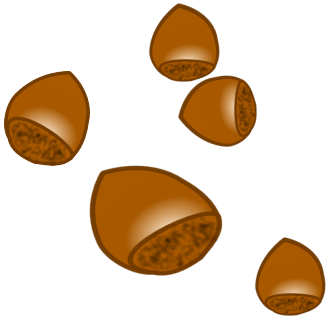
TAMIAS : A privacy-aware & secure distributed storage

Jean Lorchat, **Cristel Pelsser,**
Randy Bush, Keiichi Shima,
Kenjiro Cho, Ray Atarashi



IIJ lab report, April 19th 2011

Tamias

- Content sharing
- User: person, company, application
- personal and work storage
- A user may belong to many groups
- Sharing with other users or groups

User has fine-grained control over his data

Objectives and use cases

- Content sharing
  - User defines sharing scope
  - No trust in storage provider
    - Anyone can provide storage
  - Easy to use
  - Resilient
  - Scalable
- Use cases
  - Personal storage solution
  - Storage solution for IIJ cloud
    - For applications and humans

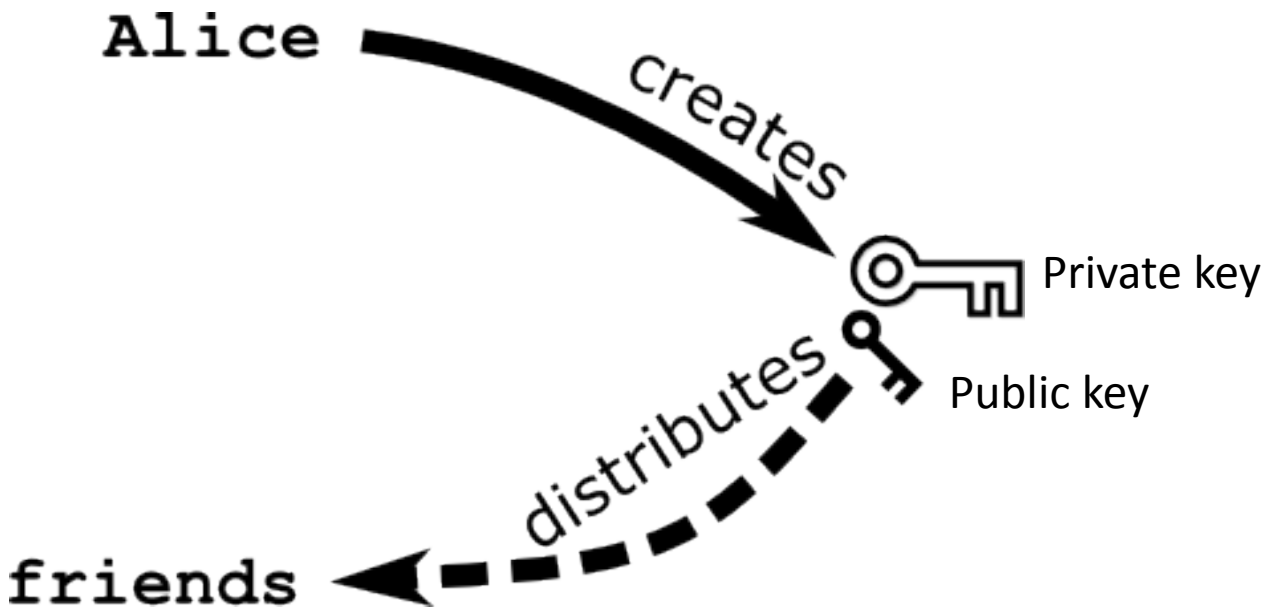
Sharing

- Sharing is offering
  - unidirectional act of giving someone access (not ownership) to data
- There is no reciprocation
  - Giving access to data does not provision a reciprocate way to receive anything from the recipient
- There may be concurrency
  - Shared data could be modified by the recipient, according to access permissions

- In our context, **sharing** needs a recipient **: identity**

Identity

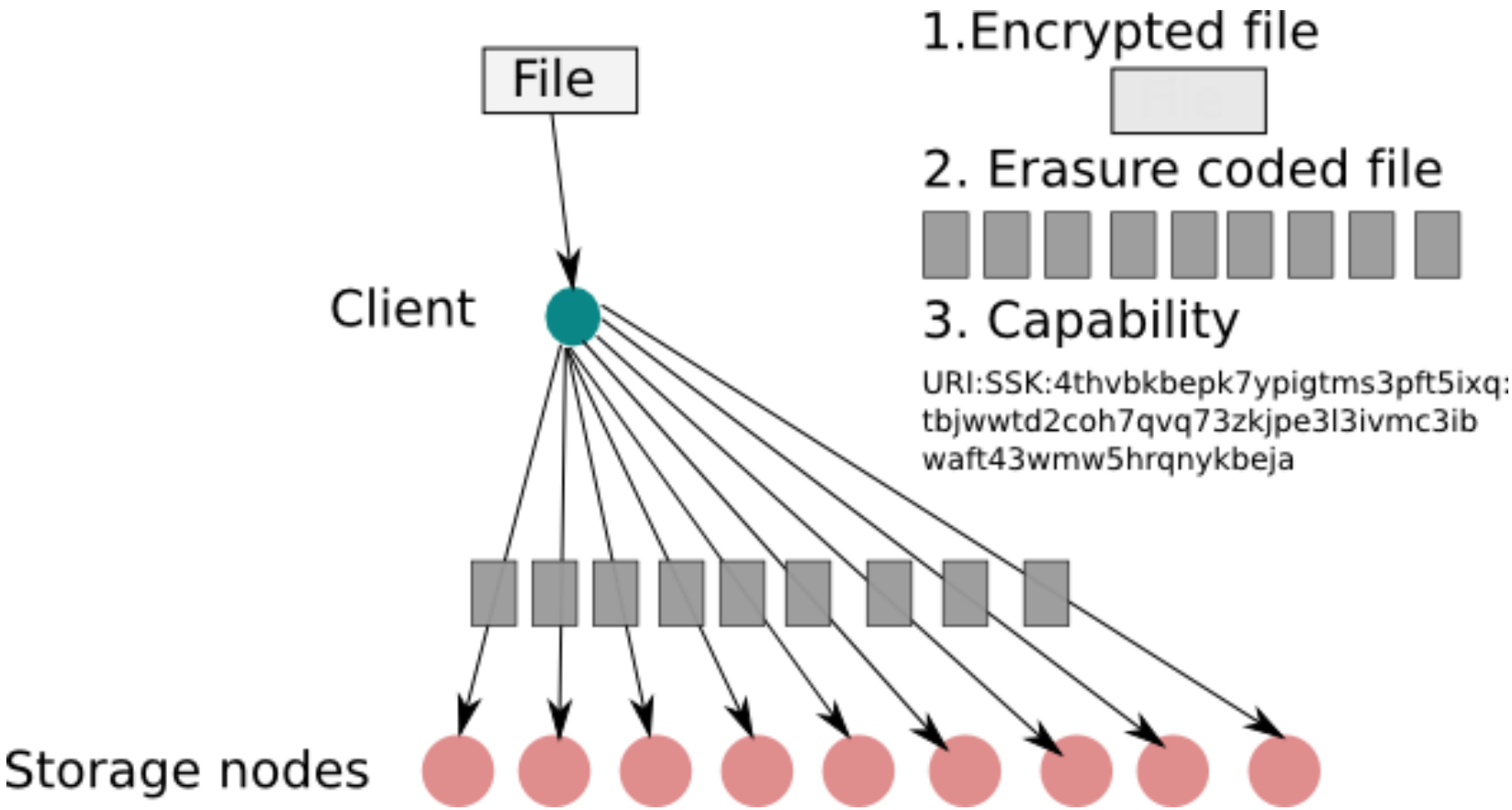
- Identity is a (private key, public key) pair
  - One person may have multiple identities
  - One identity -> content owned and accessible



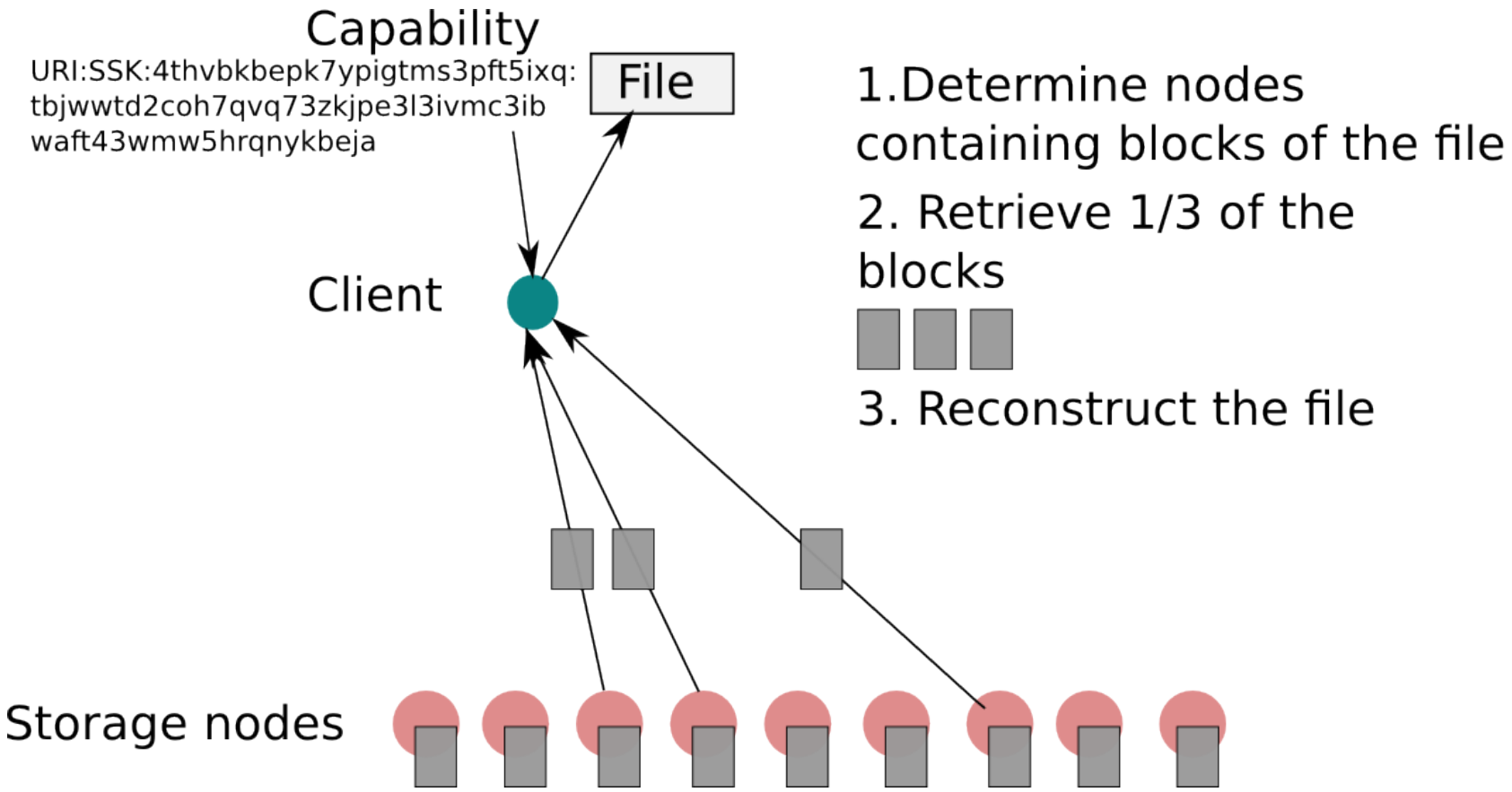
Overview

- This project is at the intersection of two classical areas of research
  - Distributed systems
  - Security and privacy
- As much as we plan to be innovative, there is no need to reinvent the wheel
  - Surveyed existing systems to review how they can fit
  - Chose the Tahoe-LAFS open-source distributed storage project as a working base for **privacy enhancements**

Tahoe-LAFS: file storing



Tahoe-LAFS: file retrieval



Why Tahoe-LAFS

- Fully distributed: **scalable**
  - Storage
  - Capabilities
- Full file encryption: **no trust** on the hosts
  - can be used in a cloud-like environment
- Erasure coding: very **resilient**
- **Open-source**

Need to add …

- Capability management feature
  - Storage and retrieval of capabilities
  - Sharing of capabilities
  - Same view from multiple devices

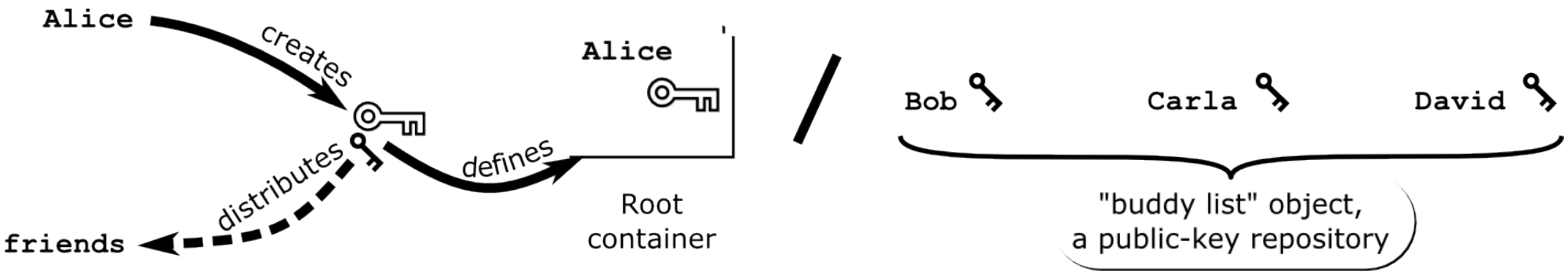
Tahoe's built in capability management is very basic

```
jean@shi-chi:~/sources/tahoe/current$ bin/tahoe create-alias root_node
Alias 'root_node' created
No such file or directory
jean@shi-chi:~/sources/tahoe/current$ bin/tahoe ls root_node:
jean@shi-chi:~/sources/tahoe/current$ bin/tahoe mkdir root_node:container
URI:DIR2:leyqyy2uszdv3ekgvo2rqsxsde:igsrcf2gpuc672xfbk3wxgeirinwseyt5bdv2tpcqu6ypzdnayxa
jean@shi-chi:~/sources/tahoe/current$ bin/tahoe cp /tmp/README.txt root_node:container/
Success: files copied
jean@shi-chi:~/sources/tahoe/current$
```

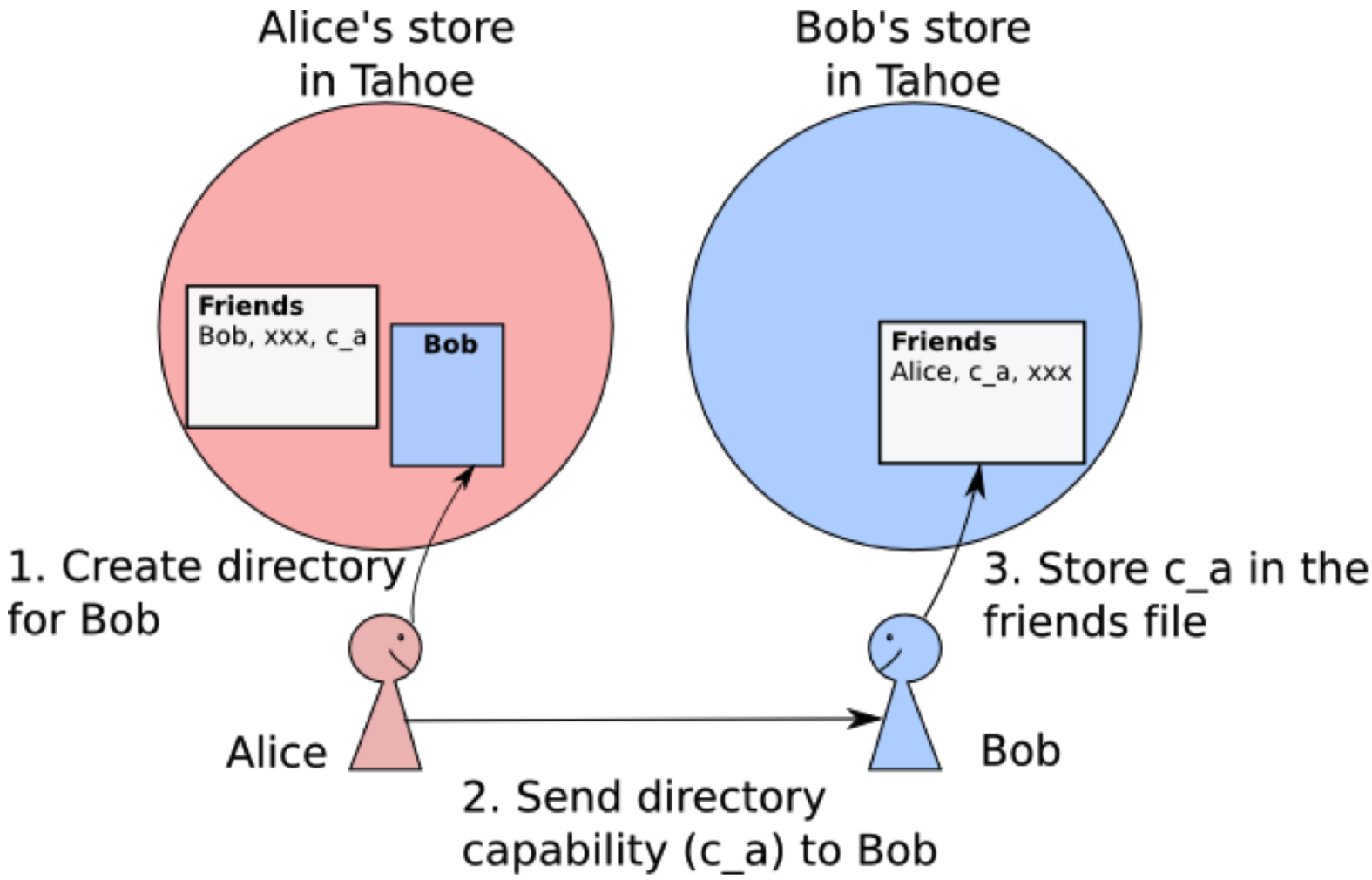
Tamias

Capability management

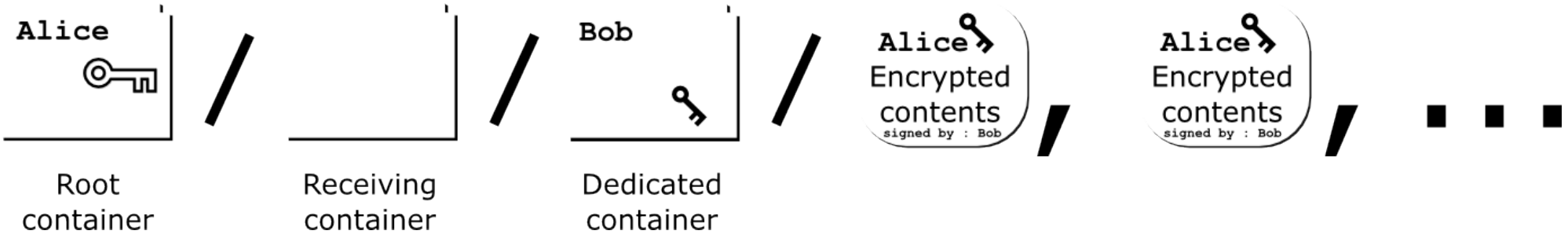
- Private key used to generate the root
- Capability to root is the entrance point into all the other capabilities
- Stored in Tahoe-LAFS itself
- Inspired from buddy list: friend -> public key, ...



Content sharing:
Alice wants to receive files from Bob

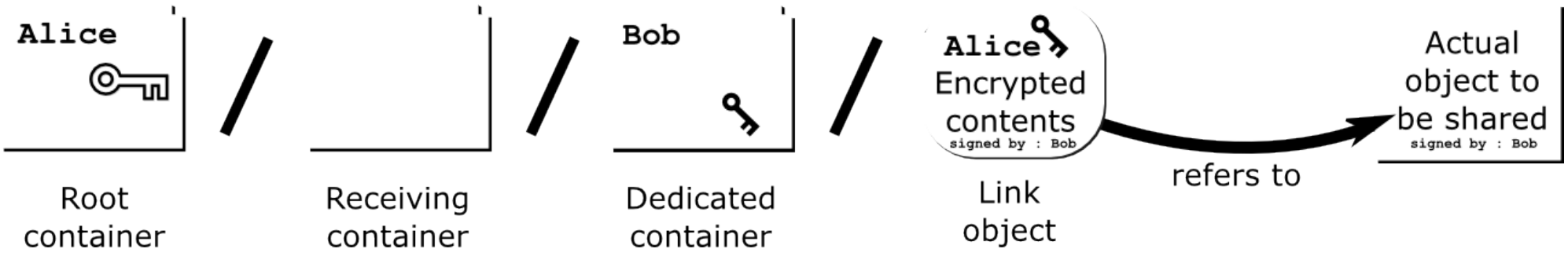


Content sharing:
Alice wants to receive files from Bob

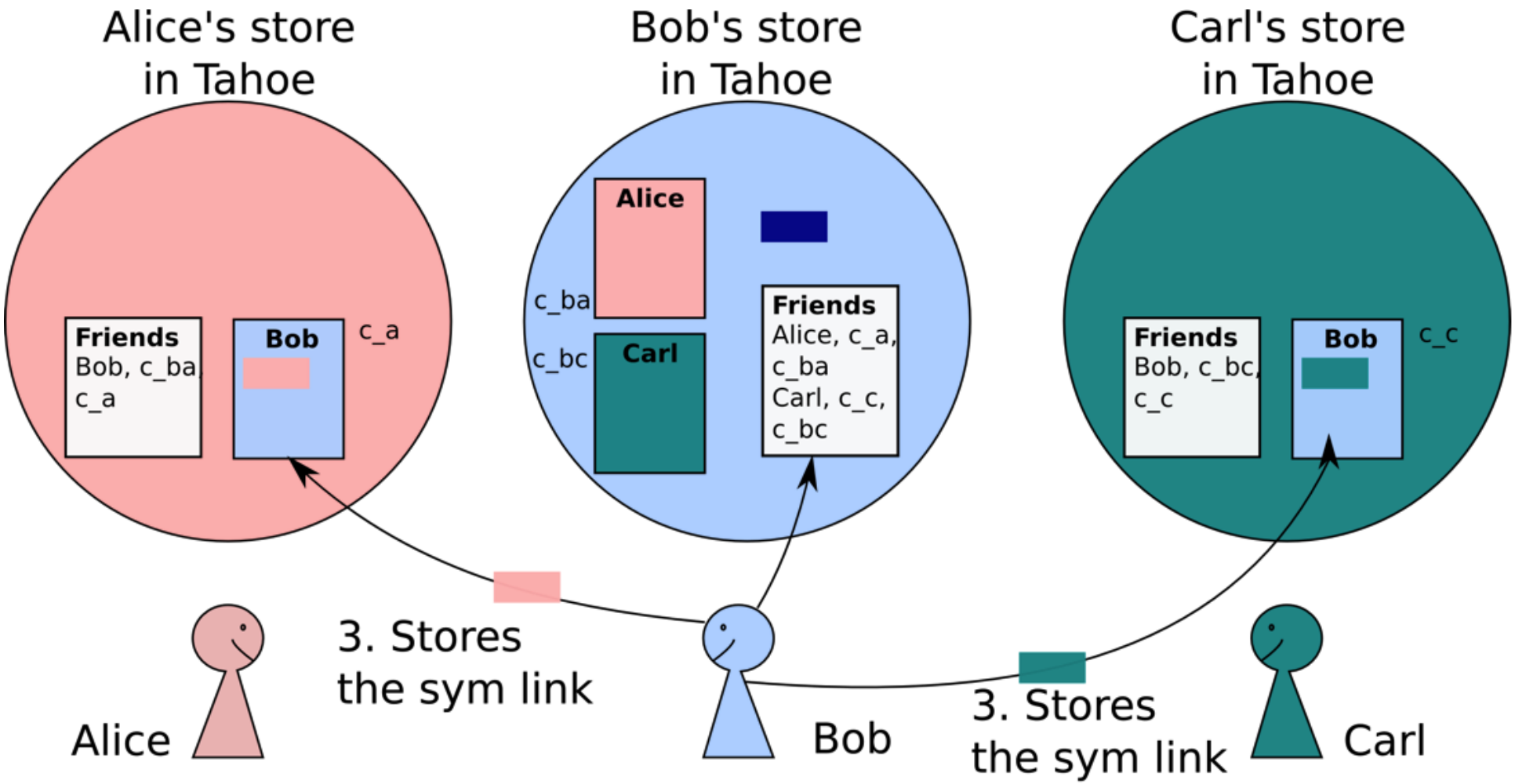


Group sharing

- Objective: be able to revoke access to files on a per user basis
- Generate a symbolic link per destination
- Revoking done by removing the sym link



Group sharing



1. Store the file in own space
2. Generate sym link per destination user

Tamias

Capability management system over Tahoe-LAFS

User perspective	Technical's perspective
Easy to use	Scalable
Multiple devices	Reliable
Fine privacy granularity	Suitable for cloud services
Reliable	

2010-2011 activities

- Survey
  - Distributed storage solutions
  - Online social network solutions
  - Meta-data
- Design of Tamias
- Prototype implementation

Still need to add …

- Delegation and revocation
- Removal of users by the storage provider
- Multiple storage domains

Questions?

http://tamias.iijlab.net/

A few screenshots

Jean’s starting page

My info (shichi)

- Friends
- Groups
- Shares

- Cristel (iij)

Welcome to iijlab distributed storage experiment based on Tahoe-LAFS with some Authority additions (tag 22)
Choose a topic in the left menu.
here is your private root capability :
URI:DIR2:g5awm53hdwtmoa7qbjobdg23ya:vwcxitubtcfqyd4rpsshqajkfpujorqsjpunknxprt3nh3rdfc6q

Here is your public-key for others to recognize you :
gcbacibqbudaskugjcdpodibaeaqkaadqiaq2abqqiaqqaucaeaqbolp6wkd24vqwhcxpsbxpct2u6xe
gdzgdsegqrz6ixz2olqvsvosjq4b6al3tiy2pvhxrt6l2fp65fl3uyyykan7bwyflvqkzpo2kikii26j
s3we5m4mkets3it4hlov6xmwnn7rcll4oipgyht6okgxgccoymamlm7imp6d3f3av42auppl3u2fm3ok
5q5jogut6utm2qqhn3xm3qwx5lek3xn4qvgrz7pjith5vyzwkmsbs7x3dvkm3qm6yxx22dxvtlmmvpnz
ip45utd2uxdqzlb53kghnuxbf4len57gx2b5nfq6sni5mvyfhgnisfccin6gbebngxvkq76wor3euu2x
ndtn3xfnttasnic7dlkxqqwokkbri3m4byzyu3cjia7xx6xvubryeeweqz5ddmycaeiq

Download your public key

Export your private key (use with CAUTION)

Jean’s friends

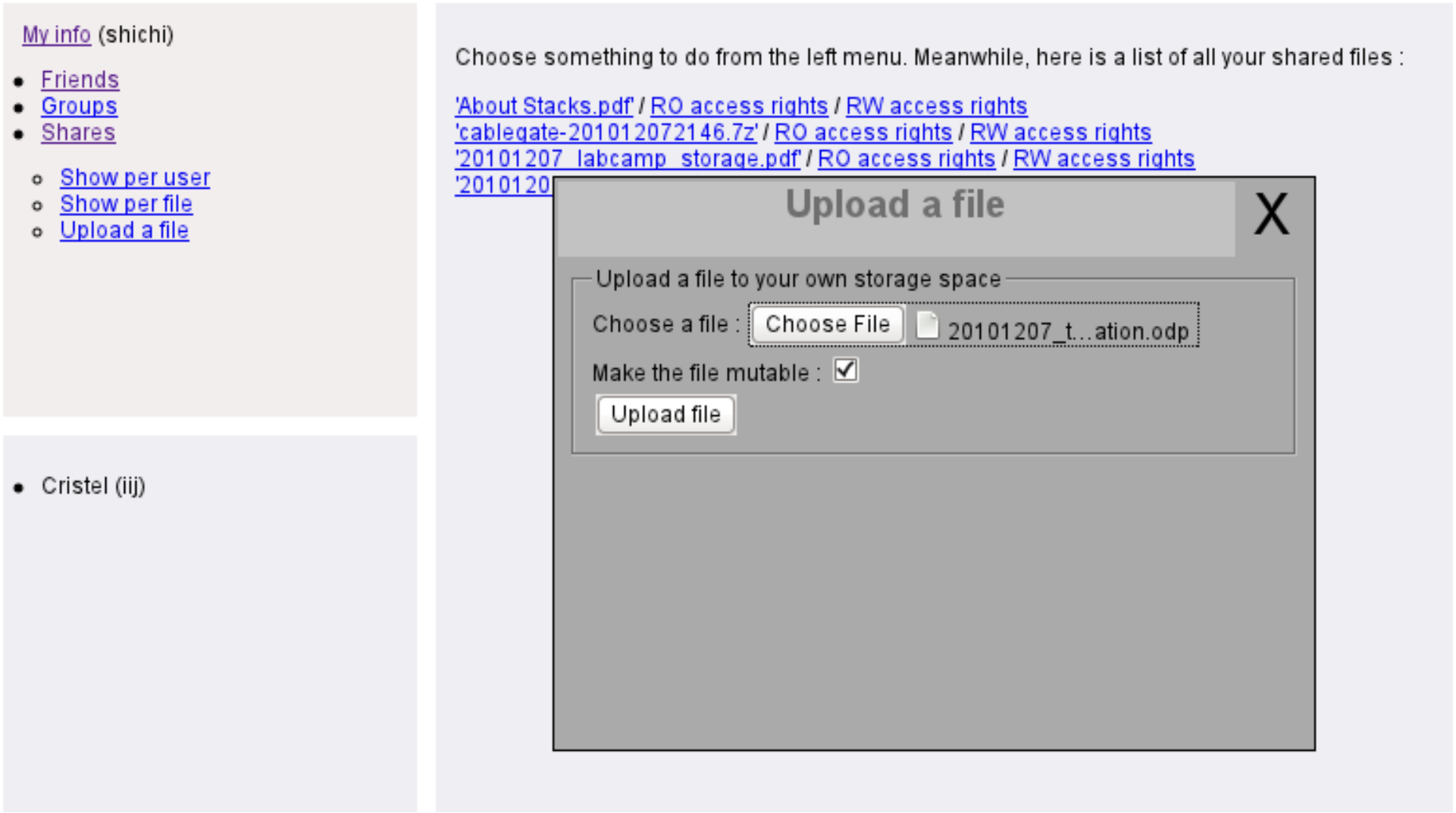
My info (shichi)

- Friends
  - Summary
  - Register a new identity
- Groups
- Shares

- Cristel (iij)

Name : Cristel (iij) (remove from list)
Public key : gcbacibqbudaskugjcdpodibaeaqkaadqiaq2abqqiaqqaucaeaqbmthewngmg4zgja4ptb6ns2jyys
6zxwaxbfrqcjrh6ento3vugdlc6v6szvow7thqzf3kxjgdmu6hqgml6adhk5444tafts44c4nsq2bnuu
zw7aqifg4ves2m7embfbtdbnkjjva6ye5dmkbvxhf6s23zvwstcxrpxjo75x23apesilg4nrs2koybsc
qv35cvumufcjxz4taomr4obk3hk7srx6lc2tyrp2uc2fw6t47x6blkyjniyr5r6n5jerukg5b7ojr7bjmjlbgzzprhvxzqxi3r4zjlwbejrrxygpj5jup72a
4uha36og65p3r5wndnpe3plvzngtitkdretj7baxrgkigeccxho5rx3qz5mj6bqwfrkykwnrp46v7yauzjrpyu56unwzkxazjzjpzkicaeiq
Sharing capability (for us to write to Cristel (iij)) :
URI:DIR2:zoke3xxbmgeysdjuxyp36ihowi:253hzsxhjzce43wcbauov4cx652onskzyrai5plg3flqfntxosvq
Sharing capability (for us to read from Cristel (iij)) :
URI:DIR2:2is3vlitjnjyxjdb34pqnslbpu:n2l7iq3mectptxafo5oq5h4ez2otbs7spom4h7jk2bfiqkru5oba

Jean uploads a file



Jean shares the file with Cristel