М. В. Величко, А. А. Осиновская, И. Д. Супруненко, Группа, порожденная тактовыми подстановками криптосистемы BelT, *Тр. Ин-та матем.*, 2007, том 15, номер 1, 15–21

Национальная академия наук Беларуси
Труды Института математики. 2007. Том 15. № 1. С. 15–21

УДК 512.542.74

ГРУППА, ПОРОЖДЕННАЯ ТАКТОВЫМИ ПОДСТАНОВКАМИ КРИПТОСИСТЕМЫ BelT

М. В. Величко, А. А. Осиновская, И. Д. Супруненко

Белорусский государственный педагогический университет
Институт математики НАН Беларуси
e-mail: mar_vel@rambler.ru, anna@im.bas-net.by, suprunenko@im.bas-net.by
Поступила 21.08.2006

Исследуется группа Г, порожденная тактовыми подстановками криптосистемы BelT [1], принадлежащими фиксированному такту t. Доказано, что эта группа является знакопеременной группой степени 2^{128}.

Алгоритм блочного шифрования BelT с длиной блока 128 битов и 256-битовым ключом разработан С.В. Агиевичем, В.А. Галинским, Н.Д. Микуличем и Ю.С. Хариным [1, 2]. Он обладает высокой производительностью, сравнимой с таковой для ведущих мировых алгоритмов шифрования (RC6, Rijndael, MARS, Twofish, Serpent, DFC, Safer+). Этот алгоритм позволяет выполнять шифрование на процессоре Pentium-200 со скоростью 18.73 Мбит/с, а на процессоре Pentium III-1000 — со скоростью 187.7 Мбит/с. Дополнительным достоинством алгоритма является быстрый, фактически не требующий вычислений способ определения тактовых ключей.

Всюду в дальнейшем Σ_n и A_n — симметрическая и знакопеременная группы степени n; $\mathcal{A}^n$ — множество всех слов длины n в алфавите $\mathcal{A} = \{0, 1\}$; $w\|v$ — конкатенация

$$w_1 \dots w_n v_1 \dots v_m$$

слов $w = w_1 \dots w_n$ и $v = v_1 \dots v_m$. Предполагаем, что слово $X \in \mathcal{A}^{128}$ записано в виде $X_1\|X_2\|X_3\|X_4$, где $X_i \in \mathcal{A}^{32}$, а каждое X_i — в виде $X_{i1}\|X_{i2}\|X_{i3}\|X_{i4}$, где $X_{ij} \in \mathcal{A}^8$. Слово $u \in \mathcal{A}^{32}$ записываем как $u = u_1\|u_2\|u_3\|u_4$, где $u_i \in \mathcal{A}^8$. Нулевое слово длины 8 или 32 обозначается символом 0. Из контекста всегда ясно, о слове какой длины идет речь.

Далее $\overline{v}$ — число $2^7 v_1 + 2^6 v_2 + \ldots + v_8$ для слова $v = v_1 \dots v_8 \in \mathcal{A}^8$; $\overline{u}$ — число

$$\overline{u_1} + 2^8\overline{u_2} + 2^{16}\overline{u_3} + 2^{24}\overline{u_4}$$

для слова $u \in \mathcal{A}^{32}$; $\langle V\rangle_i$ — слово $v \in \mathcal{A}^i$ такое, что $\overline{v} \equiv V (\mathrm{mod}\, 2^i)$, $i = 8$ или 32; $u \oplus v$ — поразрядная по модулю 2 сумма двоичных слов $u, v \in \mathcal{A}^{32}$; $u \boxplus v$ — слово $\langle \overline{u} + \overline{v}\rangle_{32}$ для слов $u, v \in \mathcal{A}^{32}$; $u \boxminus v$ — слово $w \in \mathcal{A}^{32}$ такое, что $u = v \boxplus w$; $\lambda(u)$ — слово $\left\langle 2\overline{u} + \left\lfloor \dfrac{\overline{u}}{2^{31}} \right\rfloor \right\rangle_{32}$ для слова $u \in \mathcal{A}^{32}$; $a \leftarrow u$ — запись значения u в регистр a; $a \leftrightarrow b$ — перестановка значений регистров a и b; S_{32} — преобразование множества $\mathcal{A}^{32}$, которое ставит в соответствие слову $u \in \mathcal{A}^{32}$ слово

$$S_{32}(u) = S(u_1)\|S(u_2)\|S(u_3)\|S(u_4),$$

где подстановка $S : \mathcal{A}^8 \to \mathcal{A}^8$ задается в работе [2, табл. 1]. Положим $G_r(u) = \lambda^r(S_{32}(u))$.

Описание алгоритма BelT. Этот алгоритм предназначен для зашифрования и расшифрования слов $X \in \mathcal{A}^{128}$ на ключе $\theta \in \mathcal{A}^{256}$. Ключу $\theta = \theta_1 \| \dots \| \theta_8$, $\theta_i \in \mathcal{A}^{32}$, ставятся в соответствие слова $\kappa_i \in \mathcal{A}^{32}$. При зашифровании κ_i является i-м элементом последовательности

$$\theta_1, \theta_2, \dots, \theta_8, \theta_1, \dots, \theta_8, \dots$$

Для криптопреобразования слова $X \in \mathcal{A}^{128}$ используются 32-разрядные регистры a, b, c, d, первоначально содержащие значения $a \leftarrow X_1$, $b \leftarrow X_2$, $c \leftarrow X_3$, $d \leftarrow X_4$. Криптопреобразование состоит в выполнении объединенных в такты вычислений над содержимым регистров. Дополнительно используется вспомогательный 32-разрядный регистр e. При зашифровании выполняются такты $1, 2, \dots, 8$. На t-м такте зашифрования выполняются шаги:

1) $b \leftarrow b \oplus G_5(a \boxplus \kappa_{7t-6})$;
2) $c \leftarrow c \oplus G_{21}(d \boxplus \kappa_{7t-5})$;
3) $a \leftarrow a \boxminus G_{13}(b \boxplus \kappa_{7t-4})$;
4) $e \leftarrow G_{21}(b \boxplus c \boxplus \kappa_{7t-3}) \oplus \langle t \rangle_{32}$;
5) $b \leftarrow b \boxplus e$;
6) $c \leftarrow c \boxminus e$;
7) $d \leftarrow d \boxplus G_{13}(c \boxplus \kappa_{7t-2})$;
8) $b \leftarrow b \oplus G_{21}(a \boxplus \kappa_{7t-1})$;
9) $c \leftarrow c \oplus G_5(d \boxplus \kappa_{7t})$;
10) $a \leftrightarrow b$;
11) $c \leftrightarrow d$;
12) $b \leftrightarrow c$.

Обозначим через Γ_t группу, порожденную всеми подстановками t-го такта с фиксированными параметрами κ_{7t-4}, κ_{7t-3} и κ_{7t-2}.

Теорема. $\Gamma = \Gamma_t = A_{2^{128}}$.

Теорема показывает, что модификации шагов 3)–7) алгоритма BelT не уменьшают группу, порожденную его тактовыми подстановками.

При доказательстве основных результатов использовались компьютерные вычисления. Программы имеются у авторов.

Далее считаем такт t фиксированным. Обозначим через St стабилизатор нулевого слова в Γ_t.

Определение. Назовем слово $v \in \mathcal{A}^8$ словом общего положения, если $8 \leq \overline{v} \leq 238$. Слово $u \in \mathcal{A}^{32}$ является словом общего положения, если все u_i — слова общего положения.

Лемма 1. *Группы* Γ *и* $\Gamma_t \subseteq A_{2^{128}}$.

Доказательство. При $\beta_0, \dots, \beta_6 \in \mathcal{A}^{32}$ обозначим символом $h(\beta_0, \dots, \beta_6)$ подстановку из $\Sigma_{2^{128}}$, соответствующую t-му такту алгоритма при значениях ключа $\kappa_{7-i} = \beta_i$. Элемент $h(\beta_0, \dots, \beta_6)$ есть произведение 10 подстановок, соответствующих шагам 1), 2), 3), 4)–6), 7), 8), 9), 10), 11) и 12). Нетрудно заметить, что каждая из этих подстановок четна при любых значениях ключа. Поэтому Γ и $\Gamma_t \subseteq A_{2^{128}}$.

Лемма 2. *Группа* Γ_t *не стабилизирует нулевое слово.*

Доказательство. Доказательство почти очевидно. Выбрав произвольные значения κ_{7t-5} и κ_{7t-6}, можно подобрать такие κ_{7t} и κ_{7t-1}, что подстановка, являющаяся результатом выполнения шагов 1)–9) такта, переводит нулевое слово в ненулевое. Ясно, что это справедливо и для тактовой подстановки, соответствующей данному ключу.

Лемма 3. *Для любого слова* $u \in \mathcal{A}^8$ *общего положения и произвольного слова* $v \in \mathcal{A}^8$ *существует набор* $\delta_1, \ldots, \delta_{2l} \in \mathcal{A}^8$ *такой, что*

$$S(\delta_1) \oplus \ldots \oplus S(\delta_{2l}) = 0, \quad \overline{\delta_i} + \overline{u} < 256, \quad S(\langle \overline{\delta_1} + \overline{u} \rangle_8) \oplus \ldots \oplus S(\langle \overline{\delta_{2l}} + \overline{u} \rangle_8) = v.$$

При этом $2 \leq l \leq 6$.

Доказательство. Лемма доказана с помощью компьютерных вычислений (см. Приложение А).

Предложение 1. *Стабилизатор нулевого слова в группе* Γ_t *действует транзитивно на множестве всех ненулевых слов.*

Доказательство. При $\sigma,\ \sigma_1,\ \sigma_2 \in \mathcal{A}^{32}$ пусть $g(\sigma),\ g'(\sigma)$ и $g_i(\sigma_1, \sigma_2) \in A_{2^{128}}\ (1 \leq i \leq 4)$ — подстановки, определяемые следующим образом:

$g(\sigma) : X \mapsto X_1 \| X_2 \oplus G_5(X_1 \boxplus \sigma) \| X_3 \| X_4$;

$g'(\sigma) : X \mapsto X_1 \| X_2 \| X_3 \| X_4 \oplus G_5(X_2 \boxplus \sigma)$;

$g_1(\sigma_1, \sigma_2) :\ X \mapsto X_1 \oplus G_{21}(X_3 \boxplus \sigma_1) \oplus G_{21}(X_3 \boxplus \sigma_2) \| X_2 \| X_3 \| X_4$;

$g_2(\sigma_1, \sigma_2) :\ X \mapsto X_1 \| X_2 \oplus G_5(X_1 \boxplus \sigma_1) \oplus G_5(X_1 \boxplus \sigma_2) \| X_3 \| X_4$;

$g_3(\sigma_1, \sigma_2) :\ X \mapsto X_1 \| X_2 \| X_3 \oplus G_{21}(X_4 \boxplus \sigma_1) \oplus G_{21}(X_4 \boxplus \sigma_2) \| X_4$;

$g_4(\sigma_1, \sigma_2) :\ X \mapsto X_1 \| X_2 \| X_3 \| X_4 \oplus G_5(X_2 \boxplus \sigma_1) \oplus G_5(X_2 \boxplus \sigma_2)$.

Покажем, что $g_i(\sigma_1, \sigma_2) \in \Gamma_t$ при $1 \leq i \leq 4$. Легко видеть, что $g_i(\sigma_1, \sigma_2),\ 1 \leq i \leq 4,$ — инволюции. Фиксируем $\beta_0, \beta_1, \ldots, \beta_5 \in \mathcal{A}^{32}$. Положим

$$h_i = h(\beta_0, \beta_1, \ldots, \beta_5, \sigma_i), \quad i = 1, 2.$$

Тогда $h_i = fg(\sigma_i)$, где $f \in A_{2^{128}}$, и $g_2(\sigma_1, \sigma_2) = h_1^{-1} h_2 \in \Gamma_t$. Заметим, что подстановки шагов 1) и 2) каждого такта коммутируют, это верно и для шагов 8) и 9). Поменяв местами шаги 1) и 2) и рассуждая, как при $i = 2$, получаем, что $g_3(\sigma_1, \sigma_2) \in \Gamma_t$. Пусть l — подстановка, получающаяся в результате выполнения шагов 10)–12); $h'_i = h(\sigma_1, \gamma_1, \ldots, \gamma_6)$, где $\gamma_j \in \mathcal{A}^{32},\ i = 1, 2$. Тогда $h'_i = lg'(\sigma_i)f'$, где $f' \in A_{2^{128}}$, и подстановка

$$h'_1 (h'_2)^{-1} = lg'(\sigma_1) g'(\sigma_2) l^{-1} = g_4(\sigma_1, \sigma_2) \in \Gamma_t.$$

Аналогично показываем, что $g_1(\sigma_1, \sigma_2) \in \Gamma_t$, поменяв местами шаги 8) и 9).

При $\sigma_1, \ldots, \sigma_{2l} \in \mathcal{A}^{32}$ положим $g_i(\sigma_1, \ldots, \sigma_{2l}) = g_i(\sigma_1, \sigma_2) \ldots g_i(\sigma_{2l-1}, \sigma_{2l})$. Обозначим через St^i подгруппу, порожденную всеми $g_i(\sigma_1, \ldots, \sigma_{2l}) \in St$. Нетрудно видеть, что подгруппа St^i абелева. Пусть St^0 — подгруппа, порожденная St^1, St^2, St^3 и St^4. Покажем, что St^0 действует транзитивно на множестве ненулевых слов. Так как λ — биективное линейное преобразование, то $g_i(\sigma_1, \ldots, \sigma_{2l}) \in St^i$ тогда и только тогда, когда

$$S_{32}(\sigma_1) \oplus S_{32}(\sigma_2) \oplus \ldots \oplus S_{32}(\sigma_{2l}) = 0.$$

Положим $\tau = (1, 2, 4, 3) \in \Sigma_4$ (τ — цикл в симметрической группе степени 4). Нетрудно заметить, что преобразование λ является линейным оператором. Используя лемму 3 и свойства оператора λ, можно доказать утверждение А.

Утверждение А. *Пусть* $X \in \mathcal{A}^{128}$ *и* X_i *— слово общего положения* $(1 \leq i \leq 4)$. *Тогда для любого* $W \in \mathcal{A}^{32}$ *существует элемент* $\gamma \in St^{\tau(i)}$ *такой, что* $\gamma(X) = Z_1 \| Z_2 \| Z_3 \| Z_4$ *с* $Z_{\tau(i)} = X_{\tau(i)} \oplus W$ *и* $Z_j = X_j$ *при* $j \neq \tau(i)$.

Докажем, что с помощью преобразований из St^0 можно перевести слово $X \in \mathcal{A}^{128}$ с подсловом X_1 общего положения в произвольное слово $Y = Y_1 \| Y_2 \| Y_3 \| Y_4,\ Y_i \in \mathcal{A}^{32}$, у которого

хотя бы одно из подслов Y_1, Y_2, Y_3, Y_4 общего положения. Действительно, из утверждения А следует, что для любых слов $A_1, A_2, A_3, A_4 \in \mathcal{A}^{32}$ существуют элементы $s_1 = g_1^1 g_3^1 g_4^1 g_2^1$, $s_2 = g_2^2$, $s_3 = g_3^3 g_4^3 g_2^3$, $s_4 = g_4^4 g_2^4$ такие, что $g_l^i \in St^l$ $(i, l = 1, 2, 3, 4)$ и $s_i(X) = Z^i$ с $Z_i^i = A_i$. Поэтому если Y_j — слово общего положения, то существует элемент $s \in St^0$ такой, что $s(X) = Z$ и $Z_j = Y_j$. Пусть $k_i = \tau^i(j)$, $i = 1, 2, 3$. Рассуждая для слова Z, как выше для X, убедимся, что существуют элементы $q_i \in St^0$ такие, что $(q_3(Z))_{k_3} = Y_{k_3}$, $(q_3(Z))_j = Y_j$, $(q_2 q_3(Z))_k = Y_k$ при $k = k_2, k_3, j$ и $q_1 q_2 q_3(Z) = Y$. Таким образом, установлено, что все слова $X \in \mathcal{A}^{128}$, у которых хотя бы одно подслово X_i общего положения, лежат в одной St^0-орбите.

При $1 \le i \le 4$ обозначим через $\Omega_i \subset \mathcal{A}^{32}$ совокупности слов $u \in \mathcal{A}^{32}$ таких, что хотя бы i из подслов u_1, u_2, u_3, u_4 являются словами общего положения. Ясно, что Ω_4 — это множество всех слов общего положения. Используя утверждение А и явную конструкцию оператора λ, покажем, что если у слова $X \in \mathcal{A}^{128}$ есть хотя бы одно подслово $X_i \in \Omega_j$, то в St^0-орбите слова X содержится слово $Y \in \mathcal{A}^{128}$, у которого хотя бы одно подслово $Y_k \in \Omega_{j+1}$, $1 \le i, k \le 4$, $1 \le j \le 4$. Отсюда следует, что все слова $X \in \mathcal{A}^{128}$, у которых хотя бы одно подслово $X_i \in \Omega_1$, лежат в одной St^0-орбите.

Теперь пусть $X \in \mathcal{A}^{128}$, $X \ne 0$ и все X_i не являются словами общего положения, т.е. $\overline{X_{ij}} < 8$ либо $\overline{X_{ij}} > 238$ для любых i и j. Для завершения доказательства предложения достаточно установить, что в St^0-орбите слова X есть слово Y с $Y_i \in \Omega_1$ хотя бы для одного i. Тогда все ненулевые слова лежат в одной St^0-орбите. Проанализируем различные возможности, при которых все X_i не являются словами общего положения.

Пусть $238 < \overline{X_{ij}} < 246$ для некоторых i и j. С использованием компьютерных вычислений (см. Приложение А) установлено, что существуют слово $Z \in \mathcal{A}^{32}$ с $\overline{Z_j} = 29$ и элемент $\sigma \in St^i$ такие, что $\sigma(X)_i = X_i \oplus \lambda^5(Z)$ или $X_i \oplus \lambda^{21}(Z)$. Отсюда следует, что слово X лежит в одной St^i-орбите со словом Y требуемого вида. Если $0 < \overline{X_{ij}} < 8$, то справедливо аналогичное утверждение, только $\overline{Z_j} = 142$.

Пусть все ненулевые $\overline{X_{ij}} \ge 246$. Выберем i и j с $X_{ij} \ne 0$ и положим $u = X_{ij}$. С помощью компьютерных вычислений установлено, что в этом случае существуют $\delta_1, \delta_2, \delta_3, \delta_4 \in \mathcal{A}^8$ со следующими свойствами:

а) $S(\delta_1) \oplus S(\delta_2) \oplus S(\delta_3) \oplus S(\delta_4) = 0$;

б) $\overline{\delta_k} + \overline{u} \ge 256$ для $1 \le k \le 4$;

в) если $\delta'_k \in \mathcal{A}^8$ и $\overline{\delta'_k} = \overline{u} + \overline{\delta'_k} - 256$, то $S(\delta'_1) \oplus S(\delta'_2) \oplus S(\delta'_3) \oplus S(\delta'_4) = 01101101$ и $\overline{S(\delta'_1) \oplus S(\delta'_2) \oplus S(\delta'_3) \oplus S(\delta'_4)} = 109$.

Используя этот факт и свойства оператора λ, можно показать, что в St^i-орбите слова X есть искомый элемент Y. Предложение доказано.

Следствие. *Группа Γ_t 2-транзитивна.*

Доказательство. Из леммы 2 и предложения 1 вытекает, что Γ_t-орбита нулевого слова есть все множество $\mathcal{A}^{128}$. Далее из предложения 1 следует 2-транзитивность.

Предложение 2. *Группа St не сопряжена с подгруппой группы $GL(128, 2)$ в группе $\Sigma_{2^{128}}$.*

Доказательство. Очевидно, что порядок множества неподвижных точек любого элемента группы $GL(128, 2)$ есть степень числа 2, так как эти точки образуют подпространство пространства слов длины 128. Поэтому достаточно указать элемент $g \in St$ с другим порядком множества неподвижных точек. Положим $k_1 = 17$, $k_2 = 11$, $k_3 = 7$, $k_4 = 0$ и $\delta_i = \langle k_i \rangle_{32}$. Тогда $g = g_1(\delta_1, \delta_2, \delta_3, \delta_4) \in St^1$. Для любого $w \in \mathcal{A}_8$ имеем $\langle \overline{w} + k_i \rangle_{32} = v_i \| z_i \| 0 \| 0$, при этом всегда $\overline{z_i} = 0$ или 1. Оказалось, что существует ровно три слова w таких, что все $z_i = 0$ и $S(v_1) \oplus S(v_2) \oplus S(v_3) \oplus S(v_4) = 0$, и не существует таких слов w, у которых

$S(v_1) \oplus S(v_2) \oplus S(v_3) \oplus S(v_4) = 0$, а $\overline{z_1} + \overline{z_2} + \overline{z_3} + \overline{z_4} = 2$ или 4 (Приложение В). Отсюда следует, что слово X неподвижно относительно элемента g тогда и только тогда, когда X_{11} равно одному из трех упомянутых выше слов. Поэтому порядок множества неподвижных точек элемента g равен $3 \cdot 2^{120}$ и не является степенью двойки. Предложение доказано.

Лемма 4. *2^{128} не представляется в виде $(q^d - 1)/(q - 1)$, где q — степень простого числа, и в виде $2^{2d-1} \pm 2^{d-1}$.*

Доказательство. 1) Пусть $2^{128} = q^{d-1} + q^{d-2} + \ldots + q + 1$. Очевидно, что q нечетно, а d четно. Предположим, что $d = 2$. Тогда $2^{128} - 1 = (2^{64} - 1)(2^{64} + 1) = q$. Но у чисел $2^{64} - 1$ и $2^{64} + 1$ разные простые делители. Получаем противоречие, поскольку q — степень простого числа.

Теперь пусть $d = 2k > 2$. Тогда

$$(q^d - 1)/(q - 1) = (q^k - 1)(q^k + 1)/(q - 1) = (q^k + 1)(q^{k-1} + q^{k-2} + \ldots + q + 1).$$

Числа $x = q^k + 1$ и $y = q^{k-1} + q^{k-2} + \ldots + q + 1$ являются степенями двойки и $x > y$. Следовательно, $y|x$. Но тогда $y|z = qy - x = q^{k-1} + q^{k-2} + \ldots + q - 1$ и $z > 0$. Приходим к противоречию, так как $z < y$.

2) Число 2^{128} нельзя представить в виде $2^{2d-1} \pm 2^{d-1}$, поскольку у последнего числа есть нечетные простые сомножители при $d > 1$.

Доказательство теоремы. В силу следствия группа Γ_t 2-транзитивна. Согласно теореме Бернсайда [3] (современное изложение в [4, § 17]), 2-транзитивная группа подстановок имеет единственную минимальную нормальную подгруппу, которая либо элементарная абелева, либо простая. Если эта подгруппа элементарная абелева, то Γ_t сопряжена с подгруппой аффинной группы и St сопряжена с подгруппой группы $GL(128, 2)$. В силу предложения 2 это невозможно.

Список чисел n, для которых существует 2-транзитивная группа подстановок степени n с неабелевой минимальной нормальной подгруппой, отличная от знакопеременной и симметрической, приведен в [5]. Это числа вида $(q^d - 1)/(q - 1)$, где q — степень простого числа, $2^{2d-1} \pm 2^{d-1}$, 11, 12, 15, 22, 23, 24, 28, 176 и 276. Очевидно, что

$$2^{128} \notin \{11, 12, 15, 22, 23, 24, 28, 176, 276\}.$$

Используя лемму 4, получаем, что Γ_t — знакопеременная группа. Теперь применим лемму 1. Теорема доказана.

Авторы благодарят директора учреждения Белорусского государственного университета "Национальный научно-исследовательский центр прикладных проблем математики и информатики" члена-корреспондента НАН Беларуси Ю.С. Харина и заведующего лабораторией этого центра С.В. Агиевича за постановку задачи, консультации и предоставление компьютерных программ, использующихся при реализации алгоритма.

ПРИЛОЖЕНИЕ А. **Свойства преобразования S, используемые при анализе стабилизатора нулевого слова.**

Для каждого ненулевого слова $u \in \mathcal{A}_8$ укажем все $v \in \mathcal{A}_8$, для которых существуют слова $\delta_1, \ldots, \delta_{12} \in \mathcal{A}_8$ такие, что

$$S(\delta_1) \oplus \ldots \oplus S(\delta_{12}) = 0, \quad \overline{\delta_i} + \overline{u} < 256 \quad \text{и} \quad S(\langle \overline{\delta_1} + \overline{u} \rangle_8) \oplus \ldots \oplus S(\langle \overline{\delta_{12}} + \overline{u} \rangle_8) = v.$$

Ниже для каждого значения $U = \overline{u}$ приведены число N искомых слов v для данного u и множество Δ значений $\overline{v}$.

$U = 1$; $N = 2$; $\Delta = \{0, 142\}$.

$U = 2$; $N = 4$; $\Delta = \{0, 142, 214, 88\}$.

$U = 3$; $N = 8$; $\Delta = \{0, 142, 214, 156, 88, 18, 196, 74\}$.

$U = 4$; $N = 16$; $\Delta = \{0, 142, 214, 88, 18, 156, 193, 196, 74, 23, 153, 79, 5, 139, 211, 93\}$.

$U = 5$; $N = 32$; $\Delta = \{0, 142, 214, 88, 18, 156, 196, 74, 23, 153, 193, 37, 79, 5, 139, 211, 93, 185, 55, 111, 225, 171, 125, 243, 174, 32, 120, 246, 188, 50, 106, 228\}$.

$U = 6$; $N = 64$; $\Delta = \{0, 142, 214, 88, 18, 156, 196, 74, 23, 153, 193, 79, 5, 139, 211, 93, 185, 55, 111, 225, 171, 46, 37, 25, 243, 174, 32, 120, 246, 188, 50, 106, 228, 97, 239, 183, 57, 115, 253, 165, 43, 118, 248, 160, 100, 234, 178, 60, 216, 86, 14, 128, 202, 68, 28, 146, 207, 65, 25, 151, 221, 83, 11, 133\}$.

$U = 7$; $N = 128$; $\Delta = \{0, 142, 214, 88, 18, 156, 196, 74, 23, 153, 193, 79, 5, 139, 211, 93, 185, 55, 111, 225, 171, 37, 125, 243, 174, 32, 120, 246, 188, 50, 106, 228, 97, 239, 183, 57, 115, 253, 165, 43, 118, 248, 252, 160, 46, 100, 234, 178, 60, 216, 86, 14, 128, 202, 68, 28, 146, 207, 65, 25, 151, 221, 83, 11, 129, 15, 87, 217, 147, 29, 69, 203, 150, 24, 64, 206, 132, 10, 82, 220, 56, 182, 238, 96, 42, 164, 114, 47, 161, 249, 119, 61, 179, 235, 224, 110, 54, 184, 242, 124, 36, 170, 247, 121, 33, 229, 107, 51, 89, 215, 143, 1, 75, 197, 157, 78, 192, 152, 92, 4, 138, 210, 22, 19, 189, 175, 101, 133\}$.

$8 \le U \le 238$; $N = 256$.

$U = 239$; $N = 128$; $\Delta = \{0, 27, 182, 4, 199, 250, 20, 157, 137, 211, 16, 15, 162, 238, 195, 178, 31, 254, 153, 141, 166, 11, 215, 234, 61, 76, 225, 103, 115, 88, 245, 41, 229, 72, 57, 99, 119, 45, 241, 92, 90, 43, 134, 63, 146, 78, 130, 47, 94, 74, 150, 59, 124, 209, 160, 180, 104, 197, 164, 213, 120, 193, 108, 176, 173, 220, 200, 185, 216, 169, 189, 204, 38, 87, 67, 50, 83, 34, 54, 71, 65, 48, 36, 85, 52, 69, 81, 32, 202, 187, 175, 222, 191, 206, 218, 171, 113, 101, 117, 97, 139, 159, 143, 155, 236, 248, 232, 252, 22, 2, 18, 6, 106, 126, 110, 122, 144, 132, 148, 128, 247, 227, 243, 231, 13, 25, 9, 29\}$.

$U = 240$; $N = 64$; $\Delta = \{0, 182, 199, 250, 157, 16, 27, 11, 234, 166, 215, 141, 61, 76, 103, 225, 241, 45, 92, 119, 90, 43, 134, 150, 74, 59, 209, 160, 124, 108, 193, 176, 220, 173, 204, 189, 87, 38, 71, 54, 48, 65, 32, 81, 187, 202, 171, 218, 113, 97, 139, 155, 236, 252, 22, 6, 106, 122, 144, 128, 247, 231, 13, 29\}$.

$U = 241$; $N = 32$; $\Delta = \{0, 199, 157, 27, 234, 182, 92, 119, 45, 241, 90, 134, 43, 193, 176, 108, 220, 173, 71, 54, 65, 48, 218, 171, 113, 155, 236, 6, 106, 128, 247, 29\}$.

$U = 242$; $N = 16$; $\Delta = \{0, 27, 182, 119, 199, 176, 108, 193, 173, 220, 171, 218, 113, 6, 106, 29\}$.

$U = 243$; $N = 8$; $\Delta = \{0, 182, 199, 108, 218, 171, 113, 29\}$.

$U = 244$; $N = 4$; $\Delta = \{0, 199, 218, 29\}$.

$U = 245$; $N = 2$; $\Delta = \{0, 29\}$.

$U \ge 246$; $N = 1$; $\Delta = \{0\}$.

Эти списки получены с помощью компьютерных вычислений; элементы множества Δ записаны в том порядке, в котором они были получены при выполнении программы.

ПРИЛОЖЕНИЕ В. **Вычисление неподвижных точек одного преобразования.**

Положим $k_1 = 17$, $k_2 = 11$, $k_3 = 7$, $k_4 = 0$ и $\delta_i = \langle k_i \rangle_{32}$. В доказательстве предложения 2 рассматривалось множество неподвижных точек преобразования $g = g_1(\delta_1, \delta_2, \delta_3, \delta_4) \in St^1$. Из конструкции оператора g следует, что $g(X) = X$ тогда и только тогда, когда X_{11} удовлетворяет следующим условиям:

$$\text{если} \quad \langle \overline{X_{11}} + k_i \rangle_{32} = v_i \| z_i \| 0 \| 0, \quad \text{то} \quad S(v_1) \oplus S(v_2) \oplus S(v_3) \oplus S(v_4) = 0 \quad \text{и}$$
$$\overline{z_1} + \overline{z_2} + \overline{z_3} + \overline{z_4} = 0, 2 \ \text{ или } \ 4. \tag{1}$$

Заметим, что в любом случае $\overline{z_i} = 0$ или 1. Непосредственно проверяется, что $\overline{z_1} + \overline{z_2} + \overline{z_3} + \overline{z_4} < 4$ и что $\overline{z_1} + \overline{z_2} + \overline{z_3} + \overline{z_4} = 2$ тогда и только тогда, когда $245 \le \overline{X_{11}} \le 248$. С помощью компьютерных вычислений установлено, что X_{11} удовлетворяет условиям (1) лишь при $\overline{X_{11}} \in \{0, 1, 2\}$.

Литература

1. *Агиевич С.В., Галинский В.А., Микулич Н.Д., Харин Ю.С.* Алгоритм блочного шифрования BelT // Комплексная защита информации: Тезисы докл. VII Междунар. конф. Минск: ОИПИ НАН Беларуси, 2003. С. 95–97.
2. *Агиевич С.В., Галинский В.А., Микулич Н.Д., Харин Ю.С.* Об одном алгоритме блочного шифрования // Управление защитой информации. 2002. Т. 6. № 4. С. 407–412.
3. *Burnside W.* Theory of groups of finite order. Cambridge: Cambridge University Press, 1911.
4. *Супруненко Д.А.* Группы подстановок. Минск: Навука і тэхніка, 1996.
5. *Камерон П.Дж.* Конечные группы подстановок и конечные простые группы // УМН. 1983. Т. 38. Вып. 2 (231). С. 135–157.

M. V. Velichko, A. A. Osinovskaya, I. D. Suprunenko
The group generated by round permutations of the cryptosystem BelT

Summary

It is proved that the group generated by all round permutations of the cryptosystem BelT is the alternating group of degree 2^{128}. This result can be used for estimating security of the cryptosystem BelT and its modifications.