# What to Expect When You're Taking the Expectation

Erin Hales & Tabitha Ogilvie
ISG, Royal Holloway University of London & Intel Labs

EPSRC
Engineering and Physical Sciences Research Council

## Why is noise important in FHE?

All LWE-based FHE ciphertexts have noise, which is essential for security. As we perform homomorphic operations, the noise associated with ciphertexts grows.

- ❑ Too much noise results in incorrect decryptions
- ❑ Some attacks and mitigations depend on the amount of noise that we have
- ❑ For libraries and implementations, we want to be able to automate noise management

If we wish to balance correctness, security and performance we must understand this noise growth.

Current noise analysis techniques for CKKS have problems with assumptions about independence and noise distributions, as well as difficulties in deciding where is best to measure the noise.

## Independence

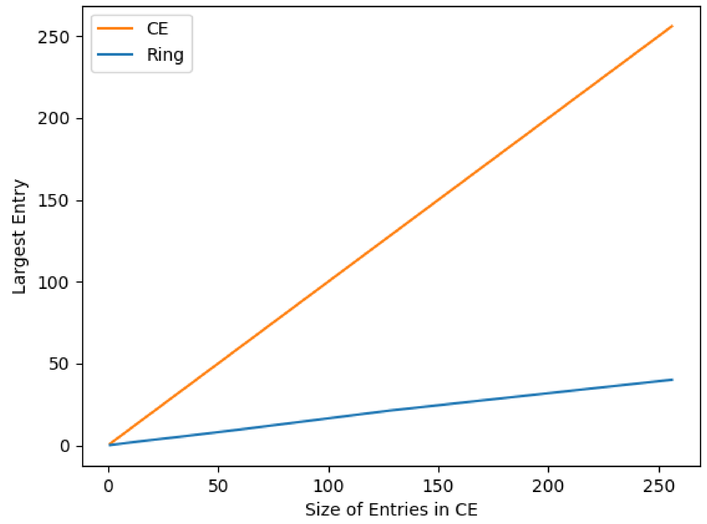
The standard method of analysing noise is to consider the variance of each term, or the term as a whole, and then bound this variance.
Formulae and techniques for doing so assume independence between the noise terms.
Consider the example of doubling a ciphertext, here noise will combine additively:

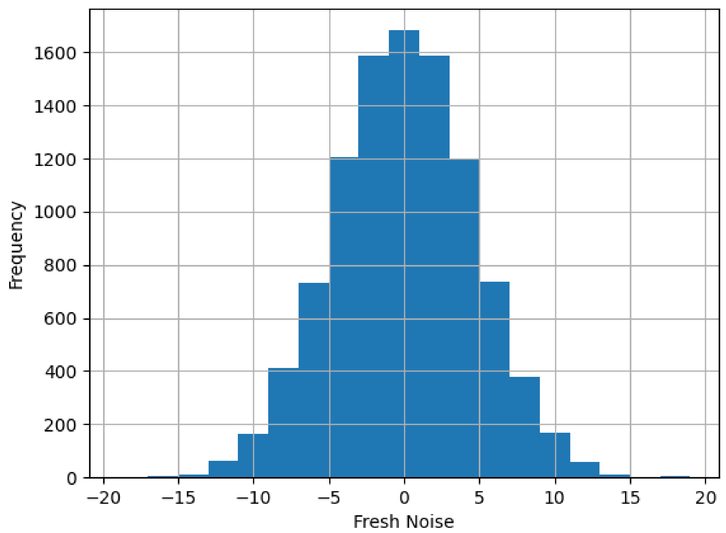
$$c,\ \text{ciphertext with associate noise } e \qquad \mathrm{Var}(2e) = 4\mathrm{Var}(e)$$
$$c_{\text{add}} = 2c,\ \text{ciphertext with associated noise } 2e \qquad \mathrm{Var}(2e) \neq \mathrm{Var}(e) + \mathrm{Var}(e)$$

Assuming independence in the terms of this equation can be problematic. When we consider the variance of terms resulting from operations combining different or even the same ciphertexts, the effects of this independence assumption compound.

## CE vs Ring

Here we compare the different ways we can think about measuring noise. Measuring using the Canonical Embedding norm and the Ring norm gives very different results.
This illustrates the heuristic to practical gap described in previous works.

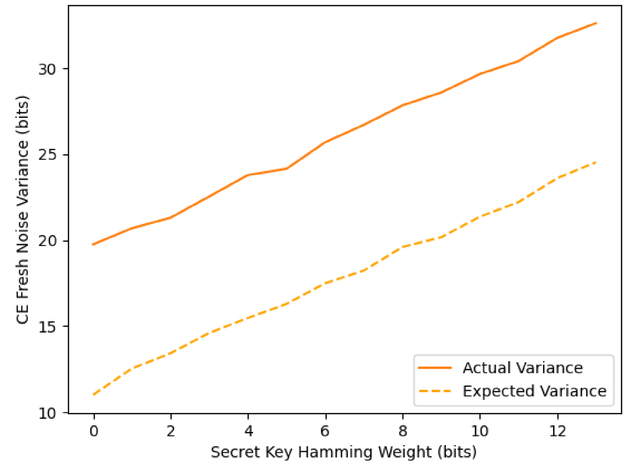



The noise of a fresh ciphertext is distributed normally. Even when we are analysing noise in the worst-case, the distribution of the noise is significant. In average case analyses, as is standard for TFHE, the distribution of noise is even more important.

## So how bad is this in the end?

The expected variance demonstrates the previous estimates of real variance in the Canonical Embedding. The variance we actually observe is far higher, demonstrating that previous estimates fail.




Experimental setup can make a huge difference to how the noise behaves, we need to be sensitive to this when modelling. Additionally, the assumptions that traditional noise analysis techniques make do not always hold.

## Application to other schemes

The issues we discuss here are not limited to CKKS. The independence assumption is of particular interest in noise analysis for TFHE.

## Contact Information

Email: erin.hales.2018@live.rhul.ac.uk
Tabitha.Ogilvie@intel.com

For more information about the graphs and to interact with us further, check out our site using the QR code

SCAN ME