The Ins and Outs of Anonymous Group Communication

Christoph Coijanovic Daniel Schadt Thorsten Strufe

KASTEL Security Research Labs, Karlsruhe Institute of Technology

Abstract

Group communication is ubiquitous in today's internet. Mainstream services expose highly personal metadata, such as who is communicating with whom, to service providers and other potential observers. In response, many anonymous group communication networks (AGCNs) have been proposed that use cryptographic building blocks to enable communication without disclosing metadata. The great variety of proposed AGCNs makes selecting the right approach for a given use case non-trivial. In this talk, we give a thorough introduction of the problem and solution space of anonymous group communication. Through a series of toy protocols, we present the main approaches and discuss tradeoffs between them.

Motivation Whether through group chats in Signal or WhatsApp, bulletin boards such as X or BlueSky, or video conference services such as Zoom, online group communication is ubiquitous. Even the most privacy-sensitive topics, such as personal health [6] and sexual preferences [8], are now commonly discussed online. Fortunately, end-to-end encryption has become the default in most mainstream communication platforms [9], preventing anyone expect the sender and intended receiver of a message to learn information about its content. However, end-to-end encryption alone cannot protect the *metadata* of communication, such as who is communicating with whom, how often, and when. It is well established that metadata can be as privacy-sensitive as the message content itself [2].

To enable group communication without metadata disclosure, a plethora of anonymous group communication networks (AGCNs) have been proposed starting in the 1980s [1]. Proposed AGCNs differ greatly in their functionality, underlying primitives, privacy guarantees, and overhead. Without an in-depth understanding of the problem and solution spaces, it is difficult to select the appropriate protocol for a given use case or design future AGCNs.

Understanding Anonymous Group Communication We compile the findings of our recent systematization of knowledge on anonymous group communication [10] to provide an overview of the different approaches and their

tradeoffs. There are three main areas where AGCNs make differing design choices:

First, there exist different functionalities under the umbrella of (anonymous) group communication. There are anonymous publish/subscribe systems, where senders associate their messages with topics to which receivers can subscribe. In Sender-Multicast systems, the sender can define a set of receivers for each message. Other systems assume predefined groups within which messages are broadcast or provide public bulletin boards to which messages can be sent.

Second, AGCNs differ in the privacy goals they aim to achieve. In many cases, AGCNs define their privacy goals ad-hoc and specific to their use case. This complicates comparisons between protocols. In our SoK, we define a set of four formal game-based privacy notions adapted from Kuhn et al.'s work in the unicast setting [3]. Our privacy notions express all common privacy goals in ACGNs and intuitively test, whether an adversary can link...

- ...honest senders to the message they send (Message Unlinkability)
- ...honest senders to their sending activity (Activity Unlinkability)
- ...senders or messages to honest receivers (Receiver Unlinkability)
- ...senders or messages to the number of honest receivers (Receiver Count Unlinkability)

AGCNs differ in which privacy notions they (aim to) achieve and against which adversary (e.g., global network adversary, malicious servers, malicious group members) they achieve them.

Third, to provide their intended functionality and achieve the desired privacy goal, systems rely on different underlying privacy primitives. For example, to achieve Receiver Unlinkability, a system could be based on mix networks, private information retrieval (PIR), or secret-sharing-based private write. The choice of primitive impacts the realizable functionality, adversary against which the privacy notion can be achieved, as well as the performance of the system.

Research and Talk Within our research group, we have experience in both designing AGCNs ourselves [7, 4, 5] as well as analyzing alternative approaches from our recent SoK. In this talk, we will leverage this experience to provide an in-depth introduction to the topic. The first part of the talk will introduce our set of formal privacy notions of AGCNs and the relevant primitives to understand the design space. We will then use the primitives to construct a series of toy protocols to highlight differences in approaches and to discuss tradeoffs between them.

References

[1] David Chaum. “The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability”. In: *J. Cryptol.* 1.1 (1988), pp. 65–75. DOI: 10.1007/BF00206326.

[2] Jonathan Mayer, Patrick Mutchler, and John C Mitchell. “Evaluating the privacy properties of telephone metadata”. In: *Proceedings of the National Academy of Sciences* (2016).

[3] Christiane Kuhn et al. “On Privacy Notions in Anonymous Communication”. In: *Proc. Priv. Enhancing Technol.* 2019.2 (2019), pp. 105–125. DOI: 10.2478/POPETS-2019-0022.

[4] Sarah Abdelwahab Gaballah et al. “2PPS - Publish/Subscribe with Provable Privacy”. In: *40th International Symposium on Reliable Distributed Systems, SRDS 2021, Chicago, IL, USA, September 20-23, 2021*. IEEE, 2021, pp. 198–209. DOI: 10.1109/SRDS53918.2021.00028.

[5] Christoph Coijanovic et al. “Pirates: Anonymous Group Calls over Fully Untrusted Infrastructure”. In: *Information Security and Privacy - 29th Australasian Conference, ACISP 2024, Sydney, NSW, Australia, July 15-17, 2024, Proceedings, Part III*. Ed. by Tianqing Zhu and Yannan Li. Vol. 14897. Lecture Notes in Computer Science. Springer, 2024, pp. 193–212. DOI: 10.1007/978-981-97-5101-3_11.

[6] Elham Hatef et al. “Effectiveness of telehealth versus in-person care during the COVID-19 pandemic: a systematic review”. In: *npj Digit. Medicine* 7.1 (2024). DOI: 10.1038/S41746-024-01152-2.

[7] Daniel Schadt et al. “PolySphinx: Extending the Sphinx Mix Format With Better Multicast Support”. In: *IEEE Symposium on Security and Privacy, SP 2024, San Francisco, CA, USA, May 19-23, 2024*. IEEE, 2024, pp. 4386–4404. DOI: 10.1109/SP54263.2024.00044.

[8] Germano Vera Cruz et al. “Online dating: predictors of problematic tinder use”. In: *BMC psychology* (2024).

[9] Rune Fiedler and Felix Günther. “Security Analysis of Signal’s PQXDH Handshake”. In: *Public-Key Cryptography - PKC 2025 - 28th IACR International Conference on Practice and Theory of Public-Key Cryptography, Røros, Norway, May 12-15, 2025, Proceedings, Part II*. Ed. by Tibor Jager and Jiaxin Pan. Vol. 15675. Lecture Notes in Computer Science. Springer, 2025, pp. 137–169. DOI: 10.1007/978-3-031-91823-0_5.

[10] Christoph Coijanovic, Daniel Schadt, and Thorsten Strufe. “SoK: Anonymous Group Communication”. In: *Upcoming* (2026).