Caliphate Journal of Science & Technology (CaJoST)

ISSN: 2705-313X (PRINT); 2705-3121 (ONLINE) Research Article

Open Access Journal available at: https://cajost.com.ng/index.php/files and https://www.ajol.info/index.php/cajost/index

DOI: https://dx.doi.org/10.4314/cajost.v7i1.7

Article Info

Received: 22nd September 2024

Revised: 21st January 2025

Accepted: 29th January 2025

Department of Mathematics, Sokoto State University, Sokoto, Nigeria

***Corresponding author's email:** siabubakar82@gmail.com

Cite this: *CaJoST*, 2025, 1, 55-65

Exploiting the Security of RSA Variant's Generalized Key Equations

Saidu I. Abubakar, Zaid Ibrahim, Sadiq Shehu, and Ahmad Rufai

The security of RSA cryptosystem and its variants rely on the intractability of integer factorization problem. Series of attacks have been reported to exploit the cryptosystem leading to polynomial time factorization of the composite integer N into its prime factors p and q. This paper presents two cryptanalysis attacks on the prime power modulus as one of the RSA variants with moduli $N_i = p_i^2 q_i^2$ where generalized key equations of the form $e_i d - k_i \varphi(N_i) = 1$ and $e_i d_i - k\varphi(N_i) = 1$ can be exploited and factored simultaneously using simultaneous Diophantine approximation method and lattice basis reduction technique. The paper also gives numerical examples to demonstrate how the attacks work.

Keywords: RSA Modulus, Key equations, Exploiting, Attacks, Simultaneous Diophantine

1. Introduction

The security of our digital information can be secured from the activities of eavesdroppers through the deployment of strong encryption schemes. These schemes can be constructed using complex mathematics and logic. Public key cryptography is the type of cryptosystem with two keys of public and private which provides confidentiality and integrity of data in our digital communication channels. RSA is the most widely applicable public key cryptosystem that has been vulnerable to so many cryptanalysis attacks such as side channel attacks, short decryption exponent attacks, continued fraction attacks, public key exponent attacks, partial key exposure attacks among others.

Among the real-world applications of RSA cryptosystem in digital signature is the use of digital ID cards by the Government of Taiwan where every citizen was issued with a unique ID using their online digital certificates. This clearly showed how a 1024-bit RSA keys was factored efficiently by an adversary for 184 different cases retrieved from the Taiwan's Citizen Digital Certificates, [1].

Similarly, Nemec et al. (2017) reported another attack on the vulnerability of the RSA and its key equations where Estania's digital identity cards and Belgium e-ID crads were practically factored using Return of Coppersmith Attack (ROCA), [2]. Moreover, a partial key exposure attack where an adversary has a knowledge of significant number of bits of the prime factors (p, q) was presented by [3]. More attacks on the vulnerabilities of the RSA variants can be found in M.N. Abdrehman and Ariffin (2016) [4], Abubakar et al. (2020)[5], Sadiq et al. (2020) [6] among others.

Our Contribution: This paper is an extension of our previous work where we showed that using continued fraction with $\varphi(N) < N - \frac{(a+b)\sqrt{N}}{\sqrt{ab}}$ as approximation of $\varphi(N)$ where private decryption exponent was obtained from the convergents of the continued fraction expansion of $\frac{e}{N - \frac{a+b}{\sqrt{ab}}\sqrt{N}}$, [7].

In this paper, we use the same approximation of $\varphi(N)$ as reported in [7] to show that given public key exponents pair (e_i, N_i), one can efficiently factor prime power moduli $N_i = p_i^2 q_i^2$ by exploiting the security of the generalized key equations of the form $e_i d - k_i \varphi(N_i) = 1$ and $e_i d_i - k\varphi(N_i) = 1$ using simultaneous Diophantine approximation and lattice basis reduction techniques which leads to the factorization of moduli N_i in polynomial time for $i = 1, \ldots j$, In the first attack, we show that public key pair (e_i, N_i) and a private key pair $(d, \varphi(N_i))$ must satisfy $e_i d - k_i \varphi(N_i) = 1$ where $e_i < N_i$. Also, if $N = \max\{N_i\}$, $(d, k_i) < N^{\gamma}$ for all

$\gamma = \frac{n(2\beta+1)}{2(3n+1)}$, $\gcd(\varphi(N_i), N_i) = \lambda_i$ and $(p_i - 1)(q_i - 1) = h_i$, then moduli N_i can be obtained simultaneously in polynomial time. While in the second attack, we establish that the attack is possible for public and private key pairs (e_i, N_i) and $(d_i, \varphi(N_i))$ satisfy $e_i d_i - k\varphi(N_i) = 1$ with $e = \min\{e_i\} = N^{\beta}$, $(d_i, k) < N^{\gamma}$ for all $\gamma = \frac{n(\beta-\delta)}{1+n}$, $\gcd(\varphi(N_i), N_i) \coloneqq \lambda_i$ and $(p_i - 1)(q_i - 1) = h_i$ where $0 < \gamma, \beta, \delta < 1$. The Paper also provides numerical examples on how the two attacks work.

The rest of the paper is organized as follows. In section one, we give an overview of some cryptanalysis attacks on RSA and its prime power modulus. We also give an account on how attacks are being carried out. Section two (preliminaries), gives definition of some basic terms and Theorems that are related to our work. Results of the major finding are reported in section three. Finally, we conclude the paper in section four.

2. Preliminaries

In this section, we give account on some basic terms applicable to this paper such as Continued fraction, simultaneous Diophantine approximations, lattice basis reduction techniques and some related theorems a s follows:

Definition 2.1 Continued fraction [8]: Given any positive real number x, define $x = x_0$ and for $i = 1,...n$ express $x_1 = \lfloor a_i \rfloor$, $x_{i+1} = \frac{1}{x_i - a_i}$ until $x \in Z$ Then the continued fraction of a real number x can be represented as $x = \{a_0, a_1, a_2, ...a_n\}$ where

$$\{a_0, a_1, a_2, ...a_n\} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 ..... + \cfrac{1}{a_n}}}}$$

and n may be infinite. All a_i that is $\{a_1, a_2, ...a_n\}$ called partial quotients are positive integers except a_0 which may be any integer. Any rational number $\frac{a}{b}$ can be expressed as a finite continued fraction $x = \{a_1, a_2, ...a_n\}$. Similarly, the convergent of x is denoted by a function $\frac{a}{b} = \{a_1, ...a_k\}$ for $k \geq 0$. It is pertinent to note here that if $x = \frac{a}{b}$ is a rational number, then; continued fraction expansion is finite .

Theorem 2.1. *Let L be a lattice of dimension τ with a basis $v_1, \ldots, v_\tau$. The LLL algorithm produces a reduced basis $b_1, \ldots, b_\omega$ satisfying*

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

for all $1 \leq i \leq \tau$ and L is the lattice [9].

1. **Theorem 2.2**: Simultaneous Diophantine Approximation [10] For any given rational numbers $\alpha_1 ... \alpha_n$ and $0 < \varepsilon < 1$, there exist polynomial time algorithm to compute integers $p_1 ... p_n$ and a positive integer q such that $\max|q\alpha_i - p_i| < \varepsilon$ and $q \leq 2^{\frac{n(n-4)}{4}} \cdot 3^n \cdot \varepsilon^{-n}$.

THEOREM 2.3: Let p and q be prime numbers where $q^2 < p^2 < 2q^2$ and $N = p^2 q^2$ be RSA variant. Given (e, N) for $e < \varphi(N)$ as a public key pair and (d, p, q) as a private key tuple and prime difference $|bq^2 - ap^2| < N^{\gamma}$. If $\frac{q^2}{p^2}$ is close to $\frac{b}{a}$ such that the relation $\left[a(b^2+1)q^2 - b(a^2+1)p^2\right](bq^2 - ap^2) > 0$ holds and $d < \frac{2\sqrt{2}}{3} N^{\frac{3}{4}-\gamma}$ then $\frac{k}{d}$ can be obtained efficiently from a convergent of the continued fraction expansion of $\frac{e}{N - \frac{a+b}{\sqrt{ab}}\sqrt{N}}$ for $k < d$ and (a, b) are positive integers less than $\log N$, Dogon daji et al. [7].

3. Results

In this paper, we give two different cryptanalysis attacks on i multi prime power moduli $N_i = p_i^2 q_i^2$ using system of equations: $e_i d - k_i \varphi(N_l) = 1$ and $e_i d_i - k\varphi(N_i) = 1$ for $i = 1, \ldots j$. In this regard i prime power moduli can be factored successfully in

polynomial time for unknown positive integers (d, k_i, d_i, k).

3.1. Attack on i prime power moduli $N_i = p_i^2 q_i^2$ in which $e_i d - k_i \varphi(N_l) = 1$ is satisfied.

Let prime power moduli $N_i = p_i^2 q_i^2$ with $j \geq 2$ .The attack works for n instances (e_i, N_i) if there exists an integer d and i integer k_i such that the key equation $e_i d - k_i \varphi(N_l) = 1$ is satisfied. We show that prime factors p_i and q_i of i multi prime power moduli N_i where $i = 1, \ldots j.$ can be found efficiently giving $N = \max\{N_i\}$, $(d, k_i) < N^{\gamma}$ for all $\gamma = \frac{n(2\beta+1)}{2(3n+1)}$. This clearly show that the RSA instance share a common decryption exponent d .

THEOREM 3.1; Let $N_i = p_i^2 q_i^2$ be prime power moduli for $i = 1, \ldots j.$, (e_i, N_i) be public key pair and $(d, \varphi(N_i))$ be private key pair such that $e_i < \varphi(N_i)$ satisfying $e_i d - k_i \varphi(N_i) = 1$ .Let $N = \max\{N_i\}$ and for all $\gamma = \frac{n(2\beta+1)}{2(3n+1)}$. If $\gcd(\varphi(N_i), N_i) = \lambda_i$ and $(p_i - 1)(q_i - 1) = h_i$ then private factors p_i and q_i of prime power moduli $N_i = p_i^2 q_i^2$ can be simultaneously recovered in polynomial time.

Proof: For $i \geq 2$, let $N_i = p_i^2 q_i^2$ $i = 1, \ldots j.$ be multi prime power moduli. Let $N = \max\{N_i\}$ and assume that $k_i < N^{\gamma}$, then equation $e_i d - k_i \varphi(N_l) = 1$ can be expressed as

$$e_i d - k_i \left(N_l - (p^2 + q^2)\right) = 1$$

$$e_i d - k_i \left(N_l - \frac{a+b}{\sqrt{ab}}\sqrt{N_i} + \frac{a+b}{\sqrt{ab}}\sqrt{N_i} - (N_i - \varphi(N_i)) \right) = 1$$

$$\left| \frac{e_i}{N_l - \frac{a+b}{\sqrt{ab}}\sqrt{N_i}} d - k_i \right| = \frac{\left| 1 - k_i (N_i - \varphi(N_i) - \frac{a+b}{\sqrt{ab}}\sqrt{N_i}) \right|}{N_l - \frac{a+b}{\sqrt{ab}}\sqrt{N_i}}$$

Taking $N = \max\{N_i\}$, $k_i < N^{\gamma}$, $N_l - \frac{a+b}{\sqrt{ab}}\sqrt{N_i} > N^{\beta}$

$$\frac{\left| 1 - k_i (N_i - \varphi(N_i) - \frac{a+b}{\sqrt{ab}}\sqrt{N_i}) \right|}{N_l - \frac{a+b}{\sqrt{ab}}\sqrt{N_i}} < \frac{\left| 1 + k_i \left(\frac{a+b}{\sqrt{ab}}\sqrt{N_i} + \varphi(N_i) - N_i \right) \right|}{N_l - \frac{a+b}{\sqrt{ab}}\sqrt{N_i}} \leq \frac{1 + N^{\gamma} \left(\frac{N^{2\gamma}}{\left(\frac{a+b}{\sqrt{ab}} + 2 \right)\sqrt{N}} \right)}{N^{\beta}}$$

$$= \frac{\left(1 + N^{3\gamma - \frac{1}{2} - \beta}\right)\sqrt{ab}}{a + b + 2\sqrt{ab}} \leq \frac{\left(1 + N^{3\gamma - \frac{1}{2} - \beta}\right)ab}{a + b + 2ab} < \frac{b}{a} N^{3\gamma - \frac{1}{2} - \beta}$$

Hence, $\left| \frac{e}{N_i - \frac{a+b}{\sqrt{ab}}\sqrt{N_i}} d - k_i \right| < \frac{b}{a} N^{3\gamma - \frac{1}{2} - \beta}$.

Next, to show that integers (d, k_i) exists, we let $\varepsilon = \frac{b}{a} N^{3\gamma - \frac{1}{2} - \beta}$ with $\gamma = \frac{n(2\beta+1)}{2(1+3n)}$ which gives

$$N^{\gamma}\varepsilon^{n} = N^{\gamma}\left(\frac{b}{a}N^{3\gamma-\frac{1}{2}-\beta}\right)^{n} = \left(\frac{b}{a}\right)^{n} N^{\gamma+3n\gamma-\frac{n}{2}-n\beta} = \left(\frac{b}{a}\right)^{n}$$

Using Theorem 2.2, we have $\left(\frac{b}{a}\right) < 2^{\frac{n(n-3)}{4}} \cdot 3^{n}$ for $n \geq 2$, $N^{\gamma}\varepsilon^{n} <. 2^{\frac{n(n-3)}{4}} \cdot 3^{n}$. It follows that if $d < N^{\gamma}$, then $d < 2^{\frac{n(n-3)}{4}} . 3^{n} . \varepsilon^{-n}$. Finally,

$$\left| \frac{e}{N_i - \frac{a+b}{\sqrt{ab}}\sqrt{N_i}} d - k_i \right| < \varepsilon$$

This satisfies Theorem 2.2. More so, we proceed to reveal the private keys (d, k_i) for $i = 1, ..., j.$

Next, from equation $e_i d - k_i \varphi(N_i) = 1$, we have $\varphi(N) = \frac{e_i d - 1}{k_i}$

Applying LLL algorithm on (d, k_i) we consider our public keys (e_i, N_i), and taking $h_i = (p_i - 1)(q_i - 1)$ and the private keys $(d, p_i, q_i, \varphi(N_i))$ such that $\gcd(\varphi(N_i), N_i) = \lambda_i$. Furthermore, define $y_i = \lambda_i - h_i + 1$ and solve the quadratic equation $x^2 - yx + \lambda_i = 0$, then the primes (p_i, q_i) can be recovered in polynomial time.

Let

$$M_1 = \frac{e_1}{N_1 - \frac{a+b}{\sqrt{ab}}\sqrt{N_1}}, \qquad M_2 = \frac{e_2}{N_2 - \frac{a+b}{\sqrt{ab}}\sqrt{N_2}}, \qquad M_3 = \frac{e_3}{N_3 - \frac{a+b}{\sqrt{ab}}\sqrt{N_3}}$$

Define

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

Consider the lattice ℓ spanned by the matrix

$$T = \begin{bmatrix} 1 & -\left[R(M_1)\right] & -\left[R(M_2)\right] & -\left[R(M_3)\right] \\ 0 & R & 0 & 0 \\ 0 & 0 & R & 0 \\ 0 & 0 & 0 & R \end{bmatrix}$$

Choosing suitable small positive integers a and b, the matrix T can be used in computing the reduced basis after applying the LLL algorithm.

Algorithm 3.1

1. Initialization : Consider the public key $(N, e), \gamma$ satisfying Theorem 3.1
2. Choose suitable public integers a, b and let $N = \max\{N_i\}$ for $i = 1, ..., j$
3. For any $(a, b, j, N, \beta, \gamma)$ do:
4. $\varepsilon = \frac{b}{a} N^{3\gamma-\frac{1}{2}-\beta}$
5. $R = \left[3^{n+1} \cdot 2^{\frac{(n+1)(n+3)}{2}} \cdot \varepsilon^{-n-1} \right]$ for $j \geq 2$
6. End for.
7. Consider the lattice ℓ spanned by the matrix T as mentioned above
8. Applying LLL algorithm to ℓ produces the reduced basis matrix V

9. For (T,V) do:
10. $U = T^{-1}$
11. $W = UV$
12. End for.
13. Produces d, k_i from W
14. Foe each $(e_i, d, k_i, h_i, \lambda_i)$, compute;
15. $\varphi(N_i) = \dfrac{e_i d - 1}{k_i}$
16. $\gcd(\varphi(N_i), N_i) := \lambda_i$
17. Define $y_i = \lambda_i - h_i + 1$
18. End for
19. Solve the quadratic equation $x^2 - y_i x + \lambda_i = 0$
20. Return primes p_i and q_i ,

Example 1.: This example illustrates how theorem 3.2 works on three (3) moduli alongside their corresponding public exponents

Let

$$N_1 = 566170180647705643604873426349688678273284056 41$$

$$N_2 = 723634647444690181152903479864994336317455782 49$$

$$N_3 = 174665654469895289877465412835375599796274783121$$

$$e_1 = 168779645317084234204056994321638729863882691 67$$

$$e_2 = 157035587325048878862914809847107999424661698 47$$

$$e_3 = 434883699024333597665058949223955463259720322 79$$

Also, let

$$h_1 = 237943308508995558562200$$

$$h_2 = 269004581269242536545248$$

$$h_3 = 417930202867402160829312$$

Observe that $N = \max\{N_1, N_2, N_3\}$

$$N = 174665654469895289877465412835375599796274783121$$

By using $a = 3$, $b = 2$ and since $j = 3$, then applying algorithm 3.1 gives

$$\gamma = \frac{n(2\beta+1)}{2(3n+1)} = 0.2568000000 \text{ And } \varepsilon := \frac{b}{a} N^{3\gamma - \frac{1}{2} - \beta} = 0.00006025259798$$

Applying Theorem 2.2 and algorithm 3.1 for $j = 3$. The computations follow as:

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

$$R = 3072924661000000000$$

Consider the lattice ℓ spanned by the matrix

$$T=\begin{bmatrix}1 & -\left[R(M_1)\right] & -\left[R(M_2)\right] & -\left[R(M_3)\right]\\ 0 & R & 0 & 0\\ 0 & 0 & R & 0\\ 0 & 0 & 0 & R\end{bmatrix}$$

Therefore, by applying the LLL algorithm to ℓ it yields reduced basis with the following entries

$$V=\begin{pmatrix}\text{-6600103} & -30089353639924 & -19113544255974 & -16007421799108\\ -38390877846767 & -2674770174036 & -154124162486 & -210975554212\\ 1029767194380 & -79367190558960 & 97844814274040 & 64740903481680\\ -9724383749484 & -21660523510672 & 116043031929928 & -87231298332624\end{pmatrix}$$

Next, from Algorithm 3.1, we compute $W=UV$

$$W=\begin{pmatrix}-6600103 & -1967541 & -1432285 & -1643298\\ -38390877846767 & -11444613241510 & -8331184903708 & -9558586098374\\ 1029767194380 & 306981447924 & 223469255858 & 256392115545\\ -9724383749484 & -2898912899806 & -2110283578691 & -2421183482547\end{pmatrix}$$

From the first row of matrix W it yields the values of (d,k_1,k_2,k_3) as follows

$d=6600103$ $k_1=1967541$ $k_2=1432285$ $k_3=1643298$

$\varphi(N_i)=\dfrac{e_i d-1}{k_i}$ can be computed using algorithm 3.1 for i = 1, 2, 3 as follows:

$$\varphi(N_1)=566170180644880127137880127495339339260537620 0$$

$$\varphi(N_2)=723634647441547653246218891642603984770285208 64$$

$$\varphi(N_3)=174665654469341607605555934830437092050673090432$$

Next, from algorithm 3.1 also y_i can equally be computed in the following way

$y_1=1184160592172$ $y_2=1168206092196$ $y_3=1324819953450$

Finally, solving the quadratic equation $x^2-y_i x+\lambda_i=0$ for I = 1, 2, 3 yields (p_1,q_1), (p_2,q_2) and (p_3,q_3) as follows:

$p_1=927663025831$ $p_2=852751119217$ $p_3=806828723417$

$q_1=256497566341$ $q_2=315454972979$ $q_3=517991230033$

3.2. Attack on i prime power moduli $N_i=p_i^{\,2}q_i^{\,2}$ satisfying $e_i d_i-k\varphi(N_l)=1$

In the second case, we consider multi prime power modulus $N_i=p_i^{\,2}q_i^{\,2}$ in which key equation $e_i d_i-k\varphi(N_l)=1$ is satisfied for unknown positive integers (k,d_i) for $i=1,...,j$. Here, each pair of multi prime power moduli has its own unique decryption exponent d_i.

THEOREM 3.2: Let $N_i=p_i^{\,2}q_i^{\,2}$ be multi prime power moduli for $i=1,...,j$, (e_i,N_i) and (d_i,N_i) be public and private key pairs respectively and $h_i=(p_i-1)(q_i-1)$ be known such that $e_i<\varphi(N_i)$ satisfying $e_i d_i-k\varphi(N_l)=1$. Taking $e=\min\{e_i\}=N^{\beta}$ and $(d_i,k)<N^{\gamma}$ for all $\gamma=\dfrac{n(\beta-\delta)}{1+n}$ then private factors p_i and q_i of multi prime power moduli N_i can be found simultaneously in polynomial time where the $\gcd(\varphi(N_i),N_i)\coloneqq\lambda_i$.

Proof: For $i \geq 2$, let $N_i = p_i^2 q_i^2$ be multi prime power moduli. $i = 1,..., j$ and public exponents $e = \min\{e_i\} = N^{\beta}$. If $d_i < N^{\gamma}$, then $e_i d_i - k\varphi(N_l) = 1$ can be expressed as

$$e_i d_i - k\left(N_l - (p^2 + q^2)\right) = 1$$

$$e_i d_i - k\left(N_l - \frac{a+b}{\sqrt{ab}}\sqrt{N_i} + \frac{a+b}{\sqrt{ab}}\sqrt{N_i} - (N_i - \varphi(N_i))\right) = 1$$

$$e_i d_i - k\left(N_i - \frac{a+b}{\sqrt{ab}}\sqrt{N_i}\right) + k\left(N_i - \varphi(N_i) - \frac{a+b}{\sqrt{ab}}\sqrt{N_i}\right) = 1$$

$$\left|\frac{k\left(N_i - \frac{a+b}{\sqrt{ab}}\sqrt{N_i}\right)}{e_i}\right| = \frac{\left|1 - k\left(N_i - \varphi(N_i) - \frac{a+b}{\sqrt{ab}}\sqrt{N_i}\right)\right|}{e_i}$$

From Theorem 2.3, it was shown that $\frac{a+b}{\sqrt{ab}}\sqrt{N_i} + \varphi(N_i) - N_i < \frac{N^{2\gamma}}{\left(\frac{a+b}{\sqrt{ab}} + 2\right)\sqrt{N_i}}$.

Taking $(d_i, k) < N^{\gamma}$, $e = \min\{e_i\} = N^{\beta}$ and $\frac{N^{2\gamma}}{\left(\frac{a+b}{\sqrt{ab}} + 2\right)\sqrt{N}} < N^{\delta}$ then

$$\frac{\left|1 - k\left(N_i - \varphi(N_i) - \frac{a+b}{\sqrt{ab}}\sqrt{N_i}\right)\right|}{e_i} \leq \frac{\left|1 + k\left(\frac{a+b}{\sqrt{ab}}\sqrt{N_i} + \varphi(N_i) - N_i\right)\right|}{e_i} < \frac{1 + N^{\gamma}\left(\frac{N^{2\gamma}}{\left(\frac{a+b}{\sqrt{ab}} + 2\right)\sqrt{N}}\right)}{N^{\beta}} < \sqrt{a}N^{\gamma+\delta-\beta}.$$

Hence, $\left|\frac{k\left(N_i - \frac{a+b}{\sqrt{ab}}\sqrt{N_i}\right)}{e_i}\right| < \sqrt{a}N^{\gamma+\delta-\beta}$ •

We now proceed to show that integers (k, d_i) exists, let $\varepsilon = \sqrt{a}N^{\gamma+\delta-\beta}$ and $\gamma = \frac{n(\beta-\delta)}{(1+n)}$, then we have

$$N^{\gamma}\varepsilon = N^{\gamma}\left(\sqrt{a}N^{\gamma+\delta-\beta}\right)^n = (a)^{\frac{n}{2}} N^{\gamma+n\gamma+n\delta-n\beta} = (a)^{\frac{n}{2}}$$

Following Theorem 2.2, we get $(a)^{\frac{n}{2}} < 2^{\frac{n(n-3)}{4}} \cdot 3^n$. for $n \geq 2$, then t $N^{\gamma}\varepsilon^n < 2^{\frac{n(n-3)}{4}} \cdot 3^n$. It follows that if $k_i < N^{\gamma}$, then k $< 2^{\frac{n(n-3)}{4}} \cdot 3^n \cdot \varepsilon^{-n}$,

Finally $\left|\frac{k\left(N_i - \frac{a+b}{\sqrt{ab}}\right)}{e_i} - d_i\right| < \varepsilon$

This satisfies the conditions of Theorem 2.2 and we proceed to reveal the private keys (d_i, k) for $i = 1,..., j$.

Next, from equation $e_i d_i - k\varphi(N_i) = 1$ we have that $\varphi(N_i) = \dfrac{e_i d_i - 1}{k}$

Applying LLL algorithm on (d_i, k), we consider (e_i, N_i), and given $h_i = (p_i - 1)(q_i - 1)$ and $(d, p, q, \varphi(N))$ such that $\gcd(\varphi(N_i), N_i) = \lambda_i$. Furthermore, define $y_i = \lambda_i - h_i + 1$ and solve the equation $x^2 - y_i x + \lambda_i = 0$, then primes (p_i, q_i) can be recovered in polynomial time.

Let

$$M_1 = \frac{N_1 - \dfrac{a+b}{\sqrt{ab}}\sqrt{N_1}}{e_i}, \qquad M_2 = \frac{N_2 - \dfrac{a+b}{\sqrt{ab}}\sqrt{N_2}}{e_2}, \qquad M_3 = \frac{N_3 - \dfrac{a+b}{\sqrt{ab}}\sqrt{N_3}}{e_3},$$ Define

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

Consider the lattice ℓ spanned by the matrix\

$$T = \begin{bmatrix} 1 & -\left[R(M_1)\right] & -\left[R(M_2)\right] & -\left[R(M_3)\right] \\ 0 & R & 0 & 0 \\ 0 & 0 & R & 0 \\ 0 & 0 & 0 & R \end{bmatrix}$$

Carefully selecting small positive integers a and b, the matrix T can be used in computing the reduced basis after applying the LLL algorithm.

Algorithm 3.2

1. Initialization : Consider the public key (e_i, N_i) and γ satisfying theorem 3.2
2. Choose suitable public integers a, b and let $N = \max\{N_i\}$ for $i = 1, ..., j$
3. For any $(a, b, j, N, \gamma, \delta)$, do:
4. $\varepsilon = \sqrt{a} N^{\gamma+\delta-\beta}$
5. $\left[3^{n+1} \cdot 2^{\frac{(n+1)(n+3)}{2}} \cdot \varepsilon^{-n-1} \right]$ for $j \geq 2$
6. End for.
7. Consider the lattice ℓ spanned by the matrix T as mentioned above
8. Applying LLL algorithm to ℓ produces the reduced basis matrix V
9. For (T, V), do:
10. $U = T^{-1}$
11. $W = UV$
12. End for.
13. Produces d, k_i from W
14. Foe each $(e_i, d_i, k, h_i, \lambda_i)$, compute:
15. $\varphi(N_i) = \dfrac{e_i d_i - 1}{k}$
16. $\gcd(\varphi(N_i), N_i) := z_i$
17. $y_i = \lambda_i - h_i + 1$
18. End for.
19. Solve the quadratic equation $x^2 - y_i x + \lambda_i = 0$
20. Return primes p_i and q_i.

Example 2. This example gives an illustration on how Theorem 3.2 works on three (3) moduli and their corresponding public exponents

$$N_1 = 136467371751927836750733047418348826778197917829013555011249$$

$$N_2 = 552123272281578546794650992147964053929727952598211842032 81$$

$$\mathrm{N}_3 = 136806182389858847933585616740741619959962535859888617212 81$$

$$e_1 = 958746151299192165746133967977808029031186262934105946202 84$$

$$e_2 = 952833644207080352914075177283147075650208715778453348469 7$$

$$e_3 = 612066528648100622089801573335328786685255778363955830299 0$$

Let

$$h_1 = 369414904615294197607056331320$$

$$h_2 = 234973035108621316823221555560$$

$$h_3 = 116964175023746824780476061872$$

Observe that $N = \max\{N_1, N_2, N_3\}$

$$N = 136467371751927836750733047418348826778197917829013555011249$$

$$e = \min\{e_1, e_2, e_3\}$$

$$e = 612066528648100622089801573335328786685255778363955830299 0$$

By using $a = 3$, $b = 2$ and $j = 3$, then using algorithm 3.2 gives

$\gamma := \dfrac{n(\beta - \delta)}{(1+n)} = 0.1479006146$ and $\varepsilon = N^{\gamma+\delta-\beta} = 0.002104706729$

Applying Theorem 2.2 and algorithm 3.2 for $j = 3$ we compute

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

$$R = 2063900066000$$

Consider the lattice ℓ spanned by the matrix

$$T = \begin{bmatrix} 1 & -\lfloor R(M_1) \rfloor & -\lfloor R(M_2) \rfloor & -\lfloor R(M_3) \rfloor \\ 0 & R & 0 & 0 \\ 0 & 0 & R & 0 \\ 0 & 0 & 0 & R \end{bmatrix}$$

Therefore, by applying the LLL algorithm to ℓ it yields reduced basis with the following entries

$$V = \begin{pmatrix} -144617 & -14070 & -26262 & -136418 \\ 3162338255 & -8269496950 & 11848747930 & -4780639730 \\ -18849073876 & 36499368040 & 32041719064 & 10048971896 \\ -25815846094 & -35664332740 & -2319010484 & 31492112724 \end{pmatrix}$$

Next, from algorithm 3.2, $W = UV$

$$W = \begin{pmatrix} -144617 & -205847 & -837989 & -323241 \\ 3162338255 & 4501253952 & 18324295705 & 7068307183 \\ -18849073876 & -26829662558 & -109221713687 & -42130548198 \\ -25815846094 & -36746125773 & -149590954400 & -57702344173 \end{pmatrix}$$

From the first row of matrix W , the values of (k, d_1, d_2, d_3) are as follows

$K = 144617$ $d_1 = 205847$ $d_2 = 837989$ $d_3 = 323241$

Using algorithm 3.2, $\varphi(N_i) = \frac{e_i d_i - 1}{k}$ for $i = 1,2,3$ can be computed as follows:

$$\varphi(N_1) = 136467371751927373505427742870013794610580083023570470074760$$
$$\varphi(N_2) = 552123272281576203252807722284604946013983661344427240940 40$$
$$\varphi(N_3) = 136806182389857826662791753643406385374422621859216721783 52$$

Next, from algorithm 3.2 y_i can equally be computed in the following way

$y_1 = 1253997333396624$ $y_2 = 997366290215600$ $y_3 = 873148375265970$

Finally, solving the quadratic equation $x^2 - y_i x + \lambda_i = 0$ for i = 1, 2, 3 yields (p_1, q_1), (p_2, q_2) and (p_3, q_3) as follows:

$p_1 = 780987054007763$ $p_2 = 615780728797579$

$p_3 = 707927916709357$ $q_1 = 473010279388861$

$q_2 = 381585561418021$ $q_3 = 165220458556613$

4. Conclusion

The security of the RSA variant's generalized key equations of the form $e_i d - k_i \varphi(N_i) = 1$ and $e_i d_i - k\varphi(N_i) = 1$ have been found to be broken using simultaneous Diophantine approximation and lattice basis reduction technique. This pose a great challenge as it exposed the weak keys of the cryptosystem. The paper also demonstrated how the two attacks were practically carried out by given numerical examples.

Conflict of interest

The authors declare no conflict of interest.

Acknowledgement

This research team wishes to acknowledge the Sokoto State University for providing conducive environment and also TEFUND for funding researches in public tertiary institutions in Nigeria.

References

1. Wan Nur Aqlili Ruzai, Muhammad Rezal Kamel Ariffin, Muhammad Asyraf Asbullah, Amir Hamzah Abd Ghafar, New Simultaneous Diophantine Attacks on generalized RSA key Equations, Journal of King Sud University-Computer and Information Sciences, 36(5), 2024.
2. Kaur and Ramkumar R.K, The recent trends in cyber security: A review. King Saud univ. Comp. Inf. Sci., 34(8), 2022.
3. Nemec M., Sys M., Svend P., Klienec D., Matyas V. The Return of Coppersmith's attack: Practical factorization of widely used RSA moduli: Proceedings of the 2017 ACM-SIGASAC Conference on Computer and Communication Security, Assocition for Computing Machinery, New York USA (2017). Pp. 1631-1648.
4. AbdRahman, N.N., and Ariffin, M.R.K. (2016): New Practical Attack on RSA Modulus of $N = p^2 q$, *International journal of Pure and Applied Mathematics*, ***110*** **(4)**, 587 – 80.
5. Abubakar, S.I. (2020): Factoring of RSA modulus $N = pq$ using Small Prime Difference Method,*Ph.D. Thesis*, Universiti Putra Malaysia, Selangor, Malaysia,

6. Abubakar, S.I., Ariffin, M.R.K., and Asbullah, M.A. (2019): A New Improved Bound for Short Decryption Exponent on RSA modulus $N = pq$ using Wiener's Method, *Malaysian Journal of Mathematical Sciences* ***13(s)***, 89 -90.
7. Dogon Daji A.M., Sani B., Ibrahim A.A., Abubakar S.I, Cryptanalysis attack on multi prime power modulus through analyzing prime difference, International Journal of Science for Global Sustainability, 9(1) 2023.
8. Abubakar, S.I., Shehu, S., and Zaid (2021): Technique of factoring multi prime power modulus $N = p^2q^2$, *Caliphate Journal of Science and Technology (CaJoST),* (accepted).
9. Lenstra, A.K., Lenstra, H.W., and Lovasz, L. (1982): Factoring polynomials with rational coefficients, Mathemasche, Annelen. **261**,515 – 534.
10. Nitaj, A. (2013): Diophantine and Lattice Cryptanalysis of the RSA Cryptosystem. *In Artificial Intelligence,* Evolutionary Computing and Met heuristics; Springer: Berlin/Heidelberg, Germany, 139–168.

