Кондачков Е.Д. 5151004/90101

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

В статье говорится, что существуют 2 давние проблемы, чтобы доказать или опровергнуть, что взломать систему RSA, также сложно, как разложить на множители целые числа и что взломать протокол Диффи-Хеллмана так же сложно, как вычислить дискретный логарифм.

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 $f_0, f_1, f_2, \dots, f_m \in R[x_1, \dots, x_k]$ такая что $f_m = f$ и для всех $i = 1, \dots, m$ многочлен f_iявляется 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 от факторизации к нарушению LE-RSA. 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 $\{P_1, \dots, P_k\}$. Обозначим выходной набор значением $A(n)$. Для не пренебрежимо-малой части $N \in \mathbb{Z}_{(2)}(n)$ множество $A(n)$ должно соответствовать N (с вероятностью, как минимум $\frac{1}{2}$ над случайными битами A).

Был сделан вывод, что факторизация не сводится к разбиению LE-RSA с использованием прямолинейных сокращений, за исключением простой факторизации.

Как результат исследования было введено 2 теоремы:

Теорема 3.3.

Предположим, что существует прямолинейное сокращение A, время работы которого равно $T(n)$. Далее предположим, что каждый RSA-SLP, сгенерированный при помощи A на входе $N \in \mathbb{Z}_{(2)}(n)$ содержит не более $O(\log T(n))$ радикальных шагов. Тогда существует реальный алгоритм разложения на множители B, время выполнения которого равно $T(n)^{O(1)}$ и он факторизует все $N \in \mathbb{Z}_{(2)}(n)$, которые сделал A.

Существуют более общие класс сокращения – алгебраические.

Алгебраическое сокращение A преобразует элемент $N \in \mathbb{Z}_{(2)}(n)$ при помощи специального оракула O. Время от времени A останавливается и предоставляет RSA-ALP для O. Затем оракул говорит «да» или «нет» в зависимости от того, равен ли RSA-SLP нулю в $\mathbb{Z}_n$. В конечном счете A останавливается и выводит набор RSA-SLP $\{P_1, \dots, P_k\}$, один из которых умножает N с вероятностью не менее $\frac{1}{2}$ (по случайным битам A).

Алгебраическое сокращение может быть преобразовано в реальный алгоритм разложения на множители.

Теорема 3.7.

Предположим, существует алгоритм алгебраического разложения на множители A, время выполнения которого равно $T(n)$. Далее предположим, что каждый из RSA-SLP сгенерированных при помощи A на входе $\in \mathbb{Z}_{(2)}(n)$ содержит не более $O(\log T(n))$ радикальных шагов. Тогда существует реальный алгоритм разложения на множители B, время выполнения которого равно $T(n)^{O(1)}$ и он факторизует все $N \in \mathbb{Z}_{(2)}(n)$, которые сделал A.

Подчеркивается, что результат исследования не указывает на какую-либо слабость системы RSA. Вместо этого он представляет некоторые доказательства того, что взлом LE-RSA может быть проще факторизации. Однако ничто в этой работе не оспаривает того, что это, вероятно, всё равно будет трудноразрешимой задачей.