A Unified Method for Private Exponent Attacks on RSA using Lattices

Hatem M Bahig, Dieaa I Nassr, Ashraf Bhery, Abderrahmane Nitaj

A Unified Method for Private Exponent Attacks on RSA using Lattices

Hatem M. Bahig[1], Dieaa I. Nassr[1], Ashraf Bhery[1], and Abderrahmane Nitaj[2]

[1] Computer Science Division, Department of Mathematics,
Faculty of Science, Ain Shams University, Cairo 11566, Egypt
h.m.bahig@gmail.com (hmbahig@sci.asu.edu.eg)
diaa.rsa@gmail.com bhery_as@yahoo.com
[2] Laboratoire de Mathématiques Nicolas Oresme
Université de Caen, Basse Normandie, France
abderrahmane.nitaj@unicaen.fr

Abstract. Let $(n = pq, e = n^{\beta})$ be an RSA public key with private exponent $d = n^{\delta}$, where p and q are large primes of the same bit size. At Eurocrypt 96, Coppersmith presented a polynomial-time algorithm for finding small roots of univariate modular equations based on lattice reduction and then succussed to factorize the RSA modulus. Since then, a series of attacks on the key equation $ed - k\phi(n) = 1$ of RSA have been presented. In this paper, we show that many of such attacks can be unified in a single attack using a new notion called *Coppersmith's interval*. We determine a Coppersmith's interval for a given RSA public key (n, e). The interval is valid for any variant of RSA, such as Multi-Prime RSA, that uses the key equation. Then we show that RSA is insecure if $\delta < \beta + \frac{1}{3}\alpha - \frac{1}{3}\sqrt{12\alpha\beta + 4\alpha^2}$ provided that we have approximation $p_0 \geq \sqrt{n}$ of p with $|p - p_0| \leq \frac{1}{2}n^{\alpha}$, $\alpha \leq \frac{1}{2}$. The attack is an extension of Coppersmith's result.

Keywords: Coppersmith's method; Cryptanalysis; LLL algorithm; lattice basis reduction; Multi-Prime RSA; private exponent attack; RSA

Key words: RSA; Multi-Prime RSA; Cryptanalysis; LLL algorithm; lattice basis reduction; Coppersmith's method; private exponent attack.

1 Introduction

The RSA cryptosystem invented by [13], is the most popular and widely used cryptosystem in the world. It can be used for encryption without the need to exchange a secret key separately.

In RSA, the modulus $n = pq$ is a product of two large primes p, q of the same bit-size with $p > q$. The public exponent e and the private exponent d satisfy $ed \equiv 1$

$(\mathrm{mod}\ \phi(n))$ where $\phi(n) = (p-1)(q-1)$ is Euler's totient function. The security of RSA is based mainly on factoring the modulus n. To encrypt a message $m \in \mathbf{Z}_n^\star$ one computes $c \equiv m^e \pmod{n}$ using the public key (n, e). To recover the message m, one computes $c^d \pmod{n}$. The main drawback of RSA is its efficiency, in particular for some devices with limited computing power such as smart cards. The RSA encryption and decryption take time $O((\log e)(\log n)^2)$ and $O((\log d)(\log n)^2)$ respectively. Many ways have been considered when implementing RSA to speed up the time of decryption (similarly, signature-generation). For example, one might be tempted to use small private exponents to speed up the decryption/signing process. Unfortunately, [20] showed that RSA is insecure if $d < \frac{1}{3}n^{\frac{1}{4}}$. Wiener's attack is based on searching d among the denominators of the convergents of the continued fraction expansion of $\frac{e}{n}$. The bound was improved to $d < n^{0.292}$ by [2]. Their attack is based on the method of [3] for finding small solutions of modular polynomial equations, which in turn uses the LLL lattice reduction algorithm by [9]. Therefore, people have been looking for vulnerabilities of RSA using Coppersmith's method. Although none of these attacks totally break RSA, they show in which cases it is insecure.

The starting point of the most known attacks on RSA is the study of the key modular equation $ed \equiv 1 \pmod{\phi(n)}$ and its linear form $ed - k\phi(n) = 1$ in addition to some extra information on the size of the private exponent d or the prime factors p, q of the modulus $n = pq$. Wiener [20] tried to solve the key equation $ed - k\phi(n) = 1$ by transforming it into an inequality of the form $\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{1}{2d^2}$, which can be efficiently solved by the continued fraction algorithm when $d < \frac{1}{3}n^{\frac{1}{4}}$. Note that the attack of Wiener takes advantage of the approximation $\phi(n) \approx n$. In a different approach, Boneh and Durfee [2] transformed the equation $ed - k\phi(n) = 1$ using $\phi(n) = n+1-p-q$ and considered the modular equation $k\left(\frac{n+1}{2} - \frac{p+q}{2}\right) + 1 \equiv 0 \pmod{e}$. Then they applied the method of [3] to find the small solutions of the polynomial equation $f(x, y) = 0 \pmod{e}$ where $f(x, y) = x(\frac{n+1}{2} + y) + 1$. In [19], de Weger studied the situation when the prime difference $|p - q| = n^\theta$ is small. Following the method of Boneh and Durfee, de Weger showed that RSA is unsafe if $\delta < \frac{1}{6}(4\theta+5) - \frac{1}{3}\sqrt{(4\theta+5)(4\theta-1)}$. Observe that when the prime factors p, q of the RSA modulus $n = pq$ are of the same bit size, then one can assume, without loss of generality, that $q < p < 2q$. This easily leads to the inequalities $\frac{\sqrt{2}}{2}\sqrt{n} < q < \sqrt{n} < p < \sqrt{2}\sqrt{n}$. It follows that when $|p - q|$ is small, then p and q are close to $\sqrt{n}$ and, consequently, $\phi(n) \approx n + 1 - 2\sqrt{n}$. This was an advantage for the attack of de Weger. Similarly, if the prime difference $|2q - p|$ is small, then one can show that $q \approx \frac{\sqrt{2}}{2}\sqrt{n}$ and $p \approx \sqrt{2}\sqrt{n}$. This shows that $\phi(n) \approx n + 1 - \frac{3\sqrt{3}}{2}\sqrt{n}$ and this was an advantage for the attack of [10]. Indeed, in case of $e \approx n$, $d < n^\delta$ and $|2q - p| < n^\gamma$, they showed that RSA is insecure if $\delta < \frac{1}{6}(4\gamma+5) - \frac{1}{3}\sqrt{(4\gamma+5)(4\gamma-1)}$. Sometimes, one can get more important results if we assume that the private exponent d or the prime factors p, q are of special forms.

These attacks are called partial key exposure attacks. Sun et al. [17] considered the situation when the prime factors share an amount of their least significant bits. Namely, if $p - q = 2^u z$ for some known u, then $p + q = 2^{2u}v + 2v_0$ where

$$v_0 \equiv p_0 + \frac{\left(n - p_0^2\right) p_0^{-1}}{2} \pmod{2^{2u}},$$

and p_0 is a solution of the congruence $x^2 \equiv n \pmod{2^u}$. Then, using the key equation $ed - k\phi(n) = 1$ with $\phi(n) = n + 1 - 2v_0 - 2^{2u}v$ and taking $e = n^\beta$, $2^u = n^\gamma$ and $d < n^\delta$, Sun et al. showed that RSA is insecure whenever $\delta < \frac{7}{6} - \frac{2}{3}\gamma - \frac{1}{3}\sqrt{-24\beta\gamma + 16\gamma^2 + 6\beta - 8\gamma + 1}$.

Our Contributions. In this paper, we unify most of the attacks on RSA that are based on applying Coppersmith's technique for solving modular polynomial equations derived from the equation $ed - k\phi(n) = 1$. We introduce the notion of *Coppersmith's intervals*. Let n be an RSA modulus and e, d be public and private exponents respectively, satisfying $ed - k\phi(n) = 1$. We said that the interval I is a *Coppersmith's interval* for the public key (n, e) if for every positive integer $m \in I$, the solution (d, k) of the equation $ed - k\phi(n) = 1$ can be found by applying Coppersmith's method to a modular polynomial equation involving a polynomial $f_m(x, y)$ derived from the key equation $ed - k\phi(n) = 1$. Then we show that for $e = n^\beta, d = n^\delta$, the interval $I = [\phi(n) - n^\alpha, \phi(n) + n^\alpha]$ is a Coppersmith's interval for (n, e) if

$$\delta < \beta + \frac{1}{3}\alpha - \frac{1}{3}\sqrt{12\alpha\beta + 4\alpha^2}.$$

This interval is also Coppersmith's interval for any variant of RSA that uses the equation $ed - k\phi(n) = 1$. Then we use the obtained Coppersmith's interval to show that some former attacks on RSA can be reformulated using Coppersmith's interval. This includes attacks of [2], [19] and [10] as well as [17]. We also use the obtained Coppersmith's interval to factor an RSA modulus $n = pq$ when an approximation p_0 of p is given. Finally, we show that the obtained Coppersmith's interval can be applied to multi-prime RSA to extend the attack of [19].

We note that the notion of Coppersmith's interval is equivalent to finding a lower bound $\phi(n) - n^\alpha$ and an upper bound $\phi(n) + n^\alpha$ for $\phi(n)$ so that Coppersmith's method will succeed in solving the modular polynomial equation $xy + mx + 1 \equiv 0 \pmod{e}$ for any m lying between the two bounds.

This paper is organized as follows. In Section 2, we present some well known facts and method that will be used through the paper. In Section 3, we define Coppersmith's interval for a given RSA public key (n, e). Then we determine Coppersmith's interval for (n, e). In Section 4, we present our application of Coppersmith's interval to attack RSA. This includes that (1) how one can obtain some former attacks on RSA (e.g. [2], [19] and [10]) from Coppersmith's interval; (2) a revised version of Copper-

smith attack on RSA; and (3) an extension of the attack of [19] on RSA to multi-prime RSA. We conclude in Section 6.

2 Preliminaries

Throughout the paper, the values n^{α}, n^{β}, n^{δ}, n^{γ}, n^{θ} represent positive integers.
In this section, we present a few basic facts about lattice basis reduction. Also, we mention some useful facts and results related to the prime factors of an RSA modulus $n = pq$.

2.1 Lattice

Let $u_1, \ldots, u_\omega \in \mathbf{Z}^n$ be ω linearly independent vectors with $\omega \leq n$. A lattice $\mathcal{L}$ spanned by $(u_1, \ldots, u_\omega)$ is the set of all integer linear combinations of $u_1, \ldots, u_\omega$, that is

$$\mathcal{L} = \left\{ \sum_{i=1}^{\omega} a_i u_i \mid a_i \in \mathbf{Z} \right\}.$$

The set $(u_1, \ldots, u_\omega)$ is called the basis of the lattice $\mathcal{L}$. Let $(u_1^*, \ldots, u_\omega^*)$ be the result of applying Gram-Schmidt orthogonalization to the basis vectors. Then the determinant of $\mathcal{L}$ is defined as

$$\det(\mathcal{L}) = \prod_{i=1}^{\omega} \|u_i^*\|,$$

where $\|v\|$ denotes the Euclidean norm of the vector v. If $\omega = n$, then $\mathcal{L}$ is a full rank lattice and the determinant of $\mathcal{L}$ is equal to the absolute value of the determinant of a lattice basis matrix. The well known LLL algorithm, due to [9] has proved to be a very efficient lattice reduction algorithm and very useful in cryptanalysis. The LLL algorithm outputs an approximation of a shortest lattice vector in time polynomial in ω and $\max_i \|u_i\|$. Next we show the result of the output of the LLL algorithm (see [11]).

Theorem 1. *[11] Let $\mathcal{L}$ be a lattice spanned by a basis $(u_1, \ldots, u_\omega)$. The LLL algorithm produces a basis $(b_1, \ldots, b_\omega)$ of $\mathcal{L}$ satisfying*

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

Using the LLL algorithm, [3] presented an algorithm that allows to efficiently and rigourously compute small integer roots of bivariate polynomials and small modular roots of univariate polynomials. The two techniques are based on the same idea: using the univariate or the bivariate polynomial to create a lattice, applying lattice reduction to find a second polynomial that has the same root as the first one, and then solving it over the integers. Later, [7] and [8] revisited the idea of Coppersmith and proposed

alternative simplifications.
The strategy of [8] is a technique that allows to find a lattice with good properties. Using an initial polynomial $f(x_1, \ldots, x_n)$, the technique creates m new polynomials $f_i(x_1, \ldots, x_n)$, $i = 1, \ldots, m$, such that the coefficients of these polynomials form a triangular matrix with easy properties for lattice reduction.

Coppersmith's method has been adapted to various multivariate modular polynomial equations under the following assumption.

Assumption 2. *[8], [8] Let $f_1, \ldots, f_n \in \mathbb{Z}[x_1, \ldots, x_n]$ be the polynomials that are found by applying Coppersmith's method. The resultant computations for the polynomials $f_1, \ldots, f_n$ yield non-zero polynomials. Equivalently, the ideal generated by the polynomial equations $f_1(x_1, \ldots, x_n) = 0, \ldots, f_n(x_1, \ldots, x_n) = 0$ has dimension zero.*

The following theorem is due to [7] where it is used to derive conditions under which the polynomial $f(x, y) \in Z[x, y]$ with the modular solution $f(x_0, y_0) \equiv 0 \pmod{e^u}$ has the same root over integer, that is $f(x_0, y_0) = 0$. The theorem uses the Euclidean norm of a bivariate polynomial $f(x, y) = \sum a_{i_1,i_2} x^{i_1} y^{i_2}$ which is defined as

$$\|f(x, y)\| = \sqrt{\sum a_{i_1,i_2}^2}.$$

Theorem 3. *[7] Let $f(x, y) \in \mathbf{Z}[x, y]$ be a polynomial which is a sum of at most ω monomials. Let e, u, X and Y be positive integers. Suppose that*

$$f(x_0, y_0) \equiv 0 \pmod{e^u}, \text{ where } |x_0| < X, |y_0| < Y,$$
$$\|f(xX, yY)\| < \frac{e^u}{\sqrt{\omega}}.$$

Then $f(x_0, y_0) = 0$ holds over the integers.

In the following theorem, it has been shown a general case in which the small inverse problem can be solved. The small inverse problem is to find small integers x and y satisfying $x(A + y) \equiv 1 \pmod{B}$ for two large integers A and B.

Theorem 4. *[18] Given two large integers A and B, let (x_0, y_0) be a solution of $x(A + y) \equiv 1 \pmod{B}$ with $|x_0| < B^u$ and $|y_0| < B^v$ for some $0 < u, v < 1$. Then (x_0, y_0) can be obtained in polynomial time when*

$$u < 1 - \sqrt{v} \qquad \text{for } \frac{1}{4} \leq v < 1,$$
$$u < 1 - \frac{2}{3}(\sqrt{(3 + 4v)v} - v) \qquad \text{for } 0 < v < \frac{1}{4}$$

2.2 Useful lemmas

We terminate this section by some useful results related to the prime factors of an RSA modulus $n = pq$.

Lemma 1. *[12], [19] Let $n = pq$ be an RSA modulus such that $q < p < 2q$. Then*

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

$$0 < p - q < \frac{\sqrt{2}}{2}\sqrt{n}, \tag{2}$$

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

Lemma 2. *[19] Let $n = pq$ be an RSA modulus such that $q < p < 2q$. Then*

$$0 < p + q - 2\sqrt{n} < \frac{(p-q)^2}{4\sqrt{n}}.$$

Proposition 1. *[10] Let l be a positive integer. If $q > \frac{2l+2}{4l+1}p$, then*

$$\left|\frac{3}{\sqrt{2}}\sqrt{n} - (p+q)\right| < \frac{l(2q-p)^2}{(\frac{3}{\sqrt{2}}+2)\sqrt{n}}.$$

The following lemma showed that if p, q share m bits of their least significant bits, then these sharing bits and $2m$ least significant bits of $p + q$ can be computed in polynomial time.

Lemma 3. *[14] Let $n = pq$ be an RSA modulus with $q < p < 2q$. Suppose that $p - q = 2^u z$ for a known value u. Then $p = 2^u p_1 + p_0$ and $q = 2^u q_1 + p_0$ where p_0 is a solution of the equation $x^2 \equiv n \pmod{2^u}$ and $p + q = 2^{2u}v + 2v_0$ with*

$$v_0 \equiv p_0 + \frac{\left(n - p_0^2\right) p_0^{-1}}{2} \pmod{2^{2u}}.$$

3 The Lattice Result

In this section we introduce the notion of Coppersmith's interval for a given public-key RSA (n, e). It is based on Coppersmith's method. In literature [3,11,8,5,22], the term Coppersmith's method is used to refer to lattice basis reduction techniques for finding small roots of polynomials modulo an integer n with unknown factorization.

3.1 Definitions

We start this section by giving definition of Coppersmith's root and Coppersmith's interval. Then we determine a Coppersmith's interval for a given public-key RSA (n, e) related the to key equation equation $ed - k\phi(n) = 1$. We start with the following definition in regards of a bivariate polynomial.

Definition 1. *(**Coppersmith's root**) Let x_0, y_0 be two integers. The tuple (x_0, y_0) is a Coppersmith's root of the polynomial $f(x, y) \in \mathbf{Z}[x, y]$ modulo an integer e if $f(x_0, y_0) \equiv 0 \pmod{e}$, where (x_0, y_0) can be computed in polynomial time using Coppersmith's method.*

Let (n, e) be an RSA public key satisfying the equation $ed - k\phi(n) = 1$. Then $k\phi(n) + 1 \equiv 0 \pmod{e}$. Let m be an integer. Then $k(\phi(n) - m) + mk + 1 \equiv 0 \pmod{e}$ This can be rewritten as $xy+mx+1 \equiv 0 \pmod{e}$ with $x = k, y = \phi(n)-m$. This leads to a bivariate polynomial $f(x, y) = xy + mx + 1 \in \mathbf{Z}[x, y]$.

Definition 2. *(**Coppersmith's interval**) Let (n, e) be an RSA public key with private exponent d satisfying $ed = 1+k\phi(n)$. An interval I is said to be a Coppersmith's interval for (n, e) if for every integer $m \in I$, $(x_0, y_0) = (k, \phi(n) - m)$ is a Coppersmith's root of the polynomial $f(x, y) = xy + mx + 1$ modulo e.*

3.2 Explicit Coppersmith's interval

Now we determine a Coppersmith's interval for an RSA public-key (n, e). It is natural to determine a Coppersmith's interval in terms of $\phi(n)$ since most small private exponent attacks on RSA try to find a good approximation of $\phi(n)$ in order to solve the key equation $ed - k\phi(n) = 1$. We note that the following result relies on the widely used and accepted Assumption 2 in order to extract the final solutions efficiently. We present in Subsection 3.3 various experimental results to verify the correctness of the attack in practice.

Theorem 5. *Let $(n, e = n^\beta)$ be an RSA public key with private exponent $d = n^\delta$. Then*

$$I = [\phi(n) - n^\alpha, \phi(n) + n^\alpha] \tag{4}$$

is a Coppersmith's interval for (n, e), where

$$\delta < \beta + \frac{1}{3}\alpha - \frac{1}{3}\sqrt{12\alpha\beta + 4\alpha^2}. \tag{5}$$

Proof. Suppose that $\phi(n) \neq m \in I$. Then $|\phi(n) - m| < n^\alpha$. Since $ed = k\phi(n) + 1$, then $k\phi(n) + 1 \equiv 0 \pmod{e}$. This can be rewritten as $k(\phi(n) - m) + km + 1 \equiv 0$

$(\mathrm{mod}\ e)$. Consider the polynomial $f(x,y) = xy + mx + 1$. Then $f(x,y)$ has root $(x_0, y_0) = (k, \phi(n) - m)$ modulo e. Observe that

$$x_0 = k < d = n^{\delta}, \qquad y_0 = |\phi(n) - m| < n^{\alpha}.$$

Hence, if δ and α are suitably small, then using Coppersmith's method we can find $(k, \phi(n) - m)$ among the small roots of the polynomial $f(x,y)$ modulo e. The main target of the proof is to show that (x_0, y_0) is also a root of some polynomial $g(x,y)$ over integers and that polynomial can be constructed form $f(x,y)$ by using Jochemsz-May strategy for small modular roots (see [8]). Define the bounds X and Y as

$$X = n^{\delta}, Y = n^{\alpha}.$$

Let u and r be positive integers to be specified later. For $0 \le t \le u$, define

$$M_t = \bigcup_{0 \le j \le r} \{x^{i_1} y^{i_2+j} : \quad x^{i_1} y^{i_2} \text{ monomial of } f^u(x,y) \\ \frac{x^{i_1} y^{i_2}}{(xy)^t} \text{ monomial of } f^{u-t}(x,y)\}.$$

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

$$\begin{aligned} f^u(x,y) &= (x(y+m)+1)^u \\ &= \sum_{i_1=0}^{u} \binom{u}{i_1} x^{i_1} (y+m)^{i_1} \\ &= \sum_{i_1=0}^{u} \binom{u}{i_1} x^{i_1} \left(\sum_{i_2=0}^{i_1} \binom{i_1}{i_2} y^{i_2} m^{i_1-i_2} \right) \\ &= \sum_{i_1=0}^{u} \sum_{i_2=0}^{i_1} \binom{u}{i_1} x^{i_1} \left(\binom{i_1}{i_2} y^{i_2} m^{i_1-i_2} \right) \end{aligned}$$

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

$$i_1 = 0, \ldots, u \text{ and } i_2 = 0, \ldots i_1.$$

Consequently, $x^{i_1} y^{i_2}$ is a monomial of $f^{u-t}(x,y)$ if

$$i_1 = 0, \ldots, u - t \text{ and } i_2 = 0, \ldots i_1.$$

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

$$i_1 = t, \ldots, u \text{ and } i_2 = t, \ldots i_1.$$

Hence, for $0 \le t \le u$, we obtain

$$x^{i_1} y^{i_2} \in M_t \text{ if } i_1 = t, \ldots, u \text{ and } i_2 = t, \ldots i_1 + r.$$

Similarly,

$$x^{i_1}y^{i_2} \in M_{t+1} \text{ if } i_1 = t+1, \ldots, u \text{ and } i_2 = t+1, \ldots i_1 + r.$$

Note that, for $0 \leq t \leq u$, we find that $x^{i_1}y^{i_2} \in M_t \setminus M_{t+1}$ if and only if

$$\{i_1 = t, \ldots, u \text{ with } i_2 = t\} \text{ or}$$

$$\{i_1 = t \text{ with } i_2 = t+1, \ldots, i_1 + r\}.$$

For $0 \leq t \leq u$, define the polynomials

$$g_{t,i_1,i_2}(x,y) = \frac{x^{i_1}y^{i_2}}{(xy)^t} f^t(x,y)e^{u-t} \text{ with } x^{i_1}y^{i_2} \in M_t \setminus M_{t+1}.$$

For $i_1 = t, \ldots, u$ and $i_2 = t$, the polynomials $g_{t,i_1,i_2}(x,y)$ reduce to

$$g_{t,i_1,t}(x,y) = G_{t,i_1}(x,y) = x^{i_1-t}f^t(x,y)e^{u-t} \text{ for } i_1 = t, \ldots, u$$

For $i_1 = t$ and $i_2 = t+1, \ldots, t+r$ the polynomials $g_{t,i_1,i_2}(x,y)$ reduce to

$$\begin{aligned} g_{t,t,i_2}(x,y) &= H_{t,i_2}(x,y) \\ &= y^{i_2-t}f^t(x,y)e^{u-t} \text{ for } i_2 = t+1, \ldots, t+r. \end{aligned}$$

Let L be the lattice spanned by the coefficient vectors of the polynomials $G_{t,i_1}(xX, yY)$ and $H_{t,i_2}(xX, yY)$. The ordering of the monomials is such that the matrix M is triangular. It is as follows: 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 $x^{i_1}y^{i_2} < x^{i_1'}y^{i_2'}$. From the triangular form of the matrix, the determinant of L is

$$\det(L) = e^{a_e}X^{a_X}Y^{a_Y}. \tag{6}$$

From the construction of the polynomials $G_{t,i_1}(xX, yY)$ and $H_{t,i_2}(xX, yY)$ we get

$$\begin{aligned} a_e &= \sum_{t=0}^{u}\sum_{i_1=t}^{u}(u-t) + \sum_{t=0}^{u}\sum_{i_2=t+1}^{t+r}(u-t) \\ &= \frac{1}{6}u(u+1)(2u+3r+4) \end{aligned}$$

Similarly, we have

$$a_X = \sum_{t=0}^{u}\sum_{i_1=t}^{u} i_1 + \sum_{t=0}^{u}\sum_{i_2=t+1}^{t+r} t = \frac{1}{6}u(u+1)(2u+3r+4)$$

and

$$\begin{aligned} a_Y &= \sum_{t=0}^{u}\sum_{i_1=t}^{u} t + \sum_{t=0}^{u}\sum_{i_2=t+1}^{t+r} i_2 \\ &= \frac{1}{6}(u+1)(u^2+3ur+3r^2+2u+3r). \end{aligned}$$

The dimension of L is calculated as

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

Let $r = u\tau$. Then

$$a_e = \frac{1}{6}u(u+1)(2u+3u\tau+4) = \frac{1}{6}(2+3\tau)u^3 + o(u^3)$$

similarly, we have

$$a_X = \frac{1}{6}u(u+1)(2u+3u\tau+4) = \frac{1}{6}(2+3\tau)u^3 + o(u^3)$$

and

$$\begin{aligned} a_Y &= \frac{1}{6}(u+1)(u^2+3u^2\tau+3u^2\tau^2+2u+3u\tau) \\ &= \frac{1}{6}(1+3\tau+3\tau^2)u^3 + o(u^3). \end{aligned}$$

Also,

$$\begin{aligned} \omega = \frac{1}{2}(u+1)(u+2r+2) &= \frac{1}{2}(u+1)(u+2u\tau+2) \\ &= \frac{1}{2}(1+2\tau)u^2 + o(u^2). \end{aligned}$$

To solve the original multivariate equation $xy + mx + 1 \equiv 0 \pmod{e}$, we need two algebraically independent integer polynomial equations $f_1(x,y) = 0$ and $f_2(x,y) = 0$. These two polynomial equations can be found by reducing the lattice basis of L using the LLL algorithm and by assuming Assumption 2. Indeed, by applying the LLL algorithm to the lattice L, the two shortest vectors in the reduced basis satisfy Theorem 1 with $i = 2$, that is

$$\|f_1(x,y)\| \leq \|f_2(x,y)\| \leq 2^{\frac{\omega}{4}} \det(\mathcal{L})^{\frac{1}{\omega-1}}.$$

To apply Howgrave-Graham's Theorem 3 to the two shortest vectors in the LLL-reduced basis of L, we have to set

$$2^{\frac{\omega}{4}} \det(L)^{\frac{1}{\omega-1}} < \frac{e^u}{\sqrt{\omega}}.$$

This transforms to

$$\det(L) < \frac{1}{2^{\frac{\omega}{4}}\sqrt{\omega}} e^{u(\omega-1)}.$$

By Neglecting $2^{\frac{\omega}{4}}$ and $\sqrt{\omega}$, we get

$$\det(L) < e^{u\omega}.$$

Using Eq. (6), we get

$$e^{a_e} X^{a_X} Y^{a_Y} < e^{u\omega}.$$

Since $e = n^\beta$, $X = n^\delta$, and $Y = n^\alpha$. Then

$$n^{\beta a_e} n^{\delta a_X} n^{\alpha a_Y} < n^{u\beta\omega}.$$

Taking logarithms, we get $\beta a_e + \delta a_X + \alpha a_Y < u\beta\omega$. Plugging the values of a_e, a_X, a_Y and ω, we get

$$\frac{1}{6}(2+3\tau)\beta + \frac{1}{6}(2+3\tau)\delta + \frac{\alpha}{6}(1+3\tau+3\tau^2) - \frac{1}{2}(1+2\tau)\beta < 0. \tag{7}$$

The optimal value for τ in the left side is $\tau = \frac{\beta-\delta-\alpha}{2\alpha}$, which leads to

$$\frac{1}{6}\alpha\beta - \frac{\alpha^2}{6} - \frac{\alpha}{3}(\beta-\delta-\alpha) - \frac{1}{8}(\beta-\delta-\alpha)^2 < 0.$$

Solving for δ, we get

$$\delta < \beta + \frac{1}{3}\alpha - \frac{1}{3}\sqrt{12\alpha\beta + 4\alpha^2}.$$

This terminates the proof.

Remark 1.

1. There is no condition on the prime factors of n. Thus, I is also Coppersmith's interval for any variant of RSA that uses the relation $ed \equiv 1 \pmod{\phi(n)}$.
2. The Coppersmith interval in Theorem 5 is neither a unique nor a maximal Coppersmith's interval. For example, we can use Herrman-May [15] linearization technique to show that the interval

   $$I' = [\phi(n) - n^\gamma, \phi(n) + n^\gamma]$$

   is another Coppersmith's interval when

   $$\delta < \beta - \sqrt{\beta\gamma}. \tag{8}$$

   Suppose that we have a monomial $u = xy + 1$. The polynomial $f(x, y) = xy + mx + 1$ modulo e can be rewritten in terms of the monomial u as a linear polynomial $\bar{f}(u, x) = u + mx$ with $xy = u - 1$.
   Define,

   $$\bar{g}_{i,k}(u, x) = x^i \bar{f}^k e^{s-k} \text{ for } k = 0, 1, \ldots, s \text{ and } i = 0, 1, \ldots, s - k,$$

and for a positive integer $t \leq s$ (to be specified latter),

$$\bar{h}_{j,k}(u,x,y) = y^j \bar{f}^k e^{s-k} \text{ for } j = 1,2,\ldots,t \text{ and } k = \lfloor \frac{s}{t} \rfloor j, \ldots, s.$$

Let $X = n^\delta$, $Y = n^\gamma$, $U = N^{\delta+\gamma}$ and let L be the lattices spanned by the coefficient vectors of the polynomials $\bar{g}_{i,k}(uU, xX)$ and $\bar{h}_{j,k}(uU, xX, yY)$. The ordering of the monomials is such that the matrix M is triangular. The monomial is either in the form $x^{i_1}u^{i'_1}$ (of order $x^{i_1+i'_1}y^{i'_1}$) or in the form $y^{i_2}u^{i'_2}$ (of order $x^{i'_2}y^{i_2+i'_2}$). The monomial of order $x^i y^j$ precedes the monomials of order $x^{i'}y^{j'}$ when either $i < i'$ or $i = i'$ and $j < j'$. In Herrmann-May [15], it has been shown that, from the triangular form of the matrix, the determinant of L is

$$det(L) = X^{s_x} Y^{s_y} U^{s_u} e^{s_e},$$

where

$$\begin{aligned}
s_x &= \sum_{k=0}^{s} \sum_{i=0}^{s-k} i = \frac{1}{6}s^3 + o(s^3),\\
s_y &= \sum_{j=1}^{\tau s} \sum_{k=\frac{1}{\tau}j}^{s} j = \frac{\tau^2}{6}s^3 + o(s^3),\\
s_u &= \sum_{k=0}^{s} \sum_{i=0}^{s-k} k + \sum_{j=1}^{\tau s} \sum_{k=\frac{1}{\tau}j}^{s} k = (\frac{1}{6} + \frac{\tau}{3})s^3 + o(s^3),\\
s_e &= \sum_{k=0}^{s} \sum_{i=0}^{s-k} (s-k) + \sum_{j=1}^{\tau s} \sum_{k=\frac{1}{\tau}j}^{s} (s-k) = (\frac{1}{3} + \frac{\tau}{6})s^3 + o(s^3),\\
dim(L) &= \sum_{k=0}^{s} \sum_{i=0}^{s-k} 1 + \sum_{j=1}^{\tau s} \sum_{k=\frac{1}{\tau}j}^{s} 1 = (\frac{1}{2} + \frac{\tau}{2})s^2 + o(s^2).
\end{aligned}$$

By applying Howgrave-Graham's theorem (Theorem 3) to the two shortest vectors in the reduced basis hat satisfy Theorem 1 with $i = 2$, we obrain

$$det(L) = X^{s_x} Y^{s_y} U^{s_u} e^{s_e} < e^{s \dim(L)}.$$

Using $e = n^\beta$, $X = n^\delta$, and $Y = n^\alpha$, this is verified if

$$\frac{\delta}{6} + \frac{\tau^2\alpha}{6} + \left(\frac{1}{6} + \frac{\tau}{3}\right)(\alpha + \delta) + \left(\frac{1}{3} + \frac{\tau}{6}\right)\beta - \left(\frac{1}{2} + \frac{\tau}{2}\right)\beta < 0.$$

The optimized value for τ is $\tau = \frac{\beta-\delta-\alpha}{\alpha}$. Plugging this value, we get

$$\alpha\beta - \beta^2 + 2\beta\delta - \delta^2 < 0,$$

which is satisfied for

$$\delta < \beta - \sqrt{\beta\alpha}.$$

3. Also, the interval
$$I' = [\phi(n) - n^{\alpha'}, \phi(n) + n^{\alpha'}],$$
is another Coppersmith's interval when
$$\delta < \beta - \sqrt{\beta\alpha'} \text{ for } \frac{\beta}{4} \leq \alpha' < \beta,$$
$$\delta < \beta - \frac{2}{3}(\sqrt{(3\beta + 4\alpha')\alpha'} - \alpha') \text{ for } 0 < \alpha' < \frac{\beta}{4}.$$
This is because of the following: The equation $ed = 1 + k\phi(n)$ can be rewritten as $ed = 1 + k(m + \phi(n) - m)$ where $m \in I'$. Since $|k| < d = n^{\delta} = e^{\delta/\beta}$ and $|\phi(n) - m| < n^{\alpha'} = e^{\alpha'/\beta}$, obtaining k and $\phi(n) - m$ is a small inverse problem in which the two known large integers are m and e, i.e., $(-k, \phi(n) - m)$ is a root of the modular equation $x(m + y) \equiv 1 \pmod{e}$. According to Theorem 4, this modular equation is solvable when
$$\frac{\delta}{\beta} < 1 - \sqrt{\frac{\alpha'}{\beta}} \text{ for } \frac{1}{4} \leq \frac{\alpha'}{\beta} < 1,$$
$$\frac{\delta}{\beta} < 1 - \frac{2}{3}\left(\sqrt{\left(3 + 4\frac{\alpha'}{\beta}\right)\frac{\alpha'}{\beta}} - \frac{\alpha'}{\beta}\right)$$
$$\text{for } 0 < \frac{\alpha'}{\beta} < \frac{1}{4}.$$
Therefore, the interval $[\phi(n) - n^{\alpha'}, \phi(n) + n^{\alpha'}]$ is another Coppersmith's interval when
$$\delta < \beta - \sqrt{\beta\alpha'} \text{ for } \frac{\beta}{4} \leq \alpha' < \beta$$
$$\delta < \beta - \frac{2}{3}(\sqrt{(3\beta + 4\alpha')\alpha'} - \alpha') \text{ for } 0 < \alpha' < \frac{\beta}{4}.$$
This leads to an interesting question what is the maximal Coppersmith's interval.

3.3 Experimental results

We experimented the attack on 1000 RSA instances with moduli $n = pq$, $e = n^{\beta}$, $d = n^{\delta}$ and $m \in [\phi(n) - n^{\alpha}, \phi(n) + n^{\alpha}]$ for various values of α and β. In all cases, Assumption 2 was verified and we were able to find the small solution $(x_0, y_0) = (k, \phi(n) - m)$ of the equation $f(x, y) = xy + mx + 1 \equiv 0 \pmod{e}$ for any m in the Coppersmith interval $I = [\phi(n) - n^{\alpha}, \phi(n) + n^{\alpha}]$ where $x_0 = k < d = n^{\delta}$, $y_0 = |\phi(n) - m| < n^{\alpha}$, with the condition $\delta < \beta + \frac{1}{3}\alpha - \frac{1}{3}\sqrt{12\alpha\beta + 4\alpha^2}$. In Table 1, we present the bounds for δ for various values of β and α.

α	0.50	0.50	0.45	0.45	0.40	0.40	0.35	0.35
β	0.987	0.990	0.998	0.975	0.984	0.973	0.995	0.992
δ	0.276	0.278	0.318	0.303	0.345	0.338	0.391	0.390
lattice parameters	$u=5$, $r=1$, $\dim=27$	$u=5$, $r=1$, $\dim=27$	$u=4$, $r=1$, $\dim=20$	$u=5$, $r=1$, $\dim=27$	$u=4$, $r=1$, $\dim=20$	$u=4$, $r=1$, $\dim=20$	$u=3$, $r=1$, $\dim=14$	$u=3$, $r=1$, $\dim=14$

Table 1. Bounds for δ in terms of α, β and the lattice dimension.

4 Cryptanalysis of RSA using Coppersmith's interval

In this section, we give an application of Coppersmith's interval to attack the RSA cryptosystem. We show that four well-known and important attacks on RSA can be derived from Theorem 5. We also present a new attack related to Theorem 5. Then we show that the result of [19] on RSA can be extended to Multi-prime RSA using Coppersmith's interval.

4.1 Application to former attacks

We show that the attack of [2] and its improvements by [19] and [10] as well as the attack presented by [17] can be obtained from Theorem 5

Corollary 1. ***[Boneh-Durfee]*** *Let (n, e) be an RSA public key with a full size public exponent e and a private exponent $d = n^{\delta}, \delta < 0.284$ where n is a product of two large primes p and q such that $q < p < 2q$. Then $n \in I$ (as in Eq. (4)).*

Proof. Using Eq. (3), we have

$$0 < n - \phi(n) = p + q - 1 < \frac{3\sqrt{2}}{2}\sqrt{n}.$$

It follows that

$$n - \phi(n) = \frac{3\sqrt{2}}{2}n^{\alpha}, \text{ with } \alpha = \frac{1}{2}.$$

Suppose that $e = n^{\beta}$. If

$$\delta < \beta + \frac{1}{6} - \frac{1}{3}\sqrt{6\beta + 1},$$

then by Theorem 5, $n \in I$ (as in Eq. (4)) and we can factor $n = pq$. For the particular case where e is full size, that is $\beta \approx 1$, the bound of d is

$$\delta < \frac{7}{6} - \frac{\sqrt{7}}{3} \approx 0.284.$$

This is precisely the first result of [2].

However, if $\delta < 0.292$, then $n \in I$ (as in Eq. (8)) by taking $\gamma = \alpha = 1/2$.

Corollary 2. ***[de Weger]*** *Let (n, e) be an RSA public key with a full size public exponent e and a private exponent $d = n^\delta$, where n is a product of two primes p and q such that $q < p < 2q$ and $p - q = n^\theta$, $\frac{1}{4} < \theta < \frac{1}{2}$. If*

$$\delta < \frac{1}{6}(4\theta + 5) - \frac{1}{3}\sqrt{(4\theta + 5)(4\theta - 1)},$$

then $\lfloor n + 1 - 2\sqrt{n} \rfloor \in I$ (as in Eq. (4)).

Proof. Using Eq. (2), we have $p - q = n^\theta$, with $\theta < \frac{1}{2}$. Note that, if $\theta \leq \frac{1}{4}$, then using Fermat's method, it is possible to compute p and q which breaks the RSA system (see [19] and [12]). In the following, we restrict θ such that $\frac{1}{4} < \theta < \frac{1}{2}$. Let $m = \lfloor n + 1 - 2\sqrt{n} \rfloor$. Then $0 < m - \phi(n) \leq n + 1 - 2\sqrt{n} - \phi(n) = p + q - 2\sqrt{n}$. Using Lemma 2, we get

$$0 < m - \phi(n) < \frac{(p - q)^2}{4\sqrt{n}} = \frac{1}{4}n^{2\theta - \frac{1}{2}}.$$

If $m = \lfloor n + 1 - 2\sqrt{n} \rfloor$, then

$$m - \phi(n) < \frac{1}{4}n^\alpha \quad \text{with} \quad \alpha = 2\theta - \frac{1}{2}.$$

Since e is full size public key, then $e = n^\beta$ with $\beta \approx 1$. Replacing α by $2\theta - \frac{1}{2}$ and by taking $\beta = 1$ in Eq. (5), we get

$$\begin{aligned} \delta &< 1 + \tfrac{1}{3}(2\theta - \tfrac{1}{2}) - \tfrac{1}{3}\sqrt{12(2\theta - \tfrac{1}{2}) + 4(2\theta - \tfrac{1}{2})^2} \\ &= \tfrac{1}{6}(4\theta + 5) - \tfrac{1}{3}\sqrt{16\theta^2 + 16\theta - 5} \\ &= \tfrac{1}{6}(4\theta + 5) - \tfrac{1}{3}\sqrt{(4\theta + 5)(4\theta - 1)}. \end{aligned}$$

Then according to Theorem 5, $\lfloor n + 1 - 2\sqrt{n} \rfloor \in I$ (as in Eq. (4)). Moreover, this matches the bound found in [19].

Corollary 3. ***[Maitra-Sarkar]*** *Let (n, e) be an RSA public key with a full size public exponent e and a private exponent $d = n^\delta$, where n is a product of two primes p and q such that $q < p < 2q$ and $2q - p = n^\gamma$ with $\gamma \leq \frac{1}{2}$. Suppose that l is a positive integer such that $q > \frac{2l+2}{4l+1}p$. If*

$$\delta < \frac{1}{6}(4\gamma + 5) - \frac{1}{3}\sqrt{(4\gamma + 5)(4\gamma - 1)},$$

then $\left\lceil n + 1 - \frac{3\sqrt{2}}{2}\sqrt{n} \right\rceil \in I$ (as in Eq. (4)).

Proof. Let $m = \left\lceil n + 1 - \frac{3}{\sqrt{2}}\sqrt{n} \right\rceil$. Then

$$\begin{aligned} 0 < \phi(n) - \left\lceil n + 1 - \frac{3\sqrt{2}}{2}\sqrt{n} \right\rceil & \\ \leq \phi(n) - \left(n + 1 - \frac{3\sqrt{2}}{2}\sqrt{n} \right) & \\ = \frac{3\sqrt{2}}{2}\sqrt{n} - (p+q). & \end{aligned}$$

If $q > \frac{2l+2}{4l+1}p$ for a positive integer l, then, using Proposition 1, we get

$$0 < \frac{3\sqrt{2}}{2}\sqrt{n} - (p+q) < \frac{l(2q-p)^2}{\left(\frac{3\sqrt{2}}{2}+2\right)\sqrt{n}} < \frac{l}{\frac{3\sqrt{2}}{2}+2} n^{2\gamma-\frac{1}{2}}.$$

It follows that if $m = \lceil n + 1 - \frac{3}{\sqrt{2}}\sqrt{n} \rceil$, then

$$\phi(n) - m < \frac{l}{\frac{3\sqrt{2}}{2}+2} n^{\alpha} \quad \text{with} \quad \alpha = 2\gamma - \frac{1}{2}.$$

Since e is full size public key, then $e = n^{\beta}$ with $\beta \approx 1$. Replacing α by $2\gamma - \frac{1}{2}$ and by taking $\beta = 1$ in Eq. (5), we get

$$\begin{aligned} \delta < 1 + \tfrac{1}{3}(2\gamma - \tfrac{1}{2}) - \tfrac{1}{3}\sqrt{12(2\gamma - \tfrac{1}{2}) + 4\left(2\gamma - \tfrac{1}{2}\right)^2} & \\ = \tfrac{1}{6}(4\gamma + 5) - \tfrac{1}{3}\sqrt{16\gamma^2 + 16\gamma - 5} & \\ = \tfrac{1}{6}(4\gamma + 5) - \tfrac{1}{3}\sqrt{(4\gamma+5)(4\gamma-1)}. & \end{aligned}$$

Then according to Theorem 5, $\lceil n + 1 - \frac{3}{\sqrt{2}}\sqrt{n} \rceil \in I$ (as in Eq. (4)). We note that the bound on δ is the same as the bound found in [10].

Corollary 4. ***[Sun et al.]*** *Let (n, e) be an RSA public key with a public exponent $e = n^{\beta}$ and a private exponent $d = n^{\delta}$, where n is the product of two primes p and q such that $q < p < 2q$ and $p - q = 2^u z$ for some known u with $2^u = n^{\gamma}$. If*

$$\delta < \frac{7}{6} - \frac{2}{3}\gamma - \frac{1}{3}\sqrt{-24\beta\gamma + 16\gamma^2 + 6\beta - 8\gamma + 1}.$$

then $n + 1 - 2v_0 \in I$ (as in Eq. (4)) where

$$v_0 \equiv p_0 + \frac{\left(n - p_0^2\right) p_0^{-1}}{2} \pmod{2^{2u}},$$

and p_0 is a solution of the congruence $x^2 \equiv n \pmod{2^u}$.

Proof. Suppose that $p - q = 2^u z$ for a known value u with $2^u = n^\gamma$. Then $p + q = 2^{2u}v + 2v_0$ where v_0 is computed as mentioned in Lemma 3. Hence $\phi(n) = n + 1 - (p + q) = n + 1 - 2v_0 - 2^{2u}v$. Define $m = n + 1 - 2v_0$. Hence $|\phi(n) - m| = 2^{2u}v$. Using Eq. (3), we get

$$v < \frac{p+q}{2^{2u}} < \frac{3\sqrt{2}}{2} n^{\frac{1}{2}-2\gamma}.$$

On the other hand, since $ed - k\phi(n) = 1$, then

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

Hence, the equation $ed - k\phi(n) = 1$ with $\phi(n) = n + 1 - 2v_0 - 2^{2u}v$ transforms into $k\left(\phi(n) - (n + 1 - 2v_0)\right) + k(n + 1 - 2v_0) + 1 \equiv 0 \pmod{e}$, or equivalently

$$-2^{2u}kv + k(n + 1 - 2v_0) + 1 \equiv 0 \pmod{e},$$

which gives rise to the polynomial $g(x, y) = 2^{2u}xy + x(n + 1 - 2v_0) + 1$ with the root $(x_0, y_0) = (k, -v)$ satisfying the bounds

$$|x_0| < X = 2n^{\beta+\delta-1}, \quad |y_0| < Y = \frac{3\sqrt{2}}{2} n^{\frac{1}{2}-2\gamma}.$$

Replacing δ by $\beta + \delta - 1$ and α by $\frac{1}{2} - 2\gamma$ in Eq. (7), we get

$$\frac{1}{12}(-12\gamma + 3)\tau^2 + \frac{1}{12}(6\delta - 12\gamma - 3)\tau + \frac{1}{6}\beta + \frac{1}{3}\delta - \frac{1}{3}\gamma - \frac{1}{4} < 0$$

The left hand side is minimized at $\tau_0 = \frac{1+4\gamma-2\delta}{2(1-4\gamma)}$, which leads to

$$-12\delta^2 + (28 - 16\gamma)\delta - 32\beta\gamma + 16\gamma^2 + 8\beta + 8\gamma - 15 < 0.$$

Solving for δ, we get

$$\delta < \frac{7}{6} - \frac{2}{3}\gamma - \frac{1}{3}\sqrt{-24\beta\gamma + 16\gamma^2 + 6\beta - 8\gamma + 1}.$$

Notice that this can be written as

$$\delta < \frac{2}{3}\left(\frac{1}{2} - \gamma\right) + \frac{5}{6} - \frac{4}{3}\sqrt{\left(\frac{1}{2} - \gamma\right)^2 + \left(\frac{3}{2}\beta - \frac{1}{2}\right)\left(\frac{1}{2} - \gamma\right) - \frac{6\beta - 1}{16}}.$$

This is the same bound found by [17].

4.2 Revising Coppersmith's Result

In the following theorem, we study the factorization of n when we know an approximation p_0 of p with $|p - p_0| \leq \frac{1}{2}n^\alpha$, $\alpha \leq \frac{1}{2}$. We show that the RSA is insecure if $\delta < \beta + \frac{1}{3}\alpha - \frac{1}{3}\sqrt{12\alpha\beta + 4\alpha^2}$ where $e = n^\beta$, $d = n^\delta$.

Theorem 6. *Let (n, e) be an RSA public key with a public exponent $e = n^\beta$ and a private exponent $d = n^\delta$, where n is the product of two large primes p and q such that $q < p < 2q$. Let $p_0 \geq \sqrt{n}$ be an approximation for p with $|p - p_0| \leq \frac{1}{2}n^\alpha$ where $\alpha \leq \frac{1}{2}$. If $\delta < \beta + \frac{1}{3}\alpha - \frac{1}{3}\sqrt{12\alpha\beta + 4\alpha^2}$, then $[n+1-\lambda_1, n+1-\lambda_2]$ is a Coppersmith's interval for (n, e), where*

$$(\lambda_1, \lambda_2) = \begin{cases} (p_0 \quad + \frac{n}{p_0} + \frac{1}{2}n^\alpha, p_0 + \frac{n}{p_0 + \frac{1}{2}n^\alpha}), \\ \quad \textit{if } p_0 \leq p; \\ \\ (p_0 \quad + \frac{n}{p_0 - \frac{1}{2}n^\alpha}, \frac{n}{p_0} + p_0 - \frac{1}{2}n^\alpha), \\ \quad \textit{if } p \leq p_0 \textit{ and } \sqrt{n} \leq p_0 - \frac{1}{2}n^\alpha, \\ \\ (2\sqrt{n} + \frac{1}{2}n^\alpha, \sqrt{n} + \frac{n}{\sqrt{n} + \frac{1}{2}n^\alpha}), \\ \quad \textit{if } p \leq p_0 \textit{ and } p_0 - \frac{1}{2}n^\alpha < \sqrt{n}. \end{cases}$$

Proof. Suppose that p_0 is an approximation for p such that $|p - p_0| \leq \frac{1}{2}n^\alpha$. Our strategy is to apply Theorem 5 by showing that there exists an interval $[n + 1 - \lambda_1, n + 1 - \lambda_2]$ that is a Coppersmith's interval for (n, e). More precisely, we show that λ_1 and λ_2 are such that $[n + 1 - \lambda_1, n + 1 - \lambda_2] \subseteq [\phi(n) - n^\alpha, \phi(n) + n^\alpha]$ where $\delta < \beta + \frac{1}{3}\alpha - \frac{1}{3}\sqrt{12\alpha\beta + 4\alpha^2}$ as it is required for applying Theorem 5. Since $[n + 1 - \lambda_1, n + 1 - \lambda_2] = [\phi(n) - (\lambda_1 - p - q), \phi(n) + (p + q - \lambda_2)]$, it is sufficient to show that

$$0 \leq \lambda_1 - p - q \leq n^\alpha \text{ and } 0 \leq p + q - \lambda_2 \leq n^\alpha. \tag{9}$$

The proof is divided into three cases according to $p_0 \leq p$ or $p \leq p_0$.
Case 1: Suppose that $p_0 \leq p$. Then $|p - p_0| \leq \frac{1}{2}n^\alpha$ and $q = \frac{n}{p}$, we get

$$p_0 \leq p \leq p_0 + \frac{1}{2}n^\alpha,$$
$$\frac{n}{p_0 + \frac{1}{2}n^\alpha} \leq q \leq \frac{n}{p_0}.$$

Define,

$$\lambda_1 = p_0 + \frac{n}{p_0} + \frac{1}{2}n^\alpha, \quad \lambda_2 = p_0 + \frac{n}{p_0 + \frac{1}{2}n^\alpha}.$$

Then, λ_1 and λ_2 satisfy $\lambda_1 \geq p+q$ and $\lambda_2 \leq p+q$. Observe that $p_0 - p \leq 0$ and $\frac{n}{p_0} - q = \frac{q(p-p_0)}{p_0} \leq \frac{1}{2}n^\alpha$. Also,

$$\lambda_1 - p - q = \frac{1}{2}n^\alpha + (p_0 - p) + \left(\frac{n}{p_0} - q\right) \leq n^\alpha.$$

It follows that $0 \leq \lambda_1 - p - q \leq n^\alpha$ which satisfies Eq. (9). On the other hand, observe that $p - p_0 \leq \frac{1}{2}n^\alpha$ and $q \leq \frac{n}{p_0}$. Then

$$\begin{aligned} p + q - \lambda_2 &= p + q - p_0 - \frac{n}{p_0 + \frac{1}{2}n^\alpha} \\ &\leq \frac{1}{2}n^\alpha + \frac{n}{p_0} - \frac{n}{p_0 + \frac{1}{2}n^\alpha} \\ &= \frac{1}{2}n^\alpha + \frac{n^{1+\alpha}}{2p_0(p_0 + \frac{1}{2}n^\alpha)} \\ &\leq n^\alpha, \end{aligned}$$

where we used $\frac{n^{1+\alpha}}{2p_0(p_0+\frac{1}{2}n^\alpha)} \leq \frac{1}{2}n^\alpha$ which is valid since $p_0 \geq \sqrt{n}$. Consequently, λ_2 is such that $0 \leq p + q - \lambda_2 \leq n^\alpha$ which satisfies Eq. (9). This proves the first case.
Case 2: Suppose that $p \leq p_0$ and $\sqrt{n} \leq p_0 - \frac{1}{2}n^\alpha$. Then, using $|p - p_0| \leq \frac{1}{2}n^\alpha$ and $q = \frac{n}{p}$, we get

$$\begin{aligned} p_0 - \frac{1}{2}n^\alpha \leq p \leq p_0, \\ \frac{n}{p_0} \leq q \leq \frac{n}{p_0 - \frac{1}{2}n^\alpha}. \end{aligned}$$

Next, define,

$$\lambda_1 = p_0 + \frac{n}{p_0 - \frac{1}{2}n^\alpha}, \quad \lambda_2 = \frac{n}{p_0} + p_0 - \frac{1}{2}n^\alpha.$$

Then, we easily get $\lambda_1 \geq p + q$. Using $p_0 - p \leq \frac{1}{2}n^\alpha$ and $\frac{n}{p_0} \leq q$, we get

$$\begin{aligned} \lambda_1 - p - q &= p_0 + \frac{n}{p_0 - \frac{1}{2}n^\alpha} - p - q \\ &\leq \frac{1}{2}n^\alpha + \frac{n}{p_0 - \frac{1}{2}n^\alpha} - \frac{n}{p_0} \\ &= \frac{1}{2}n^\alpha + \frac{n^{1+\alpha}}{2p_0(p_0 - \frac{1}{2}n^\alpha)} \\ &\leq n^\alpha, \end{aligned}$$

where we used $\frac{n^{1+\alpha}}{2p_0(p_0-\frac{1}{2}n^\alpha)} \leq \frac{1}{2}n^\alpha$ for $p_0 - \frac{1}{2}n^\alpha \geq \sqrt{n}$. This shows that λ_1 satisfies Eq. (9). Similarly, we have $\lambda_2 \leq p+q$ and using $p \leq p_0$ and $q \leq \frac{n}{p_0-\frac{1}{2}n^\alpha}$, we get

$$\begin{aligned} p+q-\lambda_2 &= p+q-\frac{n}{p_0}-p_0+\frac{1}{2}n^\alpha \\ &\leq \frac{n}{p_0-\frac{1}{2}n^\alpha}-\frac{n}{p_0}+\frac{1}{2}n^\alpha \\ &= \frac{n^{1+\alpha}}{2p_0(p_0-\frac{1}{2}n^\alpha)}+\frac{1}{2}n^\alpha \\ &\leq n^\alpha. \end{aligned}$$

It follows that λ_2 also satisfies Eq. (9). This proves the second case.
Case 3: Suppose that $p \leq p_0$ and $p_0 - \frac{1}{2}n^\alpha < \sqrt{n}$. Then $p - \sqrt{n} \leq \frac{1}{2}n^\alpha$, which means that $\sqrt{n}$ is an approximation of p satisfying Case 1. Then, plugging $p_0 = \sqrt{n}$ in Case 1, we get that the interval

$$\left[n+1-(2\sqrt{n}+\frac{1}{2}n^\alpha), n+1-(\sqrt{n}+\frac{n}{\sqrt{n}+\frac{1}{2}n^\alpha})\right],$$

is a Coppersmith's interval for (n,e).

In [16], Sarkar, Maitra and Sarkar presented an attack on RSA when $e \approx n$, $d = n^\delta$, $|p-p_0| < n^\alpha$ and showed that $n = pq$ can be factored if $\delta < 1 + \frac{\alpha}{3} - \frac{2}{3}\sqrt{\alpha(\alpha+3)}$. This can be retrieved by our attack when $\beta = 1$ in the inequality of Theorem 6. Hence, our attack is actually a generalization of the attack of Sarkar et al.
Figure 1 illustrates the difference between our attack and the previous attacks assuming that e has the same size of n and we have an approximation p_0 for p where $|p-p_0| < \frac{1}{2}n^\alpha$, $\alpha < \frac{1}{2}$.

4.3 Extending de Weger's Attack to Multi-Prime RSA

In Multi-prime RSA (MPRSA), the modulus n is the product of $r \geq 3$ primes, that is $n = p_1 \cdots p_r$, where $p_1 < p_2 < \cdots < p_r$. As with RSA, we only consider $\frac{1}{2}n^{1/r} < p_i < 2n^{1/r}$ for $1 \leq i \leq r$. In this case, n is said to be a product of distinct r-balanced primes.

Let $p_r - p_1 = n^\theta$, $\theta < 1/r$. In the case of standard RSA, i.e., $r = 2$, [19] has showed that d can be recovered if $\delta < \frac{1}{6}(4\theta+5) - \frac{1}{3}\sqrt{(4\theta+5)(4\theta-1)}$. In this section, we extend de Weger's result in the case of MPRSA, i.e., $r \geq 3$, we show that d can be recovered if

$$\delta < \beta + \frac{\theta}{3} + \frac{r-2}{3r} - \frac{2}{3}\sqrt{3\beta\theta + \frac{3\beta(r-2)}{r} + \left(\theta + \frac{r-2}{r}\right)^2}.$$

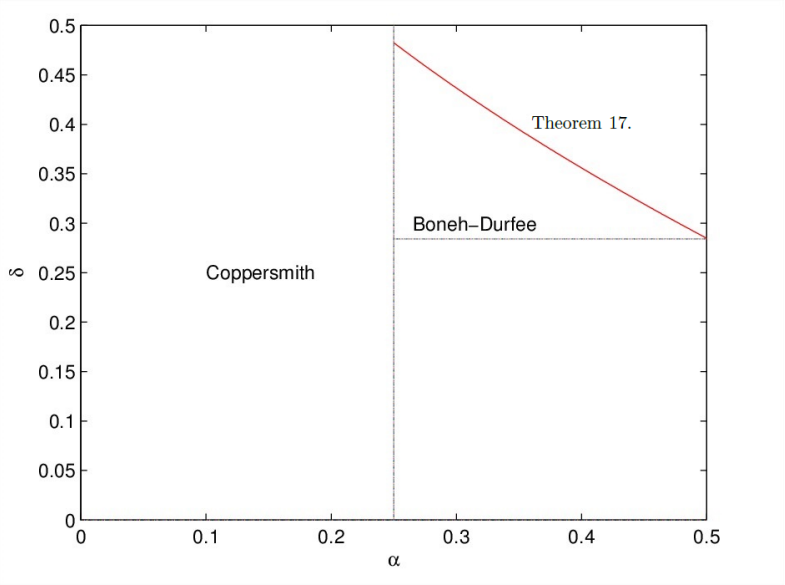

Fig. 1. Comparison between our attack and previous attacks, where δ and α as in Theorem 6.

To find an approximation of $\phi(n)$, define Γ as

$$\Gamma = \sum_{i}^{r} \frac{n}{n^{1/r}} - \sum_{\substack{i,j \\ i<j}}^{r} \frac{n}{n^{2/r}} + \sum_{\substack{i,j,k=1 \\ i<j<k}}^{r} \frac{n}{n^{3/r}} + ... - (-1)^r,$$

following by [1]

$$\begin{aligned} \Lambda &= n - \phi(n) \\ &= \sum_{i}^{r} \frac{n}{p_i} - \sum_{\substack{i,j=1 \\ i<j}}^{r} \frac{n}{p_i p_j} + \sum_{\substack{i,j,k=1 \\ i<j<k}}^{r} \frac{n}{p_i p_j p_k} + ... - (-1)^r. \end{aligned}$$

The relation between Γ and Λ is given in the following proposition.

Proposition 2. *[[1]] Let $n = p_1 p_2 \cdots p_r$ be a product of distinct r-balanced primes and $p_r - p_1 = n^{\theta}, \theta \leq 1/r$. Suppose that k is an integer such that $2 \leq k \leq r$. If $2^k(2^k - 1)\binom{r}{k} \leq \frac{n^{1/r}}{r-1}$, then*

$$|\Lambda - \Gamma| < 3rn^{1+\theta-2/r}.$$

Theorem 7. *Let $n = p_1 p_2 \cdots p_r$ be an MPRSA modulus and a product of distinct $(r \geq 3)$-balanced primes with $p_r - p_1 = n^{\theta}$, $\theta \leq 1/r$. Let $e = n^{\beta}$ be a public*

exponent with a private exponent $d = n^\delta$. Suppose that $2^k(2^k-1)\binom{r}{k} \leq \frac{n^{1/r}}{r-1}$ for every $2 \leq k \leq r$. If

$$\delta < \beta + \frac{\theta}{3} + \frac{r-2}{3r} - \frac{2}{3}\sqrt{3\beta\theta + \frac{3\beta(r-2)}{r} + \left(\theta + \frac{r-2}{r}\right)^2},$$

then d can be recovered.

Proof. By choosing $m = n - \Gamma$, we show that $m \in I$, where I is the Coppersmith's interval given in Theorem 5. Using Proposition 2, we have

$$|m - \phi(n)| = |\Lambda - \Gamma| < 3rn^{1+\theta-2/r}.$$

By neglecting $3r$ and replacing α by $1 + \theta - \frac{2}{r}$ in Eq. (5), we get $m \in I$ if

$$\begin{aligned}\delta &< \beta + \frac{1}{3}\left(1 + \theta - \frac{2}{r}\right) \\ &- \frac{1}{3}\sqrt{12\beta\left(1+\theta-\frac{2}{r}\right) + 4\left(1+\theta-\frac{2}{r}\right)^2} \\ &= \beta + \frac{\theta}{3} + \frac{r-2}{3r} \\ &- \frac{2}{3}\sqrt{3\beta\theta + \frac{3\beta(r-2)}{r} + \left(\theta + \frac{r-2}{r}\right)^2}.\end{aligned}$$

This terminates the proof.

For the particular case when $\theta = 1/r$ and e is full size, i.e., $\beta \approx 1$, the bound of Theorem 7 gives

$$\delta < \frac{1}{3r}(4r - 1 - 2\sqrt{(r-1)(4r-1)}).$$

This is precisely the result of [5].

Remark 2. Suppose for simplicity that $\beta/4 \leq \alpha' < \beta$. As stated in Remark 1, the interval

$$I' = [\phi(n) - n^{\alpha'}, \phi(n) + n^{\alpha'}]$$

with $\delta < \beta - \sqrt{\beta\alpha'}$ is also Coppersmith's interval. Thus, for $\beta/4 + 2/r - 1 \leq \theta < \beta + 2/r - 1$, d in Theorem 7 can be recovered when

$$\delta < \beta - \sqrt{\beta + \beta\theta - 2\beta/r} \tag{10}$$

This is because of the following: using Proposition 2, if we set $m = n - \Gamma$, then $|m - \phi(n)| = |\Lambda - \Gamma| < 3rn^{1+\theta-2/r}$. By neglecting $3r$ and replacing α' by $1+\theta-2/r$,

we get $m \in I'$ in the case of Eq. (10). For a particular case where e is full size, i.e., $\beta \approx 1$, we get $m \in I'$ when

$$\delta < 1 - \sqrt{1 + \theta - 2/r} \text{ for } 2/r - \frac{3}{4} \leq \theta < 2/r$$

This is similar to the result in [21].

In [22], Zhang and Takagi presented an improved attack on Multi-prime RSA with modulus $n = p_1 \dots p_r$ where $p_r - p_1 < n^\theta$ and showed that $d = n^\delta$ can be recovered if $\delta < 1 - \sqrt{1 + 2\theta - \frac{3}{r}}$ under the condition $\frac{3}{2}\left(\frac{1}{r} - \frac{1}{4}\right) \leq \theta < \frac{1}{r}$. We show below that this bound can be retrieved using a Coppersmith's interval. Define $\Gamma' = rn^{\frac{r-1}{r}}$. The method of Zhang and Takagi makes use of the following result.

Proposition 3. *[22] Let $n = p_1 p_2 \cdots p_r$ be a product of distinct r-balanced primes and $p_r - p_1 = n^\theta, \theta \leq 1/r$. Then*

$$|\Lambda - \Gamma'| < 2(r-1)n^{1+2\theta-3/r}.$$

Theorem 8. *Let $n = p_1 p_2 \cdots p_r$ be an MPRSA modulus and a product of distinct $(r \geq 3)$-balanced primes with $p_r - p_1 = n^\theta$, $\theta \leq 1/r$. Let $e = n^\beta$ be a public exponent with a private exponent $d = n^\delta$. If*

$$\begin{aligned}\delta <& \beta + \frac{2\theta}{3} + \frac{r-3}{3r} \\ & - \frac{2}{3}\sqrt{6\beta\theta + \frac{3\beta(r-3)}{r} + \left(2\theta + \frac{r-3}{r}\right)^2},\end{aligned}$$

then d can be recovered.

Proof. By choosing $m = n - \Gamma'$, we show that $m \in I$, where I is the Coppersmith's interval given in Theorem 5. Using Proposition 3, we have

$$|m - \phi(n)| = |\Lambda - \Gamma'| < 2(r-1)n^{1+2\theta-3/r}.$$

By neglecting $2(r-1)$ and replacing α by $1 + 2\theta - \frac{3}{r}$ in Eq. (5), we get $m \in I$ if

$$\begin{aligned}\delta &< \beta + \frac{1}{3}\left(1 + 2\theta - \frac{3}{r}\right) \\ &\quad - \frac{1}{3}\sqrt{12\beta\left(1 + 2\theta - \frac{3}{r}\right) + 4\left(1 + 2\theta - \frac{3}{r}\right)^2} \\ &= \beta + \frac{2\theta}{3} + \frac{r-3}{3r} \\ &\quad - \frac{2}{3}\sqrt{6\beta\theta + \frac{3\beta(r-3)}{r} + \left(2\theta + \frac{r-3}{r}\right)^2}.\end{aligned}$$

This terminates the proof.

Remark 3. Suppose for simplicity that $\beta/4 \leq \alpha' < \beta$. As stated in Remark 1, the interval

$$I' = [\phi(n) - n^{\alpha'}, \phi(n) + n^{\alpha'}]$$

with $\delta < \beta - \sqrt{\beta\alpha'}$ is also a Coppersmith's interval. If we set $m = n - I'$ in Proposition 3, we get $|m-\phi(n)| = |I-I'| < 2(r-1)n^{1+2\theta-3/r}$. Plugging $\alpha' = 1+2\theta-3/r$, in $\delta < \beta - \sqrt{\beta\alpha'}$, we get $\delta < \beta - \sqrt{\beta\left(1+2\theta-\frac{3}{r}\right)}$. Moreover, if e is full size, i.e., $\beta \approx 1$, we get $m \in I'$ if $\frac{3}{2}\left(\frac{1}{r}-\frac{1}{4}\right) \leq \theta < \frac{3}{2r}$ and $\delta < 1 - \sqrt{1+2\theta-\frac{3}{r}}$, which retrieves the result of [22].

5 Conclusion

Based on Coppersmith's method, we have unified several previous private exponent attacks on RSA and Multi-Prime RSA by proposing the notion Coppersmith's interval. We have determined a Coppersmith's interval for RSA modulus n with public exponent $e = n^{\beta}$, and private exponent $d = n^{\delta}$. The obtained interval is valid for any variant of RSA that satisfies $ed \equiv 1 \pmod{\phi(n)}$. We also have extended Coppersmith's result on a factorization.

References

1. H. Bahig, A. Bhery and D. Nassr, Cryptanalysis of multi-prime RSA with small prime difference, Information and Communications Security - 14th International Conference, ICICS 2012, Hong Kong, China, October 29-31, 2012. Proceedings , Lecture Notes in Computer Science 7618, (Springer, 2012), pp. 334
2. D. Boneh, G. Durfee, Cryptanalysis of RSA with private key d less than $N^{0.292}$, IEEE Trans. on Information Theory, Vol. 46(4), pp. 1339–1349, 2000.
3. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), pp. 233–260 (1997)
4. A. Dujella, Continued fractions and RSA with small secret exponent, Tatra Mt. Math. Publ, 29, pp. 101-112, 2004.
5. Hinek, M.J.: Cryptanalysis of RSA and its variants. Chapman & Hall/CRC (2010)
6. Hinek, M.J., Low, M.K., Teske, E.: On Some Attacks on Multi-prime RSA. In: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol. 2595, pp. 385404. Springer, Heidelberg (2003)
7. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited, In Cryptography and Coding, LNCS 1355, pp. 131-142, Springer-Verlag (1997)
8. Jochemsz, E. & May, A. (2006). 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.
9. Lenstra, A.K., Lenstra, H.W., Lovász,L.: Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, pp. 513–534, 1982.

10. S. Maitra, S. Sarkar, Revisiting Wiener's Attack - New Weak Keys in RSA, 11th Information Security Conference September 15-18, 2008, Taipei, Taiwan, Lecture Notes in Computer Science, Springer, pp. 228-243, 2008.
11. A. May, New RSA Vulnerabilities using Lattics Reduction Methods, Ph.D. Dissertation. University of Paderborn. 2003.
12. Nitaj, A.: Another generalization of Wieners attack on RSA, In: Vaudenay, S. (ed.) Africacrypt 2008. LNCS, vol. 5023, pp. 174190. Springer, Heidelberg (2008)
13. R. Rivest, A. Shamir, L. Adleman. A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol. 21 (2), 120-126 (1978).
14. 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)
15. M. Herrmann and A. May, Maximizing small root bounds by linearization and applications to small secret exponent RSA, May 26-28, 2010.
16. S. Sarkar, S. Maitra and S. Sarkar, RSA cryptanalysis with increased bounds on the secret exponent using less lattice dimension, IACR Cryptology ePrint Archive 2008 (2008)
17. Hung-Min Sun, Mu-EnWu, R. Steinfeld, Jian Guo, and Huaxiong Wang: 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, pp. 49–63, 2008.
18. A. Takayasu and N. Kunihiro, General bounds for small inverse problems and its applications to multi-prime RSA, Proc. ICISC 2014, LNCS 8949, pp. 317, Springer, 2014.
19. B. de Weger, Cryptanalysis of RSA with small prime difference, Applicable Algebra in Engineering, Communication and Computing, Vol. 13(1), pp. 17-28, 2002.
20. M. Wiener. Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, 553-558 (1990).
21. H.Zhang, T. Takagi, Attacks on Multi-Prime RSA with Small prime Difference, ACISP 2013. LNCS, vol. 7959, pp. 41-56 Springer, Heidelberg (2013)
22. H. Zhang and T. Takagi, Improved attacks on multi-prime RSA with small prime difference, IEICE Transactions 97-A(7) (2014) pp. 15331541.