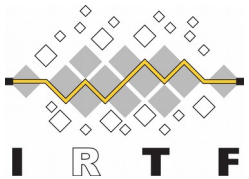
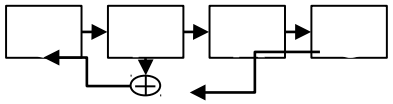


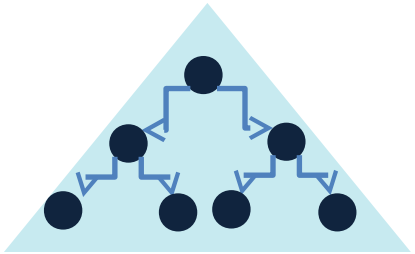


State Management in Hash-Based Signatures

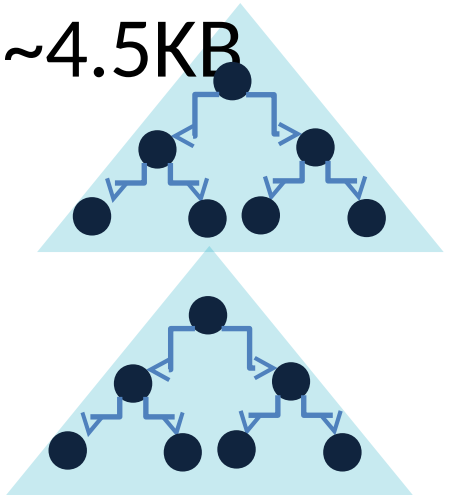
David McGrew, Panos Kampanakis, Scott Fluhrer,
Stefan-Lukas Gazdag, Denis Butin, Johannes Buchmann
{mcgrew,pkampana,sfluhrer}@cisco.com
stefan-lukas_gazdag@genua.eu
{dbutin,buchmann}@cdc.informatik.tu-darmstadt.de

- One-Time Signatures
- 1 Signature
- ~2KB

- Merkle
- Signatures
- 1024 Signatures
- ~2.5KB



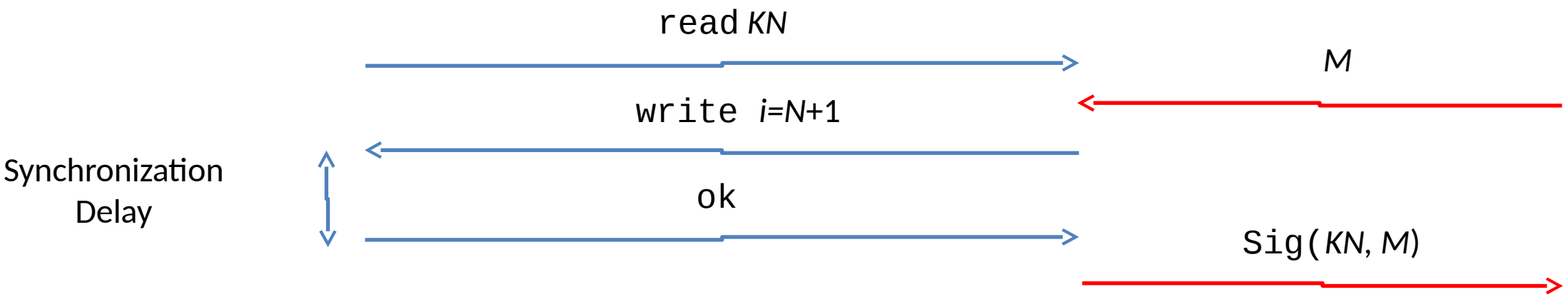
- Hierarchical
- Signatures
- 1,048,576 Signatures
- ~4.5KB



Private key state management

Disk Cache

File System Cache

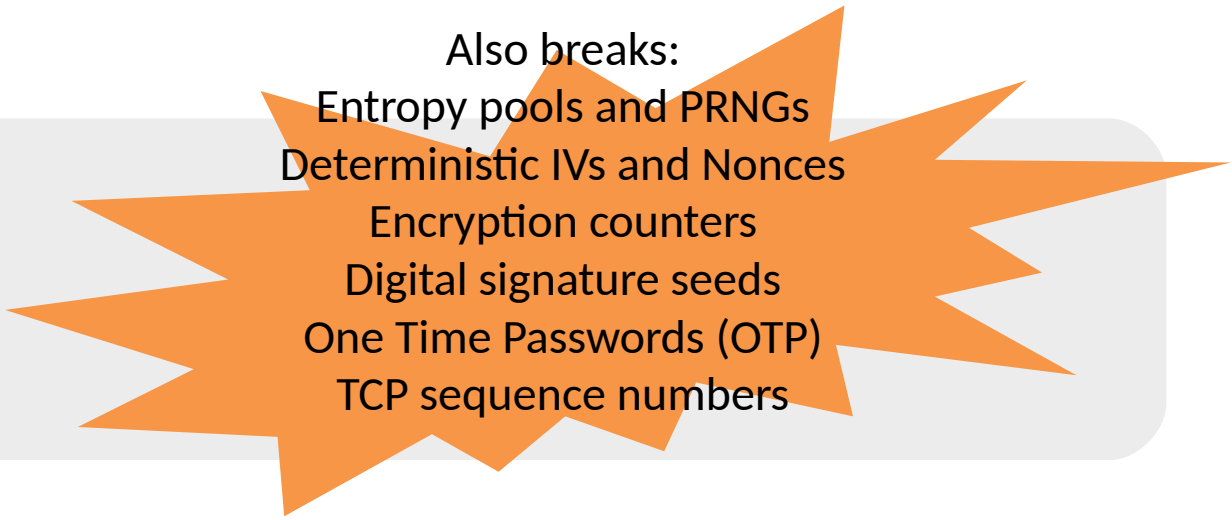


State management issues

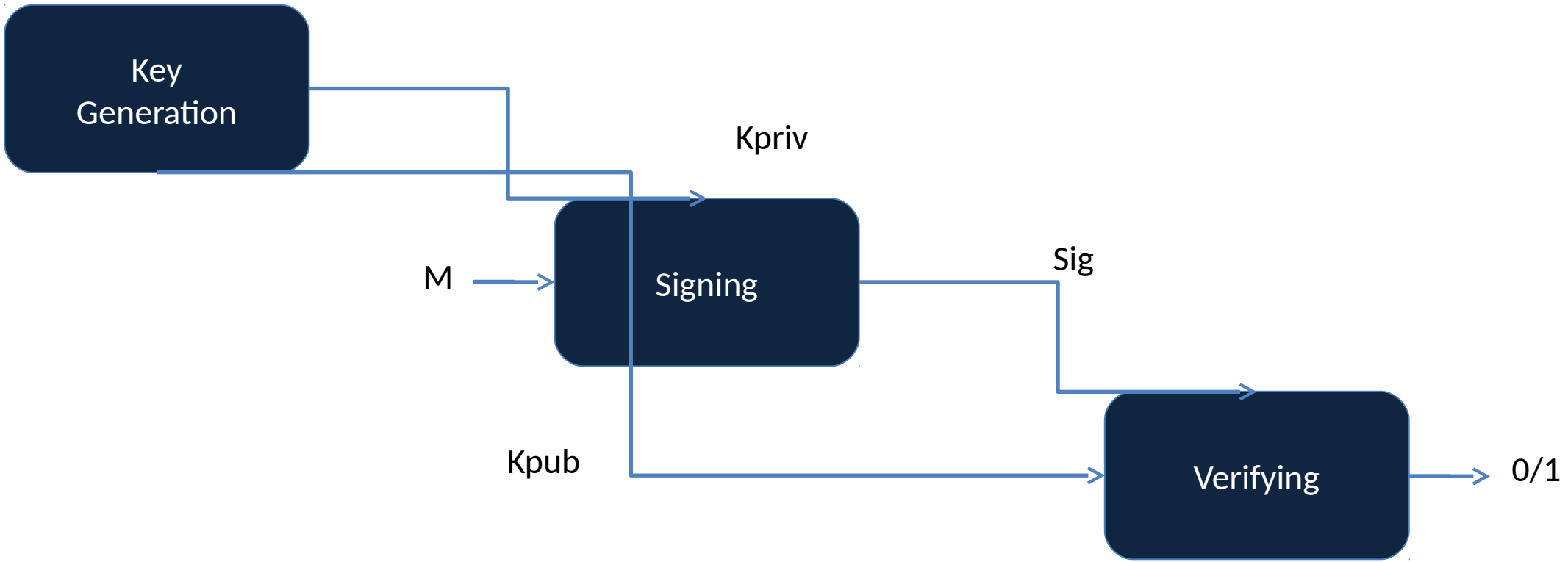
- Synchronization delay — Performance
- Synchronization failure — Security; testable
  - Implementation problem — Security; not testable
- Nonvolatile cloning
  - System backup — Security; not testable
- Volatile cloning
  - VM cloning

State management issues

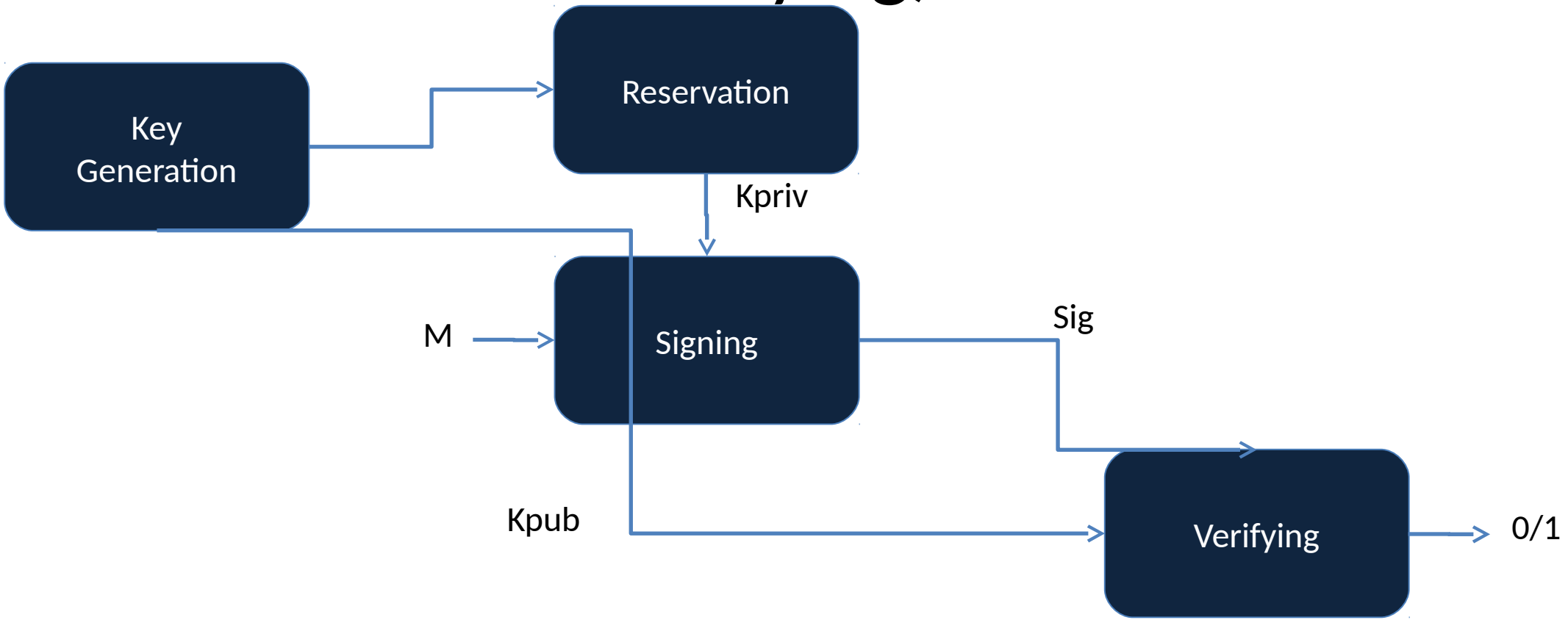
- Synchronization delay — Performance
- Synchronization failure — Security; testable
  - Implementation problem
- Nonvolatile cloning — Security; not testable
  - System backup
- Volatile cloning
  - VM cloning



Scheme = (Key Generation, Signing, Verifying)



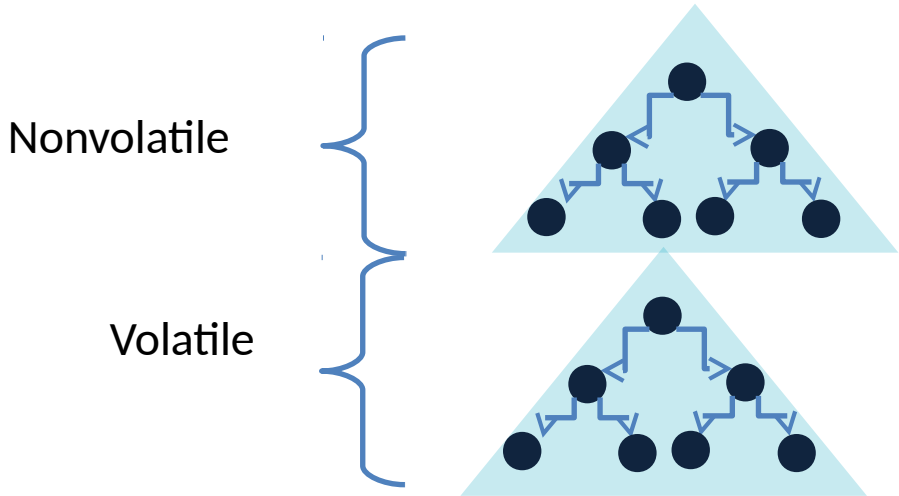
Scheme = (Key Generation, **Reservation**, Signing, Verifying)



Signing with State Reservation

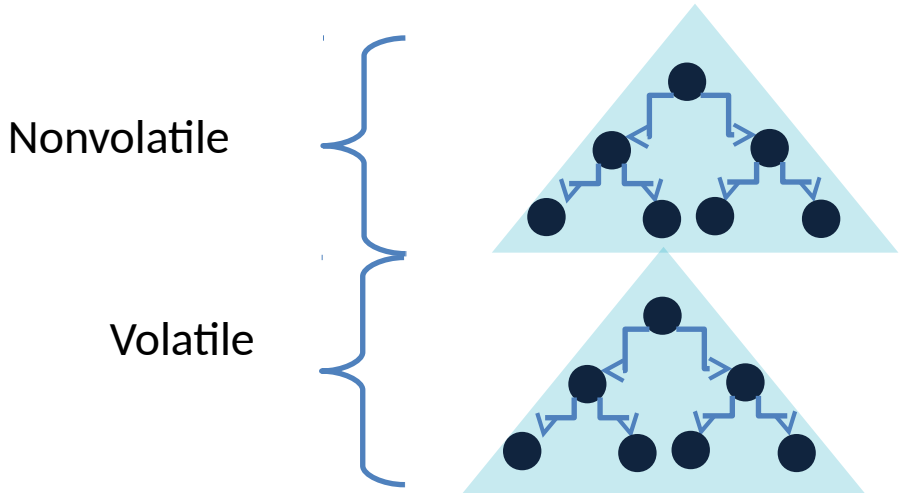
```
{
  reserve next R OTS keys Kj, Kj+1, … , Kj+R
    while j < R {
        sign message Mj with Kj and increment i
  }
}
```

Hierarchical signatures and state reservation



Hierarchical signatures and state reservation

- Synchronization delay **SOLVED**
- Synchronization failure **SOLVED**
- Unintended cloning **NOT SOLVED**
  - Nonvolatile **NONISSUE**
  - Volatile

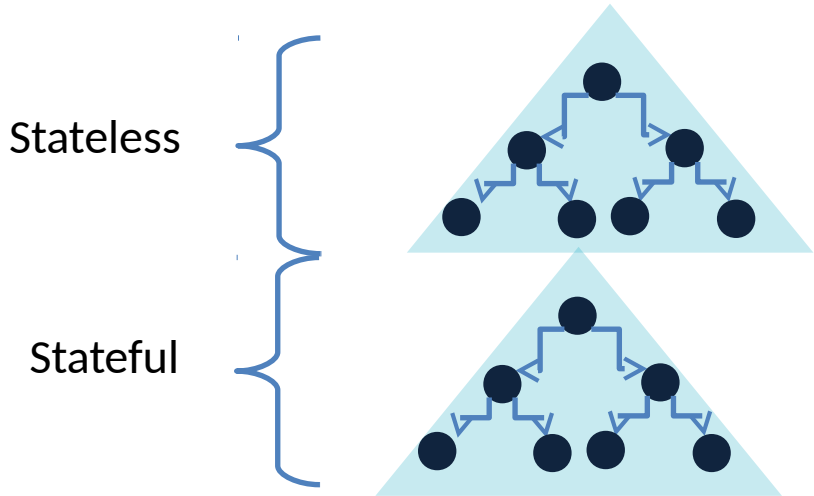


Stateless HBS

- No synchronization or cloning issues!
- SPHINCS
  - ~ 45 KB signatures
  - Significantly slower signing times

Hybrid stateful/stateless signatures

- Synchronization delay **SOLVED**
- Synchronization failure **SOLVED**
- Unintended cloning **SOLVED**
  - Nonvolatile **NONISSUE**
  - Volatile



1979 Technology Rocks!