A.S. Makeyev

<u>On the Estimation of the k-RSA Attack</u>

Keywords: RSA, LLL-algorithm, Coppersmith algorithm.

In this paper, we discuss the attack on the RSA cryptosystem with k modules ($k \geq 2$). We also provide estimation of the attacks's complexity. Finally, we give the experimental results for different modules and open exponents.

А.С. Макеев

ОБ ОЦЕНКЕ ТРУДОЁМКОСТИ АТАКИ НА k-RSA

k-RSA является модификацией RSA, которая была предложена в [Hin07]. В [3] рассматриваются три атаки: в первой атаке приводятся такие модули $n_1, \ldots, n_k$, что существуют $x \in$ и $y_i, z_i \in$, удовлетворяющие равенствам

$$e_i x \quad y_i \varphi(n_i) = z_i, 1 \leq i \leq k,$$

где $\varphi(n_i)$ – функция Эйлера,   – кольцо целых чисел, e_i – открытые экспоненты RSA. В [3] показано, что число n_i факторизуется за полиномиальное время, если

$$x, y_i < n^{\delta}, |z_i| < \{(p_i \quad q_i)/3(p_i + q_i)\} y_i n^{0,25},$$

где p_i, q_i – множители n_i, $\delta = \{k/2(k+1)\}$, $n = \min\{n_i \mid i \in \{2, \ldots, k\}\}$.

Атаки на k-RSA основаны на применении LLL-алгоритма [1] и метода Копперсмита [2]. С помощью LLL-алгоритма [1] находится вектор наименьшей длины в решётке . Как следует из [1], с помощью этого алгоритма можно получить такой базис $\{b_1, \ldots, b_w\}$, что выполняется условие

$$\|b_1\| \leq \|b_2\| \leq \quad \leq \|b_i\| \leq 2^{\frac{w(w-1)}{4(w+1-i)}} \det(\quad)^{\frac{1}{w+1-i}}, 1 \leq i \leq w,$$

где $\det(\quad)$ – определитель решётки .

Метод Копперсмита [2] применяется для нахождения решения системы уравнений от двух переменных за полиномиальное время, а также факторизации модуля $n = pq$ криптосистмы RSA, если половина значимых или наименее значимых битов числа p известна.

В работе [3] предложена следующая атака на k-RSA. Выбирается наибольший модуль n из данных k модулей$n_1, \ldots, n_k (k \geq 2)$. Далее строится матрица M, первая строка которой

$$(1 \quad [ce_1/(n_1+1)] \quad [ce_2/(n_2+1)] \ \ldots \quad [ce_k/(n_k+1)]),$$

где $c = \left(3^{k+1} \quad 2^{\{(n+1)(n-4)\}/4} \quad \varepsilon^{-k-1}\right)$, $\varepsilon = \sqrt{5} n^{(\delta-1)/2}, \delta = k/\{2(k+1)\}$.

Остальные k строк матрицы M задаются матрицей

$$M' = \begin{bmatrix} 0 & c & 0 & \ldots & 0 \\ 0 & 0 & c & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & c \end{bmatrix}.$$

Пусть K – результат применения LLL-алгоритма к матрице M. Далее находится матрица $K \quad M^{-1}$, элементы первой строки которой$(a_1, a_2, \ldots, a_{k+1})$ обозначим как

$$x = a_1, y_1 = a_2, y_2 = a_3, \ldots, y_k = a_{k+1}\ (x, y_1, \ldots, y_k \geq 0).$$

Тогда $s_i = (n_i + 1 \quad (e_i x)/y_i)$, $d_i = \sqrt{s_i^2 \quad 4n_i}$, $\widetilde{p_i} = \frac{1}{2}(s_i + d_i)(i = 1, \ldots, k)$. Применяя метод Копперсмита [Etr10] и используя $\widetilde{p_i}$, находятся множители $p_1, \ldots, p_k$ модулей $n_1, \ldots, n_k$ соответственно.

В [3] описана атака на криптосистему k-RSA, основанная на применении LLL-алгоритма и метода Копперсмита, но не получена оценка трудоёмкости атаки. В данной работе оценивается теоретическая трудоёмкость этой атаки и проводится экспериментальная оценка.

Трудоёмкость атаки зависит от трудоёмкости следующих этапов: 1) LLL-алгоритма; 2) метода Копперсмита. Приведём оценки трудоёмкостей каждого из этих этапов. В качестве элементарной операции (э.о.) будем считать операции умножения, сложения и присвоения.

1) Трудоёмкость LLL-алгоритма:

а) трудоёмкость ортогонализации Грамма–Шмидта – $O(m^2)$э.о.;

б) трудоёмкость сокращения решетки – $O(m^3\theta)$э.о.*,* где θ – параметр, зависящий от исходной матрицы.

2) Трудоёмкость алгоритма Копперсмита:

а) построение многочленов – $O(\delta m^2)$э.о.;

б) построение матрицы по полученным многочленам – $O(\delta m^2)$э.о.;

в) получение многочлена и нахождение его корня – $O(\{m^3\theta\} + \{len\})$э.о., где len – длина корней многочлена.

Таким образом, искомая трудоёмкость равна $O(m^3\theta + \delta m^2)$э.о.

Экспериментальные результаты приведены в таблице.

Таблица

n, бит	8	16	32	64	128	256	512	1024
Время, мс	0,039	0,133	0,052	0,056	0,064	0,079	0,123	0,141

Из таблицы следует, что полученные в ходе эксперимента значения совпадают с теоретическими.

СПИСОК ЛИТЕРАТУРЫ:

1. Helfer Etienne: LLL lattice basis reduction algorithm. In: ago.epfl.ch/_media/en/projects/bachelor_semester/rapportetiennehelfer.pdf

2. Chris Peikert: Coppersmith, Cryptanalysis. In: Lattices in Cryptograhy, lecture 4, Georgia Tech, Fall 2013.

3. Abderrahmane Nitaj, Muhammad R.K. A., Dieaa I. N.: New Attacks on the RSA Cryptosystem. In:eprint.iacr.org/2014/549, 2014.

REFERENCES:

1. Helfer Etienne: LLL lattice basis reduction algorithm. In: algo.epfl.ch/_media/en/projects/bachelor_semester/rapportetiennehelfer.pdf

2. Chris Peikert: Coppersmith, Cryptanalysis. In: Lattices in Cryptograhy, lecture 4, Georgia Tech, Fall 2013.

3. Abderrahmane Nitaj, Muhammad R. K. A., Dieaa I. N.: New Attacks on the RSA Cryptosystem. In: eprint.iacr.org/2014/549, 2014.