XXIX Неделя науки СПбГТУ. Материалы межвузовской научной конференции. Ч.V: С.90-91, 2001.

УДК 681.3.053

П.В. Трифонов (4 курс, каф. РВКС), Е.А.Крук, д.т.н., проф.

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ШИФРА SNAKE

В настоящее время остро стоит проблема защиты информации от несанкционированного доступа. Одним из путей достижения этого является использование шифрования. Целью доклада является описание модификации симметричного блочного шифра SNAKE, позволяющей повысить его безопасность.

Конструкция шифра была предложена в работе [1]. Шифр принадлежит семейству шифров Фейстеля и имеет круговую функцию, алгоритм работы которой может быть описан в виде следующих функций:

$$Y_2 = \frac{1}{X_1 + K_1},\ Y_3 = \frac{1}{X_2 + K_2 + Y_2},\ Y_4 = \frac{1}{X_3 + K_3 + Y_3},\ Y_1 = \frac{1}{X_4 + K_4 + Y_4},$$

где X_i – подблоки входных данных, K_i – подблоки кругового ключа, Y_i – подблоки выходных данных. Все операции выполняются над конечным полем (в исходном варианте –над полем $GF(2^8)$). Отличительной особенностью данного шифра является его доказанная устойчивость к дифференциальному и линейному криптоанализу. В ходе работы был произведен анализ имеющейся литературы, посвященной его криптоанализу. Согласно [2], существует возможность восстановления ключей шифра путем интерполирования его выхода с помощью рациональных функций. Возможно, что путем выбора другого семейства функций можно построить еще более эффективную атаку на шифр.

Таким образом, наиболее очевидным способом вскрытия шифра является использование его сравнительно простой алгебраической структуры.

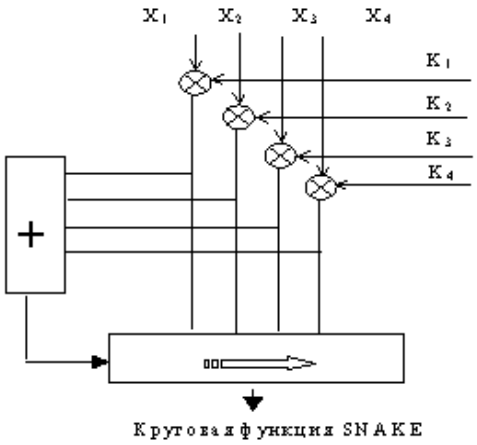

Рис. 1. Модифицированная круговая функция

Наиболее очевидным способом предотвращения таких атак является введение в круговую функцию шифра неаналитических элементов. Одним из таких элементов, предложенных в [3], является циклический сдвиг на вычисляемое число позиций.

В ходе проведенной работы была предложена модификация круговой функции, представленная на рис. 1. В данном случае байты данных после суммирования по модулю 2 с ключом суммируются между собой по модулю 256, после чего для обеспечения зависимости величины сдвига от всех битов данных результат суммирования суммируется по модулю 2 со своим сдвигом вправо на 3. После этого сумма сообщения и ключа циклически сдвигается вправо на вычисленное значение. Результат сдвига передается в обычную круговую функцию SNAKE (без суммирования с ключом). Данная конструкция позволяет устранить явную аналитическую зависимость выхода шифратора от входа.

Для анализа модифицированной функции были проведены эксперименты с шифром, состоящие в проверке сохранения им свойств исходного шифра. Их результаты показывают, что сохраняются основные свойства исходного шифра: высокое быстродействие, сложность применимости линейного и дифференциального криптоанализа. Также сохранена простота реализации.

Таким образом, в результате проведенной работы предложена простая модификация блочного симметричного шифра, позволяющая предотвратить некоторые атаки на него. Установлено, что она сохраняет основные его характеристики. Однако шифр нуждается в дальнейшем криптоанализе на предмет поиска новых атак.

ЛИТЕРАТУРА:

1. C. Lee and Y. Cha, The block cipher: SNAKE with provable resistance against DC and LC attacks, Proc. 1997 Korea-Japan Joint Workshop on Information Security and Cryptology (JW-ISC’97), pp.3-17, 1997

2. S. Moriai, T. Shimoyama, T. Kaneko, “An efficient interpolation attack”, IEICE Trans. Fundamentals, vol. E83-A, NO.1, pp. 39-47, 2000

3. R.L. Rivest, “The RC5 Encryption Algorithm”, Fast Software Encryption, LNCS 1008, Springer-Verlag, 1995, pp. 86-96