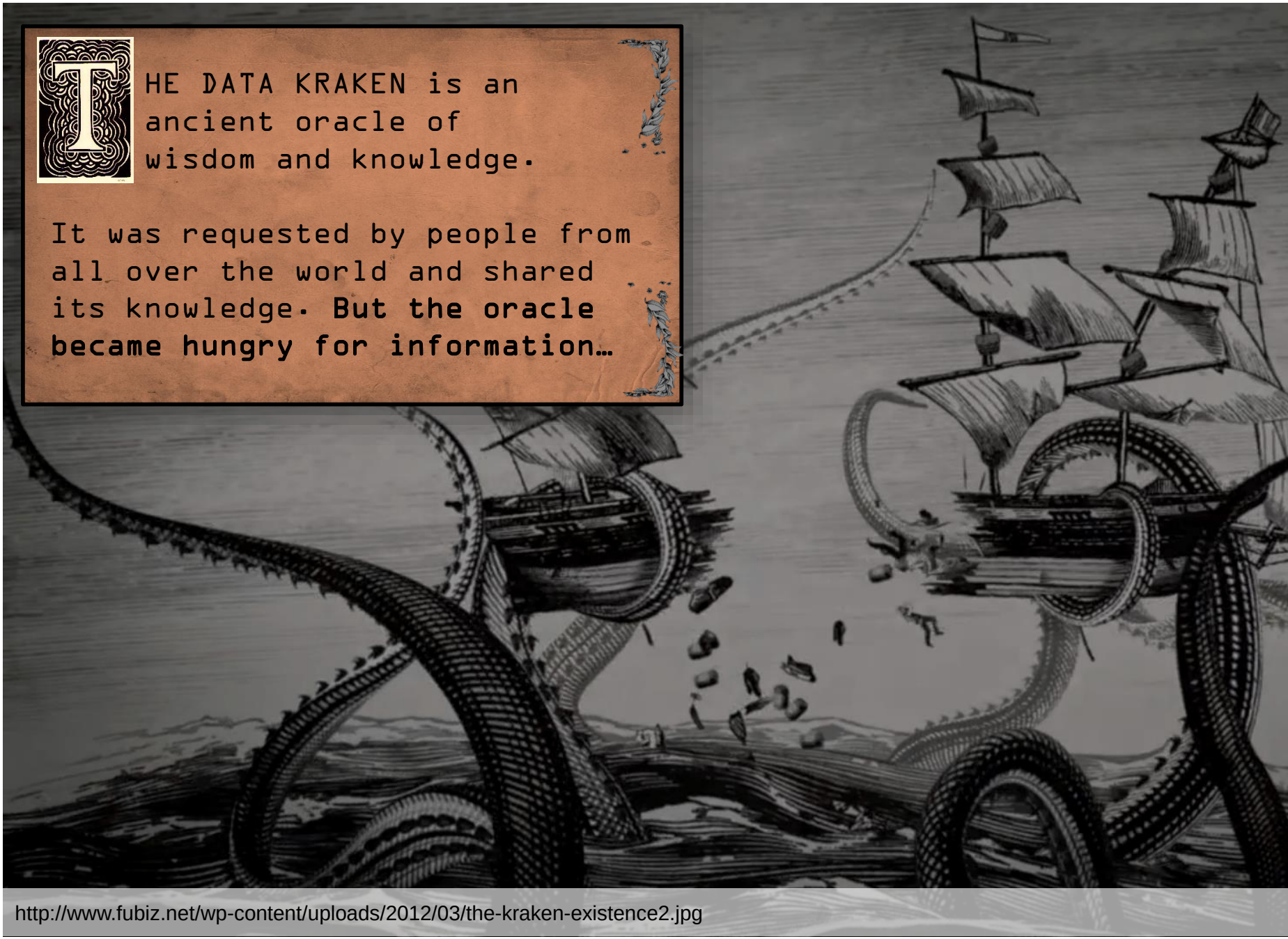
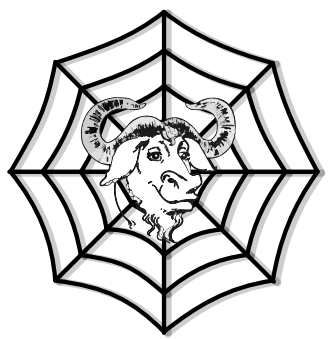


http://www.fubiz.net/wp-content/uploads/2012/03/the-kraken-existence2.jpg

Practical Mix Network Design

Jeff Burdges David Stainton



Panoramix

27.12.2017

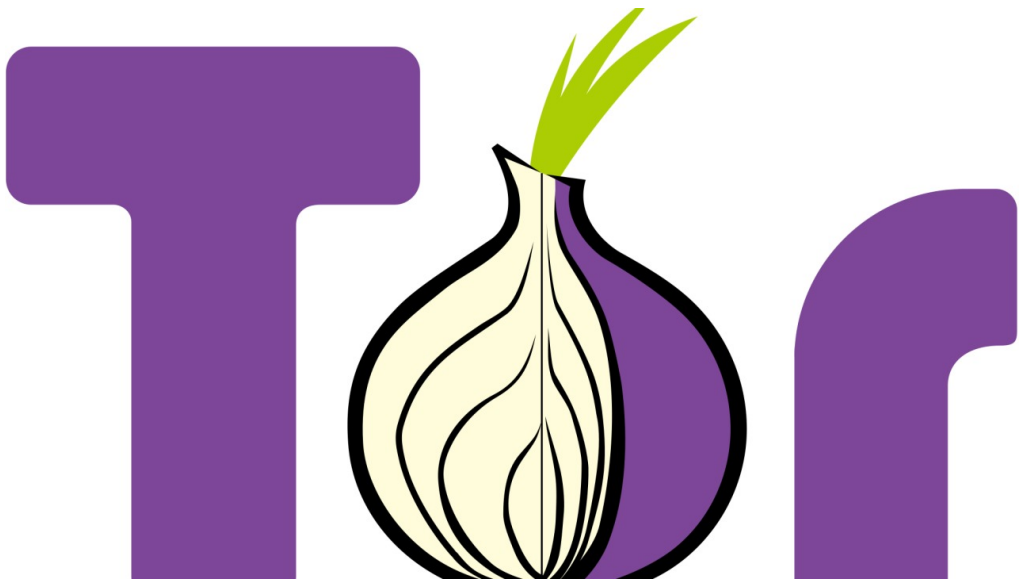
"Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."

–Edward Snowden (2013)

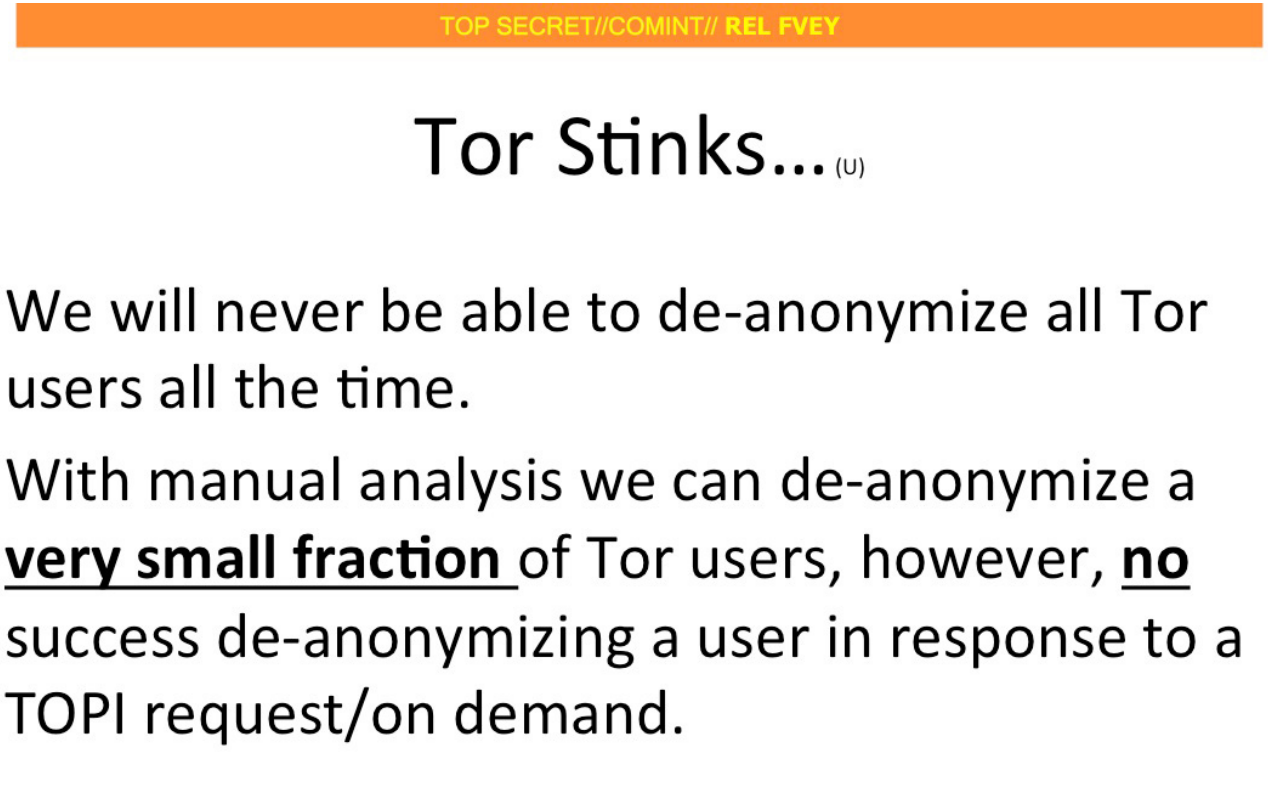
"We kill people based on metadata"
–Michael Hayden (Ex-NSA Director)

Time to resist traffic analysis!

Existing solutions?



Five years ago the NSA considered Tor effective, at least against mass location tracking.



Tor is not enough

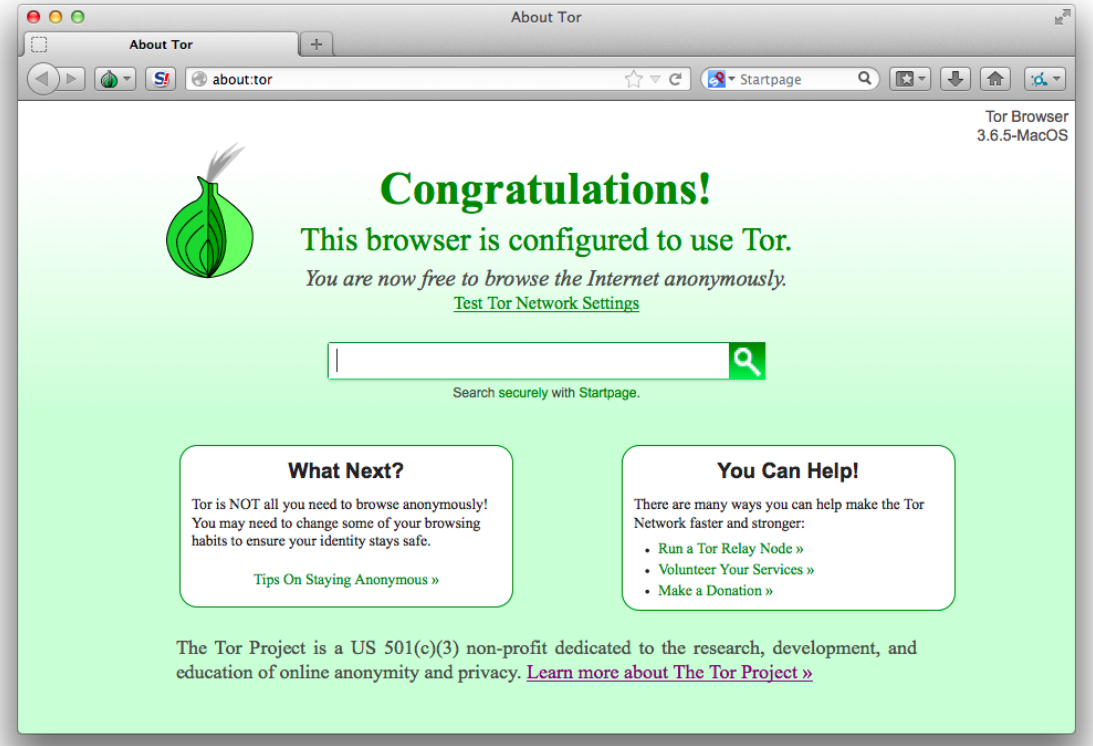
"[Tor does not] protect against an attacker who can see .. both traffic going into [and] coming out of the Tor network .. as simple statistics let you decide whether [both flows] match up."

–Roger Dingledine, "One cell is enough .."

See:

Johnson, Wacek, Jansen, Scherr, Syverson. *Users Get Routed: Traffic Correlation on Tor By Realistic Adversaries.* (CCS 2013)

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



Admit defeat on the web for now..

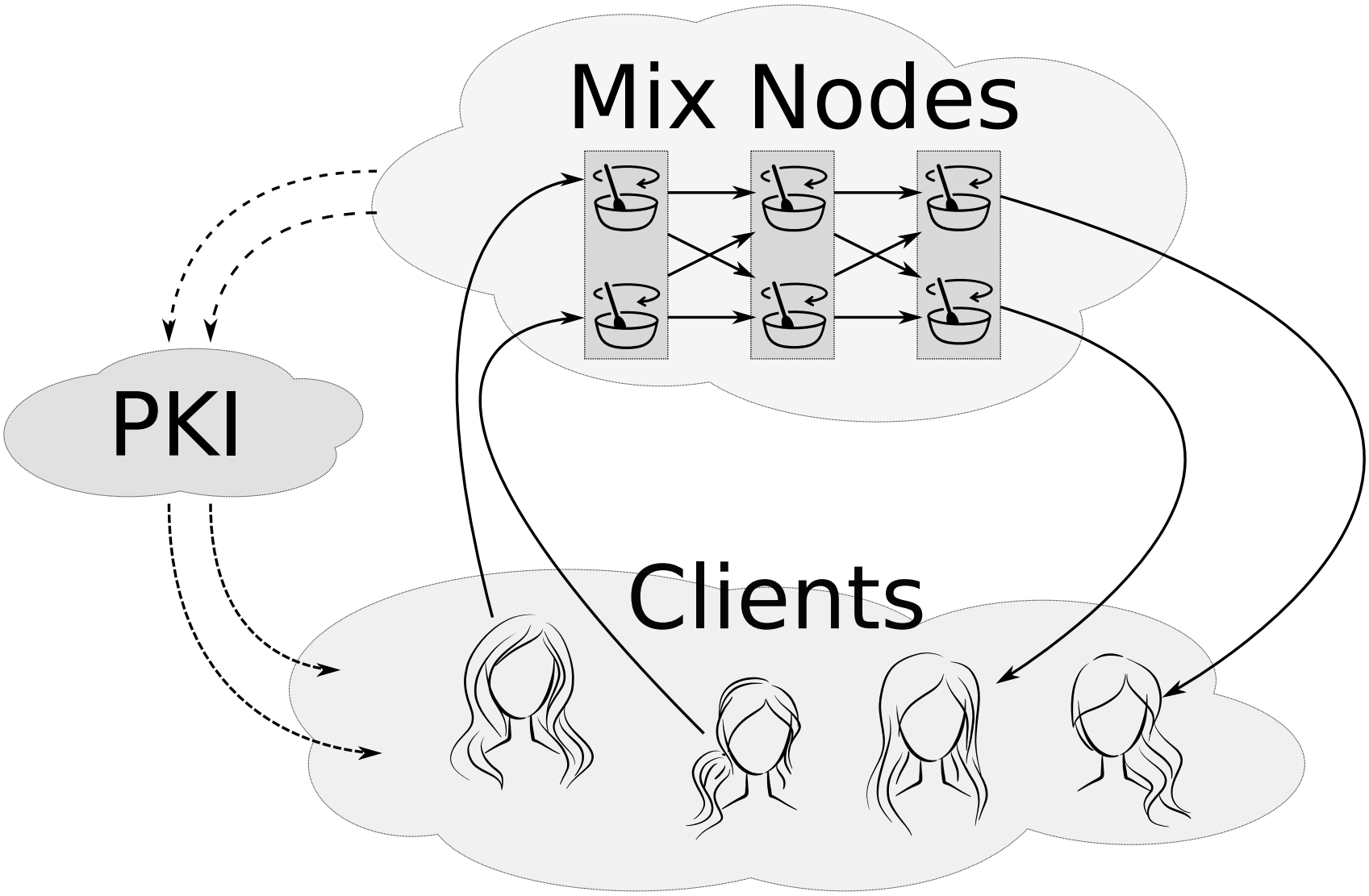
Can we message our friend's over Tor?

How can we keep messaging metadata private?

What is a mix network?

1. Message oriented
2. Unreliable packet switching network
3. Layered encryption in a single packet
4. Added latency per hop, aka they mix

What is a mix network?



Mix networks are among the oldest anonymity tools, dating back to

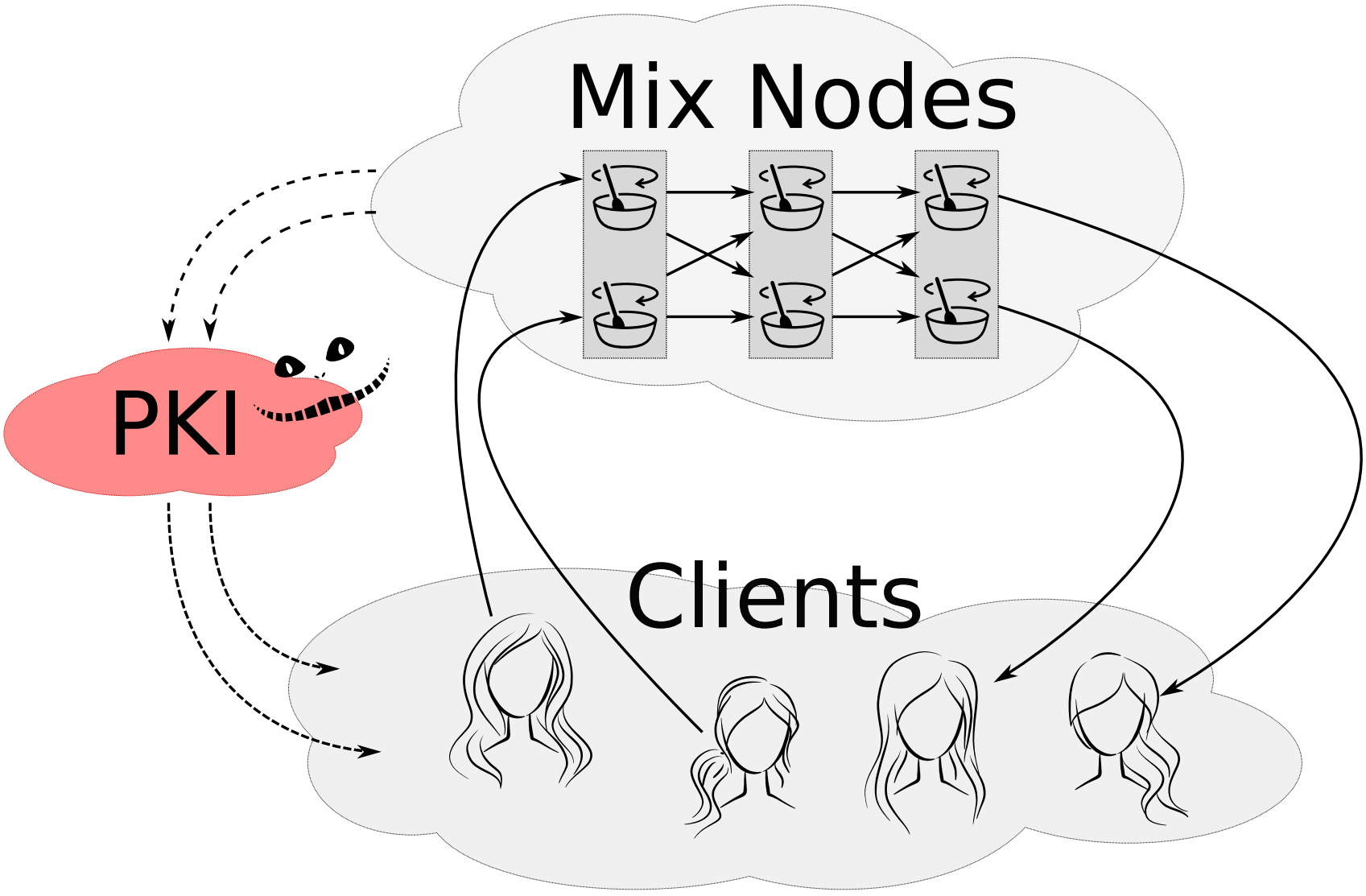
David Chaum. *Untraceable electronic mail, return addresses, and digital pseudonyms*, Comm. ACM, 24, 2 (Feb. 1981); 84-90

We know other anonymity system designs, like

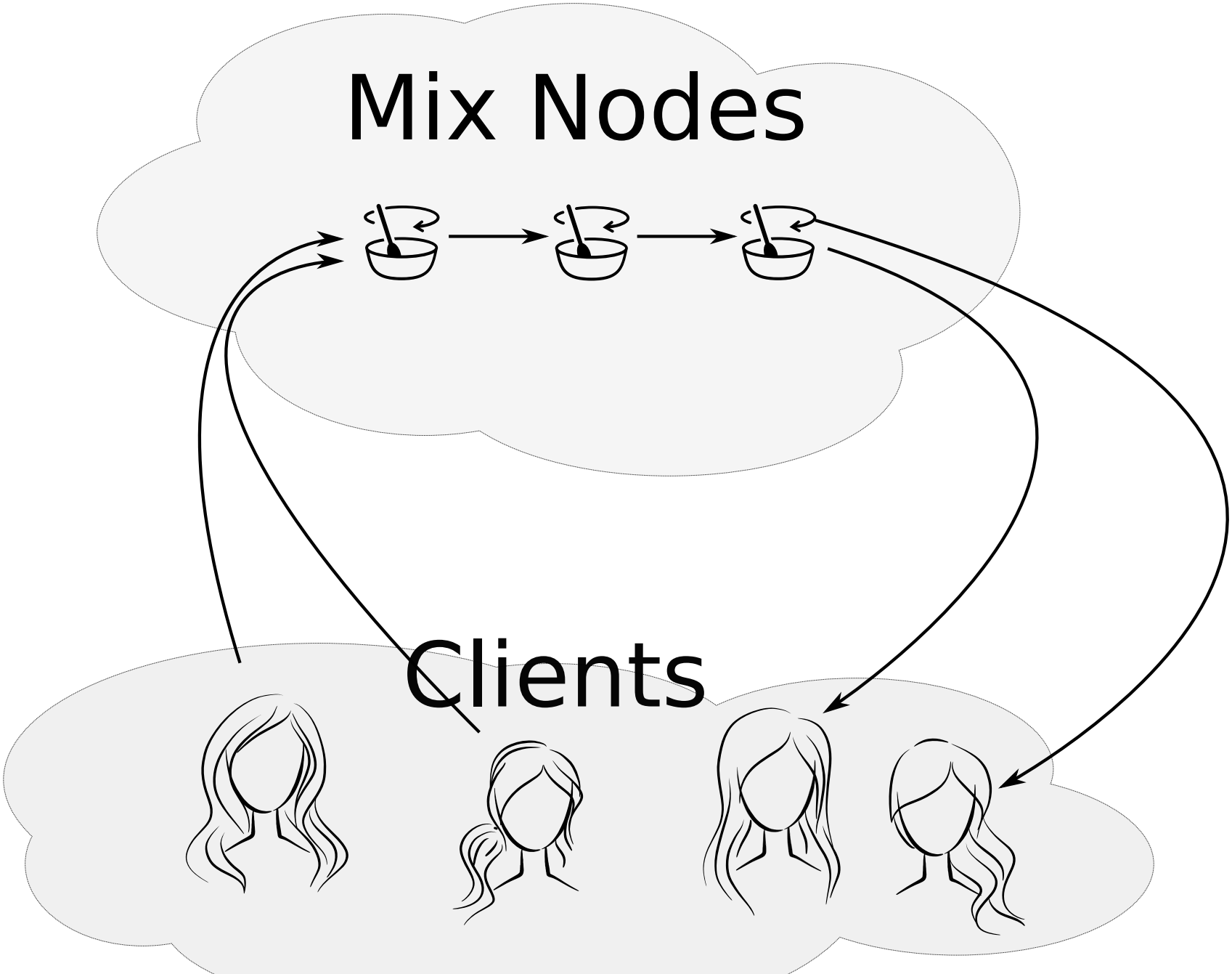
- Dining cryptographer's networks (DC-nets)
- Private Information Retrieval (PIR)

but they all scale poorly.. most need quadratic bandwidth per user.

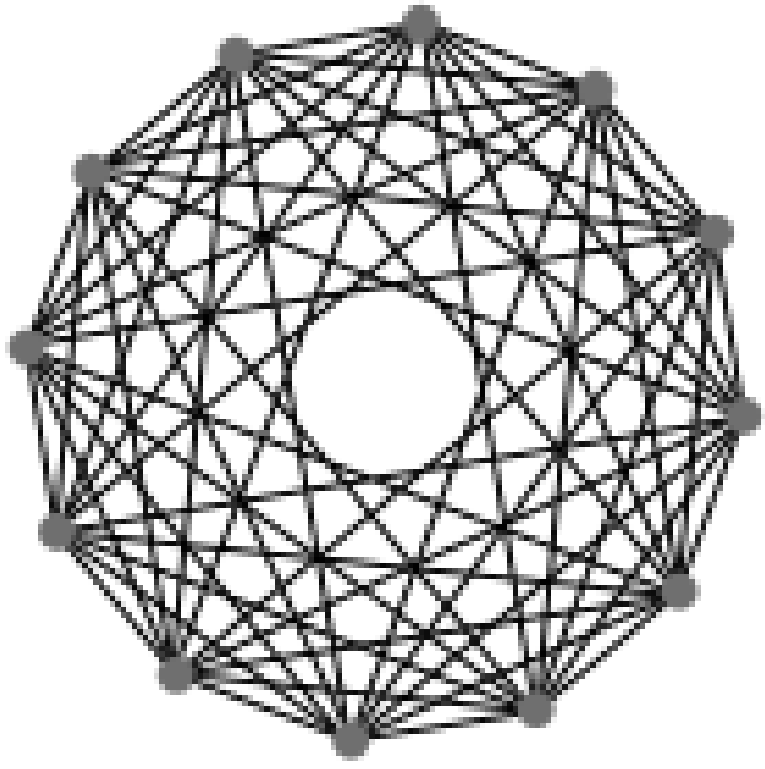
Attack: Epistemic



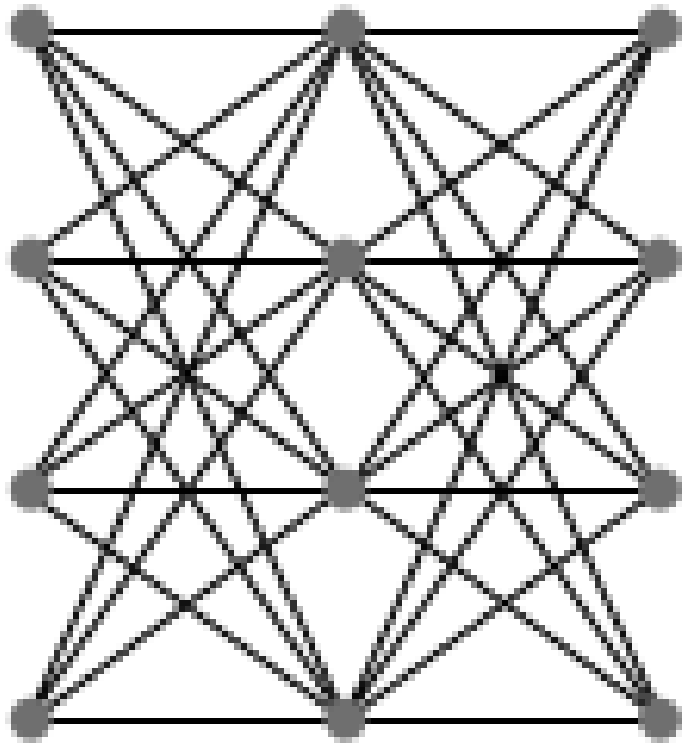
Topology: Cascade



Topology: Free route

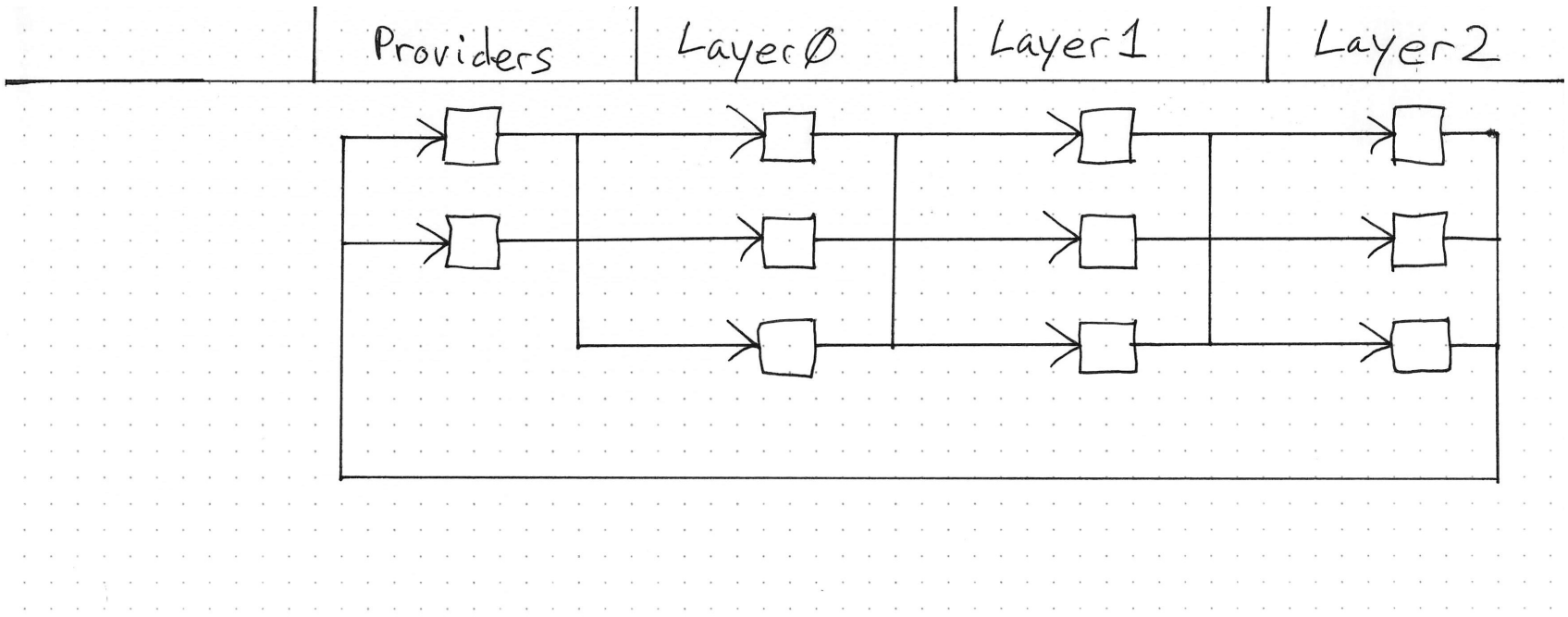


Topology: Stratified



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

Topology: Stratified



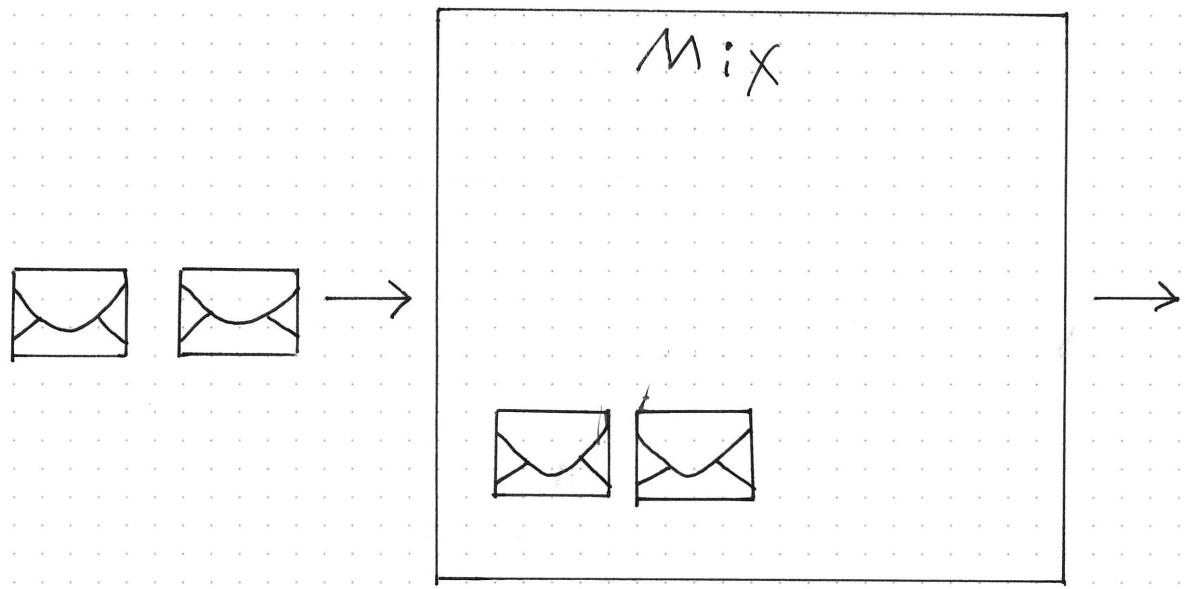
Isn't this just Tor?

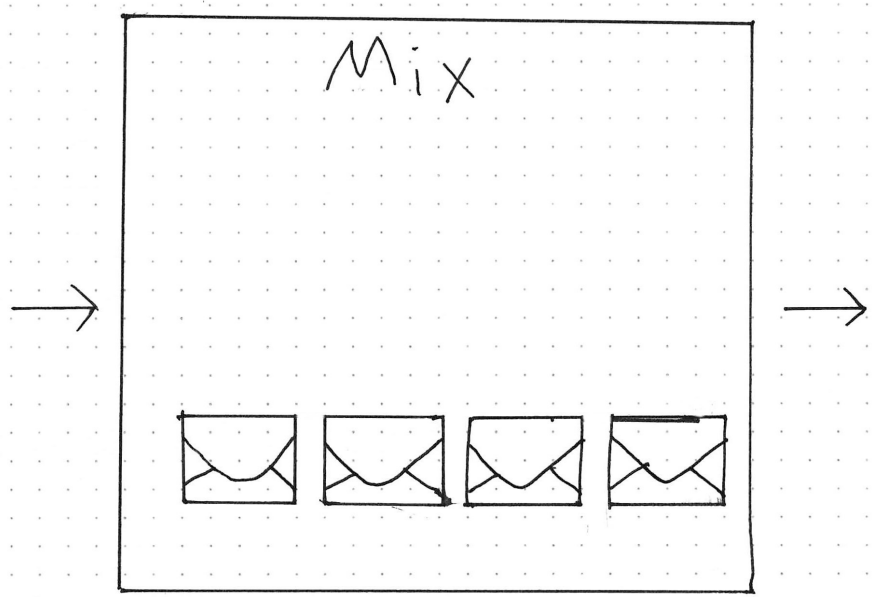
No: Onion routers provde cryptographic unlinkability, ..
but they do not mix!

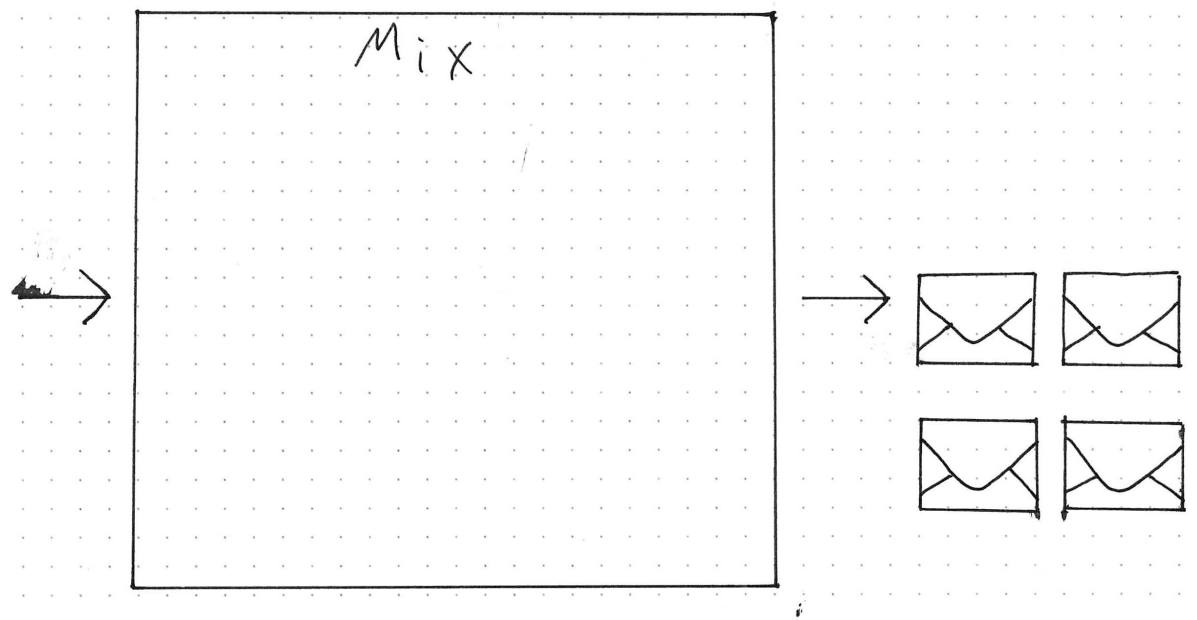
Mix strategies delay packets to reduce correlation between incoming and outgoing packets.. adding *latency*.

See:

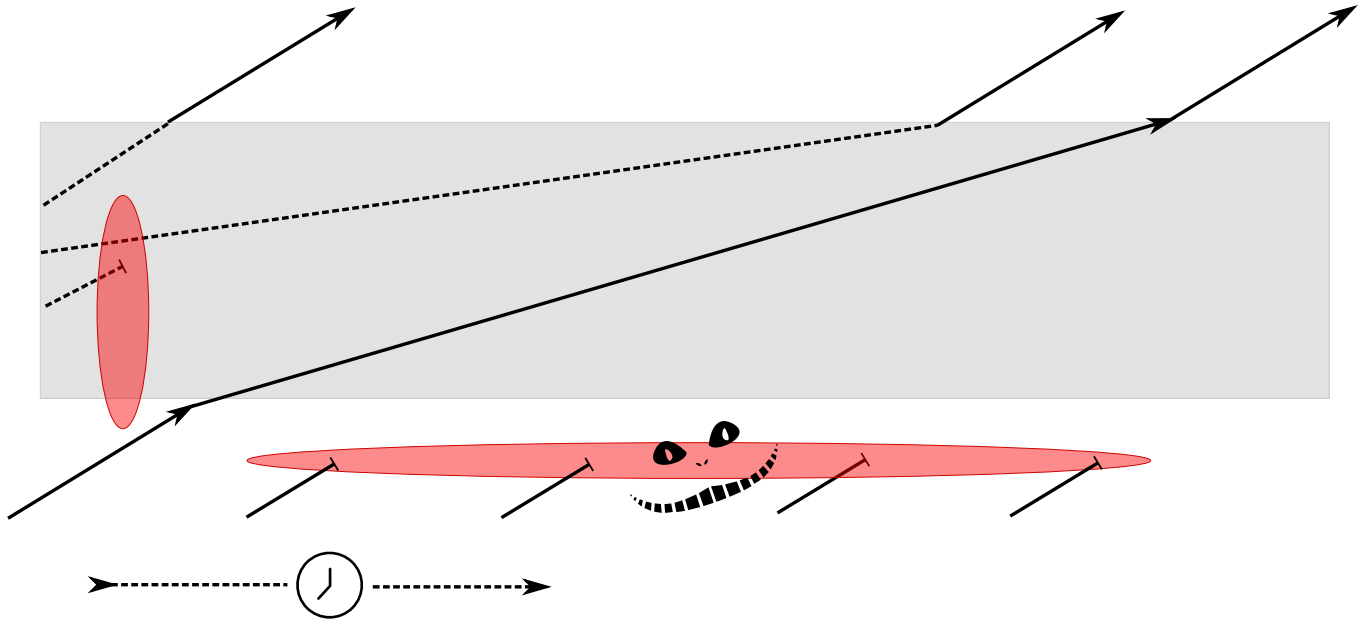
Claudia Diaz & Andrei Serjantov. *Generalising Mixes.* PET 2003


Mix

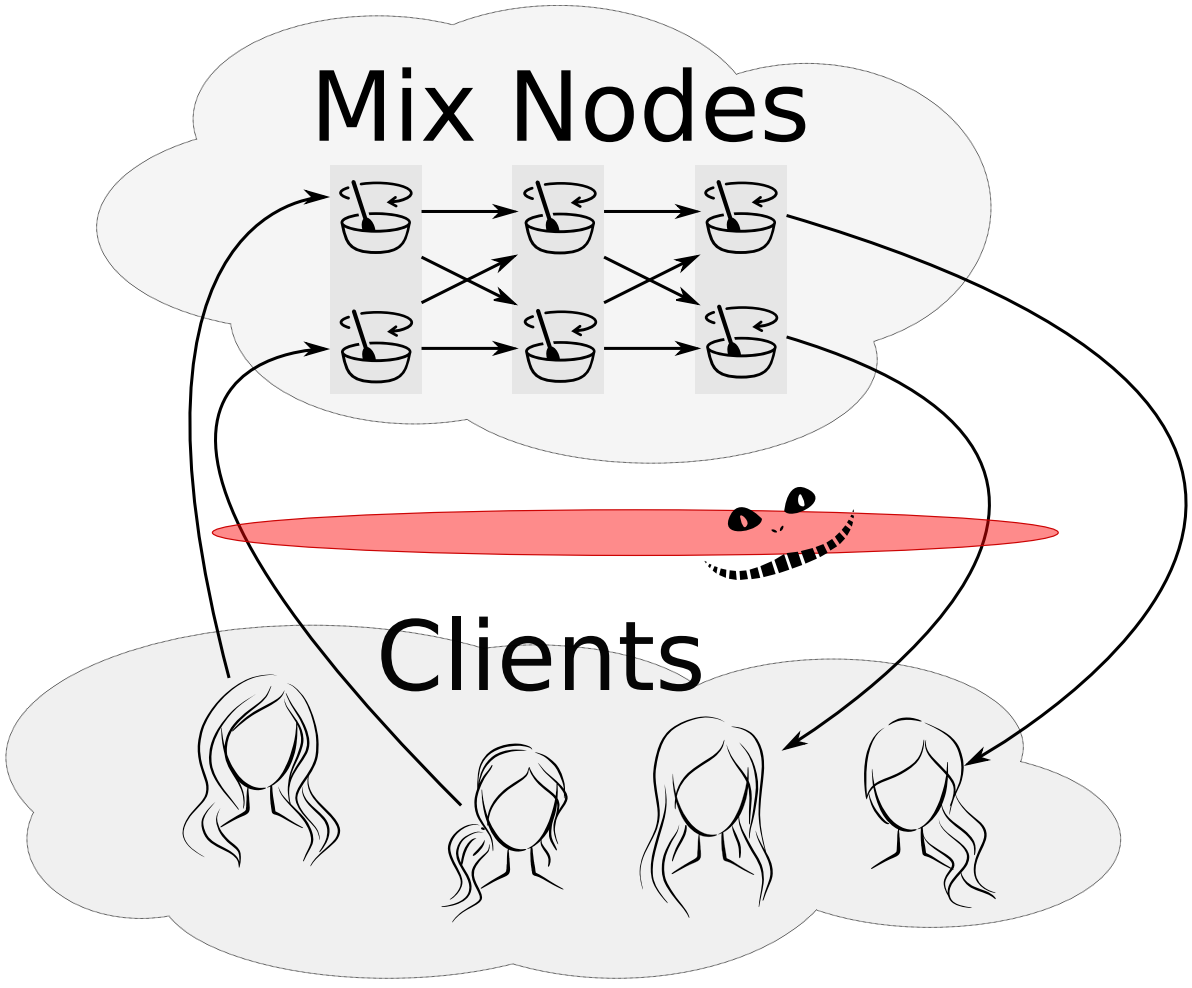

Mix


Mix

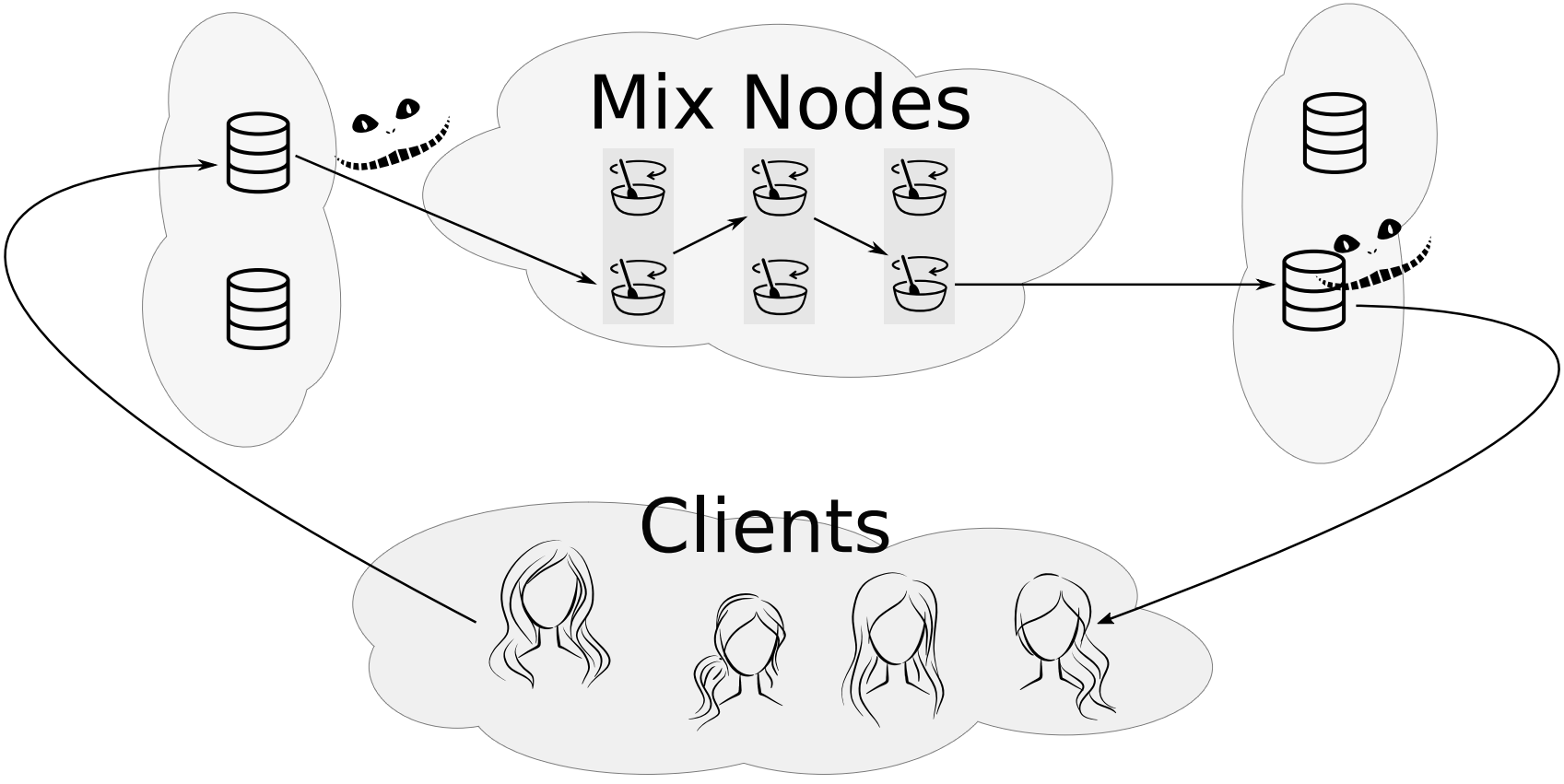
Attack: Blending aka n-1



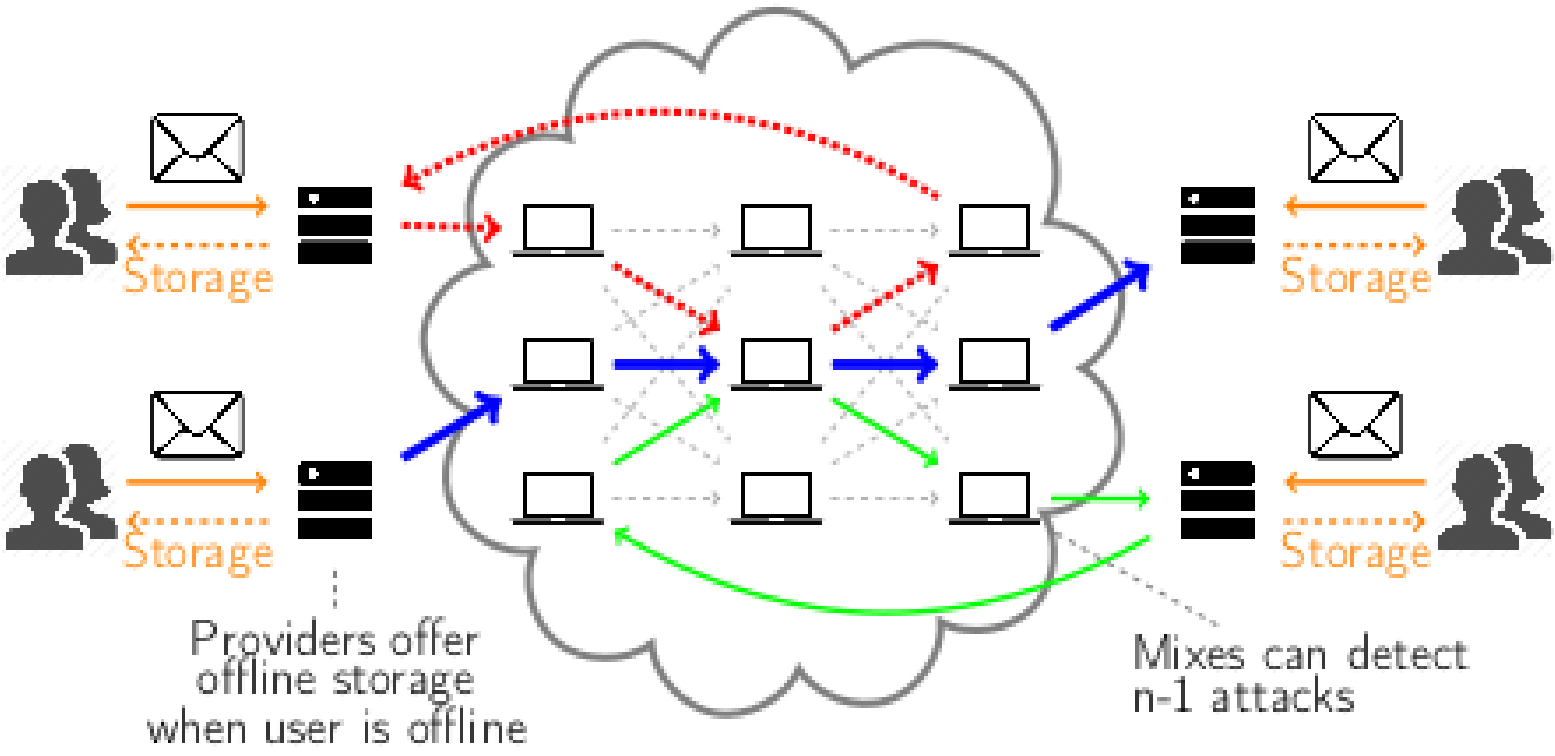
Attack: Statistical disclosure



Attack: Statistical disclosure

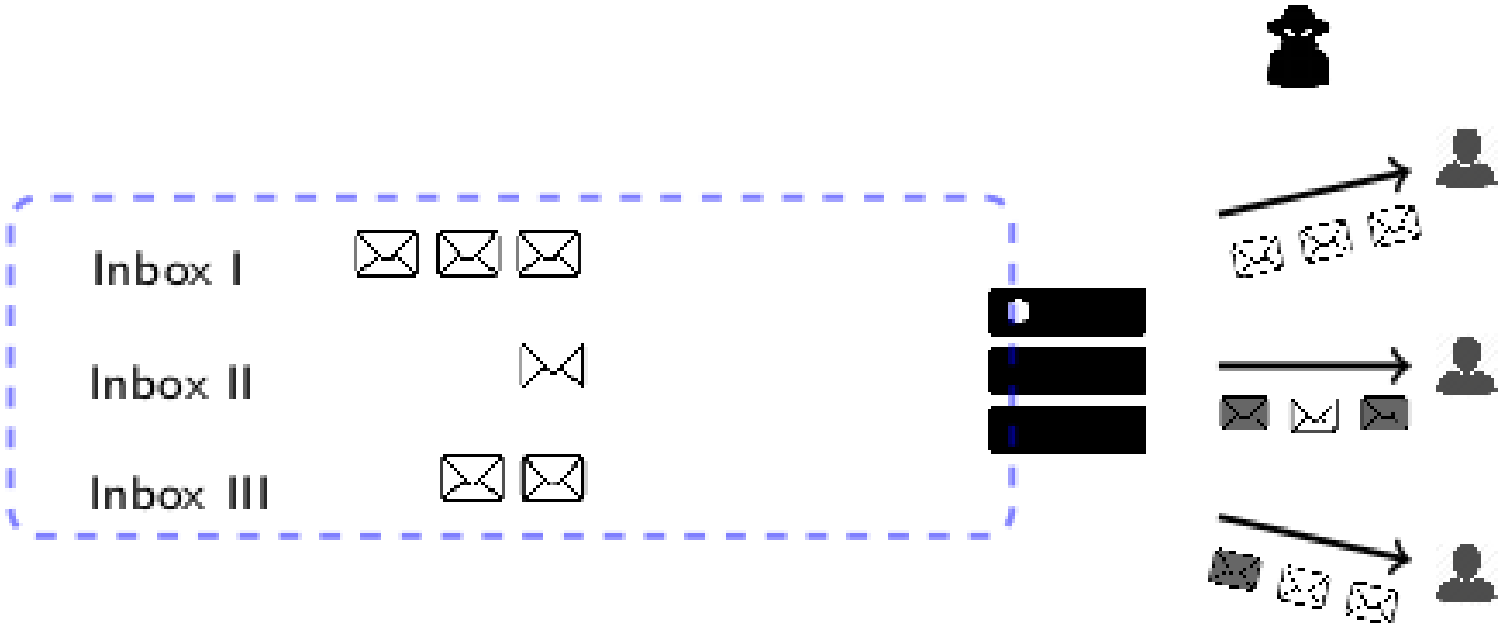


Loopix Achitecture



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

Loopix Provider to Client traffic padding



Anonymity Trilemma (Das, Meiser, Mohammadi, Kate (2017))

Anonymity cannot scale better than $|\text{cover traffic}| \cdot |\text{latency}|$

Take aways:

Tor's situation: $|\text{cover traffic}| * 0 = 0$

Anonymity cost still looks quadratic too.. *but not in users.* –

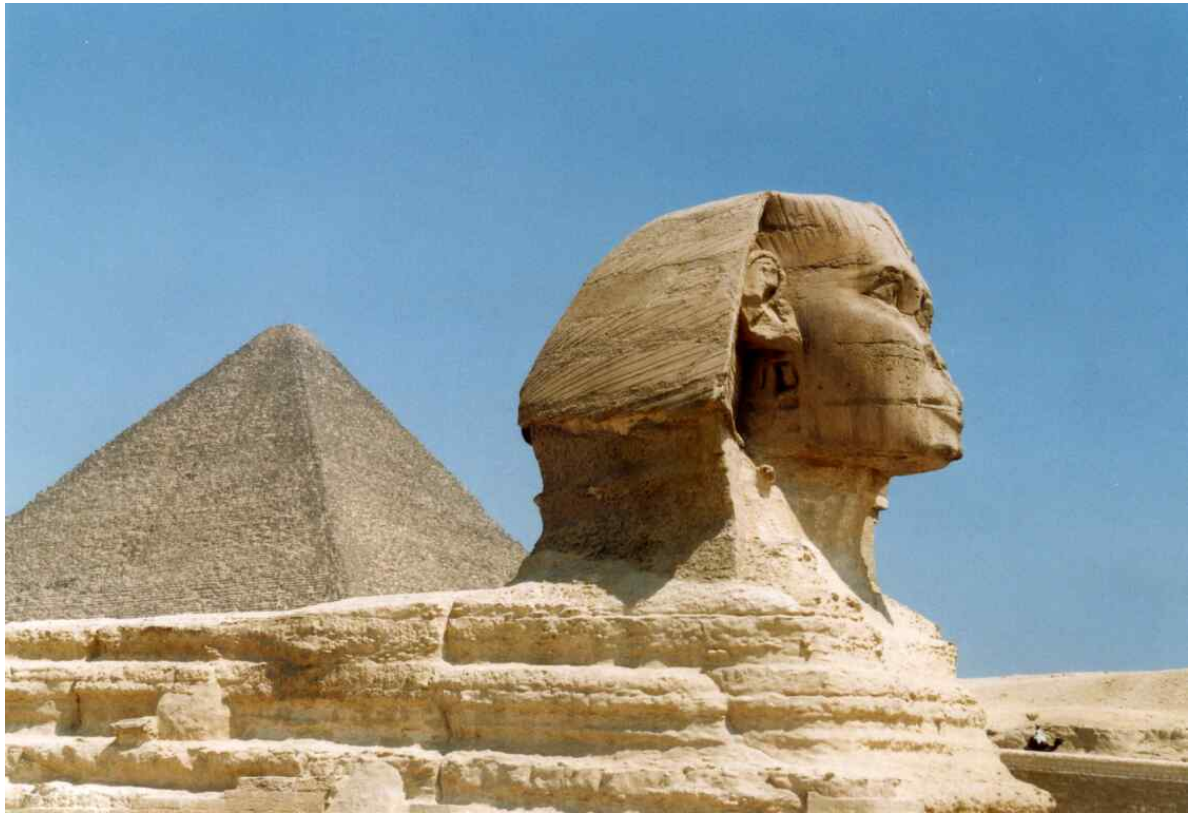
"The universe believes in encryption"

–Julian Assange (2012)

Encryption is free, but you must pay for anonymity.

Don't roll your own packet format!

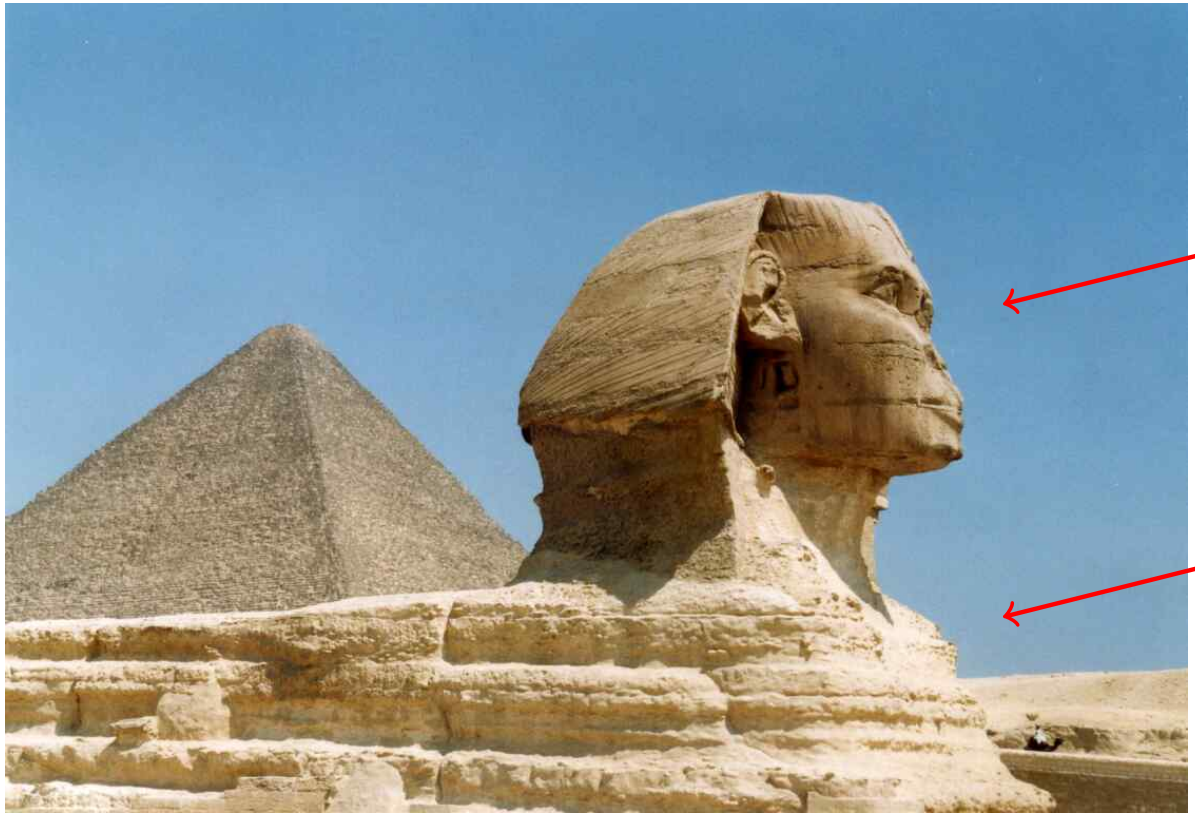
Sphinx is a remarkably compact and secure packet format designed by George Danezis and Ian Goldberg.



Security proof in the universal composability model,
using on 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.

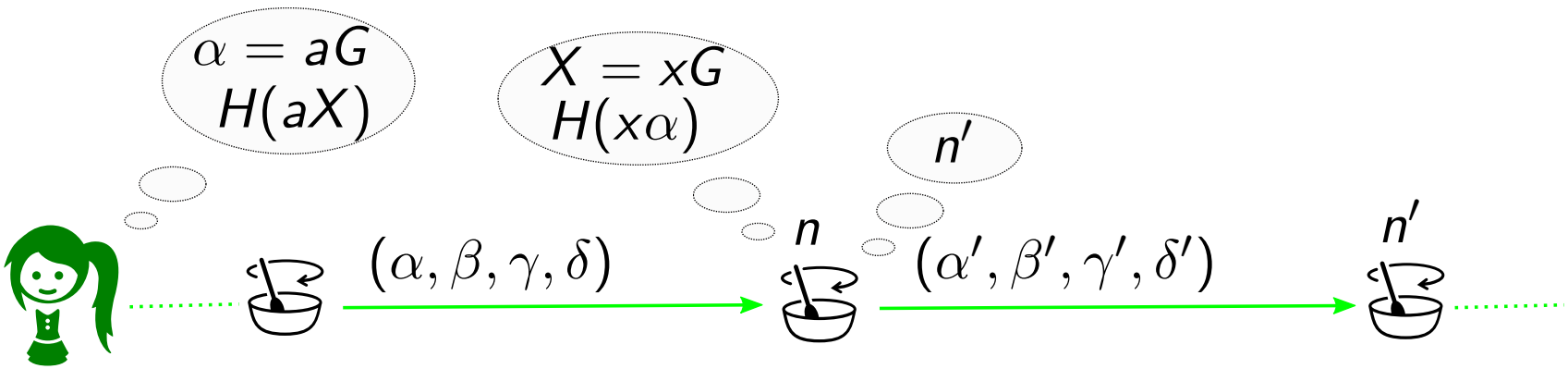


Security proof in the universal composability model, using on earlier work by Camenisch & Lysyanskaya 2005.

A Sphinx packet is a tuple $(\alpha, \beta, \gamma, \delta)$ where

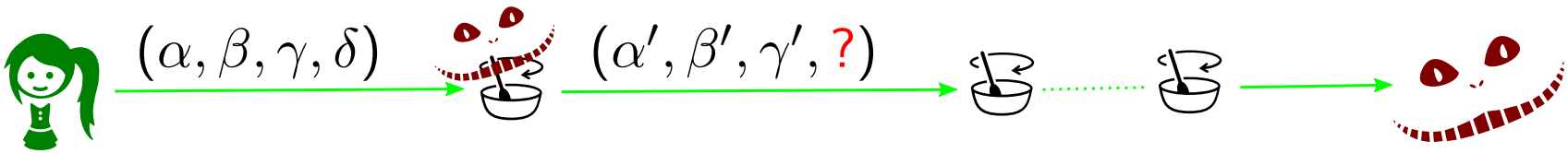
α is an elliptic curve point,
β is routing data onion encrypted with a stream cipher,
γ is a MAC for β, and
} header

δ is the packet body onion encrypted with a wide-block cipher.



Attack: Tagging

Question: Why is the body δ not MACed?



An unMACed stream cipher is dangerous

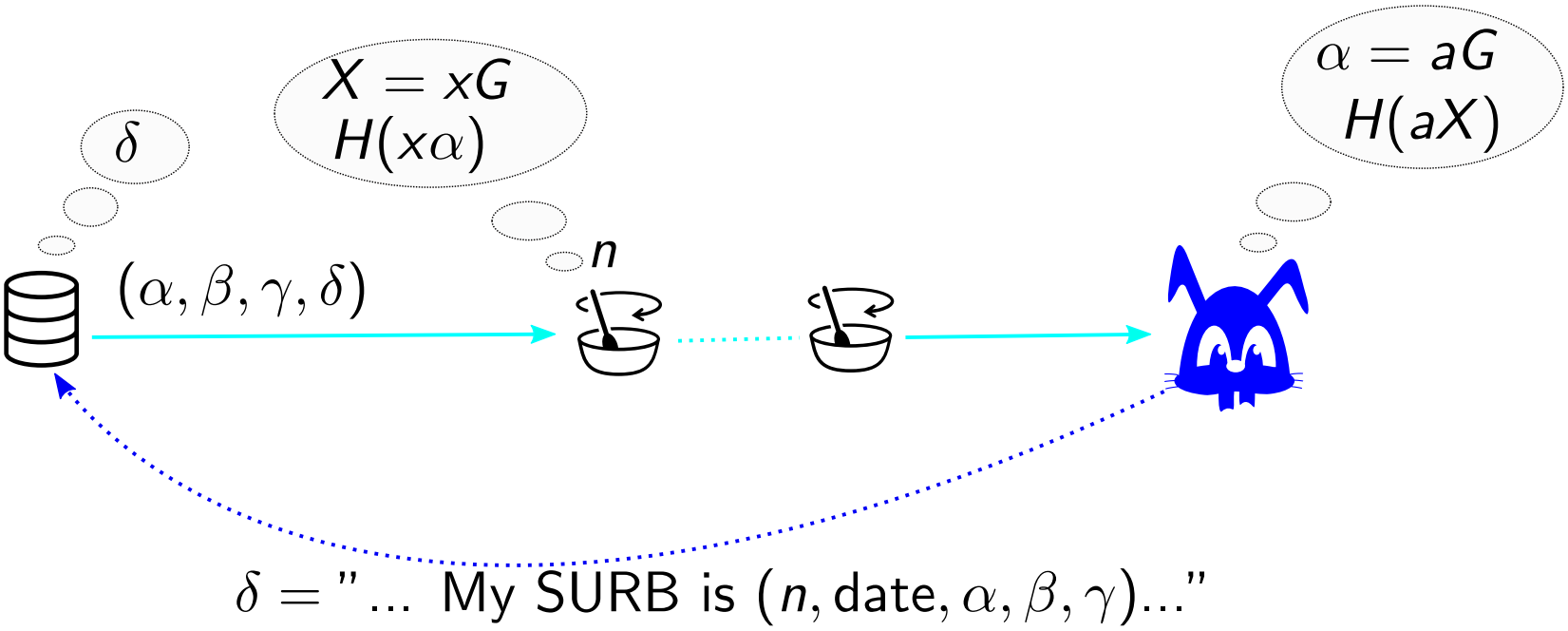
$$? = \delta' \oplus \text{"}\texttt{Hello Eve, This is Alice's message.}\text{"}$$

but a wide-block cipher admits only a fractional bit *tagging attack*

Single-use Reply Blocks (SURBs)

Anonymous receivers matter:

- Journalistic sources
- Services: CENO, money, etc.
- Protocol ACKs!



Attack: Compromise

We want protocols to be forward-secure, aka have key erasure.

Problem: α is ephemeral, but the node's key X is not! Uh oh!

Idea 1: Replay attacks necessitate a Bloom filter,
which necessitates key rotation.. so rotate faster?

Meh. Don't stress the PKI.
SURB lifetime = Node key lifetime

Can we do better?

Attack: Compromise

We want protocols to be forward-secure, aka have key erasure.

Problem: α is ephemeral, but the node's key X is not! Uh oh!

Idea 1: Replay attacks necessitate a Bloom filter,
which necessitates key rotation.. so rotate faster?

Meh. Don't stress the PKI.
SURB lifetime = Node key lifetime

Idea 2: Tor is forward-secure..
so use more packets but not like Tor?

George Danezis (2003): Use packets in different key epochs.

Jeff: First use a loop to get an answer.. and then double ratchet.

Meh. This is cheating. Not all hops.

Sphinx' opinions on key exchanges

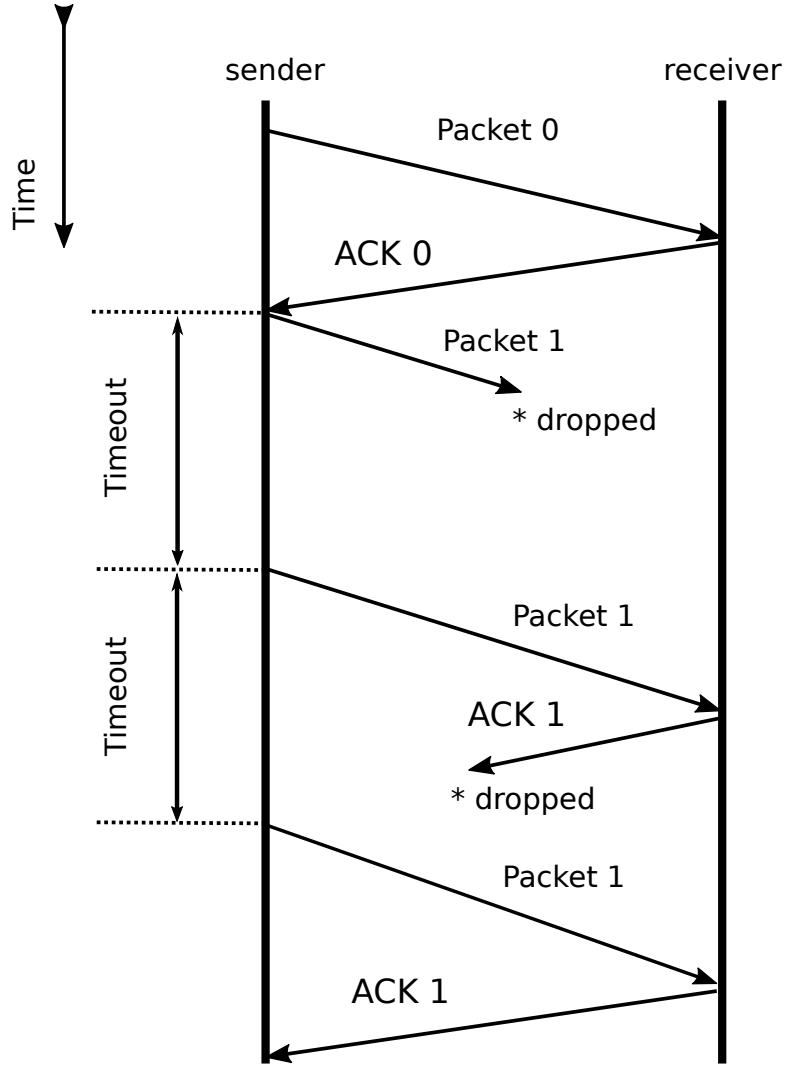
	Long-term keys	Blinding	Key erasure	Post-quantum	Hybrid PQ	Performance
ECC	✓	✓		✗		good
Pairing	✓	✓	$\Rightarrow$	✗		$O(\lvert\text{packets}\rvert)$
LWE	✓	?	?	✓	✗	elephant
SIDH	?	✓	?	✓	✗	snail
cheat	✓	✓	$\Leftrightarrow$	✓	✓	good

FS PQ Sphinx Conjecture

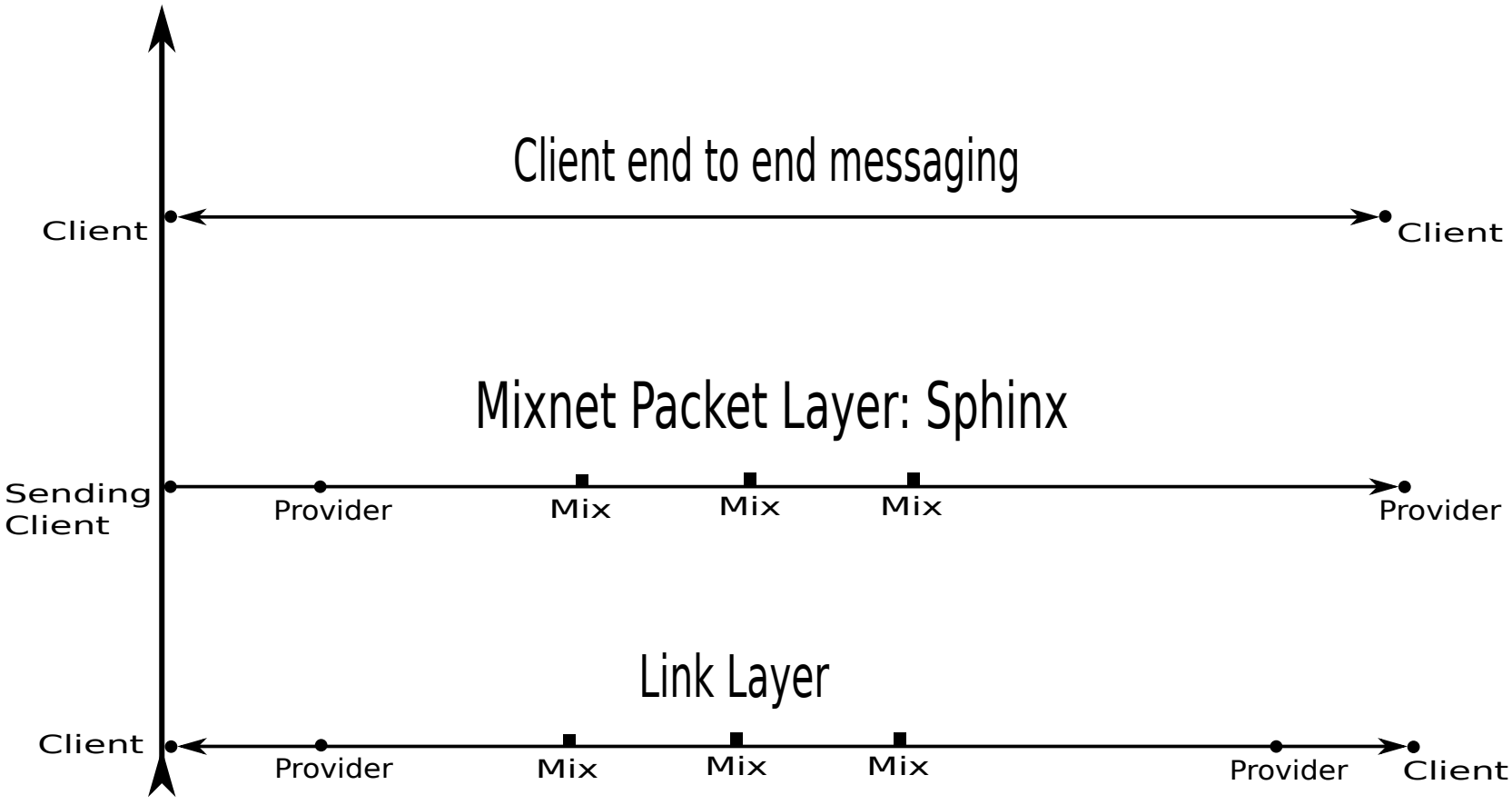
There is a fast-ish efficient LWE key exchange with fast efficient blinding and punctures, but no scheme with hybrid blinding.

The case of the lost packet

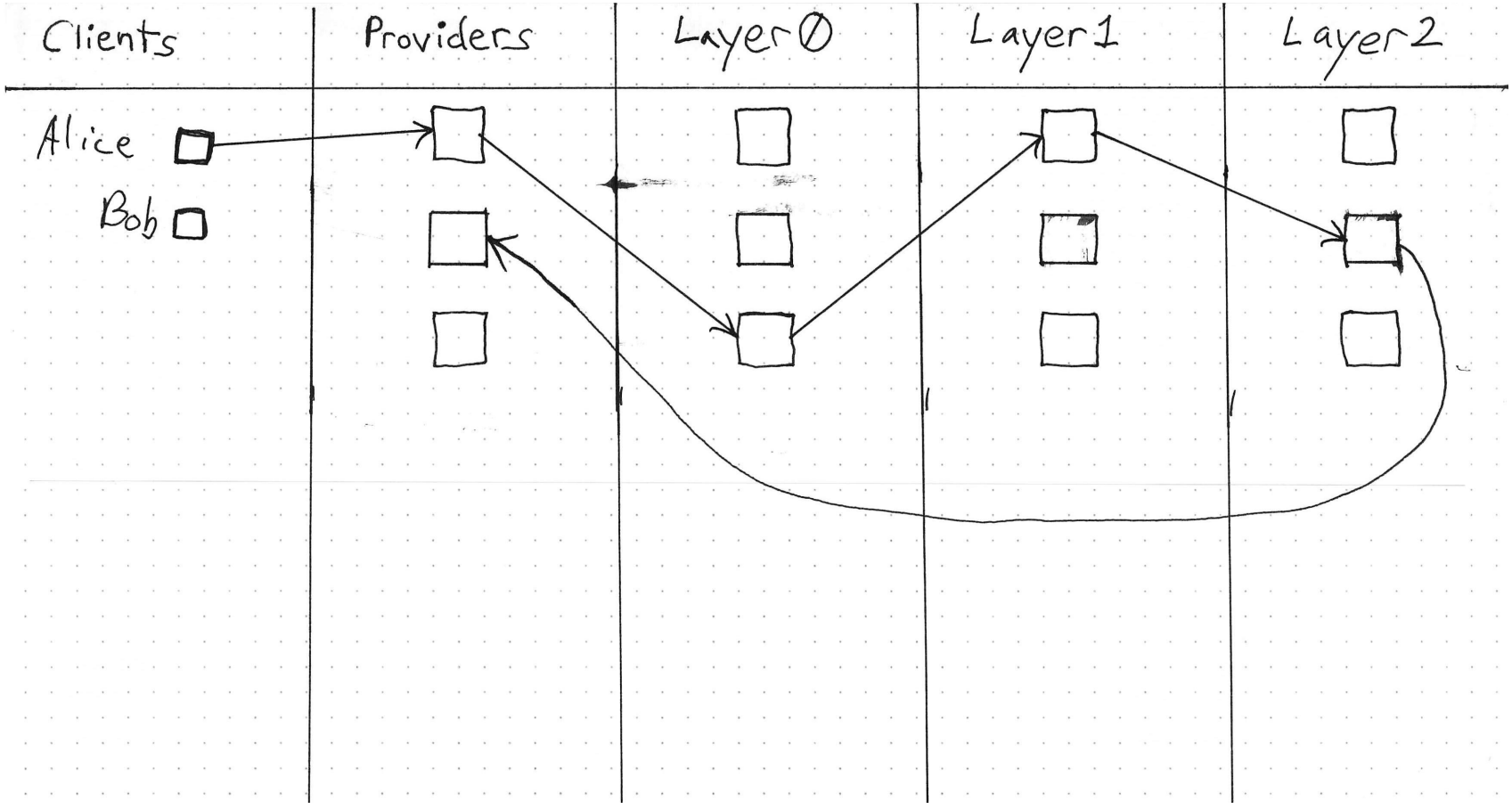
The case of the lost ACK



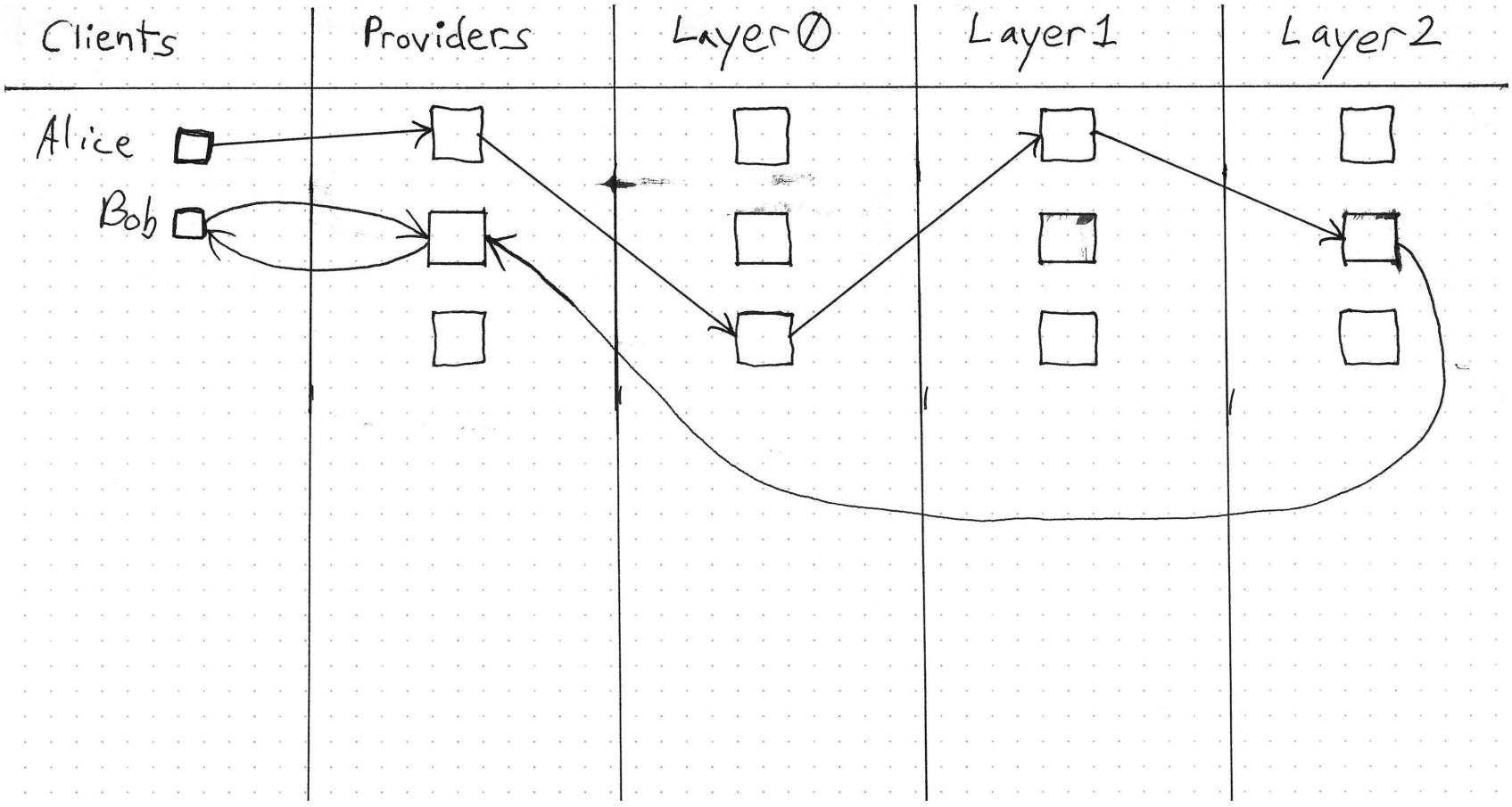
Katzenpost: crypto layers



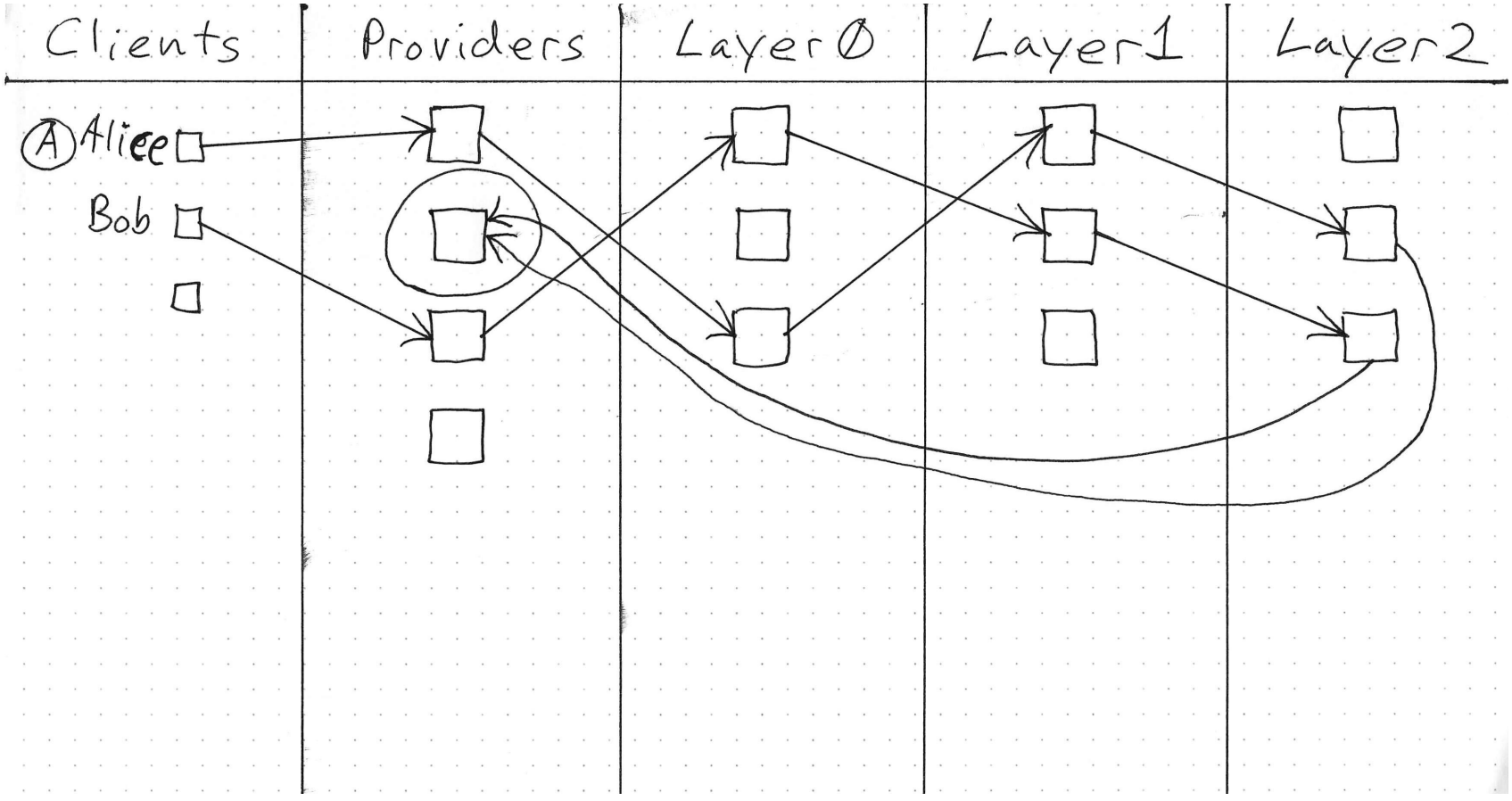
Loopix: Alice sends a message to Bob



Loopix: Bob retreives message from his Provider.

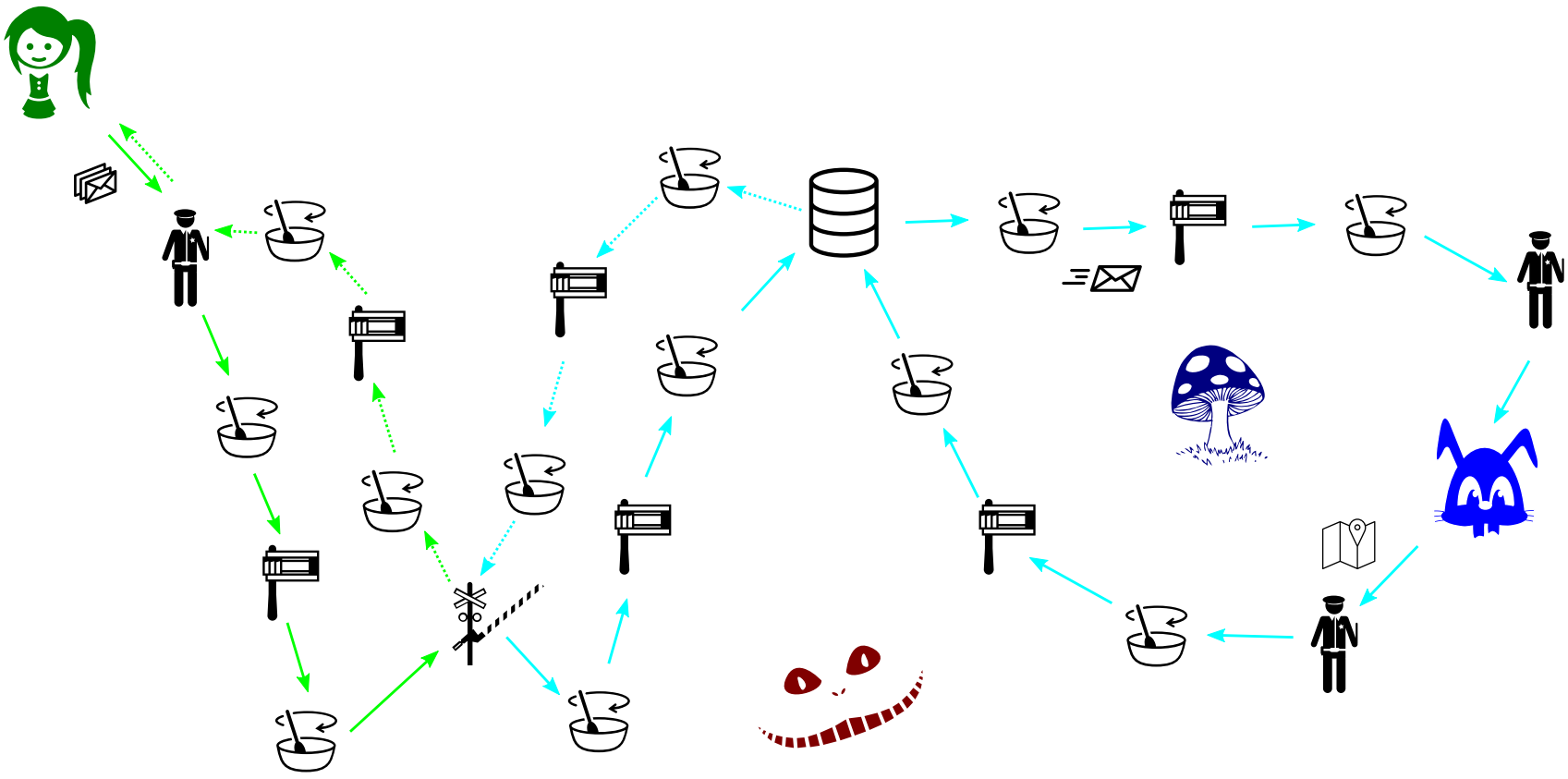


Stronger location hiding properties.



Lake Proposal

Can both sender and receiver be protected by the mixnet? Yes!



Application: Money

Taler's RSA blind signatures have information theoretically secure blinding.

Zcash requires at least inverting hash functions

Application: Web-ish

Application: Relax!

We want to design applications so that
users experience the latency as a benefit..
as productive disengagement.

"Work at a different speed" –Brian Eno, Oblique Strategies (1974)

Thanks to the following people:

Yawning Angel
George Danezis
Claudia Diaz
Christian Grothoff
Ania Piotrowska

Katzenpost project page:

design docs, specifications and mailing lists
https://katzenpost.mixnetworks.org/