О сбоях в работе связанных генераторов псевдослучайных чисел RC4

Д.С. Кудияров

Аннотация. В настоящей статье приводятся уточненные определения сбоев и расхождений в работе связанных генераторов псевдослучайных чисел RC4. Выполнена классификация сбоев, определено множество их возможных комбинаций в некоторый момент времени t в работе $N-1$ пары связанных генераторов $g_{N-1,0}$ и $g_{N-1,\delta}$, где $\delta \in [1; N-1]$, оценены вероятности каждой комбинации.

Ключевые слова: RC4, сбой, генератор, псевдослучайный.

Введение

RC4 это семейство генераторов псевдослучайных чисел (далее – ГПСЧ) RC4(M). Параметр $M \geq 2$ определяет множество внутренних состояний RC4. RC4(8) является промышленно используемой реализацией на сегодняшний день. Далее обозначение RC4 будет говорить о том, что речь идет о RC4(M) с любым значением M.

RC4 состоит из процедуры инициализации KSA (Key Scheduling Algorithm) и процедуры выработки псевдослучайных чисел PRGA (Pseudorandom Generation Algorithm). Данные процедуры похожи, поэтому, в целях упрощения записи, для элементов внутренних состояний будут введены одинаковые обозначения. Внутреннее состояние RC4 в момент времени t будет обозначаться $v_t = (i_t, j_t, s_t)$, где $i_t \in \mathbb{Z}_N, j_t \in \mathbb{Z}_N, s_t \in \mathbb{S}_N, N = 2^M$. Если принадлежность обозначений частей внутренних состояний KSA и PRGA не будет понятна из контекста, то она будет указана явно, например, состояние в момент времени t процедуры KSA: $v_{K,t} = \left(i_t, j_{K,t}, s_{K,t}\right)$.

KSA предназначена для выработки начального состояния ГПСЧ на основе ключа. Ключ, используемый для инициализации, представляет собой последовательность элементов кольца $\mathbb{Z}_N$: $k = (k_x)_{x=0}^{N-1}, k_x \in \mathbb{Z}_N$. Начальное состояние RC4 до KSA $v_{-1} = (i_{-1}, j_{-1}, s_{-1}) = (0,0,e)$, где e – тождественная подстановка. В каждый момент времени $t \in [0; N-1]$ происходит переход в новое состояние $v_t = (i_t, j_t, s_t) = \left(i_{t-1} \boxplus 1, j_{t-1} \boxplus s_{t-1}(i_t) \boxplus k_t, s_{t-1} \circ \left(s_{t-1}(i_t), s_{t-1}(j_t)\right)\right)$, где $\boxplus$ – операция сложения по модулю N, $\circ$ - операция композиции подстановок.

Процедура PRGA предназначена для выработки выходной последовательности псевдослучайных чисел и изменения внутреннего состояния RC4. Начальное состояние RC4 перед выполнением PRGA зависит только от состояния, в которое перешел RC4 после KSA: $v_{P,0} = \left(i_{P,0}, j_{P,0}, s_{P,0}\right) = \left(0,0, s_{K,N-1}\right)$. В каждый момент времени $t \in [1; \infty]$ генератор переходит в следующее состояние $v_t = (i_t, j_t, s_t) = \left(i_{t-1} \boxplus 1, j_{t-1} \boxplus s_{t-1}(i_t), s_{t-1} \circ \left(s_{t-1}(i_t), s_{t-1}(j_t)\right)\right)$. После перехода в новое состояние вырабатывается выходное значение $\gamma_t = s_t\left(s_t(i_t) \boxplus s_t(j_t)\right)$. То есть в каждый момент времени при выполнении PRGA последовательно выполняется:

$$\begin{aligned} i_t &= i_{t-1} \boxplus 1 \\ j_t &= j_{t-1} \boxplus s_{t-1}(i_t) \\ s_t &= s_{t-1} \circ \big(s_{t-1}(i_t), s_{t-1}(j_t)\big) \\ \gamma_t &= s_t\big(s_t(i_t) \boxplus s_t(j_t)\big) \end{aligned} \tag{1}$$

В работе рассматривается вопрос влияния связанных ключей на функционирование RC4 и, в частности, на выработку данными генераторами выходных последовательностей. Со времени создания ГПСЧ RC4 было опубликовано около двух десятков работ, посвященных анализу связанных генераторов RC4.

В [1] впервые было введено понятие связанных ключей и показано что, метод анализа, основанный на них, может быть применим к большому количеству генераторов (в том числе RC4), использующих процедуры инициализации.

В [2] определен класс связанных ключей ГПСЧ RC4, и показано, что пара связанных RC4 вырабатывает схожие начала выходных последовательностей, что авторы подтвердили серией экспериментов. Также в данной работе даны экспериментальные оценки длин начал таких схожих последовательностей.

В [3] впервые приведены методы, позволяющие вычислить весь ключ RC4 k по выходным символам генераторов, функционирующих согласно протоколу WEP, то есть инициализированных ключами, полученными конкатенацией известного инициализационного вектора k_{iv} и неизвестной части ключа k_s: $k = k_{iv}|k_s$ и $k = k_s|k_{iv}$, где символ | - операция конкатенации. Трудоемкость данных методов составляет 2^{16} операций и не зависит от M. В [4 - 8] были приведены другие методы решения данной задачи, отличающиеся от описанного выше трудоемкостью и вероятностью успешного завершения. В [9] был опубликован метод вычислений 128-битного ключа RC4 в режиме протокола WPA по 2^{32} пакетам с трудоемкостью 2^{96}, а также ключа RC4, функционирующего в режиме WEP, по 4000 пакетов с трудоемкостью 2^{26} и вероятностью 0,5.

В работах [10-15] описаны классы ключей, приводящих к коллизиям – формированию одинаковых начальных состояний RC4, а, соответственно, и к выработке ими одинаковых выходных последовательностей. В данных работах были приведены методы и трудоемкость поиска ключей, принадлежащих таким классам, и оценены их мощности.

В [16] опубликован метод вычисления ключа генератора RC4 по начальным подстановкам связанных генераторов. Для решения указанной задачи для RC4(8) требуется 2^{23} операций и столько же начальных подстановок, полученных на основе ключей, связанных с искомым. Вероятность успешного вычисления ключа составляет 1. Для применения метода аналитик должен обладать возможностью выбирать, каким образом связанный ключ будет отличаться от искомого. В [17] авторы развили идею, описанную в [16], и привели два новых метода вычисления ключа по связанным генераторам. Для работы первого необходимо, чтобы аналитик обладал возможностью генерировать выходные последовательности по ключу с заданным им отличиями от искомого и получать информацию об отличиях в выходном потоке. Данный метод позволяет вычислить ключ длины N символов за 2^{23} таких генераций с вероятностью 1. Второй метод позволяет вычислить используемый циклически 40 битный ключ за $2^{24,75}$ операций. Предполагается, что аналитик обладает знанием начальных состояний RC4(8) и обладает возможностью инициализировать генератор RC4 неизвестным ему искомым ключом и отличиям от него.

В [2] были приведены определения связанных ключей RC4, связанных генераторов, расхождения связанных генераторов и сбоев в их работе. Уточним их все, за исключением определений связанного ключа и связанных генераторов.

Определение 1. Два ключа $k_{n,0} = \left(k_{n,0,x}\right)_{x=0}^{N-1}$ и $k_{n.\delta} = \left(k_{n,\delta,x}\right)_{x=0}^{N-1}$ являются связанными, если: $k_{n.\delta} = \begin{cases} (k_0, k_1, \dots, k_{n-1}, k_n \boxplus \delta, k_{n+1} \boxminus \delta, k_{n+2}, \dots k_{N-1}), & n \in [0, N-2] \\ (k_0, k_1, \dots, k_{N-2}, k_{N-1} \boxplus \delta), & n = N-1 \end{cases}$, $(\delta \in [0; N-1])$.

Определение 2. Два генератора RC4 $g_{n,0}$ и $g_{n,\delta}$ ($\delta \in [0; N-1]$) являются связанными, если они были инициализированы связанными ключами $k_{n,0}$ и $k_{n,\delta}$.

Определение 3. В момент времени $d_{n,\delta} = t$ произошло ***расхождение*** в работе двух связанных генераторов $g_{n,0}$ и $g_{n,\delta}$ ($\delta \in [1; N-1]$) RC4(M), если во время выполнения PRGA выполнилось условие $s_{n,0,t-1}(i_t) \neq s_{n,\delta,t-1}(i_t)$, где t положительно и минимально.

Определение 4. В момент времени $t > 0$ произошел ***сбой*** в работе двух связанных генераторов RC4 $g_{n,0}$ и $g_{n,\delta}$ ($\delta \in [1; N-1]$), если во время выполнения PRGA в момент времени t до их расхождения ($d_{n,\delta} > t$) выполняется хотя бы одно из условий: $s_{n,0,t-1}(j_{n,0,t}) \neq s_{n,\delta,t-1}(j_{n,0,t})$, либо $s_{n,0,t}\left(s_{n,0,t}(i_t) \boxplus s_{n,0,t}(j_{n,0,t})\right) \neq s_{n,\delta,t}\left(s_{n,\delta,t}(i_t) \boxplus s_{n,0,t}(j_{n,0,t})\right)$.

Введем еще одно определение.

Определение 5. Будем говорить, что в момент времени $d_{\text{общ}} = \min t'$ процедуры PRGA произошло общее расхождение, если не существует такой пары генераторов $g_{n,0}$ и $g_{n,\delta}$ ($\delta \in [1; N-1]$) в работе которых не произошло расхождения в любой из моментов времени $t \in [1; t']$.

Связанные генераторы, рассматриваемые в настоящей статье, всегда инициализируются ключами, отличающимися в последнем элементе (под номером $N-1$). Поэтому, в рамках настоящей работы в целях простоты изложения не будет указываться номер отличающегося элемента ключа. Далее генератор $g_{N-1,0}$, и связанный с ним $g_{N-1,\delta}$, в момент времени t (соответственно) обладающие внутренними состояниями $v_{N-1,0,t} = (i_t, j_{N-1,0,t}, s_{N-1,0,t})$ и $v_{N-1,\delta,t} = (i_t, j_{N-1,\delta,t}, s_{N-1,\delta,t})$, и вырабатывающие выходные значения $\gamma_{N-1,0,t}$ и $\gamma_{N-1,\delta,t}$, будут обозначаться как генераторы g_0 и связанный с ним g_δ, в момент времени t (соответственно) обладающие внутренними состояниями $v_{0,t} = (i_t, j_{0,t}, s_{0,t})$ и $v_{\delta,t} = (i_t, j_{\delta,t}, s_{\delta,t})$, и вырабатывающие выходные значения $\gamma_{0,t}$ и $\gamma_{\delta,t}$. Аналогично будет обозначаться и момент расхождения связанных генераторов g_0 и g_δ: $d_{0,\delta}$.

В статье, в отличие от [2], где авторы рассматривали одну пару связанных генераторов, рассматривается $N-1$ пара связанных генераторов g_0 и g_δ, где $\delta \in [1; N-1]$.

Цели статьи:

– классифицировать сбои в работе пар связанных генераторов RC4 g_0 и g_δ ($\delta \in [1; N-1]$);

– определить причины появления данных сбоев;

– вычислить вероятности возникновения комбинаций сбоев в каждый из моментов времени $t \in [1; N-2]$ процедуры PRGA в работе всех пар генераторов g_0 и g_δ ($\delta \in [1; N-1]$).

В рамках настоящей работы предполагается истинным, что общее расхождение $d_{\text{общ}} > N-2$.

1. Анализ влияния связанных ключей RC4 на процедуру PRGA

1.1. Подстановки связанных генераторов

Обозначим $z_{\delta,t\ldots t'}(x)$ номер такого перехода в подстановке $s_{\delta,t'}$, который удовлетворяет $s_{\delta,t'}\left(z_{\delta,t\ldots t'}(x)\right) = s_{\delta,t}(x)$. То есть $z_{\delta,t\ldots t'}(x)$ это позиция, на которую был перемещен переход $s_{\delta,t}(x)$ с момента времени $t+1$ до t' PRGA включительно. В силу (1):

$$\forall x \in [0; N-1] \& x \notin \{i_t, j_{0,t}\}: x = z_{\delta,t-1\ldots t}(x), i_t = z_{\delta,t-1\ldots t}(j_{\delta,t}), j_{\delta,t} = z_{\delta,t-1\ldots t}(i_t),$$

где $\delta \in [0; N-1], t > 0$

В момент времени $N-1$ KSA подстановка $s_{K,0,N-2}$ генератора g_0 умножается слева на транспозицию $\left(s_{K,0,N-2}(N-1), s_{K,0,N-2}(j_{K,0,N-1})\right)$, а связанного с ним g_δ – на $\left(s_{K,0,N-2}(N-1), s_{K,0,N-2}(j_{K,\delta,N-1})\right)$. До момента $N-1$ подстановки были одинаковы: $\forall t \in [0; N-2]: s_{0,t} = s_{\delta,t}$. Соответственно, для подстановок $s_{0,0}$ и $s_{\delta,0}$ при выполнении PRGA верно: $\forall x \in [0; N-1] \& x \notin \{j_{K,0,N-1}, j_{K,\delta,N-1}, N-1\}, \delta \in [1; N-1]: s_{0,0}(x) = s_{\delta,0}(x)$.

Будем говорить, что подстановки s и s' обладают отличием или отличаются в переходе под номером x, если $s(x) \neq s'(x)$.

Рассмотрим три случая:

– если $j_{K,0,N-1} \neq N-1, j_{K,\delta,N-1} \neq N-1$, то $s_{0,0}$ и $s_{\delta,0}$ имеют 3 отличия, причем: $s_{0,0}(j_{K,0,N-1}) = s_{\delta,0}(j_{K,\delta,N-1}), s_{0,0}(j_{K,\delta,N-1}) = s_{\delta,0}(N-1), s_{0,0}(N-1) = s_{\delta,0}(j_{K,0,N-1})$;

– если $j_{K,0,N-1} = N-1$ то $s_{0,0}$ и $s_{\delta,0}$ имеют 2 отличающихся перехода, причем: $s_{0,0}(N-1) = s_{\delta,0}(j_{K,\delta,N-1}), s_{0,0}(j_{K,\delta,N-1}) = s_{\delta,0}(N-1)$;

– если $j_{K,0,N-1} \neq N-1, j_{K,\delta,N-1} = N-1$ то $s_{0,0}$ и $s_{\delta,0}$ имеют 2 отличающихся перехода, причем: $s_{0,0}(j_{K,0,N-1}) = s_{\delta,0}(N-1), s_{0,0}(N-1) = s_{\delta,0}(j_{K,0,N-1})$.

<u>Утверждение 1</u>. В любой момент времени $t < d_{0,\delta}$ процедуры PRGA подстановки $s_{0,t}$ и $s_{\delta,t}$ во внутренних состояниях пары генераторов g_0 и g_δ ($\delta \in [1; N-1]$) будут содержать неизменное количество отличий, то есть $\forall\delta \in [1; N-1], \forall t, t' \in [0; d_{0,\delta}-1]: \left|\{x: x \in [0; N-1], s_{0,t}(x) \neq s_{\delta,t}(x)\}\right| = \left|\{y: y \in [0; N-1], s_{0,t'}(y) \neq s_{\delta,t'}(y)\}\right|$.

Доказательство Утверждения 1. Для доказательства Утверждения 1 достаточно доказать, что $\forall x \in [0; N-1]: z_{0,t-1\dots t}(x) = z_{\delta,t-1\dots t}(x)$. Предположим обратное: $\exists x: z_{0,t-1\dots t}(x) \neq z_{\delta,t-1\dots t}(x)$. Для переходов под номерами $x \in \{0,1,\dots,i_t-1, i_t+1,\dots,j_{0,t}-1, j_{0,t}+1,\dots,N-1\}$ ложность данного предположения очевидна. Если $x = i_t$, то необходимо чтобы выполнялось $j_{0,t} \neq j_{\delta,t}$, что является противоречием (так как генераторы связаны и не разошлись, то $j_{0,t} = j_{0,t}$). Если $x = j_{0,t}$, то необходимо чтобы $i_t \neq i_t$, что так же является противоречием. Утверждение 1 доказано.

Соответственно, в момент времени t отличия в подстановках пары связанных генераторов g_0 и g_δ до их расхождения будут располагаться в переходах под номерами $z_{\delta,0\dots t}(j_{K,0,N-1})$, $z_{\delta,0\dots t}(j_{K,\delta,N-1})$, $z_{\delta,0\dots t}(N-1)$ при наличии трех отличающихся переходов до начала PRGA и $z_{\delta,0\dots t}(j_{K,\delta,N-1})$, $z_{\delta,0\dots t}(N-1)$ или $z_{\delta,0\dots t}(j_{K,0,N-1})$, $z_{\delta,0\dots t}(N-1)$ при наличии двух отличий.

Если в момент времени $N-1$ KSA выполняется $j_{K,0,N-1} \neq N-1$, то пара связанных генераторов g_0, $g_{N\boxminus 1\boxminus j_{K,0,N-1}}$ будет обладать двумя отличиями в $s_{0,0}$ и $s_{N\boxminus 1\boxminus j_{K,0,N-1},0}$, причем $s_{0,0}(j_{K,0,N-1}) = s_{N\boxminus 1\boxminus j_{K,0,N-1},0}(N-1)$ и $s_{0,0}(N-1) = s_{N\boxminus 1\boxminus j_{K,0,N-1},0}(j_{K,0,N-1})$. Все остальные пары g_0, g_δ ($\delta \neq N \boxminus 1 \boxminus j_{K,0,N-1}$) будут обладать тремя отличиями в подстановках $s_{0,0}$ и $s_{\delta,0}$, причем $s_{0,0}(j_{K,0,N-1}) = s_{\delta,0}(j_{K,\delta,N-1})$, $s_{0,0}(j_{K,\delta,N-1}) = s_{\delta,0}(N-1)$ и $s_{0,0}(N-1) = s_{\delta,0}(j_{K,0,N-1})$.

Согласно Утверждению 1, в момент времени t ($t < d_\delta$) в подстановках $s_{0,t}$ и $s_{N\boxminus 1\boxminus j_{K,0,N-1},t}$ останется так же два отличия, причем:

$$s_{0,t}\left(z_{0,0\dots t}(j_{K,0,N-1})\right) = s_{N\boxminus 1\boxminus j_{K,0,N-1},t}\left(z_{0,0\dots t}(N-1)\right),$$
$$s_{0,t}\left(z_{0,0\dots t}(N-1)\right) = s_{N\boxminus 1\boxminus j_{K,0,N-1},t}\left(z_{0,0\dots t}(j_{K,0,N-1})\right) \quad (2)$$

Аналогично в подстановках $s_{0,t}$ и $s_{\delta,t}$ ($\delta \neq N \boxminus 1 \boxminus j_{K,0,N-1}$) останется три отличия, причем:

$$s_{0,t}\left(z_{0,0\dots t}(j_{K,0,N-1})\right) = s_{\delta,t}\left(z_{0,0\dots t}(j_{K,\delta,N-1})\right), \quad s_{0,t}\left(z_{0,0\dots t}(j_{K,\delta,N-1})\right) = s_{\delta,t}\left(z_{0,0\dots t}(N-1)\right),$$
$$s_{0,t}\left(z_{0,0\dots t}(N-1)\right) = s_{\delta,t}\left(z_{0,0\dots t}(j_{K,0,N-1})\right) \quad (3)$$

Если в момент времени $N-1$ KSA выполняется $j_{K,0,N-1} = N-1$, то все пары связанных генераторов g_0, g_δ будут обладать двумя отличиями в $s_{0,0}$ и $s_{\delta,0}$, причем $s_{0,0}(j_{K,0,N-1}) = s_{\delta,0}(N-1)$ и $s_{0,0}(N-1) = s_{\delta,0}(j_{K,0,N-1})$. Соответственно, в $s_{0,t}$ и $s_{\delta,t}$ так же будет два отличия:

$$s_{0,t}\left(z_{0,0\dots t}(N-1)\right) = s_{\delta,t}\left(z_{0,0\dots t}(j_{K,0,N-1})\right), s_{0,t}\left(z_{0,0\dots t}(j_{K,0,N-1})\right) = s_{\delta,t}\left(z_{0,0\dots t}(N-1)\right) \quad (4)$$

Так как до расхождения генераторов g_0, g_δ в любой момент времени $t < d_\delta$ выполняется равенство $j_{0,t} = j_{\delta,t}$, то все отличия, расположенные под номерами $j_{K,0,N-1}$ и $N-1$ и характерные для всех δ, будут находиться к моменту времени t на позициях с номерами $z_{0,0\dots t}\left(j_{K,0,N-1}\right)$ и $z_{0,0\dots t}(N-1)$ соответственно для всех δ.

1.2. Классификация сбоев в работе RC4

Согласно *Определению 4*, при сбое в работе связанных генераторов RC4 g_0 и g_δ до их расхождения выполняется хотя бы одно из условий $s_{0,t-1}\left(j_{0,t}\right) \neq s_{\delta,t-1}\left(j_{0,t}\right)$, $s_{0,t}\left(s_{0,t}(i_t) \boxplus s_{0,t}\left(j_{0,t}\right)\right) \neq s_{\delta,t}\left(s_{\delta,t}(i_t) \boxplus s_{0,t}\left(j_{0,t}\right)\right)$.

Заметим, что при выполнении условия $s_{0,t}\left(s_{0,t}(i_t) \boxplus s_{0,t}\left(j_{0,t}\right)\right) \neq s_{\delta,t}\left(s_{\delta,t}(i_t) \boxplus s_{0,t}\left(j_{0,t}\right)\right)$, выходные значения генераторов различны, при невыполнении – иначе. Соответственно, не всегда сбой в работе пары связанных генераторов сопровождается различными выходными значениями.

Определение 6. В момент времени t произошел ***явный сбой*** в работе двух связанных генераторов g_0 и g_δ ($\delta \in [1; N-1]$), если в их работе произошел сбой и $\gamma_{0,t} \neq \gamma_{\delta,t}$.

Определение 7. В момент времени t произошел ***неявный сбой*** в работе двух связанных генераторов g_0 и g_δ ($\delta \in [1; N-1]$), если в их работе произошел сбой и $\gamma_{0,t} = \gamma_{\delta,t}$.

Определение 8. Явный сбой, произошедший в работе двух связанных генераторов g_0 и g_δ ($\delta \in [1; N-1]$) в момент времени t, принадлежит роду 1, если истинно: $s_{0,t-1}\left(j_{0,t}\right) \neq s_{\delta,t-1}\left(j_{0,t}\right)$ и $s_{0,t}\left(s_{0,t}(i_t) \boxplus s_{0,t}\left(j_{0,t}\right)\right) \neq s_{\delta,t}\left(s_{\delta,t}(i_t) \boxplus s_{0,t}\left(j_{0,t}\right)\right)$.

Определение 9. Явный сбой, произошедший в работе двух связанных генераторов g_0 и g_δ ($\delta \in [1; N-1]$) в момент времени t, принадлежит роду 2, если истинно $s_{0,t-1}\left(j_{0,t}\right) \neq s_{\delta,t-1}\left(j_{0,t}\right)$, но ложно $s_{0,t}\left(s_{0,t}(i_t) \boxplus s_{0,t}\left(j_{0,t}\right)\right) \neq s_{\delta,t}\left(s_{\delta,t}(i_t) \boxplus s_{0,t}\left(j_{0,t}\right)\right)$.

<u>Утверждение 2.</u> Если в работе связанных генераторов g_0 и g_δ ($\delta \in [1; N-1]$) в момент времени $t < d_{0,\delta}$ происходит сбой рода 1 или неявный сбой, то одно из отличий в подстановках $s_{0,t}$ и $s_{\delta,t}$ будет перемещено на позицию под номером i_t.

Доказательство Утверждения 2. Согласно Определению 8, при сбое 1 рода и неявном сбое выполняется неравенство $s_{0,t-1}\left(j_{0,t}\right) \neq s_{\delta,t-1}\left(j_{0,t}\right)$. Так как в момент времени t подстановки $s_{0,t} = \left(s_{0,t-1}(i_t), s_{0,t-1}\left(j_{0,t}\right)\right) \circ s_{0,t-1}$ и $s_{\delta,t} = \left(s_{\delta,t-1}(i_t), s_{\delta,t-1}\left(j_{0,t}\right)\right) \circ s_{\delta,t-1}$ то $s_{0,t-1}\left(j_{0,t}\right) = s_{0,t}(i_t)$ и $s_{\delta,t}(i_t) = s_{\delta,t-1}\left(j_{0,t}\right)$, что и требовалось доказать.

Заметим, что условие $s_{0,t-1}\left(j_{0,t}\right) \neq s_{\delta,t-1}\left(j_{0,t}\right)$, необходимое для появления явного сбоя 1 рода, может быть выполнено, только если $j_{0,t} \in \left\{z_{0,0\dots t-1}\left(j_{K,0,N-1}\right), z_{0,0\dots t-1}\left(j_{K,\delta,N-1}\right), z_{0,0\dots t-1}(N-1)\right\}$, так как только переходы под номерами $z_{0,0\dots t-1}\left(j_{K,0,N-1}\right), z_{0,0\dots t-1}\left(j_{K,\delta,N-1}\right), z_{0,0\dots t-1}(N-1)$ (или их подмножеством) являются различными в $s_{0,t-1}$ и $s_{\delta,t-1}$.

Так же заметим, что условие $s_{0,t}\left(s_{0,t}(i_t) \boxplus s_{0,t}\left(j_{0,t}\right)\right) \neq s_{\delta,t}\left(s_{\delta,t}(i_t) \boxplus s_{0,t}\left(j_{0,t}\right)\right)$, необходимое для появления явного сбоя 2 рода, может быть выполнено, только если $s_{\delta,t}(i_t) \boxplus s_{0,t}\left(j_{0,t}\right) \in \left\{z_{0,0\dots t}\left(j_{K,0,N-1}\right), z_{0,0\dots t}\left(j_{K,\delta,N-1}\right), z_{0,0\dots t}(N-1)\right\}$, так как только переходы под номерами $z_{0,0\dots t}\left(j_{K,0,N-1}\right), z_{0,0\dots t}\left(j_{K,\delta,N-1}\right), z_{0,0\dots t}(N-1)$ (или их подмножеством) различны в $s_{0,t}$ и $s_{\delta,t}$. Так как при явном сбое 2 рода отличающиеся переходы не перемещаются, то $z_{0,0\dots t}\left(j_{K,0,N-1}\right) = z_{0,0\dots t-1}\left(j_{K,0,N-1}\right)$, $z_{0,0\dots t}\left(j_{K,\delta,N-1}\right) = z_{0,0\dots t-1}\left(j_{K,\delta,N-1}\right), z_{0,0\dots t}(N-1) = z_{0,0\dots t-1}(N-1)$.

Согласно приведенным замечаниям, каждый род сбоев можно разделить на несколько типов.

Определение 10. Явный сбой 1 рода, произошедший в работе двух связанных генераторов RC4 g_0 и g_δ ($\delta \in [1; N-1]$) в момент времени t, принадлежит к типу 1а, если $j_{0,t} = z_{0,0\dots t-1}\left(j_{K,0,N-1}\right)$.

Определение 11. Явный сбой 1 рода, произошедший в работе двух связанных генераторов g_0 и g_δ ($\delta \in [1; N-1]$) в момент времени t, принадлежит к типу 1b, если $j_{0,t} = z_{0,0\ldots t-1}(j_{K,\delta,N-1})$.

Определение 12. Явный сбой 1 рода, произошедший в работе двух связанных генераторов g_0 и g_δ в момент времени t, принадлежит к типу 1c, если $j_{0,t} = z_{0,0\ldots t-1}(N-1)$.

Определение 13. Явный сбой 2 рода в работе двух связанных генераторов g_0 и g_δ ($\delta \in [1; N-1]$) в момент времени t принадлежит к типу 2a, если $s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\ldots t}(j_{K,0,N-1})$.

Определение 14. Явный сбой 2 рода в работе двух связанных генераторов g_0 и g_δ ($\delta \in [1; N-1]$) в момент времени t принадлежит к типу 2b, если $s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\ldots t}(j_{K,\delta,N-1})$.

Определение 15. Явный сбой 2 рода в работе двух связанных генераторов g_0 и g_δ ($\delta \in [1; N-1]$) в момент времени t принадлежит к типу 2c, если $s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\ldots t}(N-1)$.

1.3. Явные сбои

При явном сбое 1 рода, согласно Определению 8, оба условия истинны: $s_{0,t-1}(j_{0,t}) \neq s_{\delta,t-1}(j_{0,t})$ и $s_{0,t}\left(s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t})\right) \neq s_{\delta,t}\left(s_{0,t}(i_t) \boxplus s_{\delta,t}(j_{0,t})\right)$. Так как $s_{0,t-1}(j_{0,t}) \neq s_{\delta,t-1}(j_{0,t})$, то при явном сбое 1 рода отличающиеся переходы под номерами $j_{0,t}$ меняются местами с переходами под номерами i_t. $s_{0,t-1}(j_{0,t}) \neq s_{\delta,t-1}(j_{0,t})$ может быть выполнено, если:

- $j_{0,t} = z_{0,0\ldots t-1}(j_{K,0,N-1})$ – явный сбой типа 1a (согласно Определению 10);
- $j_{0,t} = z_{0,0\ldots t-1}(j_{K,\delta,N-1})$ – явный сбой типа 1b (согласно Определению 11);
- $j_{0,t} = z_{0,0\ldots t-1}(N-1)$ – явный сбой типа 1c (согласно Определению 12).

Если $j_{K,0,N-1} \neq N-1$ и $\delta \neq N \boxminus 1 \boxminus j_{K,0,N-1}$, то выполняется (3), соответственно, являются возможными сбои всех трех типов: 1a, 1b, 1c. Если $j_{K,0,N-1} \neq N-1$ и $\delta = N \boxminus 1 \boxminus j_{K,0,N-1}$, то выполняется (2), соответственно, являются возможными сбои двух типов: 1a, 1c. Если $j_{K,0,N-1} = N-1$, то выполняется (4), соответственно, являются возможными сбои двух типов: 1b, 1c.

В случае явного сбоя типа 1a истинно $j_{0,t} = z_{0,0\ldots t-1}(j_{K,0,N-1})$, следовательно, данный сбой будет происходить в работе любой неразошедшейся пары g_0 и g_δ в момент времени t при любом $\delta \neq 0$. В случае явного сбоя типа 1c выполняется равенство $j_{0,t} = z_{0,0\ldots t-1}(N-1)$, следовательно, данный сбой будет происходить в работе любой неразошедшейся пары связанных генераторов g_0 и g_δ в момент времени t при любом $\delta \neq 0$. В случае явного сбоя типа 1b выполняется равенство $j_{0,t} = z_{0,0\ldots t-1}(j_{K,\delta,N-1})$, следовательно, данный сбой в момент времени t будет происходить в работе только одной пары связанных генераторов, если данная пара не разошлась.

При явном сбое 2 рода, согласно Определению 9, выполняются условия: $s_{0,t-1}(j_{0,t}) = s_{\delta,t-1}(j_{0,t})$ и $s_{0,t}\left(s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t})\right) \neq s_{\delta,t}\left(s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t})\right)$. Так как $s_{0,t-1}(j_{0,t}) = s_{\delta,t-1}(j_{0,t})$, то при явном сбое 2 рода отличающиеся переходы не будут перемещены.

$s_{0,t-1}(j_{0,t}) = s_{\delta,t-1}(j_{0,t})$ и $s_{0,t}\left(s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t})\right) \neq s_{\delta,t}\left(s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t})\right)$ истинны, если:

- $s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\ldots t}(j_{K,0,N-1})$ – явный сбой типа 2a (согласно Определению 13);
- $s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\ldots t}(j_{K,\delta,N-1})$ – явный сбой типа 2b (согласно Определению 14);
- $s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\ldots t}(N-1)$ – явный сбой типа 2c (согласно Определению 15).

Если $j_{K,0,N-1} \neq N-1$ и $\delta \neq N \boxminus 1 \boxminus j_{K,0,N-1}$, то выполняется (3), соответственно, являются возможными сбои всех трех типов: 2a, 2b, 2c. Если $j_{K,0,N-1} \neq N-1$ и $\delta = N \boxminus 1 \boxminus j_{K,0,N-1}$, то выполняется (2), соответственно, являются возможными сбои двух типов: 2a, 2c. Если $j_{K,0,N-1} = N-1$, то выполняется (4), соответственно, являются возможными сбои двух типов: 2b, 2c.

В случае явного сбоя типа 2a выполняется $s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\ldots t}(j_{K,0,N-1})$, соответственно, данный сбой будет происходить в момент времени t в работе любой неразошедшейся пары связанных генераторов g_0 и g_δ ($\delta \neq 0$), за исключением пары, для которой верно $j_{0,t} = z_{0,0\dots t-1}(j_{K,\delta,N-1})$, в работе которой происходит явный сбой типа 1b.

В случае явного сбоя типа 2c выполняется $s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\dots t}(N-1)$, соответственно, данный сбой будет происходить в момент времени t в работе любой неразошедшейся пары связанных генераторов g_0 и g_δ ($\delta \neq 0$), за исключением пары, для которой верно $j_{0,t} = z_{0,0\dots t-1}(j_{K,\delta,N-1})$, происходит явный сбой типа 1b.

В случае явного сбоя типа 2b выполняется $s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\dots t}(j_{K,\delta,N-1})$, следовательно, данный сбой будет происходить в работе любой неразошедшейся пары связанных генераторов в момент времени t ($\delta \neq 0$), при условии, что для данной пары не является верным $j_{0,t} = z_{0,0\dots t-1}(j_{K,\delta,N-1})$, так как в данном случае в ее работе произойдет явный сбой типа 1b.

1.4. Неявные сбои

При неявном сбое, согласно Определению 7, отличие перемещается в силу выполнения неравенства $s_{0,t-1}(j_{0,t}) \neq s_{\delta,t-1}(j_{0,t})$, однако выходные значения связанных генераторов совпадают: $s_{0,t}\left(s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t})\right) = s_{\delta,t}\left(s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t})\right)$. Если $j_{K,0,N-1} \neq N-1$ и $\delta \neq N \boxminus 1 \boxminus j_{K,0,N-1}$, то истинно (3), и неявный сбой возможен, если $j_{0,t} \in \{z_{0,0\dots t-1}(j_{K,0,N-1}), z_{0,0\dots t-1}(j_{K,\delta,N-1}), z_{0,0\dots t-1}(N-1)\}$ и выполняется одно из условий:

– $\begin{cases} s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\dots t}(j_{K,0,N-1}) \\ s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\dots t}(j_{K,\delta,N-1}) \end{cases}$

– $\begin{cases} s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\dots t}(j_{K,\delta,N-1}) \\ s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\dots t}(N-1) \end{cases}$

– $\begin{cases} s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\dots t}(N-1) \\ s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\dots t}(j_{K,0,N-1}) \end{cases}$

Если $j_{K,0,N-1} \neq N-1$ и $\delta = N \boxminus 1 \boxminus j_{K,0,N-1}$, то выполняется (2), и неявный сбой возможен, если $j_{0,t} \in \{z_{0,0\dots t-1}(j_{K,0,N-1}), z_{0,0\dots t-1}(N-1)\}$ и выполняется одно из следующих условий:

– $\begin{cases} s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\dots t}(j_{K,0,N-1}) \\ s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\dots t}(N-1) \end{cases}$

– $\begin{cases} s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\dots t}(N-1) \\ s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\dots t}(j_{K,0,N-1}) \end{cases}$

Если $j_{K,0,N-1} = N-1$, то выполняется (4), и неявный сбой возможен, если $j_{0,t} \in \{z_{0,0\dots t-1}(j_{K,\delta,N-1}), z_{0,0\dots t-1}(N-1)\}$ и выполняется одно из следующих условий:

– $\begin{cases} s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\dots t}(j_{K,\delta,N-1}) \\ s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\dots t}(N-1) \end{cases}$

– $\begin{cases} s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\dots t}(N-1) \\ s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t}) = z_{0,0\dots t}(j_{K,\delta,N-1}) \end{cases}$

Допустим, что $j_{0,t}$, $s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t})$, $s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t})$, $z_{0,0\dots t}(j_{K,0,N-1})$, $z_{0,0\dots t}(j_{K,\delta,N-1})$ и $z_{0,0\dots t}(N-1)$ случайные равномерно распределенные на множестве $[0; N-1]$ величины. Тогда, вероятность неявного сбоя равна:

– В случае $j_{K,0,N-1} \neq N-1$ и $\delta \neq N \boxminus 1 \boxminus j_{K,0,N-1}$: $\frac{3}{N} \cdot 3 \cdot \left(\frac{1}{N}\right)^2 = \frac{9}{N^3}$;

– В случае $j_{K,0,N-1} \neq N-1$ и $\delta = N \boxminus 1 \boxminus j_{K,0,N-1}$: $\frac{2}{N} \cdot 2 \cdot \left(\frac{1}{N}\right)^2 = \frac{4}{N^3}$;

– В случае $j_{K,0,N-1} = N-1$: $\frac{2}{N} \cdot 2 \cdot \left(\frac{1}{N}\right)^2 = \frac{4}{N^3}$;

Данные вероятности пренебрежительно малы и, например, для RC4(8) составляют приблизительно $5{,}3 \cdot 10^{-7}$, $2{,}4 \cdot 10^{-7}$ и $2{,}4 \cdot 10^{-7}$ соответственно. В связи с этим, в дальнейших расчетах возможность появления неявного сбоя в работе связанных генераторов в какой-либо момент времени не рассматривается. В целях простоты изложения ниже по тексту будет использоваться термин «сбой» вместо термина «явный сбой».

1.5. Расхождение связанных генераторов

Согласно *Определению 3*, при расхождении g_0 и g_δ выполняется условие $s_{0,t-1}(i_t) \neq s_{\delta,t-1}(i_t)$ при минимальном t. Так как до расхождения g_0 и g_δ, обладают подстановками не более чем с тремя отличиями (согласно Утверждению 1), то разойдутся они в следующих случаях:

– при $j_{K,0,N-1} \neq N-1$ возможно расхождение при выполнении одного из следующих условий: $i_t = z_{0,0\ldots t}(j_{K,\delta,N-1})$, $i_t = z_{0,0\ldots t}(j_{K,0,N-1})$ или $i_t = z_{0,0\ldots t}(N-1)$;

– при $j_{K,0,N-1} = N-1$ возможно расхождение при выполнении одного из следующих условий: $i_t = z_{0,0\ldots t}(j_{K,\delta,N-1})$ или $i_t = z_{0,0\ldots t}(N-1)$.

Определение 16. Расхождение, произошедшее в момент времени t в работе связанных генераторов g_0 и g_δ ($\delta \in [1; N-1]$), принадлежит к типу a, если истинно $i_t = z_{0,0\ldots t-1}(j_{K,0,N-1})$.

Определение 17. Расхождение, произошедшее в момент времени t в работе связанных генераторов g_0 и g_δ ($\delta \in [1; N-1]$), принадлежит к типу b, если истинно $i_t = z_{0,0\ldots t-1}(j_{K,\delta,N-1})$.

Определение 18. Расхождение, произошедшее в момент времени t в работе связанных генераторов g_0 и g_δ ($\delta \in [1; N-1]$), принадлежит к типу c, если истинно $i_t = z_{0,0\ldots t-1}(N-1)$.

Утверждение 3. В любой момент времени t среди всех пар генераторов g_0 и g_δ, $\delta \in [1; N-1]$, найдется не более чем одна пара, в работе которой произойдет расхождение типа b.

Для доказательства Утверждения 3 необходимо предварительно доказать Утверждение 4.

Утверждение 4. Среди всех пар генераторов g_0 и g_δ, $\delta \in [1; N-1]$, для которых $t < d_{0,\delta}$, не существует таких двух пар g_0, g_{δ_1} и g_0, g_{δ_2} ($\delta_1, \delta_2 \in [1; N-1]$,), для которых выполнялось бы $z_{0,0\ldots t}(j_{K,\delta_1,N-1}) = z_{0,0\ldots t}(j_{K,\delta_2,N-1})$.

Доказательство Утверждения 4. Так как $j_{K,\delta,N-1} = j_{K,0,N-1} \boxplus \delta$ для всех $\delta \in [1; N-1]$, то не существует таких δ_1 и δ_2, $\delta_1 \neq \delta_2$ для которых $j_{K,\delta_1,N-1} = j_{K,\delta_2,N-1}$. Это значит, что не существует таких δ_1 и δ_2, для которых $z_{0,0\ldots 0}(j_{K,\delta_1,N-1}) = z_{0,0\ldots 0}(j_{K,\delta_2,N-1})$. Допустим, противоположное: в некоторый момент времени $t < d_{0,\delta_1}, t < d_{0,\delta_2}$ появляются такие δ_1 и δ_2, для которых $z_{0,0\ldots t}(j_{K,\delta_1,N-1}) = z_{0,0\ldots t}(j_{K,\delta_2,N-1})$ и $z_{0,0\ldots t-1}(j_{K,\delta_1,N-1}) \neq z_{0,0\ldots t-1}(j_{K,\delta_2,N-1})$. Так как пары генераторов еще не разошлись, то $j_{\delta_1,t} = z_{0,0\ldots t-1}(j_{K,\delta_1,N-1})$ и $j_{\delta_2,t} = z_{0,0\ldots t-1}(j_{K,\delta_1,N-1})$. Соответственно $j_{\delta_1,t} \neq j_{\delta_2,t}$, что является противоречием, так как до расхождения (при $t < d_{0,\delta_1}, t < d_{0,\delta_2}$) $j_{\delta_1,t} = j_{\delta_2,t} = j_{0,\mathrm{t}}$. То есть $z_{0,0\ldots t}(j_{K,\delta_1,N-1}) \neq z_{0,0\ldots t}(j_{K,\delta_2,N-1})$ для всех $\delta_1, \delta_2 \in [1; N-1], \delta_1 \neq \delta_2$ и $t < d_{0,\delta_1}, t < d_{0,\delta_2}$. Утверждение 4 доказано.

Доказательство Утверждения 3. Так как для расхождения типа b необходимо выполнение условия $i_t = z_{0,0\ldots t-1}(j_{K,\delta,N-1})$, и в силу Утверждения 4, истинность Утверждения 3 очевидна.

Утверждение 5. Если в некоторый момент времени t среди всех пар g_0 и g_δ, $\delta \in [1; N-1]$ найдется такая, в работе которой произойдет расхождение типа a или c, то и в работе остальных пар, не разошедшихся ранее t, так же произойдет расхождение типа a или c (соответственно).

Доказательство. Для расхождения типа a необходимо выполнение условия $i_t = z_{0,0\ldots t-1}(j_{K,0,N-1})$, для типа c – условия $i_t = z_{0,0\ldots t-1}(N-1)$. $j_{K,0,N-1}$ и $N-1$ не зависят от δ, следовательно, $z_{0,0\ldots t-1}(j_{K,0,N-1}) = z_{0,0\ldots t-1}(j_{K,0,N-1})$ и $z_{0,0\ldots t-1}(N-1) = z_{0,0\ldots t-1}(N-1)$. Соответственно, условия $i_t = z_{0,0\ldots t-1}(j_{K,0,N-1})$ и $i_t = z_{0,0\ldots t-1}(N-1)$ будут выполняться для всех пар неразошедшихся до t пар генераторов. Утверждение 5 доказано.

Согласно Утверждению 3, расхождение типа b в момент времени t будет происходить в работе не более чем одной пары генераторов. Согласно Утверждению 5, расхождение типов a и c в момент времени t будет происходить в работе всех неразошедшихся ранее генераторов. Следовательно, $d_{\text{общ}}$ момент времени, в который происходит расхождение типа a или c.

Согласно Утверждению 3, в каждый момент времени t в работе одной пары генераторов g_0 и g_δ, для которой верны равенства $i_t = j_{K,\delta,N-1} = t$ произойдет расхождение типа b. Заметим, что расхождение типа b не произойдет, если отличающийся переход в подстановках $s_{0,0}$ и $s_{\delta,t}$ будет перемещен до момента времени $t = i_t = j_{K,\delta,N-1}$.

Предположим, что $j_{0,x}$, где $x \in [1; t-1]$ – случайные величины, равномерно распределенные на $[0; N-1]$. Вычислим вероятность события, заключающегося в том, что в момент времени t PRGA среди всех пар g_0 и g_δ, $\delta \in [1; N-1]$ в работе одной и них произойдет расхождение типа b. Для наступления данного события необходимо и достаточно выполнения условия $\forall x \in [1; t-1]: j_{0,x} \neq t$, то есть отличие в переходах под номером $t = j_{K,\delta,N-1}$ не должно быть перемещено в процессе выполнения PRGA. Соответственно, вероятность данного события равна:

$$P_b(d_{0,\delta} = t) = \left(\frac{N-1}{N}\right)^{t-1} \qquad (5)$$

Теперь вычислим математическое ожидание количества пар генераторов, в работе которых в момент времени t или ранее произошло расхождение типа b. Обозначим его Y_t. Учитывая (5), и так как в каждый момент времени в работе только одной пары генераторов может произойти расхождение типа b то математическое ожидание количества пар генераторов, в работе которых в момент времени t или ранее произошло расхождение типа b равно:

$$Y_t = \sum_{x=1}^{t} 1 \cdot \left(\frac{N-1}{N}\right)^{x-1} = N - N \cdot \left(\frac{N-1}{N}\right)^{t} \qquad (6)$$

1.6. Возможные комбинации сбоев

<u>Утверждение 6.</u> В любой момент времени t возможны следующие комбинации сбоев, что (рассматриваются не разошедшиеся пары генераторов, то есть для которых верно $t < d_{0,\delta}$):

– в работе всех пар g_0 и g_δ происходит сбой типа 1a;
– в работе одной пары g_0 и g_δ происходит сбой типа 1b;
– в работе всех пар g_0 и g_δ происходит сбой типа 1c;
– в работе всех пар g_0 и g_δ происходит сбой типа 2a;
– в работе одной пары g_0 и g_δ происходит сбой типа 2b;
– в работе всех пар g_0 и g_δ происходит сбой типа 2c;
– в работе всех пар g_0 и g_δ происходит сбой типа 2a, за исключением одной пары g_0 и g_{δ_1}, в работе которой произошел сбой типа 1b;
– в работе одной пары g_0 и g_{δ_1} происходит сбой типа 2b и в работе другой пары g_0 и g_{δ_2} происходит сбой типа 1b;
– в работе всех пар g_0 и g_δ происходит сбой типа 2c, за исключением одной пары g_0 и g_{δ_1}, в работе которой произошел сбой типа 1b;
– в работе всех пар g_0 и g_δ, не происходит сбоев.

Доказательство. Согласно Определению 8 и Определению 9, сбой 1 рода происходит, если оба неравенства истинны: $s_{0,t-1}(j_{0,t}) \neq s_{\delta,t-1}(j_{0,t})$, $s_{0,t}\left(s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t})\right) \neq s_{\delta,t}\left(s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t})\right)$, а сбой 2 рода – если истинно только неравенство $s_{0,t}\left(s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t})\right) \neq s_{\delta,t}\left(s_{\delta,t}(i_t) \boxplus s_{0,t}(j_{0,t})\right)$. Следовательно, если в работе пары генераторов в некоторый момент времени произошел сбой 1 рода, то в этот же момент времени в работе данной пары не может произойти сбой 2 рода.

Как было показано выше, неравенство $s_{0,t-1}(j_{0,t}) \neq s_{\delta,t-1}(j_{0,t})$ может выполняться в двух или трех случаях, так как подстановки $s_{0,t}$ и $s_{\delta,t}$ отличаются в двух или трех переходах:

– $j_{0,t} = z_{0,0\ldots t-1}(j_{K,0,N-1})$, что соответствует явному сбою типа 1a (см. Определение 10);
– $j_{0,t} = z_{0,0\ldots t-1}(j_{K,\delta,N-1})$, что соответствует явному сбою типа 1b (см. Определение 11);
– $j_{0,t} = z_{0,0\ldots t-1}(N-1)$, что соответствует явному сбою типа 1c (см. Определение 12).

Как было показано выше, сбои типов 1a и 1c происходят в работе всех неразошедшихся к моменту времени t пар генераторов g_0 и g_δ ($\delta \in [1; N-1]$), следовательно, если в работе хотя бы одной пары генераторов g_0 и g_δ произошел сбой типа 1a или 1c, то аналогичный сбой в момент времени t произойдет и в работе всех остальных неразошедшихся пар связанных генераторов RC4. Следовательно, в момент времени t в работе всех неразошедшихся пар генераторов g_0 и g_δ ($\delta \in [1; N-1], t < d_{0,\delta}$) являются возможными только следующие комбинации, включающие в себя хотя бы один сбой типа 1a или 1c:

– в работе всех пар g_0 и g_δ происходит сбой типа 1a;
– в работе всех пар g_0 и g_δ происходит сбой типа 1c.

Так как величина $j_{K,\delta,N-1}$, а соответственно и $z_{0,0\ldots t-1}(j_{K,\delta,N-1})$, уникальны для каждой неразошедшейся к моменту времени t пары генераторов g_0 и g_δ, а значение $j_{0,t}$ – одинаково, то сбой типа 1b может произойти в работе не более чем одной пары генераторов.

Учитывая изложенное выше, можно утверждать, что необходимым (но не достаточным) условием для сбоя 2 рода в момент времени t в работе хотя бы одной пары связанных генераторов является отсутствие сбоев типов 1a или 1c в работе любой пары g_0 и g_δ в момент времени t.

Поэтому очевидно, что являются возможными только два случая (предполагается, что сбоев типов 1a или 1c в момент времени t не происходит), при которых может появиться сбой 2 рода в работе неразошедшихся к моменту времени t пар генераторов g_0 и g_δ ($\delta \in [1; N-1]$):

– если в работе одной из пар g_0 и g_δ происходит сбой типа 1b;
– если в работе всех пар g_0 и g_δ не происходит сбоя типа 1b.

Как было показано выше, сбои типов 2a и 2c происходят в работе всех неразошедшихся к моменту времени t пар g_0 и g_δ ($\delta \in [1; N-1]$), следовательно, если в работе хотя бы одной пары произошел сбой типа 2a или 2c, то аналогичный сбой в момент времени t произойдет и в работе всех остальных неразошедшихся пар связанных RC4, в работе которых не произошло сбоя типа 1b. Следовательно, в момент времени t являются возможными только следующие комбинации, включающие в себя сбой типа 2a или 2c в работе хотя бы одного из неразошедшихся генераторов:

– в работе всех пар g_0 и g_δ происходит сбой типа 2a;
– в работе всех пар g_0 и g_δ происходит сбой типа 2c;
– в работе всех пар g_0 и g_δ происходит сбой типа 2a, за исключением одной пары g_0 и g_{δ_1}, в работе которой произошел сбой типа 1b;
– в работе всех пар g_0 и g_δ происходит сбой типа 2c, за исключением одной пары g_0 и g_{δ_1}, в работе которой произошел сбой типа 1b.

Так как величина $j_{K,\delta,N-1}$, а соответственно и $z_{0,0\ldots t-1}(j_{K,\delta,N-1})$, уникальны для каждой неразошедшейся к моменту времени t пары g_0 и g_δ, а сумма $s_{0,t}(i_t) \boxplus s_{0,t}(j_{0,t})$ – одинакова, то сбой типа 2b может произойти в работе не более чем одной пары генераторов, в работе которой не произошло сбоя 1 рода. Учитывая изложенное выше, в момент времени t возможны только следующие комбинации, не включающие в себя сбои типов 1a, 1c, 2a или 2c:

– в работе одной пары g_0 и g_δ происходит сбой типа 1b;
– в работе одной пары g_0 и g_δ происходит сбой типа 2b;
– в работе одной пары g_0 и g_{δ_1} происходит сбой типа 2b и в работе другой пары g_0 и g_{δ_2}

происходит сбой типа 1b;

– в работе всех пар g_0 и g_δ, не происходит сбоев.

Утверждение 6 доказано.

1.7. Вероятности появления комбинаций сбоев в работе связанных генераторов

Подсчитаем вероятность того, что в момент времени t среди всех пар g_0 и g_δ, для которых верно $t < d_{0,\delta}$, происходит сбой типа 1a (предполагается, что $t < d_{\text{общ}}$). Пусть $j_{K,0,N-1}$ и $j_{0,t}$ случайные величины, распределенные равномерно на промежутке $[0; N-1]$.

При $j_{K,0,N-1} \neq N-1$ данный случай возможен, если $j_{0,t} = z_{0,0\ldots t-1}(j_{K,0,N-1})$. Если $j_{K,0,N-1} = N-1$ данный случай невозможен, так как $j_{0,t} = z_{0,0\ldots t-1}(j_{K,0,N-1}) = z_{0,0\ldots t-1}(N-1)$, т.е. произойдет сбой типа 1c. Соответственно, вероятность рассматриваемого случая равна:

$$\mathrm{P_{1a,t}} = \mathrm{P}\big(\mathrm{j_{K,0,N-1}} \neq \mathrm{N}-1\big) \cdot \mathrm{P}\big(\mathrm{j_{0,t}} = \mathrm{z_{0,0\ldots t-1}}(\mathrm{j_{K,0,N-1}})\big|\mathrm{j_{K,0,N-1}} \neq \mathrm{N}-1\big) = \frac{\mathrm{N}-1}{\mathrm{N}} \cdot \frac{1}{\mathrm{N}}$$
$$P_{1a,t} = \frac{N-1}{N^2}$$

График зависимости $P_{1a,t}$ от момента времени t для генератора RC4(8) приведен на Рис. 1.

Подсчитаем вероятность того, что в момент времени t среди всех пар g_0 и g_δ, для которых $t < d_{0,\delta}$, в работе только одной пары происходит сбой типа 1b (предполагается, что $t < d_{\text{общ}}$).

Пусть $j_{K,0,N-1}$, $j_{0,t}$, $s_{0,t}^{-1}(\gamma_{0,t})$ случайные величины, распределенные равномерно на промежутке $[0; N-1]$, а δ_{1b} и δ_{2b} - случайные величины, распределенные равномерно на $[1; N-1]$.

В каждый момент времени, если не происходит сбоев типов 1a и 1c всегда найдется одна пара генераторов, в работе которых произойдет сбой типа 1b, так как при сбое типа 1b, согласно Определению 11, выполняется равенство $j_{0,t} = z_{0,0\ldots t-1}(j_{K,\delta,N-1})$, а значение $j_{K,\delta,N-1}$ (соответственно и $z_{0,0\ldots t-1}(j_{K,\delta,N-1})$) принимает уникальное значение для каждой из пар g_0 и g_δ. Однако, к рассматриваемому моменту времени пара генераторов, для которой верно $j_{0,t} = z_{0,0\ldots t-1}(j_{K,\delta,N-1})$, уже может разойтись. Математическое ожидание количества таких разошедшихся пар в момент времени t равно Y_t (см. (6)). Кроме сбоя 1b в тот же момент времени среди других пар генераторов либо в работе одной может произойти сбой типа 2b либо во всех остальных произойдут сбои 2a или 2c. Для сбоя 2b, согласно *Определению 14*, необходимо чтобы выполнялось равенство $s_{0,t}^{-1}(\gamma_{0,t}) = z_{0,0\ldots t-1}(j_{K,\delta,N-1})$. Для рассматриваемого случая необходимо, чтобы пара, для которой верно $s_{0,t}^{-1}(\gamma_{0,t}) = z_{0,0\ldots t-1}(j_{K,\delta,N-1})$ уже разошлась или отсутствовала.

При $j_{K,0,N-1} \neq N-1$ рассматриваемая комбинация сбоев возможна, если одновременно:

- $j_{0,t} \neq z_{0,0\ldots t-1}(j_{K,0,N-1}), z_{0,0\ldots t-1}(N-1)$ (сбои типов 1a и 1c соответственно);
- $s_{0,t}^{-1}(\gamma_{0,t}) \neq z_{0,0\ldots t-1}(j_{K,0,N-1}), z_{0,0\ldots t-1}(N-1)$ (сбои типов 2a и 2c соответственно);
- Выполняется одно из условий:
  - $\delta_{1b} \neq \delta_{2b}$ (в работе пары g_0 и $g_{\delta_{1b}}$ произошел сбой типа 1b, пары g_0 и $g_{\delta_{1b}}$ – 2b), при этом $d_{0,\delta_{1b}} > t$ и $d_{0,\delta_{2b}} \leq t$ (пара g_0 и $g_{\delta_{2b}}$ разошлась, g_0 и $g_{\delta_{1b}}$ - нет);
  - $\delta_{1b} = \delta_{2b}$, при этом $d_{0,\delta_{1b}} > t$.

При $j_{K,0,N-1} = N-1$ данный случай возможен, если выполняются все следующие условия:

- $j_{0,t} \neq z_{0,0\ldots t-1}(N-1)$ (сбой типа 1c);
- $s_{0,t}^{-1}(\gamma_{0,t}) \neq z_{0,0\ldots t-1}(N-1)$ (сбой типа 2c);
- Выполняется одно из условий:
  - $\delta_{1b} \neq \delta_{2b}$, при этом $d_{0,\delta_{1b}} > t$ и $d_{0,\delta_{2b}} \leq t$;
  - $\delta_{1b} = \delta_{2b}$, при этом $d_{0,\delta_{1b}} > t$.

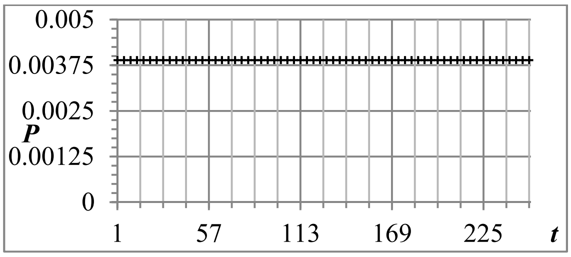

Рис. 1. Вероятность $P_{1a,t}$

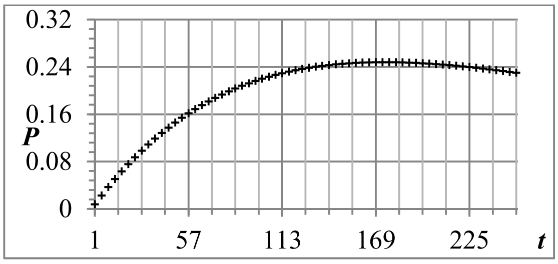

Рис. 2. Вероятность $P_{1b,t}$

Соответственно, вероятность рассматриваемого случая равна:

$$P_{1b,t} = P(j_{K,0,N-1} \neq N-1) \cdot P\left(j_{0,t} \neq z_{0,0\ldots t-1}(j_{K,0,N-1}), z_{0,0\ldots t-1}(N-1)\right) \cdot P\left(s_{0,t}^{-1}(\gamma_{0,t}) \neq z_{0,0\ldots t-1}(j_{K,0,N-1}), z_{0,0\ldots t-1}(N-1)\right) \cdot \left(P(\delta_{1b} \neq \delta_{2b}) \cdot P(d_{0,\delta_{1b}} > t | \delta_{1b} \neq \delta_{2b}) \cdot P(d0,_{\delta_{2b}} \leq t | \delta_{1b} \neq \delta_{2b}) + P(\delta_{1b} = \delta_{2b}) \cdot P(d_{\delta 0,_{1b}} > t | \delta_{1b} = \delta_{2b})\right) + P(j_{K,0,N-1} = N-1) \cdot P\left(j_{0,t} \neq z_{0,0\ldots t-1}(N-1)\right) \cdot P\left(s_{0,t}^{-1}(\gamma_{0,t}) \neq z_{0,0\ldots t-1}(N-1)\right) \cdot \left(P(\delta_{1b} \neq \delta_{2b}) \cdot P(d_{0,\delta_{1b}} > t | \delta_{1b} \neq \delta_{2b}) \cdot P(d_{0,\delta_{2b}} \leq t | \delta_{1b} \neq \delta_{2b}) + P(\delta_{1b} = \delta_{2b}) \cdot P(d_{0,\delta_{1b}} > t | \delta_{1b} = \delta_{2b})\right) = \frac{N-1}{N} \cdot \frac{N-2}{N} \cdot \frac{N-2}{N} \cdot \left(\frac{N-3}{N-2} \cdot \frac{N-Y_t-2}{N-2} \cdot \frac{Y_t}{N-3} + \frac{1}{N-2} \cdot \frac{N-Y_t-2}{N-2}\right) + \frac{1}{N} \cdot \frac{N-1}{N} \cdot \frac{N-1}{N} \cdot \left(\frac{N-2}{N-1} \cdot \frac{N-Y_t-1}{N-1} \cdot \frac{Y_t}{N-2} + \frac{1}{N-1} \cdot \frac{N-Y_t-1}{N-1}\right)$$

$$P_{1b,t} = \frac{(Y_t+1) \cdot (N^2 - N \cdot Y_t - 2 \cdot N + 1)}{N^3}$$

График зависимости $P_{1b,t}$ от момента времени t для генератора RC4(8) приведен на Рис. 2.

Подсчитаем вероятность того, что в момент t среди всех пар g_0 и g_δ, для которых верно $t < d_{0,\delta}$, происходит сбой типа 1с (предполагается, что $t < d_{\text{общ}}$). Пусть $j_{K,0,N-1}$ и $j_{0,t}$, случайные величины, распределенные равномерно на $[0; N-1]$.

И при $j_{K,0,N-1} \neq N-1$, и при $j_{K,0,N-1} = N-1$ данный случай возможен, если $j_{0,t} = z_{0,0\ldots t-1}(N-1)$. Соответственно, вероятность рассматриваемого случая равна:

$$P_{1c,t} = P(j_{K,0,N-1} \neq N-1) \cdot P(j_{0,t} = z_{0,0\ldots t-1}(N-1) | j_{K,0,N-1} \neq N-1) + P(j_{K,0,N-1} = N-1) \cdot P(j_{0,t} = z_{0,0\ldots t-1}(N-1) | j_{K,0,N-1} = N-1) = \frac{N-1}{N} \cdot \frac{1}{N} + \frac{1}{N} \cdot \frac{1}{N}$$

$$P_{1c,t} = \frac{1}{N}$$

График зависимости $P_{1c,t}$ от момента времени t для генератора RC4(8) приведен на Рис. 3.

Подсчитаем вероятность того, что в момент t в работе всех пар g_0 и g_δ, удовлетворяющих $t < d_{0,\delta}$, происходит сбой типа 2а (предполагается, что $t < d_{\text{общ}}$). Пусть $j_{K,0,N-1}$, $j_{0,t}$, $s_{0,t}^{-1}(\gamma_{0,t})$ случайные величины, распределенные равномерно на $[0; N-1]$, а δ_{1b} - на $[1; N-1]$.

При $j_{K,0,N-1} \neq N-1$ данный случай возможен, если выполняются все следующие условия:

- $j_{0,t} \neq z_{0,0\ldots t-1}(j_{K,0,N-1}), z_{0,0\ldots t-1}(N-1)$ (сбои типов 1а и 1с соответственно);
- $s_{0,t}^{-1}(\gamma_{0,t}) = z_{0,0\ldots t-1}(j_{K,0,N-1})$;
- $d_{0,\delta_{1b}} \leq t$.

При $j_{K,0,N-1} = N-1$ данный случай невозможен.

Соответственно, вероятность рассматриваемого случая равна:

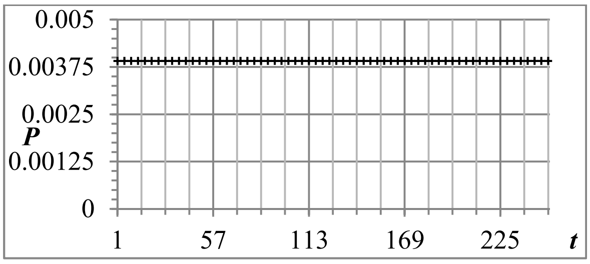

Рис. 3. Вероятность $P_{1c,t}$

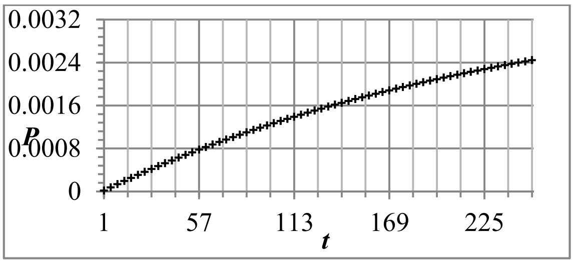

Рис. 4. Вероятность $P_{2a,t}$

$$P_{2a,t} = P(j_{K,0,N-1} \neq N-1) \cdot P\left(j_{0,t} \neq z_{0,0\dots t-1}(j_{K,0,N-1}), z_{0,0\dots t-1}(N-1)\right) \cdot P\left(s_{0,t}^{-1}(\gamma_{0,t}) = z_{0,0\dots t-1}(j_{K,0,N-1})\right) \cdot P(d_{0,\delta_{1b}} \leq t) = \frac{N-1}{N} \cdot \frac{N-2}{N} \cdot \frac{1}{N} \cdot \frac{Y_t}{N-2}$$

$$P_{2a,t} = \frac{Y_t \cdot (N-1)}{N^3}$$

График зависимости $P_{2a,t}$ от момента времени t для генератора RC4(8) приведен на Рис. 4.

Подсчитаем вероятность того, что в момент времени t среди всех пар g_0 и g_δ, для которых верно $t < d_{0,\delta}$, только в одной паре происходит только сбой типа 2b (предполагается, что $t < d_{общ}$). Пусть $j_{K,0,N-1}$, $j_{0,t}$, $s_{0,t}^{-1}(\gamma_{0,t})$ случайные величины, распределенные равномерно на $[0; N-1]$, а δ_{1b} и δ_{2b} - на $[1; N-1]$.

При $j_{K,0,N-1} \neq N-1$ данный случай возможен, если выполняются все следующие условия:

– $j_{0,t} \neq z_{0,0\dots t-1}(j_{K,0,N-1}), z_{0,0\dots t-1}(N-1)$ (сбои типов 1a и 1c соответственно);

– $s_{0,t}^{-1}(\gamma_{0,t}) \neq z_{0,0\dots t-1}(j_{K,0,N-1}), z_{0,0\dots t-1}(N-1)$ (сбои типов 2a и 2c соответственно);

– $\delta_{1b} \neq \delta_{2b}$, при этом $d_{0,\delta_{1b}} \leq t$ и $d_{0,\delta_{2b}} > t$ (пара g_0 и $g_{\delta_{1b}}$ разошлась, g_0 и $g_{\delta_{2b}}$ - нет).

При $j_{K,0,N-1} = N-1$ данный случай возможен, если выполняются все следующие условия:

– $j_{0,t} \neq z_{0,0\dots t-1}(N-1)$ (сбой типа 1c);

– $s_{0,t}^{-1}(\gamma_{0,t}) \neq z_{0,0\dots t-1}(N-1)$ (сбой типа 2c);

– $\delta_{1b} \neq \delta_{2b}$, при этом $d_{0,\delta_{1b}} \leq t$ и $d_{0,\delta_{2b}} > t$

Соответственно, вероятность рассматриваемого случая равна:

$$P_{2b,t} = P(j_{K,0,N-1} \neq N-1) \cdot P\left(j_{0,t} \neq z_{0,0\dots t-1}(j_{K,0,N-1}), z_{0,0\dots t-1}(N-1)\right) \cdot P\left(s_{0,t}^{-1}(\gamma_{0,t}) \neq z_{0,0\dots t-1}(j_{K,0,N-1}), z_{0,0\dots t-1}(N-1)\right) \cdot P(\delta_{1b} \neq \delta_{2b}) \cdot P(d_{0,\delta_{1b}} \leq t | \delta_{1b} \neq \delta_{2b}) \cdot P(d_{0,\delta_{2b}} > t | \delta_{1b} \neq \delta_{2b}) + P(j_{K,0,N-1} = N-1) \cdot P\left(j_{0,t} \neq z_{0,0\dots t-1}(N-1)\right) \cdot P\left(s_{0,t}^{-1}(\gamma_{0,t}) \neq z_{0,0\dots t-1}(N-1)\right) \cdot\cdot P(\delta_{1b} \neq \delta_{2b}) \cdot P(d_{0,\delta_{1b}} \leq t | \delta_{1b} \neq \delta_{2b}) \cdot P(d_{0,\delta_{2b}} > t | \delta_{1b} \neq \delta_{2b}) = \frac{N-1}{N} \cdot \frac{N-2}{N} \cdot \frac{N-2}{N} \cdot \frac{N-3}{N-2} \cdot \frac{Y_t}{N-2} \cdot \frac{N-Y_t-2}{N-3} + \frac{1}{N} \cdot \frac{N-1}{N} \cdot \frac{N-1}{N} \cdot \frac{N-2}{N-1} \cdot \frac{Y_t}{N-1} \cdot \frac{N-Y_t-1}{N-2}$$

$$P_{2b,t} = \frac{Y_t \cdot (N^2 - N \cdot Y_t - 2 \cdot N + 1)}{N^3}$$

График зависимости $P_{2b,t}$ от момента времени t для генератора RC4(8) приведен на Рис. 5.

Подсчитаем вероятность того, что в момент времени t в работе всех пар g_0 и g_δ, удовлетворяющих $t < d_{0,\delta}$, кроме одной происходит сбой типа 2a и в работе одной – 1b (предполагается, что $t < d_{общ}$). Пусть $j_{K,0,N-1}$, $j_{0,t}$, $s_{0,t}^{-1}(\gamma_{0,t})$ случайные величины, распределенные равномерно на $[0; N-1]$, а δ_{1b} - на $[1; N-1]$.

При $j_{K,0,N-1} \neq N-1$ данный случай возможен, если выполняются все следующие условия:

– $j_{0,t} \neq z_{0,0\ldots t-1}(j_{K,0,N-1}), z_{0,0\ldots t-1}(N-1)$ (сбои типов 1a и 1c соответственно);
– $s_{0,t}^{-1}(\gamma_{0,t}) = z_{0,0\ldots t-1}(j_{K,0,N-1})$;
– $d_{0,\delta_{1b}} > t$.

При $j_{K,0,N-1} = N-1$ данный случай невозможен.

Соответственно, вероятность рассматриваемого случая равна:

$$\mathrm{P}_{1b,2a,t} = \mathrm{P}(\mathrm{j}_{K,0,N-1} \neq \mathrm{N}-1) \cdot \mathrm{P}\left(\mathrm{j}_{0,t} \neq \mathrm{z}_{0,0\ldots t-1}(\mathrm{j}_{K,0,N-1}), \mathrm{z}_{0,0\ldots t-1}(\mathrm{N}-1)\right) \cdot \mathrm{P}\left(\mathrm{s}_{0,t}^{-1}(\gamma_{0,t}) = \mathrm{z}_{0,0\ldots t-1}(\mathrm{j}_{K,0,N-1})\right) \cdot \mathrm{P}(\mathrm{d}_{0,\delta_{1b}} > \mathrm{t}) = \frac{\mathrm{N}-1}{\mathrm{N}} \cdot \frac{\mathrm{N}-2}{\mathrm{N}} \cdot \frac{1}{\mathrm{N}} \cdot \frac{\mathrm{N}-\mathrm{Y}_t-2}{\mathrm{N}-2}$$

$$\mathrm{P}_{1b,2a,t} = \frac{(\mathrm{N}-\mathrm{Y}_t-2)\cdot(\mathrm{N}-1)}{\mathrm{N}^3}$$

График зависимости $P_{1b,2a,t}$ от момента времени t для RC4(8) приведен на Рис. 6.

Подсчитаем вероятность того, что в момент времени t среди всех пар g_0 и g_δ, для которых $t < d_{0,\delta}$, в одной паре происходит только сбой типа 1b и в работе другой пары – сбой 2b (предполагается, что $t < d_{\text{общ}}$). Пусть $j_{K,0,N-1}$, $j_{0,t}$, $s_{0,t}^{-1}(\gamma_{0,t})$ случайные величины, распределенные равномерно на $[0; N-1]$, а δ_{1b} и δ_{2b} - на $[1; N-1]$.

При $j_{K,0,N-1} \neq N-1$ данный случай возможен, если выполняются все следующие условия:
– $j_{0,t} \neq z_{0,0\ldots t-1}(j_{K,0,N-1}), z_{0,0\ldots t-1}(N-1)$;
– $s_{0,t}^{-1}(\gamma_{0,t}) \neq z_{0,0\ldots t-1}(j_{K,0,N-1}), z_{0,0\ldots t-1}(N-1)$;
– $\delta_{1b} \neq \delta_{2b}$, при этом $d_{0,\delta_{1b}} > t$ и $d_{0,\delta_{2b}} > t$.

При $j_{K,0,N-1} = N-1$ данный случай возможен, если выполняются все следующие условия:
– $j_{0,t} \neq z_{0,0\ldots t-1}(N-1)$;
– $s_{0,t}^{-1}(\gamma_{0,t}) \neq z_{0,0\ldots t-1}(N-1)$;
– $\delta_{1b} \neq \delta_{2b}$, при этом $d_{0\delta_{1b}} > t$ и $d_{0,\delta_{2b}} > t$.

Соответственно, вероятность рассматриваемого случая равна:

$$\mathrm{P}_{1b,2b,t} = \mathrm{P}(\mathrm{j}_{K,0,N-1} \neq \mathrm{N}-1) \cdot \mathrm{P}\left(\mathrm{j}_{0,t} \neq \mathrm{z}_{0,0\ldots t-1}(\mathrm{j}_{K,0,N-1}), \mathrm{z}_{0,0\ldots t-1}(\mathrm{N}-1)\right) \cdot \mathrm{P}\left(\mathrm{s}_{0,t}^{-1}(\gamma_{0,t}) \neq \mathrm{z}_{0,0\ldots t-1}(\mathrm{j}_{K,0,N-1}), \mathrm{z}_{0,0\ldots t-1}(\mathrm{N}-1)\right) \cdot \mathrm{P}(\delta_{1b} \neq \delta_{2b}) \cdot \mathrm{P}(\mathrm{d}_{0,\delta_{1b}} > \mathrm{t} | \delta_{1b} \neq \delta_{2b}) \cdot \mathrm{P}(\mathrm{d}_{0,\delta_{2b}} > \mathrm{t} | \delta_{1b} \neq \delta_{2b}) + \mathrm{P}(\mathrm{j}_{K,0,N-1} = \mathrm{N}-1) \cdot \mathrm{P}\left(\mathrm{j}_{0,t} \neq \mathrm{z}_{0,0\ldots t-1}(\mathrm{N}-1)\right) \cdot \mathrm{P}\left(\mathrm{s}_{0,t}^{-1}(\gamma_{0,t}) \neq \mathrm{z}_{0,0\ldots t-1}(\mathrm{N}-1)\right) \cdot \mathrm{P}(\delta_{1b} \neq \delta_{2b}) \cdot \mathrm{P}(\mathrm{d}_{0,\delta_{1b}} > \mathrm{t} | \delta_{1b} \neq \delta_{2b}) \cdot \mathrm{P}(\mathrm{d}_{0,\delta_{2b}} > \mathrm{t} | \delta_{1b} \neq \delta_{2b}) = \frac{\mathrm{N}-1}{\mathrm{N}} \cdot \frac{\mathrm{N}-2}{\mathrm{N}} \cdot \frac{\mathrm{N}-2}{\mathrm{N}} \cdot \frac{\mathrm{N}-3}{\mathrm{N}-2} \cdot \frac{\mathrm{N}-\mathrm{Y}_t-2}{\mathrm{N}-2} \cdot \frac{\mathrm{N}-\mathrm{Y}_t-3}{\mathrm{N}-3} + \frac{1}{\mathrm{N}} \cdot \frac{\mathrm{N}-1}{\mathrm{N}} \cdot \frac{\mathrm{N}-1}{\mathrm{N}} \cdot \frac{\mathrm{N}-2}{\mathrm{N}-1} \cdot \frac{\mathrm{N}-\mathrm{Y}_t-1}{\mathrm{N}-1} \cdot \frac{\mathrm{N}-\mathrm{Y}_t-2}{\mathrm{N}-2}$$

$$\mathrm{P}_{1b,2b,t} = \frac{(\mathrm{N}-\mathrm{Y}_t-2)\cdot(\mathrm{N}^2-\mathrm{N}\cdot\mathrm{Y}_t-3\cdot\mathrm{N}+2)}{\mathrm{N}^3}$$

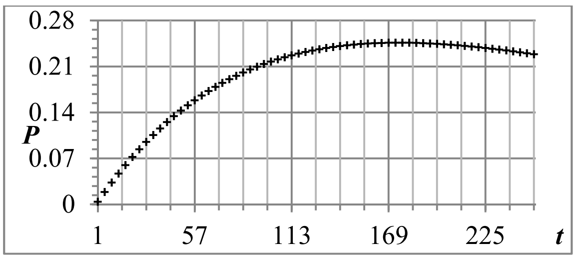

Рис. 5. Вероятность $\mathrm{P}_{2b,t}$

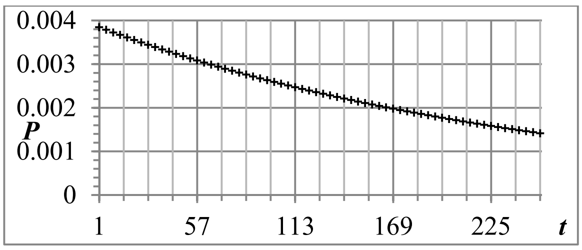

Рис. 6. Вероятность $\mathrm{P}_{1b,2a,t}$

График зависимости $P_{1b,2b,t}$ от момента времени t для RC4(8) приведен на Рис. 7.

Подсчитаем вероятность того, что при t в работе всех пар g_0 и g_δ, для которых верно $t < d_{0,\delta}$, происходит сбой типа 2c (предполагается, что $t < d_{\text{общ}}$). Пусть $j_{K,0,N-1}$, $j_{0,t}$, $s_{0,t}^{-1}(\gamma_{0,t})$ случайные величины, распределенные равномерно на $[0; N-1]$, а δ_{1b} и δ_{2b} - на $[1; N-1]$.

При $j_{K,0,N-1} \neq N-1$ данный случай возможен, если выполняются все следующие условия:

– $j_{0,t} \neq z_{0,0\ldots t-1}(j_{K,0,N-1}), z_{0,0\ldots t-1}(N-1)$ (сбои типов 1a и 1c соответственно);

– $s_{0,t}^{-1}(\gamma_{0,t}) = z_{0,0\ldots t-1}(\mathrm{N}-1)$;

– $d_{0,\delta_{1b}} \leq t$.

При $j_{K,0,N-1} = N-1$ данный случай возможен, если выполняются все следующие условия:

– $j_{0,t} \neq z_{0,0\ldots t-1}(N-1)$ (сбой типа 1c);

– $s_{0,t}^{-1}(\gamma_{0,t}) = z_{0,0\ldots t-1}(\mathrm{N}-1)$;

– $d_{0,\delta_{1b}} \leq t$.

Соответственно, вероятность рассматриваемого случая равна:

$$\mathrm{P}_{2c,t} = \mathrm{P}(\mathrm{j}_{K,0,N-1} \neq \mathrm{N}-1) \cdot \mathrm{P}\left(\mathrm{j}_{0,t} \neq \mathrm{z}_{0,0\ldots t-1}(\mathrm{j}_{K,0,N-1}), \mathrm{z}_{0,0\ldots t-1}(\mathrm{N}-1)\right) \cdot \mathrm{P}\left(\mathrm{s}_{0,t}^{-1}(\gamma_{0,t}) = \mathrm{z}_{0,0\ldots t-1}(\mathrm{N}-1)\right) \cdot \mathrm{P}(\mathrm{d}_{0,\delta_{1b}} \leq \mathrm{t}) + \mathrm{P}(\mathrm{j}_{K,0,N-1} = \mathrm{N}-1) \cdot \mathrm{P}\left(\mathrm{j}_{0,t} \neq \mathrm{z}_{0,0\ldots t-1}(\mathrm{N}-1)\right) \cdot \mathrm{P}\left(\mathrm{s}_{0,t}^{-1}(\gamma_{0,t}) = \mathrm{z}_{0,0\ldots t-1}(\mathrm{N}-1)\right) \cdot \mathrm{P}(\mathrm{d}_{0,\delta_{1b}} \leq \mathrm{t}) = \frac{\mathrm{N}-1}{\mathrm{N}} \cdot \frac{\mathrm{N}-2}{\mathrm{N}} \cdot \frac{1}{\mathrm{N}} \cdot \frac{\mathrm{Y_t}}{\mathrm{N}-2} + \frac{1}{\mathrm{N}} \cdot \frac{\mathrm{N}-1}{\mathrm{N}} \cdot \frac{1}{\mathrm{N}} \cdot \frac{\mathrm{Y_t}}{\mathrm{N}-1}$$

$$\mathrm{P}_{2c,t} = \frac{\mathrm{Y_t}}{\mathrm{N}^2}$$

График зависимости $P_{1c,t}$ от момента времени t для генератора RC4(8) приведен на Рис. 8.

Подсчитаем вероятность того, что в момент времени t для всех пар g_0 и g_δ, щих $t < d_{0,\delta}$, кроме одной происходит сбой типа 2c и для одной – 1b (предполагается, что $t < d_{\text{общ}}$). Пусть $j_{K,0,N-1}$, $j_{0,t}$, $s_{0,t}^{-1}(\gamma_{0,t})$ случайные величины, распределенные равномерно на $[0; N-1]$, а δ_{1b} - на $[1; N-1]$.

При $j_{K,0,N-1} \neq N-1$ данный случай возможен, если выполняются все следующие условия:

– $j_{0,t} \neq z_{0,0\ldots t-1}(j_{K,0,N-1}), z_{0,0\ldots t-1}(N-1)$;

– $s_{0,t}^{-1}(\gamma_{0,t}) = z_{0,0\ldots t-1}(\mathrm{N}-1)$;

– $d_{0,\delta_{1b}} > t$.

При $j_{K,0,N-1} = N-1$ данный случай возможен, если выполняются все следующие условия:

– $j_{0,t} \neq z_{0,0\ldots t-1}(N-1)$;

– $s_{0,t}^{-1}(\gamma_{0,t}) = z_{0,0\ldots t-1}(\mathrm{N}-1)$;

– $d_{0,\delta_{1b}} > t$.

Соответственно, вероятность рассматриваемого случая равна:

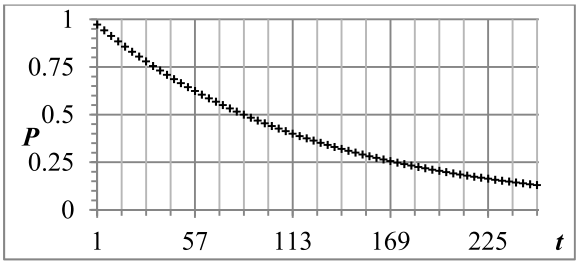

Рис. 7. Вероятность $\mathrm{P}_{1b,2b,t}$

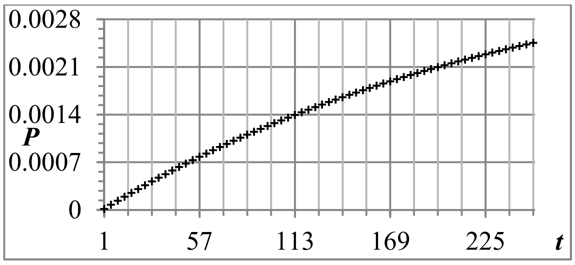

Рис. 8. Вероятность $\mathrm{P}_{1c,t}$

$$\mathrm{P}_{1b,2c,t} = \mathrm{P}(\mathrm{j}_{K,0,N-1} \neq N-1) \cdot \mathrm{P}\left(\mathrm{j}_{0,t} \neq \mathrm{z}_{0,0\ldots t-1}(\mathrm{j}_{K,0,N-1}), \mathrm{z}_{0,0\ldots t-1}(N-1)\right) \cdot \mathrm{P}\left(\mathrm{s}_{0,t}^{-1}(\gamma_{0,t}) = \mathrm{z}_{0,0\ldots t-1}(N-1)\right) \cdot \mathrm{P}(\mathrm{d}_{0\delta_{1b}} > t) + \mathrm{P}(\mathrm{j}_{K,0,N-1} = N-1) \cdot \mathrm{P}\left(\mathrm{j}_{0,t} \neq \mathrm{z}_{0,0\ldots t-1}(N-1)\right) \cdot \mathrm{P}\left(\mathrm{s}_{0,t}^{-1}(\gamma_{0,t}) = \mathrm{z}_{0,0\ldots t-1}(N-1)\right) \cdot \mathrm{P}(\mathrm{d}_{0,\delta_{1b}} > t) = \frac{N-1}{N} \cdot \frac{N-2}{N} \cdot \frac{1}{N} \cdot \frac{N-Y_t-2}{N-2} + \frac{1}{N} \cdot \frac{N-1}{N} \cdot \frac{1}{N} \cdot \frac{N-Y_t-1}{N-1}$$

$$\mathrm{P}_{1b,2c,t} = \frac{N \cdot (N-Y_t-2)+1}{N^3}$$

График зависимости $P_{1b,2c,t}$ от момента времени t для RC4(8) приведен на Рис. 9.

Подсчитаем вероятность того, что в момент времени t среди всех пар g_0 и g_δ, не происходит сбоев (предполагается, что $t < d_{общ}$). Пусть $j_{K,0,N-1}$, $j_{0,t}$, $s_{0,t}^{-1}(\gamma_{0,t})$ случайные величины, распределенные равномерно на $[0; N-1]$, а δ_{1b} и δ_{2b} - на $[1; N-1]$.

При $j_{K,0,N-1} \neq N-1$ данный случай возможен, если выполняются все следующие условия:

– $j_{0,t} \neq z_{0,0\ldots t-1}(j_{K,0,N-1}), z_{0,0\ldots t-1}(N-1)$;
– $s_{0,t}^{-1}(\gamma_{0,t}) \neq z_{0,0\ldots t-1}(j_{K,0,N-1}), z_{0,0\ldots t-1}(N-1)$;
– Выполняется одно из условий:
  - o $\delta_{1b} \neq \delta_{2b}$, при этом $d_{0,\delta_{1b}} \leq t$ и $d_{0,\delta_{2b}} \leq t$;
  - o $\delta_{1b} = \delta_{2b}$, при этом $d_{0,\delta_{1b}} \leq t$.

При $j_{K,0,N-1} = N-1$ данный случай возможен, если выполняются все следующие условия:

– $j_{0,t} \neq z_{0,0\ldots t-1}(N-1)$;
– $s_{0,t}^{-1}(\gamma_{0,t}) \neq z_{0,0\ldots t-1}(N-1)$;
– Выполняется одно из условий:
  - o $\delta_{1b} \neq \delta_{2b}$, при этом $d_{0,\delta_{1b}} \leq t$ и $d_{0,\delta_{2b}} \leq t$;
  - o $\delta_{1b} = \delta_{2b}$, при этом $d_{0,\delta_{1b}} \leq t$.

Соответственно, вероятность рассматриваемого случая равна:

$$\mathrm{P}_{none,t} = \mathrm{P}(\mathrm{j}_{K,0,N-1} \neq N-1) \cdot \mathrm{P}\left(\mathrm{j}_{0,t} \neq \mathrm{z}_{0,0\ldots t-1}(\mathrm{j}_{K,0,N-1}), \mathrm{z}_{0,0\ldots t-1}(N-1)\right) \cdot \mathrm{P}\left(\mathrm{s}_{0,t}^{-1}(\gamma_{0,t}) \neq \mathrm{z}_{0,0\ldots t-1}(\mathrm{j}_{K,0,N-1}), \mathrm{z}_{0,0\ldots t-1}(N-1)\right) \cdot \left(\mathrm{P}(\delta_{1b} \neq \delta_{2b}) \cdot \mathrm{P}(\mathrm{d}0,_{\delta_{1b}} \leq t | \delta_{1b} \neq \delta_{2b}) \cdot \mathrm{P}(\mathrm{d}_{0,\delta_{2b}} \leq t | \delta_{1b} \neq \delta_{2b}) + \mathrm{P}(\delta_{1b} = \delta_{2b}) \cdot \mathrm{P}(\mathrm{d}0,_{\delta_{1b}} \leq t | \delta_{1b} = \delta_{2b})\right) + \mathrm{P}(\mathrm{j}_{K,0,N-1} = N-1) \cdot \mathrm{P}\left(\mathrm{j}_{0,t} \neq \mathrm{z}_{0,0\ldots t-1}(N-1)\right) \cdot \mathrm{P}\left(\mathrm{s}_{0,t}^{-1}(\gamma_{0,t}) \neq \mathrm{z}_{0,0\ldots t-1}(N-1)\right) \cdot \left(\mathrm{P}(\delta_{1b} \neq \delta_{2b}) \cdot \mathrm{P}(\mathrm{d}_{0,\delta_{1b}} \leq t | \delta_{1b} \neq \delta_{2b}) \cdot \mathrm{P}(\mathrm{d}_{0,\delta_{2b}} \leq t | \delta_{1b} \neq \delta_{2b}) + \mathrm{P}(\delta_{1b} = \delta_{2b}) \cdot \mathrm{P}(\mathrm{d}0,_{\delta_{1b}} \leq t | \delta_{1b} = \delta_{2b})\right) = \frac{N-1}{N} \cdot \frac{N-2}{N} \cdot \frac{N-2}{N} \cdot \left(\frac{N-3}{N-2} \cdot \frac{Y_t}{N-2} \cdot \frac{Y_t-1}{N-3} + \frac{1}{N-2} \cdot \frac{Y_t}{N-2}\right) + \frac{1}{N} \cdot \frac{N-1}{N} \cdot \frac{N-1}{N} \cdot \left(\frac{N-2}{N-1} \cdot \frac{Y_t}{N-1} \cdot \frac{Y_t-1}{N-2} + \frac{1}{N-1} \cdot \frac{Y_t}{N-1}\right)$$

$$\mathrm{P}_{none,t} = \frac{Y_t^2}{N^2}$$

График зависимости $P_{none,t}$ от момента времени t для RC4(8) приведен на Рис. 10.

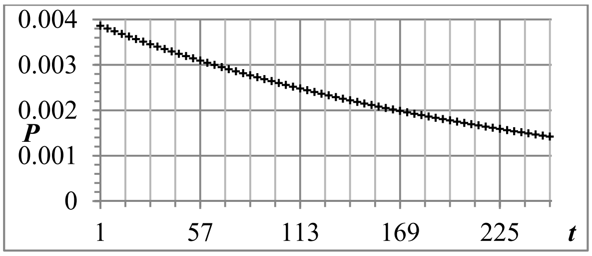

Рис. 9. Вероятность $P_{1b,2c,t}$

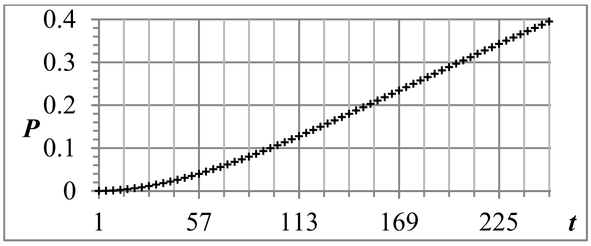

Рис. 10. Вероятность $P_{none,t}$

Заключение

Среди опубликованных ранее работ по теме анализа влияния связанных ключей на функционирование RC4 вне протоколов WEP и WPA вопрос влияния связанных ключей на работу PRGA рассматривался только в [2]. Однако авторы данного исследования сосредоточили свое внимание на различиях в выходных последовательностях генераторов RC4, инициализированных связанными ключами, и оценках количества совпадающих выходных символов. Основные отличия настоящей работы от [2] заключаются в следующем:

– рассмотрено влияние связанных ключей на работу семейства связанных генераторов RC4(M), а не только версии RC4(8);

– уточнены причины появления сбоев, показано, что сбои, описанные в [2], это сбои 1 рода в терминологии настоящей статьи, показано существование неявных сбоев, не приводящих к выработке различных значений связанными генераторами, описан более общий класс сбоев в работе связанных генераторов RC4, включающий в себя сбои, описанные в [2], выполнена классификация сбоев на основе причин их появления;

– рассмотрены наборы из N пар связанных генераторов RC4, выявлены все возможные комбинации сбоев, вычислены вероятности появления каждой из таких комбинаций в работе N пар связанных генераторов в зависимости от момента времени t (в [2] рассматривались только одиночные пары).

Как было показано выше, сбои в работе связанных ГПСЧ RC4 могут быть классифицированы на явные и неявные. Явные сбои, в свою очередь, подразделяются на 1 и 2 рода и типы 1a, 1b, 1c, 2a, 2b и 2c. В каждый момент времени $t \leq N - 2 < d_{\text{общ}}$ в работе $N - 1$ пары связанных генераторов g_0 и g_δ ($\delta \in [1; N - 1]$) возможно возникновение одной и только одной из 10 комбинаций перечисленных типов сбоев. Вычислены вероятности возникновения каждой из возможных комбинаций сбоев в каждый из моментов времени t до общего расхождения всех N связанных генераторов RC4.

Выявленные особенности функционирования связанных генераторов RC4 и вычисленные вероятности комбинаций сбоев будут в дальнейшем использованы автором настоящей статьи для решения задачи вычисления внутренних состояний связанных генераторов по сбоям в их работе.

Литература

1. Kelsey J., Schneier B. Wagner D. Key-Schedule Cryptanalysis of 3-WAY, IDEA, G-DES, RC4, SAFER, and Triple-DES // Lecture Notes in Computer Science. – 1996. – Т. 1109. – С. 237-251. – ISBN 978-3-540-68697-2
2. Grosul A. L., Wallach D. S. «A Related-Key Cryptanalysis of RC4». Rice University, 2000 [В Интернете.. URL: http://cohesion.rice.edu/engineering/computerscience/tr/TR_Download.cfm?SDID=126. [Дата обращения: 24.08.2014.
3. Fluhrer S., Mantin I., Shamir A. Weaknesses in the Key Scheduling Algorithm of RC4 // Lecture Notes in Computer Science. – 2001. – Т. 2259. – С. 1-24. – ISBN 978-3-540-45537-0
4. Mantin I. A Practical Attack on the Fixed RC4 in the WEP Mode // Lecture Notes in Computer Science. – 2005. – Т. 3788. – С. 395-411. – ISBN 978-3-540-32267-2
5. Klein A. Attacks on the RC4 stream cipher // Designs, Codes and Cryptography. – 2008. – Т. 48. – № 43. – С. 269-286. – ISSN 1573-7586
6. Vaudenay S., Vuagnoux M. Passive–only Key Recovery Attacks on RC4 // Lecture Notes in Computer Science. – 2007. – Т. 4876. – С. 344-359. – ISBN 978-3-540-77360-3
7. Tews E., Weinmann R.-P., Pyshkin A. Breaking 104 Bit WEP in Less Than 60 Seconds // Lecture Notes in Computer Science. – 2007. – Т. 4867. – С. 188-202. – ISBN 978-3-540-77535-5
8. Beck M., Tews E. Practical attacks against WEP and WPA // Proceeding WiSec '09 Proceedings of the second ACM conference on Wireless network security. – 2009. – С. 79-86. – ISBN 978-1-60558-460-7
9. Sepehrdad P., Vaudenay S., Vuagnoux M. Statistical attack on RC4 distinguishing WPA // Lecture Notes in Computer Science. – 2011. – Т. 6632. – С. 343-363. – ISBN 978-3-642-20465-4
10. Matsui M. Key Collisions of the RC4 Stream // Lecture Notes in Computer Science. – 2009. – Т. 5665. – С. 38-50. – ISBN 978-3-642-03317-9
11. Chen J., Miyaji A. A New Class of RC4 Colliding Key Pairs With Greater Hamming Distance // Lecture Notes in Computer Science. – 2010. – Т. 6047. – С. 30-44. – ISBN 978-3-642-12827-1

12. Chen J., Miyaji A. Generalized RC4 Key Collisions and Hash Collisions // Lecture Notes in Computer Science. – 2010. – Т. 6280. – С. 73-87. – ISBN 978-3-642-15317-4
13. Chen J., Miyaji A. Generalized Analysis on Key Collisions of Stream Cipher RC4 // IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences. – 2010. – Т. E94-A. – № 11. – С. 2194-2206. – ISSN 1745-1337
14. Chen J., Miyaji A. How to Find Short RC4 Colliding Key Pairs // Lecture Notes in Computer Science. – 2011. – Т. 7001. – С. 32-46. – ISBN 978-3-642-24861-0
15. Chen J., Miyaji A. Novel strategies for searching RC4 key collisions // Computers & Mathematics with Applications. – 2013. – Т. 66. – № 1. – С. 81–90. – ISSN 0898-1221
16. Chen J., Miyaji A. A New Practical Key Recovery Attack on the Stream Cipher RC4 under Related-Key Model // Lecture Notes in Computer Science. – 2011. – Т. 6584. – С. 62-76. – ISBN 978-3-642-21518-6
17. Chen J., Miyaji A. Cryptanalysis of Stream Ciphers from a New Aspect: How to Apply Key Collisions to Key Recovery Attack // IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Science. – 2012. – Т. E95-A. – № 12. – С. 2148-2159. – ISSN 1745-1337.

Кудияров Дмитрий Сергеевич. Аспирант. Российский государственный социальный университет.
E-mail: dmitry.kudiyarov@gmail.com