QIC 891 Topics in Quantum Safe Cryptography

Module 1: *Post-Quantum Cryptography*

Homework

Student:Your Name Here *Due date: June 2, 2016*

You are encouraged to write up your solution using LaTeX. A template .tex file is available at the course webpage.

1. Review a few major directions for post-quantum cryptography: *lattice*-based, *code*-based, *multivariate quadratic polynomial* (MQ)-based.
   (a) (3 points) For each direction, give examples of proposed schemes for public-key **encryption** and **signature**.
   (b) (3 points) For each direction, give examples of some hard problems and popular algorithms for them.

2. Digital signature.
   (a) (2 points) Hash-based signature scheme is based on a generic construction from one-way functions. Describe the two steps of the generic construction.
   (b) (2 points) Given a 3-round identification scheme $(G,(P,V))$. Describe how to turn it into a signature scheme by the Fiat-Shamir transformation.
   (c) (2 points) Suppose that we want to prove the security of an identification scheme and the Fiat-Shamir transformation against quantum attackers. Describe two (or more) challenges.

3. Public-key encryption.
   (a) (4 points) Based on lattices, codes and MQ each, describe a candidate function f and a corresponding trapdoor f^{-1}.
   (b) (4 points) Describe a method of constructing an IND-CPA encryption scheme from a injective trapdoor one-way function $(f, f^{-}1)$ and a random oracle $\mathcal{O}$. Give your justification why the construction is secure and explain possible difficulties of proving security against quantum attackers.