681.3.06:519.248.681

А.В. КАЗИМИРОВ, Р.В. ОЛЕЙНИКОВ

Харьковский национальный университет радиоэлектроники

АЛГЕБРАИЧЕСКИЕ СВОЙСТВА СХЕМЫ РАЗВОРАЧИВАНИЯ КЛЮЧЕЙ БЛОЧНОГО СИММЕТРИЧНОГО ШИФРА «КАЛИНА»

Выполнен анализ показателей криптографической стойкости схемы разворачивания ключей шифра «Калина» к алгебраической атаке, строящейся на основе описания S-блоков с помощью переопределенной системы уравнений. Приведено обоснование стойкости СРК шифра «Калина» с точки зрения алгебраического анализа.

Ключевые слова: *блочный симметричный шифр, алгебраический анализ, схема разворачивания ключей, переопределённая система уравнений, алгоритм шифрования «Калина».*

Введение

В Украине проходит заключительный этап открытого криптографического конкурса, предполагающего выбор алгоритма-прототипа национального стандарта блочного симметричного шифра [1]. Одним из финалистов стал шифр «Калина», разработанный в ЗАО «Институт информационных технологий» [2].

Методы, примененные при разработке этого алгоритма, используют идеи алгоритмов, представленных в конкурсах AES и NESSIE [3]. В то же время в шифре «Калина» реализован ряд новых подходов, в частности, при разработке схемы разворачивания ключей (СРК).

Традиционный подход построения СРК для симметричных блочных алгоритмов предполагает использование биективного отображения из множества ключей шифрования во множество раундовых ключей (подключей). Для получения низкой сложности реализации (при сохранении биективности) в большинстве шифров выбрана сравнительно простая СРК, для которой возможно и обратное преобразование, т.е. нахождение ключа шифрования по одному или нескольким подключам.

Такой подход оптимален с точки зрения обеспечения равенства мощности множества ключей шифрования и множества подключей, минимизации сложности реализации и гарантирует требуемые свойства СРК шифров с точки зрения стойкости к дифференциальному и линейному криптоанализу [4]. Однако использование такого подхода имеет и ряд существенных недостатков. В частности, простая процедура получения ключа шифрования по цикловым ключам значительно упрощает атаки на реализацию [5]. Кроме того, традиционный подход допускает слабые свойства распространения (propagation properties), которые, в свою очередь, обуславливают существование значительной корреляции между цикловыми ключами.

Иллюстрацией недостатков традиционного подхода к построению СРК стала теоретическая атака на связанных ключах для AES-192 и AES-256 [6], сложность которой значительно ниже полного перебора ключей.

Подход, использованный при построении СРК алгоритма «Калина», позволяет избавиться от этих уязвимостей. В работе [7] был выполнен анализ статистических свойств перспективной СРК. В представленной статье приводится обоснование стойкости СРК шифра «Калина» к алгебраическому анализу.

1. Описание функции разворачивания ключа шифра «Калина»

Алгоритм разворачивания ключей включает в себя два этапа:

- выработку ключевого состояния KS_{len}^{j}, где j – порядковый номер ключевого состояния, *len* – длина ключевого состояния в битах;
- на основе KS_{len}^{j} формируется цикловые подключи K_i.

На вход процедуры подаётся мастер-ключ, константа C_{len}^{j}, которая зависит от длины ключа шифрования и размера блока, на выходе формируется ключевое состояние KS_{len}^{j}.

Псевдокод функции вычисления KS_{len}^{j} приведен на рис. 1.

```
void Kalina_KeyExpansionKS( byte key[ 8 * Nk ], const Ci, byte KS[ 8 * Nk ])
{
      byte state[ Nk  ] = Ci

      XORRoundKey(state, key )
      Kalina_S_boxes( state )
      ShiftRows( state )
      MixColumns( state )
      Add32RoundKey(state, ~( key ) )
      Kalina_S_boxes( state )
      ShiftRows( state )
      MixColumns( state )
      XORRoundKey(state, key)

      KS = state
}
```

Рис. 1. Функция вычисления ключевого состояния для шифра «Калина»

На рис. 1 использованы следующие обозначения:

- XORRoundKey – сумма по модулю 2;
- Kalina_S_boxes – нелинейное отображение «байт в байт»;
- ShiftRows – циклический сдвиг строк состояния;
- MixColumns – умножение на фиксированную матрицу над полем $GF(2^8)$;
- Add32RoundKey – сложение по модулю 2^{32};
- Nk – длина ключа в восьмибайтовых словах;
- Ci – константные значения приведённые в спецификации шифра;
- KS – ключевое состояние;
- key – мастер-ключ;
- ~(x) – побитовая инверсия вектора x.

В качестве нелинейного отображения используются восемь фиксированных подстановок (S-блоков) [2].

Линейными частями в СРК являются циклический сдвиг строк и умножение на фиксированную матрицу над полем $GF(2^8)$, причём матрица выбрана таким образом, чтобы обеспечивать максимально возможный индекс ветвления (branch number).

Ключевое состояние KS^j_{len} представляет собой промежуточное значение, вычисленное на основе мастер-ключа и совпадает с ним по размеру. В зависимости от размера блока и длины ключа шифрования, из одного KS^j_{len} вырабатывается от четырёх до шести подключей.

Все подключи с номерами, кратными 4 (K_{4*j}, $j = 0,1,\ldots$), формируются непосредственно на основе KS^j_{len}. Остальные подключи формируются путём циклического сдвига на различное количество байт (табл. 1).

Таблица 1. Порядок формирования подключей

Размер блока, биты	Циклический сдвиг подключа K_{4*j} вправо, байты		
	K_{4*j+1}	K_{4*j+2}	K_{4*j+3}
128	$(K_{4*j})>>>5$	$(K_{4*j})>>>7$	$(K_{4*j})>>>11$
256	$(K_{4*j})>>>11$	$(K_{4*j})>>>17$	$(K_{4*j})>>>29$
512	$(K_{4*j})>>>17$	$(K_{4*j})>>>31$	$(K_{4*j})>>>47$

2. Принципы построения алгебраической атаки

S-блок симметричного шифра может быть представлен как набор булевых функций вида: $y_h = f_h(x_n, x_{n-1}, \ldots, x_0), h = 0,1,\ldots,k$. Разработчики большинства современных шифров, включая алгоритм «Калина», максимизировали степень таких функций. В то же время, если использовать общий вариант описания S-блока системой уравнений, где используются произведения входных и выходных переменных, можно получить более низкую степень термов, чем при функциональной зависимости выхода от входа. В работе [8] показаны принципы построения такой системы для случая, когда степень каждого из термов не превышает вторую. В общем случае для описания S-блока можно использовать степень большую, чем вторую.

Для поиска системы используется алгоритм, основанный на построении матрицы, описывающей все возможные значения термов для всех вариантов входных переменных S-блока.

Пусть X = $\{x_7,x_6,x_5,x_4,x_3,x_2,x_1,x_0\}$ – байт, который подаётся на вход S-блока, а Y = $\{y_7,y_6,y_5,y_4,y_3,y_2,y_1,y_0\}$ – байт на выходе S-блока. Тогда строка матрицы A, необходимой для формирования системы уравнений, будет включать в себя все возможные сочетания битов $\{x_7,x_6,x_5,x_4,x_3,x_2,x_1,x_0, y_7,y_6,y_5,y_4,y_3,y_2,y_1,y_0\}$ до максимальной степени термов системы и 1. Так, для нахождения матрицы, описывающей S-блок, с термами не выше третей степени, строка матрицы будет содержать все возможные сочетания третей степени, второй степени, биты входа и выхода S-блока и константу 1.

Для k битов на входе S-блока размерность матрицы составит:

$$|A| = \left(2^k\right) \times \left(\sum_{i=0}^{p} C_{2k}^i\right),$$

где C_m^n – число сочетаний из m элементов по n;

p – максимальная степень терма матрицы.

Применение к этой матрице преобразования NullSpace [9] позволяет получить новую матрицу – систему уравнений (если такая существует), которой и будет описываться S-блок.

3. Применение алгебраической атаки к функции разворачивания ключа шифра «Калина»

В дальнейшем будет рассмотрена схема разворачивания ключей шифра «Калина» с размером блока и длиной ключа, равной 128 битам. Для 256 и 512 битов могут быть получены аналогичные результаты.

Для S-блоков алгоритма «Калина» не существует детерминированной системы уравнений второй степени, которая описывала бы S-блоки, поэтому степень была увеличена до третьей.

Размерность матрицы описания S-блоков составила при этом $\left(2^8\right)\times\left(C_{16}^3+C_{16}^2+16+1\right)=256\times 697$, из которой после применения преобразования Null-Space были получены переопределённые системы уравнений для всех восьми S-блоков, состоящих из 441 уравнений каждая. Для обратного S-блока, применяемого при расшифровании, можно построить систему, также состоящую из 441 уравнения, причём они будут отличаться от уже сформированных.

Таким образом, каждый из S-блоков шифра «Калина» описывается системой третьей степени над $GF(2)$ из $2\cdot 441=882$ уравнений.

Поскольку операция сложения по модулю 2^{32} является нелинейной в поле $GF(2)$, что приводит к значительному усложнению системы (повышению её степени с 3 до 31), и, соответственно, невозможности даже теоретического решения, для реализации атаки было сделано предположение в пользу криптоаналитика и построена упрощённая схема 128-битной функции разворачивания ключа алгоритма «Калина» (рис. 2). От приведенной в спецификации она отличается тем, что операция сложения по модулю 2^{32} была заменена операцией XOR.

Для нахождения системы уравнений, описывающей СРК, рассмотрим по отдельности её основные компоненты.

Операция XOR представляет собой побитовую сумму по модулю 2. Пусть входное сообщение имеет вид A= (a_{127},a_{126}, … , a_1,a_0), а ключ – K= (k_{127},k_{126}, … , k_1, k_0), тогда сообщение после операции XOR примет вид B = ($a_{127}\oplus k_{127}$,$a_{126}\oplus k_{126}$, … , $a_1\oplus k_1$,$a_0\oplus k_0$).

На вход S-блока подаются 128 битов сообщения B, разбитые на 16 байт, т.е. X_{15} = ($a_{127}\oplus k_{127}$, … , $a_{120}\oplus k_{120}$), X_{14} = ($a_{119}\oplus k_{119}$, … , $a_{112}\oplus k_{112}$), … , X_0 = ($a_7\oplus k_7$, … , $a_0\oplus k_0$) (рис. 3).

Пусть E = (e_{127},e_{126}, … , e_1,e_0) – сообщение на выходе после первого преобразования MixColumns. Применив к E операцию, обратную к MixColumns, получим сообщение D = (d_{127}, d_{126}, … , d_1, d_0), которое является выходом операции ShiftRow.

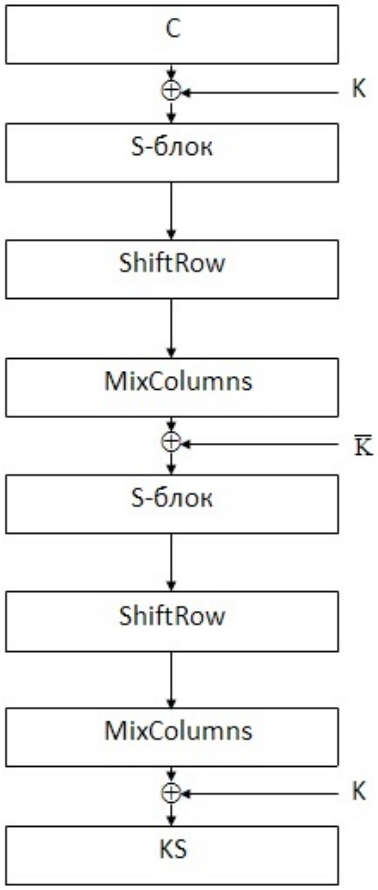

Рис. 2. Упрощённая СРК шифра «Калина»

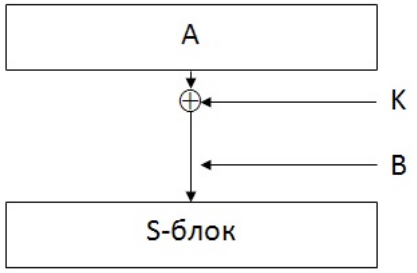

Рис. 3. Представление сообщения на входе S-блока

Значение C = (d_{127}, d_{126}, … ,d_{97}, d_{96}, d_{31}, d_{30}, … , d_1, d_0, d_{63}, d_{62}, … , d_{33}, d_{32}, d_{95}, d_{94}, … ,d_{65}, d_{64}) разбивается на блоки по шестнадцать байт – Y_{15} = (d_{127}, d_{126}, … ,d_{120}); Y_{14} = (d_{119}, d_{118}, … ,d_{112}); … ; Y_0 = (d_{71}, d_{70}, … ,d_{64}) (рис. 4). Полученные значения являются выходом из S-блоков.

Поставив полученные значения в систему уравнений, описывающей S-блок, получим новую систему, которая связывает вход в СРК, промежуточное значение после операции MixColumns, и ключ.

Обозначим промежуточное значение как неизвестные, тогда упрощенную СРК можно описать с

помощью $2 \cdot 16 \cdot 882 = 28224$ уравнений с 256 неизвестными (с учётом того, что значения на входе и выходе известны).

Исходя из вышесказанного, можно сделать следующие выводы: система, построенная для получения 128-битового ключа шифрования и описывающая нелинейную дискретную функцию (оператор) только на основе одной пары 128-битового входа и выхода, содержит 256 неизвестных. Дополнительные неизвестные появились при задании промежуточных значений и являются независимыми переменными для рассматриваемого типа СРК.

Таким образом, однозначное определение ключа шифрования по известному ключевому состоянию с помощью рассмотренного метода невозможно, и система является недоопределенной. Решением системы будет полное множество комбинаций ключа шифрования и промежуточных значений. Конкретное значение ключа можно получить только после задания значения промежуточного состояния.

Сложность поиска ключа шифрования через задание промежуточного состояния (по всему множеству значений) сопоставима со сложностью полного перебора.

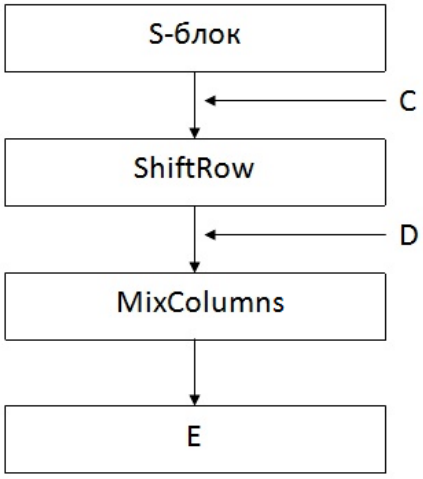

Рис. 4. Представление сообщения на выходе S-блока

Тем не менее, рассмотрим возможные варианты решения построенной системы.

Для линеаризации необходимо, чтобы выполнялось условие:

$$m \le \sum_{i=1}^{3} C_n^i ,$$

где m – количество уравнений;

n – количество неизвестных.

Для нашего случая $28224 \ge 2796416$, что не позволяет выполнить прямую линеаризацию.

В дальнейшем можно воспользоваться XL методом [10,11], позволяющим увеличить количество линейно независимых уравнений в системе. Сложность применения метода определяется через параметр D для максимальной степени терма d, который вычисляется из формулы

$$m \ge \frac{(n-D+d)\cdot(n-D+d-1)\cdots(n-D+1)}{D\cdot(D-1)\cdots(D-d+1)} .$$

В результате может быть получено необходимое количество уравнений, теоретически позволяющих выполнить линеаризацию.

Для нашего случая d=3, D = 10, следовательно, D – 3 = 7. После применения XL метода новая система будет иметь около 2^{59} уравнений с приблизительно 2^{59} неизвестными первой степени, причём $n < m$ (система линейная и теоретически может быть решена).

Отметим, что только для хранения такой системы, описывающей упрощенную СРК, требуется объем памяти, равный $2^{59} \cdot 2^{59} = 2^{118}$ битам или 2^{75} терабайтам, что неосуществимо на практике.

Построение переопределенной системы для СРК, приведенной в спецификации шифра, также возможно после введения в систему дополнительных неизвестных. При рассмотрении входа и выхода A, B модульного сумматора с ключом ($B = A + \overline{K} \left(\mathrm{mod}\, 2^{32} \right)$) можно заметить, что для любой фиксированной пары значений A, B существует эквивалентное сложение по модулю 2 на другом ключе K_2, дающее тот же результат: $B = A \oplus K_2$ (заметим, что в общем случае пара A, B является уникальной для каждого K_2).

Поскольку переопределенная система строится для уникальной пары входов и выходов СРК, этот описанный подход применим и здесь, т.е. вместо модульного сложения с инверсией ключа вводится сложение по модулю 2 с дополнительным неизвестным ключом K_2. Т.е., предполагаем (рис. 5) что:

$$F = E \oplus K_2;$$

$$F = E + \overline{K} \left(\mathrm{mod}\, 2^{32} \right);$$

$$K_2 = \left(E + \overline{K} \left(\mathrm{mod}\, 2^{32} \right) \right) \oplus E;$$

Исходя из этого, полный вариант СРК шифра «Калина» удается описать при помощи 28224 уравнений с 384 неизвестными. Применение XL метода, для решения данной системы позволит получить систему уравнений с приблизительно 2^{84} уравнениями с 2^{84} переменными первой степени (хранение которой требует 2^{125} ТБ).

Опять же отметим, что как и для случая с упрощенной СРК, система является недоопределенной для однозначного получения ключа шифрования по подключам.

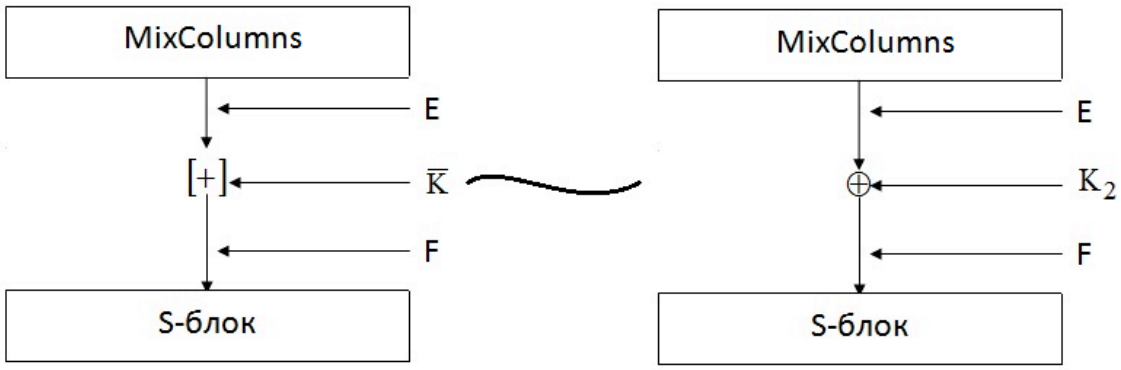

Рис. 5. Эквивалентная замена ключей

ВЫВОДЫ

Применение алгебраического анализа позволяет описать схему разворачивания ключей алгоритма «Калина» (128/128) системой уравнений 3-й степени, содержащей 28224 уравнения с 384 неизвестными (или 256 неизвестными для упрощенного варианта, отличающегося от приведенного в спецификации).

Решениями такой системы являются все возможные комбинации промежуточных состояний и ключей шифрования, а однозначное определение ключа шифрования по известному ключевому состоянию с помощью рассмотренного метода невозможно. Сложность доопределения промежуточных состояний (по всему множеству значений) для вычисления ключа шифрования является не меньшей, чем поиск с полным перебором.

Таким образом, подход, использованный при разработке схемы разворачивания ключей алгоритма «Калина» обеспечивает стойкость к алгебраическим методам криптоанализа при попытке восстановить значение ключа шифрования по известным ключам, что, в свою очередь, обеспечивает дополнительный уровень защиты от атак на реализацию.

Литература

1. Положення про проведення відкритого конкурсу криптографічних алгоритмів [Електронний ресурс] / ДССЗІУ. – Режим доступу : WWW/URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=48383&cat_id=38710 - 05.06.2009 г. – Загл. с экрана.

2. Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікація [Текст]/ І.Д. Горбенко, В.І. Долгов, Р.В. Олійников [та ін.]. Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. Харьков. Том 6, №2, 2007 г.

3. Daemen J. AES Proposal: Rijndael, AES algorithm submission [Electronic resource] / J. Daemen, V. Rijmen - AES home page: http://www. nist. gov/aes, 1998 – Last access: 2009. – Title from the screen.

4. Daemen J. The Design of Rijndael [Text] / J. Daemen, V. Rijmen. Springer-Verlag, 2002.

5. Biham E. Differential Fault Analysis of Secret key Cryptosystems [Text] / E. Biham, A. Shamir. Proc. of the 17th Annual International Cryptology Conf. on Advances in Cryptology. Springer-Verlag, 1997.

6. Biryukov A. Related-key cryptoanalysis of the full AES-192 and AES-256 [Electronic resource] / A. Biryukov, D. Khovratovich. Mode of access : WWW.URL: https://cryptolux.org/mediawiki/uploads/1/1a/Aes-192-256.pdf – Last access: 2009. – Title from the screen.

7. Олейников Р.В. Анализ свойств схемы разворачивания ключей алгоритма шифрования «Калина» [Текст] / Р.В. Олейников, В.И. Руженцев. 12-ая Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах», тезисы докладов. – К.: ЧП «ЕКМО» НИЦ «ТЕЗИС» НТУУ «КПИ», 2009.

8. Олейников Р.В. Построение переопределенной системы уравнений для описания алгоритма шифрования „Лабиринт" [Текст] / Р.В. Олейников, А.В. Казимиров. Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. Харьков. Том 8, №3, 2009 г.

9. Trefethen L. N. Numerical Linear Algebra [Text] / L. N. Trefethen, D. Bau. SIAM, 1997. – 361 pages. – ISBN 978-089-871-361-9.

10. Courtis N. T. Cryptanalysis of Block Cipher with Overdefined System of Equations [Electronic resource] / N. T. Courtois, J. Pieprzyk. // Asiacrypt 2002: Mode of access : WWW.URL: http://eprint.iacr.org/2002/044.pdf – Last access: 2009. – Title from the screen.

11. Courtis N. T. Higher Order Correlation Attacks, XL Algorithm and Cryptanalysis of Toyocrypt [Electronic resource] / N. T. Courtois Mode of access : WWW.URL: http://eprint.iacr.org/2002/087.pdf – Last access: 2009. – Title from the screen.

Поступила в редакцию 04.01.2010

Рецензент: д-р техн. наук, проф., зав. каф. безопасности информационных технологий И.Д. Горбенко, Харьковский национальный университет радиоэлектроники, Харьков.

АЛГЕБРАЇЧНІ ВЛАСТИВОСТІ СХЕМИ РОЗГОРТАННЯ КЛЮЧІВ БЛОКОВОГО СИМЕТРИЧНОГО ШИФРУ «КАЛИНА»

О.В. КАЗИМИРОВ, Р.В. ОЛІЙНИКОВ

Виконано аналіз показників криптографічного стійкості схеми розгортання ключів шифру «Калина» до алгебраїчної атаки, що будується на основі опису S-блоків за допомогою перевизначеної системи рівнянь. Наведено обґрунтування стійкості СРК шифру «Калина» з точки зору алгебраїчного аналізу.

Ключові слова: *блоковий симетричний шифр, алгебраїчній аналіз, схема розгортання ключів, перевизначена система рівнянь, алгоритм шифрування «Калина».*

ALGEBRAIC PROPERTIES OF SYMMETRIC BLOCK CIPHER “KALYNA” KEY SCHEDULE

O.V. Kazymyrov, R.V. Oliynykov

It is performed an analysis of strengths factors of symmetric block cipher “Kalyna” key schedule to algebraic attack based on S-boxes description with overdefined system of equations. Proof of cipher “Kalyna” key schedule strength to algebraic analysis is given.

Key words: symmetric block cipher, XL attack, key schedule, overdefined systems of equation, cipher «Kalyna».