ПРИМЕНЕНИЕ КВАЗИГРУПП ДЛЯ ПОТОКОВОГО ШИФРОВАНИЯ

Пихтильков С.А., Кальдяева Н.В.
Оренбургский государственный университет, г. Оренбург

В 20-30-е годы XX века стали интенсивно изучаться неассоциативные алгебраические структуры. Эти исследования привели к созданию теории квазигрупп [5, 6]. Квазигруппы находят разнообразные приложения в дифференциальной геометрии, теории автоматов, физике, криптографии и т.д. Также интерес к квазигруппам обусловлен применением их в криптографии. В данной статье рассмотрено построение поточного квазигруппового шифра, криптографическая стойкость которого основана на сложности решения таких задач, как факторизация целых чисел или дискретное логарифмирование в конечных полях.

В работах [1, 2, 3] был предложен подход использования квазигрупп для потокового шифрования. По заданной квазигруппе (Q, *) и любому элементу (лидеру) *a* определяется преобразование $E_{\alpha}^{(1)}$ множества Q^{+}:

$$E_{\alpha}^{(1)}(x_1, \dots, x_k) = (y_1, \dots, y_k), \quad (1)$$

где $y_1 = a * x_1$, $y_i = y_i * x_{i+1}$, $i = 1, \dots, k-1$. Композиция из n таких преобразований, соответствует квазигруппам (Q, $*_i$) и выбранным элементам a_i, $i = 1, \dots, n$. Полученное преобразование обозначается $E_{a_n, \dots, a_1}^{(n)}$. Преобразование $E_a^{(1)}$ обратимо, и обратное преобразование определяется так:

$$D_a^{(1)}(y_1, \dots, y_k) = (x_1, \dots, x_k), \quad (2)$$

где $x_1 = a \backslash y_1$, $x_{i+1} = y_i \backslash y_{i+1}$, $i = 1, \dots, k-1$. Тогда можно найти обратное преобразование для $E_{a_n, \dots, a_1}^{(n)}$, которое обозначается $D_{a_1, \dots, a_n}^{(n)}$. Для шифрования информации используют преобразование $E_{a_n, \dots, a_1}^{(n)}$, в качестве ключей берут операции $*_i$. В работах [2, 3] показано, что преобразования $E_{a_n, \dots, a_1}^{(n)}$ и $D_{a_1, \dots, a_n}^{(n)}$ обладают некоторыми нужными криптографическими качествами.

В ряде работ квазигрупповые преобразования слов используются для построения поточных шифров. Рассмотрим один из таких шифров, рассмотренный в работе [4]. Данный шифр получается путем комбинирования шифра типа Эль-Гамаля и поточного квазигруппового шифра.

Описание шифра.

В качестве поточного квазигруппового шифра берется шифр в алфавите $Q = Z_p^*$ с функциями шифрования $E_{a_n, \dots, a_1}^{(n)}$ и расшифрования $D_{a_1, \dots, a_n}^{(n)}$ из [2, 3], который обозначается E_{α} и E_{α}^{-1} при $\alpha = (a_1, \dots, a_n)$. При этом предполагается, что они определены для случая, когда все квазигруппы $(Q, *_i)$ совпадают с одной и той же квазигруппой $(Q, *)$.

В работе [4] квазигрупповая операция * на *Q* определятся следующим

образом.

Для произвольного $K \in \{1, \dots, p-2\}$ задается отображение $f_K : Q \to Q$ по формуле

$$f_K(i) = \frac{1}{1+(K+j)(mod\, p-1)} (mod\, p) \quad (3)$$

и полагается

$$i * j = i \cdot \mathrm{f_K}(j) (\mathrm{mod\ p}).$$

Отображение f_K является подстановкой, а группоид *(Q, *)* – квазигруппой с левой обратной операцией

$$i \backslash j = \left(i \cdot j^{-1} (\mathrm{mod}\, p)\right) - 1 - K) (\mathrm{mod}\, p-1) \quad (4)$$

при условии, что вместо 0 берется $p-1$.

В алгоритме установление связи, выработка и передача ключей осуществляется с помощью шифра Эль-Гамаля, а шифрование исходного открытого сообщения и его расшифровывание – с помощью квазигруппового шифра. В итоге получается существенный выигрыш в скорости по сравнению с известными ассиметричными шифрами.

Авторами разработана программа для потокового шифрования с использованием квазигрупп.

В качестве простого числа было выбрано число *p*=257.

Ключами $a_i,\ i = 1, \dots, 5$ могут быть выбраны любые натуральные числа от 1 до 255.

Пример работы программы.

При выбранных ключах 234, 13, 198, 84, 255 кодируется слово «криптография».

Передается сообщение (65, 22, 104, 47, 229, 133, 108, 5, 255, 7, 80, 40), которое затем декодируется в исходное слово.

В статье рассмотрен шифр, предложенный в статье [4] и приведен пример. Также следует отметить, что в настоящее время данному вопросу уделяется внимание. Этому свидетельствуют разработки новых шифров и появлению обзоров [1, 7].

Список литературы

1. *Глухов. М.М. О применениях квазигрупп в криптографии// Глухов М.М. - М.: Прикладная дискретная математика, 2008, № 2, 28 – 32.*
2. *Markovski S., Gligoroski D., Bakeva V. Quasigroup String Processing: Part 1 // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci. XX. 1 – 2.- 1999.- P. 13 – 28.*
3. *Markovski S., Kusacatov V. Quasigroup String Processing: Part 2 // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci. XXI. 1 – 2. - 2000.- P. 15 – 32.*
4. *Gligoroski D. Stream cipher based on quasigroup string transformation in $\mathbf{Z}_p^*$// Universitet "St. Cyril and Methodious", Faculty of Natural Sciences, Institute*

of Informatics, P.O. Box 162, Scopje, Republic of Macedonia. ArXiv:cs.CR/0403043 V2 22 Apr 2004.

5. Moufang R. Zur Struktur von Alternativkoerpern // Math. Ann. 1935. V. 110. №. 1. P.416-430.

6. Белоусов В.Д. Основы теории квазигрупп и луп. М.: Наука, 1967, 223 с.

Shcherbacov V. A. Quasigroups in cryptology // Comput. Sci. J. Moldova. 2009. V. 17. No. 2(50). P. 193–228.