GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

Quantifying the impact of external de-anonymization in mix networks

Autor: **Lydia Vian de Fuentes**

Director: **Stefanie Roos**

Co-Director: **Georgy Ishmaev**

Delft

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título

Quantifying the impact of external de-anonymization in mix networks

en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el

curso académico **2019/2020** es de mi autoría, original e inédito y

no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido

tomada de otros documentos está debidamente referenciada.

Fdo.: **Lydia Vian de Fuentes** Fecha: 23/ 08/ 2020

Autorizada la entrega del proyecto

STEFANIE ROOS

GEORGY ISHMAEV

S. Roos

Fdo.: **Stefanie Roos** Fecha: 23/ 08/ 2020

COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

Quantifying the impact of external de-anonymization in mix networks

Autor: **Lydia Vian de Fuentes**

Director: **Stefanie Roos**

Co-Director: **Georgy Ishmaev**

Delft

Acknowledgments

+ ¿Has empezado con el proyecto de los Bitcoins?
- Mamá, mi TGF no va de Bitcoins…
+ Bueno, con el proyecto.
- Mamá, ¡Está acabado!
+ Revísalo por si acaso, que no me fío.

A mi madre. Quiero agradecer este proyecto a la persona más importante de mi vida, mi madre. Gracias a ti estoy dónde estoy y he conseguido todo lo que me orgullece hoy. Me has formado como persona, hija y amiga. Si estoy escribiendo esta sección de agradecimientos en TU Delft ahora, después de 4 años con ICAI es gracias a ti, y solo a ti. Por su puesto, no puedo dejar de mencionarte Po. Bedankt voor dat je mij altijd hebt ondersteund en mij altijd geholpen hebt.

En segundo lugar, me gustaría agradecer el apoyo que las instituciones Techniek Universiteit Delft y la Universidad Pontificia Comillas han ofrecido a este Trabajo Fin de Grado. Siendo TU Delft la universidad a la cual pertenecen mis tutores de proyecto Stefanie Roos y Georgi Ishmaev. A pesar de las dificultades que hayan podido acaecer este año, siempre habéis estado disponibles y atentos para ayudarme con mi progreso y aportarme los mejores consejos y directrices. Agradecer a la Universidasd Pontificia Comillas, en concreto la facultad de ICAI, por su enorme flexibilidad y atención humana y personalizada que siempre he recibido de vuestra parte desde el día 1 de Septiembre de 2016 que empecé mi formación universitaria con vosotros y de la que no podría estar más contenta y orgullosa. Quiero hacer especial mención a Rafael Palacios por que siempre me has sido de ayuda cuando he tenido alguna dificultad y agradezco enormemente la paciencia que has tenido con todas mis peticiones, preguntas y sin fin de correos.

Quiero mencionar que no hubiese llegado a este punto de mi vida tan feliz y orgullosa como estoy ahora sin las carcajadas, momentos inolvidables y apoyo de las amistades que ICAI me ha aportado directa o indirectamente. Por todas las dudas que me habéis solucionado, por alegrarme los laboratorios a las ocho de la mañana (cosa no fácil), descansos de 5 minutos que se convierten en sesiones intensas de cotilleos non-stop y usar como única motivación post-exámenes: "*pff el pachá que nos vamos a marcar*". GRACIAS. Vosotros sabéis quien sois.

Este último año lo he pasado fuera de mi casa. Mi primera aventura *riding solo*. Un año que puedo describir con dos palabras: Extraordinario e Inolvidable. Quiero hacer especial mención en este párrafo a las personas que han hecho de estos 12 meses algo inigualable. Me gustaría empezar con mi Quinteto Estrella (Ainhoa, Hannah, Laura y Sara). Yo llegué como una estudiante española loca por disfrutar de la experiencia Erasmus y vosotras me hicisteis y me hacéis sentir en casa, aunque esté a más de 1.500 km. Seccondly, perdonad mi cambio de lenguaje pero quiero hacerlo más personal, Ezra Wierenga and Yang Zhao, you two provided the friendship I needed when the world decided to become a scary science fiction movie. You were my support when my social Erasmus ended. In March, I thought the world ended for me, but you taught me how to get the best out of this situation and you gave the motivation I needed to finally start and finish this thesis. Thank you. Finally, I want to end this paragraph with the most joyful surprise 2020 gave me:

Nout van den Bos. Wij hebben elkaar onverwachts ontmoet en ik zou daar niet blijer over kunnen zijn. Jij brengt rust in mijn gestoorde leefstijl en ik voel me een beter mens wanneer ik met jou ben. Ik bewonder je passie en toewijding aan alles wat je doet, en dat is ook precies wat mij motiveert om een betere versie van mezelf te zijn. Dankjewel voor het verschijnen en het blijven.

Finalmente quiero recalcar que me siento muy afortunada por tener a personas tan maravillosas en mi vida. Tengo mucho que agradeceros. Gracias a todos vosotros que habéis contribuido a mi formación como persona. Vosotros sois los principales actores por lo que hoy me puedo llamar finalmente INGENIERA.

Resumen

La sociedad de la información en la que vivimos está fundamentada en dos pilares: la privacidad y el anonimato. Esta sociedad está evolucionando rápidamente a una era online gracias a la digitalización. Esta transición genera algunas dudas sobre cómo nuestros datos privados y nuestro anonimato se gestiona dentro del mundo virtual y cómo de anónimos de verdad somos. En algunas redes, como la blockchain, cada acción ejecutada por los usuarios se guarda y se enumera en dicho sistema. Esto implica que un ataque o evento no esperado en la red podría revelar datos personales y confidenciales de los usuarios, por ejemplo, dirección privada, información bancaria o datos secretos. Ese es exactamente el foco de esta tesis: Cuantificar el impacto de la externa de-anonimización en mix networks. En otras palabras, ¿Cómo sabemos cuánto cambió el anonimato proporcionado por la red después de un evento de de-anonimización? El término de-anonimización hace referencia a los posibles errores que los usuarios de la red pueden cometer a propósito o sin darse cuenta y que podrían comprometer el anonimato total de la red mixta utilizada en este Trabajo Fin de Grado.

En este proyecto analizaremos un tipo específico de red llamada red mixta donde los mensajes enviados por los usuarios pasan por una serie de componentes llamados *mixes* que mezclan todos los mensajes entrantes y preparan un orden aleatorio para reenviarlos al siguiente salto, que podría ser otra *mix* o el destinatario deseado. Dado que esta red mixta está altamente interconectada, un evento de anonimización que afecta usuario (directamente) solo a un usuario, podría cambiar drásticamente el anonimato total proporcionado por la mix-net al disminuir número efectivo de usuarios involucrados en la comunicación no solo por uno (que sería lo que intuitivamente pensemos), sino por más.

La investigación realizada en este documento se centra en varias métricas utilizadas como herramientas para mostrar por qué la reducción en el número total de usuarios efectivos de la red (llamado conjunto de anonimato, o *anonymity set* en inglés) a través de un evento externo de de-anonimización puede afectar negativamente a los usuarios restantes, más allá de la simple disminución del tamaño de la red. Se creó una medida para mostrar la diferencia y la relación entre el número de usuarios efectivos antes y después de un evento de de-anonimización: tasa de anonimato *AR* (*anonymity rate*). Junto con la medida Grado de anonimato *d* (*degree of anonymity*), se concluye y se demuestra que si un usuario pierde su anonimato en una red con N usuarios, eso genera una de-anonimización total o parcial del sistema, siendo el nuevo anonimato real establecido en la red menos de N -1.

Esto se debe al hecho de que los usuarios están relacionados entre sí y desarrollan dependencias dentro de la red que deben tenerse en cuenta.

Finalmente, con esta tesis ahora podemos cuantificar el impacto de la de-anonimización externa cuando los usuarios pierden su anonimato a propósito o inadvertidamente. El impacto de esto es que ahora somos conscientes de que la pérdida de anonimato de un usuario impacta de manera más fuerte en la red que lo que podríamos pensar en un principio; en lugar de restar un solo usuario al número total de usuarios de la red. El objetivo final es diseñar un sistema que sea lo suficientemente resistente como para que apenas se vea afectado cuando un usuario sea de-anonimizado. Lo que significa que la red objetivo que deseamos alcanzar debe poder disminuir el impacto que tiene un evento de pérdida de anonimato sobre la red mixta, siendo el *ultimate goal* que la red mantenga el mismo nivel de anonimato proporcionado a los usuarios antes y después de dicho evento.

Abstract

Privacy and Anonymity are the two main important topics of the quickly transitioning society to an online era thanks to Digitalization. This transition does generate some hesitations regarding our private data and our anonymity inside the virtual world. In some online networks, such as blockchain, every action executed by the users is saved and listed at the system. This could imply that a possible attack or non-expected event in the network could reveal sensitive personal data of the users, for instance private address, banking information or secret data. And that is exactly the goal of this thesis: Quantifying the impact of external de-anonymization in mix networks or How does the external de-anonymization affect the users'anonymity guarantee of mix networks?. In other words, how do we know how much the anonymity provided by the network changed after a de-anonymization event took place. The term de-anonymization refers to possible mistakes that network users may do purposefully or inadvertently that could result in compromising the total anonymity of the mix network.

In this thesis we will look into a specific type of network called mix network where the messages sent by the users go through a series of components called mixes that shuffle all the inbound messages and prepare a random order to forward them to the next hop that could be another mix or the actual desired recipient. Since this mix network is highly interconnected, a de-anonymization event affecting only one user (directly) could severely change the total anonymity provided by the system by decreasing the effective number of users involved in the communication not only by one, but more.

The research and approach done in this paper is focused on several metrics used as a tool to show why reduction in total number of effective users of the network (anonymity set) through an external de-anonymization event can negatively affect the remaining users, beyond the simple decrease of the network size. One measure was created to show the difference and relation between the number of effective users before and after a de-anonymization event: Anonymity Rate *AR*. Together with the value Degree of Anonymity *d*, it is concluded and proven that if one user de-anonymizes itself in a network with N users, that generates a total or partial de-anonymization of the system being the new real anonymity set less than N-1. This is due to the fact that users are inter-related, and they develop dependencies inside the network that must be taken into account.

Finally, with this thesis we are now able to quantify de impact of external de-anonymization when users lost their anonymity purposefully or inadvertently. The impact of this is that, consequently, we are aware that the loss of one user impacts in a stronger way in the network, rather than only subtracting one user of the total number of network

users. The ultimate goal is to design a system that is resilient enough to being hardly affected when a user is de-anonymized. Meaning that the desirable network must be able to decrease the impact that a de-anonymized event has over the mix network. Being the final purpose that the network maintains the same level of anonymity provided to users before and after said event.

Index of the Thesis

Chapter 1. Introduction 5

1.1. Approach of the Project 5

1.2. Privacy and Cryptography 7

1.3. Characterizing Anonymity 9

1.4. Information Theory Background 12

1.5. Problem Statement and Research Objectives 13

1.6. Motivation 13

1.7. Thesis Outline 15

Chapter 2. Description of the Technologies 17

2.1 Unobservability, Untraceability and Unlinkability 17

2.2 General Anonymity Metrics 20

2.3 Unlinkability and Mix Networks 21

2.4 Adversarial Threat Models 22

2.5 Mix Networks 24

2.6 Synchronous Batching 28

2.7 How to measure Anonymity? 29

2.8 Related Work 33

2.8.1 Anonymity Solutions for Blockchain 33

2.8.2 Onion Routing for Mix Networks 34

2.8.3 Development for Mix Networks 35

Chapter 3. Description of the Developed Model 37

3.1. Objectives and Specification 37

3.1.1. Simple example based on Chaum Mix Network 38

3.2. Data used: Mixing strategies considered 45

3.2.1. Comparison of Batching Strategies Between Mixes 45

3.3. Algorithms, Method & Models 49

3.4. Numerical Implementation 54

Chapter 4. Analysis of the Results 60

4.1. Examples and Results 60

4.1.1. GPA Attack Example 63

4.1.2. De-anonymization Example 69

Chapter 5. Conclusions 75

5.1. Conclusions on the Methodology and Results 75

5.2. Recommendations for Future Studies 76

Chapter 6. References 78

Chapter 7. Appendixes 83

Appendix SDG 83

Appendix I 87

Appendix II 87

Appendix III 88

Appendix IV 89

Appendix V 90

Index of the Figures

Figure 1. Sender Untraceability. 17
Figure 2. Receiver Untraceability. 18
Figure 3. Unlinkability. 18
Figure 4. Traffic Analysis vs Traffic Confirmation Attacks. 19
Figure 5. Cascade Example. 25
Figure 6. Cascade Encryption Procedure. 26
Figure 7. Anonymity set. 32
Figure 8. Example Chaum. 38
Figure 9. Active Attack Example 40
Figure 10. Passive Attack Example 43
Figure 11. Value of p with d = 0.8 44
Figure 12. Comparison of batching strategies between mixes. 48
Figure 13. First Scenario: Threshold Mix with anonymity set. 49
Figure 14. Second Scenario Threshold Mix with anonymity set. 50
Figure 15. Anonymity rate example (AR = 1) 54
Figure 16. Anonymity Rate example (AR < 1). 56
Figure 17. Anonymity Rate graph with N = 2 58
Figure 18. Anonymity Rate graph with N = 3 59
Figure 19. Third Scenario One Threshold Mix with effective anonymity set size. 60
Figure 20. Notation for anonymity probability distribution. 61
Figure 21. Notation example for effective anonymity set size with several mixes. 62
Figure 22. Global Passive Attack Example. 63
Figure 23. Global Passive Attack Specific Example. 64
Figure 24. De-anonymization Layout Example. 69
Figure 25. Specific User De-Anonymizing Example 70

Index of the Tables

Table 1. Glossary for the mixes types. 46

Table 2. Comparing Batching Strategies for mixes. 47

Chapter 1. INTRODUCTION

1.1. APPROACH OF THE PROJECT

Blockchain networks are usually associated with anonymity in the general public eye [1]. Initially some people considered the Blockchain as the perfect method to hide anonymous transactions on black markets, even though most of the volume of Blockchain transaction, have little to do with crime [2]. It is needed to be mention that in blockchain, every transaction made between senders and recipients is listed at the blockchain system. Thus, a de-anonymization attack could have the result of revealing quite sensitive personal data of users, such as banking history, passwords or private information. Additionally, the Internet environment is quickly changing, evolving and developing since the world is transitioning to an online era thanks to Digitalization. We are advised to not provide personal data, not sharing private information and not exchanging confidential facts. However, following all those recommendations may seem very problematical in some circumstances. This has enhanced the concern about the protection of anonymity in Internet users.

According to the European Union Law, digital infrastructures need to find the balance between guaranteeing the preservation of our values and fundamental rights such as respect to private life (Article 7 from [3]) and protection of personal data together with a fair data processing for specific purposes (Article 8 from [3]). This is important as more of the daily life activities are moving online, but effective tools for privacy, which includes anonymity systems, are lagging behind compared to de-anonymization tools. However, several papers have explicit statements confirming the opposite [4], there is a major lack of anonymity in blockchain networks, where effective anonymity still has not been achieved, thus they do not guarantee financial privacy.

This thesis will not be based on the Blockchain technology but in the Mix Networks, nevertheless the same statements can be applied for this technology. The main goal of this paper is to study how this de-anonymization of users may change the degree of users' anonymity in mix networks.

But, how do we remain unknown when we are almost forced to give away all our personal information to fulfill online tasks or requirements? This is false to think that this trade-off is inevitable, in fact we can participate in online activities without losing too much privacy if we do so anonymously. Anonymity is not only valuable on its own (not being known in the network) but also an important tool for privacy protection (users can interact in a network that makes correlation of personal data more difficult).

In the following sections it will be discussed the concrete definitions of privacy, cryptography and anonymity together with the techniques used to answer the research question of this BSc thesis: **How does the external de-anonymization affect the users' anonymity guarantee of mix networks?** The external de-anonymization refers to possible mistakes that network users may do purposefully or inadvertently that could result in compromising the total anonymity of the mix network. This can be done in several ways, for instance, a user could include extra identifiable information such as name, credit card details or personal addresses in the message sent when it is not needed. If we assume that the recipient it is an untrusted user, the send is completely de-anonymized. These scenarios can also be extrapolated to the blockchain transaction context where all the movements are generally public, and everyone could have access to it.

At this paper, I propose several measurements as a tool to show why reduction in total number of effective users of the network (anonymity set) through external de-anonymization can negatively affect the remaining users, beyond the simple decrease of the network size. In other words, in this thesis will be study and proven that if one user de-anonymizes itself in a network with N users, that could generate a total or partial de-anonymization of the system that would result in being the new real anonymity set less than N-1. Further in the research, I will show how the users are related and how the dependencies inside the network must take into account.

1.2. PRIVACY AND CRYPTOGRAPHY

Humans beings have the fundamental need for personal and intimate spaces to communicate or express our most deep thoughts and feelings. When these secret spaces are threatened by surveillance, governments or attackers, the effects are devastating. The surveillance may have some negative effects for individuals, such as conformism and loss of autonomy. Moreover, this could also affect the entire society, not only individual people, by producing social exclusion and discrimination, social homogenization, behavioral conformism and decline of solidarity [5].

Privacy and Anonymity are two key concepts for the human's essential need for personal and intimate spaces to express themselves. **Privacy** is defined by the Cambridge Dictionary as "*the state of being free from public attention*". A trivial example would be if you go to any clothing shops and you want to try some clothes on, you would close the dressing room not because you are doing something illegal or planning how to steal that item, but simply because you want to keep that activity to yourself. This term was first technically defined by Westin in 1967 [6]. However, that definition seems now outdated and a vast number of developments have taken place in the Privacy field since that year, therefore a more accurate definition of *privacy* is needed for this thesis. Privacy could be defined, in this thesis background, as the relationship between the data exchange during online communications, the public expectation of privacy and legal or/and political issues surrounding this topic. [7]

This search of intimacy for ourselves or to communicate had a crucial role in creating secure communication via private conversation [8]. It may seem easy to ambush and understand a standard private conversation, standing next to the place where the conversation is taking place, having micros or intercept the message are examples on how to make a private conversation, not so private. However, if the message communicated is not understandable for third parties (people not involved in the conversation), it will remain as a private conversation. This is what Cryptology studies and tries to achieve.

For a deeper understanding of this concept, it is necessary to know the differences between Cryptology, Cryptography and Cryptanalysis? This is a mathematically complex, wide and interesting field. According to the Cambridge Dictionary: **Cryptology** is the study of codes, both creating and solving them, **Cryptography** is the art of creating codes, and **Cryptanalysis** is the art of surreptitiously revealing the contents of coded messages, breaking codes, that were not intended for you as a recipient.

Let's explain these ideas with an example. Imagine you want to communicate a secret message to a friend, for instance, "meet me at 4 PM". If you have knowledge on ***cryptology***, you would know that "meet me at 4 PM" can be coded as "103A". By sending "103A" instead of the previous message you are making use of ***cryptography***. Now, suppose that someone wants to intercept your message and decode it. They will need to use ***cryptanalysis*** skills and methods to do so.

Encryption is the process of taking a message and mixing its contents so only certain people can have access to your message. There are two types of encryption: symmetric and asymmetric encryption. This paper focuses on asymmetric encryption, but it is necessary to explain how symmetric encryption works, so we can understand why asymmetric encryption was created.

- ***Symmetric encryption:*** A (sender) wants to share a sensitive message to B (receptor). A uses an encryption algorithm to protect her document with a password (key) that A chooses. A sends the message to B. However, B cannot decode the message because B does not have the password or key that A used to encrypt the message. How does A share the key securely with B? Sending the key as A did with the message is risky because others might find the key and use it to decrypt any messages between A and B. This is exactly the kind of problem that asymmetric encryption aims to solve.

- ***Asymmetric encryption:*** Sender A and receptor B will have to generate a keypair on their computers in order to provide secure communication (a popular and secure way of doing this is by using the RSA algorithm [9]). Public keys can be used to encrypt data and only the matching private key can be used to decrypt it. Even though the keys are linked together, they cannot be derived from each other. Once we send a message to B, they are the only one who has the private key that is needed to open it. This communication starts by exchanging public keys. B gives his/her public key to A and A gives his/her public key to B. Now A can send the message encrypted with B's public key and B can "unlock" it using his/her

> private key. The security of this type of communication fully relays on A and B keeping their private keys well protected[1].

The concept of **public key cryptography** was first introduced in the seventies by W. Diffie & M.E. Hellman [10] and R.C. Merkle [11]. Nowadays, we can define public key cryptography, also known as asymmetric cryptography, as the system that uses a pair of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. The generation of such keys depends on cryptographic algorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security [12]. (*This subject will be explained in more details in Section 2.1.*)

1.3. CHARACTERIZING ANONYMITY

In contrast to confidential communication where message content is private, but identities of parties may be public., sometimes you would want people to know the action but not who carried it out. For example, if you donate anonymously a large amount of money to a charity event, everyone would know that action took place but not the name of the person that did it. This is when **anonymity** takes a lead role.

In order to standardize further terminology Pfitzmann and Köhntopp published in 2000 their paper "*Anonymity, unobservability and pseudonymity – a proposal for terminology*" where they make an attempt to clarify and define different concepts that will be important for this thesis. They define anonymity as:

> "Anonymity is the state of being not identifiable within a set of subjects, the anonymity set. Anonymity is stronger, the larger the respective anonymity set is and the more evenly distributed the sending or receiving, respectively, of the subjects within that set is". [13]

[1] Example based on Christof Paar, Jan Pelzl, "Introduction to Public-Key Cryptography", Chapter 6 of "Understanding Cryptography, A Textbook for Students and Practitioners". (companion web site contains online cryptography course that covers public-key cryptography), Springer, 2009.

Following the anonymity description above, the concept "***even distribution***" becomes a new requirement for judging the quality of anonymity provided by a mix network. Not only size but also distribution. But what is even distribution? It is understood as evenly distributed something that is spread equally. In mathematics it is denoted as **f(x) = f(-x)**. In other words, being as symmetrical as possible.

The main focus of this thesis is going to be in the **online anonymity**, more specifically in the network layer of distributed systems like blockchain. As I have previously mentioned, anonymity depends on how others behave, thus the key element of this research thesis will be how the purposefully or inadvertently de-anonymizing themselves.

Before describing any anonymity related measure, some standards terms which are useful in describing anonymity systems will be introduced following the terminology by Pfitzmann and Köhntopp [13]. This thesis will treat the anonymity protection of multi – party[2] asynchronous communications protocol[3] in which participants send messages to each other [14]. Some of these messages are ***real***, meaning that contain relevant information that needs the protection of the **sender** (person who originates the message, or have the ability to send it, and sends it to the receptor), the **message** (information that the sender sends to the receptor. Could be emails, request for websites or any other stream of data) and the **receiver/recipient** (person who gets the message and tries to understand what the sender wants to convey and then responds according. The recipients can be either *active*, if they send answers back to the senders, or *passive,* if they do not react to the received message.). It gives the protection against the attackers by making it (almost) impossible to decode what's said, who sent it and who received it. This is done by using a computer called a ***mix*** [15] that provides anonymity between the 3 elements mentioned. A mix is a computer that hides information such as the correspondences between items in its inputs and outputs and a mix network [15] refers to the system of interconnected people that uses a mix as a way of protection. It can be described as a router that slow

[2] The term *Multi – party* makes reference to the fact the system involves several users in the form of senders and/or recipients.

[3] Serial communications or *asynchronous communication* is the process of sending data one bit at a time through a channel. In contrast to parallel or synchronous communication where several bits are sent as a whole on a link with several parallel channels.

down the messages and re-arrange them to cover incoming and outgoing messages. [16] (*This subject will be explained in more details in Section 2.3.*)

The goal of the attacker or the adversary that we are trying to avoid is to discover senders and recipients of these *real* messages. Other messages, called *dummy messages*, do not contain relevant information and are just sent automatically to confuse the attacker [14].

The senders, above explained, can be grouped into something called the *set of senders*, that is also called the ***anonymity set***, this concept was first mentioned by Chaum in 1988. The anonymity set is defined as the total number of users that could have sent a specific message and seen by an adversary who has compromised the network. [17]. It is argued that the **size** is a good indicator of how good anonymity provided by the network is. In the worst-case scenario, the size of the anonymity set is 1, meaning that only one user is sending a message, there is no anonymity provided to this specific user. In the best-case scenario, the size of the anonymity set equals the size of the network, meaning that everyone could have sent that message.

For instance, if we are in a room (with very good acoustics) full of people and, suddenly, a phone rings, we are unable to determine who is the owner of that phone. All the people standing in that room has the same probability of being guilty from disturbing the event. However, if there is only one person there and a phone rings, you have a 100% probability of being the owner. (Assuming no one left their phone there). Therefore, the **size of the anonymity set** could be used as an **anonymity metric** [18]. A deeper look will be given to this subject in Section 2.7 where it will be discussed how to measure the mix network degree of anonymity.

1.4. INFORMATION THEORY BACKGROUND

We have now discussed several terms that are need for a deeper comprehension of my thesis. Since the main goal of my BSc thesis is to measure anonymity under a series of assumptions and scenarios, terminology regarding Information Theory [19] is needed.

Information theory studies the quantification, storage, and communication of information. Applications of information theory include lossless data compression[4] (ZIP files), lossy data compressions[5] (MP3s and JPEGs), and channel coding (DSL). A key measure in information theory is ***entropy*** [19].

Definitions needed:

- **Random Variable X**: A random variable is described informally as a variable whose values depend on outcomes of a random phenomenon [20] and formally as a measurable function defined on a probability space that maps from the sample space to the real numbers [21].
- **Possible outcome x_i:** an outcome is a possible result of an experiment or trial. All of the possible outcomes of an experiment form the elements of a sample space [22].
- **Probability $P_X(x_i)$:** Probability is a numerical description of how likely an event is to occur or how likely it is that a proposition is true. **$P_X(x_i)$** denotes the probability of getting the outcome **x_i** of a random variable **X**.
- **Entropy:** An entropy is a basic quantity in information theory associated with any random variable. It is defined as the average level of *information*, *surprise*, or *uncertainty* inherent in the variable's possible outcomes.

[4] Lossless compression is a type of compression that allows the original data to be perfectly reconstructed from the compressed data.
[5] Lossy compression is the class of data encoding methods that uses inexact approximations and partial data discarding to represent the content.

1.5. PROBLEM STATEMENT AND RESEARCH OBJECTIVES

The specific question that will be addressed in this thesis is: **How does the external de-anonymization affect the users' anonymity guarantee of mix networks?** The external de-anonymization refers to possible de-anonymizing behaviour that network users may do purposefully or inadvertently that could result in compromising the total anonymity of the mix network.

Moreover, this research also has ethical significance, since users of anonymous systems can be exposed to significant harms if such systems fails. Thus, it is important that limitations of anonymity can be accurately assessed by the users and designers of these systems.

1.6. MOTIVATION

As it was already mentioned, Mix network anonymity was first mentioned in 1981 by David L. Chaum at his paper in *Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms*.

This paper published 40 years ago, was used as a starting point of TOR[6], an open-source software based on the Onion Routing Protocol widely used techniques to anonymize communications over a computer network. In an *onion* network, the information is encapsulated in layers of encryption, similar to layers of an onion. The encrypted information is forwarded through a series of network nodes called *onion routers*, each of which decrypts the *superficial* layer (following with the onion example, the routers will *peel away* a single layer), uncovering the data's next destination. When the final layer is decrypted, the message arrives at its receiver. The sender remains anonymous because each intermediary knows only the location of the immediately preceding and following nodes [23]. In other words, by using this protocol, the user will remain anonymous by the receiver or any node in the network between the sender and the receiver [24].

[6] The name is derived from an acronym for the original software project name "The Onion Router".

However, there is a lack of research on external de-anonymization factors that could result in the de-anonymization of the users, for instance, the probability of a mix network user doing a mistake that could result in a general drop of the anonymity level of the network. The closest study or research done in this field was exposed in the paper *How Do Tor users interacts with Onion Services?* [25]. In that paper Winter et al. studied how people perceive, understand and use onion services based on data obtained via interviews and an online survey done to TOR users. The paper provides answers, that could be used as motivation for my work, to the following questions: (1) What are users' mental models of onion services? (2) How do users use and manage onion services? These questions serve as a reference for blockchain anonymity systems since the paper acknowledges the fact that external de-anonymization is common in TOR networks. In other words, my research will contribute to the area of knowledge on the probabilistic assessment of anonymity changes caused by user's actions not in TOR networks, but in **mix networks**.

Another paper treating users interaction in the Blockchain Ethereum[7] network that could lead to their possible de-anonymization is [26]. Béres et al. showed that is possible and not so difficult to pair Ethereum user accounts that are run by the same identity. Users might have several different accounts for different purposes and [26] exposes 3 measures (transaction timestamp or daily activity behavior of the account owner, the gas[8] price distribution and transaction graph analysis or general user's interaction), that lead to an inadvertent de-anonymization of Ethereum users by linking two or more accounts to the same person or organization. Users that are owners of multiple accounts might interact with the same addresses several times and by doing so, they may unintentionally reveal their personal address [26].

[7] Ethereum (ETH) is a cryptocurrency launched in 2015, known as the world's programmable blockchain. In other words, Ethereum is digital money that can be sent to any person at any place in the world instantaneously. The supply of ETH is not controlled by any government or company, meaning that it is decentralized, these decentralized applications receive the name of *dapps*. The difference between Ethereum at the other most famous cryptocurrency (Bitcoin) is that Ethereum is programmable, which means that developers can use it to build any sort of applications.
Definition based on Ethereum official website: https://ethereum.org/what-is-ethereum/

[8] The "gas" term in Ethereum refers to the fee that users are required to pay in order to successfully perform a transaction using this cryptocurrency.

1.7. THESIS OUTLINE

This thesis provides a first general idea of mistakes and procedures that mix network users could do to inadvertently de-anonymized themselves. However, my thesis it is not based on the Blockchain scheme mentioned on the previous section, but on the mix networks. It is also important to mention that this project will not have its focused on the actions done by the users that lead to a de-anonymization event, but on how the mix network anonymity is affected after this event takes place. Nevertheless, those 3 examples and ideas serve as motivation to show that this de-anonymization event can happen, also, in the mix-net background because those mistakes can be done in any kind of network. It will be always possible to determine the timestamps of the messages and it will be always possible than a user provides more information than necessary in a message, producing its possible de-anonymization.

In order to address the de-anonymization issues and results, statistics and probabilistic models will be used. The parameters will be defined, explained and justified, and a simulation of the models will be done. It is important to mention that a further look at the mixes will not be done, meaning that this thesis will not do any coding regarding the setting up of the mixes nor real-world implementation out of the scope of the thesis.

We will know that the results obtained are good if the thesis fulfills 3 aspects. Firstly, the thesis detailed a realistic situation that could be easily related to reality just by adding more components and elements. In this case, I have designed a network with 5 users where 1 of them is completely de-anonymized. Secondly, sufficient repetition has been done, meaning that the results will be consistent. The method exposed in this thesis is being repeated and explained over the entire project, ending with 2 complete examples in Section 4.1.1 and Section 4.1.2. Thirdly, the result of this thesis will discuss the ethical implications of the findings exposed at the Appendix SDGs.

The remainder of this paper is organized as follows. In Chapter 2, it is presented a brief, high-level overview of the technology studied, an explanation of all the mixes types and proposals of the most suitable mix for this work, general anonymity metrics and possible adversarial threat models will be included. In Chapter 3, it is explained the description of the developed model together with a discussion of the mix type chosen, including the objectives and specification, data used, algorithms needed and the numerical implementation. In Chapter 4, it is exhibited the analysis of my research with the main results. Finally, the research concludes in Chapter 5 with the conclusions of the project, discussing remaining open problems and possible future work.

Chapter 2. DESCRIPTION OF THE TECHNOLOGIES

2.1 UNOBSERVABILITY, UNTRACEABILITY AND UNLINKABILITY

In order to measure anonymity, it is necessary to understand 3 concepts: unobservability, untraceability and unlinkability. After a specific time determined by the network (a run of the protocol), the *real* messages are sent by the senders and received by the recipients. Depending on the protocols used the network could provide to the ***sender untraceability*** (also called ***unobservability***). "*Unobservability ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used*." [32]. In other words, the adversary is not able to determine whether a particular user has sent any real messages or not (see Figure *1*). On the other hand, if the attacker or the adversary is unable to determine whether a particular user has received any real messages or not, the protocol provides ***receiver untraceability*** [14] (see Figure *2*). A very strong protocol might provide both sender and receiver untraceability.

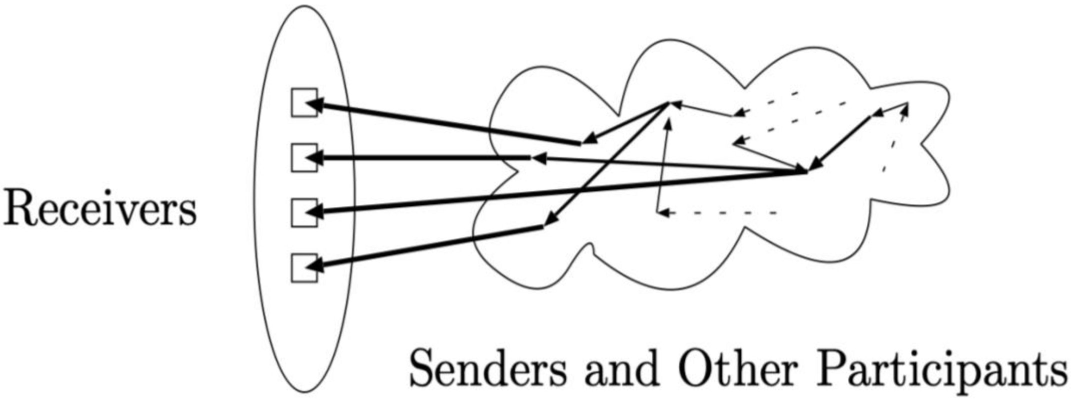


Figure 1. *Sender Untraceability.*
A system which provides only sender untraceability as seen by the adversary. [14]

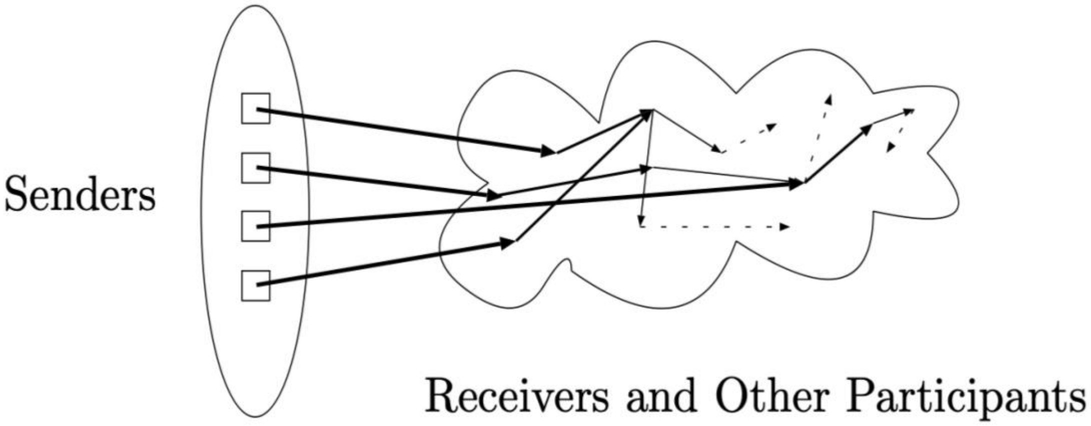


Figure 2. *Receiver Untraceability*.
A system which provides only receiver untraceability as seen by the adversary. *[14]*

Lastly, the protocol could provide ***unlinkability.*** *"Unlinkability ensures that a user may make multiple uses of resources or services without others being able to link these uses together."* [32]. Meaning that if the set of users if known by the attackers (senders and recipients), but they cannot determine which of the senders sent the *real* messages to which of the receivers, the system is providing unlinkability (see Figure *3*).

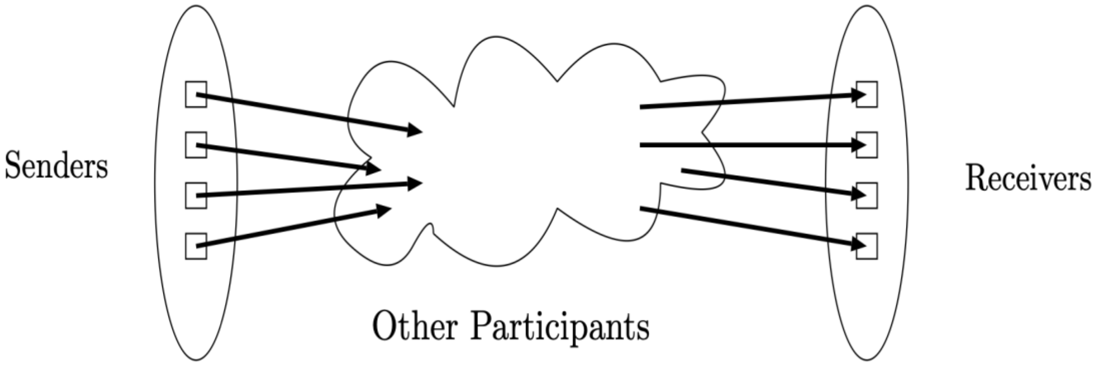


Figure 3. *Unlinkability*.
A system which provides unlinkability as seen by the adversary. *[14]*

Unlinkability can be also defined as ***relationship anonymity*** [33] defined by Pfitzmann, Köhntopp and Shostack in 2001 as "*relationship anonymity means that it is untraceable who communicates with whom*" [13]. In other words, the goal of relationship anonymity or unlinkability is to hide that a sender A is communicating with a receptor B. Whereas the goal of *sender anonymity* is to hide the fact that sender A sent a message and the goal of *recipient anonymity* is to hide the fact that receptor B is the desired destination. **It is important to mention that in this thesis we will be dealing mainly with systems that provide unlinkability.**

Generally, there are two types of attack that the adversary can perform on these systems (See Figure 4). (1) A ***traffic confirmation attack*** is where an adversary only examines on two ends of the network with the only goal of linking the sender and receiver of communication happening in the network [34]. (2) And a ***traffic analysis attack*** consists in the process of intercepting and analyzing messages in order to gather and deduce information from patterns in communication within in the specific network, so later on the attackers can decrypt the messages [35] [36]. This last type of attack is usually the one that the adversaries use.

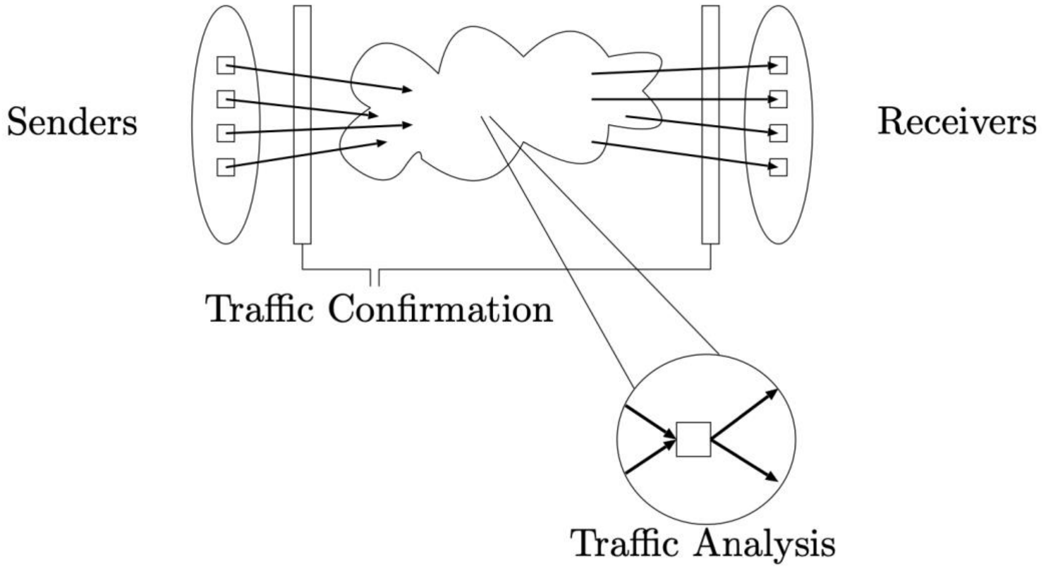


Figure 4. *Traffic Analysis vs Traffic Confirmation Attacks*.
A traffic confirmation attack examines only the communications between the senders and the anonymity system and the anonymity system and the receivers. A traffic analysis attack also makes use of traffic patterns within the anonymity system *[14]*

2.2 GENERAL ANONYMITY METRICS

Díaz et al. propose a distinction between ***data anonymity*** and ***connection anonymity*** [27]. On the one hand, data anonymity has been defined as a process where personal data is irreversible changed in a way that an user can no longer be identified by the data controller [28]. In other words, data anonymity is based on identifying private information out of the data that is exchanged between the sender and the receiver. On the other hand, connection anonymity is based on keeping unknown the identities of the sender and the receiver during the entire communication process. My thesis will be based on this anonymity level.

Regarding the question of how to measure anonymity, there have been several answers to measure the degree of anonymity of a user provided by an anonymous system. In this thesis, that system will be formed by a mix network. Those attempts are explained below.

Reiter and Rubin [29] define the degree of anonymity as $\boldsymbol{1-p}$, where $\boldsymbol{p}$ denotes the probability assigned to a particular user by the attacker. Berthold et al. [30] define the degree of anonymity as $\boldsymbol{A = \log_2(N)}$ where $\boldsymbol{N}$ is the number of users of the system.

The size of the network (number of users) plays an important role as a good indicator of how good the anonymity provided by the network is. In the worst-case scenario, the size of the network will be 1 (that very user was the one sending the message) and in the best-case scenario, it is the total number of users of the network (any user could have sent the message) [15]. Let's explain this with an example: if I have an accident with my personal car and neither no one has access to it nor I let other people use it, there is a 100% probability that I am the one driving the car at the moment of the accident. However, if it is a company car that everyone can use because at our first day at work we all receive a key to it (and there is no control about who takes the car) we cannot know exactly who was at the car accident, all the employees at the company share the same probability of being inside the car. Using the concept of quantiles [31] it would be possible to determine lower and higher bound outliers that would help us determine the number of users for our specific network that is necessary to provide, for instance, 90% of anonymity. (*The concept of quantile would be explained in more details later on).*

The anonymity metrics that would establish the foundations of this thesis were proposed in two papers presented at the *2nd Workshop on Privacy Enhancing Technologies*. The paper by Serjantov and Danezis [18] uses entropy as a measure of the ***effective anonymity set size*** *(See Section 3.3 for more information).* The one presented by Díaz et al. [27] normalize the entropy presented in [18] to obtain a ***degree of anonymity*** in the scale from 0 to 1. *(See Section 2.7 for more information).*

2.3 UNLINKABILITY AND MIX NETWORKS

The BSc Thesis that I am writing is based on Chaum's idea of anonymity in mix networks. The development of anonymity systems started with a paper by this author in 1981 proposing a course of action for untraceable electronic mail. The paper of David L. Chaum presents a solution to the traffic analysis problem presented in Section 2.2 based on the public key cryptography protocol presented in Section 1.2.

The system proposed by Chaum provides anonymity in the field of email services thanks to the use of several mixes. The mix explained in that paper is known as the ***threshold mix*** (*the different types of mixes will be discussed in Section 3.2)* where the sender S aims to send an anonymous message to recipient R via several mixes. Each mix has a public and private key pair; the public keys are given to the senders in advance. The sender prepares the message by padding the information in a concrete number of bytes used by all senders and encrypts the message with the public key of the recipient. In other to explain the process, let's suppose that in order to send a message from S to R, the messages need to go through 3 mixes (M1, M2 and M3. Being M1 the closest to S and furthest form R, M2 the *middle* one, and M3 the closest to R and furthest to S). Then, the sender needs to append the address of the recipient R and need to encrypt it with M3 public key, append the address of M3, encrypt with M2 public key, append the address of M2, encrypt with M1 public key, and finally sending the entire assemblage to M1 [14].

When the message is first sent to M1, it is decrypted, and placed inside the mix. Now a ***flushing algorithm*** [37] must be executed to decide how, when and which messages are going to be forwarded to the next mix or to their recipients. The simplest example of a flushing algorithm is waiting until ***n*** messages are inside the mix and once it gets to *n* messages, the mix reorders them and sends them all out to their next destination. A mix executing this algorithm is called a ***threshold mix*** [14]. Other flushing algorithms that may result in more efficiency for this thesis will be discussed in the following sections.

KEY IDEAS OF CHAUM'S PAPER RELATED WITH UNLINKABILITY::

Chaum proposed hiding the correspondence between sender and recipient by packaging messages in covers of public key encryption and forwarding them to a network made on mixes. Then each mix must decrypt, delay and reorder the messages received before forwarding them to the next hop.

The system exposed at Chaum's paper in 1981 provides 2 types of unlinkability. (1) It provides ***unlinkability between inputs and outputs of a mix*** [14]. This means that an adversary that does not know the private key of a mix but he is able to watch the input and output route of it, cannot correlate incoming and outgoing messages to the senders and/or the recipients. (2) It provides ***unlinkability against any pair of non-consecutive collaborating mixes*** [14]. Meaning that, for instance, if the first and third mix are compromised, it is not possible to determine which messages were processed by which machine.

2.4 ADVERSARIAL THREAT MODELS

After explaining how the mix system operates, it is time to study the adversarial thread models that could decrease the degree of anonymity of a network. This degree of anonymity fully depends on the probabilities that the network users have over sending a particular message [27]. These probabilities are set by the attacker according to their knowledge on the network. Concrete assumptions over the type of attacker must be taken later on in this thesis. There are several adversarial thread models that could affect the degree of anonymity, the following represents the attacker properties that must be considered [36] [38]:

- ***Internal vs External***: An internal adversary has the control of one or several components of the network (e.g., a mix) and could have access to internal data of it. An external adversary can only intercept communication channels (e.g., he can monitor or *spy* a concrete message)

- ***Passive vs Active:*** A passive adversary does not modify the network but only pay attention to the communication or data (e.g., he can read internal information of the system but not acting on it). An active adversary is capable to append, delete and change the communication process, together with the data (e.g., he can remove a message sent from S to M1).

- ***Local vs Global:*** A local adversary has only access to control part of the network (e.g., he can control M1). On the other hand, a global adversary has access to the whole communication process (e.g., he can control the entire system).

- ***Static vs Adaptive:*** A static adversary has the control of a specific part of the network and he is unable to change later on the communication. An adaptive adversary can gain control over new resources or modify their behavior depending on how the communication takes place.

- ***Temporary vs Permanent:*** A temporary adversary observes or attacks the network at a specific time ***t₀*** and he does not have more information before that time. A permanent adversary has been observing the network since it first started the communication.

Several different combinations of the above properties are possible. At this juncture, it will be exposed to the most frequent combinations of attacks. (1) ***Global passive attacker***. According to Andrei Serjantov "*this is the most common threat model in the literature*". The adversary is only able to observe (passive) all the network communication process (global). (2) ***Global active attacker.*** The adversary is able to observe and make changes (active) to all the network communication process (global). (3). ***Global passive attacker with many compromised mixes.*** This specific concrete behavior was first studied in [30]. Berthold et al. explained that this attack is a very strong one, where the adversary knows the private key of the mix compromised and can eavesdrop the messages between the sender and the recipient. (4) ***Global active attacker with many compromised mixes.*** Same idea as defined in (3) with the difference that, now, the adversary is running the mix and can modify it.

It is important to specify that my thesis will no study in deep detail an attack *per se*. The main focus is on **users de–anonymizing themselves** and how this action could affect the degree of anonymity of the network.

2.5 MIX NETWORKS

As has been already mentioned, a user of the public key cryptosystem has to create a pair of keys K and K-1 following a random generating algorithm. The public key K can be known by all the users in the network but the K-1 can never be divulged. The encryption of a message X is denoted as K(X).

These two keys are inverses of each other meaning that $\mathbf{K_{-1}(K(X)) = K(K_{-1}(X)) = X}$

However, encrypting a message by only using the pair of keys is not enough because anyone could verify a guess that Y = X by checking whether K(Y) = K(X). This threat can be eliminated by attaching a string of random bits R to the message X. The encryption will look like this now: **K (R, X).**

If we want to escalate this to the mail system, the encryption explained it is not enough. We will need to use a computer call mix that will difficult the connection between the sender, message and recipient by processing each item before it is delivered. A ***mix*** is a server that accepts incoming messages and forwards them to their desired destination in such a way that an external observer cannot link an outgoing message with an incoming message. The mixes are usually implemented in networks that aim to provide a high level of anonymity to their users [33]. Now we will denote this as it follows:

$$\mathbf{K1(R_1, K_A(R_0, M), A) \rightarrow K_A(R_0, M), A}$$

Where A stands for a specific address of a network user. If one user of the network wants to send a message M to another user at the address A, it will be needed to, first adding the random string R_0, then encrypting the message with A’s public key K_A and then sealing the result with the mix's public key K_1. After doing this, the mix does the transformation from the input (before the →) to the output (after the →) using its private key K_{-1} to throw away the random string and outputs the reminder.

However, in mix networks one single mix it is not enough to satisfy the requirements of the network and series of mixes must be used. When these series of mixes use an already determined route through the network that it is fixed, it is known as ***cascade***. This set-up offers the advantage of providing a higher degree or anonymity since the messages are going to be mixed several times with other messages forwarded by many different origins. In order to properly encrypt a message in a cascade layout we need to seal the message with the public keys of the mixes that will intercept the message during the whole communication from sender to recipient. Look at Figure 5: (It is necessary to mention first that the lay-out exposed there, it is not the common schema that mix networks follow. Generally, in mix networks all the messages send by the senders pass through the same number of mixes. In the Figure 5 and Figure 6, this is not the case. However, it is not a problem because I created both figures just as an example to explain how the cascade encryption works).

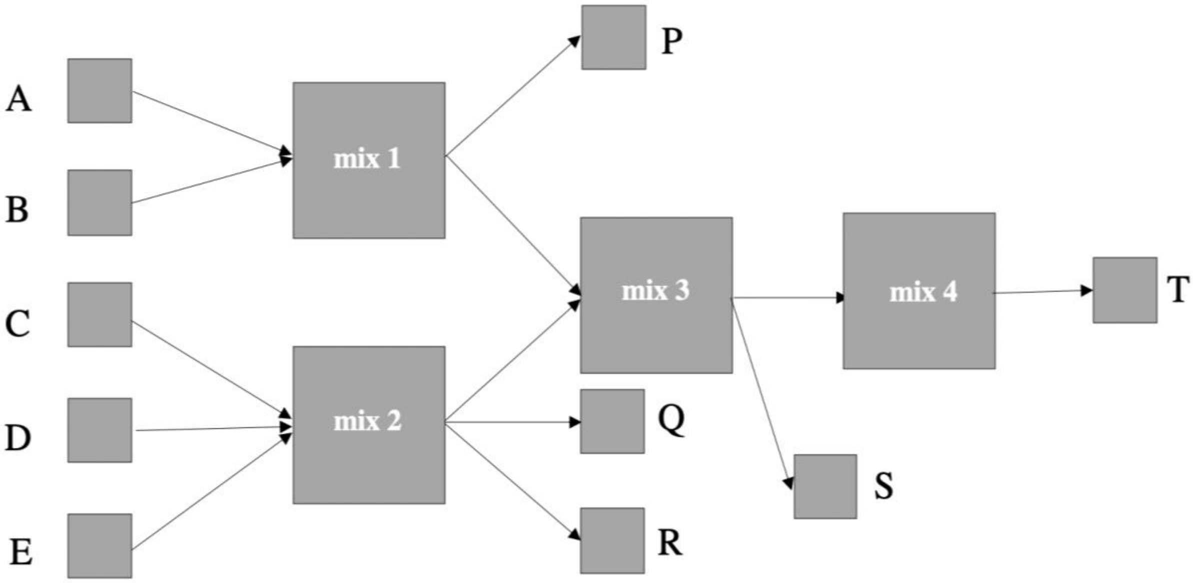


Figure 5. *Cascade Example.*
Example use to show notation regarding mix cascades.

If A wants to send a message M to T, this message must be encrypted with T, mix4, mix3 and mix1 public keys, being the encryption of T the deepest layer and the encryption of mix 1 the most *superficial* one. This will be denoted as:

$$\mathbf{K_1(R_1, K_3(R_3, K_4(R_4, K_T(R_0, M), T)))}$$

It is possible to perform this encryption procedure because the network has a fixed mix route due to the fact that the mix network is following a cascade layout and, as it was already mentioned, the main characteristic of a cascade is that the route is known before sending the messages.

The encryption procedure is shown in *Figure 6*:

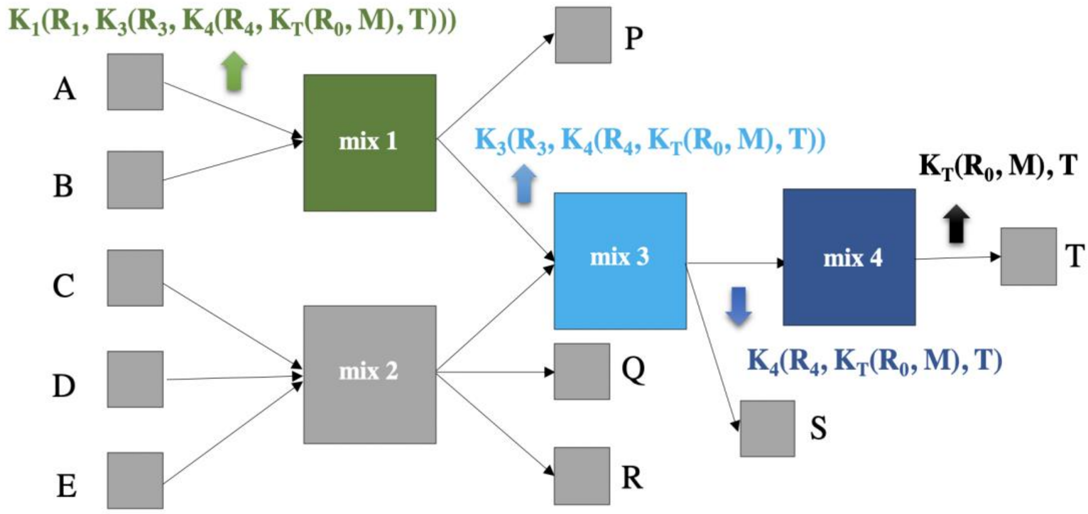

$K_1(R_1, K_3(R_3, K_4(R_4, K_T(R_0, M), T)))$
A
B
C
D
E
mix 1
mix 2
P
Q
R
$K_3(R_3, K_4(R_4, K_T(R_0, M), T))$
mix 3
S
$K_4(R_4, K_T(R_0, M), T)$
mix 4
$K_T(R_0, M), T$
T

Figure 6. *Cascade Encryption Procedure*.

That is the notation for a specific example, the general notation is as follows:

$$\mathbf{K_n(R_n, K_{n-1}(R_{n-1}, K_{n-2}(R_{n-2}, \dots , K_2 (R_2, K_1(R_1, K_A(R_0, M), A))))}$$

being ***A*** the address of the recipient, ***M*** the message sent and ***R₀*** the random string.

That describes the process that allows a user ***x*** to send messages to the desired user ***y*** using one single mix or series of mixes. Now it will be explained how y needs to respond to x while still keeping the identity of x unknown for y.

A solution will be that x creates an untraceable return address using the public key encryption idea [$K_1(R_1, A_x)$, K_x] where A_x is its own real address, K_x is a public key chosen for the occasion, and R_1 is the random string. Then, x can send this return address to y as part of a message sent first. Using the notation explain, y will receive this untraceable return address [$K_1(R_1, A_x)$, K_x] + the output of the mix [(R_0, M)]

$$\mathbf{K_1(R_1, A_x), K_x(R_0, M) \rightarrow A_x, R_1,(K_x(R_0, M))}$$

This mix uses the string of bits R_1 that it finds after decrypting the address part $K_1(R_1, A_x)$, as a key to re-encrypt the message part $K_x(R_0, M)$.

With a cascade of mixes, the messages are prepared to be returned in the same way as using a single mix:

$$\mathbf{K_1(R_1, K_2(R_2, \dots , K_{n-2} (R_{n-2}, K_{n-1}(R_{n-1}, K_n(R_n, A_x))) \dots)), K_x(R_0, M) \rightarrow}$$

obtaining as result of the first mix:

$$\mathbf{K_2(R_2, \dots , K_{n-2} (R_{n-2}, K_{n-1}(R_{n-1}, K_n(R_n, A_x))) \dots), K_x(R_0, M) \rightarrow}$$

and the final result for the remaining n – 1 mixes is:

$$\mathbf{A_x, R_{n-1}, R_{n-1} \dots R_2(R_1(K_x(R_0, M))) \dots)}$$

This technique of untraceable return addresses was first used as a possibility to obtain a *certified mail* communication [15]. Nevertheless, this system can be also implemented to obtain other types of secure communications, not only in the certified mail domain. These Chaum's ideas are used in this thesis to build anonymous telecommunications.

All that notation and explanation can be summarized with the following: In "*normal*" communications, the sender would send the message to the recipient directly. However, in mix networks, the sender sends the message to a **mix**. The mix collects ***n*** messages together and after it encrypts and decrypts them following the showed procedure above and forward them in random order. By sending the message in random order the mix is hiding from the attacker or adversary the direct connection between the sender and the receptor.

2.6 SYNCHRONOUS BATCHING

At the cascade networks mentioned a ***synchronous batching*** is widely used. In a synchronous batching network, each *batch* of messages enters are either send to the next hop or received by the network together in the same lot. In other words, a group of messages is either forwarded or received together at a certain time. This group of message gathered together is what it is defined as a ***batch***. Depending on the batching strategy used by the mix, the messages will stay inside the mix a different period $\boldsymbol{t}$ of time [39]. (*See Section 3.2. for more information regarding this.*)

When a network uses synchronous batching it has a fixed **batch period** $\boldsymbol{t_{batch}}$ [39] which pays reference to the maximum expected latency time of the system generated by different factors such as the threshold number (quantity of messages that must be inside the mix before forwarding all the messages inside the mix to the next hop), pool mix number (minimum amount of message that must be at all times inside the mix before forwarding the other messages to the next destination) and so on.

The messages incoming the network in each batch period are queued till the beginning of the next period before they can be forward it again. When $\boldsymbol{t_{batch}}$ has expired the messages can be sent through the network synchronously to the next hop. In cascade networks, all routes have a fixed length of $\boldsymbol{l}$ hops and the messages are sent at a rate of *one hop per hop period* t_{hop} [39].

A commonly used measure in mix networks is the **width** $\boldsymbol{w}$. Under a synchronous batching environment, the width is defined as the "*numbers of nodes that simultaneously process messages from a given batch in each hop period*" [39]. In the case of cascades, $\boldsymbol{w = 1}$. This is like that because the messages will be processed at the same time at all the mixes. Depending on the type of mix the network is using, for instance threshold mix or pool mix the moment of batching will be different; in a threshold mix the messages will be process at the same time in different mixes when a certain number of incoming messages is reached and in a pool mix, the messages will be processed once the mix has a specific number of messages inside the mix. (*In Section 3.2. it will be discussed this topic in more details*)

The latency of this networks must be always between $\boldsymbol{l \cdot t_{hop}}$ and $\boldsymbol{t_{batch} + l \cdot t_{hop}}$, because $\boldsymbol{l \cdot t_{hop}}$ refers to the minimum time a message would take from the sender to the recipient (we multiply the total number of $\boldsymbol{l}$ hops by the time the message expends in every mix, t_{hop}) and $\boldsymbol{t_{batch} + l \cdot t_{hop}}$ refers to the maximum time of the communication from sender to recipient (we add the minimum time $l \cdot t_{hop}$ required to have a successful communication and the maximum latency time expected $\boldsymbol{t_{batch}}$).

2.7 HOW TO MEASURE ANONYMITY?

In agreement with previous definitions already mentioned in this thesis, in a network with $\boldsymbol{N}$ users, the maximum level of anonymity can be obtained when all the users have equal probabilities of being the sender of a message to the attacker's eyes. Therefore, the degree of anonymity will depend on the even distribution of probabilities, in contrast to order measures explained in Section 1.3, for instance, the anonymity set. Nonetheless, the anonymity set will be used to calculate the user's distribution of probabilities, due to the fact that **the addition of all the user's probabilities must equal 1**. In other words, the probabilities given by the attacker to the users, after obtaining information by observing the network in its optimal situation (none of the network users are compromised), will be $\boldsymbol{1/N}$.

In order to make calculations working with probabilities distributions, the concept of *entropy* in Information Theory (Section 1.4) provides an accurate measure for the degree of anonymity [40]. Entropy is used as a tool to calculate this degree of user anonymity in this mix network [27]. It is important to remember that a high entropy value implies that the network provides a high level of anonymity [33].

The **Hartley function** [41] is a measure of **uncertainty**, introduced by Ralph Hartley in 1928. It is denoted as $\boldsymbol{H_M}$ the maximum entropy of the network we are interested in measuring, being $\boldsymbol{N}$ the size of the anonymity set.

$$\boldsymbol{H_M = log_b|N|}$$

Equation 1. Maximun level of Entropy

If the base of the logarithm is 2, then the unit of uncertainty is defined as the ***shannon*** (Sh) or more commonly known as the *bit* (base 2). If the natural logarithm is used, then the unit is called the ***nat*** (base e). Hartley tended to use a base 10 logarithm, so the unit of information with this base is called the ***hartley*** (hart)in his honor.

Given the discrete random variable ***X*** with possible outcomes $\mathbf{x_i}$ (meaning that ***X = i***), each with probability $\mathbf{P_X(x_i)} = \boldsymbol{p_i}$. In this case, each ***i*** corresponds to an element of the anonymity set (an honest sender). The Shannon-Entropy of **X**, denoted as **H(X)**, calculates the entropy of the system after the attack has taken place [31] [27]:

$$\boldsymbol{H(X) = -\sum_i P_X(x_i) log_b P_X(x_i) = -\sum_i p_i log_b p_i = \sum_i p_i I_X(x_i) = E[I_X]}$$

$$\boldsymbol{H(X) = -\sum_i p_i log_b p_i}$$

Equation 2. *Entropy*

Where $\boldsymbol{I_X(x_i)}$ is the ***self-information*** [9] associated with a particular outcome $\mathbf{x_i}$; $\boldsymbol{I_X}$ is the self-information of the random variable in general. The self-information of an event X is defined as $\boldsymbol{I_X = -log_b P_X(x_i)}$ [31]. ***H(X)*** is also called the ***effective anonymity set size*** because it takes into account the number of users (or IOI) and the probabilities assigned to them [38]. (*See Section 3 for more information regarding this.*)

The base of the logarithm, ***b***, is a new parameter that can be set different ways to determine the choice of units for information entropy. Working with anonymity measures ***b*** will be always equal to 2 because only 2 bits of entropy are only needed: anonymous or not anonymous.

The information that the adversary has learned after the attack can be denoted as $\boldsymbol{H_M - H(x)}$ [Maximum entropy of the system – Entropy after an attack = Adversary knowledge]. Then the ***degree of anonymity d*** provided by the network is [27]:

[9] Self-information or Shannon information is a basic quantity derived from the probability of a particular event occurring from a random variable. It can be thought of as an alternative way of expressing probability: can be interpreted as quantifying the level of "surprise" of a particular outcome.

$$When\ N > 1: \boldsymbol{d} = \frac{\boldsymbol{H_M} - \ \boldsymbol{H(X)}}{\boldsymbol{H_M}} = \frac{\boldsymbol{H(X)}}{\boldsymbol{H_M}}$$

$$\boldsymbol{d} = \frac{\boldsymbol{H(X)}}{\boldsymbol{H_M}}$$

Equation 3. *Degree of Anonymity*

$When\ N = 1: \boldsymbol{d} = \boldsymbol{0}$ because the probability of that 1 user being the sender is 1, no anonymity is provided.

The formula is divided by H_M in order to normalize the value.

The maximum degree of anonymity ***d* = *1*** is obtained when all the users have the same probability of being the sender of the message $\boldsymbol{P_X(x_i) = p_i = \frac{1}{N}}$. By saying this, we are using the ***beyond suspicious*** property introduced in [29] that refers to the fact that the destination with which the user is communicating should not appear significantly more likely than any other possible destination.

Note: The anonymity degree evaluates the level anonymity provided by a system not taking into account the total number of network users. Its goal is to provide an approximation on how close the anonymity of the network users is to the maximum anonymity degree achievable [38]. The *degree of anonymity* and *effective anonymity set size* must not be confused. The difference relays on the fact that the **effective anonymity set size** focusses on the anonymity using as a main source of data the specific number of network users, while the **degree of anonymity** is independent on the number of users and it is mainly focused on the performance of the system [38].

However, Entropy does not always capture the right anonymity property in all the scenarios. Shmatikov and Wang invite us to consider, for example, a distribution of 100 potential destinations, in which all but one are equally likely with probability 0.009, and a single destination has probability 0.109. In this case, the *beyond suspicion property* is destroyed because one destination is 100 times likelier than any other.

For instance, following Figure *7* schema, different subjects may appear as having a higher or lower probability p_i of being the senders or IOI (Item Of Interest) to the eyes of the adversary. These probabilities depend on the information obtained by the adversary in the attack.

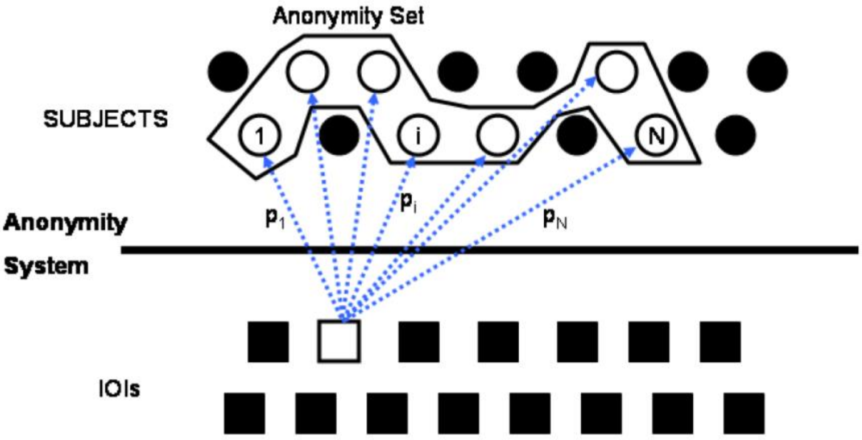


Figure 7. *Anonymity set.*
Different probabilities in the same anonymity set. *[38]*

Nevertheless, some conclusions of the investigation done by Shmatikov and Wang may be relevant for my research (proof can be obtained at [33] if needed):

- **Anonymity decreases with free route selection[10]:** For instance, when 50 routes of 5 nodes each are selected randomly from 50 mixes, the routes have relatively few “synchronized” intersections, resulting in very poor mixing.

- **Anonymity decreases with skewed destination distribution:** If most users are communicating with a relatively small subset of destinations, then it is easier for the attacker to infer whom a certain user is communicating. In other words, with highly skewed distributions, even a perfect mix network provides poor relationship anonymity.

Those two conclusions are worth keeping in mind at my research as 2 other factors that affect the degree of anonymity of the network users.

[10] A free-route network, is defined as the network where the destination of each hop is selected randomly from all mixes in the system. [33]

2.8 RELATED WORK

At this Related Work, it will be highlighted the main works done by other authors that could have a relation with my own work. A small summary of the previous authors work will be added, together with an explanation relaying on why and how my work differs from them.

This section is divided in four areas of research:

- Anonymity Solutions for Blockchain
- Onion Routing
- Developments for mix networks

2.8.1 ANONYMITY SOLUTIONS FOR BLOCKCHAIN

DANDELION:

Bitcoin and Anonymity. Venkatakrishnan, Fanti and Viswanath studied the user anonymity provided in Bitcoin. Although Bitcoin does not claim to provide a high degree of anonymity, the general public associates wrongly anonymity with blockchain [1]. The authors explain a simple networking solution that will provide "*quasi-optimal network-wide anonymity with minimal cost to the network's utility*". This solution is called **Dandelion** [1]. The main goal of Dandelion is to provide network-wide anonymity to all nodes involved, but without requiring human users to change their behavior. However, my thesis aims to provide network-wide anonymity being the main focus placed at the **user's behavior, not on external attackers,** meaning that the users would need to change their behavior. The actions of the user will be a study in detail and the change of the anonymity level will be measure according to user de-anonymizing themselves. Meaning that some guidelines and recommendations about how users should act will be included.

DANDELION++:

The original proposal of Dandelion was discovered to contain various faults and errors that could lead to users' de-anonymization over time due to some utopic and idealistic assumptions of potential attackers. An improved version of the original Dandelion Protocol was proposed in June 2018: **Dandelion++** [42]. This updated version of Dandelion++ provides a good solution regarding the anonymity level of users in Bitcoin. Nevertheless, the main approach of my thesis is the anonymity level in mixing networks. The main difference between the Dandelion++ protocol and mix networks is the following: Dandelion++ base its anonymity on the message being forwarded to a single random user based on an algorithm. Then, that user forwards the message to another single user, and the process continues until eventually (and randomly) one of the users broadcasts the message in the typical way of diffusion to the rest of the network [43]. In contrast, mix networks hide information about the senders and recipients following the public key protocol mentioned in Section 1.2. The Dandelion++ findings could help me as a general goal-oriented overview, but another approach must be followed to obtain precise and concise results in the measure of anonymity for users in mix networks.

2.8.2 ONION ROUTING FOR MIX NETWORKS

ONION ROUTING:

Onion Routing [23] is a technique for anonymous communication over a computer public network. In an onion network, the information or messages send are encapsulated in layers of encryption, similar to layers of an onion. The communication process of the encrypted message takes place through a series of network nodes called *onion routers*, each of them de-encrypts a single layer, revealing the message next destination. When the final layer is uncovered, the message arrives at its destination or desired recipient. The sender of the message remains completely anonymous during the entire communication because each node only knows the location of the directly previous and following nodes [23]. The network formed but these several onion router is named TOR (by its English acronym "*The Onion Router*"). Onion Routing gets its security from the assumption that it is difficult for an adversary to have access to all the intermediate nodes that are necessary to know the final destination. At the unlikely scenario that an adversary has access to all the nodes, Onion Routing loses its entirely security and anonymity.

In this thesis, mix networks will be used. This type of network is an improvement of the Onion Routing that overcome the problem of the adversary that had access to all the nodes. The mix-net is specifically designed to provide security even if an adversary can see the entire path. In order to accomplish this, the mix-net distributes the messages to nodes called *mix* that holds all the messages that are sent there and forward them following specific a specific order depending on the batching strategy used. Although everyone could see all the messages that were sent to the mix, it is not possible to determine which one will be forwarded to the next hop. The mix-net creates and provides uncertainty for the adversary that they are not able to overcome.

2.8.3 DEVELOPMENT FOR MIX NETWORKS

MIXMINION:

Mixminion [44] is an anonymous protocol based in message communication that does not distinguish forwarded messages from returned answered messages. This provides the users with higher anonymity due to the fact that messages sent and answered share the same anonymity set, ergo the anonymity set will be larger than usual. This protocol is widely used to send and receive anonymous e-mails.

Mixminion uses an *asynchronous communication* protocol, meaning that messages can be input and output of the network at any time and in order to forward them, the mix can do so without waiting for the latency period mentioned in Section 2.6. This characteristic does not go into alliance with the synchronous batching that I am proposing in this thesis with the use of cascades to provide anonymity to the system. Besides, this mix type uses *free routes* and this thesis will base its research in cascades network where the hops are known and fixed. Those are the two attributes, asynchronous communication and the use of free routes, that make the ideas of my thesis different from the ones proposed in this paper.

LOOPIX:

The Loopix Anonymity System [45]**.** One of the well-known problems of mixing networks is their high latency period, meaning that the waiting time or delay of sending messages cannot accommodate real-time communications. Loopix appeared as a solution to this problem presenting a low-latency anonymous communication system that provides bidirectional "*third-party*" anonymity and unobservability, in other words, hides the sender-receiver communication from third parties.

The success of this paper, according to their author, relays on the mixes arranged in a ***stratified topology*** [39], where the mixes are arranged in different layers where each layer ***l*** is connected to every mix in layer *l+1* y *l-1*, and to the ***Poisson mixing****,* a term used by the authors for the simplification of the Stop-ang-go mix strategy defined in [46]. These two strategies seem to be effective and provide good results in the anonymity levels studied for 4 possible thread models: global passive adversary (GPA), corrupt mixes, corrupt providers of the network and insiders. It is the last that I am interested in; when the adversary has the ability to participate in the Loopix system as a compromised user who can bias the protocol. Remember that my thesis goal is to measure the anonymity when users purposefully or inadvertently make mistakes, this approach would serve as a prior study regarding users committing faults on purpose.

The worst results obtained in the Loopix system analysis of unobservability and unlinkability was obtained with the scenario of the *insider threat* [45], not an external passive adversary but a corrupted user. Therefore, a more extensive study on how to improve these results using mix networks is needed. Thus, this thesis will focus on that insider threat, users doing mistakes purposefully or inadvertently.

Chapter 3. DESCRIPTION OF THE DEVELOPED MODEL

3.1. OBJECTIVES AND SPECIFICATION

The specific question that will be addressed in this thesis is: **How does the external de-anonymization affect the users' anonymity guarantee of mix networks?** The external de-anonymization refers to possible mistakes that network users may do purposefully or inadvertently that could result in compromising the total anonymity of the mix network.

The objective of the thesis is to measure the degree of anonymity in a mix network after users de-anonymizes themselves doing mistakes at the network.

In order to start with the simulation and models some assumptions are needed to be mentioned:

> ***Assumption 1:*** We consider every user equally likely to send the message and to receive one.
>
> ***Assumption 2:*** Every sender sends one message at a time, and every recipient receives one message at a time.
>
> ***Assumption 3:*** This assumption is a consequence of the assumption 2. Every message input to the mix originates from different users.
>
> ***Assumption 4:*** We have the ability of distinguishing between different senders in the mix network. Meaning that even though we want to provide a good degree of anonymity, in order to calculate and model different scenarios, it is necessary to be able of differentiating all senders.
>
> ***Assumption 5:*** The behavior of the users in the network is unique, meaning that there are not messages with the same content nor with the same recipient.

Assumption 6: The historical data is not being taken into account, meaning that we have no data regarding the messages that a sender sent, or a recipient received before.

Assumption 7: The mixes have a significant delay due to the large amount of message to mix and their internal frequency of received messages (threshold, pool mix and so on). That is why it will be assumed that this delay is not a problem because the mix network will be used for activities when a postponement of a few minutes is not an obstacle, unlike web-browsing where a few seconds delay could generate unhappiness with the network.

Assumption 8: The de-anonymization can only occur outside the mix. In other words, we trust that the mixes process are 100% reliable and they will not make any computer mistake that could result in the sender or recipient being de-anonymized.

3.1.1. SIMPLE EXAMPLE BASED ON CHAUM MIX NETWORK

Figure *8* represents 10 potential senders of one message, one mix network and a recipient. In this example, the degree of sender anonymity will be measured, since there is only one recipient. The adversary wants to discover which of the senders sent the message. The procedure of any attack starts with the adversary assigning a specific probability to each sender user.

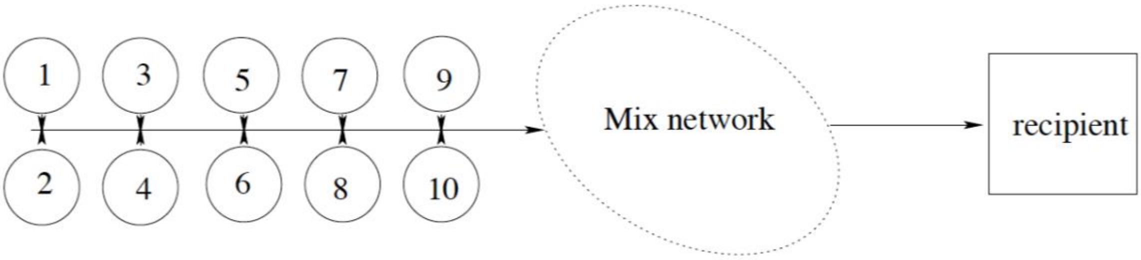


Figure 8. *Example Chaum.*
Simple mix network based on Chaum's email system *[27]*

Two attacks are considered and explained:

Active attack: Let's consider an active internal adversary that is able to control 8 of the senders. Since these 8 senders are compromised, they must be excluded from the anonymity set, meaning that the anonymity set size N is 2 honest users (10 total user – 8 compromised users). The adversary now assigns the probability to the 2 remaining honest users: *user1* and *user2*. The distribution of probabilities is:

$$p_1 = p \qquad p_2 = 1 - p$$

Since we are certain that one of those two users sent the message, the adversary assigns a probability ***p*** to *user1*, ergo the probability to *user2* must be ***1 – p***. If there was only one honest user, user1 would have ***p₁ = 1.***

To make a reference to this thesis topic, this example can be better understood regarding user de-anonymizing themselves with the example of package delivery. Let's suppose that a e-commerce delivery worker enters a building, with only two flats on it, to deliver one package. Looking at the time that the delivery worker spends inside the building, it can be established the 2 probabilities mentioned above $p_1 = p$ and $p_2 = 1 - p$. In that case, we are not looking at a user completely de-anonymizing itself but **partially**.

The ***maximum degree of anonymity*** (d = 1), will be obtained when both remaining honest users are equiprobable $\left(\boldsymbol{p} = \frac{1}{2}.\right)$ In this scenario, the adversary has not gained any information about which of the two honest users is the real sender of the message by analyzing the traffic in the mix network. The ***minimum degree of anonymity*** (d = 0) is reached when the attacker can assign probability one to one of the remaining users, for example: $\boldsymbol{p_1 = 1}$ and $\boldsymbol{p_2 = 0}$ [27].

Using the concept of Entropy $\boldsymbol{H(X)}$ and the Equation *2*, the entropy of this example is:

$$H(X) = -\sum_i p_i log_b\, p_i = -(p\ log_2 p + (1-p)\, log_2(1-p))$$

In order to calculate the degree of anonymity ***d***, it is necessary to know the maximum entropy $\boldsymbol{H_M}$ for these 2 honest users (

Equation 1).

$$H_M = log_b|N| = log_2 2 = 1$$

Now it is possible to calculate the degree of anonymity (Equation *3*)

$$d = \frac{H(X)}{H_M} = \frac{-(p\ log_2 p + (1-p)\, log_2(1-p))}{1}$$

Being $d = -(p\ log_2 p + (1-p)\, log_2(1-p))$ it is possible to create a model that relates $\boldsymbol{d}$ and $\boldsymbol{p}$. In the Figure *9*, you can see the changes of the degree of anonymity regarding the probability assigned by the attacker to each user. (Code detailed in APPENDIX I)

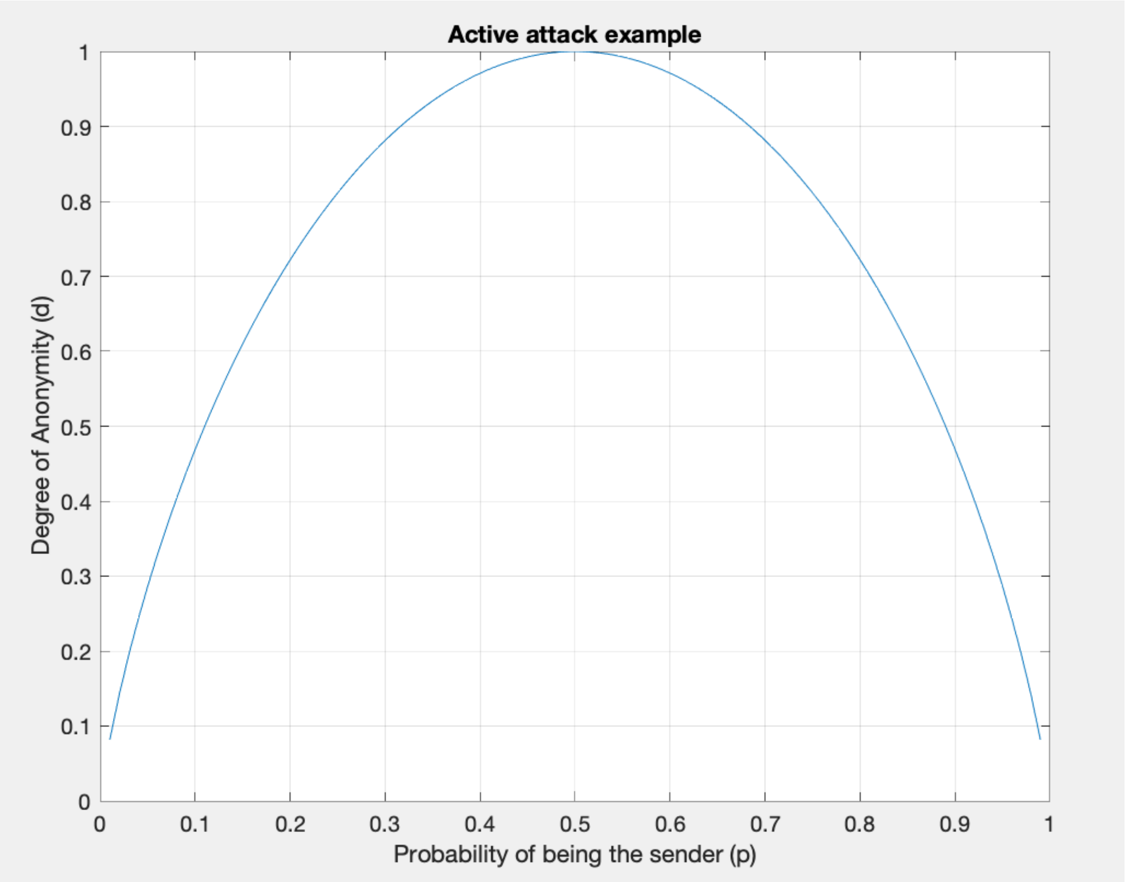


Figure 9. Active Attack Example
Simple active attack example modelled with Matlab

It is observed that all the example guesses mentioned above are correct: the maximum degree of anonymity is in $\left(\frac{1}{2}, 1\right)$ and the minimum degree of anonymity is found when the attack can assign to one of the users a $p = 1$.

With this simple example, I can introduce the concept of **reference value**. The reference value is the minimum degree of anonymity that is still adequate and that provides a *decent* level of security to the users [27]. This reference value must be determined within the network once it is first created by its developers.

Since it was explained in [24, using a reference value of 0.8 it is good enough in order to provide a decent level or anonymity. Meaning that if the network provides a degree of anonymity equal or above 0.8 ($d \geq 0.8$), it will be considered *"good enough".* So, in the example above mentioned, this reference value corresponds to the attacker assigning $p \approx 0.25$ to one user and $p \approx 0.75$ to the other user. (Those numbers are obtained looking at Figure 9). Meaning that the system will provide a *decent* degree of anonymity in every scenario where the attacker assigns probability p_i to both users between [0.25, 0.75]. If, for instance, the attacker manages to assign a $p_1 = 0.1$ and $p_2 = 0.9$, the system is not providing a good and/or enough degree of anonymity.

Passive attack: Let's consider now a passive global external adversary who has no control over the network but that is able to analyze the traffic in the whole system. Since none of the users are compromised, the anonymity set size N = 10.

The passive adversary comes up with the following distributions of probability:

$$\boldsymbol{p_i = \frac{p}{4}, \quad 1 \leq i \leq 4 \qquad\qquad p_i = \frac{1-p}{6}, \quad 5 \leq i \leq 10}$$

Equation 4. *Passive attack example.*

In this scenario we have 2 groups of users. The first group with 4 users and the second group with 6 users.

Continuing with the delivery package example, in this scenario we now see the e-commerce delivery worker entering a building with 2 floors. The first floor has 4 flats and the second floor has 6 flats. Looking at the time that the delivery worker spends inside the building, it can be established the 2 groups of probabilities mentioned above. Again, we are not looking at a user completely de-anonymizing itself but **partially**.

The maximum degree of anonymity (d = 1) can be obtained in the equiprobable distribution:

$$\boldsymbol{\frac{p}{4} = \frac{1-p}{6} \rightarrow 6p = 4 - 4p \rightarrow 10p = 4 \rightarrow p = \frac{2}{5} \rightarrow p = 0.4}$$

Obtaining d = 0 with each scenario it is not possible because in the worst case, the adversary is able to see 4 users (the group with the least number of users) with probability $\boldsymbol{\frac{1}{4}}$. In other words, the adversary cannot identify a single user as sender of the message [27].

Following the steps detailed in the previous example and

Equation 1, Equation *2* and Equation *3*:

$$H(X) = -\sum_{i} p_i log_b\, p_i = -\left(4\left(\frac{p}{4}\, log_2 \frac{p}{4}\right) + \left(6\, \frac{1-p}{6}\, log_2 \frac{1-p}{6}\right)\right)$$

$$H_M = log_b|N| = log_2 10 \approx 3.322$$

$$d = \frac{H(X)}{H_M} = \frac{-\left(4\left(\frac{p}{4}\, log_2 \frac{p}{4}\right) + \left(6\, \frac{1-p}{6}\, log_2 \frac{1-p}{6}\right)\right)}{log_2 10}$$

Being $d = \frac{-\left(4\left(\frac{p}{4}\, log_2 \frac{p}{4}\right) + \left(6\, \frac{1-p}{6}\, log_2 \frac{1-p}{6}\right)\right)}{log_2 10}$ I can create a model that relates $\boldsymbol{d}$ and $\boldsymbol{p}$ as it was done in the previous example. In the Figure *10*, it is possible to see the changes of the degree of anonymity regarding the probability assigned by the attacker to each user. (Code detailed in APPENDIX II).

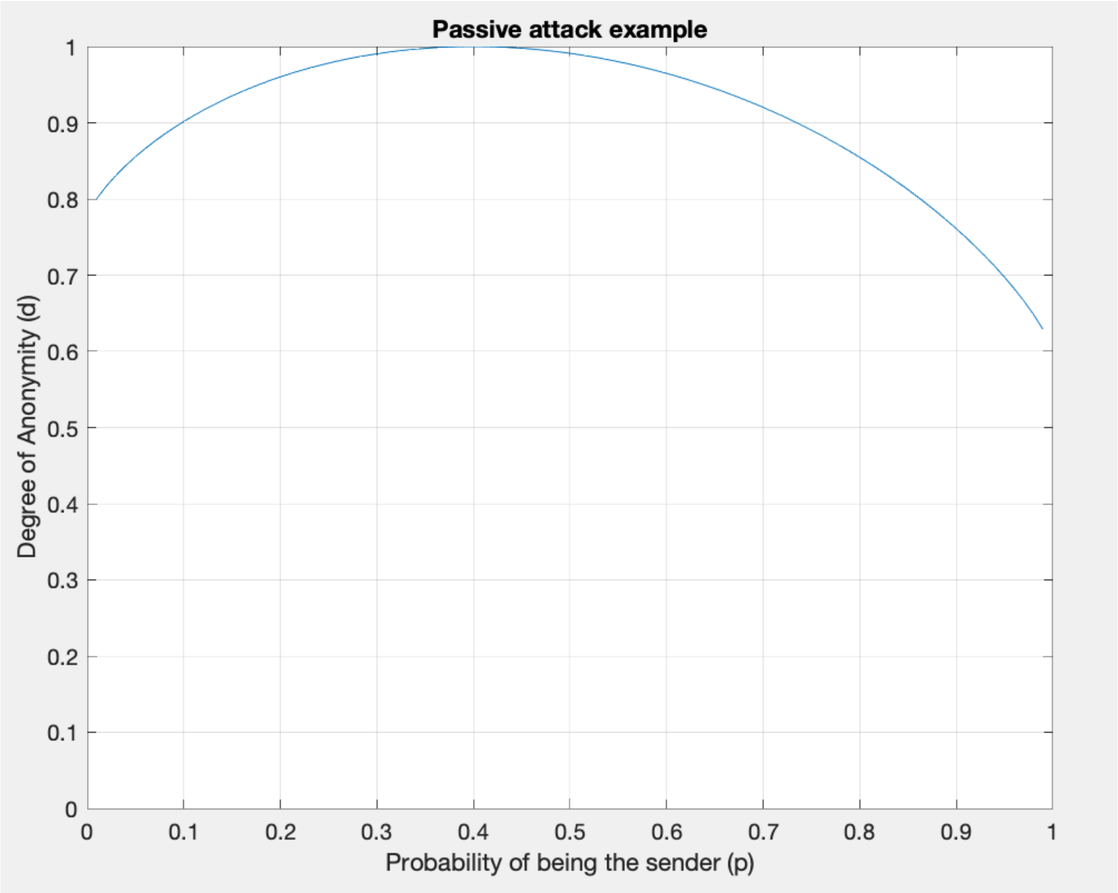


Figure 10. Passive Attack Example
Simple passive attack example modelled with Matlab

Looking at the reference value of 0.8 at the Figure *10* we able to determine that $d \approx 0.8$ can be obtained in $p \approx 0.85$ (That number is obtained looking at Figure *11*).

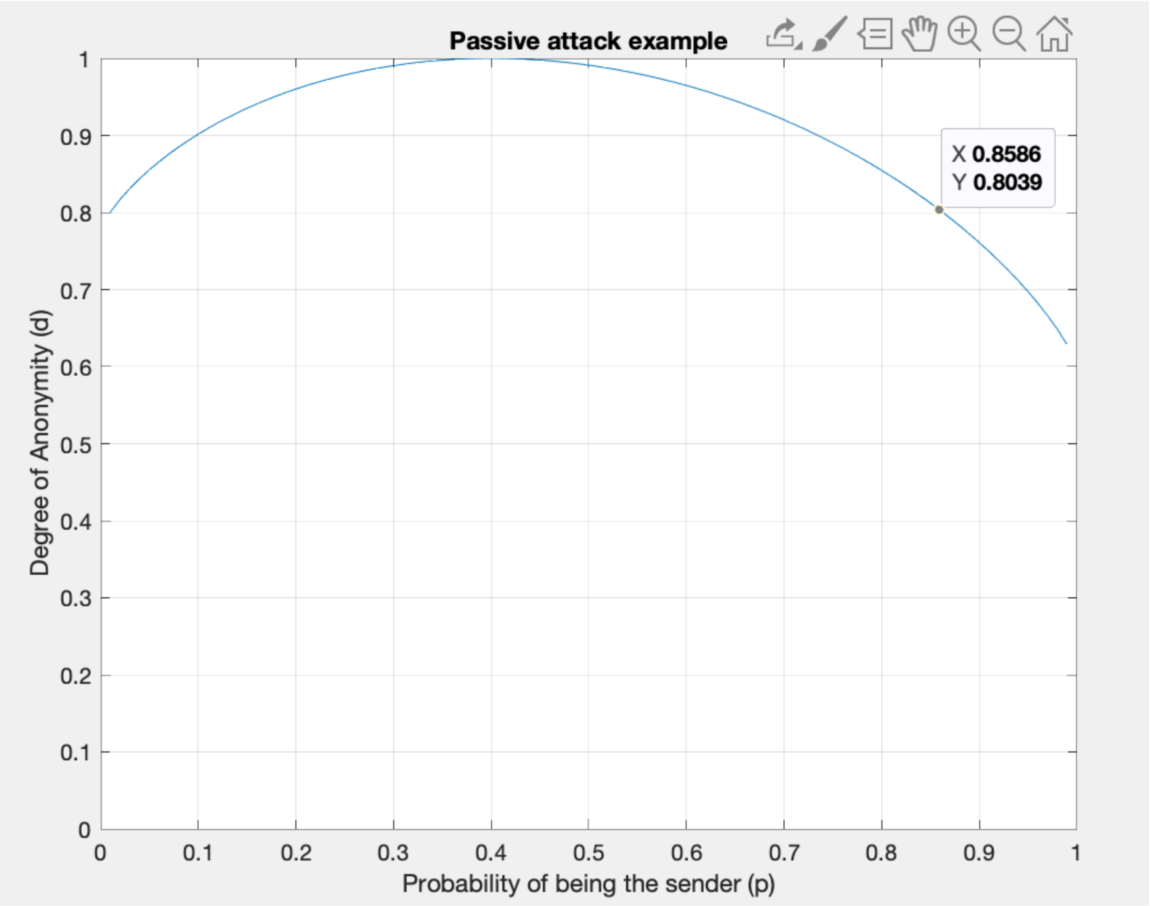


Figure 11. *Value of p with d = 0.8*

Being $p \approx 0.85$, and going back to Equation 4, we can determine that this value is reached when the group of 4 users are assigned the probability $p_i = \frac{\mathbf{0.85}}{\mathbf{4}} = 0.2125$ and when the other 6 users are assigned the probability $p_i = \frac{\mathbf{1- 0.85}}{\mathbf{6}} = 0.025$.

Meaning that the system will provide a *decent* degree of anonymity in every scenario where the attacker assigns probability p_i to the users of the first group between [0, 0.2125] and to the other 6 remaining users between [0, 0.025].

3.2. DATA USED: MIXING STRATEGIES CONSIDERED

Before starting with the models, it is necessary to choose the type of mix that will be used to develop this thesis. The majority of modern anonymity systems are based on the threshold mix introduced by Chaum in 1981 [16]. However, new mixes have been framed after Chaum's paper such as Mixmaster [47], Mixminion [48], Babel [49], Real-Time Mixes [50], Flash Mixing [51], the Stop-and-go-MIXes [46] and the Binomial Mix [16].

They one of the key parameter than distinguish one mix from the other is the ***batching strategy*** [52] [16]. The batching strategy is defined as the algorithm that determines how the message will be mixed inside the mix, and when they will be forwarded to the next hop. This *waiting time* results in a few minutes delay but as it was mentioned at assumption 4, that it is not a problem.

3.2.1. COMPARISON OF BATCHING STRATEGIES BETWEEN MIXES

Let's examine the different types of mixes now. Besides the mixes announce above, there are more variety of mixes that it must be taken into account. In 2002, Serjantov, Dingledine and Syverson pursued a survey where they asked the general mix network user, which kind of mixes were they familiar with [53]. The answer was threshold mix, timed mix, timed pool mix, the timed dynamic pool mix (also called Cottrell mix) and threshold pool mix. As a result of this survey, I will present the main characteristics of these mixes together with a glossary (See Table 1):

N	**Number of messages that the mix receives**
N	Number of messages inside the mix at the time of flushing
n_t	Threshold. Number of messages needed to be received by the mix in order to send *n* messages to the next hop
T	Time period of the mix which specify how often we flush the mix. When the timer is out, the mix can forward *n* messages to the next hop
N_P	Pool of messages. Number of messages needed to be inside the mix at every time
F	Number of output messages for the Cottrell mix. Is a fraction of the difference between n and n_p

Table 1. *Glossary for the mixes types*.

Now, it will we describe the different algorithms of the most used mixes according to Serjantov, Dingledine and Syverson survey. Table 2 show us the 5 types of mixes already mentioned: threshold mix, timed mix, timed pool mix, the timed dynamic pool mix and threshold pool mix, together with the mix parameters that determine the network. The algorithm implemented by every mix is also detailed alongside with the function ***P(n)*** that models the fraction of messages that will be forwarded out of the mix.

MIX TYPE	MIX PARAMETERS	DESCRIPTION / ALGORITHM	FLUSHED MESSAGES FUNCTION
Simple proxy	none	No batching, nor reordering. A Simple proxy is not a mix network	-
Timed mix	*t*	If timer *t* times out, send all *n* messages	This mix forwards to the next hop all the messages at time of flushing, meaning that 100% of the messages will be flushed. $\boldsymbol{P(n) = 1}$
Timed pool mix	*t*, n_p	If timer *t* times out and the mix has received N messages after it flushed out last time, then n_p *randomly* picked messages from n (n = $N + n_p$) are kept inside the mix and the rest are forwarded.	Since n_p messages are always inside the mix (pool), the mix forwards n – n_p messages. The percentage of messages sent can be expressed as $\boldsymbol{P(n) = 1 - \frac{n_p}{n}}$
Timed dynamic pool mix	*t*, *f*, n_p	If timer *t* times out and n > n_p, send $f \cdot (n - n_p)$ messages. Otherwise, the mix will not forward anything till that condition becomes true.	In this case, the percentage of messages sent can be expressed as $\boldsymbol{P(n) = f \cdot \left(1 - \frac{n_p}{n}\right)}$
Threshold mix	N_T	If $n = N_T$, send *n* messages	Since this mix does not depend on the time period, but only on achieving a specific number of messages inside the mix, if we set t = 0, the function will be $\boldsymbol{P(n) = 0}$ everywhere except for the N_T point where the mix will forward all the messages. Meaning that this mix are represented by a single point at **(N_T, 1)**

Table 2. *Comparing Batching Strategies for mixes*.

The comparison can be observed at Figure *12*. (code detailed in APPENDIX III)

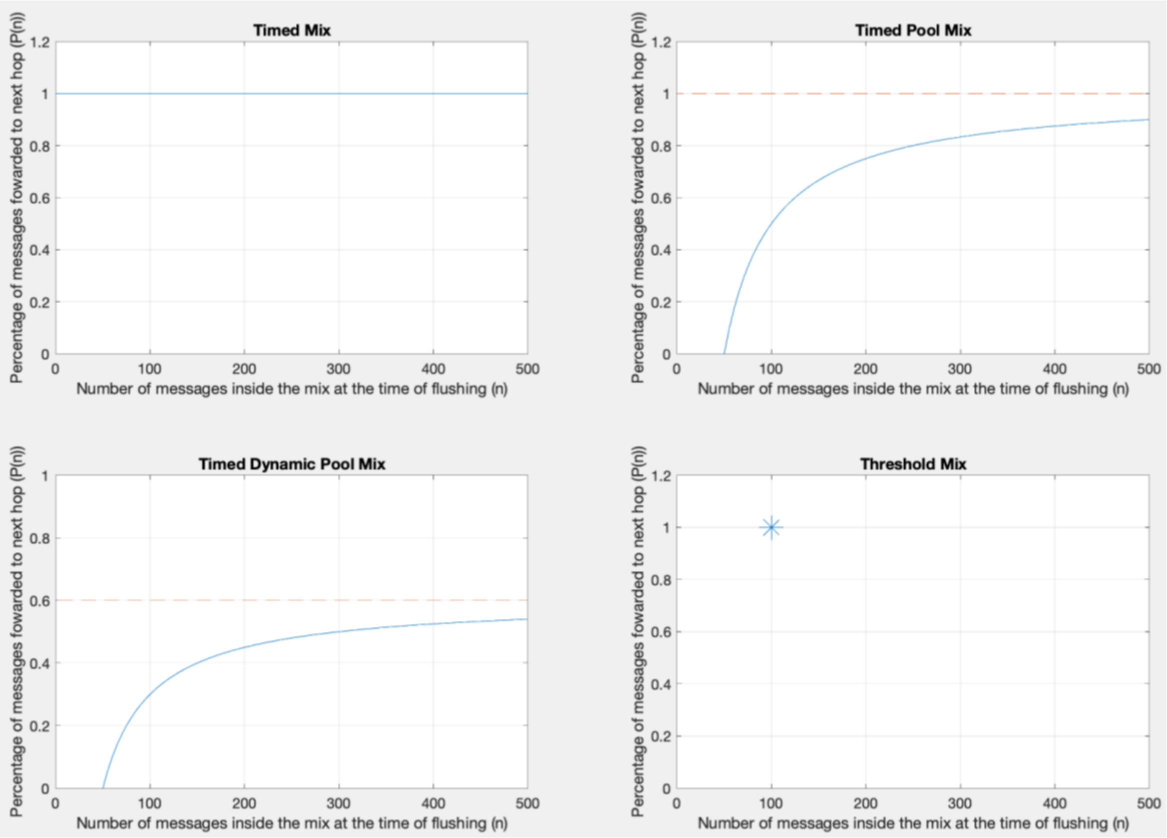


Figure 12. *Comparison of batching strategies between mixes*.
Representing the most used and know mixes as functions of the percentage from the number of messages inside the mix to the fraction of messages forwarded to the next hop at the time of flushing.

Seeing the results obtained, I decide to continue my thesis using the concept of ***threshold mix*** due to the fact that the majority of mix networks use this kind of mix and I can find more literature and research regarding this topic.

3.3. ALGORITHMS, METHOD & MODELS

As we discussed in Chapter 2 of this thesis, the anonymity set is a good measure in order calculate *high level* anonymity in not complex mix networks. Let's take the Figure *13* scenario as an example:

We have a mix network of N users, only one threshold mix with a $\boldsymbol{n_t}$ threshold (there is only one round of flushing in this example). So, if under this N-users-one-threshold-mix network, we suppose that ***k*** users de-anonymize themselves it is easy to deduct that the new anonymity set is ***N-k***.

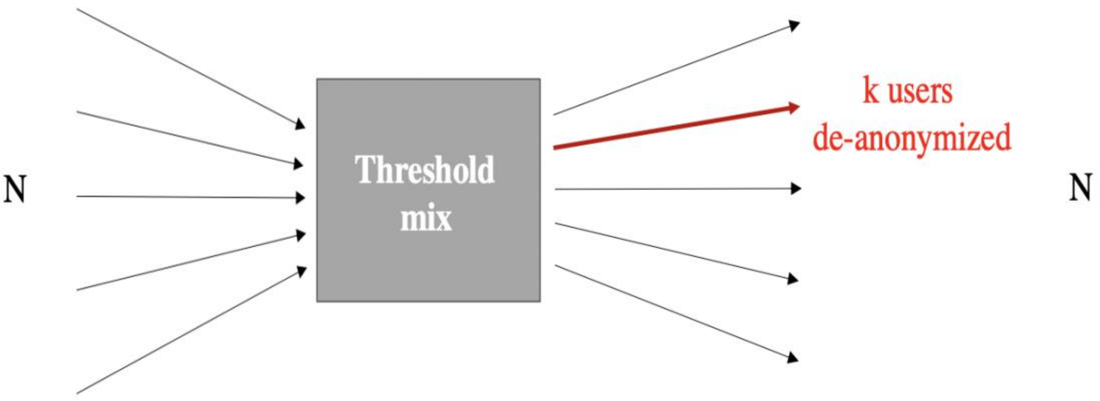


Figure 13. *First Scenario: Threshold Mix with anonymity set.*
Simple example explaining how the anonymity set can be used as an anonymity measure in simple mix networks.

That first scenario is the easiest one and it will not happen in a real network. However, it serves this thesis as a first example.

Now I will describe a second scenario where the use of anonymity set is a not so accurate metric when we have several mixes. Consider the network expressed in Figure *14* where the small grey boxes are the senders {A, B, C, D and E}, the bigger grey boxes are 3 threshold mixes with $\boldsymbol{n_t = 2}$ (not likely to happen in real-life networks but it is enough to prove a valid point in this thesis) and the recipients are the arrow endings {Q, P, R, S and T}.

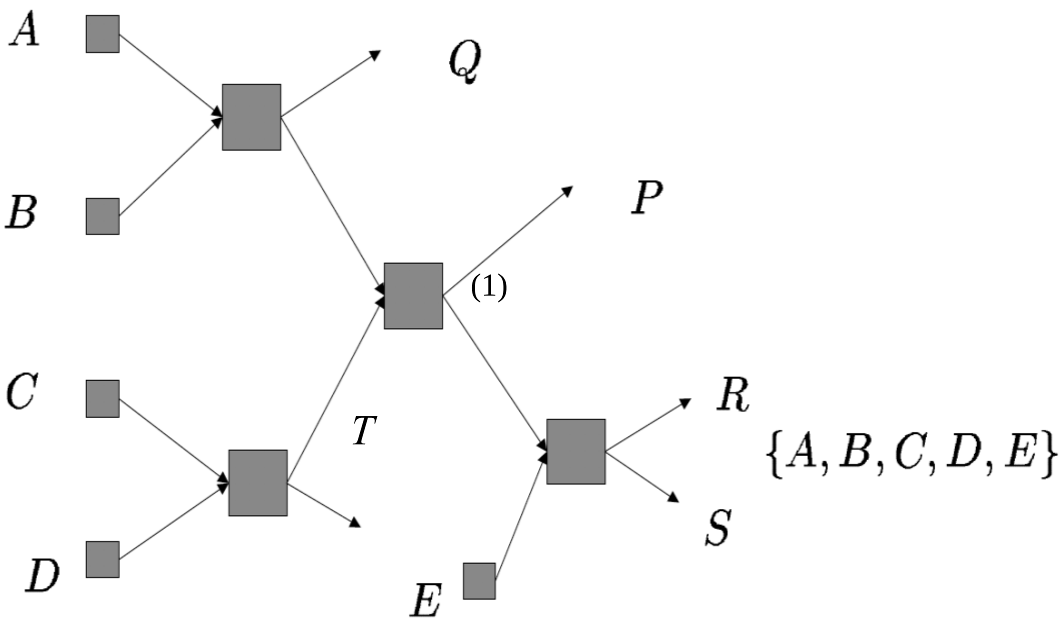


Figure 14. *Second Scenario Threshold Mix with anonymity set.*
Simple example explaining the vulnerability of Anonymity set in mix networks with several mixes [18].

Suppose that sender A makes a mistake, implying its own de-anonymization, ergo the entire network can now have the knowledge of *with who A is communicating to*. Imagine that A was sending a message to R (denoted as A → R). According to the assumption 2 of this thesis, every sender and recipient sends/receives a message at a time, so if A → R we can deduce that E → S. This is known because the arrow noted as (1) can only contain a message from A, B, C or D. In other words, in order to expose the connection between E (sender) and S (recipient) it is enough with one of A, B, C, D de-anonymizing themselves to know that they are communicating with R, for instance. And yet, this de-anonymization it is not reflected in S's sender anonymity set even though it is indeed comprised [18].

With this example, I expose that not all senders are equally vulnerable to de-anonymization and even when de-anonymization happens, the anonymity set stays unchangeable providing not the accurate data of the real state of the mix network. Under most optimal circumstances, the anonymity set of the scenario exposed in Figure *14* is N = 5. If the user A de-anonymize itself the new anonymity set is be N = 4. However, as it was shown in the example, this is not the case due to the fact that if one user de-anonymizes itself, that could generate a total or partial de-anonymization of the system that would result in being the new real anonymity set less than 4. In other words, the **dependencies are not considered**.

In addition, another issue of the anonymity set measure is that it **does not take into account the probabilities** of the users being the real sender of an observed message.

One way of solving this problem is with the use of the ***effective anonymity set size S***, first introduced in [18]. In order to define this new measure, it is necessary to recall the concept of entropy as a tool to calculate this degree of user anonymity in this mix network:

$$\boldsymbol{H(X) = -\sum_{i} p_i log_2\, p_i}$$

Let's remember that the higher the entropy, the greater the disorder. Meaning that with high values of entropy, the mix network will provide a better degree of anonymity. This way of thinking can also be applied to the effective size. The higher the effective size, the better the anonymity because the network has a higher number of possible users that could have done the one mistake that leaded to partial or total de-anonymization. Going back to our delivery package example. Consider a building with only 2 flats where it is clear that neighbor 1 left the building a few minutes ago through the front door (instead of through the garage to keep his information anonymous). A package delivery worker enters the building with a package for either one of those 2 flats, since neighbor 1 is not inside the building it is obvious that the package was to neighbor 2 (assume that the delivery worker only can hand over the package to the person, not leave it in front of its door), ergo its anonymity is compromised. The probability of neighbor 2 being the recipient of the package is $p_2 = 1$ and the entropy is 0.

Consider now a building with 10 flats with the same situation, neighbor 1 is gone. If the delivery worker comes inside the building with a package and gets out of it without the package, the situation it is not so clear. The probability of the neighbors from neighbor 2 to neighbor 10 is $p_{2\to 9} = \frac{1}{9}$ and the entropy is 2.8177. With the same situation and a building with 1000 flats, the $p_{2\to 999} = \frac{1}{999}$ and the entropy is 9.9544. *(The calculations of these entropies can be checked in Appendix IV).* As you could see, the higher the entropy the higher the degree of anonymity.

Given a mix network with *N* users with the assumption that only one user makes a mistake, let *U* be the users' *a-posteriori* probability distribution of users u $(u \in N)$ of being the one doing the mistake that leads to de-anonymization. Let *r* be the anonymity probability distribution of U. In other words, $U(u, r)$ is the matrix $U{:}\, N\ x\ 1$ that shows the probability distribution of possible senders or recipients being the one de-anonymized. The effective size is equal to:

$$\boldsymbol{S = -\sum_{u<N} p_u log_2\, p_u}$$

Equation 5. *Effective Anonymity Set Size*.

This effective size can be interpreted as the number of bits of extra data that must be added to know with total certainty which other user(s) were affected by de-anonymized of ***i*** (the specific user that de-anonymized itself), what was its role (sender or recipient) and the message communicated [18]. It is clear to show that if one user is assigned a probability $\boldsymbol{p_i = 1}$ of being the sender or the recipient of one particular message, then the anonymity effective set size is ***S = 0*** when calculated for that specific message, which means that the network already has enough data to identify which user made the mistake that lead to the de-anonymization of itself. For other messages this might not be true and it is necessary to calculate it for every possible scenario.

Why do we need this new measure in this thesis? As it was explained and proved in the pages above, when an only user does a mistake that leads to its de-anonymization, we may think that the anonymity set changes from *N* to *N – 1*. Nonetheless, in most of the cases that is not true because the network is not only *losing* one user, but also some connections may be revealed as a consequence of that particular user de-anonymization, being the other links exposed, ergo subtracting only that one user out of the anonymity set N seems not precise. If we preform the anonymity calculations with the $N - 1$ measure (only deducting that particular user), the results obtained will appear better than the real anonymity provided because the larger the anonymity set, the higher the chances. (*This topic will be covered in more details in Section 3.3.1*)

In order to achieve a reliable measure, it is important to use the effective anonymity set size ***S***. This value symbolizes the *real* anonymity set that the network will have. It is important to be aware of this difference because the total number of the network users after an event such as de-anonymization may differ from the number of active users in the mix network. Considerations regarding this measure and sum up:

- The effective anonymity set size is computed using log_2 , the mix network has its most optimal anonymity level when **S** = $\boldsymbol{log_2\, N}$. In other words, if the network examined has an anonymity set equal to eight users ($N = 8$), its effective anonymity set size will be 3 ($S = 3$).
- The following statement is always true: $\mathbf{0 \leq S \leq} \boldsymbol{log_2\, N}$, being N the finite set of all users or anonymity set.
- The anonymity set size S is an accurate indicator on of how good the anonymity provided by the network is. In the worst-case scenario, the effective anonymity set size of the network is 0. if $\boldsymbol{S = 0}$, then the communication is providing zero anonymity and it is already known who made the mistake. In the best-case scenario, S will be equal to the base 2 logarithm of the total number of users of the network and that means that any user could have sent the message and that all users have equal probabilities of being the sender of the message compromised.

For this thesis, a new measure called **Anonymity Rate *AR*** will be used to determine the accuracy and to define how optimal a mix network is. The anonymity rate is defined as follows:

$$\boldsymbol{AR} = \frac{\boldsymbol{S}}{\boldsymbol{log_2(N)}}$$

Equation 6. Anonymity Rate.

Where all the values of AR are contained between 0 and 1, $\boldsymbol{0 \leq AR \leq 1}$**.** Where AR = 0 is the least optimal network scenario and AR = 1 is the wished situation, most optimal.

3.4. NUMERICAL IMPLEMENTATION

If the anonymity rate ***AR = 1***, then the network is providing the maximum level of anonymity that it is possible for its own characteristics. Meaning than all the users in the mix network are equally likely to be the author of the jeopardized message. (See Figure *15*)

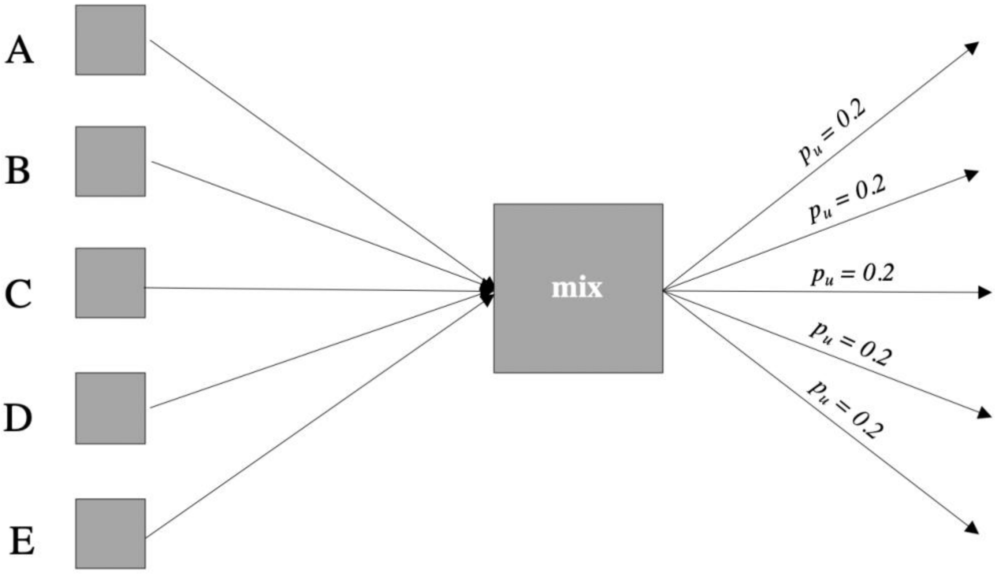


Figure 15. *Anonymity rate example (AR = 1).*

At Figure *15* it is showed the probability of message being originally send by, for example, user *C*. As it can be noted, all the messages are equally likely of being the one sent by the observed sender *C* being $p_u = 0.2$ and $N = 5$, equal to the number of senders. Following Equation *5* we can calculate the effective anonymity set size shown of Figure *15*:

$$S_{Figure15} = -\sum_{u<N} p_u log_2\, p_u$$
$$= -(0.2\, log_2 0.2 + 0.2\, log_2 0.2 + 0.2\, log_2 0.2 + 0.2\, log_2 0.2 + 0.2\, log_2 0.2) = -(0.2\, log_2 0.2\; x\; 5) \approx 2.322$$

Using the measure that I have just introduced, the *anonymity rate*, and operating *Equation* 6, it can be proved that *AR = 1*:

$$AR = \frac{S}{log_2(N)} = \frac{2.322}{log_2(5)} = 1$$

Thus, the anonymity provided in the mix network is positioned at its maximum level. No users made mistakes, no one is de-anonymized, and all the users are equally likely of being the sender of the messages.

However, that is an improbable scenario. There will be always some flaws at the system, for instance an internal attacker or users providing more data than necessary. When a situation like that happens, not all the users are equiprobable of being the sender of the message that originated at *B*, for example. Depending on that amount of data given inadvertently to the network or known information by the adversary, the probabilities $\boldsymbol{p_u}$ (or *a-posteriori* probability distribution of a message being sent by a concrete sender) will no longer be equiprobable and they will have different value that will add to one, $\sum_u p_u = 1$. (See Figure *16*).

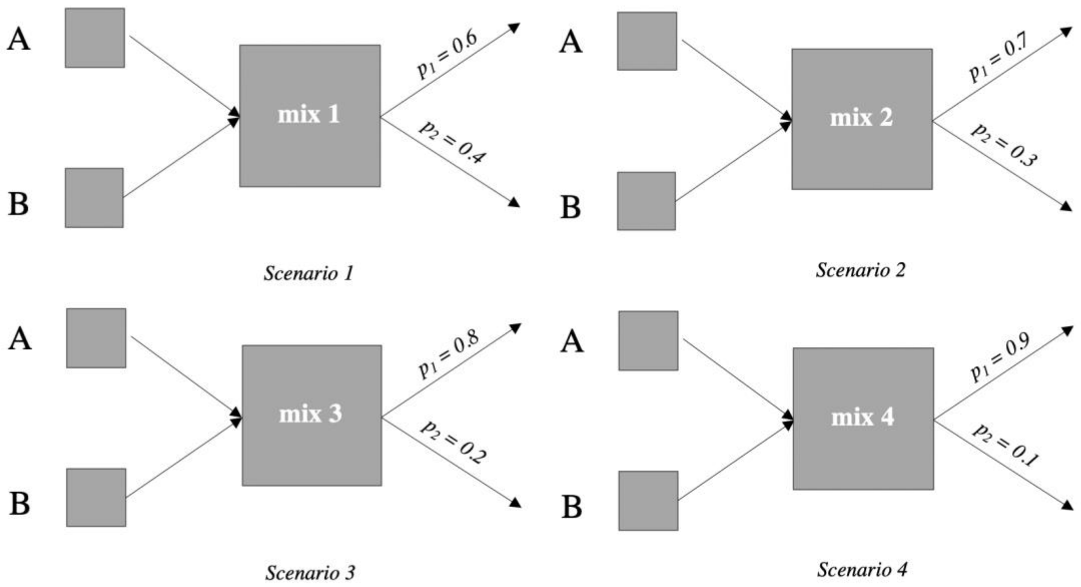


Figure 16. *Anonymity Rate example (AR < 1).*

When the users are not equally likely of being the sends, the effective anonymity set size it is no longer equal to $log_2\, N$, but it will acquire a smaller value. In addition, the bigger the difference between the probabilities p_u, the smaller will be S. Consequently, the parameter AR will be closer to 0 as the difference between p_u increases.

Following the scenarios showed at Figure *16* where the anonymity set is always 2 (*N =2)* and implementing Equation *5* and

Equation 6 it can be proved the statement from above:

- *Scenario 1*:

$$S_{scenario1} = -\sum_{u<N} p_u log_2\, p_u = -(0.6\, log_2 0.6 + \ 0.4\, log_2 0.4) \approx 0.971$$

$$AR_{scenario1} = \frac{0.971}{log_2\, 2} = 0.971$$

- *Scenario 2*:

$$AR_{scenario2} = \ 0.881$$

- *Scenario 3*:

$$AR_{scenario3} = 0.712$$

- *Scenario 4*:

$$AR_{scenario4} = 0.469$$

These four scenarios perfectly reflect what I stated before. The value of the Anonymity Rate will be closer to one (our goal) when the differences between probabilities p_u are considerable small or inexistent. On the other hand, the AR measure will indicate an extremely poor anonymity mix network when the differences between probabilities p_u grow.

Figure *17* shows this anonymity rate changes mentioned, where the most optimal point is located in (0.5, 1). In that point both senders are equally likely of being the send of the observed message. At the figure, the anonymity rate is calculated subsequently by *Equation 6* using $N = 2$ and S is calculated following Equation 5 where p_u ($u < N$ → $u < 2$ → p_1 and p_2) is understood as $p_1 = p$ and $p_2 = 1 - p$ in order to make it possible to plot using a 2D graph.

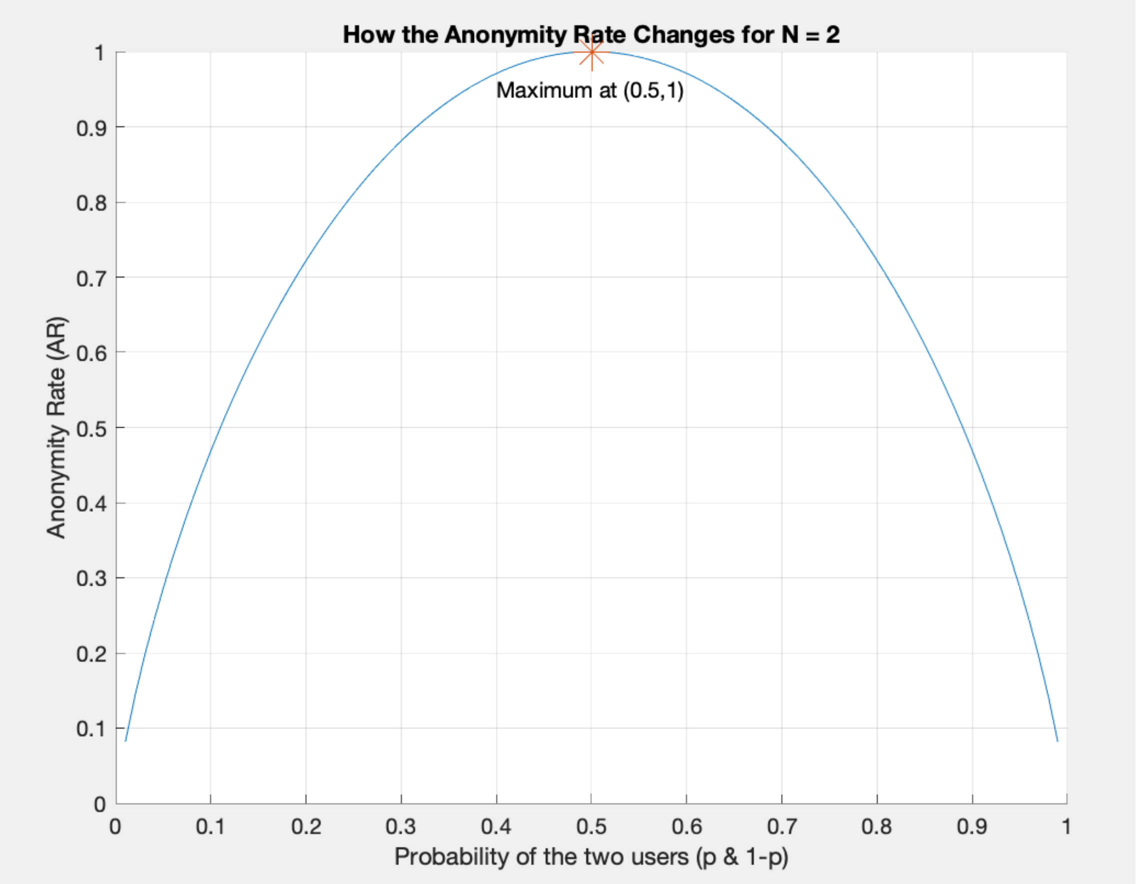


Figure 17. Anonymity Rate graph with N = 2

At the graph we can see how the anonymity rate drops when the probability has a different value than 0.5. Also, it is possible to distinguish where the maximum point is located.

The same concept and technique can be applied for mix networks where the number of users is bigger than two. (N = 3, N = 4, N = 5…). At Figure *18*, it was plotted in 3D the most optimal point where the mix network is proposed with 3 senders. In this case, the anonymity rate is calculated using

Equation 6 with *N = 3* and Equation 5 where p_u $(u < N \rightarrow u < 3 \rightarrow p_1, p_2$and $p_3)$ is understood as $p_1 . p_2$ and $p_3\ = 1 - p_2 - p_1$ in order to make it possible to plot using a 3D graph.

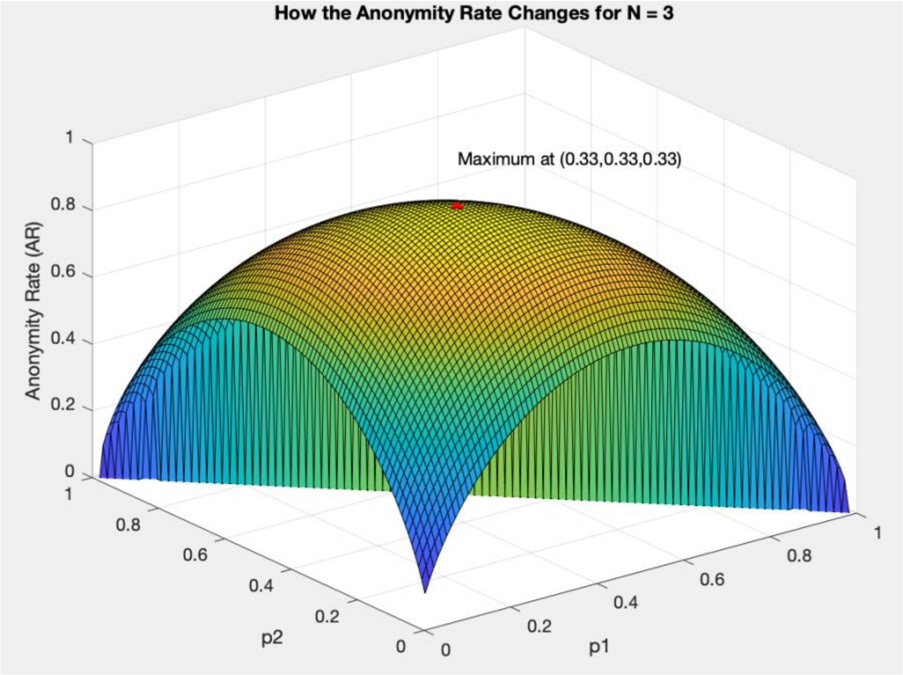


Figure 18. Anonymity Rate graph with N = 3

At the 3D graph we can interpret how the anonymity rate drops when the probability is not equiprobable at the point (0.333, 0.333, 0.333) which matches, also, where the maximum of the display is located.

As it can be deducted, for N ≥ 4, it is not possible to exhibit it graphically since it is beyond the 3 dimensions.

The code use to obtain Figure *17* and Figure *18* can be found at the Appendix V.

Chapter 4. ANALYSIS OF THE RESULTS

4.1. EXAMPLES AND RESULTS

Let's consider the scenario illustrated in Figure *19* where we have 3 possible senders and only 1 threshold mix. The sender anonymity is going to be calculated using the concept of effective size. The mix network used is based on a $\boldsymbol{n_t}$ **– threshold mix**. Historical data, in order words, *a-priori* knowledge about the mix network users are not provided, all the users are equally likely of being the de-anonymized user.

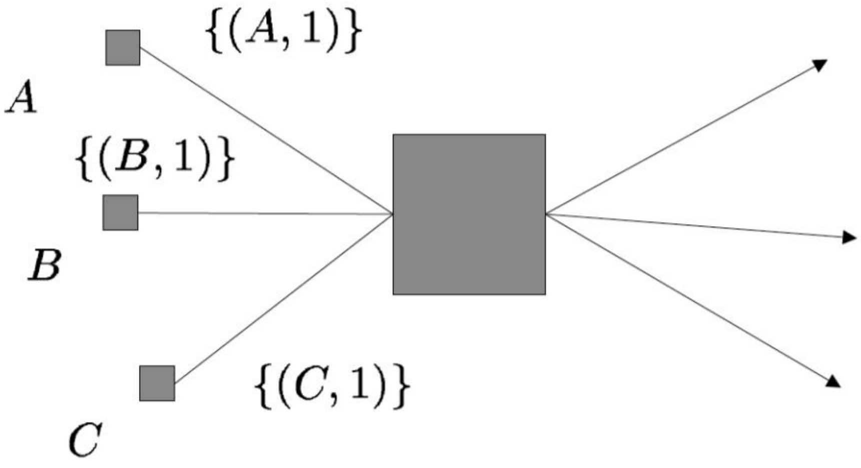


Figure 19. *Third Scenario One Threshold Mix with effective anonymity set size.* Simple example explaining the how the effective anonymity set size works with only one mix [18].

Each sender {A, B and C} sends 1 message at a time. The mix receives *n* incoming messages, in this example, 3 incoming messages with probability distributions of being the de-anonymized user L_0, L_1 and L_2. For a general mix network this will be denoted as L_0 , … , L_{n-1} . (See Figure *20*)

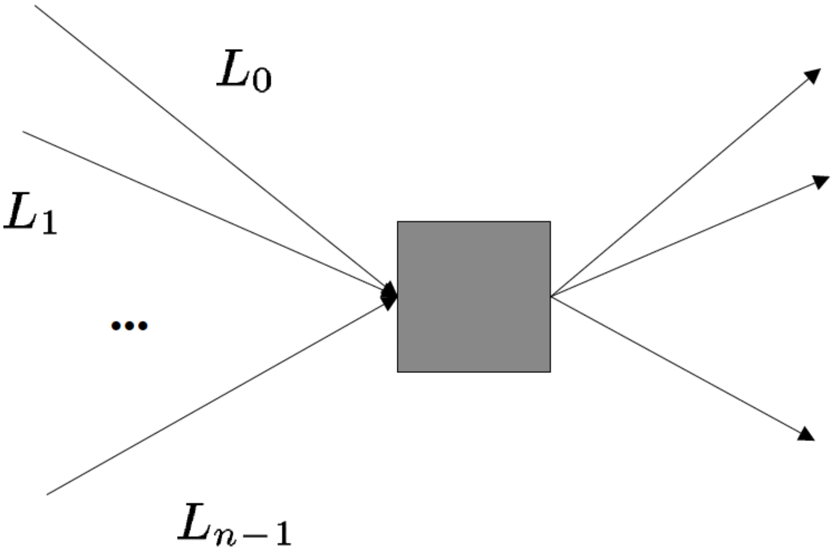


Figure 20. *Notation for anonymity probability distribution*.
General threshold mix with n incoming messages with anonymity probability distributions L_0, ... , L_{n-1}. [18]

Going back to Figure *14*, the anonymity probability distribution for every sender is $\left\{\left(A,\frac{1}{3}\right),\left(B,\frac{1}{3}\right),\left(C,\frac{1}{3}\right)\right\}$. The main difference that we can notice with this measure is that with the use of anonymity probability distribution is that we have a matrix of values assigned to every sender where anonymity changes in one sender affects to the anonymity of the others senders of the network, instead of having only values assigned to different **non-related** probabilities where anonymity changes in one specific sender did not result in changes on the other senders, as it was shown in Figure *13*.

After studying the behavior of one mix, the real mix networks are composed of several individual mixes connected together. In this scenario it is not as simple to calculate the effective anonymity set size of the network as it was with only one mix. First, we need to calculate the effective anonymity set size of each mix of the network.

Let's consider a mix network with ***l*** number of mixes in the first hop after the senders send the messages, each of them with effective sender anonymity size of $\boldsymbol{S_i}$, where $0 < i < l$. After that, all those mixes will forward the messages to a second mix denoted as ***sec***. The probability that a message that has been forwarded to *sec* originated at mix *i* is $\boldsymbol{p_i}$, where $0 < i < l$ and $\sum_i p_i = 1$ [18].

Using the concept of effective size introduced at the beginning of this section, it is possible to determine $\boldsymbol{S_{sec}}$ as

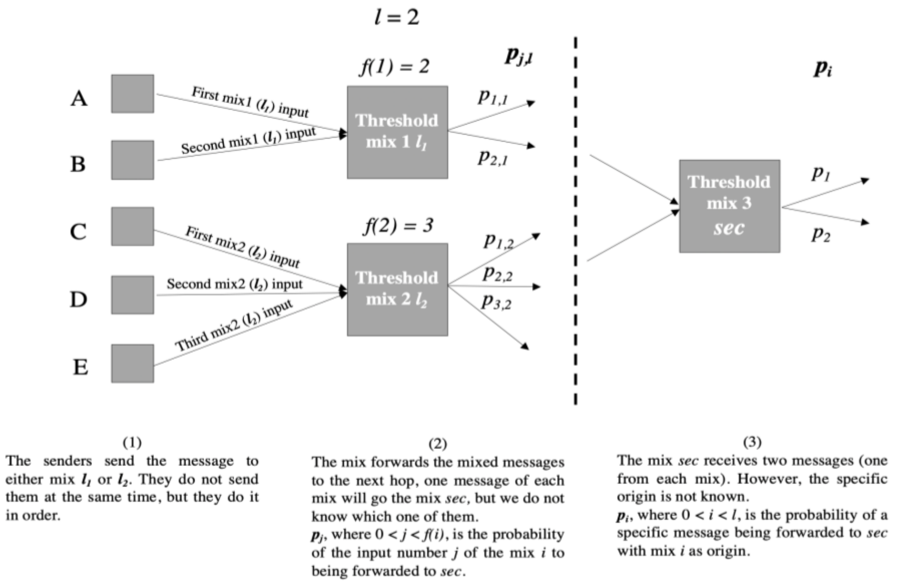
$$\boldsymbol{S_{sec}} = -\sum_{\boldsymbol{0<i<l}} \boldsymbol{p_i log_2\, p_i}$$

Hence, the effective sender anonymity size of the network defined is

$$\boldsymbol{S_{network}} = -\sum_{\boldsymbol{0<i\leq l}} \sum_{\boldsymbol{0<j\leq f(i)}} \boldsymbol{p_j\, p_i log_2\, (p_j\, p_i)}\ [16]$$

where *f(i)* is the number of inputs that the mix *i* receives and p_j, where *0 < j < f(i)* is the probability of the input number *j* of the mix *i* being forwarded to the mix called *sec.* That formula is like that because in order to obtain $\boldsymbol{S_{network}}$ it is necessary to multiply all possible probabilities of each message.

This whole example can be better understood looking at Figure *21*.



(1)
The senders send the message to either mix $\boldsymbol{l_1}$ or $\boldsymbol{l_2}$. They do not send them at the same time, but they do it in order.

(2)
The mix forwards the mixed messages to the next hop, one message of each mix will go the mix *sec*, but we do not know which one of them.
$\boldsymbol{p_j}$, where $0 < j < f(i)$, is the probability of the input number *j* of the mix *i* to being forwarded to *sec*.

(3)
The mix *sec* receives two messages (one from each mix). However, the specific origin is not known.
$\boldsymbol{p_i}$, where $0 < i < l$, is the probability of a specific message being forwarded to *sec* with mix *i* as origin.

Figure 21. *Notation example for effective anonymity set size with several mixes*. Example explaining the notation and values used in order to calculate the effective anonymity set size with several mixes.

However, the schema shown in Figure *21* is not the common scenario of a Global Passive Adversary, it is only used to present the notation used.

4.1.1. GPA ATTACK EXAMPLE

Since the GPA attack is the most frequent attack in mix network it will be studied now an example using the arrangement showed in Figure *22*:

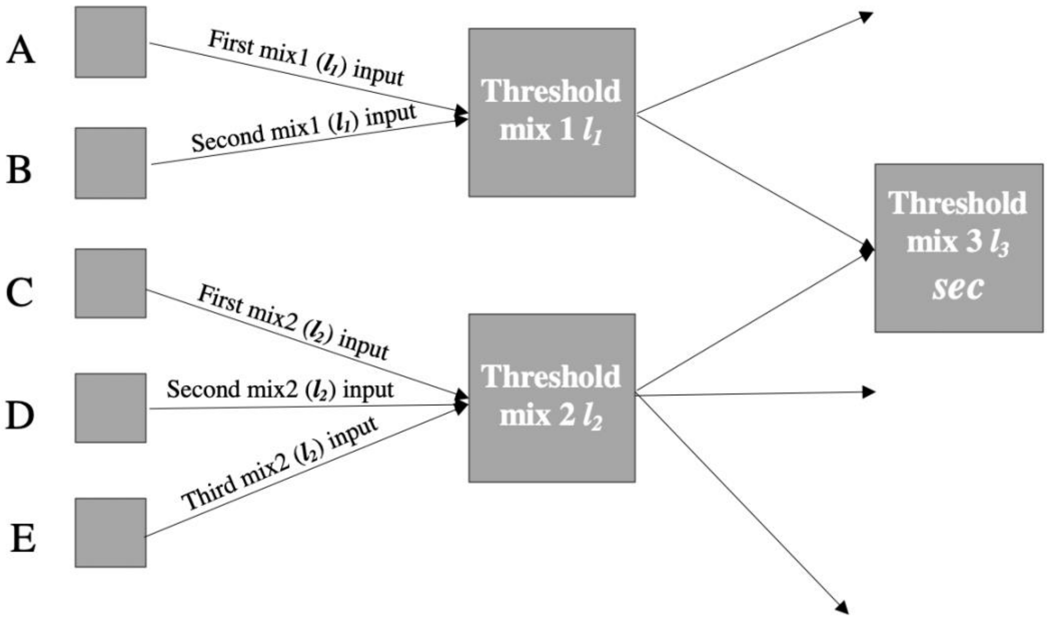


Figure 22. *Global Passive Attack Example*.
GPA example using effective anonymity set size with several mixes.

Let's suppose that the mixes (*l*) forward the messages to the next hop with the following probabilities $\boldsymbol{p_i}$. Where p_i was known as the probability of a message going into sec, originated from mix *i*. For instance, we want to calculate the effective anonymity set size of the network when the targeted message is the one that *B* sends, being the probabilities that a message that has been forwarded to *sec* originated at mix *i*…

- From mix l_1: $p_1 = 0.7$
- From mix l_2: $p_2 = 0.3$

Also, it must be taken into account the probability of the ***j**-th* element arriving at mix ***i*** of being forwarded to *sec* (if $j = 2$ and $i = 1$, it is known that we are referring to the second message that came as input of the mix 1). Besides, there is also a relation between the outgoing probabilities for the first set of mixes and the incoming probabilities of the second set of mixes, in this scenario, incoming messages to sec. In this example, where we want to calculate the effective anonymity set size of the network when the targeted message is the one that *B* sends, it is assumed that the attacker does not know that B sends the message to mix1. Another way of looking at this but with the same outcome is checking the outgoing messages of *sec* and using the $\boldsymbol{p_i}$ and the $\boldsymbol{p_j}$ probabilities to calculate the chances of those messages being originated by *B*. The probabilities $\boldsymbol{p_j}$ in this example are as follow:

- For mix l_1:
  - $p_1 = 0.6$
  - $p_2 = 0.4$
- For mix l_2:
  - $p_1 = 0.3$
  - $p_2 = 0.4$
  - $p_3 = 0.3$

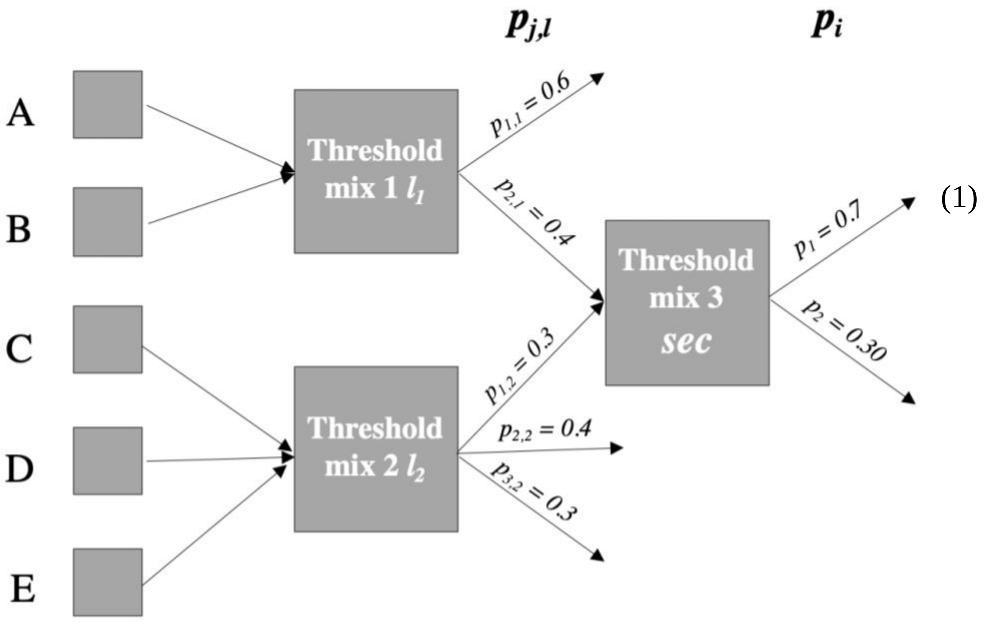


Figure 23. *Global Passive Attack Specific Example*.

So, being

$$S_{network} = -\sum_{0<i\leq l}\sum_{0<j\leq f(i)} p_{j,l}\, p_i log_2\,(p_j\, p_i)$$

$$= -(\,p_{1,1}\, p_1 log_2(p_{1,1}\, p_1) + \;p_{2,1}\, p_1 log_2(p_{2,1}\, p_1) + \,p_{1,2}\, p_2 log_2(p_{1,2}\, p_2)$$

$$+ \;p_{2,2}\, p_2 log_2(p_{2,2}\, p_2) + \,p_{3,2}\, p_2 log_2(p_{3,2}\, p_2)) =$$

$$-\,(0.6 \cdot 0.7 \cdot log_2(0.6 \cdot 0.7) \,+\, 0.4 \,\cdot\, 0.7 \,\cdot\, log_2(0.4 \cdot 0.7)$$

$$+\; 0.3 \,\cdot\, 0.3 \,\cdot\, log_2(0.3 \cdot 0.3) + \;0.4 \,\cdot\, 0.3 \,\cdot\, log_2(0.4 \cdot 0.3)$$

$$+\, 0.3 \,\cdot\, 0.3 \,\cdot\, log_2(0.3 \cdot 0.3)) \approx\, 2.0322$$

After calculating the effective anonymity set size of the network $S_{network}$ when observing an outgoing message trying to determine if it was originated by B or not we obtain that $\boldsymbol{S_{network} \approx 2.0322}$.

A quick check to revise whether or not the value obtained is correct or accurate is testing if the result verifies the first property that I introduced together with the effective anonymity set size concept, which is: $0 \leq$ S $\leq log_2\, N$. In this example, since we have 5 senders, following assumption number 2, we can stablish that even though they do not appear at Figure *23*, there are 5 other recipients, being the total number of users = *senders + recipients = 5 + 5 = 10.* Nevertheless, the anonymity set ***N*** corresponds to the number of possible senders of the messages, so *N = 5.* Therefore, $0\, \leq\, 2.0322\, \leq\, log_2\, 5 \rightarrow 0\, \leq\, 2.0322\, \leq\, 2.322$. The property is fulfilled, so that indicates that it was a good calculation.

Since the value of *S* is already calculated, it is possible to determine the Anonymity Rate *AR* defined at Section 3.4. which will show us the ratio of anonymity currently provided to the system compared with its most optimal scenario. Using

Equation 6 we can define that the AR of this Global Passive Attack example is:

$$AR = \frac{2.0322}{log_2(5)} \approx 0.8752$$

Result 1. *Anonymity Rate Example GPA*

Making an analysis of the result, the outcome obtained is not far away from the *AR = 1* desired, it can be concluded that the mix network is providing an 87.52% anonymity of its maximum optimal point.

Now, suppose we also want to determine the degree of anonymity this scenario provides if we are observing the message (1) showed in Figure *23*. Using the concept of Entropy $\boldsymbol{H}(\boldsymbol{X})$ and the Equation *2*, the entropy of this example for that message is:

$$H(X) = -\sum_{j,l} p_{j,l} \cdot p_1 \, log_b \, p_{j,l} \cdot p_1 \; =$$

$$= -(\, p_{2,1}\, p_1 log_2(p_{2,1}\, p_1) + \, p_{1,2}\, p_1 log_2(p_{1,2}\, p_1)) =$$

$$-(\, 0.4 \;\cdot\; 0.7 \;\cdot\; log_2(0.4 \cdot 0.7) + \; 0.3 \;\cdot\; 0.7 \;\cdot\; log_2(0.3 \cdot 0.7)) \approx \; 0.988$$

A common mistake would have been to compute the Entropy as follows:

$$H(X) = -\sum_{j,l} p_{j,l} \cdot p_1 \, log_b \, p_{j,l} \cdot p_1 \; =$$

$$= -(\, p_{1,1}\, p_1 log_2(p_{1,1}\, p_1) + \; p_{2,1}\, p_1 log_2(p_{2,1}\, p_1) + \, p_{1,2}\, p_1 log_2(p_{1,2}\, p_1) + \; p_{2,2}\, p_1 log_2(p_{2,2}\, p_1) + \, p_{3,2}\, p_1 log_2(p_{3,2}\, p_1)) =$$

$$-(0.6 \cdot 0.7 \cdot log_2(0.6 \cdot 0.7) \; + \; 0.4 \;\cdot\; 0.7 \;\cdot\; log_2(0.4 \cdot 0.7) + \; 0.3 \;\cdot\; 0.7 \;\cdot\; log_2(0.3 \cdot 0.7) + \; 0.4 \;\cdot\; 0.7 \;\cdot\; log_2(0.4 \cdot 0.7) + \; 0.3 \;\cdot\; 0.7 \;\cdot\; log_2(0.3 \cdot 0.7)) \approx 2.4997$$

By doing that we are calculating the probabilities of all the message and that is not correct procedure to follow because in a Global Passive Adversary attack, the adversary has knowledge of the entire network, ergo he is aware of all the possible connections, being $p_{2,1}$ and $p_{1,2}$ the only two connections linked to *sec*.

In order to calculate the degree of anonymity ***d***, it is necessary to know the maximum entropy ***H_M*** the users of the network (

Equation 1). In this case, the measure used is the Anonymity set **N = 5** and not the effective anonymity set size (*S = 2.0322)* because we are looking at the maximum level of entropy, and that is achieved when the mix network is at its most optimal state.

$$H_M = log_b|N| = \ log_2 5 \approx 2.322$$

Now it is possible to calculate the degree of anonymity (Equation *3*):

$$d = \frac{H(X)}{H_M} = \frac{0.988}{2.322} \approx 0.426$$

Result 2. *Degree of Anonymity Example GPA*

Conclusively, the final degree of anonymity that this example provides is ***d = 0.426***. At a first glance, the outcome obtained seems correct because it fulfills the condition $0 \leq d \leq 1$. Another comment is that the result is located under the $d = 0.8$ barrier that it was stablished at Section 3.1.1. meaning that the anonymity provided is not optimal. Yet, this fact should not be a problem because the entire example was made up to show how the metrics work and their effectiveness and accuracy. If this were to happen in a real-life network, I would advise to add several mixes creating more hops. Also, the number of network users should be extremely larger. By following these 2 advises, the mixes will provide more anonymity to the system because every time a message enters any mix, it is not possible to determine the original sender of an outgoing message to the next hop. In addition, having more network users increases the number of *possible original sender of the message*, which makes it harder for the adversary to determine accurate probabilities to each sender.

We can compare the result that it would have been obtained if the measure used had been the effective anonymity set $S = 2.0322$. Using

Equation 1 and Equation *3*:

$$H_M = log_b|S| = \ log_2 2.0322 \approx 1.322$$

$$d = \frac{H(X)}{H_M} = \frac{0.988}{1.322} \approx 0.747$$

As it can be observed, the outcome obtained ***d = 0.747*** in the example where the measure used is not the anonymity size ***N***, but the effective anonymity set size ***S***, the networks has a higher degree of anonymity in comparison with the one obtained (***d = 0.426***) using the anonymity set.

This result was to be expected due to two reasons. First, reducing the network size from 5 to (approx.) 2 takes away multiple possibilities and gives a non-correct sense of the maximum level of entropy. Second, but also related the first one, the degree of anonymity ***d*** is calculated as a division where the numerator is the total entropy of the network (in both scenarios that entropy stays the same way) but the denominator is the maximum entropy of the system calculated based on the network size. For the first scenario, the network size was equal to the anonymity set, which was $N = 5$ that led to a maximum level of entropy of $H_{Mscenario1} = 2.322$. On the other hand, for the second scenario the network size was equal to the effective anonymity set size or $S = 2.0322$. This number gave us a maximum level of entropy of $H_{MScenario2} = 1.322$. Since $H_{MScenario1} > H_{Mscenario2}$, the highest result was expected for the lowest denominator.

With these two scenarios I have shown how these two measures (effective anonymity set size *S* and anonymity set *N*) works under a mix network set-up and given clear reasons with examples on whether to use the one or the other in order to get an adequate estimation of the anonymity rate or the degree of anonymity of the network that we are interested in.

In summary, **Anonymity Rate *AR*** is used to determine the accuracy and to define how optimal a mix network is after an attack. Its goal is to expose how much the mix-net was affected by this event in terms of “number of users that are still anonymous after the attack” being that number also known as effective anonymity set size ***S***. Then, the **Degree of Anonymity *d*** is a measure depending on the number of users before the attack (best possible scenario) and it is mainly focused on the performance of the system. Its goal is to generate a general awareness on how anonymous a system is. This measure depends on the probabilities assigned by the adversary to every sender or recipient. The value obtained will change according to these probabilities being the best scenario or $d = 1$, when all the users have the same probability of being the sender or the recipient of the message.

4.1.2. DE-ANONYMIZATION EXAMPLE

Let's consider the same layout as it was exposed in Section 3.3.1. with the variation of only studying now the process of user de-anonymization.

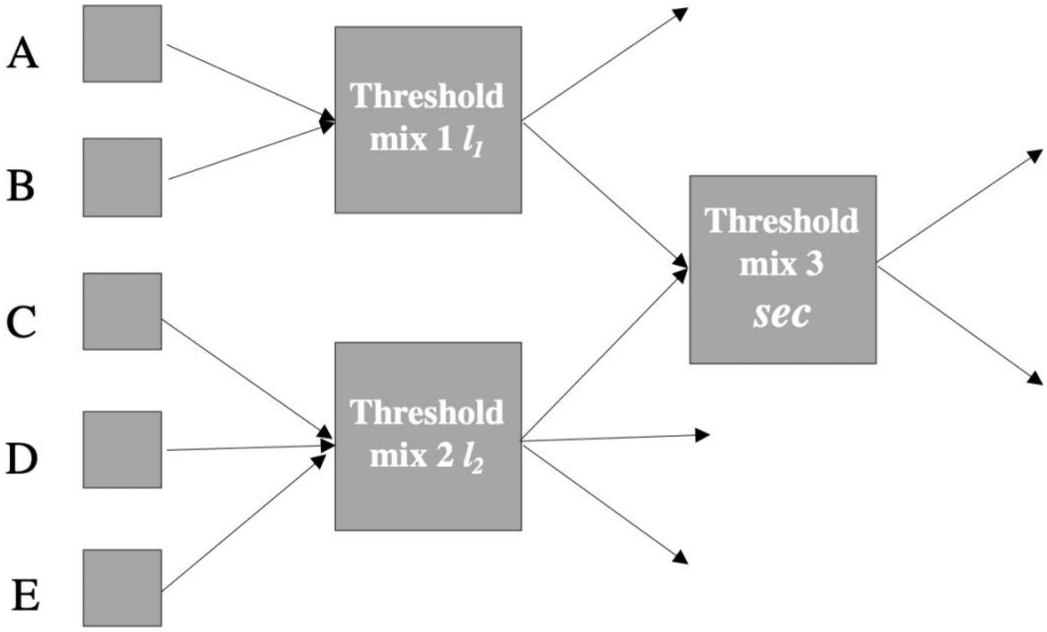


Figure 24. *De-anonymization Layout Example*.

When talking about de-anonymization in this example, we are referring to the possibility where on user makes a mistake that leads to the event of de-anonymizing itself. This can be done in several ways, for instance, a user could include extra identifiable information such as name, credit card details or personal addresses in the message sent when it is not needed. If we assume that the recipient it is an untrusted user, the send is completely de-anonymized. These scenarios can also be extrapolated to the blockchain transaction context where all the movements are generally public, and everyone could have access to it.

For this example, I am considering the same probabilities as it was contemplated at the last example and, also, calculating the effective anonymity set size of the network when the targeted message is the one that *B* sends (See Figure *23*). Let's now suppose that sender *A* makes a mistake (which kind of mistake the user did is not relevant for this case). This mistake would lead to its complete de-anonymization which would change Figure *23* into Figure *25* where it can be observed that all the movements of A are public and known:

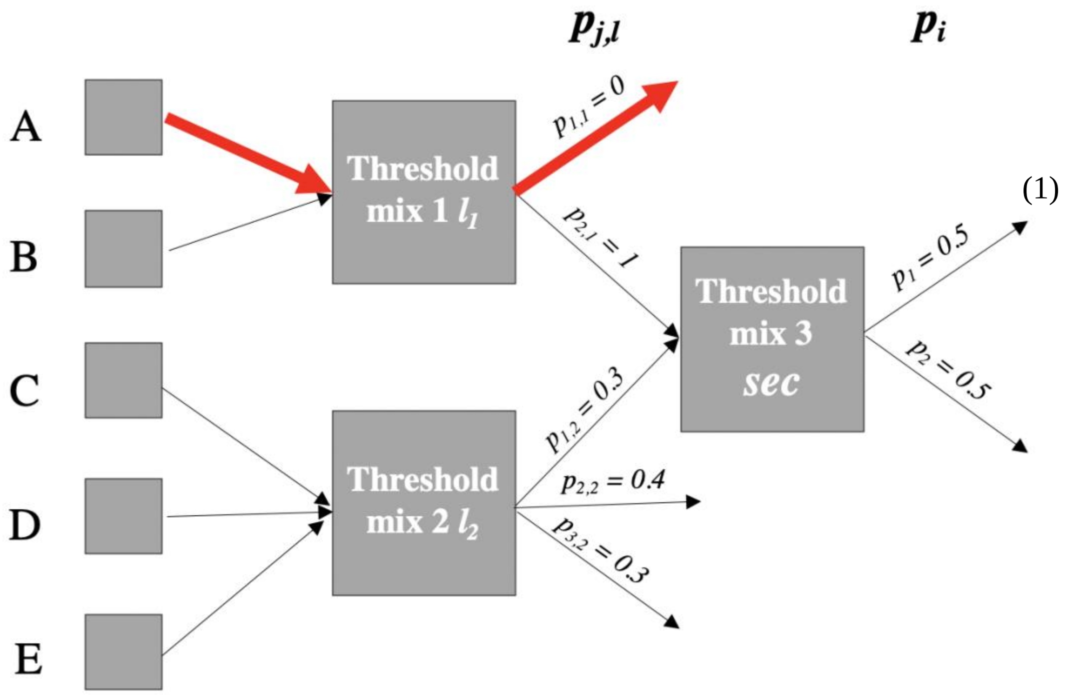


Figure 25. *Specific User De-Anonymizing Example*

The effective anonymity set size ***S*** of this scenario is:

$$S_{network} = -\sum_{0<i\le l}\ \sum_{0<j\le f(i)} p_{j,l}\, p_i log_2\,(p_j\, p_i)$$

$$= -(\,p_{1,1}\,p_1 log_2(p_{1,1}\,p_1) + \ p_{2,1}\,p_1 log_2(p_{2,1}\,p_1) + \ p_{1,2}\,p_2 log_2(p_{1,2}\,p_2) + \ p_{2,2}\,p_2 log_2(p_{2,2}\,p_2) + \ p_{3,2}\,p_2 log_2(p_{3,2}\,p_2)) =$$

$$- (0 + 1 \cdot 0.5 \cdot log_2(1 \cdot 0.5)$$

$$+ 0.3 \cdot 0.5 \cdot log_2(0.3 \cdot 0.5) + 0.4 \cdot 0.5 \cdot log_2(0.4 \cdot 0.5)$$

$$+ 0.3 \cdot 0.5 \cdot log_2(0.3 \cdot 0.5)) \approx 1.7855$$

As it was expected, the effective anonymity set size S when the user *A* de-anonymize itself is lower than in a *normal* example where no de-anonymizing occurs. This is this way because when all the movements and information about A gets uncovered, it directly infers with the B sender's probability. In the first case, the probability of a message that was being forwarded by the first set of mix to *sec*, of being originated by sender *B* was measured by $\boldsymbol{p_{j,l}}$. At the original example $p_{1,1} = 0.6$ and $p_{2,1} = 0.4$. Nonetheless, in this second example, since *A* lost its anonymity the network can know with 100% accuracy that the message that is being forward to *sec* is the one sent by user *B*, being the new probabilities $p_{1,1} = 0$ and $p_{2,1} = 1$ because it is known that the arrow referring to $p_{1,1}$ corresponds to *A* (since it is de-anonymized we are aware of its past and present steps) and that that message is being forwarded to another mix that is not *sec*, leaving the arrow referring to $p_{2,1}$ with $p_{2,1} = 1$. Since there are only 2 users sending messages to the first mix l_1, if the network has information that one of those two messages is not going to the mix *sec*, then it is public knowledge which one is actually going to *sec*.

Besides, subsequently it is known that one of the two messages than are inside the mix *sec* belongs to sender *B*, so the probabilities $\boldsymbol{p_i}$ are also changed. Instead of being $p_1 = 0.7$ and $p_2 = 0.3$ (values randomly generated for the first scenario) now the probabilities are $p_1 = 0.5$ and $p_2 = 0.5$ because the message (1) has equal probability of being the one created by *B* or by C/D/E.

Continuing with the above scenario, suppose we also want to calculate the degree of anonymity this second example provides if we are observing the message (1) showed in Figure *25*. Using the concept of Entropy $\boldsymbol{H(X)}$ and the Equation *2*, the entropy of this example for the second example is:

$$H(X) = -\sum_{j,l} p_{j,l} \cdot p_1 \, log_b \, p_{j,l} \cdot p_1 =$$

$$= -(\, p_{2,1} \, p_1 log_2(p_{2,1} \, p_1) + \, p_{1,2} \, p_1 log_2(p_{1,2} \, p_1)) =$$

$$-(\, 1 \cdot \, 0.5 \, \cdot \, log_2(1 \cdot 0.5) + \, 0.3 \, \cdot \, 0.5 \, \cdot \, log_2(0.3 \cdot 0.5)) \approx \, 0.9105$$

In order to calculate the degree of anonymity ***d***, it is necessary to know the maximum entropy ***H_M*** the users of the network (

Equation 1).

$$H_M = log_b|N| = \, log_2 5 \approx 2.322$$

Now it is possible to calculate the degree of anonymity (Equation *3*)

$$d = \frac{H(X)}{H_M} = \frac{0.9105}{2.322} \approx 0.3921$$

Result 3. *Degree of Anonymity Example De-Anonymization*

At a first sight, the result obtained seems correct because it fulfills the condition $0 \leq d \leq 1$. Another comment is that the result is located way under the $d = 0.8$ barrier that it was stablished at Section 3.1.1. meaning that the anonymity provided is quite not optimal. However, as it was mentioned at the previous example, this circumstance it is not a problem because the example is not based on a real scenario and I created with the only purpose of showing how the metrics work and their characteristics.

Additionally, we need to calculate the Anonymity Rate of the mix-net. Since the value of *S* is already calculated previously at the example, it is possible to determine the Anonymity Rate *AR* defined at Section 3.4. which will show us the ratio of anonymity currently provided to the system compared with its most optimal scenario. Using *Equation 6* we can define that the AR of the de-anonymization example is:

$$AR = \frac{1.7855}{log_2(5)} \approx 0.7690$$

Result 4. *Anonymity Rate Example De-Anonymization*

Formulating an exploration of the result, the outcome obtained it is a bit far from the *AR = 1* desired, due to the fact that the score is located bellow the 0.8 barrier than we are using in this thesis. It can be concluded that the mix network is providing an 76.90% anonymity of its maximum optimal point.

To obtain Result *3* and Result *4* I have considered the anonymity set *N = 5*, which was the total number of users before the event of de-anonymization happened. However, since that particular user (in this example, user A) is completely de-anonymized, some might think that considering the anonymity set *N = 4* could provide a more accurate result. Now, using N = 4 as the chosen measure and

Equation 1, Equation *3* and

Equation 6:

$$H_M = log_b|N| = log_2 4 \approx 2$$

$$d = \frac{H(X)}{H_M} = \frac{0.9105}{2} \approx 0.4553$$

$$AR = \frac{1.7855}{log_2(4)} \approx 0.8928$$

Comparing these results with the ones obtained using *N = 5*, it is clear that the numbers are higher when *N = 4* is implemented. Nevertheless, the degree of anonymity and anonymity rate obtained using *N = 4* does not show the real factors of our network, but it creates a new network with 4 users that provides a general overview on how close this new network to the remaining anonymity is. In other words, using N = 4 as metric tells us how close the network is to the best the network can get (as the 5th user just cannot get any anonymity because it was completely de-anonymized). Using N = 5 as metric tells us how close the network is to what the system aims to provide or what the users expect, namely anonymity for 5 users.

Summing up this example, the **Anonymity Rate *AR*** is used to determine the accuracy and to define how optimal a mix network is after a de-anonymization event took place. Its goal is to expose how much the mix-net was affected by this event in terms of “number of users that are still anonymous after the users' de-anonymization". Then, the **Degree of Anonymity *d*** is a measure depending on the number of users before the de-anonymization event (best possible scenario) and it is mainly focused on the performance of the system. Its goal is to generate a general awareness on how anonymous a system is. This measure depends on the probabilities that each sender (or recipient) has on being the original sender (or recipient) of the message studied. The value obtained will change according to these probabilities being the best scenario or $d = 1$, when all the users have the same probability of being the sender or the recipient of the message.

Chapter 5. CONCLUSIONS

5.1. *CONCLUSIONS ON THE METHODOLOGY AND RESULTS*

This thesis presents a definition and calculation aproach for measuring how the users' anonymity provided by the network in mix networks changes before and after a de-anonymization event. The simulations show that an unexpected de-anonymization incident leads to a significant change in the effective number of mix network users (effective anonymity set size), do not confuse this with the *normal* number of mix network users (anonymity set) . The effects of the loss of one user does not affect to the total number remaining users in a linear way, but that number will decrease significantly more than one as the relations between users and their connections may be revealed as a consequence of that particular user de-anonymization. This means that other network users links exposed, ergo by subtracting only one user out of the effective number of users, we are underestimated the impact of such events.

The scenarios studied in this project also demonstrate the importance of using the correct metric for the appropriate case scenario and knowing the difference between the metric created for this thesis, the anonymity rate, and the already existing measure degree of anonymity. All the other previous paper related to users' anonymity utilize the Degree of Anonymity d as a measure depending on the number of users before an attack (best possible scenario) and it is mainly focused on the anonymity performance (*how much anonymity are we providing*?) of the system. Its goal is to generate a general awareness on how anonymous a system is. This measure depends on the probabilities that each sender (or recipient) has on being the original sender (or recipient) of the message studied. The value obtained will change according to these probabilities being the best scenario or $d = 1$, when all the users have the same probability of being the sender or the recipient of the message. Finally, this thesis uses for the first time the value d related with inadvertently de-anonymization and introduces a new outcome or metric called Anonymity Rate *AR*. *AR* is used to determine the accuracy and to define how optimal a mix network is after a de-anonymization event took place. Its goal is to expose how much the mix-net was affected by this event in terms of "*number of users that are still anonymous after the users' de-anonymization*".

5.2. Recommendations for Future Studies

The motivation of this thesis is based on the idea of mix network anonymity by David L. Chaum that originated vast studies in anonymity protocols (Onion Rounting Protocol – TOR) and users's interaction for Blockchain Anonymity (specifically in Ethereum). However, there is no comprehensive research yet on how the external de-anonymization factors could result in the de-anonymization of mix network users, and this thesis serves as first step in this field.

Since this project is the opening contact with the users' de-anonymization field, I feel that more sophisticated metrics should be developed. Nevertheless, a metric and approach providing accurate information about the mix network status after a de-anonymization event is defined and studied here. However, this thesis only focused on sender anonymity; recipient anonymity can be treated analogously. I propose a thorough analysis on the procedures and entropies explained in this thesis to design later on a tailored measure for the concrete problem or receiver anonymity.

The usefulness of my model should be more intensively examined. Since this project is based on the mix network setting and the use of mixes imply a few seconds delay in the communication, it would be interesting to measure the right balance between performance and privacy. It would be a worthy topic of research investigating about the optimal point between the time delayed (because of the mix network) and the anonymity provided by the mix-net. The question here will be: Is it worthy, for instance, 5 seconds delayed for the anonymity that we are experiencing thanks to the use of a mix network?

Additionally, this model is based on the probability's adversaries assign to users; knowing in advance these probability distributions in real situations is, however, not easy. So, it would be interesting to take into account the a priori information the adversary or the network may have over the users and mix-net distribution, and use the model design to calculate the amount of information the adversary has gained with the attack or the amount of information the network has lost with the de-anonymization event.

And a deeper study on how to determine these distributions is needed. Another question that still remains open is the sufficient level of anonymity a mix network should provide to have anonymity and privacy levels certified. In other words, how much level of anonymity is *good enough* for a being a trustworthy network? To answer this question several aspects must be considered, since it depends on the legal and social consequences of the breach of privacy/anonymity in different situations. This is context dependent, and requirements may vary from systems to system.

In the future, I would also like to consider other batching strategies as in this paper it was only measured the threshold mix. If further research is carried away it could be showed (or not) that other approaches such as timed mix, pool mix, timed pool mix or timed dynamic pool mix could provide better results in the anonymity topic studied, reducing the differences between the anonymity degree measured before and after the de-anonymization event. The ultimate goal is to design a network where the loss of one user hardly affects the mix-net.

Chapter 6. REFERENCES

[1] S. B. Venkatakrishnan, G. Fanti and P. Viswanath, Dandelion: Redesigning the Bitcoin Network for Anonymity, vol. 1, University of Illinois at Urbana-Champaign: Proc. ACM Meas. Anal. Comput. Syst., 2017, pp. 1-34.

[2] N. Christin, Travelling the silk road: A measurement analysis of a large anonymous online marketplace, In Proceedings of the 22nd international conference on World Wide Web, 2013, pp. 213-224.

[3] C. o. F. R. o. t. E. Union, "EUR-Lex," 26 October 2012. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT. [Accessed 13 June 2020].

[4] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008.

[5] E. Orrú, Effects and Effectiveness of Surveillance Technologies: Mapping Perceptions, Reducing Harm., vol. 39, SURVEILLE Project. Surveillance: Ethical Issues, Legal Limitations, and Efficiency; EUI Working Paper LAW, 2015.

[6] A. Westin, Privacy and Freedom, New York: Atheneum, 1967.

[7] L. Floridi, The ontological interpretation of informational privacy, Oxford: Springer, 2006, p. 1–16.

[8] W. Diffie and S. Landau, Privacy on the Line .The Politics of Wiretapping and Encryption, The MIT Press, 2017.

[9] R. Rivest, A. Shamir and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, 1978, pp. 120-126.

[10] W. Diffie and M. Hellman, New directions in cryptography, vol. 6, IEEE Trans. Information Theory 1T-22, 1976, pp. 644-654.

[11] R. Merkle, Secure communications over insecure channels, vol. 4, Comm. ACM 21, 1978, pp. 294-299.

[12] F. Hirsch, "Apache HTTP Server Project. SSL/TLS Strong Encryption: An Introduction," Apache HTTP Server, [Online]. Available: https://httpd.apache.org/docs/trunk/ssl/ssl_intro.html.

[13] A. Pfitzmann and M. Kohntopp, Anonymity, unobservability and pseudonymity – a proposal for terminology. In Designing Privacy Enhanceing Technologies: Proceeding of the International Workshop on the Design Issues in Anonymity and Observability, H. Federrath, 2001, pp. 1-9.

[14] A. Serjantov, On the anonymity of anonymity systems, Cambridge: University of Cambridge, Computer Laboratory, 2004.

[15] D. Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms., vol. 4(2), Communications of the ACM, 1981, pp. 84-88.

[16] C. Díaz and A. Serjantov, Generalising Mixes. In International Workshop on Privacy Enhancing Technologies, Berlin, Heidelberg: Springer, 2013, pp. 18-31.

[17] D. Chaum, The dining cryptographers problem: Unconditional sender and recipient untraceability, vol. 1(1), Journal of Cryptology: the journal of the International Association for Cryptologic Research, 1988, pp. 65-75.

[18] A. Serjantov and D. George, Towards an Information Theoretic Metric for Anonymity, Dingledine and Syverson (Ed.) Designing Privacy Enhancing Technologies, LNCS 2482, 2002, pp. 41-53.

[19] C. E. Shannon, A mathematical theory of communication, vol. 27, The Bell System Technical Journal, 1948, pp. 379-423.

[20] J. Blitzstein and J. Hwang, Introduction to Probability, CRC Press, 2014.

[21] D. G. Steigerwald, Economics 245A – Introduction to Measure Theory, Santa Barbara, California: University of California, 2013.

[22] J. Albert, Listing All Possible Outcomes (The Sample Space), Ohio: Bowling Green State University, 1998.

[23] D. Goldschlag, M. Reed and P. Syverson, Onion Routing for Anonymous and Private Internet Connections, Naval Research Lab Washington DC, 1999.

[24] R. Dingledine, N. Mathewson and P. Syverson, Tor: The second-generation onion router, Naval Research Lab Washington DC, 2004.

[25] P. Winter, A. Edmundson, L. Roberts, A. Dutkowska-Zuk, M. Chetty and N. Feamster, How Do Tor Users interacts with Onion Services?, Baltimore, MD, USA: Proceedings of the 27th USENIX Security Symposium. USENIX Association, 2018, p. 411–428.

[26] F. Béres, I. A. Seres, A. A. Benczúr and M. Quintyne-Collins, Blockchain is Watching You: Profiling and Deanonymizing Ethereum Users, Budapest: Institute for Computer Science and Control (SZTAKI), 2020, pp. 1 - 18.

[27] C. Díaz, S. Seys, J. Claessens and B. Preneel, Toward measuring anonymity, Leuven-Heverlee: K.U.Leuven ESAT-COSIC, 2002.

[28] I. 25237:2017, "Health informatics — Pseudonymization," ISO, 2017.

[29] M. Reiter and A. Rubin, Crowds: Anonymity for Web Transactions, vol. 42 (2), Com- munications of the ACM, 1999, pp. 32-48.

[30] O. Berthold, A. Pfiztmann and R. Standtke, The Disavantages of Free MIX Routes and How to Overcome Them, In Hannes Federath (Ed.), Designing Privacy Enhancing Technologies, Lecture Notes in Computer Science, LNCS 2009,, 2009, pp. 30-45.

[31] S. Clauß and S. Schiffner, Structuring Anonymity Metrics, vol. 6, Proceedings of the second ACM workshop on Digital Identity management, 2006, pp. 55-62.

[32] ISO, Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408, 1999.

[33] V. Shmatikov and M.-H. Wang, Measuring Relationship Anonymity in Mix Networks, Alexandria, Virginia: The University of Texas at Austin, 2006.

[34] J. Hayes, Traffic Confirmation Attacks Despite Noise, San Diego, California: University College London, 2016.

[35] R. Soltani, D. Goeckel, D. Towsley and A. Houmansadr, Towards Provably Invisible Network Flow Fingerprints, Pacific Grove, California: 51st Asilomar Conference on Signals, Systems, and Computers , 2017, p. 258–262.

[36] J.-F. Raymond, Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems, Berlin, Heidelberg: In Hannes Federath. Designing Privacy Enhancing Technologies, Lec- ture Notes in Computer Science, LNCS, 2001, pp. 10 - 29.

[37] A. Zarrabi, A Generic Process Migration Algorithm, vol. 3, Selangor: International Journal of Distributed and Parallel Systems (IJDPS), 2012.

[38] C. Díaz, Anonymity Metrics Revisited, Schloss Dagstuhl-Leibniz-Zentrum für Informatik: In Dagstuhl Seminar Proceedings, 2005.

[39] R. Dingledine, V. Shmatikov and P. Syverson, Synchronous batching: From cascades to free routes, Springer. In International Workshop on Privacy Enhancing Technologies , 2004, p. 186–206.

[40] T. M. Cover and J. A. Thomas, Elements of Information Theory, John Wiley & Sons, Inc, 2012.

[41] R. Hartley, Transmission of Information, vol. 7, Bell System Technical Journal, 1928, p. 535–563.

[42] G. Fanti, S. B. Venkatakrishnan, S. Bakshi, B. Denby, S. Bhargava, A. Miller and P. Viswanath, Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees, vol. 2, Proc. ACM Meas. Anal. Comput. Syst., 2018., pp. 1-35.

[43] B. Curran, "BLOCKONOMI," 4 October 2018. [Online]. Available: https://blockonomi.com/dandelion-protocol/. [Accessed 17 April 2020].

[44] G. Danezis, R. Dingledine and N. Mathewson, Mixminion: Design of a Type III Anonymous Remailer Protocol, Proceedings of the 2003 IEEE Symposium on Security and Privacy, 2003, pp. 2 - 15.

[45] A. Piotrowska, J. Hayes, T. Elahi, S. Meiser and G. Danezis, The Loopix Anonymity System, Proceedings of the 26th USENIX Security Symposium. USENIX Association, 2017, pp. 1199-1216.

[46] D. Kesdogan, J. Egner and R. Büschkes, Stop-and-go mixes providing probabilistic anonymity in an open system, Springer. In International Workshop on Information Hiding, 1998, pp. 83-98.

[47] L. Cottrell, Mixmaster and remailer attacks, 1995.

[48] G. Danezis, R. Dingledine and N. Mathewson, Mixminion: design of a type III anonymous remailer protocol. Symposium on Security and Privacy, Berkeley, California, 2003, pp. 2-15.

[49] C. Gulcu and G. Tsudik, Mixing E-mail with Babel. Proceedings of Internet Society Symposium on Network and Distributed Systems Security, San Diego, California, 1996, pp. 2-16.

[50] A. Jerichow, J. Müller, A. Pfitzmann, B. Pfitzmann and M. Waidner, Real-Time Mixes: A Bandwidth-Efficient Anonymity Protocol, vol. 16, IEEE Journal on selected areas in communication, 1998, pp. 495-509.

[51] M. Jakobsson, Flash Mixing, Murray Hill, New Jersey: ACM. Information Sciences Research Center, Bell Labs, 1999.

[52] M. Renukadevi, N. Bhaskar and R. Prabu, Anomaly Protection Using Batching Strategies, vol. 4, Journal of Computer Applications (JCA) , 2011, pp. 113-118.

[53] A. Serjantov, R. Dingledine and P. Syverson, From a Trickle to a Flood: Active Attacks on Several Mix Types, vol. 2578 of LNCS, Washington D.C., Washington: Naval Research Laboratory. In 5th Workshop on Information Hiding, 2002.

[54] K. Michael, S. Kobran, R. Abbas and S. Hamdoun, "Privacy, Data Rights and Cybersecurity," Miriam Cunningham and Paul Cunningham, 2019.

[55] United Nations, "Sustainable Development Goals: Knowledge Platform - Technology," [Online]. Available: https://sustainabledevelopment.un.org/topics/technology. [Accessed 10 July 2020].

[56] United Nations, "Universal Declarations of Human Rights," [Online]. Available: https://www.un.org/en/universal-declaration-human-rights/. [Accessed 11 July 2020].

[57] M. Michael, K. Michael and C. Perakslis, Überveillance, the web of things, and people: What is the culmination of all this surveillance?, vol. 4, IEEE Consumer Electronics Magazine, 2015, pp. 107-113.

Chapter 7. APPENDIXES

APPENDIX SDG

When technology is used in a good-will way with the honest end of directing its power to reach sustainable development goals, human rights are also attached to this idea. In the context of technology, privacy, security, anonymity and innovation techniques are four areas that are key in providing the freedom and dignity that all individuals are entitled to [54]. These four topics are, in fact, the topics that this thesis works on.

Nowadays, one of the matters that concerns the most to the United Nations is to bring developing countries on par with already developed countries, the fast implementation of technology and innovation is often seen as the answer to the achievement of the 17 Sustainable Development Goals (SDG) that the United Nations asks to all the nations to fulfill before 2030.

Technology is also describe as a way of "*achieving innovation, business opportunities and development, trade of environmental goods and services, finance and investment, and institutional capabilities*" [55].

The main topic that is studied and research on my thesis and that is, also, a concern in the Sustainable Development Goals by the United Nations is the role of privacy regarding communications networks and technology. "***Goal 9: Build resilient infrastructure, promote sustainable industrialization and foster innovation***" is the primary Social Development Goal involved and treated in this BSc project.

The idea of this SDG is to upgrade the current world industrialization status by providing inclusive and sustainable technologies that, together with innovation and infrastructure, can unleash dynamic and competitive economic flows that generate employment and income. Nevertheless, the countries still have a long path to walk (by increasing the investment and funds in scientific research and innovation) if they want to reach the 2030 target.

Goal 9 focuses its action plan in 3 sectors: manufacture, industrialization and innovation. However, my thesis is mainly focused on the innovation and technological progress that are key to finding lasting and trustworthy solutions for online privacy in the communication infrastructure scenario. Nevertheless, in my project I do not search for the specific trustworthy solutions that are needed for privacy, but rather making sure that all the trustworthy solutions for communication infrastructures implement are in alliance and respectful of fundamental human rights showed at the European Union Law such as respect to private life (Article 7 from [3]) and protection of personal data together with a fair data processing for specific purposes (Article 8 from [3]).

In terms of communications infrastructure, more than half of the world's population is now online and almost the entire world population lives in an area covered by a mobile network. The United Nations estimated in their Economic and Social Council in July 2020 that in 2019, 96.5 per cent of the world citizens. were covered by at least a 2G network.

Investment in sustainable communication infrastructure and in scientific and technological research regarding increasing anonymity and privacy levels in the online set-up will raise economic growth, create jobs and promote prosperity and security. In other words, Goal 9 aims to build resilient infrastructure, promote industrialization and foster innovation. In addition, my thesis work contributes to the understanding of how we can implement such infrastructures in a way that is respectful of human rights.

Goal 9 aims to support technology development, research and innovation especially in developing countries, where (maybe) privacy on the Internet is not listed as Top 3 problems they need to deal with. Nevertheless, it is our duty, together with small-scale industrial and other companies with greater access, to financially reliable and secure communication services including universal and affordable access to the Internet in the least developed countries of the world.

Within this SDG, there are two sub-goals that this thesis is involved in. Since this BSc project is focused on metrics for measuring anonymity and technologies that provide to the mix network users a decent degree of privacy, the thesis can be linked first with sub-goal 9.5. This target aims to "*enhance the scientific research and upgrade the technological capabilities of industrial sectors in all countries*". Second, the thesis proposed in this document is based on a mix network setting with the main purpose of providing a secure online communication service. For this reason, my research can be linked to a secondary degree with sub-goal 9.c. This objective explains that the countries must "*increase access to information and communications technology and strive to provide universal and affordable access to the Internet in the least developed countries by 2020*". As it was already mentioned above in this appendix, 96.5% of the world population has access to the Internet, meaning that this sub-goal is about reaching its objective.

However, the goal 9 is not my only concern out of the 17 SDGs. **Goal 3: "*Ensure healthy lives and promote well-being for all at all ages*"** it is also exposed in my thesis as a secondary Social Development Goal involved and treated in this work. How? Article 12 of the Universal Declaration of Human Rights states the right to all individuals to privacy as a key principle that ensures their freedom: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor or reputation*" [56].

In the era of social media, communication, mobile and computer devices and the online world that is continuously keeping track of all our transactions and movements leaving behind a digital footprint, it seems difficult, almost impossible, to preserve privacy [57]. Exactly, my thesis aims to provide a mix-net network where the privacy is maintained, and every user is aware of the amount of private information that is known by the network.

Lastly, non-updated, corrupted or non-existent digital infrastructure makes conducting your activities weakly secured and challenging. Our online communication must rely on resources, worthy service support from all servers involved and must provide the ability to access the network used efficiently. These all factors are key to establishing secure and anonymous communication between different parties.

Privacy, security, anonymity and innovation techniques present each a unique challenge in order to fulfill the SDGs. Each of the four topics mentioned is vital for the successful implementation of any new technology is development countries. By committing to sustainable industrialization and promoting innovation in the anonymizing field, users from all different kind of regions and social classes can contribute to developing an upgrading local infrastructure, investing in communications technologies. These will make these technologies available to all people, including marginalized groups, who might not have access otherwise. Having secure access to the online world must be able for all citizens.

APPENDIX I

```
%Active Attacker Example


p = linspace(0,1);
d = -((p.*(log2(p)))+((1-p).*(log2(1-p))));
plot(p,d);
title('Active attack example')
xlabel('Probability of being the sender (p)')
ylabel('Degree of Anonymity (d)')
axis([0 1 0 1])
grid on
```

APPENDIX II

```
%Passive Attacker Example


p = linspace(0,1);
d = (-((4*((p/4).*(log2(p/4))))+((6*(((1-p)/6).*(log2((1-
p)/6)))))))/(log2(10));
plot(p,d);
title('Passive attack example')
xlabel('Probability of being the sender (p)')
ylabel('Degree of Anonymity (d)')
axis([0 1 0 1])
grid on
```

APPENDIX III

```
%%Comparison Batching Strategies Models
n = linspace(0,500);

%For the pool related mixes it will be considered a pool np=50
np = 50;

%For the timed dynamic pool mix f = 0.6
f = 0.6;

%For the threshold mix Nt = 100
Nt = 100;

%Timed mix
n1 = 0;
n2 = 500;
p_n1 = 1;
subplot(2,2,1)
plot([n1, n2], [p_n1, p_n1])
title('Timed Mix')
xlabel('Number of messages inside the mix at the time of flushing
(n)')
ylabel('Percentage of messages fowarded to next hop (P(n))')
axis([0 500 0 1.2])
grid on

%Timed pool mix
p_n2 = 1-(np./n);
asymptote1 = 1;
subplot(2,2,2)
plot(n,p_n2,[n1, n2], [asymptote1, asymptote1],'--')
title('Timed Pool Mix')
xlabel('Number of messages inside the mix at the time of flushing
(n)')
ylabel('Percentage of messages fowarded to next hop (P(n))')
axis([0 500 0 1.2])
```

```
grid on

%Timed dynamic pool mix
p_n3 = f.*(1-(np./n));
asymptote2 = f;
subplot(2,2,3)
plot(n,p_n3,[n1, n2],[asymptote2, asymptote2],'--')
title('Timed Dynamic Pool Mix')
xlabel('Number of messages inside the mix at the time of flushing
(n)')
ylabel('Percentage of messages fowarded to next hop (P(n))')
axis([0 500 0 1])
grid on

%Threshold mix
subplot(2,2,4)
plot(Nt,1,'*','MarkerSize',15)
title('Threshold Mix')
xlabel('Number of messages inside the mix at the time of flushing
(n)')
ylabel('Percentage of messages fowarded to next hop (P(n))')
axis([0 500 0 1.2])
grid on
```

APPENDIX IV

```
%Entropy n = 9 loop
n = 9;
H_x1 = 0;
p_i = (1/n);

for i=2:n
    H_x1 = H_x1 + (p_i*(log2(p_i)));
end

H_x1 = -(H_x1);

disp(H_x1)
```

```
%Entropy n = 9999 loop
n = 999;
H_x2 = 0;
p_i = (1/n);

for i=2:n
    H_x2 = H_x2 + (p_i*(log2(p_i)));
end

H_x2 = -(H_x2);

disp(H_x2)
```

APPENDIX V

```
%% AR PLOTS EXAMPLES

% N = 2
p = linspace(0,1);
AR2 = -((p.*(log2(p)))+((1-p).*(log2(1-p))));

hold on;
plot(p,AR2);
plot(0.5,1,'*','MarkerSize',15)
title('How the Anonymity Rate Changes for N = 2')
xlabel('Probability of the two users (p & 1-p)')
ylabel('Anonymity Rate (AR)')
text(0.4,0.95, 'Maximum at (0.5,1)');
axis([0 1 0 1])
grid on

% N = 3
N   = 3;
dp  = 0.01;

ps = dp:dp:1-dp;
S = zeros(length(ps));
```

```
for i = 1:length(ps)
    for j = 1:length(ps)
        if ps(i)+ps(j) >= 1
            continue;
        end


       p3 = 1-ps(i)-ps(j);

        p       = [ps(i) ps(j) p3];
        S(i,j) = -sum(p.*log2(p));

    end
end

AR = S/log2(N);

figure();
surf(ps,ps,AR);
hold on;
scatter3(0.33,0.33,max(AR(:)),40, 'filled', 'r');
text(0.33,0.33,max(AR(:))+0.15,'Maximum at (0.33,0.33,0.33)');

title('How the Anonymity Rate Changes for N = 3')
zlabel('Anonymity Rate (AR)')
xlabel("p1");
ylabel("p2");
grid on
```