Семинар “Индустриальная математика” факультета математики и компьютерных наук СПбГУ

Вторник, 9 июня 2020, 15:30 (Moscow time, GMT+3)
Zoom ID: 884-9095-2648, password: ind

Пост-квантовые криптосистемы на решетках и кодах

Елена Киршанова

(Балтийский Федеральный Университет им. И.Канта)

В своём докладе я расскажу о построении криптографических примитивов с открытым ключом, сложность которых основана на задачах в евклидовых решётках и в кодах. Мы сформулируем эти “трудные” задачи, рассмотрим существующие алгоритмы их решения и методы построения шифрования на примере кандидатов к стандартизации NIST (Национальное бюро стандартов США). Мы поговорим о том, как осуществляется криптоанализ систем на решётках и кодах, и сравним их производительность с существующими стандартами. В докладе я буду предполагать от слушателя базовые знания линейной алгебры, основы теории вероятности и теории сложности.

Приглашаются все желающие!