МАТЕМАТИЧНЕ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ

МАТЕМАТИЧЕСКОЕ И КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ

MATHEMATICAL AND COMPUTER MODELLING

УДК 004.056.55

Калинин Д. А.[1], Козина Г. Л.[2]

[1]Студент, Запорожский национальный технический университет, Украина
[2]Канд. физ.-мат. наук, доцент, Запорожский национальный технический университет, Украина, E-mail: ainc@ukrpost.net

БЫСТРОДЕЙСТВИЕ ШИФРОВ «КАЛИНА» И AES

В данной статье приводится сравнение быстродействия симметричных блочных шифров «Калина» и AES. Показано, что «Калина» уступает в скорости AES более чем в 1,7 раз, а также в более чем 2,7 раз при использовании заранее подготовленной таблицы подстановок для алгоритма AES.

Ключевые слова: алгоритм шифрования, быстродействие, стандарт шифрования, симметричный блочный шифр.

ВВЕДЕНИЕ

«Калина» – симметричный блочный шифр, разработанный ЗАО «Институт информационных технологий» г. Харькова [1–2]. Алгоритм имеет размер блока 128, 256 и 512 битов и поддерживает такие же длины ключей. При построении шифра основное внимание разработчиками было уделено обеспечению высокого уровня криптографической стойкости, а также достижению высоких показателей производительности в аппаратной и программной реализациях. Был учтен интеллектуальный вклад в практику проектирования и криптоанализа блочных шифров ведущих криптографов, получивший значительное развитие в ходе проведения международных проектов NESSIE и AES. Широко применялись результаты научных работ по методам криптоанализа и проектированию симметричных шифров последних лет, опубликованных отечественными авторами, а также собственные исследования и разработки ЗАО «ИИТ» в этом направлении.

1. СТРУКТУРА АЛГОРИТМА «КАЛИНА»

Алгоритм шифрования «Калина» является итеративной процедурой, состоящей из предварительной и финальной рандомизации и двух различных итеративных последовательных шифрующих преобразований. Структура алгоритма аналогична структуре AES, обеспечивает хорошее рассеивание и перемешивание. На вход каждого шифрующего преобразования подаётся текущее состояние и необходимое количество ключевых данных (подключ). Открытый текст копируется в текущее состояние перед началом зашифрования, а по его завершению в текущем состоянии находится шифртекст. Количество циклов шифрования зависит от длины ключа (мастер-ключа), при этом длина ключа не может быть меньше размера шифруемого блока.

2. ИСПОЛЬЗУЕМЫЕ ШИФРУЮЩИЕ ПРЕОБРАЗОВАНИЯ

При шифровании, в алгоритмах «Калина» и AES используется ряд процедур, выполняющих преобразование текущего состояния шифра.

В ходе преобразования XORRoundKey производится побитовое сложение по модулю 2 циклового подключа и текущего состояния. Скорость выполнения данного преобразования для «Калина-128» соответствует скорости аналогичного преобразования AddRoundKey для AES-128.

При выполнении преобразования Add32RoundKey производится сложение 32-битных слов циклового подключа и текущего состояния по модулю 2^{32}. Введение данного преобразования увеличивает нелинейность шифра, вводит дополнительные зависимости между ре-

зультирующими значениями, значительно увеличивает стойкость к алгебраическим атакам, дифференциальному, линейному и другим методам криптоанализа. Но, по сравнению с AES, также приводит к дополнительным временным затратам [3].

Преобразование Kalina_S_boxes заключается в том, что для каждого байта текущего состояния выполняется замена в соответствии с заданной таблицей подстановки. В преобразовании используется 8 различных подстановок «байт-в-байт», причем для байтов одной строки текущего состояния шифра используется одна и та же подстановка. Использование 8 подстановок вместо одной улучшает статистические свойства, повышает уровень стойкости к дифференциальному и линейному криптоанализу. Скорость выполнения данного преобразования соответствует скорости аналогичного преобразования SubBytes для AES-128 при использовании заранее сгенерированных таблиц подстановки.

В ходе преобразования ShiftRows производится равномерное распределение байтов каждой 64-битной колонки среди остальных колонок. Это достигается путем циклического сдвига строк состояния вправо на различное количество байтов в зависимости от размера блока. Скорость выполнения данного преобразования соответствует скорости аналогичного преобразования ShiftRows для AES-128.

В ходе преобразования MixColumns выполняется последовательная обработка всех колонок текущего состояния. Каждая 8-байтная колонка рассматривается как полином над полем GF(2^8) с 8 термами, а в ходе преобразования выполняется умножение этого полинома по модулю x^8+1 на фиксированный полином $c(x)$, где

$$c(x)=\{01\}x^7+\{05\}x^6+\{01\}x^5+\{08\}x^4+ \\ +\{06\}x^3+\{07\}x^2+\{04\}x+\{01\}. \quad (1)$$

В алгоритме AES в качестве полинома над полем GF(2^8) рассматривается 4-байтная колонка текущего состояния и выполняется его умножение по модулю x^4+1 на фиксированный полином $a(x)$:

$$a(x)=\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}. \quad (2)$$

Эти операции эквивалентны матричному умножению над GF(2^8) исходного 8-байтного вектора для «Калины» и 4-байтного вектора для AES на фиксированные матрицы. Поскольку используется вдвое большая размерность исходного вектора и фиксированной матрицы, данное преобразование в алгоритме «Калина» выполняется значительно медленнее аналогичного преобразования MixColumns для AES-128.

При расшифровании используются обратные версии перечисленных преобразований, процедура XORRoundKey/AddRoundKey является обратной к самой себе.

Кроме процедур шифрования и расшифрования, в алгоритмах используется схемы разворачивания ключей [4] для получения цикловых подключей из исходного мастер-ключа. В связи с наличием существенных недостатков схемы выработки подключей AES при разработке шифра «Калина» было принято решение использовать принципиально новую схему разворачивания ключей. Время выполнения данного преобразования значительно больше времени выполнения аналогичного преобразования для AES-128, но поскольку выработка подключей происходит единожды, им можно пренебречь.

Для оценки быстродействия авторами статьи были реализованы оба алгоритма в единой идеологии средствами пакета MAPLE 14. Результаты измерения скорости выполнения всех используемых алгоритмами процедур при выполнении 1000 циклов шифрования отображены в табл. 1.

3. СРАВНЕНИЕ БЫСТРОДЕЙСТВИЯ ШИФРОВ «КАЛИНА» И AES

Алгоритмы AES и «Калина» используют алгебраические операции в конечных полях, наиболее трудоемкой из которых является умножение в GF(2^8). Увеличение числа операций умножения в поле в алгоритме «Калина» является основной причиной отставания в скорости по сравнению с алгоритмом AES. Оценка числа элементарных операций была проведена в [5]. Результаты вычислений приведены в табл. 2.

Результаты практических испытаний, проведенные авторами, представлены в табл. 3.

На основании вычислений, представленных в табл. 1–3 можно заключить, что шифр «Калина» уступает в скорости AES более чем в 1,7 раз, а также в более чем 2,7 раз, при использовании заранее подготовленной таблицы подстановок для алгоритма AES. Например, время шифрования файла размером 10000 байт для алгоритма «Калина» составило 106,563 секунды, а для алгоритма AES – 59,594 секунды, при использовании сгенериро-

Таблица 1. Быстродействие используемых алгоритмами преобразований

Преобразования	Калина-128	AES-128
XORRoundKey/AddRound Key	0,047 с	0,047 с
Add32RoundKey	0,125 с	–
Kalina_S_boxes/SubBytes	0,532 с	4,094 с / 0,593 с
ShiftRows/ShiftRows	0,063 с	0,078 с
MixColumns/MixColumns	16,109 с	5,594 с
Kalina_KeyExpansion/Key Expansion	102,688 с	12,265 с

Таблица 2. Вычислительные затраты шифров

Число раундов	1	2	3	4	5	6	7	8	9	10
Калина	125	181	237	293	349	405	461	517	573	629
AES	48	84	120	156	192	228	264	300	336	393

Таблица 3. Показатели быстродействия реализаций, сравниваемых алгоритмов в пакете MAPLE 14, при размере ключа и блока 128 бит

Размер файла	Калина, 10 раундов	AES, 10 раундов	Показатели быстродействия
10 байт	0,297 с	0,093 с / 0,062 с	3,193 раз / 4,790 раз
100 байт	1,266 с	0,640 с / 0,500 с	1,978 раз / 2,532 раз
1000 байт	10,828 с	6,000 с / 3,860 с	1,804 раз / 2,805 раз
10000 байт	106,563 с	59,594 с / 38,484 с	1,788 раз / 2,769 раз
50000 байт	540,546 с	302,000 с / 194,047 с	1,789 раз / 2,786 раз
100000 байт	1099,844 с	612,235 с / 396,343 с	1,796 раз / 2,775 раз

ванной таблицы подстановок – 38,484 секунды. При этом соотношения скоростей обоих шифров составили 1,788 раз и 2,769 раз, соответственно.

ВЫВОДЫ

В данной статье были рассмотрены процедуры, используемые при шифровании алгоритмами AES и «Калина», была произведена оценка их быстродействия. Поскольку в основе алгоритма «Калина» заложены идеи, использованные в шифре AES, то можно произвести сравнение их быстродействия на уровне используемых алгоритмами шифрующих преобразований. При этом можно оценить, оправдана ли модификация структуры шифра AES. Использование различных модулей преобразований для введения ключевой информации, новой схемы выработки подключей позволяет устранить ряд потенциальных слабостей, выявленных в процессе исследований AES. Алгоритм «Калина» может быть использован для обеспечения более высокого уровня стойкости [6–8] относительно увеличения временных затрат на шифрование.

По результатам, полученным в данной статье, можно заключить, что шифр «Калина» существенно уступает шифру AES в быстродействии. Однако, он может быть успешно использован при шифровании информации длительного хранения, а также в ситуациях, когда быстродействие шифра не является критичным.

СПИСОК ЛИТЕРАТУРЫ

1. *Горбенко, І. Д.* Перспективний блоковий симетричний шифр «Калина» : основні положення та специфікації / І. Д. Горбенко, В. І. Долгов, Р. В. Олейніков [та ін.] // Прикладна радіоелектроніка. – 2007. – Т. 6, № 2. – С. 195–208.
2. *Долгов, В. И.* Подстановочные конструкции современных симметричных блочных шифров / В. И. Долгов, Р. В. Олейников, И. В. Лисицкая [та ін.] // Радіоелектронні і комп'ютерні системі. – 2009. – № 6 (40). – С. 89–93.
3. *Кузнецов, О. О.* Захист інформації в інформаційних системах : монографія / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид-во ХНЕУ, 2010. – 511 с.
4. *Казимиров, А. В.* Алгебраические свойства схемы разворачивания ключей блочного симметричного шифра «Калина» / А. В. Казимиров, Р. В. Олейников // Радіоелектронні і комп'ютерні системі. – 2010. – № 5 (46). – С. 61–66.
5. *Сорока, Л. С.* Исследование дифференциальных свойств блочно-симметричных шифров / Л. С. Сорока [и др.] // Системи обробки інформації. – Вип. 6 (87). – 2010. – С. 286–294.
6. *Алексейчук, А. Н.* Верхние оценки несбалансированности билинейных аппроксимаций раундовых функций блочных шифров ГОСТ 28147-89 и «Калина» / А. Н. Алексейчук, А. С. Шевцов // Сучасний захист інформації. – 2010. – № 2. – С. 23–30.
7. *Долгов, В. И.* Дифференциальные свойства блочных симметричных шифров / В. И. Долгов, А. А. Кузнецов, С. А. Исаев // Электронное моделирование. – 2011. – Т. 33, № 6. – С. 81–99.
8. *Лисицкая, И. В.* О новой методике оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / И. В. Лисицкая // Системи обробки інформації. – 2011. – Вип. 4 (94). – С. 167–173.

Стаття надійшла до редакції 16.08.2012.

Калінін Д. О.[1], Козіна Г. Л.[2]

[1]Студент, Запорізький національний технічний університет, Україна

[2]Канд. физ.-мат. наук, доцент, Запорізький національний технічний університет, Україна

ШВИДКОДІЯ ШИФРІВ «КАЛИНА» Й AES

У даній статті наведене порівняння швидкодії симетричних блочних шифрів «Калина» й AES. Показано, що «Калина» поступається у швидкості AES більш ніж в 1,7 разів, а також у більш ніж 2,7 разів при використанні заздалегідь підготовленої таблиці підстановок для алгоритму AES.

Ключові слова: алгоритм шифрування, швидкодія, стандарт шифрування, симетричний блочний шифр.

Kalinin D. A.[1], Kozina G. L.[2]
[1]Student, Zaporizhzhya National Technical University, Ukraine
[2]Candidate of Phys.-Math. sciences, associate professor, Zaporizhzhya National Technical University, Ukraine

SPEED OF CODES «KALINA» AND AES

Speed of symmetric block codes «Kalina» and AES comparison is given in this article. As the basis for the algorithm of «Kalina» laid ideas used in cipher AES, it is possible to compare their performance at the level of encryption transformations of the algorithms. From the structure of AES and of the «Kalina» ciphers one can conclude that most of «Kalina» transformations are less efficient but have more useful properties than similar AES transformations. The comparison of the ciphers encryption transformations has discovered the most time-consuming ones. It is shown that «Kalina» concedes in speed of AES more than in 1,7 times, and also in more than 2,7 times, when using in advance prepared table of substitutions for AES-algorithm.

Keywords: enciphering, speed, enciphering standard, symmetric block code.

REFERENCES

1. Horbenko I. D., Dolhov V. I., Oleinikov R. V., Ruzhentsev V. I., Mykhailenko M. S., Horbenko Yu. I., Totskii O. S., Kazmina S. V. Perspektyvnyi blokovyi symetrychnyi shyfr «Kalyna»: osnovni polozhennia ta spetsyfikatsii. *Prykladna radioelektronika*, 2007, vol.6, No. 2, pp. 195–208.
2. Dolgov V. I., Olejnikov R. V., Lisiczkaya I. V., Sergienko R. V., Drovot'ko E. V., Mel'nichuk E. D. Podstanovochny'e konstrukcii sovremenny'x simmetrichny'x blochny'x shifrov. *Radioelektronni i kompiuterni systemy*, 2009, No. 6 (40), pp. 89–93.
3. Kuznetsov O. O., Yevseiev S. P., Korol O. H. Zakhyst informatsii v informatsiinykh systemakh : monohrafiia, Kharkov, KhNEU, 2010, 511 p.
4. Kazimirov A. V., Olejnikov R. V. Algebraicheskie svojstva cxemy' razvorachivaniya klyuchej blochnogo simmetrichnogo shifra «Kalina», *Radioelektronni i kompiuterni systemiy,* 2010, No. 5 (46), pp. 61–66.
5. *Soroka L. S., Kuznetsov A. A., Moskovchenko I. V., Isaev S. A.* Issledovanie differentsial'ny'x svojstv blochno-simmetrichny'x shifrov, *Systmy obrobky informatsii,* Vyp. 6 (87), 2010, pp. 286–294.
6. Aleksejchuk A. N., Shevczov A. S. Verxnie ocenki nesbalansirovannosti bilinejny'x approksimacij raundovy'x funkcij blochny'x shifrov GOST 28147-89 i «Kalina», *Suchasnyi zakhyst informatsii,* 2010, No. 2, pp. 23–30.
7. Dolgov V. I., Kuzntczov A. A., Isaev S. A. Differencial'ny'e svojstva blochny'x simmetrichny'x, *E'lektronnoe modelirovanie,* 2011, vol. 33, No. 6, pp. 81–99.
8. Lisiczkaya I. V. O novoj metodike ocenki stojkosti blochny'x simmetrichny'x shifrov k atakam differencial'nogo i linejnogo kriptoanaliza, *Systemy obrobky informatsii,* 2011, Vyp. 4 (94), pp. 167–173.