Privacy preserving ML with HE

Generative AI tools such as ChatGPT have gained popularity and are increasingly integrated into our everyday lives. Users often rely on these tools for various tasks, including asking sensitive and private questions. Ideally, such queries should remain confidential, and the content of the data should be hidden from the cloud service provider. The conventional solution for this type of problem involves protection techniques such as encryption. However, traditional encryption schemes do not allow any useful computations, so they cannot compute an answer to the question. Can we think of an encryption scheme that allows manipulation of the underlying data?

The answer to the above question is *yes*, and this type of cryptography is known as homomorphic encryption (HE). With an HE scheme, any untrusted party can evaluate functions over encrypted data without knowledge of the decryption key, so the content remains secret. As a result, the cloud server can perform machine learning algorithms, while at the same time protecting the user's privacy concerns.

The goal of this thesis is to develop privacy preserving machine learning algorithms based on the recently proposed homomorphic encryption schemes such as [1]. The student will first analyse cryptographic protocols and existing machine learning algorithms, such as decision trees. These need to be adapted to the homomorphic setting and implemented in an HE library. Finally, the student will assess the performance and compare it to related work.

Practicalities

Promoter:	Emmanuela Orsini emmanuela.orsini@unibocconi.it Office 2-C2-03
Nature of the work:	40% literature, 20% theoretical work, 40% software
Number of students:	Max 2
Prerequisites:	A background in cryptography and programming skills are required

[1] Robin Geelen and Frederik Vercauteren. *Fully homomorphic encryption for cyclotomic prime moduli*, EUROCRYPT 2025. Available at: `https://eprint.iacr.org/2024/1587`.