УДК 512.772

КРИПТОГРАФИЯ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ: РАСШИРЕНИЕ НА ЭЛЛИПС И КОНХОИДУ СЛЮЗА

ВладимироваЭ.В.
Академическая гимназия им. Д.К.Фаддеева Санкт-Петербургского государственного университета, г.Санкт-Петербург
Научный руководитель – к.ф.м-н. Г.М. Головачев,
преподаватель Академической гимназии им. Д.К.Фаддеева Санкт-Петербургского государственного университета, г.Санкт-Петербург

Сегодня наибольшую ценность представляет информация, а значит, требуется защита от доступа к ней лиц, не имеющих права на это. Современные методы шифрования и алгоритмы цифровой подписи построены на нескольких фактах алгебраической геометрии, в частности, на возможности сложения точек эллиптической кривой, представленной в форме Вейерштрасса. Возникает вопрос о том, можно ли получить аналогичный алгоритм на иной кривой.

В работе ответ на поставленный вопрос получен в результате изучения инверсии кривых второго порядка. Известно, что образами коник при инверсии являются кривые третьего или четвертого порядка. При инверсии рациональные точки кривых переходят в рациональные точки, и это означает, что между множествами рациональных точек прообраза и образа можно установить взаимно однозначное соответствие. Данные факты общеизвестны, однако в каждом конкретном примере "прообраз-образ" поиск такого соответствия является отдельной прикладной задачей. В работе получены формулы для преобразований координат, переводящих рациональные точки эллипса, гиперболы и параболы в рациональные точки образов, кривых третьего порядка, − конхоиды Слюза и циссоиды Диокла соответственно.

Обобщение полученных результатов на случай произвольного положения кривой второго порядка приводит к методу поиска рациональных точек на кривых четвертого порядка, являющиеся образами коник при инверсии. Это метод также позволяет решать соответствующие уравнения в рациональных числах.

На следующем этапе оказалось возможным перевести эллипс, а затем конхоиду Слюза, в рациональную кривую в форме Вейерштрасса. Показаны все необходимые преобразования и получены рациональные параметризации всех уравнений.

Практическое применение полученных результатов позволяет построить новый алгоритм шифрования. Структура такого алгоритма аналогична известному алгоритму эллиптической криптографии: имеются публичные и секретные ключи. Метод нового алгоритма основан на выборе секретного ключа, в качестве которого выступает уравнение исходного эллипса. Его образ – особая кривая третьего порядка в форме Вейерштрасса – является публичным ключом, поскольку обратное преобразование в эллипс неоднозначно. Шифрование на кривой сводится к изменению параметризации точек, двух известных и одной шифруемой. Только владелец уравнения эллипса сможет правильно определить значения рационального параметра и восстановить передаваемую точку кривой третьего порядка. Поэтому потенциальный злоумышленник, получивший доступ к публичным сведениям такого шифра, не сможет восстановить исходное положение передаваемой точки из-за неоднозначности выбора рационального параметра и образа эллипса.

Владимирова Э.В. (автор) 

Головачев Г.М. (научный руководитель)