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.

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

© Васьковский М. М., Кондратенок Н. В., 2015.
Let $J_\rho$ be the set of all invertible elements of $\mathbb{Z}[\sqrt{D}]$ with zero. For any $N \in \mathbb{Z}[\sqrt{D}] \setminus J_\rho$, denote by $Z_N[\sqrt{D}]$ and $Z_N^*[\sqrt{D}]$ the additive group of residue classes modulo $N$ and the multiplicative group of primitive residue classes modulo $N$ respectively. Let $\alpha_\rho(N) = |Z_N[\sqrt{D}]|$, $\varphi_\rho(N) = |Z_N^*[\sqrt{D}]|$. An element $p \in \mathbb{Z}[\sqrt{D}] \setminus J_\rho$ 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 $\mathbb{Z}[\sqrt{D}]$ is a unique factorization domain.

**Proposition 1.** For any $N \in \mathbb{Z}[\sqrt{D}] \setminus J_\rho$ there holds $\alpha_\rho(N) = \varphi_\rho(N)$.

**Proof.** At first we prove that the function $\alpha_\rho : \mathbb{Z}[\sqrt{D}] \setminus J_\rho \to \mathbb{N}$ is totally multiplicative. Let $N_1, N_2 \in \mathbb{Z}[\sqrt{D}] \setminus J_\rho$, $\alpha_\rho(N_1) = m_1$, $\alpha_\rho(N_2) = m_2$. Let $x_1, x_2, \ldots, x_{m_1}$ be elements of $\mathbb{Z}[\sqrt{D}]$ such that $x_i \equiv x_i (mod N_1)$ for any $i = 1, \ldots, m_1$. Similarly, $y_1, y_2, \ldots, y_{m_2}$ be elements of $\mathbb{Z}[\sqrt{D}]$ such that $y_i \equiv y_i (mod N_2)$ for any $i = 1, \ldots, m_2$. It’s easy to see that the set $\{x_i + N_1 y_j | i = 1, \ldots, m_1, j = 1, \ldots, m_2\}$ forms a complete residue 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 $p \equiv 1 (mod 4)$, then $a_1 + b_1 \sqrt{D} \equiv a_2 + b_2 \sqrt{D} (mod N)$ iff $a_1 \equiv a_2 (mod N)$ and $b_1 \equiv b_2 (mod N)$, hence, $\alpha_\rho(N) = N^2$. If $p \equiv 1 (mod 4)$ and $N$ is odd, then $a_1 + b_1 \sqrt{D} \equiv (a_2 + b_2 \sqrt{D})/2 (mod N)$ iff $a_1 \equiv a_2 (mod N)$ and $b_1 \equiv b_2 (mod N)$, hence, $\alpha_\rho(N) = N^2$. Suppose that $p \equiv 1 (mod 4)$ and $N = 2^k$, $k \in \mathbb{N}$. Let $a_1, a_2 \equiv (a_2 + b_2 \sqrt{D})/2 (mod N)$, where $a_1 \equiv b_1 (mod N)$, $a_2 \equiv b_2 (mod N)$. It’s easy to see that there exist exactly $2^{k-1}$ pairs $(a_1, b_1), \ldots, (a_{2^{k-1}}, b_{2^{k-1}})$ such that $a_1 + b_1 \sqrt{D} \equiv (a_2 + b_2 \sqrt{D})/2 (mod N)$ for any $i = 1, \ldots, 2^{k-1}$, $i \neq j$, where $a_1, b_1, a_2, b_2$ are even. Analogously there exist exactly $2^{k-1}$ pairs $(a_1, b_1), \ldots, (a_{2^{k-1}}, b_{2^{k-1}})$ such that $a_1 + b_1 \sqrt{D} \equiv (a_2 + b_2 \sqrt{D})/2 (mod N)$ for any $i = 1, \ldots, 2^{k-1}$, $i \neq j$, where $a_1, b_1, a_2, b_2$ are odd. Hence, $\alpha_\rho(2^k) = 2^{k-1} + 2^{k-1} = 2^{k-1}$. Taking into account the total multiplicativity of the function $\alpha_\rho$ we conclude that $\alpha_\rho(N) = \varphi_\rho(N)$ for any $N \in \mathbb{Z} \setminus J_\rho$.

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

**Proposition 2.** For any $N \in \mathbb{Z}[\sqrt{D}] \setminus J_\rho$ there holds $\varphi_\rho(N) = \prod_{i=1}^{\ell} (p_i^{a_i} - 1)$, where $N = \prod_{i=1}^{\ell} p_i^{a_i}$, $p_i$ are distinct prime elements from $\mathbb{Z}[\sqrt{D}]$, $q_i \in \mathbb{N}$.

**Proof.** Let $N_1, N_2 \in \mathbb{Z}[\sqrt{D}] \setminus J_\rho$ be coprime. Since $Z_{N_1 N_2}[\sqrt{D}] \cong Z_{N_1}[\sqrt{D}] \times Z_{N_2}[\sqrt{D}]$, so $\varphi_\rho(N_1 N_2) = \varphi_\rho(N_1) \varphi_\rho(N_2)$.

Let $p$ be a prime element of $\mathbb{Z}[\sqrt{D}]$, $k \in \mathbb{N}$. 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 $\varphi_\rho(p^k) = (\varphi_\rho(p))^{k-1}(\varphi_\rho(p) - 1)$. Since the function $\varphi_\rho$ is multiplicative, the statement of the proposition is valid.

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

**Proposition 3.** Let $N \in \mathbb{Z}[\sqrt{D}] \setminus J_\rho$, then for any $m \in \mathbb{Z}[\sqrt{D}]$, $(m, N) = 1$, there holds $m^{\varphi_\rho(N)} \equiv 1 (mod N)$.

**Corollary 1.** Let $p$ be a prime element of $\mathbb{Z}[\sqrt{D}]$, then for any $m \in \mathbb{Z}[\sqrt{D}]$ there holds $m^{\varphi_\rho(p)} \equiv m (mod p)$.

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

**Proposition 4.** Let $m_1, \ldots, m_k, c_1, \ldots, c_k \in \mathbb{Z}[\sqrt{D}]$, $(m_i, m_j) = 1$ for any $i \neq j$. Then the system of congruences $x \equiv c_i (mod m_i), i = 1, \ldots, k$, has a unique solution $x \equiv \sum_{i=1}^{k} c_i x_i/m_i (mod m)$, where $m = \prod_{i=1}^{k} m_i$, $x_i \equiv 1 (mod m_i), i = 1, \ldots, k$.

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

**Proposition 5.** An element $p \in \mathbb{Z}[\sqrt{D}] \setminus J_\rho$ is prime iff there holds the congruence $\prod_{x \in \mathbb{Z}[\sqrt{D}], x \neq 0} x \equiv -1 (mod p)$. 

19
Proof. If \( p \) is prime, then for any \( x \in \mathbb{Z}_p^*[\sqrt{p}] \), \( x \neq \pm 1 \text{ (mod } p) \) there exists a unique \( y \in \mathbb{Z}_p^*[\sqrt{p}] \), \( y \neq x \), such that \( xy \equiv 1 \text{ (mod } p) \). Hence, \( \prod_{x \in \mathbb{Z}_p^*[\sqrt{p}]} x^x \equiv 1 \text{ (mod } p) \). If \( p \) is not prime, then the ring \( \mathbb{Z}_p^*[\sqrt{p}] \) has divisors of zero, so \( \prod_{x \in \mathbb{Z}_p^*[\sqrt{p}]} x^x \equiv 0 \text{ (mod } p) \). This contradiction finishes the proof.

**Proposition 6.** An element \( N \in \mathbb{Z}[\sqrt{p}] \) is prime iff there exists \( a \in \mathbb{Z}[\sqrt{p}] \), \( (a,N) = 1 \), such that there holds: 1) \( a^{v_p(N)-1} \equiv 1 \text{ (mod } N) \), 2) \( a^{v_p(N)-1/q} \equiv 1 \text{ (mod } N) \) for any prime divisor \( q \) of \( v_p(N) - 1 \).

**Proof.** If \( N \) is prime, then \( Z_N[\sqrt{p}] \) 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, \( a = v_p(N) - 1 \) in the group \( Z_N[\sqrt{p}] \). The Lagrange theorem implies that \( (v_p(N) - 1) \phi(N) \). By proposition 1, \( \phi(N) \leq (N-1)^{1-1} = v_p(N) - 1 \). Consequently, \( \phi_p(N) = \alpha_p(N) - 1 \). The last one implies the primality of the element \( N \). The proposition is proved.

**Proposition 7.** Let \( N \in \mathbb{Z}[\sqrt{p}] \) and there exists a prime number \( q > \sqrt{v_p(N)} - 1 \) such that \( q \mid (v_p(N) - 1) \). If there exists an element \( a \in \mathbb{Z}[\sqrt{p}] \) such that the following two conditions hold: 1) \( a^{v_p(N)-1} \equiv 1 \text{ (mod } N) \), 2) \( a^{v_p(N)-1/q} \equiv 1 \text{ (mod } N) \) then the element \( N \) is prime in \( \mathbb{Z}[\sqrt{p}] \).

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

\[
\begin{align*}
a^{v_p(N)-1/q} &\equiv a^{uq(v_p(N)-1)/q} = a^{u(v_p(N)-1)} \equiv 1 \text{ (mod } p). 
\end{align*}
\]

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 \( p_A, q_A \in \mathbb{Z}[\sqrt{p}] \) and calculates \( \phi_p(N_A) \), where \( N_A = p_Aq_A \). Further \( A \) chooses a random natural number \( e_A \in [1, \phi_p(N_A)] \) and finds a natural number \( d_A \) such that \( e_Ad_A \equiv 1 \text{ (mod } \phi_p(N_A)) \) 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 primary key of \( A \). Then \( f_A: \mathbb{Z}_N[\sqrt{p}] \rightarrow \mathbb{Z}_N[\sqrt{p}] \), \( f_A(x) = x^{e_A} \text{ (mod } N_A) \), is an encryption function of \( A \), the function \( f_A^{-1}: \mathbb{Z}_N[\sqrt{p}] \rightarrow \mathbb{Z}_N[\sqrt{p}] \), \( f_A^{-1}(x) = x^{d_A} \text{ (mod } N_A) \), 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. In the case of classical RSA-cryptosystem is given in \([11, \text{ Ch. } 14]\).

**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 \( m \in \mathbb{Z}[\sqrt{p}] \) is a secret message, \( P \in \mathbb{Z}[\sqrt{p}] \) is a signature of \( A \) (open text), where \( N = N_A \) if \( \psi_p(N_A) \leq \psi_p(N_A) \), and \( N = N_B \) if \( \psi_p(N_B) > \psi_p(N_A) \). Suppose that for any two RSA-modulus \( N_1 \) and \( N_2, v_p(N_1) \leq v_p(N_2) \), there is defined an injective mapping \( g_{N_1, N_2}: \mathbb{Z}_N[\sqrt{p}] \rightarrow \mathbb{Z}_N[\sqrt{p}] \) such that values of the mappings \( g_{N_1, N_2} \) and \( g_{N_1, N_2}^{-1} \) are easy computable. If \( v_p(N_A) \leq v_p(N_B) \), then the subscriber \( A \) sends to \( B \) the pair \( (m_1, P_1) \), where \( m_1 = f_A(m), P_1 = f_B(g_{N_A, N_B}(f_A(P))) \). The subscriber \( B \) computes \( m_2 = f_A^{-1}(m_1), P_2 = f_B(g_{N_B, N_A}(f_A(P))) \). If \( v_p(N_B) > v_p(N_A) \), then the subscriber \( A \) sends to \( B \) the pair \( (m_1, P_1) \), where \( m_1 = f_A(m), P_1 = f_B^{-1}(g_{N_B, N_A}(f_A(P))) \). The subscriber \( B \) computes \( m_2 = f_A^{-1}(m_1), P_2 = f_B^{-1}(g_{N_B, N_A}(f_A(P))) \). 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 \([11, \text{ Ch. } 14]\).

**Theorem 1.** Let the domain \( \mathbb{Z}[\sqrt{p}] \) 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 \( \log v_p(N) \), number of arithmetic operations in \( \mathbb{Z}[\sqrt{p}] \).

**Proof.** Let \( x = ed^{-1} = 2^t u \), where \( t, u \in \mathbb{N}, u \) is odd. Since \( \phi_p(N) \backslash x \), so \( x^u \equiv 1 \text{ (mod } N) \) for any \( x \in \mathbb{Z}_N^*[\sqrt{p}] \). Construct the set

\[
B = \{ x \in \mathbb{Z}_N^*[\sqrt{p}] \mid \exists j \in \{0, \ldots, t-1\}, x^{2^j u} \equiv -1 \text{ (mod } N) \text{ or } x^u \equiv 1 \text{ (mod } N) \}.
\]
Let $A = \mathbb{Z}_N^* \setminus B$. Let’s consider an arbitrary element $a \in A$. Take the smallest natural number $k$ such that $a^{2^k} \equiv 1 \pmod{N}$. Let $b \equiv a^{2^{k-1}} \pmod{N}$. It’s easy to see that $b^2 \equiv 1 \pmod{N}$ and $b \not\equiv \pm 1 \pmod{N}$. Hence, $(b-1,N)$ is a nontrivial divisor of $N$. There exists a constant $\gamma_0 \in (0,1)$ such that for any $a,b \in \mathbb{Z}_N^* \setminus \{0\}$, $v_p(a) \geq v_p(b)$, one can find $q, r \in \mathbb{Z}_N^*$ such that $a = bq + r$, where $r = 0$ or $v_p(r) \leq \gamma_0 v_p(b)$ [10]. Hence, the greatest divisor $(b-1,N)$ can be computed with the help of the Euclidean algorithm at polynomial number on $\log v_p(N)$ of arithmetic operations in $\mathbb{Z}_N^*$. It remains to show that $|B| \leq \frac{\varphi(N)}{2}$.

Let $N = pq$, where $p, q$ are distinct prime elements of $\mathbb{Z}^*_N$. Let $\varphi_p(p) = 2v_1u_1, \varphi_p(q) = 2v_2u_2$, where $v_1, v_2, u_1, u_2 \in \mathbb{N}$, and $u_1$ and $u_2$ are odd. Denote $v = \min \{v_1, v_2\}, K = (u_1v_1)(u_2v_2)$. It’s easy to see that the congruence $x^u \equiv 1 \pmod{N}$ is equivalent to the system $u \log_{\alpha x} x \equiv 0 \pmod{\varphi_p(p)}$, $u \log_{\beta x} x \equiv 0 \pmod{\varphi_p(q)}$, where $\alpha$ and $\beta$ are primitive elements in $\mathbb{Z}_p^*$ and $\mathbb{Z}_q^*$ respectively. Since $u$ is odd, so, by proposition 4, the congruence $x^u \equiv 1 \pmod{N}$ has exactly $K$ solutions. Let’s consider the congruence $x^{2^ju} \equiv 1 \pmod{N}$, where $j \in \{0,\ldots,t-1\}$. If $j < v$, then the similar arguments imply that the number of solutions is $4^jK$. If $j \geq v$, then the congruence has no solutions. Therefore $|B| = (1 + 1 + 4 + \ldots + 4^{v-1}) = \frac{4^v + 2}{3}$. Since $\varphi_p(N) = 2v_1v_2u_1u_2 \geq 4^vK$, so $\frac{|B|}{\varphi_p(N)} \leq \frac{1}{2}$ The theorem is proved.

Remark 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].

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

Proof. Let $N = pq$, where $p, q$ are distinct prime elements of $\mathbb{Z}_N^*$. Let $ed - 1 = k\varphi_p(N), \ k \in \mathbb{N}$. Since $v_p(p) + v_p(q) < (\alpha + 1)v_p(N)$, so

$$v_p(N) - \varphi_p(N) = v_p(p) + v_p(q) - 1 < (\alpha + 1)v_p(N).$$

(1)

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

$$\frac{(\alpha + 1)k}{d\sqrt{v_p(N)}} \leq \frac{(\alpha + 1)}{\sqrt{v_p(N)}} < \frac{1}{2d^2}$$

(2)

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

$$\left| \frac{e}{v_p(N) - \varphi_p(N)} - \frac{k}{d} \right| = \frac{1 - k(v_p(N) - \varphi_p(N))}{v_p(N)d} \leq \frac{(\alpha + 1)\sqrt{v_p(N)}}{v_p(N)d} < \frac{1}{2d^2}.$$  
(3)

Relation (3) means that $\frac{k}{d}$ is a successive fraction for the non-secret fraction $\frac{e}{v_p(N)}$. 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 $y = x^e \pmod{N}$ be an encrypted message $x \in \mathbb{Z}_N \setminus \{0\}$. To try to find the original text $x$ a cryptanalytic computes the terms of the sequence $y_i = y^{e^i} \pmod{N}, \ i = 1,2,\ldots$, 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.
Proposition 8. Let \( N = pq \), \( p, q \) be distinct prime elements of \( \mathbb{Z}[\sqrt{D}] \), \( \varphi_p(p) = rk \), \( \varphi_q(q) = sl \), where \( r \) and \( s \) are distinct prime numbers, \( (r, k) = (s, l) = 1 \). If \( y \in \mathbb{Z}_N^*[\sqrt{D}] \) is a random element, then \( \mathbb{P}(rs | \text{ord} y) = (1 - r^{-1})(1 - s^{-1}) \).

Proof. For any \( t_1 | k, t_2 | l \) there exist exactly \( \varphi(r(t_1)\varphi(st_2)) \) elements \( y \in \mathbb{Z}_N^*[\sqrt{D}] \) such that \( \text{ord} y = rs(t_1, t_2) \). Consequently, the number of elements \( y \in \mathbb{Z}_N^*[\sqrt{D}] \) such that \( rs | \text{ord} y \) is equal to

\[
\sum_{t_1 | k, t_2 | l} \varphi(r(t_1)\varphi(st_2)) = (r - 1)(s - 1) \sum_{t_1 | k, t_2 | l} \varphi(t_1)t_2 = (r - 1)(s - 1)k.
\]

(4)

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

Theorem 3. Let \( (N, e, d) \), \( N = pq \), be parameters of the generalized RSA-cryptosystem. Suppose that the numbers \( \varphi_p(p) \), \( \varphi_q(q) \) have distinct prime divisors \( r, s \) respectively, and the numbers \( r - 1, s - 1 \) have prime divisors \( r_1, s_1 \) respectively, then \( \mathbb{P}(m \geq r_1s_1) \geq (1 - r^{-1})(1 - s^{-1})(1 - r_1^{-1})(1 - s_1^{-1}) \), where \( m \) is the smallest natural number such that \( y^m = y \mod N \), \( y \in \mathbb{Z}_N^*[\sqrt{D}] \) is a random element.

Proof. Note that \( y^m = y \mod N \) iff \( \text{ord} y | (e^m - 1) \). By proposition 8,

\[
\mathbb{P}(rs | (e^m - 1)) \geq \mathbb{P}(rs | \text{ord} y) = (1 - r^{-1})(1 - s^{-1})
\]

Applying Theorem 14.1 [11], we conclude that

\[
\mathbb{P}(m \geq r_1s_1) \geq \mathbb{P}(r_1s_1 | m) \geq \mathbb{P}(r_1s_1 | \text{ord} e, rs | \text{ord} y) \geq (1 - r^{-1})(1 - s^{-1})(1 - r_1^{-1})(1 - s_1^{-1})
\]

The theorem is proved.

Remark 2. To secure the generalized RSA-cryptosystem of the iterated encryption attack we should take prime elements \( p, q \in \mathbb{Z}[\sqrt{D}] \) such that one can find big \( r, s \) and \( r_1, s_1 \) respectively.

Remark 3. If \( N = pq \), where \( p \) and \( q \) are such that the difference \( |v_p(p) - v_q(q)| \) is small, then it is easy to find the representation \( N = t^2 - s^2 \), where \( t, s \in \mathbb{Z}[\sqrt{D}] \) and this representation gives us the factorization of \( N \). Hence, the difference \( |v_p(p) - v_q(q)| \) should be quite large.

Remark 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 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 \( \mathbb{Z}[\sqrt{D}] \), 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 \( \mathbb{Z}[\sqrt{D}] \) – imaginary quadratic domain. We say that an element \( x = x_1 + x_2\sqrt{D} \in \mathbb{Z}[\sqrt{D}] \) is \( n \)-bit if integers \( x_1 \) and \( x_2 \) have less than \( n + 1 \) bits in the binary value. Let \( p = p_1 + p_2\sqrt{D}, q = q_1 + q_2\sqrt{D} \) be distinct prime \( n \)-bit elements of the domain \( \mathbb{Z}[\sqrt{D}] \). Let’s call RSA-cryptosystem with parameters \( p \) and \( q \) \( n \)-bit. Multiplication modulo \( N = pq \) of two \( n \)-bit elements of the domain \( \mathbb{Z}[\sqrt{D}] \) has the complexity \( O(n^2) \) and involution of \( n \)-bit element \( x \in \mathbb{Z}[\sqrt{D}] \) in the domain \( \mathbb{Z}[\sqrt{D}] \) has the complexity \( O(n^2 \log k) \). So encryption and decryption using the generalized RSA-cryptosystem in the domain \( \mathbb{Z}[\sqrt{D}] \) 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 \( \mathbb{Z}[\sqrt{D}] \). 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 \( \mathbb{Z}[\sqrt{D}] \) 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 \( \mathbb{Z}[\sqrt{D}] \) has the complexity \( O(16^n n^2 \log n) \). And also the number of binary operations to factorize RSA-modulus in the domain \( \mathbb{Z}[\sqrt{D}] \), is not less than the number of binary operations to factorize RSA-modulus in classical RSA-cryptosystem.

Example. Let the subscriber \( A \) wishes to send the secret message \( m = 1 + i \) with the signature \( P = 2t \) to the subscriber \( B \) with the help of the generalized RSA-cryptosystem in \( \mathbb{Z}[\sqrt{-1}] \) with \( \rho = -1 \). Let
\((N_A,e_A,d_A) = (589,7,98743)\) and \((N_B,e_B,d_B) = (559,13,167173)\), \(g_{N_B,N_A}(X) = x_1 + i x_2 + N_A\mathbb{Z}[i]\), \(X \in \mathbb{Z}_{N_B}[i]\), where \(x_1, x_2\) are the smallest nonnegative integers such that \(X = x_1 + i x_2 + N_B\mathbb{Z}[i]\). The subscriber \(A\) computes

\[m_1 = m^e_B \pmod{N_B} = 495 + 495i\]

and

\[P_1 = (P^e_B \pmod{N_B})^d_A \pmod{N_A} = 192i.\]

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

\[m_2 = m_1^{d_B} \pmod{N_B} = 1 + i\]

and

\[P_2 = (P_1^{e_A} \pmod{N_A})^{d_B} \pmod{N_B} = 2i.\]

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

References


Received 24.06.2015