HOW TO SPREAD MESSAGES ANONYMOUSLY:

Anonymity matters.

How can we empower people to speak without fear of social or political retribution?

The Problem:
Design a distributed messaging algorithm that:

a) Prevents a powerful adversary from identifying the true message source,

b) Spreads content quickly over contact graphs.

The Adversary:
Colluding “spies” share message contents, metadata, and underlying graph structure to infer message authorship.

Most social networks spread content symmetrically based on user input. (user approves message → message gets passed to friends)

Wildfire is an anonymous messaging app powered by adaptive diffusion.

Adaptive diffusion breaks symmetry to provide strong anonymity.

Intuition: carefully adapt the information flow rate and direction

Theorem: On regular trees, adaptive diffusion lets the source hide among N-1 nodes and spreads the message exponentially quickly.

Simulation: On social graphs and irregular trees, adaptive diffusion hides the source among \( \Omega(N) \) nodes and spreads exponentially quickly.

Provable anonymity guarantees

Remaining challenges

Peek-to-peer dynamic networks

Hiding relays

Multiple message sources

Mobile development

Message caching

Wildfire Release

Fully-distributed implementation

Secure message transmission via Tox

Device-centric architecture

Code at github.com/cpx0rpc/wildfire.git

Advised by Professors Sewoong Oh, Kannan Ramchandran, and Pramod Viswanath