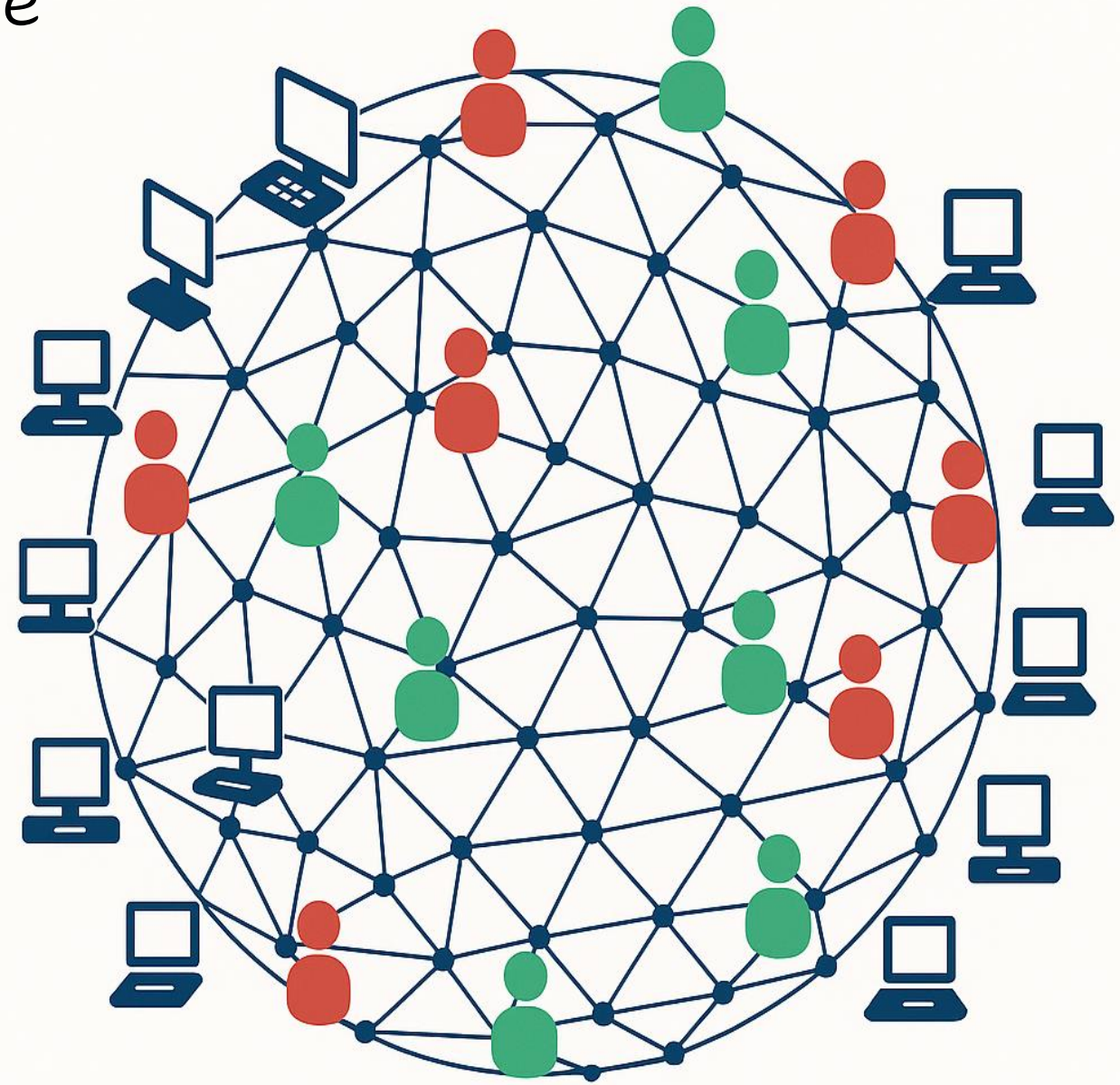
DP-Mix: Differentially Private Routing in Mix Networks



Mahdi Rahimi

mahdi.rahimi@kuleuven.be

COSIC, KU Leuven, Belgium

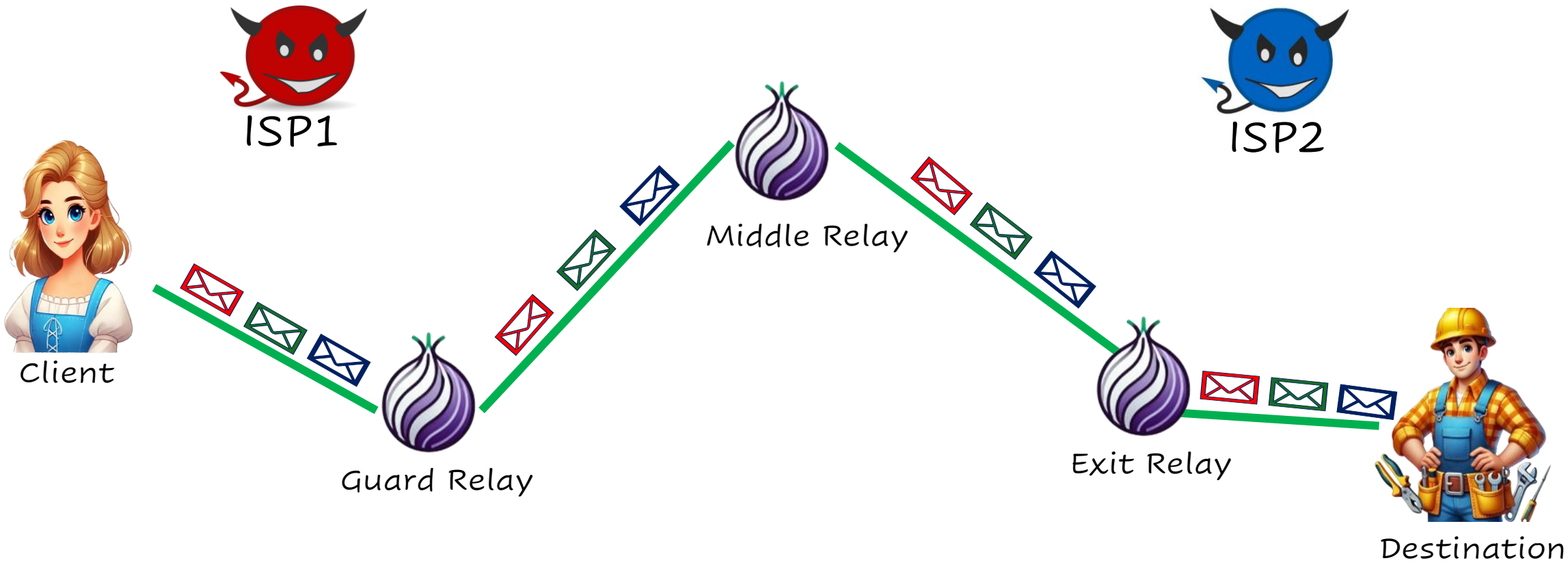
COSIC

41st Annual Computer Security Applications Conference (ACSAC)
December 8–12, 2025, *Honolulu, Hawaii, USA.*

End users on the internet are not anonymized by default.

This creates privacy issues.

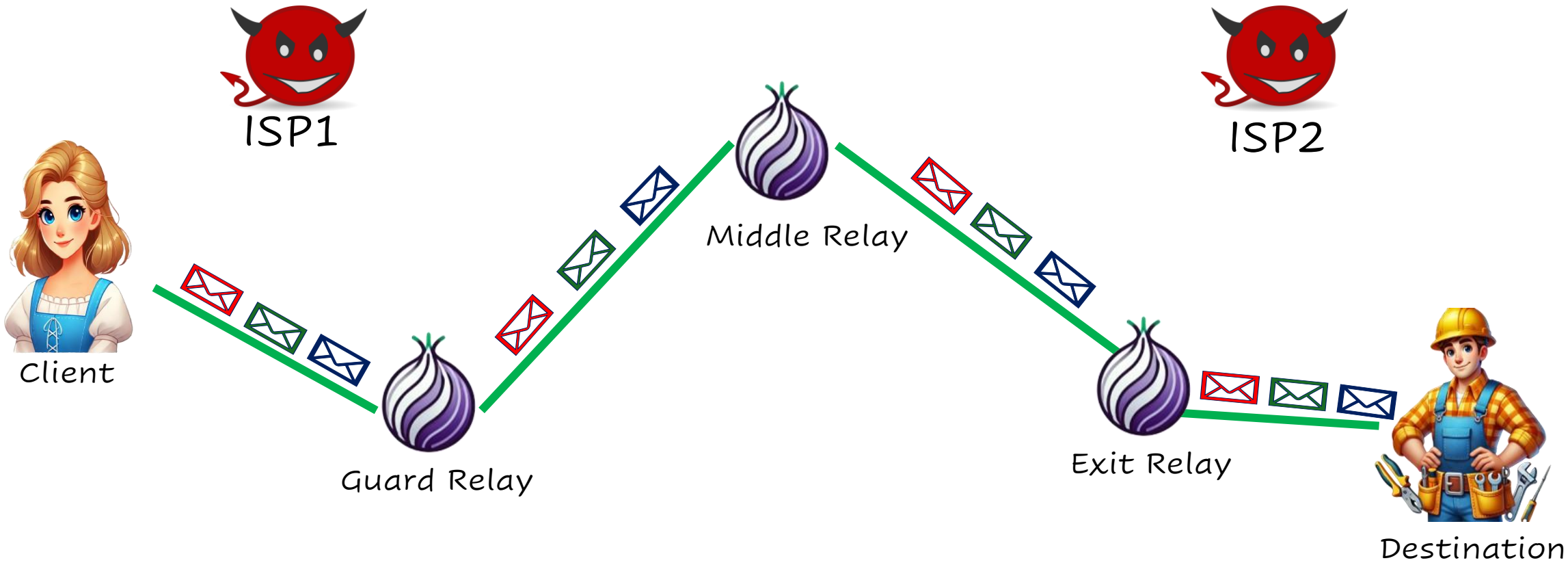
Tor Network



ISP: Internet Service Provider.

ISP1 does not collude with ISP2.

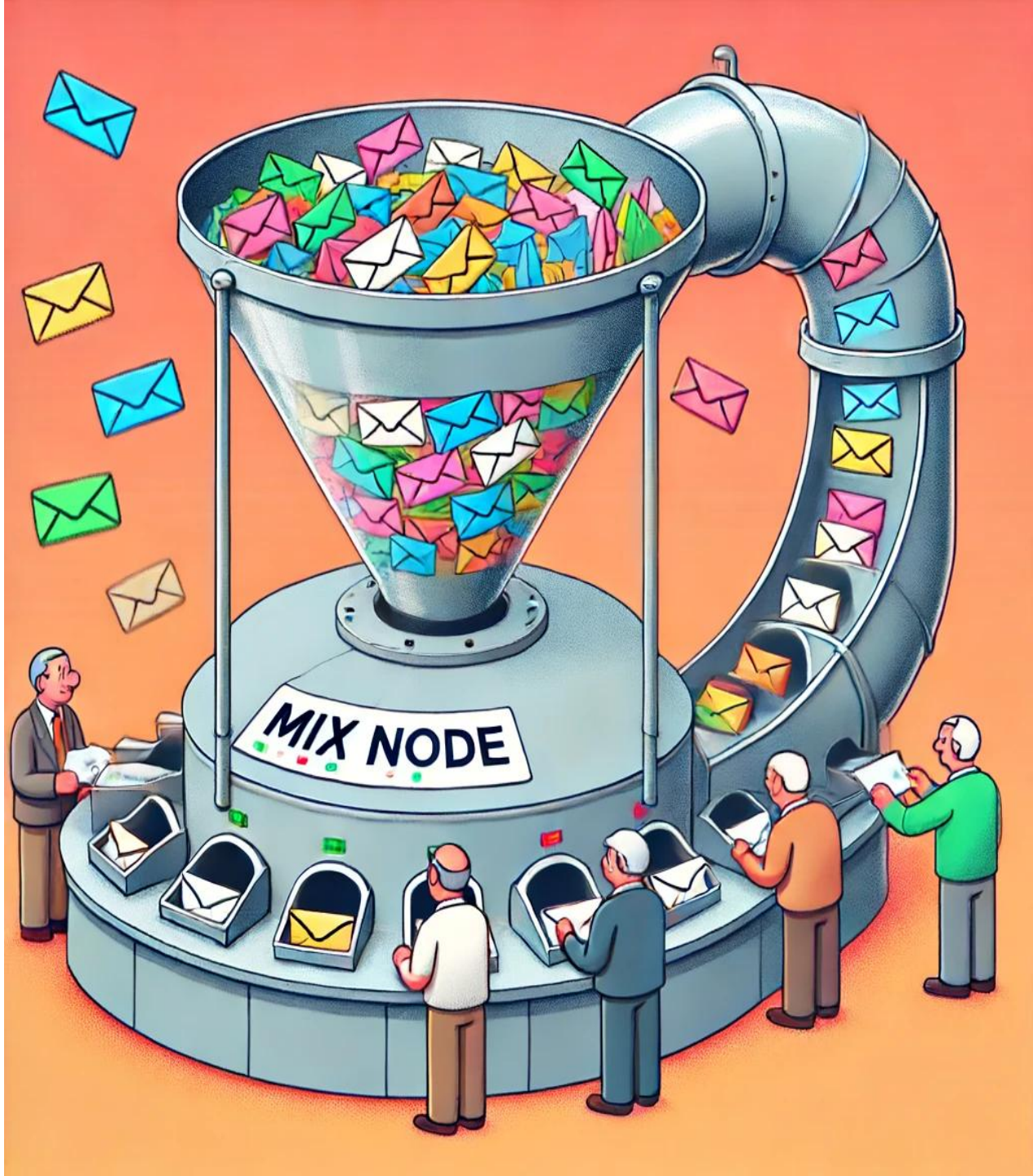
End-to-End Correlation Attacks



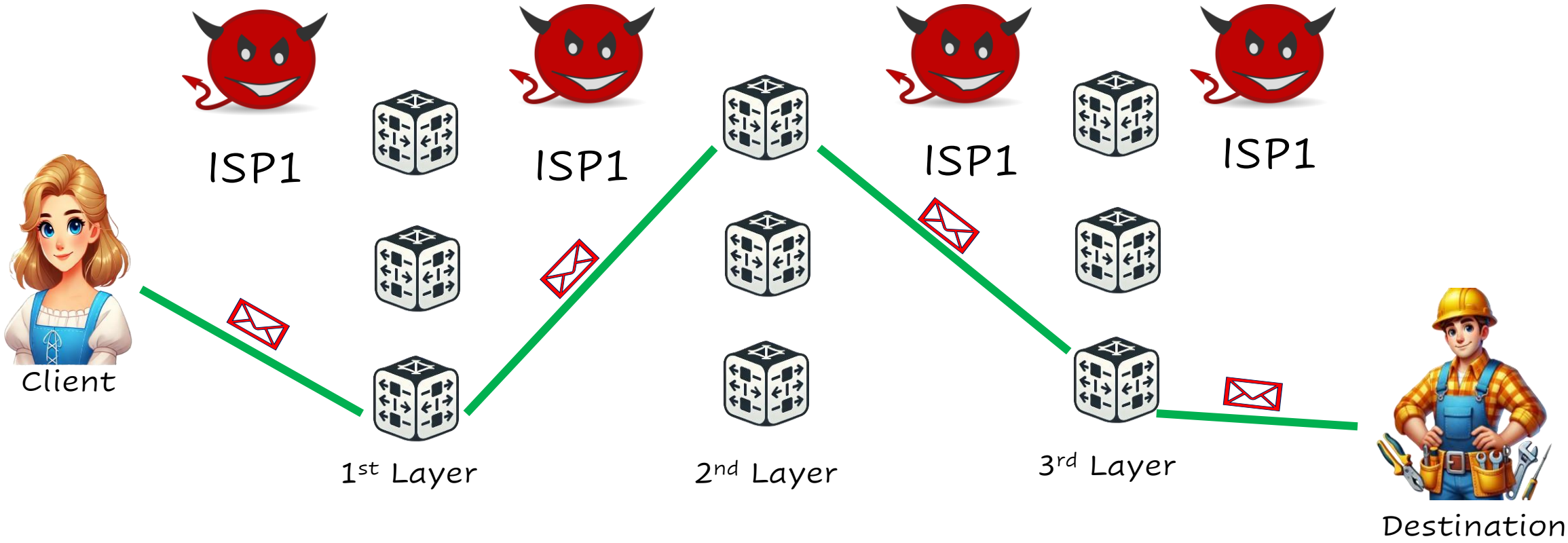
If ISP1 colludes with ISP2, they can deanonymize the client-destination connection.

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

Mixnodes make their input and output unlinkable.

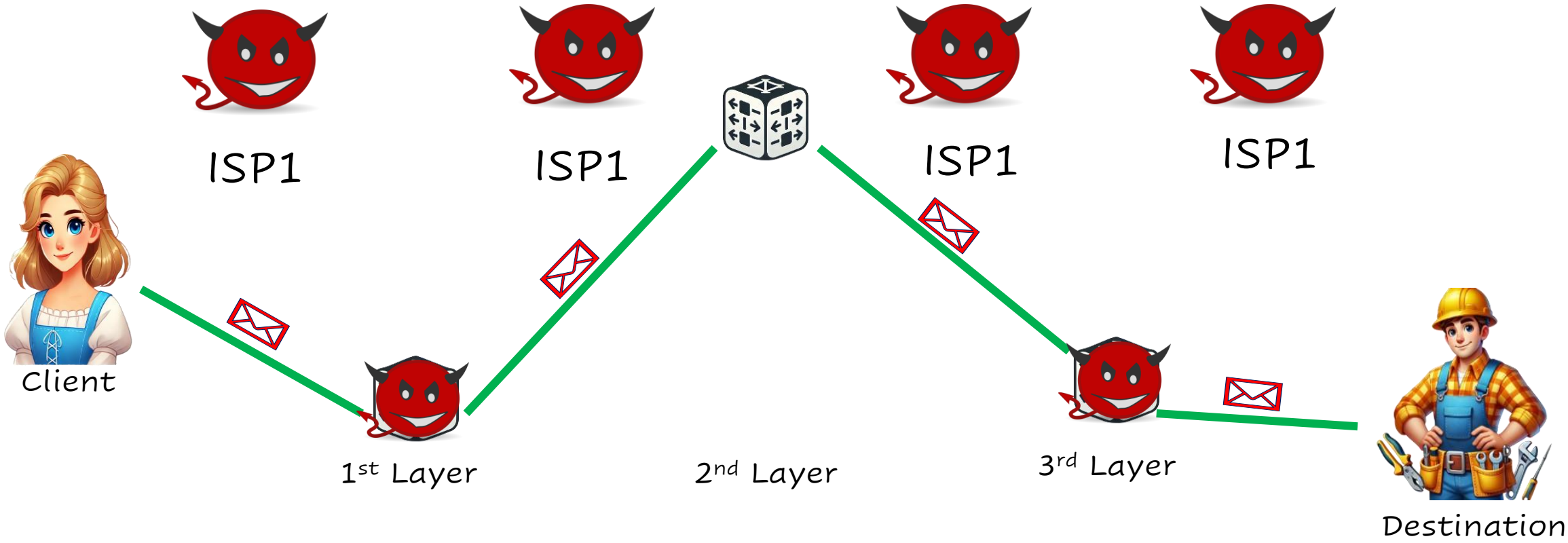


Mix Network (Mixnet)



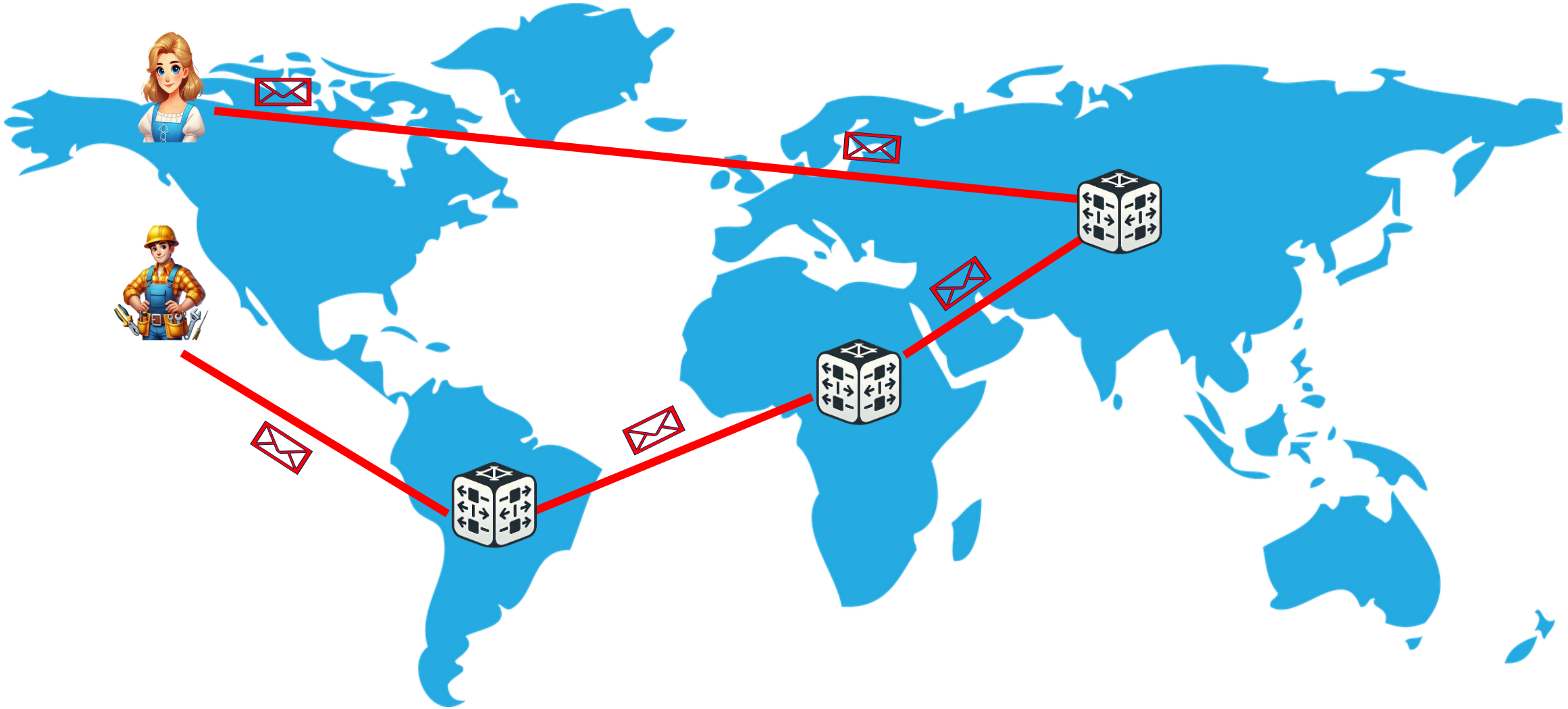
A mixnet is a network consisting of mixnodes, typically arranged in a layered format.

Anonymity Requirement



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

End-to-End Latency



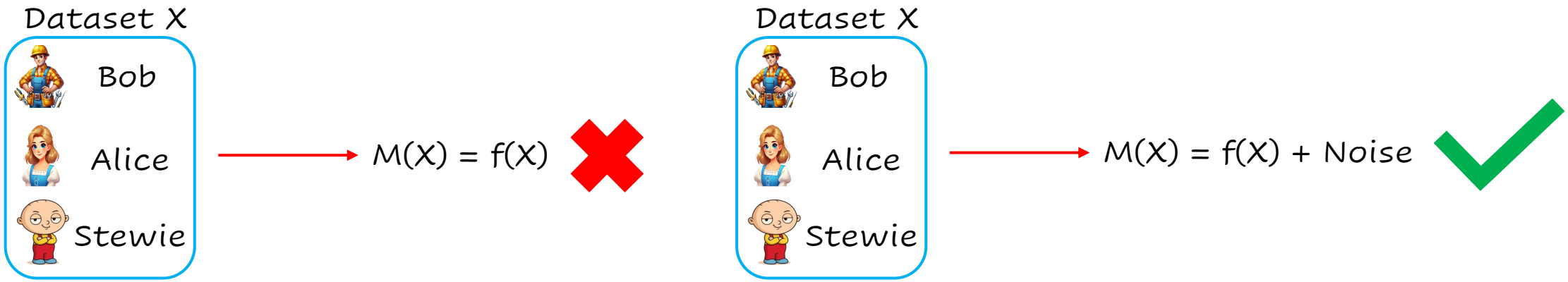
As a result of routing through intermediate mixnodes and mixing delays at each mixnode, the end-to-end latency is high.

Differential Privacy

Dataset X

M(X) = f(X)

Differential Privacy



Differential Privacy

Dataset X


Bob


Alice


Stewie

→ M(X) = f(X) ✖

Dataset X


Bob


Alice


Stewie

→ M(X) = f(X) + Noise ✓

? e^{ε}

Dataset X1


Bob


Alice


Stewie

Dataset X2

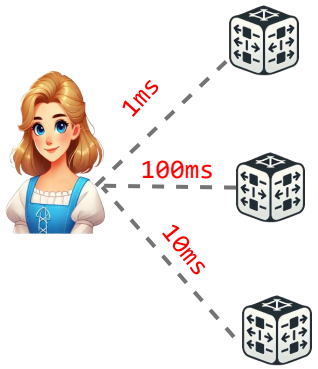

Bob


Alice

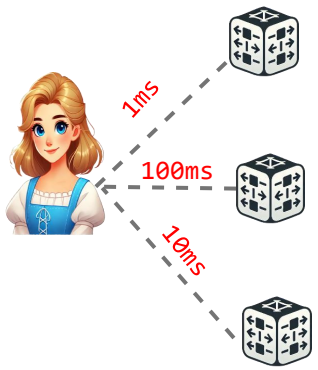

Peter

Differential privacy keeps data private by making sure that adding or removing one person's information doesn't change the analysis results much.

DP-Mix



DP-Mix

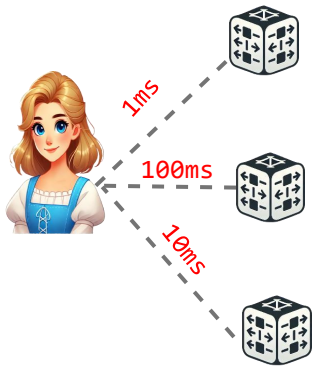


1) Assign scores to each path within the mixnet.

2) Apply the exponential mechanism.

3) Sample a path from the resulting distribution.

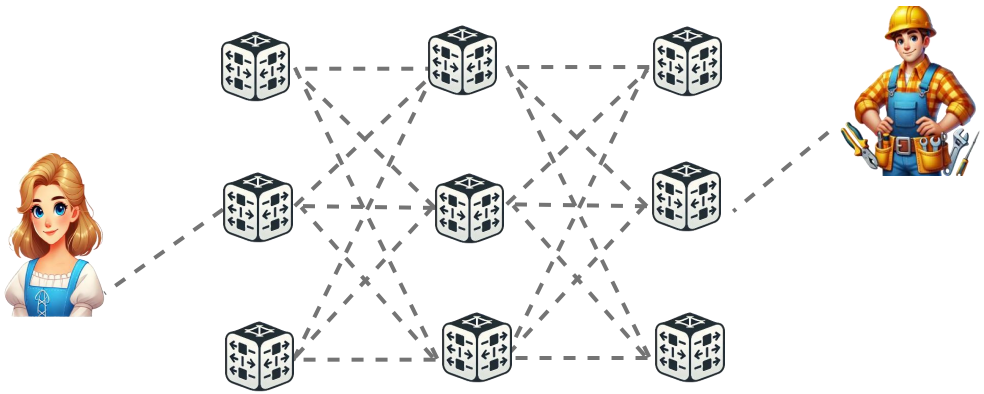
DP-Mix



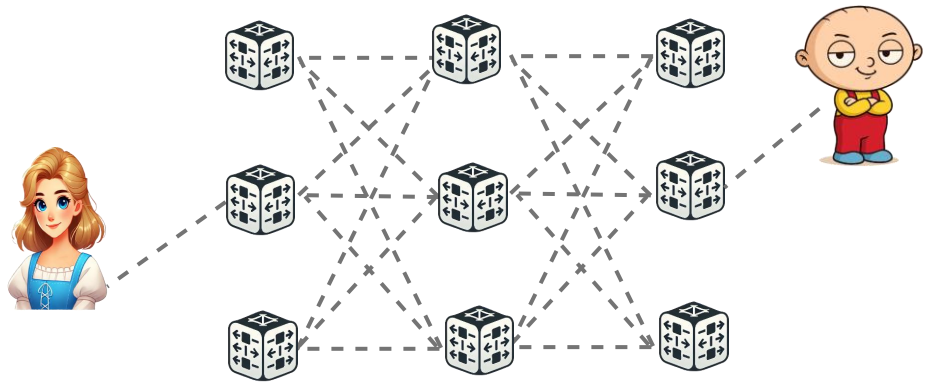
1) Assign scores to each path within the mixnet.

2) Apply the exponential mechanism.

3) Sample a path from the resulting distribution.



1st Scenario



2nd Scenario

DP-Mix can be applied to objectives such as low latency, reliability, and diversity awareness, and has proven to be effective while providing formal DP guarantees.

Results

Approach \ Metrics	Latency (ms)	Privacy loss (ε)
Vanilla setting	240	0
Client-Exit Optimization	60	1.5
End-to-End Optimization	20	3

DP-Mix achieves up to a 75% reduction in latency through client-to-exit node optimization, and up to 92% through full end-to-end optimization, while incurring only a minimal privacy trade-off.

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 DP-Mix which improves the performance of mixnets by up to 92%.

DP-Mix is applicable to other optimization scenarios, including reliability enhancement, congestion avoidance, and similar performance improvements.

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.