ОБ ОДНОМ ПОДХОДЕ К КРИПТОАНАЛИЗУ ГЕНЕРАТОРОВ КЛЮЧЕВОГО ПОТОКА

Фисенко Д. Л., студент 5 курса ИМЭИ ИГУ

Аннотация: Работа посвящена разработке и проверке метода криптоанализа генератора ключевого потока, основанного на РСЛОС. В данной работе в качестве примеров таких генераторов рассматриваются пороговый и суммирующий генераторы.

Ключевые слова: криптоанализ, генераторы ключевого потока, РСЛОС

Исследования в области криптоанализа систем шифрования позволяют оценить криптостойкость этих систем. Учет результатов таких исследования также полезен при создании новых шифров.

В данной работе рассматриваются симметричные поточные двоично-аддитивные шифры [1]. В таких шифрах на основе секретного ключа с помощью генератора ключевого потока порождается двоичная последовательность, которая в дальнейшем используется для шифрования данных. Генератором ключевого потока будем называть детерминированный алгоритм, который, получая на вход случайную последовательность длины n, выдаёт на выходе последовательность длины $m >> n$.

Многие генераторы ключевого потока в своей работе используют регистры сдвига с линейной обратной связью (РСЛОС). РСЛОС – одномерный массив бит, каждый такт сдвигающихся сонаправленно, на одну позицию, при этом последний бит подаётся на выход. В освободившуюся ячейку записывается бит – выход функции обратной связи, которая в качестве входных данных использует значения некоторых из заполненных ячеек РСЛОС. Каждый такт работы генератора выходные биты нескольких РСЛОС смешиваются с помощью некоторой нелинейной функции. Криптоанализом генераторов ключевого потока, основанных на РСЛОС, будем называть нахождение неизвестного начального заполнения всех РСЛОС генератора (секретный ключ) по известному фрагменту ключевого потока.

Криптоанализ генераторов ключевого потока можно свести к решению систем булевых уравнений (т.н. «логический криптоанализ», см. [2]). Предложенный в [3] подход к криптоанализу основывается на «угадывании» заполнения нескольких РСЛОС генератора. Отталкиваясь от этого «знания», проводится анализ возможных заполнений остальных ячеек РСЛОС генератора. Подобный подход не позволяет уменьшить количество перебираемых вариантов заполнения РСЛОС до начала непосредственного процесса криптоанализа. По данной схеме, в худшем случае, нам придётся проводить процесс криптоанализа 2^k раз, где k – суммарное количество ячеек «известных» РСЛОС (т.е. нам придётся провести криптоанализ для каждого возможного заполнения «угадываемых» РСЛОС).

Подход к криптоанализу, реализованный в данной работе, состоит в «угадывании» значений p последних ячеек каждого из РСЛОС. Т.к. фрагмент ключевого потока известен, то, основываясь на знании его первых p бит, можно исключить из рассмотрения невозможные заполнения p последних бит всех РСЛОС генератора. Данный подход позволяет сократить количество перебираемых вариантов в 2^p раз, т.к. знание p последних ячеек каждого из РСЛОС генератора даёт нам однозначное заполнение первых p значений ключевого потока.

Возможно два варианта генерации:

- Потоковая. Генерируются все возможные заполнения первых p бит РСЛОС, затем сортируются по 2^p файлам, каждый из которых соответствует конкретным p битам ключевого потока. При криптоанализе на основе конкретного ключевого потока выбирается соответствующий файл, далее проводится анализ на основании его содержимого, все прочие варианты игнорируются.

- Поключная. Перед криптоанализом конкретного ключевого потока на основании его первых p бит генерируются только те заполнения p последних бит РСЛОС, которые могли бы его породить. Таким образом, мы избавляемся от этапа предварительной обработки и сокращаем общее количество работы по генерации в 2^p раз.

Также, в силу того, что генератор является криптографической функцией, имеет смысл провести сортировку заполнений РСЛОС в порядке убывания вероятности того, что они окажутся «верными». Наиболее вероятно, что количество «0» и «1» в блоке РСЛОС будет примерно одинаковым. Исходя из этого, заполнения РСЛОС в файлах сортируются, ориентируясь на увеличение разницы между количеством «0» и «1».

Литература

1. Menezes A., Van Oorschot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, 1996. 657 p.
2. Massacci F., Marraro L. Logical Cryptanalysis as a SAT Problem // J. Autom. Reasoning. 2000. Vol. 24, No. 1/2. pp. 165-203.
3. Заикин О.С. Реализация процедур прогнозирования трудоемкости параллельного решения SAT-задач // Вестник УГАТУ. 2010. Т. 14, № 4. С. 210-220.