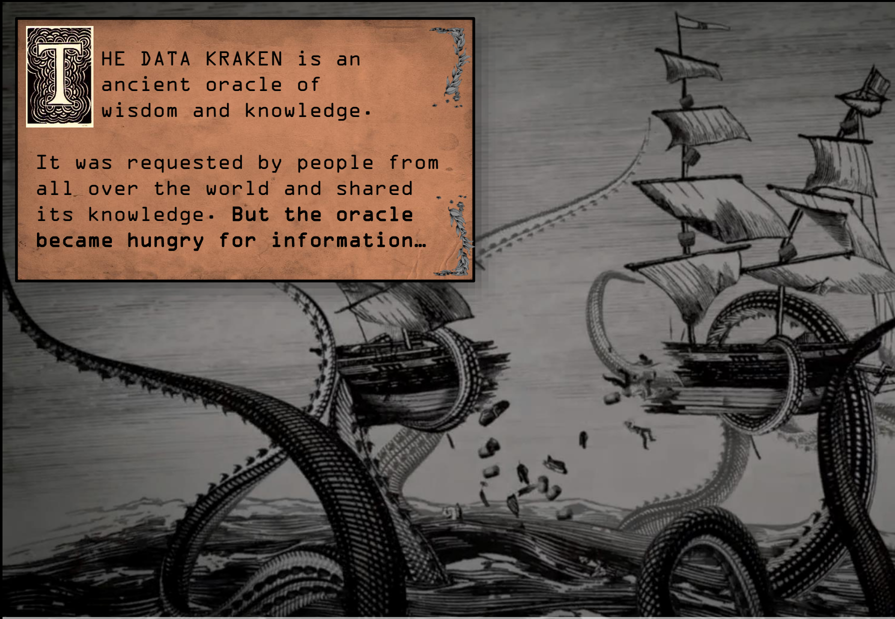
THE DATA KRAKEN is an ancient oracle of wisdom and knowledge.

It was requested by people from all over the world and shared its knowledge. **But the oracle became hungry for information…**



http://www.fubiz.net/wp-content/uploads/2012/03/the-kraken-existence2.jpg

The Katzenpost Mix Network System

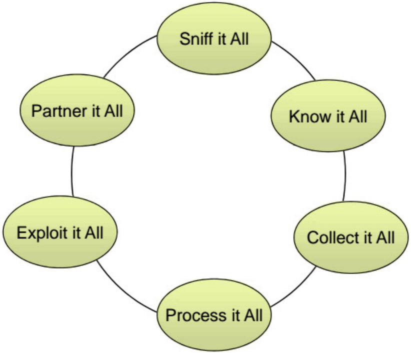
David Stainton

Panoramix

This project has received funding from the European Unions Horizon 2020 research and innovation programme under the Grant Agreement No 653497, Privacy and Accountability in Networks via Optimized Randomized Mix-nets (Panoramix).

"we kill people based on metadata"
–Michael Hayden (Ex-NSA and Ex-CIA Director)

Field Site Responsibilities



Sniff it All

Know it All

Collect it All

Process it All

Exploit it All

Partner it All

Meta-data leakage

Encryption is NOT sufficient!

Leaked meta-data:

- Geographical location
- Message sender
- Message receiver
- Message send time
- Message receive time
- Frequency of received messages
- Frequency of sent messages
- Size of the message
- Message sequence

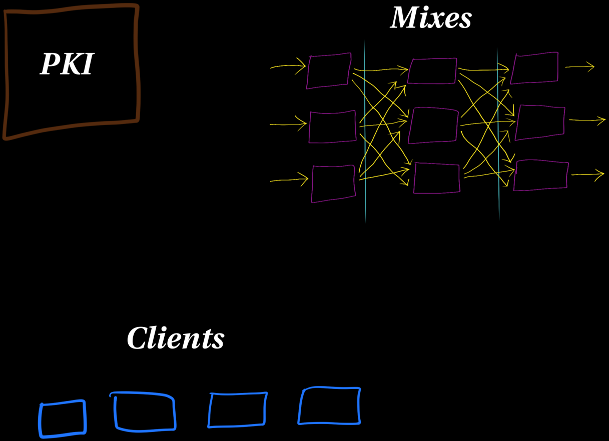
anonymity options

- decryption mix networks
- private information retrieval
- dining cryptographer networks
- broadcast based designs
- oblivious random access memory
- secure multi-party computation
- verified mix shuffles

David Chaum. *Untraceable electronic mail, return addresses, and digital pseudonyms*, Comm. ACM, 24, 2 (Feb. 1981); 84-90

Chaum came up with many big ideas in this paper such as:

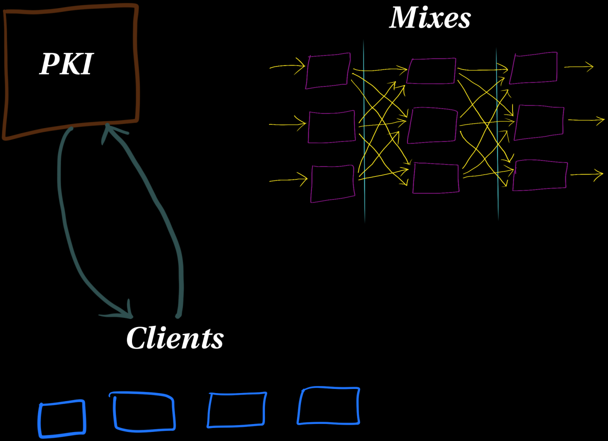
- Sender anonymity
- Anonymous replies
- Message receipts for reliability
- Pseudonyms for persistent communication



PKI

Mixes

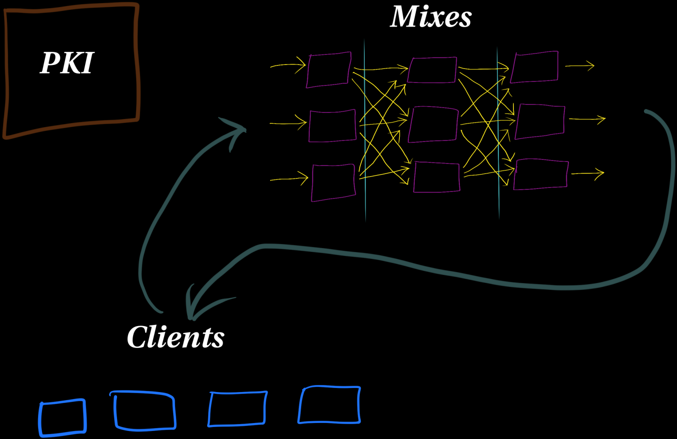
Clients



PKI

Mixes

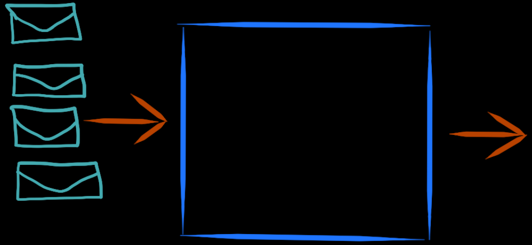
Clients

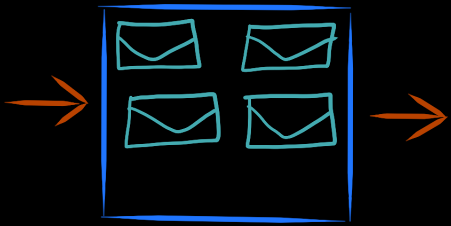


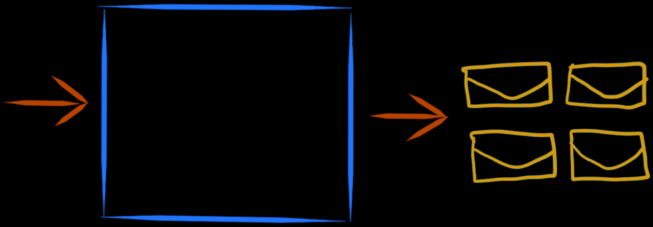
PKI

Mixes

Clients

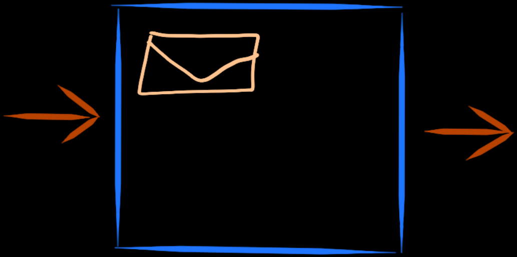


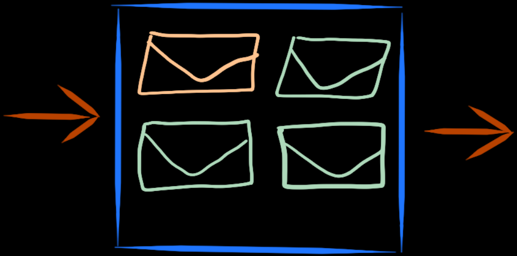


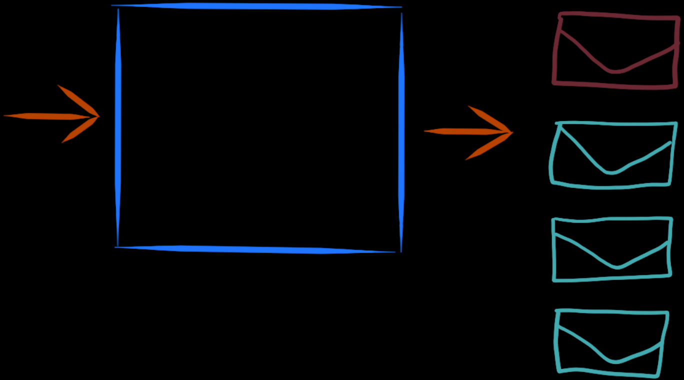


See:

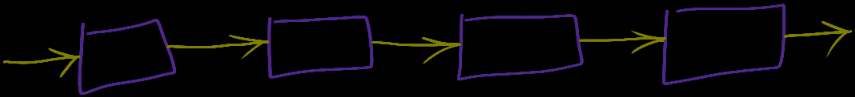
Claudia Diaz & Andrei Serjantov. *Generalising Mixes.* PETS 2003

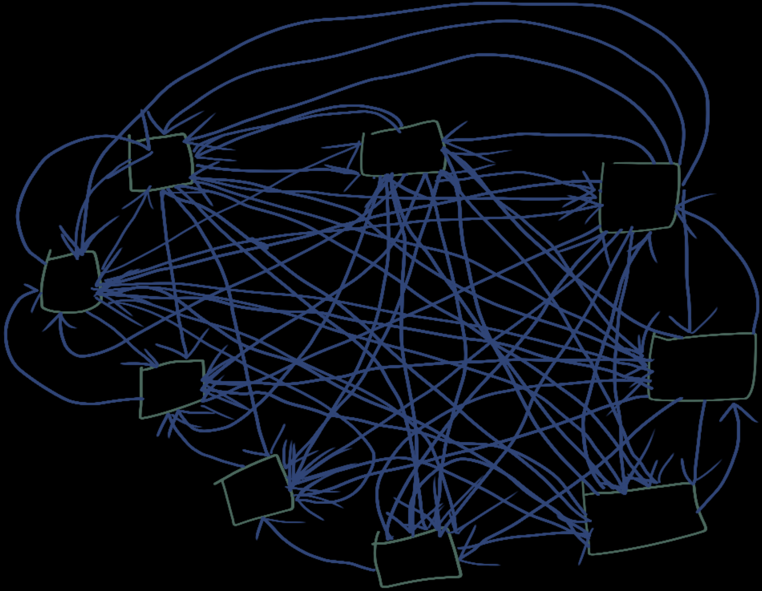


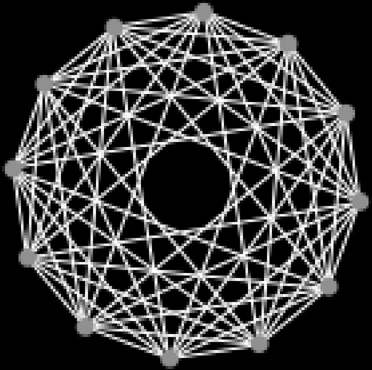


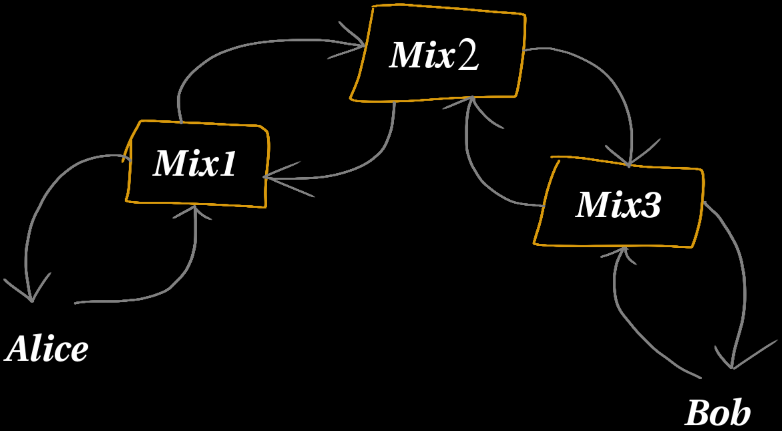


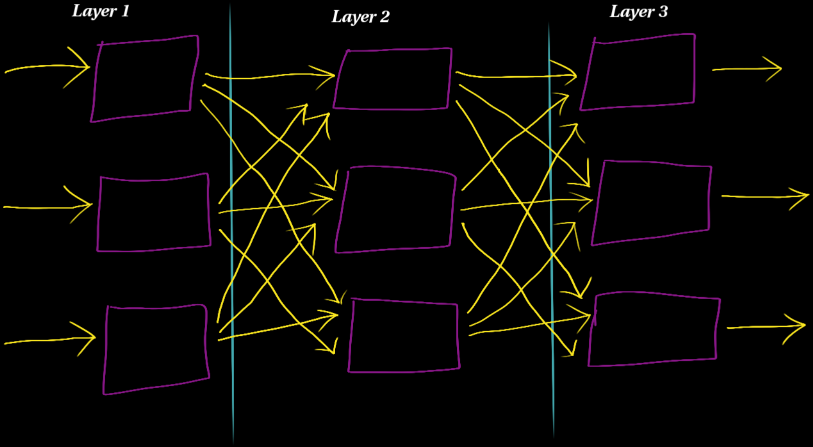
Cascade Topology







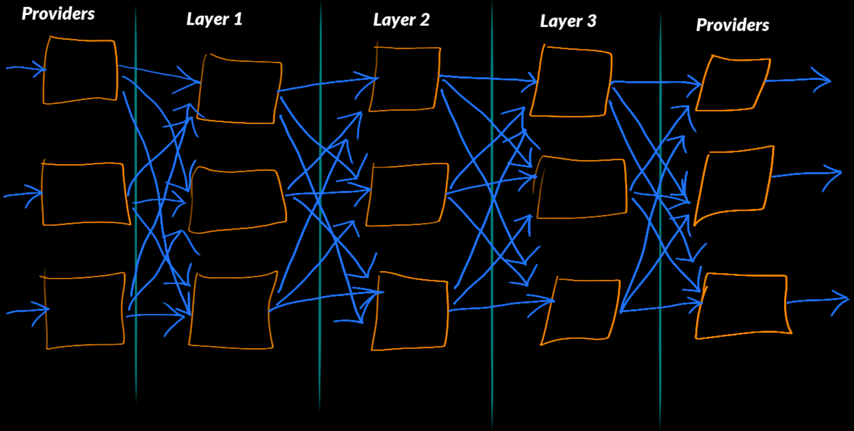

Mix2
Mix1
Mix3
Alice
Bob



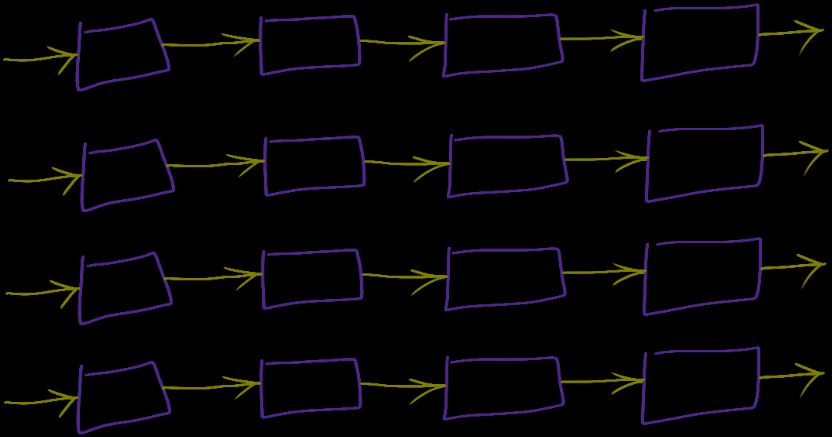
Layer 1

Layer 2

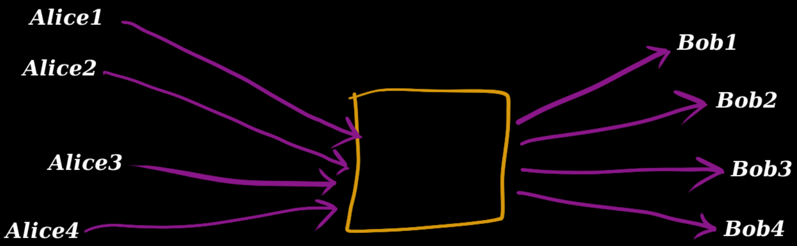
Layer 3

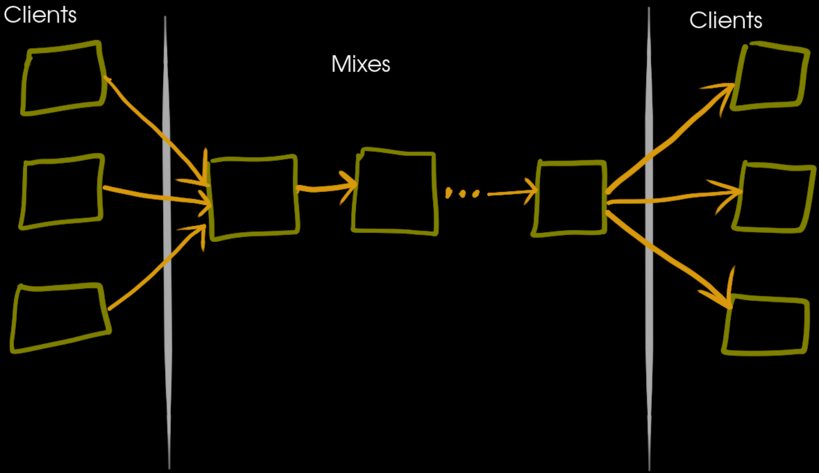

Providers
Layer 1
Layer 2
Layer 3
Providers

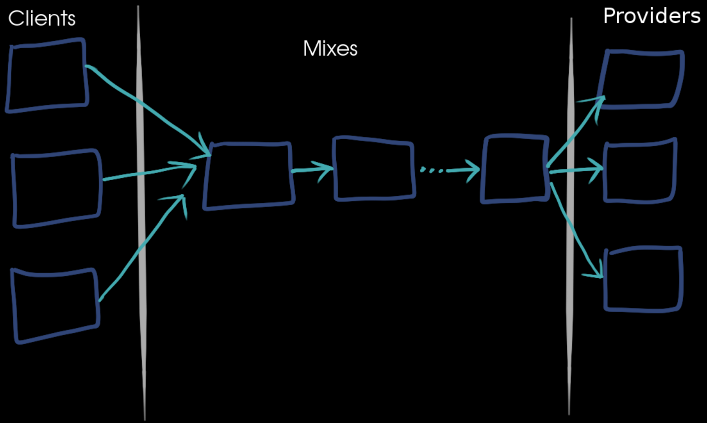
Multi Cascade Topology

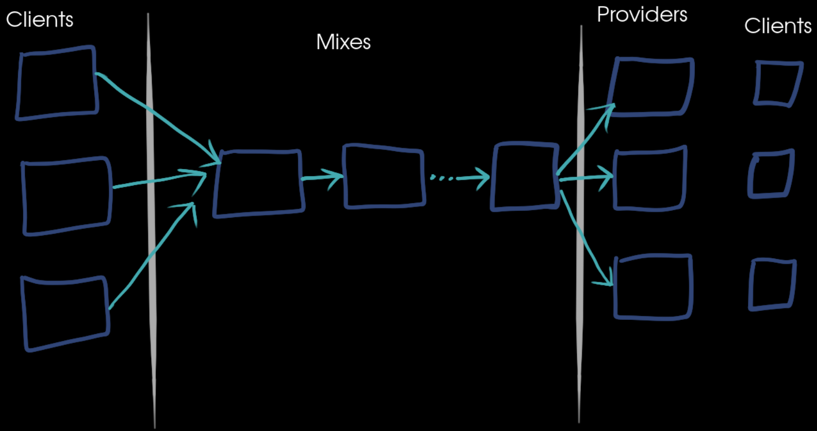


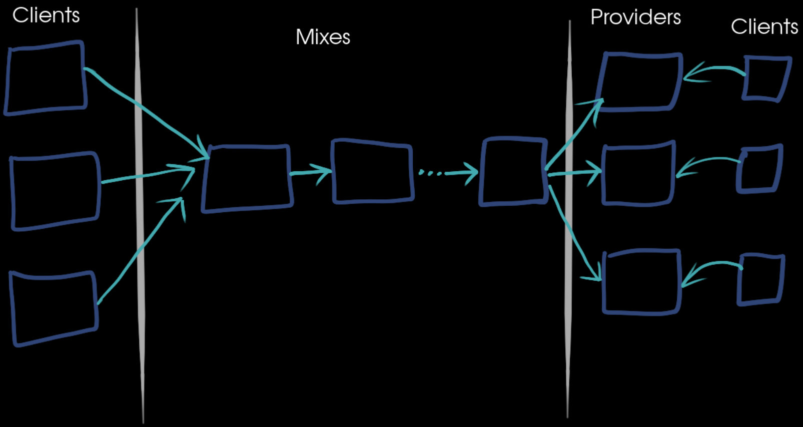
Diaz, Murdoch, Troncoso. *Impact of Network Topology on Anonymity and Overhead in Low-Latency Anonymity Networks*
PETs 2010

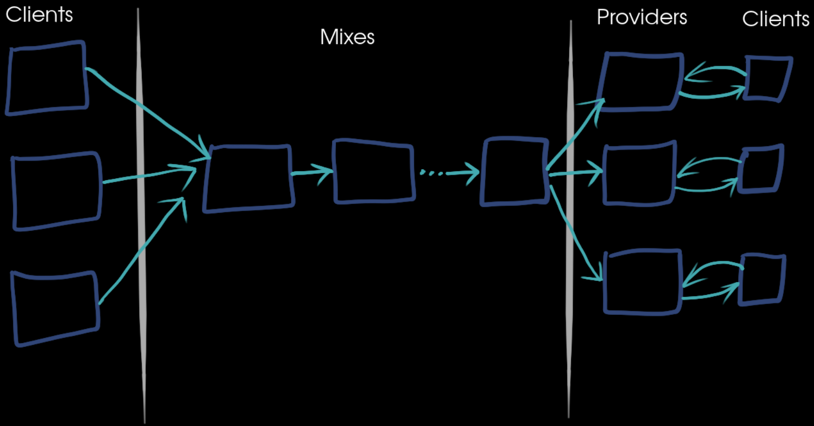

Alice1
Alice2
Alice3
Alice4
Bob1
Bob2
Bob3
Bob4

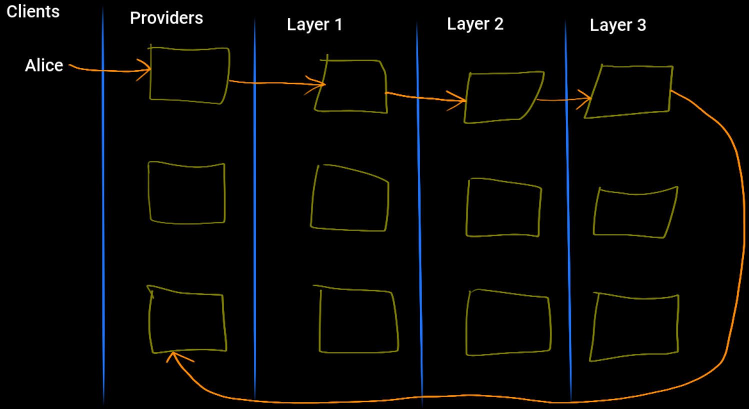

Clients
Mixes
Clients


Clients
Mixes
Providers


Clients
Mixes
Providers
Clients


Clients
Mixes
Providers
Clients


Clients
Mixes
Providers
Clients



Clients

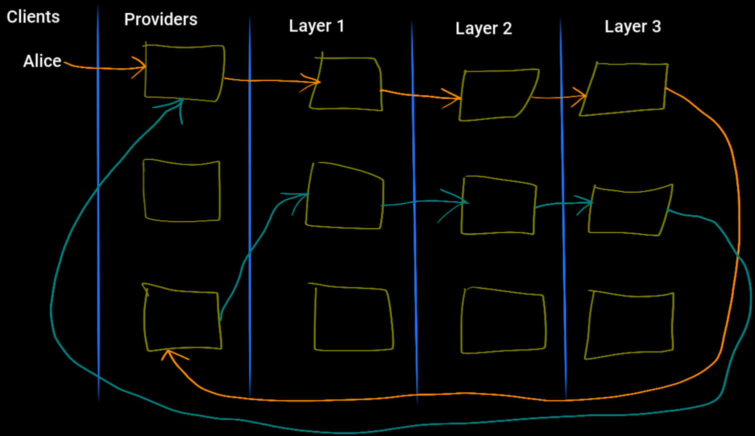
Alice

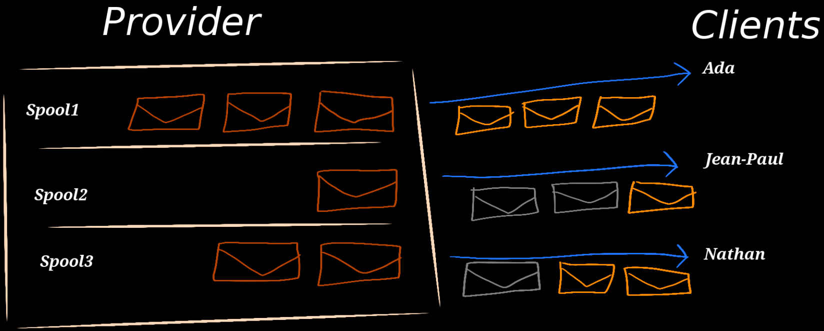
Providers

Layer 1

Layer 2

Layer 3


Clients
Providers
Layer 1
Layer 2
Layer 3
Alice



Provider

Clients

Spool1

Spool2

Spool3

Ada

Jean-Paul

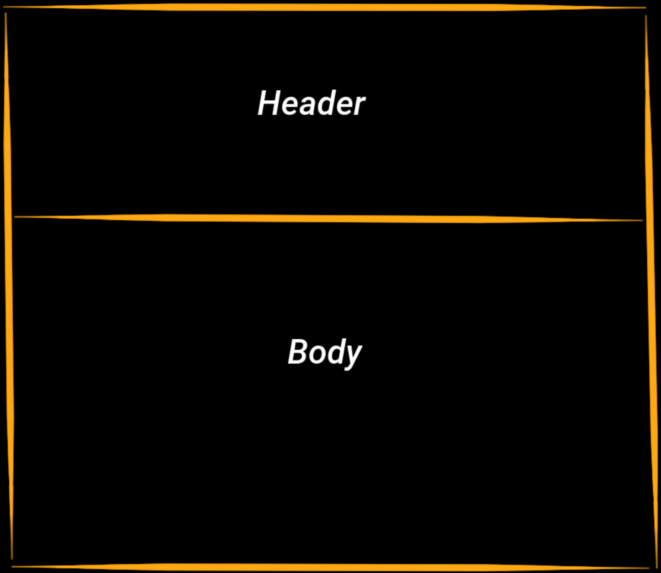
Nathan

Don't roll your own cryptographic packet format!

"Sphinx: A Compact and Provably Secure Mix Format" by George Danezis and Ian Goldberg.

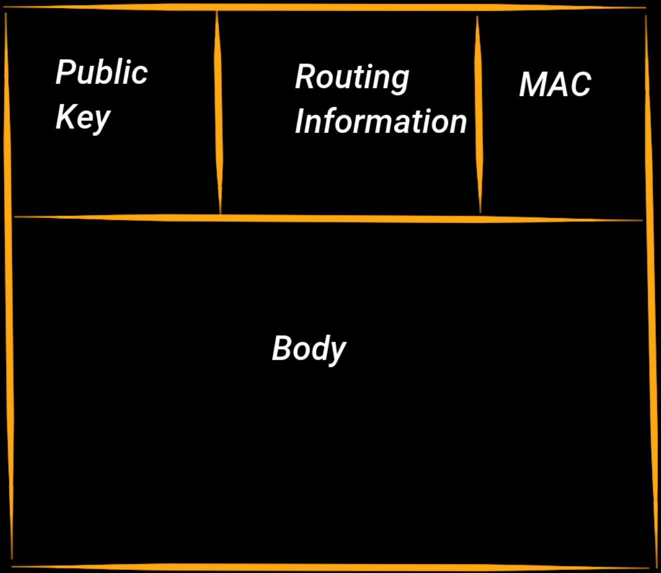
Sphinx features

- per hop bitwise unlinkability
- Single Use Reply Blocks
- indistinguishable replies
- hidden path length
- hidden relay position
- tagging attack detection
- replay attack detection



Header

Body



Public Key

Routing Information

MAC

Body

Compulsion Attacks

- legal action
- police raid
- pwn

Compulsion Attacks Defenses via Mix Key Erasure

- Mix key rotation
- Forward secure mixes

“Forward Secure Mixes” by George Danezis, Proceedings of 7th Nordic Workshop on Secure IT Systems, 2002

“Xolotl: A request-and-forward mixnet format with selective statefulness for forward secure and hybrid post-quantum anonymity” by Jeffrey Burdges and Christian Grothoff

Other Defenses for Compulsion Attacks

- multicast routing hops
- compulsion traps
- plausibly deniable routing

"Compulsion Resistant Anonymous Communications" by George Danezis and Jolyon Clulow, Proceedings of Information Hiding Workshop, June 2005

Other Considerations for Compulsion Attacks

“No right to ramain silent: Isolating Malicious Mixes” by Hemi Leibowitz, Ania Piotrowska, George Danezis and Amir Herzberg

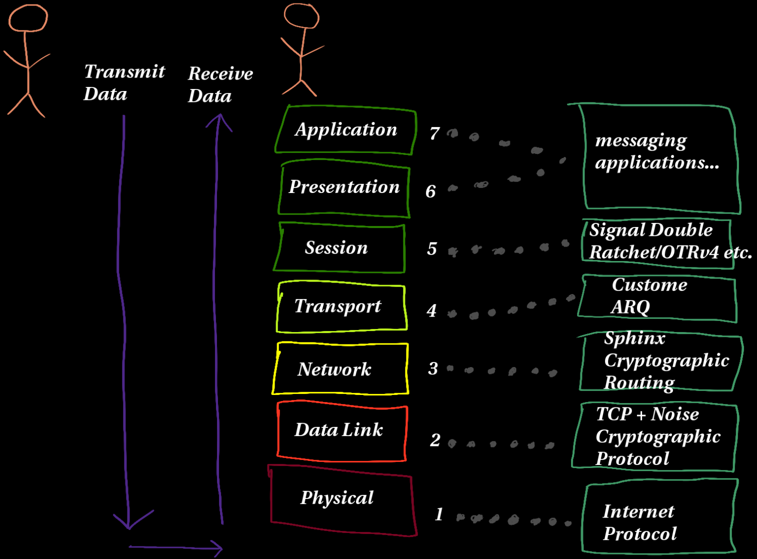
“Two Cents for Strong Anonymity: The Anonymous Post-office Protocol” by Nethanel Gelernter, Amir Herzberg, and Hemi Leibowitz

- mix server
- pki server
- clients

Ania Piotrowska, Jamie Hayes, Tariq Elahi, Sebastian Meiser, and George Danezis. *The Loopix Anonymity System* Usenix 26, 2017.

What is Katzenpost?

- message oriented network
- anonymous
- decentralized



Transmit Data

Receive Data

Application 7 messaging applications...

Presentation 6

Session 5 Signal Double Ratchet/OTRv4 etc.

Transport 4 Custome ARQ

Network 3 Sphinx Cryptographic Routing

Data Link 2 TCP + Noise Cryptographic Protocol

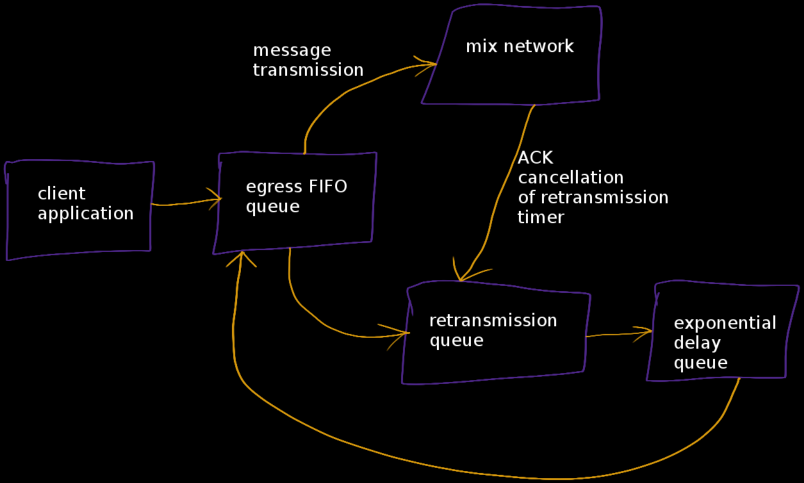
Physical 1 Internet Protocol

Our Noise Cryptographic Link Layer:

TCP

+

Noise_XXhfs_25519+NewHopeSimple_ChaChaPoly_Blake2b


client application

egress FIFO queue

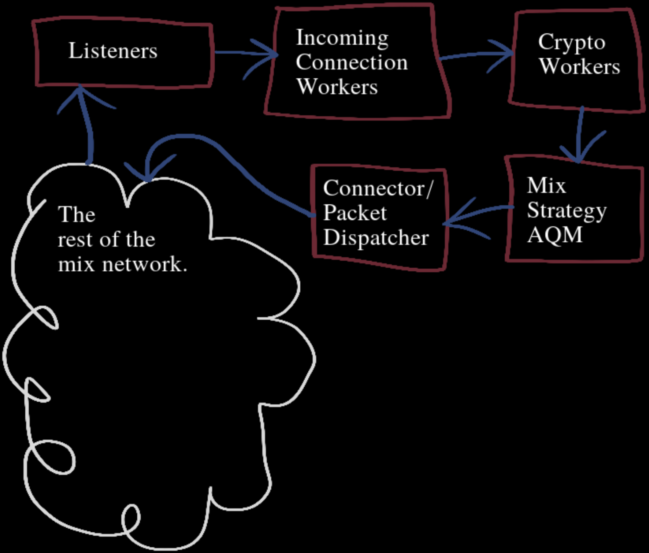
message transmission

mix network

ACK cancellation of retransmission timer

retransmission queue

exponential delay queue



Listeners

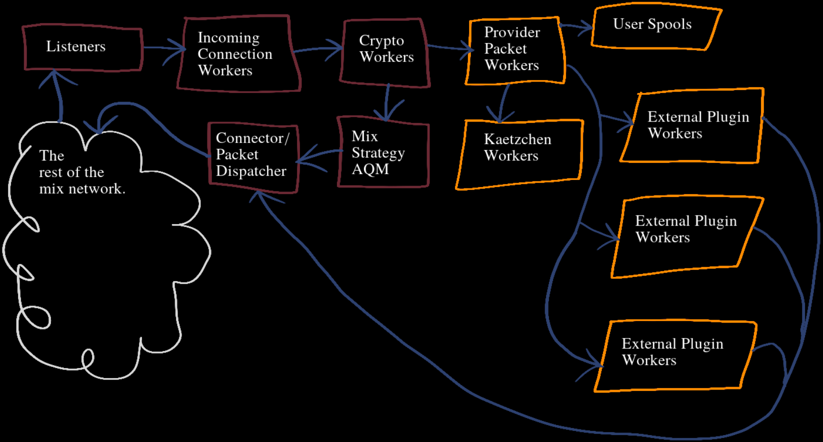
Incoming Connection Workers

Crypto Workers

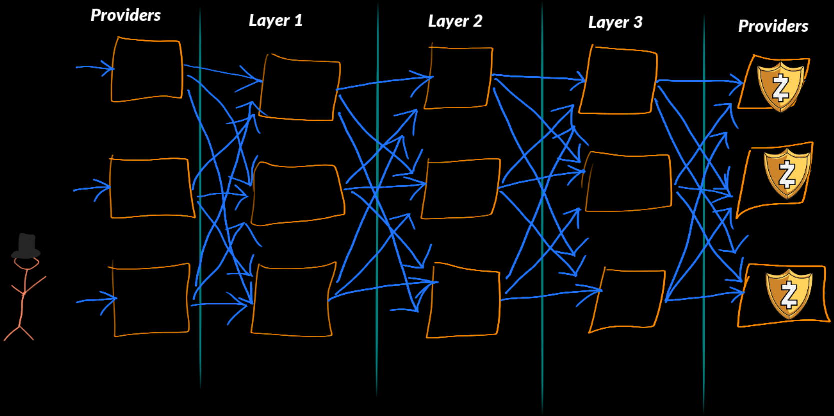
Mix Strategy AQM

Connector/ Packet Dispatcher

The rest of the mix network.


Listeners
Incoming Connection Workers
Crypto Workers
Provider Packet Workers
User Spools
External Plugin Workers
Kaetzchen Workers
Mix Strategy AQM
Connector/ Packet Dispatcher
The rest of the mix network.
External Plugin Workers
External Plugin Workers

Zcash Mix Network?



The Katzenpost Free Software Project

Website:
https://katzenpost.mixnetworks.org/

Github:
https://github.com/katzenpost/

IRC: #katzenpost on OFTC

- Questions? Contact me: dawuud@riseup.net
- Follow me on twitter: @david415