Math-Net.Ru

Общероссийский математический портал

Б. А. Погорелов, М. А. Пудовкина, Факторструктуры преобразований, *Матем. вопр. криптогр.*, 2012, том 3, выпуск 3, 81–104

DOI: <https://doi.org/10.4213/mvk62>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.89.56.158

26 апреля 2023 г., 12:37:57

Факторструктуры преобразований

Б. А. Погорелов¹, М. А. Пудовкина²

¹ Академия криптографии Российской Федерации, Москва

² Национальный исследовательский ядерный университет (МИФИ), Москва

Получено 20.V.2011

Наличие нетривиальных линейных структур является слабостью криптографического преобразования. В работе рассматриваются факторструктуры, являющиеся обобщением линейных структур. Описаны сохраняющие их преобразования. В терминах операции сплетения полугрупп преобразований установлена связь двух классов методов криптографического анализа: разностного и гомоморфизмов.

Ключевые слова: линейная структура, сплетение, метод гомоморфизмов, разностный метод, разности высших порядков

Factor structures of transformations

B.A. Pogorelov¹, M.A. Pudovkina²

¹ Academy of Cryptography of the Russian Federation, Moscow

² National Nuclear Research University, Moscow

Abstract. The existence of nontrivial linear structures is a weakness of cryptographic transformations. We consider factor structures as a generalization of linear structures and describe transformations preserving such factor structures. On the base of the wreath product of transformation semigroups we establish a relationship between the differential attack and the homomorphism attack.

Key words: linear structure, wreath product, homomorphism attack, differential attack, higher order differentials

Citation: *Mathematical Aspects of Cryptography*, 2012, vol. 3, no. 3, pp. 81–104 (Russian).

§ 1. Введение

Линейные структуры преобразований (блочных шифрсистем) рассматривались в работах [1, 2, 4, 6] и др. Некоторые свойства преобразований с линейными структурами приведены в работе [5]. Наличие нетривиальной линейной структуры является слабостью криптографического преобразования, поскольку возникает возможность применять методы разностного и линейного криптоанализа или строить факторсистемы для данной криптографической системы и применять метод гомоморфизмов [1]. Таким образом, описание преобразований, обладающих линейными структурами, важно для синтеза и анализа шифрсистем.

В данной работе рассматриваются преобразования множеств, которые сохраняют их факторструктуры, являющиеся обобщением линейных структур. Показано, что в некоторых случаях множества таких преобразований описываются с помощью операции сплетения полугрупп преобразований. Приведены примеры факторструктур и соответствующих полугрупп преобразований над полем $GF(p^m)$, векторным пространством $V_m(p)$ размерности m над полем $GF(p)$ и кольцом вычетов $\mathbb{Z}_{p^m}$, $m > 1$. Для преобразований, обладающих факторструктурой, рассмотрены свойства разностей высших порядков. Для некоторых классов преобразований приведены точные значения разностей высших порядков. Описаны множества постановок, у которых разности высших порядков принимают фиксированные значения.

Кроме того, в терминах операции сплетения полугрупп преобразований установлена связь двух классов методов криптографического анализа: разностного и гомоморфизмов. Аппроксимация преобразований сплетениями полугрупп возникает довольно естественно, поскольку эти полугруппы обладают большим порядком и хорошей симметрией. Показано, что оценка эффективности нахождения ключа разностным методом и методом гомоморфизмов может быть выражена через расстояние Хемминга между табличными заданиями функций зашифрования и подстановками из некоторой группы сплетения.

В статье используются следующие обозначения: R — конечное коммутативное кольцо с единицей e_R ; $S(Z)$ — симметрическая группа на множестве Z ; $P(Z)$ — симметрическая полугруппа на множестве Z ; $G(Z) \in \{S(Z), P(Z)\}$; $G_b = G(Z)$ при $|Z| = b$; p — простое число; H — конечная (аддитивная) абелева группа, $H^\times = H \setminus \{0\}$; H_m — аддитивная группа поля $GF(p^m)$, векторного пространства $V_m(p)$ размерности m над полем $GF(p)$ или кольца $\mathbb{Z}_{p^m}$, $m > 1$ (обозначаем $H_m \in \{GF(p^m), V_m(p), \mathbb{Z}_{p^m}\}^+$).

В работе рассматривается сплетение групп $S_\omega \int S_r$ в его импримитивном действии, т. е. максимальная группа подстановок, сохраняющая систему импримитивности $W = \{W_1, \dots, W_r\}$ с r блоками мощности ω .

§ 2. Факторструктуры и сплетения

Напомним (см., например, [5]), что преобразование $g \in S(H)$ обладает *линейной структурой*, если в H существует такой ненулевой элемент α , что $(\beta + \alpha)^g = \beta^g + \gamma_\alpha$, для любого $\beta \in H$, где γ_α — некоторый фиксированный элемент из $H^\times$. Элемент α называется *линейным транслятором* отображения g . Множество всех линейных трансляторов отображения g вместе с нулевым вектором образуют подгруппу.

Данное понятие очевидным образом переносится на подполугруппы симметрической полугруппы. На полугруппы преобразований также легко обобщить понятия, аналогичные понятиям теории групп подстановок [8]: подобие полугрупп преобразований, блок импримитивности, импримитивная полугруппа, естественный гомоморфизм импримитивных полугрупп преобразований, операция сплетения. Для транзитивной полугруппы преобразований $G \leq P(H)$ классы эквивалентности нетривиального отношения на H , инвариантного относительно действия G , называются *блоками импримитивности*, а множество блоков импримитивности — *системой импримитивности*. Как и в случае групп подстановок, полугруппа преобразований вкладывается в сплетение $(B, \Delta \times \Gamma) = (K, \Delta) \int (R, \Gamma)$ полугрупп преобразований (K, Δ) и (R, Γ) при некоторой биекции $\phi: H \rightarrow \Delta \times \Gamma$, где Δ — блок импримитивности, Γ — множество (всех) блоков импримитивности. Здесь абстрактная полугруппа $K \int R$ задается множеством всех пар вида (f, r) , где $f: \Gamma \rightarrow K$, $r \in (R, \Gamma)$ и $(\delta, \gamma)^{(f, r)} = (\delta^{f(\gamma)}, \gamma^r)$ для всех блоков $\delta \in \Delta$, $\gamma \in \Gamma$. Такое вложение индуцирует естественный гомоморфизм полугруппы G в полугруппу (R, Γ) с ядром (K, Δ) .

Пусть W, X — произвольные непустые подмножества группы H одинаковой мощности, $W \neq H$ и

$$\begin{aligned} \Pi_{\alpha, \gamma}^G &= \{g \in G(H) \mid (\beta + \alpha)^g - \beta^g = \gamma \ \forall \beta \in H\}, \quad \alpha, \gamma \in H^\times, \\ \Pi_{W, X}^G &= \{g \in G(H) \mid (\beta + W)^g \subseteq \beta^g + X \ \forall \beta \in H\}. \end{aligned}$$

Будем говорить, что преобразование $g \in G(H)$ обладает *факторструктурой*, задаваемой собственными подмножествами $W, X \subset H$, $|W| = |X|$, если $(\beta + W)^g \subseteq \beta^g + X$ для любого $\beta \in H$. Другими словами, преобразование g сохраняет соответствующую факторструктуру множества H , задаваемую подмножествами $W, X \subset H$.

Очевидно, что линейное преобразование $g \in G(H)$ обладает факторструктурой. Также обладает факторструктурой и полугруппа, порожденная преобразованиями вида

$$\sigma: (v_1, \dots, v_r) \mapsto (\sigma_1(v_1), \dots, \sigma_r(v_r)), \quad g: (v_1, \dots, v_r) \mapsto (g_1(v_{i_1}), \dots, g_r(v_{i_r})),$$

где $v_1, \dots, v_r$ — векторы одинаковой размерности, $\{i_1, \dots, i_r\} = \{1, \dots, r\}$, $r > 1$. Факторструктура может задавать систему импримитивности, что может привести, например, к возможности применения метода гомоморфизмов.

Для произвольной подгруппы $W \leq H$ приведем характеризацию множества $\Pi_{W,W}^G$ в терминах действия полугруппы $G(H)$.

Утверждение 1. Пусть H — конечная абелева группа, $|H| = b$, W — ее собственная подгруппа, $|W| = d$, $d > 1$. Тогда:

1. Множество $\Pi_{W,W}^G \leq G(H)$ является импримитивной полугруппой с системой импримитивности $\{\beta + W | \beta \in H\}$. Полугруппа $\Pi_{W,W}^G$ подобна полугруппе $G_d \int G_{d^{-1}b}$.
2. Если найдется такой $g \in S(H)$, что $(\beta + W)^g = \beta^g + W^g$ то:
 - a. W^g — подгруппа группы H ;
 - b. $\Pi_{W,W^g}^S = \Pi_{W,W}^S g = (S_d \int S_{d^{-1}b}) g$.

Доказательство. 1. Покажем, что $\Pi_{W,W}^G$ является полугруппой. Если $h_1, h_2 \in \Pi_{W,W}^G$, то для любого $\alpha \in W$ и некоторых $\alpha' \in W$, $\alpha'' \in H$ справедливы равенства

$$(\beta + \alpha)^{h_1} = \beta^{h_1} + \alpha', \quad (\beta^{h_1} + \alpha')^{h_2} = \beta^{h_1 h_2} + \alpha''.$$

Тогда из соотношения

$$(\beta + \alpha)^{h_1 h_2} - \beta^{h_1 h_2} = (\beta^{h_1} + \alpha')^{h_2} - (\beta^{h_1})^{h_2} = \beta^{h_1 h_2} + \alpha'' - \beta^{h_1 h_2} = \alpha'' \in W$$

следует, что $\alpha'' \in W$. Значит, $h_1 h_2 \in \Pi_{W,W}^G$. Очевидно, что $e_H \in \Pi_{W,W}^G$. Таким образом, $\Pi_{W,W}^G$ — полугруппа.

Для любого преобразования $h \in \Pi_{W,W}^G$ включение $(\beta + W)^h - \beta^h \subseteq W$ эквивалентно тому, что $h: \beta + W \rightarrow \beta^h + W'$ для каждого $\beta \in H$ и некоторого $W' \subseteq W$. Полугруппа, порождаемая всеми такими преобразованиями, является импримитивной с системой импримитивности $\{\beta + W | \beta \in H\}$ и совпадает с полугруппой $G_d \int G_{d^{-1}b}$.

2.a. Так как равенство $(\beta + W)^g = \beta^g + W^g$ справедливо для любого $\beta \in W$, то $W^g = W^g + W^g$. Отсюда и из конечности W^g следует, что W^g — группа.

2.b. Из справедливости равенства $(\beta + W)^g = \beta^g + W^g$ для любого $\beta \in W$ следует, что $\Pi_{W, W^g}^S \subseteq \Pi_{W, W^g}^S$.

Предположим существование такого преобразования $g': W \rightarrow W^g$, что $g' \in \Pi_{W, W^g}^S$ и $\Pi_{W, W^g}^S \cap \Pi_{W, W^g}^S g' \neq \emptyset$. Тогда найдутся такие элементы $s, s' \in \Pi_{W, W}^S$, что $sg = s'g'$. Значит, $g' = (s')^{-1}sg$ и $\Pi_{W, W^g}^S = \Pi_{W, W^g}^S g'$.

Предположим существование такого преобразования $g': W \rightarrow W^g$, что $g' \in \Pi_{W, W^g}^S$ и $\Pi_{W, W^g}^S \cap \Pi_{W, W^g}^S g' = \emptyset$, т. е. $\Pi_{W, W^g}^S = \Pi_{W, W^g}^S \neq \Pi_{W, W^g}^S g'$. Так как $\Pi_{W, W^g}^S \subseteq \Pi_{W, W^g}^S$ и $\Pi_{W, W^g}^S g' \subseteq \Pi_{W, W^g}^S$, то для произвольных элементов $sg \in \Pi_{W, W^g}^S$, $s'g' \in \Pi_{W, W^g}^S g'$ справедливо включение $sg(s'g')^{-1} \in \Pi_{W, W}^S$. Отсюда получаем, что $g(g')^{-1} \in \Pi_{W, W}^S$. Следовательно, $g \in \Pi_{W, W^g}^S g'$. Значит, $\Pi_{W, W^g}^S = \Pi_{W, W^g}^S g'$ и $\Pi_{W, W^g}^S = \Pi_{W, W^g}^S = (S_d \int S_{d^{-1}b})g$. ■

В криптосистемах часто используются преобразования векторных пространств $V_m(p)$, полей Галуа $GF(p^m)$ или колец вычетов $\mathbb{Z}_{p^m}$. В этих случаях утверждение 1 допускает уточнение.

Следствие 2. Пусть $H_m \in \{GF(p^m), V_m(p)\}^+$, $W < H_m$, $|W| = p^t$, $t \in \{1, \dots, m-1\}$. Тогда:

а) $\Pi_{W, W}^G$ — импримитивная полугруппа из $G(H_m)$ с системой импримитивности $\{\beta + W \mid \beta \in H_m\}$, подобная подполугруппе $G_{p^t} \int G_{p^{m-t}}$;

б) если $\alpha \in H_m^\times$, то $\Pi_{\alpha, \alpha}^G$ — импримитивная полугруппа из $G(H_m)$ с системой импримитивности $\{\beta + \langle \alpha \rangle \mid \beta \in H_m\}$, подобная полугруппе $(\mathbb{Z}_p, +) \int G_{p^{m-1}}$.

Доказательство непосредственно следует из утверждения 1. ■

Следствие 3. Пусть W — идеал кольца вычетов $\mathbb{Z}_{p^m}$, $|W| = p^t$, $t \in \{1, \dots, m-1\}$. Тогда:

а) $\Pi_{W, W}^G$ — импримитивная полугруппа из $G(\mathbb{Z}_{p^m})$ с системой импримитивности $\{\beta + W \mid \beta \in \mathbb{Z}_{p^m}\}$, подобная подполугруппе $G_{p^t} \int G_{p^{m-t}}$;

б) если $\alpha \in \mathbb{Z}_{p^m}^\times$, $|\langle \alpha \rangle| = p^t$, $t \in \{1, \dots, m\}$, то $\Pi_{\alpha, \alpha}^G$ — импримитивная полугруппа из $G(\mathbb{Z}_{p^m})$ с системой импримитивности $\{\beta + \langle \alpha \rangle \mid \beta \in \mathbb{Z}_{p^m}\}$, подобная полугруппе $(\mathbb{Z}_{p^t}, +) \int G_{p^{m-t}}$.

Доказательство следует из включений $\Pi_{\alpha,\alpha}^P > \Pi_{\alpha,\alpha}^S \geq \mathbb{Z}_d \int S_{b/d}$ и утверждения 1. ■

Следствие 4. Пусть α — произвольный ненулевой элемент $\mathbb{Z}_l$ -модуля H , $|H| = b$, $l \in \mathbb{N}$, $l \geq 2$, $\langle \alpha \rangle$ — аддитивная группа, $d = |\langle \alpha \rangle| > 1$. Тогда $\Pi_{\alpha,\alpha}^G$ — импримитивная полугруппа с системой импримитивности $\{\beta + \langle \alpha \rangle \mid \beta \in H\}$, подобная полугруппе $(\mathbb{Z}_d, +) \int G_{d^{-1}b}$.

Доказательство. Аналогично утверждению 1 для подмодуля W показывается, что $\Pi_{W,W}^G$ — полугруппа.

Так как $(\alpha + \beta)^h = \alpha + \beta^h$ для любых $\beta \in H$, $h \in \Pi_{\alpha,\alpha}^G$, то $(\alpha c + \beta)^h = \alpha c + \beta^h$ для любых $\alpha c \in \langle \alpha \rangle$, $c \in \mathbb{Z}_l$ и любого $\beta \in H$. Значит, $(\beta + \langle \alpha \rangle)^h = \beta^h + \langle \alpha \rangle$ для любого элемента $\beta \in H$ и $\{\beta + \langle \alpha \rangle \mid \beta \in H\}$ — система импримитивности полугруппы $\Pi_{\alpha,\alpha}^G$.

Рассмотрим действие полугруппы $\Pi_{\alpha,\alpha}^G$ на произвольном блоке $\langle \alpha \rangle + \beta$. В этом случае $\beta^h - \beta \in \langle \alpha \rangle$. Пусть $\beta^h = \alpha r + \beta$ для некоторого элемента $\alpha r \in \langle \alpha \rangle$. Тогда $(\alpha c + \beta)^h = \beta + \alpha(c + r)$, если $\alpha c \in \langle \alpha \rangle$. Значит, полугруппа $\Pi_{\alpha,\alpha}^G$ при ее действии на блоке $\langle \alpha \rangle + \beta$ подобна аддитивной группе кольца вычетов $\mathbb{Z}_d$ по сложению. ■

Утверждение 5. Пусть H — $\mathbb{Z}_l$ -модуль, $|H| = b$, $l \in \mathbb{N}$, $l \geq 2$, W — собственный подмодуль, $X \subseteq H$, $|W| = |X| = d > 1$. Тогда

$$\Pi_{W,X}^S = \begin{cases} \emptyset, & \text{если } X \text{ не является подмодулем } H, \\ \Pi_{W,W}^S g = (S_d \int S_{d^{-1}b}) g, & \text{если } X \text{ — подмодуль } H, \end{cases}$$

где $g \in S(H)$, $g: W \rightarrow X$ — произвольное линейное отображение.

Доказательство. Если X — не подмодуль, но $\Pi_{W,X}^S \neq \emptyset$, то из утверждения 1 следует, что X — абелева подгруппа группы H . Поскольку H — модуль над кольцом вычетов, то X — подмодуль H . Противоречие.

Если X — подмодуль, то для любых подмодулей одинаковой мощности существует биективное линейное отображение $g \in S(H)$, удовлетворяющее равенству $W^g = X$. В этом случае из утверждения 1 следует справедливость равенства $(\beta + W)^g = \beta^g + X$ для всех $\beta \in H$, а потому и справедливость утверждения 5. ■

Группы $H_m \in \{GF(p^m), V_m(p), \mathbb{Z}_{p^m}\}^+$ удовлетворяют условиям утверждения 5.

Утверждение 6. Пусть α, γ — произвольные ненулевые элементы $\mathbb{Z}_l$ -модуля H , $\alpha \neq \gamma$, $|\langle \alpha \rangle| = d$, $|H| = b$, $2 \leq l$ — произвольное натуральное число. Тогда

$$\Pi_{\alpha, \gamma}^G = \begin{cases} (\Pi_{\alpha, \alpha}^G)g = ((\mathbb{Z}_d, +) \int G_{d^{-1}b})h, & \text{если } |\langle \alpha \rangle| = |\langle \gamma \rangle|, \\ \emptyset, & \text{если } |\langle \alpha \rangle| \neq |\langle \gamma \rangle|, \end{cases}$$

где g — произвольное линейное биективное отображение из $\Pi_{\alpha, \gamma}^G$, $\alpha^g = \gamma$.

Доказательство. Для всех $h \in \Pi_{\alpha, \gamma}^G$, $\beta \in H$, $r \in \mathbb{Z}_l$ справедливо равенство $(\alpha r + \beta)^h = \beta^h + \gamma r$. Если $\Pi_{\alpha, \gamma}^G \neq \emptyset$ при $|\langle \alpha \rangle| \neq |\langle \gamma \rangle|$, то $\beta^h = \beta^h + \gamma d$ и $\gamma d \neq 0$ при $r = d$, что невозможно. Значит, $\Pi_{\alpha, \gamma}^G = \emptyset$ при $|\langle \alpha \rangle| \neq |\langle \gamma \rangle|$.

Если $|\langle \alpha \rangle| = |\langle \gamma \rangle|$, то существует такое линейное отображение $g \in G(H)$, что $\alpha^g = \gamma$ и $g \in \Pi_{\alpha, \gamma}^G$. Следовательно, $\Pi_{\alpha, \gamma}^G \neq \emptyset$. Очевидно, что $\Pi_{\alpha, \gamma}^G \cap \Pi_{\alpha, \alpha}^G = \emptyset$ при $\alpha \neq \gamma$.

Пусть h — произвольное преобразование из $\Pi_{\alpha, \gamma}^G$. Тогда

$$(\beta + \alpha)^{hg^{-1}} = (\beta^h + \gamma)^{g^{-1}} = \beta^{hg^{-1}} + \alpha.$$

Значит, $hg^{-1} \in \Pi_{\alpha, \alpha}^G$ и $\Pi_{\alpha, \gamma}^G \subseteq (\Pi_{\alpha, \alpha}^G)g$.

Покажем, что $\Pi_{\alpha, \gamma}^G \supseteq (\Pi_{\alpha, \alpha}^G)g$. Если $h \in \Pi_{\alpha, \alpha}^G$, то

$$(\beta + \alpha)^{hg} = (\beta^h + \alpha)^g = \beta^{hg} + \gamma.$$

Таким образом, $hg \in \Pi_{\alpha, \gamma}^G$. Значит, $\Pi_{\alpha, \gamma}^G = \Pi_{\alpha, \alpha}^G g$.

Согласно следствию 4 справедливо равенство $\Pi_{\alpha, \alpha}^G = (\mathbb{Z}_d, +) \int G_{d^{-1}b}$. Значит, $\Pi_{\alpha, \gamma}^G = ((\mathbb{Z}_d, +) \int G_{d^{-1}b})g$. ■

Следствие 7. Пусть выполнены условия утверждения 6. Тогда

$$|\Pi_{\alpha, \gamma}^P| = \begin{cases} (b/d)^{b/d} \cdot d^{b/d}, & \text{если } |\langle \alpha \rangle| = |\langle \gamma \rangle|, \\ 0, & \text{если } |\langle \alpha \rangle| \neq |\langle \gamma \rangle|. \end{cases}$$

Доказательство следует из утверждения 6. ■

Следствие 8. Пусть $H_m \in \{GF(p^m), V_m(p)\}^+$. Тогда

$$\Pi_{\alpha, \gamma}^G = \Pi_{\alpha, \alpha}^G g = \left((\mathbb{Z}_p, +) \int G_{p^{m-1}} \right) g$$

для любых элементов $\alpha, \gamma \in H_m^\times$, где g — произвольное биективное линейное преобразование из $\Pi_{\alpha, \gamma}^G$. Кроме того, число подстановок из $S(H_m)$, обладающих линейным транслятором α , равно $(p^m - 1) \cdot p^{p^{m-1}} \cdot (p^{m-1}!)$. Число преобразований из $P(H_m)$ с линейным транслятором α равно $(p^m - 1) \cdot p^{p^{m-1}} \cdot (p^{m-1})^{p^{m-1}}$.

Доказательство следует из утверждения 6. ■

Следствие 9. Пусть α, γ — произвольные элементы кольца $\mathbb{Z}_{p^m}^\times$, $\alpha \neq \gamma$, $|\langle \alpha \rangle| = p^t$, $t \in \{1, \dots, m\}$. Тогда

$$\Pi_{\alpha, \gamma}^G = \begin{cases} \left(\Pi_{\alpha, \alpha}^G \right) h = \left(\mathbb{Z}_{p^t} \int G_{p^{m-1}} \right) h, & \text{если } |\langle \alpha \rangle| = |\langle \gamma \rangle|, \\ \emptyset, & \text{если } |\langle \alpha \rangle| \neq |\langle \gamma \rangle|, \end{cases}$$

где h — произвольное линейное отображение из $\Pi_{\alpha, \gamma}^G$, $\alpha^h = \gamma$. Кроме того, число преобразований из $P(\mathbb{Z}_{p^m})$ с линейным транслятором α равно $(p^{m-t} - p^{m-t-1}) \cdot p^{t \cdot p^{m-t}} \cdot (p^{m-t})^{p^{m-t}}$, а число подстановок из $S(\mathbb{Z}_{p^m})$ с линейным транслятором α равно $(p^{m-t} - p^{m-t-1}) \cdot p^{t \cdot p^{m-t}} \cdot (p^{m-t}!)$.

Доказательство следует из утверждения 6 и равенства

$$|\{\gamma \in \mathbb{Z}_{p^m} \mid |\langle \gamma \rangle| = p^t\}| = \phi(p^{m-t}) = p^{m-t} - p^{m-t-1}. \quad \blacksquare$$

Пусть $H_m \in \{GF(p^m), V_m(p)\}^+$, $\{\alpha_1, \alpha_2, \dots, \alpha_k\} \subseteq H_m \setminus 0$, $k \geq 1$. Покажем, что множество $\bigcap_{i=1}^k \Pi_{\langle \alpha_i \rangle, \langle \alpha_i \rangle}^G$ также является сплетением полугрупп преобразований.

Теорема 10. Пусть $H_m \in \{GF(p^m), V_m(p)\}^+$, $\{\alpha_1, \alpha_2, \dots, \alpha_k\} \subseteq H_m$, $k \in \{1, \dots, p^m\}$, $\dim \langle \alpha_1, \alpha_2, \dots, \alpha_k \rangle = t \geq 1$. Тогда:

- 1) $\bigcap_{i=1}^k \Pi_{\langle \alpha_i \rangle, \langle \alpha_i \rangle}^G = \underbrace{G_p \int \dots \int G_p \int G_{p^{m-t}}}_t;$
- 2) $\bigcap_{i=1}^k \Pi_{\alpha_i, \alpha_i}^G = \underbrace{(\mathbb{Z}_p, +) \int \dots \int (\mathbb{Z}_p, +) \int G_{p^{m-t}}}_t.$

Доказательство. 1) Обозначим $G^{(1)} = \bigcap_{i=1}^k \Pi_{\langle \alpha_i \rangle, \langle \alpha_i \rangle}^G$. Аналогично

утверждению 1 показывается, что $G^{(1)}$ — полугруппа.

Предположим, что элементы $\alpha_1, \dots, \alpha_t \in H_m$ линейно независимы и $\gamma \in H_m$. Положим $X_\gamma^{(0)} = \gamma$, $X_\gamma^{(1)} = \gamma + \langle \alpha_1, \dots, \alpha_t \rangle$, $[X^{(1)}] = \{X_\gamma^{(1)} \mid \gamma \in H_m^\times\}$, $X_\gamma^{(2)} = \gamma + \langle \alpha_2, \dots, \alpha_t \rangle$ для $\gamma \in X_0^{(1)}$, $[X^{(2)}] = \{X_\gamma^{(2)} \mid \gamma \in X_0^{(1)}\}, \dots, X_\gamma^{(t-1)} = \gamma + \langle \alpha_t \rangle$ для $\gamma \in X_0^{(t-2)}$, $[X^{(t-1)}] = \{X_\gamma^{(t-1)} \mid \gamma \in X_0^{(t-2)}\}$, $X_\gamma^{(t)} = \gamma$ для $\gamma \in X_0^{(t-1)}$.

Система импримитивности $\{X_\gamma^{(1)} \mid \gamma \in H_m^\times\}$ является максимальной для полугруппы $G^{(1)}$, а система $\{X_\gamma^{(1)} \mid \gamma \in X_0^{(j-1)}\}$ — максимальной для полугруппы $G^{(1)}$ при ограничении ее действия на множество $X_0^{(j-1)}$, $j = 2, \dots, t-1$.

Для $j = 1, \dots, t-1$ рассмотрим естественный гомоморфизм $\phi_j: G^{(j)} \rightarrow \bar{G}^{(j)}$ импримитивной полугруппы $G^{(j)}$ с блоками импримитивности $X_\gamma^{(j)}$ и ядром $\text{Ker} \phi_j = G^{(j+1)}$. Нетрудно убедиться, что $\text{Im} \phi_j = G([X^{(j)}])$ и $G^{(j)} = G^{(j+1)} \int \bar{G}^{(j)}$. Кроме того, $G([X^{(j)}]) = G_{p^{m-t}}$ при $j = 1$ и $G([X^{(j)}]) = G_p$ при $j \geq 2$, $G^{(t)} = G_p$.

Значит,

$$G^{(1)} = G^{(2)} \int G_{p^{m-t}} = G^{(3)} \int G_p \int G_{p^{m-t}} = \dots = G_p \int \dots \int G_p \int G_{p^{m-t}}.$$

2) Доказательство проводится аналогично. ■

Утверждение 11. Пусть W_1 — собственный подмодуль $\mathbb{Z}_l$ -модуля H , $l \geq 2$, $W_1 = \langle \alpha_1, \dots, \alpha_t \rangle$, $t \geq 1$, $I = W_1 + \alpha$, $\alpha \in H \setminus W_1$, $|H| = b$, $|W_1| = d_1 > 1$. Пусть также $W_2 = \langle \alpha_1, \dots, \alpha_t, \alpha \rangle$, $|W_2| = d_2$. Тогда $\Pi_{I,I}^G$ — импримитивная полугруппа из $G(H)$ с системой импримитивности $\{\beta + W_2 \mid \beta \in H\}$, подобная полугруппе $G_{d_1} \int G_{d_1^{-1}d_2} \int G_{d_2^{-1}b}$.

Доказательство следует из повторного применения утверждения 1. ■

§ 3. Разности высшего порядка

Пусть $\oplus$ — операция сложения векторов в пространстве $V_m(2)$. Сумму множества элементов в векторном пространстве $V_m(2)$ будем обозначать символом $\sum \oplus$.

Напомним, что производной отображения $g: V_m(2) \rightarrow V_m(2)$ по направлению $\alpha \in V_m(2)^\times$ называется отображение $d_\alpha g: V_m(2) \rightarrow V_m(2)$, где $(d_\alpha g): \beta \rightarrow (\beta \oplus \alpha)^g \oplus \beta^g$.

При $p = 2$ производной d_L отображения g по направлению подпространства $L \leq V_m$ называется отображение $d_L g: V_m(2) \rightarrow V_m(2)$, заданное как $d_L g: \beta \rightarrow \sum_{\alpha \in L} (\alpha \oplus \beta)^g$. Так как

$$\sum_{\alpha \in L} (\alpha \oplus \beta)^g = \sum_{\alpha \in L} ((\alpha \oplus \beta)^g \oplus \beta^g),$$

то производная отображения g по направлению подпространства называется также *разностью высшего порядка* [3].

Для произвольных подгруппы W абелевой группы H и подстановки $g \in S(H)$ введем обобщение $(ad_W): H \rightarrow H$ разности высшего порядка, положив $(ad_W g): \beta \rightarrow \sum_{\alpha \in W} ((\alpha + \beta)^g - \beta^g)$. Отметим, что

$$\sum_{\alpha \in W} ((\alpha + \beta)^g - \beta^g) = \sum_{\alpha \in W} (\alpha + \beta)^g - |W|\beta^g.$$

При $H = (V_m(2), \oplus)$ получаем, что $ad_W = d_W$ для любого подпространства $W < V_m(2)$.

Покажем, что множества $\Pi_{W,X}^S$ характеризуют некоторые свойства разностей высшего порядка отображения g .

Пусть $r_p(G)$ — p -ранг группы G , p — простое число.

Утверждение 12. Пусть H — произвольная конечная абелева группа, W, X — ее ненулевые собственные подгруппы одинаковой мощности и $\Pi_{W,X}^S \neq \emptyset$,

$$X \cong \mathbb{Z}_{p_1}^{r_{11}} + \dots + \mathbb{Z}_{p_1}^{r_{1d_1}} + \dots + \mathbb{Z}_{p_t}^{r_{t1}} + \dots + \mathbb{Z}_{p_t}^{r_{td_t}},$$

$t \in \mathbb{N}$, p_i — простые числа, $p_i < p_{i+1}$, $r_{ij} \in \mathbb{N}$, $j = 1, \dots, d_i - 1$, $r_{ij} \leq r_{ij+1}$, $i = 1, \dots, t - 1$, $d = d_1 + \dots + d_t$, $q = |X|$, e_{11} — произвольный элемент порядка $2^{r_{11}}$ группы X при $p_1 = 2$. Тогда для $g \in \Pi_{W,X}^S$, $\beta \in H$ выполняются равенства

$$\beta^{ad_W g} = \sum_{\theta \in X} \theta = \begin{cases} 2^{r_{11}-1} e_{11}, & \text{если } r_2(X) = 1, \\ \vec{0} & \text{в противном случае.} \end{cases}$$

Доказательство. Так как $g \in \Pi_{W,X}^S$, то $(\beta + W)^g = \beta^g + X$ для любого $\beta \in H$. Это означает, что

$$\beta^{ad_W g} = \sum_{\alpha \in W} (\alpha + \beta)^g - |W|\beta^g = |W|\beta^g + \sum_{\theta \in X} \theta - |W|\beta^g = \sum_{\theta \in X} \theta.$$

Вычислим $\sum_{\theta \in X} \theta$. Легко видеть, что

$$\sum_{\beta \in \mathbb{Z}_{p_i}^{r_{ij}}} \beta = 2^{-1} p_i^{r_{ij}} (p_i^{r_{ij}} - 1) = \begin{cases} 0 \pmod{p_i^{r_{ij}}}, & \text{если } p_i > 2, \\ p_i^{r_{ij}-1} \pmod{p_i^{r_{ij}}}, & \text{если } p_i = 2. \end{cases}$$

Поэтому $\sum_{\theta \in X} \theta = 0$, если $p_1 > 2$.

Пусть $p_1 = 2$ и $2^{r_{1j}-1} = a_{1j}$, $j = 1, \dots, d_1$. Если $X' = \mathbb{Z}_{2^{r_{1i}}} + \mathbb{Z}_{2^{r_{1j}}}$, то $\sum_{\theta \in X'} \theta = a_{1i} 2^{r_{1j}} + a_{1j} 2^{r_{1i}}$. Так как элементы a_{1j} порядка $2^{r_{1j}-1}$, то правая часть последнего равенства равна 0. Поэтому $\sum_{\theta \in X} \theta = 0$, если $r_2(X) = d_1 \geq 2$. ■

ЗАМЕЧАНИЕ. Если $X = V_m(2)$ то

$$\sum_{\theta \in X} \oplus \theta = \begin{cases} \alpha^s \oplus \vec{0}^s, & \text{если } X = \langle \alpha \rangle, \\ \vec{0}, & \text{если } \dim X > 1. \end{cases}$$

Следствие 13. Пусть W , X — ненулевые собственные подпространства V_m , $|X| = |W|$, β — произвольный вектор из V_m , $g \in \Pi_{W,X}$. Тогда

$$\beta^{d_W g} = \begin{cases} \vec{0}^g \oplus \alpha^g, & \text{если } W = \langle \alpha \rangle, \\ \vec{0}, & \text{если } \dim W > 1. \end{cases}$$

Доказательство непосредственно следует из утверждения 12. ■

Из следствия 13 получаем описание преобразований из группы $S(V_m(2))$, у которых разность высшего порядка равна $\vec{0}$, и оценку их числа.

Пусть $W < V_m(2)$, $\Lambda_{W, \vec{0}}^G$ — множество всех подстановок $g \in G(V_m(2))$, удовлетворяющих равенству $\beta^{d_W g} = \vec{0}$ для любого $\beta \in V_m(2)$, $\Lambda_{mt} = \bigcup_{X \in V_m^{(t)}} \Pi_{W,X}^S$. Пусть также $V_m^{(t)}$ — множество всех различных подпространств пространства $V_m(2)$ размерности t .

Следствие 14. Пусть W — собственное подпространство $V_m(2)$, $\dim W = t$, $t \in \{3, \dots, m-1\}$. Тогда

$$\begin{aligned} \Lambda_{mt} &\subseteq \Lambda_{W, \vec{0}}^S, \\ |\Lambda_{mt}| &= \left| V_m^{(t)} \right| |S_{2^t} \wr S_{2^{m-t}}| = (2^t!)^{2^{m-t}} \cdot (2^{m-t}!) \times \\ &\times \frac{(2^m - 1)(2^{m-1} - 1) \dots (2^{m-t+1} - 1)}{(2^t - 1)(2^{t-1} - 1) \dots (2^2 - 1)} \leq \left| \Lambda_{W, \vec{0}}^S \right|. \end{aligned}$$

Доказательство. Из утверждения 5 и следствия 7 получаем, что $\bigcup_{X \in V_m^{(t)}} \Pi_{W,X}^S \subseteq \Lambda_{W,\vec{0}}^S$.

Пусть X, X' — произвольные различные подпространства из $V_m^{(t)}$. Если $h \in \Pi_{W,X}^S$, то $W^h = X$ и $h \notin \Pi_{W,X'}^S$, в противном случае $W^h = X'$. Следовательно, $\Pi_{W,X}^S \cap \Pi_{W,X'}^S = \emptyset$. Значит,

$$\begin{aligned} \left| \bigcup_{X \in V_m^{(t)}} \Pi_{W,X}^S \right| &= |V_m^{(t)}| \cdot |\Pi_{W,W}^S| = \\ &= \frac{(2^m - 1)(2^{m-1} - 1) \dots (2^{m-t+1} - 1)}{(2^t - 1)(2^{t-1} - 1) \dots (2^2 - 1)} (2^t!)^{2^{m-t}} \cdot (2^{m-t}!) \leq |\Lambda_{W,\vec{0}}^S|. \blacksquare \end{aligned}$$

Отметим, что $\Lambda_{W,\vec{0}}^S = \emptyset$, если $\dim W = 1$.

Рассмотрим еще одно свойство обобщенных линейных структур, связанное с разностями высших порядков. Пусть

$$\Lambda_{W,X}^G = \left\{ g \in G(H) \mid \{ \alpha^{d_w(g)} \mid \alpha \in H \} = X \right\},$$

где W — подгруппа абелевой группы H , $X \subseteq H$, т. е. $g \in \Lambda_{W,X}^G$ тогда и только тогда, когда одновременно выполняются условия:

1. $\alpha^{d_w(g)} \in X$ для всех $\alpha \in H$.
2. Для каждого $\beta \in X$ существует такой элемент $\alpha \in H$, что $\alpha^{d_w(g)} = \beta$.

Рассмотрим сначала $H = V_m(2)$. Покажем, что $\Lambda_{W,\gamma}^S \neq \emptyset$ для произвольных $\gamma \in H$, $W < H$, и приведем конструкцию, позволяющую построить подмножество подстановок из $\Lambda_{W,\gamma}^S$. Эта проблема несколько сложнее описания множества $\Lambda_{W,X}^P$.

Выше было показано (следствие 14), что $\bigcup_{X \in V_m^{(t)}} \Pi_{W,X}^S \subseteq \Lambda_{W,\vec{0}}^S$, если W — нетривиальное подпространство $V_m(2)$, $\dim W = t$.

Утверждение 15. Пусть W — собственное нетривиальное подпространство $V_m(2)$, $\dim W = t \geq 1$, γ — произвольный вектор из $V_m(2)$. Тогда $|\Lambda_{W,\gamma}^S| \leq |\Lambda_{W,\gamma}^S|$.

Доказательство. Построим разбиение пространства V_m на такие подмножества мощности 2^t , что сумма элементов каждого такого подмножества равна γ .

Пусть $\beta_1, \beta_2, \dots, \beta_m$ — базис пространства V_m , $\gamma = \beta_m$. Для вектора $\delta \in \langle \beta_{t+1}, \dots, \beta_m \rangle^\times$ положим:

$$\begin{aligned}\Theta_\gamma(\vec{0}) &= \{\vec{0}\} \cup (\langle \beta_1, \dots, \beta_t \rangle^\times \oplus \gamma), \\ \Theta_\gamma(\delta) &= \Theta_\gamma(\vec{0}) \oplus \delta = \{\delta\} \cup (\langle \beta_1, \dots, \beta_t \rangle^\times \oplus \delta \oplus \gamma).\end{aligned}$$

По построению $\sum_{\theta \in \Theta_\gamma(\delta)} \oplus \theta = \gamma$ и $|\Theta_\gamma(\delta)| = 2^t$. Кроме того, для любых различных векторов $\delta, \delta' \in \langle \beta_{t+1}, \dots, \beta_m \rangle$ имеем $\Theta_\gamma(\delta) \cap \Theta_\gamma(\delta') = \emptyset$ и $|\{\Theta_\gamma(\delta) | \delta \in \langle \beta_{t+1}, \dots, \beta_m \rangle\}| = 2^{m-t}$. Значит, множество $\{\Theta_\gamma(\delta) | \delta \in \langle \beta_{t+1}, \dots, \beta_m \rangle\}$ является разбиением V_m .

Рассмотрим смежные классы $(V_m : W) = \{\alpha_1 \oplus W, \dots, \alpha_{2^{m-t}} \oplus W\}$. Если $s \in \Lambda_{W, \gamma}^S$, то

$$\sum_{\theta \in \alpha_i \oplus W} \oplus \theta^s = \gamma, \quad i = 1, \dots, 2^{m-t}. \quad (1)$$

Для $i = 1, \dots, 2^{m-t}$ обозначим $C_{i, \gamma}(s) = \{\theta^s | \theta \in \alpha_i \oplus W\} = \{\alpha_i \oplus W\}^s = W(\alpha_i)^s$.

Пусть $h: \{1, \dots, 2^{m-t}\} \rightarrow \langle \beta_{t+1}, \dots, \beta_m \rangle$ — произвольное биективное отображение, $i^h = \delta_i$, $\delta_i \in \langle \beta_{t+1}, \dots, \beta_m \rangle$. Если подстановки $s \in S(V_m)$ удовлетворяют равенствам $C_{i^h, \gamma}(s) = \Theta_\gamma(\delta_i)$, $i = 1, \dots, 2^{m-t}$, то справедливы также равенства (1). Значит, $s \in \Lambda_{W, \gamma}^S$.

Поэтому для построения подмножества подстановок $\Lambda_{W, \gamma}^S(\langle \beta_1, \dots, \beta_t \rangle)$ из $\Lambda_{W, \gamma}^S$, сохраняющих разбиение $\{\Theta_\gamma(\delta) | \delta \in \langle \beta_{t+1}, \dots, \beta_m \rangle\}$, достаточно для каждого биективного отображения $h: \{1, \dots, 2^{m-t}\} \rightarrow \langle \beta_{t+1}, \dots, \beta_m \rangle$, $i^h = \delta_i$, сформировать все подстановки $s_h \in S(V_m)$, удовлетворяющие равенствам $C_{i^h, \gamma}(s) = \Theta_\gamma(\delta_i)$, $i = 1, \dots, 2^{m-t}$. Число таких подстановок s_h для каждого $h: \{1, \dots, 2^{m-t}\} \rightarrow \langle \beta_{t+1}, \dots, \beta_m \rangle$ равно $(2^t!)^{2^{m-t}}$. Следовательно, $|\Lambda_{W, \gamma}^S(\langle \beta_1, \dots, \beta_t \rangle)| = 2^{m-t}! \cdot (2^t!)^{2^{m-t}}$.

Каждое разбиение $\{\Theta_\gamma(\delta) | \delta \in \langle \beta_{t+1}, \dots, \beta_m \rangle\}$ и, соответственно, множество подстановок $\Lambda_{W, \gamma}^S(\langle \beta_1, \dots, \beta_t \rangle)$ однозначно задается подпространством $\langle \beta_1, \dots, \beta_t \rangle$. Действительно, пусть $B = \langle \beta_1, \dots, \beta_t \rangle$, $B' = \langle \beta'_1, \dots, \beta'_t \rangle$ — два различных подпространства V_m одинаковой размерности t . Пусть также

$$\begin{aligned}\overline{B} &= \langle \beta_{t+1}, \dots, \beta_m \rangle, \quad \overline{B}' = \langle \beta'_{t+1}, \dots, \beta'_m \rangle, \\ \Theta_\gamma &= \{\Theta_\gamma(\delta) | \delta \in \overline{B}\}, \quad \Theta'_\gamma = \{\Theta'_\gamma(\delta') | \delta' \in \overline{B}'\},\end{aligned}$$

$$\begin{aligned}\Theta_\gamma(\delta) &= \{\delta\} \cup (\langle \beta_1, \dots, \beta_t \rangle^\times \oplus \delta \oplus \gamma), \quad \delta \in \overline{B}, \\ \Theta'_\gamma(\delta') &= \{\delta'\} \cup (\langle \beta'_1, \dots, \beta'_t \rangle^\times \oplus \delta' \oplus \gamma), \quad \delta' \in \overline{B'}.\end{aligned}$$

По построению единственное множество в Θ_γ (или Θ'_γ), содержащее вектор γ , есть $\Theta_\gamma(\gamma)$ (соответственно $\Theta'_\gamma(\gamma)$). Оно также имеет подмножество $B^\times = \Theta_\gamma(\gamma) \setminus \{\gamma\}$, $(B'^\times = \Theta'_\gamma(\gamma) \setminus \{\gamma\})$. Значит, если $\Theta_\gamma = \Theta'_\gamma$, то $\Theta_\gamma(\gamma) = \Theta'_\gamma(\gamma)$. Тогда $B^\times = B'^\times$, что невозможно, так как $B \neq B'$.

Следовательно, справедливы соотношения $|\Lambda_{mt}| \leq |\Lambda_{W,\gamma}^S|$ и $\overline{\Lambda}_{W,\gamma}^S \subseteq \Lambda_{W,\gamma}^S$, где $\overline{\Lambda}_{W,\gamma}^S = \bigcup_{B \in V_m^{(t)}} \Lambda_{W,\gamma}^S(B)$. ■

Из доказательства утверждения 15 следуют равенства $\overline{\Lambda}_{W,\vec{0}}^S(B) = \Pi_{W,B}^S$, $\bigcup_{X \in V_m^{(t)}} \Pi_{W,X}^S = \overline{\Lambda}_{W,\vec{0}}^S$ и способ построения подмножества $\overline{\Lambda}_{W,\gamma}^S \subset \Lambda_{W,\gamma}^S$ мощности $|\overline{\Lambda}_{W,\gamma}^S| = |\Lambda_{mt}|$, где $W \leq V_m$, $\dim W = t$, γ — произвольный вектор из V_m .

I. Для каждого подпространства $B = \langle \beta_1, \dots, \beta_t \rangle \leq V_m$, где $\gamma \notin B$, $\dim B = t$, выполняем следующие шаги:

1. Полагаем:

$$\begin{aligned}V_m &= \langle \beta_1, \dots, \beta_t, \beta_{t+1}, \dots, \beta_m \rangle, \quad \beta_m = \gamma, \quad \overline{B} = \langle \beta_{t+1}, \dots, \beta_m \rangle, \\ \Theta_\gamma(\vec{0}) &= \{\vec{0}\} \cup (B^\times \oplus \gamma), \\ \Theta_\gamma(\delta) &= \Theta_\gamma(\vec{0}) \oplus \delta = \{\delta\} \cup (B^\times \oplus \delta \oplus \gamma), \quad \delta \in \overline{B}.\end{aligned}$$

2. Формируем все смежные классы $\alpha_1 \oplus W, \dots, \alpha_{2^{m-t}} \oplus W$ по подгруппе W в V_m .

3. Для каждого биективного отображения $h: \{1, \dots, 2^{m-t}\} \rightarrow \overline{B}$, $i^h = \delta_i$, полагаем: $\Lambda_\gamma^S(h, B) = \{g \in S(V_m) \mid \{\theta^g \mid \theta \in \alpha_{i^h} \oplus W\} = \Theta_\gamma(\delta_i), i = 1, \dots, 2^{m-t}\}$.

4. Находим $\Lambda_{W,\gamma}^S(B) = \bigcup_{h: \{1, \dots, 2^{m-t}\} \rightarrow \overline{B}} \Lambda_\gamma^S(h, B)$.

II. Находим $\Lambda_{W,\gamma}^S = \bigcup_{B \in V_m^{(t)}} \Lambda_{W,\gamma}^S(B)$.

Покажем, что для вектора $\gamma \in V_m$ существует связь между множествами $\overline{\Lambda}_{W,\gamma}^S$ и $\Lambda_{W,\vec{0}}^S(B)$, в частности, между множествами $\Pi_{W,B}^S$, где $B \in V_m^{(t)}$, $\dim W = t$.

Следствие 16. Пусть $V_m = \langle \beta_1, \dots, \beta_t, \beta_{t+1}, \dots, \beta_m \rangle$, $B = \langle \beta_1, \dots, \beta_t \rangle$, $\bar{B} = \langle \beta_{t+1}, \dots, \beta_m \rangle$, $\beta_m = \gamma$. Пусть также W — собственное подпространство из V_m , $\dim W = t \geq 1$, $\gamma \in V_m$, отображение $h_{W,B,\gamma}: V_m \rightarrow V_m$ задано равенством

$$\theta^{h_{W,B,\gamma}} = \begin{cases} \theta \oplus \gamma, & \text{если } \theta \notin \bar{B}, \\ \theta, & \text{если } \theta \in \bar{B}. \end{cases}$$

Тогда

$$\bar{\Lambda}_{W,\gamma}^S = \bigcup_{B \in V_m^{(t)}} \Lambda_{W,\bar{0}}^S(B) h_{W,B,\gamma} = \bigcup_{B \in V_m^{(t)}} \Pi_{W,B}^S h_{W,B,\gamma}.$$

Доказательство. Воспользуемся обозначениями утверждения 15. Покажем, что отображение $h_{W,B,\gamma}$ является подстановкой. Для любого $\delta \in \bar{B}$ имеем $h_{W,B,\gamma}: \delta \rightarrow \delta$, т. е. $h_{W,B,\gamma}$ стабилизирует подпространство $\bar{B}$ в целом.

Пусть θ — произвольный вектор из $V_m \setminus \bar{B}$. Тогда $\theta^{h_{W,B,\gamma}} = \theta \oplus \gamma$ и $\theta \oplus \gamma \notin \bar{B}$. Значит, $h_{W,B,\gamma}$ также стабилизирует множество $V_m \setminus \bar{B}$ в целом. Ясно, что равенство $\theta \oplus \gamma = \theta' \oplus \gamma$ для $\theta' \in V_m \setminus \bar{B}$ возможно тогда и только тогда, когда $\theta = \theta'$, т. е. $h_{W,B,\gamma} \in S(V_m)$.

Значит, для любого $\delta \in \bar{B}$ имеем

$$\begin{aligned} h_{W,B,\gamma}: B^\times \oplus \delta \oplus \gamma &\rightarrow B^\times \oplus \delta, \\ h_{W,B,\gamma}: B^\times \oplus \delta &\rightarrow B^\times \oplus \delta \oplus \gamma. \end{aligned}$$

Следовательно,

$$\begin{aligned} h_{W,B,\gamma}: \Theta_{\bar{0}}(\delta) &\rightarrow \Theta_\gamma(\delta), \\ h_{W,B,\gamma}: \Theta_\gamma(\delta) &\rightarrow \Theta_{\bar{0}}(\delta). \end{aligned}$$

Значит, $\Lambda_{W,\gamma}^S(B) = \Lambda_{W,\bar{0}}^S(B) h_{W,B,\gamma}$.

Нетрудно убедиться в том, что подстановки из множества $\Pi_{W,B}^S$ совпадают с подстановками из множества $\bar{\Lambda}_{W,\bar{0}}^S(B)$, т. е. $\Lambda_{W,\bar{0}}^S(B) = \Pi_{W,B}^S$.

Из доказательства утверждения 15 следует, что

$$\bar{\Lambda}_{W,\gamma}^S = \bigcup_{B \in V_m^{(t)}} \Lambda_{W,\gamma}^S(B) = \bigcup_{B \in V_m^{(t)}} \Lambda_{W,\bar{0}}^S(B) h_{W,B,\gamma} = \bigcup_{B \in V_m^{(t)}} \Pi_{W,B}^S h_{W,B,\gamma}. \blacksquare$$

Следующее утверждение показывает, что каждое из множеств $\Lambda_{W,\gamma}^S$ является подмножеством $\Lambda_{X,\bar{0}}^S$, где $W < X$.

Утверждение 17. Пусть X — собственное подпространство V_m , $\dim X = t + 1$, $t \in \{1, \dots, m - 2\}$. Тогда

$$\bigcup_{W \in V_m^{(t)}, \gamma \in V_m} \Lambda_{W, \gamma}^S \subseteq \Lambda_{X, \vec{0}}^S.$$

Доказательство. Пусть $X = \langle \beta_1, \dots, \beta_t, \beta_{t+1} \rangle$, $W = \langle \beta_1, \dots, \beta_t \rangle$, $\dim W = t$. Тогда для любых $g \in \Lambda_{W, \gamma}^S$ и $\alpha \in V_m$ справедливы равенства

$$\sum_{\theta \in \alpha \oplus W} \oplus \theta^g = \gamma, \quad \sum_{\theta \in \alpha \oplus \beta_{t+1} \oplus W} \oplus \theta^g = \gamma.$$

Сложив последние два равенства, получаем

$$\sum_{\theta \in \alpha \oplus W} \oplus \theta^g \oplus \sum_{\theta \in \alpha \oplus \beta_{t+1} \oplus W} \oplus \theta^g = \sum_{\theta \in \alpha \oplus \langle \beta_1, \dots, \beta_t, \beta_{t+1} \rangle} \oplus \theta^g = \gamma \oplus \gamma = \vec{0}.$$

Поэтому $\Lambda_{W, \gamma}^S \subseteq \Lambda_{X, \vec{0}}^S$ для любых $W \in V_m^{(t)}$, $\gamma \in V_m$. Отсюда следует, что

$$\bigcup_{W \in V_m^{(t)}, \gamma \in V_m} \Lambda_{W, \gamma}^S \subseteq \Lambda_{X, \vec{0}}^S. \blacksquare$$

Покажем, что задача описания множества

$$\Lambda_{W, X}^P = \left\{ h \in P(H) \mid \{ \alpha^{d_w(h)} \mid \alpha \in H \} = X \right\}$$

проще задачи описания множества $\Lambda_{W, X}^S$. В частности, получим точное значение для $|\Lambda_{W, X}^P|$.

Для произвольных подмножества $X = \{\lambda_1, \dots, \lambda_d\} \subseteq V_m$, вектора $\gamma = (\gamma_1, \dots, \gamma_{2^{m-1}}) \in V_m^{2^{m-1}}$, $(r_1, \dots, r_d) \in \mathbb{N}^d$, $r_1 + \dots + r_d = 2^{m-t}$, собственного подпространства $W < V_m$, $(V_m : W) = \{\alpha_1 \oplus W, \dots, \alpha_{2^{m-1}} \oplus W\}$ положим:

$$\begin{aligned} \Gamma_{t, X}(r_1, \dots, r_d) &= \\ &= \{ (\gamma_1, \dots, \gamma_{2^{m-t}}) \in V_m^{2^{m-t}} \mid |\{j \in \{1, \dots, 2^{m-t}\} \mid \gamma_j = \lambda_i\}| = r_i, i = 1, \dots, d \}, \\ \Theta_W(\gamma) &= \left\{ h \in P(V_m) \mid \alpha_i^{d_w(h)} = \gamma_i, i = 1, \dots, 2^{m-t} \right\}, \\ \Theta_{W, X}(r_1, \dots, r_d) &= \bigcup_{\gamma \in \Gamma_{t, X}(r_1, \dots, r_d)} \Theta_W(\gamma). \end{aligned}$$

Утверждение 18. Пусть W — собственное подпространство V_m , $\dim W = t \geq 1$, $X = \{\lambda_1, \dots, \lambda_d\}$ — произвольное подмножество из V_m , $(V_m : W) = \{\alpha_1 \oplus W, \dots, \alpha_{2^{m-1}} \oplus W\}$. Тогда:

1. $|\Theta_W(\gamma)| = 2^{m(2^m-2^t)}$;
2. $|\Theta_{W,X}(r_1, \dots, r_d)| = 2^{m(2^m-2^t)} \frac{2^{m-t}!}{r_1! \dots r_d!}$;
3. $|\Lambda_{W,X}^P| = \left(\sum_{i=0}^{d-1} (-1)^i \binom{d}{i} (d-i)^{2^{m-t}} \right) \cdot 2^{m(2^m-2^t)}$.

В частности, $|\Lambda_{W,\delta}^P| = 2^{m(2^m-2^t)}$.

Доказательство. Пусть $g \in \Lambda_{W,X}^P$. Очевидно, что для любого $\alpha'_i \in \alpha_i \oplus W$ выполняется равенство $(\alpha'_i)^{d_W(g)} = \alpha_i^{d_W(g)}$. Следовательно, достаточно рассматривать значения $d_W(g)$ на представителях смежных классов $\alpha_1, \dots, \alpha_{2^{m-t}}$.

Для произвольных $i \in \{1, \dots, 2^{m-t}\}$, $\gamma_i \in V_m$ равенство $\alpha_i^{d_W(h)} = \gamma_i$ справедливо для любых таких преобразований $h \in P(V_m)$, что для любого $\theta \in (\alpha_i \oplus W) \setminus \{\alpha_i\}$ образ θ^h равен произвольному вектору из V_m , а $\alpha_i^h = \gamma_i \oplus \sum_{\theta \in (\alpha_i \oplus W) \setminus \{\alpha_i\}} \theta^h$. Следовательно,

$$|\Theta_W(\gamma)| = \left((2^m)^{(2^t-1)} \right)^{2^{m-t}} = 2^{m(2^m-2^t)}.$$

Учитывая, что $|\Gamma_{t,X}(r_1, \dots, r_d)| = \frac{2^{m-t}!}{r_1! \dots r_d!}$, получаем

$$\begin{aligned} |\Theta_{W,X}(r_1, \dots, r_d)| &= \left| \bigcup_{\gamma \in \Gamma_{t,X}(r_1, \dots, r_d)} \Theta_W(\gamma) \right| = \sum_{\gamma \in \Gamma_{t,X}(r_1, \dots, r_d)} |\Theta_W(\gamma)| = \\ &= |\Theta_W(\gamma)| \cdot |\Gamma_{t,X}(r_1, \dots, r_d)| = 2^{m(2^m-2^t)} \frac{2^{m-t}!}{r_1! \dots r_d!}. \end{aligned}$$

С помощью формулы включения-исключения получаем, что число таких векторов $\gamma = (\gamma_1, \dots, \gamma_{2^{m-t}}) \in V_m^{2^{m-t}}$, что $\{\gamma_1, \dots, \gamma_{2^{m-t}}\} = X$, равно

$$\sum_{i=0}^{d-1} (-1)^i \binom{d}{i} (d-i)^{2^{m-t}}.$$

Значит,

$$\begin{aligned} |\Lambda_{W,X}^P| &= \sum_{(\gamma_1, \dots, \gamma_{2^m-t}) \in V_m^{2^m-t} : \{\gamma_1, \dots, \gamma_{2^m-t}\} = X} |\Theta_W(\gamma)| = \\ &= \left(\sum_{i=0}^{d-1} (-1)^i \binom{d}{i} (d-i)^{2^{m-t}} \right) \cdot (2^m)^{(2^t-1) \cdot 2^{m-t}}. \blacksquare \end{aligned}$$

Отметим, что из доказательства утверждения 18 непосредственно следует описание всех преобразований из множества $\Lambda_{W,X}^P$.

§ 4. Приближение подстановок сплетением групп

Укажем связь полученных результатов с некоторыми методами криптоанализа, в частности, с методом гомоморфизмов и разностным методом.

Пусть X — аддитивная абелева группа, $|X| = n = \omega r$, $\omega, r \in \mathbb{N}$. Рассмотрим l -раундовый алгоритм блочного шифрования. Пусть $K^{(i)}$ — множество всех раундовых ключей i -го раунда; $G^{(i)} = \{g_k^{(i)} | k \in K^{(i)}\}$ — множество раундовых функций i -го раунда; $G^{(i)} \subseteq S(X)$; $f_{k^{(i)}}^{(j)} = g_{k_1}^{(1)} \dots g_{k_j}^{(j)}$, $f_k^{(j)} \in S(X)$, $k^{(j)} = (k_1, \dots, k_j) \in K_1 \times \dots \times K_j = K^{(j)}$, $j = 1, \dots, l$, $G = G^{(1)} \dots G^{(l)}$; $S_\omega \circ S_r \leq S(X)$.

4.1. Разностный метод

Покажем, что разностный метод и некоторые его модификации сводятся к оценке расстояния между подстановками из $S(X)$ и группой $S_\omega \circ S_r \leq S(X)$.

Обозначим: $\{h_1, \dots, h_t\}^{-1} = \{h_1^{-1}, \dots, h_t^{-1}\}$ для $H = \{h_1, \dots, h_t\} \subseteq S(X)$; $\chi(g, h)$ — расстояние Хемминга между подстановками g, h , т.е. $\chi(g, h) = |\{\alpha \in X | g(\alpha) \neq h(\alpha)\}|$; X_ω^r — множество всех разбиений множества X на r блоков мощности ω каждый, $1 < \omega < |X|$; $B, B' \in X_\omega^r$; $B^g = \{b^g | b \in B\}$;

$$\begin{aligned} \text{Isom}(X_\omega^r; B, B') &= \{g \in S(X) | B^g = B'\}, \\ d(g, (B, B')) &= \min \{ \chi(g, h) | h \in \text{Isom}(X_\omega^r; B, B') \}, \\ d_{cp}(H, (B, B')) &= |H|^{-1} \sum_{h \in H} d(h, (B, B')) \end{aligned}$$

для $g \in S(X)$, $H \subseteq S(X)$. Назовем $d_{cp}(H, (B, B'))$ средним расстоянием между множествами H и $\text{Isom}(X_\omega^r; B, B')$.

Для произвольных $B, B' \in X_{\omega}^r$, $g \in S(X)$, $B^g = B'$ очевидны следующие соотношения:

- 1) $\text{Isom}(X_{\omega}^r; B, B) = S_{\omega} \int S_r$;
- 2) $\text{Isom}(X_{\omega}^r; B, B') = \text{Isom}(X_{\omega}^r; B', B)^{-1}$;
- 3) $\text{Isom}(X_{\omega}^r; B, B') = \text{Isom}(X_{\omega}^r; B, B) g$.

Из последних соотношений следует, что для $h, h' \in \text{Isom}(X_{\omega}^r; B, B')$ существуют $s, s' \in S_{\omega} \int S_r$, и $g \in S(X)$, где $B^g = B'$, со свойством $h = sg$, $h' = s'g$. Тогда $\chi(h, h') = \chi(s, s')$, т.е. расстояние Хемминга между подстановками h, h' равно расстоянию между соответствующими подстановками из группы $S_{\omega} \int S_r$. Следовательно, для нахождения или оценки расстояния между подстановками из множества $\text{Isom}(X_{\omega}^r; B, B')$ достаточно получить расстояние или оценку расстояния между подстановками из группы $S_{\omega} \int S_r$ при некоторой фиксированной системе импримитивности с параметрами (ω, r) .

Покажем, что разностный метод фактически использует оценки расстояния между множествами шифрующих преобразований $\{f_{k^{(l-1)}}^{(l-1)} | k^{(l-1)} \in K^{(l-1)}\}$, $K^{(l-1)} = K_1 \times \dots \times K_{l-1}$ и множеством $\text{Isom}(X_{\omega}^r; B, B')$, $B, B' \in X_{\omega}^r$. Напомним, что в разностном методе при атаке на l -раундовый алгоритм блочного шифрования рассматривается «усредненная» вероятность

$$p_{\varepsilon\gamma} = P \left\{ \alpha \in_U X, k^{(l-1)} \in_U K^{(1)} \times \dots \times K^{(l-1)} \mid f_{k^{(l-1)}}^{(l-1)}(\alpha \oplus \varepsilon) = f_{k^{(l-1)}}^{(l-1)}(\alpha) \oplus \gamma \right\} \approx \frac{\left| \left\{ \alpha \in X, k^{(l-1)} \in K^{(1)} \times \dots \times K^{(l-1)} \mid f_{k^{(l-1)}}^{(l-1)}(\alpha \oplus \varepsilon) = f_{k^{(l-1)}}^{(l-1)}(\alpha) \oplus \gamma \right\} \right|}{|X| \cdot |K^{(1)}| \cdot \dots \cdot |K^{(l-1)}|}$$

для $\varepsilon, \gamma \in X^{\times}$. Здесь $\in_U$ означает равномерное распределение элементов на множестве. При этом ищутся такие элементы $\varepsilon, \gamma \in X^{\times}$, что вероятность $p_{\varepsilon\gamma}$ является наибольшей.

Пусть $X \in \{V_m, GF(2^m)\}$, $n = 2^m$; такая ситуация встречается во многих алгоритмах блочного шифрования, например, в алгоритмах AES, DES, Anubis, Camellia, CAST. В этом случае разностный метод можно интерпретировать следующим образом.

Рассмотрим системы импримитивности группы $S_2 \int S_{2^m-1}$ вида $B_{\varepsilon} = \{\{\alpha, \alpha \oplus \varepsilon\} | \alpha \in V_m\}$, $\varepsilon \in V_m$. Тогда в разностном методе ищутся такие элементы $\varepsilon, \gamma \in V_m^{\times}$ и аппроксимирующее преобразование $\tilde{f}_{k^{(l-1)}}^{(l-1)} \in$

$\in \text{Isom} \left(X_2^{2^{m-1}}; B_\varepsilon, B_\gamma \right)$ преобразования $f_{k^{(l-1)}}^{(l-1)}$, где $k^{(l-1)} \in K^{(1)} \times \dots \times K^{(l-1)}$, что величина

$$p(\varepsilon, \gamma) = \frac{1}{2^m (|K^{(1)}| \cdot \dots \cdot |K^{(l-1)}|)} \sum_{k^{(l-1)} \in K^{(1)} \times \dots \times K^{(l-1)}} \chi \left(f_{k^{(l-1)}}^{(l-1)}, \tilde{f}_{k^{(l-1)}}^{(l-1)} \right)$$

является наименьшей. Это равносильно тому, что $\chi \left(f_{k^{(l-1)}}^{(l-1)}, \tilde{f}_{k^{(l-1)}}^{(l-1)} \right) = d \left(f_{k^{(l-1)}}^{(l-1)}, (B_\varepsilon, B_\gamma) \right)$ для всех $k^{(l-1)} \in K^{(1)} \times \dots \times K^{(l-1)}$, т. е. имеет место равенство

$$p(\varepsilon, \gamma) = \frac{1}{2^m (|K^{(1)}| \cdot \dots \cdot |K^{(l-1)}|)} \sum_{k^{(l-1)} \in K^{(1)} \times \dots \times K^{(l-1)}} d \left(f_{k^{(l-1)}}^{(l-1)}, (B_\varepsilon, B_\gamma) \right).$$

Покажем, что справедлива оценка

$$p(\varepsilon, \gamma) \leq 1 - p_{\varepsilon\gamma}.$$

Действительно, зафиксируем произвольный ключ $k^{(l-1)} \in K^{(1)} \times \dots \times K^{(l-1)}$, и пусть

$$\begin{aligned} \{ \alpha_1, \dots, \alpha_{t(k^{(l-1)})} \} &= \left\{ \alpha \in V_m \mid f_{k^{(l-1)}}^{(l-1)}(\alpha \oplus \varepsilon) = f_{k^{(l-1)}}^{(l-1)}(\alpha) \oplus \gamma \right\}, \\ \{ \alpha_{t(k^{(l-1)})+1}, \dots, \alpha_n \} &= V_m \setminus \{ \alpha_1, \dots, \alpha_{t(k^{(l-1)})} \}. \end{aligned}$$

Полагая $\tilde{f}_{k^{(l-1)}}^{(l-1)}(\alpha) = f_{k^{(l-1)}}^{(l-1)}(\alpha)$ для всех $\alpha \in \{ \alpha_1, \dots, \alpha_{t(k^{(l-1)})} \}$, имеем

$$d \left(f_{k^{(l-1)}}^{(l-1)}, (B_\varepsilon, B_\gamma) \right) \leq \chi \left(f_{k^{(l-1)}}^{(l-1)}, \tilde{f}_{k^{(l-1)}}^{(l-1)} \right) \leq 2^m - t(k^{(l-1)}).$$

Следовательно,

$$p(\varepsilon, \gamma) \leq \frac{1}{2^m (|K^{(1)}| \cdot \dots \cdot |K^{(l-1)}|)} \sum_{k^{(l-1)} \in K^{(1)} \times \dots \times K^{(l-1)}} (2^m - t(k^{(l-1)})) = 1 - p_{\varepsilon\gamma}.$$

Значит, нахождение разностей с максимальной вероятностью в разностном методе можно трактовать как оценку среднего расстояния, на которое преобразования из множества $F^{(l-1)} = \{ f_{k^{(l-1)}}^{(l-1)} \mid k^{(l-1)} \in K^{(1)} \times \dots \times K^{(l-1)} \}$ удалены от множества $\text{Isom} \left(X_2^{2^{m-1}}; B_\varepsilon, B_\gamma \right)$. Кроме того, фактически при

$\varepsilon = \gamma$ вычисляется среднее расстояние от множества $F^{(l-1)}$ до группы сплетения $S_2 \int S_{2^{m-1}}$ и ищется система импримитивности B_ε , при которой данное расстояние минимально.

Поэтому имеется связь разностного метода со следующей задачей: для заданного множества преобразований $H \subseteq S(X)$ оценить среднее расстояние $d_{cp}(H, (B_\varepsilon, B_\varepsilon))$ до группы $S_2 \int S_{2^{m-1}}$. Аналогично рассматривается задача оценки среднего расстояния $d_{cp}(H, (B_\varepsilon, B_\gamma))$ до множества $\text{Isom}(X_2^{2^{m-1}}; B_\varepsilon, B_\gamma)$, если $\varepsilon \neq \gamma$.

В общем случае для произвольного множества $X, |X| = n = \omega r$, можно рассматривать следующее обобщение разностного метода, основанное на построении аппроксимирующих преобразований из множества $\text{Isom}(X_\omega^r; B, B')$ для некоторых систем импримитивности $B, B' \in X_\omega^r$.

Выбираем параметры $\omega, r, n = \omega r$. Находим пары $B, B' \in X_\omega^r$ и аппроксимирующее преобразование $\tilde{f}_{k^{(l-1)}}^{(l-1)} \in \text{Isom}(X_\omega^r; B, B')$ преобразования $f_{k^{(l-1)}}^{(l-1)}$ с минимальной величиной

$$p(B, B') = \frac{1}{|X| \cdot (|K^{(1)}| \cdot \dots \cdot |K^{(l-1)}|)} \sum_{k^{(l-1)} \in K^{(1)} \times \dots \times K^{(l-1)}} \chi(f_{k^{(l-1)}}^{(l-1)}, \tilde{f}_{k^{(l-1)}}^{(l-1)}).$$

Это равносильно равенству $\chi(f_{k^{(l-1)}}^{(l-1)}, \tilde{f}_{k^{(l-1)}}^{(l-1)}) = d(f_{k^{(l-1)}}^{(l-1)}, (B, B'))$ для всех $k^{(l-1)} \in K^{(1)} \times \dots \times K^{(l-1)}$, т. е. справедливо равенство

$$\begin{aligned} p(B, B') &= \frac{1}{|X| \cdot (|K^{(1)}| \cdot \dots \cdot |K^{(l-1)}|)} \sum_{k^{(l-1)} \in K^{(1)} \times \dots \times K^{(l-1)}} d(f_{k^{(l-1)}}^{(l-1)}, (B, B')) = \\ &= \frac{1}{|X|} d_{cp}(\{f_{k^{(l-1)}}^{(l-1)} | k^{(l-1)} \in K^{(1)} \times \dots \times K^{(l-1)}\}, (B, B')). \end{aligned}$$

Метод нахождения раундового ключа на основе построения аппроксимирующих преобразований из множества $\text{Isom}(X_\omega^r; B, B')$ для множества преобразований $\{f_{k^{(l-1)}}^{(l-1)} | k^{(l-1)} \in K^{(1)} \times \dots \times K^{(l-1)}\}$ можно описать следующим образом.

Вход: число $t \in \mathbb{N}; 2 \leq t \leq \omega$; системы импримитивности $B = \{B_1, \dots, B_r\}, B' = \{B'_1, \dots, B'_r\}$ группы $S_\omega \int S_r$; t -граммы блоков открытых текстов $(\alpha_1^{(1,1)}, \dots, \alpha_t^{(1,1)}), \dots, (\alpha_1^{(d,1)}, \dots, \alpha_t^{(d,1)})$, где $\{\alpha_1^{(j,1)}, \dots, \alpha_t^{(j,1)}\} \subseteq B_{i_j}$ для некоторых $i_j \in \{1, \dots, r\}, j = 1, \dots, d$.

I. Для $j = 1, \dots, d$ находим соответствующие t -граммы шифртекстов $(\alpha_1^{(j,l)}, \dots, \alpha_t^{(j,l)}) = (f_{k^{(l)}}^{(l)}(\alpha_1^{(j,1)}), \dots, f_{k^{(l)}}^{(l)}(\alpha_t^{(j,1)}))$.

II. Для каждого $k_l^* \in K^{(l)}$ выполняем:

1. $v(k_l^*) = 0$.

2. Для $j = 1, \dots, d$ расшифровываем t -грамму шифртекста $(\alpha_1^{(j,l)}, \dots, \alpha_t^{(j,l)})$ на ключе k_l^* и проверяем, существует ли $c_j \in \{1, \dots, r\}$, для которого $\{(g_{k_l^*}^{(l)})^{-1}(\alpha_1^{(j,l)}), \dots, (g_{k_l^*}^{(l)})^{-1}(\alpha_t^{(j,l)})\} \subseteq B_{c_j}$. Если такое c_j существует, то полагаем $v(k_l^*) \leftarrow v(k_l^*) + 1$.

III. Истинным раундовым ключом k_l считается элемент k_l^* с наибольшим значением $v(k_l^*)$.

Выход: раундовый ключ k_l .

Будем считать, что блочная шифрсистема может быть успешно атакована, если $p(B, B') > |X|^{\omega-1}$. Отметим, что метод усеченных разностей как раз попадает в данную схему. Как и в разностном методе, сложнее всего подобрать «наилучшие» системы импримитивности $B = \{B_1, \dots, B_r\}$, $B' = \{B'_1, \dots, B'_r\}$.

В разностном методе при $X \in \{V_m, GF(2^m)\}$, $r = 2^{m-1}$, $\omega = 2$, $B = B_\varepsilon$, $B' = B_\gamma$, $\varepsilon, \gamma \in V_m^*$, имеем $t = \omega = 2$, $(\alpha_1^{(j,1)}, \alpha_2^{(j,1)}) = (\alpha_1^{(j,1)}, \alpha_1^{(j,1)} \oplus \varepsilon)$. Кроме того, элемент $c_j \in \{1, \dots, r\}$, для которого $\{(g_{k_l}^{(l)})^{-1}(\alpha_1^{(j,l)}), (g_{k_l}^{(l)})^{-1}(\alpha_2^{(j,l)})\} \subseteq B_{c_j}$, существует тогда и только тогда, когда $(g_{k_l}^{(l)})^{-1}(\alpha_1^{(j,l)}) \oplus (g_{k_l}^{(l)})^{-1}(\alpha_2^{(j,l)}) = \gamma$.

Покажем, что для произвольного множества преобразований H для применимости описанного подхода достаточно уметь находить расстояние до группы $S_\omega \int S_r$ с системой импримитивности $B \in X_\omega^r$. Действительно, пусть B, B' — произвольные различные системы импримитивности из X_ω^r , $B^g = B'$, $g \in S(X)$, $H = \{h_1, \dots, h_t\}$, $f_i \in \text{Isom}(X_\omega^r; B, B')$ — преобразование, аппроксимирующее h_i , $i = 1, \dots, t$. Тогда $f_i = s_i g$, где подстановка $s_i \in S_\omega \int S_r$ сохраняет систему импримитивности B , $i = 1, \dots, t$. Поскольку $\chi(h_i, f_i) = \chi(h_i, s_i g) = \chi(h_i g^{-1}, s_i)$ для $i = 1, \dots, t$, постольку для нахождения среднего расстояния $d_{cp}(H, (B, B'))$ между множествами $H, \text{Isom}(X_\omega^r; B, B')$ достаточно найти среднее расстояние $d_{cp}(H g^{-1}, (B, B))$ между множеством H и группой $S_\omega \int S_r$ с системой импримитивности B . Таким образом,

$$d_{cp}(H g^{-1}, (B, B)) = d_{cp}(H, (B, B')).$$

В связи с этим возникает задача нахождения минимального расстояния при заданной системе импримитивности от подстановки $g \in S(X)$ до группы

$S_w \int S_r$. В общем случае ее можно сформулировать следующим образом: найти среднее расстояние $d_{cr}(H, (B, B))$ между множеством H и группой $S_w \int S_r$ с системой импримитивности B .

4.2. Метод гомоморфизмов

Покажем также, что имеет место связь между аппроксимацией раундовых функций подстановками из группы сплетения $S_w \int S_r$ и методом гомоморфизмов.

Пусть $F(H, H') = \{\lambda | \lambda: H \rightarrow H'\}$, $H, H' \subseteq S(X)$; $(S_w \int S_r, B)$ — группа сплетения $S_w \int S_r$ с системой импримитивности $B \in X_w^r$; $\tilde{G}$ — некоторое подмножество из группы $(S_w \int S_r, B)$; $\rho: G \rightarrow \tilde{G}$ — взаимно однозначное отображение; ϕ — естественный гомоморфизм группы $S_w \int S_r$ в группу S_r , действующую на множестве X' , $|X'| = r$, $\psi: X \rightarrow X'$. Подстановку $\rho(g)$ назовем (B, ρ) -аппроксимацией подстановки $g \in G$ в группе $S_w \int S_r$. Пусть

$$\delta_{B,\rho}(g, \tilde{G}) = |X|^{-1} \cdot \left| \left\{ \alpha \in X \mid \psi(\alpha^g) \neq \psi(\alpha)^{\phi(\rho(g))} \right\} \right|,$$

$$\delta_{B,\rho}(G, \tilde{G}) = |G|^{-1} \cdot \sum_{g \in G} \delta_{B,\rho}(g, \tilde{G}).$$

Метод гомоморфизмов применим, если существуют такие $B \in X_w^r$, $\tilde{G} \subseteq (S_w \int S_r, B)$, $\rho \in F(G, \tilde{G})$, что имеет место равенство

$$\delta_{B,\rho}(G, \tilde{G}) = \min \{ \delta_{B',\rho'}(G, G') \mid B' \in X_w^r, G' \subseteq (S_w \int S_r, B'), \rho' \in F(G, G') \}.$$

В этом случае вместо нахождения ключа $k^{(l)}$ преобразования $f_{k^{(l)}}^{(l)} \in_U G$ можно найти часть ключа или весь ключ $\tilde{k}^{(l)}$ соответствующего преобразования $\rho(f_{k^{(l)}}^{(l)})$ с помощью гомоморфизма ϕ с «усредненной вероятностью» $\delta_{B,\rho}(G, \tilde{G})$.

В связи с этим возникает задача оценки расстояния $d(g, S_w \int S_r)$ между произвольной подстановкой из $S(X)$ и группой $S_w \int S_r$, действующей на множестве X .

Список литературы

1. Chaum D., Evertse J. H. Cryptanalysis of DES with a reduced number of rounds sequences: of linear factors in block ciphers // CRYPTO'85 // Lect. Notes Comput. Sci. — 1986. — V. 218. — P. 192–211.

2. *Evertse J. H.* Linear structures in blockciphers // EUROCRYPT'87 // Lect. Notes Comput. Sci. — 1987. — V. 304. — P. 249–266.
3. *Knudsen L. R.* Truncated and higher order differentials // FSE'95 // Lect. Notes Comput. Sci. — 1995. — V. 1008. — P. 196–211.
4. *Алексейчук А. Н., Скрынник Е. В.* Классы отображений с тривиальной линейной структурой над конечным полем // Реєстрація, зберігання і обробка даних. — 2008. — Т. 10. № 3. — С. 80–88.
5. *Логачев О. А., Сальников А. А., Яценко В. В.* Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004. — 470 с.
6. *Пудовкина М. А.* Линейные структуры групп подстановок над конечным модулем // Прикладная дискретная математика. — Томск: ТГУ, 2008. — Т. 1. — С. 25–28.
7. *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. — М.: МЦНМО, 2004.
8. Энциклопедия дискретной математики. — М.: «Большая Российская энциклопедия», 2004. — 382 с.