Implementing the lookup table:

Lookup table should be a vector of packed Z3<81> elements of size 2^16.

Each element in the vector will be the result of multiplication of the 81X16 packed slice of the original Randomization Z3 matrix with 1-BYTE (16bit) of the input.

The input to the function that creates this is the Z3 matrix, and the output will be a C++ vector of 2^16 Z3<81> elements.

There will be 16 such C++ vectors, one for each slice of the R3 matrix. Each slice of the R3 matrix will be a 16- Z3<81> packed elements

There will be two functions:

CreateLookupTable – creates the lookup table

Input: Z3 matrix

Output: 16 C++ vectors. Each C++ vector is of size 2^16. Packed Z3<81> elements

UseLookupTable – calculate the multiplication

Input: input vector X

Output: packed version of the multiplication of the Z3 matrix with this input