Revisiting Wiener's Attack – New Weak Keys in RSA*

Subhamoy Maitra and Santanu Sarkar

Indian Statistical Institute, 203 B T Road, Kolkata 700 108, India
{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 $0.3 \leq \delta \leq 0.5$. Given ρ ($1 \leq \rho \leq 2$) is known to the attacker, we show that the RSA keys are weak when $d = N^{\delta}$ and $\delta < \frac{1}{2} - \frac{\gamma}{2}$, where $|\rho q - p| \leq \frac{N^{\gamma}}{16}$. This presents additional results over the work of de Weger (AAECC 2002). We also discuss how the lattice based idea of Boneh-Durfee (IEEE-IT 2000) works better to find weak keys beyond the bound $\delta < \frac{1}{2} - \frac{\gamma}{2}$. 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 techniques we also present new results over the work of Blömer 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:

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

In this paper we exploit the Wiener's method [23] of continued fraction (CF) to find new weaknesses in RSA (see [15] for Legendre's theorem related to CF expression). Wiener [23] 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 [25, Section 4], Wiener's attack [23] has been extended estimating $\phi(N)$ as $N - 2\sqrt{N} + 1$.

* This is a substantially revised (with some corrections and generalizations) and extended version of the paper that has been presented in "ISC 2008, 11th Information Security Conference" September 15-18, 2008, Taipei, Taiwan, published in Pages 228–243, volume 5222, Lecture Notes in Computer Science, Springer, 2008. The introduction of the parameter ρ is a generalization in Theorems 1, 4; in the conference version, we have used $\rho = 2$. Further, Sections 2.1, 3.1 present additional materials that were not included in the conference version of this paper.

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 [24]. 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 [3]. 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 work of [23] initiates the application of Continued Fraction (CF) expression for the attack. In the work of [6], important results have been shown regarding small solutions to polynomial equations that in turn show vulnerabilities of low exponent RSA. In [4, 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 [23] in many papers [4, 5, 25, 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 [23] can be exploited to find weaknesses of RSA when d is small. In [25, Section 4], some extension of the work [23] has been mentioned and it has also been noted that similar extension will work on the results of [22]. The result of [22] 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 [22]. 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 [23], 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 [19], 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 [23] 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 [23], $\phi(N)$ has been approximated by N to get the results. A better result has been obtained in [25, 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 [25] gives similar bound on d as in [23], 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 [25, Section 5, 6], the attack of [4, 5] has been extended considering the value of β, where $p - q = N^{\beta}$. Instead of considering $p - q = N^{\beta}$, we here consider $|\rho q - p| \leq \frac{N^{\gamma}}{16}$ where $1 \leq \rho \leq 2$ to get additional results. These results are presented in Section 2. Further, in Section 2.1, we also study the idea of Boneh and Durfee [4, 5] to demonstrate that it compares better than the idea presented in the beginning of Section 2 which uses the idea of CF expansion only.

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 2.2.

In [2], it has been shown that p, q can be found in polynomial time for every N, e satisfying $ex + y \equiv 0 \bmod \phi(N)$, 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 [23] in their proof. We also provide additional result over [2].This is presented in Section 3.

We here highlight the contribution of this paper.

1. Given ρ with $1 \leq \rho \leq 2$ known to the attacker RSA is insecure when $d = N^{\delta}$ and $\delta < \frac{1}{2} - \frac{\gamma}{2}$, where $|\rho q - p| \leq \frac{N^{\gamma}}{16}$ and $\gamma \leq \frac{1}{2}$. Further we show that this bound on δ can be extended using the lattice based techniques.
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 $m > 0$, $0 < x \leq \frac{1}{6}\sqrt{\frac{\phi(N)}{e}}N^{\frac{1}{2}-\frac{\gamma}{2}}$ for and $|y| \leq \frac{N^{\gamma}}{\phi(N)N^{\frac{1}{4}}}ex$ where $|\rho q - p| \leq N^{\gamma}$ where $\gamma \leq \frac{1}{2}$ and ρ is known to the attacker.

In the conference version of this paper, we have considered $\rho = 2$, whereas, the case for $\rho = 1$ has been studied [25]. Taking ρ in the range of $[1, 2]$ generalizes both these ideas. One may ask a question that how ρ can be available to the attacker. In fact, one may try to guess ρ for different values (that are computationally feasible) to mount the attack. Further, one may note that the knowledge of most significant bits (MSBs) of p or q can provide some approximation of ρ that may also be used. In [21], it has also been studied how a few MSBs of p or q can be found from the knowledge of N only.

Our result in 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 [7, 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.

In [20], Sun and Yang proposed a variant of RSA where the public encryption exponent e and the private decryption exponent d are such that $\log_2 e + \log_2 d \approx \log_2 N + l_k$, where l_k is a positive integer. The main idea was to keep the bit size d as well as e quite less and the value of l_k is related to the security of this variant of RSA. Though the class of the exponents in [20] are not covered by our Theorem 3, one needs to be cautious while choosing e, d, when both of them are restricted by some upper bound.

Before proceeding further, let us explain the Continued Fraction (CF) expression. We follow the material from [18, 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 $p - q < N^{\frac{1}{4}}$ [17] (see also [25, 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 [25], 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 $O(N^{0.5})$.

Proposition 2. *Let $|p - \rho q| \leq \frac{N^\gamma}{16}$, where $\gamma < \frac{1}{2}$ and $1 \leq \rho \leq 2$. Then $|p + q - (\sqrt{\rho} + \frac{1}{\sqrt{\rho}})\sqrt{N}| < \frac{N^\gamma}{8}$.*

Proof. We have $|p - \rho q| \leq \frac{N^\gamma}{16}$. So $|p^2 - \rho N| \leq \frac{pN^\gamma}{16}$. Hence $|p - \sqrt{\rho N}| \cdot |p + \sqrt{\rho N}| \leq \frac{pN^\gamma}{16}$, i.e., $|p - \sqrt{\rho N}| \cdot |1 + \frac{\sqrt{\rho N}}{p}| \leq \frac{N^\gamma}{16}$. As $|1 + \frac{\sqrt{\rho N}}{p}| > 1$, we have $|p - \sqrt{\rho N}| < \frac{N^\gamma}{16}$. Again multiplying q with the inequality $|p - \rho q| \leq \frac{N^\gamma}{16}$, we have $|N - \rho q^2| \leq \frac{qN^\gamma}{16}$. So we have $|\sqrt{\rho} q - \sqrt{N}| \cdot |\sqrt{\rho} + \frac{\sqrt{N}}{q}| \leq \frac{N^\gamma}{16}$. As $\rho \geq 1$, we have $|\sqrt{\rho} + \frac{\sqrt{N}}{q}| > 1$. Hence, $|\sqrt{\rho} q - \sqrt{N}| < \frac{N^\gamma}{16}$ i.e., $|q - \sqrt{\frac{N}{\rho}}| < \frac{N^\gamma}{16\sqrt{\rho}} \leq \frac{N^\gamma}{16}$, as $\rho \geq 1$. Now $|p + q - (\sqrt{\rho} + \frac{1}{\sqrt{\rho}})\sqrt{N}| \leq |p - \sqrt{\rho N}| + |q - \sqrt{\frac{N}{\rho}}| < \frac{N^\gamma}{8}$. □

Theorem 1. *Let $|p-\rho q| \leq \frac{N^\gamma}{16}$ with $1 \leq \rho \leq 2$, $\gamma \leq \frac{1}{2}$ and $d = N^\delta$. Then N can be factored in $O(poly(\log(N)))$ time when $\delta < \frac{1-\gamma}{2}$.*

Proof. Since $|p-\rho q| \leq \frac{N^\gamma}{16}$, we have $|p+q-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}| < \frac{N^\gamma}{8}$,

i.e., $|\phi(N)-N-1+(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}| < \frac{N^\gamma}{8}$. Now,

$$\begin{aligned}
|\frac{e}{N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1} - \frac{t}{d}| &\leq |\frac{e}{N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1} - \frac{e}{\phi(N)}| + |\frac{e}{\phi(N)} - \frac{t}{d}| \\
&= \frac{e|\phi(N) - \big(N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1\big)|}{\phi(N)\big(N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1\big)} + \frac{1}{d\phi(N)} \\
&< \frac{|\phi(N) - \big(N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1\big)|}{\big(N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1\big)} + \frac{1}{d\phi(N)} \\
&< \frac{N^\gamma}{8\frac{N}{2}} + \frac{1}{4d^2},
\end{aligned}$$

assuming $N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1 > \frac{N}{2}$ and $\phi(N) > 4d$.

Thus, $|\frac{e}{N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1} - \frac{t}{d}| < \frac{N^\gamma}{8\frac{N}{2}} + \frac{1}{4d^2} = \frac{N^{\gamma-1}}{4} + \frac{1}{4d^2}$.

When $\frac{N^{\gamma-1}}{4} < \frac{1}{4d^2}$, we get $|\frac{e}{N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1} - \frac{t}{d}| < \frac{1}{2d^2}$.

Putting $d = N^\delta$ in the inequality $\frac{N^{\gamma-1}}{4} < \frac{1}{4d^2}$, we get $\delta < \frac{1-\gamma}{2}$. This gives the proof. □

For experimental evidences, we work with primes $p, q \geq 10^{160}$, i.e., $N \geq 10^{320}$ and $\rho = 2$. So in this case we study the Continued Fraction of $\frac{e}{N-\frac{3}{\sqrt{2}}\sqrt{N}+1}$. 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 [17] (see also [25, Section 3]). Thus we consider the scenario when $2q-p > N^{\frac{1}{3}}$. All the examples in this paper (apart from the results related to lattice reduction) 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, $2q-p < \frac{N^{0.352}}{16}$. 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 $\phi(N)$.

We consider p, q respectively as

213240012369375032891677978840508057002476631792587679131233694906832986110135 42

482710293984079429269505393966895473715804331857655334272013326966301014512312663 and

106620006184687516445838989420254028501238315896298839565616847453416493055067 71

241355146992039714634752696983447736857902165928827667136006663483150507256156183, which gives N as

227356514376456085145407643699497785267575964192664414706015618659113920770516 06

876372813657802669960516535143810533128200855625818799416971008924610927914638 14

72361264666736466411449942059568093916061632275622633234439324940363916123064654

02555303399548519028121978759763373757433442757741456334433042737747175925664532 9.

Note that $2q - p > N^{\frac{1}{3}}$. One can check that $\phi(N)$ is

22735651437645608514540764369949778526757596419266441470601561865911392077051606

87637281365780266996051653514381053312820085562581879941697100892461092791463814

40375262811330211477698245233491885365690137506733981364754270704338968206544340

30148759301936604637696169664729052700062792979093156193631043692802023748817648 4.

Taking $\gamma = 0.352$, we get $\delta < \frac{1-\gamma}{2} = 0.324$. Thus, in this case for any $d < N^{0.324}$, RSA will be insecure.

Now take $N^{0.323} < d < N^{0.324}$. We consider $d =$

44138452180807132553854898960195837050529634687636859759755568727353610483058810149497334438480706535427

(a 104 digit number). The corresponding e is

85356738187677927267094758044990579754357485762742350715347494115752841684037367

61958050516985955514963349897936619515552408960795697318670660889152163280842447

75560973766638533120643123534024611720642739938697649334533161511773864127534483

56073872108358709307048969215446586611896268736369229047317637983628682308907311. The value of t is

16570953848141161450099797936855484729106684488828631895806571167212612482288825100679308747791603915419.

Here $\frac{t}{d}$ could be found in the CF expression of $\frac{e}{N-\lceil \frac{3}{\sqrt{2}}\sqrt{N}\rceil+1}$. 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, 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.

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 $\frac{t}{d}$. This example corresponds to Theorem 1. □

In fact, Theorem 1 presents a sufficient condition on d when RSA will be weak. In Example 3, 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 3 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 lattice based idea

In this section, we exploit lattice based techniques following the idea of [4, Section 4]. This idea has been used in [25, Section 5] when $p-q$ is bounded. We use similar idea when $\rho q-p$ is bounded. In this section we refer to the earlier works and do not explain the idea related to lattices in details. To follow our results, one may need to go through the detailed ideas presented in [4, 5, 25, 1, 16].

Let $d = N^{\delta}$. We assume $e = N$ as for $e < N$ one can get better upper bound on δ [4, Page 9]. We have $ed = 1+t\phi(N) = 1+t(N+1-p-q) = 1+t\big(N+1-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}-(p+q-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N})\big) = 1+x(A+y)$, where $x = t < d = N^{\delta}$, $A = N+1-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}$, $y = -(p+q-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N})$.

Using $e = N$, we have, $x < e^{\delta}$, $|y| < \frac{e^{\gamma}}{8}$.

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 $|y_0| < e^{\gamma}$. So we have to find the roots of the polynomial $f(x,y) = 1+x(A+y)$. Let $X = e^{\delta}, Y = e^{\gamma}$. Then X, Y are the upper bounds of x_0, y_0 neglecting the constant terms. As the polynomial $f(x,y)$ we have described here is same as the polynomial in [16, Theorems 3, 4, 5], the upper bounds X, Y of the roots will also same. Hence, we can use the same analysis of [16, Theorems 3, 4, 5] to note that RSA is insecure under the following conditions:

$$\delta < \frac{\gamma+3-2\sqrt{\gamma(\gamma+3)}}{3}; \tag{1}$$

$$1-2\gamma < \delta < 1-\sqrt{\gamma}; \tag{2}$$

$$\delta < \frac{\sqrt{16\gamma^2-4\gamma+4}-(6\gamma-2)}{5}. \tag{3}$$

The shaded region in Figure 1 identifies the values of γ, δ for which we find that RSA is insecure. In the figure, $g(\gamma) = \frac{\gamma+3-2\sqrt{\gamma(\gamma+3)}}{3}$ (corresponding to Inequality 1), $f(\gamma) = 1-\sqrt{\gamma}$ (corresponding to Inequality 2) and $h(\gamma) = \frac{\sqrt{16\gamma^2-4\gamma+4}-(6\gamma-2)}{5}$ (corresponding to Inequality 3). The lower bound of the Inequality 2, i.e., $1-2\gamma$ is marked by a straight line.

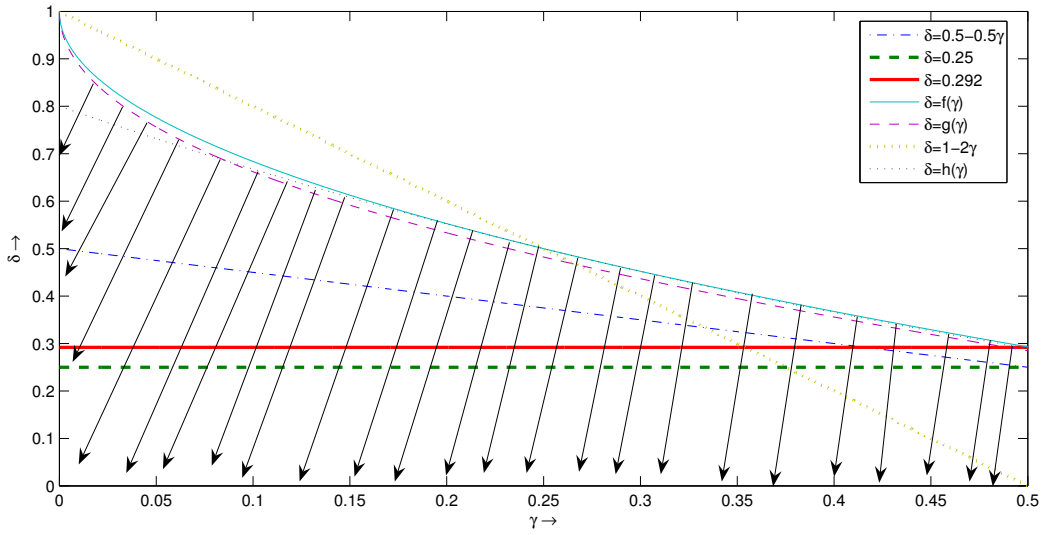

Fig. 1. The region for δ and γ values for which RSA is insecure.

The case $\delta = 0.25$ corresponds to the result of [23], the case $\delta = 0.292$ corresponds to the result of [5] and the case $\delta = 0.5 - 0.5\gamma$ corresponds to our Theorem 1.

Example 2. For lattice based strategy, we have implemented the program in SAGE 2.10.1 over Linux Ubuntu 7.04 on a computer with Dual CORE Intel(R) Pentium(R) D CPU 2.80GHz, 1 GB RAM and 2 MB Cache. The lattice parameters used here are $m = 7, t = 3$ and one may refer to [16] for description of these lattice parameters. The attacker knows only N, e as described below and tries to find out d.

We consider same N as in Example 1. The public exponent e is

968545944720251695897037715913140862041259865394769027160325103716564451

704935459523900224473726651569335320384485865377243077222160184965716219

829301274193800900813491646892647872093725247818205448106997599371658702

630582585917946622177236243496259549473722969391510051505787653540435397

86283576135592426293702846987845.

The corresponding decryption exponent d (121 digit number) is

258224987808690858965591917200301187432970579282922351283065935654064762

2016841194629645353280137831435903171972747493377, which gives δ is 0.376.

The value of t is

110004661820872535644569180841244472278368782736420977567878308 08

537855730230353060585975508496387987197764863540962721 21.

For the cases corresponding to Inequalities 1, 2 and 3, we get the lattices of dimension $w = 60, 51$ and 32 respectively and the required times to find d are 789, 774 and 409 seconds.

The idea of continued fraction method as explained in Theorem 1 will not work in this case as the value of δ is higher. □

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 $0 < \delta \leq \frac{1}{2}$. Let A, B be as in Proposition 1. Then for $e \leq \frac{2N^{1-2\delta} - \frac{N}{N-A+1}}{\frac{N}{N-B} - \frac{N}{N-A+1}}$, 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* $\frac{N}{N-B+1} \leq \frac{z_1}{z_2} < \frac{2}{e}N^{1-2\delta} + \frac{N}{e}\frac{e-1}{N-A+1}$ *and*
2. $\frac{t}{d} - \frac{e}{N}\frac{z_1}{z_2} < \frac{1}{2d^2}$ *when* $\frac{N}{N-B+1} - \frac{2}{e}N^{1-2k} < \frac{z_1}{z_2} \leq \frac{N}{e}\frac{e-1}{N-A+1}$.

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

1. $\frac{t}{d} - \frac{e}{N} \geq \frac{1}{2d^2}$ but $0 \leq \frac{e}{N}\frac{z_1}{z_2} - \frac{t}{d} < \frac{1}{2d^2}$.
2. $\frac{t}{d} - \frac{e}{N} \geq \frac{1}{2d^2}$ but $0 \leq \frac{t}{d} - \frac{e}{N}\frac{z_1}{z_2} < \frac{1}{2d^2}$.

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

Thus, we have to satisfy $0 \leq \frac{edz_1 - tNz_2}{Ndz_2} < \frac{1}{2d^2}$, i.e., $0 \leq \frac{z_1 + z_1 t\phi(N) - tNz_2}{Nz_2} < \frac{1}{2d}$.

Let $2d < N^{\delta}$, for $\delta > 0$. Then $0 \leq \frac{z_1 + z_1 t\phi(N) - tNz_2}{Nz_2} < \frac{1}{N^{\delta}}$ implies $0 \leq \frac{z_1 + z_1 t\phi(N) - tNz_2}{Nz_2} < \frac{1}{2d}$.

So we need to estimate $\frac{z_1}{z_2}$ considering $0 \leq \frac{z_1 + z_1 t\phi(N) - tNz_2}{Nz_2} < \frac{1}{N^{\delta}}$.

Now $0 \leq \frac{z_1 + z_1 t\phi(N) - tNz_2}{Nz_2} < \frac{1}{N^{\delta}}$ iff $0 \leq \frac{z_1}{z_2}(1 + t\phi(N)) - tN < N^{1-\delta}$ iff

$tN \leq \frac{z_1}{z_2}(1 + t\phi(N)) < N^{1-k} + tN$ iff $\frac{tN}{1+t\phi(N)} \leq \frac{z_1}{z_2} < \frac{N^{1-\delta}+tN}{1+t\phi(N)}$ if

$\frac{N}{\phi(N)} \leq \frac{z_1}{z_2} < \frac{N^{1-\delta}+tN}{ed}$ 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

$[\frac{N}{N-B+1}, \frac{2}{e}N^{1-2k} + \frac{N}{e}\frac{e-1}{N-A+1})$, 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, $\frac{N}{N-B} \leq \frac{2}{e}N^{1-2k} + \frac{N}{e}\frac{e-1}{N-A+1}$ 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 $\frac{N}{N-B+1} \leq \frac{z_1}{z_2} < \frac{2}{e}N^{1-2k} + \frac{N}{e}\frac{e-1}{N-A+1}$ and $\frac{N}{N-B+1} - \frac{2}{e}N^{1-2k} < \frac{z_1}{z_2} \leq \frac{N}{e}\frac{e-1}{N-A+1}$.

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 $O(N^{\frac{3}{2}-2\delta})$. □

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 [25, 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 [25, 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 [25] 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, δ.
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 3. Refer to p, q of Example 1. We consider $d > N^{\frac{1}{3}}$, which is

610336206651046900389953871563838676523222261232966853897231339740301854484426748686480182822423852911584 93

(a 107 digit number). The corresponding e is

256070337470608788319481009607488523602511607514442544529285221432548011674213 62

255131579900075236835353282765120152184163423407904512662705681137425889040591 35

278866096421869787394806422548152901989481102614144150711908553040651733174615 87

219152177320300403509021656688133531875180594146046602509905386718318283402 53.

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

277527825083860833403033559610727151722777672339402519575839704365461757777008 18

566756820931984066399154520747827146667220780066819468476440668625084009465404 80

958270163105516686900033446501197661512346429175036283679930367111121556002491 71

858250543822132777886134760974691919179847616254071357103111675902815747786 53,

which is greater than e indeed. The value of t is

687418167173701703542021027522012363784411840109884330984502170326678378077779701089832928385613474642.

Here $\frac{t}{d}$ could be found in the CF expression of $\frac{e}{N - \lceil \frac{3}{\sqrt{2}}\sqrt{N} \rceil + 1}$. 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, 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.

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 $\frac{t}{d}$). This example corresponds to Corollary 1. □

One may check that $\frac{t}{d}$ will not be found in the continued fraction expression of $\frac{e}{N}$ (Weiner's result [23]) or $\frac{e}{N-2\sqrt{N}+1}$ (Weger's result [25, Section 4]) in Example 3. In this example, $ed^2 \approx N^{1.653}$. Actually, the bound $ed^2 \leq N^{1.5}$ in Theorem 3 is a conservative approximation of the result in Corollary 1. In practice, we may get results when ed^2 is greater than $N^{1.5}$.

In [25, Sections 5, 6], the approach of [4] has been used to slightly improve the bounds of [25, 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 3, $N^{0.4995} < p-q < N^{0.4996}$. 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 [25, 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 [25, Section 6]. Now we present another example.

Example 4. Refer to p, q of Example 1.

We consider $d > N^{\frac{1}{3}}$. Let $d =$

610336206651046900389953871563838676523222261232966853897231339740301854484426 74

868648018282242385291149523 (a 107 digit number). The corresponding e is

505408409935867461766002774357176472683450320736166597066744874470822439779184 13

692304683202474477009807257762032527139262517197626102515313556312250520329589 25

157211857561248864618212213360890463950145483676903110885853791616203089465206 09

520549715193549617689418034694789347338477123329904576457251773888159675951647 63 .

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

277527825083860833403033559610727151722777672339402519575839704365461757777008 18

566756820931984066399162678299562973911555797293075406456976069250679242551518 89

806609322681839683564678529827434934279838966610424980004749617613593480863946 93

979893584592196652265784344928251903142309270176277560775331141341737345151 3,

which is smaller than e and thus the condition in Corollary 1 is not satisfied. The value of t is

135676363870987527877259750300665521941092949755408029431458162405448731998510 54

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 $\frac{e}{N-\lceil\frac{3}{\sqrt{2}}\sqrt{N}\rceil+1}$. □

Remark 1. We present Example 4 to show the effects of the upper bound on d in Theorem 1 as well as the upper bounds on d, e in Corollary 1. Note that

"d of Example 1" < "d of Example 4" < "d of Example 3".

For the "d of Example 4", $\frac{t}{d}$ cannot be found in the CF expression of $\frac{e}{N-\lceil\frac{3}{\sqrt{2}}\sqrt{N}\rceil+1}$. The "$d$ of Example 4" does not satisfy the condition given in Theorem 1. On the other hand, though "d of Example 4" < "d of Example 3", the bound on e corresponding to Corollary 1 is not satisfied in Example 4.

One may note that in Example 4, the CF expression of $\frac{t}{d}$ does not match only in 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 [22] 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 $ex + y \equiv 0 \bmod \phi(N)$, 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 $ex+y = m(N-p-q+1)$. This gives $\frac{e}{N} - \frac{m}{x} = -\frac{m(p+q-1)+y}{Nx}$. If $|\frac{e}{N} - \frac{m}{x}| = |\frac{m(p+q-1)+y}{Nx}| < \frac{1}{2x^2}$, then the fraction $\frac{m}{x}$ appears among the convergents of $\frac{e}{N}$. Thus one needs to find out the

conditions such that $|m(p+q-1)+y| < \frac{N}{2x}$ 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 $\frac{m}{x}$ among the convergents of $\frac{e}{N}$, a better attempt will be to find $\frac{m}{x}$ among the convergents of $\frac{e}{\phi'(N)}$, where $\phi'(N)$ is a better estimate than N for $\phi(N)$. Following the idea of [25], $\phi'(N)$ 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 $\frac{m}{x}$ 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 $ex + y \equiv 0 \bmod \phi(N)$, with $x \leq \frac{1}{3}\sqrt{\frac{\phi(N)}{e}}\frac{N^{\frac{3}{4}}}{p-q}$ and $|y| \leq \frac{p-q}{\phi(N)N^{\frac{1}{4}}}ex$.

Now we start with the following Lemma.

Lemma 2. *Let $ex + y = m\phi(N)$ for $m > 0$. Then $|\frac{e}{N-\frac{3}{\sqrt{2}}\sqrt{N}+1} - \frac{m}{x}| < \frac{1}{2x^2}$ 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], $\frac{3}{4}\frac{ex}{\phi(N)} \leq m \leq \frac{5}{4}\frac{ex}{\phi(N)}$.

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

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

Now, $\frac{m((\frac{3}{\sqrt{2}}-2)\sqrt{N})+|y|}{x(N-\frac{3}{\sqrt{2}}\sqrt{N}+1)} < \frac{1}{2x^2}$ 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 $\rho q-p$ (as presented in Proposition 2) instead of $p-q$.

Theorem 4. *Let $|\rho q-p|\leq N^{\gamma}$ where $1\leq\rho\leq 2$ and $\gamma\leq\frac{1}{2}$. Suppose e satisfies the equation $ex+y=m\phi(N)$, for $m>0$. Then N can be factored in $O(poly(\log(N)))$ time when $0<x\leq\frac{1}{6}\sqrt{\frac{\phi(N)}{e}}N^{\frac{1-\gamma}{2}}$ and $|y|\leq\frac{|\rho q-p|}{\phi(N)N^{\frac{1}{4}}}ex$.*

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

$$\left|\frac{e}{N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1}-\frac{m}{x}\right|=\frac{|ex-m\left(N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1\right)|}{x\left(N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1\right)}$$

$$=\frac{|m\left((\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}-p-q\right)-y|}{x\left(N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1\right)}\text{ (putting }ex=-y+m\phi(N))$$

$$\leq\frac{|m\left((\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}-p-q\right)|+|y|}{x\left(N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1\right)}$$

$$\leq\frac{\left(\frac{ex}{\phi(N)}(1+\frac{|\rho q-p|}{\phi(N)N^{\frac{1}{4}}})\right)\left((\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}-p-q\right)+\frac{|\rho q-p|}{\phi(N)N^{\frac{1}{4}}}ex}{x\left(N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1\right)}\text{ (putting the upper bound on }m\text{ and using the upper bound of }y)$$

$$=\frac{\left(\frac{e}{\phi(N)}(1+\frac{|\rho q-p|}{\phi(N)N^{\frac{1}{4}}})\right)\left((\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}-p-q\right)+\frac{|\rho q-p|}{\phi(N)N^{\frac{1}{4}}}e}{\left(N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1\right)}$$

$$<\frac{e}{\phi(N)}\frac{2N^{\gamma}+2N^{2\gamma-\frac{5}{4}}+N^{\gamma-\frac{1}{4}}}{N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1}\text{ (Using }|\rho q-p|\leq N^{\gamma}\text{ and }|\sqrt{\rho}+\tfrac{1}{\sqrt{\rho}})\sqrt{N}-p-q|<2N^{\gamma})$$

$$<\frac{e}{\phi(N)}\frac{3N^{\gamma}}{N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1}$$

$$<\frac{e}{\phi(N)}18N^{\gamma-1}(\text{Assume }N-(\sqrt{\rho}+\tfrac{1}{\sqrt{\rho}})\sqrt{N}+1>\tfrac{N}{6}).$$

So we get $\frac{m}{x}$ via CF expansion of $\frac{e}{N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1}$ if

$\frac{e}{\phi(N)}18N^{\gamma-1}<\frac{1}{2x^2}$ i,e. $x<\frac{1}{6}\sqrt{\frac{\phi(N)}{e}}N^{\frac{1-\gamma}{2}}$.

Given, $|\frac{e}{N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1}-\frac{m}{x}|<\frac{1}{2x^2}$, N can be factorized using [2, Algorithm Generalized Wiener Attack II]. □

The result of [2, Theorem 4, Section 4] states that p,q can be found in polynomial time for every N,e satisfying $ex+y\equiv 0 \bmod \phi(N)$, 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 $\rho q - p$ where ρ is known to the attacker. Thus the results of this section present 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 $|\rho q - p|$ is upper bounded.

3.1 A Practical Example and Enumeration of Weak Keys

Example 5. We consider same N (1065-bit integer) as in Example 1 and take $\rho = 2$. Here public exponent e is 1050-bit integer

731660696691222992551774827115980002401699309267481290861785625839815569869904014214507211670878229589357491737767519489224384382491072221346741159263851358208676632050398269179045285578074682025304721268896486630441089024356080939607899405292696883857119393298310114651409619888904078263105602705370785972844688747 5.

Using the convergents of CF expression, we find x as

203703597633448608626844568840937816105146839366593625063614044935438129976333670618339784 6 and m as

655542756589831037023496123946587650092123122293878983335729962117053171156275253612 53.

As, $N + 1 - \frac{ex}{m} = p + q + \frac{y}{m}$, with the knowledge of N, e, x, m one can get a good approximation of $p + q$ when y is in the specified bound (in this case, y is indeed inside the bound having the value $_{4398}$). Then using the idea of [6], the values of factors p, q can be known in $O(poly(\log(N)))$ time.

In this example, d is 1063-bit integer

592946616620725624515194559625566074811072375918567720936334503415197060308735631814452416223275635395917821963407946749576657635610798800949232299425518828784702388418473387340984356269401580701488054997090095217429224985215727140825246462715190439471308096595689959562286727747581108960515329673266149286499656901141 03.

□

Now we like to point out that the weak key of Example 5 is not covered by the works of [23, 25, 2]. In this case, the decryption exponent d is a 320-digit integer ($d > N^{0.99}$) and hence the bound of [23] that $d < \frac{1}{3}N^{\frac{1}{4}}$ will not work here.

Here $p - q > N^{0.49}$ and according to [25, Section 6] one can consider $\beta = 0.49$. If $d = N^{\delta}$, then according to [25, Section 6] the bound of δ will be $2 - 4\beta < \delta < 1 - \sqrt{2\beta - \frac{1}{2}}$ for RSA to be insecure. Putting $\beta = 0.49$, one can get $0.04 < \delta < 0.31$. In Example 5, $d > N^{0.99}$ and hence the weak keys of [25] does not cover our result.

In [2, Theorem 4, Section 4], it has been shown that p, q can be found in polynomial time for every N, e satisfying $ex + y = m\phi(N)$, with $0 < x \leq \frac{1}{3}\sqrt{\frac{\phi(N)}{e}}\frac{N^{\frac{3}{4}}}{p-q}$ and $|y| \leq \frac{p-q}{\phi(N)N^{\frac{1}{4}}}ex$. According to [2], convergents of the CF expression of $\frac{e}{N-\lfloor 2\sqrt{N}\rfloor}$ will provide $\frac{m}{x}$. For the parameters in Example 5, we calculated all the convergents with $x \leq \frac{1}{3}\sqrt{\frac{\phi(N)}{e}}\frac{N^{\frac{3}{4}}}{p-q}$ and we find that for each such m, x, $|ex - m\phi(N)| > \frac{p-q}{\phi(N)N^{\frac{1}{4}}}ex$. As $y = ex - m\phi(N)$, the bound on

$|y|$ is not satisfied. Thus the weak key presented in Example 5 is not covered by the work of [2].

To estimate the number of weak keys, we use the same approach as in [2]. We first 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 $ex + y \equiv 0 \bmod \phi(N)$ 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 $|\rho q - p| = N^{\frac{1}{4}+\gamma_1}$ with $0 < \gamma_1 \leq \frac{1}{4}$. 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 $size_C(N) = \Omega(N^{\frac{3}{4}})$.*

Proof. Here $f(N,e) = \frac{1}{6}\sqrt{\frac{\phi(N)}{e}}\sqrt{\frac{N}{|\rho q - p|}}$, and $g(N,e) = \frac{|\rho q - p|}{\phi(N)N^{\frac{1}{4}}}e$. Clearly $f(N,e) \geq 2$. Also, $f^2(N,e)g(N,e) < \phi(N)$.

Again $g(N,e) \leq f(N,e)$. Hence, we can apply Lemma 1. Since $g(N,e) = \Omega(N_1^{\gamma})$, the term

$$\frac{f^2(N,e)g(N,e)}{8\log\log^2(N^2)}$$

dominates the error term $O(f^2(N,e)N^{\epsilon})$. Using $f^2(N,e)g(N,e) = \Omega(N^{\frac{3}{4}})$, 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 [23], 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., [25, 2]. In this paper we have studied both the upper and lower bounds of $\phi(N)$ carefully and used $N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1$ as an estimate of $\phi(N)$. We extensively study the cases when $\frac{t}{d}$ can be found in the CF expression of $\frac{e}{N-(\sqrt{\rho}+\frac{1}{\sqrt{\rho}})\sqrt{N}+1}$. Our results provide new weak keys over the work of [25, 2] and to the best of our knowledge the weak keys identified in our paper have not been presented earlier.

Acknowledgments: The authors like to thank Prof. Benne de Weger for his detailed comments on an initial version of this paper posted at http://eprint.iacr.org/2008/228 on 11-Jul-2008. Motivated by that, we have introduced the parameter ρ in this paper. Prof. Weger has also pointed out that the parameter τ (in the said version of this paper) cannot be considered small. Based on these, we have modified Theorems 1 and 4 in this version. We also thank the anonymous reviewers of this paper for their comments that improved the technical as well as editorial quality of this paper.

The second author likes to acknowledge the Council of Scientific and Industrial Research (CSIR), India for supporting his research fellowship.

References

1. J. Blömer and A. May. Low secret exponent RSA revisited. CaLC 2001, LNCS 2146, pp. 4–19, 2001.
2. J. Blömer and A. May. A generalized Wiener attack on RSA. PKC 2004, LNCS 2947, pp. 1–13, 2004.
3. D. Boneh. Twenty Years of Attacks on the RSA Cryptosystem. Notices of the AMS, 46(2):203–213, February, 1999.
4. D. Boneh and G. Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. Eurocrypt 1999, LNCS 1592, pp. 1–11, 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 A. 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, LNCS 4622, pp 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. S. Sarkar, S. Maitra and S. Sarkar. RSA Cryptanalysis with Increased Bounds on the Secret Exponent using Less Lattice Dimension. Cryptology ePrint Archive: Report 2008/315, Available at http://eprint.iacr.org/2008/315.
17. R. D. Silverman. Fast generation of random, strong RSA primes. Cryptobytes, 3(1):9–13, 1997.
18. D. R. Stinson. Cryptography – Theory and Practice. 2nd Edition, Chapman & Hall/CRC, 2002.
19. 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.
20. H. -M. Sun and C. -T. Tang. RSA with Balanced Short Exponents and Its Application to Entity Authentication. PKC 2005, LNCS 3386, pp. 199–215, 2005
21. H. -M. Sun, M. -E. Wu and Y. -H. Chen. Estimating the prime-factors of an RSA modulus and an extension of the Wiener attack. ACNS 2007, LNCS 4521, pp. 116–128, 2007.
22. 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.
23. M. Wiener. Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory, 36(3):553–558, 1990.
24. H. C. Williams. A $p + 1$ method of factoring. Mathematics of Computation, 39(159):225–234, July 1982.
25. B. de Weger. Cryptanalysis of RSA with small prime difference. Applicable Algebra in Engineering, Communication and Computing, 13(1):17–28, 2002.