New Attacks on the RSA Cryptosystem

Abderrahmane Nitaj, Muhammad Rezal Kamel Ariffin, Dieaa I Nassr, Hatem M Bahig

New Attacks on the RSA Cryptosystem

Abderrahmane Nitaj[1], Muhammad Rezal Kamel Ariffin[2,3], Dieaa I. Nassr[4],
and Hatem M. Bahig[4]

[1] Laboratoire de Mathématiques Nicolas Oresme
Université de Caen Basse Normandie, France
abderrahmane.nitaj@unicaen.fr
[2] Al-Kindi Cryptography Research Laboratory,
Institute for Mathematical Research,
[3] Department of Mathematics, Faculty of Science,
Universiti Putra Malaysia (UPM), Selangor, Malaysia
rezal@upm.edu.my
[4] Computer Science Division, Department of Mathematics,
Faculty of Science, Ain Shams University, Cairo, Egypt
hmbahig@sci.asu.edu.eg, diaa_rsa@yahoo.com

Abstract. This paper presents three new attacks on the RSA cryptosystem. The first two attacks work when k RSA public keys (N_i, e_i) are such that there exist k relations of the shape $e_i x - y_i \phi(N_i) = z_i$ or of the shape $e_i x_i - y\phi(N_i) = z_i$ where $N_i = p_i q_i$, $\phi(N_i) = (p_i - 1)(q_i - 1)$ and the parameters x, x_i, y, y_i, z_i are suitably small in terms of the prime factors of the moduli. We show that our attacks enable us to simultaneously factor the k RSA moduli N_i. The third attack works when the prime factors p and q of the modulus $N = pq$ share an amount of their least significant bits (LSBs) in the presence of two decryption exponents d_1 and d_2 sharing an amount of their most significant bits (MSBs). The three attacks improve the bounds of some former attacks that make RSA insecure.

Keywords: RSA, Cryptanalysis, Factorization, LLL algorithm, Simultaneous diophantine approximations, Coppersmith's method

1 Introduction

The RSA cryptosystem [14] is currently the most widely known and widely used public key cryptosystem. The main parameters in RSA are the RSA modulus N and the public exponent e. The modulus $N = pq$ is the product of two large primes of equal bit-size and e satisfies $\gcd(e, \phi(N)) = 1$ where $\phi(N) = (p-1)(q-1)$ is the Euler totient function. The integer d satisfying $ed \equiv 1 \pmod{\phi(N)}$ is the private exponent. The RSA cryptosystem is deployed in various application systems for encryption, signing and for providing privacy and ensuring authenticity of digital data. Therefore, most research is focused on reducing the encryption/decryption execution time or the signature verification/generation time. For example, to reduce the decryption time or the signature generation time, one may wish to use a small private exponent d. Unfortunately, based on the convergents of the continued fraction expansion of $\frac{e}{N}$, Wiener [19] showed that the RSA cryptosystem is insecure when $d < N^{1/4}$. Boneh and Durfee [3] proposed an extension of Wiener's attack that allows the RSA cryptosystem to be broken when $d < N^{0.292}$. Their Method is based on lattice basis reduction techniques. Similarly, Blömer and May [2] proposed an extension of Wiener's attack and showed that the RSA cryptosystem is insecure if there exist three integers x, y and z satisfying $ex - y\phi(N) = z$ with $x < \frac{1}{3}N^{1/4}$ and $|z| < exN^{-3/4}$. Their method combines lattice basis reduction techniques and the continued fraction algorithm. In general, the use of short secret exponent encounters serious security problem in various instances of RSA. A typical example is when a single user generates many instances of RSA (N, e_i) with the same modulus and small private exponents [8]. Another example is when a single user generates k instances of RSA (N_i, e_i), each with the same small private exponent d. Using k equations $e_i d - k_i\phi(N_i) = 1$, Hinek [6] showed that it is possible to factor the k modulus N_i if $d < N^\delta$ with $\delta = \frac{k}{2(k+1)} - \varepsilon$ where ε is a small constant depending on the size of $\max N_i$. Similarly, to improve the computational efficiency of server-aided signature generation (see [16]), one may use RSA with a modulus $N = pq$ such that the prime factors p and q share a large number of least significant bits (LSBs). The security of this variant of RSA has been analyzed under the partial key exposure attacks in [16], [17], [20], and [18]. In [18], Sun et al. showed that RSA is more vulnerable in the situation when p and q share a large number of LSBs than the standard scenario when the prime factors p and q differ in the first LSBs. When $e = N^\gamma$, they showed that RSA is vulnerable if $|p - q| = 2^m x$ with $2^m = N^\alpha$ and $d < N^\delta$ whenever $\delta < \frac{7}{6} - \frac{2}{3}\alpha - \frac{1}{3}\sqrt{(1-4\alpha)(1-4\alpha+6\gamma)}$. For example, if $\gamma = 1$, and $\alpha = 0.2$, then $\delta < 0.662$, that is, RSA is insecure if the private exponent is such that $d < N^{0.662}$. In [8], Howgrave-Graham and Seifert extended Wiener's attack in the presence of many decryption exponents for a single RSA modulus. They showed that RSA is insecure if one knows two public exponents e_1 and e_2 such that the corresponding private exponents d_1 and d_2 satisfy $d_1, d_2 < N^{0.357}$. In [11], Sarkar and Maitra improved this bound up to $d_1, d_2 < N^{0.416}$.

In this paper, we present three new attacks on RSA. The first attack works for $k \geq 2$ moduli $N_i = p_i q_i$, $i = 1, \ldots, k$, when k instances (N_i, e_i) are such that there exist an integer x, k integers y_i, and k integers z_i satisfying $e_i x - y_i\phi(N_i) = z_i$. We show that the k RSA moduli N_i can be factored in polynomial time if $N = \min_i N_i$ and

$$x < N^\delta,\ y_i < N^\delta,\ |z_i| < \frac{p_i - q_i}{3(p_i + q_i)} y_i N^{1/4} \text{ where } \delta = \frac{k}{2(k+1)}.$$

The second attack works when the k instances (N_i, e_i) of RSA are such that there exist an integer y, and k integers x_i, and k integers z_i satisfying $e_i x_i - y\phi(N_i) = z_i$. Similarly, we show that the k RSA moduli N_i can be factored in polynomial time if $N = \min_i N_i$, $\min_i e_i = N^\alpha$, and

$$x_i < N^\delta,\ y < N^\delta,\ |z_i| < \frac{p_i - q_i}{3(p_i + q_i)} y N^{1/4} \text{ where } \delta = \frac{(2\alpha - 1)k}{2(k+1)}.$$

In both scenarios, we transform the equations into a simultaneous diophantine problem and apply lattice basis reduction techniques to find the parameters (x, y_i) or (y, x_i). This leads to a suitable approximation of $p_i + q_i$ which allows us to apply Coppersmith's method [4] to compute the prime factors p_i and q_i of the moduli N_i.

The third attack enables us to factor an RSA modulus $N = pq$ when the prime factors share their LSBs in the presence of two public exponents e_1 and e_2 such that the corresponding decryption exponents d_1 and d_2 share their MSBs. To be more precise, suppose that $e = N^\gamma$, $|p - q| = 2^m x$ with $2^m = N^\alpha$, and $|d_1 - d_2| < N^\beta$. We show that one can factor the RSA modulus if $d_1, d_2 < N^\delta$ under the condition

$$\delta < \frac{5}{2} - 2\alpha - \beta - \frac{1}{4}\sqrt{6(1 - 4\alpha)(5 + 4\gamma - 4\alpha - 4\beta)}. \tag{1}$$

As an example, observe that, in the situation that $\gamma = 1$, $\alpha = 0.2$, and $\beta = \delta$, that is d_1 and d_2 differ in the first MSBs, then the condition (1) gives $\delta < 0.736$ which improves the bound $\delta < 0.662$ obtained in [18]. On the other hand, in the standard situation $\gamma = 1$, $\alpha = 0$, and $\beta = \delta$, that is when the prime integers p, q do not share any LSBs and d_1, d_2 do not share any MSBs, the condition (1) gives $\delta < 0.422$ which also improves the bound $\delta < 0.416$ found in [11]. Our method is based on Coppersmith's method for solving polynomial equations

The remainder of this paper is organized as follows. In Section 2, we review the tools that we apply in the scenarios, namely Coppersmith's method, lattice basis reduction and simultaneous diophantine approximations. We also present some useful results that will be used through the paper. In Section 3, we present the first attack. In Section 4, we present the second attack and in Section 5, we present the third attack. We conclude in Section 6.

2 Preliminaries

In this section, we give some basics on Coppersmith's method, lattice basis reduction techniques and simultaneous diophantine equations that will be used in this paper.

2.1 Coppersmith's method

At Eurocrypt'96, Coppersmith [4] proposed an algorithm for finding small roots of bivariate integer polynomial equations in polynomial-time. The algorithm is based on the LLL algorithm [10] for lattice reduction. A clever application of Coppersmith's algorithm is to factor an RSA modulus $N = pq$ when half of the least significant or most significants bits of p are known.

Theorem 1 (Coppersmith). *Let $N = pq$ be the product of two unknown integers such that $q < p < 2q$. Given an approximation of p with additive error term at most $N^{\frac{1}{4}}$, then p and q can be found in polynomial time.*

Coppersmith's method has been heuristically extended to many variables. To find the small roots of a multivariate polynomial $f(x_1, \cdots, x_n)$, we construct a set of coprime polynomials with small coefficients which contain the same roots over the integers. This can be done by applying the LLL algorithm to a lattice that can be built using the strategy of Jochemsz and May [9]. To this end, a practical way is the use the following result of Howgrave-Graham [7].

Theorem 2 (Howgrave-Graham). *Let $h(x_1, \cdots, x_n) \in \mathbb{Z}[x_1, \cdots, x_n]$ be a polynomial with at most ω monomials. Suppose that $h\left(x_1^{(0)}, \cdots, x_n^{(0)}\right) \equiv 0 \pmod{R}$ where $|x_i^{(0)}| < X_i$ for $i = 1, \ldots, n$, and*

$$h(x_1X_1, \cdots, x_nX_n) < \frac{R}{\sqrt{\omega}}.$$

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

To find the small roots of the first polynomials of the LLL-reduced basis, we can use Gröbner bases or evaluation of resultants.

2.2 Lattice reductions and simultaneous diophantine approximations

Let $u_1 \ldots, u_d$ be d linearly independent vectors of $\mathbb{R}^n$ with $d \leq n$. The set of all integer linear combinations of the vectors $u_1 \ldots, u_d$ is called a lattice and is in the form

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

The set $(u_1, \ldots, u_d)$ is called a basis of $\mathcal{L}$ and d is its dimension. The determinant of $\mathcal{L}$ is defined as $\det(\mathcal{L}) = \sqrt{\det(U^TU)}$ where U is the the matrix of the u_i's in the canonical basis of $\mathbb{R}^n$. Define $\|v\|$ to be the Euclidean norm of a vector $v \in \mathcal{L}$. A central problem in lattice reduction is to find a short non-zero vector in $\mathcal{L}$. The LLL algorithm of Lenstra, Lenstra, and Lovász [10] produces a reduced basis and answers positively but partially this problem. The following result fixes the sizes of the reduced basis vectors (see [12]).

Theorem 3. *Let L be a lattice of dimension ω with a basis $\{v_1, \ldots, v_\omega\}$. The LLL algorithm produces a reduced basis $\{b_1, \cdots, b_\omega\}$ satisfying*

$$\|b_1\| \leq \|b_2\| \leq \cdots \leq \|b_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i}} \det(L)^{\frac{1}{\omega+1-i}},$$

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

One important application of the LLL algorithm is that it provides a solution to the simultaneous diophantine approximations problem which is defined as follows. Let $\alpha_1, \ldots, \alpha_n$ be n real numbers and ε a real number such that $0 < \varepsilon < 1$. A classical theorem of Dirichlet asserts that there exist integers $p_1, \cdots, p_n$ and a positive integer $q \leq \varepsilon^{-n}$ such that

$$|q\alpha_i - p_i| < \varepsilon \quad \text{for} \quad 1 \leq i \leq n.$$

In 1982, Lenstra, Lenstra and Lovász[10] described a method to find simultaneous diophantine approximations to rational numbers. In their work, they considered a lattice with real entries. We state below a similar result for a lattice with integer entries.

Theorem 4 (Simultaneous Diophantine Approximations). *There is a polynomial time algorithm, for given rational numbers $\alpha_1, \ldots, \alpha_n$ and $0 < \varepsilon < 1$, to compute integers $p_1, \cdots, p_n$ and a positive integer q such that*

$$\max_i |q\alpha_i - p_i| < \varepsilon \quad \textit{and} \quad q \leq 2^{n(n-3)/4} \cdot 3^n \cdot \varepsilon^{-n}.$$

Proof. See Appendix A. □

2.3 Primes sharing LSBs

The following lemma is reformulation of a result of [15]. It concerns an RSA modulus $N = pq$ when the prime factors p and q share an amount of their LSBs.

Lemma 1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose that $p - q = 2^m u$ for a known value m. Then $p = 2^m p_1 + u_0$ and $q = 2^m q_1 + u_0$ where u_0 is a solution of the equation $x^2 \equiv N \pmod{2^m}$ and $p + q = 2^{2m} v + v_0$ with*

$$v_0 \equiv 2u_0 + \left(N - u_0^2\right) u_0^{-1} \pmod{2^{2m}}.$$

Proof. See Appendix B. □

2.4 Approximations of the primes in RSA

Let $N = pq$ be an RSA modulus with $q < p < 2q$. Then $p + q$ satisfies the following inequalities (see [13])

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

The following result shows that any approximation of $p + q$ will lead to an approximation of p.

Lemma 2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose we know an approximation S of $p + q$ such that $S > 2N^{\frac{1}{2}}$ and*

$$|p + q - S| < \frac{p - q}{3(p + q)} N^{\frac{1}{4}}.$$

Then $\tilde{P} = \frac{1}{2}\left(S + \sqrt{S^2 - 4N}\right)$ is an approximation of p satisfying $|p - \tilde{P}| < N^{\frac{1}{4}}$.

Proof. See Appendix C. □

Remark 1. Notice that in Section 4.1.2 of the ANSI X9.31:1998 standard for public key cryptography [1], there are a number of recommendations for the generation of the primes in $N = pq$. One criteria is that the primes p, q shall satisfy $p - q > 2^{-100}\sqrt{N}$. Combining with (2) when $q < p < 2q$ and $N > 2^{1024}$, this implies that the term $\frac{p-q}{3(p+q)} N^{\frac{1}{4}}$ satisfies

$$\frac{p - q}{3(p + q)} N^{\frac{1}{4}} > \frac{2^{-100}\sqrt{N}}{9\frac{\sqrt{2}}{2}\sqrt{N}} \cdot 2^{256} = \frac{2^{157}}{9\sqrt{2}}.$$

This shows that, when $N = pq > 2^{1024}$ and the prime factors p and q are chosen following the ANSI X9.31:1998 standard, the approximation extra term $\frac{(p-q)}{3(p+q)} N^{\frac{1}{4}}$ of $p + q$ is not too small.

3 The First Attack on *k* RSA Moduli

In this section, we are given $k \geq 2$ moduli $N_i = p_i q_i$ with the same size N. We suppose in this scenario that the RSA moduli satisfy k equations $e_i x - y_i \phi(N_i) = z_i$. Notice that the parameters $\phi(N_i) = (p_i - 1)(q_i - 1)$ are also unknown. We show that it is possible to factor the RSA moduli N_i if the unknown parameters x, y_i and z_i are suitably small.

Theorem 5. *For $k \geq 2$, let $N_i = p_i q_i$, $1 \leq i \leq k$, be k RSA moduli. Let $N = \min_i N_i$. Let e_i, $i = 1, \ldots, k$, be k public exponents. Define $\delta = \frac{k}{2(k+1)}$. If there exist an integer $x < N^{\delta}$ and k integers $y_i < N^{\delta}$ and $|z_i| < \frac{p_i - q_i}{3(p_i + q_i)} y_i N^{1/4}$ such that $e_i x - y_i \phi(N_i) = z_i$ for $i = 1, \ldots, k$, then one can factor the k RSA moduli $N_1, \cdots N_k$ in polynomial time.*

Proof. For $k \geq 2$ and $i = 1, \ldots, k$, the equation $e_i x - y_i \phi(N_i) = z_i$ can be rewritten as $e_i x - y_i(N_i + 1) = z_i - y_i(p_i + q_i)$. Hence

$$\left| \frac{e_i}{N_i + 1} x - y_i \right| = \frac{|z_i - y_i(p_i + q_i)|}{N_i + 1}. \tag{3}$$

Let $N = \min_i N_i$ and suppose that $y_i < N^{\delta}$ and $|z_i| < \frac{p_i - q_i}{3(p_i+q_i)} y_i N^{1/4}$. Then $|z_i| < y_i N^{1/4} < N^{\delta+\frac{1}{4}}$. Since by (2) we have $p_i + q_i < \frac{3\sqrt{2}}{2}\sqrt{N}$, we will get

$$\begin{aligned}\frac{|z_i - y_i(p_i+q_i)|}{N_i+1} &\leq \frac{|z_i| + y_i(p_i+q_i)}{N} \\ &< \frac{N^{\delta+1/4} + \frac{3\sqrt{2}}{2}N^{\delta+1/2}}{N} \\ &< \frac{\sqrt{5}N^{\delta+1/2}}{N} \\ &= \sqrt{5}N^{\delta-1/2}.\end{aligned}$$

Plugging in (3), we get

$$\left|\frac{e_i}{N_i+1}x - y_i\right| < \sqrt{5}N^{\delta-1/2}.$$

We now proceed to prove the existence of the integer x. Let $\varepsilon = \sqrt{5}N^{\delta-1/2}$, $\delta = \frac{k}{2(k+1)}$. We have

$$N^{\delta} = N^{k/2-k\delta} < 2^{k(k-3)/4} \cdot 3^k \cdot \left(\sqrt{5}N^{\delta-1/2}\right)^{-k} = 2^{k(k-3)/4} \cdot 3^k \cdot \varepsilon^{-k}.$$

It follows that if $x < N^{\delta}$, then $x < 2^{k(k-3)/4} \cdot 3^k \varepsilon^{-k}$. Summarizing, for $i = 1, \ldots, k$, we have

$$\left|\frac{e_i}{N_i+1}x - y_i\right| < \varepsilon, \quad x < 2^{k(k-3)/4} \cdot 3^k \cdot \varepsilon^{-k}.$$

It follows that the conditions of Theorem 4 are fulfilled which will find x and y_i for $i = 1, \ldots, k$. Next, using the equation $e_i x - y_i \phi(N_i) = z_i$, we get

$$p_i + q_i = N_i + 1 - \frac{e_i x}{y_i} + \frac{z_i}{y_i}.$$

Since $|z_i| < \frac{p_i - q_i}{3(p_i+q_i)} y_i N^{1/4}$, then $\frac{z_i}{y_i} < \frac{p_i - q_i}{3(p_i+q_i)} N^{1/4}$ and $S_i = N_i + 1 - \frac{e_i x}{y_i}$ is an approximation of $p_i + q_i$ with an error of at most $\frac{p_i - q_i}{3(p_i+q_i)} N^{1/4}$. Hence, using Lemma 2, we can find an approximation $\tilde{P}_i = \frac{1}{2}\left(S_i + \sqrt{S_i^2 - 4N_i}\right)$ of p_i such that $|p_i - \tilde{P}_i| < N^{1/4}$. Then, for each $i = 1, \ldots, k$, we find p_i using Theorem 1. This leads to the factorization of the k RSA moduli $N_1, \ldots, N_k$. □

Remark 2. It is conjectured in [3] that an RSA instance with a modulus $N = pq$ and a public exponent e is insecure if $ed - y\phi(N) = 1$ with $d < N^{1/2}$. This conjecture can be related to Theorem 5 as follows. Suppose that k RSA moduli $N_1, \cdots, N_k$ and k public exponents $e_1, \ldots, e_k$ satisfy $e_1 d - y_1 \phi(N_1) = 1$ and $e_i d - y_i \phi(N_i) = z_i$, $i = 2, \ldots, k$, where $d < N^{\delta}$, $y_i < N_1^{\delta}$ and $|z_i| < \frac{p_i - q_i}{3(p_i+q_i)} y_i N^{1/4}$ with $\delta = \frac{k}{2(k+1)}$. Then, by Theorem 5, one can factor the RSA moduli $N_1, \cdots, N_k$. Observe that, for sufficiently large k, we have $\delta \approx \frac{1}{2}$, which answer positively the conjecture in this case.

Example 1. Consider the following 3 RSA moduli and public exponents

$$\begin{aligned}
N_1 &= 133935451509182385915180124 1, \ e_1 = 1050185284614316002488409263,\\
N_2 &= 5761318740014279657192789531, \ e_2 = 1492152853356436953159599262\\
N_3 &= 1257936900682879025849691469, \ e_3 = 1039188969087059416671255 87.
\end{aligned}$$

Then $N = \max(N_1, N_2, N_3) = 5761318740014279657192789531$. Since $k = 3$, we get $\delta = \frac{k}{2(k+1)} = 0.375$ and $\varepsilon = \sqrt{5}N^{\delta-1/2} \approx 0.000757$. Using (11) with $n = k = 3$, we find

$$C = \left\lfloor 3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1} \right\rfloor = 123330787675873.$$

Consider the lattice $\mathcal{L}$ spanned by the matrix

$$M = \begin{bmatrix} 1 & -[Ce_1/(N_1+1)] & -\lceil Ce_2/(N_2+1)] & -[Ce_3/(N_3+1)\rceil \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}.$$

Then, applying the LLL algorithm to $\mathcal{L}$, we get a reduced basis with the matrix

$$K = \begin{bmatrix} -3779027519, -18311525449, -3194797920, -5032583842 \\ 7689269805, -1894087712, 24623557005, -10208017761 \\ 33347077827, -5532195789, -23880055457, -2777199762 \\ 1955330759, -28195205997, 36977018712, 75348896931 \end{bmatrix}.$$

Next, computing $K \cdot M^{-1}$, we observe that the first row is

$$[-3779027519, -2963128168, -978749302, -312187655],$$

from which we deduce $x = 3779027519$, $y_1 = 2963128168$, $y_2 = 978749302$ and $y_3 = 312187655$. Using x and y_i for $i = 1, 2, 3$, define $S_i = \left\lfloor N_i + 1 - \frac{e_i x}{y_i} \right\rceil$. We get

$$S_1 = 73202632183869, \quad S_2 = 152156156125079, \quad S_3 = 102878795201660.$$

For $i = 1, 2, 3$, let $D_i = \left\lfloor \sqrt{S_i^2 - 4N_i} \right\rceil$. We get

$$D_1 = 1098771258961, \quad D_2 = 10306351764921, \quad D_3 = 74513749733949.$$

By Lemma 2, for $i = 1, 2, 3$, $\tilde{P}_i = \frac{1}{2}(S_i + D_i)$ is a candidate for an approximation of p_i. Applying Coppersmith's method 1 with $\tilde{P}_i$ for $i = 1, 2, 3$, we get

$$p_1 = 37150702190747, \quad p_2 = 81231254125183, \quad p_3 = 88696272470797.$$

This leads us to the factorization of the 3 RSA moduli N_1, N_2 and N_3. Observe that $x > N^{0.344}$ is much larger than Blömer-May's bound $x < \frac{1}{3}N^{1/4}$. This shows that Blömer-May's attack will not give the factorization of the RSA moduli in this example.

4 The Second Attack on k RSA Moduli

In this section, we consider the second scenario when the k RSA moduli satisfy k equations of the shape $e_ix_i - y\phi(N_i) = z_i$ where the parameters x_i, y and z_i are suitably small unknown parameters.

Theorem 6. *For $k \geq 3$, let $N_i = p_iq_i$, $1 \leq i \leq k$, be k RSA moduli with the same size N. Let e_i, $i = 1, \dots, k$, be k public exponents with $\min_i e_i = N^\alpha$. Let $\delta = \frac{(2\alpha-1)k}{2(k+1)}$. If there exist an integer $y < N^\delta$ and k integers $x_i < N^\delta$ and $|z_i| < \frac{p_i-q_i}{3(p_i+q_i)}yN^{1/4}$ such that $e_ix_i - y\phi(N_i) = z_i$ for $i = 1, \dots, k$, then one can factor the k RSA moduli $N_1, \cdots N_k$ in polynomial time.*

Proof. For $i = 1, \dots, k$, the equation $e_ix_i - y\phi(N_i) = z_i$ can be transformed into $e_ix_i - y(N_i + 1) = z_i - y(p_i + q_i)$. Hence

$$\left|\frac{N_i+1}{e_i}y - x_i\right| = \frac{|z_i - y(p_i+q_i)|}{e_i}. \tag{4}$$

Let $N = \max_i N_i$. Suppose that $y < N^\delta$ and $|z_i| < \frac{p_i-q_i}{3(p_i+q_i)}yN^{1/4}$. Also, suppose that $\min_i e_i = N^\alpha$. Since by (2) we have $p_i + q_i < \frac{\sqrt{3}}{2}\sqrt{N_i}$, then we get

$$\begin{aligned}\frac{|z_i - y(p_i+q_i)|}{e_i} &\leq \frac{|z_i| + y(p_i+q_i)}{N^\alpha}\\ &< \frac{N^{\delta+\frac{1}{4}} + \frac{3\sqrt{2}}{2}N_i^{\delta+\frac{1}{2}}}{N^\alpha}\\ &< \frac{\sqrt{5}N^{\delta+\frac{1}{2}}}{N^\alpha}\\ &= \sqrt{5}N^{\delta+\frac{1}{2}-\alpha}.\end{aligned}$$

Using this in (4), we get

$$\left|\frac{N_i+1}{e_i}y - x_i\right| < \sqrt{5}N^{\delta+\frac{1}{2}-\alpha}.$$

We now proceed to prove the existence of y and the integers x_i. Let $\varepsilon = \sqrt{5}N^{\delta+\frac{1}{2}-\alpha}$, $\delta = \frac{(2\alpha-1)k}{2(k+1)}$. We have

$$N^\delta\varepsilon^k = 5^{\frac{k}{2}}N^{\delta+k\delta+\frac{k}{2}-k\alpha} = 5^{\frac{k}{2}}.$$

Then, since $5^{\frac{k}{2}} < 2^{\frac{k(k-3)}{4}} \cdot 3^k$ for $k \geq 2$, we get $N^\delta\varepsilon^k < 2^{k(k-3)/4} \cdot 3^k$. It follows that if $y < N^\delta$, then $y < 2^{k(k-3)/4} \cdot 3^k\varepsilon^{-k}$. Summarizing, we have

$$\left|\frac{N_i+1}{e_i}y - x_i\right| < \varepsilon, \quad y < 2^{k(k-3)/4} \cdot 3^k \cdot \varepsilon^{-k}, \quad \text{for} \quad i = 1, \dots, k,$$

It follows that the conditions of Theorem 4 are fulfilled and we will obtain y and x_i for $i = 1, \dots, k$. Next, by utilizing the equation $e_ix_i - y\phi(N_i) = z_i$, we get

$$p_i + q_i = N_i + 1 - \frac{e_ix_i}{y} + \frac{z_i}{y}.$$

Since $|z_i| < \frac{p_i-q_i}{3(p_i+q_i)}yN^{1/4}$, then $\frac{|z_i|}{y} < \frac{p_i-q_i}{3(p_i+q_i)}N^{1/4}$ and $S_i = N_i + 1 - \frac{e_ix_i}{y}$ is an approximation of $p_i + q_i$ with an error of at most $\frac{p_i-q_i}{3(p_i+q_i)}N^{1/4}$. Hence, using Lemma 2, we can find an approximation $\tilde{P}_i = \frac{1}{2}\left(S_i + \sqrt{S_i^2 - 4N_i}\right)$ of p_i such that $|p_i - \tilde{P}_i| < N^{1/4}$. Then, using Theorem 1, we find p_i for $i = 1, \ldots, k$. This leads to the factorization of the k RSA moduli $N_1, \ldots, N_k$. □

Example 2. Consider the following three RSA moduli and three public exponents

$$\begin{aligned}
N_1 &= 701404527220444023808491592451,\\
e_1 &= 598872437015970469816654047240,\\
N_2 &= 287595248854210987719090191831,\\
e_2 &= 166801923182837419445821944696,\\
N_3 &= 431174708848373283683684641751,\\
e_3 &= 373743791338260494286817160907.
\end{aligned}$$

Then $N = \max(N_1, N_2, N_3) = 701404527220444023808491592451$. We also get $\min(e_1, e_2, e_3) = N^\alpha$ with $\alpha \approx 0.9791$. Since $k = 3$, we get $\delta = \frac{k(2\alpha-1)}{2(k+1)} = 0.359325$ and $\varepsilon = \sqrt{5}N^{\delta+1/2-\alpha} \approx 0.000595$. Using (11) with $n = k = 3$, let

$$C = \left[3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1}\right] = 323072188568099.$$

Consider the lattice $\mathcal{L}$ spanned by the the rows of the matrix

$$M = \begin{bmatrix} 1 & -[C(N_1+1)/e_1] & -\lceil C(N_2+1)/e_2] & -[C(N_3+1)/e_3\rceil \\ 0 & C & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & C \end{bmatrix}.$$

Then, applying the LLL algorithm to $\mathcal{L}$, we get a reduced basis with the matrix

$$K = \begin{bmatrix} 9963214223 & -13283752558 & -23775330798 & -12098528625 \\ -23587427317 & -20479775765 & -11829398252 & 7542788188 \\ -80616201478 & 123609103667 & -102601176821 & -4090837289 \\ -641512285490 & -64738610576 & -108985237738 & -147068239663 \end{bmatrix}.$$

Next, we get

$$K \cdot M^{-1} = \begin{bmatrix} 9963214223 & 11669001827 & 17178297583 & 11494200282 \\ -23587427317 & -27625796886 & -40668787863 & -27211962691 \\ -80616201478 & -94418385601 & -138996218289 & -93003999013 \\ -41512285490 & -48619544294 & -71574331088 & -47891223947 \end{bmatrix}.$$

From the first row, we deduce $y = 9963214223$, $x_1 = 11669001827$, $x_2 = 17178297583$, and $x_3 = 11494200282$. Using y and x_i for $i = 1, 2, 3$, define $S_i = \left[N_i + 1 - \frac{e_ix_i}{y}\right]$. We get

$$S_1 = 1677562597323852, \quad S_2 = 1169977613299368, \quad S_3 = 1377024442150848.$$

For $i = 1, 2, 3$, let $D_i = \left[\sqrt{S_i^2 - 4N_i}\right]$. We get

$$D_1 = 92726258730590, \quad D_2 = 467404129426390, \quad D_3 = 414122540907110.$$

By Lemma 2, for $i = 1, 2, 3$, $\tilde{P}_i = \frac{1}{2}(S_i + D_i)$ is a candidate for an approximation of p_i. Applying Coppersmith's method 1 with $\tilde{P}_i$ for $i = 1, 2, 3$, we get

$$p_1 = 885144428027221, \quad p_2 = 818690871362879, \quad p_3 = 895573491528979.$$

This leads to the factorization of the three RSA moduli N_1, N_2 and N_3. Observe that $\min(x_1, x_2, x_3) > N^{0.337}$ is much larger than Blömer-May's bound $x < \frac{1}{3}N^{1/4}$. This shows that Blömer-May's attack does not work in this case.

5 The Third Attack on RSA With Primes and Decryption Exponents Sharing Bits

In this section, we present the attack which applies when the prime factors of an RSA modulus share an amount of their LSBs in the presence of two decryption exponents d_1 and d_2 sharing an amount of their MSBs.

5.1 The attack

Theorem 7. *Let $N = pq$ be an RSA modulus such that $p - q = 2^m u$ where $2^m \approx N^\alpha$. Let e_1 and e_2 be two public exponents satisfying $e_1, e_2 \approx N^\gamma$, $e_1 d_1 - k_1\phi(N) = 1$, and $e_2 d_2 - k_2\phi(N) = 1$. Suppose that $d_1, d_2 < N^\delta$ and $|d_1 - d_2| < N^\beta$. Then one can factor N in polynomial time if*

$$\delta < \frac{5}{2} - 2\alpha - \beta - \frac{1}{4}\sqrt{6(1-4\alpha)(5 + 4\gamma - 4\alpha - 4\beta)}.$$

Proof. Suppose that e_1 and e_2 are two public exponents satisfying $e_1 d_1 - k_1\phi(N) = 1$, $e_2 d_2 - k_2\phi(N) = 1$. Multiplying the first equation by e_2 and the second by e_1 and subtracting, we get

$$e_1 e_2 (d_1 - d_2) - e_2 k_1 \phi(N) + e_1 k_2 \phi(N) = e_2 - e_1. \tag{5}$$

Suppose that $p - q = 2^m u$. Then, Lemma 1 shows that $p + q$ is in the form $p + q = v_0 + 2^{2m} v$ where $v_0 \equiv 2u_0 + \left(\left(N - u_0^2\right) u_0^{-1} \pmod{2^{2m}}\right)$ and u_0 is a solution of the modular equation $x^2 \equiv N \pmod{2^m}$. Hence

$$\phi(N) = N + 1 - (p + q) = N + 1 - v_0 - 2^{2m} v.$$

Plugging this in (5), we get

$$\begin{aligned} &e_1 e_2 (d_1 - d_2) - e_2 k_1 \left(N + 1 - v_0 - 2^{2m} v\right) + e_1 k_2 \left(N + 1 - v_0 - 2^{2m} v\right) \\ &= e_2 - e_1. \end{aligned}$$

which can be rewritten as

$$\begin{aligned} &e_1e_2(d_1-d_2)-e_2(N+1-v_0)k_1+2^{2m}e_2k_1v+e_1(N+1-v_0)k_2\\ &\quad-2^{2m}e_1k_2v+(e_1-e_2)=0. \end{aligned} \tag{6}$$

Fix the known and the unknown parameters as follows

$$\begin{cases} a_1{=}e_1e_2,\\ a_2{=}{-}e_2(N+1-v_0),\\ a_3{=}2^{2m}e_2,\\ a_4{=}e_1(N+1-v_0),\\ a_5{=}{-}2^{2m}e_1,\\ a_6{=}e_1-e_2, \end{cases} \quad \text{and} \quad \begin{cases} x_1{=}d_1-d_2,\\ x_2{=}k_1,\\ x_3{=}k_2,\\ x_4{=}v. \end{cases}$$

Hence, the equation (6) becomes $a_1x_1+a_2x_2+a_3x_2x_4+a_4x_3+a_5x_3x_4+a_6=0$. Consider the polynomial

$$f(x_1,x_2,x_3,x_4)=a_1x_1+a_2x_2+a_3x_2x_4+a_4x_3+a_5x_3x_4+a_6.$$

Then (d_1-d_2,k_1,k_2,v) is a root of $f(x_1,x_2,x_3,x_4)$ which can be small enough to be found by Coppersmith's technique. To find the small roots of $f(x_1,x_2,x_3,x_4)$ using this method, we use the extended strategy of Jochemsz and May [9]. We will need the following bounds.

- $\max(e_1,e_2)=N^{\gamma}$,
- $\max(d_1,d_2)<N^{\delta}$,
- $|d_1-d_2|<X_1=N^{\beta}$,
- $k_1=\frac{e_1d_1-1}{\phi(N)}<X_2=N^{\gamma+\delta-1}$,
- $k_2=\frac{e_2d_2-1}{\phi(N)}<X_3=N^{\gamma+\delta-1}$,
- $p-q=2^mu$ with $2^m=N^{\alpha}$ and $\alpha<\frac{1}{4}$.
- By (2) and Lemma 1, $p+q=2^{2m}v+v_0$ with $v<X_4=3N^{1/2-2\alpha}$.

Observe that $\alpha<\frac{1}{4}$, otherwise p and q can be found using Coppersmith's metho [4]. Let us fix the bounds of the unknown parameters

$$X_1=N^{\beta},\quad X_2=N^{\gamma+\delta-1},\quad X_3=N^{\gamma+\delta-1},\quad X_4=3N^{1/2-2\alpha}. \tag{7}$$

Let m and t be two positive integers. Define the set

$$S=\bigcup_{0\leq j\leq t}\{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_3^{i_3+j}\ \Big|\ x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}\quad\text{monomial of}\quad f^{m-1}\}.$$

and the set

$$M=\{\text{monomials of}\quad x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}f\ \Big|\ x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}\in S\}.$$

Neglecting the coefficients, it is easy to find that $f^{m-1}(x_1,x_2,x_3,x_4)$ satisfies

$$f^{m-1}(x_1,x_2,x_3,x_4)=\sum_{i_1=0}^{m-1}\sum_{i_2=0}^{m-1-i_1}\sum_{i_3=0}^{m-1-i_1-i_2}\sum_{i_4=0}^{i_2+i_3}x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}.$$

This leads to the characterization of the monomials $x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}$ of S:

$$x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4} \in S \quad \text{if} \quad \begin{cases} i_1{=}0,\dots,m-1, \\ i_2{=}0,\dots,m-1-i_1, \\ i_3{=}0,\dots,m-1-i_1-i_2, \\ i_4{=}0,\dots,i_2+i_3+t. \end{cases}$$

We also easily find

$$x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4} \in M \quad \text{if} \quad \begin{cases} i_1{=}0,\dots,m, \\ i_2{=}0,\dots,m-i_1, \\ i_3{=}0,\dots,m-i_1-i_2, \\ i_4{=}0,\dots,i_2+i_3+t. \end{cases}$$

Define

$$\begin{aligned} W &= \|f(x_1X_1,x_2X_2,x_3X_3,x_4X_4)\|_\infty \\ &= \max(|a_1|X_1,|a_2|X_2,|a_3|X_2X_3,|a_4|X_4,|a_5|X_4X_3,|a_6|). \end{aligned}$$

Then W satisfies

$$W \geq |a_2|X_2 = e_2(N+1-v_0)N^{\gamma+\delta-1} \approx N^{2\gamma+\delta}. \tag{8}$$

Next, define

$$R = WX_1^{m-1}X_2^{m-1}X_3^{m-1}X_4^{m-1+t}.$$

Without loss of generality, suppose that $a_6 = e_1 - e_2$ is coprime with R. We define $f'(x_1,x_2,x_3,x_4) = a_6^{-1}f(x_1,x_2,x_3,x_4) \pmod{R}$ so that $f'(0,0,0,0) = 1$. Next, define the polynomials

$$\begin{aligned} g_{i_1,i_2,i_3,i_4} &= x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}f'X_1^{m-1-i_1}X_2^{m-1-i_2}X_3^{m-1-i_3}X_4^{m-1+t-i_4}, \\ &\quad \text{with} \quad x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4} \in S, \\ h_{i_1,i_2,i_3,i_4} &= x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}R, \\ &\quad \text{with} \quad x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4} \in M\backslash S. \end{aligned}$$

The monomials of $M\backslash S$ reduce to $x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}$ with $(x_1,x_2,x_3,x_4) \in S_i$ for $i = 1,2,3$ where

$$S_1 = \{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}\} \text{ for } \begin{cases} i_1{=}m, \\ i_2{=}0,\dots,m-i_1, \\ i_3{=}0,\dots,m-i_1-i_2, \\ i_4{=}0,\dots,i_2+i_3+t. \end{cases}$$

$$S_2 = \{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}\} \text{ for } \begin{cases} i_1{=}0,\dots,m-1, \\ i_2{=}m-i_1, \\ i_3{=}0,\dots,m-i_1-i_2, \\ i_4{=}0,\dots,i_2+i_3+t. \end{cases}$$

$$S_3 = \{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}\} \text{ for } \begin{cases} i_1{=}0,\dots,m-1, \\ i_2{=}0,\dots,m-1-i_1, \\ i_3{=}m-i_1-i_2, \\ i_4{=}0,\dots,i_2+i_3+t. \end{cases}$$

As shown in [9], we use the coefficients of $g_{i_1,i_2,i_3,i_4}(x_1X_1, x_2X_2, x_3X_3, x_4X_4)$ and $h_{i_1,i_2,i_3,i_4}(x_1X_1, x_2X_2, x_3X_3, x_4X_4)$ to build a basis of a lattice L with dimension

$$\omega = \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4} \in M} 1 = \frac{1}{12}(m+1)(m+2)(m+3)(m+2t+2).$$

The following ordering of the monomials is performed to construct an upper triangular matrix: if $\sum i_j < \sum i'_j$ then $x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4} < x_1^{i'_1}x_2^{i'_2}x_3^{i'_3}x_4^{i'_4}$ and if $\sum i_j = \sum i'_j$ then the monomials are lexicographically ordered. The diagonal entries of the matrix are of the form

$$\begin{cases} (X_1X_2X_3)^{m-1}X_4^{m-1+t} & \text{for the polynomials } g \\ WX_1^{m-1+i_1}X_2^{m-1+i_2}X_3^{m-1+i_3}X_4^{m-1+t+i_4} & \text{for the polynomials } h. \end{cases}$$

Define

$$s_j = \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4} \in M\backslash S} i_j, \text{ for } j = 1, \ldots, 4. \tag{9}$$

The determinant of L is then

$$\begin{aligned} \det(L) &= W^{|M\backslash S|}X_4^{(m-1+t)|S|+(m-1+t)|M\backslash S|+s_4}\prod_{j=1}^{3}X_j^{(m-1)|S|+(m-1)|M\backslash S|+s_j} \\ &= W^{|M\backslash S|}x_4^{(m-1+t)\omega+s_4}\prod_{j=1}^{3}X_j^{(m-1)\omega+s_j}. \end{aligned}$$

All the polynomials $g(x_1, x_2, x_3, x_4)$ and $h(x_1, x_2, x_3, x_4)$ and their combinations share the root $(d_1 - d_2, k_1, k_2, v)$ modulo R. Applying the LLL algorithm to the lattice L with the basis spanned by the polynomials $g(x_1X_1, x_2X_2, x_3X_3, x_4X_4)$ and $h(x_1X_1, x_2X_2, x_3X_3, x_4X_4)$, we get a new basis with short vectors. Let $f_i(x_1X_1, x_2X_2, x_3X_3, x_4X_4)$, $i = 1, 2, 3$ be three short vectors of the reduced basis. Each f_i is a combination of g and h, and then share the root $(d_1 - d_2, k_1, k_2, v)$. Then, by Theorem 3, we have for $i = 1, 2, 3$

$$\|f_i(x_1X_1, x_2X_2, x_3X_3, x_4X_4)\| < 2^{\frac{\omega(\omega-1)}{4(\omega-2)}}\det(L)^{\frac{1}{\omega-2}}.$$

For $i = 1, 2, 3$, we force the polynomials f_i to satisfy Howgrave-Graham's bound $\|f_i(x_1X_1, x_2X_2, x_3X_3, x_4X_4)\| < \frac{R}{\sqrt{\omega}}$. A sufficient condition is

$$2^{\frac{\omega(\omega-1)}{4(\omega-2}}\det(L)^{\frac{1}{\omega-2}} < \frac{R}{\sqrt{\omega}},$$

which can be transformed into $\det(L) < R^{\omega}$, that is

$$W^{|M\backslash S|}x_4^{(m-1+t)\omega+s_4}\prod_{j=1}^{3}X_j^{(m-1)\omega+s_j} < \left(WX_1^{m-1}X_2^{m-1}X_3^{m-1}X_4^{m-1+t}\right)^{\omega}.$$

Using $\omega = |M|$ and $|M| - |M \backslash S| = |S|$, we get

$$\prod_{j=1}^{4} X_j^{s_j} < W^{|S|}. \tag{10}$$

Using (9), we easily get

$$\begin{aligned}
s_1 &= \frac{1}{12} m(m+1)(m+2)(m+2t+1),\\
s_2 &= \frac{1}{24} m(m+1)(m+2)(3m+4t+5),\\
s_3 &= \frac{1}{24} m(m+1)(m+2)(3m+4t+5),\\
s_4 &= \frac{1}{24} (m+1)(m+2)(3m^2+5m+8tm+6t+6t^2).
\end{aligned}$$

Similarly, we get

$$|S| = \sum_{x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} \in S} 1 = \frac{1}{12} m(m+1)(m+2)(m+2t+1).$$

Set $t = \tau m$, then,

$$\begin{aligned}
s_1 &= \frac{1}{12}(2\tau+1)m^4 + o(m^4),\\
s_2 &= \frac{1}{24}(4\tau+3)m^4 + o(m^4),\\
s_3 &= \frac{1}{24}(4\tau+3)m^4 + o(m^4),\\
s_4 &= \frac{1}{24}(6\tau^2+8\tau+3)m^4 + o(m^4),\\
|S| &= \frac{1}{12}(2\tau+1)m^4 + o(m^4).
\end{aligned}$$

Using this, and after simplifying by m^4, the inequation (10) transforms into

$$X_1^{\frac{1}{12}(2\tau+1)} X_2^{\frac{1}{24}(4\tau+3)} X_3^{\frac{1}{24}(4\tau+3)} X_4^{\frac{1}{24}(6\tau^2+8\tau+3)} < W^{\frac{1}{12}(2\tau+1)}.$$

Substituting the values of X_1, X_2, X_3, X_4 from (7) and W from (8), we get

$$\begin{aligned}
\frac{1}{12}(2\tau+1)\beta + \frac{1}{24}(4\tau+3)(\gamma+\delta-1) + \frac{1}{24}(4\tau+3)(\gamma+\delta-1)&\\
+ \frac{1}{24}(6\tau^2+8\tau+3)\left(\frac{1}{2}-2\alpha\right) < \frac{1}{12}(2\tau+1)(2\gamma+\delta),&
\end{aligned}$$

or equivalently,

$$(6-24\alpha)\tau^2 + (8\beta+8\delta-8-32\alpha)\tau + 4\gamma + 4\beta + 8\delta - 9 - 12\alpha < 0.$$

For the optimal value $\tau = \frac{2(1+4\alpha-\beta-\delta)}{3(1-4\alpha)}$, this reduces to

$$-8\delta^2 + (40 - 32\alpha - 16\beta)\delta + 16\alpha^2 - 48\gamma\alpha + 16\beta\alpha + 8\alpha + 28\beta - 35 + 12\gamma - 8\beta^2 < 0,$$

which is valid if

$$\delta < \frac{5}{2} - 2\alpha - \beta - \frac{1}{4}\sqrt{6(1-4\alpha)(5+4\gamma-4\alpha-4\beta)}.$$

Under this condition, we find four polynomials, namely f, f_1, f_2 and f_3 with the root $(d_1 - d_2, k_1, k_2, v)$. Using the resultant technique, we find the solution $(d_1 - d_2, k_1, k_2, v)$. Using v, we compute $p - q = 2^m v$. Since $N = pq$, we get $p^2 - 2^m vp - N = 0$ which leads to the factorization of the RSA modulus $N = pq$. This terminates the proof. □

5.2 Comparison with former attacks

We compare the bound on δ of Theorem 7 with two former bounds, namely the bound obtained by Sarkar and Maitra in [11] and the bound obtained by Sun et al. in [18].

5.2.1 Comparison with the bound of Sarkar and Maitra. In [11], Sarkar and Maitra showed that for $d_1, d_2 < N^\delta$, and $|d_1 - d_2| < N^\beta$, RSA is insecure if $\delta < \frac{5}{8} - \frac{1}{2}\beta$. To compare this with the bound of Theorem 7, we consider $\gamma = 1$ and $\alpha = 0$ in the next result. This corresponds to the situation when $e_1 \approx e_2 \approx N$ and p and d differ in their first LSBs.

Corollary 1. *Let $N = pq$ be an RSA modulus. Let e_1 and e_2 be two public exponents satisfying $e_1 d_1 - k_1\phi(N) = 1$, $e_2 d_2 - k_2\phi(N) = 1$. Suppose that $d_1, d_2 \leq N^\delta$ and $|d_1 - d_2| < N^\beta$. Then one can factor N in polynomial time if*

$$\delta < \frac{5}{2} - \beta - \frac{1}{4}\sqrt{6(9-4\beta)}.$$

Proof. This is a direct application of Theorem 7 with $\gamma = 1$ and $\alpha = 0$. □

In Table 1, we compare the bound $\delta < \frac{5}{8} - \frac{1}{2}\beta$. of Sarkar and Maitra and the bound of Corollary 1 for various values of $\beta = \log_N(|d_1 - d_2|)$.

$\beta = \log_N(\lvert d_1 - d_2\rvert)$	$\beta = 0.6$	$\beta = 0.5$	$\beta = 0.4$	$\beta = 0.3$	$\beta = 0.25$
Bound for δ in [11]	0.325	0.375	0.425	0.475	0.5
Bound for δ in Corollary 1	0.326	0.379	0.434	0.489	0.517

Table 1. Comparison of the new method with the method of [11].

One may note that when d_1 and d_2 differ in their first MSBs, then $\beta = \delta$ and the bound of Sarkar and Maitra is valid if $\delta < \frac{5}{12} \approx 0.416$, while the bound of Corollary 1 gives $\delta < 0.422$.

5.2.2 Comparison with the bound in Sun et al.

In [18], Sun et al. showed that RSA is insecure when $e = N^{\gamma}$, $p - q = 2^m v$ with $2^m = N^{\alpha}$, and $d < N^{\delta}$, if $\delta < \frac{7}{6} - \frac{2}{3}\alpha - \frac{1}{3}\sqrt{(1-4\alpha)(1-4\alpha+6\gamma)}$. To compare our method with the method of Sun et al., we consider Theorem 7 with $\beta = \delta$, that is when d_1 and d_2 do not share any amount of their MSBs. We get the following corollary.

Corollary 2. *Let $N = pq$ be an RSA modulus such that $p - q = 2^m u$ where $2^m \approx N^{\alpha}$. Let e_1 and e_2 be two public exponents satisfying $e_1, e_2 \approx N^{\gamma}$, and $e_1 d_1 - k_1\phi(N) = 1$, $e_2 d_2 - k_2\phi(N) = 1$. Suppose that $d_1, d_2 \leq N^{\delta}$. Then one can factor N in polynomial time if*

$$\delta < \frac{17}{16} - \frac{1}{4}\alpha - \frac{1}{16}\sqrt{3(1-4\alpha)(3+32\gamma-12\alpha)}.$$

Proof. In the bound of δ in Theorem 7, if we plug $\beta = \delta$ and solve the inequation for δ, we get the desired bound on δ. □

In Table 2, we compare the largest values of δ of Corollary 2 and the the largest values obtained in [18] for various values of $\gamma = \log_N(e)$ and $\alpha = \log_N(2^m)$.

$\gamma = \log_N(e)$	$\gamma = 1$	$\gamma = 0.9$	$\gamma = 0.8$	$\gamma = 0.7$	$\gamma = 0.6$
Bound for δ in [18] with $\alpha = 0$	0.284	0.323	0.363	0.406	0.451
New bound for δ with $\alpha = 0$	0.422	0.452	0.483	0.516	0.552
Bound for δ in [18] with $\alpha = 0.1$	0.436	0.467	0.500	0.534	0.570
New bound for δ with $\alpha = 0.1$	0.550	0.573	0.598	0.625	0.653
Bound for δ in [18] with $\alpha = 0.2$	0.662	0.680	0.699	0.720	0.742
New bound for δ with $\alpha = 0.2$	0.736	0.750	0.764	0.780	0.797
Bound for δ in [18] with $\alpha = 0.25$	1	1	1	1	1
New bound for δ with $\alpha = 0.25$	1	1	1	1	1

Table 2. Comparisons of the new method with the method of [18] for $\alpha = \log_N(2^m)$.

6 Conclusion

For $k \geq 2$ and $i = 1, \ldots, k$, let (N_i, e_i) be k RSA instances with k moduli $N_i = p_i q_i$ and k public exponents e_i. In this paper, we proposed a new method to factor all the RSA moduli $N_1, \ldots, N_k$ in the scenario that the RSA instances satisfy k equations of the shape $e_i x - y_i\phi(N_i) = z_i$ or of the shape $e_i x_i - y\phi(N_i) = z_i$ with suitably small parameters x_i, y_i, z_i, x, y where $\phi(N_i) = (p_i - 1)(q_i - 1)$. We also proposed an attack on RSA when the prime factors p and q of the RSA modulus $N = pq$ are of the same bit-size. The attack factors N when p and q share a number of their least significant bits (LSBs) in the presence of two public exponents e_1 and e_2 with decryption exponents d_1 and d_2 sharing an amount of their most significant bits (MSBs).

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.: A generalized Wiener attack on RSA. In Public Key Cryptography - PKC 2004, volume 2947 of Lecture Notes in Computer Science, 1–13. Springer-Verlag (2004)
3. 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, 1–11 (1999)
4. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), 233–260 (1997)
5. Hastad, J.: On using RSA with low exponent in a public key network, in Proceedings of CRYPTO'85, Springer-Verlag, 403–408 (1986)
6. Hinek, J.: On the Security of Some Variants of RSA, Phd. Thesis, Waterloo, Ontario, Canada (2007)
7. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited, In Cryptography and Coding, LNCS 1355, 131–142, Springer-Verlag (1997)
8. Howgrave-Graham, N., Seifert, J.-P.: Extending Wieners attack in the presence of many decrypting exponents. In Secure Networking- CQRE (Secure)'99, LNCS 1740, 153–166, Springer-Verlag (1999)
9. Jochemsz, E., May, A.: A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants, in: ASIACRYPT 2006, LNCS 4284, 2006, 267-282, Springer-Verlag (2006)
10. Lenstra, A.K. , Lenstra, H.W., L. Lovász, L.: Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, 513–534, (1982)
11. Sarkar, S., Maitra, S.: Cryptanalysis of RSA with two decryption exponents, Information Processing Letters, Vol. 110, 178–181, (2010)
12. May, A.: New RSA Vulnerabilities Using Lattice Reduction Methods. Ph.D. thesis, University of Paderborn (2003)
13. Nitaj, A.: Another generalization of Wiener's attack on RSA, In: Vaudenay, S. (ed.) Africacrypt 2008. LNCS, vol. 5023, 174–190. Springer, Heidelberg (2008)
14. Rivest, R., Shamir, A., Adleman, L.: A Method for Obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol. 21 (2), 120–126 (1978)
15. Steinfeld, R., Zheng, Y.: On the Security of RSA with Primes Sharing Least-Significant Bits. Appl. Algebra Eng. Commun. Comput. 15(3-4), 179200 (2004)
16. Steinfeld, R., Zheng, Y.: An advantage of Low-Exponent RSA with Modulus Primes Sharing Least Significant Bits. In: Naccache, D. (ed.) CT-RSA 2001. LNCS 2020, Springer, Heidelberg, 52–62 (2001)
17. Steinfeld, R., Zheng, Y.: On the Security of RSA with Primes Sharing Least-Significant Bits. Appl. Algebra Eng. Commun. Comput. 15(3-4), 179–200 (2004)
18. Sun, H.M, Mu-EnWu, Steinfeld, R., Guo, J., Wang, H.: Cryptanalysis of Short Exponent RSA with Primes Sharing Least Significant Bits. M.K. Franklin, L.C.K. Hui, D.S. Wong (Eds.): CANS 2008, LNCS 5339, 49–63 (2008)
19. Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, 553–558 (1990)
20. Zhao, Y.-D., Qi, W.-F.: Small private-exponent attack on RSA with primes sharing bits. In: Garay, J., et al. (eds.) ISC 2007. LNCS 4779, Springer, Heidelberg, 221–229 (2007)

A Proof of Theorem 4

Proof. Let $\varepsilon \in (0,1)$. Set

$$C = \left\lceil 3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1} \right\rceil, \tag{11}$$

where $\lceil x \rceil$ is the integer greater than or equal to x. Consider the lattice $\mathcal{L}$ spanned by the rows of the matrix

$$M = \begin{bmatrix} 1 & -[C\alpha_1] & -[C\alpha_2] & \cdots & -[C\alpha_n] \\ 0 & C & 0 & \cdots & 0 \\ 0 & 0 & C & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & C \end{bmatrix},$$

where $[x]$ is the nearest integer to x. The determinant of $\mathcal{L}$ is $\det(\mathcal{L}) = C^n$ and the dimension is $n+1$. Applying the LLL algorithm, we find a reduced basis $(b_1, \cdots, b_{n+1})$ with

$$\|b_1\| \leq 2^{n/4} \det(\mathcal{L})^{1/(n+1)} = 2^{n/4} C^{n/(n+1)}.$$

Since $b_1 \in \mathcal{L}$, we can write $b_1 = \pm[q, p_1, p_2, \ldots, p_n]M$, that is

$$b_1 = \pm \left[q, Cp_1 - q\left[C\alpha_1\right], Cp_2 - q\left[C\alpha_2\right], \cdots, Cp_n - q\left[C\alpha_n\right]\right], \tag{12}$$

where $q > 0$. Hence, the norm of b_1 satisfies

$$\|b_1\| = \left(q^2 + \sum_{i=1}^{n} \left|Cp_i - q\left[C\alpha_i\right]\right|^2\right)^{1/2} \leq 2^{n/4} C^{n/(n+1)},$$

which leads to

$$q \leq \left\lfloor 2^{n/4} C^{n/(n+1)} \right\rfloor \quad \text{and} \quad \max_i \left|Cp_i - q\left[C\alpha_i\right]\right| \leq 2^{n/4} C^{n/(n+1)}. \tag{13}$$

Let us consider the entries $q\alpha_i - p_i$. We have

$$\begin{aligned} |q\alpha_i - p_i| &= \frac{1}{C} \left|Cq\alpha_i - Cp_i\right| \\ &\leq \frac{1}{C} \left(|Cq\alpha_i - q[C\alpha_i]| + |q[C\alpha_i] - Cp_i|\right) \\ &= \frac{1}{C} \left(q|C\alpha_i - [C\alpha_i]| + |q[C\alpha_i] - Cp_i|\right) \\ &\leq \frac{1}{C} \left(\frac{1}{2}q + |q[C\alpha_i] - Cp_i|\right). \end{aligned}$$

Using the two inequalities in (13), we get

$$|q\alpha_i - p_i| \leq \frac{1}{C} \left(\frac{1}{2} \cdot 2^{n/4} C^{n/(n+1)} + 2^{n/4} C^{n/(n+1)}\right) = \frac{3 \cdot 2^{(n-4)/4}}{C^{1/(n+1)}}$$

Observe that (11) gives

$$3^{n+1}\cdot 2^{\frac{(n+1)(n-4)}{4}}\cdot\varepsilon^{-n-1} \le C \le\le 3^{n+1}\cdot 2^{\frac{(n+1)(n-3)}{4}}\varepsilon^{-n-1}, \tag{14}$$

which leads to $\varepsilon \ge \frac{3\cdot 2^{(n-4)/4}}{C^{1/(n+1)}}$. As a consequence, we get $|q\alpha_i - p_i| \le \varepsilon$. On the other hand, using (13) and (14) , we get

$$q \le \left\lfloor 2^{n/4}C^{n/(n+1)}\right\rfloor \le 2^{n/4}C^{n/(n+1)} \le 2^{n(n-3)/4}\cdot 3^n\cdot\varepsilon^{-n}.$$

To compute the vector $[q, p_1, p_2, \ldots, p_n]$, we use (12)

$$[q, p_1, p_2, \ldots, p_n] = \pm\left[q, Cp_1 - q\left[C\alpha_1\right], Cp_2 - q\left[C\alpha_2\right], \cdots, Cp_n - q\left[C\alpha_n\right]\right]M^{-1}.$$

This terminates the proof. □

B Proof of Lemma 1

Proof. Suppose that $p - q = 2^m u$. Then $p = q + 2^m u$ and $N = q^2 + 2^m uq$. Hence $q^2 \equiv N \pmod{2^m}$. Let u_0 be a solution of the congruence $x^2 \equiv N \pmod{2^m}$. For $m \le 2$, this equation has only one solution and for $m \ge 3$, there are four solutions that can be found in polynomial time using Hensel's Lemma. Then $q \equiv u_0 \pmod{2^m}$ for one of the solutions u_0 which implies that $q = 2^m q_1 + u_0$ for a positive integer q_1. Now, we have

$$p = q + 2^m u = 2^m q_1 + u_0 + 2^m u = 2^m(q_1 + u) + u_0 = 2^m p_1 + u_0,$$

where $p_1 = q_1 + u$. Using $N = pq$, we get

$$N = \left(2^m p_1 + u_0\right)\left(2^m q_1 + u_0\right) = 2^{2m} p_1 q_1 + 2^m u_0(p_1 + q_1) + u_0^2.$$

From this, we deduce $2^m u_0(p_1 + q_1) + u_0^2 \equiv N \pmod{2^{2m}}$. Since u_0 is odd, we obtain

$$2^m(p_1 + q_1) \equiv \left(N - u_0^2\right)u_0^{-1} \pmod{2^{2m}},$$

which can be rewritten as $2^m(p_1 + q_1) = 2^{2m}v + t_0$ with

$$t_0 \equiv \left(N - u_0^2\right)u_0^{-1} \pmod{2^{2m}}.$$

Finally, we get

$$\begin{aligned} p + q &= 2^m p_1 + u_0 + 2^m q_1 + u_0 \\ &= 2^m(p_1 + q_1) + 2u_0 \\ &= 2^{2m}v + t_0 + 2u_0 \\ &= 2^{2m}v + v_0, \end{aligned}$$

where $v_0 = t_0 + 2u_0$. This terminates the proof. □

C Proof of Lemma 2

Proof. Suppose that $S > 2N^{\frac{1}{2}}$ and let $D = \sqrt{S^2 - 4N}$. We have

$$\left|(p-q)^2 - D^2\right| = \left|(p-q)^2 - S^2 + 4N\right| = \left|(p+q)^2 - S^2\right|.$$

Dividing by $p - q + D$, we get

$$|p - q - D| = \frac{(p+q+S)|p+q-S|}{p-q+D}$$

Next, suppose $|p + q - S| < \frac{p-q}{3(p+q)}N^{\frac{1}{4}}$. Since $\frac{p-q}{3(p+q)}N^{\frac{1}{4}} < N^{\frac{1}{4}}$, then

$$p + q + S < 2(p+q) + N^{\frac{1}{4}} < 3(p+q).$$

Combining with $p - q + D > p - q$, we deduce

$$|p - q - D| < \frac{3(p+q)|p+q-S|}{p-q} < \frac{3(p+q)}{p-q} \cdot \frac{p-q}{3(p+q)}N^{\frac{1}{4}} = N^{\frac{1}{4}}.$$

Now, set $\tilde{P} = \frac{1}{2}(S + D)$. We have

$$\begin{aligned}
\left|p - \tilde{P}\right| &= \left|p - \frac{1}{2}(S+D)\right| \\
&= \frac{1}{2}|p + q - S + p - q - D| \\
&\leq \frac{1}{2} \cdot |p + q - S| + \frac{1}{2}|p - q - D| \\
&< \frac{1}{2} \cdot \frac{p-q}{3(p+q)}N^{\frac{1}{4}} + \frac{1}{2}N^{\frac{1}{4}} \\
&< N^{\frac{1}{4}},
\end{aligned}$$

where we used $\frac{1}{2} \cdot \frac{p-q}{3(p+q)} < \frac{1}{2}$. This terminates the proof. □