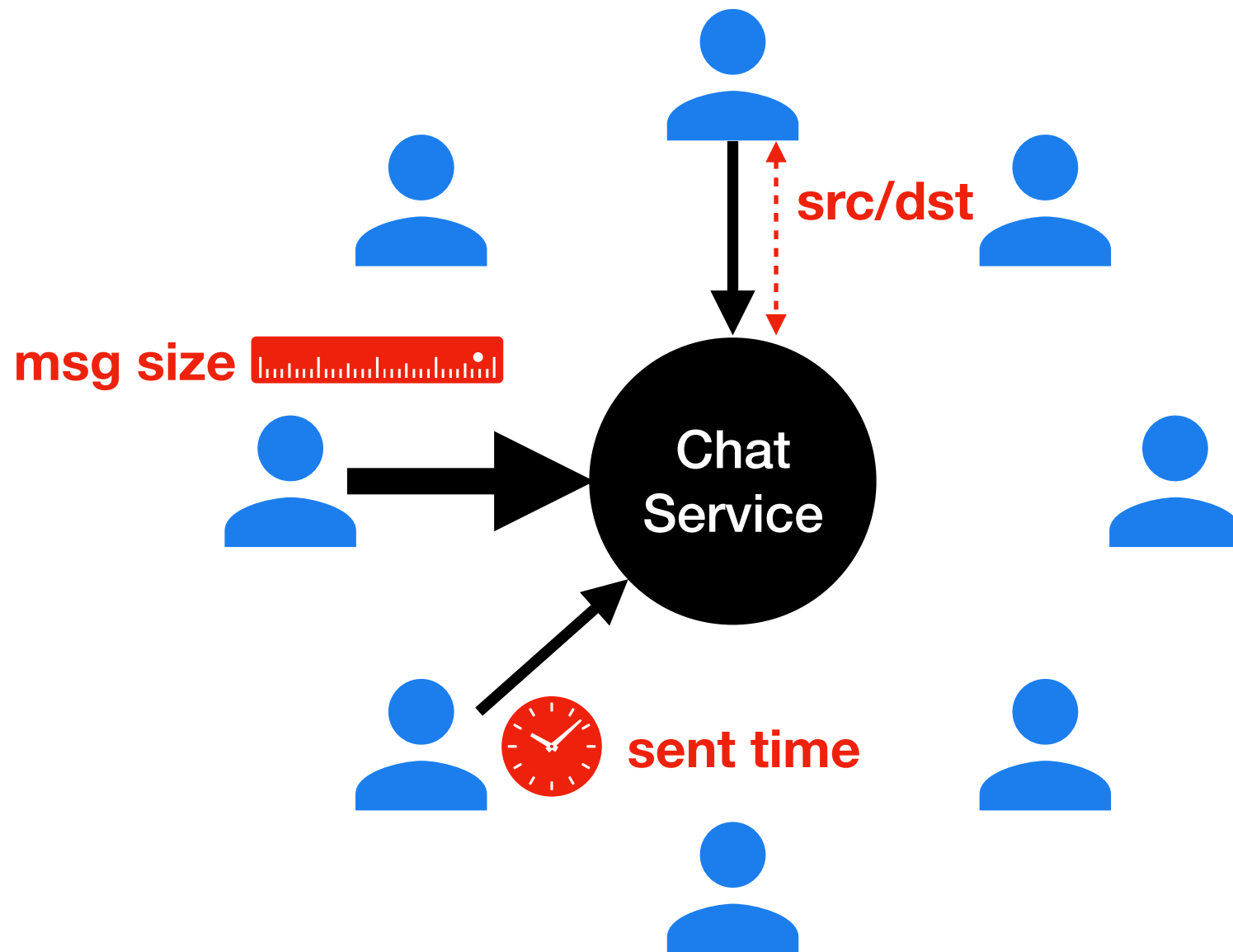


Yodel: Strong Metadata Security for Real-Time Voice Calls

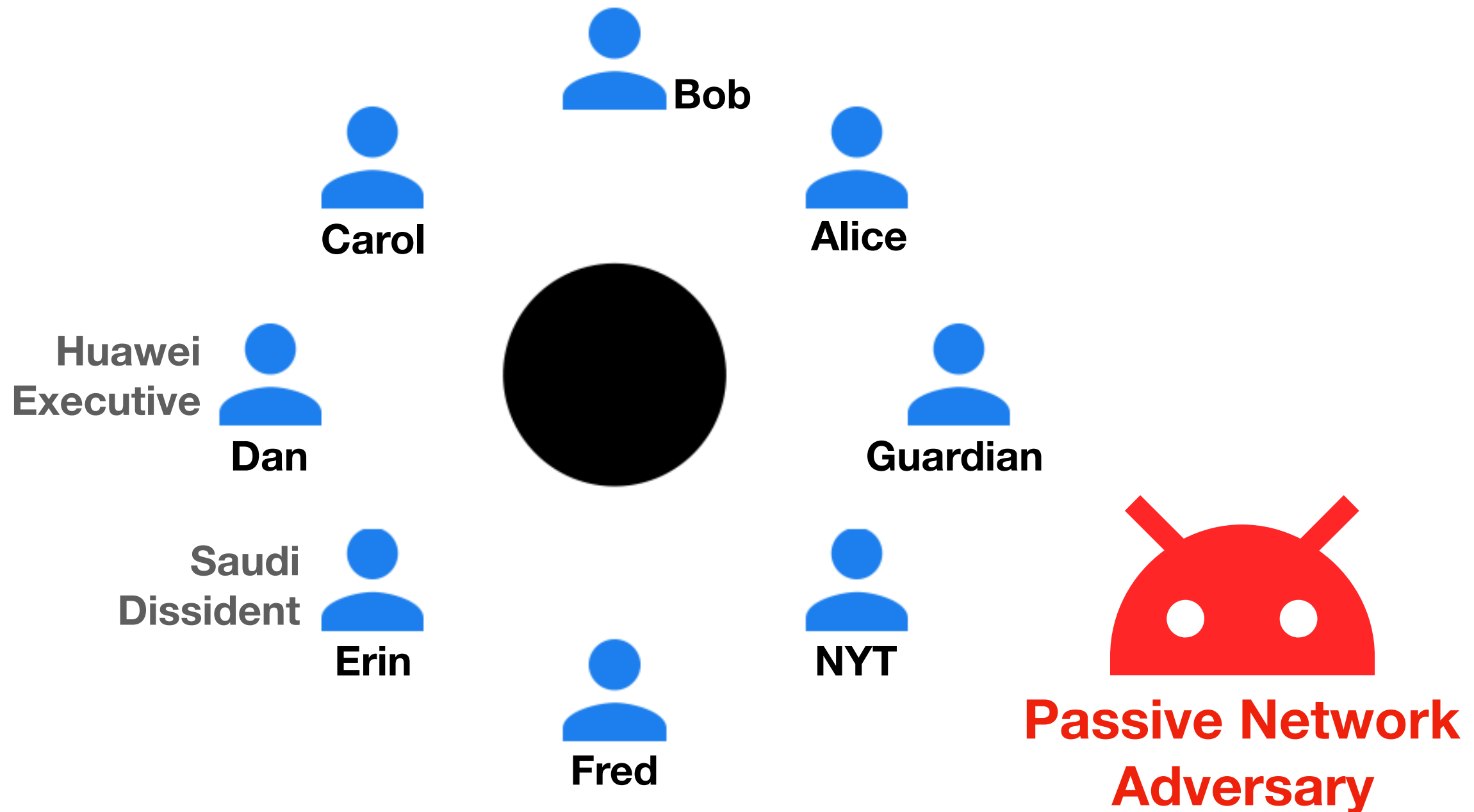
David Lazar, Yossi Gilad, Nickolai Zeldovich

MIT CSAIL

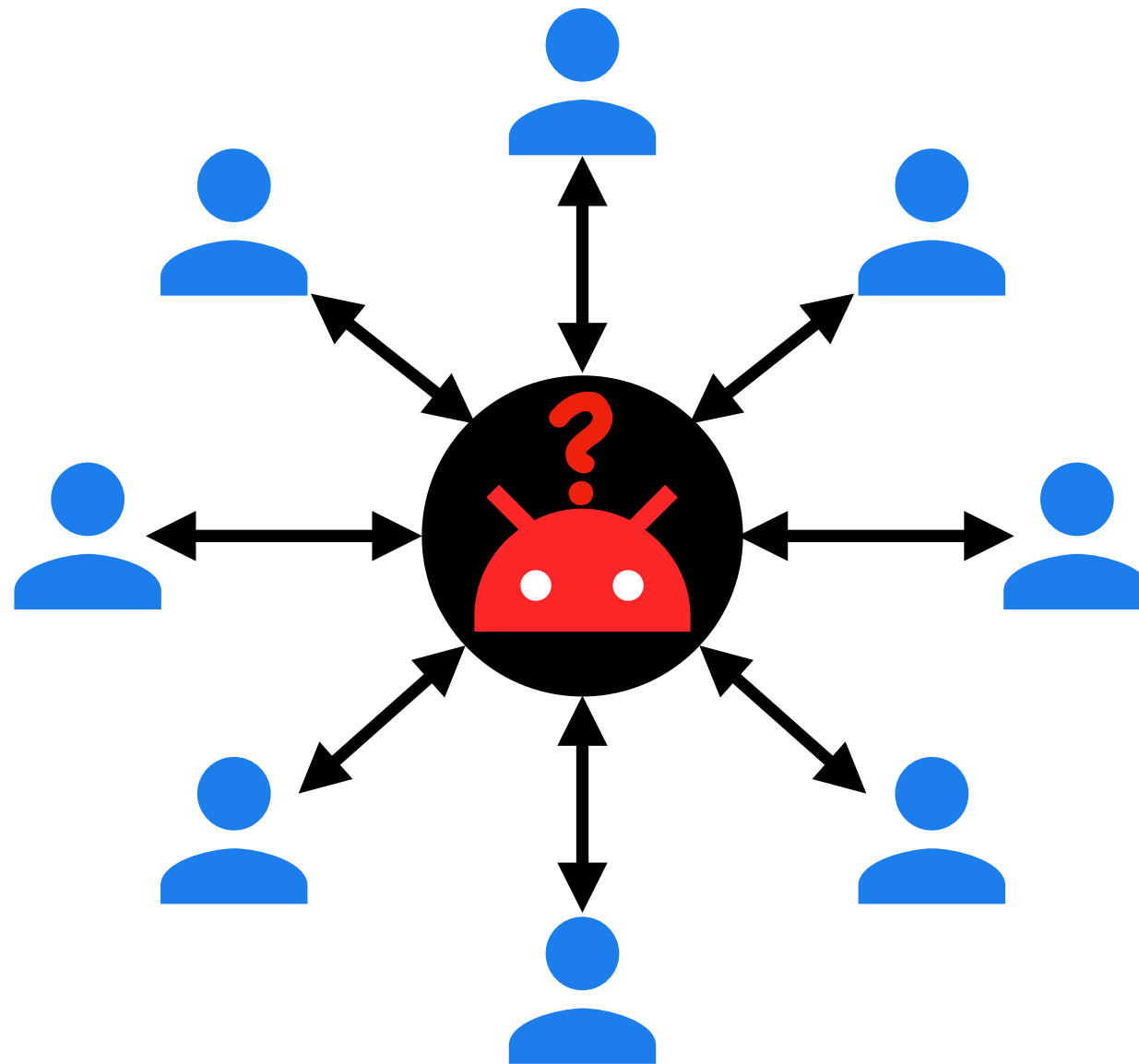
Metadata is data that can't be encrypted



What can you learn from metadata?



Security goal: hide who is talking to whom

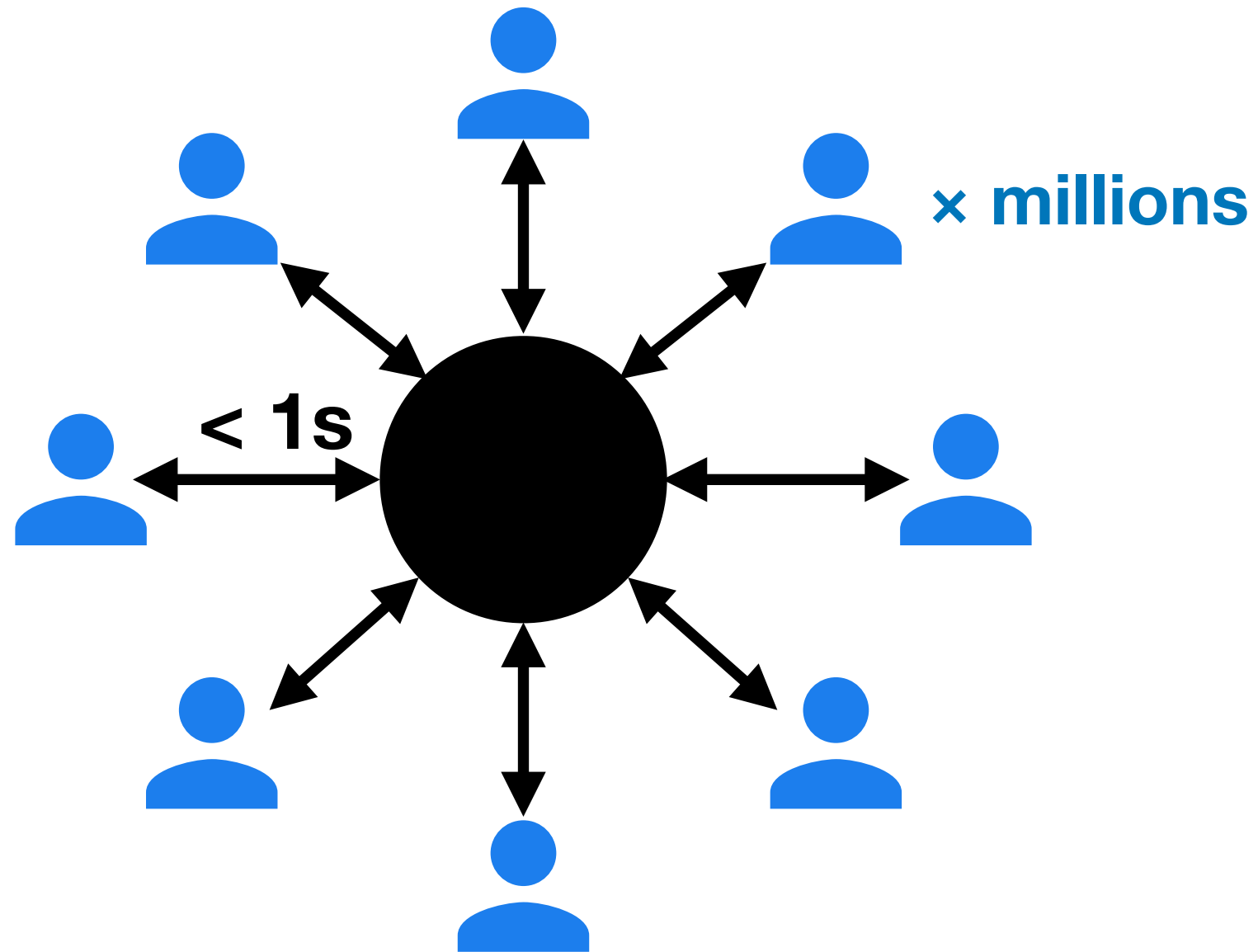


**Active Network
Adversary**

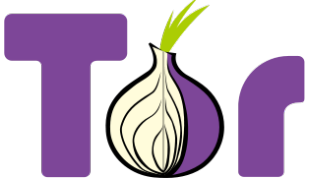














**Passive Network
Adversary**

Performance goal: sub-second latency



Prior work doesn't meet goals

	Passive attacks	Active attacks	Performance
			
Pung [OSDI 2016]			
Karaoke [OSDI 2018]		 Differential privacy	 7s
Herd [SIGCOMM 2015]	 Trusted server		

Contributions

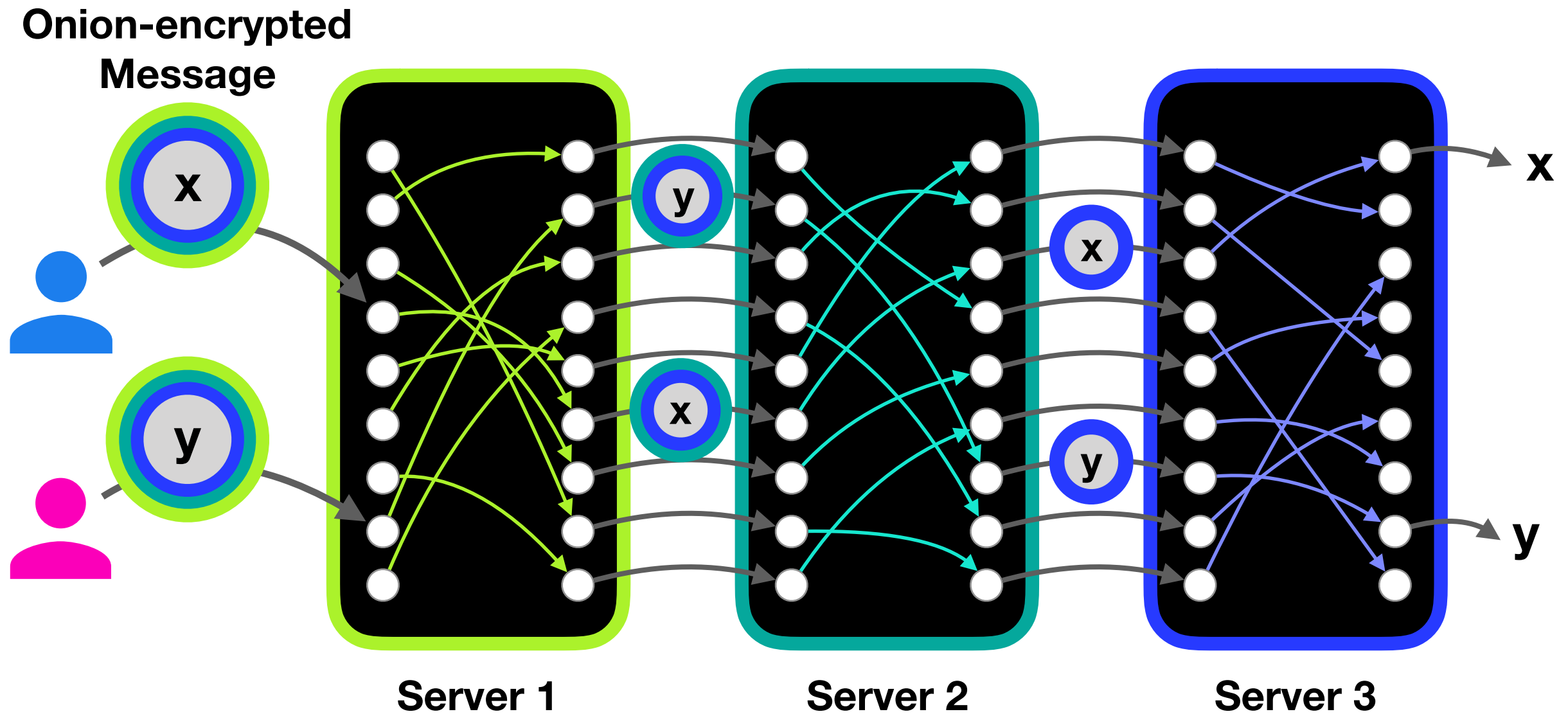
Yodel: the first system for real-time voice calls with

- Strong protection against passive & active attacks
- Distributed trust (any-trust or fractional trust)
- Sub-second latency for 5M users with 100 servers

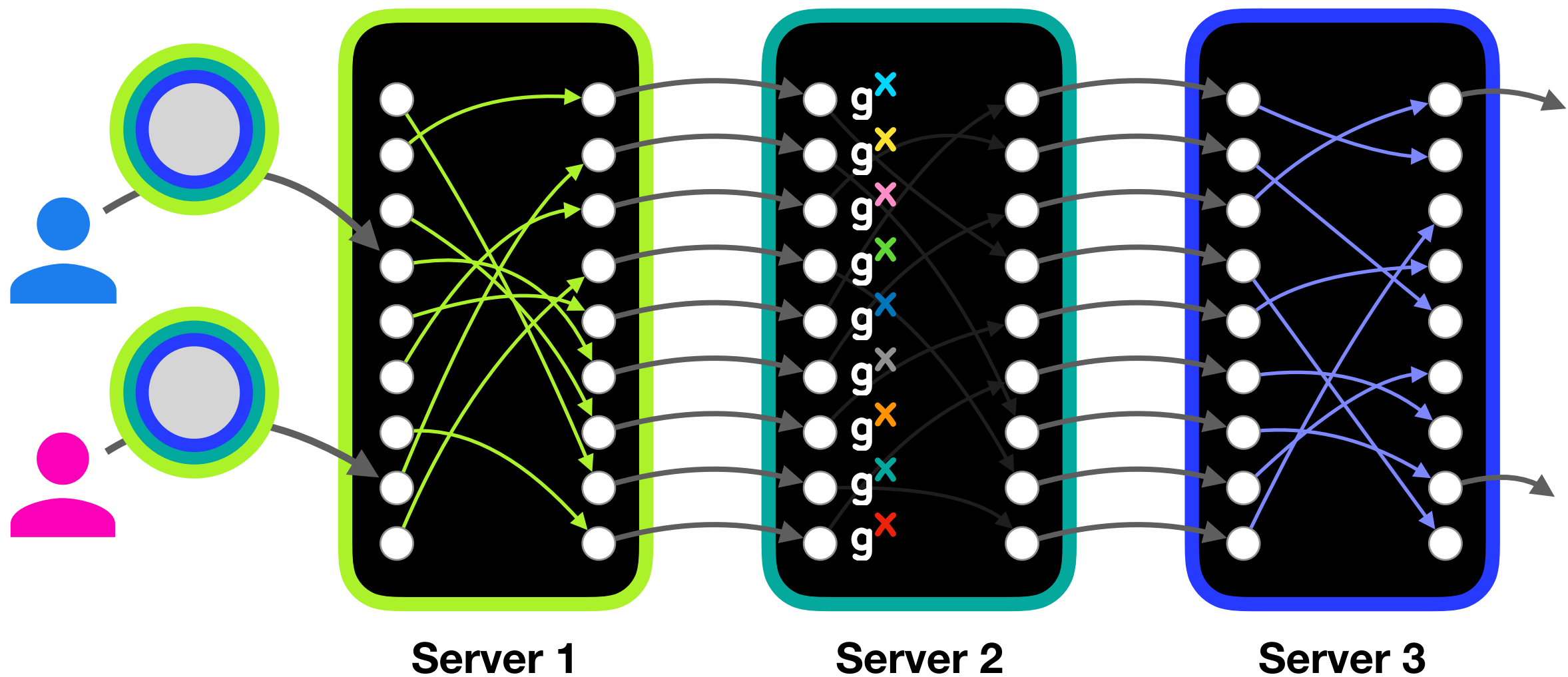
Two key insights

- **Self-healing circuits & Guarded circuit exchange**

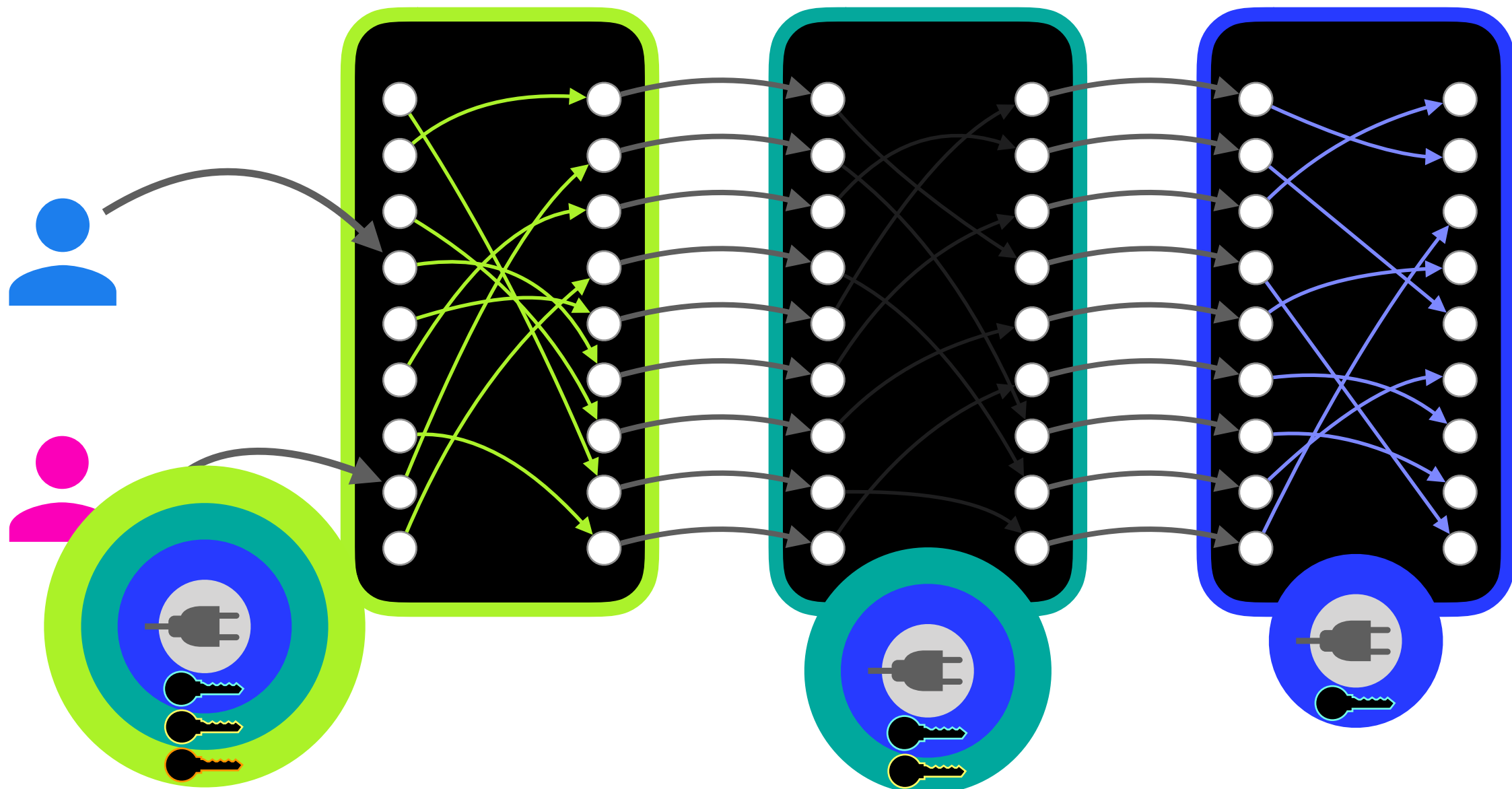
Mixnets hide who sent which message



Mixing is expensive: public key operation for each message at every hop

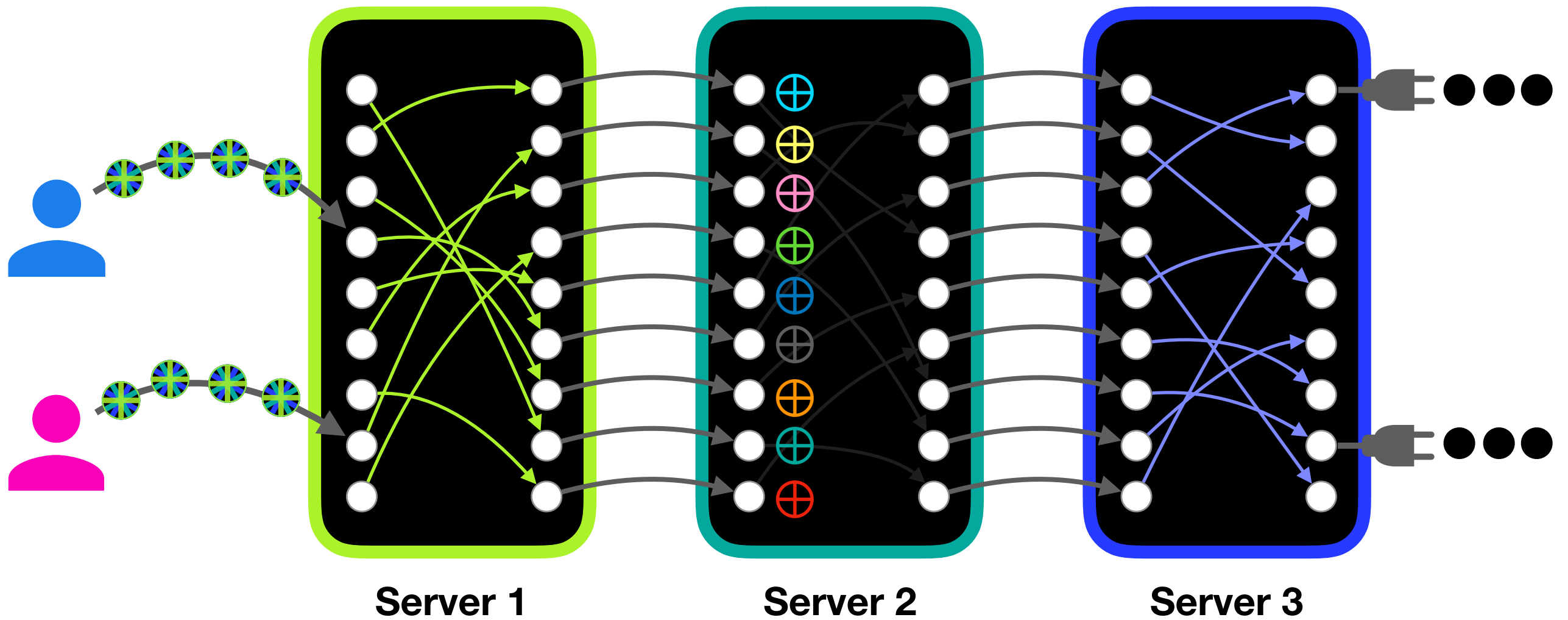


Yodel's mixnet: send public key onions to setup symmetric key circuits



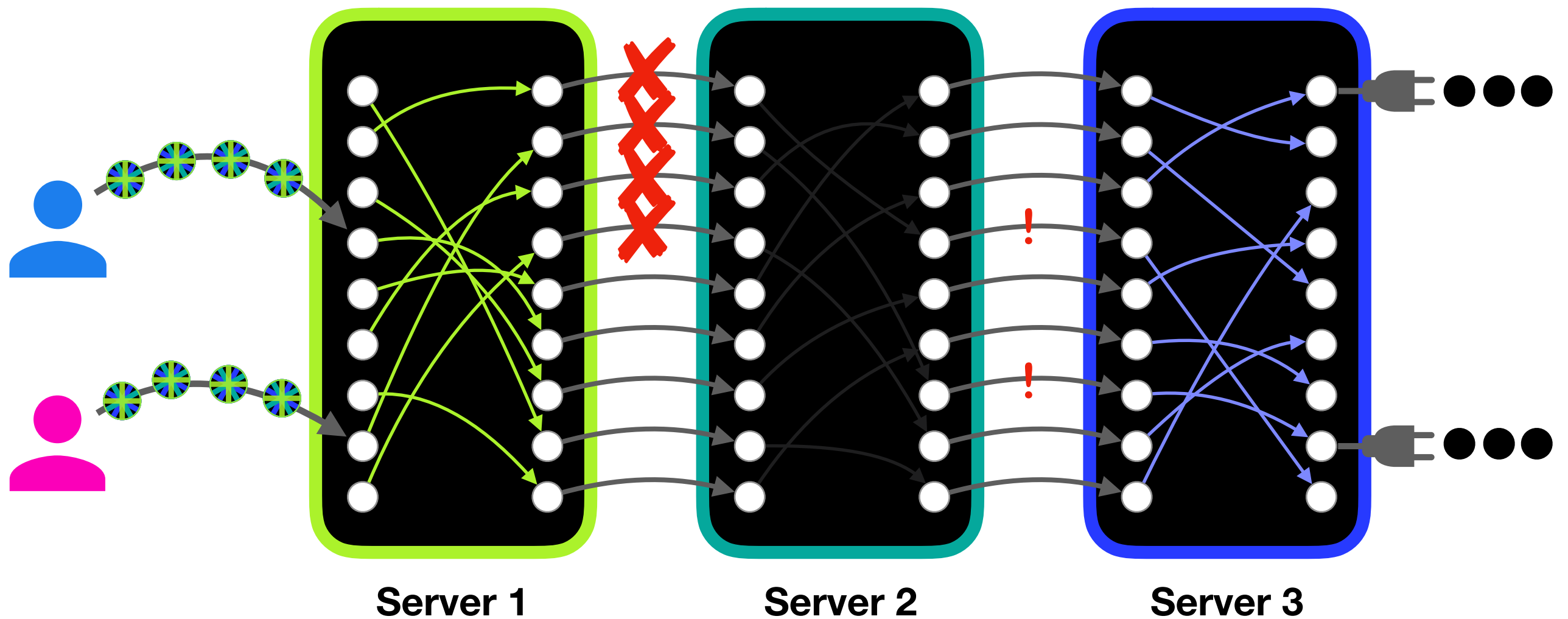
Circuit setup onion

Circuit messaging

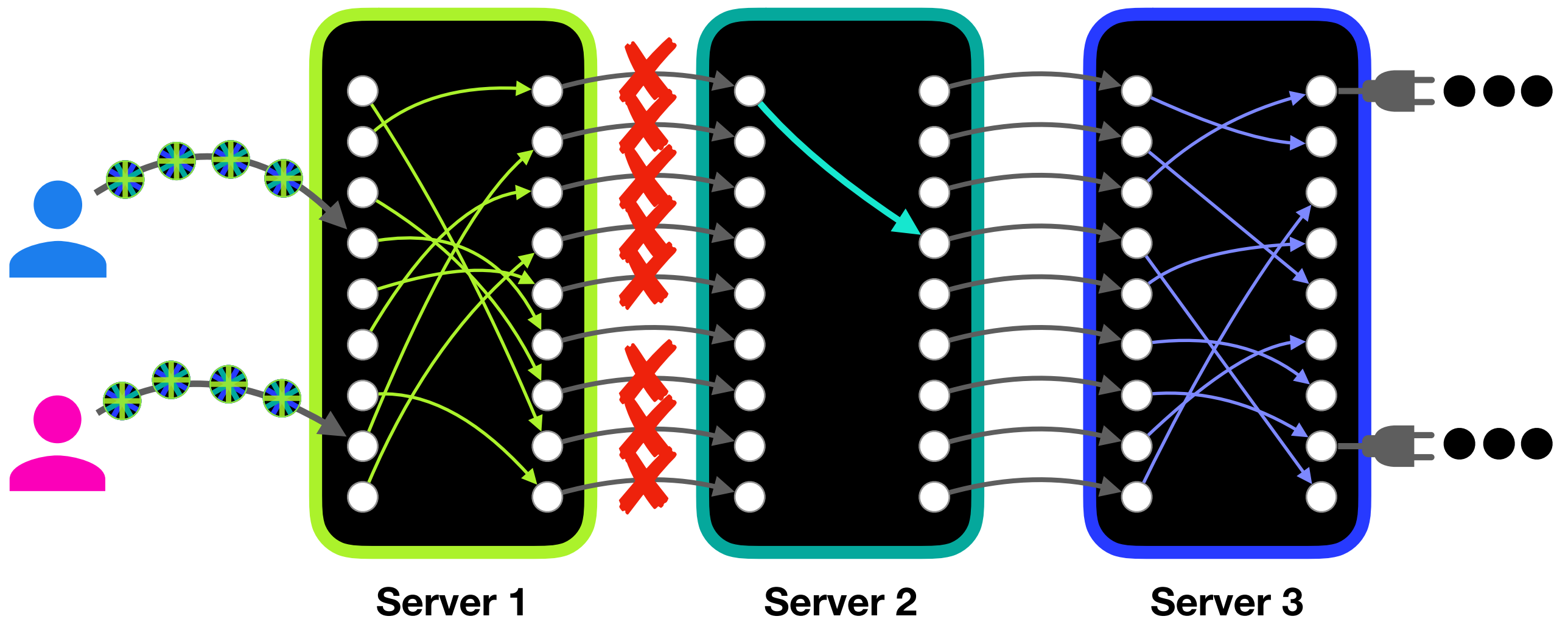


 = circuit (symmetric key) onion

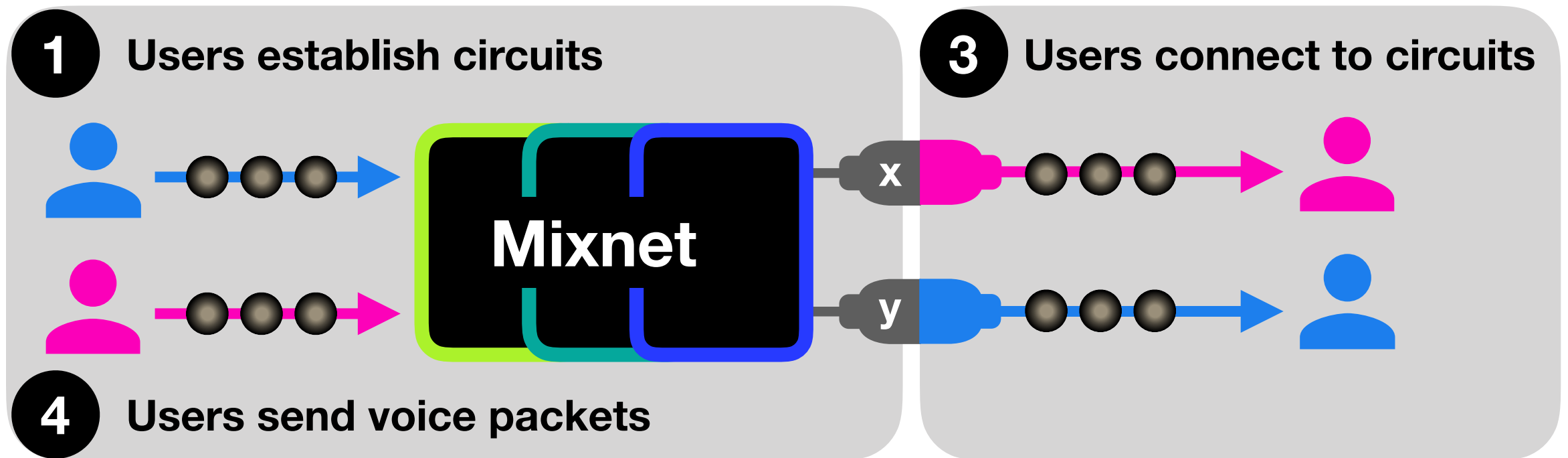
Challenge: attacker has many chances to learn shuffle of honest server!



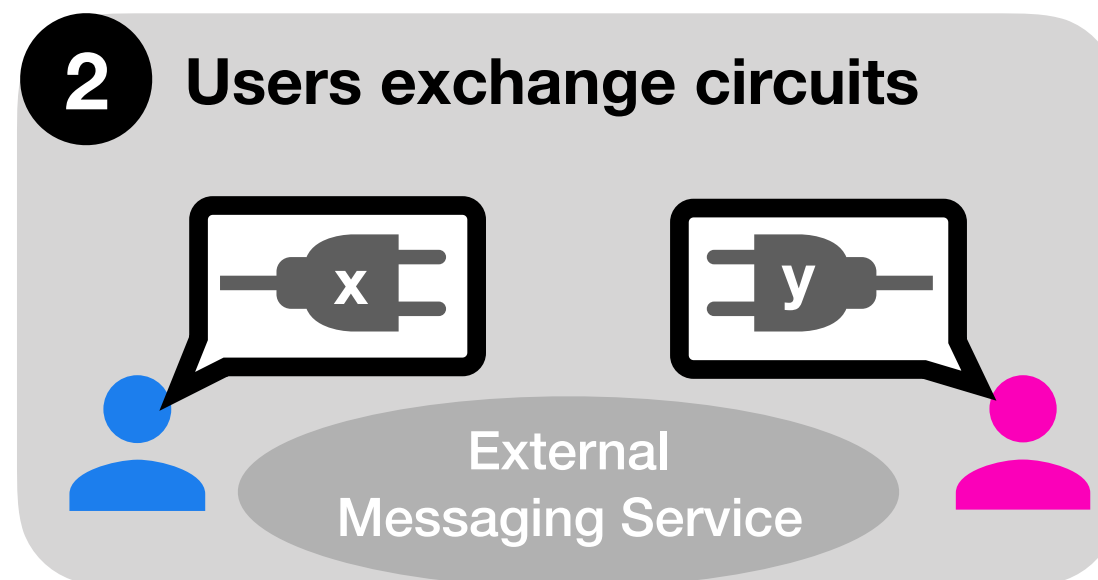
Yodel's key insight: self-healing circuits



Yodel round steps



 = random string

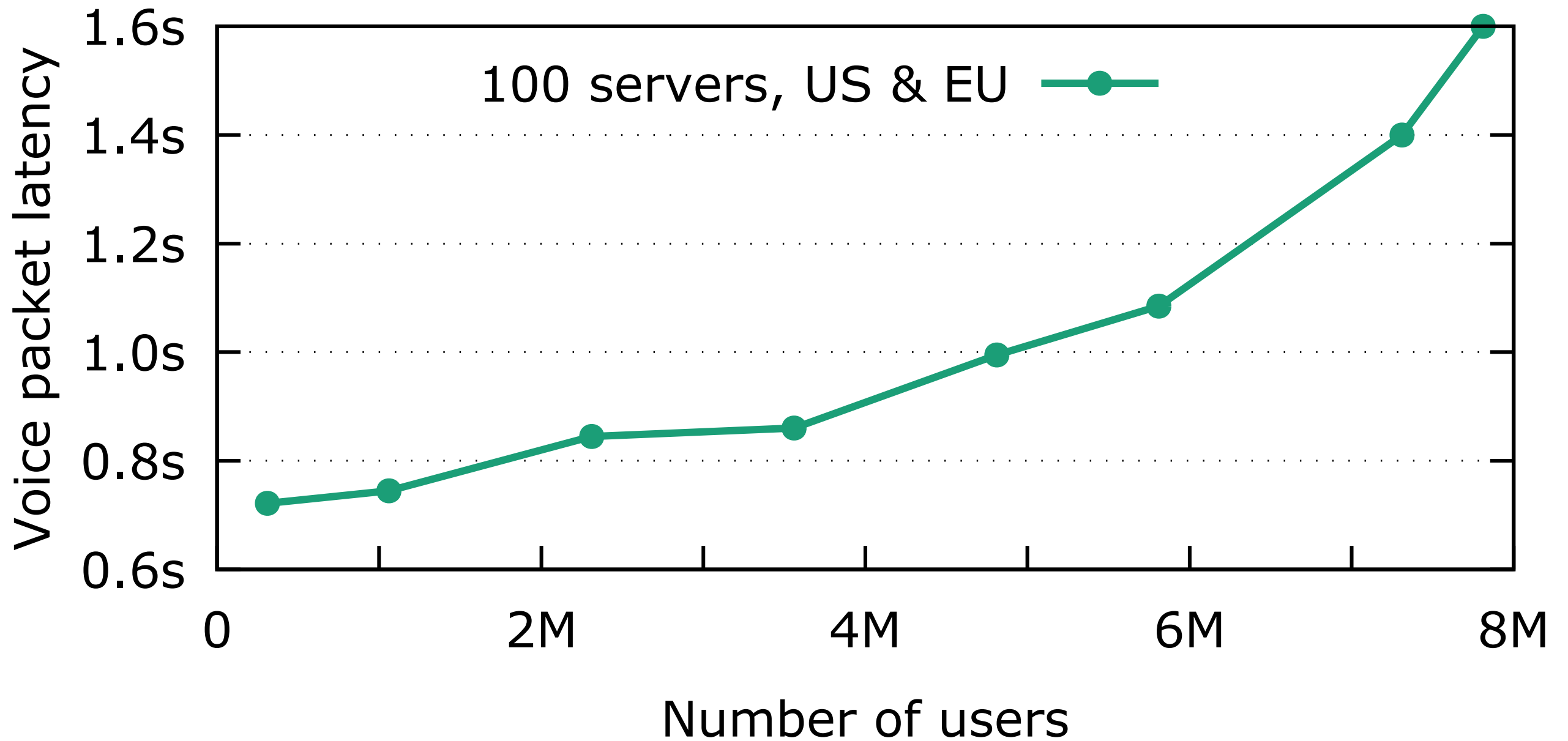


Evaluation

Does Yodel achieve low latency for large numbers of users?

Does Yodel offer acceptable voice quality?

Yodel achieves sub-second latency for 5M users



Yodel achieves acceptable voice quality

- Joanna and I had a short conversation over Yodel, with 5M other “users” actively using the system
- She ran Yodel over her laptop speakers and recorded the convo with her phone
 - (phone records her voice directly)
- Some latency (~1s) is due to us waiting to not talk over each other

Pre-recorded demo

Conclusion

Yodel: the first system for real-time voice calls with

- Strong metadata privacy (against passive & active attacks)
- Distributed trust (any-trust or fractional trust)
- Sub-second latency for 5M users with 100 servers

Full paper and code coming soon:

- vuvuzela.io
- davidlazar.org