

Криптографические свойства и эффективная реализация максимально рассеивающих матриц с нетривиальными группами автоморфизмов

Буров Д. А., Костарев С. В.

В основе синтеза современных алгоритмов блочного шифрования лежат принципы Шеннона: функция зашифрования представляется в виде итерации раундовых преобразований, а сами раундовые преобразования — в виде итерации перемешивающих и рассеивающих преобразований.

Классическим примером построения алгоритмов блочного шифрования по такому принципу являются XSL-алгоритмы, раундовое преобразование которых состоит из прибавления ключа (X-слой), параллельного действия s-боксов (S-слой) и линейного рассеивающего преобразования (L-слой).

Алгоритмы блочного шифрования, являющиеся XSL-алгоритмами

- Кузнечик (ГОСТ Р 34.12-2015)
- AES
- Khazad
- Anubis

Некоторые криптографические характеристики

Одними из наиболее важных характеристик матрицы линейного рассеивающего преобразования являются коэффициенты рассеивания относительно разностного и линейного методов.

Определение

Коэффициентом рассеивания квадратной матрицы A порядка n над полем $\mathbb{F}_{2^r}$ относительно линейного метода называется величина

$$\beta_l(A) = \min_{x \in \mathbb{F}_{2^r}^n \setminus \{0\}} \left(w(x) + w(xA^\top) \right).$$

Коэффициентом рассеивания квадратной матрицы A порядка n над полем $\mathbb{F}_{2^r}$ относительно разностного метода называется величина

$$\beta_d(A) = \min_{x \in \mathbb{F}_{2^r}^n \setminus \{0\}} \left(w(x) + w(xA) \right).$$

Определение

Квадратная матрица A порядка n над полем $\mathbb{F}_{2^r}$ называется максимально рассеивающей или МР-матрицей, если $\beta_l(A) = \beta_d(A) = n + 1$.

Наиболее распространенные способы синтеза линейных рассеивающих преобразований

Одними из наиболее распространенных способов синтеза максимально рассеивающих преобразований являются

- алгебраические: использование МДР-кодов, матрицы Коши («Стрибог»), МР-матрицы на основе матриц Вандермонда,
- случайный выбор из некоторого класса: из циркулянтных матриц (AES), FFH-матриц (Khazad, Anubis),
- рекурсивные матрицы: матрицы, представляющиеся степенью сопровождающей матрицы («Кузнечик», Photon).

Группа автоморфизмов линейных рассеивающих преобразований

Определим действие группы $S_n \times S_n$ на множестве квадратных матриц порядка n над полем $\mathbb{F}_{2^r}$. Если $g = (g_1, g_2) \in S_n \times S_n$ и $A = (a_{i,j})$, то

$$A^g = A^{(g_1, g_2)} = (a_{g_1(i), g_2(j)}).$$

Определение

Группой автоморфизмов квадратной матрицы A порядка n над полем $\mathbb{F}_{2^r}$ назовем группу

$$\text{Aut}_d(A) = \{g = (g_1, g_2) \in S_n \times S_n \mid A^g = A\}.$$

Группа автоморфизмов матриц	Примеры алгоритмов блочного шифрования
$\mathbb{Z}_2^3$	Khazad
$\mathbb{Z}_8$	Whirlpool, SM4
$\mathbb{Z}_2^2$	CLEFIA, Anubis
$\mathbb{Z}_4$	AES, KLEIN, CAMELIA, PRINCE, Piccolo
$\mathbb{Z}_3, \mathbb{Z}_7$	FOX
S_4	Midori64
D_{10}	ITUbee
$S_4^2 \rtimes \mathbb{Z}_2$	Aria

Идея применения групп автоморфизмов матрицы

Утверждение (Ф.Дж. Мак-Вильямс, Н.Дж.А. Слоэн)

Матрица $A \in (\mathbb{F}_{2^r})_{n,n}$ является МР-матрицей тогда и только тогда, когда все ее квадратные подматрицы невырождены.

Группа автоморфизмов и синтез МР-матриц (СТCrypt 2025)

В матрице A над полем $\mathbb{F}_{2^r}$ с нетривиальной группой автоморфизмов число различных миноров меньше по сравнению с произвольной матрицей. А именно: если $(\{i_1, \dots, i_k\}, \{j_1, \dots, j_k\})$ и $(\{i'_1, \dots, i'_k\}, \{j'_1, \dots, j'_k\})$ находятся на одной орбите группы автоморфизмов, то определители подматриц $A(i_1, \dots, i_k \mid j_1, \dots, j_k)$ и $A(i'_1, \dots, i'_k \mid j'_1, \dots, j'_k)$ равны.

Множество квадратных матриц A порядка n над полем $\mathbb{F}_{2^r}$ таких, что $\{(g, g) \mid g \in G\} < \text{Aut}_d(A)$, $G < S_n$, обозначим через $M_{n,r}(G)$.

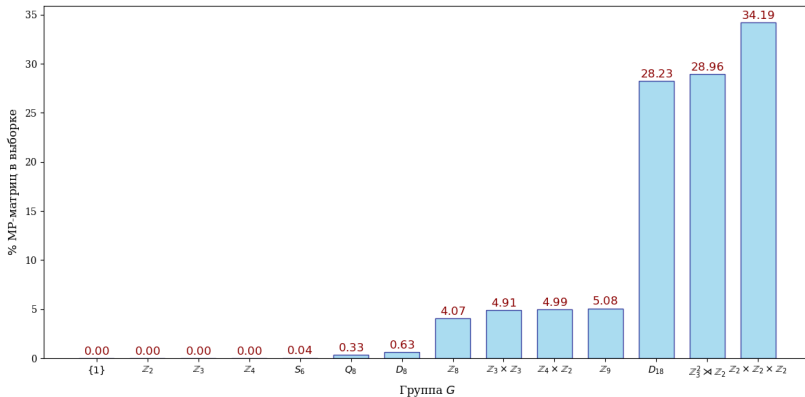


Рис.: Доля, выраженная в %, МР-матриц в выборке объема 10^6 из множества $M_{9,10}(G)$, $G < S_9$.

Теорема

Пусть $A \in \text{GL}(n, 2^r)$ является МР-матрицей. Тогда $\text{Aut}_A(A) = \{(g, \sigma(g)) \mid g \in G\}$, $G < S_n$, σ — изоморфизм подгрупп в S_n . Если G — транзитивная группа, то в зависимости от четности n группа G может быть одного из следующих типов:

- 1) n четное и G — регулярная группа;
- 2) n нечетное и G — регулярная группа;
- 3) n нечетное и $G = K \rtimes \langle h \rangle$ — группа Фробениуса, где K — регулярная абелева группа, являющаяся ядром Фробениуса, а h — инволюция группы G .

Кроме того, $\sigma: g \mapsto t^{-1}gt$, $g \in G$, для подходящего элемента $t \in S_n$ и матрица $A\hat{t}^{-1}$ является МР-матрицей с группой автоморфизмов $\{(g, g) \mid g \in G\}$.

Также описаны все возможные классы интранзитивных групп автоморфизмов МР-матриц.

Описание группы автоморфизмов (G, σ) в случае интранзитивной группы G

В случае интранзитивной группы G возможен один из следующих случаев:

- 1 G — полурегулярная группа;
- 2 G имеют ровно одну неподвижную точку, на остальном множестве G действует регулярно;
- 3 G действует на всех орбитах за исключением одной регулярно, на оставшейся орбите G действует как группа Фробениуса.

При этом σ — сопряжение в S_n

«Симметрии» потенциально должны облегчать программную и аппаратную реализации. В связи с этим естественными направлениями дальнейшего исследования свойств МР-матриц с нетривиальными группами автоморфизмов являются

- инволютивность
- ортогональность
- симметричность
- число битовых сложений (d-Xor), необходимых для «наивной» реализации умножения строки на матрицу с нетривиальной группой автоморфизмов

О несуществовании инволютивных и ортогональных МР-циркулянтов

Свойство максимальной рассеиваемости налагает существенные ограничения на существование инволютивных и ортогональных циркулянтов.

Теорема (К. Gupta, I. Ray, 2015)

Пусть A — МР-циркулянт порядка $n \geq 3$ над полем $\mathbb{F}_{2^r}$. Тогда

- ❶ A не инволютивен,
- ❷ если $n = 2^m$, то A не ортогонален.

Доказано¹, что над полем характеристики 2 не существует инволютивных МР- g -циркулянтов порядка 2^m , если $g^2 \equiv 1 \pmod{2^m}$. Также известно², что ортогональных МР- g -циркулянтов порядка 2^m не существует, также как не существует ортогональных МР-циклических матриц порядка 2^m над полем характеристики 2.

¹T. Chatterjee, A. Laha, «On MDS Property of g -Circulant Matrices», 2024

²T. Chatterjee, A. Laha, «A note on cyclic MDS and non-MDS matrices», 2025

Теорема

Пусть $A = (a_{i,j}) \in M_{n,r}(G)$ — МР-матрица, $G < S_n$ — регулярная абелева группа. Тогда

- 1 A инволютивна если и только если $n = 2^m$, G — элементарная абелева 2-группа и $a_{1,1} + a_{1,2} + \dots + a_{1,n} = 1$,
- 2 если A ортогональна, то силовская 2-подгруппа группы G либо тривиальная, либо элементарная абелева 2-группа.

Утверждение

Пусть $G < S_n$ — регулярная абелева группа, индуцирующая на $\Omega = \{1, \dots, n\}$ групповую операцию $\circ$, $A \in \text{GL}(n, 2^r) \cap M_{n,r}(G)$ — МР-матрица. Тогда следующие условия равносильны:

- 1 $\text{Aut}(A) = (F, 1)$, где $F = \langle G, \tau \rangle$, $\tau: x \mapsto x^{-1}$, $x \in \Omega$,
- 2 A — симметричная матрица.

При этом из справедливости любого из этих условий следует, что либо G — элементарная абелева 2-группа и τ — тождественный автоморфизм, либо n — нечетное число.

Утверждения накладывает существенное ограничение на строение силовской 2-подгруппы группы G .

Следствие

Пусть $G < S_n$ — регулярная группа, $A \in \text{GL}(n, 2^r) \cap M_{n,r}(G)$ — симметричная МР-матрица. Тогда силовская 2-подгруппа группы G либо тривиальна, либо является элементарной абелевой 2-группой.

Необходимые условия симметричности МР-матрицы с нетривиальной группой автоморфизмов

Утверждение

Пусть $G < S_n$ — регулярная группа, индуцирующая на $\Omega = \{1, \dots, n\}$ групповую операцию $\circ$, $A = (a_{i,j}) \in M_{n,r}(G)$ — симметричная МР-матрица. Тогда для любых $\alpha, \omega \in \Omega$ справедлива импликация

$$\alpha^{-1} = \omega^{-1} \alpha \omega \implies (\alpha = 1 \vee \text{ord } \omega \in \{1, 2\}). \quad (1)$$

Представленные ниже группы удовлетворяют условию (1). Кроме того, экспериментально проверено, что других групп порядка меньше 1024, удовлетворяющих (1), нет.

- ❶ Любая группа нечетного порядка;
- ❷ $\mathbb{Z}_2^m$, $n = 2^m$;
- ❸ Обобщенная группа диэдра GM_{2m} , m — нечетное число;
- ❹ $\text{AGL}(1, 2^m)$
- ❺ $K \rtimes_{\varphi} H$, где K — абелева группа нечетного порядка, для всех элементов H справедливо (1), $\varphi: H \rightarrow \text{Aut}(K)$ — гомоморфизм, и $K \rtimes \varphi(H) \in \{GD_{2m}, \text{AGL}(1, 2^t)\}$, m — нечетное число;
- ❻ $\text{PSL}(2, 2^m)$.

Задана матрица A порядка n над полем $\mathbb{F}_{2^r}$. Рассмотрим линейное преобразование $x \mapsto xA$, $x \in \mathbb{F}_{2^r}^n$, как преобразование над полем $\mathbb{F}_2$, выбрав некоторый базис $\mathbb{F}_{2^r}$ над $\mathbb{F}_2$. Этому преобразованию соответствует матрица $\tilde{A}$ над $\mathbb{F}_2$ порядка nr .

Определение (К. Khoongming, Т. Perrin, А. Poschmann, Н. Yap, 2014)

Значением d-Xor квадратной матрицы $\tilde{A}$ порядка nr над полем $\mathbb{F}_2$ называется величина

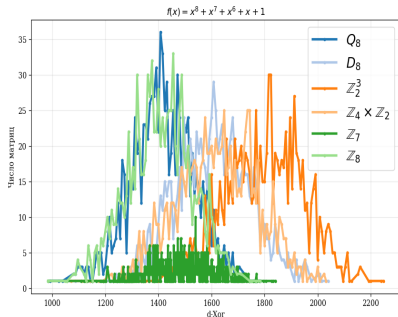
$$d\text{-Xor}(\tilde{A}) = \omega(A) - nr,$$

где $\omega(\tilde{A})$ — число единиц в $\tilde{A}$. В случае, когда $A \in \text{GL}(n, 2^r)$, $r \geq 2$, под величиной $d\text{-Xor}(A)$ будем понимать $d\text{-Xor}(\tilde{A})$.

Величина $d\text{-Xor}(A)$ соответствует числу операций XOR, необходимых для «наивной» реализации умножения. Низкое значение $d\text{-Xor}(A)$ ведет к уменьшению аппаратных затрат (площади кристалла, GE)³.

³К. Khoongming, Т. Perrin, А. Poschmann, Н. Yap, «FOAM: searching for hardware-optimal SPN structures and components with a fair comparison», 2014

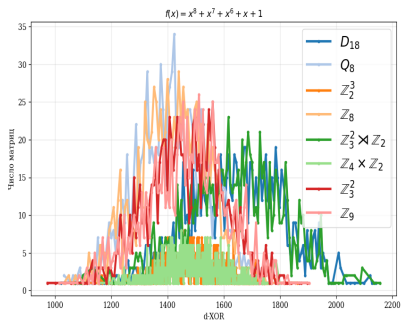
$$\begin{pmatrix} b & a & c & b & d & c & 1 & d \\ b & c & a & d & b & 1 & c & 1 \\ c & b & d & a & 1 & b & 1 & c \\ c & d & b & 1 & a & 1 & b & d \\ d & c & 1 & b & 1 & a & d & b \\ d & 1 & c & 1 & b & d & a & c \\ 1 & d & 1 & c & d & b & c & a \\ 1 & 1 & d & d & c & c & b & b \end{pmatrix}$$



Группа G	v_1	c
Q_8	24	6
$\mathbb{Z}_8^+$	24	6
$\mathbb{Z}_7^+$	21	8
$(\mathbb{Z}_4 \times \mathbb{Z}_2)^+$	16	7
D_8^+	16	7
$(\mathbb{Z}_2^3)^+$	8	8

(a) Распределение значения d-Xor в равновероятной выборке без возвращения объема 10^3 МР-матриц над $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/f(x)$, построенных в классах матриц $M_{8,8}(G)$

(b) Максимальное число единиц v_1 и минимальное число различных элементов s в МР-матрицах из классов $M_{8,8}(G)$



(a) Распределение значения d-Хор в равновероятной выборке без возвращения объема 10^3 МР-матриц размеров 8×8 над $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/f(x)$, построенных с использованием матриц из $M_{9,8}(G)$

Группа G	v_1	c
Q_8	24	6
$\mathbb{Z}_8^+$	24	6
$\mathbb{Z}_9^+$	22	6
$(\mathbb{Z}_3^2)^+$	22	6
$(\mathbb{Z}_2^3)^+$	21	8
D_8^+	21	8
$(\mathbb{Z}_4 \times \mathbb{Z}_2)^+$	21	8
D_{18}	15	5
$(\mathbb{Z}_3^2 \rtimes \langle B \rangle)^+$	15	5

(b) Максимальное число единиц v_1 и минимальное число различных элементов c в МР-матрицах, полученных вычеркивание строки и столбца в классах $M_{9,8}(G)$

Построение МР–матрицы с минимально возможным значением d-Xor

Пусть, например, в матрице с группой автоморфизмов $\{(g, g) | g \in G\}$, $G < S_8$, участвуют переменные a, b, c, d, e . Пусть также $f(x)$ — неприводимый многочлен степени 8, θ — корень $f(x)$, а C_f — сопровождающая матрица многочлена f . Для выбранного представления поля $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/f(x)$ подбирается такое подмножество его ненулевых элементов $\{\theta^{j_1}, \theta^{j_2}, \theta^{j_3}, \theta^{j_4}, \theta^{j_5}\}$, чтобы сумма

$$\omega(C_f^{j_1}) + \omega(C_f^{j_2}) + \omega(C_f^{j_3}) + \omega(C_f^{j_4}) + \omega(C_f^{j_5}) = Q$$

была минимальной. Затем перебираются все перестановки множества $\{\theta^{j_1}, \theta^{j_2}, \theta^{j_3}, \theta^{j_4}, \theta^{j_5}\}$ в качестве значений переменных (a, b, c, d, e) и проверяется, является ли полученная матрица максимально рассеивающей. Если ни для одной перестановки МР–матрица не найдена, то параметр Q увеличивается, и поиск подходящего подмножества элементов повторяется. После чего процедура построения матрицы повторяется. Алгоритм завершает работу, как только будет найдена МР–матрица.

Таблица: Минимальное значение d-Хор МР-матрицы в классе $M_{8,8}(G)$,
 $G < S_8$, над полем $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/f(x)$

$G \backslash f(x)$	$x^8 + x^4 + x^3 + x^2 + 1$	$x^8 + x^7 + x^6 + x + 1$
Q_8	768	744
$\mathbb{Z}_8$	720	688
$\mathbb{Z}_7$	723	681
$\mathbb{Z}_4 \times \mathbb{Z}_2$	744	720
D_8	880	784
$\mathbb{Z}_2^3$	832	768

Таблица: Минимальное значение d-Хор МР-матриц размеров 8×8 ,
 построенных с использованием матриц из $M_{9,8}(G)$, $G < S_9$, над полем
 $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/f(x)$

$G \backslash f(x)$	$x^8 + x^4 + x^3 + x^2 + 1$	$x^8 + x^7 + x^6 + x + 1$
Q_8	832	776
$\mathbb{Z}_8$	752	688
$\mathbb{Z}_9$	917	798
$\mathbb{Z}_3^2$	987	833
$\mathbb{Z}_2^3$	757	733
$\mathbb{Z}_4 \times \mathbb{Z}_2$	798	806
D_{18}	861	805
$\mathbb{Z}_3^2 \rtimes \mathbb{Z}_2$	868	819

Таблица: Результаты по оптимизации параметра d-Xor с применением подхода, основанном на использовании группы автоморфизмов

8×8 МР–матрица над полем $\mathbb{F}_{2^8}$	d-Xor
Построенная матрица	681
Лучшая из известных авторам матриц по параметру d-Xor	680*
Матрица алгоритма «Стрибог»	1674
Матрица алгоритма «Whirlpool»	840

На конференции STCrypt 2025 Д.Б. Фомин и А.С. Соловьев представили реализацию умножения на матрицу алгоритма «Стрибог», требующую 727 битовых операций Xor (s-Xor). Построенная в настоящей работе матрица может быть реализована за 448 (s-Xor) операций Xor.

Таблица: Результаты по оптимизации параметра d-Xor с применением подхода, основанном на использовании группы автоморфизмов

5×5 МР-матрица над полем $\mathbb{F}_{2^8}$	d-Xor
Построенная матрица	209
Лучшая из известных авторам матриц по параметру d-Xor	215*

Спасибо за внимание!

Лемма

Пусть $A \in \text{GL}(n, 2^r)$. Тогда $\text{Aut}_d(A)_1 \cong \text{Aut}_d(A)_2$ и

$$\text{Aut}_d(A) = \{(g_1, \sigma(g_1)) \mid g_1 \in \text{Aut}_d(A)_1\},$$

где $\sigma: \text{Aut}_d(A)_1 \rightarrow \text{Aut}_d(A)_2$ — изоморфизм групп.

Из леммы следует, что группа автоморфизмов матрицы $A \in \text{GL}(n, 2^r)$ однозначно определяется парой (G, σ) , где $G < S_n$ и σ — изоморфизм подгрупп в S_n .

Через $M_{n,r}(G, \sigma)$, $G < S_n$, обозначим подмножество квадратных матриц порядка n над полем $\mathbb{F}_{2^r}$ с группой автоморфизмов следующего вида

$$M_{n,r}(G, \sigma) = \left\{ A \in (\mathbb{F}_{2^r})_{n,n} \mid \text{Aut}_d(A) = \{(g, \sigma(g)) \mid g \in G\} \right\},$$

где σ — изоморфизм групп.

В случае, когда σ — тождественное отображение, будем использовать обозначение $M_{n,r}(G)$.

Теорема

Пусть $A \in \text{GL}(n, 2^r) \cap M_{n,r}(G, \sigma)$ является МР-матрицей, $G < S_n$ — транзитивная группа. Тогда в зависимости от четности n группа G может быть одного из следующих типов:

- 1) n четное и G — регулярная группа;
- 2) n нечетное и G — регулярная группа;
- 3) n нечетное и $G = K \rtimes \langle h \rangle$ — группа Фробениуса, где K — регулярная абелева группа, являющаяся ядром Фробениуса, а h — инволюция группы G .

Кроме того, $\sigma: g \mapsto t^{-1}gt$, $g \in G$, для подходящего элемента $t \in S_n$ и матрица $A\hat{t}^{-1}$ является МР-матрицей с группой автоморфизмов $(G, 1)$.

Также описаны все возможные классы интранзитивных групп автоморфизмов МР-матриц.

Необходимые и достаточные условия симметричности, инволютивности и ортогональности

Лемма

Пусть $A = (a_{i,j}) \in \text{GL}(n, 2^r) \cap M_{n,r}(G)$, $G < S_n$ — регулярная группа, индуцирующая на $\Omega = \{1, \dots, n\}$ групповую операцию $\circ$. Тогда

$$\begin{cases} a_{1,i} + a_{1,i^{-1}} = 0, \\ i = 1, \dots, n, \end{cases} \Leftrightarrow A^\top = A$$

$$\begin{cases} \sum_{i=1}^n a_{1,i} a_{1,i^{-1}} = 1, \\ \sum_{i=1}^n a_{1,i} a_{i^{-1} \circ k} = 0, k = 2, \dots, n, \end{cases} \Leftrightarrow A^{-1} = A$$

$$\begin{cases} \sum_{i=1}^n a_{1,i} = 1, \\ \sum_{i=1}^n a_{1,i} a_{i \circ k} = 0, k = 2, \dots, n. \end{cases} \Leftrightarrow A^{-1} = A^\top$$

В случае симметричной матрицы, т.е. $A^\top = A$, от условия $A \in \text{GL}(n, 2^r)$ можно отказаться.

Таблица: Минимальное значение d-Хор МР–матриц, построенных с использованием группы автоморфизмов $(G, 1)$, $G < S_n$, над полем $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/f(x)$

n	G	$f(x) = x^8 + x^4 + x^3 + x^2 + 1$	$f(x) = x^8 + x^7 + x^6 + x + 1$
5	D_{10}	220	215
	$\mathbb{Z}_4$	214	209
	$\mathbb{Z}_2^2$	223	215
6	$\mathbb{Z}_6$	372	348
	D_6	390	360
	$\mathbb{Z}_5$	383	363
7	D_{14}	504	483
	$\mathbb{Z}_6$	514	502
	D_6	537	505

Лучшие по параметру d-Хор из известных авторам МР–матриц* размеров $n \in \{5, 6, 7\}$ над полем $\mathbb{F}_{2^8}$ имеют значения d-Хор соответственно 215, 348, 483. Предлагаемый в настоящей работе подход в случае $n = 5$ позволяет построить матрицу с меньшим значением d-Хор равным 209. В случаях же $n = 6, 7$ удается построить МР–матрицы с аналогичными значениями параметра d-Хор.

*М. Liu, S. Sim «Lightweight MDS Generalized Circulant Matrices», 2016

Лемма

Пусть $G < S_n$ — интранзитивная группа, $\Delta_1, \dots, \Delta_t$ — орбиты группы G , упорядоченные по убыванию мощности, и для любого $g \in G \setminus \{1\}$ выполнено $|\text{fix}(g)| \leq 1$. Тогда возможны следующие три случая.

- ❶ Если $|\Delta_i| \geq 2$ для всех $i = 1, \dots, t$ и $n \equiv 0 \pmod{|G|}$, то G — полурегулярная группа и существуют такие биекции $g_{1,i}: \Delta_1 \rightarrow \Delta_i$, $i = 2, \dots, t$, что

$$G = \{g_1 g_1^{g_{1,2}} \dots g_1^{g_{1,t}} \mid g_1 \in G^{\Delta_1}\}, \quad g_1^{g_{1,i}} = g_{1,i}^{-1} g_1 g_{1,i}, \quad i = 2, \dots, t.$$

- ❷ Если $|\Delta_i| \geq 2$ для всех $i = 1, \dots, t$ и $n \not\equiv 0 \pmod{|G|}$, то G^{ψ_t} — группа Фробениуса, G^{ψ_i} — регулярная группа при всех $i \in \{1, \dots, t-1\}$ и существуют такие биекции $g_{1,i}: \Delta_1 \rightarrow \Delta_i$, $i = 2, \dots, t-1$, что

$$G = \{g_1 g_1^{g_{1,2}} \dots g_1^{g_{1,t-1}} \sigma(g_1) \mid g_1 \in G^{\Delta_1}\}, \quad g_1^{g_{1,i}} = g_{1,i}^{-1} g_1 g_{1,i}, \\ i = 2, \dots, t-1,$$

где $\sigma: G^{\Delta_1} \rightarrow G^{\Delta_t}$ — изоморфизм групп.

- ❸ Если $|\Delta_t| = 1$, то G^{ψ_i} — регулярная группа при всех $i \in \{1, \dots, t-1\}$ и существуют такие биекции $g_{1,i}: \Delta_1 \rightarrow \Delta_i$, $i = 2, \dots, t-1$, что

$$G = \{g_1 g_1^{g_{1,2}} \dots g_1^{g_{1,t-1}} \mid g_1 \in G^{\Delta_1}\}, \quad g_1^{g_{1,i}} = g_{1,i}^{-1} g_1 g_{1,i}, \quad i = 2, \dots, t-1.$$

Теорема

Пусть $A \in \text{GL}(n, 2^r) \cap M_{n,r}(G, \sigma)$ является МР-матрицей, $G < S_n$ — интранзитивная группа, $\Delta_1, \dots, \Delta_t$ — орбиты группы G , упорядоченные по убыванию мощности. Тогда G имеет один из трех видов, перечисленных в лемме, $\sigma: g \mapsto t^{-1}gt$, $g \in G$, для подходящего элемента $t \in S_n$ и матрица $A\hat{t}^{-1}$ является МР-матрицей с группой автоморфизмов $(G, 1)$. Если G имеет вид 2, то $|\Delta_t|$ — нечетное число, $|\Delta_i| = 2|\Delta_t| = |G|$ при $i \in \{1, \dots, t-1\}$.

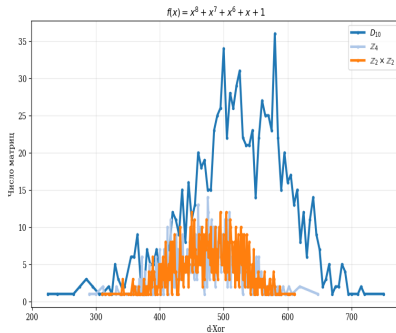
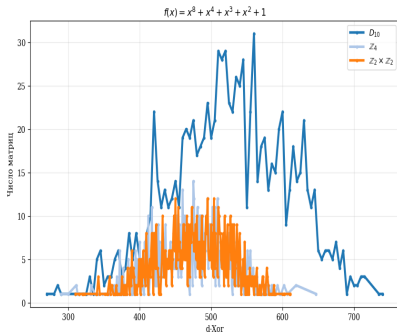


Рис.: Распределение значения d-Xor в равновероятной выборке без возвращения объема 10^3 МР-матриц над $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/f(x)$, построенных с использованием оптимальных 5×5 бирегулярных шаблонов

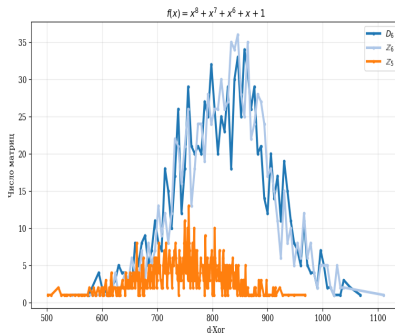
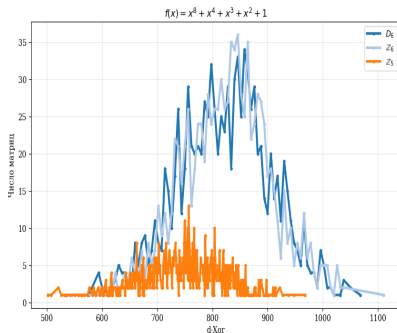


Рис.: Распределение значения d-Xor в равновероятной выборке без возвращения объема 10^3 МР-матриц над $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/f(x)$, построенных с использованием оптимальных 6×6 бирегулярных шаблонов

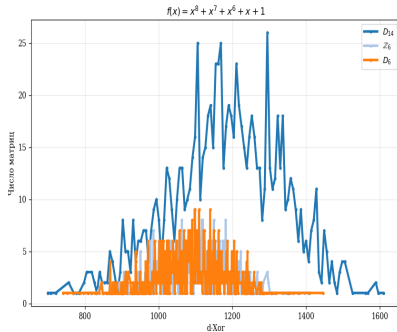
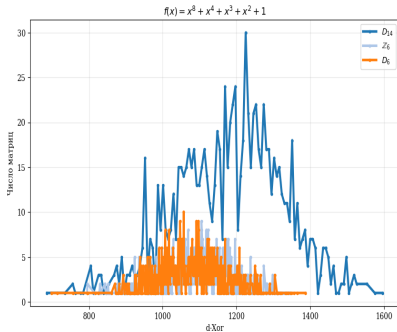


Рис.: Распределение значения d-Xor в равновероятной выборке без возвращения объема 10^3 МР-матриц над $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/f(x)$, построенных с использованием оптимальных 7×7 бирегулярных шаблонов