Enhancing Applicability of Mix Networks

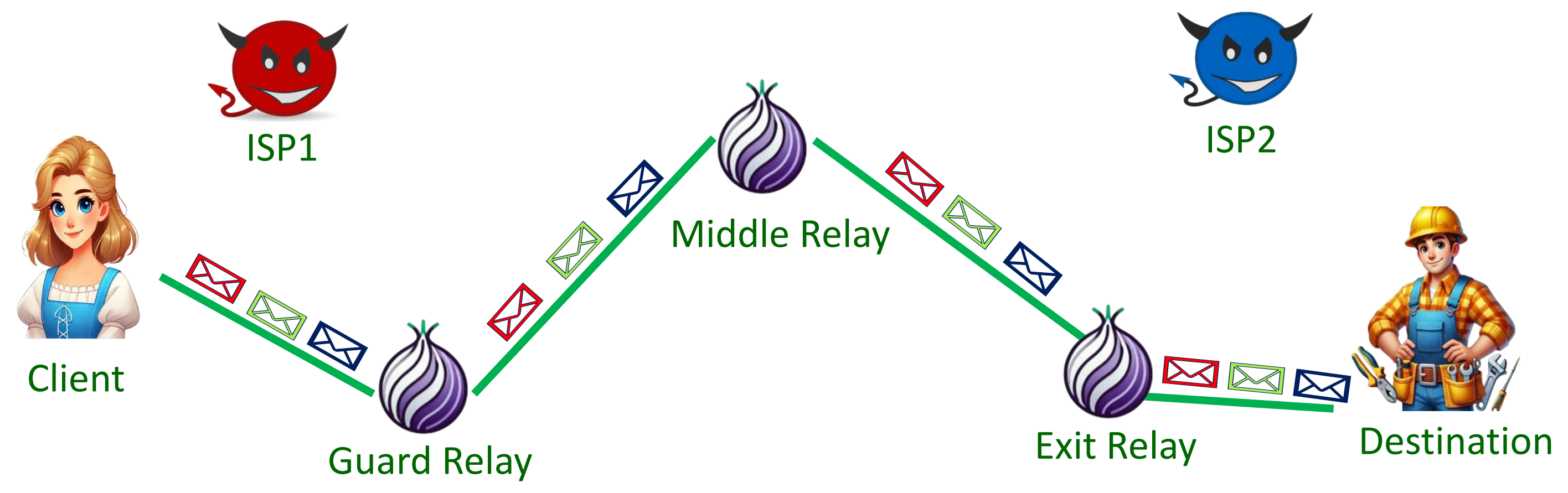
Mahdi Rahimi, COSIC (KU Leuven), Leuven, Belgium, October 2025

Backgrounds and Motivations

End users on the internet are not anonymized by default.

This poses serious privacy risk.

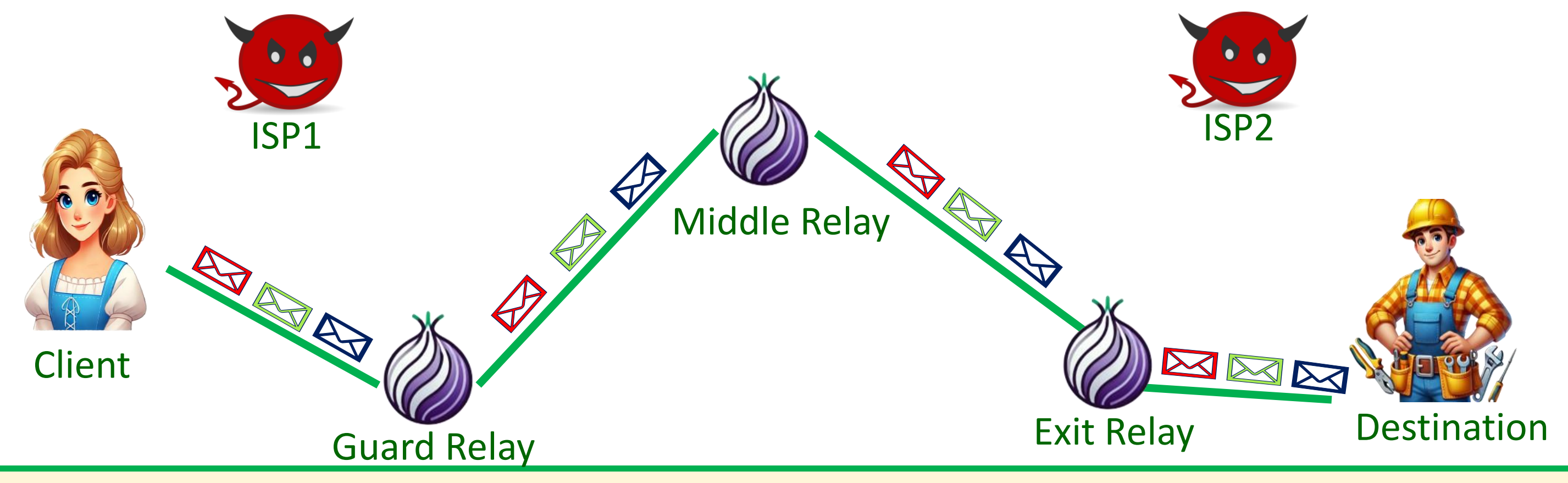
Tor Network



ISP: Internet Service Provider

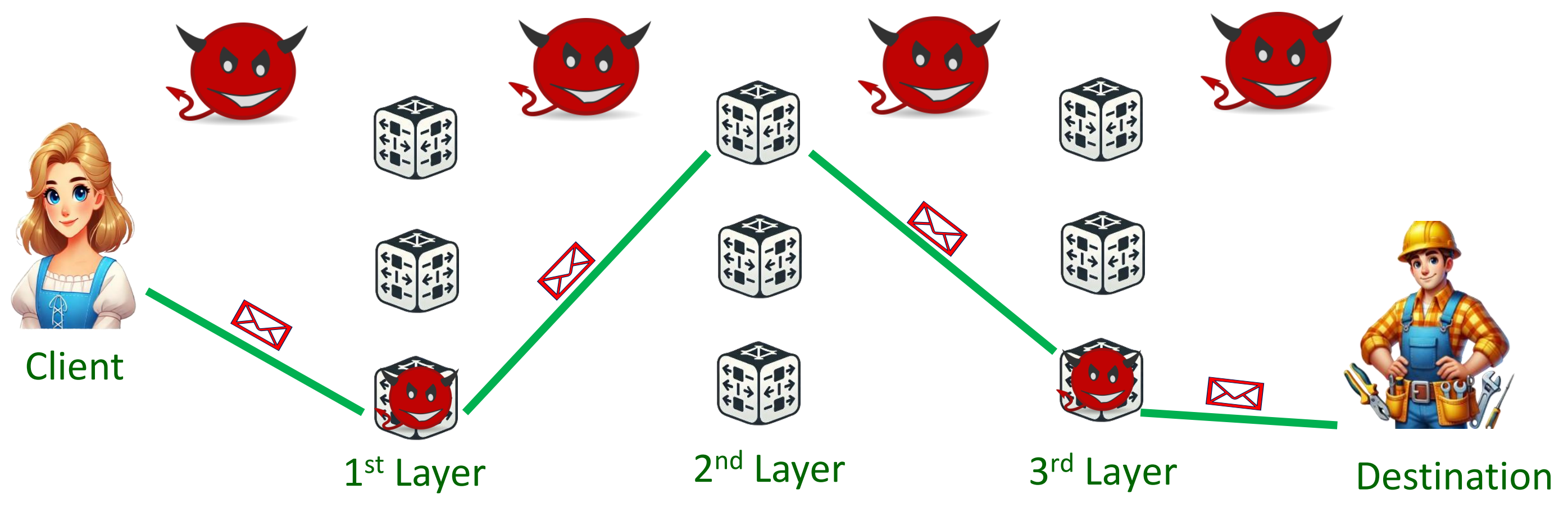
ISP1 does not collude with ISP2.

End-to-End Correlation Attacks



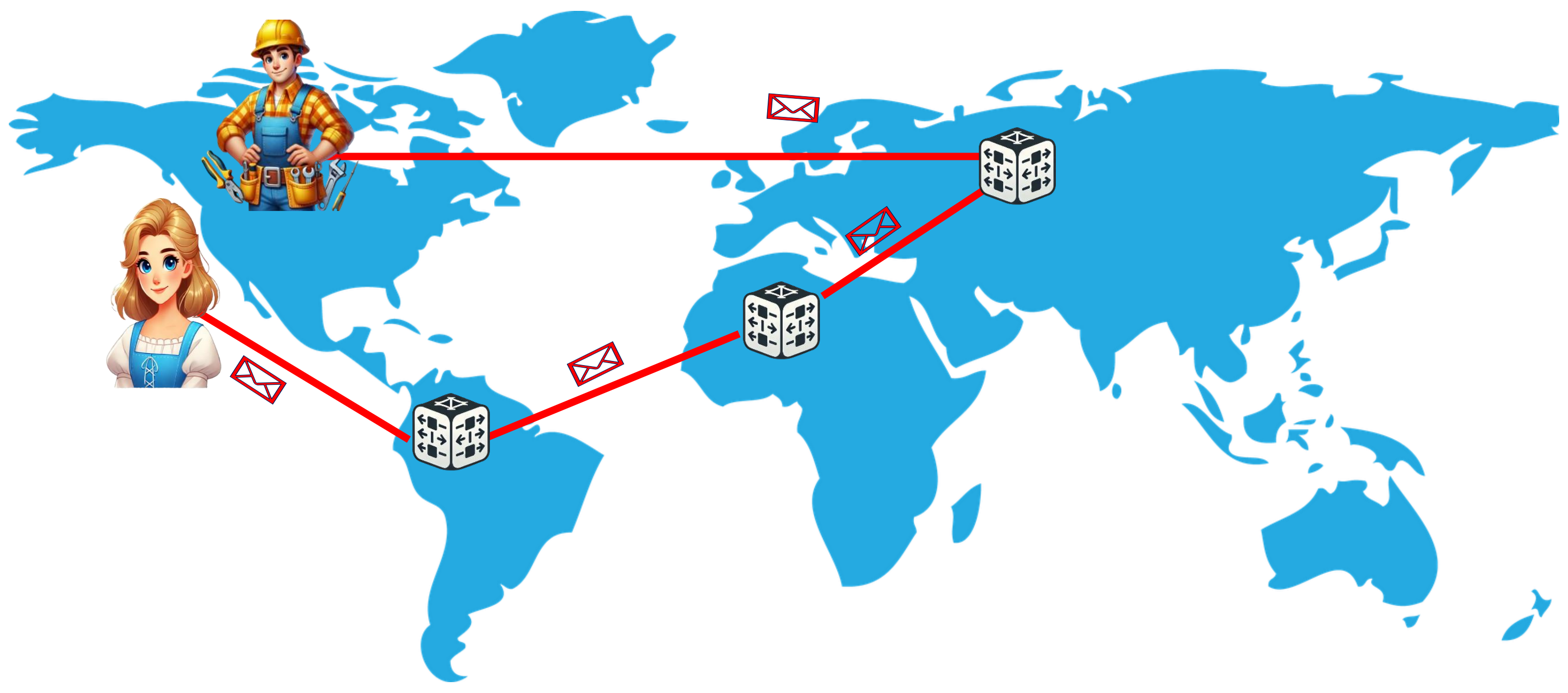
If ISP1 colludes with ISP2, they can deanonymize the client-destination connection.

Mix Networks (Mixnets)



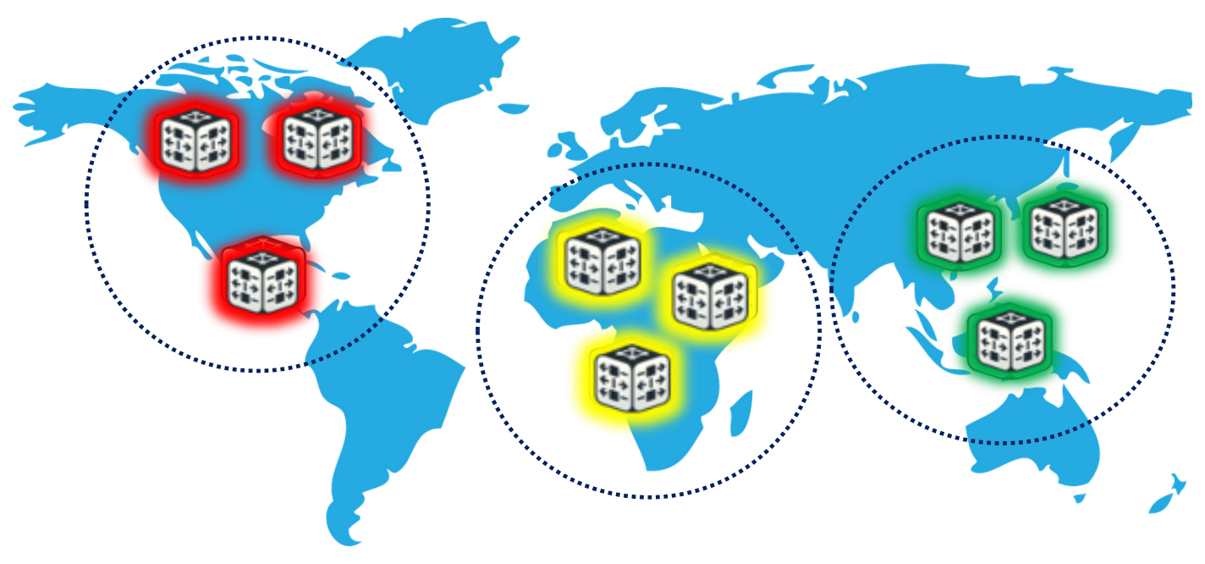
Mixnets provide strong anonymity by breaking the linkability of traffic flows.

High End-to-End Latency

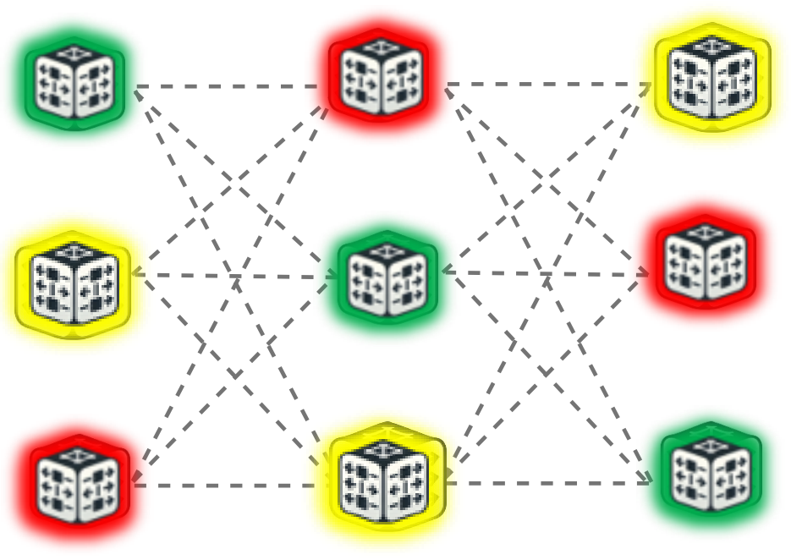


As a result of routing through intermediate nodes and mixing delays at each mixnode, the end-to-end latency is high.

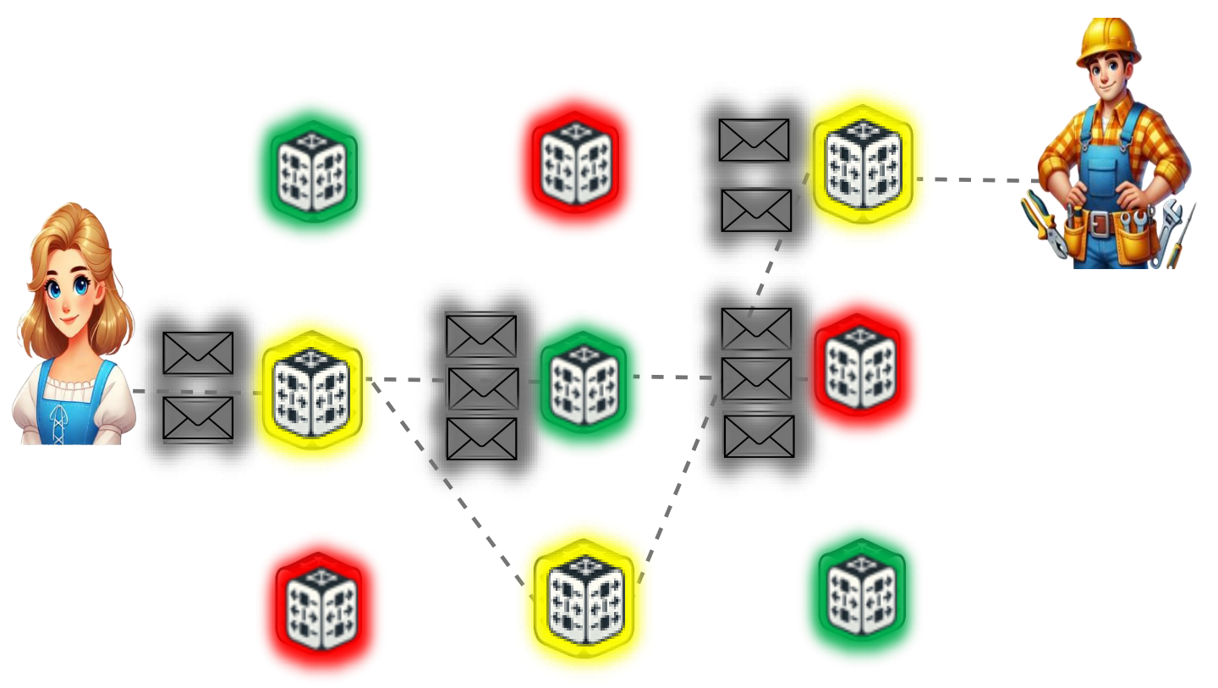
LARMix [1]



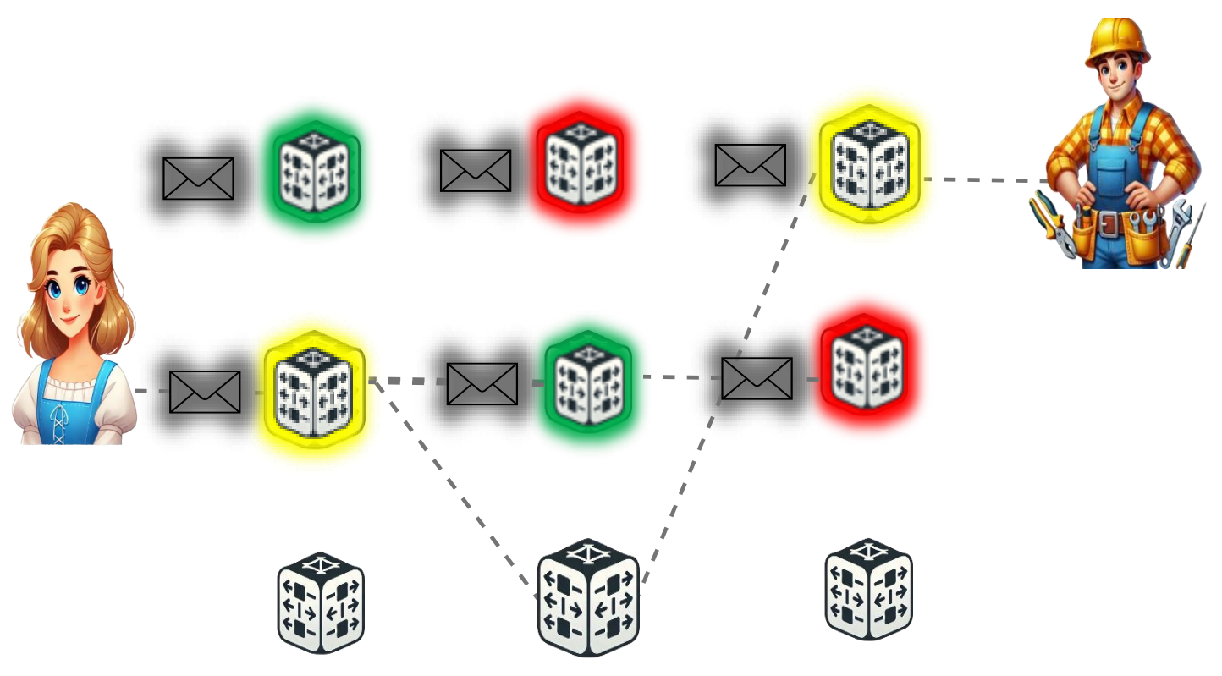
Clustering



Diversification

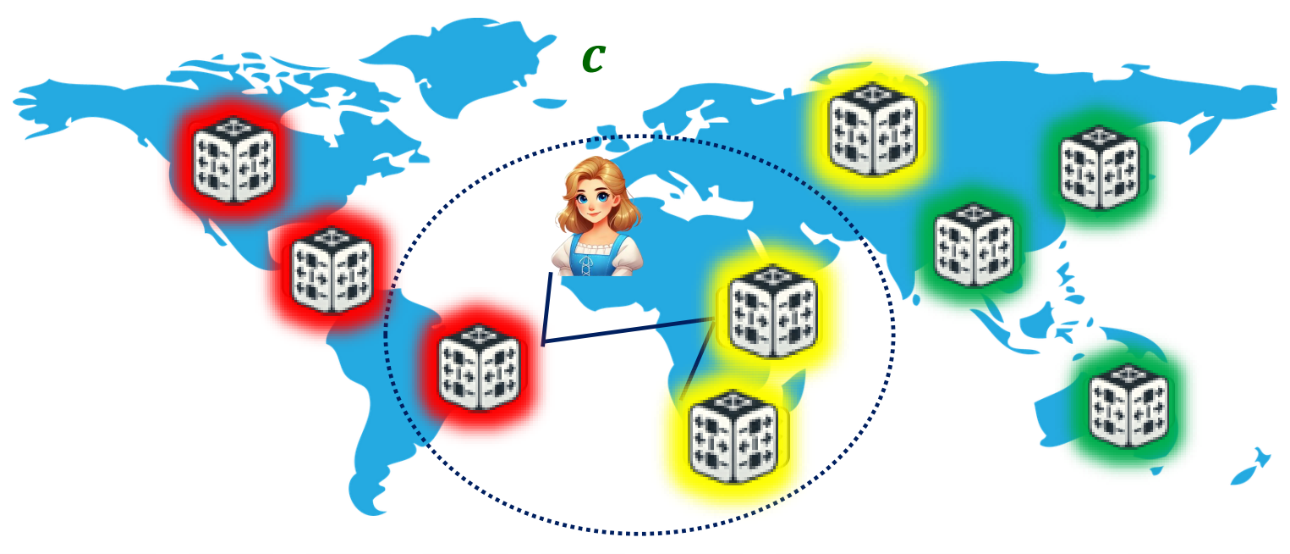


Low-latency routing

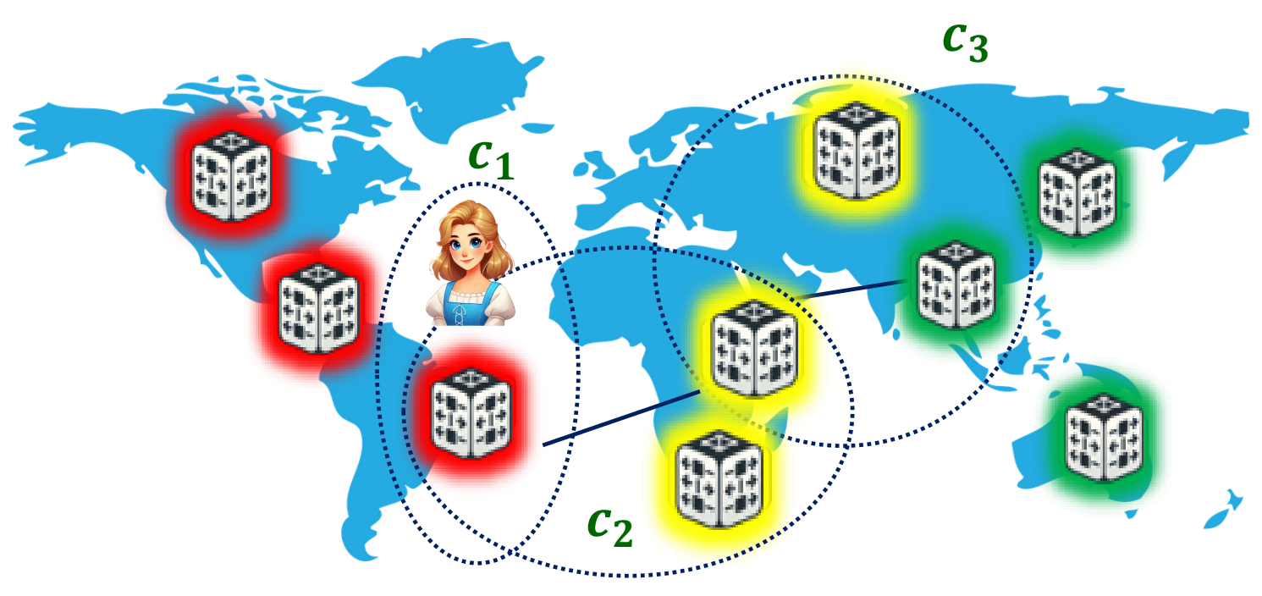


Load balancing

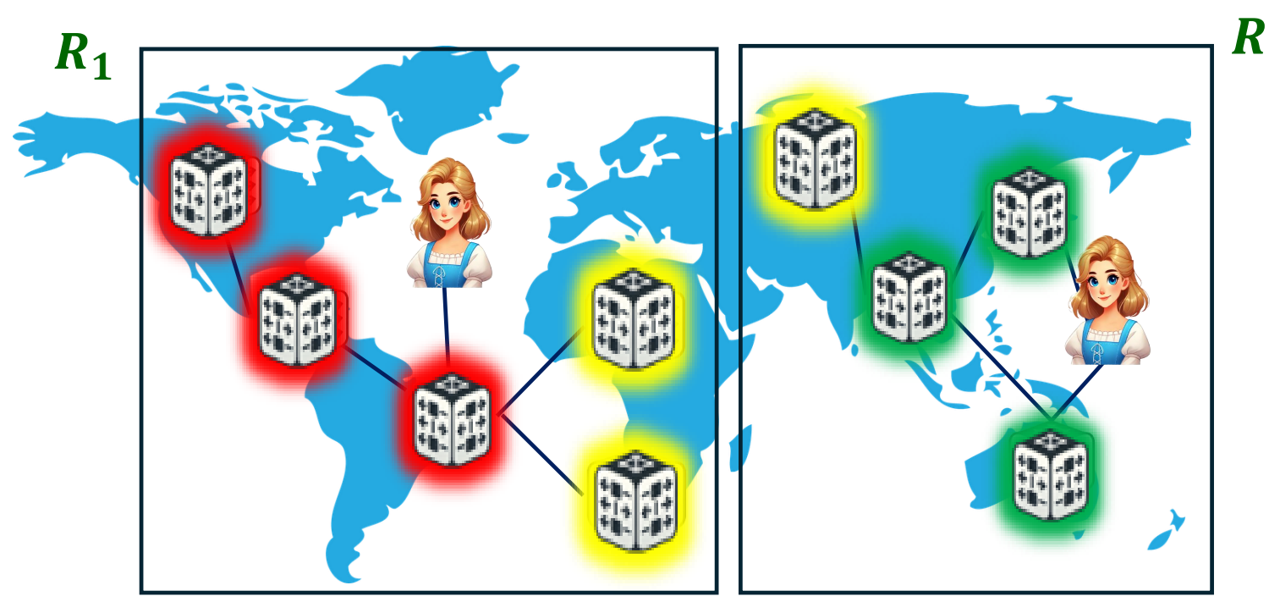
LAMP [2]



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



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



Regional Mixnets (RM):
1- Efficient approach
2- Variant low-latency links

Results

Approach \ Metrics	Latency	Entropy	Gain	Complexity
Vanilla	153.4 ms	5.9 bits	38.5	t
LARMix [1]	68 ms	3.9 bits	57.35	13958t
Single Circle [2]	52 ms	4.2 bits	80.77	t
Multiple Circles [2]	20 ms	3.8 bits	190	56t
Regional Mixnet (EU) [2]	18 ms	3.75 bits	208.3	8t
Regional Mixnet (NA) [2]	46 ms	2.4 bits	52.2	t

Conclusions

Hiding who communicates with whom is **necessary** on the Internet.

Mixnets provide **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%**.

Acknowledgments
This work is supported by CyberSecurity Research Flanders.

References

[1]. M. Rahimi, P. Kumar & C. Diaz, “LARMix: Latency-Aware Routing in Mix Networks,” in NDSS 2024: 31st Symposium on Network and Distributed System Security, Internet Society.

[2]. M. Rahimi, P. Kumar & C. Diaz, “LAMP: Lightweight Approaches for Latency Minimization in Mixnets with Practical Deployment Considerations,” in NDSS 2025: 32nd Symposium on Network and Distributed System Security, Internet Society.