Converse Results to the Wiener Attack on RSA

Ron Steinfeld, Scott Contini, Huaxiong Wang, and Josef Pieprzyk

Dept. of Computing, Macquarie University, North Ryde, Australia
{rons,scontini,hwang,josef}@ics.mq.edu.au
http://www.ics.mq.edu.au/acac/

Abstract. A well-known attack on RSA with low secret-exponent d was given by Wiener about 15 years ago. Wiener showed that using continued fractions, one can efficiently recover the secret-exponent d from the public key (N, e) as long as $d < N^{1/4}$. Interestingly, Wiener stated that his attack may sometimes also work when d is slightly *larger* than $N^{1/4}$. This raises the question of how much larger d can be: could the attack work with non-negligible probability for $d = N^{1/4+\rho}$ for some constant $\rho > 0$? We answer this question in the negative by proving a converse to Wiener's result. Our result shows that, for *any* fixed $\epsilon > 0$ and all sufficiently large modulus lengths, Wiener's attack succeeds with negligible probability over a random choice of $d < N^{\delta}$ (in an interval of size $\Omega(N^{\delta})$) as soon as $\delta > 1/4 + \epsilon$. Thus Wiener's success bound $d < N^{1/4}$ for his algorithm is essentially tight. We also obtain a converse result for a natural class of extensions of the Wiener attack, which are guaranteed to succeed even when $\delta > 1/4$. The known attacks in this class (by Verheul and Van Tilborg and Dujella) run in exponential time, so it is natural to ask whether there exists an attack in this class with subexponential run-time. Our second converse result answers this question also in the negative.

1 Introduction

The RSA public-key cryptosystem is one of the most popular systems in use today. Accordingly, the study of the security of special variants of RSA designed for computational efficiency is a major area of research. One natural RSA variant which is attractive for speeding up secret operations (signature generation or decryption) is *Low Secret-Exponent RSA*. In this variant the RSA secret exponent d is chosen to be small compared to the RSA modulus N. A well-known attack on RSA with low secret-exponent d was given by Wiener[10] about 15 years ago. Wiener showed that using continued fractions, one can efficiently recover the secret-exponent d from the public key (N, e) as long as $d < N^{1/4}$. Interestingly, Wiener stated that his attack may sometimes also work when d is slightly *larger* than $N^{1/4}$. This raises the question of how much larger d can be: could the attack work with non-negligible probability for $d = N^{1/4+\rho}$ for some constant $\rho > 0$?

In this paper, we answer the above question in the negative by proving a converse to Wiener's result. Our result shows that, for *any* fixed $\epsilon > 0$ and all sufficiently large modulus lengths, Wiener's attack succeeds with negligible probability over a random choice of $d < N^{\delta}$ (in an interval of size $\Omega(N^{\delta})$) as soon as $\delta > 1/4 + \epsilon$. Thus Wiener's bound $d < N^{1/4}$ for his attack is essentially tight. We also obtain a converse result for a natural class of extensions of the Wiener attack, which are guaranteed to succeed even when $\delta > 1/4$. The known attacks in this class (by Verheul and Van Tilborg [8] and Dujella [3]) run in exponential time, so it is natural to ask whether there exists an attack in this class with subexponential run-time. Our second converse result answers this question also in the negative.

Related Work. To our knowledge, the converse results in this paper provide the first *proven* evidence for the limitations of the Wiener attack [10] and its extensions by Verheul and Van Tilborg [8] and Duejlla [3]. Essentially, our results prove that when $\delta > 1/4$, the linear equation (satisfied by the secret key) which is exploited by the Wiener attack cannot lead by itself to a key-recovery attack which runs in subexponential time (because there are too many solutions). In order to obtain a subexponential attack when $\delta > 1/4$ one must exploit some other property of the secret key. Indeed, the lattice-based Boneh-Durfee attack [2] and its variant given by Blömer and May [1], exploit a non-linear equation satisfied by the secret key, which gives an attack that heuristically succeeds in polynomial-time when $\delta < 0.292$. Finding proven limitations on the Boneh-Durfee attack and its variants is currently an open problem, but we believe our results on provable limitations of the Wiener attack are a first step in this direction.

Organization of This Paper. Section 2 presents definitions and known results from number theory that we use. In Section 3, we define the standard RSA key-generation algorithm that our results apply to and review Wiener's result. In Section 4, we state and prove our converse to Wiener's result. In Section 5, we present our generalized converse result which applies to a natural class of extensions of the Wiener attack. Section 6 concludes the paper.

2 Preliminaries

2.1 Continued Fractions

Here we collect several known results that we use about continued fractions, which can be found in [5, 6].

For positive integers $a_1, \ldots, a_n$, we define the rational number

$$x \stackrel{\text{def}}{=} \frac{1}{a_1 + \frac{1}{a_2 + \ldots + \frac{1}{a_n}}}.$$

For brevity, we write $x = (a_1, a_2, \ldots, a_n)$, and we call the sequence $(a_1, \ldots, a_n)$ a *continued fraction expansion of length* n *for* x.

Theorem 1 (Continued Fractions). *Let* $x = \frac{r}{s}$ *for positive integers* r, s *with* $\gcd(r, s) = 1$ *and* $r < s$. *Then the rational* x *has a* unique *continued fraction expansion* $x = (a_1, \ldots, a_n)$ *with* $a_n > 1$, *which can be computed in time* $O(\log^2 s)$ *by the following algorithm:*

1. *Initialize* $x_0 = x$.
2. *Compute iteratively* $x_i = \frac{1}{x_{i-1} - \lfloor x_{i-1} \rfloor}$ *for* $i = 1, \ldots, n$, *where* $n \leq 2\log(s)$ *is the smallest value of* i *such that* $\lfloor x_i \rfloor = x_i$.
3. *Return* $(a_1, \ldots, a_n)$, *where* $a_i = \lfloor x_i \rfloor$ *for* $i = 1, \ldots, n$.

Let $(a_1, \ldots, a_n)$ denote the continued fraction expansion of rational x. For $i = 1, \ldots, n$, the rationals $y_i = \frac{r_i}{s_i} \stackrel{\text{def}}{=} (a_1, \ldots, a_i)$ are called the *convergents* of (the continued fraction expansion for) x. The convergents y_i to x become successively closer to x with increasing index i until the last convergent y_n which is equal to x.

Theorem 2 (Convergents). *Let* $y_1, \ldots, y_n$ *denote the convergents of a rational* $x = \frac{r}{s}$ *for positive integers* r, s *with* $\gcd(r, s) = 1$ *and* $r < s$. *For* $i = 1, \ldots, n-1$, *let us write* $y_i = \frac{r_i}{s_i}$ *for integers* r_i, s_i *with* $\gcd(r_i, s_i) = 1$. *Then the following statements hold:*

(1) *For* $i \in \{1, \ldots, n-1\}$, $y_i = \frac{r_i}{s_i}$ *is a* best approximation *to* x *in the sense that* $|s_i \cdot x - r_i| < |s' \cdot x - r'|$ *for all* r', s' *such that* $0 < s' \leq s_i$ *and* $\frac{r'}{s'} \neq y_i$ *(note: this implies that* $|\frac{r_i}{s_i} - x| < |\frac{r'}{s'} - x|$ *for all* r', s' *such that* $0 < s' \leq s_i$ *and* $\frac{r'}{s'} \neq y_i$*).*
(2) *For* $i \in \{1, \ldots, n-1\}$, $|\frac{r_i}{s_i} - x| < \frac{1}{s_i^2}$ *and* $s_{i+1} \geq 2s_i$.
(3) *Let* $y = \frac{\widehat{r}}{\widehat{s}}$ *be any rational such that* $|\frac{\widehat{r}}{\widehat{s}} - x| < \frac{1}{2\widehat{s}^2}$. *Then* y *is equal to one of the convergents of* x, *i.e.* $y = y_i$ *for some* $i \in \{1, \ldots, n\}$.

3 Review of Wiener's Attack

3.1 The RSA Key-Generation Algorithm

In this paper we assume the following natural key-generation algorithm $\mathsf{RSAKG}_{\delta,\beta_1,\beta_2}(\ell)$ for RSA, which would typically be used when the goal is to produce a modulus N in the order of 2^ℓ and a secret exponent d in the order of N^δ for some fixed $0 < \delta \leq 1$. The fixed real-valued parameters $\beta_1 > 0$ and $\beta_2 > 0$ control the size of the intervals from which the prime factors of N and the secret exponent d are chosen from (typically, we set $\beta_1 = \beta_2 = 1$, to fix a certain bit-length for p, q and d).

All the probabilities computed in this paper are evaluated over the random choices of algorithm $\mathsf{RSAKG}_{\delta,\beta_1,\beta_2}(\ell)$.

$\mathsf{RSAKG}_{\delta,\beta_1,\beta_2}(\ell)$: **RSA Key-Generation Algorithm**

1 Pick uniformly at random a prime $p \in \mathcal{P}_{\ell/2,\beta_1}$ (Here $\mathcal{P}_{\ell/2,\beta_1}$ denotes the set of all primes in the interval $[2^{\ell/2-\beta_1}, 2^{\ell/2}]$ and typically we set $\beta_1 = 1$).
2 Pick uniformly at random a prime $q \in \mathcal{P}_{\ell/2,\beta_1}$.

3 Compute integers $N = pq$ and $\phi = (p-1)(q-1)$.
4 Pick uniformly at random a secret exponent $d \in \mathcal{D}_{\ell,\delta,\beta_2}(\phi)$ (Here $\mathcal{D}_{\ell,\delta,\beta_1}(\phi)$ denotes the set of all integers in the interval $[2^{\delta\cdot\ell-\beta_2}, 2^{\delta\cdot\ell}]$ which are coprime to ϕ, and typically we set $\beta_2 = 1$).
5 Compute $e = d^{-1} \bmod \phi$ (note: this implicitly defines the integer $k = (ed-1)/\phi$).
6 Return secret-exponent d and public key (N, e).

3.2 Wiener's Attack

The idea behind Wiener's attack on RSA with small secret-exponent d is that for small d, the publicly known fraction e/N is a very good approximation to the secret fraction k/d (here $k = (ed-1)/\phi$), and hence k/d can be found from the convergents of the continued-fraction expansion of e/N, using the results of Section 2.1.

$\mathsf{WienAtk}(N, e)$: Wiener Attack Algorithm

1 Compute the continued fraction convergents $\left(\frac{k_1}{d_1}, \ldots, \frac{k_n}{d_n}\right)$ of $\frac{e}{N}$ using the algorithm of Theorem 1.
2 Return $\left(\frac{k_1}{d_1}, \ldots, \frac{k_n}{d_n}\right)$.

We say that algorithm WienAtk *succeeds* on input (N, e) if it outputs $\left(\frac{k_1}{d_1}, \ldots, \frac{k_n}{d_n}\right)$ with $\frac{k_i}{d_i} = \frac{k}{d}$ for some $i \in \{1, \ldots, n\}$ (where $d = e^{-1} \bmod \phi$ and $k = (ed-1)/\phi$).

To obtain Wiener's sufficient condition for the success of algorithm WienAtk, we observe that, from the equation $ed - 1 = k\phi$ it follows that the approximation error of k/d by e/N is given by:

$$\frac{k}{d} - \frac{e}{N} = e \cdot \left(\frac{1}{\phi} - \frac{1}{N}\right) - \frac{1}{\phi \cdot d} \tag{1}$$

$$= e \cdot \left(\frac{1}{N-s} - \frac{1}{N}\right) - \frac{1}{(N-s)\cdot d} \text{ where } s = p+q-1 \tag{2}$$

$$= \left(\frac{s}{N-s}\right)\left(\frac{e}{N} - \frac{1}{d \cdot s}\right) \tag{3}$$

$$< \frac{s}{N-s} < \frac{2^{2\beta_1+1}}{2^{\ell/2}}. \tag{4}$$

The last bound uses the fact that $s < 2^{\ell/2+1}$ since p and q are not even. Note also that $\frac{k}{d} - \frac{e}{N} > 0$.

From Theorem 2 part (3), we know that k/d will be one of the convergents of the continued fraction expansion of e/N if $\frac{k}{d} - \frac{e}{N} < \frac{1}{2d^2}$. Using the above bound on $\frac{k}{d} - \frac{e}{N}$ and the fact that $d < 2^{\delta\cdot\ell}$, we conclude that a sufficient condition for success of algorithm WienAtk is that $\frac{2^{2\beta_1+1}}{2^{\ell/2}} < \frac{1}{2^{2\delta\cdot\ell+1}}$. This immediately gives us the following result due to Wiener [10].

Theorem 3 (WienAtk **Sufficient Condition).** *Suppose that the key-generation parameters* $(\delta, \beta_1, \beta_2, \ell)$ *satisfy the condition*

$$\delta < 1/4 - \frac{\beta_1 + 1}{\ell}.$$

Then on input (N, e)*, where* $(N, e, d) = \mathsf{RSAKG}_{\delta,\beta_1,\beta_2}(\ell)$*, the Wiener attack algorithm* WienAtk *succeeds with probability 1.*

4 A Converse to Wiener's Result

The following statement is our *necessary* condition for success of Wiener's algorithm. It shows that whenever δ exceeds the Wiener sufficiency threshold $1/4$ by any positive constant ϵ, the Wiener attack algorithm succeeds with negligible probability $2^{-c\cdot\ell}$ for some constant $c > 0$.

Theorem 4 (WienAtk **Necessary Condition).** *Fix positive constants* $0 < \epsilon < 3/4$*,* β_1 *and* β_2*, and suppose that the key-generation parameter* δ *satisfies the condition*

$$\delta = 1/4 + \epsilon.$$

Then there exist positive constants c *and* ℓ_0 *(depending on* ϵ*,*β_1 *and* β_2*) such that on input* (N, e)*, where* $(N, e, d) = \mathsf{RSAKG}_{\delta,\beta_1,\beta_2}(\ell)$*, the Wiener attack algorithm* WienAtk *succeeds with probability at most* $2^{-c\cdot\ell}$ *for all* $\ell \geq \ell_0$*.*

Proof. By definition, if WienAtk succeeds on input (N, e), then one of the convergents $\left(\frac{k_1}{d_1}, \ldots, \frac{k_n}{d_n}\right)$ of $\frac{e}{N}$ is equal to $\frac{k}{d}$. But by Theorem 2 part (2), it follows that $\frac{k}{d} - \frac{e}{N} < \frac{1}{d^2}$. Using $d > 2^{\delta\cdot\ell-\beta_2}$ and $\delta = 1/4 + \epsilon$, we obtain the necessary success condition

$$\frac{k}{d} - \frac{e}{N} < 2^{2\beta_2-(1/2+2\epsilon)\cdot\ell}. \tag{5}$$

We now show that, for any $\epsilon > 0$, the probability that (5) holds is negligible over the random choice of $d \in \mathcal{D}_{\ell,\delta,\beta_2}(\phi)$. We first reduce the problem to upper bounding the probability that $\frac{e}{N}$ is negligibly small.

Lemma 1. *Fix positive constants* c_1 *and* η_1*. Then there exist positive constants* c_2 *and* η_2 *such that*

$$\Pr\left[\frac{k}{d} - \frac{e}{N} < c_1 \cdot 2^{-(1/2+\eta_1)\cdot\ell}\right] \leq \Pr\left[\frac{e}{N} < c_2 \cdot 2^{-\eta_2\cdot\ell}\right].$$

Proof. Let $\Delta = \frac{k}{d} - \frac{e}{N}$. From (3) in Section 3.2 we have $\Delta = \left(\frac{s}{N-s}\right) \cdot \left(\frac{e}{N} - \frac{1}{d\cdot s}\right)$, and using $s = p+q-1 > N^{1/2}$ we get $\Delta > N^{-1/2} \cdot \left(\frac{e}{N} - \frac{1}{dN^{1/2}}\right)$. Using $d > 2^{\delta\cdot\ell-\beta_2}$ and $N > 2^{\ell-2\beta_1}$ we get $\Delta > N^{-1/2} \cdot \left(\frac{e}{N} - 2^{\beta_1+\beta_2-(1/2+\delta)\cdot\ell}\right)$, and then using

$N < 2^\ell$ we get $\Delta > 2^{-\ell/2} \cdot \left(\frac{e}{N} - 2^{\beta_1+\beta_2-(1/2+\delta)\cdot\ell}\right)$. Let $C = 2^{\beta_1+\beta_2-(1/2+\delta)\cdot\ell}$. Then we have

$$\begin{aligned}\Pr\left[\Delta < c_1 \cdot 2^{-(1/2+\eta_1)\cdot\ell}\right] &\le \Pr\left[2^{-\ell/2} \cdot \left(\frac{e}{N} - C\right) < c_1 \cdot 2^{-(1/2+\eta_1)\cdot\ell}\right] \\ &= \Pr\left[\frac{e}{N} < c_1 \cdot 2^{-\eta_1\cdot\ell} + C\right] \\ &\le \Pr\left[\frac{e}{N} < c_2 \cdot 2^{-\eta_2\cdot\ell}\right],\end{aligned}$$

for positive constants $c_2 = 2\max(c_1, 2^{\beta+1+\beta_2})$ and $\eta_2 = \min(\eta_1, 1/2+\delta)$, as claimed. □

To bound $\Pr\left[\frac{e}{N} < c_2 \cdot 2^{-\eta_2\cdot\ell}\right]$, we need an upper bound on the number of $d \in \mathcal{D}_{\ell,\delta,\beta_2}(\phi)$ such that $\frac{e}{N} < c_2 \cdot 2^{-\eta_2\cdot\ell}$ holds, and a lower bound on the total size of the set $\mathcal{D}_{\ell,\delta,\beta_2}(\phi)$. These bounds are provided by the following two counting results.

Lemma 2. *Fix positive constants c_1, c_2 and δ. The size of the set M of secret-exponents $d < 2^{\delta\cdot\ell}$ such that the corresponding public exponent $e = d^{-1} \bmod \phi$ satisfies $\frac{e}{N} < c_1 \cdot 2^{-c_2\cdot\ell}$ is bounded as follows:*

$$\#M = O\left(2^{\left(\delta - c_2 + \frac{c_3}{\log \ell}\right)\cdot\ell}\right),$$

with constant $c_3 = 2(1+\delta)$.

Proof. For each $d \in M$, we have $e \cdot d = 1 + k \cdot \phi$ for some positive integer k, where $k < \frac{ed}{\phi} = O\left(2^{(\delta-c_2)\cdot\ell}\right)$ using the fact that $N/\phi = O(1)$. So, to get an upper bound on the number of (e,d) pairs, we only need to consider the possibilities for k, from 1 up to some integer $K = O\left(2^{(\delta-c_2)\cdot\ell}\right)$.

For each $k \in \{1, \ldots, K\}$, let $m = 1 + k\cdot\phi = O\left(2^{(1+\delta-c_2)\cdot\ell}\right)$. The possible (e,d) pairs for this k correspond to factorizations of m as a product of two integers. The number of such factorizations is equal to $\tau(m)$, the number of divisors of m. It is known (see Theorem 317 of [4]) that $\tau(m) = O\left(2^{\frac{2\log m}{\log\log m}}\right)$, and using the bounds $m = O(k \cdot \phi) = O\left(2^{(1+\delta)\cdot\ell}\right)$ and $m = \Omega(N) = \Omega\left(2^\ell\right)$ we conclude that $\tau(m) = O\left(2^{\frac{2(1+\delta)}{\log \ell}\cdot\ell}\right)$.

Thus the total number of possible (e,d) pairs satisfying the required conditions is bounded as $\#M = O\left(K \cdot \tau(m)\right) = O\left(2^{\left(\delta - c_2 + \frac{c_3}{\log \ell}\right)\cdot\ell}\right)$ where $c_3 = 2(1+\delta)$, as required. □

Lemma 3. *Fix positive constants β_1, β_2 and δ. The size of the set $\mathcal{D}_{\ell,\delta,\beta_1}(\phi)$ of all integers in the interval $[2^{\delta\cdot\ell-\beta_2}, 2^{\delta\cdot\ell}]$ which are coprime to ϕ is lower bounded as follows:*

$$\#\mathcal{D}_{\ell,\delta,\beta_1}(\phi) = \Omega\left(2^{\left(\delta - \frac{\log\log \ell}{\ell}\right)\cdot\ell}\right).$$

Proof. For an integer $d \geq 1$, we denote by $\mu(m)$ the Möbius function. We recall that $\mu(1) = 1$, $\mu(d) = 0$ if $d \geq 2$ is not square-free and $\mu(d) = (-1)^{\omega(d)}$ otherwise, where for integer d we denote by $\omega(d)$ the number of distinct prime factors of d.

Fix any integers $m, J \geq 1$. Using the Möbius function $\mu(d)$ over the divisors of q to detect the co-primality condition (see Section 3.d of Chapter 2 of [9]) and interchanging the order of summation, we obtain the Legendre formula

$$\sum_{\substack{j=1 \\ \gcd(j,m)=1}}^{J} 1 = \sum_{d|m} \mu(d) \left\lfloor \frac{J}{d} \right\rfloor = J \sum_{d|m} \frac{\mu(d)}{d} + O\left(\sum_{d|m} |\mu(d)| \right). \tag{6}$$

Observe that

$$\sum_{d|m} |\mu(d)| = \sum_{k=0}^{\omega(m)} |(-1)^k| \binom{\omega(m)}{k} = 2^{\omega(m)},$$

and recall that the Möbius function satisfies

$$\sum_{d|m} \frac{\mu(d)}{d} = \frac{\varphi(m)}{m},$$

where $\varphi(m)$ denotes Euler's phi function evaluated at m. So, for any integers $J_{max} > J_{min} \geq 1$, applying (6) to both intervals $[1, \ldots, J_{min}]$ and $[1, \ldots, J_{max}]$ and subtracting gives us

$$\sum_{\substack{J_{min} \leq j \leq J_{max} \\ \gcd(j,m)=1}} 1 = \frac{\varphi(m)}{m}(J_{max} - J_{min}) + O(2^{\omega(m)}).$$

But $2^{\omega(m)}$ is the number of square-free divisors of m, which is upper bounded by the total number $\tau(m)$ of divisors of m. It is known (see Theorem 317 of [4]) that $\tau(m) = O\left(2^{\frac{2\log m}{\log\log m}}\right)$. Setting $m = \phi$, $J_{min} = 2^{\delta \cdot \ell}/2^{\beta_2}$ and $J_{max} = 2^{\delta \cdot \ell}$, we get

$$\#\mathcal{D}_{\ell,\delta,\beta_2}(\phi) = \Omega\left(\frac{\varphi(\phi)}{\phi} \cdot 2^{\delta \cdot \ell} \right) + O\left(2^{\frac{2\log\phi}{\log\log\phi}} \right). \tag{7}$$

We now observe that $\phi = \Theta(2^\ell)$ so $2^{\frac{2\log\phi}{\log\log\phi}} = O\left(2^{\frac{c_5 \ell}{\log \ell}}\right)$ for some positive constant c_5. Furthermore, it is known [7] that $\frac{\phi}{\varphi(\phi)} = O(\log\log\phi) = O(2^{\log\log\ell})$. Plugging these results in (7) and using the fact that $2^{\frac{c_5\ell}{\log\ell}} = o\left(2^{\delta\cdot\ell - \log\log\ell}\right)$ we obtain the claimed result $\#M = \Omega\left(2^{\left(\delta - \frac{\log\log\ell}{\ell}\right)\cdot\ell}\right)$. $\square$

Using Lemma 1 and the fact that d is chosen uniformly at random from the set $\mathcal{D}_{\ell,\delta,\beta_2}(\phi)$, we conclude that WienAtk's success probability p is upper bounded as $p \leq \frac{\#M}{\#\mathcal{D}_{\ell,\delta,\beta_2}(\phi)}$, where M denotes the set of all secret-exponents $d < 2^{\delta\cdot\ell}$ such that the corresponding public exponent $e = d^{-1} \bmod \phi$ satisfies $\frac{e}{N} < c_2 \cdot 2^{-\eta_2\cdot\ell}$. Taking the ratio of the bounds on $\#M$ and $\#\mathcal{D}_{\ell,\delta,\beta_2}(\phi)$ from

Lemma 2 and Lemma 3, we have that $p = O\left(2^{-\left(\eta_2 - \frac{c_3}{\log \ell} - \frac{\log\log \ell}{\ell}\right)\cdot \ell}\right)$ for some positive constants η_2 and c_3. It follows that there exists a constant ℓ_0 such that $p \leq 2^{-c\cdot\ell}$ for all $\ell \geq \ell_0$, where $c = \eta_2/2 > 0$. This completes the proof of the theorem. $\square$

5 A Converse Result for Improved Variants of Wiener Attack

Since Wiener's attack fails as soon as $\delta > 1/4$, it is natural to investigate improved variants of the Wiener attack which may succeed even in this case. In particular, Verheul and Van Tilborg (VVT) [8], and more recently Dujella [3], presented improved variants of Wiener's attack which are guaranteed to succeed even when $\delta > 1/4$. However, the run-time of these attacks when $\delta = 1/4+\epsilon$ (for some positive constant ϵ) is exponential in $\epsilon \cdot \ell$, so these attacks are asymptotically slower than the generic attack of factoring the RSA modulus, which runs in *subexponential* time. As we explain below, both the VVT and Dujella attacks can be viewed as members of a natural class of extensions of the Wiener attack (which are all guaranteed to succeed when $\delta > 1/4$), which we call the *Wiener Search Variant* (WSV) class of attacks (essentially, a WSV attack searches an interval near the known fraction e/N for the secret fraction k/d — see below for a precise definition). It is interesting to ask whether one can substantially improve on the VVT and Dujella attacks — in particular: does there exist an attack in the WSV class which has *subexponential* run-time? In this section, we answer this question in the negative by proving the following 'converse' result: For any attack algorithm in the WSV class and any subexponential run-time bound T, the probability (over the random choices of the key generation algorithm RSAKG) that the attack halts with success after a run-time less than T is negligible whenever $\delta = 1/4 + \epsilon$ for any constant $\epsilon > 0$. Thus there are no WSV attacks which are asymptotically faster than factoring (and hence the VVT and Dujella attacks are optimal in the sense that all WSV attacks must have at least exponential run-time).

The Wiener Search Variant (WSV) Attack Class. Recall that the central idea behind Wiener's attack is that the public fraction e/N is a good approximation to the secret fraction k/d. Indeed, when $\delta < 1/4-\epsilon$, k/d is the *best* approximation to e/N among all fractions with denominator at most d (see Theorem 2), and Wiener's continued fractions attack efficiently finds this best approximation. Our converse result in the previous section shows that when $\delta > 1/4$, k/d is likely to no longer be the *best* approximation to e/N in the set of all fractions with denominator at most d, but it is still likely to be a good approximation. So, a natural extension of the Wiener attack is to search through the set of fractions with denominator less than $2^{\delta\cdot\ell}$ (and greater than $2^{\delta\cdot\ell-\beta_2}$) in an interval close to e/N, until k/d is found. This leads to the following definition.

Definition 1 (Wiener Search Variant Attack Class – WSV). *An attack algorithm $\mathsf{A}_{\delta,\beta_2,\ell}$ is said to belong to the* Wiener Search Variant *(WSV) attack class if it has the following form.*

$\mathsf{A}_{\delta,\beta_2,\ell}(N,e)$**: WSV Attack Algorithm**

1 *Enumerate a set $S(N,e)$ of approximations to $\frac{k}{d}$, where $S(N,e)$ is guaranteed to contain the set $\widehat{S}(N,e)$ of all fractions $\frac{k'}{d'}$ in the interval $[\frac{e}{N},\frac{k}{d}]$ with denominator $d' \in [2^{\delta\cdot\ell-\beta_2}, 2^{\delta\cdot\ell}]$.*
2 *Return a list containing all elements of the set $S(N,e)$.*

We note that the above definition gives rise to a class of attacks, since it allows any choice for the set $S(N,e)$ (subject to the constraint that $S(N,e)$ contains $\widehat{S}(N,e)$). As in the case of the original Wiener attack, we say that a WSV attack *succeeds* if it outputs a set of approximations $S(N,e)$ which contains the desired secret fraction k/d. From the definition, it is in fact clear that any WSV attack succeeds with probability 1 because of the requirement that $S(N,e) \supseteq \widehat{S}(N,e)$ and the fact that $k/d \in \widehat{S}(N,e)$. The central question is, therefore, how large is the running-time of the attack for $\delta = 1/4+\epsilon$. The running-time depends on the size of the set $S(N,e)$ output by the attack, and on the efficiency by which the elements of $S(N,e)$ are enumerated.

Known WSV Attacks. The VVT [8] and Dujella [3] attacks are both members of the WSV class. Let $\delta = 1/4+\epsilon$ with $\epsilon > 0$. In the VVT attack [8], it is shown, using continued fraction techniques, how to enumerate a set of approximations $S_{VVT}(N,e)$ (containing $\widehat{S}(N,e)$ as defined in Def. 1) of size $\#S_{VVT}(N,e) = O(A^2 \cdot 2^{2\epsilon\cdot\ell})$ in time $T_{VVT} = O(\ell^2 \#S_{VVT}(N,e))$, where the integer A is proportional to certain coefficients in the continued fraction expansion of e/N and heuristically expected to be small with high probability. The Dujella attack [3] improves on the VVT attack by using results from diophantine approximation to enumerate a smaller set $\#S_{Duj}(N,e)$ (containing $\widehat{S}(N,e)$) of size $\#S_{Duj}(N,e) = O(\log(A)\cdot 2^{2\epsilon\cdot\ell})$ in time $T_{Duj} = O(\ell^2\#S_{Duj}(N,e))$, where the integer A is the same as in the VVT attack. Moreover, Dujella proves that $\#S_{Duj}(N,e) = O(\ell \cdot 2^{2\epsilon\cdot\ell})$.

Our Result: A Lower Bound on WSV Attack Running-Time. The known WSV attacks have exponential run-times for $\delta = 1/4+\epsilon$ with $\epsilon > 0$. We now address the following question: Does there exist a WSV attack with *subexponential* run-time for $\delta = 1/4+\epsilon$? The following result shows that the answer is no. Therefore, the WSV class does not contain an attack faster than factoring.

Theorem 5 (WSV Attack Lower Bound). *Let $\mathsf{A}_{\delta,\beta_2,\ell}$ denote any 'Wiener Search Variant' (WSV) attack algorithm (see Def. 1). Let $T(\ell) = 2^{g(\ell)}$ denote any subexponential function, where $g(\ell) = o(\ell)$. Fix positive constants $0 < \epsilon < 3/4$, β_1 and β_2, and suppose that the key-generation parameter δ satisfies the condition*

$$\delta = 1/4 + \epsilon.$$

Then there exist positive constants c and ℓ_0 (depending on ϵ,β_1, β_2 and $g(\ell)$) such that on input (N,e), where $(N,e,d) = \mathsf{RSAKG}_{\delta,\beta_1,\beta_2}(\ell)$, the running-time of the WSV attack algorithm $\mathsf{A}_{\delta,\beta_2,\ell}$ is less than $T(\ell)$ with probability at most $2^{-c\cdot\ell}$ for all $\ell \geq \ell_0$.

Proof. The set $S(N,e)$ output by $\mathsf{A}_{\delta,\beta_2,\ell}$ is guaranteed by Def. 1 to contain the set $\widehat{S}(N,e)$, where

$$\widehat{S}(N,e) = (\mathcal{F}_{2^{\delta\cdot\ell}} \setminus \mathcal{F}_{2^{\delta\cdot\ell-\beta_2}}) \cap [\frac{e}{N}, \frac{k}{d}],$$

and for any $m > 0$, we denote by $\mathcal{F}_m$ the *Farey set of order* m which consists of all rational numbers k'/d' with $k', d' \in \mathbb{Z}$, $0 < d' \leq m$ and $0 \leq k' < d'$. So the running-time T_A of $\mathsf{A}_{\delta,\beta_2,\ell}$ on input (N,e) is certainly lower bounded as $T_A = \Omega(\#\widehat{S}(N,e))$. To prove the theorem, it therefore suffices to show that for any subexponential bound $T = 2^{g(\ell)}$ with $g(\ell) = o(\ell)$, there exist positive constants c and ℓ_0 such that

$$\Pr[\#\widehat{S}(N,e) < T] \leq 2^{-c\cdot\ell} \text{ for all } \ell \geq \ell_0. \tag{8}$$

We will first reduce this problem to several simpler problems. To do so, we introduce the following definitions. For an element $\frac{k'}{d'} \in \mathcal{F}_{2^{\delta\cdot\ell}} \setminus \mathcal{F}_{2^{\delta\cdot\ell-\beta_2}}$, we denote by $A^-_{\delta,\beta_2,\ell}(\frac{k'}{d'})$ the *adjacent* element of $\frac{k'}{d'}$ in $\mathcal{F}_{2^{\delta\cdot\ell}} \setminus \mathcal{F}_{2^{\delta\cdot\ell-\beta_2}}$ in the '$-$' direction, i.e. the largest element of $\mathcal{F}_{2^{\delta\cdot\ell}} \setminus \mathcal{F}_{2^{\delta\cdot\ell-\beta_2}}$ which is strictly less than $\frac{k'}{d'}$. We will be interested in elements $\frac{k'}{d'}$ for which the gap $\frac{k'}{d'} - A^-_{\delta,\beta_2,\ell}(\frac{k'}{d'})$ is 'large'. Accordingly, for positive $\widehat{\Delta}$, let $\widehat{S}^*_{\delta,\beta_2,\ell}(\widehat{\Delta})$ denote the set of all elements $\frac{k'}{d'}$ in $\mathcal{F}_{2^{\delta\cdot\ell}} \setminus \mathcal{F}_{2^{\delta\cdot\ell-\beta_2}}$ such that $\frac{k'}{d'} - A^-_{\delta,\beta_2,\ell}(\frac{k'}{d'}) \geq \widehat{\Delta}$.

We now have the following result.

Lemma 4. *For any $\Delta_{min} > 0$, we have*

$$\Pr[\#\widehat{S}(N,e) < T] \leq T \cdot \#\widehat{S}^*_{\delta,\beta_2,\ell}\left(\frac{\Delta_{min}}{T}\right) \cdot p^* + \Pr\left[\frac{k}{d} - \frac{e}{N} < \Delta_{min}\right], \tag{9}$$

where

$$p^* = \max_{\frac{k'}{d'} \in \mathcal{F}_{2^{\delta\cdot\ell}} \setminus \mathcal{F}_{2^{\delta\cdot\ell-\beta_2}}} \left(\Pr\left[\frac{k}{d} = \frac{k'}{d'}\right]\right).$$

Proof. For a positive integer i, let $\frac{k_i}{d_i}$ denote the ith closest element in $\mathcal{F}_{2^{\delta\cdot\ell}} \setminus \mathcal{F}_{2^{\delta\cdot\ell-\beta_2}}$ to $\frac{k}{d}$ in the '$-$' direction (if i exceeds the number of elements of $\mathcal{F}_{2^{\delta\cdot\ell}} \setminus \mathcal{F}_{2^{\delta\cdot\ell-\beta_2}}$ which are less than $\frac{k}{d}$ then we define $\frac{k_i}{d_i} = 0$). Also, we define $\frac{k_0}{d_0} = \frac{k}{d}$. Then $\#\widehat{S}(N,e) < T$ implies that $\frac{k}{d} - \frac{k_T}{d_T} > \Delta$, where $\Delta = \frac{k}{d} - \frac{e}{N}$, and hence that

$$\sum_{r=0}^{T-1} \left(\frac{k_r}{d_r} - A^-_{\delta,\beta_2,\ell}\left(\frac{k_r}{d_r}\right)\right) > \Delta.$$

It follows that there exists $r^* \in \{0, \ldots, T-1\}$ such that $\frac{k_{r^*}}{d_{r^*}} - A^-_{\delta,\beta_2,\ell}(\frac{k_{r^*}}{d_{r^*}}) > \frac{\Delta}{T}$. So, for any $\Delta_{min} > 0$:

$$\Pr[\#\widehat{S}(N,e) < T] \leq \Pr\left[\exists r^* < T : \frac{k_{r^*}}{d_{r^*}} - A^-_{\delta,\beta_2,\ell}\left(\frac{k_{r^*}}{d_{r^*}}\right) > \frac{\Delta}{T}\right]$$

$$= \Pr\left[\left(\exists r^* < T : \frac{k_{r^*}}{d_{r^*}} - A^-_{\delta,\beta_2,\ell}\left(\frac{k_{r^*}}{d_{r^*}}\right) > \frac{\Delta}{T}\right) \text{ and } \Delta \geq \Delta_{min}\right]$$
$$+ \Pr\left[\left(\exists r^* < T : \frac{k_{r^*}}{d_{r^*}} - A^-_{\delta,\beta_2,\ell}\left(\frac{k_{r^*}}{d_{r^*}}\right) > \frac{\Delta}{T}\right) \text{ and } \Delta < \Delta_{min}\right]$$
$$\leq \Pr\left[\exists r^* < T : \frac{k_{r^*}}{d_{r^*}} - A^-_{\delta,\beta_2,\ell}\left(\frac{k_{r^*}}{d_{r^*}}\right) > \frac{\Delta_{min}}{T}\right] + \Pr[\Delta < \Delta_{min}]$$
$$\leq \left(\sum_{r=0}^{T-1} p_r\right) + \Pr[\Delta < \Delta_{min}], \tag{10}$$

where, for each $r \in \{0, \ldots, T-1\}$,

$$p_r = \Pr\left[\frac{k_r}{d_r} - A^-_{\delta,\beta_2,\ell}\left(\frac{k_r}{d_r}\right) > \frac{\Delta_{min}}{T}\right]$$
$$= \Pr\left[\frac{k_r}{d_r} \in \widehat{S}^*_{\delta,\beta_2,\ell}(\Delta_{min}/T)\right] \tag{11}$$
$$\leq \#\widehat{S}^*_{\delta,\beta_2,\ell}(\Delta_{min}/T) \cdot p^*_r, \tag{12}$$

and

$$p^*_r = \max_{\frac{k'}{d'} \in \widehat{S}^*_{\delta,\beta_2,\ell}(\Delta_{min}/T)} \left(\Pr\left[\frac{k_r}{d_r} = \frac{k'}{d'}\right]\right)$$
$$\leq \max_{\frac{k'}{d'} \in \mathcal{F}_{2^{\delta\cdot\ell}} \setminus \mathcal{F}_{2^{\delta\cdot\ell-\beta_2}}} \left(\Pr\left[\frac{k}{d} = \frac{k'}{d'}\right]\right) = p^* \text{ for all } r, \tag{13}$$

where the last inequality follows because the probability that $\frac{k_r}{d_r} = \frac{k'}{d'}$ is equal to the probability that $\frac{k}{d}$ coincides with the rth closest element in $\mathcal{F}_{2^{\delta\cdot\ell}} \setminus \mathcal{F}_{2^{\delta\cdot\ell-\beta_2}}$ to $\frac{k'}{d'}$ in the '+' direction.

Plugging (13) into (12) and the result into (10), the claimed bound on $\Pr[\#\widehat{S}(N,e) < T]$ follows immediately. □

Let us now apply Lemma 4 with the parameter $\Delta_{min} = 2^{-(1/2+\eta_2)\cdot\ell}$ for some positive constant η_2 such that $\eta_2 < 2\cdot\epsilon$ (recall that $\delta = 1/4+\epsilon$), and upper bound each of the terms on the right-hand side of (9). First, combining Lemmas 1, 2 and 3 from the proof of Theorem 4, we conclude that there exists a positive constant c_3 such that

$$\Pr\left[\frac{k}{d} - \frac{e}{N} < \Delta_{min}\right] = O\left(2^{-c_3\cdot\ell}\right). \tag{14}$$

Next, we upper bound $\#\widehat{S}^*_{\delta,\beta_2,\ell}\left(\frac{\Delta_{min}}{T}\right)$. Let us define $n = 2^{\delta\cdot\ell} = 2^{(1/4+\epsilon)\cdot\ell}$. Then we have, using $T = 2^{g(\ell)}$ with $g(\ell)/\ell = o(1)$, that there exist positive constants $\widehat{\epsilon}$ and $\widehat{\ell}_0$ such that

$$\frac{\Delta_{min}}{T} = \frac{1}{2^{(\eta_2+g(\ell)/\ell)\cdot\ell} \cdot 2^{\ell/2}}$$

$$
\begin{aligned}
&= \frac{2^{2\epsilon\cdot\ell}}{2^{(\eta_2+g(\ell)/\ell)\cdot\ell}} \cdot \left(\frac{1}{2^{2\epsilon\cdot\ell}\cdot 2^{\ell/2}}\right) \\
&= n^{(2\epsilon-(\eta_2+g(\ell)/\ell))/\delta} \cdot n^{-2} \\
&\geq n^{-2\cdot(1-\widehat{\epsilon})} \text{ for all } \ell \geq \widehat{\ell}_0, \qquad (15)
\end{aligned}
$$

where we have used the fact that $0 < \eta_2 < 2\epsilon$ to obtain the last inequality.

The following lemma shows that 'large' gaps (exponentially larger than n^{-2}) between adjacent elements of the set $\mathcal{F}_n \setminus \mathcal{F}_{n/2^{\beta_2}}$ are very 'rare' (negligible fraction).

Lemma 5. *Fix positive constants β_2, ν, and δ. For any $n = 2^{\delta\cdot\ell}$, and any $\nu' > \nu$ we have*

$$\#\widehat{S}^*_{\delta,\beta_2,\ell}(n^{-(2-\nu')}) = O(n^{2-\nu}).$$

Proof. For brevity, in the following we let $\mathcal{F}$ denote the set $\mathcal{F}_n \setminus \mathcal{F}_{n/2^{\beta_2}}$. For each $x \in \mathcal{F}$, let $d(x) = x - A^-_{\delta,\beta_2,\ell}(x)$ denote the distance to the adjacent element to x in $\mathcal{F}$ in the '-' direction (and $d(0) = 0$). Notice that $\widehat{S}^*_{\delta,\beta_2,\ell}(n^{-(2-\nu)}) = \{x \in \mathcal{F} : d(x) > n^{-(2-\nu)}\}$.

Let X denote a random variable uniformly distributed in $\mathcal{F}$. The expected value of $d(X)$ is

$$E[d(X)] = \frac{1}{\#\mathcal{F}} \cdot \sum_{x\in\mathcal{F}} d(x) < \frac{1}{\#\mathcal{F}},$$

since $\sum_{x\in\mathcal{F}} d(x) = \max_{x\in\mathcal{F}} x < 1$. Now recall that by the Markov inequality, the probability that $d(X)$ exceeds $r \cdot E[d(X)]$ is at most $1/r$ for any $r > 0$. Hence, for any constant $c > 0$, we have:

$$\Pr\left[d(X) \geq \frac{c\cdot n^{\nu}}{\#\mathcal{F}}\right] \leq \Pr\left[d(X) \geq c \cdot n^{\nu} \cdot E[d(X)]\ \right] \leq c^{-1}n^{-\nu}.$$

Since X is uniformly random in $\mathcal{F}$, it follows that

$$\#\widehat{S}^*_{\delta,\beta_2,\ell}\left(c \cdot \frac{n^{\nu}}{\#\mathcal{F}}\right) \leq c^{-1} \cdot n^{-\nu} \cdot \#\mathcal{F} \leq c^{-1} \cdot n^{2-\nu}, \qquad (16)$$

using $\#\mathcal{F} \leq n^2$. Below we will show that $\#\mathcal{F} = \Omega(n^{2-h(\ell)})$ where $h(\ell) = o(\ell)$. Plugging this in (16) we obtain $\#\widehat{S}^*_{\delta,\beta_2,\ell}\left(\frac{n^{\nu+h(\ell)}}{n^2}\right) = O(n^{2-\nu})$ and hence $\#\widehat{S}^*_{\delta,\beta_2,\ell}\left(\frac{n^{\nu'}}{n^2}\right) = O(n^{2-\nu})$ for any any $0 < \nu' < \nu$, as claimed.

It remains to show that $\#\mathcal{F} = \Omega(n^{2-h(\ell)})$ where $h(\ell) = o(\ell)$. Indeed, for every $d' \in [n/2^{\beta_2}, n]$ there are $\varphi(d')$ fractions $k'/d' \in \mathcal{F}$ with $\gcd(k', d') = 1$, and from [7] we know that $\varphi(d') = \Omega(d'/\log\log d') = \Omega(n/\log\log n)$. Since there are $\Omega(n)$ choices for d', we have $\#\mathcal{F} = \Omega(n^2/\log\log n) = \Omega(n^{2-h(\ell)})$ with $h(\ell) = \log\log\delta\ell/(\delta\ell) = o(\ell)$, as required. This completes the proof of the lemma. □

The next lemma shows that, thanks to the uniformly random choice of p and q in $\mathcal{P}_{\ell/2,\beta_1}$ and d in $\mathcal{D}_{\ell,\delta,\beta_2}(\phi)$, the resulting probability distribution of k/d is 'close' to uniform in the set $\mathcal{F}_n \setminus \mathcal{F}_{n/2^{\beta_2}}$.

Lemma 6. *Fix positive constants β_1, β_2 and set $n = 2^{\delta\cdot\ell}$. There exists a positive constant c_7 such that*

$$p^* = \max_{\frac{k'}{d'} \in \mathcal{F}_{2^{\delta\cdot\ell}} \setminus \mathcal{F}_{2^{\delta\cdot\ell-\beta_2}}} \left(\Pr\left[\frac{k}{d} = \frac{k'}{d'}\right]\right) = O\left(n^{-(2-c_7/\log\ell)}\right).$$

Proof. The algorithm RSAKG always generates k and d such that $\gcd(k,d) = 1$ and $\frac{k}{d} \in \mathcal{F}_{2^{\delta\cdot\ell}} \setminus \mathcal{F}_{2^{\delta\cdot\ell-\beta_2}}$. So, in bounding p^* it is enough to consider any fixed k' and d' with $\gcd(k', d') = 1$ and $\frac{k}{d} \in \mathcal{F}_{2^{\delta\cdot\ell}} \setminus \mathcal{F}_{2^{\delta\cdot\ell-\beta_2}}$, and we have $\Pr[k/d = k'/d'] = \Pr[k = k' \text{ and } d = d']$. But from $ed - 1 = k\phi$ we have that $k = -\phi^{-1} \bmod d$ and hence

$$\begin{aligned}
\Pr\left[\frac{k}{d} = \frac{k'}{d'}\right] &= \Pr[-\phi^{-1} \bmod d = k' \text{ and } d = d'] \\
&= \Pr[-\phi^{-1} \bmod d' = k' \text{ and } d = d'] \\
&= \Pr[-\phi^{-1} \equiv k' \pmod{d'} \text{ and } d = d'] \\
&= \Pr[\phi \equiv (-k')^{-1} \pmod{d'} \text{ and } d = d'] \\
&= \Pr[\phi \equiv (-k')^{-1} \pmod{d'}] \cdot \Pr[d = d' | \phi \equiv (-k')^{-1} \pmod{d'}] \quad (17)
\end{aligned}$$

We now upper bound each of the two probabilities in the right-hand side of (17). First we upper bound the probability $\Pr[d = d' | \phi \equiv (-k')^{-1} \pmod{d'}]$. To do so, observe that for any fixed ϕ' in the support of ϕ and any fixed $d' \in \mathbb{Z}$ we have

$$\Pr[d = d' | \phi = \phi'] \leq 1/\#\mathcal{D}_{\ell,\delta,\beta_2}(\phi) \leq p, \quad (18)$$

for some fixed $p = O\left(n^{-(1-\frac{\log\ell}{\delta\cdot\ell})}\right)$, using Lemma 3. Letting Φ denote the set of ϕ' in the support of ϕ satisfying $\phi \equiv (-k')^{-1} \pmod{d'}$, we have

$$\begin{aligned}
\Pr\left[d = d' | \phi \equiv (-k')^{-1} \bmod d'\right] &= \frac{\Pr[d = d' \text{ and } \phi \equiv (-k')^{-1} \pmod{d'}]}{\Pr[\phi \equiv (-k')^{-1} \pmod{d'}]} \\
&= \frac{\sum_{\phi' \in \Phi} \Pr[d = d' \text{ and } \phi = \phi']}{\Pr[\phi \equiv (-k')^{-1} \pmod{d'}]} \\
&= \frac{\sum_{\phi' \in \Phi} \Pr[d = d' | \phi = \phi'] \cdot \Pr[\phi = \phi']}{\Pr[\phi \equiv (-k')^{-1} \pmod{d'}]} \\
&\leq \frac{\sum_{\phi' \in \Phi} p \cdot \Pr[\phi = \phi']}{\Pr[\phi \equiv (-k')^{-1} \pmod{d'}]} \\
&= p = O\left(n^{-(1-\frac{\log\ell}{\delta\cdot\ell})}\right), \quad (19)
\end{aligned}$$

where we used (18) to get the inequality in the fourth line.

Fix $\phi' = (-k')^{-1} \bmod d'$. We now focus on upper bounding $\Pr[\phi \equiv \phi' \pmod{d'}]$. First, observe that $\phi < N < 2^\ell$. So

$$\Pr[\phi \equiv \phi' \bmod d'] \leq \#\{\widehat{\phi} \in \mathbb{Z}_{2^\ell} : \widehat{\phi} \equiv \phi' \pmod{d'}\} \cdot \max_{2^\ell/4 < \widehat{\phi} < 2^\ell} \Pr[\phi = \widehat{\phi}].$$

But

$$\#\{\widehat{\phi} \in \mathbb{Z}_{2^\ell} : \widehat{\phi} \equiv \phi' \pmod{d'}\} = \#\{h \in \mathbb{Z} : h \geq 0 \text{ and } \phi' + h \cdot d' < 2^\ell\} \leq \frac{2^\ell}{d'} + 1.$$

Now recall that $\phi = (p-1) \cdot (q-1)$. So, for any $\widehat{\phi} < 2^\ell$, we have using the uniform distribution of (p,q) in $\mathcal{P}^2_{\ell/2,\beta_1}$, that $\Pr[\phi = \widehat{\phi}] = \#\{(p,q) \in \mathcal{P}^2_{\ell/2,\beta_1} : (p-1)(q-1) = \widehat{\phi}\}/\#\mathcal{P}^2_{\ell/2,\beta_1} \leq \tau(\widehat{\phi})/\#\mathcal{P}^2_{\ell/2,\beta_1}$, where $\tau(\widehat{\phi})$ denotes the total number of divisors of $\widehat{\phi}$. It is known (see Theorem 317 of [4]) that $\tau(\widehat{\phi}) = O\left(2^{2\log(\widehat{\phi})/\log\log(\widehat{\phi})}\right) = O(n^{c_2/\log \ell})$ for some positive constant c_2, using the fact that $2^\ell/4 < \widehat{\phi} < 2^\ell$. Also, from the prime number theorem (see Theorem 6 of [4]), we have that $c_L \cdot x/\ln x < \pi(x) < c_H \cdot x/\ln x$ for any constants $c_L < 1$ and $c_H > 1$ for all sufficiently large x, where $\pi(x)$ denotes the number of primes less than or equal to x. It follows that $\#\mathcal{P}_{\ell/2,\beta_1} = \pi(2^{\ell/2}) - \pi(2^{\ell/2-\beta_1}) = \Omega(2^{\ell/2}/\ell)$ meaning that $\#\mathcal{P}^2_{\ell/2,\beta_1} = \Omega(2^\ell/\ell^2)$. So we conclude that

$$\Pr[\phi = \widehat{\phi}] = O\left(\frac{n^{c_2/\log \ell}}{2^\ell/\ell^2}\right) = O\left(\frac{n^{c_3/\log \ell}}{2^\ell}\right),$$

for some positive constant c_3. Hence, using the fact that $d' \in [n/2^{\beta_2}, n]$, we have

$$\Pr[\phi \equiv \phi' \bmod d'] = O\left(\left(2^\ell/d' + 1\right) \cdot \left(\frac{n^{c_3/\log \ell}}{2^\ell}\right)\right) = O\left(n^{-(1-c_3/\log \ell)}\right). \quad (20)$$

Plugging in (19) and (20) into (17), we finally obtain

$$\Pr\left[\frac{k}{d} = \frac{k'}{d'}\right] = O\left(n^{-(2-c_7/\log \ell)}\right)$$

for some positive constant c_7, as claimed. This completes the proof of the lemma. □

Combining (15) and Lemma 5 we know that (with $n = 2^{\delta \cdot \ell}$) there exists a positive constant ν such that

$$\#\widehat{S}^*_{\delta,\beta_2,\ell}\,(\Delta_{min}/T) = O\left(n^{2-\nu}\right). \quad (21)$$

Using the bounds from Lemma 6 and (21) and the fact that $T = 2^{g(\ell)}$ with $g(\ell)/\ell = o(1)$, we get, for some positive constant ϵ' that

$$T \cdot \#\widehat{S}^*_{\delta,\beta_2,\ell}\,(\Delta_{min}/T) \cdot p^* = O\left(2^{g(\ell)} \cdot n^{2-\nu/2} \cdot n^{-(2-c_7/\log \ell)}\right) = O\left(2^{-\epsilon' \cdot \ell}\right). \quad (22)$$

Finally, plugging in the bounds from (14) and (22) into (9), we conclude that there exist positive constants c and ℓ_0 such that (8) holds. This completes the proof of the theorem. □

6 Conclusions

We obtained converse results to the Wiener attack on low secret-exponent RSA and its extensions. Our results show that the Wiener approach alone cannot lead to a subexponential-time attack when the RSA secret exponent $d > N^{1/4}$. Obtaining converse results for the lattice-based Boneh-Durfee attack and its extensions, which heuristically succeed in polynomial-time when $d < N^{0.292}$, is currently an interesting open problem. We believe our results are a first step towards a solution to this open problem.

Acknowledgements. We would like to thank Igor Shparlinski for helpful discussions and assistance with the proof of Lemma 3. This work was supported by ARC Discovery Grants DP0345366 and DP0451484.

References

1. J. Blömer and A. May. Low Secret Exponent RSA Revisited. In *CaLC 2001*, volume 2146 of *LNCS*, pages 110–125, Berlin, 2001. Springer-Verlag.
2. D. Boneh and G. Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. *IEEE Trans. on Info. Theory*, 46(4):1339–1349, 2000.
3. A. Dujella. Continued Fractions and RSA with Small Secret Exponents. *Tatra Mt. Math. Publ. (to appear)*, 2004. Available at `http://www.math.hr/ duje/papers1.html`.
4. G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, London, 1965.
5. W.J. LeVeque. *Fundamentals of Number Theory.* Dover Publications, New York, 1996.
6. L. Lovász. *An Algorithmic Theory of Numbers, Graphs and Convexity.* Society for Industrial and Applied Mathematics, Philadelphia, 1986.
7. J.B. Rosser and L. Schoenfeld. Approximate Formulas for Some Functions of Prime Numbers. *Illinois. J. Math.*, 6:64–94, 1962.
8. E. Verheul and H. van Tilborg. Cryptanalysis of 'Less Short' RSA Secret Exponents. *Applicable Algebra in Engineering, Communication and Computing*, 8:425–435, 1997.
9. I.M. Vinogradov. *Elements of Number Theory.* Dover Publications, New York, 1954.
10. M.J. Wiener. Cryptanalysis of Short RSA Secret Exponents. *IEEE Trans. on Information Theory*, 36:553–558, 1990.