«Криптография на решётках» А. В. Устинов

Курс посвящён относительно новому направлению в криптографии — криптографии на решётках, которая известна также как постквантовая криптография. Как всегда, в основе криптографических протоколов лежит некоторая алгоритмически сложная задача. Здесь роль такой задачи выполняет задача о поиске кратчайшего вектора в решётке большой размерности. Все известные алгоритмы поиска короткого вектора имеют экспоненциальную (в зависимости от размерности) сложность. Поэтому, выбирая размерность достаточно большой (например, 1000), можно полагаться на стойкость криптосистем.

В первой части курса будет дано краткое введение в геометрию чисел. Будет рассказано о решётках и их основных свойствах. Затем мы с разных сторон посмотрим на задачу о поиске короткого вектора в данной решётке. В частности, мы изучим алгоритм Эрмита, который можно рассматривать как предварительную версию LLL-алгоритма.

Главная цель курса — познакомиться с LLL-алгоритмом — первым алгоритмом поиска короткого вектора, для которого удалось доказать полиномиальную сложность. Этот алгоритм позволил решать самые разнообразные задачи, но все его приложения останутся за границами курса.

В заключение мы познакомимся с тем, как устроены криптографические протоколы на решётках, и поймём, зачем вообще надо искать короткие векторы.

Программа курса

1. Решётки и их свойства. Матрица Грама.
2. Теорема Минковского о выпуклом теле. Процесс ортогонализации Грама — Шмидта. Укороченные базисы.
3. Минимумы Минковского. Константы Эрмита. Алгоритм Лагранжа построения приведённого базиса в двумерной решётке. Вычисление константы Эрмита в размерности 2. Неравенство Эрмита.
4. Алгоритмы Эрмита. LLL-приведённые базисы и их свойства. LLL-алгоритм.
5. Криптографические протоколы на решётках