УДК 681.3.06: 519.248.681

ОЦЕНКА И АНАЛИЗ ХАРАКТЕРИСТИК ПОДМНОЖЕСТВА ОДНОЦИКЛОВЫХ ПОДСТАНОВОК

И.В. Кононова

Обсуждаются свойства и характеристики множества таблиц, составленных из одноцикловых подстановок степени **n** при их использовании в качестве долговременных ключей в алгоритме ГОСТ 28147-89.

В последнее время проявлен интерес к использованию в алгоритме симметричного шифрования по ГОСТ 28147-89 в качестве долговременных ключей таблиц подстановок сгенерированных случайным образом. Возникает вопрос о том, какие же ограничения необходимо наложить на подстановки, из которых составляются таблицы, поскольку какие-либо требования к отбору подстановок в доступной литературе отсутствуют.

Таблицу, составленную из **m** подстановок степени **n**, будем в дальнейшем представлять в виде матрицы

$$\mathbf{S_{m,n}} = \begin{vmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \dots & \mathbf{n} \\ \mathbf{i_{11}} & \mathbf{i_{12}} & \mathbf{i_{13}} & \dots & \mathbf{i_{1n}} \\ \mathbf{i_{21}} & \mathbf{i_{22}} & \mathbf{i_{23}} & \dots & \mathbf{i_{2n}} \\ \dots & \dots & \dots & \dots & \dots \\ \mathbf{i_{m1}} & \mathbf{i_{m2}} & \mathbf{i_{m3}} & \dots & \mathbf{i_{mn}} \end{vmatrix}. \qquad (1)$$

Верхнюю строку будем называть нулевой, а остальные пронумеруем соответственно от **1**-й до **m**-й.

Представляется, что одно из ограничений по составлению таблицы (1) может быть сформулировано непосредственно исходя из смысла и предназначения самой процедуры подстановки. Действительно в результате подстановки на основе непредсказуемой для злоумышленника замены одного блока данных другим решается задача по быстрому и эффективному уменьшению статистической связи между текстом на входе шифратора и текстом на его выходе. Поэтому будет естественным постараться избежать при построении подстановок тождественных переходов, т. е. ситуа-

ций, когда процедура подстановки как бы не участвует в процессе шифрования.

В результате можно сформулировать первое требование по отбору таблиц подстановок в следующем виде.

Требование 1. В таблицу подстановок должны входить подстановки, не имеющие совпадений с нулевой строкой.

Второе ограничение к отбору ″подходящих″ подстановок можно сформулировать опять - таки исходя из представляющегося естественным стремления обеспечить определенную степень различия (непохожести) самих подстановок, из которых строится таблица, в следующем виде.

Требование 2. При построении таблицы подстановок в их число не должны включаться подстановки, содержащие одинаковые (совпадающие) переходы (фрагменты).

Известно, что отсутствие тождественных переходов гарантирует использование так называемых одноцикловых подстановок, т.е. подстановок, имеющих единственный цикл максимально возможной длины [1].

В этой работе будет выполнена оценка числа подстановок (таблиц подстановок) такого типа, удовлетворяющих приведенным требованиям.

Воспользуемся идеей, состоящей в том, что любую случайную перестановку можно трактовать как одноцикловую подстановку.

Действительно, пусть некоторым методом получена случайная перестановка из $\mathbf{n}$ элементов $\mathbf{(P_1,P_2,...,P_n)}$.

Здесь $\mathbf{P_1,P_2,...,P_n}$ - числа из множества $\mathbf{1}$, $\mathbf{2}$, $\mathbf{...}$, $\mathbf{n}$, расположенные в некотором случайном порядке.

Будем теперь трактовать эту перестановку как циклическую подстановку в виде

$$\boxed{\rightarrow \mathbf{P_1} \rightarrow \mathbf{P_2} \rightarrow \mathbf{...} \rightarrow \mathbf{P_n}}\,, \qquad (2)$$

т.е. как единственный цикл подстановки

$$\begin{pmatrix} \mathbf{P_1} & \mathbf{P_2} & \cdots & \mathbf{P_{n-1}} & \mathbf{P_n} \\ \mathbf{P_2} & \mathbf{P_3} & \cdots & \mathbf{P_n} & \mathbf{P_1} \end{pmatrix}.$$

Упорядочивая для удобства верхнюю строку по возрастанию, зафиксируем в левой верхней позиции элемент $\mathbf{1}$, так что все разнообразие достигается различными преобразованиями элементов $\mathbf{2 - n}$

$$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ P_{i1} & P_{i2} & \cdots & P_{in-1} & P_{in} \end{pmatrix}.$$

Число таких подстановок (одноцикловых) будет не **n!**, а **(n-1)!**, что для $n = 16$ (для ГОСТа) составит величину $N = 1{,}3 \cdot 10^{12}$.

Будем называть подстановки, полученные таким методом, циклическими.

Требование 2*. Циклические подстановки допустимого множества (из которых строится расширенная таблица (1)) не должны содержать идентичных сегментов (фрагментов) длины $t \geq 2$.

Действительно, любые два подряд следующих символа одной циклической подстановки (2), совпадающие с двумя подряд следующими символами другой циклической подстановки, будут приводить при естественной записи таблицы подстановок [2,3] к совпадению элементов, попадающих в один и тот же столбец. При увеличении длины совпадающих фрагментов будет увеличиваться и число столбцов с совпадением элементов.

Одновременно с фрагментами длины $t \geq 2$ будем запрещать и их инверсии (наборы элементов, следующих в обратном порядке). Причем фрагменты длины **t** будем называть отрезками (сегментами) из **t** символов подстановки (2), получающимися при всех ее циклических сдвигах.

В отмеченных условиях все числа участвуют в построении каждой из подстановок совершенно равноправно. А поэтому подстановки допустимого множества обладают свойством симметрии в том смысле, что все выводы, относящиеся к фрагментам подстановок, начинающихся с единицы, совпадают с выводами для фрагментов подстановок, начинающихся с любого другого числа (естественно, что фрагмент может содержать произвольный набор чисел).

Ориентируясь теперь на требование 2*, перейдем к получению необходимых расчетных соотношений для оценки допустимого множества подстановок циклического типа. Нам для этого потребуется воспользоваться утверждениями, доказанными ниже.

Утверждение 1. Вероятность того, что в случайно взятой циклической подстановке из **n** элементов два отмеченных элемента стоят рядом, равна $2/(n-1)$, $n \geq 3$.

Доказательство. Действительно, всего циклических подстановок из **n** элементов (у которых 1 стоит на первой позиции) имеется **(n-1)!**. Пусть отмечены два элемента **i** и **k**. Элемент **k** временно отбросим и построим

все возможные перестановки (с 1 на первой позиции) из оставшихся **n - 2** элементов. Их будет **(n-2)!**. Но тогда **i**-й элемент может быть поставлен рядом с **k**-м на двух позициях (слева от **k** и справа от **k**), что дает **2(n-2)!** возможных циклических подстановок **n-**го порядка, где элементы **i** и **k** стоят рядом.

Таким образом, вероятность получить такую перестановку (циклическую подстановку), равна

$$\mathbf{P_n^{(2)} = \frac{2(n-2)!}{(n-1)!} = \frac{2}{n-1}}, \tag{3}$$

что и т.д.

Используя этот результат, можно убедиться в справедливости следующего утверждения.

Утверждение 2. Вероятность случайного выбора циклической подстановки, не имеющей совпадающих фрагментов длины $\mathbf{t \geq 2}$ с некоторой произвольно взятой (циклической подстановкой), оценивается вычисление

$$\mathbf{P_{1n}^{(2)} \approx \left(1 - \frac{2}{n-1}\right)^n}, \tag{4}$$

причем для общего числа таких подстановок конечной степени **n** справедлива оценка

$$\mathbf{W_{1n}^{(2)} \geq (n-1)! \cdot P_{1n}^{(2)}}, \tag{5}$$

т.е. результат (4) является границей снизу.

В силу описанного выше свойства симметрии рассматриваемого множества подстановок доказательство можно провести, взяв в качестве фиксированной (исходной) циклической подстановки нулевую строку в (1), т.е. подстановку **1, 2, 3, ..., n**.

В результате необходимо определить вероятность выбора циклической подстановки типа (2), в которой 1 не стоит рядом с **2, 2** рядом с **3, ...,**
n - 1 рядом с **n, n** рядом с **1** (в которой имеются только совпадающие фрагменты длиной $\mathbf{t = 1}$).

Очевидно, что интересующая нас вероятность $\mathbf{P_{1n}^{(2)}}$ может быть представлена в виде произведения условных вероятностей определяющих ее элементарные события: $\overline{\mathbf{1.2}}$ - единица не стоит рядом с двойкой, $\overline{\mathbf{2.3}}$ -

двойка не стоит рядом с тройкой, и т.д. $\overline{\mathbf{n.1}}$ - **n** не стоит рядом с 1, а именно

$$\mathbf{P}_{1n}^{(2)} = \mathbf{P}\left(\overline{\mathbf{1.2}};\overline{\mathbf{2.3}};\ldots;\overline{\mathbf{(n-1).n}};\overline{\mathbf{n.1}}\right) =$$

$$= \mathbf{P}(\overline{\mathbf{1.2}})\mathbf{P}\left(\overline{\mathbf{2.3}} \,/\, \overline{\mathbf{1.2}}\right)\cdots\mathbf{P}\left(\overline{\mathbf{n-1.n}} \,/\, \overline{\mathbf{1.2}},\overline{\mathbf{2.3}},\ldots,\overline{\mathbf{n-2.n-1}}\right)\times(6)$$

$$\times\,\mathbf{P}\left(\overline{\mathbf{n.1}} \,/\, \overline{\mathbf{1.2}},\overline{\mathbf{2.3}},\ldots,\overline{\mathbf{n-1.n}}\right).$$

Рассмотрим один из сомножителей этого выражения, представив его в виде отношения чисел подстановок, определяющих его значение

$$\mathbf{P}(\overline{\mathbf{s-1.s}}/\,\overline{\mathbf{1.2}};\overline{\mathbf{2.3}};\ldots;\overline{\mathbf{s-1.s}}) =$$

$$= \frac{\mathbf{N}\left(\overline{\mathbf{1.2}};\overline{\mathbf{2.3}};\ldots;\overline{\mathbf{s-2.s-1}}\right) - \mathbf{N}\left(\overline{\mathbf{1.2}};\overline{\mathbf{2.3}};\ldots;\overline{\mathbf{s-2.s-1}},\overline{\mathbf{s-1.s}}\right)}{\mathbf{N}\left(\overline{\mathbf{1.2}};\overline{\mathbf{2.3}};\ldots;\overline{\mathbf{s-2.s-1}}\right)}.$$

В этом выражении $\mathbf{N}(\overline{\mathbf{1.2}},\overline{\mathbf{2.3}},\ldots,\overline{\mathbf{s-2.s-1}})$ - число циклических подстановок, не имеющих рядом стоящих элементов **1** и **2, 2 и 3,…, s – 2** и **s-1**, $\mathbf{N}(\overline{\mathbf{1.2}},\overline{\mathbf{2.3}},\ldots,\overline{\mathbf{s-2.s-1}},\overline{\mathbf{s-1.s}})$ - число подстановок, не имеющих рядом стоящих элементов **1** и **2**, **2** и **3, ..., s - 2** и **s - 1** и в то же время содержащих стоящие рядом элементы **s-1** и **s**, так что число подстановок в которых отсутствуют рядом стоящие числа **1.2, 2.3,.. .., s-2.s-1, s-1.s** определяется как

$$\mathbf{N}(\overline{\mathbf{1.2}},\overline{\mathbf{2.3}},\ldots,\overline{\mathbf{s-2.s-1}}) - \mathbf{N}(\overline{\mathbf{1.2}},\overline{\mathbf{2.3}},\ldots,\overline{\mathbf{s-2.s-1}},\overline{\mathbf{s-1.s}}) =$$

$$= \mathbf{N}(\overline{\mathbf{1.2}},\overline{\mathbf{2.3}},\ldots,\overline{\mathbf{s-2.s-1}},\overline{\mathbf{s-1.s}})$$

Очевидно, что число подстановок, имеющих рядом стоящие элементы **s - 1** и **s**, и при этом не имеющих рядом стоящих элементов **1.2, 2.3, ...,**

$\mathbf{s - 2.s - 1}$, т.е. $\mathbf{N(\overline{1.2}, \overline{2.3}, \ldots, \overline{s-2.s-1}, \overline{s-1.s})}$ будет всегда меньше числа подстановок, имеющих совпадающие элементы $\mathbf{s - 1}$ и $\mathbf{s}$ без других ограничений. В соответствии с объяснениями при доказательстве утверждения 1 таких подстановок будет $\mathbf{2(n-2)!}$. Очевидно также неравенство

$$\mathbf{(n-1)! > N(\overline{1.2}, \overline{2.3}, \ldots, \overline{s-2.s-1})}$$

С учетом отмеченных моментов для условных вероятностей $\mathbf{P(s\text{-}1.s/12,23,...,s\text{-}2.s\text{-}1)}$, $\mathbf{s = 3, 4, ...}$ оказывается справедлива оценка

$$\mathbf{P}\left(\overline{s-1.s} \,/\, \overline{1.2}, \overline{2.3}, \ldots, \overline{s-2.s-1}\right) > 1 - \frac{2}{n-1},$$

$\mathbf{s = 3, 4, ..., n+1;}$ $\mathbf{n.n+1 \rightarrow n.1}$.

Полученный результат позволяет заменить в соотношении (6) условные вероятности их оценочными значениями, и в конечном итоге убедиться в справедливости утверждения 2 и правомерности соотношения (4) и (5).

Пользуясь теперь соотношением (3), можем получить, что при $\mathbf{n = 16}$ $\mathbf{P_{1n}^{(2)} = 0{,}01}$, т.е. не менее 10% случайно сгенерированных циклических подстановок удовлетворяют требованию 2*.

Их число составит (при $\mathbf{n = 16}$)

$$\mathbf{W_{1n}^{(2)} = (n-1)! \cdot P_n^2 = 1.3 \cdot 10^{11}}. \qquad (7)$$

Заметим также, что при $\mathbf{n \rightarrow \infty}$ число, определяемое соотношением (4), стремится к пределу

$$\mathbf{\lim_{n \to \infty} \left(1 - \frac{2}{n-1}\right)^n = e^{-2} = 0.13533}.$$

Рассмотрим теперь задачу отбора из полученного множества подстановок (не имеющих совпадающих элементов с заданной) подстановки, не имеющей совпадающих фрагментов ни с одной из ранее выбранных. Воспользуемся и здесь идеей независимости формирования случайных подстановок.

В соответствии с идеей независимости построения случайных подстановок число подстановок, не имеющих совпадений фрагментов с некоторыми двумя фиксированными подстановками, вычисляется по формуле

$$\mathbf{\overline{\overline{W}}_{2,n}^{(2)} = (n-1)!\left(P_{n,1}^{(2)}\right)^2}.$$

При $n = 16$ имеем $\tilde{W}^{(2)}_{2,n} \approx 1.3 \cdot 10^{10}$.

Отметим, что если провести более точный подсчет множества допустимых подстановок для этого случая, то для вероятности выбора циклической подстановки, не имеющей совпадающих фрагментов длиной $t \geq 2$ с некоторыми двумя произвольно взятыми циклическими подстановками, можно получить другую формулу

$$P^{(2)}_{n,2} \approx \left(1 - \frac{4}{n-1} + \frac{2}{(n-1)(n-2)}\right)^n. \qquad (9)$$

Действительно, из общего числа $(n-1)!$ циклических подстановок, как показано выше, равно $2(n-2)!$ имеют пару отмеченных элементов (фрагмент одной из фиксированных подстановок) стоящих рядом (например, элементы 1.2). У второй фиксированной подстановки пусть другая пара имеет вид 1.3. Следовательно, можно также указать $2(n-2)!$ циклических подстановок, содержащих вторую пару отмеченных стоящих рядом элементов 1 и 3. Но подстановки с парой 1.2 содержат подстановки с парой 1.3 и наоборот. Для оценки числа совпадающих в этих подмножествах подстановок (в каждом из подмножеств) воспользуемся утверждениями, доказанными ниже.

Утверждение 3. Циклическая подстановка n-ой степени, содержащая комбинацию 1. 2. 3, имеет вероятность $1/(n-1)(n-2)$.

Доказательство выполняется аналогично утверждению 1. Только теперь изымается два элемента 2 и 3. Из оставшихся элементов можно сформулировать $(n-3)!$ всевозможных циклических подстановок (с единицей на первой позиции). Возвращение элементов 2 и 3 на дозволенные места не увеличивает количества допустимых перестановок. Таким образом, искомая вероятность получается делением $(n-3)!$ на $(n-1)!$

Утверждение 4. Циклическая подстановка n-й степени содержащая комбинации 1.2 и 3.4 имеет вероятность $1/(n-1)(n-2)$.

Доказательство и здесь аналогично доказательству утверждения 3.

Пользуясь теперь приведенными утверждениями для подсчета числа подстановок $N(1.2,1.3)$, не имеющих фрагментов 1.2 и 1.3 (с учетом их инверсий), т.е. не имеющих рядом стоящих элементов 1.2 и 1.3, можно записать выражение

$$N(\overline{1.2}, \overline{2.3}) = (n-1)! - 2(n-2)! - 2(n-3)! + 2(n-3)!.$$

При записи этого выражения мы из общего числа циклических подстановок вначале вычли подстановки, содержащие фрагменты 1.2 и 1.3 и затем последним слагаемым компенсировали подстановки, дважды вычтенные в первых двух членах.

В итоге для определения вероятности выбора циклической подстановки, не содержащей двух фиксированных (произвольных) фрагментов длины $\mathbf{t \geq 2}$, т.е. не имеющих совпадений в двух фрагментах, принадлежащим разным подстановкам, получим выражение

$$\frac{1}{(n-1)!}\left[(n-1)!-4(n-2)!+2(n-3)!\right]=1-\frac{4}{n-1}+\frac{2}{(n-1)(n-2)}.$$

Если рассматривать фрагменты фиксированных подстановок, начинающиеся с одной и той же цифры, то для вычисления вероятности того, что произвольно взятая подстановка не будет иметь ни одного из фрагментов длиной $\mathbf{t \geq 2}$, начинающегося с любой цифры и совпадающего с соответствующими по началу фрагментами любых двух произвольно выбранных циклических подстановок, в свою очередь не имеющих между собой совпадающих фрагментов длины $\mathbf{t \geq 2}$, как раз и потребуется воспользоваться соотношением (6) (нет совпадений ни по фрагментам, начинающимся с **1**, ни по фрагментам, начинающимся с **2, ...**, ни по фрагментам, начинающимся с **n** - всего **n** независимых событий).

Расчеты, выполненные в соответствии с этим соотношением, практически повторяют результат, полученный ранее. Близость результатов для интересующих нас значений **n** легко видеть из соотношения

$$\left(1-\frac{2}{n-1}\right)^{2n}\approx\left(1-\frac{4}{n-1}+\frac{2}{(n-1)(n-2)}\right)^{n}.$$

С учетом приведенных результатов оценим возможности выполнения требования 2*, в частности, нас будет интересовать число вариантов построения таблицы из 8-ми (для ГОСТа) упорядоченных циклических подстановок

$$\begin{cases} 1p_2^{(1)}p_3^{(1)}\dots p_{16}^{(1)} \\ 1p_2^{(2)}p_3^{(2)}\dots p_{16}^{(2)} \\ \dots\dots \\ 1p_2^{(8)}p_3^{(8)}\dots p_{16}^{(8)} \end{cases}, \qquad (10)$$

в которых отсутствуют совпадающие фрагменты длиной $\mathbf{t \geq 2}$.

При выполнении окончательных расчетов мы наложим еще одно ограничение - отсутствие в подстановках, попавших в таблицу (10), переходов

$\mathbf{i \rightarrow i + 1}$ и наоборот, т.е. добавим в таблицу (10) нулевую строку **1, 2, ..., n**. Пользуясь идеей независимости сочетания фрагментов при построении любой подстановки, для числа допустимых подстановок в каждой из строк таблицы (10) получим оценки:

$$\overset{\approx}{W}{}^{(2)}_{1,16} \geq (n-1)!\,P_{1,16} = 1.3\cdot 10^{11};$$

$$\overset{\approx}{W}{}^{(2)}_{2,16} \geq (n-1)!\,(P_{1,16})^2 = 1.3\cdot 10^{10};$$

$$\overset{\approx}{W}{}^{(2)}_{3,16} \geq (n-1)!\,(P_{1,16})^3 = 1.3\cdot 10^{9};$$

$$\overset{\approx}{W}{}^{(2)}_{4,16} \geq (n-1)!\,(P_{1,16})^4 = 1.3\cdot 10^{8};$$

$$\overset{\approx}{W}{}^{(2)}_{5,16} \geq (n-1)!\,(P_{1,16})^5 = 1.3\cdot 10^{7};$$

$$\overset{\approx}{W}{}^{(2)}_{6,16} \geq (n-1)!\,(P_{1,16})^6 = 1.3\cdot 10^{6};$$

$$\overset{\approx}{W}{}^{(2)}_{7,16} \geq (n-1)!\,(P_{1,16})^7 = 1.3\cdot 10^{5};$$

$$\overset{\approx}{W}{}^{(2)}_{8,16} \geq (n-1)!\,(P_{1,16})^8 = 1.3\cdot 10^{4}.$$

В результате набор из 8×6 допустимых циклических подстановок рассматриваемого типа может быть выбран более, чем

$$\prod_{i=1}^{8} \tilde{W}_{i,16}^{(2)} \approx 1.28 \cdot 10^{62}$$

способами, и здесь имеется вполне достаточное пространство для формирования долговременных ключей, хотя оно получилось значительно меньше по мощности, чем в первом подходе. Это и понятно, так как в данном случае множество возможных подстановок ограничено подстановками циклического типа (одноцикловыми подстановками).

С другой стороны, ограничения, накладываемые при втором подходе, можно считать наиболее жесткими, так как при их выполнении таблица подстановок **K(0)**, **K(1)**, **...**, **K(7)** содержит полностью отличающиеся друг от друга наборы чисел (нет совпадений ни по столбцам, ни по строкам, и нет переходов $\mathbf{i \to i + 1, i \to i - 1)}$. При ослаблении ограничений пространство допустимых подстановок будет увеличиваться.

В рамках развиваемого общего подхода можно отказаться от запрета инверсий фрагментов и можно пойти на запреты фрагментов длины $\mathbf{t \geq 3}$ и т.д. Например, если в качестве первой строки в таблице (10) взять произвольную циклическую подстановку, сняв запрет на переходы $\mathbf{i \to i + 1}$, $\mathbf{i \to i - 1}$ и сохранив все остальные ограничения, то

$$\prod_{i=1}^{8} \tilde{W}_{i,16}^{(2)} \approx 1.3 \cdot 10^{70} .$$

Соответствующие оценки допустимых множеств долговременных ключей легко могут быть получены и для других случаев.

В итоге, на наш взгляд, представленные результаты позволяют перейти уже к непосредственной практической отработке алгоритмов формирования долговременных ключей, что может стать важным шагом на пути широкого применения алгоритма ГОСТ 28147-89.

ЛИТЕРАТУРА

1. Сачков В.Н. Комбинаторные методы дискретной математики. - М.: Наука, 1977. - 319 с.

2. Завало С.Т., Костарчук В.Н., Хацет Б.И. Алгебра и теория чисел. - ч. 2. - К.: Вища школа, 1980. - 407 с.

3. Математическая энциклопедия: в 5 т./ Гл. ред. И.М. Виноградов - Советская энциклопедия. - М., 1979. - Т. 2: Д - КОО. - 1103 с.