A new attack on RSA with a composed decryption exponent

Abderrahmane Nitaj[1] and Mohamed Ould Douh[1,2]

[1] Laboratoire de Mathématiques Nicolas Oresme
Université de Caen, Basse Normandie, France
abderrahmane.nitaj@unicaen.fr
mohamed.douh@unicaen.fr
[2] Université des Sciences, de Technologie et de Médecine
Nouakchott - Mauritania
mdouh@univ-nkc.mr

Abstract. In this paper, we consider an RSA modulus $N = pq$, where the prime factors p, q are of the same size. We present an attack on RSA when the decryption exponent d is in the form $d = Md_1 + d_0$ where M is a given positive integer and d_1 and d_0 are two suitably small unknown integers. In 1999, Boneh and Durfee presented an attack on RSA when $d < N^{0.292}$. When $d = Md_1 + d_0$, our attack enables one to overcome Boneh and Durfee's bound and to factor the RSA modulus.

KEYWORDS: RSA, Cryptanalysis, Factorization, LLL algorithm, Coppersmith's method

1 Introduction

The RSA cryptosystem [13] (see also [1] and [3]) was invented in 1978 by Rivest, Shamir and Adleman and is today one of the most popular cryptosystems. The main parameters in RSA are the modulus $N = pq$, which is the product of two large primes of the same bit-size, that is $q < p < 2q$, and a public exponent e such that $\gcd(e, \phi(N)) = 1$ where $\phi(N)$ is Euler's totient function. The public exponent e is related to the private exponent d by an equation of the form $ed - k\phi(N) = 1$. For efficiency reasons, it might be tempting to select a small RSA private exponent d. In 1990, Wiener[14] showed that RSA is insecure if $d < \frac{1}{3}N^{0.25}$. His attack makes use of the continued fractions method and had an important impact on the design of RSA. Wiener's bound was later subsequently improved to $d < N^{0.292}$ by Boneh and Durfee[4]. Their method is based on Coppersmith's technique[6] for finding small solutions of modular polynomial equations, which in turn is based on the LLL lattice reduction algorithm [10]. A related problem is to attack the RSA cryptosystem when an amount of bits of the private exponent d are known to the adversary. This problem was introduced by Boneh, Durfee and Frankel [5] in 1998. It is called the partial key exposure problem and is related to the study of side channel attacks such as fault attacks, timing attacks and power analysis. In most cases, the partial key exposure attacks are based on the knowledge of the most significant bits or the least significant bits of the private exponent d. Boneh, Durfee and Frankel showed that for low public exponent e and full private exponent d, that is $d \approx N \approx 2^n$, if $d = Md_1 + d_0$ where d_0 and $M \geq 2^{\frac{n}{4}}$ are known, then all d can be computed in polynomial time. Their method makes use of Coppersmith's technique [6]. More partial key exposure attacks are presented by Blömer and May in [2] and by Ernst, Jochemsz, May and de Weger in [7]. These attacks extend the size of the public exponent e up to N.

All partial key exposure results on RSA presented so far have in common that the private exponent d is of the shape $d = Md_1 + d_0$ where $M \geq 2^{\frac{n}{4}}$ and d_0 are known, or of the shape $d = d_1 + d_0$ where d_1 is known and d_0 is small. In this paper, we consider the situation with $d = Md_1 + d_0$ where M is known and d_1 and d_0 are unknown. We show that one can find the factorization of N if d_1 and d_0 are suitably small. Namely, suppose that

$$e = N^{\alpha}, \quad M = N^{\beta}, \quad d_1 < N^{\delta}, \quad d_0 < N^{\gamma}.$$

We show that if

$$\delta < \frac{1}{4}\left(5 - 4\gamma - \sqrt{12\alpha + 12\beta - 12\gamma + 3}\right),$$

then there is a polynomial time algorithm to factor the modulus N, which breaks the RSA cryptosystem. The starting point of the attack is the key equation $ed - k\phi(N) = 1$, which can be rewritten as

$$ed_0 - kN + k(p + q - 1) - 1 \equiv 0 \pmod{Me}.$$

From the left side, we derive a polynomial $f(x, y, z) = ex - Ny + yz - 1$ and use Coppersmith's method to solve the modular equation $f(x, y, z) \equiv 0 \pmod{Me}$. When we perform the LLL algorithm in Coppersmith's method, we find three polynomials $h_i(x, y, z)$ for $1 \leq i \leq 3$. Since $(d_0, k, p+q-1)$ is a small solution of the equation $f(x, y, z) \equiv 0 \pmod{Me}$, then, using the resultant process or the Gröbner basis computation, we can find z_0 such that $z_0 = p+q-1$. Hence using $p + q - 1 = z_0$ and $pq = N$, one can find p and q. We note that Coppersmith's method applied with multivariate polynomials relies on the following heuristic assumption which is supposed to hold true for $n \geq 3$ variables.

Assumption 1. *The resultant computations for the polynomials* $h_i(x, y, z)$ *for* $1 \leq i \leq 3$ *yield nonzero polynomials.*

The rest of the paper is organized as follows. In Section 2, we give some basics on lattices, lattice reduction and Coppersmith's method. In Section 3, we present our attack on RSA when the private exponent d satisfies $d = Md_1 + d_0$ with known M. We conclude in Section 4.

2 Preliminaries

In this section, we present a few basic facts about lattices, lattice basis reduction, Coppersmith's method for solving modular polynomial equations and Howgrave-Graham's theorem.

Let $b_1, \cdots, b_\omega \in \mathbb{R}^n$ be ω linearly independent vectors where ω and n are two positive integers satisfying $\omega \leq n$. The lattice $\mathcal{L}$ spanned by $\{b_1, \cdots, b_\omega\}$ is the set of linear combinations of the vectors $b_1, \cdots, b_\omega \in \mathbb{R}^n$ using integer coefficients, that is

$$\mathcal{L} = \left\{ \sum_{i=1}^{\omega} \lambda_i b_i \mid x_i \in \mathbb{Z} \right\}.$$

We say that the set $\{b_1, \cdots, b_\omega\}$ is a lattice basis for $\mathcal{L}$, and ω is its dimension. This is denoted as $\dim(\mathcal{L}) = \omega$. The lattice is called full rank if $\omega = n$. When $\omega = n$, the determinant is equal to the absolute value of the determinant of the matrix whose rows are the basis vectors $b_1, \cdots, b_\omega$, that is

$$\det(\mathcal{L}) = |\det(b_1, \cdots, b_\omega)|$$

If $b = \sum_{i=1}^{\omega} \lambda_i b_i$ is a vector of $\mathcal{L}$, the Euclidean norm of b is

$$\|b\| = \left(\sum_{i=1}^{\omega} \lambda_i^2 \right)^{\frac{1}{2}}.$$

A lattice has infinitely many bases with the same determinant and it is useful to find a basis of small vectors. However, finding the shortest nonzero vector in a lattice is very hard in general. In 1982, Lenstra, Lenstra and Lovász [10] invented the so-called LLL algorithm to reduce a basis and to approximate a shortest lattice vector in time polynomial in the bit-length of the entries of the basis matrix and in the dimension of the lattice. In the following theorem, we state a general result on the size of the individual reduced basis vectors. A proof can be found in [11].

Theorem 1 (LLL). *Let $\mathcal{L}$ be a lattice of dimension ω. In polynomial time, the LLL- algorithm outputs a reduced basis $\{v_1, \cdots, v_\omega\}$ that satisfy*

$$\|v_1\| \leq \|v_2\| \leq \cdots \leq \|v_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i}} \det(\mathcal{L})^{\frac{1}{\omega+1-i}},$$

for all $1 \leq i \leq \omega$.

In 1996, Coppersmith [6] proposed rigorous techniques to compute small roots of bivariate polynomials over the integers and univariate modular polynomials using the LLL algorithm. The methods extend heuristically to more variables. In 1997, Howgrave-Graham [8] reformulated Coppersmith's techniques and proposed the following result in terms of the Euclidean norm of the polynomial $f(x_1, \ldots, x_n) = \sum a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$ which is defined by

$$\|f(x_1, \ldots, x_n)\| = \sqrt{\sum a_{i_1,\ldots,i_n}^2}.$$

Theorem 2 (Howgrave-Graham). *Let $f(x_1,\dots,x_n) \in \mathbb{Z}[x_1,\dots,x_n]$ be a polynomial which is a sum of at most ω monomials. Suppose that*

$$\begin{aligned} &f\left(x_1^{(0)},\dots,x_n^{(0)}\right) \equiv 0 \pmod{(Me)^m},\\ &\left|x_1^{(0)}\right| < X_1,\dots,\left|x_n^{(0)}\right| < X_n,\\ &\|f(x_1X_1,\dots,x_nX_n)\| < \frac{(Me)^m}{\sqrt{\omega}}. \end{aligned}$$

Then $f\left(x_1^{(0)},\dots,x_n^{(0)}\right) = 0$ holds over the integers.

Using Theorem 1, if

$$2^{\frac{\omega(\omega-1)}{4(\omega+1-n)}}\det(\mathcal{L})^{\frac{1}{\omega+1-n}} \leq \frac{(Me)^m}{\sqrt{\omega}},$$

then we can find n polynomials $v_i(x_1,\dots,x_n)$, $1 \leq i \leq n$, that share the root $\left(x_1^{(0)},\dots,x_n^{(0)}\right)$ over the integers.

We terminate this section by two useful results (see. [12]). Let $N = pq$ be an RSA modulus with $q < p < 2q$. Then the prime factors p and q satisfy the following properties

$$\frac{\sqrt{2}\sqrt{N}}{2} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N}, \tag{1}$$

$$2\sqrt{N} < p+q < \frac{3\sqrt{2}\sqrt{N}}{2}. \tag{2}$$

3 The Attack

In this section, we present our new attack on RSA when the private exponent is in the form $d = Md_1 + d_0$ with a known integer M and suitably small unknown integers d_1 and d_2. A typical example is $M = 2^m$ for some positive integer m.

Theorem 3. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $M = N^\beta$ be a positive integer and $e = N^\alpha$ a public exponent satisfying $ed - k\phi(N) = 1$ with $d = Md_1 + d_0$. Suppose that $d_1 \leq N^\delta$ and $d_0 < N^\gamma$. Then one can factor N in polynomial time if*

$$\delta < \frac{1}{4}\left(5 - 4\gamma - \sqrt{12\alpha + 12\beta - 12\gamma + 3}\right).$$

Proof. Let M be a known integer. Suppose that $d = Md_1 + d_0$. The starting point is the RSA key equation $ed - k\phi(N) = 1$ where $\phi(N) = N - p - q + 1$. Hence $e\left(Md_1 + d_0\right) - k(N-p-q+1) = 1$ and $Med_1 + ed_0 - kN + k(p+q-1) = 1$. Taking this equation modulo Me, we get $ed_0 - kN + k(p+q-1) - 1 \equiv 0 \pmod{Me}$. Consider the polynomial

$$f(x,y,z) = ex - Ny + yz - 1.$$

Then $(x_0, y_0, z_0) = (d_0, k, p+q-1)$ is a root modulo Me. Define

$$e = N^{\alpha}, \quad M = N^{\beta}, \quad X = N^{\gamma}, \quad Y = 2N^{\alpha+\beta+\delta-1}, \quad Z = \frac{3\sqrt{2}}{2}N^{\frac{1}{2}}. \tag{3}$$

Suppose that $d_1 < N^{\delta}$ and $d_0 < N^{\gamma}$ where $\gamma < \beta+\delta$. Then $d = Md_1 + d_0 < 2N^{\beta+\delta}$. Hence, since $\phi(N) \approx N$, we get

$$k = \frac{ed-1}{\phi(N)} < \frac{ed}{\phi(N)} < \frac{2N^{\alpha+\beta+\delta}}{\phi(N)} \approx 2N^{\alpha+\beta+\delta-1} = Y.$$

On the other hand, using (2), we get $p+q < \frac{3\sqrt{2}}{2}N^{\frac{1}{2}}$. Summarizing, the root $(x_0, y_0, z_0) = (d_0, k, p+q-1)$ modulo Me of the polynomial $f(x,y,z)$ satisfies

$$x_0 < X, \quad y_0 < Y, \quad z_0 < Z.$$

To apply Coppersmith's method [6] to find the small modular roots of the equation $f(x,y,z) \equiv 0 \pmod{Me}$, we use the extended strategy of Jochemsz and May [9]. Define the set

$$M_k = \bigcup_{0\le j\le t} \{x^{i_1}y^{i_2}z^{i_3+j} \;\Big|\; x^{i_1}y^{i_2}z^{i_3} \quad \text{monomial of} \quad f^m(x,y,z)$$
$$\text{and} \quad \frac{x^{i_1}y^{i_2}z^{i_3}}{(yz)^k} \quad \text{monomial of} \quad f^{m-k}\}.$$

Observe that $f^m(x,y,z)$ is in the form

$$f^m(x,y,z) = \sum_{i_1=0}^{m}\sum_{i_2=0}^{m-i_1}\sum_{i_3=0}^{i_2} a_{i_1,i_2,i_3}x^{i_1}y^{i_2}z^{i_3},$$

where the coefficients a_{i_1,i_2,i_3} do not depend on x, y nor z. This gives the following properties

$$\begin{aligned} x^{i_1}y^{i_2}z^{i_3} \in f^m &\;\text{ if }\; i_1 = 0,\ldots,m,\; i_2 = 0,\ldots,m-i_1,\; i_3 = 0,\ldots,i_2, \\ x^{i_1}y^{i_2}z^{i_3} \in f^{m-k} &\;\text{ if }\; i_1 = 0,\ldots,m-k,\; i_2 = 0,\ldots,m-k-i_1,\; i_3 = 0,\ldots,i_2. \end{aligned}$$

Hence, if $x^{i_1}y^{i_2}z^{i_3}$ is a monomial of $f^m(x,y,z)$, then $\frac{x^{i_1}y^{i_2}z^{i_3}}{y^kz^k}$ is a monomial of $f^{m-k}(x,y,z)$ for

$$i_1 = 0,\ldots,m-k, \quad i_2 = k,\ldots,m-i_1, \quad i_3 = k,\ldots,i_2.$$

For $0 \le k \le m$, we obtain

$$x^{i_1}y^{i_2}z^{i_3} \in M_k \quad \text{if} \quad i_1 = 0,\ldots,m-k, \quad i_2 = k,\ldots,m-i_1, \quad i_3 = k,\ldots,i_2+t.$$

From this, we deduce

$$x^{i_1}y^{i_2}z^{i_3} \in M_{k+1} \text{ if } i_1 = 0,\ldots,m-k-1, \quad i_2 = k+1,\ldots,m-i_1,\; i_3 = k+1,\ldots,i_2+t.$$

For $0 \leq k \leq m$, define the polynomials

$$g_{k,i_1,i_2,i_3}(x,y,z) = \frac{x^{i_1}y^{i_2}z^{i_3}}{y^k z^k} f(x,y,z)^k (Me)^{m-k} \quad \text{with} \quad x^{i_1}y^{i_2}z^{i_3} \in M_k \setminus M_{k+1}.$$

These polynomials reduce to the following sets

$$\begin{cases} k = 0,\dots,m, \\ i_1 = 0,\dots,m-k, \\ i_2 = k,\dots,m-i_1, \\ i_3 = k, \end{cases} \quad \text{or} \quad \begin{cases} k = 0,\dots,m, \\ i_1 = 0,\dots,m-k, \\ i_2 = k, \\ i_3 = k+1,\dots,i_2+t. \end{cases} \tag{4}$$

Consequently, the polynomials $g_{k,i_1,i_2,i_3}(x,y,z)$ are in one of the following forms

$$\begin{aligned} &G_{k,i_1,i_2,i_3}(x,y,z) = x^{i_1}y^{i_2-k} f(x,y,z)^k (Me)^{m-k}, \\ &\text{for} \quad k = 0,\dots m, \quad i_1 = 0,\dots m-k, \quad i_2 = k,\dots,m-i_1, \quad i_3 = k, \\ &H_{k,i_1,i_2,i_3}(x,y,z) = x^{i_1}z^{i_3-k} f(x,y,z)^k (Me)^{m-k}, \\ &\text{for} \quad k = 0,\dots m, \quad i_1 = 0,\dots,m-k, \quad i_2 = k, \quad i_3 = k+1,\dots,i_2+t. \end{aligned}$$

Define the lattice $\mathcal{L}$ spanned by the coefficients of the vectors $G_{k,i_1,i_2,i_3}(x,y,z)$ and $H_{k,i_1,i_2,i_3}(x,y,z)$. For $m = 2$ and $t = 1$, the matrix of $\mathcal{L}$ is presented in Table 1. The non-zero elements are marked with an '$\circledast$'.

	1	y	y^2	x	xy	x^2	yz	y^2z	xyz	y^2z^2	z	xz	x^2z	yz^2	xyz^2	y^2z^3
$G_{0,0,0,0}$	$(Me)^2$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,0,1,0}$	0	$(Me)^2Y$	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,0,2,0}$	0	0	$(Me)^2Y^2$	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,1,0,0}$	0	0	0	$(Me)^2X$	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,1,1,0}$	0	0	0	0	$(Me)^2XY$	0	0	0	0	0	0	0	0	0	0	0
$G_{0,2,0,0}$	0	0	0	0	0	$(Me)^2X^2$	0	0	0	0	0	0	0	0	0	0
$G_{1,0,1,1}$	⊛	⊛	0	⊛	0	0	$MeYZ$	0	0	0	0	0	0	0	0	0
$G_{1,0,2,1}$	0	⊛	⊛	0	⊛	0	0	MeY^2Z	0	0	0	0	0	0	0	0
$G_{1,1,1,1}$	0	0	0	⊛	⊛	⊛	0	0	$MeXYZ$	0	0	0	0	0	0	0
$G_{2,0,2,2}$	⊛	⊛	⊛	⊛	⊛	⊛	⊛	⊛	⊛	Y^2Z^2	0	0	0	0	0	0
$H_{0,0,0,1}$	0	0	0	0	0	0	0	0	0	0	$(Me)^2Z$	0	0	0	0	0
$H_{0,1,0,1}$	0	0	0	0	0	0	0	0	0	0	0	$(Me)^2XZ$	0	0	0	0
$H_{0,2,0,1}$	0	0	0	0	0	0	0	0	0	0	0	0	$(Me)^2X^2Z$	0	0	0
$H_{1,0,1,2}$	0	0	0	0	0	0	⊛	0	0	0	⊛	⊛	0	$MeYZ^2$	0	0
$H_{1,1,1,2}$	0	0	0	0	0	0	0	0	⊛	0	0	⊛	⊛	0	$MeXYZ^2$	0
$H_{2,0,2,3}$	0	0	0	0	0	0	⊛	⊛	⊛	⊛	⊛	⊛	⊛	⊛	⊛	Y^2Z^3

Table 1. The coefficient matrix for the case $m = 2$, $t = 1$.

Notice that the matrix is triangular so that the values marked with the symbol $\circledast$ do not contribute in the calculation of the determinant. Indeed, the determinant is in the form

$$\det(\mathcal{L}) = (Me)^{n_e} X^{n_X} Y^{n_Y} Z^{n_Z}. \tag{5}$$

Using the bounds (4), we get

$$\begin{aligned} n_e &= \sum_{k=0}^{m}\sum_{i_1=0}^{m-k}\sum_{i_2=k}^{m-i_1}\sum_{i_3=k}^{k}(m-k) + \sum_{k=0}^{m}\sum_{i_1=0}^{m-k}\sum_{i_2=k}^{k}\sum_{i_3=k+1}^{i_2+t}(m-k) \\ &= \frac{1}{24}m(m+1)(m+2)(3m+8t+9). \end{aligned}$$

Similarly, we have

$$\begin{aligned} n_X &= \sum_{k=0}^{m}\sum_{i_1=0}^{i_1}\sum_{i_2=k}^{m-i_1}\sum_{i_3=k}^{k} i_1 + \sum_{k=0}^{m}\sum_{i_1=0}^{m-k}\sum_{i_2=k}^{k}\sum_{i_3=k+1}^{i_2+t} i_1 \\ &= \frac{1}{24}m(m+1)(m+2)(m+4t+3). \end{aligned}$$

and

$$\begin{aligned} n_Y &= \sum_{k=0}^{m}\sum_{i_1=0}^{m-k}\sum_{i_2=k}^{m-i_1}\sum_{i_3=k}^{k} i_2 + \sum_{k=0}^{m}\sum_{i_1=0}^{m-k}\sum_{i_2=k}^{k}\sum_{i_3=k+1}^{i_2+t} i_2 \\ &= \frac{1}{12}m(m+1)(m+2)(m+2t+3). \end{aligned}$$

and finally

$$\begin{aligned} n_Z &= \sum_{k=0}^{m}\sum_{i_1=0}^{m-k}\sum_{i_2=k}^{m-i_1}\sum_{i_3=k}^{k} i_3 + \sum_{k=0}^{m}\sum_{i_1=0}^{m-k}\sum_{i_2=k}^{k}\sum_{i_3=k+1}^{i_2+t} i_3 \\ &= \frac{1}{24}(m+1)(m+2)(m^2+3m+4tm+6t^2+6t). \end{aligned}$$

On the other hand, the dimension of $\mathcal{L}$ is

$$\begin{aligned} \omega &= \sum_{k=0}^{m}\sum_{i_1=0}^{m-k}\sum_{i_2=k}^{m-i_1}\sum_{i_3=k}^{k} 1 + \sum_{k=0}^{m}\sum_{i_1=0}^{m-k}\sum_{i_2=k}^{k}\sum_{i_3=k+1}^{i_2+t} 1 \\ &= \frac{1}{6}(m+1)(m+2)(m+3t+3). \end{aligned}$$

In the following, we set $t = \tau m$. For sufficiently large m, the exponents n_e, n_X, n_Y, n_Z as well as the dimension ω reduce to

$$\begin{aligned}
n_e &= \tfrac{1}{24}(8\tau + 3)m^4 + o(m^4),\\
n_X &= \tfrac{1}{24}(4\tau + 1)m^4 + o(m^4),\\
n_Y &= \tfrac{1}{24}(4\tau + 2\tau + 1)m^4 + o(m^4),\\
n_Z &= \tfrac{1}{24}(6\tau^2 + 4\tau + 1)m^4 + o(m^4),\\
\omega &= \tfrac{1}{24}(12\tau + 4)m^3 + o(m^3).
\end{aligned} \tag{6}$$

Applying the LLL algorithm, we get a new basis $\{v_1, \ldots, v_\omega\}$. Using Theorem 1, such a bais is LLL-reduced and satisfies

$$\|v_1\| \leq \|v_2\| \leq \|v_3\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(\mathcal{L})^{\frac{1}{\omega-2}}.$$

According to Theorem 2, we need $\|v_3\| \leq \frac{(Me)^m}{\sqrt{\omega}}$. This is satisfied if

$$2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(\mathcal{L})^{\frac{1}{\omega-2}} < \frac{(Me)^m}{\sqrt{\omega}}.$$

From this, we deduce

$$\det(\mathcal{L}) < \frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-2)}}\sqrt{\omega}\right)^{\omega-2}}(Me)^{m(\omega-2)} < (Me)^{m\omega}.$$

Using (5), we get the inequality

$$(Me)^{n_e} X^{n_X} Y^{n_Y} Z^{n_Z} < (Me)^{m\omega}.$$

Using the values (6) as well as the values (3) and taking logarithms, neglecting low order terms and after simplifying by m^4, we get

$$\begin{aligned}
&2(\alpha+\beta)(3+8\tau) + 2\gamma(1+4\tau) + 2(\alpha+\beta+\delta-1)(2+4\tau) + 1 + 4\tau + 6\tau^2\\
&< 2(4+12\tau)(\alpha+\beta).
\end{aligned}$$

Transforming this inequality, we get

$$6\tau^2 + (8\delta + 8\gamma - 4)\tau + 2\alpha + 2\beta + 4\delta + 2\gamma - 3 < 0.$$

The left hand side is minimized with the value $\tau_0 = \frac{1}{3}(1 - 2\delta - 2\gamma)$. Plugging τ_0 in the former inequality, we get

$$\delta < \frac{1}{4}\left(5 - 4\gamma - \sqrt{12\alpha + 12\beta - 12\gamma + 3}\right).$$

From the three vectors $v_1(xX, yY, zZ)$, $v_2(xX, yY, zZ)$, and $v_3(xX, yY, zZ)$, we obtain three polynomials $h_1(x, y, z)$, $h_2(x, y, z)$, $h_3(x, y, z)$ with the common root

(x_0, y_0, z_0). Next, we use Assumption 1. Let $g_1(y, z)$ be the resultant polynomial of $h_1(x, y, z)$ and $h_2(x, y, z)$ with respect of x. Similarly, let $g_2(y, z)$ be the resultant polynomial of $h_1(x, y, z)$ and $h_3(x, y, z)$ with respect of x. Then, computing the resultant of $g_1(y, z)$ and $g_2(y, z)$ with respect to y, we find a polynomial $g(z)$ with the root z_0. Using $z_0 = p+q-1$ and $pq = N$, the factorization of N follows. This terminates the proof. □

In Table 2, we present some values of δ and $\delta+\beta$. Recall that $M = N^\beta$, $d_1 < N^\delta$, $d_0 < N^\gamma$ and $d = Md + d_0 < 2N^{\delta+\beta}$. Notice that in all the presented cases, we have $\delta + \beta > 0.292$. This shows that Wiener's attack [14] as well as Boneh and Durfee's method [4] will not give the factorization of the RSA modulus in these situations.

$\alpha = \log_N(e)$	$\beta = \log_N(M)$	$\gamma = \log_N(d_0)$	$\delta = \log_N(d_1)$	$\beta + \delta$
1	0.5	0.1	0.03	0.53
1	0.4	0.1	0.07	0.47
1	0.3	0.2	0.04	0.34
1	0.3	0.1	0.10	0.40
1	0.25	0.25	0.03	0.28
0.75	0.5	0.3	0.003	0.50
0.75	0.4	0.2	0.10	0.50
0.75	0.3	0.2	0.14	0.44
0.75	0.25	0.25	0.13	0.38

Table 2. Values of δ and $\beta + \delta$ in terms of α, β and γ.

To test the validity of Assumption 1, we performed several experiments with various parameters α, β and γ. We implemented the new attack on an Intel Core 2 Duo running Maple 17. All the experiments gave the factorization of the RSA modulus N.

Using the trivariate polynomial $f(x, y, z) = ex - Ny + yz - 1$, we constructed a set of polynomials with the same root (x_0, y_0, z_0) and at most ω monomials. Using this set of polynomials, we constructed a basis of a lattice $\mathcal{L}$ and applied the LLL ALgorithm to find a set of trivariate polynomials $h_i(x, y, z)$ for $1 \leq i \leq \omega$. The shortest three polynomials $h_1(x, y, z)$, $h_2(x, y, z)$, $h_3(x, y, z)$ are such that they satisfy Theorem 1. Then, we forced them to verify Howgrave-Graham's Theorem 2, that is we set

$$\|h_1(x, y, z)\| \leq \|h_2(x, y, z)\| \leq \|h_3(x, y, z)\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(\mathcal{L})^{\frac{1}{\omega-2}}.$$

This implies that the small root (x_0, y_0, z_0) of $h_1(x, y, z)$, $h_2(x, y, z)$ and $h_3(x, y, z)$ hold over the integers. Then, we take the resultants with respect to x, and then another resultant with respect to y, which gives an univariate polynomial leading to the solution $z_0 = p + q - 1$. Using the RSA modulus $N = pq$, it is easy to find p and q and then factor N. We note that all the experiments were successful and that Asssumption 1 was verified in all cases. We note also, that in the most of the cases, the size of the private exponent d was such that $d > N^{0.292}$ which implies that the classical method of Boneh and Durfee will not give a solution in this situation.

4 Conclusion

In this paper, we consider an RSA instance $N = pq$ with a private exponent d of the form $d = Md_1 + d_0$. Unlike the partial key exposure attacks where M and d_0 are known, we suppose that M is the only known parameter. We show that when d_1 and d_0 are suitably small, then one can find the factorization of N. The method is based on transforming the key equation $ed - k\phi(N) = 1$ into the modular equation $f(x, y, z) = ex - Ny + yz - 1 \equiv 0 \pmod{Me}$ where $(x_0, y_0, z_0) = (d_0, k, p + q - 1)$ is a small solution. Using Coppersmith's technique and the LLL algorithm, we can easily find $z_0 = p + q - 1$, which leads to the factorization of N. We note that the classical attacks on RSA gives the factorization of N when $d < N^{0.292}$ as it is the case with the attack of Boneh and Durfee. Our method enables us to find the private exponent d even when $d > N^{0.292}$ depending on the possibility that d has the form $d = Md_1 + d_0$ for a suitable known integer M and suitable unknown parameters d_1 and d_0. The encryption and decryption in RSA require taking heavy exponential multiplications modulus the large integer N and many ways have been considered using special private exponent d. Once again, our results show that one should be more careful when using RSA with special private exponents.

References

1. ANSI Standard X9.31-1998, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA).
2. Blömer, J., May, A.: New partial key exposure attacks on RSA, Proceedings of CRYPTO 2003, LNCS 2729 (2003), pp. 27–43. Springer Verlag (2003)
3. Boneh, D.: Twenty years of attacks on the RSA cryptosystem, Notices Amer. Math. Soc. 46 (2), 203–213, (1999)
4. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$, Advances in Cryptology Eurocrypt'99, Lecture Notes in Computer Science Vol. 1592, Springer-Verlag, pp. 1–11 (1999)
5. Boneh, D., Durfee, G., Frankel, Y.: An attack on RSA given a small fraction of the private key bits. In: Ohta, K., Pei, D. (eds.) Advances in Cryptology Asiacrypt'98. Lecture Notes in Computer Science, vol. 1514, pp. 25–34. Springer-Verlag (1998)
6. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), pp. 233–260 (1997)
7. Ernst, M., Jochemsz, E., May, A., de Weger, B.: Partial key exposure attacks on RSA up to full size exponents. In: Cramer, R. (ed.) Advances in Cryptology Eurocrypt 2005. Lecture Notes in Computer Science, vol. 3494, pp. 371–386. Springer-Verlag (2005)

8. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited, In Cryptography and Coding, LNCS 1355, pp. 131–142, Springer-Verlag (1997)
9. Jochemsz, E., May, A.: A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants, in: ASIACRYPT 2006, LNCS, vol. 4284, 2006, pp. 267–282, Springer-Verlag.
10. Lenstra, A.K., Lenstra, H.W., Lovász,L.: Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, pp. 513–534, 1982.
11. May, A.: New RSA Vulnerabilities Using Lattice Reduction Methods. PhD thesis, University of Paderborn (2003). Available at `http://wwwcs.upb.de/cs/ag-bloemer/personen/alex/publikationen/`
12. Nitaj, A.: Another generalization of Wiener's attack on RSA, In: Vaudenay, S. (ed.) Africacrypt 2008. LNCS, vol. 5023, pp. 174–190. Springer, Heidelberg (2008)
13. Rivest, R., Shamir, A., Adleman, L.: A Method for Obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol. 21 (2), pp. 120–126 (1978)
14. Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, 553–558 (1990)