Extra Project Cryptography

Chiara Spadafora
chiara.spadafora@unitn.it

Irene Villa
irene.villa@unitn.it

Trento, 23 May 2023

The extra project consists in writing a MAGMA code which find a solution to the *Closest Vector Problem* over lattices. These solutions must be encoded in a .mag file called **yourname_yoursurname.mag**.

Write a function called *MyClosestVector(L,w)* with the following specifications:

```
NAME:  MyClosestVector(L,w)
INPUTS:   -L, a lattice
          -w, a vector with real coefficients and with the same dimension as L
OUTPUTS:  -v, one of the closest element in L to w
```

Clearly, you cannot use the already implemented MAGMA functions to solve the *Closest Vector Problem*. To test the correctness of your code, you can create the lattices and the vectors by yourself, and then check it using the already implemented MAGMA functions.
Our test will be performed as displayed.

```
Input L: a lattice of dimension n
      V: VectorSpace(RealField(3),n)
      Test: a list of elements in V

for w in Test do
    W:=ClosestVectors(L, w);
    v:=MyClosestVector(L,w);
        if not v in W then
        "error";  break;
        end if;
end for;
```

All the code must be **completely written in MAGMA language**, without calling any external program.
The project will be tested and evaluated during the lecture on **06/06/2023**. During the lecture, the probability that your code works correctly will be evaluated, together with the speed.

The 7 participants presenting the most successful algorithm will receive one extra point. In case of dispute, we will consider the speed of the algorithm.