АНАЛИЗ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ ШИФРА HC-128 В ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СЕТЯХ

Лысов А.В., Фёдоров А.В.
Научный руководитель: Фёдоров А.В.
Харьковский национальный университет радоэлектроники, Украина
E-mail: kyle-mp@inbox.ru

Аннотация — Выполнен анализ эффективности использования современного поточного шифра *HC*-128 семейства *eStream* в каналах с ошибками (открытых информационных сетях). Основное внимание уделено анализу криптографической стойкости шифра *HC*-128.

1. Введение

Наиболее распространенным решением, используемым для обеспечения конфиденциальности данных, является применение блочных криптоалгоритмов. Однако эти алгоритмы в случае возникновения искажений символов шифртекста при их передаче вносят дополнительные искажения при дешифровании криптограммы. Данное явление получило название лавинного эффекта. В свою очередь, поточные криптоалгоритмы, лишенные лавинного эффекта, хотя и обладают меньшей стойкостью к взлому, тем не менее больше подходят для использования в каналах связи с ошибками. Данная работа посвящена анализу эффективности применения поточного шифра *HC*-128 семейства *eStream*. Основное внимание уделено оценке криптографической стойкости шифра *HC*-128.

2. Основная часть

В дальнейшем мы будем использовать следующие обозначения [1]: P — таблица состоящая из 512 32-битовых элементов. Каждый элемент обозначается через $P[i]$, $0 \le i \le 511$; Q — таблица состоящая из 512 32-битовых элементов. Каждый элемент обозначается через $Q[i]$, $0 \le i \le 511$; K — 128-битовый ключ *HC*-128; IV — 128-битовый вектор инициализации *HC*-128; s — генерируемая шифром *HC*-128 псевдослучайная последовательность (ПСП).

Для управления процессом генерации ключевого потока s шифр использует ключ K и вектор инициализации IV на очередном шаге работы алгоритма обновляется один элемент таблицы с помощью функции с нелинейной обратной связью. Все элементы двух таблиц полностью обновляются через каждые 1024 шага. На каждом шаге на выходе нелинейной фильтрующей функции формируется одно 32-битовое значение гаммы шифрующей.

Рассмотрим подробней алгоритм начальной инициализации шифра. Ключ K и вектор IV расширяются в массив W_i, $0 \le i \le 1279$ по следующему алгоритму:

$$W_i = \begin{cases} K_i, 0 \le i \le 7, \\ IV_{i-8}, 8 \le i \le 15, \\ f_2(W_{i-2}) + f_{10}(W_{i-15}) + W_{i-16} + i, 16 \le i \le 1279. \end{cases} \quad (1)$$

Затем обновляются таблицы P и Q:

$$\begin{aligned} P[i] &= W_{i+256}, \text{при } 0 \le i \le 511; \\ Q[i] &= W_{i+768}, \text{при } 0 \le i \le 511. \end{aligned} \quad (2)$$

Функции $f_1(x)$ и $f_2(x)$ совпадают с функциями преобразования сообщения $\sigma_0(x)$ и $\sigma_1(x)$ алгоритма *SHA*-256 [2]. Для функции $h_1(x)$ в качестве S-блока используется таблица Q. В свою очередь, таблица P используется в качестве S-блока для функции $h_2(x)$:

$$\begin{aligned} P[i] &= (P[i] + g_1(P[i \boxminus 3], P[i \boxminus 10], P[i \boxminus \\ &\boxminus 511])) \oplus h_1(P[i \boxminus 12]); \\ Q[i] &= (Q[i] + g_2(Q[i \boxminus 3], Q[i \boxminus 10], Q[i \boxminus \\ &\boxminus 511])) \oplus h_2(Q[i \boxminus 12]). \end{aligned} \quad (3)$$

Здесь $x \boxminus y$ означает $x - y \pmod{512}$. Функции g_1, g_2, h_1 и h_2 имеют вид:

$$\begin{aligned} g_1(x,y,z) &= ((x >>> 10) \oplus (z >>> 23)) + (x >>> 8); \\ g_2(x,y,z) &= ((x <<< 10) \oplus (z <<< 23)) + (y <<< 8); \\ h_1(x) &= Q[x_0] + Q[256 + x_2]; \\ h_2(x) &= P[x_0] + P[256 + x_2]. \end{aligned} \quad (4)$$

На каждом шаге работы алгоритма происходит обновление одного элемента таблицы и формируется одно выходное 32-битовое значение гаммы согласно (3). Каждый S-блок используется для генерации только 512 выходных слов, затем он обновляется в течение следующих 512 шагов.

Для оценки криптографической стойкости шифра *HC*-128 в работе были использованы как стандартные тесты Кнута, так и оригинальные, суть которых состояла в вычислении попарных коэффициентов корреляции для ПСП сгенерированных на различных ключах. Затем по полученным данным строилась гистограмма, которая сравнивалась с аналогичной гистограммой, найденной для алгоритма *RC*4. Для определения степени сходства распределений, представленных гистограммами, использовалось расстояние Кульбака-Лейблера.

3. Заключение

Проведенные тесты показали, что, как и следовало ожидать, алгоритм *HC*-128 является стойким. Однако наличие функций $\sigma_0(x)$ и $\sigma_1(x)$ в структуре шифра делает возможными атаки, разработанные для хэш-функций семейства SHA.

4. Список литературы

[1] HC-128 / Ecrypt. — http://www.ecrypt.eu.org/stream/e2-HC128.html. — 20.02.13.
[2] FIPS 180-4: Secure Hash Standard / NIST. — http://csrc.nist.gov/publications/PubsFIPS.html. — 20.02.13.

ANALYSIS OF EFFICIENCY OF APPLYING THE *HC*-128 CIPHER IN OPEN INFORMATION NETWORKS

Lysov A.V., Fedorov A.V.
Scientific adviser: Fedorov A.V.
Kharkov National University of Radioelectronics, Ukraine

Abstract — Analysis of efficiency of applying the modern *eStream* cipher *HC*-128 over error channels (open networks) has been done. The major attention is paid to analysis of the *HC*-128 cipher cryptographic strength.