Public-Key Encryption
公钥加密(非对称加密)

密钥管理

Key Management

key distribution problems

- public-key encryption helps key distribution

- two aspects:
  - ✓ distribution of public keys
  - ✓ use of public-key encryption to distribute secret keys

Distribution of Public Keys

can be considered as using one of:

- public announcement of public-key(发布）
- publicly available directory （可访问目录）
- public-key authority（授权）
- public-key certificates （证书）

Public announcement of public-key(发布）

- users distribute public keys to recipients
  or broadcast to community
- major weakness is forgery （伪造）
  - anyone can create a key claiming to be someone else and broadcast it
  - until forgery is discovered can masquerade（假冒） as claimed user

Figure 10.1 Uncontrolled Public Key Distribution

publicly available directory （可访问目录）

greater security by registering keys with a public directory

- directory must be trusted with properties:
  - contains {name,public-key} entries
  - register securely with directory
  - replace key at any time
  - periodically published
  - accessed electronically

- still vulnerable（攻击） to tampering （篡改）or forgery （假冒）

注册公钥

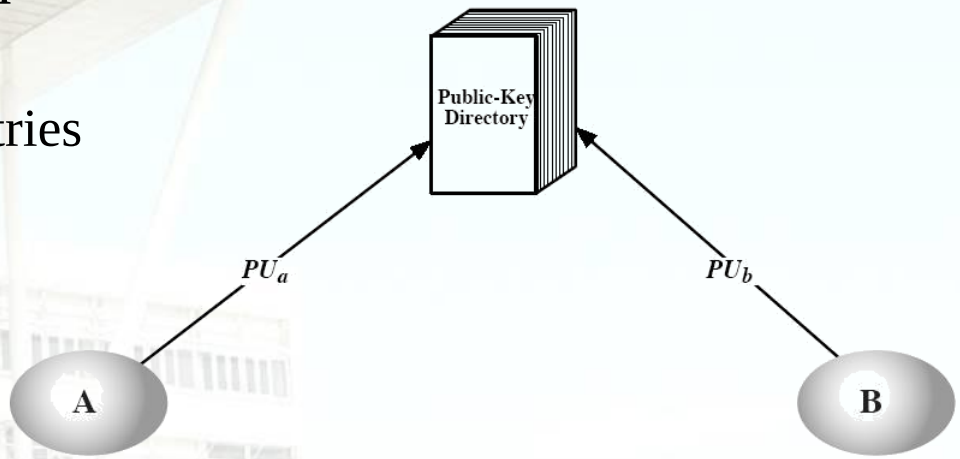
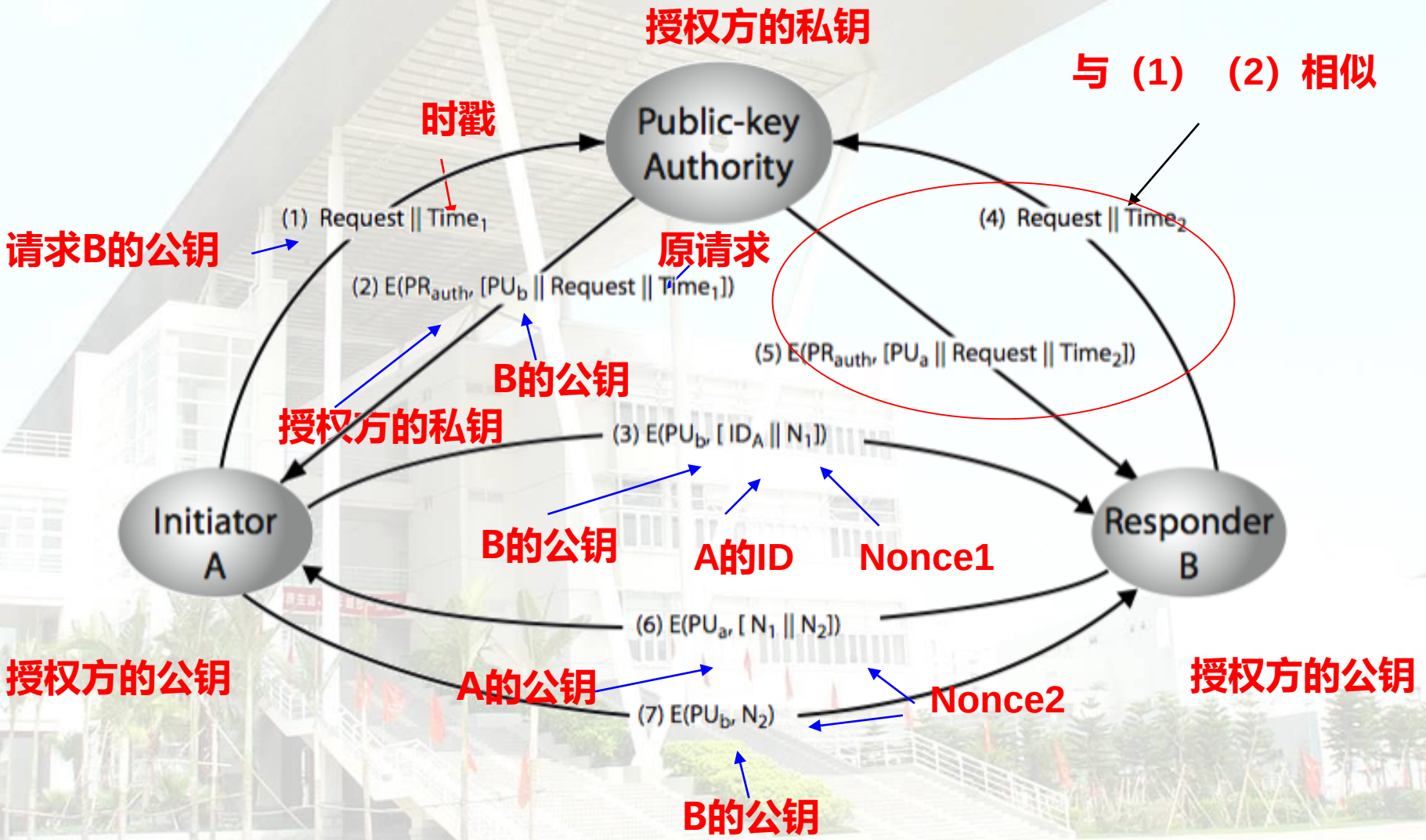


Figure 10.2 Public Key Publication

public-key authority（授权）

- tightening control（严密控制） over distribution of keys from directory
- requires users to know public key for the directory
- users interact with directory to obtain any desired public key securely

Public-Key Authority



public-key certificates （证书）

- allow key exchange without real-time access to public-key authority
- binds **identity** to **public key**
  - usually with other info such as period of validity, rights of use etc
- with all contents **signed** by a trusted（信赖）Public-Key or Certificate Authority (CA)
- can be verified by anyone who knows the public-key authorities public-key

Public-Key Distribution of Secret Keys

* use for secrecy or authentication

* public-key algorithms are slow
  usually use symmetric-key encryption to protect message contents
* need a session key

How to negotiate a suitable session key?

Simple Secret Key Distribution

- proposed by Merkle in 1979
  - "A" generates a new temporary public key pair
  - "A" sends "B" the public key and the identity
  - B generates a session key "K" sends it to "A" encrypted using the supplied A's public key
  - "A" decrypts the session key and will use for coming comm.
- problem is that an opponent can intercept（截取）and impersonate（模仿）

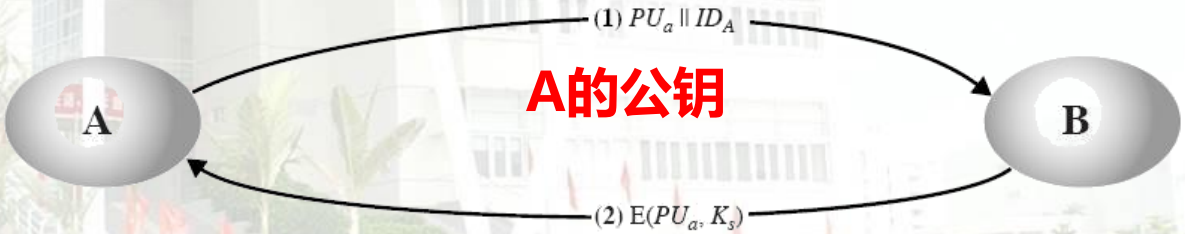


Figure 10.5 Simple Use of Public-Key Encryption to Establish a Session Key

Secret Key Distribution with confidentiality and authentication

- if have securely exchanged public-keys:

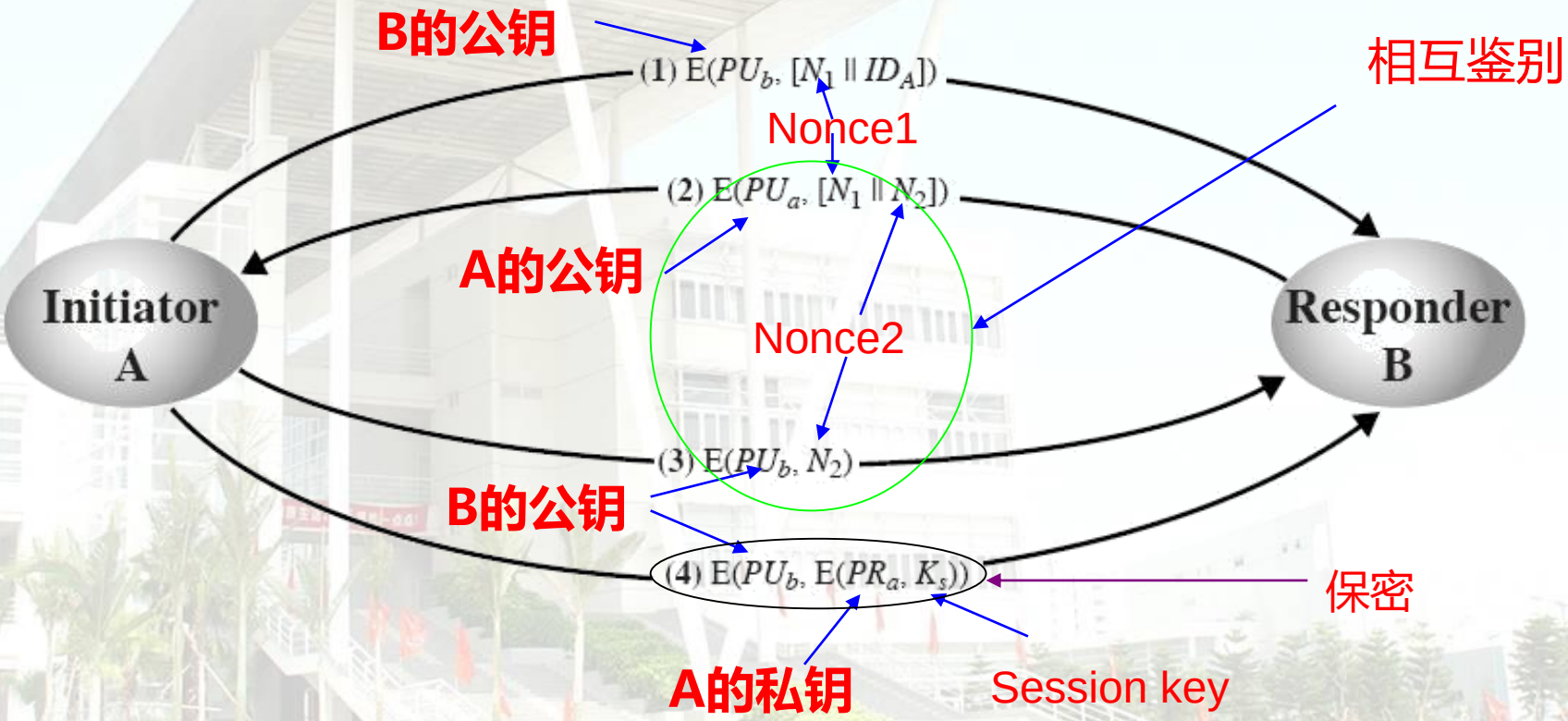


Figure 10.6 Public-Key Distribution of Secret Keys