On the precision loss in approximate homomorphic encryption

Anamaria Costache[1], Benjamin R. Curtis[2], Erin Hales[3], Sean Murphy[3], Tabitha Ogilvie[3], and Rachel Player[3]

[1] Norwegian University of Science and Technology (NTNU), Norway
anamaria.costache@ntnu.no
[2] Zama, Paris, France
ben.curtis@zama.ai
[3] Royal Holloway, University of London, UK
{erin.hales.2018}, {tabitha.ogilvie.2019} @live.rhul.ac.uk
{s.murphy}, {rachel.player} @rhul.ac.uk

Abstract. Since its introduction at Asiacrypt 2017, the CKKS approximate homomorphic encryption scheme has become one of the most widely used and implemented homomorphic encryption schemes. Due to the approximate nature of the scheme, application developers using CKKS must ensure that the evaluation output is within a tolerable error of the corresponding cleartext computation. This is achieved by scaling the underlying raw data by an appropriate amount, known as the *scale parameter*, in order to preserve a certain amount of significant figures. Unfortunately, there is no clear guidance available for choosing an appropriate scale parameter, with a trial-and-error approach typically advised. In this work, we significantly improve the state-of-affairs and present the following main contributions. We give a comprehensive theoretical and experimental analysis of CKKS noise, that considers noise coming from the encoding and homomorphic evaluation operations separately. This enables us to give the first explicit definition for precision in the CKKS context. Additionally, we demonstrate the applicability of our analysis to determine convergence properties of iterative algorithms that are commonly used in applications.