Значения Num_Trans, Num_Best являются параметрами алгоритма. Вычислительные эксперименты показали, что при $Num\_Best = 10$, $Num\_Trans = 500$ на первой итерации и $Num\_Trans = 100$ на последующих за приемлемое число итераций можно получить 8-битовые подстановки с характеристиками (3) и алгебраической степенью 7.

Наиболее трудоёмким этапом алгоритма является вычисление ℓ_F, δ_F, линейного и разностного спектров. С целью оптимизации этих вычислений теория из работы [9] применена для определения ячеек в DDT и LAT, в которых возникают изменения значений при умножении на транспозицию только 4-битовой подстановки $\widehat{\pi}_1$ или $\widehat{\pi}_2$. Асимптотические оценки трудоёмкости нахождения разностного спектра, дифференциальной равномерности, линейного спектра и линейности совпадают с приведёнными в [9]. Так, алгоритм вычисления разностного спектра и показателя дифференциальной равномерности примерно в 2^{2m} раз быстрее по сравнению с алгоритмом их вычисления для произвольной подстановки, а трудоёмкость алгоритма пересчёта линейного спектра и линейности примерно в $2m$ раз меньше трудоёмкости их нахождения для произвольной подстановки. По сравнению с [9] при вычислении криптографических характеристик можно получить выигрыш по памяти за счёт уменьшения числа хранимых ячеек в DDT и LAT в силу особенностей обобщённой конструкции.

ЛИТЕРАТУРА

1. *Menyachikhin A. V.* Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters // Матем. вопр. криптогр. 2017. Т. 8. Вып. 2. С. 97–116.
2. *Фомин Д. Б.* О подходах к построению низкоресурсных нелинейных преобразований // Обозрение прикладной и промышленной математики. 2018. Т. 25. Вып. 4. С. 379–381.
3. *Фомин Д. Б.* Об алгебраической степени и дифференциальной равномерности подстановок пространства V_{2m}, построенных с использованием $(2m, m)$-функций // Матем. вопр. криптогр. 2020. Т. 11. № 4. С. 133–149.
4. *Кострикин А. И.* Введение в алгебру. Ч. I. Основы алгебры: учебник для вузов. 3-е изд. М.: Физматлит, 2004. 272 с.
5. *O'Connor L.* Properties of linear approximation tables // LNCS. 1995. V. 1008. P. 131–136.
6. *Biryukov A., Perrin L., and Udovenko A.* Reverse-engineering the s-box of Streebog, Kuznyechik and STRIBOBr1 // LNCS. 2016. V. 9665. P. 372–402.
7. *Browning K. A., Dillon J. F., McQuistan M. T., and Wolfe A. J.* An APN permutation in dimension six // 9th Int. Conf. Finite Fields Appl. 2009. Contemp. Math. 2010. V. 518. P. 33–42.
8. *Canteaut A. and Perrin L.* On CCZ-Equivalence, Extended-Affine Equivalence, and Function Twisting. Cryptology ePrint Archive, Report 2018/713. `https://eprint.iacr.org/2018/713`.
9. *Menyachikhin A. V.* The change in linear and differential characteristics of substitution after the multiplication by transposition // Матем. вопр. криптогр. 2020. Т. 11. № 2. С. 111–123.

УДК 519.688 DOI 10.17223/2226308X/14/43

О НЕКОТОРЫХ ПОДГРУППАХ БЕРНСАЙДОВОЙ ГРУППЫ $B_0(2,5)$

А. А. Кузнецов, А. С. Кузнецова

Пусть $B_0(2,5) = \langle x, y\rangle$ — наибольшая конечная двупорождённая бернсайдова группа периода 5, порядок которой равен 5^{34}. В работе изучена серия подгрупп $H_i = \langle a_i, b_i\rangle$ группы $B_0(2,5)$, где $a_0 = x$, $b_0 = y$, $a_i = a_{i-1}b_{i-1}$ и $b_i = b_{i-1}a_{i-1}$

для $i \in \mathbb{N}$. Получено, что группа H_4 является абелевой, поэтому H_5 — циклическая группа, и серия подгрупп прерывается. Показано, что элементы $a_4 = xy^2xyx^2y^2x^2yxy^2x$ и $b_4 = yx^2yxy^2x^2y^2xyx^2y$ длины 16 порождают в $B_0(2,5)$ абелеву подгруппу порядка 25, и никакие другие два групповых слова, длины которых меньше 16, не порождают нециклическую абелеву подгруппу в $B_0(2,5)$.

Ключевые слова: *некоммутативная криптография, группа Бернсайда.*

Наиболее распространённые в настоящее время криптографические алгоритмы, такие, как RSA, Диффи — Хеллмана, на эллиптических кривых и др., зависят от структуры коммутативных групп и связаны со сложностью решения задачи факторизации целых чисел и дискретного логарифмирования. Однако в 1994 г. П. Шор представил квантовый алгоритм полиномиальной сложности, решающий эти проблемы [1]. Данный факт побудил исследователей к поиску альтернативных методов построения криптосистем. В последние два десятилетия были разработаны новые криптосистемы и протоколы обмена ключами, основанные на различных некоммутативных алгебраических системах (группы кос, полициклические группы, линейные группы и др.).

Пусть $B(m,n) = \langle x_1, \ldots, x_m \rangle$ — свободная бернсайдова группа периода n, в которой для любого элемента группы g выполняется тождество $g^n = 1$. В работах [2–4] в качестве криптографических примитивов предложено использовать бернсайдовы группы периода $n = 3$. Для $n > 3$ вопрос пока не рассматривался. Заметим, что, помимо прикладного интереса, изучение бернсайдовых групп имеет большое значение и для алгебры, поскольку там до сих пор остаётся ряд нерешённых проблем. Например, неизвестно, конечна ли группа $B(2,5)$.

Пусть $B_0(2,5) = \langle x, y \rangle$ — наибольшая конечная двупорождённая бернсайдова группа периода 5, порядок которой равен 5^{34} [5]. Если группа $B(2,5)$ конечна, то $B_0(2,5) = B(2,5)$.

Рассмотрим подгруппы H_i группы $B_0(2,5)$ следующего вида:

$$H_i = \langle a_i, b_i \rangle,$$

где $a_0 = x$, $b_0 = y$, $a_i = a_{i-1}b_{i-1}$ и $b_i = b_{i-1}a_{i-1}$ для $i \in \mathbb{N}$.

Обозначим N_i и E_i — класс нильпотентности и энгелев индекс подгруппы H_i соответственно. В таблице представлены свойства групп H_i, полученные при помощи компьютерных вычислений.

i	a_i, b_i	$\lvert H_i \rvert$	N_i	E_i	H_i абелева?
1	xy, yx	5^{14}	6	5	Нет
2	xy^2x, yx^2y	5^6	4	4	Нет
3	xy^2xyx^2y, yx^2yxy^2x	5^3	2	2	Нет
4	$xy^2xyx^2y^2x^2yxy^2x$, $yx^2yxy^2x^2y^2xyx^2y$	5^2	1	1	Да

Заметим, что группа H_1 уже изучена ранее [6].

Поскольку группа H_4 является абелевой, то H_5 — циклическая группа порядка 5, и серия подгрупп прерывается.

В качестве примера далее представлено коммутаторное представление (power commutator presentation) подгруппы $H_2 = \langle a_2, b_2 \rangle = \langle xy^2x, yx^2y \rangle$.

Для каждого элемента данной группы H_2 существует уникальное коммутаторное представление вида $c_1^{\alpha_1} \ldots c_6^{\alpha_6}$, где $\alpha_i \in \mathbb{Z}_5$, $i = 1, 2, \ldots, 6$. Здесь $c_1 = a_2$ и $c_2 = b_2$ — порождающие элементы H_2; c_3, c_4, c_5, c_6 — коммутаторы, которые вычисляются рекурсивно через c_1 и c_2:

$c_i^5 = 1$ $(1 \leqslant i \leqslant 6)$, $[c_2, c_1] = c_3$, $[c_3, c_1] = c_4$, $[c_3, c_2] = c_5$, $[c_4, c_1] = c_6$,
$[c_4, c_2] = 1$, $[c_4, c_3] = 1$, $[c_5, c_1] = 1$, $[c_5, c_2] = c_6^4$, $[c_5, c_3] = 1$, $[c_5, c_4] = 1$,
$[c_6, c_1] = 1$, $[c_6, c_2] = 1$, $[c_6, c_3] = 1$, $[c_6, c_4] = 1$, $[c_6, c_5] = 1$.

Для быстрого умножения элементов на основе алгоритма из [7] вычислены полиномы Холла группы H_2.

Пусть $c_1^{\alpha_1} \dots c_6^{\alpha_6}$ и $c_1^{\beta_1} \dots c_6^{\beta_6}$ — два произвольных элемента из H_2. Тогда

$$c_1^{\alpha_1} \dots c_6^{\alpha_6} \cdot c_1^{\beta_1} \dots c_6^{\beta_6} = c_1^{\gamma_1} \dots c_6^{\gamma_6}, \quad \alpha_i, \beta_i, \gamma_i \in \mathbb{Z}_5,$$

где
$\gamma_1 = \alpha_1 + \beta_1$,
$\gamma_2 = \alpha_2 + \beta_2$,
$\gamma_3 = \alpha_3 + \beta_3 + \alpha_2\beta_1$,
$\gamma_4 = \alpha_4 + \beta_4 + \binom{\beta_1}{2}\alpha_2 + \alpha_3\beta_1$,
$\gamma_5 = \alpha_5 + \beta_5 + \binom{\alpha_2}{2}\beta_1 + \alpha_3\beta_2 + \alpha_2\beta_1\beta_2$,
$\gamma_6 = \alpha_6 + \beta_6 + \binom{\beta_1}{2}\alpha_3 + \binom{\beta_1}{3}\alpha_2 + 4\binom{\alpha_2}{3}\beta_1 + 4\binom{\beta_2}{2}\alpha_3 + \alpha_4\beta_1 + 4\alpha_5\beta_2 + 4\binom{\alpha_2}{2}\beta_1\beta_2 +$
$+ 4\binom{\beta_2}{2}\alpha_2\beta_1$.

Заслуживает внимания также тот факт, что элементы

$$a_4 = xy^2xyx^2y^2x^2yxy^2x, \quad b_4 = yx^2yxy^2x^2y^2xyx^2y$$

порождают в $B_0(2,5)$ абелеву подгруппу порядка 25. Длина каждого из этих элементов равна 16. При помощи компьютерных вычислений проведена проверка, которая показала, что никакие другие два групповых слова, длины которых меньше 16, не порождают нециклическую абелеву подгруппу в $B_0(2,5)$.

ЛИТЕРАТУРА

1. *Shor P.* Algorithms for quantum computation: Discrete logarithms and factoring // Proc. 35th Ann. Symp. Foundations Comput. Sci. 1994. P. 124–134.
2. *Baumslag G., Fazio N., Nicolosi A. R., et al.* Generalized learning problems and applications to non-commutative cryptography // LNCS. 2011. V. 6980. P. 324—339.
3. *Fazio N., Iga K., Nicolosi A. R., et al.* Hardness of learning problems over Burnside groups of exponent 3 // Designs, Codes Cryptogr. 2015. V. 75(1). P. 59—70.
4. *Kahrobaei D. and Noce M.* Algorithmic problems in Engel groups and cryptographic applications // Intern. J. Group Theory. 2020. V. 9(4). P. 231—250.
5. *Havas G., Wall G., and Wamsley J.* The two generator restricted Burnside group of exponent five // Bull. Austral. Math. Soc. 1974. No. 10. P. 459—470.
6. *Кузнецов А. А.* Об одной подгруппе бернсайдовой групы $B_0(2,5)$ // Тр. Института математики и механики УрО РАН. 2011. Т. 17. № 4. С. 176–180.
7. *Кузнецов А. А., Кузнецова А. С.* Быстрое умножение элементов в конечных двупорождённых группах периода пять // Прикладная дискретная математика. 2013. № 1(19). С. 110–116.