УДК 004.056

И.В. Лысенко

Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ», Харьков

СИММЕТРИЧНАЯ СИСТЕМА ШИФРОВАНИЯ А.П. СТАХОВА И ПРИНЦИП ДИВЕРСНОСТИ

Рассматривается подход, реализующий симметричное шифрование данных на основе матриц Фибоначчи, а также его модификация на основе принципа диверсности. Предлагается классификация моделей системы шифрования на основе принципа диверсности.

Ключевые слова: *симметричное шифрование, матрицы Фибоначчи, принцип диверсности.*

Введение

Один из способов реализации симметричного шифрования основан на матричных криптопреобразованиях вида $Y = AX$, $X = A^{-1}Y$, где X – исходный текст, Y – шифртекст, A – невырожденная квадратная матрица, выступающая в качестве ключа, A^{-1} – матрица, обратная к A.

Как замечается в [1], реализация данного подхода не обеспечивает требуемой криптостойкости. Так, в [2] показано, что при криптоанализе на основе шифртекстов и известных открытых текстов для матрицы размерности 100×100, элементами которой являются 0 и 1 (матрица над конечным полем GF_2), раскрытие ключа (формирование шифрующей матрицы) осуществляется со сложностью порядка 10^6 операций.

В то же время, в рамках данного подхода А.П. Стаховым была предложена криптосистема [3, 4], основанная на использовании симметрических гиперболических функций Фибоначчи, обладающая, как представляется, криптостойкостью, удовлетворяющей современным требованиям.

Целью статьи является рассмотрение подхода, предложенного А.П. Стаховым, а также его модификация на основе принципа диверсности.

Система шифрования А.П. Стахова

Суть предложенного А.П. Стаховым подхода состоит в следующем [3, 4].

Для шифрования исходных данных используется матрица Фибоначчи

$$Q(2x) = \begin{pmatrix} cFs(2x+1) & sFs(2x) \\ sFs(2x) & cFs(2x-1) \end{pmatrix}, \qquad (1)$$

где cFs(x), sFs(x) – соответственно симметричные косинус и синус Фибоначчи действительного аргумента x, определяемые по формулам

$$cFs(x) = \frac{\tau^x + \bar{\tau}^x}{\sqrt{5}}, \quad sFs(x) = \frac{\tau^x - \bar{\tau}^x}{\sqrt{5}}, \qquad (2)$$

где $\tau = \left(1+\sqrt{5}\right)/2$ – константа «золотого» сечения.

Шифруемый текст разбивается на блоки таким образом, чтобы в каждом из них было 4 одинаковых по величине фрагмента, и формируются матрицы M_j (j = 1,…N) размерности 2×2, каждый элемент m_{jl} (l =1,…,4) которых – это один из фрагментов соответствующего блока исходных данных. Очевидно, что существует 4! = 24 способа размещения элементов m_{jl} в матрице M_j, что соответствует числу перестановок P_j из четырёх элементов.

Шифрование данных производится путём умножения матриц M_j на матрицу (1), в результате чего получается матрица шифртекста C_j:

$$M_j \times Q(2x) = C_j \ . \qquad (3)$$

Матрица Q(-2x) , инверсная к (1), используется для расшифрования шифртекста. Данная матрица получается путём деления преобразованной матрицы (1) на её определитель. Само же это преобразование, как известно из теории матриц, состоит в том, что для матрицы размерности 2×2 элементы главной диагонали матрицы меняются местами, а остальные элементы меняют свой знак на противоположный. Т.е., матрица A^{-1}, инверсная по отношению к квадратной матрице $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, равна

$$A^{-1} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}^{-1} = \frac{1}{\det A}\begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}.$$

Поскольку, как показано в [3], определитель матрицы (1) равен 1, следовательно

$$Q(-2x) = \begin{pmatrix} cFs(2x-1) & -sFs(2x) \\ -sFs(2x) & cFs(2x+1) \end{pmatrix}. \qquad (4)$$

Расшифрование зашифрованных данных осуществляется посредством умножения матрицы шифртекста C_j (3) на матрицу (4).

Автор описанного подхода упоминает о том, что увеличения криптостойкости можно добиться варьированием значениями параметров P_j и x для каждого блока данных. При этом, очевидно, использование разных значений параметров P_j и x для каждого блока данных, представленного значениями m_1, m_2, m_3, m_4, ведёт к увеличению размерности ключа и тем больше, чем больше размерность шифруемых данных.

В работе [5] данный подход был модифицирован посредством использования в качестве матриц шифрования и дешифрования так называемых G_r-матриц, элементами которых являются гиперболические функции Фибоначчи порядка r.

Эти функции имеют вид

$$sF_r(x) = \frac{1}{\sqrt{4+r^2}}\left[\left(\frac{r+\sqrt{4+r^2}}{2}\right)^x - \left(\frac{r+\sqrt{4+r^2}}{2}\right)^{-x}\right];$$

$$cF_r(x) = \frac{1}{\sqrt{4+r^2}}\left[\left(\frac{r+\sqrt{4+r^2}}{2}\right)^x + \left(\frac{r+\sqrt{4+r^2}}{2}\right)^{-x}\right].$$

Использование этих функций позволяет помимо перестановки P_j и значения x также использовать в качестве ключевого параметра величину r, на что указывает А.П. Стахов.

Модификация системы шифрования А.П. Стахова на основе принципа диверсности

В упомянутой работе [5] автором предлагается использовать так называемое множественное шифрование, суть которого состоит в том, чтобы набор ключевых параметров P_j , x, r для шифрования каждого очередного блока данных формировать в зависимости от наборов параметров, использованных для шифрования предыдущих блоков данных. При этом в работе нет указаний на то, каким образом может быть реализована эта идея.

Кроме того, следует обратить внимание на следующее обстоятельство. При использовании значений $r > 1$ для корректного расшифрования необходимо использовать алгебраические выражения для компонент матрицы C_j, что крайне проблематично. В противном случае вычисление инверсной матрицы из исходной матрицы M_j приводит к тому, что матрица C_j становится близкой к сингулярной, в результате чего дешифрование выполняется некорректно. Таким образом, возможность использования гиперболических функций Фибоначчи r-го порядка для криптопреобразований является только теоретической, и набор ключевых параметров задаётся двойкой $K = \{P_j, x_s\}$.

По нашему мнению, подход, предложенный в работах А.П. Стахова [3 – 5], можно реализовать, используя принцип диверсности. Общая идея в этом случае состоит в том, чтобы задаться множествами несекретных значений каждого из ключевых параметров, а затем, используя некоторый начальный секретный ключ, по некоторому несекретному правилу выбирать значения этих параметров для каждого блока данных неочевидным для злоумышленника образом.

В связи с отмеченным выше возникают вопросы:

1. Можно ли, не используя гиперболических функций Фибоначчи r-го порядка, остаться в рамках *трёх* ключевых параметров, задающих так называемое поле диверсности (число параметров, допускающих варьирование)?

2. В чём может состоять способ (правило) формирования ключевых параметров для шифрования?

Что касается первого вопроса, то реализовать диверсный подход, оставаясь в рамках трёх ключевых параметров, можно и не прибегая к использованию G_r-матриц, а основываясь на обычных матрицах Фибоначчи (1) и (4). Так, если в выражениях (2) в знаменателе под корнем использовать любое натуральное число g, то все вышеприведенные рассуждения окажутся справедливыми.

Покажем это, назвав величины

$$cF^g s(x) = \frac{\tau^x + \bar{\tau}^x}{\sqrt{g}} \quad \text{и} \quad sF^g s(x) = \frac{\tau^x - \bar{\tau}^x}{\sqrt{g}}$$

g-косинусами и g-синусами Фибоначчи соответственно. Очевидно, что формулы (2) – это частный случай данных соотношений при g=5.

Так, очевидно, что эти величины связаны с формулами (2) соотношениями

$$cF^g s(x) = \frac{\sqrt{5}}{\sqrt{g}} cFs(x); \quad sF^g s(x) = \frac{\sqrt{5}}{\sqrt{g}} sFs(x).$$

В таком случае матрица шифрования вида (1) может быть представлена в виде

$$Q^{2x} = \begin{pmatrix} \frac{\sqrt{5}}{\sqrt{g}} cFs(2x+1) & \frac{\sqrt{5}}{\sqrt{g}} sFs(2x) \\ \frac{\sqrt{5}}{\sqrt{g}} sFs(2x) & \frac{\sqrt{5}}{\sqrt{g}} cFs(2x-1) \end{pmatrix}.$$

Учитывая основное тождество для фибоначчиевых функций [5]:

$$cFs(2x+1)cFs(2x-1) - [cFs(2x)]^2 = 1,$$

определитель данной матрицы будет равен $5 / g$.

Тогда матрица расшифрования будет

$$Q^{-2x} = \frac{g}{5}\begin{pmatrix} cFs(2x-1) & -sFs(2x) \\ -sFs(2x) & cFs(2x+1) \end{pmatrix}.$$

Таким образом, имеем *тройку* ключевых параметров $K = \{P_{ij}, x_s, g_v\}$, $i=1,\ldots,24$; $s=1,\ldots,N_x$; $v=1,\ldots,N_g$, где N_x, N_g – число значений параметров x и g соответственно.

Таким образом, в зависимости от количества используемых значений ключевых параметров можно составить классификацию моделей криптопреобразования (вариантов диверсной модели) (табл. 1).

Произведём оценку размерности ключа для предложенного множества моделей. Для этого введём обозначения: N_p , N_x, N_g – число используемых параметров P_i, x, g соответственно; n_p , n_x, n_g – число битов, необходимое для представления этих параметров в двоичном виде. Очевидно, что в этом случае длина ключа $L_k = N_x n_x + N_p n_p + N_g n_g$.

Для формирования перестановки P_i достаточно 8 битов, если, во-первых, первыми четырьмя числами считать 0,1,2,3, и, во-вторых, – закодировать каждый

Таблица 1

Классификация моделей криптопреобразования

№ п/п	Варианты диверсной модели	Тип диверсности
1	С постоянными параметрами P_i, x, g **$K = \{P_i, x, g\}$, $P_i = P_{ij}$ & $x_j = x \; \forall \; j = =1,\ldots, N$; $N_g = 1$.**	тривиальная
2	С постоянными параметрами x и e **$K = \{P_{ij}, x, g\}$, $x_j = x \; \forall \; j = 1,\ldots, N$; $N_g = 1$.**	частичная
3	С постоянными параметрами x и P_i **$K = \{P_{ij}, x, g_v\}$, $P_{ij} = P_i \; \forall \; i = 1,\ldots,24$; $x_j = x \; \forall \; j = 1,\ldots, N$; $N_g > 1$.**	
4	С постоянными параметрами P_i и g **$K = \{P_{ij}, x_s, g\}$, $P_{ij} = P_i \; \forall \; i = 1,\ldots, 24$; $N_g = 1$.**	
5	С постоянным параметром x **$K = \{P_{ij}, x, g_v\}$, $x_j = x \; \forall \; j = 1,\ldots, N$; $N_g > 1$.**	
6	С постоянным параметром g **$K = \{P_{ij}, x_s, g\}$, $N_g = 1$.**	
7	С постоянным параметром P_i **$K = \{P_i, x_s, g_v\}$, $P_{ij} = P_i \; \forall \; i = 1,\ldots, 24$; $N_g > 1$.**	
8	С переменными параметрами P_i, x, g **$K = \{P_i, x_s, g_v\}$.**	полная

элемент матрицы M_j двумя битами, например, элементу m_{11} поставить в соответствие 0, m_{12} – число 1, m_{21} – число 2 и m_{22} – число 3. Поэтому $n_p = 8$.

Если V_x, V_g – число десятичных разрядов параметров x и g, то для их двоичного представления требуется максимум $3V_x + 1$ и $3V_g + 1$ битов соответственно, т.е. $n_x = 3V_x + 1$ и $n_g = 3V_g + 1$.

В таком случае, например, для модели №5 (табл. 1) длина ключа $L_k = (3v_x + 1) + N_g(3v_g + 1) + 8N_p$, а для модели №2 – $L_k = 3(v_x + v_g) + 2 + 8N_p$.

Что касается второго вопроса, то правило формирования последовательности номеров ключевых параметров P_{ij}, x, g для шифрования блоков данных M_j может быть представлено следующим алгоритмом:

0. $K_{(2)} \rightarrow K_{(10)}$.

1. $K_{(10)} (\text{mod } H) = t_{1(10)}$.

2. $t_{1(10)} \rightarrow t_{1(2)}$; $K_{(2)} \oplus t_{1(2)} = S_{1(2)}$; $S_{1(2)} \rightarrow S_{1(10)}$; $S_{1(10)} (\text{mod } H) = t_{2(10)}$.

for j = 3 … N do

$t_{j-1(10)} \rightarrow t_{j-1(2)}$; $S_{j-2(2)} \oplus t_{j-1(2)} = S_{j-1(2)}$; $S_{j-1(2)} \rightarrow S_{j-1(10)}$; $S_{j-1(10)} (\text{mod } H) = t_{j(10)}$.

В алгоритме приняты следующие обозначения:

– $H = \{N_p, N_x, N_g\}$;

– K – секретный ключ длиной l_k битов;

– $t_{j(10)}$, $t_{j(2)}$ – соответственно десятичный и двоичный порядковые номера использования переменного параметра для преобразования блока данных M_j.

Заключение

Использование рассмотренного подхода, как предполагается, должно усилить криптостойкость предложенной А.П. Стаховым системы шифрования за счёт увеличения поля диверсности (числа варьируемых ключевых параметров).

Целью дальнейших исследований является программная реализация предложенного подхода, а также проверка его быстродействия в сравнении с существующими симметричными блочными криптоалгоритмами.

Список литературы

1. Konheim A. Cryptography. A Primer / A. Konheim. – New York, J. Wiley & Sons, 1981.

2. Ростовцев А.Г. О матричном шифровании (критика криптосистемы Ероша и Скуратова) / А.Г. Ростовцев [Электронный ресурс]. – Режим доступа к ресурсу: http://www.ssl.stu.neva.ru/psw/crypto/rostovtsev/Erosh_Skuratov.pdf.

3. Стахов А.П. «Золотая» криптография / А.П. Стахов // Перспективные информационные технологии и интеллектуальные системы. 2006. – №4. – С. 48-55. [Электронный ресурс]. – Режим доступа к ресурсу: http://elibrary.ru/contents.asp?issueid=434418.

4. Stakhov A.P. The «golden» cryptography. [Электронный ресурс] / A.P. Stakhov. – Режим доступа к ресурсу: http://www.trinitas.ru/rus/doc/0232/004a/02321058.htm.

5. Stakhov A.P. Gazale formulas, a new class of the hyperbolic Fibonacci and Lucas functions, and the improved method of the "golden" cryptography. [Электронный ресурс] / A.P. Stakhov. – Режим доступа к ресурсу: http://www.trinitas.ru/rus/doc/0232/004a/02321063.htm.

Поступила в редколлегию 20.03.2014

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

СИМЕТРИЧНА СИСТЕМА ШИФРУВАННЯ О.П. СТАХОВА І ПРИНЦИП ДІВЕРСНОСТІ

І.В. Лисенко

Розглядається підхід, що реалізує симетричне шифрування даних на основі матриць Фібоначчі, а також його модифікація на основі принципу діверсності. Пропонується класифікація моделей системи шифрування на основі принципу діверсності.

Ключові слова: *симетричне шифрування, матриці Фібоначчі, принцип діверсності.*

THE SYMMETRIC SYSTEM OF CIPHERING OF A.P. STAKHOV AND DIVERSITY PRINCIPLE

I.V. Lysenko

An approach that realizes symmetric ciphering of data on the basis of Fibonacci matrixes is considered. The modification of this approach on the basis of diversity principle is considered. The classification of the models of ciphering system on the basis of diversity principle is proposed.

Keywords: *symmetric ciphering, Fibonacci matrixes, diversity principle.*