Атака на ГОСТ Р 34.10-2001

М.А.Черепнёв

ГОСТ Р 34.10-2001 предлагает к использованию в схемах цифровой подписи и процедурах распределения ключей подгруппу простого порядка p на эллиптической кривой над некоторым простым полем $\mathbb{F}_r$ при соблюдении условия $ord^p r > 31$ (имеется ввиду порядок r по модулю p). Других ограничений на r и p, кроме требования их достаточно большой величины стандарт не накладывает. В докладе будет предложено несколько подходов, разработанных зарубежными математиками, а также автором доклада, к решению задачи дискретного логарифмирования и вскрытию протокола Диффи-Хеллмэна, использующих разложение $p-1$ на простые множители и малость величин $ord^p r, p-r$. Будет представлено несколько новых неравенств на сложность вскрытия рассматриваемых протоколов и решения некоторых теоретико-числовых задач.