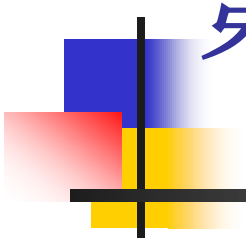
第10章 网络安全发展趋势和新领域



10.1 无线网络安全技术研究

10.2 协议的形式化验证分析技术

10.3 网格安全

10.4 量子密码和量子信息安全

USTC SIST 23

10.1 无线网络技术概述

- 无线网络（**Wireless Network**）是采用无线通信技术实现的网络。
- 主流应用的无线网络分为通过公众移动通信网实现的无线网络（如**4G，3G**或**GPRS**）和无线局域网（**WiFi**）两种方式。
- 无线局域网**(Wireless LAN / WLAN)**，是指用户通过无线网卡**(Wireless Card / PCMCIA**卡**)**连接访问点**(Access Point)**构成的网络。

USTC SIST 23

无线认证与加密

1.无加密认证 （SSID，MAC）

2.WEP （Wired Equivalent Privacy）有线等效加密技术

- IEEE 802.11b标准中定义的最基本的加密技术，多用于小型的、对安全性要求不高的场合。

3.WPA（Wi-Fi Protected Access）Wi-Fi（Wireless Fidelity，无线保真技术）保护存取

- TKIP （Temporal Key Integrity protocol） 临时密钥完整性协议
- AES（Advanced Encryption Standard）高级加密标准

4.IEEE 802.1x认证协议(基于端口的访问控制协议）

USTC SIST 23

1.无加密认证

- SSID
  - 只要使用者能够提出正确的SSID，存取点AP就接受用户端的登入请求。
  - 通常情况下，无线接入点AP会向外广播其SSID。
  - 我们可以通过Disable SSID Broadcast来提高无线网络安全性。
- MAC
  - AP可以通过stations的MAC address来对特定的stations进行filter管理，从而可以表示是allow 还是deny这些stations来associate该AP

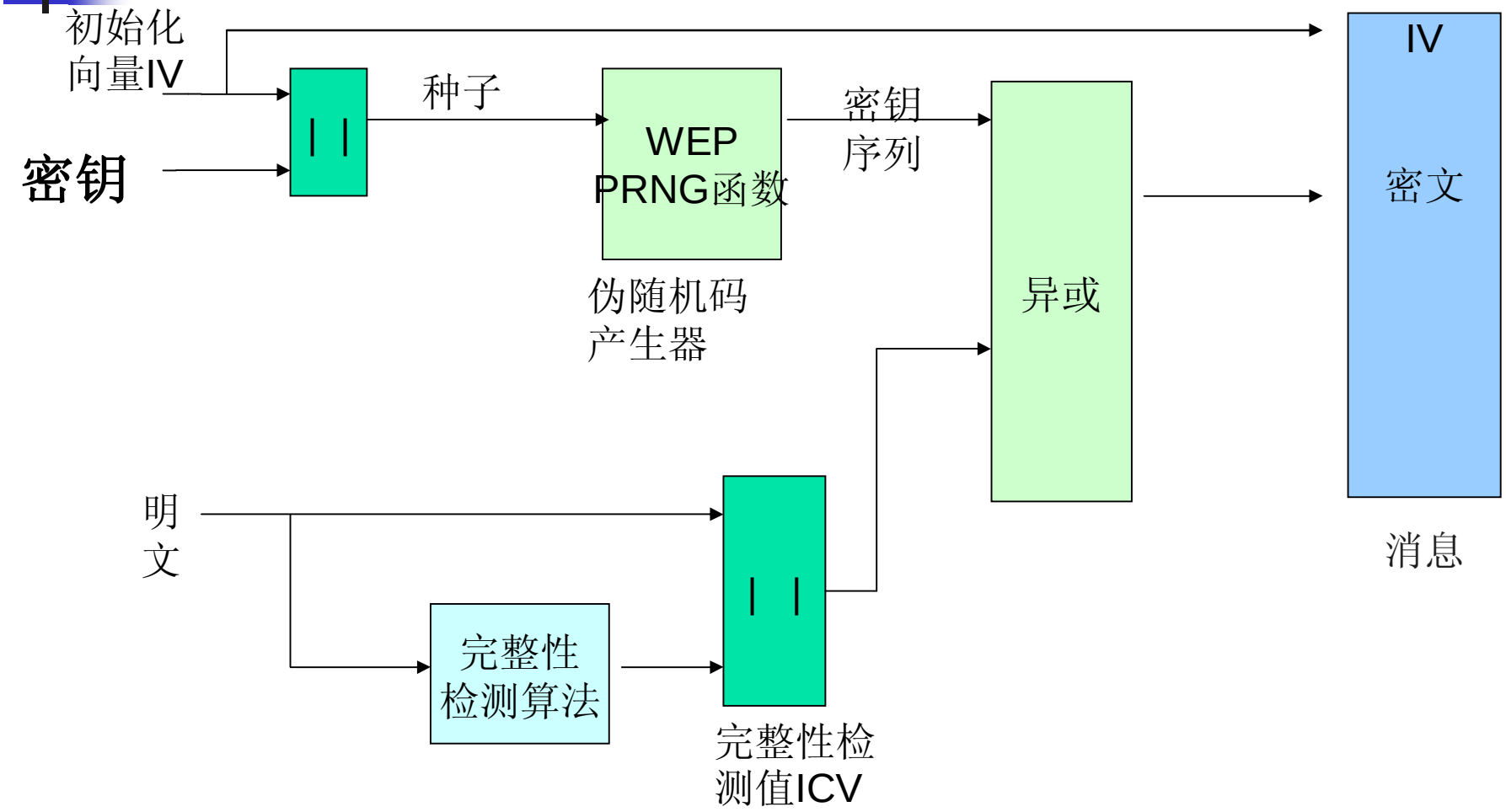
USTC SIST 23

2. WEP

- WEP（Wired Equivalent Privacy）是由802.11b标准定义的，是一种对称加密，其中加密和解密的密钥及算法(RC4和XOR演算法)相同。WEP只对数据帧的实体加密，而不对数据帧控制域以及其他类型帧加密。使用了该技术的无线局域网，所有客户端(STA)与无线接入点(AP)的数据都会以一个共享的密钥进行加密，密钥的长度有64/128/256bits几种方式(对应的key value分别是40/104/232bits)，其中包括24位是初始向量IV。
- 经过WEP加密的封包中，只有MAC地址和IV是明码，其余部分都是经过RC4加密后来传送的。

USTC SIST 23

WEP加密流程图


初始化
向量IV
密钥
||
种子
WEP
PRNG函数
伪随机码
产生器
密钥
序列
异或
IV
密文
消息
明
文
完整性
检测算法
||
完整性检
测值ICV

WEP的安全弱点

A.802.2头信息和简单的RC4流密码算法导致攻击者在有客户端并有大量有效通信时，可以分析出WEP的密码。

B.IV重复使用导致在攻击者在有客户端少量通信或者没有通讯时，可以使用 ARP重放的方法获得大量有效数据。

C.无身份验证机制，使用线性函数 CRC32 进行完整性校验，导致攻击者能用 XOR 文件伪造一个ARP包，然后依靠这个包去捕获大量有效数据。

D.WEP加密现在已经有软件可以轻易破解

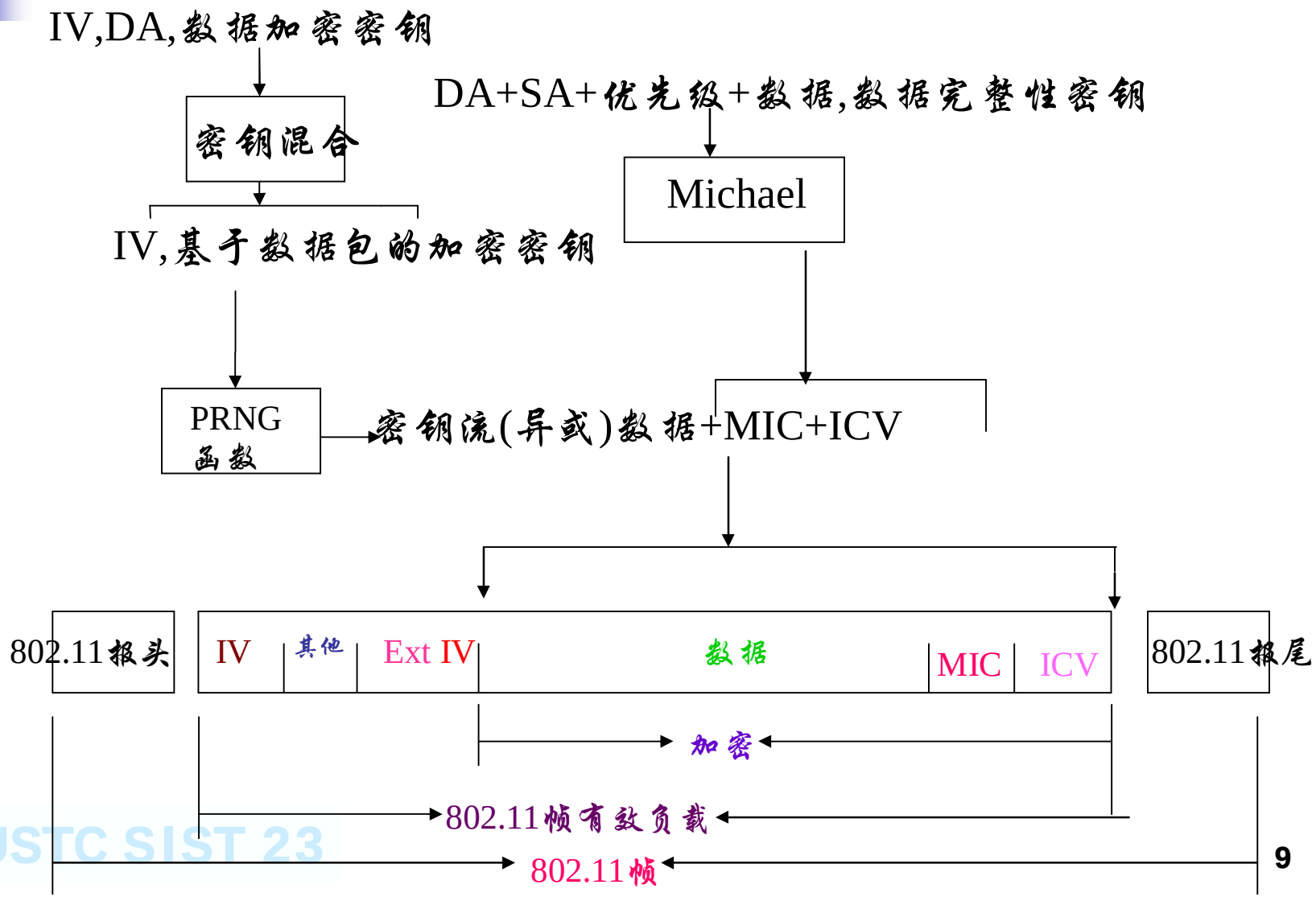
USTC SIST 23

3.WPA （Wi-Fi Protected Access ）

- 无线联盟制定的一种等级更高的数据保护和访问控制标准，用于升级现存的或将来的无线局域网系统。采用RADIUS和Pre-Shared Key(预共享密钥)两种认证方式。
- RADIUS方式：用户提供认证所需的凭证，如用户名密码，通过特定的用户认证服务器（一般是RADIUS服务器）来实现。适用于大型企业网络。
- 如果采用PSK方式：仅要求在每个WLAN节点(AP、无线路由器、网卡等)预先输入一个密钥即可实现。只要密钥正确，客户就可以获得WLAN的访问权。适用于家庭网络。
- WPA包含了认证、加密和数据完整性校验三个组成部分，是一个完整的安全性方案

USTC SIST 23

WPA加密过程图

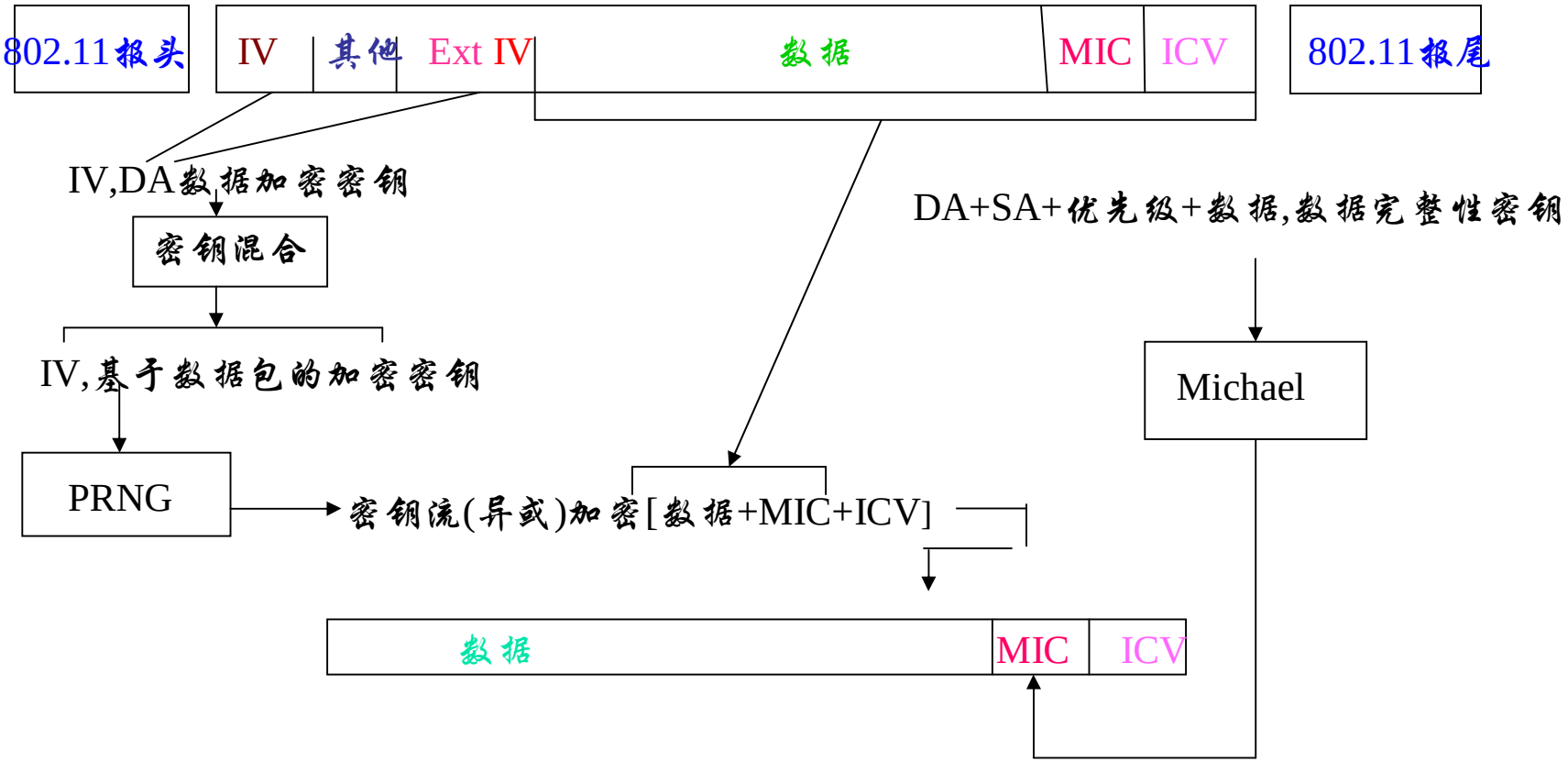


USTC SIST 23

WPA加密过程

1. IV,DA和数据加密密钥被输入WPA密钥混合函数.
2. DA,SA,优先级,数据(非加密802.11有效负载)和数据完整性密钥被输入Michael数据完整性算法以生成MIC.
3. ICV是从CRC-32校验和计算出来的.
4. IV和基于每个数据包的加密密钥被输入RC4 PRNG函数以生成与数据,MIC和ICV大小相同的密钥流.
5. 密钥流与数据,MIC和ICV的组合进行异或逻辑运算,生成802.11有效负载的加密部分.
6. IV被添加到IV和扩展IV两个字段中的802.11有效负载的加密部分,其结果被802.11报头和报尾封装了起来.

WPA解密过程图



USTC SIST 23

WPA解密过程

1.从802.11帧有效负载的IV和扩展IV两个字段中提取IV值,然后将此值与DA和数据加密密钥一起输入密钥混合函数,生成基于数据包的加密密钥.

2.IV和基于数据包的加密密钥被输入RC4 PRNG函数,生成与加密的数据,MIC和ICV大小相同的密钥流.

3.密钥流与加密的数据,MIC和ICV进行异或逻辑运算,生成非加密数据,MIC和ICV.

4.计算ICV,并将其与非加密ICV值相比较.如果两个ICV值不匹配,数据就会被悄悄丢弃.

5.DA,SA,优先级,数据和数据完整性密钥被输入Michel完整性算法以生成MIC.

6.MIC的计算值与非加密MIC的值相比较.如果两个MIC值不匹配,数据就会被悄悄丢弃.如果两个MIC值相匹配,数据就会被传输到上一级网络层进行处理.

USTC SIST 23

消息完整性校验MIC

- 消息完整性校验(MIC)，是为了防止攻击者从中间截获数据报文、篡改后重发而设置的。除了和802.11一样继续保留对每个数据分段(MPDU)进行CRC校验外，WPA为802.11的每个数据分组(MSDU)都增加了一个8个字节的消息完整性校验值，这和802.11对每个数据分段(MPDU)进行ICV校验的目的不同。
- ICV的目的是为了保证数据在传输途中不会因为噪声等物理因素导致报文出错，因此采用相对简单高效的CRC算法，但是黑客可以通过修改ICV值来使之和被篡改过的报文相吻合，可以说没有任何安全的功能。
- 而WPA中的MIC则是为了防止黑客的篡改而定制的，采用Michael算法，具有很高的安全特性。当MIC发生错误的时候，数据很可能已经被篡改，系统很可能正在受到攻击。此时，WPA还会采取一系列的对策，比如立刻更换组密钥、暂停活动60秒等，来阻止黑客的攻击。

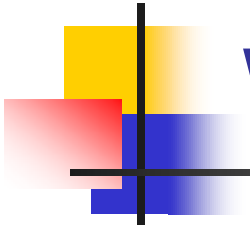
TKIP (Temporal Key Integrity Protocol)

- 加密技术TKIP与WEP一样基于RC4加密算法，但为了解决WEP静态密钥容易被他人获得的问题，对现有的WEP进行了改进，追加了4种算法，从而提高了加密安全强度
  - 密钥细分（每发一个包重新生成一个新的密钥）
  - 消息完整性检查（MIC）
  - 具有序列功能的初始向量（IV）
  - 密钥生成和定期更新功能

- WPA采用TKIP来对密钥进行管理，该协议要求加密密钥在一定时间间隔内就要更换，更换的时间间隔要小于最成熟的破解者破解密钥所需要的最短时间。即使密钥每10分钟被更换一次，一个Wi-Fi客户端还是需要知道用哪个密钥开始。WPA规范要求WPA产品自动产生这一密钥。

AES (Advanced Encryption Standard)

- AES 是一个迭代的、对称密钥分组的密码，可以使用128、192 和 256 位密钥，并且用 128 位（16字节）分组加密和解密数据。
- AES 算法是基于置换和代替的。置换是数据的重新排列，而代替是用一个单元数据替换另一个。AES 使用了几种不同的技术来实现置换和替换。
- AES提供比WEP/TKIP中RC4算法更高的加密性能，将在IEEE 802.11i最终确认后，成为取代WEP的新一代的加密技术，为无线网络带来更强大的安全防护。



WPA2

- WPA是一个中间过渡标准，最终的安全解决标准是802.11i，WPA的认证方式是802.1x；加密方法是WEP、TKIP；WPA2的认证方式是802.1x；加密方法是WEP、TKIP和CCMP。 即
  - WPA=802.11i草案3=802.1x/EAP+WEP(可选)/TKIP
  - WPA2=802.11i=802.1x/EAP+WEP（可选）/TKIP/CCMP（AES-CCMP）
- WAPI是中国无线局域网强制性标准中的安全机制，已获得ISO认可，将成为国际标准。
- WAPI和802.11i物理层是一样的，只是协议和MAC层不一样，因此很容易在一个芯片上支持两种标准。

4. IEEE 802.1x认证协议 (基于端口的访问控制协议)

- 略

蓝牙安全

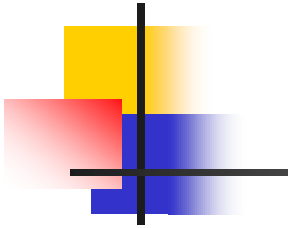
- 蓝牙应用协议栈

（1）射频协议（RF/Radio Protocol）：定义了蓝牙发送器和接收器的各个参数，包括发送器的调制特性，接收器的灵敏度、抗干扰性能、互调特性和接收信号强度指示等。

（2）基带/链路控制协议（Baseband/LC Protocol）：定义了基带部分协议和其他低层链路功能，是蓝牙技术的核心。

（3）链路管理协议（LMP）：用于链路的建立、安全和控制，定义了许多过程来完成不同的功能。

（4）主机控制器接口（HCI：Host Controller Interface）协议：描述了主机控制接口功能上的标准，提供了一个基带控制器和链路管理器（LM）得知硬件状态和控制寄存器命令的接口，在蓝牙中起着中间层的作用：向下给链路控制器协议和链路管理协议提供接口，提供一个访问蓝牙基带的统一方法。HCI是在硬件和软件都包含的部分。



（5）逻辑链路控制和适配协议（L2CAP：Logical Link Control and Adaptation Protocol）：支持高层协议复用、帧的组装和拆分、传送QoS信息。L2CAP提供面各连接和非连接两种业务，允许高层最多达64kbit/s的数据，以一种有限状态机（FSM）的方式来进行控制，目前只支持异步无连接链路（ACL）。

（6）服务发现协议（SDP：Service Discover Protocol）：如何发现蓝牙设备所提供服务的协议，使高层应用能够得知可提供的服务。在两个蓝牙设备第一次通信时，需要通过SDP来了解对方能够提供何种服务，并将自己可提供的服务通知对方。

（7）高层协议：包括串口通信协议（RFCOMM）、电话控制协议（TCS）、对象交换协议（OBEX）、控制命令（AT-Command）、电子商务标准协议（vCard和vCalender）和PPP，IP，TCP，UDP等相关的Internet协议以及WAP协议。其中，串口通信协议是ETSI TS07.10标准的子集，并且加入了蓝牙特有的部分；电话控制协议使用了一个以比特为基础的协议，定义了在蓝牙设备之间建立语音和数据呼叫的控制信令，对象交换协议提供了与IrDA协议系列相同的特性，并且使各种应用可以在IrDA协议栈和蓝牙协议栈上使用。

蓝牙系统安全性要求

（1）蓝牙设备地址（BD_ADDR）：是一个对每个蓝牙单元唯一的48位IEEE地址。

（2）个人确认码（PIN：Personal Identification Number）：是由蓝牙单元提供的1-16位（八进制）数字，可以固定或者由用户选择。一般来讲，这个PIN码是随单元一起提供的一个固定数字。但当该单元有人机接口时，用户可以任意选择PIN的值，从而进入通信单元。蓝牙基带标准中要求PIN的值是可以改变的。

（3）鉴权字：是长度为128位的数字，用于系统的鉴权。

（4）加密字：长度8-128位，可以改变。这是因为不同的国家有许多不同的对加密算法的要求，同时也是各种不同应用的需要，还有利于算法和加密硬件系统的升级。

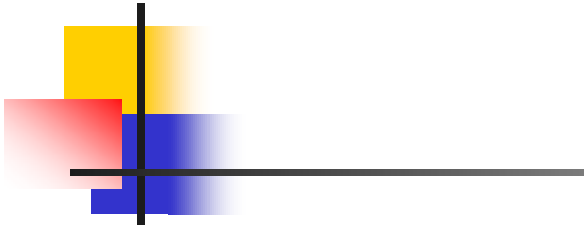
如何保护蓝牙

（1）不使用就不启用

- 如果希望保护蓝牙的安全，一个首要的原则是在不需要使用蓝牙的时候将其关闭。对于移动电话来说可以在蓝牙设置页面中将蓝牙关闭，而对于计算机上的蓝牙适配器可以通过附带的工具软件或操作系统本身的蓝牙软件将其设置为不可连接状态。

（2）使用安全设置

- 在蓝牙规范中定义了三种安全模式，没有任何保护的无安全模式、通过验证码保护的服务级安全、可以应用加密的设备级安全，在适用的情况下尽可能应用较高的安全模式。对便利性要求不是特别高的环境不要将蓝牙设置为可见状态，这通常不会对验证受到信任的设备造成麻烦。



（3）选择强壮的PIN码

- 正常的蓝牙设备连接会使用PIN码进行验证，相当于计算机的访问密码。通常在设备出厂时这个PIN码不会被设置或者被设置为一个特定的四位数字，这样的PIN码设置仍然很容易受到攻击。根据我的经验每一百部蓝牙手机中会有接近百分之十到百分之二十使用1111或1234这样简单的密码，设置一个尽量复杂的PIN码非常的重要。

（4）保持对安全更新的跟踪

- 通常存在安全漏洞的手机都可以通过厂商提供的更新进行解决，所以应该了解自己的设备是否有安全漏洞并及时从厂商处获取更新。另外更多的了解蓝牙安全方面的知识并应用一些免费的蓝牙安全工具也可以有效的减少受攻击的可能。

（5）足够的警惕性

- 恶意攻击并不总是隐密的进行，在攻击过程中蓝牙连接的状态图标可能会发生变化，设备可能会产生某些声音，还可能会出现可疑的配对请求。蓝牙用户有责任对安全问题保持足够的警惕，而且这样才能阻止各种社交工程行为。

10.2 协议的形式化验证分析技术

- 略

10.3 网格安全

- 网格是一种虚拟计算环境，利用计算机网络将分布异地的计算、存储、网络、软件、信息、知识等资源连成一个逻辑整体，如同一台超级计算机为用户提供一体化的信息应用服务，实现互联网上所有资源的全面连通与共享，消除信息孤岛和资源孤岛。
- 云计算，美国国家标准与技术研究院（NIST）：云计算是一种按使用量付费的模式，这种模式提供可用的、便捷的、按需的网络访问，进入可配置的计算资源共享池（资源包括网络、服务器、存储、应用软件、服务），这些资源能够被快速提供，只需投入很少的管理工作，或与服务供应商进行很少的交互。
- 云计算是从网格计算演化来的，能够随需应变地提供资源。

特点

- 网格安全技术可防止非法用户使用或获取网格的资源，具有以下特征：

（1）异构资源管理

- 网格可以包含跨地理分布的多种异构资源、不同体系结构的超大型计算机和不同结构的操作系统及应用软件

（2）可扩展性

- 网格的用户、资源和结构为动态变化，要求网格系统安全结构具有可扩展性，以适应网格规模的变化。

（3）结构不可预测性

- 传统计算，资源独占，系统的行为可预测。在网格计算系统中，资源共享造成系统行为和系统性能经常变化，具有不可预测性。

（4）多级管理域

- 由于计算网格的分布性特点，与用户和资源有关的各种属性可以跨越物理层属于多个组织机构。并且使用不同的安全机制，需要各个机构或组织共同参与解决多级管理域的问题。

USTC SIST 23

关键技术

（1）安全认证技术

- 公钥基础设施PKI（Public Key Infrastructure)，包括加密、数字签名和数字证书等技术。网格系统只对用户一次认证，就可访问多个节点资源。

（2）网格中的授权

- 将属于不同独立组织的资源和人员进行组织，创建一个虚拟组织（Virtual Organization，VO)。可通过用户在本地组织中角色加入VO解决社区授权服务(Community Authorization Service，CAS)负担过重的问题。网格安全基础设施（Grid Security Infrastructure，GSI）是基于公钥加密、X.509证书和安全套接层SSL通信协议的一种安全机制，用于解决VO中的认证和消息保护问题。

（3）网格访问控制

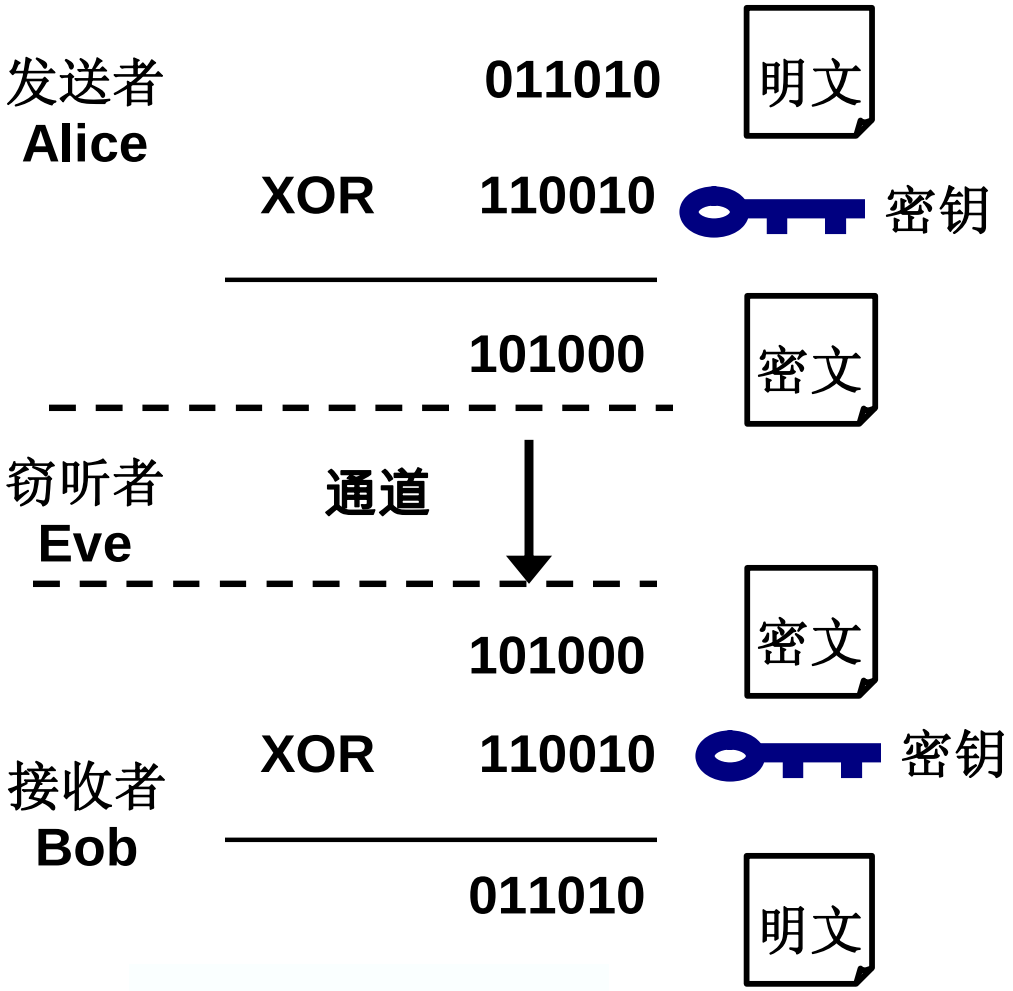
- 可通过区域授权服务或虚拟组织成员服务提供。社区授权服务(Community Authorization Service，CAS)允许虚拟组织维护自己的策略，并可使用这些策略与本地站点交互。可通过扩展传统的资源访问控制列表（ACL）生成扩展访问控制列表(Extended Access Control List)。

（4）网格安全标准

- 为实施网格环境中的资源共享，网格环境中使用安全声明标记语言SAML（Security Assertion Markup Language）来交换鉴定和授权信息

USTC SIST 23

“一次一密”加密方式 One-time Pad (OTP)



XOR=
Exclusive-OR

如果
1）密钥的长度=信息的长度
2）密钥只使用一次

“一次一密”原理上绝对安全
(Shannon 1949)

如何在发送者与接收者间建立密钥？密钥分配问题
如何防止窃听？

USTC SIST 23

10.4 量子密码和量子信息安全

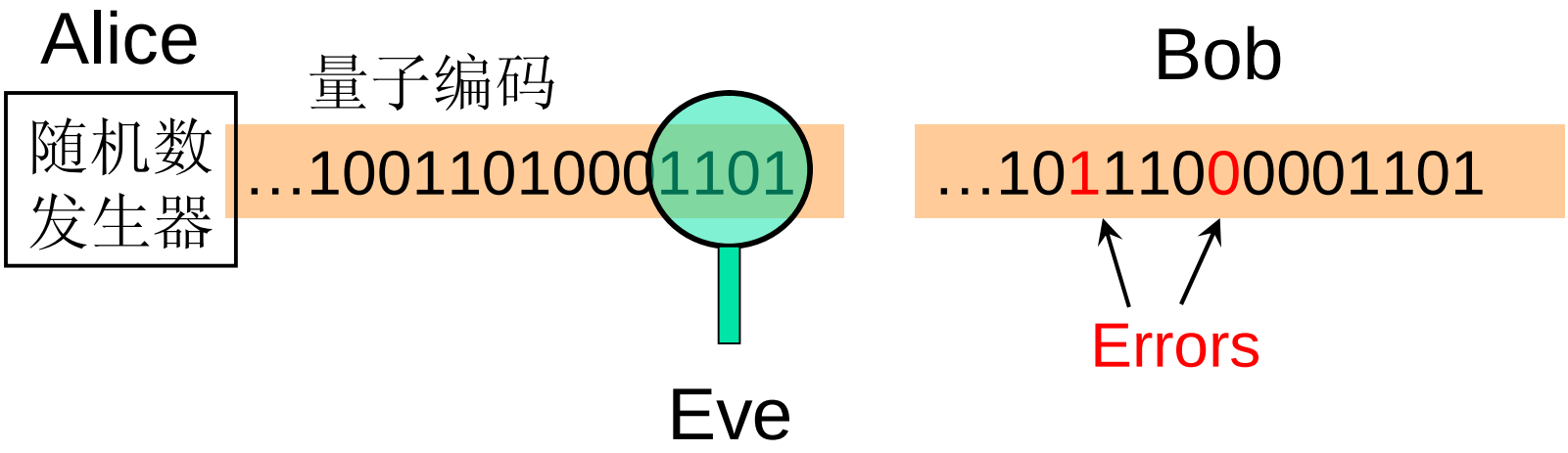
- 信息的获取涉及测量过程；
- 测量精度决定可获取的信息量；
- 经典物理
  - 测量过程可以不改变被测物体状态；
  - 窃听者可以获取信息而不被发现。
- 量子物理
  - 测量过程一般会改变被测物体状态（测不准原理）；
  - 量子力学提供了探测窃听的手段。
- 量子密钥分发体制 - 现在还没有进入实用阶段

量子密钥

- 量子密钥在1984年由Bennett，Brassard和Wiesner共同提出。 BB84协议
  - 可以抵抗任何破译技术和计算工具的攻击，原因在于它的保密性由物理定律来保证。
- 传统光信号需要用成千上万个光子来传输一比特的信息，如果从这些光子里抽取少量，不会明显的影响所要传输的信息。所以窃取是可能的。
- 在量子密钥分发中，用一个光子携带一比特的信息，根据量子的不可分割性，不能用分流信号的办法来窃听。光子有很多物理量可以做传输的载体，例如偏振态和相位。

量子密钥分配的基本原理

量子力学：测量过程 **à** 对量子态产生扰动



过高的比特误码率 **à** 窃听者的存在

A: Alice　　B: Bob　　C: Eve

量子密钥分配的基本原理

- 安全性的直观理解
  - 量子力学：不可能区分0°/45°/90°/135°偏振的单光子 ó 量子非克隆原理；
  - Eve随机选取基测量，再发送 à 引入比特误差（25%）；Eve获得的信息量越大 à 比特误差率越高；
  - 安全性证明：建立比特误差率与Eve的最大信息量间的关系。只要I(A:B)>I(A:E)或者I(A:B)>I(E:B)，Alice和Bob就可以产生密钥。

- 实际系统中噪声的影响
  - 无法区分噪声引入的比特误差与Eve引入的比特误差；
  - 保守的估计：所有的比特误差归结于Eve的攻击；
  - 高噪声的系统无法证明安全性。

USTC SIST 23

量子密钥协议

- BB84协议中，使用了四个偏振态，1992年，Bennett提出B92协议，只用两个非正交偏振态实现密钥分配。这种协议简单，但效率减半。
- 英国人Ekert在1991年基于量子力学的另一种概念提出一种基于EPR关联对的协议。EPR关联是指非局域的量子相关效应，与上述两种协议原则上的不同是，EPR关联对协议利用了纠缠光子间的纠缠特性来保证密钥分发过程的安全性。

量子密钥实现

- 量子密钥最早的实现正是基于偏振态的，由Bennett等在89年演示成功，光子在自由空间中只传输了32cm，误码率为4%
- 美国JohnsHopkins大学采用BB84协议,用He2Ne激光器和电光调制器产生光脉冲,成功地在白天室外条件下传输单光子,自由空间光程为75m,比特传输率为1kHz,误码率为2%。
- 美国LosAlamos国家实验室采用B92协议,进行了夜晚条件下室外光路950m和白天室外光路500m的量子密码术实验,误码率分别为1.5%和1.6%。后来,他们又进行了1.6km自由空间量子密码术实验。该实验是在白天室外条件下,采用B92协议,平均误码率为5.3%。

USTC SIST 23

量子密钥 QK

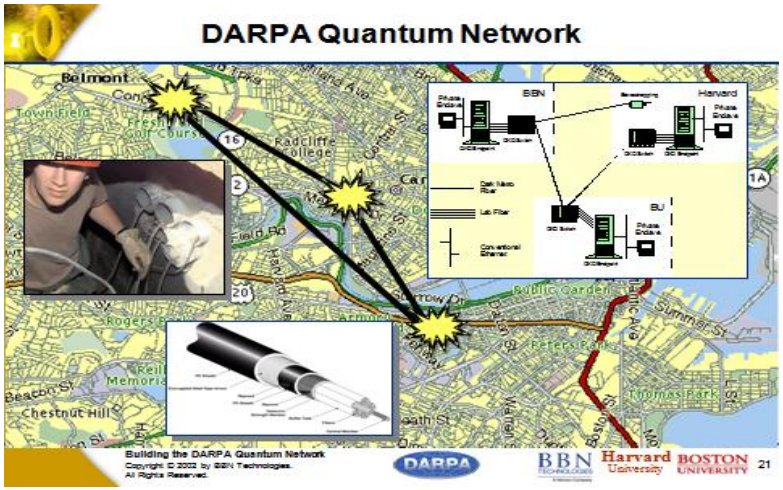
- 从93年实现光纤中相位编码方式的密钥分配机制以来，光纤量子密码术取得了很大的进展。
- 1993年，美国的los Almos国家实验室的Hughes等人采用两台M-Z干涉仪，但使用B92协议，使用衰减为0.3db/km光通信光纤，性能更好的InGaAs探测器，他们成功的在48km的地下光缆中进行了密钥传送，误码率为9.3%。
- 而在自由空间中，传输的最远距离为1.9km，是由英国人Rarity等完成的。
- 量子密钥在光纤网络中分配也是可行的。

量子密钥 QK

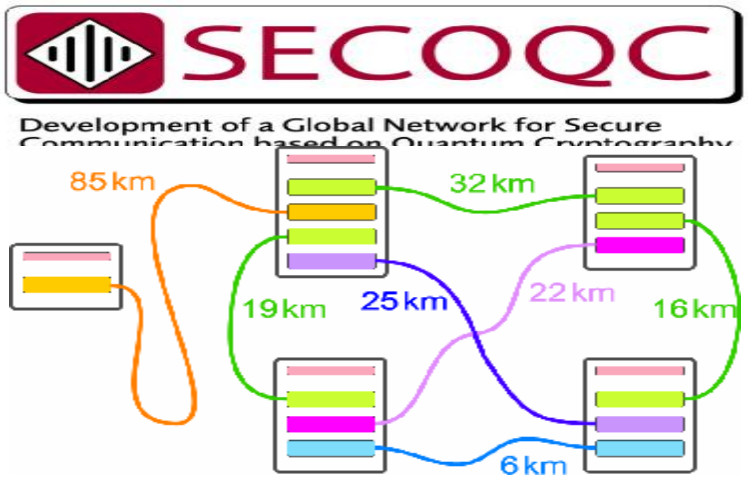
- 中国科学技术大学合肥微尺度物质科学国家实验室
  - 2006年实现诱骗态量子密钥分发实验
  - 2008年 世界上首个3节点链状光量子电话网
  - 2010年 将通信距离扩大到了97公里
  - 。 。 。 。

QKD 网络

美国(2005)

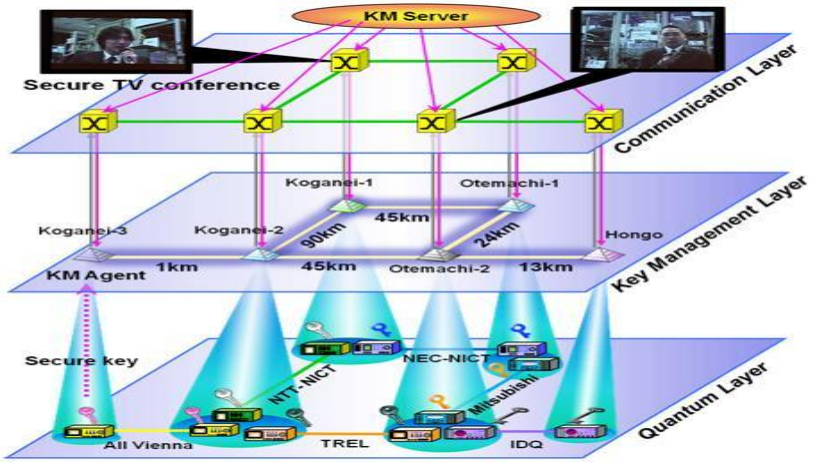


欧盟(2008)



中国(2009)USTC

日本(2010)



商业化QKD系统

美国， MAGIQ TECH.

瑞士， ID QUANTIQUE

中国，安徽问天量子科技股份有限公司

量子密码术的技术挑战

- 量子密码术的实现还有一些技术问题，具体有以下几个方面
- 光子源：难以实现真正的单光子脉冲。
- 信息通道：目前还没有理想的单模光纤。
- 单光子探测器：预计会在不久的将来出现商用的红外单光子探测器。

量子密码通信系统的前景及方向

- 量子密码通信的新领域：如签名，身份认证等
- 增加传输距离：这样才会有更大的发展空间。
- 提高比特传输率。
- 小型化，集成化。

USTC SIST 23