

Об эвристическом подходе к построению биективных векторных булевых функций с заданными криптографическими характеристиками

М. А. Коврижных, Д. Б. Фомин

Национальный исследовательский университет «Высшая школа экономики», г. Москва
makovrizhnykh@gmail.com, dfomin@hse.ru

Новосибирск,
9 сентября, 2021



Предложен эвристический алгоритм построения биективных булевых функций с заданными криптографическими свойствами — нелинейностью и дифференциальной δ -равномерностью — на основе обобщённой конструкции.

Производится поиск вспомогательных подстановок меньшей размерности в обобщённой конструкции с использованием идей спектрально-линейного и спектрально-разностного методов. Исследована возможность оптимизации вычисления криптографических характеристик на каждой итерации алгоритма.

Экспериментально получены 8-битовые b -равномерные подстановки с нелинейностью 108.

- Векторные булевы функции (S -блоки) — одни из основных примитивов современных симметричных шифров, обеспечивающих свойство перемешивания¹.
- При этом биективные S -блоки (подстановки) представляют наибольший интерес для использования в современных симметричных шифрах.
- S -блоки должны иметь криптографические характеристики, гарантирующие неосуществимость применения известных методов (в частности, разностного и линейного методов) криптографического анализа.

Так, S -блоки с высокой нелинейностью позволяют гарантировать стойкостью к линейному криптографическому анализу. А для конструирования криптографических алгоритмов, стойких к разностному анализу, используют S -блоки с минимально возможным показателем дифференциальной δ -равномерности.

¹Shannon C.E. Communication theory of secrecy systems // Bell System Technical Journal. – 1949. – Vol. 28. – P. 656–715.

- Построение подстановок размерности $n \geq 8$ бит с криптографическими характеристиками, гарантирующими стойкость шифров к разностному и линейному методам криптоанализа, является сложной задачей, что подтверждается большим количеством новейших научных публикаций и докладов на всероссийских и международных конференциях посвященных данной тематике.
- 8-битовые подстановки используются в современных криптографических алгоритмах, например, ГОСТ 34.12-2018 “Кузнечик”, AES, BelT и других.

- V_n — n -мерное векторное пространство над полем из двух элементов \mathbb{F}_2 ,
 $V_n^\times = V_n \setminus \{0\}$.
- \mathbb{F}_{2^n} — конечное поле из 2^n элементов. Операции сложения и умножения в поле \mathbb{F}_{2^n} будем обозначать знаками “+” и “·” соответственно.
- *Конкатенацию* двух векторов $a \| b \in V_{n+m}$ $a \in V_n, b \in V_m$ будем обозначать $a \| b \in V_{n+m}$.
- *Скалярным произведением* двух векторов $a, b \in V_n$ называется элемент поля \mathbb{F}_2 , вычисляемый по формуле $\langle a, b \rangle = a_{n-1}b_{n-1} + \dots + a_0b_0$.
- *Векторной булевой (n, m) -функцией* называется преобразование $V_n \rightarrow V_m$.
- *Подстановкой* называется биективная (n, n) -функция. $S(V_n)$ — симметрическая группа всех подстановок пространства V_n .

Мономиальные подстановки поля \mathbb{F}_{2^m} это подстановки вида x^d , где d — такое положительное целое, что $\gcd(d, 2^m - 1) = 1$. В частности, для $m = 4$ мономиальные подстановки получаются для $d \in \{1, 2, 4, 7, 8, 11, 13, 14\}$.

При этом, если $d \in \{1, 2, 4, 8\}$, то x^d задает линейную подстановку.

- *Транспозиция* — это цикл длины 2. Умножение подстановки G на транспозицию справа $G \circ (i_1, i_2)$ приводит к транспозиции элементов i_1 и i_2 в верхней строке подстановки G ²[с. 51], другими словами, в нижней строке подстановки G меняются местами образы элементов i_1 и i_2 .
- *Индикаторной функцией* $I_b(x)$ для $b, x \in V_n$ называется

$$I_b(x) = \begin{cases} 1, & b = x, \\ 0, & b \neq x. \end{cases}$$

²Кострикин А.И. Введение в алгебру. Ч. I. Основы алгебры: учебник для вузов. 3-е изд. М.: Физматлит, 2004. С. 272.

Определение

Подстановка $F \in S(V_n)$ называется дифференциально δ_F -равномерной, если

$$\delta_F = \max_{a \in V_n^\times, b \in V_n} \delta_F(a, b),$$

где $\delta_F(a, b) = |\{x \in V_n : F(x + a) + F(x) = b\}|$.

Значение δ_F называется показателем дифференциальной равномерности подстановки F .

Определение

Таблицей распределения разностей (Difference Distribution Table — DDT) подстановки F называется такая $2^n \times 2^n$ таблица DDT_F , что $DDT_F[a, b] = \delta_F(a, b)$.

Определение

Для всех элементов $\delta \in \{0, 2, \dots, 2^n\}$ определим множества

$$D_F(\delta) = \{(a, b) \in V_n^\times \times V_n : \delta_F(a, b) = \delta\}.$$

Разностным спектром подстановки F называется множество пар $D_F = \{(\delta, |D_F(\delta)|)\}$.

Определение

Преобразованием Уолша — Адамара $W_F(a, b)$ подстановки $F \in S(V_n)$ называется отображение $W_F : V_n \times V_n \rightarrow \mathbb{Z}$, заданное равенством

$$W_F(a, b) = \sum_{x \in V_n} (-1)^{\langle a, x \rangle + \langle b, F(x) \rangle} \quad \text{для любых } a, b \in V_n.$$

Определение

Линейность ℓ_F подстановки F определяется как

$$\ell_F = \max_{a \in V_n, b \in V_n^\times} |W_F(a, b)|.$$

Нелинейность N_F подстановки F вычисляется по формуле $N_F = 2^{n-1} - \frac{1}{2}\ell_F$.

Определение

Таблицей линейных приближений (*Linear Approximation Table* — *LAT*) подстановки F называется такая $2^n \times 2^n$ таблица LAT_F , что $LAT_F[a, b] = \ell_F(a, b)$, где






$$\ell_F(a, b) = |\{x \in V_n : \langle a, x \rangle = \langle b, F(x) \rangle\}| - 2^{n-1} = \frac{1}{2}W_F(a, b).$$

Определение

Для всех элементов $\ell \in \{0, 2, \dots, 2^{n-1}\}$ определим множества

$$L_F(\ell) = \{(a, b) \in V_n \times V_n^\times \mid |\ell_F(a, b)| = \ell\}.$$

Линейным спектром подстановки F называется множество пар $L_F = \{(\ell, |L_F(\ell)|)\}$.

-  **Yuyin Yu, Mingsheng Wang, and Yongqiang Li**, Constructing differential 4-uniform permutations from know ones, Cryptology ePrint Archive, Report 2011/047. 2011. <https://eprint.iacr.org/2011/047>
-  **Menyachikhin A. V.** Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters // Матем. вопр. криптогр. 2017. Т. 8, Вып. 2. С. 97–116.
-  **Menyachikhin A. V.** The change in linear and differential characteristics of substitution after the multiplication by transposition // Матем. вопр. криптогр. 2020. Т. 11, № 2. С. 111–123.
-  **Фомин Д. Б.** О подходах к построению низкоресурсных нелинейных преобразований // Обозрение прикладной и промышленной математики. 2018. Т. 25, Вып. 4. С. 379–381.
-  **Фомин Д. Б.** Об алгебраической степени и дифференциальной равномерности подстановок пространства V_{2m} , построенных с использованием $(2m, m)$ -функций // Матем. вопр. криптогр. 2020. Т. 11, № 4. С. 133-149.

Рассмотрим $(2m, 2m)$ -функцию $F(x_1, x_2) = y_1 \| y_2$, где $x_1, x_2, y_1, y_2 \in V_m$, задаваемую следующей *обобщённой* конструкцией, впервые введенной в ³:

$$\begin{aligned} y_1 = G_1(x_1, x_2) &= \begin{cases} x_1^\alpha \cdot x_2^\beta, & x_2 \neq 0, \\ \widehat{\pi}_1(x_1), & x_2 = 0, \end{cases} \\ y_2 = G_2(x_1, x_2) &= \begin{cases} x_1^\gamma \cdot x_2^\delta, & x_1 \neq 0, \\ \widehat{\pi}_2(x_2), & x_1 = 0. \end{cases} \end{aligned} \quad (1)$$

В силу существования взаимно-однозначного отображения $V_m \rightarrow \mathbb{F}_{2^m}$ в (1) и далее операции возведения в степень и умножения производятся в поле \mathbb{F}_{2^m} .

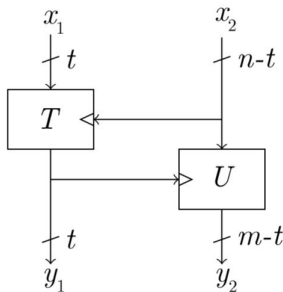
Параметрами функции (1) являются набор показателей степеней $(\alpha, \beta, \gamma, \delta)$ мономиальных подстановок и значения подстановок $\widehat{\pi}_1, \widehat{\pi}_2 \in S(V_m)$. Без ограничения общности будем предполагать, что

$$\widehat{\pi}_1(0) = 0, \quad \widehat{\pi}_2(0) = 0. \quad (2)$$

³Фомин Д.Б. О подходах к построению низкоресурсных нелинейных преобразований //Обозрение прикладной и промышленной математики. 2018. Т. 25, Вып. 4. С. 379–381.

Отметим, что конструкция (1) основана на структуре типа «бабочка», предложенной в ⁴, и полученной при изучении декомпозиции APN-подстановки Диллона ⁵.

Обобщенная конструкция допускает TU -представление ⁶.



⁴ Biryukov A., Perrin L., and Udovenko A. “Reverse-engineering the s-box of Streebog, Kuznyechik and STRIBOBr1” // LNCS. 2016. V. 9665. P. 372–402.

⁵ Browning K. A., Dillon J. F., McQuistan M. T., and Wolfe A. J. An APN permutation in dimension six // 9th Int. Conf. Finite Fields Appl. 2009. Contemp. Math. 2010. V. 518. P. 33–42.

⁶ Canteaut A., Perrin L. “On ccz-equivalence, extended-affine equivalence, and function twisting”, Cryptology ePrint Archive, Report 2018/713. <https://eprint.iacr.org/2018/713>.

Параметры обобщенной конструкции (1) — набор показателей степеней $(\alpha, \beta, \gamma, \delta)$ мономиальных подстановок и значения подстановок $\hat{\pi}_1, \hat{\pi}_2 \in S(V_m)$ — выбираются независимо друг от друга.

В работе ⁷ в случае $m = 4$ на множестве наборов $(\alpha, \beta, \gamma, \delta)$ было введено отношение эквивалентности и получено разбиение этого множества на непересекающиеся классы. Обоснованы утверждения, позволяющие по одному представителю класса эквивалентности

- 1** отбраковать функции, у которых показатель дифференциальной δ -равномерности $\delta_F \geq 8$ (при $m = 4$);
- 2** среди оставшихся функций отбраковать те, которые не являются подстановками.

⁷Fomin D., Kovrizhnykh M. “On Differential Uniformity of Permutations Derived Using a Generalized Construction” // X симпозиум «Современные тенденции в криптографии» CTCrypt 2021.

https://ctcrypt.ru/files/files/2021/Fomin_Kovrizhnylh.pdf

Сводная таблица классов эквивалентности при $m = 4$

№	Представитель класса эквивалентности	Количество элементов в классе эквивалентности	Причина отбраковки
1	Обобщенный представитель: $(\alpha, \beta, \gamma, \delta)$, где $\alpha, \gamma \in \{1, 2, 4, 8\}$	1792	$\delta_F \geq 14$
2	$(7,7,7,7)$	64	$\delta_F \geq 14$
3	$(11,1,1,13)$	128	$\delta_F \geq 14$
4	$(7,1,1,7)$	128	$\delta_F \geq 14$
5	$(7,7,7,13)$	64	не является подстановкой
6	$(1,7,7,7)$	256	
7	$(4,7,7,7)$	256	
8	$(7,7,2,2)$	128	
9	$(1,1,7,13)$	128	
10	$(2,7,7,7)$	256	
11	$(7,2,2,7)$	128	
12	$(1,1,7,11)$	256	не отбракованы
13	$(1,7,7,11)$	256	
14	$(1,7,7,2)$	128	
15	$(7,7,7,11)$	128	

Осталось научиться выбирать вспомогательные подстановки $\hat{\pi}_1$ и $\hat{\pi}_2$ так, чтобы итоговая 8-битовая подстановка $F(1)$ имела $\delta_F = 6$, $N_F = 108$.

Предложен эвристический подход, использующий идеи спектрально-линейного и спектрально-разностного методов⁸:

1. начальные случайно сгенерированные 4-битовые подстановки $\hat{\pi}_i$ итеративно умножаются на транспозиции;
2. среди полученных 8-битовых подстановок отбираются лучшие по нелинейности, показателю дифференциальной равномерности и соответствующим значениям в линейном и разностном спектрах;
3. если заданные характеристики $\delta_F \leq 6$ и $N_F \geq 108$ достигнуты, выход;
4. 4-битовые подстановки $\hat{\pi}_i$, соответствующие лучшим на 2-м шаге, итеративно умножаются на транспозиции, переходим к шагу 2;

⁸*Menyachikhin A. V. Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters //Матем. вопр. криптогр. 2017. Т. 8, Вып. 2. С. 97–116.*

Алгоритм 1.

Вход: Подстановка $F \in S(V_8)$, построенная по формулам (1) с использованием одного из 768 наборов параметров $(\alpha, \beta, \gamma, \delta)$ [3] и произвольных 4-битовых подстановок $\widehat{\pi}_1, \widehat{\pi}_2$ (2), с криптографическими характеристиками $\ell_F > 40$ или $\delta_F > 6$.

Параметры: Num_Trans — количество умножений на транспозиции, Num_Best — количество отбираемых пар $(\widehat{\pi}_1, \widehat{\pi}_2)$ на каждой итерации алгоритма.

- 1: Сформировать список $Best$ из одной пары подстановок $(\widehat{\pi}_1, \widehat{\pi}_2)$.
- 2: Для всех пар подстановок $(\widehat{\pi}_1, \widehat{\pi}_2)$ из списка $Best$:
 - 3: запомнить пару $(\widehat{\pi}_1, \widehat{\pi}_2)$ как просмотренную;
 - 4: псевдослучайно выбрать номер $t \in \{1, 2\}$.
 - 5: Для $i = 1, \dots, Num_Trans$
 - 6: псевдослучайно выбрать $x, y \in V_4^X, x \neq y$, получить подстановку $\widehat{\pi}_t = \widehat{\pi}_t \circ (x, y)$.
 - 7: Если пара $(\widehat{\pi}_1, \widehat{\pi}_2)$ ещё не просмотрена, то
 - 8: встроить $\widehat{\pi}_t$ в F ;
 - 9: вычислить набор характеристик подстановки $(\ell_F, \delta_F, |L_F(\ell_F/2)|, |D_F(\delta_F)|)$;
 - 10: добавить пару $(\widehat{\pi}_1, \widehat{\pi}_2)$ в список $Best$.
 - 11: Отобрать (по принципу многоуровневой сортировки по возрастанию) Num_Best лучших (т.е. с меньшими значениями с учётом приоритетов) из всех наборов характеристик подстановок F , порождённых парами $(\widehat{\pi}_1, \widehat{\pi}_2)$ из текущего списка $Best$, считая, что в наборе приоритет убывает от ℓ_F к $|D_F(\delta_F)|$.
 - 12: Если в наилучшем наборе значения $\ell_F = 40$ и $\delta_F = 6$, то
 - 13: Вывести подстановки $\widehat{\pi}_1, \widehat{\pi}_2$, порождающие подстановку F ,
 - 14: иначе
 - 15: Сформировать новый список $Best$ из Num_Best пар подстановок $(\widehat{\pi}_1, \widehat{\pi}_2)$, соответствующих лучшему набору, отобранному на шаге 11.
 - 16: Перейти к шагу 2.

Выход: Подстановка $F \in S(V_8)$, отличающаяся от исходной только значениями подстановок $\widehat{\pi}_1, \widehat{\pi}_2$, такая, что

$$\ell_F = 40 \quad (N_F = 108), \quad \delta_F = 6. \quad (3)$$

Значения Num_Trans , Num_Best являются параметрами алгоритма. Вычислительные эксперименты показали, что при $Num_Best = 10$, $Num_Trans = 500$ на первой итерации и $Num_Trans = 100$ на последующих за приемлемое число итераций можно получить 8-битовые подстановки с характеристиками $N_F = 108$, $\delta_F = 6$ и алгебраической степенью 7.

$(\alpha, \beta, \gamma, \delta)$	Количество итераций алгоритма до достижения $N_F = 108, \delta_F = 6$	Полученные $\hat{\pi}_1, \hat{\pi}_2$
(1,1,7,11)	16	$\hat{\pi}_1 = [0, 10, 6, 3, 14, 2, 5, 4, 9, 15, 7, 13, 8, 1, 12, 11]$ $\hat{\pi}_2 = [0, 1, 7, 14, 2, 9, 6, 12, 13, 3, 4, 5, 10, 15, 11, 8]$
(1,2,13,7)	31	$\hat{\pi}_1 = [0, 3, 11, 1, 4, 10, 8, 5, 2, 13, 9, 14, 7, 6, 15, 12]$ $\hat{\pi}_2 = [0, 6, 1, 7, 10, 8, 9, 12, 2, 11, 5, 13, 3, 4, 15, 14]$
(1,1,7,11)	50	$\hat{\pi}_1 = [0, 3, 13, 14, 6, 8, 2, 15, 4, 1, 12, 7, 9, 5, 10, 11]$ $\hat{\pi}_2 = [0, 7, 2, 11, 9, 4, 10, 13, 3, 5, 6, 8, 1, 14, 15, 12]$
(7,7,11,13)	56	$\hat{\pi}_1 = [0, 1, 14, 7, 8, 9, 3, 4, 6, 11, 15, 5, 12, 10, 13, 2]$ $\hat{\pi}_2 = [0, 12, 6, 11, 4, 8, 13, 3, 1, 5, 14, 7, 15, 10, 9, 2]$
(1,2,13,7)	63	$\hat{\pi}_1 = [0, 15, 8, 1, 14, 4, 5, 6, 7, 2, 11, 10, 9, 13, 3, 12]$ $\hat{\pi}_2 = [0, 2, 9, 11, 7, 8, 5, 13, 3, 6, 15, 12, 10, 1, 4, 14]$
(1,1,7,11)	111	$\hat{\pi}_1 = [0, 14, 6, 12, 2, 10, 5, 11, 7, 8, 4, 1, 9, 13, 15, 3]$ $\hat{\pi}_2 = [0, 11, 14, 5, 4, 6, 15, 3, 9, 1, 10, 7, 13, 8, 2, 12]$
(4,4,14,7)	134	$\hat{\pi}_1 = [0, 2, 13, 4, 8, 14, 10, 9, 7, 6, 12, 11, 15, 5, 3, 1]$ $\hat{\pi}_2 = [0, 15, 10, 14, 5, 8, 3, 11, 1, 13, 12, 7, 9, 6, 2, 4]$

При этом исследованы вопросы оптимизации вычисления линейного и разностного спектров на каждой итерации алгоритма.

Результаты из работы ⁹ применены для определения ячеек в DDT и LAT 8-битовой подстановки (1), в которых возникают изменения значений при умножении на транспозицию только 4-битовой подстановки $\hat{\pi}_1$ или $\hat{\pi}_2$.

Сформулированы утверждения о величинах получающихся разностей в ячейках DDT и LAT.

На основе этих утверждений указаны ячейки в DDT и LAT, которые не изменяются при умножении на транспозицию подстановки $\hat{\pi}_1$ (или $\hat{\pi}_2$), что позволяет экономить память при хранении DDT и LAT в алгоритмах⁵ вычисления линейного и разностного спектров.

⁹*Menyachikhin A.* The change in linear and differential characteristics of substitution multiplied by transposition [Электронный ресурс] // VIII симпозиум «Современные тенденции в криптографии» СТСCrypt'19. 2019.

Утверждение 1

Пусть 8-битовая подстановка $G = G(x_1, x_2) = y_1 \| y_2$ задана обобщенной конструкцией с параметрами $(\alpha, \beta, \gamma, \delta)$ из одного из четырех неотбракованных классов и произвольными 4-битовыми подстановками $\hat{\pi}_1, \hat{\pi}_2$ (2), а подстановка H получена из G одной транспозицией подстановки $\hat{\pi}_2$, т. е.

$$H = G \circ (0 \| x, 0 \| y), \quad x, y \in V_4^\times, \quad x \neq y. \quad (3)$$

Пусть $a \in V_8^\times, b \in V_8$ — произвольные, при этом $a = a_1 \| a_2, b = b_1 \| b_2$, тогда выполняются соотношения

$$\delta_H(a, b) - \delta_G(a, b) = \begin{cases} 0, & a_1 = 0, b_1 \neq 0, \\ 0, & a_1 = 0, b_1 = 0, a_2 = x + y, \\ 2(I_1 + I_3 - I_0 - I_2), & a_1 = 0, b_1 = 0, a_2 \neq x + y, \\ 2(\tilde{I}_1 + \tilde{I}_3 - \tilde{I}_0 - \tilde{I}_2), & a_1 \neq 0, \end{cases} \quad (4)$$

где

$$\begin{aligned} I_1 &:= I_{b_2}(\hat{\pi}_2(x + a_2) + \hat{\pi}_2(y)), & I_3 &:= I_{b_2}(\hat{\pi}_2(y + a_2) + \hat{\pi}_2(x)), \\ I_0 &:= I_{b_2}(\hat{\pi}_2(x + a_2) + \hat{\pi}_2(x)), & I_2 &:= I_{b_2}(\hat{\pi}_2(y + a_2) + \hat{\pi}_2(y)), \\ \tilde{I}_1 &:= I_b(g_{1,x} \| (g_{2,x} + \hat{\pi}_2(y))), & \tilde{I}_3 &:= I_b(g_{1,y} \| (g_{2,y} + \hat{\pi}_2(x))), \\ \tilde{I}_0 &:= I_b(g_{1,x} \| (g_{2,x} + \hat{\pi}_2(x))), & \tilde{I}_2 &:= I_b(g_{1,y} \| (g_{2,y} + \hat{\pi}_2(y))), \\ G(a_1, x + a_2) &:= (g_{1,x} \| g_{2,x}), & G(a_1, y + a_2) &:= (g_{1,y} \| g_{2,y}). \end{aligned} \quad (5)$$

Утверждение 2

Пусть 8-битовая подстановка $G = G(x_1, x_2) = y_1 \| y_2$ построена по формулам (1) с параметрами $(\alpha, \beta, \gamma, \delta)$ из одного из четырех неотбракованных классов и произвольными 4-битовыми подстановками $\hat{\pi}_1, \hat{\pi}_2$ (2), а подстановка H получена из G одной транспозицией подстановки $\hat{\pi}_2$, т. е.

$$H = G \circ (0 \| x, 0 \| y), \quad x, y \in V_4^\times, \quad x \neq y.$$

Пусть $a \in V_8, b \in V_8^\times$ — произвольные, при этом $a = a_1 \| a_2, b = b_1 \| b_2$, тогда выполняются соотношения

$$\ell_H(a, b) - \ell_G(a, b) = \begin{cases} 0, & \langle a_2, x + y \rangle = 0 \text{ или } \langle b_2, \hat{\pi}_2(x) + \hat{\pi}_2(y) \rangle = 0, \\ (-1)^{\langle a_2, x \rangle + \langle b_2, \hat{\pi}_2(x) \rangle + 1} \cdot 2, & \text{в противном случае.} \end{cases} \quad (6)$$

Спасибо за внимание!



Заметим, что множества $\{1, 2, 4, 8\}$ и $\{7, 11, 13, 14\}$ замкнуты относительно умножения на $d \in \{1, 2, 4, 8\}$ по $\text{mod } 15$.

$8^4 = 4096$ всевозможных наборов $(\alpha, \beta, \gamma, \delta)$ параметров преобразований из семейства (1) разбиваются на непересекающиеся классы эквивалентности. При этом отдельный класс эквивалентности можно получить по одному его представителю $(\alpha, \beta, \gamma, \delta)$, составляя различные наборы из следующих

$$(\alpha \cdot d_1 \cdot d_3, \quad \beta \cdot d_1 \cdot d_4, \quad \gamma \cdot d_2 \cdot d_3, \quad \delta \cdot d_2 \cdot d_4) \text{ mod } 2^m - 1,$$

$$(\gamma \cdot d_1 \cdot d_3, \quad \delta \cdot d_1 \cdot d_4, \quad \alpha \cdot d_2 \cdot d_3, \quad \beta \cdot d_2 \cdot d_4) \text{ mod } 2^m - 1,$$

$$(\beta \cdot d_1 \cdot d_3, \quad \alpha \cdot d_1 \cdot d_4, \quad \delta \cdot d_2 \cdot d_3, \quad \gamma \cdot d_2 \cdot d_4) \text{ mod } 2^m - 1,$$

$$(\delta \cdot d_1 \cdot d_3, \quad \gamma \cdot d_1 \cdot d_4, \quad \beta \cdot d_2 \cdot d_3, \quad \alpha \cdot d_2 \cdot d_4) \text{ mod } 2^m - 1,$$

где $m = 4$, $d_1, d_2, d_3, d_4 \in \{1, 2, 4, 8\}$.

Intel(R) Core(TM) i7 CPU @ 1.8GHz 4 ядра RAM 12Gb

Python 3.8.10

При значениях параметров $Num_Best = 10$, $Num_Trans = 100$ (начиная со 2-й итерации) одна итерация алгоритма в среднем вычисляется за ~ 9 минут.

Definition. Алгебраической степенью $\text{deg}(F)$ (n, m) -функции F называется минимальная степень многочлена Жегалкина среди всевозможных линейных комбинаций ее координатных функций $\langle a, F(x) \rangle$ по всем $a \in V_m^\times$:

$$\text{deg}(F) = \min_{a \in V_m^\times} \text{deg}(\langle a, F(x) \rangle).$$

Для подстановок $G \in S(V_n)$ максимально возможная степень нелинейности равна $n - 1$.