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

of

MOHAMMAD HAJIABADI

MSc (University of Victoria, 2011)
BSc (Sharif University of Technology, 2009)

“Encryption Security Against Key-Dependent-Message Attacks: Applications, Realizations and Separations”

Department of Computer Science

Thursday, August 4, 2016
10:00 A.M.
David Turpin Building
Room A136

Supervisory Committee:
Dr. Bruce Kapron, Department of Computer Science, University of Victoria (Supervisor)
Dr. Venkatesh Srinivasan, Department of Computer Science, UVic (Member)
Dr. Audrey Yap, Department of Philosophy, UVic (Outside Member)

External Examiner:
Dr. Rafael Pass, Department of Computer Science, Cornell University

Chair of Oral Examination:
Dr. Angela Downey, School of Business, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies
Abstract

In this thesis we study the notion of circular security for bit-encryption schemes. Informally speaking, a bit-encryption scheme is circular secure if it remains secure even if the key of the system is used to encrypt its own individual bits. This notion (or slight extensions thereof) has foundational applications, most notably in the context of fully-homomorphic encryption and amplification techniques for key dependent message security.

We explore the notion of circular security from three different perspectives, stemming from (1) assumptions sufficient to realize this notion, (2) minimal black-box assumptions on which this notion can be based and (c) applications of this notion when combined with other properties. Our main results are as follows:

• We give a construction of circular-secure public-key bit encryption based on any public-key encryption scheme that satisfies two special properties. We show that our construed scheme besides circular security also offers two forms of key-leakage resilience. Our construction unifies two existing specific constructions of circular-secure schemes in the literature and also gives rise to the first construction based on homomorphic hash proof systems.

• We show that seed-circular-secure public-key bit-encryption schemes cannot be based on semantically-secure public-key encryption schemes in a fully-blackbox way. A scheme is seed-circular-secure if it allows for the bits of the seed (used to generate the public/secret keys) to be securely encrypted under the (corresponding) public key. We then extend this result to rule out a large and non-trivial class of constructions for circular security that we call key-isolating constructions.

• We give generic constructions of several fundamental cryptographic primitives based on a public-key bit-encryption scheme that combines circular security with a structural property called reproducibility. The main primitives that we build include families of trapdoor functions with strong security properties (i.e., one-wayness under correlated inputs), adaptive-chosen-ciphertext (CCA2) secure encryption schemes and deterministic encryption schemes.