Recent Advancements in Privacy Preserving Network Layer Approaches

Andreas Kramer, Filip Rezabek*, Richard von Seck*
*Chair of Network Architectures and Services, Department of Informatics
Technical University of Munich, Germany
Email: andreas.kramer@tum.de, frezabek@net.in.tum.de, seck@net.in.tum.de,

***Abstract*—Due to the rapid growth of internet communications, privacy becomes ever more important in our digital age. But since cryptography is not enough to preserve the users' privacy, solutions on the network layer become crucial. Tor and I2P offer their users privacy protection with considerable performance but have some robustness drawbacks. Therefore, we introduce the recently released anonymity infrastructure Nym that protects privacy on the network layer and addresses certain technical shortcomings of the currently most well-known anonymity networks. In this survey, we find out that for Tor and I2P a wide range of vulnerabilities of privacy against global adversaries are known, while Nym offers a high level of privacy even against this kind of attacker. However, privacy is not always the only goal that such solutions must achieve because the quality of service and an acceptable level of latency must also be maintained. A future challenge for Nym is to identify whether incentivizing its operators leads to a larger user base, which would result in the required and desired performance as well as increase the strength of the anonymity properties.**

***Index Terms*—privacy, quality of service, mix nets, onion routing, i2p, nym**

1. Introduction

In the 1990s the U.S. government tried to constrain the use of strong cryptography to ensure that national security and law enforcement agencies could break all ongoing encrypted communications via backdoors. This led to a heated debate known as the "Cryptowars" [1]. In 1993, Eric Hughes wrote the Cyphernomicon, a pamphlet arguing for cryptography with the fundamental goal of achieving and supporting personal privacy in the digital world:

> "Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one does not want the whole world to know, but a secret matter is something one does not want anybody to know. Privacy is the power to selectively reveal oneself to the world." [2]

But protecting only the content of the user messages does not automatically preserve its privacy. Due to the structure of the Internet protocol (IP), the OSI layer three plays a crucial role when privacy should be preserved. In addition to the payload, an IP datagram consists of a header that contains metadata such as the source and destination address [3]. The application of cryptography helps to protect the confidentiality and integrity [4] of messages, but even if all possible fields are encrypted and none of this header information is revealed, attackers can still detect communication patterns. Therefore, the difficulty of eavesdropping packets in the network and traffic analysis, including matching the amount of data or examining connection establishment or termination [5], should be increased to defend the users' privacy. But privacy comes with the cost of latency. Thus, often a trade-off between privacy and Quality Of Service (QoS) exists. Bounded Privacy is describing this problem where for a given threshold on the QoS a feasible level of privacy is guaranteed [6]. This survey focuses on solutions that aim to protect the privacy of its users and hence also its meta data. In Sections 2 and 3, a definition of privacy and the privacy-enhancing technologies mix network and onion routing are given and used to argue about concrete implementations of these technologies like I2P [7] and Tor [8], which offer a good level of privacy but still have weaknesses, especially against powerful adversaries that can watch the entire network and traffic. Additionally, in Section 4 the newly released privacy infrastructure Nym [9] is described, which is based on a mix net system and economic incentives for operating components of it and aims to solve these problems.
In Section 5, the presented solutions are then compared regarding their weaknesses against a global adversary, a conclusion is drawn, as well as future work is named.

2. Background

In this section we introduce a definition of privacy and the attacker models as which later described solutions can be attacked.

2.1. Attacker Models

To precisely describe the attacks, we define and distinguish different attacker models by their capabilities. An attacker may control various subsets of nodes in a network. Depending on the distribution of the nodes, an attacker may gain more or less information.
Depending on the network position there are **external** and **internal** attackers. An **external** adversary can compromise the communication links and an **internal** one participates in the anonymous system and therefore can compromise connections or peers. These are of special interest as they provide routing or enhanced security functions [10].
Depending on the geographic location we distinguish between **global** and **local** attackers. An adversary with

doi: 10.2313/NET-2023-06-1_04

access to all communication links is called **global** while a **local** one can just act on specific connections or peers. Attackers that can just eavesdrop on the communication medium are defined as **passive**. **Active** ones can delay, modify, and omit messages and may be able to compromise peers.
The standard threat model for symbolic protocol analysis is the **Dolev-Yao model (DY)** [11]. This adversary can read, modify, destroy all message traffic, and perform any operation possible for a normal protocol user without breaking the cryptographic primitives [12]. In literature, a protocol that is secure under DY is also seen as secure under a less powerful attacker [13], [14].

2.2. Privacy

According to A. Pfitzmann and M. Köhntopp [15] privacy is defined by the terms anonymity, pseudonymity, unlinkability, and unobservability. These provide protection against the discovery and misuse of identity by other users [16]. In order to show the properties of privacy-enhancing technologies we now introduce the mentioned terms.
Anonymity is defined as not being identifiable from other subjects in the same set which is called *anonymity set*. We unite all subjects that might cause an action in that anonymity set. Depending on that set, there exist two different types of anonymity. The *sender anonymity set* is the subset of all subjects that might send traffic in the same network. The *recipient anonymity set* is the subset of all subjects that might receive traffic in the same network. These sets may be disjoint but also overlap. In general, one can state that anonymity becomes stronger with the size of the set [15].
Pseudonyms, like identifiers, are used to not reveal data about subjects during specific actions. Nevertheless, user actions can still be linked with pseudonyms by the system itself. *Pseudonymity* ensures that users may use resources or services without revealing their identity so that they are still accountable for their use [16].
Unlinkability is described as the inability to connect or combine subjects with initially separate information. This means that the probability of finding a relation between those items stays the same before (a-priori knowledge) and after an action within a system (a-posteriori knowledge of the attacker) [15].
Unobservability requires that subjects cannot determine whether a specific action was performed. This means that the Items Of Interest (IOI) are indistinguishable from other IOIs. [15].

3. Existing Privacy-Enhancing Solutions

In this section, we take a closer look at solutions that offer network privacy. The anonymity concepts mix network and onion routing are described as a basis to argue about concrete implementations, their characteristics, and their weaknesses.

3.1. Anonymity Concepts

A **mix network (mix net)** is an overlay network of mix nodes that routes messages through the network anonymously [17].

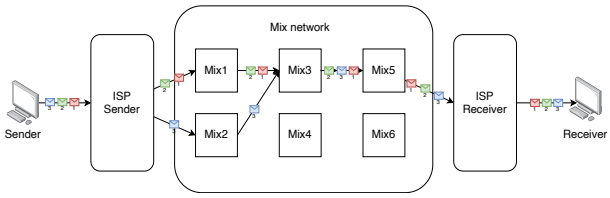

Figure 1: Mix network infrastructure

Secure mix nets can be classified as Decryption-Mix Network (DMN) which was initially proposed by Chaum [18] already in 1981, and Re-Encryption Mix Network (RMN), a concept by Park et al. [19]. A mix net protocol run includes a set of senders S_1, ... , S_n, the mix servers M_1, ... , M_n and a public bulletin board B. RMNs additionally have trustees T_1, ... , T_n. The senders transmit their ciphertexts to the mix servers which add delay and then publish them in random order. Channels are used to ensure that eligible senders S_i securely submit messages to the bulletin board B. The protocol run is split into three phases. In the *setup phase*, all required parameters are generated. The *submission phase* is then used to generate and submit the senders' messages. Lastly, in the *mixing phase*, the mix servers collaboratively mix the input.
The purpose of a mix net is to provide unlinkability, so to hide the links between the communication partners and their messages [18]. This can be assured by delaying the messages and then shuffling (also called mixing) before forwarding them. Figure 1 displays both the network position of such mix nets and illustrates the message shuffling. The sent messages are fixed-sized due to message padding, where random data is attached to messages of deviating size [4]. Additionally, whenever the user does not have any actual payload to send to the mix network, the client sends instead loop cover packets, which are messages with dummy payload that have the same receiver as sender. This leads to the indistinguishability of real messages from cover messages and therefore to unobservability [20]. Mix nets are hence designed to provide meta data protection against global adversaries. As long as not all mix servers of the message path are corrupted, the mix net can guarantee sender anonymity.
With *Decryption-Mix Networks* the sender is required to iteratively encrypt the input messages m_i with the public keys pk_1, ... , pk_n of the mix servers M_1, ... , M_n. This can be achieved with public key cryptographic systems like RSA. The message is encrypted in reverse order and the resulting layered ciphertext c_i is then submitted to the first mix server M_1. The mix server M_i then uses his private key sk_i to decrypt the outermost encryption layer of all input ciphertexts, shuffles the decrypted messages and forwards them to the next mix server M_{i+1}. The last mix server could then output the plain messages initially chosen by the senders in random order. To offer a higher level of privacy messages are stored until an adequate threshold is reached and they are then forwarded to the next hop [20].
For *re-encryption mixnets* we need to use a public-key encryption scheme that allows for re-encrypting a given ciphertext without knowing the secret key or the encrypted message like ElGamal, an asymmetric key encryption algorithm for public-key cryptography [21].

doi: 10.2313/NET-2023-06-1_04

As mentioned before RMNs additionally use trustees t_1, ..., t_n with whom each sender s_i shares the secret key of its public key pk. With this information, the sender s_i encrypts its message. The mix server M_i then re-encrypts all ciphertexts with coins chosen independently and uniformly at random, shuffles the re-encrypted ciphertexts, and forwards them to the next mix server M_{i+1}. This procedure is repeated until the last mix server is reached. It then outputs a list of ciphertexts that encrypt the input messages initially chosen by the senders but under different random coins and in a random order [20].

Onion Routing is a general-purpose infrastructure for privacy in public networks that allows lower latency than mix nets as messages are not mixed or delayed [22].

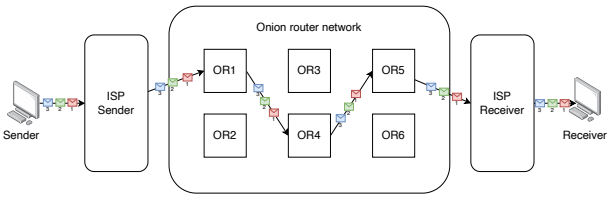

Figure 2: Onion routing network infrastructure

Similar to mix nets, messages are sent over multiple Onion Routers (ORs) inside the network. As shown in Figure 2, the messages are relayed through the OR network without delaying them and thus without shuffling. This allows in comparison to mix nets a lower latency. ORs work as intermediate proxies, their physical location in the network is unknown [23]. The onion data structure sent to the ORs consists of several encryption layers around the payload. ORs accept fixed-length messages through message padding. Additionally, they perform cryptographic operations like removing one layer of encryption using its own private key on the messages like a DMN before forwarding it to the next mix server. The path through the network is defined by the client, which builds a circuit. Every OR knows only its predecessor and the successor but has no further information about other routers in its circuits like the origin, destination, or the payload. As described before, in DMNs the mix servers introduce a delay before forwarding their messages. Onion routing works without these delays, which may lower the anonymity [8], [22] but also lower the latency.

3.2. Anonymity Networks

Tor is a distributed overlay network that offers anonymity on TCP-based communications in networks and is based on the onion routing protocol described in Section 3.1 [8]. It additionally includes several improvements like perfect forward secrecy [24], hidden services, which provide receiver anonymity, and rendezvous points to connect to them [8]. Tor is not fully distributed as it uses directory services to store statistics and information about Tor nodes. It cannot defend against end-to-end correlation attacks from global adversaries because it does not employ delays for cells. Also, deanonymizing of hidden services is possible [8], [25], [26]. But even local attackers can determine the visited webpages with fingerprinting attacks [27]. As mentioned before, the anonymity of a system depends also on the size of the anonymity set. This means for Tor more hops (ORs) and more users may lead to higher anonymity. As the Tor network does not incentivize the operation of components like routers, the network size remained roughly the same in the last years [28].

The **Invisible Internet Project (I2P)** is a fully encrypted private network layer on the basis of a peer-to-peer network. I2P, like Tor, uses a variant of onion routing named garlic routing to create anonymous connections [7].

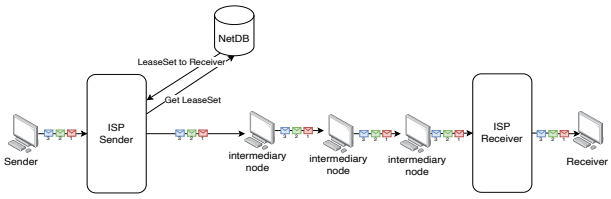

Figure 3: Architecture of a I2P network

The participants work both as clients and as proxy routers that forward the messages sent through the network. To achieve a fully distributed architecture, I2P uses a Network Database (NetDB), which is implemented as a Distributed Hash Table (DHT) using the Kademlia algorithm [29]. In NetDB information about peers and services is saved. To communicate with other peers the sender has to get leaseSets from the database, which contain data such as public keys for communication [30]. Figure 3 depicts the message flow through the I2P network and the preliminary request to NetDB. Nevertheless, I2P has some weaknesses. Its anonymity set is small because of the modest size of the current network [31]. A consequence is the current bad performance of its services, because of the overhead for encryption and routing which limits the bandwidth. Also, effective defenses against Sybil attacks remain an open question [31].

3.3. Summary and Challenges of Solutions

As described in Section 3.2 the currently two most well-known anonymity networks Tor and I2P still suffer from some weaknesses, especially against global, passive, or stronger adversaries. Another problem of both remains the lack of growth that comes with latency and leads to a smaller anonymity set. With an increased number of participants, some of the weaknesses would be reduced [31], [32]. Tor got a lot of attention from researchers which led to constant improvement and good documentation. I2P on the other hand got less attention due to the missing clear design documentation [17]. Nevertheless, in both networks, the key components are run on a volunteer basis which led to a consistent number of operators. Nym now explores the impact of node incentives. This mechanism should not only lead to more node operators in the network but also prevent freeloading [33] and limit the possibilities of malicious users in the network [17].

4. Nym

This section describes the newly released anonymity infrastructure Nym. Its design goal is to support privacy-enhanced access to applications and services. Node operators are incentivized by their own tokens, named Nym tokens, to support the operational costs with proof of

doi: 10.2313/NET-2023-06-1_04

mixing. Proof of mixing is defined as incentivizing node operators to correctly and reliably process, route, and deliver messages. This shall lead to dynamic scaling for privacy and high quality of service.

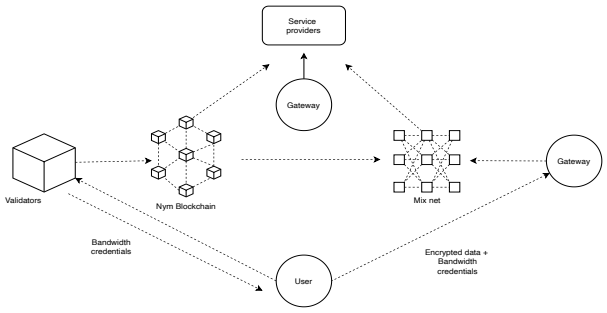

Figure 4: Nym architecture [34]

Figure 4 depicts Nym's architecture and its three types of nodes: **Validators**, **Gateways**, and **Mix Nodes**.

Mix Nodes. Mix nodes provide communication privacy and are part of the mix network. Nym uses a Loopix [35] design for its mix net, modified to provide better QoS guarantees. Loopix is a low-latency anonymous communication system that provides sender and receiver anonymity as well as unobservability. As described in Section 3.1 mix nodes receive data packets that they transform cryptographically and reorder. Sphinx [36] is used as a packet format, which is cryptographic and relays anonymized messages within the mix network. It supports indistinguishable replies, hides the path length and relay position as well as provides unlinkability. Loopix also uses a continuous-time mixing strategy, where each message is delayed individually and independently of the others [37]. The concrete mixing delay is chosen by the original sender and encoded in the Sphinx header. Additionally, Loopix applies dummy traffic and message padding. This ensures a minimum level of anonymity at all times, obfuscates the timing and volume of user communication, and therefore achieves unobservability [9], [17].

Gateways. Gateways mediate the access to the network and its services. They act as proxies between the mix net and the participants. Users may always choose the same gateway for all their traffic or multiple ones. Gateways cache received messages for offline or unreachable participants. Users need to show valid unspent bandwidth credentials, provided by the validators, to send messages through the mixnet [9], [17].

Validators. Validators maintain the Nym blockchain and handle transactions for two types of credentials. Bandwidth credentials prove the right to send traffic through the mixnet. Service credentials can encode arbitrary attributes for the proof of access rights for a service [17]. These credentials are provided with a modified version of coconut, a cryptographic signature scheme, which supports decentralized credential issuance and thus is resistant to local adversaries [9], [38]. The Nym blockchain works as a broadcast channel for network-wide information and includes data like the list of nodes and their public keys, network configuration parameters, or participants' stake.

Service providers. Nym as an infrastructure supports privacy for third-party applications and services that are accessible through the network. These can send and receive messages to privately communicate and use the Nym credentials to grant access to their services [17].

5. Comparison of Solutions

In this section, we compare the offered privacy for the presented anonymity networks against global adversaries. Table 1 depicts the known vulnerabilities ordered by in Section 2.2 defined privacy terms. The concrete value describes whether vulnerabilities for the solution on given requirement exist or not. The table is only valid for this type of attacker and the current amount of users.

	Tor	I2P	Nym
Anonymity	Yes	Yes	No
Unlinkability	Yes	Yes	No
Unobservability	Yes	Yes	No

TABLE 1: Known vulnerabilities of privacy requirements against global adversaries

Tor in general does not provide protection against global attackers [39], [40]. As described in Section 3.2, onion routing encrypts the messages between each OR so that only the last hop can see the decrypted message. But still, Tor suffers weaknesses against global adversaries, because though the packets are encrypted, Tor does not add timing obfuscation to conceal the traffic patterns. Additionally, Tor's design uses a centralized directory authority to build tunnels through the network which may be another attack vector. As shown by the different deanonymization attacks, Tor suffers known vulnerabilities in anonymity against this kind of attacker [41], [42]. Also, unlinkability cannot be preserved, as shown by attacks [43]. As no cover traffic is included in either the onion routing protocol or in Tor unobservability cannot be guaranteed either [44].

Though I2P is based on a peer-to-peer architecture, like Tor the network cannot defend against global attackers. I2P replaces Tor's directory authority with a DHT for routing. As described in Section 3.2 the usage of a distributed hash table may be an attack vector. It is open to several attacks that isolate, misdirect, or deanonymize users like brute-force, timing, or intersection attacks [7], [30], [31]. Therefore, I2P is not able to guarantee anonymity or unlinkability against global adversaries. I2P also does not use cover traffic. Due to that reason, the network cannot grant unobservability [31], [44].

Nym aims to protect also against global adversaries by the usage of the in Section 4 described Loopix mix net. Mentioned Loopix mix net aims to protect the users' unlinkability [9], [17]. Neither Loopix nor Nym have so far known vulnerabilities of anonymity, unlinkability, or unobservability. Therefore, all values in Table 1 are no. Since Nym modified Loopix to provide a better QoS it cannot be ruled out that there are yet undocumented vulnerabilities. Comparable to the vulnerabilities of Tor's directory services, the gateways, for example, could provide an attack vector. Unlike I2P or Tor, Nym adds cover traffic and timing obfuscation, which should prevent unobservability [17], [45]. Nevertheless, it is important to mention that not much research could be conducted yet to identify possible weaknesses.

6. Conclusion and Future Work

In this paper, we provided an overview of recent anonymity concepts and networks as well as a comparison of them with the newly released Nym. Section 5 has shown that, with current knowledge, Nym provides a high level of privacy for its users, even against global attackers, considering that the solution is relatively new and not much research has been done on it. However, the privacy provided by mix networks comes with latency, where always a trade-off between privacy and QoS exists. The question in the future will be whether the market will adopt the concept chosen by Nym tech of rewarding their operators, so that with a larger user base, also more operators will run mix servers, validators, or gateways, so that the required and desired performance is given in addition to privacy. Future challenges and opportunities lie in the question of how the latency currently compares to the other solutions described in this survey and how it scales with the addition of more mix servers. Low latency and thus good performance could be next to privacy a major argument to use Nym. And a large amount of users would increase the strength of anonymity properties.

Acronyms

DHT	Distributed Hash Table. 3, 4
DMN	Decryption-Mix Network. 2, 3
DY	Dolev-Yao model. 2
I2P	Invisible Internet Project. 3, 4
IOI	Items Of Interest. 2
IP	Internet protocol. 1
NetDB	Network Database. 3
OR	Onion Router. 3, 4
OSI	Open Systems Interconnection. 1
QoS	Quality Of Service. 1, 4
RMN	Re-Encryption Mix Network. 2

References

[1] B.-J. Koops and E. Kosta, "Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark"," *Computer Law and Security Review*, vol. 34, no. 4, pp. 890–900, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0267364918302413

[2] E. Hughes, "A Cypherpunk's Manifesto," https://www.activism.net/cypherpunk/manifesto.html, 1993, [Online; accessed 10-October-2022].

[3] J. Postel, "Internet Protocol," RFC 791 (Internet Standard), RFC Editor, Fremont, CA, USA, Sep. 1981, updated by RFCs 1349, 2474, 6864. [Online]. Available: https://www.rfc-editor.org/rfc/rfc791.txt

[4] M. Bishop, *Introduction to Computer Security*. Addison-Wesley Professional, 2004.

[5] J. Ren and J. Wu, "Survey on anonymous communications in computer networks," *Computer Communications*, vol. 33, pp. 420–431, 03 2010.

[6] L. Hartmann, "Bounded Privacy: Formalising the Trade-Off Between Privacy and Quality of Service," in *SICHERHEIT 2018*, H. Langweg, M. Meier, B. C. Witt, and D. Reinhardt, Eds. Bonn: Gesellschaft für Informatik e.V., 2018, pp. 267–272.

[7] "Invisible Internet Project (I2P)," https://geti2p.net, [Online; accessed 16-September-2022].

[8] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-Generation Onion Router," in *13th USENIX Security Symposium (USENIX Security 04)*. San Diego, CA: USENIX Association, Aug. 2004. [Online]. Available: https://www.usenix.org/conference/13th-usenix-security-symposium/tor-second-generation-onion-router

[9] "NYM - Building the next generation of privacy infrastructure," https://nymtech.net, [Online; accessed 16-September-2022].

[10] R. Staudemeyer, D. Umuhoza, and C. Omlin, "Attacker models, traffic analysis and privacy threats in IP networks," 01 2005, p. 7.

[11] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[12] Q. Chen, C. Zhang, and S. Zhang, *Secure Transaction Protocol Analysis: Models and Applications*, 01 2008, vol. 5111.

[13] W. Arsac, G. Bella, X. Chantry, and L. Compagna, "Multi-Attacker Protocol Validation," *J. Autom. Reasoning*, vol. 46, pp. 353–388, 04 2011.

[14] I. Cervesato, "The Dolev-Yao Intruder is the most Powerful Attacker," 2010.

[15] H. Federrath, *Designing Privacy Enhancing Technologies International Workshop on design issues in anonymity and unobservability, Berkeley, CA, USA, July 25-26, 2000. proceedings*. Springer Berlin Heidelberg, 2001, pp. 1–9.

[16] "Common Criteria for Information Technology Security Evaluation," *Part 2: Security functional components*, 2017.

[17] Diaz, Halpin, and Kiayisas, "The Nym Network - The Next Generation of Privacy Infrastructure," vol. 1.0, 2021.

[18] D. L. Chaum, "Untraceable Electronic Mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, p. 84–90, 1981.

[19] C. Park, K. Itoh, and K. Kurosawa, "Efficient Anonymous Channel and All/Nothing Election Scheme," in *Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, ser. EUROCRYPT '93. Berlin, Heidelberg: Springer-Verlag, 1994, p. 248–259.

[20] T. Haines and J. Müller, "SoK: Techniques for Verifiable Mix Nets," in *2020 IEEE 33rd Computer Security Foundations Symposium (CSF)*, 2020, pp. 49–64.

[21] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[22] D. Goldschlag, M. Reed, and P. Syverson, "Onion Routing for Anonymous and Private Internet Connections," *Communications of the ACM*, vol. 42, 02 1999.

[23] N. Dutta, N. Jadav, S. Tanwar, H. Deva Sarma, and E. Pricop, *Cyber Security: Issues and Current Trends*, 01 2022.

[24] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*, 1st ed. USA: CRC Press, Inc., 1996.

[25] A. Biryukov, I. Pustogarov, and R.-P. Weinmann, "Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization," in *2013 IEEE Symposium on Security and Privacy*, 2013, pp. 80–94.

[26] R. Jansen, F. Tschorsch, A. Johnson, and B. Scheuermann, "The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network," 01 2014.

[27] M. Juarez, S. Afroz, G. Acar, C. Diaz, and R. Greenstadt, "A Critical Evaluation of Website Fingerprinting Attacks," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 263–274. [Online]. Available: https://doi.org/10.1145/2660267.2660368

[28] "Tor Metrics," https://metrics.torproject.org/networksize.html, [Online; accessed 21-September-2022].

[29] P. Maymounkov and D. Eres, "Kademlia: A peer-to-peer information system based on the xor metric," vol. 2429, 04 2002.

[30] C. Egger, J. Schlumberger, C. Kruegel, and G. Vigna, "Practical Attacks against the I2P Network," in *Proceedings of the 16th International Symposium on Research in Attacks, Intrusions, and Defenses - Volume 8145*, ser. RAID 2013. Berlin, Heidelberg: Springer-Verlag, 2013, p. 432–451. [Online]. Available: https://doi.org/10.1007/978-3-642-41284-4_22

[31] "Invisible Internet Project (I2P): Threat models," https://geti2p.net/de/docs/how/threat-model, [Online; accessed 20-September-2022].

[32] E. Erdin, C. Zachor, and M. H. Gunes, "How to Find Hidden Users: A Survey of Attacks on Anonymity Networks," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2296–2316, 2015.

[33] Z. Zhang, W. Zhou, and M. Sherr, "Bypassing Tor Exit Blocking with Exit Bridge Onion Services," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 3–16. [Online]. Available: https://doi.org/10.1145/3372297.3417245

[34] "Choose your Character: an Overview of Nym Network Actors," https://blog.nymtech.net/choose-your-character-an-overview-of-nym-network-actors-19e6a9808540, [Online; accessed 10-October-2022].

[35] A. M. Piotrowska, J. Hayes, T. Elahi, S. Meiser, and G. Danezis, "The Loopix Anonymity System," in *Proceedings of the 26th USENIX Conference on Security Symposium*, ser. SEC'17. USA: USENIX Association, 2017, p. 1199–1216.

[36] G. Danezis and I. Goldberg, "Sphinx: A Compact and Provably Secure Mix Format," in *2009 30th IEEE Symposium on Security and Privacy*, 2009, pp. 269–282.

[37] G. Danezis, "The traffic analysis of continuous-time mixes," in *Proceedings of the 4th International Conference on Privacy Enhancing Technologies*, ser. PET'04. Berlin, Heidelberg: Springer-Verlag, 2004, p. 35–50. [Online]. Available: https://doi.org/10.1007/11423409_3

[38] A. Sonnino, M. Al-Bassam, S. Bano, and G. Danezis, "Coconut: Threshold Issuance Selective Disclosure Credentials with Applications to Distributed Ledgers," 02 2018.

[39] P. Syverson, G. Tsudik, M. Reed, and C. Landwehr, *Towards an Analysis of Onion Routing Security*, 03 2001, pp. 96–114.

[40] S. Chakravarty, A. Stavrou, and A. D. Keromytis, "Approximating a Global Passive Adversary Against Tor," 2008. [Online]. Available: https://academiccommons.columbia.edu/doi/10.7916/D82J6QBM

[41] F. Buccafurri, V. Angelis, M. Idone, C. Labrini, and S. Lazzaro, "Achieving Sender Anonymity in Tor against the Global Passive Adversary," *Applied Sciences*, vol. 12, p. 137, 12 2021.

[42] I. Karunanayake, N. Ahmed, R. Malaney, R. Islam, and S. K. Jha, "De-Anonymisation Attacks on Tor: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 4, pp. 2324–2350, 2021.

[43] S. Murdoch and G. Danezis, "Low-cost traffic analysis of Tor," in *2005 IEEE Symposium on Security and Privacy*, 2005, pp. 183–195.

[44] J. Ren and J. Wu, "Survey on anonymous communications in computer networks," *Computer Communications*, vol. 33, pp. 420–431, 03 2010.

[45] "NYM - Documention," https://nymtech.net/docs, [Online; accessed 22-September-2022].