R.D. Ginyatullin, I.O. Motroni

About Computational Complexity of Dujella and Coppersmith Attacks

Keywords: RSA, Wiener theorem, Dujella theorem, Coppersmith theorem
Annotation: In this paper we consider attacks on RSA, based on the approaches by Wiener, Coppersmith and Dujella. Comparison of computational complexity of attacks and conclusions of the appropriateness of their use was made.

Р.Д. Гинятуллин, И.О. Мотрони

О ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ АТАК ДЮЖЕЛЛА И КОППЕРСМИТА

В работе рассматриваются атаки на RSA, основанные на подходах, предложенных Винером, Копперсмитом и Дюжелла. Произведено сравнение вычислительных сложностей атак, и сделаны выводы о целесообразности их использования. Рассмотрены границы их применения.

RSA – одна из самых распространенных в мире шифрсистем с открытым ключом. Её можно использовать как для шифрования, так и для создания цифровых подписей. С момента своего создания RSA успешно противостоит многочисленным попыткам криптоаналитического вскрытия. Стойкость криптосистемы основана на трудоемкости факторизации больших чисел.

Пусть p, q – простые числа, длина в битах которых совпадает, $n = pq$. В RSA используются открытый ключ e и секретный ключ d, удовлетворяющие условиям $\text{НОД}(e, \varphi(n)) = 1$, $ed \equiv 1 \pmod{\varphi(n)}$, где φ – функция Эйлера.

Пусть x – блок открытого текста из Z_n. Функция зашифрования криптосистемы RSA задается условием $y = x^e \bmod n$, а функция расшифрования – $x = y^d \bmod n$.

Существует ряд условий на параметры системы RSA, при которых она является нестойкой. Одна из известных слабостей – секретная экспонента d небольшой длины. Для таких секретных экспонент известна полиномиальная атака Копперсмита [Cop97], позволяющая восстанавливать значение $d < n^{0.292}$. Существует класс атак на d, основанных на непрерывных дробях. Например, это атака Винера [Win90] и её различные модификации (атаки Дюжелла [Duj04], де Вегера [Weg02]). Атаки, основанные на вычислении цепных дробей, находят ключ за полиномиальное время, но для d небольшой длины, например, атака Винера восстанавливает экспоненту $d < \frac{1}{3}n^{0.25}$.

Атака Винера с модификацией Копперсмита основывается на трех теоремах.

Теорема (Винера) [Win90]. Пусть p, q, d в криптосистеме RSA удовлетворяют условиям $p < q < 2p$, $d < \frac{1}{3}\sqrt[4]{n}$. Тогда по открытому ключу можно вычислять секретный ключ d.

Теоремы (Копперсмита)[Blm04].

Пусть существует аппроксимация p с ошибкой не более $n^{\frac{1}{4}}$. Тогда трудоемкость факторизации n оценивается как $O(\log n)$.

Пусть $c \leq 1$, $p - q \geq cn^{\frac{1}{2}}$, e знак прин. $Z^*_{\varphi(n)}$ и удовлетворяет условию

$$ex + y = k\varphi(n),$$

где $0 < x \leq \frac{1}{3}n^{\frac{1}{4}}$ и $|y| \leq cn^{-\frac{3}{4}}ex$. Тогда n факторизуется за полиномиальное время.

В алгоритме Копперсмита используется значение β, получаемое с помощью следующих равенств:

$$s = n + 1 - \frac{ex}{k}, t = \sqrt{s^2 - 4n}, \qquad \beta = 1/2(s + t).$$

Модификация применима, если $d < n^{0.292}$.

В работе [Ver97] предложено искать отношение k/d среди дробей вида $\frac{rp_{m+1}+sq_m}{rq_{m+1}+sq_m}$, где p_i/q_i – i-я подходящая дробь для числа e/n. Так как определитель системы

$$rp_{m+1} + sp_m = k,$$
$$rq_{m+1} + sq_m = d$$

всегда обратим, то для любого mсуществуют такие целые r и s, что выполняется равенство $\frac{k}{d} = \frac{rp_{m+1}+sp}{rq_{m+1}+sq_m}$. В работе [Duj09], переформулирован результат из [Ver97], и указано такое m, что для чисел r и s выполняются следующие оценки:

$$r < \max\left\{\sqrt{2{,}122(a_{m+3} + 2)}(a_{m+2} + 1)D, \sqrt{2{,}122(a_{m+2} + 2)}D\right\},$$
$$s < \max\left\{2\sqrt{2{,}122(a_{m+3} + 2)}D, \sqrt{2{,}122(a_{m+2} + 2)}(a_{m+1} + 1)D\right\},$$

где $d' = d/n^{0{,}25}$. В работе [Duj09] получены оценки для чисел r и s в случае, когда дробь $\frac{k}{d}$ ищется среди дробей вида $\frac{rp_{m+1}+sp_m}{rQ_{m+1}+sQ_m}, \frac{rp_{m+2}-sp_{m+1}}{rq_{m+2}-sq_{m+1}}, \frac{rp_{m+3}+sp_{m+2}}{rq_{m+3}+sq_{m+2}}$ для специально выбранного m. и экспериментально установлено, что с вероятностью 98 % числа r и s не превосходят $4d'$. В [Duj09] эти оценки получены с помощью неравенств $\frac{2e}{n\sqrt{n}} < \frac{k}{d} - \frac{e}{n} < \frac{2{,}122e}{n\sqrt{n}} < \frac{2{,}122D^2}{d^2}$теоремы:

Теорема Дюжелла [Duj04, теорема 1]**.** Пусть $\alpha \in N$, a и b – простые числа, удовлетворяющие условию $\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^2}$, где c – некоторая константа. Тогда НОД$(a, b) = (rp_{m+1} \pm sp_m, rq_{m+1} \pm sq_m)$ для таких целых r, s и m, что $rs < 2c$.

Атака Винера может применяться при $n \le n^{0{,}25}/3$. Такая граница будет вычислена атакой Дюжелла ($d' = d/n^{0{,}25} \cong d' = \frac{1}{3}$), однако, как видно из табл.1 [Zhu13], увеличение длины ключа резко увеличивает время работы атаки.

Таблица 1. Эксперименты с 1024-битовым модулем

d'	d, бит	Время, с	Память, МБ
10^3	266	0,2	<1
10^6	276	135	48
10^7	280	1500	480
10^8	283	17200	4800
10^9	286	193000	48000

Атака Винера, модифицированная с помощью алгоритма Копперсмита, находит $d < n^{0{,}292}$. Подобная граница, будучи вычисляемой с помощью алгоритма Дюжелла, подразумевает перебор $3d'^2$ значений (3 возможных дроби, итерация и по r, и по s), где $d' = d/N^{0{,}25} = n^{0{,}042}$. Для модуля n длины 2048 имеет место оценка $d' = 2^{2048 \cdot 0{,}042}$. Отсюда видно, что длина d' порядка 2^{86}, поэтому полный перебор ключа невозможен.

Таким образом, атака Дюжелла, не дает преимущества по сравнению с атакой Копперсмита: помимо возрастающего объема памяти, необходимого для вычислений, она имеет большую вычислительную сложность при $d \sim n^{0,292}$.

СПИСОК ЛИТЕРАТУРЫ:

1. [Win90] Wiener M.J. Cryptanalysis of short RSA secret exponents // IEEE Trans. Inform. Theory. 1990. V. 36. P. 553–558.
2. [Blm04] Blömer J., May A. «A Generalized Wiener Attack on RSA», 2004.
3. [Ver97] Verheul E.R., van Tilborg H.C.A. Cryptanalysis of 'less short' RSA secret exponents // Appl.Algebra Eng.Comm.Computing. 1997. V. 8. P. 425– 435.
4. [Duj04] Dujella A. Continued fractions and RSA with small secret exponent // Tatra Mt. Math. Publ. 2004. V. 29. P. 101–112.
5. [Duj09] Dujella A. A variant of Wiener's attack on RSA, Computing. 2009. V. 85. P. 77–83.
6. [Cop97] D. Coppersmith, «Small solutions to polynomial equations and low exponent vulnerabilities», Journal of Cryptology. 1997. Vol. 10(4). Pp. 223–260.
7. [Weg02] Weger B. Cryptanalysis of RSA with small prime difference // Appl. AlgebraEng. Comm. Computing. 2002. V. 13. P. 17–28.
8. [Zhu13] Жуков К.Д. Об обобщении метода Дюжелла // Математические вопросы криптографии. 2013. Т. 4, вып. 3. С. 7–19.

REFERENCES:

1. [Win90] Wiener M.J. Cryptanalysis of short RSA secret exponents // IEEE Trans. Inform. Theory. 1990. V. 36. Pp. 553–558.
2. [Blm04] Blömer J., May A. «A Generalized Wiener Attack on RSA», 2004.
3. [Ver97] Verheul E.R., van Tilborg H.C.A. Cryptanalysis of 'less short' RSA secret exponents // Appl. Algebra Eng. Comm. Computing. 1997. V. 8. Pp. 425– 435.
4. [Duj04] Dujella A. Continued fractions and RSA with small secret exponent // Tatra Mt. Math. Publ. 2004. V. 29. P. 101–112.
5. [Duj09] Dujella A. A variant of Wiener's attack on RSA, Computing. 2009. V. 85. Pp. 77–83.
6. [Cop97] D. Coppersmith, «Small solutions to polynomial equations and low exponent vulnerabilities», Journal of Cryptology. 1997. Vol. 10(4). Pp. 223–260.
7. [Weg02] Weger B. Cryptanalysis of RSA with small prime difference // Appl. AlgebraEng. Comm. Computing. 2002. V. 13. Pp. 17–28.
8. [Zhu13] Zhukov K.D. On a generalization of the Dujella method, 2013.