Кондачков Е.Д. 5151004/90101

Резюме по статье «Breaking RSA may not be equivalent to factoring»

В статье дается опровержение утверждению, что взлом LE-RSA (RSA с низким показателем) эквивалентен факторизации. В статье приводятся доказательства тому, что нарушение алгоритма на самом деле может быть гораздо проще.

В исследовании используются прямолинейные программы (SLP) для многочленов. SLP для многочлена $f \in R[x_1, \dots, x_k]$ представляет собой последовательность многочленов $\mathrm{f}_0, f_1, f_2, \dots, f_m \in R[x_1, \dots, x_k]$ такая что $f_m = f$ и для всех $i = 1, \dots, m$ значение многочлена f_i является известной величиной и равно либо равен 1, либо переменной x_j или $g_i = g_k \circ g_l$, где $k, l < i$ и $\circ \in \{+, -, *\}$.

Далее определяется понятие прямолинейного сокращения RSA-SLP – алгебраическая схема, в которой элементы выполняют арифметические операции, а также извлекают корни e.

Прямолинейное сокращение – это рандомизированный алгоритм A, который на входе получает n, а на выходе набор RSA-SLP $\{P_1, \dots, P_k\}$. Для не пренебрежимо-малой части $\mathrm{N} \in \mathbb{Z}_{(2)}(n)$ описанный набор должен соответствовать N (с вероятностью, как минимум $\frac{1}{2}$ над случайными битами A).