Project title: **Dealing with Financial Fraud through Privacy-Enhancing Technologies**

Contact

Main Supervisor: Dr Aydin Abadi, email: aydin.abadi@ncl.ac.uk

Research project

Sharing data is crucial in dealing with crime. Collaborative data analysis among law enforcement agencies and relevant stakeholders can significantly enhance crime prevention, investigation, and overall public safety. Typically, inputs for collaborative data analysis come from different parties, each of which may have concerns about the privacy of their data. Federated Learning (FL) schemes and secure Multi-party Computation (MPC) protocols are examples of mechanisms that allow parties to collaboratively analyze shared data while maintaining the privacy of their input data. The goal of this project is twofold: (i) to identify types of financial fraud that can be more effectively addressed through enhanced collaboration and data analysis from various stakeholders, and (ii) to develop appropriate Privacy-Enhancing Technologies (PETs), such as FL or MPC, to combat fraud while ensuring data privacy.

Project title: **Incentivizing Participation in Privacy-Enhancing Technologies**

Research project

Privacy-Enhancing Technologies (PETs), such as Secure Multi-party Computation (MPC) and Federated Learning (FL) allow parties to collaboratively analyze a collection of data partitions where each data partition is contributed by a different party (such as banks, or law enforcement agencies). Two facts about PETs exist: (i) the output of PETs reveals some information about the parties' private input sets (i.e., the computation result in FL or MPC), and (ii) various variants of PETs do not output the result to all parties, even in those PETs that do, not all of the parties are necessarily interested in it. Given these facts, a natural question arises: How can we incentivize parties that do not receive the result or do not express interest in it to participate in PETs? This project aims to develop new Privacy-Enhancing Technologies (PETs) that incentivize participants to share their sensitive data by fairly rewarding them. Additionally, the project aims to ensure these PETs remain secure even when adversaries compromise some parties.

Project title: **Enhancing Federated Learning Efficiency and Scalability with Advanced Cryptographic Protocols**

Research project

Federated Learning (FL) is a machine learning framework where multiple parties collaboratively build machine learning models without revealing their sensitive input to their counterparts. FL has found applications in various domains such as dealing with financial fraud, detecting online grooming, and enhancing healthcare services. Often FL schemes rely on cryptographic protocols to preserve the privacy of parties such as data contributors.

This research seeks to enhance FL's real-world adoption by improving the efficiency and scalability of cryptographic protocols used in FL. Specifically, the project aims to improve the computational and communicational efficiency of cryptographic protocols to ensure they do not become a bottleneck in the FL process. It also aims to enhance the scalability of these protocols so that FL can be applied to large-scale datasets and numerous participants without compromising performance.

Project title: **Mitigating Insider Threats in Financial Sectors through the Development and Use of Privacy-Enhancing Technologies**

Research project

Insider attacks pose imminent threats to various organizations and their clients, such as financial institutions and their customers. Insiders may collaborate with external fraudsters, obtaining highly valuable data. The aim of this project is to develop new Privacy-Enhancing Technologies (PETs), with a particular focus on Secure Multi-party Computation (MPC), to enable bank customers to send queries and requests to their banks in a way that preserves their privacy. The goal is to ensure that customers can interact with their banks without having to disclose their sensitive data and queries to any single employee of the bank. This approach addresses privacy concerns and enhances data security in financial transactions and communications.

Project title: **Improving Federated Learning Model Quality with Privacy-Preserving Data Cleaning Techniques**

Research project

This project aims to enhance the quality of federated learning (FL) models by developing innovative privacy-preserving data-cleaning techniques. FL lets multiple parties collaboratively train machine learning models without centralizing their data, but data inconsistencies and noise at local nodes can degrade model performance. Traditional data cleaning methods often compromise data privacy, posing challenges in sensitive environments such as healthcare or finance services. This research will investigate novel privacy-preserving approaches for effective data preprocessing in FL settings.

Applicant skills/background: Candidates should possess or be highly motivated to acquire strong knowledge in the following areas: (1) cryptography, (2) PETs such as MPC or FL, (3) mathematics (including number theory), and (4) computer programming in C++, Java, or Python.