ISC 2017

2017 中国互联网安全大会
China Internet Security Conference

密码技术前沿应用与发展趋势

林东岱

中国科学院信息工程研究所
信息安全国家重点实验室 主任

目录

从信息安全谈起...

二十世纪最伟大的发明是什么？

信息安全风险

- 人们在享受信息技术带来便利的同时也面临着更大信息安全风险
  - 我们的数据在哪儿？
  - 谁在控制它？
  - 谁可接触它？
  - 和谁在共享？
  - 它们怎样被使用？
  - 怎样验证我的数据的所有权？
  - 怎样保护我们的隐私？
  - 怎样保证信息是真实的？
  - 谁在照看我们的利益？

国家安全 社会稳定 经济发展

没有网络安全就没有国家安全
没有信息化就没有现代化

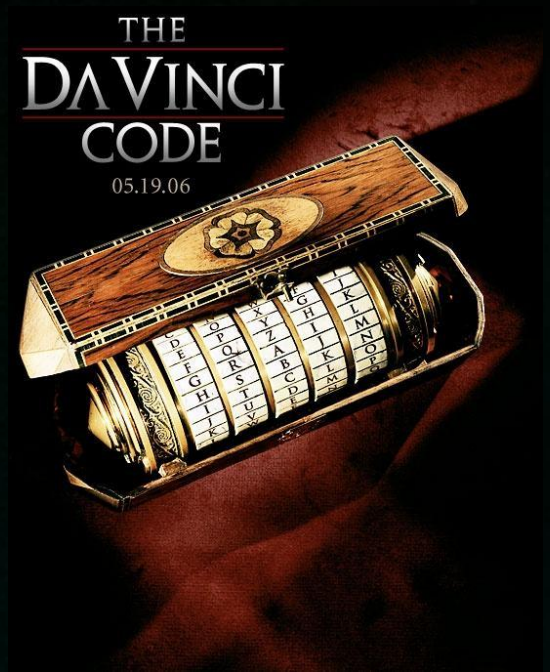
—— 习近平

信息安全的基本要素

- 信息安全的基本要素
  - 机密性（Confidentiality）
  - 完整性（Integrity）
  - 可认证性（Authentication）
    - ✓ 数据源认证
    - ✓ 身份认证

- 密码学是网络空间安全的核心技术

什么是密码学？



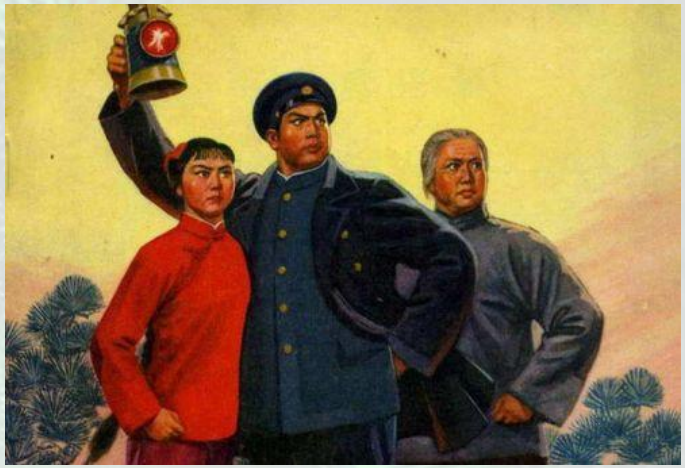
什么是密码学？

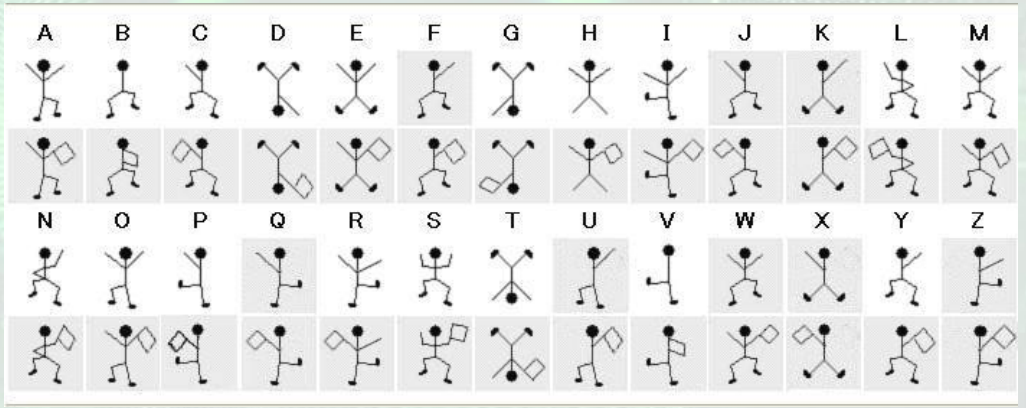
- 经典定义：密码学是研究保密通信的一门科学。研究在不安全的环境中，如何把所要传输的信息在发给接收者之前进行秘密转换以防止第三者对信息的窃取。

- 现代定义：密码学主要研究如何构建能够经受住任何滥用的安全方案，即：在任何恶意企图使它们偏离规定的情况下，该方案仍能维护它所设计的功能（From *Foundations of Cryptography* – O. Goldreich）

什么是密码学？

- 几个实例
  - ✓黑话
  - ✓《红灯记》中的密电码
  - ✓慈禧太后用的漏隔板
  - ✓跳舞的小人
  - ✓……





算法与密钥

$E_{Ke}(M)=C$, $D_{Kd}(C)=M$, $D_{Kd}(E_{Ke}(M))=M$

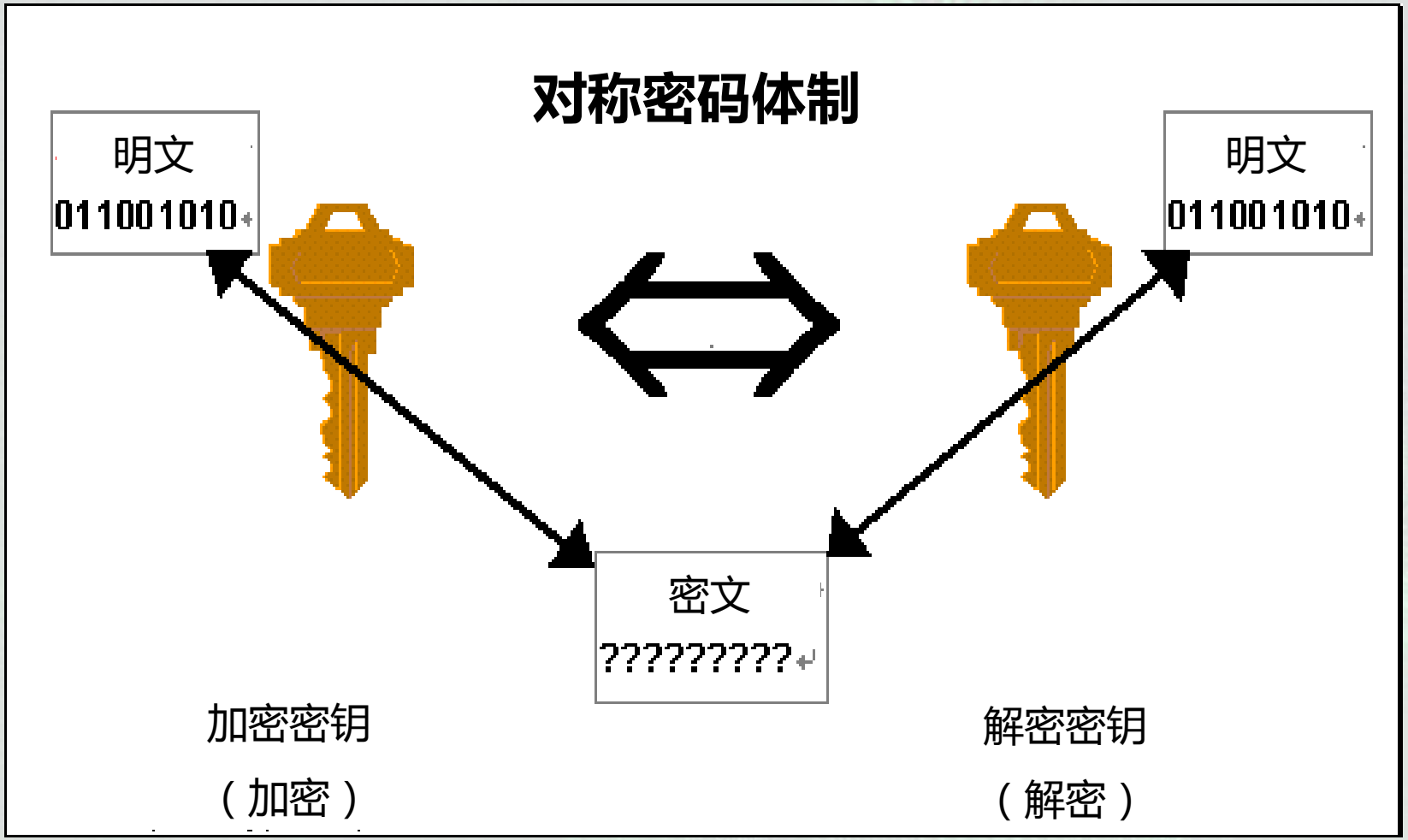
明文：通信的过程中, 发送者想给接收者发送的消息。

加密: 用某种方法伪装消息以隐藏其内容的过程。

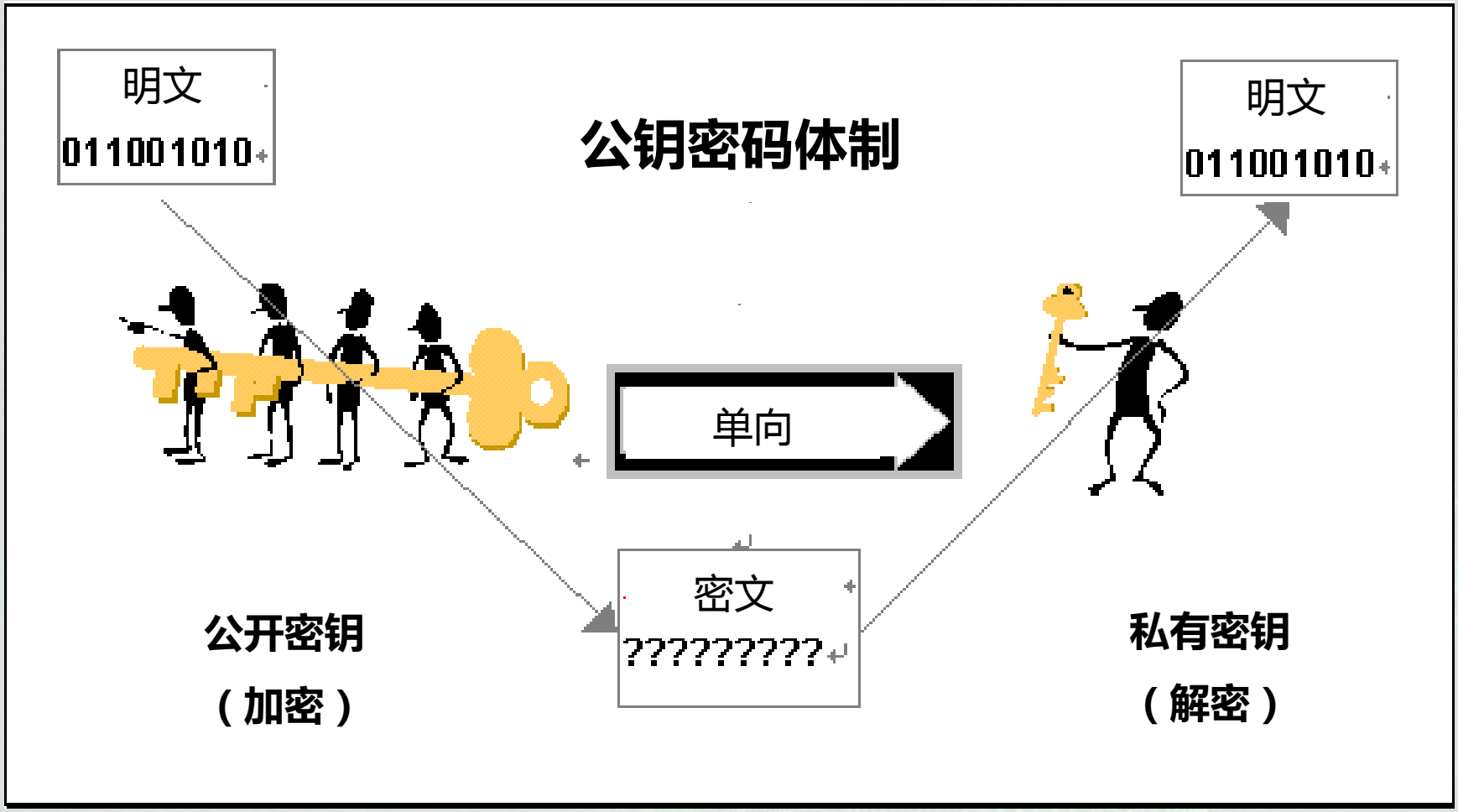
密文：被加密的消息称为密文(ciphertext)。

解密：把密文转变成明文的过程。

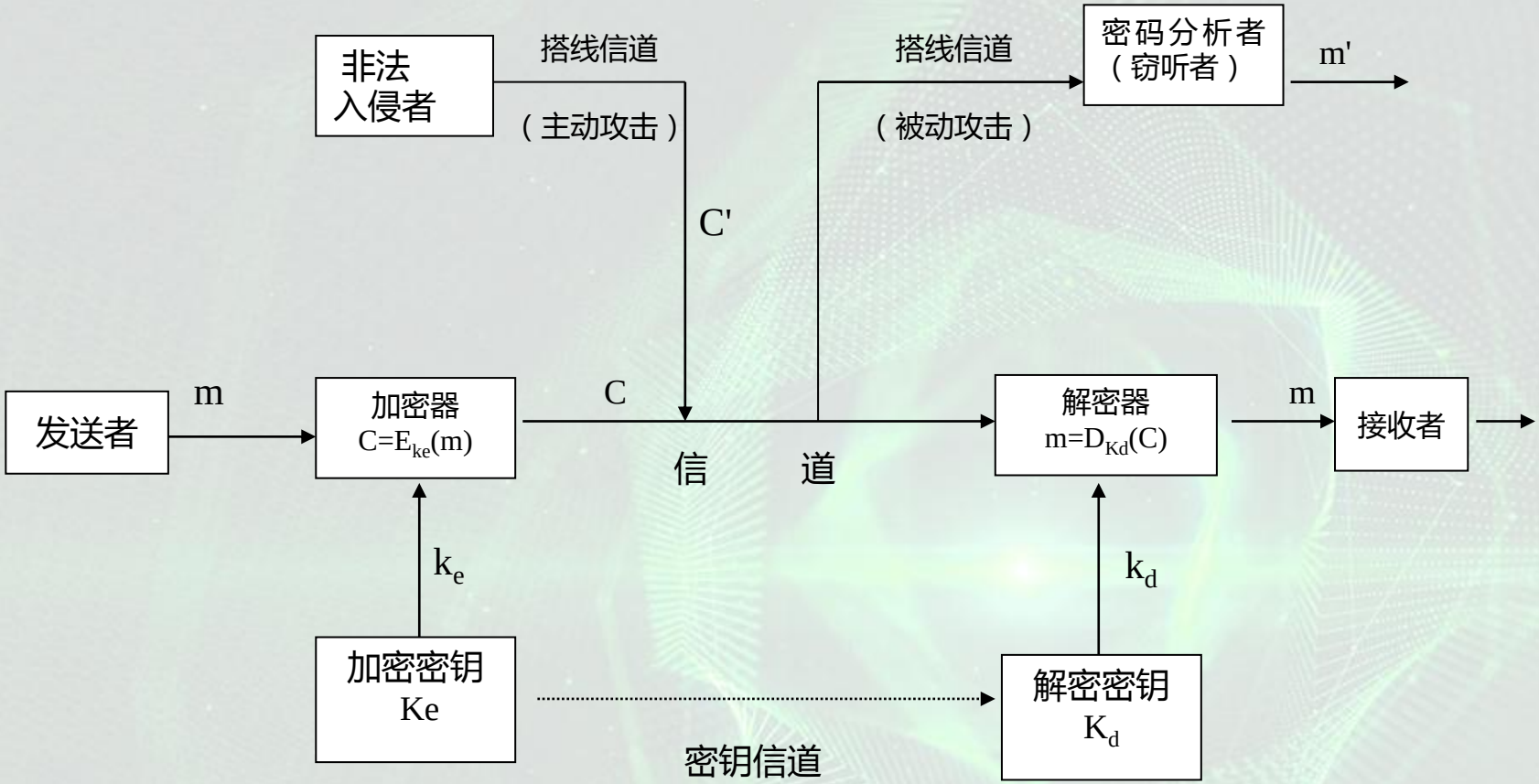
对称密码体制



公钥密码体制



一般保密系统模型


非法
入侵者
搭线信道
（主动攻击）
C'
搭线信道
（被动攻击）
密码分析者
（窃听者）
m'
发送者
m
加密器
C=E_ke(m)
C
信
道
解密器
m=D_Kd(C)
m
接收者
k_e
k_d
加密密钥
Ke
解密密钥
K_d
密钥信道

什么是密码学？

新方法/
新手段

新型计算技术
编码技术的发展

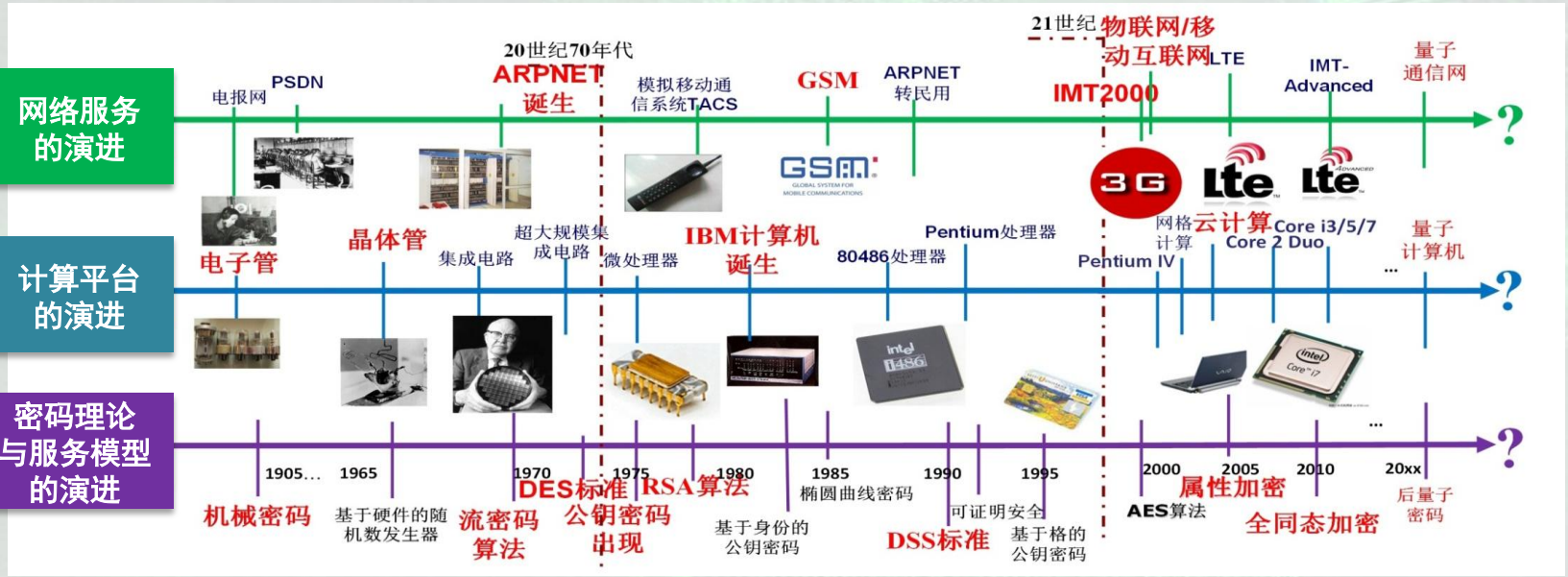
新思想/
新结构

新的应用驱动
分析技术的发展

两个分支形成既对立又统一的矛盾体

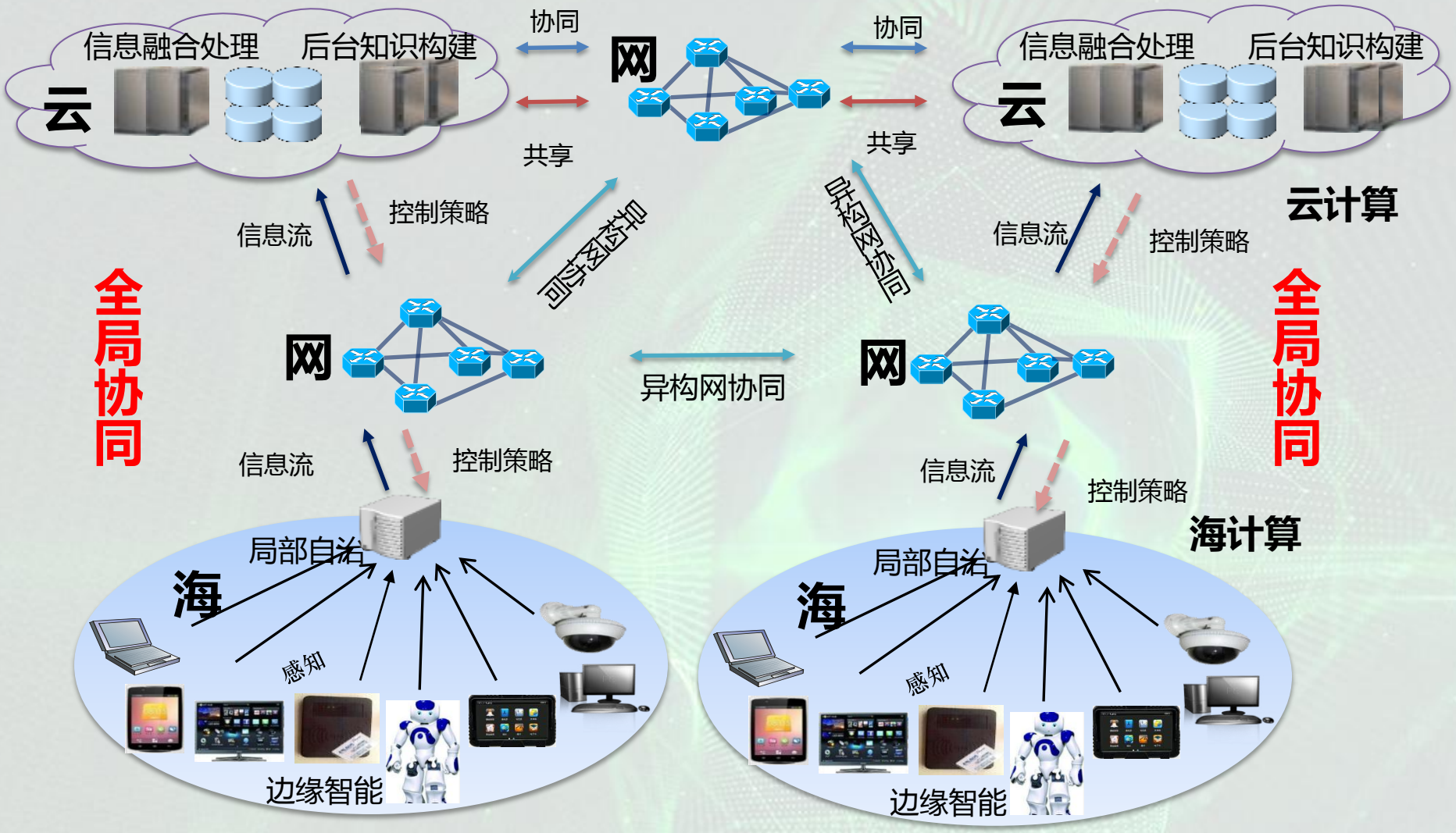
新环境、新挑战

- ✓ 移动互联、云计算、大数据、物联网的出现，导致数据的所有权、管辖权与使用权**相分离**，使得传统的数据保护密码算法**难以满足**数据协同管控的**多元化需求**
- ✓ 新型融合环境的**非可信性**和**高开放性**等特点，以及量子计算的发展，使得数据保护面临的**攻击手段**呈现出**多样化**趋势，为密码方案的设计带来了**新的挑战**



新的应用模式丰富了密码的多样化需求

多元化需求 - 海云计算环境

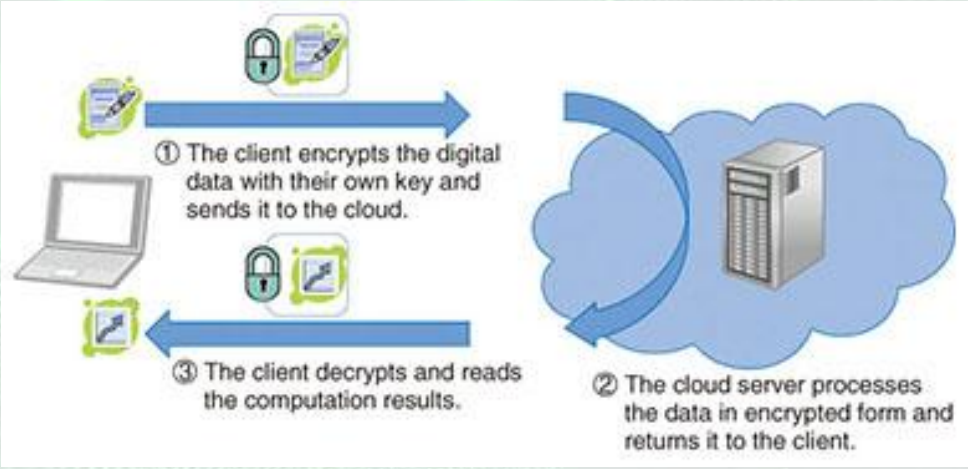


轻量级密码

- 物联网：RFID、智能卡、无线传感器等
- 资源受限：计算能力、电力供应
- 轻量级密码/轻量级协议/非对称密码协议
  - 消耗资源少/低能耗
  - 计算量少
  - 电路简单
- 例子：DESL、HIGHT、PRESENT、MIBS、KATAN/KTANTAN、LBLOCK、Hammingbird、RECTANGLE、WG-7、Grain、A2U2

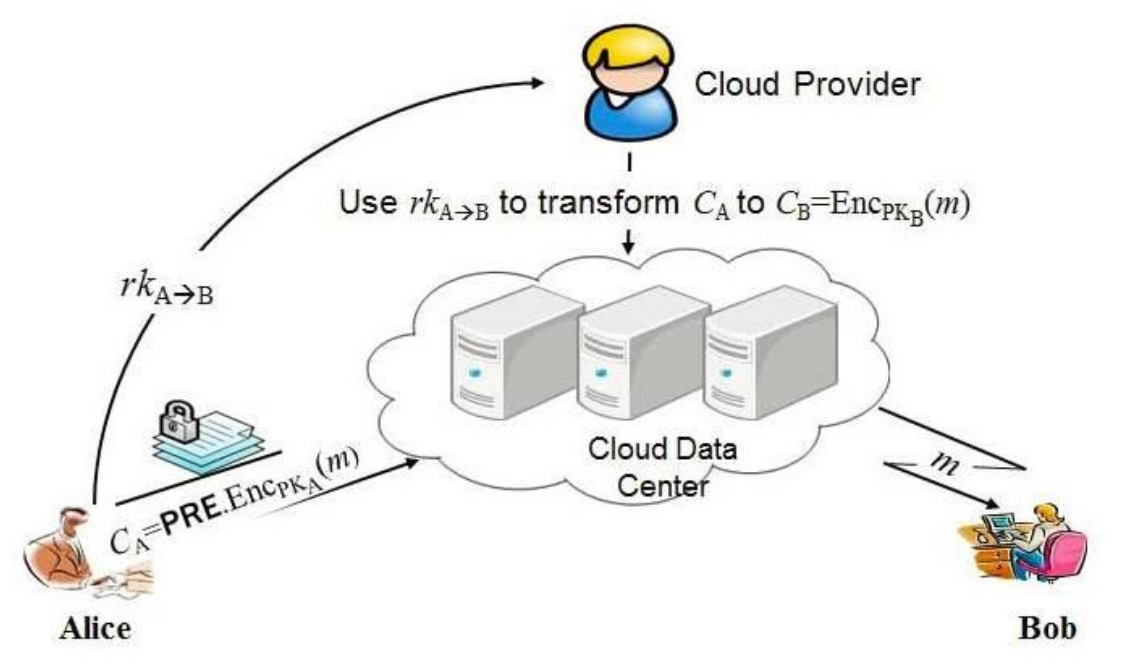
同态密码/功能加密

- 从云计算谈起…
- 数据拥有者对硬件没有控制权，访问控制的软件有安全漏洞，内部人员攻击（服务器不可信）
- 云计算等数据外包使得数据的使用权和所有权相分离，催生了密文计算的新需求
- 同态密码/功能加密
  - 加密运算和明文运算可交换
  - 全同态加密
- 可验证计算



代理重加密/签名

- 服务器：半可信第三方
- 实用举例：云存储中的安全数据共享、加密邮件转发、安全文件系统、



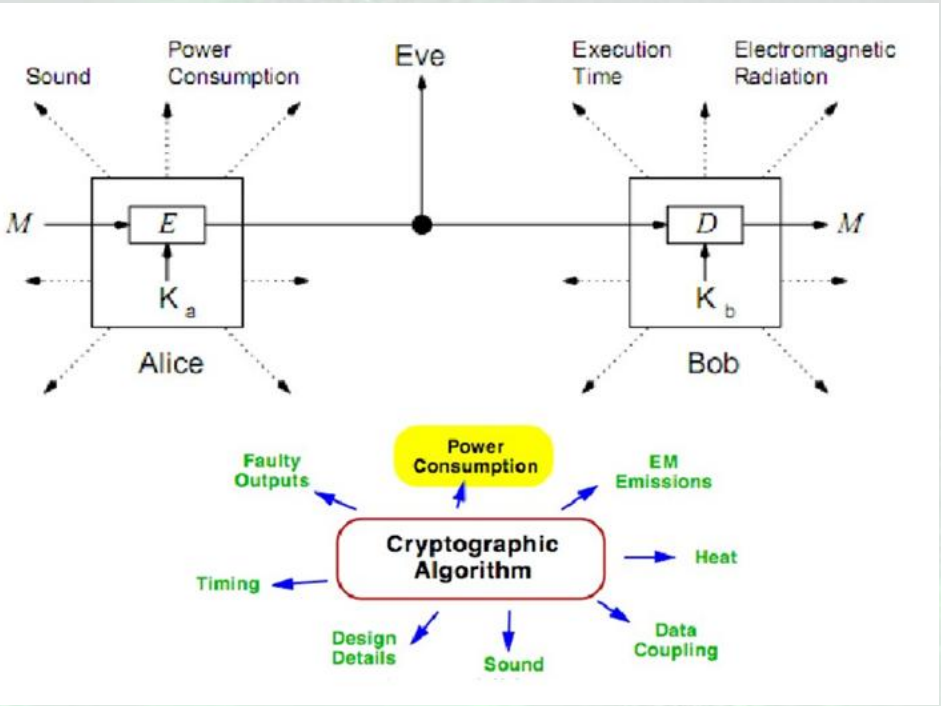
ISC 2017 中国互联网安全大会

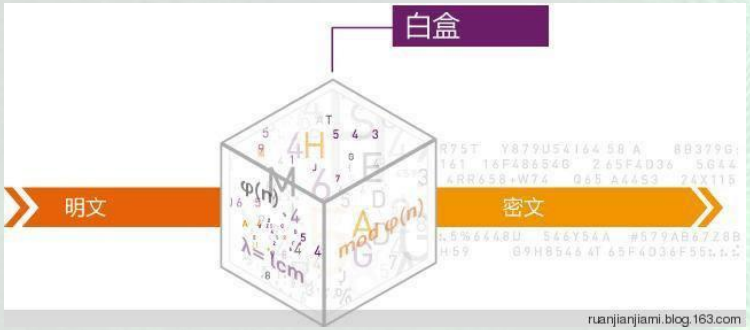
360互联网安全中心

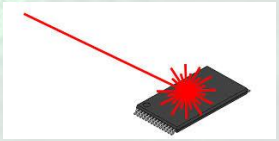
融合环境下多元化攻击催生新型密码理论

多元化攻击

- 侧信道攻击：能耗攻击、错误注入攻击
- 白盒攻击
- 灰盒攻击
- 内存攻击
- 冷启动攻击

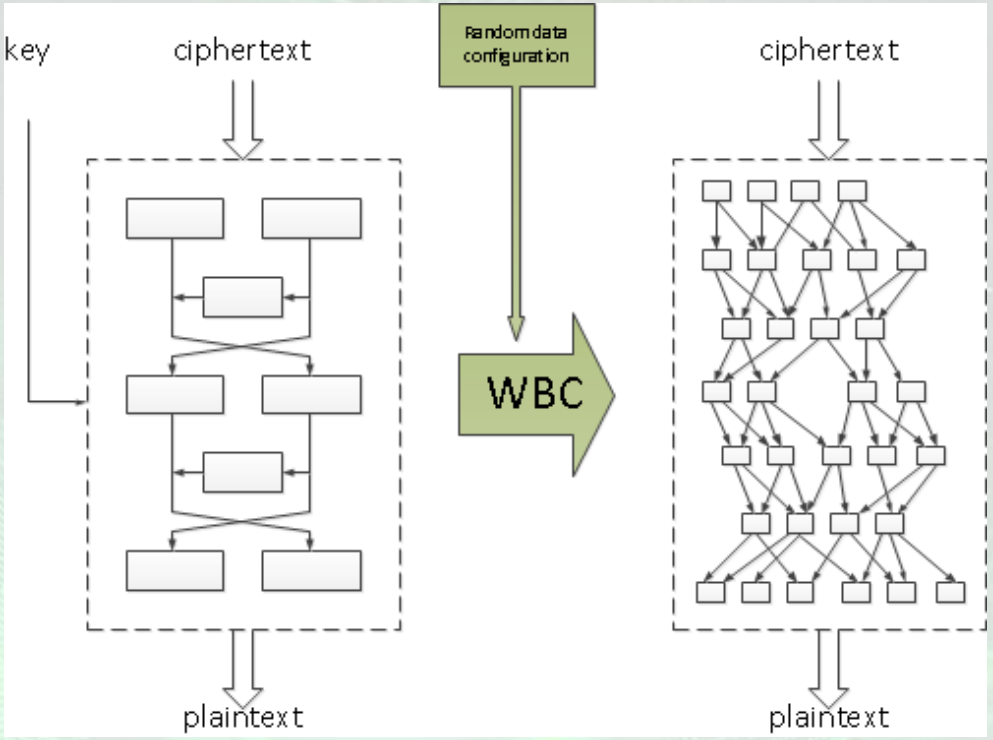






多元化攻击

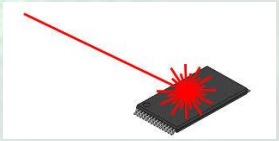
- 白盒密码
- 灰盒密码
- 代码混淆
- 抗泄漏密码学
- ……









ISC 2017 中国互联网安全大会

360互联网安全中心

量子计算促进密码变革

量子计算来了

量子计算核心突破!
Shor算法实现或使密码成摆设？

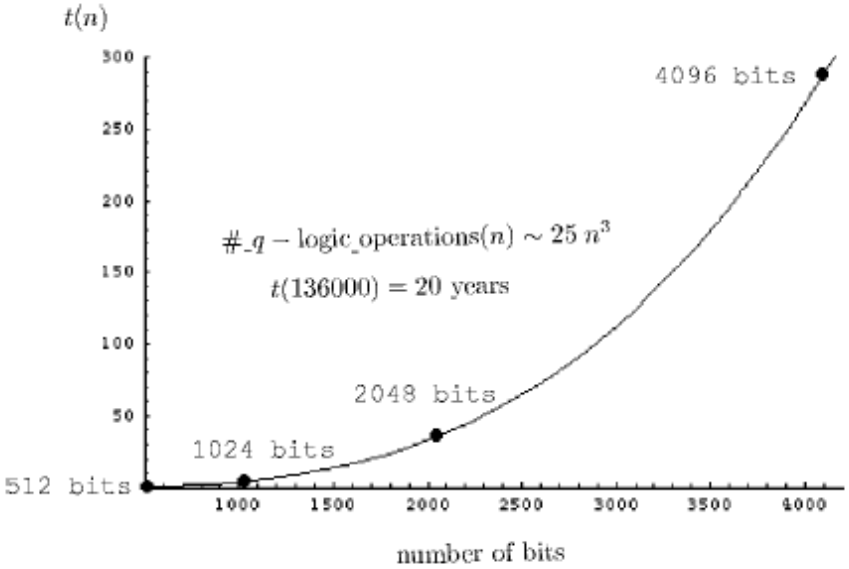


FIG. 41. Factorization times with a hypothetical quantum computer at a nominal clock frequency of 100 MHz. The time $t(n)$, in minutes, is shown as a function of the number of bits.

量子计算带来的冲击

- 现代实用的公钥密码算法的安全性基本上都是建立在大数分解和离散对数困难性问题之上

密码算法	类型型	功能	量子计算的冲击
RSA	公钥密码	数据加密 数字签名	丧失安全性
ECDSA/ECDH	公钥密码	数字签名 密钥交换	丧失安全性
DSA	公钥密码	数字签名	丧失安全性
AES	对称密码	数据加密	加大密钥长度
SHA-2/SHA-3	哈希函数	数据指纹	增加散列长度

量子计算、量子模拟

D-Wave Two

Integrated quantum computing system with 512 qubit chipset

量子计算

RESEARCH | REPORTS

QUANTUM COMPUTING

Defining and detecting quantum speedup

Troels F. Rønnow,[1] Zhihui Wang,[2,3] Joshua Job,[3,4] Sergio Boixo,[5,6] Sergei V. Isakov,[7] David Wecker,[8] John M. Martinis,[9] Daniel A. Lidar,[2,3,4,6,10] Matthias Troyer[1]*

The development of small-scale quantum devices raises the question of how to fairly assess and detect quantum speedup. Here, we show how to define and measure quantum speedup and how to avoid pitfalls that might mask or fake such a speedup. We illustrate our discussion with data from tests run on a D-Wave Two device with up to 503 qubits. By using random spin glass instances as a benchmark, we found no evidence of quantum speedup when the entire data set is considered and obtained inconclusive results when comparing subsets of instances on an instance-by-instance basis. Our results do not rule out the possibility of speedup for other classes of problems and illustrate the subtle nature of the quantum speedup question.

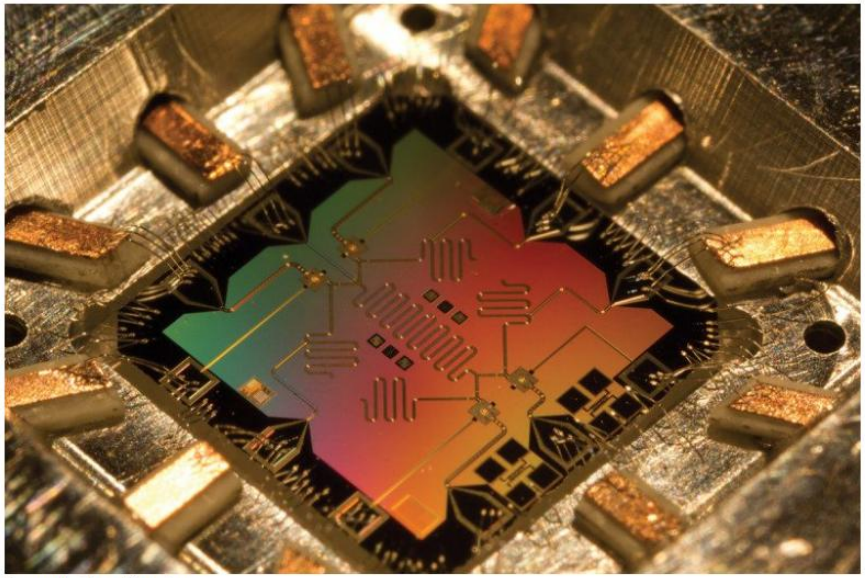
量子计算机的建成
图为D-Wave公司宣称的
具有512qubit的量子计算机
量子加速成疑?

Science 345, 420 (2014)

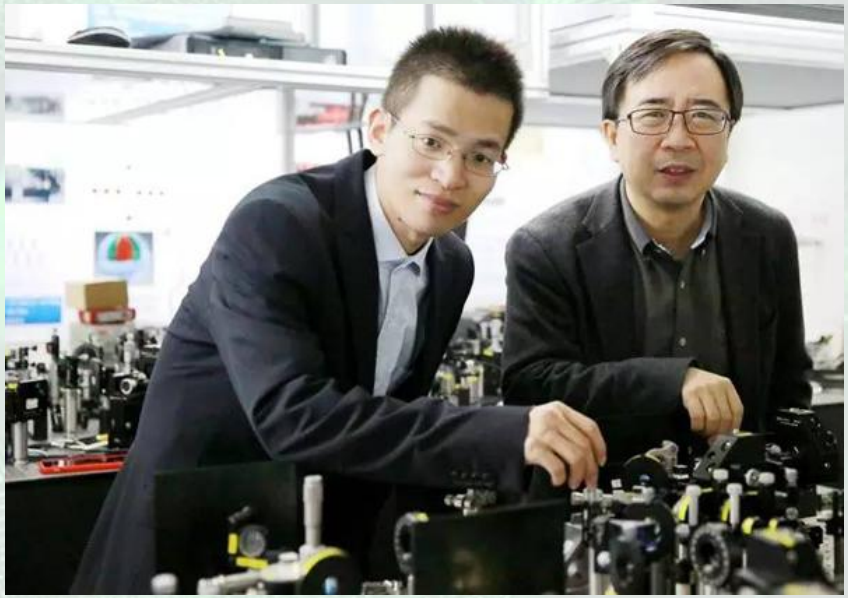
量子霸权

New Scientist

Revealed: Google's plan for quantum computer supremacy



Superconducting qubits are tops



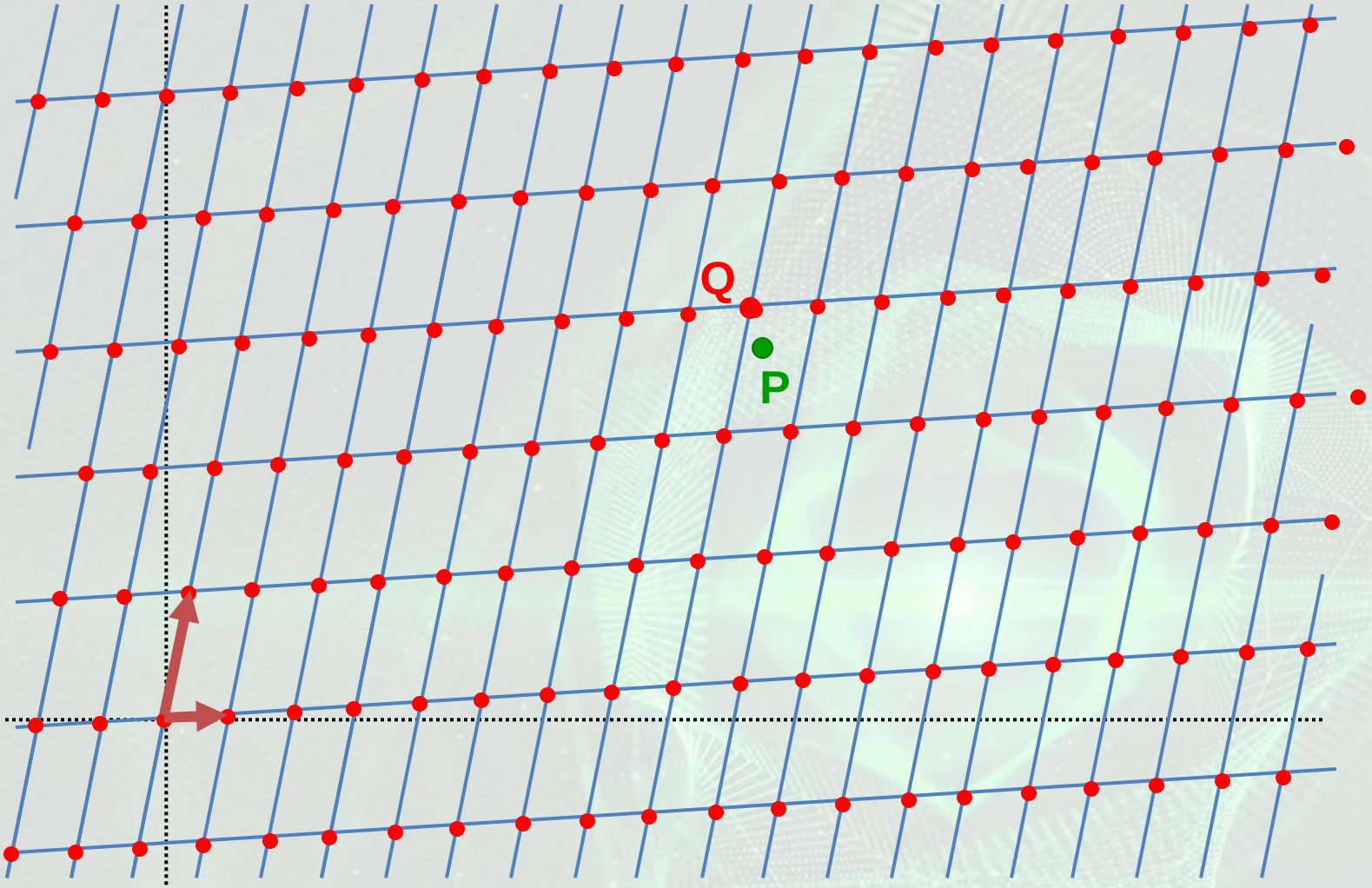
密码何去何从？

- 密码学家：善于在危急中寻找生机
- 抗量子计算密码学（后量子密码学）
  - 必须马上研究
  - 密码算法迁移需要时间
  - 信息的脱密需要时间（一旦量子计算机出现，可用来破解以前加密的东西，现在拦截将来破译）

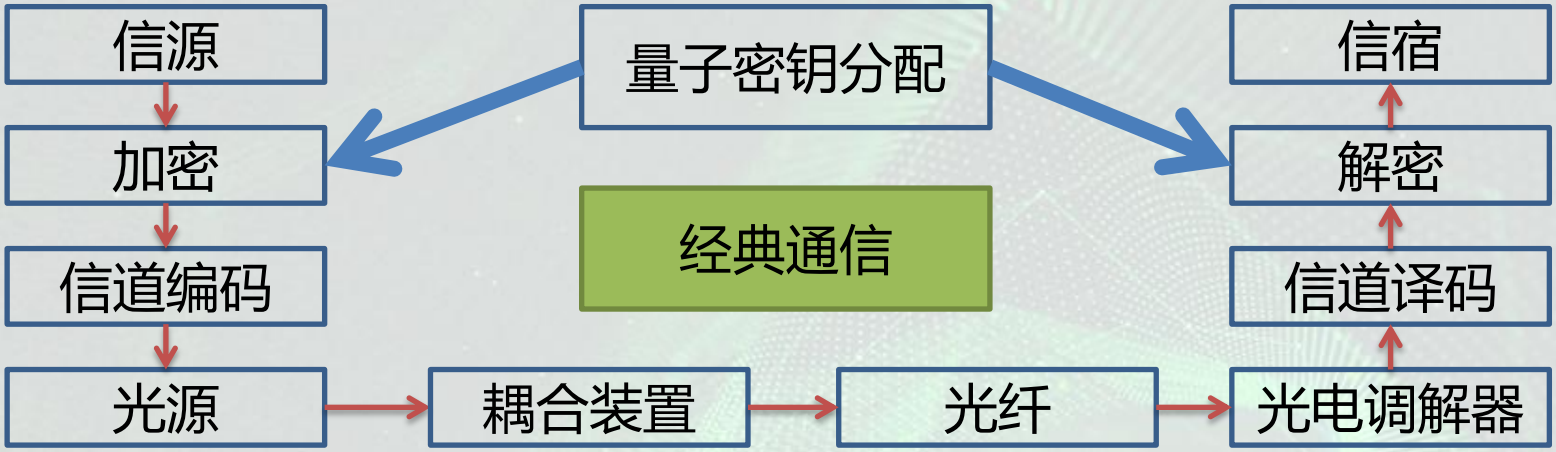
后量子密码学

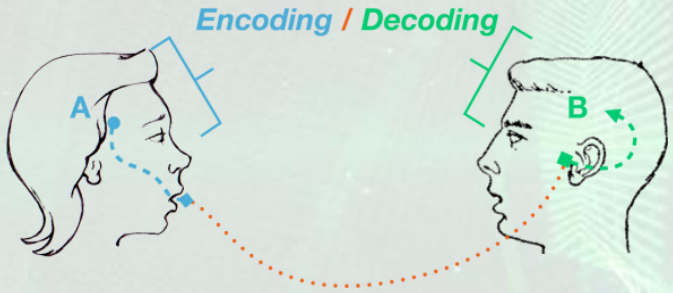
- 抗量子计算密码算法
  - 基于格的密码学
  - 基于散列函数的密码学
  - 基于纠错码的密码学
  - 基于多变量的密码学
- 量子密钥传输

实例：基于格的密码学



经典光通讯和量子保密通讯





Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

量子密码通过量子信道当时产生并应用

总结与展望

密码的标准化趋势

- 从密码发展史来看，密码标准是密码理论与技术发展的结晶，也是推动密码学发展的源动力

密码的公理化/自动化趋势

- 追求算法的可证明安全性是目前的时尚，密码协议的形式化分析方法、可证明安全性理论等仍将是密码协议研究的主流方向

面向社会应用的实用化趋势

- 密码技术本身及其应用水平都有待于提高，适度安全的密码技术的研究已成为当前很受关注的方向

面向新技术发展的适应性趋势

- 日益增强的计算能力和快速变化的计算模式对现有密码技术带来了巨大挑战，具有可变计算安全性和适用新型计算模式的密码技术是未来的重要发展方向

谢　谢