ПОЛИНОМИАЛЬНАЯ ЭКВИВАЛЕНТНОСТЬ ВЫЧИСЛЕНИЯ ФУНКЦИИ ЭЙЛЕРА RSA-МОДУЛЯ И ПОИСКА СЕКРЕТНОГО КЛЮЧА В КВАДРАТИЧНЫХ ЕВКЛИДОВЫХ КОЛЬЦАХ

М. М. Васьковский

Белорусский государственный университет
Минск, Беларусь
e-mail: vaskovskii@bsu.by

В настоящей работе доказана полиномиальная эквивалентность вычисления функции Эйлера RSA-модуля и нахождения секретного ключа в квадратичных евклидовых кольцах.

Ключевые слова: RSA-криптосистема; квадратичное евклидово кольцо; полиномиальный алгоритм.

POLYNOMIAL EQUIVALENCE OF COMPUTING EULER'S FUNCTION FROM RSA MODULUS AND SEARCHING FOR PRIVATE KEY IN EUCLIDEAN QUADRIATIC DOMAINS

M. M. Vaskouski

Belarusian State University
Minsk, Belarus

In the present paper there was proved polynomial equivalence of computing Euler's function from RSA-modulus and searching for private key in Euclidean quadratic domains.

Keywords: RSA-cryptosystem; quadratic Euclidean domain; polynomial algorithm.

В 1978 г. была построена первая криптосистема с открытым ключом – RSA-криптосистема, основанная на вычислительной сложности задачи факторизации больших натуральных чисел, а также доказано существование вероятностного алгоритма полиномиальной сложности для факторизации RSA-модуля по известному секретному ключу [1]. Детерминированный полиномиальный алгоритм факторизации RSA-модуля по известному секретному ключу, основанный на теореме Копперсмита о малых решениях полиномиальных уравнений, построен в работе [2]. В статьях [3], [4] построен аналог RSA-криптосистемы в квадратичных факториальных кольцах, доказаны аналоги теоремы Винера о малом секретном ключе и предложен метод защиты против атаки повторного шифрования.

Цель настоящей работы состоит в доказательстве возможности эффективно реализовать аналог RSA-криптосистемы в квадратичных евклидовых кольцах, в том числе и в действительных, а также в обосновании полиномиальной эквивалентности по-

иска секретного ключа и вычисления функции Эйлера модуля RSA-криптосистемы в квадратичных евклидовых кольцах.

Пусть $\theta \neq 1$ – целое число, свободное от квадратов Через $\mathcal{O}_K$ обозначим кольцо всех целых алгебраических элементов квадратичного поля $K = \mathbb{Q}(\sqrt{\theta})$. Известно, что $\mathcal{O}_K = \{a + b\sqrt{\theta} : a, b \in \mathbb{Z}\}$ при $\theta \not\equiv 1 (\mathrm{mod}\ 4)$, $\mathcal{O}_K = \left\{\frac{a+b\sqrt{\theta}}{2} : a, b \in \mathbb{Z}, a \equiv b (\mathrm{mod}\ 2)\right\}$ при $\theta \equiv 1 (\mathrm{mod}\ 4)$ [5]. Определим норму в кольце $\mathcal{O}_K$ следующим образом: $\mathrm{Nm}(a + b\sqrt{\theta}) = |a^2 - \theta b^2|$, $a + b\sqrt{\theta} \in \mathcal{O}_K$, $a, b \in \mathbb{Q}$. Существует в точности 5 мнимых квадратичных евклидовых колец $\mathcal{O}_K$ (при $\theta = -1, -2, -3, -7, -11$) и 16 действительных квадратичных евклидовых колец $\mathcal{O}_K$ (при $\theta = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$) [5]. Пусть $\mathcal{O}_K^\times$ – множество всех обратимых элементов кольца $\mathcal{O}_K$ в объединении с нулем. Для любого $N \in \mathcal{O}_K \setminus \mathcal{O}_K^\times$ обозначим через $\mathcal{O}_{K,N}$ и $\mathcal{O}_{K,N}^\times$ полную систему вычетов и приведенную систему вычетов по модулю N. Функция Эйлера $\varphi_K(N) = |\mathcal{O}_{K,N}^\times|$ в кольце $\mathcal{O}_K$ может быть легко вычислена с помощью соотношения $\varphi_K(N) = \prod_{i=1}^{k} (\mathrm{Nm}(p_i))^{q_i - 1} (\mathrm{Nm}(p_i) - 1)$, если известно каноническое разложение числа $N = \prod_{i=1}^{k} p_i^{q_i}$, где p_i $(i = 1, \dots, k)$ – простые элементы кольца $\mathcal{O}_K$ (попарно взаимно простые), q_i $(i = 1, \dots, k)$ – натуральные числа [4].

В дальнейшем будем предполагать, что кольцо $\mathcal{O}_K$ является евклидовым с определенной выше нормой.

Приведем алгоритм криптосистемы RSA в кольце $\mathcal{O}_K$, следуя работе [4]. Любой пользователь A выбирает два больших простых числа $p_A, q_A \in \mathcal{O}_K$, $(p_A, q_A) = 1$, и вычисляет $\varphi_K(N_A)$, где $N_A = p_A q_A$. Затем пользователь A выбирает случайное натуральное число $e_A \in [1, \varphi_K(N_A)]$, $(e_A, \varphi_K(N_A)) = 1$, и с помощью расширенного алгоритма Евклида находит натуральное число d_A такое, что $e_A d_A \equiv 1 (\mathrm{mod}\ \varphi_K(N_A))$. Пара (N_A, e_A) – это открытый ключ пользователя A, пара (N_A, d_A) – секретный ключ пользователя A. Функции шифрования $f_A : \mathcal{O}_{K,N_A} \to \mathcal{O}_{K,N_A}$ и дешифрования $f_A^{-1} : \mathcal{O}_{K,N_A} \to \mathcal{O}_{K,N_A}$ задаются следующим образом: $f_A(x) = x^{e_A} (\mathrm{mod}\ N_A)$, $f_A^{-1}(x) = x^{d_A} (\mathrm{mod}\ N_A)$. Корректность работы криптосистемы вытекает из теоремы Эйлера [4]. Любой набор (N_A, e_A, d_A), удовлетворяющий перечисленным выше условиям, будем называть параметрами RSA-криптосистемы в кольце $\mathcal{O}_K$. Отметим, что знание $\varphi_K(N_A)$ позволяет за полиномиальное время найти секретный ключ d_A и, как следствие, вскрыть криптосистему.

Предложение 1. Операции сложения, умножения, деления с остатком в кольце $\mathcal{O}_K$ имеют такую же сложность, как и в кольце целых чисел, т. е. для любого натурального N и любых $a, b \in \mathcal{O}_K$, $\mathrm{Nm}(a) \leq N$, $\mathrm{Nm}(b) \leq N$, любая из указанных операций над числами a, b может быть выполнена за $O(f(N))$ битовых операций, где $f(n)$ – оценка числа битовых операций, необходимых для выполнения аналогичной операции в кольце целых чисел над любыми числами $c, d \in \mathbb{Z}$, $|c| \leq \sqrt{N}$, $|d| \leq \sqrt{N}$.

Доказательство. Для операций сложения и умножения утверждение очевидно. Докажем утверждение для операции деления с остатком. Для каждых $\lambda \in \mathcal{O}_K$ и действительного $r \in (0,1)$ определим окрестность $U[\lambda; r]$ точки λ радиуса r следующим образом: $U[\lambda; r] = \{\beta \in K : \mathrm{Nm}(\beta - \lambda) \leq r\}$. Определим фундаментальную прямоугольную область $F_K = \left\{r + s\sqrt{\theta} : r, s \in \mathbb{Q} \cap \left[0, \frac{1}{2}\right]\right\}$ при $\theta \not\equiv 1 (\mathrm{mod}\ 4)$ и $F_K = \left\{r + s\sqrt{\theta} : r \in \mathbb{Q} \cap \left[0, \frac{1}{2}\right], s \in \mathbb{Q} \cap \left[0, \frac{1}{4}\right]\right\}$ при $\theta \equiv 1 (\mathrm{mod}\ 4)$. Для любого θ, такого что кольцо $\mathcal{O}_K$ является евклидовым, существует конечное множество $G_\theta \subset \mathcal{O}_K$, для которого имеет

место включение $F_K \subseteq \bigcup_{\lambda \in G_\theta} U[\lambda; 0{,}996]$. Действительно, непосредственной проверкой можно убедиться, что при $\theta \notin \{33, 37, 41, 57{,}73\}$ можно положить $G_\theta = \{0{,}1, 2, -1{,}4 - \sqrt{\theta}, 2 + \sqrt{\theta}, -5 - \sqrt{\theta}, 3 + \sqrt{\theta}, 6 - \sqrt{\theta}, 7 - \sqrt{\theta}, 19 - 4\sqrt{\theta}, -2 + \sqrt{\theta}, -7 + 2\sqrt{\theta}, -90 + 21\sqrt{\theta}, -430 + 99\sqrt{\theta}\}$, а при $\theta \in \{33, 37, 41, 57{,}73\}$ можно положить $G_\theta = \left\{1{,}2, -1, -\frac{3}{2} + \frac{1}{2}\sqrt{\theta}, \frac{5}{2} + \frac{1}{2}\sqrt{\theta}, -6 + \sqrt{\theta}, \frac{11}{2} - \frac{1}{2}\sqrt{\theta}, -\frac{21}{2} + \frac{3}{2}\sqrt{\theta}, -10 - \sqrt{\theta}, -27 - 3\sqrt{\theta}, 7 + \sqrt{\theta}, \frac{57}{2} + \frac{7}{2}\sqrt{\theta}\right\}$. Нетрудно видеть, что для любых ненулевых $a, b \in \mathcal{O}_K$ найдутся $q, r \in \mathcal{O}_K$ такие, что $a = bq + r$ и $\mathrm{Nm}(r) \leq 0{,}996\mathrm{Nm}(b)$. Укажем алгоритм, который находит такие q, r со сложностью целочисленного деления с остатком. Пусть $a = a_1 + a_2\sqrt{\theta}$, $b = b_1 + b_2\sqrt{\theta}$, имеем $\frac{a}{b} = \alpha_1 + \alpha_2\sqrt{\theta}$, где $\alpha_1 = \frac{a_1 b_1 - \theta a_2 b_2}{b_1^2 - \theta b_2^2}$, $\alpha_2 = \frac{a_2 b_1 - a_1 b_2}{b_1^2 - \theta b_2^2}$. Положим $r_1 = \{\alpha_1\}$, $r_2 = \{\alpha_2\}$. Определим числа r_1', r_2' следующим образом. Пусть $\theta \not\equiv 1 (\mathrm{mod}\ 4)$: если $r_i < \frac{1}{2}$, то положим $r_i' = r_i$, иначе $r_i' = 1 - r_i$. Пусть $\theta \equiv 1 (\mathrm{mod}\ 4)$: $r_1' = r_1$ при $r_1 < \frac{1}{2}$, $r_1' = r_1 - \frac{1}{2}$ при $r_1 \geq \frac{1}{2}$, $r_2' = r_2$ при $r_2 < \frac{1}{4}$, $r_2' = \frac{1}{2} - r_2$ при $\frac{1}{4} \leq r_2 < \frac{1}{2}$, $r_2' = r_2 - \frac{1}{2}$ при $\frac{1}{2} \leq r_2 < \frac{3}{4}$, $r_2' = 1 - r_2$ при $r_2 \geq \frac{3}{4}$. Очевидно, что число $r' = r_1' + r_2'\sqrt{\theta}$ принадлежит фундаментальной прямоугольной области F_K. За O(1) операций можем найти $\lambda \in G_\theta$ такое, что $r' \in U[\lambda; 0{,}996]$. Теперь требуемые числа q, r восстанавливаются очевидным образом. Следовательно, сложность деления с остатком чисел a, b определяется сложностью вычисления значений α_1, α_2.

Следствие 1. Модулярные арифметические операции и алгоритм Евклида в кольце $\mathcal{O}_K$ для чисел $a, b \in \mathcal{O}_K$, $\mathrm{Nm}(a) \leq N$, $\mathrm{Nm}(b) \leq N$, имеют такую же сложность, как аналогичные целочисленные операции для чисел $c, d \in \mathbb{Z}$, $|c| \leq \sqrt{N}$, $|d| \leq \sqrt{N}$.

Следствие 2. Алгоритм RSA-криптосистемы в кольце $\mathcal{O}_K$ с модулями, не превосходящими по норме числа N, может быть реализован с такой же сложностью, как и алгоритм RSA-криптосистемы в кольце целых чисел с модулями, не превосходящими числа $\sqrt{N}$.

Теорема 1. Пусть (N, e, d) – параметры RSA-криптосистемы в евклидовом кольце $\mathcal{O}_K$. Предположим, что известен секретный ключ d, тогда существует алгоритм сложности $O(\log^3(\mathrm{Nm}(N)))$, который с вероятностью не менее $\frac{1}{2}$ находит факторизацию модуля N.

Доказательство. Пусть $s = ed - 1 = 2^t u$, $t, u \in \mathbb{N}$, u – нечетное. Так как $\varphi_K(N) | s$, то $x^s \equiv 1 (\mathrm{mod}\ N)$ для любого $x \in \mathcal{O}_{K,N}^\times$. Обозначим через S_N множество всех $a \in \mathcal{O}_{K,N}^\times$, для которых выполняется одно из условий: 1) $a^u \equiv 1 (\mathrm{mod}\ N)$; 2) существует $k \in \{0, \dots, t-1\}$ такое, что $a^{2^k u} \equiv -1 (\mathrm{mod}\ N)$. Пусть $A = \mathcal{O}_{K,N}^\times \setminus S_N$. Выберем произвольное $a \in A$ и найдем наименьшее натуральное k такое, что $a^{2^k u} \equiv 1 (\mathrm{mod}\ N)$. Пусть $b = a^{2^{k-1} u}$, тогда $b^2 \equiv 1 (\mathrm{mod}\ N)$ и $b \not\equiv \pm 1 (\mathrm{mod}\ N)$. Следовательно, $(b - 1, N)$ – нетривиальный делитель числа N. Согласно следствию 1, этот наибольший общий делитель можно вычислить с помощью алгоритма Евклида за $O(\log^3(\mathrm{Nm}(N)))$ битовых операций. Так как $|S_N| \leq \frac{\varphi_K(N)}{2}$ [4, теорема 6], то описанный алгоритм найдет факторизацию модуля N с вероятностью не менее $\frac{1}{2}$ за $O(\log^3(\mathrm{Nm}(N)))$ битовых операций [4, предложение 7].

Теорема 2. Пусть $(N = pq, e, d)$ – параметры RSA-криптосистемы в евклидовом кольце $\mathcal{O}_K$, где p, q – большие простые числа кольца $\mathcal{O}_K$, $\mathrm{Nm}(p)$ и $\mathrm{Nm}(q)$ имеют оди-

наковую битовую длину, $ed \leq \left(\mathrm{Nm}(N)\right)^{3/2}$. Если известен секретный ключ d, то значение $\varphi_K(N)$ можно вычислить за $O(\log^2(\mathrm{Nm}(N)))$ битовых операций.

Доказательство. Пусть $\mathrm{Nm}(p) \leq \mathrm{Nm}(q)$. Нетрудно видеть, что $\mathrm{Nm}(p) \leq$ $\leq 2\left(\mathrm{Nm}(N)\right)^{\frac{1}{2}}$. Отсюда получаем неравенства $\mathrm{Nm}(p) + \mathrm{Nm}(q) < 3\left(\mathrm{Nm}(N)\right)^{\frac{1}{2}} \leq$ $\leq \frac{1}{2}\mathrm{Nm}(N)$, справедливые для всех N таких, что $\mathrm{Nm}(N) \geq 36$ (в дальнейшем будем рассматривать только такие N). Теперь получаем, что $\varphi_K(N) = \mathrm{Nm}(N) + 1 -$ $-\left(\mathrm{Nm}(p) + \mathrm{Nm}(q)\right) > \frac{1}{2}\mathrm{Nm}(N)$. Так как $ed \equiv 1\left(\mathrm{mod}\, \varphi_K(N)\right)$, то число $k = \frac{ed-1}{\varphi_K(N)}$ является натуральным. Положим $k_1 = \frac{ed-1}{\mathrm{Nm}\,(N)}$. Тогда $k - k_1 < \frac{6(ed-1)}{\left(\mathrm{Nm}\,(N)\right)^{\frac{3}{2}}} \leq 6$. Следовательно, $k = [k_1] + i$ для некоторого $i \in \{0,1,2,3,4,5\}$. Таким образом, истинное значение k может быть найдено за $O(\log^2(\mathrm{Nm}(N)))$ битовых операций, а вместе с ним и значение $\varphi_K(N)$.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. 1978. Vol. 21. P. 120–126.
2. Coron J. S., May A. Deterministic polynomial-time equivalence of computing the RSA secret key and factoring // J. Cryptology. 2007. Vol. 20. № 1. P. 39–50.
3. Vaskouski M., Kondratyonok N. An analogue of RSA-cryptosystem in quadratic unique factorization domains // Doklady NASB. 2015. № 5. P. 18–23.
4. Vaskouski M., Kondratyonok N., Prochorov N. Primes in quadratic unique factorization domains // J. Number Theory. 2016. Vol. 168. P. 101–116.
5. Selfridge J. L., Lacampagne C. B., Eggleton R. B. Euclidean quadratic fields // Amer. Math. Monthly. 1992. Vol. 99. № 9. P. 829–837.