О ДИНАМИКЕ ПАМЯТИ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ МАКЛАРЕНА-МАРСАЛЬИ

УДК 004.421.5-519.217.2

И.Б. Бережной, Ю.С. Харин,
НИИ ППМИ БГУ, г. Минск

Аннотация

Рассматривается класс криптографических генераторов псевдослучайных последовательностей Макларена-Марсальи. Исследуется вероятностная модель динамики памяти генераторов Макларена-Марсальи. Получены отдельные вероятностные свойства памяти.

Введение

В системах криптографической защиты информации важную роль играют последовательности случайных чисел [1, 2]. На практике для их генерации в основном используют программные генераторы, когда детерминированным алгоритмом создается псевдослучайная последовательность, как можно больше похожая на случайную. В последнее время особое внимание уделяется генераторам с памятью. Так, в конкурсе eSTREAM, целью которого было создание европейских стандартов для поточных систем шифрования, два из четырех финалистов в профиле «поточные шифры для программного применения с большой пропускной способностью» являются такими генераторами [3]. Современные генераторы в подавляющем большинстве представляют собой комплексы комбинированных определенным образом модулей, представляющих собой различные криптографические примитивы [1, 2]. Данные примитивы для эффективной работы всего генератора должны иметь достаточно простую структуру и при этом обладать хорошими криптографическими свойствами. Одним из таких широко известных примитивов является класс генераторов Макларена-Марсальи [4], которые сочетает свойство простоты реализации с достаточно высоким качеством выходной последовательности [5]. Об этом свидетельствует и тот факт, что один из участников конкурса eSTREAM, получивший хорошую оценку, поточный шифр «Ямб» [6] содержит модуль аналогичной структуры.

Ранее класс генераторов Макларена-Марсальи изучался авторами в статье [7], в которой представлена формула для периода выходной последовательности, уточняющая приведенную в [2] формулу, доказаны некоторые вероятностные свойства, на основании которых построены формулы и оценки, характеризующие влияние генератора на некоторые статистические характеристики выходной последовательности. В данной статье продолжено исследование класса генераторов Макларена-Марсальи: исследуется вероятностная модель динамики памяти генераторов Макларена-Марсальи при различных условиях, доказан критерий равномерности предельного распределения вероятностей памяти, получена формула для предельного распределения в общем случае, на основании которой найдены некоторые вероятностные характеристики динамики памяти.

1 Математическая модель генераторов Макларена-Марсальи

Генераторы Макларена-Марсальи, исследуемые в данной статье, имеют структуру, представленную на рисунке 1. Любой генератор данного семейства состоит из модифицируемой памяти размера L и двух простейших генераторов псевдослучайных последовательностей: G_1 и G_2. Генератор G_1 порождает «заполняющую» («исходную») последовательность $\{\zeta_t\}$ над некоторым конечным множеством V, генератор G_2 – «управляющую» последовательность над множеством $A = \{0,1, ..., L–1\}$. Результирующей (выходной) последовательностью является последовательность над V. Имеется некоторое начальное заполнение памяти – вектор-столбец $X_0 = (x_{0,1}, x_{0,2}, ..., x_{0,L})^T \in V^L$ (T – знак транспонирования).

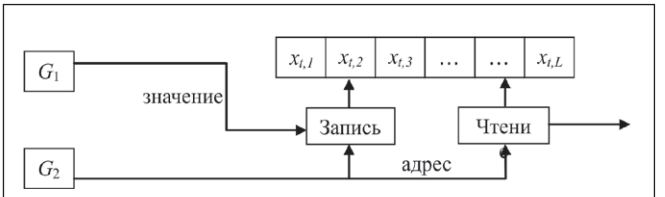

Рисунок 1 – Схема генератора Макларена-Марсальи

Определим функцию $Y = \chi(X, v, a)$, где $X, Y \in V^L$, $v \in V$, $a \in A$, следующим образом:

$$Y=(y_1, y_2, ..., y_L), \quad y_i = \begin{cases} x_i, & \text{если } i \neq a; \\ v, & \text{если } i = a. \end{cases} \qquad (1)$$

Другими словами, функция $\chi(X, v, a)$ заменяет в векторе X значение элемента с номером a на значение v.

Пусть $\{X_t: t = 1, 2, ...\}$ – последовательность состояний памяти X, X_0 – некоторое начальное заполнение памяти. Тогда динамика генератора на тактах $t = 1, 2, ...$ опишется формулами:

$$\begin{aligned} y_t &= x_{t-1,\zeta_t}, \\ X_t &= \chi(X_{t-1}, \zeta_t, \eta_t). \end{aligned} \qquad (2)$$

Таким образом, на каждом такте в выходную последовательность считывается элемент из памяти X по адресу, определяемому генератором G_2, затем по этому адресу в память заносится новый элемент из последовательности, порождаемой генератором G_1.

2 Вероятностная модель динамики памяти

Пусть $\{\zeta_t\}$ и $\{\eta_t\}$ – определенные на некотором вероятностном пространстве (Ω, F, P) последовательности независимых в совокупности случайных величин с распределениями вероятностей:

$$\begin{aligned} P\{\zeta_t = i\} &= \lambda_i \neq 0, \ i \in V, \ \sum_{i \in V} \lambda_i = 1; \\ P\{\eta_t = j\} &= \gamma_j \neq 0, \ j \in A, \ \sum_{j \in A} \gamma_j = 1. \end{aligned} \qquad (3)$$

Теорема 1. Пусть $\{\zeta_t\}$ и $\{\eta_t\}$ – определенные на некотором вероятностном пространстве (Ω, F, P) последовательности независимых в совокупности случайных величин с распределениями вероятностей (3). Тогда последователь-

ность $\{X_t\}$ состояний памяти представляет собой регулярную цепь Маркова первого порядка с пространством состояний V^L и матрицей переходных вероятностей $P = (p_{j,k})$:

$$p_{JK} = P\{X_{t+1} = K | X_t = J\} = \sum_{i\in V}\sum_{j\in A}\lambda_i\gamma_j\delta_{K,\chi(J,i,j)}, \quad J,K \in V^L, \tag{4}$$

где $\delta_{J,K} = \begin{cases}1, J = K;\\ 0, J \neq K.\end{cases}$ – символ Кронекера.

Обозначим: $H(U, W) = \sum_{i=1}^{L}\left(1-\delta_{Ai,Bj}\right)$ – количество несовпадающих элементов векторов $U, W \in V^L$.

Следствие 1. При выполнении условий (3) элементы матрицы P переходных вероятностей имеют следующий вид:

$$p_{J,K} = \begin{cases}\sum_{i=1}^{L}\gamma_i\lambda_{ji}, & \text{если } H(J,K) = 0, \text{ т.е. } K = J = (j_1, j_2, ..., j_L);\\ \gamma_i\lambda_{s,} & \text{если } H(J,K) = 1, \text{ т.е. } K = \chi(J,s,i), s \neq j_i;\\ 0, & \text{если } H(J,K) \geq 2.\end{cases} \tag{5}$$

Теорема 2. Пусть $\{\zeta_t\}$ и $\{\eta_t\}$ – определенные на некотором вероятностном пространстве (Ω, F, P) последовательности независимых в совокупности случайных величин с распределениями вероятностей (3). Тогда стационарное распределение вероятностей α цепи Маркова $\{X_t\}$ существует и имеет мультипликативный вид:

$$\alpha_K = \lambda_{K_1}\cdot\lambda_{K_2}\cdot\ldots\cdot\lambda_{K_L}, K = (k_1, k_2, ..., k_L) \in V^L. \tag{6}$$

Следствие 2. Стационарное распределение вероятностей (6) состояний памяти $\{X_t\}$ не зависит от распределения вероятностей $\{\gamma_i\}$ управляющей последовательности $\{\eta_t\}$.

Следствие 3. Пусть выполняются условия теоремы 2. Стационарное распределение вероятностей α состояний памяти $\{X_t\}$ является равномерным (т.е. $\forall K \in V^L$ $\alpha_K = 1/|V^L|$) тогда и только тогда, когда распределение вероятностей $\{\lambda_i\}$ элементов заполняющей последовательности $\{\zeta_t\}$ – равномерное ($\lambda_i \equiv 1/|V|$).

Данные следствия определяют, что равномерность стационарного распределения вероятностей состояний памяти $\{X_t\}$ эквивалентна равномерности распределения вероятностей элементов заполняющей последовательности $\{\zeta_t\}$, если $\{\zeta_t\}$ и $\{\eta_t\}$ – последовательности независимых в совокупности случайных величин. Другими словами, вероятностные свойства $\{X_t\}$ не ухудшаются в сравнении с $\{\zeta_t\}$.

Введем следующие обозначения:
$u_K^{(n)}$ – частота вектора K в последовательности состояний памяти $\{X_t\}$, $t \in \{1, 2, ..., n\}$, т.е.

$$u_K^{(n)} = \frac{1}{n}\sum_{i=1}^{n}\delta_{X_i,K};$$

f_K – время первого возврата в состояние K, т.е.
$f_K = n \in N : X_n = X_0 = K, \ \forall i = \overline{1,n-1}\ X_i \neq K.$

Следствие 4. Пусть выполняются теоремы 2. Тогда верны следующие утверждения:

1. Вне зависимости от начального распределения математическое ожидание $u_K^{(n)}$ при $n\to\infty$ удовлетворяет предельному соотношению:

$$E\{u_K^{(n)}\} \to \lambda_{K_1}\cdot\lambda_{K_2}\cdot\ldots\cdot\lambda_{K_L}, K = (k_1, k_2, ..., k_L) \in V^L. \tag{7}$$

2. Математическое ожидание времени возврата в исходное состояние памяти K определяется формулой:

$$E\{f_K\} = \frac{1}{\lambda_{K_1}\cdot\lambda_{K_2}\cdot\ldots\cdot\lambda_{K_L}}. \tag{8}$$

Данное следствие описывает частотные характеристики динамики памяти генератора. С их помощью можно оценить, как часто элемент выходной последовательности выбирался из заданного состояния памяти и имел соответствующее условное распределение вероятностей.

Теорема 3. Пусть $\{\zeta_t\}$ и $\{\eta_t\}$ – определенные на некотором вероятностном пространстве (Ω, F, P) последовательности случайных величин с распределениями вероятностей (3), причем элементы $\{\eta_t\}$ независимы в совокупности, а $\{\zeta_t\}$ представляет собой цепь Маркова первого порядка с матрицей переходных вероятностей $Q = (q_{u,v})$, $u,v \in V$. Тогда случайная последовательность состояний памяти $\{X_t\}$ представляет собой однородную цепь Маркова второго порядка с матрицей переходных вероятностей $P = (p_{I,J,K})$:

$$p_{I,J,K} = P\{X_{t+1} = K | X_t = J, X_{t-1} = I\} = \frac{\sum_{i\in V}\sum_{j\in A}\left(\lambda_i\gamma_j\delta_{J,\chi(I,i,j)}\sum_{l\in V}\sum_{s\in A}q_{j,l}\lambda_s\delta_{K,\chi(J,l,s)}\right)}{\sum_{i\in V}\sum_{j\in A}\lambda_i\gamma_j\delta_{J,\chi(I,i,j)}}, \quad I, J, K \in V^L. \tag{9}$$

Следствие 5. При выполнении условий теоремы 3 элементы матрицы переходных вероятностей $P = (p_{I,J,K})$ имеют следующий вид:

$$p_{I,J,K} = \begin{cases}\dfrac{\sum_{s\in A}\left(\gamma_s\lambda_{K_s}\sum_{r\in A}\left(\gamma_r q_{k_s,k_r}\right)\right)}{\sum_{s\in A}\gamma_s\lambda_{k_s}}, & \text{если } K = J = I;\\ \dfrac{\sum_{s\in A}\left(\gamma_s\lambda_{j_s}\cdot\gamma_r q_{j_s,k_r}\right)}{\sum_{s\in A}\gamma_s\lambda_{j_s}}, & \text{если } K = \chi(J,k_r,r), k_r \neq j_r, J = I;\\ \sum_{r\in A}\left(\gamma_r q_{j_s,k_r}\right) & \text{если } K = J = \chi(I,j_s,s), j_s \neq i_s;\\ \gamma_r\cdot q_{j_s,k_r}, & \text{если } K = \chi(J,k_r,r), k_r \neq j_r, J = \chi(I,j_s,s), j_s \neq i_s;\\ 0, & \text{если } H(I,J) \geq 2 \text{ или } H(J,K) \geq 2,\end{cases} \tag{10}$$

где $K = (k_1, k_2, ..., k_L)$, $J = (j_1, j_2, ..., j_L)$, $I = (i_1, i_2, ..., i_L)$.

Следствие 6. Если в условиях теоремы 3 одномерные распределения вероятностей λ и γ элементов последовательностей $\{\zeta_t\}$ и $\{\eta_t\}$ – равномерные, то элементы матрицы переходных вероятностей $P = (p_{I,J,K})$ имеют следующий вид:

$$p_{I,J,K} = \begin{cases} \frac{1}{L^2}\sum_{s\in A}\sum_{r\in A} q_{k_s,k_r}, \text{ если } K = J = I; \\ \frac{1}{L^2}\sum_{s\in A}\left(q_{j_s,k_r}\right) \text{ если } K = \chi(J, k_r, r),\ k_r \neq j_r,\ J = I; \\ \frac{1}{L}\sum_{r\in A}\left(q_{j_s,k_r}\right) \text{ если } K = J = \chi(I, j_s, s),\ j_s \neq i_s; \\ \frac{1}{L} q_{j_s,k_r}, \text{ если } K = \chi(J, k_r, r),\ k_r \neq j_r,\ J = \chi(I, j_s, s),\ j_s \neq i_s; \\ 0, \text{ если } H(I, J) \geq 2 \text{ или } H(J, K) \geq 2. \end{cases} \quad (11)$$

Следствие 6 наглядно иллюстрирует связь между матрицей переходных вероятностей $P = (p_{I,J,K})$ последовательности состояний памяти $\{X_t\}$ и матрицей переходных вероятностей $Q = (q_{u,v})$ заполняющей последовательности $\{\zeta_t\}$. Формула (11) также позволяет проводить оценку параметров заполняющей последовательности $\{\zeta_t\}$ по выборке из последовательности $\{X_t\}$.

Полученные результаты компьютерных экспериментов иллюстрируют согласие результатов компьютерного моделирования с теоретическими результатами анализа динамики памяти генератора Макларена-Марсальи.

Заключение

В данной статье продолжено исследование класса генераторов Макларена-Марсальи. Построена вероятностная модель динамики памяти генераторов Макларена-Марсальи. Формулы, описывающие данную модель, позволяют рассматривать выходные последовательности как скрытые цепи Маркова и применять в дальнейшем известные методы их анализа (например, алгоритм Витерби). Доказан критерий равномерности стационарного распределения вероятностей памяти. Получена формула для предельного распределения в общем случае, на основании которой найдены некоторые вероятностные характеристики динамики памяти, позволяющие повысить точность общих алгоритмов анализа скрытых цепей Маркова. Результаты компьютерных экспериментов иллюстрируют согласие с теоретическими результатами.

Литература:

1. Математические и компьютерные основы криптологии / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Минск: Новое знание, 2003.

2. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2005. – 480 с.

3. eSTREAM: the ECRYPT Stream Cipher Project. – Mode of access: http://www.ecrypt.eu.org/stream/pro ject.html. – Date of access: 10.04.2013.

4. MacLaren, M. Uniform Random Number Generators / M. MacLaren, G. Marsaglia // Journal of the Association for Computing Machinery. – 1965. – V. 12(1). – P. 83–89.

5. Кнут, Д. Искусство программирования, том 2. Получисленные алгоритмы = The Art of Computer Programming, vol.2. Seminumerical Algorithms. – 3-е изд. / Д. Кнут. – М.: Вильямс, 2007.

6. «Yamb», LAN Crypto Submission to the ECRYPT Stream Cipher Project / Starodubtzev Sergey A., Lebedev Anatoly N., Volchkov Alexey A. – Mode of access: http://www.ecrypt.eu.org/stream/yamb.html. – Date of access: 10.04.2013.

7. Бережной, И.Б. О периодичности и вероятностных свойствах генератора Макларена-Марсальи / И.Б. Бережной, Ю.С. Харин // Материалы XI международной научно-практической конференции «Информационная безопасность-2010», 22–25 июня 2010 г. – Таганрог. – Ч. 3. – С. 83–85.

8. Кемени, Дж. Конечные цепи Маркова / Джон Дж. Кемени, Дж. Лори Снелл. – М.: Наука, 1970ю – 272 с.

Abstract

A family of the Maclaren-Marsaglia cryptographic generators for pseudorandom sequences is considered. A probabilistic model of the memory dynamics for the Maclaren-Marsaglia generators is proposed and analysed. Some probabilistic properties of the memory are presented.

Поступила в редакцию 18.05.2013 г.

ИЕРАРХИЧЕСКАЯ НЕЙРОСЕТЕВАЯ СИСТЕМА ДЛЯ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК

УДК 004.8.032.26

Л.Ю. Войцехович, В.А. Головко
БрГТУ, г. Брест

Аннотация

В работе представлена иерархическая многоагентная система обнаружения атак в компьютерных сетях, описана ее структура и изложены основные результаты экспериментов. Отдельный агент представляет собой комбинацию нелинейной рециркуляционной нейронной сети и персептрона. Данная модель основана на многослойной архитектуре взаимодействия агентов, которая задается набором правил, представленных в виде графа. Модель может выполнять классификацию сетевых атак по классам и типам сетевой активности. Эксперименты свидетельствуют о том, что такое архитектурное решение позволяет сократить число ложных срабатываний, повысить точность распознавания и обнаруживать новые и модифицированные образы сетевых атак.

Введение

Безопасность компьютерных систем – одна из наиболее актуальных проблем современной индустрии информационных технологий. Ее актуальность постоянно возрастает, так как