Can Fully Homomorphic Polynomial Encryption Be Completely Noiseless?

Yes!

Problem Statement and Goals

• Currently, every existing fully homomorphic encryption system has noise.
• This puts a hard upper limit on the number of computations within a certain accuracy range, since noise increases exponentially with multiplication.
• Finding an algorithm which is able to eliminate the need for noise would increase precision of results, in addition to allowing for more computations.

Approach

• Used Galois Theory to compose suitable rules and restrictions for a finite ring of polynomials over another finite ring.
• Constructed a system of recurrence relations which needed to be satisfied.
• Designed a family of systems which satisfied these relations, and confirmed their cryptographic security.
• Implemented the fastest of these in c++ and measured its speed for a variety of sizes.

Results

• Can compute 1000 multiplications in one second, where the elements were polynomials of degree 64 over the ring Z/[8192].
• Works with any ring, so long as division is sufficiently hard to protect the private key.
• The next step is to use this to perform machine learning on encrypted data and to implement several optimizations.
• In addition, I would like to implement systems which allow for arbitrary integer size, which would support arbitrary cryptographic difficulty with minimal speed cost. I am also trying to find a ring with properties conducive to matrix multiplication.
• Acknowledgements: Dr. Vishnu Boddeti, my advisor.