

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

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

Верхнюю строку будем называть нулевой, а остальные пронумеруем соответственно от $\mathbf{1}$ -й до \mathbf{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 эффективно 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 - так 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 n элементов (P_1, P_2, \dots, P_n) .

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

Будем теперь трактовать эту перестановку как циклическую подстановку в виде

$$\boxed{\rightarrow P_1 \rightarrow P_2 \rightarrow \dots \rightarrow P_n \rightarrow}, \quad (2)$$

т.е. как единственный цикл подстановки

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

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

$$\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ P_{i_1} & P_{i_2} & \dots & P_{i_{n-1}} & P_{i_n} \end{pmatrix}.$$

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

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

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 $t \geq 2$ с некоторой произвольно взятой (циклической подстановкой), оценивается вычисление

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

причем для общего числа таких подстановок конечной степени n справедлива оценка

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

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 $1, 2, 3, \dots, n$.

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 $t = 1$).

Очевидно, что интересующая нас вероятность $P_{1n}^{(2)}$ может быть представлена в виде произведения условных вероятностей определяющих ее

элементарные события: $\overline{1.2}$ - единица не стоит рядом с двойкой, $\overline{2.3}$ -

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

$$\begin{aligned}
 P_{1n}^{(2)} &= P\left(\overline{1.2}; \overline{2.3}; \dots; \overline{(n-1).n}; \overline{n.1}\right) = \\
 &= P(\overline{1.2}) P\left(\overline{2.3} / \overline{1.2}\right) \dots P\left(\overline{n-1.n} / \overline{1.2, 2.3, \dots, n-2.n-1}\right) \times (6) \\
 &\quad \times P\left(\overline{n.1} / \overline{1.2, 2.3, \dots, n-1.n}\right).
 \end{aligned}$$

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

$$\begin{aligned}
 &P(\overline{s-1.s} / \overline{1.2}; \overline{2.3}; \dots; \overline{s-1.s}) = \\
 &= \frac{N\left(\overline{1.2}; \overline{2.3}; \dots; \overline{s-2.s-1}\right) - N\left(\overline{1.2}; \overline{2.3}; \dots; \overline{s-2.s-1, s-1.s}\right)}{N\left(\overline{1.2}; \overline{2.3}; \dots; \overline{s-2.s-1}\right)}.
 \end{aligned}$$

В этом выражении $N(\overline{1.2}, \overline{2.3}, \dots, \overline{s-2.s-1})$ - число циклических подстановок, не имеющих рядом стоящих элементов 1 и 2 , 2 и $3, \dots, s-2$ и $s-1$, $N(\overline{1.2}, \overline{2.3}, \dots, \overline{s-2.s-1, s-1.s})$ - число подстановок, не имеющих рядом стоящих элементов 1 и 2 , 2 и $3, \dots, s-2$ 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 $1.2, 2.3, \dots, s-2.s-1, s-1.s$ определяется как

$$\begin{aligned}
 &N(\overline{1.2}, \overline{2.3}, \dots, \overline{s-2.s-1}) - N(\overline{1.2}, \overline{2.3}, \dots, \overline{s-2.s-1, s-1.s}) = \\
 &= N(\overline{1.2}, \overline{2.3}, \dots, \overline{s-2.s-1, s-1.s})
 \end{aligned}$$

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

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

$$(n-1)! > N(1.2, 2.3, \dots, s - 2.s - 1)$$

С учетом отмеченных моментов для условных вероятностей $P(s-1.s/1.2, 2.3, \dots, s-2.s-1)$, $s = 3, 4, \dots$ оказывается справедлива оценка

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

$$s = 3, 4, \dots, n+1; \quad n.n+1 \rightarrow n.1.$$

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 $n = 16$ $P_{1n}^{(2)} = 0,01$, т.е. не менее 10% случайно сгенерированных циклических подстановок удовлетворяют требованию 2*.

Их число составит (при $n = 16$)

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

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

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

Рассмотрим теперь задачу отбора из полученного множества подстановок (не имеющих совпадающих элементов с заданной) подстановки, не имеющие 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

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

При $n = 16$ имеем $\overset{\approx (2)}{W_{2,n}} \approx 1.3 \cdot 10^{10}$.

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

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

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 $\overline{\overline{N(1.2,1.3)}}$, 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

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

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 $t \geq 2$, т.е. не имеющих совпадений в двух фрагментах, принадлежащим разным подстановкам, получим выражение

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

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 $t \geq 2$, 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 $t \geq 2$, как раз и потребуется воспользоваться соотношением (6) (нет совпадений ни по фрагментам, начинающимся с 1 , ни по фрагментам, начинающимся с $2, \dots$, 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

$$\left\{ \begin{array}{l} 1p_2^{(1)} p_3^{(1)} \dots p_{16}^{(1)} \\ 1p_2^{(2)} p_3^{(2)} \dots p_{16}^{(2)} \\ \dots \\ 1p_2^{(8)} p_3^{(8)} \dots p_{16}^{(8)} \end{array} \right., \quad (10)$$

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

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

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

$$\begin{aligned} \overset{\approx}{\mathbf{W}}_{1,16}^{(2)} &\geq (n-1)!P_{1,16} = 1.3 \cdot 10^{11}; \\ \overset{\approx}{\mathbf{W}}_{2,16}^{(2)} &\geq (n-1)!(P_{1,16})^2 = 1.3 \cdot 10^{10}; \\ \overset{\approx}{\mathbf{W}}_{3,16}^{(2)} &\geq (n-1)!(P_{1,16})^3 = 1.3 \cdot 10^9; \\ \overset{\approx}{\mathbf{W}}_{4,16}^{(2)} &\geq (n-1)!(P_{1,16})^4 = 1.3 \cdot 10^8; \\ \overset{\approx}{\mathbf{W}}_{5,16}^{(2)} &\geq (n-1)!(P_{1,16})^5 = 1.3 \cdot 10^7; \\ \overset{\approx}{\mathbf{W}}_{6,16}^{(2)} &\geq (n-1)!(P_{1,16})^6 = 1.3 \cdot 10^6; \\ \overset{\approx}{\mathbf{W}}_{7,16}^{(2)} &\geq (n-1)!(P_{1,16})^7 = 1.3 \cdot 10^5; \\ \overset{\approx}{\mathbf{W}}_{8,16}^{(2)} &\geq (n-1)!(P_{1,16})^8 = 1.3 \cdot 10^4. \end{aligned}$$

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 $i \rightarrow i + 1$, $i \rightarrow i - 1$). 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 $t \geq 3$ и т.д. Например, если в качестве первой строки в таблице (10) взять произвольную циклическую подстановку, сняв запрет на переходы $i \rightarrow i + 1$, $i \rightarrow i - 1$ 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.
-