XXXIII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V: С.136-137, 2005.

УДК 50.41.00, 50.37.23

А.Г.Столбунов (асп., каф. ИБКС), А.Г.Ростовцев, д.т.н., проф.

НОВЫЕ КРИПТОСИСТЕМЫ ДЛЯ ЗАЩИТЫ ОТ КВАНТОВЫХ АТАК

Современные криптосистемы с открытым ключом уязвимы для квантовых атак. В работе предложены алгоритмы шифрования с открытым ключом, обеспечивающие стойкость к квантовому взлому. Их безопасность основывается на задаче поиска изогении между эллиптическими кривыми. Криптосистемы на изогениях являются новым словом в криптографии.

Изогения – это алгебраическое отображение между эллиптическими кривыми. Н.Элкис предложил критерий для степени изогении, при котором каждая эллиптическая кривая имеет две изогенные с ней кривые.

В работе предложена структура звезды изогенных эллиптических кривых. Звезда – это граф, состоящий из простого числа изогенных эллиптических кривых, связанных изогениями степеней Элкиса. Пример звезды над полем F_{83} приведён на рис. 1, где в вершинах указаны j-инварианты изогенных эллиптических кривых.

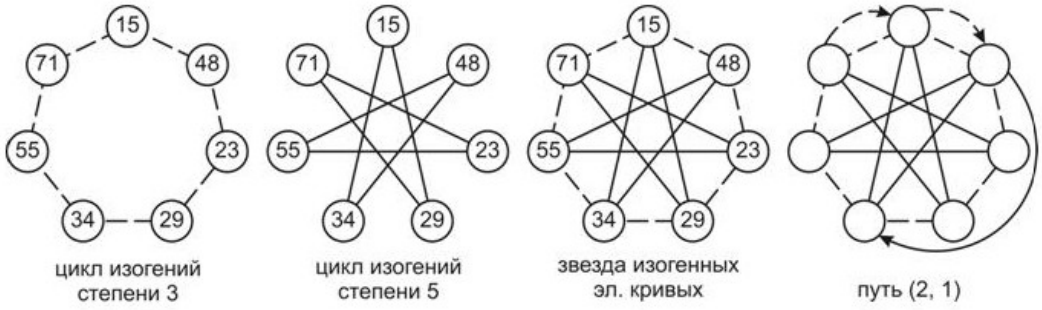

Рис. 1.

В работе предложен алгоритм определения направления в цикле изогенных эллиптических кривых. Способ задания направления основан на действии эндоморфизма Фробениуса на ядре изогении. Путь на звезде – это совокупность направленных изогений. Пример пути приведён на рисунке 1.

Шифрование с открытым ключом выполняется по схеме Эль-Гамаля (рис. 2).

Рис. 2.

Алгоритм 1: шифрование производится на основе j-инварианта секретной эллиптической кривой. Криптографическая стойкость основывается на задаче поиска любого из путей между двумя эллиптическими кривыми на звезде.

Алгоритм 2: изогениями отображается рациональная точка. Шифрование производится на основе координаты образа точки на секретной кривой. Криптографическая стойкость основывается на задаче поиска одного конкретного пути между двумя эллиптическими кривыми.

К преимуществам предложенных криптосистем можно отнести следующее:

1. Стойкость к взлому на квантовом компьютере. Для поиска пути на звезде требуется реализация вычисления пути. Вычисление пути длины n требует последовательного решения $O(n)$ уравнений, либо решения одного уравнения степени $O(\exp n)$. Квантовый компьютер не даёт преимуществ в решении этих задач. Количество необходимых ресурсов выражается экспонентой от размера задачи ($\log n$). На основании сказанного можно предположить, что поиск пути с использованием квантового компьютера обладает экспоненциальной сложностью.
2. Непригодность классических методов дискретного логарифмирования (Полларда, giant step – baby step, встречи на случайном дереве) для поиска пути на звезде.

В работе предложен метод генерации параметров для криптосистем. Работа криптоалгоритмов проверена на звезде из 55103 эллиптических кривых и 6 степеней изогений над полем $F_{2038074743}$.

Подбор параметров для криптосистем требует вычисления числа классов и обладает экспоненциальной сложностью. Данный факт пока затрудняет использование алгоритмов на практике.

Таким образом, настоящая работа выявила принципиальную возможность построения криптосистем на изогениях эллиптических кривых. Помимо шифрования с открытым ключом, на изогениях возможна реализация схем ЭЦП, установления сеансового ключа и других криптографических примитивов. Криптосистемы на изогениях обеспечивают стойкость к взлому на квантовом компьютере.