Attacking RSA Using an Arbitrary Parameter

Muhammad Rezal Kamel Ariffin[1,2(✉)], Amir Hamzah Abd Ghafar[1], and Muhammad Asyraf Asbullah[1,3]

[1] Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor Darul Ehsan, Malaysia
rezal@upm.edu.my
[2] Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor Darul Ehsan, Malaysia
[3] Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor Darul Ehsan, Malaysia

Abstract. In this paper, we introduce a parameter u that is related to N via an arbitrary relation. By knowing the parameter along with RSA public key pairs, (N, e), we conduct two new attacks on the RSA cryptosystem. The first attack works on the equation $eX - uY = Z - \phi_b$ where ϕ_b is the best known lower bound of $\phi(N)$. It combines the continued fraction method and Coppersmith's method to factor N in polynomial time. The second attack shows that given (N_i, e_i) for $1 \leq i \leq k$ and a fixed X, we can simultaneously factor the k RSA moduli. It manipulates the result from diophantine approximation to enable the conditions of Coppersmith's method. These attacks show that there are more possible weak RSA key pairs.

Keywords: RSA cryptosystem · Cryptanalysis · Coppersmith's method · Diophantine approximation

1 Introduction

The RSA cryptosystem [16] is one of the vital components in transferring data securely over the internet. This cryptosystem is comprised of three main algorithms. Namely, key generation algorithm, encryption algorithm and decryption algorithm. While the details of encryption and decryption algorithms can be viewed in [16], for the key generation algorithm, one must generate two different primes p and q where $q < p < 2p$. The product of the primes, N is known as RSA modulus. Using the value of the modulus, the RSA public exponent,e is chosen such that $e < \phi(N)$ and $\gcd(e, \phi(N)) = 1$ where $\phi(N)$ is Euler's totient function. Then, the corresponding RSA private exponent, d is computed via the RSA key relation,

$$d \equiv e^{-1} \pmod{\phi(N)}. \tag{1}$$

The RSA public key, (N, e) and secret parameters $(p, q, \phi(N), d)$ are said to be the outputs of the algorithm. The security strength of RSA is embedded in

A. Nitaj and A. Youssef (Eds.): AFRICACRYPT 2020, LNCS 12174, pp. 382–399, 2020.
https://doi.org/10.1007/978-3-030-51938-4_19

the difficulty to factor its RSA modulus, $N = pq$ since p and q are n–bit primes where n is typically set to be 1024. The problem to factor N in polynomial time is dubbed the integer factorization problem and the best algorithm to solve it still runs in sub-exponential time [4]. However, previous attacks on RSA showed that a small size of d can compromise the security of RSA [2,10,17]. This type of attack is known as small private exponent attacks and it manipulates the form of (1) by using suitable approximation of $\phi(N)$. This type of attack may generalize by using the following equation.

$$ex - uy = z \tag{2}$$

for suitable integers x, y, z [11–13]. These attacks usually combine the continued fraction method and Coppersmith's method to formulate a new strategy in factoring N.

In this paper, we present two new attacks upon RSA. These new attacks do not depend on the RSA diophantine key equation as previous research did. To initiate the attack, first we define a parameter u that can be computed from the best known upper and lower bounds of $\phi(N)$. However it should be noted that u can be an arbitrary value that is suitably larger than N. Using u, we show an attack upon RSA that works when there exist integers X, Y and Z verifying the equation $eX - uY = Z - \phi_b$ such that

$$1 \leq Y < X < \frac{u}{2\left(\phi(N) - \phi_b\right)}, \quad \phi(N) + \frac{p-q}{p+q}N^{1/4} < N - 2N^{1/2},$$
$$|Z - \phi(N)| < \frac{p-q}{p+q}N^{1/4}$$

where ϕ_b is the best known lower bound of $\phi(N)$. The first attack combines the continued fraction method in [17] and Coppersmith's method in [6] upon the equation $eX - uY = Z - \phi_b$. Note that this equation is not derived from the RSA key equation.

The second attack generalizes the result from the first attack. We assume that the adversary is given k instances of weak RSA moduli $N_i = p_i q_i$ with its corresponding public exponent e_i. We show that if there exist an integer $X < N^{\delta}$ and k integers $Y_i < N^{\delta}$ and $|Z_i - \phi(N_i)| < \frac{p_i - q_i}{p_i + q_i}N^{1/4}$ such that $e_i X - Y_i u_i = Z_i - \phi_b$ for $i = 1, \ldots, k$, and $|Z_i - \phi_{b_i}| < \lambda N^{\delta + \frac{1}{4}}$ where $\lambda < \frac{3}{2}\left(2^{\frac{k+5}{4}} - 3\right)$ then $N_i = p_i q_i$ can be factored in polynomial time.

From these two attacks, we realized there are about $N^{\frac{1}{2}-\epsilon}$ many pairs of (N, e) that are probable candidates of weak keys of RSA. This may expose some of the RSA users into using weak RSA public key pairs, (N, e).

The paper is organized as follows. In Sect. 2, a brief introduction to the continued fractions expansion via Legendre's Theorem, the lattice basis reduction and also simultaneous Diophantine approximation. Section 3 and Sect. 4 presents the first and second attacks, respectively. Section 5 compares our findings against previous findings with respect to their conditions. Then, the conclusion of our work is presented in Sect. 6.

2 Preliminaries

We first show the theorem of continued fractions below:

Theorem 1 (Legendre's theorem). *Let R is a rational number. Let x and y are integers where $y \neq 0$ and $gcd(x, y) = 1$. Suppose*

$$\left| R - \frac{x}{y} \right| < \frac{1}{2y^2}$$

Then $\frac{x}{y}$ is a convergent of the continued fraction expansion of R.

Proof. See [7].

To find the private keys of RSA using the weak RSA public keys (N, e), we use Coppersmith's method [5] to find the integer roots of a univariate or bivariate polynomials modulo N. Particularly, given a large integer N, let

$$F(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0.$$

If there exists $x_0 < N^{1/n}$ such that $F(x_0) \equiv 0 \pmod{N}$, then [5] showed that x_0 can be found in polynomial time with the aid of the LLL algorithm. The LLL algorithm [9] produces a different polynomial f that is related to $F(x)$ that satisfy the conditions imposed for x_0 with smaller values. Due to the smaller values, this method runs in polynomial time. Coppersmith also applied the method in [6] to factor N, given certain approximation of p as shown in the next theorem.

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

Proof. See [6].

In the system of equations of k weak RSA moduli $N_i = p_i q_i$, the next theorem is required for the adversary to find p_i and q_i.

Theorem 3 (Simultaneous Diophantine Approximations). *There is a polynomial time algorithm with respect to $\log(p_i)$ where $i = 1, \ldots, n$, for given rational numbers $\alpha_1, ..., \alpha_n$ and $0 < \epsilon < 1$, to compute integers $p_1, \cdots, p_n$ and a positive integer q such that*

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

Proof. See [15].

3 The First Attack

We first define a parameter u in the following definition.

Definition 1. *Let ϕ_a be the smallest integer value of known upper bound of $\phi(N)$. Let ϕ_b be the largest integer value of known lower bound of $\phi(N)$. Then we define $u = \phi_a + \phi_b$.*

The next remark shows how we can find the best current approximation values for ϕ_a and ϕ_b.

Remark 1. From [14] we know that $2\sqrt{N} < p + q < \frac{3}{\sqrt{2}}\sqrt{N}$. This means $N - \frac{3}{\sqrt{2}}\sqrt{N} + 1 < \phi(N) < N - 2\sqrt{N} + 1$ as $N - (p + q) + 1 = \phi(N)$. Hence the best current approximation for ϕ_a is $\left\lfloor N - 2\sqrt{N} + 1 \right\rfloor$ and the best current approximation for ϕ_b is $\left\lceil N - \frac{3}{\sqrt{2}}\sqrt{N} + 1 \right\rceil$.

It should be noted that u can be an arbitrary value that is suitably larger than N. However, in our case, we use $u = \phi_a + \phi_b$ as in Definition 1. The following lemmas and theorem show the conditions to be fulfilled by parameters in our equation so that its information can be computed in order to find an approximation of p which satisfies Theorem 2.

Lemma 1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose we know an approximation S of $p + q$ such that $S > 2N^{1/2}$, $\sqrt{S^2 - 4N} > p - q$ and*

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

Then $\tilde{P} = \frac{1}{2}\left(S + \sqrt{S^2 - 4N}\right)$ where $|p - \tilde{P}| < N^{1/4}$.

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

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

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

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

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

$$\begin{aligned} p + q + S &< 2(p + q) + N^{1/4} \\ &< 2(p + q) + 2N^{1/4} \\ &= 2(p + q) + \frac{2N^{1/2}}{N^{1/4}} \\ &< 2(p + q) + \frac{p + q}{N^{1/4}} \\ &= \left(2 + \frac{1}{N^{1/4}}\right)(p + q) \end{aligned}$$

as $2N^{1/2} < (p+q)$. Let $\sqrt{S^2-4N} > p-q$, then combining with $p-q+D > p-q+(p-q) = 2(p-q)$, we deduce

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

as $\frac{1}{2N^{1/4}}$ tends to be negligible for large N. Now, set $\tilde{P} = \frac{1}{2}(S+D)$. Finally we can have

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

as $\frac{(p-q)}{(p+q)} < 1$. This terminates the proof.

Lemma 2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let e satisfy the equation $eX - uY = Z - \phi_b$ where X, Y are positive integers with $\gcd(X,Y) = 1$. If $1 \leq Y < X < \left|\frac{u}{2(\phi(N)-\phi_b)}\right|$ and $|Z-\phi(N)| < \frac{p-q}{p+q} N^{1/4}$ then $\frac{Y}{X}$ is a convergent of $\frac{e}{u} - \frac{N^{1/4}}{2u}$.*

Proof. Consider the equation

$$eX - uY = Z - \phi_b \tag{3}$$

Let $|Z - \phi(N)| < \frac{p-q}{p+q} N^{1/4}$. Then divide (3) by uX we get

$$\begin{aligned} \frac{e}{u} - \frac{Y}{X} &= \frac{Z - \phi_b}{uX} \\ &\leq \frac{\frac{p-q}{p+q} N^{1/4} + \phi(N) - \phi_b}{uX} \\ &< \frac{\frac{N^{1/2}}{2N^{1/2}} N^{1/4} + \phi(N) - \phi_b}{uX} \\ &< \frac{XN^{1/4}}{2uX} + \frac{\phi(N) - \phi_b}{uX} \\ &\leq \frac{N^{1/4}}{2u} + \frac{\phi(N) - \phi_b}{uX} \end{aligned} \tag{4}$$

since $q - p < N^{1/2}$, $p + q > 2N^{1/2}$ and $X > 1$. If $X < \left| \frac{u}{2(\phi(N) - \phi_b)} \right|$ then $\frac{1}{2X} > \left| \frac{2(\phi(N) - \phi_b)}{u} \right|$. As uX will always be a positive value, rearranging (4), we obtain

$$\begin{aligned} \left| \left(\frac{e}{u} - \frac{N^{1/4}}{2u} \right) - \frac{Y}{X} \right| &< \left| \frac{\phi(N) - \phi_b}{uX} \right| \\ &< \frac{1}{2X^2} \end{aligned}$$

which satisfies Theorem 1. This terminates the proof.

Theorem 4. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let e satisfies the equation $eX - uY = Z - \phi_b$ where X, Y are positive integers with $\gcd(X, Y) = 1$. If*

$$1 \leq Y < X < \frac{u}{2\left(\phi(N) - \phi_b\right)}, \quad \phi(N) + \frac{p-q}{p+q} N^{1/4} < N - 2N^{1/2},$$
$$|Z - \phi(N)| < \frac{p-q}{p+q} N^{1/4}$$

then N can be factored in polynomial time.

Proof. Suppose e satisfies an equation $eX - uY = Z - \phi_b$. Let X, Y and Z satisfy the conditions in Lemma 2, then we can find the values of X and Y by computing $\frac{e}{u} - \frac{N^{1/4}}{2u}$. From the values of X and Y, we define

$$S = N - (eX - uY + \phi_b) = N - Z.$$

Since $\phi(N) + \frac{p-q}{p+q} N^{1/4} < N - 2N^{1/2}$ then $S \geq N - \left(\phi(N) + \frac{p-q}{p+q} N^{1/4} \right) > N - \left(N - 2N^{1/2} \right) = 2N^{1/2}$. We also have

$$\begin{aligned} S^2 - 4N &= (N - Z)^2 - 4N \\ &= N^2 - 2NZ + Z^2 - 4N \\ &= N(N - 2Z - 4) + Z^2 \\ &> N. \end{aligned}$$

Thus $\sqrt{S^2-4N} > N^{1/2} > p-q$. We also observe that

$$\begin{aligned} S &= N - Z \\ &> N - \left(\frac{p-q}{p+q}N^{1/4} + \phi(N)\right) \\ &> N - \phi(N) - \frac{p-q}{p+q}N^{1/4} \\ &= p+q-1-\frac{p-q}{p+q}N^{1/4} \end{aligned} \tag{5}$$

Rearranging (5), we get

$$|p+q-S-1| < |p+q-S| < \frac{p-q}{p+q}N^{1/4}$$

which satisfies Lemma 1. Thus we can find $\tilde{P} = \frac{1}{2}\left(S+\sqrt{S^2-4N}\right)$ such that $|p-\tilde{P}| < N^{1/4}$. Based on Theorem 2, we can factor N in polynomial time.

Remark 2. Observe that $\frac{Y}{X}$ is a convergent of the terms $\frac{e}{u} - \frac{N^{\frac{1}{4}}}{2u}$. Since $u \approx N$, the condition $Y < X$ will always hold. The convergents of $\frac{e}{u} - \frac{N^{\frac{1}{4}}}{2u}$ will produce a sequence, where candidates of X begins from the smallest possible integer till $2u^2$. Since $1 < \frac{u}{2(\phi(N)-\phi_b)} < 2u^2$, there will exist candidates of X where $1 < X < \frac{u}{2(\phi(N)-\phi_b)}$. Moreover, since the continued fractions process ends in polynomial time, candidates for X can be tested in polynomial time. Thus, we can guarantee the existence of the pair (X, Y) satisfying the conditions of Theorem 4.

Given (N, e) the following is an algorithm to initiate factoring $N = pq$ by using the continued fraction and Coppersmith's method via the LLL algorithm. The algorithm is as follows:

Algorithm 1. Factoring RSA moduli satisfying Theorem 4.

Input: The RSA public key pair (N, e) and u.
Output: The prime factors p, q or $\perp$.

1: Compute A to be the continued fraction of $\left(\frac{e}{u} - \frac{N^{1/4}}{2u}\right)$
2: Set Y = numerator of A and X = denominator of A such that $\gcd(X, Y) = 1$.
3: For each convergent $\frac{Y}{X}$ of $\left(\frac{e}{u} - \frac{N^{1/4}}{2u}\right)$, compute $Z = eX - uY + \phi_b$
4: Compute $S = N - Z$ and $\tilde{P} = \frac{1}{2}\left(S + \sqrt{S^2-4N}\right)$
5: Consider the polynomials $F(v) = (v + \tilde{P})$
6: Construct a matrix M of coefficient vectors of elements of $\langle F(v), N\rangle$.
7: Run LLL algorithm onto M.
8: Construct the polynomials $M'(v)$ from the first row of output of Step 7.
9: Factor $M'(v)$ to obtain small root v_0.
10: Compute $p = v_0 + \tilde{P}$ and $q = \frac{N}{p}$.
11: **if** $q \in \mathbb{Z}$, **then** output p, q.
12: **else** Algorithm fails or $\perp$.

Remark 3. Due to the fact that the equation being manipulated given by $eX - uY = Z - \phi_b$ does not represent the RSA key equation, we do not need an upper bound of the decryption exponent d for the attack to work properly. Indeed, there is no need to discuss the bound for d, since neither d nor its generalized parameter is in our equation. Upon factoring $N = pq$, one is able to retrieve $d \approx N$. This is a major finding. All previous results related to studying the RSA key equation has the condition the maximum bound of d is given by $d < N^{1/2}$.

The following is an example to illustrate Algorithm 1.

Example 1. We use RSA-129 modulus in this example. Specifically, we are given

$$N = 35110530776384842467159479027161914659 9$$

and

$$e = 94383702447496973551039638622969051 7$$

Then we compute

$$\begin{aligned}\phi_a &= \left\lfloor N - 2\sqrt{N} + 1 \right\rfloor \\ &= 35110530776384842463411918179016292223 5\end{aligned}$$

and

$$\begin{aligned}\phi_b &= \left\lceil N - \frac{3}{\sqrt{2}}\sqrt{N} + 1 \right\rceil \\ &= 35110530776384842463184590494212446011 5\end{aligned}$$

which values are used to compute

$$\begin{aligned}u &= \phi_a + \phi_b \\ &= 70221061552769684926596508673228738235 0.\end{aligned}$$

Then we obtain the continued fraction expansion of $\frac{e}{u} - \frac{N^{1/4}}{2u}$ which is

$$\left[0, \frac{1}{743}, \frac{1}{744}, \frac{228}{169631}, \cdots, \frac{19879}{14789889}, \frac{1040411704253353285}{774061754625882738716}, \ldots\right]$$

Taking $\frac{Y}{X} = \frac{19879}{14789889}$, then we compute

$$\begin{aligned}Z &= eX - uY + \phi_b \\ &= 35110530776384842463278509205250150707 8.\end{aligned}$$

Then we compute

$$\begin{aligned}S &= N - Z \\ &= 38809698219117639522\end{aligned}$$

and

$$\begin{aligned}\tilde{P} &= \frac{1}{2}\left(S + \sqrt{S^2 - 4N}\right) \\ &= 24448940821740240387\end{aligned}$$

Let $F(v) = (v + \tilde{P})$ and $V = 8000000$, be the upper bound of the unknown $|p - \tilde{P}|$. We consider the polynomials, $N^2, NF(v), F(v)^2, vF(v)^2$ and $v^2F(v)^2$ and build a matrix, M corresponding to these polynomials. Particularly,

$$M = \begin{bmatrix} N^2 & 0 & 0 & 0 & 0 \\ N\tilde{P} & N \cdot V & 0 & 0 & 0 \\ \tilde{P}^2 & 2\tilde{P}V & V^2 & 0 & 0 \\ 0 & \tilde{P}^2V & 2\tilde{P}V^2 & V^3 & 0 \\ 0 & 0 & \tilde{P}^2V^2 & 2\tilde{P}V^3 & V^4. \end{bmatrix}$$

Let M_{LLL} as the LLL-reduced matrix, we use the coefficients of the first row of M_{LLL} to construct the polynomial $M'(v)$ where

$$\begin{aligned}M'(v) = &-80322272v^4 + 4316657527524354v^3 - 171232356434129597494 19v^2 \\ &-25819107876857731036710641043v + 16394904467315025730472619833372752.\end{aligned}$$

By finding the integer roots of $M'(v)$, we obtain

$$v = 493424.$$

Observe

$$\begin{aligned}p &= v + \tilde{P} \\ &= 24448940821740733811\end{aligned}$$

Now we can solve the factorization of N by finding

$$\begin{aligned}q &= \frac{N}{p} \\ &= 14360757397377109309.\end{aligned}$$

Remark 4. The RSA private exponent, d corresponding with (N, e) as given in Example 1 such that $ed \equiv 1 \pmod{\phi(N)}$ is

$$d = 44601440284214524132897789887339371933 \approx N^{0.97675} \approx N.$$

Remark 5. Observe that values of X and Y in Example 1 satisfy conditions posed in Theorem 4.

Remark 6. Observe that since $1 \leq Y < X < \frac{u}{2(\phi(N)-\phi_b)}$,

$$\begin{aligned} e = \frac{Z-\phi_b+uY}{X} &\geq \frac{Z-\phi_b+u}{X} \\ &> \frac{Z-\phi_b+u}{u} \cdot 2(\phi(N)-\phi_b) \\ &= 2(\phi(N)-\phi_b)\left(1+\frac{Z-\phi_b}{u}\right) \\ &> 2(\phi(N)-\phi_b) \approx N^{1/2}. \end{aligned}$$

This means our attack only works if $e > N^{1/2}$.

3.1 Estimating Numbers of (N, e)'s Satisfying $eX - uY = Z - \phi_b$

In this section, we give an estimation of the numbers of e satisfying $eX - uY = Z - \phi_b$. The following lemma states that the public parameter $e < N$ satisfies at most one equation $eX - uY = Z - \phi_b$ where the unknown parameters X,Y and Z satisfy the conditions of Theorem 4.

Lemma 3. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. For $i = 1, 2$, let e satisfies the equation $eX_i - uY_i = Z_i - \phi_b$ with $\gcd(X, Y) = 1$,*

$$1 \leq Y_i < X_i < \frac{u}{2\left(\phi(N)-\phi_b\right)}, \quad \phi(N) + \frac{p-q}{p+q}N^{1/4} < N - 2N^{1/2},$$

and $|Z_i - \phi(N)| < \frac{p-q}{p+q}N^{1/4}$.

Then $X_1 = X_2$, $Y_1 = Y_2$ and $Z_1 = Z_2$.

Proof. Suppose that e satisfying two equations

$$eX_1 - uY_1 = Z_1 - \phi_b \quad \text{and} \quad eX_2 - uY_2 = Z_2 - \phi_b$$

with

$$X_1, X_2 < \frac{u}{2\left(\phi(N)-\phi_b\right)} \quad \text{and} \quad |Z_1 - \phi(N)|, |Z_2 - \phi(N)| < \frac{p-q}{p+q}N^{1/4}.$$

Then, equating the term e, we have

$$\frac{Z_1 - \phi_b + uY_1}{X_1} = \frac{Z_2 - \phi_b + uY_2}{X_2} \tag{6}$$

Rearranged (6) to

$$X_2(Z_1 - \phi_b) + X_1(\phi_b - Z_2) = u(X_1Y_2 - X_2Y_1). \tag{7}$$

Suppose $X_1, X_2 < \frac{u}{2(\phi(N)-\phi_b)}$. Observe that

$$|Z_1 - Z_2| < \frac{2(p-q)}{p+q}N^{1/4} \quad \text{and} \quad \phi(N) - \phi_b > N^{1/4}$$

which implies $\frac{Z_1-Z_2}{(\phi(N)-\phi_b)} < 1$. Consider the left hand side of (7),

$$\begin{aligned} X_2(Z_1-\phi_b)+X_1(\phi_b-Z_2) &< \frac{u}{2\,(\phi(N)-\phi_b)}(Z_1-\phi_b)+\frac{u}{2\,(\phi(N)-\phi_b)}(\phi_b-Z_2) \\ &= \frac{u}{2}\left(\frac{Z_1-\phi_b}{(\phi(N)-\phi_b)}+\frac{\phi_b-Z_2}{(\phi(N)-\phi_b)}\right) \\ &= \frac{u}{2}\left(\frac{Z_1-Z_2}{(\phi(N)-\phi_b)}\right) \\ &< u \end{aligned} \tag{8}$$

Hence from the right hand side of (7), we deduce that $X_1Y_2 - X_2Y_1 = 0$. Since $\gcd(X_1, Y_1) = \gcd(X_2, Y_2) = 1$, it shows that $X_1 = X_2$ and $Y_1 = Y_2$. Thus, from (6), this leads to $Z_1 = Z_2$.

The following result give the estimation of the number of e's for which the Theorem 4 applies.

Lemma 4. *Let X and Y be two integers satisfying $1 \leq Y < X < \frac{p-q}{p+q}N^{\frac{1}{4}}$ and $\gcd(X, Y) = 1$. Then there exists an integer Z such that $Z \equiv \phi_b - uY \pmod{X}$ and $|Z - \phi(N)| < \frac{p-q}{p+q}N^{\frac{1}{4}}$.*

Proof. Assume that X and Y are fixed with $\gcd(X, Y) = 1$. Let $Z_0 = \phi_b - uY$. Let $\beta \equiv \phi(N) - Z_0 \pmod{X}$ with $0 \leq \beta < X$ and set $Z = \phi(N) - \beta$. Then

$$Z = \phi(N) - \beta \equiv Z_0 \equiv \phi_b - uY \pmod{X}.$$

Define $e = \frac{Z-Z_0}{X}$. Then $eX = Z - Z_0 = Z - \phi_b + uY$, that is $eX - uY = Z - \phi_b$. Moreover, we have

$$|Z - \phi(N)| = \beta < X < \frac{p-q}{p+q}N^{\frac{1}{4}}.$$

This terminates the proof. □

Theorem 5. *Let $N = pq$ be the product of two balanced prime integers such that $p - q > c_1\sqrt{N}$. The number of possible values of the parameter $e < N$ in Theorem 4 where*

$$e = \frac{Z - \phi_b + uY}{X}$$

and $\gcd(X, Y) = 1$ with

$$1 \leq Y < X < \frac{p-q}{p+q}N^{\frac{1}{4}}$$

is at least $N^{\frac{1}{2}-\epsilon}$ where $\epsilon > 0$ is arbitrarily small for suitably large N.

Proof. Let X and Y be two integers satisfying $1 \leq Y < X < \frac{p-q}{p+q}N^{\frac{1}{4}}$ and $\gcd(X,Y) = 1$. Then by Lemma 4, there exists an integer Z such that $e = \frac{Z-\phi_b+uY}{X}$ is also an integer. Let $z = Z - \phi_b$. Then

$$e = \frac{z+uY}{X}.$$

The number of the parameter e's satisfying the equation $e = \frac{z+uY}{X}$ with the conditions given in the Theorem 4 is

$$\#(e) = \sum_{X=1}^{\mathcal{N}_1} \sum_{\substack{Y=1 \\ \gcd(X,Y)=1}}^{X-1} 1, \tag{9}$$

where

$$\mathcal{N}_1 = \frac{p-q}{p+q}N^{\frac{1}{4}} \approx c_1 N^{\frac{1}{4}}$$

when p and q are balanced with $p - q > c_2\sqrt{N}$ for some positive constants c_1 and c_2.

Observe that for $1 \leq Y < X < \frac{p-q}{p+q}N^{\frac{1}{4}}$ we have the following.

$$\sum_{\substack{Y=1 \\ \gcd(X,Y)=1}}^{X-1} 1 = \phi(X) > \frac{c_3 X}{\log\log X} > \frac{c_3 X}{\log\log N}, \tag{10}$$

where c_3 is a constant (see [7], Theorem 328). Substitute (10) in (9), we obtain

$$\#(e) > \frac{c_3}{\log\log N} \sum_{X=1}^{\mathcal{N}_1} X \tag{11}$$

Next, for $\sum_{X=1}^{\mathcal{N}_1} X$, we have

$$\sum_{X=1}^{\mathcal{N}_1} X = \frac{\mathcal{N}_1(\mathcal{N}_1+1)}{2} > \frac{\mathcal{N}_1^2}{2} = \frac{\left(c_1 N^{\frac{1}{4}}\right)^2}{2} \tag{12}$$

Substitute (12) in (11), we obtain

$$\begin{aligned} \#(e) &> \frac{c_3}{\log\log N} \times \frac{\left(c_1 N^{\frac{1}{4}}\right)^2}{2} \\ &> \frac{c_1^2 c_3}{2\log\log N} N^{\frac{1}{2}} \\ &= N^{\frac{1}{2}-\epsilon} \end{aligned} \tag{13}$$

Hence a good approximation for the number of weak keys e is at least $N^{\frac{1}{2}-\epsilon}$ where $\epsilon > 0$ is arbitrarily small for suitably large N where $N^{-\epsilon} = \frac{c_1^2 c_3}{2\log\log N}$. □

4 The Second Attack

In this section, we are given k RSA moduli $N_i = p_i q_i$ with its corresponding public exponent e_i and u_i where $u_i = \phi_{a_i} + \phi_{b_i}$ follows Definition 1. By using the following theorem, we can factor k RSA moduli N_i simultaneously if there exist suitable X and Y_i that satisfy conditions required in the theorem. The ability to factor these moduli simultaneously are based on the results from Theorem 2 and Theorem 3.

Theorem 6. *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 $Y_i < N^{\delta}$ with $\gcd(X, Y_i) = 1$ and $|Z_i - \phi(N_i)| < \frac{p_i - q_i}{p_i + q_i} N^{1/4}$ such that $e_i X - Y_i u_i = Z_i - \phi_{b_i}$ for $i = 1, \ldots, k$, and $|Z_i - \phi_{b_i}| < \lambda N^{\delta + \frac{1}{4}}$ where $\lambda < \frac{3}{2}\left(2^{\frac{k+5}{4}} - 3\right)$ 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 $e_i X - u_i Y_i = Z_i - \phi_{b_i}$ can be rewritten as

$$e_i X - \left(N_i - 2\sqrt{N_i} + 1 + N_i - \frac{3}{\sqrt{2}}\sqrt{N_i} + 1\right) Y_i = Z_i - \phi_{b_i}$$

as $u_i = \phi_{a_i} + \phi_{b_i}$ and $\phi_{a_i} = N_i - 2\sqrt{N_i} + 1, \phi_{a_i} = N_i - \frac{3}{\sqrt{2}}\sqrt{N_i} + 1$. This implies

$$e_i X - (2(N_i + 1))\, Y_i = Z_i - \phi_{b_i} - \left(2\sqrt{N_i} + \frac{3}{\sqrt{2}}\sqrt{N_i}\right) Y_i.$$

Hence

$$\left|\frac{e_i X}{2(N_i + 1)} - Y_i\right| = \frac{\left|Z_i - \phi_{b_i} - \left(2\sqrt{N_i} + \frac{3}{\sqrt{2}}\sqrt{N_i}\right) Y_i\right|}{2(N_i + 1)}. \tag{14}$$

Let $N = \min_i N_i$ and suppose that $Y_i < N^{\delta}$ and $|Z_i - \phi_{b_i}| < \lambda N^{\delta + \frac{1}{4}}$. Then $|Z_i - \phi_{b_i}| < \lambda \frac{p_i - q_i}{p_i + q_i} N^{1/4} < \lambda N^{\delta + \frac{1}{4}}$. Since $2\sqrt{N_i} + \frac{3}{\sqrt{2}}\sqrt{N_i} < \frac{9}{2}\sqrt{N_i}$, we will get

$$\begin{aligned}
\frac{\left|Z_i - \phi_{b_i} - \left(2\sqrt{N_i} + \frac{3}{\sqrt{2}}\sqrt{N_i}\right) Y_i\right|}{2N_i} &\leq \frac{|Z_i - \phi_{b_i}| + \left(2\sqrt{N} + \frac{3}{\sqrt{2}}\sqrt{N}\right) Y_i}{2N} \\
&< \frac{\lambda N^{\delta + \frac{1}{4}} + \left(\frac{9}{2}\sqrt{N}\right) Y_i}{2N} \\
&< \frac{\lambda N^{\delta + \frac{1}{4}} + \frac{9}{2} N^{\delta + \frac{1}{2}}}{2N} \\
&< \frac{\left(\frac{9}{2} + \lambda\right) N^{\delta + \frac{1}{2}}}{2N} \\
&= \left(\frac{\frac{9}{2} + \lambda}{2}\right) N^{\delta - \frac{1}{2}}
\end{aligned}$$

Plugging in (14), we get

$$\left|\frac{e_i X}{2(N_i+1)} - Y_i\right| < \left(\frac{\frac{9}{2}+\lambda}{2}\right) N^{\delta-\frac{1}{2}}$$

We now proceed to prove the existence of the integer X. Let $\epsilon = \left(\frac{\frac{9}{2}+\lambda}{2}\right) N^{\delta-\frac{1}{2}}$, $\delta = \frac{k}{2(k+1)}$. We have

$$N^{\delta} \cdot \epsilon^k = N^{\delta} \cdot N^{k\delta-\frac{k}{2}} \left(\frac{\frac{9}{2}+\lambda}{2}\right)^k = N^{\delta(k+1)-\frac{k}{2}} \cdot \left(\frac{\frac{9}{2}+\lambda}{2}\right)^k. \tag{15}$$

Since $\delta = \frac{k}{2(k+1)}$, (15) becomes

$$N^0 \cdot \left(\frac{\frac{9}{2}+\lambda}{2}\right)^k = \left(\frac{\frac{9}{2}+\lambda}{2}\right)^k. \tag{16}$$

Suppose $\lambda < \frac{3}{2}\left(2^{\frac{k+5}{4}} - 3\right)$ then (16) becomes

$$\begin{aligned}\left(\frac{\frac{9}{2}+\lambda}{2}\right)^k &< \left(\frac{\frac{9}{2}+\frac{3}{2}\left(2^{\frac{k+5}{4}}-3\right)}{2}\right)^k \\ &= \left(\frac{9}{4}+\frac{3}{4}\left(2^{\frac{k+5}{4}}-3\right)\right)^k \\ &= \left(2^{\frac{k+5}{4}} \cdot 3 \cdot 2^{-2}\right)^k \\ &= 2^{\frac{k(k-3)}{4}} \cdot 3^k. \end{aligned} \tag{17}$$

Combining (15) and (17), we obtain

$$N^{\delta} < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \epsilon^{-k}$$

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

$$\left|\frac{e_i X}{2(N_i+1)} - Y_i\right| < \epsilon, \quad X < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \epsilon^{-k}$$

which satisfies the conditions in Theorem 3 which will find X and Y_i for $i = 1, \ldots, k$. Next, using the equation $e_i X - u_i Y_i + \phi_{b_i} = Z_i$, we get the value of Z_i. We also observe that

$$\begin{aligned} S_i &= N_i - Z_i \\ &\geq N_i - \left(\frac{p_i - q_i}{p_i + q_i} N_i^{1/4} + \phi(N_i)\right) \\ &= N_i - \phi(N_i) - \frac{p_i - q_i}{p_i + q_i} N_i^{1/4} \\ &= p_i + q_i - 1 - \frac{p_i - q_i}{p_i + q_i} N_i^{1/4} \end{aligned} \tag{18}$$

Rearranging (18), we get

$$|p_i + q_i - S_i - 1| < |p_i + q_i - S_i| < \frac{p_i - q_i}{p_i + q_i} N_i^{1/4}$$

which satisfies Lemma 1. Thus we can find $\tilde{p_i} = \frac{1}{2}\left(S_i + \sqrt{S_i^2 - 4N_i}\right)$ such that $|p_i - \tilde{p_i}| < N_i^{1/4}$. Based on Theorem 2, we can factor N_i in polynomial time.

We can build an algorithm to factor k RSA moduli N_i simultaneously. The algorithm is shown in Algorithm 1:

Algorithm 2. Factoring k RSA moduli simultaneously satisfying Theorem 6

Input: The public RSA key pairs (N_i, e_i) and u_i for $i = 2, 3, \ldots, k$.
Output: The prime factors p_i, q_i.

1: **for** $i = 2, 3, \ldots, k$ **do**
2: Compute $\phi_{a_i} = \left\lfloor N_i - 2\sqrt{N_i} + 1 \right\rfloor$.
3: Compute $\phi_{b_i} = \left\lceil N_i - \frac{3}{\sqrt{2}}\sqrt{N_i} + 1 \right\rceil$.
4: Compute $u_i = \phi_{a_i} + \phi_{b_i}$.
5: **end for**
6: Set $N = \min(N_1, N_2, N_3)$.
7: Compute $\delta = \frac{k}{2(k+1)}$.
8: Compute $\lambda = \left\lfloor \frac{3}{2}\left(2^{\frac{k+5}{4}} - 3\right) \right\rfloor$.
9: Compute $\epsilon = \left(\frac{\frac{9}{2}+\lambda}{2}\right) N^{\delta - \frac{1}{2}}$.
10: Compute $C = \left\lceil 3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} 4 \cdot \epsilon^{-n-1} \right\rceil$.
11: Compute lattice $\mathcal{L}$ spanned by the rows of the matrix M shown in proof of Theorem 4 in [15].
12: Compute matrix K by applying LLL algorithm onto M.
13: Compute matrix $H = KM^{-1}$.
14: Assign every element in the first row of H (starting from most left) as $X, Y_1, \ldots, Y_k$ respectively.
15: **for** $i = 2, 3, \ldots, k$ **do**
16: Compute $S_i = N_i - Z_i = N_i - (e_i X - u_i Y_i) + \phi_{b_i}$.
17: Compute $D_i = \left\lceil \sqrt{S_i^2 - 4N_i} \right\rceil$.
18: Compute $\tilde{P_i} = \frac{1}{2}(S_i + D_i)$.
19: Applying Coppersmith's method in Theorem 2 onto each P_i to output p_i.
20: Compute $q_i = N_i / p_i$.
21: **if** $q_i \in \mathbb{Z}$, **then** output p_i, q_i.
22: **else** Algorithm fails or $\perp$.
23: **end for**

5 Comparative Analysis

In this section, we compare our findings against previous findings with respect to the form of the modified key equations and their conditions. The comparisons are illustrated in Table 1.

Table 1. Comparison of Our Methods Against Previous Findings

Findings	Manipulated equation	Conditions
Blömer and May [3]	$ex - y\phi(N) = z$	$x < \frac{1}{3}N^{1/4}$ and $\lvert z\rvert < exN^{-3/4}$
Hinek [8]	$e_i d - k_i\phi(N_i) = 1$	$d < N^{\delta}$ with $\delta = \frac{k}{2(k+1)} - \epsilon$ where ϵ depending on N
Nitaj *et al.* (Theorem 5 in [15])	$e_i x - y_i\phi(N_i) = z_i$	$N = \min_i N_i$, $x < N^{\delta}$, $y_i < N^{\delta}$, $\lvert z_i\rvert < \frac{p_i - q_i}{3(p_i+q_i)} y_i N^{1/4}$ where $\delta = \frac{k}{2(k+1)}$
Nitaj *et al.* (Theorem 6 in [15])	$e_i x_i - y\phi(N_i) = z_i$	$N = \min_i N_i$, $\min_i e_i = N^{\alpha}$, $x_i < N^{\delta}, y < N^{\delta}$, $\lvert z_i\rvert < \frac{p_i - q_i}{3(p_i+q_i)} y N^{1/4}$ where $\delta = \frac{(2\alpha-1)k}{2(k+1)}$
Ariffin *et al.* (Theorem 13 in [1])	$ed - k\phi(N) = 1$	$\lvert b^2 p - a^2 q\rvert < N^{\gamma}$ $(a^2(b^4+1)p - b^2(a^4+1)q)(b^2 p - a^2 q) > 0$ $d < \frac{\sqrt{3}}{\sqrt{2}} N^{\frac{3}{4}\gamma}$
Our method: Theorem 4	$eX - uY = Z - \phi_b$	$1 \le Y < X < \frac{u}{2(\phi(N) - \phi_b)}$, $\phi(N) + \frac{p-q}{p+q} N^{1/4} < N - 2N^{1/2}$, $\lvert Z - \phi(N)\rvert < \frac{p-q}{p+q} N^{1/4}$
Our method: Theorem 6	$e_i X - Y_i u_i = Z_i - \phi_{b_i}$	$N = \min_i N_i$, $X < N^{\delta}$, $Y_i < N^{\delta}$, $\lvert Z_i - \phi(N_i)\rvert < \frac{p_i - q_i}{p_i+q_i} N^{1/4}$ $\lvert Z_i - \phi_{b_i}\rvert < \lambda N^{\delta + \frac{1}{4}}$ where $\lambda < \frac{3}{2}\left(2^{\frac{k+5}{4}} - 3\right)$ and $\delta = \frac{k}{2(k+1)}$

From Table 1, based on the references given, we can see that all earlier first 5 findings from Blömer and May [3] till Ariffin *et al.* [1] type of attacks zoomed into the RSA diophantine equation either in its original or generalized form. The first 5 findings had to dictate conditions upon the decryption exponent d or its corresponding generalized parameter.

In retrospect, our equation did not utilize the RSA diophantine equation either in its original or generalized form. As a result, our strategy enables us to factor $N = pq$ for a set of weak keys with $d \approx N$. This is a new and important result. The conditions upon our parameters cannot not be compared to conditions upon parameters of earlier results. This is due do the fact that there is no relation between our parameters X and Y and the parameters d and $\phi(N)$.

6 Conclusion

We have formulated two new attacks on RSA using a method derived from past literature regarding attacks on the RSA key equation. In our method, we utilized an equation that does not represent the RSA key equation, which under our defined conditions can be utilized to factor N in polynomial time. The strategy

uses a combination of continued fractions and Coppersmith's methods. Implicitly, the insertion of u into the equation will render a particular (N, e) to be a weak RSA public key pair. We also estimate the number of e's that satisfying our theorem is at least $N^{\frac{1}{2}-\epsilon}$. Finally, we have presented a case where given k weak RSA public key pairs, we can find the prime factors of each N simultaneously in polynomial time.

References

1. Ariffin, M.R.K., Abubakar, S.I., Yunos, F., Asbullah, M.A.: New cryptanalytic attack on RSA modulus $N = pq$ using small prime difference method. Cryptography **3**(1), 2 (2019)
2. Asbullah, M., Ariffin, M.: New attacks on RSA with modulus $N = p^2q$ using continued fractions. J. Phy. Conf. Ser. **622**, 012019 (2015)
3. Blömer, J., May, A.: A generalized wiener attack on RSA. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 1–13. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24632-9_1
4. Buhler, J.P., Lenstra, H.W., Pomerance, C.: Factoring integers with the number field sieve. In: Lenstra, A.K., Lenstra, H.W. (eds.) The Development of the Number Field Sieve. LNM, vol. 1554, pp. 50–94. Springer, Heidelberg (1993). https://doi.org/10.1007/BFb0091539
5. Coppersmith, D.: Finding a small root of a bivariate integer equation; factoring with high bits known. In: Maurer, U. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 178–189. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68339-9_16
6. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptol. **10**(4), 233–260 (1997)
7. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Oxford University Press, Oxford (1979)
8. Hinek, M.J.: On the security of some variants of RSA. Ph.D. thesis, University of Waterloo (2007)
9. Lenstra Jr., H.W.: Factoring integers with elliptic curves. Ann. Math. **126**, 649–673 (1987)
10. Maitra, S., Santanu, S.: Revisiting Wiener's attack - new weak keys in RSA. In: Wu, T.-C., Lei, C.-L., Rijmen, V., Lee, D.-T. (eds.) ISC 2008. LNCS, vol. 5222, pp. 228–243. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85886-7_16
11. Nitaj, A.: Cryptanalysis of RSA using the ratio of the primes. In: Preneel, B. (ed.) AFRICACRYPT 2009. LNCS, vol. 5580, pp. 98–115. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-02384-2_7
12. Nitaj, A.: A new vulnerable class of exponents in RSA. JP J. Algebra Number Theory Appl. **21**(2), 203–220 (2011)
13. Nitaj, A.: New weak RSA keys. JP J. Algebra Number Theory Appl. **23**(2), 131–148 (2011)
14. Nitaj, A.: Diophantine and lattice cryptanalysis of the RSA cryptosystem. In: Yang, X.S. (ed.) Artificial Intelligence, Evolutionary Computing and Metaheuristics. Studies in Computational Intelligence, vol. 427, pp. 139–168. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-29694-9_7

15. Nitaj, A., Ariffin, M.R.K., Nassr, D.I., Bahig, H.M.: New attacks on the RSA cryptosystem. In: Pointcheval, D., Vergnaud, D. (eds.) AFRICACRYPT 2014. LNCS, vol. 8469, pp. 178–198. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-06734-6_12
16. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
17. Wiener, M.J.: Cryptanalysis of short RSA secret exponents. IEEE Trans. Inf. Theory **36**(3), 553–558 (1990)