Artifact Evaluated
NDSS SYMPOSIUM
Available
Functional
Reproduced

LAMP: Lightweight Approaches for Latency Minimization in Mixnets with Practical Deployment Considerations

Mahdi Rahimi, Piyush Kumar Sharma and Claudia Diaz

mahdi.rahimi@kuleuven.be

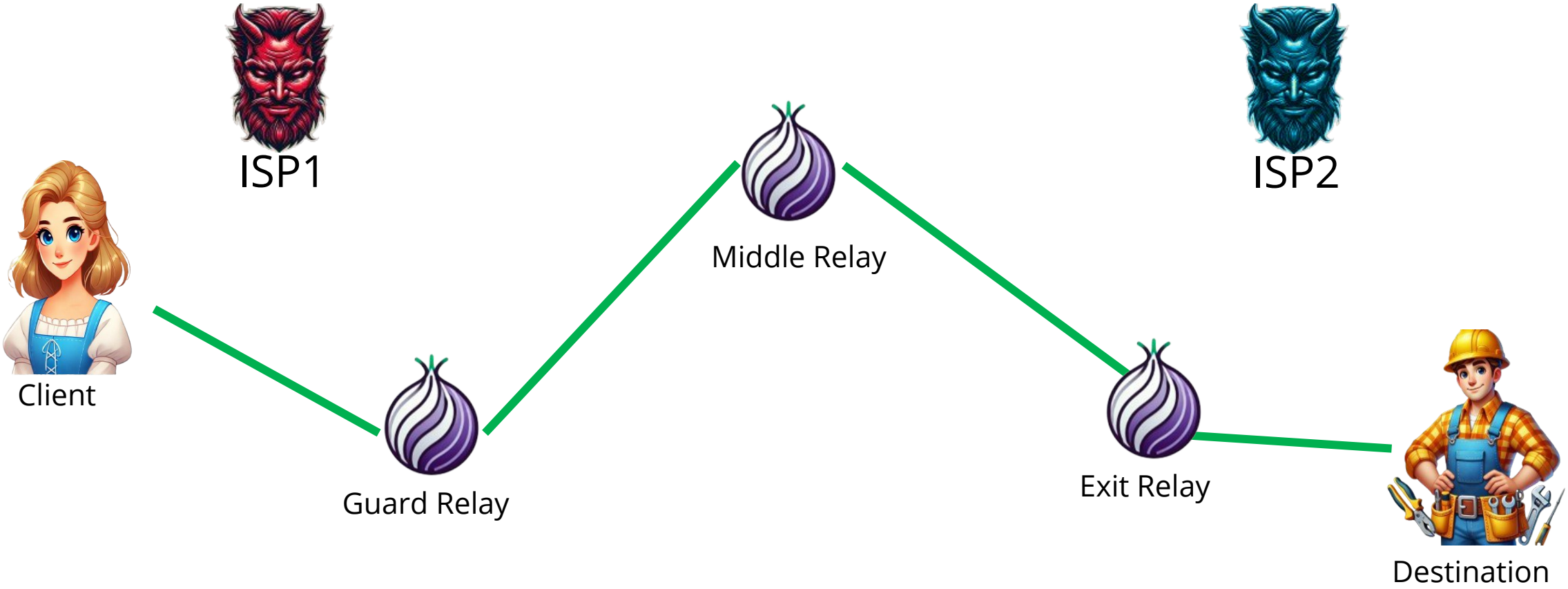
COSIC, KU Leuven, Belgium

NDSS SYMPOSIUM
32nd the Network and Distributed System Security (NDSS) Symposium, 24th-28th February 2025, San Diego, California.

End users on the internet are not anonymized by default.

This creates privacy issues.

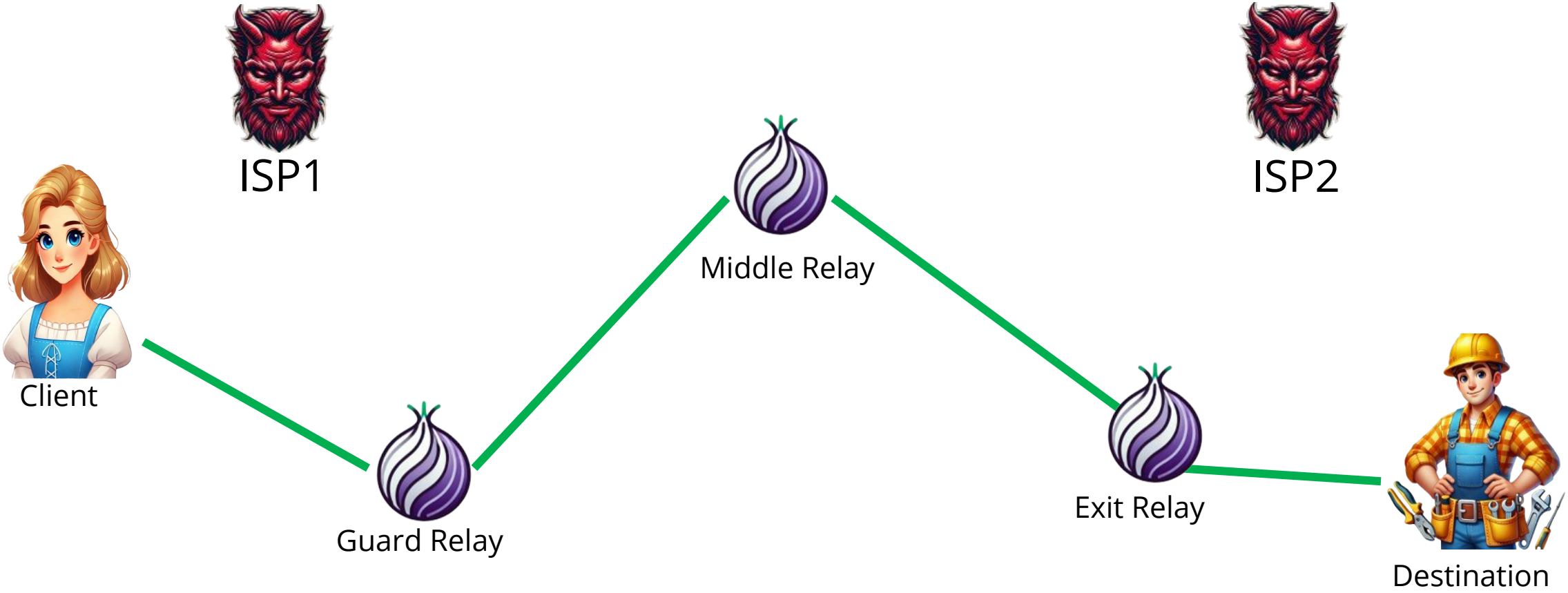
Tor Network



ISP: Internet Service Provider.

ISP1 does not collude with ISP2.

End-to-End Correlation Attacks

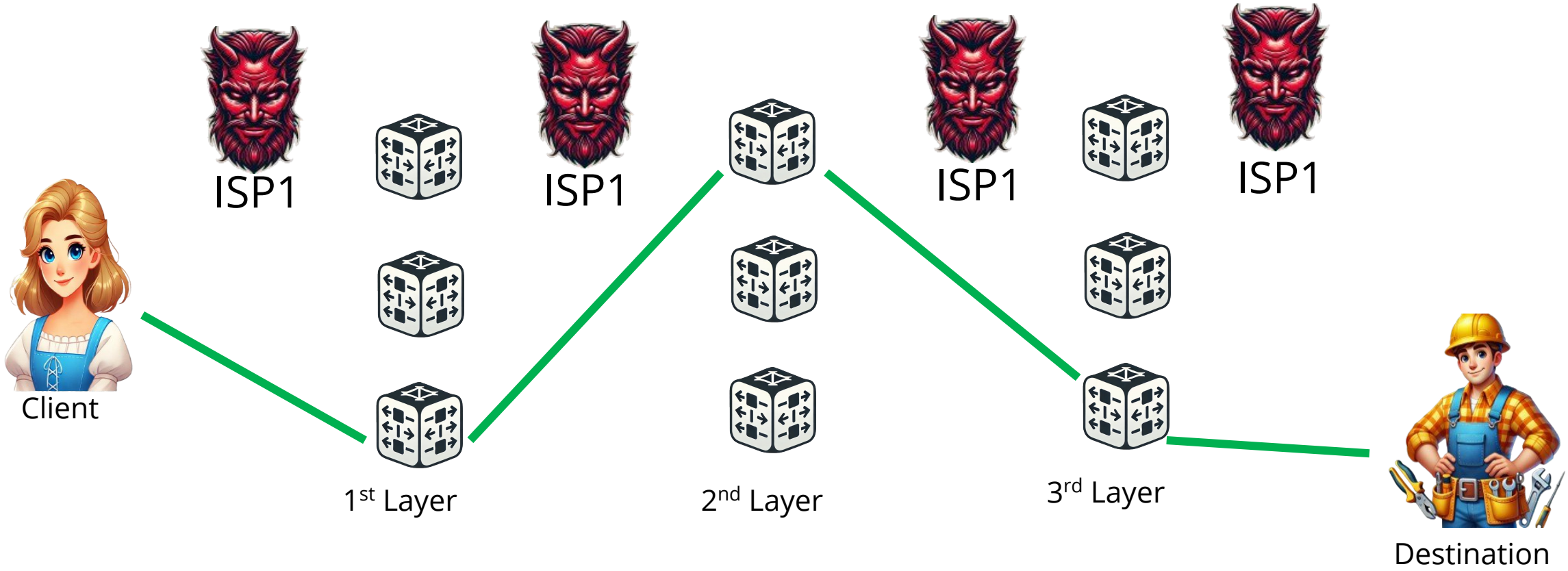


If ISP1 colludes with ISP2, they can deanonymize the client-destination connection.

To have strong tools to provide anonymity, we can consider using mixnodes.

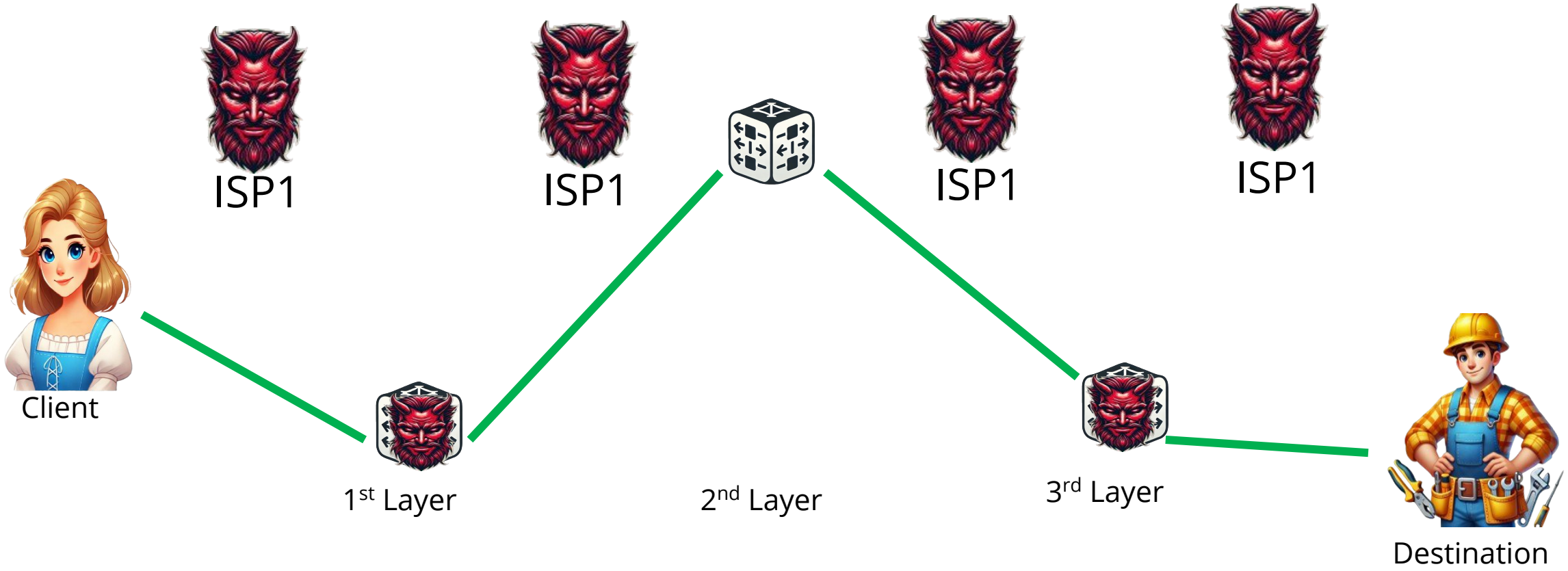
Mixnodes make their input and output unlinkable.

Mix Network(Mixnet)



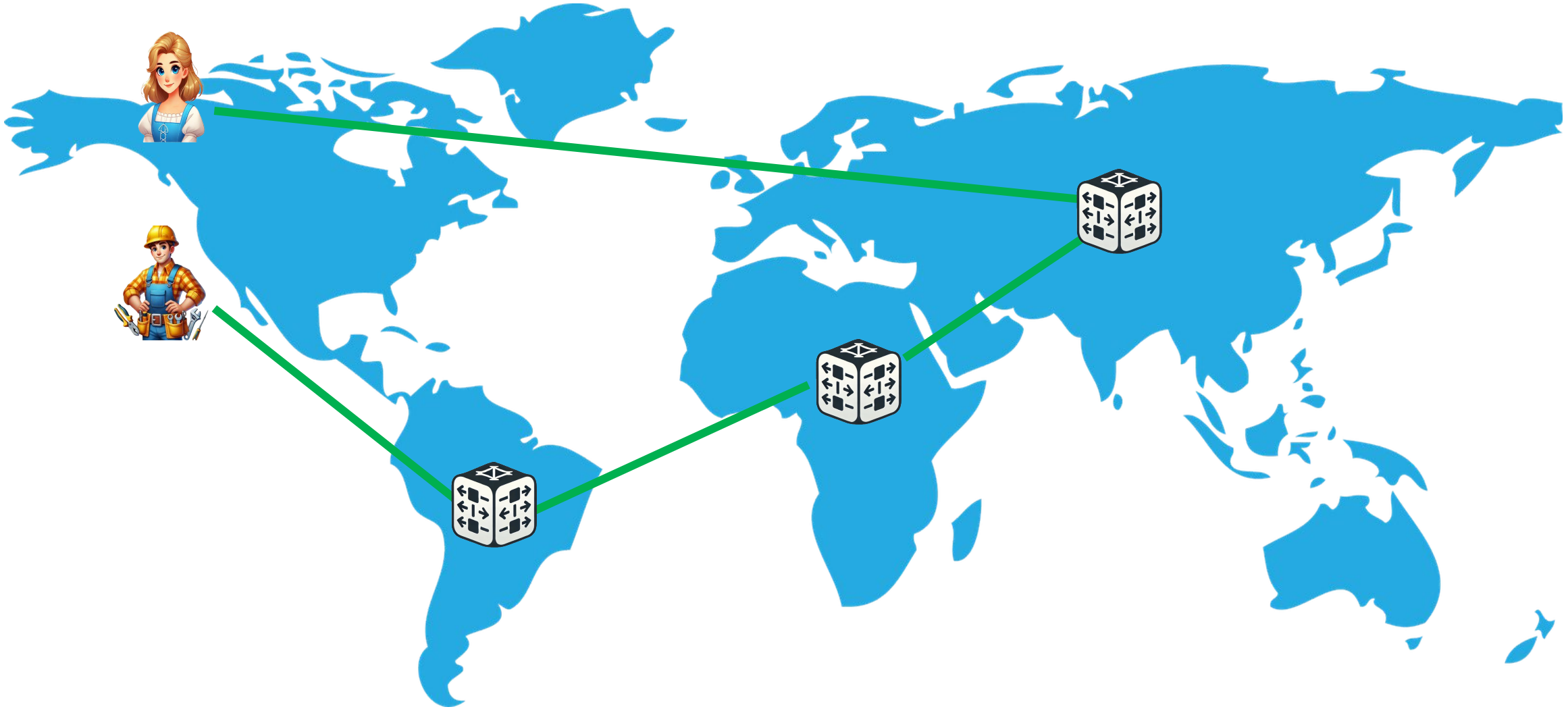
A mixnet is a network consisting of mixnodes, typically arranged in a layered format.

Anonymity Requirement



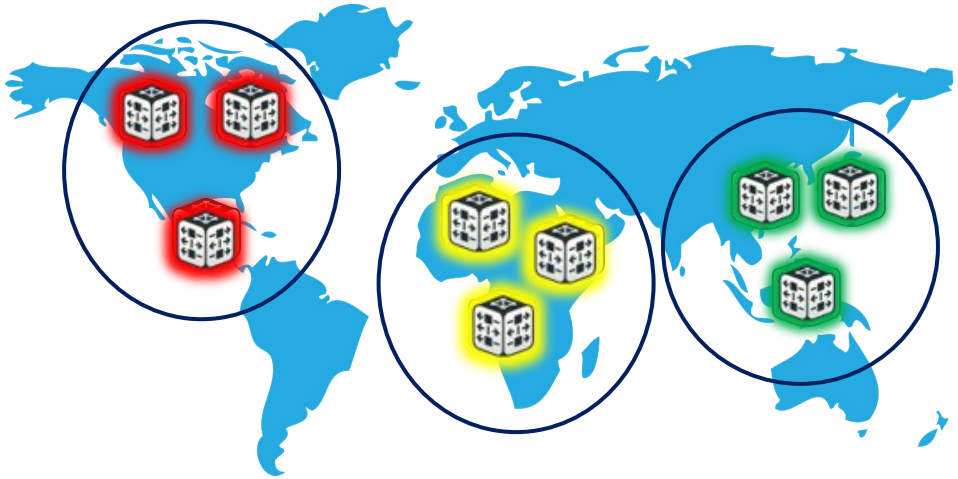
As long as one mixnode in the message route is honest, the client-destination connection will be anonymized.

End-to-End Latency



As a result of routing through intermediate mixnodes and intentional delays at each mixnode, the end-to-end latency is very high when using a mixnet.

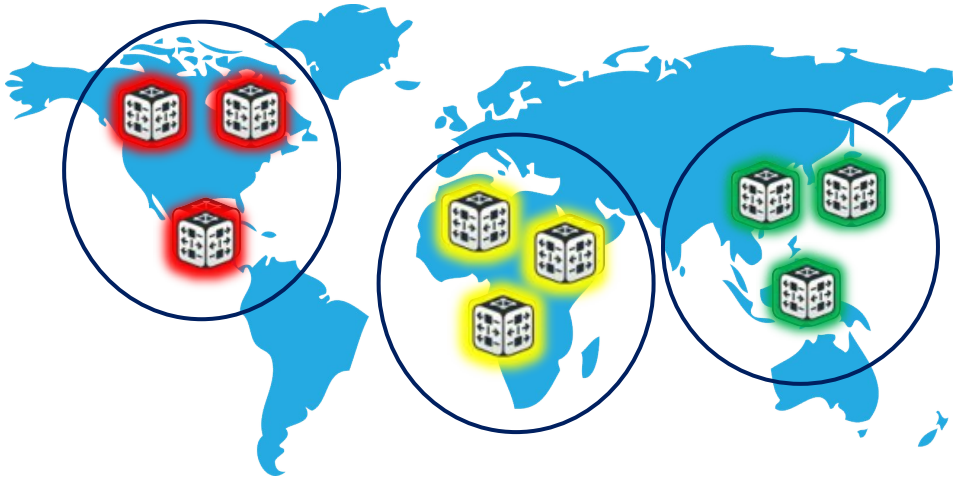
LARMix*



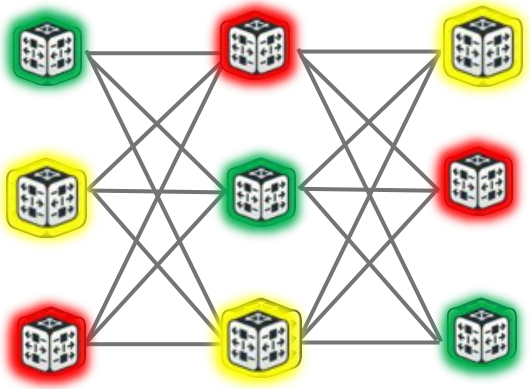
1) Clustering

*: **Mahdi Rahimi**, Piyush Kumar Sharma, and Claudia Diaz. "LARMix: Latency-Aware Routing in Mix Networks." NDSS, 2024.

LARMix*



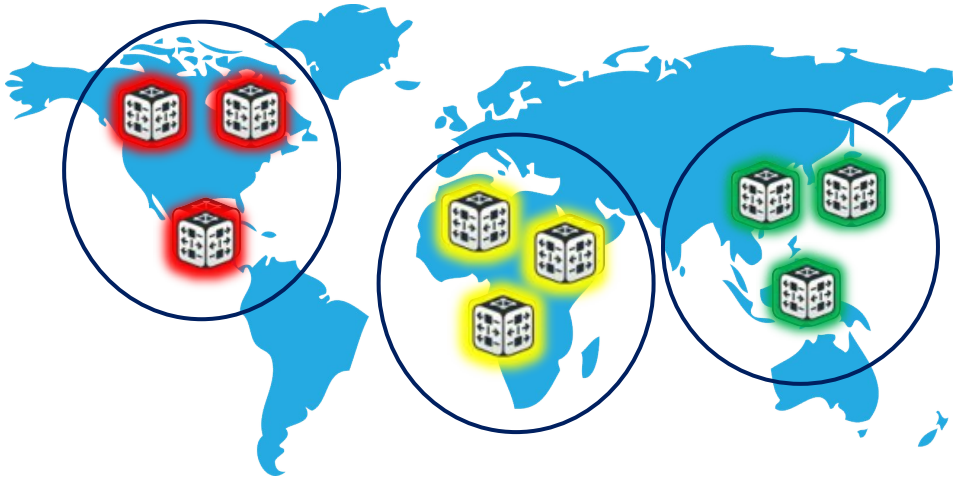
1) Clustering



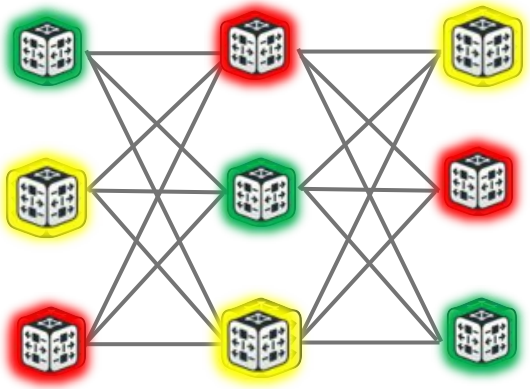
2) Diversification

*: **Mahdi Rahimi**, Piyush Kumar Sharma, and Claudia Diaz. "LARMix: Latency-Aware Routing in Mix Networks." NDSS, 2024.

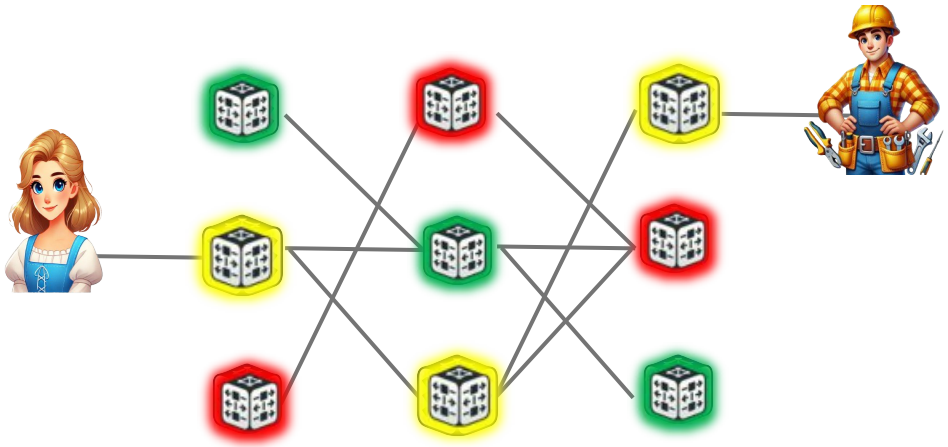
LARMix*



1) Clustering



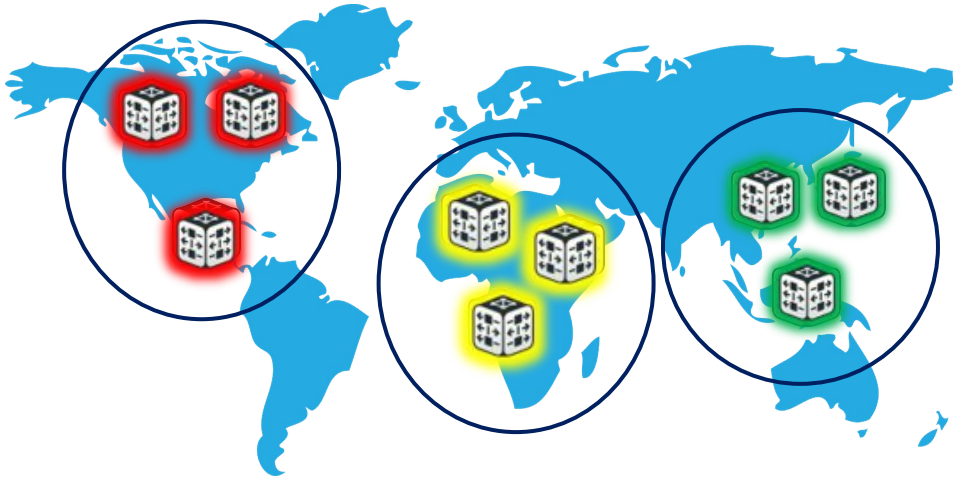
2) Diversification



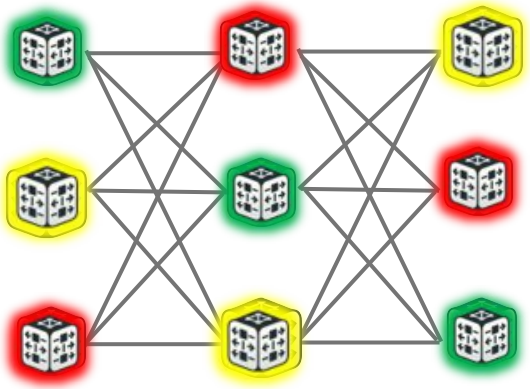
3) Low-latency routing

*: **Mahdi Rahimi**, Piyush Kumar Sharma, and Claudia Diaz. "LARMix: Latency-Aware Routing in Mix Networks." NDSS, 2024.

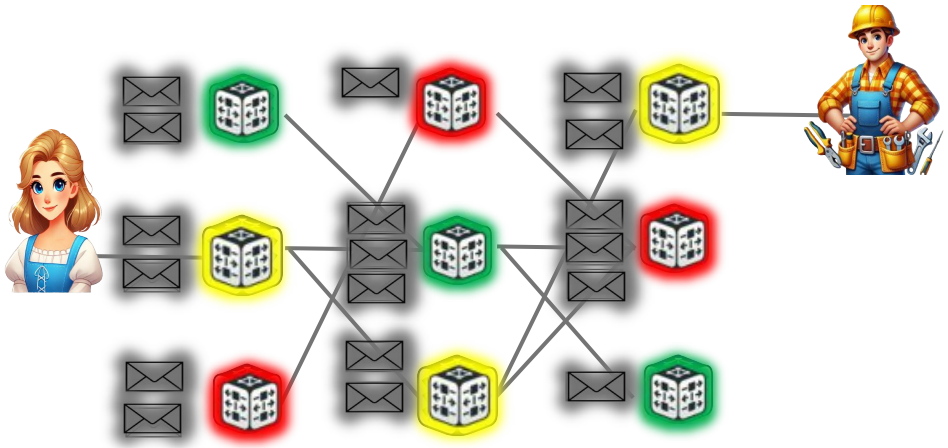
LARMix*



1) Clustering



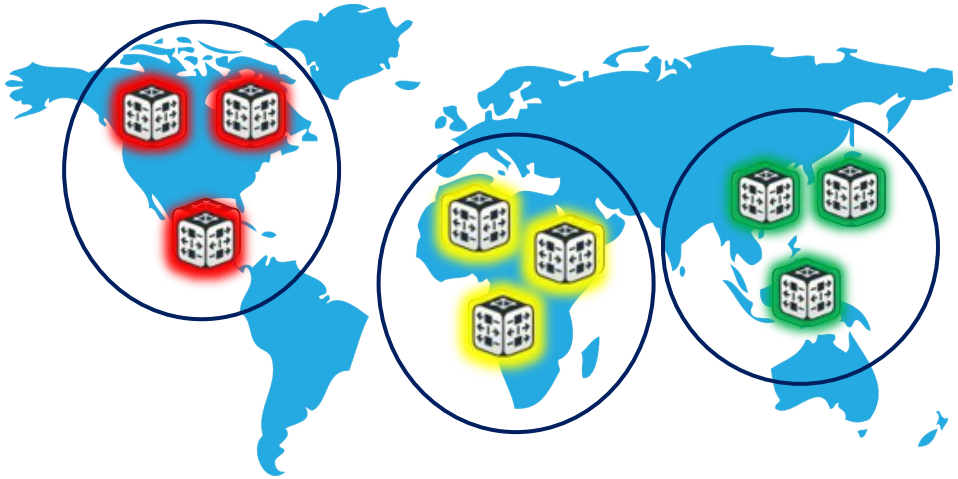
2) Diversification



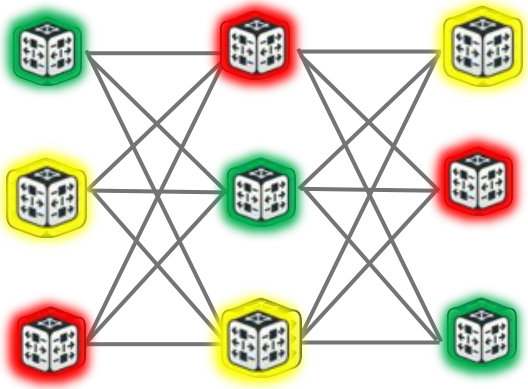
3) Low-latency routing

*: **Mahdi Rahimi**, Piyush Kumar Sharma, and Claudia Diaz. "LARMix: Latency-Aware Routing in Mix Networks." NDSS, 2024.

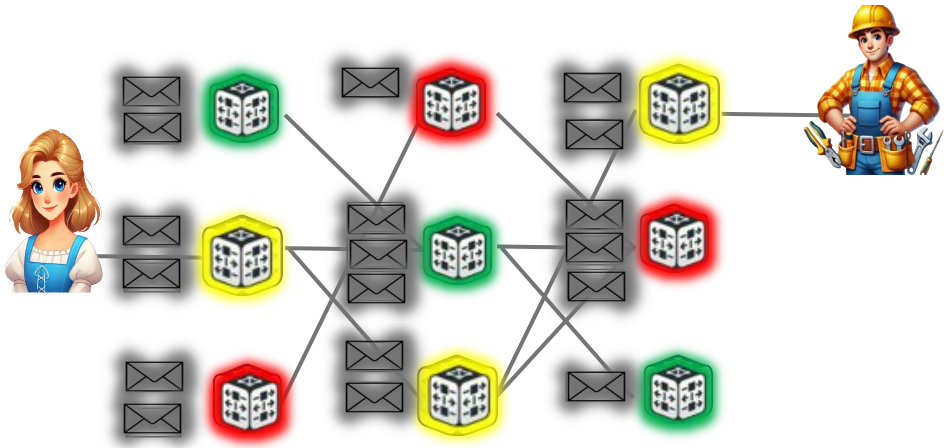
LARMix*



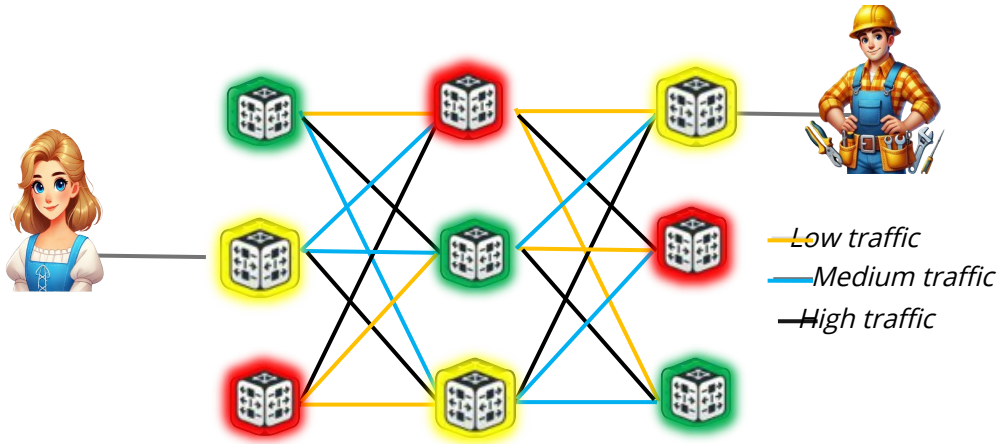
1) Clustering



2) Diversification



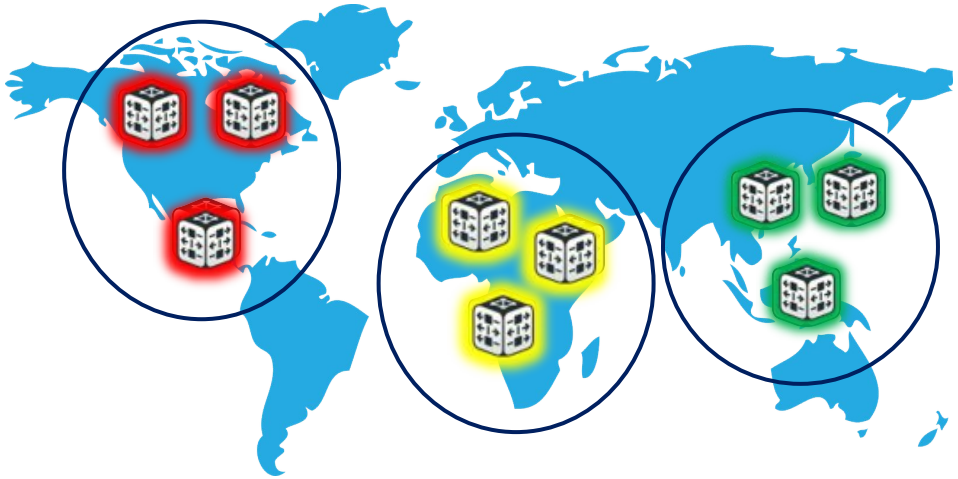
3) Low-latency routing



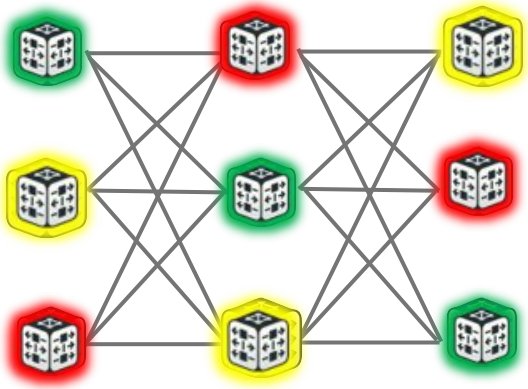
4) Load balancing

*: **Mahdi Rahimi**, Piyush Kumar Sharma, and Claudia Diaz. "LARMix: Latency-Aware Routing in Mix Networks." NDSS, 2024.

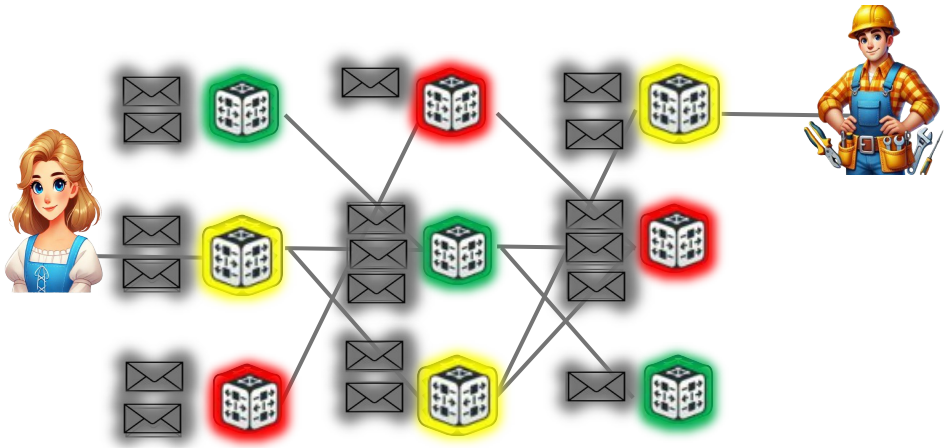
LARMix*



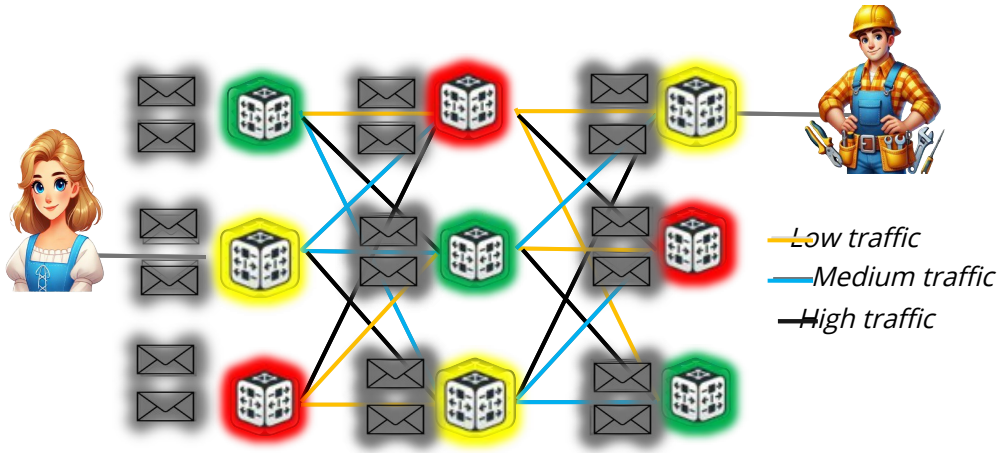
1) Clustering



2) Diversification



3) Low-latency routing



4) Load balancing

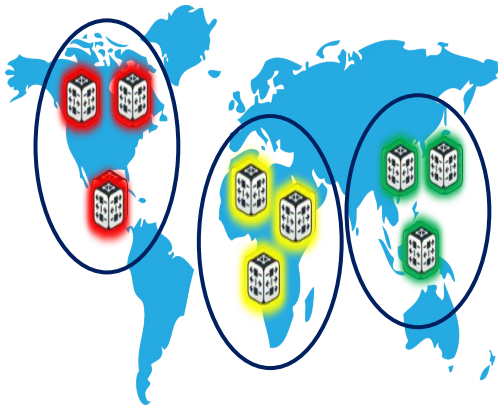
*: **Mahdi Rahimi**, Piyush Kumar Sharma, and Claudia Diaz. "LARMix: Latency-Aware Routing in Mix Networks." NDSS, 2024.

LARMix Inefficiency

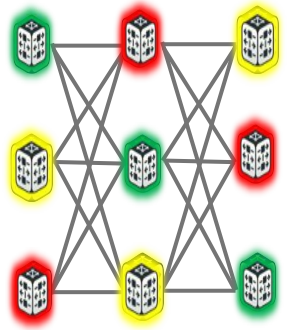
High Computational Cost ($O(N^5)$) due to node assignment and load balancing.

Naive Approach to Message Forwarding from clients, which may lead to inefficiencies

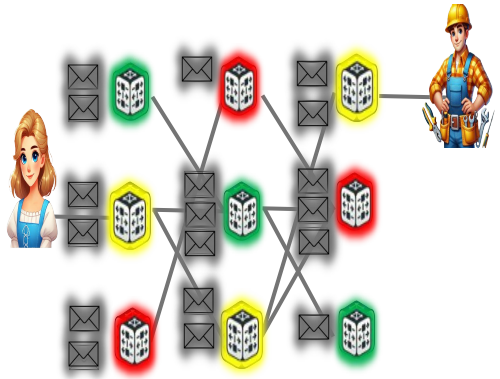
Can we do better?



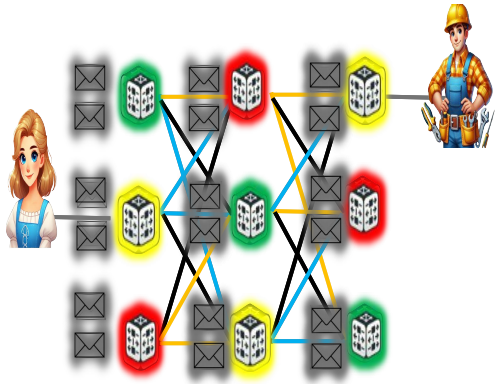
1) Clustering



2) Diversification

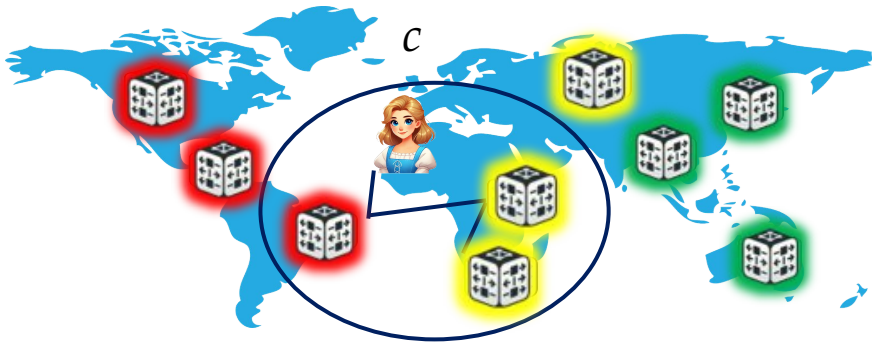


3) Low-latency routing



4) Load balancing

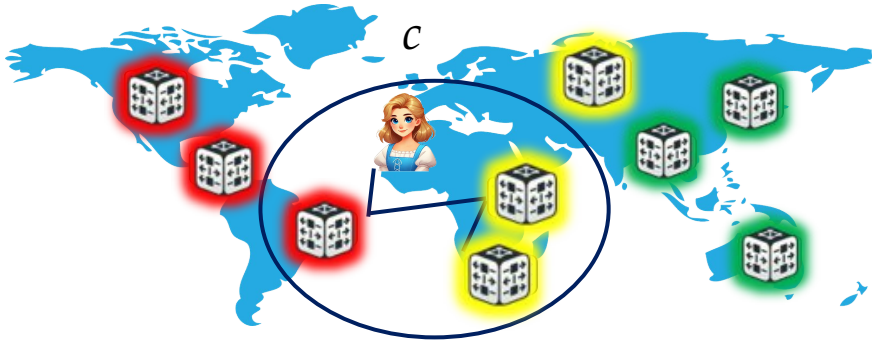
LAMP



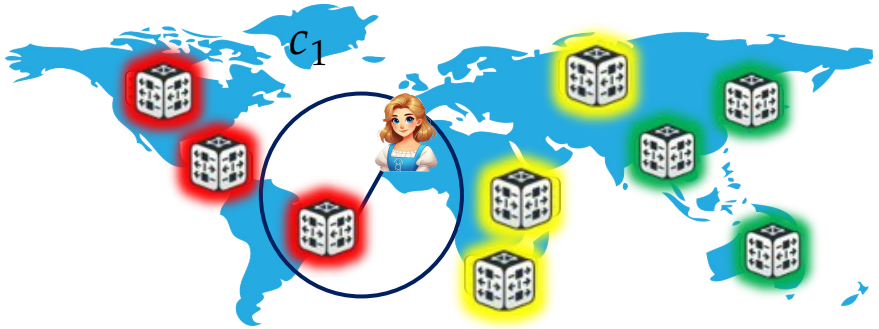
Single Circle (SC):
1- Super effcient approach
2- Moderate low-latency links

LAMP, in contrast to LARMix, eliminates node assignment and load balancing, instead determining client routes using lightweight approaches.

LAMP



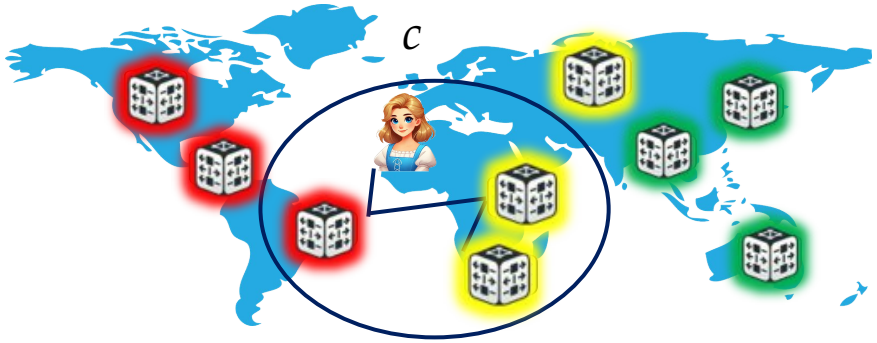
Single Circle (SC):
1- Super effcient approach
2- Moderate low-latency links



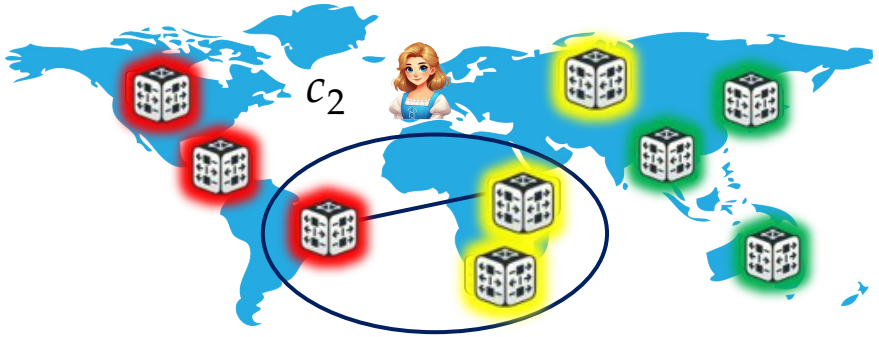
Multiple Circles (MC):
1- Effcient approach
2- Very low-latency links

LAMP, in contrast to LARMix, eliminates node assignment and load balancing, instead determining client routes using lightweight approaches.

LAMP



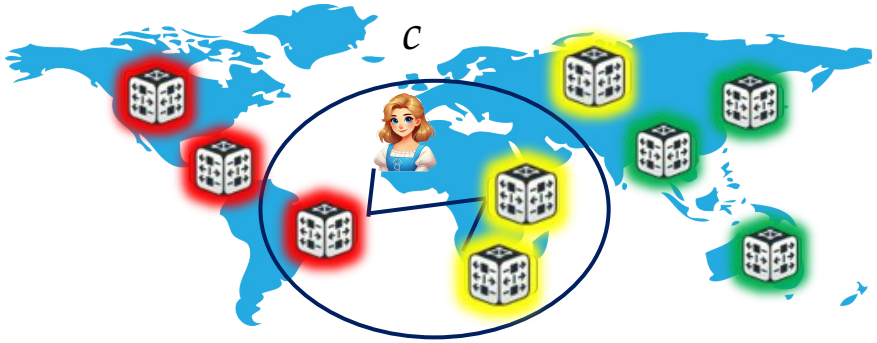
Single Circle (SC):
1- Super effcient approach
2- Moderate low-latency links



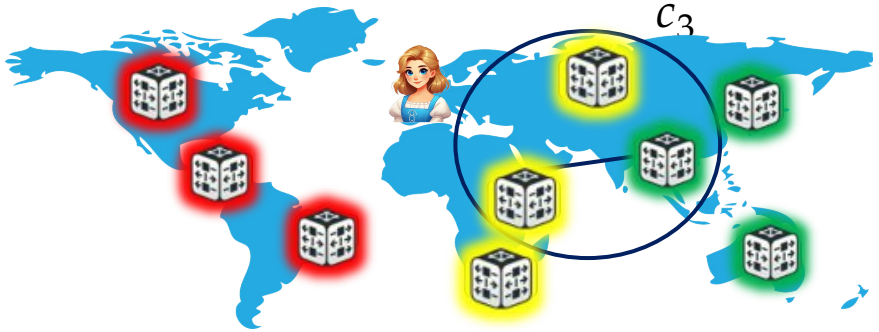
Multiple Circles (MC):
1- Effcient approach
2- Very low-latency links

LAMP, in contrast to LARMix, eliminates node assignment and load balancing, instead determining client routes using lightweight approaches.

LAMP



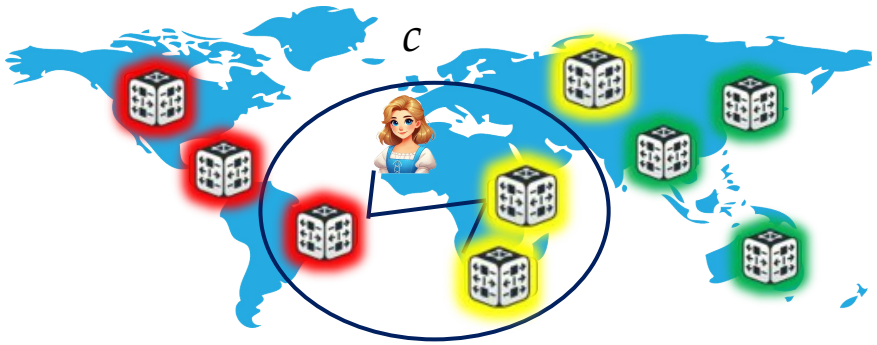
Single Circle (SC):
1- Super effcient approach
2- Moderate low-latency links



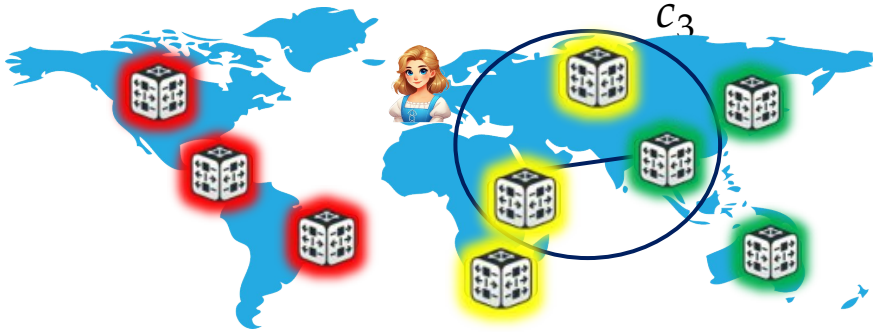
Multiple Circles (MC):
1- Effcient approach
2- Very low-latency links

LAMP, in contrast to LARMix, eliminates node assignment and load balancing, instead determining client routes using lightweight approaches.

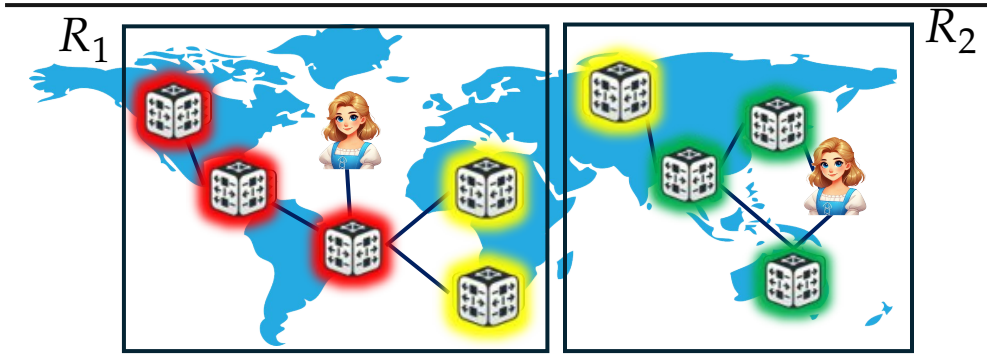
LAMP



Single Circle (SC):
1- Super effcient approach
2- Moderate low-latency links



Multiple Circles (MC):
1- Effcient approach
2- Very low-latency links

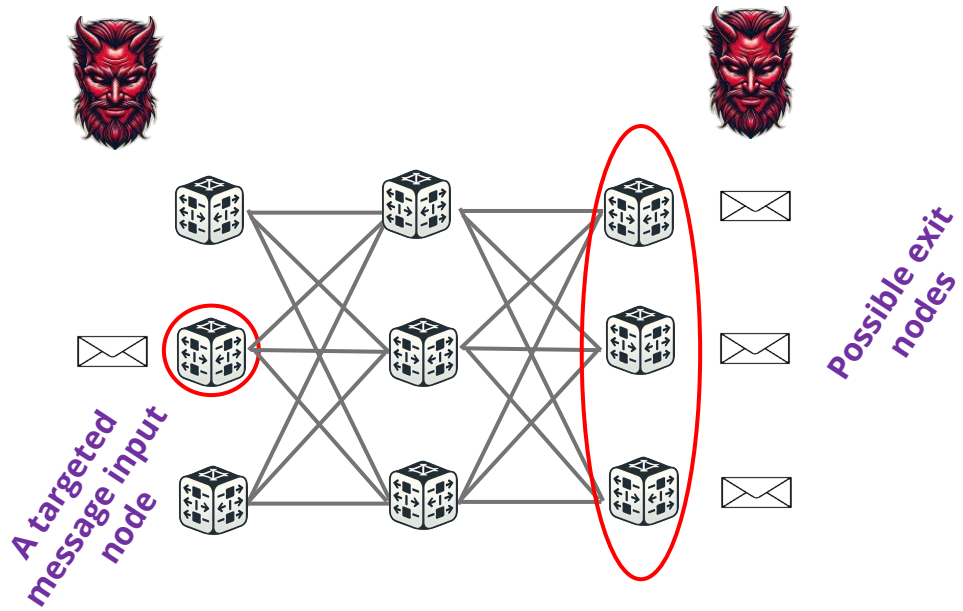


Regional Mixnets (RM):
1- Effcient approach
2- Varient low-latency links

LAMP, in contrast to LARMix, eliminates node assignment and load balancing, instead determining client routes using lightweight approaches.

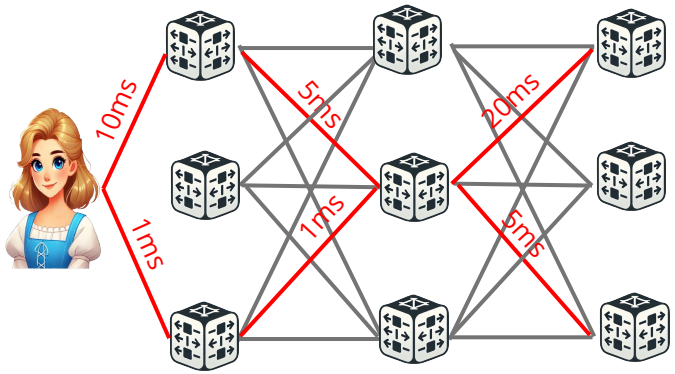
Metrics

Anonymity



Anonymity is measured using the **entropy** of a targeted message's exit mixnode, based on its corresponding input mixnode.

Latency



Average latency is useful for measuring the latency reduction.

Results

Approach \ Metrics	Latency	Entropy	Gain	Complexity
Vanilla	153.4 ms	5.9 bits	38.5	t
LARMix	68 ms	3.9 bits	57.35	13958t
Single Circle	52 ms	4.2 bits	80.77	t
Multiple Circles	20 ms	3.8 bits	190	56t
Regional Mixnet (EU)	18 ms	3.75 bits	208.3	8t
Regional Mixnet (NA)	46 ms	2.4 bits	52.2	t

Gain is defined as **Entropy/Latency**, while **Complexity** refers to the computation time required to execute the approach.

Conclusions

Hiding who communicates with whom is necessary on the Internet.

The Tor Network can reliably provide this anonymity but is vulnerable to traffic correlations.

Mixnet provides high degree of anonymity at the cost of high latency.

To reduce the high latency, we can use LAMP which improves the performance of mixnets by up to 87%.

Thank you for listening!

Scan the QR code to access the artifact.

You can find the slides from this talk, along with other related papers and blog posts, on my webpage.

If you'd like to learn more about mix networks or anonymous communications, feel free to connect with me through LinkedIn.