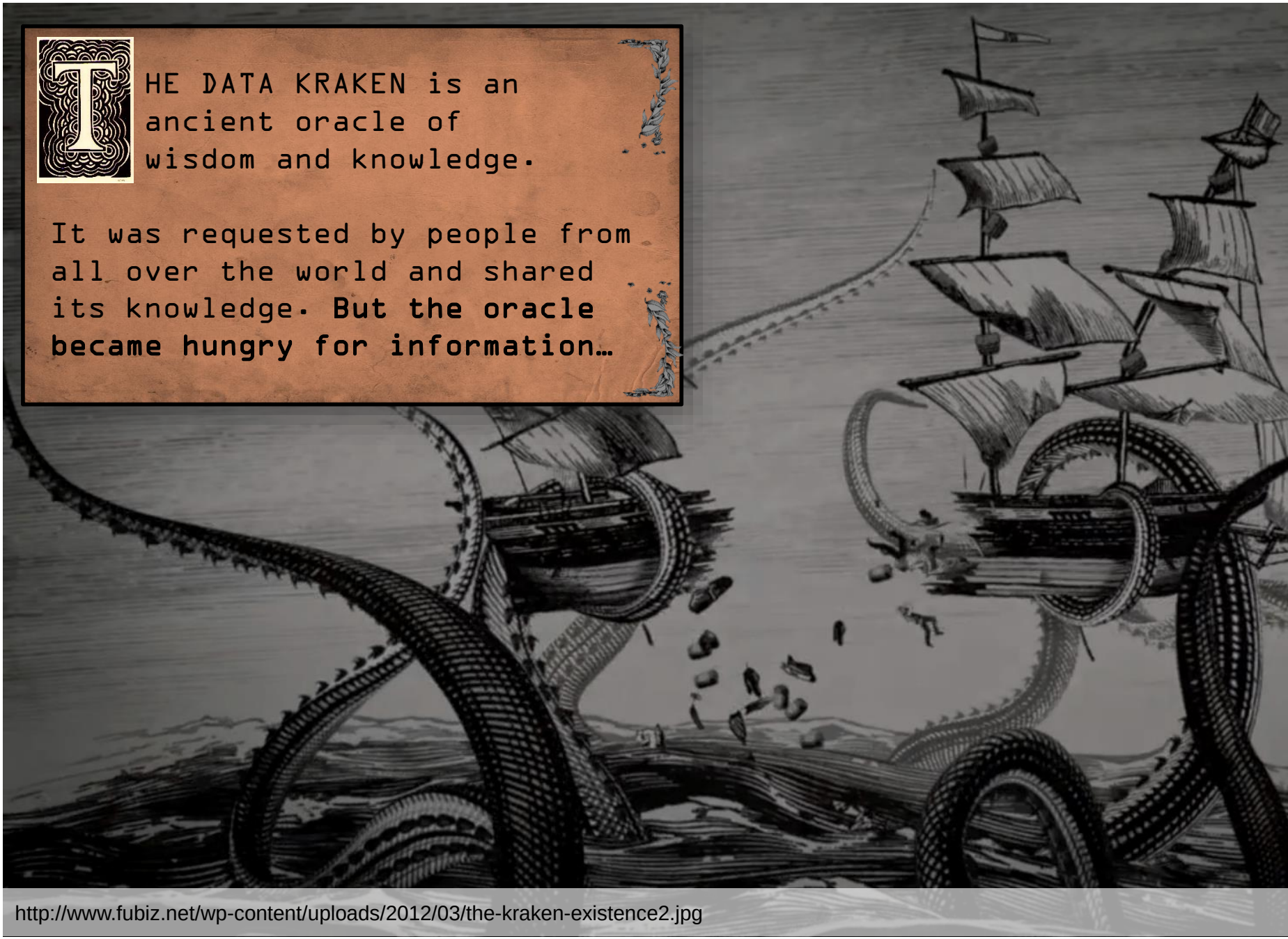


http://www.fubiz.net/wp-content/uploads/2012/03/the-kraken-existence2.jpg

Modern Mix Network Design

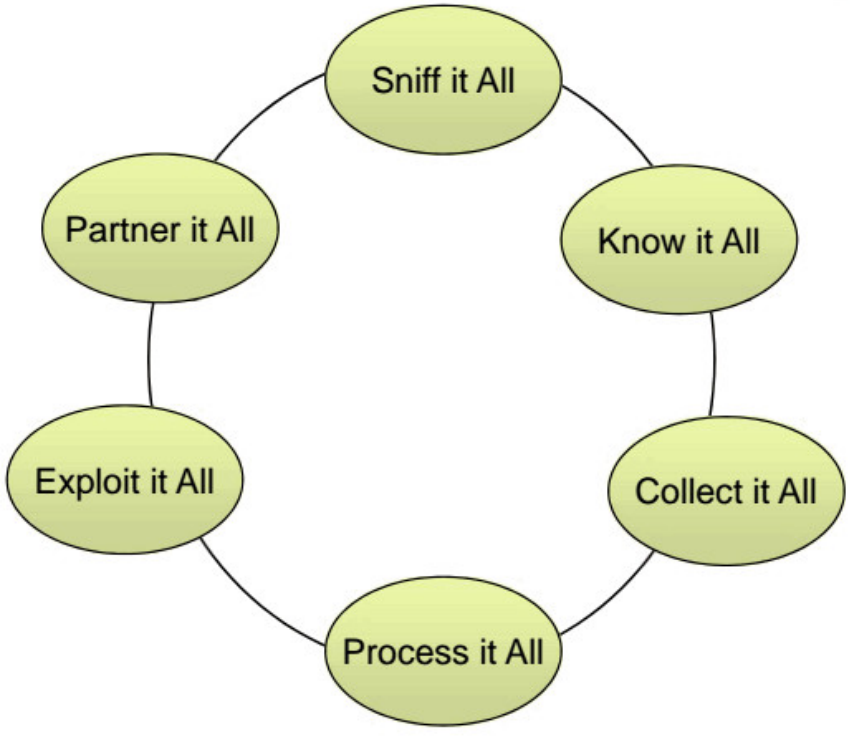
David Stainton

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



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

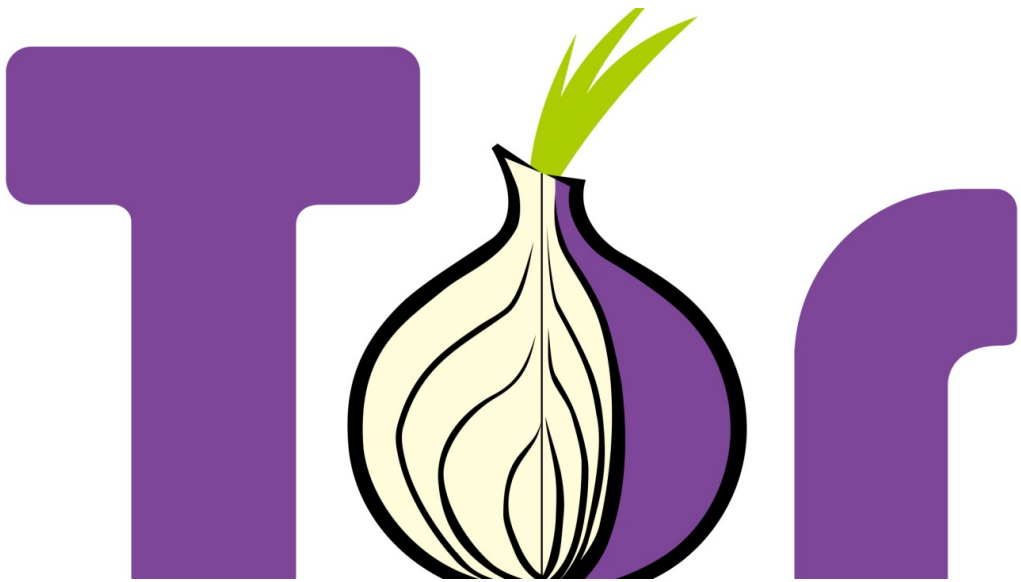
Meta-data leakage

Why not use a VPN?

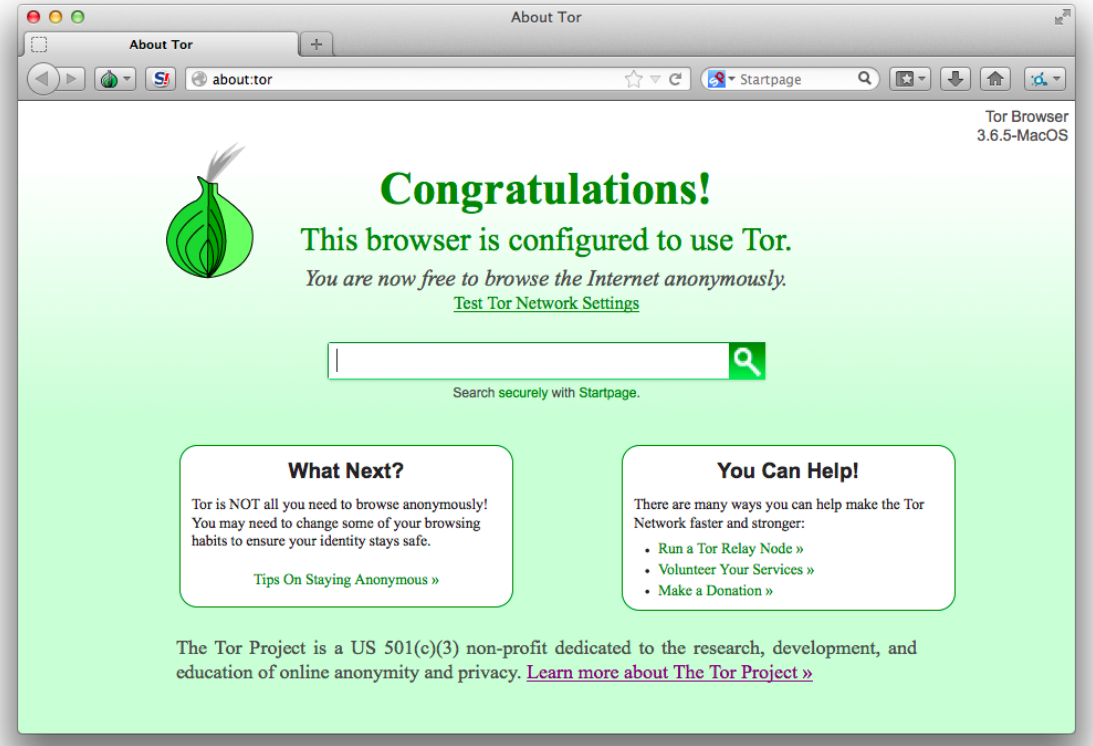
Major problems:

- Plaintext intermediary
- Traffic fingerprinting
- Possible leakage of client identity keys

Existing solutions?



You only need one side if the other side behaves predictably, like a website.



Admit defeat on the web for now..

Should we message our friend's over Tor?
Should we send crypto currency transactions over Tor?

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:

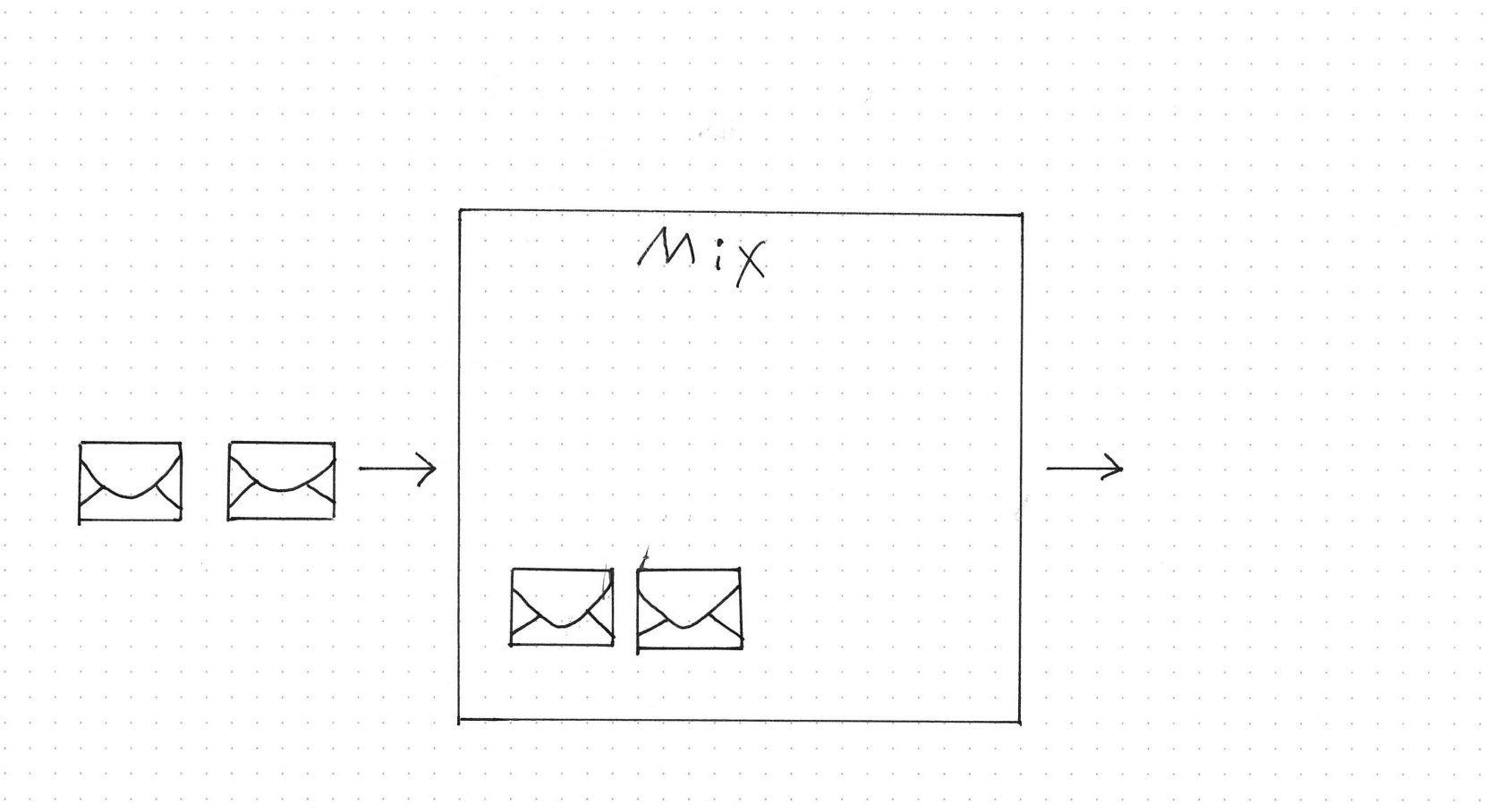
- Sender anonymity
- Anonymous replies
- Message receipts for reliability
- Pseudonyms for persistent communication

Mix Properties

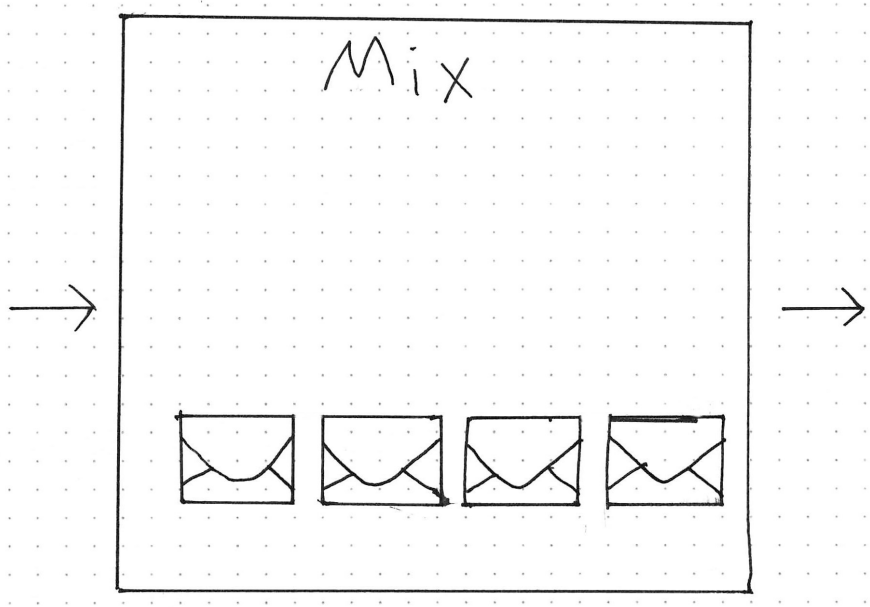
Required mix properties to defeat global passive adversaries:

- Bitwise unlinkability between input and output messages
- Latency (aka mixing)

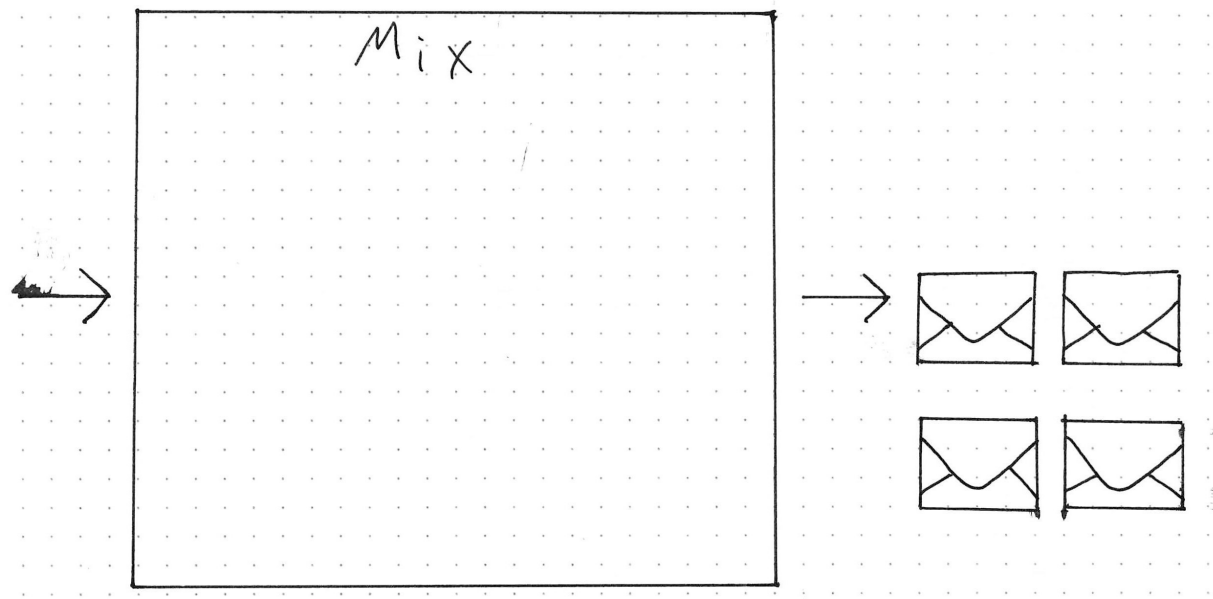
n-1 attack on threshold mix strategy



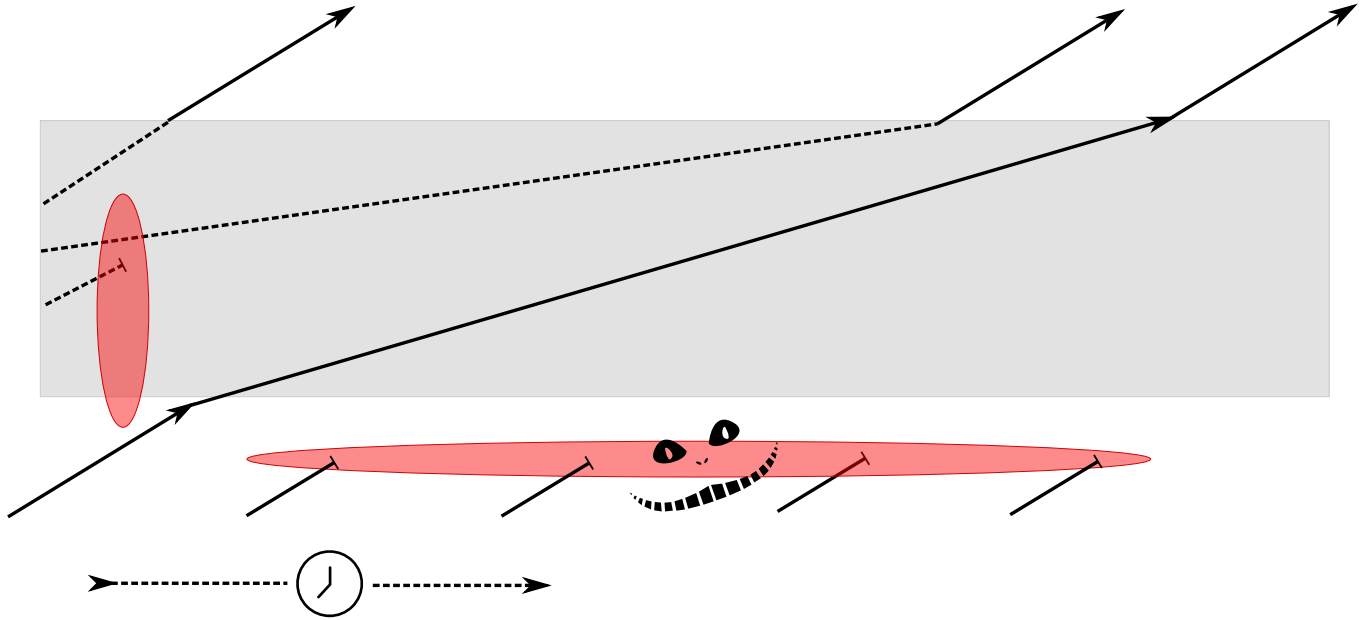
n-1 attack on threshold mix strategy



n-1 attack on threshold mix strategy



n-1 attacks against continuous time mix strategies



Tor is not a mix network.

See:

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

What is a mix network?

- A closed network (no exit relays)
- Message oriented
- Unreliable packet switching network
- Layered encryption in a single packet
- Added latency per hop, aka they mix
- Can optionally use route unpredictability
- Can optionally use decoy traffic

Topology: Cascade

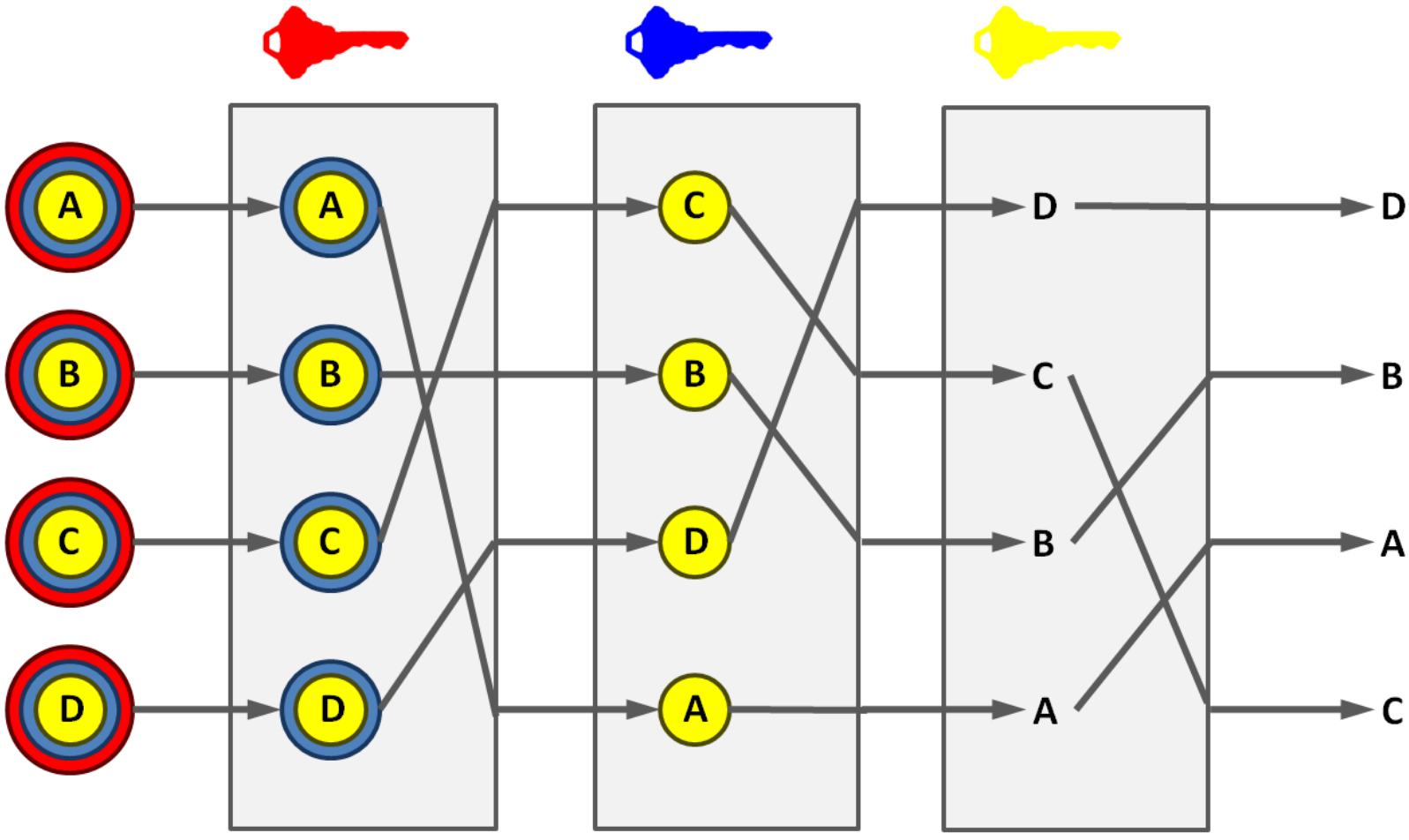
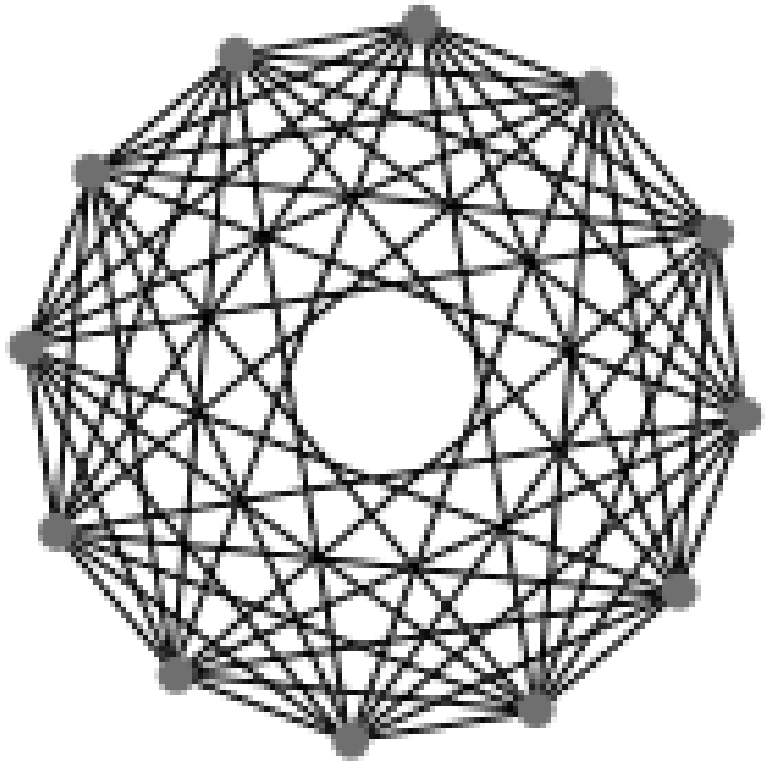
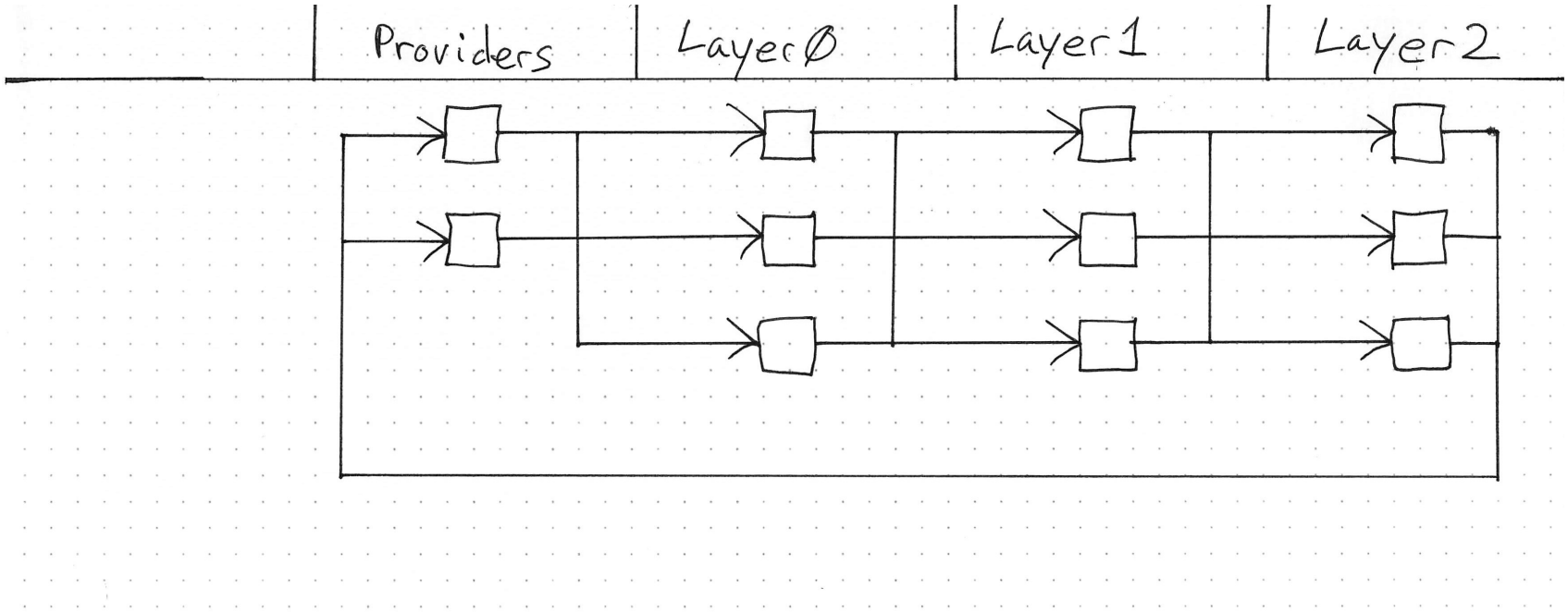


Diagram borrowed from wikipedia.

Topology: Free route



Topology: Stratified



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

Don't roll your own packet format!

Sphinx is a remarkably compact and secure packet format designed by George Danezis and Ian Goldberg.

Security proof in the universal composability model, using earlier work by Camenisch & Lysyanskaya 2005.

Don't roll your own packet format!

Sphinx is a remarkably compact and secure packet format designed by George Danezis and Ian Goldberg.

Security proof in the universal composability model, using earlier work by Camenisch & Lysyanskaya 2005.

Sphinx features

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

Compulsion Attacks

Mix key compromise can take several forms such as:

- Compromising mixes through software vulnerabilities
- Compel the mix operator to hand over the keys (legal action)
- Physical access to the mix (police raid)

Forward Secrecy

- Under the compulsion threat model Tor is more secure because interactive bidirectional circuits allow for frequent ephemeral key exchanges.

- Mix key erasure reduces possible flight time of messages

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

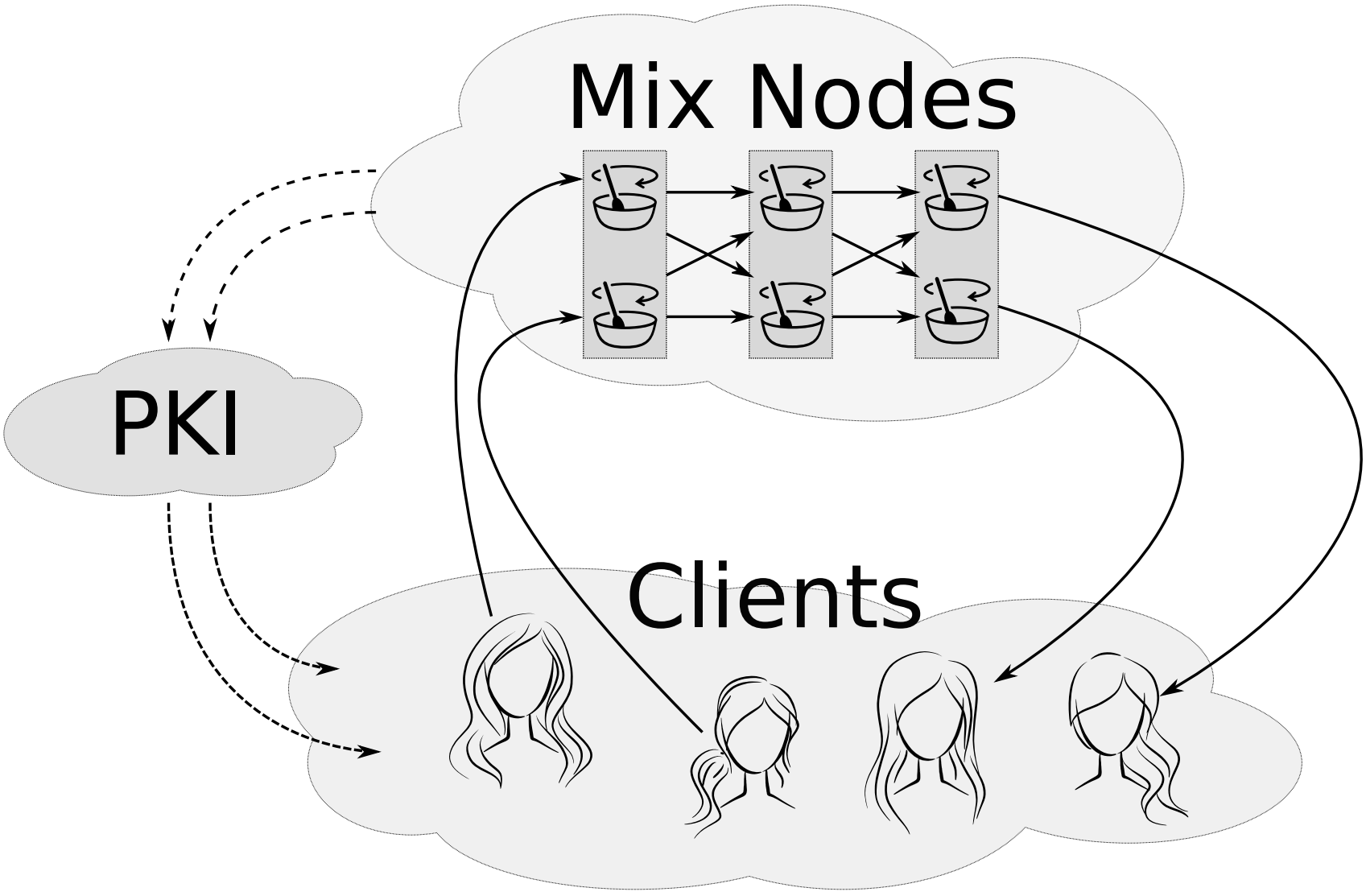
"Compulsion Resistant Anonymous Communications" by George Danezis and Jolyon Clulow, Proceedings of Information Hiding Workshop, June 2005

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

Epistemic Attacks



Statistical disclosure attack on p2p mixnet

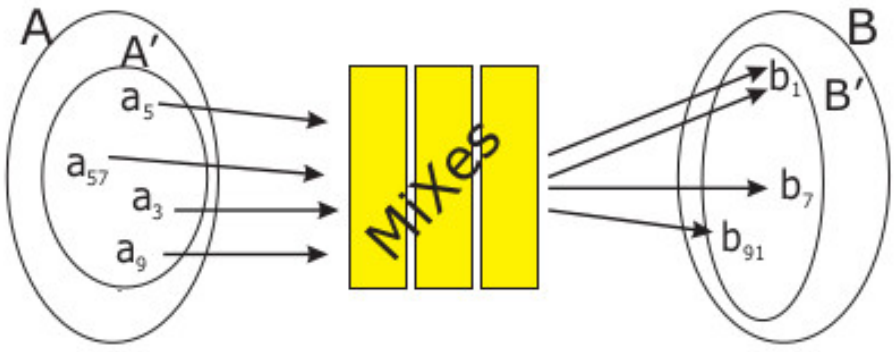


Diagram borrowed from "The Hitting Set Attack on Anonymity Protocols" by Dogan Kesdogan and Lexi Pimenidis

Statistical disclosure attack on mixnet with Provider model

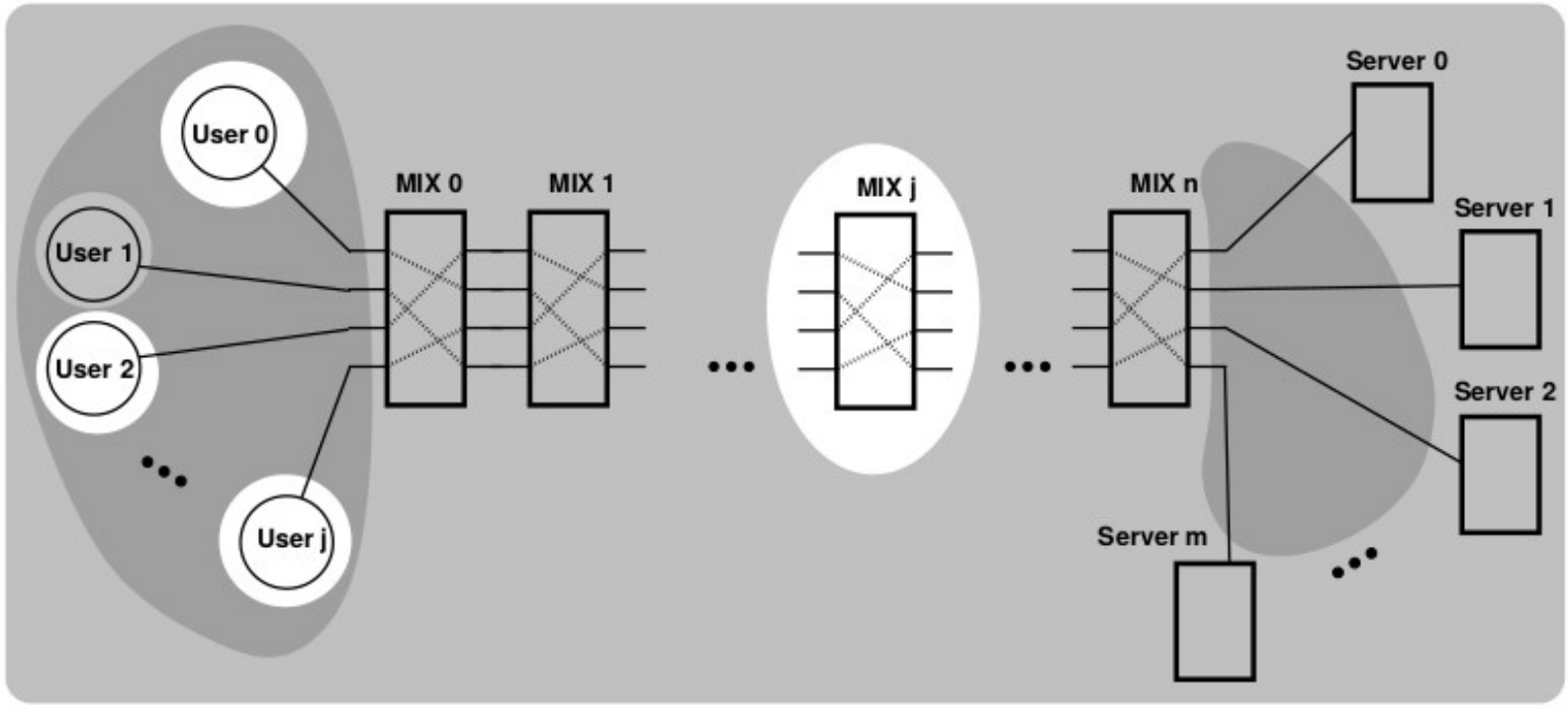
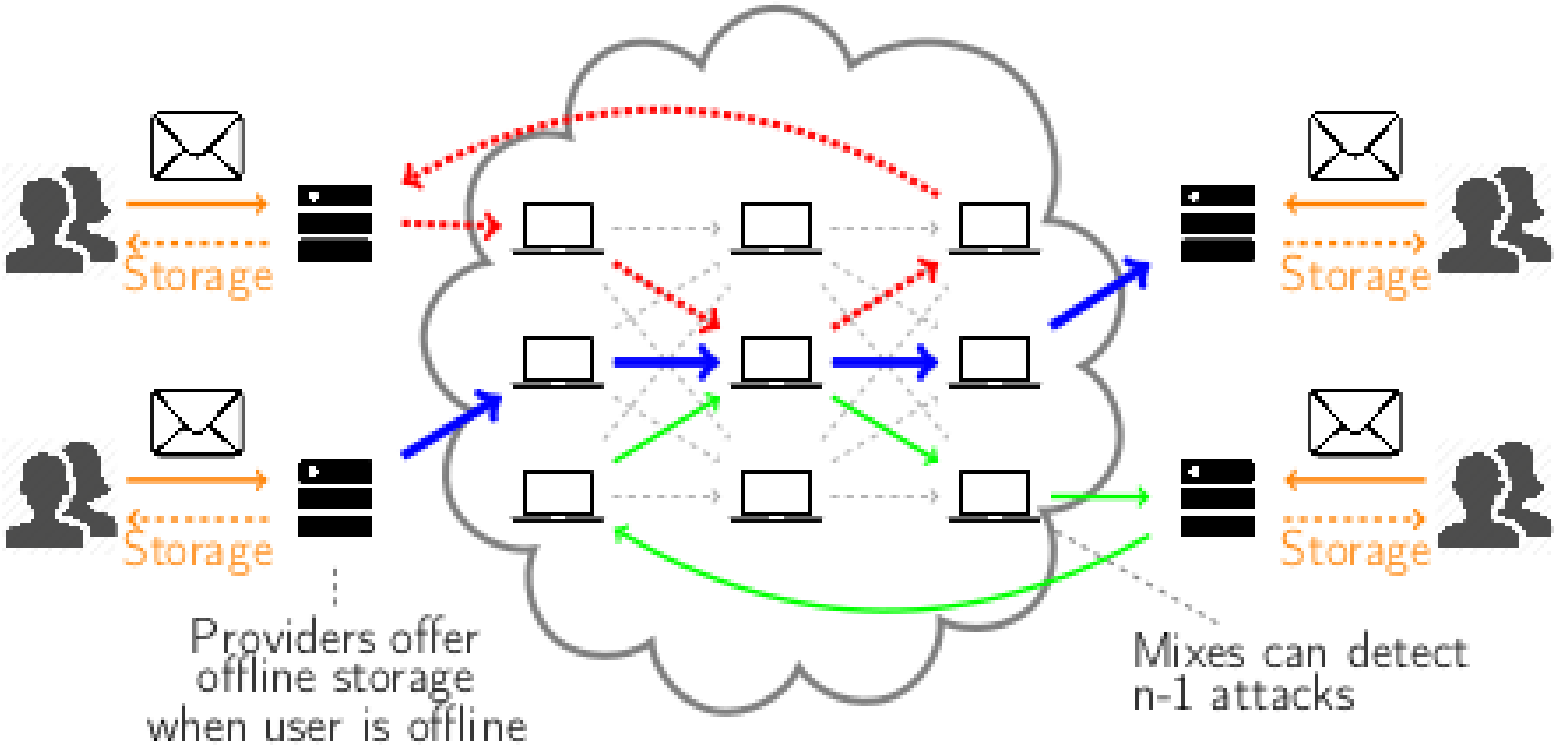


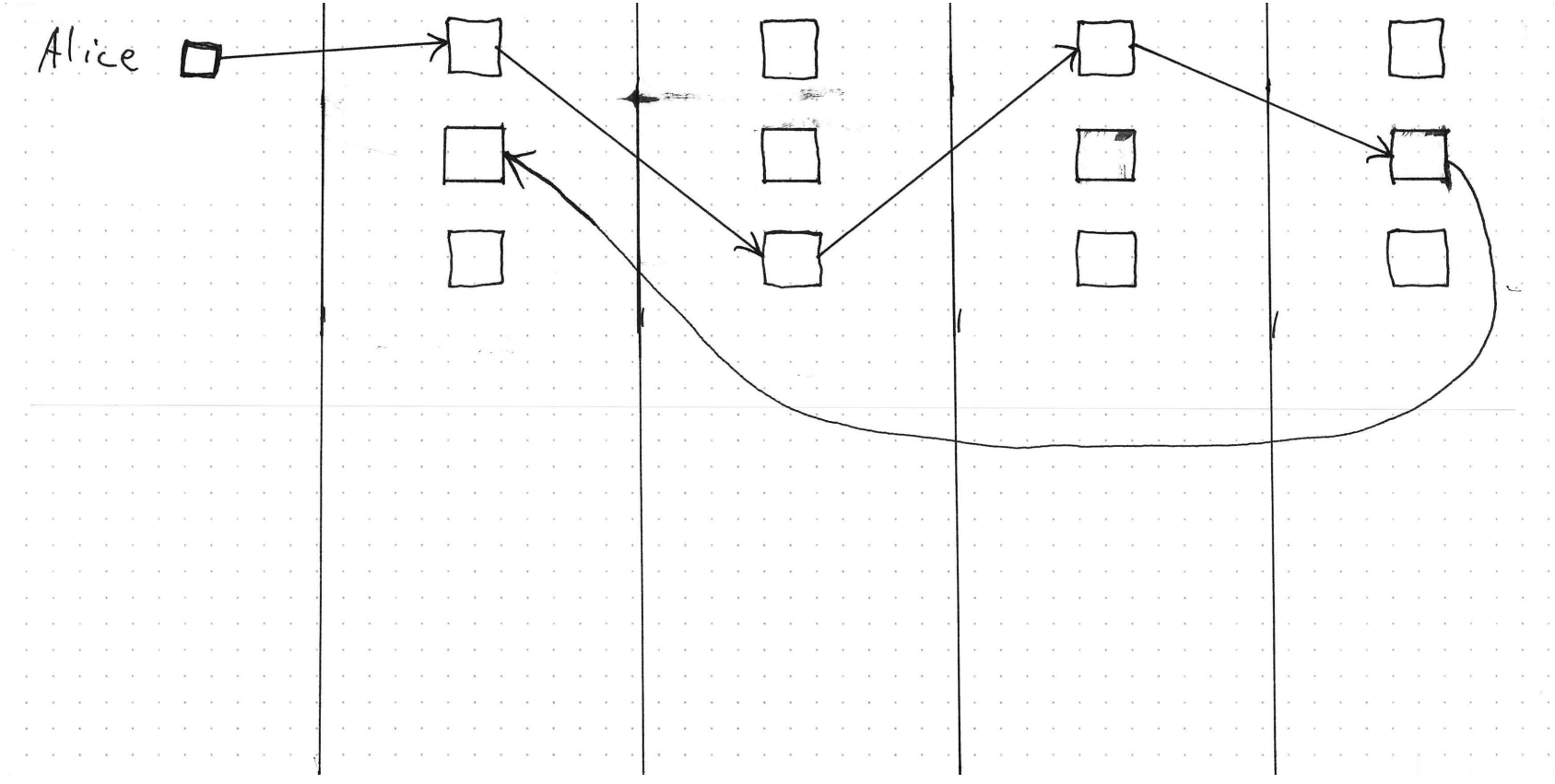
Diagram borrowed from "Dummy Traffic Against Long Term Intersection Attacks" by Oliver Berthold and Heinrich Langos

Katzenpost is Loopix

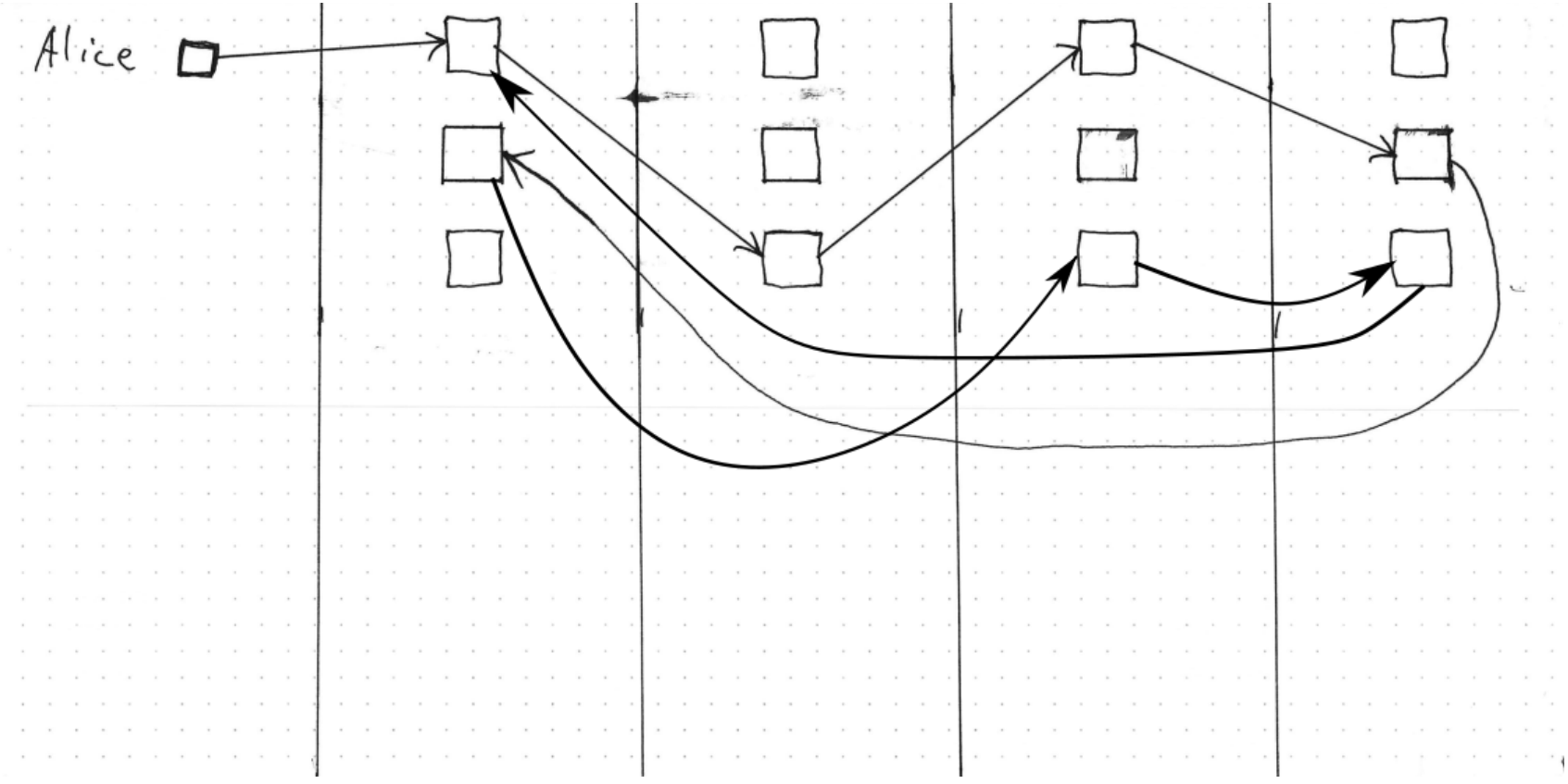


Ania Piotrowska, Jamie Hayes, Tariq Elahi, Sebastian Meiser, and George Danezis. *The Loopix Anonymity System* Usenix 26, 2017.

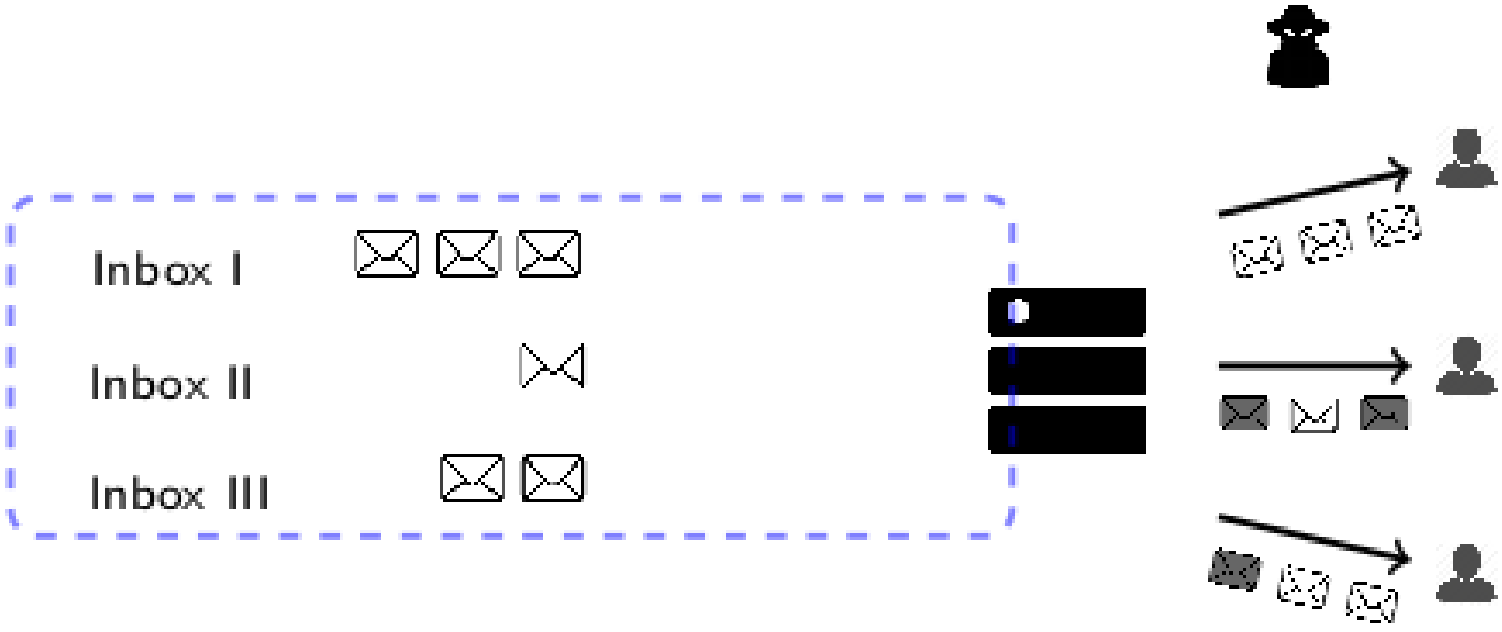
client decoy drop messages



client decoy loop messages



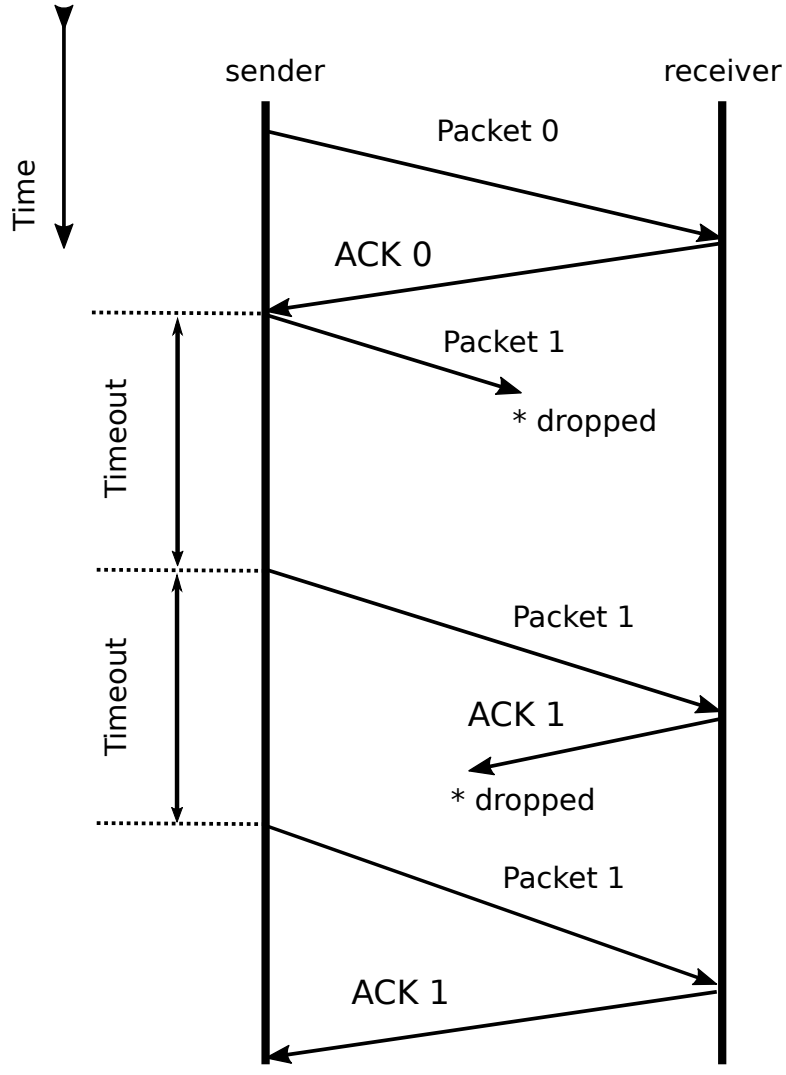
Loopix Provider to Client traffic padding



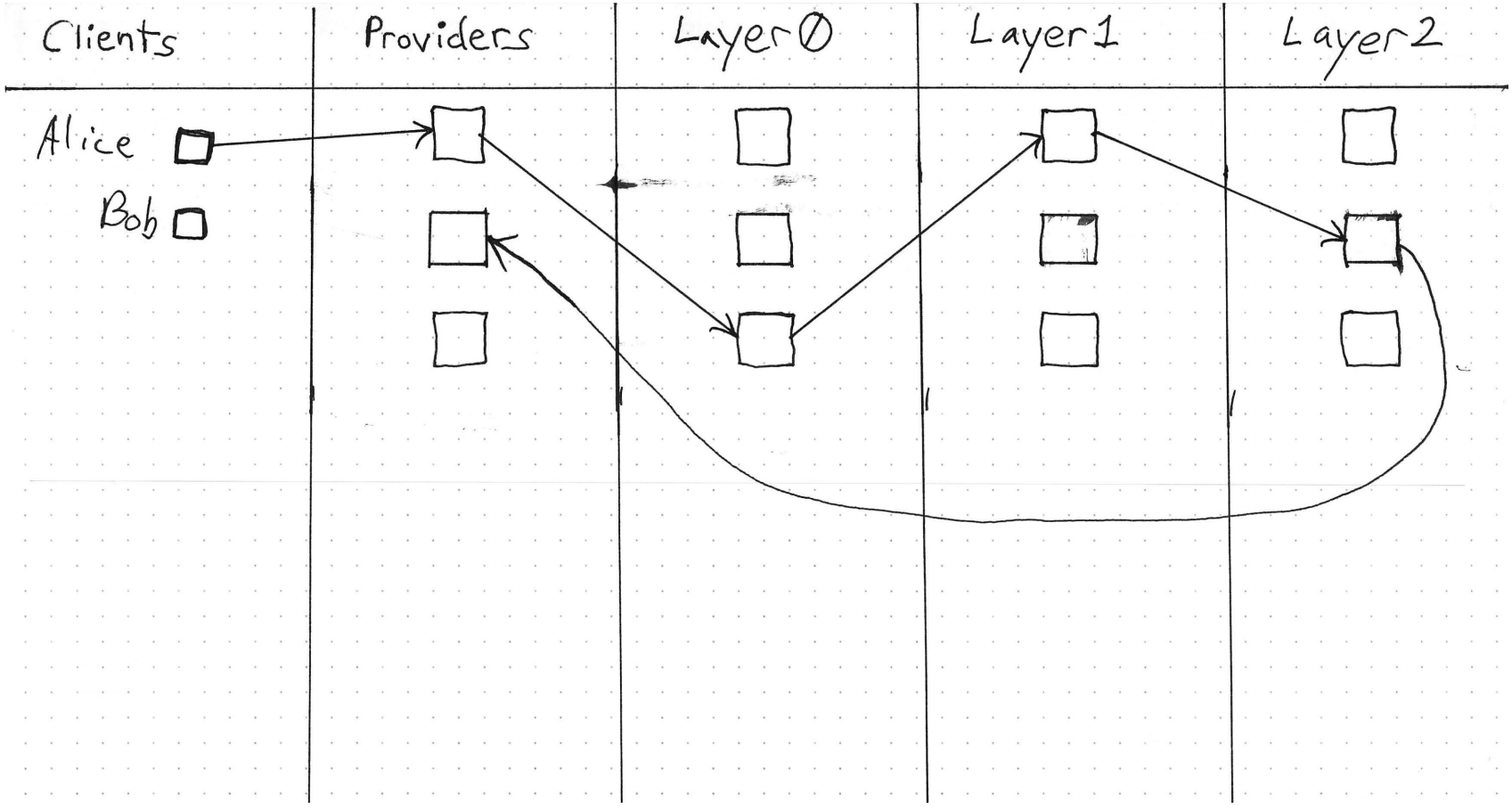
Automatic Repeat reQuest protocol schemes using mixnets?

The case of the lost packet

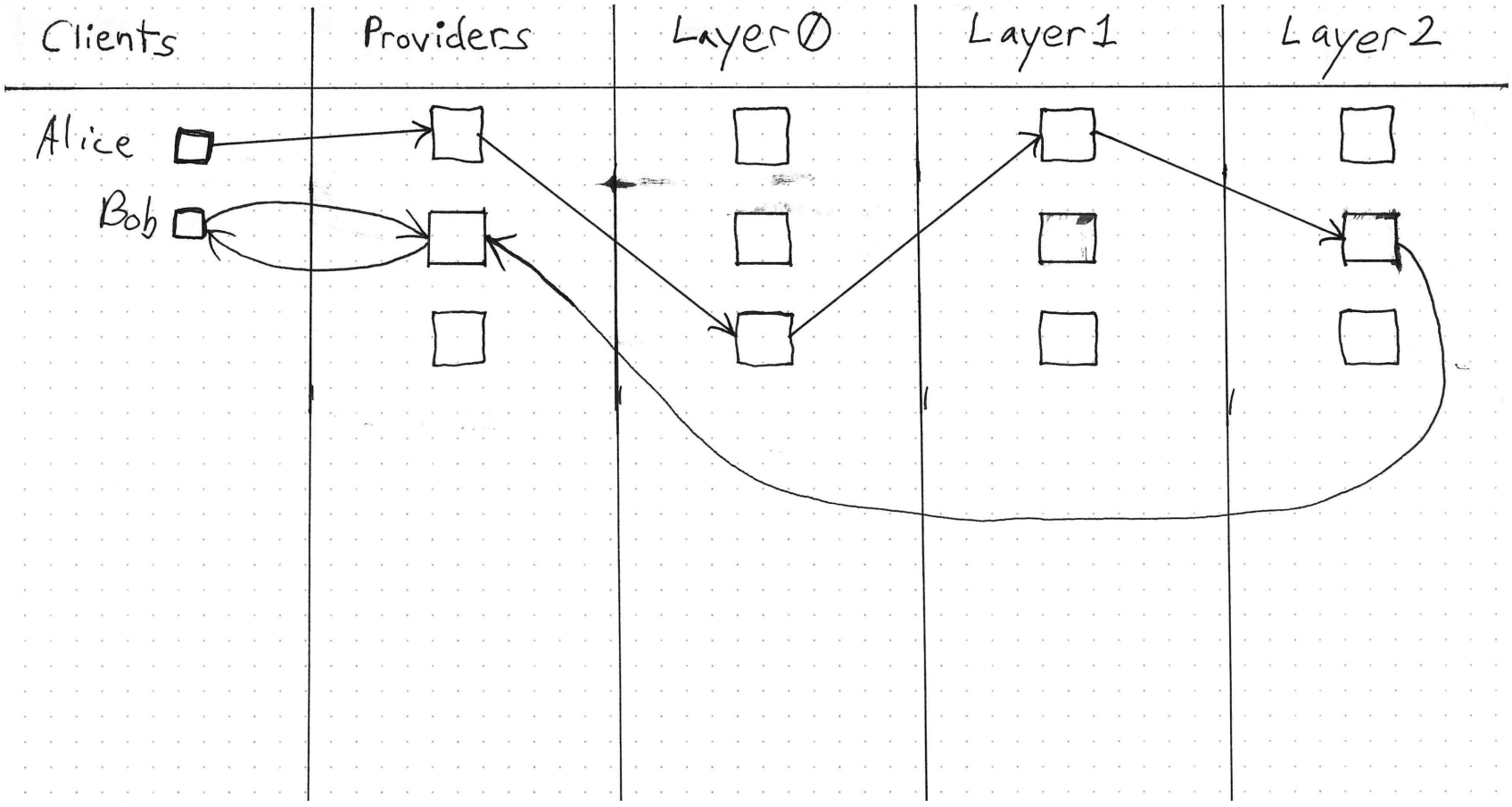
The case of the lost ACK



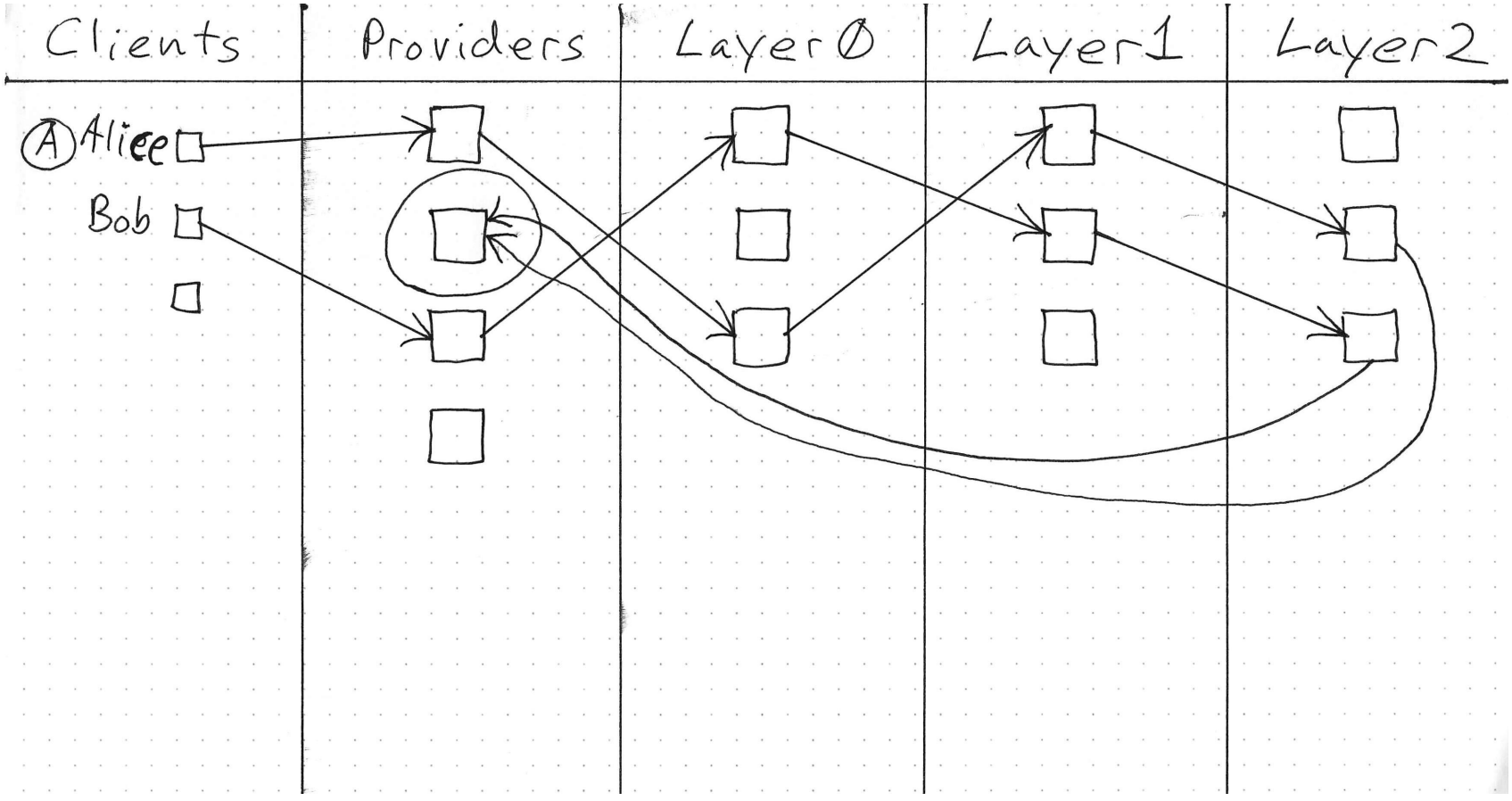
Loopix: Alice sends a message to Bob



Loopix: Bob retreives message from his Provider.



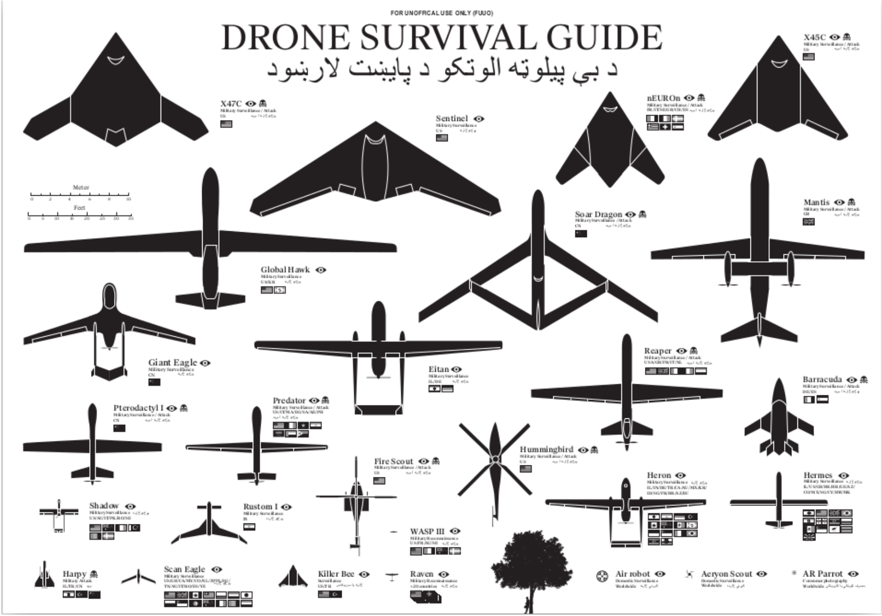
Stronger location hiding properties.

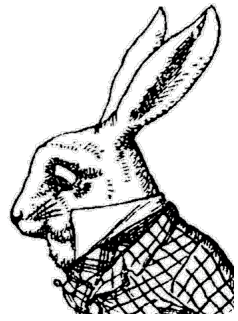


Network privacy for crypto currency transactions?

Does it make sense to use mixnets with Bitcoin?
Yes! We get pseudonymity.
With Zcash we get anonymity.

- use-case is tolerant of latency
- needs reliability but doesn't need explicit ACKs
- only needs one or two kinds of Loopix decoy traffic
- minimal exposure to statistical disclosure attack


FOR UNOFFICIAL USE ONLY (FUUO)
DRONE SURVIVAL GUIDE
د بې پیلوټه الوتکو د پایښت لارښود
X47C
Sentinel
nEUROn
X45C
Meter
Feet
Soar Dragon
Mantis
Global Hawk
Giant Eagle
Eitan
Reaper
Barracuda
Pterodactyl I
Predator
Fire Scout
Hummingbird
Heron
Hermes
Shadow
Rustom I
WASP III
Harpy
Scan Eagle
Killer Bee
Raven
Air robot
Aeryon Scout
AR Parrot



Thanks to the rest of the Katzenpost design team:

Yawning Angel
George Danezis
Claudia Diaz
Ania Piotrowska