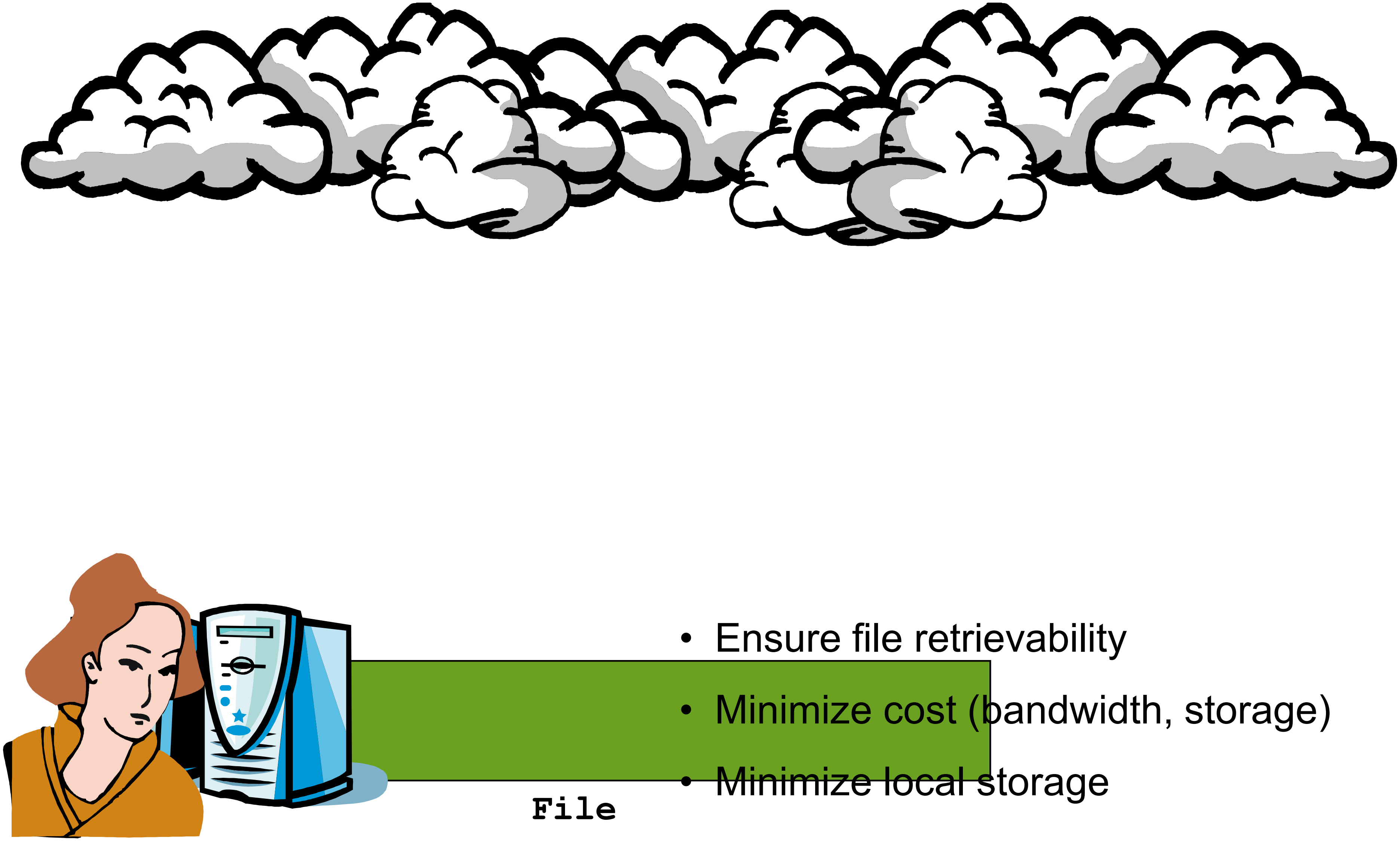
Proofs of Retrievability: Theory and Implementation

Kevin Bowers, Ari Juels & Alina Oprea
RSA Laboratories

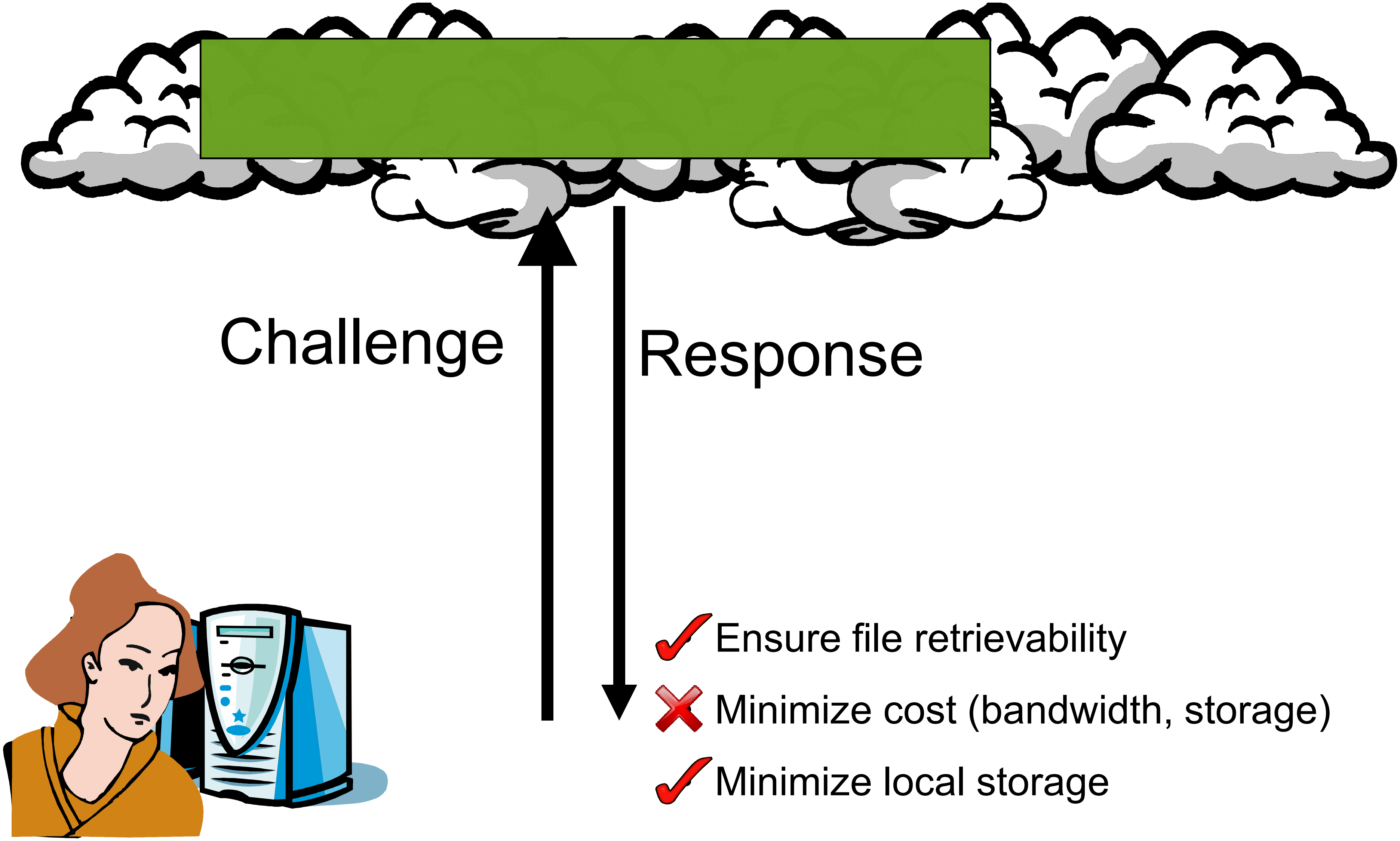
November 27, 2009

The Setup



- Ensure file retrievability
- Minimize cost (bandwidth, storage)
- Minimize local storage

Simple Approach



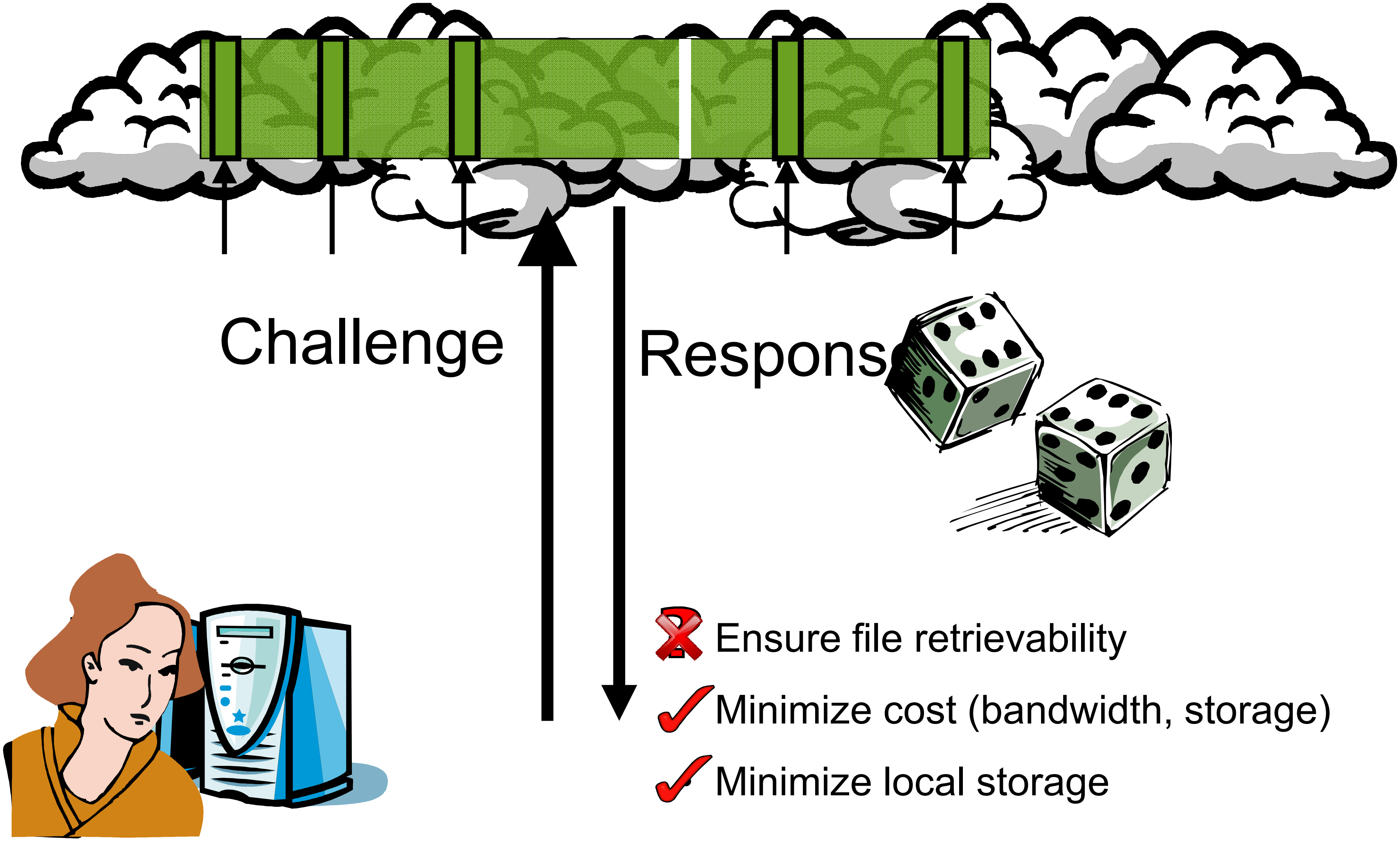
Challenge

Response

- ✓ Ensure file retrievability
- ✗ Minimize cost (bandwidth, storage)
- ✓ Minimize local storage

Sampling

EMC²
where information lives®

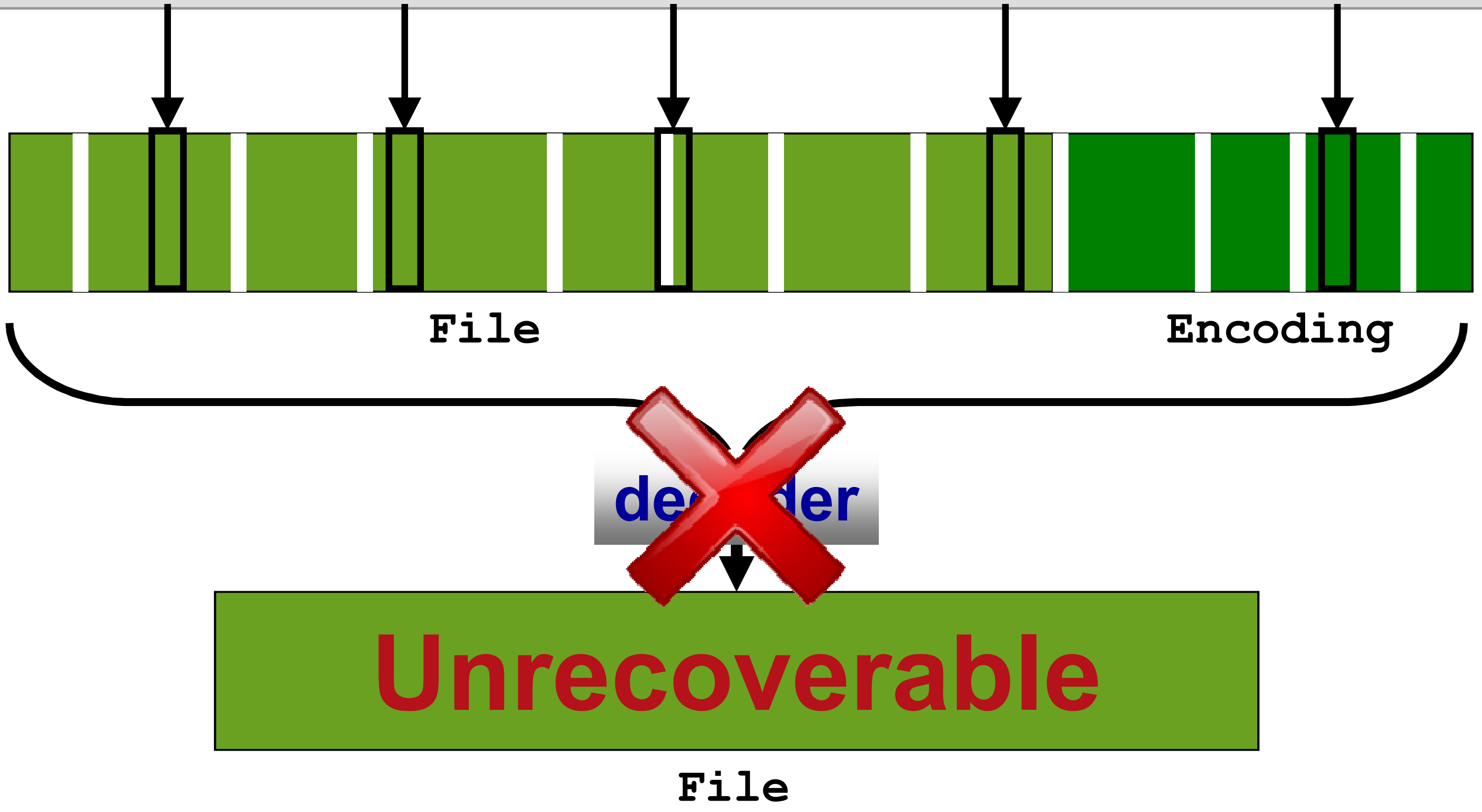


Challenge

Respons

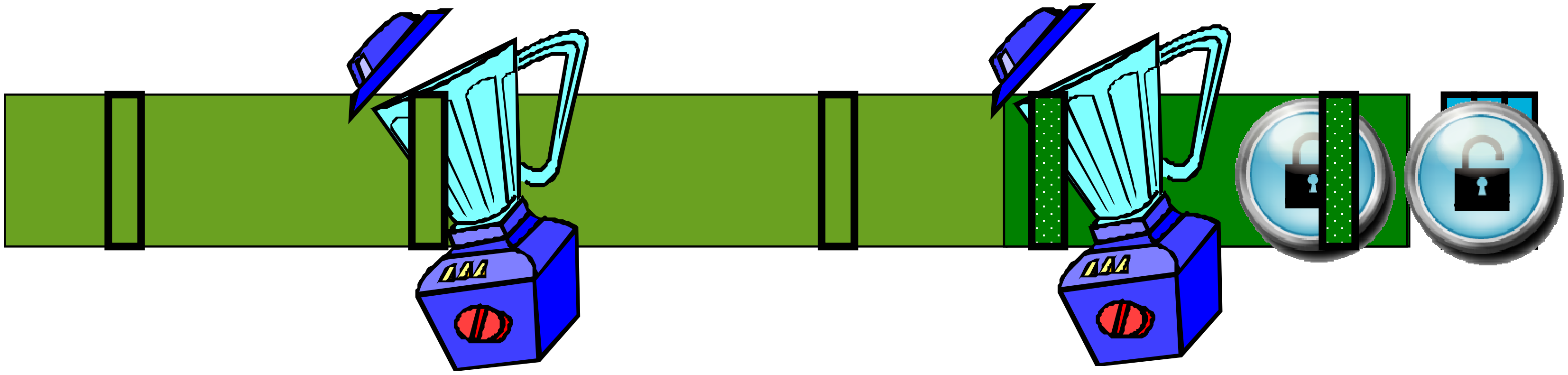
- ✗ Ensure file retrievability
- ✓ Minimize cost (bandwidth, storage)
- ✓ Minimize local storage

Encoding

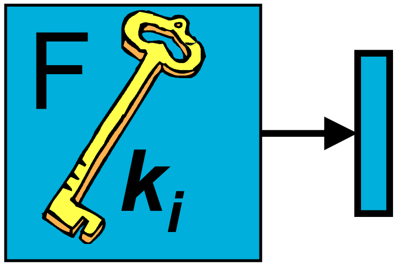


- Ensure file retrievability
- Minimize cost (bandwidth, storage)
- Minimize local storage

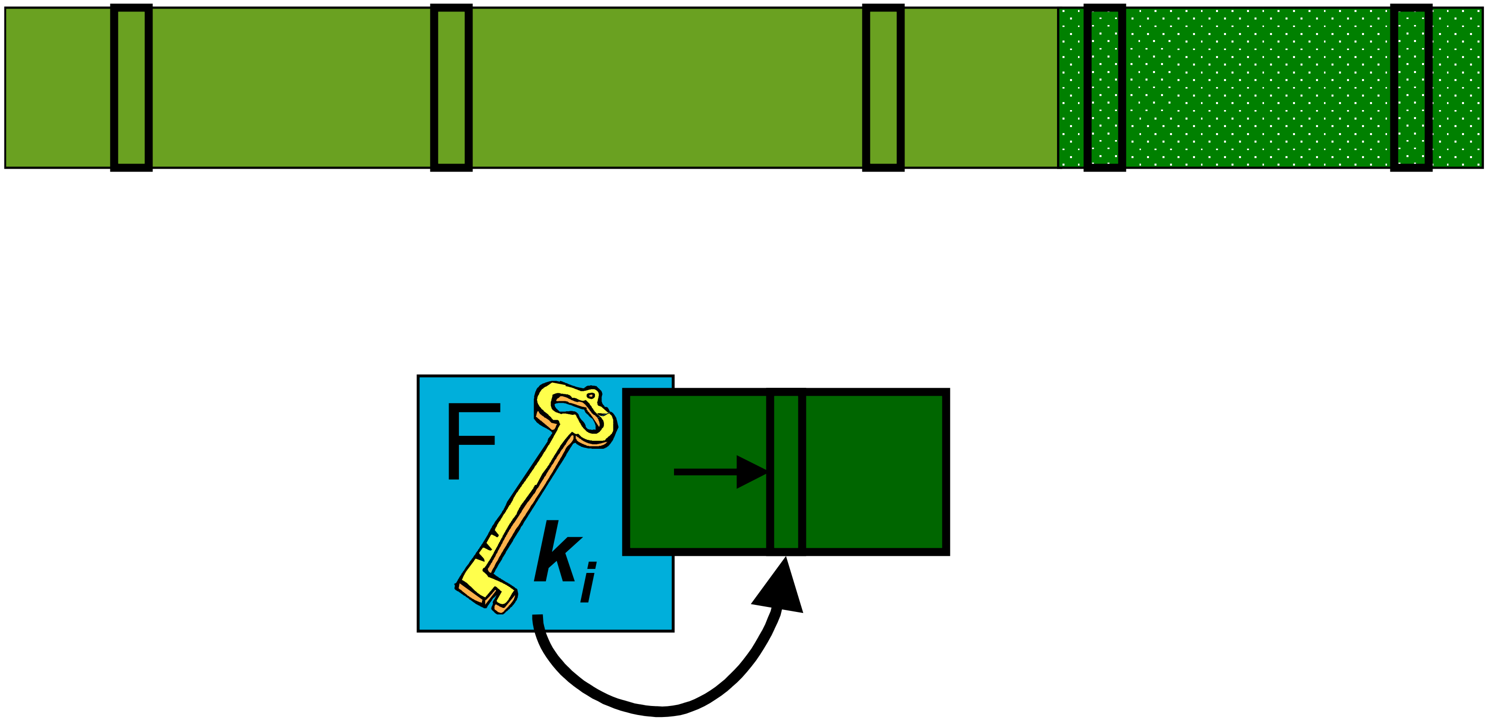
Adversarial Encoding



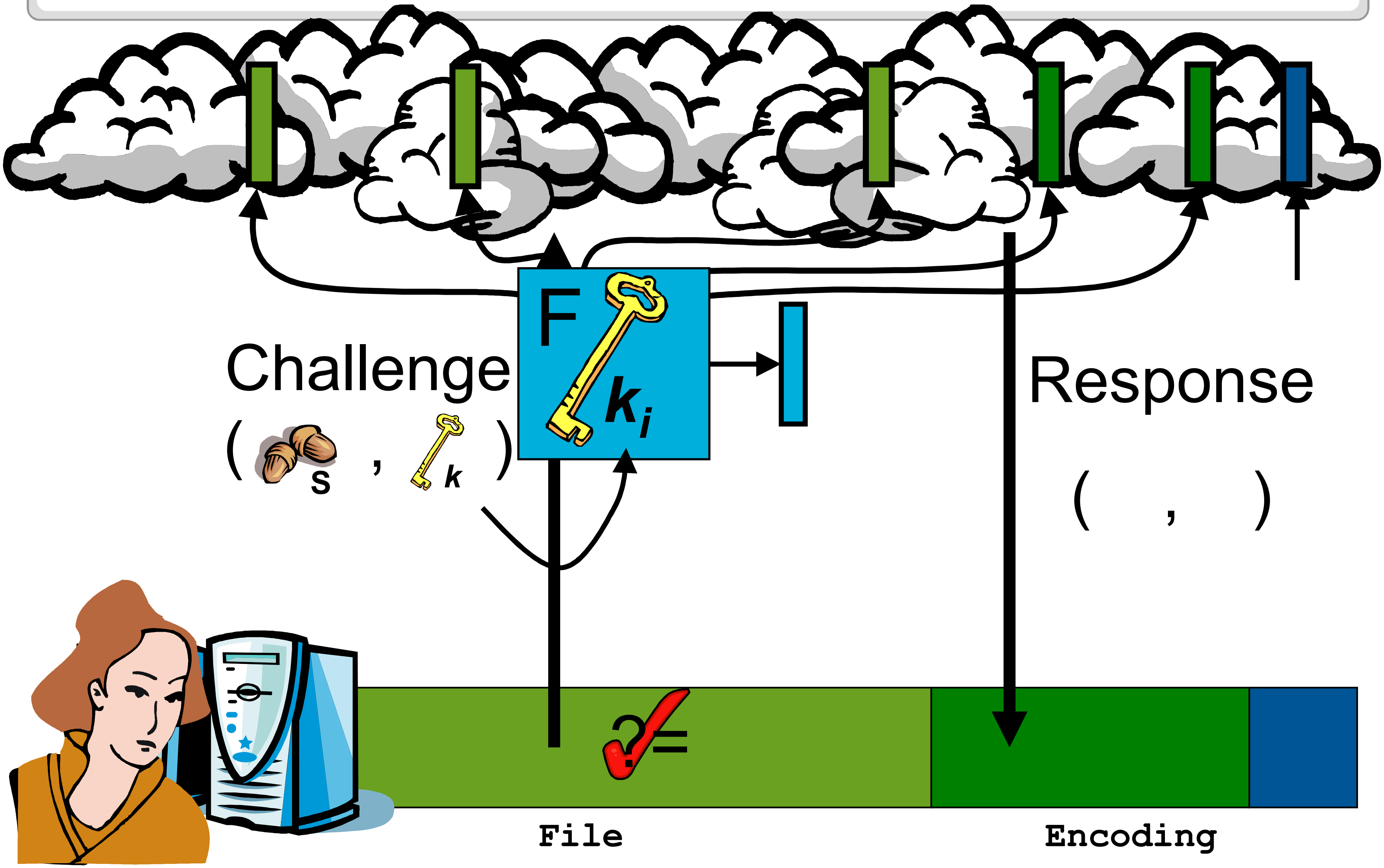
- Rearrange file
- Compute ECC values
- Return file to original order
- Rearrange and encrypt ECC values
- Pre-compute and encrypt responses



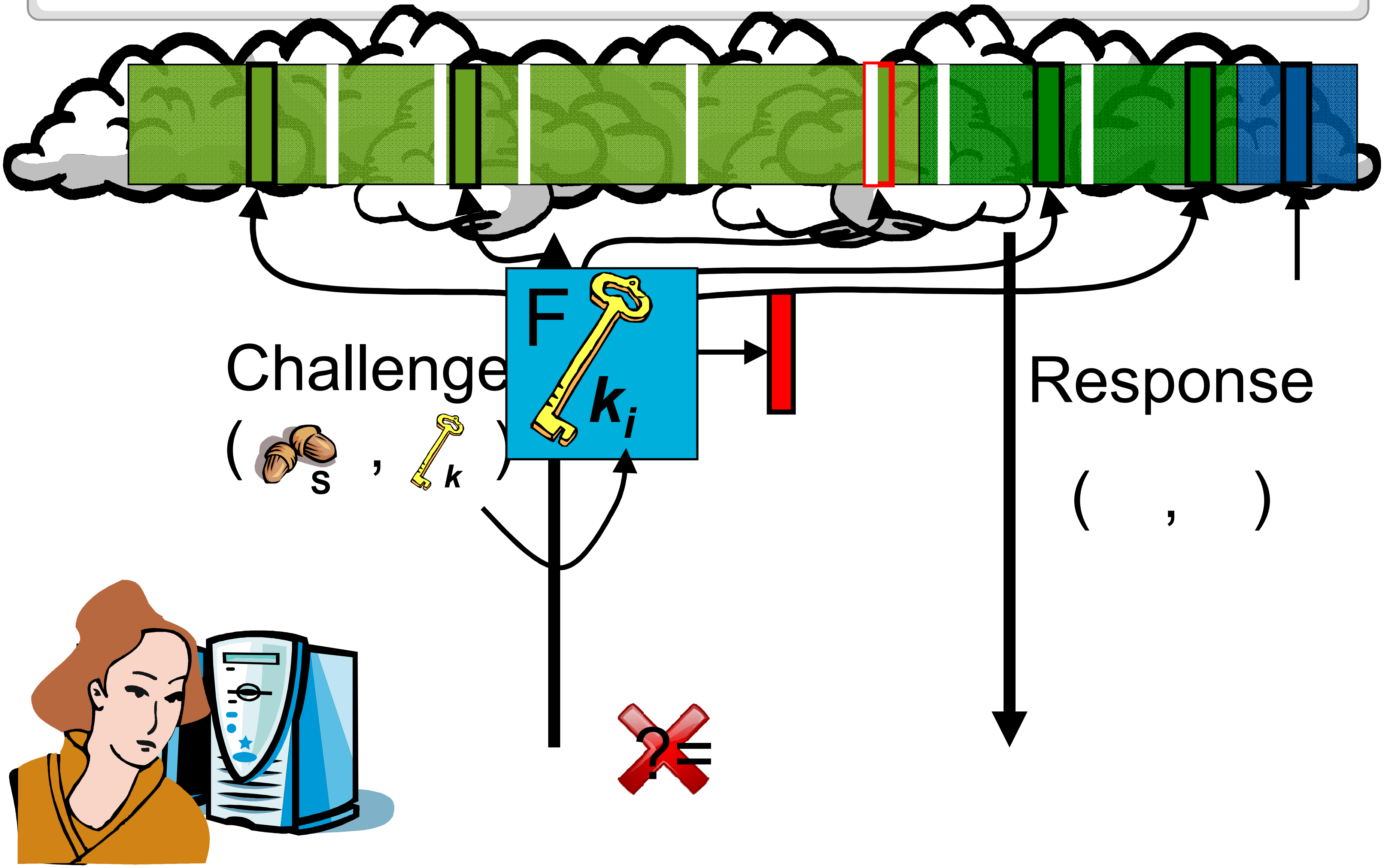
Aggregation Code



Proof of Retrievability



Proof of Retrievability



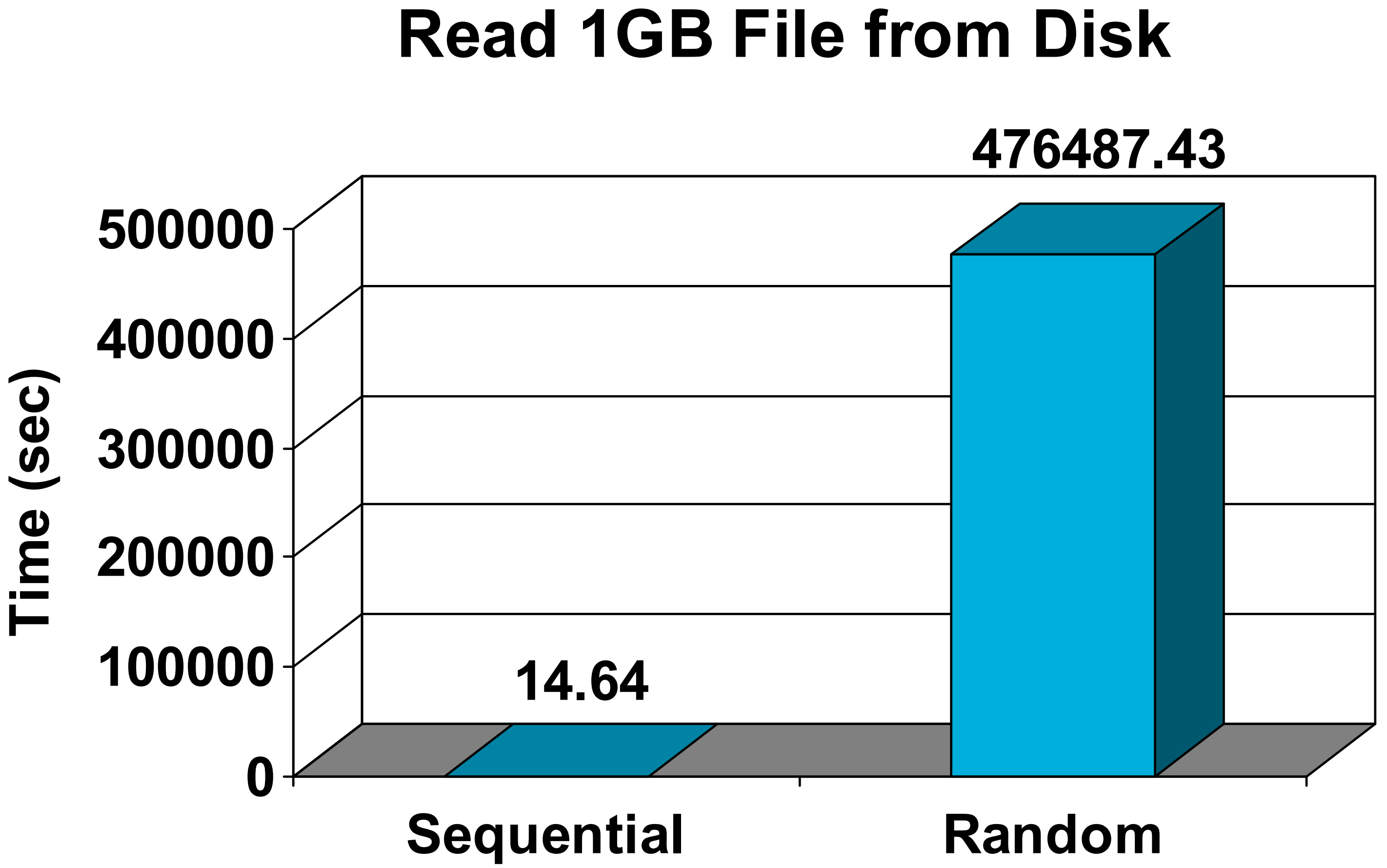
Intermediate PRPs

Ordinal Sorting	<	?	<	Cycle Walking	<	Block Ciphers
2^{25}				2^{55}		2^{64}

- 6-Round Feistel construction using AES-based Ordinal Sorting

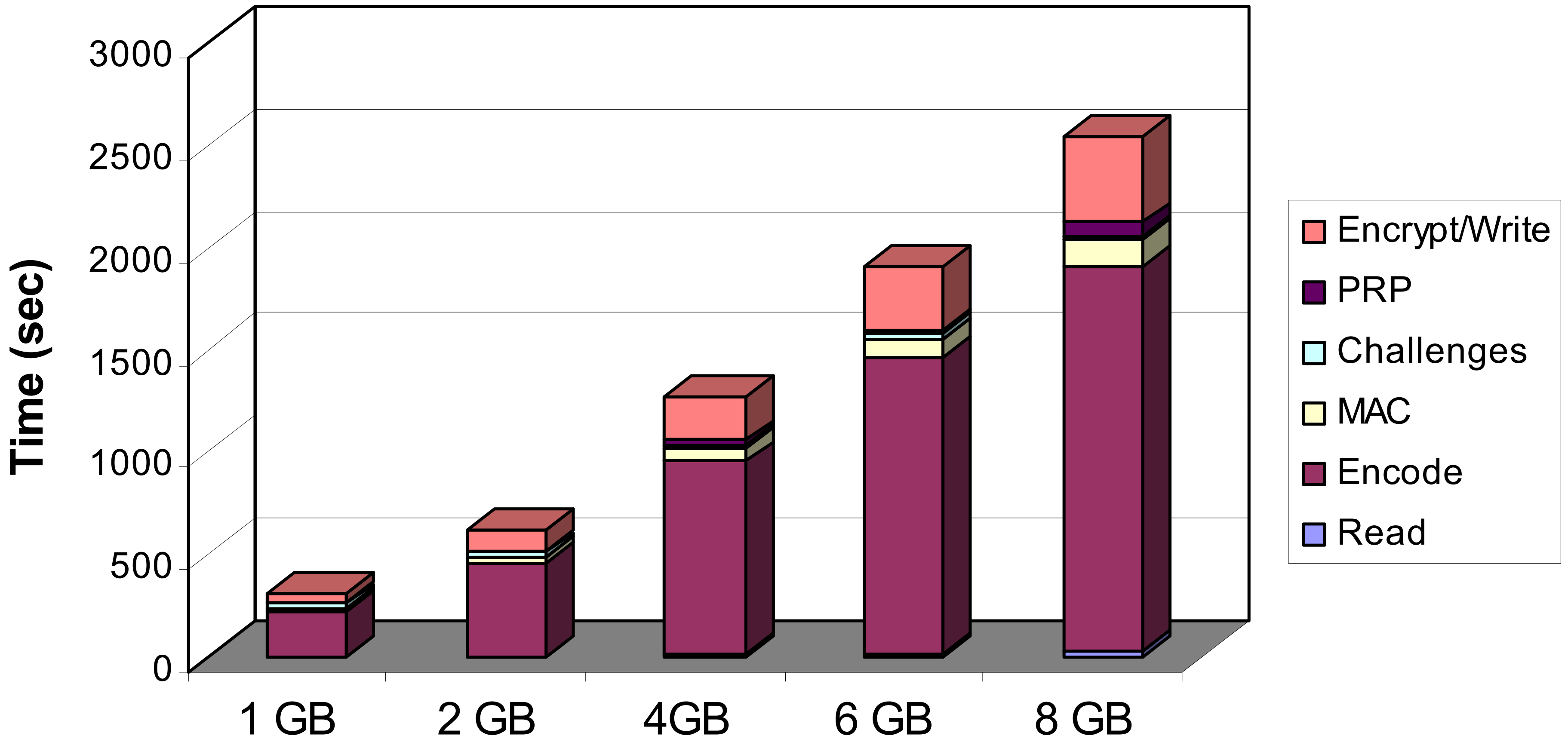
Incremental Encoding

- Seek: 10 ms, Latency: 4.2 ms, Throughput: 70 MB/sec



Performance

POR Encoding



Questions

Proofs of Retrievability: Theory and Implementation

Kevin Bowers, Ari Juels, & Alina Oprea

http://www.rsalabs.com

Questions?

EMC^{2}®

where information lives®