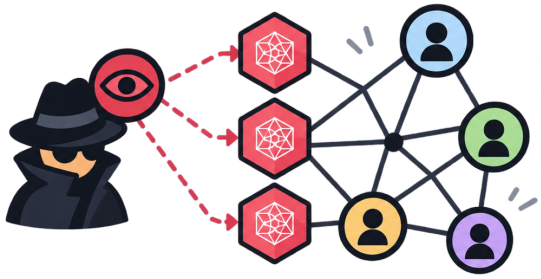
Machine Learning-Based Anonymity Evaluation in Mixnets



Mixnets are Internet overlay networks designed to provide online anonymity by obscuring users' communication patterns, even against powerful network adversaries with substantial observational capabilities. However, their anonymity guarantees against such adversaries have not been thoroughly evaluated.

In this master's thesis, we aim to develop a machine-learning-based adversarial model to evaluate mixnet anonymity against an adversary that collects communication traces over time. The goal is to train a model that can effectively correlate observed connections with their originating clients, thereby assessing the extent to which long-term traffic observations can compromise anonymity.

The student is expected to have a solid background in machine learning, particularly neural networks, and strong Python programming skills.

Practicalities

Promotor:	Bart Preneel		
Daily supervisor:	Mahdi Rahimi	mahdi.rahimi@esat.kuleuven.be	office B01.27
	Alireza Aghabagherloo	Alireza.Aghabagherloo@esat.kuleuven.be	office B01.27

Nature of the work:	20% literature, 20% theoretical work, 60% software
Number of students:	1

 © 2025 – 2026 COSIC