



# POST: A Secure, Resilient, Cooperative Messaging System

A. Mislove, A. Post, C. Reis, P. Willmann, P. Druschel,  
D. S. Wallach *Rice University*

X. Bonnaire, P. Sens, J.-M. Busca, L. Arantes-Bezerra  
*University of Paris 6 (LIP6)*



# Motivation

---

- Provide a generic, serverless platform for user-driven collaborative applications (email, IM, calendars, etc.)
- Show that a wide range collaborative services can be supported by one serverless platform securely, with high availability
- Demonstrate that p2p paradigm is mature enough to support secure, resilient, “mission-critical” applications



# POST Architecture

---

- Provides three basic services to applications:
  - Secure single-copy message storage
  - User metadata based on single-writer logs
  - Event notification
- These basic services are sufficient to support a variety of collaborative applications



# Sample Application: ePOST

---

- Email service based on POST
  - Email is a well-understood, demanding application
  - Availability of realistic workloads
- Interoperates seamlessly with existing email protocols and clients (IMAP, SMTP, Outlook, etc...)
- Participating organizations remain autonomous
  - Local storage controlled by local participants by scoped insertion
- Provides better spam prevention
  - Crypto-based message authentication and privacy
  - Sender overhead is proportional to the number of recipients
  - Receivers pull messages



# Experimental Setup

---

- Implemented ePOST prototype

Performs well

- Realistic ePOST storage requirements?

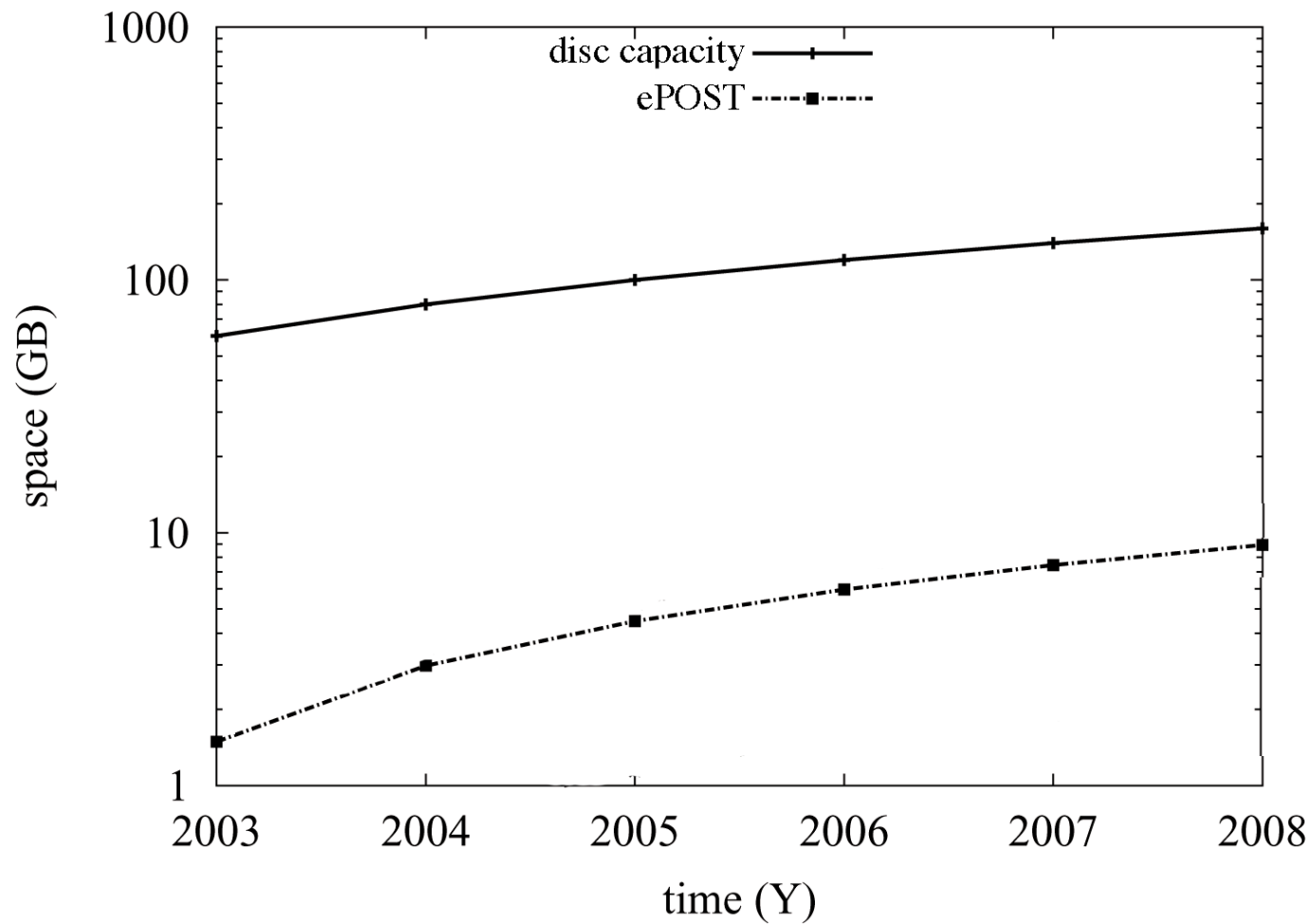
Examined email usage by ~250 members of Rice CS department

Conservative assumptions:

- No deletion
- Local insertion
- Full replication with 10 replicas
- All messages are unique

# ePOST Storage Requirements

ePOST Storage Requirements





# Status and Conclusions

---

- Ongoing work:

  - We plan to begin using prototype as primary email system this summer

  - Answer open questions

    - Appropriate level of replication
    - Measures to ensure failure independence
    - Administrative cost

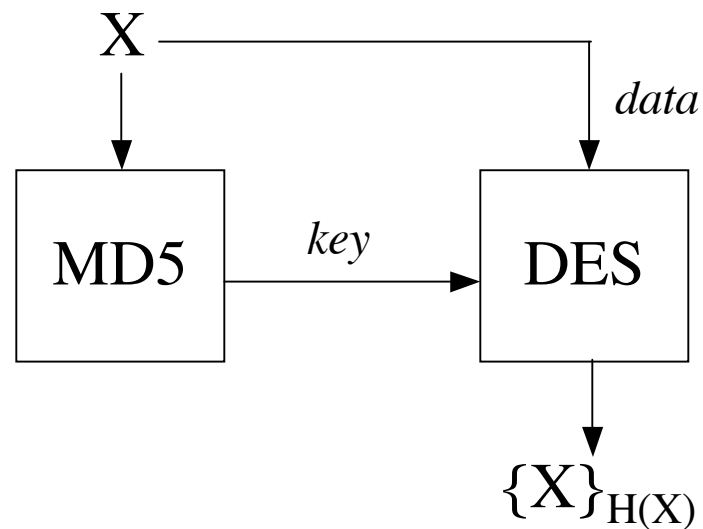
- Also working on IM and calendar applications on POST

- Related effort: p2p incentives for fair sharing of resources

# Single-copy Message Storage

---

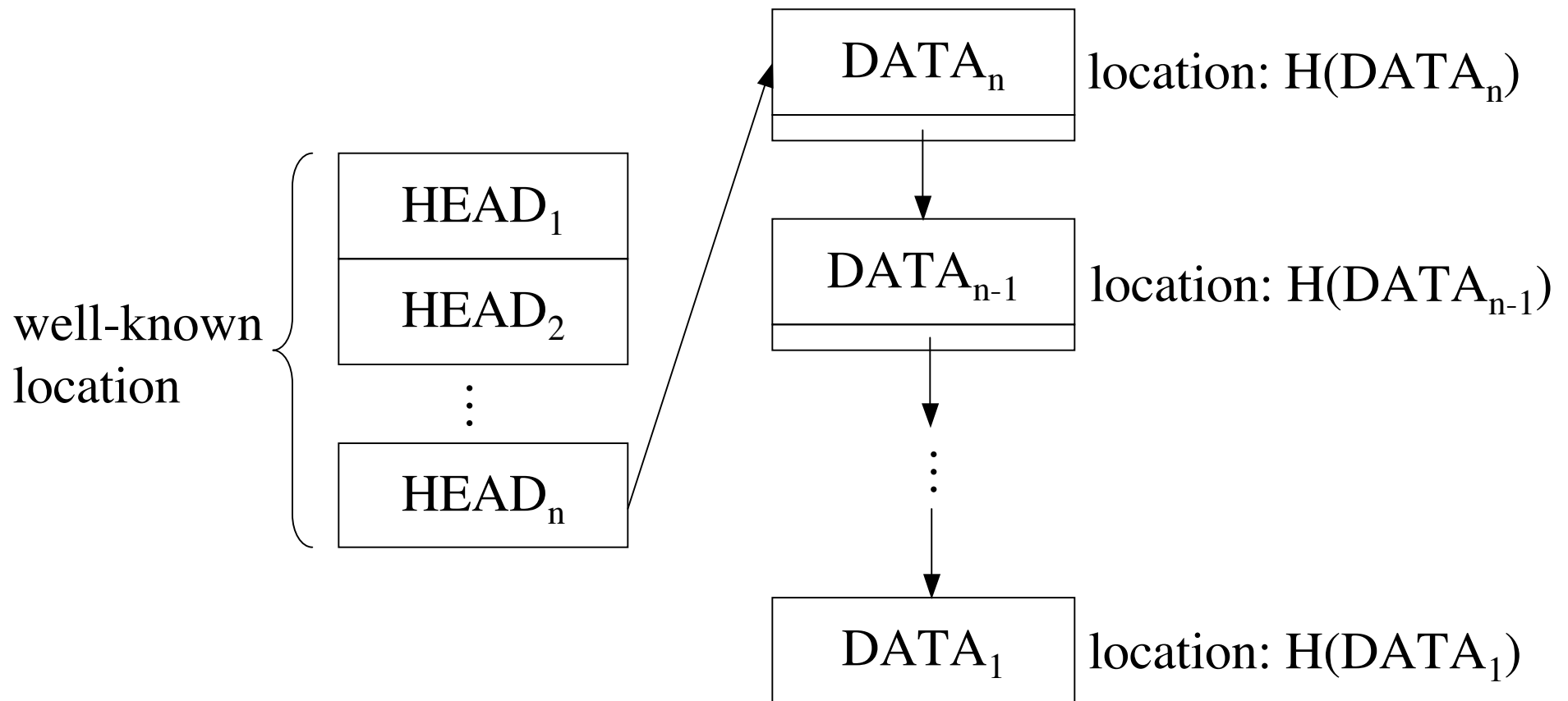
- Achieved using convergent encryption
- Allows multiple copies of encrypted data to be coalesced





# User-specific Metadata

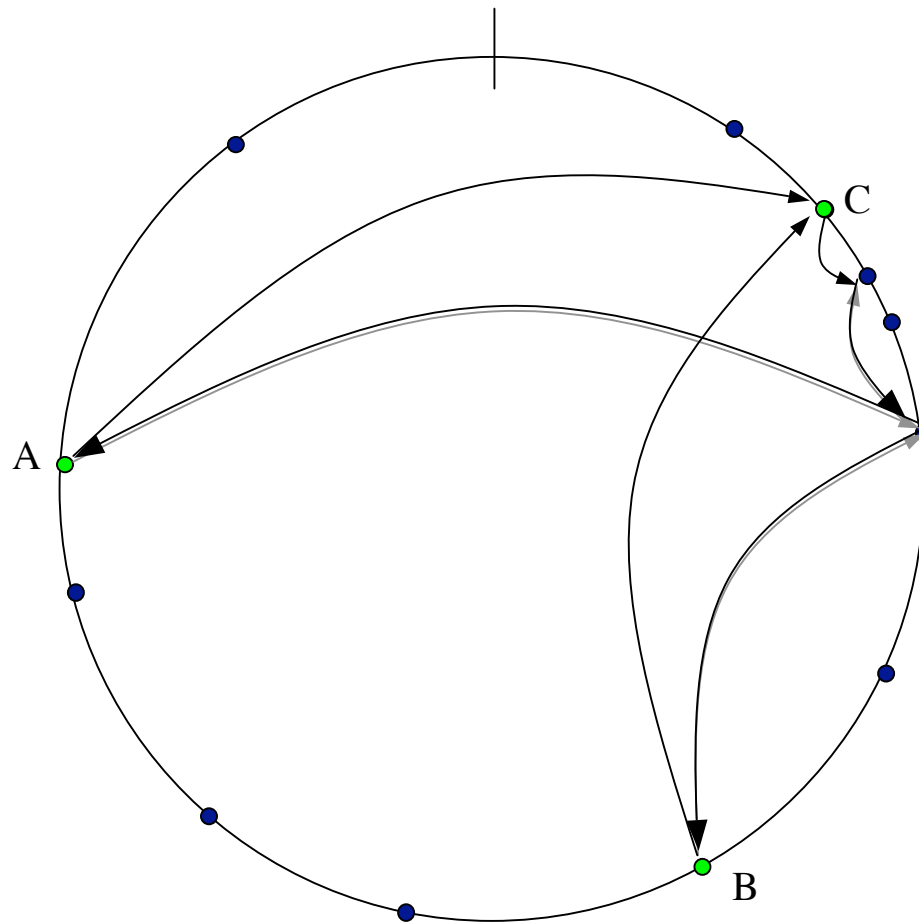
- Based on the Ivy file system



# User Notification

---

- Suppose A and B want to send to C





# Security

---