УДК 004.056.55

О ВЫБОРЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ В КРИПТОГРАФИИ

Хуцаева А. Ф., Давыдов В. В. (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный̆ исследовательский̆ университет ИТМО»)

Научный̆ руководитель – преподаватель Давыдов В. В.
(Федеральное государственное автономное образовательное учреждение высшего образования «Национальный̆ исследовательский̆ университет ИТМО»)

Аннотация. Данная работа посвящена исследованию свойств эллиптических кривых, оценка которых используется для построения эффективных и защищённых криптографических схем. Проанализированы основные параметры, влияющие на выбор кривых.

Введение. На сегодняшний день эллиптические кривые являются одним из важных инструментов в криптографии. Используя кривые, можно строить как классические криптографические схемы, основанные на задаче дискретного логарифмирования в группе точек, так и постквантовые схемы, основанные на поиске пути в графе изогенных кривых. Вопрос построения криптосистем и протоколов, основанных на изогениях эллиптических кривых, на сегодняшний день является крайне актуальным из-за необходимости построения постквантовых систем ввиду угрозы появления полноценного квантового компьютера. Однако для того, чтобы построить надёжную и эффективную криптосистему, важно выбирать кривые с определёнными свойствами, например, с большим количеством точек и большим числом изогенных кривых.

Основная часть. В работе проанализирован выбор эллиптических кривых для криптографических схем.

Во-первых, предпочтительно использовать суперсингулярные эллиптические кривые. Это следует из того, что суперсингулярные графы изогений гораздо более связаны, чем графы регулярных кривых, и почти всегда являются графами Рамануджана, что делает их источником псевдослучайности. Суперсингулярные кривые уязвимы к MOV-атаке, однако, это никак не влияет на их применение в постквантовой криптографии, так как основной задачей является поиск пути в изогенном графе.

Во-вторых, при использовании кривых над конечным полем при решении задачи дискретного логарифмирования важно выбирать группы большого порядка, в качестве генератора группы лучше всего использовать точку, генерирующую все точки эллиптической кривой, таким образом максимально увеличивая порядок выбранной группы и сложность решения задачи дискретного логарифмирования для злоумышленника.

Говоря о конечных полях, важно отметить их роль в формировании кривых и скорости вычислений. Так, характеристика поля может определяться различными типами простых чисел, одними из таких являются простые числа Монтгомери (Montgomery-friendly) и псевдо-Мерсенна. В зависимости от выбранного представления простого числа на эллиптическую кривую накладывается ряд ограничений, а именно на коэффициенты, след Фробениуса, следовательно, и на порядок кривой. Данные условия в свою очередь влияют на количество изогений у кривой, что может ставить под вопрос безопасность применения таких кривых в постквантовых криптосистемах.

Выводы. Таким образом, основополагающими параметрами при выборе кривой являются характеристика поля, след Фробениуса и порядок группы точек. Соблюдение накладываемых ограничений на данные параметры крайне важно с практической точки зрения.

Хуцаева А. Ф. Подпись

Давыдов В. В. Подпись