Collaborative Fraud Detection in Financial Networks using Secure Multi-Party Computation (MPC)

Financial institutions operate extensive fraud detection frameworks combining rule-based systems, anomaly detection, and machine learning models. However, each institution only observes a partial view of the interbank transaction network, limiting the effectiveness of network-derived indicators such as PageRank-style centrality or community risk propagation. Secure Multi-Party Computation (MPC) enables multiple institutions to jointly compute such network features without revealing private data. Prior work has demonstrated that collaboratively computing PageRank on coupled transaction graphs using additively homomorphic encryption can efficiently approximate the true global PageRank and improve indicator quality compared to siloed approaches.

The goal of this thesis is to design and evaluate MPC-friendly algorithms that enrich existing fraud indicators with information from a joint financial transaction network. The outcome should include a proof-of-concept (PoC) demonstrating feasibility and analyzing performance and accuracy trade-offs in a collaborative, privacy-preserving setting.

The thesis will start with a survey of privacy-preserving graph analytics and fraud detection techniques. Different MPC paradigms and secure graph primitives will be compared. Based on this, suitable fraud indicators that are both impactful and MPC-friendly will be identified. One or more MPC-compatible algorithms will then be proposed, focusing on linear or low-depth computations to minimize MPC overhead. An appropriate MPC framework will be selected, and communication patterns will be designed to prevent information leakage while keeping the number of rounds and ciphertext volume manageable. A selected approach will be implemented end-to-end and integrated with a synthetic multi-bank transaction graph generator that preserves key statistics. The evaluation will measure the uplift from MPC-computed network features, as well as time/CPU, communication rounds and volume, scalability with respect to nodes/edges/parties, numerical effects such as rounding error and convergence, and the underlying security assumptions.

The student should have strong mathematical system modeling skills and solid knowledge of cryptography. A strong interest in privacy preserving technologies and willingness to learn can bridge the gap in case prior knowledge is not present. The ideal master student for this thesis would have followed the following courses:

- System Identification and Modeling (H03E1B)
- Computer Algebra for Cryptography (H0E74A)
- Cryptography and Network Security (H05E1B)
- Privacy Technologies (H09L2A)

Practicalities

Promotor:	Prof. dr. ir. Bart Preneel
	Dr. Aysajan Abidin
Daily supervisor:	Qasim Naqvi qasim.naqvi@kbc.be office KBC
Nature of the work:	30% literature, 30% theoretical work, 40% implementation
Number of students:	1

 © 2026 – 2027 COSIC