TIME-SPECIFIC SIGNATURES IN THE ATTRIBUTE-BASED SETTING

4Feb2011

Madeline González Muñiz
(joint work with Peeter Laud)

Digital Signatures

- Schemes used to prove the following in a document:
  - Authenticity
  - Integrity
  - Non-repudiation
- Algorithms:
  - Key Generation Algorithm
  - Signing Algorithm
  - Verification Algorithm

Time-Specific Signatures

- In addition, we want the following possibilities:
  - Create a signature only during a specific time interval
    - Key generation authority
      - ID-based, attribute-based
    - Pre-computation may or may not be allowed
  - Verify a signature only during a specific time interval

Attribute-Based Signatures (ABS)

- Attribute authority gives keys to users based on their attributes

•Baseball player
•University student
•Computer science

•Salsa dancer
•University student
•Mathematics

Attribute-Based Keys

D_B
D_U
D_C

D_S
D_U
D_M

What if they want to join forces and sign using D_B and D_S?

Coalition Resistance

- Users may not combine secret keys to sign documents
- How does the attribute authority ensure this?

Lagrange interpolation

Lagrange Interpolation

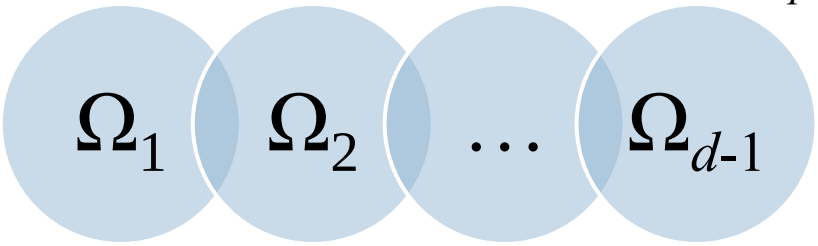
$f(D_B, D_U, D_C)$

$q(D_S, D_U, D_M)$

Different polynomials, but $f(0)=q(0)$

Key Generation

Default Attribute Set from Z_p



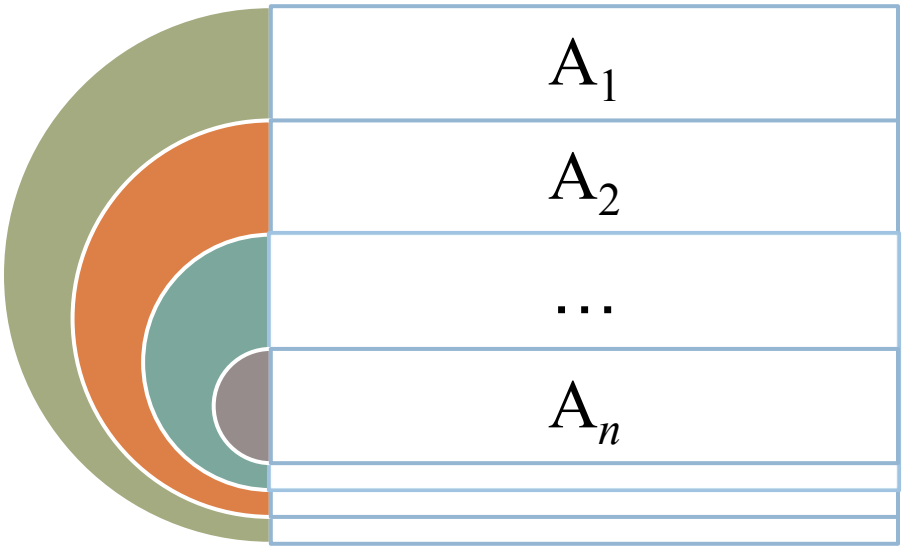
- Polynomial q of degree d-1 is chosen at random with $q(0)=x$
- g^x is the attribute authority public key
- D_i is the secret key for attribute i in $\omega \cup \Omega$
  - Each D_i is constructed using $q(i)$ in the exponent
  - Also, contains $\mathrm{H}_1(i)$ which is used in verification

Signing Predicate

Signer

Attributes

$\{a_1,\ldots,a_j\}$



Prove having k out of n attributes

Selecting Attributes

Select k-intersection

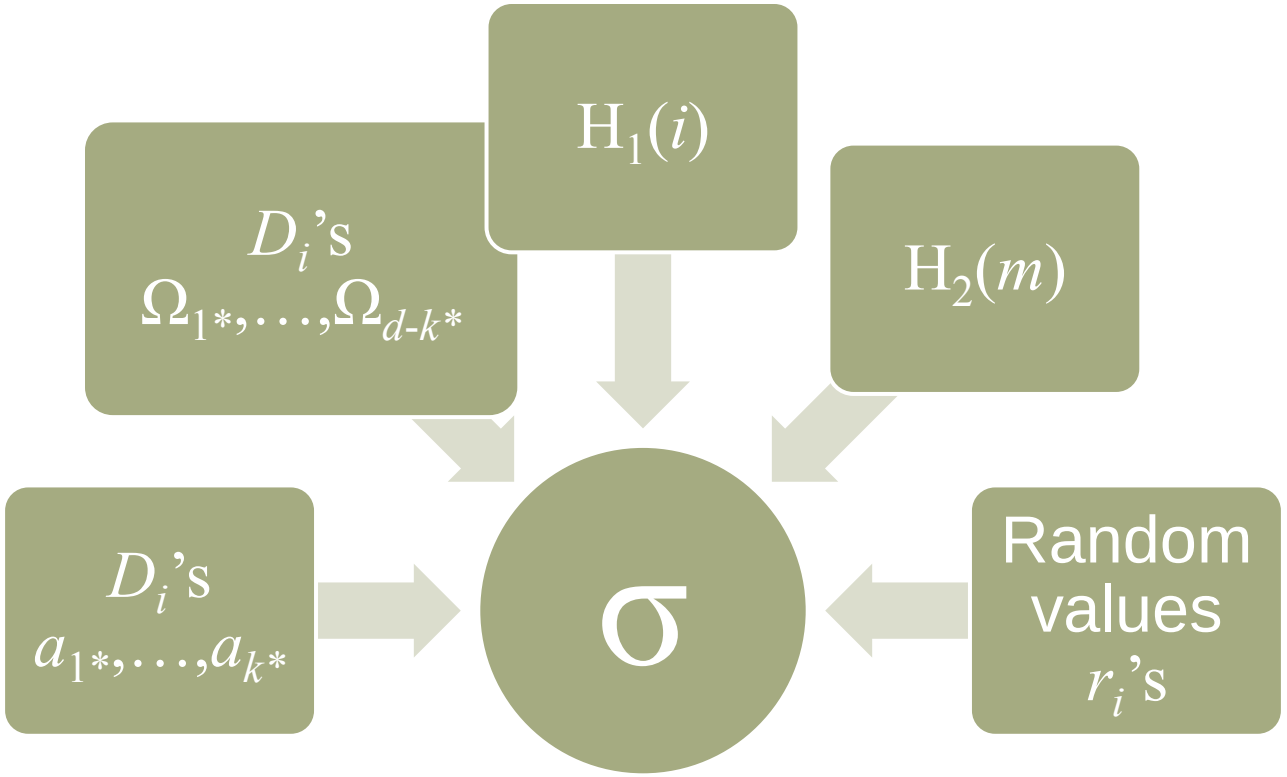
$a_{1*},\ldots,a_{k*}$

Select from default attributes $(d\text{-}k)$

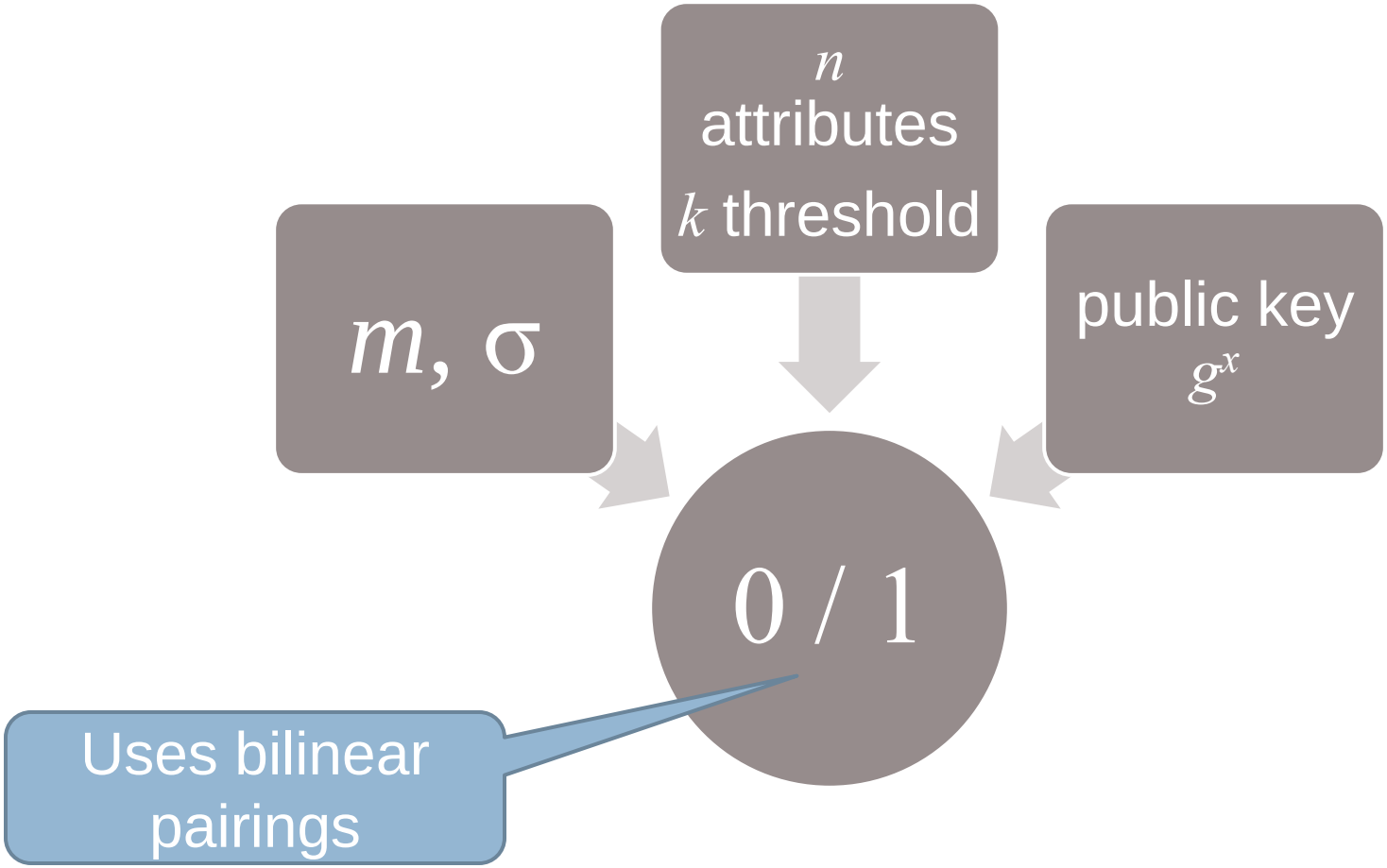
$\Omega_{1*},\ldots,\Omega_{d\text{-}k*}$

In the signature, the corresponding secret keys are raised to the Lagrange coefficient which is used in the interpolation

ABS Signing Algorithm



ABS Verification Algorithm

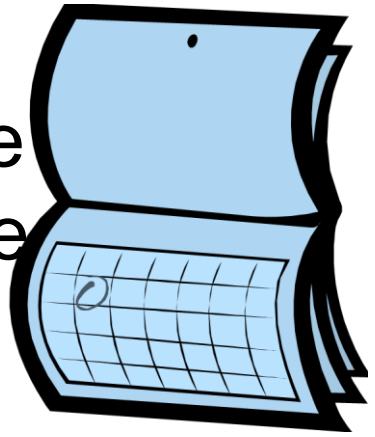


Why are ABS useful?

- Prove credentials
- This access is time unlimited
- Why limit the time validity intervals of the attributes?
  - Attribute revocation

Time-Specific Encryption

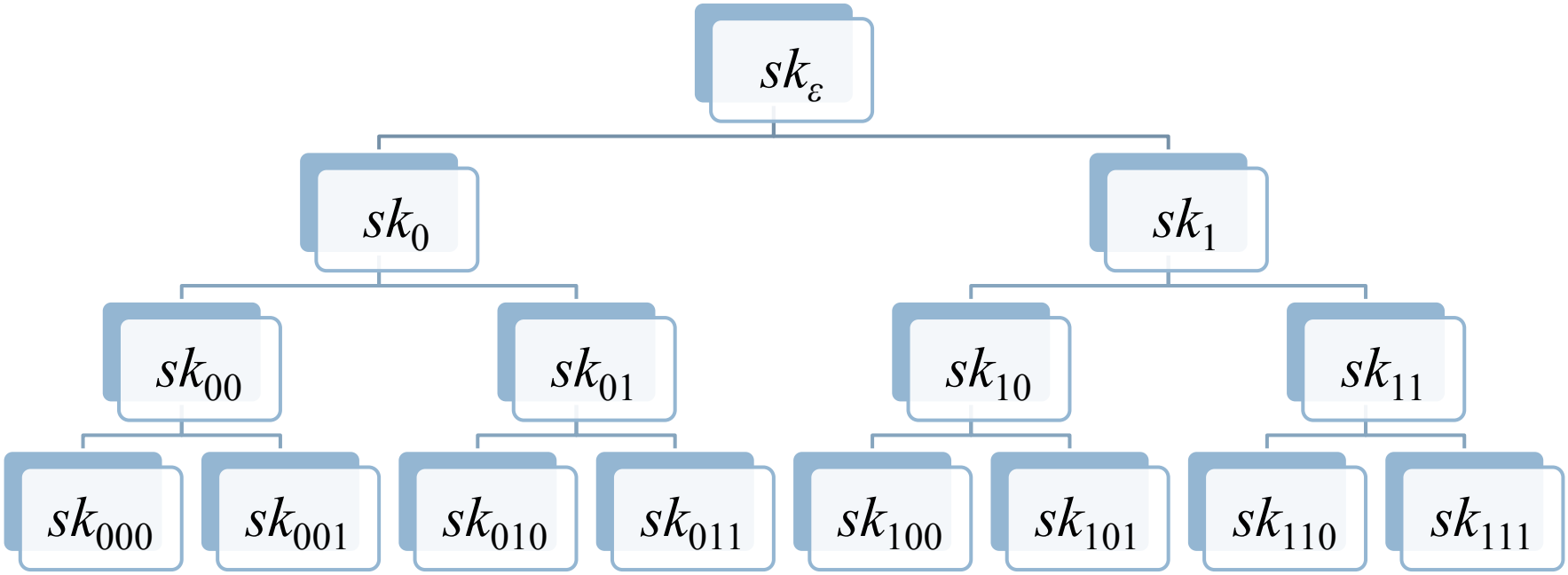
- Users get an encryption to be decrypted in the future
- A “time server” (TS) broadcasts the “time instant key” (TIK) which is the secret key for the current time period



Time Server

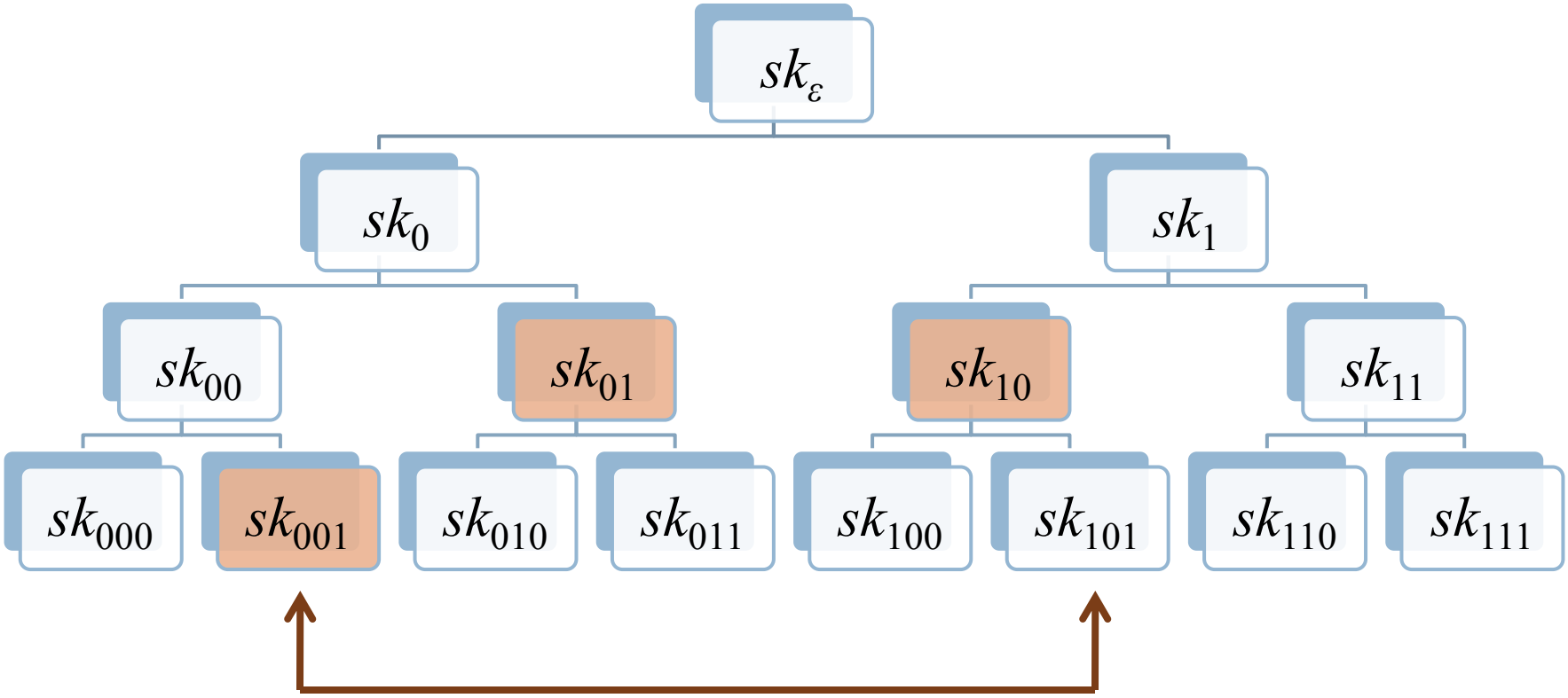
- Binary tree
  - Leaves are time periods
- Each TIK broadcast is a path from the root node to a leaf
- Each interval has a unique "cover"
- The TIK and cover intersect at one node

Binary Tree of Depth 3

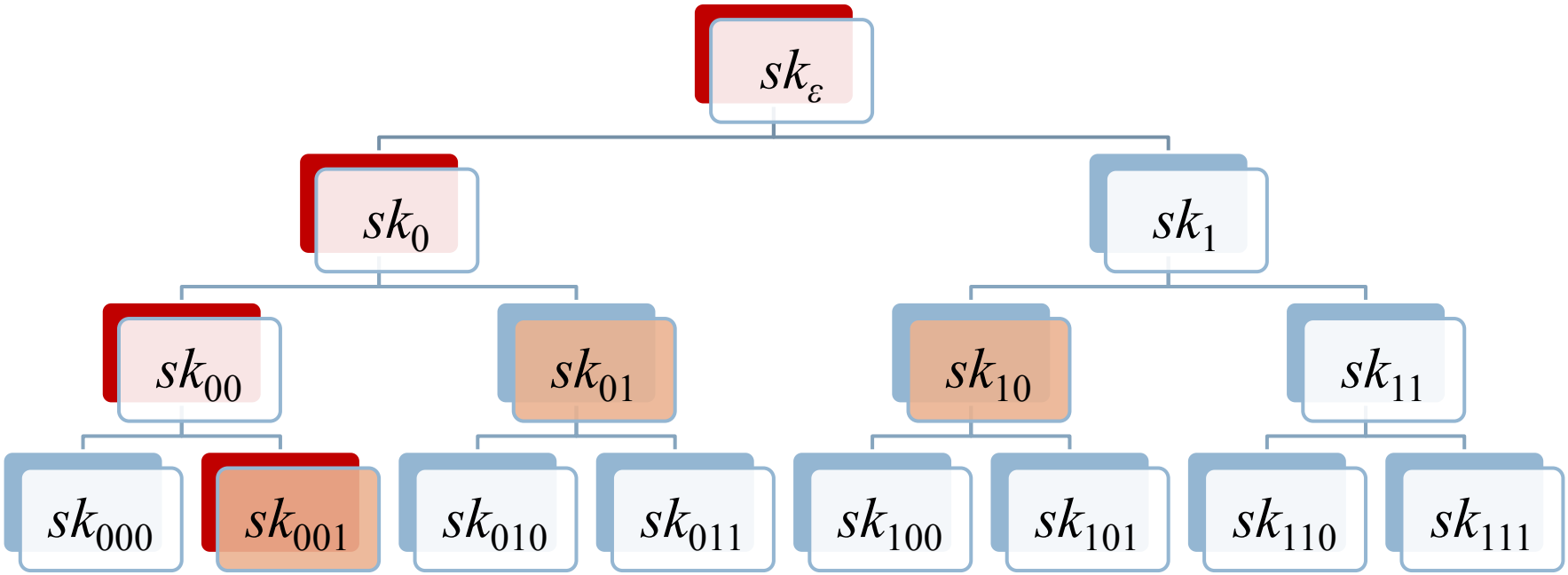


2^3 time periods for interval $[0,7]$

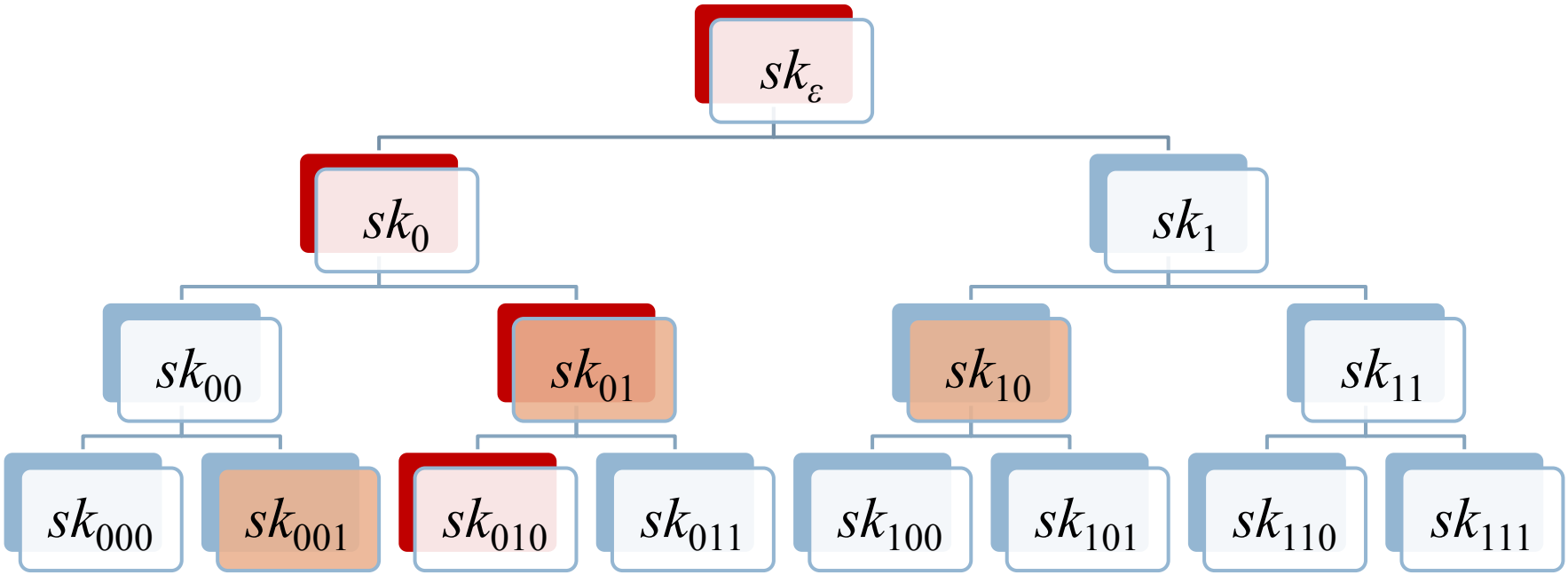
Cover for [1,5]


sk_ε
sk_0
sk_1
sk_{00}
sk_{01}
sk_{10}
sk_{11}
sk_{000}
sk_{001}
sk_{010}
sk_{011}
sk_{100}
sk_{101}
sk_{110}
sk_{111}

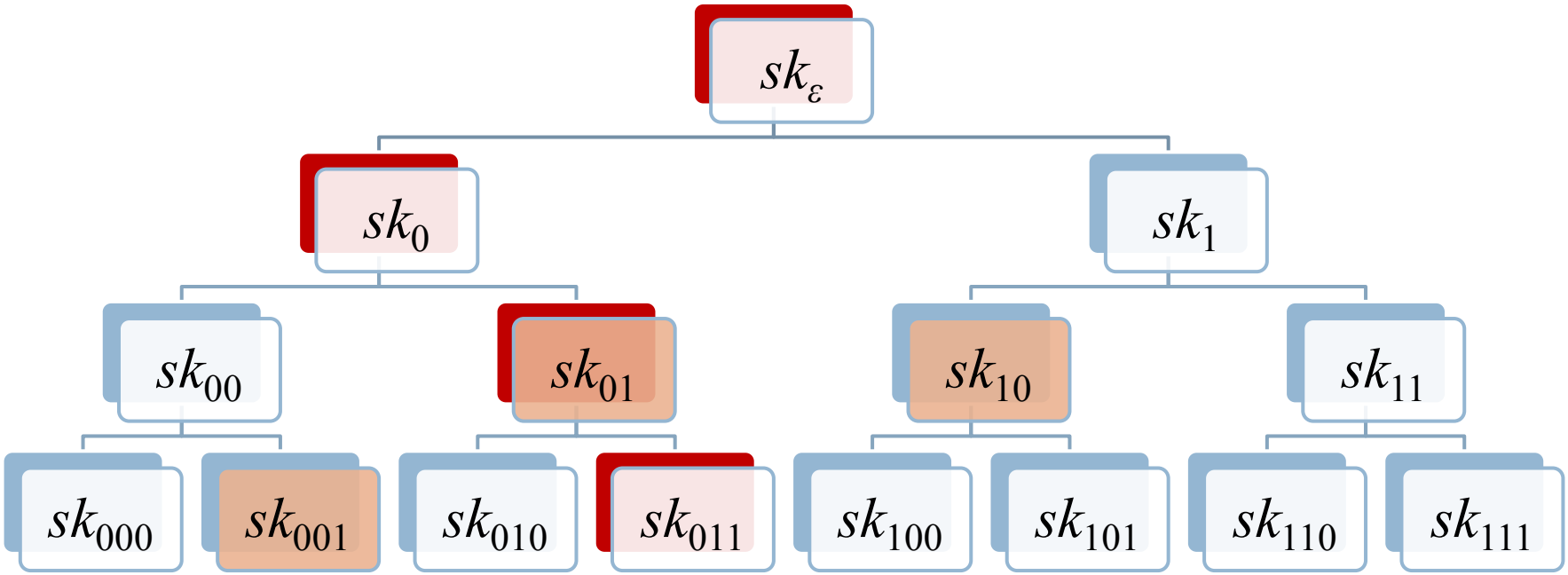
TIK for t=1(001)



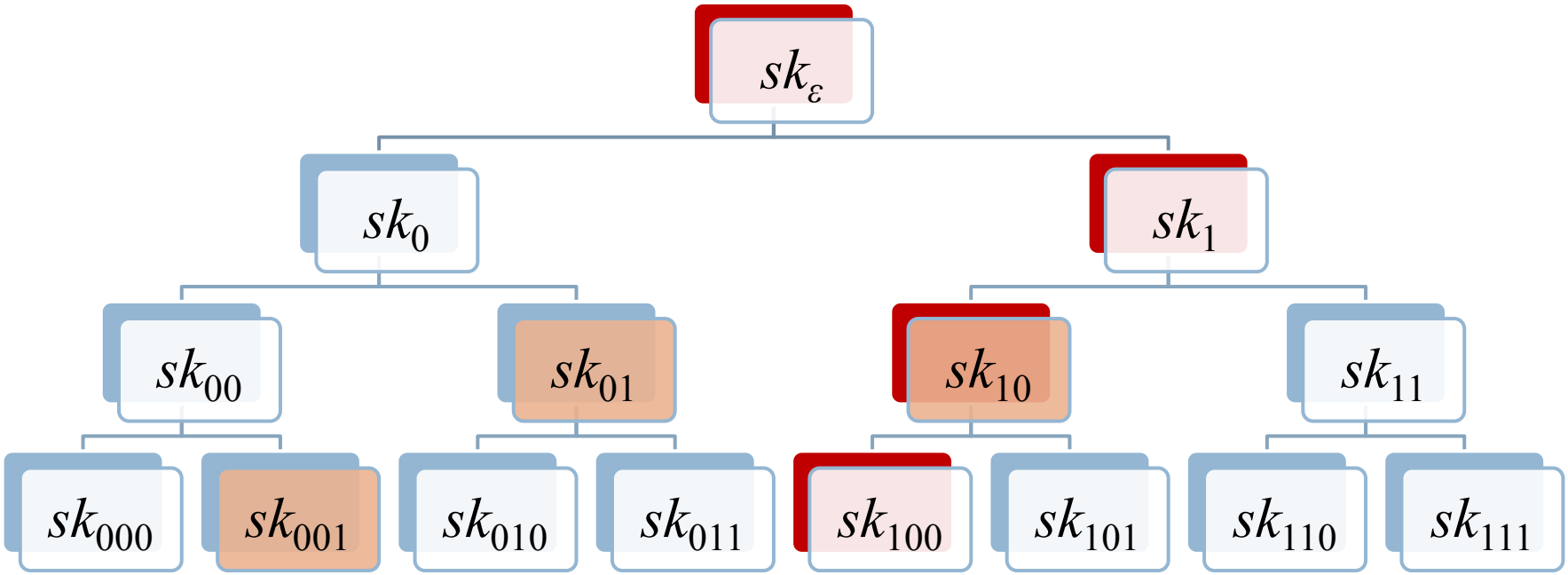
TIK for t=2(010)



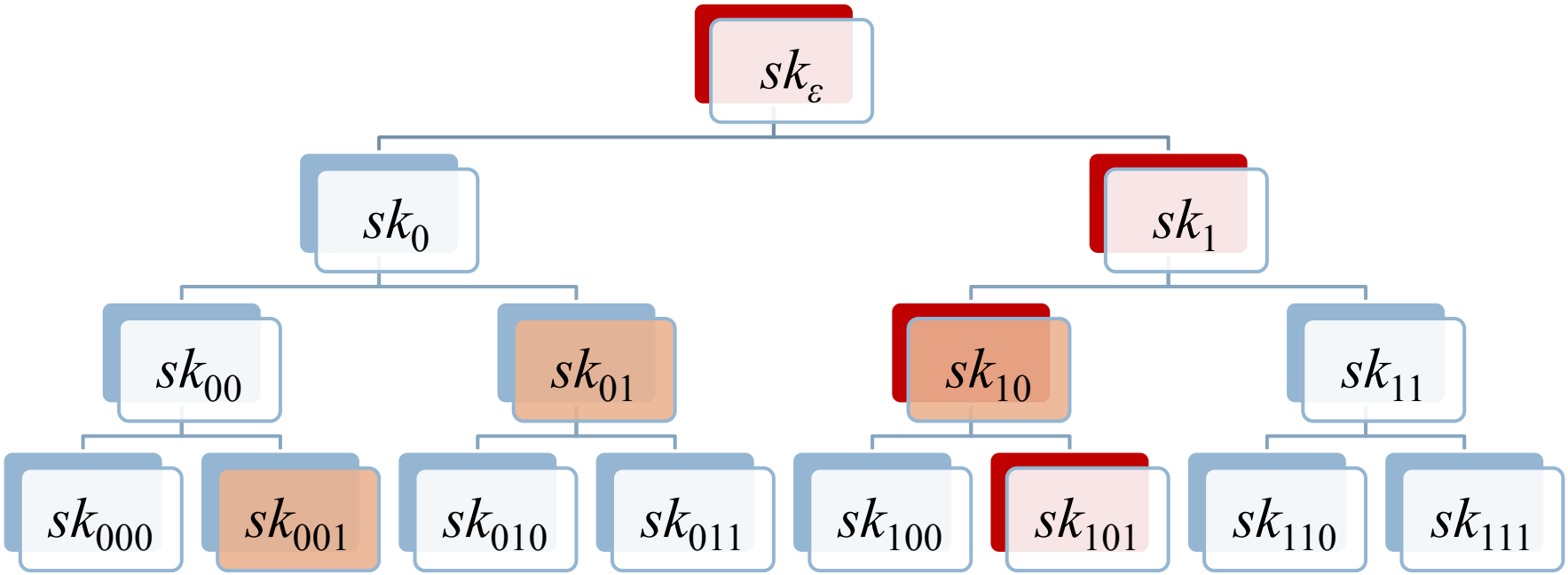
TIK for t=3(011)



TIK for t=4(100)



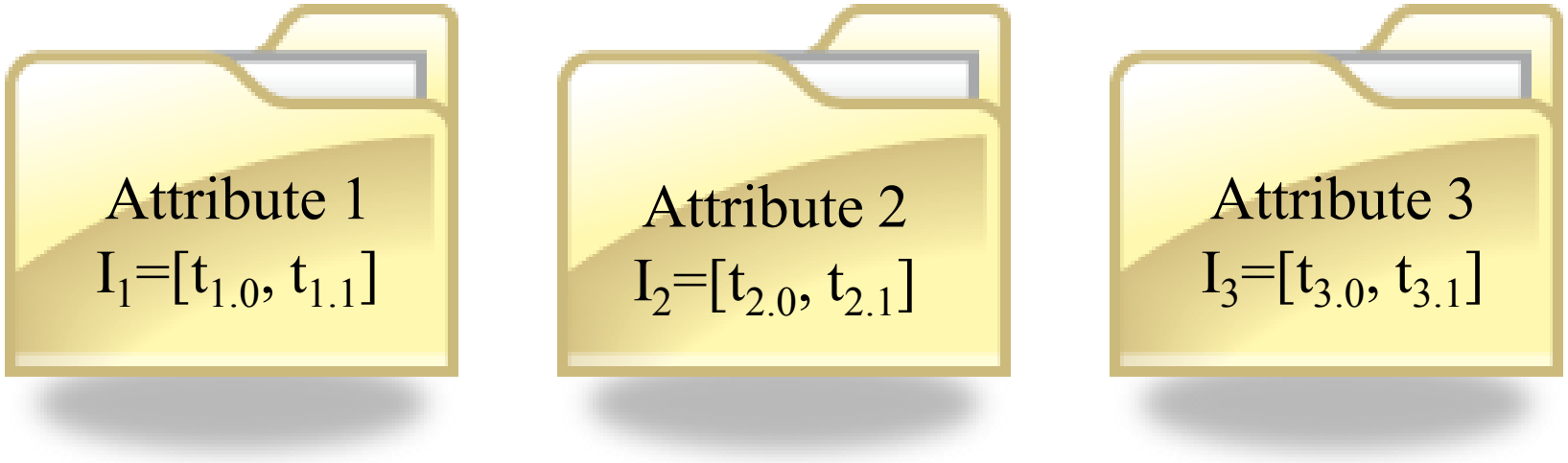
TIK for t=5(101)



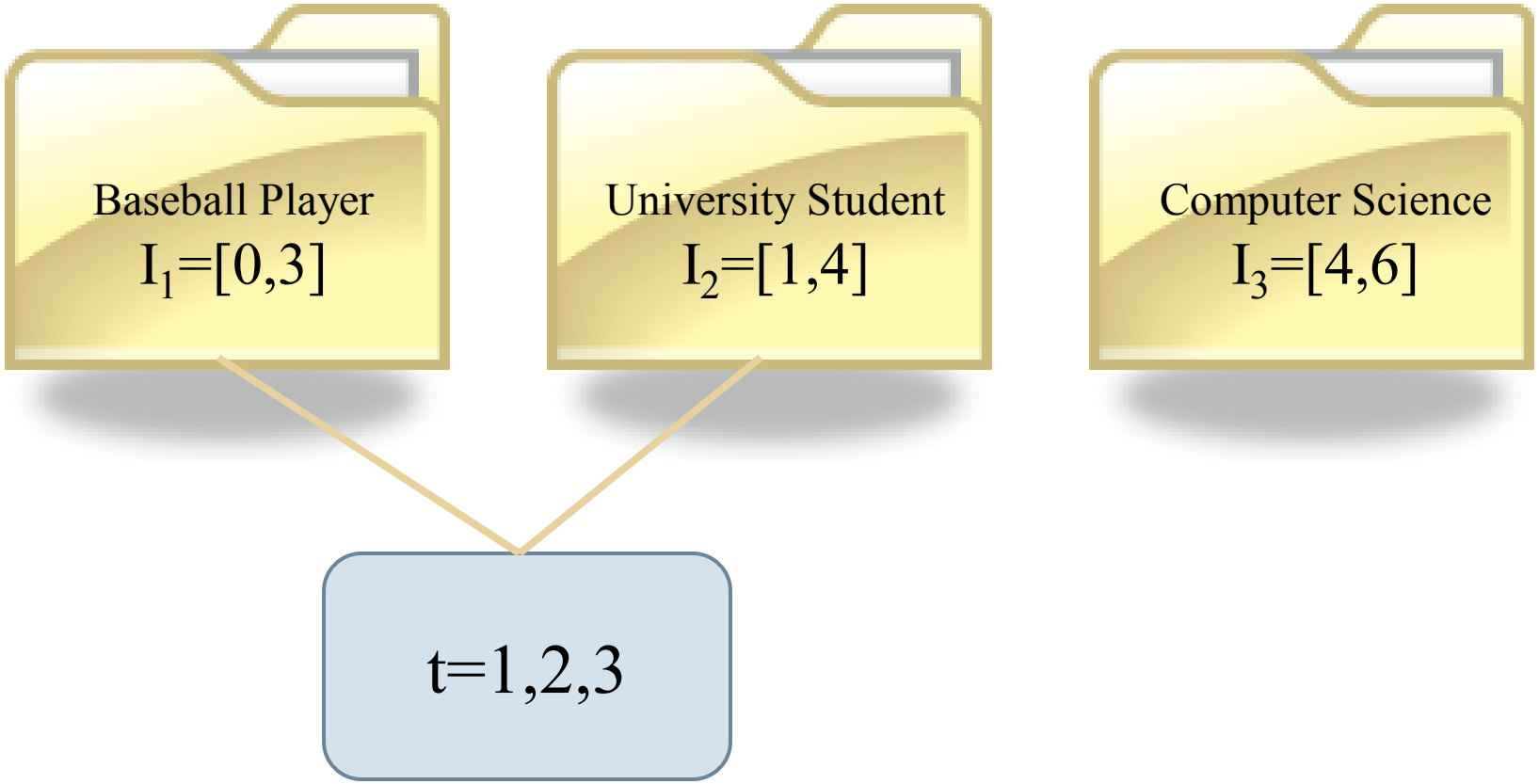
Key Generation w/ TS

- Recall D_i is the secret key for attribute i in $\omega \cup \Omega$
- D_i is constructed using $\mathrm{H}_1(i)$ which is used in verification
- Thus, we modify this to $\mathrm{H}_1\,(i||t_{i0}||t_{i1})$

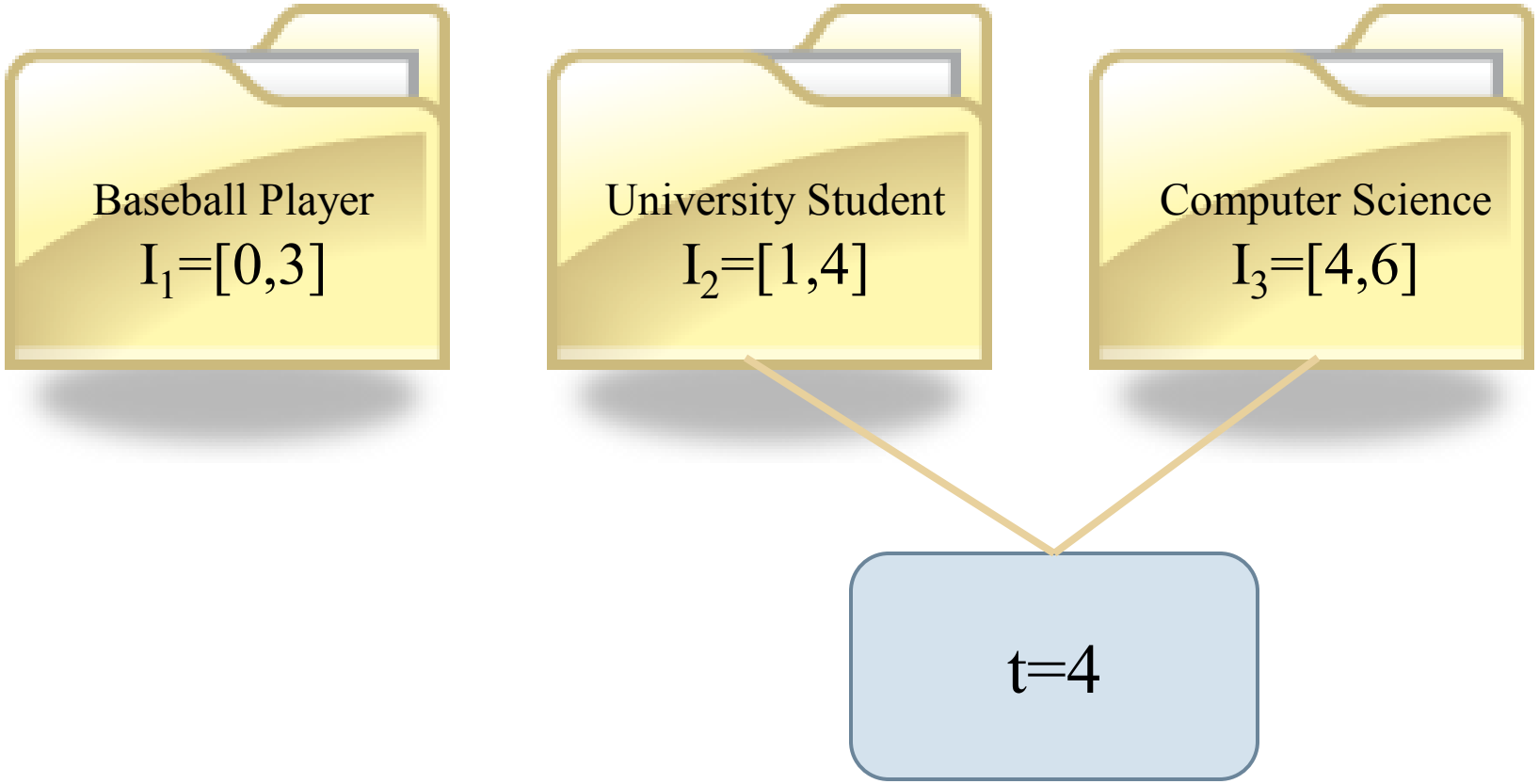
Attribute-Based Time-Specific Signatures (ATS)



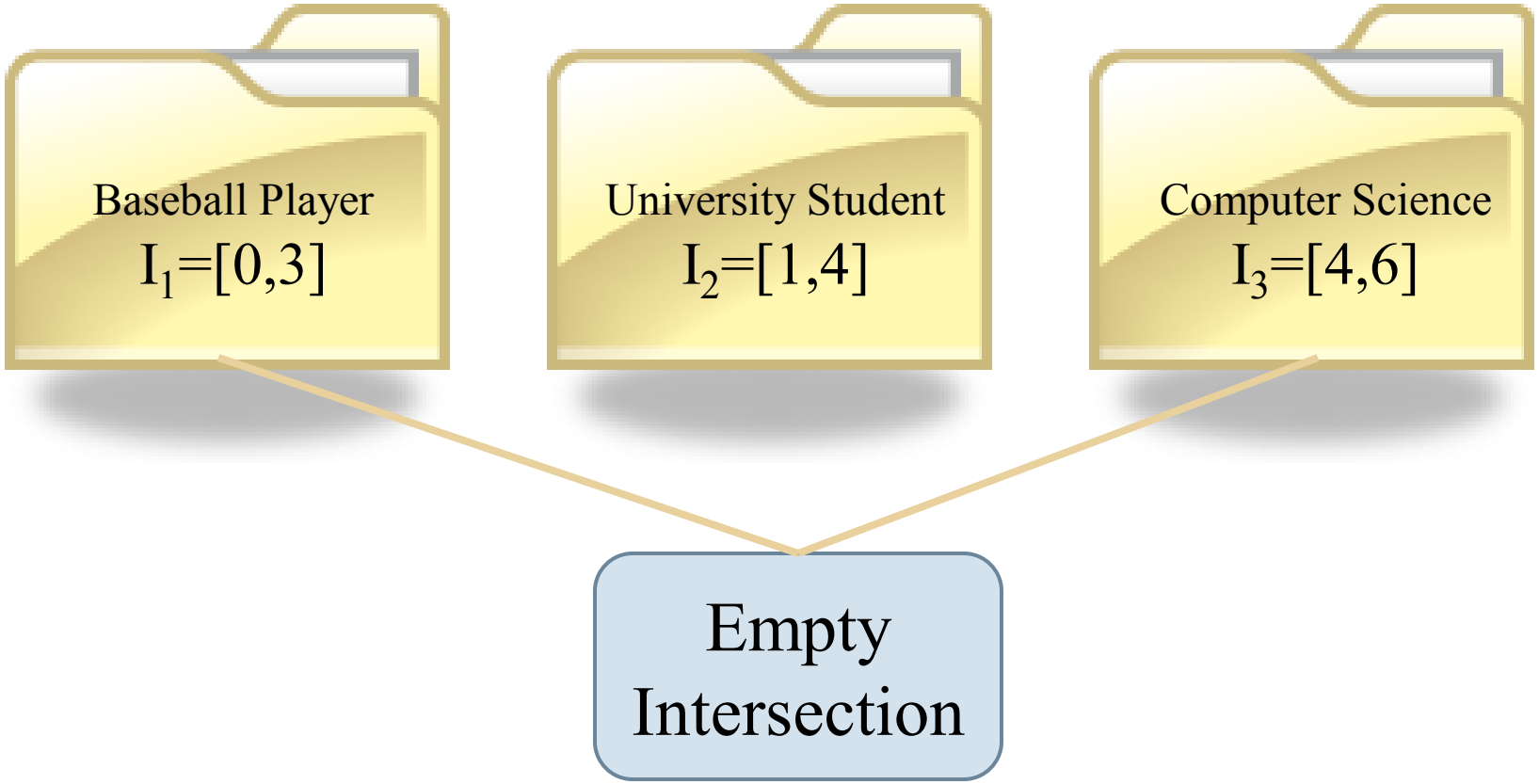
Combining Attributes



Combining Attributes



Combining Attributes



No Pre-computation

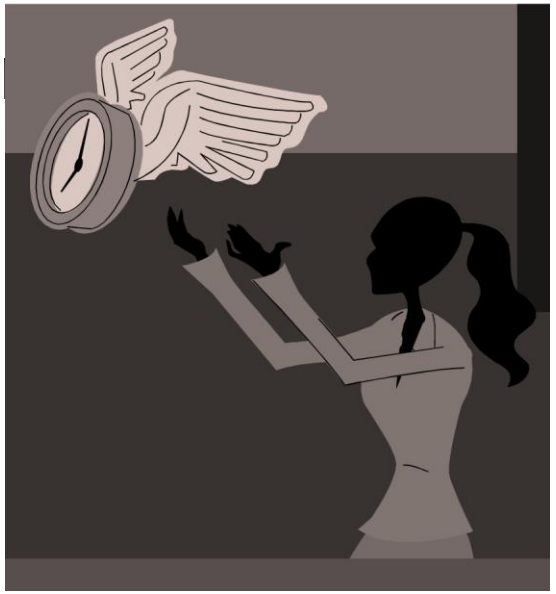
- Signer may not begin computing the signature until a TIK has been broadcast for each attribute being used
- Solution:
  - Attibute i has time validity $I_i=[t_{i0},t_{i1}]$
  - Encrypt sk_i under a cover for I_i using a TSE scheme
- Verification:
  - ABS scheme verification
  - Non-empty intersection of intervals

With Pre-computation

- Signer may begin computing the signature, but it will not be valid until a TIK has been broadcast for each attribute being used
- Verification:
  - ABS scheme verification
  - Non-empty intersection of intervals
    - Call this intersection J
  - TIK from J appended

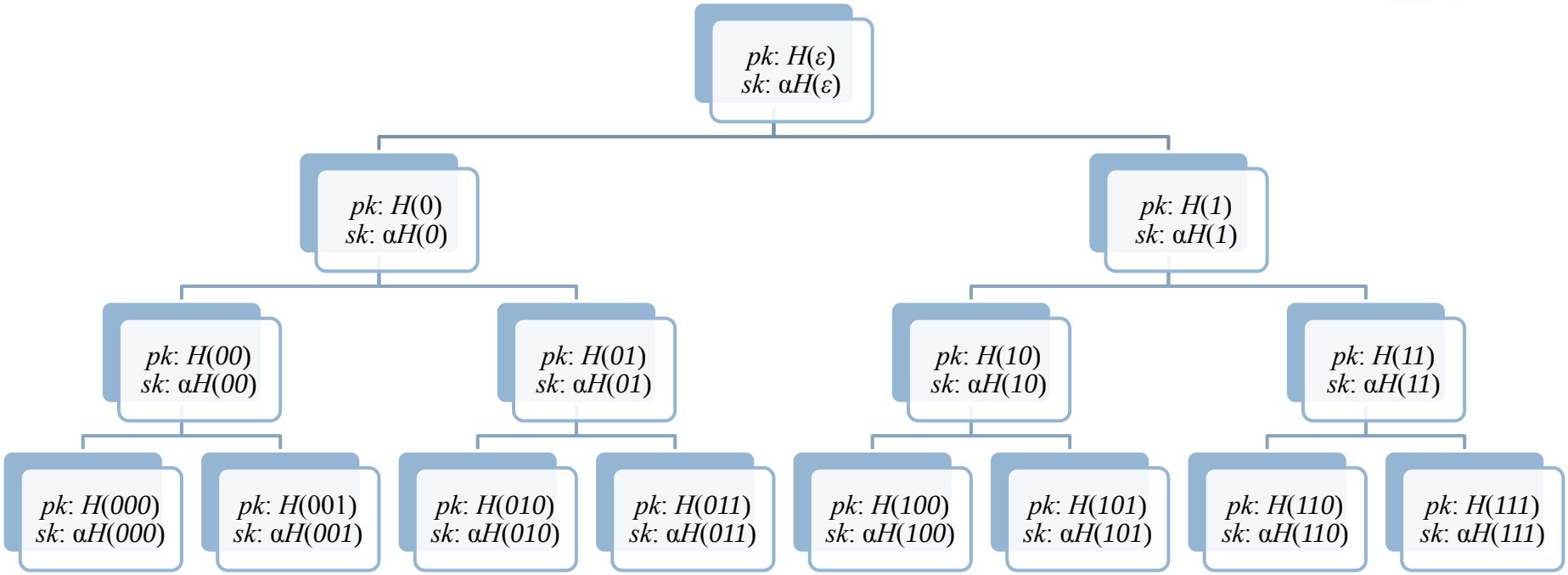
Delayed Verification

- Part of the signature may be encrypted so that the verification occurs in the futu
- May be generalized since a key generation authority is not necessary



Ex: Binary Tree Time Serve

TS Private Key α and Public Key g^{α}



- Select (r, g^r)
- Use a bilinear pairing $e(g^{\alpha}, H(t))^r$ to encrypt
- Recover term using TIK $\alpha H(t)$ by computing $e(g^r, \alpha H(t))$

Summary

- Attribute-Based Signatures
- Time-Specific Encryption
  - Time Server
- Time-Specific Attribute-Based Signatures

Questions?