Спецсеминар для студентов 3 и 4 курсов, магистров, аспирантов «Теория управляющих систем и математические модели СБИС»

Руководители: *зав.каф., проф. Ложкин С.А., доц. Романов Д.С., доц. Шуплецов М.С., н.с. Данилов Б.Р.*

Проходит по пятницам с 17.30 до 19.00

На заседании семинара 4 марта 2022 года состоится доклад студента бакалавриата Демиденко Александра по статье **Benjamin Wesolowski, Ryan Williams Lower bounds for the depth of modular squaring // Cryptology ePrint Archive. – 2020**

Аннотация доклада.

В данной работе рассматриваются нижние оценки глубины схем из функциональных элементов для одной специальной функции, так называемой функции возведения в степень по модулю. Для заданного аргумента n-битного аргумента x, параметра T и n-битного модуля $m \in [2^{n-1}, 2^n - 1]$ данная функция вычисляет $x^{2^T} \bmod m$. Полученные в работе результаты используют классические результаты из теории чисел и теории схемной сложности, в том числе результаты Храпченко В.М.

Общая информация, темы спецсеминаров и аннотация доступны на сайте

http://mk.cs.msu.ru