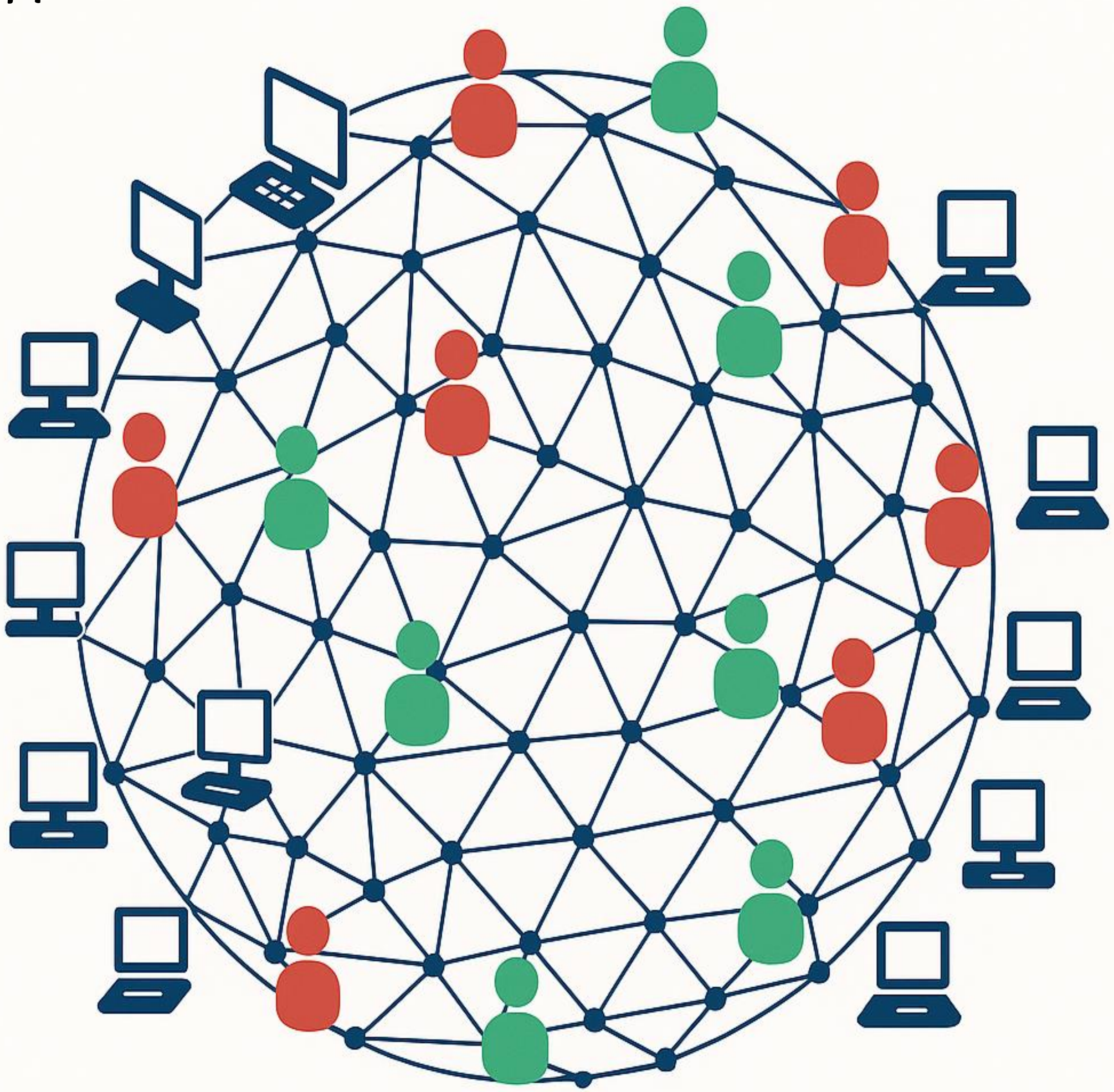
MOCHA: Mixnet Optimization Considering Honest Client Anonymity

Mahdi Rahimi

mahdi.rahimi@kuleuven.be

COSIC, KU Leuven, Belgium

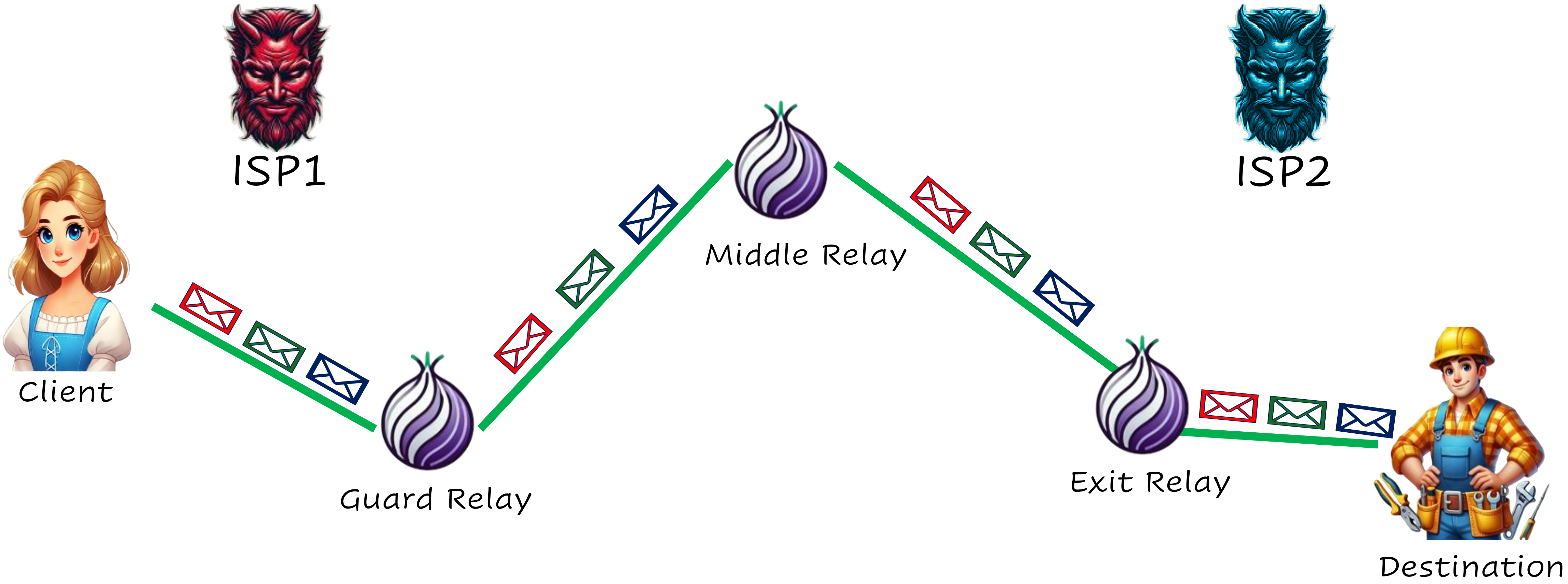


13th ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec) 2025, San Jose, CA, June 18-20.

End users on the internet are not anonymized by default.

This creates privacy issues.

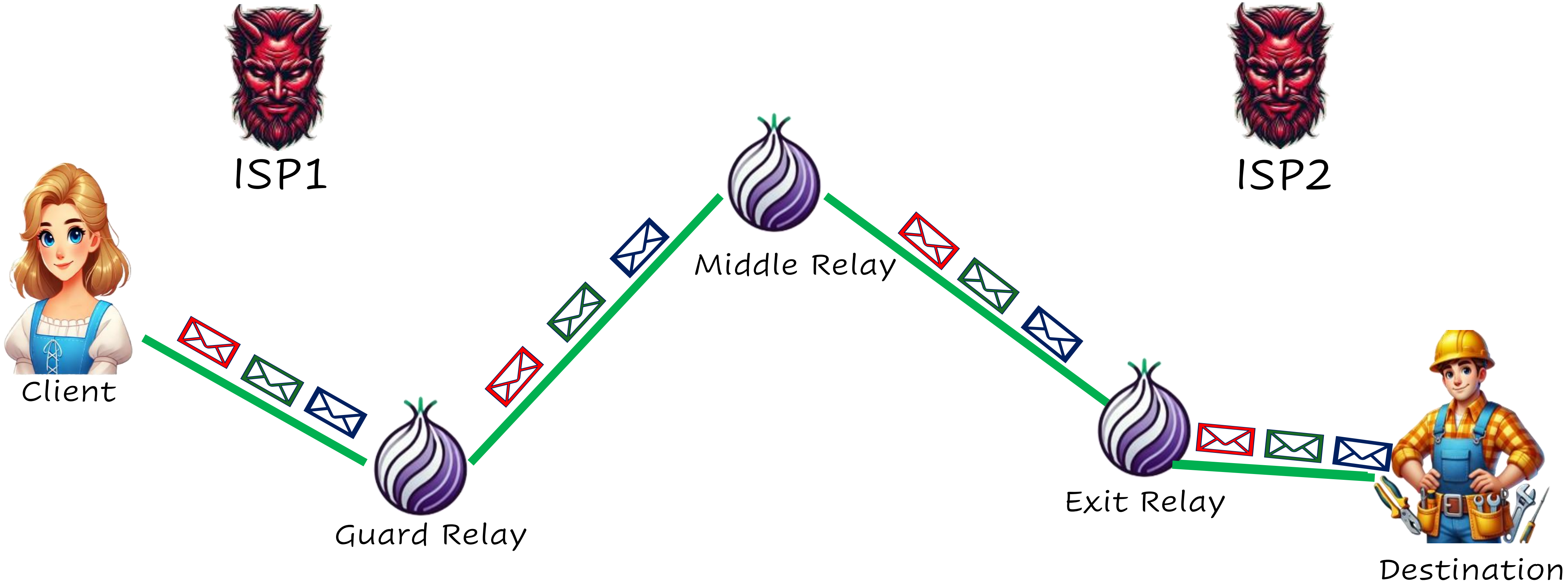
Tor Network



ISP: Internet Service Provider.

ISP1 does not collude with ISP2.

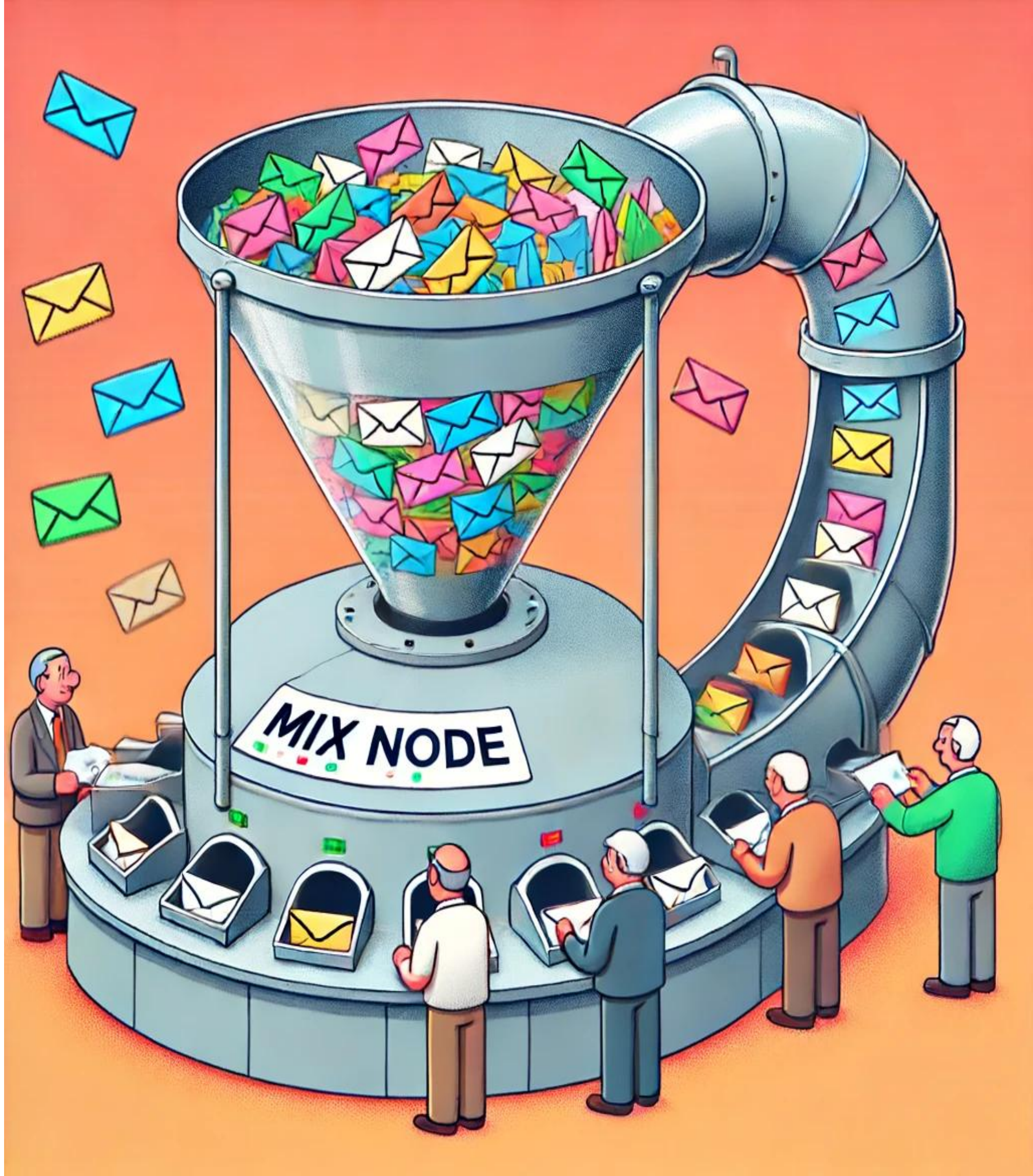
End-to-End Correlation Attacks



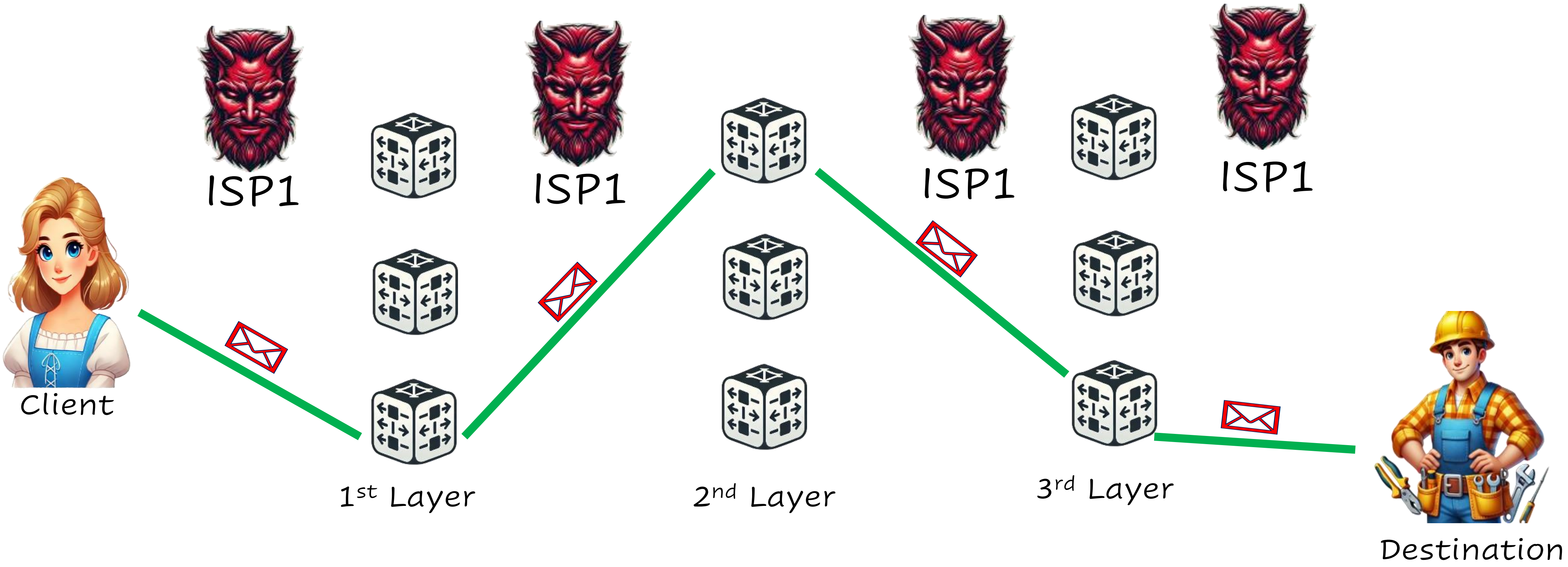
If ISP1 colludes with ISP2, they can deanonymize the client-destination connection.

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

Mixnodes make their input and output unlinkable.

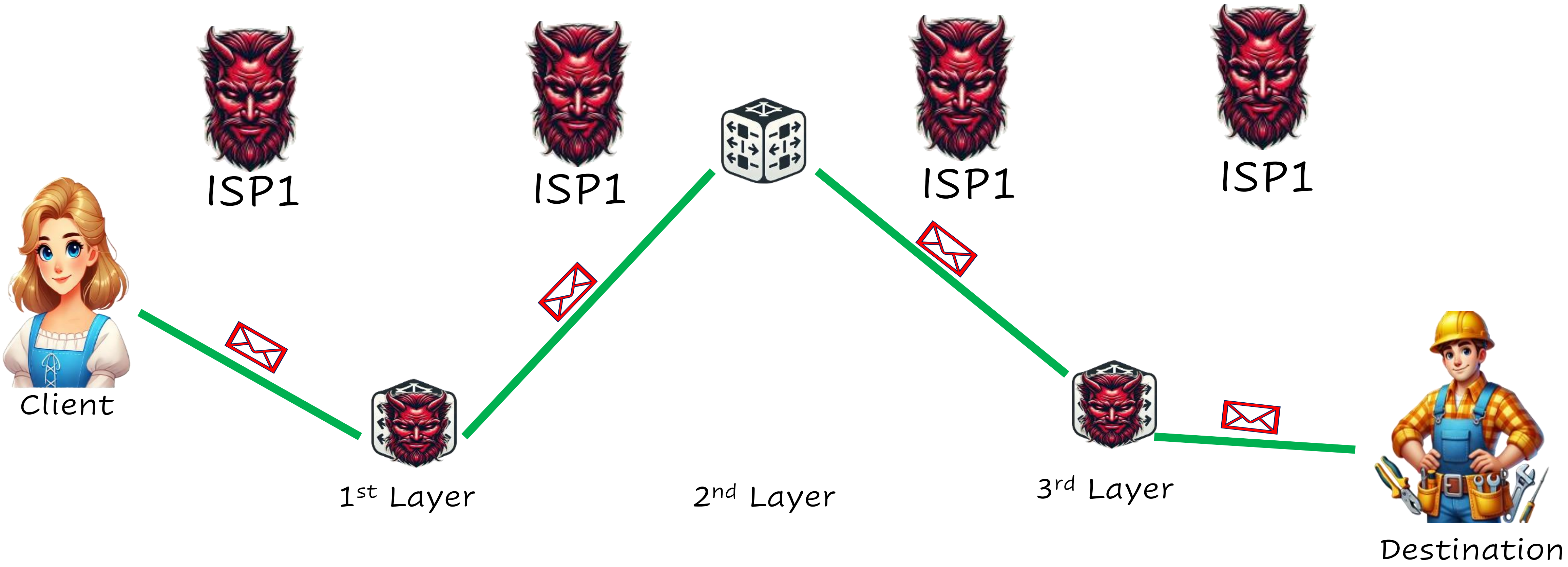


Mix Network (Mixnet)



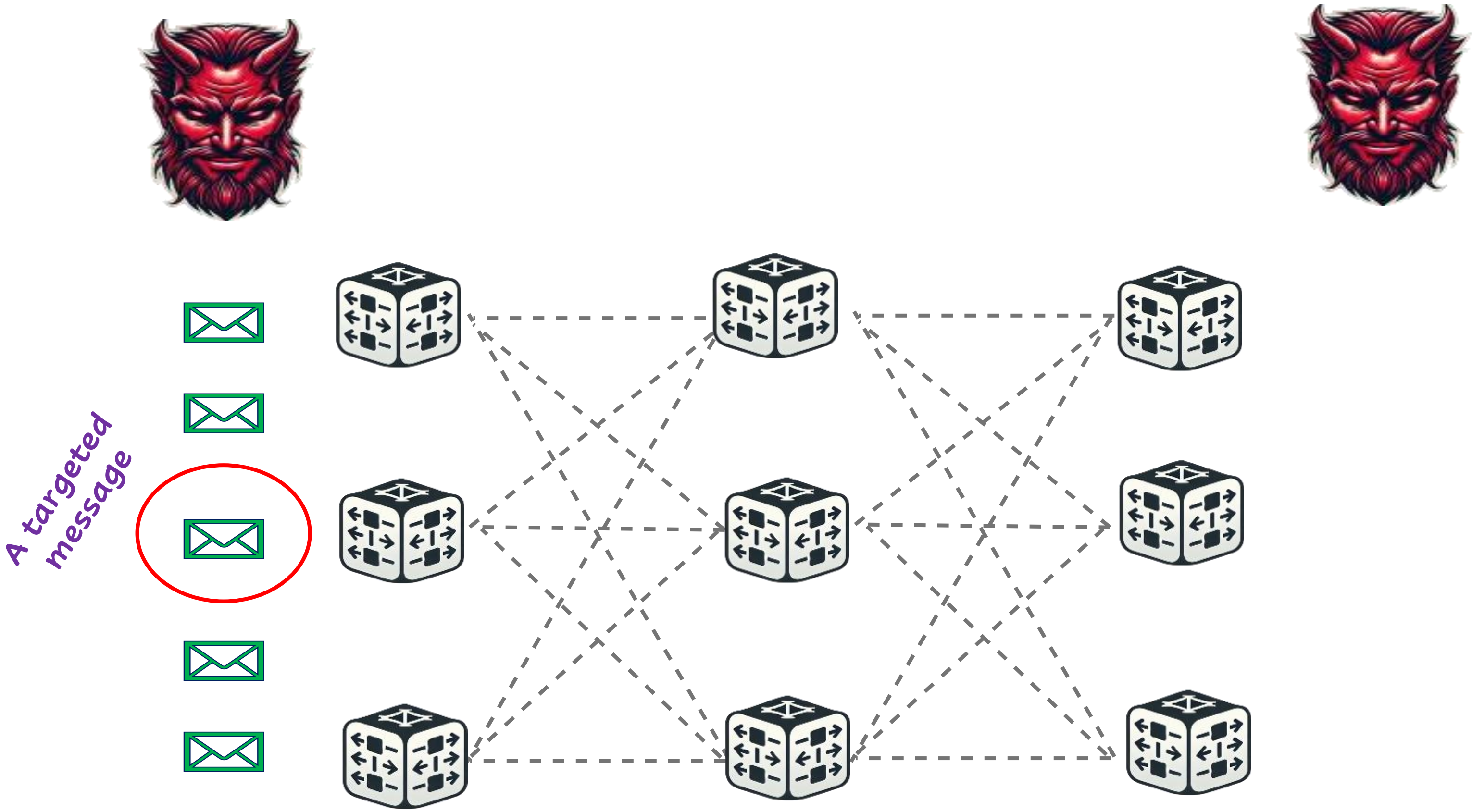
A mixnet is a network consisting of mixnodes, typically arranged in a layered format.

Anonymity Requirement

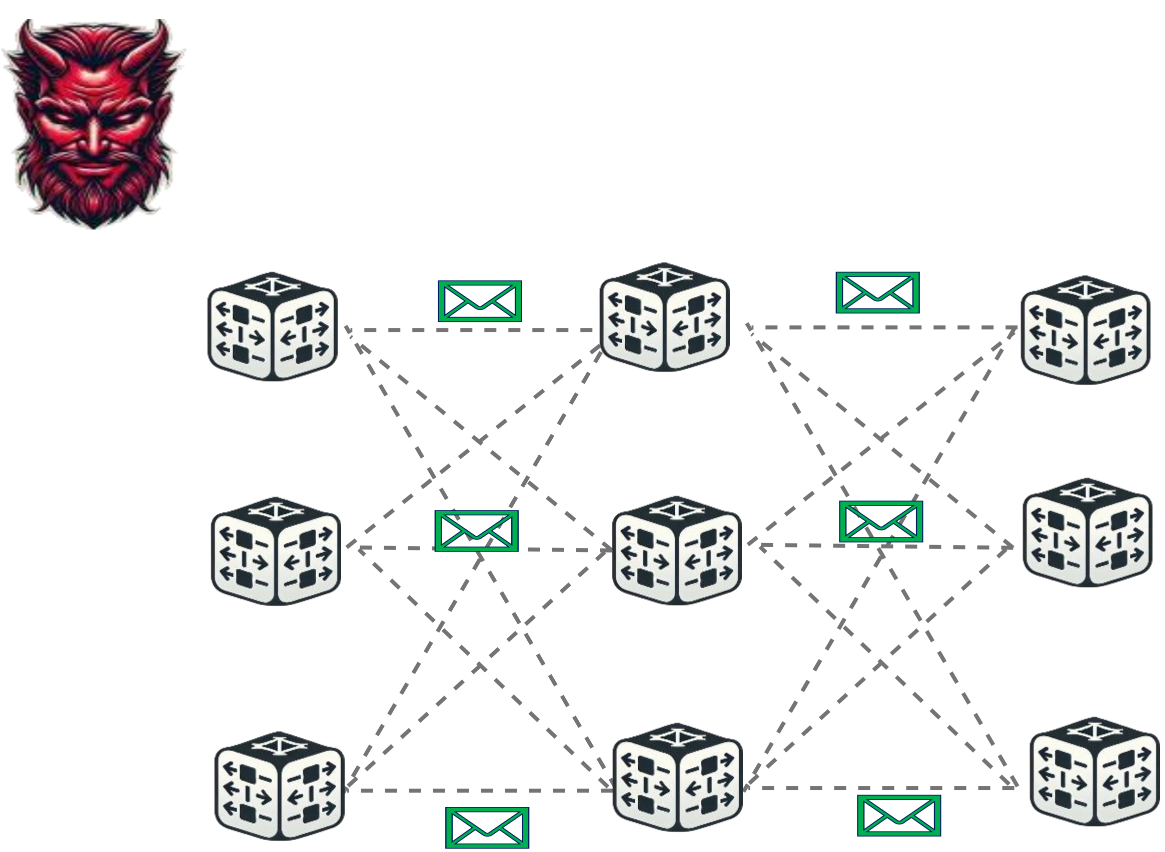


As long as one mixnode in the message route is honest, the client-destination connection will be anonymized.

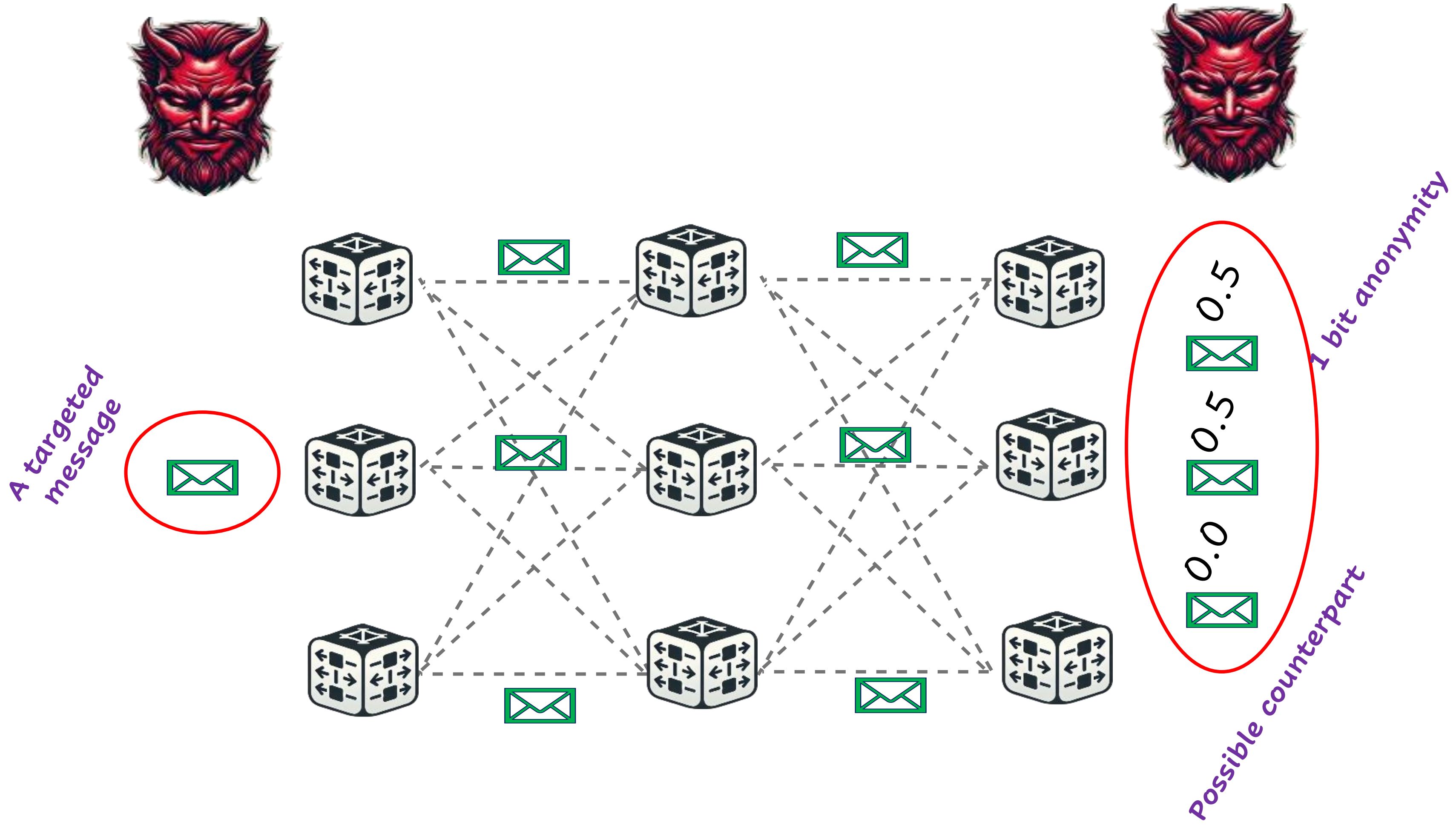
How strong is the anonymity?



How strong is the anonymity?

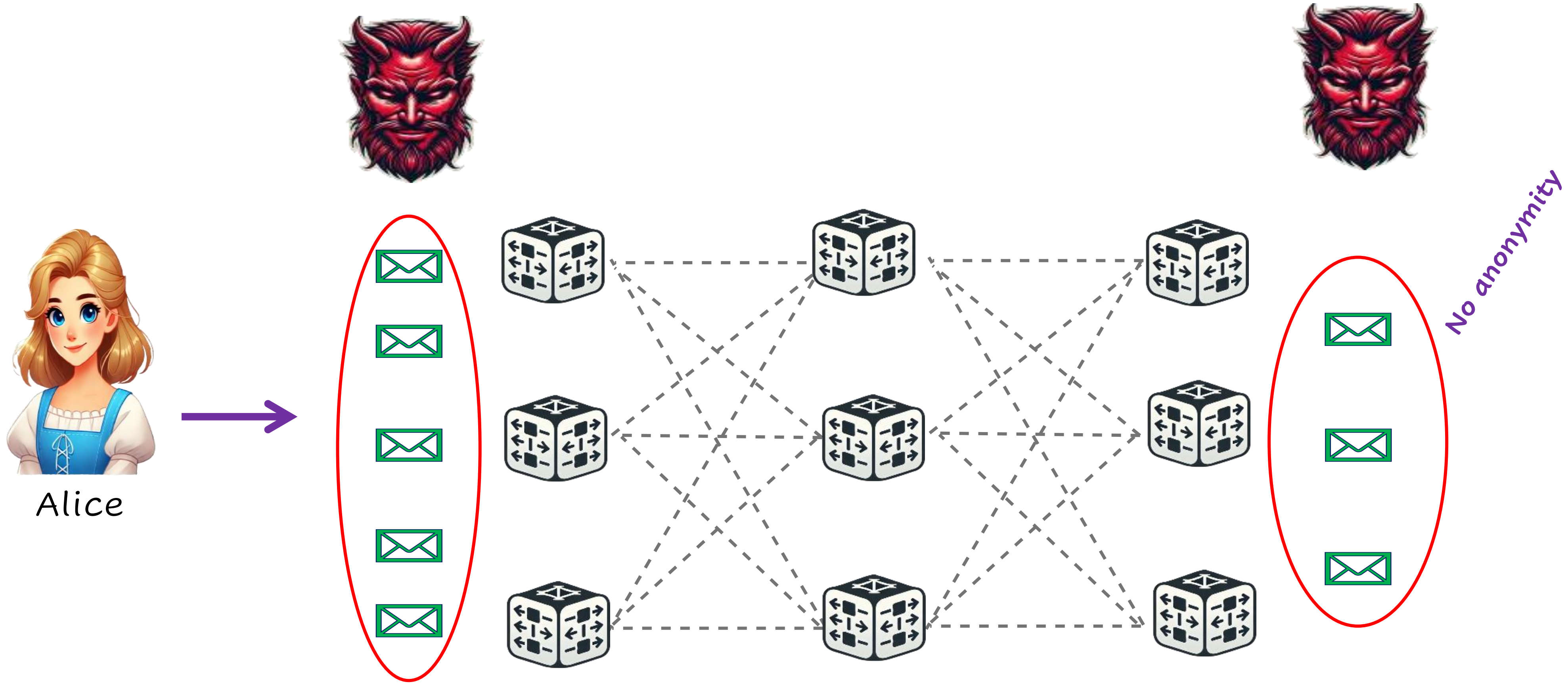


How strong is the anonymity?



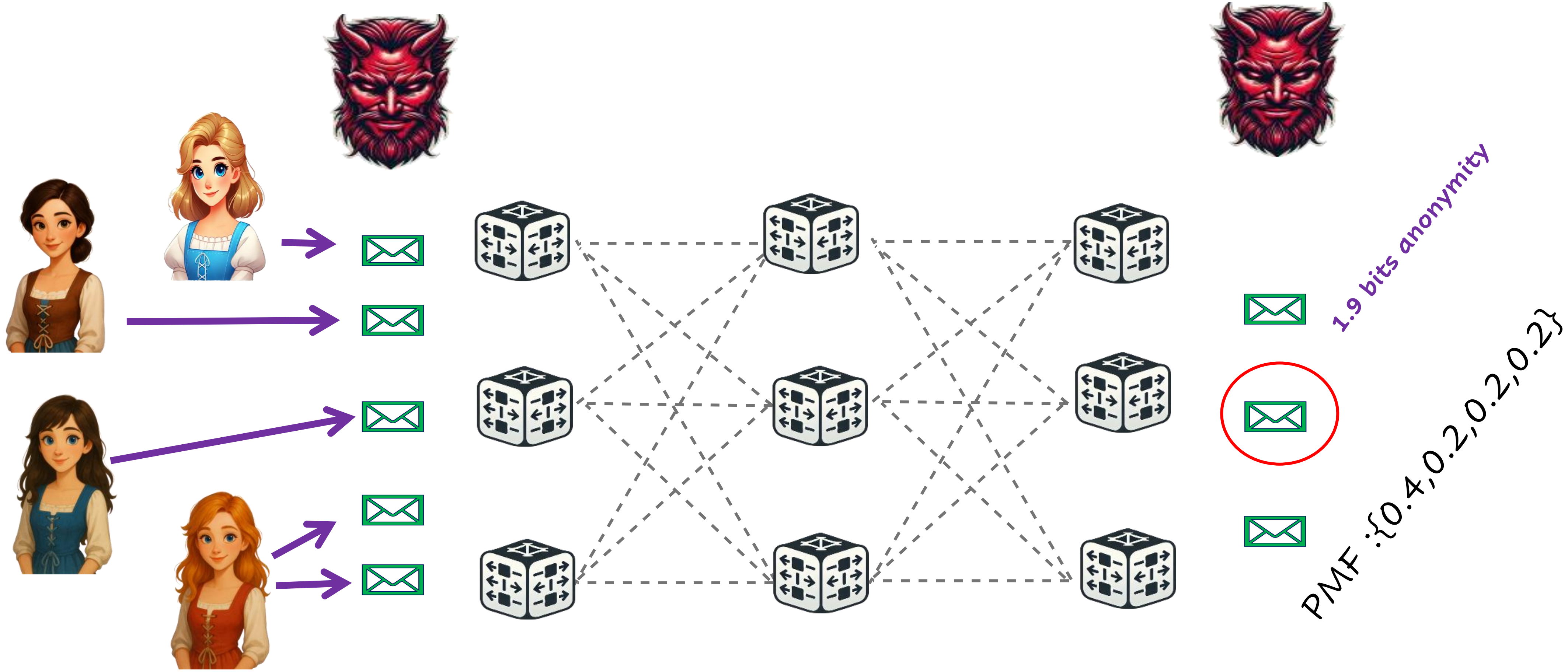
Message anonymity is the state-of-the-art metric for evaluating anonymity in mixnets.

What if one client generates all?



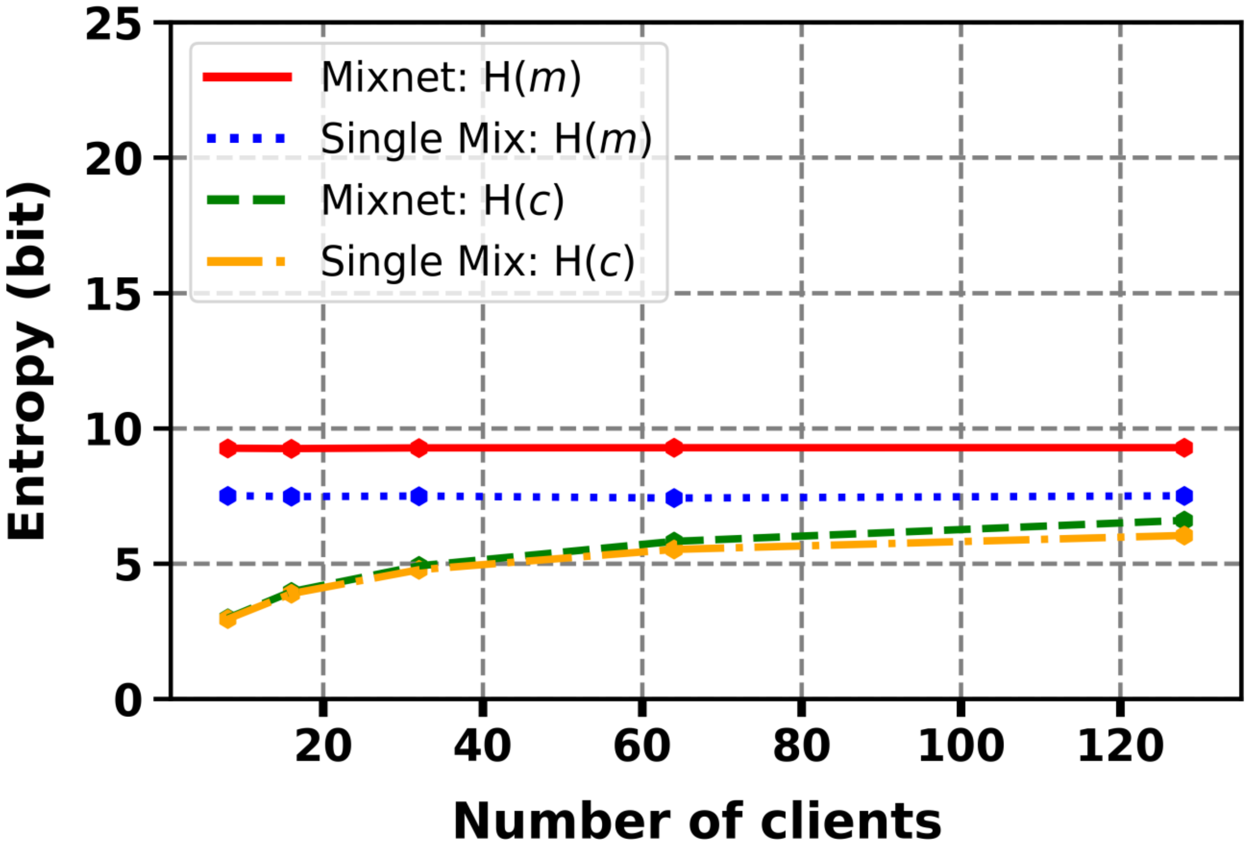
Message anonymity represents an upper bound on the anonymity that can be provided by mixnets.

MOCHA



Client anonymity is an accurate measure of anonymity in mixnets.

Results



The number of clients does not affect message anonymity.

Increasing the number of hops in mixnets does not necessarily increase anonymity.

Message anonymity: H(m).
Client anonymity: H(C).

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.

However, its anonymity should be quantified carefully to avoid misleading or exaggerated anonymity expectations.

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.