Malaysian Journal Of Science 39(1): 72-80 (February 2020)

CRYPTANALYSIS OF RSA KEY EQUATION OF $N=p^2q$ FOR SMALL $|2q - p|$ USING CONTINUED FRACTION

Normahirah Nek Abd Rahman[1a], Muhammad Asyraf Asbullah[2b,c*], Muhammad Rezal Kamel Ariffin[3b,d], Siti Hasana Sapar[4b,d] and Faridah Yunos[5b,d]

[a]Pusat PERMATA Pintar Negara, Universiti Kebangsaan Malaysia, MALAYSIA. Email: normahirah@ukm.edu.my[1]
[b]Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research, Universiti Putra Malaysia, MALAYSIA. Email: ma_asyraf@upm.edu.my[2] ; rezal@math.upm.edu.my[3] ; sitihas@upm.edu.my[4] ; faridahy@upm.edu.my[5]
[c]Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, Serdang, 43400, MALAYSIA. Email: ma_asyraf@upm.edu.my[2]
[d]Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, MALAYSIA. Email: rezal@math.upm.edu.my[3] ; sitihas@upm.edu.my[4] ; faridahy@upm.edu.my[5]
*Corresponding author: ma_asyraf@upm.edu.my
Received: 20th Mar 2019 Accepted: 4th Dec 2019 Published: 29th Feb 2020
DOI: https://doi.org/10.22452/mjs.vol39no1.6

ABSTRACT This paper presents a new factoring technique on the modulus $N = p^2q$, where p and q are large prime numbers. Suppose there exists an integer e satisfies the equation $ed - k\phi(N) = 1$, for some unknown integer d, k and $\phi(N)$ is the Euler's totient function. Our method exploits the term $N - \left((2^{2/3} + 2^{-1/3})N^{2/3} - 2^{1/3}N^{1/3}\right)$ to be the closest integer to the unknown parameter $\phi(N)$. Hence we show that the unknown parameters k and d can be recovered from the list of the continued fractions expansion of $\frac{e}{N-\left((2^{2/3}+2^{-1/3})N^{2/3}-2^{1/3}N^{1/3}\right)}$. Furthermore, we present an algorithm to compute the prime factors of $N = p^2q$ in polynomial time after obtaining the correct tuple $d, k,$ and $\phi(N)$.

Keywords: RSA cryptosystem, continued fractions, secret exponent, cryptanalysis.

1. INTRODUCTION

From the beginning of time until the 1970s, the technology for practicing secret communication, which is widely known as encryption and decryption, were always done in a symmetrical manner. In early 1978, the RSA cryptosystem (Rivest et al., 1978) that was introduced (abbreviated accordingly to its creator; Rivest, Shamir, and Adleman) became a phenomenon in the world of secrecy of which was regarded as the first practical realization of the asymmetric cryptosystem as opposed to symmetric cryptosystem.

Invented in 1978, the RSA cryptosystem was amongst the most commercialized asymmetric cryptosystem. The RSA cryptosystem has competed for the vital role of reassuring the confidentiality, integrity, authenticity, and non-reputability of modern age digital communications and information (Rahman et al., 2018). The security aspects of RSA cryptosystem hardly depend on the following three parameters as follows. The first one is the product of two large primes p and q or widely known as the modulus $N = pq$, secondly the secret value of $\phi(N)$, which derived from the Euler's totient function, and finally the public and private exponent e and d which related by the congruence relation $ed \equiv 1 \bmod \left(\phi(N)\right)$. Hence, based on three hard mathematical problems lies the difficulties in breaking the RSA cryptosystem (Abubakar et al., 2018). The first one is the integer factorization problem of $N = pq$. Multiplying the two primes to form an integer N is straightforward. However, determining the prime numbers primes p and q given N are impracticable because of the time it might take even using the fastest computers. Second, the eth root problem from $C \equiv M^e \pmod N$ and the third one is to solve the Diophantine key equation $ed - k\phi(N) = 1$ that contains three variables namely $d, \phi(N)$ and k. There are several problems to consider on implementing RSA cryptosystem, which includes reducing the execution of encryption and/or decryption time (Abubakar et al., 2018). For example, if the secret exponent d is relatively small, then the RSA cryptosystem seems to have faster decryption process. However, the knowledge of secret exponent d will lead to the factorization of N in polynomial time.

In 1990, Wiener (1990) proved that RSA to be totally insecure if the secret exponent $d < \frac{1}{3}N^{1/4}$. Wiener was able to obtain the integer solutions through the continued fractions of $\frac{e}{N}$ and eventually lead to factor the modulus $N = pq$. Next, Bunder and Tonien (2017) presents a new attack based on Wiener's approach upon the RSA cryptosystem using the mid-point technique and continued fractions. Furthering this, by using another proving technique, Asbullah and Ariffin (2019) proposed an extension of Wiener's work which RSA insecure when the secret exponent $d < \frac{1}{2}N^{1/4}$. Alternatively, de Weger (2002) proposed an attack to the RSA cryptosystem considering the generated modulus is resulted from multiplying two relatively near its respective prime factors. de Weger (2002) showed that, if the distance between p and q is relatively near, then $N - 2\sqrt{N} + 1$ is a good choice to be the closest integer to the unknown parameter to $\phi(N)$ compared to N. Hence, $\frac{k}{d}$ is recovered in polynomial time amongst the enumeration of the continued fractions $\frac{e}{N-2\sqrt{N}+1}$. Maitra and Sarkar (2010), on the other hand, using in a different setting, presented a situation of when p and $2q$ are small when being subtracted. They used the term $N - \frac{3}{\sqrt{2}}\sqrt{N} + 1$ as a good approximation to $\phi(N)$ instead of N. Hence, they proved that $\frac{k}{d}$ can be recovered amongst the list of the continued fractions expansion of $\frac{e}{N-\frac{3}{\sqrt{2}}\sqrt{N}+1}$. Most of the time, the utilization of short secret exponent encounters a significant security drawback in varied instances of RSA.

Numerous cryptosystems, including variant designs of the RSA utilizing $N = p^2q$ to accomplish better throughput. One of the reasons is to improve the computational efficiency while keeping up the level of security. In 1998, Takagi (1998) showed that the decryption process is about three times faster than RSA cryptosystem using Chinese Remainder Theorem if they choose the 768-bit modulus p^2q for 256-bit primes p and q. Later, Okamoto and Uchiyama (1998) presented a public key cryptosystem that is provably as secure as factoring a modulus of the form $N = p^2q$. Alternatively, Mahad et al., (2017) presented efficient methods that manipulate the mathematical structure of the modulus to overcome Rabin cryptosystem decryption failure which was due to a four-to-one mapping scenario. Additionally, the design of Rabin cryptosystem (Asbullah & Ariffin, 2016) incorporating the hardness of factoring integer as its source of security which successfully eliminates the decryption failure of any variant of Rabin-based cryptosystem. Recently, the enhanced version of the cryptosystem Asbullah et al., 2018) was introduced which replace their original decryption mechanism with the Rabin decryption yet still retain the use of the modulus.

Motivated from de Weger's generalization attack (de Weger, 2002) and Maitra and Sarkar's attack (Maitra and Sarkar, 2010), a new attack on RSA-type modulus $N = p^2 q$ (Asbullah & Ariffin, 2015) was proposed by applying the term $N - \left(2N^{2/3} N^{1/3}\right)$ as a better choice of integer that closest to $\phi(N)$ for solving unknown integer d, k implicitly from the equation $ed - k\phi(N) = 1$. Hence, they showed that $\frac{k}{d}$ is one of the convergent of the continued fractions expansion of $\frac{e}{N-(2N^{2/3}-N^{1/3})}$ and able to determine, in polynomial time the prime factors of $N = p^2 q$. A more general result for factoring the modulus in form of $N = p^r q$ for $r \geq 2$ can be found in Nitaj & Rachidi (2015). In 2018, Rahman et al. (2018) extends the result of Asbullah & Ariffin (2015) to multiple moduli $N_i = p_i^2 q_i$ for some integer i. Rahman et al. (2018) proves that solving a system of equations by combining the set of $N_i = p_i^2 q_i$ and the approximation of $\phi(N)$ from Asbullah & Ariffin (2015) lead to a successful factorization in polynomial time. In 2018, Bunder et.al (2018) proposed cryptanalytical results upon several variants of RSA, i.e. based on Lucas sequences, Gaussian integers, and elliptic curves. The common mathematical equation between those variants is the use of modified Euler's function in the form $\phi(N) = (p^2 - 1)(q^2 - 1)$ and relates to the modified RSA variant key equation in the form $ed + k\phi(N) = 1$. The results in Bunder et al., (2018) was generalized later by Nitaj et al., (2018) where $ex + y\phi(N) = 1$ for some unknown integer x, y. Working in the same direction as Bunder et al., (2018) and Nitaj et al., (2018), recently Rahman et al., (2019) presents three different attacks on a generalized RSA key equation in the form of $ex + y\phi(N) = 1$ where $N = p^2 q$.

Our contribution: In this work, a new factoring technique on the integer of the form $N = p^2 q$, by using the continued fractions expansion method is presented. We consider the difference between $2q$ and p is small instead of p and q is small as in Asbullah & Ariffin, (2015) . We prove that if we apply the term $N - \left(\left(2^{2/3} + 2^{-1/3}\right)N^{2/3} - 2^{1/3} N^{1/3}\right)$ as a good approximation of $\phi(N)$ satisfies the key equation $ed - k\phi(N) = 1$, then $\frac{k}{d}$ is one of the convergent of the continued fraction $\frac{e}{N-\left((2^{2/3}+2^{-1/3})N^{2/3}-2^{1/3}N^{1/3}\right)}$ satisfy $2p^{5/3}\left|2^{1/3}q^{1/3} - p^{1/3}\right| < \frac{1}{6}N^{\gamma}$ and $\sigma < \frac{1-\gamma}{2}$.

The layout of the paper is as follows. In Section 2, we begin with a brief review on continued fraction expansion and a very important theorem that will be used throughout the paper. In Section 3 we present our new cryptanalysis. Section 4 shows the factoring algorithm of the modulus $N = p^2 q$ together with an example. We summarized our work in Section 5.

2. PRELIMINARIES

In this section, we state the definition of continued fraction and a useful theorem that form the basis for this paper.

Definition 2.1 (Continued fraction) *Each rational number x can be written as an expression of the form*

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \ddots}}}$$

A simple way to show the above expression is by the form $x = [a_0, a_1, a_2 \ldots . a_n]$. We define that the i^{th} term from the list of the continued fraction to be $[a_0, a_1, a_2, \ldots, a_i]$ for $i \geq 0$.

An important result on continued fractions that will be used is the following theorem.

Theorem 2.1 (Legendre's Theorem (Hardy & Wright, 1965)) *Suppose x is written in its continued fraction expansion $[a_0, a_1, a_2, \ldots]$ form. If $y, z \in \mathbb{Z}$ and coprimes such that*

$$|x - \frac{y}{z}| < \frac{1}{2z^2}$$

then $\frac{y}{z}$ is a rational number amongst the continued fraction's convergent of x.

Theorem 2.2 (Approximation of $\phi(N)$ (Asbullah & Ariffin, 2015)) *Let $N = p^2q$ with $q < p < 2q$ and $\phi(N)$ is the Euler's Totient function for N. Then*

$$2N^{2/3} - N^{\frac{1}{3}} < N - \phi(N) < \left((2^{2/3} + 2^{-1/3})N^{2/3} - 2^{1/3}N^{1/3}\right)$$

The Theorem 2.2 shows that $N - (2N^{2/3} - N^{\frac{1}{3}})$ is regarded as a better approximation to $\phi(N)$ whenever the prime q closed to the prime p. While $\phi(N)$ can be approximated better by the term $N - \left((2^{2/3} + 2^{-1/3})N^{2/3} - 2^{1/3}N^{1/3}\right)$ for the case of the prime p closed to the prime $2q$.

3. RESULTS

Throughout this work, we assume that the modulus $N = p^2q$ is an RSA modulus where the bit-length of the primes p and q are in the same size (i.e. $q < p < 2q$). In this section, we will introduce our new cryptanalysis. Based on Theorem 2.2 in Asbullah & Ariffin, (2015**)**, the term $N - \left((2^{2/3} + 2^{-1/3})N^{2/3} - 2^{1/3}N^{1/3}\right)$ is a better choice of integer that closest to $\phi(N)$ satisfy the key equation $ed - k\phi(N) = 1$. Thus, the following results proves that the enumeration of the computed continued fraction $\frac{e}{N-((2^{2/3}+2^{-1/3})N^{2/3}-2^{1/3}N^{1/3})}$ produced the desired unknown parameters k and d.

Lemma 3.1 *Let $N = p^2q$ and $\phi(N) = N - (p^2 + pq - p)$ with $q < p < 2q$. Then,*

$$\left|N - \left((2^{2/3} + 2^{-1/3})N^{2/3} - 2^{1/3}N^{1/3}\right) - \phi(N)\right| < 2p^{5/3}\left|2^{1/3}q^{1/3} - p^{1/3}\right|.$$

Proof. Let $N = p^2q$. By using $\phi(N) = p(p-1)(q-1) = N - (p^2 + pq - p)$, we get

$$\begin{aligned}
&\left|N - \left((2^{2/3} + 2^{-1/3})N^{2/3} - 2^{\frac{1}{3}}N^{\frac{1}{3}} - \phi(N)\right)\right| \\
&= \left|p^2 + pq - p - \left((2^{2/3} + 2^{-1/3})N^{2/3} - 2^{\frac{1}{3}}N^{\frac{1}{3}}\right)\right| \\
&= \left|p^2 + pq - p - \left((2^{2/3} + 2^{-1/3})(p^2q)^{2/3} - 2^{\frac{1}{3}}(p^2q)^{\frac{1}{3}}\right)\right| \\
&= \left|2^{\frac{1}{3}}q^{\frac{1}{3}} - p^{\frac{1}{3}}\right| \cdot p^{2/3}\left(p + 2^{\frac{1}{3}}p^{2/3}q^{\frac{1}{3}} - 2^{-1/3}p^{1/3}q^{\frac{2}{3}} - 1\right) \\
&< \left|2^{1/3}q^{1/3} - p^{1/3}\right| \cdot p^{2/3}\left(p + 2^{1/3}p^{2/3}q^{1/3}\right)
\end{aligned}$$

$$< \left|2^{\frac{1}{3}}q^{\frac{1}{3}} - p^{\frac{1}{3}}\right| \cdot p^{2/3} \cdot 2p$$
$$< 2p^{\frac{5}{3}}\left|2^{\frac{1}{3}}q^{\frac{1}{3}} - p^{\frac{1}{3}}\right|$$

Now we present our new cryptanalysis on the modulus of the form $N = p^2q$ with $q < p < 2q$ by using the continued fractions to solve for the unknown values k and d.

Theorem 3.1. *Let* $N = p^2q$ *with* $q < p < 2q$. *Let* $\Phi = (2^{2/3} + 2^{-1/3})N^{2/3} - 2^{1/3}N^{1/3}$. *Let* $1 < e < \phi(N) < N - \Phi$ *satisfy* $ed - k\phi(N) = 1$ *where* $\phi(N), d$ *and* k *are unknown integers. Suppose* $\phi(N) > \frac{2}{3}N$ *and* $N > 6d$. *Suppose* $2p^{5/3}|2^{1/3}q^{1/3} - p^{1/3}| < \frac{1}{6}N^{\gamma}$ *and* $d = N^{\sigma}$. *If* $\sigma < \frac{1-\gamma}{2}$, *then* $\left|\frac{e}{N-\Phi} - \frac{k}{d}\right| < \frac{1}{2d^2}$.

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

$$ed - k\big(N - (p^2 + pq - p)\big) = 1$$
$$ed - k\Big(N - \big(N - \phi(N)\big)\Big) = 1$$
$$ed - k\big(N - \Phi + \Phi - (N - \phi(N))\big) = 1$$

And we rearrange,

$$ed - k(N - \Phi) = 1 - k(N - \phi(N) - \Phi) \qquad (1)$$

Observed on the left-hand side, divides (1) by $d(N - \Phi)$, we obtain the following inequalities.

$$\begin{aligned}\left|\frac{e}{N-\Phi} - \frac{k}{d}\right| &= \left|\frac{e}{N-\Phi} - \frac{e}{\phi(N)} + \frac{e}{\phi(N)} - \frac{k}{d}\right| \\ &\leq \left|\frac{e}{N-\Phi} - \frac{e}{\phi(N)}\right| + \left|\frac{e}{\phi(N)} - \frac{k}{d}\right| \\ &\leq e\left|\frac{\phi(N) - (N-\Phi)}{\phi(N)(N-\Phi)}\right| + \left|\frac{ed + k\phi(N)}{\phi(N)d}\right| \\ &\leq e\left|\frac{(N-\Phi) - \phi(N)}{\phi(N)(N-\Phi)}\right| + \left|\frac{ed + k\phi(N)}{\phi(N)d}\right|\end{aligned}$$

Since $e < N - \Phi$ and $ed - k\phi(N) = 1$, then we have

$$\left|\frac{e}{N-\Phi} - \frac{k}{d}\right| < \left|\frac{(N-\Phi) - \phi(N)}{\phi(N)}\right| + \frac{1}{\phi(N)d}.$$

By using Lemma 3.1 which $2p^{5/3}|2^{1/3}q^{1/3} - p^{1/3}| < \frac{1}{6}N^{\gamma}$, $\phi(N) > \frac{2}{3}N$, $N > 6d$ and $d = N^{\sigma}$, we get

$$\left|\frac{(N-\Phi) - \phi(N)}{\phi(N)}\right| + \frac{1}{\phi(N)d} < \frac{2p^{5/3}|2^{1/3}q^{1/3} - p^{1/3}|}{\phi(N)} + \frac{1}{\phi(N)d}$$

$$
\begin{aligned}
&< \frac{\frac{1}{6}N^{\gamma}}{\frac{2}{3}N} + \frac{1}{4d^2} \\
&= \frac{1}{4}N^{\gamma-1} + \frac{1}{4d^2} \\
&= \frac{1}{4}N^{\gamma-1} + \frac{1}{4}N^{-2\sigma}
\end{aligned}
$$

Obviously from the Theorem 2.1, it suffices to take $\gamma - 1 < -2\sigma$. Therefore, we obtain $\sigma < \frac{1-\gamma}{2}$.

4. FACTORING ALGORITHM

Suppose we are given the tuple (N, e) which satisfy all condition of Theorem 3.1, then in this section we present the factoring algorithm of the modulus of the form $N = p^2q$ and its proof of correctness. For completion, we also provide a numerical illustration of our result.

Corollary 4.1 *The modulus $N = p^2q$ can be factored in polynomial time if d and k are appeared amongst the enumeration of the continued fraction expansion of* $\left|\frac{e}{N-\left((2^{2/3}+2^{-1/3})N^{2/3}-2^{1/3}N^{1/3}\right)}\right|$.

Proof. From Theorem 3.1, suppose the unknown d and k have appeared amongst the enumeration once the computation of continued fraction $\left|\frac{e}{N-\left((2^{2/3}+2^{-1/3})N^{2/3}-2^{1/3}N^{1/3}\right)}\right|$ finished, then we have $\frac{ed-1}{k} = \phi(N)$. From Lemma 3.1, evidently, $\phi(N)$ is a multiple of prime p. Therefore, by determining the $\gcd\left(\frac{ed-1}{k}, N\right)$, we obtain the prime factor p. Hence we obtain the prime q.

Algorithm 1. Factoring algorithm of $N = p^2q$

1. Determine all the list of the continued fraction $\frac{e}{N-\left((2^{2/3}+2^{-1/3})N^{2/3}-2^{1/3}N^{1/3}\right)}$.
2. For each convergent $\frac{k}{d}$ of $\frac{e}{N-\left((2^{2/3}+2^{-1/3})N^{2/3}-2^{1/3}N^{1/3}\right)}$, compute $\phi(N) = \frac{ed-1}{k}$.
3. Calculate $p' = \gcd\left(\frac{ed-1}{k}, N\right)$
4. For every odd integer p' such that $1 < p' < N$, compute $q' = \frac{N}{p'^2}$.
5. Return the prime factor $p = p'$ and $q = q'$.

Example 4.1 Suppose we are given $N = 120148413337333$ and $e = 55708935964259$ fulfils the condition as strictly dictated as in Theorem 3.1. Determine $N - \left((2^{2/3} + 2^{-1/3})N^{2/3} - 2^{1/3}N^{1/3}\right)$ and compute $\frac{e}{N-\left((2^{2/3}+2^{-1/3})N^{2/3}-2^{1/3}N^{1/3}\right)}$. The candidates of $\frac{k}{d}$ from the enumeration of the computed continued fraction expansion are as follows;

$$\left[0, \frac{1}{2}, \frac{6}{13}, \frac{13}{28}, \frac{19}{41}, \frac{32}{69}, \frac{83}{179}, \frac{862}{1859}, \frac{1807}{3897}, \ldots\right]$$

By applying the Step 2 in Algorithm 1, with the convergent $\frac{83}{179}$, we obtain

$$\phi(N) = \frac{\big((55708935964259)(179) - 1\big)}{83} = 120143367922920$$

Hence, by computing $\gcd(120143367922920, 120148413337333)$, then we obtain 52511 which leads to the factorization of N since $p = 52511$ and $q = \frac{N}{p^2} = 43573$.

5. CONCLUSIONS

In conclusion, this paper presents new cryptanalysis of the modulus of type $N = p^2q$. We prove that if we use the term $N - \big((2^{2/3} + 2^{-1/3})N^{2/3} - 2^{1/3}N^{1/3}\big)$ as a good approximation of $\phi(N)$ satisfy the key equation $ed - k\phi(N) = 1$, the unknown parameters k and d be recovered among the convergents of the continued fractions expansion $\frac{e}{N-\left((2^{2/3}+2^{-1/3})N^{2/3}-2^{1/3}N^{1/3}\right)}$ which enable one to obtained p and q in polynomial time. In addition, we also come up with new algorithm to factor $N = p^2q$ as we show in Algorithm 1. Observe that the results in this work only consider the balanced prime factors for the modulus where the bit-length of the primes p and q are in the same size (i.e. $q < p < 2q$). In the future work, we aim to extend our result on factoring the modulus with unbalanced prime factors, which in general be defined as $q < p < \delta q$ where $\delta > 2$. Remark that such type of modulus has a limited number of cryptanalytical from earlier and recent publications. Therefore, observed from the trend of publications related to factoring the modulus with unbalanced primes, there is an opportunity to further analysis and mathematical proves specifically using the continued fraction and its variants.

6. ACKNOWLEDGMENTS

The present research was partially supported by the Putra Grant - Putra Young Initiative (IPM) -GP-IPM-2017-9519200.

7. REFERENCES

Abubakar, S.I., Ariffin, M.R.K., and Asbullah, M. A. (2018). A New Simultaneous Diophantine Attack Upon RSA Moduli $N = pq$. In Cryptology and Information Security Conference 2018 (p. 119).

Asbullah, M. A. and Ariffin, M. R. K. (2015). New Attack on RSA with Modulus $N = p^2q$ Using Continued Fractions, Journal of Physics, vol. 622, pp.191–199.

Asbullah, M. A. and Ariffin, M. R. K. (2016). Design of Rabin-like cryptosystem without decryption failure. *Malaysian Journal of Mathematical Sciences* **10 (S)** 1-18.

Asbullah, M.A., Ariffin, M.R.K., and Mahad, Z. (2018). Enhanced AA_β cryptosystem: The design. Proceedings of the 6th International Cryptology and Information Security Conference 2018, CRYPTOLOGY 2018, 94-102.

Asbullah, M. A. and Ariffin, M. R. K. (2019). Another Proof Of Wiener's Short Secret Exponent. Malaysian Journal of Science, MJS (1) 62-68.

Bunder, M. W., & Tonien, J. (2017). A new attack on the RSA cryptosystem based on continued fractions. Malaysian Journal of Mathematical Sciences 11(S), August: 45 – 57

Bunder, M., Nitaj, A., Susilo, W. & Tonien, J. (2018). Cryptanalysis of RSA-type cryptosystems based on Lucas sequences, Gaussian integers and elliptic curves. Journal of Information Security and Applications, 40 193-198.

de Weger, B. (2002). Cryptanalysis of RSA with Small Prime Difference. Applicable Algebra in Engineering Communication and Computing, 13(1), 1728.

Hardy, G and Wright, E. (1965). An Introduction to the Theory of Numbers. Oxford University Press, London.

Mahad, Z., Asbullah, M.A., and Ariffin, M.R.K. (2017). Efficient methods to overcome Rabin cryptosystem decryption failure. Malaysian Journal of Mathematical Sciences, 11 (S2), 9-20.

Nitaj, A., & Rachidi, T. (2015). New attacks on RSA with Moduli $N = p^r q$. In International Conference on Codes, Cryptology, and Information Security (pp. 352-360). Springer, Cham.

Nitaj, A., Pan, Y., & Tonien, J. (2018). A Generalized Attack on Some Variants of the RSA Cryptosystem. In International Conference on Selected Areas in Cryptography (pp. 421-433). Springer, Cham

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

Rahman, N.N.A., Ariffin, M.R.K., Asbullah, M.A. and Yunos, F. (2018). New Vulnerability on System of $N_i = p_i^2 q_i$ Using Good Approximation of $\varphi(N)$. In Cryptology and Information Security Conference 2018 (p. 139).

Rahman, N.N.A., Ariffin, M.R.K., and Asbullah, M.A. (2019). Successful Cryptanalysis upon a Generalized RSA Key Equation, ASM Science Journal, 12, Special Issue 1, 191-202.

Rivest, R., Shamir, A., Adleman, L. (1978). A Method For Obtaining Digital Signatures and Public Key Cryptosystems. Communication of the ACM 21(2), vol. 21, No. 2, pp. 120-126.

Sarkar, S. and Maitra, S. (2010). Cryptanalysis of RSA with two decryption exponents, Information Processing Letters, vol. 110(5) pp. 178-181.

Takagi, T. (1998). Fast RSA-type cryptosystem modulo $p^k q$, Annual International Cryptology Conference, Springer, 318-326.

Wiener, M. (1990). Cryptanalysis of Short RSA Secret Exponents. IEEE Transaction on Information Theory IT-36, vol. 36, pp. 553–558.