An Attack on RSA Using LSBs of Multiples of the Prime Factors

Abderrahmane Nitaj

Laboratoire de Mathématiques Nicolas Oresme
Université de Caen, Basse Normandie, France
abderrahmane.nitaj@unicaen.fr

Abstract. Let $N = pq$ be an RSA modulus with a public exponent e and a private exponent d. Wiener's famous attack on RSA with $d < N^{0.25}$ and its extension by Boneh and Durfee to $d < N^{0.292}$ show that using a small d makes RSA completely insecure. However, for larger d, it is known that RSA can be broken in polynomial time under special conditions. For example, various partial key exposure attacks on RSA and some attacks using additional information encoded in the public exponent e are efficient to factor the RSA modulus. These attacks were later improved and extended in various ways. In this paper, we present a new attack on RSA with a public exponent e satisfying an equation $ed-k(N+1-ap-bq) = 1$ where $\frac{a}{b}$ is an unknown approximation of $\frac{q}{p}$. We show that RSA is insecure when certain amount of the Least Significant Bits (LSBs) of ap and bq are known. Further, we show that the existence of good approximations $\frac{a}{b}$ of $\frac{q}{p}$ with small a and b substantially reduces the requirement of LSBs of ap and bq.

Keywords: RSA, Cryptanalysis, Factorization, Lattice, LLL algorithm, Coppersmith's method

1 Introduction

The RSA cryptosystem was invented by Rivest, Shamir and Adleman [16] in 1977 and is today's most important public-key cryptosystem. The standard notations in RSA are as follows:

- p and q are two large primes of the same bit size.
- $N = pq$ is the RSA modulus and $\phi(N) = (p-1)(q-1)$ is Euler's totient function.
- e and d are respectively the public and the private exponents and satisfy $ed - k\phi(N) = 1$ for some positive integer k.

There have been a large number of attacks on RSA. Some attacks, called small private key attacks can break RSA in polynomial time when the private key is small. For example, Wiener [17] showed that if the private key satisfies $d < \frac{1}{3}N^{\frac{1}{4}}$, then N can be factored and Boneh and Durfee [4] showed that RSA is insecure if

$d < N^{0.292}$. Some attacks, called partial key exposure attacks exploit the knowledge of a portion of the private exponent or of one of the prime factors. Partial key exposure attacks are mainly motivated by using side-channel attacks, such as fault attacks, power analysis and timing attacks ([10], [11]). Using a side-channel, an attacker can expose a part of one of the modulus prime factors p or q or of the private key d. In 1998, Boneh, Durfee and Frankel [5] presented several partial key exposure attacks on RSA with a public key $e < N^{1/2}$ where the attacker requires knowledge of most significant bits (MSBs) or least significant bits (LSBs) of the private exponent d. In [2], Ernest et al. [7] proposed several partial key exposure attacks that work for $e > N^{1/2}$. Notice that Wiener's attack[17] and the attack of Boneh and Durfee[4] can be seen as partial key exposure attacks because the most significant bits of the private exponent are known and are equal to zero. Sometimes, it is possible to factor the RSA modulus even if the private key is large and no bits are exposed. Such attacks exploit the knowledge of special conditions verified by the modulus prime factors or by the exponents. In 2004, Blömer and May [3] showed that RSA can be broken if the public exponent e satisfies an equation $ex = y + k\phi(N)$ with $x < \frac{1}{3}N^{\frac{1}{4}}$ and $|y| < N^{-\frac{3}{4}}ex$. At Africacrypt 2009, Nitaj [15] presented an attack when the exponent e satisfies an equation $eX - (N - (ap + bq))Y = Z$ with the constraints that $\frac{a}{b}$ is an unknown convergent of the continued fraction expansion of $\frac{q}{p}$, $1 \leq Y \leq X < \frac{1}{2}\frac{N^{\frac{1}{4}}}{\sqrt{a}}$, $\gcd(X, Y) = 1$, and Z depends on the size of $|ap - bq|$. Nitaj's attack combines techniques from the theory of continued fractions, Coppersmith's method [6] for finding small roots of bivariate polynomial equations and the Elliptic Curve Method [12] for integer factorization.

In this paper we revisit Nitaj's attack by studying the generalized RSA equation $ed - k(N + 1 - ap - bq) = 1$ with different constraints using Coppersmith's method [6] only. We consider the situation when an amount of LSBs of ap and bq are exposed where $\frac{a}{b}$ is an unknown approximation of $\frac{q}{p}$, that is when $a = \left[\frac{bq}{p}\right]$. More precisely, assume that $ap = 2^{m_0}p_1 + p_0$ and $bq = 2^{m_0}q_1 + q_0$ where m_0, p_0 and q_0 are known to the attacker. We show that one can factor the RSA modulus if the public key e satisfies an equation $ed_1 - k_1(N + 1 - ap - bq) = 1$ where $e = N^{\gamma}$, $d_1 < N^{\delta}$, $2^{m_0} = N^{\beta}$ and $a < b < N^{\alpha}$ satisfy

$$\delta \leq \begin{cases} \delta_1 & \text{if} \quad \gamma \geq \frac{1}{2}(1 + 2\alpha - 2\beta), \\ \delta_2 & \text{if} \quad \gamma < \frac{1}{2}(1 + 2\alpha - 2\beta). \end{cases}$$

with

$$\delta_1 = \frac{7}{6} + \frac{1}{3}(\alpha - \beta) - \frac{1}{3}\sqrt{4(\alpha - \beta)^2 + 4(3\gamma + 1)(\alpha - \beta) + 6\gamma + 1},$$
$$\delta_2 = \frac{1}{4}(3 - 2(\alpha - \beta) - 2\gamma).$$

We notice the following facts

- When $a = b = 1$, the equation becomes $ed_1 - k_1(N + 1 - p - q) = 1$ as in standard RSA.

- When $\gamma = 1$ and $\alpha = \beta$, the RSA instance is insecure if $d < \frac{7}{6} - \frac{\sqrt{7}}{3} \approx 0.284$. This is a well known boundary in the cryptanalysis of RSA (see e.g. [4]).
- When $\gamma = 1$ and $\beta = 0$, that is no LSBs of ap nor of bq are known, the RSA instance is insecure if $\delta < \frac{7}{6} + \frac{1}{3}\alpha - \frac{1}{3}\sqrt{\alpha^2 + 16\alpha + 7}$. This considerably improve the bound $\delta < \frac{1}{4}(1 - 2\alpha)$ of [15].
- The ANSI X9.31 standard [1] requires that the prime factors p and q shall not be near the ratio of two small integers. Our new attack shows that this requirement is necessary and can be easily checked once one has generated two primes simply by computing the convergents of the continued fraction expansion of $\frac{q}{p}$.

The rest of the paper is organized as follows. In Section 2 we review some basic results from lattice theory and their application to solve modular equations as well as two useful lemmas. In Section 3 we describe the new attack on RSA. In Section 4, we present various numerical experiments. Finally, we conclude in Section 5.

2 Preliminaries

2.1 Lattices

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

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

The set $\langle b_1 \ldots, b_\omega \rangle$ is called a lattice basis for $\mathcal{L}$. The lattice dimension is $\dim(\mathcal{L}) = \omega$. We say that the lattice is full rank if $\omega = n$. If the lattice is full rank, then the determinant of $\mathcal{L}$ is equal to the absolute value of the determinant of the matrix whose rows are the basis vectors $b_1, \cdots, b_\omega$. In 1982, Lenstra, Lenstra and Lovász [13] invented the so-called LLL algorithm to reduce a basis and to find a short lattice vector in time polynomial in the bit-length of the entries of the basis matrix and in the dimension of the lattice. The following lemma, gives bounds on LLL-reduced basis vectors.

Theorem 1 (Lenstra, Lenstra, Lovász). *Let $\mathcal{L}$ be a lattice of dimension ω. In polynomial time, the LLL- algorithm outputs two reduced basis vectors v_1 and v_2 that satisfy*

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

Using the LLL algorithm, Coppersmith [6] proposed a method to efficiently compute small roots of bivariate polynomials over the integers or univariate modular polynomials. Howgrave-Graham [8] gave a simple reformulation of Coppersmith's method in terms of the norm of the polynomial $f(x,y) = \sum a_{ij}x^iy^j$ which is defined by

$$\|f(x,y)\| = \sqrt{\sum a_{ij}^2}.$$

Theorem 2 (Howgrave-Graham). *Let $f(x,y) \in \mathbb{Z}[x,y]$ be a polynomial which is a sum of at most ω monomials. Suppose that $f(x_0,y_0) \equiv 0 \pmod{e^m}$ where $|x_0| < X$ and $|y_0| < Y$ and $\|f(xX,yY)\| < \frac{e^m}{\sqrt{\omega}}$. Then $f(x_0,y_0) = 0$ holds over the integers.*

2.2 Useful Lemmas

Let $N = pq$ be an RSA modulus. The following lemma is useful to find a value of $ap - bq$ using a known value of $ap + bq$.

Lemma 1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$ and S be a positive integer. Suppose that $ap + bq = S$ where $\frac{a}{b}$ is an unknown approximation of $\frac{q}{p}$. Then*

$$ab = \left\lfloor \frac{S^2}{4N} \right\rfloor \quad \textit{and} \quad |ap - bq| = \sqrt{S^2 - 4\left\lfloor \frac{S^2}{4N} \right\rfloor N}.$$

Proof. Observe that multiplying $q < p < 2q$ by p gives $N < p^2 < 2N$ and consequently $\sqrt{N} < p < \sqrt{2}\sqrt{N}$. Suppose that $\frac{a}{b}$ is an approximation of $\frac{q}{p}$, that is $a = \left[\frac{bq}{p}\right]$. Hence $\left|a - \frac{bq}{p}\right| \leq \frac{1}{2}$, which gives

$$|ap - bq| \leq \frac{p}{2} \leq \frac{\sqrt{2}\sqrt{N}}{2} < 2\sqrt{N}.$$

Next, suppose that $ap + bq = S$. We have $S^2 = (ap + bq)^2 = (ap - bq)^2 + 4abN$. Since $|ap - bq| < 2\sqrt{N}$, then the quotient and the remainder in the Euclidean division of S^2 by $4N$ are respectively ab and $(ap - bq)^2$. Hence

$$ab = \left\lfloor \frac{S^2}{4N} \right\rfloor \quad \text{and} \quad |ap - bq| = \sqrt{S^2 - 4abN},$$

which terminates the proof. □

The following lemma shows how to factor $N = pq$ using a known value of $ap+bq$.

Lemma 2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$ and S be a positive integer. Suppose that $ap + bq = S$ where $\frac{a}{b}$ is an unknown approximation of $\frac{q}{p}$. Then N can be factored.*

Proof. Suppose that $\frac{a}{b}$ is an approximation of $\frac{q}{p}$ and that $ap + bq = S$. By Lemma 1, we get $ab = \left\lfloor \frac{S^2}{4N} \right\rfloor$ and $|ap - bq| = D$ where

$$D = \sqrt{S^2 - 4abN}.$$

Hence $ap - bq = \pm D$. Combining with $ap + bq = S$, we get $2ap = S \pm D$. Since $a < q$, then $\gcd(N, S \pm D) = \gcd(N, 2ap) = p$. This gives the factorization of N. □

3 The New Attack

Let e, d_1, k_1 be positive integers such that $ed_1 - k_1(N + 1 - ap - bq) = 1$. In this section, we consider the following parameters.

- $2^{m_0} = N^{\beta}$ where m_0 is a known integer.
- $a < b < N^{\alpha}$ with $\alpha < \frac{1}{2}$ where $\frac{a}{b}$ is an unknown approximation of $\frac{q}{p}$.
- $ap = 2^{m_0} p_1 + p_0$ where p_0 is a known integer.
- $bq = 2^{m_0} q_1 + q_0$ where q_0 is a known integer.
- $e = N^{\gamma}$.
- $d_1 = N^{\delta}$.

The aim in this section is to prove the following result.

Theorem 3. *Suppose that $ap = 2^{m_0} p_1 + p_0$ and $bq = 2^{m_0} q_1 + q_0$ where m_0, p_0 and q_0 are known with $2^{m_0} = N^{\beta}$ and $\frac{a}{b}$ is an unknown approximation of $\frac{q}{p}$ satisfying $a, b < N^{\alpha}$. Let $e = N^{\gamma}$, $d_1 = N^{\delta}$ and k_1 be positive integers satisfying an equation $ed_1 - k_1(N + 1 - ap - bq) = 1$. Then one can factor N in polynomial time when*

$$\delta \leq \begin{cases} \delta_1 & \text{if} \quad \gamma \geq \frac{1}{2}(1 + 2\alpha - 2\beta), \\ \delta_2 & \text{if} \quad \gamma \leq \frac{1}{2}(1 + 2\alpha - 2\beta), \end{cases}$$

where

$$\delta_1 = \frac{7}{6} + \frac{1}{3}(\alpha - \beta) - \frac{1}{3}\sqrt{4(\alpha - \beta)^2 + 4(3\gamma + 1)(\alpha - \beta) + 6\gamma + 1},$$
$$\delta_2 = \frac{1}{4}(3 - 2(\alpha - \beta) - 2\gamma).$$

Proof. Suppose that $ap = 2^{m_0} p_1 + p_0$ and $bq = 2^{m_0} q_1 + q_0$ with known m_0, p_0 and q_0. Then $ap + bq = 2^{m_0}(p_1 + q_1) + p_0 + q_0$. Starting with the variant RSA equation $ed_1 - k_1(N + 1 - ap - bq) = 1$, we get

$$ed_1 - k_1 \left(N + 1 - p_0 - q_0 - 2^{m_0}(p_1 + q_1)\right) = 1.$$

Reducing modulo e, we get

$$-2^{m_0} k_1(p_1 + q_1) + (N + 1 - p_0 - q_0)k_1 + 1 \equiv 0 \pmod{e}.$$

Observe that $\gcd(2^{m_0}, e) = 1$. Then multiplying by $-2^{-m_0} \pmod{e}$, we get

$$k_1(p_1 + q_1) + a_1 k_1 + a_2 \equiv 0 \pmod{e},$$

where

$$\begin{aligned} &a_1 \equiv -(N + 1 - p_0 - q_0)2^{-m_0} \pmod{e}, \\ &a_2 \equiv -2^{-m_0} \pmod{e}. \end{aligned}$$

Consider the polynomial

$$f(x, y) = xy + a_1 x + a_2.$$

Then $(x, y) = (k_1, p_1 + q_1)$ is a modular root of the equation $f(x, y) \equiv 0 \pmod{e}$. Assuming that $\alpha \ll \frac{1}{2}$, we get

$$k_1 = \frac{ed_1 - 1}{N + 1 - ap - bq} \sim N^{\gamma+\delta-1}.$$

On the other hand, we have

$$p_1 + q_1 < \frac{ap + bq}{2^{m_0}} < N^{\frac{1}{2}+\alpha-\beta}.$$

Define the bounds X and Y as

$$X = N^{\gamma+\delta-1}, \quad Y = N^{\frac{1}{2}+\alpha-\beta}.$$

To find the small modular roots of the equation $f(x, y) \equiv 0 \pmod{e}$, we apply the extended strategy of Jochemsz and May [9]. Let m and t be positive integers to be specified later. For $0 \leq k \leq m$, define the set

$$\begin{aligned} M_k = \bigcup_{0\leq j\leq t} \{x^{i_1} y^{i_2+j} \;\Big|\; & \; x^{i_1} y^{i_2} \quad \text{monomial of} \quad f^m(x, y) \\ & \text{and} \quad \frac{x^{i_1} y^{i_2}}{(xy)^k} \quad \text{monomial of} \quad f^{m-k}\}. \end{aligned}$$

Observe that $f^m(x, y)$ satisfies

$$\begin{aligned} f^m(x, y) &= \sum_{i_1=0}^{m} \binom{m}{i_1} x^{i_1} (y + a_1)^{i_1} a_2^{m-i_1} \\ &= \sum_{i_1=0}^{m} \binom{m}{i_1} x^{i_1} \left(\sum_{i_2=0}^{i_1} \binom{i_1}{i_2} y^{i_2} a_1^{i_1-i_2} a_2^{m-i_1} \right) \\ &= \sum_{i_1=0}^{m} \sum_{i_2=0}^{i_1} \binom{m}{i_1} \binom{i_1}{i_2} x^{i_1} y^{i_2} a_1^{i_1-i_2} a_2^{m-i_1}. \end{aligned}$$

Hence, $x^{i_1}y^{i_2}$ is a monomial of $f^m(x,y)$ if

$$i_1 = 0, \ldots, m, \quad i_2 = 0, \ldots, i_1.$$

Consequently, for $0 \le k \le m$, when $x^{i_1}y^{i_2}$ is a monomial of $f^m(x,y)$, then $\frac{x^{i_1}y^{i_2}}{(xy)^k}$ is a monomial of $f^{m-k}(x,y)$ if

$$i_1 = k, \ldots, m, \quad i_2 = k, \ldots, i_1.$$

Hence, for $0 \le k \le m$, we obtain

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

Similarly,

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

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

$$g_{k,i_1,i_2}(x,y) = \frac{x^{i_1}y^{i_2}}{(xy)^k} f(x,y)^k e^{m-k} \quad \text{with} \quad x^{i_1}y^{i_2} \in M_k \Big\backslash M_{k+1}.$$

For $0 \le k \le m$, these polynomials reduce to the following sets

$$\begin{cases} k = 0, \ldots, m, \\ i_1 = k, \ldots, m, \\ i_2 = k, \end{cases} \quad \text{or} \quad \begin{cases} k = 0, \ldots, m, \\ i_1 = k, \\ i_2 = k+1, \ldots, i_1 + t. \end{cases}$$

This gives rise to the polynomials

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

Let $\mathcal{L}$ denote the lattice spanned by the coefficient vectors of the polynomials $G_{k,i_1}(xX, yY)$ and $H_{k,i_2}(xX, yY)$. The ordering of two monomials $x^{i_1}y^{i_2}$, $x^{i_1'}y^{i_2'}$ is as in the following rule: if $i_1 < i_1'$, then $x^{i_1}y^{i_2} < x^{i_1'}y^{i_2}$ and if $i_1 = i_1'$ and $i_2 < i_2'$, then $x^{i_1}y^{i_2} < x^{i_1'}y^{i_2'}$. Notice that the matrix is left triangular. For $m = 3$ and $t = 1$, the coefficient matrix for $\mathcal{L}$ is presented in Table 1. The non-zero elements are marked with an '⊛'.

From the triangular form of the matrix, the ⊛ marked values do not contribute in the calculation of the determinant. Hence, the determinant of $\mathcal{L}$ is

$$\det(\mathcal{L}) = e^{n_e} X^{n_X} Y^{n_Y}. \tag{1}$$

From the construction of the polynomials $G_{k,i_1}(x,y)$ and $H_{k,i_2}(x,y)$, we get

$$n_e = \sum_{k=0}^{m} \sum_{i_1=k}^{m} (m-k) + \sum_{k=0}^{m} \sum_{i_2=k+1}^{k+t} (m-k) = \frac{1}{6} m(m+1)(2m+3t+4).$$

	1	x	x^2	x^3	y	xy	x^2y	x^3y	xy^2	x^2y^2	x^3y^2	x^2y^3	x^3y^3	x^3y^4
$G_{0,0}$	e^3	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,1}$	0	Xe^3	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,2}$	0	0	X^2e^3	0	0	0	0	0	0	0	0	0	0	0
$G_{0,3}$	0	0	0	X^3e^3	0	0	0	0	0	0	0	0	0	0
$H_{0,1}$	0	0	0	0	Ye^3	0	0	0	0	0	0	0	0	0
$G_{1,1}$	$\circledast$	$\circledast$	0	0	0	XYe^2	0	0	0	0	0	0	0	0
$G_{1,2}$	0	$\circledast$	$\circledast$	0	0	0	X^2Ye^2	0	0	0	0	0	0	0
$G_{1,3}$	0	0	$\circledast$	$\circledast$	0	0	0	X^3Ye^2	0	0	0	0	0	0
$H_{1,2}$	0	0	0	0	$\circledast$	$\circledast$	0	0	XY^2e^2	0	0	0	0	0
$G_{2,2}$	$\circledast$	$\circledast$	$\circledast$	0	0	$\circledast$	$\circledast$	0	0	X^2Y^2	0	0	0	0
$G_{2,3}$	0	$\circledast$	$\circledast$	$\circledast$	0	0	$\circledast$	$\circledast$	0	0	X^3Y^2e	0	0	0
$H_{2,3}$	0	0	0	0	$\circledast$	$\circledast$	$\circledast$	0	$\circledast$	$\circledast$	0	X^2Y^3e	0	0
$G_{3,3}$	$\circledast$	$\circledast$	$\circledast$	$\circledast$	0	$\circledast$	$\circledast$	$\circledast$	0	$\circledast$	$\circledast$	0	X^3Y^3	0
$H_{3,4}$	0	0	0	0	$\circledast$	$\circledast$	$\circledast$	0	$\circledast$	$\circledast$	$\circledast$	$\circledast$	$\circledast$	X^3Y^4

Table 1. The coefficient matrix for the case $m = 3$, $t = 1$.

Similarly, we have

$$n_X = \sum_{k=0}^{m}\sum_{i_1=k}^{m} i_1 + \sum_{k=0}^{m}\sum_{i_2=k+1}^{k+t} k = \frac{1}{6}m(m+1)(2m+3t+4),$$

and

$$n_Y = \sum_{k=0}^{m}\sum_{i_1=k}^{m} k + \sum_{k=0}^{m}\sum_{i_2=k+1}^{k+t} i_2 = \frac{1}{6}(m+1)(m^2+3mt+3t^2+2m+3t).$$

Finally, we can calculate the dimension of $\mathcal{L}$ as

$$\omega = \sum_{k=0}^{m}\sum_{i_1=k}^{m} 1 + \sum_{k=0}^{m}\sum_{i_2=k+1}^{k+t} 1 = \frac{1}{2}(m+1)(m+2t+2).$$

For the following asymptotic analysis we let $t = \tau m$. For sufficiently large m, the exponents n_e, n_X, n_Y and the dimension ω reduce to

$$\begin{aligned} n_e &= \frac{1}{6}(3\tau+2)m^3 + o(m^3), \\ n_X &= \frac{1}{6}(3\tau+2)m^3 + o(m^3), \\ n_Y &= \frac{1}{6}(3\tau^2+3\tau+1)m^3 + o(m^3), \\ \omega &= \frac{1}{2}(2\tau+1)m^2 + o(m^2). \end{aligned}$$

To apply Theorem 2 to the shortest vector in the LLL-reduced basis of $\mathcal{L}$, we have to set

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

This transforms to

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

Using (1), we get

$$e^{n_e} X^{n_X} Y^{n_Y} < e^{m\omega}.$$

Plugging n_e, n_X, n_Y, ω as well as the values $e = N^{\gamma}$, $X = N^{\gamma+\delta-1}$, and $Y = N^{\frac{1}{2}+\alpha-\beta}$, we get

$$\frac{1}{6}(3\tau+2)m^3\gamma + \frac{1}{6}(3\tau+2)m^3\left(\gamma+\delta-1\right) + \frac{1}{6}(3\tau^2+3\tau+1)m^3(\frac{1}{2}+\alpha-\beta) < \frac{1}{2}(2\tau+1)m^3\gamma,$$

which transforms to

$$3(2\alpha-2\beta+1)\tau^2 + 3(2\alpha+2\delta-2\beta-1)\tau + (2\gamma+2\alpha+4\delta-2\beta-3) < 0. \quad (2)$$

Next, we consider the cases $\tau \neq 0$ and $\tau = 0$ separately. First, we consider the case $\tau > 0$. The optimal value for τ in the left side of (2) is

$$\tau = \frac{1+2\beta-2\alpha-2\delta}{2(1+2\alpha-2\beta)}. \quad (3)$$

Observe that for $\alpha < \frac{1}{2}$ and $\beta < \frac{1}{2}$, we have $1+2\alpha-2\beta > 0$. To ensure $\tau > 0$, δ should satisfy $\delta < \delta_0$ where

$$\delta_0 = \frac{1}{2}\left(1-2(\alpha-\beta)\right). \quad (4)$$

Replacing τ by the optimal value (3) in the inequation (2), we get

$$-12\delta^2 + 4(7+2\alpha-2\beta)\delta + 4(\alpha-\beta)^2 + 4(4\gamma-1)(\alpha-\beta) + 8\gamma - 15 < 0,$$

which will be true if $\delta < \delta_1$ where

$$\delta_1 = \frac{1}{3}(\alpha-\beta) + \frac{7}{6} - \frac{1}{3}\sqrt{4(\alpha-\beta)^2 + 4(3\gamma+1)(\alpha-\beta) + 6\gamma + 1}. \quad (5)$$

Since δ has to satisfy both $\delta < \delta_0$ and $\delta < \delta_1$ according to (4) and (5), let us find the minimum $\min(\delta_0, \delta_1)$. A straightforward calculation shows that

$$\min(\delta_0,\delta_1) = \begin{cases} \delta_0 & \text{if} \quad \gamma \leq \frac{1}{2}(1+2\alpha-2\beta), \\ \delta_1 & \text{if} \quad \gamma \geq \frac{1}{2}(1+2\alpha-2\beta). \end{cases}$$

Now, consider the case $\tau = 0$, that is $t = 0$. Then the inequation (2) becomes

$$2\gamma + 2\alpha + 4\delta - 2\beta - 3 < 0,$$

which leads to $\delta < \delta_2$ where

$$\delta_2 = \frac{1}{4}(2\beta + 3 - 2\gamma - 2\alpha). \tag{6}$$

To obtain an optimal value for δ, we compare δ_2 as in (6) to $\min(\delta_0, \delta_1)$, obtained respectively with $\tau > 0$ and $\tau = 0$. First suppose that $\gamma \leq \frac{1}{2}(1 + 2\alpha - 2\beta)$. Then

$$\min(\delta_0, \delta_1) - \delta_2 = \delta_0 - \delta_2 = \frac{1}{2}\left(g - \frac{1}{2}(1 + 2\alpha - 2\beta)\right) \leq 0.$$

Hence $\min(\delta_0, \delta_1) \leq \delta_2$. Next suppose that $\gamma \geq \frac{1}{2}(1 + 2(\alpha - \beta))$. Then

$$\begin{aligned}\min(\delta_0, \delta_1) - \delta_2 &= \delta_1 - \delta_2 \\ &= \frac{5}{6}(\alpha - \beta) + \frac{1}{2}\gamma + \frac{5}{12} \\ &\quad - \frac{1}{3}\sqrt{4(\alpha - \beta)^2 + 4(3\gamma + 1)(\alpha - \beta) + 6\gamma + 1}.\end{aligned}$$

On the other hand, we have

$$\begin{aligned}&\left(\frac{5}{6}(\alpha - \beta) + \frac{1}{2}\gamma + \frac{5}{12}\right)^2 - \left(\frac{1}{3}\sqrt{4(\alpha - \beta)^2 + 4(3\gamma + 1)(\alpha - \beta) + 6\gamma + 1}\right)^2 \\ &= \frac{1}{16}(1 + 2(\alpha - \beta) - 2\gamma)^2,\end{aligned}$$

which implies that $\min(\delta_0, \delta_1) \geq \delta_2$.
Summarizing, the attack will succeed to find k_1, $p_1 + q_1$ and $d_1 = N^\delta$ when $\delta < \delta'$ with

$$\delta' = \begin{cases} \delta_1 & \text{if} \quad \gamma \geq \frac{1}{2}(1 + 2\alpha - 2\beta), \\ \delta_2 & \text{if} \quad \gamma \leq \frac{1}{2}(1 + 2\alpha - 2\beta), \end{cases}$$

where δ_1 and δ_2 are given by (5) and (6).
Next, using the known value of $p_1 + q_1$, we can precisely calculate the value $ap + bq = 2^{m_0}(p_1 + q_1) + p_0 + q_0 = S$. Then using Lemma 1 and Lemma 2, we can find p and q. Since every step in the method can be done in polynomial time, then N can be factored in polynomial time. This terminates the proof. □

For example, consider the standard instance with the following parameters

- $2^{m_0} = N^\beta$ with $\beta = 0$.
- $a \leq b \leq N^\alpha$ with $\alpha = 0$, that is $ap + bq = p + q$.
- $ap = 2^{m_0}p_1 + p_0 = p_1$, that is $p_0 = 0$.
- $bq = 2^{m_0}q_1 + q_0 = q_1$, that is $q_0 = 0$.
- $e = N^\gamma$ with $\gamma = 1$.
- $d_1 = N^\delta$.

Then $\gamma \geq \frac{1}{2}(1 + 2\alpha - 2\beta) > \frac{1}{2}$ and the instance is insecure if $\delta < \delta_1$, that is if $\delta < \frac{7}{6} - \frac{\sqrt{7}}{3} \approx 0.284$ which is the same boundary as in various cryptanalytic approaches to RSA (see e.g. [4]).
Now suppose that $\gamma = 1$ and that a, b are small. Then $\alpha \approx 0$ and the boundary (5) becomes

$$\delta_1 < \frac{7}{6} - \frac{1}{3}\beta - \frac{1}{3}\sqrt{4\beta^2 - 16\beta + 7},$$

where the right side increases from 0.284 to 1 when $\beta \in \left[0, \frac{1}{2}\right[$. This implies that the existence of good approximation $\frac{a}{b}$ of $\frac{q}{p}$ substantially reduces the requirement of LSBs of ap and bq for the new attack. This confirms the recommendation of the X9.31-1997 standard for public key cryptography [1] regarding the generation of primes, namely that $\frac{q}{p}$ shall not be near the ratio of two small integers.

4 Experimental Results

We have implemented the new attack for various parameters. The machine was with Windows 7 and Intel(R) Core(TM)2 Duo CPU, 2GHz and the algebra system was Maple 12 [14]. For each set of parameters, we solved the modular equation $f(x, y) \equiv 0 \pmod{e}$ using the method described in Section 3. We obtained two polynomials $f_1(x, y)$ and $f_2(x, y)$ with the expected root $(k_1, p_1 + q_1)$. We then solved the equation obtained using the resultant of $f_1(x, y)$ and $f_2(x, y)$ in one of the variables. For every instance, we could recover k_1 and $p_1 + q_1$ and hence factor N. The experimental results are shown in Table 2

N	γ	β	α	δ	lattice parameters	LLL-time (sec)
2048	0.999	0.219	0.008	0.340	$m = 2$, $t = 1$, dim=9	54
2048	0.999	0.230	0.018	0.340	$m = 3$, $t = 2$, dim=18	2818
2048	0.999	0.172	0.114	0.273	$m = 2$, $t = 1$, dim=9	22
2048	0.999	0.150	0.096	0.272	$m = 2$, $t = 1$, dim=9	20
2048	0.999	0.091	0.019	0.280	$m = 2$, $t = 1$, dim=9	16
1024	0.999	0.326	0.123	0.368	$m = 3$, $t = 2$, dim=18	429
1024	0.999	0.326	0.123	0.339	$m = 2$, $t = 1$, dim=9	7
1024	0.998	0.229	0.050	0.326	$m = 2$, $t = 1$, dim=9	7
1024	0.995	0.102	0.008	0.297	$m = 2$, $t = 1$, dim=9	4
1024	0.999	0.131	0.123	0.239	$m = 2$, $t = 1$, dim=9	4

Table 2. Experimental results.

In the rest of this section, we present a detailed numerical example. Consider an instance of a 200-bit RSA public key with the following parameters.

- $N = 2463200821438139415679553190953343235761287240746891883363309$.

- $e = 266625289801406462041749617541089513158406651283204161816153$. Hence $e = N^{\gamma}$ with $\gamma = 0.984$.
- $m_0 = 35$. Hence $2^{m_0} = N^{\beta}$ with $\beta = 0.174$.
- $a < b < N^{0.080}$. Hence $\alpha = 0.080$.
- $m = 4$, $t = 2$.

Now suppose we know $p_0 = 28297245379$ and $q_0 = 28341074839$ such that $ap = 2^{m_0} p_1 + p_0$ and $bq = 2^{m_0} q_1 + q_0$. The modular equation to solve is then $f(x, y) = xy + a_1 x + a_2 \equiv 0 \pmod{e}$, where

$$a_1 = 396478470953448665961811597015453367067409367629970817 13297,$$

$$a_2 = 230870662106105785001116936880561535466903107693317985538102.$$

Working with $m = 4$ and $t = 2$, we get a lattice with dimension $\omega = 25$. Using the parameters $\gamma = 0.984$, $\alpha = 0.080$, and $\beta = 0.174$, the method will succeed with the bounds X and Y satisfying

$$\begin{aligned} p_1 + q_1 &< X = N^{\gamma+\delta-1} \approx 2^{52}, \\ k_1 &< Y = N^{\frac{1}{2}+\alpha-\beta} \approx 2^{81}, \end{aligned}$$

if $\delta < 0.356$. Applying the LLL algorithm, we find two polynomials $f_1(x, y)$ and $f_2(x, y)$ sharing the same integer solution. Then solving the resultant equation in y, we get $x = 4535179907267444$ and solving the resultant equation in x, we get $y = 3609045068101717298446784$. Hence

$$\begin{aligned} p_1 + q_1 &= 4535179907267444, \\ k_1 &= 3609045068101717298446784. \end{aligned}$$

Next, define

$$S = 2^{m_0}(p_1 + q_1) + p_0 + q_0 = 124005844298295748786131327649328730.$$

Then S is a candidate for $ap + bq$, and using Lemma 1, we get

$$\begin{aligned} ab &= \left\lfloor \frac{S^2}{4N} \right\rfloor = 1560718201, \\ |ap - bq| &= D = \sqrt{S^2 - 4abN} = 108928763058542141383405605909 2. \end{aligned}$$

Using S for $ap + bq$ and D for $|ap - bq|$, we get $2ap = S - D$, and finally

$$p = \gcd(N, S - D) = 297359251380425791004550126 1169.$$

Hence $q = \frac{N}{p} = 828358562917839001533347328061$. This terminates the factorization of the modulus N. Using the equation $ed_1 = k_1(N + 1 - ap - bq) + 1$, we get $d_1 = 41897971798817657 \approx N^{0.275}$. We notice that, with the standard RSA equation $ed - k\phi(N) = 1$, we have $d \equiv e^{-1} \pmod{\phi(N)} \approx N^{0.994}$ which is out of reach of the attack of Boneh and Durfee as well as the attack of Blömer and May. Also, using $2ap = S - D$, we get $a = \frac{S-D}{2p} = 20851$. Similarly, using $2bq = S + D$, we get $b = \frac{S+D}{2q} = 74851$. We notice that $\gcd(a, b) = 1$ and $\frac{a}{b}$ is not among the convergents of $\frac{q}{p}$. This shows that Nitaj's attack as presented in [15] can not succeed to factor the RSA modulus in this example.

5 Conclusion

In this paper, we propose a new polynomial time attack on RSA with a public exponent satisfying an equation $ed_1 - k_1(N + 1 - ap - bq) = 1$ where $\frac{a}{b}$ is an unknown approximation of $\frac{q}{p}$ and where certain amount of the Least Significant Bits of ap and aq are known to the attacker. The attack is based on the method of Coppersmith for solving modular polynomial equations. This attack can be seen as an extension of the well known partial key attack on RSA when $a = b = 1$ and certain amount of the Least Significant Bits of one of the modulus prime factors is known.

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. Blömer, J., May, A.: A generalized Wiener attack on RSA. In Public Key Cryptography - PKC 2004, volume 2947 of Lecture Notes in Computer Science, pp. 1–13. Springer-Verlag (2004)
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 (2006)
10. Kocher, P.: Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems. Crypto 1996, LNCS 1109, pp. 104–113 (1996)
11. Kocher, P., Jaffe, J. and Jun, B.: Differential power analysis. Crypto 1999, LNCS 1666, pp. 388–397 (1999)
12. Lenstra, H.W.: Factoring integers with elliptic curves, Annals of Mathematics, vol. 126, 649–673 (1987)
13. Lenstra, A.K., Lenstra, H.W., Lovász, L. : Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, pp. 513–534 (1982)
14. Maple, http://www.maplesoft.com/products/maple/

15. Nitaj, A.: Cryptanalysis of RSA using the ratio of the primes. In proceeding of: Progress in Cryptology - Africacrypt 2009, Second International Conference on Cryptology in Africa, Gammarth, Tunisia, pp. 98–115 (2009)
16. 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)
17. M. Wiener: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, pp. 553–558 (1990)