2) если $p \equiv 5 \pmod 8$ и $r = \binom{(p-1)/2}{(p-1)/4}$, то при $r \not\equiv 0 \pmod p$ кривая имеет p-ранг 1. В этом случае многочлен Фробениуса по модулю p равен

$$\chi(\lambda) \equiv \lambda^{2g} + r\lambda^{2g-1} \pmod p.$$

Теорема 7. Пусть группа автоморфизмов G кривой C равна $D_8 \times C_2$. Тогда кривая имеет модель $y^2 = x^8 + \alpha x^4 + 1$, где $\alpha \in K$. Пусть $a = P_{(p-1)/4}(\rho)$, $b = P_{(p-3)/4}(\rho)$, $c = P_{(p-1)/2}(\rho)$, где $\rho = -\alpha/2$. Тогда

1) если $p \equiv 1 \pmod 4$, то p-ранг кривой равен 1 при $a \equiv 0$, $c \not\equiv 0 \pmod p$. В этом случае многочлен Фробениуса по модулю p равен

$$\chi(\lambda) \equiv \lambda^{2g} + c\lambda^{2g-1} \pmod p;$$

2) если $p \equiv 3 \pmod 4$, то p-ранг кривой равен 1 при $b \equiv 0$, $c \not\equiv 0 \pmod p$. В этом случае многочлен Фробениуса по модулю p равен

$$\chi(\lambda) \equiv \lambda^{2g} + c\lambda^{2g-1} \pmod p.$$

Заключение

В работе получены характеристические многочлены $\pmod p$ гиперэллиптических кривых рода $2, 3$ и p-ранга 1 для кривых с автоморфизмами.

В дальнейшем на основе полученных результатов планируется построить алгоритм подсчёта числа точек на кривых, изоморфных кривым с автоморфизмами над расширением конечного поля, по аналогии с работой [5] и исследовать их степени вложения с целью анализа возможности применения таких кривых как в классических криптосистемах, так и в криптосистемах на основе билинейных спариваний и изогений.

ЛИТЕРАТУРА

1. *Singh V., Zatysev A., and McGuire G.* On the Characteristic Polynomial of Frobenius of Supersingular Abelian Varieties of Dimension up to 7 over Finite Fields. arXiv preprint arXiv:1011.2257. 2010.
2. *Novoselov S. A.* Hyperelliptic curves, Cartier — Manin matrices and Legendre polynomials // Прикладная дискретная математика. 2017. № 37. С. 20–31.
3. *Мельничук Е. М., Новоселов С. А.* p-Ранги гиперэллиптических кривых рода 3 с нетривиальной группой автоморфизмов // Труды математического центра имени Н. И. Лобачевского. 2018. Т. 56. С. 188–192.
4. *Bouw I. I., Diem C., and Scholten J.* Ordinary elliptic curves of high rank over with constant j-invariant // Manuscripta Mathematica. 2004. V. 114. No. 4. P. 487–501.
5. *Novoselov S. A.* Counting points on hyperelliptic curves of type $y^2 = x^{2g+1} + ax^{g+1} + bx$. `https://arxiv.org/abs/1902.05992`. 2019.

УДК 519.7 DOI 10.17223/2226308X/12/6

ВАРИАЦИИ ОРТОМОРФИЗМОВ И ПСЕВДОАДАМАРОВЫХ ПРЕОБРАЗОВАНИЙ НА НЕАБЕЛЕВОЙ ГРУППЕ

Б. А. Погорелов, М. А. Пудовкина

В криптографии ортоморфизмы на абелевой группе используются как S-боксы в схемах Лея — Месси, квази-Фейстеля, в блочной шифрсистеме FOX, в режиме

блочного шифрования Дэвиса — Мейера, а также в кодах аутентификации. В работе рассматриваются ортоморфизмы, полные преобразования и их вариации на конечной неабелевой группе $(X,\cdot)$ наложения ключа. В алгоритме блочного шифрования SAFER для обеспечения принципа рассеивания используется псевдоадамарово преобразование. Предложено десять аналогов псевдоадамарова преобразования, задаваемых подстановкой s на неабелевой группе $(X,\cdot)$. Доказано, что биективность аналогов псевдоадамарова преобразования равносильна справедливости следующего условия: подстановка s является ортоморфизмом, полным преобразованием или их вариацией.

Ключевые слова: *ортоморфизм, полное преобразование, конечная неабелева группа, псевдоадамарово преобразование, алгоритм блочного шифрования SAFER.*

Пусть $S(X)$ — симметрическая группа на конечном множестве X, $g(\alpha)$ — образ элемента $\alpha \in X$ при действии на него подстановкой $g \in S(X)$, $\alpha^g = \alpha g = g(\alpha)$. Рассмотрим произвольную конечную неабелеву группу $(X,\cdot)$. Каждой подстановке $s \in S(X)$ поставим в соответствие преобразования $\pi_i^{(s)} : X \to X$, $i = 1,\dots,4$, заданные условиями

$$\pi_1^{(s)} : \alpha \mapsto \alpha^{-1}\alpha^s, \quad \pi_2^{(s)} : \alpha \mapsto \alpha\alpha^s, \quad \pi_3^{(s)} : \alpha \mapsto \alpha^s\alpha^{-1}, \quad \pi_4^{(s)} : \alpha \mapsto \alpha^s\alpha.$$

Определение 1. Пусть $s \in S(X)$, тогда

1) если $\pi_1^{(s)} \in S(X)$, то s называется *ортоморфизмом* [1];
2) если $\pi_2^{(s)} \in S(X)$, то s называется *полным преобразованием* [1];
3) если $\pi_3^{(s)} \in S(X)$, то s называется *левым ортоморфизмом*;
4) если $\pi_4^{(s)} \in S(X)$, то s называется *полным левым преобразованием.*

Очевидно, что для коммутативной группы $\pi_1^{(s)} = \pi_3^{(s)}$, $\pi_2^{(s)} = \pi_4^{(s)}$. В этом случае говорят, что $\pi_1^{(s)}$ — ортоморфизм, а $\pi_2^{(s)}$ — полное преобразование. Заметим, что для неабелевой группы $\pi_1^{(s)}$ можно называть правым ортоморфизм, а $\pi_2^{(s)}$ — полным правым преобразованием.

В дискретной математике ортоморфизмы и полные преобразования находят применение, например, при построении систем ортогональных латинских квадратов, квазигрупп [2–4]. В настоящее время открытым является вопрос полной классификации всех ортоморфизмов и полных преобразований на произвольной конечной группе. В криптографии ортоморфизмы используются как S-боксы [5], компоненты функции шифрования в схемах Лея — Месси [6], квази-Фейстеля [7], в алгоритме блочного шифрования FOX [8], в режиме блочного шифрования Дэвиса — Мейера [9], а также в кодах аутентификации.

Известно [1], что каждому ортоморфизму $s \in S(X)$ соответствует полное преобразование $\pi_1^{(s)}$. Наоборот, каждому полному преобразованию $s \in S(X)$ соответствует ортоморфизм $\pi_2^{(s)}$. Аналогичная связь существует между левым ортоморфизмом и полным левым преобразованием.

В алгоритме блочного шифрования SAFER [10] для обеспечения принципа рассеивания используется псевдоадамарово преобразование $h : \mathbb{Z}_{256}^2 \to \mathbb{Z}_{256}^2$, заданное условием

$$h : (\alpha_1, \alpha_2) \mapsto (2\alpha_1 + \alpha_2, \alpha_1 + \alpha_2),\ (\alpha_1, \alpha_2) \in \mathbb{Z}_{256}^2.$$

Очевидно, что h — подстановка на $\mathbb{Z}_{256}^2$. При этом преобразование $x \mapsto 2x \bmod 256$ не является биективным ортоморфизмом.

Для подстановки $s \in S(X)$ и каждого $\alpha \in X$ положим

$$\mathrm{A}^{(s)}(\alpha) = \left\{\alpha, \alpha^{-1}, \alpha^s, (\alpha^s)^{-1}\right\}.$$

Пусть $d = \left(d_1^{(1)}, d_2^{(1)}, d_1^{(2)}, d_2^{(2)}\right)$ — набор отображений, удовлетворяющих условиям $d_i^{(j)} : X^2 \to X$, $d_i^{(j)}(\alpha_1, \alpha_2) \in \mathrm{A}^{(s)}(\alpha_1) \cup \mathrm{A}^{(s)}(\alpha_2)$ для каждой пары $(\alpha_1, \alpha_2) \in X^2$, $i, j = 1, 2$. Обозначим через $D^{(s)}$ множество всех таких наборов отображений.

Для алгоритма блочного шифрования с неабелевой группой наложения ключа $(X, \cdot)$ рассмотрим аналог псевдоадамарова преобразования $h^{(s,d)} : X^2 \to X^2$, $d \in D^{(s)}$, заданного условием

$$h^{(s,d)} : (\alpha_1, \alpha_2) \mapsto \left(d_1^{(1)}(\alpha_1, \alpha_2) d_2^{(1)}(\alpha_1, \alpha_2), d_1^{(2)}(\alpha_1, \alpha_2) d_2^{(2)}(\alpha_1, \alpha_2)\right).$$

Для $s \in S(X)$ рассмотрим преобразования $h_i^{(s)} : X^2 \to X^2$ при $i = 1, \ldots, 10$, заданные условиями

$$\begin{aligned}
&h_1^{(s)} : (\alpha_1, \alpha_2) \mapsto (\alpha_1^s \alpha_2, \alpha_1 \alpha_2), && h_2^{(s)} : (\alpha_1, \alpha_2) \mapsto (\alpha_1^s \alpha_2^{-1}, \alpha_2 \alpha_1),\\
&h_3^{(s)} : (\alpha_1, \alpha_2) \mapsto (\alpha_1^s \alpha_2, \alpha_1 \alpha_2^{-1}), && h_4^{(s)} : (\alpha_1, \alpha_2) \mapsto (\alpha_1^s \alpha_2^{-1}, \alpha_1 \alpha_2^{-1}),\\
&h_5^{(s)} : (\alpha_1, \alpha_2) \mapsto ((\alpha_1^s)^{-1} \alpha_2, \alpha_1 \alpha_2), && h_6^{(s)} : (\alpha_1, \alpha_2) \mapsto ((\alpha_1^s)^{-1} \alpha_2^{-1}, \alpha_1 \alpha_2^{-1}),\\
&h_7^{(s)} : (\alpha_1, \alpha_2) \mapsto (\alpha_1 \alpha_2^s, \alpha_1 \alpha_2), && h_8^{(s)} : (\alpha_1, \alpha_2) \mapsto (\alpha_1 (\alpha_2^s)^{-1}, \alpha_1 \alpha_2),\\
&h_9^{(s)} : (\alpha_1, \alpha_2) \mapsto (\alpha_1 \alpha_2^s, \alpha_1 \alpha_2^{-1}), && h_{10}^{(s)} : (\alpha_1, \alpha_2) \mapsto (\alpha_1 (\alpha_2^s)^{-1}, \alpha_1 \alpha_2^{-1}).
\end{aligned}$$

Очевидно, что $h_i^{(s)} \in \left\{h^{(s,d)} : d \in D^{(s)}\right\}$ для $i = 1, \ldots, 10$.

Получен критерий биективности преобразования $h_j^{(s)}$ для каждого $j \in \{1, \ldots, 10\}$.

Теорема 1. Пусть $s \in S(X)$.

1. Для каждого $j \in \{1, 4\}$ тогда и только тогда $h_j^{(s)} \in S(X^2)$, когда $\pi_3^{(s)} \in S(X)$.
2. Для каждого $j \in \{2, 3, 8\}$ тогда и только тогда $h_j^{(s)} \in S(X^2)$, когда $\pi_4^{(s)} \in S(X)$.
3. Для каждого $j \in \{5, 6, 9\}$ тогда и только тогда $h_j^{(s)} \in S(X^2)$, когда $\pi_2^{(s)} \in S(X)$.
4. Для каждого $j \in \{7, 10\}$ тогда и только тогда $h_j^{(s)} \in S(X^2)$, когда $\pi_1^{(s)} \in S(X)$.

Кроме того, пусть $\mathrm{Aut}(X)$ — группа автоморфизмов. Доказано, что если $s \in \mathrm{Aut}(X)$, то для каждого $\{i, j\} \in \{\{1, 3\}, \{2, 4\}\}$ условия $\pi_i^{(s)} \in S(X)$ и $\pi_j^{(s)} \in S(X)$ равносильны.

ЛИТЕРАТУРА

1. *Evans A.* Orthomorphisms Graphs and Groups. Berlin: Springer Verlag, 1992.
2. *Johnson D. M., Dulmage A. L., and Mendelsohn N. S.* Orthomorphisms of groups and orthogonal Latin squares // Canad. J. Math. 1961. V. 13. P. 356–372.
3. *Глухов М. М.* О применениях квазигрупп в криптографии // Прикладная дискретная математика. 2008. Т. 2. № 2. С. 28–32.
4. *Глухов М. М.* О методах построения систем ортогональных квазигрупп с использованием групп // Математические вопросы криптографии. 2011. Т. 2. № 4. С. 5–24.
5. *Mittenthal L.* Block substitutions using orthomorphic mappings // Adv. Appl. Math. 1995. V. 16. No. 1. P. 59–71.
6. *Vaudenay S.* On the Lai — Massey schemes // ASIACRYPT'99. LNCS. 1999. V. 1716. P. 8–19.
7. *Yun A., Park J., and Lee J.* On Lai — Massey and quasi-Feistel ciphers // Des. Codes Cryptogr. 2011. V. 58. P. 45–72.

8. *Junod P. and Vaudenay S.* FOX: A new family of block ciphers // Selected Areas in Cryptography'04. LNCS. 2005. V. 3357. P. 114–129.
9. *Gilboa S. and Gueron S.* Balanced permutations Even-Mansour ciphers // Cryptology ePrint Archive. 2014. Report 2014/642.
10. *Massey J. L.* SAFER K-64: a byte-oriented block-ciphering algorithm // FSE'94. LNCS. 1994. V. 809. P. 1–17.

УДК 519.7 DOI 10.17223/2226308X/12/7

О КЛАССЕ СТЕПЕННЫХ КУСОЧНО-АФФИННЫХ ПОДСТАНОВОК НА НЕАБЕЛЕВОЙ ГРУППЕ ПОРЯДКА 2^m, ОБЛАДАЮЩЕЙ ЦИКЛИЧЕСКОЙ ПОДГРУППОЙ ИНДЕКСА ДВА

Б. А. Погорелов, М. А. Пудовкина

Четыре неабелевы группы порядка 2^m, $m \geqslant 4$, имеют циклические подгруппы индекса два. Примерами являются широко известная группа диэдра и обобщённая группа кватернионов. Произвольная неабелева группа G порядка 2^m, обладающая циклической подгруппой индекса два, в определённом смысле близка к встречающейся в качестве группы наложения ключа аддитивной абелевой группе кольца вычетов $\mathbb{Z}_{2^m}$. В данной работе на группе G задаются два класса преобразований, названных степенными кусочно-аффинными, для которых доказаны критерии биективности. Они позволят далее провести полную классификацию ортоморфизмов, полных преобразований и их вариаций во множестве всех степенных кусочно-аффинных подстановок.

Ключевые слова: *неабелева группа, группа диэдра, обобщённая группа кватернионов, критерий биективности, ортоморфизм.*

В ARX-шифрсистемах используются просто реализуемые операции сложения в кольце вычетов, в векторном пространстве над полем GF(2), а также циклический сдвиг. Возникает вопрос о переходе к просто реализуемой группе наложения ключа, относительно которой вместе с некоторым преобразованием g могут эффективно обеспечиваться перемешивающие и рассеивающие свойства.

Неабелевы группы порядка 2^m, обладающие циклической подгруппой индекса два, в определенном смысле преемственны широко встречающимся в качестве групп наложения ключа аддитивным абелевым группами m-мерного векторного пространства $V_m(2)$ над полем GF(2) и кольца вычетов $\mathbb{Z}_{2^m}$. В [1] описана связь между неабелевостью группы наложения ключа и свойством марковости алгоритмов блочного шифрования.

Из теоремы 12.5.1 [2] следует, что неабелевыми группами порядка 2^m, имеющими циклическую подгруппу индекса два, являются только четыре группы с двумя образующим a, u, удовлетворяющими следующим определяющим соотношениям:

1) обобщённая группа кватернионов Q_{2^m}, $m \geqslant 3$,

$$a^{2^{m-1}} = e,\ u^2 = a^{2^{m-2}},\ ua = a^{-1}u;$$

2) группа диэдра $D_{2^{m-1}}$, $m \geqslant 3$,

$$a^{2^{m-1}} = e,\ u^2 = e,\ ua = a^{-1}u;$$

3) $m \geqslant 4$,

$$a^{2^{m-1}} = e,\ u^2 = e,\ ua = a^{1+2^{m-2}}u;$$