*Література: **1**. НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу". **2**. Дубровский В. В. CDMA − Взгляд глазами профессионала.//mailto:v_dubrovskii@mail.ru. **3.** Акушский И. Я., Юдицкий Д. И. Машинная арифметика в остаточных классах. // М.: Сов. радио, 1966. – 421 с. **4.** Василенко В. С., Будько М. М., Короленко М. П. Контроль и відновлення цілісності інформації в автоматизованих системах. К. НТУ "КПІ" // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. Випуск 4// 2002, с. 119 – 128.*

УДК 621.391:519.2

НИЖНЯЯ ГРАНИЦА ВЕРОЯТНОСТИ РАЗЛИЧЕНИЯ ВНУТРЕННИХ СОСТОЯНИЙ КОМБИНИРУЮЩЕГО ГЕНЕРАТОРА ГАММЫ С НЕРАВНОМЕРНЫМ ДВИЖЕНИЕМ

Антон Алексейчук, Роман Проскуровский
СФ СБ Украины ВИТИ НТУУ "КПИ"

Аннотация: **Исследуется вероятностная модель функционирования комбинирующего генератора гаммы с неравномерным движением в режиме реинициализации начального состояния. Получена аналитическая нижняя граница вероятности правильного различения двух простых гипотез о распределении внутреннего состояния генератора.**
Summary: **A probabilistic model of combine generator is investigated with irregular clocking in procedure of reinitialization of initial state. The analytic lower bound is obtained for probability of the right distinguishing of two simple hypothesis about distribution of the inner state of generator.**
Ключевые слова: **Корреляционный криптоанализ, генератор гаммы с неравномерным движением, проверка гипотез.**

I Введение

Перспективный класс генераторов псевдослучайных последовательностей, используемых при построении поточных криптосистем, образуют генераторы гаммы (ГГ) с неравномерным движением, построенные на основе двоичных линейных регистов сдвига (ЛРС) [1, 2]. Известно, что неравномерность движения ЛРС генератора при определенных условиях улучшает его криптографические свойства (приводит к увеличению периодов и эквивалентных линейных сложностей его выходных последовательностей, повышает стойкость генератора относительно традиционных корреляционных атак) [3 – 6].

В настоящее время наиболее полно исследованны генераторы гаммы с неравномерным движением, состоящие из единственного ЛРС. Обзор методов их криптоанализа приведен в [5, 6]. Следует отметить, что большинство указанных методов основывается на упрощенном вероятностном описании функционирования ЛРС с неравномерным движением, что, отчасти, связано с аналитическими трудностями исследования свойств таких ЛРС в рамках более точных математичеких моделей.

Известным примером ГГ с неравномерным движением, состоящим из нескольких ЛРС, является генератор гаммы шифра A5/1. В [7] предложен статистический метод криптоанализа этого генератора, функционирующего в режиме реинициализации начального состояния (см. [1, 8]). Основным параметром, характеризующим практическую эффективность метода [7], является наименьшее число векторов инициализации (кадров или запусков ГГ), достаточное для восстановления начального состояния ГГ с заданной надежностью.

В настоящей статье описана вероятностная модель функционирования произвольного комбинирующего ГГ с неравномерным движением и равновероятной функцией усложнения, на основе которой получена нижняя граница вероятности различения внутренних состояний генератора по наблюдаемым знакам его выходных последовательностей в серии "независимых запусков". Получена также оценка надежности корреляционной атаки, аналогичной [7], на комбинирующий генератор гаммы с неравномерным движением и линейной функцией усложнения, функционирующий в режиме реинициализации начального состояния. В качестве следствия установлена верхняя граница наименьшего числа запусков ГГ, достаточного для успешной реализации указанной корреляционной атаки с заданной надежностью.

II Постановка задачи

Рассмотрим комбинирующий генератор гаммы, состоящий из n полноцикловых двоичных линейных регистров сдвига и равновероятной булевой функции $f = f(z_1, \dots, z_n)$ [1, 2]. Предполагается, что закон движения ЛРС генератора является, в общем случае, неравномерным и определяется последовательностью неотрицательных целочисленных векторов $\varepsilon(i) = (\varepsilon_1(i), \dots, \varepsilon_n(i))$, $i = 0, 1, \dots$, вырабатываемых некоторым дополнительным устройством – блоком управления движением данного ГГ. Для любых $j \in \overline{1, n}$, $i = 0, 1, \dots$ величина сдвига j-го ЛРС генератора в такте с номером i равна $\varepsilon_j(i)$.

Обозначим $x_j(0), x_j(1), \dots$ линейную рекуррентную последовательность, вырабатываемую j-м ЛРС по фиксированному неизвестному начальному состоянию в режиме равномерного движения, $j \in \overline{1, n}$; положим $\delta(i) = (\delta_1(i), \dots, \delta_n(i)) = \sum_{j=0}^{i-1} \varepsilon(j)$, $i = 1, 2, \dots$, $\delta(0) = (0, \dots, 0)$. Заметим, что j-я координата вектора $\delta(i)$ равна суммарной величине сдвигов j-го ЛРС ($j \in \overline{1, n}$) в тактах с номерами $0, 1, \dots, i-1$.

По определению знак выходной последовательности комбинирующего ГГ в i-м такте имеет следующий вид: $\gamma_i = f(x_1(\delta_1(i)), \dots, x_n(\delta_n(i)))$, $i = 0, 1, \dots$. Задача криптоанализа рассматриваемого ГГ заключается в построении алгоритмов восстановления начальных состояний ЛРС по известному отрезку выходной последовательности и априорной информации о законе функционирования блока управления движением данного генератора гаммы.

Ниже решается частная задача криптоанализа комбинирующего ГГ с неравномерным движением, состоящая в построении статистического критерия различения его внутренних состояний в серии независимых испытаний (запусков генератора). Для уточнения постановки задачи рассмотрим следующую вероятностную модель функционирования генератора гаммы.

Зафиксируем натуральное число i_0. Обозначим символом $\delta = (\delta_1, \dots, \delta_n)$ целочисленный вектор, равный суммарной величине сдвигов ЛРС генератора в тактах с номерами $0, 1, \dots, i_0 - 1$. Предположим, что δ является случайным вектором, распределенным по известному закону на некотором множестве $\Delta \subseteq \{0, 1, \dots, L-1\}^n$, где $L \in \mathbf{N}$.

Зафиксируем вектор $a = (a_1, \dots, a_n) \in \Delta$ и введем в рассмотрение множества

$$U_\nu = \{(x_j(i) : j \in \overline{1, n}, i \in \overline{0, L-1}) \in \{0,1\}^{nL} \mid f(x_1(a_1), \dots, x_n(a_n)) = \nu\}, \ \nu \in \{0, 1\}.$$

Отметим, что в силу равновероятности функции f множества U_0 и U_1 имеют одинаковую мощность, равную 2^{nL-1}.

Функционирование ГГ происходит следующим образом. Вначале с вероятностью $1/2$ выбирается число $\nu \in \{0, 1\}$. Затем производится t испытаний (запусков генератора), в ходе которых реализуются последовательности независимых в совокупности случайных векторов $X^{(1)}, \dots, X^{(t)}$, $\delta^{(1)}, \dots, \delta^{(t)}$, где вектор $X^{(l)} = (X_j^{(l)}(i) : j \in \overline{1, n}, i \in \overline{0, L-1})$ имеет равномерное распределение вероятностей на множестве U_ν, а закон распределения вектора $\delta^{(l)} = (\delta_1^{(l)}, \dots, \delta_n^{(l)})$ совпадает с законом распределения случайного вектора δ, $l \in \overline{1, t}$. В результате на выходе ГГ формируется случайная двоичная последовательность

$$\Gamma_t = \gamma^{(1)}, \dots, \gamma^{(t)}, \quad (1)$$

где

$$\gamma^{(l)} = f(X_1^{(l)}(\delta_1^{(l)}), \dots, X_n^{(l)}(\delta_n^{(l)})), \ l \in \overline{1, t}. \quad (2)$$

Требуется разработать статистический критерий различения (проверки) по наблюдаемой реализации

случайной последовательности (1) двух простых гипотез $H_0 : \nu = 0$ и $H_1 : \nu = 1$.

Итак, сформулированная задача состоит в построении определенной статистической атаки на комбинирующий ГГ с неравномерным движением по наблюдаемым (в некоторый фиксированный момент времени i_0) знакам его выходных последовательностей, полученным при t "независимых запусках" генератора. Отметим, что к решению подобных задач приводит исследование практической стойкости генераторов гаммы, используемых в режиме реинициализации начального состояния, относительно корреляционных атак [7, 8].

В силу сделанных выше предположений априорные вероятности гипотез H_0, H_1 равны $1/2$. Как известно [9], оптимальным статистическим критерием различения указанных гипотез является байесовский критерий, в соответствии с которым гипотеза H_ν принимается в том и только в том случае, когда

$$\mathbf{P}\left(f(X_1(a_1), ..., X_n(a_n)) = \nu \Big/ \Gamma_t = \gamma_t \right) > \mathbf{P}\left(f(X_1(a_1), ..., X_n(a_n)) = \nu \oplus 1 \Big/ \Gamma_t = \gamma_t \right),$$

где $\gamma_t \in \{0,1\}^t$ – наблюдаемая реализация случайной последовательности (1).

Отметим, что произвольный критерий различения гипотез H_0 и H_1 определяется как отображение $g : \{0,1\}^t \to \{0,1\}$ такое, что гипотеза H_ν принимается, если $\gamma_t \in g^{-1}(\nu)$, $\nu \in \{0,1\}$. Вероятность правильного различения гипотез с помощью критерия g определяется по формуле $\lambda_g = \mathbf{P}\{g(\Gamma_t) = f(X_1(a_1), ..., X_n(a_n))\}$. Справедливо неравенство $\lambda_g \le \lambda^*$, где λ^* – вероятность правильного различения гипотез H_0 и H_1 с помощью байесовского критерия (см., например, [9]).

Ниже описан один из возможных критериев проверки указанных простых гипотез. Получены нижняя граница вероятности их правильного различения и верхняя граница минимального объема выборки (количества запусков ГГ), достаточного для их различения с заданной вероятностью.

III Формулировки основных результатов

Рассмотрим частный случай поставленной задачи, в котором число запусков генератора гаммы $t = 1$. В этом случае функционирование ГГ можно описать следующим образом.

Вначале независимо друг от друга, случайно и равновероятно генерируются двоичные символы $X_j(i),\ j \in \overline{1,n},\ i \in \overline{0, L-1}$. Затем реализуется случайный вектор $\delta = (\delta_1, ..., \delta_n)$ и формируется двоичный знак

$$\gamma = f(X_1(\delta_1), ..., X_n(\delta_n)). \qquad (3)$$

Требуется построить статистический критерий различения гипотез $H_0 : f(X_1(a_1), ..., X_n(a_n)) = 0$ и $H_1 : f(X_1(a_1), ..., X_n(a_n)) = 1$ по наблюдаемому знаку (3).

Для любых $\gamma, \nu \in \{0,1\}$ положим

$$\pi_f(\nu, \gamma) = \mathbf{P}\left(f(X_1(a_1), ..., X_n(a_n)) = \nu \Big/ f(X_1(\delta_1), ..., X_n(\delta_n)) = \gamma \right). \qquad (4)$$

Подчеркнем, что в выражении (4) $X_j(i)$ суть независимые случайные величины с равномерным законом распределения на множестве $\{0,1\}$, $(\delta_1, ..., \delta_n)$ – случайный вектор, распределенный на множестве $\Delta \subseteq \{0,1,...,L-1\}^n$ и не зависящий от случайных величин $X_j(i)$, $j \in \overline{1,n}$, $i \in \overline{0, L-1}$, $a = (a_1, ..., a_n)$ – фиксированный вектор, принадлежащий множеству Δ.

Обозначим V_n множество двоичных векторов длины n. Для любого $y = (y_1, ..., y_n) \in V_n$ обозначим $\mathrm{supp}(y)$ множество номеров ненулевых координат вектора y. Для любого $u = (u_1, ..., u_n) \in \mathbf{N}_0^n$ положим $u_{\mathrm{supp}(y)} = (u_{i_1}, ..., u_{i_s})$, где $\{i_1, ..., i_s\} = \mathrm{supp}(y),\ 1 \le i_1 < ... < i_s \le n$.

Теорема 1. Для любых $\gamma, \nu \in \{0,1\}$ выполняется равенство

$$\pi_f(\nu,\gamma)=\frac{1}{2}(1+2^{-2n}\sum_{y\in V_n\setminus\{0\}}(-1)^{\nu\oplus\gamma}\left|\hat{f}(y)\right|^2\mathbf{P}\{\delta_{\mathrm{supp}(y)}=a_{\mathrm{supp}(y)}\}). \quad (5)$$

где

$$\hat{f}(y)=\sum_{x\in V_n}(-1)^{f(x)\oplus xy},\ y\in V_n$$

преобразование Уолша-Адамара булевой функции f. Оптимальный критерий различения гипотез H_0 и H_1 по наблюдаемому знаку γ вида (3) состоит в принятии гипотезы H_γ. Вероятность правильного различения гипотез с помощью этого критерия равна

$$\lambda_f^*=\pi_f(0,0)=\frac{1}{2}(1+2^{-2n}\sum_{y\in V_n\setminus\{0\}}\left|\hat{f}(y)\right|^2\mathrm{P}\{\delta_{\mathrm{supp}(y)}=a_{\mathrm{supp}(y)}\}). \quad (6)$$

Отметим важное следствие, вытекающее из теоремы 1. Введем в рассмотрение величину

$$\min\{\lambda_f^*: f\in R_n\}, \quad (7)$$

где R_n обозначает множество всех равновероятных булевых функций n переменных.

Следствие 1. Минимум (7) достигается на линейной функции $f_0(z_1,...,z_n)=z_1\oplus...\oplus z_n$ и определяется по формуле

$$\lambda_{f_0}^*=\frac{1}{2}(1+\mathbf{P}\{\delta=a\}). \quad (8)$$

Рассмотрим задачу различения гипотез H_0 и H_1 в общем случае. Введем в рассмотрение случайную величину $\gamma_\Sigma=\sum_{l=1}^{t}\gamma^{(l)}$, где знаки $\gamma^{(l)}$ $(l\in\overline{1,t})$ определяются по формуле (2).

Предлагаемый критерий различения указанных гипотез состоит в следующем: если $\gamma_\Sigma < t/2$, то принимается гипотеза H_0; в противном случае принимается гипотеза H_1. Обозначим Λ_t вероятность правильного различения гипотез H_0 и H_1 с помощью этого критерия.

Теорема 2. Для любого натурального t справедливо неравенство

$$\Lambda_t \geq 1-\exp\{-\frac{t}{2}(2\lambda_f^*-1)^2\}, \quad (9)$$

где λ_f^* определяется по формуле (6). В частности, $\Lambda_t\to 1$ при $t\to\infty$.

Непосредственно из неравенства (9) вытекает такой результат.

Следствие 2. Пусть $c\in(0,1)$ и $t\geq\frac{-2\ln c}{(2\lambda_f^*-1)^2}$. Тогда $\Lambda_t\geq 1-c$. Таким образом, минимальное число t_c запусков комбинирующего ГГ с неравномерным движением, достаточное для различения гипотез H_0 и H_1 с вероятностью не менее $1-c$, удовлетворяет неравенству

$$t_c\leq\left\lceil\frac{-2\ln c}{(2\lambda_f^*-1)^2}\right\rceil. \quad (10)$$

IV Доказательства теорем

Введем ряд обозначений. Для любых векторов $u=(u_1,...,u_n)$, $v=(v_1,...,v_n)\in\mathbf{N}_0^n$ положим

$I(u,v)=\{j\in\overline{1,n}:\ u_j=v_j\}$. Пусть $A=\{i_1,...,i_s\}\subseteq\{1,2,...,n\}$, где $1\le i_1<...<i_s\le n$. Для любого вектора $x=(x_1,...,x_n)$ обозначим символом x_A вектор $(x_{i_1},...,x_{i_s})$. Вектор x условимся записывать в виде $x=(x_A,x_{\overline{A}})$, где $\overline{A}=\{1,2,...,n\}\setminus A$. Для любых $g:V_n\to\{0,1\}$, $\alpha=(\alpha_1,...,\alpha_s)\in V_s$ обозначим g_A^{α} подфункцию функции g, получаемую в результате фиксации ее переменных с номерами из множества A соответствующими координатами вектора α. Отметим, что g_A^{α} является функцией переменных набора $x_{\overline{A}}$, если g – булева функция переменных $x_1,...,x_n$. Положим $V_{(A)}=\{x_A:x\in V_n\}$. Ясно, что $V_{(A)}=V_{\#A}$, где $\#A$ – мощность множества A.

Перейдем к доказательству теоремы 1. Прежде всего, получим выражение условной вероятности

$$\rho_a(v)\overset{\text{def}}{=}\mathbf{P}\left(f(X_1(\delta_1),...,X_n(\delta_n))=0\Big/X_1(a_1)=v_1,...,X_n(a_n)=v_n\right), \tag{11}$$

где $v=(v_1,...,v_n)\in V_n$.

Докажем ряд вспомогательных утверждений.

Лемма 1. Для любых $a\in\Delta,\ v\in V_n$ справедливо следующее равенство:

$$\rho_a(v)=\frac{1}{2}\Big(1+\sum_{\substack{A\subseteq\overline{1,n}\\A\neq\varnothing}}\sum_{\substack{u\in\Delta:\\I(a,u)=A}}(2\mathbf{P}\{f_A^{v_A}(Y_{\overline{A}})=0\}-1)\mathbf{P}\{\delta=u\}\Big). \tag{12}$$

Доказательство. По формуле полной вероятности в силу независимости и равновероятности случайных величин $X_1(a_1),...,X_n(a_n)$ получим, что

$$\rho_a(v)=2^n\mathbf{P}\{f(X_1(\delta_1),...,X_n(\delta_n))=0,\ X_1(a_1)=v_1,...,X_n(a_n)=v_n\}=$$

$$=2^n\sum_{A\subseteq\overline{1,n}}\sum_{\substack{u\in\Delta:\\I(a,u)=A}}\mathbf{P}\{\delta=u\}\mathbf{P}\{X(a)=v,\ f(X_A(a_A),Y_{\overline{A}})=0\}=$$

$$=2^n\sum_{A\subseteq\overline{1,n}}\sum_{\substack{u\in\Delta:\\I(a,u)=A}}\mathbf{P}\{\delta=u\}\mathbf{P}\{X(a)=v,\ f(v_A,Y_{\overline{A}})=0\}=$$

$$=\sum_{A\subseteq\overline{1,n}}\sum_{\substack{u\in\Delta:\\I(a,u)=A}}\mathbf{P}\{\delta=u\}\mathbf{P}\{f_A^{v_A}(Y_{\overline{A}})=0\}. \tag{13}$$

Обозначим $d(a,u)$ расстояние Хэмминга между векторами a и u. В выражении (13) выделим слагаемое

$$\frac{1}{2}\sum_{\substack{u\in\Delta:\\d(a,u)=n}}\mathbf{P}\{\delta=u\}=\frac{1}{2}\Big(1-\sum_{\substack{A\subseteq\overline{1,n}:\\A\neq\varnothing}}\sum_{\substack{u\in\Delta:\\I(a,u)=A}}\mathbf{P}\{\delta=u\}\Big),$$

соответствующее множеству $A=\varnothing$. В результате получим, что

$$\rho_a(v)=\sum_{\substack{A\subseteq\overline{1,n}:\\A\neq\varnothing}}\sum_{\substack{u\in\Delta:\\I(a,u)=A}}\mathbf{P}\{\delta=u\}\mathbf{P}\{f_A^{v_A}(Y_{\overline{A}})=0\}+\frac{1}{2}\Big(1-\sum_{\substack{A\subseteq\overline{1,n}:\\A\neq\varnothing}}\sum_{\substack{u\in\Delta:\\I(a,u)=A}}\mathbf{P}\{\delta=u\}\Big).$$

Из полученного равенства непосредственно следует формула (12). Лемма доказана.

Лемма 2. Пусть $A\subseteq\overline{1,n}$, $A\neq\varnothing$. Тогда

$$\sum_{\substack{u\in\Delta:\\I(a,u)=A}}\mathbf{P}\{\delta=u\}=\sum_{B\supseteq A}(-1)^{\#B-\#A}\mathbf{P}\{\delta_B=a_B\}. \tag{14}$$

Доказательство. Обозначим

$$\kappa_A(a) = \mathbf{P}\{\delta_A = a_A, \delta_j \neq a_j, j \in \overline{A}\} \quad (15)$$

выражение в левой части равенства (14). Для доказательства этого равенства применим метод включения-исключения. В качестве "предметов" (см. [10]), рассмотрим векторы $u \in \mathrm{N}_0^n$, удовлетворяющие условию $u_A = a_A$. "Вес" вектора u определим как вероятность $\mathbf{P}\{\delta = u\}$. Скажем, что вектор u обладает "свойством" j (где $j \in \overline{A}$), если $u_A = a_A$ и $u_j = a_j$. Заметим, что на основании формулы (15) число $\kappa_A(a)$ равно суммарному "весу" "предметов", не обладающих ни одним из указанных "свойств". Следовательно, по формуле включения-исключения [10]

$$\kappa_A(a) = \sum_{s=0}^{n-\#A} (-1)^s \sum_{\substack{C \subseteq \overline{A}: \\ \#C = s}} \mathbf{P}\{\delta_A = a_A, \delta_C = a_C\} = \sum_{B \supseteq A} (-1)^{\#B-\#A} \mathbf{P}\{\delta_B = a_B\},$$

что и требовалось доказать.

Лемма 3. Для любых $A \subseteq \overline{1,n}$, $A \neq \varnothing$, $v \in V_n$ выполняется равенство

$$2^{-(n-\#A)} \sum_{z_{\overline{A}} \in V_{(\overline{A})}} (-1)^{f(v_A, z_{\overline{A}})} = 2^{-n} \sum_{\substack{\beta \in V_n: \\ \mathrm{supp}(\beta) \subseteq A}} \hat{f}(\beta)(-1)^{v\beta} \quad (16)$$

где $\hat{f}(\beta), \beta \in V_n$ – преобразование Уолша-Адамара функции f.

Доказательство. Обозначим

$$C_A = \{(0_A, x_{\overline{A}}) \in V_n : x_{\overline{A}} \in V_{(\overline{A})}\},$$
$$C_A^{\perp} = C_{\overline{A}} = \{(x_A, 0_{\overline{A}}) : x_A \in V_{(A)}\}. \quad (17)$$

Отметим, что C_A является подпространством векторного пространства V_n, а $C_A^{\perp}$ – ортогональным дополнением к C_A. Используя формулу для выражения булевой функции через ее преобразование Уолша-Адамара (см., например, [11]), получим

$$2^{-(n-\#A)} \sum_{z_{\overline{A}} \in V_{(\overline{A})}} (-1)^{f(v_A, z_{\overline{A}})} = 2^{-(n-\#A)} \sum_{x \in C_A \oplus (v_A, 0_{\overline{A}})} (-1)^{f(x)} = 2^{-(n-\#A)} \sum_{x \in C_A \oplus (v_A, 0_{\overline{A}})} 2^{-n} \sum_{\beta \in V_n} \hat{f}(\beta)(-1)^{x\beta} =$$
$$= 2^{-(n-\#A)} \sum_{\beta \in V_n} 2^{-n} \hat{f}(\beta) \sum_{x \in C_A} (-1)^{x\beta} (-1)^{v_A \beta_A} = 2^{-n} \sum_{\beta \in C_A^{\perp}} \hat{f}(\beta)(-1)^{v_A \beta_A}.$$

Из полученных соотношений на основании равенств (17) следует формула (16). Лемма доказана.

Лемма 4. Для любых $a \in \Delta$, $v \in V_n$ имеет место равенство

$$\rho_a(v) = \frac{1}{2}(1 + 2^{-n} \sum_{y \in V_n \setminus \{0\}} \hat{f}(y)(-1)^{vy} \mathbf{P}\{\delta_{\mathrm{supp}(y)} = a_{\mathrm{supp}(y)}\}). \quad (18)$$

Доказательство. Подставляя равенство (14) в формулу (12), получим, что

$$\rho_a(v) = \frac{1}{2}(1 + \sum_{\substack{A \subseteq \overline{1,n}: \\ A \neq \varnothing}} (2\mathbf{P}\{f_A^{v_A}(Y_{\overline{A}}) = 0\} - 1) \sum_{B \supseteq A} (-1)^{\#B-\#A} \mathbf{P}\{\delta_B = a_B\}) =$$

$$= \frac{1}{2}(1 + \sum_{B \neq \varnothing} \mathbf{P}\{\delta_B = a_B\} \sum_{\varnothing \neq A \subseteq B} (-1)^{\#B-\#A} (2^{-(n-\#A)} \sum_{z_{\overline{A}} \in V_{(\overline{A})}} (-1)^{f(v_A, z_{\overline{A}})})). \quad (19)$$

На основании равенств (16) и (19) получим

$$\rho_a(v) = \frac{1}{2}(1 + 2^{-n} \sum_{B \neq \varnothing} \mathbf{P}\{\delta_B = a_B\} \sum_{\varnothing \neq A \subseteq B} (-1)^{\#B-\#A} \sum_{\substack{y \in V_n: \\ \mathrm{supp}(y) \subseteq A}} \hat{f}(y)(-1)^{vy}) =$$

$$= \frac{1}{2}(1 + 2^{-n} \sum_{y \in V_n \setminus \{0\}} \hat{f}(y)(-1)^{vy} \sum_{B \neq \varnothing} \mathbf{P}\{\delta_B = a_B\} \sum_{\mathrm{supp}(y) \subseteq A \subseteq B} (-1)^{\#B - \#A}). \quad (20)$$

Поскольку

$$\sum_{\mathrm{supp}(y) \subseteq A \subseteq B} (-1)^{\#B - \#A} = 1, \text{ если } B = \mathrm{supp}(y); \quad \sum_{\mathrm{supp}(y) \subseteq A \subseteq B} (-1)^{\#B - \#A} = 0 \text{ – в противном случае,}$$

то равенство (18) следует непосредственно из формулы (20). Лемма доказана.

Доказательство теоремы 1. Убедимся в справедливости формулы (5). Заметим, что на основании равенства (11)

$$\rho_a(v) = 2^{n-1} \mathbf{P}\left(X_1(a_1) = v_1, ..., X_n(a_n) = v_n \Big/ f(X_1(\delta_1), ..., X_n(\delta_n)) = 0 \right).$$

Следовательно, согласно формуле (4), $\pi_f(0,0) = 2^{-(n-1)} \sum_{\substack{v \in V_n: \\ f(v)=0}} \rho_a(v)$, откуда, принимая во внимание равенство $\sum_{\substack{v \in V_n: \\ f(v)=0}} (-1)^{v \cdot y} = \frac{1}{2} \hat{f}(y), y \in V_n \setminus \{0\}$, вытекающее из условия равновероятности функции f, и формулу (18), находим, что

$$\pi_f(0,0) = \frac{1}{2}(1 + 2^{1-2n} \sum_{y \in V_n \setminus \{0\}} \hat{f}(y) \mathbf{P}\{\delta_{\mathrm{supp}(y)} = a_{\mathrm{supp}(y)}\} \sum_{\substack{v \in V_n: \\ f(v)=0}} (-1)^{vy}) =$$

$$= \frac{1}{2}(1 + 2^{-2n} \sum_{y \in V_n \setminus \{0\}} \left| \hat{f}(y) \right|^2 \mathbf{P}\{\delta_{\mathrm{supp}(y)} = a_{\mathrm{supp}(y)}\}). \quad (21)$$

Далее, на основании равенства (21)

$$\pi_f(1,0) = \frac{1}{2}(1 - 2^{-2n} \sum_{y \in V_n \setminus \{0\}} \left| \hat{f}(y) \right|^2 \mathbf{P}\{\delta_{\mathrm{supp}(y)} = a_{\mathrm{supp}(y)}\}). \quad (22)$$

Поскольку $\pi_f(0,1) = \pi_f(1,0), \pi_f(1,1) = 1 - \pi_f(0,1)$, то из равенств (21), (22) следует справедливость формулы (5) для всех $\nu, \gamma \in \{0,1\}$.

Заметим теперь, что в силу неравенств $\pi(0,0) \geq \pi(1,0), \pi(1,1) \geq \pi(0,1)$, вытекающих из соотношений (21), (22), оптимальный критерий различения гипотез H_0 и H_1 по наблюдаемой реализации случайной величины γ вида (3) состоит в принятии гипотезы H_γ. Вероятность правильного различения гипотез с помощью этого критерия равна

$$\lambda^*_f = \mathbf{P}\{f(X_1(a_1), ..., X_n(a_n)) = f(X_1(\delta_1), ..., X_n(\delta_n))\} = \frac{1}{2}(\pi(0,0) + \pi(1,1)) = \pi(0,0).$$

Таким образом, теорема 1 полностью доказана.

Доказательство следствия 1. Пусть $f_0(z) = z_1 \oplus ... \oplus z_n, z = (z_1, ..., z_n) \in V_n$. Тогда $\hat{f}_0(y) = 0$ для любого $y \in V_n \setminus \{1\}$, где 1 – вектор длины n, все координаты которого равны 1. Следовательно, на основании формулы (6) при $f = f_0$ выполняется равенство $\lambda^*_{f_0} = \frac{1}{2}(1 + \mathbf{P}\{\delta = a\})$, то есть справедлива формула (8). Далее, используя равенство $2^{-2n} \sum_{y \in V_n} \left| \hat{f}(y) \right|^2 = 1$ [11] и соотношения

$$\mathbf{P}\{\delta_{\mathrm{supp}(y)} = a_{\mathrm{supp}(y)}\} \geq \mathbf{P}\{\delta_{\mathrm{supp}(1)} = a_{\mathrm{supp}(1)}\} = \mathbf{P}\{\delta = a\}, \ y \in V_n \setminus \{0\},$$

на основании формул (6), (8) получим

$$\lambda^*_f - \lambda^*_{f_0} = 2^{-2n-1} \sum_{y \in V_n \setminus \{0\}} \left| \hat{f}(y) \right|^2 (\mathbf{P}\{\delta_{\mathrm{supp}(y)} = a_{\mathrm{supp}(y)}\} - \mathbf{P}\{\delta = a\}) \geq 0,$$

что и требовалось доказать.

Доказательство теоремы 2. Напомним, что предлагаемый критерий различения гипотез H_0 и H_1 по наблюдаемой реализации случайной последовательности (1) основан на статистике

$$\gamma_\Sigma = \sum_{l=1}^{t} \gamma^{(l)}, \qquad (23)$$

где случайные величины $\gamma^{(l)}$ $(l \in \overline{1, t})$ определяются по формуле (2).

Заметим, что в силу независимости случайных векторов $X^{(l)} = (X_j^{(l)}(i) : j \in \overline{1, n}, i \in \overline{0, L-1})$, $\delta^{(l)}$, $l \in \overline{1, t}$, случайные величины $\gamma^{(l)}$ $(l \in \overline{1, t})$ независимы в совокупности.

При этом, если справедлива гипотеза H_ν, то

$$\mathbf{P}_\nu\{\gamma^{(l)} = 1\} = |U_\nu|^{-1} \sum_{x \in U_\nu} \sum_{\substack{u=(u_1, \ldots, u_n) \in \Delta: \\ f(x_1(u_1), \ldots, x_n(u_n))=1}} \mathbf{P}\{\delta = u\} =$$

$$= \mathbf{P}\left(f(X_1(\delta_1), \ldots, X_n(\delta_n)) = 1 \Big/ f(X_1(a_1), \ldots, X_n(a_n)) = \nu \right) = \pi_f(\nu, 1), \qquad (24)$$

где

$$U_\nu = \{x = (x_j(i) : j \in \overline{1, n}, i \in \overline{0, L-1}) \in V_{nL} \mid f(x_1(a_1), \ldots, x_n(a_n)) = \nu\}, \ \nu \in \{0, 1\}. \qquad (25)$$

Итак, на основании формулы (24) в случае справедливости гипотезы H_ν случайная величина (23) распределена по биномиальному закону с параметром

$$p_\nu = \pi_f(\nu, 1), \ \nu \in \{0, 1\}. \qquad (26)$$

Отсюда следует, что вероятность $1 - \Lambda_t$ неправильного различения гипотез H_0 и H_1 равна

$$1 - \Lambda_t = \frac{1}{2}(\mathbf{P}_0\{\gamma_\Sigma \geq \frac{t}{2}\} + \mathbf{P}_1\{\gamma_\Sigma < \frac{t}{2}\}) = \frac{1}{2}\Big(\sum_{t/2 \leq i \leq t} \binom{t}{i} p_0^i (1-p_0)^{t-i} + \sum_{0 \leq i < t/2} \binom{t}{i} p_1^i (1-p_1)^{t-i} \Big). \qquad (27)$$

В силу соотношений $p_0 \leq 1/2 \leq p_1$, вытекающих из формул (5) и (26), справедливы неравенства [12]

$$\sum_{t/2 \leq i \leq t} \binom{t}{i} p_0^i (1-p_0)^{t-i} \leq e^{-2t(1/2 - p_0)^2}, \quad \sum_{0 \leq i < t/2} \binom{t}{i} p_1^i (1-p_1)^{t-i} \leq e^{-2t(p_1 - 1/2)^2},$$

из которых на основании равенств (6), (27) непосредственно следует неравенство (9). Теорема доказана.

V Оценка надежности корреляционной атаки на комбинирующий ГГ с неравномерным движением и линейной функцией усложнения

Покажем, что полученные выше результаты позволяют оценить надежность практически реализуемой корреляционной атаки на комбинирующий ГГ с неравномерным движением и линейной функцией усложнения, функционирующий в режиме реинициализации начального состояния.

На практике реинициализация (переустановка) начального состояния ГГ синхронного поточного шифра осуществляется при синхронизации передающего и принимающего шифрующих устройств [1, 8]. Как правило, в этом случае по исходному начальному состоянию $x^{(0)}$ генератора и двоичным векторам инициализации $c^{(1)}, \ldots, c^{(t)}$, передаваемым в открытом виде по каналу связи ($x^{(0)}, c^{(l)} \in V_{nL}$, $l \in \overline{1, t}$), формируются начальные состояния ГГ $x^{(l)} = x^{(0)} \oplus c^{(l)}$, $l \in \overline{1, t}$, по которым вырабатываются отрезки шифрующей гаммы. Задача криптоаналитика состоит в разработке алгоритмов восстановления вектора

$x^{(0)}$ по известным векторам $c^{(1)}, ..., c^{(t)}$ и соответствующим им выходным последовательностям генератора [8].

Предположим, что функция усложнения f комбинирующего ГГ с неравномерным движением является линейной, $f(z) = z_1 \oplus ... \oplus z_n$, $z = (z_1, ..., z_n) \in V_n$ (см. следствие 1). Обозначим $x_j^{(0)}(0),\ x_j^{(0)}(1),\ ...$ ($c_j^{(l)}(0),\ c_j^{(l)}(1),\ ...$) знаки линейной рекурренты, вырабатываемые равномерно движущимся j-м ЛРС генератора гаммы при установке последнего в начальное состояние $x^{(0)}$ ($c^{(l)}$, $l \in \overline{1, t}$), $j \in \overline{1, n}$.

Предлагаемый алгоритм корреляционного криптоанализа ГГ в режиме реинициализации начального состояния заключается в построении статистической оценки значения

$$f(x_1^{(0)}(a_1),...,x_n^{(0)}(a_n)) = x_1^{(0)}(a_1) \oplus ... \oplus x_n^{(0)}(a_n) \quad (28)$$

для фиксированных $a_1, ..., a_n \in \mathbf{N}_0$ и состоит в выполнении следующих действий.

- Фиксируем число $i_0 \in \mathbf{N}$ (номер знака выходной последовательности ГГ) и вектор $a = (a_1, ..., a_n) \in \Delta$ (где $\Delta \subseteq \{0, 1, ..., L-1\}^n$ – носитель распределения вероятностей случайного вектора $\delta = \delta(i_0)$, $L \in \mathbf{N}$; см. п. II).

- По известным векторам инициализации $c^{(1)}, ..., c^{(t)}$ вычисляем значения

$$g^{(l)} = f(c_1^{(l)}(a_1),...,c_n^{(l)}(a_n)),\ l \in \overline{1,t}. \quad (29)$$

- По известным знакам гаммы $\gamma^{(1)}, ..., \gamma^{(t)}$, выработанным генератором в момент времени i_0 при начальных состояниях $x^{(0)} \oplus c^{(1)}, ..., x^{(0)} \oplus c^{(t)}$ соответственно, находим значение статистики

$$\widetilde{\gamma}_\Sigma = \sum_{l=1}^{t} (\gamma^{(l)} \oplus g^{(l)}), \quad (30)$$

по которому принимаем решение о значении параметра (28). Если $\widetilde{\gamma}_\Sigma < t/2$, то полагаем $f(x_1^{(0)}(a_1),...,x_n^{(0)}(a_n)) = 0$; в противном случае полагаем $f(x_1^{(0)}(a_1),...,x_n^{(0)}(a_n)) = 1$.

Отметим, что описанный алгоритм аналогичен первому этапу предложенного в [7] алгоритма корреляционного криптоанализа шифра A5/1. Основное отличие между указанными алгоритмами состоит в применении различных решающих процедур для построения оценки значения (28) (в [7] вместо функции (30) используется статистика отношения правдоподобия).

С целью оценки надежности изложенного алгоритма, а также минимального числа запусков ГГ, достаточного для восстановления значения (28) с заданной надежностью, рассмотрим вероятностную модель функционирования ГГ, по существу аналогичную модели, описанной в п. II.

Предположим, что

1) упорядоченный набор $x^{(0)} = (x_j^{(0)}(i) : j \in \overline{1, n}, i \in \overline{0, L-1})$ с априорной вероятностью $1/2$ имеет равномерное распределение на одном из множеств U_0, U_1, где U_ν ($\nu \in \{0, 1\}$) определяется по формуле (25);

2) значения $g^{(1)}, ..., g^{(t)}$ вида (29) известны (не случайны), и для любого $l \in \overline{1, t}$ двоичный набор $(c_j^{(l)}(i) : j \in \overline{1, n}, i \in \overline{0, L-1})$ является реализацией случайного вектора

$$C^{(l)} = (C_j^{(l)}(i) : j \in \overline{1, n}, i \in \overline{0, L-1})$$

с равномерным законом распределения на множестве $U_{g^{(l)}}$;

3) знаки $\gamma^{(1)}, ..., \gamma^{(t)}$, выработанные генератором по начальным состояниям $x^{(0)} \oplus c^{(1)}, ..., x^{(0)} \oplus c^{(t)}$ соответственно, определяются по формуле

$$\gamma^{(l)} = f(x_1^{(0)}(\delta_1^{(l)}) \oplus C_1^{(l)}(\delta_1^{(l)}), ..., x_n^{(0)}(\delta_n^{(l)}) \oplus C_n^{(l)}(\delta_n^{(l)})),\ l \in \overline{1,t}, \quad (31)$$

где случайные векторы $\delta^{(l)} = (\delta_1^{(l)}, ..., \delta_n^{(l)})$, $l \in \overline{1,t}$, имеют тот же закон распределения, что и вектор δ;

4) случайные векторы $x^{(0)}, C^{(l)}, \delta^{(l)}$, $l \in \overline{1,t}$, независимы в совокупности.

При сделанных предположениях рассмотрим критерий различения гипотез $H_\nu : f(x_1^{(0)}(a_1), \dots, x_n^{(0)}(a_n)) = \nu$, $\nu \in \{0,1\}$, основанный на статистике (30).

Заметим, что в силу предположений 1) и 4) случайные величины $\tilde{\gamma}^{(l)} = \gamma^{(l)} \oplus g^{(l)}$, $l \in \overline{1,t}$, независимы в совокупности при выполнени каждой из гипотез H_0, H_1. При этом, если справедлива гипотеза H_ν, то на основании предположений 1), 2), 4) и линейности функции f случайный вектор $x^{(0)} \oplus C^{(l)}$ имеет равномерное распределение на множестве $U_{\nu(l)}$, где $\nu(l) = \nu \oplus g^{(l)}$, $l \in \overline{1,t}$. Следовательно, согласно равенству (31),

$$\mathbf{P}_\nu\{\tilde{\gamma}^{(l)} = 1\} = \mathbf{P}_\nu\{\gamma^{(l)} = g^{(l)} \oplus 1\} = \left|U_{\nu(l)}\right|^{-1} \sum_{x \in U_{\nu(l)}} \sum_{\substack{u=(u_1,\dots,u_n)\in\Delta: \\ f(x_1(u_1),\dots,x_n(u_n))=g^{(l)}\oplus 1}} \mathbf{P}\{\delta = u\}. \quad (32)$$

Заметим теперь, что выражение в правой части равенства (32) совпадает с условной вероятностью

$$\mathbf{P}\left(f(\chi_1(\delta_1), ..., \chi_n(\delta_n)) = g^{(l)} \oplus 1 \Big/ f(\chi_1(a_1), ..., \chi_n(a_n)) = \nu(l) \right) \quad (33)$$

где $\chi = (\chi_j(i) : j \in \overline{1,n}, i \in \overline{0, L-1})$ – случайный вектор, равномерно распределенный на множестве V_{nL} и не зависящий от случайного вектора $\delta = (\delta_1, ..., \delta_n)$. В силу линейности функции f и равенства (5) вероятность (33) равна $\pi_f(\nu(l), g^{(l)} \oplus 1) = \frac{1}{2}(1 + (-1)^{\nu \oplus 1}\mathbf{P}\{\delta = a\})$.

Итак, при выполнении гипотезы H_ν ($\nu \in \{0,1\}$) слагаемые $\gamma^{(l)} \oplus g^{(l)}$ в выражении (30) независимы в совокупности и распределены по закону

$$\mathbf{P}_\nu\{\gamma^{(l)} \oplus g^{(l)} = 1\} = 1 - \mathbf{P}_\nu\{\gamma^{(l)} \oplus g^{(l)} = 0\} = \frac{1}{2}(1 + (-1)^{\nu \oplus 1}\mathbf{P}\{\delta = a\}),\ l \in \overline{1,t}.$$

Отсюда, повторяя рассуждения, проведенные при доказательстве теоремы 2, получим следующую оценку надежности $\Lambda_0^{(t)}$ описанного выше алгоритма корреляционного криптоанализа комбинирующего ГГ с неравномерным движением и линейной функцией усложнения:

$$\Lambda_0^{(t)} \geq 1 - \exp\{-\frac{t}{2}\mathbf{P}\{\delta = a\}^2\}. \quad (34)$$

Из формулы (34) следует, что минимальное число t_c запусков указанного генератора, достаточное для восстановления значения (28) с надежностью $1-c$, $c \in (0,1)$, удовлетворяет неравенству

$$t_c \leq \left\lceil \frac{-2\ln c}{(\mathbf{P}\{\delta = a\})^2} \right\rceil. \quad (35)$$

VII Выводы

На основе вероятностной модели функционирования комбинирующего ГГ с неравномерным движением, получены аналитические границы (9) и (10) соответственно вероятности различения состояний генератора по его выходным последовательностям в серии “независимых запусков” и объема материала (числа запусков ГГ), достаточного для различения его состояний с заданной вероятностью.

Как видно из формул (9), (10), основным параметром, характеризующим вероятность различения

состояний генератора, является величина λ_f^*, определяемая по формуле (6). Увеличение значений этой величины (при замене функции усложнения или блока управления движением ГГ) приводит к экспоненциальному уменьшению верхней границы средней вероятности ошибки оптимального критерия различения состояний ГГ в описанной вероятностной модели. Минимум значений λ_f^* по всей совокупности равновероятных булевых функций n переменных достигается на линейной функции $f_0(z_1, ..., z_n) = z_1 \oplus ... \oplus z_n$ и определяется по формуле (8).

Получена аналитическая граница надежности практически реализуемой корреляционной атаки на комбинирующий ГГ с неравномерным движением и линейной функцией усложнения, функционирующий в режиме реинициализации начального состояния (см. формулу (34)). Указанная атака аналогична первому этапу алгоритма корреляционного криптоанализа шифра A5/1 [7] и отличается от него лишь процедурой проверки соответствующих статистических гипотез. Получена также верхняя оценка объема материала, достаточного для успешного проведения описанной корреляционной атаки с заданной надежностью (см. формулу (35).

Моделирование на ЭВМ изложенных алгоритмов криптоанализа комбинирующих ГГ с неравномерным движением и проверка корректности применения полученных теоретических выводов к реальным ГГ составляют задачи дальнейших исследований авторов.

Литература: ***1.*** *Фомичев В. М. Дискретная математика и криптология. – М.: ДИАЛОГ-МИФИ, 2003. – 400 с.* ***2.*** *Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002.* ***3.*** *Meneses A., van Oorschot P., Vanderstone S. Handbook of applied cryptography. – CRC Press, 1997.* ***4.*** *Ekdahl P. On LFSR-based stream cipher: analysis and design. – Ph. D. Th., 2003.* ***5.*** *Kholosha A. A. Clock-controlled shift registers for key-stream generation. // http://eprint.iacr.org/2001/061.* ***6.*** *Gollman D., Chambers W. G. Clock-controlled shift registers: a review // IEEE J. on Selected Areas in Communication. – 1989. – V. 7. – № 4. – P. 525 – 533.* ***7.*** *Ekdahl P., Johansson T. Another attack on A5/1 // IEEE Trans. on Inform. Theory. – 2003. – Vol. 49. – P. 1 – 7.* ***8.*** *Armknecht F., Lano J., Preenel B. Extending the resynchronizating attack // http://eprint.iacr.org./2004/232.* ***9.*** *Боровков А. А. Математическая статистика. – М.: Наука., 1984. – 472 с.* ***10.*** *Сачков В. Н. Введение в комбинаторные методы дискретной математики. – М.: Наука, 1982. – 384 с.* ***11.*** *Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. – М.: МЦНМО, 2004. – 470 с.* ***12.*** *Ширяев А. Н. Вероятность. – М.: Наука, 1989. – 638 с.*

УДК 621.391:519.2

АЛГОРИТМЫ НЕЛИНЕЙНОГО СЛУЧАЙНОГО КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ СООБЩЕНИЙ Z_4-ЛИНЕЙНЫМИ КОДАМИ В МОДЕЛИ WIRE-TAP CHANNEL

Антон Алексейчук, Сергей Гришаков
СФ СБ Украины в составе ВИТИ НТУУ "КПИ"

Аннотация: **Рассматривается модель системы передачи информации по каналу связи с отводом, состоящая из бесшумного основного канала и двоичного симметричного отводного канала. Для данной модели предложены практически реализуемые алгоритмы случайного кодирования и декодирования сообщений двоичными нелинейными кодами, соответствующими линейным кодам над кольцом вычетов по модулю 4 при отображении Грея. Показано, что предложенные алгоритмы имеют не более чем квадратичные от длины используемого кода временную и емкостную сложности.**

Summary: **It is considering the model of information transmission system with the wiretap, which consists of the noiseless main channel and binary symmetrical wiretap channel. Practically realizable algorithms of the random messages coding and decoding by binary non-linear codes, which correspond to linear codes over the residue ring modulo 4 by Gray mapping are proposed for this model. It is shown that proposed algorithms have no more than quadratic time and space complexities from the length of using code.**

Ключевые слова: **Криптографическая защита информации, безусловно стойкий протокол согласования ключей, отводной канал, случайное кодирование, четверичный линейный код.**