М.А. Пудовкина

Московский государственный инженерно-физический институт (технический университет)

Методы криптоанализа семейства алгоритмов поточного шифрования CRAM.

В настоящей работе предложены методы, определения начального заполнения (ключа) по выходной последовательности $\{\gamma\}_i$ для трех вариантов криптосхемы CRAM. Решение поставленной задачи основано на анализе алгебраических связей криптоалгоритма.

В предлагаемой работе начато исследование семейства алгоритмов поточного шифрования CRAM предложенных фирмой «Лан-Крипто» в 1995 в [1]. С криптографической точки зрения алгоритм представляет собой синхронный поточный шифр в режиме обратной связи по выходу (Output Feedback –OFB). Сердцем криптосхем CRAM являются: L битные регистры R_A, R_B, R_C , регистры R_0, R_1 размера $K<L/2$ и массив памяти, состоящий из $N=2^K$ L-битных слов: M(0),…,M(N-1).

Для первого и второго варианта криптосхемы CRAM ключевая последовательность на i такте равна содержимому регистров R_A, R_B: $к_{2i}= R_A$ и $к_{2i+1}= R_B$. Для третьего варианта криптосхемы ключевая последовательность на i такте равна содержимому регистра R_B: $к_i= R_B$.

Варианты криптосхемы CRAM за один такт своей работы выполняют покоординатное булево сложение ключевой последовательности с одним или двумя L битными словами открытого текста.

Ключом для i-го такта работы алгоритма является заполнение массива памяти ***M*** и регистров R_A, R_B, R_C, R_0, R_1 после выполнения (i-1)-го такта. Для первого такта это заполнение (начальное заполнение) можно произвести, например, при помощи любого другого криптоалгоритма.

В настоящей работе решается задача определения начального заполнения памяти ***M*** и регистров R_A, R_B, R_C, R_0, R_1 по выходной последовательности $\{\gamma\}_i$ для трех вариантов криптосхемы CRAM. Решение поставленной задачи основано на анализе алгебраических связей в криптоалгоритме.

Методы для определения начальных заполнений вариантов 1 и 2 криптосхемы являются сходными. Они основаны на опробование значений величины $\{R_C\}_1^{m-1}$, после чего величины $\{ R_A \}_1^{m-1}$, $\{ R_B \}_1^{m-1}$ определяются из анализа алгебраических соотношений. Знание величин $\{ R_A \}_1^{m-1}$,$\{ R_B \}_1^{m-1}$ и $\{R_C\}_1^{m-1}$ позволяет в среднем за $m=\lceil 2^к/3 \rceil$ тактов работы криптосхемы восстановить заполнение массива памяти ***M***.

Исходя из этого получено, что определение начального заполнения в обоих случаях по трудоемкости эквивалентно перебору 1/3 ключевого множества.

Способ решение поставленной задачи для 3 варианта криптосхемы CRAM основан на опробовании значений величины $\{ R_A \}_1^{m-1}$, после чего значения величин $\{ R_B \}_1^{m-1}$ определяются из анализа алгебраических соотношений. Знание величин $\{ R_A \}_1^{m-1}$и $\{ R_B \}_1^{m-1}$ позволяет в среднем за m= $m=2^{к-1}$ тактов работы криптосхемы восстановить заполнение массива памяти ***M***.

Благодаря этому получено, что определение начального заполнения в этом случае по трудоемкости эквивалентно перебору 1/2 ключевого множества.

В настоящее время ведутся исследования, задача которых определить слабые места данной криптосхемы и предложить способы ее улучшения. Они заключает в себя исследование цикловой структуры криптосхемы, выяснение является ли функция переходов состояний криптосхемы регулярной.

Список литературы.

1. http:\\www.lancrypto.com\main.html
2. Schneier B., “ Applied Cryptography ”, Second edition,1996.
3. Konheim A. G. “ Cryptography, a Premiere ”, J Wiley & Sons N.Y,1981
4. Кнут Д. “Искусство программирования для ЭВМ”, т.2, М. : Мир, 1977.
5. Rueppel R.A. “Analysis and Design of Stream Ciphers”