

Федеральное государственное автономное образовательное  
учреждение высшего образования  
"Национальный исследовательский университет  
"Высшая школа экономики"  
Московский институт электроники и математики им. А.Н.Тихонова

Руководитель проекта  
Преподаватель кафедры  
«Компьютерная безопасность»  
\_\_\_\_\_ А. Б. Чухно

**Руководство пользователя к проекту №2005  
«Построение низкоресурсных ARX подстановок с малыми  
характеристиками»**

Участники проекта:

Программист/аналитик  
Студент 4 курса факультета  
МИЭМ им.Тихонова программы  
«Компьютерная безопасность»  
\_\_\_\_\_ В. И. Нагаева

Программист/аналитик  
Студент 4 курса факультета  
МИЭМ им.Тихонова программы  
«Компьютерная безопасность»  
\_\_\_\_\_ В. А. Новиков

2025г.

## Руководство пользователя по работе с WEB-интерфейсом

В документе представлены сведения для обеспечения корректной работы пользователя с разработанным сайтом для получения генеративных ARX подстановок и их характеристик. Работа происходит с подстановками, который строится по следующему алгоритму:

Отображение  $\sigma_{r_i, s_i}(X_L, X_R) : V_{2n} \rightarrow V_{2n} = ((X_R \lll_{r_i})X_L), ((X_R \lll_{r_i})X_L) \lll_{s_i} \oplus X_R$  называется итерацией ARX  $X_L$  – старшее полуслово,  $X_R$  – младшее полуслово. Одна итерация ARX изображена на рисунке 1.

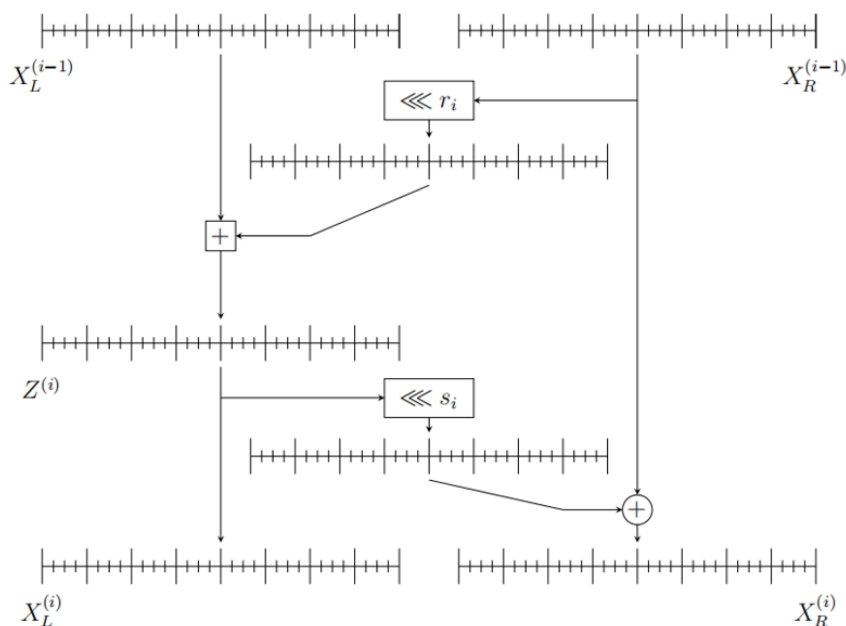


Рис. 1: Строение одной ARX итерации

Алгоритм работы с сайтом:

1. Перейти на сайт по следующему адресу: <http://193.19.119.246/>

The screenshot shows the initial page of the website. It has a title "Выбор чисел" (Number Selection). Below the title, there is a prompt "Выберите число N (от 5 до 7):" (Select number N (from 5 to 7):). Under this prompt is a dropdown menu with the text "Выберите число" (Select number). Below the dropdown menu is a button labeled "Рассчитать" (Calculate).

Рис. 2: Начальная страница сайта

2. Из выпадающего списка выбрать число ARX-итераций для построения подстановок.

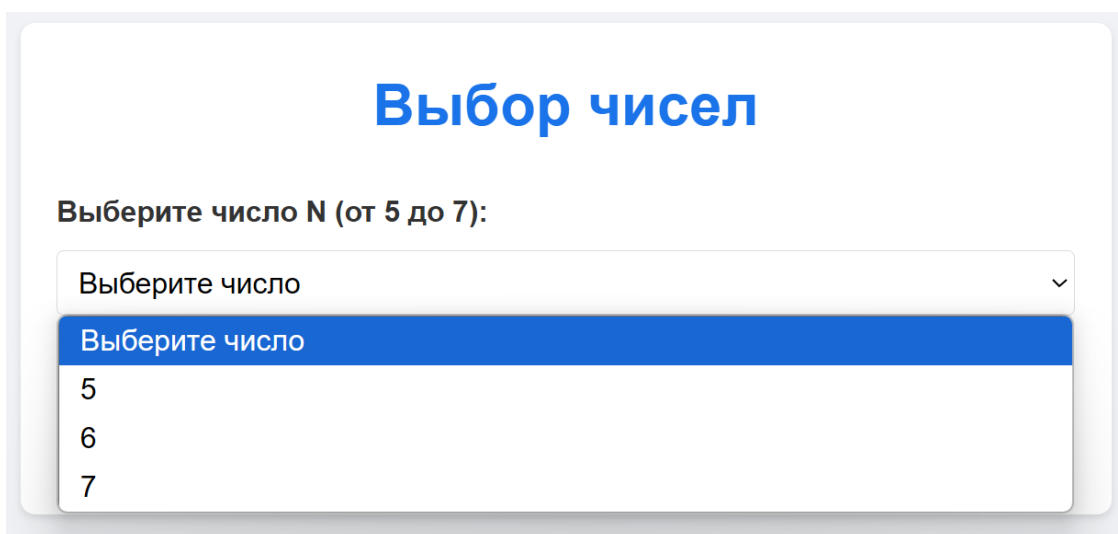


Рис. 3: Поле для выбора количества итераций

3. Для каждой итерации указать количество битовых сдвигов левой и правой части числа.

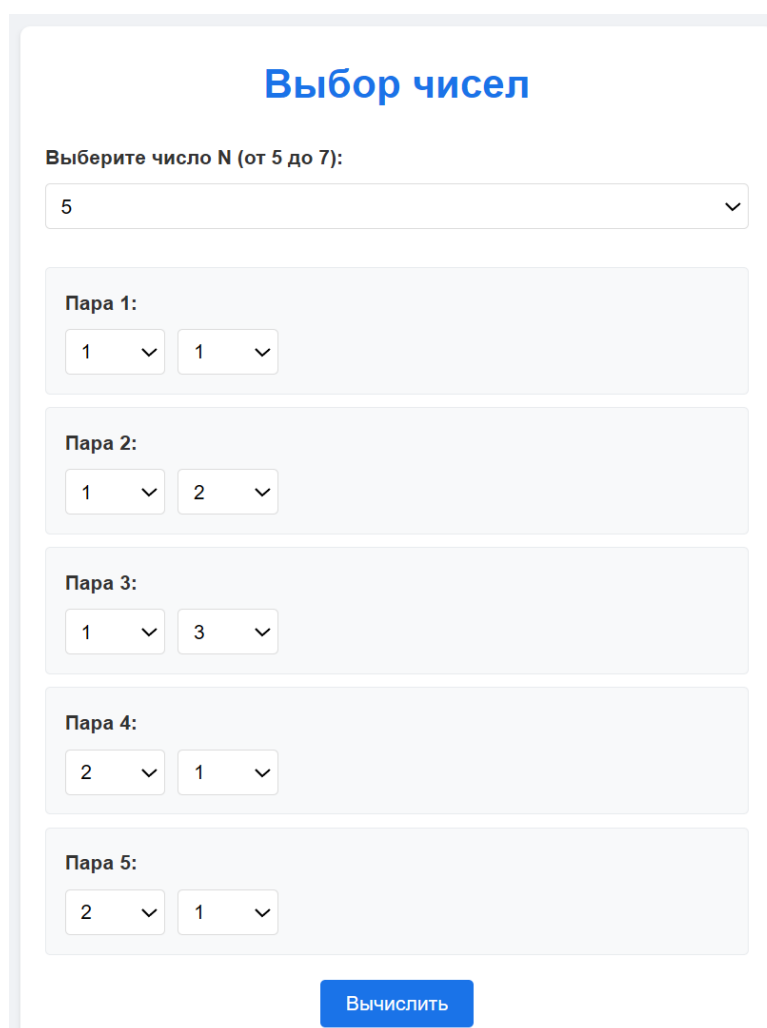


Рис. 4: Окно для выбора пар сдвигов

4. После того, как пользователь задал все необходимые значения, можно нажимать кнопку «Рассчитать» и получать результат – одна ARX-подстановка, заданной итеративной генерации и её характеристики.

**Результаты:**

Используемые пары: (1, 1), (1, 2), (1, 3), (2, 1), (2, 1)

Количество итераций: 5

Характеристики:

- Разностная характеристика: 0.00390625
- Линейная характеристика: 0.4375
- Степень нелинейности: 4

Сгенерированная подстановка (256 чисел):

0	131	70	197	147	186	92	17	234	12	246	217	114	245
---	-----	----	-----	-----	-----	----	----	-----	----	-----	-----	-----	-----

Рис.

5: Результат генерации

5. Далее значения параметров можно менять в свободной форме и генерировать иные значения подстановок.