

УДК 519.61+519.7

О ПОРЯДКЕ РОСТА ЧИСЛА ИНЪЕКТИВНЫХ И СВЕРХРАСТУЩИХ ВЕКТОРОВ И НЕКОТОРЫХ ОСОБЕННОСТЯХ СИЛЬНОГО МОДУЛЬНОГО УМНОЖЕНИЯ

Д. М. Мурин

В 1978 г. Р. Меркль и М. Хеллман [1] предложили знаменитую ранцевую криптосистему. В ее основе лежит преобразование сверхрастающего вектора $A = (a_1, a_2, \dots, a_n)$ ($a_i \in \mathbb{N}, i = 1, \dots, n$) с помощью сильного модульного умножения относительно натурального модуля $m \in \left(\sum_{i=1}^n a_i, 2 \sum_{i=1}^n a_i \right]$ и натурального множителя $t \in (1, m)$ в инъективный вектор $B = (b_1, b_2, \dots, b_n)$ ($b_i \in \mathbb{N}, i = 1, \dots, n$), который служит открытым ключом.

В настоящей работе рассматриваются вопросы о том, какую часть от множества всех возможных векторов размерности n составляют инъективные и сверхрастающие векторы, и о равномерности покрытия множества упорядоченных инъективных векторов размерности n векторами, полученными из сверхрастающих векторов с помощью операции сильного модульного умножения и процедуры сортировки элементов вектора по возрастанию. Определения понятий упорядоченного (возрастающего), инъективного и сверхрастающего вектора, сильного модульного умножения можно найти в монографии [2].

О порядке роста числа инъективных и сверхрастающих векторов

Обозначим через $F_1(n, M)$ число упорядоченных инъективных векторов размерности n , максимальный элемент которых равен M , а через $F_2(n, M)$ — число сверхрастающих векторов размерности n , максимальный элемент которых равен M .

Число векторов с максимальным элементом M , имеющих размерность n , равно $\sum_{k=1}^n C_n^k (M-1)^{n-k}$, из чего можно заключить, что $F_1(n, M) \leq \frac{n(M-1)^{n-1}}{n!}$, т. е. $F_1(n, M)$ при фиксированном n ограничено сверху некоторым полиномом степени $n-1$ от M . Оказывается, что справедлива следующая

Теорема. При фиксированном $n \geq 2$ и $M \geq 2^{n-1}$ выполняется неравенство $F_1(n, M) \geq F_2(n, M) \geq P(M)$, где $P(M)$ — некоторый полином $(n-1)$ -й степени от M .

Например, $F_2(n, M) \geq \left(\frac{M - 2^{n-1} + 1}{2^{n-2}} - 1 \right) \left(\frac{M - 2^{n-1} + 1}{2^{n-1}} \right)^{n-2}$ при $n \geq 2$ и $M \geq 2^{n-1}$. Это позволяет заключить, что функции $F_1(n, M)$ и $F_2(n, M)$ ведут себя подобно полиномам степени $n-1$ от M , а пределы $\lim_{M \rightarrow \infty} \frac{F_1(n, M)}{\sum_{k=1}^n C_n^k (M-1)^{n-k}}$, $\lim_{M \rightarrow \infty} \frac{F_2(n, M)}{\sum_{k=1}^n C_n^k (M-1)^{n-k}}$ при фиксированном n существуют, конечны и не равны 0.

Отметим, что $F_2(n, M) = 0$ при фиксированном $n \geq 2$ и $M < 2^{n-1}$.

О некоторых особенностях сильного модульного умножения

Рассмотрим множество сверхрастающих векторов размерности n , максимальный элемент которых строго меньше M . Операция сильного модульного умножения с модулем $m \leq M$ с последующим применением процедуры сортировки элементов вектора по возрастанию отображает указанное множество во множество упорядоченных инъективных векторов размерности n , максимальный элемент которых строго меньше M .

Обозначим через $F_3(n, < M)$ число упорядоченных инъективных векторов размерности n , максимальный элемент которых строго меньше M (т. е. мощность множества упорядоченных потенциальных векторов шифрования).

Обозначим через $F_4(n, < M)$ число различных упорядоченных инъективных векторов размерности n , полученных с помощью сильного модульного умножения относительно модуля m и всех возможных множителей $1 < t < m$ из сверххрастающих векторов размерности n , максимальный элемент которых строго меньше M , при условии, что для каждого сверххрастающего вектора $A = (a_1, \dots, a_n)$ модуль m пробегает интервал $(\sum_{i=1}^n a_i, \min(2 \sum_{i=1}^n a_i, M)]$. Таким образом, $F_4(n, < M)$ — мощность множества упорядоченных действительных векторов шифрования.

Различные тройки (сверххрастающий вектор, модуль, множитель) могут определять один упорядоченный инъективный вектор. Число троек, определяющих один упорядоченный инъективный вектор, назовем *числом представлений* данного вектора.

Обозначим через $F(n, < M)$ отношение $F_4(n, < M)/F_3(n, < M)$.

Проведенные вычислительные эксперименты позволяют выдвинуть следующую гипотезу.

Гипотеза. При фиксированном $n \in \mathbb{N}$ значение $F(n, < M)$ достигает 0,9 при значениях M , близких к 2^{2n} .

Так, при $n = 3$ и 4 значение $F(n, < M)$ достигает 0,9 при $M = 2^{2n-2} + 2^n - 1$.

В ходе проведения компьютерных экспериментов установлено, что в результате применения к сверххрастающим векторам операции сильного модульного умножения (при выборе модуля и множителя описанным выше способом) с последующим применением процедуры сортировки элементов вектора по возрастанию чаще получаются векторы, имеющие малую евклидову длину. На рис. 1 приведены результаты одного из экспериментов для $n = 3$ и $M = 34$. Каждому натуральному числу на оси Ln соответствует упорядоченный инъективный вектор. Меньшим натуральным числам соответствуют векторы с меньшей евклидовой длиной. По оси Representation number отложено число представлений упорядоченного инъективного вектора.

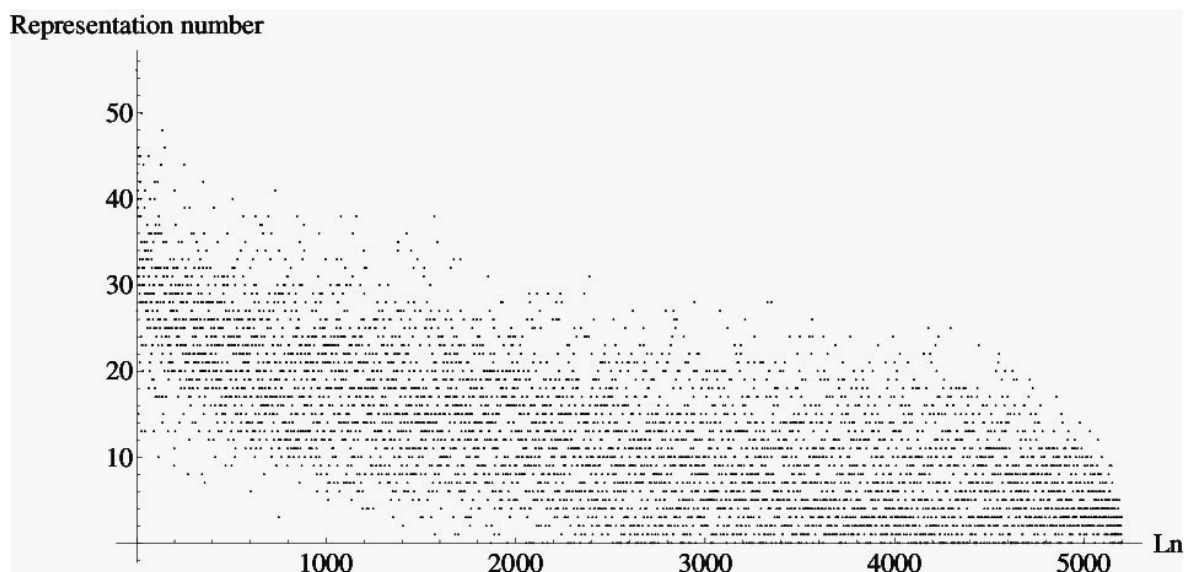


Рис. 1. Число представлений упорядоченных инъективных векторов при $n = 3$, $M = 34$

ЛИТЕРАТУРА

1. Merkle R. C. and Hellman M. E. Hiding information and signatures in trap-door knapsacks // IEEE Trans. Inform. Theory. 1978. V. IT-24. P. 525–530.
2. Саломая А. Криптография с открытым ключом. М.: Мир, 1995. 318 с.

УДК 512.542.74

ОПИСАНИЕ КЛАССА ПОДСТАНОВОК, ПРЕДСТАВИМЫХ В ВИДЕ ПРОИЗВЕДЕНИЯ ДВУХ ПОДСТАНОВОК С ФИКСИРОВАННЫМ ЧИСЛОМ МОБИЛЬНЫХ ТОЧЕК. II

А. Б. Пичкур

Пусть подстановка $G \in S_N$, $\Gamma(G) \subseteq \{1, \dots, N\}$ — множество мобильных точек подстановки G , $2 \leq q \leq N$, $\Gamma_N(q) = \{G \in S_N : |\Gamma(G)| = q\}$ — множество всех подстановок степени N , имеющих ровно q мобильных точек.

В предшествующей работе (см. [1]) полностью описано строение множества $\Gamma_N(q) \cdot \Gamma_N(q)$ при $4 \leq q \leq N/2$ и $N \geq 8$.

В данной работе описано множество всех подстановок из $\Gamma_N(q) \cdot \Gamma_N(q+t)$ при $t \geq 1$. Этот результат имеет практические приложения в криптографии.

Сначала приведём результаты о строении множества $\Gamma_N(q) \cdot \Gamma_N(q+1)$.

Утверждение 1. Если $N \geq 6$, $2 \leq q_1 < q_2 < N$, то имеет место включение $\Gamma_N(q_1) \cdot \Gamma_N(q_2) \subseteq \Gamma_N(q_1+1) \cdot \Gamma_N(q_2+1)$.

Теорема 1. Пусть $N \geq 8$, $3 \leq q \leq N/2$, $G \in S_N$. Если $1 < |\Gamma(G)| \leq 2q-1$, то существуют подстановки $H_1 \in \Gamma_N(q)$, $H_2 \in \Gamma_N(q+1)$, для которых выполняется равенство $G = H_1 \cdot H_2$.

Далее рассмотрим, какие подстановки из множеств $\Gamma_N(2q+1)$, $\Gamma_N(2q)$ принадлежат произведению $\Gamma_N(q) \cdot \Gamma_N(q+1)$.

Утверждение 2. Пусть $N \geq 4$, $2 \leq q < N/2$, подстановка $G \in \Gamma_N(2q+1)$ является произведением r неединичных циклов, длины которых равны $m_1, m_2, \dots, m_r$, $\sum_{i=1}^r m_i = 2q+1$. Подстановка G принадлежит множеству $\Gamma_N(q) \cdot \Gamma_N(q+1)$ в том и только в том случае, когда существует такое подмножество $\{i_1, \dots, i_k\} \subseteq \{1, \dots, r\}$, что $m_{i_1} + \dots + m_{i_k} = q$.

Утверждение 3. Пусть $N \geq 4$, $2 \leq q \leq N/2$, подстановка $G \in \Gamma_N(2q)$ является произведением r неединичных циклов, длины которых равны $m_1, m_2, \dots, m_r$, $\sum_{i=1}^r m_i = 2q$. Подстановка G принадлежит множеству $\Gamma_N(q) \cdot \Gamma_N(q+1)$ в том и только в том случае, когда выполнено условие: существует $i_0 \in \{1, \dots, r\}$ и существует такое подмножество $\{i_1, \dots, i_k\} \subseteq \{1, \dots, r\} \setminus \{i_0\}$, что $m_{i_0} > 2$ и $q - m_{i_1} + m_{i_2} + \dots + m_{i_k} \in \{2, \dots, m_{i_0} - 1\}$.

Итак, в теореме 1 и утверждениях 2 и 3 полностью описано строение множества $\Gamma_N(q) \cdot \Gamma_N(q+1)$ при $3 \leq q \leq N/2$.

Наконец, приведем результаты о строении множества $\Gamma_N(q) \cdot \Gamma_N(q+t)$, $t \geq 2$.

Теорема 2. Пусть $N > 10$, $2 \leq t < N-2$, $2 \leq q < (N-t)/2+1$, $G \in S_N$. Если $t \leq |\Gamma(G)| \leq 2q+t-2$, то существуют подстановки $H_1 \in \Gamma_N(q)$, $H_2 \in \Gamma_N(q+t)$, для которых выполняется равенство $G = H_1 \cdot H_2$.