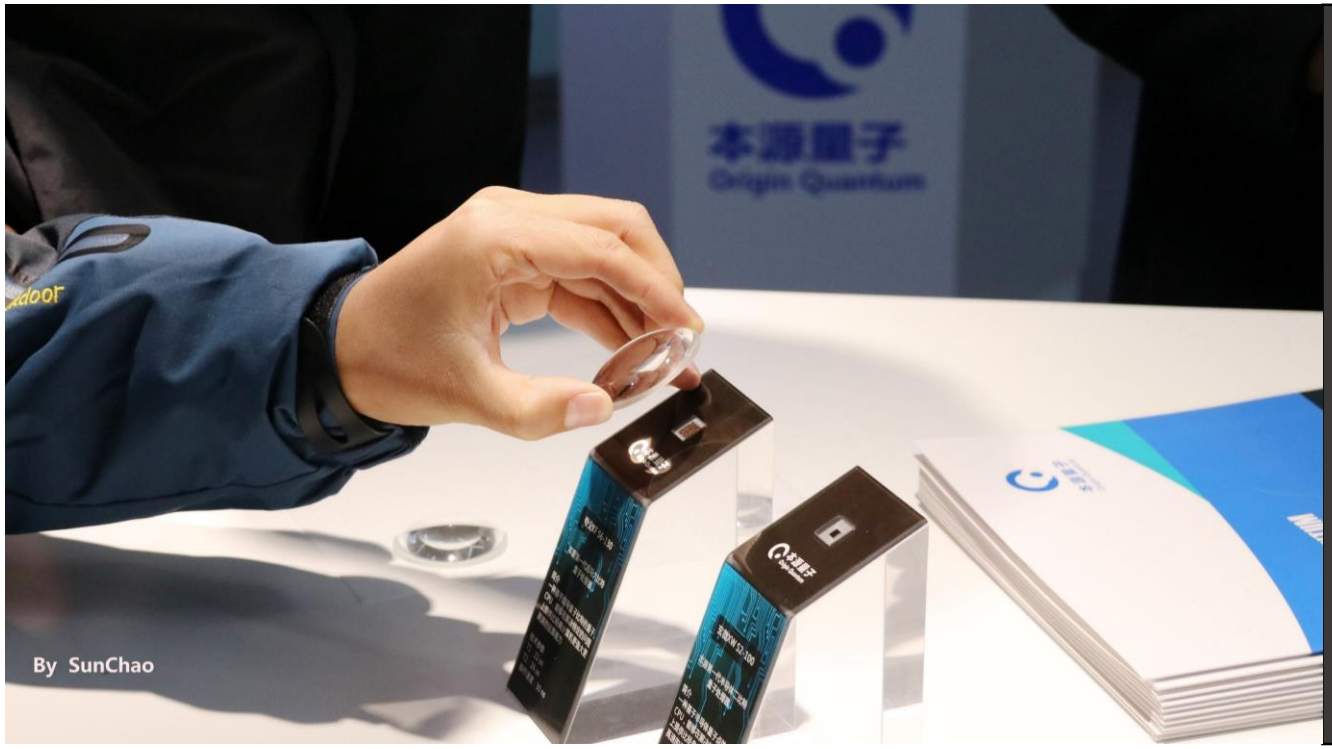


量子算法　　量子指令　　物理指令　　量子处理器



本源量子

量子后端芯片的支持



本源芯片类型：

1．半导体量子芯片

2．超导量子芯片

本源量子

追本溯源 高掌远跖

https://www.originqc.com.cn