Journal of Applied Mathematics and Computation, 2020, 4(4), 230-240
https://www.hillpublisher.com/journals/JAMC/
ISSN Online: 2576-0653
ISSN Print: 2576-0645

Polynomial Time Attacks for Modulus $N = p^2q^2$

Sadiq Shehu, Saidu Isah Abubakar*, Zaid Ibrahim

Department of Mathematics, Faculty of Science, Sokoto State University, Sokoto, Nigeria.

How to cite this paper: Sadiq Shehu, Saidu Isah Abubakar, Zaid Ibrahim. (2020) Polynomial Time Attacks for Modulus $N = p^2 q^2$. *Journal of Applied Mathematics and Computation*, 4(4), 230-240.
DOI: 10.26855/jamc.2020.12.014

Received: October 20, 2020
Accepted: November 25, 2020
Published: December 18, 2020

***Corresponding author:** Saidu Isah Abubakar, Department of Mathematics, Faculty of Science, Sokoto State University, Sokoto, Nigeria.
Email: siabubakar82@gmail.com

Abstract

This research proposes three polynomial time attacks on prime power modulus $N = p^2q^2$. In the first attack, we show that if $q^2 < p^2 < 2q^2$, then the decryption exponent $d < \frac{1}{2}(N + 2^{\frac{1}{4}}N^{\frac{1}{2}} - \left(2^{\frac{1}{2}}N^{\frac{3}{4}} + 2^{\frac{1}{4}}N^{\frac{3}{4}}\right))N^{-\delta}$ can be found from the convergent of the continued fraction expansion of $\frac{e}{N+2^{\frac{1}{4}}N^{\frac{1}{2}}-\left(2^{\frac{1}{2}}N^{\frac{3}{4}}+2^{\frac{1}{4}}N^{\frac{3}{4}}\right)}$ where approximation of $\varphi(N)$ is prove to be $\varphi(N) = N + 2^{\frac{1}{4}}N^{\frac{1}{2}} - \left(2^{\frac{1}{2}}N^{\frac{3}{4}} + 2^{\frac{1}{4}}N^{\frac{3}{4}}\right)$. We present second and third attacks on j multi prime power moduli $N_m = p_m^2 q_m^2$ by transforming system of equation $e_m d - k_m \varphi(N_m) = 1$ and $e_m d_m - k\varphi(N_m) = 1$ into simultaneous Diophantine approximation problem from which we apply lattice basis reduction techniques to find unknown integers (d, k_m) and (d_m, k), which leads to successful factorization of j moduli N_m in polynomial time for $m = 1, 2, \ldots \ldots, j$.

Keywords

Polynomial Time, Prime power, Modulus Attacks, Approximation, Continued fractions, LLL

1. Introduction

Before the invention of public key cryptography, the only secure medium of communication for users was through symmetric cryptography also known as private key cryptography, which was found to have a drawback of key distribution. This changed in 1976, when Diffie and Hellman introduced a method for secret key agreement over a public channel [1]. The simplest version of the Diffie-Hellman key exchange protocol uses a multiplicative group of integers modulo p and a generator g.

The security of Diffie-Hellman key exchange is based on the Computational Diffie-Hellman (CDH) assumption, which states that it is hard to compute g^{ab} mod p when p, g, g^a mod p and g^b mod p are given. The CDH assumption is related to the Discrete Logarithm Problem (DLP), which states that it is very hard to compute a when p, g and $A = g^a$ mod p are given [2]. However, this simple version of Diffie-Hellman key exchange does not provide authentication of the origin of information. Hence, it is vulnerable to a man-in-the-middle attack.

The problem of providing secret communication over insecure medium is the most traditional and basic problem of cryptography. The setting consists of two parties communicating over a channel that possibly may be tapped by an adversary, the parties wish to exchange information with each other, but keep the adversary as ignorant as possible regarding the contents of this information. To this end, Public Key Cryptography is a protocol allowing these parties to communicate secretly with each other.

Typically, public key cryptography consists of a pair of algorithms called encryption algorithm used by the party sending the message, while the other called decryption algorithm which is used by the receiver. Hence in order to send a message, the sender first applies the encryption algorithm to the message and sends the result, called the ciphertext over the channel. Upon receiving the ciphertext, the receiver will applies the decryption algorithm to the ciphertext and retrieve the original

message called plaintext.

The RSA cryptosystem is the first published public key cryptosystem, developed by Rivest, Shamir and Adleman, presented in their article 1978, based on the Di e-Hellman proposal, and it has been the most popular and successful public key cryptosystem in used today [3].

The attacks are based on the mathematical structure of the RSA cryptosystem (the form of modulus or the key equation) and exploit certain parameter choices.

In recent years there were a number of proposed cryptosystems that rely on the difficulty of factoring modulus of the form $N = p^2q$. One of such was Fujioke, Okamoto, and Miyaguchi (1997) that used the prime power modulus $N = p^2q$ in an electronic cash scheme [4]. Okamoto and Uchiyama (1998) developed a public-key cryptosystem that is provably as secure as factoring a prime power modulus of the form $N = p^2q$ [5].

In 2001, HIME (R) Cryptosystem (Nishioka, Satoh, and Sakurai) proposed a cryptosystem based on modular squaring $N = p^2q$ instead of $N = pq$ and utilize his proposed method over Z_N to solve the decryption process. Previously, a modified RSA scheme was proposed that utilizes such N and applies the original method to make the decryption speed of RSA faster. The original method was done over Z_p^2 after Z_N is divided into Z_p^2 and Z_q by using the Chinese Remainder Theorem (CRT), and the values on Z_p^2 and Z_q were combined on Z_N by using CRT [6].

In 2013, Ariffin et al. introduced a new scheme based on the hardness of factoring integers of the shape $N = p^2q$. Their scheme uses a combination of modular linear and modular squaring. They showed that the decryption is 1-to-1 which is of great advantage over Rabin's cryptosystem. Its encryption speed has a complexity order faster than RSA and ECC. For decryption its speed is better than RSA and is marginally behind ECC [7].

In 2014, Sarkar proved that using the lattice reduction techniques, if the decryption exponent $d\ N^{0:395}$, then one can factor the prime power modulus $N = p^2q$ in polynomial time [8]. Asbullah (2015) proved that by taking the term $N - (2N^{\frac{2}{3}} - N^{\frac{1}{3}})$ as a good approximation of $\varphi(N)$ satisfying the RSA key equation $ed - k\varphi(N) = 1$, one can yield the factorization of the prime power modulus $N = p^2q$ in polynomial time [9].

As motivated by the works of [4], [5], [9] and [12], we propose a polynomial time attacks using both continued fractions expansion and lattice basis reduction techniques to show that the multi prime power modulus $N = p^2q^2$ can be factored in polynomial time without any prior information to attacker. Other researches that exploited the generalization of Takagi's cryptosystem with moduli $N = p^rq^s$ for gcd(r,s) = 1 using Coppersmith lattice reduction method can be found in [10] and [11].

This research considers multi prime power modulus of the shape $N = p^2q^2$ using continued fractions method. Given public exponents (e, N), we show that private keys ((N), d, k) can be found such that $ed - k\varphi(N) = 1$ is satisfied. This is done by choosing right $\frac{k}{d}$ from the convergent of the continued fractions expansion of $\frac{e}{N+2^{\frac{1}{4}}N^{\frac{1}{2}}-\left(2^{\frac{1}{2}}N^{\frac{3}{4}}+2^{\frac{1}{4}}N^{\frac{3}{4}}\right)}$ which leads to the successful factorization of modulus $N = p^2q^2$ in polynomial time.

In the second attack, we prove that for public keys(N_m, e_m, h_m) there exists an unknown integer (d, k_m) such that $e_m d - k_m \varphi(N_m) = 1$ holds where $d, k_m < N^{\omega}$, for $\omega = \frac{j(4\epsilon+1)}{4(j+1)}$. Similarly, in the third attack, we exploit the security of $e_m d_m - k\varphi(N_m) = 1$ by taking $d_m, k < N^{\Upsilon}$ where $\Upsilon = \frac{j(4\alpha-3)}{4(j+1)}$ for $N = \min\{N_m\}, \min\{e_m\} = N^{\alpha}$ and $m = 1, 2, \ldots\ldots, j$.

The rest of the research is organized as follows. In section 2, we give a brief review of basic facts about the continued fraction, theorems related to lattice basis reduction and simultaneous Diophantine approximations. In section 3, we present the findings of this research work. We conclude the paper in section 4.

2. Preliminaries

We start with definitions as well as important results concerning the continued fraction, lattice basis reduction technique and simultaneous Diophantine equations.

Definition 2.1. (Public Key Cryptography) [2]

Let M denote the message space, C denote the ciphertext space, K denote the key space, m denote the plaintext and c denote the ciphertext. The public key cryptography is defined as follows:

1. The randomized key generation algorithm K (takes no inputs and) returns a pair (e, d) of keys, the public key and matching secret key, respectively.
2. The encryption algorithm E takes the public key e and a plaintext message m ϵ M to return a value called the ciphertext c ϵ C. We write $C = E_e(M)$
3. The deterministic decryption algorithm D takes the secret key d and a ciphertext c ϵ C to return a plaintext message m

ϵ M. We write M = $D_d(C) = D_d(E_e(M))$.

Definition 2.2. (Continued fraction). A continued fraction is an expression of the form $[x_0, x_1, \dots, x_m, \dots] =$

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{\ddots + \cfrac{1}{x_m + \ddots}}}$$

where x_0 is an integer and x_n are positive integers for $n \geq 1$. The x_n are called the partial quotients of the continued fraction.

Definition 2.3. (Convergent) Let $y \in \mathbb{R}$ with $y = [x_0, x_1, \dots, x_m]$. For $0 \leq n \leq m$, the n^{th} convergents of the continued fraction expansion of y is $[x_0, x_1, \dots, x_n]$.

Theorem 2.4. *(Legendre). Let* $\propto$ *be a real positive number. If* u *and* v *are positive integers such that* $\gcd(u, v) = 1$ *and*

$$\left| \propto - \frac{v}{u} \right| < \frac{1}{2u^2}$$

then $\frac{v}{u}$ *is a convergent of the continued fraction expansion of* $\propto$.

Definition 2.5. (Lattices) Let $m \leq n$ be two positive integers and $b_1, \dots, b_m \in \mathbb{R}^n$ be n linearly independent vectors. A lattice $\mathcal{L}$ spanned by $\{b_1, \dots, b_m\}$ is the set of all integer linear combinations of $b_1, \dots, b_m$, that is

$\mathcal{L} = \mathcal{L}(b_1, \dots, b_m) = \{\sum_{-=1}^{m} \propto_i b_i | \propto_i \in \mathbb{Z}\}$.

The b_i are called basis vectors of $\mathcal{L}$ and B is the set of all integer linear combinations of the basis vectors in B.

Theorem 2.6. *Let L be a lattice of dimension* ω *with a basis* $v_1, \dots, v_\omega$. *The LLL algorithm produces a reduced basis* $b_1, \dots, b_\omega$ *satisfying*

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

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

Remark 2.7. One of the application of the LLL algorithm is that it provides a solution to the simultaneous Diophantine approximations problem which is defined as follows. Let $\propto_1, \dots, \propto_n$ be n real numbers and ε is a real number such that $0 < \varepsilon < 1$. A classical theorem of Dirichlet asserts that there exist integers $p_1, \dots, p_n$ and a positive integer $q \leq \varepsilon^{-n}$ such that

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

A method to find simultaneous Diophantine approximations to rational numbers was described by [13]. In their work, they considered a lattice with real entries. Below is a similar result for a lattice with integer entries.

Theorem 2.8. (Simultaneous Diophantine Approximations). There is a polynomial time algorithm, for given rational numbers $\propto_1, \dots, \propto_n$ and $0 < \varepsilon < 1$, to compute integers $p_1, \dots, p_n$ and a positive integer q such that

$$\max|q \propto_i - p_i| < \varepsilon \text{ and } q \leq 2^{\frac{n(n-3)}{4}}$$

Proof. See [14] Appendix A.

3. Results

In this section, we present our research finding into two parts. In the first part, we consider the polynomial attack of factoring $N = p^2q^2$ using continued fractions, while second part reports two cases of factoring m prime power moduli $N_m = p_m^2 q_m^2$ for $m = 1, 2, \dots, j$.

3.1 First Approach on Multi Prime Power Modulus $N = p^2q^2$

In this section, we present our result based on continued fraction on how to factor the multi prime power modulus $N = p^2q^2$ for some unknown parameters $\varphi(N)$, d, k using approximation of $\varphi(N) = N + 2^{\frac{1}{4}}N^{\frac{1}{2}} - \left(2^{\frac{1}{2}}N^{\frac{3}{4}} + 2^{\frac{1}{4}}N^{\frac{3}{4}}\right)$, where (N, e) are public keys satisfying $ed - k\varphi(N) = 1$.

Lemma 3.1. *Let* $N = p^2q^2$ *be a prime power modulus. If* $q^2 < p^2 < 2q^2$, *then*

$$2^{-1/4}N^{1/4} < q < N^{1/4} < p < 2^{1/4}N^{1/4}$$

and

$$\varphi(N) = N + 2^{1/4}N^{1/2} - \left(2^{1/2}N^{3/4} + 2^{1/4}N^{3/4}\right)$$

Proof. Let $N = p^2q^2$and suppose $q^2 < p^2 < 2q^2$. Then multiplying by p^2 we get $p^2q^2 < p^2p^2 < 2p^2q^2$ which implies $N < p^4 < 2N$, that is $N^{\frac{1}{4}} < p < 2^{1/4}N^{1/4}$. Also, since $N = p^2q^2$, then $q^2 = \frac{N}{p^2}$ which in turn implies $2^{-1/4}N^{\frac{1}{4}} < q < N^{1/4}$.

Hence,

$$2^{-1/4}N^{1/4} < q < N^{1/4} < p < 2^{1/4}N^{1/4}$$

Let $N = p^2q^2$ where $\varphi(N) = p^{2-1}q^{2-1}(p-1)(q-1)$we compute the approximation of $\varphi(N)$ with $p \approx N^{\frac{1}{4}}$, $q \approx 2^{\frac{1}{4}}N^{\frac{1}{4}}$ as follows:

$$\begin{aligned}\varphi(N) &= p^{2-1}q^{2-1}(pq - p - q + 1)\\ &= p^2q^2 - p^2q - pq^2 + pq\\ &= N - (p^2q + pq^2 - pq)\\ &= N + pq - (p^2q + pq^2).\end{aligned}$$

Using $p \approx N^{\frac{1}{4}}$, $q \approx 2^{\frac{1}{4}}N^{\frac{1}{4}}$ gives:

$$\begin{aligned}\varphi(N) &= N + 2^{1/4}N^{2/4} - \left(\left(2^{1/4}N^{1/4}\right)^2 + \left(2^{1/4}N^{1/4}\right)\left(N^{1/4}\right)^2\right)\\ &= N + 2^{1/4}N^{1/2} - \left(2^{1/2}N^{3/4} + 2^{1/4}N^{3/4}\right)\end{aligned}$$

which is a good approximation to $\varphi(N)$.

Theorem 3.2. Let $N = p^2q^2$be a multi prime power modulus with $q^2 < p^2 < 2q^2$ and the relation $1 < e < \varphi(N) < \left(N + 2^{1/4}N^{1/2} - \left(2^{1/2}N^{3/4} + 2^{1/4}N^{3/4}\right)\right)$ hold satisfying equation $ed - k\varphi(N) = 1$ for some unknown integers $\varphi(N)$, d, k *and* $\xi = 2^{1/2}N^{3/4} + 2^{1/4}N^{3/4}$. If $d < \frac{1}{2}\left(N + 2^{1/2}N^{3/4} - \xi\right)N^{-\delta}$, then

$$\left|\frac{e}{N + 2^{1/2}N^{3/4} - \xi} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

Proof. Equation $ed - k\varphi(N) = 1$, we can rewrite it as:

$$\begin{aligned}ed - k(p^{2-1}q^{2-1}(p-1)(q-1)) &= 1\\ ed - k\left(pq(pq - p - q + 1)\right) &= 1\\ ed - k(p^2q^2 - p^2q - pq^2 + pq) &= 1\\ ed - k\left(N - (p^2q + pq^2 - pq)\right) &= 1\\ ed - k\left(N + pq - (p^2q + pq^2)\right) &= 1\\ ed - k\left(N + 2^{1/4}N^{1/2} - \left(2^{1/2}N^{3/4} + 2^{1/4}N^{3/4}\right)\right) &= 1\\ ed - k\left(N + 2^{1/4}N^{1/2} - \xi + \xi - \left(2^{1/2}N^{3/4} + 2^{1/4}N^{3/4}\right)\right) &= 1\\ ed - k\left(N + 2^{1/4}N^{1/2} - \xi\right) &= 1 + k\left(\xi - \left(2^{1/2}N^{3/4} + 2^{1/4}N^{3/4}\right)\right)\end{aligned}$$

Dividing by $d\left(N + 2^{1/4}N^{1/2} - \xi\right)$ gives

$$\begin{aligned}\left|\frac{e}{N + 2^{1/2}N^{3/4} - \xi} - \frac{k}{d}\right| &= \left|\frac{1 + k\left(\xi - \left(2^{1/2}N^{3/4} + 2^{1/4}N^{3/4}\right)\right)}{d(N + 2^{1/4}N^{1/2} - \xi)}\right|\\ &< \left|\frac{1 + k}{d(N + 2^{1/4}N^{1/2} - \xi)}\right|\\ &< \frac{N^{\delta}}{d(N + 2^{1/4}N^{1/2} - \xi)}.\end{aligned}$$

Therefore, since

$$\frac{N^{\delta}}{d(N + 2^{1/4}N^{1/2} - \xi)} < \frac{1}{2d^2}$$

then

$$d < \frac{1}{2}\left(N + 2^{1/4}N^{1/2} - \xi\right)\mathrm{N}^{-\delta}.$$

Hence $\frac{k}{d}$ is found among the convergrnts of the continued fraction expansion of $\frac{e}{N+2^{1/2}N^{3/4}-\xi}$.

Algorithm 1

Input: $N = p^2q^2$, with $q^2 < p^2 < 2q^2$, and public key $(e,\ N,\ g_2 = (p-1)(q-1))\ satisfying$ Theorem 3.2.

Output: The prime factors p and q.

1: Compute the continued fraction expansion of $\frac{e}{N+2^{1/2}N^{3/4}-\xi}$

2: For each convergent $\frac{k}{d}$of $\frac{e}{N+2^{1/2}N^{3/4}-\xi}$, compute $\varphi(N) = \frac{ed-1}{k}$

3: Compute$g_1 = \gcd\left(N,\ \frac{ed-1}{k}\right)$ and

4: Compute $g_3 = g_1 - g_2 + 1$

5. Solve the quadratic equation $x^2 - g_3x + g_1 = 0$

6. Return the prime factors $(p,\ q)$

Example 3.1. We give an example to illustrate our attack for $N = p^2q^2$, Let the public keys be as follows:

$$N = 20632711221263816428499388813976066250801497748144736482761$$
$$e = 91584113072032668951302351786493812579579527374786600793 79$$
$$g_2 = 14364091068098791650467027 9040$$

Suppose that N and e satisfy all the condition stated in Theorem 3.2, then taking the continued fraction expansion of $\frac{e}{N+2^{1/2}N^{3/4}-\xi}$ we get,

$$[0, 2, 3, 1, 21, 38, 2, 1, 2, 14, 3, 2, 1, 4, 1, 1, 1, 1, 7, 1, 1, 2, 1, 3, 3, 4, 1, 9, 2, 1, 1, 1,1, 1,1, 3, 1, 1, 7, 4, 1]$$
$$[1, 1, 3, 1, 23, 15, 4, 1, 1, 1, 9, 1, 3, 15, 1, 3, 5, 1, 43, 1, 1, 1, 2, 1, 14, 1, 65, 1, 31, 3, 1, 1, 1, 4, 8, 1, 4, 1, 5, 1, 2]$$
$$[1, 1, 6, 1, 22, 2, 3, 1, 2, 2, 2, 1, 5, 20, 1, 22, 1, 1, 7, 11, 18, 1, 1, 2, 6, 1, 6, 1, 5, 9, 1, 23, 1 3, 2, 10,2, 3]$$

Applying the factorization algorithm with the convergent $\frac{k}{d} = \frac{22364884}{50385179}$, we obtained

$$\frac{ed-1}{k} = 20632711221263682471856823750498596501616401102344295493760$$

Hence, using Algorithm 1 we get the following:

$$g_1 = 14364091068098884908468477 4819$$
$$g_3 = 932580014495780.$$

Finally, we solve the quadratic equation $x^2 - g_3x + g_1 = 0$, which leads to the factorization of N efficiently and return the prime factors as $p = 737924799162049$ and $q = 194655215333731$.

3.2 Simultaneous Diophantine Attacks on j Prime Power Moduli $N_m = p_m^2q_m^2$

In this section, we present two simultaneous Diophantine cryptanalysis attacks that can lead to the factorization of m prime power moduli $N_m = p_m^2q_m^2$ for $m = 1, \dots, j$

Theorem 3.3 Let $N_m = p_m^2q_m^2$, $1 \le m \le j$, be j prime power moduli and $N = \max\{N_m\}$, e_m, $g_{2m,} = (p_m -$

$1qm-1$, be j public exponents.

Define $\omega = \frac{j(4\epsilon+1)}{4(j+1)}\ where\ 0 < \omega, \epsilon < \frac{3}{4}.$ Let $1 < e_m < \phi(N_m) < N + 2^{\frac{1}{4}}N_m^{\frac{1}{2}} - \xi$ with $\xi = 2^{\frac{1}{2}}N_m^{\frac{3}{4}} + 2^{\frac{1}{4}}N_m^{\frac{3}{4}}.$

If there exists an integers $d < N^{\epsilon}$ and j integers $k_m < N^{\epsilon}$ such that $e_md - k_m\phi(N_m) = 1$ holds for $m = 1, \dots j$, then one can factor j prime power moduli $N_1, \dots, N_j$ in polynomial time.

Proof. Suppose that $N_m = p_m^2q_m^2, for\ 1 \le m \le j$ be j moduli and let $N = \max\{N_1,\ N_2,\ N_3\}$, if $k_m < N^{\epsilon}$ then $e_md - k_m\phi(N_m) = 1$ can be rewritten as

$$e_md - k_m(N_m - (N_m - \phi(N_m))) = 1$$

$$e_m d - k_m\left(N + 2^{\frac{1}{4}}N_m^{\frac{1}{2}} - \xi + \xi - (2^{\frac{1}{2}}N_m^{\frac{3}{4}} + 2^{\frac{1}{4}}N_m^{\frac{3}{4}})\right) = 1$$

$$e_m d - k_m\left(N_m + 2^{\frac{1}{4}}N_m^{\frac{1}{2}} - \xi\right) = 1 + k_m\left(\xi - (2^{\frac{1}{2}}N_m^{\frac{3}{4}} + 2^{\frac{1}{4}}N_m^{\frac{3}{4}})\right)$$

$$\left|\frac{e_m}{N_m + 2^{\frac{1}{4}}N_m^{\frac{1}{2}} - \xi}d - k_m\right| = \frac{\left|1 + k\left(\xi + 2^{\frac{1}{2}}N_m^{\frac{3}{4}} + 2^{\frac{1}{4}}N_m^{\frac{3}{4}}\right)\right|}{N_m + 2^{\frac{1}{4}}N_m^{\frac{1}{2}} - \xi} \quad (1)$$

Suppose that $N = \max\{N_1, N_2, N_3\}$, $k_m < N^{\omega}$ and $1 < e_m < \phi(N_m) < N + 2^{\frac{1}{4}}N_m^{\frac{1}{2}} - \xi < \frac{1}{4}N^{\epsilon+1}$, then

$$\left|\frac{e_m}{N_m + 2^{\frac{1}{4}}N_m^{\frac{1}{2}} - \xi}d - k_m\right| \leq \frac{\left|N^{\omega}\left(2N_m^{\frac{3}{4}} + N_m^{\frac{3}{4}}\right)\right|}{\frac{1}{4}N^{\epsilon+1}} < \frac{N^{\omega}\left(3N_m^{\frac{3}{4}}\right)}{\frac{1}{4}N^{\epsilon+1}} < \frac{3}{4}N_m^{\frac{3}{4}+\omega-\epsilon-1}.$$

Plugging in to equation (1), to get

$$\left|\frac{e_m}{N_m + 2^{\frac{1}{4}}N_m^{\frac{1}{2}} - \xi}d - k_m\right| < \frac{3}{4}N_m^{\frac{3}{4}+\omega-\epsilon-1}$$

For unknown integers d, we define $\Omega = \frac{3}{4}N_m^{\frac{3}{4}+\omega-\epsilon-1}$ with $\omega = \frac{j(4\epsilon+1)}{4(j+1)}$, then

$$N^{\omega}\Omega^j = (\frac{3}{4})^j N^{\omega+\frac{3}{4}j+\omega j-\epsilon j-j} = (\frac{3}{4})^j$$

For $\left(\frac{3}{4}\right)^j < 2^{\frac{j(j-3)}{4}} \times 3^j$ with$j \geq 2$, we get $N^{\omega}\Omega^j < 2^{\frac{j(j-3)}{4}} \times 3^j$. It follows that if $d < N^{\omega}$, then $d < 2^{\frac{j(j-3)}{4}} \times 3^j \times \Omega^{-j}$. For $m = 1, \ldots, j$, we have

$$\left|\frac{e_m}{N_m + 2^{\frac{1}{4}}N_m^{\frac{1}{2}} - \xi}d - k_m\right| < \Omega,$$

$$d < 2^{\frac{j(j-3)}{4}} \times 3^j \times \Omega^{-j}$$

Hence, by Theorem 2.8, we can obtain the parameters d and k_m for $m = 1, \ldots, j$. From $e_m d - k_m\phi(N_m) = 1$ we get

$$\frac{e_m d - 1}{k_m} = \phi(N_m) = p_m^2 q_m^2 (p_m - 1)(q_m - 1) = D_m$$

$$g_{1m} = \gcd(N_m, D_m)$$

$$g_{3m} = g_{1m} - g_{2m} + 1.$$

Solving $x^2 + g_{3m} + g_{1m} = 0$, the prime factors p_m and q_m can be revealed, which leads to factorization of j moduli $N_m, \ldots, N_j$. This completes the proof.

Let

$$\psi_1 = \frac{e_1}{N_1 + 2^{\frac{1}{4}}N_1^{\frac{1}{2}} - \left(2^{\frac{1}{2}}N_1^{\frac{3}{4}} + 2^{\frac{1}{4}}N_1^{\frac{3}{4}}\right)}, \quad \psi_2 = \frac{e_2}{N_2 + 2^{\frac{1}{4}}N_2^{\frac{1}{2}} - \left(2^{\frac{1}{2}}N_2^{\frac{3}{4}} + 2^{\frac{1}{4}}N_2^{\frac{3}{4}}\right)}, \quad \psi_3 = \frac{e_3}{N_3 + 2^{\frac{1}{4}}N_3^{\frac{1}{2}} - \left(2^{\frac{1}{2}}N_3^{\frac{3}{4}} + 2^{\frac{1}{4}}N_3^{\frac{3}{4}}\right)}$$

Algorithm 2

1: Initialization: The public key $(e_m, N_m, q_{2,} = (p_m - 1)(q_m - 1))$ satisfying Theorem 3.3.
2: Choose $\epsilon, \omega, N = \max\{N_m\}$.
3: For **any** (ϵ, ω, N, j)**do**
4: $\Omega = \frac{3}{4}N_m^{\frac{3}{4}+\omega-\epsilon-1}$

5: $Z = 2^{\frac{(j+1)(j-3)}{4}} \times 3^{j+1} \times \Omega^{-j-1}$
6: **end for**
7: Consider the lattice L spanned by the matrix H as stated above
8: Applying the LLL algorithm to L yields the reduced basis matrix G,
9: For **any**(H, G)**do**
10: Compute $U := H^{-1}$ and $W = U \times G$
11: **end for**
12: Produce d, k_m from W
13: For **each** triplet (d, k_m, e_m)**do**
14: $D_m = \frac{e_m d-1}{k_m}$ for $m = 1, \ldots, j$
15: Compute $g_{1m} = \gcd(N_m, D_m)$
16: Compute $g_{3m} = g_{1m} - g_{2m} + 1$
17: **end for**
18: Solve quadratic equation $x^2 + g_{3m} + g_{1m} = 0$
19: Return prime factors (p_m, q_m).

Example 3.2. We consider the following three prime power and their three public exponents respectively.

$$N_1 = 24505207527375505016122165685028726835373551536 1$$
$$N_2 = 13418740703597663735427268339151833715402009164 9$$
$$N_3 = 13373197029344502834610198056533683341475459129$$
$$e_1 = 83244445987587128591535352069641179479493099489$$
$$e_2 = 17730658094517334089790815415549737336858136289$$
$$e_3 = 12144642046030350716113947667305925180835460781$$
$$g_{21} = 495027348004418319553600$$
$$g_{22} = 366315993419577026932800$$
$$g_{23} = 115642539876728161630828$$

Then, $N = max(N_1, N_2, N_3) = 24505207527375505016122165685028726835373551536 1$

$j = 3\ with\ \epsilon = 0.714$ we get $\omega = \frac{j(4\epsilon+1)}{4(j+1)} = 0.2410714286$ and $\Omega = \frac{3}{4} N_m^{\frac{3}{4}+\omega-\epsilon-1} = 0.0001166798491.$

Using Theorem 2.8, we obtain $Z = 2^{\frac{(j+1)(j-3)}{4}} \times 3^{j+1} \times \Omega^{-j-1} = 218510136400000000.$
Consider the lattice L spanned by the matrix

$$H = \begin{bmatrix} 1 & -[Z\psi_1] & -[Z\psi_2] & -[Z\psi_3] \\ 0 & Z & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & Z \end{bmatrix}$$

Therefore, applying the LLL algorithm to L, we obtain the reduced basis with following matrix

$$G = \begin{bmatrix} 108354209 & -5676920464763 & -1741139600425 & -741814579509 \\ -5424268084759 & 3186459013613 & -4281329595825 & 2801857254941 \\ 7176383742073 & 2961742771389 & -778722476225 & -13910914056173 \\ -9250654139360 & -2771420912480 & 10585742092000 & -1247016148640 \end{bmatrix}$$

Next, we compute

$$W = \begin{bmatrix} 108354209 & 36808038 & 14317226 & 98400037 \\ -5424268084759 & -1842629535380 & -716727783543 & -4925957054776 \\ 7176383742073 & 2437825054687 & 948241040623 & 6517111169592 \\ -9250654139360 & -3142456875733 & -1222321746275 & -8400824647128 \end{bmatrix}$$

Then, from the first row of matrix W, we obtain $d = 8400824647128, k_1 = 36808038$
$k_2 = 14317226, k_3 = 98400037$. Hence, using $d\ and\ k_m$ for $m = 1,2,3,$ we compute
$\frac{e_m d-1}{k_m} = \phi(N_m) = p_m^2 q_m^2 (p_m - 1)(q_m - 1) = D_m, g_{1m}, g_{3m}$ as follows:

$$D_1 = 24505207527302126609185464243007146744217951840 0$$
$$D_2 = 13418740703547411852603421778889975539207315040 0$$
$$D_3 = 13373197029242582925422175942457508262752058844$$
$$g_{11} = 495027348005900629717519$$
$$g_{12} = 366315993420948844809343$$
$$g_{13} = 115642539877609497420373$$
$$g_{31} = 1482310163920,\ g_{32} = 1371817876544, g_{33} = 881335789546$$

Finally, we solve quadratic equation $x^2 + g_{3m} + g_{1m} = 0$, for $m = 1, 2, 3$ which produces prime factors as follows:

$$p_1 = 974143295201,\ p_2 = 1008639597151,\ p_3 = 720927869807$$
$$q_1 = 508166868719,\ q_2 = 363178279393,\ q_3 = 160407919739.$$

This leads to the factorization of three moduli N_1, N_2 and N_3 in polynomial time.

Theorem 3.4 Let $N_m = p_m^2 q_m^2$ be j prime power moduli, $e_m, q_{2m,} = (p_m - 1)(q_m - 1)$ be j public exponents with $e_m = N^\alpha$ and $N = \max\{N_m\}, 0 < \alpha < 1$. Also, define $\gamma = \frac{j(4\alpha-3)}{4(j+1)}$. If there exists unknown positive integers $k, d_m < N^\gamma$ such that $e_m d_m - k\phi(N_m) = 1$ holds for $m = 1, \dots j$, then one can factor j prime power moduli $N_1, \dots, N_j$ in polynomial time.

Proof. Suppose $N_m = p_m^2 q_m^2$ be j prime power moduli for $1 \le m \le j$. Then equation $e_m d_m - k\phi(N_m) = 1$ can be rewritten as

$$\left| \frac{N_m + 2^{\frac{1}{4}} N_m^{\frac{1}{2}} - \xi}{e_m} k - d_m \right| = \frac{\left| 1 + k\left(\xi + 2^{\frac{1}{2}} N_m^{\frac{3}{4}} + 2^{\frac{1}{4}} N_m^{\frac{3}{4}} \right) \right|}{e_m} \tag{2}$$

Also, suppose $N = \max\{N_m\}, k < N^\gamma$ and $\min\{e_m\} = N^\alpha$, then

$$\frac{\left| 1 + k\left(\xi + 2^{\frac{1}{2}} N_m^{\frac{3}{4}} + 2^{\frac{1}{4}} N_m^{\frac{3}{4}} \right) \right|}{e_m} \le \frac{\left| N^\gamma \left(N^{\frac{3}{4}} + N^{\frac{3}{4}} \right) \right|}{N^\alpha} < \frac{N^\gamma \left(2N^{\frac{3}{4}} \right)}{N^\alpha} < 2N^{\frac{3}{4}+\gamma-\alpha}.$$

This gives

$$\left| \frac{N_m + 2^{\frac{1}{4}} N_m^{\frac{1}{2}} - \xi}{e_m} k - d_m \right| < 2N^{\frac{3}{4}+\gamma-\alpha}$$

For unknown integers k, d_m, we define $\sigma = 2N_m^{\frac{3}{4}+\gamma-\alpha}$ with $\gamma = \frac{j(4\alpha-3)}{4(j+1)}$, which implies

$$N^\gamma \sigma^j = 3^j N^{\gamma + \frac{3}{4}j + \gamma j - \alpha j} = 3^j$$

For $(2)^j < 2^{\frac{j(j-3)}{4}} \times 3^j$ with $j \ge 3$, we get $N^\gamma \sigma^j < 2^{\frac{j(j-3)}{4}} \times 3^j$. This shows that if $k < N^\gamma$, then $k < 2^{\frac{j(j-3)}{4}} \times 3^j \times \sigma^{-j}$. For $m = 1, \dots, j$, we have

$$\left| \frac{N_m + 2^{\frac{1}{4}} N_m^{\frac{1}{2}} - \xi}{e_m} k - d_m \right| < \sigma,$$
$$k < 2^{\frac{j(j-3)}{4}} \times 3^j \times \sigma^{-j}$$

Hence, by Theorem 2.8, we can recover unknown integers k, d_m for $m = 1, \dots, j$. Next, from $e_m d_m - k\phi(N_m) = 1$ we get

$$\frac{e_m d_m - 1}{k} = \phi(N_m) = p_m^2 q_m^2 (p_m - 1)(q_m - 1) = D_m$$
$$g_{1m} = \gcd(N_m, D_m)$$
$$g_{3m} = g_{1m} - g_{2m} + 1.$$

Therefore, by finding the roots of $x^2 + g_{3m} + g_{1m} = 0$,the prime factors p_m and q_m can be revealed, which leads to factorization of j moduli $N_m, \dots, N_j$. This completes the proof.

Let

$$\psi_{11} = \frac{N_1 + 2^{\frac{1}{4}} N_1^{\frac{1}{2}} - \left(2^{\frac{1}{2}} N_1^{\frac{3}{4}} + 2^{\frac{1}{4}} N_1^{\frac{3}{4}}\right)}{e_1}, \ \psi_{12} = \frac{N_2 + 2^{\frac{1}{4}} N_2^{\frac{1}{2}} - \left(2^{\frac{1}{2}} N_2^{\frac{3}{4}} + 2^{\frac{1}{4}} N_2^{\frac{3}{4}}\right)}{e_2}, \ \psi_{13} = \frac{N_3 + 2^{\frac{1}{4}} N_3^{\frac{1}{2}} - \left(2^{\frac{1}{2}} N_3^{\frac{3}{4}} + 2^{\frac{1}{4}} N_3^{\frac{3}{4}}\right)}{e_3}$$

Algorithm 3

1: Initialization: The public key $(e_m, N_m, h_{2m,} = (p_m - 1)(q_m - 1))$ satisfying Theorem 3.4.
2: Choose $\epsilon, \omega, N = \max\{N_m\}$.
3: For **any** (ϵ, ω, N, j)**do**
4: $\sigma = 2N^{\frac{3}{4}+\gamma-\alpha}$
5: $Z = 2^{\frac{(j+1)(j-3)}{4}} \times 3^{j+1} \times \Omega^{-j-1}$
6: **end for**
7: Consider the lattice L spanned by the matrix H as stated above
8: Applying the LLL algorithm to L yields the reduced basis matrix G,
9: For **any**(H, G)**do**
10: Compute $U := H^{-1}$ and $W = U \times G$
11: **end for**
12: Produce d, k_m from W
13: For **each** triplet (d, k_m, e_m)**do**
14: $D_m = \frac{e_m d - 1}{k_m}$ for $m = 1, \dots, j$
15: Compute $g_{1m} = \gcd(N_m, D_m)$
16: Compute $g_{3m} = g_{1m} - g_{2m} + 1$
17: **end for**
18: Solve quadratic equation $x^2 + g_{3m} + g_{1m} = 0$
19: Return prime factors (p_m, q_m).

Example 3.3. We consider the following three prime power and their three public exponents respectively.

$$N_1 = 108436990500987658528161179204357809$$
$$N_2 = 560075121810496042634946302210992 81$$
$$N_3 = 213170198658945505453653102774829 21$$
$$e_1 = 128319785134805416016769665948723 30$$
$$e_2 = 222100318161030838853463922156493 52$$
$$e_3 = 575937251484872853628737945870373 5$$
$$g_{21} = 329297722017578496$$
$$g_{22} = 236659062105533184$$
$$g_{23} = 146003491771136352$$

Then $N = \max\{N_1, N_2, N_3\} = 108436990500987658528161179204357809$. Also, $\min\{e_1, e_2, e_3\} = N^{\alpha} = 575937251484872853628737945870373 5$, with $\alpha = 0.988$ and $j = 3$ we get $\gamma = \frac{j(4\alpha+1)}{4(j+1)} = 0.1785000000$ and $\sigma = 2N^{\frac{3}{4}+\gamma-\alpha} = 0.01646026933$.

Using Theorem 2.8, we obtain $Z_1 = 2^{\frac{(j+1)(j-3)}{4}} \times 3^{j+1} \times \sigma^{-j-1} = 551705451$.

Consider the lattice L spanned by the matrix

$$H = \begin{bmatrix} 1 & -[Z_1\psi_{11}] & -[Z_1\psi_{12}] & -[Z_1\psi_{13}] \\ 0 & Z_1 & 0 & 0 \\ 0 & 0 & Z_1 & 0 \\ 0 & 0 & 0 & Z_1 \end{bmatrix}$$

Therefore, applying the LLL algorithm to L, we obtain the reduced basis with following matrix

$$G_1 = \begin{bmatrix} 46521 & 196035 & 21696 & 39954 \\ 1375558 & 1586425 & -4102192 & -6740616 \\ 3111176 & -1037923 & -6720083 & 5577519 \\ -9255262 & 2103476 & -4624718 & 2570409 \end{bmatrix}$$

Next, we compute

$$W_1 = \begin{bmatrix} 46521 & 393127 & 117313 & 172187 \\ 1375558 & 11624191 & 3468774 & 5091318 \\ 3111176 & 26291079 & 7845519 & 11515317 \\ -9255262 & -78211848 & -23339192 & -34256267 \end{bmatrix}$$

Then, from the first row of matrix W_1, we obtain $k = 8400824647128, d_1 = 393127$ $d_2 = 117313,\ d_3 = 172187$. Hence, using Algorithm 3 and the value of $k\ and\ d_m$ for $m = 1,2,3,$ we compute $D_m = \frac{e_m d_m - 1}{k} = \phi(N_m) = p_m^2 q_m^2 (p_m - 1)(q_m - 1), g_{1m}, g_{3m}$ as follows:

$$D_1 = 10843699011347702926081685360465971 2$$
$$D_2 = 56007511928860107904852460394111744$$
$$D_3 = 21317019737629415113125577843464672$$

$$g_{11} = 329297723194357447$$
$$g_{12} = 236659063171156841$$
$$g_{13} = 146003492649643661$$
$$g_{31} = 1176778952, g_{32} = 1065623658, g_{33} = 878507310.$$

Finally, we solve the quadratic equation $x^2 + g_{3m} + g_{1m} = 0$, for $m = 1,2,3$ which produces prime factors as follows:

$p_1 = 718406599,\ p_2 = 750135049,\ p_3 = 655910713$
$q_1 = 458372353,\ q_2 = 315488609,\ q_3 = 222596597.$
This leads to the factorization of three moduli N_1, N_2 and N_3 in polynomial time.

4. Conclusion

From our findings, we established that $\frac{k}{d}$ can be recovered among the convergent of the continued fraction expansion $\frac{e}{N+2^{\frac{1}{4}}N^{\frac{1}{2}}-\left(2^{\frac{1}{2}}N^{\frac{3}{4}}+2^{\frac{1}{4}}N^{\frac{3}{4}}\right)}$ where $N + 2^{\frac{1}{4}}N^{\frac{1}{2}} - \left(2^{\frac{1}{2}}N^{\frac{3}{4}} + 2^{\frac{1}{4}}N^{\frac{3}{4}}\right)$ is considered to be good approximation of $\phi(N)$, which yielded the factorization of the prime power modulus $N = p^2q^2$ in polynomial time. Furthermore, for j public keys (N_m, e_m, g_{2m}) where $g_{2m} = (p_m - 1)(q_m - 1)$ we were able to recover unknown integers k_m, d, k, d_m through LLL algorithm which led to the simultaneous factorization of j prime power moduli $N_m\ for\ m = 1,2,3$ in polynomial time. The paper also gave numerical results to justify its findings. This has not been reported by other works based on the available literature within our reach.

References

[1] Batina, L., Mentens, N., Sakiyama, K., Preneel, B., & Verbauwhede, I. (2007). Public-Key Cryptography. *EEE International Symposium on Circuits and Systems*, 1831-1834.

[2] Diffie W., & Hellman, M. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6), 644-654.

[3] Rivest, R., Shamir, A., Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2), 120-126.

[4] Atsushi Fujioka, Tatsuki Okamoto, & Shoji Miyaguchi. (1991). ESIGN: An Efficient Digital Signature Implementation for Smart Cards. *In: Workshop on the Theory and Application of Cryptographic Techniques*, Springer, 446-457.

[5] Okamoto, T., & Uchiyama, S. (1998). A New Public-Key Cryptosystem as Secure as Factoring. In: *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 308-318.

[6] Nishioka, M., Satoh, H., & Sakurai, K. (2001). Design and Analysis of Fast Provably Secure Public-Key Cryptosystems Based on A Modular Squaring. *Springe*r, Berlin, Heidelberg, 81-102.

[7] Ariffin, K. Rezal, M., Asbullah, M. A., Abu, N. A., & Mahad, Z. (2013). A New Efficient Asymmetric Cryptosystem Based on the Integer Factorization Problem of $N = p^2q$. *Malaysian Journal of Mathematical Sciences*, 7(S), 19-37.

[8] Sarkar, S. (2014). Small Secret Exponent Attack on RSA Variant with Modulus $N = p^rq$. *Designs, Codes and Cryptography*, 73(2), 383-392.

[9] Asbullah, M. A., & M. R. K. Arin. (2015). New Attacks on RSA with Modulus $N = p^2q$ Using Continued Fractions. *Journal of Physics, Conference Series*, 622(1). IOP Publishing.

[10] Lim, S., Kim, S., Yie, I., & Lee, H. (2000). A Generalized Takagi-Cryptosystem with a Modulus of the Form p^rq^s. *International Conference on Cryptology*, Springer India, 283-294.

[11] Lu, Yao, Liqiang Peng, & Santanu Sarkar. (2017). Cryptanalysis of an RSA Variant with Moduli $N = p^rq^l$'. *Journal of Mathematical Cryptology*, 11(2), 117-130.

[12] Nitaj Abderrahmane & Tajjeeddine Rachidi. (2015). New Attacks on RSA with Moduli $N = p^rq$'. *Codes, Cryptology, and Information Security*. Springer International Publishing, 352-360.

[13] Lenstra, A. K., Lenstra, H. W., & L. Lovasz. (1982). Factoring Polynomials with Rational Coefficients. *MathematischeAnnalen*, 261, 513-534.

[14] Nitaj, A., Arin, M. R. K., Nassr, D. I., & Bahig, H. M. (2014). New Attacks on the RSA Cryptosystem. *Progress in Cryptology-AFRICACRYPT*. Springer International Publishing, 178-198.