УДК 514.18

ПРИМЕНЕНИЕ КРИВЫХ ЛИНИЙ И ПОВЕРХНОСТЕЙ В КРИПТОГРАФИИ

Лебедько А.С., аспирант[*],
Юрченко В.В., аспирант[*],
Кучеренко В.В. к.т.н.,
Найдыш А.В., д.т.н.
Мелитопольская школа прикладной геометрии,
Мелитопольский педагогический университет
им. Богдана Хмельницкого (Украина)

В статье рассматриваются возможности применения кривых линий и поверхностей, определённых в точечном БН-исчислении, в решении задач криптографического характера.

Ключевые слова: эллиптическая кривая, криптостойкость, криптография, поверхность, точечное исчисление Балюбы-Найдыша (БН-исчисление).

Постановка проблемы. Проблема защиты данных от взлома становится всё острее с каждым годом. Это обусловлено появлением новых алгоритмов криптоанализа и увеличением вычислительных мощностей современных компьютеров, что позволяется успешно использовать даже простые алгоритмы перебора для объектов, обладающих низким уровнем защиты. И хотя большинство случаев взлома данных связаны с «дырами» в системах защиты, а не со взломом самого шифра или подбором пароля, оставлять без внимания модернизацию шифрования данных просто невозможно, тем более, что в современном мире процесс взлома и похищения данных превращён в высоко прибыльный бизнес, а количество хакерских атак растёт с лавинообразной скоростью.

Анализ последних исследований и публикаций. В работах [1,2], а также в работах многих других авторов описано применение эллиптических кривых на конечных полях для шифрования данных. Краткий анализ преимуществ и недостатков этого метода шифрования был проведён в работе [3]. Общие преимущества методов, основанных на эллиптических кривых, в сравнении с криптографическими алгоритмами с открытым ключом, основанных на проблеме факторизации больших чисел (RSA) и дискретного логарифмирования

[*] Научный руководитель – д.т.н., проф. Найдыш А.В.

(Эль-Гамаль) и широко использующихся на практике, сводятся к получению такого же уровня криптостойкости с более короткой длиной ключа. Проблемы использования эллиптических алгоритмов сводятся, скорее, к чисто техническим аспектам, под которыми подразумевается отказ некоторых организаций переходить на новые протоколы шифрования, а также сертифицировать эллиптическую криптографию.

В работе [4], а также других работах этих авторов, предлагается модернизировать эллиптическое шифрование путём применения кривых Эдвардса, а также кривых в форме Вейерштрасса.

Формулирование целей статьи. Провести анализ возможностей получения новых способов шифрования данных, основанных на геометрических алгоритмах с применением точечного БН-исчисления.

Основная часть. Как отмечается во многих современных источниках, с каждым новым скачком человечества в области развития компьютерной техники и, как следствие, увеличения вычислительных мощностей, растут возможности в использовании всё новых математических алгоритмов для взлома и похищения защищённых данных.

Последнее десятилетие активно развиваются и внедряются в защитные системы алгоритмы шифрования данных на основе эллиптических кривых. Этот способ не лишён недостатков, но, тем не менее, является хорошей альтернативой алгоритмам, применяемым в настоящее время в подавляющем большинстве компьютерных систем.

Основой алгоритма шифрования на базе эллиптической кривой является однопараметрическая зависимость – точка, которая принадлежит кривой. Рассмотрим общий алгоритм шифрования для отдельного блока [5]:

1. Определяется десятичное значение блока (буквы) t.
2. Выбирается случайное число k ($0<k<n$).
3. Определяется точка $P_k(x_{Pk}, y_{Pk}) = k * P$.
4. Определяется точка $Q_k(x_{Qk}, y_{Qk}) = k * Q$.
5. Вычисляется $c = (t * x_{Pk}) \bmod n$.
6. Получаем шифрограмму – пара $[P_k, c]$.

Таким образом, шифрование на базе эллиптической кривой является вариацией шифрования Эль-Гамаля. Если стойкость алгоритма шифрования Эль-Гамаля базируется на сложности решения задачи дискретного логарифмирования, то стойкость шифрования с помощью эллиптических кривых базируется на сложности нахождения множителя k точки P по их произведению. Т.е. если

$Q = k * P$, то зная P и k довольно легко вычислить Q. Эффективное решение обратной задачи – найти k при известных P и Q, на текущий момент пока не опубликовано.

Суть предстоящей работы состоит в модернизации эллиптического способа шифрования при помощи точечного БН-исчисления [3] и предложении новых способов, основанных на использовании геометрических алгоритмов.

Известно, что любая кривая, включая эллиптические, является однопараметрическим множеством точек. Любая поверхность, в свою очередь, является однопараметрическим множеством прямых или кривых линий. Таким образом, поверхность можно рассматривать как двухпараметрическое множество точек или как многопараметрическое для поверхностей в пространствах с размерностью больше 3-х.

Указанное свойство поверхности, по нашему мнению, уместно использовать для шифрования пары «логин / пароль» (по количеству рабочих параметров). Совокупно наличие двух параметров, имеющих конечную длину, а также существование огромного количества всевозможных поверхностей, при наличии даже средне сложного алгоритма шифрования, обеспечат достаточно высокую криптостойкость такого способа защиты информации.

В теории аппарата точечного БН-исчисления, на данный момент, разработано значительное количество геометрического представления поверхностей с различными напередзадаваемыми свойствами, но, на наш взгляд, наиболее уместным является использование способа «Лупа», представленного в работе [6]. Данный способ примечателен тем, что поверхность разделяется на прямолинейные сегменты с равномерным или неравномерным шагом, или криволинейные сегменты с неравномерным шагом, который изменяется в пределах одной из направляющих. При этом, количество ячеек, которые будут входить в состав сегмента, на который наведено лупу, будет зависеть от порядка кривых, которые ограничивают данный сегмент. Опорными точками для способа будут выступать численные значения шифруемой пары «логин / пароль».

Выводы. В статье рассмотрены аспекты шифрования на базе эллиптической кривой с точки зрения прикладной геометрии и предложен способ повышения криптостойкости данных за счет использования плоскости как базового объекта для шифрования, что позволит повысить надежность информации.

Литература

1. Эксперты призывают готовиться к криптоапокалипсису [Електронний ресурс]. – Режим доступу: URL: http://habrahabr.ru/

post/188846/.
2. Элементарное введение в эллиптическую криптографию / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских. – М.: КомКнига, 2006. – 608 с.
3. Лебідько О.С. Використання скручених кривих едвардса у криптографії / О. С. Лебідько, В. О. Лебедєв // Збірник тез доповідей XI Міжнародної науково-практичної конференції «Обухівські читання» (1-го березня 2016 року) / Національний університет біоресурсів і природокористування України. – К., 2016. – 24-25 с.
4. Бессалов А.В. Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем / А.В. Бессалов, А.А. Дихтенко, Д.Б. Третьяков // Сучасний захист інформації. – №4. – 2011. – С. 33–36.
5. Криптографические методы защиты информации [Електронний ресурс]. – Режим доступу: URL: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema8.
6. Кучеренко В. В. Формалізовані геометричні моделі нерегулярної поверхні для гіперкількісної дискретної скінченої множини точок : дис... канд. техн. наук: 05.01.01 / В. В. Кучеренко . – Мелітополь: ТДАТУ, 2013. – 208 с.

ЗАСТОСУВАННЯ КРИВИХ ЛІНІЙ ТА ПОВЕРХОНЬ У КРИПТОГРАФІЇ

Лебідько О.С., Юрченко В.В., Кучеренко В.В., Найдиш А.В.

У статті розглядаються можливості застосування кривих ліній та поверхонь, що задані у точковому БН-численні, для розв'язку задач криптографічного характеру.

Ключові слова: еліптична крива, криптостійкість, криптографія, поверхня, точкове числення Балюби-Найдиша.

USING OF CURVES AND SURFACES IN CRYPTOGRAPHY

A. Lebedko, V. Urchenko, V. Kycherenko, A. Naydish

In the article describes the use of curves and surfaces defined in BN-calculus in the solution of problems of a cryptographic nature.

Keywords: elliptic curve crypto, cryptography, surface-point calculus Balyuby Naydysha.