



A cMix implementation

By Tsioris Ioannis

cMix Protocol

A mixnet protocol

Its goal is to provide anonymity to its users.

Messages are sent to the network in a particular order and, after some process, their order is changed and their recipients are revealed. Thus, it is very difficult to determine who-sent-what.

Designed to be practical

The cMix protocol is designed to be useful even for real-time applications, such as chat platforms.

Main idea: precompute expensive public key operations in a precomputation phase. These computations are cached in order to be used in the lightweight real-time phase.

Complete protocol definition:

<https://eprint.iacr.org/2016/008.pdf>

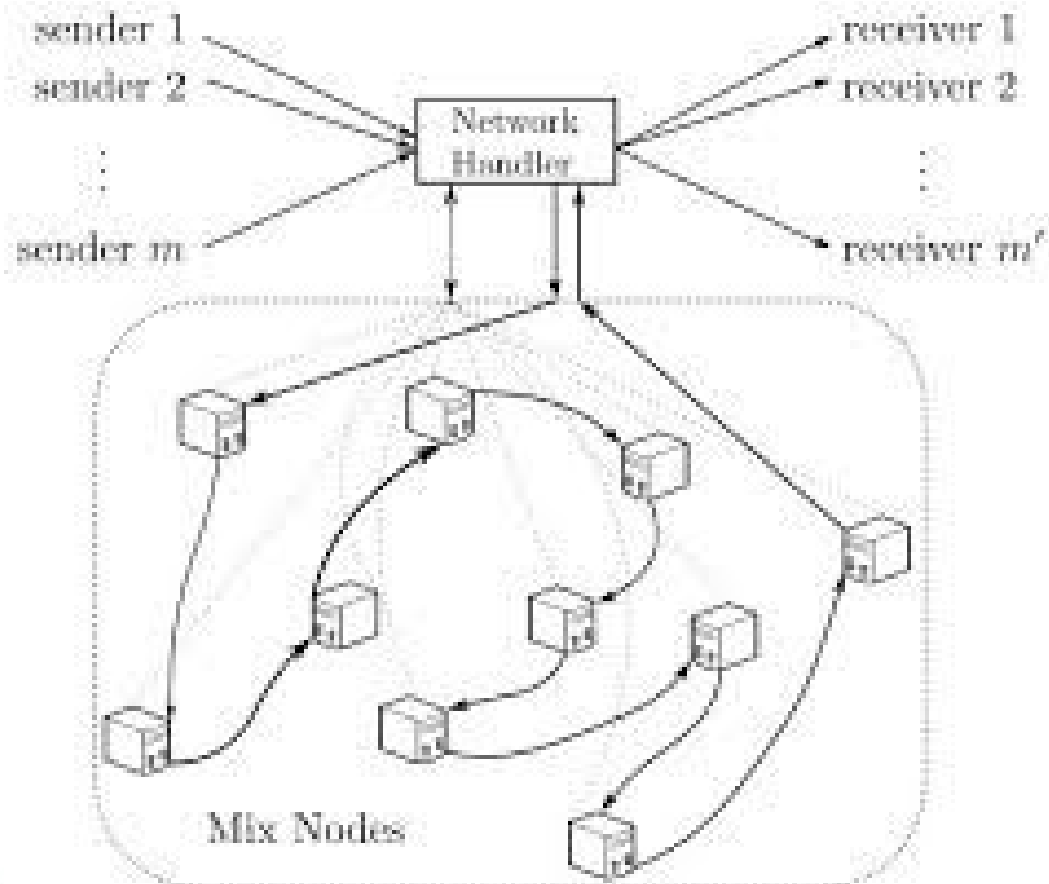
A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, suggesting different levels of connectivity or importance. The lines are thin and gray, creating a mesh-like structure.

1.

Overview of the protocol


A decorative network diagram in the bottom-right corner, similar to the one in the top-left, showing a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, suggesting different levels of connectivity or importance. The lines are thin and gray, creating a mesh-like structure.

Overview of the protocol





Overview of the protocol

- ◎ The protocol consists of 3 distinct entities: the network handler, the mix nodes and the users of the system.
 - ◎ The users send messages to and receive responses from the network handler.
 - ◎ The network handler coordinates the mix nodes and the users.
 - ◎ The mix nodes carry out the mixnet operations.
- 

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles inside, suggesting different levels or types of nodes. The lines are thin and gray, connecting the nodes in a non-linear fashion.

2.

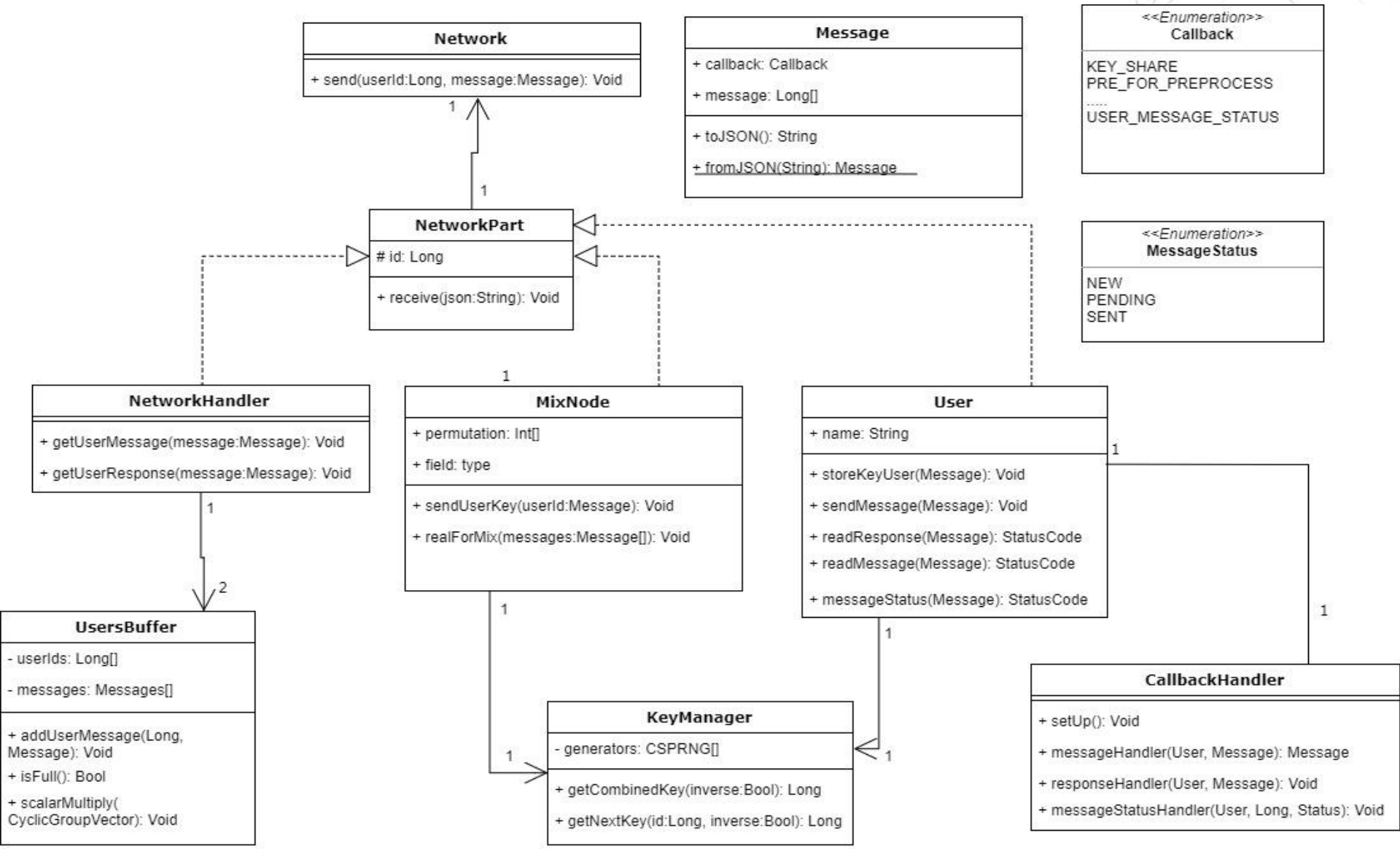
Overview of the implementation

A decorative network diagram in the bottom-right corner, similar to the one in the top-left. It shows a cluster of nodes connected by lines, with some nodes being larger and having concentric circles, indicating a hierarchical or layered structure.

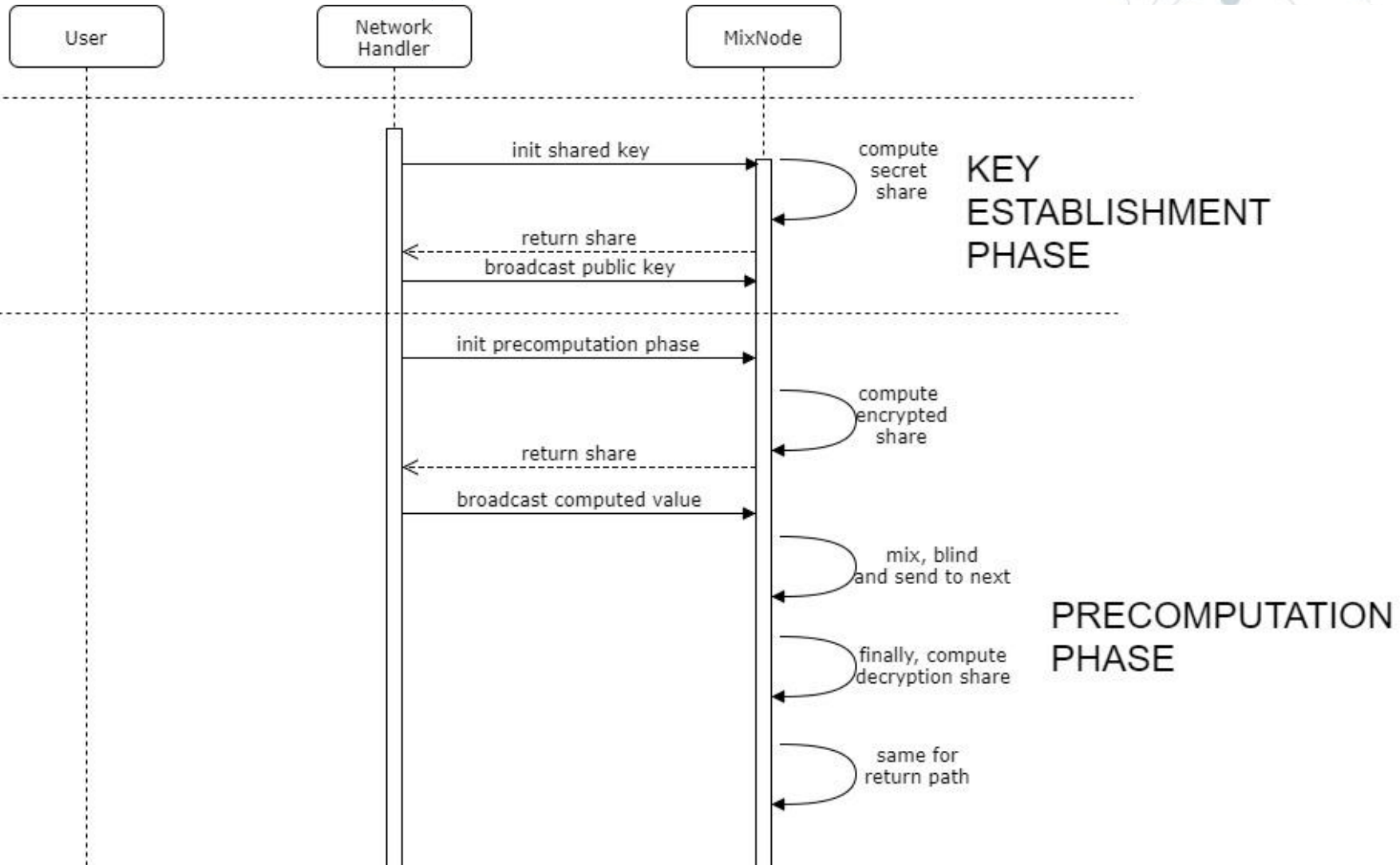
Overview of the implementation

- ◎ The project is implemented in Python 2.7
- ◎ Crypto operations are supported by the [pyCrypto](#) library.
- ◎ A mock network is introduced to exchange messages.

Overview of the implementation Class Diagram

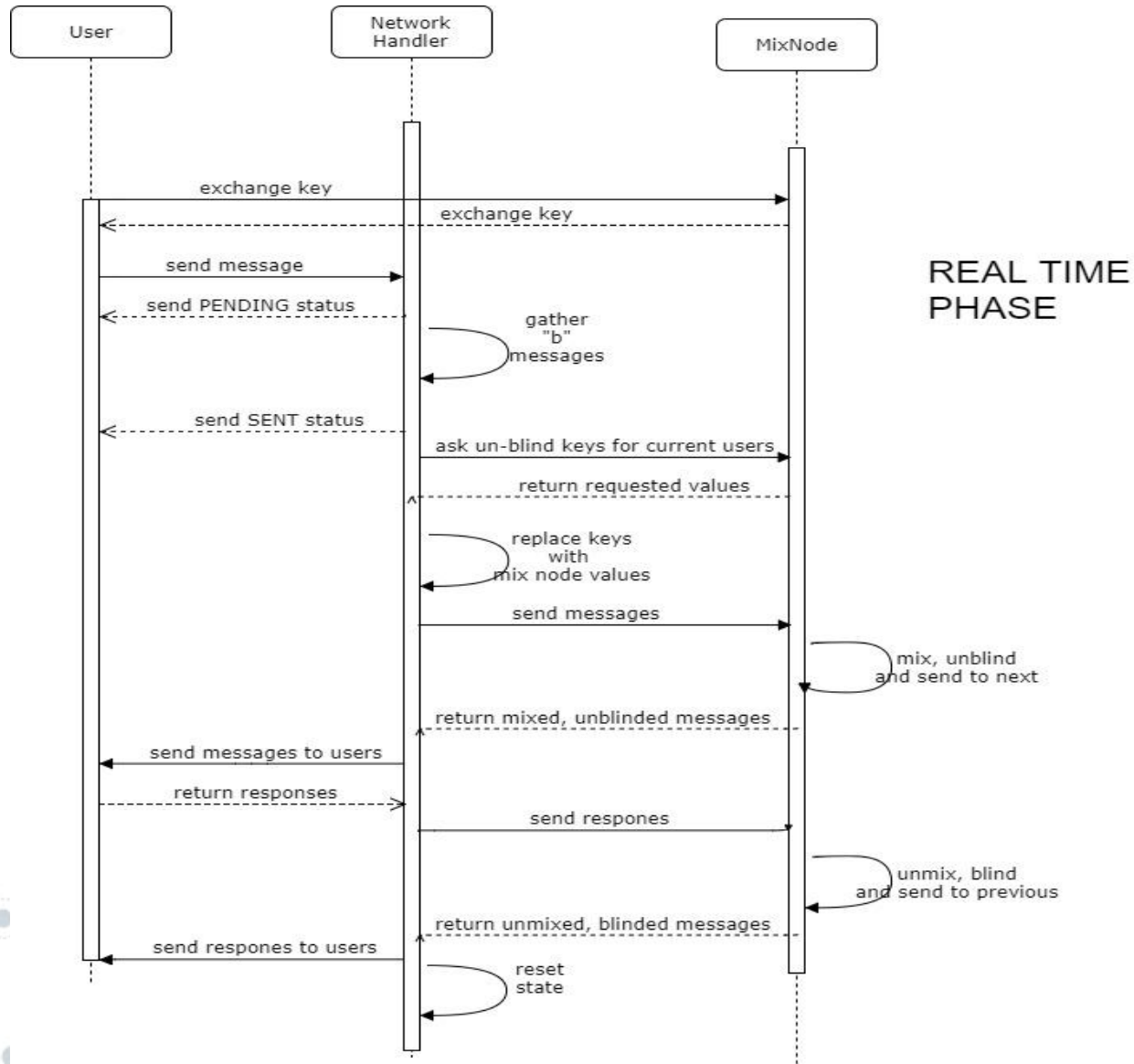


Overview of the implementation Sequence Diagram (1)



Overview of the implementation

Sequence Diagram (2)



A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by circles of varying sizes, some with concentric rings, and the lines are thin and grey. The diagram is partially cut off by the left edge of the slide.

3.

A demo application

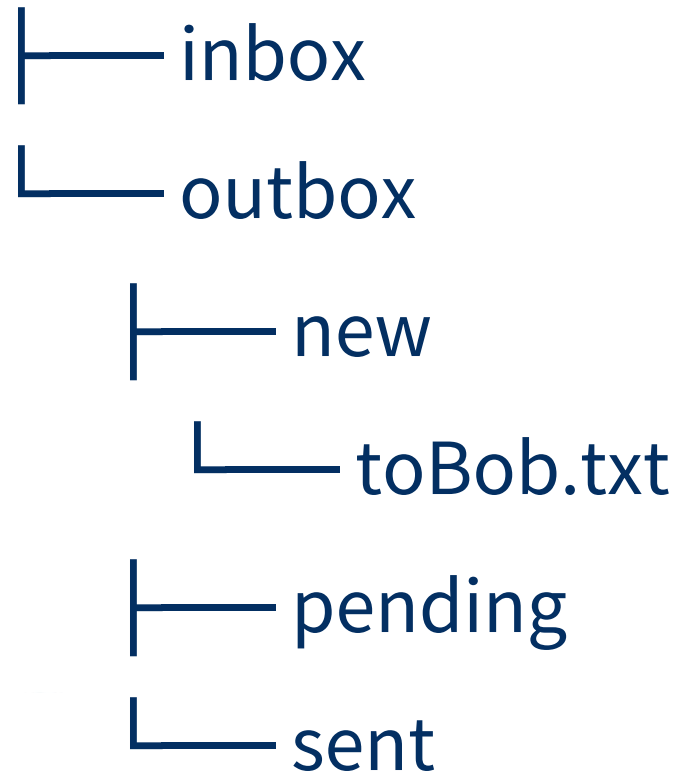
A decorative network diagram in the bottom-right corner, similar to the one in the top-left, showing a complex web of interconnected nodes and lines. The nodes are circles of varying sizes, some with concentric rings, and the lines are thin and grey. The diagram is partially cut off by the bottom and right edges of the slide.

A demo application

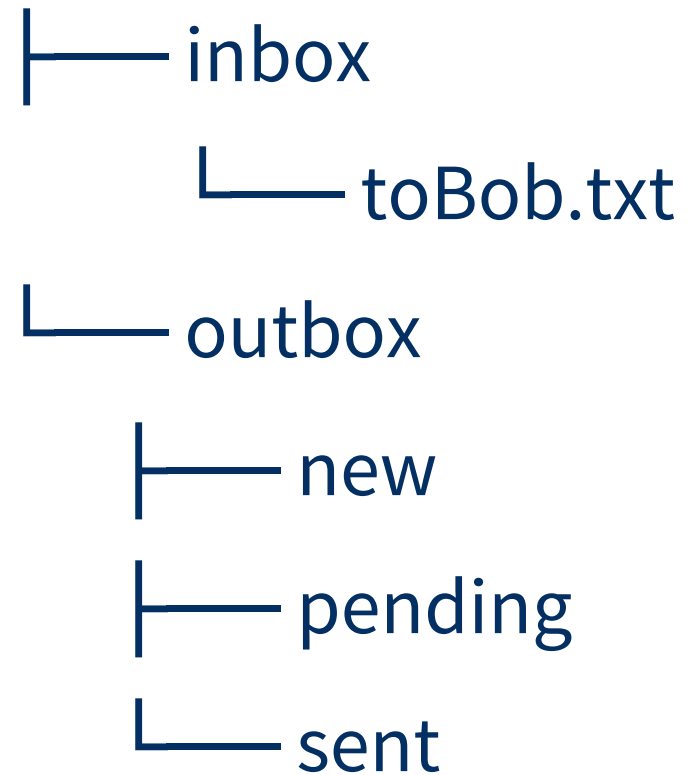
- ◎ Suppose that multiple users have access to the same PC (and file system).
- ◎ Each user has unique access to a directory that stores his/her incoming and outgoing messages.
- ◎ The mixnet application also has proper access to these directories; thus, it can deliver messages anonymously.

A demo application

Alice



Bob





Thanks!

Any questions?

You can find me at:

jtsioris@gmail.com

Project source code:

<https://github.com/johntsr/cmiX>



Credits

Special thanks to all the people who made and released these awesome resources for free:

- ◎ Presentation template by SlidesCarnival
- ◎ Photographs by Unsplash & Death to the Stock Photo (license)