University of Victoria | Graduate Studies

Notice of the Final Oral Examination
for the Degree of Doctor of Philosophy

of

# MOSTAFA ESMAEILI

MSc (Isfahan University of Technology, 2012)
BSc (Isfahan University of Technology, 2009)

## "Application of Linear Block Codes in Cryptography"

Department of Electrical and Computer Engineering

Friday, March 15, 2019
9:00 A.M.
Engineering and Computer Science Building
Room 468

Supervisory Committee:
Dr. T. Aaron Gulliver, Department of Electrical and Computer Engineering, University of Victoria (Supervisor)
Dr. Stephen Neville, Department of Electrical and Computer Engineering, UVic (Member)
Dr. Bruce Kapron, Department of Computer Science, UVic (Outside Member)

External Examiner:
Dr. Masoud Ardakani, Department of Electrical and Computer Engineering, University of Alberta

Chair of Oral Examination:
Dr. Michael Masson, Department of Psychology, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

## Abstract

Recently, there has been a renewed interest in code based cryptosystems. Amongst the reasons for this interest is that they have shown to be resistant to quantum attacks, making them candidates for post-quantum cryptosystems. In fact, the National Institute of Standards and Technology is currently considering candidates for secure communication in the post quantum era. Three of the proposals are code based cryptosystems. Other reasons for this renewed interest include efficient encryption and decryption. In this dissertation, new code based cryptosystems (symmetric key and public key) are presented that use high rate codes and have small key sizes. Hence they overcome the drawbacks of code based cryptosystems (low information rate and very large key size). The techniques used in designing these cryptosystems include random bit/block deletions, random bit insertions, random interleaving, and random bit flipping. An advantage of the proposed cryptosystems over other code based cryptosystems is that the code can be/is not secret. These cryptosystems are among the first with this advantage. Having a public code eliminates the need for permutation and scrambling matrices. The absence of permutation and scrambling matrices results in a significant reduction in the key size. In fact, it is shown that with simple random bit flipping and interleaving the key size is comparable to most well known symmetric key cryptosystems in use today such as Advanced Encryption Standard (AES).

The security of the new cryptosystems are analysed. It is shown that they are immune against previously proposed attacks for code based cryptosystems. This is because scrambling or permutation matrices are not used and the random bit flipping is beyond the error correcting capability of the code. It is also shown that having a public code does not limit the security of a cryptosystem. This is proved in two ways, by finding the probability of an adversary being able to break the cryptosystem and showing that this probability is extremely small, and showing that the cryptosystem has indistinguishability against a chosen plaintext attack (i.e. is IND-CPA secure). IND-CPA security is among the primary necessities for a cryptosystem to be practical. This means that a ciphertext reveals no information about the corresponding plaintext other than its length. It is also shown that having a public code results in smaller key sizes.