

Email Security

Yuan Xue



Big Picture

- ◆ Application/Transport layer based solutions
 - Secure network-based applications
 - ◆ Web – SSL, transportation layer solution
 - ◆ Email – PGP, application layer solution
- ◆ Network/Link layer based solutions (next class)
 - Secure network + support for application
 - ◆ IPsec
 - ◆ Internet Security
 - BGP security
 - ◆ Wireless Security
 - IEEE 802.11 security



Top down Approach

Bigger Picture

◆ Approach to Network Security

- Cryptographic Approach
 - ◆ Encryption
 - ◆ Authentication
 - ◆ Digital Signature
- Authentication Protocol
- Network Approach
 - ◆ Routing control
- System Approach
 - ◆ Intrusion detection systems
 - ◆ Firewall
 - ◆ Access Control

◆ Beyond network security

- System Security
- Program Security



Outline

◆ PGP

- Link the security principle with design practice

◆ S/MIME

◆ Spam

- Get to know some non-cryptographic approaches



Pretty Good Privacy

◆ Overview

- [Phil Zimmermann](#) in 1991
- Open PGP
 - ◆ Open Standard followed by PGP, GnuPG
- PGP vs. GnuPG
 - ◆ PGP goes commercial in 1996
 - ◆ GnuPG is a free replacement for PGP

◆ Basics

- Select the existing cryptographic algorithms as building blocks
- Build a general-purpose application that is independent of OS

◆ Operations

- Encryption
- Signature
- Key management



Overview

◆ Key Generation

- A pair of public and privacy keys

◆ Key Distribution

- Fingerprint
- Web of Trust

◆ Key Storage

- Import/export

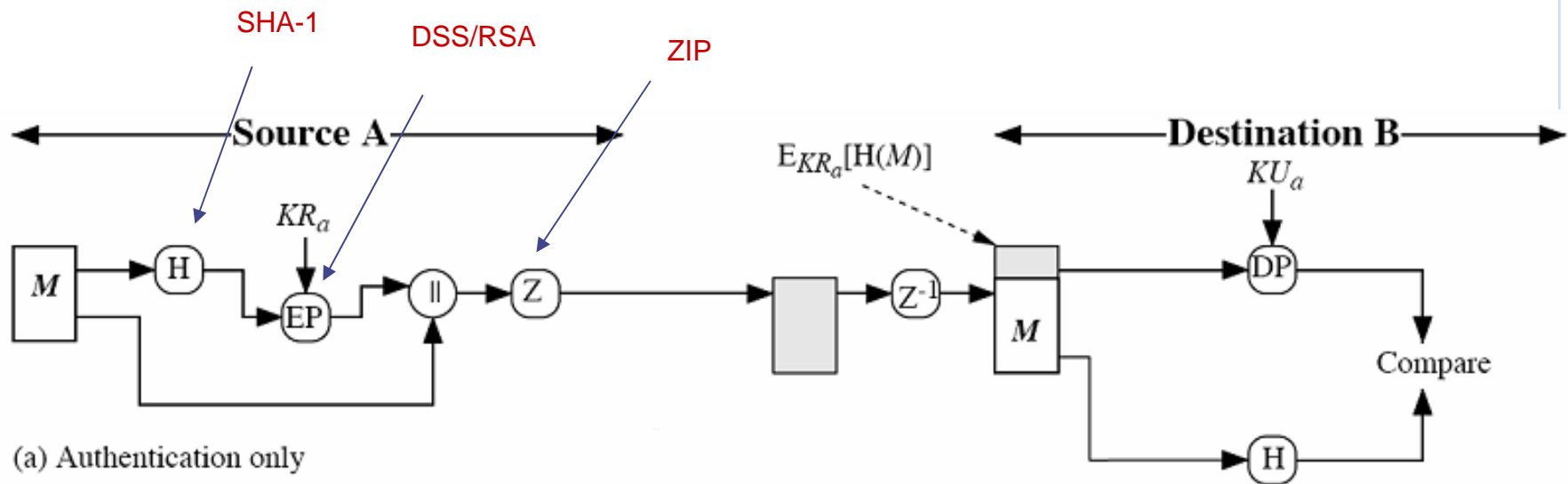
◆ Security Operations

- Encryption
- Message Authentication
- Signature and Verification

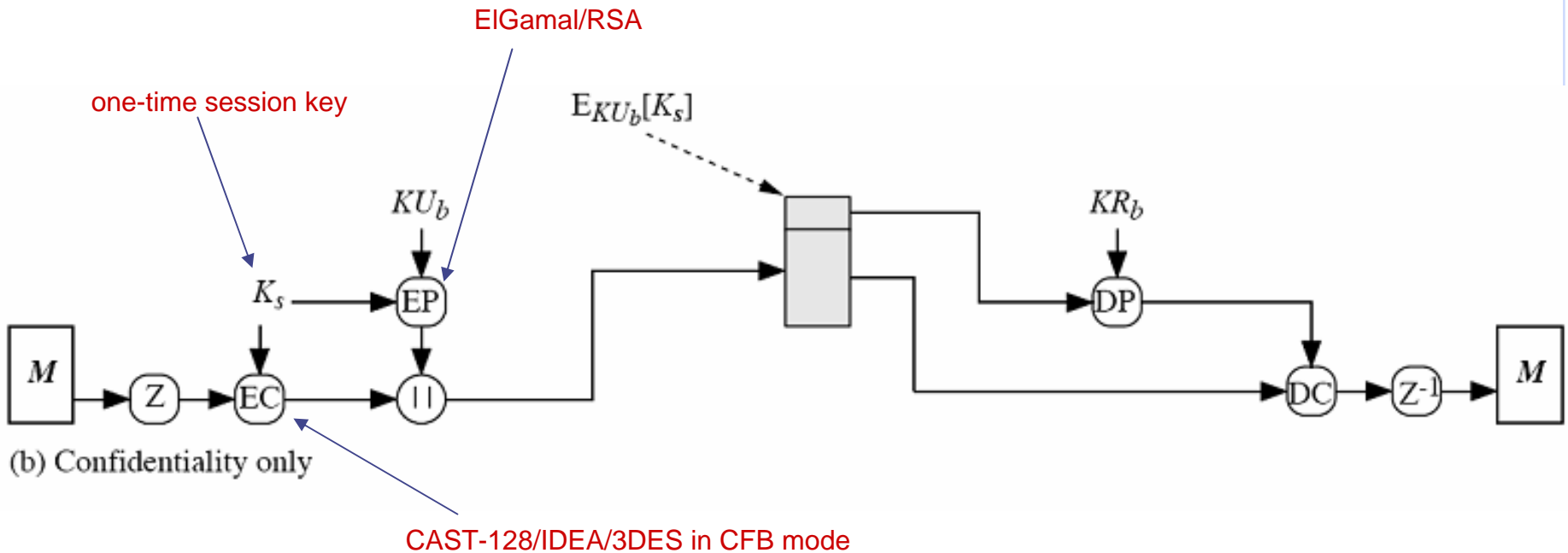
Start with



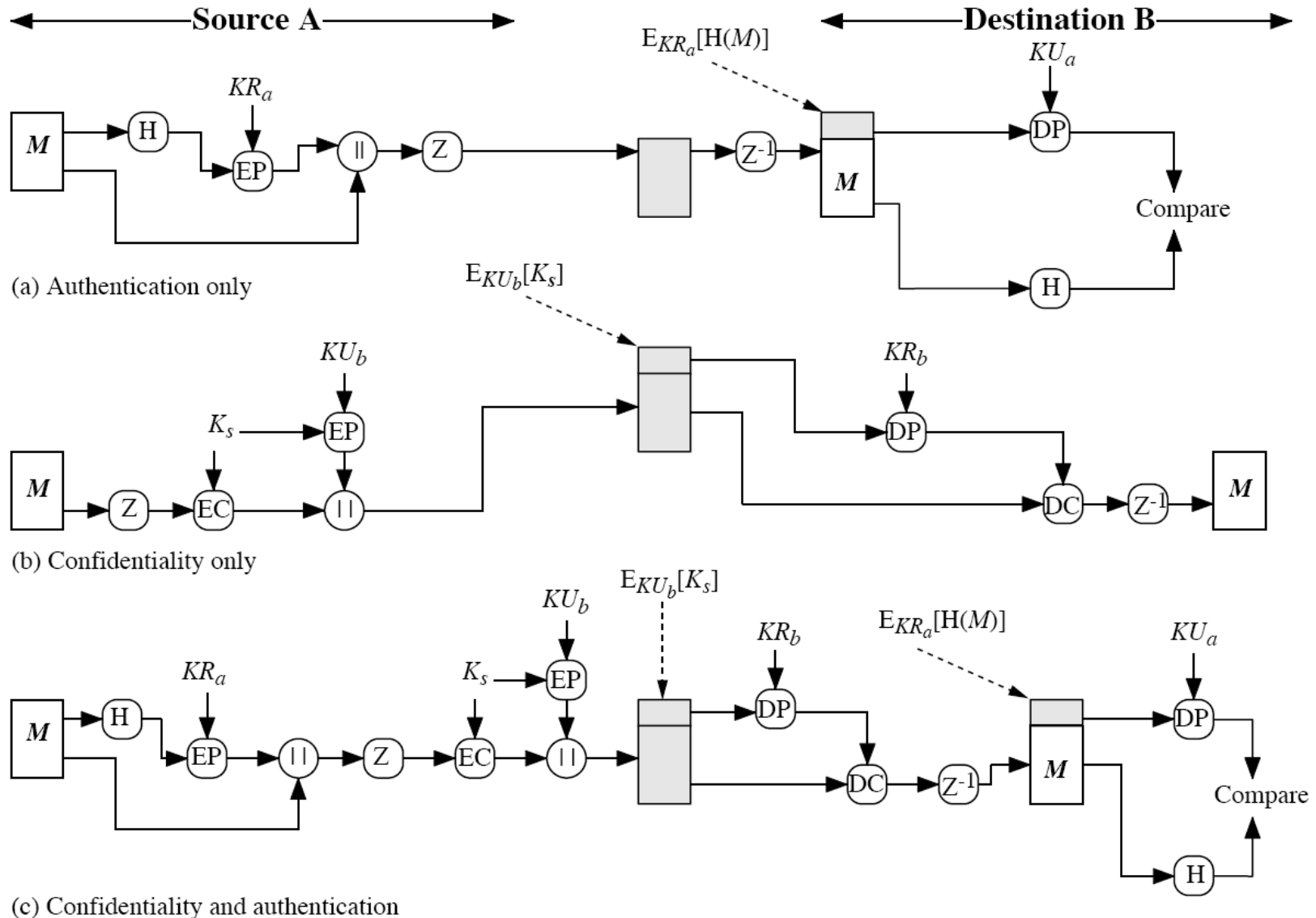
Operation -- Authentication



Operation -- Encryption



Operation – Put two together



Details

◆ Compression

- Signature before compression
 - ◆ Convenience of future verification
 - ◆ Flexibility in compression algorithm choice
- Message encryption after compression
 - ◆ Less redundancy in plaintext strengthen cryptographic security

◆ Email Capability

- Usage of ASCII in Email
- Converting 8-bit binary code to ASCII characters
- Radix-64 conversion
 - ◆ 3 octets of binary code → 4 ASCII characters
 - ◆ 33% expansion + compression offset

Keys

◆ Types

- Public and private key pair
- One-time session symmetric key

◆ Issues

- Key generation
- Key storage
- Key management (distribution)



Key Identifier

- ◆ A user may have multiple keys
- ◆ Which key is used?
 - Which key encrypts the session key
 - Which key signs the document
- ◆ Need an ID
 - Unique to user ID with very high probability
 - Key ID of $KU_a = KU_a \bmod 2^{64}$



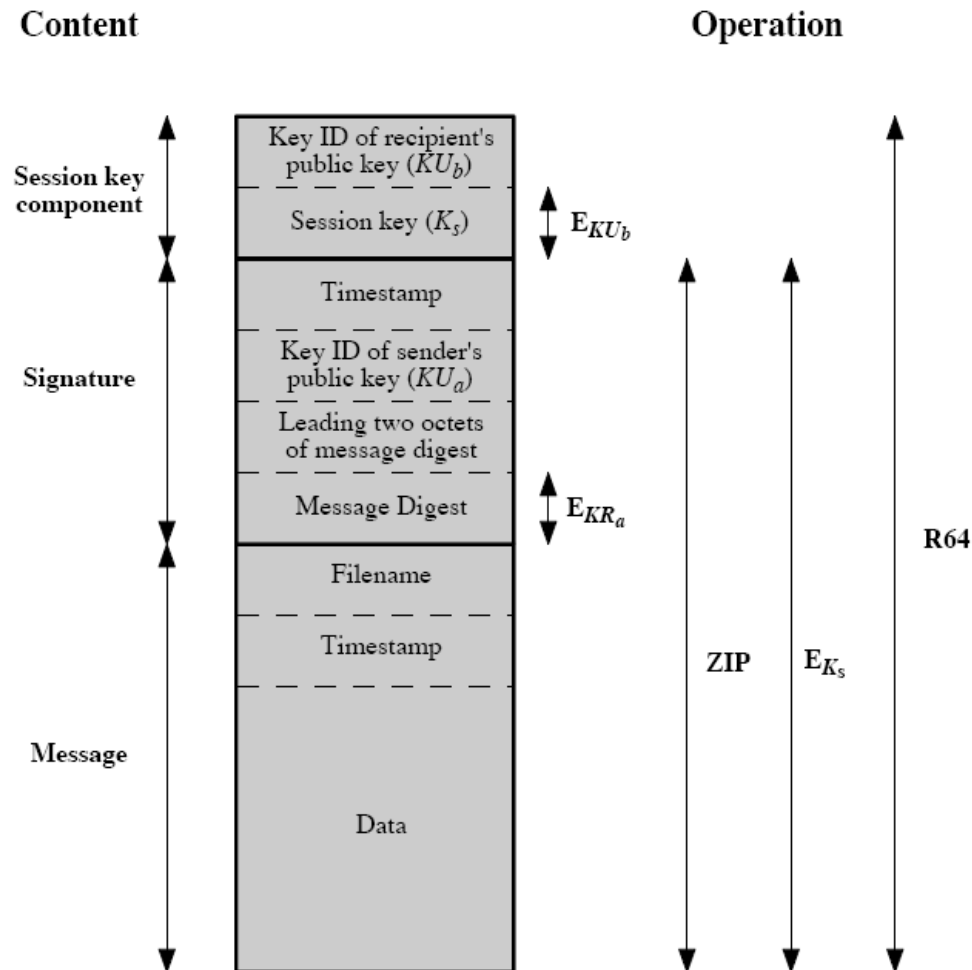
Key Generation

◆ Session Key Generation

- Generating unpredictable session keys
- E.g., 128-bit CAST key
- Two 64-bit blocks encrypted by a 128-bit key in CFB mode → two 64-bit ciphertext as the 128-bit session key
- Two 64-bit blocks from a 128-bit random stream based on keystroke input from the user
- Previous session key and the random stream forms the 128-bit key input



PGP Message Format



Key Storage

- ◆ Key Ring
- ◆ Secure the private key with passphrase
 - Passphrase → hash code via SHA-1
 - Encrypt the private key via CAST-128/IDEA/3DES with the hash code as the key
 - Store the encrypted private key

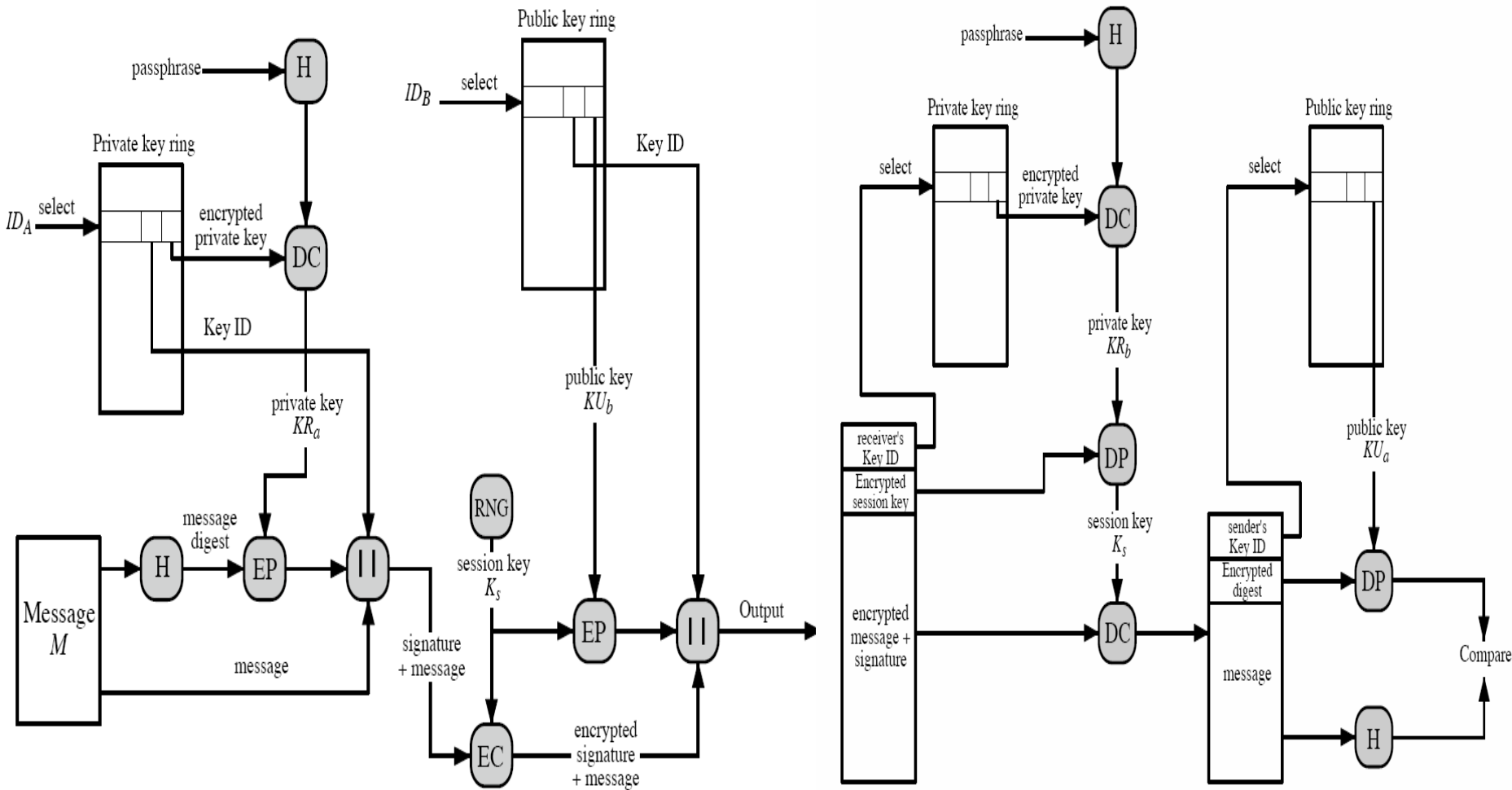
Private Key Ring

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
⋮	⋮	⋮	⋮	⋮
T_i	$KU_i \bmod 2^{64}$	KU_i	$E_{H(P)}[KR_i]$	User i
⋮	⋮	⋮	⋮	⋮

Public Key Ring

Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
T_i	$KU_i \bmod 2^{64}$	Ku_i	trust_flag $_i$	User i	trust_flag $_i$		
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

* = field used to index table



Put things together

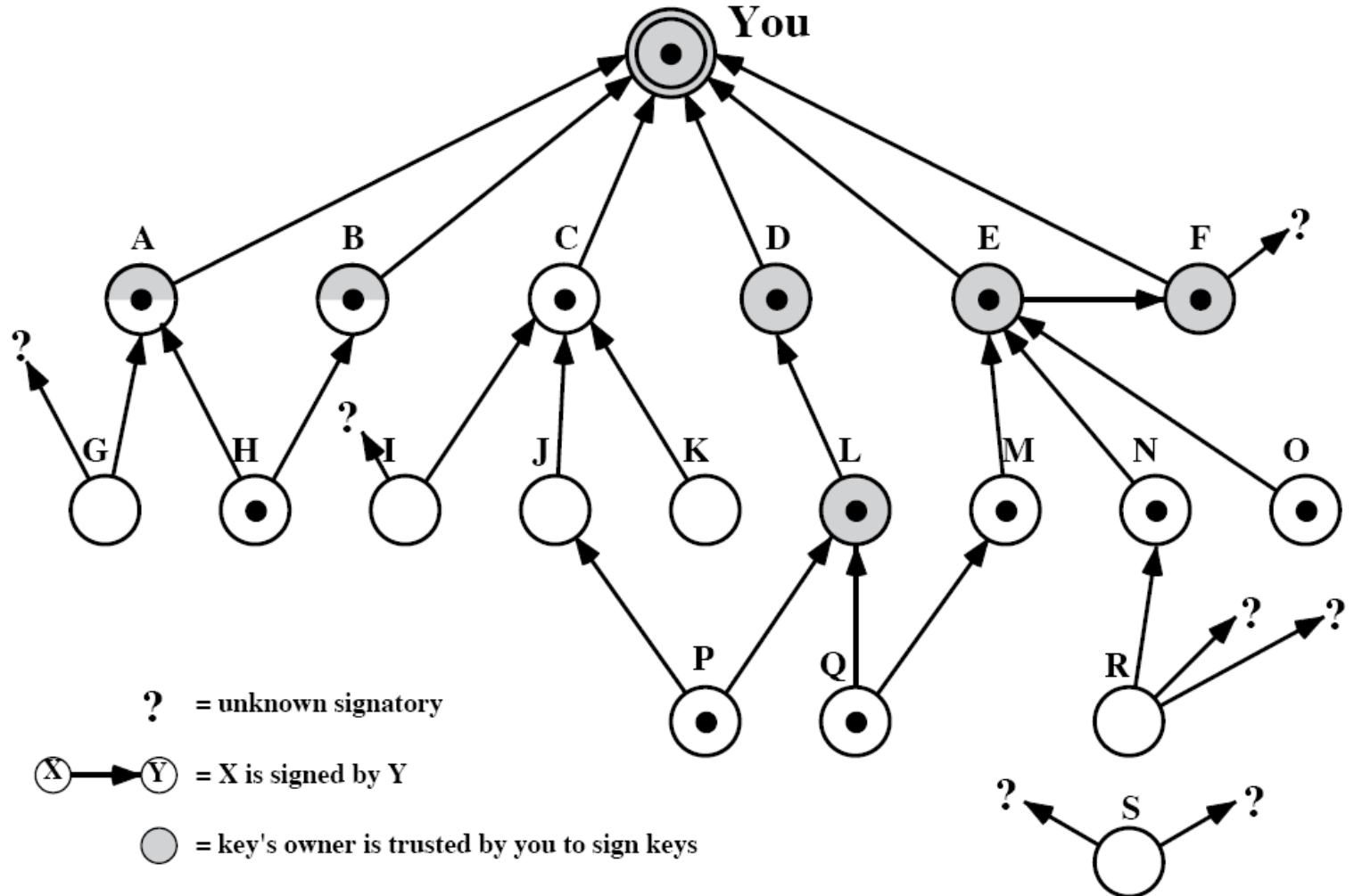


Key management

- ◆ Direct Verification
 - Physical delivery
 - Fingerprint
- ◆ Trusted Third Party
 - Signed certificate of a key
- ◆ Web of Trust
 - A self-organized trust management mechanism
- ◆ Revoke Public Key
 - Key revocation certificate



Example



? = unknown signatory

(X) → (Y) = X is signed by Y

● = key's owner is trusted by you to sign keys

◐ = key's owner is partly trusted by you to sign keys

● = key is deemed legitimate by you

S/MIME

◆ Background

- RFC 822
- MIME – Multipurpose Internet Mail Extension
- S/MIME – Secure/Multipurpose Internet Mail Extension

◆ PGP vs. S/MIME

- Both are official email security systems which are currently NIST specified standards
- Similar design, but not compatible with each other
- PGP -- personal email security
- S/MIME – commercial use

Spam

◆ Spam

- Unsolicited bulk email
- 10% of the incoming message in 1997

◆ Anti-spam

- Blacklist of frequent spammer
- Lists of trusted user
- Keyword pattern matching
- Machine learning
 - ◆ Bayesian Network