R.D. Ginyatullin

On Properties of GGHN Stream Cipher

Keywords: RC4, GGHN, transfer function.

In this paper we discuss properties of a state transition function of the GGHN cryptosystem, which was proposed in 2005 in CISC as a modification of RC4. For describing the state transition function of GGNH we use automatic language.We also describe statistical properties of keystream in this cryptosystem.

Р.Д. Гинятуллин

О СВОЙСТВАХ АЛГОРИТМА ПОТОЧНОГО ШИФРОВАНИЯ GGHN

RC4 – поточная шифрсистема, предложенная и разработанная в 1987 году Р. Ривестом. Она используется в различных приложениях и протоколах, в том числе: SSL и WEP. Стойкость RC4 анализировалась во многих работах, например [Flu01, Pud01].

RC4 имеет множество модификаций, которые создавались с целью улучшения определенных характеристик шифрсистемы. Одна из таких модификаций – GGHN [Inf05] (название состоит из первых символов фамилий четырех соавторов: Gong, Gupta, Hell и Nawaz). Свойства этой шифрсистемы рассматривались в различных работах, например [Pau06, Kir10].

Опишем алгоритм поточного шифрования GGNH (n, m) (для практических приложений используются $n = 8, m = 32$) на автоматном языке. Состоянием алгоритма в такте $t \geq 1$ является $V_t = (i_t, j_t, k_t, s_t) \in Z_{2^n} \times Z_{2^n} \times Z_{2^m} \times Z_{2^m}^{2^n}$, начальное состояние – (i_0, j_0, k_0, s_0), где $i_0 = 0$ и $j_0 = 0$.

Приведем описание *t*-го $(t = 1,2 \ldots.)$ такта работы алгоритма GGHN(n, m):

Функция переходов F

$$i_t = i_{t-1} + 1 \ (\mathrm{mod}\ 2^n);$$
$$j_t = j_{t-1} + s_{t-1}[i_t] (\mathrm{mod}\ 2^n);$$
$$k_t = k_{t-1} + s_{t-1}[j_t] (\mathrm{mod}\ 2^m)$$
$$s_t[s_{t-1}[i_t] + s_{t-1}[j_t] (\mathrm{mod}\ 2^n)] = k_t + s_{t-1}[i_t] \ (\mathrm{mod}\ 2^m)$$

Функция выходов f

Выход: $z_t = (s_t[(s_t[j_t] + s_t[i_t]) (\mathrm{mod} 2^n)] + k_t) \ (\mathrm{mod}\ 2^m)$.

В работе [Ban11] описаны циклы длины 2^n и свойства различных начальных состояний. В отличие от RC4, в GGHN изменение состояния V_tпроисходит за счет изменения шагов 3 и 4 функции переходов GGNH по сравнению с функцией переходов в RC4, из-за чего возникают циклы с подходами. Для анализа состояний были построены ориентированные графы для различных *n* и *m*.

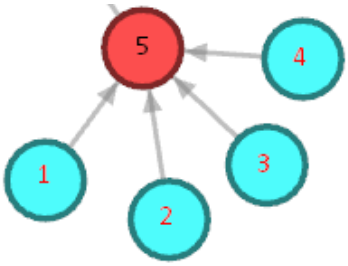

Рис. 1

Каждая из вершин графа (рис. 1) обозначает одно из состояний (i_t, j_t, k_t, s_t) шифр-системы на t-м такте. На рисунке изображены четыре начальных состояния (1, 2, 3, 4) которые переходят в общее состояние 5 на 1-м такте. В результате анализа полученных графов доказаны некоторые их свойства.

Заметим, что каждая из вершин имеет полустепень исхода, равную 1.

Обозначим через $M_{n,m}$ множество всех вершин графа, $M_{n,m}^{(j)}$ – множество всех вершин графа, достижимых за j тактов, тогда $M_{n,m}^{(0)}$ – множество всех начальных состояний алгоритма GGHN(n, m), а $\rho(x, y)$ – кратчайшее расстояние между вершинами x и y графа функции переходов. Положим $\mathrm{R}_{n,m}^{(j)}(v_0) = \{\omega_0 \in M_{n,m} | \rho(v_0, \omega) = j\}$, где $v_0 \in M_{n,m}^{(0)}$.

Утверждение. У состояний (i_0, j_0, k_0, s_0) вершин, входящих в $\mathrm{R}_{n,m}^{(1)}(v_0)$, всегда совпадает элемент $s_0[1]$

Замечание. Общее число состояний GGHN(n, m) равно $2^{n^2} 2^{m^{2^n+1}}$.

Отметим, что достижимых вершин оказалось меньше: при $n = 2, m = 2$ достигается всего примерно 18 %, при $n = 2,\ m = 3\ \div\ 12$ %.

Проведено исследование свойств гаммы алгоритма GGHN. Для проверки статистических свойств гаммы использовались тесты NIST. Приведем некоторые результаты: частотный тест прошло 25 % проверяемых последовательностей, тест рангов бинарных матриц – 100 %, тест кумулятивных сумм – 100 %, проверку линейной сложности – 95 %. Остальные тесты не прошла ни одна последовательность. Это позволяет сделать предположение о существовании зависимостей в гамме алгоритма GGNH.

СПИСОК ЛИТЕРАТУРЫ:

1. [Flu01] Fluhrer, S.R., Mantin, I., Shamir, A.: Weaknesses in the key scheduling algorithm of RC4. In: Selected Areas in Cryptography 2001. LNCS, vol. 2259, pp. 1–24. Springer, New York (2001).
2. [Knu98] Knudsen, L.R., Meier, W., Prenel, B., Rijmen, V., Verdoolaege, S.: Analysis methods for (Alleged) RC4. In: ASIACRYPT'98. LNCS, vol. 1514, pp. 327–341. Springer, New York (1998).
3. [Ban11] Subhadeep B., Subhamoy M., Santanu S.: On the Evolution of GGHN Cipher (2011).
4. [Pau06] Paul, S., Preneel, B.: On the (In) security of Stream Ciphers Based on Arrays and Modular Addition. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 69–83. Springer, Heidelberg (2006).
5. [Kir10] Kircanski, A., Youssef, A.M.: On the structural weakness of the GGHN stream cipher. Cryptography and Communications (Discrete Structures, Boolean Functions and Sequences) 2(1), 1–17 (2010).
6. [Inf05] Information Security and Cryptology: First SKLOIS Conference, CISC 2005.
7. [Pud01] Pudovkina M., Short cycles of the alleged RC4 keystream generator // 3nd International Workshop on Computer Science and Information Technologies – CSIT'2001– UFA– 2001.

REFERENCES:

1. [Flu01] Fluhrer, S.R., Mantin, I., Shamir, A.: Weaknesses in the key scheduling algorithm of RC4. In: Selected Areas in Cryptography 2001. LNCS, vol. 2259, pp. 1–24. Springer, New York (2001).
2. [Knu98] Knudsen, L.R., Meier, W., Prenel, B., Rijmen, V., Verdoolaege, S.: Analysis methods for (Alleged) RC4. In: ASIACRYPT'98. LNCS, vol. 1514, pp. 327–341. Springer, New York (1998).
3. [Ban11] Subhadeep B., Subhamoy M., Santanu S.: On the Evolution of GGHN Cipher (2011).
4. [Pau06] Paul, S., Preneel, B.: On the (In) security of Stream Ciphers Based on Arrays and Modular Addition. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 69–83. Springer, Heidelberg (2006).
5. [Kir10] Kircanski, A., Youssef, A.M.: On the structural weakness of the GGHN stream cipher. Cryptography and Communications (Discrete Structures, Boolean Functions and Sequences) 2(1), 1–17 (2010).
6. [Inf05] Information Security and Cryptology: First SKLOIS Conference, CISC 2005.
7. [Pud01] Pudovkina M., Short cycles of the alleged RC4 keystream generator // 3nd International Workshop on Computer Science and Information Technologies – CSIT'2001– UFA– 2001.