**S-box**

Харьков 2020

**Функциональное назначение и структура**

Программное обеспечение (ПО) Sbox предназначено для генерации нелинейных узлов замены (S-блоков). ПО предусматривает генерацию S-блоков на основе различных векторных булевых функций и с различной нелинейностью.

Структурная схема ПО приведена на рис.1. Файл параметров конфигурации parameters.txt поступает на вход программы Generation\_Sboxes. Для генерации нелинейных таблиц замены программа использует файл со случайными данными (источник энтропии). Результатом работы программы являются сгенерированные S-блоки, которые вместе с их характеристиками записываются в файл S-boxes.txt.

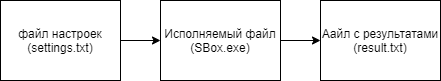


Рис. 1. Структурная схема ПО

**Технические средства**

ПО может использоваться на персональном компьютере с операционными системами Windows, Linux.

**Вызов и загрузка**

Для того чтобы выполнить генерацию S-блока необходимо выполнить следующие шаги.

1. В директорию с файлом Sbox.exe поместить файл с настройками. Если файл не буде обнаружен, то установятся значения по умолчанию.\

2. Из командной строки или двойным щелчком запустить файл Sbox.exe.

3. Необходимо дождаться сообщения об успешном завершении работы программы.

**Входные данные**

Входные данные для работы программы задаются пользователем в файле параметров конфигурации settings.txt. Пример файла параметров конфигурации settings.txt приведен в приложении А. В файле settings.txt необходимо задать значения параметров, представленных в табл. 1.

Таблица 1

|  |  |  |
| --- | --- | --- |
| Имя параметра | Описание параметра | Допустимые значения |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

После имени параметра и знака «:» необходимо ввести значение данного параметра, если этого не будет сделано будут взяты параметры по умолчанию.

**Выходные данные**

Выходными данными работы программы является сгенерированный S-блок, с желаемыми параметрами, или максимально приближенный к ним. В результате работы программы создается файл result.txt, в который записываются характеристики сгенерированного S-блока, сам S-блок и время, затраченное на его генерацию. При каждом новом запуске программы предыдущее содержимое файла result.txt удаляется. Примеры сформированных S-блоков приведены в приложении Б.

**Обработка ошибок**

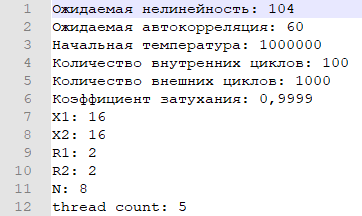
В табл. 2 приведен список ошибок, которые могут возникнуть в процессе работы программы.

Таблица 2

Сообщение об ошибке Причина ошибки Can't open file parameters.txt! Check that file parameters.txt exists and it is in the same folder than Generation\_Sboxes.exe. Файл параметров конфигурации parameters.txt отсутствует в папке с исполняемым файлом. The value of initial\_powis incorrect! Please, check it in parameters.txt Значение параметра initial\_pow некорректно. Необходимо удостовериться, что введенное значение входят в список допустимых значений, прописанный в файле parameters.txt. The value of number\_Sboxes is incorrect! Please, check it in parameters.txt Значение параметра number\_Sboxes некорректно. Необходимо удостовериться, что введенное значение входят в список допустимых значений, прописанный в файле parameters.txt. The value of non\_linearity is incorrect! Please, check it in parameters.txt Значение параметра non-linearity некорректно. Необходимо удостовериться, что введенное значение входят в список допустимых значений, прописанный в файле parameters.txt. Can't open file "имя\_файла"! Check value of random\_data in parameters.txt Невозможно открыть файл со случайными данными. Возможно, имя файла задано некорректно в файле parameters.txt. File "имя\_файла" is empty! Please, check value of random\_data in parameters.txt Файл со случайными данными пуст. File parameters.txt was corrupted! There no 'initial\_pow' parameter. Нарушена целостность файла parameters.txt: отсутствует параметр initial\_pow. File parameters.txt was corrupted! There no 'number\_Sboxes' parameter. Нарушена целостность файла parameters.txt: отсутствует параметр number\_Sboxes. 5 Таблица 2 (продолжение) Сообщение об ошибке Причина ошибки File parameters.txt was corrupted! There no 'non\_linearity' parameter. Нарушена целостность файла parameters.txt: отсутствует параметр nonlinearity. File parameters.txt was corrupted! There no 'random\_data' parameter. Нарушена целостность файла parameters.txt: отсутствует параметр random\_data. Warning: the end of file with random data! Достигнут конец файла со случайными данными. Generation has been interrupted. "количество\_сгенерированных\_Sблоков" S-boxes are in S-boxes.txt Генерация подстановок преждевременно завершена в виду достижения конца файла со случайными данными.

**Приложение А**

Пример файла параметров конфигурации settings.txt



**Приложение Б**

Пример сформированногоS-блока

