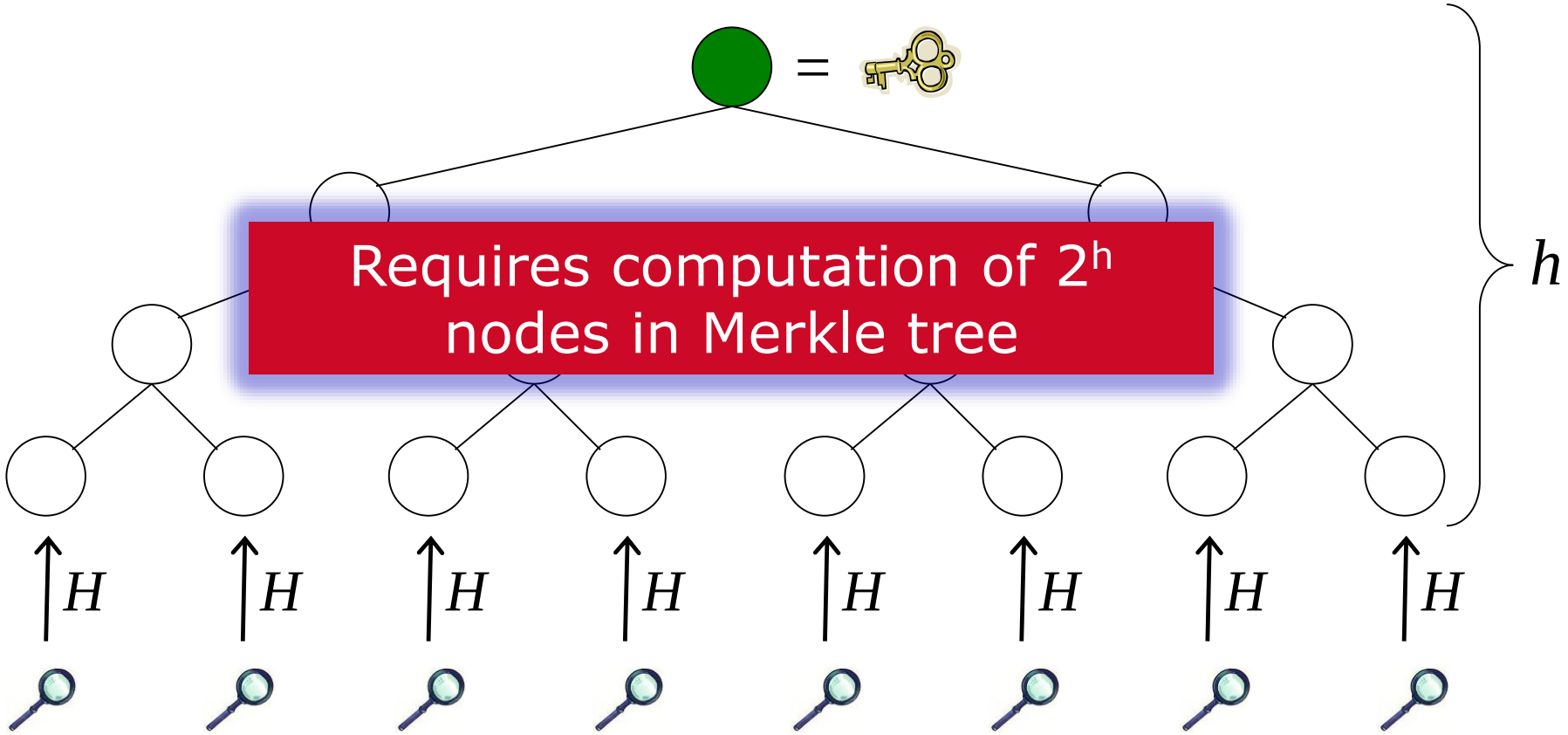
Hash-Based Signatures

Johannes Buchmann, Andreas Hülsung
Supported by DFG and DAAD

Part IX:
Public key generation

XMSS Public Key Generation

CASED

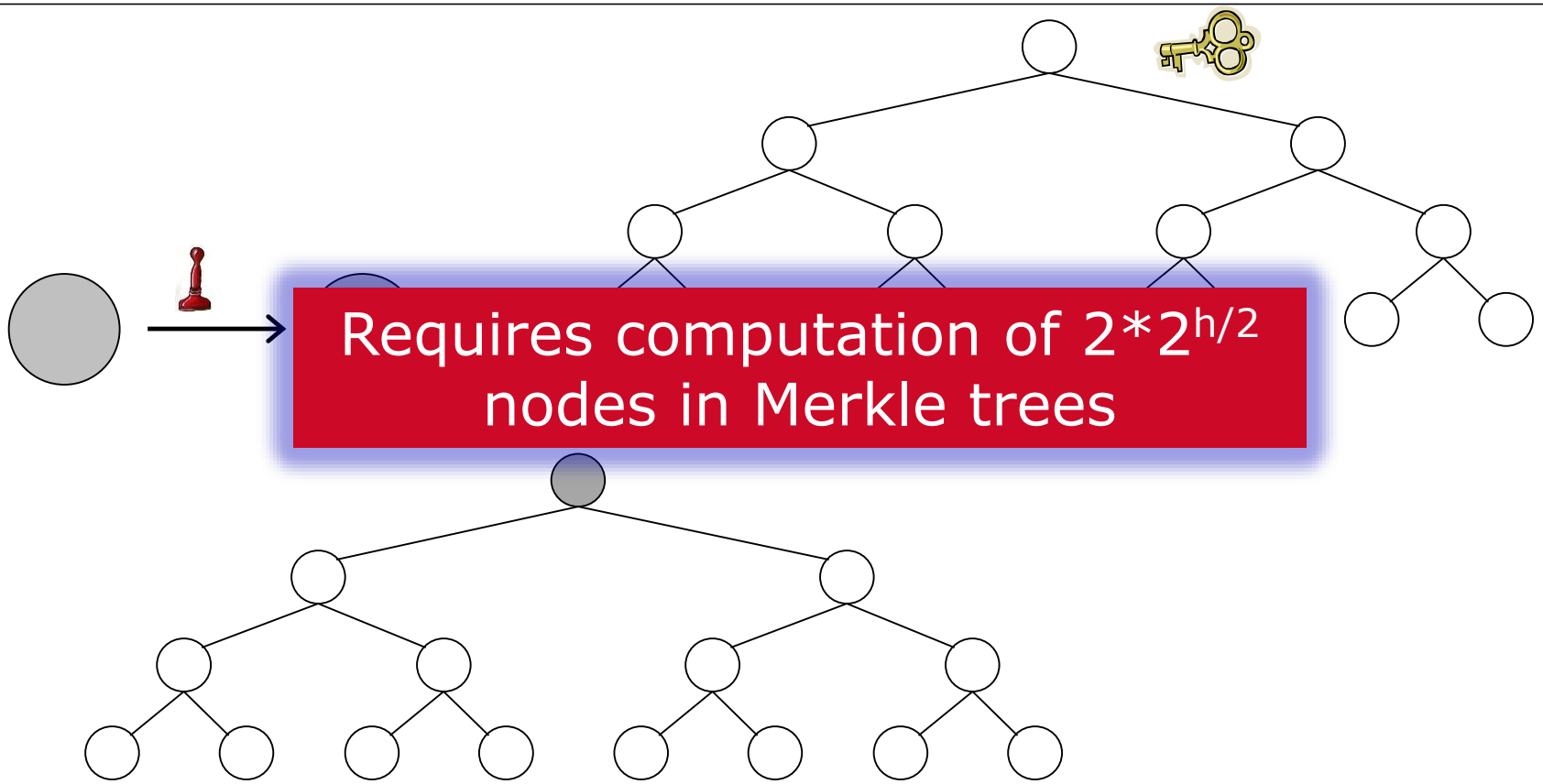


CASED

Tree Chaining

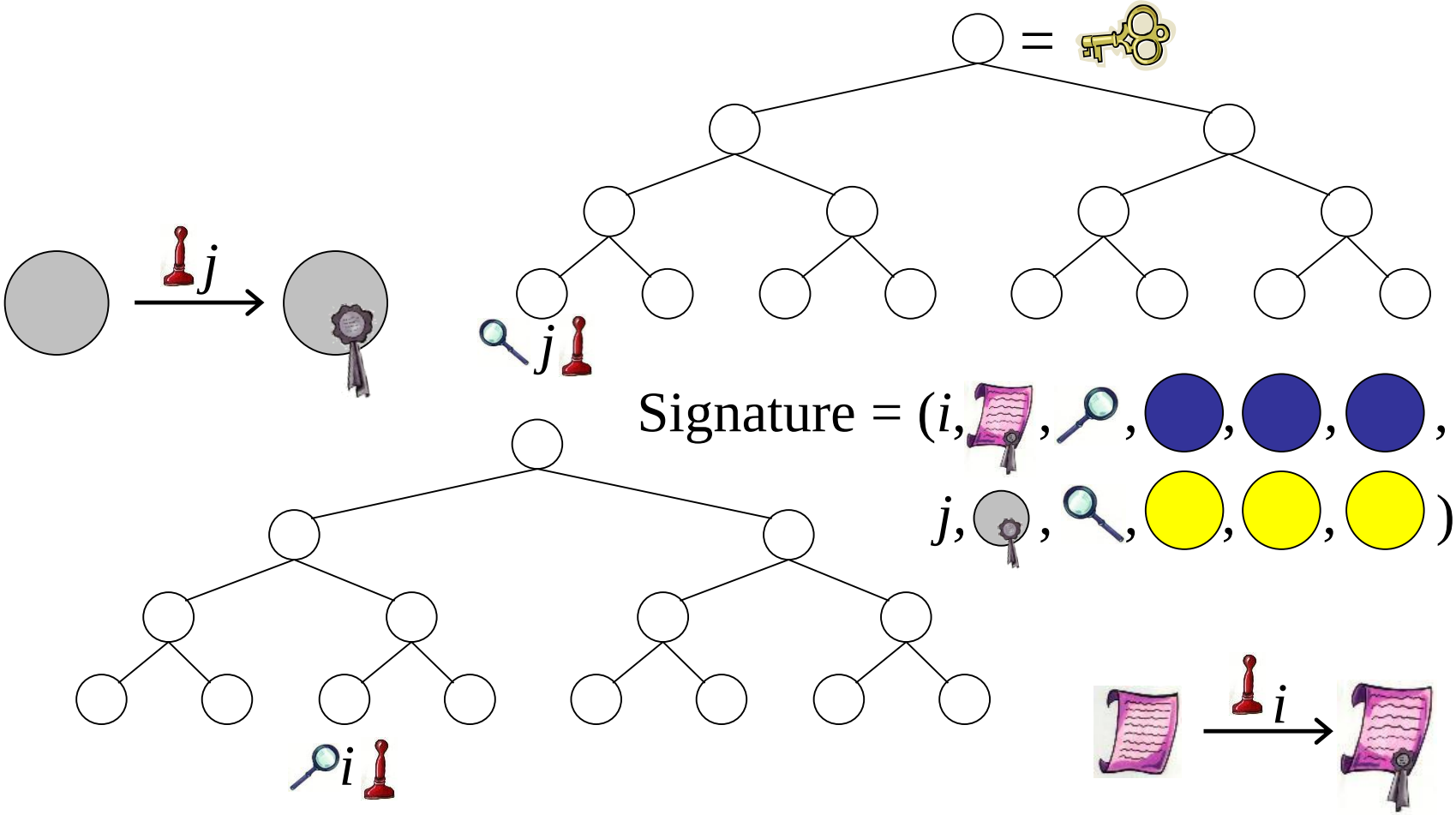
Two Levels
Key generation

CASED



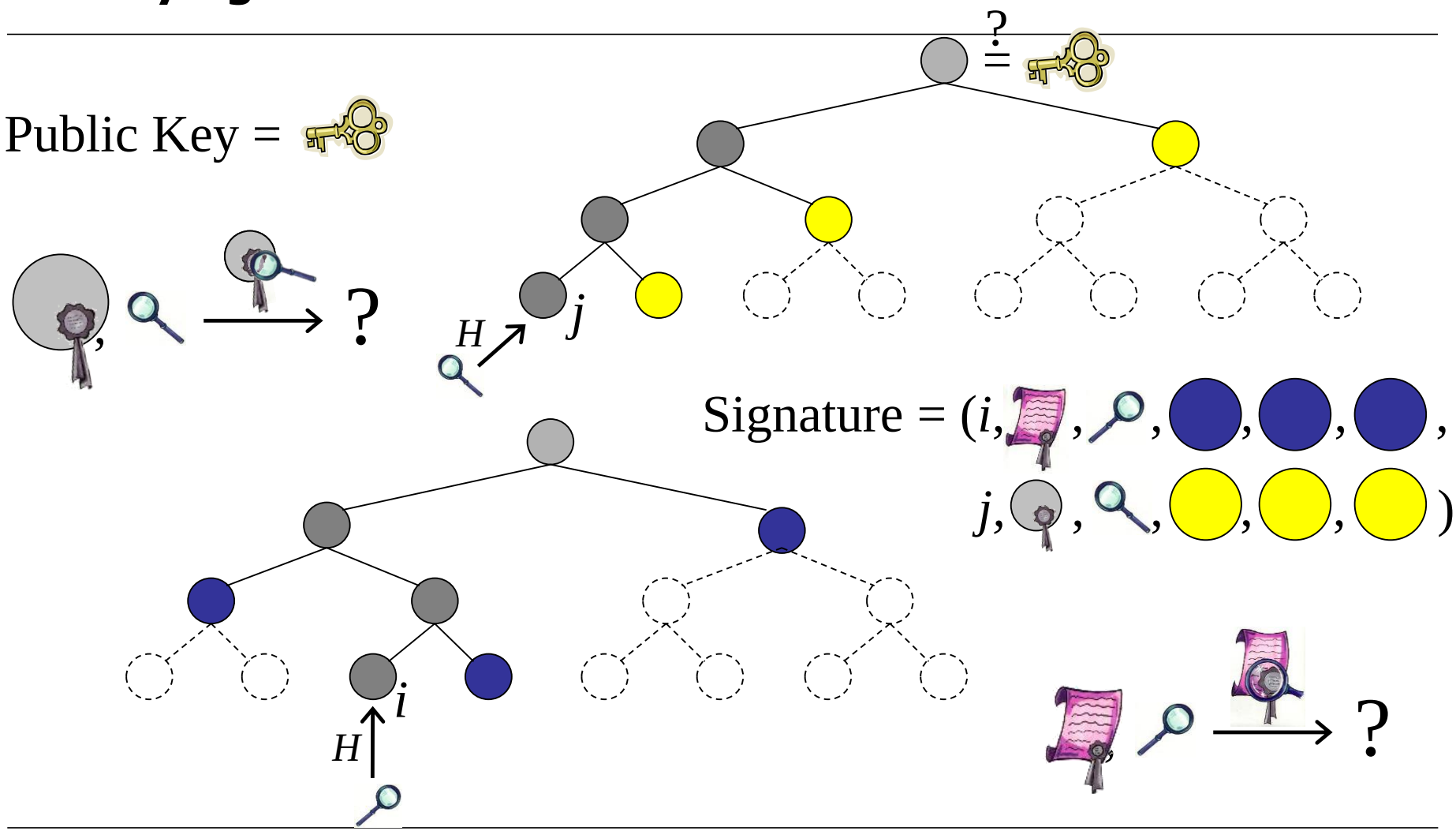
Two Levels
Signing

CASED



Two Levels
Verifying

CASED

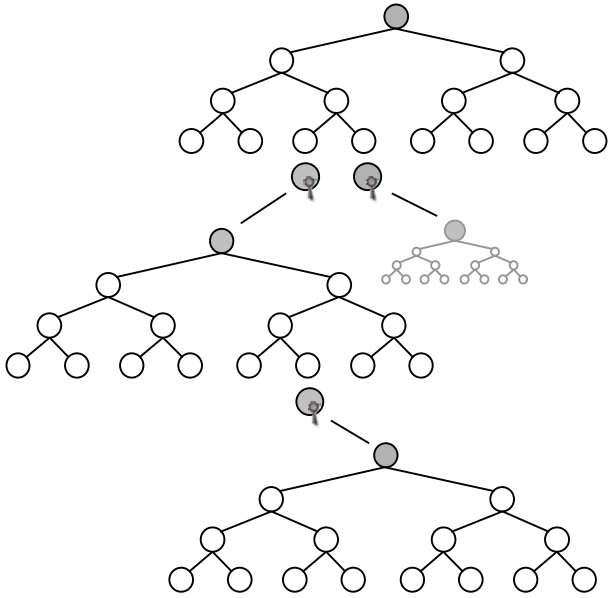


CASED

Distributed Signature Generation

Distributed Computation

CASED

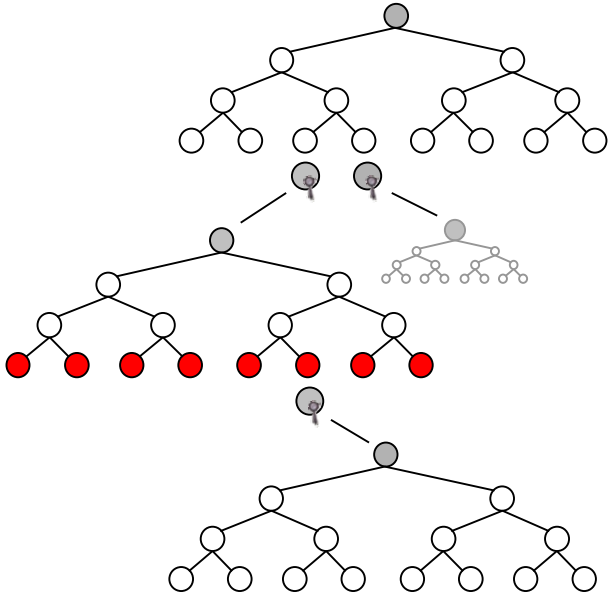


Store one-time signatures that don't change so often

Precompute upcoming signatures

Distributed Computation

CASED

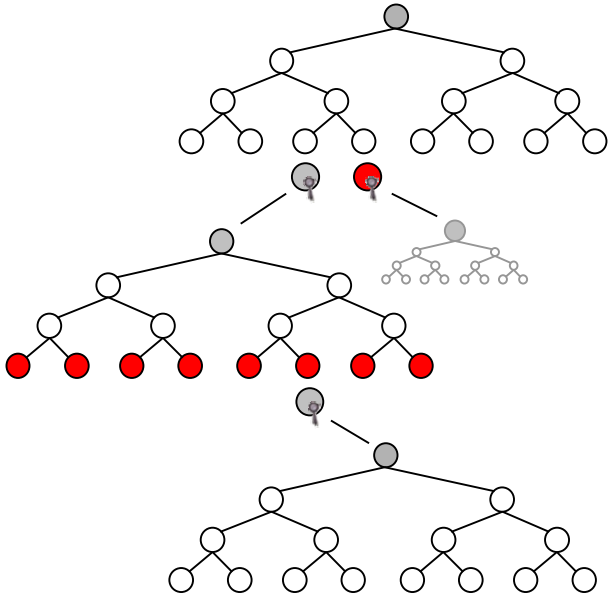


Store one-time signatures that don't change so often

Precompute upcoming signatures

Distributed Computation

CASED



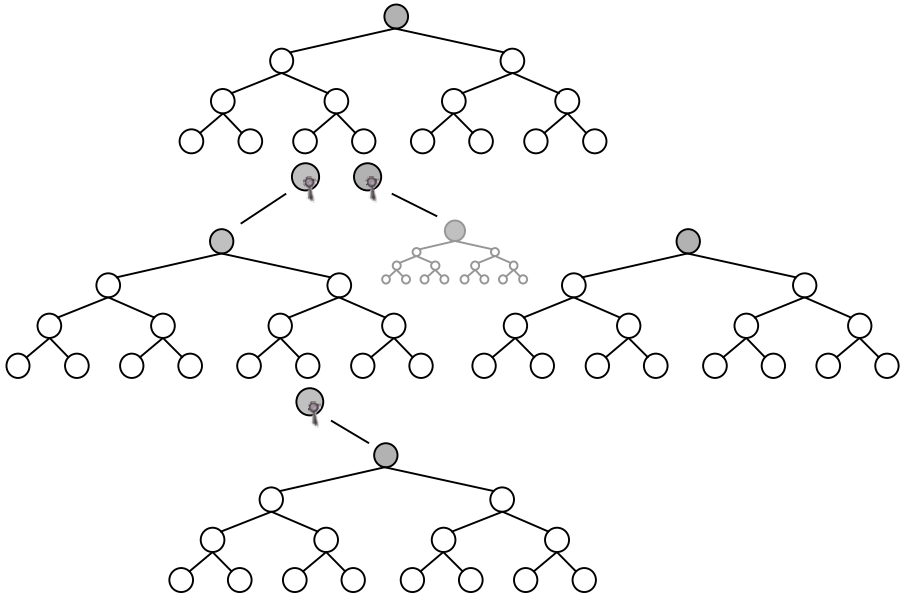
Store one-time signatures that don't change so often

Precompute upcoming signatures

Precompute upcoming roots

Distributed Computation

CASED



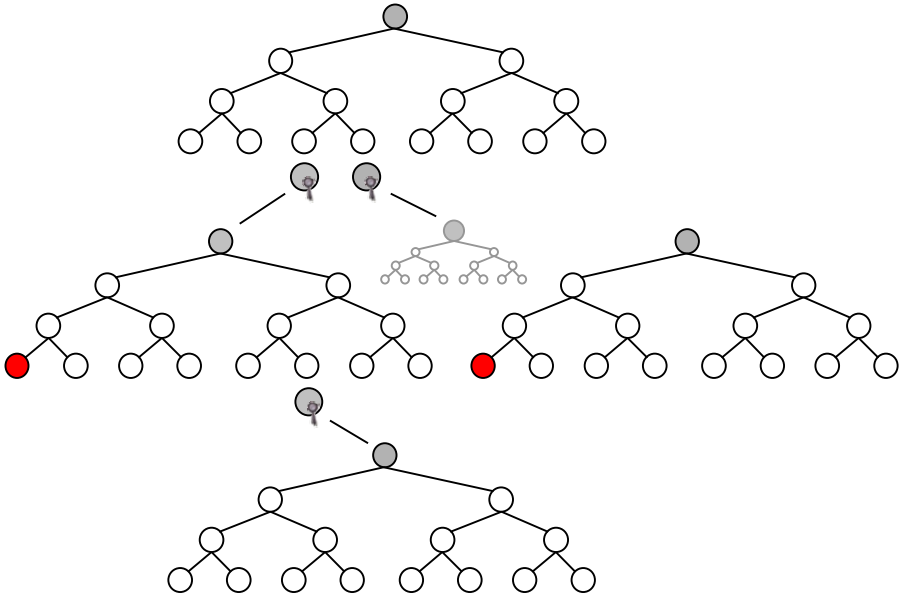
Store one-time signatures that don't change so often

Precompute upcoming signatures

Precompute upcoming roots

Distributed Computation

CASED



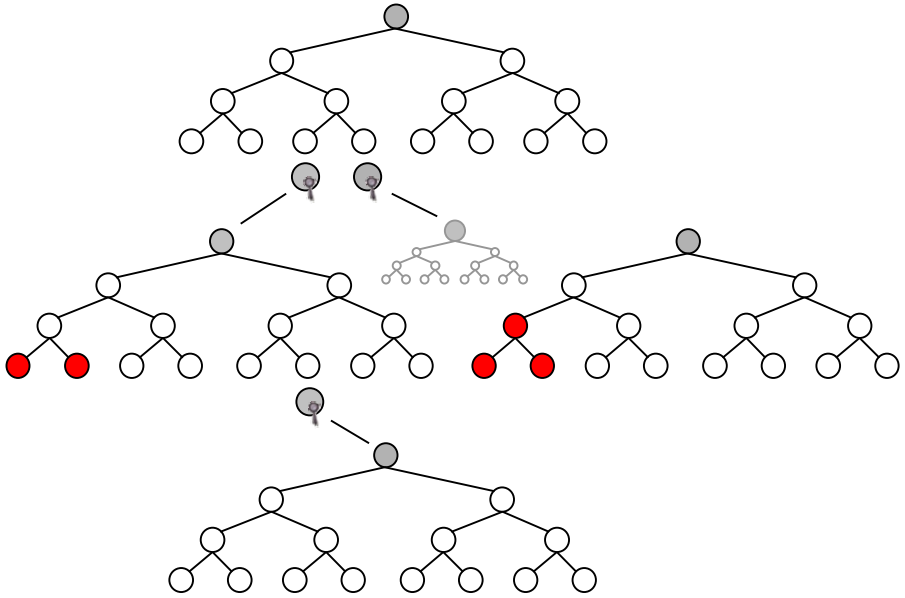
Store one-time signatures that don't change so often

Precompute upcoming signatures

Precompute upcoming roots

Distributed Computation

CASED



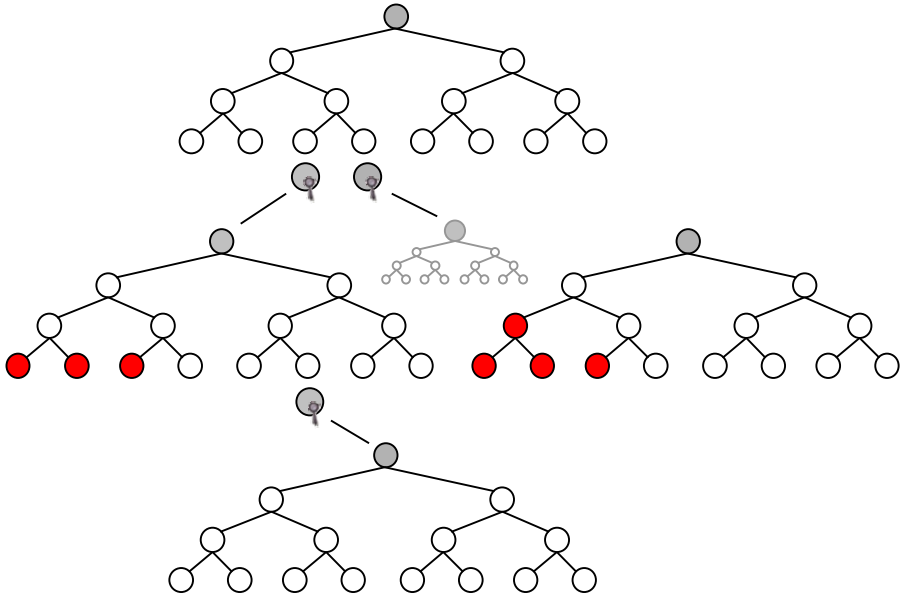
Store one-time signatures that don't change so often

Precompute upcoming signatures

Precompute upcoming roots

Distributed Computation

CASED



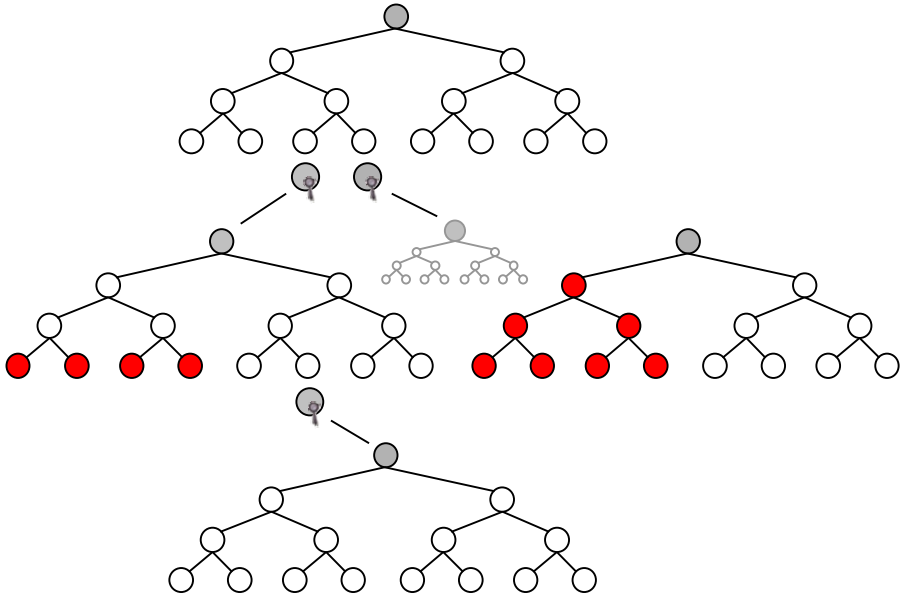
Store one-time signatures that don't change so often

Precompute upcoming signatures

Precompute upcoming roots

Distributed Computation

CASED



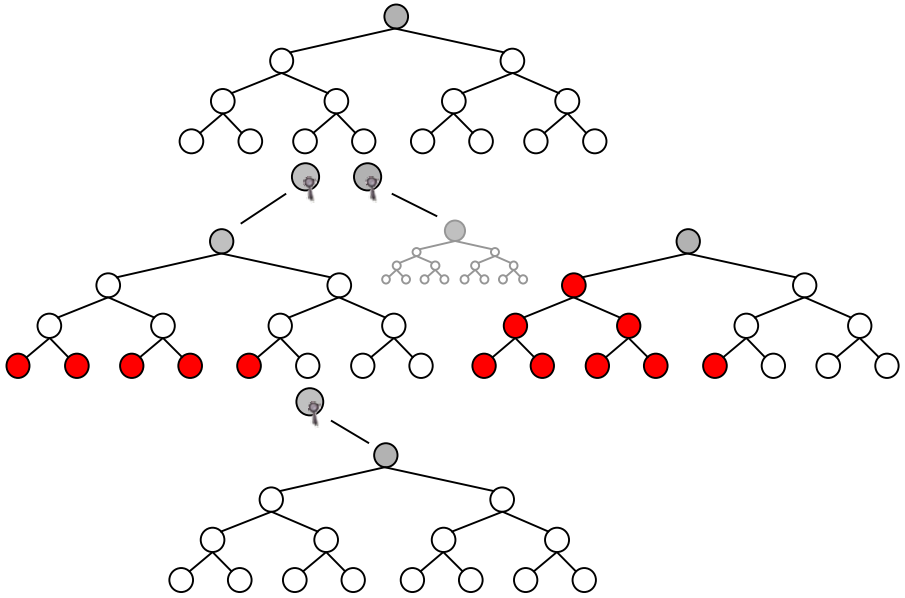
Store one-time signatures that don't change so often

Precompute upcoming signatures

Precompute upcoming roots

Distributed Computation

CASED



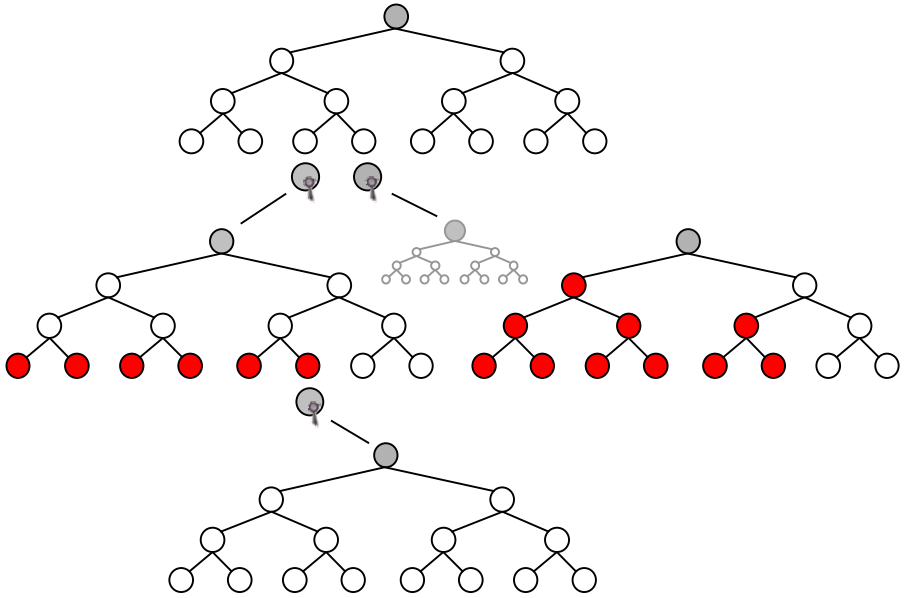
Store one-time signatures that don't change so often

Precompute upcoming signatures

Precompute upcoming roots

Distributed Computation

CASED



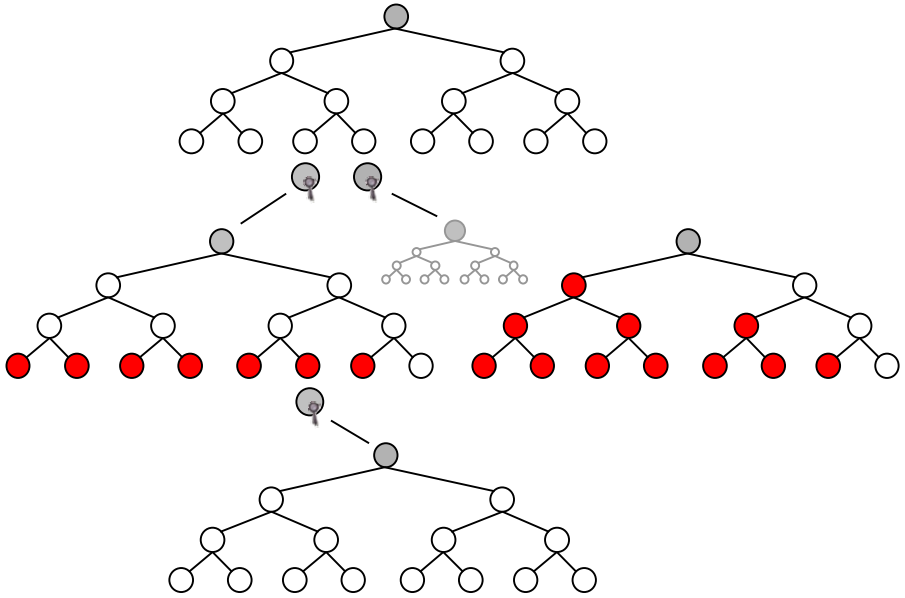
Store one-time signatures that don't change so often

Precompute upcoming signatures

Precompute upcoming roots

Distributed Computation

CASED



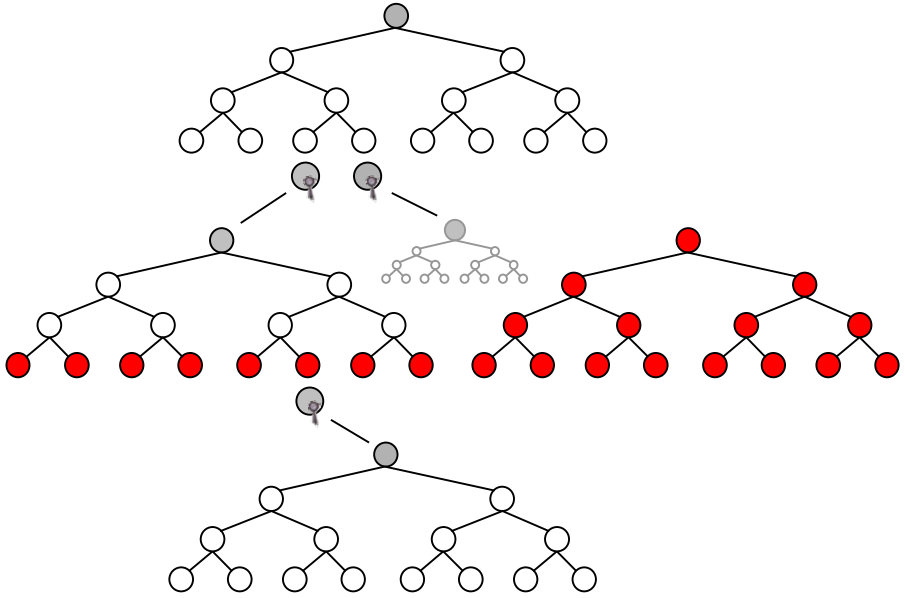
Store one-time signatures that don't change so often

Precompute upcoming signatures

Precompute upcoming roots

Distributed Computation

CASED



Store one-time signatures that don't change so often

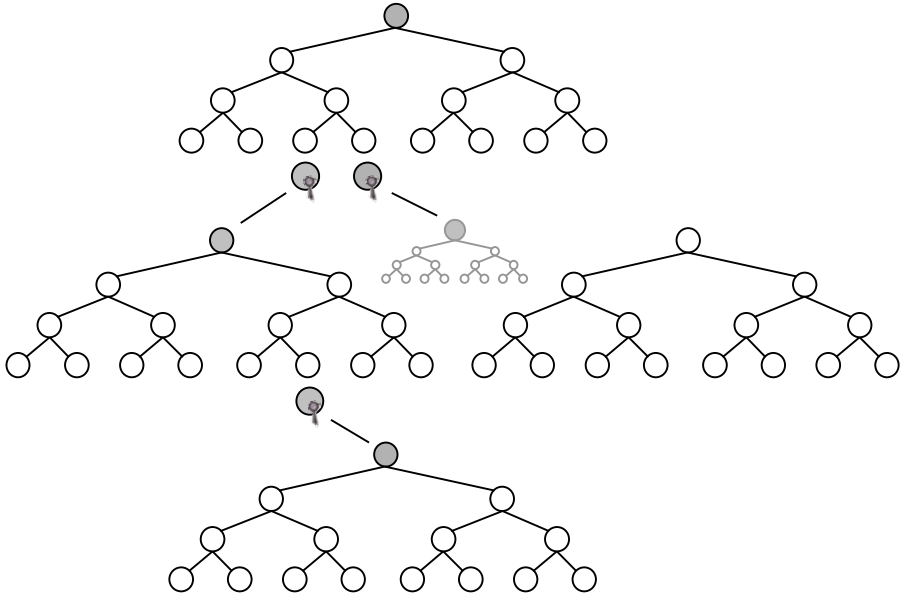
Precompute upcoming signatures

Precompute upcoming roots

Precompute upcoming leaves

Distributed Computation

CASED



Store one-time signatures that don't change so often

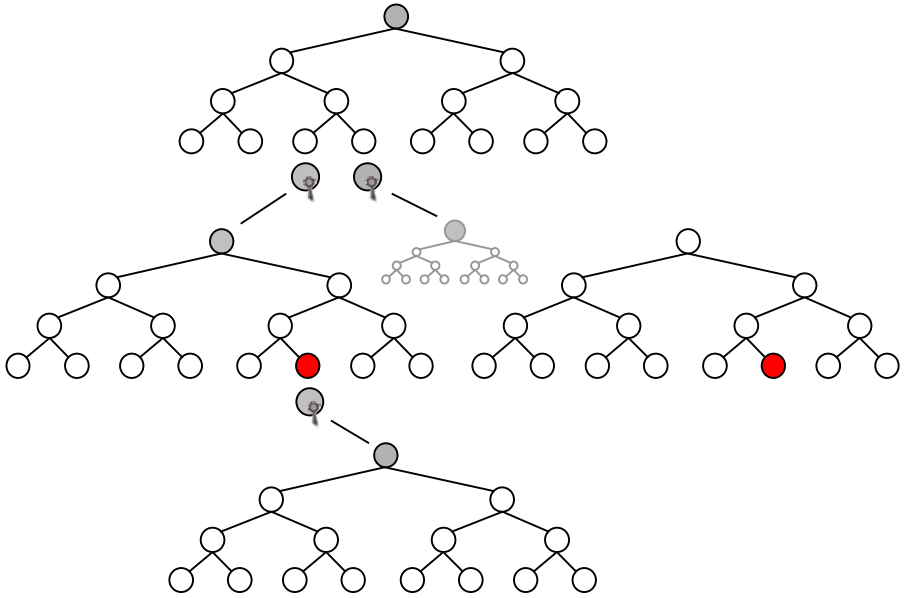
Precompute upcoming signatures

Precompute upcoming roots

Precompute upcoming leaves

Distributed Computation

CASED



Store one-time signatures that don't change so often

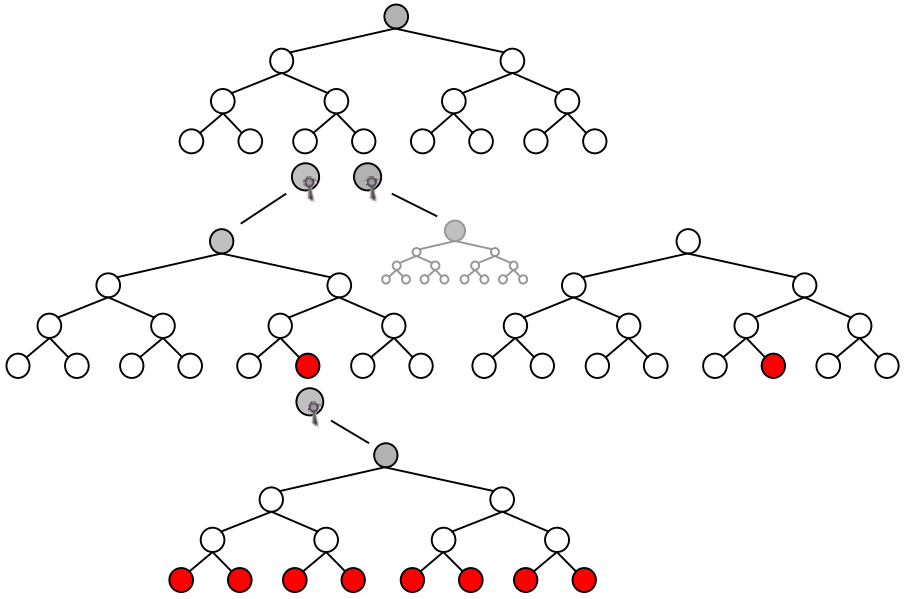
Precompute upcoming signatures

Precompute upcoming roots

Precompute upcoming leaves

Distributed Computation

CASED



Store one-time signatures that don't change so often

Precompute upcoming signatures

Precompute upcoming roots

Precompute upcoming leaves