Continuous Non-Malleable Secret Sharing

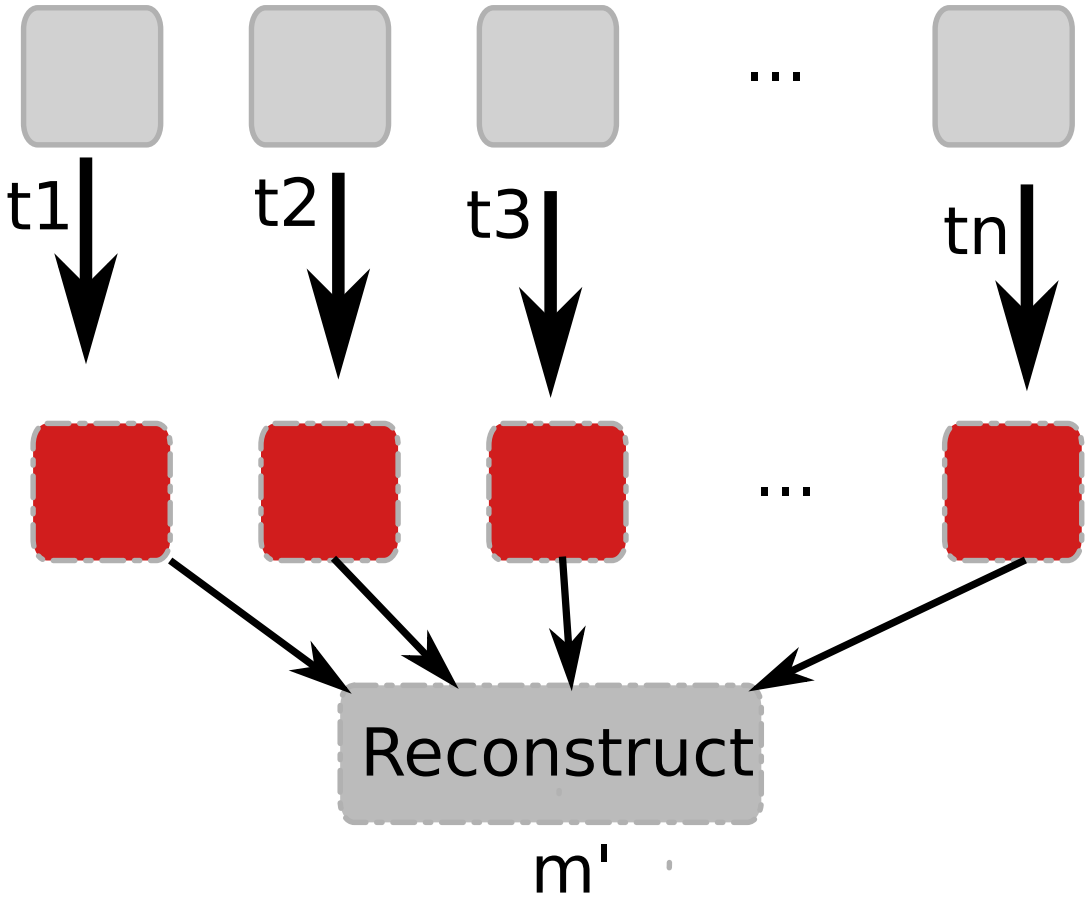
A. Faonio
IMDEA Software Institute.


Secret Sharing

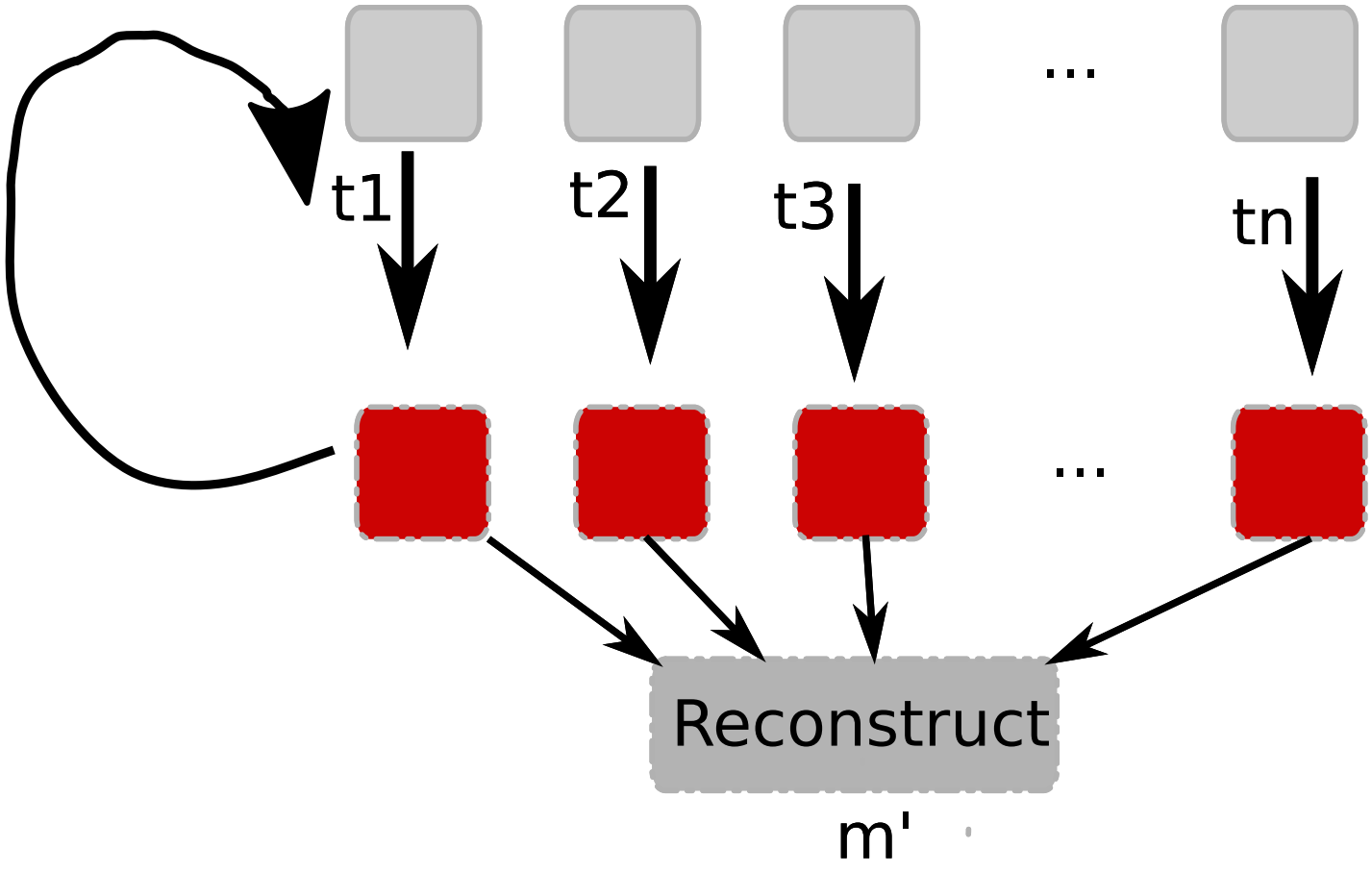

Secret Sharing
Non-Malleability

Goyal and Kumar STOC'18: Non-Malleable Secret Sharing!

Goyal and Kumar STOC'18: Non-Malleable Secret Sharing!



Goyal and Kumar STOC'18: Non-Malleable Secret Sharing!



Continuous?

Our results: simple compiler, rate-1, split-state, based on one-way function only.

How do we do it:

- A **special** CNM Code (2-out-of-2 CNM-Secret Share)
- A threshold SS
- Authenticated Encryption

Our results: simple compiler, rate-1, split-state, based on one-way function only.

How do we do it:

- A **special** CNM Code (2-out-of-2 CNM-Secret Share)
- A threshold SS
- Authenticated Encryption
- Love