密码理论与技术

典型安全协议概览

数字签名方案的应用：公钥证书

(续上一讲)

- 问题：

  如何将公钥与持有者可靠地联系起来？

工具：公钥证书及其管理协议(x.509/RFC2553)

机制：发布者对下辖用户的公钥做数字签名

用户#i的公钥证书$M(i)$是包含其公钥PK(i)及其安全属性的电子文件。

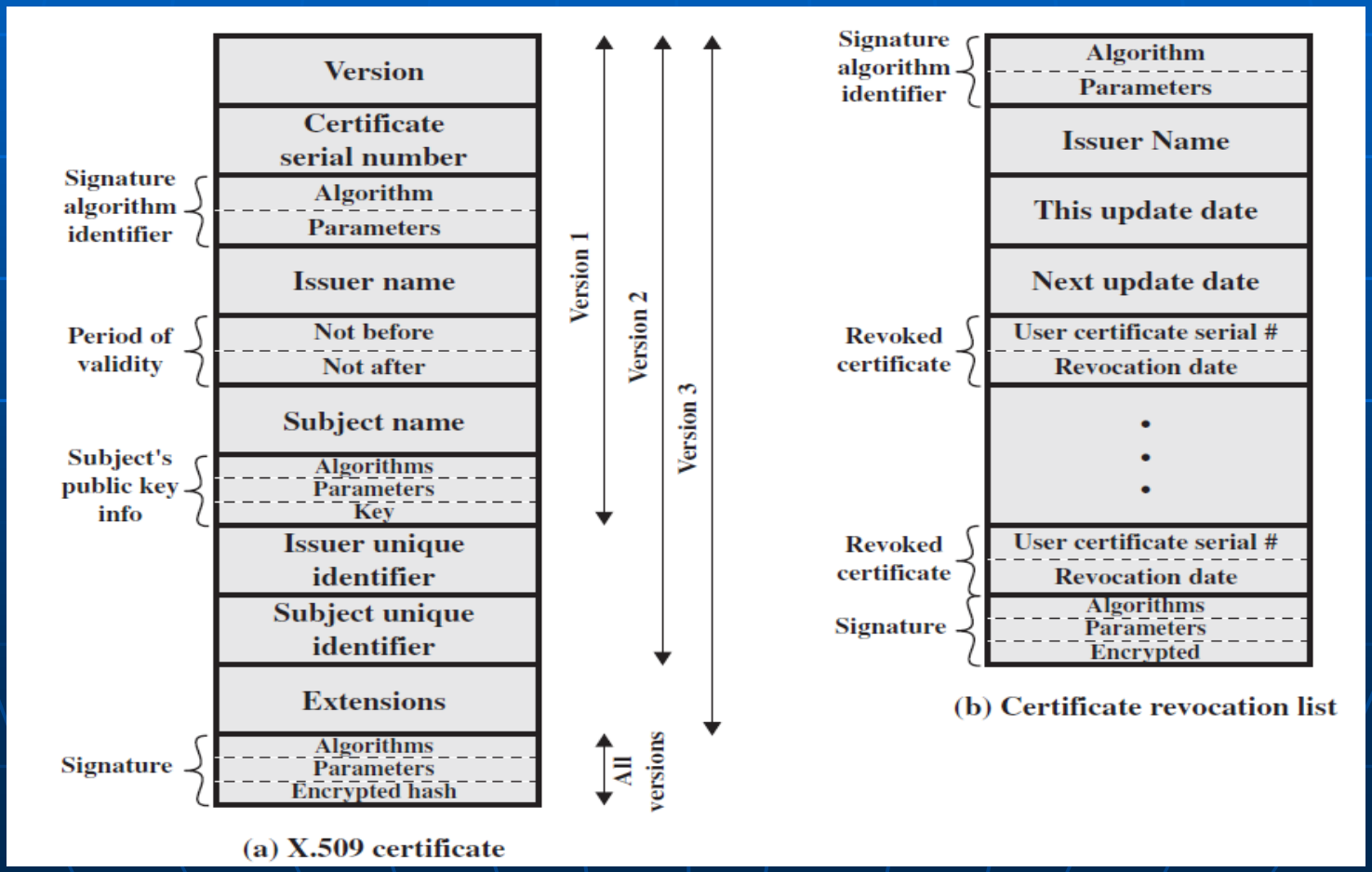
公钥发布者A以期私钥 sk(A) 生成数字签名$\sigma(i)$ =Sig(sk(A), $M(i)$)。

发布者发布完整的证书文件[$M(i)$, $\sigma(i)$]。

公钥PK(i)的使用者用A的公钥vk(A)验证证书文件的数字签名。

数字签名方案的应用：公钥证书

- 公钥证书数据结构的IT标准：
- X.509/RFC2559, 参阅Stalling 14.4



其他基础类安全方案(1)

“让我们设计一个多方保密通信的方案”。
“呀...这可是个新问题！”

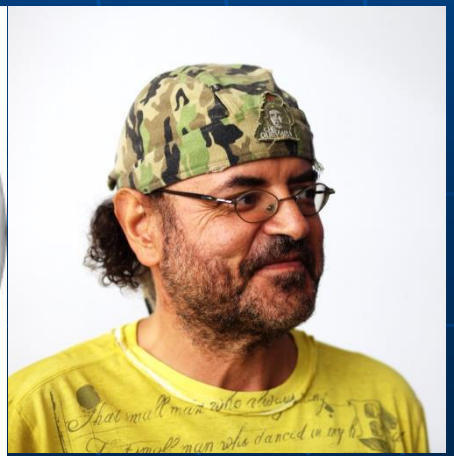
- 无须公钥证书的公钥加密方案
- 无须公钥证书的签名方案
- (2001, Pairing-based/ECC, Identity-based Crypt.)
- 组群加密方案
- 组群签字方案 (2000, Group Crypt.)
- 密钥时变加密方案
- 密钥时变签字方案
- 等

“让我们设计一个密钥能够自动随时间更新的签字方案”。
“呀...这可是个新问题！”

其他基础类安全方案(2)

- IBE(Identity-based Encryption)：通用框架

- 一个IBE方案Π=(Setup, UKG, E, D)是一组算法，其中：
- (1)Setup是全局密钥生成算法，输出全局公钥-私钥偶(mpk, msk)；
- (2)UKG是用户私钥生成算法，以全局私钥msk、用户身份标识*a*为输入，输出*a*的私钥usk(*a*)；
- (3)E是加密算法，以全局公钥mpk、用户身份标识*a*和消息M为输入并输出密文y；
- (4)D是解密算法，以全局公钥mpk、用户私钥usk(*a*)和密文y为输入并输出明文M。



IBE之父：D.Boneh & Franklin

其他基础类安全方案(3)

- IBE(Identity-based Encryption)：通用框架(续)

- (1)所有以上算法须满足一致性关系：对任何k、a和M，若
- P[(mpk,msk)←Setup(k);
- usk(a)←UKG(msk,a);
- y←E(mpk, a, M);
- 则　　D(mpk, usk(a), y)=M]=1恒成立
- (2)由于IBE方案的特殊结构，在刻画其保密性质时需要考虑所谓合谋攻击，这时攻击者可能(通过非法入侵或合谋)持有某些合法用户a^1,…,a^n的私钥usk(a^1),…usk(a^n).
- **IBE方案的保密性要求**：如果攻击者不持有私钥usk(a)，无论事先能获得多少usk(a^1),…usk(a^n)(a^1,…,$a^n \neq a$)都无法从密文E(mpk, a, M)有效获取关于明文M的信息。

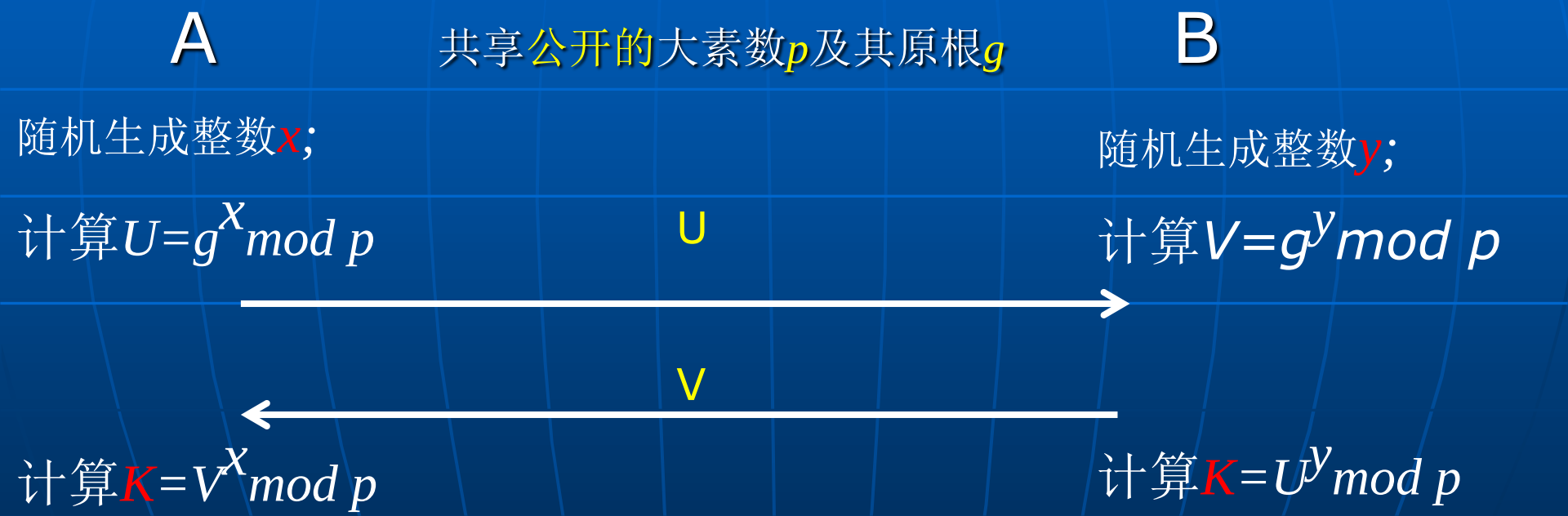
典型的网络安全协议类

- 密钥交换协议
- 密钥分配协议
- 身份认证协议
- 带身份认证的密钥交换协议
- 基于口令的认证-密钥交换协议
- 组群安全协议
- 零知识证明协议

D.Boneh， O.Goldreich，R.Conneti

密钥交换原理

- 问题:如何通过公共网络在线生成共享密钥?
- 例子:*Diffie-Hellman*协议:



(1) **K = g^{xy} mod p就是共享的对称密钥！**

(2) 安全基础：计算性Diffie-Hellman问题难解。

本单元其余课时内容预告

- 典型公钥加密方案：教程第9章、第10章10.1~10.2
- 其他公钥加密方案：补充内容
- 混合加密方案：补充内容
- 数字签名方案：教程13.1~13.3
- 对称型数据认证类方案：
- 教程11.1~11.5、12.1~12.4
- （本章HMAC等算法以理解为主，不须记忆）