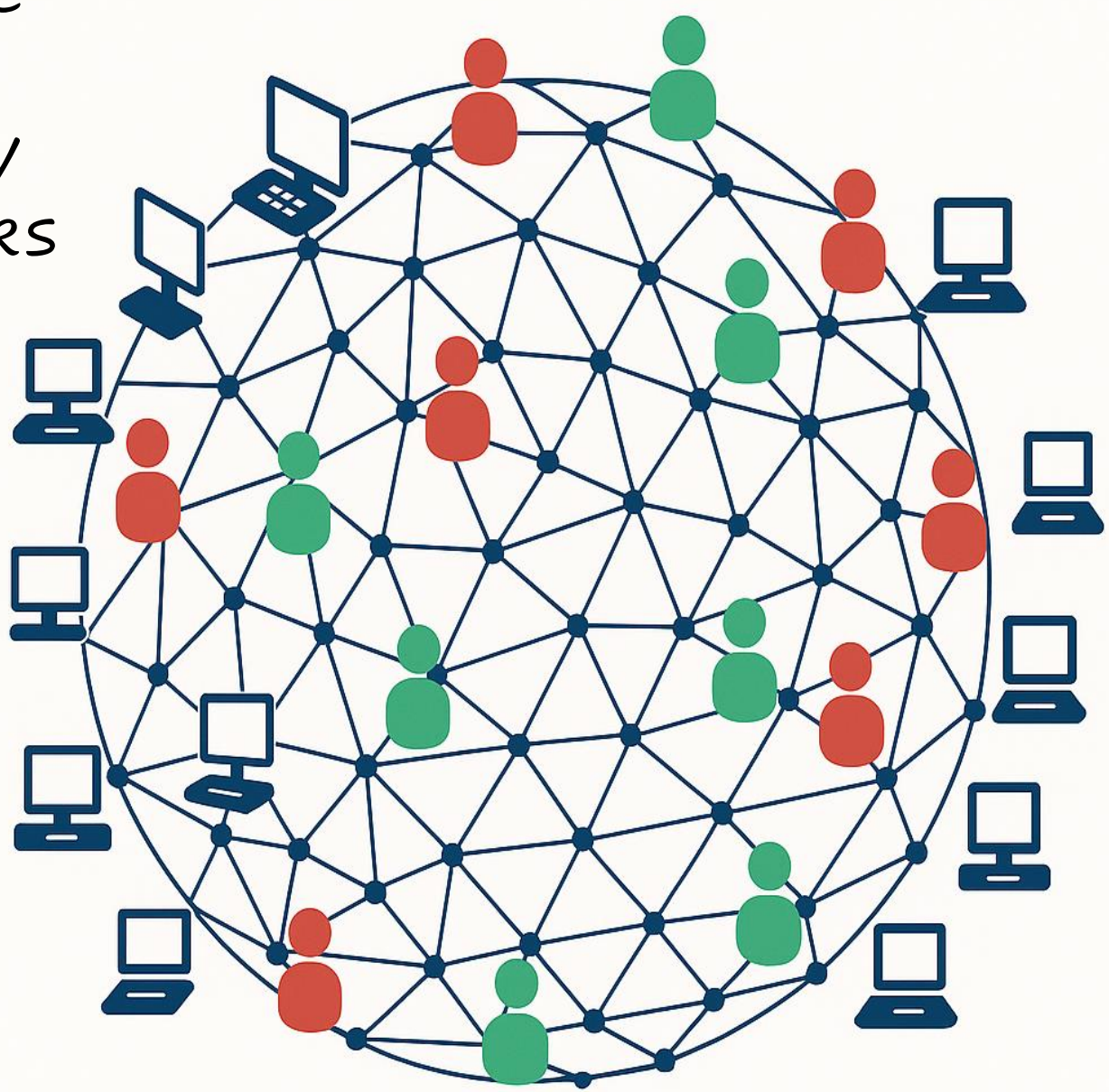
PARSAN-Mix: Packet-Aware Routing and Shuffling with Additional Noise for Latency Optimization in Mix Networks

Mahdi Rahimi

mahdi.rahimi@kuleuven.be

COSIC, KU Leuven, Belgium

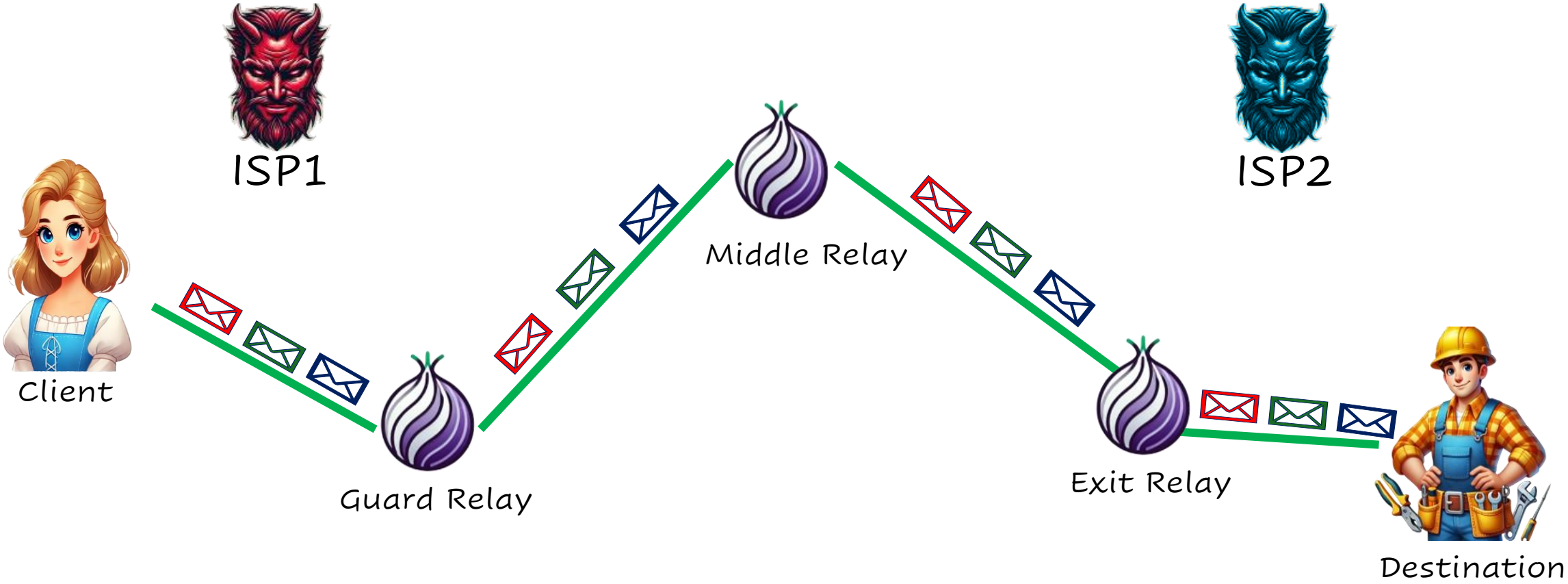


23rd International Conference on Applied Cryptography and Network Security (ACNS), 23rd-26th June 2025, Munich, Germany.

End users on the internet are not anonymized by default.

This creates privacy issues.

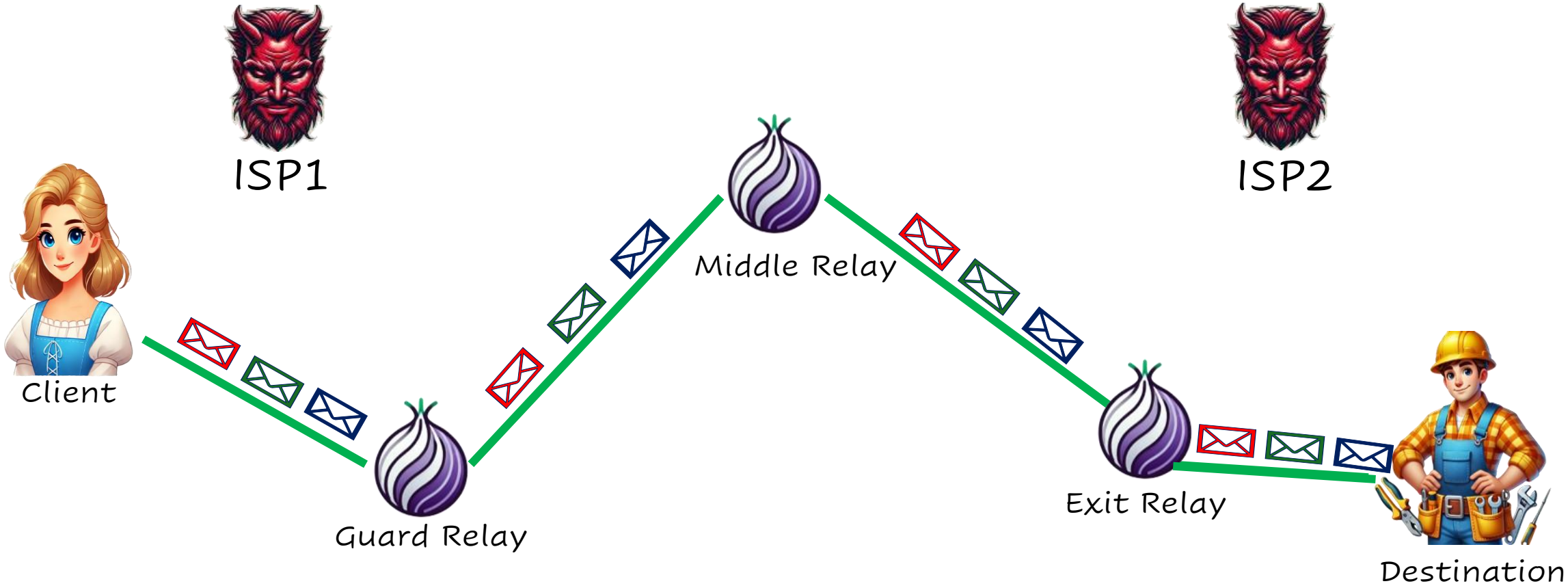
Tor Network



ISP: Internet Service Provider.

ISP1 does not collude with ISP2.

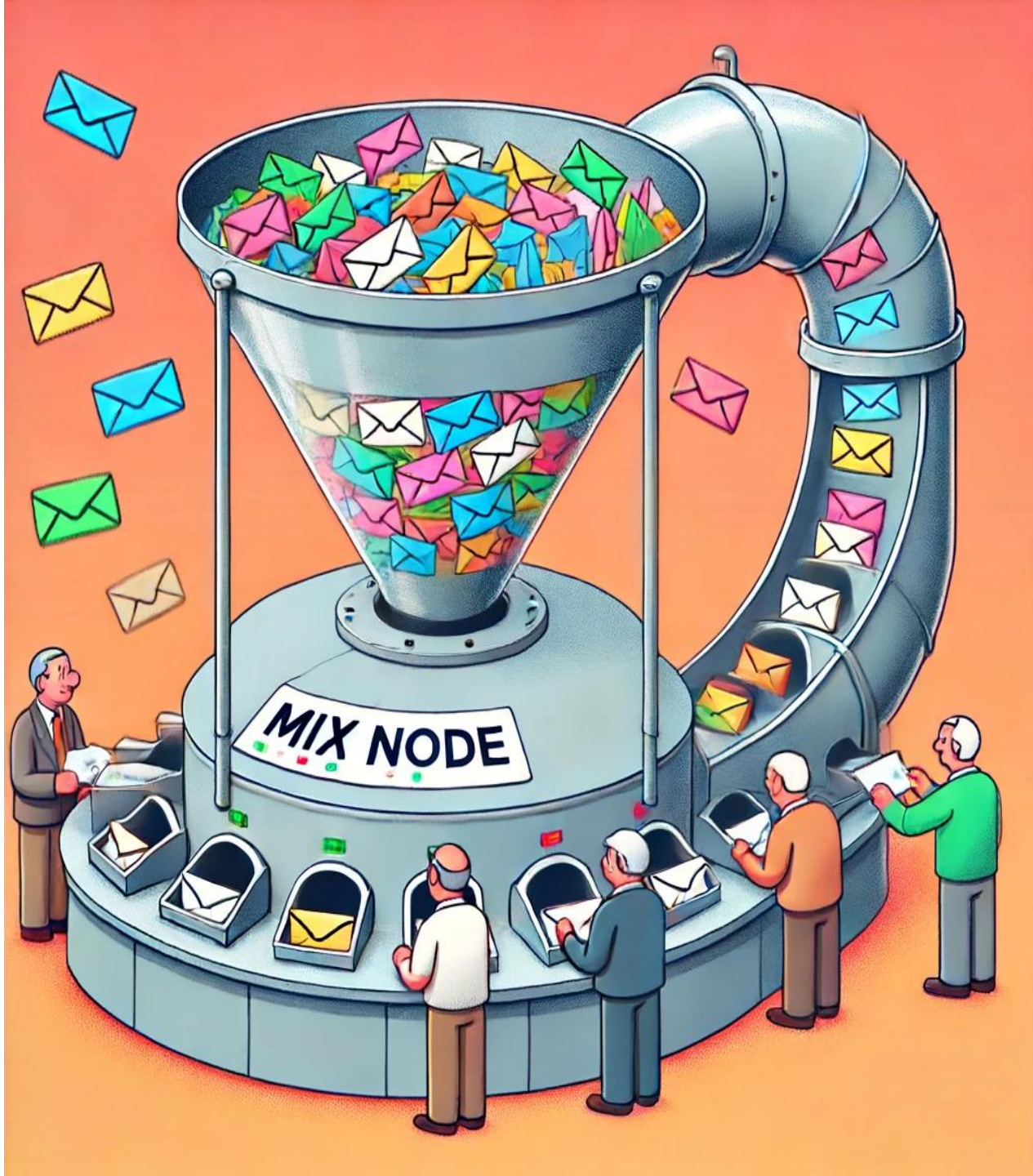
End-to-End Correlation Attacks



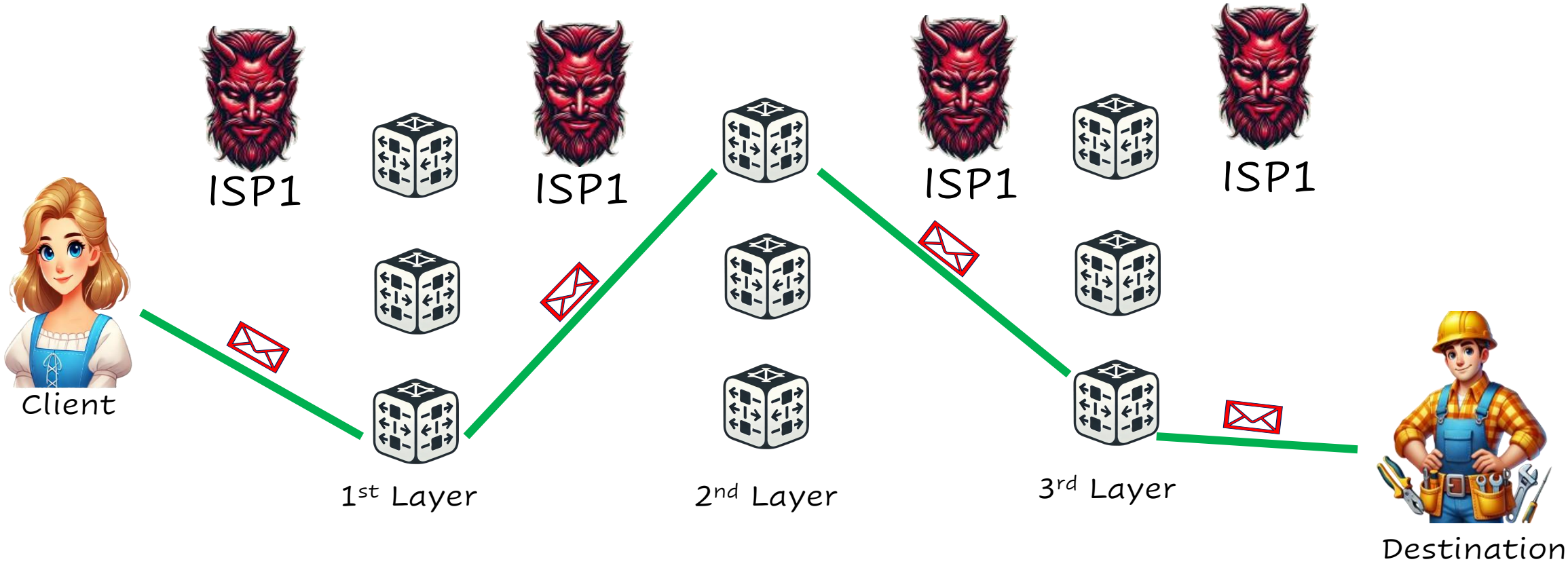
If ISP1 colludes with ISP2, they can deanonymize the client-destination connection.

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

Mixnodes make their input and output unlinkable.

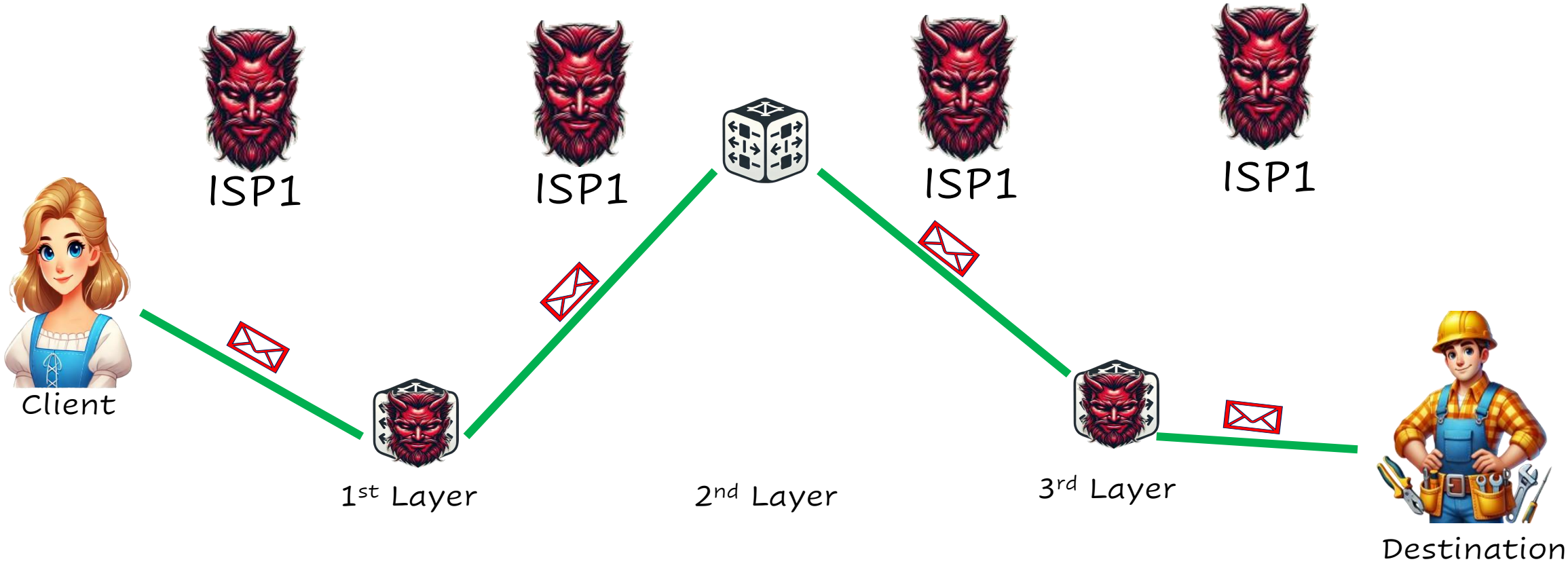


Mix Network (Mixnet)



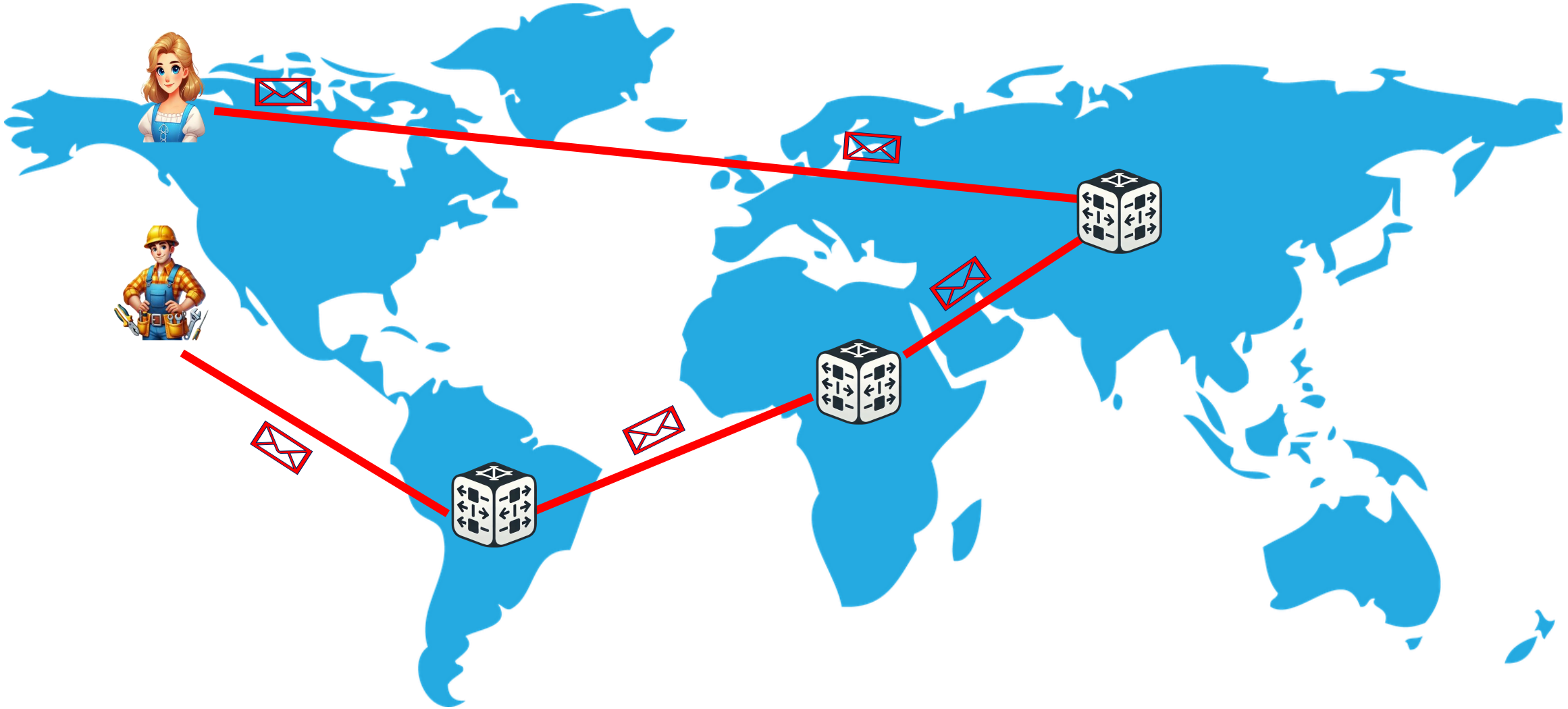
A mixnet is a network consisting of mixnodes, typically arranged in a layered format.

Anonymity Requirement



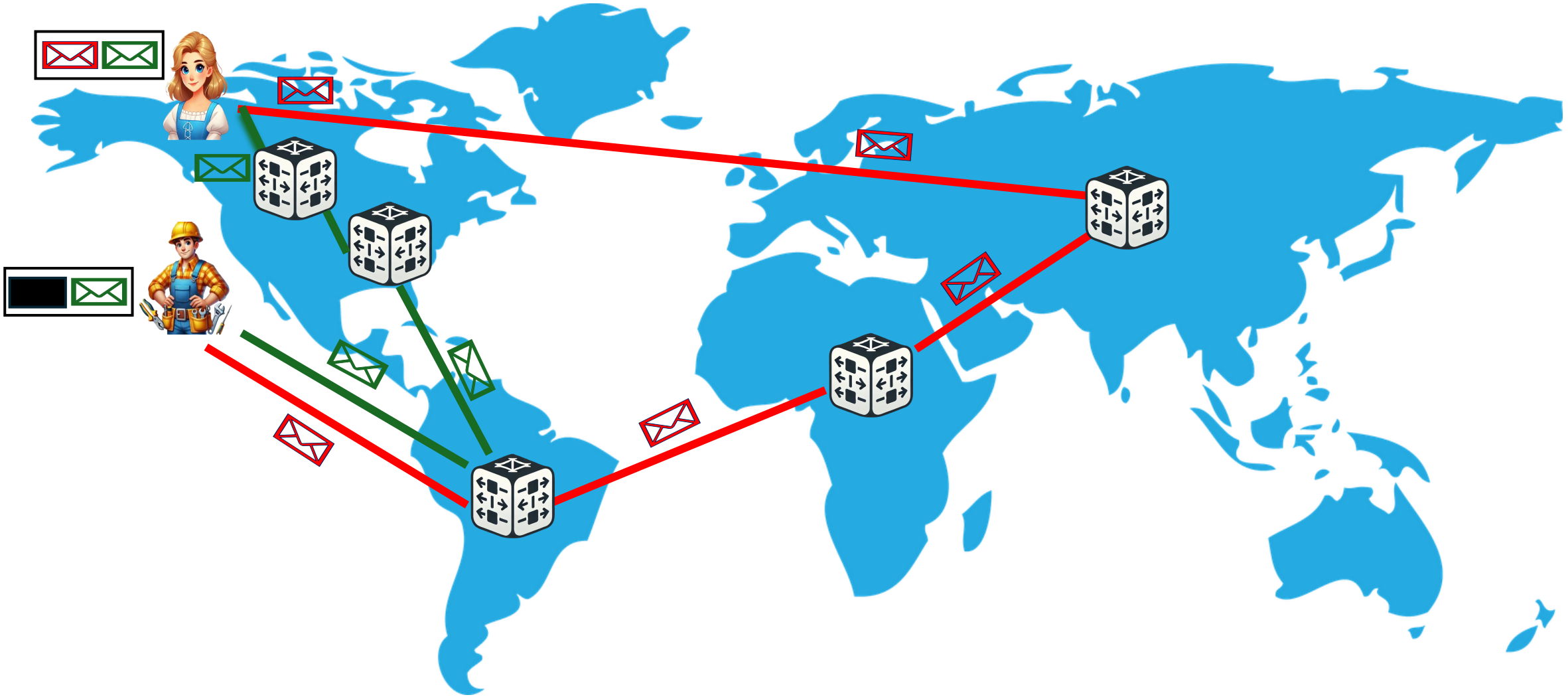
As long as one mixnode in the message route is honest, the client-destination connection will be anonymized.

End-to-End Latency



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

End-to-End Latency



Additionally, as packets are routed through different paths, the latency increases.

Methodology

Packet-Aware Routings (PAR)

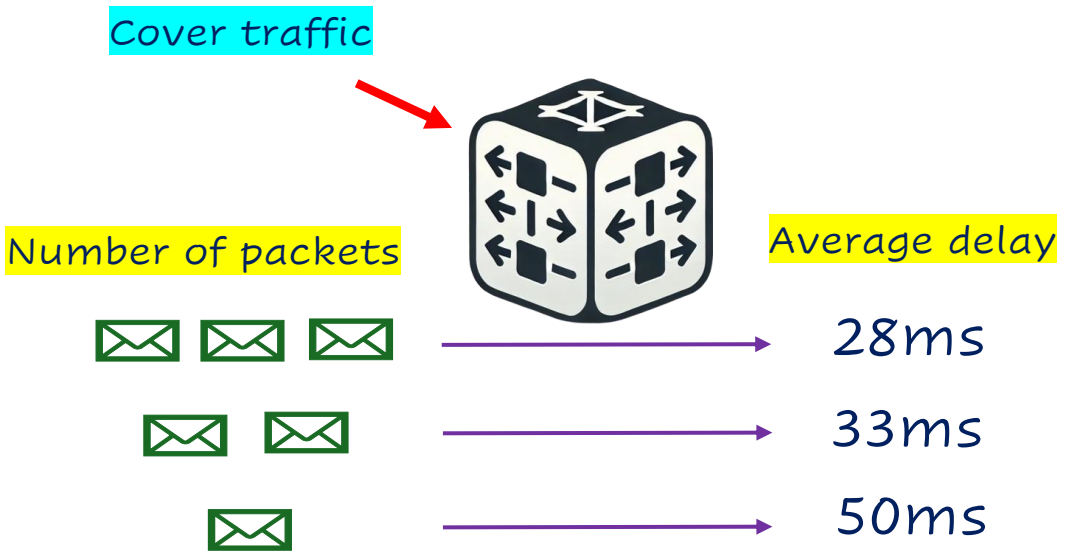
For messages embedding a higher number of packets, select faster links.

Methodology

Packet-Aware Routings (PAR)

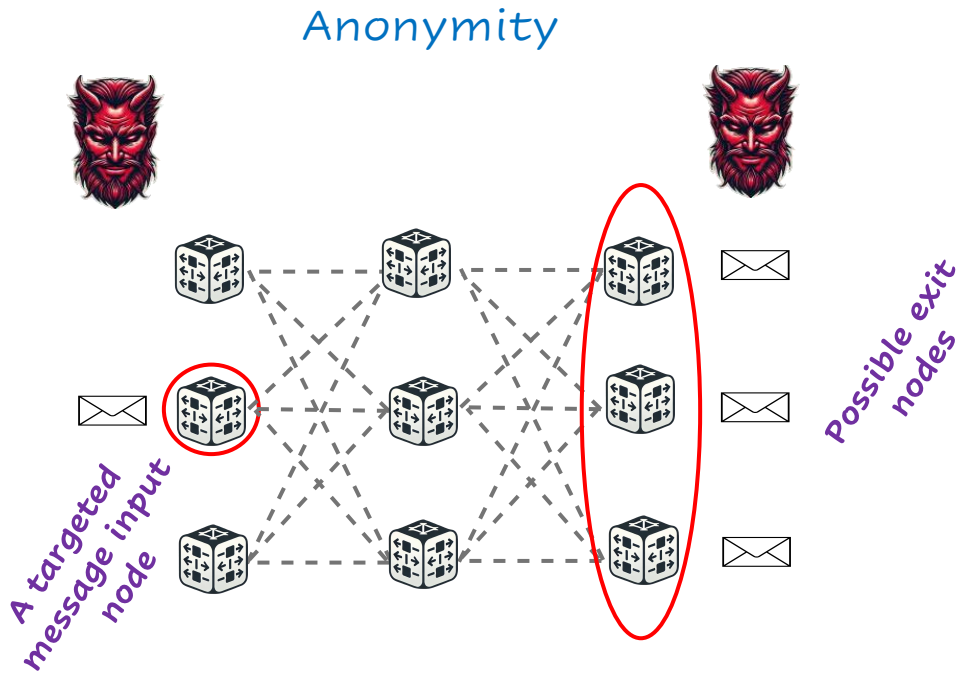
For messages embedding a higher number of packets, select faster links.

Managing Shuffling Delay (MSD)



The higher the number of packets, the lower the average mixing delay.

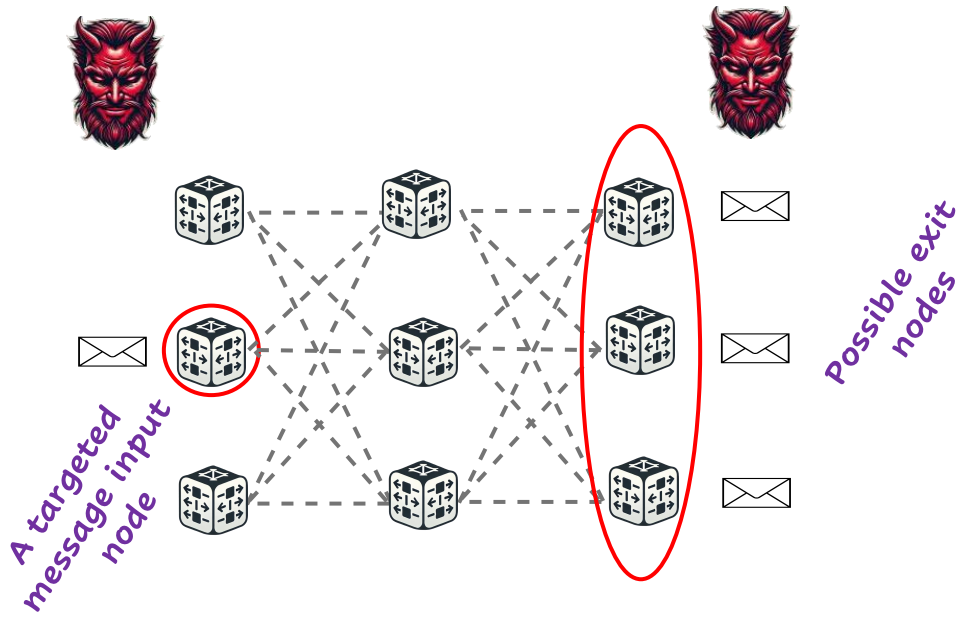
Metrics



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

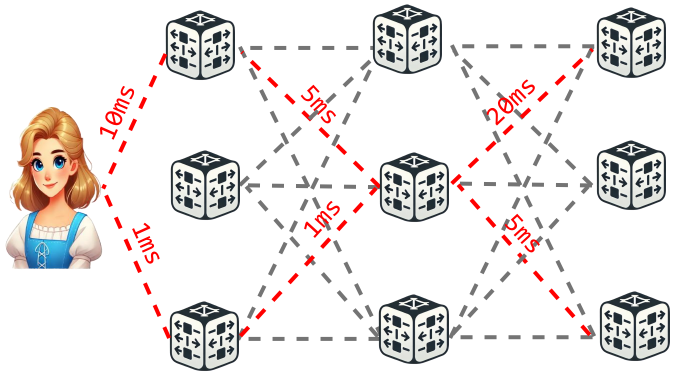
Metrics

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 (ms)	Anonymity (bits)	Complexity
Vanilla setting	400	7.2	Low
Packet-Aware Routings	320	6	Low
Managing Shuffling Delay	192	7.2	High

Higher latency reduction without anonymity loss can be achieved with high computational complexity, while moderate latency reduction with low complexity results in slight anonymity loss.

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 PARSAN-Mix which improves the performance of mixnets by up to 52%.

Thank you for listening!

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.