Доклады Национальной академии наук Беларуси

2015 **сентябрь–октябрь** **Том 59 № 5**

UDC 511.622+519.719.2

M. VASKOUSKI, N. KONDRATYONOK

ANALOGUE OF THE RSA-CRYPTOSYSTEM IN QUADRATIC UNIQUE FACTORIZATION DOMAINS

(Communicated by Academician N. A. Izobov)

Belarusian State University, Minsk, Belarus
vaskovskii@bsu.by; nkondr2006@rambler.ru

In the article, the analogue of a RSA-cryptosystem in general quadratic unique factorization domains is obtained. A scheme of digital signature on the basis of the generalized RSA-cryptosystem is suggested. The analogue of Wiener's theorem on low private key is obtained. We prove the equivalence of the problems of generalized RSA-modulus factorization and private key search when the domain of all algebraic integer elements of the quadratic field is Euclidean. A method to secure the generalized RSA-cryptosystem of the iterated encryption cracking is proposed.

Keywords: RSA-cryptosystem, digital signature, unique factorization domain, euclidean domain, quadratic number field.

М. М. ВАСЬКОВСКИЙ, Н. В. КОДРАТЕНОК

АНАЛОГ RSA-КРИПТОСИСТЕМЫ В КВАДРАТИЧНЫХ ФАКТОРИАЛЬНЫХ КОЛЬЦАХ

Белорусский государственный университет, Минск, Беларусь
vaskovskii@bsu.by; nkondr2006@rambler.ru

Цель данной работы заключается в построении аналога RSA-криптосистемы в квадратичных факториальных кольцах. В работе предложен алгоритм построения электронной цифровой подписи. Доказан аналог поиска секретного ключа и факторизации модуля криптосистемы в случае, когда целые алгебраические элементы поля образуют Евклидово кольцо. Даны ограничения на параметры криптосистемы для защиты от метода повторного цифрования. Так же проведено исследование скорости работы и взлома полученной криптосистемы.

Ключевые слова: RSA-криптосистема, электронная цифровая подпись, факториальное кольцо, евклидово кольцо, квадратичное числовое поле.

In 1978 there was constructed [1] one of the most high-usage public-key cryptosystem, which is named as RSA-cryptosystem and is based on the difficulty of the factorization of big natural numbers. In the papers [2–6] there were obtained and investigated analogues of RSA-cryptosystem based on using of polynomials and Gaussian integers instead of natural numbers. The present paper is devoted to constructing and analysis of RSA-cryptosystem in the domain of algebraic integer elements of a general quadratic number field.

Let $\rho \neq 1$ be an integer squarefree number. Denote by $\mathbb{Z}[\sqrt{\rho}]$ the domain of all integer algebraic elements of the quadratic number field $\mathbb{Q}[\sqrt{\rho}]$ and we assume that $\mathbb{Z}[\sqrt{\rho}]$ is a unique factorization domain. It is known [7] that $\mathbb{Z}[\sqrt{\rho}] = \{a + b\sqrt{\rho} \mid a, b \in \mathbb{Z}\}$ if $\rho \not\equiv 1 (\mathrm{mod}\ 4)$, and $\mathbb{Z}[\sqrt{\rho}] = \{(a + b\sqrt{\rho})/2 \mid a, b \in \mathbb{Z}, a \equiv b (\mathrm{mod}\ 2)\}$ if $\rho \equiv 1 (\mathrm{mod}\ 4)$. Let the norm v_ρ in $\mathbb{Z}[\sqrt{\rho}]$ be defined by the relation $v_\rho(a + b\sqrt{\rho}) = |a^2 - \rho b^2|$, $a + b\sqrt{\rho} \in \mathbb{Z}[\sqrt{\rho}]$. We recall that a domain $\mathbb{K}$ is called Euclidean if one can define a function $\nu : \mathbb{K} \setminus \{0\} \to \mathbb{N} \cup \{0\}$ such that for any a, $b \in \mathbb{K} \setminus \{0\}$ the inequality $\nu(ab) \geq \nu(a)$ holds, and for any a, $b \in \mathbb{K} \setminus \{0\}$ one can find elements q, $r \in \mathbb{K}$ such that $a = bq + r$, where $r = 0$ or $\nu(r) < \nu(b)$. There exist exactly five Euclidean imaginary quadratic domains $\mathbb{Z}[\sqrt{\rho}]$ (for $\rho = -1, -2, -3, -7, -11$), and exactly sixteen Euclidean real quadratic domains $\mathbb{Z}[\sqrt{\rho}]$ (for $\rho = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$) with respect to the norm v_ρ. In another quadratic domains there doesn't exist a norm, with respect to which these domains will be Euclidean [7].

Let J_ρ be the set of all invertible elements of $\mathbb{Z}[\sqrt{\rho}]$ with zero. For any $N \in \mathbb{Z}[\sqrt{\rho}] \setminus J_\rho$ denote by $\mathbb{Z}_N[\sqrt{\rho}]$ and $\mathbb{Z}^*_N[\sqrt{\rho}]$ the additive group of residue classes modulo N and the multiplicative group of primitive residue classes modulo N respectively. Let $\alpha_\rho(N) = |\mathbb{Z}_N[\sqrt{\rho}]|$, $\varphi_\rho(N) = |\mathbb{Z}^*_N[\sqrt{\rho}]|$. An element $p \in \mathbb{Z}[\sqrt{\rho}] \setminus J_\rho$ is called prime element if for any divisor q of p there holds $q \in J_\rho$ or $p/q \in J_\rho$. Any prime element $p > 1$ of $\mathbb{Z}$ will be called a prime number.

In further we suppose that $\mathbb{Z}[\sqrt{\rho}]$ is a unique factorization domain.

P r o p o s i t i o n 1. *For any* $N \in \mathbb{Z}[\sqrt{\rho}] \setminus J_\rho$ *there holds* $\alpha_\rho(N) = v_\rho(N)$.

P r o o f. At first we prove that the function $\alpha_\rho : \mathbb{Z}[\sqrt{\rho}] \setminus J_\rho \to \mathbb{N}$ is totally multiplicative. Let N_1, $N_2 \in \mathbb{Z}[\sqrt{\rho}] \setminus J_\rho$, $\alpha_\rho(N_1) = m_1$, $\alpha_\rho(N_2) = m_2$. Let $x_1, \ldots, x_{m_1}$, $y_1, \ldots, y_{m_2}$ be elements of $\mathbb{Z}[\sqrt{\rho}]$ such that $x_i \not\equiv x_j \pmod{N_1}$ for any $i, j = 1, \ldots, m_1$, $i \neq j$, and $y_i \not\equiv y_j \pmod{N_2}$ for any $i, j = 1, \ldots, m_2$, $i \neq j$. It's easy to see that the set $\{x_i + N_1 y_j \mid i = 1, \ldots, m_1, j = 1, \ldots, m_2\}$ forms a complete residues system modulo $N_1 N_2$, hence, $\alpha_\rho(N_1 N_2) = m_1 m_2$.

Let $N \in \mathbb{Z} \setminus J_\rho$. If $\rho \not\equiv 1 \pmod 4$, then $a_1 + b_1\sqrt{\rho} \equiv a_2 + b_2\sqrt{\rho} \pmod N$ iff $a_1 \equiv a_2 \pmod N$ and $b_1 \equiv b_2 \pmod N$, hence, $\alpha_\rho(N) = N^2$. If $\rho \equiv 1 \pmod 4$ and N is odd, then $(a_1 + b_1\sqrt{\rho})/2 \equiv (a_2 + b_2\sqrt{\rho})/2 \pmod N$ iff $a_1 \equiv a_2 \pmod N$ and $b_1 \equiv b_2 \pmod N$, hence, $\alpha_\rho(N) = N^2$. Suppose that $\rho \equiv 1 \pmod 4$, $N = 2^k$, $k \in \mathbb{N}$. Let $(a_1 + b_1\sqrt{\rho})/2 \equiv (a_2 + b_2\sqrt{\rho})/2 \pmod N$, where $a_1 \equiv b_1 \pmod N$, $a_2 \equiv b_2 \pmod N$. It's easy to see that there exist exactly 2^{2k-1} pairs $(a_1, b_1), \ldots, (a_{2^{2k-1}}, b_{2^{2k-1}})$ such that $(a_i + b_i\sqrt{\rho})/2 \not\equiv (a_j + b_j\sqrt{\rho})/2 \pmod N$ for any $i, j = 1, \ldots, 2^{2k-1}$, $i \neq j$, where a_i, b_i, a_j, b_j are even. Analogously there exist exactly 2^{2k-1} pairs $(\alpha_1, \beta_1), \ldots, (\alpha_{2^{2k-1}}, \beta_{2^{2k-1}})$ such that $(\alpha_i + \beta_i\sqrt{\rho})/2 \not\equiv (\alpha_j + \beta_j\sqrt{\rho})/2 \pmod N$ for any $i, j = 1, \ldots, 2^{2k-1}$, $i \neq j$, where α_i, β_i, α_j, β_j are odd. Hence, $\alpha_\rho(2^k) = 2^{2k-1} + 2^{2k-1} = 2^{2k}$. Taking into account the total multiplicativity of the function α_ρ we conclude that $\alpha_\rho(N) = v_\rho(N)$ for any $N \in \mathbb{Z} \setminus J_\rho$.

Let $N \in \mathbb{Z}[\sqrt{\rho}] \setminus J_\rho$. Since $x \equiv y \pmod N$ iff $\overline{x} \equiv \overline{y} \pmod{\overline{N}}$ for any $x, y \in \mathbb{Z}[\sqrt{\rho}]$, so $\alpha_\rho(N) = \alpha_\rho(\overline{N})$, where $\overline{N}$ is the conjugate number to N. So, $\alpha_\rho(N) = \sqrt{\alpha_\rho(N)\alpha_\rho(\overline{N})} = \sqrt{\alpha_\rho(N\overline{N})} = \sqrt{v_\rho(N\overline{N})} = v_\rho(N)$. The proposition is proved.

P r o p o s i t i o n 2. *For any* $N \in \mathbb{Z}[\sqrt{\rho}] \setminus J_\rho$ *there holds* $\varphi_\rho(N) = \prod_{i=1}^{k} (v_\rho(p_i))^{q_i - 1}(v_\rho(p_i) - 1)$, *where* $N = \prod_{i=1}^{k} p_i^{q_i}$, *$p_i$ are distinct prime elements from* $\mathbb{Z}[\sqrt{\rho}]$, $q_i \in \mathbb{N}$.

P r o o f. Let N_1, $N_2 \in \mathbb{Z}[\sqrt{\rho}] \setminus J_\rho$ be coprime. Since $\mathbb{Z}^*_{N_1 N_2}[\rho] \cong \mathbb{Z}^*_{N_1}[\rho] \times \mathbb{Z}^*_{N_2}[\rho]$, so $\varphi_\rho(N_1 N_2) = \varphi_\rho(N_1)\varphi_\rho(N_2)$.

Let p be a prime element of $\mathbb{Z}[\sqrt{\rho}]$, $k \in \mathbb{N}$. It's easy to see that $\varphi_\rho(p) = \alpha_\rho(p) - 1$, and $\varphi_\rho(p^k) = \alpha_\rho(p^k) - \alpha_\rho(p^{k-1})$ if $k > 1$. By proposition 1, we have $\varphi_\rho(p^k) = (v_\rho(p))^{k-1}(v_\rho(p) - 1)$. Since the function φ_ρ is multiplicative, so the statement of the proposition is valid.

The Lagrange theorem immediately implies the following statement, which is an analogue of the Euler theorem.

P r o p o s i t i o n 3. *Let* $N \in \mathbb{Z}[\sqrt{\rho}] \setminus J_\rho$, *then for any* $m \in \mathbb{Z}[\sqrt{\rho}]$, $(m, N) = 1$, *there holds* $m^{\varphi_\rho(N)} \equiv 1 \pmod N$.

C o r o l l a r y 1. *Let p be a prime element of* $\mathbb{Z}[\sqrt{\rho}]$, *then for any* $m \in \mathbb{Z}[\sqrt{\rho}]$ *there holds* $m^{v_\rho(p)} \equiv m \pmod p$.

It's easy to see that there holds an analogue of the Chinese remainder theorem in the domain $\mathbb{Z}[\sqrt{\rho}]$.

P r o p o s i t i o n 4. *Let* $m_1, \ldots, m_k$, $c_1, \ldots, c_k \in \mathbb{Z}[\sqrt{\rho}]$, $(m_i, m_j) = 1$ *for any* $i \neq j$. *Then the system of congruencies* $x \equiv c_i \pmod{m_i}$, $i = 1, \ldots, k$, *has a unique solution* $x \equiv \sum_{i=1}^{k} c_i x_i \dfrac{m}{m_i} \pmod m$, *where* $m = \prod_{i=1}^{k} m_i$, $x_i \in \mathbb{Z}[\sqrt{\rho}]$, $\dfrac{m}{m_i} x_i \equiv 1 \pmod{m_i}$, $i = 1, \ldots, k$.

The following three statements are analogues of Wilson's, Lucas' [8] and Pocklington's criterions [9] of primality.

P r o p o s i t i o n 5. *An element* $p \in \mathbb{Z}[\sqrt{\rho}] \setminus J_\rho$ *is prime iff there holds the congruence*

$$\prod_{x \in \mathbb{Z}_p[\sqrt{\rho}],\, x \neq 0} x \equiv -1 \pmod p.$$

P r o o f. If p is prime, then for any $x \in \mathbb{Z}^*_p[\sqrt{\rho}]$, $x \not\equiv \pm 1 (\mathrm{mod}\ p)$ there exists a unique $y \in \mathbb{Z}^*_p[\sqrt{\rho}]$, $y \neq x$, such that $xy \equiv 1 (\mathrm{mod}\ p)$. Hence, $\prod_{x \in \mathbb{Z}_p[\sqrt{\rho}], x \neq 0} x \equiv -1 (\mathrm{mod}\ p)$. If p is not prime, then the ring $\mathbb{Z}_p[\sqrt{\rho}]$ has divisors of zero, so $\prod_{x \in \mathbb{Z}_p[\sqrt{\rho}], x \neq 0} x \equiv 0 (\mathrm{mod}\ p)$. This contradiction finishes the proof.

P r o p o s i t i o n 6. *An element* $N \in \mathbb{Z}[\sqrt{\rho}] \setminus J_\rho$ *is prime iff there exists* $a \in \mathbb{Z}[\sqrt{\rho}]$, $(a, N) = 1$, *such that there holds: 1)* $a^{v_\rho(N)-1} \equiv 1 (\mathrm{mod}\ N)$, *2)* $a^{(v_\rho(N)-1)/q} \not\equiv 1 (\mathrm{mod}\ N)$ *for any prime divisor* q *of* $v_\rho(N) - 1$.

P r o o f. If N is prime, then $\mathbb{Z}_N[\sqrt{\rho}]$ is a finite field, and we can get any primitive element a of this field. Conditions 1) and 2) of the proposition are satisfied.

Let for any a there hold conditions 1) and 2) of the proposition. Hence, $\mathrm{ord}\ a = v_\rho(N) - 1$ in the group $\mathbb{Z}^*_N[\sqrt{\rho}]$. The Lagrange theorem implies that $(v_\rho(N) - 1) \mid \varphi_\rho(N)$. By proposition 1, $\varphi_\rho(N) \leq \alpha_\rho(N) - 1 = v_\rho(N) - 1$. Consequently, $\varphi_\rho(N) = \alpha_\rho(N) - 1$. The last one implies the primality of the element N. The proposition is proved.

P r o p o s i t i o n 7. *Let* $N \in \mathbb{Z}[\sqrt{\rho}] \setminus J_\rho$ *and there exists a prime number* $q > \sqrt{v_\rho(N)} - 1$ *such that* $q \mid (v_\rho(N) - 1)$. *If there exists an element* $a \in \mathbb{Z}[\sqrt{\rho}]$ *such that the following two conditions hold: 1)* $a^{v_\rho(N)-1} \equiv 1 (\mathrm{mod}\ N)$, *2)* $(a^{(v_\rho(N)-1)/q} - 1, N) = 1$; *then the element N is prime in* $\mathbb{Z}[\sqrt{\rho}]$.

P r o o f. Let the conditions of the proposition be satisfied but N is not prime element of $\mathbb{Z}[\sqrt{\rho}]$. Hence, there exists a prime element $p \in \mathbb{Z}[\sqrt{\rho}]$ such that $p \mid N$ and $v_\rho(p) \leq \sqrt{v_\rho(N)}$. Since $q > \sqrt{v_\rho(N)} - 1$, so $(q, v_\rho(p) - 1) = 1$ and therefore there exists a natural number u such that $uq \equiv 1 (\mathrm{mod}\ v_\rho(p) - 1)$. Consequently, by condition 1) and proposition 3, we have

$$a^{(v_\rho(N)-1)/q} \equiv a^{uq(v_\rho(N)-1)/q} = a^{u(v_\rho(N)-1)} \equiv 1 (\mathrm{mod}\ p).$$

The last one contradicts with condition 2). The proposition is proved.

Algorithm of the generalized RSA-cryptosystem. Any subscriber A chooses two distinct big prime elements p_A, $q_A \in \mathbb{Z}[\sqrt{\rho}]$ and calculates $\varphi_\rho(N_A)$, where $N_A = p_A q_A$. Further A chooses a random natural number $e_A \in [1, \varphi_\rho(N_A)]$ and finds a natural number d_A such that $e_A d_A \equiv 1 (\mathrm{mod}\ \varphi_\rho(N_A))$ with the help of the extended Euclidean algorithm [8]. The pair (N_A, e_A) is a public key of A, the pair (N_A, d_A) is a private key of A. Then $f_A : \mathbb{Z}_{N_A}[\sqrt{\rho}] \to \mathbb{Z}_{N_A}[\sqrt{\rho}]$, $f_A(x) \equiv x^{e_A} (\mathrm{mod}\ N_A)$, is an encryption function of A, the function $f_A^{-1} : \mathbb{Z}_{N_A}[\sqrt{\rho}] \to \mathbb{Z}_{N_A}[\sqrt{\rho}]$, $f_A^{-1}(x) \equiv x^{d_A} (\mathrm{mod}\ N_A)$ is a decryption function of A. Any such triple (N_A, e_A, d_A) is called parameters of the generalized RSA-cryptosystem. Corollary 1 implies the correctness of the work of the the generalized RSA-cryptosystem.

Scheme of digital signature based on the generalized RSA-cryptosystem. Suppose that a subscriber A wants to send to a subscriber B a signed message (m, P), where $m \in \mathbb{Z}_{N_B}[\sqrt{\rho}]$ is a secret message, $P \in \mathbb{Z}_N[\sqrt{\rho}]$ is a signature of A (open text), where $N = N_A$ if $v_\rho(N_A) \leq v_\rho(N_B)$, and $N = N_B$ if $v_\rho(N_A) > v_\rho(N_B)$. Suppose that for any two RSA-modulus N_1 and N_2, $v_\rho(N_1) \leq v_\rho(N_2)$, there is defined an injective mapping $g_{N_1,N_2} : \mathbb{Z}_{N_1}[\sqrt{\rho}] \to \mathbb{Z}_{N_2}[\sqrt{\rho}]$ such that values of the mappings g_{N_1,N_2} and $g^{-1}_{N_1,N_2}$ are easy computable. If $v_\rho(N_A) \leq v_\rho(N_B)$, then the subscriber A send to B the pair (m_1, P_1), where $m_1 = f_B(m)$, $P_1 = f_B(g_{N_A,N_B}(f_A^{-1}(P)))$. The subscriber B computes $m_2 = f_B^{-1}(m_1)$, $P_2 = f_A(g^{-1}_{N_A,N_B}(f_B^{-1}(P_1)))$. If $v_\rho(N_A) > v_\rho(N_B)$, then the subscriber A send to B the pair (m_1, P_1), where $m_1 = f_B(m)$, $P_1 = f_A^{-1}(g_{N_B,N_A}(f_B(P)))$. The subscriber B computes $m_2 = f_B^{-1}(m_1)$, $P_2 = f_B^{-1}(g^{-1}_{N_B,N_A}(f_A(P_1)))$. Then, by corollary 1, $m_2 = m$, $P_2 = P$.

Analysis of security of the generalized RSA-cryptosystem. It's easy that knowledge of the RSA-modulus factorization $N = pq$ gives an effective way to find the private key. The following theorem establishes the inverse statement and in the case of classical RSA-cryptosystem is given in [11, Ch. 14].

T h e o r e m 1. *Let the domain* $\mathbb{Z}[\sqrt{\rho}]$ *be Euclidean,* (N, e, d) *be parameters of the generalized RSA-cryptosystem. If the number d is known, then the number N can be effectively factorized with probability at least* $\frac{1}{2}$ *at polynomial, with respect to* $\log v_\rho(N)$, *number of arithmetic operations in* $\mathbb{Z}[\sqrt{\rho}]$.

P r o o f. Let $s = ed - 1 = 2^t u$, where t, $u \in \mathbb{N}$, u is odd. Since $\varphi_\rho(N) \mid s$, so $x^s \equiv 1 (\mathrm{mod}\ N)$ for any $x \in \mathbb{Z}^*_N[\rho]$. Construct the set

$$B = \{x \in \mathbb{Z}^*_N[\rho] \mid \exists j \in \{0, \ldots, t-1\} : x^{2^j u} \equiv -1 (\mathrm{mod}\ N) \ \text{ or } \ x^u \equiv 1 (\mathrm{mod}\ N)\}.$$

Let $A = \mathbb{Z}^*_N[\rho] \setminus B$. Let's consider an arbitrary element $a \in A$. Take the smallest natural number k such that $a^{2^k u} \equiv 1 (\bmod N)$. Let $b \equiv a^{2^{k-1} u} (\bmod N)$. It's easy to see that $b^2 \equiv 1 (\bmod N)$ and $b \not\equiv \pm 1 (\bmod N)$. Hence, $(b-1, N)$ is a nontrivial divisor of N. There exists a constant $\gamma_\rho \in (0,1)$ such that for any $a, b \in \mathbb{Z}[\sqrt{\rho}] \setminus \{0\}$, $v_\rho(a) \ge v_\rho(b)$, one can find q, $r \in \mathbb{Z}[\sqrt{\rho}]$ such that $a = bq + r$, where $r = 0$ or $v_\rho(r) \le \gamma_\rho v_\rho(b)$ [10]. Hence, the greatest divisor $(b-1, N)$ can be computed with the help of the Euclidean algorithm at polynomial number on $\log v_\rho(N)$ of arithmetic operations in $\mathbb{Z}[\sqrt{\rho}]$ [7]. It remains to show that $|B| \le \frac{\varphi_\rho(N)}{2}$.

Let $N = pq$, where p, q are distinct prime elements of $\mathbb{Z}[\sqrt{\rho}]$. Let $\varphi_\rho(p) = 2^{v_1} u_1$, $\varphi_\rho(q) = 2^{v_2} u_2$, where $v_1, v_2, u_1, u_2 \in \mathbb{N}$, u_1 and u_2 are odd. Denote $v = \min\{v_1, v_2\}$, $K = (u, u_1)(u, u_2)$. It's easy to see that the congruence $x^u \equiv 1 (\bmod N)$ is equivalent to the system $u \log_\alpha x \equiv 0 (\bmod \varphi_\rho(p))$, $u \log_\beta x \equiv 0 (\bmod \varphi_\rho(q))$, where α and β are primitive elements in $\mathbb{Z}^*_p[\rho]$ and $\mathbb{Z}^*_q[\rho]$ respectively. Since u is odd, so, by proposition 4, the congruence $x^u \equiv 1 (\bmod N)$ has exactly K solutions. Let's consider the congruence $x^{2^j u} \equiv -1 (\bmod N)$, where $j \in \{0, \ldots, t-1\}$. If $j < v$, then the similar arguments imply that the number of solutions is $4^j K$. If $j \ge v$, then the congruence has no solutions. Therefore $|B| = (1 + 1 + 4 + \ldots + 4^{v-1}) K = \frac{4^v + 2}{3} K$. Since $\varphi_\rho(N) = 2^{v_1 + v_2} u_1 u_2 \ge 4^v K$, so $\frac{|B|}{\varphi_\rho(N)} \le \frac{1}{2}$. The theorem is proved.

R e m a r k 1. As in the case of classical RSA-cryptosystem the question on the equivalence of breaking of the generalized RSA-cryptosystem and factorization of the RSA-modulus is open.

The following theorem is an analogue of the Wiener theorem on low private key for the classical RSA-cryptosystem [11, Ch. 14].

T h e o r e m 2. *Let (N, e, d), $N = pq$, be parameters of the generalized RSA-cryptosystem such that $v_\rho(q) < v_\rho(p) < \alpha^2 v_\rho(q)$, where $\alpha > 1$. If $d < \frac{1}{\sqrt{2\alpha + 2}} (v_\rho(N))^{1/4}$, then the number d can be effectively computed at polynomial, with respect to $\log v_\rho(N)$, number of arithmetic operations in $\mathbb{Z}$.*

P r o o f. Let $N = pq$, where p, q are distinct prime elements of $\mathbb{Z}[\sqrt{\rho}]$. Let $ed - 1 = k\varphi_\rho(N)$, $k \in \mathbb{N}$. Since $v_\rho(p) + v_\rho(q) < (\alpha + 1)\sqrt{v_\rho(N)}$, so

$$v_\rho(N) - \varphi_\rho(N) = v_\rho(p) + v_\rho(q) - 1 < (\alpha + 1)\sqrt{v_\rho(N)}. \tag{1}$$

We have $k\varphi_\rho(N) < ed$, $e < \varphi_\rho(N)$. Therefore $k < d$. The last one implies the relations

$$\frac{(\alpha + 1)k}{d\sqrt{v_\rho(N)}} \le \frac{(\alpha + 1)}{\sqrt{v_\rho(N)}} < \frac{1}{2d^2}. \tag{2}$$

In view of (1) and (2) we get

$$\left| \frac{e}{v_\rho(N)} - \frac{k}{d} \right| = \left| \frac{1 - k(v_\rho(N) - \varphi_\rho(N))}{v_\rho(N) d} \right| \le \frac{(\alpha + 1)\sqrt{v_\rho(N)}}{v_\rho(N) d} < \frac{1}{2d^2}. \tag{3}$$

Relation (3) means that $\frac{k}{d}$ is a successive fraction for the non-secret fraction $\frac{e}{v_\rho(N)}$. Hence, the fraction $\frac{k}{d}$ can be computed effectively with the help of the Euclidean algorithm in $\mathbb{Z}$. The theorem is proved.

One of the well-known methods of breaking of RSA-cryptosystem is the method of iterated encryption. Let (N, e, d) be parameters of the generalized RSA-cryptosystem. Let $y = x^e (\bmod N)$ be an encrypted message $x \in \mathbb{Z}_N[\sqrt{\rho}]$. To try to find the original text x a cryptanalytic computes the terms of the sequence $y_i = y^{e^i} (\bmod N)$, $i = 1, 2, \ldots$, until one has $y_m = y$ for the first time. It's easy to see that $y_{m-1} = x$. So, we need to choose the parameters of the generalized RSA-cryptosystem to make the value m to be quite big.

P r o p o s i t i o n 8. *Let* $N = pq$, p, q *be distinct prime elements of* $\mathbb{Z}[\sqrt{\rho}]$, $\varphi_\rho(p) = rk$, $\varphi_\rho(q) = sl$, *where* r *and* s *are distinct prime numbers,* $(r,k) = (s,l) = 1$. *If* $y \in \mathbb{Z}^*_N[\sqrt{\rho}]$ *is a random element, then* $\mathbb{P}(rs \mid \operatorname{ord} y) = (1 - r^{-1})(1 - s^{-1})$.

P r o o f. For any $t_1 \mid k$, $t_2 \mid l$ there exist exactly $\varphi(rt_1)\varphi(st_2)$ of elements $y \in \mathbb{Z}^*_N[\sqrt{\rho}]$ such that $\operatorname{ord} y = rs(t_1, t_2)$. Consequently, the number of elements $y \in \mathbb{Z}^*_N[\sqrt{\rho}]$ such that $rs \mid \operatorname{ord} y$ is equal to

$$\sum_{t_1|k,t_2|l} \varphi(rt_1)\varphi(st_2) = (r-1)(s-1) \sum_{t_1|k,t_2|l} \varphi(t_1)\varphi(t_2) = (r-1)(s-1)kl. \tag{4}$$

So, the statement of the proposition follows from relation (4) and equality $|\mathbb{Z}^*_N[\sqrt{\rho}]| = rksl$.

T h e o r e m 3. *Let* (N, e, d), $N = pq$, *be parameters of the generalized RSA-cryptosystem. Suppose that the numbers* $\varphi_\rho(p)$, $\varphi_\rho(q)$ *have distinct prime divisors* r, s *respectively, and the numbers* $r-1$, $s-1$ *have prime divisors* r_1, s_1 *respectively, then* $\mathbb{P}(m \ge r_1 s_1) \ge (1 - r^{-1})(1 - s^{-1})(1 - r_1^{-1})(1 - s_1^{-1})$, *where* m *is the smallest natural number such that* $y^{e^m} = y \pmod N$, $y \in \mathbb{Z}^*_N[\sqrt{\rho}]$ *is a random element.*

P r o o f. Note that $y^{e^m} = y \pmod N$ iff $\operatorname{ord} y \mid (e^m - 1)$. By proposition 8,

$$\mathbb{P}(rs \mid (e^m - 1)) \ge \mathbb{P}(rs \mid \operatorname{ord} y) = (1 - r^{-1})(1 - s^{-1}).$$

Applying Theorem 14.1 [11], we conclude that

$$\mathbb{P}(m \ge r_1 s_1) \ge \mathbb{P}(r_1 s_1 \mid m) \ge \mathbb{P}(r_1 s_1 \mid \operatorname{ord} e, rs \mid \operatorname{ord} y) \ge (1 - r^{-1})(1 - s^{-1})(1 - r_1^{-1})(1 - s_1^{-1}).$$

The theorem is proved.

R e m a r k 2. To secure the generalized RSA-cryptosystem of the iterated encryption attack we should take prime elements p, $q \in \mathbb{Z}[\sqrt{\rho}]$ such that one can find big distinct prime divisors r, s of $\varphi_\rho(p)$, $\varphi_\rho(q)$ and one can find big prime divisors r_1, s_1 of $r-1$, $s-1$.

R e m a r k 3. If $N = pq$, where p and q are such that the difference $|v_\rho(p) - v_\rho(q)|$ is small, then it is easy to find the representation $N = t^2 - s^2$, where t, $s \in \mathbb{Z}[\sqrt{\rho}]$ and this representation gives us the factorization of N. Hence, the difference $|v_\rho(p) - v_\rho(q)|$ should be quite large.

R e m a r k 4. The generalized RSA-cryptosystem provides more security than the classical variant of RSA-cryptosystem, since the number of elements which are chosen to represent the message m is about square of those used in the classical variant. This advantage enables to use shorter keys than in the classical version of RSA-cryptosystem. Note that all our results cover the case of the classical RSA-cryptosystem: it's enough to take the ring $\mathbb{Z}$ instead of $\mathbb{Z}[\sqrt{\rho}]$, and to define the norm of $a \in \mathbb{Z}$ as the absolute value $|a|$.

Estimate of computational efficiency of the generalized RSA-cryptosystem in imaginary quadratic domains. Let $\mathbb{Z}[\sqrt{\rho}]$ – imaginary quadratic domain. We say that an element $x = x_1 + x_2\sqrt{\rho} \in \mathbb{Z}[\sqrt{\rho}]$ is n-bit if integers x_1 and x_2 have less than $n+1$ bits in the binary value. Let $p = p_1 + p_2\sqrt{\rho}$, $q = q_1 + q_2\sqrt{\rho}$ be distinct prime n-bit elements of the domain $\mathbb{Z}[\sqrt{\rho}]$. Let's call RSA-cryptosystem with parameters p and q n-bit. Multiplication modulo $N = pq$ of two n-bit elements of the domain $\mathbb{Z}[\sqrt{\rho}]$ has the complexity $O(n^2)$ and involution of n-bit element $x \in \mathbb{Z}[\sqrt{\rho}]$ in the domain $\mathbb{Z}[\sqrt{\rho}]$ has the complexity $O(n^2 \log k)$. So encryption and decryption using the generalized RSA-cryptosystem in the domain $\mathbb{Z}[\sqrt{\rho}]$ have the complexity $O(n^2 \log n)$. The complexity of generating the pair of keys d, e is defined by the complexity of calculating of inverse element in the domain $\mathbb{Z}[\sqrt{\rho}]$. So it has the complexity $O(n^2)$. Note that the complexity of encrypting, decrypting and generation of keys d, e using n-bit RSA-cryptosystem in the domain $\mathbb{Z}[\sqrt{\rho}]$ can be estimated as $O(M)$, where M – the number of binary operations to encrypt, decrypt and generation of keys in classical n-bit RSA-cryptosystem. Breaking of classical n-bit cryptosystem using checking of every possible message has the complexity $O(4^n n^2 \log n)$, analogical breaking for n-bit RSA-cryptosystem in the domain $\mathbb{Z}[\sqrt{\rho}]$ has the complexity $O(16^n n^2 \log n)$. And also the number of binary operations to factorize RSA-modulus in the domain $\mathbb{Z}[\sqrt{\rho}]$, is not less than the number of binary operations to factorize RSA-modulus in classical RSA-cryptosystem.

E x a m p l e. Let the subscriber A wishes to send the secret message $m = 1 + i$ with the signature $P = 2i$ to the subscriber B with the help of the generalized RSA-cryptosystem in $\mathbb{Z}[\sqrt{\rho}]$ with $\rho = -1$. Let

$(N_A, e_A, d_A) = (589, 7, 98743)$ and $(N_B, e_B, d_B) = (559, 13, 167173)$, $g_{N_B, N_A}(X) = x_1 + ix_2 + N_A\mathbb{Z}[i]$, $X \in \mathbb{Z}_{N_B}[i]$, where x_1, x_2 are the smallest nonnegative integers such that $X = x_1 + ix_2 + N_B\mathbb{Z}[i]$. The subscriber A computes

$$m_1 = m^{eB} (\bmod N_B) = 495 + 495i$$

and

$$P_1 = (P^{eB} (\bmod N_B))^{dA} (\bmod N_A) = 192i.$$

So, the encrypted signed message is $(m_1, P_1) = (495 + 495i, 192i)$. The subscriber B gets the pair (m_1, P_1) and calculates

$$m_2 = m_1^{dB} (\bmod N_B) = 1 + i$$

and

$$P_2 = (P_1^{eA} (\bmod N_A))^{dB} (\bmod N_B) = 2i.$$

So the pair (m_2, P_2) is the decrypted message.

References

1. *Rivest, R. L.* A method for obtaining digital signatures and public-key cryptosystems / R. L. Rivest, A. Shamir, L. Adleman // Communications of the ACM. – 1978. – Vol. 21. – P. 120–126.

2. *Elkamchouchi, H.* Extended RSA Cryptosystem and digital signature schemes in the domain of Gaussian integers / H. Elkamchouchi, K. Elshenawy, H. Shaban // Proceedings of the 8th International conference on communication systems. – 2002. – P. 91–95.

3. *Li, B.* Generalizations of RSA public key cryptosystem / B. Li // IACR. – Cryptology ePrint Arc. 2005.

4. Modified RSA in the domains of Gaussian integers and polynomials over finite fields / A. N. El-Kassar [et al.] // Proceedings of the ISCA 18th International conference on computer applications in industry and engineering. – Hawaii, USA, 2005. – P. 298–303.

5. *Koval, A.* Analysis of RSA over Gaussian integers algorithm // 5th international conference on information technology: new generations (ITNG 2008) / A. Koval, B. Verkhovsky. – Las Vegas, Nevada, USA, 2008. – P. 101–105.

6. Proceedings of the second international conference of soft computing for problem solving / B. V. Babu [et al.] // Advances in intelligent systems and computing. – 2014. – Vol. 236.

7. *Rodossky, K. A.* Euclidean algorithm / K. A. Rodossky. – Moscow: Nauka, 1988.

8. Introduction to number theoretical methods in cryptography / M. M. Gluhov [et al.]. – Saint-Petersburg: Lan', 2011.

9. *Koblitz, N.* Course in number theory and cryptography / N. Koblitz. – Moscow: TVP, 2001.

10. *Eggleton, R. B.* Euclidean quadratic fields / R. B. Eggleton, C. B. Lacampagne, J. L. Selfridge // Amer. Math. Monthly. – 1992. – Vol. 99, N 9. – P. 829–837.

11. Cryptology / Y. S. Kharin [et al.]. – Minsk: BSU, 2013.

Received 24.06.2015