Building the next generation of privacy infrastructure to end mass surveillance

Overview

- Why privacy?
- What is privacy anyway?
- Mixnets for network privacy
- Decentralised credentials
- Nym in action
- Discussion

NYM

Our goals

Our goals

- **Ending mass surveillance**

Our goals

- **Ending mass surveillance**
  - How?

NYM

Our goals

- **Ending mass surveillance**
  - How?

NYM

Our goals

- **Ending mass surveillance**
  - Why?
  - How?

Two core technologies

1. **Mixnet:** A ‘better than Tor’ network security layer
2. **Signature scheme** that provides
    - Blind issuance
    - Re-randomizable signatures
    - Selective attribute disclosure
    - Threshold issuance of signatures

NYM

Privacy

The ability of an individual or a group to decide **which information they want to expose** about themselves

NYM

Anonymity

- A property that allows users to hide their relations to particular operations and maintain an indistinguishable identity among other users (**anonymity set**) performing similar actions
- In context of anonymous communication, the main goal is to **hide who is communicating with whom**

NYM

Network-layer privacy: Metadata

- **Everything about the communication but the content**
  - Who is communicating with whom?
  - How often and at what time?
  - From which location?
  - What are the volumes or frequency of traffic?
  - What is the sequence of communication?
  - What is the dynamic of the group?

NYM

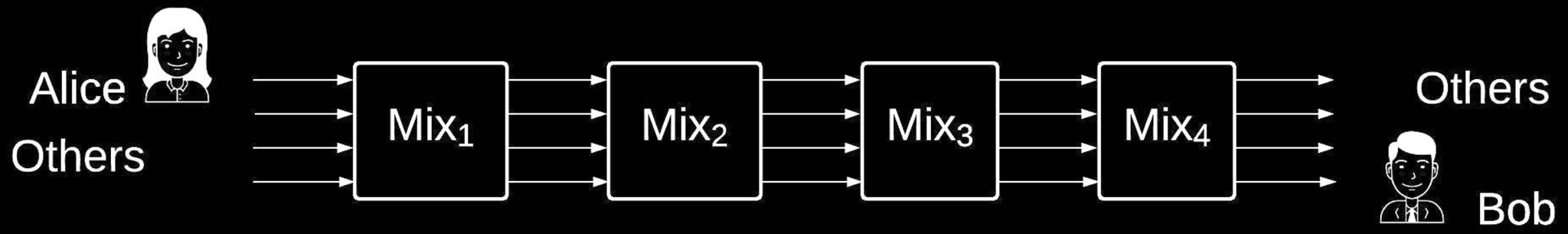
Network-layer privacy

- What about end-to-end encryption
  - e.g. WhatsApp, Telegram, Signal
- What about Zcash?
- What about VPNs?

NYM

Mixnets: Background

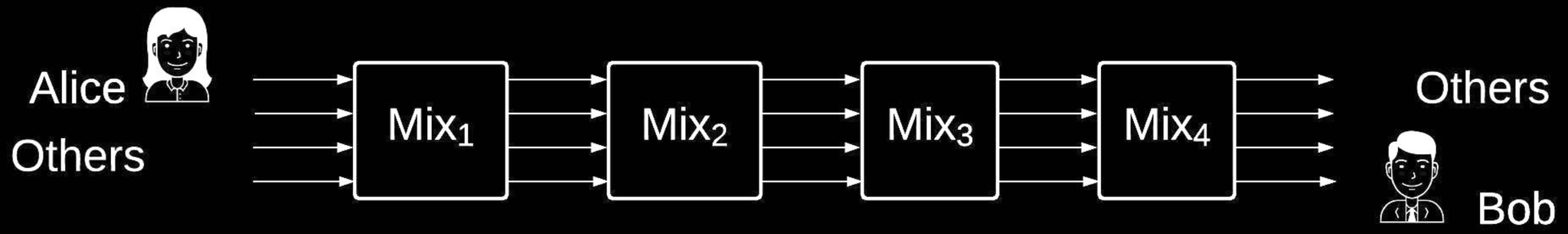
David Chaum proposed the first anonymous network in the early 1980s, the so-called **mix network**, a set of cryptographic relays hiding input and output correspondence



NYM

Mixnets: Background

- **How?**
  - Source routing
  - Layer encryption
  - Secret permutation



Nym Mixnet

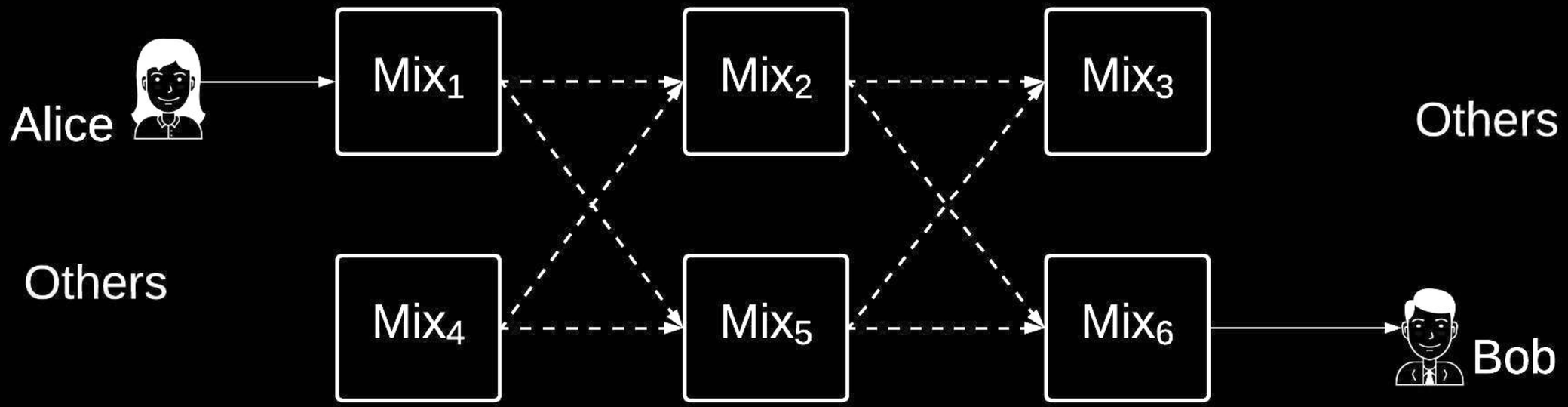
- Early mixnet designs had significant limitations in terms of **scalability**, **performance** and **latency overhead**
- Nym's mixnet is based on a modern mix-network design **Loopix***, which tackles the problem of traditional mixnets!

**The Loopix Anonymity System*, A.M. Piotrowska, J.Hayes, T.Elahi, S.Meiser, G.Danezis, USENIX 2017 https://arxiv.org/abs/1703.00536

NYM

Nym Mixnet: Network topology

Horizontal scalability: Adding more servers increases overall server capacity



Nym Mixnet: Cryptographic packet format

- **Sphinx** cryptographic packet format*
  - All packets padded to the same length
  - Bitwise unlinkability
  - Resistant to tagging attacks and replay attacks
  - All necessary routing information encapsulated in the packet

**Sphinx: A Compact and Provably Secure Mix Format*, George Danezis and Ian Goldberg, S&P 2009 https://ieeexplore.ieee.org/document/5207650

NYM

Nym Mixnet: Continuous time mixes

- Each packet is independently **delayed** according to a random delay selected by the sender
- Once the delay has time out, packet is forwarded
- No synchronized rounds required
- Delays drawn randomly from **exponential distribution**
- **Memoryless property**: larger anonymity set

NYM

Nym Mixnet: Tunable cover traffic

- Both mixes and clients generate cover traffic in the form of loop packets
- Loop cover packets indistinguishable from other messages
- Mixes generate loop packets at random intervals that follow an independent Poisson process
- Clients follow Poisson process to schedule user's messages; if no message is queued for sending a loop cover packet is sent

NYM

Nym Mixnet: How it comes together

- In order to send a packet via Nym's mixnet
  - **Sender client builds an independent mix route:** a single mix is randomly picked from each layer
  - For **each mix in the route**, a random delay d_i is selected from an exponential distribution
  - Layer encodes the content and routing information (mix route and delays) into Sphinx packet format

NYM

Nym Mixnet

- Scalable network
- Tunable cover traffic
- Resistance to active attacks
- Anonymity vs performance trade-off

Privacy-preserving credentials

All signature schemes have three algorithms:

- **keygen**
- **verify**
- **sign**

NYM

Privacy-preserving credentials

All signature schemes have three algorithms:

- **keygen**
- **verify**
- **sign**

NYM

Privacy-preserving credentials

Nym signatures:

- keygen
- verify
- sign
- **blind issuance**

Privacy-preserving credentials

Nym signatures:

- keygen
- verify
- sign
- **blind issuance**

Privacy-preserving credentials

Nym signatures:

- keygen
- verify
- sign
- blind issuance
- **re-randomizable signatures**

NYM

Privacy-preserving credentials

Nym signatures:

- keygen
- verify
- sign
- blind issuance
- **re-randomizable signatures**

NYM

Privacy-preserving credentials

Nym signatures:

- keygen
- verify
- sign
- blind issuance
- re-randomizable signatures
- **selective disclosure**

NYM

Selective disclosure

Passport attributes:

- name
- nationality
- age
- photo
- place of issue

Selective disclosure

Passport attributes:

- name
- nationality
- **age**
- **photo**
- place of issue

Privacy-preserving credentials

Nym signatures:

- keygen
- verify
- sign
- blind issuance
- re-randomizable signatures
- **selective disclosure**

NYM

Privacy-preserving credentials

Nym signatures:

- keygen
- verify
- sign
- blind issuance
- re-randomizable signatures
- **selective disclosure**

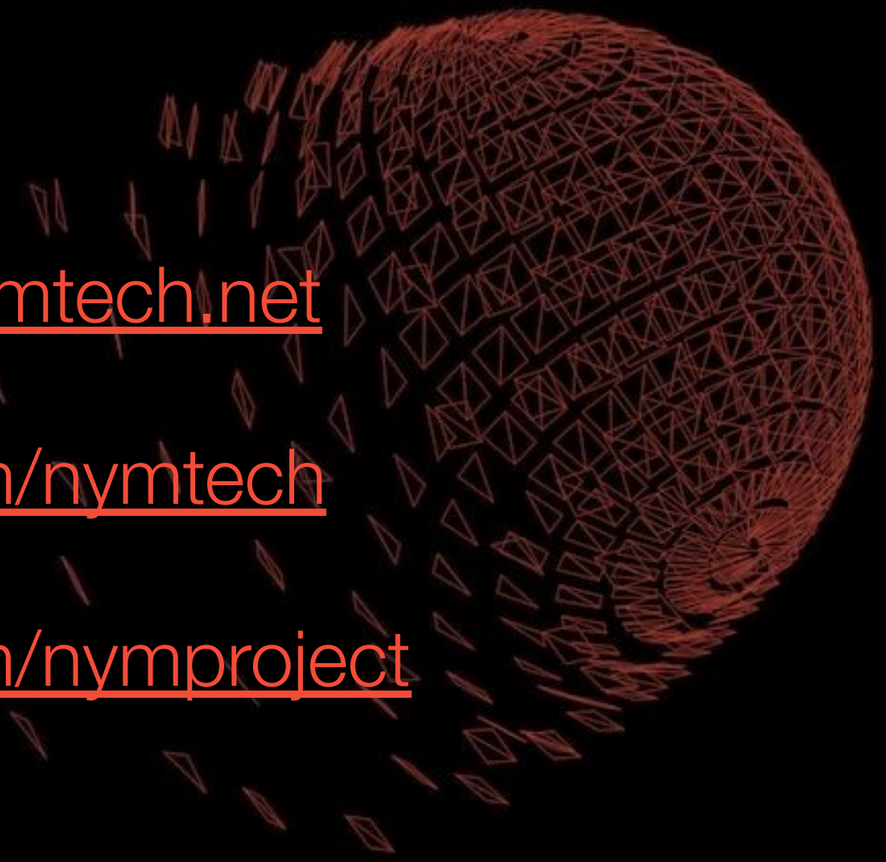
NYM

Privacy-preserving credentials

Nym signatures:

- keygen
- verify
- sign
- blind issuance
- re-randomizable signatures
- selective disclosure
- **threshold issuance**

Thank you



Web nymtech.net

Email contact@nymtech.net

Github github.com/nymtech

Twitter twitter.com/nymproject