

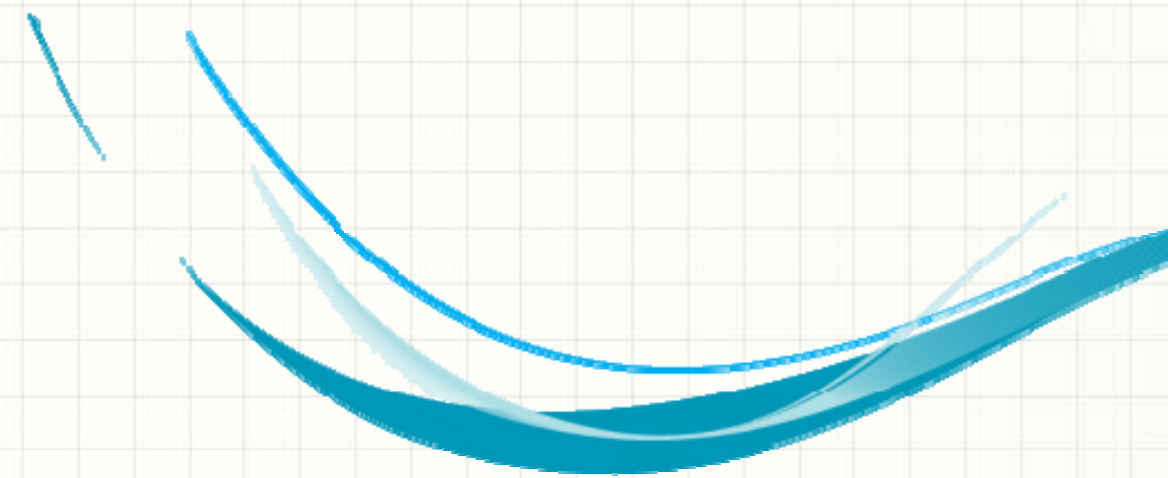


OWASP GLOBAL APPSEC ASIA 2011 (北京市 8-11 Nov 2011)

Daniel Ng, C-PISA

Date/time ??

Profile



吴，清华（丹尼尔）开始于1990年作为计算机程序员的职业生涯，然后对信息和通信技术安全，计算机取证，财务会计与审计千年后的进展。最近，他开始了他在英国有信誉的研究所博士（保安及鉴证）和香港理工大学，后收入作为公司董事在上市实体的一个很好的股票期权。他的兴趣是网络安全，健康信息，Facebook的调查，取证实验室的数字证据标准，网络取证。专业，他是一个委员会的成员，专业的网络安全专家（香港/中国），方正，ISACA中国 - 中国独立私校联盟（C - PISA）的专家顾问，香港特区立法会会议员谭伟豪，亚洲PacificCSSLP传播者，授权培训师。在知识密集型工程的强大影响力，丹尼尔分行到电子学习的主题，特别是移动学习。这项研究是与马来西亚政府MIMOS，本体和语义网的全国性组织。在学术上，丹尼尔在知识管理的强烈与全球行动纲领“3.8毕业，获硕士学位。

Internet Article (through Google)

List of Fellows - The Hong Kong Computer Society

www.hkcs.org.hk/en_hk/intro/lofellows.asp - 頁庫存檔2011年5月26日 – Mr. Ng Cheung Shing. 吳長勝先生. Mr. Ng Ching Wa, Daniel. 吳靖華先生. Ms. Shen Shuk Ching, Susanna. 孫淑貞女士. Mr. Sin Chung Kai, SBS, ...

NG, CHING WA (Daniel) - Overview Program

<https://www.swisscyberstorm.com/speakers/chingwa> - 頁庫存檔30 May 2011 – NG, CHING WA (Daniel) started the career as computer programmer in 1990, and then progressing towards ICT Security, Computer Forensics, ...
[PDF]

Cyber Warfare Prediction

media.hacking-lab.com/scs3/.../SCS3_2011_Weng.pdf - 翻譯這個網頁

檔案類型: PDF/Adobe Acrobat - HTML 版

Daniel Ng (Ching Wa). •. PhD Researcher (KM, Forensics, Surveillance,. eHR, Textile Dying & Colorimetry). •. Corporate Director, CPA (Aust) in listed Family ...

OWASP Global AppSec Asia 2011 - OWASP

https://www.owasp.org/.../OWASP_Global_AppSec_Asia_2... - 頁庫存檔Daniel_ng.jpg, NG, CHING WA (Daniel) started the career as computer programmer in 1990, and then progressing towards ICT Security, Computer Forensics, ...

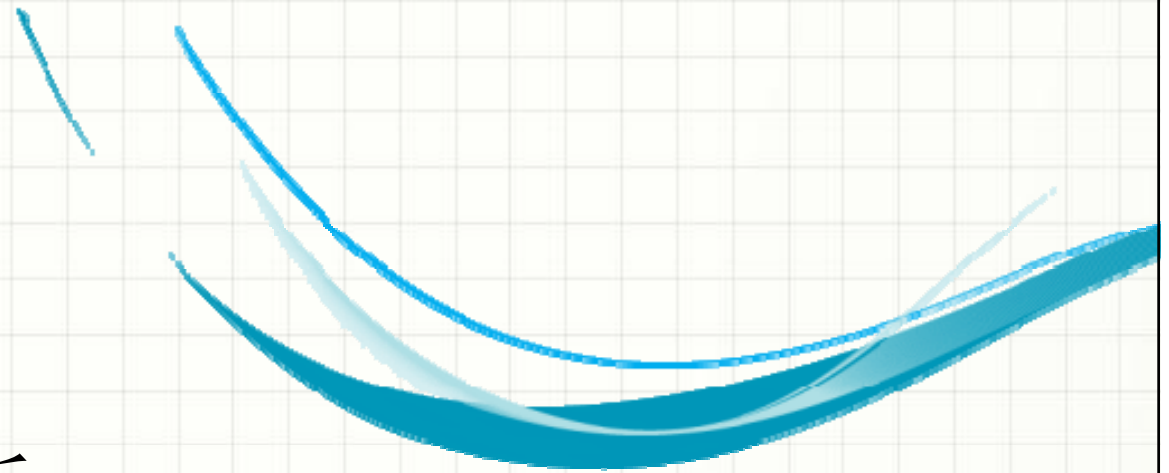
Daniel NG Ching Wa, PH.D | microlearning.org

www.microlearning.org/.../daniel-ng-ching-w... - 頁庫存檔 - 翻譯這個網頁

NG, CHING WA (Daniel) started the career as computer programmer in 1990, and then progressing towards ICT Security, Computer Forensics, Financial ...

研究重点

1. 社会语义
2. 队医经济与创新
3. 存储和转发消息与本体
4. 机斜塔上的特征值
5. 网络编码
6. 隐马尔可夫链与遗传编程
7. GPU的聚类和OpenCL的



加密 - 键的代码页

- 移位字母表

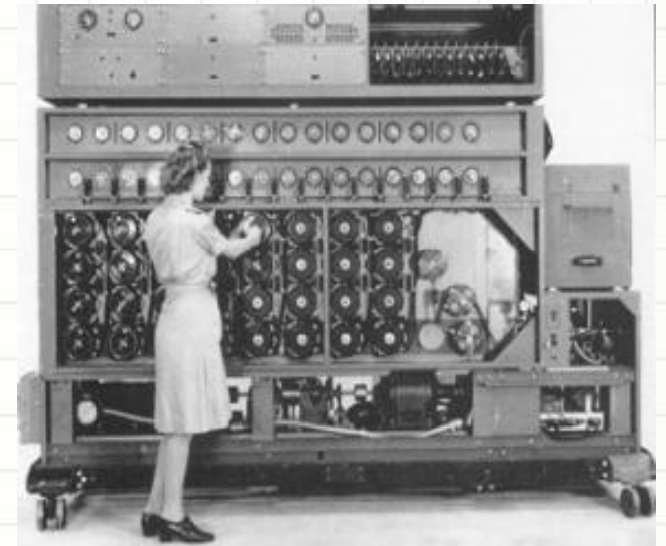
1. 例如凯撒密码 $A = D$, $B = E$, $C = F$
2. 可能永远不会上当的人（除凯撒）
3. 发达国家从16世纪到20世纪中叶的许多更复杂的系统
4. 换人和换位的信件
5. 一些基本上是牢不可破的，通过人工手段
6. 大约1940年由电脑过时

加密 - 键的代码页

谜与人类 - 谜胜!



谜与计算机
- 计算机胜!



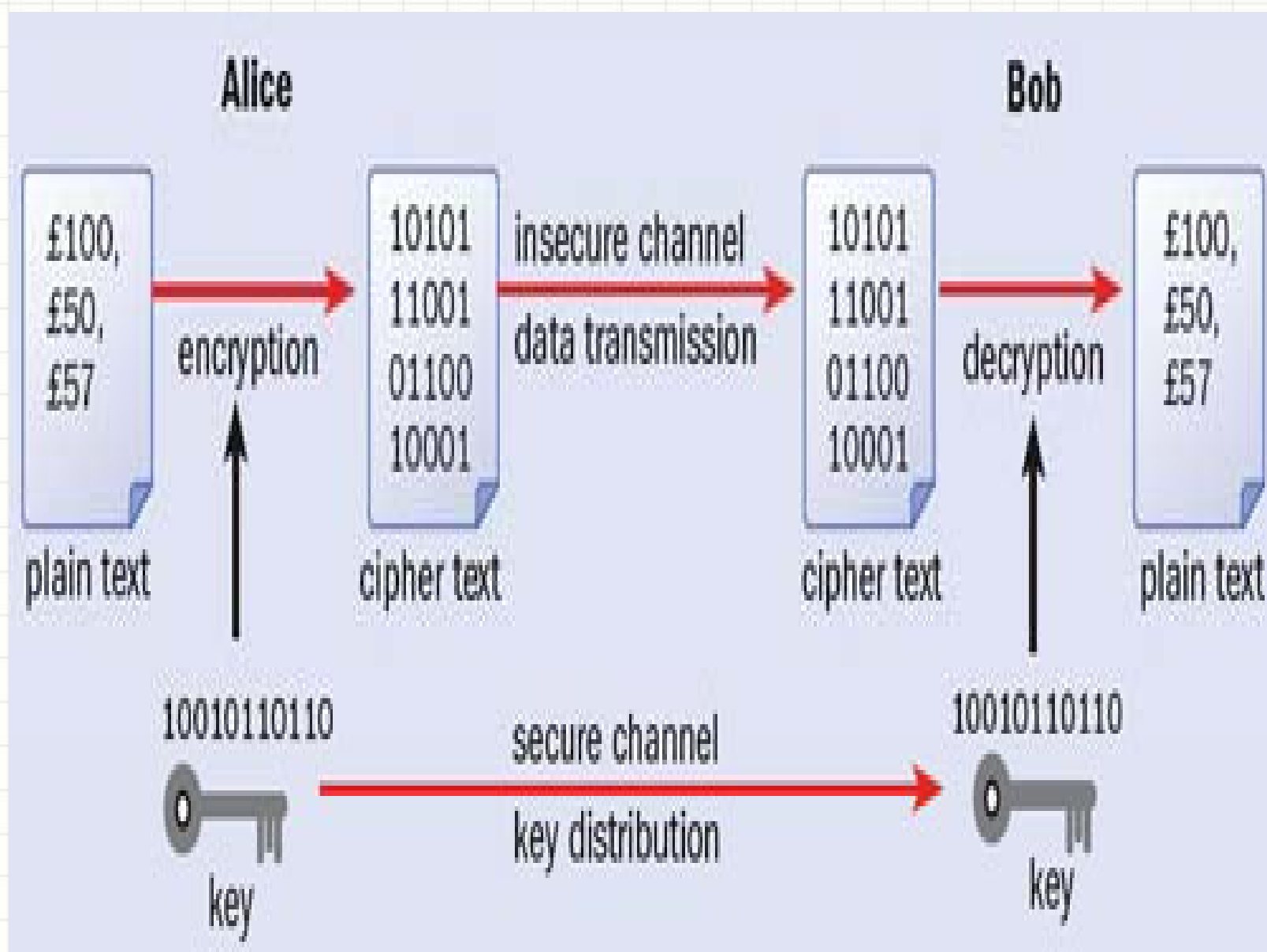
Turing's machine



Desch's machines – even faster

薄弱环节的密码系统

加密 - 键的代码页



加密 - 键的代码页

- 其一：在数学难问题
 - 破坏系统需要解决一个难题的有效算法 - 例如保理业务的大量涌现，离散对数
 - 例如：RSA，厄尔尼诺贾迈勒
 - 在公钥系统使用
 - 缓慢
- 二：信息理论
 - 文本炒重复移位和置换的应用
 - 例如：DES，AES
 - 在私钥系统使用
 - 快速

加密 - 光子水平（但复杂）

RSA
Cryptosystem

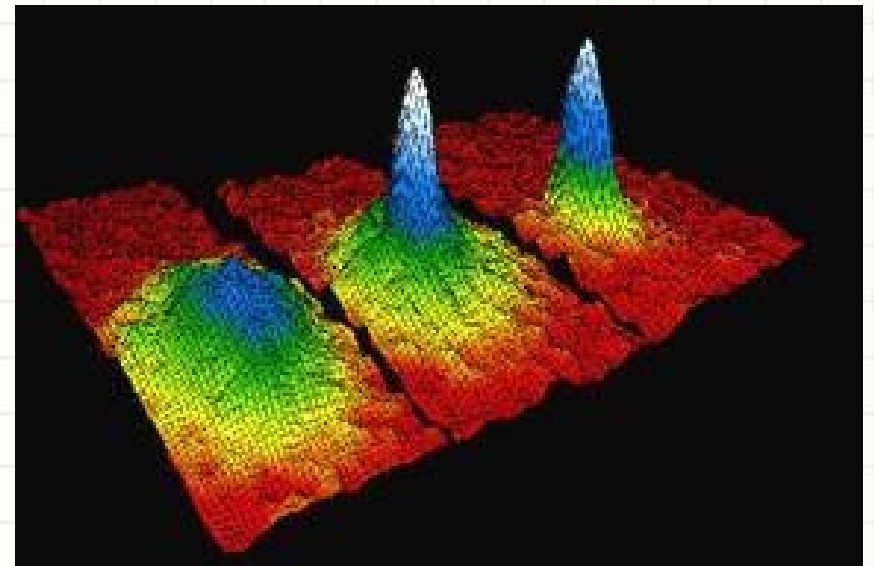
$$C = M^e \bmod n$$

$$d = e^{-1} \bmod ((p-1)(q-1))$$



Earth Simulator

RSA vs. supercomputer: 40 Tflop/s (4×10^{12} flop/sec)
– RSA wins!

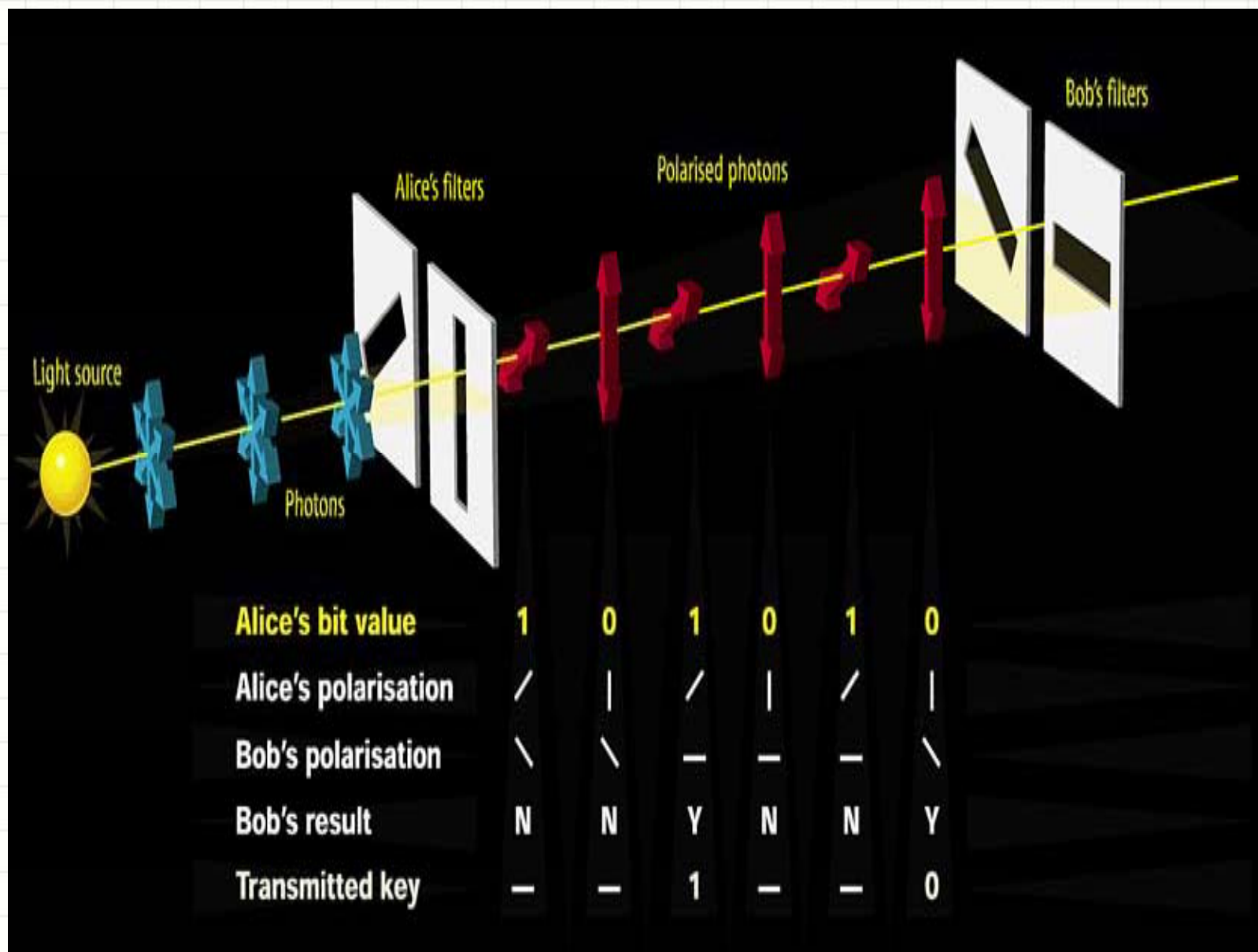


RSA vs. Quantum Computer
– computer wins!

加密 - 光子水平 (但复杂)

Alice transmits 1 +45°	Bob measures with -45° filter	Photons always blocked
	Bob measures with 90° filter	Some photons blocked Some photons pass
Alice transmits 0 +0°	Bob measures with -45° filter	Some photons pass Some photons blocked
	Bob measures with 90° filter	Photons always blocked

加密 - 光子水平（但复杂）





量子加密

快速，复杂，昂贵



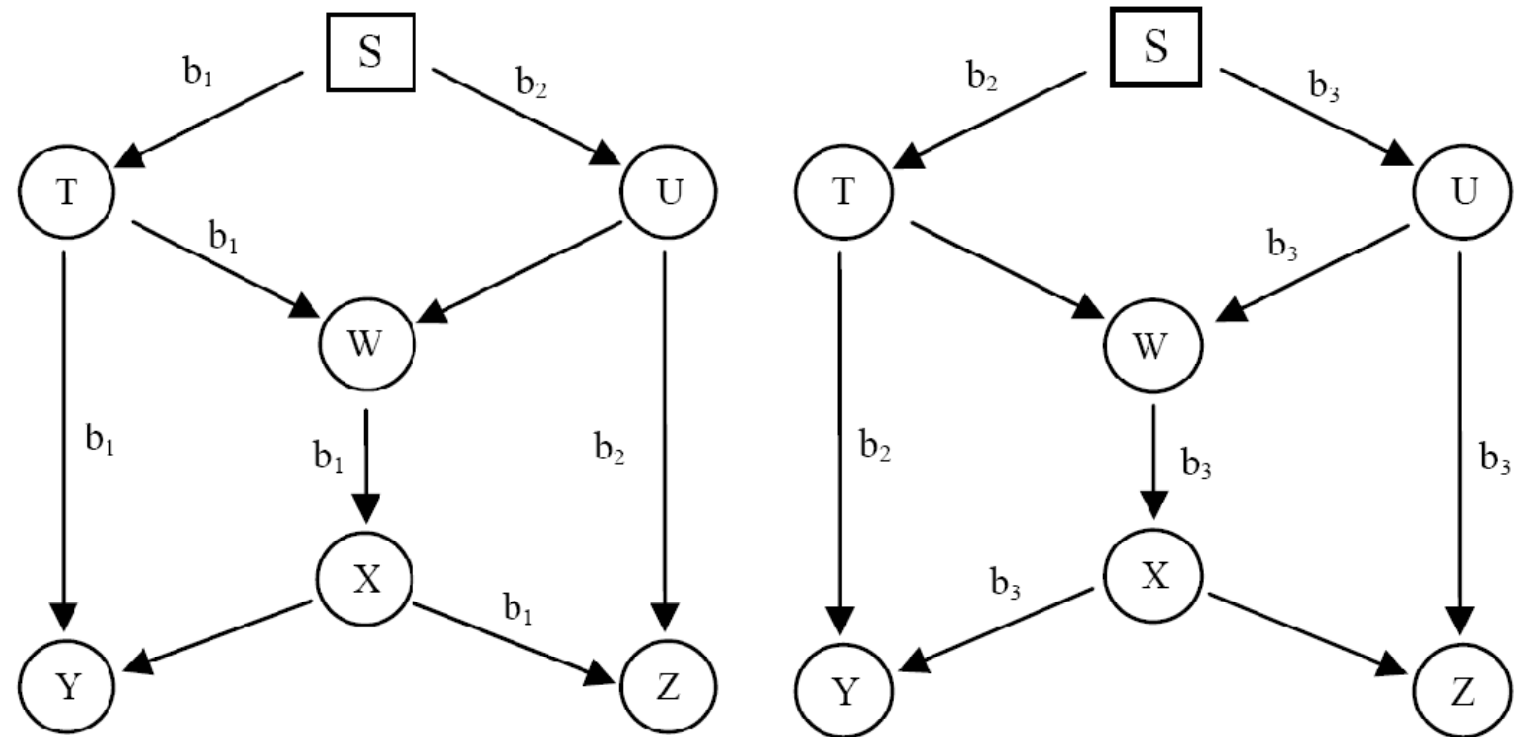
网络编码??



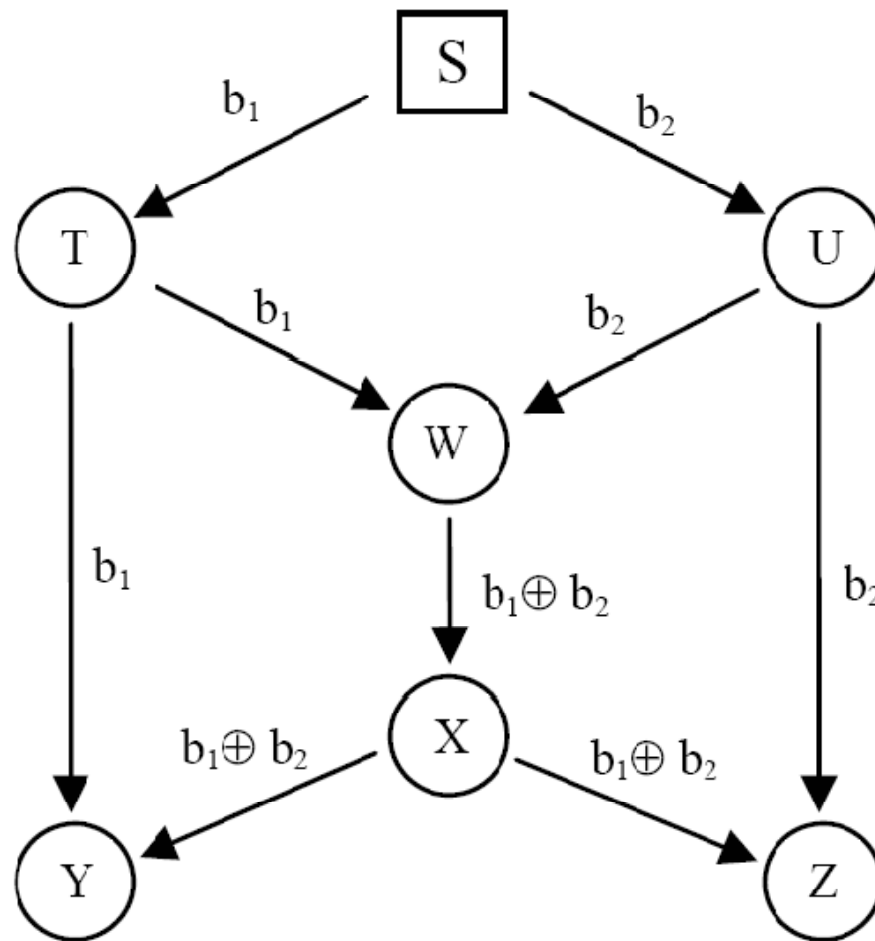
定义

网络编码是一种在网络数据处理技术，
利用介质的特点，特别是
（尤其是广播通信信道）
为了增加网络的容量或吞吐量

- 没有网络编码
- 简单的存储和转发
- 组播率**1.5%**，单位时间内的位

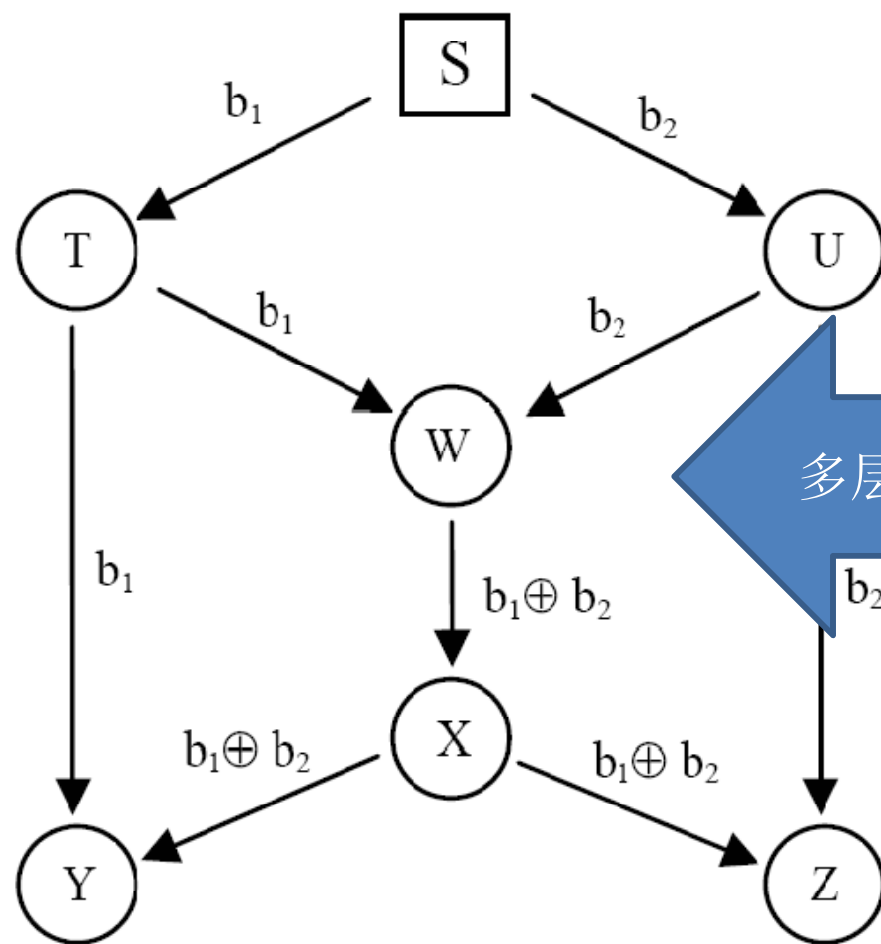


- 随着网络编码
- **X或** 是一个最简单的形式编码数据
 - 2位单位时间内的组播速率
 - 缺点
 - 须事先同意





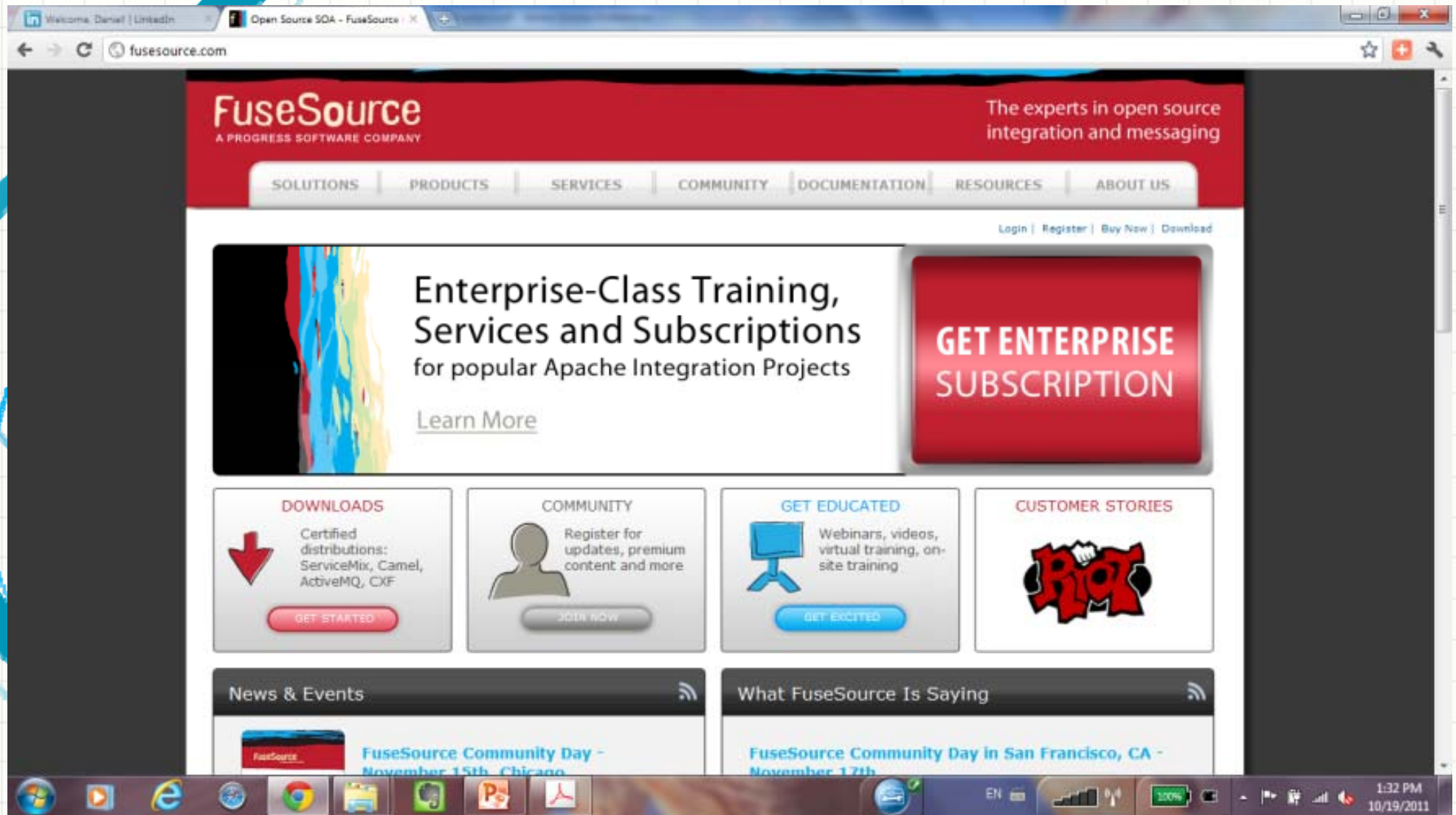
网络编码发
生在光纤和/
或OSI二层。



多层次的XOR加密*

* Engineering of Encryption, Bruce
Schneider

网络编码的原型工具





通过马尔
可夫链的
灾难能力
和准确性

隐马尔可夫链

Used in Kinect (Microsoft) on Motion Command

- ◆ 一个随机序列的马尔可夫属性，如果它的分布是完全由它当前的状态决定。任何有此属性的随机过程称为马尔可夫随机过程。
- ◆ 对于观察到的状态序列（状态是从已知的数据），这将导致一个马尔可夫链模型。
- ◆ 非观察国，这将导致一个隐马尔可夫模型（HMM）。

隐马尔可夫链

Used in Kinect (Microsoft) on Motion Command

◆ 长期“隐藏”

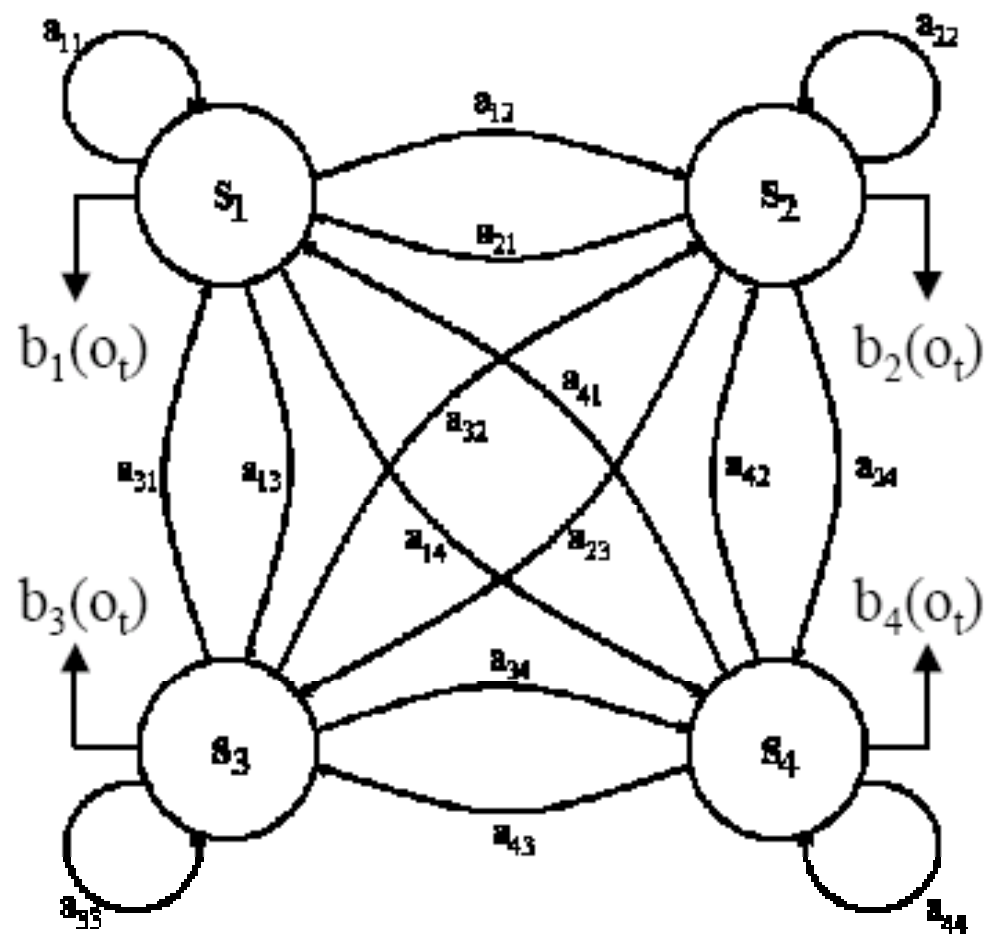
- - 我们只能访问可见符号（观察）
- - 不知道国家的隐藏序列得出结论

◆ 因果关系：概率依赖于以前的状态

◆ 对于任何给定的初始状态转换序列遍历，如果每个国家都访问

◆ 最终或吸收的状态：状态，如果进入，是从来没有离开过

隐马尔可夫链



隐马尔可夫链

- 隐马尔可夫模型（HMM）是一个离散时间有限状态马尔可夫链加上一个马尔可夫链时发出的访问其国家的字母顺序。

状态 (Q): q_1 q_2 q_3 ...

字 (O): o_1 o_2 o_3

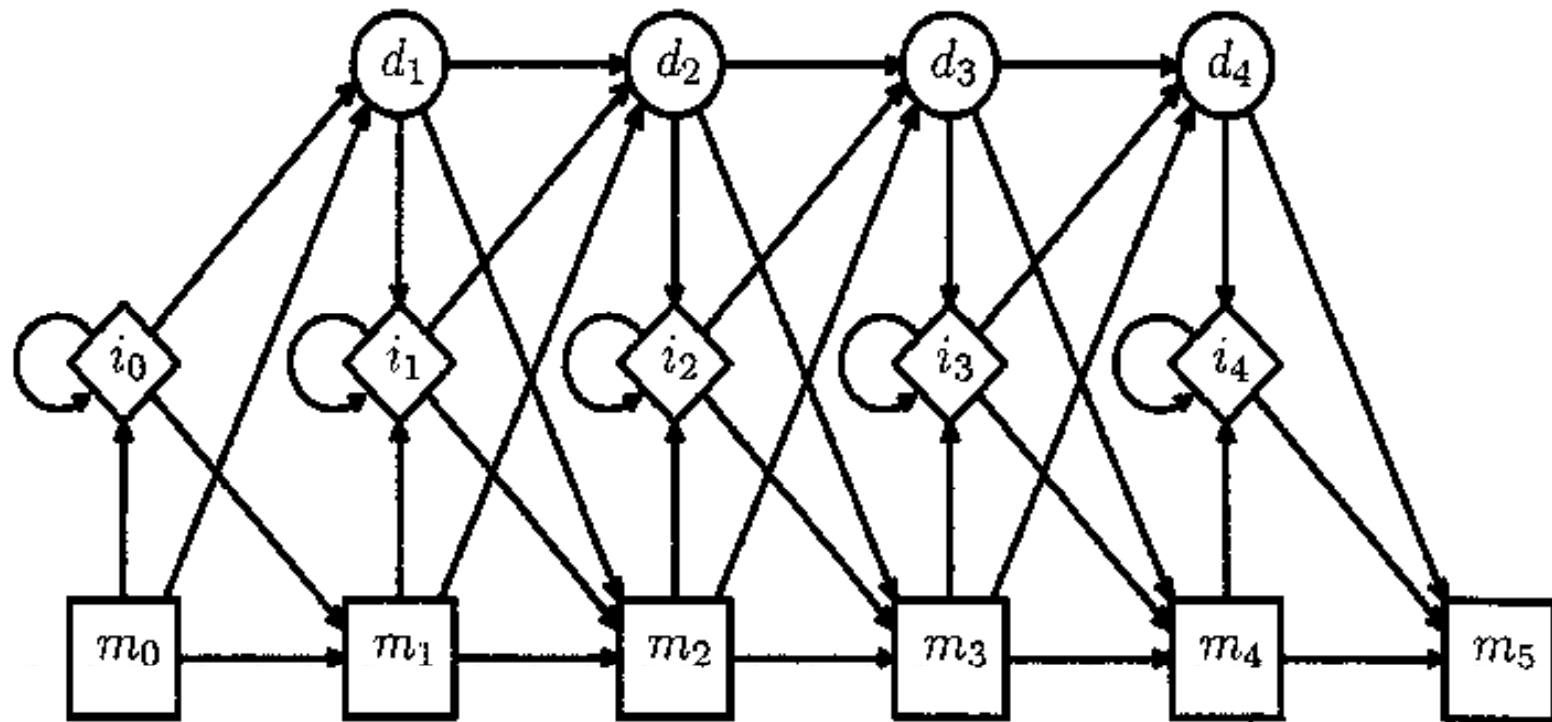
```
graph LR; q1 --> q2; q2 --> q3; q3 --> dots[...]; o1 --> o2; o2 --> o3; o3 --> dots2[...]; q1 -.-> o1; q2 -.-> o2; q3 -.-> o3;
```

隐马尔可夫链

- 蛋白家族建模：
- (1) 构建多序列比对
- (2) 确定一个查询序列的家庭
- 基因发现通过半隐马尔可夫模型 (semiHMM)

隐马尔可夫链

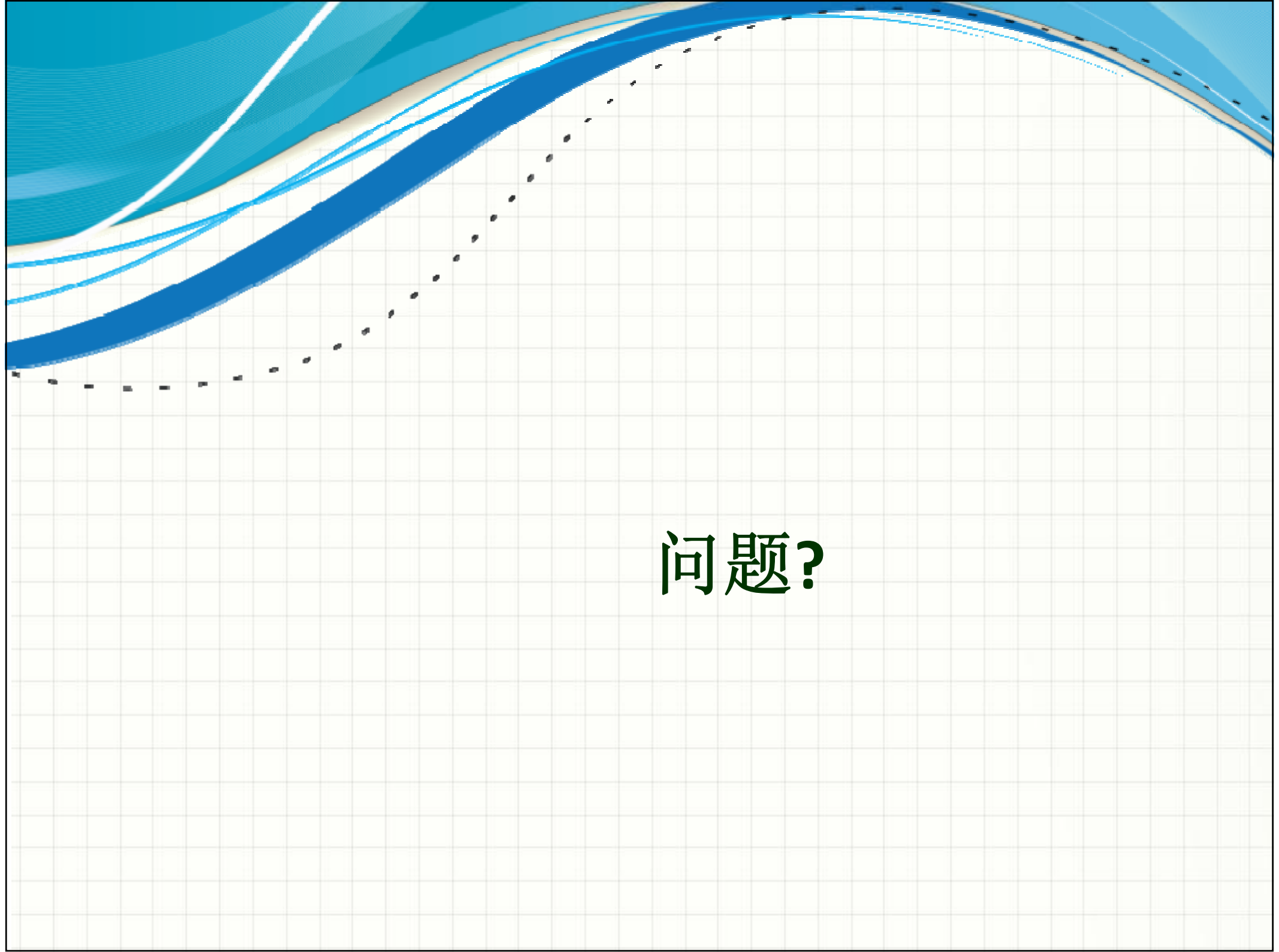
[HMM的序列比对]考虑以下的马尔可夫链基本与一个HMM，三种类型的国家： $\square \rightarrow$ “match”； \rightarrow “insert”； $\circ \rightarrow$ “delete”



概括

- 云安全的数据运动
- 使用标准的硬件
- 打开常用工具，
如Python





问题?