A Survey of Sender Anonymity in Messaging and Communication

Sahil Basia
Indian Institute Of Technology Kanpur
Kanpur, Uttar Pradesh, India
sahilbasia8@gmail.com

Adithya Vadapalli
Indian Institute Of Technology Kanpur
Kanpur, Uttar Pradesh, India
avadapalli@cse.iitk.ac.in

ABSTRACT

In this era of the digital world, where communication happens digitally, the anonymity of senders has become a critical aspect of privacy and security. This survey paper explores the various angles of sender anonymity in messaging and communication systems and discusses the methods and technologies used to ensure that the identity and privacy of users remain anonymous and hidden, respectively, from intermediate tracker parties. We have reviewed the cryptographic techniques, routing protocols, and secure infrastructures, which aim to provide sender anonymity. This paper will also provide a comprehensive analysis that will showcase the advancement achieved in achieving the sender's anonymity.

KEYWORDS

Anonymity, Cryptography, Communication, Sender anonymity, Secure Messaging, Multi-Party Computation

1 INTRODUCTION

In today's digitalized world, where data tracking and privacy concerns are very ubiquitous, the aim of achieving the sender's anonymity in communication systems becomes critically essential. A safe and anonymous communication system ensures that individuals send messages without exposing their identities and protects them from interference from surveillance organizations. These anonymous systems provide a platform for whistleblowers, and activists the freedom of speech in systems where everything is tracked by intermediate parties.

Sender anonymity depends on two critical concepts: untraceability and unlinkability The untraceability ensures that no one can trace the message to the source of the message, whereas unlinkability ensures that if multiple messages are sent from the same individual, an adversary cannot link them together to get the original message. These ensure long-term anonymity, especially in areas where communication over non-anonymous channels happens prominently.

Traffic analysis is one the most common attacks where intermediate parties or adversaries try to study the pattern of message timings, message size, etc. Even if the messages are encrypted, using the above information, adversaries can reveal the sender's identity. However, technologies like mix networks and onion routing protocols are used to disrupt these patterns, and thus can add an extra layer of protection to the sender's identity.

Another key feature that can be implemented to achieve the sender's anonymity is deniability. This allows the sender to deny a particular message sent by the user, thus providing protection against coercion. The anonymous system ensures that if someone tries to prove the source of the message, then the system does not retain any identifiable evidence to prove the source of the message. This technique ensures that even if the sender's identity gets revealed, his past messages will remain untraceable or unidentifiable to adversaries.

However, achieving sender anonymity involves a lot of challenges. One of the most difficult challenges is to achieve anonymity and accountability hand in hand. Some communication systems require traceability to prevent fraud or illegal activities, for eg. in areas like finance or illegal shops. Therefore, protocols can be implemented that selectively trace the information whenever necessary without compromising the anonymity of legitimate users.

In the cases where the anonymity of the recipient is also needed, the task of achieving the sender's anonymity becomes more complex. Now, the system has to ensure neither party's identity is compromised. Furthermore, as the scalability of messaging systems grows, challenges such as collusion attacks rise.

In this survey paper, our aim is to provide a comprehensive analysis of various research papers that have been published in the field of sender anonymity in messaging and communication. The analysis will summarize the cryptographic protocols used, tools or technologies used, etc, to achieve the goal of sender anonymity.

2 METHODOLOGY

In this survey research, we carried out a thorough review of the research papers on "sender anonymity in messaging and communication." To collect research papers, we followed the best academic tools and research resources available online. We further used "Connected Papers" to find more relevant papers in the required domain. We picked one of the papers published in top-1 tier Computer Security Conferences, and searched in connected papers to find more applicable papers. The connected papers platform helped us visualize the graph of connected papers, thus ensuring we get all key contributors.

Below are the steps of our methodology:

1. We first gathered the relevant papers that majorly discuss the anonymity of the sender in messaging or communication. This ensures that all the papers that are selected are directly linked to the main topic of our survey.

2. After collecting the relevant papers, we then filtered the collected papers based on their publication in top-tier conferences. The papers from top conferences were prioritized to ensure that the research of those collected papers had gone through a strict review process and, therefore, would represent contributions to the major field.

Secure Computation Project Report 2024(I), 1–7

https://doi.org/XXXXXXX.XXXXXXX

3. We further focussed majorly on papers that introduced some new unexplored tools, protocols, and decentralized network systems for secure, anonymous communication. This ensures that the survey provides a wide view of the latest advancements in the domain of sender anonymity in messaging and communication.

Following this structured approach allowed us to highlight the latest advancements in tools, protocols, and techniques that are used to achieve the major goal. Also, it provided us with enough information to produce a comprehensive analysis of the technologies used in each paper referenced.

3 RELATED WORK

Jordan Yuen Jia Jun, et al. [15] (2024) presented ChatAlone, an anonymous messaging application for enhanced privacy that aims to provide user privacy in messaging and open communication. The app provides sender anonymity by using localized Bluetooth-based communication and requires no personal information registration while using the app. The app also provides the feature of setting random usernames, thus allowing users to communicate without disclosing their identities. ChatAlone further leverages the sender's anonymity by using no centralized server and stores all the data locally on the user's device using Hive.

Adithya Vadapalli, et al. [13] (2022) introduced Sabre: Sender-Anonymous Messaging with Fast Audits, which focuses on improving the anonymity of senders in messaging or communication. The authors have used Distributed point function[DPFs] techniques to ensure sender anonymity while allowing fast, scalable audits to detect any malicious behavior or message tampering. Along with DPFs, authors have used secure multi-party communication techniques, thus improving users' anonymity. The authors have also discussed the system design saber in both of the sender-anonymous bulletin-board model (Sabre-BB) and the sender-anonymous mailbox model (Sabre-M). An auditing protocol has been implemented to detect any malicious behavior by checking whether the DPF keys are well-formed or not. This auditing protocol implemented by authors works in $O(\lambda \lg n)$ work to the $O(\lambda n)$ work required by Riposte and Express auditing,

Christoph Coijanovic, et al. [2] (2023) proposed Panini — Anonymous Anycast and an Instantiation, that addresses an unexplored communication called anonymous anycast system that enhances sender and recipient anonymity. The system aims to protect the identity of the sender while also ensuring that the message sent by the sender is delivered to one of many possible recipients in the group and no information about the recipient is shared with the sender in this process. The system uses linkable ring signatures to verify the keys of the receiver without revealing the identity of the receiver. The system/protocol relies on Nym mixnet infrastructure that hides the IP address and traffic patterns and thus making the communication channel anonymous.

John P. Podolanko, et al. [9] (2017) developed LiLAC: Lightweight Low-latency Anonymous Chat, which ensures that users can send messages anonymously. The system implements a low-latency anonymous communication system using onion routing and dependent-link padding. The onion routing uses anonymous relays, which keep the identity of the user anonymous. The dependent link padding ensures that adversaries cannot detect the pattern of timing and volume of messages during traffic analysis. LiLAC also includes the Socialist Millionaire's Protocol (SMP), which ensures the secure key exchange between users and thus helps verify the authenticity of both the communicating parties. This helps in preventing any type of MITM attack during communication.

Mohammad Reza Nosouhi, et al. [8] (2019) introduced HSDC–net: Secure Anonymous Messaging Online Social Networks. Harmonized and Stable Dining Cryptographers Network (HSDC–net) is a novel protocol that advances the original DC-net protocol and solves the drawbacks of original DC-net protocol. The HSDC-net protocol aims to provide anonymity to the sender. To achieve anonymity, the authors use Stable DC-net protocol. Also, HSDC-net uses a slot reservation protocol where each user anonymously selects a slot to publish their message. This SR protocol ensures there is no collision in slots that the original DC-net protocol faced. HSDC-net also uses a Disruption Managemenet (DM) protocol that ensures that if any disruption occurs during communication, then the identity of the disruptor will be revealed, but the identity of the sender will remain hidden and intact.

Raymond Cheng, et al. [1] (2020) introduced Talek: Private Group Messaging with Hidden Access Patterns. It's a private group messaging system designed to secure both the content of the message and metadata associated with the communication. This helps whistleblowers, activists, and journalists to remain anonymous. The system uses an access sequence indistinguishability notion, which ensures that the adversaries cannot detect which messages were accessed. Talek system operates under anytrust model that ensures if at least one of the servers is compromised, the system remains secure. The Private Information Retrieval (PIR) is a core technology in the Talek system, and it ensures that servers cannot determine which specific messages a user is accessing, thus preventing the footprint of messages on the server. Talek further uses a Blocked Cuckoo hashing data structure to organize messages on the server efficiently. This data structure also ensures the load balancing between other distributed servers.

Henry Corrigan-Gibbs, et al. [3] (2015) introduced Riposte: An Anonymous Messaging System Handling Millions of Users. Riposte is an anonymous messaging system that is designed to handle communication at the scale of millions of users. This messaging system focuses on ensuring strong anonymity by preventing adversaries from determining who is sending messages, thus helping privacy-concerned people like activists, whistleblowers, and journalists to broadcast their messages on shared bulletin boards. The anonymity is achieved by techniques like secure multi-party communication and private information retrieval(PIR). Riposte also uses Distributed Point Functions(DPF) to reduce the bandwidth required for a client to make written requests on the bulletin board. Using DPF, the server will never know which exact data row of the database they are targeting, thus making their request anonymous to the server. The system also provides resistance to traffic analysis as the message is shared across multiple servers using MPC along with DPF.

Roger Dingledine, et al. [4] (2004) presented Tor: The Second-Generation Onion Router. Tor is a circuit-based low latency anonymous communication system that builder on the onion routing design. The TOR system allows users to communicate globally without revealing their identity or location, which can be captured during traffic analysis by routing data through multiple relay nodes.

Each message is encrypted in multiple layers, and each hop of the circuit adds one encryption layer to the message. To further obfuscate user communication, the system adds padding to the message to prevent adversaries from detecting any recurrent communication patterns. Since it is an advancement of the original onion routing protocol, therefore it introduces new enhancements like perfect forward secrecy, congestion control, directory servers, and location-hidden servers.

Saba Eskandarian, et al. [6] (2020) proposed Express: Lowering the Cost of Metadata-hiding Communication with Cryptographic Privacy. Express is a system that aims to reduce the cost of hiding communication metadata while still maintaining the users' strong privacy. Express is a two-server system that provides cryptographic security against any arbitrary number of malicious clients and one malicious server. Along with metadata hiding, Express also prevents any malformed messages from malicious clients from being written in unauthorized mailboxes. Express uses SNIP proof system to prevent malicious servers from learning which specific mailbox has been modified by any client's write request. Also, it uses the Distributed Point Function(DPF) protocol to ensure that servers do not learn which mailbox was updated, thus protecting metadata privacy in communication.

Nirvan Tyagi, et al. [11] (2017) introduced Stadium: A Distributed Metadata-Private Messaging System. The Stadium system is designed to protect both the content of user messages and their metadata, which are vulnerable to attacks like traffic analysis. The privacy of messages and metadata is achieved by spreading communication across multiple low-cost servers operated by different organizations, thus ensuring no single server can link users to their messages. To solve the problem of limiting the information revealed from many observable traffic links, the paper has proposed a differentially private routing as well as a verifiable parallel mixnet design. Each mixnet has a public key, which the user uses to encapsulate the message along with the routing metadata. Along with this, the honest servers inject noise messages into the system to obscure the observable variables that are exposed to the attackers.

Jelle van den Hooff, et al. [14] (2015) proposed Vuvuzela: Scalable Private Messaging Resistant to Traffic Analysis. Vuvuzela is a point-to-point private messaging system designed to hide message content and metadata by resisting adversaries from detecting patterns from traffic analysis. The system achieves this by introducing cover traffic to obscure the communication patterns, making it extremely difficult for adversaries to analyze the source and recipient of communication. Vuvuzela's key insight is to minimize the number of variables observable by an attacker and to use differential privacy techniques to add noise to all observable variables in a way that provably hides information about which users are communicating. The system further routes the messages through a chain of servers, thus guaranteeing secure privacy even in case of strong adversaries. The system also uses dead drops technique to communicate, making the communication more anonymous.

Saba Eskandarian, et al. [5] (2021) introduced Clarion: Anonymous Communication from Multiparty Shuffling Protocols. Clarion is an anonymous communication system that provides anonymity by using multiparty shuffling protocols. Along with providing anonymous communication, the system also hides metadata thus hiding the information of sender and receiver from adversaries. Clarion uses symmetric key cryptographic algorithms as they are computationally faster, thus reducing the cost of computation done in communication. To further improve the security, the system uses secure multiparty communication primitive like beavers triples, which is used for the blind Mac verification process.

Zachary Newman, et al. [7] (2020) proposed Spectrum: High-bandwidth Anonymous Broadcast. Spectrum is a system designed for high-bandwidth anonymous broadcasts. This system is usable in scenarios where there are few broadcasters but many subscribers, thus making it perfect for whistleblowing and other privacy-concerned activity. Spectrum also ensures that metadata from adversaries are hidden from traffic analysis, thus preventing the leakage of the source of the message. The spectrum uses Dining Cryptographer's Networks (DC-nets) to allow anonymous messages. The system also uses a blind access control which is based on the Carter-Wegman Message Authentication Code (MAC). This blind access control prevents malicious broadcaster users from sending messages to the channel. The system further uses the BlameGame protocol, which is used to counter audit attacks.

Sajin Sasy, et al. [10] (2021) presented SoK: Metadata-Protecting Communication Systems. Metadata information like who is communicating with whom, time and amount of data transmitted can be detected during traffic analysis by adversaries, even if the message is encrypted. Thus, the authors of this paper have emphasized metadata protection and have introduced SoK. Sok is a comprehensive analysis of various systems aimed at protecting metadata in communication networks. The authors have surveyed 31 different metadata-protecting communication systems(MPCS). The paper talks about different techniques used in MPCS, such as Dining Cryptographers Networks (DC-nets), Mixnets, Private Information Retrieval (PIR), Differential Privacy (DP), and more. The paper also provides a high-level overview of some of the metadata-protecting systems, such as Tor, Talek, Vuvuzela, Dissent, and more.

Tyagi, et al. [12] (2023) introduced Orca: Blocklisting in Sender-Anonymous Messaging. Orca protocol is a novel approach that addresses the challenges identified in Signals sealed sender protocol. Orca uses group signatures to allow the initialization of anonymous communication. The group signatures allow senders to sign messages anonymously, thus ensuring sender anonymity and metadata protection. Orca further uses One-Time-Use (OTU) Authentication Tokens to allow the recipient to identify whether the source of the message is from an authentic sender. The tokens are signed using algebraic Message Authentication Codes (MACs). These tokens also allow the recipient to block any malicious or unwanted sender, thus providing the feature of a privacy-preserving blocklisting mechanism.

4 TABLE

Table 1 provides a comparative review and analysis of systems and techniques to attain the anonymity of the sender in messaging and communication.

.

Table 1: A Comparative Review And Analysis

System	Objective	Technologies & Cryptographic Algorithms	Setup Requirement	Use Cases	Audit Complexity	Merits	Demerits
ChatAlone [15]	Anonymous messaging and communication system using Bluetooth technology	Front end using Flutter, local storage and backend using hive, Bluetooth	Requires Bluetooth device pairing and hive configuration for local data storage on users device	Classroom feedback, conferences, and local anonymous group discussions	N/A.	Offline, peer-to-peer communication without the internet, suitable for low-connectivity environments, low overhead, and setup	Provides short-range communication; Bluetooth range restricts usability, user's device storage space used, susceptible to Bluetooth attacks.
Sabre [13]	Protocol for sender-anonymity and provides anonymous bulletin board and mailboxes.	Distributed Point Functions (DPFs), MPC-in-the-head, Zero-Knowledge Proofs (ZKPs), LowMC Block Cipher.	Distributed Point Function (DPF) setup, Multi-Party Computation (MPC) initialization.	Can be used by whistleblowers, anonymous bulletin boards, secure and anonymous email systems.	$O(logN)$	Scalable sender-anonymity with strong privacy guarantees, efficient for bulletin boards, faster auditing protocol.	Relies on semi-honest servers for correctness, high overhead for large mailboxes.
Panini [2]	Anonymous anycast messaging with provable guarantees for political activism and whistleblowing.	Linkable Ring Signatures, Nym-based Unicast for secure transmission.	Setup includes authenticated unicast and unlinkable sender-message pair unicast.	Political activism, dead man switches, sensitive communication.	N/A	Receiver anonymity with low resource usage, effective for sensitive communications.	Requires external unicast channels (e.g., Nym) for security, encounters capacity limits that restrict its effective expansion.
LiLAC [9]	Low-latency anonymous chat system using Dependent Link Padding and Onion routing for stronger anonymity.	Onion Routing, Dependent Link Padding (DLP), Browser-based deployment.	Requires Onion Routing circuit and directory server setup and configuration of Dependent Link Padding (DLP).	Instant messaging can be used for sensitive communications and whistleblowing.	N/A	Low latency, strong anonymity with usable web interface.	Browser-based implementation is vulnerable to adversaries and web attacks.
HSDC-net [8]	Anonymous group messaging using Stable Dining Cryptographers Network (SDC-net) and improved disruption management.	Stable DC-nets, Slot Reservation (SR) and Disruption Management (DM), Symmetric Key Encryption.	Network topology setup with LAN connections and setup.	Social networks, cryptocurrency transactions, anonymous journalism.	N/A	Strong anonymity in group messaging, efficient disruption resistance with low-latency message delivery.	Possible deanonymization in long-term use due to message collisions.

Table 1: A Comparative Review And Analysis

System	Objective	Technologies & Cryptographic Algorithms	Setup Requirement	Use Cases	Audit Complexity	Merits	Demerits
Talek [1]	System for Private communication using PIR-based data sharing.	Private Information Retrieval (PIR), cuckoo hashing, client-side logs.	N/A	Private communication for small groups, whistleblowing.	N/A	Strong privacy guarantees for small groups; efficient for untrusted environments.	Lack of liveness guarantees; potential downtime due to server failures.
Riposte [3]	Anonymous messaging system for whistleblowers at large scale, provides anonymous bulletin board.	Multi-Party Computation (MPC), Reverse Private Information Retrieval (RPIR), Distributed Point Functions (DPFs).	Requires Multi-Party Computation (MPC) setup and Reverse Private Information Retrieval (RPIR) configuration.	Anonymous posting in large-scale public forums like whistleblowing.	O(N)	Can be scaled to millions of users, strong anonymity guarantees for large-scale private messaging.	High setup cost, Anonymous set must be large enough, vulnerable to DoS attack.
Tor [4]	Circuit-based low-latency anonymous communication system for internet browsing and instant messaging.	Onion Routing, Incremental Telescoping with Encrypted SOCKS Proxy.	Onion Routing setup with incremental telescoping and mixnet configuration.	Web browsing, secure chat, SSH tunneling.	N/A	Widely used, strong anonymity with low latency for web traffic and chat.	Vulnerable to traffic confirmation attacks, needs better padding strategies, vulnerable to pattern detection attacks.
Express [6]	Lowering the cost of metadata-hiding communication using symmetric cryptography provides anonymous mailboxes.	Symmetric Key Cryptography, Reverse PIR, Traffic Padding, Distributed Point Functions (DPFs).	Setting up Reverse PIR and symmetric key cryptography protocols, epoch system implementation.	Whistleblowing, anonymous messaging, anonymous mail system.	O(N)	Highly efficient for whistleblowing systems, bandwidth, and computation savings.	Read access metadata can be leaked, vulnerable to DoS attacks.
Stadium [11]	Distributed metadata-private messaging system using differential privacy.	Differential Privacy (DP), Mixnets with Parallel Shuffling.	Parallel mixnet configuration with verifiable shuffling and distributed servers setup.	Large-scale messaging in sensitive settings (e.g., journalism).	N/A	Supports millions of users with differential privacy, strong traffic analysis protection.	High computation costs, latency increases with additional providers.
Vuvuzela [14]	Scalable private messaging resistant to traffic analysis.	Differential Privacy (DP), noise generation, chain of servers.	Noise generation setup for Differential Privacy (DP) mechanisms.	Whistleblowing, anonymous communication in oppressive regimes.	N/A	Scales to millions of users with differential privacy, robust against powerful adversaries.	High bandwidth consumption, requires cover traffic for privacy guarantees.

Table 1: A Comparative Review And Analysis

System	Objective	Technologies & Cryptographic Algorithms	Setup Requirement	Use Cases	Audit Complexity	Merits	Demerits
Spectrum [7]	High-bandwidth anonymous broadcasting, strong disruption resistance.	Dining Cryptographers (DC) Nets, Anonymous Access Control, Blind Verifiable Shuffling.	Configuration of Dining Cryptographers (DC) nets and protocols for disruption resistance.	High-bandwidth file sharing and anonymous live broadcasting.	O(1)	High-bandwidth broadcasting, robust against disruption.	High bandwidth and hardware costs, effective in case of a pool of large anonymity sets.
Orca [12]	Ensures anonymous communication and sender anonymity and provides a privacy-preserving blocklist for abuse prevention.	Group Signatures, One-time Tokens, Elliptic Curve Cryptography (ECC), Zero-Knowledge Proofs, Oblivious token minting protocol.	Setting up Group signature with verifier local revocation, configuration of multiple intermediate authorities.	Provides abuse-resistant sender-anonymous messaging platforms.	N/A	Provides efficient blocklist without revealing sender identity, effective for abuse-resistant messaging.	Group signatures require expensive tasks and a computationally intensive system.
Clarion [5]	Anonymous broadcast and messaging using multi-party shuffling protocols.	Secret-shared shuffling, Multi-Party Computation (MPC), Non-Interactive Zero-Knowledge Proofs (NIZK).	3 non-colluding servers, Secret-shared shuffling setup with Multi-Party Computation (MPC).	Anonymous messaging for live events and political forums, whistle-blowing, anonymous journal.	N/A	Improved scalability, improved speed for message integrity checks.	Requires pre-processing phase for scaling, vulnerable if all servers collude.

REFERENCES

[1] Raymond Cheng, William Scott, Elisaweta Masserova, Irene Zhang, Vipul Goyal, Thomas Anderson, Arvind Krishnamurthy, and Bryan Parno. 2020. Talek: Private Group Messaging with Hidden Access Patterns. In *Proceedings of the 36th Annual Computer Security Applications Conference* (Austin, USA) *(ACSAC '20)*. Association for Computing Machinery, New York, NY, USA, 84–99. https://doi.org/10.1145/3427228.3427231

[2] Christoph Coijanovic, Christiane Weis, and Thorsten Strufe. 2024. Panini — Anonymous Anycast andnbsp;annbsp;Instantiation. In *Computer Security – ESORICS 2023: 28th European Symposium on Research in Computer Security, The Hague, The Netherlands, September 25–29, 2023, Proceedings, Part II* (The Hague, The Netherlands). Springer-Verlag, Berlin, Heidelberg, 193–211. https://doi.org/10.1007/978-3-031-51476-0_10

[3] Henry Corrigan-Gibbs, Dan Boneh, and David Mazières. 2015. Riposte: An Anonymous Messaging System Handling Millions of Users. In *Proceedings of the 2015 IEEE Symposium on Security and Privacy (SP '15)*. IEEE Computer Society, USA, 321–338. https://doi.org/10.1109/SP.2015.27

[4] Roger Dingledine, Nick Mathewson, and Paul Syverson. 2004. Tor: the second-generation onion router. In *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13* (San Diego, CA) *(SSYM'04)*. USENIX Association, USA, 21.

[5] Saba Eskandarian and Dan Boneh. 2022. Clarion: Anonymous Communication from Multiparty Shuffling Protocols. In *29th Annual Network and Distributed System Security Symposium, NDSS 2022, San Diego, California, USA, April 24-28, 2022*. The Internet Society. https://www.ndss-symposium.org/ndss-paper/auto-draft-243/

[6] Saba Eskandarian, Henry Corrigan-Gibbs, Matei Zaharia, and Dan Boneh. 2021. Express: Lowering the Cost of Metadata-hiding Communication with Cryptographic Privacy. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 1775–1792. https://www.usenix.org/conference/usenixsecurity21/presentation/eskand-arian

[7] Zachary Newman, Sacha Servan-Schreiber, and Srinivas Devadas. 2022. Spectrum: High-bandwidth Anonymous Broadcast. In *19th USENIX Symposium on Networked Systems Design and Implementation (NSDI 22)*. USENIX Association, Renton, WA, 229–248. https://www.usenix.org/conference/nsdi22/presentation/newman

[8] Mohammad Reza Nosouhi, Shui Yu, Keshav Sood, and Marthie Grobler. 2019. HSDC–Net: Secure Anonymous Messaging in Online Social Networks. In *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. 350–357. https://doi.org/10.1109/TrustCom/BigDataSE.2019.00054

[9] John P. Podolanko, Revanth Pobala, Hussain Mucklai, George Danezis, and Matthew Wright. 2017. LiLAC: Lightweight Low-Latency Anonymous Chat. In *2017 IEEE Symposium on Privacy-Aware Computing (PAC)*. 141–151. https://doi.org/10.1109/PAC.2017.14

[10] Sajin Sasy and Ian Goldberg. 2024. SoK: Metadata-Protecting Communication Systems. *Proc. Priv. Enhancing Technol.* 2024, 1 (2024), 509–524. https://doi.org/10.56553/POPETS-2024-0030

[11] Nirvan Tyagi, Yossi Gilad, Derek Leung, Matei Zaharia, and Nickolai Zeldovich. 2017. Stadium: A Distributed Metadata-Private Messaging System. In *Proceedings of the 26th Symposium on Operating Systems Principles* (Shanghai, China) *(SOSP '17)*. Association for Computing Machinery, New York, NY, USA, 423–440. https://doi.org/10.1145/3132747.3132783

[12] Nirvan Tyagi, Julia Len, Ian Miers, and Thomas Ristenpart. 2022. Orca: Blocklisting in Sender-Anonymous Messaging. In *31st USENIX Security Symposium, USENIX Security 2022, Boston, MA, USA, August 10-12, 2022*, Kevin R. B. Butler and Kurt Thomas (Eds.). USENIX Association, 2299–2316. https://www.usenix.org/conference/usenixsecurity22/presentation/tyagi

[13] Adithya Vadapalli, Kyle Storrier, and Ryan Henry. 2022. Sabre: Sender-Anonymous Messaging with Fast Audits. *2022 IEEE Symposium on Security and Privacy (SP)* (2022), 1953–1970. https://api.semanticscholar.org/CorpusID:251151048

[14] Jelle van den Hooff, David Lazar, Matei Zaharia, and Nickolai Zeldovich. 2015. Vuvuzela: scalable private messaging resistant to traffic analysis. In *Proceedings of the 25th Symposium on Operating Systems Principles* (Monterey, California) *(SOSP '15)*. Association for Computing Machinery, New York, NY, USA, 137–152. https://doi.org/10.1145/2815400.2815417

[15] Jordan Yuen Jia Jun and Owen Noel Newton Fernando. 2024. ChatAlone: An Anonymous Messaging Application for Enhanced Privacy and Open Communication. In *Human-Centered Design, Operation and Evaluation of Mobile Communications: 5th International Conference, MOBILE 2024, Held as Part of the 26th HCI International Conference, HCII 2024, Washington, DC, USA, June 29–July 4, 2024, Proceedings, Part II* (Washington DC, USA). Springer-Verlag, Berlin, Heidelberg, 166–175. https://doi.org/10.1007/978-3-031-60487-4_13