А.А.Варфоломеев, М.А.Пудовкина

Исследование алгоритма поточного шифрования Solitaire .

Введение.

Алгоритм поточного шифрования "Solitaire"(" Пасьянс") предложен B. Schneier в 1999 г в [1]. Согласно замыслу автора он предназначен для применения в качестве ручного шифра. Алгоритм представляет собой синхронную поточную систему и относится к классу псевдопростых генераторов, соответствующих режиму обратной связи по выходу (Output Feedback –OFB). Ключ определяет только начальное состояние генератора .

В предлагаемой работе произведено обобщение данной криптосхемы и начато ее исследование, а именно исследовалась цикловая структура. В ходе изучения криптосхемы Solitaire была доказана нерегулярность функции перехода, полностью описаны необратимые состояния и получен еще целый ряд утверждений.

Проведено исследование изменения цикловой структуры при перестановке четырех преобразований, используемых в функции перехода криптосхемы Solitaire, друг относительно друга. Получена, классификация по 6 классам эквивалентных перестановок, имеющих одинаковую цикловую структуру.

1 Описание алгоритма поточного шифрования Solitaire .

Ниже приводится перевод описания криптосхемы Solitaire предложной B. Schneier в [1] .

Каждую букву английского алфавита заменяем числом от 0 до 25.

Solitaire генерирует ключевую последовательность, используя колоду карт состоящую из 52 карт и двух джокеров. Колода карт рассматривается, как перестановка из 54 элементов. Назовем один джокер A, другой джокер B.

Ниже приводится алгоритм генерации ключевой последовательность криптосхемы Solitaire, состоящий из 5 шагов. Он выполняется для каждой буквы открытого текста.

Алгоритм генерации ключевой последовательности.

1. В колоде карт находим джокер A. Его перемещаем на одну карту вниз. Если он является последней картой колоды, тогда джокер A перемещаем за первую карту.
2. В колоде карт находим джокер B. Его перемещаем на две карты вниз. Если джокер B является последней картой колоды, тогда перемещаем его за вторую карту. Если джокер B является предпоследней картой колоды, тогда его перемещаем за первую карту.
3. Переставляем карты, находящиеся до первого джокера слева, с картами расположенными за вторым джокером. Карты расположенные между джокерами A , B и сами джокеры не переставляются
4. Преобразуем последнюю карту колоды в число от 1 до 53. Для этого используется порядок расположения карт для игры в бридж: “трефы”, “бубны”, “черви” и “пики”. Если карта “трефы”, тогда ее значение не

меняется. Если карта “бубны”, тогда к ее значению прибавляется 13. Если карта “черви”, тогда к ее значению прибавляется 26. Если карта “пики”, тогда к ее значению прибавляется 39.

Пусть значение последней карты равно *p*. Тогда переставляем первые *p* карт со следующими 53- *p* картами. Последняя карта не переставляется.

5. Определяем элемент ключевой последовательности. Для этого преобразуем первую карту в число, как это было сделано в шаге 4, и находим карту с этим номером. Если найденная карта является джокером, тогда переходим к шагу 1 и выполняем все шаги снова. Если найденная карта не является джокером, тогда преобразуем ее в число, как было сделано в шаге 4. Для полученного числа определяем его остаток при деление на 26. Полученный остаток и будет являться элементом ключевой последовательности.

Ключ.

Ключом является порядок начального расположение карт. Он либо генерируется случайным образом отправителем и передается получателю, либо используется ключевая фраза, позволяющий получить начальное расположение карт в колоде. Ключевое фраза согласуется отправителем и получателем шифрованного сообщения.

Алгоритм генерации начального состояния по ключевой фразе следующий. Первоначально карты колоды располагаются в порядке для игры в бридж. Предпоследней картой колоды является джокер A , а последней картой колоды - джокер B.

Для каждой элемента ключевой фразы выполняем шаги 1,2,3, 4′ алгоритма генерации ключевой последовательности. Шаг 4′, описывается ниже.

4′. Пусть значение элемента ключевой фразы равно *p*. Тогда переставляем первые *p* карт со следующими 54- *p* картами.

Шифрование

Пусть M= m_1..... m_N - открытый текст и C=c_1..... c_N –шифртекст сообщения M.

В каждый такт работы алгоритма выполняется:

Уравнение зашифрования:

$$c_i = m_i + k_i \pmod{26},\ i=1\ldots\ldots N$$

Уравнение расшифрования:

$$m_i = c_i - k_i \pmod{26},\ i=1\ldots\ldots N$$

2 Описание математической модели криптосхемы Solitaire.

Ниже предлагается описание математической модели криптосхемы Solitaire в общем случае.

Пусть алфавиты открытого текста и шифртекста совпадают и их мощности равна m. Каждую букву алфавита заменяем числом от 0 до m-1.

Рассматриваем перестановку S из n элементов, являющуюся состоянием криптосхемы .

Будем через S_i обозначать состояние криптосхемы на i такте ее работы.

Элемент перестановки Si, находящийся на j месте будем обозначать через si[j], где j=0..n-1 . Элементы перестановки S с номерами n-2 и n-1 назовем джокерами и будем обозначать их A и B соответственно.

В описание криптосхемы Solitaire, приведенным в параграфе 1, используются следующие числовые значения m =26 и n=54.

Генерация ключевого потока.

Работа криптосистемы описывается следующими соотношениями:

$$S_{i+1}=\boldsymbol{F}(S_i)$$

$$к_i=\boldsymbol{f}(S_{i+1}),\ i=1,2,\ldots..,$$

F –функция переходов состояний.

f -функция выхода.

Ниже приводятся описания функция переходов состояний ***F*** и функция выхода ***f***.

Функция переходов состояний *F*

Функция перехода ***F*** представима в виде композиции четырех преобразований ***F***= $F_4 F_3 F_2 F_1$, которые будут описаны ниже. Преобразования F_4, F_3, F_2, F_1 выполняют перестановку элементов состояния S=s[0]… s[n-1].

1. Функция F_1 выполняет следующее преобразование:
   Пусть j номер джокера A в перестановке S: s[j]=A. Если j≠ n-1, тогда джокер A переставляется через 1 элемент вправо: s[j]=s[j+1] , s[j+1]=A.
   Если j=n-1 джокер A ставится на место элемента s[1].

2. Функция F_2 выполняет следующее преобразование:
   Пусть j номер джокера B в перестановке S: s[j]=B. Если j≠ n-1 и n-2 , тогда джокер B переставляется через 2 элемент вправо: s[j]=s[j+1] , s[j+1]=s[j+2], s[j+2]=B. Если j=n-1 или n-2 джокер B ставится на место элементов s[1] или s[2] соответственно.

3. Функция F_3 выполняет следующее преобразование:
   Переставляется элементы, находящиеся до первого джокера слева, с элементами расположенными за вторым джокером.
   Пусть $s[к_0]$=A и $s[к_1]$=B, тогда если $к_0 < к_1$ переставляются элементы с номерами s[0]…$s[к_0-1]$ с элементами $s[к_1+1]$…s[n-1] . Если $к_0 > к_1$ переставляются элементы s[0]…$s[к_1-1]$ с элементами $s[к_0+1]$…s[n-1] . Элементы расположенные между джокерами A и B не переставляются

4. Функция F_4 выполняет следующее преобразование:
   Пусть s[n-1]=k. Переставляются элементы s[0],…,s[k] с элементами s[k+1],…,s[n-2] . Элемент s[n-1] не переставляется.

Функция выхода *f*

Рассмотрим состояние $S_{i+1}= \boldsymbol{F}(S_i)$.

Пусть $s_{i+1}[0]$=k.

a) Если $s_{i+1}[k]$ является джокером, выходного элемента нет.

b) Если $s_{i+1}[k]$ не является джокером, тогда элемент ключевой последовательности: $\boldsymbol{к_{i+1}= s_{i+1}[k] \pmod m = s_{i+1}[s_{i+1}[0]] \pmod m}$.

Ключ.

Как и было описано в параграфе 1 ключом является порядок начального расположение элементов перестановки. Он либо генерируется случайным образом отправителем и передается получателю, либо используется ключевая фраза, позволяющий получить начальную перестановку.

Ниже приводится описание алгоритм генерации начального состояния по ключевой фразе для рассматриваемой математической модели криптосхемы Solitaire.

Алгоритм генерации начального состояния.

Пусть $\boldsymbol{K}=к_0 \ldots к_{h-1}$ ключевая фраза длины h.
В начальный момент состоянием является тождественная перестановка:
$S_0=\{0,1,\ldots, n-1\}$, s[j]=j.
Для каждой буквы ключевой фразы выполняется функция перехода
$\boldsymbol{F'}= F'_4 F_3 F_2 F_1$. Состояние на i такте равно $S_i=(\boldsymbol{F'})^i(S_0)$
Функция перехода $\boldsymbol{F'}$ отличается от описанной выше функции перехода $\boldsymbol{F}$ изменением преобразования F_4. Ниже приводится описание преобразования F'_4.

4′. Функция F'_4 выполняет следующее преобразование:
Переставляются элементы s[0],…,s[$к_j$] с элементами s[$к_j$ +1],…,s[n-1] .

Шифрование

Пусть M= $m_1 \ldots\ldots\ldots m_N$ - открытый текст и C=$c_1 \ldots\ldots c_N$ –шифртекст сообщения M.
В каждый такт работы алгоритма выполняется:
Уравнение зашифрования:

$$c_i=m_i + k_i \pmod m,\ i=1\ldots\ldots N$$

Уравнение расшифрования:

$$m_i=c_i - k_i \pmod m,\ i=1\ldots\ldots N$$

3 Цикловая структура функции перехода.

Для наглядности на рис.1, рис.2, рис.3 и рис.4 приводится цикловая структура функции перехода $\boldsymbol{F}$ для значений n=4 и 5. Для n=4 цикловая структура функции перехода $\boldsymbol{F}$ состоит из одного цикла длины 8, n=5 она состоит из трех циклов длины 13, 17 и 22.

Полученные результаты показывают нерегулярность функции перехода $\boldsymbol{F}$. Благодаря анализу наблюдаемых связей, удалось доказать не регулярность этого отображения для произвольных значений параметра n.

Было получено, что не регулярность функции перехода $\boldsymbol{F}$ возникла в силу необратимости преобразований F_1 и F_2, и как следствие этого композиции преобразований $F_2 F_1$. Для каждого из преобразований F_1, F_2 и F_2F_1 удалось выписать все необратимые элементы. Это позволило описать концевые вершины графа переходных состояний функции перехода $\boldsymbol{F}$. Их число ровно $2\cdot(n-1)!-(n-2)!$.

Утверждение 1 посвящено описанию необратимых элементов преобразований F_2, F_1 и $(F_2 F_1)$ соответственно и как следствие, это доказывает не регулярность данных преобразований.

Утверждение1.

1. Отображение F_2 не имеет прообраза для элементов вида B s[1]… s[n-1] .
2. Отображение F_1 не имеет прообраза для элементов вида A s[1]… s[n-1].
3. Отображение $(F_2 F_1)$ не имеет прообраза для элементов вида F_2(A s[1]… s[n-2] C), где C≠B и B s[1]… s[n-1].

#

Действительно. Если элемент B s[1]… s[n-1] имеет прообраз, тогда джокер B в прообразе F_2^{-1}(B s[1]… s[n-1]) должен находиться на последних местах.
Поскольку F_2: s[0]…s[n-4] B C_1 C_2 -> s[0]…s[n-4] C_1 C_2 B и
F_2: C_1 s’[1]…s’[n-3] B C_2-> C_1 B s’[1]…s’[n-3] C_2 и

F_2: C_1 C_2 s[2]…s[n-2] B -> C_1 C_2 B s[2]…s[n-2], то ввиду конструкции отображения F_2, элемент B s[1]… s[n-1] невозможен.
Таким же образом доказываются пункты 2 и 3.

#

Утверждение 2.
Число концевых вершин в графе переходных состояний равно: 2·(n-1)!-(n-2)!.
#
Согласно утверждениям 1-3.
Число элементов вида B s[1]… s[n-1] равно (n-1)!.
Число элементов вида A s[1]… s[n-2]C, где C≠B равно (n-1)!-(n-2)!.
Поскольку концевые вершины, являются необратимыми элементами отображения F= F_4 F_3 F_2 F_1, тогда их число в графе переходных состояний равно: 2·(n-1)!-(n-2)!.

#

Утверждение 3.
Степени вершин графа переходных состояний не превышают 3.
#
Если степень вершины больше 2, тогда имеет место соотношение:
F_1(A C s[2]… s[n-1])= F_1(C s[2]… s[n-1] A) = C A s[2]… s[n-1] .
Если степень вершины равна 4, тогда должны выполнятся соотношения:
C A s[2]… s[n-1]= B C_1 C_2 s_1[3]… s_1[n-1] (1) и
C A s[2]… s[n-1]= C_1 C_2 s_1[3]… s_1[n-1] B (2).
Тогда из соотношения (1) следует B=C, A= C_1 и s[2]… s[n-1]= C_2 s_1[3]… s_1[n-1].
Из соотношения (2) получаем C_1=C, A=C_2 и s[2]… s[n-1]= s_1[3]… s_1[n-1] B.
Одновременно эти равенства выполнятся не могут. Следовательно степени вершин графа переходных состояний не превышают 3.

#

Были рассмотрены множества состояний, которые получаются после применения преобразований F_1, F_2 F_1, F_3 F_2 F_1 и F_4 F_3 F_2 F_1 к множеству всевозможных начальных состояний S_n. Для них была описана их структура и определена мощность каждого из рассматриваемых множеств. Полученные результаты приводятся в теореме 1.

Теорема 1 .
Пусть V_i –множество всевозможных состояний, таких что: V_0=S_n,
F_1: V_0 -> V_1 ,
F_2: V_1 -> V_2 ,
F_3: V_2 -> V_3 ,
F_4: V_3 -> V_4 .
Тогда мощности данных множеств удовлетворяют соотношениям:
$|V_0| = |S_n| = n!$, $|V_1| = n!-(n-1)!$, $|V_2| = |V_3| = |V_4| = n!-2\cdot(n-1)! +(n-2)!$.
#
Поскольку отображение F_1 не регулярно, элементы C s[1]… s[n-1] A и A C s[2]… s[n-1] имеют одинаковый образ. Число пар элементов, имеющих одинаковый образ равно (n-1)!. Следовательно мощность $|V_1| = n!-(n-1)!$.
Поскольку элемент A s[1]… s[n-1] не имеет прообраза относительно отображения F_1, тогда A s[1]… s[n-1]$\notin$ V_1.
Поскольку элемент B s[1]… s[n-1] не имеет прообраза относительно отображения F_2, тогда B s[1]… s[n-1]$\notin$ V_2. Таких элементов (n-1)!. Однако для элементов A B s[2]… s[n-1] выполняется F_1: A B s[2]… s[n-1] -> B A s[2]… s[n-1] . Но элементы вида A B s[2]… s[n-1]$\notin$ V_1 и число таких элементов

(n -2)!.
Следовательно мощность $|V_2| = |V_1| - ((n-1)! - (n-2)!) = n! - 2\cdot(n-1)! + (n-2)!$.
В силу регулярности отображений F_4 и F_3 имеем:
$|V_2| = |V_3| = |V_4| = n! - 2\cdot(n-1)! + (n-2)!$.

#

Следствие 1.1.
Элементы вида:
1) B s[1]… s[n-1] $\notin V_2$
2) A C_1 C_2 s[3]… s[n-1] $\notin V_2$, где $C_2 \neq B$.

Следствие 2.1.
Элементы вида:
1) s_1[0]… s[$к_1$] B s[$к_1$+2]… s[n-2] A $\notin V_3$ и
2) s_1[0]… s[$к_1$] A C_1 C_2 s[$к_1$+5]… s[n-2] B $\notin V_3$.

Замечание.
Элементы вида s[0]… s[n-4] A C_1 B $\in V_3$.
#
Поскольку в силу утверждения 6 элемент A C_1 B s[0]… s[n-4]$\in V_2$.
Тогда F_3 : A C_1 B S-> S A C_1 B $\in$ V_3.

#

Преобразование F_4 обладает интересным свойством, которым не обладают преобразования F_1, F_2 , F_3. Данное свойство заключается в наличие у преобразования F_4 группы инерции. В приводимом ниже утверждение 4 описаны элементы группы инерции и сосчитан ее порядок.

Утверждение 4.
Пусть H-множество элементов, таких что H$\subset V_3$ и F_4(H)=H.
Тогда мощность множества $|H| = (n-2)!$.
#
Поскольку отображение F_4 не изменяет элементы, оканчивающиеся на джокер.
Тогда если элементы вида A S_2 B $S_1 \in V_2$ и B S_2 A $S_1 \in V_2$ тогда:
F_3 : A S_2 B S_1-> S_1 A S_2 B $\in$H .
F_3 : B S_2 A S_1-> S_1 B S_2 A $\in$H.
Но в силу следствия 2 и замечания 1, только элементы вида
s[0]… s[n-4] A C_1 B $\in V_3$. Таких элементов (n -2)!. Следовательно мощность множества $|H| = (n-2)!$.

#

Была предпринята попытка определить множество элементов, являющихся цикловыми. Основываясь на том, что определены все необратимые элементы и они заведомо не являются цикловыми, в утверждение 5, приводимом ниже, явно выписано некоторое множество не цикловых элементов. Данное утверждение являются следствиям утверждения 1, но в силу получившихся запретов на ряд состояний в цикловой структуре, оно представляет самостоятельный интерес .

Утверждение 5.
Пусть состоянием криптосхемы S является перестановки следующих видов:
1) S =A s[1] s[2]... s[n-2] B
2) S = s[0]s[1] s[2]... s[n-3] A B
3) S = s[0]...s[p-1] B s[p+1]… s[n-2] A .
4) S = s[0]...s[p-1] A s[p+1]… s[n-2] B и s[n-3]$\neq$A.
Тогда не существует состояние $(F)^{-1}(S)$.

Следствие 5.1.
Циклу не принадлежат состояния, оканчивающиеся на джокер A.
Следствие 5.2.
Если циклу принадлежит состояние, оканчивающиеся на джокер B, тогда выполнена связь:

$$A\ B\ s[n-2]\ s[0]...s[n-4] \rightarrow s[0]\ldots\ s[n-4]\ A\ s[n-2]\ B.$$

В приводимом ниже утверждение 6 описан ряд эквивалентных состояний.
Утверждение 6.
Состояния S =A B s[2] s[3]...s[n-1] и S1=A s1[1] s1[2]...s1[n-2] B являются эквивалентными, где s[i+1]= s1[i] i=1… n-2.
#
F_1(A B s[2] s[3]...s[n-1])= A s[2] B s[3]...s[n-1].
F_1(A s1[1] s1[2]...s1[n-2] B)= A s1[1] B s1[2]...s1[n-2].
Следовательно $F_1(S)= F_1(S1)$ и состояния S, S1 эквивалентны.
#

В графе функции переходных состояний значительную долю занимают концевые точки, длина подхода к циклу которых равна 1. Ниже приводится утверждение, характеризующие данные точки.
Утверждение 7.
Если состояние S=A B s[2] s[3]...s[n-1] принадлежит циклу, то состояние S1=A s1[1] s1[2]...s1[n-2] B, где s[i+1]= s1[i] i=1… n-2, принадлежит подходу к циклу длины 1 и кроме того F(S)= F(S1).
#
Согласно утверждению 6 состояние A s1[1] s1[2]...s1[n-2] B необратимо и выполняется F(S)= F(S1). Следовательно состояние A s1[1] s1[2]...s1[n-2] B принадлежит подходу к циклу длины 1. #

Следствие 7.1.
Согласно утверждению 7 и следствию 5.2, если циклу принадлежит состояние, оканчивающиеся на джокер B, тогда принадлежит состояние, начинающиеся на джокер A.
Обозначим через N(i,s) –сколько раз в состояниях, принадлежащих циклу, на i месте перестановки встречается символ s.
Тогда имеет место неравенство: $N(0,A) \geq N(n-1,B)$.

4 Перестановка базовых преобразований в функции перехода.

Удалось доказать, что возможно 6 классов эквивалентных перестановок, имеющих сходную цикловую структуру. Элементы одного класса характеризуются циклическим сдвигом преобразований F_1, F_3, F_2, F_4.

Функции преобразований, принадлежащие разным классам эквивалентности, имеют различную структуру необратимых элементов. Причем необратимые элементы возникают в результате не регулярности преобразований F_1, F_2. Ниже в утверждении 1 описана структура необратимых элементов для каждого класса эквивалентности.

Полученные в результате числового эксперимента цикловые структуры для каждого эквивалентного класса отличаются структурой циклов. Данное различие связано с разной структурой необратимых элементов.

Утверждение.

1. Множество необратимых элементов преобразования $F_2=F_4 F_2 F_3 F_1$ следующее: F_4 (B s[0]… …. s[n-1]). Число не обратимых элементов равно (n-1)!.
2. Необратимые элементы преобразования $F_3=F_3 F_2 F_4 F_1$ имеют следующие конструкции:
   a) F_3 (B s[0]… …. s[n-1]) .
   b) $F_3 F_2 F_4$ (A s[0]… …. s[n-1]), если к= s[n-1] и s[к+1]≠ B .
   Число не обратимых элементов равно 2·(n-1)!- (n-2)!.
3. Необратимые элементы преобразования $F_5= F_1 F_2 F_4 F_3$ имеют следующие конструкции:
   a) $F_4 F_3$ (A s[0]… …. s[n-1]) .
   b) $F_4F_3 F_1$ (B s[0]… …. s[n-1]), если s[n-1]≠ A .
   Число не обратимых элементов равно 2·(n-1)!- (n-2)!.
4. Необратимые элементы преобразования $F_6= F_3 F_4 F_1 F_2$ имеют следующие конструкции:
   a) $F_3 F_4$ (A s[0]… …. s[n-1]) .
   b) $F_3F_4 F_1$ (B s[0]… …. s[n-1]), если s[n-1]≠ A .
   Число не обратимых элементов равно 2·(n-1)!- (n-2)!.

#

Доказательство каждого из этих пунктов является сходными и основаны на анализе не обратимых элементов преобразований F_1, F_2. В качестве типового доказательства, оно приводится для пункта 3.

1) Состояние $S_1= F_4 F_3$ (A s[0]… …. s[n-1]) является необратимым, так как элемент A s[1]… …. s[n-1] необратим относительно преобразования F_1.
2) Необратимые элементы также могут поражаться элементами вида: $S_2=$ B c[1]… …. c[n-1]. Они являются необратимыми относительно преобразования F_2.

Докажем, что в данном случае состояния $S_3= F_4F_3 F_1$ (B s[1]… …. s[n-1]), если s[n-1]≠ A являются обратимыми.
Действительно.
F_1 (B s[1]…s[n-2] A)= B A s[1]…s[n-2]
$(F_1)^{-1}$(B A s[1]…s[n-2])= A B s[1]…s[n-2]
Следовательно ∃ $(F_2)^{-1}$(A B s[1]…s[n-2])= A s[1]… s[n-3]B s[n-2]

#

Замечание 1
Необратимые элементы преобразования $F_1=F_4 F_3 F_2 F_1$ описано в параграфе 3.

Замечание 2

Поскольку преобразование $F_4=F_3 F_4 F_2 F_1$ отличается от преобразования $F_1=F_4 F_3 F_2 F_1$ только перестановкой регулярных преобразований F_4, F_3 и не регулярным является общее преобразование $F_2 F_1$, то для отображения F_4 сохраняются ранее доказанные для преобразования F_1 свойства нерегулярных элементов.

Теорема.
При перестановки преобразований F_2, F_1, F_4, F_3 относительно друг друга, они разбиваются на 6 эквивалентных классов перестановок, имеющих сходную

цикловую структуру. Эти классы строятся на основе циклического сдвига преобразований.

Эквивалентные классы следующие:

1) $\boldsymbol{\Phi_1}$={ $F_1 F_2 F_3 F_4$, $F_4 F_1 F_2 F_3$, $F_3 F_4 F_1 F_2$, $F_2 F_3 F_4 F_1$ }
2) $\boldsymbol{\Phi_2}$={ $F_2 F_1 F_3 F_4$, $F_4 F_2 F_1 F_3$, $F_3 F_4 F_2 F_1$, $F_1 F_3 F_4 F_2$ }
3) $\boldsymbol{\Phi_3}$={ $F_1 F_2 F_4 F_3$, $F_3 F_1 F_2 F_4$, $F_4 F_3 F_1 F_2$, $F_2 F_4 F_3 F_1$ }
4) $\boldsymbol{\Phi_4}$={ $F_2 F_1 F_4 F_3$, $F_3 F_2 F_1 F_4$, $F_4 F_3 F_2 F_1$, $F_1 F_4 F_3 F_2$ }
5) $\boldsymbol{\Phi_5}$={ $F_1 F_4 F_2 F_3$, $F_3 F_1 F_4 F_2$, $F_4 F_2 F_3 F_1$, $F_2 F_3 F_1 F_4$ }
6) $\boldsymbol{\Phi_6}$={ $F_1 F_3 F_2 F_4$, $F_4 F_1 F_3 F_2$, $F_3 F_2 F_4 F_1$, $F_2 F_4 F_1 F_3$ }

#

Обозначим через $\boldsymbol{\Phi}$={$\Phi_4 \Phi_3 \Phi_2 \Phi_1$, $\Phi_1 \Phi_4 \Phi_3 \Phi_2$, $\Phi_2 \Phi_1 \Phi_4 \Phi_3$, $\Phi_3 \Phi_2 \Phi_1 \Phi_4$ } один из эквивалентных классов 1-6 $\boldsymbol{\Phi} \in \{ \boldsymbol{\Phi_1}, \boldsymbol{\Phi_2}, \boldsymbol{\Phi_3}, \boldsymbol{\Phi_4}, \boldsymbol{\Phi_5}, \boldsymbol{\Phi_6}\}$.

Рассмотрим непрерывную последовательность: $\Phi_4 \Phi_3 \Phi_2 \Phi_1 \Phi_4 \Phi_3 \Phi_2 \Phi_1 \Phi_3 \Phi_3 \Phi_2 \Phi_1$..... $\Phi_4 \Phi_3 \Phi_2 \Phi_1 \Phi_4 \Phi_3 \Phi_2 \Phi_1$ .....

Каждое из преобразований класса получается простым сдвигом.

Пусть $\boldsymbol{T_1}=\Phi_4 \Phi_3 \Phi_2 \Phi_1$, $\boldsymbol{T_2}= \Phi_1 \Phi_4 \Phi_3 \Phi_2$, $\boldsymbol{T_3}= \Phi_2 \Phi_1 \Phi_4 \Phi_3$, $\boldsymbol{T_4}=\Phi_3 \Phi_2 \Phi_1 \Phi_4$.

Тогда имеют место следующие соотношения:

$(\boldsymbol{T_2})^{\kappa} = \Phi_1 (\boldsymbol{T_1})^{\kappa} (\Phi_1)^{-1}$, $(\boldsymbol{T_3})^{\kappa} = \Phi_2\Phi_1 (\boldsymbol{T_1})^{\kappa}(\Phi_2\Phi_1)^{-1}$, $(\boldsymbol{T_4})^{\kappa} = \Phi_3\Phi_2\Phi_1 (\boldsymbol{T_1})^{\kappa} (\Phi_3\Phi_2\Phi_1)^{-1}$,

или $(\boldsymbol{T_1})^{\kappa} = \Phi_4 (\boldsymbol{T_4})^{\kappa} (\Phi_4)^{-1}$

Они задают отображения одного преобразования в другое.

#

5 Заключение.

В данной статье были приведены результаты, полученные при исследование цикловой структуры функции перехода криптосистемы Solitaire.

Полученные в результате исследования результаты позволяют утверждать, что нерегулярность функции перехода $\boldsymbol{F}$ ослабляет криптографические свойства криптосистемы Solitaire.

Выбор последовательности применения этапов F_4, F_3, F_2, F_1 не является оптимальным. При другой последовательности их выборов цикловая структура может быть лучше, чем при выбранной последовательности.

Возможно незначительно изменить этапы преобразования $\boldsymbol{F}$, чтобы оно стало регулярным. При этом происходит изменение цикловой структуры в сторону ее улучшения.

Представляет интерес исследовать поведение джокеров на этапах преобразования $\boldsymbol{F}$. Также в дальнейшем произвести исследование алгоритма генерации начального состояния с помощью ключевой фразы.

Литература.

1. Bruce Schineier, “ The Solitaire Encryption Algorithm ”, http://www.counterpane.com/solitaire.html.
2. Konheim A. G. “ Cryptography, a Primier ” , J Wiley& Sons N.Y,1981
3. Rueppel R.A. “Analisis and Design of Stream Ciphers”.
4. Bruce Schineier, Applied Cryptography. Second edition,1996.

Рис. 1
Цикловая структура графа переходных состояний с n= 4.

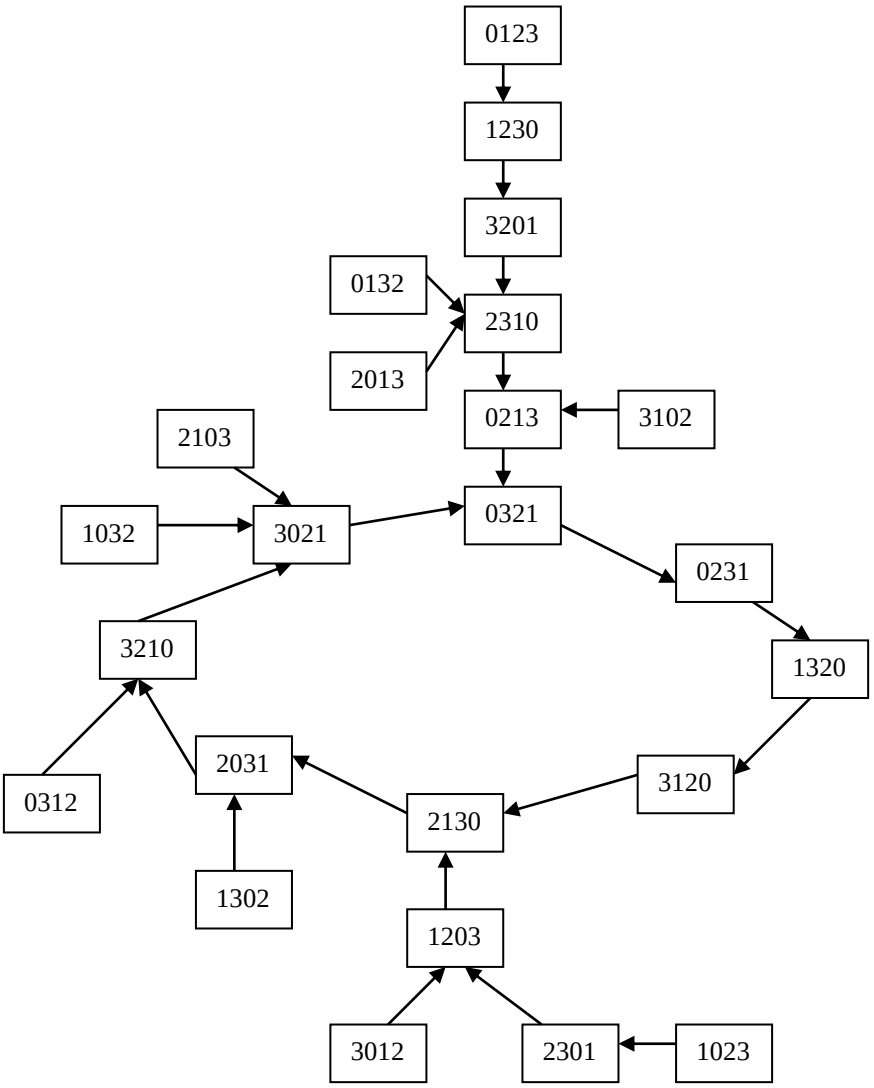

Рис. 2

Цикловая структура графа переходных состояний с n= 5. Цикл 1.

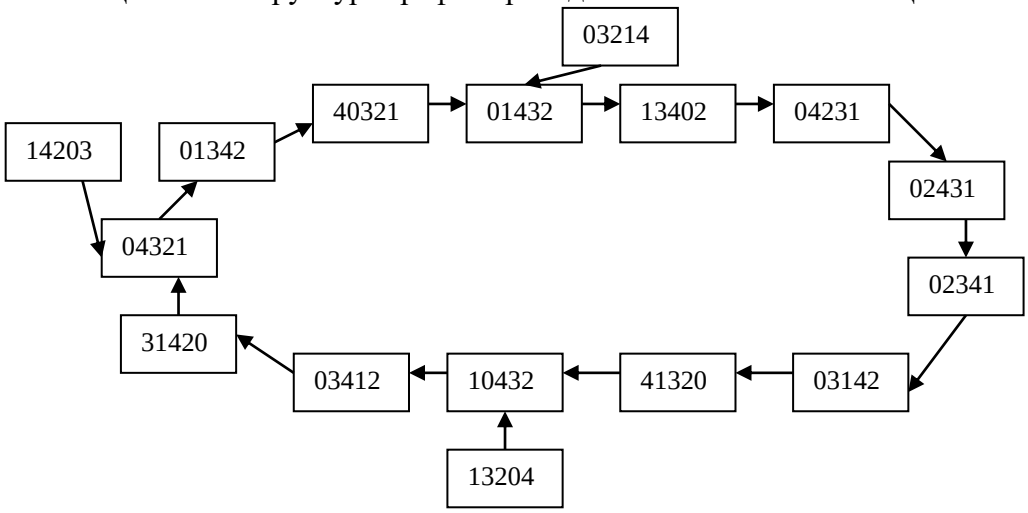

Рис. 3
Цикловая структура графа переходных состояний с n= 5. Цикл 2.

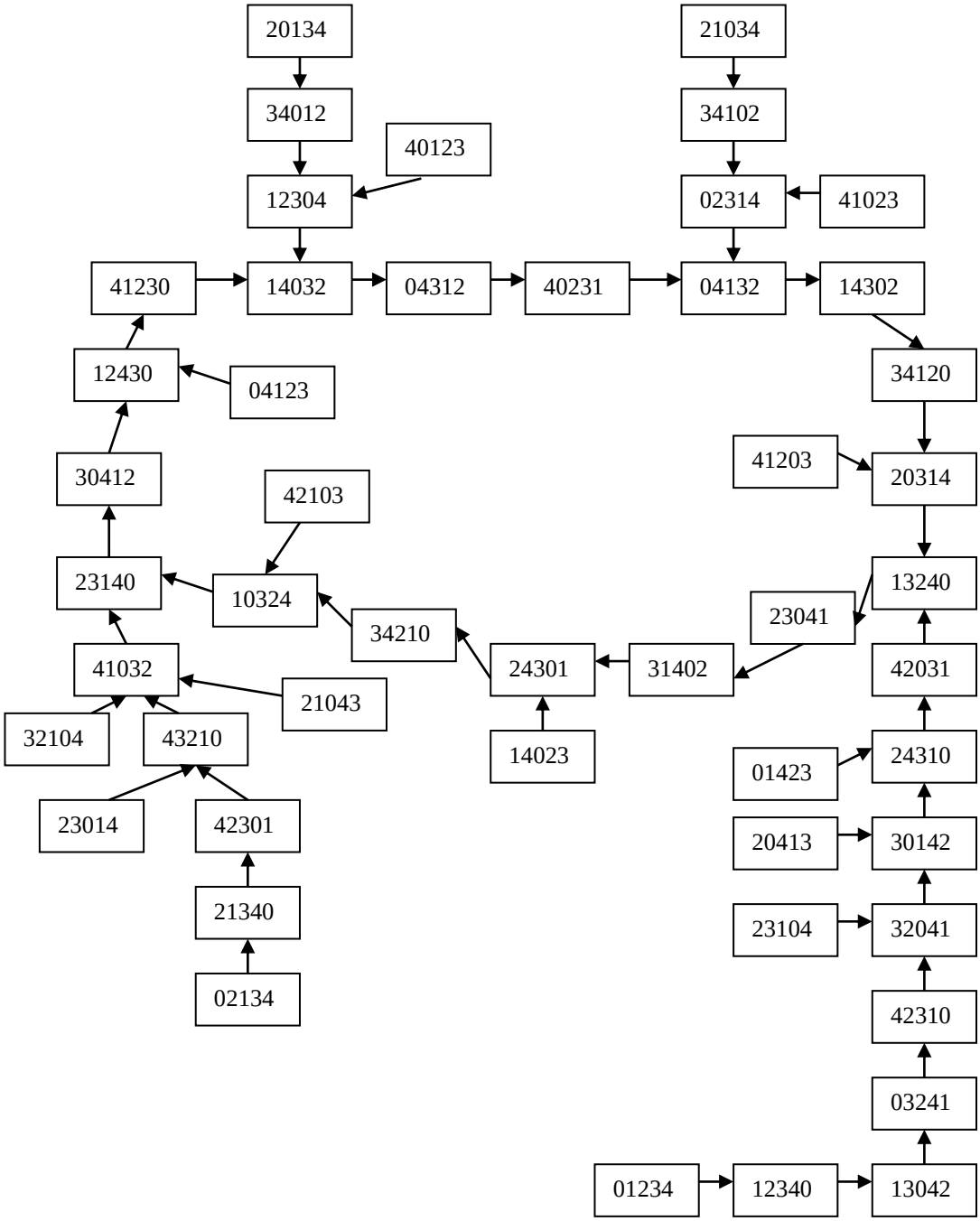

Рис. 4

Цикловая структура графа переходных состояний с n= 5. Цикл 3.

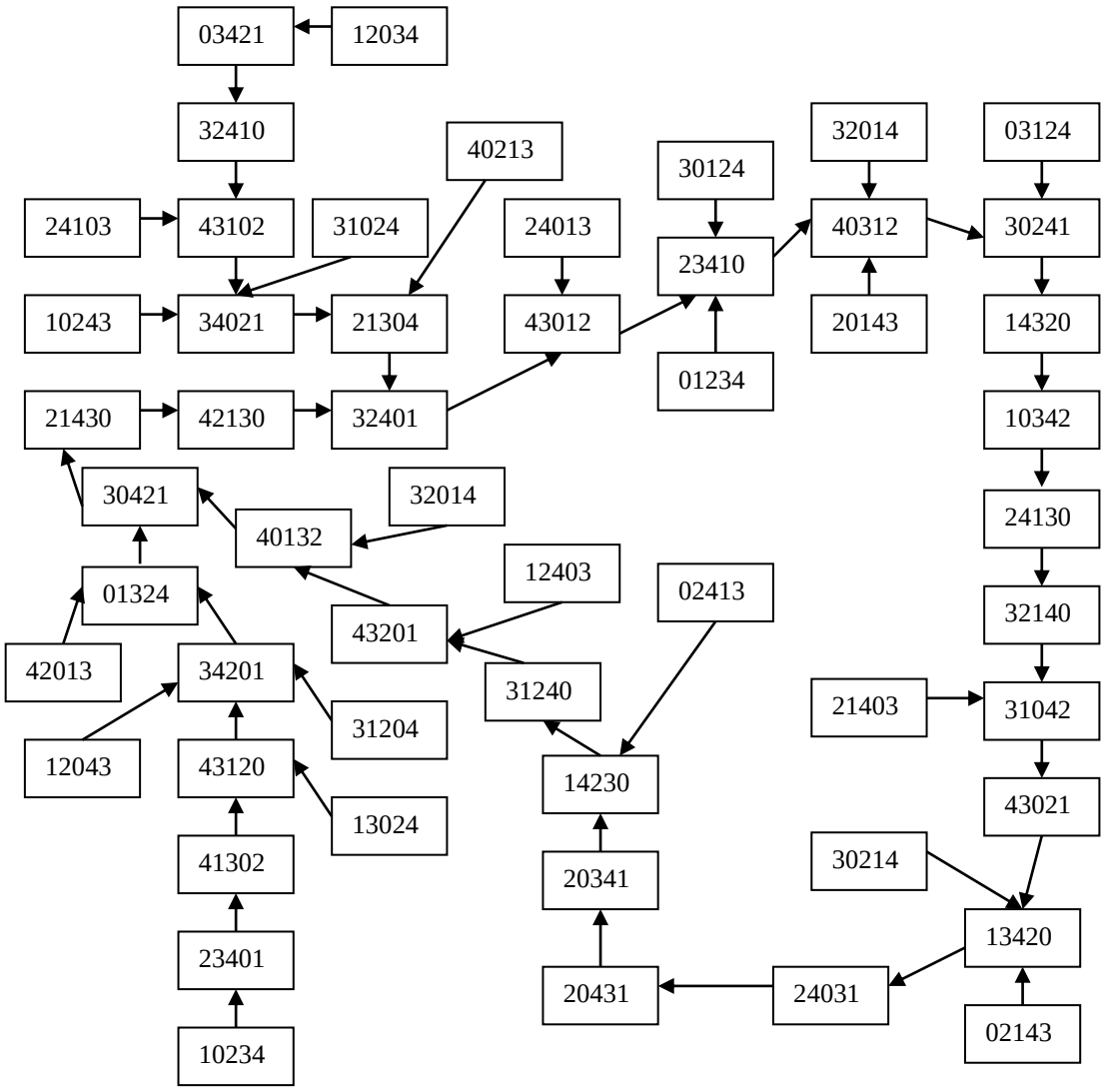

Рис. 4
Цикловая структура графа переходных состояний с n= 6. Цикл 1.