On the Improvement Attack Upon Some Variants of RSA Cryptosystem via the Continued Fractions Method

WAN NUR AQLILI RUZAI\textsuperscript{1,1}, MUHAMMAD REZAL KAMEL ARIFFIN\textsuperscript{1,2}, MUHAMMAD ASYRAF ASBULLAH\textsuperscript{1,3}, ZAHARI MAHAD\textsuperscript{1}, AND ATHIRAH NAWAWI\textsuperscript{1,2}

\textsuperscript{1}Institute for Mathematical Research, Universiti Putra Malaysia, Selangor 43400, Malaysia
\textsuperscript{2}Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, Selangor 43400, Malaysia
\textsuperscript{3}Centre of Foundation Studies for Agriculture Science, Universiti Putra Malaysia, Selangor 43400, Malaysia

Corresponding author: Muhammad Rezal Kamel Ariffin (rezal@upm.edu.my)

Received March 30, 2020, accepted April 20, 2020, date of publication April 28, 2020, date of current version May 14, 2020.

\begin{abstract}
Let \(N = pq\) be an RSA modulus where \(p\) and \(q\) are primes not necessarily of the same bit size. Previous cryptanalysis results on the difficulty of factoring the public modulus \(N = pq\) deployed on variants of RSA cryptosystem are revisited. Each of these variants share a common key relation utilizing the modified Euler quotient \((p^2 - 1)(q^2 - 1)\), given by the key relation \(ed - k(p^2 - 1)(q^2 - 1) = 1\) where \(e\) and \(d\) are the public and private keys respectively. By conducting continuous midpoint subdivision analysis upon an interval containing \((p^2 - 1)(q^2 - 1)\) together with continued fractions on the key relation, we increase the security bound for \(d\) exponentially.
\end{abstract}

\begin{IEEEkeywords}
Algebraic cryptanalysis, continued fractions method, integer factorization problem, RSA-variants.
\end{IEEEkeywords}

I. INTRODUCTION

With the realization of the quantum computer coming into reality in the near future, expected in 2030 \[20\], the demise of traditional asymmetric encryption schemes is imminent. However, transition towards post-quantum requires resources and a seamless methodology. As such, in the near future, traditional asymmetric encryption schemes are still the choice to provide cryptographic security. Entrenched within most of the digital platforms we have today is the RSA cryptosystem. Since its introduction in 1978 by Rivest \textit{et al.} \[10\], RSA has become the most broadly used public key cryptosystem in the world. RSA is one of the main default cryptosystem in most web browsers with the objective to provide confidentiality, integrity, authenticity and to disallow repudiation. It is a fact that many cryptographic technologies utilize RSA for privacy protection \[19\]. Hence, research on the security of RSA and its variants are ever more important and still ongoing.

RSA is described as follows. Let a public RSA modulus be presented by \(N = pq\) where \(p\) and \(q\) are distinct prime factors. In RSA key generation algorithm, the positive integers \(e\) and \(d\) are associated by the modular relation \(ed \equiv 1 \pmod{\phi(N)}\) where the Euler’s totient function or Euler quotient be represented by \(\phi(N) = (p - 1)(q - 1)\). Both public exponent \(e\) and private exponent \(d\) satisfy the RSA key equation \(ed \equiv k\phi(N) \equiv 1\) for a positive integer \(k\). The algorithm returns the public key pair \((N, e)\) while the tuple \((p, q, d)\) contains the secret components of the RSA cryptosystem where \(d\) is private key. In the encryption algorithm, a message \(M\) is encrypted as \(C \equiv M^e \pmod{N}\) while in the decryption algorithm, one simply computes \(M \equiv C^d \pmod{N}\) to retrieve the message \(M\).

For more than four decades, studies on improving the efficiency of RSA’s decryption execution time and its relation upon RSA’s overall security features are discussed in-depth by the cryptographic research community. In the process, many variants of RSA were proposed to overcome possible vulnerabilities. As an example, to speed up the decryption process of either the RSA or its variants, one is tempted to use a relatively small private exponent \(d\). Thus, the importance of identifying the threshold value for such small private exponents, in order to balance out between speed and security.
In this paper, we essentially focus on the following three variants of the RSA cryptosystem.

1) Kuwakado et al. [7] in 1995 proposed a variant of RSA cryptosystem which is based on singular cubic curves $y^3 \equiv x^3 + bx^2 \mod N$ where $N = pq$ is an RSA modulus such that $(x, y)$ is the set of points in $\mathbb{Z}_N \times \mathbb{Z}_N$ and $b \in \mathbb{Z}/N\mathbb{Z}$.

2) Elkamchouchi et al. [5] in 2002 suggested an idea to extend RSA cryptosystem into the domain of Gaussian integers for $N = PQ$, where $P$ and $Q$ are the Gaussian primes which relate to the ordinary primes i.e. $p = |P|$ and $q = |Q|$.

3) Castagnos [4] in 2007 introduced a probabilistic version of variant of RSA cryptosystem which is working over quadratic field quotients using Lucas sequences with an RSA modulus $N = pq$.

Interested readers may refer to the following literatures [3], [12] and [14] for the details of these variants of RSA cryptosystem.

Notice that the public key $e$ and private key $d$ of these three variant schemes satisfies the modified key equation of the form $ed - k(p^2 - 1)(q^2 - 1) = 1$ for a positive integer $k$. For simplicity, we refer the term $\omega(N) = (p^2 - 1)(q^2 - 1)$ as the modified Euler quotient. One can rewrite the modified key equation in modular form as $ed \equiv 1 \mod \omega(N)$. Hence, solving the unknowns $d, p$ and $q$ from this particular key equation becomes the topic of interest in this work.

The integer factorization problem upon the public modulus $N = pq$ is an important security feature of the RSA. A popular strategy to factor the public modulus is to scrutinize the upper bound defined by practitioners, especially when decryption speed up is one of their objectives. The seminal work by Wiener [11] proved that if $d < \frac{1}{4}N^{0.25}$, the secret parameters $p$ and $d$ can be computed efficiently using the continued fractions algorithm. Subsequently, Boneh and Durfee [2] proved that by utilizing Coppersmith’s lattice reduction based method, RSA is insecure if the decryption exponent $d < N^{0.292}$.

Motivated by Wiener’s attack on RSA, Bander et al. [3] in 2016 proved that RSA variant cryptosystems in [4], [5] and [7] are insecure if $d < \sqrt{T \frac{N^3 - 18N^2}{e}}$. This is done by finding the private parameters $k$ amongst the convergents of the continued fractions expansion of $\sqrt{T \frac{N^3 - 18N^2}{e}}$. In 2016, Bunder et al. [3] proved that the lower and upper bounds of the modified Euler quotient ($\omega(N)$) are $N^2 - \frac{5}{2}N + 1$ and $N^2 - 2N + 1$ respectively. Observe that the denominator term of $\frac{e}{N^2 - \frac{5}{2}N + 1}$ is the midpoint of the interval $(N^2 - \frac{5}{2}N + 1, N^2 - 2N + 1)$. Then in 2017, Bunder et al. [12] extended their previous work in [3] by considering the general key equation of the form $ex - y(p^2 - 1)(q^2 - 1) = z$ where the unknown parameters $x, y$ and $z$ fulfill the conditions $xy < 2N - 4\sqrt{2N}^z$ and $|z| < (p - q)\sqrt{2N}^z$. The unknowns $x$ and $y$ can be found among the convergents of the public rational number $\frac{e}{N^2 - \frac{5}{2}N + 1}$ via the continued fractions algorithm.

Then, Coppersmith’s technique [13] is applied to factor primes $p$ and $q$. For the parameters $e \approx N^{\beta}, x \approx N^\lambda$ and $|z| \approx N^\gamma$, the bound of $\delta$ in [12] is given by $\delta < \frac{3-\beta}{\gamma}$.

In 2016, Peng et al. [16] analyzed the key equation given by $ed - k(p^2 - 1)(q^2 - 1) = 1$ via lattice methods. Suppose the private parameter $d \approx N^\delta$, they obtained that for $\delta < 2 - \sqrt{\beta}$, where $\beta \geq 1$, the equation is insecure. That is, one is able to identify the variable pair $(d, k)$ and subsequently factor the modulus $N = pq$. The work in 2017 by Bunder et al. [12], was actually an attempt to generalize work by Peng et al. [16]. The generalization was in a sense successful. That is, Bunder et al. [12] identified a potential Diophantine equation that would render factorization of the modulus $N = pq$ easily. Nevertheless, for the case $|z| = 1$, the work by Bunder et al. [12] did not extend the bound by Peng et al. [16].

Subsequently, Zheng et al. [17] presented a new direction as in [16] for $\beta$ within $[1, 4]$. Following through, Nitaj et al. [18] ascertained new weaknesses within the key equation in [12] via Coppersmith’s method. That is, from the equation $ex - y(p^2 - 1)(q^2 - 1) = z$, when $|z| = 1$ and $x \approx N^\delta$, for $\delta < \sqrt{\frac{2}{3}} - \sqrt{\frac{\sqrt{2} - 1}{\sqrt{2} - 2}} - \epsilon$, Nitaj et al. [18] extended the bound by Bunder et al. [12] and enabled one to factor the public modulus $N = pq$.

Recently in 2018, Bunder et al. [14] published a new result considering the case for the modulus $N = pq$ where the primes $p$ and $q$ are of arbitrary sizes or they are said to be unbalanced primes. Generally, let $N = pq$ be an RSA modulus where $q < p < \lambda q$. Then, the modified Euler quotient $\omega(N)$ is proven to be within the interval $N^2 + 1 - (\lambda + \frac{1}{2})N < \omega(N) < N^2 + 1 - 2N$. Their result showed that if $d < \frac{N(N^2 - (\lambda + 1)N^2)}{\sqrt{N^2 + 1 - (\lambda + 1)N^2}} \approx \frac{\sqrt{2N^2 - 1}}{\lambda N^2}$, then $\frac{e}{N^2 + 1 - \frac{\lambda + 1}{\lambda}N}$ is a convergent of continued fraction expansion of $\frac{e}{N^2 + 1 - \frac{\lambda + 1}{\lambda}N}$ and one can factor $N$ in polynomial time.

Later, Tonien [15] extended the work in [3] by introducing a new attack based on the continued fractions method. The attack is applicable whenever $d < \sqrt{\frac{2N^2 - 2N}{e(N + 1)}} \approx \sqrt{\frac{2N^3}{e}}$ for a fixed positive integer $t$ with time complexity $O(t \log(N))$.

As a continuation of work in [3] and [14], we propose a new result for the case when the primes $p$ and $q$ are unbalanced primes such that $q < p < \lambda q$; where $\lambda$ is a chosen parameter specifically $\lambda > 2$. Note that, if $k = 2$, then the primes $p$ and $q$ are balanced primes having the same bit size. In this work, we successfully extend and improve previously mentioned attacks in [3] and [14]. For a chosen $\lambda$, previous RSA variants as mentioned earlier are insecure when $d < \sqrt{\frac{\lambda(\lambda - 1)p(2N^2 - 1)\lambda(N^2 + 1 - \frac{\lambda - 1}{\lambda}N^2)}{\frac{e}{\lambda N^2 + 1}}}$.
for certain values of $i$ and $j$, where $i$ is the number of midpoint subdivision process within the interval $(N^2 + 1 - (\lambda + \frac{1}{2})N, N^2 + 1 - 2N)$ whilst $j$ represents each midpoint term in $i$-th where $j = 0, 1, \cdots, 2^i - 1$.

The layout of the paper is organized as follows. We dedicate Section II to introduce our proposed method and highlight the significant existing results related to our method. We present our first and second attacks followed by numerical examples in Section III and Section IV respectively. We briefly conclude our work in Section V.

II. PRELIMINARIES

This section reviews the fundamental concept of the continued fractions and presents some existing results relevant to our algebraic cryptanalysis method.

**Definition 1 (Continued Fractions, [6]):** The continued fractions expansion of a real number $x \in \mathbb{R}$ is an expression of the form

$$x = [x_0, x_1, x_2, \cdots] = x_0 + \frac{1}{x_1 + \frac{1}{x_2 + \frac{1}{x_3 + \cdots}}}$$

where $x_0 \in \mathbb{Z}$ and $x_i \in \mathbb{N}$ for $i > 0$.

As observed from Definition 1,

I. The numbers $x_1, x_2, x_3, \cdots$ are called the partial quotients.

II. For $i \geq 0$, the fractions $\frac{x_i}{\omega_i} = [x_0, x_1, x_2, \cdots, x_i]$ are called the convergents of the continued fractions expansion of $x$.

III. For $x = \frac{a}{b}$, the continued fractions algorithm (i.e. the Euclidean algorithm) computes the convergents in polynomial time where the complexity is $O((\log b)^2)$ [8].

The following theorem is a significant result concerning the continued fractions that will be used thoroughly in this paper. This theorem guarantees that the unknown numbers $y$ and $z$ are amongst the list of convergents of the continued fractions expansion of a rational number $x$ fulfilled the given inequality as in (1).

**Theorem 1 (Legendre’s Theorem, [6]):** Let $x$ be a rational number and $y$ and $z$ be positive integers where $\gcd(y, z) = 1$. Suppose

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

(1)

then $\frac{y}{z}$ is a convergent of the continued fractions expansion of $x$.

The following lemmas are important as we will utilize these bounds of $\omega(N) = (p^2 - 1)(q^2 - 1)$ to improve the previous attacks in [3] and [14]. We will consider the case when the prime factors $p$ and $q$ have the same bits size and when the primes are of arbitrary sizes.

**Lemma 1:** [3] Suppose an RSA modulus $N = pq$ such that $q < p < 2q$. Then $\alpha_1 < (p^2 - 1)(q^2 - 1) < \alpha_2$ where $\alpha_1 = N^2 + 1 - \frac{5}{2}N$ and $\alpha_2 = N^2 + 1 - 2N$.

**Lemma 2:** [14] Suppose an RSA modulus $N = pq$ such that $q < p < \lambda q$. Then $\phi_1 < (p^2 - 1)(q^2 - 1) < \phi_2$ where $\phi_1 = N^2 + 1 - (\lambda + \frac{1}{2})N$ and $\phi_2 = N^2 + 1 - 2N$.

We apply the result of Lemma 1 and introduce a method known as the continuous midpoint subdivision analysis that is defined as follows.

**Definition 2 (Continuous Midpoint Subdivision Analysis):** As from Lemma 1, suppose that $\omega(N) \in (\alpha_1, \alpha_2)$ where $\omega(N) = (p^2 - 1)(q^2 - 1)$. $\alpha_1 = N^2 + 1 - \frac{5}{2}N$ and $\alpha_2 = N^2 + 1 - 2N$. Then, suppose we divide equally the interval $(\alpha_1, \alpha_2)$ to obtain a midpoint term denoted as $\mu(0, 0) = N^2 + 1 - \frac{7}{4}N$ as illustrated in Figure 1. We denote this process as $i = 0$.

Observe that, no matter where $\omega(N)$ is situated on the interval, we always have

$$|\omega(N) - \mu(0, 0)| < \frac{\alpha_2 - \alpha_1}{2}.$$  

Continuing, we divide equally between the midpoint of the above intervals; $(\alpha_1, \mu(0, 0))$ and $(\mu(0, 0), \alpha_2)$, which yields another two midpoints; $\mu(1, 0) = N^2 + 1 - \frac{19}{16}N$ and $\mu(1, 1) = N^2 + 1 - \frac{15}{16}N$ as illustrated in Figure 2.

Note that, this process is the first division between the midpoints and we denote this process as $i = 1$. Then, no matter where $\omega(N)$ is situated on the interval, we always have

$$|\omega(N) - \mu(1, j)| < \frac{\alpha_2 - \alpha_1}{4}, \quad 0 \leq j \leq 1.$$  

Continuously after the first division between midpoints, we equally divide between midpoints obtained previously as illustrated by the following Figure 3 and denoted the process with $i = 2$.

Here, the midpoints obtained from the second division of midpoints are $\mu(2, 0) = N^2 + 1 - \frac{29}{32}N$, $\mu(2, 1) = N^2 + 1 - \frac{27}{32}N$, $\mu(2, 2) = N^2 + 1 - \frac{35}{16}N$ and $\mu(2, 3) = N^2 + 1 - \frac{33}{16}N$. Then, no matter where $\omega(N)$ is situated on the interval, we always have

$$|\omega(N) - \mu(2, j)| < \frac{\alpha_2 - \alpha_1}{8}, \quad 0 \leq j \leq 3.$$  

Similarly, the process continues and the midpoints obtained from the third division between the previous midpoints are as follows; $\mu(3, 0) = N^2 + 1 - \frac{79}{512}N$, $\mu(3, 1) = N^2 + 1 - \frac{77}{512}N$, $\mu(3, 2) = N^2 + 1 - \frac{75}{512}N$, $\mu(3, 3) = N^2 + 1 - \frac{73}{512}N$, $\mu(3, 4) = N^2 + 1 - \frac{71}{512}N$, $\mu(3, 5) = N^2 + 1 - \frac{69}{512}N$, $\mu(3, 6) = N^2 + 1 - \frac{67}{512}N$ and $\mu(3, 7) = N^2 + 1 - \frac{65}{512}N$. Note that
this process is denoted as \( i = 3 \). Refer to Figure 4 for the illustration of the process.

Therefore, regardless of where the interval of \( \omega(N) \) may situate, we always have

\[
|\omega(N) - \mu(3,j)| < \frac{\alpha_2 - \alpha_1}{16}, \quad 0 \leq j \leq 7.
\]

To sum up, we have the following general result.

Suppose \( \omega(N) \in (\alpha_1, \alpha_2) \) such that \( \omega(N) = (p^2 - 1)(q^2 - 1) \), \( \alpha_1 = N^2 + 1 - \frac{5}{2}N \) and \( \alpha_2 = N^2 + 1 - 2N \). Let \( i \) and \( j \) be fixed positive integers for

\[
\mu_{(i,j)} = N^2 + 1 - \frac{10(2^i - 1)}{2^{i+2}}jN,
\]

then

\[
|\omega(N) - \mu_{(i,j)}| < \frac{\alpha_2 - \alpha_1}{2^{i+1}}\]

for the specific \( \mu_{(i,j)} \).

**Remark 1:** An integer \( i \) is the number of subdivision process between the midpoints in the interval of \( \omega(N) \) where \( \omega(N) \in (N^2 - \frac{5}{2}N + 1, N^2 - 2N + 1) \) whilst \( j \) denotes each midpoint term in the \( i \)-th subdivision process.

### III. Attack I

As a consequence of Definition 2, we propose the following result by considering the case when the distinct primes \( p \) and \( q \) have the same-bit sizes. Remark that Theorem 2 can be regarded as the extension and improved result upon [3].

**Theorem 2:** Suppose \( i \) and \( j \) are fixed positive integers. Consider a variant of the RSA cryptosystem with the public key pair \( (N, e) \) such that \( N = pq \) where \( q < p < 2q \). If \( e \in (p^2-1)(q^2-1) \) satisfies an equation \( ed - k(p^2 - 1)(q^2 - 1) = 1 \) for some positive integers \( k \) and \( d \) with

\[
d < \sqrt{\frac{2^{i+1}N^3 - [2^{i+1}(5 + 4(2^i)) - 2j]N^2}{e}},
\]

then \( \frac{k}{d} \) can be found amongst the convergents of the public rational number \( \frac{e}{\mu_{(i,j)}} \) given that \( \mu_{(i,j)} = N^2 + 1 - \frac{10(2^i - 1)}{2^{i+2}}jN \) for some \( j \in [0, 2^i - 1] \).

**Proof:** Let \( \omega(N) = (p^2 - 1)(q^2 - 1) \) be the modified Euler quotient. Suppose \( \omega(N) \in (\alpha_1, \alpha_2) \) where \( \alpha_1 = N^2 + 1 - \frac{5}{2}N \) and \( \alpha_2 = N^2 + 1 - 2N \). Let \( \mu_{(i,j)} = N^2 + 1 - \frac{10(2^i - 1)}{2^{i+2}}jN \) be the general term for midpoint in the interval of \( (\alpha_1, \alpha_2) \). Then, there exists a \( \mu_{(i,j)} \) such that

\[
|\omega(N) - \mu_{(i,j)}| < \frac{\alpha_2 - \alpha_1}{2^{i+1}} = \frac{1}{2^{i+1}}N \tag{2}
\]

From the equation \( ed - k\omega(N) = 1 \), dividing by \( d\omega(N) \) to obtain

\[
\frac{e}{\omega(N)} - \frac{k}{d} = \frac{1}{d\omega(N)}
\]

Let \( \mu_{(i,j)} \) be the approximation of \( \omega(N) \) and observe

\[
\left| \frac{e}{\mu_{(i,j)}} - \frac{k}{d} \right| = \left| \frac{e}{\mu_{(i,j)}} - \frac{e}{\omega(N)} + \frac{e}{\omega(N)} - \frac{k}{d} \right| \\
\leq \left| \frac{e}{\mu_{(i,j)}} - \frac{e}{\omega(N)} \right| + \left| \frac{e}{\omega(N)} - \frac{k}{d} \right| \\
\leq \frac{e}{\omega(N) - \mu_{(i,j)}} + \frac{1}{d\omega(N)} \tag{3}
\]

Next, since \( d = \frac{1 + k\omega(N)}{e} \) and from (2), then (3) yields

\[
\left| \frac{e}{\mu_{(i,j)}} - \frac{k}{d} \right| < \frac{Ne}{2^{i+2} \cdot \mu_{(i,j)} \cdot \omega(N)} + \frac{1}{\omega(N) \cdot [1 + k\omega(N)]}
\]

(4)

Observe from Lemma 1,

\[
\alpha_1 < \omega(N) < \alpha_2 \implies \frac{1}{\alpha_2} < \frac{1}{\omega(N)} < \frac{1}{\alpha_1}
\]

which will lead (4) to

\[
\left| \frac{e}{\mu_{(i,j)}} - \frac{k}{d} \right| < \frac{Ne}{2^{i+2} \cdot \mu_{(i,j)} \cdot \omega(N)} + \frac{e}{\omega(N) \cdot (\alpha_1)(\alpha_1)} \\
= \frac{e(N + 2^{i+2})}{2^{i+2} \cdot (\alpha_1)^2} \\
< \frac{e(N + 2^{i+2})}{2^{i+2} \cdot (\alpha_1 - 1)^2} \\
= \frac{e(N + 2^{i+2})}{2^{i+2}(N^2 - \frac{5}{2}N)^2} \tag{5}
\]

To ensure (5) satisfies the condition of Legendre’s Theorem which yields

\[
\frac{e(N + 2^{i+2})}{2^{i+2}(N^2 - \frac{5}{2}N)^2} < \frac{1}{2^{i+1}}
\]

we solve for \( d \) to obtain

\[
d < \sqrt{\frac{2^{i+2}(N^4 - 5N^3 + \frac{25}{2}N^2)}{2e(N + 2^{i+2})}} \tag{6}
\]

Observe

\[
\sqrt{\frac{2^{i+2}(N^4 - 5N^3 + \frac{25}{2}N^2)}{2e(N + 2^{i+2})}} < \sqrt{\frac{2^{i+1}N^3 - 2^{i+1}(5 + 4(2^i))N^2}{e}}
\]

Thus

\[
d < \sqrt{\frac{2^{i+1}N^3 - 2^{i+1}(5 + 4(2^i))N^2}{e}} \tag{7}
\]

Furthermore

\[
\sqrt{\frac{2^{i+1}N^3 - 2^{i+1}(5 + 4(2^i))N^2}{e}} < \frac{1}{\sqrt{\frac{2^{i+1}N^3 - [2^{i+1}(5 + 4(2^i)) - 2j]N^2}{e}}}
\]
Hence, we deduce for each midpoint term $j$

$$d < \sqrt{2^{i+1}N^3 - [2^{i+1}(5 + 4(2^i)) - 2j]N^2}$$

(8)

If (8) holds, then (5) satisfies the condition of Legendre’s Theorem

$$\left| \frac{e}{\mu_{(i,j)}} - k \right| < \frac{1}{2d^2}.$$ 

Thus $\frac{e}{d}$ is amongst the convergents of the continued fractions expansion of $\frac{e}{\mu_{(i,j)}}$.

Consequently, with the knowledge of $k$ and $d$ implies that one can obtain the prime factorization of modulus $N = pq$ efficiently as proved in the following corollary.

Corollary 1: Suppose we obtain the private parameters $k$ and $d$ according to Theorem 2, then $N = pq$ can be factored in polynomial time.

Proof: Based on the relation $\omega(N) = (p^2 - 1)(q^2 - 1) = ed - 1$ from Theorem 2, by finding the roots of quadratic polynomial $X^2 - (N^2 - \omega(N) + 1)X + N^2 = 0$, one can retrieve the prime factors modulus $N = pq$.

Next, we provide an algorithm referring to Theorem 2 and Corollary 1.

Algorithm 1 Algorithm for Factoring Modulus $N$

Input: The public key pair $(N, e)$

Output: The prime factors $p$ and $q$

1. Compute the continued fractions of $\frac{e}{\mu_{(i,j)}} = \frac{1}{2^{i+1}N^3 - [2^{i+1}(5 + 4(2^i)) - 2j]N^2}$.

2. For each convergent $\frac{e}{k}$ of $\frac{e}{\mu_{(i,j)}}$, compute $\omega(N)^j = \frac{ed - 1}{k}$.

3. For $\omega(N)^j$ be an integer, proceed to Step 4. Else, repeat Step 2.

4. Solve the roots $X_1$ and $X_2$ of the polynomial $X^2 - (N^2 - \omega(N)^j + 1)X + N^2 = 0$.

5. Return the value of primes $p = \sqrt{X_1}$ and $q = \sqrt{X_2}$.

Remark 2: One can observe that the continuous midpoint subdivision analysis increases the upper bound of private exponent $d$ exponentially from $d < \sqrt{2N - 18} \approx \sqrt{2}N$ to $d < \sqrt{2^{i+1}N - [2^{i+1}(5 + 4(2^i)) - 2j]} \approx \sqrt{2}N$ for $e < N^2$. This can be achieved by increasing the number of subdivisions $i$ on the interval of modified Euler quotient. Based on the current technologically advancement, $i = 112$ is a feasible target [1].

Remark 3: In relation with Theorem 2, this method is applicable whenever

$$e > \frac{N^2 + 1 - \frac{5N}{2}}{d} \approx \frac{1}{2^{i+1}N}.$$ 

Remark 4: By letting $i = 0, j = 0$ and applying to Theorem 2, we obtain the result as in [3]. We recall that the attack in [3] works only if the condition $d < \sqrt{2^{i+1}N^3 - [2^{i+1}(5 + 4(2^i)) - 2j]N^2}$ is satisfied.

A. NUMERICAL EXAMPLES

In this section, we demonstrate the proposed attack based on Theorem 2.

By considering the case when $i = 1, j = 0$, we will have two midpoints which are; $\mu_{(1,0)} = N^2 - \frac{19}{8}N + 1$, the midpoint of the interval ($N^2 - \frac{19}{8}N + 1, N^2 - \frac{17}{8}N + 1$) and $\mu_{(1,1)} = N^2 - \frac{17}{8}N + 1$, the midpoint of the interval ($N^2 - \frac{17}{8}N + 1, N^2 - 2N + 1$). Note that the former midpoint is the situation when $j = 0$ while the latter is the situation when $j = 1$.

Example 1: When $i = 1, j = 0$.

As an illustration of our first attack, on input of an RSA modulus $N$ and public exponent $e$ satisfying the condition stated in Theorem 2,

$$N = 173276358253790788733361489927580784671, e = 2802331803465028017651205628479261648419547\ 6841032411777890597828347435382031.$$ 

We begin the process of factoring $N$.

Let $\mu_{(1,0)} = N^2 - \frac{19}{8}N + 1$, then $\frac{e}{d}$ amongst the convergents of continued fractions expansion of $\frac{e}{\mu_{(1,0)}}$.

We list the convergents are

$$\left[0, 1, \frac{17}{49}, \frac{19}{52}, \frac{14927}{37325}, \frac{19}{5384020490006295699}, \frac{5768538188285732038}{19936121815667976239}, \frac{23991245551777600906}{25704660003951708271} \right].$$ 

Now, from the list of the above convergents, we obtain the candidate for $\frac{k}{d}$ by applying Step 2 from Algorithm 1 to compute $\omega(N) = \frac{ed}{k}$ which will result in $\omega(N) = 300246963296960511957383885901114896096\ 69139785147342564797732538621308286400$.

We continue to find the roots $X_1$ and $X_2$ of the polynomial $X^2 - (N^2 - \omega(N) + 1)X + N^2 = 0$ upon obtaining the value of $\omega(N)$; which returns the value of primes $p = \sqrt{X_1}$ and $q = \sqrt{X_2}$ where in this case, $p = 1825991824606033389$ and $q = 9489437799013092539$. This completes the factorization of $N$.

Observe from Example 1, we can verify that the condition $d < \sqrt{\frac{2N^3 - 18N}{e}} \approx 27250795559553171350$ is met as required by Theorem 2. Moreover, the approach in [3] will fail to retrieve primes $p$ and $q$ as $d > \sqrt{\frac{2N^3 - 18N}{e}} \approx 1926922232888305241$.

Example 2: When $i = 1, j = 1$.

Now, on input of the following RSA modulus $N$ and public exponent $e$ satisfying the condition stated in Theorem 2,

$$N = 14589658033221814696078687868248654687, e = 20205411156411990435099327599556561348468\ 5332722445850230242816060657421597.$$ 

We begin the process of factoring $N$. 
Let \( \mu_{(1)} = N^2 - \frac{q}{c} \times N + 1 \), then \( \frac{k}{d} \) is amongst the convergents of continued fractions expansion of \( e^{\mu_{(1)}} \). The list of the convergents are

\[
\begin{bmatrix}
0, 1, 0, 18, 19, 51, 131, 158, 175, 192, 209, 226, 0.369045\%
\end{bmatrix}
\]

We solve for the roots \( X_1 \) and \( X_2 \) from the polynomial \( X^2 - (N^2 - \omega(N) + 1)X + N^2 = 0 \) upon obtaining the value of \( \omega(N) \); which returns the value of primes \( p = \sqrt{X_1} \) and \( q = \sqrt{X_2} \) where in this case, \( p = 13119615460534710209 \) and \( q = 922649036772134793 \). This completes the factorization of \( N \).

As observed from Example 3, we certify that the condition \( d < \frac{\sqrt{2048N^2 - 839848N^2}}{e} \approx 734405316607763478232 \) is met as required by Theorem 2.

On input of an RSA modulus \( N \) and public exponent \( e \) satisfying the condition stated in Theorem 2,

\[
N = 1703779965194420095617575767091446971, e = 23666170319596025875311781968690724514705
\]

We begin the process of factoring \( N \). Let \( \mu_{(2,0)} = N^2 - 10485759N + 1 \), then \( \frac{k}{d} \) is amongst the convergents of continued fractions expansion of \( e^{\mu_{(2,0)}} \). The list of the convergents are

\[
\begin{bmatrix}
0, 1, 3, 4, 5, 15, 79, 173, 771, 2486, 13201, 398516, 888583
\end{bmatrix}
\]

We begin the process of factoring \( 36833459837695661230 \) from the list of the above convergents, and we apply Step 2 from Algorithm 1 to compute \( \omega(N) = \frac{ed-1}{k} \) which will result in

\[
\omega(N) = 289573426212253812227849261346361688311
\]

We continue to find the roots \( X_1 \) and \( X_2 \) from the polynomial \( X^2 - (N^2 - \omega(N) + 1)X + N^2 = 0 \) upon obtaining the value of \( \omega(N) \); which returns the value of primes \( p = \sqrt{X_1} \) and \( q = \sqrt{X_2} \) where in this case, \( p = 1838477923891572031 \) and \( q = 926733980963082741 \). This completes the factorization of \( N \).
retrieve primes $p$ and $q$ as $d > \sqrt{2N^3 - 18N^2} \approx 64650407337215126215$. In this case, $d = 36860175068451$ 2962801 is 3 bits larger than the bound in [3]. We can observe that our strategy is able to identify the private exponent $d$ which is up to $\frac{d}{2} = 3080$ to 10 bits longer than the bound in [3].

IV. ATTACK II

In this section, we present an improvement upon [14] by considering the distinct primes $p$ and $q$ to be unbalanced or the primes are said to be of arbitrary sizes (i.e. $q < p < \lambda q$ for a chosen parameter $\lambda$).

Consequently from Definition 2, we extend our method (i.e. the continuous midpoint subdivision analysis) for the case when the primes $p$ and $q$ are said to be unbalanced.

**Lemma 3:** Suppose $o(N) = (p^2 - 1)(q^2 - 1)$ such that $o(N) \in (\phi_1, \phi_2)$, $\phi_1 = N^2 + 1 - (\lambda + \frac{1}{\lambda})N$ and $\phi_2 = N^2 + 1 - 2N$. Let $i, j \in \mathbb{Z}^+$ be fixed integers and define $\mu_{(i,j)} = N^2 + 1 - \frac{(\lambda^2 + 1)(2^{i+1}) - (\lambda - 1)^2}{\lambda(2^{i+1})}N$, then

$$|o(N) - \mu_{(i,j)}| < \frac{\phi_2 - \phi_1}{2^{i+1}}$$

for the specific $\mu_{(i,j)}$.

**Theorem 3:** Suppose $i$ and $j$ are fixed positive integers. Consider a variant of the RSA cryptosystem with the public key pair $(N, e)$ such that $N = pq$ where $q < p < \lambda q$. If $e < (p^2 - 1)(q^2 - 1)$ satisfies an equation $ed - k(p^2 - 1)(q^2 - 1) = 1$ for some positive integers $k$ and $d$ where $d$ as shown at the bottom of the next page, then the unknown $\frac{k}{e}$ is a convergent of continued fractions expansion of public rational number $\frac{e}{\mu_{(i,j)}}$ given that $\mu_{(i,j)} = N^2 + 1 - \frac{(\lambda^2 + 1)(2^{i+1}) - (\lambda - 1)^2}{\lambda(2^{i+1})}N$ for some $j \in [0, 2^i - 1]$.

**Proof:** Let $o(N) = (p^2 - 1)(q^2 - 1)$ be the modified Euler quotient. From Lemma 2, we have $o(N) \in (\phi_1, \phi_2)$ where $\phi_1 = N^2 + 1 - (\lambda + \frac{1}{\lambda})N$ and $\phi_2 = N^2 + 1 - 2N$. Let $\mu_{(i,j)} = N^2 + 1 - \frac{(\lambda^2 + 1)(2^{i+1}) - (\lambda - 1)^2}{\lambda(2^{i+1})}N$ represents the general term for midpoint in the interval of $(\phi_1, \phi_2)$. Then, for a chosen parameter $\lambda$, there exists a $\mu_{(i,j)}$ such that

$$|o(N) - \mu_{(i,j)}| < \frac{\phi_2 - \phi_1}{2^{i+1}} = \frac{(\lambda - 1)^2}{\lambda(2^{i+1})}N \quad (9)$$

From the equation $ed - k\omega(N) = 1$, divide with $d\omega(N)$ to obtain

$$\frac{e}{\omega(N)} - \frac{k}{d} = \frac{1}{d\omega(N)}$$

Let $\mu_{(i,j)}$ be the approximation of $\omega(N)$ and observe

$$\left| \frac{e}{\mu_{(i,j)}} - \frac{k}{d} \right| = \left| \frac{\omega(N) - \mu_{(i,j)} \omega(N)}{\mu_{(i,j)} \omega(N)} \right| < \frac{1}{\mu_{(i,j)} \omega(N)} \quad (10)$$

Since $d = \frac{1 + k\omega(N)}{e}$ and from (9), then (10) yields

$$\left| \frac{e}{\mu_{(i,j)}} - \frac{k}{d} \right| < \frac{(\lambda - 1)^2Ne}{\lambda(2^{i+1}) \cdot \omega(N)} + \frac{1}{\mu_{(i,j)} \omega(N)} \quad (11)$$

Then from Lemma 2, we observe $\phi_1 < o(N) < \phi_2 \implies \frac{1}{\phi_2} < \frac{1}{o(N)} < \frac{1}{\phi_1}$ will lead (11) to

$$\left| \frac{e}{\mu_{(i,j)}} - \frac{k}{d} \right| < \frac{(\lambda - 1)^2Ne}{\lambda(2^{i+1}) \cdot o(N) + \phi_1}$$

To ensure (12) satisfies the condition of Legendre’s Theorem which yields

$$\frac{e(\lambda - 1)^2N + 2^{i+1}}{2^{i+1}N^2(N - (\lambda + \frac{1}{\lambda})^2)} < \frac{1}{2d^2}$$

we solve for $d$ to obtain

$$d < \sqrt{\frac{2(N^4 - 2(\lambda + \frac{1}{\lambda})N^2 + (\lambda + \frac{1}{\lambda})^2N^2)}{e(\lambda - 1)^2N + 2^{i+1}}} \quad (13)$$

Observe that (13) is less than

$$d < \sqrt{\frac{\lambda(\lambda - 1)^2(2^i)^N^3 - 2^i(1)(\lambda - 1)^2(\lambda^2 + 1) + \lambda^2(2^i)N^2}{(\lambda - 1)^4e}}$$

Thus

$$d < \sqrt{\frac{\lambda(\lambda - 1)^2(2^i)^N^3 - 2^i(1)(\lambda - 1)^2(\lambda^2 + 1) + \lambda^2(2^i)N^2}{(\lambda - 1)^4e}} \quad (14)$$

Furthermore, for each midpoint term $\frac{k}{e}$, (14) is less than (15) as shown at the bottom of the next page. If (16) holds as shown at the bottom of the next page, then (12) satisfies the condition of Legendre’s Theorem;

$$\left| \frac{e}{\mu_{(i,j)}} - \frac{k}{d} \right| < \frac{1}{2d^2}$$

Thus, the unknowns $\frac{k}{e}$ can be obtained amongst convergents of the continued fractions expansion of $\frac{e}{\mu_{(i,j)}}$. This terminates the proof.
Consequently, with the knowledge of \( k \) and \( d \) implies that one can efficiently find the prime factorization of modulus \( N = pq \).

Suppose we obtain the private parameters \( k \) and \( d \) according to Theorem 3, then \( N = pq \) can be factored in polynomial time. The proof is similar to the proof in Corollary 1.

Next, we provide an algorithm referring to Theorem 3.

**Algorithm 2 Algorithm to cryptanalyse modulus \( N = pq \)**

**Input:** The public key pair \( \left( N, e \right) \)

**Output:** The prime factors \( p \) and \( q \)

1. Compute the continued fractions of 
   \[
   \frac{e}{\mu_{10,0}} = \frac{1}{N^2 + 1 - \frac{1}{\mu^{0,0}}},
   \]
   where for each convergent \( \frac{e}{d} \), compute \( \omega(N) = \frac{ed - 1}{k} \).

2. For each convergent, \( \frac{e}{d} \), compute \( \omega(N) \) be an integer, proceed to Step 4. Else, repeat Step 2.

3. Solve the roots \( X_1 \) and \( X_2 \) of the polynomial 
   \[ X^2 - (N^2 - \omega(N) + 1)X + N^2 = 0. \]

4. Return the value of primes \( p = \sqrt{X_1} \) and \( q = \sqrt{X_2} \).

**Remark 5:** In the case when the primes \( p \) and \( q \) are of arbitrary sizes, one can observe that the continuous mid-point subdivision analysis increases the upper bound of private exponent \( d \) exponentially from \( d \approx \sqrt{\frac{\lambda}{\lambda - 1}} \sqrt{N} \) to \( d \approx \sqrt{\frac{\lambda}{\lambda - 1}} \sqrt{N} \) for \( e < N^2 \). This can be achieved by increasing the number of subdivisions \( i \) on the interval of modified Euler quotient. Based on the current technologically advancement, \( i = 112 \) is a feasible target [1].

**Remark 6:** In relation with Theorem 3, this method is applicable whenever 
\[
e > \frac{N^2 + 1 - (\lambda + \frac{1}{2})N}{\lambda \cdot d} \approx \frac{(\lambda - 1)^2}{\lambda \cdot 2^e} N.
\]

**A. NUMERICAL EXAMPLES**

**Arbitrary size primes \( p \) and \( q \) where \( q < p < 6q \)**

In this section, we illustrate the proposed attack by running Algorithm 2.

Now we contemplate a chosen parameter \( \lambda \) to be an even integer which we set \( \lambda = 6 \). We choose two distinct unbalanced bits of RSA primes \( p \) and \( q \) satisfying \( q < p < 6q \). We run Algorithm 2 to verify that we successfully extend the proposed result in [14].

In Example 5, we consider the case when \( i = 10 \) and \( j = 0 \), which yields the midpoint term \( \mu_{10,0} = N^2 + 1 - \frac{75751}{12288} \) whilst in Example 6 we consider the case when \( i = 20 \) and \( j = 0 \), which yields the midpoint term \( \mu_{20,0} = N^2 + 1 - \frac{75759}{12288} \).

**Example 5:** When \( i = 10 \), \( j = 0 \).

On input of an RSA modulus \( N \) and public exponent \( e \) satisfying the condition stated in Theorem 3,

\[
N = 61868200535000364246892296276769053449,
\]

\[
e = 63287295168316059964575337334742966045748
\]

We begin the process of factoring \( N \).

Let \( \mu_{10,0} = N^2 + 1 - \frac{75751}{12288} \), then \( \frac{1}{d} \) is amongst the convergents of continued fractions expansion of \( \frac{e}{\mu_{10,0}} \). The list of the convergents are

\[
0, 601, 10, 1005, 11, 13807, 260068, 54, 2546247, 847402775949226659914729376261.
\]

Now, from the list of the above convergents, we acquire the candidate for \( k = \frac{1}{d} \) and after applying Step 2 from Algorithm 2 to compute \( \omega(N) = \frac{ed - 1}{k} \) which will result in

\[
\omega(N) = 38276742374390193568245536722032094354
\]

\[
225587828807047923029122296719435929600.
\]

We proceed to find the roots \( X_1 \) and \( X_2 \) for the polynomial 
\[
X^2 - (N^2 - \omega(N) + 1)X + N^2 = 0
\]

once we acquire the value of \( \omega(N) \), which returns the value of primes \( p = \sqrt{X_1} \) and \( q = \sqrt{X_2} \) where in this case, \( p = 60972476407428265289 \)

\[
\sqrt{(\lambda - 1)^2(2^e)N^2 - [2^i]((\lambda - 1)^2(2^e) + \lambda^2(2^e)) - 2(\lambda - 1)^4]} \quad (15)
\]

\[
d < \sqrt{(\lambda - 1)^2(2^e)N^3 - [2^i]((\lambda - 1)^2(2^e) + \lambda^2(2^e)) - 2(\lambda - 1)^4]} \quad (16)
\]
and \( q = 10146906305984149441 \). This completes the factorization of \( N \).

We observe from Example 5, that the condition \( d < \sqrt{153600N^3 - 77391872N^2} \approx 30324842827054009052754 \) is met as required by Theorem 3. However, for this case, the approach in [14] fails to retrieve primes \( p \) and \( q \) as in this case \( d > \sqrt{150N^3 - 1922N^2} \approx 947651338345437782899 \). That is, \( d = 12238123148187295412941 \) is 4 bits larger than the proposed bound in [14]. We can observe that our strategy is able to identify the private exponent \( d \) which is up to \( \frac{d}{2} = \frac{10}{2} = 5 \) bits longer than the bound in [14].

**Example 6:** When \( i = 20, j = 0 \).

Now, we consider the following public pair \((N, e)\) of variants of RSA cryptosystem fulfilling the condition of Theorem 3,

\[
N = 1729220360784955854194824786156685018953,
\]

\[
e = 33621600455964098963558750498741521029151729820619974758772567091715109605851.
\]

We begin the process of factoring \( N \).

Let \( \mu_2(20) = N^2 + 1 - 77594599 = 1282593 \), then \( k \) can be found amongst the convergents of continued fractions expansion of \( \frac{e}{\mu_2(20)} \). The list of the convergents are

\[
[0, 1, 1, 9, \ldots, 254, 809, 2681, 16895, 70261, 368200, 806661, 1981522, 2788183, 31046071, 13134254, 3274659, 7174198, 17625055, 24797253, 92014847, 70812067, 234556940281038764442, 208007820614857874672911, \ldots]
\]

We obtain the candidate for \( \ell = 2^{324556940281038764442} \) from the list of the above convergents, and applied Step 2 from Algorithm 2 to compute \( \omega(N) = \frac{ed - 1}{k} \) which results in

\[
\omega(N) = 2990203056153252890165920546744298798584296283994609533493059694192540895674880.
\]

Then, we solve for the roots \( X_1 \) and \( X_2 \) from the polynomial \( X^2 - (N^2 - \omega(N) + 1)X + N^2 = 0 \), which returns the value of primes \( p = \sqrt{X_1} \) and \( q = \sqrt{X_2} \) such that \( p = 101859262917187999631 \) and \( q = 16976564636942436263 \). This completes the factorization of \( N \).

We verify that \( d < \sqrt{157286400N^3 - 79166777065472N^2} \approx 62211675327338161310123 \) fulfilled the condition of Theorem 3. Again, the approach in [14] failed to retrieve the required primes \( p \) and \( q \) as in this case \( d > \sqrt{150N^3 - 1922N^2} \approx 60753589186853673154 \). That is, \( d = 20860782061488758742611 \) is 9 bits larger than the condition of \( d \) in [14]. We observe that our strategy is able to identify the private exponent \( d \) which is up to \( \frac{d}{2} = \frac{20}{2} = 10 \) bits longer than the bound in [14].

**V. Conclusion**

In conclusion, the work presented in this paper focuses on a cryptanalysis method to factor the modulus \( N = pq \) of some RSA cryptosystem variants where the prime factors \( p \) and \( q \) are of arbitrary sizes satisfying \( q < p < \lambda q \) for a chosen parameter \( \lambda \). Precisely, we propose a generalization of previous works in [3] and [14] by introducing a strategy known as the continuous midpoint subdivision analysis. We demonstrate that the unknowns \( d \) and \( k \) can be found using the continued fractions expansion of certain related numbers under certain assumptions. Remark that we have successfully improved earlier attacks exponentially.

**REFERENCES**

[1] E. Barker, “NIST special publication 800-57—Part 1 revision 4; Recommendation for key management—Part 1: General,” Dept. Comm., Nat. Inst. Standards Technol. Gaithersburg, MD, USA, Jan. 2016, doi: 10.6028/NIST.SP.800-57pt1r4.

[2] D. Boneh and G. Durfee, “Cryptanalysis of RSA with private key \( d \) less than \( \frac{N}{3} \),” IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1339–1349, Jul. 2000.

[3] M. Bunder, A. Nitaj, W. Susilo, and J. Tonien, “A new attack on three variants of the RSA cryptosystem,” in Proc. Australas. Conf. Inf. Secur. Privacy, 2016, pp. 258–268.

[4] G. Castagnos, “An efficient probabilistic public-key cryptosystem over quadratic fields quotients,” Finite Fields Their Appl., vol. 13, no. 3, pp. 563–576, Jul. 2007.

[5] H. Elkamchouchi, K. Elshenawy, and H. Shaban, “Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers,” in Proc. 8th Int. Conf. Commun. Syst. ICCS, Nov. 2002, pp. 91–95.

[6] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers. London, U.K.: Oxford Univ. Press, 1965.

[7] H. Kuwakado, K. Koyama, and Y. Tsuruoka, “A new RSA-type scheme based on singular cubic curves \( y^2 = x^3 + bx^2 \) (mod \( n \)),” IEICE Trans. Fundamentals Electron., vol. 78, no. 1, pp. 27–33, 1995.

[8] A. Nitaj, “Another generalization of Wiener’s attack on RSA,” in Proc. Int. Conf. Cryptol. Afr., 2008, pp. 174–190.

[9] A. Nitaj, “Diophantine and lattice cryptanalysis of the RSA cryptosystem,” in Artificial Intelligence, Evolutoinary Computing and Metaheuristics. Berlin, Germany: Springer, 2013, pp. 139–168.

[10] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM, vol. 26, no. 1, pp. 96–99, Jan. 1983.

[11] M. J. Wiener, “Cryptanalysis of short RSA secret exponents,” IEEE Trans. Inf. Theory, vol. 36, no. 3, pp. 553–558, May. 1990.

[12] M. Bunder, A. Nitaj, W. Susilo, and J. Tonien, “A generalized attack on RSA type cryptosystems,” Theor. Comput. Sci., vol. 704, pp. 74–81, Dec. 2017.

[13] D. Coppersmith, “Small solutions to polynomial equations, and low exponent RSA vulnerabilities,” J. Cryptol., vol. 10, no. 4, pp. 233–260, Sep. 1997.

[14] M. Bunder, A. Nitaj, W. Susilo, and J. Tonien, “Cryptanalysis of RSA-type cryptosystems based on Lucas sequences, Gaussian integers and elliptic curves,” J. Inf. Secur. Appl., vol. 40, pp. 193–198, Jun. 2018.

[15] J. Tonien, “Continued fractions and their applications,” Ph.D. dissertation, School Math. Appl. Statist., Univ. Wollongong, Wollongong, Australia, 2016.

[16] L. Feng, L. Hu, Y. Lu, and H. Wei, “An improved analysis on three variants of the RSA cryptosystem,” in Proc. Int. Conf. Inf. Secur. Crypto., 2016, pp. 140–149.

[17] M. Zheng, N. Kumhiro, and H. Hu, “Cryptanalysis of RSA variants with modified Euler quotient,” in Proc. Int. Conf. Cryptol. Afr., 2018, pp. 266–281.

[18] A. Nitaj, Y. Pan, and J. Tonien, “A generalized attack on some variants of the RSA cryptosystem,” in Proc. Int. Conf. Sel. Areas Cryptogr., 2018, pp. 421–433.
W. N. A. Ruzai et al.: On the Improvement Attack Upon Some Variants of RSA Cryptosystem via the Continued Fractions Method

[19] X. Zhang, S.-H. Seo, and C. Wang, “A lightweight encryption method for privacy protection in surveillance videos,” IEEE Access, vol. 6, pp. 18074-18087, 2018.

[20] L. Chen, S. Jordan, Y. K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, “Report on post-quantum cryptography,” in US Department of Commerce, National Institute of Standards and Technology, vol. 28. Gaithersburg, MD, USA, Apr. 2016, doi: 10.6028/NIST.IR.8105.

WAN NUR AQLILI RUZAI received the B.S. degree in mathematical sciences from International Islamic University Malaysia, Malaysia, in 2014, and the M.S. degree in mathematics from Universiti Kebangsaan Malaysia, Malaysia, in 2016. She is currently pursuing the Ph.D. degree in mathematical cryptography with the Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia. Her current research interests include mathematical cryptography, algebraic cryptanalysis, and post-quantum cryptography. She is a member of the Malaysian Society of Cryptology Research (MSCR).

MUHAMMAD REZAL KAMEL ARIFFIN received the B.S. and M.S. degrees in mathematics from Universiti Putra Malaysia, Malaysia, in 1999 and 2002, respectively, and the Ph.D. degree in mathematics from Universiti Kebangsaan Malaysia, Malaysia, in 2009. He has been the Deputy President of MSCR, since 2018. He is currently the Director of the Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia. His research interests include mathematical cryptography, information security, cryptographic programming, and chaotic secure communication. He has been a member of Malaysian Society for Cryptology Research (MSCR), since 2007.

MUHAMMAD ASYRAF ASBULLAH received the B.S. degree in mathematics education from Universiti Teknologi Malaysia, Malaysia, and the M.S. degree in computational mathematics and the Ph.D. degree in mathematical cryptography from Universiti Putra Malaysia, Malaysia, in 2010 and 2015, respectively. Since 2016, he has been an Associate Researcher with the Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia. He is the author of more than 20 publications and holds eight intellectual properties. His research interests involve mathematical cryptography, design, and analysis of asymmetric cryptosystems, and computational number theory. He was a recipient of the Malaysian Science and Mathematics Association Award for Excellence Doctoral Thesis, in 2016, and the Best Paper Award, in 2017. He has also been acting as the Secretary of the Malaysian Society of Cryptology Research (MSCR), since 2013. He was appointed as a Reviewer for several IEEE conferences and journals.

ZAHARI MAHAD received the B.S. degree in computer sciences and software engineering and the M.S. degree in mathematical cryptography from Universiti Putra Malaysia, in 2009 and 2014, respectively. He is currently a Research Officer with the Laboratory of Cryptography, Analysis, and Structure, Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia. His research interests are cryptography, information security, and chaotic secure communication. He has been a member of Malaysian Society for Cryptology Research (MSCR), since 2007.

ATHIRAH NAWAWI received the B.S. degree in mathematics (with education) from Universiti Putra Malaysia, in 2006, and the M.S. and Ph.D. degrees in pure mathematics from the University of Manchester, U.K., in 2013 and 2008, respectively. She is currently a Senior Lecturer with the Department of Mathematics, Faculty of Science, and an Associate Researcher with the Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research (INSPEM), UPM. She has been actively involved with schools and community outreach activities as well as collaborates with the Ministry of Education Malaysia and Malaysian Examinations Council for numerous programs.