Public-Key Certificates

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 4

ravi.utsa@gmail.com
www.profsandhu.com

Public-Key Certificates

- authenticated distribution of public-keys
- public-key encryption
  - sender needs public key of receiver
- public-key digital signatures
  - receiver needs public key of sender
- ~~public-key key agreement~~
  - ~~both need each other's public keys~~

X.509v1 Certificate

VERSION

SERIAL NUMBER

SIGNATURE ALGORITHM

ISSUER (Certificate Authority)

VALIDITY

SUBJECT

SUBJECT PUBLIC KEY INFO

SIGNATURE

X.509v1 Certificate

1
1234567891011121314
RSA+SHA-3, 2048
C=US, S=TX, O=UTSA, OU=CS
1/1/17-12/31/18
C=US, S=TX, O=UTSA, OU=CS, CN=Ravi Sandhu
RSA, 2048, xxxxxxxxxxxxxxxxxxxxxxxxxxx
SIGNATURE

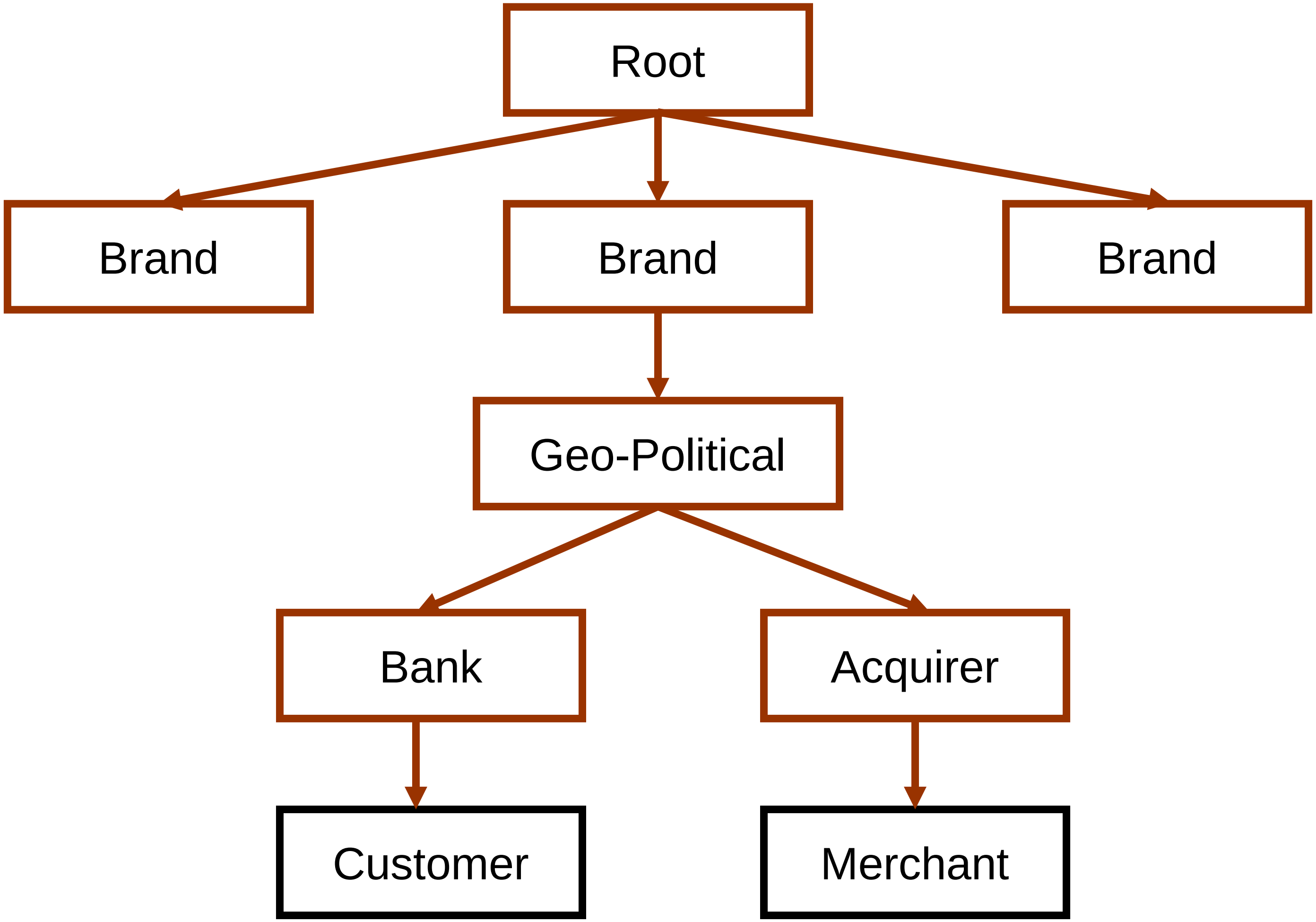
Certificate Trust

- how to acquire public key of the issuer to verify signature
- whether or not to trust certificates signed by the issuer for this subject
  - prefix rule is not universally applicable

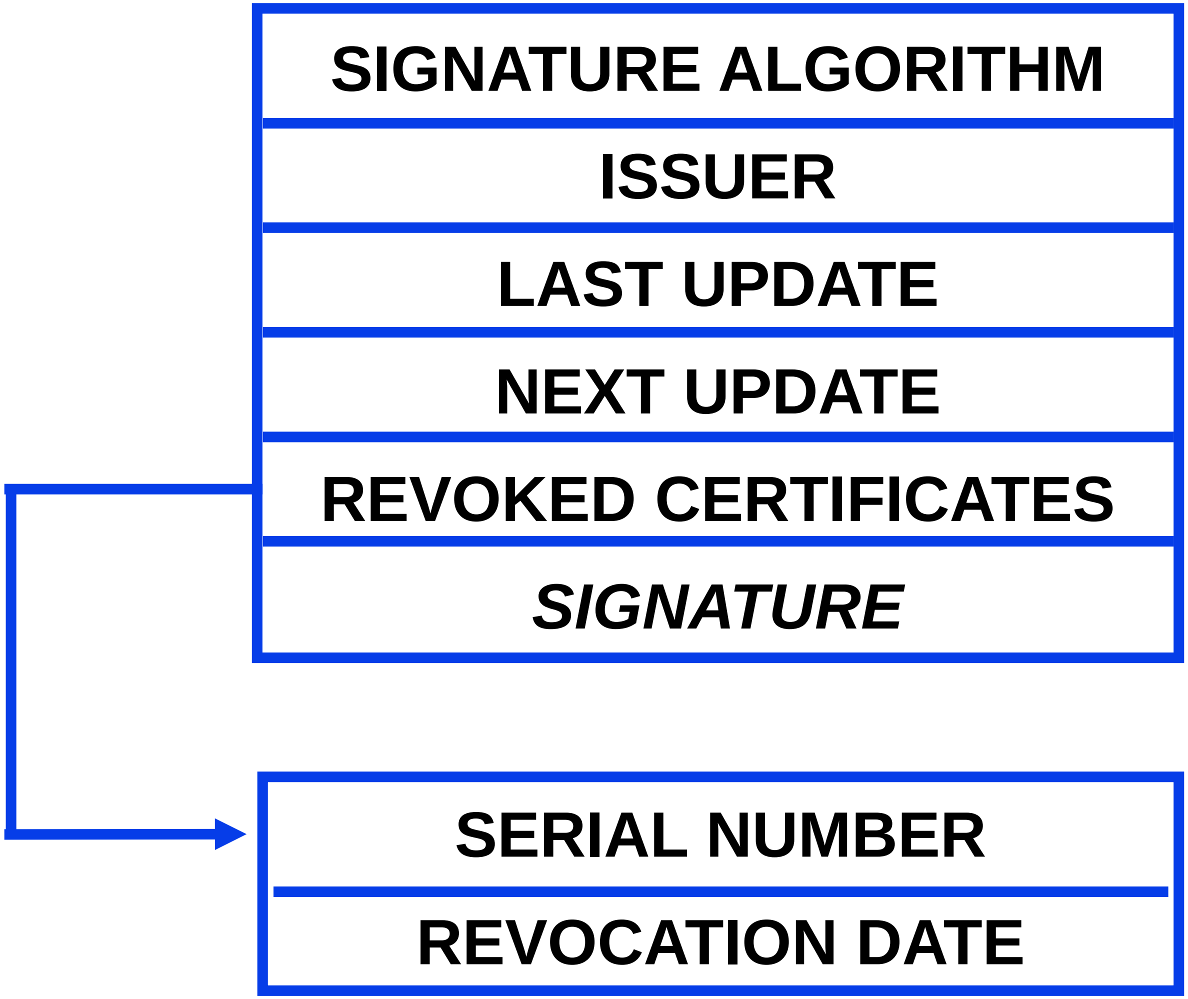
X.509v1 Certificate

1
1234567891011121314
RSA+SHA-3, 2048
C=US, S=VA, O=GMU, OU=ISE
1/1/17-12/31/18
C=US, S=TX, O=UTSA, OU=CS, CN=Ravi Sandhu
RSA, 2048, xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
SIGNATURE

SET CA Hierarchy



Certificate Revocation Lists (CRLs)



SIGNATURE ALGORITHM

ISSUER

LAST UPDATE

NEXT UPDATE

REVOKED CERTIFICATES

SIGNATURE

SERIAL NUMBER

REVOCATION DATE

X.509 Certificates

- X.509v1
  - very basic
- X.509v2
  - adds unique identifiers to prevent against reuse of X.500 names
- X.509v3
  - adds many extensions
  - can be further extended

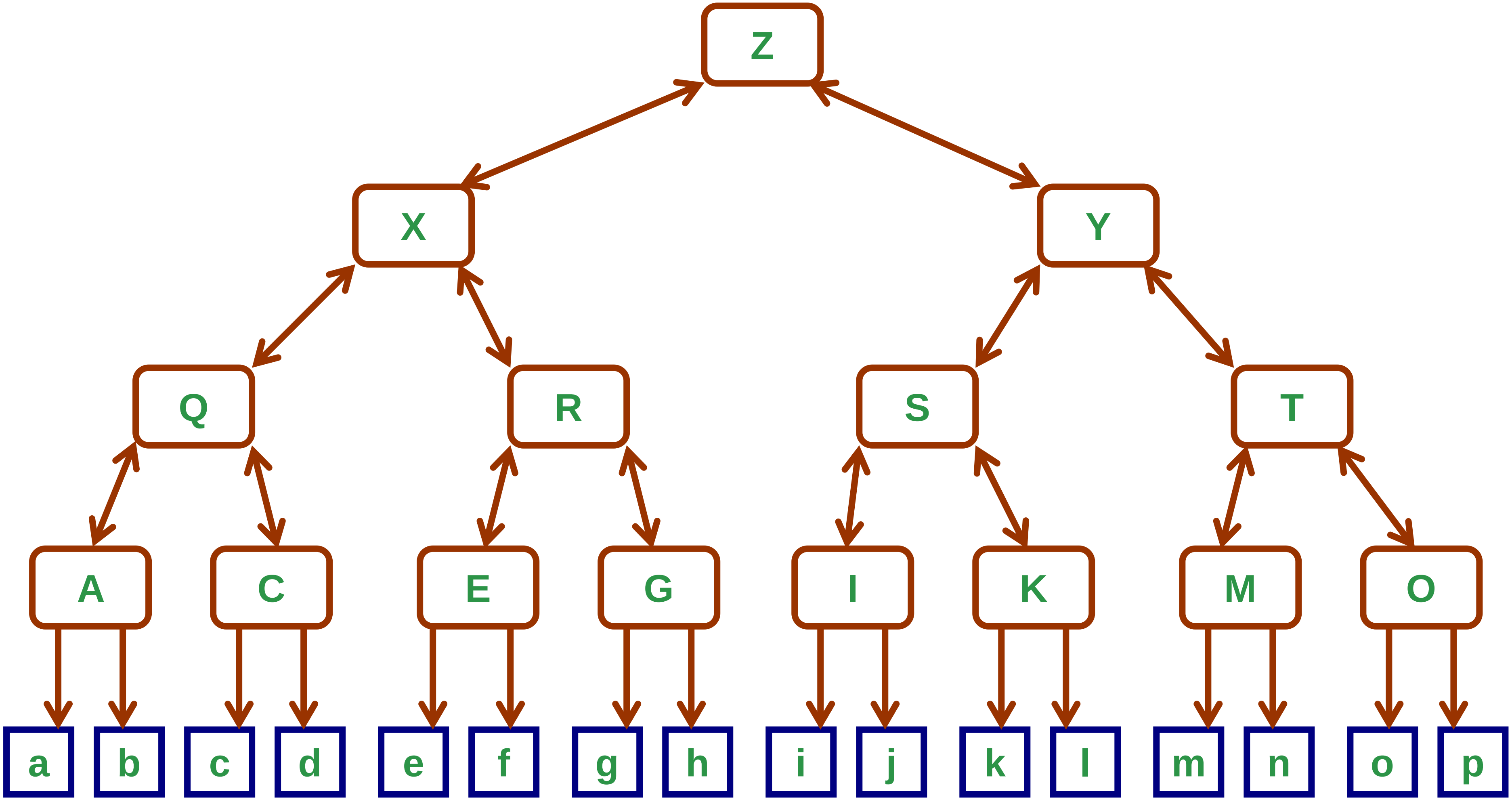
X.509v3 Innovations

- distinguish various certificates
  - signature, encryption, key-agreement
- identification info in addition to X.500 name
  - internet names: email addresses, host names, URLs
- issuer can state policy and usage
  - ok for casual email but not for signing checks
- extensible
  - proprietary extensions can be defined and registered
- attribute certificates
  - to enable attribute-based authorization

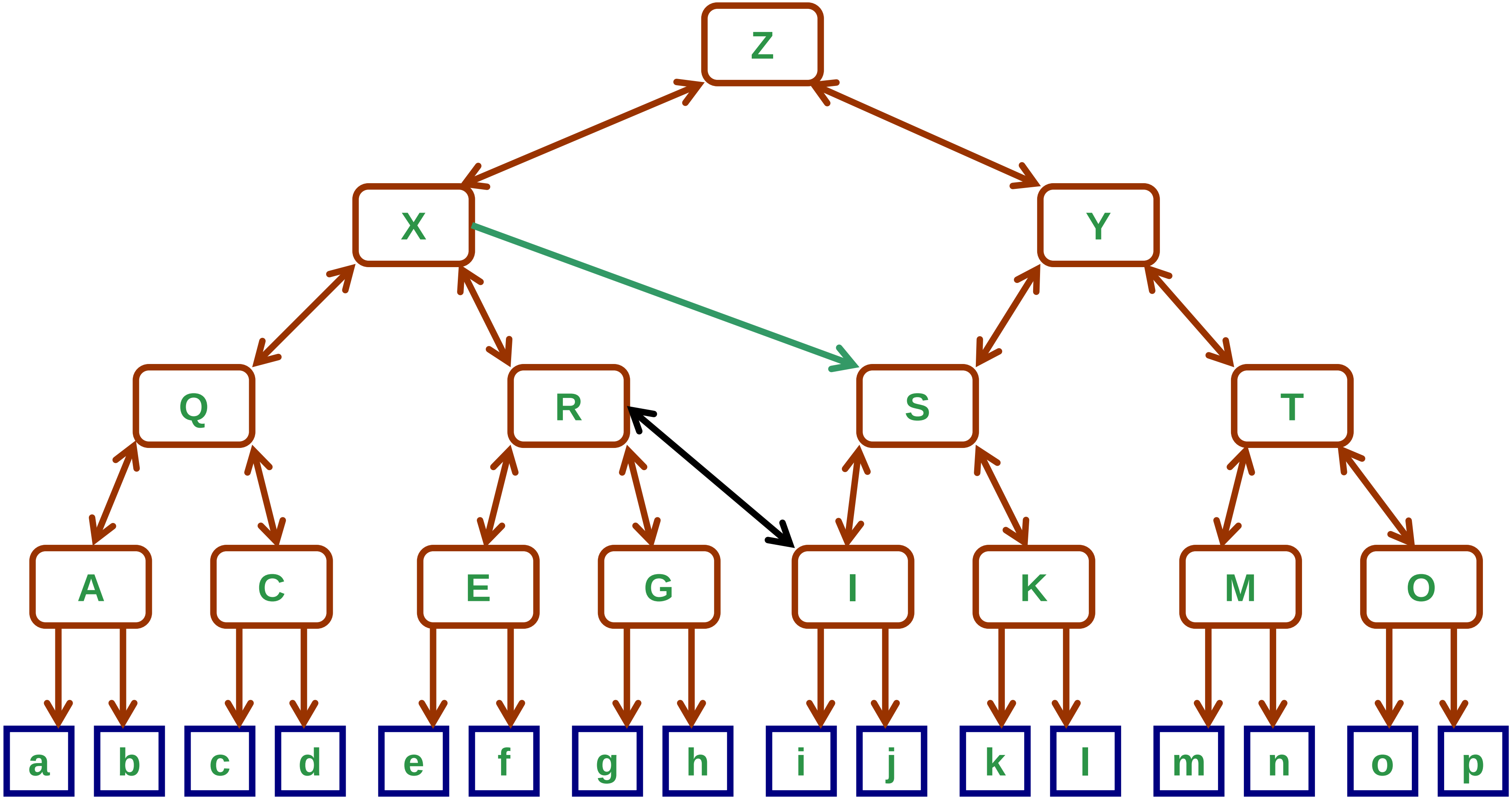
X.509v2 CRL Innovations

- CRL distribution points
- indirect CRLs
- delta CRLs
- revocation reason
- push CRLs

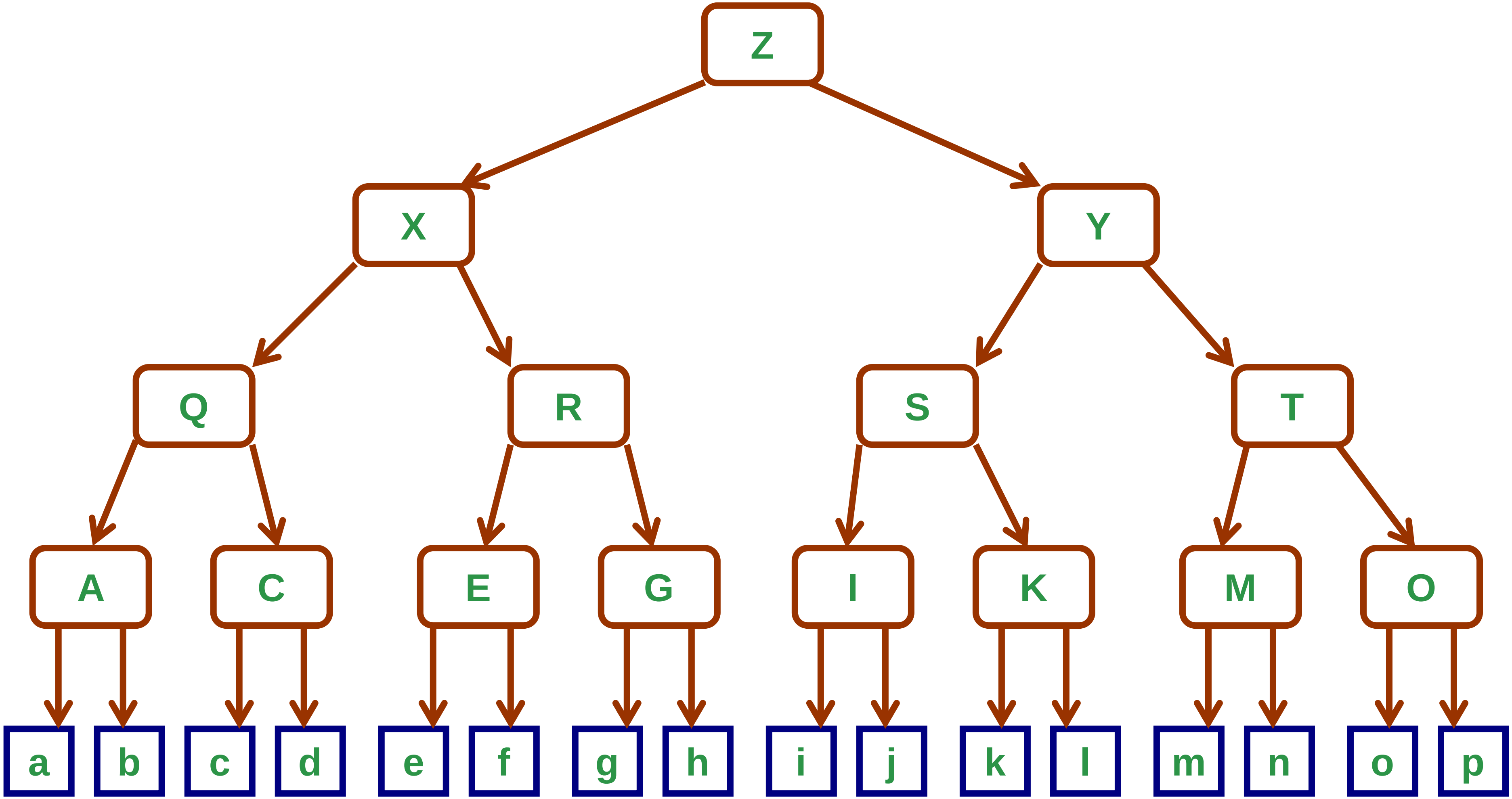
General Hierarchical Structure



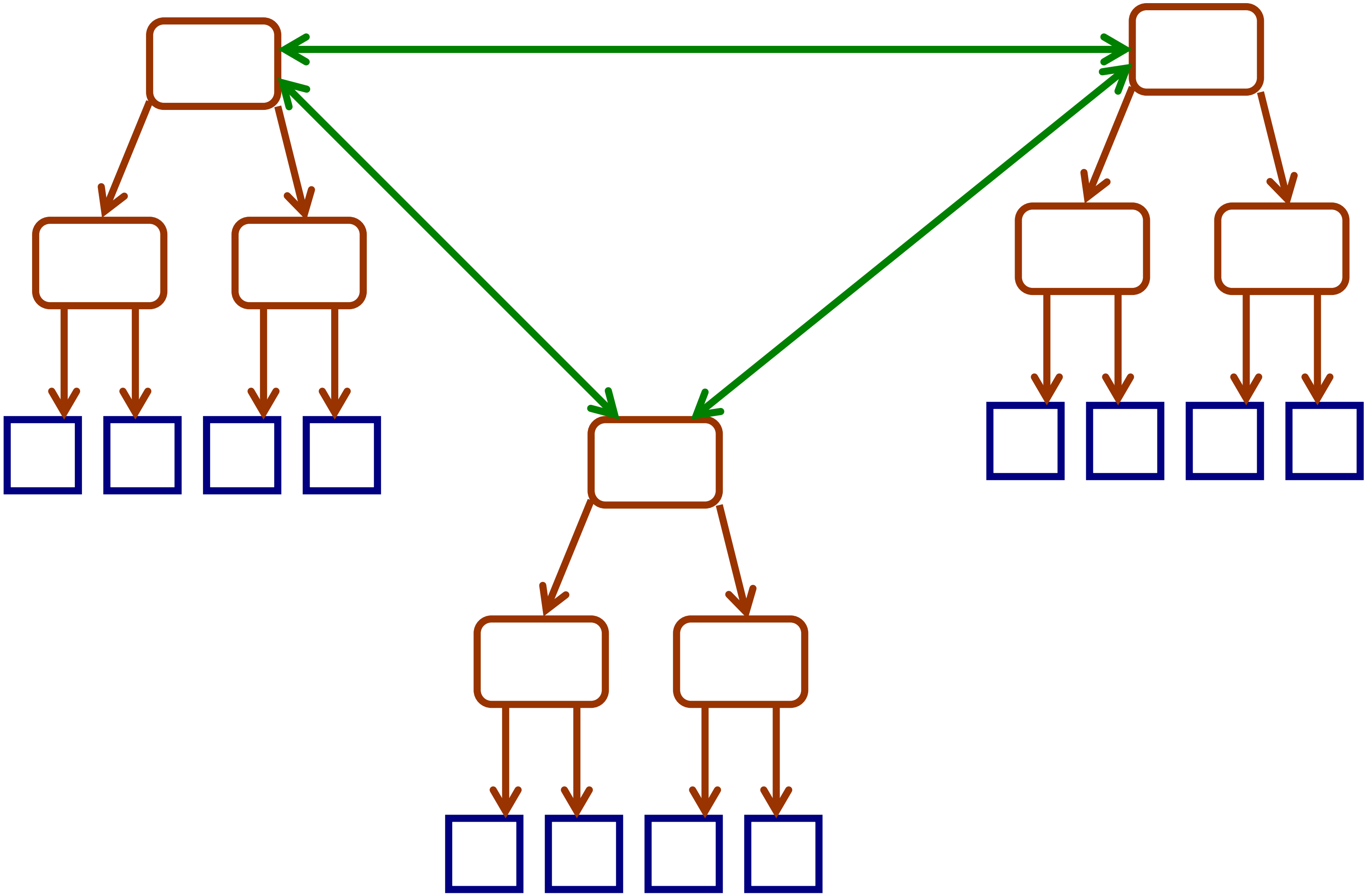
General Hierarchical Structure with Added Links



Top-Down Hierarchical Structure



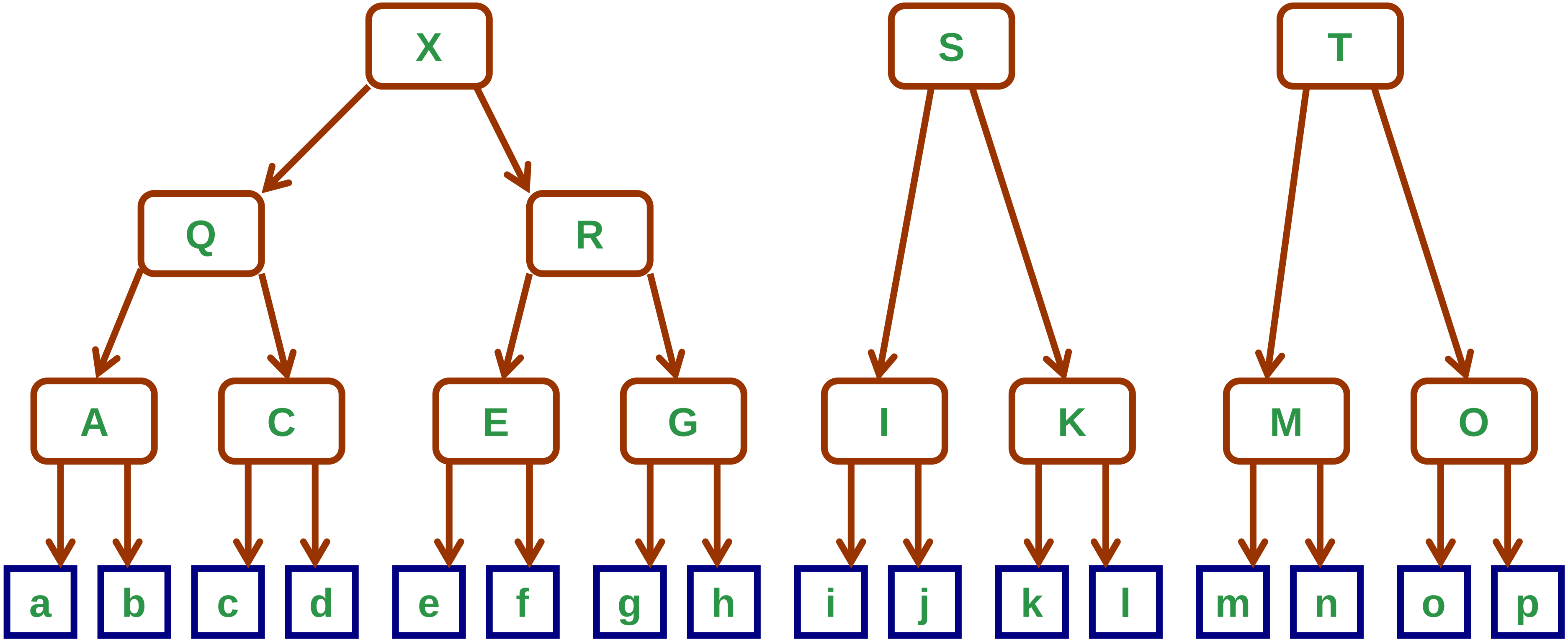
Forest of Hierarchies



© Ravi Sandhu

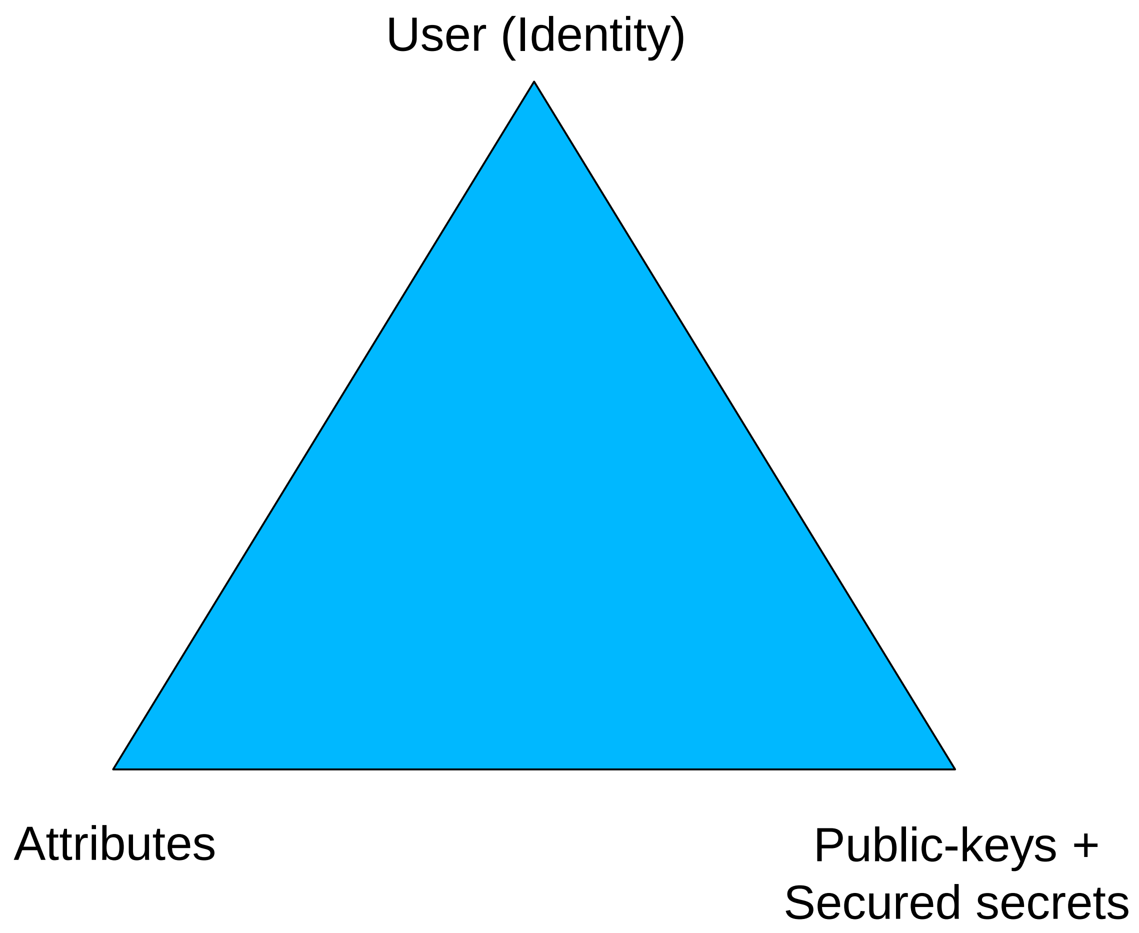
World-Leading Research with Real-World Impact!

Multiple Root CA's Plus Intermediate CA's



Model on the web today

Certificate Triangle



User (Identity)

Attributes

Public-keys +
Secured secrets

© Ravi Sandhu

World-Leading Research with Real-World Impact!