**Thesis:** Homomorphic Secret Sharing from Paillier Encryption

**Abstract:** Secure Multi-Party Computation (MPC) allows a group of parties to compute a joint function on their inputs without revealing any information beyond the result of the computation. Cloud Computing is the use of computer system resources without direct active management by the user, is an example of a secure MPC application. As these services gain popularity, concerns regarding data privacy are arising. One approach to preserving data privacy is Homomorphic Secret Sharing (HSS), which allows a non-interactive computation over the shares of the secret input with low computation complexity. We present an HSS based on the circular security of the Paillier encryption scheme which allows the non-interactive computation of Branching Programs over shares of the secret inputs. Additionally, we offer a verification technique to directly check correctness of the actual computation. This results in fewer repetitions of the overall computation for a given error bound.

We also applied Paillier encryption as an underlying scheme to present a publicly evaluable perceptual hashing (PH). A robust PH allows social media platforms to prevent uploading explicit multimedia files of their users without their consent. Using PH algorithms raise a vital privacy concern; If users are aware that an explicit image of theirs is in another’s possession and want to prevent such an image from being posted, they have to provide the image to the social media platform so that the PH can be evaluated on it and added to the blacklist. Is it possible to have robust and publicly evaluable perceptual hash functions? We answered this question in an affirmative

**Committee:**

- Professor Rosario Gennaro, mentor, The City College of New York
- Professor Nelly Fazio, The City College of New York
- Professor William E. Skeith, The City College of New York

**Outside Member:**

- Markus Jakobsson, Security Researcher at ByteDance