Дальневосточный математический журнал. 2020. Т. 20. № 2. С. 150–154

УДК 512.624.95
MSC2010 35Q31

© В. А. Быковский[1]

Вычисление случайных пар простых чисел, произведение которых лежит в заданном коротком интервале

В работе предложены эвристические алгоритмы для построения пар случайных простых чисел, произведение которых лежит в заданном интервале $(\Delta,\ \Delta+\delta)$. Один алгоритм относится к случаю $\delta=\sqrt{\Delta}$, а второй — к $\delta=30\Delta^{1/3}$. Они позволяют в известной криптосистеме выбрать более короткие открытые ключи (в два раза для первого алгоритма и в три раза — для второго).

Ключевые слова: *теория чисел, криптография, криптосистема RSA.*

DOI: https://doi.org/10.47910/FEMJ202016

Введение

В работе [1] Райвест, Шамир и Адлеман предложили алгоритм для процедур обмена секретными ключами и формирования цифровых сигнатур, получивший широкую известность под названием RSA. В качестве личного ключа пользователя выбирается пара (p_1, p_2) больших простых чисел, а их произведение $q{=}p_1p_2$ – открытый ключ. Из открытых ключей администратор сети формирует таблицу открытых ключей пользователей T. Объём T пропорционален числу пользователей и может достигать значительной величины. В работе предлагается следующая модификация RSA-криптосистемы на этапе формирования секретных ключей. Администратор выбирает пару натуральных чисел (Δ, δ) с $0{<}\delta{<}\Delta$. Каждый пользователь формирует личный ключ (p_1, p_2) (пара простых чисел), для которого

$$\Delta < q = p_1p_2 < \Delta + \delta. \tag{1}$$

При таком выборе можно считать, что $k{=}q-\Delta$ – открытый ключ, по которому однозначно вычисляется произведение $q{=}\Delta+k$. Тогда объем таблицы открытых ключей уменьшается приблизительно в

$$\log_2 \Delta/\log_2 \delta$$

[1] Хабаровское отделение Института прикладной математики ДВО РАН, 680000, г. Хабаровск, ул. Дзержинского, 54. Электронная почта: vab@iam.khv.ru

раз. В работе предлагается два алгоритма, реализующих эту идею. В первом случае выбирается $\delta=\sqrt{\Delta}$, что приводит к уменьшению объёма T в два раза. Второй, более трудоемкий алгоритм, дает трехкратный выигрыш, поскольку в нем предполагается, что $\delta=30\Delta^{1/3}$.

1. Некоторые замечания о простых числах

Пусть $1<x<\infty$ и

$$\log_2^2 x \leqslant y \leqslant \Theta(x)x, \tag{2}$$

где $\Theta(x)\to 0$. Эвристические соображения позволяют предположить, что

$$\sum_{x<p\leqslant x+y} 1 = \frac{y}{\log x}(1+o(1)), \tag{3}$$

где сумма слева означает число простых чисел в промежутке $(x, x+y]$. Следовательно, у нас есть основания считать, что случайно выбранное число

$$p \in (x,\, x+y]$$

с вероятностью $1/\log x$ является простым.

Отметим, что Хаксли в [2] доказал асимптотическую формулу (3) с

$$x^{\frac{7}{12}+\varepsilon} < y \leqslant \Theta(x)x$$

$\forall \varepsilon > 0$.

2. Алгоритмы вычисления случайных пар простых чисел, произведение которых лежит в заданном интервале

АЛГОРИТМ 1. Пусть $\delta=\sqrt{\Delta}$. Находим случайное простое p_1 с условием

$$\sqrt{\Delta}/2\log_2^2\Delta < p_1 < \sqrt{\Delta}/\log_2^2\Delta.$$

Затем находим второе случайное p_2, для которого

$$\Delta/p_1 < p_2 < \Delta/p_1 + \log_2^2\Delta.$$

Очевидно, что при таком выборе

$$\Delta < p_1p_2 < \Delta+\delta.$$

Соотношения (2) и (3) в некотором смысле гарантируют, что за $O(\log\Delta)$ испытаний мы найдем требуемую пару (p_1, p_2).

АЛГОРИТМ 2. *Первый этап.*

Предположим, что Δ достаточно большое и $\delta=30\Delta^{1/3}$. Вычислим натуральное u, для которого

$$\sqrt{\Delta} < u < 2\sqrt{\Delta}$$

и при некоторых $\alpha, \beta \in \mathbb{N}$ с $(\alpha, \beta) = 1$

$$\frac{\Delta}{u^2} = \frac{\alpha}{\beta} + \frac{\Theta}{\beta^2}, \tag{4}$$

$$-1 \leqslant \Theta \leqslant 1, \quad \Delta^{1/6}/2 \leqslant \beta \leqslant 2\Delta^{1/6}.$$

Условие (4) проверяется с помощью подходящих дробей

$$\frac{P_i}{Q_i} = \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_s}}}}.$$

Они возникают из разложения Δ/u^2 в цепную дробь

$$\Delta/u^2 = \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_s}}}}.$$

Если для некоторого i выполнено неравенство

$$\Delta^{1/6}/2 \leqslant Q_i \leqslant 2\Delta^{1/6},$$

то полагаем $\alpha = P_i$ и $\beta = Q_i$.

Пусть $I(\Delta)$ – объединение отрезков

$$\left[\frac{\alpha}{\beta} - \frac{1}{\beta^2},\ \frac{\alpha}{\beta} + \frac{1}{\beta^2}\right]$$

по всем взаимно простым натуральным α, β, для которых

$$\Delta^{1/6}/2 \leqslant \beta \leqslant 2\Delta^{1/6}, \quad \beta/4 - 1/\beta \leqslant \alpha \leqslant \beta + 1/\beta.$$

Нетрудно показать, что $\operatorname{mes} I(\Delta) \geqslant c$, где c — некоторая абсолютная постоянная. Кроме того,

$$I(\Delta) \subset \left[\frac{1}{4} - \frac{4}{\Delta^{1/3}},\ 1 + \frac{1}{\Delta^{1/3}}\right].$$

Из вероятностных соображений заключаем, что добиться выполнения условия (4) можно за $O(1)$ раз испытаний путем случайного перебора u.

Второй этап. По формуле Тейлора с остаточным членом в форме Лагранжа для $f(u) = \Delta/u$ находим

$$f(u+t) = f(u) + f'(u)t + f''(\xi)t^2/2,$$

где $u<\xi<u+t$ $(t>0)$. При этом

$$f''(\xi)=\frac{2\Delta}{\xi^3}<\frac{2}{\sqrt{\Delta}}.$$

Выберем натуральное γ из условия

$$\frac{\gamma}{\beta}-\frac{1}{2\beta}\leqslant\frac{\Delta}{u}+\frac{7}{\Delta^{1/6}}\leqslant\frac{\gamma}{\beta}+\frac{1}{2\beta}$$

и целое $0\leqslant t<\beta$ из сравнения

$$\gamma-\alpha t\equiv 0\ (\mathrm{mod}\ \beta).$$

Тогда

$$\begin{gathered}\left|\frac{\Delta}{u+t}-\frac{\gamma-\alpha t}{\beta}+\frac{7}{\Delta^{1/6}}\right|\leqslant\left|\frac{\Delta}{u}+\frac{7}{\Delta^{1/6}}-\frac{\Delta}{u^2}t-\frac{\gamma}{\beta}+\frac{\alpha}{\beta}t\right|+\frac{\beta^2}{\sqrt{\Delta}}\leqslant\\ \leqslant\left|\frac{\Delta}{u}+\frac{7}{\Delta^{1/6}}-\frac{\gamma}{\beta}\right|+\left|\frac{\Delta}{u^2}-\frac{\alpha}{\beta}\right|t+\frac{\beta^2}{\sqrt{\Delta}}<\frac{1}{2\beta}+\frac{1}{\beta}+\frac{\beta^2}{\sqrt{\Delta}}\leqslant\\ \leqslant\frac{1}{\Delta^{1/6}}+\frac{2}{\Delta^{1/6}}+\frac{4}{\Delta^{1/6}}=\frac{7}{\Delta^{1/6}}.\end{gathered}$$

Следовательно, для достаточно большого Δ

$$0<(u+t)\frac{\gamma-\alpha t}{\beta}-\Delta<\frac{14}{\Delta^{1/6}}\left(2\Delta^{1/2}+2\Delta^{1/6}\right)<30\Delta^{1/3}.$$

Далее проверяем на простоту числа

$$p_1=u+t,\quad p_2=\frac{\gamma-\alpha t}{\beta}.$$

Второй этап пройден.

Таким образом, за $O\left(\log^2\Delta\right)$ испытаний путем выбора случайных значений получим нужную пару простых чисел (p_1,p_2).

Список литературы

[1] Rivest R. L., Shamir A., Adleman L., “Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, *Commun. ACM*, **21**:2, (1978), 120–126 doi https://doi.org/10.1145/359340.359342.

[2] Hyxley M. N., “On the difference between consecutive primes”, *Invent. math.*, **15**, (1972), 164–170.

Поступила в редакцию
20 октября 2020 г.

Bykovskii V. A. Calculation of random pairs of primes whose product lies in a given short interval. *Far Eastern Mathematical Journal.* 2020. V. 20. No 2. P. 150–154.

ABSTRACT

The paper proposes heuristic algorithms for constructing pairs of random primes, the product of which lies in a given interval $(\Delta,\, \Delta + \delta)$. One algorithm refers to the case $\delta = \sqrt{\Delta}$, and the second to $\delta = 30\Delta^{1/3}$. They allow in the well-known RSA cryptosystem to choose shorter public keys (twice for the first algorithm and three times for the second).

Key words: *Number theory, cryptography, RSA cryptosystem.*