University of Victoria | Graduate Studies

# Notice of the Final Oral Examination
# for the Degree of Master of Applied Science

of

## ALI SAEED ALZAHRANI

BSc (Umm Alqura University, 2010)

## "CRT Based Somewhat Homomorphic Encryption Over the Integers"

Department of Electrical and Computer Engineering

**Thursday April 23, 2015**
**10:00 A.M.**
**Engineering Office Wing**
**Room 430**

Supervisory Committee:
Dr. Fayez Gebali, Department of Electrical and Computer Engineering, University of Victoria (Supervisor)
Dr. Haytham El Miligi, Department of Electrical and Computer Engineering, UVic (Member)

External Examiner:
Dr. Faheem Ahmed, Department of Computer Science, Thompson Rivers University

Chair of Oral Examination:
Dr. Marc Lapprand, Department of French, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

# Abstract

Over the last decade, the demand for privacy and data confidentiality in communication and storage processes have increased exponentially. Cryptography can be the solution for this demand. However, the critical issue occurs when there is a need for computing publicly on sensitive information or delegating computation to untrusted machines. This must be done in such a way that preserve the information privacy and excitability. For this reason, we need an encryption algorithm that allows

computation on information without revealing details about them. In 1978 Rivest, Adleman and Dertouzos [RAD78] raised a crucial question can we use a special privacy homomorphism to encrypt the data and do an unlimited computations on it while it remains encrypted without the necessity of decrypting it? Researchers made an extensive efforts to achieve such encryption algorithm. In this thesis, we have introduced the implementation of the CRT-based somewhat homomorphic encryption over the integers scheme. The main goal is to provide a proof of concept of this new and promising encryption algorithm.