Аналог RSA-криптосистемы в квадратичных Евклидовых кольцах

Кондратенок Никита Васильевич, Беларусь, г.Минск, Гимназия 41 им.В.Х.Серебряного, 11"В" класс

Научный руководитель: Васьковский Максим Михайлович, кандидат физ.-мат. наук, доцент, доцент кафедры высшей математики БГУ

В феврале 1978 года в журнале "Communications of the ACM" было впервые опубликовано полное описание RSA-криптосистемы [6]. С 1982 года алгоритм начал активно использоваться в зарождающейся сети Internet. В ноябре 1993 года опубликована статья, описывающая применение RSA для шифрования и создания электронной подписи.

В данной работе будет рассмотрен аналог RSA-криптосистемы, используемой как для шифрования, так и для электронной подписи. Отличие криптосистемы, описанной в данной работе, от классической в том, что числа p и q выбираются из произвольного квадратического Евклидового кольца, а не из целых чисел.

Так же в работе рассмотрены ограничения на p и q, которые возникают из различных алгоритмов факторизации, таких как $(p-1)$ -метод Полларда и метод Ферма [3]. А также из алгоритма дешифрования с помощью метода повторного шифрования [4].

Основной частью RSA-криптосистемы является вычисление публичного ключа, которое производится с помощью алгоритма Евклида. В статье Роллетсчека [7] доказано, что алгоритм Евклида с выбором минимального по норме остатка имеет наименьшую длину во всех квадратичных Евклидовых кольцах, кроме $Z[\sqrt{11}]$. В статье авторов [2] аналогичное утверждение рассмотрено в более общем классе колец. Так же авторами в статье [5] доказано, что алгоритм Евклида имеет логарифмическую сложность в квадратичных Евклидовых кольцах. Следовательно, поиск публичного ключа будет иметь такую же сложность, как и для целых чисел.

В работе получены результаты, которые позволили оценить возможность использования RSA-криптосистемы для квадратичных Евклидовых колец. Доказано, что в этом случае, даже с учетом ограничений, перспективы использования такой криптосистемы значительно шире, чем у существующей. Направлением дальнейших исследований представляется целесообразным назвать детальный сравнительный анализ криптостойкости существующих систем и предлагаемого аналога. Рассматривается возможность применения полученных результатов в областях, требующих использования цифровой подписи.

[1] Базылев Д.Ф., Васьковский М.М., Матвеев Г.В., Размыслович Г.П. Сборник задач по прикладной алгебре. – Минск: БГУ, 2011.

[2] Васьковский М.М., Кондратенок Н.В. Конечные обобщенные цепные дроби в Евклидовых кольцах // Вестник БГУ. Серия 1. Физика. Математика. Информатика. – №3. – 2013. – С. 117-123.

[3] Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. – СПб.: Лань, 2011.

[4] Харин Ю.С., Агиевич С.В., Васильев Д.В., Матвеев Г.В. Криптология. – Минск: БГУ, 2013.

[5] M.Vaskouski, N.Kondratyonok. Shortest division chains in unique factorization domains // Symbolic Computation.(appear in print)

[6] R.L.Rivest, A.Shamir, L.Adleman. A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. – New York, NY, USA: ACM, 1978, p. 120-126.

[7] H.Rolletschek. Shortest division chains in imaginary quadratic number fields // Symbolic Computation, 1990, p. 321-354.

[8] J.L. Selfridge, C.B. Lacampagne, R.B. Eggleton. Euclidean quadratic fields // Amer. Math. Monthly, 99, 1992, p. 829-837.