Quest Journals
Journal of Research in Applied Mathematics
Volume 7 ~ Issue 8 (2021) pp: 20-33
ISSN(Online) : 2394-0743 ISSN (Print):2394-0735
www.questjournals.org

Research Paper

VulnerableAttacksof$N=p^rq$

SadiqShehu[1],SaiduIsahAbubakar[2],ZaidIbrahim[3]
[1,2,3]*DepartmentofMathematics,FacultyofScience*
SokotoStateUniversity,Sokoto,Nigeria

ABSTRACT

RSA is one of the most popular and accepted cryptosystems in the history of cryptology. Let $N = p^r q$ be an RSA prime power modulus for $r \geq 2$ and $q < p < 2q$. The study was present to factor the modulus $N = p^r q$ based on the RSA key equation $ex - y\phi(N) = 1$ where $\phi(N) = p^{r-1}(p-1)(q-1)$. For $\left|\left(2^{\frac{r-1}{r+1}}q^{\frac{r-1}{r+1}} - p^{\frac{r^2-r-1}{r+1}}\right)\right| p^{\frac{r}{r+1}}\left(p + 2^{\frac{1}{r+1}}p^{\frac{r^2-r}{r+1}}q^{\frac{1}{r+1}}\right) < \frac{1}{4}N^{\lambda+\kappa}$ with $d = N^{\alpha}$. If $\alpha < \frac{1-\lambda-\kappa}{2}$ we shows that $\frac{y}{x}$ is one of the convergents of the continued fractions expansions of $\frac{e}{N-\left(\left(2^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}\right)N^{\frac{r}{r+1}}-2^{\frac{r-1}{r+1}}N^{\frac{r-1}{r+1}}\right)}$.

The second part of this research consider two cryptanalytic attacks on ω instances of RSA moduli $N_i = p_i^r q_i$ for $i = 1, ..., \omega$ satisfying a variant of the form $e_i x - y_i\phi(N_i) = 1$ or of the form $e_i x_i - y\phi(N_i) = 1$ for the unknown positive integers x, x_i, y, y_i, applying the LLL algorithm on ω prime power public keys (N_i, e_i) we were able to factorize the ω prime power moduli $N_i = p_i^r q_i$ simultaneously in polynomial time.

Keywords: Prime Power, Factorization, LLL algorithm, Simultaneous diophantine approximations, Continued fraction

Received 06 August, 2021; Revised: 18 August, 2021; Accepted 20 August, 2021 © The author(s) 2021. Published with open access at www.questjournals.org

I. INTRODUCTION

In the RSA cryptosystem, the modulus $N = pq$ is a product of two primes of equal bit-size. Let e and x be two positive integers satisfying $ex \equiv 1 \bmod \phi(N)$ where $\phi(N) = (p-1)(q-1)$ is Euler's totient function. Commonly, N is called the RSA modulus, e the encryption exponent and x the decryption exponent. The modular equation $ex \equiv 1 \bmod \phi(N)$ is sometimes used as an equation $ex - y\phi(N) = 1$, where k is some positive integer, is called the RSA key equation. It is based on the dramatic difference between the ease of finding large prime numbers and computing modular powers on the one hand, and the difficulty of factorizing a product of large prime numbers as well as inverting the modular exponentiation [18].

In prime power, the modulus N is in the form $N = p^r q$ for $r \geq 2$. Takagi showed how to use the prime power to speed up the decryption process when the public and private exponents satisfy an equation $ex - y\phi(N) = 1$ [20]. As in the standard RSA cryptosystem, the security of the prime power depends on

the difficulty of factoring integers of the form $N = p^r q$.

As describe in Boneh, et al., (1999), the schemes with modulus of the form $N = p^r q$ are more susceptible to attacks that leak bits of p than the original RSA-scheme. Using Coppersmith's method for solving univariate modular equations, they showed that it suffices to know a fraction of $\frac{1}{r+1}$ of the MSBs of p to factor the modulus.
In 2007 Hinek, started to look at system of equations involving the moduli $N_i = p_i q_i$, he showed that it is possible to factor the ω modulus N_i using ω equations of the form $e_i x - y_i \phi(N_i) = 1$ if $x < N^\delta$ with $\delta = \frac{k}{2(k+1)} - \varepsilon$ where ε is a small constant depending on the size of max N_i [8].
Very recently, with ω RSA public keys (N_i, e_i), Nitaj, et al. presented a method that factor the k RSA moduli N_i using ω equations of the shape $e_i x - y_i \phi(N_i) = z_i$ or of the shape $e_i x_i - y\phi(N_i) = z_i$ where $N_i = p_i q_i$, $\phi(N_i) = (p_i - 1)(q_i - 1)$ and the parameters x, x_i, y, y_i, z_i are suitably small in terms of the prime factors of the moduli [13].
Asbullah (2015) proved that by taking the term $N - (2N^{2/3} - N^{1/3})$ as a good approximation of $\phi(N)$ satisfying the RSA key equation $ex - y\phi(N) = 1$, one can yield the factorization of the prime power modulus $N = p^r q$ for $r = 2$ in polynomial time.

Our contribution, The research, proposes two cryptanalytic attacks on the prime power modulus $N = p^r q$. First cryptanalytic attack, consider $N - \left(\left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) N^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}}\right)$ as a good approximation of $\phi(N)$ with public of exponent e satisfying the equation $ex - y\phi(N) = 1$ for some unknown integers $\phi(N)$, x,y. Hence using continued fraction we show that $\frac{y}{x}$ can be recovered among the convergents of the continued fractions expansions of $\frac{e}{N - \left(\left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) N^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}}\right)}$ which lead to the factorization of the modulus $N = p^r q$ in polynomial time.

The second cryptanalytic attacks consider the public key exponents (N_i, e_i) for the unknown integers x, x_i and ω integers y, y_i, and transform the equations into a simultaneous diophantine problem $e_i x - y_i \phi(N_i) = 1$ and $e_i x_i - y\phi(N_i) = 1$, from which we apply lattice basis reduction techniques so as to enable us to find the parameters (x, y_i) or (y, x_i) which leads to factorization of ω moduli N_i in polynomial time if $N = max_i\ N_i$ and

$$x < N^\alpha, \quad y_i < N^\alpha, \quad where \quad \alpha = \frac{\omega - \lambda\omega - \kappa\omega}{(\omega + 1)}$$

$$x_i < N^\alpha, \quad y < N^\alpha, \quad where \quad \alpha = \frac{\beta\omega - \lambda\omega - \kappa\omega}{(1 + \omega)}$$

The rest of the paper is organized as follows. In section 2, we present a brief review of some preliminary result for the continued fraction and lattice basis reduction, simultaneous diophantine approximations with some useful results needed for the attack. In section 3, 4 we put forward the first and second of our cryptanalytic attacks. We conclude this paper in section 5.

2. Preliminaries

In this section we state some basics definition concerning the continued fraction, lattice basis reduction techniques and simultaneous diophantine equations as will as some useful lemmas needed for the attacks.

Definition 2.1 (Continued Fraction). The continued fraction of a real number R is an expression of the form

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

Where $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{N} - 0$ for $i \geq 1$. The number $a_0, a_1, a_2....$ are called the partial quotients. We use the notation $R = [a_0, a_1, a_2....]$. For $i \geq 1$ the rational $\frac{r_i}{s_i} = [a_0, a_1, a_2, ...]$ are called the convergents of the continued fraction expansion of R. If $R = \frac{a}{b}$ is a rational number such that $gcd(a, b) = 1$, then the continued fraction expansion is finite.

Theorem 2.2. (Legendre). Let $x = [a_0, a_1, a_2, ...a_m]$ be a continued fraction expansion of x. If X and Y are coprime integers such that

$$\left| x - \frac{Y}{X} \right| < \frac{1}{2X^2}$$

Then $Y = p_n$ and $X = q_n$ for some convergent $\frac{p_n}{q_n}$ of x with $n \geq 0$.

2.3 Lattice

A lattice is a discrete (additive) subgroup of $\mathbb{R}^n$. Equivalently, given $m \leq n$ linearly independent vectors $v_1, ..., v_m \in \mathbb{R}^n$, the set

$$\mathcal{L} = \mathcal{L}(v_1, ..., v_m) = \left\{ \sum_{i=1}^{m} \alpha_i v_i | \alpha_i \in \mathbb{Z} \right\}.$$

is a lattice. The v_i are called basis vectors of $\mathcal{L}$ and $B = v_1, ..., v_m$ is called a lattice basis for $\mathcal{L}$. Thus, the lattice generated by a basis B is the set of all integer linear combinations of the basis vectors in B.

Theorem 2.4 Let L be a lattice of dimension ω with a basis $c_1, ..., c_\omega$. The LLL algorithm produces a reduced basis $v_1, ...v_\omega$ satisfying

$$\|v_1\| \leq \|v_2\| \leq ... \leq \|v_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} det\mathcal{L}^{\frac{1}{\omega+1-i}}$$

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

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

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

A method to find simultaneous diophantine approximations to rational numbers was described by [10] In their work, they considered a lattice with real entries.

Theorem 2.5 (Simultaneous Diophantine Approximations). There is a polynomial time algorithm, for given rational numbers $\alpha_1, ..., \alpha_n$ and $0 < \varepsilon < 1$, to compute integers $p_1, ..., p_n$ and a positive integer q such that

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

Proof. See [13] Appendix A.

3. First Cryptanalytic Attack on Modulus $N = p^r q$

We present our finding using continued fractions to factor the prime power modulus $N = p^r q$. Let (N, e) be a public key satisfying an equation satisfying an equation $ex - y\phi(N) = 1$ for some unknown integers $\phi(N)$, x,y.

Lemma 3.1. Let $N = p^r q$ be a prime power modulus with $q < p < 2q$. Then

$$2^{-\frac{r}{r+1}} N^{\frac{1}{r+1}} < q < N^{\frac{1}{r+1}} < p < 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$$

Proof. Let $N = p^r q$ and suppose $q < p < 2q$. Then multiplying by p^r we get $p^r q < p^r p < 2p^r q$ which implies $N < p^{r+1} < 2N$, that is $N^{\frac{1}{r+1}} < p < 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$. Also since $N = p^r q$, then $q = \frac{N}{p^r}$ which in turn implies $2^{-\frac{r}{r+1}} N^{\frac{1}{r+1}} < q < N^{\frac{1}{r+1}}$. Hence

$$2^{-\frac{r}{r+1}} N^{\frac{1}{r+1}} < q < N^{\frac{1}{r+1}} < p < 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$$

Let $N = p^r q$ therefore for $\phi(N) = p^{r-1}(p-1)(q-1)$ we compute the approximation of $\phi(N)$ using $p \approx 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$ and $q \approx N^{\frac{1}{r+1}}$

$$\begin{aligned}\phi(N) &= p^{r-1}(pq - p - q + 1)\\ &= p^r q - p^r - p^{r-1}q + p^{r-1}\\ &= N - (p^r + p^{r-1}q - p^{r-1})\end{aligned}$$

$$\begin{aligned}&N - \left((2^{\frac{1}{r+1}} N^{\frac{1}{r+1}})^r + (2^{\frac{1}{r+1}} N^{\frac{1}{r+1}})^{r-1} N^{\frac{1}{r+1}} - (2^{\frac{1}{r+1}} N^{\frac{1}{r+1}})^{r-1}\right)\\ &= N - \left((2^{\frac{r}{r+1}} N^{\frac{r}{r+1}}) + (2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}})(N^{\frac{1}{r+1}}) - (2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}})\right)\\ &= N - \left((2^{\frac{r}{r+1}} N^{\frac{r}{r+1}}) + (2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}+\frac{1}{r+1}}) - (2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}})\right)\\ &= N - \left(2^{\frac{r}{r+1}} N^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} N^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}}\right)\\ &= N - \left(\left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) N^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}}\right)\end{aligned}$$

Which is also a good approximation to $\phi(N)$.

□

Lemma 3.2 For $\phi(N) = N - (p^r + p^{r-1}q - p^{r-1})$, If $N = p^r q$ is a prime power modulus with $q < p < 2q$, then $\left|N - \left(\left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) N^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}}\right) - \phi(N)\right| < \left|2^{\frac{r-1}{r+1}} q^{\frac{r-1}{r+1}} - p^{\frac{r^2-r-1}{r+1}}\right| P^{\frac{r}{r+1}} \left(p + 2^{\frac{1}{r+1}} p^{\frac{r^2-r}{r+1}} q^{\frac{1}{r+1}}\right)$.

Proof. Let $N = p^r q$ be a prime power modulus and suppose that $\phi(N) = p^{r-1}(p-1)(q-1) = p^r q - p^r - p^{r-1}q + p^{r-1} = N - (p^r + p^{r-1}q - p^{r-1})$ Then

$$\begin{aligned}&\left|N - \left(\left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) N^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}}\right) - \phi(N)\right|\\ &= \left|N - \phi(N) - \left(\left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) N^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}}\right)\right|\\ &= \left|p^r + p^{r-1}q - p^{r-1} - \left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) N^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}}\right|\\ &= \left|p^r + p^{r-1}q - p^{r-1} - \left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) (p^r q)^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} (p^r q)^{\frac{r-1}{r+1}}\right|\\ &= \left|p^r + p^{r-1}q - p^{r-1} - \left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) p^{\frac{r^2}{r+1}} q^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} p^{\frac{r^2-r}{r+1}} q^{\frac{r-1}{r+1}}\right|\end{aligned}$$

$$= \left| p^r + p^{r-1}q - p^{r-1} - 2^{\frac{r}{r+1}} p^{\frac{r^2}{r+1}} q^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} p^{\frac{r^2}{r+1}} q^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} p^{\frac{r^2-r}{r+1}} q^{\frac{r-1}{r+1}} \right|$$

$$= \left| -2^{\frac{r}{r+1}} p^{\frac{r^2}{r+1}} q^{\frac{r}{r+1}} + p^{r-1}q - 2^{\frac{r-1}{r+1}} p^{\frac{r^2}{r+1}} q^{\frac{r}{r+1}} + p^r + 2^{\frac{r-1}{r+1}} p^{\frac{r^2-r}{r+1}} q^{\frac{r-1}{r+1}} - p^{r-1} \right|$$

$$= \left| 2^{\frac{r}{r+1}} p^{\frac{r^2}{r+1}} q^{\frac{r}{r+1}} - p^{r-1}q + 2^{\frac{r-1}{r+1}} p^{\frac{r^2}{r+1}} q^{\frac{r}{r+1}} - p^r - 2^{\frac{r-1}{r+1}} p^{\frac{r^2-r}{r+1}} q^{\frac{r-1}{r+1}} + p^{r-1} \right|$$

$$= \left| 2^{\frac{r+1}{r+1}} p^{\frac{2r+1}{r+1}} q^{\frac{r-1}{r+1}} + 2^{\frac{r}{r+1}} p^{\frac{r^2}{r+1}} q^{\frac{r}{r+1}} - 2^{-\frac{2}{r+1}} p^{\frac{r^2-1}{r+1}} q^{\frac{r+1}{r+1}} - 2^{\frac{r-1}{r+1}} p^{\frac{2r+1}{r+1}} q^{\frac{r-1}{r+1}} - p^r - 2^{\frac{r-1}{r+1}} p^{\frac{r^2}{r+1}} q^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} p^{\frac{r^2-r}{r+1}} \right.$$

$$= \left| \left(2^{\frac{r-1}{r+1}} q^{\frac{r-1}{r+1}} - p^{\frac{r^2-r-1}{r+1}} \right) p^{\frac{r}{r+1}} \left(p + 2^{\frac{1}{r+1}} p^{\frac{r^2-r}{r+1}} q^{\frac{1}{r+1}} - 2^{-\frac{(r-1)}{r+1}} p^{\frac{r^2-r-1}{r+1}} q^{\frac{2}{r+1}} - 1 \right) \right|$$

$$< \left| \left(2^{\frac{r-1}{r+1}} q^{\frac{r-1}{r+1}} - p^{\frac{r^2-r-1}{r+1}} \right) \right| p^{\frac{r}{r+1}} \left(p + 2^{\frac{1}{r+1}} p^{\frac{r^2-r}{r+1}} q^{\frac{1}{r+1}} \right)$$

Which terminate the proof.

Theorem 3.3 Suppose that $N = p^r q$ is a prime power modulus with $q < p < 2q$, and $e < \phi(N) < N - \left(\left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} \right) N^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}} \right)$ satisfying an equation $ex - y\phi(N) = 1$ for some unknown integers $\phi(N)$, x,y. If $\phi(N) > \frac{3}{4}N$ with $N > 4x$ and $\left| \left(2^{\frac{r-1}{r+1}} q^{\frac{r-1}{r+1}} - p^{\frac{r^2-r-1}{r+1}} \right) \right| p^{\frac{r}{r+1}} \left(p + 2^{\frac{1}{r+1}} p^{\frac{r^2-r}{r+1}} q^{\frac{1}{r+1}} \right) < \frac{1}{4} N^{\lambda+\kappa}$ where $\lambda < 1$, $\kappa < 1$ and $x < N^{\alpha}$. If $\alpha < \frac{1-\lambda-\kappa}{2}$, then

$$\left| \frac{e}{N - \left(\left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} \right) N^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}} \right)} - \frac{y}{x} \right| < \frac{1}{2x^2}$$

Proof. We write the equation $ed - k\phi(N) = 1$ as

$$\begin{aligned} ex - y(p^{r-1}(p-1)(q-1)) &= 1 \\ ex - y(p^{r-1}(pq - p - q + 1)) &= 1 \\ ex - y(p^{r-1}pq - p^{r-1}p - p^{r-1}q + p^{r-1}) &= 1 \\ ex - y(p^r q - p^r - p^{r-1}q + p^{r-1}) &= 1 \\ ex - y(N - (p^r + p^{r-1}q - p^{r-1})) &= 1 \\ ex - y(N - (N - \phi(N))) &= 1 \end{aligned}$$

Since $N - \phi(N) = p^r + p^{r-1}q - p^{r-1}$ then

$$ex - y\left(N - \left(\left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} \right) N^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}} \right) - (N - \phi(N)) \right) = 1$$

$$ex - y\left(N - \left(\left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} \right) N^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}} \right) \right) = 1 + y\left(N - \phi(N) - \left(\left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} \right) N^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}} \right) \right)$$

Divide by $x\left(\left(2^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}\right)N^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}N^{\frac{r-1}{r+1}}\right)$ we get

$$\begin{aligned}
&\left|\frac{e}{N-\left(2^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}\right)N^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}N^{\frac{r-1}{r+1}}}-\frac{y}{x}\right| \\
&=\left|\frac{e}{N-\left(2^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}\right)N^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}N^{\frac{r-1}{r+1}}}-\frac{e}{\phi(N)}+\frac{e}{\phi(N)}-\frac{y}{x}\right| \\
&\leq\left|\frac{e}{N-\left(2^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}\right)N^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}N^{\frac{r-1}{r+1}}}-\frac{e}{\phi(N)}\right|+\left|\frac{e}{\phi(N)}-\frac{y}{x}\right| \\
&\leq\left|\frac{e\phi(N)-e\left(N-\left(2^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}\right)N^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}N^{\frac{r-1}{r+1}}\right)}{\phi(N)\left(N-\left(2^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}\right)N^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}N^{\frac{r-1}{r+1}}\right)}\right|+\left|\frac{ex-y\phi(N)}{\phi(N)x}\right| \\
&\leq e\left|\frac{N-\left(2^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}\right)N^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}N^{\frac{r-1}{r+1}}-\phi(N)}{\phi(N)\left(N-\left(2^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}\right)N^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}N^{\frac{r-1}{r+1}}\right)}\right|+\frac{1}{\phi(N)x} \\
&\leq e\left|\frac{N-\left(2^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}\right)N^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}N^{\frac{r-1}{r+1}}-\phi(N)}{\phi(N)}\right|+\frac{1}{\phi(N)x}
\end{aligned}$$

For $e<\phi(N)<N-\left(2^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}\right)N^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}N^{\frac{r-1}{r+1}}-\phi(N)$ and $ex-y\phi(N)=1$, $\phi(N)>\frac{3}{4}N$ with $N>4x$, then we have $\phi(N)>\frac{3}{4}N>\frac{3}{4}\times 4x>3x$ from the theorem $\left|\left(2^{\frac{r-1}{r+1}}q^{\frac{r-1}{r+1}}-p^{\frac{r^2-r-1}{r+1}}\right)\right|p^{\frac{r}{r+1}}\left(p+2^{\frac{1}{r+1}}p^{\frac{r^2-r}{r+1}}q^{\frac{1}{r+1}}\right)<\frac{1}{4}N^{\lambda+\kappa}$ and $x<N^{\alpha}$ then

$$\begin{aligned}
&\left|\frac{N-\left(2^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}\right)N^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}N^{\frac{r-1}{r+1}}-\phi(N)}{\phi(N)}\right|+\frac{1}{\phi(N)x} \\
&<\frac{\left|\left(2^{\frac{r-1}{r+1}}q^{\frac{r-1}{r+1}}-p^{\frac{r^2-r-1}{r+1}}\right)\right|p^{\frac{r}{r+1}}\left(p+2^{\frac{1}{r+1}}p^{\frac{r^2-r}{r+1}}q^{\frac{1}{r+1}}\right)}{\phi(N)}+\frac{1}{\phi(N)x} \\
&<\frac{\frac{1}{4}N^{\lambda+\kappa}}{\frac{3}{4}N}+\frac{1}{3x^2} \\
&<\frac{1}{3}N^{\lambda+\kappa-1}+\frac{1}{3}N^{-2\alpha}
\end{aligned}$$

For the Theorem 2.2, to satisfy it is suffice to shows that if $\lambda+\kappa-1<-2\alpha$

then $\alpha < \frac{1-\lambda-\kappa}{2}$, that is if

$$\begin{aligned}\frac{1}{3}N^{\lambda+\kappa-1} + \frac{1}{3}N^{-2\alpha} &< \frac{1}{3}N^{\lambda+\kappa-1} + \frac{1}{3}N^{-2\times\frac{(1-\lambda-\kappa)}{2}} \\ &< \frac{1}{3}N^{\lambda+\kappa-1} + \frac{1}{3}N^{\lambda+\kappa-1} \\ &< \frac{1}{2x^2}\end{aligned}$$

Hence $\frac{y}{x}$ among the convergent of the continued fraction expansion of $\frac{e}{N-\left(2^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}\right)N^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}N^{\frac{r-1}{r+1}}}$

□

The following algorithm is designed to recover the prime factors for prime power modulus $N = p^r q$ in polynomial time.

Algorithm 1

Input: $N = p^r q$, with $q < p < 2q$ and public key (e, N) and Theorem (3.3).
Output: the prime factors p and q.
1: Compute the continued fraction expansion of $\frac{e}{N-\left(2^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}\right)N^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}N^{\frac{r-1}{r+1}}}$.
2: For each convergent $\frac{y}{x}$ of $\frac{e}{N-\left(2^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}\right)N^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}N^{\frac{r-1}{r+1}}}$, compute $\frac{ex-1}{y}$
3: Compute $p^{r-1} = gcd\left(N, \frac{ex-1}{y}\right)$
4: If $1 < p^{r-1} < N$, then $q = \frac{N}{p^r}$

Example 1. As an example to illustrate our attack for $r = 3$, $x = 8033$, $y = 3700$, let us take for N and e the numbers

$$N = 458495589823381314471544276605711 23$$

$$e = 211183078718127931904080956360016 97$$

Suppose that N and e satisfy all the condition stated in Theorem 3.3, then taking the continued fraction expansion of $\frac{e}{N-\left(2^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}\right)N^{\frac{r}{r+1}}+2^{\frac{r-1}{r+1}}N^{\frac{r-1}{r+1}}}$ we get,

$[0, 2, 5, 1, 5, 2, 5, 1, 1, 1, 1, 1, 4, 1, 1, 3, 2, 1, 2, 6, 2, 5, 2, 1, 1, 2, 1, 1, 4, 1, 1, 5, 2, 2, 6, 1, 1, 7, 2,]$
$[14, 7, 2, 5, 1, 44, 38, 7, 1, 51, 1, 1, 7, 1, 2, 4, 1, 16, 3, 1, 6, 1, 1, 9, 5, 2, 2, 29, 10, 2, 2]$

Applying the factorization algorithm with the convergent $\frac{y}{x} = \frac{3700}{8033}$, we obtain

$$\begin{aligned}\frac{ex-1}{y} &= \frac{(211183078718127931904080956360016 97)(8033)-1}{3700} \\ &= 458495586849384237023103330389193 60\end{aligned}$$

Hence we compute

$$p = \sqrt{gcd\left(N, \frac{ex-1}{y}\right)} = 605174881.$$

Finally for $p = 605174881$ we compute $q = \frac{N}{p^3} = 206867603$, which leads to the factorization of N.

4. Second Cryptanalytic Attacks on ω Moduli $N_i = p_i^r q_i$

Suppose that $N_i = p_i^r q_i$, $i = 1, ..., \omega$, for $\omega \geq 2$, $r \geq 2$, with ω instances (N_i, e_i) satisfying $e_i x - y_i \phi(N_i) = 1$, or relation of the form $e_i x_i - y\phi(N_i) = 1$, with unknown parameters x_i, y, x, y_i. We shows that the ω moduli N_i for $i = 1, ..., \omega$, can be factored in polynomial time if $N = max\ N_i$ and

$$x < N^{\alpha}, \quad y_i < N^{\alpha}, \quad where \quad \alpha = \frac{\omega - \lambda\omega - \kappa\omega}{(\omega + 1)},$$

$$x_i < N^{\alpha}, \quad y < N^{\alpha}, \quad \alpha = \frac{\beta\omega - \lambda\omega - \kappa\omega}{(1 + \omega)}$$

Theorem 4.1 Suppose that $N_i = p_i^r q_i$, $1 \leq i \leq \omega$ for $\omega \geq 2$, be ω moduli. Let $N = min\ N_i$ and e_i, $i = 1, ..., \omega$, be ω public exponents. Define $\alpha = \frac{\omega - \lambda\omega - \kappa\omega}{(\omega+1)}$ where $0 < \lambda \leq 1$. Let $e_i < \phi(N_i) < N_i - H$ where $H = \left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) N_i^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} N_i^{\frac{r-1}{r+1}}$. If there exist an integer $x < N^{\alpha}$ and ω integers $y_i < N^{\alpha}$ such that

$$e_i x - y_i \phi(N_i) = 1$$

for $i = 1, ..., \omega$, then one can factor the ω moduli $N_1, ..., N_\omega$ in polynomial time.

Proof. Suppose that $N_i = p_i^r q_i$, $1 \leq i \leq \omega$ be ω moduli for $\omega \geq 2$, and $r \geq 2$,. Let $N = min\ N_i$, and $y_i < N^{\alpha}$. Then we can rewrite the equation $e_i x - y_i \phi(N_i) = 1$ as

$$e_i x - y_i(N_i - (N_i - \phi(N_i))) = 1$$

$$e_i x - y_i(N_i - H + H - (N_i - \phi(N_i)) = 1$$

$$e_i x - y_i(N_i - H) = 1 - y_i(N_i - \phi(N_i) - H)$$

$$\left| \frac{e_i}{N_i - H} x - y_i \right| = \frac{|1 - y_i(N_i - \phi(N_i) - H)|}{N_i - H} \tag{1}$$

Let $N = min\ N_i$, and suppose that $y_i < N^{\alpha}$, and $|(N_i - \phi(N_i) - H)| < \left| \left(2^{\frac{r-1}{r+1}} q_i^{\frac{r-1}{r+1}} - p_i^{\frac{r^2-r-1}{r+1}}\right) \right| p_i^{\frac{r}{r+1}} \left(p_i + 2^{\frac{1}{r+1}} p_i^{\frac{r^2-r}{r+1}} q_i^{\frac{1}{r+1}}\right)$. Then

$$\begin{aligned}
\frac{|1 - y_i(N_i - \phi(N_i) - H)|}{N_i - H} &\leq \frac{|1 + y_i(N_i - \phi(N_i) - H)|}{N - H} \\
&< \frac{1 + N^{\alpha}\left(N_i - \left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) N_i^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} N_i^{\frac{r-1}{r+1}} - \phi(N)\right)}{\phi(N)} \\
&< \frac{1 + N^{\alpha}\left|\left(2^{\frac{r-1}{r+1}} q_i^{\frac{r-1}{r+1}} - p_i^{\frac{r^2-r-1}{r+1}}\right)\right| p_i^{\frac{r}{r+1}} \left(p_i + 2^{\frac{1}{r+1}} p_i^{\frac{r^2-r}{r+1}} q_i^{\frac{1}{r+1}}\right)}{\phi(N)} \\
&< \frac{N^{\alpha}(\frac{1}{4} N^{\lambda+\kappa})}{\frac{3}{4} N} \\
&< \frac{1}{3} N^{\alpha+\lambda+\kappa-1}
\end{aligned}$$

Plugging in to (1), to get

$$\left|\frac{e_i}{N_i - H}x - y_i\right| < \frac{1}{3}N^{\alpha+\lambda+\kappa-1}$$

Hence to shows the existence of the integer x, we let $\varepsilon = \frac{1}{3}N^{\alpha+\lambda+\kappa-1}$, with $\alpha = \frac{\omega-\lambda\omega-\kappa\omega}{(\omega+1)}$. Then we have

$$N^{\alpha}\varepsilon^{\omega} = \left(\frac{1}{3}\right)^{\omega} N^{\alpha+\alpha\omega+\lambda\omega-\kappa\omega-\omega} = \left(\frac{1}{3}\right)^{\omega}$$

Therefore since $\left(\frac{1}{3}\right)^{\omega} < 2^{\frac{\omega(\omega-3)}{4}} \cdot 3^{\omega}$ for $\omega \geq 2$, we get $N^{\alpha}\varepsilon^{\omega} < 2^{\frac{\omega(\omega-3)}{4}} \cdot 3^{\omega}$. It follows that if $x < N^{\alpha}$ then $x < 2^{\frac{\omega(\omega-3)}{4}} \cdot 3^{\omega} \cdot \varepsilon^{-\omega}$ summarizing for $i = 1, ..., \omega$, we have

$$\left|\frac{e_i}{N_i - H}x - y_i\right| < \varepsilon, \qquad x < 2^{\frac{\omega(\omega-3)}{4}} \cdot 3^{\omega} \cdot \varepsilon^{-\omega}$$

Hence Theorem 2.5, is satisfy and the unknown integers x and y_i for $i = 1, ..., \omega$ can be obtain. Next from the equation $e_i x - y_i\phi(N_i) = 1$ we get

$$\frac{e_i x - 1}{y_i} = \phi(N_i) = p^{r-1}(p-1)(q-1)$$

Therefore by computing $p_i^{r-1} = gcd\left(\frac{e_i x-1}{y_i}, N_i\right)$ leads to factorization of ω moduli $N_i, ..., N_\omega$. □

Let

$$\xi_1 = \frac{e_1}{N_1 - \left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) N_1^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} N_1^{\frac{r-1}{r+1}}}$$

$$\xi_2 = \frac{e_2}{N_2 - \left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) N_2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} N_2^{\frac{r-1}{r+1}}}$$

$$\xi_3 = \frac{e_3}{N_3 - \left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) N_3^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} N_3^{\frac{r-1}{r+1}}}$$

Example 2. Illustration to our attack on ω moduli, we consider the following three prime power and three public exponents

$N_1 = 928341199909994290732455365234942973217632709783985888749 97$

$N_2 = 1174901653049192383040523075729091734962538796695910699998 47$

$N_3 = 1022356009308111073911440091822917340215808728312793507646 43$

$e_1 = 7647354300421501813784765398161583149894707406045749302185 7$

$e_2 = 1571110809941992486405873410115969813108779185422778705137$

$e_3 = 6793277619057906483809985354490457049071977440005476277001 7$

Then $N = max(N_1, N_2, N_3) = 1174901653049192383040523075729091734962538796695910699998 47$. For $\omega = 3$ and $r = 3$ with $\lambda = 0.6927$, $\kappa = 0.12243$ we get $\delta = \frac{\omega-\lambda\omega-\kappa\omega}{(\omega+1)} = 0.1386525000$ and $\varepsilon = \frac{1}{3}N^{\alpha+\lambda+\kappa-1} = 0.0006205988269$. Using Theorem 2.5, we

obtained.

$$C = [3^{\omega+1} \cdot 2^{\frac{(\omega+1)(\omega-4)}{4}} \cdot \varepsilon^{-\omega-1}] = 273030536100000$$

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

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

Therefore applying the LLL algorithm to $\mathcal{L}$, we obtain the reduced basis with following matrix

$$K = \begin{bmatrix} 10051167073 & 11435870083 & 8947157134 & 7987573842 \\ -21757124738 & 45676506202 & 9014673796 & -51529437252 \\ 86233011652 & -58001813108 & 20484851416 & -33435255192 \\ -46334050577 & -28503478067 & 129626888434 & -34165974258 \end{bmatrix}$$

Next we compute

$$K \cdot M^{-1} = \begin{bmatrix} 10051167073 & 8279804424 & 134406971 & 6678727146 \\ -21757124738 & -17922768207 & -290942257 & -14457017633 \\ 86233011652 & 71035777854 & 1153131553 & 57299490857 \\ -46334050577 & -38168391209 & -619591670 & -30787716404 \end{bmatrix}$$

Then from the first row we obtained $x = 10051167073$, $y_1 = 8279804424$, $y_2 = 134406971$, $y_3 = 6678727146$. Hence using x and y_i for $i = 1, 2, 3$, define $G_i = \frac{e_i x - 1}{y_i} = \phi(N_i) = p^{r-1}(p-1)(q-1)$

$$G_1 = 928341199909984118387229329549094181475962197155108509574 40$$

$$G_2 = 1174901653049179712514770899313240300384488622673387595740 00$$

$$G_3 = 1022356009308104573529528323409492037427111936277653647614 40$$

Therefore for $i = 1, 2, 3$ we compute $p_i = \sqrt{gcd\left(\frac{e_i x - 1}{y_i}, N_i\right)}$, that is

$$p_1 = 973239535413133, p_2 = 1049228426328463, p_3 = 805770174557867$$

And finally for $i = 1, 2, 3$ we find $q_i = \frac{N_i}{p_i^3}$, hence

$$q_1 = 100704388509281, q_2 = 101716491133001, q_3 = 195419811496561$$

Which leads to the factorization of three moduli N_1,N_2,and N_3.

Theorem 4.2. Suppose that $N_i = p_i^r q_i$, $1 \leq i \leq \omega$ be ω moduli with the same size N. Let e_i, $i = 1, ..., \omega$, be ω public exponents with $min\ e_i = N^\beta$, $0 < \beta < 1$. Let $\alpha = \frac{\beta\omega - \lambda\omega - \kappa\omega}{(1+\omega)}$here $0 < \lambda \leq 1$. If there exist an integer $y < N^\alpha$

and ω integers $x_i < N^\alpha$ such that $e_i x_i - y\phi(N_i) = 1$ for $i = 1, ..., \omega$, then one can factor the ω moduli $N_1, ...N_\omega$ in polynomial time.

Proof. Suppose that $N_i = p_i^r q_i$, $1 \leq i \leq \omega$ be ω moduli for $\omega \geq 2$, and $r \geq 2$. Then we transform $e_i x_i - y\phi(N_i) = 1$ as

$$\left| \frac{N_i - H}{e_i} y - x_i \right| = \frac{|1 - y(N_i - \phi(N_i)) - H|}{e_i} \qquad (2)$$

Let $N = max\ N_i$, and suppose that $y < N^{\alpha}$, $min\ e_i = N^{\beta}$ and $|(N_i - \phi(N_i) - H)| < \left|\left(2^{\frac{r-1}{r+1}} q_i^{\frac{r-1}{r+1}} - p_i^{\frac{r^2-r-1}{r+1}}\right)\right| p_i^{\frac{r}{r+1}} \left(p_i + 2^{\frac{1}{r+1}} p_i^{\frac{r^2-r}{r+1}} q_i^{\frac{1}{r+1}}\right)$.Then

$$\begin{aligned}
\frac{|1 - y(N_i - \phi(N_i) - H)|}{e_i} &\leq \frac{|1 + y(N_i - \phi(N_i) - H)|}{N^{\beta}} \\
&< \frac{1 + N^{\delta}\left|\left(2^{\frac{r-1}{r+1}} q_i^{\frac{r-1}{r+1}} - p_i^{\frac{r^2-r-1}{r+1}}\right)\right| p_i^{\frac{r}{r+1}} \left(p_i + 2^{\frac{1}{r+1}} p_i^{\frac{r^2-r}{r+1}} q_i^{\frac{1}{r+1}}\right)}{N^{\beta}} \\
&< \frac{N^{\alpha}(\frac{1}{4}N^{\lambda+\kappa})}{N^{\beta}} \\
&< \frac{1}{4}N^{\alpha+\lambda+\kappa-\beta}
\end{aligned}$$

Plugging in to (2), to get

$$\left|\frac{N_i - \psi}{e_i} y - x_i\right| < \frac{1}{4}N^{\alpha+\lambda+\kappa-\beta}$$

For the unknown integers y, x_i, we let $\varepsilon = \frac{1}{4}N^{\alpha+\lambda+\kappa-\beta}$, with $\alpha = \frac{\beta\omega-\lambda\omega-\kappa\omega}{(1+\omega)}$. Then we have

$$N^{\alpha}\varepsilon^{\omega} = \left(\frac{1}{4}\right)^{\omega} N^{\alpha+\alpha\omega+\lambda\omega-\beta\omega} = \left(\frac{1}{4}\right)^{\omega}$$

Therefore since $\left(\frac{1}{4}\right)^{\omega} < 2^{\frac{\omega(\omega-3)}{4}} \cdot 3^{\omega}$ for $\omega \geq 2$, we get $N^{\alpha}\varepsilon^{\omega} < 2^{\frac{\omega(\omega-3)}{4}} \cdot 3^{\omega}$. It follows that if $y < N^{\alpha}$ then $y < 2^{\frac{\omega(\omega-3)}{4}} \cdot 3^{\omega} \cdot \varepsilon^{-\omega}$ summarizing for $i = 1, ..., \omega$, we have

$$\left|\frac{N_i - H}{e_i} y - x_i\right| < \varepsilon, \qquad y < 2^{\frac{\omega(\omega-3)}{4}} \cdot 3^{\omega} \cdot \varepsilon^{-\omega}$$

Which satisfy Theorem 8, and we can obtain the unknown integers y and x_i for $i = 1, ..., \omega$. Next from the equation $e_i x_i - y\phi(N_i) = 1$ we get

$$\frac{e_i x_i - 1}{y} = \phi(N_i) = p_i^{r-1}(p_i - 1)(q_i - 1)$$

Therefore by computing $p_i^{r-1} = \left(\frac{e_i x_i - 1}{y}, N_i\right)$ leads to factorization of n prime power moduli $N_i, ..., N_{\omega}$. □

Let

$$\xi_1 = \frac{N_1 - \left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) N_1^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} N_1^{\frac{r-1}{r+1}}}{e_1}$$

$$\xi_2 = \frac{N_2 - \left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) N_2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} N_2^{\frac{r-1}{r+1}}}{e_2}$$

$$\xi_3 = \frac{N_3 - \left(2^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}}\right) N_3^{\frac{r}{r+1}} + 2^{\frac{r-1}{r+1}} N_3^{\frac{r-1}{r+1}}}{e_3}$$

Example 3. As an illustration to our attack on j moduli, we consider the following three prime power and three public exponents

$$N_1 = 576368854286072552732993676292162968993090466390722140264 87$$

$$N_2 = 125540335187551827855109380266951398925768981505296611543087$$

$$N_3 = 240186170434146331525450410273159000180343864860931245777863$$

$$e_1 = 769023589883942484484013625385529960256346369870428118313690$$

$$e_2 = 753983599731561399576153151492532227137545413538055121385040$$

$$e_3 = 773736998802267434448670530004044440902084785945909743038 51$$

Then $N = max(N_1, N_2, N_3) = 240186170434146331525450410273159000180343864860931245777863$. Also $min(e_1, e_2, e_3) = N^{\beta}$ with $\beta = 0.9999$ For $\omega = 3$ and $r = 3$ with $\kappa = 0.3432$, $\lambda = 0.4327$, we get $\alpha = \frac{\beta\omega - \lambda\omega - \kappa\omega}{(1+\omega)} = 0.1680000000$ and $\varepsilon = \frac{1}{4}N^{\alpha+\lambda+\kappa-\beta} = 0.0001182032236$. Using Theorem 8, with $n = j = 3$, we obtained.

$$C = [3^{n+1} \cdot 2^{\frac{(n+1)(n-4)}{4}} \cdot \varepsilon^{-n-1}] = 207461608400000000$$

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

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

Therefore applying the LLL algorithm to $\mathcal{L}$, we obtain the reduced basis with following matrix

$$K = \begin{bmatrix} -5532261737 & 948039897921 & 313793070313 & 7531989267121 \\ -3320877029800 & -1353380776600 & -4633361459800 & -3021047096600 \\ 2401296503990 & 9342022006330 & -5290000899510 & -2962293677670 \\ 15375269038166 & -6714117170278 & -7611550523734 & 3970888144122 \end{bmatrix}$$

Next we compute

$$K \cdot M^{-1} = \begin{bmatrix} -5532261737 & -414632711 & -921136737 & -17173442171 \\ -3320877029800 & -248893546839 & -552935124300 & -10308783701763 \\ 2401296503990 & 179972699539 & 399822447203 & 7454189372656 \\ 15375269038166 & 1152347771439 & 2560024421403 & 47728452890173 \end{bmatrix}$$

Then from the first row we obtained $y = 5532261737$, $x_1 = 414632711$, $x_2 = 921136737$, $x_3 = 17173442171$. Hence using x_i and y for $i = 1, 2, 3$, define $G_i = \frac{e_i x_i - 1}{y} = \phi(N_i) = p_i^{r-1}(p_i - 1)(q_i - 1)$

$$G_1 = 576368854286062582417694467904638669471561826602681451235 60$$

$$G_2 = 125540335187551258029122944400939831305892068355651575680096$$

$$G_3 = 240186170434145459686893635756705659314071968044721498433640$$

Therefore for $i = 1, 2, 3$ we compute $p_i = \sqrt{gcd\left(\frac{e_i x_i - 1}{y}, N_i\right)}$, that is

$$p_1 = 978944784719861, p_2 = 736406367949009, p_3 = 836146835627221$$

And finally for $i = 1, 2, 3$ we find $q_i = \frac{N_i}{p_i^3}$, hence

$$q_1 = 61436421782227, q_2 = 314362459443103, q_3 = 410866134500483$$

Which leads to the factorization of three prime power moduli N_1,N_2,and N_3.

6. Conclusion

In this research we proposed cryptanalytic attacks using the modulus $N = p^r q$, $r \geq 2$ to we show that $\frac{y}{x}$ can be recovered among the convergents of the continued fraction expansion of $\frac{e}{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}}}$ which lead factorization of prime power modulus $N = p^r q$ in polynomial time as $N - \left(2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}}\right)$ as a good approximation of $\phi(N_i)$. Furthermore, it has been shows that by transforming the generalizing key equations $e_i x - y_i \phi(N_i) = 1$, $e_i x_i - y \phi(N_i) = 1$, where the parameters x, x_i, y, y_i, are unknown, $i = 1, ..., \omega$ into a simultaneous Diophantine approximations and applied the LLL algorithm with lattice basis reduction techniques for $\omega \geq 2$, $r \geq 2$, yield the factorization of ω prime power moduli $N_i = p_i^r q_i$, $i = 1, ..., \omega$ simultaneously in polynomial time

References

1. Asbullah, M. A., and M. R. K. Ariffin. New Attacks on RSA with Modulus $N = p^2 q$ Using Continued Fractions. Journal of Physics: Conference Series. Vol. 622. No. 1. IOP Publishing, (2015).
2. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$, Advances in Cryptology - Eurocrypt'99, Lecture Notes in Computer Science Vol. 1592, Springer-Verlag, 1-11 (1999)
3. Blomer, J., May, A.: A generalized Wiener attack on RSA. In Public Key Cryptography - PKC 2004, volume 2947 of Lecture Notes in Computer Science, 1-13. Springer-Verlag (2004)
4. Chen C. Y, Hsueh C. C. and Lin Y. F. A Generalization of de Wegers Method In the 5th IAS/IEEE International Conference on Information Assurance and Security (IAS 2009) pp. 344-347.
5. de Weger B (2002) Cryptanalysis of RSA with Small Prime Difference Applicable Algebra in Engineering Communication and Computing 13(1) pp. 1728.
6. Howgrave-Graham, N., Seifert, J.-P.: Extending Wieners attack in the presence of many decrypting exponents. In Secure Networking- CQRE (Secure)'99, LNCS 1740, 153-166, Springer-Verlag (1999)
7. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Oxford University Press, London (1975).
8. Hinek, J.: On the Security of Some Variants of RSA, Phd. Thesis, Waterloo, Ontario, Canada (2007)
9. Hinek, M. Jason. "Lattice attacks in cryptography: A partial overview." School of Computer Science, University of Waterloo, Canada (2004).
10. Lenstra, A.K. , Lenstra, H.W., L. Lovasz, L.: Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, 513-534, (1982)

11. May, A.: New RSA Vulnerabilities Using Lattice Reduction Methods. PhD. thesis, University of Paderborn (2003)

12. Maitra, S. and Sarkar, S. Revisiting wieners attackew weak keys in RSA. In International Conference on Information Security, pages 22843. (2008) Springer.

13. Nitaj, A., Ariffin, M. R. K., Nassr, D. I., and Bahig, H. M. New Attacks on the RSA Cryptosystem, Progress in Cryptology-AFRICACRYPT 2014. Springer International Publishing, 178-198. (2014)

14. Nitaj, Abderrahmane. Diophantine and Lattice Cryptanalysis of the RSA Cryptosystem. Artificial Intelligence, Evolutionary Computing and Metaheuristics. Springer Berlin Heidelberg, 139-168 (2013)

15. Nitaj, Abderrahmane. Cryptanalysis of RSA Using the Ratio of the Primes." Progress in Cryptology-AFRICACRYPT 2009. Springer Berlin Heidelberg, 98-115 (2009)

16. Nitaj, Abderrahmane, and Tajjeeddine Rachidi.: New Attacks on RSA with Moduli $N = p^r q$. Codes, Cryptology, and Information Security. Springer International Publishing, 2015. 352-360.

17. Nitaj, Abderrahmane.: A New Vulnerable Class of Exponents in RSA. (2011).

18. Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21.2 (1978): 120-126.

19. Sarkar, S.: Small secret exponent attack on RSA variant with modulus $N = p^r q$, Designs, Codes and Cryptography, Volume 73, Issue 2 , pp 383-392 (2015)

20. Takagi, T.: Fast RSA-type cryptosystem modulo $p^k q$. In Advances in Cryptology-Crypto'98, pp. 318-326. Springer, (1998)

21. Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, 553-558 (1990)

Declarations':

. Availabilityofdataandmaterials

Datasharingnotapplicabletothisarticleasnodatasetsweregeneratedoranalyzedduringthecurrentstudy.

.Funding

Notapplicable.

.Competinginterests

Theauthorsdeclarethattheyhavenocompetinginterests.

.Authorscontributions

SS. Proposed the research idea and drafted the manuscript. SIA. Participatedin all the algebra of this research while ZI. Used maple software to generate alltheexamplesinthisresearch.

.Acknowledgments

Notapplicable.