18 октября 2013 года состоится доклад М.А.Черепнева

"Стойкость теоретико-числовых конструкций в системах защиты информации."

Аннотация.

В докладе будет сделан обзор результатов подготовленной автором докторской диссертации.

В работе, в частности, получены следующие результаты:

Доказана оценка сверху на сложность задачи дискретного логарифмирования через сложность

задачи Диффи-Хеллмана из которой, в частности следует, что эти задачи полиномиально

эквивалентны при условии ограниченности дерева Пратта, построенного для порядка рассматриваемой

группы. Получены новые оценки на количество и величину "первых" узлов дерева Пратта. Получена

новая оценка снизу для функции Эйлера. Доказана нестойкость схемы распределения ключей Сидельникова

в случае использования в ней группы матриц или образов эллиптических модулей (предложение

Панчишкина). Построен математический аппарат для электронного замка повышенной стойкости, доказана

единственность открывающей последовательности. Получены оценки снизу на число первообразных корней,

удовлетворяющих условию Бризолиса. Доказано, что при одном из двух возможных значений рода

гиперэллиптической кривой над полем характеристики два порядок ядра гомоморфизма спуска Вейля

не делится на два. Отсюда следует невырожденность спуска Вейля. Получен новый алгоритм решения

разреженных систем линейных уравнений над полем из двух элементов, доказана асимптотически лучшая

оценка времени его работы по сравнению с известным алгоритмом Видемана-Копперсмита.