Revisiting Wiener's Attack – New Weak Keys in RSA

Subhamoy Maitra and Santanu Sarkar

Indian Statistical Institute, 203 B T Road, Kolkata 700 108
{subho, santanu_r}@isical.ac.in

Abstract. In this paper we revisit Wiener's method (IEEE-IT, 1990) of continued fraction (CF) to find new weaknesses in RSA. We consider RSA with $n = pq$, $q < p < 2q$, public encryption exponent e and private decryption exponent d. Our motivation is to find out when RSA is insecure given d is $O(n^{\delta})$, where we are mostly interested in the range $0.3 \leq \delta \leq 0.5$. We use both the upper and lower bounds on $\phi(n)$ and then try to find out what are the cases when $\frac{t}{d}$ is a convergent in the CF expression of $\frac{e}{n - \frac{3}{\sqrt{2}}\sqrt{n}+1}$. First we show that the RSA keys are weak when $d = n^{\delta}$ and $\delta < \frac{3}{4} - \gamma - \tau$, where $2q - p = n^{\gamma}$ and τ is a small value based on certain parameters. This presents additional results over the work of de Weger (AAECC 2002). Further we show that, the RSA keys are weak when $d < \frac{1}{2}n^{\delta}$ and e is $O(n^{\frac{3}{2}-2\delta})$ for $\delta \leq \frac{1}{2}$. Using similar idea we also present new results over the work of Blomer and May (PKC 2004).

Keywords: Cryptanalysis, RSA, Factorization, Weak Keys.

1 Introduction

RSA [14] is one of the most popular cryptosystems in the history of cryptology. Here, we use the standard notations in RSA as follows:

- primes p, q, with $q < p < 2q$;
- $n = pq$, $\phi(n) = (p-1)(q-1)$;
- $p - q = n^{\beta}$ where $n^{\frac{1}{4}} < n^{\beta} < \frac{n^{\frac{1}{2}}}{\sqrt{2}}$;
- e, d are such that $ed = 1 + t\phi(n)$, $t \geq 1$;
- n, e are available in public and the message M is encrypted as $C = M^e \bmod n$;
- the secret key d is required to decrypt the message as $M = C^d \bmod n$.

In this paper we exploit the Wiener's method [20] of continued fraction (CF) to find new weaknesses in RSA (see [15] for Legendre's theorem related to CF expression). Wiener [20] showed that if $d < \frac{1}{3}n^{0.25}$, then $|\frac{e}{n} - \frac{t}{d}| < \frac{1}{2d^2}$ and $\frac{t}{d}$ (which in turn reveals p, q) could be estimated in $poly(\log n)$ time from the CF expression of the publicly available quantity $\frac{e}{n}$.

From $ed = 1 + t\phi(n)$, it is easy to see that $\frac{e}{\phi(n)} - \frac{t}{d} = \frac{1}{d\phi(n)}$, i.e., $\frac{e}{\phi(n)} - \frac{t}{d} < \frac{1}{2d^2}$ whenever $2d < \phi(n)$. Thus a good estimation of $\phi(n)$ can be of use while exploiting CF expression. It is known that for $q < p < 2q$, $n - \frac{3}{\sqrt{2}}\sqrt{n} + 1 < \phi(n) < n - 2\sqrt{n} + 1$. In [22, Section 4], Wiener's attack [20] has been extended estimating $\phi(n)$ as $n - 2\sqrt{n} + 1$. In our approach, both side of the bound of $\phi(n)$ is exploited to get the results.

Lots of weaknesses of RSA have been identified in past three decades, but still RSA can be securely used with proper precautions as a public key cryptosystem. The security of RSA depends on the hardness of factorization. Let us now briefly discuss some weaknesses of RSA. RSA is found to be weak when the prime factors of either $p-1$ or $q-1$ are small [13]. Similarly, RSA is weak too when the prime factors of either $p+1$ or $q+1$ are small [21]. In [10], it has been pointed out that short public exponents may cause weakness if same message is broadcast to many parties. An outstanding survey on the attacks on RSA is available in [4]. For very recent results on RSA one may refer to [7, 12, 9] and the references therein.

In this paper we study the weaknesses of RSA when the secret decryption exponent d is upper bounded. The pioneering work in this area [20] uses Continued Fraction (CF) expression for the attack. In the seminal work in [6], important results have been shown regarding small solutions to polynomial equations that in turn show vulnerabilities of low exponent RSA. In [5], the method of [6] has been exploited to show that RSA is insecure if $d < n^{0.292}$. The results from [6] have been used along with the results of [20] in many papers [5, 22, 2, 11] to get the weaknesses when d is less than n^{δ}.

In this paper, we like to find out how the idea of CF expression from [20] can be exploited to find weaknesses of RSA when d is small. Note that here we do not use the ideas of [6] directly and the development in that area [7, 12, 9] at all. In [22, Section 4], some extension of the work [20] has been mentioned and it has also been noted that similar extension will work on the results of [19]. The result of [19] works for d with a few more bits longer than $n^{\frac{1}{4}}$. In [8], an extension of Legendre's result has been studied to get more weak keys in the direction of [19]. However, we find that new weak keys of RSA can be identified using the CF technique. These weak keys have not been explored in the literature before to the best of our knowledge.

In [20], it has been shown that RSA is not secure when $d < \frac{1}{3}n^{0.25}$ as under this condition, $|\frac{e}{n} - \frac{t}{d}| < \frac{1}{2d^2}$ and $\frac{t}{d}$ can be found in the CF expression of $\frac{e}{n}$. The knowledge of d helps in getting p, q immediately. In [18], a negative result has been identified that Wiener's attack will work with negligible success for $d > n^{\frac{1}{4}}$. Thus there is a deep interest to find out cases where the Wiener's strategy [20] can be extended to get more weak keys.

One may easily check that $\frac{e}{\phi(n)} > \frac{t}{d}$ and $\frac{e}{n} < \frac{t}{d}$. In [20], $\phi(n)$ has been approximated by n to get the results. A better result has been obtained in [22, Section 4] where $\phi(n)$ is approximated by $n - 2\sqrt{n} + 1$. It has been shown that $|\frac{e}{n-2\sqrt{n}+1} - \frac{t}{d}| < \frac{1}{2d^2}$ when $\delta < \frac{3}{4} - \beta$, where $p - q = n^{\beta}$ and $d = n^{\delta}$. Note that, for $\beta = \frac{1}{2}$, the result of [22] gives similar bound on d as in [20], which is of the order $n^{\frac{1}{4}}$. The improvement is obtained when β decreases. Only at $\beta = \frac{1}{4}$, d becomes of the order of $n^{\frac{1}{2}}$. In [22, Section 5, 6], the attack of [5] has been extended considering the value of β, where $p - q = n^{\beta}$. Instead of considering $p - q = n^{\beta}$, we here consider $2q - p = n^{\gamma}$ to get additional results. These results are presented in Section 2.

Further, instead of relating n^{β}, $\frac{1}{4} \leq \beta \leq \frac{1}{2}$, with $d = n^{\delta}$, we put the constraint on e. We find that RSA is insecure when d is of the order of n^{δ} for $\delta \leq 0.5$. The constraint in our case is on the public exponent e, which is related to the difference of the primes. We show that our attack works when $e \leq \frac{2n^{1-2\delta} - \frac{n}{n-A+1}}{\frac{n}{n-B} - \frac{n}{n-A+1}}$, which can be estimated as $O(n^{1.5-2\delta})$ in general. Here $A = \sqrt{n^{2\beta} + 4n}$ and $B = \frac{3}{\sqrt{2}}\sqrt{n}$. The conservative upper bound on e, i.e., $O(n^{1.5-2\delta})$, ignores the term $n^{2\beta}$ in A and thus the difference between the two primes does not come into the picture for the attack in general. These results are presented in Section 2.

In [2], it has been shown that p, q can be found in polynomial time for every n, e satisfying $ex+y = 0 \bmod \phi(n)$, with $x \leq \frac{1}{3}n^{\frac{1}{4}}$ and $|y| = O(n^{-\frac{3}{4}}ex)$; further some extensions considering the difference $p-q$ have also been considered. The work of [2] also uses the result of [6] as well as the idea of CF expression [20] in their proof. We also provide additional result over [2] using the lower bound of $\phi(n)$. This is presented in Section 3.

We here highlight the contribution of this paper with enumeration of the cases where we find new weak keys of RSA considering the CF expression of $\frac{e}{n-\frac{3}{\sqrt{2}}\sqrt{n}+1}$.

1. $d = n^{\delta}$ and $\delta < \frac{3}{4} - \gamma - \tau$, where $2q - p = n^{\gamma}$ and τ is a small value based on certain parameters.
2. $d < \frac{1}{2}n^{\delta}$ and e is $O(n^{\frac{3}{2}-2\delta})$ for $\delta \leq \frac{1}{2}$.
3. $ex + y = m\phi(n)$ for $m > 0$, $x \leq \frac{7}{4}n^{\frac{1}{4}}$, $|y| \leq cn^{-\frac{3}{4}}ex$, $c \leq 1$ and $p - q \geq cn^{\frac{1}{2}}$.
4. $ex + y = m\phi(n)$, for $m > 0$, $0 < x \leq \sqrt{\frac{3}{4l}}\sqrt{\frac{\phi(n)}{e}\frac{n^{\frac{3}{4}}}{2q-p}}$ for some positive integer l based on certain parameters and $|y| \leq \frac{2q-p}{\phi(n)n^{\frac{1}{4}}}ex$.

Before proceeding further, let us explain the Continued Fraction (CF) expression. We follow the material from [17, Chapter 5] for this. Given a positive rational number $\frac{a}{b}$, a finite CF expression of $\frac{a}{b}$ can be written as $q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \ldots + \frac{1}{q_m}}}$ or in short $[q_1, q_2, q_3, \ldots q_m]$. As an example, take the rational number $\frac{34}{99}$. One can write this as follows in the CF expression: $\frac{34}{99} = 0 + \frac{1}{\frac{99}{34}} = 0 + \frac{1}{2+\frac{31}{34}} = 0 + \frac{1}{2+\frac{1}{\frac{34}{31}}} = 0 + \frac{1}{2+\frac{1}{1+\frac{3}{31}}} = 0 + \frac{1}{2+\frac{1}{1+\frac{1}{\frac{31}{3}}}} = 0 + \frac{1}{2+\frac{1}{1+\frac{1}{10+\frac{1}{3}}}}$, and in short $[0, 2, 1, 10, 3]$. Consider a subsequence of $[0, 2, 1, 10, 3]$ as $[0, 2, 1]$. Note that $0 + \frac{1}{2+\frac{1}{1}} = \frac{1}{3} = \frac{33}{99}$, which is very close to $\frac{34}{99}$, i.e., a subsequence of CF will give an approximation of the rational number. Given that a, b are t bit integers, the CF expression $[q_1, q_2, q_3, \ldots, q_m]$ of $\frac{a}{b}$ can be found in $O(poly(t))$ time and can be stored in $O(poly(t))$ space. Any initial subsequence of $[q_1, q_2, q_3, \ldots, q_m]$, i.e, $[q_1, q_2, q_3, \ldots, q_r]$, where $1 \leq r \leq m$ is called the convergent of $[q_1, q_2, q_3, \ldots, q_m]$. As example, $[0, 2, 1]$ is a convergent of $[0, 2, 1, 10, 3]$, i.e., $\frac{1}{3} = \frac{33}{99}$ is a convergent of $\frac{34}{99}$. Also note that if the subsequence has a 1 at the end then that may also written by adding the 1 to the previous integer and removing the 1. That is, both $[0, 2, 1]$ and $[0, 3]$ provides the same rational number.

2 New Weak Keys I

It is known that if $p - q < n^{\frac{1}{4}}$ [16] (see also [22, Section 3]), then RSA is weak by Fermat's factorization technique. Thus we are interested in the range $n^{\frac{1}{4}} < p - q < \frac{\sqrt{n}}{\sqrt{2}}$ only.

Proposition 1. *Let p, q be of same bit size, i.e., $q < p < 2q$. Then $\phi(n) > n - B + 1$, where $B = \frac{3}{\sqrt{2}}\sqrt{n}$. Further, if $p - q = n^{\beta}$ where $n^{\frac{1}{4}} < n^{\beta} < \frac{n^{\frac{1}{2}}}{\sqrt{2}}$, then $\phi(n) = n - A + 1$, where $A = \sqrt{n^{2\beta} + 4n}$.*

Proof. Since $(p-2q)(2p-q) < 0$, we have $n - \frac{3}{\sqrt{2}}\sqrt{n} + 1 < \phi(n)$. Also, as $p - q = n^\beta$, we have $p^2 - n^\beta p - n = 0$, putting $q = \frac{n}{p}$. Thus $p = \frac{n^\beta + \sqrt{n^{2\beta}+4n}}{2}$. So we get $p + q = p + \frac{n}{p} = \frac{n^\beta+\sqrt{n^{2\beta}+4n}}{2} + \frac{2n}{n^\beta+\sqrt{n^{2\beta}+4n}} = \sqrt{n^{2\beta}+4n}$. Then $\phi(n) = n - (p+q) + 1 = n - A + 1$. □

In [22], it has been identified that if $p - q = n^\beta$, then RSA is weak for $d = n^\delta$ when $\delta < \frac{3}{4} - \beta$. In such a case $\frac{t}{d}$ could be found as a convergent in the CF expression of $\frac{e}{n-2\sqrt{n}+1}$. Thus the result works better when p, q are close. As example, if $p - q = n^{\frac{1}{4}+\epsilon}$, then δ is bounded by $\frac{1}{2} - \epsilon$. As example, for $\epsilon = 0.05$, RSA becomes insecure if $d = n^{0.44} < n^{0.45}$. However, this improvement is not significant when $p - q$ is $O(n^{0.5})$. We present the following approach when $p - q$ is large, which gives $2q - p$ is small.

Proposition 2. *Let l be a positive integer. For $q > \frac{2l+2}{4l+1}p$, $|\frac{3}{\sqrt{2}}\sqrt{n} - (p+q)| < \frac{l(2q-p)^2}{(\frac{3}{\sqrt{2}}+2)\sqrt{n}}$.*

Proof. We have $\frac{1}{l}(\frac{3}{\sqrt{2}}\sqrt{n}-(p+q))(\frac{3}{\sqrt{2}}\sqrt{n}+(p+q)) < (2q-p)^2$ iff $((4l+1)q-(2l+2)p)(2q-p) > 0$. As $(2q-p) > 0$, we need $(4l+1)q - (2l+2)p > 0$. Thus, $q > \frac{2l+2}{4l+1}p$.

Hence, $|\frac{3}{\sqrt{2}}\sqrt{n} - (p+q)| < \frac{l(2q-p)^2}{\frac{3}{\sqrt{2}}\sqrt{n}+(p+q)}$.

As $2\sqrt{n} < p + q < \frac{3}{\sqrt{2}}\sqrt{n}$, we have, $|\frac{3}{\sqrt{2}}\sqrt{n} - (p+q)| < \frac{l(2q-p)^2}{\frac{3}{\sqrt{2}}\sqrt{n}+2\sqrt{n}}$, which gives

$|\frac{3}{\sqrt{2}}\sqrt{n} - (p+q)| < \frac{l(2q-p)^2}{(\frac{3}{\sqrt{2}}+2)\sqrt{n}}$. □

As example, for $l = 15$, we get $q > \frac{32}{61}p$. If l becomes larger then the constraint on q will almost reach the constraint that $q > \frac{1}{2}p$.

Theorem 1. *Let l be a positive integer, $q > \frac{2l+2}{4l+1}p$, $2q - p = n^\gamma$ and $d = n^\delta$. Then n can be factored in $O(poly(\log(n)))$ time when $\delta < \frac{3}{4} - \gamma - \tau$, where $2\tau > (\log \frac{4l}{\frac{3}{\sqrt{2}}+2})\frac{1}{\log n}$.*

Proof. Let $2q - p = n^\gamma$. Then

$|\frac{3}{\sqrt{2}}\sqrt{n} - (p+q)| < \frac{ln^{2\gamma}}{(\frac{3}{\sqrt{2}}+2)\sqrt{n}}$.

i.e., $|\phi(n) - n - 1 + \frac{3}{\sqrt{2}}\sqrt{n}| < \frac{ln^{2\gamma}}{(\frac{3}{\sqrt{2}}+2)\sqrt{n}}$.

Now, $|\frac{e}{n-\frac{3}{\sqrt{2}}\sqrt{n}+1} - \frac{t}{d}|$

$\leq |\frac{e}{n-\frac{3}{\sqrt{2}}\sqrt{n}+1} - \frac{e}{\phi(n)}| + |\frac{e}{\phi(n)} - \frac{t}{d}|$

$= \frac{e|\phi(n)-(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)|}{\phi(n)(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)} + \frac{1}{d\phi(n)}$

$< \frac{e\frac{ln^{2\gamma}}{(\frac{3}{\sqrt{2}}+2)\sqrt{n}}}{\phi(n)(n-\frac{3}{\sqrt{2}}+1)} + \frac{1}{d\phi(n)}$

$< \frac{ln^{2\gamma}}{(\frac{3}{\sqrt{2}}+2)\sqrt{n}(n-\frac{3}{\sqrt{2}}+1)} + \frac{1}{d\phi(n)}$.

Assume, $n - \frac{3}{\sqrt{2}}\sqrt{n} + 1 > \frac{3}{4}n$ and $n > 8d$. Putting $d = n^\delta$, we get

$|\frac{e}{n-\frac{3}{\sqrt{2}}\sqrt{n}+1} - \frac{t}{d}|$

$< \frac{ln^{2\gamma}}{(\frac{3}{\sqrt{2}}+2)\sqrt{n}\frac{3}{4}n} + \frac{4}{3nd}$

$= \frac{\frac{4l}{3}n^{2\gamma-\frac{3}{2}}}{(\frac{3}{\sqrt{2}}+2)} + \frac{4}{3nd}$

$< \frac{\frac{4l}{3}n^{2\gamma-\frac{3}{2}}}{(\frac{3}{\sqrt{2}}+2)} + \frac{1}{6n^{2\delta}}$.

Now, $\frac{\frac{4l}{3}n^{2\gamma-\frac{3}{2}}}{(2+\frac{3}{\sqrt{2}})} < \frac{1}{3}n^{2\gamma-\frac{3}{2}+2\tau}$, for $2\tau > (\log \frac{4l}{\frac{3}{\sqrt{2}}+2})\frac{1}{\log n}$

So we get, $|\frac{e}{n-\frac{3}{\sqrt{2}}\sqrt{n}+1} - \frac{t}{d}| < \frac{1}{3}n^{2\gamma-\frac{3}{2}+2\tau} + \frac{1}{6n^{2\delta}}$.

Thus, $|\frac{e}{n-\frac{3}{\sqrt{2}}\sqrt{n}+1} - \frac{t}{d}| < \frac{1}{2d^2}$, when $2\gamma - \frac{3}{2} + 2\tau < -2\delta$, i.e., $\delta < \frac{3}{4} - \gamma - \tau$.

In such a case, $\frac{t}{d}$ is a convergent of the CF expression of $\frac{e}{n-\frac{3}{\sqrt{2}+1}\sqrt{n}}$, and we can find it in $O(poly(\log(n)))$ time. □

In the above case, we consider the bound on $2q-p$ to extend the limit of d beyond $n^{0.3}$. The result of [22, Section 4] concentrated on the case when $p-q$ is bounded. On the other hand, our result does not consider the bound on $p-q$ and it works when $2q-p$ is bounded.

For practical implication, we work with primes $p, q \geq 10^{160}$, i.e., $n \geq 10^{320}$. It is clear that our attack will work better compared to existing works when p, q are away (i.e., p is close to $2q$) with the bound $q < p < 2q$. However, the experiments when $2q - p < n^{\frac{1}{4}}$ may not be of interest as in that case the factorization can be done in polynomial time similar to the argument of Fermat's factorization strategy [16] (see also [22, Section 3]). Thus we consider the scenario when $2q - p > n^{\frac{1}{3}}$. Below we present a practical example. All the examples in this paper involving large integers are implemented in LINUX environment using C with GMP.

Example 1. We choose a random prime $q \in [10^{160}, 10^{161}]$. Then we choose a random prime p, such that $2q - p > n^{\frac{1}{3}}$. In this example, $n^{0.346} < 2q - p < n^{0.347}$. We then choose the first d greater than or equal to n^{δ} for $\delta \geq \frac{1}{3}$ such that d is coprime to $\phi(n)$. In such a case if e is in our prescribed limit then our attack succeeds.

We consider p, q respectively as

21324001236937503289167797884050805700247663179258767913123369490683298611013542
48271029398407942926950539396689547371580433185765533427201332696630101451231266 3

and

10662000618468751644583898942025402850123831589629883956561684745341649305506771
24135514699203971463475269698344773685790216592882766713600666348315050725615618 3,

which gives n as

22735651437645608514540764369949778526757596419266441470601561865911392077051606
87637281365780266996051653514381053312820085562581879941697100892461092791463814
72361264666736466411449942059568093916061632275622633234439324940363916123064654
02555303399548519028121978759763373757433442757741456334433042737747175925664532 9.

Note that $2q - p > n^{\frac{1}{3}}$.

One can check that $\phi(n)$ is

22735651437645608514540764369949778526757596419266441470601561865911392077051606
87637281365780266996051653514381053312820085562581879941697100892461092791463814
40375262811330211477698245233491885365690137506733981364754270704338968206544340
301487593019366046376961696647290527000627929790931561936310436928020237488176484.

In Theorem 1, we require $q > \frac{2l+2}{4l+1}p$. Here this is satisfied for $l = 10^{50}$. Also we have $2\tau > (\log \frac{4l}{\frac{3}{\sqrt{2}}+2})\frac{1}{\log n}$, and it is enough to take $\tau = \frac{5}{64} = 0.078125$ in this case. Taking $\gamma = 0.347$ and $\tau = 0.078125$, we get $\delta < \frac{3}{4} - \gamma - \tau = 0.324875$. Thus, in this case for any $d < n^{0.324875}$, RSA will be insecure.

Now take $n^{0.32} < d < n^{0.324875}$. We consider $d =$
44138452180807132553854898960195837050529634687636859759755568727353610483058810
149497334438480706535427 (a 104 digit number).

The corresponding e is
85356738187677927267094758044990579754357485762742350715347494115752841684037367
61958050516985955514963349897936619515552408960795697318670660889152163280842447
75560973766638533120643123534024611720642739938697649334533161511773864127534483
56073872108358709307048969215446586611896268736369229047317637983628682308907311.

The value of t is
16570953848141161450099797936855484729106684488828631895806571167212612482288825
100679308747791603915419.

Here $\frac{t}{d}$ could be found in the CF expression (see Appendix A) of $\frac{e}{n-\lceil\frac{3}{\sqrt{2}}\sqrt{n}\rceil+1}$. The | mark in the CF expression of $\frac{e}{n-\lceil\frac{3}{\sqrt{2}}\sqrt{n}\rceil+1}$ points the termination of the subsequence for the CF expression of $\frac{t}{d}$).

In fact, Theorem 1 presents a sufficient condition on d when RSA will be weak. In Example 2, it is shown that even for some d, greater than the bound in Theorem 1, RSA can be insecure based on some condition on e. Example 2 shows that there exists some d even greater than $n^{\frac{1}{3}}$ when RSA is insecure. That is presented in Section 2.2, where we try to remove the constraint on the difference between the primes; instead an upper bound on e is considered.

2.1 Extension using the idea of Boneh-Durfee [5]

In this section, we follow the idea of [5, Section 4]. Similar idea of [1] can also be applied. This idea has been used in [22, Section 5] when $p - q$ is bounded. We use similar idea when $2q - p$ is bounded.

Let $d = n^{\delta}$. Using the idea of [5], we show that, RSA is insecure if $\delta < \frac{4\gamma+5}{6} - \frac{\sqrt{(4\gamma+5)(4\gamma-1)}}{3}$. We assume $e = n$ as for $e < n$ one can get better upper bound on δ [5, Page 9].

We have $ed = 1 + t\phi(n) = 1 + t(n+1-p-q) = 1 + t(n+1-\frac{3}{\sqrt{2}}\sqrt{n} - (p+q-\frac{3}{\sqrt{2}}\sqrt{n})) = 1 + x(A+y)$, where $x = t < d = n^{\delta}$, $A = n+1-\frac{3}{\sqrt{2}}\sqrt{n}$ $y = -(p+q-\frac{3}{\sqrt{2}}\sqrt{n})$. Now, $|y| < \frac{(2q-p)^2 l}{(\frac{3}{\sqrt{2}}+2)\sqrt{n}}$. Considering $\frac{l}{(\frac{3}{\sqrt{2}}+2)} < 1$ (i.e., $l \leq 4$) and using $e = n$, we have, $x < e^{\delta}$, $|y| < e^{2\gamma-\frac{1}{2}}$.

We have to find x_0, y_0 such that $1+x_0(A+y_0) \equiv 0 \bmod e$, where $|x_0| < e^{\delta}$ and $|y_0| < e^{2\gamma-\frac{1}{2}}$. Let $X = e^{\delta}, Y = e^{2\gamma-\frac{1}{2}}$. Note that we consider the same X as in [5, Section 4], but our Y is generalized as Y has been taken as $e^{\frac{1}{2}}$ in [5, Section 4].

One may refer to [5, Section 4] for $det_x = e^{m(m+1)(m+2)/3}X^{m(m+1)(m+2)/3}Y^{m(m+1)(m+2)/6}$ and $det_y = e^{tm(m+1)/2}X^{tm(m+1)/2}Y^{t(m+1)(m+t+1)/2}$. Plugging in the values of X and Y (note that our Y is different than [5, Section 4]), we obtain, $det_x = e^{m^3(\frac{1}{4}+\frac{\delta+\gamma}{3})+o(m^3)}$, $det_y = e^{tm^2(\frac{1}{4}+\frac{\delta}{2}+\gamma)} + t^2m(\gamma-\frac{1}{4}) + o(tm^2)$. Now $det(L) = det_x det_y$ and we need to satisfy $det(L) < e^{mw}$. Note that $w = (m+1)(m+2)/2 + t(m+1)$, the dimension of L. To satisfy $det(L) < e^{mw}$, we need $m^3(\frac{1}{4}+\frac{\delta+\gamma}{3}) + tm^2(\frac{1}{4}+\frac{\delta}{2}+\gamma) + t^2m(\gamma-\frac{1}{4}) < (tm+\frac{m^2}{2})m$. This leads to $m^2(-\frac{1}{4}+\frac{\delta}{3}+\frac{\gamma}{3}) + tm(-\frac{3}{4}+\frac{\delta}{2}+\gamma) + t^2(\gamma-\frac{1}{4}) < 0$. After fixing an m, the left hand side is minimized at $t = \frac{\frac{3}{4}-\frac{\delta}{2}-\gamma}{2\gamma-\frac{1}{2}}$. Substituting this, $16\gamma^2 + 8\gamma - 15 + (16\gamma+20)\delta - 12\delta^2 < 0$. Hence, $\delta < \frac{4\gamma+5}{6} - \frac{\sqrt{(4\gamma+5)(4\gamma-1)}}{3}$.

Similar to the idea in [5, Section 4], if the smallest two elements of the reduced basis out of the LLL algorithm are algebraically independent, then we will get x_0, y_0 correctly which will in turn provide the factorization of n.

One may note that the upper bound of δ here as $\delta < \frac{4\gamma+5}{6} - \frac{\sqrt{(4\gamma+5)(4\gamma-1)}}{3}$ is greater than the upper bound $\delta < \frac{3}{4} - \gamma - \tau$ in Theorem 1 given $0 \le \gamma \le \frac{1}{2}$.

2.2 RSA is weak when ed^2 is $O(n^{\frac{3}{2}})$ and d is $O(n^{\frac{1}{2}})$

Lemma 1. *Let $2d < n^{\delta}$, where $0 < \delta \le \frac{1}{2}$. Let A, B be as in Proposition 1. Then for $e \le \frac{2n^{1-2\delta} - \frac{n}{n-A+1}}{\frac{n}{n-B} - \frac{n}{n-A+1}}$, it is possible to get $\frac{z_1}{z_2}$ such that*

1. $\frac{e}{n}\frac{z_1}{z_2} - \frac{t}{d} < \frac{1}{2d^2}$ when $\frac{n}{n-B+1} \le \frac{z_1}{z_2} < \frac{2}{e}n^{1-2\delta} + \frac{n}{e}\frac{e-1}{n-A+1}$ and
2. $\frac{t}{d} - \frac{e}{n}\frac{z_1}{z_2} < \frac{1}{2d^2}$ when $\frac{n}{n-B+1} - \frac{2}{e}n^{1-2\delta} < \frac{z_1}{z_2} \le \frac{n}{e}\frac{e-1}{n-A+1}$.

Proof. As we have $\frac{e}{n} < \frac{t}{d}$, there are two cases with the condition $\frac{z_1}{z_2} > 1$.

1. $\frac{t}{d} - \frac{e}{n} \ge \frac{1}{2d^2}$ but $0 \le \frac{e}{n}\frac{z_1}{z_2} - \frac{t}{d} < \frac{1}{2d^2}$.
2. $\frac{t}{d} - \frac{e}{n} \ge \frac{1}{2d^2}$ but $0 \le \frac{t}{d} - \frac{e}{n}\frac{z_1}{z_2} < \frac{1}{2d^2}$.

Case 1. The condition here is: $\frac{t}{d} - \frac{e}{n} \ge \frac{1}{2d^2}$ but $0 \le \frac{e}{n}\frac{z_1}{z_2} - \frac{t}{d} < \frac{1}{2d^2}$.

Thus, we have to satisfy $0 \le \frac{edz_1 - tnz_2}{ndz_2} < \frac{1}{2d^2}$, i.e., $0 \le \frac{z_1 + z_1t\phi(n) - tnz_2}{nz_2} < \frac{1}{2d}$.

Let $2d < n^{\delta}$, for $\delta > 0$. Then $0 \le \frac{z_1+z_1t\phi(n)-tnz_2}{nz_2} < \frac{1}{n^{\delta}}$ implies $0 \le \frac{z_1+z_1t\phi(n)-tnz_2}{nz_2} < \frac{1}{2d}$.

So we need to estimate $\frac{z_1}{z_2}$ considering $0 \le \frac{z_1+z_1t\phi(n)-tnz_2}{nz_2} < \frac{1}{n^{\delta}}$.

Now $0 \le \frac{z_1+z_1t\phi(n)-tnz_2}{nz_2} < \frac{1}{n^{\delta}}$ iff
$0 \le \frac{z_1}{z_2}(1+t\phi(n)) - tn < n^{1-\delta}$ iff
$tn \le \frac{z_1}{z_2}(1+t\phi(n)) < n^{1-\delta} + tn$ iff
$\frac{tn}{1+t\phi(n)} \le \frac{z_1}{z_2} < \frac{n^{1-\delta}+tn}{1+t\phi(n)}$ if
$\frac{n}{\phi(n)} \le \frac{z_1}{z_2} < \frac{n^{1-\delta}+tn}{ed}$ if

$\frac{n}{n-B+1} \leq \frac{z_1}{z_2} < \frac{2}{e}n^{1-2\delta} + \frac{n}{e}\frac{e-1}{n-A+1}$, following
(i) Proposition 1,
(ii) $\frac{1}{d} > \frac{2}{n^\delta} \Rightarrow \frac{n^{1-\delta}}{ed} > \frac{2}{e}n^{1-2\delta}$, and
(iii) $ed = 1 + t\phi(n) \Rightarrow \frac{t}{d} = \frac{e-\frac{1}{d}}{\phi(n)} \Rightarrow \frac{t}{d} > \frac{e-1}{n-A+1}$.
To have an $\frac{z_1}{z_2}$, we need $\frac{n}{n-B+1} < \frac{2}{e}n^{1-2\delta} + \frac{n}{e}\frac{e-1}{n-A+1}$.

For the guarantee of getting a rational $\frac{z_1}{z_2}$ in the interval $[\frac{n}{n-B+1}, \frac{2}{e}n^{1-2\delta} + \frac{n}{e}\frac{e-1}{n-A+1})$, one may choose $\frac{n}{n-\lceil B\rceil+1}$. Clearly, $\frac{n}{n-B+1} < \frac{n}{n-\lceil B\rceil+1} < \frac{n}{n-(B+1)+1} = \frac{n}{n-B}$. Thus,

$$\frac{n}{n-B} \leq \frac{2}{e}n^{1-2\delta} + \frac{n}{e}\frac{e-1}{n-A+1} \tag{1}$$

need to be satisfied. This gives, $e \leq \frac{2n^{1-2\delta} - \frac{n}{n-A+1}}{\frac{n}{n-B} - \frac{n}{n-A+1}}$.

Case 2. The condition here is: $\frac{t}{d} - \frac{e}{n} \geq \frac{1}{2d^2}$ but $0 \leq \frac{t}{d} - \frac{e}{n}\frac{z_1}{z_2} < \frac{1}{2d^2}$. With similar analysis, we get $\frac{n}{n-B+1} - \frac{2}{e}n^{1-2\delta} < \frac{z_1}{z_2} \leq \frac{n}{e}\frac{e-1}{n-A+1}$, which again gives the same upper bound for e. □

Theorem 2. *Consider the interval I such that $I = (\frac{n}{n-B+1} - \frac{2}{e}n^{1-2\delta}, \frac{2}{e}n^{1-2\delta} + \frac{n}{e}\frac{e-1}{n-A+1})$. Let $2d < n^\delta$, where $0 < \delta \leq \frac{1}{2}$. Then for $e \leq \frac{2n^{1-2\delta} - \frac{n}{n-A+1}}{\frac{n}{n-B} - \frac{n}{n-A+1}}$, and $\frac{z_1}{z_2} \in I$, $|\frac{e}{n}\frac{z_1}{z_2} - \frac{t}{d}| < \frac{1}{2d^2}$.*

Proof. From Lemma 1 we get that $|\frac{e}{n}\frac{z_1}{z_2} - \frac{t}{d}| < \frac{1}{2d^2}$ for the intervals $\frac{n}{n-B+1} \leq \frac{z_1}{z_2} < \frac{2}{e}n^{1-2\delta} + \frac{n}{e}\frac{e-1}{n-A+1}$ and $\frac{n}{n-B+1} - \frac{2}{e}n^{1-2\delta} < \frac{z_1}{z_2} \leq \frac{n}{e}\frac{e-1}{n-A+1}$.

Since, $\frac{n}{n-B+1} - \frac{2}{e}n^{1-2\delta} < \frac{n}{e}\frac{e-1}{n-A+1} < \frac{n}{n-B+1} \leq \frac{z_1}{z_2} < \frac{2}{e}n^{1-2\delta} + \frac{n}{e}\frac{e-1}{n-A+1}$, it is enough to have $\frac{z_1}{z_2}$ in the interval $I = (\frac{n}{n-B+1} - \frac{2}{e}n^{1-2\delta}, \frac{2}{e}n^{1-2\delta} + \frac{n}{e}\frac{e-1}{n-A+1})$ to get $|\frac{e}{n}\frac{z_1}{z_2} - \frac{t}{d}| < \frac{1}{2d^2}$ for $2n^{1-\delta} \leq e < \frac{2n^{1-2\delta} - \frac{n}{n-A+1}}{\frac{n}{n-B} - \frac{n}{n-A+1}}$. □

Corollary 1. *Let $2d < n^\delta$, where $0 < \delta \leq \frac{1}{2}$ and $e \leq \frac{2n^{1-2\delta} - \frac{n}{n-A+1}}{\frac{n}{n-B} - \frac{n}{n-A+1}}$. Then n can be factored in poly$(\log n)$ time.*

Proof. The proof follows from Lemma 1 as $\frac{n}{n-B+1} < \frac{e}{n-\lceil B\rceil+1} < \frac{2}{e}n^{1-2\delta} + \frac{n}{e}\frac{e-1}{n-A+1}$. Then $\frac{t}{d}$ will be found in the CF expression of $\frac{e}{n}\frac{z_1}{z_2}$ when $\frac{z_1}{z_2} = \frac{n}{n-\lceil B\rceil+1}$. Thus $\frac{t}{d}$ will be found in the CF expression of $\frac{e}{n-\lceil B\rceil+1}$. □

Below we present the summarized result which is a conservative one as the upper bound of e is underestimated. This result is general as it does not require the parameter β for the proof, where $p - q = n^\beta$.

Theorem 3. *Let $n = pq$, where p, q are primes such that $q < p < 2q$. Then n can be factored in poly$(\log n)$ time from the knowledge of n, e when $d < \frac{1}{2}n^\delta$ and e is $O(n^{\frac{3}{2}-2\delta})$ for $\delta \leq \frac{1}{2}$.*

Proof. We have, $e \leq \frac{2n^{1-2\delta} - \frac{n}{n-A+1}}{\frac{n}{n-B} - \frac{n}{n-A+1}} = \frac{\left(2n^{-2\delta}(n-A+1)-1\right)(n-B)}{B-A+1}$, and this increases as A increases. Also the lower bound of A is $2\sqrt{n}$, when $n^{2\beta}$ is neglected. Thus, $e \leq \frac{2n^{1-2\delta} - \frac{n}{n-2\sqrt{n}+1}}{\frac{n}{n-\frac{3}{\sqrt{2}}\sqrt{n}} - \frac{n}{n-2\sqrt{n}+1}}$ and this is $O(n^{\frac{3}{2}-2\delta})$. □

Theorem 3 shows that n can be factorized from the knowledge of e (d not known) when ed^2 is $O(n^{\frac{3}{2}})$ and d is $O(n^{\frac{1}{2}})$. We like to point out an important result [3, Theorem 2] that should be stated in this context, where it has been shown that for $ed \leq n^{\frac{3}{2}}$, with the knowledge of e, d, the integer n can be factorized in $O(\log^2 n)$ time.

The results given in Theorems 2, 3 do not put any constraint on the difference of the primes to get a better bound on d, but the constraint is imposed on e. When $d < \frac{1}{2}n^{\delta}$, then with increase in the value of δ, the value of e becomes upper bounded by $\frac{2n^{1-2\delta} - \frac{n}{n-A+1}}{\frac{n}{n-B} - \frac{n}{n-A+1}}$.

In [22, Section 4], CF expression of only a specific value $\frac{e}{n-2\sqrt{n}+1}$ has been exploited to get $\frac{t}{d}$. Thus compared to our case, $\frac{z_1}{z_2}$ is approximated by $\frac{n}{n-2\sqrt{n}+1}$ in [22, Section 4]. Considering Lemma 1, if $\frac{n}{n-2\sqrt{n}+1} < \frac{n}{n-B+1} - \frac{2}{e}n^{1-2\delta}$, then the approach of [22] may not be used to get the primes, but our method will work.

The exact algorithm for our proposed attack is as follows.

Input: n, e.

---

1. Compute the CF expression of $\frac{e}{n - \frac{3}{\sqrt{2}}\sqrt{n}+1}$.
2. For every convergent $\frac{t_1}{d_1}$ of the expression above
   - if the roots of $x^2 - (n + 1 - \frac{ed_1-1}{t_1})x + n = 0$ are positive integers less than n
     - then return the roots as p, q;
3. Return ("failure");

Our conservative estimate shows that the RSA keys are weak when $d < \frac{1}{2}n^{\delta}$ and e is $O(n^{\frac{3}{2}-2\delta})$. For example, considering $\delta = 0.3$, 0.4, 0.45, 0.5, e is bounded by $O(n^{0.9})$, $O(n^{0.7})$, $O(n^{0.6})$, $O(n^{0.5})$ respectively.

However, we like to point out that this is a conservative estimate and actually the upper bound of e is much better. We have $e \leq \frac{2n^{1-2\delta} - \frac{n}{n-A+1}}{\frac{n}{n-B} - \frac{n}{n-A+1}}$ and the attack works for $2d < n^{\delta}$. Thus the attack will work when $e \leq \frac{\frac{2n}{(2d+1)^2} - \frac{n}{n-A+1}}{\frac{n}{n-B} - \frac{n}{n-A+1}}$, taking $n^{\delta} = 2d + 1$.

Example 2. Refer to p, q of Example 1. We consider $d > n^{\frac{1}{3}}$, which is
61033620665104690038995387156383867652322226123296685389723133974030185448442674
868648018282242385291158493 (a 107 digit number).

The corresponding e is
25607033747060878831948100960748852360251160751444254452928522143254801167421362
25513157990007523683535328276512015218416342340790451266270568113742588904059135
27886609642186978739480642254815290198948110261414415071190855304065173317461587
21915217732030040350902165668813353187518059414604660250990538671831828340253.

Note that, we need to check $e \leq \frac{\frac{2n}{(2d+1)^2} - \frac{n}{n-A+1}}{\frac{n}{n-B} - \frac{n}{n-A+1}}$, taking $n^{\delta} = 2d + 1$ and the value of $\frac{\frac{2n}{(2d+1)^2} - \frac{n}{n-A+1}}{\frac{n}{n-B} - \frac{n}{n-A+1}}$ is
27752782508386083340303355961072715172277767233940251957583970436546175777700818
56675682093198406639915452074782714666722078006681946847644066862508400946540480

`9582701631055166869000334465011976615123464291750362836799303671111215560024917`1
`8582505438221327778861347609746919191798476162540713571031116759028157477865`3,

which is greater than e indeed.

The value of t is
`68741816717370170354202102752220123637844118401098843309845021703266783780777797`
`0108983292838561347464`2.

Here $\frac{t}{d}$ could be found in the CF expression (see Appendix A) of $\frac{e}{n-\lceil \frac{3}{\sqrt{2}}\sqrt{n}\rceil+1}$. The | mark in the CF expression of $\frac{e}{n-\lceil \frac{3}{\sqrt{2}}\sqrt{n}\rceil+1}$ points the termination of the subsequence for the CF expression of $\frac{t}{d}$).

One may check that $\frac{t}{d}$ will not be found in the continued fraction expression of $\frac{e}{n}$ (Weiner's result [20]) or $\frac{e}{n-2\sqrt{n}+1}$ (Weger's result [22, Section 4]) in Example 2.

In [22, Sections 5, 6], the approach of [5] has been used to slightly improve the bounds of [22, Sections 4]. The improvement in that case is not evident when $p-q$ approaches $\sqrt{n}$ and it does not cover our results. In Example 2, $n^{0.4995} < p-q < n^{0.4996}$. Thus, for $p-q = n^{\beta}$, $\beta > 0.4995$. For $\beta = 0.4995$, we get $\delta < 1 - \sqrt{2\beta - \frac{1}{2}} = 0.2936$. Thus the method of [22, Section 6] will work for $d < n^{0.2936}$. Our example considers $d > n^{\frac{1}{3}}$ and hence not contained in the weak keys presented in [22, Section 6].

Remark 1. We also present Example 3 in Appendix A to show the effects of the upper bound on d in Theorem 1 as well as the upper bounds on d, e in Theorem 2. Note that

"d of Example 1" < "d of Example 3" < "d of Example 2".

For the "d of Example 3", $\frac{t}{d}$ cannot be found in the CF expression of $\frac{e}{n-\lceil \frac{3}{\sqrt{2}}\sqrt{n}\rceil+1}$. The "$d$ of Example 3" does not satisfy the condition given in Theorem 1. On the other hand, though "d of Example 3" < "d of Example 2", the bound on e is not satisfied in Example 3.

One may note that in Example 3, the CF expression of $\frac{t}{d}$ does not match only in only three places at the end with the initial subsequence of the CF expression of $\frac{e}{n-\lceil \frac{3}{\sqrt{2}}\sqrt{n}\rceil+1}$. Thus, the idea of search in the line of [19] will actually provide the exact result with some extra effort.

3 New Weak Keys II

Let us restate the result of [2, Theorem 2], where it was proved that p, q can be found in polynomial time for every n, e satisfying $ex + y = 0 \bmod \phi(n)$, with $x \leq \frac{1}{3}n^{\frac{1}{4}}$ and $|y| = O(n^{-\frac{3}{4}}ex)$.

Consider that $ex + y \equiv 0 \bmod \phi(n)$ and the interest is on the nontrivial cases. Thus $ex+y = k(n-p-q+1)$. This gives $\frac{e}{n} - \frac{k}{x} = -\frac{k(p+q-1)+y}{nx}$. If $|\frac{e}{n} - \frac{k}{x}| = |\frac{k(p+q-1)+y}{nx}| < \frac{1}{2x^2}$, then the fraction $\frac{k}{x}$ appears among the convergents of $\frac{e}{n}$. Thus one needs to find out the conditions such that $|k(p+q-1)+y| < \frac{n}{2x}$ is satisfied. Calculation shows that for $|y| = O(n^{-\frac{3}{4}}ex)$, one gets $x \leq \frac{1}{3}n^{\frac{1}{4}}$.

Note that instead of trying to find $\frac{k}{x}$ among the convergents of $\frac{e}{n}$, a better attempt will be to find $\frac{k}{x}$ among the convergents of $\frac{e}{\phi'(n)}$, where $\phi'(n)$ is a better estimate than n for $\phi(n)$. Following the idea of [22], $\phi'(n)$ has been taken as $n - \lfloor 2\sqrt{n} \rfloor$ (i.e., the upper bound of $\phi(n)$) and the CF expression of $\frac{e}{n-\lfloor 2\sqrt{n}\rfloor}$ has been considered to estimate $\frac{k}{x}$ in [2, Section 4]. It has been proved in [2, Theorem 4, Section 4] that p, q can be found in polynomial time for every n, e satisfying $ex + y = 0 \bmod \phi(n)$, with $x \leq \frac{1}{3}\sqrt{\frac{\phi(n)}{e}\frac{n^{\frac{3}{4}}}{p-q}}$ and $|y| \leq \frac{p-q}{\phi(n)n^{\frac{1}{4}}}ex$.

As we have done in the previous section, instead of considering the CF expression of $\frac{e}{n-\lfloor 2\sqrt{n}\rfloor}$, we consider the CF expression of $\frac{e}{n-\lceil \frac{3}{\sqrt{2}}\sqrt{n}\rceil+1}$ to get additional results.

Lemma 2. *Let $ex + y = k\phi(n)$ for $k > 0$. Then $|\frac{e}{n-\frac{3}{\sqrt{2}}\sqrt{n}+1} - \frac{k}{x}| < \frac{1}{2x^2}$ for $x \leq \frac{7}{4}n^{\frac{1}{4}}$ when $|y| \leq cn^{-\frac{3}{4}}ex$, where $c \leq 1$ and $p - q \geq cn^{\frac{1}{2}}$.*

Proof. Let us list the following observations.

1. From Proposition 1, we have $n - \frac{3}{\sqrt{2}}\sqrt{n}+1 < \phi(n) < n - 2\sqrt{n}+1$, which gives, $(2-\frac{3}{\sqrt{2}})\sqrt{n} < p+q-\frac{3}{\sqrt{2}}\sqrt{n} < 0$. Thus, $|(2-\frac{3}{\sqrt{2}})\sqrt{n}| > |p+q-\frac{3}{\sqrt{2}}\sqrt{n}|$, i.e., $(\frac{3}{\sqrt{2}}-2)\sqrt{n} > |p+q-\frac{3}{\sqrt{2}}\sqrt{n}|$.
2. Also note that $|y| \leq cn^{-\frac{3}{4}}ex$, which gives $|y| < xn^{\frac{1}{4}}$ as $e < n$ and $c \leq 1$.
3. From [2, Proof of Theorem 2], $\frac{3}{4}\frac{ex}{\phi(n)} \leq k \leq \frac{5}{4}\frac{ex}{\phi(n)}$.

Now, $\frac{e}{n-\frac{3}{\sqrt{2}}\sqrt{n}+1} - \frac{k}{x} = \frac{k(-p-q+\frac{3}{\sqrt{2}}\sqrt{n})-y}{x(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)}$.

This gives, $|\frac{e}{n-\frac{3}{\sqrt{2}}\sqrt{n}+1} - \frac{k}{x}| < \frac{k((\frac{3}{\sqrt{2}}-2)\sqrt{n})+|y|}{x(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)}$ using item 1.

Now, $\frac{k((\frac{3}{\sqrt{2}}-2)\sqrt{n})+|y|}{x(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)} < \frac{1}{2x^2}$

if $\frac{\frac{5}{4}\frac{ex}{\phi(n)}((\frac{3}{\sqrt{2}}-2)\sqrt{n})+xn^{\frac{1}{4}}}{x(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)} < \frac{1}{2x^2}$ (using items 2, 3)

if $\frac{\frac{5}{4}x((\frac{3}{\sqrt{2}}-2)\sqrt{n})+xn^{\frac{1}{4}}}{x(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)} < \frac{1}{2x^2}$ (as $\frac{e}{\phi(n)} < 1$)

iff $\frac{\frac{5}{4}((\frac{3}{\sqrt{2}}-2)\sqrt{n})+n^{\frac{1}{4}}}{(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)} < \frac{1}{2x^2}$

if $\frac{\frac{5}{4}\times 0.13\sqrt{n}}{(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)} < \frac{1}{2x^2}$ (as $\frac{3}{\sqrt{2}} - 2 < 0.13$ and $\frac{5}{4}(\frac{3}{\sqrt{2}}-2)\sqrt{n}) + n^{\frac{1}{4}} < \frac{5}{4}\times 0.13\sqrt{n}$ for large n)

iff $\frac{5}{2}\times 0.13x^2 < \sqrt{n} + \frac{1}{\sqrt{n}} - \frac{3}{\sqrt{2}}$

if $x^2 < 3.076\sqrt{n}$, for large n

if $x \leq 1.75n^{\frac{1}{4}}$. ◻

This shows that the class of weak keys identified in [2, Theorem 2] can be extended by $\frac{21}{4}$, i.e., by more than 5 times.

In the improved result of [2, Theorem 4, Section 4], it has been shown that p, q can be found in polynomial time for every n, e satisfying $ex + y = 0 \bmod \phi(n)$, with $0 < x \leq$

$\frac{1}{3}\sqrt{\frac{\phi(n)}{e}}\frac{n^{\frac{3}{4}}}{p-q}$ and $|y| \leq \frac{p-q}{\phi(n)n^{\frac{1}{4}}}ex$. Our result in Lemma 2 provides new weak keys which are not covered by the result of [2, Theorem 4, Section 4] in certain cases as follows.

Let $p-q = c\sqrt{n}$. As, $q < p < 2q$, we have $p-q < \sqrt{\frac{n}{2}}$. Thus, $c < \frac{1}{\sqrt{2}}$. In [2, Theorem 4, Section 4], it is given that $x \leq \frac{1}{3}\sqrt{\frac{\phi(n)}{e}}\frac{n^{\frac{3}{4}}}{p-q}$. Putting $p-q = c\sqrt{n}$, we find $x \leq \frac{1}{3c}\sqrt{\frac{\phi(n)}{e}}n^{\frac{1}{4}}$. Thus our result in Lemma 2 provides extra weak keys than [2, Theorem 4, Section 4] when

$$\frac{1}{3c}\sqrt{\frac{\phi(n)}{e}}n^{\frac{1}{4}} < \frac{7}{4}n^{\frac{1}{4}},$$

which is true for $\frac{e}{\phi(n)} > \left(\frac{4}{21c}\right)^2$. As $e < \phi(n)$, $\frac{4}{21c} < 1$, which gives $c > \frac{4}{21}$. Thus the result our Lemma 2 presents new weak keys over In [2, Theorem 4, Section 4] when

$\frac{e}{\phi(n)} > \left(\frac{4}{21c}\right)^2$ for $\frac{4}{21} < c < \frac{1}{\sqrt{2}}$.

Next we use our idea of considering $2q-p$ (as presented in Proposition 2) instead of $p-q$.

Theorem 4. *Let l be a positive integer such that $l > \frac{2(\frac{3}{\sqrt{2}}+2)}{\frac{3}{\sqrt{2}}-2\epsilon}$, where $\epsilon > \frac{2q-p}{\phi(n)n^{\frac{1}{4}}}$. Let $q > \frac{2l+2}{4l+1}p$. Suppose e satisfies the equation $ex+y = k\phi(n)$, for $k > 0$. Then n can be factored in $O(poly(\log(n)))$ time when $0 < x \leq \sqrt{\frac{3}{4l}}\sqrt{\frac{\phi(n)}{e}}\frac{n^{\frac{3}{4}}}{2q-p}$ and $|y| \leq \frac{2q-p}{\phi(n)n^{\frac{1}{4}}}ex$.*

Proof. We have $k = \frac{ex+y}{\phi(n)}$. Using the bound on $|y|$, we get $k \leq \frac{ex}{\phi(n)}\left(1+\frac{2q-p}{\phi(n)n^{\frac{1}{4}}}\right)$.

Now, $|\frac{e}{n-\frac{3}{\sqrt{2}}\sqrt{n}+1} - \frac{k}{x}|$

$= \frac{|ex-k(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)|}{x(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)}$

$= \frac{|k(\frac{3}{\sqrt{2}}\sqrt{n}-p-q)-y|}{x(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)}$ (putting $ex = -y+k\phi(n)$)

$\leq \frac{|k(\frac{3}{\sqrt{2}}\sqrt{n}-p-q)|+|y|}{x(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)}$

$< \frac{(\frac{ex}{\phi(n)}\left(1+\frac{2q-p}{\phi(n)n^{\frac{1}{4}}}\right))(\frac{l(2q-p)^2}{(\frac{3}{\sqrt{2}}+2)\sqrt{n}})+\frac{2q-p}{\phi(n)n^{\frac{1}{4}}}ex}{x(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)}$ (putting the upper bound on k, using $|\frac{3}{\sqrt{2}}\sqrt{n}-(p+q)| < \frac{l(2q-p)^2}{(\frac{3}{\sqrt{2}}+2)\sqrt{n}}$ from Proposition 2 and the upper bound of y)

$= \frac{(\frac{e}{\phi(n)}\left(1+\frac{2q-p}{\phi(n)n^{\frac{1}{4}}}\right))(\frac{l(2q-p)^2}{(\frac{3}{\sqrt{2}}+2)\sqrt{n}})+\frac{2q-p}{\phi(n)n^{\frac{1}{4}}}e}{(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)}$

$= \frac{\frac{e}{\phi(n)}\left((1+\frac{2q-p}{\phi(n)n^{\frac{1}{4}}})(\frac{l(2q-p)^2}{(\frac{3}{\sqrt{2}}+2)\sqrt{n}})+\frac{2q-p}{n^{\frac{1}{4}}}\right)}{(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)}$

$\leq \frac{\frac{e}{\phi(n)}\left(\frac{l(2q-p)^2}{2\sqrt{n}}\right)}{(n-\frac{3}{\sqrt{2}}\sqrt{n}+1)}$, because of the following.

Let $X = \frac{2q-p}{n^{\frac{1}{4}}}$. Thus, $(1+\frac{2q-p}{\phi(n)n^{\frac{1}{4}}})(\frac{l(2q-p)^2}{(\frac{3}{\sqrt{2}}+2)\sqrt{n}})+\frac{2q-p}{n^{\frac{1}{4}}} = (1+\frac{X}{\phi(n)})(\frac{lX^2}{\frac{3}{\sqrt{2}}+2}+X) < (1+\epsilon)(\frac{lX^2}{\frac{3}{\sqrt{2}}+2}+X) < \frac{l}{2}X^2$ if $l > \frac{2(\frac{3}{\sqrt{2}}+2)}{\frac{3}{\sqrt{2}}-2\epsilon}$, when $\epsilon > \frac{X}{\phi(n)}$, a very small quantity of $O(n^{-\frac{3}{4}})$. This is because, the numerator $2q-p$ is $O(n^{\frac{1}{2}})$ and the denominator contains $n^{\frac{1}{4}}\phi(n)$, where $\phi(n)$ is $O(n)$.

Now assume $n - \frac{3}{\sqrt{2}}\sqrt{n} > \frac{3}{4}n$. So we have $|\frac{e}{n-\frac{3}{\sqrt{2}}\sqrt{n}+1} - \frac{k}{x}| < \frac{\frac{e}{\phi(n)}\left(\frac{l(2q-p)^2}{2\sqrt{n}}\right)}{\frac{3}{4}n}$.

Thus, $|\frac{e}{n-\frac{3}{\sqrt{2}}\sqrt{n}+1} - \frac{k}{x}| < \frac{1}{2x^2}$

if $\frac{\frac{e}{\phi(n)}\left(\frac{l(2q-p)^2}{2\sqrt{n}}\right)}{\frac{3}{4}n} \leq \frac{1}{2x^2}$

iff $0 < 2x^2 \leq \frac{\phi(n)}{e}\frac{\frac{3}{2}n^{\frac{3}{2}}}{l(2q-p)^2}$

iff $0 < x \leq \sqrt{\frac{3}{4l}}\sqrt{\frac{\phi(n)}{e}}\frac{n^{\frac{3}{4}}}{2q-p}$.

Given, $|\frac{e}{n-\frac{3}{\sqrt{2}}\sqrt{n}+1} - \frac{k}{x}| < \frac{1}{2x^2}$, n can be factorized using [2, Algorithm Generalized Wiener Attack II]. □

Note that [2, Algorithm Generalized Wiener Attack II] uses Coppersmith's [6] which is actually a probabilistic polynomial time algorithm, though in practice it works very well.

We have $l > \frac{2(\frac{3}{\sqrt{2}}+2)}{\frac{3}{\sqrt{2}}-2\epsilon}$. Now, $\frac{2(\frac{3}{\sqrt{2}}+2)}{\frac{3}{\sqrt{2}}} = 3.88561808316412673173$. Since 2ϵ is very small, one may assume $l = 4$ as a specific value. In such a case, $\sqrt{\frac{3}{4l}} > \frac{2}{5} > \frac{1}{3}$, when $q > \frac{10}{17}p$.

The result of [2, Theorem 4, Section 4] states that p, q can be found in polynomial time for every n, e satisfying $ex + y = 0 \bmod \phi(n)$, with $0 < x \leq \frac{1}{3}\sqrt{\frac{\phi(n)}{e}}\frac{n^{\frac{3}{4}}}{p-q}$ and $|y| \leq \frac{p-q}{\phi(n)n^{\frac{1}{4}}}ex$. In our result $p-q$ is replaced by $2q-p$. Thus the results of this section presents new weak keys other than those presented in [2]. The result of [2, Theorem 4, Section 4] works efficiently when $p-q$ is upper bounded and our work gives better results when $2q-p$ is upper bounded.

To estimate the number of weak keys in our approach, we use the following existing result.

Lemma 3. *[2, Lemma 6] Let $f(n,e), g(n,e)$ be functions such that $f^2(n,e)g(n,e) < \phi(n)$, $f(n,e) \geq 2$ and $g(n,e) \leq f(n,e)$. The number of public keys $e \in Z^*_\phi(n), e \geq \frac{\phi(n)}{4}$ that satisfy an equation $ex + y = 0 \bmod \phi(n)$ for $x \leq f(n,e)$ and $|y| \leq g(n,e)x$ is at least*

$$\frac{f^2(n,e)g(n,e)}{8\log\log^2(n^2)} - O(f^2(n,e)n^\epsilon),$$

where $\epsilon > 0$ is arbitrarily small for n suitably large.

Now we present our estimate using similar analysis as in [2, Theorem 7]. First let us present the definition of the class of weak keys as presented in [2, Definition 5].

Definition 1. *Let C be a class of RSA public keys (n,e). The size of the class C is defined by $size_C(n) = |\{e \in Z*_{\phi_n} |(n,e) \in C|$. C is called weak if*

1. $size_C(n) = \Omega(n^\gamma)$ *for some* $\gamma > 0$.
2. *There exists a probabilistic algorithm which on every input* $(n, e) \in C$ *outputs the factorization of* n *in* $O(poly(\log n))$ *time.*

Theorem 5. *Let* $2q - p = n^{\frac{1}{4}+\gamma}$ *with* $0 < \gamma \leq \frac{1}{4}$. *Further, let* C *be the weak class that is given by the public key tuples* (n, e) *defined in the Theorem 4 with the additional restrictions that* $e \in Z^*_\phi(n)$ *and* $e \geq \frac{\phi(n)}{4}$. *Then* $size_C(n) = \Omega(\frac{n^{1-\gamma}}{\log\log^2(n^2)})$.

Proof. Here $f(n, e) = \sqrt{\frac{3}{4l}}\sqrt{\frac{\phi(n)}{e}}\frac{n^{\frac{3}{4}}}{2q-p}$, and $g(n, e) = \frac{2q-p}{\phi(n)n^{\frac{1}{4}}}e$. Clearly $f(n, e) \geq 2$. Also, $f^2(n, e)g(n, e) = \frac{3}{4l}\frac{n^{\frac{5}{4}}}{2q-p} < \phi(n)$ since $2q - p > n^{\frac{1}{4}}$.

Again $g(n, e) \leq f(n, e)$ as $(2q - p)^2 \leq \sqrt{\frac{3}{4l}}\sqrt{\frac{\phi(n)}{e}}n\phi(n)$. Hence, we can apply Lemma 1. Since $g(n, e) = \Omega(n^\gamma)$, the term

$$\frac{f^2(n, e)g(n, e)}{8loglog^2(n^2)}$$

dominates the error term $O(f^2(n, e)n^\epsilon)$. Using $f^2(n, e)g(n, e) = \Omega(\frac{n^{\frac{5}{4}}}{2q-p})$ and $2q - p = n^{\frac{1}{4}+\gamma}$, we get the estimate. □

4 Conclusion

In this paper we study the well known method of Continued Fraction (CF) expression to demonstrate new weak keys of RSA. The idea is to factorize n using the knowledge of e and some estimate of $\phi(n)$. One may note that in most of the cases $\frac{t}{d}$ can be found in the CF expression of $\frac{e}{\phi(n)}$. This idea was first proposed in [20], where the CF expression $\frac{e}{n}$ has been used to estimate $\frac{t}{d}$, i.e., n has been used as an estimate of $\phi(n)$. Later to that, $n - 2\sqrt{n} + 1$ (an upper bound of $\phi(n)$) has been used as an estimate of $\phi(n)$ in many works, e.g., [22, 2]. In this paper we have studied both the upper and lower bounds of $\phi(n)$ carefully and used $n - \frac{3}{\sqrt{2}}\sqrt{n} + 1$ (a lower bound of $\phi(n)$) as an estimate of $\phi(n)$. We extensively study the cases when $\frac{t}{d}$ can be found in the CF expression of $\frac{e}{n-\frac{3}{\sqrt{2}}\sqrt{n}+1}$. Our results provide new weak keys over the work of [22, 2] and to the best of our knowledge the weak keys identified in our paper have not been presented earlier.

References

1. J. Blomer and A. May. Low secret exponent RSA revised. CaLC 2001, LNCS 2146, pp. 4–19, 2001.
2. J. Blomer and A. May. A generalized Wiener attack on RSA. PKC 2004, LNCS 2947, pp. 1–13, 2004.
3. J. -S. Coron and A. May. Deterministic polynomial-time equivalence of computing the RSA secret key and factoring. Journal of Cryptology, 20: 39–50, 2007.
4. D. Boneh. Twenty Years of Attacks on the RSA Cryptosystem. Notices of the AMS, 46(2):203–213, February, 1999.
5. D. Boneh and G. Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. IEEE Trans. on Information Theory, 46(4):1339–1349, 2000.

6. D. Copppersmith. Small solutions to polynomial equations and low exponent vulnerabilities. Journal of Cryptology, 10(4):223–260, 1997.
7. J. -S. Coron and Alexander May. Deterministic Polynomial-Time Equivalence of Computing the RSA Secret Key and Factoring. J. Cryptology 20(1):39–50 (2007).
8. A. Duejella. Continued fractions and RSA with small secret exponent. Tatra Mt. Math. Publ, vol. 29, pp. 101–112, 2004.
9. E. Jochemsz. Cryptanalysis of RSA variants using small roots of polynomials. Ph. D. thesis, Technische Universiteit Eindhoven, 2007.
10. J. Hastad. On using RSA with low exponent in public key network. Lecture Notes in Computer Science, Advances in Cryplogy-CRYPTO'85 Proceedings. New York: Springer-Verlag, pp 403–408.
11. D. Ibrahim, H. M. Bahig, A. Bhery and S. S. Daoud. A new RSA vulnerability using continued fractions. In the 6th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA 2008), March 31–April 4, 2008, Doha, Qatar.
12. E. Jochemsz and A. May. A Polynomial Time Attack on RSA with Private CRT-Exponents Smaller Than $N^{0.073}$. CRYPTO 2007: 395–411.
13. J. M. Pollard. Theorems on factorization and primality testing. Proc. of Combridge Philos. Soc., vol. 76, pp 521–528, 1974.
14. R. L. Rivest, A. Shamir and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. Communications of ACM, 21(2):158–164, Feb. 1978.
15. K. H. Rosen. Elementary Number Theory. Addison-Wesley, Reading Mass, 1984.
16. R. D. Silverman. Fast generation of random, strong RSA primes. Cryptobytes, 3(1):9–13, 1997.
17. D. R. Stinson. Cryptography – Theory and Practice. 2nd Edition, Chapman & Hall/CRC, 2002.
18. R. Steinfeld, S. Contini, J. Pieprzyk and H. Wang. Converse results to the Wiener attack on RSA. PKC 2005, LNCS 3386, pp. 184–198, 2005.
19. E. R. Verheul and H. C. A. van Tilborg. Cryptanalysis of 'less short' RSA secret exponents. Applicable Algebra in Engineering, Communication and Computing, vol. 8, pp. 425–435, 1997.
20. M. Wiener. Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory, 36(3):553–558, 1990.
21. H. C. Williams. A $p + 1$ method of factoring. Mathematics of Computation, 39(159):225–234, July 1982.
22. B. de Weger. Cryptanalysis of RSA with small prime difference. Applicable Algebra in Engineering, Communication and Computing, 13(1):17–28, 2002.

Appendix A

Example 1 The CF expression of $\frac{e}{n-\lceil \frac{3}{\sqrt{2}}\sqrt{n}\rceil+1}$ is as follows.

0, 2, 1, 1, 1, 35, 1, 1, 1, 1, 4, 1, 1, 2, 11, 1, 3, 1, 1, 3, 2, 8, 30, 1, 1, 1, 16, 1, 1, 1, 1, 7, 1, 5, 1, 2, 1, 1, 1, 2,
1, 3, 1, 1, 1, 1, 2, 4, 2, 5, 1, 6, 1, 1, 1, 5, 4, 31, 7, 4, 1, 5, 5, 3, 1, 145, 1, 54, 5, 1, 4, 3, 2, 18, 1, 1, 1, 2, 1, 3,
3, 11, 6, 1, 1, 1, 1, 27, 4, 2, 1, 5, 1, 1, 3, 1, 11, 4, 3, 10, 1, 2, 1, 2, 3, 8, 1, 1, 1, 2, 1, 7, 1, 2, 3, 4, 1, 6, 3, 1,
4, 1, 8, 621, 1, 4, 2, 11, 1, 1, 35, 1, 113, 7, 1, 13, 1, 2, 1, 20, 1, 2, 6, 2, 1, 5, 3, 4, 1, 2, 17, 3, 2, 3, 3, 1, 1, 1, 2, 4,
1, 22, 1, 1, 4, 1, 1, 4, 1, 1, 3, 3, 1, 150, 4, 1, 1, 4, 2, 1, 1, 1, 9, 6, 1, 1, 1, 8, 1, 1, 30, 26, 1, 1, 1, 1, 9, 1, 6, 3,
3, 12, 1, 1, 1, 2, 2, 1, 14, 1, 3, 7, 1, 2, 1 |, 1242, 1, 1, 1, 2, 1, 4, 5, 12, 1, 1, 4, 13, 5, 4, 10, 1, 1, 1, 12, 1, 30, 2, 65, 10,
1, 2, 3, 1, 6, 1, 1, 15, 14, 6, 2, 9, 3, 2, 13, 2, 10, 1, 7, 1, 2, 1, 1, 1, 2, 1, 1, 1, 1, 1, 2, 17, 1,4, 1, 33, 1, 2, 5, 5,
26, 2, 1, 1, 3, 1, 1, 1, 1, 1, 1, 1, 1, 4, 2, 1, 1, 48, 1, 1, 136, 1, 17, 1, 3, 1, 9, 6, 14, 1, 24, 2, 4, 31, 2, 2, 1, 1, 2, 2,
1, 3, 1, 2, 2, 1, 1, 1, 10, 1, 20, 7, 12, 3, 6, 1, 2, 5, 5, 1, 2, 5, 1, 1, 1, 3, 3, 1, 11, 8, 3, 2, 1, 75, 1, 1, 34, 1, 1, 3,
7, 2, 1, 2, 7, 1, 5, 1, 5, 1, 1, 16, 1, 1, 4, 2, 14, 1, 2, 8, 6, 6, 1, 1, 5, 1, 1, 2, 1, 1, 2, 523, 4, 1, 6, 1, 1, 2, 1, 4,
2, 1, 1, 1, 1, 2, 2, 11, 7, 1, 2, 28, 21, 1, 8, 11, 3, 1, 18, 1, 2, 1, 47, 1, 5, 1, 10, 2, 9, 1, 2, 3, 18, 1, 2, 1, 2, 7, 1, 6,
5, 3, 3, 14, 1, 1, 3, 2, 1, 1, 1, 2, 1, 10, 2, 2, 3, 3, 4, 1, 1, 2, 1, 4, 2, 1, 1, 3, 3, 1, 2, 1, 1, 1, 11, 1, 3, 1, 257, 2,
3, 5, 2, 1, 10, 1, 2, 2, 1, 1, 7, 1, 1, 2, 1, 4, 1, 10, 8, 3, 5, 1, 3, 1, 5, 1, 1, 1, 2, 4, 4, 2, 45, 1, 2, 60, 3, 1, 1, 1,
1, 5, 4, 3, 1, 2, 1, 1, 1, 15, 4, 2, 1, 1, 1, 1, 1, 1, 20, 3, 1, 4, 1, 1, 7, 3, 1, 4, 1, 1, 2, 5, 1, 3, 1, 2, 1, 1, 1, 1,

1, 28, 3, 49, 9, 9, 13, 7, 4, 3, 5, 2, 17, 1, 8, 1, 2, 2, 4, 5, 1, 1, 5, 1, 94, 1, 6, 1, 3, 1, 2, 1, 1, 12, 6, 1, 2, 1, 114, 2,
2, 24, 2, 3, 155, 1, 7, 1, 2, 1, 2, 19, 1, 9, 1, 6, 1, 3, 1, 1, 1, 1, 2, 2, 6, 1, 4, 1, 1, 5, 1, 2, 6, 1, 4, 1, 8, 1, 1, 1,
2, 84, 3.

The CF expression of $\frac{t}{d}$ is as follows.

0, 2, 1, 1, 1, 35, 1, 1, 1, 1, 4, 1, 1, 2, 11, 1, 3, 1, 1, 3, 2, 8, 30, 1, 1, 1, 16, 1, 1, 1, 1, 7, 1, 5, 1, 2, 1, 1, 1, 2,
1, 3, 1, 1, 1, 1, 2, 4, 2, 5, 1, 6, 1, 1, 1, 5, 4, 31, 7, 4, 1, 5, 5, 3, 1, 145, 1, 54, 5, 1, 4, 3, 2, 18, 1, 1, 1, 2, 1, 3,
3, 11, 6, 1, 1, 1, 1, 27, 4, 2, 1, 5, 1, 1, 3, 1, 11, 4, 3, 10, 1, 2, 1, 2, 3, 8, 1, 1, 1, 2, 1, 7, 1, 2, 3, 4, 1, 6, 3, 1,
4, 1, 8, 621, 1, 4, 2, 11, 1, 1, 35, 1, 113, 7, 1, 13, 1, 2, 1, 20, 1, 2, 6, 2, 1, 5, 3, 4, 1, 2, 17, 3, 2, 3, 3, 1, 1, 1, 2, 4,
1, 22, 1, 1, 4, 1, 1, 4, 1, 1, 3, 3, 1, 150, 4, 1, 1, 4, 2, 1, 1, 1, 9, 6, 1, 1, 1, 8, 1, 1, 30, 26, 1, 1, 1, 1, 9, 1, 6, 3,
3, 12, 1, 1, 1, 2, 2, 1, 14, 1, 3, 7, 1, 3.

Example 2 The CF expression of $\frac{e}{n-\lceil\frac{3}{\sqrt{2}}\sqrt{n}\rceil+1}$ is as follows.

0, 8878, 1, 2, 14, 12, 1, 1, 1, 3, 18, 1, 54, 2, 7, 10, 1, 2, 4124, 1, 1, 1, 168, 22, 9, 3, 1, 1, 8, 1, 2, 1, 1, 4, 2, 2, 1, 1, 4, 3,
1, 1, 1, 9, 2, 1, 1, 1, 206, 1, 11, 1, 9, 4, 39, 3, 1, 86, 1, 2, 1, 6, 1, 1, 2, 5, 4, 3, 1, 6, 1, 4, 1, 6, 1, 2, 2, 4, 8, 7,
1, 24, 1, 1, 2, 17, 1, 165, 1, 1, 16, 1, 2, 17, 9, 1, 3, 5, 2, 1, 3, 1, 2, 5, 1, 2, 3, 2, 4, 2, 22, 2, 4, 1, 1, 2, 4, 1, 3, 1,
2, 1, 131, 1, 2, 22, 5, 11, 1, 4, 14, 2, 2, 2, 10, 1, 2, 2, 1, 3, 1, 3, 1, 17, 1, 1, 2, 1, 3, 10, 1, 1, 1, 4, 1, 11, 1, 1, 1, 2,
69, 2, 1, 1, 1, 168, 3, 1, 1, 2, 4, 4, 1, 1, 53, 1, 15, 18, 6, 2, 3, 2, 1, 2, 4, 1, 23, 1, 4 |, 1, 1, 28, 2, 1, 1, 1, 1, 1, 1, 1,
2, 2, 3, 1, 2, 1, 3, 5, 3, 28, 1, 2, 2, 2, 2, 7, 4, 1, 1, 1, 1, 1, 6, 2, 3, 3, 47, 1, 1, 4, 2, 1, 1, 2, 1, 30, 4, 1, 1, 315,
1, 3, 30, 2, 1, 4, 1, 21, 1, 10, 1, 2, 1, 5, 9, 1, 26, 1, 1, 1, 4, 1, 5, 2, 457, 1, 1, 13, 9, 25, 2, 3, 1, 92, 1, 1, 3, 1, 2, 4,
158, 3, 4, 6, 2, 22, 1, 5, 1, 1, 1, 2, 4, 1, 1, 2, 6, 4, 2, 5, 2, 1, 1, 16, 47, 4, 1, 1, 2, 1, 2, 1, 1, 2, 3, 2, 3, 12, 7, 2,
2, 1, 5, 2, 1, 1, 1, 3, 1, 15, 1, 1, 1, 1, 1, 1, 7, 1, 101, 2, 1, 1, 5, 1, 1, 1, 1, 5, 1, 1, 1, 3, 4, 1, 9, 2, 1, 228, 1, 1,
3, 1, 2, 3, 7, 1, 1, 1, 12, 1, 2, 2, 10, 3, 2, 1, 14, 5, 2, 2, 1, 32, 1, 59, 2, 110, 1, 9, 1, 7, 9, 1, 7, 2, 1, 2, 1, 3, 5, 1,
1, 1, 1, 3, 8, 2, 2, 1, 2, 6, 1, 3, 7, 1, 7, 1, 1, 1, 10, 1, 1, 1, 1, 2, 1, 2, 1, 1, 1, 4, 3, 3, 18, 3, 3, 1, 1, 1, 1, 8,
1, 3, 1, 1, 6, 4, 9, 1, 3, 5, 1, 1, 3, 26, 38, 3, 6, 2, 2, 1, 1, 14, 1, 4, 1, 1, 3, 4, 1, 4, 1, 2, 2, 2, 1, 3, 15, 4, 1, 2,
1, 1, 6, 2, 1, 1, 1, 6, 11, 15, 1, 7, 3, 1, 1, 1, 3, 1, 1, 1, 11, 1, 1, 1, 5, 1, 5, 1, 1, 1, 9, 1, 1, 6, 25, 2, 2, 6, 2, 7,
4, 3, 1, 1, 1, 3, 2, 1, 6, 14, 2, 1, 1, 1, 2, 1, 6, 1, 17, 1, 1, 1, 18, 2, 1, 1, 1, 1, 1, 3, 1, 2, 1, 2, 34, 2, 3, 30, 1, 3,
2, 4, 1, 2, 1, 2, 1, 3, 1, 5, 1, 2, 1, 1, 1, 7, 1, 4, 6, 3, 5, 2, 2, 4, 2, 1, 10, 2, 1, 6, 1, 5, 1, 1, 11, 1, 6, 28, 1, 2,
9, 1, 2, 2, 1, 3, 1, 1, 2, 2, 2, 2, 2, 2, 1, 1, 1, 1, 1, 3, 4, 1, 1, 17, 1, 1, 4, 2, 7, 6, 6, 3, 4, 2, 14, 1, 6, 1, 2.

The CF expression of $\frac{t}{d}$ is as follows.

0, 8878, 1, 2, 14, 12, 1, 1, 1, 3, 18, 1, 54, 2, 7, 10, 1, 2, 4124, 1, 1, 1, 168, 22, 9, 3, 1, 1, 8, 1, 2, 1, 1, 4, 2, 2, 1, 1, 4, 3,
1, 1, 1, 9, 2, 1, 1, 1, 206, 1, 11, 1, 9, 4, 39, 3, 1, 86, 1, 2, 1, 6, 1, 1, 2, 5, 4, 3, 1, 6, 1, 4, 1, 6, 1, 2, 2, 4, 8, 7,
1, 24, 1, 1, 2, 17, 1, 165, 1, 1, 16, 1, 2, 17, 9, 1, 3, 5, 2, 1, 3, 1, 2, 5, 1, 2, 3, 2, 4, 2, 22, 2, 4, 1, 1, 2, 4, 1, 3, 1,
2, 1, 131, 1, 2, 22, 5, 11, 1, 4, 14, 2, 2, 2, 10, 1, 2, 2, 1, 3, 1, 3, 1, 17, 1, 1, 2, 1, 3, 10, 1, 1, 1, 4, 1, 11, 1, 1, 1, 2,
69, 2, 1, 1, 1, 168, 3, 1, 1, 2, 4, 4, 1, 1, 53, 1, 15, 18, 6, 2, 3, 2, 1, 2, 4, 1, 23, 1, 4.

Example 3. Refer to p, q of Example 1.

We consider $d > n^{\frac{1}{3}}$. Let $d =$
61033620665104690038995387156383867652322226123296685389723133974030185448442674
868648018282242385291149523 (a 107 digit number).

The corresponding e is
50540840993586746176600277435717647268345032073616659706674487447082243977918413
69230468320247447700980725776203252713926251719762610251531355631225052032958925

15721185756124886461821221336089046395014548367690311088585379161620308946520609
52054971519354961768941803469478934733847712332990457645725177388815967595164763 .

Now the value of $\frac{\frac{2n}{(2d+1)^2}-\frac{n}{n-A+1}}{\frac{n}{n-B}-\frac{n}{n-A+1}}$ is
27752782508386083340303355961072715172277767233940251957583970436546175777700818
56675682093198406639916267829956297391155579729307540645697606925067924255151889
80660932268183968356467852982743493427983896661042498000474961761359348086394693
97989358459219665226578434492825190314230927017627756077533311413417373451513,

which is smaller than e.

The value of t is
13567636387098752787725975030066552194109294975540802943145816240544873199851054
057524379767989315810471872.

The CF expression of $\frac{e}{n-\lceil\frac{3}{\sqrt{2}}\sqrt{n}\rceil+1}$ is as follows.

0, 4, 2, 163, 49, 1, 6, 10, 74, 1, 3, 2, 12, 1, 3, 1, 4, 1, 1, 1, 1, 2, 1, 1 ,4, 1, 2, 42, 21, 1, 1, 9, 2, 3, 1, 3, 1, 6, 1, 1,
2, 3, 19, 1, 2, 1, 2, 1, 7, 1, 35, 1, 11, 3, 14, 1, 2, 1, 3, 188, 1, 3, 5, 3, 1, 3, 1, 26, 2, 2, 1, 1, 1, 9, 1, 1, 3, 1, 4, 1,
1, 1, 3, 3, 1, 1, 1, 1, 2, 1, 1, 2, 4, 1, 11, 5, 2, 1, 7, 2, 1, 6, 3, 1, 3, 7, 1, 1, 1, 3, 1, 8, 9, 3, 5, 1, 4, 2, 1, 16,
1, 1, 1, 5, 2, 4, 1, 2, 1, 5, 1, 12, 2, 3, 2, 21, 2, 1, 6, 2, 3, 2, 1, 11, 1, 2, 1, 8, 1, 1, 2, 5, 1, 4, 4, 20, 2, 2, 22, 3,
2, 1, 2, 9, 6, 1, 1, 2, 3, 1, 1, 2, 1, 1, 15, 15, 1, 4, 1, 7, 1, 1, 1, 1, 1, 1, 5, 1, 2, 1, 1, 7, 7, 1, 2, 2, 7, 2, 11, 6,
1, 2, 223, 2, 4, 5, 1, 1, 9, 3, 3, 2, 1, 1, 5, 1, 3, 5, 1, 1, 1, 2, 26, 1, 1, 7, 10, 2, 1, 7, 4, 7, 1, 1, 5, 1, 4, 2, 2, 2,
3, 1, 5, 2, 1, 1, 2, 1, 1, 6, 6, 1, 10, 1, 33, 1, 6, 1, 3, 1, 2, 1, 2, 1, 1, 11, 3, 2, 8, 1, 29, 3, 2, 2, 36, 1, 5, 1, 2, 10,
9, 1, 4, 1, 9, 3, 1, 22, 4, 6, 10, 1, 1, 5, 10, 234, 1, 3, 13, 4, 9, 2, 1, 1, 2, 2, 1, 14, 1, 1, 2, 1, 1, 2, 5, 4, 1, 5, 1, 1,
4, 1, 62, 4, 8, 1, 8, 47, 10, 3, 2, 3, 7, 2, 2, 1, 2, 1, 1, 20, 1, 1, 1, 19, 440, 3, 3, 1, 6, 1, 2, 3, 2, 1, 3, 1, 1, 3, 1, 1,
48, 6, 2, 15, 21, 1, 4, 2, 3, 4, 234, 19, 50, 2, 18, 1, 3, 2, 2, 3, 3, 4, 1, 1, 5, 9, 7, 1, 3, 1, 1, 3, 1, 8, 1, 6, 2, 1, 24, 2,
14, 1, 6, 2, 2, 4, 6, 2, 1, 6, 7, 16, 3, 4, 8, 1, 1, 1, 3, 1, 2, 2, 1, 8, 1, 2, 2, 2, 1, 2, 1, 1, 4, 5, 1, 5, 1, 1, 14, 1,
1, 78, 2, 1, 2, 3, 3, 1, 1, 2, 4, 16, 1, 1, 1, 1, 1, 1, 1, 6, 2, 76, 2, 1, 2, 2, 2, 1, 1, 1, 1, 5, 2, 1, 1, 1, 1, 6, 1, 1,
1, 1, 5, 1, 29, 1, 40, 2, 1, 1, 7, 1, 3, 1, 4, 1, 5, 1, 4, 2, 1, 3, 1, 1, 2, 1, 15, 2, 9, 2, 1, 15, 1, 3, 2, 1, 1, 2, 9, 1,
2, 27, 2, 2, 1, 2, 3, 5, 3, 1, 4, 4, 1, 1, 1, 1, 7, 2, 5, 1, 1, 8, 2, 3, 1, 2, 1, 2, 1, 1, 1, 1, 1, 36, 1, 1, 3, 16, 1, 1,
1, 1, 1, 6, 1, 1, 3, 1, 6, 2, 1, 1, 3, 5, 53, 3, 2, 2, 3, 4, 1, 3, 1, 1, 1, 1, 9, 1, 2, 9, 3, 1, 5, 1, 1, 1, 39, 3, 1, 1,
1, 2, 1, 18, 1, 1, 2, 1, 2, 4, 1, 1, 1, 1, 6, 1, 2, 1, 1, 4, 1, 1, 1, 4, 2, 30, 1, 3, 1, 18, 9, 1, 1, 1, 1, 31, 2, 44, 3117868, 11,
1, 3.

The CF expression of $\frac{t}{d}$ is as follows.

0, 4, 2, 163, 49, 1, 6, 10, 74, 1, 3, 2, 12, 1, 3, 1, 4, 1, 1, 1, 1, 2, 1, 1, 4, 1, 2, 42, 21, 1, 1, 9, 2, 3, 1, 3, 1, 6, 1, 1,
2, 3, 19, 1, 2, 1, 2, 1, 7, 1, 35, 1, 11, 3, 14, 1, 2, 1, 3, 188, 1, 3, 5, 3, 1, 3, 1, 26, 2, 2, 1, 1, 1, 9, 1, 1, 3, 1, 4, 1,
1, 1, 3, 3, 1, 1, 1, 1, 2, 1, 1, 2, 4, 1, 11, 5, 2, 1, 7, 2, 1, 6, 3, 1, 3, 7, 1, 1, 1, 3, 1, 8, 9, 3, 5, 1, 4, 2, 1, 16,
1, 1, 1, 5, 2, 4, 1, 2, 1, 5, 1, 12, 2, 3, 2, 21, 2, 1, 6, 2, 3, 2, 1, 11, 1, 2, 1, 8, 1, 1, 2, 5, 1, 4, 4, 20, 2, 2, 22, 3,
2, 1, 2, 9, 6, 1, 1, 2, 3, 1, 1, 2, 1, 1, 15, 15, 1, 4, 1, 7, 1, 1, 1, 1, 1, 1, 5, 1, 2, 1, 1, 7, 7, 1, 2, 2, 7, 2, 11, 6,
1, 2, 223, 2, 4, 5, 1, 1, 9, 3, 3, 2, 1, 1, 5, 2, 2, 10.

Note that the CF expression of $\frac{t}{d}$ could not be found (last three places do not match) in the CF expression of $\frac{e}{n-\lceil\frac{3}{\sqrt{2}}\sqrt{n}\rceil+1}$.