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.

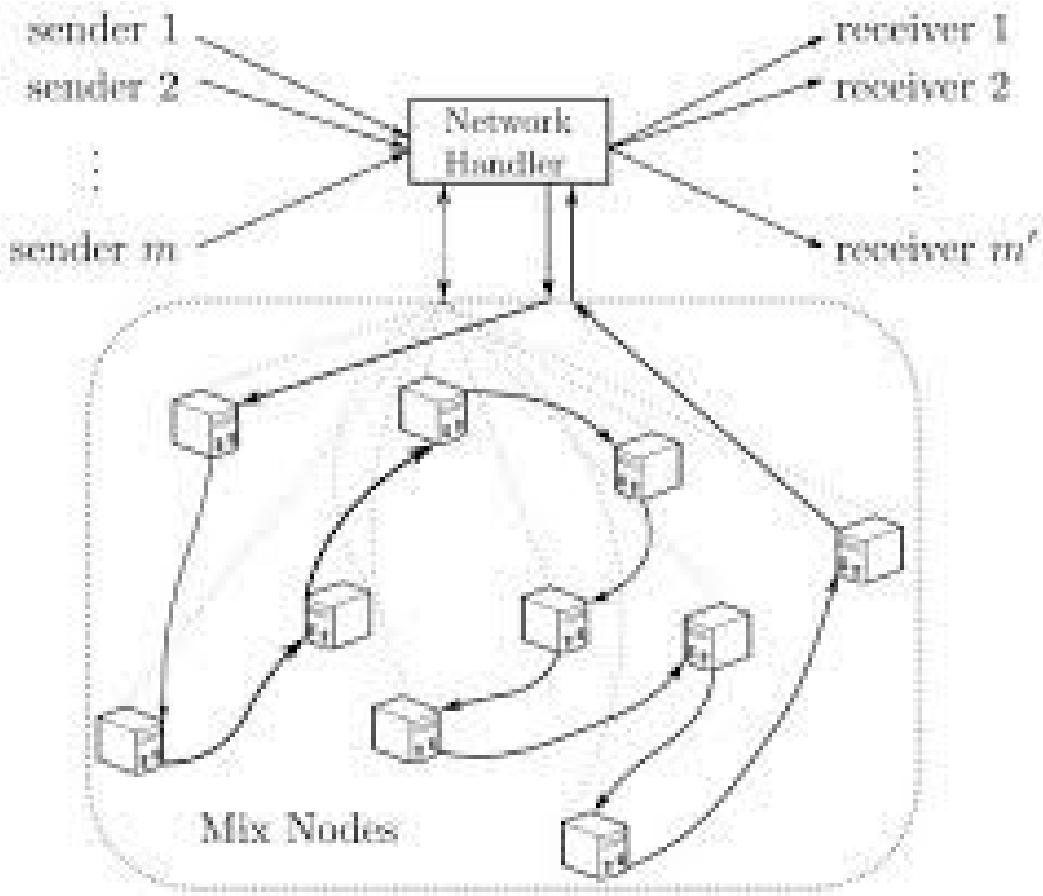
Main idea: precompute expensive public key operations in a precomputation phase. These computations are cached in order to be used in the lightweight real-time phase.

Complete protocol definition:

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

1. Overview of the protocol

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.

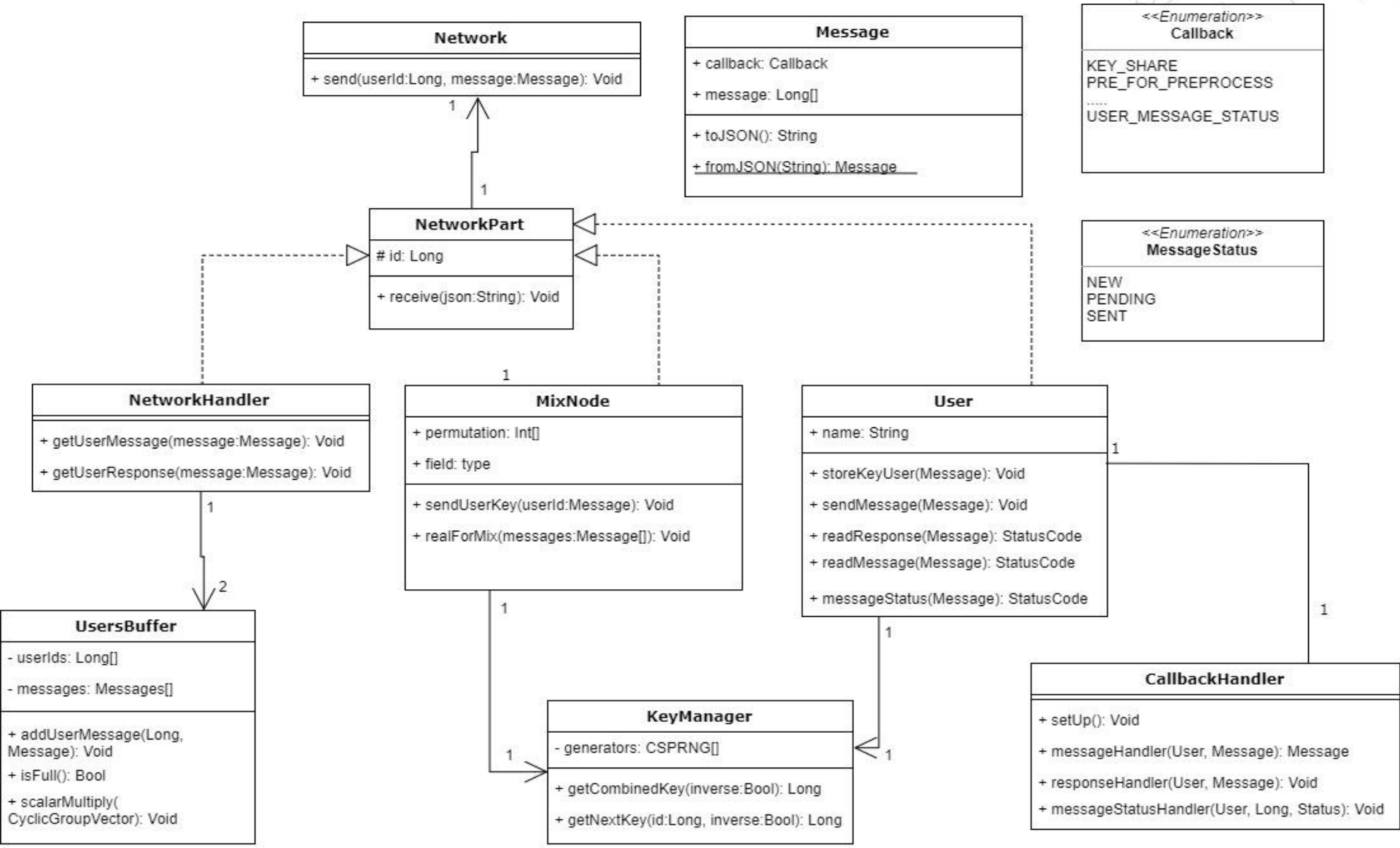
2.

Overview of the implementation

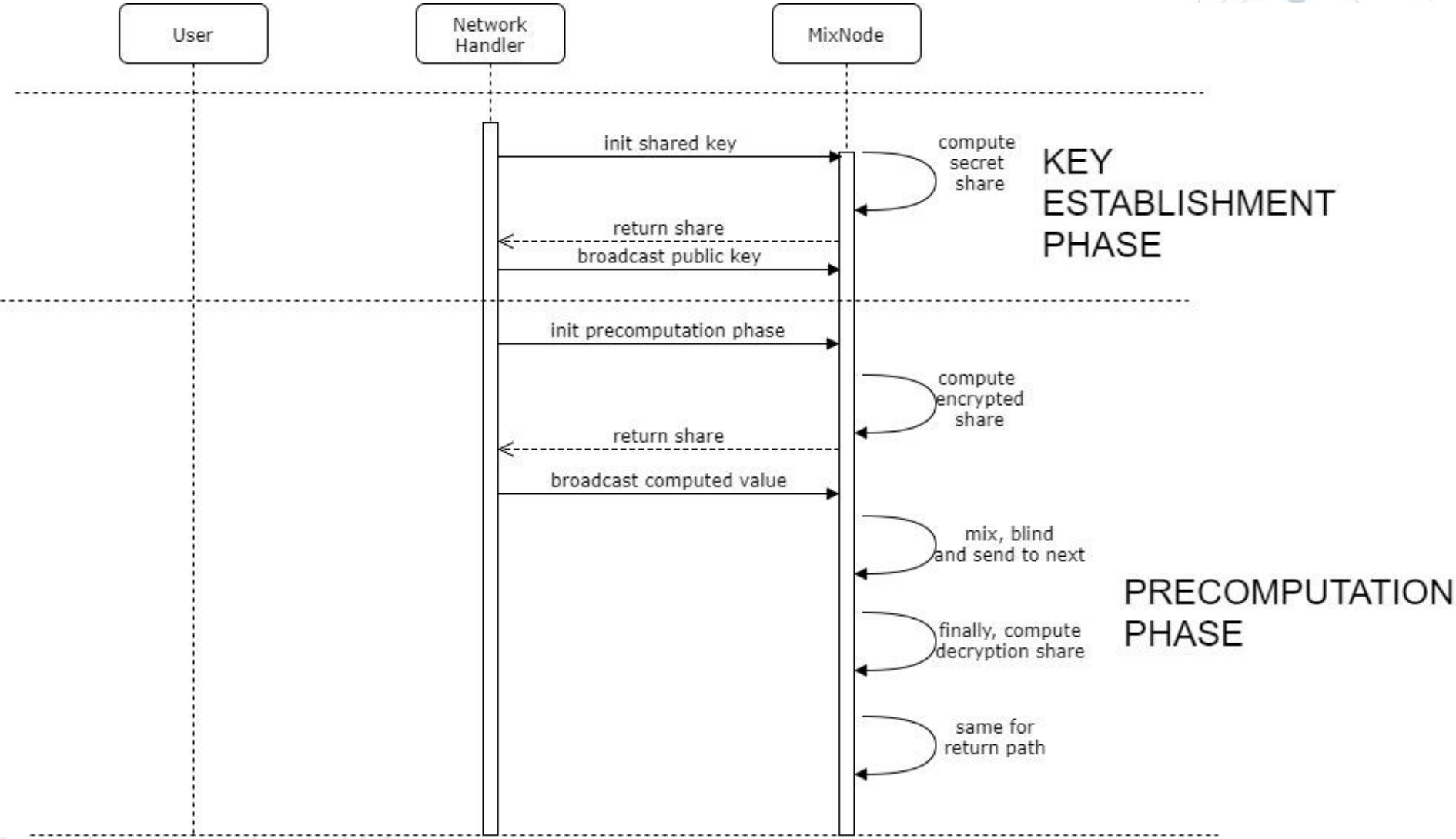
Overview of the implementation

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

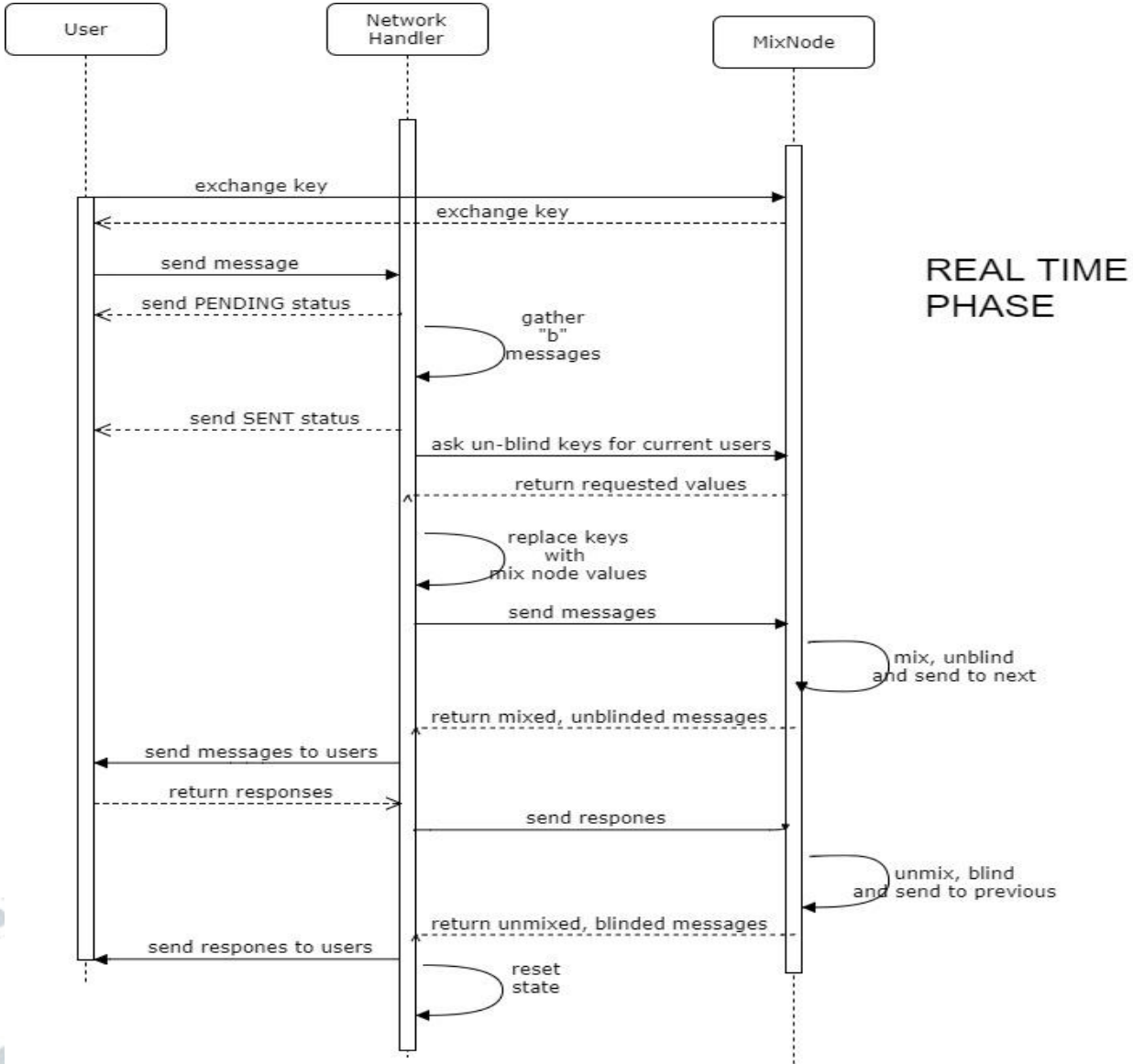
Overview of the implementation
Class Diagram



Overview of the implementation
Sequence Diagram (1)



Overview of the implementation
Sequence Diagram (2)



3.
A demo application

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 outcoming messages.
- The mixnet application also has proper access to these directories; thus, it can deliver messages anonymously.

A demo application

```
Alice
├── inbox
└── outbox
    ├── new
    │   └── toBob.txt
    ├── pending
    └── sent
```

```
Bob
├── inbox
│   └── toBob.txt
└── outbox
    ├── new
    ├── pending
    └── sent
```

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)