Cryptanalysis of ‘less short’ RSA Secret Exponents*

Eric R. Verheul
Department of the Interior
P.O. Box 20010
2500 EA, the Hague, the Netherlands
E-mail Eric.Verheul@pobox.com

Henk C.A. van Tilborg
Department of Mathematics and Computing Science
Eindhoven University of Technology
P.O. Box 513
5600 MB, Eindhoven, the Netherlands
E-mail henkvt@win.tue.nl

Abstract

In some applications of RSA, it is desirable to have a short secret exponent d. Wiener [6], describes a technique to use continued fractions (CF) in a cryptanalytic attack on an RSA cryptosystem having a ‘short’ secret exponent. Let $n = p \cdot q$ be the modulus of the system. In the typical case that $G = \gcd(p-1, q-1)$ is small, Wiener’s method will give the secret exponent d when d does not exceed (approximately) $n^{1/4}$.

Here, we describe a general method to compute the CF-convergents of the continued fraction expansion of the same number as in Wiener (which has denominator $d \cdot G$) up to the point where the denominator of the CF-convergent exceeds approximately $n^{1/4}$. When $d < n^{1/4}$ this technique determines d, p, and q as does Wiener’s method. For larger values of d there is still information available on the secret key. An estimate is made of the remaining workload to determine d, p, and q. Roughly speaking this workload corresponds to an exhaustive search for about $2r + 8$ bit, where $r = \ln_2 d/n^{1/4}$.

*To Appear in *Applicable Algebra in Engineering, Computing and Communication*

Key words RSA system, cryptanalysis, continued fractions

Dedicated to Aimo Tietäväinen on the occasion of his 60th birthday

1 Introduction

An RSA system [5] can be described by the modulus n being the product of two (large) primes p, q, and by the public and secret exponents e and d which are related by $e \cdot d \equiv 1 \pmod{\operatorname{lcm}(p-1, q-1)}$. The public exponent e and the modulus n are made public; the remaining parameters are kept secret. In a *typical* RSA system one has that $\gcd(p-1, q-1)$ is small, $e < n$, and p and q have approximately the same number of bits.
It is well-known that factoring the public modulus $n = p \cdot q$ of an RSA system is sufficient to determine the plain-text from cipher-text. Moreover, it is conjectured that any such method, will also give a factorization of n. So actually, it is commonly conjectured that the security of RSA wholly depends on the problem of factoring large numbers.

In some applications of RSA, it is desirable to have a short secret exponent d, as this reduces the execution times. For instance when RSA is used in the communications between a smart card an a larger computer. In [6], an attack on a typical RSA system with a "small" secret exponent is described. This attack will give the secret exponent d (as well as the prime-factors of n), provided that d is 'small'. Here 'small' means that the number of bits in d must not exceed (approximately) one-quarter of the number of bits in n. One of the intriguing aspects of this attack is that it does not only make use of knowledge of the modulus n. Indeed, it also highly depends on information obtained from the public exponent e. So in this situation the problem of breaking RSA is essentially different from the problem of the factorization of n where only information on n is available. Wiener's approach and the present work leads us to disagree with Conjecture 1 in [2] which states that the difficulty of breaking the RSA system is not affected by its exponent value e.

However, a tempting countermeasure against this attack would be to choose a small d (in the order of $n^{1/4}$) and simply *try* the attack: if it succeeds slightly increment the d, otherwise you are safe from it. In the third section of [6, Section VII] the author hints at an extension of his attack that appears to neutralize the effect of this countermeasure. This attack consists of a

binary tree exhaustive key search, the complexity of which consists of about $\ln_2(n) \cdot 2^{2r}$ simple (polynomial time) "guess checks" (see [6, p.556]). Here $r = \ln_2 d/n^{1/4}$. If this attack fails, then no information is gained at all.
In the present paper, we describe a different extension of Wiener's attack. Here we always obtain an amount of "secret" information from n and e in a typical RSA system, i.e. when d is not small. As in [6], our attack will be based on the theory of continued fractions. To be able to describe our cryptanalytic attack in Section 3, we need to derive some properties of continued fractions. This shall be the topic of Section 2.

2 Continued Fractions

One of the important properties of continued fractions is that they provide a representation of (real) numbers different from the standard positional (e.g. decimal) number system. In this section we shall develop some theory concerning continued fractions. For a general background we refer to [1], [3] and [4].
The *continued fraction representation* (or *CF-representation* for short) of a real number x will be denoted by $x = \langle a_0, a_1, \ldots a_m \rangle$, where m may be infinite. Here all a_i, called *partial quotients*, are positive integers, except for a_0 which may be any integer. Moreover, to have unique CF-representations we shall (nearly) always use the *standard* representation, with $a_m \geq 2$ (if m is finite). The number $m+1$ will be called the *length* of the expansion. Numbers with a finite CF-representation are exactly the rational numbers. In our situation, x will always be nonnegative rational number, hence a_0 will be nonnegative. For $0 \leq i \leq m$ the rational number $x_i = \frac{p_i}{q_i} = \langle a_0, \ldots, a_i \rangle$, with p_i and q_i non-negative integers, is called the *i-th convergent* of x. The determination of the terms in the CF-representation of a number x is described in Table 1.
Moreover, the numbers p_i and q_i in the i-th convergent of x are determined by the (well-known) relations described in Table 2. These numbers also satisfy:

$$p_{i-1}q_i - p_i q_{i-1} = (-1)^i, \ i \geq 1. \tag{1}$$

Further, $x_i \leq x$ for i even and $x_i \geq x$ for i odd. Also, the distance $|x_i - x|$ of the i-th convergent to x is a strictly decreasing sequence (up to the length, if that is finite). Two more standard results about continued fractions approximations that we need are the following:

```
$\alpha_0 = x$,
$a_0 = \lfloor \alpha_0 \rfloor$,
$i = 0$,
while $\alpha_i > a_i$ do
    begin
    $i = i + 1$,
    $\alpha_i = 1/(\alpha_{i-1} - a_{i-1})$,
    $a_i = \lfloor \alpha_i \rfloor$,
    end
$m = i$.
```

Table 1: Evaluation of the CF-representation of x

$$\begin{array}{rcll} p_0 & = & a_0, & q_0 = 1, \\ p_1 & = & a_1 a_0 + 1, & q_1 = a_1, \\ p_i & = & a_i p_{i-1} + p_{i-2}, & i \geq 2, \\ q_i & = & a_i q_{i-1} + q_{i-2}, & i \geq 2, \end{array}$$

Table 2: Evaluation of the convergents of x

Proposition 2.1 *Let $x_i = p_i/q_i$ be the i-th convergent of $x = \langle a_0, a_1, \ldots, a_m \rangle$ and let $A(i+1)$ denote $\langle a_{i+1}, a_{i+2}, \ldots, a_m \rangle$. Then, for $2 \leq i < m$*

$$x = \frac{(a_i + 1/A(i+1))p_{i-1} + p_{i-2}}{(a_i + 1/A(i+1))q_{i-1} + q_{i-2}}. \qquad (2)$$

Proposition 2.2 (Best Approximation) *Let $x_i = p_i/q_i$ be the i-th convergent of x and suppose that a/b is a fraction with $|x - \frac{a}{b}| < |x - \frac{p_i}{q_i}|$. Then b is strictly greater than q_i.*

In the rest of this chapter we shall be interested in the relative positions of the convergents of two different rational numbers. So, let $x = p/q$ and $y = u/v$ be two rational numbers. Let the CF-representations of x and y have length $m+1$ resp. $n+1$ and let they be given by $\langle a_0, a_1, \ldots, a_m \rangle$, resp. $\langle b_0, b_1, \ldots, b_n \rangle$. Also denote the i-th convergent of p/q by $x_i,\ 0 \leq i \leq m$, and that of u/v by $y_i,\ 1 \leq i \leq n$. Finally, let $l = \min\{m, n\}$.

Lemma 2.3 *Let the notation be as above and assume that $x < y$. Then $x_i \leq y_i$ for $0 \leq i \leq l$. Moreover, if $m < i \leq n$ then $y_i \geq x$, while if $n < i \leq m$ then $x_i \leq y$.*

Proof: Suppose that the first statement of the lemma is not true. Among all $x = p/q < y = u/v$ for which the first statement of the lemma does not hold, choose p/q and u/v such that the sum of their lengths, $m + n + 2$, is minimal. By assumption there exists a $0 \leq i \leq l = \min\{m, n\}$ with:

$$\langle a_0, a_1, \ldots, a_i \rangle > \langle b_0, b_1, \ldots, b_i \rangle . \tag{3}$$

The condition $p/q < u/v$ implies that $a_0 = \lfloor p/q \rfloor \leq \lfloor u/v \rfloor = b_0$. Hence we must have $1 \leq i \leq l$. On the other hand, inequality (3) implies that $a_0 \geq b_0$, because $a_0 + 1 > \langle a_0, \ldots, a_i \rangle > \langle b_0, \ldots, b_i \rangle \geq b_0$. We conclude that $a_0 = b_0$. By replacing x by $x - a_0$ and y by $y - b_0$ we may assume without loss of generality that $a_0 = b_0 = 0$. Now consider $\langle b_1, \ldots, b_n \rangle$, which equals $1/y$, and $\langle a_1, \ldots, a_m \rangle$, which equals $1/x$. Then

$$\langle b_1, \ldots, b_n \rangle = 1/y < 1/x = \langle a_1, \ldots, a_m \rangle ,$$

$$\langle b_1, \ldots, b_i \rangle > \langle a_1, \ldots, a_i \rangle ,$$

while the sum of the lengths of $1/y$ and $1/x$ equals $m + n$. A contradiction with our assumption on the minimality of the sum of the lengths.

For a proof of the second part of the lemma, let $m < i \leq n$. Let f be the first even number greater than or equal to m. As y_f is smaller than all its successors, it suffices to prove that $y_f \geq x$. To this end, if $f = m$, i.e. if m is even, then this follows from the first part of the lemma. So let m be odd, i.e. $f = m + 1$. Now consider $x^{(A)} :=< a_0, \ldots, a_m, A >$ where A is integer, $A \geq 2$. Then $x^{(A)} < x < y$ and

$$\lim_{A \to \infty} x^{(A)} = x.$$

Moreover, by the first part of the lemma the f-th convergent of $x^{(A)}$, which is $x^{(A)}$ itself, is less than or equal to the f-th convergent of y, so $x^{(A)} \leq y_f$. Hence, by taking limits, $p/q \leq y_f$.
The last part of the lemma follows in a similar way.

□

Lemma 2.4 *Let the notation be as above with $x < y$.*
If $0 \leq i \leq \min\{m - 1, n\}$ and i even then

$$y_i \geq x, \;\; \Rightarrow \;\; x_{i+1} \in [x, y_i], \tag{4}$$

If $0 \leq i \leq \min\{m, n - 1\}$ and i odd then

$$x_i \leq y, \;\; \Rightarrow \;\; y_{i+1} \in [x_i, y], \tag{5}$$

Proof: We only show (4), because (5) can be proved in a similar fashion. First we consider the situation that $i = n$, i.e. $y_n = y$, with $n < m$ and n even. By Lemma 2.3 $x_{n+1} \leq y$. Also, as $n+1$ is odd, $x \leq x_{n+1}$. Hence $x_{n+1} \in [x, y] = [x, y_n]$.

Next, we consider the case that $i < n$, i.e. $y_i \neq y$. Since $i+1$ is odd it follows that $x_{i+1} \geq x$. Now suppose the contrary of (4), i.e. suppose that $x_{i+1} > y_i$. Then, $|y_i - x| < |x_{i+1} - x|$. So by the "best approximation" property of continued fractions we conclude that the denominator of y_i is strictly larger than that of x_{i+1}.

On the other hand, we claim that $|x_{i+1} - y| < |y_i - y|$. This directly results in a contradiction. Indeed, from the "best approximation" property of continued fractions it now follows that the denominator of x_{i+1} is strictly larger than that of y_i.

So let us show the claim. If $x_{i+1} \leq y$ the claim is evidently true. So assume that $x_{i+1} > y$. By Lemma 2.3 this actually implies that $y < x_{i+1} \leq y_{i+1}$. Hence $|x_{i+1} - y| \leq |y_{i+1} - y| < |y_i - y|$.

□

Theorem 2.5 *Let the notation be as above with $x < y$. Then, for each i, $0 \leq i \leq l = \min\{m, n\}$, the following conditions are equivalent :*

$$x_i \neq y_i \tag{6}$$

$$y_i \in (x, y], \textit{ if } i \textit{ is even, and } x_i \in [x, y) \textit{ if } i \textit{ is odd,} \tag{7}$$

$$|y - y_i| < |y - x|, \textit{ if } i \textit{ is even, and } |x_i - x| < |y - x| \textit{ if } i \textit{ is odd.} \tag{8}$$

Proof: Recall that $y_i \leq y$ for i even and $x_i \geq x$ for i odd. Hence, the equivalence of (7) and (8) follows readily.

Similarly, $x_i \leq x$ for i is even and $y_i \geq y$ for i odd. So if i is even and $y_i \in (x, y]$, it follows that $x_i \neq y_i$. The case that i is odd goes similarly. This proves the implication (7) $\Rightarrow$ (6).

We are left with the proof of the implication (6) $\Rightarrow$ (7). Let j be the first number in $\{0, \ldots, l\}$ for which $x_j \neq y_j$. Then j is also the first number in $\{0, \ldots, l\}$ with $a_j \neq b_j$. Further (6) implies that $i \geq j$.

We first show that (6) implies the following:

$$y_j \in (x, y], \text{ if } j \text{ is even,} \tag{9}$$

$$x_j \in [x, y), \text{ if } j \text{ is odd.} \tag{10}$$

Let us prove (10) by the method of contradiction. So, suppose that j is odd (hence $x_j \geq x$) and that $x_j \geq y$.
By construction of j this implies that

$$\langle b_0, b_1, \ldots, b_n \rangle = y \leq x_j = \langle a_0, a_1, \ldots, a_{j-1}, a_j \rangle = \langle b_0, b_1, \ldots, b_{j-1}, a_j \rangle .$$

As j is odd one obtains $b_j \geq a_j$.
On the other hand, by Lemma 2.3 $x_j \leq y_j$. By construction of j this means:

$$\langle b_0, b_1, \ldots, b_{j-1}, a_j \rangle = \langle a_0, a_1, \ldots, a_{j-1}, a_j \rangle \leq \langle b_0, b_1, \ldots, b_{j-1}, b_j \rangle .$$

As j is odd one obtains $a_j \geq b_j$. Together with the previous result we conclude that $a_j = b_j$, contradicting our assumption on j.
Inequality (9) can be proven similarly.
It remains to be shown that (9) and (10) imply (7) (for $i \geq j$). We shall only do this for j odd, since the even case again can be handled in the same way.
We distinguish two cases. If i is also odd, then by (10), $x_i \in [x, x_j] \subset [x, y)$, as the odd convergents are descending. If i is even, then $l \geq i > j$. According to Lemma 2.4 (because $x_j \leq y$) $y_{j+1} \in [x_j, y] \subset (x, y]$. Therefore, $y_i \in [y_{j+1}, y] \subset (x, y]$, as the even convergents are increasing.

□

The equivalence of conditions (6) and (8) in Theorem 2.5 shall be the key for obtaining information on the secret key in the RSA system from the public information e and n.

Let x, y be the rational numbers as introduced at the beginning of Section 2. Suppose that $x = p/q < y = u/v$ are close to another. other. If $|y - x|$ is small enough then the first partial quotients a_0 (of x) and b_0 (of y) will coincide. Actually, if $|y - x|$ is small enough then up to a certain index, say t with $0 \leq t \leq l = \min\{m, n\}$, all i-th partial quotients of x and y will coincide.
Evidently, if both x and y (or equivalently x and $|y-x|$) are known then the value of t can easily be found by simply comparing the CF-representations of x and y. Another, and more elaborate, method would be to use Theorem 2.5. Indeed, by this result t is simply the largest $j \in \{0, \ldots, l\}$ with $|x_j - x| \geq |y - x|$ if j is odd and $|y - y_j| \geq |y - x|$ if j is even.

This brings us to the following type of problem. Suppose we only know x and we would like to know y, $y > x$. Let u be some (nice) upperbound of

$|y-x|$. Suppose that we have a technique to determine j, the largest odd integer in $\{1,\ldots,l\}$ satisfying:

$$|y-x| \leq u \leq |x_j - x|. \tag{11}$$

It follows from Theorem 2.5 that all a_i, b_i and x_i, y_i coincide up to j, i.e. a lowerbound of t is determined. Hence, in such a fashion one obtains information of the CF-representation of y. Similarly, lowerbounds of $|y-x|$ can be used to obtain upperbounds of t.

Observe however that we have just used some implicit information on (the unknown) y, namely on its CF-length n. As an alternative to this, one might determine the largest odd number, j, from $\{1,\ldots,m\}$ that satisfies inequality (11). The question now arises whether all a_i, b_i and x_i, y_i coincide up to j. By Theorem 2.5 this is the case except when the found odd value of j is not larger than n. So, let us analyze the situation that for an odd value of j, $j > n$, inequality (11) holds. Since $j \leq m$, it follows that in this case $n < j \leq m$. This implies that either

$$|y-x| \leq |x_n - x| \text{ and } n \text{ is odd,}$$

or

$$|y-x| \leq |x_{n-1} - x| \text{ and } n \text{ is even.}$$

By Theorem 2.5, the first possibility gives rise to the relation $x_n = y_n = y$, which contradicts the assumption that $j > n$.
With the second possibility, Lemma 2.3 implies $x_{n+1} \leq y$, hence, as $n+1$ is odd, $x_{n+1} \in [x,y]$. Therefore, the second possibility gives rise to two sub-cases, namely $x_{n+1} \in [x,y)$, which violates $j > n$, or $x_{n+1} = y$. From the latter it follows that $y_{n+1} = y$, as $x_{n+1} = y_{n+1}$ by Theorem 2.5 and $j \geq n+1$. In particular it also follows that the upperbound u of $|y-x|$ actually equals $|y-x|$. One might argue that this is not very likely to occur, but let us analyze it a little further.
First observe that $j \leq n+2$ as $|x - x_{n+3}| < |x - x_{n+1}| = |x-y|$. Moreover, since n is even and j odd, it follows that $j = n+1$. So, we end up with two different CF-representations of y: the original (standard) one and the (longer) one formed by the partial quotients of x up to $n+1$. This means that the last representation is not standard, i.e. the last partial quotient of the last representation equals 1. Hence, in the CF-representation of y where the last partial quotient is decremented one and one extra partial quotient

1 is added, all partial quotients (and convergents) up to $n+1$ coincide. So the a_i, b_i and x_i, y_i obtained above are essentially correct.

As an illustration of the last, one could consider $x = \langle 0,1,1,1,2\rangle$ and $y = \langle 0,1,2\rangle = \langle 0,1,1,1\rangle$.

The above discussion leads to the first part of the following result.

Theorem 2.6 *Let $x < y$ and let u be an upperbound of $|y-x|$. If j is the largest* **odd** *number in $\{1,\dots,m\}$ satisfying inequality*

$$|y-x| \leq u \leq |x_j - x|,$$

then either $x_j = y$ or all partial quotients and convergents of x and y coincide up to j.
Moreover, if q_j denotes the denominator of the j-th convergent of x, then the largest odd number j' in $\{1,\dots,m\}$, such that

$$q_{j'} \leq \frac{1}{\sqrt{u}},$$

is a lowerbound of j.

Proof: The last part of the theorem directly follows from the well-known inequality $|x_j - x| < 1/(q_j)^2$, cf. [3, p.341].

□

The following simple result is helpful when applying the previous theorem in the context of the RSA system.

Lemma 2.7 *Let $0 < x < y$, and let δ be such that $x = (1-\delta)y$. Also let δ_{max} (resp. δ_{min}) be an upperbound (resp. non-negative lowerbound) of δ. Then,*

$$|y-x| \leq \frac{\delta_{max}}{1-\delta_{min}} \cdot x, \tag{12}$$

$$\textit{if } y \leq 1 \textit{ then } |y-x| \leq \delta_{max}. \tag{13}$$

Proof: Inequality (12) follows from the relation $(y-x) = \frac{\delta}{1-\delta}x$. The other inequality follows from inequality (12) and $x/(1-\delta_{min}) \leq y \leq 1$.

□

We remark that Theorem 2.6 can be readily modified to the situation where x is unknown, y is known and bounds on $|y-x|$ or δ (in the sense of Lemma 2.7) are available.

3 Cryptanalysis of RSA

In the context of RSA we have the following (cf. [6]). There exists an integer K such that:

$$e \cdot d = 1 + K \cdot \mathrm{lcm}(p-1, q-1) = 1 + \frac{K}{G}(p-1)(q-1), \tag{14}$$

where $G = \gcd(p-1, q-1)$. Equivalently,

$$\begin{aligned} \frac{e}{pq} &= \frac{K(p-1)(q-1)}{dGpq} + \frac{1}{dpq} = \frac{K}{dG}\left(\frac{pq - p - q + 1 + \frac{G}{K}}{pq}\right) \\ &= \frac{K}{dG}(1-\delta) = \frac{k}{dg}(1-\delta), \end{aligned}$$

where

$$\delta = \frac{p + q - 1 - \frac{g}{k}}{pq}.$$

and the fraction k/dg is a reduced representation of K/dG, i.e. $k = K/\gcd(K,G)$ and $g = G/\gcd(K,G)$ (note that (14) implies that $\gcd(K,d) = 1$). This brings us to the theory of the previous section with $x = e/pq$ and $y = k/dg$. In a *typical* RSA-system, one may expect g to be very small. For instance, when p and q are strong primes (i.e. of the form two times a prime plus one), the value of g will be 1 or 2. Also, from (14) and $e < pq$ it follows that $k = d \cdot g \cdot e/(p-1)(q-1) - g/(p-1)(q-1) \leq dg$, i.e. $y = k/dg \leq 1$.

As $\sqrt{2 \cdot p \cdot q} \leq p + q$, the quantity $\sqrt{2}/\sqrt{n}$ always yields a lowerbound of δ. Assume without loss of generality that $p < q$. Then the quantity $2/p$ yields an upperbound of δ. Moreover, as the number of bits in p and q typically differ by a small number, say 2, the last upperbound of δ can be approximated by $2/y$ where y equals $\sqrt{n}$ with a small number of bits, say 1, removed. Therefore, we obtain upper and lowerbounds of δ approximately of size $1/\sqrt{n}$ ($\delta_{min} \approx \sqrt{2}/\sqrt{n}$, and $\delta_{max} \approx 4/\sqrt{n}$). Consequently, $4/\sqrt{n}$ is an upperbound of $|y - x|$ by the second part of Lemma 2.7.

By using Theorem 2.6, the CF-representation and convergents of k/dg can now be determined up to the point j where the number of bits in the denominator of the convergent is approximately one quarter of the number of bits in n. In particular, if $d < n^{1/4}$ it can be determined completely. This is the result of Wiener [6]. Above that bound Wiener's method fails to give any (partial) information. The derivations before show that in general the convergents of k/dg are known up to the point that the denominator is about $n^{1/4}$.

Consider a non-standard RSA system where e is taken larger than n by adding suitable many multiples of $\text{lcm}(p-1, q-1)$ to it. In this situation, denote $e = n^{\theta}$ with $\theta > 1$. Then, by the first part of Lemma 2.7, $n^{\theta - 1.5}$ yields an upperbound of $|y - x|$. As explained above, the CF-representation and convergents of k/dg can be determined up to the point j where the number of bits in the denominator of the convergent is approximately $(\theta/2 - 0.75)\ln_2(n)$. So in this situation the Wiener type of attacks are less successful than in the standard situation. Moreover, if $\theta \geq 1.5$ these attacks give no information at all. Compare [6, Section VI].

Let us analyze what kind of information the above approach yields in general for a standard RSA system, e.g., how much more information is needed to determine d, p, and q. To this end, write $x = e/pq$ with CF-representation $\langle a_0, a_1, \ldots, a_m \rangle$ and successive convergents $x_i = p_i/q_i$ and $y = k/dg$ with CF-representation $\langle b_0, b_1, \ldots, b_n \rangle$ and successive convergents $y_i = u_i/v_i$. Assume that u an upperbound on $|y - x|$, the integer j is the maximum odd integer for which

$$|y - x| \leq u \leq |x_j - x|. \tag{15}$$

Since $x < y$, it follows that $a_{j+1} \leq b_{j+1}$. Put $b_{j+1} = a_{j+1} + \Delta$. Further, let $B(j+2)$ be defined by $\langle b_{j+2}, \ldots, b_n \rangle$. Write $B(j+2) = U/V$ with $\gcd(U, V) = 1$. Note that $U \geq V$. Combining the above we get

$$b_{j+1} + \frac{1}{B(j+2)} \;=\; a_{j+1} + \Delta + V/U.$$

It follows from (2) and the equalities of the convergents up to j that

$$\begin{aligned}
\frac{k}{dg} &= \frac{(a_{j+1} + \Delta + V/U)p_j + p_{j-1}}{(a_{j+1} + \Delta + V/U)q_j + q_{j-1}} = \frac{(a_{j+1}p_j + p_{j-1}) + (\Delta + V/U)p_j}{(a_{j+1}q_j + q_{j-1}) + (\Delta + V/U)q_j} \\
&= \frac{p_{j+1} + (\Delta + V/U)p_j}{q_{j+1} + (\Delta + V/U)q_j} = \frac{p_{j+1}U + (U\Delta + V)p_j}{q_{j+1}U + (U\Delta + V)q_j}. \qquad (16)
\end{aligned}$$

We claim that the numerator, denoted by N, and the denominator, denoted by D, of the righthand side of equality (16) are relatively prime, so $N = k$ and $D = dg$. To prove this, consider the following equalities:

$$\begin{aligned} q_{j+1}N - p_{j+1}D &= q_{j+1}(p_{j+1}U + (U\Delta + V)p_j) \\ &\quad - p_{j+1}(q_{j+1}U + (U\Delta + V)q_j) \\ &= q_{j+1}(U\Delta + V)p_j - p_{j+1}(U\Delta + V)q_j \\ &= (U\Delta + V)(q_{j+1}p_j - p_{j+1}q_j) \\ &= \pm(U\Delta + V). \qquad (17) \end{aligned}$$

The last equality follows from equality (1); the other equalities are straightforward verifications. From equality (17) it follows that any common denominator C of N and D must divide $(U\Delta + V)$. By the form of N and D it follows that C must divide $p_{j+1}U$ and $q_{j+1}U$, that is C must divide U, and consequently it must divide $V = (U\Delta + V) - U\Delta$. Hence, C is a common denominator of U and V, so $C = 1$ by assumption. This finishes the proof of the claim.

Now by virtue of equality (16), any guess of Δ, V and U $(U \geq V)$, gives an estimate for k/dg. In [6] a polynomial time test is described to verify whether such an estimate is correct. If so, this test also produces the secret d, p and q.

Using the estimate $u = 4/\sqrt{n}$, the integer j defined in (15) satisfies

$$|x_{j+2} - x| < 4/\sqrt{n}. \qquad (18)$$

On the other hand, writing $A(j+3) =< a_{j+3}, \ldots, a_n >$, and thus having $a_{j+3} \leq A(j+3) \leq a_{j+3} + 1$ one has by (2) and (1)

$$\begin{aligned} |x - x_{j+2}| &= \left| \frac{A(j+3)p_{j+2} + p_{j+1}}{A(j+3)q_{j+2} + q_{j+1}} - \frac{p_{j+2}}{q_{j+2}} \right| = \\ &= \left| \frac{p_{j+1}q_{j+2} - p_{j+2}q_{j+1}}{q_{j+2}(A(j+3)q_{j+2} + q_{j+1})} \right| = \\ &= \left| \frac{1}{q_{j+2}(A(j+3)q_{j+2} + q_{j+1})} \right| = \\ &\geq \left| \frac{1}{q_{j+2}((a_{j+3}+1)q_{j+2} + q_{j+1})} \right|. \qquad (19) \end{aligned}$$

In [3, page 352] the distribution of the partial quotients a_i of a random real $x =< a_0, a_1, \ldots, a_n >$ is given. Approximately a_i will be 1 with probability

41.5%, $a_i = 2$ with probability 17.0%, etc. Since $q_{j+2} = a_{j+2}q_{j+1} + q_j$ by Table 2 one can now estimate q_{j+2} by $2q_{j+1}$. So the righthand side in (19) is about $1/10q_{j+1}^2$. It now follows from (19) and (18) that (approximately and with (reasonable) probability 20%)

$$4/n^{1/2} > |x_{j+2} - x| \geq 1/10q_{j+1}^2.$$

We conclude that $q_{j+1} > n^{1/4}/7$, or, alternatively, the number of bits in the binary representation of q_{j+1} is at least one quarter of those in $n^{1/4}$ (minus 3).
Finally, since g is small (very likely $g = 1, 2$), the number of bits of dg is that of d plus one. To estimate the complexity of our method for $d > n^{1/4}$, we define

$$\ln_2 d = \ln_2 n^{1/4} \ + \ r.$$

It follows from (16) and the claim following it, that $q_{j+1}U$ must be less than or equal to dg. So, $\ln_2 U + \ln_2 n^{1/4} - 3 \ \leq \ \ln_2 n^{1/4} \ + \ r \ + \ 1$. It follows that

$$\ln_2 U \leq r + 4.$$

Since $V \leq U$ the same inequality applies to V. Now, the value of Δ is small in general, because of two reasons. First, because $\Delta = b_{j+1} - a_{j+1}$ and the values of the partial quotients are small as we already observed before. Second, in 50 percent of the cases the (maximal) position up to where the partial quotients of x and y coincide, will be even; in which case Δ is zero. We conclude that in view of (16), the uncertainty about k/dg and thus about d, p, and q is about $2r + 8$ bits. Note that this is about a factor $\ln_2 n$ better than Wiener's extension as described in the introduction.

We have implemented the above approach with Arjen K. Lenstra's Freelip multi-precision integer library. That is, we have calculated the odd convergents x_i of e/pq up to the point where $u \leq |e/pq - x_i|$ and then searched the remaining information on d, p and q by exhaustive search. For u (an upperbound of $|e/pq - k/dg|$) we used $u = 1/\sqrt{n}$, which is actually a bit too small. However, it turned out that taking this u gave rather satisfactory results: the predicted coincidence of odd convergents of e/pq and k/dg almost never exceeded the real coincidence. Actually, the predicted coincidence often equaled the real coincidence (i.e. gave the optimal result).
As an illustration, consider

$$pq = 318776675486242237348233 \quad \text{and} \quad e = 71151678048087652104.$$

Then $u = 1/178543181187$. The largest odd i for which $u \leq |x - x_i|$ equals 7; the 7-th convergent of e/pq equals 1493/6689, and the 8-th convergent equals 34668/155321. In view of equality (16), this means that

$$\frac{k}{dg} = \frac{34668U + (U\Delta + V)1439}{155321U + (U\Delta + V)6689}. \tag{20}$$

Then an exhaustive search for U, Δ and V $(\leq U)$ together with Wiener's polynomial time test for an estimate of k/dg yields $U = 21$ (5 bits), $V = 5$ (3 bits), $\Delta = 0$, $g = 2$, $d = 1647593$ (21 bits), $p = 119922166271$ (37 bits) and 265819644023 (38 bits). Hence, an exhaustive search for 8 bit had to be performed. As the number of bits d is 3 more than that in $n^{1/4}$, this is consistent with the above estimate. Also observe that the 9-th convergent of e/pq (=174833/783294)and k/dg (=140165/627973) differ; hence Wiener's original method is not successful here.

4 Conclusion

We have described an extension of Wiener's attack [6]. The remaining complexity in determining the secret key d and the factorization of the modulus n corresponds to an exhaustive search of about $2r{+}8$ bit, where $r = \ln_2 d/n^{1/4}$. Contrary to the extension suggested in [6, Section VII], we always obtains an amount of "secret" information from n and e in a typical RSA system, even when d is not small. Also our attack is about a factor $\ln_2 n$ better than Wiener's extension. These forms of attacks are less successful on (non-typical) RSA systems with $e > n$. In fact, if $e \geq n^{1.5}$ no useful information is gained at all.

References

[1] H. Davenport, *The Higher Arithmetic,* 5th ed., Cambridge University Press, 1981.

[2] K. Koyama, *Direct demonstration of the power to break public-key cryptosystems*, in Advances in Cryptology – AUSCRYPT'90 (ed. J. Seberry and J. Pieprzyk), Lecture Notes in Computer Science 453, Springer–Verlag, Berlin etc., pp. 14–21, 1990.

[3] D. Knuth, *The Art of Computer Programming: Volume 2, Seminumerical Algorithms,* 2-nd edition, Addison-Wesley, 1981.

[4] O. Perron, *Die Lehre von den Kettenbruchen,* 3rd ed. (Stuttgart: Teubner, 1954), 2 vols.

[5] R.L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital and public key Cryptosystems,* Commun. ACM. vol. 21, no. 2, pp. 158-164, Feb. 1978.

[6] M.J. Wiener, *Cryptanalysis of Short RSA Secret Exponents,* IEEE Transactions on Information Theory, IT–36, May 1990, pp. 553-558.