Team Members

- Miguel Tulla
- Maria Chrysafis
- David Hu
- Edward Wan

Preliminary Topics

- **Prompt encryption with LLMs**. Ideally, we would have LLMs trained on unencrypted data and then adjusted so they can leverage FHE when running inference on prompts. However, this is too computationally intensive to realistically do with current technology. Nonetheless, it would be interesting to analyze
  - What computational advances are necessary to use FHE with LLMs?
  - Are there ways to not fully encrypt prompts but increase privacy by modifying the prompt? For example, changing certain words or phrases with less detailed paraphrasing could provide very similar results without exposing the full text.
  - Is it possible to build a very small LLM that uses FHE but is still useful (e.g. has ok performance on a simple task such as sentiment analysis)?
- In this project, we plan to explore zero-knowledge proofs. Zero-knowldge proofs enable one party (the prover) to convince another party (the verifier) of the truth of a statement without revealing additional knowledge (such as how the truth was found). We will investigate and implement specific zero-knowledge protocols, such as zk-SNARKs and zk-SPARKs. Some applications may be an anonymous credentials systems (https://eprint.iacr.org/2022/878.pdf), a platform for data sharing, or anonymous payment systems (https://www.mdpi.com/2813-5288/2/1/2).
- This project proposes to explore the theoretical foundations of elliptic curve cryptography (ECC) and implement several prominent ECC schemes, including elliptic curve Diffie-Hellman (ECDH), Elliptic Curve Integrated Encryption Scheme (ECIES), and Elliptic Curve Digital Signature Algorithm (ECDSA)/EdDSA. Through this implementation, we will provide an overview of the mathematics behind ECC operations, e.g. point addition and scalar multiplication, and understand how these operations underpin the security of ECC-based cryptographic protocols. Furthermore, we intend to compare the performance of these ECC schemes with their counterparts based on modular arithmetic over finite fields (Z_p), providing insights into the efficiency and computational overhead of ECC in practical cryptographic applications.

Regular Weekly Meeting Time

Proposition: Wednesday 5PM