CryptoWorks21: Post-quantum cryptography - QIP 891
Assignment

Javad Doliskani and Geovandro Pereira

July 30th - Aug 2nd, 2018

August 2, 2018

1. Problem 1. 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/.

2. Problem 2.

   a) Implement the Mersenne LH cryptosystem using your favorite language. Use the parameters n = 1279, h = 17. The prime is defined as $p = 2^n - 1$. The original reference can be obtained at `https://eprint.iacr.org/2017/481.pdf`

   b) (Bonus) For a given security parameter λ, i.e. to have λ bits of classical security, it is needed that $\binom{n-1}{h-1} \geq 2^{\lambda}$. Explain.