CrowdMixer: Differentially Private Anonymous Communications

Alex Yang and Sebastian Angel, University of Pennsylvania

Introduction

When you talk to someone over the internet, no one can see what you're saying. However, surveillance agencies and malicious actors can see who you're talking with and when you are talking. This is known as metadata, which alone can reveal habits, associations, and geographic locations. Metadata is a huge problem for individuals who need to communicate anonymously, such as a government whistleblower or a journalist under a repressive regime.

CrowdMixer is a system that hides user metadata while bringing new capabilities to increase the number of people connected to the system and store messages for a longer period of time. It operates on a mathematically provable standard of privacy known as differential privacy.

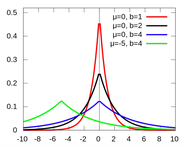
Project Overview

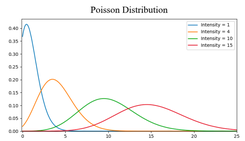
First, CrowdMixer solves the problem of a small user base. Many existing anonymous communications systems are used by a small pool of people, so it is easy for an adversary to infer relationships through tracking all users. CrowdMixer uses a Chrome extension in order to mimic fake communications traffic so it appears to an adversary that more users are connected.

Second, CrowdMixer also solves the issue of storing messages. User A can store a message for up to 6 hours to be picked up by User B, a capability that previously did not exist in the protocol that this system is based off of [1].

Hiding Metadata

We assume that the adversary can see traffic between all users and all servers. Since the adversary can see when users connect to the system, it can correlate user connection times to learn user associations. To prevent this from happening, CrowdMixer users Laplace and Poisson distributions to generate fake messages. The privacy loss is measured by ε and δ, where ε measures information leakage and δ measures how often the system leaks more than ε.



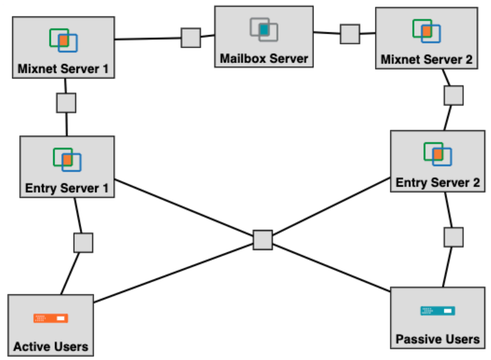


Protocol

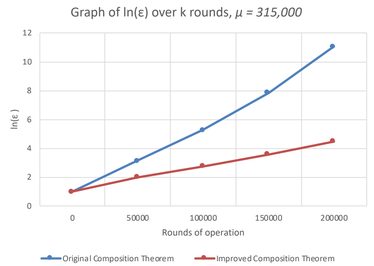
CrowdMixer is composed of entry servers, mixnet servers, and a mailbox server. For User A to send a message to User B, both users send a message to each entry server. The entry servers add fake messages and randomly shuffle the order of the requests before sending the messages to the mixnet servers. The mixnets take in the input messages, add more noise, and perform another random shuffle. The mailbox server exchanges User A's and User B's messages and returns them down the chain so that they arrive at their destination.

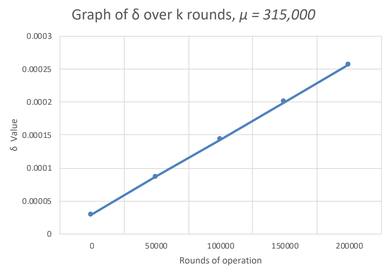
Each chain of the server network only needs to generate half of the total required fake messages, which decreases the computational load on a single server and decreases the time it takes for messages to be processed in the system.

Server Topography



Privacy Degradation





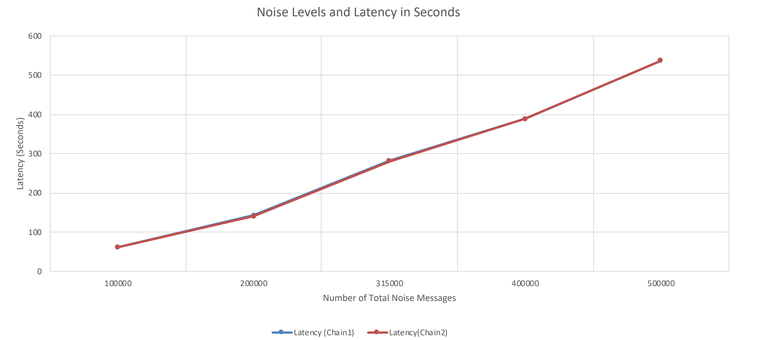
Graph 1 and 2: These graphs represent the degradation of privacy over time. The privacy leakage remains small even after 50,000-100,000 rounds so users can continue to communicate securely.

Results and Discussion

Each server generates on average 157,000 fake messages, which allows for the system to be used continuously for 5.7 years before privacy guarantees degrade to unacceptable levels. Our use of an improved composition theorem[3] allowed us to increase this time by 260% over the previous composition theorem[4].

The amount of fake messages can be decreased proportionally to the number of passive users that are connected to the system. Combined with our distributed server architecture, message processing time were relatively low, with an average of 286.86 seconds collected over 10 trials.

Overall, our system maintains $\varepsilon < \ln(2)$ and $\delta < 1\text{x}10^{-4}$ bounds for privacy leakage over k = 50,000 rounds.



Graph 3: Relationship between increased average noise levels and latency

Conclusions and Future Work

- Bootstrapping existing anonymous communications systems to increase the size of the anonymity set is simple and effective
- Adding capabilities for non-ephemeral communications increases the sensitivity linearly, causing a linear increase in the necessary noise
- A more distributed server topography significantly improves latency

There are several improvements that could explored in future research:

- Making the server network more distributed as to decrease vulnerability to DDoS attacks
- Statistical model fitting to determine better distributions to use
- Expanding the number of concurrent user connections

Contact

Alexander Yang
Distributed Systems Lab, University of Pennsylvania
Email: ayang015@seas.upenn.edu
Phone: 651-280-7946

References

1. J. van den Hooff, D. Lazar, M. Zaharia, and N. Zeldovich. Vuvuzela: Scalable private messaging resistant to traffic analysis. In Proceedings of the ACM Symposium on Operating Systems Principles (SOSP), Oct. 2015.
2. Lazar, D., Gilad, Y., & Zeldovich, N. (2018). Karaoke: Distributed Private Messaging Immune to Passive Traffic Analysis. *OSDI*. Retrieved from https://www.usenix.org/conference/osdi18/presentation/lazar
3. Kairouz, P., Oh, S., & Viswanath, P. (2015). The Composition Theorem for Differential Privacy. *MLR* . Retrieved from http://procee4dings.mlr.press/v37/kairouz15.pdf
4. Roth, A., & Dwork, C. *The Algorithmic Foundations of Differential Privacy* (Vol. 9).
5. Sommer, D., Dhar, A., Malisa, L., Mohammadi, E., Ronzani, D., & Capkun, S. (2017). CoverUp: Privacy Through "Forced" Participation in Anonymous Communication Networks. *The International Association for Cryptologic Research*. Retrieved from https://eprint.iacr.org/2017/191.pdf