New Attacks on RSA with Moduli $N = p^r q$

Abderrahmane Nitaj[1(✉)] and Tajjeeddine Rachidi[2]

[1] Laboratoire de Mathématiques Nicolas Oresme,
Université de Caen Basse Normandie, France
abderrahmane.nitaj@unicaen.fr
[2] School of Science and Engineering
Al Akhawayn University in Ifrane, Morocco
T.Rachidi@aui.ma

Abstract. We present three attacks on the Prime Power RSA with modulus $N = p^r q$. In the first attack, we consider a public exponent e satisfying an equation $ex - \phi(N)y = z$ where $\phi(N) = p^{r-1}(p-1)(q-1)$. We show that one can factor N if the parameters $|x|$ and $|z|$ satisfy $|xz| < N^{\frac{r(r-1)}{(r+1)^2}}$ thereby extending the recent results of Sakar [16]. In the second attack, we consider two public exponents e_1 and e_2 and their corresponding private exponents d_1 and d_2. We show that one can factor N when d_1 and d_2 share a suitable amount of their most significant bits, that is $|d_1 - d_2| < N^{\frac{r(r-1)}{(r+1)^2}}$. The third attack enables us to factor two Prime Power RSA moduli $N_1 = p_1^r q_1$ and $N_2 = p_2^r q_2$ when p_1 and p_2 share a suitable amount of their most significant bits, namely, $|p_1 - p_2| < \frac{p_1}{2rq_1q_2}$.

Keywords: RSA · Cryptanalysis · Factorization · Coppersmith's method · Prime Power RSA

1 Introduction

The RSA public-key cryptosystem, invented in 1978 by Rivest, Shamir and Adleman [15], is one of the most popular systems in use today. In the RSA cryptosystem, the public key is (N, e) where the modulus $N = pq$ is a product of two primes of the same bitsize, and the public exponent is a positive integer satisfying $ed \equiv 1 \pmod{\phi(N)}$. In RSA, encryption and decryption require executing heavy exponential multiplications modulo the large integer N. To reduce the decryption time, one may be tempted to use a small private exponent d. However, in 1990 Wiener [18] showed that RSA is insecure if $d < \frac{1}{3}N^{0.25}$, and Boneh and Durfee [2] improved the bound to $d < N^{0.292}$. In 2004, Blömer and May [1] combined both Wiener's method and Boneh and Durfee's method to show that RSA is insecure if the public exponent e satisfies an equation $ex + y = k\phi(N)$ with $x < \frac{1}{3}N^{\frac{1}{4}}$ and $|y| \leq N^{-\frac{3}{4}}ex$.

Partially supported by the French SIMPATIC (SIM and PAiring Theory for Information and Communications security).

S. El Hajji et al. (Eds.): C2SI 2015, LNCS 9084, pp. 352–360, 2015.
DOI: 10.1007/978-3-319-18681-8_28

Concurrent to these efforts, many RSA variants have been proposed in order to ensure computational efficiency while maintaining the acceptable levels of security. One such important variant is the Prime Power RSA. In Prime Power RSA the modulus N is in the form $N = p^r q$ for $r \geq 2$. In [17], Takagi showed how to use the Prime Power RSA to speed up the decryption process when the public and private exponents satisfy an equation $ed \equiv 1 \pmod{(p-1)(q-1)}$. As in the standard RSA cryptosystem, the security of the Prime Power RSA depends on the difficulty of factoring integers of the form $N = p^r q$.

Therefore, a Prime Power RSA modulus must be appropriately chosen, since it has to resist factoring algorithms such as the Number Field Sieve [10] and the Elliptic Curve Method [9]. Table 1, shows the suggested secure Power RSA forms as a function of the size of the modulus back in 2002 (see [4]). Note that, due to the ever increasing development of computing hardware, the form $N = p^2 q$ is no longer recommended for 1024 bit modulus.

Table 1. Optimal number of prime factors of a Prime Power RSA modulus [4]

Modulus size (bits)	1024	1536	2048	3072	4096	8192
Form of the modulus N	pq, p^2q	pq, p^2q	pq, p^2q	pq, p^2q	pq, p^2q, p^3q	pq, p^2q, p^3q, p^4q

In 1999, Boneh, Durfee, and Howgrave-Graham [3] presented a method for factoring $N = p^r q$ when r is large. Furthermore, Takagi [17] proved that one can factor N if $d < N^{\frac{1}{2(r+1)}}$, and May [13] improved the bound to $d < N^{\frac{r}{(r+1)^2}}$ or $d < N^{\frac{(r-1)^2}{(r+1)^2}}$. Very recently, Lu, Zhang and Lin [12] improved the bound to $d < N^{\frac{r(r-1)}{(r+1)^2}}$, and Sarkar [16] improved the bound for $N = p^2 q$ to $d < N^{0.395}$ and gave explicit bounds for $r = 3, 4, 5$.

In this paper, we focus on the Prime Power RSA with a modulus $N = p^r q$, and present three new attacks: In the first attack we consider a public exponent e satisfying an equation $ex - \phi(N)y = z$ where x and y are positive integers. Using a recent result of Lu, Zhang and Lin [12], we show that one can factor N in polynomial time if $|xz| < N^{\frac{r(r-1)}{(r+1)^2}}$. In the standard situation $z = 1$, the condition becomes $d = x < N^{\frac{r(r-1)}{(r+1)^2}}$ which improves the bound of May [13] for $r \geq 3$ and retrieves the bound of Lu, Zhang and Lin [12]. Note that unlike Sarkar [16] who solves $ex - \phi(N)y = 1$, we solve a more general equation $ex - \phi(N)y = z$. This leads to less constraints on the solution space, which in turn leads to an increase in the number of solutions to the equation. Intuitively speaking, our method has higher likelihood of finding solutions; that is, factoring RSA. In section 3, we shall present an example supporting this claim.

In the second attack, we consider an instance of the Prime Power RSA with modulus $N = p^r q$. We show that one can factor N if two private keys d_1 and d_2 share an amount of their most significant bits, that is if $|d_1 - d_2|$ is small enough. More precisely, we show that if $|d_1 - d_2| < N^{\frac{r(r-1)}{(r+1)^2}}$, then N can be factored in

polynomial time. The method we present is based on a recent result of [12] with Coppersmith's method for solving an univariate linear equation.

In the third attack, we consider two instances of the Prime Power RSA with two moduli $N_1 = p_1^r q_1$ and $N_2 = p_2^r q_2$ such that the prime factors p_1 and p_2 share an amount of their most significant bits, that is $|p_1 - p_2|$ is small. More precisely, we show that one can factor the RSA moduli N_1 and N_2 in polynomial time if $|p_1 - p_2| < \frac{p_1}{2rq_1q_2}$. The method we use for this attack is based on the continued fraction algorithm.

The rest of this paper is organized as follows: In Section 2, we briefly review the preliminaries necessary for the attacks, namely Coppersmith's technique for solving linear equations and the continued fractions theorem. In Section 3, we present the first attack on the Prime Power RSA, which is valid with no conditions on the prime factors. In Section 4, we present the second attack in the situation where two decryption exponents share an amount of their most significant bits. In Section 5, we present the third attack on the Prime Power RSA when the prime factors share an amount of their most significant bits. We then conclude the paper in Section 6.

2 Preliminaries

In this section, we present some basics on Coppersmith's method for solving linear modular polynomial equations and an overview of the continued fraction algorithm. Both techniques are used in the crafting of our attacks.

First, observe that if $N = p^r q$ with $q < p$, then $p^{r+1} > p^r q = N$, and $p > N^{\frac{1}{r+1}}$. Hence throughout this paper, we will use the inequality $p > N^\beta$ where $\beta = \frac{1}{r+1}$.

2.1 Linear Modular Polynomial Equations

In 1995, Coppersmith [5] developed powerful lattice-based techniques for solving both modular polynomial diophantine equations with one variable and two variables. These techniques have been generalized to more variables, and have served for cryptanalysis of many instances of RSA. More on this can be found in [14,8]. In [7], Herrmann and May presented a method for finding the small roots of a modular polynomial equation $f(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ where $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ and p is an unknown divisor of a known integer N. Their method is based on the seminal work of Coppersmith [5]. Very recently, Lu, Zhang and Lin [12] presented a generalization for finding the small roots of a modular polynomial equation $f(x_1, \ldots, x_n) \equiv 0 \pmod{p^v}$, where p^v is a divisor of some composite integer N. For the bivariate case, they proved the following result, which we shall use in the crafting of our attacks.

Theorem 1 (Lu, Zhang and Lin). *Let N be a composite integer with a divisor p^u such that $p \geq N^\beta$ for some $0 < \beta \leq 1$. Let $f(x, y) \in \mathbb{Z}[x, y]$ be a homogenous linear polynomial. Then one can find all the solutions (x, y) of*

the equation $f(x, y) = 0 \mod p^v$ *with* $\gcd(x, y) = 1$, $|x| < N^{\gamma_1}$, $|y| < N^{\gamma_2}$, *in polynomial time if*

$$\gamma_1 + \gamma_2 < uv\beta^2.$$

2.2 The Continued Fractions Algorithm

We present here the well known result of Legendre on convergents of a continued fraction expansion of a real number. The details can be found in [6]. Let ξ be a positive real number. Define $\xi_0 = \xi$ and for $i = 0, 1, \ldots, n$, $a_i = \lfloor \xi_i \rfloor$, $\xi_{i+1} = 1/(\xi_i - a_i)$ unless ξ_i is an integer. This expands ξ as a continued fraction in the following form:

$$\xi = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \cfrac{1}{\ddots}}}}, \; a_0 \in \mathbb{N}, \text{ and } a_i \in \mathbb{N}^* \text{ for } i \geq 1,$$

which is often rewritten as $\xi = [a_0, a_1, \ldots, a_n, \ldots]$. For $i \geq 0$, the rational numbers $[a_0, a_1, \ldots, a_i]$ are the convergents of ξ. If $\xi = \frac{a}{b}$ is a rational number, then $\xi = [a_0, a_1, \ldots, a_n]$ for some positive integer n, and the continued fraction expansion of ξ is finite with the total number of convergents being polynomial in $\log(b)$. The following result enables one to determine if a rational number $\frac{a}{b}$ is a convergent of the continued fraction expansion of a real number ξ (see Theorem 184 of [6]).

Theorem 2 (Legendre). *Let* ξ *be a positive real number. Suppose* $\gcd(a, b) = 1$ *and*

$$\left| \xi - \frac{a}{b} \right| < \frac{1}{2b^2}.$$

Then $\frac{a}{b}$ *is one of the convergents of the continued fraction expansion of* ξ.

Note that the continued fractions expansion process is polynomial in time.

3 The First Attack on Prime Power RSA with Modulus $N = p^r q$

In this section, we present an attack on the Prime Power RSA when the public key (N, e) satisfies an equation $ex - \phi(N)y = z$ with small parameters x and $|z|$.

Theorem 3. *Let* $N = p^r q$ *be a Prime Power RSA modulus and* e *a public exponent satisfying the equation* $ex - \phi(N)y = z$ *with* $1 < e < \phi(N)$ *and* $\gcd(e, \phi(N)) = 1$. *Then one can factor* N *in polynomial time if*

$$|xz| < N^{\frac{r(r-1)}{(r+1)^2}}.$$

Proof. Suppose that $e < N$ satisfies an equation $ex - \phi(N)y = z$ with $|x| < N^{\delta}$ and $|z| < N^{\gamma}$. Then, since $\phi(N) = p^{r-1}(p-1)(q-1)$, we get $ex - z \equiv 0 \pmod{p^{r-1}}$. Applying Theorem 1 with $u = r$, $v = r-1$ and $\beta = \frac{1}{r+1}$, we can solve the equation in polynomial time if

$$\delta + \gamma < uv\beta^2 = \frac{r(r-1)}{(r+1)^2},$$

that is $|xz| < N^{\frac{r(r-1)}{(r+1)^2}}$. Since $\frac{e}{\phi(N)} < 1$, then, using x and z in the equation $ex - \phi(N)y = z$, we get for sufficiently large N comparatively to r,

$$y = \frac{ex - z}{\phi(N)} < \frac{e|x|}{\phi(N)} + \frac{|z|}{\phi(N)} < |x| + |z| \leq 1 + |xz| < 1 + N^{\frac{r(r-1)}{(r+1)^2}} < N.$$

Hence

$$\gcd(ex - z, N) = \gcd(p^{r-1}(p-1)(q-1)y, p^r q) = g,$$

with $g = p^{r-1}$, $g = p^r$ or $g = p^{r-1}q$. If $g = p^{r-1}$, then $p = g^{\frac{1}{r-1}}$, if $g = p^r$, then $p = g^{\frac{1}{r}}$ and if $g = p^{r-1}q$, then $p = \frac{N}{g}$. This leads to the factorization of N. □

Example 1. For $r = 2$ and $N = p^r q$, let us take for N and e the 55 digit numbers

$$N = 813804457829711731948201844114807225219999676952237102 1,$$
$$e = 119999523060102112620134365161110795748025135435588302 9.$$

In order to solve the diophantine equation $ex - \phi(N)y = z$, we transformed it into the equation $ex - z \equiv 0 \pmod{p^{r-1}}$ using Theorem 3. To be able to apply Coppersmith's technique via Theorem 1, we chose the parameters $m = 7$, $t = 6$ so that the dimension of constructed the lattice is 36, and $X = \left\lfloor N^{\frac{r(r-1)}{(r+1)^2}} \right\rfloor = 1592999974064$. We built the lattice using the polynomial $f(x_1, x_2) = x_1 + ex_2$, then applied the LLL algorithm [11], and used Gröbner basis method to find the smallest solution $x_1 = -11537$ and $x_2 = 7053$ to $f(x_1, x_2) \equiv 0 \pmod{p^{r-1}}$ in 174 seconds using an off-the-shelf computer. From this solution, we deduced $p = gcd(x_1 + ex_2, N) = 2294269585934949239$, and finally recovered $q = \frac{N}{p^2} = 1546077175000723901$. We then computed $\phi(N)$ and $d \equiv e^{-1} \pmod{\phi(N)}$ as follows:

$$\phi(N) = 813804457829711731067122766808956194625789692526157980 0,$$
$$d = 201599474774838877298243639381121331736197186551075626 9.$$

Observe that $d \approx N^{0.98}$ which is out of range of Sarkar's bound [16] which can only retrieve private keys $d < N^{0.395}$ for $r = 2$.

4 The Second Attack on Prime Power RSA Using Two Decryption Exponents

In this section, we present an attack on the Prime Power RSA when two private exponents d_1 and d_2 share an amount of their most significant bits, that is $|d_1 - d_2|$ is small.

Theorem 4. *Let $N = p^r q$ be an RSA modulus and d_1 and d_2 be two private exponents. Then, one can factor N in polynomial time, if*

$$|d_1 - d_2| < N^{\frac{r(r-1)}{(r+1)^2}}.$$

Proof. Suppose that $e_1 d_1 - k_1\phi(N) = 1$ and $e_2 d_2 - k_2\phi(N) = 1$ with $e_1 > e_2$. Hence $e_1 d_1 \equiv 1 \pmod{\phi(N)}$ and $e_2 d_2 \equiv 1 \pmod{\phi(N)}$. Multiplying the first equation by e_2 and the second by e_1 and subtracting, we get

$$e_1 e_2 (d_1 - d_2) \equiv e_2 - e_1 \pmod{\phi(N)}.$$

Since $\phi(N) = p^{r-1}(p-1)(q-1)$, we get $e_1 e_2 (d_1 - d_2) \equiv e_2 - e_1 \pmod{p^{r-1}}$. Now, consider the modular linear equation

$$e_1 e_2 x - (e_2 - e_1) \equiv 0 \pmod{p^{r-1}},$$

$d_1 - d_2$ is a root of such equation. Suppose further that $|d_1 - d_2| < N^{\delta}$, then applying Theorem 1 with $u = r$, $v = r - 1$ and $\beta = \frac{1}{r+1}$ will lead to the solution $x = d_1 - d_2$ obtained in polynomial time if

$$\delta < uv\beta^2 = \frac{r(r-1)}{(r+1)^2}.$$

That is if $|d_1 - d_2| < N^{\frac{r(r-1)}{(r+1)^2}}$. Computing

$$\gcd(e_1 e_2 x - (e_2 - e_1), N) = \gcd\left(p^{r-1}(p-1)(q-1)y, p^r q\right) = g,$$

will lead to determining p, hence factoring N as follows: $p = g^{\frac{1}{r-1}}$ when $g = p^{r-1}$, or $p = g^{\frac{1}{r}}$ when $g = p^r$, or $p = \frac{N}{g}$ if $g = p^{r-1}q$. □

Example 2. Let us present an example corresponding to Theorem 4. Consider $N = p^2 q$ with

$$\begin{aligned} N &= 609325385148612087885947195839973772588594652655362621 9, \\ e_1 &= 274960038184748738971596476723561880252967585560637741 1, \\ e_2 &= 357508124495241400931639650151237222654589255889827655 1. \end{aligned}$$

The polynomial equation is $f(x) = e_1 e_2 x - (e_2 - e_1) \equiv 0 \pmod{p^{r-1}}$, which can be transformed into $g(x) = x - a \equiv 0 \pmod{p^{r-1}}$ where $a \equiv (e_2 - e1)(e_1 e_2)^{-1} \pmod{N}$. Using $m = 8$ and $t = 6$, we built a lattice with dimension $\omega = 9$. Applying the LLL algorithm [11] and solving the first reduced polynomials, we get the solution $x_0 = 1826732340$. Hence $\gcd(f(x_0), N) = p = 1789386140116417697$ and finally $q = \frac{N}{p^2} = 1903010275819064491$. The whole process took less than 4 seconds using an off-the-shelf computer. Then, using $\phi(N) = p(p-1)(q-1)$, we retrieved the private exponents $d_1 \equiv e_1^{-1} \pmod{\phi(N)}$ and $d_2 \equiv e_2^{-1} \pmod{\phi(N)}$. Note that again $d_1 \approx d_2 \approx N^{0.99}$ which Sarkar's method with the bound $d < N^{0.395}$ could not possibly retrieve.

5 The Third Attack on Prime Power RSA with Two RSA Moduli

In this section, we consider two Prime Power RSA moduli $N_1 = p_1^r q_1$ and $N_2 = p_2^r q_2$, where p_1 and p_2 share an amount of their most significant bits.

Theorem 5. *Let $N_1 = p_1^r q_1$ and $N_2 = p_2^r q_2$ be two RSA moduli with $p_1 > p_2$. If*

$$|p_1 - p_2| < \frac{p_1}{2rq_1q_2},$$

then, one can factor N in polynomial time.

Proof. Suppose that $N_1 = p_1^r q_1$ and $N_2 = p_2^r q_2$ with $p_1 > p_2$. Then $q_2 N_1 - q_1 N_2 = q_1 q_2 (p_1^r - p_2^r)$. Hence

$$\left| \frac{N_2}{N_1} - \frac{q_2}{q_1} \right| = \frac{q_1 q_2 \, |p_1^r - p_2^r|}{q_1^2 p_1^r}.$$

In order to apply Theorem 2, we need that $\frac{q_1 q_2 |p_1^r - p_2^r|}{q_1^2 p_1^r} < \frac{1}{2q_1^2}$, or equivalently

$$|p_1^r - p_2^r| < \frac{p_1^r}{2q_1 q_2}. \tag{1}$$

Observe that

$$|p_1^r - p_2^r| = |p_1 - p_2| \sum_{i=0}^{r-1} p_1^{r-1-i} p_2^i < r|p_1 - p_2| p_1^{r-1}.$$

Then (1) is fulfilled if $r|p_1 - p_2| p_1^{r-1} < \frac{p_1^r}{2q_1 q_2}$, that is if

$$|p_1 - p_2| < \frac{p_1}{2rq_1q_2}.$$

Under this condition, we get $\frac{q_2}{q_1}$ among the convergents of the continued fraction expansion of $\frac{N_2}{N_1}$. Using q_1 and q_2, we get $p_1 = \left(\frac{N_1}{q_1}\right)^{\frac{1}{r}}$ and $p_2 = \left(\frac{N_2}{q_2}\right)^{\frac{1}{r}}$. □

Example 3. We present here an example corresponding to Theorem 5. Consider $N_1 = p_1^2 q_1$ and $N_2 = p_2^2 q_2$ with

$$N_1 = 17098723391376942050589691743730471981669135383303448246 1,$$
$$N_2 = 12053291181972688288163071400313523776667560282425096592 1.$$

We applied the continued fraction algorithm to compute the first 40 convergents of $\frac{N_2}{N_1}$. Every convergent is a candidate for the ratio $\frac{q_2}{q_1}$ of the prime factors. One of the convergents is $\frac{36443689}{51698789}$ leading to $q_2 = 36443689$ and $q_1 = 51698789$. This gives the prime factors p_1 and p_2

$$p_1 = \sqrt{\frac{N_1}{q_1}} = 1818618724382942951460443,$$

$$p_2 = \sqrt{\frac{N_2}{q_2}} = 1818618724382943035672683.$$

6 Conclusion

In this paper, we have considered the Prime Power RSA with modulus $N = p^r q$ and public exponent e. We presented three new attacks to factor the modulus in polynomial time. The first attack can be applied if small parameters x, y and z satisfying the equation $ex - \phi(N)y = z$ can be found . The second attack can be applied when two private exponents d_1 and d_2 share an amount of their most significant bits. The third attack can be applied when two Prime Power RSA moduli $N_1 = p_1^r q_1$ and $N_2 = p_2^r q_2$ are such that p_1 and p_2 share an amount of their most significant bits.

References

1. Blömer, J., May, A.: A Generalized Wiener Attack on RSA. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 1–13. Springer, Heidelberg (2004)
2. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 1–11. Springer, Heidelberg (1999)
3. Boneh, D., Durfee, G., Howgrave-Graham, N.: Factoring tex2html_wrap_inline127 for Large r. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 326–337. Springer, Heidelberg (1999)
4. Compaq Computer Corperation. Cryptography using Compaq multiprime technology in a parallel processing environment (2002), ftp://ftp.compaq.com/pub/solutions/CompaqMultiPrimeWP.pdf
5. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology 10(4), 233–260 (1997)
6. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Oxford University Press, London (1975)
7. Herrmann, M., May, A.: Solving linear equations modulo divisors: On factoring given any bits. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 406–424. Springer, Heidelberg (2008)
8. Hinek, M.J.: Cryptanalysis of RSA and its variants. Chapman & Hall/CRC Cryptography and Network Security. CRC Press, Boca Raton (2010)
9. Lenstra, H.: Factoring integers with elliptic curves. Annals of Mathematics 126, 649–673 (1987)
10. Lenstra, A.K., Lenstra Jr., H.W.: The Development of the Number Field Sieve. Lecture Notes in Mathematics, vol. 1554. Springer, Heidelberg (1993)
11. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische Annalen 261, 513–534 (1982)
12. Lu, Y., Zhang, R., Lin, D.: New Results on Solving Linear Equations Modulo Unknown Divisors and its Applications, Cryptology ePrint Archive, Report 2014/343 (2014), https://eprint.iacr.org/2014/343
13. May, A.: Secret Exponent Attacks on RSA-type Schemes with Moduli $N = p^r q$. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 218–230. Springer, Heidelberg (2004)
14. May, A.: Using LLL-reduction for solving RSA and factorization problems: a survey. In: LLL+25 Conference in Honour of the 25th Birthday of the LLL Algorithm. Springer, Heidelberg (2007)

15. Rivest, R., Shamir, A., Adleman, L.: A Method for Obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21(2), 120–126 (1978)
16. Sarkar, S.: Small secret exponent attack on RSA variant with modulus $N = p^r q$. Designs, Codes and Cryptography 73(2), 383–392 (2015)
17. Takagi, T.: Fast RSA-type cryptosystem modulo $p^k q$. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 318–326. Springer, Heidelberg (1998)
18. Wiener, M.: Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory 36, 553–558 (1990)