

CryptoWorks21: Post-quantum cryptography

Assignment

(Due date: August 31, 2020)

Geovandro Pereira

August 4, 2020

Problem 1

- a) Give a few reasons (among the ones mentioned in class) of why it can be relevant to migrate the current classical cryptography infrastructure to a post-quantum one.
- b) Why hash-based signatures are a potential better candidate for digital signatures? For which type of applications they may not be a good fit?

Problem 2

Consider the definition of the Rainbow signature scheme (slide 24 from the set of MPKC slides available at [cw21-post-quantum-II.pdf](#)). Also consider the UOV signature scheme magma implementation provided at [uov-impl.mag](#). Now, extend the UOV implementation to the simplest case of Rainbow, i.e., a two layer Rainbow with parameters given in the toy example (slide 26) w.r.t the following operations:

- a) Key pair generation
- b) Sign
- c) Verify

P.S.: You can use the Magma website to test your code: <http://magma.maths.usyd.edu.au/calc/> and the online documentation to learn about the Magma language itself <http://magma.maths.usyd.edu.au/magma/handbook/>.