

Ludwig-Maximilians-Universität München

Prof. Dr. D. Kranzlmüller, Dr. N. gentschen Felde, Jan Schmidt

Data Science & Ethics

– *Microsoft SEAL* –

Exercise 1: *Game of Life*

Microsoft's *Simple Encrypted Arithmetic Library* (SEAL)¹ is a publicly available homomorphic encryption library. It can be found and downloaded at <http://sealcrypto.codeplex.com/>.

Implement the *Game of Life* using homomorphic encryption for any operation / calculation using the MS SEAL.

Note: Rules for *Game of Life*

- A dead cell having exactly three living neighbors will be newly born in the next round.
- A living cell with less than two living neighbors will die in the next round.
- A living cell with two or three living neighbors will survive the next round.
- Living cells with more than three living neighbors will die in the next round.
- Please note that any other cell is not alive

due date: 18.07.2019 (EOB)
no. of students: 2
deliverables: 1. Implementation (including source code(s))
2. Documentation (max. 10 pages)
3. Presentation (10 – max. 15 minutes)

¹<https://www.microsoft.com/en-us/research/publication/simple-encrypted-arithmetic-library-seal-v2-0/#>