РАСПАРАЛЛЕЛИВАНИЕ АЛГОРИТМА ФАКТОРИЗАЦИИ «КВАДРАТИЧНОЕ РЕШЕТО»

И.И. Худяшов

Томский государственный университет

На экспоненциальной сложности задачи факторизации числа основана стойкость многих современных криптосистем. В данной работе рассматривается алгоритм факторизации «Квадратичное решето» [1]. Распараллеливание этого алгоритма не снизит его экспоненциальную сложность до полиномиальной, но в некоторых случаях может заметно понизить время его работы.

Алгоритм факторизации «Квадратичное решето» решает задачу 2-факторизации, в которой требуется найти нетривиальный делитель d заданного составного числа n.

Рассматриваемый алгоритм относится к методам, основанным на следующей идее. Пусть n – число, которое необходимо факторизовать, и пусть найдены такие a и b, что $a^2 = b^2 \bmod n$, но $a \neq \pm b \bmod n$; тогда нетривиальный делитель d определяется как наибольший общий делитель чисел $a–b$ и n или $a+b$ и n. Методы отличаются друг от друга способом нахождения чисел a и b, удовлетворяющих указанным условиям.

В алгоритме фиксируется t первых простых чисел, образующих множество S, называемое фактор-базой. Находятся пары чисел (x_i, y_i) такие, что $x_i^2 = y_i \bmod n$ ($i = 1,\ldots t, t+1$), и все простые делители числа y_i входят в множество S. После этого составляется и решается однородная система из t линейных уравнений с булевыми векторами размера $(t+1)$ в качестве решений. Из множества последних берется ненулевой булев вектор, и по нему выписываются пары чисел (x_i, y_i), соответствующие единичным компонентам вектора. Затем вычисляется число a как произведение выписанных x_i и число b как произведение квадратных корней из выписанных y_i. По найденным a и b, если они удовлетворяют описанным выше условиям, находится d – нетривиальный делитель n.

Вся сложность этого алгоритма заключена в поиске $(t+1)$ пар чисел (x_i, y_i), который заключается в переборе $O(2^k)$ чисел, где k – число бит в двоичном представлении числа n. Распараллеливание именно этого шага позволит уменьшить время работы алгоритма. Взаимодействие параллельных процессов осуществляется следующим образом.

Пусть имеется s+1 процессов, один из них назовем управляющим, а остальные – рабочими. На вход управляющему процессу поступают число n и размер t фактор-базы S. Управляющий процесс, после построения им S, рассылает n и S рабочим процессам. Рабочий процесс с номером r строит свои пары чисел (x_i, y_i) по следующим правилам: $x_1 = [\sqrt{n}] + r$, $y_1 = x_1^2 \bmod n$; $x_i = x_{i-1} + k$, $y_i = x_i^2 \bmod n$ для $i > 1$. Для каждой из таких пар проверяется возможность разложения y_i в фактор-базе. Как только находится подходящая пара, она передается управляющему процессу, который после набора необходимого числа пар останавливает работу всех рабочих процессов и продолжает вычисления согласно алгоритму. В случае, если необходимое число пар не найдено в течение заданного интервала времени, управляющий процесс принудительно завершает работу рабочих процессов и сообщает о невозможности факторизации числа за указанное время.

Литература

1. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. – CRC Press, 1997.