УДК 629.3.06

ОЦЕНКА ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ ПРОСТЫХ ДЕЛИТЕЛЕЙ В КОМБИНИРОВАННОМ ТЕСТЕ ПРОСТОТЫ

к.т.н. А.В. Шостак
(представил д.ф.- м.н. С.В. Смеляков)

В статье приводится экспериментальная оценка эффекта от деления на простые числа в комбинированном тесте оценки простоты.

В настоящее время в системах защиты информации широко применяются несимметричные криптографические преобразования, которые в качестве ключевых параметров используют простые числа. Актуальна проблема построения быстрого алгоритма формирования простых чисел, основным этапом которого является тест проверки простоты [1]. Наибольшее распространение находит комбинированный тест простоты, одним из этапов которого является деление тестируемого числа на простые числа [1].

Деление на простые числа преследует цель уменьшить мощность множества **M(k)** для повышения вероятности выбора простых чисел из него (**M(k)** - множество целых чисел не кратных первым **k** простым числам). Рассмотрим числа множества **M(k)** и множества простых чисел **Z**, не превышающие некоторое число **X**. Мощности множеств **M(k)**и **Z** будут равны (с точностью до **k**) при $\mathbf{k} = \pi(\sqrt{\mathbf{X}}) = \mathbf{k}'$, где $\pi(\sqrt{\mathbf{X}})$ - число простых чисел, не превосходящих $\sqrt{\mathbf{X}}$ [2]. Эффект от последовательного деления на первые **k** простых чисел оценим относительным количеством составных чисел, удаленных из множества целых чисел, не превосходящих **X** - $\mathbf{E(k) = (X - \|M(k)\| - k)/X - \|Z\|}$, где $\|\mathbf{M(k)}\|$, $\|\mathbf{Z}\|$ - мощности соответствующих множеств. Очевидно, что $\|\mathbf{M(k')}\| + \mathbf{k'} = \|\mathbf{Z}\|$ и $\mathbf{E(k') = 1}$, т.е. после проведения деления на $\pi(\sqrt{\mathbf{X}})$ первых простых чисел множество **M(k')** будет состоять только из простых чисел. Достаточно просто вычислить $\|\mathbf{M(1)}\| = \mathbf{f(1,X) = X - 1 - [X/2] + 1}$, где второе слагаемое учитывает, что число '**1**' не принадлежит к простым числам; $[\mathbf{X/2}]$ - ближайшее целое, не превосходящее $\mathbf{X/2}$ и равное количеству чисел кратных 2 и не превосходящих **X**; четвертое слагаемое учитывает, что число '**2**' является простым. Формула для вычисления $\|\mathbf{M(2)}\|$ имеет вид

$$\|\mathbf{M(2)}\| = \mathbf{f(2,X) = X - 1 - [X/2] - [X/3] + 2 + [X/(2 \cdot 3)]}. \qquad (1)$$

Последнее слагаемое (1) учитывает количество чисел одновременно делящихся на 2 и 3. Аналогичный вид имеют и формулы для $\mathbf{k > 2}$.

Результаты экспериментальной оценки **E(k)** при **X**=6000 приведены в табл. 1. Отметим, что $\pi(6000) = 783,\ \pi(\sqrt{6000}) = 21$ [2].

Таблица 1

Оценка эффективности от использования простых делителей в комбинированном тесте простоты

Число делителей, **k**	Относительное число делителей, **k/21**	**E(k)**	$\|M(k)\|$	Относительное количество простых чисел в **M(k)**, $783/\|M(k)\|$
1	0.0476	0.5750	3000	0.2610
2	0.0952	0.7665	2001	0.3913
3	0.1429	0.8430	1602	0.4888
4	0.1905	0.8867	1374	0.5699
5	0.2381	0.9103	1251	0.6259
6	0.2857	0.9285	1156	0.6773
7	0.3333	0.9412	1090	0.7183
8	0.3810	0.9523	1032	0.7687
9	0.4286	0.9613	985	0.7949
10	0.4762	0.9684	948	0.8259
11	0.5238	0.9749	914	0.8567
12	0.5714	0.9799	888	0.8818
13	0.6190	0.9841	866	0.9042
14	0.6667	0.9881	845	0.9266
15	0.7143	0.9914	828	0.9457
16	0.7619	0.9942	813	0.9631
17	0.8095	0.9962	803	0.9751
18	0.8571	0.9977	795	0.9849
19	0.9048	0.9988	789	0.9924
20	0.9524	0.9996	785	0.9975
21	1.0	1.0	783	1.0

Третья строка табл.1 показывает, что после деления на 14.29% первых простых делителей относительное количество удаленных составных чисел достигнет 84.3%, а $\pi(6000)/\|M(3)\| = 0.4888$. Величину $\pi(X)/\|M(k)\|$ естественно использовать в качестве оценки вероятности выбора простого числа из множества **M(k)**. Приведенные относительные оценки не претерпят существенных изменений и при **X>6000**.

ЛИТЕРАТУРА

1. Качко Е.Г., Свинарев А.В., Мельникова О.А. Анализ вычислительной сложности алгоритмов тестирования на простоту чисел многократной точности // Радиоэлектроника и информатика. – 1998. – №1. – С. 44 - 47.

2. Бухштаб А.А. Теория чисел. – М.: Просвещение, 1966. – 384 с.

Поступила в редколлегию 15.12.2000