Project Proposal:

- **Topic area and problem statement:** The general area and the specific goal that you set out to achieve (in a few sentences).
    - **Homomorphic Encryption** - Implementation based project with a lit review (background and related work section) that demonstrates a comprehensive understanding of multiple peer reviewed papers. The lit review will include papers on HE as a stand-alone encryption method, I will also include papers that elaborate on the different schemes present within this topic derived from the Learning with Errors (LWE) problem (ie. CKKS, BFV), and lastly papers in which HE is coupled with Federated Learning. I have attached a list of the papers I plan to review below.
    - The implementation side of the project will consist of implementing a working version of the CKKS scheme (I will be doing my best to re-implement the existing structure using the math theory outlined in the first blog post linked below). I will then be comparing it to a unique HE scheme (following BFV a little more which I will build, which will simply: generate keys, encrypt and decrypt and run different operations on encrypted data.
    - I will then extend this implementation by running the TenSEAL library github tutorial. The tutorial consists of training a PyTorch model on MNIST, then implement an equivalent one using TenSEAL, following an evaluation of encrypted inputs. I will complete the tutorial twice: firstly, following the original tutorial and then again with modifications.
    - Different modifications may include the following:
        - The principal modification I will be doing on the second tutorial will subbing in my new HE scheme where CKKS is used. We can then compare the encrypted data performance of both models.
        - Differ the model architecture (ie. Activation function, kernel, number of CNN layers, starting weights…) (I would love feedback on what you may think may be best)
- **Expected results: A description of the results/outcomes/contributions that you expect to achieve from completing the project (in a few sentences)**
    - I expect to note the performance differences between CKKS and a BFV structured HE scheme. Since we know that CKKS is more suited for arithmetic on real numbers, where we can have approximate but close results, while BFV is more suited for arithmetic on integers – then we may expect to see stronger performance from CKKS as the square activation function is used. But if we were to change the activation function to sigmoid or softmax, then we could expect to see BFV perform much better. That being said, I believe that I should (at least) test for different activation functions for both HE schemes – particularly those that have been tried and tested and proven to produce high accuracy on the MNIST dataset.
- **Primary resources:** Academic and/or non-academic references and tools, software libraries, or hardware (where applicable) that will serve as the starting point and that will play a key role in helping you complete your project. List the resources and in one or two sentences each briefly describe each item, how it relates to your project, and how you plan to make use of it
    - Cheon, Jung Hee, et al. "Homomorphic encryption for arithmetic of approximate numbers." *International Conference on the Theory and Application of Cryptology and Information Security* . Springer, Cham, 2017.
        - A description of methods to construct a homomorphic encryption scheme for approximate arithmetic. This will help me understand the underlying concrete construction foundation of RLWE schemes – then delineates a clear algorithm for CKKS with an additional rescaling procedure.
    - Kim, Andrey, Antonis Papadimitriou, and Yuriy Polyakov. "Approximate homomorphic encryption with reduced approximation error." *Cryptology ePrint Archive* (2020).
        - This will be part of the lit review to showcase my understanding of the different improvements that have been made to the original LWE and RLWE HE schemes
    - MLAAslett, Louis JM, Pedro M. Esperança, and Chris C. Holmes. "A review of homomorphic encryption and software tools for encrypted statistical machine learning." *arXiv preprint arXiv:1508.06574* (2015).
    - Fan, Junfeng, and Frederik Vercauteren. "Somewhat practical fully homomorphic encryption." *Cryptology ePrint Archive* (2012).APA

        - This paper was incredibly handy in learning the differences in schemes derived from LWE and Ring LWE (RLWE) problems.
    - Li, Jing, et al. "Privacy preservation for machine learning training and classification based on homomorphic encryption schemes." *Information Sciences* 526 (2020): 166-179.APA
    - Fang, Haokun, and Quan Qian. "Privacy preserving machine learning with homomorphic encryption and federated learning." *Future Internet* 13.4 (2021): 94.
        - These last two papers will demonstrate the importance and relevance of HE in different ML applications which work with sensitive client data (health, financial, personal)
    - Li, Wenqi, et al. "Privacy-preserving federated brain tumour segmentation." *International workshop on machine learning in medical imaging* . Springer, Cham, 2019.
        - These last three papers above I have included because the idea of coupling federated learning and homomorphic learning was incredibly intriguing to think about in terms of increasing the preservation of privacy within different ML applications. I have yet to think about a way in which I can extend the idea of my project to include FE.
        - I think I will still include these in my lit review section in order to showcase the next steps and different directions(predicted future implementations) of HE.
    - https://blog.openmined.org/ckks-explained-part-1-simple-encoding-and-decoding/
        - This blog was jam packed with resources that outlined different topics. From their definitions to different fields of application and even tutorials which inspired the idea for this project.
    - https://blog.openmined.org/private-machine-learning-explained/
    - https://developer.nvidia.com/blog/federated-learning-with-homomorphic-encryption/
        - This was one of the resources that was shared by the professor and it honestly was what inspired me to dig a little deeper into all of the different resources and
    - Benaissa, Ayoub, et al. "Tenseal: A library for encrypted tensor operations using homomorphic encryption." *arXiv preprint arXiv:2104.03152* (2021).
        - open-source library for Privacy-Preserving Machine Learning using Homomorphic Encryption that can be easily integrated within popular machine learning frameworks.
    - https://github.com/OpenMined/TenSEAL
        - This is the github which hosts the TenSEAL library and helpful tutorials – particularly relevant to this project, as the main goal is to imitate the results of the original and official documentation.