Homomorphic encryption is a method of encryption such that, with operations addition and multiplication defined on both the set of plaintexts and the set of ciphertexts, decryption is a homomorphism from the set of ciphertexts to the set of plaintexts. In other words, decrypting the sum of two ciphertexts gives the sum of the decryptions of the two ciphertexts, and the same for the products. Fully homomorphic encryption allows for both multiplication and addition, while partial homomorphic encryption only has addition.

The importance of this type of encryption is that it allows one to perform operations on encrypted data. As an example, one commonly used in applications of homomorphic encryption in machine learning[1], a user could send an encrypted vector to a server, which then performs the required operations (that being matrix-vector multiplication, convolutions, and squaring each term), and then sends the encrypted result back to be decrypted. At no point in this process did anyone but the user know the data that was sent, but response was correct.

Integer homomorphic encryption was theorized, proved, and then created by Craig Gentry[2], but (in order to preserve security) had to include noise. This noise, taking the form of a small error, would grow rapidly, and quickly rendered the results useless after only a few multiplications. Polynomial homomorphic encryption, with the current best being Fan and Vercauteren’s[3], can process more data at once than a single integer, can be made with far less noise, and is much faster than individual integer operations.

However, there is still noise. To compensate for this, most of polynomial homomorphic encryption innovation is focused on speed and machine learning, since machine learning does not require exact results and speed is the only limiting factor.[1] All current systems have noise[2], though, and this imposes a complexity event horizon. Once too many calculations are made, the data becomes unusable, forcing the machine learning to be quite simplistic.

This system of homomorphic encryption is based on a pair of recurrence relations which must be satisfied for decryption to be possible. This recurrence was satisfied through the introduction of another recurrence, which provided the information to properly complete multiplication without sacrificing security. The purpose of this system of homomorphic encryption is to provide a simple, fast, and noiseless system which can be applied to any ring.

Addition of ciphertexts takes place in, asymptotically, the same time as the addition of plaintexts, and multiplication of ciphertexts takes place in the maximum of the asymptotic times for plaintext addition and multiplication. Moreover, multiplication by an unencrypted element is possible, taking the same asymptotic time as plaintext multiplication. Adding an unencrypted element is even easier, taking the same time as plaintext addition.

It is hoped that this system will provide an alternative to current models in cases where precision is necessary, the elements have unconventional addition or multiplication, or numerous computations are required.