

## **Abstract**

Fully Homomorphic Encryption has been dubbed the Swiss Army knife of cryptography, as it offers a single tool that can be uniformly applied to many cryptographic applications. It allows one to compute arbitrary functions over encrypted data without the decryption key.

This thesis traces the development of Homomorphic Encryption leading up to the first construction of a Fully Homomorphic Scheme by Gentry in 2009. We begin by presenting the basics mathematical foundation as well as a brief treatment of what constitutes a cryptosystem. We then proceed to offer details of Partially Homomorphic Encryption and Somewhat Homomorphic Encryption, both of which are essential pillars of achieving Fully Homomorphic Encryption. Next, we provide an in-depth exposition of Gentry's key result. We end with a treatment of practical applications stemming from the advent of Homomorphic Encryption.