Brief Announcement: Robust and Private Distributed Shared Atomic Memory in Message Passing Networks

PODC'15

Shlomi Dolev [1] **Thomas Petig** [2] Elad M. Schiller [2]

[1]Ben-Gurion University of the Negev

[2]Chalmers University of Technology
Gothenburg University

Distributed Computing and Systems
Chalmers university of technology

August 21, 2015

Content

We focus on emulation **shared memory** in **message passing** networks.

Opportunity: Cadambe et al. (2014): A **coded shared atomic memory algorithm** for message passing architectures.

We are going to see how to provide

- **robustness** against semi-Byzantine attacks,
  - i.e., corruption of stored data,
- and **privacy** of the data.

in these networks.

Content

We focus on emulation **shared memory** in **message passing** networks.

Opportunity: Cadambe et al. (2014): A **coded shared atomic memory algorithm** for message passing architectures.

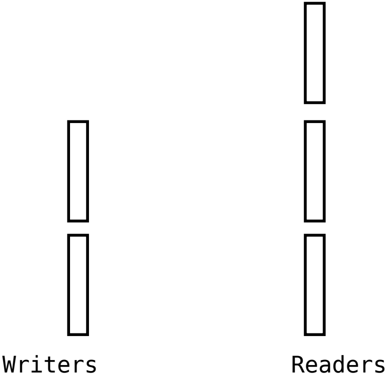
We are going to see how to provide

- **robustness** against semi-Byzantine attacks,
  - i.e., corruption of stored data,
- and **privacy** of the data.

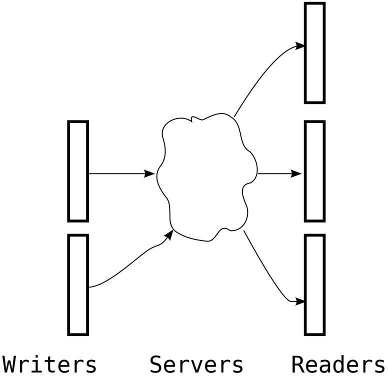
in these networks.

We use **Reed-Solomon codes**

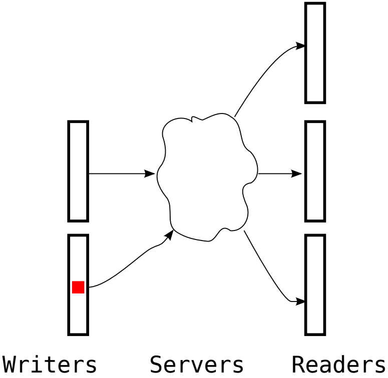
Multi Reader Multi Writer Shared Memory in Message Passing Networks



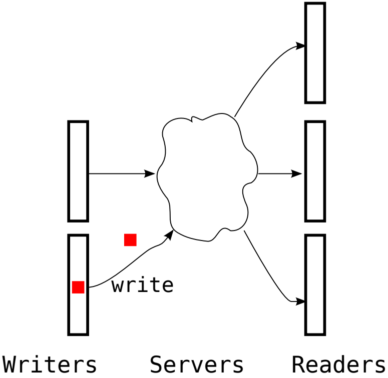
Multi Reader Multi Writer Shared Memory in Message Passing Networks



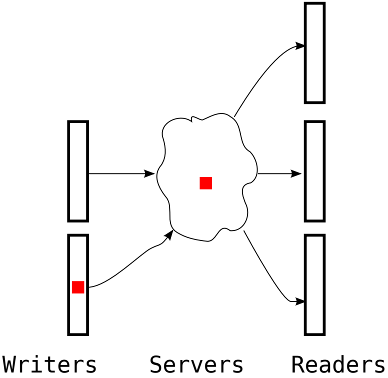
Multi Reader Multi Writer Shared Memory in Message Passing Networks



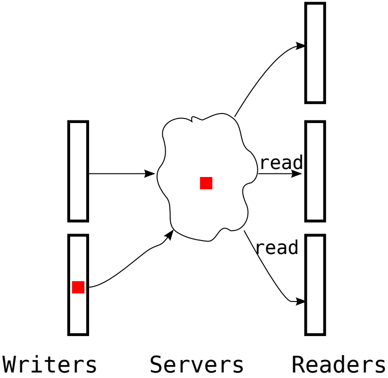
Multi Reader Multi Writer Shared Memory in Message Passing Networks



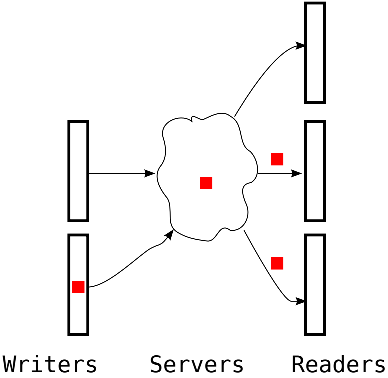
Multi Reader Multi Writer Shared Memory in Message Passing Networks



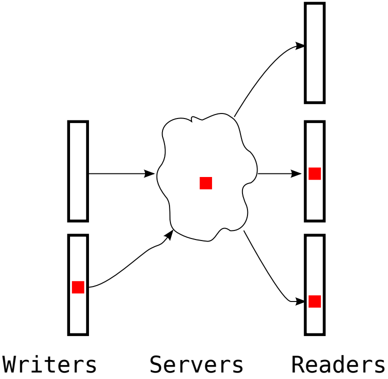
Multi Reader Multi Writer Shared Memory in Message Passing Networks



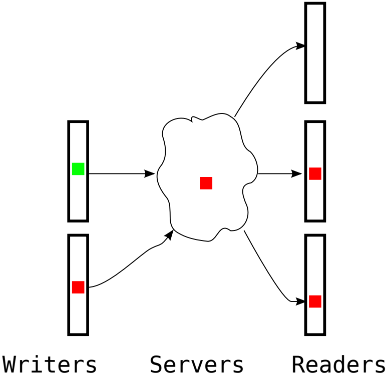
Multi Reader Multi Writer Shared Memory in Message Passing Networks



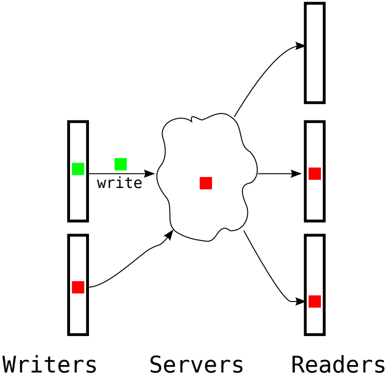
Multi Reader Multi Writer Shared Memory in Message Passing Networks



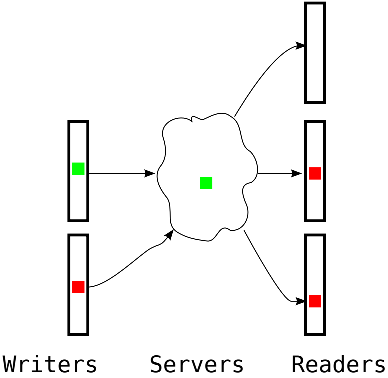
Multi Reader Multi Writer Shared Memory in Message Passing Networks



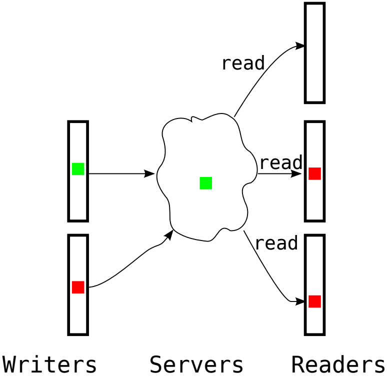
Multi Reader Multi Writer Shared Memory in Message Passing Networks



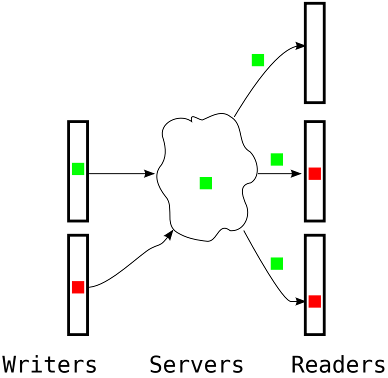
Multi Reader Multi Writer Shared Memory in Message Passing Networks



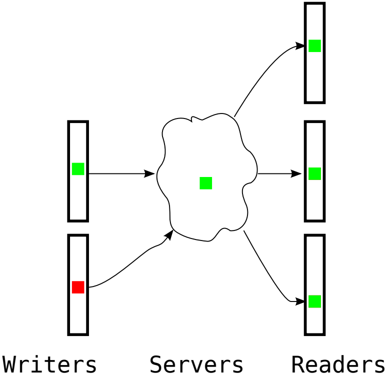
Multi Reader Multi Writer Shared Memory in Message Passing Networks



Multi Reader Multi Writer Shared Memory in Message Passing Networks



Multi Reader Multi Writer Shared Memory in Message Passing Networks



Multi Reader Multi Writer Shared Memory in Message Passing Networks

(Most) related work: Attiya, Bar-Noy, and Dolev (ABD), Cadambe et. al

Cadambe et al. address the following:

- atomicity and liveness and
- storage and communication costs.

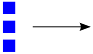
They solve atomicity and liveness in a ABD-like manner.

Erasure Coding: (N, k)-maximum distance separable codes

- length k vector $\rightarrow$ length N vector.
- tolerates $\leq N - k$ erasures.

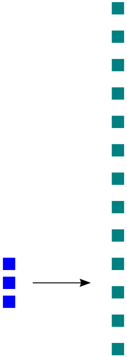
Erasure Coding: (N, k)-maximum distance separable codes

- length k vector → length N vector.
- tolerates $\leq N - k$ erasures.



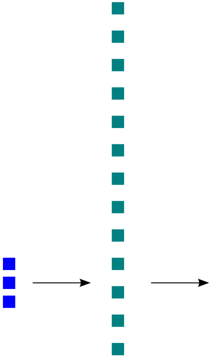
Erasure Coding: (N, k)-maximum distance separable codes

- length k vector → length N vector.
- tolerates $\leq N - k$ erasures.



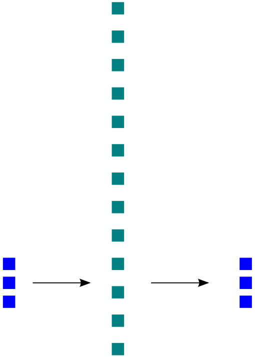
Erasure Coding: (N, k)-maximum distance separable codes

- length k vector → length N vector.
- tolerates $\leq N - k$ erasures.



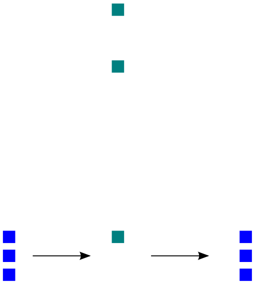
Erasure Coding: (N, k)-maximum distance separable codes

- length k vector → length N vector.
- tolerates $\leq N - k$ erasures.



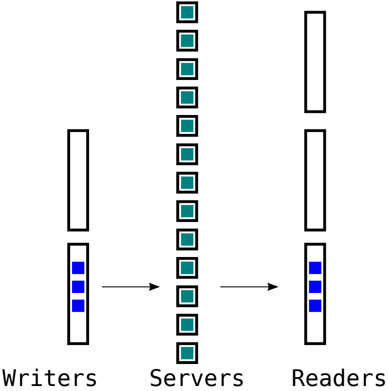
Erasure Coding: (N, k)-maximum distance separable codes

- length k vector → length N vector.
- tolerates $\leq N - k$ erasures.



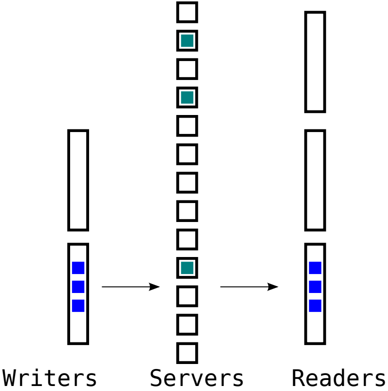
Coded Atomic Storage Algorithm

- N servers.
- $\lceil \frac{N+k}{2} \rceil$-quorums.



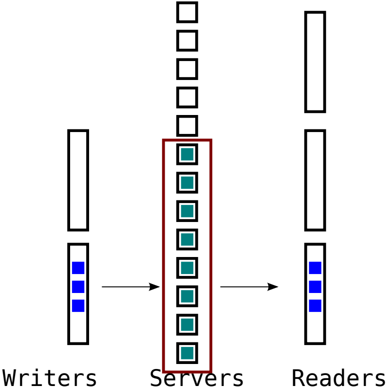
Coded Atomic Storage Algorithm

- N servers.
- $\lceil \frac{N+k}{2} \rceil$-quorums.



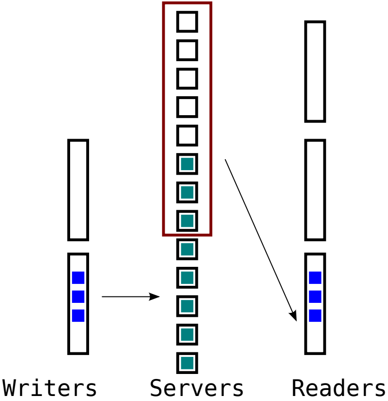
Coded Atomic Storage Algorithm

- N servers.
- $\lceil \frac{N+k}{2} \rceil$-quorums.



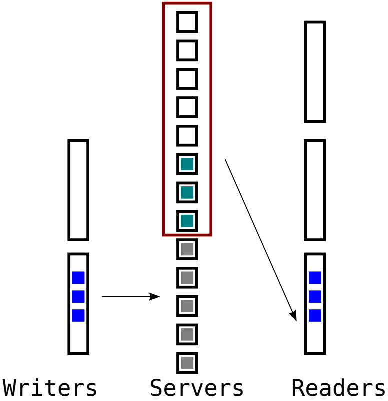
Coded Atomic Storage Algorithm

- N servers.
- $\lceil \frac{N+k}{2} \rceil$-quorums.



Coded Atomic Storage Algorithm

- N servers.
- $\lceil \frac{N+k}{2} \rceil$-quorums.



Our contribution

We address:

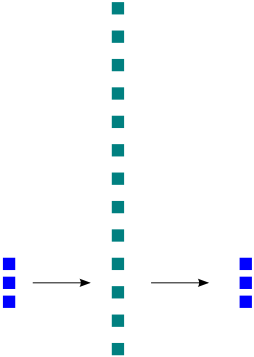
- Robustness against semi-Byzantine attacks.
- Privacy of the data.

We use

- (N, k)-**Reed-Solomon** codes and
- **Berlekamp-Welch** error correction.

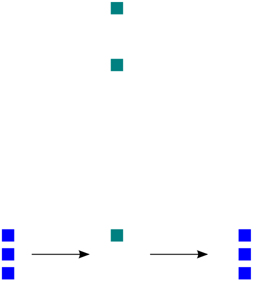
Robust and Private Coded Atomic Storage

- (N, k)-Reed-Solomon code.
- For e corrupt elements, we need to read $2e$ more elements.



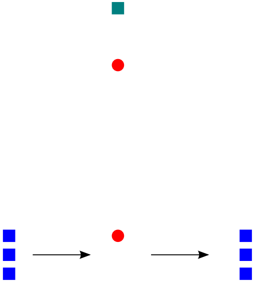
Robust and Private Coded Atomic Storage

- (N, k)-Reed-Solomon code.
- For e corrupt elements, we need to read $2e$ more elements.



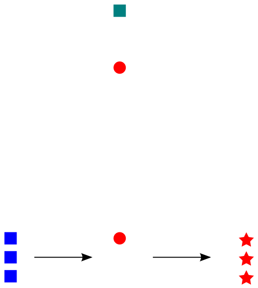
Robust and Private Coded Atomic Storage

- (N, k)-Reed-Solomon code.
- For e corrupt elements, we need to read $2e$ more elements.



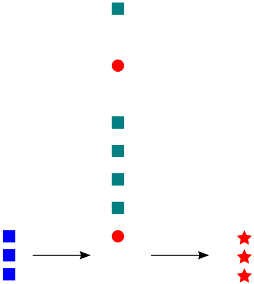
Robust and Private Coded Atomic Storage

- (N, k)-Reed-Solomon code.
- For e corrupt elements, we need to read $2e$ more elements.



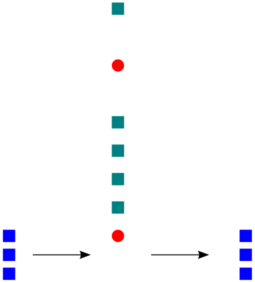
Robust and Private Coded Atomic Storage

- (N, k)-Reed-Solomon code.
- For e corrupt elements, we need to read $2e$ more elements.



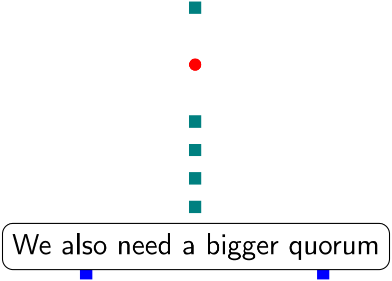
Robust and Private Coded Atomic Storage

- (N, k)-Reed-Solomon code.
- For e corrupt elements, we need to read $2e$ more elements.



Robust and Private Coded Atomic Storage

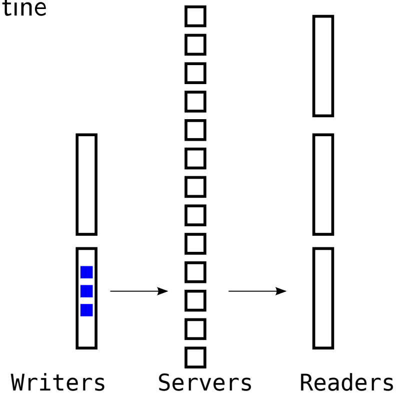
- (N, k)-Reed-Solomon code.
- For e corrupt elements, we need to read $2e$ more elements.



We also need a bigger quorum

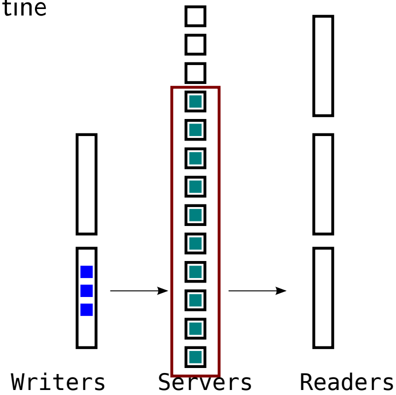
Robust and Private Coded Atomic Storage

- $\lceil \frac{N+k+2e}{2} \rceil$-quorums.
- Up to $f < N - \lceil \frac{N+k+2e}{2} \rceil$ failures.
- Up to e semi-Byzantine servers.



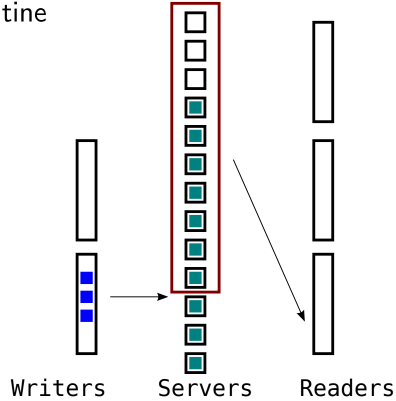
Robust and Private Coded Atomic Storage

- $\lceil \frac{N+k+2e}{2} \rceil$-quorums.
- Up to $f < N - \lceil \frac{N+k+2e}{2} \rceil$ failures.
- Up to e semi-Byzantine servers.



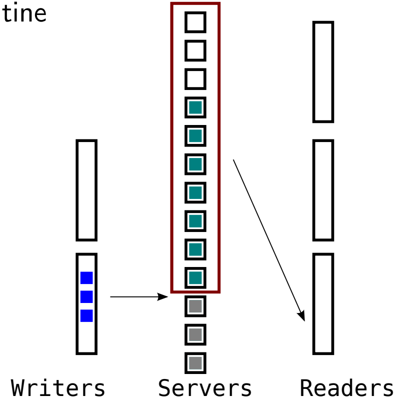
Robust and Private Coded Atomic Storage

- $\lceil \frac{N+k+2e}{2} \rceil$-quorums.
- Up to $f < N - \lceil \frac{N+k+2e}{2} \rceil$ failures.
- Up to e semi-Byzantine servers.



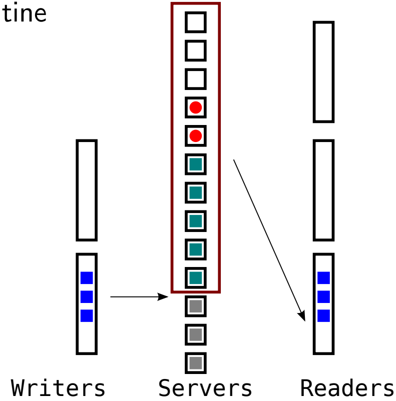
Robust and Private Coded Atomic Storage

- $\lceil \frac{N+k+2e}{2} \rceil$-quorums.
- Up to $f < N - \lceil \frac{N+k+2e}{2} \rceil$ failures.
- Up to e semi-Byzantine servers.



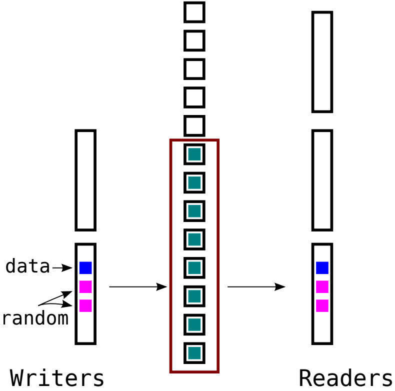
Robust and Private Coded Atomic Storage

- $\lceil \frac{N+k+2e}{2} \rceil$-quorums.
- Up to $f < N - \lceil \frac{N+k+2e}{2} \rceil$ failures.
- Up to e semi-Byzantine servers.



Robust and Private Coded Atomic Storage

- McEliece & Sarwate: Reed-Solomon codes are related to Shamir's **secret sharing**.
- Only sets of $\geq k$ server can reveal the secret.



Conclusion

Using special cases of coding (Reed-Solomon) and decoding (Berlekamp-Welch), we show:

- *robustness*, corrupted data by Byzantine server can be tolerated and
- *privacy*, even a small amount of server cannot restore the data.