Поиск эффективно реализуемых подстановок с оптимальными криптографическими характеристиками

Чичаева Анастасия Александровна

Студент

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: ac17@bk.ru

Научный руководитель *— Применко Эдуард Андреевич*

Подстановки (S-блоки) являются неотъемлемой частью почти всех современных блочных шифров. В частности, они используются в таких известных шифрах, как : AES, ГОСТ 34.12 – 2018. Подстановки зачастую являются единственным нелинейным преобразованием в алгоритме, поэтому они должны быть тщательно выбраны для того, чтобы шифр был устойчив к различным атакам. При построении блочных шифров есть два основных подхода для выбора S-блока, можно выбрать случайную большую подстановку, либо маленькие, но с хорошими криптографическими характеристиками. При этом большие подстановки имеют существенный недостаток, связанный с эффективностью их реализации. Поэтому при выборе хорошей подстановки важно уделять внимание не только криптографическим характеристикам, но и эксплуатационным.

Данная работа сфокусирована на 4-битовых подстановках. Такие подстановки являются составной частью некоторых шифров, а также могут использоваться для генерации 8-битовых подстановок с хорошими криптографическими характеристиками [1]. 4-битовые подстановки хорошо изучены и для них известны оптимальные значения криптографических характеристик.

В работе исследуется вопрос эффективной реализации подстановок, в частности для рассмотрения выбрана их битовая (: bit-slice) реализация. Битовое представление подстановок — это представление подстановки в виде битовых инструкций, таких как : NOT, XOR, AND, OR, MOV. Такая реализация позволяет использовать параллельные вычисления, ведь современные процессоры работают с регистрами длиной большей чем 1 бит.

Вопрос битового представления 4-битовых подстановок был рассмотрен в работах [2–3]. Авторы [2] искали оптимальных представителей классов аффинной эквивалентности 4-битовых подстановок. Оптимальным представителем класса называется подстановка, битовая реализация которой требует наименьшего числа инструкций.

В результате авторами были найдены наиболее эффективные представители для 272 из 302 классов аффинной эквивалентности.

В данной работе изучается битовое представление подстановок из оставшихся классов эквивалентности, описаны методы поиска эффективных представителей и приведены результаты исследования. В итоге был проведен поиск эффективно реализуемых подстановок из 30 классов аффинной эквивалентности, для которых ранее не были обнаружены представители. В результате поиска были найдены представители для 10 классов, которые обладают хорошими криптографическими и эксплуатационными характеристиками. Найденные подстановки можно использовать в дальнейшем при создании новых криптографических механизмов.

Литература

1. Canteaut A., Duval S., Leurent G. Construction of Lightweight S-Boxes using Feistel and MISTY structures //IACR Cryptol. ePrint Arch. 2015. Т. 2015, С. 711.
2. Ullrich M., De Canniere C., Indesteege S., Kucuk O., Mouha N., Preneel B. Finding optimal bitsliced implementations of 4×4-bit S-boxes //SKEW 2011 Symmetric Key Encryption Workshop, Copenhagen, Denmark. 2011. С. 16–17.
3. Clavier C. and Reynaud L. Systematic and Random Searches for compact 4-Bit and 8-Bit Cryptographic S-Boxes : дис. IACR Cryptology ePrint Archive, 2019.