УДК 512.624.2

Сибирский журнал науки и технологий. 2017. Т. 18, № 3. С. 505–509

ВОЗМОЖНЫЕ ВАРИАНТЫ ПОВЫШЕНИЯ КРИПТОСТОЙКОСТИ АЛГОРИТМОВ ШИФРОВАНИЯ НА ОСНОВЕ КОНСТРУКЦИИ НИБЕРГ

М. А. Дмитриев

Сибирский федеральный университет
Российская Федерация, 660041, г. Красноярск, просп. Свободный, 79
E-mail: makcmad@mail.ru

В настоящее время одним из наиболее применяемых средств обеспечения защиты информации от несанкционированного доступа являются блочные симметричные криптографические алгоритмы, как, например, рассматриваемый в данной статье алгоритм Rijndael. Стремительный рост вычислительной мощности ЭВМ и существенное развитие линейного криптоанализа делают актуальной задачу дальнейшего наращивания криптостойкости существующих алгоритмов, а также разработки новых. Важным компонентом, определяющим устойчивость блочного симметричного криптографического алгоритма к наиболее распространенным видам криптоанализа, является качество блока замен – S-блока подстановки. Цель работы – провести вычисления и получить все возможные блоки замен на основе неприводимых полиномов над полем $GF(2^8)$, а также их композиций. Для этого был разработан ряд программ, с помощью которых были получены блоки замен, обладающие различными криптографическими характеристиками. Был произведен расчет количественных оценок данных характеристик путем представления таблиц замен в виде наборов булевых функций. Особое внимание было уделено таким характеристикам, как нелинейность булевых функций, максимум модуля коэффициентов корреляции и количество нулей корреляционной матрицы блоков замен, как наиболее значимым характеристикам. Полученные блоки замен могут стать основой для дальнейшего изучения возможных вариантов повышения криптостойкости алгоритма Rijndael.

Ключевые слова: алгоритм Rijndael, S-блок, неприводимый полином над полем Галуа.

Siberian Journal of Science and Technology. 2017, Vol. 18, No. 3, P. 505–509

POSSIBLE OPTIONS TO IMPROVE CRYPTOGRAPHIC RELIABILITY OF ALGORITHMS BASED ON NYBERG CONSTRUCTION

M. A. Dmitriev

Siberian Federal University
79, Svobodny Av., Krasnoyarsk, 660041, Russian Federation
E-mail: makcmad@mail.ru

Nowadays one of the most used tools to protect data from unauthorized access is block symmetric-key cryptographic algorithms. The rapid growth of computer processing power and significant development of linear cryptanalysis actualize the task to continue increasing reliability of the existing algorithms, as well as developing new ones. An important component in determining the stability of a block symmetric-key cryptographic algorithm to the most common types of cryptanalysis is the quality of S-box substitution. This work was aimed at calculating and achieving all possible S-box substitutions, based on irreducible polynomials over the Galois field and their compositions. For this purpose a set of programs to obtain S-box substitutions which have different cryptographic characteristics with its help was developed. Calculation of the quantitative values of these characteristics was performed by presenting S-box substitutions in the form of sets of Boolean functions. Particular attention was paid to such characteristics as nonlinearity of Boolean functions, the maximum modulus of the correlation coefficients and the numbers of zeros of the correlation matrix of S-box substitutions, as those are the most important characteristics. These blocks substitutions can be the basis for further study of possible options to improve Rijndael algorithm's cryptographic reliability.

Keywords: Rijndael algorithm, S-box, irreducible polynomial over the Galois field.

Введение. Применительно к формированию таблиц замен можно выделить три основных подхода в разработке алгоритмов шифрования [1].

Одним из решений является выбор таблиц замен в процессе разработки стандарта и открытое опубликование полученных таблиц, одинаковых для всех пользователей данного алгоритма. Такой подход был реализован в алгоритме DES, а в 2015 году применен в алгоритме «Кузнечик», ставшем стандартом Российской Федерации с 2016 года [2].

Применяются также алгоритмы, в которых таблицы замен не определены однозначно, а выбираются каждым пользователем самостоятельно. Такой подход реализован, например, в алгоритме ГОСТ 28147–89 [3; 4], долгое время являвшемся стандартом СССР и позднее многих стран СНГ. Отметим, что при надлежащем уровне квалификации пользователь имеет возможность выбрать качественные блоки замен, притом известные только этому пользователю, что можно трактовать как дополнительное повышение стойкости шифрования.

Блочный шифр Rijndael. Наиболее характерным примером третьего подхода может служить также считающийся стойким алгоритм Rijndael [5], в котором блок замен полностью определяется заданием неприводимого полинома над полем Галуа [6]. В Rijndael использована конструкция Ниберг, представляющая собой отображение в виде мультипликативно обратных элементов поля Галуа $GF\left(2^k\right)$:

$$y = x^{-1} \bmod d[f(z), p], \quad y, x \in GF\left(2^k\right), \qquad (1)$$

скомбинированная вместе с аффинным преобразованием

$$b = A \cdot y + a, \quad a, b \in GF\left(2^k\right), \qquad (2)$$

где $f(z) = z^8 + z^4 + z^2 + z + 1$ – неприводимый над полем $GF\left(2^8\right)$ полином; A – невырожденная матрица аффинного преобразования; a – вектор сдвига; $p = 2$ – характеристика расширенного поля Галуа; $0^{-1} \equiv 0$ – по определению; a, b, x, y – элементы расширенного поля Галуа $GF\left(2^k\right)$; рассматриваются как десятичные числа либо двоичные векторы, либо полиномы степени $k-1$.

Количественные характеристики блоков замен. Показателями качества блока замен [7–9] наиболее часто предлагаются следующие:

– максимум из модулей элементов матрицы коэффициентов корреляции входных и выходных битов;

– количество нулей в матрице коэффициентов корреляции;

– нелинейность как расстояние до множества аффинных функций [10–13];

– алгебраическая степень нелинейности [14];

– период возврата подстановочной конструкции в исходное состояние.

На данный момент подробно исследованы нелинейные преобразования конструкции Ниберг на основе всех изоморфных и автоморфных представлений полей $GF\left(2^k\right)$ для $k \le 8$: выписаны все неприводимые полиномы над полями, вычислены криптографические показатели качества определяемых этими полиномами *S*-блоков. Таким образом, полином из (1) является не единственно возможным для построения шифра. Возможность же выбора неприводимого полинома (одного из множества в определенном смысле эквивалентных) имеет практическое значение. Поэтому появилась возможность соединить плюсы подходов ГОСТа и Rijndael.

В работе [5] приведена таблица криптографических характеристик *S*-блоков на базе полного класса неприводимых полиномов степени 8. Данные этой таблицы свидетельствуют о разнообразии выбора полиномов для использования в блочных шифрах в соответствии с решением использования того или иного критерия.

В связи с этим представляется актуальным рассмотрение конструкции, аналогичной AES [15], однако либо с использованием композиции неприводимых полиномов, либо с использованием в разных раундах различных полиномов или их композиций, что можно считать одним из возможных вариантов повышения стойкости алгоритма, аналогичного AES.

В данной статье проведены вычисления и получены все возможные таблицы замен на основе композиции неприводимых полиномов над $GF(2^8)$. Композицией неприводимых полиномов считается последовательное выполнение двух операций SubBytes в каждом раунде. Определены пары полиномов, обеспечивающих таблицы замен с близкими к оптимальным свойствами корреляционной матрицы.

Табл. 1 представляет собой данные по криптографическим характеристикам *S*-блоков, полученных в результате выполнения операции SubBytes для всех возможных неприводимых полиномов над $GF(2^8)$, где сам полином записан в виде десятичных эквивалентов.

Аналогичные данные были получены для композиций неприводимых полиномов (в графе «Композиция» полиномы записаны в порядке выполнения операции SubBytes). Ввиду большого объема полученных данных в данной статье хотелось бы заострить внимание на тех композициях, корреляционная матрица которых обладает наиболее примечательными криптографическими характеристиками. Полученные данные приведены в табл. 2–4.

Таблица 1

Криптографические характеристики *S*-блоков неприводимых полиномов

№ п/п	Полином	Максимум модуля	Количество нулей	Степень нелинейности							
1	283	**0,125**	4	112	112	112	112	112	112	112	112
2	285	**0,125**	5	112	112	112	112	112	112	112	112
3	299	**0,125**	10	112	112	112	112	112	112	112	112
4	301	**0,125**	2	112	112	112	112	112	112	112	112
5	313	**0,125**	7	112	112	112	112	112	112	112	112

Окончание табл. 1

№ п/п	Полином	Максимум модуля	Количество нулей	Степень нелинейности							
6	319	0,109375	6	112	112	112	112	112	112	112	112
7	333	**0,125**	7	112	112	112	112	112	112	112	112
8	351	**0,125**	2	112	112	112	112	112	112	112	112
9	355	0,109375	2	112	112	112	112	112	112	112	112
10	357	**0,09375**	6	112	112	112	112	112	112	112	112
11	361	**0,125**	4	112	112	112	112	112	112	112	112
12	369	**0,125**	5	112	112	112	112	112	112	112	112
13	375	0,109375	2	112	112	112	112	112	112	112	112
14	379	**0,125**	3	112	112	112	112	112	112	112	112
15	391	**0,125**	5	112	112	112	112	112	112	112	112
16	395	**0,125**	5	112	112	112	112	112	112	112	112
17	397	0,109375	5	112	112	112	112	112	112	112	112
18	415	0,109375	3	112	112	112	112	112	112	112	112
19	419	0,109375	**11**	112	112	112	112	112	112	112	112
20	425	0,109375	3	112	112	112	112	112	112	112	112
21	433	0,109375	2	112	112	112	112	112	112	112	112
22	463	**0,125**	3	112	112	112	112	112	112	112	112
23	445	**0,125**	**0**	112	112	112	112	112	112	112	112
24	451	0,109375	3	112	112	112	112	112	112	112	112
25	471	**0,125**	3	112	112	112	112	112	112	112	112
26	477	**0,125**	4	112	112	112	112	112	112	112	112
27	487	**0,125**	3	112	112	112	112	112	112	112	112
28	499	**0,125**	7	112	112	112	112	112	112	112	112
29	501	0,109375	4	112	112	112	112	112	112	112	112
30	505	**0,125**	8	112	112	112	112	112	112	112	112

Таблица 2

Композиции с максимальным и минимальным значением максимума модуля корреляционной матрицы

№ п/п	Композиция	Максимум модуля	Количество нулей	Степень нелинейности							
1	301–477	**0,109375**	6	102	102	106	106	102	98	102	108
2	319–477	**0,296875**	6	102	94	106	100	104	102	104	96
3	357–433	**0,109375**	7	106	104	104	104	104	108	104	100
4	361–351	**0,109375**	4	104	106	102	102	106	106	106	102
5	369–361	**0,109375**	7	106	102	102	108	106	102	106	102
6	369–375	**0,109375**	10	104	104	108	104	104	102	104	104
7	369–395	**0,109375**	4	108	106	102	102	106	102	106	106
8	391–283	**0,109375**	3	104	104	102	104	104	104	104	104
9	391–433	**0,109375**	7	104	100	104	104	106	106	106	104
10	425–313	**0,109375**	8	104	104	104	102	106	100	106	104
11	463–357	**0,109375**	4	104	104	102	102	102	98	102	102
12	445–333	**0,109375**	13	104	104	106	106	106	102	106	100
13	451–369	**0,109375**	10	102	98	104	104	106	106	106	106
14	471–375	**0,109375**	10	100	98	104	102	106	104	106	106
15	501–425	**0,109375**	6	102	102	104	104	106	108	106	104

Таблица 3

Композиции с максимальным и минимальным значением нелинейности

№ п/п	Композиция	Максимум модуля	Количество нулей	Степень нелинейности							
1	283–351	0,203125	9	104	102	102	104	**110**	102	**110**	106
2	299–285	0,171875	8	**110**	104	102	102	104	102	104	102
3	299–445	0,140625	5	104	104	104	106	**110**	108	**110**	106
4	301–285	0,15625	9	100	98	104	106	**110**	106	**110**	104
5	301–375	0,125	7	106	106	106	106	106	**110**	106	102
6	319–499	0,140625	4	**110**	108	106	102	108	106	108	100
7	351–299	0,171875	5	106	106	**110**	104	106	106	106	108
8	351–357	0,140625	4	102	102	104	106	**110**	104	**110**	102
9	355–471	0,171875	5	106	104	104	**110**	106	104	106	106
10	361–299	0,15625	4	106	102	104	**88**	102	100	102	104
11	361–477	0,125	7	**110**	106	104	104	106	106	106	102
12	379–415	0,1875	5	108	102	**110**	100	104	104	104	108
13	419–471	0,1875	7	106	106	104	**110**	102	96	102	104
14	425–299	0,140625	6	104	108	96	104	106	**110**	106	106
15	433–357	0,203125	6	**110**	102	106	104	104	106	104	104
16	451–319	0,140625	7	102	106	104	96	104	98	104	**110**
17	451–451	0,203125	8	100	102	104	100	108	106	108	**110**
18	451–505	0,15625	4	102	106	**110**	104	100	98	100	98
19	487–299	0,15625	5	104	106	104	102	106	100	106	**110**
20	505–283	0,125	2	106	104	102	106	104	104	104	**88**
21	505–285	0,171875	6	102	106	108	**110**	108	104	108	108
22	505–301	0,171875	6	**110**	104	98	106	96	104	96	106
23	505–499	0,15625	2	106	108	104	102	106	104	106	**110**

Таблица 4

Композиции с максимальным и минимальным количеством нулевых значений корреляционной матрицы

№ п/п	Композиция	Максимум модуля	Количество нулей	Степень нелинейности							
1	283–445	0,171875	**15**	106	104	98	106	108	104	108	108
2	379–391	0,234375	**15**	98	104	98	102	96	104	96	108
3	487–361	0,203125	**0**	108	102	102	100	104	108	104	102

Таким образом, мы видим, что для обеспечения равномерной минимизации матрицы коэффициентов корреляции (согласно табл. 1) целесообразнее всего использовать полином для обращения элементов с минимальным количеством нулей, например, полином 445. Применение данного полинома позволит затруднить линейную аппроксимацию шифра аффинными булевыми функциями, увеличивая его сопротивляемость атакам дифференциального криптоанализа. Эти полиномы обладают лучшими (минимальными) значениями корреляции векторов выхода и входа *S*-блока подстановки по сравнению с полиномом, применяемым в алгоритме Rijndael, в то же время при использовании композиции полиномов (согласно табл. 4) наиболее подходящей в этом случае окажется композиция полиномов 487–361 либо композиции полиномов 285–471, 299–369, 313–395, 319–379, 351–477, 357–397, 361–313, 361–487, 391–379, 477–463 с количеством нулей корреляционной матрицы, равным одному.

Для обеспечения отсутствия корреляции векторов выхода и входа наиболее предпочтительным будет полином 419 либо композиции 283–445, 379–391 с наибольшим количеством нулей, а также 46 различных композиций, количество нулей корреляционной матрицы которых варьируется от 11 до 14. Они обладают наибольшим количеством нулей в матрицах коэффициентов корреляции входа и выхода, что затруднит корреляционный криптоанализ, однако упростит аппроксимацию шифра аффинными булевыми функциями за счет большего количества единичных значений элементов в полной матрице коэффициентов корреляции со всеми аффинными функциями.

Заключение. Полученные результаты позволяют сделать вывод о том, что большинство композиций неприводимых полиномов над $GF(2^8)$ обладают более интересными криптографическими характеристиками в зависимости от потребностей использующего шифр как в части максимума модуля корреляционной матрицы, так и в количестве нулей корреляционной матрицы, но в то же время расстояние композиций до множества аффинных функций уменьшилось и варьируется от 88 до 110.

Множество композиций неприводимых полиномов может использоваться как более обширный источник *S*-блоков для шифра Rijndael. К примеру, множество композиций неприводимых полиномов, максимум модуля корреляционных матриц которых превышает

0,125 (максимальное значение максимума модуля корреляционной матрицы неприводимого полинома), насчитывает 795 штук из 900 возможных.

Дальнейшее изучение возможных вариантов повышения стойкости алгоритма Rijndael будет основываться на полученных характеристиках блоков замен, а также включать в себя оценку криптостойкости алгоритма в случае применения полученных результатов, а именно, использование различных полиномов или их композиций в различных раундах.

Библиографические ссылки

1. Mister S., Adams C. Practical *S*-box design // Proceedings, Workshop in selected areas of cryptography. SAC'96. 1996. 78–81 с.

2. Бабенко Л. К. Современные алгоритмы блочного шифрования и методы их анализа. М. : Гелиос АРВ, 2006. 376 с.

3. Мазурков М. И. Алгебраические свойства криптографических таблиц замен шифра Rijndael и шифра ГОСТ 28147–89 // Труды СИЭТ. 2012. С. 149–151.

4. Медведева Т. Е. Оценка криптостойкости таблиц замен алгоритма ГОСТ 28147–89 // Решетневские чтения : материалы Междунар. науч.-практ. конф. Красноярск, 2012. С. 666.

5. Мазурков М. И., Соколов А. В. Криптографические свойства нелинейного преобразования шифра Rijndael на базе полных классов неприводимых полиномов // Праці Одеського політехнічного університету. 2012. № 2. 183–189 с.

6. Лидл Р., Нидеррайтер Г. Конечные поля. М. : Мир, 1988. 667 с.

7. Жданов О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования. М. : Инфра-М. 2013. 19–34 с.

8. Nyberg K. Differentially uniform mappings for cryptography. I Advances in cryptology // Proc. of EUROCRYPT'93. 1994. Vol. 765. P. 55–65.

9. Жданов О. Н., Золотарев В. В. Методы и средства криптографической защиты информации / СибГАУ. Красноярск, 2008. 253 с.

10. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. М. : МЦНМО, 2004. 470 с.

11. Вашкевич А. В., Жданов О. Н. Нахождение нелинейности булевой функции с помощью преобразования Уолша // Решетневские чтения : материалы Междунар. науч.-практ. конф. Красноярск, 2012. 655–700 с.

12. Никитин Д. А., Дьяконов К. В. О распределении значений нелинейности булевых функций // Актуальные проблемы безопасности информационных технологий : материалы IV Междунар. науч.-практ. конф. / СибГАУ. Красноярск, 2010. 15–22 с.

13. Жуков А. Е. Нелинейность булевых функций : пособие по курсу «Криптографические методы защиты информации». М. : МГТУ им. Баумана, 2002. 45–112 с.

14. Fuller J., Millan. W. Linear Redundancy in *S*-Boxes // Fast Software Encryption : 10th International Workshop. 2003. Vol. 2887. P. 74–86.

15. Daemen J., Rijmen V. The Design of Rijndael. Springer-Verlag Berlin Heidelberg, 2002. 31–51 с.

References

1. Mister S., Adams C. Practical *S*-box design. *Proceedings, Workshop in selected areas of cryptography*. SAC'96. 1996, P. 78–81.

2. Babenko L. K. *Sovremennye algoritmy blochnogo shifrovaniya i metody ikh analiza* [Current block encryption algorithms and methods of their analysis]. Moscow, Gelios ARV Publ., 2006, 376 p.

3. Mazurkov M. I. [Algebraic properties of cryptographic substitution tables of Rijndael and GOST 28147–89 cipher]. *Trudy SIET*. 2012, P. 149–151 (In Russ.).

4. Medvedeva T. E. [Evaluation of the reliability of GOST 28147–89 algorithm's substitution tables]. *Reshetnevskie chteniya* [Reshetnev readings]. 2012, P. 666 (In Russ.).

5. Mazurkov M. I., Sokolov A. V. [Cryptographic properties of nonlinear transform of Rijndael cipher based on complete classes of irreducible polynomials], *Pratsi Odes'kogo politekhnichnogo universitetu*. 2012, No. 2, P. 183–189 (In Russ.).

6. Lidl R., Niderrayter G. *Konechnye polya* [Finite fields]. Moscow, Mir Publ., 1988, 667 p.

7. Zhdanov O. N. *Metodika vybora klyuchevoy informatsii dlya algoritma blochnogo shifrovaniya* [Key information selection for the block cipher algorithm]. Moscow, INFRA-M Publ., 2013, P. 19–34.

8. Nyberg, K. Differentially uniform mappings for cryptography. *Advances in cryptology. Proc. of EUROCRYPT'93*. *Lecture Notes in Compuer Springer-Verlag*. Berlin, Heidelberg, New York, 1994, Vol. 765, P. 55–65.

9. Zhdanov O. N., Zolotarev V. V. *Metody i sredstva kriptograficheskoy zashchity informatsii* [Methods and means of cryptographic protection of information]. Krasnoyarsk, SibSAU Publ., 2008, 253 p.

10. Logachev O. A., Sal'nikov A. A., Yashchenko V. V. *Bulevy funktsii v teorii kodirovaniya i kriptologii* [Boolean functions in coding theory and cryptology]. Moscow, MTsNMO Publ., 2004, 470 p.

11. Vashkevich A. V., Zhdanov O. N. [Finding nonlinearity of a Boolean function by Walsh converting]. *Reshetnevskie chteniya* [Reshetnev readings]. Krasnoyarsk, 2012, P. 655–700 (In Russ.).

12. Nikitin D. A., D'yakonov K. V. [On the distribution of the values of the nonlinearity of Boolean functions]. *Actual Problems of Information Technology Security: Materials of IV International scientific-practical conference* [Actual problems of information technology security: materials of the IV International Scientific and Practical Conference]. Krasnoyarsk, SibSAU Publ., 2010, P. 15–22 (In Russ.).

13. Zhukov A. E. *Nelineynost' bulevykh funktsiy* [Nonlinearity of Boolean functions]. Moscow, MGTU im. Baumana Publ., 2002, P 45–112.

14. Fuller J. Millan. W. Linear Redundancy in S-Boxes. *Fast Software Encryption, 10th International Workshop*. Sweden, Lund, 2003. Vol. 2887. P. 74–86.

15. Daemen J., Rijmen V. The Design of Rijndael. Springer-Verlag Berlin Heidelberg. Springer. 2002, P. 31–51.