Методы генерации Rijndael S-блоков и их модификации

Криптографические S-блоки являются важным компонентом в структуре различных видов криптографических алгоритмов. Их криптографические свойства напрямую влияют на устойчивость криптографических алгоритмов к различным криптоаналитическим атакам. Таким образом, генерация криптографических S-блоков с необходимыми криптографическими характеристиками является безусловно актуальной и важной задачей.

Существуют три основных подхода в построении S-блоков: алгебраические конструкции, псевдослучайная генерация, эвристический подход.

При алгебраическом подходе S-блоки проектируются в соответствии с некоторыми доказанными математическими соотношениями и принципами. Классическим алгебраическим методом генерации S-блоков является метод, основанный на применении одного из ряда преобразований, приведенных в работе Ниберга [1], в комбинации с аффинными преобразованиями. С помощью этого метода был построен S-блок для алгоритма Rijndael [2] (победитель конкурса AES). Существует ряд модификаций этого метода, основанные на варьировании выбора определенного неприводимого многочлена, по модулю которого определяется умножение в поле $GF(2^8)$, выбора первого преобразования из альтернативных преобразований в работе Ниберга, выбора определенной матрицы аффинного преобразования и выбора определенной сдвиговой константы. Т.е. можно построить другие S-блоки, варьируя наборы выбираемых компонентов, используемых в конструкции наподобие Rijndael S-блока.

Далее рассматривается этот метод и ряд его модификаций.

В криптографическом алгоритме симметричного блочного шифрования Rijndael S-блок $F: GF(2^8) \to GF(2^8)$ определяется как композиция $F = g \circ f$ двух преобразований $g: GF(2^8) \to GF(2^8)$ и $f: GF(2^8) \to GF(2^8)$ []. Первое преобразование $g: GF(2^8) \to GF(2^8)$ определяется по формулам: $g(a) = \begin{cases} a^{-1}, \text{если } a \neq 0 \\ 0, \text{если } a = 0 \end{cases}$, где $a \in GF(2^8)$, a^{-1} – обратный элемент для a относительно умножения в поле $GF(2^8)$, 0 – нулевой элемент поля $GF(2^8)$. Умножение выполняется по модулю неприводимого многочлена $m(x) = x^8 + x^4 + x^3 + x + 1$ ($11B$ в шестнадцатеричном представлении или 100011011 в двоичном). Второе преобразование $f: GF(2^8) \to GF(2^8)$ является аффинным преобразованием и определяется по формуле: $f(a) = b$, где

$$\begin{pmatrix} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{pmatrix} = \begin{pmatrix} 11111000 \\ 01111100 \\ 00111110 \\ 00011111 \\ 10001111 \\ 11000111 \\ 11100011 \\ 11110001 \end{pmatrix} \times \begin{pmatrix} a_7 \\ a_6 \\ a_5 \\ a_4 \\ a_3 \\ a_2 \\ a_1 \\ a_0 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}.$$

Таким образом, $F(a) = f\big(g(a)\big)$ для любого $a \in GF(2^8)$. Аффинное преобразование f в полиномиальном представлении определяется следующим образом: $b(x) = u(x) \times a(x) \oplus v(x) \, mod \, x^8 + 1$, где $b(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$ - полиномиальное представление элемента b, $a(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ - полиномиальное представление элемента a, $u(x) = 0x^7 + 0x^6 + 0x^5 + 1x^4 + 1x^3 + 1x^2 + 1x + 1 = x^4 + x^3 + x^2 + x + 1$ – многочлен, соответствующий матрице аффинного преобразования, $v(x) = 0x^7 + 1x^6 + 1x^5 + 0x^4 + 0x^3 + 0x^2 + 1x + 1 = x^6 + x^5 + x + 1$ – полиномиальное представление сдвиговой константы.

Применение интерполяции Лагранжа дает полиномиальное представление S-блока $F(x) = 05 \cdot x^{254} + 09 \cdot x^{253} + \mathrm{F9} \cdot x^{251} + 25 \cdot x^{247} + \mathrm{F4} \cdot x^{239} + 01 \cdot x^{223} + \mathrm{B5} \cdot x^{191} + 8\mathrm{F} \cdot x^{127} + 63$ с коэффициентами из $GF(2^8)$.

Неприводимый многочлен, по модулю которого определяется умножение в поле $GF(2^8)$, выбран из списка 30 неприводимых многочленов степени 8 [3].

№	Неприводимый многочлен 8 степени	Двоичное представление	Шестнадцатеричное представление
1	$x^8 + x^4 + x^3 + x + 1$	100011011	$11B$
2	$x^8 + x^4 + x^3 + x^2 + 1$	100011101	$11D$
3	$x^8 + x^5 + x^3 + x + 1$	100101011	$12B$
4	$x^8 + x^5 + x^3 + x^2 + 1$	100101101	$12D$
5	$x^8 + x^5 + x^4 + x^3 + 1$	100111001	139
6	$x^8 + x^5 + x^4 + x^3 + x^2 + x + 1$	100111111	$13F$
7	$x^8 + x^6 + x^3 + x^2 + 1$	101001101	$14D$
8	$x^8 + x^6 + x^4 + x^3 + x^2 + x + 1$	101011111	$15F$
9	$x^8 + x^6 + x^5 + x + 1$	101100011	163
10	$x^8 + x^6 + x^5 + x^2 + 1$	101100101	165
11	$x^8 + x^6 + x^5 + x^3 + 1$	101101001	169
12	$x^8 + x^6 + x^5 + x^4 + 1$	101110001	171

13	$x^8+x^6+x^5+x^4+x^2+x+1$	101110111	177
14	$x^8+x^6+x^5+x^4+x^3+x+1$	101111011	$17B$
15	$x^8+x^7+x^2+x+1$	110000111	187
16	$x^8+x^7+x^3+x+1$	110001011	$18B$
17	$x^8+x^7+x^3+x^2+1$	110001101	$18D$
18	$x^8+x^7+x^4+x^3+x+1$	110011011	$19F$
19	$x^8+x^7+x^5+x+1$	110100011	$1A3$
20	$x^8+x^7+x^5+x^3+1$	110101001	$1A9$
21	$x^8+x^7+x^5+x^4+1$	110110001	$1B1$
22	$x^8+x^7+x^5+x^4+x^3+x^2+1$	110111101	$1BD$
23	$x^8+x^7+x^6+x+1$	111000011	$1C3$
24	$x^8+x^7+x^6+x^3+x^2+x+1$	111001111	$1CF$
25	$x^8+x^7+x^6+x^4+x^2+x+1$	111010111	$1D7$
26	$x^8+x^7+x^6+x^4+x^3+x^2+1$	111011101	$1DD$
27	$x^8+x^7+x^6+x^5+x^2+x+1$	111100111	$1E7$
28	$x^8+x^7+x^6+x^5+x^4+x+1$	111110011	$1F3$
29	$x^8+x^7+x^6+x^5+x^4+x^2+1$	111110101	$1F5$
30	$x^8+x^7+x^6+x^5+x^4+x^3+1$	111111001	$1F9$

Первое преобразование является одним из преобразований, перечисленных в работе Ниберга [1], определяющих S-блоки с хорошей нелинейностью. Это преобразование имеет очень простое алгебраическое выражение. Поэтому применяется комбинация со вторым преобразованием, являющимся обратимым аффинным преобразованием. Второе преобразование не влияет на нелинейность, имеет простое описание, но в комбинации с первым преобразованием дает сложное алгебраическое выражение для S-блока. Многочлен $v(x)=0x^7+1x^6+1x^5+0x^4+0x^3+0x^2+1x+1=x^6+x^5+x+1$, представляющий сдвиговую константу 63 (в шестнадцатеричном представлении) или 01100011 (в двоичном), выбран таким образом, что S-блок не имеет неподвижных точек (т.е. таких элементов $a \in GF(2^8)$, что $F(a)=a$) и противоположных неподвижных точек (т.е. таких элементов $a \in GF(2^8)$, что $F(a)=\bar{a}$, где $a \oplus \bar{a}=0$).

Таким образом, Rijndael S-блок конструируется на основе выбора определенного неприводимого многочлена, по модулю которого определяется умножение в поле $GF(2^8)$, выбора первого преобразования из альтернативных преобразований в работе Ниберга, выбора определенной матрицы аффинного преобразования и выбора определенной

сдвиговой константы. Аналогичным образом, можно построить другие S-блоки, варьируя наборы выбираемых компонентов, используемых в конструкции наподобие Rijndael S-блока.

Например, в работе [4] аналогичные S-блоки построены на основе выбора неприводимого многочлена $m(x) = x^8 + x^4 + x^3 + x^2 + 1$ ($11D$ в шестнадцатеричном представлении или 100011101 в двоичном) и целого ряда сдвиговых констант таких, что построенные S-блоки не имеют неподвижных точек и противоположных неподвижных точек. Список 36 выбранных констант приведен ниже:

$$0A, 0F, 15, 2A, 2B, 31, 32, 35, 38, 40, 4A, 4E, 54, 5E, 62, 6E, 74, 7E,$$
$$F5, F0, EA, D5, D4, CE, CD, CA, C7, BF, B5, B1, AB, A1, 9D, 91, 2B, 81.$$

В работе [5] Rijndael-подобные S-блоки построены на основе выбора матриц аффинного преобразования. Неприводимый многочлен, сдвиговая константа, первое преобразование определяются также как в Rijndael S-блоке. Всего существует 255 матриц аффинного преобразования 8-го порядка. Из них только 190 матриц являются обратимыми. Используя эти обратимые матрицы, были построены 190 Rijndael-подобных S-блоков. Однако не все из них не имеют неподвижных точек и противоположных неподвижных точек. 79 S-блоков, построенных с помощью этих матриц, обладают одной или двумя неподвижными точками. Ряд S-блоков не удовлетворяют ряду других критериев. В тоже время ряд построенных S-блоков обладают характеристиками, лучшими чем Rijndael S-блок. Ниже приведены примеры матриц аффинного преобразования из работы [5].

$$A_1 = \begin{pmatrix} 00011010 \\ 00001101 \\ 10000110 \\ 01000011 \\ 10100001 \\ 11010000 \\ 00110100 \\ 00011010 \end{pmatrix},\ A_2 = \begin{pmatrix} 11001000 \\ 01100100 \\ 00110010 \\ 00011001 \\ 10001100 \\ 01000110 \\ 00100011 \\ 10010001 \end{pmatrix},\ A_3 = \begin{pmatrix} 11011100 \\ 01101110 \\ 00110111 \\ 10011011 \\ 11001101 \\ 11100110 \\ 01110011 \\ 10111001 \end{pmatrix},\ A_4 = \begin{pmatrix} 11101111 \\ 11110111 \\ 11111011 \\ 11111101 \\ 11111110 \\ 01111111 \\ 10111111 \\ 11011111 \end{pmatrix},\ A_5 =$$

$$\begin{pmatrix} 10110101 \\ 11011010 \\ 01101101 \\ 10110110 \\ 01011011 \\ 10101101 \\ 11010110 \\ 01101011 \end{pmatrix},\quad A_6 = \begin{pmatrix} 11010101 \\ 11101010 \\ 01110101 \\ 10111010 \\ 01011101 \\ 10101110 \\ 01010111 \\ 10101011 \end{pmatrix},\quad A_7 = \begin{pmatrix} 01110000 \\ 00111000 \\ 00011100 \\ 00001110 \\ 00000111 \\ 10000011 \\ 11000001 \\ 11100000 \end{pmatrix},\quad A_8 = \begin{pmatrix} 11101001 \\ 11110100 \\ 01111010 \\ 00111101 \\ 10011110 \\ 01001111 \\ 10100111 \\ 11010011 \end{pmatrix},\quad A_9 =$$

$$\begin{pmatrix} 01111010 \\ 00111101 \\ 10011110 \\ 01001111 \\ 10100111 \\ 11010011 \\ 11101001 \\ 11110100 \end{pmatrix}, A_{10} = \begin{pmatrix} 01111100 \\ 00111110 \\ 00011111 \\ 10001111 \\ 11000111 \\ 11100011 \\ 11110001 \\ 11111000 \end{pmatrix}.$$

В работе [6] построены 30 различных Rijndael S-блоков, выбирая неприводимые многочлены из списка 30 неприводимых многочленов степени 8 [3].

Существует еще одна модификация метода конструирования Rijndael S-блоков, основанная на последовательном применении аналогичных преобразований.

В работе [7] S-блок $F: GF(2^8) \to GF(2^8)$ определяется как композиция $F = f \circ g \circ f$ с помощью двух преобразований $g: GF(2^8) \to GF(2^8)$ и $f: GF(2^8) \to GF(2^8)$. Первое преобразование $g: GF(2^8) \to GF(2^8)$ определяется по формулам: $g(a) = \begin{cases} a^{-1}, \text{если } a \neq 0 \\ 0, \text{если } a = 0 \end{cases}$, где $a \in GF(2^8)$, a^{-1} – обратный элемент для a относительно умножения в поле $GF(2^8)$, 0 – нулевой элемент поля $GF(2^8)$. Умножение выполняется по модулю неприводимого многочлена $m(x) = x^8 + x^4 + x^3 + x + 1$ ($11B$ в шестнадцатеричном представлении или 100011011 в двоичном). Т.е. используются то же преобразование из работы Ниберга [3] и тот же неприводимый многочлен, что и в Rijndael S-блоке. Второе преобразование $f: GF(2^8) \to GF(2^8)$ является аффинным преобразованием и определяется по формуле: $f(a) = b$, где

$$\begin{pmatrix} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{pmatrix} = \begin{pmatrix} 11011010 \\ 01101101 \\ 10110110 \\ 01011011 \\ 10101101 \\ 11010110 \\ 01101011 \\ 10110101 \end{pmatrix} \times \begin{pmatrix} a_7 \\ a_6 \\ a_5 \\ a_4 \\ a_3 \\ a_2 \\ a_1 \\ a_0 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}.$$

Таким образом, $F(a) = f\big(g(f(a))\big)$ для любого $a \in GF(2^8)$. Аффинное преобразование f отличается от аналогичного в Rijndael S-блоке и использует другие аффинную матрицу и сдвиговую константу. Более того в отличие от Rijndael S-блока для построения конечного результата (S-блока) аффинное преобразование применяется дважды. В полиномиальном представлении преобразование определяется следующим образом: $b(x) = u(x) \times a(x) \oplus v(x) \, mod \, x^8 + 1$, где $b(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$ - полиномиальное представление элемента b, $a(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ - полиномиальное представление элемента a, $u(x) = 0x^7 + 1x^6 + 0x^5 + 1x^4 + 1x^3 + 0x^2 + 1x + 1 = x^6 + x^4 + x^3 + x + 1$ – многочлен, соответствующий матрице аффинного преобразования, $v(x) = 0x^7 + 1x^6 + 0x^5 + 1x^4 + 1x^3 + 1x^2 + 0x + 1 = x^6 + x^4 + x^3 + x^2 + 1$ – полиномиальное представление сдвиговой константы.

Существует еще один метод получения новых S-блоков из уже известных, в частности, из Rijndael-подобных S-блоков. Имеющий S-блок рассматривается в табличном представлении. Элементы соответствующей таблицы рассматриваются в двоичной форме. И к ним применяются перестановки из группы перестановок S_8. В результате получаются 40320 новых S-блоков. Например, в работе [8] такой подход применяется к оригинальному Rijndael S-блоку, получая в результате 40320 новых Rijndael-подобных S-блоков.

На основе вышеописанных методов генерации Rijndael-подобных S-блоков можно сформулировать следующий обобщенный метод [9].

1) Выбирается неприводимый многочлен из списка 30 неприводимых многочленов 8-ой степени [3].

2) Выбирается одно из преобразований, перечисленных в работе Ниберга [1].

3) Выбирается обратимая

матрица аффиного преобразования.

4) Выбирается сдвиговая константа аффинного преобразования.

5) Выбирается и осуществляется определенная последовательность выбранных преобразований.

6) К элементам табличного представления полученного S-блока применяется перестановка из группы перестановок S_8.

7) Проверка полученного S-блока на соответствие критериям оптимальности.

Рассмотренные методы генерации S-блоков позволяют получить новые S-блоки, обладающие необходимыми криптографическими свойствами, такими же или даже лучше, чем у S-блока, построенного для алгоритма Rijndael.

1. Nyberg, K. Differentially uniform mappings for cryptography // Advances in Cryptology, Proc. Eurocrypt'93, LNCS 165, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 55-64.

2. Daemen, J., Rijmen, V. The Design of Rijndael: AES - The Advanced Encryption Standard // Springer-Verlag Berlin Heidelberg, 2002, 238 p., doi: 10.1007/978-3-662-04722-4.

3. Church, R. Tables of irreducible polynomials for the first four prime moduli // The Annals of Maths., 2nd Series, vol. 36, no. 1, pp. 198-209, Jan (1935) http://www .jstor.org/stable/1968675.

4. Das, S., Uz Zaman, J.K.M.S., Ghosh, R. Generation of AES S-boxes with Various Modulus and Additive Constant Polynomials and Testing their Randomization // Procedia Technology, Volume 10, 2013, pp. 957-962, ISSN 2212-0173, https://doi.org/10.1016/j.protcy.2013.12.443.

5. Waqas, U., Afzal, S., Mir, M., Yousaf, M. Generation of AES-Like S-Boxes by Replacing Affine Matrix // 2014 12th International Conference on Frontiers of Information Technology (FIT), Islamabad, Pakistan, 2014, pp. 159-164. doi: 10.1109/FIT.2014.38

6. Wang, D., Sun, S.L. Replacement and Structure of S-boxes in Rijndael // Computer Science and Software Engineering, 2008 International Conference, December 2008, pp. 782-784, doi: 10.1109/CSSE.2008.296.

7. Cui, J., Huang, L., Zhong, H., Chang, C., Yang, W. An improved AES S-box and its performance analysis // International Journal of Innovative Computing, Information and Control, Volume 7, Number 5(A), 2011, pp. 2291–2302.

8. Hussain, I., Shah, T., Hasan, M. A New Algorithm to Construct Secure Keys for AES // Int. J. Contemp. Math. Sciences. 5, 2010, pp.1263-1270.

9. Оспанов, Р., Сейткулов, Е., Ергалиева, Б. (2022). Обобщенный алгебраический метод конструирования 8-битных Rijndael S-блоков. Вестник КазАТК, 120(1), 156–163. https://doi.org/10.52167/1609-1817-2022-120-1-156-163