Evaluation of the Complexity of Fully Homomorphic Encryption Schemes in Implementations of Programs

Chakarov, Dimitar (School: Model High School of Mathematics "Akademik Kiril Popov")

This paper shows a thorough examination of fully homomorphic encryption schemes and their performance in programs. We do an analysis of one specific, widely-used scheme – the Gentry-Sahai-Waters scheme. We statistically measure the time needed to perform a binary operation in two of the best fully homomorphic libraries – TFHE and FHEW. We aim to devise an abstraction level that enables us to assess the real-world speed performance of fully homomorphic operations without actually working with encrypted data. We propose an algorithm that uses the gathered statistical data combined with our mathematical model to evaluate the performance of fully homomorphic implementations of arbitrary computer programs. Also, we expand the set of supported binary operations to arithmetic ones. Finally, we perform several simulations to find how classical algorithms (searching and sorting) would perform if they were implemented fully homomorphically, so that we can show how our abstraction could be used in practice.

Awards Won:

Innopolis University : Full tuition scholarships for the Bachelor program in Computer Science