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

of

BEN KIMMETT

BSc (University of Victoria, 2010)

“Improvement and Simulation of King & Saia’s Expected-Polynomial Time Byzantine Agreement Algorithm”

Department of Computer Science

Friday, May 29, 2020
10:30 A.M.
Remote Defence

Supervisory Committee:
Dr. Valerie King, Department of Computer Science, University of Victoria (Co-Supervisor)
Dr. Yvonne Coady, Department of Computer Science, UVic (Co-Supervisor)

External Examiner:
Dr. Peter Smith, Principal Software Engineer/Researcher, Galvanize

Chair of Oral Examination:
Dr. Timothy Iles, Department of Pacific and Asian Studies, UVic

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

We present a partial implementation of King and Saia 2016's expected-polynomial time byzantine agreement algorithm, which extends Bracha's byzantine agreement algorithm by adding an interactive consistency algorithm to generate a shared coin flip. In addition to implementing the King-Saia algorithm, we detail a new version of its shared coin flip subalgorithm, which improves the subalgorithm's resilience from $t < n=4$ to $t < n=3$. We test the King-Saia algorithm, and detail a series of adversarial attacks against it; we also create a Monte Carlo simulation to further test one particular attack's level of success at biasing the shared coin flip.